• 10 Presentations

• 360 Seconds Each

• At end of 360 Seconds

• Speaker Stops Speaking

• Audience Erupts Into Applause

• Next Speaker Takes Stage
J. Jewitt

- Wanted: Dead or Alive (Use Cases and Reminders for Live and Dead Box Imaging)
Wanted: Dead or Alive

Tips, Reminders and Use Cases for Live vs. Dead Box Imaging
Caveats

• These methodologies are mine
• Not inflexible
• Methods might vary based on value of target
  – baseline is a routine civil collection
Dead Drive Imaging

- OS not interacting with volume (not system volume)
- OK to boot hardware RAID
- Typically easiest to do “forensically” and “defensibility”
Live Imaging

Imaging software is run on a system that can interact with the target.

Software Solutions

• Forensic Enterprise Software
  – F-Response, Encase Enterprise, FTK Enterprise, etc.

• Live imaging host software
  – FTK Imager, dclfdd, etc.
Less-Than-Forensic

Administrative, built-in file manipulation:

• Robocopy
• Windows Copy
• 3rd party non-forensic tools

Note: Using these methods do not change need for documentation/Chain of Custody
Major Decisions

• What’s the platform?
• What is the target data?
• Are applications running or stopped?
• How much change is likely to occur to a system during imaging process?
General Protocols

In order from least to most proof of integrity

- Application Data Dumps
- Forensic/Non-Forensic File Copy
- Live Logical Image
- Live Physical Image
- Dead Drive Image
When I Do Application Data Dumps

Databases, Email Servers, Financial Applications

• Includes use of 3rd party live extraction tools

• Whenever possible AND
  – Integrity of target data is not in doubt
  – Server cannot be taken down
  – Data requires intensive manipulation to get into equivalent format
  – Output is suitable for its purpose
When I do File Copies

Log Files, User Documents, File Share Data
• Files are not locked by another process
• Interaction with operating system/file system is not a component of investigation
• Media is very large and data needed is much smaller - payoff
• Deleted files are not of concern
• Unallocated space is useless
Live Partition and Drive Collection & “Image Blur”

- $MFT$ Data Read Early
- Data of importance can:
  - Grow
  - Shrink
  - Move
  - Be Created
- Results in apparent corruption
When I Do Live Logical Images

• System cannot be brought offline
• Enterprise agent-based collection
• System is already on (don’t forget the memory dump if needed)
• Blur, corruption of changing data is not a problem
• Physical disk is encrypted
• MBR, unused disk space is not of concern
When I Do Live Physical Images

• System cannot be brought offline
• Enterprise agent-based collection
• System is already on (don’t forget the memory dump if needed)
• Blur, corruption of changing data is not a problem
• Physical disk is encrypted
• MBR, unused disk space is not of concern
When I do Dead Box Imaging

- System is off on arrival, even if I intend to do a logical image too
- After Logical Image
- After Memory Dump
- Defendability:
  - Same hash across multiple images of the same device
  - Usually “best evidence”
  - Logical partition image if SSD drive if hashes must match across multiple images
Stacey Randolph

- The E-Discovery and Forensics Balancing Act
THE E-DISCOVERY & FORENSICS BALANCING ACT

Stacey Randolph Edwards
June 10, 2014
E-DISCOVERY

• What is it?

• What does a client think e-discovery is?

• What does a forensics/e-discovery firm think e-discovery is?
• What is it?

• What does a client think digital forensics is?

• What does a forensics/e-discovery firm think digital forensics is?
CLIENT REQUEST

“We need to collect, search, and produce ALL of the data!”

What is ALL of the data?
QUESTIONS TO ASK CLIENT

• Do you have a court order?
• Do you have all parties identified?
• Do you know how your data is stored?
• Do you need deleted data?
• Do you need searches performed over the data?
• Do you need analysis performed on the data?
IDENTIFYING SOURCES

Human Component
- Court order
- Interviews

Data Component
- Servers
- Computers
- Cloud
- USB/Externals
- BYOD
SEARCHING & PROCESSING

SEARCHING
• Active Files
• Deleted Files
• System Files
• User Documents
• Special Programs

PROCESSING
• Emails
• Documents
• Special Files
• OCR
• Unreadable Files
• Infected Files
DELIVERABLES

- Bates Numbers & Format
- DocID Numbers & Format
- Stamping
  - Page numbers
  - Bates/DocID
  - Confidential
- Special Requests

