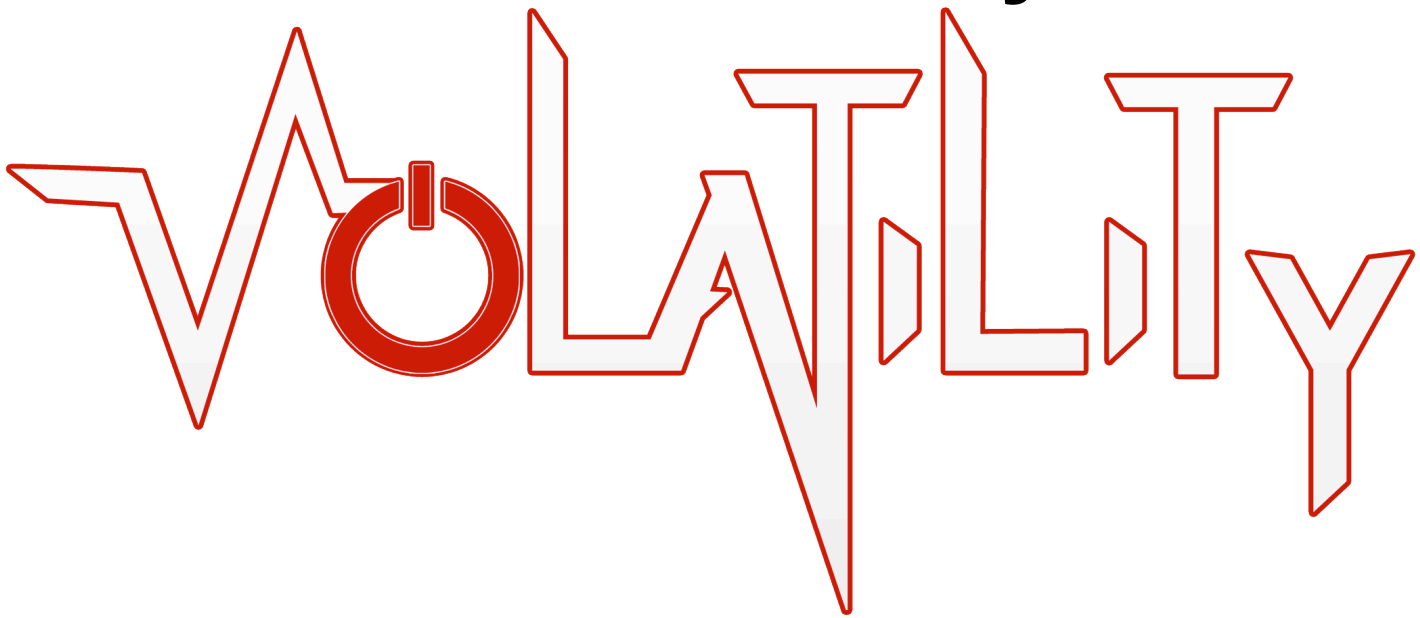
THE VOLATILITY FOUNDATION

Next Generation Memory Forensics



Volatility Developers

November 5, 2014

EMPOWERING INVESTIGATORS

Volatility Development Team

- Core Developers:
  - Mike Auty (ikelos)
  - Andrew Case (attc)
  - Brendan Dolan-Gavitt (moyix)
  - Michael Hale Ligh (MHL)
  - Jamie Levy (gleeda)
  - AAron Walters (labarum)

Thank You!

- The Volatility Community (OOV)
  - Numerous research collaborators/testing/bugs
  - Academia, government, industry
  - Mailing lists, blogs, irc (#volatility)
  - Moved: https://github.com/volatilityfoundation/volatility
  - @volatility

VOLATILITY

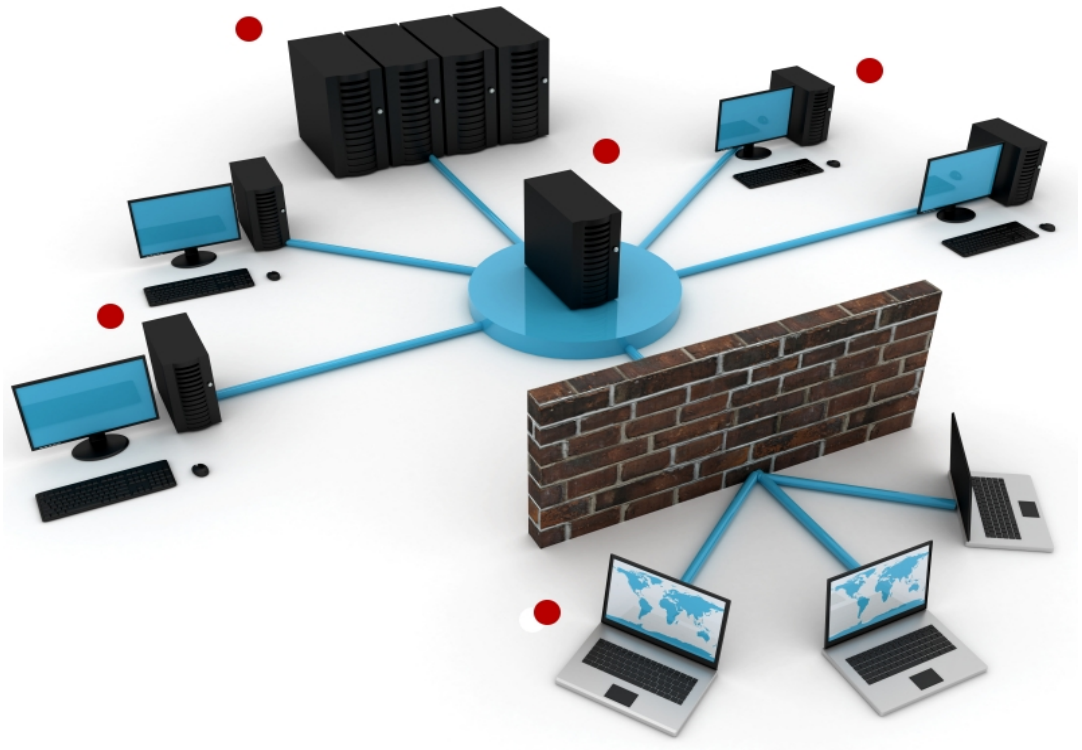
Volatility Foundation

- Volatility development is supported by an independent foundation
  - US 501(c)(3) Nonprofit
- The Volatility Foundation was established:
  - to support the development of Volatility
  - to promote the use of Volatility and memory analysis in the forensics community
  - to protect the intellectual property and the framework's long-term viability
  - to advance the state of the art in memory analysis research.
- But….development driven by Volatility community

VOLATILITY

Opaque Systems/Enterprise

- Opaque components of information infrastructure
  - Can your systems be trusted? (patches, malware)



