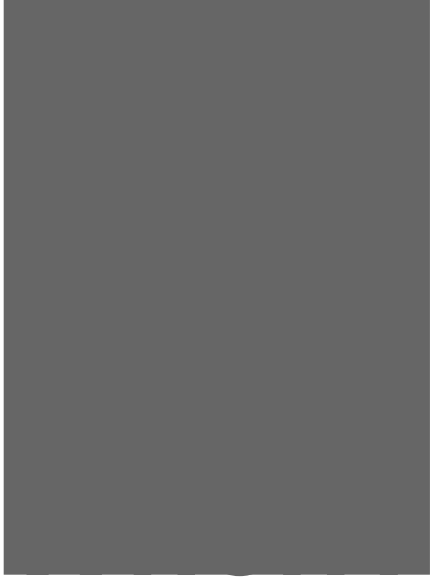
These views are mine alone and don’t reflect those of my employer

You are compromised

- Player (1) Insert coin -



Why?

```
login: root
Password: **********

  Welcome back, root.


root@localhost:~# _
```

```
login: root
Password: **********

  Welcome back, root._


_
root@localhost:~# _
```

3 PILLARS OF INCIDENT RESPONSE

FLEET MANAGEMENT.
DATA COLLECTION.
DETECTION AND RESPONSE.

FLEET MANAGEMENT.

DATA COLLECTION.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

L: github.com/kbandla/APTnotes

Hall of shame of intel sharing.

[on a 3-page threat intel document]

“Here’s a list of domains related to malware X to review your network logs for. Typically, they’re used for phishing or C&C.”

`[proceeds with a list of domains]`

- Hello? C2 traffic and phishing are two very different things.

Hall of shame of intel sharing.

[... on a sample's C2 callback format ...]

```
GET /{ID1}/{ID2} HTTP/1.0
User-Agent: {IE6_UA}HOST: {C2_HOSTNAME}:{PORT}”
```

- Oooooh, shiny! Signature!
- Wait, is it a typo?

Hall of shame of intel sharing.

Same report, later on, in a packet capture of the sample:

```
POST /{ID1} HTTP/1.0
User-Agent: {IE6_UA}
HOST: {IP}:{PORT}
Pragma: no-c ache
```

- Probably a typo... what about that Pragma? Signature or typo?

ALT+F4… == (ノ°□°) ノ ⌒ ┻━━┻

Hall of shame of intel sharing.

[... talking about a phishing e-mail …]

“The hash of the message is _____”

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

```
C:\> md5sum a.exe
10e4a1d2132ccb5c6759f038cdb6f3c9 a.exe

[append data to a.exe]
C:\> md5sum a.exe
17e6317e1a13844078943ba876a31e70 a.exe
C:\> a.exe

[still runs fine :(]
```

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

DETECTION AND RESPONSE.

