iSEC
information security inc.

FAME

Information Security Inc.

Contents

- About FAME
- FAME Architecture
- Testing Environment
- Installing FAME
- Using FAME
- References

About FAME

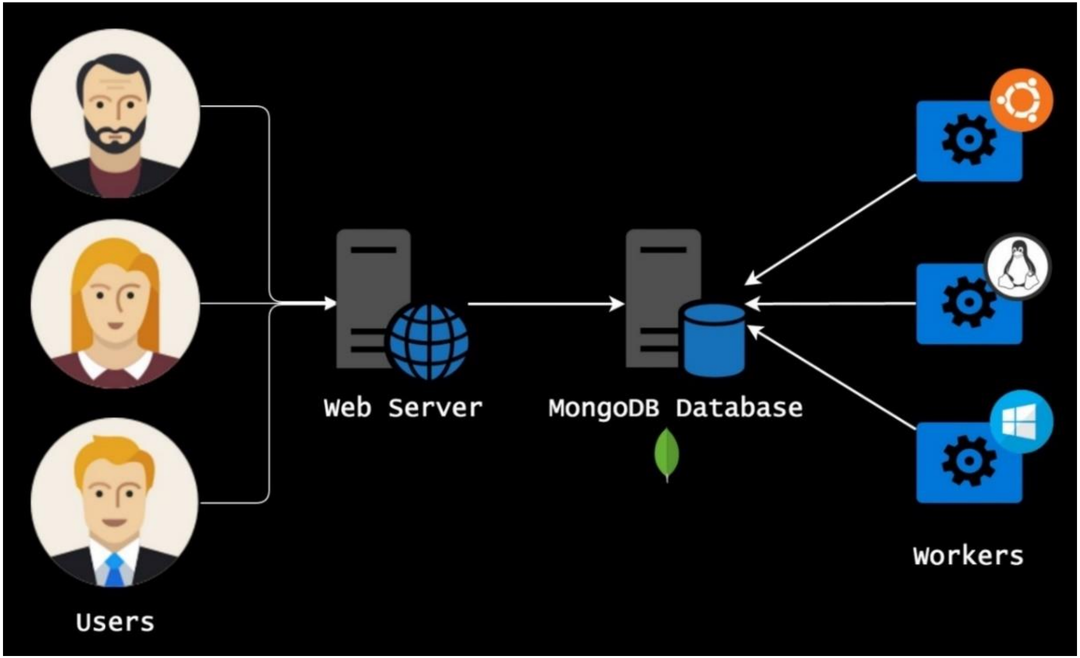
- FAME is a recursive acronym meaning “FAME Automates Malware Evaluation”
- It is meant to facilitate analysis of malicious files, leveraging as much knowledge as possible in order to speed up and automate end-to-end analysis

FAME Architecture

FAME relies on three components:

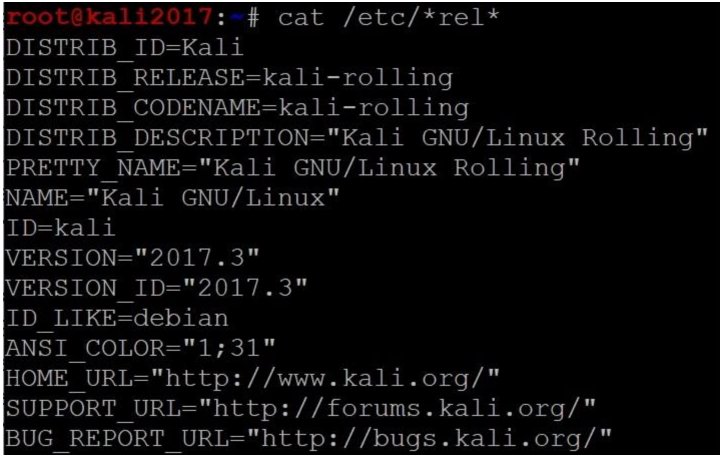
- A MongoDB database, storing everything and serving as a link between other components.
- A web server, that is serving the web application, and exposing internal services.
- Any number of workers (at least 1), which are performing the actual analysis tasks.