- Native Files
- TIFF Files
- PDF Files
- Specific Program
  - Concordance
  - Summation
IDENTIFICATION

E-discovery or Forensics?
CONTACT INFORMATION

COMPANY
The Sylint Group
Sarasota, FL
(941) 951-6015
SEdwards@usinfosec.com

SOCIAL MEDIA
Twitter: @4n6woman
LinkedIn: Stacey Randolph
Jonathan Spruill

- How Bad Guys Steal Stuff
HOW BAD GUYS STEAL STUFF

Jonathan Spruill
Senior Security Consultant, SpiderLabs
NOPE
Pete Hainlen

- DNS Hunting Like a Boss
DNS Hunting Like a Boss

Hid.den.net
a2d5xiop8sstun34thxvm.ru
fdxiopstunthxvdyuucqophks.cc
evil.info
sneaky.me
my.crimeware.domain.su
Pete Hainlen

• Threat Analyst, CISSP
• Developer for 4 years
• Sysadmin for 11 years
• Security for 2 years
• Host and network forensics, incident response, proactive hunting
What’s the Big Deal

- Malware goes undetected by antivirus or IDS

“The least-detected malware ... went undetected by the majority of AV scanners for months, and in some cases was never detected at all.”

Picture Source: http://www.funnyjunk.com/funny_pictures/296361/the/

Quote source: http://securityaffairs.co/wordpress/25385/malware/zero-day-malware-detection.html
Why DNS?

• All domain name resolutions are logged
• Easy to pick out the bad stuff
• Augments current detection mechanisms
• It’s cool to impress your boss
Issues

• Scalability
  • 28k per minute
  • 50 million++ DNS requests daily
  • 100,000++ endpoints

• DNS Aggregation
Techniques

• SIEM data export or syslog
• Batch vs. Realtime
• Scripting
  • Python, PowerShell
• Reporting
  • HTML, CSV
Filter

- Only DNS queries with periods
- Known TLDs: com, edu, net
- Only external domains
- Domains you don’t own
- Whitelist: top talkers, trusted domains
Identify

• Threat intelligence Domains
• HR policy violation Domains (porn)
• Phishing Domains
  • Contains: update, helpdesk, admin, account
  • helpdesk-updateweb2014.org
  • Contains: company name derivative
  • your-company-password-update.info
  • Contains: Elevate if 1 or more dashes or .info TLD
• Dynamic DNS: kuozbcwo.servequake.com
• Free DNS: qwfrjali.freehostia.com
• Suspicious TLD’s: .cc, .cn, .ru, .su
Domain Generation Algorithms

• Malware authors use so they don’t get sinkholed

• Domains containing more than 3 digits
  • g4bnv35fw9p.info
  • [regex]::matches($FQDN,\"[0-9]\\").count

• Lengthy DNS names –≥ 20
  • ipudklsbqlddihalsdkhfbpshkd.ru

• 1-hit wonders
Results

• Filtering 50 million++ DNS queries per day down to 1,000 candidate domains
• Not a week has gone by that we haven’t detected threats missed by antivirus
Thanks for your time.
Andrew Hay

- Internet of Perjury (IoP): Asset Identification and Confirmation
Internet of Perjury (IoP): Asset Identification and Confirmation

Andrew Hay, Sr. Security Research Lead & Evangelist, OpenDNS
I wonder if we knew about (and collected) all of the Internet-enabled devices pertinent to this case?
Introduction

● Prove *Internet of Things (IoT)* usage, within a location, based on DNS queries

● The Taxonomy

● Next Steps
Source of Information

- 50m+ Daily Active Users
- 50b+ Queries Per Day
- 10k+ Paying Security Customers
OpenDNS IoT Taxonomy (Io2T)
Personal Electronics

- **Fitness**
  - FitBit, scales, etc.
- **Toys**
  - Helicopters, children’s tablets, etc.
- **Gadgets**
  - Video and still cameras
Personal Electronics: Examples

- Fitness & Health
  - Fitbit Flex/One/Zip
  - Fitbit Aria WiFi Scale
  - iFit

- Toys
  - Microgear Cloud Rover
  - LeapFrog LeapPad
  - Vtech InnoTab

- Gadgets
  - Pebble watch
  - WD MyCloud
  - Amazon Kindle
Personal Electronics: Examples

api.nike.com

wd2go.com
Consumer Appliances

- Large appliances
  - Refrigerators, stoves, etc.
- Small appliances
  - Toasters, blenders, etc.
- Entertainment
  - Televisions, media players, game consoles, etc.
Consumer Appliances: Examples