VOLATILITY

Adversaries Challenges

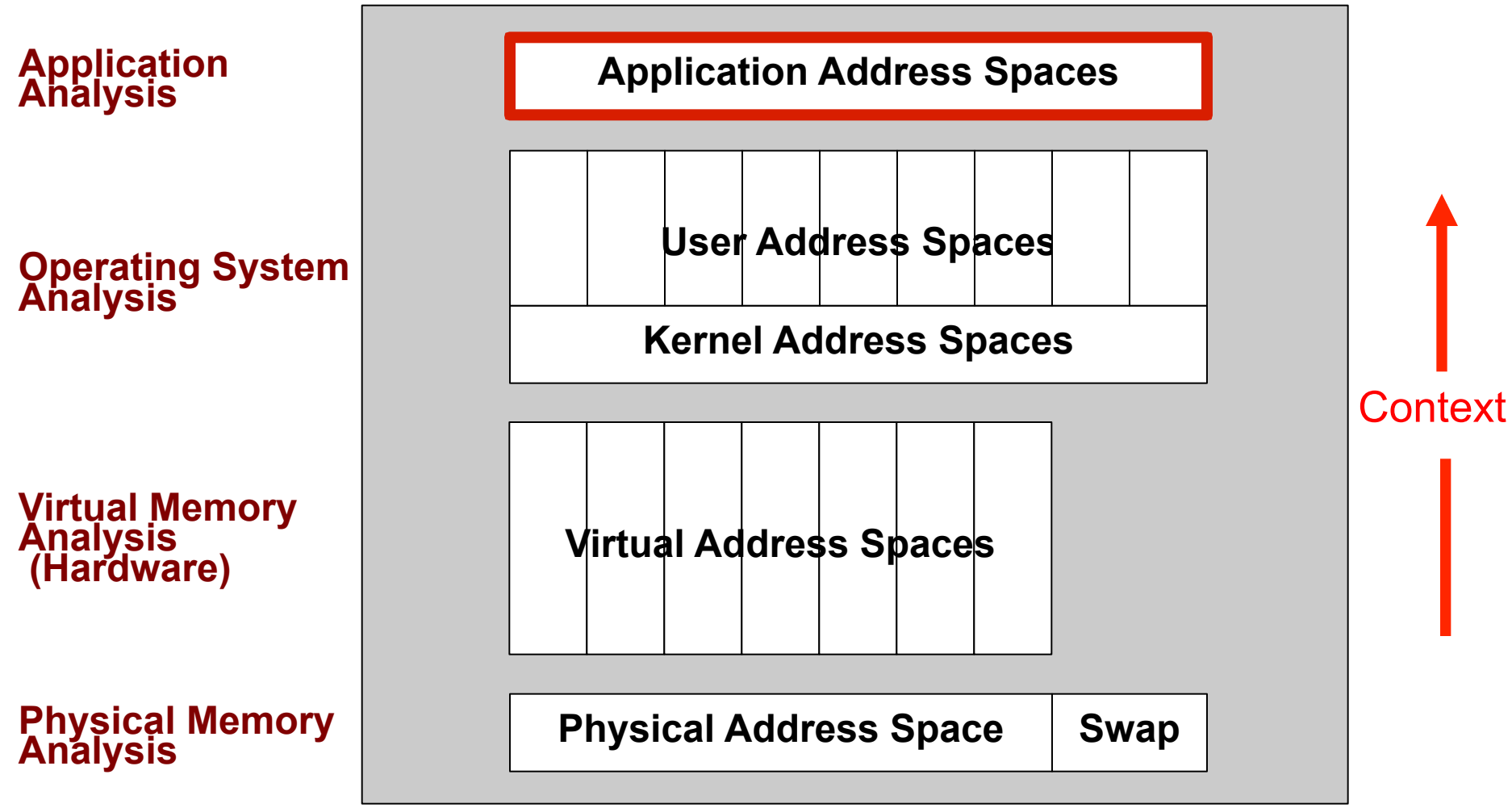
- Adversaries Challenges
  - They want to remain undetected (stealthy)
  - They want to execute a mission
  - They rely on components of the operating system
- Consume system resources
  - Memory (stack, heap, pool)
  - Objects (thread, process, mutex, driver)
- Modify control flow (execution) of the system
  - Hide the allocated resources
  - Perform mission

What is Memory Forensics?

- Memory forensics is the process of acquiring and analyzing physical memory (RAM) in order to find artifacts and evidence
  - Analysis does not depend on OS (trust)
  - Unconstrained analysis (entire state of OS/historical)
  - Removes the active adversary
- Usually performed in conjunction with disk and network forensics (memory only artifacts)
- Rapid triage/analysis leads (sandbox)

VOLATILITY

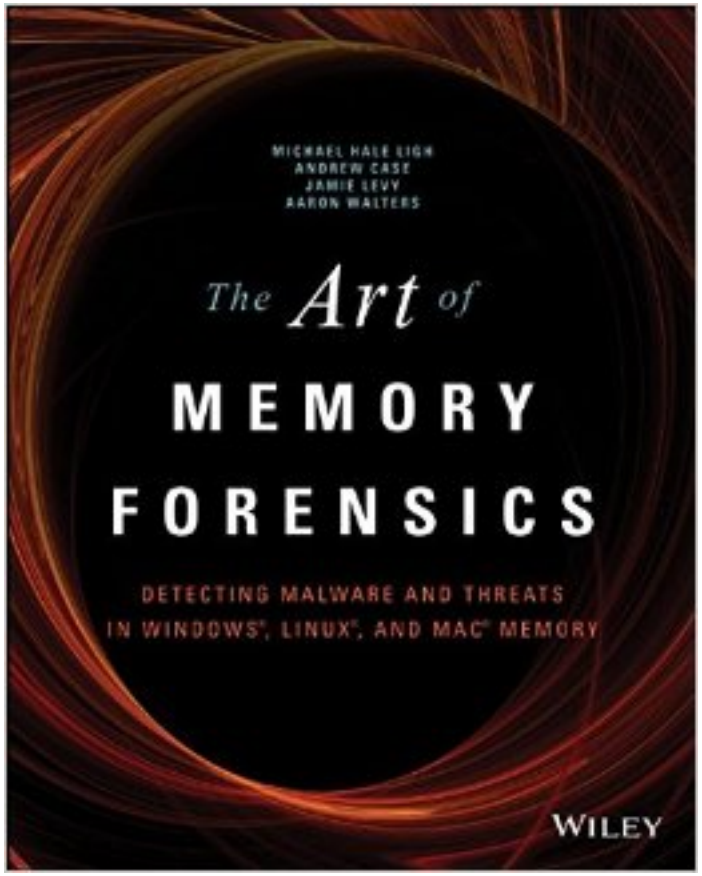
Next Generation Analysis



Volatility Framework

- Volatile memory artifact extraction utility framework
- Completely open source (GPLv2/Python)
- Cross platform (Python)
- Single, cohesive analysis framework
  - Windows, Mac, Linux, Android, …
- Command-line tools/scriptable
- Modular architecture
- Unparalleled features!
- Active Community
  - Industry, academics, government, law enforcement

