Volatility

OSDFC 2015

Volatility 2.5

- Unified Output
  - Improves how you interface with Volatility (command line, web, thick UI)
  - Extends options for what to do with Volatility output (store, inspect, morph/label)
- Community Integration
  - Instantly sync plugins from various authors around the world
- New OS Profiles
  - Keeping up to date with Windows, Mac, and Linux

Unified Output

- Users: flexibility to specify how you want your output
- Plugin writers: less code results in more functionality
- Framework developers: easy APIs (JSON, DB, etc.)
  - Sqlite3
  - JSON
  - HTML
  - XLSX or CSV
  - Body (pipe delimited)
  - Dot graphs
  - Plain text
- https://github.com/volatilityfoundation/volatility/wiki/Unified-Output

Unified Output: Options

$ **python vol.py pslist -h**

Volatility Foundation Volatility Framework 2.5

Usage: Volatility - A memory forensics analysis platform.

[snip]

Module Output Options: dot, html, json, quick, quicksqlite, sqlite, text, xlsx

---

Module PSList

Print all running processes by following the EPROCESS lists

Unified Output: HTML

$ **python vol.py -f <FILE> pslist --output=html --output-file=pslist.html**

Volatility Foundation Volatility Framework 2.5

Show 10 entries Search:

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
2181173712	userinit.exe	1836	624	0	-1	0	0	2012-04-28 02:20:55 UTC+0000	2012-04-28 02:22:05 UTC+0000
2181210144	alg.exe	1880	672	5	102	0	0	2012-04-28 01:56:53 UTC+0000	
2182193184	smss.exe	360	4	3	19	-1	0	2012-04-28 01:56:37 UTC+0000	

Unified Output: JSON

$ **python vol.py -f <FILE>--output=json --output-file=pslist.json**
Volatility Foundation Volatility Framework 2.5

$ **python -m json.tool < pslist.json**


```
{
   "columns": [
      "Offset(V)", "Name", "PID", "PPID",
      "Thds", "Hnds", "Sess", "Wow64", "Start", "Exit"
   ],
   "rows": [
   [
         2182193184, "smss.exe", 360, 4, 3, 19, -1, 0,
         "2012-04-28 01:56:37 UTC+0000", ""
   ],
```

Unified Output: Sqlite3

$ **python vol.py -f <FILE> pslist --output=sqlite --output-file=pslist.db**
Volatility Foundation Volatility Framework 2.5

$ **sqlite3 pslist.db**
SQLite version 3.7.13 2012-07-17 17:46:21
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> **select * from PSList limit 5;**
1|0|2185005104|System|4|0|51|269|-1|0||
2|0|2182193184|smss.exe|360|4|3|19|-1|0|2012-04-28 01:56:37 UTC+0000|
3|0|2182255136|csrss.exe|596|360|11|340|0|0|2012-04-28 01:56:38 UTC+0000|
4|0|2182692896|winlogon.exe|624|360|17|535|0|0|2012-04-28 01:56:39 UTC +0000|
5|0|2182374496|services.exe|672|624|15|238|0|0|2012-04-28 01:56:39 UTC +0000|

Unified Output: Framework Authors

```
import copy, libapi # see contrib/library_example
import volatility.plugins.taskmods as taskmods
import volatility.plugins.filescan as filescan

config = libapi.get_config(
                "/samples/mem.dmp", "Win7SP1x64")

plugins = (taskmods.PSList, filescan.FileScan)

for plugin in plugins:
    data = libapi.get_json(copy.deepcopy(config),
taskmods.PSList)
```

Community Repo

- Central repository easily links to your Volatility installation
- 40+ plugins from 25+ authors
- https://github.com/volatilityfoundation/community

Community Repo: Setup

1. Git clone the Volatility repository or Download a *Release
2. Git clone the Community repository to $PLUGINSPATH
3. Pass --plugins=$PLUGINSPATH to Volatility when you run it

