

---

# **QBDI Documentation**

***Release 0.8.1-devel***

**Quarkslab**

**Mar 28, 2022**



# CONTENTS

<b>1</b>	<b>Status</b>	<b>3</b>
<b>2</b>	<b>Contents</b>	<b>5</b>
2.1	Introduction . . . . .	5
2.2	Installation and Integration . . . . .	6
2.3	Getting Started . . . . .	12
2.4	Tutorials . . . . .	36
2.5	API . . . . .	49
2.6	Architecture Support . . . . .	158
2.7	Developer Documentation . . . . .	162
2.8	CHANGELOG . . . . .	189
2.9	References . . . . .	195
<b>3</b>	<b>Indices and Tables</b>	<b>197</b>
	<b>Index</b>	<b>199</b>



Quarkslab Dynamic binary Instrumentation (QBDI) is a modular, cross-platform and cross-architecture DBI framework. It aims to support Linux, macOS, Android, iOS and Windows operating systems running on x86, x86-64, ARM and AArch64 architectures. In addition of C/C++ API, Python and JS/frida bindings are available to script QBDI. Information about what is a DBI framework and how QBDI works can be found in the [documentation introduction](#).

QBDI modularity means it doesn't contain a preferred injection method and it is designed to be used in conjunction with an external injection tool. QBDI includes a tiny (LD\_PRELOAD based) Linux and macOS injector for dynamic executables (QBDIPreload). QBDI is also fully integrated with [Frida](#), a reference dynamic instrumentation toolkit, allowing anybody to use their combined powers.

A current limitation is that QBDI doesn't handle signals, multithreading (it doesn't deal with new threads creation) and C++ exception mechanisms. However, those system-dependent features will probably not be part of the core library (KISS), and should be integrated as a new layer (to be determined how).



## STATUS

CPU	Operating Systems	Execution	Memory Access Information
x86-64	Android, Linux, macOS, Windows	Supported	Supported
x86	Android, Linux, macOS, Windows	Supported	Supported
ARM	Linux, Android, iOS	Planned (*)	Planned (*)
AArch64	Android, Linux, macOS	Supported (*)	Supported (*)

\* The ARM and AArch64 instruction sets are supported for internal use at the moment.

**stable**

**dev**





## CONTENTS

## 2.1 Introduction

### 2.1.1 Why a DBI?

Debuggers are a popular approach to analyze the execution of a binary. While those tools are convenient, they are also quite slow. This performance problem is imperceptible to human users but really takes its toll on automated tools trying to single step through a complete program. Such automated tools are useful for tracking the evolution of the program states, extracting execution statistics and verifying that some runtime conditions hold true. Examples of usage include memory corruption debuggers, profilers, timeless debuggers and side-channel attack tools.

This performance cost is due to the kernel playing the role of a middleman between the debugger and the debuggee. The only way to get rid of the problem is to place the tool inside the binary being analyzed and this is what Dynamic Binary Instrumentation does: injecting instrumentation code inside the binary at runtime.

### 2.1.2 Why QBDI?

Existing DBI framework were designed more than 15 years ago, focusing on features and platforms that made sense at the time. Mobile platform support is often unstable or inexistent and instrumentation features are either simplistic or buried in low-level details.

QBDI attempts to retain the interesting features of those frameworks while avoiding their pitfalls and bringing new designs and ideas. Its goal is to be a cross-platform and multi-architectures modular DBI framework. The modular design exposes the DBI engine as a library that can start an instrumented execution anywhere, anytime and easily be incorporated in other tools.

### 2.1.3 QBDI : How does it work?

The core of DBI frameworks relies on the Just-In-Time (JIT) recompilation of the original program. This allows to interleave additional assembly code which can instrument any part of the execution. The DBI engine performing the JIT recompilation and the JITed code itself run in the same process but need to each have their own processor context. This requires to perform context switches between the two like a virtual machine would. We thus call the DBI context the **host** and the original program context the **guest**.

The **host** is composed of QBDI components and the **instrumentation tool**. The **instrumentation tool** is the code written by the user which interacts with the **QBDI VM** through a **C API** or a **C++ API**. The **instrumentation tool** can register **callbacks** to occur on specific events triggered either by QBDI or by the instrumentation code inserted inside the original program. The user documentation further details these APIs and how callbacks work.

Inside the VM resides the **QBDI Engine** which manages the instrumented execution. The engine runs the JIT loop which reads the **original program** code and generates the **instrumented code** which is then executed. Each loop iteration operates on a basic block, a sequence of instructions which ends with a branching instruction. This basic block is first patched, to accommodate the JIT process, and then instrumented as instructed by the instrumentation tool. This instrumented basic block is written in executable memory, executed and returns the address of the next basic block to execute. To avoid doing twice the same work, this **instrumented code** is actually written in a code cache.

## 2.1.4 Limitations

The **host** and the **guest** share the same process and thus the same resources. This means that they use the same heap and the same libraries and this will cause issues with any non-reentrant code. We could have chosen to shield users from those issues by forbidding instrumentation tools to use any external libraries like some other DBI frameworks have done. However we believe this is an overblown issue and that there are effective mechanisms to mitigate the problem. Nonetheless users need to be aware of this design limitation and the mitigations side-effects.

For example, tracing the heap memory allocator will cause deadlocks because it is not reentrant. There are other problematic cases but they are mostly limited to the standard C library and the OS loader. To avoid such issues we have an execution brokering system that allows to whitelist/blacklist specific pieces of code. These will be executed outside of the instrumentation process via a call hooking mechanism. This execution broker system is documented in the [API description](#).

Moreover, the **host** relies on the loader loading and initializing its library dependencies which means the instrumentation process cannot be started before the loader has finished its job. As a result the loader itself cannot be instrumented.

## 2.2 Installation and Integration

### 2.2.1 C/C++ API installation

When a new stable version of QBDI is released, prebuilt packages can be downloaded through the [release page](#) on Github. In order to make sure you have downloaded the right package, you can verify its integrity with the file SHA256.

A GPG signature of SHA256 by our [developer key](#) (2763 2215 DED8 D717 AD08 477D 874D 3F16 4D45 2193) is available in SHA256.sig.

```
# check the hash of the prebuilt package
sha256 -c SHA256

# verify the signature
wget https://qbdi.quarkslab.com/qbdi.asc -O - | gpg --import -
gpg --verify SHA256.sig
```

### Debian / Ubuntu

Debian and Ubuntu packages are provided for stable and LTS releases, and can be installed using dpkg:

```
dpkg -i QBDI-**-X86_64.deb
```

## Arch Linux

Arch Linux packages can be installed using `pacman`:

```
pacman -U QBDI-**-X86_64.tar.zst
```

## macOS

A software installer is provided for macOS. Opening the `.pkg` in Finder and following the instructions should install QBDI seamlessly.

## Windows

A software installer is provided for Windows. Running the `.exe` and following the instructions should install QBDI seamlessly.

## Android

The Android package is an archive you solely need to extract. Afterwards, you have to manually push the files onto the device.

## Devel packages

Devel packages embed the latest features the developers are currently working on for the next release (available on the [dev-next branch](#)). It's worth mentioning that since some parts are still under development, those are likely to be **unstable** – you must be aware that it may contain some bugs and are not as reliable as release packages.

- [Windows devel packages](#)
- [Linux \(Ubuntu\) devel packages](#)
- [Android devel packages](#)
- [OSX devel packages](#)

### 2.2.2 PyQBDI installation

Every time a new stable release of PyQBDI is available, it is automatically pushed onto the [PyPI platform](#), thus can be easily installed with `pip` (`>= 19.3`).

```
pip install --user --update pip
pip install --user PyQBDI
```

If you want to use a devel version, download the corresponding prebuilt wheel file and run the following commands:

```
pip install --user --update pip
pip install --user PyQBDI-*.whl
```

The devel wheel files which contain the latest versions of the [dev-next branch](#) are available at:

- [PyQBDI for Windows](#)
- [PyQBDI for Linux](#)

- [PyQBDI for OSX](#)

---

**Note:** Only Python3 is supported. If you need to use Python2, we recommend using QBDI 0.7.0 instead.

---

---

**Note:** A 32-bit version of Python is needed if you want to use PyQBDI on x86 targets.

---

### 2.2.3 Frida/QBDI installation

QBDI can be used alongside Frida to make it even more powerful. This feature is included in the C/C++ package. Using it requires having Frida installed ( $\geq 14.0$ ) on your workstation as well as [frida-compile](#) for compiling your scripts.

```
# install Frida
pip install frida-tools

# install frida-compile and add the binary directory to your PATH env variable
npm install frida-compile babelify
export PATH=$PATH:$(pwd)/node_modules/.bin
```

#### Android target

In order to use Frida/QBDI on an Android device, the Frida server must be running on the target device and the `libQBDI.so` library have to be placed in `/data/local/tmp`.

---

**Note:** Latest Frida server binaries are available on the [Frida official release page](#).

---

### 2.2.4 Docker Linux images

The Docker image is available on [Docker Hub](#). It has been built to keep it as small as possible so it does not contain any compiler. You have to install the needed application or modify the following Dockerfile according to your needs.

```
FROM qbdi/qbdi:x86_ubuntu

ENV USER="docker" \
    HOME="/home/docker"

# install some needed tools
RUN apt-get update && \
    apt-get upgrade -y && \
    apt-get install -y \
        build-essential \
        cmake \
        libstdc++-8-dev \
        python \
        python-dev \
        #gdb \
        #vim \
```

(continues on next page)

(continued from previous page)

```

    sudo \
    bash && \
    apt-get clean && \
    rm -rf /var/lib/apt/lists/*

# create a user
RUN adduser --disabled-password --gecos '' $USER && \
    adduser $USER sudo && \
    echo '%sudo ALL=(ALL) NOPASSWD:ALL' >> /etc/sudoers

# switch to new user
USER $USER
WORKDIR $HOME

# TODO : Add yours needed files
#ADD --chown=$USER . $HOME/

CMD ["/bin/bash"]

```

To run the container, we recommend allowing the usage of PTRACE which is mandatory to use QBDIPreload.

```
docker run -it --rm --cap-add=SYS_PTRACE --security-opt seccomp:unconfined <image> bash
```

## 2.2.5 Compilation from source code

To build this project, the following dependencies are needed on your system:

- cmake >= 3.12
- ninja or make
- C++17 toolchain (gcc, clang, Visual Studio 2019, ...)

The compilation is a two-step process:

- local library distribution of LLVM is built.
- QBDI is built using the LLVM library.

This local built of LLVM is required because QBDI uses private APIs not exported by regular LLVM installations and because our code is only compatible with a specific version of those APIs. This first step is cached and only needs to be run once, subsequent builds only need to repeat the second step.

QBDI build system relies on CMake and requires to pass build configuration flags. To help with this step we provide shell scripts for common build configurations which follow the naming pattern `config-OS-ARCH.sh`. Modifying these scripts is necessary if you want to compile in debug mode or cross-compile QBDI.

## Linux

### x86-64

Create a new directory at the root of the source tree, and execute the Linux configuration script:

```
mkdir build
cd build
../cmake/config/config-linux-X86_64.sh
ninja
```

### x86

You can follow the same instructions as for x86-64 but instead, use the `config-linux-X86.sh` configuration script.

## macOS

Compiling QBDI on macOS requires a few things:

- A modern version of **macOS** (like Sierra)
- **Xcode** (from the *App Store* or *Apple Developer Tools*)
- the **Command Line Tools** (`xcode-select --install`)
- a package manager (preferably **MacPorts**, but *HomeBrew* should also be fine)
- some packages (`port install cmake wget ninja`)

Once requirements are met, create a new directory at the root of the source tree, and execute the macOS configuration script:

```
mkdir build
cd build
../cmake/config/config-macOS-X86_64.sh
ninja
```

## Windows

Building on Windows requires a pure Windows installation of *Python 3* (from the official packages, this is mandatory) in order to build our dependencies (we really hope to improve this in the future). It also requires an up-to-date CMake and Ninja.

First of all, the Visual Studio environment must be set up. This can be done with a command such as:

```
"C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\VC\Auxiliary\Build\  
↪vcvarsall.bat" x64
```

Then, the following commands must be run:

```
mkdir build
cd build
python ../cmake/config/config-win-X86_64.py
ninja
```

## Android

Cross-compiling for Android requires the NDK (or the SDK) to be installed on your workstation. For now, it has only been tested under Linux. If not already installed, you can download the latest Android NDK package through the [official website](#) and extract it. Afterwards, the `config-android-*.sh` configuration script needs to be customised to match your NDK installation directory and the target platform.:

```
# Configure and compile QBDI X86_64 with a NDK
mkdir build && cd build
NDK_PATH=<your_NDK_PATH> ../cmake/config/config-android-X86_64.sh
ninja

# Configure and compile QBDI X86 with a SDK
mkdir build && cd build
ANDROID_SDK_ROOT=<your_SDK_PATH> ../cmake/config/config-android-X86.sh
ninja
```

## PyQBDI compilation

The PyQBDI library (apart from the wheel package) can be built by solely passing the ‘**DQBDI\_TOOLS\_PYQBDI=ON**’ option to the CMake build system.

However, if you want to build the wheel package, you can run these commands:

```
python -m pip install --upgrade pip
python -m pip install setuptools wheel
python setup.py bdist_wheel
```

A 32-bit version of Python is mandatory for the X86 architecture whereas a 64-bit one is required for the X86-64 architecture.

## 2.2.6 CMake integration

### Single architecture

If you want to use only one architecture of QBDI in your CMake project, you can import the QBDI and QBDIPreload packages:

```
find_package(QBDI REQUIRED)
find_package(QBDIPreload REQUIRED) # if available for your current platform
# or
find_package(QBDI REQUIRED HINTS "${EXTRACT_DIRECTORY}" NO_DEFAULT_PATH)
find_package(QBDIPreload REQUIRED HINTS "${EXTRACT_DIRECTORY}" NO_DEFAULT_PATH)
```

Once the CMake package is found, you can link your executable either with the dynamic or the static library:

```
add_executable(example example.c)

target_link_libraries(example QBDI::QBDI)
# or
target_link_libraries(example QBDI::QBDI_static)
```

(continues on next page)

(continued from previous page)

```
add_executable(example_preload example_preload.c)
target_link_libraries(example_preload QBDI::QBDI_static QBDIPreload::QBDIPreload)
```

## Multi-architecture

If two or more architectures of QBDI are needed within the same project, you should import the package `QBDI<arch>` and `QBDIPreload<arch>`.

```
find_package(QBDIX86 REQUIRED HINTS "${EXTRACT_DIRECTORY_X86}" NO_DEFAULT_PATH)
find_package(QBDIPreloadX86 REQUIRED HINTS "${EXTRACT_DIRECTORY_X86}" NO_DEFAULT_PATH)

add_executable(example_preload86 example_preload.c)
set_target_properties(example_preload86 PROPERTIES COMPILE_FLAGS "-m32" LINK_FLAGS "-m32"
↳")
target_link_libraries(example_preload86 QBDI::X86::QBDI_static
↳QBDIPreload::X86::QBDIPreload)

find_package(QBDIX86_64 REQUIRED HINTS "${EXTRACT_DIRECTORY_X86_64}" NO_DEFAULT_PATH)
find_package(QBDIPreloadX86_64 REQUIRED HINTS "${EXTRACT_DIRECTORY_X86_64}" NO_DEFAULT_
↳PATH)

add_executable(example_preload64 example_preload.c)
target_link_libraries(example_preload64 QBDI::X86_64::QBDI_static QBDIPreload::X86_
↳64::QBDIPreload)
```

## 2.3 Getting Started

The following sections explain how one can take advantage of QBDI through different use cases.

### 2.3.1 C API

A step-by-step example illustrating a basic (yet powerful) usage of the QBDI C API.

#### Load the target code

In this tutorial, we aim at figuring out how many iterations a Fibonacci function is doing. To do so, we will rely on QBDI to instrument the function. For convenience sake, its source code is compiled along with the one we are about to write.

```
int fibonacci(int n) {
    if(n <= 2)
        return 1;
    return fibonacci(n-1) + fibonacci(n-2);
}
```

However, it's not always the case. Sometimes, we need to look into a function we don't have the source code of – that is, it has been already compiled. As a result, we have to find a way to load the code we want to inspect into our process'



memory space. For instance, if the function of interest is embedded in a dynamic library, we can link our code with this library when compiling or import it at runtime by calling either `dlopen` or `LoadLibraryA`.

Note that if you want to instrument a whole binary, `QBDIPreload` should be preferred (see [QBDIPreload in C](#)).

## Initialise the virtual machine

First off, we need to initialise the virtual machine (often referred to as VM) itself. The type `VMInstanceRef` represents an instance of the VM. The `qbdi_initVM()` function needs to be called to set the instance up. The second, third and fourth arguments are used to customise the instance depending on what you want to do.

```
#include "QBDI.h"

VMInstanceRef vm;
qbdi_initVM(&vm, NULL, NULL, 0);
```

## Retrieve the VM context

Prior to initialising the virtual stack (see next section), we need to get a pointer to the virtual machine state (`GPRState`), which can be obtained by calling `qbdi_getGPRState()`. This object represents the current VM's context.

```
GPRState *state = qbdi_getGPRState(vm);
assert(state != NULL);
```

## Allocate a virtual stack

The virtual machine does not work with the regular stack that your process uses – instead, QBDI needs its own stack. Therefore, we have to ask for a virtual stack using `qbdi_allocateVirtualStack()`. This function is responsible for allocating an aligned memory space, set the stack pointer register accordingly and return the top address of this brand-new memory region.

```
uint8_t* fakestack;
bool res = qbdi_allocateVirtualStack(state, STACK_SIZE, &fakestack);
assert(res == true);
```

## Write our first callback function

Now that the virtual machine has been set up, we can start playing with QBDI core features.

To have a trace of our execution, we will need a callback that will retrieve the current address and the disassembly of the instruction and print it.

As the callback will be called on an instruction, the callback must follow the `InstCallback` type. Inside the callback, we can get an `InstAnalysis` of the current instruction with `qbdi_getInstAnalysis()`. To have the address and the disassembly, the `InstAnalysis` needs to have the type `QBDI_ANALYSIS_INSTRUCTION` (for the address) and `QBDI_ANALYSIS_DISASSEMBLY` (for the disassembly).

```
VMAction showInstruction(VMInstanceRef vm, GPRState *gprState, FPRState *fprState, void_
↪ *data) {
    // Obtain an analysis of the instruction from the VM
    const InstAnalysis* instAnalysis = qbdi_getInstAnalysis(vm, QBDI_ANALYSIS_
↪ INSTRUCTION | QBDI_ANALYSIS_DISASSEMBLY);
```

(continues on next page)

(continued from previous page)

```
// Printing disassembly
printf("0x%" PRIxWORD ": %s\n", instAnalysis->address, instAnalysis->disassembly);

return QBDI_CONTINUE;
}
```

An *InstCallback* must always return an action (*VMAction*) to the VM to specify if the execution should continue or stop. In most cases *QBDI\_CONTINUE* should be returned to continue the execution.

## Register a callback

The callback must be registered in the VM. The function *qbd\_i\_addCodeCB()* allows registering a callback for every instruction. The callback can be called before the instruction (*QBDI\_PREINST*) or after the instruction (*QBDI\_POSTINST*).

```
uint32_t cid = qbd_i_addCodeCB(vm, QBDI_PREINST, showInstruction, NULL, 0);
assert(cid != QBDI_INVALID_EVENTID);
```

The function returns a callback ID or the special ID *QBDI\_INVALID\_EVENTID* if the registration fails. The callback ID can be kept if you want to unregister the callback later.

## Count the iterations

With the current implementation of Fibonacci, the function will iterate by recursively calling itself. Consequently, we can determine the number of iterations the function is doing by counting the number of calls. *qbd\_i\_addMnemonicCB()* can be used to register a callback which is solely called when encountering specific instructions. All QBDI callbacks allow users to pass a custom parameter data of type void \*.

```
VMAction countIteration(VMInstanceRef vm, GPRState *gprState, FPRState *fprState, void_
↳ *data) {
    *((unsigned*) data)++;

    return QBDI_CONTINUE;
}

unsigned iterationCount = 0;
qbd_i_addMnemonicCB(vm, "CALL*", QBDI_PREINST, countIteration, &iterationCount, 0);
```

## Set instrumented ranges

QBDI needs a range of addresses where the code should be instrumented. If the execution goes out of this scope, QBDI will try to restore an uninstrumented execution.

In our example, we need to include the function we are looking into in the instrumented range. *qbd\_i\_addInstrumentedModuleFromAddr()* can be used to add a whole module (binary or library) in the range of instrumentation with a single address of this module.

```
res = qbd_i_addInstrumentedModuleFromAddr(vm, (rword) &fibonacci);
assert(res == true);
```

## Run the instrumentation

We can finally run the instrumentation using the `qbdi_call()` function. It aligns the stack, sets the argument(s) (if needed) and a fake return address and calls the target function through QBDI. The execution stops when the instrumented code returns to the fake address.

```
rword retval;
res = qbdi_call(vm, &retval, (rword) fibonacci, 1, 25);
assert(res == true);
```

`qbdi_call()` returns if the function has completely run in the context of QBDI. The first argument has been filled with the value of the return register (e.g. RAX for X86\_64).

It may turn out that the function does not expect the calling convention `qbdi_call()` uses. In this precise case, you must set up the proper context and the stack yourself and call `qbdi_run()` afterwards.

## Terminate the execution properly

At last, before exiting, we need to free up the resources we have allocated: both the virtual stack and the virtual machine by respectively calling `qbdi_alignedFree()` and `qbdi_terminateVM()`.

```
qbdi_alignedFree(fakestack);
qbdi_terminateVM(vm);
```

## Full example

Merging everything we have learnt throughout this tutorial, we are now able to write our C source code file:

```
#include <assert.h>
#include <inttypes.h>
#include <stdio.h>
#include <stdlib.h>

#include "QBDI.h"

int fibonacci(int n) {
    if (n <= 2)
        return 1;
    return fibonacci(n - 1) + fibonacci(n - 2);
}

VMAction showInstruction(VMInstanceRef vm, GPRState *gprState,
                        FPRState *fprState, void *data) {
    // Obtain an analysis of the instruction from the VM
    const InstAnalysis *instAnalysis = qbdi_getInstAnalysis(
        vm, QBDI_ANALYSIS_INSTRUCTION | QBDI_ANALYSIS_DISASSEMBLY);

    // Printing disassembly
    printf("0x%" PRIxWORD ": %s\n", instAnalysis->address,
        instAnalysis->disassembly);

    return QBDI_CONTINUE;
```

(continues on next page)

(continued from previous page)

```

}

VMAction countIteration(VMInstanceRef vm, GPRState *gprState,
                        FPRState *fprState, void *data) {
    (*((int *)data))++;

    return QBDI_CONTINUE;
}

static const size_t STACK_SIZE = 0x100000; // 1MB

int main(int argc, char **argv) {
    int n = 0;

    int iterationCount = 0;
    uint8_t *fakestack;
    VMInstanceRef vm;
    GPRState *state;
    rword retvalue;

    if (argc >= 2) {
        n = atoi(argv[1]);
    }
    if (n < 1) {
        n = 1;
    }

    // Constructing a new QBDI VM
    qbdi_initVM(&vm, NULL, NULL, 0);

    // Get a pointer to the GPR state of the VM
    state = qbdi_getGPRState(vm);
    assert(state != NULL);

    // Setup initial GPR state,
    qbdi_allocateVirtualStack(state, STACK_SIZE, &fakestack);

    // Registering showInstruction() callback to print a trace of the execution
    uint32_t cid = qbdi_addCodeCB(vm, QBDI_PREINST, showInstruction, NULL, 0);
    assert(cid != QBDI_INVALID_EVENTID);

    // Registering countIteration() callback
    qbdi_addMnemonicCB(vm, "CALL*", QBDI_PREINST, countIteration, &iterationCount,
                       0);

    // Setup Instrumentation Range
    bool res = qbdi_addInstrumentedModuleFromAddr(vm, (rword)&fibonacci);
    assert(res == true);

    // Running DBI execution
    printf("Running fibonacci(%d) ...\n", n);
    res = qbdi_call(vm, &retvalue, (rword)fibonacci, 1, n);

```

(continues on next page)

(continued from previous page)

```

assert(res == true);

printf("fibonnaci(%d) returns %ld after %d recursions\n", n, retvalue,
       iterationCount);

// cleanup
qbdi_alignedFree(fakestack);
qbdi_terminateVM(vm);

return 0;
}

```

### Generate a template

A QBDI template can be considered as a baseline project, a minimal component you can modify and build your instrumentation tool on. They are provided to help you effortlessly start off a new QBDI based project. The binary responsible for generating a template is shipped in the release packages and can be used as follows:

```

mkdir new_project
cd new_project
qbdi-template

```

A template consists of a simple C source code file and a basic CMake build script. A file called `README.txt` is also present, it describes the compilation procedure.

### 2.3.2 C++ API

A step-by-step example illustrating a basic (yet powerful) usage of the QBDI C++ API.

#### Load the target code

In this tutorial, we aim at figuring out how many iterations a Fibonacci function is doing. To do so, we will rely on QBDI to instrument the function. For convenience sake, its source code is compiled along with the one we are about to write.

```

int fibonacci(int n) {
    if(n <= 2)
        return 1;
    return fibonacci(n-1) + fibonacci(n-2);
}

```

However, it's not always the case. Sometimes, we need to look into a function we don't have the source code of – that is, it has been already compiled. As a result, we have to find a way to load the code we want to inspect into our process' memory space. For instance, if the function of interest is embedded in a dynamic library, we can link our code with this library when compiling or import it at runtime by calling either `dlopen` or `LoadLibraryA`.

Note that if you want to instrument a whole binary, `QBDIPreload` should be preferred (see [QBDIPreload in C++](#)).

## Initialise the virtual machine

First off, we need to initialise the virtual machine (`QBDI::VM`) itself.

```
#include "QBDI.h"
```

```
QBDI::VM vm;
```

## Retrieve the VM context

Prior to initialising the virtual stack (see next section), we need to get a pointer to the virtual machine state (`QBDI::GPRState`), which can be obtained by calling `QBDI::VM::getGPRState()`. This object represents the current VM's context.

```
QBDI::GPRState *state = vm.getGPRState();  
assert(state != NULL);
```

## Allocate a virtual stack

The virtual machine does not work with the regular stack that your process uses – instead, QBDI needs its own stack. Therefore, we have to ask for a virtual stack using `QBDI::allocateVirtualStack()`. This function is responsible for allocating an aligned memory space, set the stack pointer register accordingly and return the top address of this brand-new memory region.

```
uint8_t* fakestack;  
bool res = QBDI::allocateVirtualStack(state, STACK_SIZE, &fakestack);  
assert(res == true);
```

## Our first callback function

Now that the virtual machine has been set up, we can start playing with QBDI core features.

To have a trace of our execution, we will need a callback that will retrieve the current address and the disassembly of the instruction and print it.

As the callback will be called on an instruction, the callback must follow the `QBDI::InstCallback` type. Inside the callback, we can get an `QBDI::InstAnalysis` of the current instruction with `QBDI::VM::getInstAnalysis()`. To have the address and the disassembly, the `QBDI::InstAnalysis` need to have the type `QBDI::AnalysisType::ANALYSIS_INSTRUCTION` (for the address) and `QBDI::AnalysisType::ANALYSIS_DISASSEMBLY` (for the disassembly). These two `QBDI::AnalysisType` are the default parameter of `QBDI::VM::getInstAnalysis()` and can be omitted.

```
QBDI::VMAction showInstruction(QBDI::VM* vm, QBDI::GPRState *gprState, QBDI::FPRState_  
↪ *fprState, void *data) {  
    // Obtain an analysis of the instruction from the VM  
    const QBDI::InstAnalysis* instAnalysis = vm->getInstAnalysis();  
  
    // Printing disassembly  
    std::cout << std::setbase(16) << instAnalysis->address << ": "  
        << instAnalysis->disassembly << std::endl << std::setbase(10);
```

(continues on next page)

(continued from previous page)

```

    return QBDI::VMAction::CONTINUE;
}

```

An `QBDI::InstCallback` must always return an action (`QBDI::VMAction`) to the VM to specify if the execution should continue or stop. In most cases `QBDI::VMAction::CONTINUE` should be returned to continue the execution.

## Register a callback

The callback must be registered in the VM. The function `QBDI::VM::addCodeCB()` allows registering a callback for every instruction. The callback can be called before the instruction (`QBDI::InstPosition::PREINST`) or after the instruction (`QBDI::InstPosition::POSTINST`).

```

uint32_t cid = vm.addCodeCB(QBDI::PREINST, showInstruction, nullptr);
assert(cid != QBDI::INVALID_EVENTID);

```

The function returns a callback ID or the special ID `QBDI::VMError::INVALID_EVENTID` if the registration fails. The callback ID can be kept if you want to unregister the callback later.

## Count the iterations

With the current implementation of Fibonacci, the function will iterate by recursively calling itself. Consequently, we can determine the number of iterations the function is doing by counting the number of calls. `QBDI::VM::addMnemonicCB()` can be used to register a callback which is solely called when encountering specific instructions. All QBDI callbacks allow users to pass a custom parameter data of type `void *`.

```

QBDI::VMAction countIteration(QBDI::VMInstanceRef vm, QBDI::GPRState *gprState,
↳ QBDI::FPRState *fprState, void *data) {
    ((*((unsigned*) data))++)++;

    return QBDI::CONTINUE;
}

unsigned iterationCount = 0;
vm.addMnemonicCB("CALL*", QBDI::PREINST, countIteration, &iterationCount);

```

## Set instrumented ranges

QBDI needs a range of addresses where the code should be instrumented. If the execution goes out of this scope, QBDI will try to restore an uninstrumented execution.

In our example, we need to include the method in the instrumented range. The method `QBDI::VM::addInstrumentedModuleFromAddr()` can be used to add a whole module (binary or library) in the range of instrumentation with a single address of this module.

```

res = vm.addInstrumentedModuleFromAddr(reinterpret_cast<QBDI::rword>(fibonacci));
assert(res == true);

```

## Run the instrumentation

We can finally run the instrumentation using the `QBDI::VM::call()` function. It aligns the stack, sets the argument(s) (if needed) and a fake return address and calls the target function through QBDI. The execution stops when the instrumented code returns to the fake address.

```
rword retval;
res = vm.call(&retval, reinterpret_cast<QBDI::rword>(fibonacci), {25});
assert(res == true);
```

`QBDI::VM::call()` returns if the function has completely run in the context of QBDI. The first argument has been filled with the value of the return register (e.g. RAX for X86\_64).

It may turn out that the function does not expect the calling convention `QBDI::VM::call()` uses. In this precise case, you must set up the proper context and the stack yourself and call `QBDI::VM::run()` afterwards.

## Terminate the execution properly

At last, before exiting, we need to free up the virtual stack we have allocated calling `QBDI::alignedFree()`.

```
QBDI::alignedFree(fakestack);
```

## Full example

Merging everything we have learnt throughout this tutorial, we are now able to write our C++ source code file:

```
#include <assert.h>
#include <cstdint>
#include <cstdlib>
#include <cstring>
#include <iomanip>
#include <iostream>

#include "QBDI.h"

int fibonacci(int n) {
    if (n <= 2)
        return 1;
    return fibonacci(n - 1) + fibonacci(n - 2);
}

QBDI::VMAction showInstruction(QBDI::VM *vm, QBDI::GPRState *gprState,
                             QBDI::FPRState *fprState, void *data) {
    // Obtain an analysis of the instruction from the VM
    const QBDI::InstAnalysis *instAnalysis = vm->getInstAnalysis();

    // Printing disassembly
    std::cout << std::setbase(16) << instAnalysis->address << ": "
              << instAnalysis->disassembly << std::endl
              << std::setbase(10);

    return QBDI::VMAction::CONTINUE;
```

(continues on next page)



(continued from previous page)

```

}

QBDI::VMAction countIteration(QBDI::VM *vm, QBDI::GPRState *gprState,
                             QBDI::FPRState *fprState, void *data) {
    (*((unsigned *)data))++;

    return QBDI::CONTINUE;
}

static const size_t STACK_SIZE = 0x100000; // 1MB

int main(int argc, char **argv) {
    int n = 0;
    bool res;
    uint32_t cid;

    unsigned iterationCount = 0;
    uint8_t *fakestack;
    QBDI::GPRState *state;
    QBDI::rword retvalue;

    // Argument to the fibonnaci call
    if (argc >= 2) {
        n = atoi(argv[1]);
    }
    if (n < 1) {
        n = 1;
    }

    // Constructing a new QBDI vm
    QBDI::VM vm{};

    // Get a pointer to the GPR state of the VM
    state = vm.getGPRState();
    assert(state != nullptr);

    // Setup initial GPR state,
    res = QBDI::allocateVirtualStack(state, STACK_SIZE, &fakestack);
    assert(res == true);

    // Registering showInstruction() callback to print a trace of the execution
    cid = vm.addCodeCB(QBDI::PREINST, showInstruction, nullptr);
    assert(cid != QBDI::INVALID_EVENTID);

    // Registering countIteration() callback
    vm.addMnemonicCB("CALL*", QBDI::PREINST, countIteration, &iterationCount);

    // Setup Instrumentation Range
    res = vm.addInstrumentedModuleFromAddr(
        reinterpret_cast<QBDI::rword>(fibonacci));
    assert(res == true);

```

(continues on next page)

(continued from previous page)

```
// Running DBI execution
std::cout << "Running fibonacci(" << n << ") ..." << std::endl;
res = vm.call(&retvalue, reinterpret_cast<QBDI::rword>(fibonacci),
             {static_cast<QBDI::rword>(n)});
assert(res == true);

std::cout << "fibonacci(" << n << ") returns " << retvalue << " after "
          << iterationCount << " recursions" << std::endl;

QBDI::alignedFree(fakestack);

return 0;
}
```

### 2.3.3 PyQBDI

PyQBDI brings Python3 bindings over the QBDI API. That way, you can take advantage of the QBDI features directly from your Python scripts without bothering using C/C++. It may be pretty useful if you need to build something quickly. However, it introduces some limitations:

- PyQBDI cannot be used to instrument a Python process
- The performances are poorer than when using the C/C++ APIs
- The Python runtime's and the target's architectures must be the same

#### Memory allocation

Unlike the C/C++ APIs, interacting with the process' memory is much more complicated while in Python – that is, memory regions cannot be allocated, read or written. Luckily, PyQBDI offers helpers to allow users perform these actions.

```
import pyqbd

value = b"bytes array"

addr = pyqbd.allocateMemory(len(value))
pyqbd.writeMemory(addr, value)
value2 = pyqbd.readMemory(addr, len(value))
assert value == value2
pyqbd.freeMemory(addr)
```

## Load the target code

In this tutorial, we aim at executing the `foo` function which lies in a shared library whose name is `mylib.so`, in the context of QBDI. PyQBDI will give us a hand doing so.

```
import pyqbd
import ctypes

mylib = ctypes.cdll.LoadLibrary("mylib.so")
funcPtr = ctypes.cast(mylib.foo, ctypes.c_void_p).value
```

Note that if you want to instrument a whole binary, `PyQBDIPreload` should be preferred (see [PyQBDIPreload](#)).

## Initialise the virtual machine

First off, we need to initialise the virtual machine (*VM*) itself. Calling the `pyqbd.VM()` is needed to craft a new instance.

```
vm = pyqbd.VM()
```

## Allocate a virtual stack

The virtual machine does not work with the regular stack that your process uses – instead, QBDI needs its own stack. Therefore, we have to ask for a virtual stack using `pyqbd.allocateVirtualStack()`. This function is responsible for allocating an aligned memory space, set the stack pointer register accordingly and return the top address of this brand-new memory region.

```
state = vm.getGPRState()
fakestack = pyqbd.allocateVirtualStack(state, 0x1000000)
assert fakestack != None
```

## Write our first callback function

Now that the virtual machine has been set up, we can start playing with QBDI core features.

To have a trace of our execution, we will need a callback that will retrieve the current address and the disassembly of the instruction and print it.

As the callback will be called on an instruction, the callback must follow the `InstCallback` type. Inside the callback, we can get an `InstAnalysis` of the current instruction with `pyqbd.VM.getInstAnalysis()`. To have the address and the disassembly, the `InstAnalysis` need to have the type `pyqbd.ANALYSIS_INSTRUCTION` (for the address) and `pyqbd.ANALYSIS_DISASSEMBLY` (for the disassembly). These two `pyqbd.AnalysisType` are the default parameter of `pyqbd.VM.getInstAnalysis()` and can be omitted.

```
def showInstruction(vm, gpr, fpr, data):
    # Obtain an analysis of the instruction from the VM
    instAnalysis = vm.getInstAnalysis()

    # Printing disassembly
    print("0x{:x}: {}".format(instAnalysis.address, instAnalysis.disassembly))

    return pyqbd.CONTINUE
```

An *InstCallback* must always return an action (*pyqbd.VMAction*) to the VM to specify if the execution should continue or stop. In most cases *CONTINUE* should be returned to continue the execution.

## Register a callback

The callback must be registered in the VM. The function *pyqbd.VM.addCodeCB()* allows registering a callback for every instruction. The callback can be called before the instruction (*pyqbd.PREINST*) or after the instruction (*pyqbd.POSTINST*).

```
cid = vm.addCodeCB(pyqbd.PREINST, showInstruction, None)
assert cid != pyqbd.INVALID_EVENTID
```

The function returns a callback ID or the special ID *pyqbd.INVALID\_EVENTID* if the registration fails. The callback ID can be kept if you want to unregister the callback later.

## Set instrumented ranges

QBDI needs a range of addresses where the code should be instrumented. If the execution goes out of this scope, QBDI will try to restore an uninstrumented execution.

In our example, we need to include the method in the instrumented range. The method *pyqbd.VM.addInstrumentedModuleFromAddr()* can be used to add a whole module (binary or library) in the range of instrumentation with a single address of this module.

```
assert vm.addInstrumentedModuleFromAddr(funcPtr)
```

## Run the instrumentation

We can finally run the instrumentation using the *pyqbd.VM.call()* function. It aligns the stack, sets the argument(s) (if needed) and a fake return address and calls the target function through QBDI. The execution stops when the instrumented code returns to the fake address.

```
asrun, retval = vm.call(funcPtr, [args1, args2])
assert asrun
```

*pyqbd.VM.call()* returns if the function has completely run in the context of QBDI. The first argument has been filled with the value of the return register (e.g. RAX for X86\_64).

It may turn out that the function does not expect the calling convention *pyqbd.VM.call()* uses. In this precise case, you must set up the proper context and the stack yourself and call *pyqbd.VM.run()* afterwards.

## Terminate the execution properly

At last, before exiting, we need to free up the virtual stack we have allocated calling *pyqbd.alignedFree()*.

```
pyqbd.alignedFree(fakestack)
```

## Full example

Merging everything we have learnt throughout this tutorial, we are now able to solve real problems. For instance, the following example shows how one can generate an execution trace of the `sin` function by using a PyQBDI script:

```
#!/usr/bin/env python3

import sys
import math
import ctypes
import pyqbd
import struct

def insnCB(vm, gpr, fpr, data):
    instAnalysis = vm.getInstAnalysis()
    print("0x{:x}: {}".format(instAnalysis.address, instAnalysis.disassembly))
    return pyqbd.CONTINUE

def run():
    # get sin function ptr
    if sys.platform == 'darwin':
        libmname = 'libSystem.dylib'
    elif sys.platform == 'win32':
        libmname = 'api-ms-win-crt-math-l1-1-0.dll'
    else:
        libmname = 'libm.so.6'
    libm = ctypes.cdll.LoadLibrary(libmname)
    funcPtr = ctypes.cast(libm.sin, ctypes.c_void_p).value

    # init VM
    vm = pyqbd.VM()

    # create stack
    state = vm.getGPRState()
    addr = pyqbd.allocateVirtualStack(state, 0x1000000)
    assert addr is not None

    # instrument library and register memory access
    vm.addInstrumentedModuleFromAddr(funcPtr)
    vm.recordMemoryAccess(pyqbd.MEMORY_READ_WRITE)

    # add callbacks on instructions
    vm.addCodeCB(pyqbd.PREINST, insnCB, None)

    # Cast double arg to long and set FPR
    arg = 1.0
    carg = struct.pack('<d', arg)
    fpr = vm.getFPRState()
    fpr.xmm0 = carg

    # call sin(1.0)
    pyqbd.simulateCall(state, 0x42424242)
```

(continues on next page)

(continued from previous page)

```
success = vm.run(funcPtr, 0x42424242)

# Retrieve output FPR state
fpr = vm.getFPRState()
# Cast long arg to double
res = struct.unpack('<d', fpr.xmm0[:8])[0]
print("%f (python) vs %f (qbdi)" % (math.sin(arg), res))

# cleanup
pyqbdi.alignedFree(addr)

if __name__ == "__main__":
    run()
```

## 2.3.4 Frida/QBDI

QBDI can team up with Frida to be even more powerful together. To be able to use QBDI bindings while injected into a process with Frida, it is necessary to understand how to use Frida to perform some common tasks beforehand. Through this simple example based on *qbdi-frida-template* (see [Generate a template](#)), we will explain a basic usage of Frida and QBDI.

### Common tasks

This section solely shows a few basic actions and gives you a general overview of what you can do with Frida. Keep in mind that Frida offers many more awesome features, all listed in the [Javascript API documentation](#).

### Read memory

Sometimes it may be necessary to have a look at a buffer or specific part of the memory. We rely on Frida to do it.

```
var arrayPtr = ptr(0xDEADBEEF)
var size = 0x80
var buffer = Memory.readByteArray(arrayPtr, size)
```

### Write memory

We also need to be able to write memory:

```
var arrayPtr = ptr(0xDEADBEEF)
var size = 0x80
var toWrite = new Uint8Array(size);
// fill your buffer eventually
Memory.writeByteArray(arrayPtr, toWrite)
```

## Allocate an array

If you have a function that takes a buffer or a string as an input, you might need to allocate a new buffer using Frida:

```
// allocate and write a 2-byte buffer
var buffer = Memory.alloc(2);
Memory.writeByteArray(buffer, [0x42, 0x42])
// allocate and write an UTF8 string
var str = Memory.allocUtf8String("Hello World !");
```

## Initialise a QBDI object

If *frida-qbdi.js* (or a script requiring it) is successfully loaded in Frida, a new `QBDI()` object becomes available. It provides an object oriented access to the framework features.

```
// initialise QBDI
var vm = new QBDI();
console.log("QBDI version is " + vm.version.string);
var state = vm.getGPRState();
```

## Instrument a function with QBDI

You can instrument a function using QBDI bindings. They are really close to the C++ ones, further details about the exposed APIs are available in the *Frida/QBDI API* documentation.

```
var functionPtr = DebugSymbol.fromName("function_name").address;
vm.addInstrumentedModule("demo.bin");

var InstructionCallback = vm.newInstCallback(function(vm, gpr, fpr, data) {
    inst = vm.getInstAnalysis();
    gpr.dump(); // display the context
    console.log("0x" + inst.address.toString(16) + " " + inst.disassembly); // display
    ↪ the instruction
    return VMACTION.CONTINUE;
});
var iid = vm.addCodeCB(InstPosition.PREINST, instructionCallback, NULL);

vm.call(functionPtr, []);
```

If you ever want to pass custom arguments to your callback, this can be done via the **data** argument:

```
// this callback is used to count the number of basic blocks executed
var userData = { counter: 0 };
var BasicBlockCallback = vm.newVMCallback(function(vm, evt, gpr, fpr, data) {
    data.counter++;
    return VMACTION.CONTINUE;
});
vm.addVMEvtCB(VMEvt.BASIC_BLOCK_ENTRY, BasicBlockCallback, userData);
console.log(userData.counter);
```

## Scripts

Bindings can simply be used in Frida REPL, or imported in a Frida script, empowering the bindings with all the *nodejs* ecosystem.

```
const qbdi = require('/usr/local/share/qbdi/frida-qbdi'); // import QBDI bindings
qbdi.import(); // set bindings to the global environment

var vm = new QBDI();
console.log("QBDI version is " + vm.version.string);
```

It will be possible to load it in Frida in place of *frida-qbdi.js*, allowing to easily create custom instrumentation tools with in-process scripts written in JavaScript and external control in Python (or any language supported by *Frida*).

## Compilation

In order to actually import QBDI bindings into your project, your script needs be *compiled* with the *frida-compile* utility. Installing it requires you to have *npm* installed. The *babelify* package might be also needed. Otherwise, you will not be able to successfully compile/load it and some errors will show up once running it with Frida.

```
# if frida-compile is not already installed
npm install frida-compile babelify
./node_modules/.bin/frida-compile MyScript.js -o MyScriptCompiled.js
# else
frida-compile MyScript.js -o MyScriptCompiled.js
```

## Run Frida/QBDI on a workstation

To use QBDI on an already existing process you can use the following syntax:

```
frida -n processName -l MyScriptCompiled.js
```

You can also spawn the process using Frida to instrument it with QBDI as soon as it starts:

```
frida -f binaryPath Arguments -l MyScriptCompiled.js
```

## Run Frida/QBDI on an Android device

Since Frida provides a great interface to instrument various types of target, we can also rely on it to use QBDI on Android, especially when it comes to inspecting applications. Nevertheless, it has some specificities you need to be aware of. Before running your script, make sure that:

- a Frida server is running on the remote device and is reachable from your workstation
- the `libQBDI.so` library has been placed in `/data/local/tmp` (available in [Android packages](#))
- SELinux has been turned into *permissive* mode (through `setenforce 0`)

Then, you should be able to inject your script into a specific Android application:



```
# if the application is already running
frida -Un com.app.example -l MyScriptCompiled.js

# if you want to spawn the application
frida -Uf com.app.example -l MyScriptCompiled.js
```

## Concrete example

If you have already had a look at the default instrumentation of the template generated with *qbd-fida-template* (see *Generate a template*), you are probably familiar with the following example. Roughly speaking, what it does is creating a native call to the *Secret()* function, and instrument it looking for *XOR*.

## Source code

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

#ifdef _MSC_VER
#define EXPORT __declspec(dllexport)
#else // _MSC_VER
#define EXPORT __attribute__((visibility("default")))
#endif

EXPORT int Secret(char *str) {
    int i;
    unsigned char XOR[] = {0x51, 0x42, 0x44, 0x49, 0x46, 0x72, 0x69, 0x64, 0x61};
    size_t len = strlen(str);

    printf("Input string is : %s\nEncrypted string is : \n", str);

    for (i = 0; i < len; i++) {
        printf("0x%x,", str[i] ^ XOR[i % sizeof(XOR)]);
    }
    printf("\n");
    fflush(stdout);
    return 0;
}

void Hello() { Secret("Hello world !"); }

int main() { Hello(); }
```

## Frida/QBDI script

```
// QBDI
const qbdi = require('/usr/local/share/qbdi/frida-qbdi'); // import QBDI bindings
qbdi.import(); // Set bindings to global environment

// Initialize QBDI
var vm = new QBDI();
var state = vm.getGPRState();
var stack = vm.allocateVirtualStack(state, 0x100000);

// Instrument "Secret" function from demo.bin
var funcPtr = Module.findExportByName(null, "Secret");
if (!funcPtr) {
    funcPtr = DebugSymbol.fromName("Secret").address;
}
vm.addInstrumentedModuleFromAddr(funcPtr);

// Callback on every instruction
// This callback will print context and display current instruction address and
↳disassembly
// We choose to print only XOR instructions
var icbk = vm.newInstCallback(function(vm, gpr, fpr, data) {
    var inst = vm.getInstAnalysis();
    if (inst.mnemonic.search("XOR")){
        return VMAction.CONTINUE;
    }
    gpr.dump(); // Display context
    console.log("0x" + inst.address.toString(16) + " " + inst.disassembly); // Display
↳instruction disassembly
    return VMAction.CONTINUE;
});
var iid = vm.addCodeCB(InstPosition.PREINST, icbk);

// Allocate a string in remote process memory
var strP = Memory.allocUtf8String("Hello world !");
// Call the Secret function using QBDI and with our string as argument
vm.call(funcPtr, [strP]);
```

## Generate a template

A QBDI template can be considered as a baseline project, a minimal component you can modify and build your instrumentation tool on. They are provided to help you effortlessly start off a new QBDI based project. If you want to get started using QBDI bindings, you can create a brand-new default project doing:

```
make NewProject
cd NewProject
qbdi-frida-template

# if you want to build the demo binary
mkdir build && cd build
cmake ..
```

(continues on next page)

(continued from previous page)

```
make

# if frida-compile is not already installed
npm install frida-compile babelify
./node_modules/.bin/frida-compile ../FridaQBDI_sample.js -o RunMe.js
# else
frida-compile ../FridaQBDI_sample.js -o RunMe.js

frida -f ./demo.bin -l ./RunMe.js
```

### 2.3.5 QBDIPreload

QBDIPreload is a small utility library that provides code injection capabilities using dynamic library injection. It works on Linux and macOS respectively with the LD\_PRELOAD and DYLD\_INSERT\_LIBRARIES mechanisms.

Thanks to QBDIPreload, you can instrument the main function of an executable that has been dynamically linked. You can also define various callbacks that are called at specific times throughout the execution.

#### Main hook process

To use QBDIPreload, you must have a minimal codebase: a constructor and several *hook* functions. Like callbacks, hook functions are directly called by QBDIPreload.

First of all, the constructor of QBDIPreload has to be initialised through declaring the macro `QBDIPRELOAD_INIT`. It's worth noting that this macro must be only defined once in your code.

The `qbdipreload_on_start()` and `qbdipreload_on_premain()` hook functions are called at different stages during the execution of the programme. They only need to return `QBDIPRELOAD_NOT_HANDLED` if you don't want to modify the hook procedure.

```
#include "QBDIPreload.h"

QBDIPRELOAD_INIT;

int qbdipreload_on_start(void *main) {
    return QBDIPRELOAD_NOT_HANDLED;
}

int qbdipreload_on_premain(void *gprCtx, void *fpuCtx) {
    return QBDIPRELOAD_NOT_HANDLED;
}
```

## Instrumentation

Once the main function is hooked by QBDIPreload, two methods are called: `qbdipreload_on_main()` and `qbdipreload_on_run()`.

At this point, you are able to capture the executable arguments inside of the `qbdipreload_on_main()` scope. The `qbdipreload_on_run()` function is called right afterwards with a ready-to-run QBDI virtual machine as first argument. Obviously, don't forget to register your callback(s) prior to running the VM.