Volatility 2.4: AMF

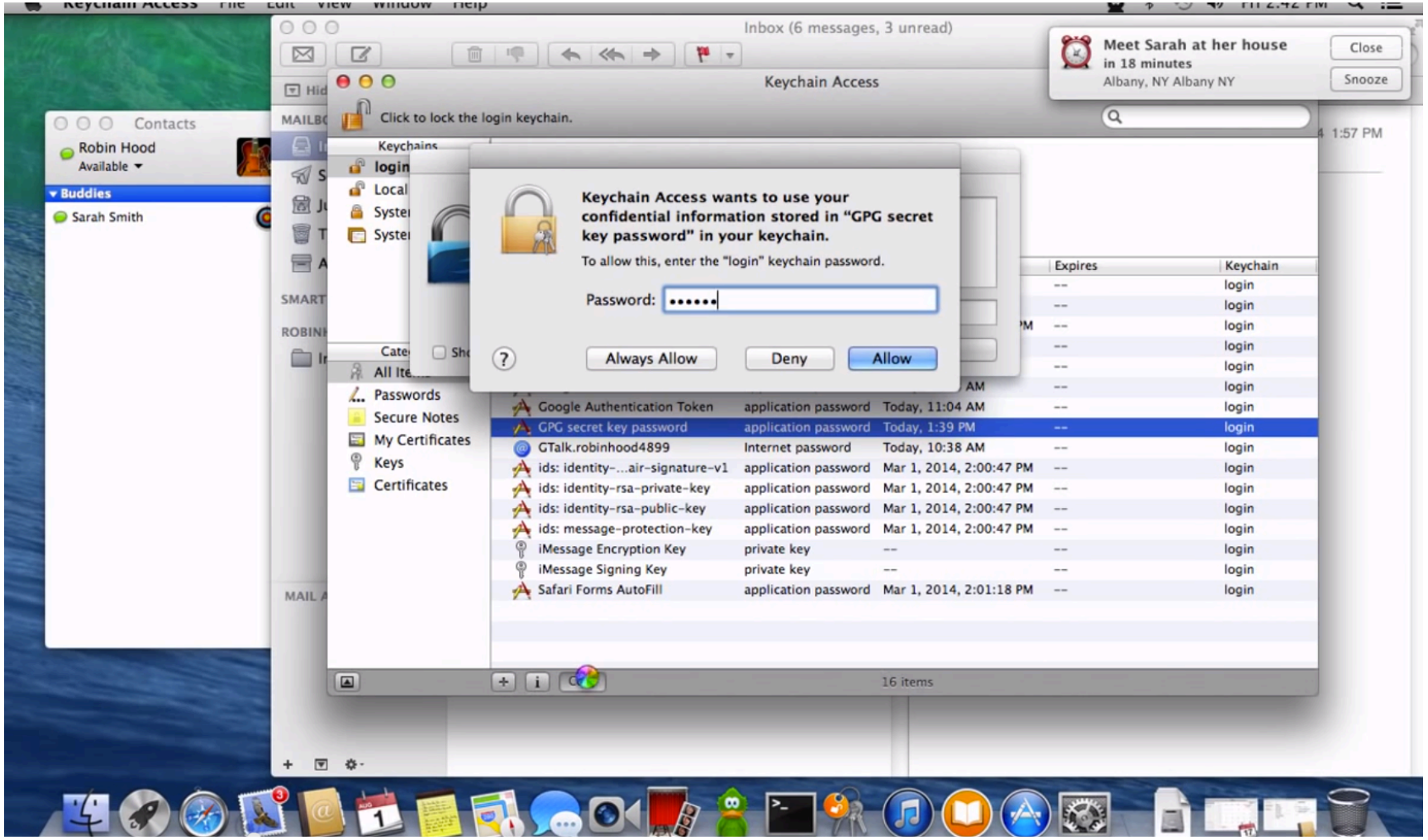


Volatility 2.4: Highlights

- Released: August 2014 at Black Hat Arsenal
- Address Spaces (3 new AS/17)
  - QEMU virtual machine memory samples
  - “split” VMware files (vmem, vmss, vmsn)
  - Windows BitMap crash dumps (Windows 8/2012)
- Mac OSX (30 new plugins/62)
  - Mavericks through 10.9.4
  - Mac string translation
  - Adium message (OTR)/Contact records/Notes artifacts
  - Apple Keychain encryption keys/clear-text PGP emails
  - API hooks in kernel and process memory
  - IP and socket filters
  - Suspicious process mappings (injected code)
  - Hidden kernel extensions (extraction)
  - Recovered files cached in memory

VOLATILITY

Application Artifacts



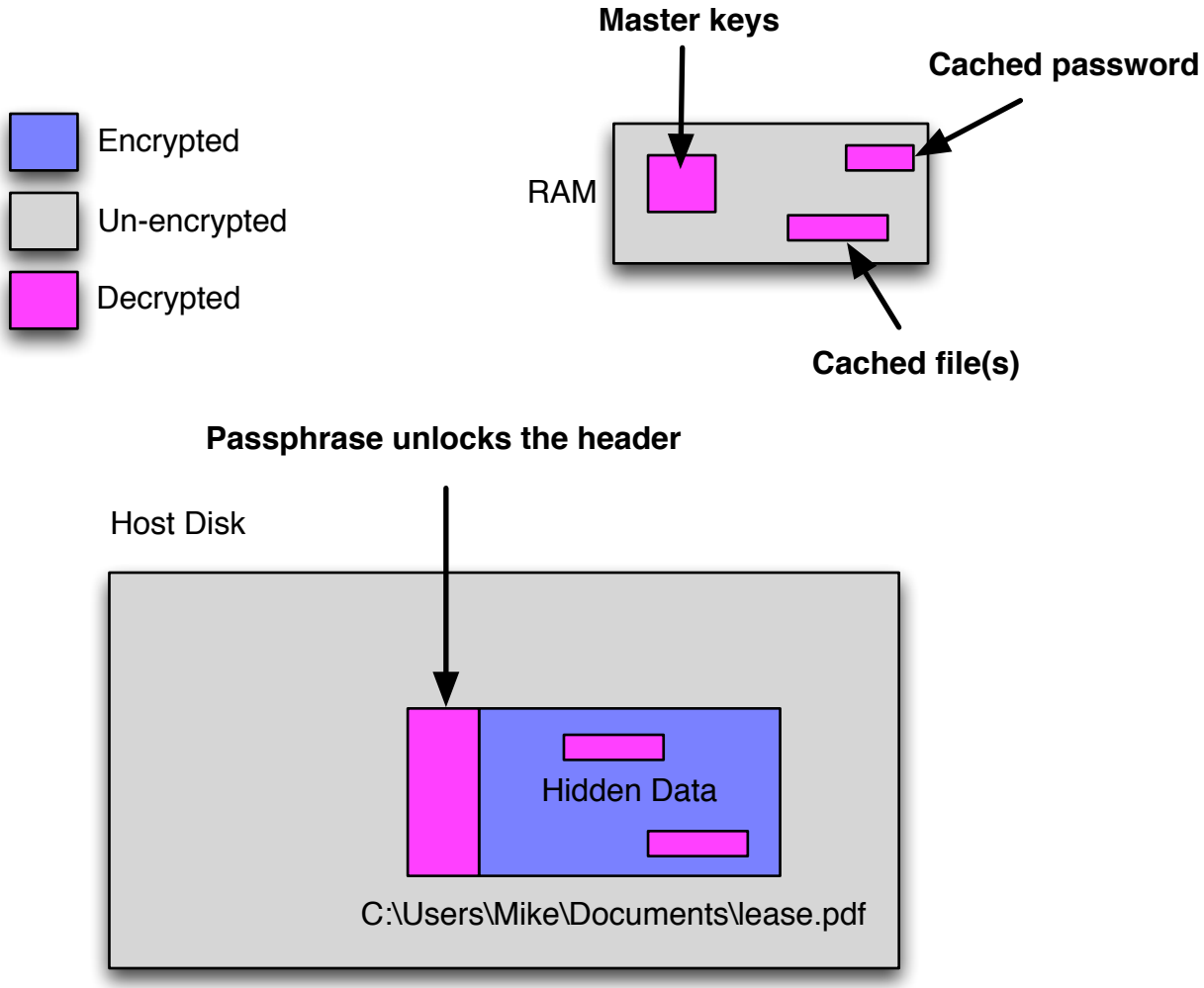
Volatility 2.4: Highlights

- Linux/Android (24 new plugins/66)
  - Linux kernels through 3.16
  - Linux string translation
  - API hooks (kernel/userland)
  - GOT/PLT overwrites
  - Hollowed executables
  - Suspicious process mappings (injected code)
  - Library listing using the loader's data structures
  - Extract process ELF executables and libraries
  - Network interfaces in promiscuous mode
  - Processes that are using raw sockets
  - Hidden kernel modules
  - Netfilter hooks
  - Cached TrueCrypt passphrases

