Convergence Forensics

Rob Lee and Heather Mahalik

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

FOR408
Windows Forensics
GCFE

FOR518
Mac Forensics

FOR526
Memory Forensics In-Depth

FOR585
Advanced Smartphone Forensics GASF

OPERATING SYSTEM & DEVICE IN-DEPTH

INCIDENT RESPONSE & THREAT HUNTING

FOR508
Advanced Incident Response
GCFA

FOR572
Advanced Network Forensics and Analysis GNFA

FOR578
Cyber Threat Intelligence

FOR610
REM: Malware Analysis
GREM

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

MGT535
Incident Response Team Management

@sansforensics

sansforensics

dfir.to/DFIRLinkedInCommunity

dfir.to/gplus-sansforensics

dfir.to/MAIL-LIST

Inch deep and a mile wide?

- Multiple DFIR sub-disciplines are needed
- Skills converge around where the evidence is
  - Data at rest, data in use, data in transit
- Understand the full scope of your artifacts!
- Never settle for mediocrity
  - Don't know "just enough to be dangerous"…
    ...know enough to be a professional
- "Jack of all trades, master of many"
- An expert's skill degrades gracefully as you deviate from core expertise

"A human being should be able to change a diaper, plan an invasion, butcher a hog, conn a ship, design a building, write a sonnet, balance accounts, build a wall, set a bone, comfort the dying, take orders, give orders, cooperate, act alone, solve equations, analyze a new problem, pitch manure, program a computer, cook a tasty meal, fight efficiently, die gallantly."

Specialization is for insects.

- Robert Heinlein, Time Enough for Love

Let the evidence speak to you

What is involved?

What is your plan of attack?

Is e ryption a concern?

What is your plan of attack?

What is your plan of attack?

Consider your actions

Will this affect your methodology?

Reality of DFIR Practices

Science

- Tools
- Processes

Art

- Intuition
- Experience

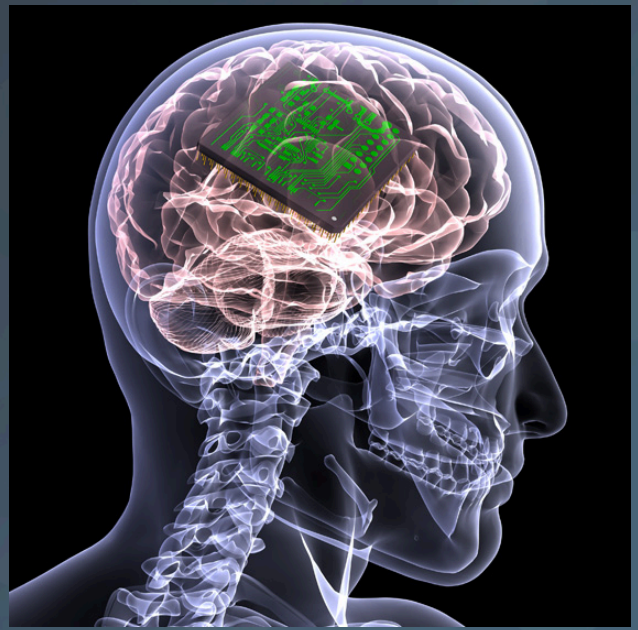
DFIR…

The disciplines

Are you forgetting something?

Memory Forensics

- Fastest access to the evidence
- Gives you hindsight
- Nothing can hide…for the most part
- Unique artifacts exist in memory
- Everything traverses memory
  - Encryption keys
  - Passwords
  - Private browsing artifacts
  - Application data



Knowing where to find this information is the hardest part!

What was that about hindsight?

Memory Forensics can provide access to:

- Previously exited processes
- Terminated network connections
- Application data (secure, deleted, etc.)

svchost.exe (6404)

- PID Relationships
- Command Line
- Chronology
- Security IDs

Process Details

Username:	
Path:	c:\windows\system32\dllhost
Parent:	PSEXESVC.EXE (2100)
Parent Process Path:	C:\Windows
Arguments:	"c:\windows\system32\dllhost\svchost.exe"
Start Time:	2012-04-06 19:22:20Z
Kernel Time Elapsed:	00:00:08
User Time Elapsed:	00:00:01
SID:	S-1-5-21-2036804247-3058324640-2116585241-1673
SID Type:	
Malware Risk Index:	97

Recovered Artifacts	Items
Web Related	
Browser Activity	612
Chrome/360 Safe Browser Carved ...	821
Firefox Carved FormHistory	20
Firefox SessionStore Artifacts	4
Flash Cookies	43
Google Maps	2
IE InPrivate/Recovery URLs	49
Internet Explorer 10 Carved Conten...	1570

The mobile brain

Smartphone Forensics

- Contains the most personal artifacts of any digital media
- Replaces the need for a computer?
  - Applications
  - Browser
  - Maps
  - Calendar
- Knowing where to find this information is the hardest part!
- Knowing how the artifact was created is key!

