EVOLUTION OF VOLATILITY MEMORY

Adam Aji Purnama
Christian
Kenn Christoval Candra
I Pasek Made Gatha P P
Stephen Mario Wijaya

Table of CONTENT

Introduction

SRAM & DRAM

Volatility GUI

Memory Acquisition

Memory Analysis

Introduction

Volatile Memory => jenis memori komputer yang memerlukan daya untuk mempertahankan data yang disimpan. Hal ini berbeda dengan memori non-volatil, yang dapat menyimpan data bahkan tanpa daya. Memori volatil digunakan di berbagai sistem dan perangkat komputer, termasuk RAM (Random Access Memory) di komputer pribadi dan perangkat seluler, serta memori cache di prosesor.

The Importance of Volatile Memory

Memori volatil memainkan peran penting dalam komputasi modern, karena memungkinkan akses data yang cepat dan efisien. RAM, misalnya, digunakan oleh CPU untuk menyimpan data dan instruksi yang sering diakses, sehingga memungkinkan waktu pemrosesan lebih cepat. Selain itu, memori volatil sering kali digunakan sebagai lokasi penyimpanan sementara untuk data yang pada akhirnya akan ditulis ke memori non-volatil, seperti hard drive atau solid-state drive.

SRAM

SRAM adalah singkatan dari Static Random Access Memory, yang merupakan jenis memori komputer yang mudah menguap. Disebut statis karena tidak perlu di-refresh seperti RAM dinamis (DRAM) dan akses acak karena setiap byte memori dapat diakses tanpa menyentuh byte sebelumnya.

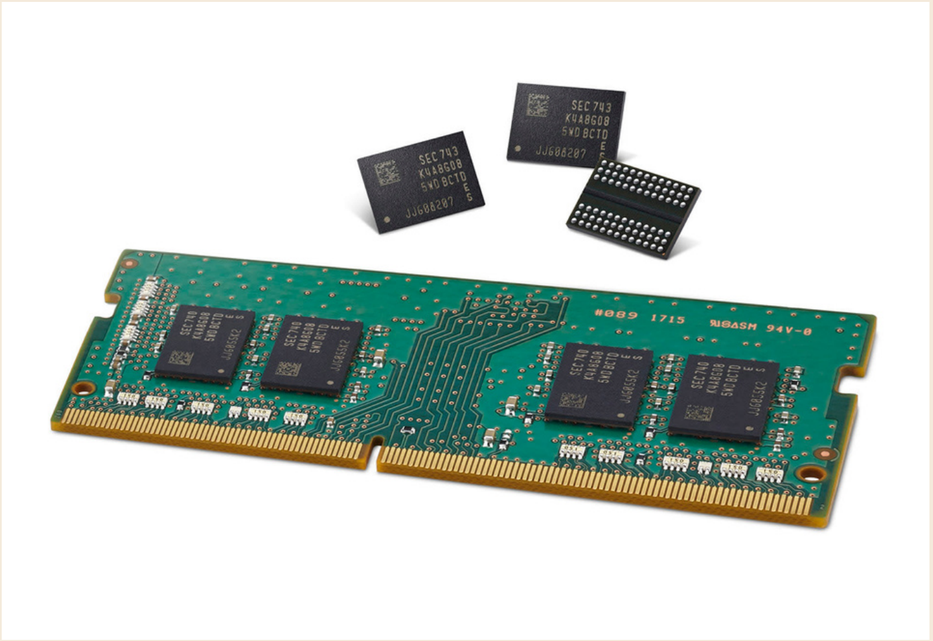
SRAM umumnya digunakan dalam memori cache, yaitu sejumlah kecil memori sangat cepat yang digunakan untuk menyimpan data yang sering diakses. Hal ini juga digunakan dalam mikroprosesor, dimana kecepatan dan konsumsi daya yang rendah lebih menguntungkan.