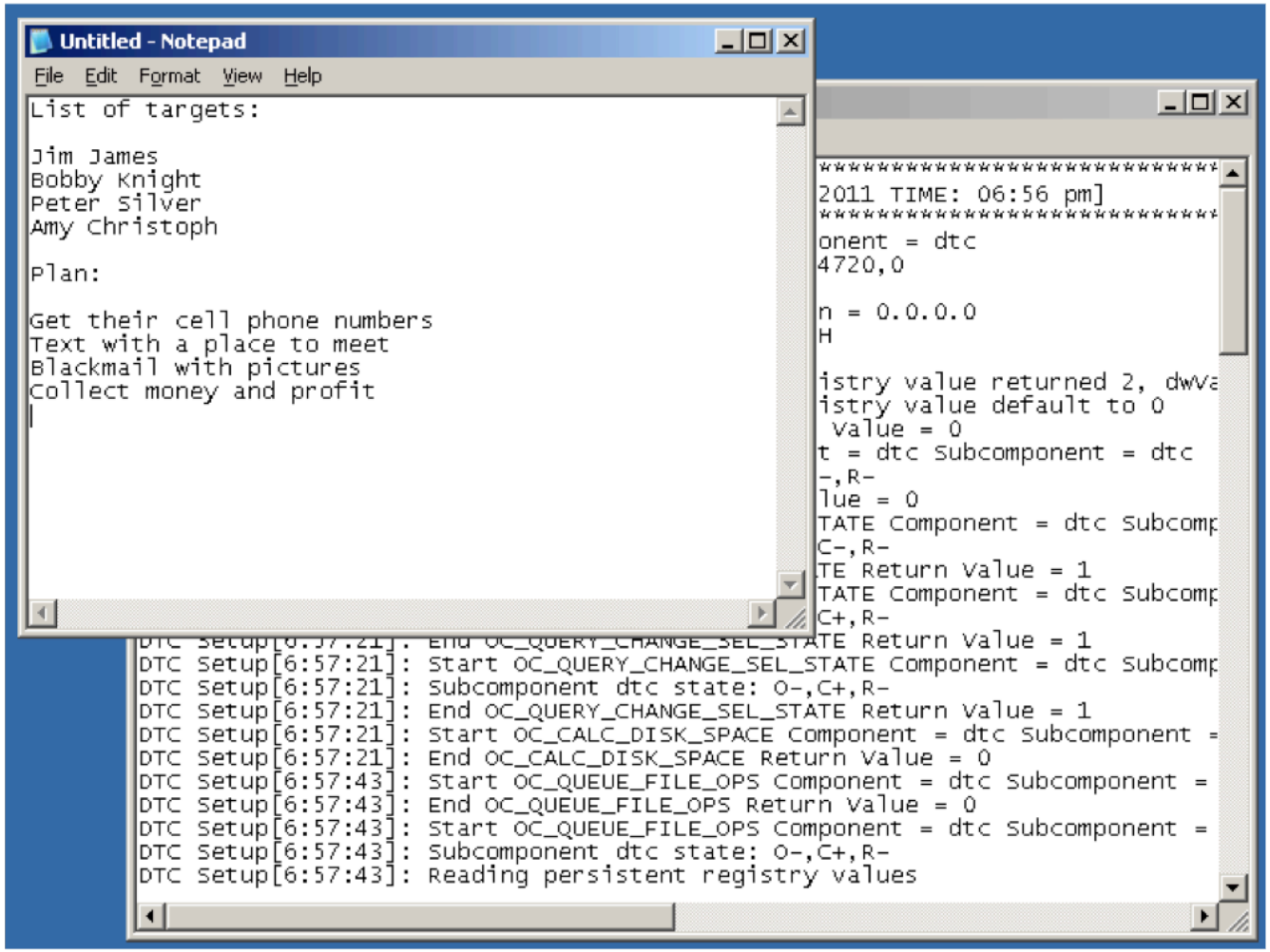
Volatility 2.4: Highlights

- Windows (14 new plugins/108)
  - Windows 8/2012 support
  - TrueCrypt plugins (summary, cached pass, master keys)
  - Apihooks (64-bit/JMP FAR)
  - hashdump, cachedump, and lsadump (x64/Win8/2012)
  - callbacks and timers (64-bit)
  - mftparser (ADS, extract MFT resident blocks)
  - Single pass executive object scanning
  - verinfo plugin (PE version info)
  - auditpol plugin (audit policies)
  - cmdline plugin (process command line arguments)
  - pooltracker plugin (kernel pool tag statistics)
  - bigpools plugin (big page pool allocations)
  - Notepad plugin (application heap)
  - svcscan enumerates service start type

TrueCrypt



Notepad's Heap



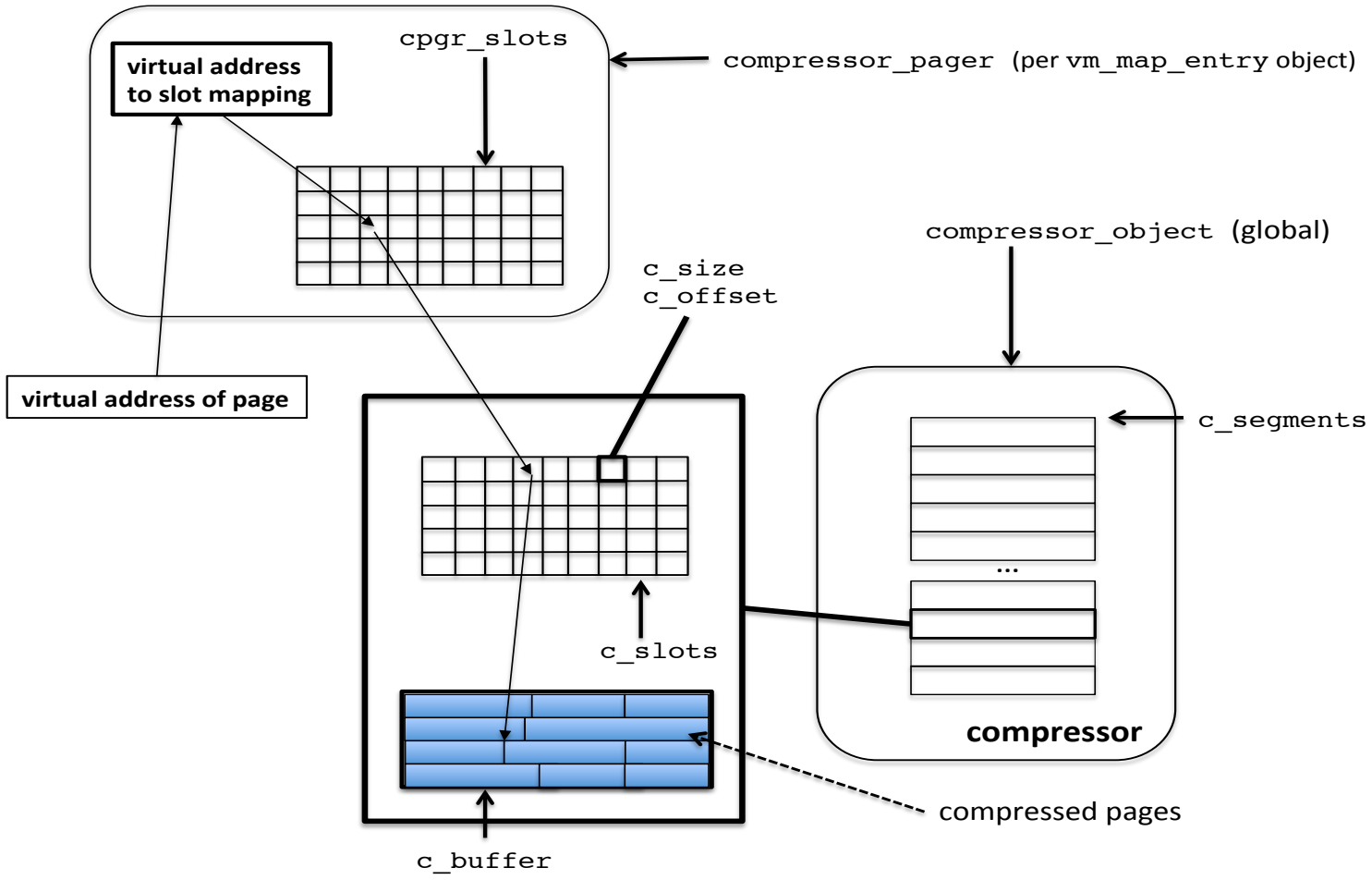
Volatility 2.4: Resources

- Official Volatility Memory Analysis Cheat Sheet
  - Windows, Linux, Mac OS X
  - RTFM-style insert for Windows
  - http://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf
- Volatility demo videos
  - Defeating Truecrypt Disk Encryption
  - Reverse Engineering Rootkits
  - Tracking Mac OS X Activity
  - https://www.youtube.com/channel/UC3AsZ6DGlqZIaPkxF6tXgAA