```
static VMAction onInstruction(VMInstanceRef vm, GPRState *gprState, FPRState *fprState,
↪void *data) {
    // ...
    return QBDI_CONTINUE;
}

int qbdipreload_on_main(int argc, char** argv) {
    return QBDIPRELOAD_NOT_HANDLED;
}

int qbdipreload_on_run(VMInstanceRef vm, rword start, rword stop) {
    // add user callbacks
    qbdi_addCodeCB(vm, QBDI_PREINST, onInstruction, NULL);

    // run the VM
    qbdi_run(vm, start, stop);
    return QBDIPRELOAD_NO_ERROR;
}
```

---

**Note:** QBDIPreload automatically takes care of blacklisting instrumentation of the C standard library and the OS loader as described in *Limitations*.

---

## Exit hook

QBDIPreload also intercepts the calls on standard exit functions (`exit` and `_exit`). Typically, these are called when the executable is about to terminate. If so, the `qbdipreload_on_exit()` method is called and can be used to save some data about the execution you want to keep before exiting. Note that the hook function is not called if the executable exits with a direct system call or a segmentation fault.

```
int qbdipreload_on_exit(int status) {
    return QBDIPRELOAD_NO_ERROR;
}
```

## Compilation and execution

Finally, you need to compile your source code to a dynamic library. Your output binary has to be statically linked with both the QBDIPreload library and the QBDI library.

Then, in order to test it against a target, simply running the following command should do the job:

```
# on Linux
LD_BIND_NOW=1 LD_PRELOAD=./libqbd_i_mytracer.so <executable> [<parameters> ...]

# on macOS
sudo DYLD_BIND_AT_LAUNCH=1 DYLD_INSERT_LIBRARIES=./libqbd_i_mytracer.so <executable> [
↪<parameters> ...]
```

As the loader is not in the instrumentation range, we recommend setting LD\_BIND\_NOW or DYLD\_BIND\_AT\_LAUNCH in order to resolve and bind all symbols before the instrumentation.

## Full example

Merging everything we have learnt throughout this tutorial, we are now able to write our C/C++ source code files. In the following examples, we aim at displaying every executed instruction of the binary we are running against.

### QBDIPreload in C

```
#include <stdio.h>
#include "QBDIPreload.h"

QBDIPRELOAD_INIT;

static VMAAction onInstruction(VMInstanceRef vm, GPRState *gprState,
                              FPRState *fprState, void *data) {
    const InstAnalysis *instAnalysis = qbdi_getInstAnalysis(
        vm, QBDI_ANALYSIS_INSTRUCTION | QBDI_ANALYSIS_DISASSEMBLY);
    printf("0x%" PRIxWORD " %s\n", instAnalysis->address,
        instAnalysis->disassembly);
    return QBDI_CONTINUE;
}

int qbdipreload_on_start(void *main) { return QBDIPRELOAD_NOT_HANDLED; }

int qbdipreload_on_premain(void *gprCtx, void *fpuCtx) {
    return QBDIPRELOAD_NOT_HANDLED;
}

int qbdipreload_on_main(int argc, char **argv) {
    return QBDIPRELOAD_NOT_HANDLED;
}

int qbdipreload_on_run(VMInstanceRef vm, rword start, rword stop) {
    qbdi_addCodeCB(vm, QBDI_PREINST, onInstruction, NULL, 0);
    qbdi_run(vm, start, stop);
    return QBDIPRELOAD_NO_ERROR;
}
```

(continues on next page)

(continued from previous page)

```

}

int qbdipreload_on_exit(int status) { return QBDIPRELOAD_NO_ERROR; }

```

## QBDIPreload in C++

```

#include <iomanip>
#include <iostream>

#include "QBDIPreload.h"

static QBDI::VMAction onInstruction(QBDI::VMInstanceRef vm,
                                   QBDI::GPRState *gprState,
                                   QBDI::FPRState *fprState, void *data) {
    const QBDI::InstAnalysis *instAnalysis = vm->getInstAnalysis();

    std::cout << std::setbase(16) << instAnalysis->address << ": "
               << instAnalysis->disassembly << std::endl
               << std::setbase(10);
    return QBDI::CONTINUE;
}

extern "C" {

QBDIPRELOAD_INIT;

int qbdipreload_on_start(void *main) { return QBDIPRELOAD_NOT_HANDLED; }

int qbdipreload_on_premain(void *gprCtx, void *fpuCtx) {
    return QBDIPRELOAD_NOT_HANDLED;
}

int qbdipreload_on_main(int argc, char **argv) {
    return QBDIPRELOAD_NOT_HANDLED;
}

int qbdipreload_on_run(QBDI::VMInstanceRef vm, QBDI::rword start,
                      QBDI::rword stop) {
    vm->addCodeCB(QBDI::PREINST, onInstruction, nullptr);
    vm->run(start, stop);
    return QBDIPRELOAD_NO_ERROR;
}

int qbdipreload_on_exit(int status) { return QBDIPRELOAD_NO_ERROR; }
}

```

## Generate a template

A QBDI template can be considered as a baseline project, a minimal component you can modify and build your instrumentation tool on. They are provided to help you effortlessly start off a new QBDI based project. The binary responsible for generating a template is shipped in the release packages and can be used as follows:

```
mkdir QBDIPreload && cd QBDIPreload
qbdipreload-template
mkdir build && cd build
cmake ..
make
```

### 2.3.6 PyQBDIPreload

PyQBDIPreload is an implementation of QBDIPreload for PyQBDI. It allows users to inject the Python runtime into a target process and execute their own script in it. The limitations are pretty much the same as those we face on QBDIPreload and PyQBDI:

- Only Linux and macOS are currently supported
- The executable should be injectable with LD\_PRELOAD or DYLD\_INSERT\_LIBRARIES
- PyQBDIPreload cannot be injected in a Python process
- The Python runtime and the target must share the same architecture
- An extra *VM* must not be created. An already prepared *VM* is provided to `pyqbdipreload_on_run()`.

---

**Note:** The Python library `libpython3.x.so` must be installed.

---

## Main hook process

Unlike QBDIPreload, the hook of the main function cannot be customised so you are unable to alter the hook process. The Python interpreter is only initialised once the main function is hooked and the script is loaded. Furthermore, some modifications are made on the environment of the interpreter before the user script loading:

- `sys.argv` are the argument of the executable
- LD\_PRELOAD or DYLD\_INSERT\_LIBRARIES are removed from `os.environ`
- `pyqbdipreload.__preload__` is set to True

## Instrumentation

Once the script is loaded, the `pyqbdipreload_on_run()` function is called with a ready-to-run *VM*. Any user callbacks should be registered to the *VM*, then the *VM* can be run with `pyqbdipreload.VM.run()`.

```
import pyqbdipreload

def instCallback(vm, gpr, fpr, data):
    # User code ...
    return pyqbdipreload.CONTINUE
```

(continues on next page)

(continued from previous page)

```
def pyqbdipreload_on_run(vm, start, stop):
    vm.addCodeCB(pyqbdi.PREINST, instCallback, None)
    vm.run(start, stop)
```

## Exit hook

The `atexit` module is triggered when the execution is finished, or when `exit` or `_exit` are called.

---

**Note:** Any `VM` object is invalidated when the `atexit` module is triggered and should never be used.

---

## Execution

A script called `pyqbdipreload.py` is brought to set the environment up and run the executable. The first parameter is the `PyQBDIPreload` script. Next are the binary followed by its respective arguments if any.

```
python3 -m pyqbdipreload <script> <executable> [<arguments> ...]
```

## Full example

Merging everything we have learnt throughout this tutorial, we are now able to write our Python script which prints the instructions that are being executed by the target executable.

```
#!/usr/bin/env python3

import pyqbdi

def showInstruction(vm, gpr, fpr, data):
    instAnalysis = vm.getInstAnalysis()
    print("0x{:x}: {}".format(instAnalysis.address, instAnalysis.disassembly))
    return pyqbdi.CONTINUE

def pyqbdipreload_on_run(vm, start, stop):
    vm.addCodeCB(pyqbdi.PREINST, showInstruction, None)
    vm.run(start, stop)
```

## 2.4 Tutorials

This section contains some tutorials on specifics points of QBDI



## 2.4.1 Basic block events

### Introduction

The *Instrument Callback* allows inserting callbacks on all or specific instruction. With a callback at each instruction, it's trivial to follow the execution pointer and obtain a trace of the execution. However, the performances are slow, as the execution should be stopped at each instruction from executing the callback. For some traces, a higher-level callback can have better performances.

The *VM callbacks* is called when some conditions are reached during the execution. This tutorial introduces 3 *VMEvent*:

- **BASIC\_BLOCK\_NEW** : this event is triggered when a new basic block has been instrumented and add to the cache. It can be used to create coverage of the execution.
- **BASIC\_BLOCK\_ENTRY**: this event is triggered before the execution of a basic block.
- **BASIC\_BLOCK\_EXIT**: this event is triggered after the execution of a basic block.

### A basic block in QBDI

QBDI doesn't analyse the whole program before the run. Basic blocks are detected dynamically and may not match the basic block given by other tools. In QBDI, a basic block is a sequence of consecutive instructions that doesn't change the instruction pointer except the last one. Any instruction that may change the instruction pointer (method call, jump, conditional jump, method return, ...) are always the last instruction of a basic block.

QBDI detects the beginning of a basic block:

- when the instruction is the first to be executed in QBDI;
- after the end of the previous basic block;
- potentially if the user changes the callback during the execution (add a new callback, clear the cache, return `BREAK_TO_VM`, ...)

Due to the dynamic detection of the basic block, some basic block can overlap others. This behavior can be observed in this code:

```
// BB
0x00000000000001000:  push rbp
0x00000000000001001:  mov  rbp, rsp
0x00000000000001004:  mov  dword ptr [rbp - 0x14], edi
0x00000000000001007:  mov  edx, dword ptr [rbp - 0x14]
0x0000000000000100a:  mov  eax, edx
0x0000000000000100c:  shl  eax, 2
0x0000000000000100f:  add  eax, edx
0x00000000000001011:  mov  dword ptr [rbp - 4], eax
0x00000000000001014:  cmp  dword ptr [rbp - 0x14], 0xa
0x00000000000001018:  jle  0x1027
// BB
0x0000000000000101e:  add  dword ptr [rbp - 4], 0x33
0x00000000000001022:  jmp  0x1033
// BB
0x00000000000001027:  mov  eax, dword ptr [rbp - 4]
0x0000000000000102a:  imul eax, eax
0x0000000000000102d:  add  eax, 0x57
0x00000000000001030:  mov  dword ptr [rbp - 4], eax
// BB
```

(continues on next page)

(continued from previous page)

```

0x00000000000001033:  mov  edx, dword ptr [rbp - 4]
0x00000000000001036:  mov  eax, dword ptr [rbp - 0x14]
0x00000000000001039:  add  eax, edx
0x0000000000000103b:  pop  rbp
0x0000000000000103c:  ret

```

In this snippet, QBDI can detect 4 different basic blocks. If the first jump is taken:

- The begin of the method, between 0x1000 and 0x101e;
- The block between 0x101e and 0x1027;
- The last block between 0x1033 and 0x103c.

If the first jump isn't taken:

- The begin of the method, between 0x1000 and 0x101e;
- The last block between 0x1027 and 0x103c.

## Getting basic block information

To receive basic block information, a `VMCallback` should be registered to the VM with `addVMEventCB` for one of `BASIC_BLOCK_*` events. Once a registered event occurs, the callback is called with a description of the VM (`VMState`).

The address of the current basic block can be retrieved with `VMState.basicBlockStart` and `VMState.basicBlockEnd`.

---

**Note:** `BASIC_BLOCK_NEW` can be triggered with `BASIC_BLOCK_ENTRY`. A callback registered with both events will only be called once. You can retrieve the events that triggered the callback in `VMState.event`.

---

The follow example registers the three events in the VM and displays the basic block's address when one event triggers.

## C basic block information

Reference: `VMCallback`, `qbd_i_addVMEventCB()`, `VMState`

```

VMAction vmcbk(VMInstanceRef vm, const VMState* vmState, GPRState* gprState, FPRState*
↳ fprState, void* data) {

    printf("start:0x%" PRIxWORD " ", end:0x%" PRIxWORD "%s%s\n",
        vmState->basicBlockStart,
        vmState->basicBlockEnd,
        (vmState->event & QBDI_BASIC_BLOCK_NEW)? " BASIC_BLOCK_NEW":"",
        (vmState->event & QBDI_BASIC_BLOCK_ENTRY)? " BASIC_BLOCK_ENTRY":"",
        (vmState->event & QBDI_BASIC_BLOCK_EXIT)? " BASIC_BLOCK_EXIT:"");
    return QBDI_CONTINUE;
}

qbd_i_addVMEventCB(vm, QBDI_BASIC_BLOCK_NEW | QBDI_BASIC_BLOCK_ENTRY | QBDI_BASIC_BLOCK_
↳ EXIT, vmcbk, NULL);

```

## C++ basic block information

Reference: `QBDI::VMCallback`, `QBDI::VM::addVMEventCB()`, `QBDI::VMState`

```
QBDI::VMAction vmcbk(QBDI::VMInstanceRef vm, const QBDI::VMState* vmState,
↳ QBDI::GPRState* gprState, QBDI::FPRState* fprState, void* data) {

    std::cout << std::setbase(16) << "start:0x" << vmState->basicBlockStart
                << ", end:0x" << vmState->basicBlockEnd;
    if (vmState->event & QBDI::BASIC_BLOCK_NEW) {
        std::cout << " BASIC_BLOCK_NEW";
    }
    if (vmState->event & QBDI::BASIC_BLOCK_ENTRY) {
        std::cout << " BASIC_BLOCK_ENTRY";
    }
    if (vmState->event & QBDI::BASIC_BLOCK_EXIT) {
        std::cout << " BASIC_BLOCK_EXIT";
    }
    std::cout << std::endl;
    return QBDI::CONTINUE;
}

vm.addVMEventCB(QBDI::BASIC_BLOCK_NEW | QBDI::BASIC_BLOCK_ENTRY | QBDI::BASIC_BLOCK_EXIT,
↳ vmcbk, nullptr);
```

## PyQBDI basic block information

Reference: `pyqbdi.VMCallback()`, `pyqbdi.VM.addVMEventCB()`, `pyqbdi.VMState`

```
def vmcbk(vm, vmState, gpr, fpr, data):
    # user callback code

    print("start:0x{:x}, end:0x{:x} {}".format(
        vmState.basicBlockStart,
        vmState.basicBlockEnd,
        vmState.event & (pyqbdi.BASIC_BLOCK_NEW | pyqbdi.BASIC_BLOCK_ENTRY | pyqbdi.
↳ BASIC_BLOCK_EXIT) ))
    return pyqbdi.CONTINUE

vm.addVMEventCB(pyqbdi.BASIC_BLOCK_NEW | pyqbdi.BASIC_BLOCK_ENTRY | pyqbdi.BASIC_BLOCK_
↳ EXIT, vmcbk, None)
```

## Frida/QBDI basic block information

Reference: `VMCallback()`, `QBDI.addVMEventCB()`, `VMState()`

```
var vmcbk = vm.newVMCallback(function(vm, state, gpr, fpr, data) {
  var msg = "start:0x" + state.basicBlockStart.toString(16) + ", end:0x" + state.
↪basicBlockEnd.toString(16);
  if (state.event & VMEvent.BASIC_BLOCK_NEW) {
    msg = msg + " BASIC_BLOCK_NEW";
  }
  if (state.event & VMEvent.BASIC_BLOCK_ENTRY) {
    msg = msg + " BASIC_BLOCK_ENTRY";
  }
  if (state.event & VMEvent.BASIC_BLOCK_EXIT) {
    msg = msg + " BASIC_BLOCK_EXIT";
  }
  console.log(msg);
  return VMACTION.CONTINUE;
});

vm.addVMEventCB(VMEvent.BASIC_BLOCK_NEW | VMEvent.BASIC_BLOCK_ENTRY | VMEvent.BASIC_
↪BLOCK_EXIT, vmcbk, null);
```

## Basic block coverage

To perform a code coverage, `BASIC_BLOCK_NEW` can be used to detect the new basic block JITed by QBDI. Some precautions should be taken:

- If a vm is reused to different coverage, the cache must be clear between each run to have independent coverage. However, if you reused the vm to perform incremental coverage, we can keep the cache between runs.
- The coverage only covers the instrumented range.
- This method supposes that the execution of the basic block won't trigger an interruption (exception, signal, ...).
- Code has no overlapping instructions or other forms of obfuscation.

For more precise coverage, `BASIC_BLOCK_ENTRY` or `BASIC_BLOCK_EXIT` can be used instead of `BASIC_BLOCK_NEW`, but the callback may be called more than once for each basic block.

## C coverage

```
// your own coverage library
#include "mycoverage.h"

VMACTION covcbk(VMInstanceRef vm, const VMState* vmState, GPRState* gprState, FPRState*
↪fprState, void* data) {

    myCoverageAdd( (myCoverageData*) data, vmState->basicBlockStart, vmState->
↪basicBlockEnd);
    return QBDI_CONTINUE;
}
```

(continues on next page)

(continued from previous page)

```

myCoverageData cover;

qbd_i_addVMEventCB(vm, QBDI_BASIC_BLOCK_NEW, covcbk, &cover);

// run the VM
// ....

// print the coverage
myCoveragePrint(&cover);

```

## C++ coverage

QBDI has a tiny range set class (*QBDI::RangeSet*), usable only with the C++ API.

```

QBDI::VMAction covcbk(QBDI::VMInstanceRef vm, const QBDI::VMState* vmState,
↳ QBDI::GPRState* gprState, QBDI::FPRState* fprState, void* data) {

    QBDI::RangeSet<QBDI::rword>* rset = static_cast<QBDI::RangeSet<QBDI::rword>*>(data);
    rset->add({vmState->basicBlockStart, vmState->basicBlockEnd});

    return QBDI::CONTINUE;
}

QBDI::RangeSet<QBDI::rword> rset;

vm.addVMEventCB(QBDI::BASIC_BLOCK_NEW, covcbk, &rset);

// run the VM
// ....

// print the coverage
for (const auto r: rset.getRanges()) {
    std::cout << std::setbase(16) << "0x" << r.start() << " to 0x" << r.end() <<
↳ std::endl;
}

```

## PyQBDI coverage

```

def covcbk(vm, vmState, gpr, fpr, data):

    if vmState.basicBlockEnd not in data['cov'] or vmState.basicBlockStart < data['cov
↳ '][vmState.basicBlockEnd][0]:
        data['cov'][vmState.basicBlockEnd] = (vmState.basicBlockStart, vmState.
↳ basicBlockEnd)
        return pyqbd_i.CONTINUE

cov = {"cov": {}}

```

(continues on next page)

(continued from previous page)

```

vm.addVMEventCB(pyqbd.BASIC_BLOCK_NEW, covcbk, cov)

# run the VM
# ....

for _, c in cov['cov'].items():
    print(f"0x{c[0]:x} to 0x{c[1]:x}")

```

In addition, a coverage script that generates DRCOV coverage is available in [examples/pyqbd/coverage.py](#).

## Frida/QBDI coverage

```

var covcbk = vm.newVMCallback(function(vm, state, gpr, fpr, cov) {
    if ( (! cov[state.basicBlockEnd]) || state.basicBlockStart < cov[state.
↪basicBlockEnd][0] ) {
        cov[state.basicBlockEnd] = [state.basicBlockStart, state.basicBlockEnd]
    }
    return VMACTION.CONTINUE;
});

var cov = {};

vm.addVMEventCB(VMEVENT.BASIC_BLOCK_NEW, covcbk, cov);

// run the VM
// ....

for(var c in cov){
    console.log("0x" + cov[c][0].toString(16) + " to 0x" + cov[c][1].toString(16));
}

```

## Edge coverage

The BASIC\_BLOCK\_EXIT event can be used to detect the edge between basic block. As the event is triggered after the execution of the basic block, the next address can be found in the GPRState. The address pair (state.basicBlockEnd, gpr.rip) is the edge to store in the coverage.

## 2.4.2 Execution transfert event

### Introduction

One limitation of QBDI is it shares the heap and some library with the instrumented code. With this design, the user may use any shared library and doesn't need to statically link all their dependencies with their code. However, some method must not be instrumented in QBDI:

- The heap allocator method (malloc, free, ...).
- Any no reentrant method shared between the target code and QBDI itself.
- Any no reentrant method shared between the target code and user callbacks.

When the target code calls one of these methods, QBDI restores the native execution. The return address is changed in order to catch the return and to continue the instrumentation of the code. Two events allow the user to detect this mechanism:

- `EXEC_TRANSFER_CALL`: called before restoring native execution for the method.
- `EXEC_TRANSFER_RETURN`: called after the execution of the method.

These two events can be used to retrieve the method and its parameters before the call and its return value after. `EXEC_TRANSFER_CALL` can also be used to emulate a method call.

## Get native call symbols

When QBDI needs to restore the native execution, the user may retrieve the name of the calling method based on the current address. The associated symbol can be found with `dladdr` (on Linux and OSX) or `SymFromAddr` (on Windows).

We recommend forcing the linker to resolve all symbols before running the VM. This can be achieved with:

- `LD_BIND_NOW=1` on Linux
- `DYLD_BIND_AT_LAUNCH=1` on OSX

## With `dladdr`

`dladdr` may not find the symbol associated with an address if it's not an exported symbol. If several symbols are associated, only one is returned.

```
static VMAction transfertcbk(VMInstanceRef vm, const VMState *vmState, GPRState_
↳ *gprState, FPRState *fprState, void *data) {
    Dl_info info = {0};
    dladdr((void*)gprState->rip, &info);

    if (info.dli_sname != NULL) {
        printf("Call %s (addr: 0x%" PRIxWORD ")\\n", info.dli_sname, gprState->rip);
    } else {
        printf("Call addr: 0x%" PRIxWORD "\\n", gprState->rip);
    }
    return QBDI_CONTINUE;
}
```

```
qbdi_addVMEventCB(vm, QBDI_EXEC_TRANSFER_CALL, transfertcbk, NULL);
```

```
import ctypes
import ctypes.util

class Dl_info(ctypes.Structure):
    _fields_ = [('dli_fname', ctypes.c_char_p),
                ('dli_fbase', ctypes.c_void_p),
                ('dli_sname', ctypes.c_char_p),
                ('dli_saddr', ctypes.c_void_p)]

libdl_path = ctypes.util.find_library('dl')
assert libdl_path != None
```

(continues on next page)

(continued from previous page)

```

libdl = ctypes.cdll.LoadLibrary(libdl_path)
libdl.dladdr.argtypes = (ctypes.c_void_p, ctypes.POINTER(Dl_info))

def dladdr(addr):

    res = Dl_info()
    result = libdl.dladdr(ctypes.cast(addr, ctypes.c_void_p), ctypes.byref(res))

    return res.dli_sname

def transfertcbk(vm, vmState, gpr, fpr, data):

    print("Call {} (addr: 0x{:x})".format(
        dladdr(gpr.rip),
        gpr.rip))

    return pyqbdι.CONTINUE

vm.addVMEventCB(pyqbdι.EXEC_TRANSFER_CALL, transfertcbk, None)

```

### With lief

[Lief](#) is a C, C++ and python library that aims to parse ELF, PE and MachO file formats. This library can extract all the symbols associated with an address, including the non-exported one. This solution can resolve more addresses, but could be slower than `dladdr`.

For ELF binary, the following code prints for each `EXEC_TRANSFER_CALL` event, the symbols associated with the target address. For PE library, the user may need to parse the PDB file of the library to get the symbol associated with the target address.

```

#include <LIEF/LIEF.hpp>

class Module {
public:
    std::string path;
    QBDI::Range<QBDI::rword> range;

    Module(const QBDI::MemoryMap& m) : path(m.name), range(m.range) {}

    void append(const QBDI::MemoryMap& m) {
        if (m.range.start() < range.start()) {
            range.setStart(m.range.start());
        }
        if (m.range.end() > range.end()) {
            range.setEnd(m.range.end());
        }
    }
};

class AddrResolver {
private:

```

(continues on next page)



(continued from previous page)

```

std::vector<Module> modules;
std::unordered_set<std::string> loaded_path;
std::unordered_map<QBDI::rword, std::unordered_set<std::string>> resolv_cache;

void cacheModules();
const Module* getModule(QBDI::rword addr, bool reload = true);
void loadModule(const Module& m);

public:
    AddrResolver() {
        cacheModules();
    }

    const std::unordered_set<std::string>& resolve(QBDI::rword addr);
};

void AddrResolver::cacheModules() {
    modules.clear();

    for (const auto& map : QBDI::getCurrentProcessMaps(true)) {
        auto r = std::find_if(std::begin(modules), std::end(modules),
            [&](const Module& m){return m.path == map.name;});
        if (r != std::end(modules)) {
            r->append(map);
        } else if (map.name.find("/") != std::string::npos) {
            modules.emplace_back(map);
        }
    }
}

const Module* AddrResolver::getModule(QBDI::rword addr, bool reload) {
    const auto r = std::find_if(std::begin(modules), std::end(modules),
        [&](const Module& m){return m.range.contains(addr);});
    if (r != std::end(modules)) {
        return &*r;
    } else if (reload) {
        cacheModules();
        return getModule(addr, false);
    } else {
        return nullptr;
    }
}

void AddrResolver::loadModule(const Module& m) {
    std::cout << "Load Module " << m.path << std::endl;
    if (loaded_path.find(m.path) != loaded_path.end()) {
        return;
    }
    std::unique_ptr<LIEF::ELF::Binary> externlib = LIEF::ELF::Parser::parse(m.path);
    if (not externlib) {
        return;
    }
}

```

(continues on next page)

(continued from previous page)

```

    for (const auto& s: externlib->symbols()) {
        QBDI::rword addr = s.value() + m.range.start();
        resolv_cache[addr].emplace(s.demangled_name());
    }

    loaded_path.emplace(m.path);
}

const std::unordered_set<std::string>& AddrResolver::resolve(QBDI::rword addr) {
    const auto & symnames = resolv_cache[addr];
    if (!symnames.empty()) {
        return symnames;
    }
    std::cout << std::setbase(16) << "Fail to found 0x" << addr << std::endl;
    const Module* m = getModule(addr);
    if (m != nullptr) {
        loadModule(*m);
    }
    return symnames;
}

QBDI::VMAction transfertCBK(QBDI::VMInstanceRef vm, const QBDI::VMState* vmState,
↳QBDI::GPRState* gprState, QBDI::FPRState* fprState, void* data) {
    const std::unordered_set<std::string>& r = static_cast<AddrResolver*>(data)->
↳resolve(gprState->rip);

    if (r.empty()) {
        std::cout << std::setbase(16) << "Call addr: 0x" << gprState->rip << std::endl;
    } else {
        std::cout << "Call ";
        for (const auto& s: r) {
            std::cout << s << " ";
        }
        std::cout << std::setbase(16) << "(addr: 0x" << gprState->rip << ")" <<
↳std::endl;
    }
    return QBDI::CONTINUE;
}

AddrResolver data;
vm->addVMEventCB(QBDI::EXEC_TRANSFER_CALL, transfertCBK, &data);

```

```

import lief
import pyqbd

class Module:
    def __init__(self, module):
        self.name = module.name
        self.range = pyqbd.Range(module.range.start, module.range.end)

    def append(self, module):
        assert module.name == self.name

```

(continues on next page)

(continued from previous page)

```

    if module.range.start < self.range.start:
        self.range.start = module.range.start
    if self.range.end < module.range.end:
        self.range.end = module.range.end

class AddrResolver:

    def __init__(self):
        self.lib_cache = []
        self.resolv_cache = {}
        self.map_cache = self.get_exec_maps()

    def get_exec_maps(self):
        maps = {}
        for m in pyqbdι.getCurrentProcessMaps(True):
            if m.name in maps:
                maps[m.name].append(m)
            elif '/' in m.name:
                maps[m.name] = Module(m)
        return maps

    def get_addr_maps(self, addr):
        for _, m in self.map_cache.items():
            if addr in m.range:
                return m
        self.map_cache = self.get_exec_maps()
        for _, m in self.map_cache.items():
            if addr in m.range:
                return m
        return None

    def load_lib(self, maps):
        if maps.name in self.lib_cache:
            return

        # use lief.PE or lief.MACO if not ELF file
        lib = lief.ELF.parse(maps.name)
        if lib is None:
            return

        for s in lib.symbols:
            addr = s.value + maps.range.start
            if addr in self.resolv_cache:
                if s.name not in self.resolv_cache[addr]:
                    self.resolv_cache[addr].append(s.name)
            else:
                self.resolv_cache[addr] = [s.name]

        self.lib_cache.append(maps.name)

    def get_names(self, addr):

```

(continues on next page)

(continued from previous page)

```

    if addr in self.resolv_cache:
        return self.resolv_cache[addr]

    maps = self.get_addr_maps(addr)
    if maps == None:
        return []
    self.load_lib(maps)
    if addr in self.resolv_cache:
        return self.resolv_cache[addr]
    self.resolv_cache[addr] = []
    return []

def transfertcbk(vm, vmState, gpr, fpr, data):

    f_names = data['resolver'].get_names(gpr.rip)
    if f_names != []:
        print("Call {} (addr: 0x{:x})".format(f_names, gpr.rip))
    else:
        print("Call addr: 0x{:x}".format(gpr.rip))

    return pyqbd.CONTINUE

ctx = {
    "resolver": AddrResolver(),
}

vm.addVMEventCB(pyqbd.EXEC_TRANSFER_CALL, transfertcbk, ctx)

```

Using this snippet with PyQBDIPreload prints the libc calls.

```

$ python -m pyqbdipreload test.py ls
Call ['__strchr_avx2'] (addr: 0x7f2aed2a8330)
Call ['setlocale', '__GI_setlocale'] (addr: 0x7f2aed17a7f0)
Call ['bindtextdomain', '__bindtextdomain'] (addr: 0x7f2aed17e000)
Call ['textdomain', '__textdomain'] (addr: 0x7f2aed1815f0)
Call ['__cxa_atexit', '__GI__cxa_atexit'] (addr: 0x7f2aed1879b0)
Call ['getopt_long'] (addr: 0x7f2aed22d3f0)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['isatty', '__isatty'] (addr: 0x7f2aed239250)
Call ['ioctl', '__ioctl', '__GI_ioctl', '__GI__ioctl'] (addr: 0x7f2aed23d590)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
Call ['__errno_location', '__GI__errno_location'] (addr: 0x7f2aed16fde0)
Call ['__libc_malloc', 'malloc', '__GI__libc_malloc', '__malloc'] (addr: 0x7f2aed1d3320)
Call ['__memcpy_avx_unaligned', '__memmove_avx_unaligned'] (addr: 0x7f2aed2ab4a0)
Call ['__errno_location', '__GI__errno_location'] (addr: 0x7f2aed16fde0)
Call ['__libc_malloc', 'malloc', '__GI__libc_malloc', '__malloc'] (addr: 0x7f2aed1d3320)
Call ['__memcpy_avx_unaligned', '__memmove_avx_unaligned'] (addr: 0x7f2aed2ab4a0)

```

(continues on next page)

(continued from previous page)

```
Call ['getenv', '__GI_getenv'] (addr: 0x7f2aed186b20)
....
```

## 2.5 API

This section contains the documentation of every QBDI API.

### 2.5.1 API description

This section gives the big picture of all the APIs QBDI offers. It may help you better understand the way QBDI works and the overall design behind it.

#### Injection

Instrumentation with QBDI implies having both QBDI and the target program inside the same process. Three types of injections are currently possible with QBDI.

#### Create a QBDI program

The first type of injection is to create an executable that uses QBDI and loads the target code. This injection is available with C, C++ and PyQBDI APIs and should be used if you can compile the target code inside the client binary or load it as a library.

The main steps of this injection are:

- Load the code (`dlopen`, `LoadLibrary`, ...)
- Initialise a new QBDI VM
- Select instrumentation ranges
- Allocate a stack for the target process
- Define callbacks
- Call a target method inside the VM

#### Inject a preload library

This injection forces the loader to add a custom library inside a new process. The preloaded library will catch the main address and allow users to instrument it. This injection should be used if you want to instrument a program from the start of the `main` method to the end.

We provide a small tool called *QBDIPreload* for doing so on Linux and macOS. QBDIPreload (and its implementation *PyQBDIPreload* for *PyQBDI*) automatically puts a hook on the `main` method and accordingly prepares a QBDI VM that can be used out of the box.

Typically, the different stages are:

- Wait for *qbdipreload\_on\_main()* or *pyqbdipreload\_on\_run()* to be called with an initialised QBDI VM
- Define callbacks

- Run the main method inside the VM

## Inject with Frida

Frida works on a wide variety of systems and brings powerful and handy injection mechanisms. It is why the Frida/QBDI subproject relies on those to inject itself into processes. On top of that, while developing their scripts, users are free to take advantage of both Frida and QBDI APIs.

Tracing a specific function can be summed up as:

- Inject a script into a process with Frida
- Put callbacks on the target functions
- Wait for the hooks to be triggered
- Create a QBDI VM, synchronise the context and define instrumentation ranges
- Register callbacks
- Remove the instrumentation added by Frida
- Run the function in the context of QBDI
- Restore the Frida hook for potential future calls
- Return the return value obtained from QBDI

## Instrumentation ranges

- Global APIs: *C*, *C++*, *PyQBDI*, *Frida/QBDI*

The Instrumentation Range is a range of addresses where QBDI will instrument the original code. When the programme counter gets out of this scope, QBDI will try to restore a native and uninstrumented execution. For performance reasons, it is rarely recommended to instrument all the guest code. Moreover, you must bear in mind that QBDI shares the same standard library as the guest and some methods are not *reentrant* (more details in *Limitations*).

The current mechanism is implemented by the `ExecBroker` and only supports external calls out of the instrumentation range. When the execution gets out of the range, `ExecBroker` will try to find an address on the stack that is inside the instrumentation range. If an address is found, it will be replaced by a custom one and the execution is restored without instrumentation. When the process returns to this address `ExecBroker` will capture its state and continue the execution at the expected address. If any valid return address is found, the instrumentation will continue until finding a valid return address.

The following limitations are known:

- The instrumentation range must be at a function level, and if possible, at library level. A range that includes only some instructions of a function will produce an unpredictable result.
- When the native instrumentation goes out of the instrumentation range, the only method to restore the instrumentation is to return to the modified address. Any other executions of code inside the instrumentation range will not be caught (callbacks, ...).
- The current `ExecBroker` doesn't support any exception mechanism, included the *setjmp/longjmp*.
- The instrumentation range, and QBDI in general, are **not** a security sandbox. The code may escape and runs without instrumentation.

The instrumentation ranges can be managed through:

- `addInstrumentedRange` and `removeInstrumentedRange` to add or remove a specific range of address

- `addInstrumentedModule` and `removeInstrumentedModule` to add or remove a library/module with his name
- `addInstrumentedModuleFromAddr` and `removeInstrumentedModuleFromAddr` to add or remove a library/module with one of his addresses
- `instrumentAllExecutableMaps` and `removeAllInstrumentedRanges` to add or remove all the executable range

## Register state

- Global APIs: *C, C++, PyQBDI, Frida/QBDI*
- Management APIs: *C, C++, PyQBDI, Frida/QBDI*

QBDI defines two structures for the registers: `GPRState` and `FPRState`.

- `GPRState` contains all the General Purpose registers such as `rax`, `rsp`, `rip` or `eflags` on X86\_64.
- `FPRState` contains the the Floating Point registers.

Inside a `InstCallback` and `VMCallback`, the current state is passed as a parameter and any change on it will affect the execution. Outside of a callback, `GPRState` and `FPRState` can be retrieved and set with `getGPRState`, `setGPRState`, `getFPRState` and `setFPRState`.

---

**Note:** A modification of the instruction counter (e.g. `RIP`) in an `InstCallback` or a `VMCallback` is not effective if `BREAK_TO_VM` is not returned.

---

## User callbacks

- Global APIs: *C, C++, PyQBDI, Frida/QBDI*

QBDI allows users to register callbacks that are called throughout the execution of the target. These callbacks can be used to determine what the program is doing or to modify its state. Some callbacks must return an action to specify whether the execution should continue or stop or if the context needs to be reevaluated.

All user callbacks must be written in C, C++, Python or JS. However, there are a few limitations:

- As the target registers are saved, the callback can use any register by respecting the standard calling convention of the current platform.
- Some methods of the VM are not *reentrant* and must not be called within the scope of a callback. (`run`, `call`, `setOptions`, `precacheBasicBlock`, `destructor`, `copy` and `move` operators)
- The `BREAK_TO_VM` action should be returned instead of the `CONTINUE` action if the state of the VM is somehow changed. It covers:
  - Add or remove callbacks
  - Modify instrumentation ranges
  - Clear the cache
  - Change the instruction counter register in `GPRState` (the other registers can be altered without the need of returning `BREAK_TO_VM`).

## Instruction callbacks

- Global APIs: *C*, *C++*, *PyQBDI*, *Frida/QBDI*

An instruction callback (`InstCallback`) is a callback that will be called **before** or **after** executing an instruction. Therefore, an `InstCallback` can be inserted at two different positions:

- before the instruction (`PREINST` – short for *pre-instruction*)
- after the instruction (`POSTINST` – short for *post-instruction*). At this point, the register state has been automatically updated so the instruction counter points to the next code address.

---

**Note:** A `POSTINST` callback will be called after the instruction and before the next one. If on a call instruction, the callback is then called before the first instruction of the called method.

---

An `InstCallback` can be registered for a specific instruction (`addCodeAddrCB`), any instruction in a specified range (`addCodeRangeCB`) or any instrumented instruction (`addCodeCB`). The instruction also be targeted by their mnemonic (or LLVM opcode) (`addMnemonicCB`).

## VM callbacks

- `VMCallback` APIs: *C*, *C++*, *PyQBDI*, *Frida/QBDI*
- `VMEvent` APIs: *C*, *C++*, *PyQBDI*, *Frida/QBDI*

A `VMEvent` callback (`VMCallback`) is a callback that will be called when the VM reaches a specific state. The current supported events are:

- At the beginning and the end of a basic block (`BASIC_BLOCK_ENTRY` and `BASIC_BLOCK_EXIT`). A basic block in QBDI consists of consecutive instructions that don't change the instruction counter except the last one. These events are triggered respectively by `SEQUENCE_ENTRY` and `SEQUENCE_EXIT` as well.
- At the beginning and the end of a sequence (`SEQUENCE_ENTRY` and `SEQUENCE_EXIT`). A sequence is a part of a basic block that has been *JIT'd* consecutively. These events should only be used for `getBBMemoryAccess`.
- When a new uncached basic block is being *JIT'd* (`BASIC_BLOCK_NEW`). This event is also always triggered by `BASIC_BLOCK_ENTRY` and `SEQUENCE_ENTRY`.
- Before and after executing some uninstrumented code with the `ExecBroker` (`EXEC_TRANSFER_CALL` and `EXEC_TRANSFER_RETURN`).

When a `VMCallback` is called, a state of the VM (`VMState`) is passed in argument. This state contains:

- A set of events that trigger the callback. If the callback is registered for several events that trigger at the same moment, the callback will be called only once.
- If the event is related to a basic block or a sequence, the start and the end addresses of the current basic block and sequence are provided.



## Memory callbacks

- Global APIs: *C, C++, PyQBDI, Frida/QBDI*

The memory callback is an `InstCallback` that will be called when the target program reads or writes the memory. The callback can be called only when a specific address is accessed (`addMemAddrCB`), when a range of address is accessed (`addMemRangeCB`) or when any memory is accessed (`addMemAccessCB`).

Unlike with the instruction callback registration, the position of a memory callback cannot be manually specified. If a memory callback is solely registered for read accesses, it will be called **before** the instruction. Otherwise, it will be called **after** executing the instruction.

## Instrumentation rule callbacks

- Global APIs: *C, C++, PyQBDI, Frida/QBDI*

Instrumentation rule callbacks are an advanced feature of QBDI. It allows users to define a callback (`InstrRuleCallback`) that will be called during the instrumentation process. The callback will be called for each instruction and can define an `InstCallback` to call before or after the current instruction. An argument contains an `InstAnalysis` of the current instruction and can be used to define the callback to insert for this instruction.

An `InstrRuleCallback` can be registered for all instructions (`addInstrRule`) or only for a specific range (`addInstrRuleRange`).

---

**Note:** The instrumentation process of QBDI responsible of *JITing* instructions may analyse more than once the same instruction. Consequently, the instrumentation rule callback must always return the same result even though the instruction has already been instrumented.

---

## Instruction analysis

- Global APIs: *C, C++, PyQBDI, Frida/QBDI*
- Getter APIs: *C, C++, PyQBDI, Frida/QBDI*

QBDI provides some basic analysis of the instruction through the `InstAnalysis` object. Within an `InstCallback`, the analysis of the current instruction should be retrieved with `getInstAnalysis`. Otherwise, the analysis of any instruction in the cache can be obtained with `getCachedInstAnalysis`. The `InstAnalysis` is cached inside QBDI and is valid until the next cache modification (add new instructions, clear cache, ...).

Four types of analysis are available. If a type of analysis is not selected, the corresponding field of the `InstAnalysis` object remains empty and should not be used.

- **ANALYSIS\_INSTRUCTION:** This analysis type provides some generic information about the instruction, like its address, its size, its mnemonic (LLVM opcode) or its condition type if the instruction is conditional.
- **ANALYSIS\_DISASSEMBLY:** This analysis type provides the disassembly of the instruction. For X86 and X86\_64, the syntax Intel is used by default. The syntax can be changed with the option `OPT_ATT_SYNTAX`.
- **ANALYSIS\_OPERANDS:** This analysis type provides information about the operand of the instruction. An operand can be a register or an immediate. If a register operand can be empty, the special type `OPERAND_INVALID` is used. The implicit register of instruction is also present with a specific flag. Moreover, the member `flagsAccess` specifies whether the instruction will use or set the generic flag.
- **ANALYSIS\_SYMBOL:** This analysis type detects whether a symbol is associated with the current instruction.

The source file `test/API/InstAnalysisTest_<arch>.cpp` shows how one can deal with instruction analysis and may be taken as a reference for the `ANALYSIS_INSTRUCTION` and `ANALYSIS_OPERANDS` types.

## Memory accesses

- Global APIs: *C, C++, PyQBDI, Frida/QBDI*
- Getter APIs: *C, C++, PyQBDI, Frida/QBDI*

Due to performance considerations, the capture of memory accesses (`MemoryAccess`) is not enabled by default. It is only turned on when a memory callback is registered or explicitly requested with `recordMemoryAccess`. Collecting read and written accesses can be enabled either together or separately.

Two APIs can be used to get the memory accesses:

- `getInstMemoryAccess` can be used within an instruction callback or a memory callback to retrieve the access of the current instruction. If the callback is before the instruction (`PREINST`), only read accesses will be available.
- `getBBMemoryAccess` must be used in a `VMEvent` callback with `SEQUENCE_EXIT` to get all the memory accesses for the last sequence.

Both return a list of `MemoryAccess`. Generally speaking, a `MemoryAccess` will have the address of the instruction responsible of the access, the access address and size, the type of access and the value read or written. However, some instructions can do complex accesses and some information can be missing or incomplete. The flags of `MemoryAccess` can be used to detect these cases:

- `MEMORY_UNKNOWN_SIZE`: the size of the access is unknown. This is currently used for instruction with `REP` prefix before the execution of the instruction. The size is determined after the instruction when the access has been completed.
- `MEMORY_MINIMUM_SIZE`: The size of the access is a minimum size. The access is complex but at least size of memory is accessed. This is currently used for the `XSAVE*` and `XRSTOR*` instructions.
- `MEMORY_UNKNOWN_VALUE`: The value of the access hasn't been captured. This flag will be used when the access size is greater than the size of a `rword`. It's also used for instructions with `REP` in `X86` and `X86_64`.

## Options

The options of the VM allow changing some internal mechanisms of QBDI. For most uses of QBDI, no option needs to be specified. The options are specified when the VM is created and can be changed with `setOptions` when the VM is not running. After changing the options, the cache needs to be cleared to apply the changes to all the instructions.

- `OPT_DISABLE_FPR`: This option disables the Floating Point Registers support. QBDI will not back up and restore any `FPRState` registers.
- `OPT_DISABLE_OPTIONAL_FPR`: if `OPT_DISABLE_FPR` is not enabled, this option will force the `FPRState` to be restored and saved before and after any instruction. By default, QBDI will try to detect the instructions that make use of floating point registers and only restore for these precise instructions.
- `OPT_ATT_SYNTAX`: For `X86` and `X86_64` architectures, this option changes the syntax of `InstAnalysis`. disassembly to AT&T instead of the Intel one.

## 2.5.2 C API

### Introduction

The C API offers bindings over the C++ API. The VM class' methods are replaced by C functions that receive an object of type `VMInstanceRef` as a first parameter.

This API is compatible with *QBDIPreload* on Linux and macOS.

### VM object

type `VMInstanceRef`

An abstract pointer to the VM object.

void `qbdi_initVM`(*VMInstanceRef* \*instance, const char \*cpu, const char \*\*mattrs, *Options* opts)  
Create and initialize a VM instance.

#### Parameters

- **instance** – [out] VM instance created.
- **cpu** – [in] A C string naming the CPU model to use. If NULL, the default architecture CPU model is used (see LLVM documentation for more details).
- **mattrs** – [in] A NULL terminated array of C strings specifying the attributes of the cpu model. If NULL, no additional features are specified.
- **opts** – [in] The options to enable in the VM

void `qbdi_terminateVM`(*VMInstanceRef* instance)  
Destroy an instance of VM. This method mustn't be called when the VM runs.

**Parameters** **instance** – [in] VM instance.

### Options

*Options* `qbdi_getOptions`(*VMInstanceRef* instance)  
Get the current Options

**Parameters** **instance** – [in] VM instance.

**Returns** The current options of the VM

void `qbdi_setOptions`(*VMInstanceRef* instance, *Options* options)  
Set the Options This method mustn't be called when the VM runs.

#### Parameters

- **instance** – [in] VM instance.
- **options** – [in] The new options of the VM.

## State management

*GPRState* \*qbdi\_getGPRState(*VMInstanceRef* instance)

Obtain the current general purpose register state.

**Parameters** *instance* – [in] VM instance.

**Returns** A structure containing the General Purpose Registers state.

*FPRState* \*qbdi\_getFPRState(*VMInstanceRef* instance)

Obtain the current floating point register state.

**Parameters** *instance* – [in] VM instance.

**Returns** A structure containing the Floating Point Registers state.

void qbdi\_setGPRState(*VMInstanceRef* instance, *GPRState* \*gprState)

Set the GPR state

**Parameters**

- *instance* – [in] VM instance.
- *gprState* – [in] A structure containing the General Purpose Registers state.

void qbdi\_setFPRState(*VMInstanceRef* instance, *FPRState* \*fprState)

Set the FPR state

**Parameters**

- *instance* – [in] VM instance.
- *fprState* – [in] A structure containing the Floating Point Registers state.

## Instrumentation range

### Addition

void qbdi\_addInstrumentedRange(*VMInstanceRef* instance, *rword* start, *rword* end)

Add an address range to the set of instrumented address ranges.

**Parameters**

- *instance* – [in] VM instance.
- *start* – [in] Start address of the range (included).
- *end* – [in] End address of the range (excluded).

bool qbdi\_addInstrumentedModule(*VMInstanceRef* instance, const char \*name)

Add the executable address ranges of a module to the set of instrumented address ranges.

**Parameters**

- *instance* – [in] VM instance.
- *name* – [in] The module's name.

**Returns** True if at least one range was added to the instrumented ranges.

bool qbdi\_addInstrumentedModuleFromAddr(*VMInstanceRef* instance, *rword* addr)

Add the executable address ranges of a module to the set of instrumented address ranges using an address belonging to the module.

**Parameters**

- **instance** – [in] VM instance.
- **addr** – [in] An address contained by module's range.

**Returns** True if at least one range was added to the instrumented ranges.

bool **qbdi\_instrumentAllExecutableMaps**(*VMInstanceRef* instance)

Adds all the executable memory maps to the instrumented range set.

**Parameters** **instance** – [in] VM instance.

**Returns** True if at least one range was added to the instrumented ranges.

**Removal**

void **qbdi\_removeInstrumentedRange**(*VMInstanceRef* instance, *rword* start, *rword* end)

Remove an address range from the set of instrumented address ranges.

**Parameters**

- **instance** – [in] VM instance.
- **start** – [in] Start address of the range (included).
- **end** – [in] End address of the range (excluded).

bool **qbdi\_removeInstrumentedModule**(*VMInstanceRef* instance, const char \*name)

Remove the executable address ranges of a module from the set of instrumented address ranges.

**Parameters**

- **instance** – [in] VM instance.
- **name** – [in] The module's name.

**Returns** True if at least one range was removed from the instrumented ranges.

bool **qbdi\_removeInstrumentedModuleFromAddr**(*VMInstanceRef* instance, *rword* addr)

Remove the executable address ranges of a module from the set of instrumented address ranges using an address belonging to the module.

**Parameters**

- **instance** – [in] VM instance.
- **addr** – [in] An address contained by module's range.

**Returns** True if at least one range was removed from the instrumented ranges.

void **qbdi\_removeAllInstrumentedRanges**(*VMInstanceRef* instance)

Remove all instrumented ranges.

**Parameters** **instance** – [in] VM instance.

## Callback management

### InstCallback

uint32\_t **qbdi\_addCodeCB**(*VMInstanceRef* instance, *InstPosition* pos, *InstCallback* cbk, void \*data, int priority)  
Register a callback event for a specific instruction event.

#### Parameters

- **instance** – [in] VM instance.
- **pos** – [in] Relative position of the event callback (QBDI\_PREINST / QBDI\_POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

uint32\_t **qbdi\_addCodeAddrCB**(*VMInstanceRef* instance, *rword* address, *InstPosition* pos, *InstCallback* cbk, void \*data, int priority)

Register a callback for when a specific address is executed.

#### Parameters

- **instance** – [in] VM instance.
- **address** – [in] Code address which will trigger the callback.
- **pos** – [in] Relative position of the callback (QBDI\_PREINST / QBDI\_POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

uint32\_t **qbdi\_addCodeRangeCB**(*VMInstanceRef* instance, *rword* start, *rword* end, *InstPosition* pos, *InstCallback* cbk, void \*data, int priority)

Register a callback for when a specific address range is executed.

#### Parameters

- **instance** – [in] VM instance.
- **start** – [in] Start of the address range which will trigger the callback.
- **end** – [in] End of the address range which will trigger the callback.
- **pos** – [in] Relative position of the callback (QBDI\_PREINST / QBDI\_POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

uint32\_t **qbdi\_addMnemonicCB**(*VMInstanceRef* instance, const char \*mnemonic, *InstPosition* pos, *InstCallback* cbk, void \*data, int priority)

Register a callback event if the instruction matches the mnemonic.

**Parameters**

- **instance** – [in] VM instance.
- **mnemonic** – [in] Mnemonic to match.
- **pos** – [in] Relative position of the event callback (QBDI\_PREINST / QBDI\_POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

**VMEvent**

uint32\_t **qbdi\_addVMEventCB**(*VMInstanceRef* instance, *VMEvent* mask, *VMCallback* cbk, void \*data)

Register a callback event for a specific VM event.

**Parameters**

- **instance** – [in] VM instance.
- **mask** – [in] A mask of VM event type which will trigger the callback.
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

**MemoryAccess**

uint32\_t **qbdi\_addMemAccessCB**(*VMInstanceRef* instance, *MemoryAccessType* type, *InstCallback* cbk, void \*data, int priority)

Register a callback event for every memory access matching the type bitfield made by the instructions.

**Parameters**

- **instance** – [in] VM instance.
- **type** – [in] A mode bitfield: either QBDI\_MEMORY\_READ, QBDI\_MEMORY\_WRITE or both (QBDI\_MEMORY\_READ\_WRITE).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

uint32\_t **qbdi\_addMemAddrCB**(*VMInstanceRef* instance, *rword* address, *MemoryAccessType* type, *InstCallback* cbk, void \*data)

Add a virtual callback which is triggered for any memory access at a specific address matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost.

**Parameters**

- **instance** – [in] VM instance.

- **address** – [in] Code address which will trigger the callback.
- **type** – [in] A mode bitfield: either QBDI\_MEMORY\_READ, QBDI\_MEMORY\_WRITE or both (QBDI\_MEMORY\_READ\_WRITE).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

uint32\_t **qbdi\_addMemRangeCB**(*VMInstanceRef* instance, *rword* start, *rword* end, *MemoryAccessType* type, *InstCallback* cbk, void \*data)

Add a virtual callback which is triggered for any memory access in a specific address range matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost.

#### Parameters

- **instance** – [in] VM instance.
- **start** – [in] Start of the address range which will trigger the callback.
- **end** – [in] End of the address range which will trigger the callback.
- **type** – [in] A mode bitfield: either QBDI\_MEMORY\_READ, QBDI\_MEMORY\_WRITE or both (QBDI\_MEMORY\_READ\_WRITE).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or QBDI\_INVALID\_EVENTID in case of failure).

## InstrRuleCallback

uint32\_t **qbdi\_addInstrRule**(*VMInstanceRef* instance, *InstrRuleCallbackC* cbk, *AnalysisType* type, void \*data)

Add a custom instrumentation rule to the VM.

#### Parameters

- **instance** – [in] VM instance.
- **cbk** – [in] A function pointer to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or VMError::INVALID\_EVENTID in case of failure).

uint32\_t **qbdi\_addInstrRuleRange**(*VMInstanceRef* instance, *rword* start, *rword* end, *InstrRuleCallbackC* cbk, *AnalysisType* type, void \*data)

Add a custom instrumentation rule to the VM for a range of address

#### Parameters

- **instance** – [in] VM instance.
- **start** – [in] Begin of the range of address where apply the rule
- **end** – [in] End of the range of address where apply the rule
- **cbk** – [in] A function pointer to the callback



- **type** – [in] Analyse type needed for this instruction function pointer to the callback
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

## Removal

bool **qbdi\_deleteInstrumentation**(*VMInstanceRef* instance, uint32\_t id)

Remove an instrumentation.

### Parameters

- **instance** – [in] VM instance.
- **id** – [in] The id of the instrumentation to remove.

**Returns** True if instrumentation has been removed.

void **qbdi\_deleteAllInstrumentations**(*VMInstanceRef* instance)

Remove all the registered instrumentations.

**Parameters** **instance** – [in] VM instance.

## Run

bool **qbdi\_run**(*VMInstanceRef* instance, *rword* start, *rword* stop)

Start the execution by the DBI from a given address (and stop when another is reached). This method mustn't be called when the VM already runs.

### Parameters

- **instance** – [in] VM instance.
- **start** – [in] Address of the first instruction to execute.
- **stop** – [in] Stop the execution when this instruction is reached.

**Returns** True if at least one block has been executed.

bool **qbdi\_call**(*VMInstanceRef* instance, *rword* \*retVal, *rword* function, uint32\_t argNum, ...)

Call a function using the DBI (and its current state). This method mustn't be called when the VM already runs.

Example:

```
// perform (with QBDI) a call similar to (*funcPtr)(42);
uint8_t *fakestack = NULL;
VMInstanceRef vm;
qbdi_initVM(&vm, NULL, NULL);
GPRState* gprState = qbdi_getGPRState(vm);
qbdi_allocateVirtualStack(gprState, 0x10000000, &fakestack);
qbdi_addInstrumentedModuleFromAddr(vm, funcPtr);
rword retVal;
qbdi_call(vm, &retVal, funcPtr, 1, 42);
```

### Parameters

- **instance** – [in] VM instance.
- **[retval]** – [in] Pointer to the returned value (optional).
- **function** – [in] Address of the function start instruction.
- **argNum** – [in] The number of arguments in the variadic list.
- **...** – [in] A variadic list of arguments.

**Returns** True if at least one block has been executed.

bool **qbdi\_callA**(*VMInstanceRef* instance, *rword* \*retval, *rword* function, uint32\_t argNum, const *rword* \*args)  
Call a function using the DBI (and its current state). This method mustn't be called when the VM already runs.

**Parameters**

- **instance** – [in] VM instance.
- **[retval]** – [in] Pointer to the returned value (optional).
- **function** – [in] Address of the function start instruction.
- **argNum** – [in] The number of arguments in the variadic list.
- **args** – [in] Arguments as an array of rword values.

**Returns** True if at least one block has been executed.

bool **qbdi\_callV**(*VMInstanceRef* instance, *rword* \*retval, *rword* function, uint32\_t argNum, va\_list ap)  
Call a function using the DBI (and its current state). This method mustn't be called when the VM already runs.

**Parameters**

- **instance** – [in] VM instance.
- **[retval]** – [in] Pointer to the returned value (optional).
- **function** – [in] Address of the function start instruction.
- **argNum** – [in] The number of arguments in the variadic list.
- **ap** – [in] An stdarg va\_list object.

**Returns** True if at least one block has been executed.

## InstAnalysis

const *InstAnalysis* \***qbdi\_getInstAnalysis**(const *VMInstanceRef* instance, *AnalysisType* type)  
Obtain the analysis of the current instruction. Analysis results are cached in the VM. The validity of the returned pointer is only guaranteed until the end of the callback, else a deepcopy of the structure is required. This method must only be used in an InstCallback.

**Parameters**

- **instance** – [in] VM instance.
- **type** – [in] Properties to retrieve during analysis.

**Returns** A *InstAnalysis* structure containing the analysis result.

const *InstAnalysis* \***qbdi\_getCachedInstAnalysis**(const *VMInstanceRef* instance, *rword* address, *AnalysisType* type)

Obtain the analysis of a cached instruction. Analysis results are cached in the VM. The validity of the returned pointer is only guaranteed until the end of the callback or a call to a noconst method of the VM instance.

### Parameters

- **instance** – [in] VM instance.
- **address** – [in] The address of the instruction to analyse.
- **type** – [in] Properties to retrieve during analysis.

**Returns** A *InstAnalysis* structure containing the analysis result. null if the instruction isn't in the cache.

## MemoryAccess

*MemoryAccess* \***qbdi\_getInstMemoryAccess**(*VMInstanceRef* instance, size\_t \*size)

Obtain the memory accesses made by the last executed instruction. The method should be called in an InstCallback. Return NULL and a size of 0 if the instruction made no memory access.

### Parameters

- **instance** – [in] VM instance.
- **size** – [out] Will be set to the number of elements in the returned array.

**Returns** An array of memory accesses made by the instruction.

*MemoryAccess* \***qbdi\_getBBMemoryAccess**(*VMInstanceRef* instance, size\_t \*size)

Obtain the memory accesses made by the last executed basic block. The method should be called in a VM-Callback with QBDI\_SEQUENCE\_EXIT. Return NULL and a size of 0 if the basic block made no memory access.

### Parameters

- **instance** – [in] VM instance.
- **size** – [out] Will be set to the number of elements in the returned array.

**Returns** An array of memory accesses made by the basic block.

bool **qbdi\_recordMemoryAccess**(*VMInstanceRef* instance, *MemoryAccessType* type)

Add instrumentation rules to log memory access using inline instrumentation and instruction shadows.

### Parameters

- **instance** – [in] VM instance.
- **type** – [in] Memory mode bitfield to activate the logging for: either QBDI\_MEMORY\_READ, QBDI\_MEMORY\_WRITE or both (QBDI\_MEMORY\_READ\_WRITE).

**Returns** True if inline memory logging is supported, False if not or in case of error.

## Cache management

bool **qbdi\_precacheBasicBlock**(*VMInstanceRef* instance, *rword* pc)

Pre-cache a known basic block This method mustn't be called when the VM runs.

### Parameters

- **instance** – [in] VM instance.
- **pc** – [in] Start address of a basic block

**Returns** True if basic block has been inserted in cache.

void **qbd\_clearCache**(*VMInstanceRef* instance, *rword* start, *rword* end)

Clear a specific address range from the translation cache.

**Parameters**

- **instance** – [in] VM instance.
- **start** – [in] Start of the address range to clear from the cache.
- **end** – [in] End of the address range to clear from the cache.

void **qbd\_clearAllCache**(*VMInstanceRef* instance)

Clear the entire translation cache.

**Parameters** **instance** – [in] VM instance.

## Register state

type **rword**

An integer of the size of a register

- uint32\_t for X86
- uint64\_t for X86\_64

struct **GPRState**

General Purpose Register context.

For X86 architecture:

```
typedef struct QBDI_ALIGNED(4) {
    rword eax;
    rword ebx;
    rword ecx;
    rword edx;
    rword esi;
    rword edi;
    rword ebp;
    rword esp;
    rword eip;
    rword eflags;
} GPRState;
```

For X86\_64 architecture:

```
typedef struct QBDI_ALIGNED(8) {
    rword rax;
    rword rbx;
    rword rcx;
    rword rdx;
    rword rsi;
    rword rdi;
    rword r8;
    rword r9;
    rword r10;
    rword r11;
```

(continues on next page)

(continued from previous page)

```

rword r12;
rword r13;
rword r14;
rword r15;
rword rbp;
rword rsp;
rword rip;
rword eflags;
// Only backup and restore with OPT_ENABLE_FS_GS
rword fs;
rword gs;
} GPRState;

```

**struct FPRState**

Floating Point Register context.

For X86 architecture:

```

typedef struct QBDI_ALIGNED(16) {
    union {
        FPControl fcw; /* x87 FPU control word */
        uint16_t rfcw;
    };
    union {
        FPStatus fsw; /* x87 FPU status word */
        uint16_t rfs;
    };
    uint8_t ftw; /* x87 FPU tag word */
    uint8_t rsrv1; /* reserved */
    uint16_t fop; /* x87 FPU Opcode */
    uint32_t ip; /* x87 FPU Instruction Pointer offset */
    uint16_t cs; /* x87 FPU Instruction Pointer Selector */
    uint16_t rsrv2; /* reserved */
    uint32_t dp; /* x87 FPU Instruction Operand(Data) Pointer offset */
    uint16_t ds; /* x87 FPU Instruction Operand(Data) Pointer Selector */
    uint16_t rsrv3; /* reserved */
    uint32_t mxcsr; /* MXCSR Register state */
    uint32_t mxcsrmask; /* MXCSR mask */
    MMSTReg stmm0; /* ST0/MM0 */
    MMSTReg stmm1; /* ST1/MM1 */
    MMSTReg stmm2; /* ST2/MM2 */
    MMSTReg stmm3; /* ST3/MM3 */
    MMSTReg stmm4; /* ST4/MM4 */
    MMSTReg stmm5; /* ST5/MM5 */
    MMSTReg stmm6; /* ST6/MM6 */
    MMSTReg stmm7; /* ST7/MM7 */
    char xmm0[16]; /* XMM 0 */
    char xmm1[16]; /* XMM 1 */
    char xmm2[16]; /* XMM 2 */
    char xmm3[16]; /* XMM 3 */
    char xmm4[16]; /* XMM 4 */
    char xmm5[16]; /* XMM 5 */
}

```

(continues on next page)

(continued from previous page)

```

char xmm6[16];      /* XMM 6 */
char xmm7[16];      /* XMM 7 */
char reserved[14 * 16];
char ymm0[16]; /* YMM0[255:128] */
char ymm1[16]; /* YMM1[255:128] */
char ymm2[16]; /* YMM2[255:128] */
char ymm3[16]; /* YMM3[255:128] */
char ymm4[16]; /* YMM4[255:128] */
char ymm5[16]; /* YMM5[255:128] */
char ymm6[16]; /* YMM6[255:128] */
char ymm7[16]; /* YMM7[255:128] */
} FPRState;

```

For X86\_64 architecture:

```

typedef struct QBDI_ALIGNED(16) {
    union {
        FPControl fcw; /* x87 FPU control word */
        uint16_t rfcw;
    };
    union {
        FPStatus fsw; /* x87 FPU status word */
        uint16_t rfsf;
    };
    uint8_t ftw; /* x87 FPU tag word */
    uint8_t rsv1; /* reserved */
    uint16_t fop; /* x87 FPU Opcode */
    uint32_t ip; /* x87 FPU Instruction Pointer offset */
    uint16_t cs; /* x87 FPU Instruction Pointer Selector */
    uint16_t rsv2; /* reserved */
    uint32_t dp; /* x87 FPU Instruction Operand(Data) Pointer offset */
    uint16_t ds; /* x87 FPU Instruction Operand(Data) Pointer Selector */
    uint16_t rsv3; /* reserved */
    uint32_t mxcsr; /* MXCSR Register state */
    uint32_t mxcsrmask; /* MXCSR mask */
    MMSTReg stmm0; /* ST0/MM0 */
    MMSTReg stmm1; /* ST1/MM1 */
    MMSTReg stmm2; /* ST2/MM2 */
    MMSTReg stmm3; /* ST3/MM3 */
    MMSTReg stmm4; /* ST4/MM4 */
    MMSTReg stmm5; /* ST5/MM5 */
    MMSTReg stmm6; /* ST6/MM6 */
    MMSTReg stmm7; /* ST7/MM7 */
    char xmm0[16]; /* XMM 0 */
    char xmm1[16]; /* XMM 1 */
    char xmm2[16]; /* XMM 2 */
    char xmm3[16]; /* XMM 3 */
    char xmm4[16]; /* XMM 4 */
    char xmm5[16]; /* XMM 5 */
    char xmm6[16]; /* XMM 6 */
    char xmm7[16]; /* XMM 7 */
}

```

(continues on next page)

(continued from previous page)

```

char xmm8[16];      /* XMM 8 */
char xmm9[16];      /* XMM 9 */
char xmm10[16];     /* XMM 10 */
char xmm11[16];     /* XMM 11 */
char xmm12[16];     /* XMM 12 */
char xmm13[16];     /* XMM 13 */
char xmm14[16];     /* XMM 14 */
char xmm15[16];     /* XMM 15 */
char reserved[6 * 16];
char ymm0[16];      /* YMM0[255:128] */
char ymm1[16];      /* YMM1[255:128] */
char ymm2[16];      /* YMM2[255:128] */
char ymm3[16];      /* YMM3[255:128] */
char ymm4[16];      /* YMM4[255:128] */
char ymm5[16];      /* YMM5[255:128] */
char ymm6[16];      /* YMM6[255:128] */
char ymm7[16];      /* YMM7[255:128] */
char ymm8[16];      /* YMM8[255:128] */
char ymm9[16];      /* YMM9[255:128] */
char ymm10[16];     /* YMM10[255:128] */
char ymm11[16];     /* YMM11[255:128] */
char ymm12[16];     /* YMM12[255:128] */
char ymm13[16];     /* YMM13[255:128] */
char ymm14[16];     /* YMM14[255:128] */
char ymm15[16];     /* YMM15[255:128] */
} FPRState;

```

struct **MMSTReg**

### Public Members

char **reg**[10]

char **rsrv**[6]

struct **FPControl**

### Public Members

uint16\_t **invalid**

uint16\_t **denorm**

uint16\_t **zdiv**

uint16\_t **ovrfl**

uint16\_t **undfl**

uint16\_t **precis**

uint16\_t **\_\_pad0\_\_**

uint16\_t **pc**

uint16\_t **rc**

uint16\_t **\_\_pad1\_\_**

uint16\_t **\_\_pad2\_\_**

struct **FPStatus**

### Public Members

uint16\_t **invalid**

uint16\_t **denorm**

uint16\_t **zdiv**



uint16\_t **ovrfl**

uint16\_t **undfl**

uint16\_t **precis**

uint16\_t **stkflt**

uint16\_t **errsumm**

uint16\_t **c0**

uint16\_t **c1**

uint16\_t **c2**

uint16\_t **tos**

uint16\_t **c3**

uint16\_t **busy**

**REG\_RETURN**

**REG\_BP**

**REG\_SP**

**REG\_PC**

**NUM\_GPR**

## Callback

typedef *VMAction* (**\*InstCallback**)(*VMInstanceRef* vm, *GPRState* \*gprState, *FPRState* \*fprState, void \*data)  
Instruction callback function type.

**Param vm** [in] VM instance of the callback.

**Param gprState** [in] A structure containing the state of the General Purpose Registers. Modifying it affects the VM execution accordingly.

**Param fprState** [in] A structure containing the state of the Floating Point Registers. Modifying it affects the VM execution accordingly.

**Param data** [in] User defined data which can be defined when registering the callback.

**Return** The callback result used to signal subsequent actions the VM needs to take.

typedef *VMAction* (**\*VMCallback**)(*VMInstanceRef* vm, const *VMState* \*vmState, *GPRState* \*gprState, *FPRState* \*fprState, void \*data)  
VM callback function type.

**Param vm** [in] VM instance of the callback.

**Param vmState** [in] A structure containing the current state of the VM.

**Param gprState** [in] A structure containing the state of the General Purpose Registers. Modifying it affects the VM execution accordingly.

**Param fprState** [in] A structure containing the state of the Floating Point Registers. Modifying it affects the VM execution accordingly.

**Param data** [in] User defined data which can be defined when registering the callback.

**Return** The callback result used to signal subsequent actions the VM needs to take.

typedef void (**\*InstrRuleCallbackC**)(*VMInstanceRef* vm, const *InstAnalysis* \*inst, *InstrRuleDataVec* cbks, void \*data)  
Instrumentation rule callback function type for C API.

**Param vm** [in] VM instance of the callback.

**Param inst** [in] AnalysisType of the current instrumented Instruction.

**Param cbks** [in] An object to add the callback to apply for this instruction. InstCallback can be add with qbdi\_addInstrRuleData.

**Param data** [in] User defined data which can be defined when registering the callback.

void **qbdi\_addInstrRuleData**(*InstrRuleDataVec* cbks, *InstPosition* position, *InstCallback* cbk, void \*data, int priority)  
Add a callback for the current instruction

### Parameters

- **cbks** – [in] InstrRuleDataVec given in argument
- **position** – [in] Relative position of the callback (QBDI\_PREINST / QBDI\_POSTINST).
- **cbk** – [in] A function pointer to the callback
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] Priority of the callback

type **InstrRuleDataVec**

An abstract type to append InstCallback for the current instruction

enum **InstPosition**

Position relative to an instruction.

*Values:*

enumerator **QBDI\_PREINST**

Positioned before the instruction.

enumerator **QBDI\_POSTINST**

Positioned after the instruction.

enum **CallbackPriority**

Priority of callback

A callback with an higher priority will be call before a callback with a lower priority.

ie:

- a. CBpre(p = 10)
- b. CBpre(p = 0)
- c. CBpre(p = -10)
- d. instrumented instruction
- e. CBpost(p = 10)
- f. CBpost(p = 0)
- g. CBpost(p = -10)

When the [MemoryAccess](#) API is used in a callback, the priority of the callback must not be greater than PRIORITY\_MEMACCESS\_LIMIT

*Values:*

enumerator **QBDI\_PRIORITY\_DEFAULT**

Default priority for callback

enumerator **QBDI\_PRIORITY\_MEMACCESS\_LIMIT**

Maximum priority if getInstMemoryAccess is used in the callback

enum **VMAction**

The callback results.

*Values:*

enumerator **QBDI\_CONTINUE**

The execution of the basic block continues.

enumerator **QBDI\_SKIP\_INST**

Available only with PREINST InstCallback. The instruction and the remained PREINST callbacks are skip. The execution continue with the POSTINST instruction.

We recommend to use this result with a low priority PREINST callback in order to emulate the instruction without skipping the POSTINST callback.

enumerator **QBDI\_SKIP\_PATCH**

Available only with InstCallback. The current instruction and the reminding callback (PRE and POST) are skip. The execution continues to the next instruction.

For instruction that change the instruction pointer (jump/call/ret), BREAK\_TO\_VM must be used instead of SKIP.

SKIP can break the record of *MemoryAccess* for the current instruction.

enumerator **QBDI\_BREAK\_TO\_VM**

The execution breaks and returns to the VM causing a complete reevaluation of the execution state. A BREAK\_TO\_VM is needed to ensure that modifications of the Program Counter or the program code are taken into account.

enumerator **QBDI\_STOP**

Stops the execution of the program. This causes the run function to return early.

## **InstAnalysis**

enum **AnalysisType**

Instruction analysis type

*Values:*

enumerator **QBDI\_ANALYSIS\_INSTRUCTION**

Instruction analysis (address, mnemonic, ...)

enumerator **QBDI\_ANALYSIS\_DISASSEMBLY**

Instruction disassembly

enumerator **QBDI\_ANALYSIS\_OPERANDS**

Instruction operands analysis

enumerator **QBDI\_ANALYSIS\_SYMBOL**

Instruction symbol

struct **InstAnalysis**

Structure containing analysis results of an instruction provided by the VM.

## Public Members

const char \***mnemonic**

LLVM mnemonic (warning: NULL if !ANALYSIS\_INSTRUCTION)

*rword* **address**

Instruction address

uint32\_t **instSize**

Instruction size (in bytes)

CPUMode **cpuMode**

Instruction CPU mode

bool **affectControlFlow**

true if instruction affects control flow

bool **isBranch**

true if instruction acts like a ‘jump’

bool **isCall**

true if instruction acts like a ‘call’

bool **isReturn**

true if instruction acts like a ‘return’

bool **isCompare**

true if instruction is a comparison

bool **isPredicable**

true if instruction contains a predicate (~is conditional)

bool **isMoveImm**

true if this instruction is a move immediate (including conditional moves) instruction.

bool **mayLoad**

true if QBDI detects a load for this instruction

bool **mayStore**

true if QBDI detects a store for this instruction

uint32\_t **loadSize**

size of the expected read access, may be 0 with mayLoad if the size isn’t determined

uint32\_t **storeSize**

size of the expected write access, may be 0 with mayStore if the size isn’t determined

*ConditionType* **condition**

Condition associated with the instruction

char **\*disassembly**

Instruction disassembly (warning: NULL if !ANALYSIS\_DISASSEMBLY)

*RegisterAccessType* **flagsAccess**

Flag access type (noaccess, r, w, rw) (warning: REGISTER\_UNUSED if !ANALYSIS\_OPERANDS)

uint8\_t **numOperands**

Number of operands used by the instruction

*OperandAnalysis* **\*operands**

Structure containing analysis results of an operand provided by the VM. (warning: NULL if !ANALYSIS\_OPERANDS)

const char **\*symbol**

Instruction symbol (warning: NULL if !ANALYSIS\_SYMBOL or not found)

uint32\_t **symbolOffset**

Instruction symbol offset

const char **\*module**

Instruction module name (warning: NULL if !ANALYSIS\_SYMBOL or not found)

uint32\_t **analysisType**

INTERNAL: Instruction analysis type (this should NOT be used)

enum **ConditionType**

Instruction Condition

*Values:*

enumerator **QBDI\_CONDITION\_NONE**

The instruction is unconditionnal

enumerator **QBDI\_CONDITION\_ALWAYS**

The instruction is always true

enumerator **QBDI\_CONDITION\_NEVER**

The instruction is always false

enumerator **QBDI\_CONDITION\_EQUALS**

Equals ('==')

enumerator **QBDI\_CONDITION\_NOT\_EQUALS**

Not Equals ('!=')

enumerator **QBDI\_CONDITION\_ABOVE**

Above ('>' unsigned)

enumerator **QBDI\_CONDITION\_BELOW\_EQUALS**

Below or Equals ('<=' unsigned)

enumerator **QBDI\_CONDITION\_ABOVE\_EQUALS**  
Above or Equals ('>=' unsigned)

enumerator **QBDI\_CONDITION\_BELOW**  
Below ('<' unsigned)

enumerator **QBDI\_CONDITION\_GREAT**  
Great ('>' signed)

enumerator **QBDI\_CONDITION\_LESS\_EQUALS**  
Less or Equals ('<=' signed)

enumerator **QBDI\_CONDITION\_GREAT\_EQUALS**  
Great or Equals ('>=' signed)

enumerator **QBDI\_CONDITION\_LESS**  
Less ('<' signed)

enumerator **QBDI\_CONDITION\_EVEN**  
Even

enumerator **QBDI\_CONDITION\_ODD**  
Odd

enumerator **QBDI\_CONDITION\_OVERFLOW**  
Overflow

enumerator **QBDI\_CONDITION\_NOT\_OVERFLOW**  
Not Overflow

enumerator **QBDI\_CONDITION\_SIGN**  
Sign

enumerator **QBDI\_CONDITION\_NOT\_SIGN**  
Not Sign

struct **OperandAnalysis**  
Structure containing analysis results of an operand provided by the VM.

## Public Members

*OperandType* **type**  
Operand type

*OperandFlag* **flag**  
Operand flag

*rword* **value**  
Operand value (if immediate), or register Id

uint8\_t **size**

Operand size (in bytes)

uint8\_t **regOff**

Sub-register offset in register (in bits)

int16\_t **regCtxIdx**

Register index in VM state (< 0 if not know)

const char \***regName**

Register name

*RegisterAccessType* **regAccess**

Register access type (r, w, rw)

enum **OperandType**

Operand type

*Values:*

enumerator **QBDI\_OPERAND\_INVALID**

Invalid operand

enumerator **QBDI\_OPERAND\_IMM**

Immediate operand

enumerator **QBDI\_OPERAND\_GPR**

Register operand

enumerator **QBDI\_OPERAND\_PRED**

Predicate operand

enumerator **QBDI\_OPERAND\_FPR**

Float register operand

enumerator **QBDI\_OPERAND\_SEG**

Segment or unsupported register operand

enum **OperandFlag**

*Values:*

enumerator **QBDI\_OPERANDFLAG\_NONE**

No flag

enumerator **QBDI\_OPERANDFLAG\_ADDR**

The operand is used to compute an address

enumerator **QBDI\_OPERANDFLAG\_PCREL**

The value of the operand is PC relative



enumerator **QBDI\_OPERANDFLAG\_UNDEFINED\_EFFECT**  
The operand role isn't fully defined

enumerator **QBDI\_OPERANDFLAG\_IMPLICIT**  
The operand is implicit

enum **RegisterAccessType**  
Access type (R/W/RW) of a register operand  
*Values:*

enumerator **QBDI\_REGISTER\_UNUSED**  
Unused register

enumerator **QBDI\_REGISTER\_READ**  
Register read access

enumerator **QBDI\_REGISTER\_WRITE**  
Register write access

enumerator **QBDI\_REGISTER\_READ\_WRITE**  
Register read/write access

## MemoryAccess

struct **MemoryAccess**  
Describe a memory access

### Public Members

*rword* **instAddress**  
Address of instruction making the access

*rword* **accessAddress**  
Address of accessed memory

*rword* **value**  
Value read from / written to memory

**uint16\_t size**  
Size of memory access (in bytes)

*MemoryAccessType* **type**  
Memory access type (READ / WRITE)

*MemoryAccessFlags* **flags**  
Memory access flags

enum **MemoryAccessType**

Memory access type (read / write / ...)

*Values:*

enumerator **QBDI\_MEMORY\_READ**

Memory read access

enumerator **QBDI\_MEMORY\_WRITE**

Memory write access

enumerator **QBDI\_MEMORY\_READ\_WRITE**

Memory read/write access

enum **MemoryAccessFlags**

Memory access flags

*Values:*

enumerator **QBDI\_MEMORY\_NO\_FLAGS**

enumerator **QBDI\_MEMORY\_UNKNOWN\_SIZE**

The size of the access isn't known.

enumerator **QBDI\_MEMORY\_MINIMUM\_SIZE**

The given size is a minimum size.

enumerator **QBDI\_MEMORY\_UNKNOWN\_VALUE**

The value of the access is unknown or hasn't been retrived.

## VMEvent

enum **VMEvent**

*Values:*

enumerator **QBDI\_NO\_EVENT**

enumerator **QBDI\_SEQUENCE\_ENTRY**

Triggered when the execution enters a sequence.

enumerator **QBDI\_SEQUENCE\_EXIT**

Triggered when the execution exits from the current sequence.

enumerator **QBDI\_BASIC\_BLOCK\_ENTRY**

Triggered when the execution enters a basic block.

enumerator **QBDI\_BASIC\_BLOCK\_EXIT**

Triggered when the execution exits from the current basic block.

enumerator **QBDI\_BASIC\_BLOCK\_NEW**

Triggered when the execution enters a new (~unknown) basic block.

enumerator **QBDI\_EXEC\_TRANSFER\_CALL**

Triggered when the ExecBroker executes an execution transfer.

enumerator **QBDI\_EXEC\_TRANSFER\_RETURN**

Triggered when the ExecBroker returns from an execution transfer.

enumerator **QBDI\_SYSCALL\_ENTRY**

Not implemented.

enumerator **QBDI\_SYSCALL\_EXIT**

Not implemented.

enumerator **QBDI\_SIGNAL**

Not implemented.

struct **VMState**

Structure describing the current VM state

## Public Members

*VMEvent* **event**

The event(s) which triggered the callback (must be checked using a mask: `event & BASIC_BLOCK_ENTRY`).

*rword* **basicBlockStart**

The current basic block start address which can also be the execution transfer destination.

*rword* **basicBlockEnd**

The current basic block end address which can also be the execution transfer destination.

*rword* **sequenceStart**

The current sequence start address which can also be the execution transfer destination.

*rword* **sequenceEnd**

The current sequence end address which can also be the execution transfer destination.

*rword* **lastSignal**

Not implemented.

## Memory management

### Allocation

void **qbdi\_alignedAlloc**(size\_t size, size\_t align)

Allocate a block of memory of a specified sized with an aligned base address.

#### Parameters

- **size** – [in] Allocation size in bytes.
- **align** – [in] Base address alignment in bytes.

**Returns** Pointer to the allocated memory or NULL in case an error was encountered.

bool **qbdi\_allocateVirtualStack**(GPRState \*ctx, uint32\_t stackSize, uint8\_t \*\*stack)

Allocate a new stack and setup the GPRState accordingly. The allocated stack needs to be freed with aligned-Free().

#### Parameters

- **ctx** – [in] GPRState which will be setup to use the new stack.
- **stackSize** – [in] Size of the stack to be allocated.
- **stack** – [out] The newly allocated stack pointer will be returned in the variable pointed by stack.

**Returns** True if stack allocation was successfull.

void **qbdi\_alignedFree**(void \*ptr)

Free a block of aligned memory allocated with alignedAlloc.

**Parameters** **ptr** – [in] Pointer to the allocated memory.

void **qbdi\_simulateCall**(GPRState \*ctx, *rword* returnAddress, uint32\_t argNum, ...)

Simulate a call by modifying the stack and registers accordingly.

#### Parameters

- **ctx** – [in] GPRState where the simulated call will be setup. The state needs to point to a valid stack for example setup with allocateVirtualStack().
- **returnAddress** – [in] Return address of the call to simulate.
- **argNum** – [in] The number of arguments in the variadic list.
- **...** – [in] A variadic list of arguments.

void **qbdi\_simulateCallV**(GPRState \*ctx, *rword* returnAddress, uint32\_t argNum, va\_list ap)

Simulate a call by modifying the stack and registers accordingly (stdarg version).

#### Parameters

- **ctx** – [in] GPRState where the simulated call will be setup. The state needs to point to a valid stack for example setup with allocateVirtualStack().
- **returnAddress** – [in] Return address of the call to simulate.
- **argNum** – [in] The number of arguments in the va\_list object.
- **ap** – [in] An stdarg va\_list object.

void **qbdi\_simulateCallA**(GPRState \*ctx, *rword* returnAddress, uint32\_t argNum, const *rword* \*args)

Simulate a call by modifying the stack and registers accordingly (C array version).

**Parameters**

- **ctx** – [in] GPRState where the simulated call will be setup. The state needs to point to a valid stack for example setup with `allocateVirtualStack()`.
- **returnAddress** – [in] Return address of the call to simulate.
- **argNum** – [in] The number of arguments in the array `args`.
- **args** – [in] An array of arguments.

**Exploration**

char \*\***qbdi\_getModuleNames**(size\_t \*size)

Get a list of all the module names loaded in the process memory. If no modules are found, size is set to 0 and this function returns NULL.

**Parameters** **size** – [out] Will be set to the number of strings in the returned array.

**Returns** An array of C strings, each one containing the name of a loaded module. This array needs to be free'd by the caller by repetively calling `free()` on each of its element then finally on the array itself.

*qbdi\_MemoryMap* \***qbdi\_getCurrentProcessMaps**(bool full\_path, size\_t \*size)

Get a list of all the memory maps (regions) of the current process.

**Parameters**

- **full\_path** – [in] Return the full path of the module in name field
- **size** – [out] Will be set to the number of strings in the returned array.

**Returns** An array of MemoryMap object.

*qbdi\_MemoryMap* \***qbdi\_getRemoteProcessMaps**(*rword* pid, bool full\_path, size\_t \*size)

Get a list of all the memory maps (regions) of a process.

**Parameters**

- **pid** – [in] The identifier of the process.
- **full\_path** – [in] Return the full path of the module in name field
- **size** – [out] Will be set to the number of strings in the returned array.

**Returns** An array of MemoryMap object.

void **qbdi\_freeMemoryMapArray**(*qbdi\_MemoryMap* \*arr, size\_t size)

Free an array of memory maps objects.

**Parameters**

- **arr** – [in] An array of MemoryMap object.
- **size** – [in] Number of elements in the array.

struct **qbdi\_MemoryMap**

Map of a memory area (region).

## Public Members

*rword* **start**

Range start value.

*rword* **end**

Range end value (always excluded).

*qbdi\_Permission* **permission**

Region access rights (PF\_READ, PF\_WRITE, PF\_EXEC).

char **\*name**

Region name or path (useful when a region is mapping a module).

enum **qbdi\_Permission**

Memory access rights.

*Values:*

enumerator **QBDI\_PF\_NONE**

No access

enumerator **QBDI\_PF\_READ**

Read access

enumerator **QBDI\_PF\_WRITE**

Write access

enumerator **QBDI\_PF\_EXEC**

Execution access

## Other globals

enum **Options**

*Values:*

enumerator **QBDI\_NO\_OPT**

Default value

enumerator **QBDI\_OPT\_DISABLE\_FPR**

Disable all operation on FPU (SSE, AVX, SIMD). May break the execution if the target use the FPU

enumerator **QBDI\_OPT\_DISABLE\_OPTIONAL\_FPR**

Disable context switch optimisation when the target execblock doesn't used FPR

enumerator **QBDI\_OPT\_ATT\_SYNTAX**

Used the AT&T syntax for instruction disassembly

enumerator **QBDI\_OPT\_ENABLE\_FS\_GS**

Enable Backup/Restore of FS/GS segment. This option uses the instructions (RD|WR)(FS|GS)BASE that must be supported by the operating system

enum **VMError**

QBDI Error values

*Values:*

enumerator **QBDI\_INVALID\_EVENTID**

Mark a returned event id as invalid

## Miscellaneous

### Version

const char \***qbdi\_getVersion**(uint32\_t \*version)

Return QBDI version.

**Parameters** **version** – [out] QBDI version encoded as an unsigned integer (0xMMmmpp).

**Returns** QBDI version as a string (major.minor.patch).

### Log

enum **LogPriority**

Each log has a priority (or level) which can be used to control verbosity. In production builds, only Warning and Error logs are kept.

*Values:*

enumerator **QBDI\_DEBUG**

Debug logs

enumerator **QBDI\_INFO**

Info logs (default)

enumerator **QBDI\_WARNING**

Warning logs

enumerator **QBDI\_ERROR**

Error logs

enumerator **QBDI\_DISABLE**

Disable logs message

void **qbdi\_setLogFile**(const char \*filename, bool truncate)

Redirect logs to a file.

**Parameters**

- **filename** – [in] the path of the file to append the log

- **truncate** – [in] Set to true to clear the file before append the log

void **qbdi\_setLogConsole**()  
Write log to the console (stderr)

void **qbdi\_setLogDefault**()  
Write log to the default location (stderr for linux, android\_logger for android)

void **qbdi\_setLogPriority**(*LogPriority* priority)  
Enable logs matching priority.

**Parameters** **priority** – [in] Filter logs with greater or equal priority.

## 2.5.3 C++ API

### Introduction

The C++ API is the primary API of QBDI. The API is compatible with *QBDIPreload* on Linux and macOS.

### VM class

class QBDI : **VM**

### Public Functions

**VM**(const std::string &cpu = "", const std::vector<std::string> &mattrs = {}, *Options* opts = *Options::NO\_OPT*)  
Construct a new *VM* for a given CPU with specific attributes

#### Parameters

- **cpu** – [in] The name of the CPU
- **mattrs** – [in] A list of additional attributes
- **opts** – [in] The options to enable in the *VM*

**VM**(*VM* &&vm)  
Move constructors. All the cache is keep. All registered callbacks will be called with the new pointer of the *VM*.

**Parameters** **vm** – [in] The *VM* to move

*VM* &**operator=**(*VM* &&vm)  
Move assignment operator All the cache is keep. All registered callbacks will be called with the new pointer of the *VM*. This operator mustn't be called when the target *VM* runs.

**Parameters** **vm** – [in] The *VM* to move

**VM**(const *VM* &vm)  
Copy constructors The state and the configuration is copied. The cache isn't duplicate. The assigned *VM* begin with an empty cache.

**Parameters** **vm** – [in] The *VM* to copy

*VM* &**operator=**(const *VM* &vm)  
Copy assignment operator The state and the configuration is copied. The cache isn't duplicate. The assigned *VM* begin with an empty cache. This operator mustn't be called when the target *VM* runs.



**Parameters** *vm* – [in] The *VM* to copy

## Options

*Options* QBDI::VM::getOptions() const

Get the current Options of the *VM*

void QBDI::VM::setOptions(*Options* options)

Set the Options of the *VM* This method mustn't be called when the *VM* runs.

If the new options is different that the current ones, the cache will be clear.

**Parameters** *options* – [in] the new options of the *VM*

## State management

*GPRState* \*QBDI::VM::getGPRState() const

Obtain the current general purpose register state.

**Returns** A structure containing the GPR state.

*FPRState* \*QBDI::VM::getFPRState() const

Obtain the current floating point register state.

**Returns** A structure containing the FPR state.

void QBDI::VM::setGPRState(const *GPRState* \*gprState)

Set the GPR state

**Parameters** *gprState* – [in] A structure containing the GPR state.

void QBDI::VM::setFPRState(const *FPRState* \*fprState)

Set the FPR state

**Parameters** *fprState* – [in] A structure containing the FPR state.

## Instrumentation range

### Addition

void QBDI::VM::addInstrumentedRange(*rword* start, *rword* end)

Add an address range to the set of instrumented address ranges.

**Parameters**

- **start** – [in] Start address of the range (included).
- **end** – [in] End address of the range (excluded).

bool QBDI::VM::addInstrumentedModule(const std::string &name)

Add the executable address ranges of a module to the set of instrumented address ranges.

**Parameters** *name* – [in] The module's name.

**Returns** True if at least one range was added to the instrumented ranges.

bool QBDI::VM::addInstrumentedModuleFromAddr(*rword* addr)

Add the executable address ranges of a module to the set of instrumented address ranges using an address belonging to the module.

**Parameters** **addr** – [in] An address contained by module's range.

**Returns** True if at least one range was added to the instrumented ranges.

bool QBDI::VM::instrumentAllExecutableMaps()

Adds all the executable memory maps to the instrumented range set.

**Returns** True if at least one range was added to the instrumented ranges.

## Removal

void QBDI::VM::removeInstrumentedRange(*rword* start, *rword* end)

Remove an address range from the set of instrumented address ranges.

**Parameters**

- **start** – [in] Start address of the range (included).
- **end** – [in] End address of the range (excluded).

bool QBDI::VM::removeInstrumentedModule(const std::string &name)

Remove the executable address ranges of a module from the set of instrumented address ranges.

**Parameters** **name** – [in] The module's name.

**Returns** True if at least one range was removed from the instrumented ranges.

bool QBDI::VM::removeInstrumentedModuleFromAddr(*rword* addr)

Remove the executable address ranges of a module from the set of instrumented address ranges using an address belonging to the module.

**Parameters** **addr** – [in] An address contained by module's range.

**Returns** True if at least one range was removed from the instrumented ranges.

void QBDI::VM::removeAllInstrumentedRanges()

Remove all instrumented ranges.

## Callback management

### InstCallback

uint32\_t QBDI::VM::addCodeCB(*InstPosition* pos, *InstCallback* cbk, void \*data, int priority = PRIORITY\_DEFAULT)

Register a callback event for every instruction executed.

**Parameters**

- **pos** – [in] Relative position of the event callback (PREINST / POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or VMErrors::INVALID\_EVENTID in case of failure).

uint32\_t QBDI::VM::addCodeCB(*InstPosition* pos, *InstCbLambda* &&cbk, int priority = PRIORITY\_DEFAULT)

uint32\_t QBDI::VM::addCodeCB(*InstPosition* pos, const *InstCbLambda* &cbk, int priority = PRIORITY\_DEFAULT)

Register a callback event for every instruction executed.

#### Parameters

- **pos** – [in] Relative position of the event callback (PREINST / POSTINST).
- **cbk** – [in] A lambda function to the callback
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or VMError::INVALID\_EVENTID in case of failure).

uint32\_t QBDI::VM::addCodeAddrCB(*rword* address, *InstPosition* pos, *InstCallback* cbk, void \*data, int priority = PRIORITY\_DEFAULT)

Register a callback for when a specific address is executed.

#### Parameters

- **address** – [in] Code address which will trigger the callback.
- **pos** – [in] Relative position of the callback (PREINST / POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or VMError::INVALID\_EVENTID in case of failure).

uint32\_t QBDI::VM::addCodeAddrCB(*rword* address, *InstPosition* pos, *InstCbLambda* &&cbk, int priority = PRIORITY\_DEFAULT)

uint32\_t QBDI::VM::addCodeAddrCB(*rword* address, *InstPosition* pos, const *InstCbLambda* &cbk, int priority = PRIORITY\_DEFAULT)

Register a callback for when a specific address is executed.

#### Parameters

- **address** – [in] Code address which will trigger the callback.
- **pos** – [in] Relative position of the callback (PREINST / POSTINST).
- **cbk** – [in] A lambda function to the callback
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or VMError::INVALID\_EVENTID in case of failure).

uint32\_t QBDI::VM::addCodeRangeCB(*rword* start, *rword* end, *InstPosition* pos, *InstCallback* cbk, void \*data, int priority = PRIORITY\_DEFAULT)

Register a callback for when a specific address range is executed.

#### Parameters

- **start** – [in] Start of the address range which will trigger the callback.
- **end** – [in] End of the address range which will trigger the callback.

- **pos** – [in] Relative position of the callback (PREINST / POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

```
uint32_t QBDI::VM::addCodeRangeCB(rword start, rword end, InstPosition pos, InstCbLambda &&cbk, int  
                                priority = PRIORITY_DEFAULT)
```

```
uint32_t QBDI::VM::addCodeRangeCB(rword start, rword end, InstPosition pos, const InstCbLambda &cbk, int  
                                priority = PRIORITY_DEFAULT)
```

Register a callback for when a specific address range is executed.

#### Parameters

- **start** – [in] Start of the address range which will trigger the callback.
- **end** – [in] End of the address range which will trigger the callback.
- **pos** – [in] Relative position of the callback (PREINST / POSTINST).
- **cbk** – [in] A lambda function to the callback
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

```
uint32_t QBDI::VM::addMnemonicCB(const char *mnemonic, InstPosition pos, InstCallback cbk, void *data, int  
                                priority = PRIORITY_DEFAULT)
```

Register a callback event if the instruction matches the mnemonic.

#### Parameters

- **mnemonic** – [in] Mnemonic to match.
- **pos** – [in] Relative position of the event callback (PREINST / POSTINST).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

```
uint32_t QBDI::VM::addMnemonicCB(const char *mnemonic, InstPosition pos, InstCbLambda &&cbk, int priority  
                                = PRIORITY_DEFAULT)
```

```
uint32_t QBDI::VM::addMnemonicCB(const char *mnemonic, InstPosition pos, const InstCbLambda &cbk, int  
                                priority = PRIORITY_DEFAULT)
```

Register a callback event if the instruction matches the mnemonic.

#### Parameters

- **mnemonic** – [in] Mnemonic to match.
- **pos** – [in] Relative position of the event callback (PREINST / POSTINST).

- **cbk** – [in] A lambda function to the callback
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

## VMEvent

```
uint32_t QBDI::VM::addVMEventCB(VMEvent mask, VMCallback cbk, void *data)
```

Register a callback event for a specific *VM* event.

### Parameters

- **mask** – [in] A mask of *VM* event type which will trigger the callback.
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

```
uint32_t QBDI::VM::addVMEventCB(VMEvent mask, VMCbLambda &&cbk)
```

```
uint32_t QBDI::VM::addVMEventCB(VMEvent mask, const VMCbLambda &cbk)
```

Register a callback event for a specific *VM* event.

### Parameters

- **mask** – [in] A mask of *VM* event type which will trigger the callback.
- **cbk** – [in] A lambda function to the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

## MemoryAccess

```
uint32_t QBDI::VM::addMemAccessCB(MemoryAccessType type, InstCallback cbk, void *data, int priority =
    PRIORITY_DEFAULT)
```

Register a callback event for every memory access matching the type bitfield made by the instructions.

### Parameters

- **type** – [in] A mode bitfield: either `QBDI::MEMORY_READ`, `QBDI::MEMORY_WRITE` or both (`QBDI::MEMORY_READ_WRITE`).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

```
uint32_t QBDI::VM::addMemAccessCB(MemoryAccessType type, InstCbLambda &&cbk, int priority =
    PRIORITY_DEFAULT)
```

```
uint32_t QBDI::VM::addMemAccessCB(MemoryAccessType type, const InstCbLambda &cbk, int priority =  
    PRIORITY_DEFAULT)
```

Register a callback event for every memory access matching the type bitfield made by the instructions.

#### Parameters

- **type** – [in] A mode bitfield: either *QBDI::MEMORY\_READ*, *QBDI::MEMORY\_WRITE* or both (*QBDI::MEMORY\_READ\_WRITE*).
- **cbk** – [in] A lambda function to the callback
- **priority** – [in] The priority of the callback.

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

```
uint32_t QBDI::VM::addMemAddrCB(rword address, MemoryAccessType type, InstCallback cbk, void *data)
```

Add a virtual callback which is triggered for any memory access at a specific address matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost. The callback has the default priority.

#### Parameters

- **address** – [in] Code address which will trigger the callback.
- **type** – [in] A mode bitfield: either *QBDI::MEMORY\_READ*, *QBDI::MEMORY\_WRITE* or both (*QBDI::MEMORY\_READ\_WRITE*).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

```
uint32_t QBDI::VM::addMemAddrCB(rword address, MemoryAccessType type, InstCbLambda &&cbk)
```

```
uint32_t QBDI::VM::addMemAddrCB(rword address, MemoryAccessType type, const InstCbLambda &cbk)
```

Add a virtual callback which is triggered for any memory access at a specific address matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost. The callback has the default priority.

#### Parameters

- **address** – [in] Code address which will trigger the callback.
- **type** – [in] A mode bitfield: either *QBDI::MEMORY\_READ*, *QBDI::MEMORY\_WRITE* or both (*QBDI::MEMORY\_READ\_WRITE*).
- **cbk** – [in] A lambda function to the callback

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

```
uint32_t QBDI::VM::addMemRangeCB(rword start, rword end, MemoryAccessType type, InstCallback cbk, void  
    *data)
```

Add a virtual callback which is triggered for any memory access in a specific address range matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost. The callback has the default priority.

#### Parameters

- **start** – [in] Start of the address range which will trigger the callback.

- **end** – [in] End of the address range which will trigger the callback.
- **type** – [in] A mode bitfield: either *QBDI::MEMORY\_READ*, *QBDI::MEMORY\_WRITE* or both (*QBDI::MEMORY\_READ\_WRITE*).
- **cbk** – [in] A function pointer to the callback.
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

```
uint32_t QBDI::VM::addMemRangeCB(rword start, rword end, MemoryAccessType type, InstCbLambda &&cbk)
```

```
uint32_t QBDI::VM::addMemRangeCB(rword start, rword end, MemoryAccessType type, const InstCbLambda &cbk)
```

Add a virtual callback which is triggered for any memory access in a specific address range matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost. The callback has the default priority.

#### Parameters

- **start** – [in] Start of the address range which will trigger the callback.
- **end** – [in] End of the address range which will trigger the callback.
- **type** – [in] A mode bitfield: either *QBDI::MEMORY\_READ*, *QBDI::MEMORY\_WRITE* or both (*QBDI::MEMORY\_READ\_WRITE*).
- **cbk** – [in] A lambda function to the callback

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

## InstrRuleCallback

```
uint32_t QBDI::VM::addInstrRule(InstrRuleCallback cbk, AnalysisType type, void *data)
```

Add a custom instrumentation rule to the *VM*.

#### Parameters

- **cbk** – [in] A function pointer to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

```
uint32_t QBDI::VM::addInstrRule(InstrRuleCbLambda &&cbk, AnalysisType type)
```