* Instructions also apply to the standalone exes

Community Repo: FYI

- Plugins only…does not include other frameworks (i.e. Cuckoo, Evolve, GVol)
- Options may conflict
    - Use --plugins=$PLUGINSPATH/subdir
- Some plugins have multiple homes
  – We will try to keep this one recent/updated

New OS Profiles: Windows

- Windows 10 (Win10x86, Win10x64)
  - ✓ Process plugins (handles, sids, privileges, dlls, vads)
  - ✓ PE plugins (dlldump, procdump, moddump)
  - ✓ Scanning plugins (processes, files, mutexes)
  - ✓ Registry plugins (printkey)
  - ✓ Misc plugins (services)
  - ❑ Isolated user mode memory
  - ❑ Compressed memory
  - ❑ Hibernation files

New OS Profiles: Mac & Linux

- Mac 10.11 (El Capitan)
- Linux Kernels 4.2.3

Volatility Plugin Contest (2015)

- 12 submissions evaluated based on creativity, usefulness, effort, completeness, and clarity of documentation

- 1st place: $1500 cash or free 5-day Windows Malware and Memory Forensics Training
- 2nd place: $500 cash
- 3rd place: $250 cash
- 4th and 5th place: swag

(1st) Shimcache Memory Scan

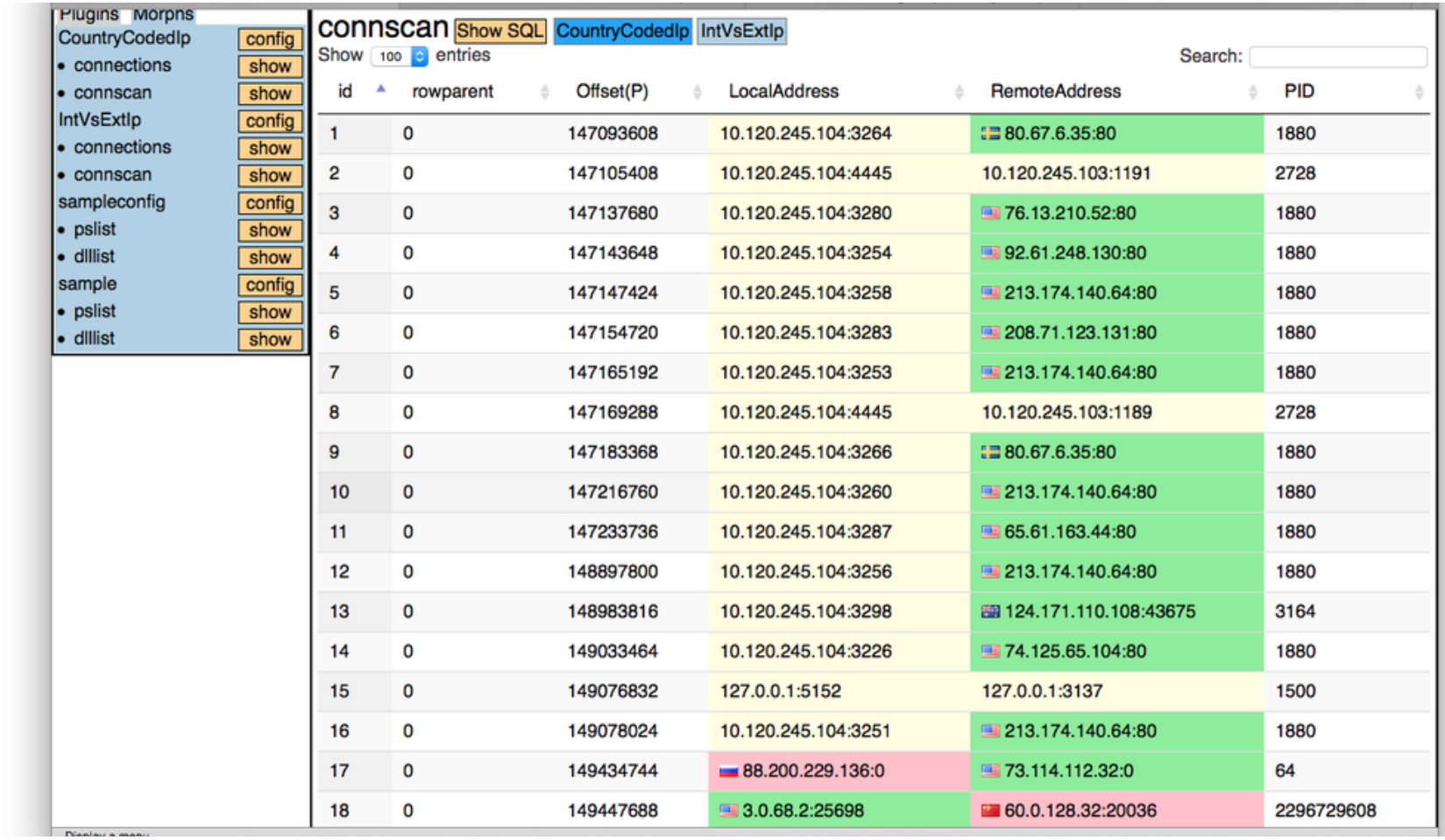
- Fred House, Andrew Davis, Claudiu Teodorescu (Mandiant/FireEye)
- Evidence of program execution *before* the system is rebooted
- Supports Windows XP SP2 through Windows 8 and Server 2012 R2
- Applicable to almost any/all types of cases