Volatility Roadmap

- Volatility 2.5 (November 2014)
  - Bug fixes
  - Unified plugin output format
- Volatility 3.0 (2015)
  - “Big Changes”: Refactor/Cleanup/API
  - Unicode improvement/Python 3.0
  - *Performance*

Compressed RAM/Swap



Social Media Artifacts

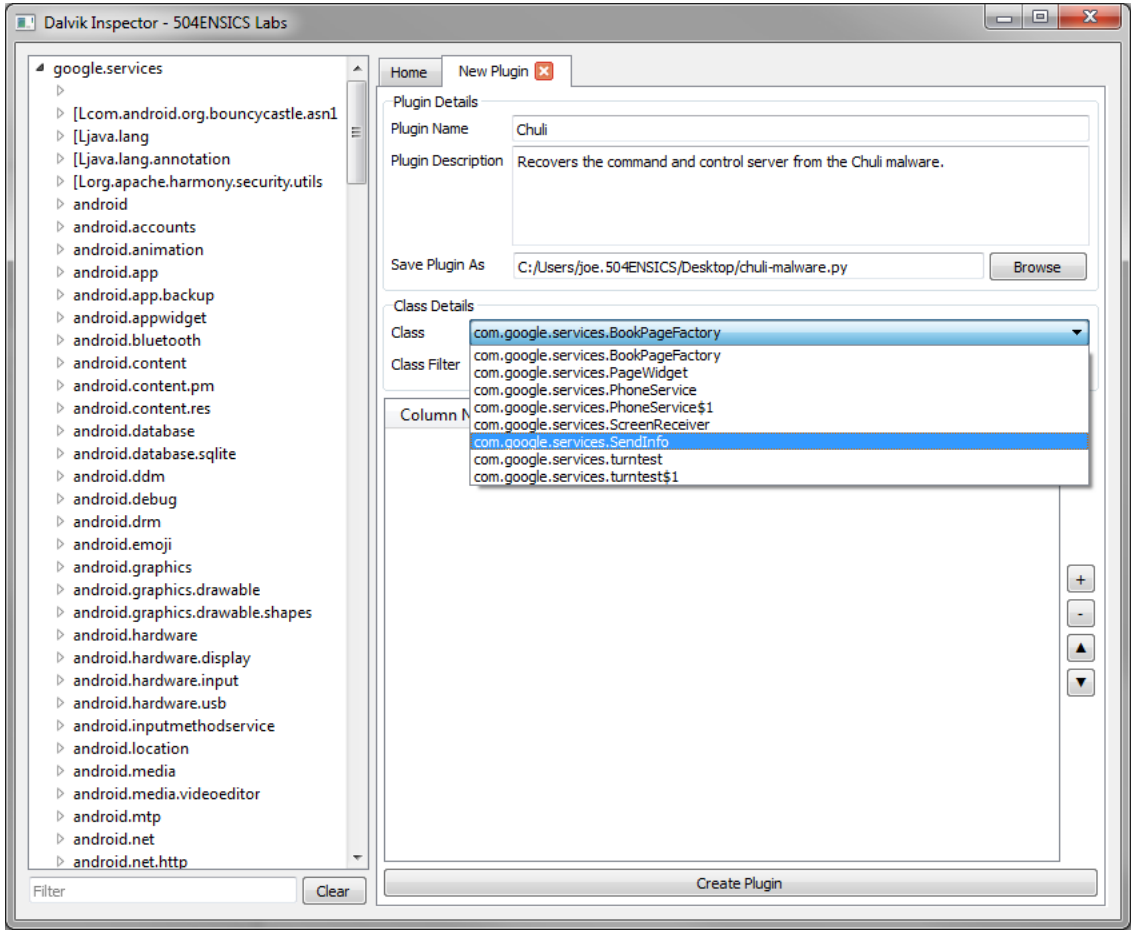
volatility social media plugins

ssl everywhere causes browsers to limit disk storage

memory is where it's at!

```
$vol.py --profile=Win7SP1x64 -f bryner/memimages/win/chrometwitter  twitter
Volatile Systems Volatility Framework 2.3_alpha
searching for browser processes...
found browser pid: 2708, chrome.exe
examining 108010118 bytes
found browser pid: 1800, chrome.exe
examining 127633456 bytes
profile: @p0wnlabs,     3,477 Tweets     921 Following     1,160 Followers
profile: @p0wnlabs,     3,477 Tweets     921 Following     1,160 Followers
6:46 PM - 20 Jul 13 (3m)        @obscuresec     Chris
                @Carlos_Perez @mattifestation @JosephBialek also, did you try HTTP/HTTPs meterpreter?
6:19 PM - 20 Jul 13 (30m)       @VinylMusicHall Vinyl Music Hall
                LIVING COLOUR tonight at Vinyl with special guests LUGOSI! Doors just opened...LUGOSI hits at
 9pm! Tickets still available at the door!
6:47 PM - 20 Jul 13 (3m)        @Carlos_Perez   Darkoperator
                @obscuresec tcp from shell I just execute powershell.exe -nologo
```

Dalvik Inspector



http://www.504ensics.com/blog/

2nd Volatility Plugin Contest

- (Inspired by the Hex-Rays IDA plugin contest)
- Create an innovative and useful extension to Volatility and win the contest!
- **Facebook doubled the prize money!**
- Prizes awarded for top 5 submissions:
  - 1: $2500, 2: $1250, 3: $750, 4-5: Volatility swag
- Core development team judges
  - creativity, usefulness, effort, completeness, submission date, and clarity of documentation.
- 12 submissions worldwide (>30 new plugins!)
- Trend: Application analysis/context

1st Place: Dave Lasalle

- Dave submitted 14 plugins (“Forensic Suite”)
- Recovering Firefox and Chrome artifacts
  - Firefox (3 plugins)
    - History, cookies, downloads
  - Chrome (6 plugins)
    - History, cookies, downloads, visits, search terms
- Java IDX files: Download history of Java archives
- Office TrustRecords : Office files from untrusted src
- Fuzzy hashing to whitelist injected code/API hooks
  - ssdeepscan, malfinddeep, apihooksdeep

Chrome History

$ python vol.py –f voltest.dmp chromehistory --output=csv > output.csv

	A	B	C	D	E	F	G	H
	index	url	title	visits	typed	last_visit	hidden	favicon_id
2	15	https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=What%20is%2		1	0	09:30.1	0	0
3	8	https://www.google.com/webhp?sourceid=chrome-instant&ion=1&e	Google	2	0	58:20.4	0	0
4	13	http://www.ubuntu.com/download/desktop/thank-you/?version=14	Thanks for downloading Ubuntu D	1	0	56:08.0	0	0
5	14	http://www.ubuntu.com/download/desktop/thank-you?country=US	Thanks for downloading Ubuntu D	1	0	56:08.0	0	0
6	12	http://www.ubuntu.com/download/desktop/contribute/?version=14	Contribute to Ubuntu | Ubuntu | U	1	0	56:04.5	0	0
7	11	http://www.ubuntu.com/download/desktop	Download Ubuntu Desktop | Down	1	0	56:01.8	0	0
8	9	https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=ubuntu%20do		1	0	55:46.2	0	0
9	5	http://www.facebook.com/	Welcome to Facebook - Log In, Sig	2	2	09:50.6	0	0
10	7	http://www.cnn.com/	CNN.com - Breaking News, U.S., W	1	1	55:33.5	0	0
11	6	https://www.facebook.com/	Welcome to Facebook - Log In, Sig	2	0	09:50.6	0	0
12	10	http://www.ubuntu.com/download	Get Ubuntu | Download | Ubuntu	1	0	55:54.3	0	0
13	4	http://www.foxnews.com/	Fox News - Breaking News Update	1	1	55:04.1	0	0
14	1	http://tools.google.com/chrome/intl/en/welcome.html	Getting Started	1	0	53:54.4	0	0
15	3	https://www.google.com/	Google	1	1	54:43.9	0	0
16	2	https://www.google.com/intl/en/chrome/browser/welcome.html	Getting Started	1	0	53:54.4	0	0
17								