L: https://medium.com/@magoo/red-teams-6faa8d95f602

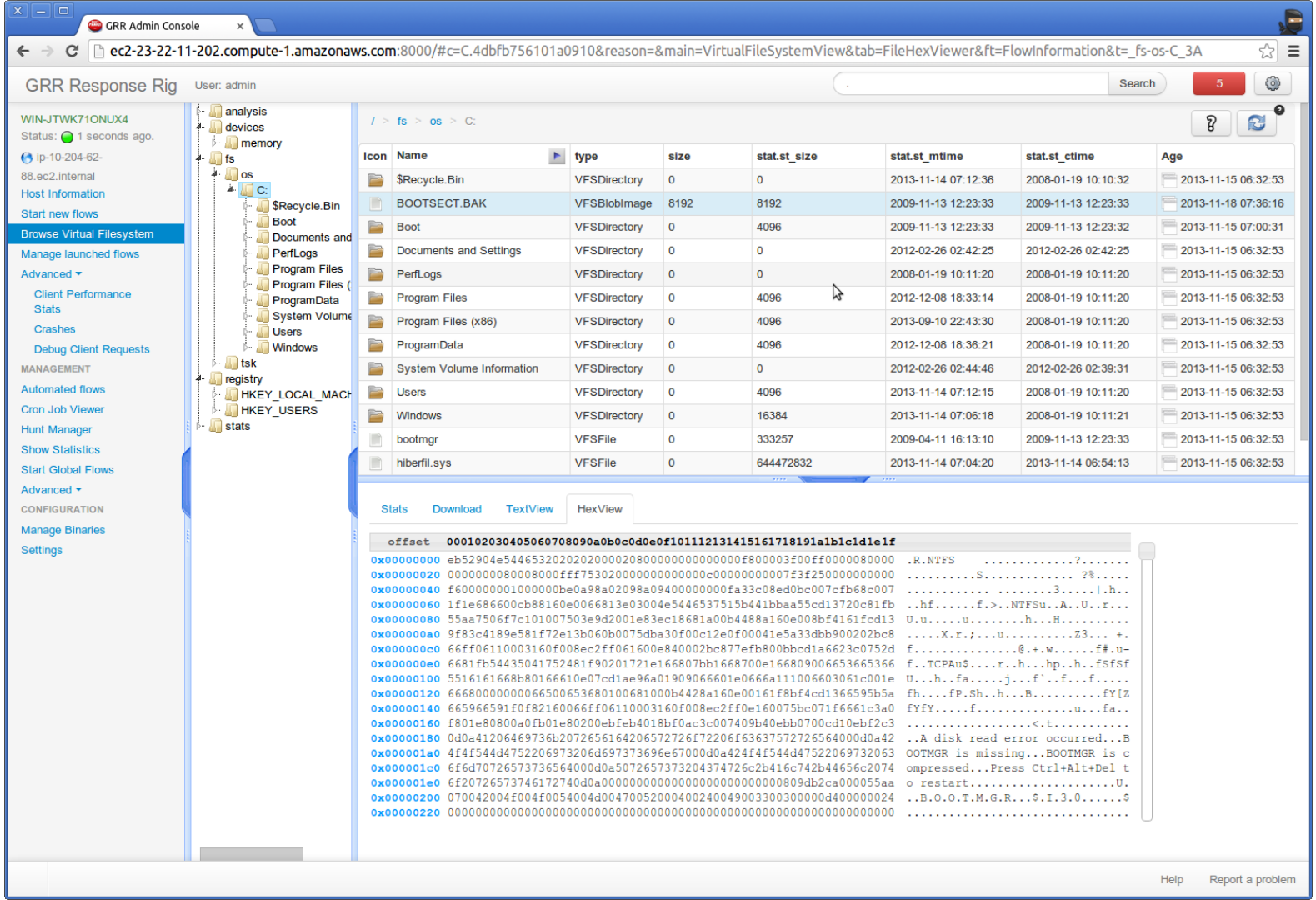
Get a grip on your fleet.
Collect everything. Keep forever. Discard later.
Hire the best. Reward them. Keep them fresh.
Know the limits of your approach. Up your game.
Use the intel. Share intel.
Hunt. Don’t wait: search.
Train. Train. Train.

Become a hunter.

PS:
YOU MIGHT WANT TO CHECK OUT

GRR: SCALABLE REMOTE FORENSICS

- Enables quick, scalable remote forensics.
- Agent-based. Cross platform (Win, OS X, Linux).
  - OS or RAW (TSK) access to the filesystem.
- Most of the logic is server-side.
- Captures state. Stores history.
- Enables hunting on the fleet for host artifacts
  - Apply flows on all or a portion of your fleet.
- Built for analysts.