Order	Last Modified	Last Update	Exec Flag	File Size	File Path
1	2015-03-12 16:44:52		True		SYSVOL\Users\Administrator\Desktop\DumpIt.exe
2	2013-08-22 11:45:14		True		SYSVOL\Windows\System32\wbem\WmiPrvSE.exe
3	2013-08-22 11:44:42		True		SYSVOL\Windows\System32\wbem\WMIADAP.exe
4	2013-08-22 11:03:41		True		SYSVOL\Windows\System32\rundll32.exe
5	2012-05-01 20:12:56		True		SYSVOL\Program Files\VMware\VMware Tools\TPAutoConnect.exe
6	2013-08-22 12:35:25		True		SYSVOL\Windows\System32\dllhost.exe
7	2013-08-22 12:39:50		True		SYSVOL\Windows\System32\OpenWith.exe
8	2012-11-01 01:05:12		True		SYSVOL\Program Files\Common Files\VMware\Drivers\vss\comreg.exe
9	2013-08-22 12:42:49		True		SYSVOL\Windows\System32\taskhost.exe
10	2012-05-01 20:12:56		True		SYSVOL\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
11	2013-08-22 10:01:15		True		SYSVOL\Windows\System32\net1.exe
12	2013-08-22 10:01:50		True		SYSVOL\Windows\System32\net.exe
13	2013-08-22 11:01:57		True		SYSVOL\Windows\System32\ThumbnailExtractionHost.exe

(2nd) James Habben: Evolve

- Web interface with AJAX, JQuery, JSON
- Run multiple plugins at once
- Query, filter, and sort the database entries from the web page
- Use or add “morphs” (color coding) to associate countries to IPs, highlight files not in NSRL, etc.