FAME Architecture



Testing Environment

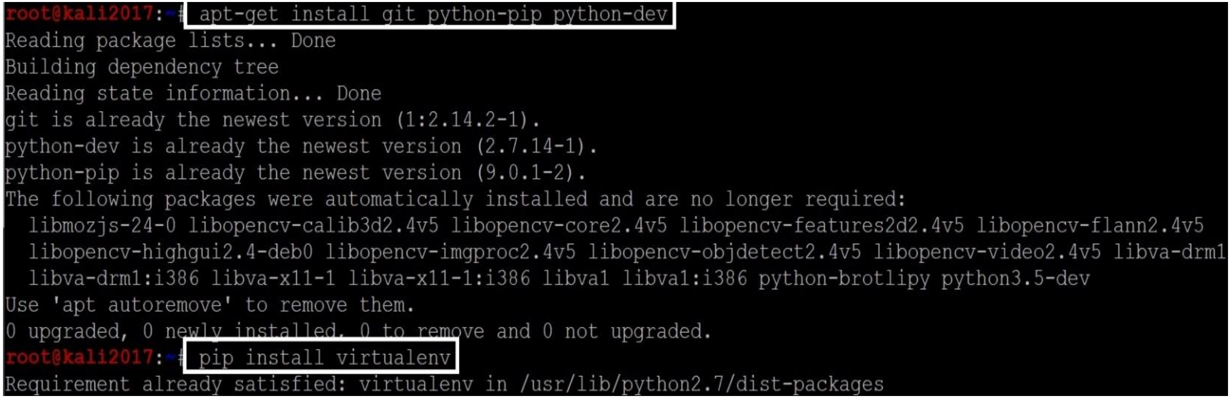
- Kali Linux 2017



```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing FAME

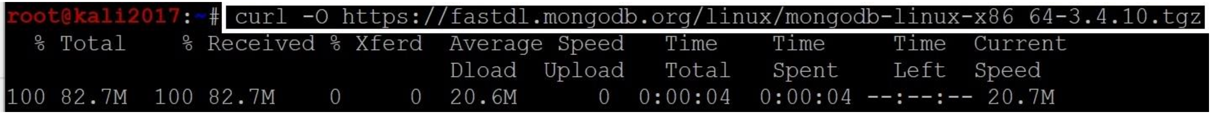
- Installing dependencies



```
root@kali2017:~# apt-get install git python-pip python-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.14.2-1).
python-dev is already the newest version (2.7.14-1).
python-pip is already the newest version (9.0.1-2).
The following packages were automatically installed and are no longer required:
  libmozjs-24-0 libopencv-calib3d2.4v5 libopencv-core2.4v5 libopencv-features2d2.4v5 libopencv-flann2.4v5
  libopencv-highgui2.4-deb0 libopencv-imgproc2.4v5 libopencv-objdetect2.4v5 libopencv-video2.4v5 libva-drm1
  libva-drm1:i386 libva-x11-1 libva-x11-1:i386 libva1 libva1:i386 python-brotlipy python3.5-dev
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali2017:~# pip install virtualenv
Requirement already satisfied: virtualenv in /usr/lib/python2.7/dist-packages
```

Installing FAME

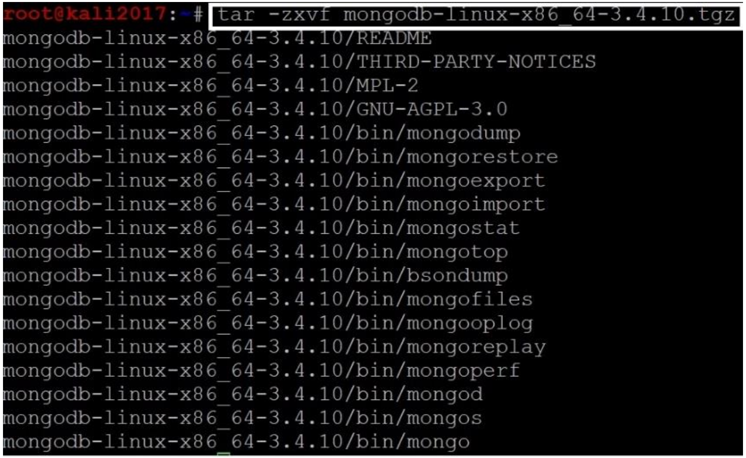
- Installing MongoDB
- Download the binary files for the desired release of MongoDB