How much does your phone know?

Digging deeper into the apps

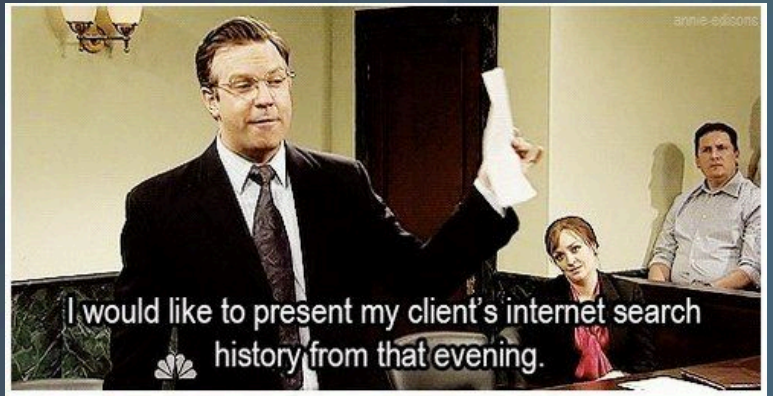
☑	docid	c0entry_id	c1text	c2modified_date
☑	1	8CC1B93F56974CD594104E20E33FBB61	First tomatoes from my garden!	1373325781
☑	2	6967D3A0F4054D399E3F937A15B97F5C	Test	1373325858

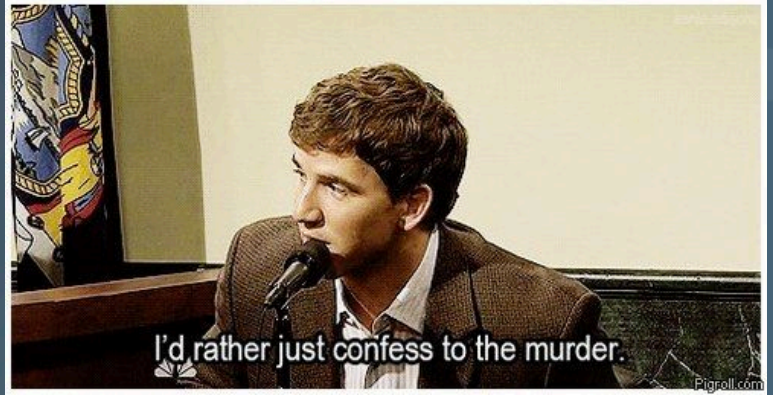

```
<?xml version="1.0" encoding="UTF-8"?>.<!DOCTYP
E plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "h
ttp://www.apple.com/DTDs/PropertyList-1.0.dtd">
.<plist version="1.0">.<dict>..<key>Creation Da
te</key>..<date>2013-07-08T23:22:35Z</date>..<k
ey>Entry Text</key>..<string>First tomatoes fro
m my garden!</string>..<key>Location</key>..<di
ct>...<key>Administrative Area</key>...<string>
Virginia</string>...<key>Country</key>...<strin
g>United States</string>...<key>Latitude</key>.
..<real>38.897663774005039</real>...<key>Locali
ty</key>...<string>Dunn Loring</string>...<key>
Longitude</key>...<real>-77.240605317128114</re
al>...<key>Place Name</key>...<string>8521 Mine
rva Ct</string>..</dict>..<key>Starred</key>..<
true/>..<key>Time Zone</key>..<string>America/N
ew_York</string>..<key>UUID</key>..<string>8CC1
B93F56974CD594104E20E33FBB61</string>..<key>Wea
ther</key>..<dict>...<key>Celsius</key>...<stri
ng>29</string>...<key>Description</key>...<stri
ng>Partly Cloudy</string>...<key>Fahrenheit</ke
y>...<string>84</string>...<key>IconName</key>.
..<string>pcloudy.png</string>..</dict>.</dict>
.</plist>.
```

