Intro to Forensics

ALBERT MORRIS

~whoami

- ❑ Cal Poly Pomona - Information Security and Forensics
- ❑ Director of Digital Forensics- FAST
- ❑ From Spain, Tenerife

https://www.linkedin.com/in/albert1337

Twitter: @cubaa15

FAST- Forensics and Security Technology

- Security focused CPP Club
- Hands on workshops by students for students
- Semesterly CTF’s
- Connected to Industry professionals
- Student chapter of the High Technology Crime Investigation Association (HTCIA)
- Opportunity for like minded students to learn and grow

- https://www.cppfast.org/
- https://htcia.org/about/

Forensics Basics

- **Forensics** = application of science to solve a legal problem.
- **electronic discovery** (eDiscovery) = any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.
- Involves the analysis of images, video, and audio encompassing computers, mobile devices, networks, and the cloud.
- The analysis focus on authenticity, comparison, and enhancement.
- Mainly used in criminal investigations, Civil Litigation, and Intelligence

- *“The best scientific evidence in the world is worthless if it’s inadmissible in a court of law.”*

Dennis Rader AKA BTK(Bind, Torture, Kill)

- Murdered people in Kansas from 1974 to 1991
- Managed to avoid capture for 30 years
- He sent a letter confessing a crime and asked to contact police via a floppy disk
- Floppy disk was analyzed for metadata with the following findings:
  - Date Created: Thursday, February 10, 2005 6:05:34 PM
  - Dated Modified: Monday, February 14, 2005 2:47:44 PM
  - Title: Christ Lutheran Church
  - Last Saved By: Dennis
- This metadata lead to the quick arrest of the President of the church, Dennis Rader

The Digital Forensics Process

1. Search Authority: warrant, subpoena, or even consent.
2. Chain of Custody: essential to maintain integrity
3. Imaging/Hashing Function: Forensic image duplicating original(Read only)
4. Validated Tools: Document tool testing + validations
5. Repeatability(Quality Analysis): Collection of practices + procedures throughout the whole forensic process helping guarantee accuracy of findings
6. Analysis: Timeline, breaking encryption, connect the dots….
7. Reporting: Know your audience! Executive summary, list items examined, methods + tools used, conclusion, relevant exhibits
8. Possible Expert Presentation: Present to judge or jury

File Systems + Volatility

- File System’s job is to keep files allocated in an orderly way
- FAT 12,FAT 16,FAT 32, FATX: File Allocation Table (USB)
- NTFS: New Technology File System (Windows)
- HSF, HSF+: Hierarchical File System (Mac)
- Allocated Data: Used Spaced
- Unallocated Data: Unused Space
- Slack Space: when original file is partially overwritten, and the remains of unallocated space can be recuperated
- Artifacts: items that get left behind based upon the activities of the end user of the device – footprints if you will.
- Volatile Data: Live data that depends on power to stay alive (RAM)

Order of Volatility

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media

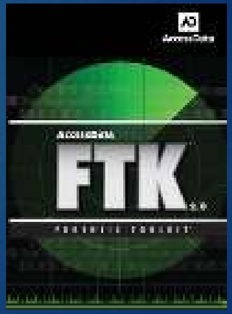
Write Blocking + Evidence in Ram

- Prevents any data from being written to the original evidence drive.
- When cloning the original source of data it’s necessary to have a software of hardware write blocker to keep data’s integrity.
- RAM can contain running processes, executed console commands, passwords in clear text, unencrypted data, instant messages, Internet protocol addresses, and Trojan horse(s)

Digital Forensic Tools

- Open Source:
  - SANS Investigative Forensic Toolkit (SIFT)
  - The Sleuth Kit (Autopsy)
  - Volatility – Memory Analysis
- Commercial
  - Forensics Tool Kit (FTK)
  - EnCase

- Information that can be found:
- E-mail addresses
- Names
- Phone numbers
- Keywords
- Web addresses
- File types