GRR Admin Console
ec2-23-22-11-202.compute-1.amazonaws.com:8000/#c=C.4dbfb756101a0910&reason=&main=VirtualFileSystemView&tab=FileHexViewer&ft=FlowInformation&t=_fs-os-C_3A
GRR Response Rig
User: admin
Search
5
WIN-JTWK71ONUX4
Status: 1 seconds ago.
ip-10-204-62-88.ec2.internal
Host Information
Start new flows
Browse Virtual Filesystem
Manage launched flows
Advanced
Client Performance Stats
Crashes
Debug Client Requests
MANAGEMENT
Automated flows
Cron Job Viewer
Hunt Manager
Show Statistics
Start Global Flows
Advanced
CONFIGURATION
Manage Binaries
Settings
analysis
devices
memory
fs
os
C:
$Recycle.Bin
Boot
Documents and
PerfLogs
Program Files
Program Files (
ProgramData
System Volume
Users
Windows
tsk
registry
HKEY_LOCAL_MACH
HKEY_USERS
stats
/ > fs > os > C:
Icon
Name
type
size
stat.st_size
stat.st_mtime
stat.st_ctime
Age
$Recycle.Bin VFSDirectory 0 0 2013-11-14 07:12:36 2008-01-19 10:10:32 2013-11-15 06:32:53
BOOTSECT.BAK VFSBlobImage 8192 8192 2009-11-13 12:23:33 2009-11-13 12:23:33 2013-11-18 07:36:16
Boot VFSDirectory 0 4096 2009-11-13 12:23:33 2009-11-13 12:23:32 2013-11-15 07:00:31
Documents and Settings VFSDirectory 0 0 2012-02-26 02:42:25 2012-02-26 02:42:25 2013-11-15 06:32:53
PerfLogs VFSDirectory 0 0 2008-01-19 10:11:20 2008-01-19 10:11:20 2013-11-15 06:32:53
Program Files VFSDirectory 0 4096 2012-12-08 18:33:14 2008-01-19 10:11:20 2013-11-15 06:32:53
Program Files (x86) VFSDirectory 0 4096 2013-09-10 22:43:30 2008-01-19 10:11:20 2013-11-15 06:32:53
ProgramData VFSDirectory 0 4096 2012-12-08 18:36:21 2008-01-19 10:11:20 2013-11-15 06:32:53
System Volume Information VFSDirectory 0 0 2012-02-26 02:44:46 2012-02-26 02:39:31 2013-11-15 06:32:53
Users VFSDirectory 0 4096 2013-11-14 07:12:15 2008-01-19 10:11:20 2013-11-15 06:32:53
Windows VFSDirectory 0 16384 2013-11-14 07:06:18 2008-01-19 10:11:21 2013-11-15 06:32:53
bootmgr VFSFile 0 333257 2009-04-11 16:13:10 2009-11-13 12:23:33 2013-11-15 06:32:53
hiberfil.sys VFSFile 0 644472832 2013-11-14 07:04:20 2013-11-14 06:54:13 2013-11-15 06:32:53
Stats
Download
TextView
HexView
offset 000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
0x00000000 eb52904e5446532020202000020800000000000000f800003f00ff0000080000 .R.NTFS ....?.....
0x00000020 0000000080008000fff753020000000000000c00000000007f3f250000000000 .....S..... ?%.....
0x00000040 f60000001000000be0a98a02098a0940000000fa33c08ed0bc007cfb68c007 ....3.....|.h..
0x00000060 1f1e686600cb88160e0066813e03004e5446537515b441bbaa55cd13720c81fb ..hf.....f.>..NTFSu..A..U..r...
0x00000080 55aa7506f7c101007503e9d2001e83ec18681a00b4488a160e008bf4161fcd13 U.u.....u.....h...H.....
0x000000a0 9f83c4189e581f72e13b060b0075dba30f00c12e0f00041e5a33dbb900202bc8 .....X.r.;...u.....Z3... +.
0x000000c0 66ff06110003160f008ec2ff061600e840002bc877efb800bbcd1a6623c0752d f.....@.+.w.....f#.u-
0x000000e0 6681fb54435041752481f90201721e166807bb1668700e166809066536653666 f..TCPAu$....r..h...hp..h..fSfSf
0x00000100 5516161668b80166610e07cd1ae96a0190906601e0666a111006603061c001e U...h..fa.....j...f`..f...f.....
0x00000120 6668000000006650065368010068100 0b4428a160e00161f8bf4cd1366595b5a fh....fP.Sh..h...B.....fY[Z
0x00000140 665966591f0f82160066ff06110003160f008ec2ff0e160075bc071f6661c3a0 fYfY.....f.....u...fa..
0x00000160 f801e80800a0fb01e80200ebfeb4018bf0ac3c007409b40ebb0700cd10ebf2c3 .....<.t.....
0x00000180 0d0a41206469736b20726561642065726f72206f6363757272656400 0d0a42 ..A disk read error occurred...B
0x000001a0 4f4f544d4752206973206d697373696e67000d0a424f4f544d47522069732063 OOTMGR is missing...BOOTMGR is c
0x000001c0 6f6d70726573736564000d0a507265737320437426c2b416c742b44656c2074 ompressed...Press Ctrl+Alt+Del t
0x000001e0 6f207265737461727740d0a000000000000000000000000809db2ca000055aa o restart.....U.
0x00000200 070042004f004f0054004d004700520004002400490033003000d400000024 ..B.O.O.T.M.G.R...$.I.3.0.....$
0x00000220 0000000000000000000000000000000000000000000000000000000000000000 .....
Help
Report a problem

