

Digital Forensics and Incident Response

Christian August Holm Hansen
@U10 6.3.17



/> whoami

Christian August Holm Hansen:

- M.Sc. NTNU/Eurécom
- Information Security Consultant
 - Pentester, advisor, incident responder
- All opinions in this presentation are my own and all facts are based on open sources



Outline

- Incident Response
- Digital Forensics
- Finding Evidence
- Demos – what do you want to see?



Digital Forensics in Incident Management

SECURITY // ATTACKS & BREACHES

NEWS
5/5/2017
12:27 PM

Sony Brings In Forensic Experts Data Breaches [MILITARY & DEFENSE](#)

More: Associated Press, Laura Green, NSA



Data Forte, Guidance Software, and Probiti will investigate what hacked into Sony's servers and how they cracked the company defenses.

The NSA Has No Idea How Much Data Edward Snowden Took Because He Covered His Digital Tracks

Change your passwords... again: Yet another Yahoo data breach affected 32 million accounts

SECURITY

Anthem's latest breach estimate says 78.8 million were affected



Chris Smith [@chris_writes](#)
March 23rd, 2017 at 8:50 AM

Share

Tweet



Jeremy Kirk

Feb 24, 2017 at 4:26 PM



Who does this?

Digital forensics is often part of an incident responder's job

- Law enforcement
- CERTs (Government/industry specific/company specific)
 - In Norway: NorCERT, KraftCert, TelenorCert, FinansCert, UIOCert++
- Company IRTs
 - In Norway: DNB IRT, Statoil CSIRT++
- SysAdmins
- Consultants
 - In Norway: Watchcom Security Group, Mnemonic IRT++
- And others...



Incident Response



Incident Management

- Incident Response Policy
- Incident Response Team



Incident Response Policy

Responsibility

- Who makes the decisions?

Asset Priority

- Which systems can be taken offline?
- Which systems can absolutely not be taken offline?

Outside Experts and Agencies

- Who you gonna call?
- At what point is Law Enforcement involved?



Incident Response Policy

As an employee, if I discover an incident, what do I do?

The policy must include information on

- Chain of escalation
- How to prevent further damage
- How to preserve evidence until the Response Team can take over



Incident Response Team

- Many names and definitions – the same principles apply to all of them (MO)
 - IRT, SIRT, CERT, CSIRT... (Response Team being the key)
- Permanent
- Virtual
- Hybrid



Red Team – Blue Team

- Derived from military wargames
- A simulated attack using security specialists
- The Incident Response Team defends the system from the attack



Incident Response Procedures

- Detect
- Respond
- Recover



Source: Ross McAfee, Microsoft (@HollisticInfoSec)



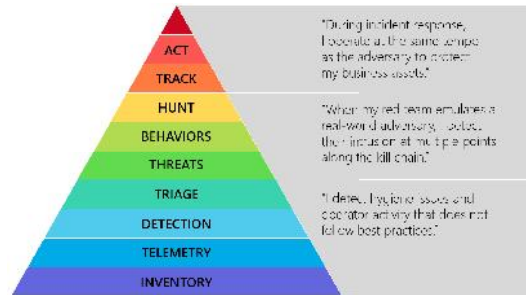
Detect

Know your assets

- If you don't know your assets, you cannot defend them

Triage

- Weed out false positives
- Categorize events
 - Type of incident
 - Source
 - Growth
 - Damage potential



Source: Ross McAfee, Microsoft (@HollisticInfoSec)



Respond

- Collect data
- Mitigate damage
- Isolate systems



Source: Ross McAfee, Microsoft (@HollisticInfoSec)



Respond (2)

- Analyze and track adversary
 - What is the root cause of the incident?
 - Who, how, when, why
- Law enforcement
 - Is it necessary?



Source: Ross McAfee, Microsoft (@HollisticInfoSec)



Recover

- Fix the problem
- Improve Incident Response Policy
- Disclosure



Source: Ross McAfee, Microsoft (@HollisticInfoSec)



Digital Forensics



Digital Forensics in Court

The BTK Killer

- Metadata in Word file led to arrest after 30 years

Krenar Lusha

- Search of laptop led to discovery of bomb-making equipment

Matt Baker

- Suicide of wife ruled murder after incriminating google searches is discovered 4 years later

Sharon Lopatka

- Emails on her computer led to her killer

Corcoran Group

- Evidence that data had been deleted led to conviction



Digital Forensics

It's all the same...