Source https://en.wikipedia.org/w/index.php?curid=27739389
Source https://en.wikipedia.org/w/index.php?curid=37287879

Forensic Image Formats

- EnCase (extension .E01)
- Access Data Custom Content Image (.AD1)
- Raw dd (.001) Open Source
- System image (.iso)

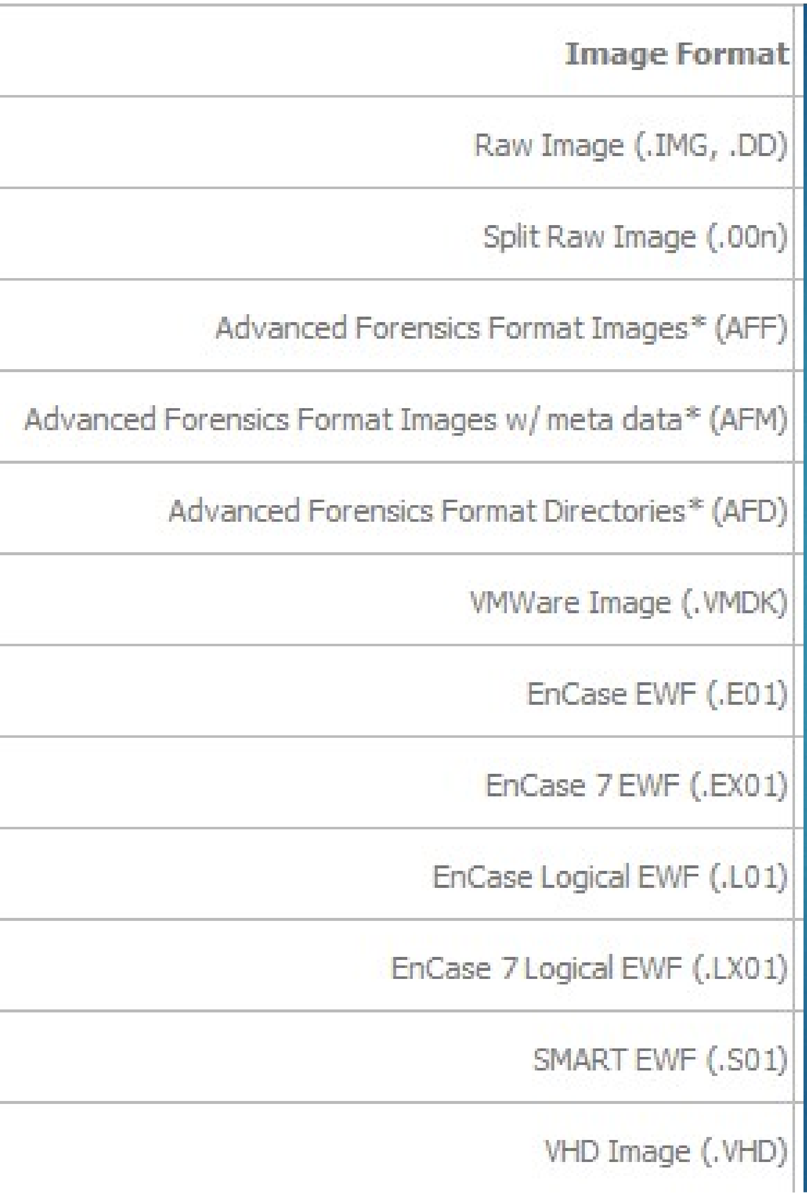


Image Format
Raw Image (.IMG, .DD)
Split Raw Image (.00n)
Advanced Forensics Format Images* (AFF)
Advanced Forensics Format Images w/ meta data* (AFM)
Advanced Forensics Format Directories* (AFD)
VMWare Image (.VMDK)
EnCase EWF (.E01)
EnCase 7 EWF (.EX01)
EnCase Logical EWF (.L01)
EnCase 7 Logical EWF (.LX01)
SMART EWF (.S01)
VHD Image (.VHD)

Incident Response (Network Forensics)

- The National Institute of Standards and Technology (NIST) outlined the incident response cycle. The phases are:

- Preparation: to respond quickly
- Prevention: patching, network + host hardening
- Detection and analysis: false positives are normal, get a picture of what the normal network traffic looks like
- Containment, eradication and recovery: minimize impact
- Post-incident activity: What did we do right/wrong? Are our policies effective? Is there a lack of resources to respond? What can we do differently?