GRR // LINK GALORE

github.com/google/grr

Presentations

Yahoo! on GRR Hunting - youtu.be/4qCvx3SnAm4
GRR + Plaso + Timesketch - goo.gl/EHjTTa
Greg Castle on Artifacts and Hunting - goo.gl/hVsNrf

PLASO & TIMESKETCH

timesketch

- Plaso is the next generation log2timelin
  - Python-based. Bye, Perl!
  - Efficient container format.
  - Powerful new capabilities: Hashing, VSS, BDE, etc.
- Timesketch: collaborative timeline analysis
  - Experimental. Horizontal view across the fleet.
  - Tagging and saving of views.

github.com/log2timeline/plaso & www.timesketch.org

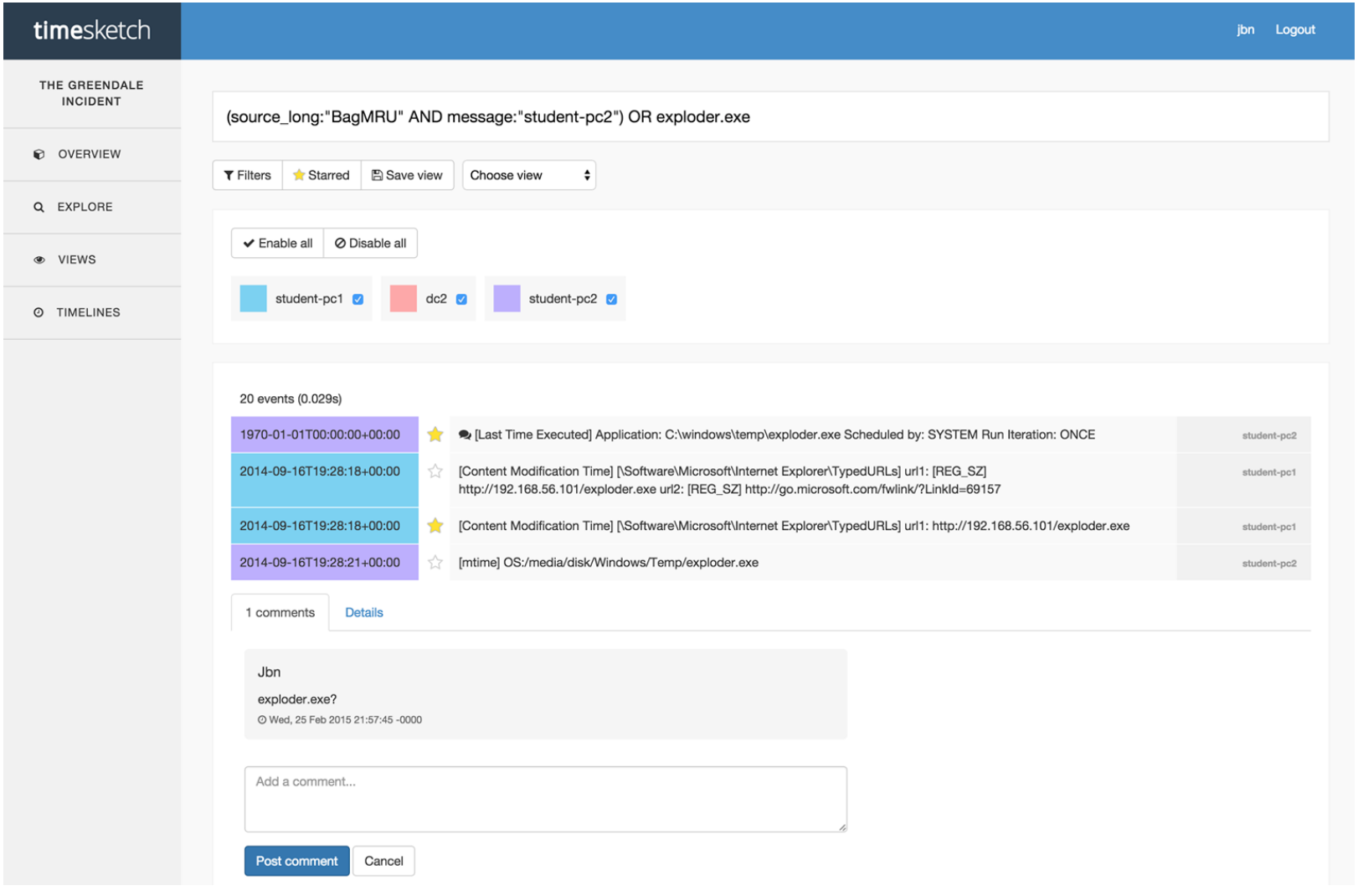
VOLATILITY: MEMORY FORENSICS

- **The original. Tried and tested.**
- **De facto standard.**
- **Bleeding-edge**
  - Has most of the state of the art in memory analysis
- **Large community.**
  - Plenty of external contributions and documentation.

www.volatilityfoundation.org

[NEW!] REKALL: MEMORY FORENSICS

- **Robust acquisition and analysis**
  - All platforms
  - Auto-detection, heap, pagefile, virtualization support...
- **Reporting**: Web UI, JSON.
- Simplicity, accuracy, reusable.
- GRR+Rekall:
  - Scalable, remote, live memory forensics **\m/**


timesketch
jbn
Logout
THE GREENDALE INCIDENT
OVERVIEW
EXPLORE
VIEWS
TIMELINES
(source_long:"BagMRU" AND message:"student-pc2") OR exploder.exe
Filters
Starred
Save view
Choose view
Enable all
Disable all
student-pc1
dc2
student-pc2
20 events (0.029s)
1970-01-01T00:00:00+00:00
[Last Time Executed] Application: C:\windows\temp\exploder.exe Scheduled by: SYSTEM Run Iteration: ONCE
student-pc2
2014-09-16T19:28:18+00:00