VOLATILITY

IDX Parser

$ python vol.py –f voltest.dmp idxparser

[*] Section 2 (Download History) found:

URL: http://javagameplay.com/offroadrally/inthejar.jar

IP: 209.188.88.156

<null>: HTTP/1.1 200 OK

content-length: 61699

last-modified: Fri, 10 Oct 2008 20:25:10 GMT

content-type: text/plain

date: Sat, 30 Aug 2014 19:53:56 GMT

server: Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/0.9.8e-fips-rhel5 DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.6

deploy-request-content-type: application/x-java-archive

VOLATILITY

apihooksdeep

- Create the whitelist:

$ vol.py -f D5XLBY3J-bf977e52_lookIE_pid_860.vmss --profile=WinXPSP2x86 vaddump -p 860 -b 0x71590000 -D dumps

[snip]

860 iexplore.exe 0x71590000 0x71608fff dumps/iexplore.exe.24296b8.0x71590000-0x71608fff.dmp

$ python hash_by_page.py -n AcLayers.DLL -f dumps/iexplore.exe.24296b8.0x71590000-0x71608fff.dmp

('AcLayers.DLL', '6:idqLvVg3F+X32xbQ7esfGkxNPWgwh9lorlcIfMfEtj/lkwSM0E/mh6l+tgdwL:eqGSGfP0FWgO9arlcIrUpEec1w'),

('AcLayers.DLL', '96:1SxccXfBWrvZnxbZ3lX26dZC6FsEzSVr6y616GpIHoib8u:uvBWrpxbxGpWEcr3UTpIHPb8u'),

[snip]

VOLATILITY

apihooksdeep

- Now those hooks are not shown:

$ vol.py -f D5XLBY3J-bf977e52_lookIE_pid_860.vmss --profile=WinXPSP2x86 apihooksdeep -p 860

Process: 860 (iexplore.exe)

Hook at 0x715b9e59 in page 0x715b9000 is 100% similar to whitelist hook AcLayers.DLL

Process: 860 (iexplore.exe)

Hook at 0x715ba067 in page 0x715ba000 is 100% similar to whitelist hook AcLayers.DLL

VOLATILITY

2nd Place: dm_dump

- Submitted by Curtis Carmony
- dm-crypt is used on Linux and Android for FDE
- Keying material in physical memory (RAM)
- dm_dump plugin recovers dm-crypt keys from memory and prints commands that can be copy/pasted to mount the volumes
- Will be incorporated into core Volatility soon

VOLATILITY

dm_dump

$ python vol.py linux_dm_dump --profile=Linux3_11_0-15-generic-i686x86 --dm_profile=3.11.0-15-generic-i686-dm.dwarf –f 3.11.0-15-generic-i686.elf

```
Volatility Foundation Volatility Framework 2.4

sda5_crypt: 0 16269312 crypt aes-xts-plain64
c2ca0a6a52980952016936047ab46fba961397978fbf3219ca39fcfdce3b46e2b6348daa09d093351113288c8258bc6
bd3c3d57afab2d6bc3cac7cfde436939b 0 /dev/sda5 4096

ubuntu--vg-swap_1: 0 1040384 linear /dev/dm-0 15163776


ubuntu--vg-root: 0 15163392 linear /dev/dm-0 384
```

$ dmsetup create volatility --table “0 16269312 crypt aes-xts-plain64 c2ca0a6a52980952016936047ab46fba961397978fbf3219ca39fcfdce3b46e2b6348daa09d093351113288c8258bc6bd3c3d57afab2d6bc3cac7cfde436939b 0 /dev/sda5 4096”

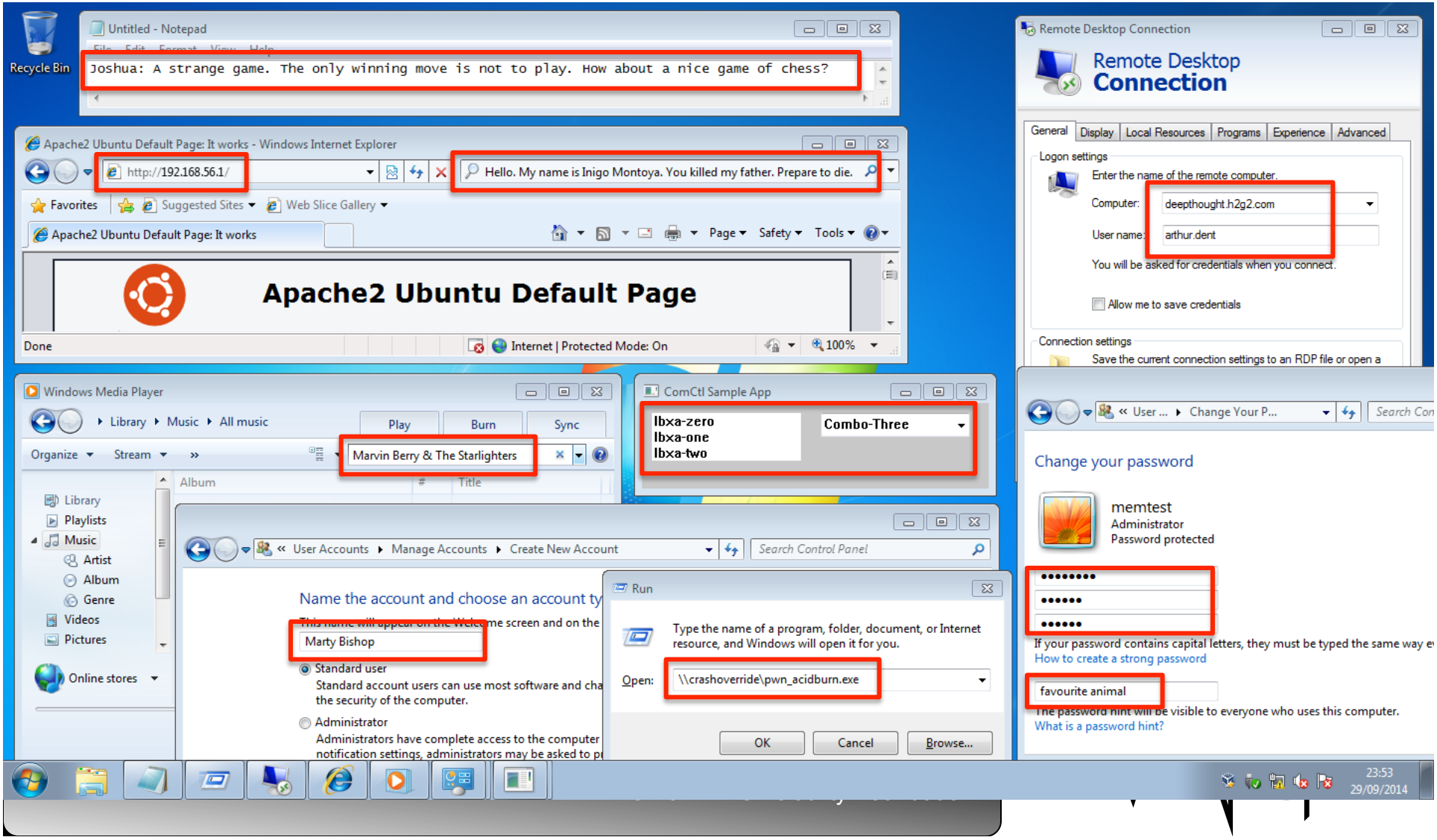
VOLATILITY

3rd Place: editbox

- Written by Adam Bridge “Bridgey The Geek”
- This plugin extracts text from the edit, combo, and list boxes of GUI applications that run on Windows
- Includes, but is not limited to:
  - Notepad window
  - Run dialog
  - Username and server name fields of Remote Desktop Connection
  - Address bar and search bar of Internet Explorer
  - Search bar of Windows Media Player
  - Username field of Create New Account wizard
  - Password of Change Password dialog