```
root@kali2017:~# curl -O https://fastdl.mongodb.org/linux/mongodb-linux-x86 64-3.4.10.tgz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 82.7M  100 82.7M    0     0  20.6M      0  0:00:04  0:00:04 --:--:-- 20.7M
```

Installing FAME

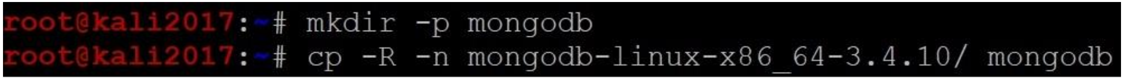
- Installing MongoDB
- Extract the files from the downloaded archive



```
root@kali2017:~# tar -zxvf mongodb-linux-x86_64-3.4.10.tgz
mongodb-linux-x86_64-3.4.10/README
mongodb-linux-x86_64-3.4.10/THIRD-PARTY-NOTICES
mongodb-linux-x86_64-3.4.10/MPL-2
mongodb-linux-x86_64-3.4.10/GNU-AGPL-3.0
mongodb-linux-x86_64-3.4.10/bin/mongodump
mongodb-linux-x86_64-3.4.10/bin/mongorestore
mongodb-linux-x86_64-3.4.10/bin/mongoexport
mongodb-linux-x86_64-3.4.10/bin/mongoimport
mongodb-linux-x86_64-3.4.10/bin/mongostat
mongodb-linux-x86_64-3.4.10/bin/mongotop
mongodb-linux-x86_64-3.4.10/bin/bsondump
mongodb-linux-x86_64-3.4.10/bin/mongofiles
mongodb-linux-x86_64-3.4.10/bin/mongooplog
mongodb-linux-x86_64-3.4.10/bin/mongoreplay
mongodb-linux-x86_64-3.4.10/bin/mongoperf
mongodb-linux-x86_64-3.4.10/bin/mongod
mongodb-linux-x86_64-3.4.10/bin/mongos
mongodb-linux-x86_64-3.4.10/bin/mongo
```

Installing FAME

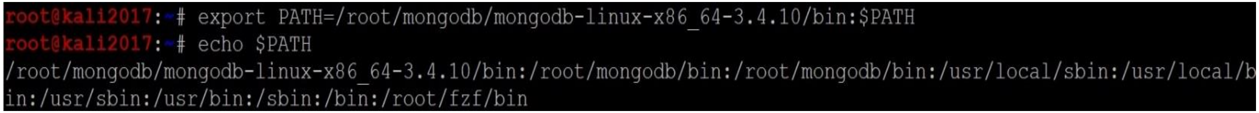
- Installing MongoDB
- Copy the extracted archive to the target directory



```
root@kali2017:~# mkdir -p mongodb
root@kali2017:~# cp -R -n mongodb-linux-x86_64-3.4.10/ mongodb
```

Installing FAME

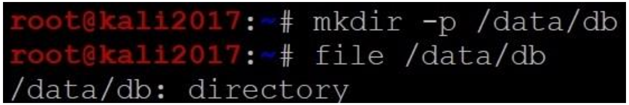
- Installing MongoDB
- Ensure the location of the binaries is in the PATH variable



