• 10 Presentations
• 360 Seconds Each
• At 1 Minute Left — Warning
• At Bell —
  — Speaker Stops Speaking
  — Audience Erupts Into Applause
  — Next Speaker Takes Stage
Kyle Maxwell

- Don’t Be a Script Kiddie
Don't be an IT script kiddie

Why you need to learn to program

Kyle Maxwell
@kylemaxwell
"THINK DIFFERENT" no more programming your //e...
so tired...
I thought you were professional...
You don't have to be this guy.
LOGICAL AWESOME
My Codes Are Perfect
EMBRACE IT
J Jewitt

- Incident Readiness – Top 10 Keys to a Successful Forensic Investigation
Incident Readiness –

Top 10 Keys to a Successful Forensic Investigation

- J Jewitt KMPG
Why these 10?

- Common issues
- Decrease accuracy of reporting
- Not related to system hardening
- Implemented without major infrastructure changes
- Relevant to external and internal threats
- 243 Days to discover APT – Mandiant Report – Need more data!
#1 Increase Log Retention

Permanently increase logging to align with retention goals

<table>
<thead>
<tr>
<th>Resource</th>
<th>Retention Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server Logs</td>
<td>6 Months</td>
</tr>
<tr>
<td>Critical Server Activity</td>
<td>6 Months</td>
</tr>
<tr>
<td>Proxy/Firewall Logs</td>
<td>12 Months</td>
</tr>
<tr>
<td>Antivirus (Central Logging)</td>
<td>12 Months</td>
</tr>
<tr>
<td>Workstation Activity</td>
<td>2 Months</td>
</tr>
<tr>
<td>Non-critical Server Activity</td>
<td>3 Months</td>
</tr>
</tbody>
</table>

* Push to 13 months whenever possible or align with legal mandates when applicable
#2 – Map The Architecture

- DMZ, VPN, DHCP Ranges
- Packet Transformation – NAT, Proxy, Load Balancers, VPN
- High Value Targets – Key Infrastructure, Vulnerable/Critical Infrastructure
#3 – Centralize Antivirus Logging

AV Detection does NOT mean you’re safe!

AV Alerts often trigger on supporting tools and downloaders
during early attack phases for sophisticated throughout for more aggressive attacks

Log antivirus events centrally
AV Management Utilities
Syslog
Multiproduct SEIM (Arcsight, Splunk, etc.)
Missed Opportunity

01.MM.2012 03:41:27  Gen: Trojan.Heur.VP.Sm0@auImLmdO file
"C:\_DIR\PASSVIEW.EXE" quarantined success

02.MM.2012 15:11:07  Gen: Trojan.Heur.VP.Sm0@auImLmdO file
"C:\_DIR\PASSVIEW.EXE" quarantined success

09.MM.2012 00:14:34  Gen: Trojan.Heur.VP process "3744|c:\_DIR\expserv.exe"
terminated success

09.MM.2012 00:14:36  Trojan.Generic.KDV file "C:\Users\Owner\Desktop\snpa.exe"
quarantined success

09.MM.2012 00:14:36  Trojan.Generic.KDV file
"c:\users\owner\appdata\roaming\explorer.exe" quarantined success

09.MM.2012 00:14:36  Trojan.Generic.KDV registry "HKEY_USERS\S-1-5-21-1212355515-3628736063-2386788563-1001\Software\Microsoft\Windows\CurrentVersion\Run|Explorer" quarantined success

09.MM.2012 00:14:36  Gen: Trojan.Heur.VP.Sm0@auImLmdO file
"C:\_DIR\PASSVIEW.EXE" quarantined success

...
#4 – NTFSDisableLastAccessUpdate = False

Windows Vista + is Default “True”
Windows XP/Server 2003 & earlier is Default “False”

Key (False) allows time to be updated when:
- Opened
- Copied
- Modified

Key (True) allows time to be updated when:
- Usually only Modified or Created
Important for: All Incidents