Old dogs should learn new tricks

Windows Forensics

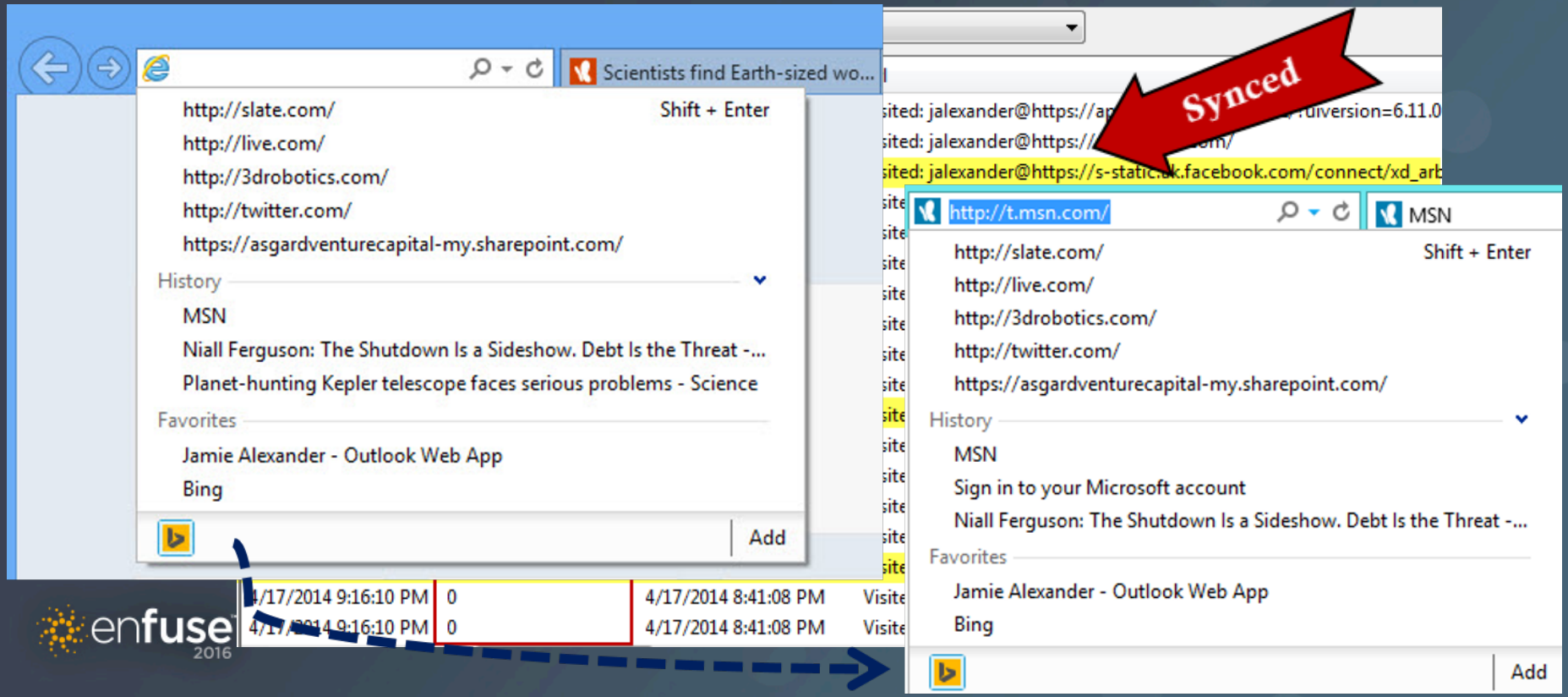
- Data synchronization
- Do you *REALLY* have time to acquire that disk drive?
- Where are the files of interest?
- Understanding the artifacts
  - Windows Registry
  - Event Logs
  - Shell bags
  - Browser history
  - Email
  - Cloud data