```
root@kali2017:~# export PATH=/root/mongodb/mongodb-linux-x86_64-3.4.10/bin:$PATH
root@kali2017:~# echo $PATH
/root/mongodb/mongodb-linux-x86_64-3.4.10/bin:/root/mongodb/bin:/root/mongodb/bin:/usr/local/sbin:/usr/local/b
in:/usr/sbin:/usr/bin:/sbin:/bin:/root/fzf/bin
```

Installing FAME

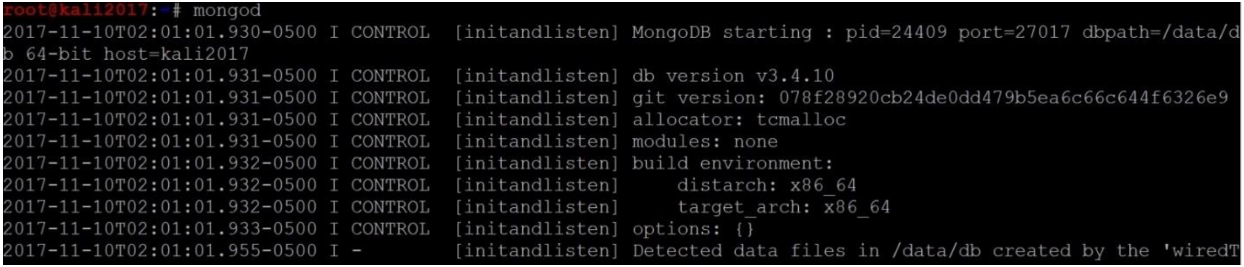
- Run MongoDB
- Create the data directory



```
root@kali2017:~# mkdir -p /data/db
root@kali2017:~# file /data/db
/data/db: directory
```

Installing FAME

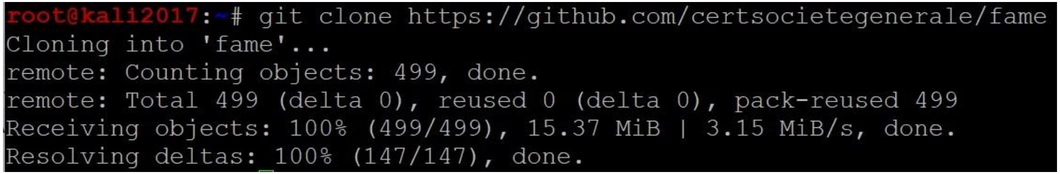
- Run MongoDB



```
root@kali2017:~# mongod
2017-11-10T02:01:01.930-0500 I CONTROL  [initandlisten] MongoDB starting : pid=24409 port=27017 dbpath=/data/d
b 64-bit host=kali2017
2017-11-10T02:01:01.931-0500 I CONTROL  [initandlisten] db version v3.4.10
2017-11-10T02:01:01.931-0500 I CONTROL  [initandlisten] git version: 078f28920cb24de0dd479b5ea6c66c644f6326e9
2017-11-10T02:01:01.931-0500 I CONTROL  [initandlisten] allocator: tcmalloc
2017-11-10T02:01:01.931-0500 I CONTROL  [initandlisten] modules: none
2017-11-10T02:01:01.932-0500 I CONTROL  [initandlisten] build environment:
2017-11-10T02:01:01.932-0500 I CONTROL  [initandlisten]     distarch: x86_64
2017-11-10T02:01:01.932-0500 I CONTROL  [initandlisten]     target_arch: x86_64
2017-11-10T02:01:01.933-0500 I CONTROL  [initandlisten] options: {}
2017-11-10T02:01:01.955-0500 I -        [initandlisten] Detected data files in /data/db created by the 'wiredT
```

Installing FAME

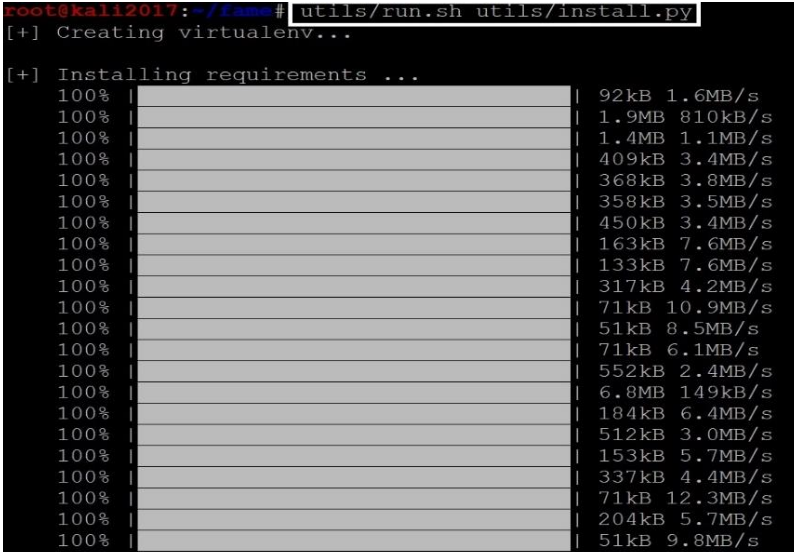
- Clone GitHub repository