Restore Points contain:
- Registry Snapshots for main registry hives and user hives
- Link Files
- Modified/replaced system binaries

Volume Shadow Copies contain:
- Registry Snapshots for main registry hives and user hives
- Link Files
- Modified/replaced system binaries
- Log files
- Modified config files
- Some modified user documents

TOOLS for VSC Analysis are improving!
#6 – Document Standard Build Vulnerabilities

- Default passwords
- Local Accounts
- Service Accounts
- Outdated or vulnerable software
- Document Baseline Installed Applications

Password re-use = spread of malware
#7 – Create and Deploy Forward Systems

Send to remote offices to speed response

- Forensic Imaging/Analysis Software (EnCase Enterprise, FTK Enterprise, iSCSI solution)
- Memory Dumping/Analysis Tools
- PSExec
- Your favorite open source analysis tools
- Encrypted USB Drives
- Consider VMWare for working with possible malware
#8 – Establish Helpdesk Protocol

- Users may have computers rebuilt or wiped when under investigation
- Request affected machines not be wiped by IT staff
- Ask them if they have noticed an increase in suspicious computer events, password lockouts, blue screens, etc.
- Access to ticketing system to identify work done to infected systems or look for patterns across locations
#9 – Establish Chain of Custody and Preservation Protocols

**Chain of custody** – documentation of personnel that have had positive control of evidence

**Preservation Protocols**

- Understand when to wipe or not wipe compromised systems
- Be able to identify, extract and ship data used in investigation
- Know when to preserve systems used by employees under suspicion

**Consider Training First Responders on Data Preservation**
#10 – Change Control Pre-Incident

Change Control advanced approval for IR Agents

- Mandiant MIR
- EnCase Enterprise
- AD Enterprise
- HB Gary
- Memory Dump Tools
NEXT!

J Jewitt
Sr. Consultant
Forensic Technology Services, KPMG
jjewitt@kpmg.com
Brian Lockrey

- Social Media Forensics
Brian Lockrey

Social Media Digital Forensics

SANS Forensics and Incident Response Summit

Austin, Texas
July 9-10, 2013
Find out more about a Social Media Photo or URL during an investigation...
Using Google Images
http://images.google.com
Social Media Digital Forensics

Google Nigeria

Please Enter Your Bank Account Number:

[Input field]

Search For Inheritance
Social Media Digital Forensics
Social Media Digital Forensics

765-543-8938

1DataRecovery.com
@1DataRecovery

Digital Forensics, Data Recovery, Insider Forensics; Investigations; Data Conversion; Disaster Recovery; Social Media Investigations ~

8,694 TWEETS
19,757 FOLLOWING
18,112 FOLLOWERS

Follow
Social Media Digital Forensics
Social Media Digital Forensics

Save As...
Social Media Digital Forensics
Social Media Digital Forensics
Social Media Forensics

Search by image
Search Google with an image instead of text.

Paste image URL | Upload an image
Choose File No file chosen  Try dragging an image here.
Social Media Forensics
Social Media Forensics
Social Media Forensics

COLUMBUS, [Ohio], [United States] - Twitter Elite By Location...
(tweet.grader.com/location/?Location=Columbus%2C...States ▼)
48 x 48 - Rank, Name, Bio, Grade, Followers, Updates, Location, Action.
1 bluejacketsnhl NHL Blue Jackets bluejackets.n
2 dealseekingmom Tara Kuczykowski dealseekingmo

Brian Lockrey | Facebook
(https://www.facebook.com/1datarecovery ▼)
50 x 50 - Brian Lockrey is on Facebook. Join Facebook to connect with Brian Lockrey and others you may know. Facebook gives people the power to share and makes ...