- **Keunggulan SRAM antara lain waktu akses lebih cepat, konsumsi daya lebih rendah, dan keandalan lebih tinggi dibandingkan DRAM.**

- **Kerugian dari SRAM termasuk biaya yang lebih tinggi dan kepadatan yang lebih rendah dibandingkan dengan DRAM.**

DRAM

Memori Akses Acak Dinamis, atau DRAM, adalah jenis memori volatil yang biasa digunakan di komputer dan perangkat digital lainnya. Ia menyimpan data sebagai serangkaian muatan listrik dalam kapasitor, yang harus terus-menerus disegarkan untuk mempertahankan muatannya. DRAM biasanya lebih cepat dan lebih murah dibandingkan jenis memori lainnya, seperti SRAM atau ROM, namun juga kurang dapat diandalkan dan memiliki konsumsi daya yang lebih tinggi.



Keuntungan dan kerugian

- **Lebih cepat dan lebih murah dibandingkan jenis memori lainnya.**

- **Memerlukan penyegaran terus-menerus, yang dapat meningkatkan konsumsi daya dan menurunkan keandalan.**

MEMORY ACQUISITION

1

Pentingnya analisis memori yang berkualitas tinggi dalam forensik komputer sangat bergantung pada kualitas "memory dump" yang diambil dari sistem tersebut, dan mendapatkan "memory dump" yang berkualitas bukanlah tugas yang mudah.

2

Sebuah gambaran memori dianggap benar jika snapshot hanya berisi nilai-nilai yang ada dalam memori pada saat snapshot diambil. Atomisitas menyiratkan bahwa snapshot memori diambil dalam suatu tindakan atomik yang tidak terputus, atau bahwa snapshot tersebut bebas dari tanda-tanda aktivitas sistem bersamaan—biasanya yang dihasilkan oleh alat akuisisi memori.

3

sebuah snapshot dianggap memiliki integritas jika nilai-nilai dalam wilayah memori tidak berubah sejak titik waktu tertentu yang dipilih oleh penyelidik. Kualitas-kualitas ini dapat diukur dan dibandingkan untuk mengevaluasi kualitas teknik akuisisi memori yang berbeda.