- Digital forensics, computer forensics, network forensics, electronic data discovery, cyberforensics, forensic computing...

Big difference in the handing of evidence

- Law enforcement
- Corporate incidents
- ... but it shouldn't be



What is digital evidence?

"Any digital data that contains reliable information that supports or refutes a hypothesis about an incident"



Forensic Investigation Process

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation



At the Crime Scene

Document the crime scene

- Document who has access
- Document any contamination

Photograph everything

- Especially the screen

Locate the media

- Follow cables
- All digital devices may contain digital evidence

If the computer is running, dump the RAM



The Digital Forensics Toolkit

- Screwdrivers
- Evidence bags
- Labels
- Forensic software
- Write Blocker
- Camera
- Notebook with numbered pages
- Storage – Large HDDs



Basic Scientific Principles

1. Best evidence
2. Minimal Intrusion
3. Minimal Force
4. Minimal Interruption
5. Transparency
6. Chain of Custody
7. Primacy of the Mission
8. Impartiality
9. Documentation



Evidence Location

- Network analysis
- Media analysis
- Software analysis
- Hardware analysis



Dealing with Evidence

R-DCITE

- Return

Or sieze...

- Original
- Clone
- Image
- Targeted copy
- Extensive copy



Admissible Evidence

- How was it gathered?
- How was it treated?
- Who handled it?
- How reliable is it?
- Is the Chain of Custody complete?



Evidence Categories

Conclusive Evidence

- This is fact

Best Evidence

- This is it

Secondary Evidence

- This how it looks

Direct Evidence

- This is what I saw



Evidence Categories

Corroborative Evidence

- That happened, because of this

Circumstantial Evidence

- That could have happened, because of this

Opinion Evidence

- I'm an expert, this is what happened

Hearsay Evidence

- I heard this about that

Digital evidence is considered hearsay unless an expert vouches for it



Finding Evidence



Finding Evidence

- Many ways to hide
- Many ways to find



Hidden Files

- Setting the "hidden" flag on the file
 - Different for Windows and *nix
- Inconspicuous folder names



Locating Hidden Files

- The “hidden” flag is ignored by default
- Forensic software can be set to show the drive as a “flat” drive
 - Ignoring folder hierarchy



Changing File Extensions

- When opening the file, the system returns an error message
- “Oh, I guess it is corrupted. Too bad.”



Discovering Changed File Extensions

- Some forensic software will point out files with mismatched extensions
- File signatures tells us what kind of file it is
 - Also called “Magic Numbers”



File Signatures

A hexadecimal code in the file, also called file “headers” and “footers”

Examples:

25 50 44 46	= %PDF	= PDF
49 44 33	= ID3	= MP3
FF D8 FF	= ÿØÿà	= JPEG
42 4D = BM	= BMP	
4D 5A = MZ	= EXE, COM, DLL	



Obscure File Names

- Hiding files by giving them inconspicuous file names
- "Blueprints_iPhone8.jpeg" becomes "Florida vacation 001.jpeg"



File Names not an Issue

- Hash functions to look for known files
 - Lists of hash sums recognize known illicit files
 - Lists of hash sums recognize known "good" files
 - We can create our own lists



Steganography

- Hiding a file inside another file
- Hiding "Nuclear Launch Codes.txt" inside "Adorable Cat.jpeg"



Steganography Example

- Command & Control traffic in images
 - Known sites - imgur, Dropbox, Instagram etc.
- ZeusVM botnet malware used image files to hide configuration files



Discovering Steganography

- Hard to determine unless you are looking for it
- Steganography software on suspect's computer a strong indicator
- File type signatures to the rescue
 - Linux tools: binwalk, file



Encrypted Files

- This is where the problems start for the investigator
- Strong encryption algorithms almost impossible to break
- "Sorry, I've forgotten my 50 character long password."