```
root@kali2017:~# git clone https://github.com/certsocietegenerale/fame
Cloning into 'fame'...
remote: Counting objects: 499, done.
remote: Total 499 (delta 0), reused 0 (delta 0), pack-reused 499
Receiving objects: 100% (499/499), 15.37 MiB | 3.15 MiB/s, done.
Resolving deltas: 100% (147/147), done.
```

Installing FAME

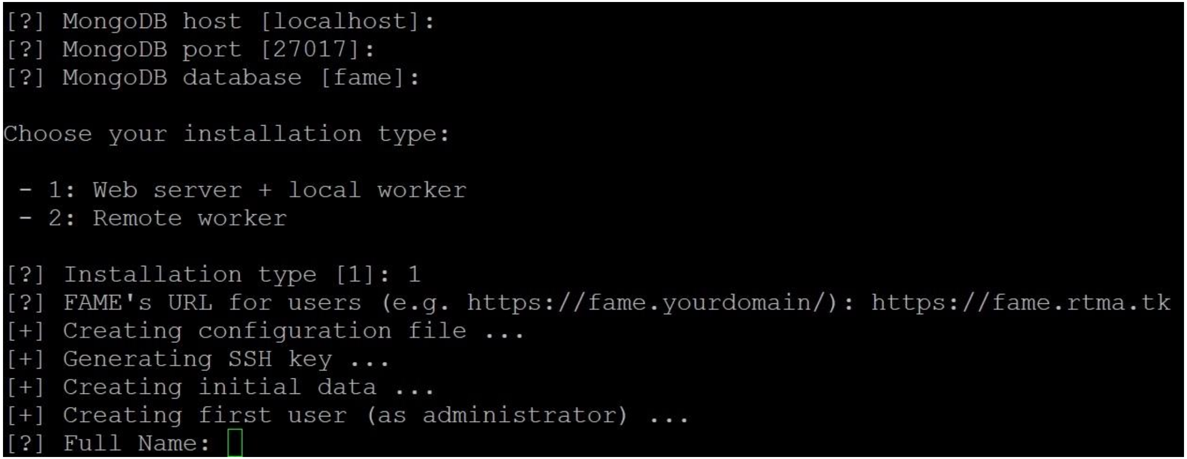
- Run the install script, and answer the questions



```
root@kali2017:~/fame# utils/run.sh utils/install.py
[+] Creating virtualenv...

[+] Installing requirements ...
    100% |████████████████████████████████| 92kB 1.6MB/s
    100% |████████████████████████████████| 1.9MB 810kB/s
    100% |████████████████████████████████| 1.4MB 1.1MB/s
    100% |████████████████████████████████| 409kB 3.4MB/s
    100% |████████████████████████████████| 368kB 3.8MB/s
    100% |████████████████████████████████| 358kB 3.5MB/s
    100% |████████████████████████████████| 450kB 3.4MB/s
    100% |████████████████████████████████| 163kB 7.6MB/s
    100% |████████████████████████████████| 133kB 7.6MB/s
    100% |████████████████████████████████| 317kB 4.2MB/s
    100% |████████████████████████████████| 71kB 10.9MB/s
    100% |████████████████████████████████| 51kB 8.5MB/s
    100% |████████████████████████████████| 71kB 6.1MB/s
    100% |████████████████████████████████| 552kB 2.4MB/s
    100% |████████████████████████████████| 6.8MB 149kB/s
    100% |████████████████████████████████| 184kB 6.4MB/s
    100% |████████████████████████████████| 512kB 3.0MB/s
    100% |████████████████████████████████| 153kB 5.7MB/s
    100% |████████████████████████████████| 337kB 4.4MB/s
    100% |████████████████████████████████| 71kB 12.3MB/s
    100% |████████████████████████████████| 204kB 5.7MB/s
    100% |████████████████████████████████| 51kB 9.8MB/s
```

Installing FAME

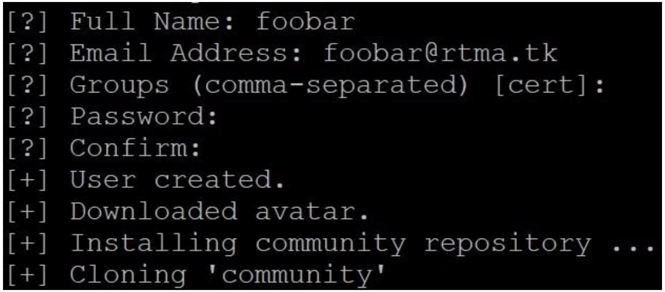
- Run the install script, and answer the questions (choose ‘1’ for installation type)