Taxonomy for memory acquisition methods

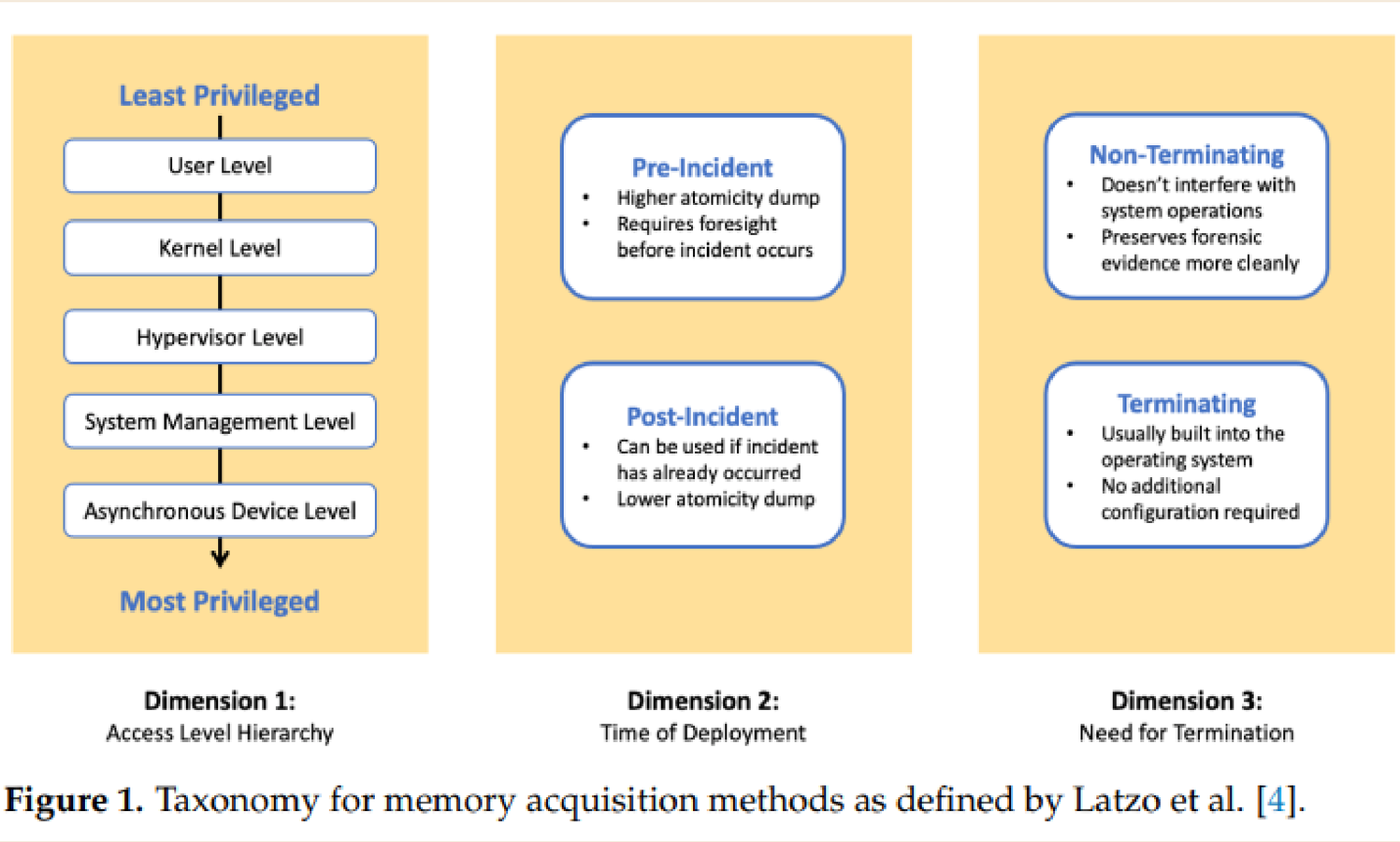
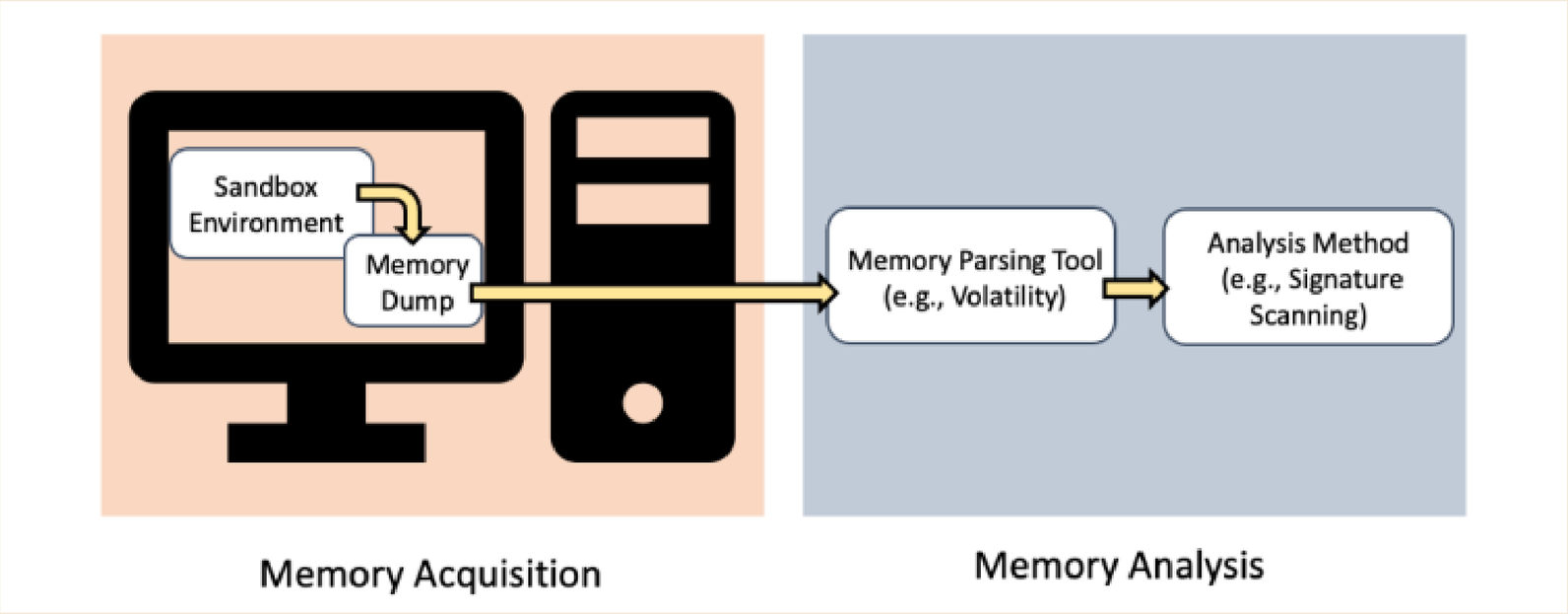