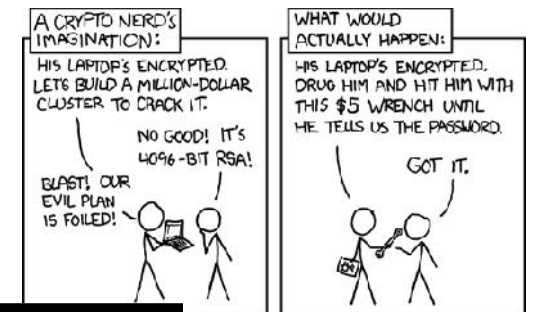


"Breaking" Encryption

- Recovering key from RAM
- Brute force
- Exploiting weaknesses in the software or the algorithm used (Cryptanalysis)
- Some countries have laws that compel the suspect to give up keys
- Less ethical methods
 - Rubber-hose cryptanalysis
 - Black-bag cryptanalysis



"Breaking" Encryption



The Intercept
BRITISH HACKER WINS COURT BATTLE OVER ENCRYPTION KEYS
From Our Top Stories
MAY 10 2018 11:37 AM



Deleting Files

- Deleting the files from the computer before law enforcement claims it
- “You can’t prove anything, there is nothing there.”



How does the System Delete Files?

- Deleting a file does not actually remove it
- In Windows, the file is renamed
 - CorporateSecrets.txt
 - ~orporateSecrets.txt
- This tells the system that the space is available to be overwritten in the future



Reclaiming Deleted Files

- Data carving
 - Ignore file system – extract file directly from the media
- Renaming the file



Reclaiming Overwritten Files

- Pieces of data can be recovered from “slack space”
- File slack, RAM slack, drive slack
- Forensics software can often recover files or parts of files from slack space

AAAA	BBBB	CCCC	DDDD	IIII	2222	3333	4444
~AAA	BBBB	CCCC	DDDD	IIII	2222	3333	4444
XXXX	YYYY	ZZZZ	DDDD	IIII	2222	3333	4444



Metadata

- What if we only have a file, and not the source media?



Using Metadata

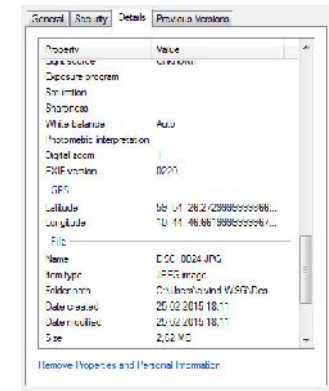
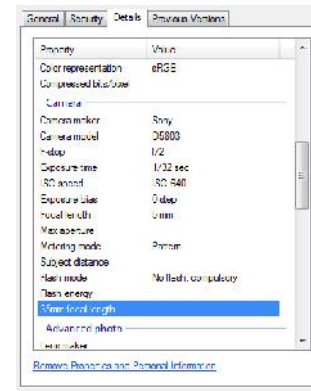
- Data about the file
 - When was the file last used?
 - When was the file created?
 - Who opened it?
 - Where was it created?
- Can prove who had access to the file



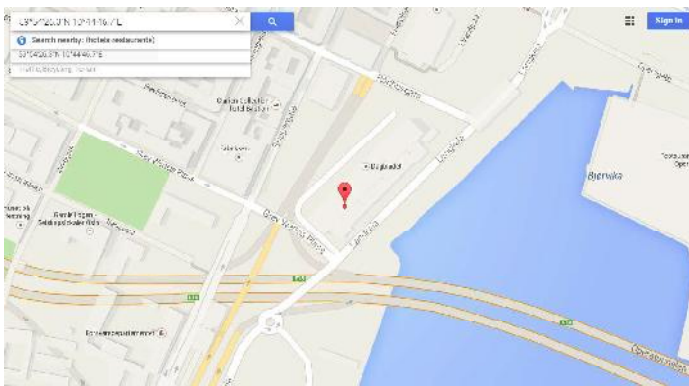
Metadata Example



Metadata Example



Metadata Example



Metadata Example 2

- Red Star OS – Appends unique system identifier to all media files



It's not all theory – if you want to learn more...

CTFs

Forums (/r/forensics, /r/netsec)

Virtual machines, tools & wargames

- Sans DBIR
- Redline
- Volatility
- Sandboxed malware (be careful...)
- Books

Courses (e.g. SANS SEC504)

- Course contents are public. Use Google to learn the goals!
- Conferences (DEFCON, Black Hat, CCC, Paranoia)
 - Videos are often published online, freely available
 - Paranoia is held in Oslo Spektrum on the 10th and 11th of May
- Books



Questions?

christian.hansen@watchcom.no



Demo time!

What do you want to see?

- Red Star OS
- Redline Live Forensics
- Steganography/data carving with *nix tools
- Gaudox Botnet
- I want to go home