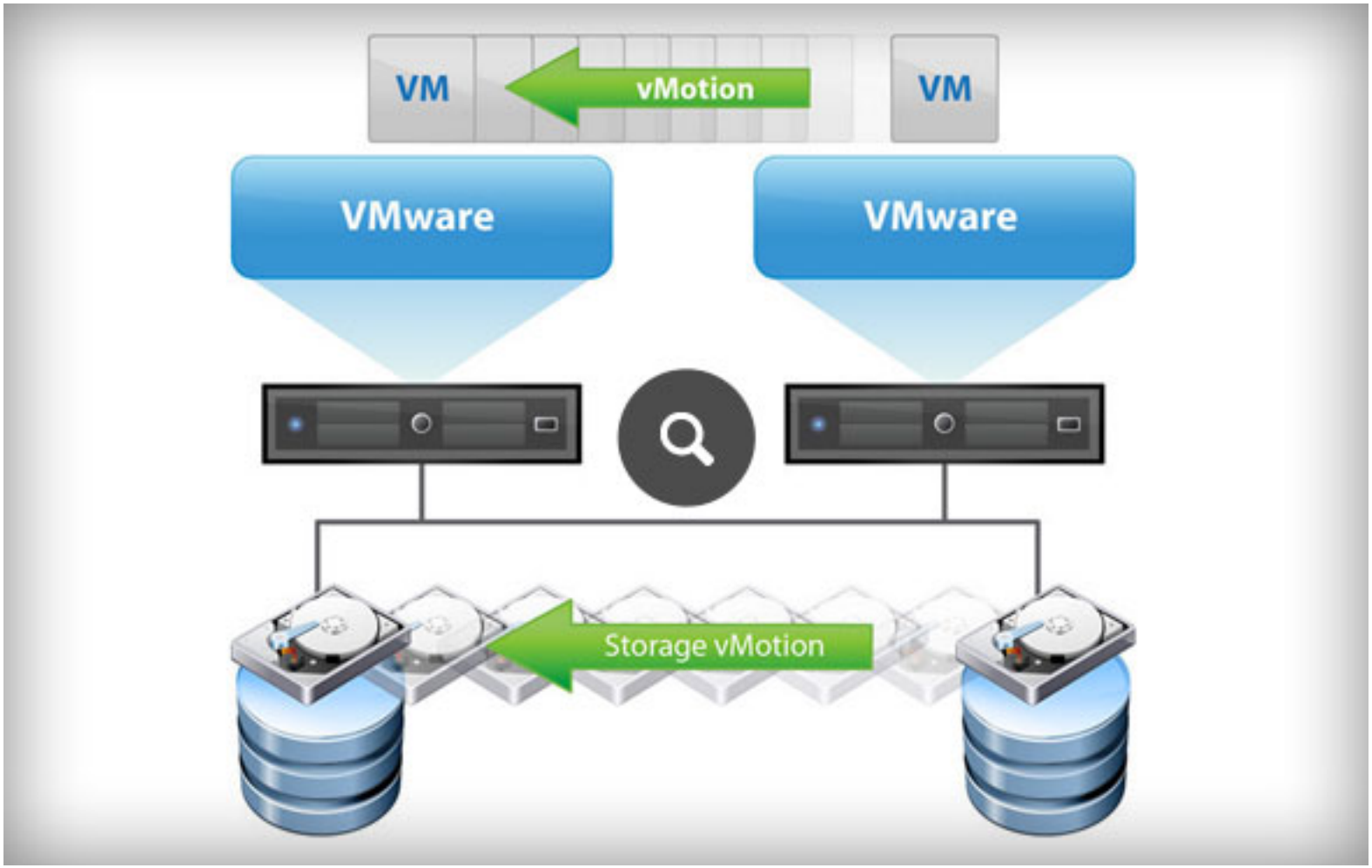
Evolve


Plugins Morphs
CountryCodedIp config
• connections show
• connscan show
IntVsExtIp config
• connections show
• connscan show
sampleconfig config
• pslist show
• dlllist show
sample config
• pslist show
• dlllist show
connscan Show SQL CountryCodedIp IntVsExtIp
Show 100 entries
Search:
id rowparent Offset(P) LocalAddress RemoteAddress PID
1 0 147093608 10.120.245.104:3264 80.67.6.35:80 1880
2 0 147105408 10.120.245.104:4445 10.120.245.103:1191 2728
3 0 147137680 10.120.245.104:3280 76.13.210.52:80 1880
4 0 147143648 10.120.245.104:3254 92.61.248.130:80 1880
5 0 147147424 10.120.245.104:3258 213.174.140.64:80 1880
6 0 147154720 10.120.245.104:3283 208.71.123.131:80 1880
7 0 147165192 10.120.245.104:3253 213.174.140.64:80 1880
8 0 147169288 10.120.245.104:4445 10.120.245.103:1189 2728
9 0 147183368 10.120.245.104:3266 80.67.6.35:80 1880
10 0 147216760 10.120.245.104:3260 213.174.140.64:80 1880
11 0 147233736 10.120.245.104:3287 65.61.163.44:80 1880
12 0 148897800 10.120.245.104:3256 213.174.140.64:80 1880
13 0 148983816 10.120.245.104:3298 124.171.110.108:43675 3164
14 0 149033464 10.120.245.104:3226 74.125.65.104:80 1880
15 0 149076832 127.0.0.1:5152 127.0.0.1:3137 1500
16 0 149078024 10.120.245.104:3251 213.174.140.64:80 1880
17 0 149434744 88.200.229.136:0 73.114.112.32:0 64
18 0 149447688 3.0.68.2:25698 60.0.128.32:20036 2296729608