Figure 1. Taxonomy for memory acquisition methods as defined by Latzo et al. [4].

MEMORY ANALYSIS



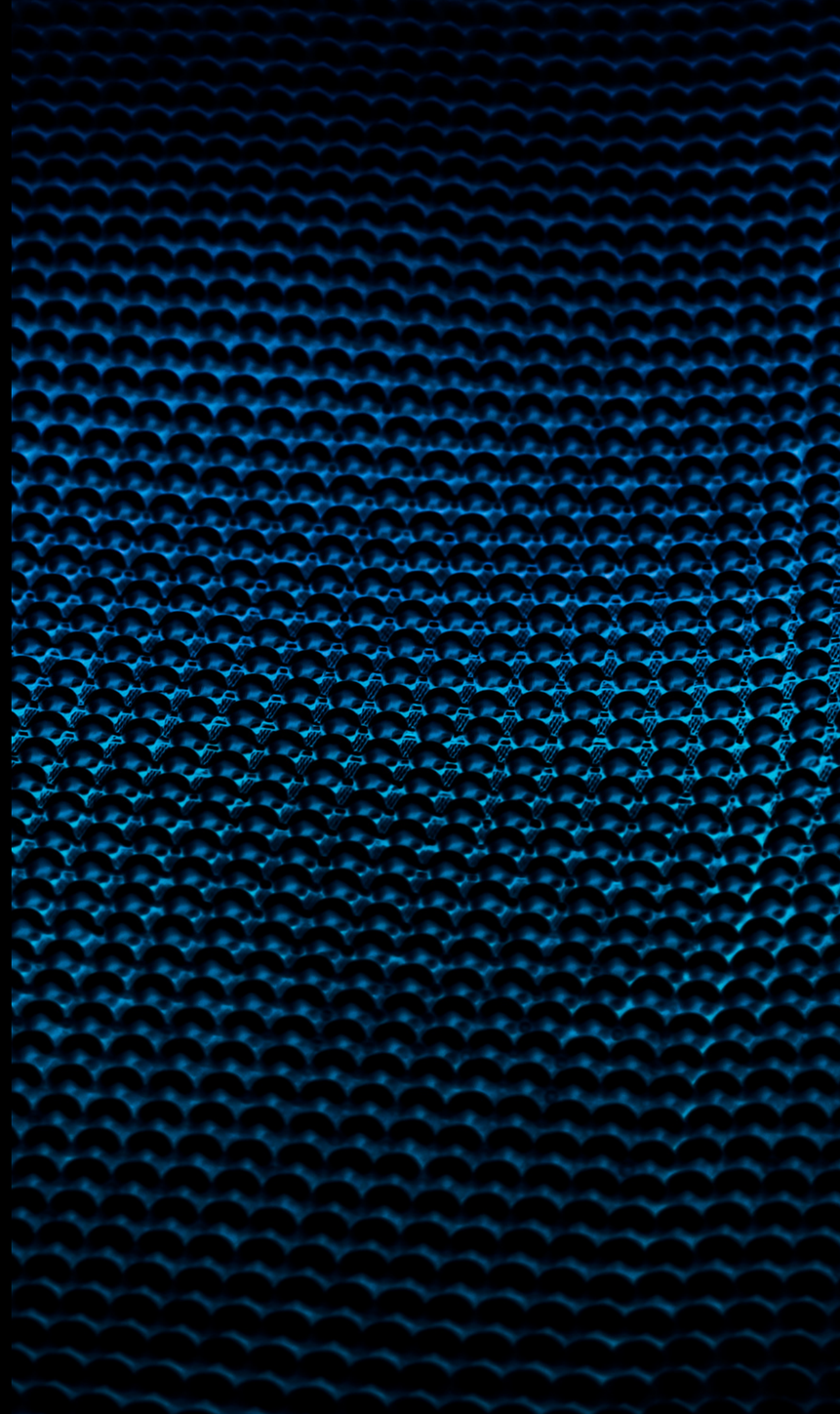
Setelah "memory dump" berhasil diperoleh, terdapat berbagai metode yang dapat digunakan untuk menganalisis "memory dump" tersebut guna mendeteksi keberadaan malware. Secara umum, proses analisis (Gambar 2) melibatkan penguraian "memory dump" untuk mengekstrak informasi yang berguna, dan kemudian menggunakan informasi tersebut dalam suatu pendekatan analisis tertentu.