```
uint32_t QBDI::VM::addInstrRule(const InstrRuleCbLambda &cbk, AnalysisType type)
```

Add a custom instrumentation rule to the *VM*.

#### Parameters

- **cbk** – [in] A lambda function to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

`uint32_t QBDI::VM::addInstrRuleRange(rword start, rword end, InstrRuleCallback cbk, AnalysisType type, void *data)`

Add a custom instrumentation rule to the *VM* on a specify range

**Parameters**

- **start** – [in] Begin of the range of address where apply the rule
- **end** – [in] End of the range of address where apply the rule
- **cbk** – [in] A function pointer to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

`uint32_t QBDI::VM::addInstrRuleRange(rword start, rword end, InstrRuleCbLambda &&cbk, AnalysisType type)`

`uint32_t QBDI::VM::addInstrRuleRange(rword start, rword end, const InstrRuleCbLambda &&cbk, AnalysisType type)`

Add a custom instrumentation rule to the *VM* on a specify range

**Parameters**

- **start** – [in] Begin of the range of address where apply the rule
- **end** – [in] End of the range of address where apply the rule
- **cbk** – [in] A lambda function to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

`uint32_t QBDI::VM::addInstrRuleRangeSet(RangeSet<rword> range, InstrRuleCallback cbk, AnalysisType type, void *data)`

Add a custom instrumentation rule to the *VM* on a specify set of range

**Parameters**

- **range** – [in] *Range* of address where apply the rule
- **cbk** – [in] A function pointer to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback
- **data** – [in] User defined data passed to the callback.

**Returns** The id of the registered instrumentation (or `VMError::INVALID_EVENTID` in case of failure).

`uint32_t QBDI::VM::addInstrRuleRangeSet(RangeSet<rword> range, InstrRuleCbLambda &&cbk, AnalysisType type)`



uint32\_t QBDI::VM::addInstrRuleRangeSet(*RangeSet*<*rword*> range, const *InstrRuleCbLambda* &cbk, *AnalysisType* type)

Add a custom instrumentation rule to the *VM* on a specify set of range

#### Parameters

- **range** – [in] *Range* of address where apply the rule
- **cbk** – [in] A lambda function to the callback
- **type** – [in] Analyse type needed for this instruction function pointer to the callback

**Returns** The id of the registered instrumentation (or *VMError::INVALID\_EVENTID* in case of failure).

## Removal

bool QBDI::VM::deleteInstrumentation(uint32\_t id)

Remove an instrumentation.

**Parameters** **id** – [in] The id of the instrumentation to remove.

**Returns** True if instrumentation has been removed.

void QBDI::VM::deleteAllInstrumentations()

Remove all the registered instrumentations.

## Run

bool QBDI::VM::run(*rword* start, *rword* stop)

Start the execution by the DBI. This method mustn't be called if the *VM* already runs.

#### Parameters

- **start** – [in] Address of the first instruction to execute.
- **stop** – [in] Stop the execution when this instruction is reached.

**Returns** True if at least one block has been executed.

bool QBDI::VM::call(*rword* \*retval, *rword* function, const std::vector<*rword*> &args = {})

Call a function using the DBI (and its current state). This method mustn't be called if the *VM* already runs.

Example:

```
// perform (with QBDI) a call similar to (*funcPtr)(42);
uint8_t *fakestack = nullptr;
QBDI::VM *vm = new QBDI::VM();
QBDI::GPRState *state = vm->getGPRState();
QBDI::allocateVirtualStack(state, 0x1000000, &fakestack);
vm->addInstrumentedModuleFromAddr(funcPtr);
rword retVal;
vm->call(&retVal, funcPtr, {42});
```

#### Parameters

- **[retval]** – [in] Pointer to the returned value (optional).

- **function** – [in] Address of the function start instruction.
- **args** – [in] A list of arguments.

**Returns** True if at least one block has been executed.

bool QBDI::VM::callA(*rword* \*retval, *rword* function, uint32\_t argNum, const *rword* \*args)

Call a function using the DBI (and its current state). This method mustn't be called if the *VM* already runs.

**Parameters**

- **[retval]** – [in] Pointer to the returned value (optional).
- **function** – [in] Address of the function start instruction.
- **argNum** – [in] The number of arguments in the array of arguments.
- **args** – [in] An array of arguments.

**Returns** True if at least one block has been executed.

bool QBDI::VM::callV(*rword* \*retval, *rword* function, uint32\_t argNum, va\_list ap)

Call a function using the DBI (and its current state). This method mustn't be called if the *VM* already runs.

**Parameters**

- **[retval]** – [in] Pointer to the returned value (optional).
- **function** – [in] Address of the function start instruction.
- **argNum** – [in] The number of arguments in the variadic list.
- **ap** – [in] An stdarg va\_list object.

**Returns** True if at least one block has been executed.

## InstAnalysis

const *InstAnalysis* \*QBDI::VM::getInstAnalysis(*AnalysisType* type = ANALYSIS\_INSTRUCTION | ANALYSIS\_DISASSEMBLY) const

Obtain the analysis of the current instruction. Analysis results are cached in the *VM*. The validity of the returned pointer is only guaranteed until the end of the callback, else a deepcopy of the structure is required. This method must only be used in an InstCallback.

**Parameters** **[type]** – [in] Properties to retrieve during analysis. This argument is optional, defaulting to *QBDI::ANALYSIS\_INSTRUCTION* | *QBDI::ANALYSIS\_DISASSEMBLY*.

**Returns** A *InstAnalysis* structure containing the analysis result.

const *InstAnalysis* \*QBDI::VM::getCachedInstAnalysis(*rword* address, *AnalysisType* type = ANALYSIS\_INSTRUCTION | ANALYSIS\_DISASSEMBLY) const

Obtain the analysis of a cached instruction. Analysis results are cached in the *VM*. The validity of the returned pointer is only guaranteed until the end of the callback or a call to a noconst method of the *VM* object.

**Parameters**

- **address** – [in] The address of the instruction to analyse.
- **[type]** – [in] Properties to retrieve during analysis. This argument is optional, defaulting to *QBDI::ANALYSIS\_INSTRUCTION* | *QBDI::ANALYSIS\_DISASSEMBLY*

**Returns** A *InstAnalysis* structure containing the analysis result. null if the instruction isn't in the cache.

## MemoryAccess

std::vector<MemoryAccess> QBDI::VM::getInstMemoryAccess() const

Obtain the memory accesses made by the last executed instruction. The method should be called in an InstCall-back.

**Returns** List of memory access made by the instruction.

std::vector<MemoryAccess> QBDI::VM::getBBMemoryAccess() const

Obtain the memory accesses made by the last executed basic block. The method should be called in a VMCall-back with VMEvent::SEQUENCE\_EXIT.

**Returns** List of memory access made by the instruction.

bool QBDI::VM::recordMemoryAccess(MemoryAccessType type)

Add instrumentation rules to log memory access using inline instrumentation and instruction shadows.

**Parameters** **type** – [in] Memory mode bitfield to activate the logging for: either QBDI::MEMORY\_READ, QBDI::MEMORY\_WRITE or both (QBDI::MEMORY\_READ\_WRITE).

**Returns** True if inline memory logging is supported, False if not or in case of error.

## Cache management

bool QBDI::VM::precacheBasicBlock(rword pc)

Pre-cache a known basic block This method mustn't be called if the VM already runs.

**Parameters** **pc** – [in] Start address of a basic block

**Returns** True if basic block has been inserted in cache.

void QBDI::VM::clearCache(rword start, rword end)

Clear a specific address range from the translation cache.

**Parameters**

- **start** – [in] Start of the address range to clear from the cache.
- **end** – [in] End of the address range to clear from the cache.

void QBDI::VM::clearAllCache()

Clear the entire translation cache.

## Register state

type QBDI::rword

An integer of the size of a register

- uint32\_t for X86
- uint64\_t for X86\_64

struct QBDI::GPRState

General Purpose Register context.

For X86 architecture:

```
typedef struct QBDI_ALIGNED(4) {  
    rword eax;  
    rword ebx;  
    rword ecx;  
    rword edx;  
    rword esi;  
    rword edi;  
    rword ebp;  
    rword esp;  
    rword eip;  
    rword eflags;  
} GPRState;
```

For X86\_64 architecture:

```
typedef struct QBDI_ALIGNED(8) {  
    rword rax;  
    rword rbx;  
    rword rcx;  
    rword rdx;  
    rword rsi;  
    rword rdi;  
    rword r8;  
    rword r9;  
    rword r10;  
    rword r11;  
    rword r12;  
    rword r13;  
    rword r14;  
    rword r15;  
    rword rbp;  
    rword rsp;  
    rword rip;  
    rword eflags;  
    // Only backup and restore with OPT_ENABLE_FS_GS  
    rword fs;  
    rword gs;  
} GPRState;
```

struct QBDI::FPRState

Floating Point Register context.

For X86 architecture:

```
typedef struct QBDI_ALIGNED(16) {  
    union {  
        FPControl fcw; /* x87 FPU control word */  
        uint16_t rfcw;  
    };  
    union {  
        FPStatus fsw; /* x87 FPU status word */  
        uint16_t rfsf;  
    };  
    uint8_t ftw; /* x87 FPU tag word */
```

(continues on next page)

(continued from previous page)

```

uint8_t rsrv1;      /* reserved */
uint16_t fop;       /* x87 FPU Opcode */
uint32_t ip;        /* x87 FPU Instruction Pointer offset */
uint16_t cs;        /* x87 FPU Instruction Pointer Selector */
uint16_t rsrv2;     /* reserved */
uint32_t dp;        /* x87 FPU Instruction Operand(Data) Pointer offset */
uint16_t ds;        /* x87 FPU Instruction Operand(Data) Pointer Selector */
uint16_t rsrv3;     /* reserved */
uint32_t mxcsr;     /* MXCSR Register state */
uint32_t mxcsrmask; /* MXCSR mask */
MMSTReg stmm0;     /* ST0/MM0 */
MMSTReg stmm1;     /* ST1/MM1 */
MMSTReg stmm2;     /* ST2/MM2 */
MMSTReg stmm3;     /* ST3/MM3 */
MMSTReg stmm4;     /* ST4/MM4 */
MMSTReg stmm5;     /* ST5/MM5 */
MMSTReg stmm6;     /* ST6/MM6 */
MMSTReg stmm7;     /* ST7/MM7 */
char xmm0[16];     /* XMM 0 */
char xmm1[16];     /* XMM 1 */
char xmm2[16];     /* XMM 2 */
char xmm3[16];     /* XMM 3 */
char xmm4[16];     /* XMM 4 */
char xmm5[16];     /* XMM 5 */
char xmm6[16];     /* XMM 6 */
char xmm7[16];     /* XMM 7 */
char reserved[14 * 16];
char ymm0[16];     /* YMM0[255:128] */
char ymm1[16];     /* YMM1[255:128] */
char ymm2[16];     /* YMM2[255:128] */
char ymm3[16];     /* YMM3[255:128] */
char ymm4[16];     /* YMM4[255:128] */
char ymm5[16];     /* YMM5[255:128] */
char ymm6[16];     /* YMM6[255:128] */
char ymm7[16];     /* YMM7[255:128] */
} FPRState;

```

For X86\_64 architecture:

```

typedef struct QBDI_ALIGNED(16) {
    union {
        FPControl fcw; /* x87 FPU control word */
        uint16_t rfcw;
    };
    union {
        FPStatus fsw; /* x87 FPU status word */
        uint16_t rfsw;
    };
    uint8_t ftw;      /* x87 FPU tag word */
    uint8_t rsrv1;    /* reserved */
    uint16_t fop;     /* x87 FPU Opcode */
    uint32_t ip;      /* x87 FPU Instruction Pointer offset */

```

(continues on next page)

(continued from previous page)

```

uint16_t cs;          /* x87 FPU Instruction Pointer Selector */
uint16_t rsrv2;       /* reserved */
uint32_t dp;          /* x87 FPU Instruction Operand(Data) Pointer offset */
uint16_t ds;          /* x87 FPU Instruction Operand(Data) Pointer Selector */
uint16_t rsrv3;       /* reserved */
uint32_t mxcsr;        /* MXCSR Register state */
uint32_t mxcsrmask;    /* MXCSR mask */
MMSTReg stmm0;        /* ST0/MM0 */
MMSTReg stmm1;        /* ST1/MM1 */
MMSTReg stmm2;        /* ST2/MM2 */
MMSTReg stmm3;        /* ST3/MM3 */
MMSTReg stmm4;        /* ST4/MM4 */
MMSTReg stmm5;        /* ST5/MM5 */
MMSTReg stmm6;        /* ST6/MM6 */
MMSTReg stmm7;        /* ST7/MM7 */
char xmm0[16];        /* XMM 0 */
char xmm1[16];        /* XMM 1 */
char xmm2[16];        /* XMM 2 */
char xmm3[16];        /* XMM 3 */
char xmm4[16];        /* XMM 4 */
char xmm5[16];        /* XMM 5 */
char xmm6[16];        /* XMM 6 */
char xmm7[16];        /* XMM 7 */
char xmm8[16];        /* XMM 8 */
char xmm9[16];        /* XMM 9 */
char xmm10[16];       /* XMM 10 */
char xmm11[16];       /* XMM 11 */
char xmm12[16];       /* XMM 12 */
char xmm13[16];       /* XMM 13 */
char xmm14[16];       /* XMM 14 */
char xmm15[16];       /* XMM 15 */
char reserved[6 * 16];
char ymm0[16];        /* YMM0[255:128] */
char ymm1[16];        /* YMM1[255:128] */
char ymm2[16];        /* YMM2[255:128] */
char ymm3[16];        /* YMM3[255:128] */
char ymm4[16];        /* YMM4[255:128] */
char ymm5[16];        /* YMM5[255:128] */
char ymm6[16];        /* YMM6[255:128] */
char ymm7[16];        /* YMM7[255:128] */
char ymm8[16];        /* YMM8[255:128] */
char ymm9[16];        /* YMM9[255:128] */
char ymm10[16];       /* YMM10[255:128] */
char ymm11[16];       /* YMM11[255:128] */
char ymm12[16];       /* YMM12[255:128] */
char ymm13[16];       /* YMM13[255:128] */
char ymm14[16];       /* YMM14[255:128] */
char ymm15[16];       /* YMM15[255:128] */
} FPRState;

```

struct QBDI::MMSTReg

### Public Members

char **reg**[10]

char **rsrv**[6]

struct QBDI::FPControl

### Public Members

uint16\_t **invalid**

uint16\_t **denorm**

uint16\_t **zdiv**

uint16\_t **ovrfl**

uint16\_t **undfl**

uint16\_t **precis**

uint16\_t **\_\_pad0\_\_**

uint16\_t **pc**

uint16\_t **rc**

uint16\_t **\_\_pad1\_\_**

uint16\_t **\_\_pad2\_\_**

struct QBDI::FPStatus

## Public Members

uint16\_t **invalid**

uint16\_t **denorm**

uint16\_t **zdiv**

uint16\_t **ovrfl**

uint16\_t **undfl**

uint16\_t **precis**

uint16\_t **stkflt**

uint16\_t **errsummm**

uint16\_t **c0**

uint16\_t **c1**

uint16\_t **c2**

uint16\_t **tos**

uint16\_t **c3**

uint16\_t **busy**

QBDI::REG\_RETURN

QBDI::REG\_BP

QBDI::REG\_SP

QBDI::REG\_PC

QBDI::NUM\_GPR



## Callback

using QBDI : **VMInstanceRef** = *VM*\*

```
typedef VMAction (*QBDI : InstCallback)(VMInstanceRef vm, GPRState *gprState, FPRState *fprState, void *data)
```

Instruction callback function type.

**Param vm [in]** *VM* instance of the callback.

**Param gprState [in]** A structure containing the state of the General Purpose Registers. Modifying it affects the *VM* execution accordingly.

**Param fprState [in]** A structure containing the state of the Floating Point Registers. Modifying it affects the *VM* execution accordingly.

**Param data [in]** User defined data which can be defined when registering the callback.

**Return** The callback result used to signal subsequent actions the *VM* needs to take.

```
typedef std::function<VMAction(VMInstanceRef vm, GPRState *gprState, FPRState *fprState)>  
QBDI : InstCbLambda
```

Instruction callback lambda type.

**Param vm [in]** *VM* instance of the callback.

**Param gprState [in]** A structure containing the state of the General Purpose Registers. Modifying it affects the *VM* execution accordingly.

**Param fprState [in]** A structure containing the state of the Floating Point Registers. Modifying it affects the *VM* execution accordingly.

**Return** The callback result used to signal subsequent actions the *VM* needs to take.

```
typedef VMAction (*QBDI : VMCallback)(VMInstanceRef vm, const VMState *vmState, GPRState *gprState, FPRState *fprState, void *data)
```

*VM* callback function type.

**Param vm [in]** *VM* instance of the callback.

**Param vmState [in]** A structure containing the current state of the *VM*.

**Param gprState [in]** A structure containing the state of the General Purpose Registers. Modifying it affects the *VM* execution accordingly.

**Param fprState [in]** A structure containing the state of the Floating Point Registers. Modifying it affects the *VM* execution accordingly.

**Param data [in]** User defined data which can be defined when registering the callback.

**Return** The callback result used to signal subsequent actions the *VM* needs to take.

```
typedef std::function<VMAction(VMInstanceRef vm, const VMState *vmState, GPRState *gprState, FPRState *fprState)> QBDI : VMCbLambda
```

*VM* callback lambda type.

**Param vm [in]** *VM* instance of the callback.

**Param vmState [in]** A structure containing the current state of the *VM*.

**Param gprState [in]** A structure containing the state of the General Purpose Registers. Modifying it affects the *VM* execution accordingly.

**Param fprState [in]** A structure containing the state of the Floating Point Registers. Modifying it affects the *VM* execution accordingly.

**Return** The callback result used to signal subsequent actions the *VM* needs to take.

```
typedef std::vector<InstrRuleDataCBK> (*QBDI::InstrRuleCallback)(VMInstanceRef vm, const InstAnalysis *inst, void *data)
```

Instrumentation rule callback function type.

**Param vm [in]** *VM* instance of the callback.

**Param inst [in]** AnalysisType of the current instrumented Instruction.

**Param data [in]** User defined data which can be defined when registering the callback.

**Return** Return cbk to call when this instruction is run.

```
typedef std::function<std::vector<InstrRuleDataCBK>(VMInstanceRef vm, const InstAnalysis *inst)> QBDI::InstrRuleCbLambda
```

Instrumentation rule callback lambda type.

**Param vm [in]** *VM* instance of the callback.

**Param inst [in]** AnalysisType of the current instrumented Instruction.

**Return** Return cbk to call when this instruction is run.

```
struct QBDI::InstrRuleDataCBK
```

## Public Members

*InstPosition* **position**

Relative position of the event callback (PREINST / POSTINST).

*InstCallback* **cbk**

Address of the function to call when the instruction is executed.

void **\*data**

User defined data which will be forward to cbk

*InstCbLambda* **lambdaCbK**

Lambda callback. Replace cbk and data if not nullptr

int **priority**

Priority of the callback

enum QBDI::InstPosition

Position relative to an instruction.

*Values:*

enumerator **PREINST**  
Positioned before the instruction.

enumerator **POSTINST**  
Positioned after the instruction.

enum **QBDI::CallbackPriority**

Priority of callback

A callback with an higher priority will be call before a callback with a lower priority.

ie:

- a. CBpre(p = 10)
- b. CBpre(p = 0)
- c. CBpre(p = -10)
- d. instrumented instruction
- e. CBpost(p = 10)
- f. CBpost(p = 0)
- g. CBpost(p = -10)

When the [MemoryAccess](#) API is used in a callback, the priority of the callback must not be greater than **PRIORITY\_MEMACCESS\_LIMIT**

*Values:*

enumerator **PRIORITY\_DEFAULT**  
Default priority for callback

enumerator **PRIORITY\_MEMACCESS\_LIMIT**  
Maximum priority if `getInstMemoryAccess` is used in the callback

enum **QBDI::VMAAction**  
The callback results.

*Values:*

enumerator **CONTINUE**  
The execution of the basic block continues.

enumerator **SKIP\_INST**  
Available only with **PREINST** `InstCallback`. The instruction and the remained **PREINST** callbacks are skip. The execution continue with the **POSTINST** instruction.

We recommand to used this result with a low priority **PREINST** callback in order to emulate the instruction without skipping the **POSTINST** callback.

enumerator **SKIP\_PATCH**  
Available only with `InstCallback`. The current instruction and the reminding callback (**PRE** and **POST**) are skip. The execution continues to the next instruction.

For instruction that change the instruction pointer (jump/call/ret), `BREAK_TO_VM` must be used instead of `SKIP`.

`SKIP` can break the record of *MemoryAccess* for the current instruction.

enumerator **BREAK\_TO\_VM**

The execution breaks and returns to the *VM* causing a complete reevaluation of the execution state. A `BREAK_TO_VM` is needed to ensure that modifications of the Program Counter or the program code are taken into account.

enumerator **STOP**

Stops the execution of the program. This causes the run function to return early.

## InstAnalysis

enum QBDI::**AnalysisType**

Instruction analysis type

*Values:*

enumerator **ANALYSIS\_INSTRUCTION**

Instruction analysis (address, mnemonic, ...)

enumerator **ANALYSIS\_DISASSEMBLY**

Instruction disassembly

enumerator **ANALYSIS\_OPERANDS**

Instruction operands analysis

enumerator **ANALYSIS\_SYMBOL**

Instruction symbol

struct QBDI::**InstAnalysis**

Structure containing analysis results of an instruction provided by the *VM*.

## Public Members

const char \***mnemonic**

LLVM mnemonic (warning: NULL if !`ANALYSIS_INSTRUCTION`)

*rword* **address**

Instruction address

uint32\_t **instSize**

Instruction size (in bytes)

CPUMode **cpuMode**

Instruction CPU mode

bool **affectControlFlow**  
true if instruction affects control flow

bool **isBranch**  
true if instruction acts like a ‘jump’

bool **isCall**  
true if instruction acts like a ‘call’

bool **isReturn**  
true if instruction acts like a ‘return’

bool **isCompare**  
true if instruction is a comparison

bool **isPredicable**  
true if instruction contains a predicate (~is conditional)

bool **isMoveImm**  
true if this instruction is a move immediate (including conditional moves) instruction.

bool **mayLoad**  
true if QBDI detects a load for this instruction

bool **mayStore**  
true if QBDI detects a store for this instruction

uint32\_t **loadSize**  
size of the expected read access, may be 0 with mayLoad if the size isn’t determined

uint32\_t **storeSize**  
size of the expected write access, may be 0 with mayStore if the size isn’t determined

*ConditionType* **condition**  
Condition associated with the instruction

char \***disassembly**  
Instruction disassembly (warning: NULL if !ANALYSIS\_DISASSEMBLY)

*RegisterAccessType* **flagsAccess**  
Flag access type (noaccess, r, w, rw) (warning: REGISTER\_UNUSED if !ANALYSIS\_OPERANDS)

uint8\_t **numOperands**  
Number of operands used by the instruction

*OperandAnalysis* \***operands**  
Structure containing analysis results of an operand provided by the *VM*. (warning: NULL if !ANALYSIS\_OPERANDS)

const char \***symbol**

Instruction symbol (warning: NULL if !ANALYSIS\_SYMBOL or not found)

uint32\_t **symbolOffset**

Instruction symbol offset

const char \***module**

Instruction module name (warning: NULL if !ANALYSIS\_SYMBOL or not found)

uint32\_t **analysisType**

INTERNAL: Instruction analysis type (this should NOT be used)

enum QBDI:: **ConditionType**

Instruction Condition

*Values:*

enumerator **CONDITION\_NONE**

The instruction is unconditionnal

enumerator **CONDITION\_ALWAYS**

The instruction is always true

enumerator **CONDITION\_NEVER**

The instruction is always false

enumerator **CONDITION\_EQUALS**

Equals ('==')

enumerator **CONDITION\_NOT\_EQUALS**

Not Equals ('!=')

enumerator **CONDITION\_ABOVE**

Above ('>' unsigned)

enumerator **CONDITION\_BELOW\_EQUALS**

Below or Equals ('<=' unsigned)

enumerator **CONDITION\_ABOVE\_EQUALS**

Above or Equals ('>=' unsigned)

enumerator **CONDITION\_BELOW**

Below ('<' unsigned)

enumerator **CONDITION\_GREAT**

Great ('>' signed)

enumerator **CONDITION\_LESS\_EQUALS**

Less or Equals ('<=' signed)

enumerator **CONDITION\_GREAT\_EQUALS**  
Great or Equals ('>=' signed)

enumerator **CONDITION\_LESS**  
Less ('<' signed)

enumerator **CONDITION\_EVEN**  
Even

enumerator **CONDITION\_ODD**  
Odd

enumerator **CONDITION\_OVERFLOW**  
Overflow

enumerator **CONDITION\_NOT\_OVERFLOW**  
Not Overflow

enumerator **CONDITION\_SIGN**  
Sign

enumerator **CONDITION\_NOT\_SIGN**  
Not Sign

struct **QBDI::OperandAnalysis**  
Structure containing analysis results of an operand provided by the *VM*.

### Public Members

*OperandType* **type**  
*Operand* type

*OperandFlag* **flag**  
*Operand* flag

*rword* **value**  
*Operand* value (if immediate), or register Id

uint8\_t **size**  
*Operand* size (in bytes)

uint8\_t **regOff**  
Sub-register offset in register (in bits)

int16\_t **regCtxIdx**  
Register index in *VM* state (< 0 if not know)

const char \***regName**  
Register name

*RegisterAccessType* **regAccess**

Register access type (r, w, rw)

enum QBDI::OperandType

*Operand* type

*Values:*

enumerator **OPERAND\_INVALID**

Invalid operand

enumerator **OPERAND\_IMM**

Immediate operand

enumerator **OPERAND\_GPR**

Register operand

enumerator **OPERAND\_PRED**

Predicate operand

enumerator **OPERAND\_FPR**

Float register operand

enumerator **OPERAND\_SEG**

Segment or unsupported register operand

enum QBDI::OperandFlag

*Values:*

enumerator **OPERANDFLAG\_NONE**

No flag

enumerator **OPERANDFLAG\_ADDR**

The operand is used to compute an address

enumerator **OPERANDFLAG\_PCREL**

The value of the operand is PC relative

enumerator **OPERANDFLAG\_UNDEFINED\_EFFECT**

The operand role isn't fully defined

enumerator **OPERANDFLAG\_IMPLICIT**

The operand is implicit

enum QBDI::RegisterAccessType

Access type (R/W/RW) of a register operand

*Values:*

enumerator **REGISTER\_UNUSED**

Unused register



enumerator **REGISTER\_READ**  
Register read access

enumerator **REGISTER\_WRITE**  
Register write access

enumerator **REGISTER\_READ\_WRITE**  
Register read/write access

## MemoryAccess

struct QBDI::MemoryAccess  
Describe a memory access

### Public Members

*rword* **instAddress**  
Address of instruction making the access

*rword* **accessAddress**  
Address of accessed memory

*rword* **value**  
Value read from / written to memory

**uint16\_t size**  
Size of memory access (in bytes)

*MemoryAccessType* **type**  
Memory access type (READ / WRITE)

*MemoryAccessFlags* **flags**  
Memory access flags

enum QBDI::MemoryAccessType  
Memory access type (read / write / ...)

*Values:*

enumerator **MEMORY\_READ**  
Memory read access

enumerator **MEMORY\_WRITE**  
Memory write access

enumerator **MEMORY\_READ\_WRITE**  
Memory read/write access

enum QBDI::MemoryAccessFlags

Memory access flags

*Values:*

enumerator MEMORY\_NO\_FLAGS

enumerator MEMORY\_UNKNOWN\_SIZE

The size of the access isn't known.

enumerator MEMORY\_MINIMUM\_SIZE

The given size is a minimum size.

enumerator MEMORY\_UNKNOWN\_VALUE

The value of the access is unknown or hasn't been retrived.

## VMEvent

enum QBDI::VMEvent

*Values:*

enumerator NO\_EVENT

enumerator SEQUENCE\_ENTRY

Triggered when the execution enters a sequence.

enumerator SEQUENCE\_EXIT

Triggered when the execution exits from the current sequence.

enumerator BASIC\_BLOCK\_ENTRY

Triggered when the execution enters a basic block.

enumerator BASIC\_BLOCK\_EXIT

Triggered when the execution exits from the current basic block.

enumerator BASIC\_BLOCK\_NEW

Triggered when the execution enters a new (~unknown) basic block.

enumerator EXEC\_TRANSFER\_CALL

Triggered when the ExecBroker executes an execution transfer.

enumerator EXEC\_TRANSFER\_RETURN

Triggered when the ExecBroker returns from an execution transfer.

enumerator SYSCALL\_ENTRY

Not implemented.

enumerator **SYSCALL\_EXIT**  
Not implemented.

enumerator **SIGNAL**  
Not implemented.

struct **QBDI::VMState**  
Structure describing the current *VM* state

## Public Members

*VMEvent* **event**  
The event(s) which triggered the callback (must be checked using a mask: `event & BASIC_BLOCK_ENTRY`).

*rword* **basicBlockStart**  
The current basic block start address which can also be the execution transfer destination.

*rword* **basicBlockEnd**  
The current basic block end address which can also be the execution transfer destination.

*rword* **sequenceStart**  
The current sequence start address which can also be the execution transfer destination.

*rword* **sequenceEnd**  
The current sequence end address which can also be the execution transfer destination.

*rword* **lastSignal**  
Not implemented.

## Memory management

### Allocation

void **\*QBDI::alignedAlloc**(size\_t size, size\_t align)  
Allocate a block of memory of a specified sized with an aligned base address.

#### Parameters

- **size** – [in] Allocation size in bytes.
- **align** – [in] Base address alignment in bytes.

**Returns** Pointer to the allocated memory or NULL in case an error was encountered.

bool **QBDI::allocateVirtualStack**(*GPRState* \*ctx, uint32\_t stackSize, uint8\_t \*\*stack)  
Allocate a new stack and setup the *GPRState* accordingly. The allocated stack needs to be freed with *alignedFree*().

#### Parameters

- **ctx** – [in] *GPRState* which will be setup to use the new stack.

- **stackSize** – [in] Size of the stack to be allocated.
- **stack** – [out] The newly allocated stack pointer will be returned in the variable pointed by stack.

**Returns** True if stack allocation was successful.

void QBDI::alignedFree(void \*ptr)

Free a block of aligned memory allocated with alignedAlloc.

**Parameters** **ptr** – [in] Pointer to the allocated memory.

void QBDI::simulateCall(*GPRState* \*ctx, *rword* returnAddress, const std::vector<*rword*> &args = {})

Simulate a call by modifying the stack and registers accordingly (std::vector version).

**Parameters**

- **ctx** – [in] GPRState where the simulated call will be setup. The state needs to point to a valid stack for example setup with *allocateVirtualStack()*.
- **returnAddress** – [in] Return address of the call to simulate.
- **args** – [in] A list of arguments.

void QBDI::simulateCallV(*GPRState* \*ctx, *rword* returnAddress, uint32\_t argNum, va\_list ap)

Simulate a call by modifying the stack and registers accordingly (stdarg version).

**Parameters**

- **ctx** – [in] GPRState where the simulated call will be setup. The state needs to point to a valid stack for example setup with *allocateVirtualStack()*.
- **returnAddress** – [in] Return address of the call to simulate.
- **argNum** – [in] The number of arguments in the va\_list object.
- **ap** – [in] An stdarg va\_list object.

void QBDI::simulateCallA(*GPRState* \*ctx, *rword* returnAddress, uint32\_t argNum, const *rword* \*args)

Simulate a call by modifying the stack and registers accordingly (C array version).

**Parameters**

- **ctx** – [in] GPRState where the simulated call will be setup. The state needs to point to a valid stack for example setup with *allocateVirtualStack()*.
- **returnAddress** – [in] Return address of the call to simulate.
- **argNum** – [in] The number of arguments in the array args.
- **args** – [in] An array of arguments.

## Exploration

std::vector<std::string> QBDI::getModuleNames()

Get a list of all the module names loaded in the process memory.

**Returns** A vector of string of module names.

std::vector<*MemoryMap*> QBDI::getCurrentProcessMaps(bool full\_path = false)

Get a list of all the memory maps (regions) of the current process.

**Parameters** **full\_path** – [in] Return the full path of the module in name field

**Returns** A vector of *MemoryMap* object.

`std::vector<MemoryMap> QBDI::getRemoteProcessMaps(QBDI::rword pid, bool full_path = false)`

Get a list of all the memory maps (regions) of a process.

#### Parameters

- **pid** – [in] The identifier of the process.
- **full\_path** – [in] Return the full path of the module in name field

**Returns** A vector of *MemoryMap* object.

`struct QBDI::MemoryMap`

Map of a memory area (region).

#### Public Members

*Range*<*rword*> **range**

A range of memory (region), delimited between a start and an (excluded) end address.

*Permission* **permission**

Region access rights (PF\_READ, PF\_WRITE, PF\_EXEC).

`std::string` **name**

Region name or path (useful when a region is mapping a module).

`enum QBDI::Permission`

Memory access rights.

*Values:*

enumerator **PF\_NONE**

No access

enumerator **PF\_READ**

Read access

enumerator **PF\_WRITE**

Write access

enumerator **PF\_EXEC**

Execution access

#### Other globals

`enum QBDI::Options`

*Values:*

enumerator **NO\_OPT**

Default value

enumerator **OPT\_DISABLE\_FPU**

Disable all operation on FPU (SSE, AVX, SIMD). May break the execution if the target use the FPU

enumerator **OPT\_DISABLE\_OPTIONAL\_FPR**

Disable context switch optimisation when the target execblock doesn't used FPR

enumerator **OPT\_ATT\_SYNTAX**

Used the AT&T syntax for instruction disassembly

enumerator **OPT\_ENABLE\_FS\_GS**

Enable Backup/Restore of FS/GS segment. This option uses the instructions (RD|WR)(FS|GS)BASE that must be supported by the operating system

enum QBDI::**VMError**

QBDI Error values

*Values:*

enumerator **INVALID\_EVENTID**

Mark a returned event id as invalid

## Miscellaneous

### Version

inline const char \*QBDI::**getVersion**(uint32\_t \*version)

Return QBDI version.

**Parameters** **version** – [out] QBDI version encoded as an unsigned integer (0xMMmmpp).

**Returns** QBDI version as a string (major.minor.patch).

## Log

enum QBDI::**LogPriority**

Each log has a priority (or level) which can be used to control verbosity. In production builds, only Warning and Error logs are kept.

*Values:*

enumerator **DEBUG**

Debug logs

enumerator **INFO**

Info logs (default)

enumerator **WARNING**

Warning logs

enumerator **ERROR**

Error logs

enumerator **DISABLE**

Disable logs message

```
void QBDI::setLogFile(const std::string &filename, bool truncate = false)
    Redirect logs to a file.
```

#### Parameters

- **filename** – [in] the path of the file to append the log
- **truncate** – [in] Set to true to clear the file before append the log

```
inline void QBDI::setLogPriority(LogPriority priority = LogPriority::INFO)
    Enable logs matching priority.
```

**Parameters** **priority** – [in] Filter logs with greater or equal priority.

```
inline void QBDI::setLogConsole()
    Write log to the console (stderr)
```

```
inline void QBDI::setLogDefault()
    Write log to the default location (stderr for linux, android_logger for android)
```

## Range

```
template<typename T>
```

```
class QBDI::Range
```

### Public Functions

```
inline T start() const
```

```
inline T end() const
```

```
inline void setStart(const T start)
```

```
inline void setEnd(const T end)
```

```
inline Range(const T start, const T end)
    Construct a new range.
```

#### Parameters

- **start** – [in] *Range* start value.
- **end** – [in] *Range* end value (excluded).

```
inline T size() const
    Return the total length of a range.
```

```
inline bool operator==(const Range &r) const
    Return True if two ranges are equal (same boundaries).
```

**Parameters** **r** – [in] *Range* to check.

**Returns** True if equal.

```
inline bool contains(const T t) const
    Return True if an value is inside current range boundaries.
```

**Parameters** **t** – [in] Value to check.

**Returns** True if contained.

inline bool **contains**(const *Range*<*T*> &r) const  
Return True if a range is inside current range boundaries.

**Parameters** **r** – [in] *Range* to check.

**Returns** True if contained.

inline bool **overlaps**(const *Range*<*T*> &r) const  
Return True if a range is overlapping current range lower or/and upper boundary.

**Parameters** **r** – [in] *Range* to check.

**Returns** True if overlapping.

inline void **display**(std::ostream &os) const  
Pretty print a range

**Parameters** **os** – [in] An output stream.

inline *Range*<*T*> **intersect**(const *Range*<*T*> &r) const  
Return the intersection of two ranges.

**Parameters** **r** – [in] *Range* to intersect with current range.

**Returns** A new range.

template<typename T>

class QBDI::RangeSet

## Public Functions

inline RangeSet()

inline const std::vector<*Range*<*T*>> &getRanges() const

inline *T* size() const

inline bool contains(const *T* t) const

inline bool contains(const *Range*<*T*> &t) const

inline bool overlaps(const *Range*<*T*> &t) const

inline void add(const *Range*<*T*> &t)

inline void add(const *RangeSet*<*T*> &t)

inline void remove(const *Range*<*T*> &t)



```

inline void remove(const RangeSet<T> &t)

inline void intersect(const RangeSet<T> &t)

inline void intersect(const Range<T> &t)

inline void clear()

inline void display(std::ostream &os) const

inline bool operator==(const RangeSet &r) const

```

## 2.5.4 PyQBDI API

### Introduction

We offer bindings for Python, the whole C/C++ API is available through them, but they are also backed up by plenty of helpers that fluidify the script writing.

On Linux and macOS, PyQBDI supports QBDIPreload as *PyQBDIPreload*.

However, you must be aware that PyQBDI has some limitations:

- The library can handle only one *VM* at a time.
- The *VM* must not be used in the `atexit` module.
- 32-bit versions of PyQBDI and Python are needed to instrument 32-bit targets.
- PyQBDI cannot be used to instrument a Python process since both the **host** and the **target** will use the Python runtime.

### VM class

```

class pyqbd.VM
    __init__(self: pyqbd.VM, cpu: str = "", matrs: List[str] = [], options: pyqbd.Options =
        <Options.NO_OPT: 0>) → None
        Construct a new VM for a given CPU with specific attributes

    property options
        Options of the VM

```

## State management

`pyqbd.VM.getGPRState(self: pyqbd.VM) → pyqbd.GPRState`

Obtain the current general purpose register state.

`pyqbd.VM.getFPRState(self: pyqbd.VM) → pyqbd.FPRState`

Obtain the current floating point register state.

`pyqbd.VM.setGPRState(self: pyqbd.VM, gprState: pyqbd.GPRState) → None`

Set the GPR state.

`pyqbd.VM.setFPRState(self: pyqbd.VM, fprState: pyqbd.FPRState) → None`

Set the FPR state.

## Instrumentation range

### Addition

`pyqbd.VM.addInstrumentedRange(self: pyqbd.VM, start: int, end: int) → None`

Add an address range to the set of instrumented address ranges.

`pyqbd.VM.addInstrumentedModule(self: pyqbd.VM, name: str) → bool`

Add the executable address ranges of a module to the set of instrumented address ranges.

`pyqbd.VM.addInstrumentedModuleFromAddr(self: pyqbd.VM, addr: int) → bool`

Add the executable address ranges of a module to the set of instrumented address ranges using an address belonging to the module.

`pyqbd.VM.instrumentAllExecutableMaps(self: pyqbd.VM) → bool`

Adds all the executable memory maps to the instrumented range set.

### Removal

`pyqbd.VM.removeInstrumentedRange(self: pyqbd.VM, start: int, end: int) → None`

Remove an address range from the set of instrumented address ranges.

`pyqbd.VM.removeInstrumentedModule(self: pyqbd.VM, name: str) → bool`

Remove the executable address ranges of a module from the set of instrumented address ranges.

`pyqbd.VM.removeInstrumentedModuleFromAddr(self: pyqbd.VM, addr: int) → bool`

Remove the executable address ranges of a module from the set of instrumented address ranges using an address belonging to the module.

`pyqbd.VM.removeAllInstrumentedRanges(self: pyqbd.VM) → None`

Remove all instrumented ranges.

## Callback management

### InstCallback

`pyqbd.VM.addCodeCB(self: pyqbd.VM, pos: pyqbd.InstPosition, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object, priority: int = <CallbackPriority.PRIORITY_DEFAULT: 0>) → object`

Register a callback event for every instruction executed.

`pyqbd.VM.addCodeAddrCB(self: pyqbd.VM, address: int, pos: pyqbd.InstPosition, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object, priority: int = <CallbackPriority.PRIORITY_DEFAULT: 0>) → object`

Register a callback for when a specific address is executed.

`pyqbd.VM.addCodeRangeCB(self: pyqbd.VM, start: int, end: int, pos: pyqbd.InstPosition, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object, priority: int = <CallbackPriority.PRIORITY_DEFAULT: 0>) → object`

Register a callback for when a specific address range is executed.

`pyqbd.VM.addMnemonicCB(self: pyqbd.VM, mnemonic: str, pos: pyqbd.InstPosition, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object, priority: int = <CallbackPriority.PRIORITY_DEFAULT: 0>) → object`

Register a callback event if the instruction matches the mnemonic.

### VMEvent

`pyqbd.VM.addVMEvtCB(self: pyqbd.VM, mask: pyqbd.VMEvent, cbk: Callable[[pyqbd.VM, pyqbd.VMState, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object) → object`

Register a callback event for a specific VM event.

### MemoryAccess

`pyqbd.VM.addMemAccessCB(self: pyqbd.VM, type: pyqbd.MemoryAccessType, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object, priority: int = <CallbackPriority.PRIORITY_DEFAULT: 0>) → object`

Register a callback event for every memory access matching the type bitfield made by the instructions.

`pyqbd.VM.addMemAddrCB(self: pyqbd.VM, address: int, type: pyqbd.MemoryAccessType, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object) → object`

Add a virtual callback which is triggered for any memory access at a specific address matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost.

`pyqbd.VM.addMemRangeCB(self: pyqbd.VM, start: int, end: int, type: pyqbd.MemoryAccessType, cbk: Callable[[pyqbd.VM, pyqbd.GPRState, pyqbd.FPRState, object], pyqbd.VMAction], data: object) → object`

Add a virtual callback which is triggered for any memory access at a specific address range matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost.

## InstrRuleCallback

`pyqdbi.VM.addInstrRule(self: pyqdbi.VM, cbk: Callable[[pyqdbi.VM, pyqdbi.InstAnalysis, object], List[pyqdbi.InstrRuleDataCBK]], type: pyqdbi.AnalysisType, data: object) → object`  
Add a custom instrumentation rule to the VM.

`pyqdbi.VM.addInstrRuleRange(self: pyqdbi.VM, start: int, end: int, cbk: Callable[[pyqdbi.VM, pyqdbi.InstAnalysis, object], List[pyqdbi.InstrRuleDataCBK]], type: pyqdbi.AnalysisType, data: object) → object`  
Add a custom instrumentation rule to the VM on a specify range.

## Removal

`pyqdbi.VM.deleteInstrumentation(self: pyqdbi.VM, id: int) → None`  
Remove an instrumentation.

`pyqdbi.VM.deleteAllInstrumentations(self: pyqdbi.VM) → None`  
Remove all the registered instrumentations.

## Run

`pyqdbi.VM.run(self: pyqdbi.VM, start: int, stop: int) → bool`  
Start the execution by the DBI.

`pyqdbi.VM.call(self: pyqdbi.VM, function: int, args: List[int]) → Tuple[bool, int]`  
Call a function using the DBI (and its current state).

## InstAnalysis

`pyqdbi.VM.getInstAnalysis(self: pyqdbi.VM, type: pyqdbi.AnalysisType = AnalysisType.ANALYSIS_INSTRUCTION | AnalysisType.ANALYSIS_DISASSEMBLY) → pyqdbi.InstAnalysis`  
Obtain the analysis of the current instruction. Analysis results are cached in the VM.

`pyqdbi.VM.getCachedInstAnalysis(self: pyqdbi.VM, address: int, type: pyqdbi.AnalysisType = AnalysisType.ANALYSIS_INSTRUCTION | AnalysisType.ANALYSIS_DISASSEMBLY) → pyqdbi.InstAnalysis`  
Obtain the analysis of a cached instruction. Analysis results are cached in the VM.

## MemoryAccess

`pyqdbi.VM.getInstMemoryAccess(self: pyqdbi.VM) → List[pyqdbi.MemoryAccess]`  
Obtain the memory accesses made by the last executed instruction.

`pyqdbi.VM.getBBMemoryAccess(self: pyqdbi.VM) → List[pyqdbi.MemoryAccess]`  
Obtain the memory accesses made by the last executed sequence.

`pyqdbi.VM.recordMemoryAccess(self: pyqdbi.VM, type: pyqdbi.MemoryAccessType) → bool`  
Add instrumentation rules to log memory access using inline instrumentation and instruction shadows.

## Cache management

`pyqbdi.VM.precacheBasicBlock(self: pyqbdi.VM, pc: int) → bool`  
Pre-cache a known basic block

`pyqbdi.VM.clearCache(self: pyqbdi.VM, start: int, end: int) → None`  
Clear a specific address range from the translation cache.

`pyqbdi.VM.clearAllCache(self: pyqbdi.VM) → None`  
Clear the entire translation cache.

## Register state

```
class pyqbdi.GPRState
    property AVAILABLE_GPR
        shadow of rbp

    property NUM_GPR
        shadow of eflags

    property REG_BP
        shadow of rbp

    property REG_FLAG
        shadow of eflags

    property REG_LR
        not available on X86_64

    property REG_PC
        shadow of rip

    property REG_RETURN
        shadow of rax

    property REG_SP
        shadow of rsp

    __getitem__(self: pyqbdi.GPRState, index: int) → int
        Get a register like QBDI_GPR_GET

    __setitem__(self: pyqbdi.GPRState, index: int, value: int) → int
        Set a register like QBDI_GPR_SET

    property eflags

    property fs

    property gs

    property r10

    property r11

    property r12

    property r13

    property r14

    property r15

    property r8
```

```
property r9
property rax
property rbp
property rbx
property rcx
property rdi
property rdx
property rip
property rsi
property rsp

class pyqbdι.FPRState
    property cs
        x87 FPU Instruction Pointer Selector

    property dp
        x87 FPU Instruction Operand(Data) Pointer offset

    property ds
        x87 FPU Instruction Operand(Data) Pointer Selector

    property fcw
        x87 FPU control word

    property fop
        x87 FPU Opcode

    property fsw
        x87 FPU status word

    property ftw
        x87 FPU tag word

    property ip
        x87 FPU Instruction Pointer offset

    property mxcsr
        MXCSR Register state

    property mxcsrmask
        MXCSR mask

    property rfcw
        x87 FPU control word

    property rfsw
        x87 FPU status word

    property stmm0
        ST0/MM0

    property stmm1
        ST1/MM1

    property stmm2
        ST2/MM2
```

**property stmm3**  
ST3/MM3

**property stmm4**  
ST4/MM4

**property stmm5**  
ST5/MM5

**property stmm6**  
ST6/MM6

**property stmm7**  
ST7/MM7

**property xmm0**  
XMM 0

**property xmm1**  
XMM 1

**property xmm10**  
XMM 10

**property xmm11**  
XMM 11

**property xmm12**  
XMM 12

**property xmm13**  
XMM 13

**property xmm14**  
XMM 14

**property xmm15**  
XMM 15

**property xmm2**  
XMM 2

**property xmm3**  
XMM 3

**property xmm4**  
XMM 4

**property xmm5**  
XMM 5

**property xmm6**  
XMM 6

**property xmm7**  
XMM 7

**property xmm8**  
XMM 8

**property xmm9**  
XMM 9

**property ymm0**  
YMM0[255:128]

**property ymm1**  
YMM1[255:128]

**property ymm10**  
YMM10[255:128]

**property ymm11**  
YMM11[255:128]

**property ymm12**  
YMM12[255:128]

**property ymm13**  
YMM13[255:128]

**property ymm14**  
YMM14[255:128]

**property ymm15**  
YMM15[255:128]

**property ymm2**  
YMM2[255:128]

**property ymm3**  
YMM3[255:128]

**property ymm4**  
YMM4[255:128]

**property ymm5**  
YMM5[255:128]

**property ymm6**  
YMM6[255:128]

**property ymm7**  
YMM7[255:128]

**property ymm8**  
YMM8[255:128]

**property ymm9**  
YMM9[255:128]

pyqbdι.REG\_RETURN

pyqbdι.REG\_BP

pyqbdι.REG\_SP

pyqbdι.REG\_PC

pyqbdι.NUM\_GPR



## Callback

`pyqbdm.InstCallback(vm: pyqbdm.VM, gpr: pyqbdm.GPRState, fpr: pyqbdm.FPRState, data: object) → pyqbdm.VMAction`

This is the prototype of a function callback for:

- `pyqbdm.VM.addCodeCB()`, `pyqbdm.VM.addCodeAddrCB()` and `pyqbdm.VM.addCodeRangeCB()`
- `pyqbdm.VM.addMnemonicCB()`
- `pyqbdm.VM.addMemAccessCB()`, `pyqbdm.VM.addMemAddrCB()` and `pyqbdm.VM.addMemRangeCB()`
- `pyqbdm.InstrRuleDataCBK`.

### Parameters

- **vm** (*VM*) – The current QBDI object
- **gpr** (*GPRState*) – The current GPRState
- **fpr** (*FPRState*) – The current FPRState
- **data** (*Object*) – A user-defined object.

**Returns** the *VMAction* to continue or stop the execution

`pyqbdm.VMCallback(vm: pyqbdm.VM, vmState: pyqbdm.VMState, gpr: pyqbdm.GPRState, fpr: pyqbdm.FPRState, data: object) → pyqbdm.VMAction`

This is the prototype of a function callback for `pyqbdm.VM.addVMEventCB()`.

### Parameters

- **vm** (*VM*) – The current QBDI object
- **vmState** (*VMState*) – A structure containing the current state of the VM.
- **gpr** (*GPRState*) – The current GPRState
- **fpr** (*FPRState*) – The current FPRState
- **data** (*Object*) – A user-defined object

**Returns** the *VMAction* to continue or stop the execution

`pyqbdm.InstrRuleCallback(vm: pyqbdm.VM, ana: pyqbdm.InstAnalysis, data: object) → List[pyqbdm.InstrRuleDataCBK]`

This is the prototype of a function callback for `pyqbdm.VM.addInstrRule()` and `pyqbdm.VM.addInstrRuleRange()`.

### Parameters

- **vm** (*VM*) – The current QBDI object
- **ana** (*InstAnalysis*) – The current QBDI object
- **data** (*Object*) – A user-defined object

**Returns** A list of `pyqbdm.InstrRuleDataCBK`

**class** `pyqbdm.InstrRuleDataCBK`

```
__init__(self: pyqbdm.InstrRuleDataCBK, cbk: Callable[[QBDI::VM, pyqbdm.GPRState, pyqbdm.FPRState,
object], pyqbdm.VMAction], data: object, position: pyqbdm.InstPosition, priority: int =
<CallbackPriority.PRIORITY_DEFAULT: 0>) → None
```

**property** `cbk`

Address of the function to call when the instruction is executed

**property data**

User defined data which will be forward to cbk.

**property position**

Relative position of the event callback (PREINST / POSTINST).

**property priority**

Priority of the callback.

`pyqbdI.InstPosition = <class 'pyqbdI.InstPosition'>`

Position relative to an instruction.

Members:

PREINST : Positioned before the instruction.

POSTINST : Positioned after the instruction.

`pyqbdI.CallbackPriority = <class 'pyqbdI.CallbackPriority'>`

Priority of callback.

Members:

PRIORITY\_DEFAULT : Default priority for callback.

PRIORITY\_MEMACCESS\_LIMIT : Maximum priority if `getInstMemoryAccess` is used in the callback.

`pyqbdI.VMAction = <class 'pyqbdI.VMAction'>`

The callback results.

Members:

CONTINUE : The execution of the basic block continues.

SKIP\_INST : Available only with PREINST InstCallback. The instruction and the remained PRE-INST callbacks are skip. The execution continue with the POSTINST instruction.

We recommand to used this result with a low priority PREINST callback in order to emulate the instruction without skipping the POSTINST callback.

SKIP\_PATCH : Available only with InstCallback. The current instruction and the reminding callback (PRE and POST) are skip. The execution continues to the next instruction.

For instruction that change the instruction pointer (jump/call/ret), `BREAK_TO_VM` must be used insted of `SKIP`.

`SKIP` can break the record of `MemoryAccess` for the current instruction.

`BREAK_TO_VM` : The execution breaks and returns to the VM causing a complete reevaluation of the execution state. A `BREAK_TO_VM` is needed to ensure that modifications of the Program Counter or the program code are taken into account.

`STOP` : Stops the execution of the program. This causes the run function to return early.

## InstAnalysis

`pyqbdI.AnalysisType = <class 'pyqbdI.AnalysisType'>`

Instruction analysis type

Members:

`ANALYSIS_INSTRUCTION` : Instruction analysis (address, mnemonic, ...)

`ANALYSIS_DISASSEMBLY` : Instruction disassembly

`ANALYSIS_OPERANDS` : Instruction operands analysis

`ANALYSIS_SYMBOL` : Instruction symbol

`class pyqbdI.InstAnalysis`

**property address**

Instruction address (if `ANALYSIS_INSTRUCTION`)

**property affectControlFlow**

True if instruction affects control flow (if `ANALYSIS_INSTRUCTION`)

**property condition**

Condition associated with the instruction (if `ANALYSIS_INSTRUCTION`)

**property disassembly**

Instruction disassembly (if `ANALYSIS_DISASSEMBLY`)

**property flagsAccess**

Flag access type (noaccess, r, w, rw) (if `ANALYSIS_OPERANDS`)

**property instSize**

Instruction size (in bytes) (if `ANALYSIS_INSTRUCTION`)

**property isBranch**

True if instruction acts like a ‘jump’ (if `ANALYSIS_INSTRUCTION`)

**property isCall**

True if instruction acts like a ‘call’ (if `ANALYSIS_INSTRUCTION`)

**property isCompare**

True if instruction is a comparison (if `ANALYSIS_INSTRUCTION`)

**property isMoveImm**

True if this instruction is a move immediate (including conditional moves) instruction. (if `ANALYSIS_INSTRUCTION`)

**property isPredicable**

True if instruction contains a predicate (~is conditional) (if `ANALYSIS_INSTRUCTION`)

**property isReturn**

True if instruction acts like a ‘return’ (if `ANALYSIS_INSTRUCTION`)

**property loadSize**

size of the expected read access (if `ANALYSIS_INSTRUCTION`)

**property mayLoad**

True if QBDI detects a load for this instruction (if `ANALYSIS_INSTRUCTION`)

**property mayStore**

True if QBDI detects a store for this instruction (if `ANALYSIS_INSTRUCTION`)

**property mnemonic**

LLVM mnemonic (if `ANALYSIS_INSTRUCTION`)

**property module**

Instruction module name (if ANALYSIS\_SYMBOL and found)

**property numOperands**

Number of operands used by the instruction (if ANALYSIS\_OPERANDS)

**property operands**

Structure containing analysis results of an operand provided by the VM (if ANALYSIS\_OPERANDS)

**property storeSize**

size of the expected write access (if ANALYSIS\_INSTRUCTION)

**property symbol**

Instruction symbol (if ANALYSIS\_SYMBOL and found)

**property symbolOffset**

Instruction symbol offset (if ANALYSIS\_SYMBOL)

`pyqbdι.ConditionType = <class 'pyqbdι.ConditionType'>`

Condition type

Members:

CONDITION\_NONE : The instruction is unconditionnal

CONDITION\_ALWAYS : The instruction is always true

CONDITION\_NEVER : The instruction is always false

CONDITION\_EQUALS : Equals ( '==' )

CONDITION\_NOT\_EQUALS : Not Equals ( '!=' )

CONDITION\_ABOVE : Above ( '>' unsigned )

CONDITION\_BELOW\_EQUALS : Below or Equals ( '<=' unsigned )

CONDITION\_ABOVE\_EQUALS : Above or Equals ( '>=' unsigned )

CONDITION\_BELOW : Below ( '<' unsigned )

CONDITION\_GREAT : Great ( '>' signed )

CONDITION\_LESS\_EQUALS : Less or Equals ( '<=' signed )

CONDITION\_GREAT\_EQUALS : Great or Equals ( '>=' signed )

CONDITION\_LESS : Less ( '<' signed )

CONDITION\_EVEN : Even

CONDITION\_ODD : Odd

CONDITION\_OVERFLOW : Overflow

CONDITION\_NOT\_OVERFLOW : Not Overflow

CONDITION\_SIGN : Sign

CONDITION\_NOT\_SIGN : Not Sign

`class pyqbdι.OperandAnalysis`

**property flag**

Operand flag

**property regAccess**

Register access type (r, w, rw)

**property regCtxIdx**

Register index in VM state

**property regName**

Register name

**property regOff**

Sub-register offset in register (in bits)

**property size**

Operand size (in bytes)

**property type**

Operand type

**property value**

Operand value (if immediate), or register Id

**pyqbdi.OperandType = <class 'pyqbdi.OperandType'>**

Operand type

Members:

OPERAND\_INVALID : Invalid operand

OPERAND\_IMM : Immediate operand

OPERAND\_GPR : Register operand

OPERAND\_PRED : Predicate operand

OPERAND\_FPR : Float register operand

OPERAND\_SEG : Segment or unsupported register operand

**pyqbdi.OperandFlag = <class 'pyqbdi.OperandFlag'>**

Operand flag

Members:

OPERANDFLAG\_NONE : No flag

OPERANDFLAG\_ADDR : The operand is used to compute an address

OPERANDFLAG\_PCREL : The value of the operand is PC relative

OPERANDFLAG\_UNDEFINED\_EFFECT : The operand role isn't fully defined

OPERANDFLAG\_IMPLICIT : The operand is implicit

**pyqbdi.RegisterAccessType = <class 'pyqbdi.RegisterAccessType'>**

Access type (R/W/RW) of a register operand

Members:

REGISTER\_UNUSED : Unused register

REGISTER\_READ : Register read access

REGISTER\_WRITE : Register write access

REGISTER\_READ\_WRITE : Register read/write access

## MemoryAccess

```
class pyqbdι.MemoryAccess
    property accessAddress
        Address of accessed memory

    property flags
        Memory access flags

    property instAddress
        Address of instruction making the access

    property size
        Size of memory access (in bytes)

    property type
        Memory access type (READ / WRITE)

    property value
        Value read from / written to memory

pyqbdι.MemoryAccessType = <class 'pyqbdι.MemoryAccessType'>
    Memory access type (read / write / ...)