(3rd) Philip Huppert: VM Live Migration

- Thesis: Virtual Machine Introspection During Live Migration
- Full control over the VM with access to migration network traffic
  - No tools installed on ESX or VM
- Offensive/penetration testing
- Forensics
- Scan a VM for malware during the migration

Step 1: Capture ESX Traffic



Step 2: Extract RAM from PCAP

```
$ ./extract.py winxp_sp3_x86_256mb_vmotion_esxi6.pcap
Processing 192.168.088.010.08000-192.168.088.011.12698
Processing 192.168.088.010.40165-192.168.088.011.08000
Found VMotion migration in
192.168.088.010.40165-192.168.088.011.08000
Saving to /home/philip/
192.168.088.010.40165-192.168.088.011.08000.vmig
Processing 192.168.088.010.25811-192.168.088.011.08000
Processing report.xml

$ mv 192.168.088.010.40165-192.168.088.011.08000.vmig winxp.vmig
```

(4th) Ying Li: Python Strings and SSH Keys

- Presented at PyCon 2015
- Extract and contextualize strings within a Python process
- Map strings back to key-value pairs in a dictionary
- Recover RSA keys from the heap of an ssh-agent
- https://www.youtube.com/watch?v=tMKXcc2-xO8

Python Strings and SSH Keys

$ **python vol.py -f <FILE> linux_python_strings**

Volatility Foundation Volatility Framework 2.5

Pid	Name	Size	String
8414	python	48	This is a python string [...]
8414	python	21	this is another value
8414	python	15	this is the key

$ **python vol.py -f <FILE> linux_ssh_keys --dump-dir /tmp**

Volatility Foundation Volatility Framework 2.5

Pid	Name	Found-Key Filename
8394	ssh-agent	/tmp/8394.ssh-agent.1
8394	ssh-agent	/tmp/8394.ssh-agent.2
8394	ssh-agent	/tmp/8394.ssh-agent.3

(5th) Adam Bridge: NDIS Packet Scan

- Finds packets/frames in NDIS shared memory
- RAM shared between the OS and DMA NIC
- Output as text or pcap
- Decodes NetBIOS in DNS traffic
- Less chance of FPs and fake/decoys

ndispktscan

Offset (V)	Prot	Source IP	Destination IP	SPort	DPort	Flags
0x870f5ff8	0x06	192.168.203.134	23.63.99.217	49311	80	ACK
0x870f6ff8	0x06	192.168.203.134	205.185.216.10	49286	80	ACK,RST
0x870f7ff8	0x06	192.168.203.134	208.146.36.220	49283	80	ACK,RST
0x870f8ff8	0x06	192.168.203.134	46.228.164.11	49278	80	ACK,RST
0x870f9ff8	0x06	192.168.203.134	208.146.36.221	49263	80	ACK,RST
0x870faff8	0x06	192.168.203.134	208.146.36.221	49271	80	ACK,RST
0x870fcff8	0x06	192.168.203.134	23.63.99.217	49311	80	ACK
0x870fdff8	0x06	192.168.203.134	23.63.99.217	49311	80	ACK
0x870feff8	0x06	192.168.203.134	23.63.99.217	49311	80	ACK
0x870ffff8	0x06	192.168.203.134	23.63.99.217	49311	80	ACK
0x87100ff8	0x06	192.168.203.134	23.63.99.217	49311	80	ACK