```
[?] MongoDB host [localhost]:
[?] MongoDB port [27017]:
[?] MongoDB database [fame]:

Choose your installation type:

 - 1: Web server + local worker
 - 2: Remote worker

[?] Installation type [1]: 1
[?] FAME's URL for users (e.g. https://fame.yourdomain/): https://fame.rtma.tk
[+] Creating configuration file ...
[+] Generating SSH key ...
[+] Creating initial data ...
[+] Creating first user (as administrator) ...
[?] Full Name:
```

Installing FAME

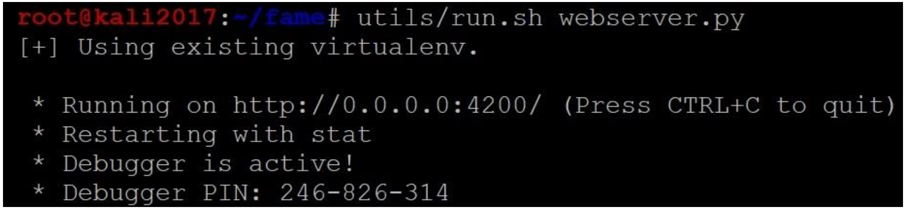
- Run the install script, and answer the questions (choose ‘1’ for installation type)



```
[?] Full Name: foobar
[?] Email Address: foobar@rtma.tk
[?] Groups (comma-separated) [cert]:
[?] Password:
[?] Confirm:
[+] User created.
[+] Downloaded avatar.
[+] Installing community repository ...
[+] Cloning 'community'
```

Using FAME

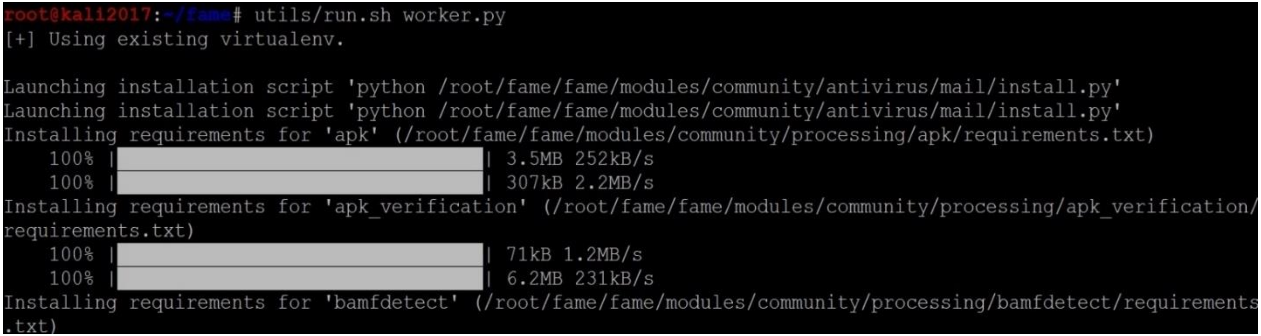
- Running FAME, starting the webserver,



```
root@kali2017:~/fame# utils/run.sh webserver.py
[+] Using existing virtualenv.