- Large Appliances
  - Refrigerator
  - Oven
  - Washer/Dryer

- Small Appliances
  - Egg Minder
  - Aros Air Conditioner
  - Kolibree Toothbrush

- Entertainment
  - AppleTV
  - Kindle Fire
  - Roku
**Consumer Appliances: Examples**

*live.xbox.com*

![Graph showing DNS queries for live.xbox.com over a period*]

*mysmartappliances.com (Whirlpool)*

![Graph showing DNS queries for mysmartappliances.com (Whirlpool) over a period*]
Home Automation

- External Home
  - e.g. lawn maintenance devices
- Power management
- Heating, ventilation, and air conditioning (HVAC)
Home Automation: Examples

- External Home
  - LiftMaster (garage)
  - SmartDroplet
  - Irrigation
  - Caddy

- Power Management
  - Philips Hue
  - Valta
  - Pivot Power Genius

- Heating, Ventilation, and Air Conditioning (HVAC)
  - Nest Thermostat
  - Honeywell Thermostat
  - Friedrich Kuhl A/C
Home Automation: Examples

cloud.irrigationcaddy.com

production.nest.com
Security & Monitoring

- Audio/Video
  - Cameras
  - Baby monitors

- Physical locks

- Alarm systems

- Environmental monitors
  - flood, CO$_2$, and fire detection
Security & Monitoring: Examples

- Audio/Video and Alarm Systems
  - D-Link Camera
  - SkyBell Wi-Fi Doorbell
  - Dropcam Baby Monitor

- Physical Locks
  - Kwikset Kevo
  - Lockitron
  - Schlage LiNK + bridge

- Environmental
  - INSTEON Water Leak Sensor
  - Nest Protect
  - Netatmo Weather Station
Security & Monitoring: Examples

signal.mydlink.com

api.lockitron.com
Home/Work Wall Eroding
A Word About Refresh Cycles…

Appliances

The life expectancy of a typical appliance depends to a great extent on the use it receives. Moreover, appliances are often replaced long before they are worn out because changes in styling, technology and consumer preferences make newer products more desirable. Of the major appliances in a home, gas ranges have the longest life expectancy: 15 years. Dryers and refrigerators last about 13 years. Some of the appliances with the shortest lifespan are: compactors (6 years), dishwashers (9 years) and microwave ovens (9 years).

Productizing Research

- Identify and categorize IoT domains into Umbrella
- Create community for IoT telemetry submissions
  - e.g. PCAPs, IPs, domains, URLs, etc.
- Provide access to Law Enforcement and DFIR community
  - Open IoT Database
Thank You!

Andrew Hay

ahay@opendns.com

linkedin.com/in/andrewhay

@andrewsmhay
Alissa Torres

- False Positive: The Eye of the Biased Examiner
False Positive:
The Eye of the Biased Examiner

Alissa Torres
SANS Institute
atorres@sans.org
@sibertor
“The eyes are not responsible when the mind does the seeing”
- Plubilius Syrus
What is Bias?

• An inclination to present or hold a partial perspective at the expense of (possibly equally valid) alternatives

• **Part of human nature** - based on how our brains subconsciously make decisions

• Bias has negative impacts on how we process data and **can lead to inaccurate findings**
Problems with ambiguity
How does Bias Affect Investigations?

Confirmation Bias

• The tendency to search for or interpret information in a way that confirms one’s preconceptions or favored theory

• When an investigator seeks evidence in a effort to support existing beliefs
How does Bias Affect Investigations?

**Anchoring**

- Effects of Outside Influences

- “Start from scratch with your research. Don’t assume the current tools and books are right.”

  - Dan Pullega “Dr. Shellbags”
How does Bias Affect Investigations?

Availability

- Basing conclusions on past experiences, assuming current case will match patterns of past investigations
How does Bias Affect Investigations?

Loyalty to the Tool

- “Don’t let your tools make you stupid”
  - Troy Larson
Strategies to Avoid Bias

- Raise Awareness.
- Admit it.
- Change the process.
- Make alternative perspectives OK.
- Seek creativity rather than consensus.
Jake Williams

- Forensics Survivor: Key Artifacts That Aren’t Being Voted off the Island
Forensics Survivor: What artifacts aren’t being voted off the island?