Members:

    MEMORY_READ : Memory read access

    MEMORY_WRITE : Memory write access

    MEMORY_READ_WRITE : Memory read/write access

pyqbdι.MemoryAccessFlags = <class 'pyqbdι.MemoryAccessFlags'>
    Memory access flags

Members:

    MEMORY_NO_FLAGS : Empty flags

    MEMORY_UNKNOWN_SIZE : The size of the access isn't known.

    MEMORY_MINIMUM_SIZE : The given size is a minimum size.

    MEMORY_UNKNOWN_VALUE : The value of the access is unknown or hasn't been retrieved.
```

## VMEvent

```
pyqbdι.VMEvent = <class 'pyqbdι.VMEvent'>
    Members:

    SEQUENCE_ENTRY : Triggered when the execution enters a sequence.

    SEQUENCE_EXIT : Triggered when the execution exits from the current sequence.

    BASIC_BLOCK_ENTRY : Triggered when the execution enters a basic block.

    BASIC_BLOCK_EXIT : Triggered when the execution exits from the current basic block.

    BASIC_BLOCK_NEW : Triggered when the execution enters a new (~unknown) basic block.

    EXEC_TRANSFER_CALL : Triggered when the ExecBroker executes an execution transfer.

    EXEC_TRANSFER_RETURN : Triggered when the ExecBroker returns from an execution transfer.

class pyqbdι.VMState
```

**property basicBlockEnd**

The current basic block end address which can also be the execution transfer destination.

**property basicBlockStart**

The current basic block start address which can also be the execution transfer destination.

**property event**

The event(s) which triggered the callback (must be checked using a mask: `event & BASIC_BLOCK_ENTRY`).

**property sequenceEnd**

The current sequence end address which can also be the execution transfer destination.

**property sequenceStart**

The current sequence start address which can also be the execution transfer destination.

## Memory management

### Allocation

`pyqbdi.alignedAlloc(size: int, align: int) → int`

Allocate a block of memory of a specified sized with an aligned base address.

`pyqbdi.allocateVirtualStack(gprstate: pyqbdi.GPRState, size: int) → object`

Allocate a new stack and setup the `GPRState` accordingly. The allocated stack needs to be freed with `alignedFree()`. The result was `int`, or `None` if the allocation fails.

`pyqbdi.alignedFree(ptr: int) → None`

Free a block of aligned memory allocated with `alignedAlloc`.

`pyqbdi.simulateCall(ctx: pyqbdi.GPRState, returnAddress: int, args: List[int] = []) → None`

Simulate a call by modifying the stack and registers accordingly.

### Exploration

`pyqbdi.getModuleNames() → List[str]`

Get a list of all the module names loaded in the process memory.

`pyqbdi.getCurrentProcessMaps(full_path: bool = False) → List[pyqbdi.MemoryMap]`

Get a list of all the memory maps (regions) of the current process.

`pyqbdi.getRemoteProcessMaps(pid: int, full_path: bool = False) → List[pyqbdi.MemoryMap]`

Get a list of all the memory maps (regions) of a process.

**class** `pyqbdi.MemoryMap`

**property name**

Region name (useful when a region is mapping a module).

**property permission**

Region access rights (`PF_READ`, `PF_WRITE`, `PF_EXEC`).

**property range**

A range of memory (region), delimited between a start and an (excluded) end address.

`pyqbdi.Permission = <class 'pyqbdi.Permission'>`

Memory access rights.

Members:

PF\_NONE : No access  
PF\_READ : Read access  
PF\_WRITE : Write access  
PF\_EXEC : Execution access

## Other globals

`pyqbd.Options` = <class 'pyqbd.Options'>

VM options

Members:

NO\_OPT : Default value  
OPT\_DISABLE\_FPR : Disable all operation on FPU (SSE, AVX, SIMD). May break the execution if the target use the FPU.  
OPT\_DISABLE\_OPTIONAL\_FPR : Disable context switch optimisation when the target execblock doesn't used FPR  
OPT\_ATT\_SYNTAX : Used the AT&T syntax for instruction disassembly  
OPT\_ENABLE\_FS\_GS : Enable Backup/Restore of FS/GS segment. This option uses the instructions (RD|WR)(FS|GS)BASE that must be supported by the operating system.

`pyqbd.VMError` = <class 'pyqbd.VMError'>

QBDI Error values

Members:

INVALID\_EVENTID : Mark a returned event id as invalid

## Miscellaneous

### Version & info

`pyqbd.__arch__`

`pyqbd.__platform__`

`pyqbd.__preload__`

Library load with `pyqbdipreload`

`pyqbd.__version__`

Version of QBDI

## Log

`pyqbd.LogPriority` = <class 'pyqbd.LogPriority'>

Each log has a priority (or level) which can be used to control verbosity In production builds, only Warning and Error logs are kept.

Members:



DEBUG : Debug logs

INFO : Info logs (default)

WARNING : Warning logs

ERROR : Error logs

DISABLE : Disable logs message

`pyqbdi.setLogPriority(priority: pyqbdi.LogPriority) → None`  
 Enable logs matching priority.

## Range

**class** `pyqbdi.Range`

**contains**(\*args, \*\*kwargs)

Overloaded function.

1. `contains(self: pyqbdi.Range, t: int) → bool`

Return True if an value is inside current range boundaries.

2. `contains(self: pyqbdi.Range, r: pyqbdi.Range) → bool`

Return True if a range is inside current range boundaries.

**property end**

Range end value (always excluded).

**intersect**(self: `pyqbdi.Range`, r: `pyqbdi.Range`) → `pyqbdi.Range`

Return the intersection of two ranges.

**overlaps**(self: `pyqbdi.Range`, r: `pyqbdi.Range`) → bool

Return True if a range is overlapping current range lower or/and upper boundary.

**size**(self: `pyqbdi.Range`) → int

Return the total length of a range.

**property start**

Range start value.

## Memory helpers

`pyqbdi.readMemory(address: int, size: int) → bytes`

Read a content from a base address.

**Parameters**

- **address** – Base address
- **size** – Read size

**Returns** Bytes of content.

**Warning:** This API is hazardous as the whole process memory can be read.

`pyqbdi.readRword(address: int) → int`

Read a rword to the specified address

**Parameters** **address** – Base address

**Returns** the value as a unsigned integer

**Warning:** This API is hazardous as the whole process memory can be read.

`pyqbdι.writeMemory(address: int, bytes: str) → None`

Write a memory content to a base address.

**Parameters**

- **address** – Base address
- **bytes** – Memory content

**Warning:** This API is hazardous as the whole process memory can be written.

`pyqbdι.writeRword(address: int, value: int) → None`

Write a rword in a base address.

**Parameters**

- **address** – Base address
- **value** – The value to write, as a unsigned integer

**Warning:** This API is hazardous as the whole process memory can be written.

`pyqbdι.allocateRword() → int`

Allocate a raw memory space to store a rword.

**Returns** Address to a memory space to store a rword

`pyqbdι.allocateMemory(length: int) → int`

Allocate a raw memory space of specified length.

**Parameters** **length** – length of the memory space to allocate

**Returns** Address to the allocated memory

`pyqbdι.freeMemory(address: int) → None`

Free a memory space allocate with allocateRword or allocateMemory.

**Parameters** **address** – Address of the allocated memory

## Float helpers

`pyqbdι.encodeFloat(val: float) → int`

Encode a float as a signed integer.

**Parameters** **val** – Float value

**Returns** a signed integer

`pyqbdι.decodeFloat(val: int) → float`

Encode a signed integer as a float.

**Parameters** **val** – signed integer value

**Returns** a float

`pyqbdI.encodeFloatU(val: float) → int`  
 Encode a float as an unsigned integer.

**Parameters** `val` – Float value

**Returns** an unsigned integer

`pyqbdI.decodeFloatU(val: int) → float`  
 Encode an unsigned integer as a float.

**Parameters** `val` – unsigned integer value

**Returns** a float

`pyqbdI.encodeDouble(val: float) → int`  
 Encode a double as a signed integer.

**Parameters** `val` – Double value

**Returns** a signed integer

`pyqbdI.decodeDouble(val: int) → float`  
 Encode a signed integer as a double.

**Parameters** `val` – signed integer value

**Returns** a double

`pyqbdI.encodeDoubleU(val: float) → int`  
 Encode a double as an unsigned integer.

**Parameters** `val` – Double value

**Returns** an unsigned integer

`pyqbdI.decodeDoubleU(val: int) → float`  
 Encode an unsigned integer as a double.

**Parameters** `val` – unsigned integer value

**Returns** a double

For more conversion utilities, check out the Python's [struct library](#).

## 2.5.5 Frida/QBDI API

### Introduction

We provide bindings for Frida, most C/C++ APIs are exported and available through them, but they are also backed up by plenty of helpers that fluidify the script writing.

Nevertheless, this API slightly differs from the C++ API:

- Every callback must be created as a native function. The callback registration can be done through calling `QBDI.newInstCallback()`, `QBDI.newVMCallback()` and `QBDI.newInstrRuleCallback()`.
- The `QBDI` class is the equivalent of the `VM` class we have in the C++ API.

## QBDI class

With Frida API, the QBDI object is the equivalent of the VM object in C++ API.

### class QBDI()

Create a new instrumentation virtual machine using “**new QBDI()**”

#### QBDI.version

QBDI version (major, minor, patch).

{string:String, integer:Number, major:Number, minor:Number, patch:Number}

## Options

### QBDI.getOptions()

Get the current options of the VM

**Returns Options** – The current option

### QBDI.setOptions(options)

Set the options of the VM

#### Arguments

- **options** (*Options()*) – The new options of the VM.

## State management

### QBDI.getGPRState()

Obtain the current general register state.

**Returns GPRState** – An object containing the General Purpose Registers state.

### QBDI.getFPRState()

Obtain the current floating point register state.

**Returns FPRState** – An object containing the Floating point Purpose Registers state.

### QBDI.setGPRState(state)

Set the GPR state

#### Arguments

- **state** (*GPRState()*) – Array of register values

### QBDI.setFPRState(state)

Set the FPR state

#### Arguments

- **state** (*FPRState()*) – Array of register values

## Instrumentation range

### Addition

**QBDI.addInstrumentedRange**(*start*, *end*)

Add an address range to the set of instrumented address ranges.

#### Arguments

- **start** (String|Number()) – Start address of the range (included).
- **end** (String|Number()) – End address of the range (excluded).

**QBDI.addInstrumentedModule**(*name*)

Add the executable address ranges of a module to the set of instrumented address ranges.

#### Arguments

- **name** (String()) – The module's name.

**Returns** **bool** – True if at least one range was added to the instrumented ranges.

**QBDI.addInstrumentedModuleFromAddr**(*addr*)

Add the executable address ranges of a module to the set of instrumented address ranges. using an address belonging to the module.

#### Arguments

- **addr** (String|Number()) – An address contained by module's range.

**Returns** **bool** – True if at least one range was removed from the instrumented ranges.

**QBDI.instrumentAllExecutableMaps**()

Adds all the executable memory maps to the instrumented range set.

**Returns** **bool** – True if at least one range was added to the instrumented ranges.

### Removal

**QBDI.removeInstrumentedRange**(*start*, *end*)

Remove an address range from the set of instrumented address ranges.

#### Arguments

- **start** (String|Number()) – Start address of the range (included).
- **end** (String|Number()) – End address of the range (excluded).

**QBDI.removeInstrumentedModule**(*name*)

Remove the executable address ranges of a module from the set of instrumented address ranges.

#### Arguments

- **name** (String()) – The module's name.

**Returns** **bool** – True if at least one range was added to the instrumented ranges.

**QBDI.removeInstrumentedModuleFromAddr**(*addr*.)

Remove the executable address ranges of a module from the set of instrumented address ranges using an address belonging to the module.

#### Arguments

- **addr:** (String|Number()) – An address contained by module's range.

**Returns** **bool** – True if at least one range was added to the instrumented ranges.

**QBDI.removeAllInstrumentedRanges()**

Remove all instrumented ranges.

## Callback management

### Creation

**QBDI.newInstCallback(*cbk*)**

Create a native **Instruction callback** from a JS function.

**Example:**

```
>>> var icbk = vm.newInstCallback(function(vm, gpr, fpr, data) {
>>>   inst = vm.getInstAnalysis();
>>>   console.log("0x" + inst.address.toString(16) + " " + inst.disassembly);
>>>   return VMAction.CONTINUE;
>>> });
```

#### Arguments

- **cbk** (*InstCallback()*) – an instruction callback (ex: function(vm, gpr, fpr, data) {});

**Returns** an native InstCallback

**QBDI.newInstrRuleCallback(*cbk*)**

Create a native **Instruction rule callback** from a JS function.

**Example:**

```
>>> var icbk = vm.newInstrRuleCallback(function(vm, ana, data) {
>>>   console.log("0x" + ana.address.toString(16) + " " + ana.disassembly);
>>>   return [new InstrRuleDataCBK(InstPosition.POSTINST, printCB, ana.
↳disassembly)];
>>> });
```

#### Arguments

- **cbk** (*InstrRuleCallback()*) – an instruction callback (ex: function(vm, ana, data) {});

**Returns** an native InstrRuleCallback

**QBDI.newVMCallback(*cbk*)**

Create a native **VM callback** from a JS function.

**Example:**

```
>>> var vcbk = vm.newVMCallback(function(vm, evt, gpr, fpr, data) {
>>>   if (evt.event & VMEvent.EXEC_TRANSFER_CALL) {
>>>     console.warn("[!] External call to 0x" + evt.basicBlockStart.
↳toString(16));
>>>   }
>>>   return VMAction.CONTINUE;
>>> });
```

**Arguments**

- **cbk** (*VMCallback()*) – a VM callback (ex: `function(vm, state, gpr, fpr, data) { };`)

**Returns** a native VMCallback

**InstCallback**

**QBDI.addCodeCB**(*pos, cbk, data, priority*)

Register a callback event for a specific instruction event.

**Arguments**

- **pos** (*InstPosition()*) – Relative position of the callback (PreInst / PostInst).
- **cbk** (*InstCallback()*) – A **native** InstCallback returned by *QBDI.newInstCallback()*.
- **data** (*Object()*) – User defined data passed to the callback.
- **priority** (*Int()*) – The priority of the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMError.INVALID_EVENTID` in case of failure).

**QBDI.addCodeAddrCB**(*addr, pos, cbk, data, priority*)

Register a callback for when a specific address is executed.

**Arguments**

- **addr** (*String|Number()*) – Code address which will trigger the callback.
- **pos** (*InstPosition()*) – Relative position of the callback (PreInst / PostInst).
- **cbk** (*InstCallback()*) – A **native** InstCallback returned by *QBDI.newInstCallback()*.
- **data** (*Object()*) – User defined data passed to the callback.
- **priority** (*Int()*) – The priority of the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMError.INVALID_EVENTID` in case of failure).

**QBDI.addCodeRangeCB**(*start, end, pos, cbk, data, priority*)

Register a callback for when a specific address range is executed.

**Arguments**

- **start** (*String|Number()*) – Start of the address range which will trigger the callback.
- **end** (*String|Number()*) – End of the address range which will trigger the callback.
- **pos** (*InstPosition()*) – Relative position of the callback (PreInst / PostInst).
- **cbk** (*InstCallback()*) – A **native** InstCallback returned by *QBDI.newInstCallback()*.
- **data** (*Object()*) – User defined data passed to the callback.
- **priority** (*Int()*) – The priority of the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMError.INVALID_EVENTID` in case of failure).

**QBDI.addMnemonicCB**(*mnem, pos, cbk, data, priority*)

Register a callback event if the instruction matches the mnemonic.

**Arguments**

- **mnm** (String()) – Mnemonic to match.
- **pos** (*InstPosition()*) – Relative position of the callback (PreInst / PostInst).
- **cbk** (*InstCallback()*) – A **native** InstCallback returned by *QBDI.newInstCallback()*.
- **data** (Object()) – User defined data passed to the callback.
- **priority** (Int()) – The priority of the callback.

**Returns** **Number** – The id of the registered instrumentation (or VMError.INVALID\_EVENTID in case of failure).

## VMEvent

QBDI.**addVMEvtCB**(*mask, cbk, data*)

Register a callback event for a specific VM event.

### Arguments

- **mask** (*VMEvt()*) – A mask of VM event type which will trigger the callback.
- **cbk** (*VMCallback()*) – A **native** VMCB returned by *QBDI.newVMCallback()*.
- **data** (Object()) – User defined data passed to the callback.

**Returns** **Number** – The id of the registered instrumentation (or VMError.INVALID\_EVENTID in case of failure).

## MemoryAccess

QBDI.**addMemAccessCB**(*type, cbk, data, priority*)

Register a callback event for every memory access matching the type bitfield made by the instruction in the range codeStart to codeEnd.

### Arguments

- **type** (*MemoryAccessType()*) – A mode bitfield: either MEMORY\_READ, MEMORY\_WRITE or both (MEMORY\_READ\_WRITE).
- **cbk** (*InstCallback()*) – A **native** InstCallback returned by *QBDI.newInstCallback()*.
- **data** (Object()) – User defined data passed to the callback.
- **priority** (Int()) – The priority of the callback.

**Returns** **Number** – The id of the registered instrumentation (or VMError.INVALID\_EVENTID in case of failure).

QBDI.**addMemAddrCB**(*addr, type, cbk, data*)

Add a virtual callback which is triggered for any memory access at a specific address matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost.

### Arguments

- **addr** (String|Number()) – Code address which will trigger the callback.
- **type** (*MemoryAccessType()*) – A mode bitfield: either MEMORY\_READ, MEMORY\_WRITE or both (MEMORY\_READ\_WRITE).
- **cbk** (*InstCallback()*) – A **native** InstCallback returned by *QBDI.newInstCallback()*.



- **data** (`Object()`) – User defined data passed to the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMErrors.INVALID_EVENTID` in case of failure).

`QBDI.addMemRangeCB(start, end, type, cbk, data)`

Add a virtual callback which is triggered for any memory access in a specific address range matching the access type. Virtual callbacks are called via callback forwarding by a gate callback triggered on every memory access. This incurs a high performance cost.

#### Arguments

- **start** (`String|Number()`) – Start of the address range which will trigger the callback.
- **end** (`String|Number()`) – End of the address range which will trigger the callback.
- **type** (`MemoryAccessType()`) – A mode bitfield: either `MEMORY_READ`, `MEMORY_WRITE` or both (`MEMORY_READ_WRITE`).
- **cbk** (`InstCallback()`) – A **native** `InstCallback` returned by `QBDI.newInstCallback()`.
- **data** (`Object()`) – User defined data passed to the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMErrors.INVALID_EVENTID` in case of failure).

## InstrRuleCallback

`QBDI.addInstrRule(cbk, type, data)`

Add a custom instrumentation rule to the VM.

#### Arguments

- **cbk** (`InstrRuleCallback()`) – A **native** `InstrRuleCallback` returned by `QBDI.newInstrRuleCallback()`.
- **type** (`AnalysisType()`) – Analyse type needed for this instruction function pointer to the callback
- **data** (`Object()`) – User defined data passed to the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMErrors.INVALID_EVENTID` in case of failure).

`QBDI.addInstrRuleRange(start, end, cbk, type, data)`

Add a custom instrumentation rule to the VM for a range of address.

#### Arguments

- **start** (`String|Number()`) – Begin of the range of address where apply the rule
- **end** (`String|Number()`) – End of the range of address where apply the rule
- **cbk** (`InstrRuleCallback()`) – A **native** `InstrRuleCallback` returned by `QBDI.newInstrRuleCallback()`.
- **type** (`AnalysisType()`) – Analyse type needed for this instruction function pointer to the callback
- **data** (`Object()`) – User defined data passed to the callback.

**Returns** **Number** – The id of the registered instrumentation (or `VMErrors.INVALID_EVENTID` in case of failure).

## Removal

**QBDI.deleteInstrumentation(*id*)**

Remove an instrumentation.

### Arguments

- **id** (Number()) – The id of the instrumentation to remove.

**Returns** **bool** – True if instrumentation has been removed.

**QBDI.deleteAllInstrumentations()**

Remove all the registered instrumentations.

## Memory management

### Allocation

**QBDI.alignedAlloc(*size, align*)**

Allocate a block of memory of a specified sized with an aligned base address.

### Arguments

- **size** (Number()) – Allocation size in bytes.
- **align** (Number()) – Base address alignment in bytes.

**Returns** Pointer (rword) to the allocated memory or NULL in case an error was encountered.

**QBDI.allocateVirtualStack(*state, stackSize*)**

Allocate a new stack and setup the GPRState accordingly. The allocated stack needs to be freed with aligned-Free().

### Arguments

- **state** (*GPRState()*) – Array of register values
- **stackSize** (Number()) – Size of the stack to be allocated.

**Returns** Pointer (rword) to the allocated memory or NULL in case an error was encountered.

**QBDI.alignedFree(*ptr*)**

Free a block of aligned memory allocated with alignedAlloc or allocateVirtualStack

### Arguments

- **ptr** (NativePtr()) – Pointer to the allocated memory.

## Exploration

**QBDI.getModuleNames()**

Use QBDI engine to retrieve loaded modules.

**Returns** list of module names (ex: ["ls", "libc", "libz"])

## Run

QBDI.**run**(*start*, *stop*)

Start the execution by the DBI from a given address (and stop when another is reached).

### Arguments

- **start** (String|Number()) – Address of the first instruction to execute.
- **stop** (String|Number()) – Stop the execution when this instruction is reached.

**Returns** **bool** – True if at least one block has been executed.

QBDI.**call**(*address*, *args*)

Call a function by its address (or through a Frida NativePointer).

Arguments can be provided, but their types need to be compatible with the `.toRword()` interface (like NativePointer or UInt64).

### Example:

```
>>> var vm = new QBDI();
>>> var state = vm.getGPRState();
>>> vm.allocateVirtualStack(state, 0x1000000);
>>> var aFunction = Module.findExportByName(null, "Secret");
>>> vm.addInstrumentedModuleFromAddr(aFunction);
>>> vm.call(aFunction, [42]);
```

### Arguments

- **address** (String|Number()) – function address (or Frida NativePointer).
- **args** (StringArray|NumberArray()) – optional list of arguments

QBDI.**simulateCall**(*state*, *retAddr*, *args*)

Simulate a call by modifying the stack and registers accordingly.

### Arguments

- **state** (*GPRState*()) – Array of register values
- **retAddr** (String|Number()) – Return address of the call to simulate.
- **args** (StringArray|NumberArray()) – A variadic list of arguments.

## InstAnalysis

QBDI.**getInstAnalysis**(*type*)

Obtain the analysis of the current instruction. Analysis results are cached in the VM. The validity of the returned pointer is only guaranteed until the end of the callback, else a deepcopy of the structure is required.

### Arguments

- **type** (*AnalysisType*()) – Properties to retrieve during analysis (default to ANALYSIS\_INSTRUCTION | ANALYSIS\_DISASSEMBLY).

**Returns** **InstAnalysis** – A *InstAnalysis*() object containing the analysis result.

QBDI.**getCachedInstAnalysis**(*addr*, *type*)

Obtain the analysis of a cached instruction. Analysis results are cached in the VM. The validity of the returned pointer is only guaranteed until the end of the callback, else a deepcopy of the structure is required.

#### Arguments

- **addr** (String|Number()) – The address of the instruction to analyse.
- **type** (*AnalysisType()*) – Properties to retrieve during analysis (default to ANALYSIS\_INSTRUCTION | ANALYSIS\_DISASSEMBLY).

**Returns** *InstAnalysis* – A *InstAnalysis()* object containing the analysis result. null if the instruction isn't in the cache.

### MemoryAccess

#### QBDI.getInstMemoryAccess()

Obtain the memory accesses made by the last executed instruction. Return NULL and a size of 0 if the instruction made no memory access.

**Returns** *Array.<MemoryAccess>* – An array of *MemoryAccess()* made by the instruction.

#### QBDI.getBBMemoryAccess()

Obtain the memory accesses made by the last executed sequence. Return NULL and a size of 0 if the basic block made no memory access.

**Returns** *Array.<MemoryAccess>* – An array of *MemoryAccess()* made by the sequence.

#### QBDI.recordMemoryAccess(type)

Obtain the memory accesses made by the last executed instruction. Return NULL and a size of 0 if the instruction made no memory access.

#### Arguments

- **type** (*MemoryAccessType()*) – Memory mode bitfield to activate the logging for: either MEMORY\_READ, MEMORY\_WRITE or both (MEMORY\_READ\_WRITE).

### Cache management

#### QBDI.precacheBasicBlock(pc)

Pre-cache a known basic block.

#### Arguments

- **pc** (String|Number()) – Start address of a basic block

**Returns** *bool* – True if basic block has been inserted in cache.

#### QBDI.clearCache(start, end)

Clear a specific address range from the translation cache.

#### Arguments

- **start** (String|Number()) – Start of the address range to clear from the cache.
- **end** (String|Number()) – End of the address range to clear from the cache.

#### QBDI.clearAllCache()

Clear the entire translation cache.

## Register state

### class GPRState()

General Purpose Register context

`GPRState.dump(color)`

Pretty print and log QBDI context.

#### Arguments

- **color** (`bool()`) – Will print a colored version of the context if set.

`GPRState.getRegister(rid)`

This function is used to get the value of a specific register.

#### Arguments

- **rid** (`String|Number()`) – Register (register name or ID can be used e.g : “RAX”, “rax”, 0)

**Returns** GPR value (ex: 0x42)

`GPRState.getRegisters()`

This function is used to get values of all registers.

**Returns** GPRs of current context (ex: {“RAX”:0x42, ... })

`GPRState.pp(color)`

Pretty print QBDI context.

#### Arguments

- **color** (`bool()`) – Will print a colored version of the context if set.

**Returns** dump of all GPRs in a pretty format

`GPRState.setRegister(rid, value)`

This function is used to set the value of a specific register.

#### Arguments

- **rid** (`String|Number()`) – Register (register name or ID can be used e.g : “RAX”, “rax”, 0)
- **value** (`String|Number()`) – Register value (use **strings** for big integers)

`GPRState.setRegisters(gprs)`

This function is used to set values of all registers.

#### Arguments

- **gprs** – Array of register values

`GPRState.synchronizeContext(FridaCtx, direction)`

This function is used to synchronise context between Frida and QBDI.

**Warning:** Currently QBDI\_TO\_FRIDA is not implemented (due to Frida limitations).

#### Arguments

- **FridaCtx** – Frida context
- **direction** (`SyncDirection()`) – Synchronization direction. (FRIDA\_TO\_QBDI or QBDI\_TO\_FRIDA)

`GPRState.synchronizeRegister(FridaCtx, rid, direction)`

This function is used to synchronise a specific register between Frida and QBDI.

**Warning:** Currently QBDI\_TO\_FRIDA is experimental. (E.G : RIP cannot be synchronized)

#### Arguments

- **FridaCtx** – Frida context
- **rid** (`String|Number()`) – Register (register name or ID can be used e.g : “RAX”, “rax”, 0)
- **direction** (`SyncDirection()`) – Synchronization direction. (FRIDA\_TO\_QBDI or QBDI\_TO\_FRIDA)

**class SyncDirection()**

Synchronisation direction between Frida and QBDI GPR contexts

`SyncDirection.QBDI_TO_FRIDA`

Constant variable used to synchronize QBDI’s context to Frida’s.

**Warning:** This is currently not supported due to the lack of context updating in Frida.

`SyncDirection.FRIDA_TO_QBDI`

Constant variable used to synchronize Frida’s context to QBDI’s.

**GPR\_NAMES**

An array holding register names.

**REG\_PC**

String of the instruction pointer register.

**REG\_RETURN**

A constant string representing the register carrying the return value of a function.

**REG\_SP**

String of the stack pointer register.

## Callback

**InstCallback**(*vm, gpr, fpr, data*)

This is the prototype of a function callback for:

- `QBDI.addCodeCB()`, `QBDI.addCodeAddrCB()` and `QBDI.addCodeRangeCB()`
- `QBDI.addMnemonicCB()`
- `QBDI.addMemAccessCB()`, `QBDI.addMemAddrCB()` and `QBDI.addMemRangeCB()`
- `InstrRuleDataCBK()`.

The function must be registered with `QBDI.newInstCallback()`.

#### Arguments

- **vm** (`QBDI()`) – The current QBDI object
- **gpr** (`GPRState()`) – The current GPRState

- **fpr** (*FPRState()*) – The current *FPRState*
- **data** (*Object()*) – A user-defined object.

**Returns** the *VMAction()* to continue or stop the execution

**VMCallback**(*vm, vmState, gpr, fpr, data*)

This is the prototype of a function callback for *QBDI.addVMEventCB()*. The function must be registered with *QBDI.newVMCallback()*.

#### Arguments

- **vm** (*QBDI()*) – The current QBDI object
- **vmState** (*VMState()*) – A structure containing the current state of the VM.
- **gpr** (*GPRState()*) – The current *GPRState*
- **fpr** (*FPRState()*) – The current *FPRState*
- **data** (*Object()*) – A user-defined object

**Returns** the *VMAction()* to continue or stop the execution

**InstrRuleCallback**(*vm, ana, data*)

This is the prototype of a function callback for *QBDI.addInstrRule()* and *QBDI.addInstrRuleRange()*. The function must be registered with *QBDI.newInstrRuleCallback()*.

#### Arguments

- **vm** (*QBDI()*) – The current QBDI object
- **ana** (*InstAnalysis()*) – The current QBDI object
- **data** (*Object()*) – A user-defined object

**Returns** An Array of *InstrRuleDataCBK()*

**class InstrRuleDataCBK**(*pos, cbk, data, priority*)

Object to define an *InstCallback()* in an *InstrRuleCallback()*

#### Arguments

- **pos** (*InstPosition()*) – Relative position of the callback (PreInst / PostInst).
- **cbk** (*InstCallback()*) – A **native** *InstCallback* returned by *QBDI.newInstCallback()*.
- **data** (*Object()*) – User defined data passed to the callback.
- **priority** (*Int()*) – The priority of the callback.

**class VMAction()**

The callback results.

**VMAction.CONTINUE**

The execution of the basic block continues.

**VMAction.SKIP\_INST**

Available only with PREINST *InstCallback*. The instruction and the remained PREINST callbacks are skip. The execution continue with the POSTINST instruction.

We recommend to used this result with a low priority PREINST callback in order to emulate the instruction without skipping the POSTINST callback.

**VMAction.SKIP\_PATCH**

Available only with *InstCallback*. The current instruction and the reminding callback (PRE and POST) are skip. The execution continues to the next instruction.

For instruction that change the instruction pointer (jump/call/ret), `BREAK_TO_VM` must be used instead of `SKIP`.

`SKIP` can break the record of `MemoryAccess` for the current instruction.

**`VMAction.BREAK_TO_VM`**

The execution breaks and returns to the VM causing a complete reevaluation of the execution state. A `VMAction.BREAK_TO_VM` is needed to ensure that modifications of the Program Counter or the program code are taken into account.

**`VMAction.STOP`**

Stops the execution of the program. This causes the run function to return early.

**`class InstPosition()`**

Position relative to an instruction.

**`InstPosition.PREINST`**

Positioned **before** the instruction.

**`InstPosition.POSTINST`**

Positioned **after** the instruction.

**`class CallbackPriority()`**

Priority of callback

**`CallbackPriority.PRIORITY_DEFAULT`**

Default priority for callback.

**`CallbackPriority.PRIORITY_MEMACCESS_LIMIT`**

Maximum priority if `getInstMemoryAccess` is used in the callback.

## InstAnalysis

**`class AnalysisType()`**

Properties to retrieve during an instruction analysis.

**`AnalysisType.ANALYSIS_INSTRUCTION`**

Instruction analysis (address, mnemonic, ...).

**`AnalysisType.ANALYSIS_DISASSEMBLY`**

Instruction disassembly.

**`AnalysisType.ANALYSIS_OPERANDS`**

Instruction operands analysis.

**`AnalysisType.ANALYSIS_SYMBOL`**

Instruction nearest symbol (and offset).

**`class InstAnalysis()`**

Object that describes the analysis of an instruction

**`InstAnalysis.address`**

Instruction address (if `ANALYSIS_INSTRUCTION`)

**`InstAnalysis.affectControlFlow`**

True if instruction affects control flow (if `ANALYSIS_INSTRUCTION`)

**`InstAnalysis.disassembly`**

Instruction disassembly (if `ANALYSIS_DISASSEMBLY`)

**`InstAnalysis.instSize`**

Instruction size (in bytes) (if `ANALYSIS_INSTRUCTION`)



**InstAnalysis.isBranch**  
True if instruction acts like a ‘jump’ (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.isCall**  
True if instruction acts like a ‘call’ (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.isCompare**  
True if instruction is a comparison (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.isPredicable**  
True if instruction contains a predicate (~is conditional) (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.isMoveImm**  
True if this instruction is a move immediate (including conditional moves) instruction (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.isReturn**  
True if instruction acts like a ‘return’ (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.mayLoad**  
True if QBDI detects a load for this instruction (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.mayStore**  
True if QBDI detects a store for this instruction (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.loadSize**  
size of the expected read access (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.storeSize**  
size of the expected written access (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.condition**  
Condition associated with the instruction (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.mnemonic**  
LLVM mnemonic (if ANALYSIS\_INSTRUCTION)

**InstAnalysis.flagsAccess**  
Flag access type (noaccess, r, w, rw) (if ANALYSIS\_OPERANDS)

**InstAnalysis.operands**  
Structure containing analysis results of an operand provided by the VM (if ANALYSIS\_OPERANDS)

**InstAnalysis.module**  
Instruction module name (if ANALYSIS\_SYMBOL and found)

**InstAnalysis.symbol**  
Instruction symbol (if ANALYSIS\_SYMBOL and found)

**class ConditionType()**  
Instruction Condition

**ConditionType.CONDITION\_NONE**  
The instruction is unconditionnal

**ConditionType.CONDITION\_ALWAYS**  
The instruction is always true

**ConditionType.CONDITION\_NEVER**  
The instruction is always false

**ConditionType.CONDITION\_EQUALS**  
Equals ( ‘==’ )

`ConditionType.CONDITION_NOT_EQUALS`  
Not Equals ( '!=' )

`ConditionType.CONDITION_ABOVE`  
Above ( '>' unsigned )

`ConditionType.CONDITION_BELOW_EQUALS`  
Below or Equals ( '<=' unsigned )

`ConditionType.CONDITION_ABOVE_EQUALS`  
Above or Equals ( '>=' unsigned )

`ConditionType.CONDITION_BELOW`  
Below ( '<' unsigned )

`ConditionType.CONDITION_GREAT`  
Great ( '>' signed )

`ConditionType.CONDITION_LESS_EQUALS`  
Less or Equals ( '<=' signed )

`ConditionType.CONDITION_GREAT_EQUALS`  
Great or Equals ( '>=' signed )

`ConditionType.CONDITION_LESS`  
Less ( '<' signed )

`ConditionType.CONDITION_EVEN`  
Even

`ConditionType.CONDITION_ODD`  
Odd

`ConditionType.CONDITION_OVERFLOW`  
Overflow

`ConditionType.CONDITION_NOT_OVERFLOW`  
Not Overflow

`ConditionType.CONDITION_SIGN`  
Sign

`ConditionType.CONDITION_NOT_SIGN`  
Not Sign

**class OperandAnalysis()**

Structure containing analysis results of an operand provided by the VM.

`OperandAnalysis.type`  
Operand type

`OperandAnalysis.flag`  
Operand flag

`OperandAnalysis.value`  
Operand value (if immediate), or register Id

`OperandAnalysis.size`  
Operand size (in bytes)

`OperandAnalysis.regOff`  
Sub-register offset in register (in bits)

**OperandAnalysis.regCtxIdx**

Register index in VM state

**OperandAnalysis.regName**

Register name

**OperandAnalysis.regAccess**

Register access type (r, w, rw)

**class OperandType()**

Register access type (read / write / rw)

**OperandType.OPERAND\_INVALID**

Invalid operand.

**OperandType.OPERAND\_IMM**

Immediate operand.

**OperandType.OPERAND\_GPR**

General purpose register operand.

**OperandType.OPERAND\_PRED**

Predicate special operand.

**OperandType.OPERAND\_FPR**

Float register operand.

**OperandType.OPERAND\_SEG**

Segment or unsupported register operand

**class OperandFlag()**

Operand flag

**OperandFlag.OPERANDFLAG\_NONE**

No flag

**OperandFlag.OPERANDFLAG\_ADDR**

The operand is used to compute an address

**OperandFlag.OPERANDFLAG\_PCREL**

The value of the operand is PC relative

**OperandFlag.OPERANDFLAG\_UNDEFINED\_EFFECT**

The operand role isn't fully defined

**OperandFlag.OPERANDFLAG\_IMPLICIT**

The operand is implicit

**class RegisterAccessType()**

Register access type (read / write / rw)

**RegisterAccessType.REGISTER\_READ**

Register is read.

**RegisterAccessType.REGISTER\_WRITE**

Register is written.

**RegisterAccessType.REGISTER\_READ\_WRITE**

Register is read/written.

## MemoryAccess

### class MemoryAccess()

Object that describes a memory access

**MemoryAccess.accessAddress**

Address of accessed memory

**MemoryAccess.instAddress**

Address of instruction making the access

**MemoryAccess.size**

Size of memory access (in bytes)

**MemoryAccess.type**

Memory access type (READ / WRITE)

**MemoryAccess.value**

Value read from / written to memory

**MemoryAccess.flags**

Memory access flags

### class MemoryAccessType()

Memory access type (read / write / ...)

**MemoryAccessType.MEMORY\_READ**

Memory read access.

**MemoryAccessType.MEMORY\_WRITE**

Memory write access.

**MemoryAccessType.MEMORY\_READ\_WRITE**

Memory read/write access.

### class MemoryAccessFlags()

Memory access flags

**MemoryAccessFlags.MEMORY\_NO\_FLAGS**

Empty flag.

**MemoryAccessFlags.MEMORY\_UNKNOWN\_SIZE**

The size of the access isn't known.

**MemoryAccessFlags.MEMORY\_MINIMUM\_SIZE**

The given size is a minimum size.

**MemoryAccessFlags.MEMORY\_UNKNOWN\_VALUE**

The value of the access is unknown or hasn't been retrieved.

## VMEvent

### class VMEvent()

Events triggered by the virtual machine.

**VMEvent.SEQUENCE\_ENTRY**

Triggered when the execution enters a sequence.

**VMEvent.SEQUENCE\_EXIT**

Triggered when the execution exits from the current sequence.

**VMEvent.BASIC\_BLOCK\_ENTRY**

Triggered when the execution enters a basic block.

**VMEvent.BASIC\_BLOCK\_EXIT**

Triggered when the execution exits from the current basic block.

**VMEvent.BASIC\_BLOCK\_NEW**

Triggered when the execution enters a new (~unknown) basic block.

**VMEvent.EXEC\_TRANSFER\_CALL**

Triggered when the ExecBroker executes an execution transfer.

**VMEvent.EXEC\_TRANSFER\_RETURN**

Triggered when the ExecBroker returns from an execution transfer.

**VMEvent.SYSCALL\_ENTRY**

Not implemented.

**VMEvent.SYSCALL\_EXIT**

Not implemented.

**VMEvent.SIGNAL**

Not implemented.

**class VMState()**

Object that describes the current VM state

**VMState.event**

The event(s) which triggered the callback (must be checked using a mask: event & BASIC\_BLOCK\_ENTRY).

**VMState.sequenceStart**

The current basic block start address which can also be the execution transfer destination.

**VMState.sequenceEnd**

The current basic block end address which can also be the execution transfer destination.

**VMState.basicBlockStart**

The current sequence start address which can also be the execution transfer destination.

**VMState.basicBlockEnd**

The current sequence end address which can also be the execution transfer destination.

**VMState.lastSignal**

Not implemented.

## Other globals

**QBDI\_LIB\_FULLPATH**

Fullpath of the QBDI library

**class Options()**

QBDI VM Options

**Options.NO\_OPT**

Default value

**Options.OPT\_DISABLE\_FPR**

Disable all operation on FPU (SSE, AVX, SIMD). May break the execution if the target use the FPU.

**Options.OPT\_DISABLE\_OPTIONAL\_FPR**

Disable context switch optimisation when the target execblock doesn't used FPR.

**Options.OPT\_ATT\_SYNTAX**

Used the AT&T syntax for instruction disassembly (for X86 and X86\_64)

**Options.OPT\_ENABLE\_FS\_GS**

Enable Backup/Restore of FS/GS segment. This option uses the instructions (RD|WR)(FS|GS)BASE that must be supported by the operating system.

**class VMErrror()**

Error return by the QBDI VM

**VMErrror.INVALID\_EVENTID**

Returned event is invalid.

## Register values

The size of a general register depends of the architecture. QBDI uses a custom type (*rword*) to represent a register value.

This binding provides a common interface (`.toRword()`) to cast values into JS types compatible with the C *rword* type.

**rword**

An alias to Frida uint type with the size of general registers (**uint64** or **uint32**)

**NativePointer.prototype.toRword()**

Convert a NativePointer into a type with the size of a register (Number or UInt64).

**Number.prototype.toRword()**

Convert a number into a type with the size of a register (Number or UInt64). Can't be used for numbers > 32 bits would cause weird results due to IEEE-754.

**UInt64.prototype.toRword()**

An identity function (returning the same UInt64 object). It exists only to provide a unified **toRword** interface.

## Helpers

Some functions helpful to interact with Frida's interface and write scripts.

**hexPointer(ptr)**

This function is used to pretty print a pointer, padded with 0 to the size of a register.

**Arguments**

- **ptr** – Pointer you want to pad

**Returns** pointer value as padded string (ex: "0x00004242")

## 2.5.6 QBDIPreload API

### Introduction

QBDIPreload is a small utility library that provides code injection capabilities using dynamic library injection. It currently only works under **Linux** using the LD\_PRELOAD mechanism and **macOS** using the DYLD\_INSERT\_LIBRARIES mechanism. For other platforms please check out *Frida/QBDI API* instead.

QBDIPreload exploits these library injection mechanisms to hijack the normal program startup. During the hijacking process QBDIPreload will call your code allowing you to setup and start your instrumentation. The compilation should produce a dynamic library (.so under **Linux**, .dylib under **macOS**) which should then be added to the matching

environment variable (LD\_PRELOAD under **Linux** and DYLD\_INSERT\_LIBRARIES under **macOS**) when running the target binary.

You can look at [Generate a template](#) for a working example with build and usage instructions.

---

**Note:** QBDIPreload automatically takes care of blacklisting instrumentation of the C standard library and the OS loader as described in [Limitations](#).

---

---

**Note:** Please note that QBDIPreload does not allow instrumenting a binary before the main function (inside the loader and the library constructors / init) as explained in [Limitations](#).

---

---

**Note:** QBDIPreload is supposed to be used with LD\_PRELOAD or DYLD\_INSERT\_LIBRARIES mechanisms to inject some code into the target process. Hence, the limitations of these also affect QBDIPreload (cannot inject suid binary, ...).

---

## Initialisation

### QBDIPRELOAD\_INIT

A C pre-processor macro declaring a constructor.

**Warning:** QBDIPRELOAD\_INIT must be used once in any project using QBDIPreload. It declares a constructor, so it must be placed like a function declaration on a single line.

## Return codes

### QBDIPRELOAD\_NO\_ERROR

No error.

### QBDIPRELOAD\_NOT\_HANDLED

Startup step not handled by callback.

### QBDIPRELOAD\_ERR\_STARTUP\_FAILED

Error in the startup (preload) process.

## User callbacks

int **qbdipreload\_on\_start**(void \*main)

Function called when preload is on a program entry point (interposed start or an early constructor). It provides the main function address, that can be used to place a hook using the qbdipreload\_hook\_main API.

**Parameters** **main** – [in] Address of the main function

**Returns** int QBDIPreload state

int **qbdipreload\_on\_premain**(void \*gprCtx, void \*fpuCtx)

Function called when preload hook on main function is triggered. It provides original (and platforms dependent) GPR and FPR contexts. They can be converted to QBDI states, using `qbdipreload_threadCtxToGPRState` and `qbdipreload_floatCtxToFPRState` APIs.

**Parameters**

- **gprCtx** – [in] Original GPR context
- **fpuCtx** – [in] Original FPU context

**Returns** int QBDIPreload state

int **qbdipreload\_on\_main**(int argc, char \*\*argv)

Function called when preload has successfully hijacked the main thread and we are in place of the original main function (with the same thread state).

**Parameters**

- **argc** – [in] Original argc
- **argv** – [in] Original argv

**Returns** int QBDIPreload state

int **qbdipreload\_on\_run**(*VMInstanceRef* vm, *rword* start, *rword* stop)

Function called when preload is done and we have a valid QBDI VM object on which we can call run (after some last initializations).

**Parameters**

- **vm** – [in] VM instance.
- **start** – [in] Start address of the range (included).
- **stop** – [in] End address of the range (excluded).

**Returns** int QBDIPreload state

int **qbdipreload\_on\_exit**(int status)

Function called when process is exiting (using `_exit` or `exit`).

**Parameters** **status** – [in] exit status

**Returns** int QBDIPreload state

## Helpers

int **qbdipreload\_hook\_main**(void \*main)

Enable QBDIPreload hook on the main function (using its address)

**Warning:** It MUST be used in `qbdipreload_on_start` if you want to handle this step. The assumed main address is provided as a callback argument.

**Parameters** **main** – [in] Pointer to the main function

void **qbdipreload\_threadCtxToGPRState**(const void \*gprCtx, *GPRState* \*gprState)

Convert a QBDIPreload GPR context (platform dependent) to a QBDI GPR state.

**Parameters**

- **gprCtx** – [in] Platform GPRState pointer



- **gprState** – [in] QBDI GPRState pointer

void **qbdipreload\_floatCtxToFPRState**(const void \*fprCtx, *FPRState* \*fprState)  
Convert a QBDIPreload FPR context (platform dependent) to a QBDI FPR state.

#### Parameters

- **fprCtx** – [in] Platform FPRState pointer
- **fprState** – [in] QBDI FPRState pointer

## 2.5.7 PyQBDIPreload API

### Introduction

PyQBDIPreload consists of two main components:

- The QBDIPreload script included in the PyQBDI library. It will load the Python runtime and execute the user script in order to instrument the target.
- An injector script called *pyqbdipreload.py* that sets up the environment variables to inject the library and the Python runtime.

---

**Note:** PyQBDIPreload has the same limitations as QBDIPreload and PyQBDI.

---

### User callback

**pyqbdipreload\_on\_run**(*vm*: *pyqbd.VM*, *start*: *int*, *end*: *int*)

This function must be present in the preloaded script

#### Parameters

- **vm** (*VM*) – VM Instance
- **start** (*int*) – Start address of the range (included).
- **end** (*int*) – End address of the range (excluded).

### QBDIPreload steps

*qbdipreload\_on\_start()* and *qbdipreload\_on\_premain()* are not available on PyQBDIPreload.

The Python interpreter and the preloaded script are loaded while executing *qbdipreload\_on\_main()*.

The *pyqbdipreload\_on\_run()* method is called while executing *qbdipreload\_on\_main()*.

The interpreter is shut down while executing *qbdipreload\_on\_exit()*, after calling all the registered methods of *atexit* module.

## PyQBDIPreload script

You can use *pyqbdipreload.py* as follows:

```
$ python3 -m pyqbdipreload <script> <target> [<args> ...]
```

with:

- **script**: The Python script
- **target**: The binary you are targeting
- **args**: Argument(s) to be passed to the binary (if any)

## 2.6 Architecture Support

Our patching system uses a generic approach which means instruction support is not explicit but implicit. Only instructions that use the program counter register (**rip** under x86-64 and **pc** under ARM) or modify the control flow needs patching and we hope the current patching rules cover all such cases. However some corner cases or bugs in the disassembly and assembly backend of LLVM might still cause troubles.

To guarantee that instrumented programs run smoothly and that no such bugs exist, we are running automated tests on a wide variety of binaries (see [Testing](#) for more details). From those tests we can establish an instruction coverage which provides an estimation of the instructions supported by QBDI. This estimation is far from complete because the other instructions were simply probably never encountered in the test suite.

Instructions below are listed using their mnemonic (or LLVM MC opcode). This naming convention distinguishes between size and operand variants of the same mnemonic: **ADD64rm** is a 64 bits add of a memory value to a register while **ADD32ri8** is a 32 bits add of an 8 bits immediate to a register.

### 2.6.1 Intel x86-64

The x86-64 support is complete and mature. Only a small part of SIMD instructions are covered by our tests but we do not expect any problems with the uncovered ones because their semantic are closely related to the covered ones. We currently don't support the following features:

- **AVX512**: the register of this extension isn't supported and will not be restored/backup during the execution
- **privileged instruction**: QBDI is an userland (ring3) application and privileged registers aren't managed
- **CET feature**: shadow stack is not implemented and the current instrumentation doesn't support indirect branch tracking.
- **HLE and RTM features** and any instructions for multithreading: QBDI allows inserting callbacks at any position and cannot guarantee that instructions of the same transactions unit will not be split.
- **MPX feature**: bound registers aren't supported.
- **XOP instructions for ADM processors**: The instructions are never been tested.

The memory access information is provided for most of general and SIMD instructions. The information is missing for:

- The instructions include in an unsupported feature
- **VGATHER\*** and **VPGATHER\*** instructions of AVX2.

## Instruction Coverage

```

ADC32mi8 ADC64mi8
ADD16mi8 ADD16mr ADD16rm ADD32i32 ADD32mi8 ADD32mr ADD32ri ADD32ri8 ADD32rm ADD32rr_
↪ADD64i32 ADD64mi32 ADD64mi8 ADD64mr ADD64ri32 ADD64ri8 ADD64rm ADD64rr ADD8rr ADDSDrm_
↪Int ADDSDrr_Int
AESENCLASTrr AESENCrr
AND16mi AND16mr AND32i32 AND32mi8 AND32mr AND32ri AND32ri8 AND32rm AND32rr AND64mi8_
↪AND64mr AND64ri8 AND64rr AND8mi AND8mr AND8ri AND8rm AND8rr ANDNPDrr ANDPDrm ANDPDrr
BSWAP32r BSWAP64r BT64rr
CALL64m CALL64pcrel32 CALL64r
CDQ CDQE
CMOV32rm CMOV32rr CMOV64rm CMOV64rr
CMP16mi8 CMP16mr CMP16rm CMP16rr CMP32i32 CMP32mi CMP32mi8 CMP32mr CMP32ri CMP32ri8_
↪CMP32rm CMP32rr CMP64i32 CMP64mi32 CMP64mi8 CMP64mr CMP64ri32 CMP64ri8 CMP64rm CMP64rr_
↪CMP8i8 CMP8mi CMP8mr CMP8ri CMP8rm CMP8rr
CMPSB
CMPSDrr_Int
CMPXCHG32rm CMPXCHG64rm
COMISDrm COMISDrr
CQO
CVTSI2SDrr_Int CVTSI642SDrm_Int CVTSI642SDrr_Int CVTTSD2SI64rr_Int CVTTSD2SIrr_Int
DEC32m DEC32r
DIV32r DIV64m DIV64r DIVSDrm_Int DIVSDrr_Int
IDIV32m IDIV32r IDIV64r
IMUL32r IMUL32rm IMUL32rr IMUL64mi8 IMUL64rr IMUL64rri32
JCC_1 JCC_4
JMP64m JMP64r
JMP_1 JMP_4
LEA64_32r LEA64r
MFENCE
MOV16mi MOV16mr MOV32mi MOV32mr MOV32ri MOV32rm MOV32rr MOV64mi32 MOV64mr MOV64ri_
↪MOV64ri32 MOV64rm MOV64rr MOV8mi MOV8mr
MOVAPDrr MOVAPSmr
MOVDQArm MOVDQArr
MOVDQUmr MOVDQUrm
MOVQI2PQIrm
MOVSDmr MOVSDrm
MOVSL MOVSQ
MOVSX32rm8 MOVSX32rr8 MOVSX64rm32 MOVSX64rm8 MOVSX64rr16 MOVSX64rr32 MOVSX64rr8
MOVUPSmr MOVUPSmr
MOVZX32rm16 MOVZX32rm8 MOVZX32rr16 MOVZX32rr8
MUL32r MUL64r MULSDrr_Int
NEG32r NEG64r
NOOP NOOP NOOPW
NOT32r NOT64m NOT64r
OR16rm OR32i32 OR32mi OR32mi8 OR32mr OR32ri OR32ri8 OR32rm OR32rr OR64i32 OR64ri8 OR64rm_
↪OR64rr OR8i8 OR8mi OR8mr OR8ri OR8rm OR8rr
ORPDrr
POP64r
PSHUFBrr PSHUFDri
PSLLDQri PSLLDri
PUSH64i8 PUSH64r PUSH64rmm

```

(continues on next page)

(continued from previous page)

```

PXORrr
RETQ
ROL32r1 ROL32ri ROL64r1 ROL64ri
ROR32ri ROR64r1 ROR64ri
ROUNDSDr_Int
SAR32r1 SAR32rCL SAR32ri SAR64r1 SAR64ri
SBB32ri8 SBB32rr SBB64ri8 SBB64rr SBB8i8 SBB8ri
SCASB
SETCCm SETCCr
SHL32rCL SHL32ri SHL64rCL SHL64ri
SHR16ri SHR32r1 SHR32rCL SHR32ri SHR64r1 SHR64rCL SHR64ri SHR8r1 SHR8ri
STOSQ
SUB32mi8 SUB32mr SUB32ri SUB32ri8 SUB32rm SUB32rr SUB64mi8 SUB64mr SUB64ri32 SUB64ri8
↳ SUB64rm SUB64rr SUB8mr SUBSDrm_Int SUBSDrr_Int
SYSCALL
TEST16mi TEST16ri TEST16rr TEST32i32 TEST32mi TEST32mr TEST32ri TEST32rr TEST64ri32
↳ TEST64rr TEST8i8 TEST8mi TEST8ri TEST8rr
UCOMISDrr
VADDSDrm_Int VADDSDrr_Int
VANDPDrr
VCOMISDrr
VFMADD132SDm_Int VFMADD132SDr_Int VFMADD213SDm_Int VFMADD231SDr_Int
VFNMADD231SDm_Int
VMOVAPDrr
VMOVPI2DIrr
VMOVQIto64rr
VMOVQI2PQIrm
VMOVSDrm
VMULSDrm_Int VMULSDrr_Int
VSTMXCSR
VSUBSDrm_Int VSUBSDrr_Int
VUCOMISDrm VUCOMISDrr
VXORPDrr
XADD32rm
XCHG32rm XCHG64rr
XOR32ri XOR32ri8 XOR32rm XOR32rr XOR64rm XOR64rr XOR8rm
XORPSrr

```

## 2.6.2 Intel x86

The x86 support is based on x86\_64 and has the same limitations. However, its integration is more recent than X86\_64 and has less been tested.

## Instruction Coverage

```

ABS_F
ADC32mi8 ADC32mr ADC32ri ADC32ri8 ADC32rm ADC32rr
ADD16mi8 ADD16mr ADD16ri ADD16rm ADD32i32 ADD32mi ADD32mi8 ADD32mr ADD32ri ADD32ri8_
↪ADD32rm ADD32rr ADD8rr
ADD_F32m ADD_FPrST0 ADD_FrST0
AESENCLASTr AESENCrr
AND16mi AND16mr AND32i32 AND32mi8 AND32mr AND32ri AND32ri8 AND32rm AND32rr AND8mi AND8mr_
↪AND8ri AND8rm AND8rr
BSWAP32r
BT32rr
CALL32m CALL32r CALLpcrel32
CDQ
CHS_F
CLD
CMOV32rm CMOV32rr
CMOVE_F
CMP16mi8 CMP16mr CMP16rm CMP32i32 CMP32mi CMP32mi8 CMP32mr CMP32ri CMP32ri8 CMP32rm_
↪CMP32rr CMP8i8 CMP8mi CMP8mr CMP8ri CMP8rm CMP8rr
CMPSB CMPSW
CMPXCHG32rm
COM_FIPr
COM_FIr
DEC32r_alt
DIV32m DIV32r
DIVR_F32m DIVR_F64m
DIV_F32m DIV_F64m
DIV_FPrST0
FCOMP64m
FLDCW16m
FLDENVm
FNSTCW16m FNSTSW16r
FRNDINT
FSTENVm
FXAM
IDIV32m
ILD_F32m ILD_F64m
IMUL32r IMUL32rm IMUL32rmi8 IMUL32rr IMUL32rri
INC32r_alt
IST_FP32m IST_FP64m
JCC_1 JCC_4
JMP32m JMP32r
JMP_1 JMP_4
LD_F0 LD_F1 LD_F32m LD_F64m LD_F80m LD_Frr
LEA32r
MOV16mi MOV16mr MOV16rm MOV32ao32 MOV32mi MOV32mr MOV32o32a MOV32ri MOV32rm MOV32rr_
↪MOV8mi MOV8mr MOV8rm MOV8rr
MOVAPSrr
MOVDQArm MOVDQArr
MOVDQUmr
MOVSB MOVSL
MOVSX32rm8 MOVSX32rr16 MOVSX32rr8

```

(continues on next page)

(continued from previous page)

```

MOVUPSmr MOVUPSmr
MOVZX32rm16 MOVZX32rm8 MOVZX32rr16 MOVZX32rr8
MUL32m MUL32r
MUL_F32m MUL_FPrST0 MUL_FST0r
NEG32r
NOOP
NOT32m NOT32r
OR16ri OR16rm OR32i32 OR32mi OR32mi8 OR32mr OR32ri OR32ri8 OR32rm OR32rr OR8i8 OR8mi
↳OR8mr OR8ri OR8rm OR8rr
POP32r
PSHUFBrr PSHUFDri
PSLLDQri PSLLDri
PUSH32i8 PUSH32r PUSH32rmm PUSHi32
PXORrr
RETL
ROL32r1 ROL32rCL ROL32ri
ROR32ri
SAHF
SAR32r1 SAR32rCL SAR32ri
SBB32mi8 SBB32ri8 SBB32rm SBB32rr SBB8i8 SBB8ri
SCASB
SETCCm SETCCr
SHL32rCL SHL32ri
SHLD32rrCL SHLD32rri8
SHR16ri SHR32r1 SHR32rCL SHR32ri SHR8m1 SHR8ri
SHRD32rri8
STOSL
ST_F64m ST_FP64m ST_FP80m ST_FPrr
SUB32i32 SUB32mi8 SUB32mr SUB32ri SUB32ri8 SUB32rm SUB32rr SUB8mr SUB8ri SUB8rm
SUBR_F64m SUBR_FPrST0
SUB_FPrST0 SUB_FrST0
TEST16mi TEST16ri TEST16rr TEST32i32 TEST32mi TEST32mr TEST32ri TEST32rr TEST8i8 TEST8mi
↳TEST8mr TEST8ri TEST8rr
UCOM_FIr UCOM_FPr
XADD32rm
XCHG32ar XCHG32rm XCHG32rr
XCH_F
XOR16rr XOR32i32 XOR32mr XOR32ri XOR32ri8 XOR32rm XOR32rr XOR8rm
XORPSrr

```

## 2.7 Developer Documentation

### 2.7.1 Compilation From Source

To build this project, the following dependencies are needed on your system:

- cmake >= 3.12
- ninja or make
- C++17 toolchain (gcc, clang, Visual Studio 2019, ...)

The compilation is a two-step process:

- local library distribution of LLVM is built.
- QBDI is built using the LLVM library.

This local built of LLVM is required because QBDI uses private APIs not exported by regular LLVM installations and because our code is only compatible with a specific version of those APIs. This first step is cached and only needs to be run once, subsequent builds only need to repeat the second step.

QBDI build system relies on CMake and requires to pass build configuration flags. To help with this step we provide shell scripts for common build configurations which follow the naming pattern `config-OS-ARCH.sh`. Modifying these scripts is necessary if you want to compile in debug mode or cross-compile QBDI.

## Linux

### x86-64

Create a new directory at the root of the source tree, and execute the Linux configuration script:

```
mkdir build
cd build
../cmake/config/config-linux-X86_64.sh
ninja
```

### x86

You can follow the same instructions as for x86-64 but instead, use the `config-linux-X86.sh` configuration script.

## macOS

Compiling QBDI on macOS requires a few things:

- A modern version of **macOS** (like Sierra)
- **Xcode** (from the *App Store* or *Apple Developer Tools*)
- the **Command Line Tools** (`xcode-select --install`)
- a package manager (preferably **MacPorts**, but *HomeBrew* should also be fine)
- some packages (`port install cmake wget ninja`)

Once requirements are met, create a new directory at the root of the source tree, and execute the macOS configuration script:

```
mkdir build
cd build
../cmake/config/config-macOS-X86_64.sh
ninja
```

## Windows

Building on Windows requires a pure Windows installation of *Python 3* (from the official packages, this is mandatory) in order to build our dependencies (we really hope to improve this in the future). It also requires an up-to-date CMake and Ninja.

First of all, the Visual Studio environment must be set up. This can be done with a command such as:

```
"C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\VC\Auxiliary\Build\  
↪vcvarsall.bat" x64
```

Then, the following commands must be run:

```
mkdir build  
cd build  
python ../cmake/config/config-win-X86_64.py  
ninja
```

## Android

Cross-compiling for Android requires the NDK (or the SDK) to be installed on your workstation. For now, it has only been tested under Linux. If not already installed, you can download the latest Android NDK package through the [official website](#) and extract it. Afterwards, the `config-android-*.sh` configuration script needs to be customised to match your NDK installation directory and the target platform.:

```
# Configure and compile QBDI X86_64 with a NDK  
mkdir build && cd build  
NDK_PATH=<your_NDK_PATH> ../cmake/config/config-android-X86_64.sh  
ninja  
  
# Configure and compile QBDI X86 with a SDK  
mkdir build && cd build  
ANDROID_SDK_ROOT=<your_SDK_PATH> ../cmake/config/config-android-X86.sh  
ninja
```

## PyQBDI compilation

The PyQBDI library (apart from the wheel package) can be built by solely passing the ‘**-DQBDI\_TOOLS\_PYQBDI=ON**’ option to the CMake build system.

However, if you want to build the wheel package, you can run these commands:

```
python -m pip install --upgrade pip  
python -m pip install setuptools wheel  
python setup.py bdist_wheel
```

A 32-bit version of Python is mandatory for the X86 architecture whereas a 64-bit one is required for the X86-64 architecture.



## CMake Parameters

The compilation of QBDI can be configured with the command line. Each parameter should be placed on the command line with the form `-D<param>=<value>`.

- `QBDI_PLATFORM` (mandatory) : Target platform of the compilation (supported: windows, linux, android, osx)
- `QBDI_ARCH` (mandatory) : Target architecture of the compilation (supported: X86\_64, X86)
- `QBDI_CCACHE` (default ON) : enable compilation optimisation with ccache or sccache.
- `QBDI_DISABLE_AVX` (default OFF) : disable the support of AVX instruction on X86 and X86\_64
- `QBDI_ASAN` (default OFF) : compile with ASAN to detect memory leak in QBDI.
- `QBDI_LOG_DEBUG` (default OFF) : enable the debug level of the logging system. Note that the support of this level has an impact on the performances, even if this log level is not enabled.
- `QBDI_STATIC_LIBRARY` (default ON) : build the static library of QBDI. Note than some subproject need `QBDI_STATIC_LIBRARY` (test, PyQBDI, ...)
- `QBDI_SHARED_LIBRARY` (default ON) : build the shared library of QBDI. Note than some subproject need `QBDI_SHARED_LIBRARY` (Frida/QBDI, examples, ...)
- `QBDI_TEST` (default ON) : build the tests suite
- `QBDI_BENCHMARK` (default OFF) : build the benchmark tools
- `QBDI_TOOLS_QBDIPRELOAD` (default ON on supported platform) : build QBDIPreload static library (supported on Linux and OSX).
- `QBDI_TOOLS_VALIDATOR` (default ON on supported platform) : build the validator library (supported on Linux and OSX).
- `QBDI_TOOLS_PYQBDI` (default ON on X86\_64) : build PyQBDI library. Supported on Linux, Windows and OSX.
- `QBDI_TOOLS_FRIDAQBDI` (default ON) : add Frida/QBDI in the package.

## 2.7.2 Repository Organization

### Root Tree

The root of the source tree is organized as follows:

**cmake/** Contains files required by the CMake build system.

**docker/** Contains the Dockerfile for the docker image and the CI.

**docs/** Contains this documentation source and configuration.

**examples/** Contains various QBDI usage examples.

**include/** Contains the public include files.

**package/** Contains the package generation scripts.

**src/** Contains QBDI source code. This tree is described further in section [Source Tree](#).

**templates/** Contains QBDI usage templates.

**test/** Contains the functional test suite.

**third-party/** Contains the third party dependency downloaded by cmake.

**tools/** Contains QBDI development tools: the validator and the validation runner.

## Source Tree

The source files are organized as follows:

**src/Engine** Contains code related to the VM API and underlying Engine controlling the overall execution.

**src/ExecBlock** Contains code used to generate, store and execute JITed code inside ExecBlocks which form a code cache managed by the ExecBlockManager.

**src/ExecBroker** Contains code implementing the execution brokering mechanism allowing to switch between instrumented execution and real execution.

**src/Patch** Contains the PatchDSL implementation and per architecture support.

**src/Utility** Contains various utility class and functions.

## 2.7.3 Testing

Making mistakes while writing a DBI framework is particularly easy and often fatal. Executing code generated at runtime is a dangerous game and close attention should be paid to the patching engine. That is why we use two different testing methods.

### Functional Test Suite

QBDI has a small functional test suite implemented using [Catch2](#) which verifies the essential functions of QBDI. This test suite is automatically built and made available in the `test/` build subdirectory:

```
$ ./test/QBDITest
=====
All tests passed (110977 assertions in 106 test cases)
```

### Validator

The validator is a generic test system allowing to compare a normal execution with an instrumented execution. This way a large number of programs can be used as a test suite to ensure that QBDI does not alter their normal functions. It is only compatible with Linux and macOS at the moment.

The idea is to pilot a debugging session using an instrumented execution of the same program. These two instances share the same environment and arguments and originated from the same fork thus have the same memory layout. This allows to compare the program state at each step and verify that both execution take the same path and give the same result. The validator is not only capable of determining if two executions differ but also capable of identifying where they diverged. It thus double down as a debugging tool.

There is, however, a few caveats to this approach. First, the two instances of the program will compete for resources. This means running `shasum test.txt` will work because the two instances can read the same file at the same time, but removing a directory `rmdir testdir/` will always fail because only one instance will be able to delete the directory. Second, the dynamic memory allocations will not match on the two instances. This is because the instrumented instance is running the whole QBDI framework and validator instrumentation which is making extra allocations in between the original program allocations. A partial mitigation was nevertheless implemented which tracks allocations on both sides and compute an allowed offset for specific memory address ranges.

One of the essential concepts of the validator are error cascades. They establish a probable causality chain between errors and allow to backtrack from the point where the execution crashed or diverged to the probable cause. Indeed, an error might only cause problems thousands of instructions later.

The validator uses dynamic library injection to take control of a program startup. Options are communicated using environment variables. The following options are available:

#### **VALIDATOR\_VERBOSITY**

- **Stat:** Only display execution statistics. This is the default.
- **Summary:** Display execution statistics and error cascade summaries.
- **Detail:** Display execution statistics and complete error cascades.
- **Full:** Display full execution trace, execution statistics and complete error cascades.

**VALIDATOR\_COVERAGE** Specify a file name where instruction coverage statistics will be written out.

## **Linux**

The validator uses LD\_PRELOAD for injection under Linux and an example command line would be:

```
$ LD_PRELOAD=./tools/validator/libvalidator.so VALIDATOR_VERBOSITY=Detail VALIDATOR_
↪ COVERAGE=coverage.txt ls
```

## **macOS**

The validator uses DYLD\_INSERT\_LIBRARIES for injection under macOS and an example command line would be:

```
$ DYLD_INSERT_LIBRARIES=./tools/validator/libvalidator.dylib VALIDATOR_VERBOSITY=Detail_
↪ VALIDATOR_COVERAGE=coverage.txt ./ls
```

Please note that, under macOS, SIP prevents from debugging system binaries. A workaround is to copy the target binary in a local directory. Also, for the moment, the validator requires root to obtain debugging rights.

## **Validation Runner**

The validation runner is an automation system to run a series of validation task specified in a configuration file and aggregate the results. Those results are stored in a database which enables to perform historical comparison between validation runs and warns in case of an anomaly.

## **2.7.4 Technical Reference**

### **Instrumentation Process**

#### **Introduction**

The Engine reads and disassembles the instrumented binary basic block per basic block. In case a conditional branch terminates a basic block, the execution result of this basic block is needed to determine the next basic block to execute. This makes the case for a per basic block processing and execution.

Every basic block is first patched to solve two main problems:

- **Relocation:** The basic block will be executed at a different location and thus every usage of the Program Counter, either directly as an operand or indirectly when using relative memory addressing, needs to be patched to make the code relocatable.
- **Control Flow Control:** Branching instructions should not be directly executed as this would result in the execution escaping from the instrumentation process. Thus the resulting target of a branching instruction needs to be computed without being taken.

Once a basic block has been patched, the instrumentations requested by the user code are applied. Both the patching and the instrumentation are expressed in an *Embedded Domain Specific Language*<sup>1</sup> called *PatchDSL* which is executed by the engine.

The resulting instrumented basic block is then handed over to the `ExecBlockManager` which handles a cache of basic blocks placed inside execution units called *ExecBlock*. The `ExecBlockManager` is tasked with finding memory space inside an `ExecBlock` to place the instrumented basic block and also retrieving cached basic blocks.

An `ExecBlock` manages on the guest side two memory pages: one for the code, the code block, and one for the data, the data block. The `ExecBlock` also handles the resolution of the relocation of the patched code before assembling it in the code block.

The instrumentation of the code allows to make callbacks to the user code directly from the instrumented binary through the `ExecBlock`. These callbacks allow to inspect and modify the state of execution of the guest on the host side at every point in time.

## Implementation

The figure below presents the *life of an instruction* and summarizes the main steps and classes involved along the way. This is intended to give an overview of what the internals do.

An instruction exists in three different representations inside QBDI:

**Bytes** Raw bytes of machine code in memory.

**MCInst** LLVM machine code representation. The instruction is only partially disassembled but still provides a list of operands. One interested in more details regarding this representation should refer to the official LLVM documentation and experiment with `llvm-mc -show-inst`.

**RelocatableInst** QBDI representation of a relocatable `MCInst`. It consists in an `MCInst` and relocation information.

There is another important class: `QBDI::Patch`. A `QBDI::Patch` aggregates the patch and the instrumentation of a single instruction in the form of a list of `QBDI::RelocatableInst`. It is the smallest unit of code which can be assembled inside an *QBDI::ExecBlock* as patching or instrumentation code cannot be split in parts without problematic side effects.

The assembly and disassembly steps are directly handled by LLVM for us. The Engine takes care of the patching and instrumentation using a programmable list of *QBDI::PatchRule* and *QBDI::InstrRule*. More details on those rules can be found in the *PatchDSL* chapter. Relocation is handled directly in the *QBDI::ExecBlock*.

---

<sup>1</sup> [https://en.wikipedia.org/wiki/Domain-specific\\_language](https://en.wikipedia.org/wiki/Domain-specific_language)

## ExecBlock

### Introduction

The ExecBlock is a concept which tries to simplify the problem of context switching between the host and the guest.

The main problem behind context switching is to be able to reference a memory location owned by the host in the context of the guest. Loading the memory location in a register effectively destroys a guest value which would thus need to be saved somewhere. One could allow the usage of the guest stack and save values on it but this design has two major drawbacks. Firstly, although supposedly unused, this modifies guest memory and could have side effects if the program uses uninitialized stack values or in the case of unforeseen optimizations. Secondly, this assumes that the stack registers always point on the stack or that a stack exists at all which might not be the case for more exotic languages or assembly code. The only possible mechanism left is to use relative addressing load and store. While x86 and x86-64 allow 32 bits offset, ARM only allows 11 bits offset<sup>1</sup>. The ExecBlock design thus only requires to be able to load and store general purpose registers with an address offset up to 4096 bytes.

---

**Note:** By default, AVX registers are also saved, one may want to disable this in case where it is not necessary, thus improving performances. It can be achieved using the environment flag `QBDI_FORCE_DISABLE_AVX`.

---

Some modern operating systems do not allow the allocation of memory pages with read, write and execute permissions (RWX) for security reasons as this greatly facilitates remote code execution exploits. It is thus necessary to allocate two separate pages, with different permissions, for code and data. By exploiting the fact that most architectures use memory pages of 4096 bytes<sup>2</sup>, allocating a data memory page next to a code memory page would allow the first instruction to address at least the first address of the data memory page.

### Memory Layout

An ExecBlock is thus composed of two contiguous memory pages: the first one is called the code block and has read and execute permissions (RX) and the second one is called the data block and has read and write permissions (RW). The code block contains a prologue, responsible for the host to guest context switching, followed by the code of the translated basic block and finally the epilogue responsible for the guest to host switching. Both the prologue and the epilogue use the beginning of the data block to store the context data. The context is split in three parts: the GPR context, the FPR context and the host context. The GPR and FPR context are straight forward and documented in the API itself as the `GPRState` and `FPRState` (see the State Management part of the API). The host context is used to store host data and a memory pointer called the selector. The selector is used by the prologue to determine on which basic block to jump next. The remaining space in the data block is used for shadows which can be used to store any data needed by the patching or instrumentation process.

---

<sup>1</sup> Thumb supports even less but this is not a problem as, with the exception of embedded ARM architectures (the Cortex-M series), one can always switch between ARM mode and Thumb mode.

<sup>2</sup> This is at least true for x86, x86\_64, ARM, ARM64 and PowerPC.

## Reference

class QBDI::ExecBlock

Manages the concept of an exec block made of two contiguous memory blocks (one for the code, the other for the data) used to store and execute instrumented basic blocks.

### Public Functions

**ExecBlock**(const LLVMCPUs &llvmCPUs, *VMInstanceRef* vminstance = nullptr, const std::vector<std::unique\_ptr<RelocatableInst>> \*execBlockPrologue = nullptr, const std::vector<std::unique\_ptr<RelocatableInst>> \*execBlockEpilogue = nullptr, uint32\_t epilogueSize = 0)

Construct a new *ExecBlock*

#### Parameters

- **llvmCPUs** – [in] LLVMCPU used to assemble instructions in the *ExecBlock*.
- **vminstance** – [in] Pointer to public engine interface
- **execBlockPrologue** – [in] cached prologue of ExecManager
- **execBlockEpilogue** – [in] cached epilogue of ExecManager
- **epilogueSize** – [in] size in bytes of the epilogue (0 is not know)

void **changeVMInstanceRef**(*VMInstanceRef* vminstance)

Change vminstance when *VM* object is moved

void **show**() const

Display the content of an exec block to stderr.

*VMAction* **execute**()

Execute the sequence currently programmed in the selector of the exec block. Take care of the callbacks handling.

SeqWriteResult **writeSequence**(std::vector<Patch>::const\_iterator seqStart, std::vector<Patch>::const\_iterator seqEnd)

Write a new sequence in the exec block. This function does not guarantee that the sequence will be written in its entirety and might stop before the end using an architecture specific terminator. Return 0 if the exec block was full and no instruction was written.

#### Parameters

- **seqStart** – [in] Iterator to the start of a list of patches.
- **seqEnd** – [in] Iterator to the end of a list of patches.

**Returns** A structure detailing the write operation result.

uint16\_t **splitSequence**(uint16\_t instID)

Split an existing sequence at instruction instID to create a new sequence.

**Parameters** **instID** – [in] ID of the instruction where to split the sequence at.

**Returns** The new sequence ID.

inline *rword* **getDataBlockBase**() const

Get the address of the DataBlock

**Returns** The DataBlock offset.

inline *rword* **getDataBlockOffset**() const

Compute the offset between the current code stream position and the start of the data block. Used for pc relative memory access to the data block.

**Returns** The computed offset.

inline *rword* **getEpilogueOffset**() const

Compute the offset between the current code stream position and the start of the exec block epilogue code. Used for computing the remaining code space left or jumping to the exec block epilogue at the end of a sequence.

**Returns** The computed offset.

inline uint32\_t **getEpilogueSize**() const

Get the size of the epilogue

**Returns** The size of the epilogue.

inline *rword* **getCurrentPC**() const

Obtain the value of the PC where the *ExecBlock* is currently writing instructions.

**Returns** The PC value.

inline uint16\_t **getNextInstID**() const

Obtain the current instruction ID.

**Returns** The current instruction ID.

uint16\_t **getInstID**(*rword* address) const

Obtain the instruction ID for a specific address (the address must exactly match the start of the instruction).

**Parameters** **address** – The address of the start of the instruction.

**Returns** The instruction ID or NOT\_FOUND.

inline uint16\_t **getCurrentInstID**() const

Obtain the current instruction ID.

**Returns** The ID of the current instruction.

const InstMetadata &**getInstMetadata**(uint16\_t instID) const

Obtain the instruction metadata for a specific instruction ID.

**Parameters** **instID** – The instruction ID.

**Returns** The metadata of the instruction.

*rword* **getInstAddress**(uint16\_t instID) const

Obtain the instruction address for a specific instruction ID.

**Parameters** **instID** – The instruction ID.

**Returns** The real address of the instruction.

*rword* **getInstInstrumentedAddress**(uint16\_t instID) const

Obtain the instrumented address for a specific instruction ID.

**Parameters** **instID** – The instruction ID.

**Returns** The address in the BasicBlock of the instruction.

const llvm::MCInst &**getOriginalMCInst**(uint16\_t instID) const

Obtain the original MCInst for a specific instruction ID.

**Parameters** **instID** – The instruction ID.

**Returns** The original MCInst of the instruction.

const *InstAnalysis* \***getInstAnalysis**(uint16\_t instID, *AnalysisType* type) const

Obtain the analysis of an instruction. Analysis results are cached in the *InstAnalysis*. The validity of the returned pointer is only guaranteed until the end of the callback, else a deepcopy of the structure is required.

**Parameters**

- **instID** – [in] The ID of the instruction to analyse.
- **type** – [in] Properties to retrieve during analysis.

**Returns** A *InstAnalysis* structure containing the analysis result.

inline uint16\_t **getNextSeqID**() const

Obtain the next sequence ID.

**Returns** The next sequence ID.

uint16\_t **getSeqID**(*rword* address) const

Obtain the sequence ID for a specific address (the address must exactly match the start of the sequence).

**Parameters** **address** – The address of the start of the sequence.

**Returns** The sequence ID or NOT\_FOUND.

uint16\_t **getSeqID**(uint16\_t instID) const

Obtain the sequence ID containing a specific instruction ID.

**Parameters** **instID** – The instruction ID.

**Returns** The sequence ID or NOT\_FOUND.

inline uint16\_t **getCurrentSeqID**() const

Obtain the current sequence ID.

**Returns** The ID of the current sequence.

uint16\_t **getSeqStart**(uint16\_t seqID) const

Obtain the sequence start address for a specific sequence ID.

**Parameters** **seqID** – The sequence ID.

**Returns** The start address of the sequence.

uint16\_t **getSeqEnd**(uint16\_t seqID) const

Obtain the instruction id of the sequence end address for a specific sequence ID.

**Parameters** **seqID** – The sequence ID.

**Returns** The end address of the sequence.

void **selectSeq**(uint16\_t seqID)

Set the selector of the exec block to a specific sequence offset. Used to program the execution of a specific sequence within the exec block.

**Parameters** **seqID** – [in] Basic block ID within the exec block.

inline Context \***getContext**() const

Get a pointer to the context structure stored in the data block.

**Returns** The context pointer.

uint16\_t **newShadow**(uint16\_t tag = ShadowReservedTag::Untagged)

Allocate a new shadow within the data block. Used by relocation to load or store data from the instrumented code.

**Parameters** **tag** – The tag associated with the registration, 0xFFFF is reserved for unregistered shadows.



**Returns** The shadow id (which is its index within the shadow array).

uint16\_t **getLastShadow**(uint16\_t tag)

Search the last *Shadow* with the tag for the current instruction. Used by relocation to load or store data from the instrumented code.

**Parameters** **tag** – The tag associated with the registration

**Returns** The shadow id (which is its index within the shadow array).

void **setShadow**(uint16\_t id, *rword* v)

Set the value of a shadow.

**Parameters**

- **id** – [in] ID of the shadow to set.
- **v** – [in] Value to assigne to the shadow.

*rword* **getShadow**(uint16\_t id) const

Get the value of a shadow.

**Parameters** **id** – [in] ID of the shadow.

**Returns** Value of the shadow.

*rword* **getShadowOffset**(uint16\_t id) const

Get the offset of a shadow within the data block.

**Parameters** **id** – [in] ID of the shadow.

**Returns** *Offset* of the shadow.

## PatchDSL

### Contents

- *PatchDSL*
  - *Language Concepts*
    - \* *Type System*
    - \* *Statements*
    - \* *Rules*
    - \* *Transforms*
  - *PatchDSL Examples*
    - \* *Basic Patching*
    - \* *Advanced Patching*
    - \* *Instrumentation Callbacks*
    - \* *Inline Instrumentation*
  - *PatchDSL Reference*
    - \* *PatchConditions*
    - \* *PatchGenerators*

\* *InstTransform*

## Language Concepts

### Type System

The PatchDSL nomenclature is formalized in function of where information belongs using two dichotomies:

- A physical dichotomy is made between data stored in the machine registers and data stored in memory.
- A conceptual dichotomy is made between data belonging or generated by the target program and data belonging or generated by QBDI.

This creates four main categories of data being manipulated by the PatchDSL. These categories and the nomenclature for their interaction are represented below.

**Reg:** They represent machine registers storing data created and used by the target program.

**Temp:** They represent machine registers storing data used by the instrumentation. Those are temporary scratch registers which were allocated by saving a Reg into the context and are bound to be deallocated by restoring the Reg value from the context.

**Context:** The context stores in memory the processor state associated with the target program. It is mostly used for context switching between the target program and the instrumentation process and also for allocating temporary registers.

**Shadows:** They represent shadow data associated with a patch and instrumented instruction. They can be used by QBDI to store constants or Tagged Shadows.

**Metadata:** Any data regarding the execution which can be generated by QBDI. For examples obtaining instruction operand values or memory access addresses.

The main objective of this strict naming convention is to make the distinction between pure (no side effects) operations and operations affecting the program state as clear as possible. To make this distinction even more apparent the DSL is strongly typed forcing variables to be declared by allocating one of the typed structures below with its constructor. Because some of those structures simply alias an integer value it can be tempting to directly use the integer value, letting the compiler do the implicit type conversion. However the point of those structures is to give a context to what those integer constants represent and the best practice is to use them everywhere possible.

struct QBDI::Reg

Structure representing a register variable in PatchDSL.

### Public Functions

inline **Reg**(unsigned int id)

Create a new register variable.

**Parameters** **id** – [in] The id of the register to represent.

inline **operator unsigned int**() const

Convert this structure to an LLVM register id.

**Returns** LLVM register id.

inline unsigned int **getID**() const

Get back the id of the register in GPRState

**Returns** GPRState register id.

inline *rword* **offset**() const

Return the offset of this register storage in the context part of the data block.

**Returns** The offset.

struct QBDI::Temp

Structure representing a temporary register variable in PatchDSL.

### Public Functions

inline **Temp**(unsigned int id)

Represent a temporary register variable identified by a unique ID. Inside a patch rules or a instrumentation rules, *Temp* with identical ids point to the same physical register. The id 0xFFFFFFFF is reserved for internal uses. The mapping from id to physical register is determined at generation time and the allocation and deallocation instructions are automatically added to the patch.

**Parameters** **id** – [in] The id of the temp to represent.

inline **operator unsigned int**() const

Convert this *Temp* to its id.

**Returns** This *Temp* id.

struct QBDI::Shadow

Structure representing a shadow variable in PatchDSL.

### Public Functions

inline **Shadow**(uint16\_t tag)

Allocate a new shadow variable in the data block with the corresponding tag.

**Parameters** **tag** – [in] The tag of the new shadow variable.

inline *rword* **getTag**() const

Return the tag associated with this shadow variable.

**Returns** The tag of the shadow variable.

struct QBDI::Constant

Structure representing a constant value in PatchDSL.

### Public Functions

inline **Constant**(*rword* v)

Represent a constant value.

**Parameters** **v** – [in] The represented value.

inline **operator rword**() const

Convert this structure to its value.

**Returns** This constant value.

struct QBDI::Offset

Structure representing a memory offset variable in PatchDSL.

## Public Functions

inline **Offset**(int64\_t offset)

Allocate a new offset variable with its offset value.

**Parameters** *offset* – [in] The offset value

inline **Offset**(*Reg* reg)

Allocate a new offset variable with the offset in the context of a specific register.

**Parameters** *reg* – [in] The register whose offset to represent.

inline **operator** int64\_t() const

Convert this structure to its value.

**Returns** This offset value.

struct QBDI::Operand

Structure representing an operand instruction variable in PatchDSL.

## Public Functions

inline **Operand**(unsigned int idx)

Represent an operand instruction identified by its index in the LLVM MCInst representation of the instruction.

**Parameters** *idx* – [in] The operand index.

inline **operator** unsigned int() const

Convert this *Operand* to its idx.

**Returns** This *Operand* idx.

## Statements

There are three main categories of statements composing PatchDSL, each characterized by a different virtual base classes. The specialization of those base classes are PatchDSL statements.

**QBDI::PatchCondition** They are used to match specific instructions. They take the instruction and its context as an input and return a boolean.

**QBDI::PatchGenerator** They represent operations generating new instructions. They take the instruction and its context as an input and return a list of QBDI::RelocatableInst constituting the patch. In some exceptional cases no output is generated.

**QBDI::InstTransform** They represent operations transforming an instruction. They only manipulate an instruction and need to be used with a QBDI::PatchGenerator to output a QBDI::RelocatableInst.

Those statements are all evaluated on an implicit context. In the case of QBDI::InstTransform the context is the instruction to modify which is determined by the QBDI::PatchGenerator which use it. In the case of QBDI::PatchCondition and QBDI::PatchGenerator this context is made of:

- the current instruction
- the current instruction size
- the current address

The output of each statement thus depends on the statement parameters and this implicit context.

## Rules

PatchDSL is used to write short sequence of statements called *rules*. There exists two variants of rules, patching rules (*QBDI::PatchRule*) and instrumentation rules (*QBDI::InstrRule*), but they both relies on the same principle. A rule is composed of two parts:

**Condition:** A *QBDI::PatchCondition* statement which express the condition under which the rule should be applied. Multiple statements can be combined in a boolean expression using *QBDI::Or* and *QBDI::And*. If the evaluation of this expression returns **true** then the generation part of the rule is evaluated.

**Generation:** A list of *QBDI::PatchGenerator* statements which will generate the patch rule. Each statement can output one or several *QBDI::RelocatableInst*, the resulting patch being the aggregation of all those statement outputs.

class *QBDI::PatchRule*

A patch rule written in PatchDSL.

### Public Functions

**PatchRule**(std::unique\_ptr<PatchCondition> &&condition, std::vector<std::unique\_ptr<PatchGenerator>> &&generators)

Allocate a new patch rule with a condition and a list of generators.

#### Parameters

- **condition** – [in] A *PatchCondition* which determine wheter or not this *PatchRule* applies.
- **generators** – [in] A vector of *PatchGenerator* which will produce the patch instructions.

bool **canBeApplied**(const llvm::MCInst &inst, *rword* address, *rword* instSize, const LLVMCPU &llvmcpu) const

Determine wheter this rule applies by evaluating this rule condition on the current context.

#### Parameters

- **inst** – [in] The current instruction.
- **address** – [in] The current instruction address.
- **instSize** – [in] The current instruction size.
- **llvmcpu** – [in] LLVMCPU object

**Returns** True if this patch condition evaluate to true on this context.

Patch **generate**(const llvm::MCInst &inst, *rword* address, *rword* instSize, const LLVMCPU &llvmcpu, Patch \*toMerge = nullptr) const

Generate this rule output patch by evaluating its generators on the current context. Also handles the temporary register management for this patch.

#### Parameters

- **inst** – [in] The current instruction.
- **address** – [in] The current instruction address.
- **instSize** – [in] The current instruction size.
- **llvmcpu** – [in] LLVMCPU object
- **toMerge** – [in] An eventual previous patch which is to be merged with the current instruction. The patch is empty after the merge.

**Returns** A Patch which is composed of the input context and a series of RelocatableInst.

class QBDI::InstrRule

An instrumentation rule written in PatchDSL.

Subclassed by QBDI::AutoUnique< InstrRule, InstrRuleBasicCBK >, QBDI::AutoUnique< InstrRule, InstrRuleDynamic >

## Public Functions

virtual bool **tryInstrument**(Patch &patch, const LLVMCPU &llvmcpu) const = 0

Determine whether this rule has to be applied on this Path and instrument if needed.

### Parameters

- **patch** – [in] The current patch to instrument.
- **llvmcpu** – [in] LLVMCPU object

void **instrument**(Patch &patch, const PatchGeneratorUniquePtrVec &patchGen, bool breakToHost, *InstPosition* position, int priority, RelocatableInstTag tag) const

Instrument a patch by evaluating its generators on the current context. Also handles the temporary register management for this patch.

### Parameters

- **patch** – [in] The current patch to instrument.
- **patchGen** – [in] The list of patchGenerator to apply
- **breakToHost** – [in] Add a break to *VM* need to be added after the patch
- **position** – [in] Add the patch before or after the instruction
- **priority** – [in] The priority of this patch
- **tag** – [in] The tag for this patch

## Transforms

Transform statements, with the QBDI::InstTransform virtual base class, are a bit more subtle than other statements.

Currently their operation is limited to the QBDI::ModifyInstruction generators which always operate on the instruction of the implicit context of a patch or instrumentation rule. However their usage could be extended in the future.

Their purpose is to allow to write more generic rules by allowing modifications which can operate on a class of instructions. Using instruction transforms requires to understand the underlying LLVM MCInst representation of an instruction and `llvm-mc -show-inst` is a helpful tool for this task.

## PatchDSL Examples

Below some real examples of patch and instrumentation rules are shown.

### Basic Patching

#### Generic PC Substitution Patch Rule

Instructions using the Program Counter (PC) in their computations are problematic because QBDI will reassemble and execute the code at another address than the original code location and thus the value of the PC will change. This kind of computation using the PC is often found when using relative memory addressing.

Some cases can be more difficult to handle, but most of these instructions can be patched using a very simple generic rule performing the following steps:

1. Allocate a scratch register by saving a register value in the context part of the data block.
2. Load the value the PC register should have, into the scratch register.
3. Perform the original instruction but with PC replaced by the scratch register.
4. Deallocate the scratch register by restoring the register value from context part of the data block.

The PatchDSL `QBDI::PatchRule` handles step 1 and 4 automatically for us. Expressing step 2 and 3 is relatively simple:

```
PatchRule(
  // Condition: Applies on every instruction using the register REG_PC
  UseReg(Reg(REG_PC)),
  // Generators: list of statements generating the patch
  {
    // Compute PC + 0 and store it in a new temp with id 0
    GetPCOffset(Temp(0), Constant(0)),
    // Modify the instruction by substituting REG_PC with the temp having id 0
    ModifyInstruction({
      SubstituteWithTemp(Reg(REG_PC), Temp(0))
    })
  }
)
```

This rule is generic and works under X86\_64 as well as ARM. Some more complex cases of instructions using PC need to be handled another way though.

#### Simple Branching Instruction Patch

Another simple case which needs to be handled using a patch rule is branching instructions. They cannot be executed because that would mean DBI process would lose the hand on the execution. Instead of executing the branch operation, the branch target is computed and used to overwrite the value of the PC in the context part of the data block. This is followed by a context switch back to the VM which will use this target as the address where to continue the execution.

The simplest cases are the “branch to an address stored in a register” instructions. Again the temporary register allocation is automatically taken care of by the `QBDI::PatchRule` and we only need to write the patching logic:

```

PatchRule(
    // Condition: only on BX or BX_pred LLVM MCInst
    Or({
        OpIs(llvm::ARM::BX),
        OpIs(llvm::ARM::BX_pred)
    }),
    // Generators
    {
        // Obtain the value of the operand with index 0 and store it in a new temp with
↪id 0
        GetOperand(Temp(0), Operand(0)),
        // Write the temp with id 0 at the offset in the data block of the context value
↪of REG_PC.
        WriteTemp(Temp(0), Offset(Reg(REG_PC)))
    }
)

```

Two things are important to notice here. First we use `QBDI::Or` to combine multiple `QBDI::PatchCondition`. Second the fact we need to stop the execution here and switch back to the context of the VM is not expressed in the patch. Indeed the patching engine simply notices that this patch overwrites the value of the PC and thus needs to end the basic block after it.

## Advanced Patching

### Conditional Branching Instruction Patch

The previous section dealt with simple patching cases where the rule does not need to be very complex. Conditional instructions can add a significant amount of complexity to the writing of a patch rules and requires some tricks. Below is the patch for the ARM conditional branching instruction:

```

PatchRule(
    // Condition: every Bcc instructions (e.g. BNE, BEQ, etc.)
    OpIs(llvm::ARM::Bcc),
    // Generators
    {
        // Compute the Bcc target (which is PC relative) and store it in a new temp with
↪id 0
        GetPCOffset(Temp(0), Operand(0)),
        // Modify the jump target such as it potentially skips the next generator
        ModifyInstruction({
            SetOperand(Operand(0), Constant(0))
        }),
        // Compute the next instruction address and store it in temp with id 0
        GetPCOffset(Temp(0), Constant(-4)),
        // At this point either:
        // * The jump was not taken and Temp(0) stores the next instruction address.
        // * The jump was taken and Temp(0) stores the Bcc target
        // We thus write Temp(0) which has the correct next address to execute in the
↪REG_PC
        // value in the context part of the data block.
        WriteTemp(Temp(0), Offset(Reg(REG_PC)))
    }
)

```

(continues on next page)



(continued from previous page)