[Content Modification Time] [\Software\Microsoft\Internet Explorer\TypedURLs] url1: [REG_SZ] http://192.168.56.101/exploder.exe url2: [REG_SZ] http://go.microsoft.com/fwlink/?LinkId=69157
student-pc1
2014-09-16T19:28:18+00:00
[Content Modification Time] [\Software\Microsoft\Internet Explorer\TypedURLs] url1: http://192.168.56.101/exploder.exe
student-pc1
2014-09-16T19:28:21+00:00
[mtime] OS:/media/disk/Windows/Temp/exploder.exe
student-pc2
1 comments
Details
Jbn
exploder.exe?
Wed, 25 Feb 2015 21:57:45 -0000
Add a comment...
Post comment
Cancel

[NEW!] OSQUERY

- “Easily ask questions about your Linux and OSX infrastructure.”
- SQL-like interface against endpoints.
- Processes, firewall rules, packages, etc.

```
osquery> SELECT uid, name FROM listening_ports l, processes p
WHERE l.pid=p.pid;
```

osquery.io

[NEWish!] SYSMON

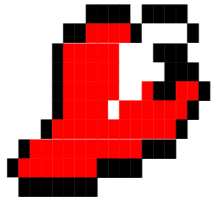
- Designed by the Sysinternals team
  - Mark Russinovich and Thomas Garnier. Enough said.
- One of the the most comprehensive background monitoring solutions for Windows.
  - Process and network monitoring.
  - Hashes of process image files.
- FREE!

[NEW!] STENOGRAPHER

- Open-source full-packet-capture solution.
- “Writes packets to disk, very quickly (~10Gbps on multi-core, multi-disk machines).”
- Designed for very light-weight querying of the data (<1%).
- Ideal for IR work.

github.com/google/stenographer

about:me



Jordi Sanchez [ˈʒɔrði]
You may remember me from….
“LNK Parsing: you’re doing it wrong”
Currently, Incident Response (+R&D)
Rekall - Linux support, Virtualization...
GRR - Rekall integration, plist.
Before: forensics & expert witness, pentester...

github.com/parkisan **@parkisan**