Monnappa Ka: Linux Memory Diff

- Compares baseline and infected Linux memory dumps
- Videos:
  - Tsunami: https://www.youtube.com/watch?v=Fw5FrVwJslw
  - Xingiquan: https://www.youtube.com/watch?v=_RuZ-lVysxQ
  - Average Coder Rootkit: https://www.youtube.com/watch?v=zKjsANieis8

```
=======================[MEMORY DIFF ANALYSIS RESULTS]=========

DIFF_PSLIST
=========================================
Offset              Name                    Pid             Uid
0xffff88001bca8000 aptd                     2667            0
0xffff88000aee96f0 nm-dispatcher.a          2701            0
0xffff8800021e44d0 tsuna                    2659            0
0xffff88001bd58000 strace                   2657            0

DIFF_PSXVIEW
=========================================
Offset(V)           Name                     PID pslist pid_hash
0xffff88001bca8000 aptd                     2667 True   True
0xffff88000aee96f0 nm-dispatcher.a          2701 True   True
0xffff8800021e44d0 tsuna                    2659 True   True
0xffff88001bd58000 strace                   2657 True   True

DIFF_PIDHASHTABLE
=========================================
Offset              Name                    Pid             Uid
0xffff88001bca8000 aptd                     2667            0
0xffff88000aee96f0 nm-dispatcher.a          2701            0
0xffff8800021e44d0 tsuna                    2659            0
0xffff88001bd58000 strace                   2657            0
```

Bartosz Inglot: Scheduled Tasks

- Finds jobs created by the `at` command and the task scheduler
- Detect persistence, lateral movement, attempts to run with SYSTEM privileges
- Based on Jamie Levy's jobparser.py

schtasks

```
$ python vol.py -f <FILE> schtasks

Offset(P):              0x12ab2118
ScheduledDate:          2012-11-26 19:30:00.000
MostRecentRunTime:      2012-11-26 19:30:00.021
Application:            wc.exe
Author:                 SYSTEM
Parameters:             -e -o h.out
RunInstanceCount:       1
MaxRunTime:             72:00:00.0
ExitCode:               0x00000000
Comment:                Created by NetScheduleJobAdd
```

Joe Greenwood: HT (RCS) Attribution

- Finds Hacking Team Galileo Remote Control System (RCS)
- Not your average signature/string based detection
- Uses heuristics on named shared memory sections
  - This never touches disk
- Attribution based on "watermarks" linked to HT customers