```
}
)
```

As we can see, this code reuses the original conditional branching instruction to create a conditional move. While this is a trick, it is an architecture independent trick which is also used under X86\_64. Some details can be noted though. First the next instruction address is PC - 4 which is an ARM specificity. Secondly, the constant used to overwrite the jump target needs to be determined by hand as QBDI does not have the capacity to compute it automatically.

## Complex InstTransform

The patch below is used to patch instructions which load their branching target from a memory address under X86\_64. It exploits QBDI::InstTransform to convert the instruction into a load from memory to obtain this branching target:

```
PatchRule(
    // Condition: applies on CALL where the target is at a relative memory location.
    ↪(thus uses REG_PC)
    And({
        OpIs(llvm::X86::CALL64m),
        UseReg(Reg(REG_PC))
    }),
    // Generators
    {
        // First compute PC + 0 and stores it into a new temp with id 0
        GetPCOffset(Temp(0), Constant(0)),
        // Transforms the CALL *[RIP + ...] into MOV Temp(1), *[Temp(0) + ...]
        ModifyInstruction({
            // RIP is replaced with Temp(0)
            SubstituteWithTemp(Reg(REG_PC), Temp(0)),
            // The opcode is changed to a 64 bits MOV from memory to a register
            SetOpcode(llvm::X86::MOV64rm),
            // We insert the destination register, a new temp with id 1, at the
            ↪beginning of
            // the operand list
            AddOperand(Operand(0), Temp(1))
        }),
        // Temp(1) thus contains the CALL target.
        // We use the X86_64 specific SimulateCall with this target.
        SimulateCall(Temp(1))
    }
)
```

A few things need to be noted. First the sequence of QBDI::InstTransform is complex because it substitutes RIP and it mutates the CALL into a MOV. Secondly, new QBDI::Temp can be instantiated and used anywhere in the program. Lastly, some complex architecture specific mechanisms have been abstracted in single QBDI::PatchGenerator, like QBDI::SimulateCall.

## Instrumentation Callbacks

`QBDI::InstrRule` allows to insert inline instrumentation inside the patch with a concept similar to the rules shown previously. Callbacks to host code are triggered by a break to host with specific variables set correctly in the host state part of the context:

- the `hostState.callback` should be set to the callback function address to call.
- the `hostState.data` should be set to the callback function data parameter.
- the `hostState.origin` should be set to the ID of the current instruction (see `QBDI::GetInstId`).

In practice, there exists a function which can generate the `PatchGenerator` needed to setup those variables correctly:

`PatchGenerator::UniquePtrVec QBDI::getCallbackGenerator(InstCallback cbk, void *data)`

Output a list of `PatchGenerator` which would set up the host state part of the context for a callback.

### Parameters

- **cbk** – [in] The callback function to call.
- **data** – [in] The data to pass as an argument to the callback function.

**Returns** A list of `PatchGenerator` to set up this callback call.

Thus, in practice, a `QBDI::InstrRule` which would set up a callback on every instruction writing data in memory would look like this:

```
InstrRule(
    // Condition: on every instruction making write access
    DoesWriteAccess(),
    // Generators: set up a callback to someCallbackFunction with someParameter
    getCallbackGenerator(someCallbackFunction, someParameter),
    // Position this instrumentation after the instruction
    InstPosition::POSTINST,
    // Break to the host after the instrumentation (required for the callback to be made)
    true
);
```

However the callback generator can be written directly in `PatchDSL` for more advantageous usages. The instrumentation rules below pass directly the written data as the callback parameter:

```
InstrRule(
    // Condition: on every instruction making write access
    DoesWriteAccess(),
    // Generators: set up a callback to someCallbackFunction with someParameter
    {
        // Set hostState.callback to the callback function address
        GetConstant(Temp(0), Constant((rword) someCallbackFunction)),
        WriteTemp(Temp(0), Offset(offsetof(Context, hostState.callback))),
        // Set hostState.data as the written value
        GetWriteValue(Temp(0)),
        WriteTemp(Temp(0), Offset(offsetof(Context, hostState.data))),
        // Set hostState.origin as the current instID
        GetInstId(Temp(0)),
        WriteTemp(Temp(0), Offset(offsetof(Context, hostState.origin)))
    }
    // Position this instrumentation after the instruction
```

(continues on next page)

(continued from previous page)

```

    QBDI::InstPosition::POSTINST,
    // Break to the host after the instrumentation (required for the callback to be made)
    true
));

```

## Inline Instrumentation

## PatchDSL Reference

## PatchConditions

## Boolean Arithmetic Operators

- QBDI::And
- QBDI::Or
- QBDI::Not
- QBDI::True

inline QBDI::And::And(PatchCondition::UniquePtrVec &&conditions)  
Return true if every PatchCondition of the list conditions return true (lazy evaluation).

**Parameters** **conditions** – [in] List of conditions to evaluate.

inline QBDI::Or::Or(PatchCondition::UniquePtrVec &&conditions)  
Return true if one of the PatchCondition of the list conditions return true (lazy evaluation).

**Parameters** **conditions** – [in] List of conditions to evaluate.

inline QBDI::Not::Not(PatchCondition::UniquePtr &&condition)  
Return the logical inverse of condition.

**Parameters** **condition** – [in] Condition to evaluate.

inline QBDI::True::True()  
Return true.

## Instruction Conditions

- QBDI::OpIs
- QBDI::UseReg
- QBDI::AddressInRange

inline QBDI::OpIs::OpIs(unsigned int op)  
Return true if the instruction opcode is equal to op.

**Parameters** **op** – [in] LLVM instruction opcode ID.

inline QBDI::UseReg::UseReg(*Reg* reg)  
Return true if the instruction uses reg as one of its operand.

**Parameters** **reg** – [in] The register to compare with.

inline QBDI::InstructionInRange::InstructionInRange(*Constant* start, *Constant* end)  
 Return true if the instruction address is in the range [start, end[ (end not included).

**Parameters**

- **start** – [in] Start of the range.
- **end** – [in] End of the range (not included).

## Memory Access Conditions

- QBDI::DoesReadAccess
- QBDI::DoesWriteAccess

inline QBDI::DoesReadAccess::DoesReadAccess()  
 Return true if the instruction read data from memory.

inline QBDI::DoesWriteAccess::DoesWriteAccess()  
 Return true if the instruction write data to memory.

## PatchGenerators

## Registry and Temporary Operations

- QBDI::LoadReg
- QBDI::SaveReg
- QBDI::CopyReg
- QBDI::WriteTemp

inline QBDI::LoadReg::LoadReg(*Reg* reg, *Offset* offset)  
 Load a register from the data block at the specified offset. This can be used to load register values from the context part of the data block.

**Parameters**

- **reg** – [in] A register where the value will be loaded.
- **offset** – [in] The offset in the data block from where the value will be loaded.

inline QBDI::SaveReg::SaveReg(*Reg* reg, *Offset* offset)  
 Save a register in the data block at the specified offset. This can be used to save register values in the context part of the data block.

**Parameters**

- **reg** – [in] A register which will be saved.
- **offset** – [in] The offset in the data block where the register will be written.

inline QBDI::CopyReg::CopyReg(*Reg* reg, *Temp* temp)  
 Copy a register in a temporary.

**Parameters**

- **reg** – [in] The register which will be copied
- **temp** – [in] A temporary where the register will be copied.

inline QBDI::WriteTemp::WriteTemp(*Temp* temp, *Offset* offset)

Write a temporary value in the data block at the specified offset. This can be used to overwrite register values in the context part of the data block.

#### Parameters

- **temp** – [in] A temporary which will be written. The value of the temporary is unchanged.
- **offset** – [in] The offset in the data block where the temporary will be written.

inline QBDI::WriteTemp::WriteTemp(*Temp* temp, *Shadow* shadow)

Write a temporary value in a shadow in the data block.

#### Parameters

- **temp** – [in] A temporary which will be written. The value of the temporary is unchanged.
- **shadow** – [in] The shadow use to store the value.

## Instruction Information Queries

- QBDI::GetOperand
- QBDI::GetConstant
- QBDI::GetPCOffset

inline QBDI::GetOperand::GetOperand(*Temp* temp, *Operand* op)

Obtain the value of the operand op and copy it's value in a temporary. If op is an immediate the immediate value is copied, if op is a register the register value is copied.

#### Parameters

- **temp** – [in] A temporary where the value will be copied.
- **op** – [in] The operand index (relative to the instruction LLVM MCInst representation) to be copied.

inline QBDI::GetConstant::GetConstant(*Temp* temp, *Constant* cst)

Copy a constant in a temporary.

#### Parameters

- **temp** – [in] A temporary where the value will be copied.
- **cst** – [in] The constant to copy.

inline QBDI::GetPCOffset::GetPCOffset(*Temp* temp, *Constant* cst)

Interpret a constant as a RIP relative offset and copy it in a temporary. It can be used to obtain the current value of RIP by using a constant of 0.

#### Parameters

- **temp** – [in] A temporary where the value will be copied.
- **cst** – [in] The constant to be used.

inline QBDI::GetPCOffset::GetPCOffset(*Temp* temp, *Operand* op)

Interpret an operand as a RIP relative offset and copy it in a temporary. It can be used to obtain jump/call targets or relative memory access addresses.

#### Parameters

- **temp** – [in] A temporary where the value will be copied.

- **op** – [in] The operand index (relative to the instruction LLVM MCInst representation) to be used.

## Memory Access Information Queries

- QBDI::GetReadAddress
- QBDI::GetWriteAddress
- QBDI::GetReadValue
- QBDI::GetWriteValue

inline QBDI::GetReadAddress::GetReadAddress(Temp temp, size\_t index = 0)

Resolve the memory address where the instructions will read its value and copy the address in a temporary. This PatchGenerator is only guaranteed to work before the instruction has been executed.

### Parameters

- **temp** – [in] A temporary where the memory address will be copied.
- **index** – [in] Index of access to saved when instruction does many read access

inline QBDI::GetWriteAddress::GetWriteAddress(Temp temp)

Resolve the memory address where the instructions will write its value and copy the address in a temporary. This PatchGenerator is only guaranteed to work before the instruction has been executed.

**Parameters** **temp** – [in] A temporary where the memory address will be copied.

inline QBDI::GetReadValue::GetReadValue(Temp temp, size\_t index = 0)

Resolve the memory address where the instructions will read its value and copy the value in a temporary. This PatchGenerator is only guaranteed to work before the instruction has been executed.

### Parameters

- **temp** – [in] A temporary where the memory value will be copied.
- **index** – [in] Index of access to saved when instruction does many read access

inline QBDI::GetWriteValue::GetWriteValue(Temp temp)

Resolve the memory address where the instructions has written its value and copy back the value in a temporary. This PatchGenerator is only guaranteed to work after the instruction has been executed.

**Parameters** **temp** – [in] A temporary where the memory value will be copied. The written address must be in the tmp.

## Special

- QBDI::ModifyInstruction
- QBDI::DoNotInstrument

QBDI::ModifyInstruction::ModifyInstruction(std::vector<std::unique\_ptr<InstTransform>>&&transforms)

Apply a list of InstTransform to the current instruction and output the result.

**Parameters** **transforms** – [in] Vector of InstTransform to be applied.

inline QBDI::DoNotInstrument::DoNotInstrument()

Adds a “do not instrument” flag to the resulting patch which allows it to skip the instrumentation process of the engine.

## X86\_64 Specific

- QBDI::SimulateCall
- QBDI::SimulateRet

inline QBDI::SimulateCall::SimulateCall(*Temp* temp)

Simulate the effects of a call to the address stored in a temporary. The target address overwrites the stored value of RIP in the context part of the data block and the return address is pushed onto the stack. This generator signals a PC modification and triggers and end of basic block.

**Parameters** *temp* – [in] Stores the call target address. Overwritten by this generator.

inline QBDI::SimulateRet::SimulateRet(*Temp* temp)

Simulate the effects of a return instruction. First the return address is popped from the stack into a temporary, then an optional stack deallocation is performed and finally the return address is written in the stored value of RIP in the context part of the data block. This generator signals a PC modification and triggers an end of basic block.

The optional deallocation is performed if the current instruction has one single immediate operand (which is the case of RETIQ and RETIW).

**Parameters** *temp* – [in] Any unused temporary, overwritten by this generator.

## Internals

- QBDI::GetInstId
- QBDI::JumpEpilogue

inline QBDI::GetInstId::GetInstId(*Temp* temp)

Copy an *ExecBlock* specific id for the current instruction in a temporary. This id is used to identify the instruction responsible for a callback in the engine and is only meant for internal use.

**Parameters** *temp* – [in] A temporary where the id will be copied.

inline QBDI::JumpEpilogue::JumpEpilogue()

Generate a jump instruction which target the epilogue of the *ExecBlock*.

## InstTransform

- QBDI::SetOperand
- QBDI::AddOperand
- QBDI::SubstituteWithTemp
- QBDI::RemoveOperand
- QBDI::SetOpcode

inline QBDI::SetOperand::SetOperand(*Operand* opn, *Temp* temp)

Set the operand opn of the instruction as the *Temp* temp.

**Parameters**

- *opn* – [in] *Operand* index in the LLVM MCInst representation.
- *temp* – [in] Temporary register which will be set as the new operand

inline QBDI::SetOperand::SetOperand(*Operand* opn, *Reg* reg)

Set the operand opn of the instruction as the *Reg* reg.

**Parameters**

- **opn** – [in] *Operand* index in the LLVM MCInst representation.
- **reg** – [in] Register which will be set as the new operand.

inline QBDI::SetOperand::SetOperand(*Operand* opn, *Constant* imm)

Set the operand opn of the instruction as the immediate imm.

**Parameters**

- **opn** – [in] *Operand* index in the LLVM MCInst representation.
- **imm** – [in] *Constant* which will be set as the new immediate operand.

inline QBDI::AddOperand::AddOperand(*Operand* opn, *Temp* temp)

Add a new temporary register operand to the instruction by inserting it at operand index opn.

**Parameters**

- **opn** – [in] *Operand* index in LLVM MCInst representation.
- **temp** – [in] *Temp* to be inserted as a new operand.

inline QBDI::AddOperand::AddOperand(*Operand* opn, *Reg* reg)

Add a new register operand to the instruction by inserting it at operand index opn.

**Parameters**

- **opn** – [in] *Operand* index in LLVM MCInst representation.
- **reg** – [in] Register to be inserted as a new operand.

inline QBDI::AddOperand::AddOperand(*Operand* opn, *Constant* imm)

Add a new immediate operand to the instruction by inserting it at operand index opn.

**Parameters**

- **opn** – [in] *Operand* index in LLVM MCInst representation.
- **imm** – [in] *Constant* to be inserted as a new immediate operand.

inline QBDI::SubstituteWithTemp::SubstituteWithTemp(*Reg* reg, *Temp* temp)

Substitute every reference to reg in the operands of the instruction with temp.

**Parameters**

- **reg** – [in] Register which will be substituted.
- **temp** – [in] Temporary register which will be substituted with.

inline QBDI::RemoveOperand::RemoveOperand(*Reg* reg)

Remove the first occurrence of reg in the operands of the instruction.

**Parameters** **reg** – [in] Register to remove from the operand list.

inline QBDI::SetOpcode::SetOpcode(unsigned int opcode)

Set the opcode of the instruction.

**Parameters** **opcode** – [in] New opcode to set as the instruction opcode.



## 2.8 CHANGELOG

### 2.8.1 Next Release

### 2.8.2 Version 0.8.0

2021-02-11 QBDI Team <qbdi@quarkslab.com>

- Fix android compilation (#126)
- Fix instrumentation of Pusha and Popa on X86 (#127)
- Fix getBBMemoryAccess (#128)
  - Improve the documentation of getBBMemoryAccess
  - Add recordMemoryAccess callback before any InstCallback
- Refactor ExecBlockManager to work with unaligned instruction on X86 and X86-64 (#129)
- Drop early support for ARM. The support hasn't been tested since 0.6.2.
- Rework cmake package export to import X86 and X86\_64 version of QBDI in one CMake (#146 and #132)
- Add `QBDI::VM::getCachedInstAnalysis()` to retrieve an InstAnalysis from an address. The address must be cached in the VM. (#148)
- Change in InstAnalysis and OperandAnalysis (#153):
  - Add InstAnalysis.flagsAccess to determine if the instruction uses or sets the flags (EFLAGS register). The analysis ANALYSIS\_OPERANDS is needed to use this field.
  - Change InstAnalysis.mayLoad and InstAnalysis.mayStore definition. The field will be true if QBDI detects memory access for the instruction.
  - Add InstAnalysis.loadSize and InstAnalysis.storeSize. If the instruction will read or write the memory, the expected size of the access is given by these fields. The analysis ANALYSIS\_INSTRUCTION is needed to use this field.
  - Add InstAnalysis.condition. With the update of LLVM, the mnemonic for conditional jump (like JE\_4) are merged in a unique mnemonic JCC\_4. This new field will contain the condition. The analysis ANALYSIS\_INSTRUCTION is needed to use this field. A new enum ConditionType has all the possible value.
  - Add OPERANDFLAG\_IMPLICIT for OperandAnalysis.flag. An operand will have this flag when a register is implicit to the instruction.
  - Add OPERAND\_FPR for OperandAnalysis.type. This type is used for floating point registers. For this type, OperandAnalysis.regCtxIdx is the offset in FPRState or -1 when an offset cannot be provided.
  - Add OPERAND\_SEG for OperandAnalysis.type. This type is used for segments or other unsupported register (like SSP).
  - Change type of OperandAnalysis.regCtxIdx to signed integer. When the value is less than 0, the index is invalid.
  - Change algorithm for OperandAnalysis. The type OPERAND\_INVALID may be present in the list of operands when a register is unset with the current instruction. Many operands may describe the used of the same register when a register is used multiple times for different purposes by the instruction.
- Add Instrumentation rule callback QBDI\_InstrRuleDataCBK and `QBDI::InstrRuleDataCBK` (#151)

The Instrumentation rule callback receives an `InstAnalysis` of each instruction during the instrumentation process. Based on this analysis, the callback may insert custom `InstCallback` for each instruction.

The call order of the callback has changed for the `PREINST` callback. If an instruction has multiple callbacks in `PREINST` position, they will be called in the reverse order of registration.

- Support SIMD `MemoryAccess` and change `QBDI::MemoryAccess` structure (#154)
  - Add `QBDI::MemoryAccess::flags`. In some cases, QBDI cannot provide all information about the access. This field describes the limitation for each access. Three limitations may be reached:
    - \* `QBDI::MemoryAccessFlags::MEMORY_UNKNOWN_SIZE`: the size of the access isn't known. Only the address is valid. The flag is only set for instruction with REP prefix before the execution of the instruction.
    - \* `QBDI::MemoryAccessFlags::MEMORY_MINIMUM_SIZE`: the size isn't the real size of the access, but the expected minimal size. This flag is used for instruction with complex access like XSAVE and XRSTOR.
    - \* `QBDI::MemoryAccessFlags::MEMORY_UNKNOWN_VALUE`: the value of the access hasn't been saved. The more common reason is that the access size is greater than the size of `QBDI::MemoryAccess::value`. This flag is also used for instruction with REP prefix when the access size cannot be determined during the instrumentation.
  - Fix `MemoryAccess` for some generic instruction.
- Add VM Options. (#144)

Some options can be provided to the VM to enable or disable some features:

- `QBDI::Options::OPT_DISABLE_FPR`: Disable FPRState backup and restore in context switches. Only the GPRState will be used.
- `QBDI::Options::OPT_DISABLE_OPTIONAL_FPR`: When `QBDI::Options::OPT_DISABLE_FPR` isn't selected, QBDI will detect if a BasicBlock needs FPRState. When BasicBlock doesn't need FPRState, the state will not be restored. This option forces the restoration and backup of FPRState to every BasicBlock.
- `QBDI::Options::OPT_ATT_SYNTAX` for X86 and X86\_64: `QBDI::InstAnalysis::disassembly` will be in AT&T syntax instead of Intel Syntax.
- Rework documentation (#156)

Internal update:

- Update LLVM to LLVM 10.0.1 (#104 and #139)
- Reduce LLVM library included in QBDI static library and reduce QBDI package size (#139 and #70)
- Replace GTest by `Catch2` (#140)
- Refactor code and switch to `cpp17` (#140 and #155)
- Use Github Actions to build dev-next package of QBDI (linux, osx and android) and PyQBDI (linux and osx) (#147, #159)
- Rewrite `frida-qbdi.js` and use `sphinx-js` for `frida-QBDI` documentation (#146). A version of `frida` greater or equals to 14.0 is needed to run `frida-qbdi.js` (need support of ES2019).
- Refactor `MemoryAccess` Code and add new tests (#154)
- Handle `VMCallback` return value (#155)
- Optimize Context Switch and FPRState restoration (#144)
- Add commit hash in devel version (#158)

### 2.8.3 Version 0.7.1

2020-02-27 QBDI Team <qbdi@quarkslab.com>

- Refactor PyQBDI, support python3, PyQBDI without Preload (#67, #121)
- Remove ncurses dependency (#123)
- Fix initFPRState (#114)

### 2.8.4 Version 0.7.0

2019-09-10 QBDI Team <qbdi@quarkslab.com>

- Add support for the x86 architecture
- Add new platforms related to Android: android-X86 and android-X86\_64
- Improve MemoryMap structure by adding the module's full path if available (#62, #71)
- Create docker images for QBDI (available on DockerHub qbdi/qbdi) (#56)
- Fix and improve operands analysis involved in memory accesses (#58) :

In the previous version, the output of the instruction analysis for **some** instructions did not contain the information related to memory accesses.

For instance, the *operand analysis* of `cmp MEM, IMM` misses information about the first operand:

```
cmp dword ptr [rbp + 4 * rbx - 4], 12345678
  [0] optype: 1, value : 12345678, size: 8, regOff: 0, regCtxIdx: 0, regName:↵
↵(null), regaccess : 0
```

This issue has been fixed and the `OperandAnalysis` structure contains a new attribute: `flag`, which is used to distinct `OperandAnalysis` involved in memory accesses from the others.

Here is an example of output:

```
cmp dword ptr [rbp + 4*rbx - 4], 12345678
  [0] optype: 2, flag: 1, value : 48, size: 8, regOff: 0, regCtxIdx: 14, regName:↵
↵RBP, regaccess : 1
  [1] optype: 1, flag: 1, value : 4, size: 8, regOff: 0, regCtxIdx: 0, regName:↵
↵(null), regaccess : 0
  [2] optype: 2, flag: 1, value : 49, size: 8, regOff: 0, regCtxIdx: 1, regName:↵
↵RBX, regaccess : 1
  [3] optype: 1, flag: 1, value : -4, size: 8, regOff: 0, regCtxIdx: 0, regName:↵
↵(null), regaccess : 0
  [4] optype: 1, flag: 0, value : 12345678, size: 4, regOff: 0, regCtxIdx: 0,↵
↵regName: (null), regaccess : 0
mov rax, qword ptr [rbp - 4]
  [0] optype: 2, flag: 0, value : 47, size: 8, regOff: 0, regCtxIdx: 0, regName:↵
↵RAX, regaccess : 2
  [1] optype: 2, flag: 1, value : 48, size: 8, regOff: 0, regCtxIdx: 14, regName:↵
↵RBP, regaccess : 1
  [2] optype: 1, flag: 1, value : 1, size: 8, regOff: 0, regCtxIdx: 0, regName:↵
↵(null), regaccess : 0
  [3] optype: 1, flag: 1, value : -4, size: 8, regOff: 0, regCtxIdx: 0, regName:↵
↵(null), regaccess : 0
```

(continues on next page)

(continued from previous page)