Beberapa alat, termasuk Volatility dan Rekall, telah dibuat untuk mengurai "memory dump." Beberapa metode analisis memori yang lebih lama dan sudah mapan melibatkan pemindaian tanda tangan atau pemindaian heuristik dari "memory dump." Metode dinamis yang lebih baru melibatkan menjalankan malware di dalam, misalnya suatu sandbox environment.

Terakhir, metode machine learning sedang di develop leboh lanjut akan fitur dari metode analisis dinamis dan menggunakannya untuk melatih algoritma klasifikasi machine learning.

What can we do for Volatility GUI?

retrieved from https://www.kalilinux.in/2021/12/volatility-gui.html



SPECIFIC THINGS YOU CAN DO WITH VOLATILITY GUI

- **Mengimpor dump memori. Volatility GUI mendukung berbagai format dump memori, termasuk Windows Hibernation Files, Windows Crash Dumps, dump mentah Linux, dan dump memori VMware ESXi.**
- **Memilih dan menganalisis modul. Volatility GUI dapat mencantumkan semua modul yang dimuat dalam dump memori dan memberikan informasi terperinci tentang setiap modul, seperti nama, ukuran, dan jalur filenya.**
- **Melihat informasi proses seperti nama, ID proses, ID proses induk, dan baris perintah.**
- **Menganalisis koneksi jaringan. Volatility GUI dapat mencantumkan semua koneksi jaringan yang aktif dalam dump memori dan memberikan informasi terperinci tentang setiap koneksi, seperti alamat IP sumber, alamat IP tujuan, dan protokol.**
- **Menyetel malware dan rootkit. Volatility GUI dapat menggunakan berbagai teknik untuk mendeteksi malware dan rootkit, seperti memindai file dan entri registri yang mencurigakan.**
- **Menyelidiki insiden keamanan. Volatility GUI dapat digunakan untuk menyelidiki insiden keamanan dengan menganalisis dump memori dari sistem yang disusupi.**