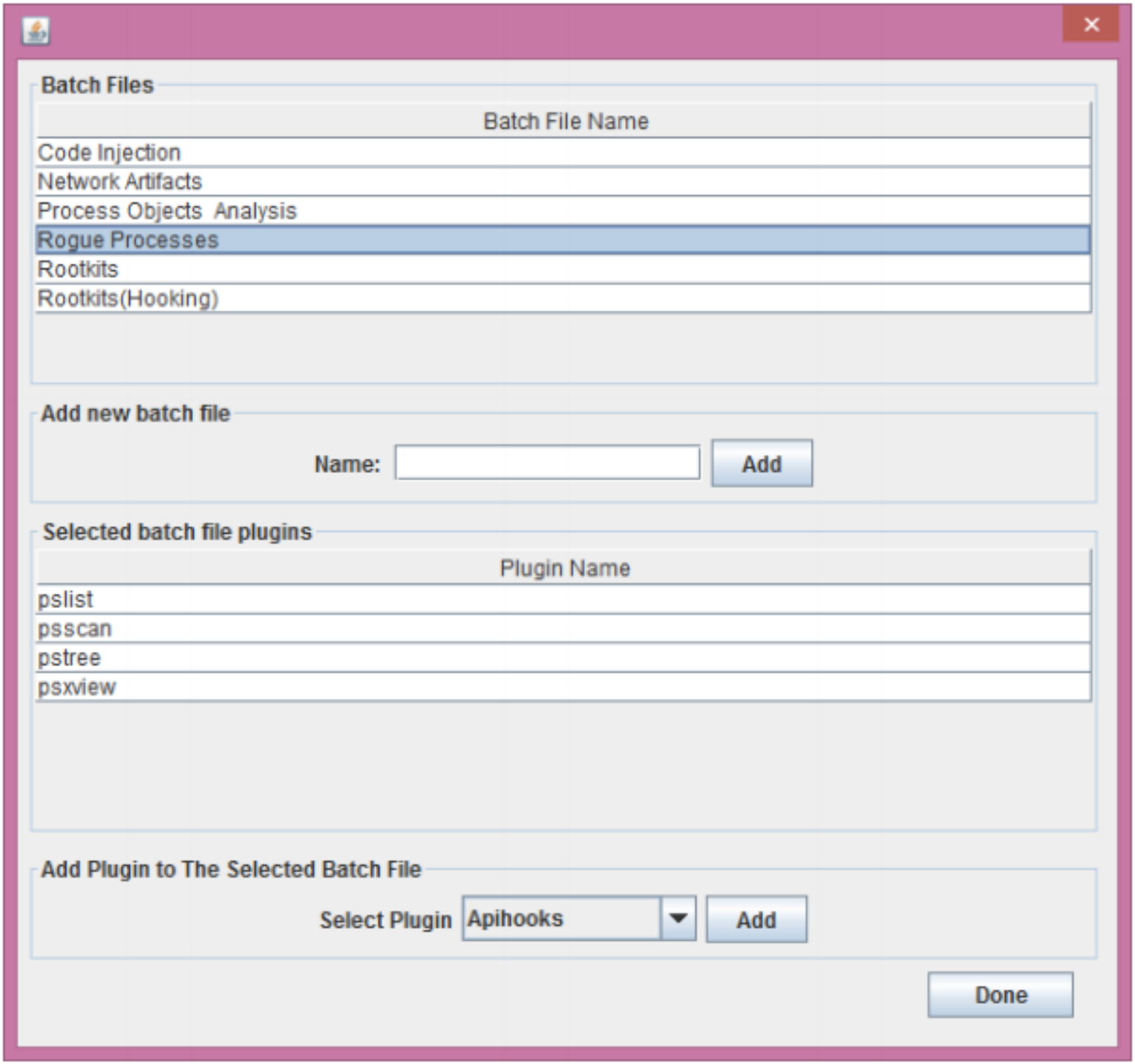
attributeht

```
$ python vol.py -f <FILE> attributeht
Volatility Foundation Volatility Framework 2.4
Hacking Team Galileo RCS Implant Detection - 4ARMED Ltd

PID    Watermark   Process       Implant Type   Attrib
2584   3OqZ1N5a    wscntfy.exe   Elite/Soldier  FAE-FURLAN
2584   3OqZ1N5     wscntfy.exe   Elite/Soldier
2896   3OqZ1N5a    explorer.exe  Elite/Soldier  FAE-FURLAN
2896   3OqZ1N5     explorer.exe  Elite/Soldier
[snip]
```