Data synchronization example

Windows Forensics



enfuse 2016

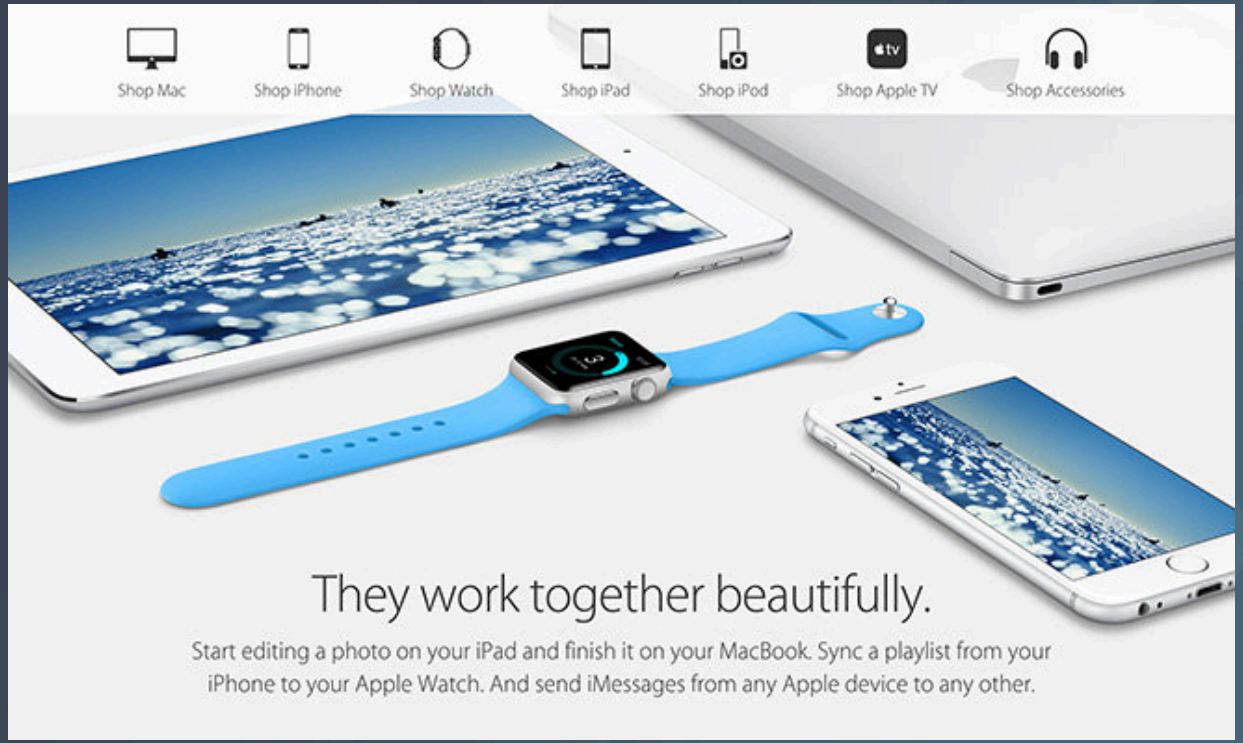
No bad Apples here

Mac Forensics

- Can you handle the investigation?
  - Malware
  - *Harder* to acquire
  - Encryption
- HFS artifacts
- Those pesky plists
- Cloud and iOS artifacts must be understood
- An apple has a brain
  - Yes, you could capture memory
- You will need method to your madness

How did that get there?