VOLATILITY

editbox


Recycle Bin
Untitled - Notepad
Joshua: A strange game. The only winning move is not to play. How about a nice game of chess?
Apache2 Ubuntu Default Page: It works - Windows Internet Explorer
http://192.168.56.1/
Hello. My name is Inigo Montoya. You killed my father. Prepare to die.
Favorites
Suggested Sites
Web Slice Gallery
Apache2 Ubuntu Default Page: It works
Page
Safety
Tools
Apache2 Ubuntu Default Page
Done
Internet | Protected Mode: On
100%
Windows Media Player
Library
Music
All music
Play
Burn
Sync
Organize
Stream
Marvin Berry & The Starlighters
Album
Title
Library
Playlists
Music
Artist
Album
Genre
Videos
Pictures
Online stores
ComCtl Sample App
lbxa-zero
lbxa-one
lbxa-two
Combo-Three
User Accounts
Manage Accounts
Create New Account
Search Control Panel
Name the account and choose an account ty
Marty Bishop
Standard user
Standard account users can use most software and cha
the security of the computer.
Administrator
Administrators have complete access to the computer
notification settings, administrators may be asked to p
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
\\crashoverride\pwn_acidburn.exe
OK
Cancel
Browse...
Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Programs
Experience
Advanced
Logon settings
Enter the name of the remote computer.
Computer:
deepthought.h2g2.com
User name:
arthur.dent
You will be asked for credentials when you connect.
Allow me to save credentials
Connection settings
Save the current connection settings to an RDP file or open a
User ...
Change Your P...
Search Con
Change your password
memtest
Administrator
Password protected
If your password contains capital letters, they must be typed the same way e
How to create a strong password
favourite animal
The password hint will be visible to everyone who uses this computer.
What is a password hint?
23:53
29/09/2014