2 - The Shorty Awards
(1st.shortyawards.com/user/1datarecovery?page=2 ▼)
80 x 80 - Assist Data Recovery; Discount Computer Repair; Data Recovery; Computer Forensics; Investigations; Disaster Recovery ~ Tweets and pics by Brian ...

GMU 2013 | Facebook
(https://www.facebook.com/events/192725607535790/ ▼)
Aug 5 - Aug 9 - George Mason University
50 x 50 - EARLY Discounted Registration for GMU 2013 is now open! Don't miss the chance to attend the return of RCFG's Computer Crime & Digital Forensics Training ...
Social Media Forensics
Social Media Digital Forensics

- New “Facebook Graph Search”
- Not Open Graph
- Not Graph API
- Turn on
  - http://www.facebook.com/about/graphsearch
- Article
Social Media Forensics

- New~ “Facebook Graph Search”
Social Media Forensics

- New: “Facebook Graph Search”
Social Media Forensics

- New ~ “Facebook Graph Search”
Introducing Graph Search

People who like Cycling and live in Seattle, Washington
Social Media Forensics

- Why???
- Criminal reasons
- Missing Persons
- Infidelity
- Malware
- Scams, Fraud, Human Trafficking…
- Child Pornography
- Illegal Media Sharing…
Why Social Media Forensics?

Photo credit: trendhunter.com
IADFI.org

Social Media Photo Database

Profile Images:
- Filenames
- Hashcodes
- URL codes
- Usernames
- Facial Recognition
Social Media Digital Forensics

Brian Lockrey
@iadfi
@InfoSecMash

765~543~8938

ComputerForensics@live.com
Alex Bond

- Finding Evil Everywhere: Combining Host-Based and Network Indicators
DFIR, or DF and IR?

Intrusion Analysis

SEC501
Advanced Security Essentials – Enterprise Defender
GCED

SEC502
Perimeter Protection In-Depth
GCFW

SEC503
Intrusion Detection In-Depth
GCIA

FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA

FOR408
Computer Forensic Investigations - Windows In-Depth
GCFE

FOR526
Windows Memory Forensics In-Depth

FOR610
Reverse Engineering Malware: Malware Analysis Tools & Techniques
GREM

Additional Information on Forensic Courses
http://computer-forensics.sans.org
Network Forensics

• Good for detecting current ongoing traffic. Harder for historical traffic. If it isn’t captured and recorded it, it’s gone.

• Good for detecting backdoor traffic. Valuable data if you can decode it.

• Attackers re-use infrastructure and tools. Tracking both in network traffic can identify new infrastructure, tools, and compromised hosts.

Host Forensics

• Good for collecting current and historical data. Can locate tools and evidence years later.

• If attacker traffic is not captured or can’t be decoded, host forensics can still yield evidence.

• Easier to identify unknown but suspicious events and identify new malware and tools – and gather new network intelligence from them.
Example 1: Host complements network

- Network alerts for two client systems communicating using an APT1 backdoor.
- Systems downloaded additional malware.
- Further communications were encrypted with an SSL certificate used by APT1.
- Systems were pulled offline for analysis.
- Prefetch analysis showed the sequence of attacker commands. The attackers were gathering information about the compromised systems.
Example 2: Network complements host

• Found a registry run key pointing to an obfuscated Javascript file.
• Analysis of the file showed it was a backdoor, capable of collecting and uploading credentials and downloading and executing additional malware.
• Created network signatures based on the analysis.
• Began seeing this backdoor’s traffic at other clients.
Frank McClain

- Chasing Malware, Not Rainbows
Chasing Malware, Not Rainbows

Frank McClain, GCFA, GCIH, CHFI
InfoSec Manager, CSIRT Lead
PrimeLending, A PlainsCapital Company
1,706 Average Daily Events
69,996 Events on 7/6/2012.
10,842 Events Between 9:01:03 and 9:03:37am.

Remote Triage

Local RAM Acquisition
A little EXIF fun from log2timeline...