Apple Continuity

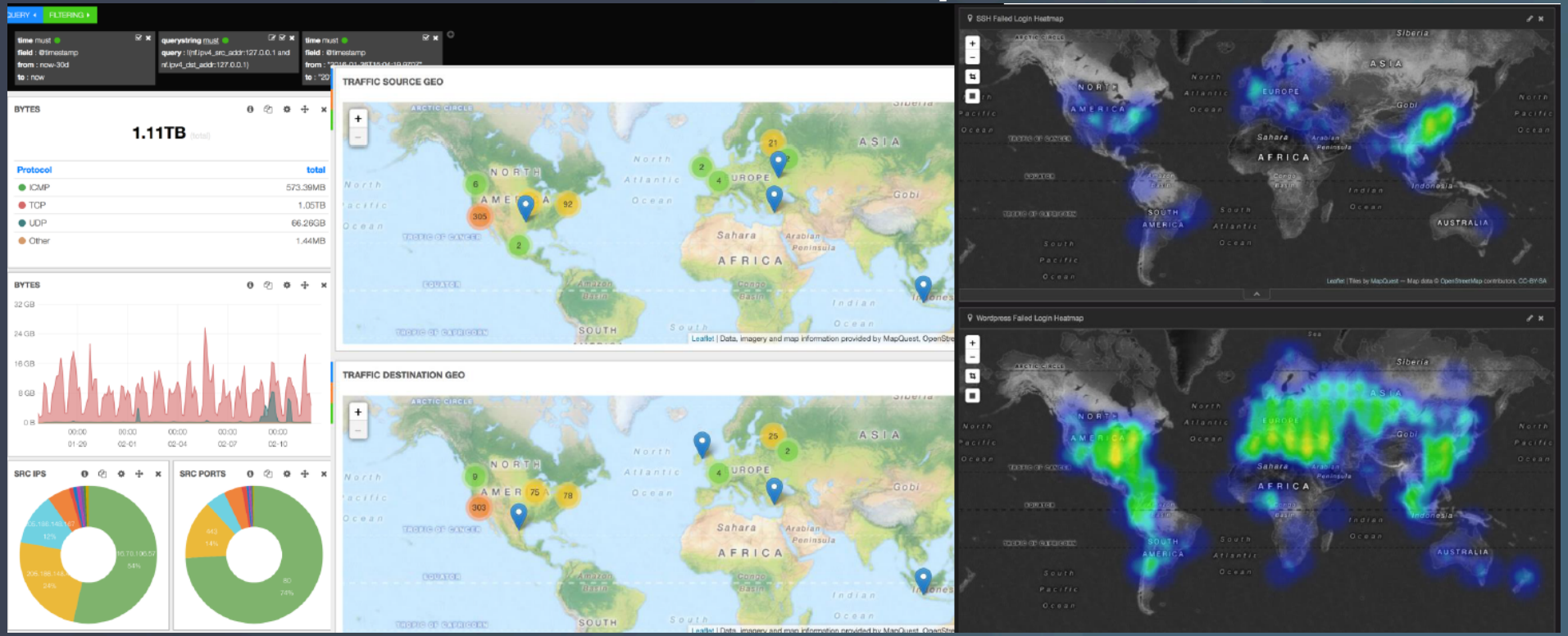


I always feel like somebody's watching me

Network Forensics

- All investigations involve not only the devices themseles but their communications
- Knowing how to examine the evidence is the first step to:
  - Scoping an incident to find the extent of a compromise
  - Identify potential endpoints of interest
  - Establish baselines of normal behavior to enable effective threat hunting
- Legality: Hard to do full-packet capture in many cases
- Volume vs fidelity: Full-packet can be REALLY hard and/or expensive to examine at scale
- Time-lining: Finding first/last/ALL instances of communications to known-bad IPs, domains, etc.
- Profiling - Finding baseline of normal activity allows quick ID of outliers that are worth chasing down