```

mov rax, qword ptr [4*rbx]
  [0] optype: 2, flag: 0, value : 47, size: 8, regOff: 0, regCtxIdx: 0, regName:
↳RAX, regaccess : 2
  [1] optype: 1, flag: 1, value : 4, size: 8, regOff: 0, regCtxIdx: 0, regName:
↳(null), regaccess : 0
  [2] optype: 2, flag: 1, value : 49, size: 8, regOff: 0, regCtxIdx: 1, regName:
↳RBX, regaccess : 1
  [3] optype: 1, flag: 1, value : 0, size: 8, regOff: 0, regCtxIdx: 0, regName:
↳(null), regaccess : 0
jne -6115
  [0] optype: 1, flag: 2, value : -6115, size: 4, regOff: 0, regCtxIdx: 0,
↳regName: (null), regaccess : 0
lea rax, [rbp + 4*rbx - 4]
  [0] optype: 2, flag: 0, value : 47, size: 8, regOff: 0, regCtxIdx: 0, regName:
↳RAX, regaccess : 2
  [1] optype: 2, flag: 4, value : 48, size: 8, regOff: 0, regCtxIdx: 14, regName:
↳RBP, regaccess : 1
  [2] optype: 1, flag: 4, value : 4, size: 8, regOff: 0, regCtxIdx: 0, regName:
↳(null), regaccess : 0
  [3] optype: 2, flag: 4, value : 49, size: 8, regOff: 0, regCtxIdx: 1, regName:
↳RBX, regaccess : 1
  [4] optype: 1, flag: 4, value : -4, size: 8, regOff: 0, regCtxIdx: 0, regName:
↳(null), regaccess : 0

```

## 2.8.5 Version 0.6.2

2018-10-19 Cedric TESSIER <[ctessier@quarkslab.com](mailto:ctessier@quarkslab.com)>

- Add support for a public CI (based on Travis and AppVeyor)
- Fix instruction operands analysis (#57, #59)
- Add missing MEMORY\_READ enum value in Python bindings (#61)
- Fix cache misbehavior on corner cases (#49, #51)
- Add missing memory access instructions on x86\_64 (#45, #47, #72)
- Enable asserts in Debug builds (#48)

## 2.8.6 Version 0.6.1

2018-03-22 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Fixing a performance regression with the addCodeAddrCB (#42):

Since 0.6, this API would trigger a complete cache flush forcing the engine to regenerate all the instrumented code after each call. Since this API is used inside VM:run(), this had the effect of completely canceling precaching optimization where used.

- Fixing support for AVX host without AVX2 support (#19):

Context switching was wrongly using AVX2 instructions instead of AVX instructions causing segfaults under hosts supporting AVX but not AVX2.

### 2.8.7 Version 0.6

2018-03-02 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Important performance improvement in the core engine (#30) **This slightly changes the behavior of VMEvents.**
- Fix the addCodeAddrCB API (#37)
- atexit and getCurrentProcessMap in python bindings (#35)
- Fix getInstAnalysis on BASIC\_BLOCK\_ENTRY (#28)
- Various documentation improvements (#34, #37, #38, #40) and an API uniformisation (#29)

### 2.8.8 Version 0.5

2017-12-22 Cedric TESSIER <[ctessier@quarkslab.com](mailto:ctessier@quarkslab.com)>

- Official public release!

### 2.8.9 Version 0.5 RC3

2017-12-10 Cedric TESSIER <[ctessier@quarkslab.com](mailto:ctessier@quarkslab.com)>

- Introducing pyqbd, full featured python bindings based on QBDIPreload library
- Revising variadic API to include more friendly prototypes
- Various bug, compilation and documentation fixes

### 2.8.10 Version 0.5 RC2

2017-10-30 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Apache 2 licensing
- New QBDIPreload library for easier dynamic injection under linux and macOS
- Various bug, compilation and documentation fixes
- Big tree cleanup

### 2.8.11 Version 0.5 RC1

2017-10-09 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- New Frida bindings
- Upgrade to LLVM 5.0
- Support for AVX registers
- New callback helpers on mnemonics and memory accesses
- Basic block precaching API
- Automatic cache invalidation when a new instrumentation is added
- Instruction and sequence level cache avoids needless retranslation
- Upgrade of the validator which now supports Linux and macOS

## 2.8.12 Version 0.4

2017-01-06 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Basic Instruction Shadows concept
- Memory access PatchDSL statements with support under X86\_64 (non SIMD memory access only)
- Shadow based memory access API and instrumentation
- C and C++ API stabilization
- Out-of-tree build and SDK
- Overhaul of the entire documentation with a complete PatchDSL explanation and a split between user and developer documentation.

## 2.8.13 Version 0.3

2016-04-29 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Partial ARM support, sufficient to run simple program e.g cat, ls, ...
- Instrumentation filtering system, ExecBroker, allowing the engine to switch between non instrumented and instrumented execution
- Complex execution validation system under linux which allows to do instruction per instruction compared execution between a non instrumented and an instrumented instance of a program
- New callback system for Engine related event e.g basic block entry / exit, ExecBroker transfer / return.
- New (internal) logging system, LogSys, which allows to do priority and tag based filtering of the debug logs.

## 2.8.14 Version 0.2

2016-01-29 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Upgrade to LLVM 3.7
- Complete X86\_64 patching support
- Support of Windows X86\_64
- Basic callback based instrumentation
- Usable C++ and C API
- User documentation with examples
- Uniformisation of PatchDSL

### 2.8.15 Version 0.1

2015-10-09 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Ported the PatchDSL from the minijit PoC
- Corrected several design flaws in the PatchDSL
- Implemented a compared execution test setup to prove the execution via the JIT yields the same registers and stack state as a normal execution
- Basic patching working for ARM and X86\_64 architectures as shown by the compared execution tests

### 2.8.16 Version 0.0

2015-09-17 Charles HUBAIN <[chubain@quarkslab.com](mailto:chubain@quarkslab.com)>

- Working dependency system for LLVM and Google Test
- ExecBlock working and tested on linux-X86\_64, linux-ARM, android-ARM and macOS-X86\_64
- Deployed buildbot infrastructure for automated build and test on linux-X86\_64 and linux-ARM

## 2.9 References

### 2.9.1 Conferences and Workshops

- 2020-10-15: BSides Delhi - Analysing programs through dynamic instrumentation with QBDI by Tom Czayka and Nicolas Surbayrole
- 2020-06-29: Pass The Salt - Why are Frida and QBDI a Great Blend on Android? by Tom Czayka
- 2019-04-23: French-Japan cybersecurity workshop - Fuzzing binaries using Dynamic Instrumentation by Paul Hernault
- 2017-12-28: 34C3 conferences - Implementing an LLVM based Dynamic Binary Instrumentation framework by Charles Hubain and Cédric Tessier

### 2.9.2 Blog Post

- 2020-08-18: Introduction to Whiteboxes and Collision-Based Attacks With QBDI by Paul Hernault
- 2020-08-04: Why are Frida and QBDI a Great Blend on Android? by Tom Czayka
- 2019-09-10: QBDI 0.7.0
- 2019-06-03: Android Native Library Analysis with QBDI by Romain Thomas
- 2018-01-24: Slaying Dragons with QBDI by Paul Hernault





## INDICES AND TABLES

- `genindex`
- `search`



## Symbols

`__getitem__()` (*pyqbdg.GPRState* method), 121  
`__init__()` (*pyqbdg.InstrRuleDataCBK* method), 125  
`__init__()` (*pyqbdg.VM* method), 117  
`__setitem__()` (*pyqbdg.GPRState* method), 121

## A

`accessAddress` (*pyqbdg.MemoryAccess* property), 130  
`addCodeAddrCB()` (in module *pyqbdg.VM*), 119  
`addCodeCB()` (in module *pyqbdg.VM*), 119  
`addCodeRangeCB()` (in module *pyqbdg.VM*), 119  
`addInstrRule()` (in module *pyqbdg.VM*), 120  
`addInstrRuleRange()` (in module *pyqbdg.VM*), 120  
`addInstrumentedModule()` (in module *pyqbdg.VM*), 118  
`addInstrumentedModuleFromAddr()` (in module *pyqbdg.VM*), 118  
`addInstrumentedRange()` (in module *pyqbdg.VM*), 118  
`addMemAccessCB()` (in module *pyqbdg.VM*), 119  
`addMemAddrCB()` (in module *pyqbdg.VM*), 119  
`addMemRangeCB()` (in module *pyqbdg.VM*), 119  
`addMnemonicCB()` (in module *pyqbdg.VM*), 119  
`address` (*pyqbdg.InstAnalysis* property), 127  
`addVMEventCB()` (in module *pyqbdg.VM*), 119  
`affectControlFlow` (*pyqbdg.InstAnalysis* property), 127  
`alignedAlloc()` (in module *pyqbdg*), 131  
`alignedFree()` (in module *pyqbdg*), 131  
`allocateMemory()` (in module *pyqbdg*), 134  
`allocateRword()` (in module *pyqbdg*), 134  
`allocateVirtualStack()` (in module *pyqbdg*), 131  
`AnalysisType` (C++ enum), 72  
`AnalysisType` (in module *pyqbdg*), 127  
`AnalysisType()` (class), 148  
`AnalysisType.ANALYSIS_DISASSEMBLY` (*AnalysisType* attribute), 148  
`AnalysisType.ANALYSIS_INSTRUCTION` (*AnalysisType* attribute), 148  
`AnalysisType.ANALYSIS_OPERANDS` (*AnalysisType* attribute), 148  
`AnalysisType.ANALYSIS_SYMBOL` (*AnalysisType* attribute), 148

`AnalysisType::QBDI_ANALYSIS_DISASSEMBLY` (C++ enumerator), 72  
`AnalysisType::QBDI_ANALYSIS_INSTRUCTION` (C++ enumerator), 72  
`AnalysisType::QBDI_ANALYSIS_OPERANDS` (C++ enumerator), 72  
`AnalysisType::QBDI_ANALYSIS_SYMBOL` (C++ enumerator), 72  
`AVAILABLE_GPR` (*pyqbdg.GPRState* property), 121

## B

`basicBlockEnd` (*pyqbdg.VMState* property), 130  
`basicBlockStart` (*pyqbdg.VMState* property), 131  
built-in function  
`pyqbdgpreload_on_run()`, 157

## C

`call()` (in module *pyqbdg.VM*), 120  
`CallbackPriority` (C++ enum), 71  
`CallbackPriority` (in module *pyqbdg*), 126  
`CallbackPriority()` (class), 148  
`CallbackPriority.PRIORITY_DEFAULT` (*CallbackPriority* attribute), 148  
`CallbackPriority.PRIORITY_MEMACCESS_LIMIT` (*CallbackPriority* attribute), 148  
`CallbackPriority::QBDI_PRIORITY_DEFAULT` (C++ enumerator), 71  
`CallbackPriority::QBDI_PRIORITY_MEMACCESS_LIMIT` (C++ enumerator), 71  
`cbk` (*pyqbdg.InstrRuleDataCBK* property), 125  
`clearAllCache()` (in module *pyqbdg.VM*), 121  
`clearCache()` (in module *pyqbdg.VM*), 121  
`condition` (*pyqbdg.InstAnalysis* property), 127  
`ConditionType` (C++ enum), 74  
`ConditionType` (in module *pyqbdg*), 128  
`ConditionType()` (class), 149  
`ConditionType.CONDITION_ABOVE` (*ConditionType* attribute), 150  
`ConditionType.CONDITION_ABOVE_EQUALS` (*ConditionType* attribute), 150  
`ConditionType.CONDITION_ALWAYS` (*ConditionType* attribute), 149

ConditionType.CONDITION\_BELOW (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_BELOW\_EQUALS (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_EQUALS (*ConditionType attribute*), 149  
 ConditionType.CONDITION\_EVEN (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_GREAT (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_GREAT\_EQUALS (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_LESS (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_LESS\_EQUALS (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_NEVER (*ConditionType attribute*), 149  
 ConditionType.CONDITION\_NONE (*ConditionType attribute*), 149  
 ConditionType.CONDITION\_NOT\_EQUALS (*ConditionType attribute*), 149  
 ConditionType.CONDITION\_NOT\_OVERFLOW (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_NOT\_SIGN (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_ODD (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_OVERFLOW (*ConditionType attribute*), 150  
 ConditionType.CONDITION\_SIGN (*ConditionType attribute*), 150  
 ConditionType::QBDI\_CONDITION\_ABOVE (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_ABOVE\_EQUALS (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_ALWAYS (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_BELOW (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_BELOW\_EQUALS (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_EQUALS (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_EVEN (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_GREAT (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_GREAT\_EQUALS (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_LESS (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_LESS\_EQUALS (C++ enumerator), 75

ConditionType::QBDI\_CONDITION\_NEVER (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_NONE (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_NOT\_EQUALS (C++ enumerator), 74  
 ConditionType::QBDI\_CONDITION\_NOT\_OVERFLOW (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_NOT\_SIGN (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_ODD (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_OVERFLOW (C++ enumerator), 75  
 ConditionType::QBDI\_CONDITION\_SIGN (C++ enumerator), 75  
 contains() (*pyqbdI.Range method*), 133  
 cs (*pyqbdI.FPRState property*), 122

## D

data (*pyqbdI.InstrRuleDataCBK property*), 125  
 decodeDouble() (*in module pyqbdI*), 135  
 decodeDoubleU() (*in module pyqbdI*), 135  
 decodeFloat() (*in module pyqbdI*), 134  
 decodeFloatU() (*in module pyqbdI*), 135  
 deleteAllInstrumentations() (*in module pyqbdI.VM*), 120  
 deleteInstrumentation() (*in module pyqbdI.VM*), 120  
 disassembly (*pyqbdI.InstAnalysis property*), 127  
 dp (*pyqbdI.FPRState property*), 122  
 ds (*pyqbdI.FPRState property*), 122

## E

eflags (*pyqbdI.GPRState property*), 121  
 encodeDouble() (*in module pyqbdI*), 135  
 encodeDoubleU() (*in module pyqbdI*), 135  
 encodeFloat() (*in module pyqbdI*), 134  
 encodeFloatU() (*in module pyqbdI*), 135  
 end (*pyqbdI.Range property*), 133  
 event (*pyqbdI.VMState property*), 131

## F

fcw (*pyqbdI.FPRState property*), 122  
 flag (*pyqbdI.OperandAnalysis property*), 128  
 flags (*pyqbdI.MemoryAccess property*), 130  
 flagsAccess (*pyqbdI.InstAnalysis property*), 127  
 fop (*pyqbdI.FPRState property*), 122  
 FPControl (C++ struct), 67  
 FPControl::\_\_pad0\_\_ (C++ member), 68  
 FPControl::\_\_pad1\_\_ (C++ member), 68  
 FPControl::\_\_pad2\_\_ (C++ member), 68  
 FPControl::denorm (C++ member), 68

[FPControl::invalid \(C++ member\)](#), 68  
[FPControl::ovrfl \(C++ member\)](#), 68  
[FPControl::pc \(C++ member\)](#), 68  
[FPControl::precis \(C++ member\)](#), 68  
[FPControl::rc \(C++ member\)](#), 68  
[FPControl::undfl \(C++ member\)](#), 68  
[FPControl::zdiv \(C++ member\)](#), 68  
[FPRState \(C++ struct\)](#), 65  
[FPRState \(class in pyqbd\)](#), 122  
[FPStatus \(C++ struct\)](#), 68  
[FPStatus::busy \(C++ member\)](#), 69  
[FPStatus::c0 \(C++ member\)](#), 69  
[FPStatus::c1 \(C++ member\)](#), 69  
[FPStatus::c2 \(C++ member\)](#), 69  
[FPStatus::c3 \(C++ member\)](#), 69  
[FPStatus::denorm \(C++ member\)](#), 68  
[FPStatus::errsumm \(C++ member\)](#), 69  
[FPStatus::invalid \(C++ member\)](#), 68  
[FPStatus::ovrfl \(C++ member\)](#), 68  
[FPStatus::precis \(C++ member\)](#), 69  
[FPStatus::stkflt \(C++ member\)](#), 69  
[FPStatus::tos \(C++ member\)](#), 69  
[FPStatus::undfl \(C++ member\)](#), 69  
[FPStatus::zdiv \(C++ member\)](#), 68  
[freeMemory\(\)](#) (in module pyqbd), 134  
[fs \(pyqbd.GPRState property\)](#), 121  
[fsw \(pyqbd.FPRState property\)](#), 122  
[ftw \(pyqbd.FPRState property\)](#), 122

## G

[getBBMemoryAccess\(\)](#) (in module pyqbd.VM), 120  
[getCachedInstAnalysis\(\)](#) (in module pyqbd.VM), 120  
[getCurrentProcessMaps\(\)](#) (in module pyqbd), 131  
[getFPRState\(\)](#) (in module pyqbd.VM), 118  
[getGPRState\(\)](#) (in module pyqbd.VM), 118  
[getInstAnalysis\(\)](#) (in module pyqbd.VM), 120  
[getInstMemoryAccess\(\)](#) (in module pyqbd.VM), 120  
[getModuleNames\(\)](#) (in module pyqbd), 131  
[getRemoteProcessMaps\(\)](#) (in module pyqbd), 131  
[GPR\\_NAMES \(None attribute\)](#), 146  
[GPRState \(C++ struct\)](#), 64  
[GPRState \(class in pyqbd\)](#), 121  
[GPRState\(\)](#) (class), 145  
[GPRState.dump\(\)](#) (GPRState method), 145  
[GPRState.getRegister\(\)](#) (GPRState method), 145  
[GPRState.getRegisters\(\)](#) (GPRState method), 145  
[GPRState.pp\(\)](#) (GPRState method), 145  
[GPRState.setRegister\(\)](#) (GPRState method), 145  
[GPRState.setRegisters\(\)](#) (GPRState method), 145  
[GPRState.synchronizeContext\(\)](#) (GPRState method), 145  
[GPRState.synchronizeRegister\(\)](#) (GPRState method), 146

[gs \(pyqbd.GPRState property\)](#), 121

## H

[hexPointer\(\)](#) (built-in function), 154

## I

[instAddress \(pyqbd.MemoryAccess property\)](#), 130  
[InstAnalysis \(C++ struct\)](#), 72  
[InstAnalysis \(class in pyqbd\)](#), 127  
[InstAnalysis\(\)](#) (class), 148  
[InstAnalysis.address \(InstAnalysis attribute\)](#), 148  
[InstAnalysis.affectControlFlow \(InstAnalysis attribute\)](#), 148  
[InstAnalysis.condition \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.disassembly \(InstAnalysis attribute\)](#), 148  
[InstAnalysis.flagsAccess \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.instSize \(InstAnalysis attribute\)](#), 148  
[InstAnalysis.isBranch \(InstAnalysis attribute\)](#), 148  
[InstAnalysis.isCall \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.isCompare \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.isMoveImm \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.isPredicable \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.isReturn \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.loadSize \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.mayLoad \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.mayStore \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.mnemonic \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.operands \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.storeSize \(InstAnalysis attribute\)](#), 149  
[InstAnalysis.symbol \(InstAnalysis attribute\)](#), 149  
[InstAnalysis::address \(C++ member\)](#), 73  
[InstAnalysis::affectControlFlow \(C++ member\)](#), 73  
[InstAnalysis::analysisType \(C++ member\)](#), 74  
[InstAnalysis::condition \(C++ member\)](#), 73  
[InstAnalysis::cpuMode \(C++ member\)](#), 73  
[InstAnalysis::disassembly \(C++ member\)](#), 73  
[InstAnalysis::flagsAccess \(C++ member\)](#), 74  
[InstAnalysis::instSize \(C++ member\)](#), 73  
[InstAnalysis::isBranch \(C++ member\)](#), 73  
[InstAnalysis::isCall \(C++ member\)](#), 73  
[InstAnalysis::isCompare \(C++ member\)](#), 73  
[InstAnalysis::isMoveImm \(C++ member\)](#), 73  
[InstAnalysis::isPredicable \(C++ member\)](#), 73  
[InstAnalysis::isReturn \(C++ member\)](#), 73  
[InstAnalysis::loadSize \(C++ member\)](#), 73  
[InstAnalysis::mayLoad \(C++ member\)](#), 73  
[InstAnalysis::mayStore \(C++ member\)](#), 73  
[InstAnalysis::mnemonic \(C++ member\)](#), 73  
[InstAnalysis::module \(C++ member\)](#), 74

InstAnalysis::numOperands (C++ member), 74  
 InstAnalysis::operands (C++ member), 74  
 InstAnalysis::storeSize (C++ member), 73  
 InstAnalysis::symbol (C++ member), 74  
 InstAnalysis::symbolOffset (C++ member), 74  
 InstCallback (C++ type), 70  
 InstCallback() (built-in function), 146  
 InstPosition (C++ enum), 71  
 InstPosition (in module pyqbd), 126  
 InstPosition() (class), 148  
 InstPosition.POSTINST (InstPosition attribute), 148  
 InstPosition.PREINST (InstPosition attribute), 148  
 InstPosition::QBDI\_POSTINST (C++ enumerator), 71  
 InstPosition::QBDI\_PREINST (C++ enumerator), 71  
 InstrRuleCallback() (built-in function), 147  
 InstrRuleCallbackC (C++ type), 70  
 InstrRuleDataCBK (class in pyqbd), 125  
 InstrRuleDataCBK() (class), 147  
 InstrRuleDataVec (C++ type), 70  
 instrumentAllExecutableMaps() (in module pyqbd.VM), 118  
 instSize (pyqbd.InstAnalysis property), 127  
 intersect() (pyqbd.Range method), 133  
 ip (pyqbd.FPRState property), 122  
 isBranch (pyqbd.InstAnalysis property), 127  
 isCall (pyqbd.InstAnalysis property), 127  
 isCompare (pyqbd.InstAnalysis property), 127  
 isMoveImm (pyqbd.InstAnalysis property), 127  
 isPredicable (pyqbd.InstAnalysis property), 127  
 isReturn (pyqbd.InstAnalysis property), 127

## L

loadSize (pyqbd.InstAnalysis property), 127  
 LogPriority (C++ enum), 83  
 LogPriority (in module pyqbd), 132  
 LogPriority::QBDI\_DEBUG (C++ enumerator), 83  
 LogPriority::QBDI\_DISABLE (C++ enumerator), 83  
 LogPriority::QBDI\_ERROR (C++ enumerator), 83  
 LogPriority::QBDI\_INFO (C++ enumerator), 83  
 LogPriority::QBDI\_WARNING (C++ enumerator), 83

## M

mayLoad (pyqbd.InstAnalysis property), 127  
 mayStore (pyqbd.InstAnalysis property), 127  
 MemoryAccess (C++ struct), 77  
 MemoryAccess (class in pyqbd), 130  
 MemoryAccess() (class), 152  
 MemoryAccess.accessAddress (MemoryAccess attribute), 152  
 MemoryAccess.flags (MemoryAccess attribute), 152  
 MemoryAccess.instAddress (MemoryAccess attribute), 152  
 MemoryAccess.size (MemoryAccess attribute), 152

MemoryAccess.type (MemoryAccess attribute), 152  
 MemoryAccess.value (MemoryAccess attribute), 152  
 MemoryAccess::accessAddress (C++ member), 77  
 MemoryAccess::flags (C++ member), 77  
 MemoryAccess::instAddress (C++ member), 77  
 MemoryAccess::size (C++ member), 77  
 MemoryAccess::type (C++ member), 77  
 MemoryAccess::value (C++ member), 77  
 MemoryAccessFlags (C++ enum), 78  
 MemoryAccessFlags (in module pyqbd), 130  
 MemoryAccessFlags() (class), 152  
 MemoryAccessFlags.MEMORY\_MINIMUM\_SIZE (MemoryAccessFlags attribute), 152  
 MemoryAccessFlags.MEMORY\_NO\_FLAGS (MemoryAccessFlags attribute), 152  
 MemoryAccessFlags.MEMORY\_UNKNOWN\_SIZE (MemoryAccessFlags attribute), 152  
 MemoryAccessFlags.MEMORY\_UNKNOWN\_VALUE (MemoryAccessFlags attribute), 152  
 MemoryAccessFlags::QBDI\_MEMORY\_MINIMUM\_SIZE (C++ enumerator), 78  
 MemoryAccessFlags::QBDI\_MEMORY\_NO\_FLAGS (C++ enumerator), 78  
 MemoryAccessFlags::QBDI\_MEMORY\_UNKNOWN\_SIZE (C++ enumerator), 78  
 MemoryAccessFlags::QBDI\_MEMORY\_UNKNOWN\_VALUE (C++ enumerator), 78  
 MemoryAccessType (C++ enum), 77  
 MemoryAccessType (in module pyqbd), 130  
 MemoryAccessType() (class), 152  
 MemoryAccessType.MEMORY\_READ (MemoryAccessType attribute), 152  
 MemoryAccessType.MEMORY\_READ\_WRITE (MemoryAccessType attribute), 152  
 MemoryAccessType.MEMORY\_WRITE (MemoryAccessType attribute), 152  
 MemoryAccessType::QBDI\_MEMORY\_READ (C++ enumerator), 78  
 MemoryAccessType::QBDI\_MEMORY\_READ\_WRITE (C++ enumerator), 78  
 MemoryAccessType::QBDI\_MEMORY\_WRITE (C++ enumerator), 78  
 MemoryMap (class in pyqbd), 131  
 MMSTReg (C++ struct), 67  
 MMSTReg::reg (C++ member), 67  
 MMSTReg::rsrv (C++ member), 67  
 mnemonic (pyqbd.InstAnalysis property), 127  
 module (pyqbd.InstAnalysis property), 127  
 mxcsr (pyqbd.FPRState property), 122  
 mxcsrmask (pyqbd.FPRState property), 122

## N

name (pyqbd.MemoryMap property), 131



- NativePointer.prototype.toRword() (NativePointer.prototype method), 154
- NUM\_GPR (built-in variable), 69
- NUM\_GPR (pyqbdI.GPRState property), 121
- Number.prototype.toRword() (Number.prototype method), 154
- numOperands (pyqbdI.InstAnalysis property), 128
- ## O
- OperandAnalysis (C++ struct), 75
- OperandAnalysis (class in pyqbdI), 128
- OperandAnalysis() (class), 150
- OperandAnalysis.flag (OperandAnalysis attribute), 150
- OperandAnalysis.regAccess (OperandAnalysis attribute), 151
- OperandAnalysis.regCtxIdx (OperandAnalysis attribute), 150
- OperandAnalysis.regName (OperandAnalysis attribute), 151
- OperandAnalysis.regOff (OperandAnalysis attribute), 150
- OperandAnalysis.size (OperandAnalysis attribute), 150
- OperandAnalysis.type (OperandAnalysis attribute), 150
- OperandAnalysis.value (OperandAnalysis attribute), 150
- OperandAnalysis::flag (C++ member), 75
- OperandAnalysis::regAccess (C++ member), 76
- OperandAnalysis::regCtxIdx (C++ member), 76
- OperandAnalysis::regName (C++ member), 76
- OperandAnalysis::regOff (C++ member), 76
- OperandAnalysis::size (C++ member), 75
- OperandAnalysis::type (C++ member), 75
- OperandAnalysis::value (C++ member), 75
- OperandFlag (C++ enum), 76
- OperandFlag (in module pyqbdI), 129
- OperandFlag() (class), 151
- OperandFlag.OPERANDFLAG\_ADDR (OperandFlag attribute), 151
- OperandFlag.OPERANDFLAG\_IMPLICIT (OperandFlag attribute), 151
- OperandFlag.OPERANDFLAG\_NONE (OperandFlag attribute), 151
- OperandFlag.OPERANDFLAG\_PCREL (OperandFlag attribute), 151
- OperandFlag.OPERANDFLAG\_UNDEFINED\_EFFECT (OperandFlag attribute), 151
- OperandFlag::QBDI\_OPERANDFLAG\_ADDR (C++ enumerator), 76
- OperandFlag::QBDI\_OPERANDFLAG\_IMPLICIT (C++ enumerator), 77
- OperandFlag::QBDI\_OPERANDFLAG\_NONE (C++ enumerator), 76
- OperandFlag::QBDI\_OPERANDFLAG\_PCREL (C++ enumerator), 76
- OperandFlag::QBDI\_OPERANDFLAG\_UNDEFINED\_EFFECT (C++ enumerator), 76
- operands (pyqbdI.InstAnalysis property), 128
- OperandType (C++ enum), 76
- OperandType (in module pyqbdI), 129
- OperandType() (class), 151
- OperandType.OPERAND\_FPR (OperandType attribute), 151
- OperandType.OPERAND\_GPR (OperandType attribute), 151
- OperandType.OPERAND\_IMM (OperandType attribute), 151
- OperandType.OPERAND\_INVALID (OperandType attribute), 151
- OperandType.OPERAND\_PRED (OperandType attribute), 151
- OperandType.OPERAND\_SEG (OperandType attribute), 151
- OperandType::QBDI\_OPERAND\_FPR (C++ enumerator), 76
- OperandType::QBDI\_OPERAND\_GPR (C++ enumerator), 76
- OperandType::QBDI\_OPERAND\_IMM (C++ enumerator), 76
- OperandType::QBDI\_OPERAND\_INVALID (C++ enumerator), 76
- OperandType::QBDI\_OPERAND\_PRED (C++ enumerator), 76
- OperandType::QBDI\_OPERAND\_SEG (C++ enumerator), 76
- Options (C++ enum), 82
- Options (in module pyqbdI), 132
- options (pyqbdI.VM property), 117
- Options() (class), 153
- Options.NO\_OPT (Options attribute), 153
- Options.OPT\_ATT\_SYNTAX (Options attribute), 153
- Options.OPT\_DISABLE\_FPR (Options attribute), 153
- Options.OPT\_DISABLE\_OPTIONAL\_FPR (Options attribute), 153
- Options.OPT\_ENABLE\_FS\_GS (Options attribute), 154
- Options::QBDI\_NO\_OPT (C++ enumerator), 82
- Options::QBDI\_OPT\_ATT\_SYNTAX (C++ enumerator), 82
- Options::QBDI\_OPT\_DISABLE\_FPR (C++ enumerator), 82
- Options::QBDI\_OPT\_DISABLE\_OPTIONAL\_FPR (C++ enumerator), 82
- Options::QBDI\_OPT\_ENABLE\_FS\_GS (C++ enumerator), 82
- overlaps() (pyqbdI.Range method), 133

## P

Permission (in module pyqbd), 131  
 permission (pyqbd.MemoryMap property), 131  
 position (pyqbd.InstrRuleDataCBK property), 126  
 precacheBasicBlock() (in module pyqbd.VM), 121  
 priority (pyqbd.InstrRuleDataCBK property), 126  
 pyqbd.\_\_arch\_\_ (in module pyqbd), 132  
 pyqbd.\_\_platform\_\_ (in module pyqbd), 132  
 pyqbd.\_\_preload\_\_ (in module pyqbd), 132  
 pyqbd.\_\_version\_\_ (in module pyqbd), 132  
 pyqbd.InstCallback() (in module pyqbd), 125  
 pyqbd.InstrRuleCallback() (in module pyqbd), 125  
 pyqbd.NUM\_GPR (in module pyqbd), 124  
 pyqbd.REG\_BP (in module pyqbd), 124  
 pyqbd.REG\_PC (in module pyqbd), 124  
 pyqbd.REG\_RETURN (in module pyqbd), 124  
 pyqbd.REG\_SP (in module pyqbd), 124  
 pyqbd.VMCallback() (in module pyqbd), 125  
 pyqbdipreload\_on\_run()  
     built-in function, 157

## Q

QBDI() (class), 136  
 QBDI.addCodeAddrCB() (QBDI method), 139  
 QBDI.addCodeCB() (QBDI method), 139  
 QBDI.addCodeRangeCB() (QBDI method), 139  
 QBDI.addInstrRule() (QBDI method), 141  
 QBDI.addInstrRuleRange() (QBDI method), 141  
 QBDI.addInstrumentedModule() (QBDI method), 137  
 QBDI.addInstrumentedModuleFromAddr() (QBDI method), 137  
 QBDI.addInstrumentedRange() (QBDI method), 137  
 QBDI.addMemAccessCB() (QBDI method), 140  
 QBDI.addMemAddrCB() (QBDI method), 140  
 QBDI.addMemRangeCB() (QBDI method), 141  
 QBDI.addMnemonicCB() (QBDI method), 139  
 QBDI.addVMEventCB() (QBDI method), 140  
 QBDI.alignedAlloc() (QBDI method), 142  
 QBDI.alignedFree() (QBDI method), 142  
 QBDI.allocateVirtualStack() (QBDI method), 142  
 QBDI.call() (QBDI method), 143  
 QBDI.clearAllCache() (QBDI method), 144  
 QBDI.clearCache() (QBDI method), 144  
 QBDI.deleteAllInstrumentations() (QBDI method), 142  
 QBDI.deleteInstrumentation() (QBDI method), 142  
 QBDI.getBBMemoryAccess() (QBDI method), 144  
 QBDI.getCachedInstAnalysis() (QBDI method), 143  
 QBDI.getFPRState() (QBDI method), 136  
 QBDI.getGPRState() (QBDI method), 136  
 QBDI.getInstAnalysis() (QBDI method), 143  
 QBDI.getInstMemoryAccess() (QBDI method), 144  
 QBDI.getModuleNames() (QBDI method), 142  
 QBDI.getOptions() (QBDI method), 136  
 QBDI.instrumentAllExecutableMaps() (QBDI method), 137  
 QBDI.newInstCallback() (QBDI method), 138  
 QBDI.newInstrRuleCallback() (QBDI method), 138  
 QBDI.newVMCallback() (QBDI method), 138  
 QBDI.precacheBasicBlock() (QBDI method), 144  
 QBDI.recordMemoryAccess() (QBDI method), 144  
 QBDI.removeAllInstrumentedRanges() (QBDI method), 138  
 QBDI.removeInstrumentedModule() (QBDI method), 137  
 QBDI.removeInstrumentedModuleFromAddr() (QBDI method), 137  
 QBDI.removeInstrumentedRange() (QBDI method), 137  
 QBDI.run() (QBDI method), 143  
 QBDI.setFPRState() (QBDI method), 136  
 QBDI.setGPRState() (QBDI method), 136  
 QBDI.setOptions() (QBDI method), 136  
 QBDI.simulateCall() (QBDI method), 143  
 QBDI.version (QBDI attribute), 136  
 QBDI::AddOperand::AddOperand(C++ function), 188  
 QBDI::alignedAlloc(C++ function), 111  
 QBDI::alignedFree(C++ function), 112  
 QBDI::allocateVirtualStack(C++ function), 111  
 QBDI::AnalysisType(C++ enum), 104  
 QBDI::AnalysisType::ANALYSIS\_DISASSEMBLY (C++ enumerator), 104  
 QBDI::AnalysisType::ANALYSIS\_INSTRUCTION (C++ enumerator), 104  
 QBDI::AnalysisType::ANALYSIS\_OPERANDS (C++ enumerator), 104  
 QBDI::AnalysisType::ANALYSIS\_SYMBOL (C++ enumerator), 104  
 QBDI::And::And(C++ function), 183  
 QBDI::CallbackPriority(C++ enum), 103  
 QBDI::CallbackPriority::PRIORITY\_DEFAULT (C++ enumerator), 103  
 QBDI::CallbackPriority::PRIORITY\_MEMACCESS\_LIMIT (C++ enumerator), 103  
 QBDI::ConditionType(C++ enum), 106  
 QBDI::ConditionType::CONDITION\_ABOVE (C++ enumerator), 106  
 QBDI::ConditionType::CONDITION\_ABOVE\_EQUALS (C++ enumerator), 106  
 QBDI::ConditionType::CONDITION\_ALWAYS (C++ enumerator), 106  
 QBDI::ConditionType::CONDITION\_BELOW (C++ enumerator), 106  
 QBDI::ConditionType::CONDITION\_BELOW\_EQUALS



(C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_EQUALS (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_EVEN (C++ *enumerator*), 107

QBDI::ConditionType::CONDITION\_GREAT (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_GREAT\_EQUALS (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_LESS (C++ *enumerator*), 107

QBDI::ConditionType::CONDITION\_LESS\_EQUALS (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_NEVER (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_NONE (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_NOT\_EQUALS (C++ *enumerator*), 106

QBDI::ConditionType::CONDITION\_NOT\_OVERFLOW (C++ *enumerator*), 107

QBDI::ConditionType::CONDITION\_NOT\_SIGN (C++ *enumerator*), 107

QBDI::ConditionType::CONDITION\_ODD (C++ *enumerator*), 107

QBDI::ConditionType::CONDITION\_OVERFLOW (C++ *enumerator*), 107

QBDI::ConditionType::CONDITION\_SIGN (C++ *enumerator*), 107

QBDI::Constant (C++ *struct*), 175

QBDI::Constant::Constant (C++ *function*), 175

QBDI::Constant::operator rword (C++ *function*), 175

QBDI::CopyReg::CopyReg (C++ *function*), 184

QBDI::DoesReadAccess::DoesReadAccess (C++ *function*), 184

QBDI::DoesWriteAccess::DoesWriteAccess (C++ *function*), 184

QBDI::DoNotInstrument::DoNotInstrument (C++ *function*), 186

QBDI::ExecBlock (C++ *class*), 170

QBDI::ExecBlock::changeVMInstanceRef (C++ *function*), 170

QBDI::ExecBlock::ExecBlock (C++ *function*), 170

QBDI::ExecBlock::execute (C++ *function*), 170

QBDI::ExecBlock::getContext (C++ *function*), 172

QBDI::ExecBlock::getCurrentInstID (C++ *function*), 171

QBDI::ExecBlock::getCurrentPC (C++ *function*), 171

QBDI::ExecBlock::getCurrentSeqID (C++ *function*), 172

QBDI::ExecBlock::getDataBlockBase (C++ *function*), 170

QBDI::ExecBlock::getDataBlockOffset (C++ *function*), 170

QBDI::ExecBlock::getEpilogueOffset (C++ *function*), 171

QBDI::ExecBlock::getEpilogueSize (C++ *function*), 171

QBDI::ExecBlock::getInstAddress (C++ *function*), 171

QBDI::ExecBlock::getInstAnalysis (C++ *function*), 171

QBDI::ExecBlock::getInstID (C++ *function*), 171

QBDI::ExecBlock::getInstInstrumentedAddress (C++ *function*), 171

QBDI::ExecBlock::getInstMetadata (C++ *function*), 171

QBDI::ExecBlock::getLastShadow (C++ *function*), 173

QBDI::ExecBlock::getNextInstID (C++ *function*), 171

QBDI::ExecBlock::getNextSeqID (C++ *function*), 172

QBDI::ExecBlock::getOriginalMCInst (C++ *function*), 171

QBDI::ExecBlock::getSeqEnd (C++ *function*), 172

QBDI::ExecBlock::getSeqID (C++ *function*), 172

QBDI::ExecBlock::getSeqStart (C++ *function*), 172

QBDI::ExecBlock::getShadow (C++ *function*), 173

QBDI::ExecBlock::getShadowOffset (C++ *function*), 173

QBDI::ExecBlock::newShadow (C++ *function*), 172

QBDI::ExecBlock::selectSeq (C++ *function*), 172

QBDI::ExecBlock::setShadow (C++ *function*), 173

QBDI::ExecBlock::show (C++ *function*), 170

QBDI::ExecBlock::splitSequence (C++ *function*), 170

QBDI::ExecBlock::writeSequence (C++ *function*), 170

QBDI::FPControl (C++ *struct*), 99

QBDI::FPControl::\_\_pad0\_\_ (C++ *member*), 99

QBDI::FPControl::\_\_pad1\_\_ (C++ *member*), 99

QBDI::FPControl::\_\_pad2\_\_ (C++ *member*), 99

QBDI::FPControl::denorm (C++ *member*), 99

QBDI::FPControl::invalid (C++ *member*), 99

QBDI::FPControl::ovrfl (C++ *member*), 99

QBDI::FPControl::pc (C++ *member*), 99

QBDI::FPControl::precis (C++ *member*), 99

QBDI::FPControl::rc (C++ *member*), 99

QBDI::FPControl::undfl (C++ *member*), 99

QBDI::FPControl::zdiv (C++ *member*), 99

QBDI::FPRState (C++ *struct*), 96

QBDI::FPStatus (C++ *struct*), 99

QBDI::FPStatus::busy (C++ *member*), 100

QBDI::FPStatus::c0 (C++ *member*), 100

QBDI::FPStatus::c1 (C++ *member*), 100

QBDI::FPStatus::c2 (C++ member), 100  
 QBDI::FPStatus::c3 (C++ member), 100  
 QBDI::FPStatus::denorm (C++ member), 100  
 QBDI::FPStatus::errsumm (C++ member), 100  
 QBDI::FPStatus::invalid (C++ member), 100  
 QBDI::FPStatus::ovrfl (C++ member), 100  
 QBDI::FPStatus::precis (C++ member), 100  
 QBDI::FPStatus::stkflt (C++ member), 100  
 QBDI::FPStatus::tos (C++ member), 100  
 QBDI::FPStatus::undfl (C++ member), 100  
 QBDI::FPStatus::zdiv (C++ member), 100  
 QBDI::getCallbackGenerator (C++ function), 182  
 QBDI::GetConstant::GetConstant (C++ function), 185  
 QBDI::getCurrentProcessMaps (C++ function), 112  
 QBDI::GetInstId::GetInstId (C++ function), 187  
 QBDI::getModuleNames (C++ function), 112  
 QBDI::GetOperand::GetOperand (C++ function), 185  
 QBDI::GetPCOffset::GetPCOffset (C++ function), 185  
 QBDI::GetReadAddress::GetReadAddress (C++ function), 186  
 QBDI::GetReadValue::GetReadValue (C++ function), 186  
 QBDI::getRemoteProcessMaps (C++ function), 112  
 QBDI::getVersion (C++ function), 114  
 QBDI::GetWriteAddress::GetWriteAddress (C++ function), 186  
 QBDI::GetWriteValue::GetWriteValue (C++ function), 186  
 QBDI::GPRState (C++ struct), 95  
 QBDI::InstAnalysis (C++ struct), 104  
 QBDI::InstAnalysis::address (C++ member), 104  
 QBDI::InstAnalysis::affectControlFlow (C++ member), 104  
 QBDI::InstAnalysis::analysisType (C++ member), 106  
 QBDI::InstAnalysis::condition (C++ member), 105  
 QBDI::InstAnalysis::cpuMode (C++ member), 104  
 QBDI::InstAnalysis::disassembly (C++ member), 105  
 QBDI::InstAnalysis::flagsAccess (C++ member), 105  
 QBDI::InstAnalysis::instSize (C++ member), 104  
 QBDI::InstAnalysis::isBranch (C++ member), 105  
 QBDI::InstAnalysis::isCall (C++ member), 105  
 QBDI::InstAnalysis::isCompare (C++ member), 105  
 QBDI::InstAnalysis::isMoveImm (C++ member), 105  
 QBDI::InstAnalysis::isPredicable (C++ member), 105  
 QBDI::InstAnalysis::isReturn (C++ member), 105  
 QBDI::InstAnalysis::loadSize (C++ member), 105  
 QBDI::InstAnalysis::mayLoad (C++ member), 105  
 QBDI::InstAnalysis::mayStore (C++ member), 105  
 QBDI::InstAnalysis::mnemonic (C++ member), 104  
 QBDI::InstAnalysis::module (C++ member), 106  
 QBDI::InstAnalysis::numOperands (C++ member), 105  
 QBDI::InstAnalysis::operands (C++ member), 105  
 QBDI::InstAnalysis::storeSize (C++ member), 105  
 QBDI::InstAnalysis::symbol (C++ member), 105  
 QBDI::InstAnalysis::symbolOffset (C++ member), 106  
 QBDI::InstCallback (C++ type), 101  
 QBDI::InstCbLambda (C++ type), 101  
 QBDI::InstPosition (C++ enum), 102  
 QBDI::InstPosition::POSTINST (C++ enumerator), 103  
 QBDI::InstPosition::PREINST (C++ enumerator), 102  
 QBDI::InstrRule (C++ class), 178  
 QBDI::InstrRule::instrument (C++ function), 178  
 QBDI::InstrRule::tryInstrument (C++ function), 178  
 QBDI::InstrRuleCallback (C++ type), 102  
 QBDI::InstrRuleCbLambda (C++ type), 102  
 QBDI::InstrRuleDataCBK (C++ struct), 102  
 QBDI::InstrRuleDataCBK::cbk (C++ member), 102  
 QBDI::InstrRuleDataCBK::data (C++ member), 102  
 QBDI::InstrRuleDataCBK::lambdaCbK (C++ member), 102  
 QBDI::InstrRuleDataCBK::position (C++ member), 102  
 QBDI::InstrRuleDataCBK::priority (C++ member), 102  
 QBDI::InstructionInRange::InstructionInRange (C++ function), 183  
 QBDI::JumpEpilogue::JumpEpilogue (C++ function), 187  
 QBDI::LoadReg::LoadReg (C++ function), 184  
 QBDI::LogPriority (C++ enum), 114  
 QBDI::LogPriority::DEBUG (C++ enumerator), 114  
 QBDI::LogPriority::DISABLE (C++ enumerator), 114  
 QBDI::LogPriority::ERROR (C++ enumerator), 114  
 QBDI::LogPriority::INFO (C++ enumerator), 114  
 QBDI::LogPriority::WARNING (C++ enumerator), 114  
 QBDI::MemoryAccess (C++ struct), 109  
 QBDI::MemoryAccess::accessAddress (C++ member), 109  
 QBDI::MemoryAccess::flags (C++ member), 109  
 QBDI::MemoryAccess::instAddress (C++ member), 109

[QBDI::MemoryAccess::size \(C++ member\), 109](#)  
[QBDI::MemoryAccess::type \(C++ member\), 109](#)  
[QBDI::MemoryAccess::value \(C++ member\), 109](#)  
[QBDI::MemoryAccessFlags \(C++ enum\), 109](#)  
[QBDI::MemoryAccessFlags::MEMORY\\_MINIMUM\\_SIZE \(C++ enumerator\), 110](#)  
[QBDI::MemoryAccessFlags::MEMORY\\_NO\\_FLAGS \(C++ enumerator\), 110](#)  
[QBDI::MemoryAccessFlags::MEMORY\\_UNKNOWN\\_SIZE \(C++ enumerator\), 110](#)  
[QBDI::MemoryAccessFlags::MEMORY\\_UNKNOWN\\_VALUE \(C++ enumerator\), 110](#)  
[QBDI::MemoryAccessType \(C++ enum\), 109](#)  
[QBDI::MemoryAccessType::MEMORY\\_READ \(C++ enumerator\), 109](#)  
[QBDI::MemoryAccessType::MEMORY\\_READ\\_WRITE \(C++ enumerator\), 109](#)  
[QBDI::MemoryAccessType::MEMORY\\_WRITE \(C++ enumerator\), 109](#)  
[QBDI::MemoryMap \(C++ struct\), 113](#)  
[QBDI::MemoryMap::name \(C++ member\), 113](#)  
[QBDI::MemoryMap::permission \(C++ member\), 113](#)  
[QBDI::MemoryMap::range \(C++ member\), 113](#)  
[QBDI::MMSTReg \(C++ struct\), 98](#)  
[QBDI::MMSTReg::reg \(C++ member\), 99](#)  
[QBDI::MMSTReg::rsrv \(C++ member\), 99](#)  
[QBDI::ModifyInstruction::ModifyInstruction \(C++ function\), 186](#)  
[QBDI::Not::Not \(C++ function\), 183](#)  
[QBDI::Offset \(C++ struct\), 175](#)  
[QBDI::Offset::Offset \(C++ function\), 176](#)  
[QBDI::Offset::operator int64\\_t \(C++ function\), 176](#)  
[QBDI::Operand \(C++ struct\), 176](#)  
[QBDI::Operand::Operand \(C++ function\), 176](#)  
[QBDI::Operand::operator unsigned int \(C++ function\), 176](#)  
[QBDI::OperandAnalysis \(C++ struct\), 107](#)  
[QBDI::OperandAnalysis::flag \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::regAccess \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::regCtxIdx \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::regName \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::regOff \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::size \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::type \(C++ member\), 107](#)  
[QBDI::OperandAnalysis::value \(C++ member\), 107](#)  
[QBDI::OperandFlag \(C++ enum\), 108](#)  
[QBDI::OperandFlag::OPERANDFLAG\\_ADDR \(C++ enumerator\), 108](#)  
[QBDI::OperandFlag::OPERANDFLAG\\_IMPLICIT \(C++ enumerator\), 108](#)  
[QBDI::OperandFlag::OPERANDFLAG\\_NONE \(C++ enumerator\), 108](#)  
[QBDI::OperandFlag::OPERANDFLAG\\_PCREL \(C++ enumerator\), 108](#)  
[QBDI::OperandFlag::OPERANDFLAG\\_UNDEFINED\\_EFFECT \(C++ enumerator\), 108](#)  
[QBDI::OperandType \(C++ enum\), 108](#)  
[QBDI::OperandType::OPERAND\\_FPR \(C++ enumerator\), 108](#)  
[QBDI::OperandType::OPERAND\\_GPR \(C++ enumerator\), 108](#)  
[QBDI::OperandType::OPERAND\\_IMM \(C++ enumerator\), 108](#)  
[QBDI::OperandType::OPERAND\\_INVALID \(C++ enumerator\), 108](#)  
[QBDI::OperandType::OPERAND\\_PRED \(C++ enumerator\), 108](#)  
[QBDI::OperandType::OPERAND\\_SEG \(C++ enumerator\), 108](#)  
[QBDI::OpIs::OpIs \(C++ function\), 183](#)  
[QBDI::Options \(C++ enum\), 113](#)  
[QBDI::Options::NO\\_OPT \(C++ enumerator\), 113](#)  
[QBDI::Options::OPT\\_ATT\\_SYNTAX \(C++ enumerator\), 114](#)  
[QBDI::Options::OPT\\_DISABLE\\_FPR \(C++ enumerator\), 113](#)  
[QBDI::Options::OPT\\_DISABLE\\_OPTIONAL\\_FPR \(C++ enumerator\), 113](#)  
[QBDI::Options::OPT\\_ENABLE\\_FS\\_GS \(C++ enumerator\), 114](#)  
[QBDI::Or::Or \(C++ function\), 183](#)  
[QBDI::PatchRule \(C++ class\), 177](#)  
[QBDI::PatchRule::canBeApplied \(C++ function\), 177](#)  
[QBDI::PatchRule::generate \(C++ function\), 177](#)  
[QBDI::PatchRule::PatchRule \(C++ function\), 177](#)  
[QBDI::Permission \(C++ enum\), 113](#)  
[QBDI::Permission::PF\\_EXEC \(C++ enumerator\), 113](#)  
[QBDI::Permission::PF\\_NONE \(C++ enumerator\), 113](#)  
[QBDI::Permission::PF\\_READ \(C++ enumerator\), 113](#)  
[QBDI::Permission::PF\\_WRITE \(C++ enumerator\), 113](#)  
[QBDI::Range \(C++ class\), 115](#)  
[QBDI::Range::contains \(C++ function\), 115, 116](#)  
[QBDI::Range::display \(C++ function\), 116](#)  
[QBDI::Range::end \(C++ function\), 115](#)  
[QBDI::Range::intersect \(C++ function\), 116](#)  
[QBDI::Range::operator== \(C++ function\), 115](#)  
[QBDI::Range::overlaps \(C++ function\), 116](#)  
[QBDI::Range::Range \(C++ function\), 115](#)  
[QBDI::Range::setEnd \(C++ function\), 115](#)  
[QBDI::Range::setStart \(C++ function\), 115](#)  
[QBDI::Range::size \(C++ function\), 115](#)

QBDI::Range::start (C++ function), 115  
 QBDI::RangeSet (C++ class), 116  
 QBDI::RangeSet::add (C++ function), 116  
 QBDI::RangeSet::clear (C++ function), 117  
 QBDI::RangeSet::contains (C++ function), 116  
 QBDI::RangeSet::display (C++ function), 117  
 QBDI::RangeSet::getRanges (C++ function), 116  
 QBDI::RangeSet::intersect (C++ function), 117  
 QBDI::RangeSet::operator== (C++ function), 117  
 QBDI::RangeSet::overlaps (C++ function), 116  
 QBDI::RangeSet::RangeSet (C++ function), 116  
 QBDI::RangeSet::remove (C++ function), 116  
 QBDI::RangeSet::size (C++ function), 116  
 QBDI::Reg (C++ struct), 174  
 QBDI::Reg::getID (C++ function), 174  
 QBDI::Reg::offset (C++ function), 175  
 QBDI::Reg::operator unsigned int (C++ function), 174  
 QBDI::Reg::Reg (C++ function), 174  
 QBDI::RegisterAccessType (C++ enum), 108  
 QBDI::RegisterAccessType::REGISTER\_READ (C++ enumerator), 108  
 QBDI::RegisterAccessType::REGISTER\_READ\_WRITE (C++ enumerator), 109  
 QBDI::RegisterAccessType::REGISTER\_UNUSED (C++ enumerator), 108  
 QBDI::RegisterAccessType::REGISTER\_WRITE (C++ enumerator), 109  
 QBDI::RemoveOperand::RemoveOperand (C++ function), 188  
 QBDI::rword (C++ type), 95  
 QBDI::SaveReg::SaveReg (C++ function), 184  
 QBDI::setLogConsole (C++ function), 115  
 QBDI::setLogDefault (C++ function), 115  
 QBDI::setLogFile (C++ function), 115  
 QBDI::setLogPriority (C++ function), 115  
 QBDI::SetOpcode::SetOpcode (C++ function), 188  
 QBDI::SetOperand::SetOperand (C++ function), 187, 188  
 QBDI::Shadow (C++ struct), 175  
 QBDI::Shadow::getTag (C++ function), 175  
 QBDI::Shadow::Shadow (C++ function), 175  
 QBDI::simulateCall (C++ function), 112  
 QBDI::SimulateCall::SimulateCall (C++ function), 187  
 QBDI::simulateCallA (C++ function), 112  
 QBDI::simulateCallV (C++ function), 112  
 QBDI::SimulateRet::SimulateRet (C++ function), 187  
 QBDI::SubstituteWithTemp::SubstituteWithTemp (C++ function), 188  
 QBDI::Temp (C++ struct), 175  
 QBDI::Temp::operator unsigned int (C++ function), 175  
 QBDI::Temp::Temp (C++ function), 175  
 QBDI::True::True (C++ function), 183  
 QBDI::UseReg::UseReg (C++ function), 183  
 QBDI::VM (C++ class), 84  
 QBDI::VM::addCodeAddrCB (C++ function), 87  
 QBDI::VM::addCodeCB (C++ function), 86, 87  
 QBDI::VM::addCodeRangeCB (C++ function), 87, 88  
 QBDI::VM::addInstrRule (C++ function), 91  
 QBDI::VM::addInstrRuleRange (C++ function), 92  
 QBDI::VM::addInstrRuleRangeSet (C++ function), 92  
 QBDI::VM::addInstrumentedModule (C++ function), 85  
 QBDI::VM::addInstrumentedModuleFromAddr (C++ function), 85  
 QBDI::VM::addInstrumentedRange (C++ function), 85  
 QBDI::VM::addMemAccessCB (C++ function), 89  
 QBDI::VM::addMemAddrCB (C++ function), 90  
 QBDI::VM::addMemRangeCB (C++ function), 90, 91  
 QBDI::VM::addMnemonicCB (C++ function), 88  
 QBDI::VM::addVMEventCB (C++ function), 89  
 QBDI::VM::call (C++ function), 93  
 QBDI::VM::callA (C++ function), 94  
 QBDI::VM::callV (C++ function), 94  
 QBDI::VM::clearAllCache (C++ function), 95  
 QBDI::VM::clearCache (C++ function), 95  
 QBDI::VM::deleteAllInstrumentations (C++ function), 93  
 QBDI::VM::deleteInstrumentation (C++ function), 93  
 QBDI::VM::getBBMemoryAccess (C++ function), 95  
 QBDI::VM::getCachedInstAnalysis (C++ function), 94  
 QBDI::VM::getFPRState (C++ function), 85  
 QBDI::VM::getGPRState (C++ function), 85  
 QBDI::VM::getInstAnalysis (C++ function), 94  
 QBDI::VM::getInstMemoryAccess (C++ function), 95  
 QBDI::VM::getOptions (C++ function), 85  
 QBDI::VM::instrumentAllExecutableMaps (C++ function), 86  
 QBDI::VM::operator= (C++ function), 84  
 QBDI::VM::precacheBasicBlock (C++ function), 95  
 QBDI::VM::recordMemoryAccess (C++ function), 95  
 QBDI::VM::removeAllInstrumentedRanges (C++ function), 86  
 QBDI::VM::removeInstrumentedModule (C++ function), 86  
 QBDI::VM::removeInstrumentedModuleFromAddr (C++ function), 86  
 QBDI::VM::removeInstrumentedRange (C++ function), 86  
 QBDI::VM::run (C++ function), 93  
 QBDI::VM::setFPRState (C++ function), 85



QBDI::VM::setGPRState (C++ function), 85  
 QBDI::VM::setOptions (C++ function), 85  
 QBDI::VM::VM (C++ function), 84  
 QBDI::VMAction (C++ enum), 103  
 QBDI::VMAction::BREAK\_TO\_VM (C++ enumerator), 104  
 QBDI::VMAction::CONTINUE (C++ enumerator), 103  
 QBDI::VMAction::SKIP\_INST (C++ enumerator), 103  
 QBDI::VMAction::SKIP\_PATCH (C++ enumerator), 103  
 QBDI::VMAction::STOP (C++ enumerator), 104  
 QBDI::VMCallback (C++ type), 101  
 QBDI::VMCbLambda (C++ type), 101  
 QBDI::VMError (C++ enum), 114  
 QBDI::VMError::INVALID\_EVENTID (C++ enumerator), 114  
 QBDI::VMEvent (C++ enum), 110  
 QBDI::VMEvent::BASIC\_BLOCK\_ENTRY (C++ enumerator), 110  
 QBDI::VMEvent::BASIC\_BLOCK\_EXIT (C++ enumerator), 110  
 QBDI::VMEvent::BASIC\_BLOCK\_NEW (C++ enumerator), 110  
 QBDI::VMEvent::EXEC\_TRANSFER\_CALL (C++ enumerator), 110  
 QBDI::VMEvent::EXEC\_TRANSFER\_RETURN (C++ enumerator), 110  
 QBDI::VMEvent::NO\_EVENT (C++ enumerator), 110  
 QBDI::VMEvent::SEQUENCE\_ENTRY (C++ enumerator), 110  
 QBDI::VMEvent::SEQUENCE\_EXIT (C++ enumerator), 110  
 QBDI::VMEvent::SIGNAL (C++ enumerator), 111  
 QBDI::VMEvent::SYSCALL\_ENTRY (C++ enumerator), 110  
 QBDI::VMEvent::SYSCALL\_EXIT (C++ enumerator), 110  
 QBDI::VMInstanceRef (C++ type), 101  
 QBDI::VMState (C++ struct), 111  
 QBDI::VMState::basicBlockEnd (C++ member), 111  
 QBDI::VMState::basicBlockStart (C++ member), 111  
 QBDI::VMState::event (C++ member), 111  
 QBDI::VMState::lastSignal (C++ member), 111  
 QBDI::VMState::sequenceEnd (C++ member), 111  
 QBDI::VMState::sequenceStart (C++ member), 111  
 QBDI::WriteTemp::WriteTemp (C++ function), 184, 185  
 qbdi\_addCodeAddrCB (C++ function), 58  
 qbdi\_addCodeCB (C++ function), 58  
 qbdi\_addCodeRangeCB (C++ function), 58  
 qbdi\_addInstrRule (C++ function), 60  
 qbdi\_addInstrRuleData (C++ function), 70  
 qbdi\_addInstrRuleRange (C++ function), 60  
 qbdi\_addInstrumentedModule (C++ function), 56  
 qbdi\_addInstrumentedModuleFromAddr (C++ function), 56  
 qbdi\_addInstrumentedRange (C++ function), 56  
 qbdi\_addMemAccessCB (C++ function), 59  
 qbdi\_addMemAddrCB (C++ function), 59  
 qbdi\_addMemRangeCB (C++ function), 60  
 qbdi\_addMnemonicCB (C++ function), 58  
 qbdi\_addVMEventCB (C++ function), 59  
 qbdi\_alignedAlloc (C++ function), 80  
 qbdi\_alignedFree (C++ function), 80  
 qbdi\_allocateVirtualStack (C++ function), 80  
 qbdi\_call (C++ function), 61  
 qbdi\_callA (C++ function), 62  
 qbdi\_callV (C++ function), 62  
 qbdi\_clearAllCache (C++ function), 64  
 qbdi\_clearCache (C++ function), 63  
 qbdi\_deleteAllInstrumentations (C++ function), 61  
 qbdi\_deleteInstrumentation (C++ function), 61  
 qbdi\_freeMemoryMapArray (C++ function), 81  
 qbdi\_getBBMemoryAccess (C++ function), 63  
 qbdi\_getCachedInstAnalysis (C++ function), 62  
 qbdi\_getCurrentProcessMaps (C++ function), 81  
 qbdi\_getFPRState (C++ function), 56  
 qbdi\_getGPRState (C++ function), 56  
 qbdi\_getInstAnalysis (C++ function), 62  
 qbdi\_getInstMemoryAccess (C++ function), 63  
 qbdi\_getModuleNames (C++ function), 81  
 qbdi\_getOptions (C++ function), 55  
 qbdi\_getRemoteProcessMaps (C++ function), 81  
 qbdi\_getVersion (C++ function), 83  
 qbdi\_initVM (C++ function), 55  
 qbdi\_instrumentAllExecutableMaps (C++ function), 57  
 QBDI\_LIB\_FULLPATH (None attribute), 153  
 qbdi\_MemoryMap (C++ struct), 81  
 qbdi\_MemoryMap::end (C++ member), 82  
 qbdi\_MemoryMap::name (C++ member), 82  
 qbdi\_MemoryMap::permission (C++ member), 82  
 qbdi\_MemoryMap::start (C++ member), 82  
 qbdi\_Permission (C++ enum), 82  
 qbdi\_Permission::QBDI\_PF\_EXEC (C++ enumerator), 82  
 qbdi\_Permission::QBDI\_PF\_NONE (C++ enumerator), 82  
 qbdi\_Permission::QBDI\_PF\_READ (C++ enumerator), 82  
 qbdi\_Permission::QBDI\_PF\_WRITE (C++ enumerator), 82  
 qbdi\_precacheBasicBlock (C++ function), 63  
 qbdi\_recordMemoryAccess (C++ function), 63  
 qbdi\_removeAllInstrumentedRanges (C++ function), 57

[qbdi\\_removeInstrumentedModule \(C++ function\), 57](#)  
[qbdi\\_removeInstrumentedModuleFromAddr \(C++ function\), 57](#)  
[qbdi\\_removeInstrumentedRange \(C++ function\), 57](#)  
[qbdi\\_run \(C++ function\), 61](#)  
[qbdi\\_setFPRState \(C++ function\), 56](#)  
[qbdi\\_setGPRState \(C++ function\), 56](#)  
[qbdi\\_setLogConsole \(C++ function\), 84](#)  
[qbdi\\_setLogDefault \(C++ function\), 84](#)  
[qbdi\\_setLogFile \(C++ function\), 83](#)  
[qbdi\\_setLogPriority \(C++ function\), 84](#)  
[qbdi\\_setOptions \(C++ function\), 55](#)  
[qbdi\\_simulateCall \(C++ function\), 80](#)  
[qbdi\\_simulateCallA \(C++ function\), 80](#)  
[qbdi\\_simulateCallV \(C++ function\), 80](#)  
[qbdi\\_terminateVM \(C++ function\), 55](#)  
[QBDIPRELOAD\\_ERR\\_STARTUP\\_FAILED \(C macro\), 155](#)  
[qbdipreload\\_floatCtxToFPRState \(C++ function\), 157](#)  
[qbdipreload\\_hook\\_main \(C++ function\), 156](#)  
[QBDIPRELOAD\\_INIT \(C macro\), 155](#)  
[QBDIPRELOAD\\_NO\\_ERROR \(C macro\), 155](#)  
[QBDIPRELOAD\\_NOT\\_HANDLED \(C macro\), 155](#)  
[qbdipreload\\_on\\_exit \(C++ function\), 156](#)  
[qbdipreload\\_on\\_main \(C++ function\), 156](#)  
[qbdipreload\\_on\\_premain \(C++ function\), 155](#)  
[qbdipreload\\_on\\_run \(C++ function\), 156](#)  
[qbdipreload\\_on\\_start \(C++ function\), 155](#)  
[qbdipreload\\_threadCtxToGPRState \(C++ function\), 156](#)

## R

[r10 \(pyqbd.GPRState property\), 121](#)  
[r11 \(pyqbd.GPRState property\), 121](#)  
[r12 \(pyqbd.GPRState property\), 121](#)  
[r13 \(pyqbd.GPRState property\), 121](#)  
[r14 \(pyqbd.GPRState property\), 121](#)  
[r15 \(pyqbd.GPRState property\), 121](#)  
[r8 \(pyqbd.GPRState property\), 121](#)  
[r9 \(pyqbd.GPRState property\), 121](#)  
[Range \(class in pyqbd\), 133](#)  
[range \(pyqbd.MemoryMap property\), 131](#)  
[rax \(pyqbd.GPRState property\), 122](#)  
[rbp \(pyqbd.GPRState property\), 122](#)  
[rbx \(pyqbd.GPRState property\), 122](#)  
[rcx \(pyqbd.GPRState property\), 122](#)  
[rdi \(pyqbd.GPRState property\), 122](#)  
[rdx \(pyqbd.GPRState property\), 122](#)  
[readMemory\(\) \(in module pyqbd\), 133](#)  
[readRword\(\) \(in module pyqbd\), 133](#)  
[recordMemoryAccess\(\) \(in module pyqbd.VM\), 120](#)  
[REG\\_BP \(built-in variable\), 69](#)  
[REG\\_BP \(pyqbd.GPRState property\), 121](#)  
[REG\\_FLAG \(pyqbd.GPRState property\), 121](#)

[REG\\_LR \(pyqbd.GPRState property\), 121](#)  
[REG\\_PC \(built-in variable\), 69](#)  
[REG\\_PC \(None attribute\), 146](#)  
[REG\\_PC \(pyqbd.GPRState property\), 121](#)  
[REG\\_RETURN \(built-in variable\), 69](#)  
[REG\\_RETURN \(None attribute\), 146](#)  
[REG\\_RETURN \(pyqbd.GPRState property\), 121](#)  
[REG\\_SP \(built-in variable\), 69](#)  
[REG\\_SP \(None attribute\), 146](#)  
[REG\\_SP \(pyqbd.GPRState property\), 121](#)  
[regAccess \(pyqbd.OperandAnalysis property\), 128](#)  
[regCtxIdx \(pyqbd.OperandAnalysis property\), 128](#)  
[RegisterAccessType \(C++ enum\), 77](#)  
[RegisterAccessType \(in module pyqbd\), 129](#)  
[RegisterAccessType\(\) \(class\), 151](#)  
[RegisterAccessType.REGISTER\\_READ \(RegisterAccessType attribute\), 151](#)  
[RegisterAccessType.REGISTER\\_READ\\_WRITE \(RegisterAccessType attribute\), 151](#)  
[RegisterAccessType.REGISTER\\_WRITE \(RegisterAccessType attribute\), 151](#)  
[RegisterAccessType::QBDI\\_REGISTER\\_READ \(C++ enumerator\), 77](#)  
[RegisterAccessType::QBDI\\_REGISTER\\_READ\\_WRITE \(C++ enumerator\), 77](#)  
[RegisterAccessType::QBDI\\_REGISTER\\_UNUSED \(C++ enumerator\), 77](#)  
[RegisterAccessType::QBDI\\_REGISTER\\_WRITE \(C++ enumerator\), 77](#)  
[regName \(pyqbd.OperandAnalysis property\), 129](#)  
[regOff \(pyqbd.OperandAnalysis property\), 129](#)  
[removeAllInstrumentedRanges\(\) \(in module pyqbd.VM\), 118](#)  
[removeInstrumentedModule\(\) \(in module pyqbd.VM\), 118](#)  
[removeInstrumentedModuleFromAddr\(\) \(in module pyqbd.VM\), 118](#)  
[removeInstrumentedRange\(\) \(in module pyqbd.VM\), 118](#)  
[rfcw \(pyqbd.FPRState property\), 122](#)  
[rfsw \(pyqbd.FPRState property\), 122](#)  
[rip \(pyqbd.GPRState property\), 122](#)  
[rsi \(pyqbd.GPRState property\), 122](#)  
[rsp \(pyqbd.GPRState property\), 122](#)  
[run\(\) \(in module pyqbd.VM\), 120](#)  
[rword \(C++ type\), 64](#)  
[rword \(None attribute\), 154](#)

## S

[sequenceEnd \(pyqbd.VMState property\), 131](#)  
[sequenceStart \(pyqbd.VMState property\), 131](#)  
[setFPRState\(\) \(in module pyqbd.VM\), 118](#)  
[setGPRState\(\) \(in module pyqbd.VM\), 118](#)  
[setLogPriority\(\) \(in module pyqbd\), 133](#)

[simulateCall\(\)](#) (in module *pyqbd*), 131  
[size](#) (*pyqbd.MemoryAccess* property), 130  
[size](#) (*pyqbd.OperandAnalysis* property), 129  
[size\(\)](#) (*pyqbd.Range* method), 133  
[start](#) (*pyqbd.Range* property), 133  
[stmm0](#) (*pyqbd.FPRState* property), 122  
[stmm1](#) (*pyqbd.FPRState* property), 122  
[stmm2](#) (*pyqbd.FPRState* property), 122  
[stmm3](#) (*pyqbd.FPRState* property), 122  
[stmm4](#) (*pyqbd.FPRState* property), 123  
[stmm5](#) (*pyqbd.FPRState* property), 123  
[stmm6](#) (*pyqbd.FPRState* property), 123  
[stmm7](#) (*pyqbd.FPRState* property), 123  
[storeSize](#) (*pyqbd.InstAnalysis* property), 128  
[symbol](#) (*pyqbd.InstAnalysis* property), 128  
[symbolOffset](#) (*pyqbd.InstAnalysis* property), 128  
[SyncDirection\(\)](#) (class), 146  
[SyncDirection.FRIDA\\_TO\\_QBDI](#) (*SyncDirection* attribute), 146  
[SyncDirection.QBDI\\_TO\\_FRIDA](#) (*SyncDirection* attribute), 146

## T

[type](#) (*pyqbd.MemoryAccess* property), 130  
[type](#) (*pyqbd.OperandAnalysis* property), 129

## U

[UInt64.prototype.toRword\(\)](#) (*UInt64.prototype* method), 154

## V

[value](#) (*pyqbd.MemoryAccess* property), 130  
[value](#) (*pyqbd.OperandAnalysis* property), 129  
[VM](#) (class in *pyqbd*), 117  
[VMAction](#) (C++ enum), 71  
[VMAction](#) (in module *pyqbd*), 126  
[VMAction\(\)](#) (class), 147  
[VMAction.BREAK\\_TO\\_VM](#) (*VMAction* attribute), 148  
[VMAction.CONTINUE](#) (*VMAction* attribute), 147  
[VMAction.SKIP\\_INST](#) (*VMAction* attribute), 147  
[VMAction.SKIP\\_PATCH](#) (*VMAction* attribute), 147  
[VMAction.STOP](#) (*VMAction* attribute), 148  
[VMAction::QBDI\\_BREAK\\_TO\\_VM](#) (C++ enumerator), 72  
[VMAction::QBDI\\_CONTINUE](#) (C++ enumerator), 71  
[VMAction::QBDI\\_SKIP\\_INST](#) (C++ enumerator), 71  
[VMAction::QBDI\\_SKIP\\_PATCH](#) (C++ enumerator), 72  
[VMAction::QBDI\\_STOP](#) (C++ enumerator), 72  
[VMCallback](#) (C++ type), 70  
[VMCallback\(\)](#) (built-in function), 147  
[VMErr](#) (C++ enum), 83  
[VMErr](#) (in module *pyqbd*), 132  
[VMErr\(\)](#) (class), 154  
[VMErr.INVALID\\_EVENTID](#) (*VMErr* attribute), 154

[VMErr::QBDI\\_INVALID\\_EVENTID](#) (C++ enumerator), 83  
[VMEvent](#) (C++ enum), 78  
[VMEvent](#) (in module *pyqbd*), 130  
[VMEvent\(\)](#) (class), 152  
[VMEvent.BASIC\\_BLOCK\\_ENTRY](#) (*VMEvent* attribute), 152  
[VMEvent.BASIC\\_BLOCK\\_EXIT](#) (*VMEvent* attribute), 153  
[VMEvent.BASIC\\_BLOCK\\_NEW](#) (*VMEvent* attribute), 153  
[VMEvent.EXEC\\_TRANSFER\\_CALL](#) (*VMEvent* attribute), 153  
[VMEvent.EXEC\\_TRANSFER\\_RETURN](#) (*VMEvent* attribute), 153  
[VMEvent.SEQUENCE\\_ENTRY](#) (*VMEvent* attribute), 152  
[VMEvent.SEQUENCE\\_EXIT](#) (*VMEvent* attribute), 152  
[VMEvent.SIGNAL](#) (*VMEvent* attribute), 153  
[VMEvent.SYSCALL\\_ENTRY](#) (*VMEvent* attribute), 153  
[VMEvent.SYSCALL\\_EXIT](#) (*VMEvent* attribute), 153  
[VMEvent::QBDI\\_BASIC\\_BLOCK\\_ENTRY](#) (C++ enumerator), 78  
[VMEvent::QBDI\\_BASIC\\_BLOCK\\_EXIT](#) (C++ enumerator), 78  
[VMEvent::QBDI\\_BASIC\\_BLOCK\\_NEW](#) (C++ enumerator), 78  
[VMEvent::QBDI\\_EXEC\\_TRANSFER\\_CALL](#) (C++ enumerator), 79  
[VMEvent::QBDI\\_EXEC\\_TRANSFER\\_RETURN](#) (C++ enumerator), 79  
[VMEvent::QBDI\\_NO\\_EVENT](#) (C++ enumerator), 78  
[VMEvent::QBDI\\_SEQUENCE\\_ENTRY](#) (C++ enumerator), 78  
[VMEvent::QBDI\\_SEQUENCE\\_EXIT](#) (C++ enumerator), 78  
[VMEvent::QBDI\\_SIGNAL](#) (C++ enumerator), 79  
[VMEvent::QBDI\\_SYSCALL\\_ENTRY](#) (C++ enumerator), 79  
[VMEvent::QBDI\\_SYSCALL\\_EXIT](#) (C++ enumerator), 79  
[VMInstanceRef](#) (C++ type), 55  
[VMState](#) (C++ struct), 79  
[VMState](#) (class in *pyqbd*), 130  
[VMState\(\)](#) (class), 153  
[VMState.basicBlockEnd](#) (*VMState* attribute), 153  
[VMState.basicBlockStart](#) (*VMState* attribute), 153  
[VMState.event](#) (*VMState* attribute), 153  
[VMState.lastSignal](#) (*VMState* attribute), 153  
[VMState.sequenceEnd](#) (*VMState* attribute), 153  
[VMState.sequenceStart](#) (*VMState* attribute), 153  
[VMState::basicBlockEnd](#) (C++ member), 79  
[VMState::basicBlockStart](#) (C++ member), 79  
[VMState::event](#) (C++ member), 79  
[VMState::lastSignal](#) (C++ member), 79  
[VMState::sequenceEnd](#) (C++ member), 79  
[VMState::sequenceStart](#) (C++ member), 79

## W

`writeMemory()` (in module *pyqbd*), 134

`writeRword()` (in module *pyqbd*), 134

## X

`xmm0` (*pyqbd.FPRState* property), 123

`xmm1` (*pyqbd.FPRState* property), 123

`xmm10` (*pyqbd.FPRState* property), 123

`xmm11` (*pyqbd.FPRState* property), 123

`xmm12` (*pyqbd.FPRState* property), 123

`xmm13` (*pyqbd.FPRState* property), 123

`xmm14` (*pyqbd.FPRState* property), 123

`xmm15` (*pyqbd.FPRState* property), 123

`xmm2` (*pyqbd.FPRState* property), 123

`xmm3` (*pyqbd.FPRState* property), 123

`xmm4` (*pyqbd.FPRState* property), 123

`xmm5` (*pyqbd.FPRState* property), 123

`xmm6` (*pyqbd.FPRState* property), 123

`xmm7` (*pyqbd.FPRState* property), 123

`xmm8` (*pyqbd.FPRState* property), 123

`xmm9` (*pyqbd.FPRState* property), 123

## Y

`ymm0` (*pyqbd.FPRState* property), 123

`ymm1` (*pyqbd.FPRState* property), 124

`ymm10` (*pyqbd.FPRState* property), 124

`ymm11` (*pyqbd.FPRState* property), 124

`ymm12` (*pyqbd.FPRState* property), 124

`ymm13` (*pyqbd.FPRState* property), 124

`ymm14` (*pyqbd.FPRState* property), 124

`ymm15` (*pyqbd.FPRState* property), 124

`ymm2` (*pyqbd.FPRState* property), 124

`ymm3` (*pyqbd.FPRState* property), 124

`ymm4` (*pyqbd.FPRState* property), 124

`ymm5` (*pyqbd.FPRState* property), 124

`ymm6` (*pyqbd.FPRState* property), 124

`ymm7` (*pyqbd.FPRState* property), 124

`ymm8` (*pyqbd.FPRState* property), 124

`ymm9` (*pyqbd.FPRState* property), 124