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>K</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>time</td>
<td>desc</td>
<td>filename</td>
</tr>
<tr>
<td>7/6/2012</td>
<td>7:51:31</td>
<td><strong>TimeStamp PE header TimeDate Stamp (when application was linked/compiled)</strong></td>
<td>ProgramData/bcdeconf.dll</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>K</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>time</td>
<td>desc</td>
<td>filename</td>
</tr>
<tr>
<td>7/6/2012</td>
<td>8:11:53</td>
<td><strong>TimeStamp PE header TimeDate Stamp (when application was linked/compiled)</strong></td>
<td>Users/mdonaldson/AppData/Local/Temp/acrobat.dll</td>
</tr>
</tbody>
</table>
And a little MFT fun as well ...

<table>
<thead>
<tr>
<th>K</th>
<th>M</th>
<th>N</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>\Users\mndonaldson\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\3RIE1PXV\hqdefault[2].jpg</td>
<td></td>
<td></td>
<td>[SUSP ENTRY - FN rec AFTER SI rec]</td>
</tr>
<tr>
<td>/Users/mndonaldson/AppData/Local/Microsoft/Windows/Temp/</td>
<td>/Users/mndonaldson/AppData/Local/Microsoft/Windows/</td>
<td>127295</td>
<td>[SUSP ENTRY - FN rec AFTER SI rec]</td>
</tr>
<tr>
<td>/profile.ak.fbcnd.net/hprofile-ak-snc4/</td>
<td>/Users/mndonaldson/AppData/Local/Microsoft/Windows/</td>
<td>1425</td>
<td>Default browser for system</td>
</tr>
<tr>
<td>/profile.ak.fbcnd.net/hprofile-ak-snc4/</td>
<td>/Users/mndonaldson/AppData/Local/Microsoft/Windows/</td>
<td>1425</td>
<td>Default browser for system</td>
</tr>
<tr>
<td>c\E fbcnd.net/hprofile-ak-snc4/*/</td>
<td>/Users/mndonaldson/AppData/Roaming/Microsoft/Windows/</td>
<td>58</td>
<td>Default browser for system</td>
</tr>
<tr>
<td>c\E fbcnd.net/hprofile-ak-snc4/*/</td>
<td>/Users/mndonaldson/AppData/Roaming/Microsoft/Windows/</td>
<td>63</td>
<td>Default browser for system</td>
</tr>
<tr>
<td>1Donaldson/AppData/Local/Microsoft/Windows/Tem/</td>
<td>/Users/mndonaldson/AppData/Local/Microsoft/Windows/</td>
<td>127295</td>
<td>[SUSP ENTRY - FN rec AFTER SI rec]</td>
</tr>
</tbody>
</table>
This Lightning Talk was made possible by the DFIRFairy
Joseph Shaw

- Raising Hacker Kids
Raising Hacker Kids

For Good or for Awesome?

Joseph W Shaw II
CISM CISSP EnCE GAWN
Keeping Smart Kids out of trouble

“Idle hands are the devil’s playground.”

- Failing to keep intelligent kids engaged and challenged will lead to shenanigans.
- Failing to equip them with the ethical tools necessary to navigate the issues can lead to serious problems.
- Keeping things age appropriate is another challenge.
- If wisdom != ability, trouble follows.
My Point Is...

- Sometimes kids do stupid things, even “smart kids.”
- Bad judgment and hubris can have serious consequences, and these are common traits of adolescents.
- If we’re going to raise the next generation of hackers, we have to impart some wisdom and ethics upon them in addition to their 1337 sk1ll5.
Wisdom

“Knowledge is knowing a tomato is a fruit, but wisdom is not putting it in a fruit salad.” - Unknown

I’m not a fan of teaching young kids skills that they don’t have the maturity to handle, i.e. lock picking and social engineering. Giving a 7 year old a set of picks and the skills to use them is dangerous. They don’t have the necessary wisdom/experience to use them appropriately.
Issues

• There are no real ethics classes/training materials for young kids and teenagers.
• There are no hard and fast age appropriateness rules. It’s your job to know and make the call.
• What works for us won’t work for you. But learn from other people’s successes and failures.
• Keep your kids engaged in ways that are important and interesting to them, and at their level of maturity.