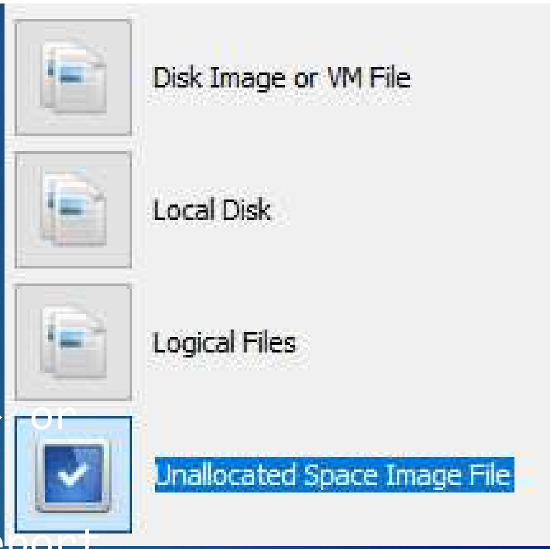
Network continued…

- Evidence: Logs and pcap files (if possible)
- Logs of interest: authentication, application, operating system, and the firewall log.
- Tools used:
  - NetIntercept
  - Netwitness Investigator
  - Snort
  - Wireshark

Workshop!!PDF Parsing

- Start by placing the pdf on the desktop of the Kali VM
- Right click desktop, open in terminal
- Type:
  - pdfid python_textbook.pdf
  - peepdf python_textbook.pdf
  - pdf-parser python_textbook.pdf | grep .exe
  - pdfdetach -saveall python_textbook.pdf
  - Move byte-of-python.pdf to your windows OS(your host) and rename it to .exe from .pdf

Workshop!! Autopsy



- ❑ Open Autopsy
- ❑ Click on New Case
- ❑ Give it a name, it can be something like <Company>.<Instance> or anything you want
- ❑ Fill in your information if you want, it will help for the report later on
- ❑ Click on Add Data Source if the prompt does not appear automatically and select “Unallocated Space Image File”
- ❑ Browse and selecte the .dd file, click next and Autopsy will take care of the rest

Workshop!! Wireshark Exercise

- Open the 2017-01-28-traffic-analysis-exercise in Wireshark
- Set up Wireshark columns with the pdf provided
- Answer the following questions:
- What was the date and time of the infection?
- What is the MAC address of the infected Windows computer?
- What is the IP address of the infected Windows computer?
- What is the host name of the infected Windows computer?
- What type of malware was the computer infected with?

Workshop!! Wireshark continued

- Filters to use:
  - http.request   See all the request made to a webserver
  - nbns   See all the netBIOS traffic
  - dhcp

Workshop!! Wireshark continued Answers

- What was the date and time of the infection?
- A: The computer was infected on 2017-01-27 around 22:54 UTC.
- Q: What is the MAC address of the infected Windows computer?
- A: 5c:26:0a:02:a8:e4 (Dell_02:a8:e4)
- Q: What is the IP address of the infected Windows computer?
- A: 172.16.4.193
- Q: What is the host name of the infected Windows computer?
- A: Stewie-PC
- Q: What type of malware was the computer infected with?
- A: Ransomware

Resources

- https://www.hackingarticles.in/step-by-step-tutorial-of-ftk-imager-beginners-guide/
- Forensics Textbook: The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics, Second Edition By John Sammons

Training Resources

- Forensics:
- https://www.cfreds.nist.gov/
- http://dftt.sourceforge.net/
- Wireshark Exercise:
- http://www.malware-traffic-analysis.net/2017/01/28/index.html