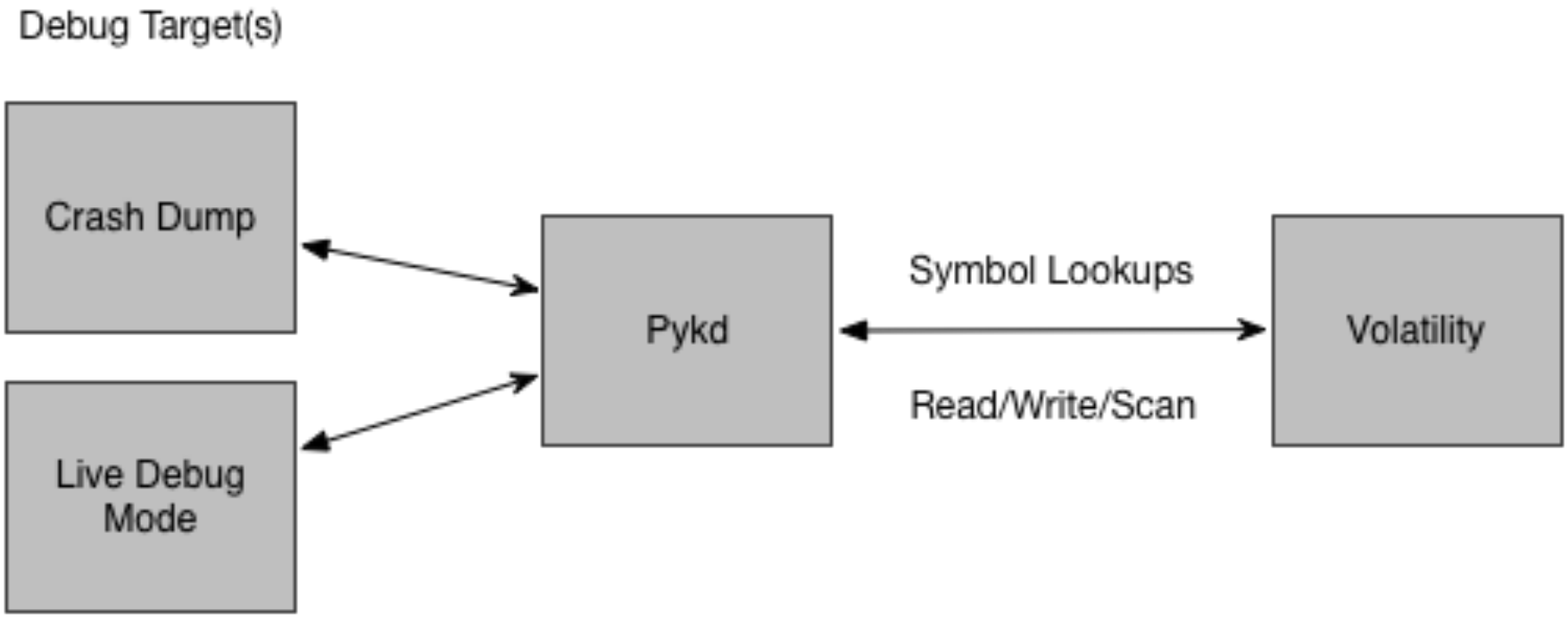
EG-CERT: GVol

- By May Medhat and Mohamad Shawkey
- Lightweight GUI written in Java
- Preconfigured and customizable batch scripts
- Users can add/register new plugins to support future versions of Volatility
- Integrates documentation from Art of Memory Forensics


Batch Files
Batch File Name
Code Injection
Network Artifacts
Process Objects Analysis
Rogue Processes
Rootkits
Rootkits(Hooking)
Add new batch file
Name:
Add
Selected batch file plugins
Plugin Name
pslist
psscan
pstree
psxview
Add Plugin to The Selected Batch File
Select Plugin
Apihooks
Add
Done

Alexander Tarasenko

- Pykd address space lets you run Volatility inside Windbg



Loïc Jaquemet: Haystack

- Interface between Volatility and Haystack
- Define structures and constraints manually or from C header files
- Scan for them throughout process memory
  - Alternate method to find _HEAPs
  - OpenSSL session keys
  - Any structures that Volatility scans for

haystackheap

$ **vol.py -f <FILE> haystackheap -p 1668**
-r haystack.structures.win32.winxp_32.HEAP
-c examples/winxpheap-relaxed.constraints

****

Pid: 1668
Record HEAP at 0x250000
Record HEAP at 0x150000
Record HEAP at 0x3f0000
Record HEAP at 0x730000
Record HEAP at 0x860000
Record HEAP at 0xba0000
Record HEAP at 0xb70000
[...]

Takeaways

- Rapidly transform memory artifact analysis into proactive use scenarios
  - Or in the very worse case, just use it
- Volatility 2.5 is out!
  - github.com/volatilityfoundation
  - volatilityfoundation.org
  - @volatility
- Congratulations to the plugin contest authors
- Get the community plugins