Good luck!
Thank you

Joseph W Shaw II
CISM, CISSP, EnCE, GAWN

Personal: josephwshaw@gmail.com
Twitter: @josephwshaw

Thanks to my wife Melissa Shaw (@melissatshaw), David Cowen (@HECFBlog), Frank McClain (@littlemac042), Hal Pomeranz (@hal_pomeranz), Jake Williams (@MalwareJake), Alissa Torres (@sibertor) and everyone else for helping me distill this talk.
Hal Pomeranz

• Fighting Your Dragons
Facing Your Dragons
"Do the thing you fear most and the death of fear is certain."

— Mark Twain

“Whether you think you can, or you think you can't--you're right.”

— Henry Ford
"You gain strength, courage and confidence by every experience in which you really stop to look fear in the face. You are able to say to yourself, 'I have lived through this horror. I can take the next thing that comes along.' You must do the thing you think you cannot do."

— Eleanor Roosevelt
“Success is not final, failure is not fatal: it is the courage to continue that counts.”

— Winston Churchill

“It is hard to fail, but it is worse never to have tried to succeed.”

— Theodore Roosevelt
“One of the greatest discoveries a person makes... is to find they can do what they were afraid they couldn't do.”

— Henry Ford
Jim Jaeger

- A Decade of Trends in Large-Scale Financial Cyber Breaches
The Threat Timeline

**Attacker Timeline**
- **Time-to-Compromise**: Milliseconds to Minutes
- **Time-to-Exfiltration**: Minutes to Days

**Defender Timeline**
- **Time-to-Prevention**: Milliseconds to Minutes
- **Time-to-Discovery**: Months to Years
- **Time-to-Containment**: Days to Weeks

**Data Exfiltration Window**
- Months to Years

**Defense Options:**
1. Prevent the Initial Compromise
2. Compress or Eliminate the Data Exfiltration Window by reducing the Time-to-Discovery and Time-to-Containment

**Speed Matters – you are in a race with the attacker!**
Timeline of Events – Breach One

**January**
Intruder gains access to the environment and begins to do reconnaissance of the network

**May – September**
**Development & Testing**
Intruder begins several months of experimenting with sniffers to capture transactions prior to being encrypted for storage

**July**
**Large Download 1**
Intruder identifies and exfiltrates transaction files containing unencrypted card data

**November**
**Large Download 2**
Intruder again downloads transaction files, but sensitive PCI data is masked or encrypted

**October – December**
**Production Downloads**
Intruder settles on sniffer and sets up production operations
Every three days, the intruder replaces folder containing transaction data and exfiltrates it

**Breach Detected**
**IR Team Sanitizes Output Files**
IR Team quickly determines download pattern and regularly sanitizes card data prior to exfiltration by the intruder
Timeline of Events – Breach Two

**January**
Intruder gains access to the environment.
The intruder begins to do reconnaissance of the network.

**March**
Backdoors first appear on the network.
The intruder is now able to access the network at will.

**December**
**Generation 2**
A production memory scraper appears on the network.
This scraper is more sophisticated than previous scrapers and outputs data files with stronger encryption.

**February**
**Development 0.1**
Memory scraper and dump utilities first appear on the network.
The intruder uses the scrapers and dump utilities to test development of gathering Track 2 data in this environment.

**June**
**Development 0.2**
A new set of memory scrapers and dump utilities appear on the network.
The intruder begins to test the next iteration of memory scrapers after further learning the environment.