Network Forensics Example

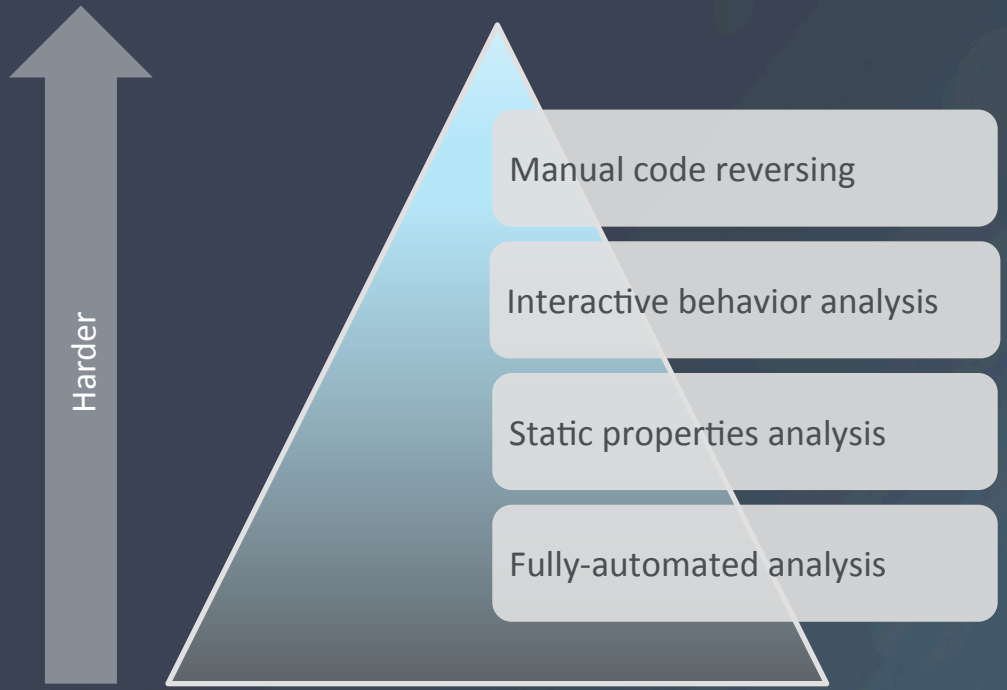


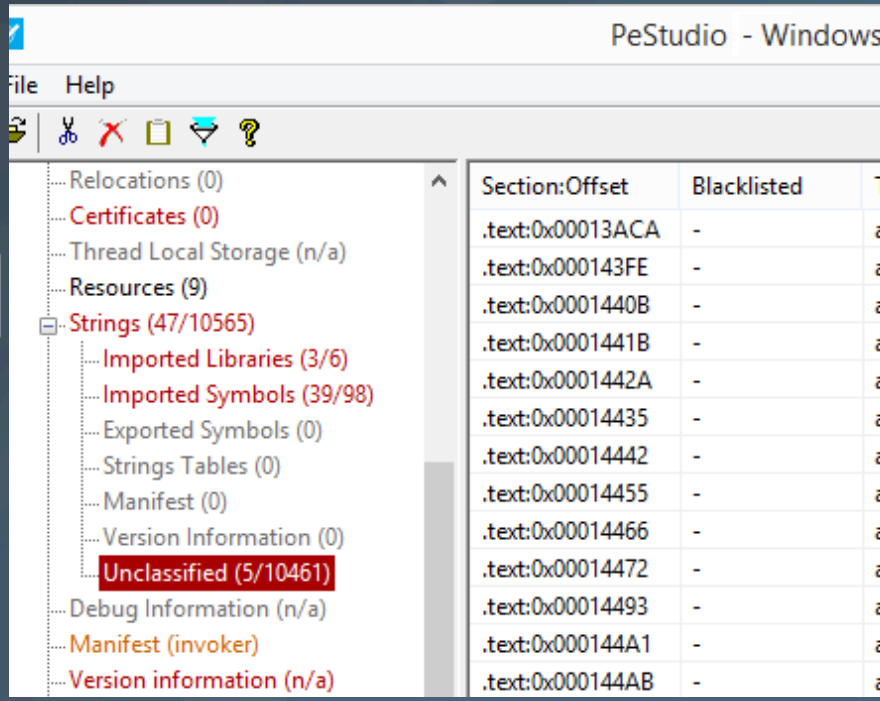
It wasn't my fault…malware did it!

Malware Forensics

- Is it a malicious executable?
- Is it acting as an app?
- What are its capabilities?
- How to detect it?
- What does it reveal about the adversary?
- Obtain a vision of the threat landscape
- Determine how to spot and track attackers' across the enterprise network
- Apply skills to mobile forensics
- Detect code-reuse to recognize attack groups and identify malware families
- Understand the trajectory of threats to anticipate adversaries' methodologies

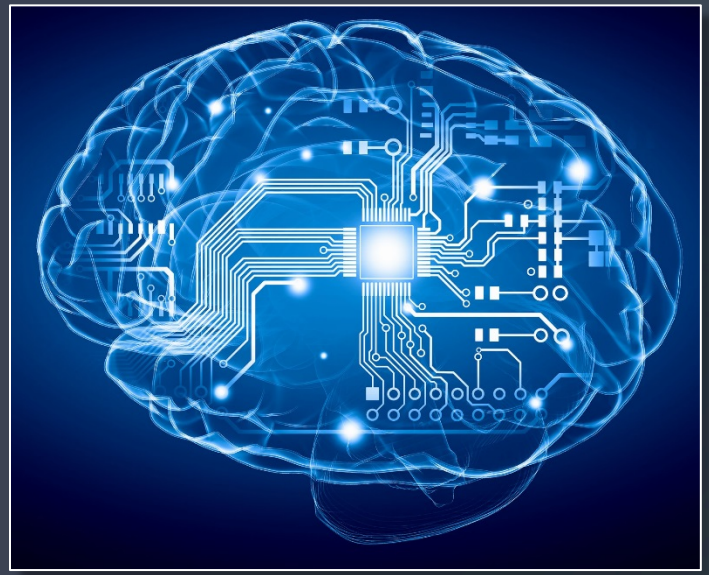
Stages of malware analysis techniques increase in complexity





Threat Intelligence

Not Just a Feed



- Effectively consuming or generating threat intelligence requires a robust IR program
- This is not a first step - more like the last!
- Look to established intel agencies as a model
- Don’t mistake a “feed subscription” for a “threat intel program”