 * Running on http://0.0.0.0:4200/ (Press CTRL+C to quit)
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 246-826-314
```

Using FAME

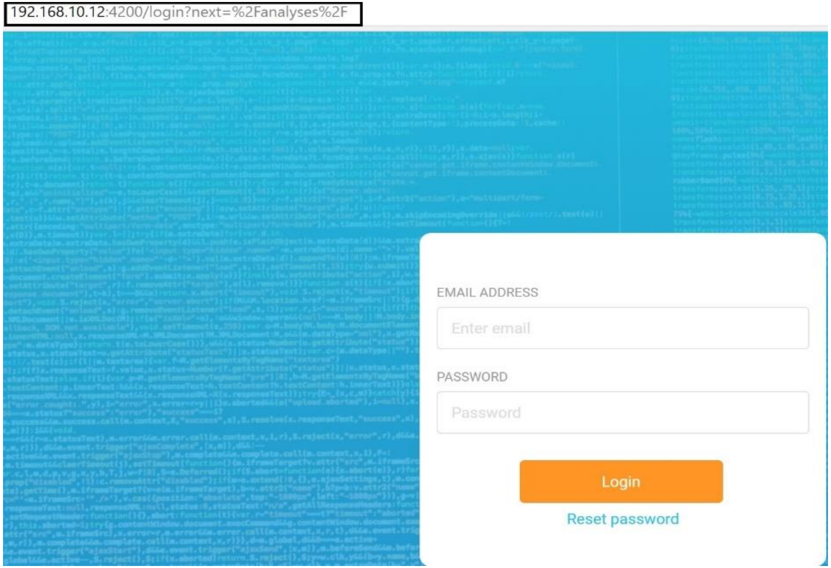
- Running FAME, starting the worker



```
root@kali2017:~/fame# utils/run.sh worker.py
[+] Using existing virtualenv.