**December**
**Generation 1**
A production memory scraper appears on the network.
This scraper outputs encrypted Track 2 data in mass quantities.
LESSON LEARNED: IF UNDETECTED AND ALLOWED EXTENDED ACCESS TO YOUR NETWORK, INTRUDERS WILL EVOLVE SOPHISTICATED MECHANISMS TO STEAL YOUR SENSITIVE DATA!

THANK YOU!

Jim Jaeger  
General Dynamics Fidelis Cybersecurity Solutions 
Ph: 443-926-1159  
jim.jaeger@fidelissecurity.com
Mike Sconzo

- Reconstructing Reconnaissance
Reconstructing Reconnaissance

Mike Sconzo
Reconnaissance (Web)

- Email Addresses
- Personnel Information
- Technical Documents
- Security Issues
Inferences

- Location
- Software
- Motivation
- Level of sophistication
Your browser fingerprint appears to be unique among the 3,079,937 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys at least 21.55 bits of identifying information.

Information Leakage

- Referer header
- Cookies (Google Analytic)
- User-Agent
- Request structure
- Plugins

https://panopticlick.eff.org/
It is possible to fake any/all information.
- Query string
- Language
- Keywords
- Current result set

ws.copernic.com
google.com
yippy.com
lexxe.com

metacrawler.com
yahoo.com
lycos.com
excite.com
turbo10.com
bing.com
search.aol.com
chacha.com
turbo10.com
baidu.com
kosmix.com
earthfrisk.org
webcrawler.com
rolyyo.com
sogou.com
oneriot.com
deeperweb.com
duckduckgo.com
youdao.com
yolink.com

leapfish.com
ask.com
yebol.com
dogpile.com
linkedin.com
teoma.com
yandex.ru
hotbot.com
wink.com
gigablast.com
abacho.com
info.com
facebook.com
scrubtheweb.com
hakia.com
ixquick.com
twitter.com
Specific Information

- Campaign
- Source
- Medium
- Content
- Keyword
Web Browsers

- User-Agents
- Language settings
- Request structure
- Plugins
- System information
GET /FAQs.xls HTTP/1.1
Host: www. .com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ro; rv:1.9.2.10) Gecko/20100914 Firefox/3.6.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ro-ro,ro;q=0.8,en-us;q=0.6,en-gb;q=0.4,en;q=0.2
Accept-Encoding: gzip, deflate
Accept-Charset: UTF-8,*
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.bing.com/search?q=filetype%3axls+(sales+OR+marketing)+(%22contact+list%22+OR+email)+all+american+companies&go=&qs=n&sk=&first=301&FORM=PORE

http://www.google.com.hk/search?as_q=marketing+reports&hl=zh-CN&newwindow=1&num=10&btnG=Google+%E6%90%9C

http://www.google.com/search?hl=en&newwindow=1&as_q=BUCKNER+&as_eq=spam+scam&num=10&lr=&as_filetype=xls&as_sitesearch=&as_qdr=all&as_rights=&as_occt=any&cr=&as_nlo=&as_nhi=&safe=images
it’s all about me. deal with it.
• https://developers.google.com/custom-search/docs/xml_results
• https://developers.google.com/analytics/devguides(collection/analyticsjs/field-reference
Michael Ahrendt

- Advanced Procurement
Applied Procurement Triage:

FIGHTING APT WITH APT
GRAND RAPIDS COMMUNITY COLLEGE
Goals

Time Saving
Easy Interface
Something Anyone Can Do
Many Vectors for Usage
A screenshot of a software interface titled "Triage: Incident Response". The interface includes a menu with options such as "File", "Tools", and "Help". The main content area displays various tabs including "System Information", "Network Information", "Registry", "Disk Information", "Evidence Collection", "Volume Shadow Copies (VSCs)", and "Options". Under the "System Information" tab, items like "System Information", "Capture Processes", "Capture Services", "Handles", "Scheduled Tasks Information", "Hostname Information", "AutoRun Information", and "Account Settings" are checked. A text box at the bottom indicates "Reading from Triage.ini configuration." with buttons to "Select All", "Select None", and "Run".
What Information Will You Get?