Investigative Scenario

On the defensive

Incident Response

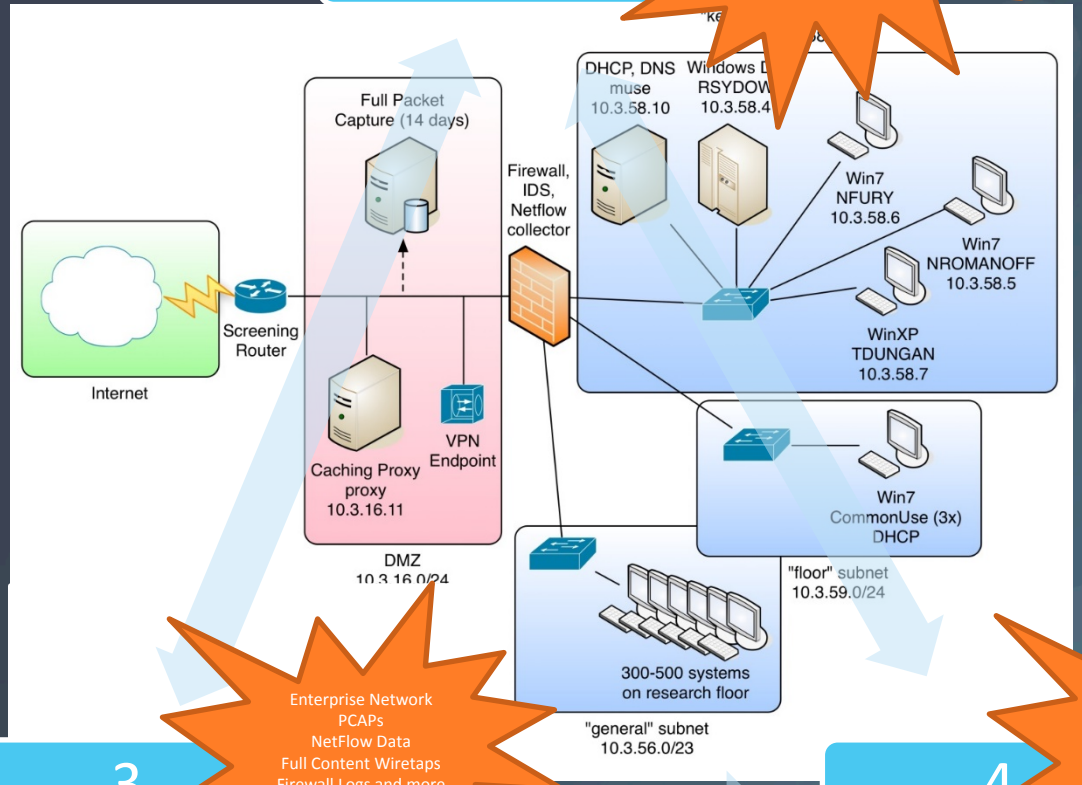
- There will be a breech
- Will you be ready?
- How the breech occurred
- How to detect compromised and affected systems
- What the attackers took or compromised
- Incident containment
- Remediation

IR Scenario

1. MEMORY

2. SYSTEM

Hard Drives
Incident Response
Data
Memory Image



3. NETWORK

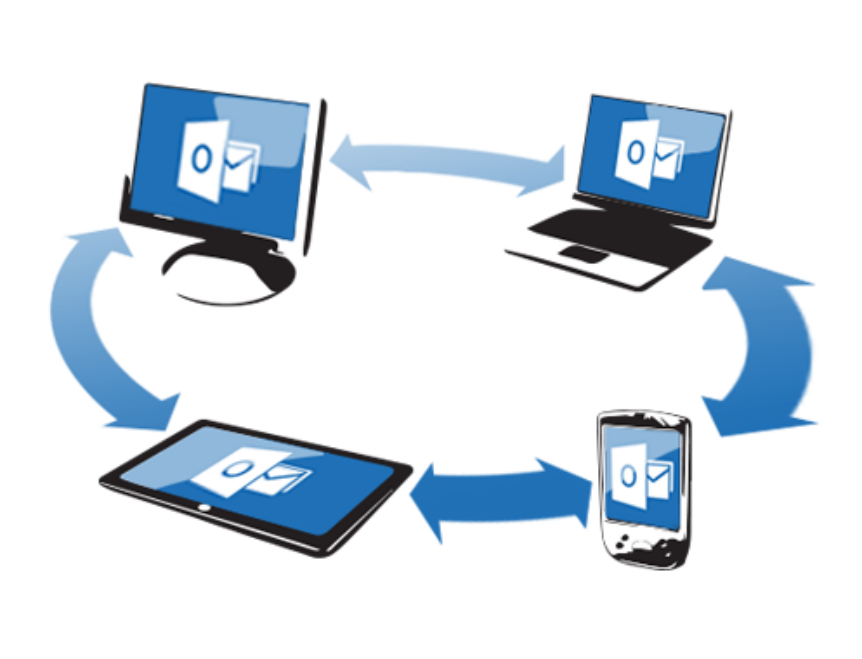
Enterprise Network
PCAPs
NetFlow Data
Full Content Wiretaps
Firewall Logs and more