Jake Williams
@MalwareJake
$\textit{whoami}$

- I only have SIX MINUTES (!?!?) to deliver this whole talk, come talk to me after if you care
What’s this all about?

- Every time I turn around, there are more and more “critical” forensics techniques to apply
  - Where will it end?
- Every new technique can’t be a “must do”
- Clearly it’s time to vote some off the island!
  - Survivor style!
Mud Volleyball?

- Do they really play volleyball on Survivor???

Voted Off The Island!!!

• Processing a full disk image before doing any analysis
• Need answers sooner, not later
• Techniques that deliver speed win!

http://gosurvive.blogspot.com
Filesystem Journals

• NTFS journaling has traditionally not been well understood
  – True correlation with $MFT was unheard of
• All of that has changed with Advanced NTFS Journal Parser (aka TriForce)
  – See David Cowen here at the Summit and talk to him about his awesome tool
Don’t Suck At Filesystem Journals

- Cowen makes it seem like we were doing it wrong when we looked at $MFT without truly correlating them to entries in $LogFile and $UsnJrnl
  - Because we were **doing it wrong**!
Voted Off The Island!!!

• Looking at $MFT$, $LogFile$ and $UsnJrnl$ in isolation
Memory Acquisition (Yesterday)

- Most memory forensics tools depend heavily on knowing the OS version
  - Currently used methods for determining version involve scanning through memory for OS structures like KDBG
- This then requires profiles to be built containing definitions for other OS structures
Voted Off The Island!!!

• Taking full memory dumps from machines with mega RAM
Memory Acquisition

• In many cases we acquire the memory image ourselves as part of IR
  – Why not acquire information about the OS as well
    – including offsets to critical structures?

• Good question – Rekall and WinPmem are working to make this a standard
  – Query the OS during the memory dump to record information that must be inferred later
Memory Artifacts

• The size of memory is growing faster than the average write speeds
  – More changes in memory *during* acquisition

• Tools that parse artifacts from live memory, with a minimal footprint need to be developed
  – Or refined – if you like the ones that already exist
Volume Shadow Copies

- Coolest. Thing. Ever. What more can I say?

Volume Shadow Copies (2)

- VSCs kick butt in a huge way
- When combined with hibernation files, they provide a true Window to the past
- Did you know that $MFT$ gets backed up in VSS? Yeah, that’s a big win!
  - $LogFile$ does too – and that makes me happy 😊
VSC + Hibernation = Holy Cow

Hiberfil.sys in VSC – Yeah Baby!

• I’ve had cases turn recently based on hibernation files in VSC
  – One case involved a laptop that hibernated when the lid was closed
  – Another case involved a desktop set to hibernate when it had been idle for too long

• Too many investigators ignore the forgotten wonders of VSC and few get the hiberfil.sys
Questions?

• Ain’t nobody got time for that, this is SANS360!
• Getting up to Speed on REKALL
Rekall Memory Forensics
Elizabeth Schweinsberg
What is Rekall?

● A fork of the Volatility memory analysis framework.
  o Fully open source and GPL - all commits are public.
  o Focus on:
    ▪ code quality - code reviews.
      ● Most of the code is rewritten/updated.
    ▪ performance.
    ▪ ease of use as a library - Integrated into other tools.
      ● E.g. GRR, plaso (nee log2timeline)
How is it different from Volatility?

- Rekall uses a different design philosophy:
  - Exact symbol information for the analyzed system
    - e.g. Fetch from Microsoft Symbol Server.
  - Store profiles in a public profile repository
    - Rekall fetches the required profile at runtime.
    - We have over 200 different kernels in the repository.
    - Matching PDB GUID increases transparency of mapping the right kernel.
How is it different from Volatility?

- This means we do not need to guess or try to deduce global symbols.
  - This makes Rekall much faster, more efficient and more accurate.
  - For example, Rekall does not use the Kernel Debugger Block
    - This can easily be overwritten by malware. Or newer versions of Windows.
How is it different from Volatility?

- Rekall distributes and supports a complete memory acquisition solution.
  - We have synergy between acquisition and analysis.
  - Support all major operating systems:
    - Windows - Winpmem tool.
    - Linux - pmem tool.
    - OSX - OSXPmem tool (supports 10.9.3).
  - Rekall acquisition tools allow for live system analysis (Triaging etc).
Rekall user interfaces.