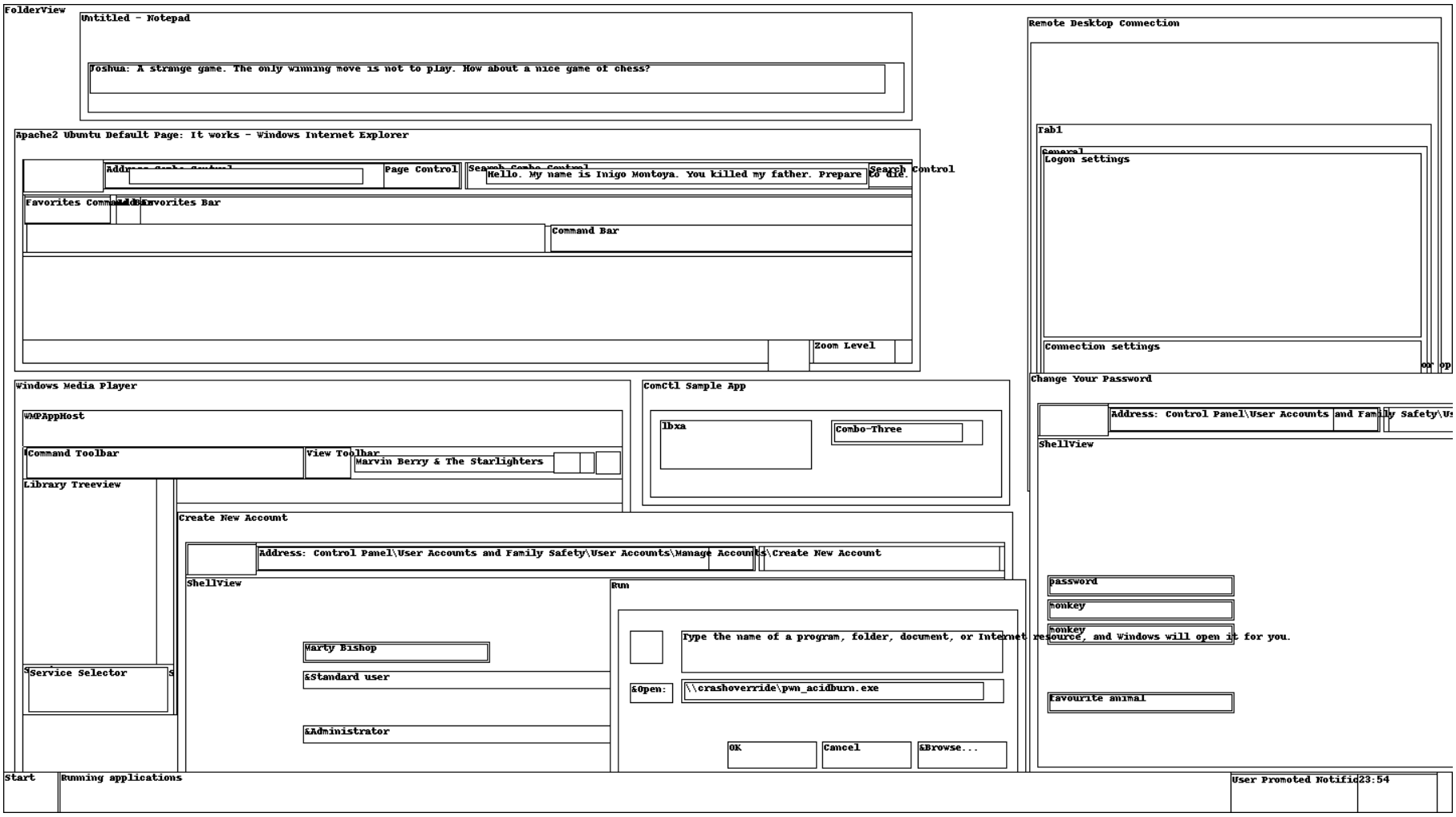
editbox

$ python vol.py --profile=Win7SP1x64 -f WIN7SP1X64-20140929-225403.raw editbox

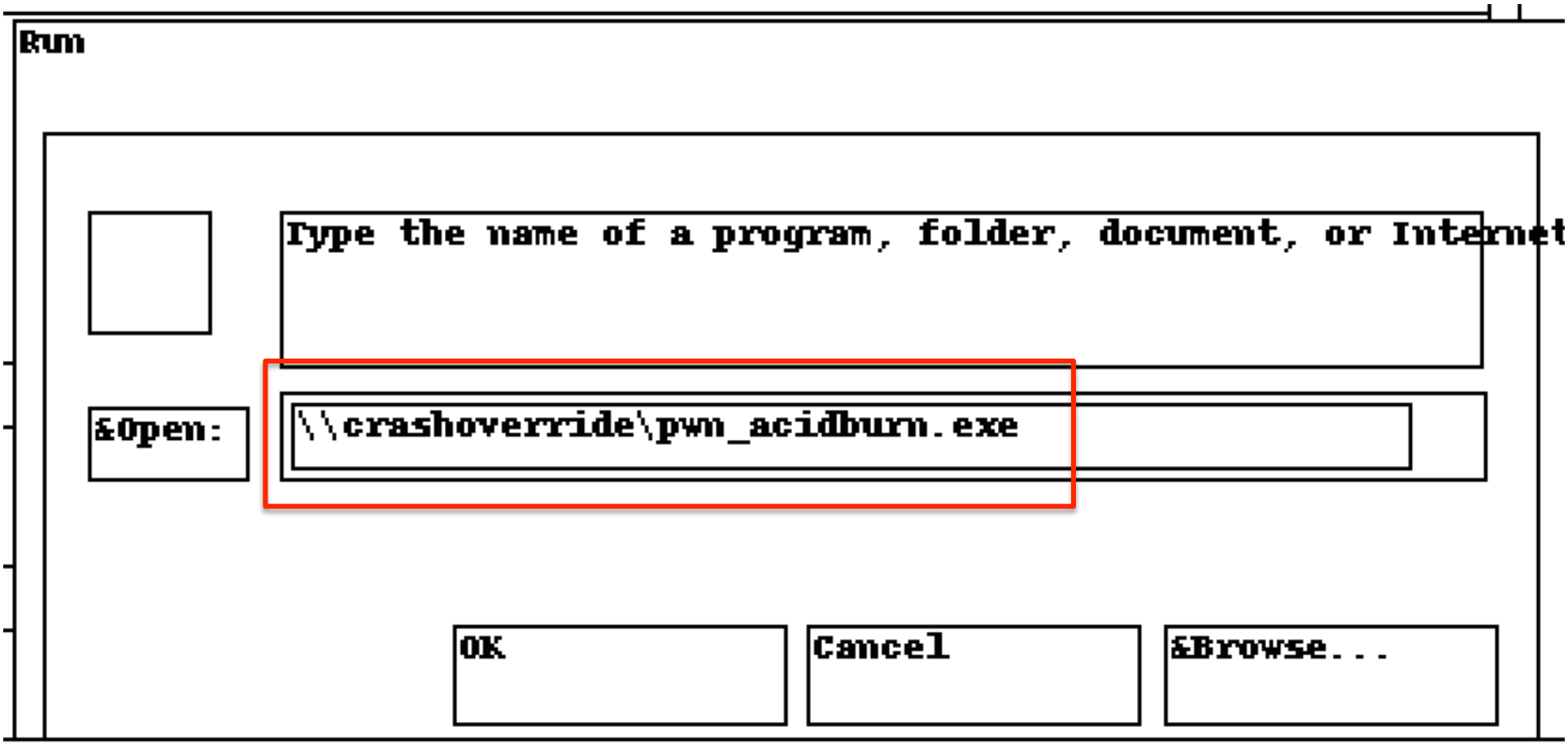
```
Volatility Foundation Volatility Framework 2.4
**************************************************
Wnd context           : 1\WinSta0\Default
pid                   : 2244
imageFileName         : mstsc.exe
wow64                 : No
atom_class            : 6.0.7601.17514!Edit
[snip]
isPwdControl          : No
deepthought.h2g2.com
**************************************************
Wnd context           : 1\WinSta0\Default
pid                   : 1748
imageFileName         : explorer.exe
wow64                 : No
atom_class            : 6.0.7601.17514!Edit
[snip]
isPwdControl          : Yes
pwdChar               : 0x25cf
monkey
```


VOLATILITY

screenshot + editbox



screenshot + editbox



Volatility 2014 Plugin Contest

- 4th Place:
  - Thomas Chopitea: Autoruns – Finding persistence
- 5th Place:
  - Takahiro Haruyama: OpenIOC Scan
- Submissions:
  - Monnappa KA: Gh0stRat Decryption
  - Jamaal Speights: MsDecompress
  - Cem Gurkok: Mac Rootkit and Bitcoin
  - Csaba Barta: Malware Analysis (Baselines)
  - Philip Huppert: OpenVPN
  - Wyatt Roersma: Hyper-V Tools

OMFW 2014

- OMFW first held 2008
- Highly technical venue for digital investigators
- 100% of the proceeds are donated to charity
- What makes OMFW unique:
  - Workshop size
  - Technical content
  - Researchers and developers
  - Peer relationships
  - Cost
  - Lightning talks
- 8 Memory forensics presentations

VOLATILITY

OMFW Agenda 2014

1300PM	The State of Volatility
1330PM	Careto: Accomplishing in 7 Minutes What AV Couldn't Do in 7 yrs
1400PM	Restructuring Memory: Extracting Results in a Reusable Way
1430PM	Science, Sharing, and Repeatability in Memory Forensics
1500PM	Break
1530PM	Many Ways to Skin a RAT: Let's Start with the Tail
1600PM	Memory Forensics for IR: Leveraging Volatility to Hunt Adv Actors
1630PM	Memory Tracing: Forensic Reverse Engineering
1700PM	DAMM: A Tool for Differential Analysis of Malware in Memory
1730PM	Closing Comments/Reception

Volatility Unified Output

List/Tree Hybrid

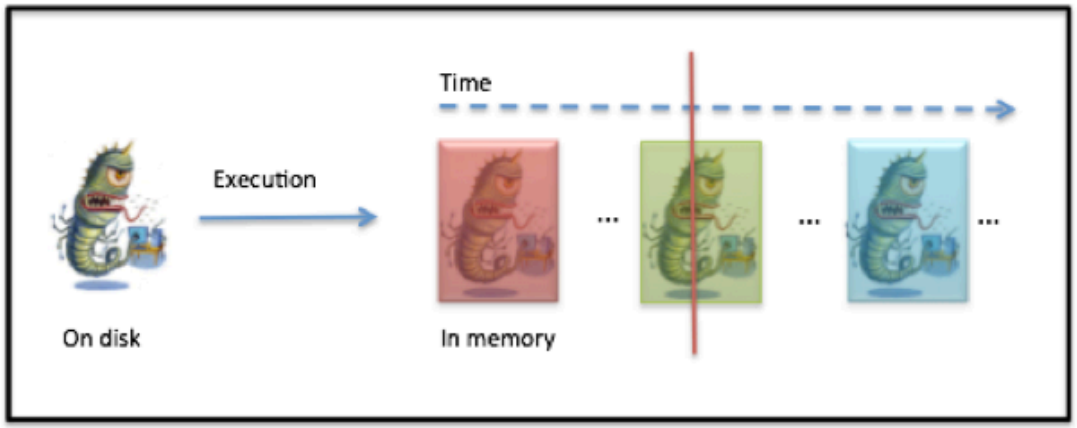
	A (int)	B (unicode)	C (float)

VOLATILITY

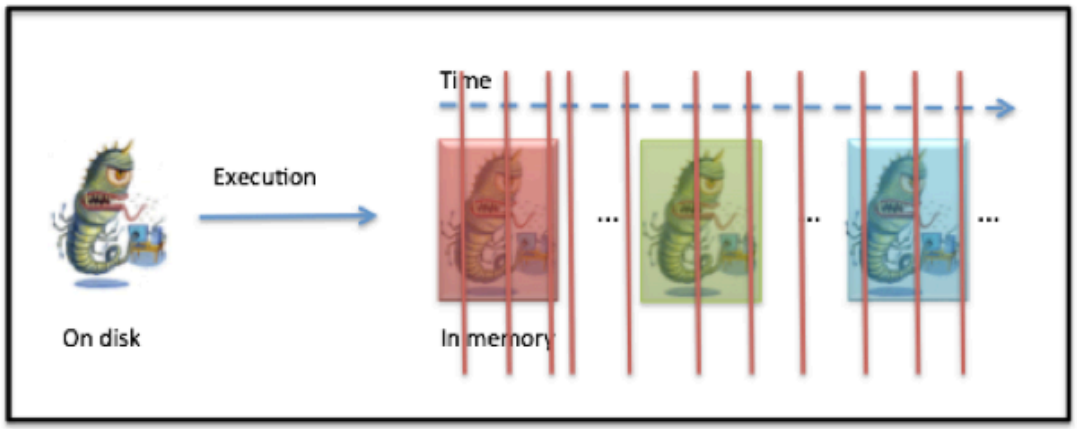
Careto: Memory vs. AV

http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

Memory Tracing



"Traditional" memory forensics



Memory tracing

- **Memory trace** = series of memory snapshots

VOLATILITY

Volatility Training/Certification

- Learn from the actual researchers and developers
- Show your support for open source developers
- Courses
  - Windows Memory Forensics & Malware Analysis
  - Memory Forensics Essentials
  - Mac Memory Forensics & Malware Analysis
  - Linux Memory Forensics & Malware Analysis
- Certifications
  - Memory Forensics Examiner
  - Memory Forensics Professional (Win/Mac/Lin)
- Information: www.memoryanalysis.net

VOLATILITY

Download Volatility 2.4

https://github.com/volatilityfoundation/volatility

http://volatility-labs.blogspot.com/

@volatility

Join the community!

VOLATILITY