4 MALWARE

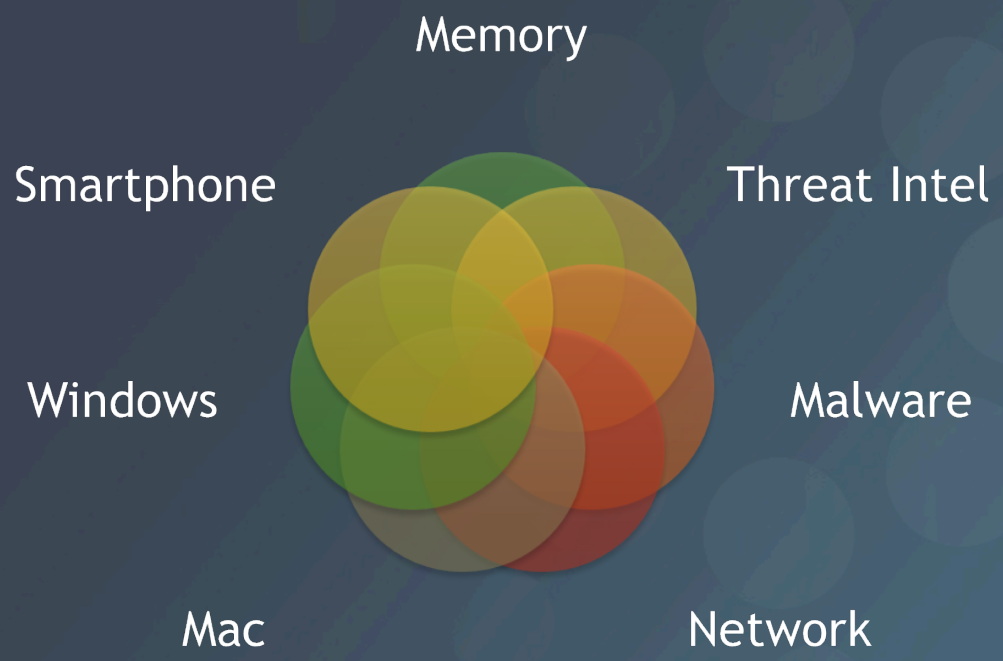
Malware Collected From Hosts
Memory Images
NetWars Challenge Inclusion

Data is everywhere

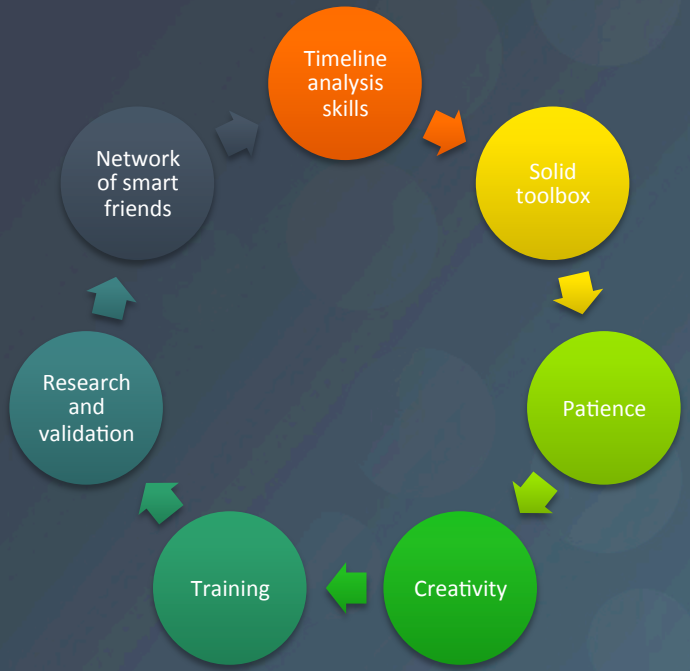
It’s real people



The Ideal DFIR Professional



What will make you better



References

http://zeltser.com/reverse-malware/automated-malware-analysis.html

http://smarterforensics.com/blog/

http://www.mac4n6.com/

http://malwarejake.blogspot.com/

https://digital-forensics.sans.org/blog

For572.com

FOR408, 508, 518, 526, 572, 585, 610

Questions?

Rob Lee

@robtlee

Email: rob_t_lee@yahoo.com

Blog: dfir.sans.org

Heather Mahalik

@heathermahalik

heather@smarterforensics.com

Blog: for585.com/blog

Thank You

Rob Lee and Heather Mahalikl SANS
Rob_t_lee@yahoo.com l @robtlee
heather@smarterforensics.com l @heathermahalik