- Command line interface.
- Interactive IPython console - very fast.
- IPython notebook.
- New web console - Rekall specific web interface.
PPHYSICAL_MEMORY_DESCRIPTOR NTAPI MmGetPhysicalMemoryRanges(void);

We can get Rekall to disassemble this function for us. First we initialize the notebook, opening the winpmem driver to analyze the live system. Since Rekall uses exact profiles generated from accurate debugging information for the running system, it can resolve all debugging symbols directly. We therefore can simply disassemble the function by name:

```
In [2]: from rekall import interactive
interactive.ImportEnvironment(filename=r'\\\pmem')

Initializing Rekall session.
Done!
```

```
In [3]: dis "nt\MmGetPhysicalMemoryRanges"

<table>
<thead>
<tr>
<th>Address</th>
<th>Rel Op Codes</th>
<th>Instruction</th>
<th>Comm</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8000002cd9690</td>
<td>0 488bc4</td>
<td>MOV RAX, RSP</td>
<td></td>
</tr>
<tr>
<td>0x8000002cd9693</td>
<td>3 48895808</td>
<td>MOV [RAX+0x8], RBX</td>
<td></td>
</tr>
<tr>
<td>0x8000002cd9697</td>
<td>7 48896610</td>
<td>MOV [RAX+0x10], RBX</td>
<td></td>
</tr>
</tbody>
</table>
```
bash  Scan the bash process for history.

<table>
<thead>
<tr>
<th>Pid</th>
<th>Name</th>
<th>Timestamp</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>ls -lah</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>dmesg</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>exit</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>ifconfig</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>halt</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>exit</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>exit</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>ifconfig</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>ifconfig -a</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>dhclient eth1</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>ifconfig -a</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>mkdir .ssh</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>apt-get install build-essential</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>apt-get update</td>
</tr>
<tr>
<td>2481</td>
<td>bash</td>
<td>2014-05-08 08:52:05+0000</td>
<td>./lmap -d</td>
</tr>
</tbody>
</table>
http://www.rekall-forensic.com/
JP Bourget

- The Need for Network Security Monitoring (a.k.a. Capture all the Things)
The Need for Network Security Monitoring

Capture all the things

JP Bourget

@punkrokk
Agenda

• What is NSM
• A reference NSM stack
• Why is it useful
• How does it apply to DFIR?
• Review
Network Security Monitoring

• Definition:
the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions (or policy violations).

Source: Richard Bejtlich

• Application: Storing Full Packet Capture (FPC), Bro logs, Snort logs and more to go back and look at interesting and anomalous network activity
Bro?

• Bro (bro.org):
  – Provides rich application protocol logging and analysis
  – Provides a network event driven, policy agnostic scripting language to interact with your network
  – You can
    • Count things, measure things, notice things, check things, match things
  – If you have never looked at Bro, you may want to
Example NSM Stack (Security Onion)

- **Ethernet SPAN/TAP**
- **pfRing / Berkeley Packet Filters**
- **Logs (https)**

**Collection**
- Bro NSM
- IDS
- PRADS Sancp
- Netflow
- Full PCAP
- OSSEC agent

**Storage & Indexing**
- squid
- ELSA & sphinx

**Presentation**
- Squil Client/Squert
- ELSA Web or Splunk
- grep/sed/awk perl/python

**Syncurity Networks**
Why is it useful for DFIR?

- Provides the Ground Truth of what happened
- It’s becoming cheap to store Full Packet Capture for long periods of time
- Let’s you put together a larger picture than host based analysis – FAST! (e.g. who clicked that phishing email)
- Let’s you figure out what actually happened with that mysterious SIEM alert – you can see the network traffic
- Warning: Encryption causes us to lose some visibility (don’t bother capturing it)
Lots of Resources

- Applied NSM by Chris Sanders (2014)
- Securityonion.net (Wiki and distro)
- Lots of great blogs: Tao Security, bammv.github.io/sguil/docs.html, David Bianco,
- #snort-gui on Freenode, various tools mailing lists
Consider It

Consider learning more about NSM – it’s becoming an important part IR!

Thanks!

JP Bourget

@punkrokk

jp@syncurity.net
• Thank you for attending!

• Please fill out speaker evaluations on your way out.