Launching installation script 'python /root/fame/fame/modules/community/antivirus/mail/install.py'
Launching installation script 'python /root/fame/fame/modules/community/antivirus/mail/install.py'
Installing requirements for 'apk' (/root/fame/fame/modules/community/processing/apk/requirements.txt)
    100% |████████████████████████████████| 3.5MB 252kB/s
    100% |████████████████████████████████| 307kB 2.2MB/s
Installing requirements for 'apk_verification' (/root/fame/fame/modules/community/processing/apk_verification/
requirements.txt)
    100% |████████████████████████████████| 71kB 1.2MB/s
    100% |████████████████████████████████| 6.2MB 231kB/s
Installing requirements for 'bamfdetect' (/root/fame/fame/modules/community/processing/bamfdetect/requirements
.txt)
```

Using FAME

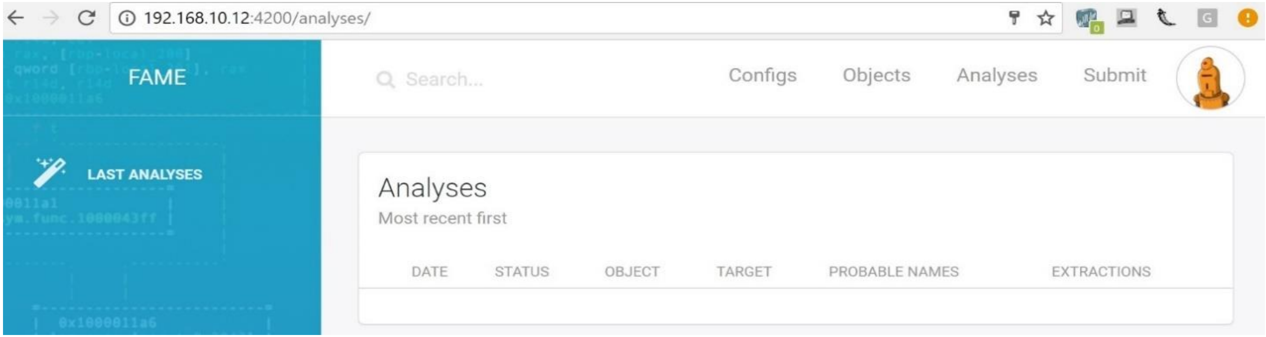
- Accessing FAME



192.168.10.12:4200/login?next=%2Fanalyses%2F

Using FAME

- Accessing FAME



192.168.10.12:4200/analyses/

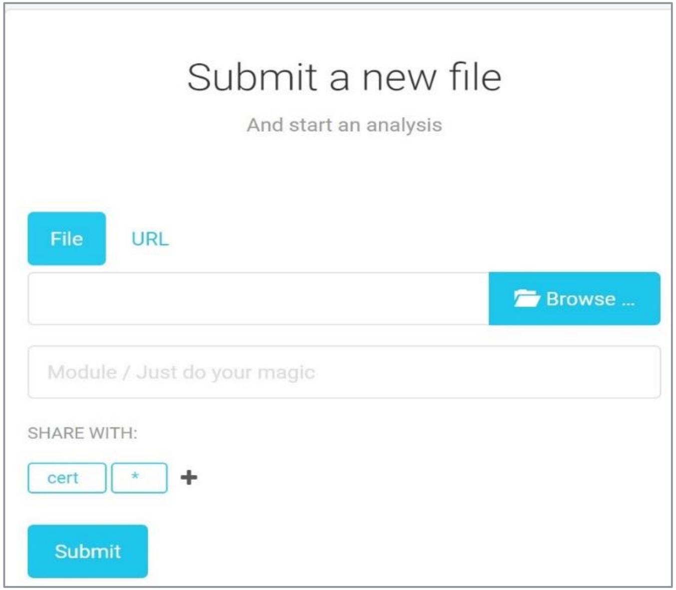
Analyses

Most recent first

DATE	STATUS	OBJECT	TARGET	PROBABLE NAMES	EXTRACTIONS

Using FAME

- Submit a new file



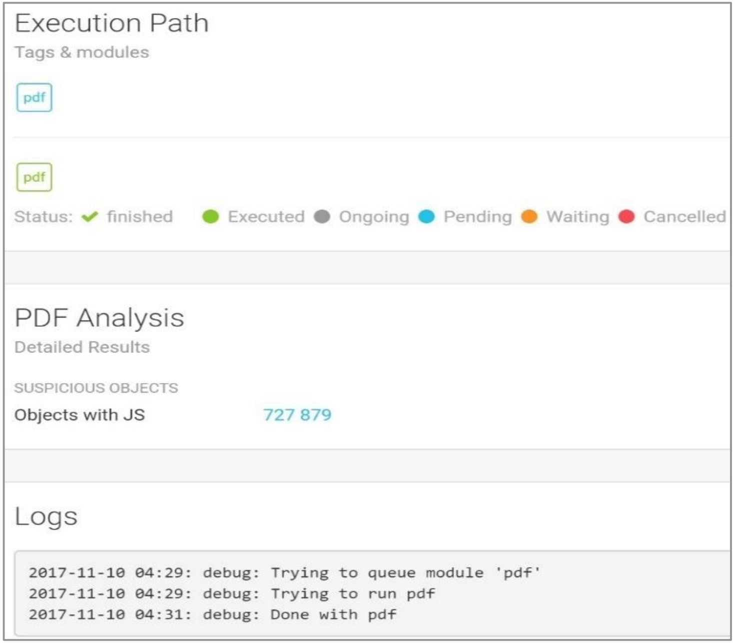
Submit a new file

And start an analysis

SHARE WITH:

Using FAME

- Submit a new file



Execution Path

Tags & modules

Status: ✓ finished ● Executed ● Ongoing ● Pending ● Waiting ● Cancelled

PDF Analysis

Detailed Results

SUSPICIOUS OBJECTS

Objects with JS 727 879

Logs

```
2017-11-10 04:29: debug: Trying to queue module 'pdf'
2017-11-10 04:29: debug: Trying to run pdf
2017-11-10 04:31: debug: Done with pdf
```

References

- FAME

https://certsocietegenerale.github.io/fame/

- Kali Linux

https://www.kali.org/downloads/

- Installing MongoDB

https://docs.mongodb.com/manual/tutorial/install-mongodb-on-linux/