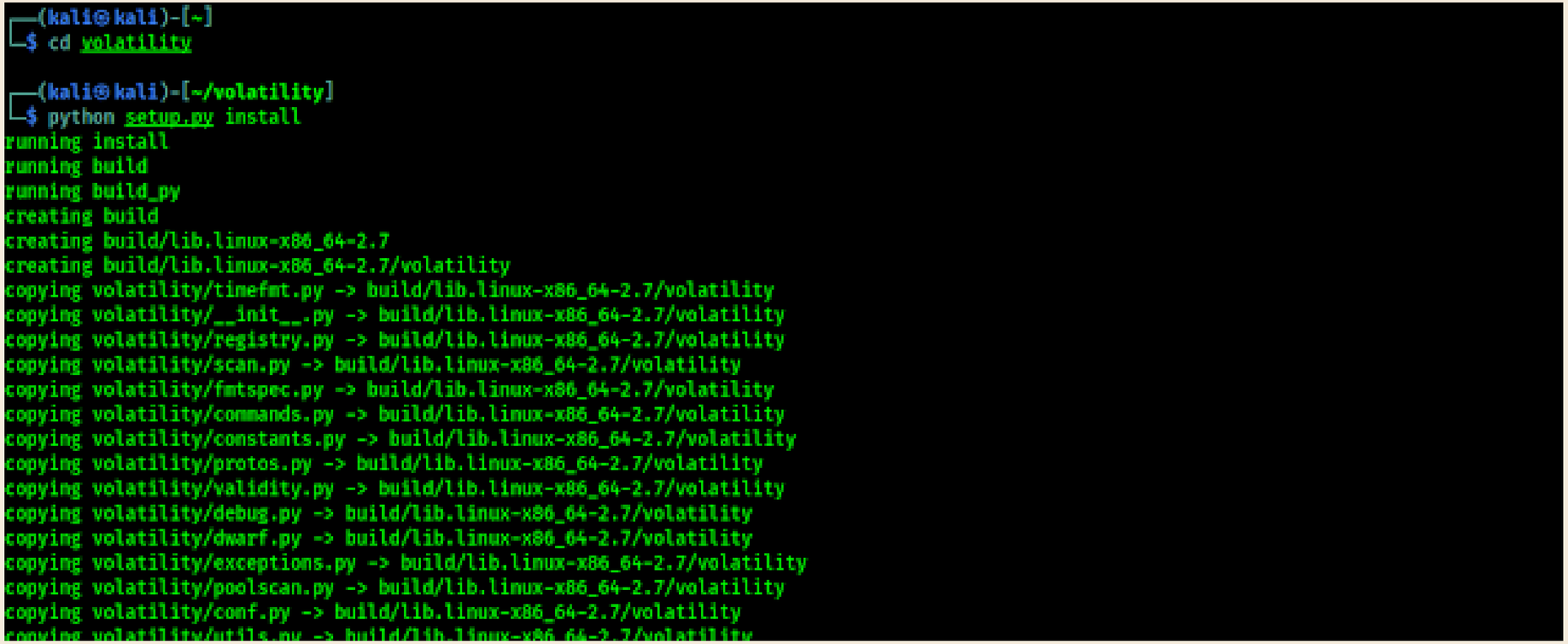
VOLATILITY GUI USING EVOLVE

Untuk menggunakan Volatility Framework, Kita dapat melakukan clone dengan menggunakan command berikut

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/volatilityfoundation/volatility
Cloning into 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Receiving objects: 100% (27411/27411), 21.10 MiB | 2.39 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.

┌──(kali㉿kali)-[~]
└─$
```

Setelah itu, kita masuk ke dalam directory volatility dengan menggunakan command “cd volatility”. Dan setelah masuk kita dapat menginstall volatility dengan menggunakan command “sudo python2 setup.py install”



Setelah selesai, kita juga perlu menginstall beberapa requirement. Dengan menggunakan command berikut ini:

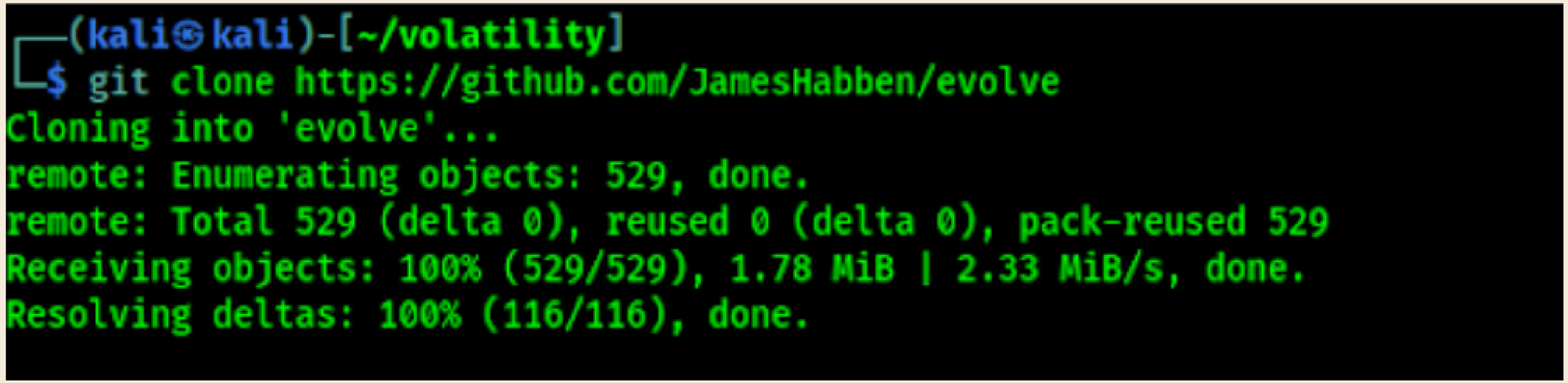
```
pip2 install bottle yara distorm3 maxminddb
```