Modularized Approach

Get What You Specify As Your Needs

Many Options....
System Information

System Specifications
Processes
Services
Handles
Scheduled Tasks
Hostname
AutoRuns Data
Account Information
Network Information

IP Configuration
Active Connections
Routes
ARP Data
DNS Data
NetBIOS

Network Shares
Shared File Information
Connected Sessions
Workgroup Computers
Registry

SYSTEM Hive
SECURITY Hive
SAM Hive
SOFTWARE Hive
NTUSER.dat
USRCLASS.dat Files (Shellbags)
Disk Information

NTFS Disk Information
Mounted Disk Data
Directory Information | Tree
Volume Information
Collect Evidence

Memory
Prefetch
Recent Folder
Jump Lists
Event Logs
Master File Table
Historical Data

Can re-acquire evidence in Volume Shadow Copies

Automated approach largely following Corey Harrell’s methodology

Extras

Hashing
- MD5
- SHA1

RegRipper Reports

Compression
Results

Reports put in Folder

Collected Evidence in a separate Folder
Report Folder

- Evidence
  - Account Details.txt
  - Application Log.csv
  - ARP Info.txt
  - AutoRun Info.csv
  - AutoRun Info.txt
  - commands.log
  - Directory Info.txt
  - Disk Mounts.txt
  - DNS Info.txt
  - Event Log Copy.txt
  - Handles.txt

- File folder
- Text Document
- Microsoft Excel
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
- Text Document
Evidence Folder
Order of Volatility

Handled within Source Code

User is not allowed to alter order (without editing the source)

Based on current best standards
Order of Volatility for TriageIR

Memory

Disk Based Artifacts
- Prefetch
- Recent
- JumpLists

Network Info

Registry

System Information
Tools Used

Sysinternals from Mark Russinovich

Custom Command Prompt (CMD) from ReactOS

The Sleuth Kit from Brian Carrier

RegRipper from Harlan Carvey

(MD5|SHA1)DEEP(64)
Forensic Copy

Data Integrity Priority One!

No Alteration of Timestamps

Few Ways to Accomplish
- Robocopy
- REG
- The Sleuth Kit
Robocopy

Robocopy Great for Most Directories | Files

Needs Special Flags to Reach Goal:
- `/copyall /ZB /TS /r:4 /w:3 /FP /NP /log`:
- `/copyall`: All File Information (Timestamps)
- `/ZB`: Attempt Restart Mode, Failback to Backup Mode
- `/r`: Retry Attempts
- `/w`: Wait Time Between Retries
- `/log`: Specify Place to Store Log of Transfer
Problem: How Do I Copy a Live Registry File?

Solution:
- REG is a built-in Windows Command
- Allows a lot to be done to Registry
- Simple as REG SAVE <KeyName> <FileName>
  - EX: REG SAVE HKLM\SAM C:\Registry
The Sleuth Kit

Problem: How Do I Copy Any Other Live System File?

Solution: Carve the Data At Block Level
- Mix of Sleuth Kit
- Use iFind to locate the MFT Entry Number > $VARIABLE
- Use iGet to read $VARIABLE and carve data
Information

Great Tools from Sysinternals

Windows Provides a lot of Great Commands (WMI)

Cross-Reference the Two and Verify
Integrity

Applications are ran from clean source

Hash everything that is collected
Incident Response

Triage Collects Data

We Need to Analyze It

◦ Volatility (Memory)
◦ RegRipper (Registry)
◦ Everything:
  ◦ SANS SIFT WorkStation
  ◦ NirSoft
  ◦ WoanWare
How Do You Get It?

Google Code:

- https://code.google.com/p/triage-ir/
• Thank you for attending!

• Please fill out speaker evaluations on your way out.