```
pip2 install yara
```

```
pip2 install distorm3
```

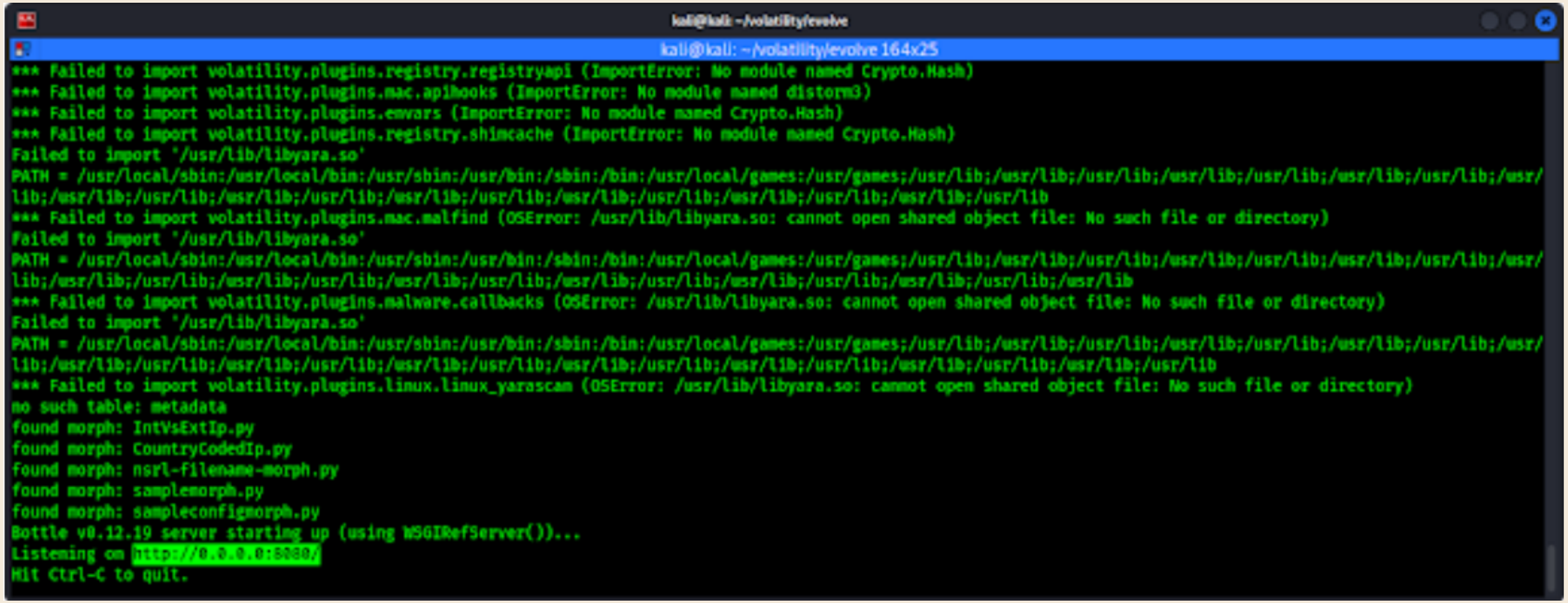
```
pip2 install maxminddb
```

Lalu untuk menginstall evolve kita perlu melakukan clone dengan menggunakan command berikut:

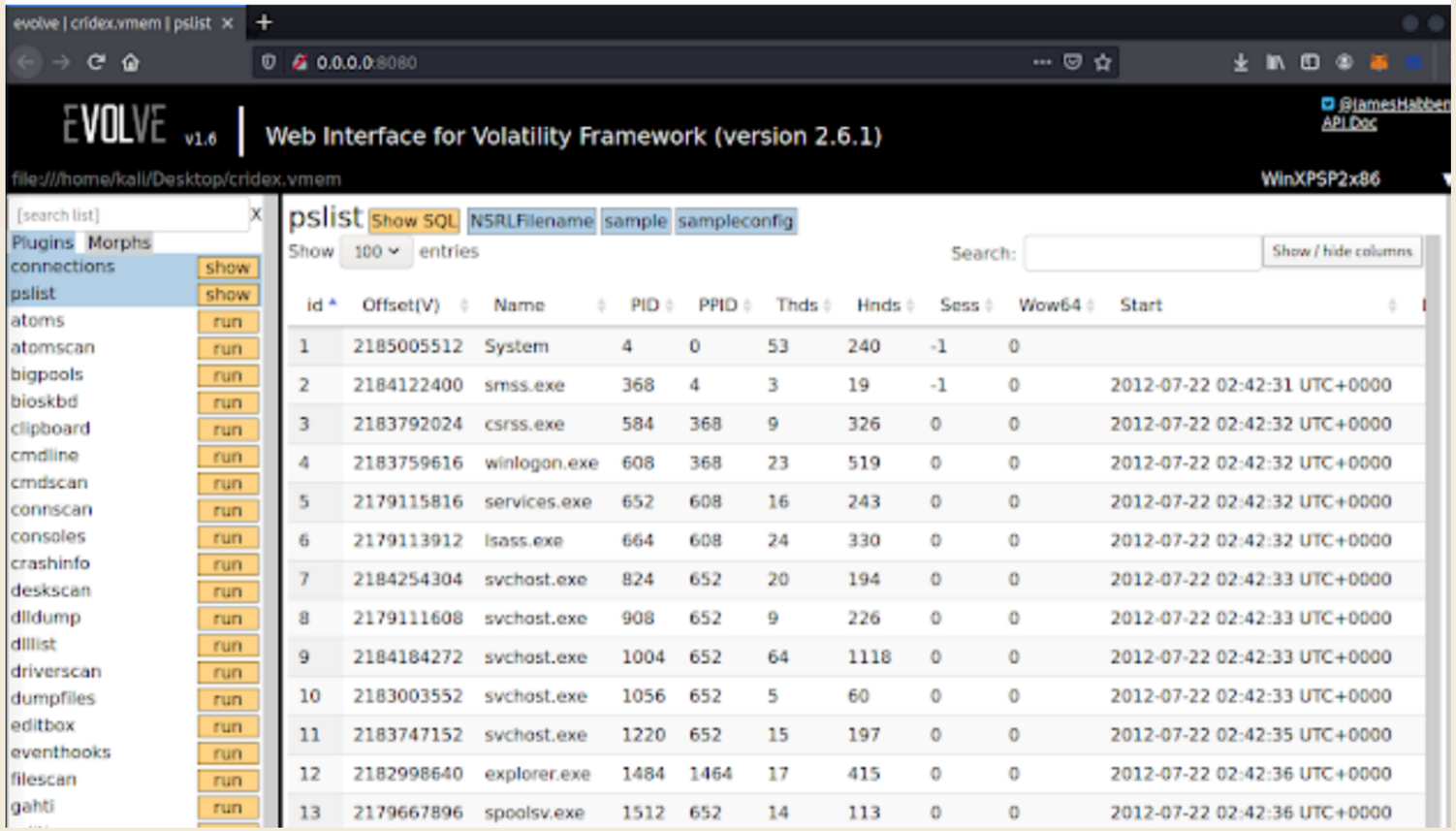


Untuk memulai menganalisa acquired memory(RAM) di GUI. Kita dapat menjalankan command seperti berikut ini. Dalam kasus ini sample acquired memory yang digunakan adalah cridex.vmew

```
python2 evolve.py -f /home/kali/Desktop/cridex.vmem
```



Kita akan mendapatkan output seperti gambar diatas. Disini dapat kita lihat bahwa terdapat localhost link yang dimana link tersebut adalah alamat dari evolve yang sedang berjalan.



Gambar diatas adalah tampilan dari Volatility Evolved

THANK YOU