Digital Forensics

Forensic Science

- Applying science to criminal and civil legal cases
- Many subfields
  - Forensic Anthropology
  - Art Forensics
  - Forensic Botany
  - Digital Forensics

Digital Forensics

- The recovery, analysis and investigation of data found in digital devices
- Any device/component which processes data
  - Hard disk, tablets, mobile phones
  - USB sticks, SD cards
  - Memory (RAM), network hardware

Digital Forensic Streams

- Criminal & Civil Law
  - Fits with the classic definition of forensics
  - Collection & analysis of digital evidence
- Incident Response
  - A cybersecurity specialist with forensic skills
  - Less strict requirements for evidence handling

Criminal vs Civil

- Digital Forensics for Crime
  - Working with Law Enforcement
  - Contribute evidence analysis towards a criminal case
  - Expert witness
- Digital Forensics for Civil Cases
  - Working in litigation
  - Contributing evidence against corporate disputes, corporate negligence, insider trading
  - Expert witness

Traditional DF

- Historically: pull-the-plug
  - Take the crime scene back to the lab
  - Forces dead-box forensics
  - A bit old fashioned and no longer recommended
  - Today, both dead-box & (where possible) live forensics
- Very strict evidence handling procedures

DF&IR

- **D**igital **F**orensics & **I**ncident **R**esponse
  - A member of the blue team
  - Live forensics during incident response
    - Memory analysis for malware identification
    - Network analysis for attacker ingress
  - Dead-box forensics during recovery
    - Recovering lost data

- Less strict evidence handling
  - Still recommended if taking attackers to court

Evidence Handling

- The Chain of Custody (CoC)
- A paper trail of
  - Collection
  - Control
  - Transfers
  - Analyses
- Name, date & time for each handling/movement

- B-CoC
  - A blockchain based solution from Cornell University

Security 360

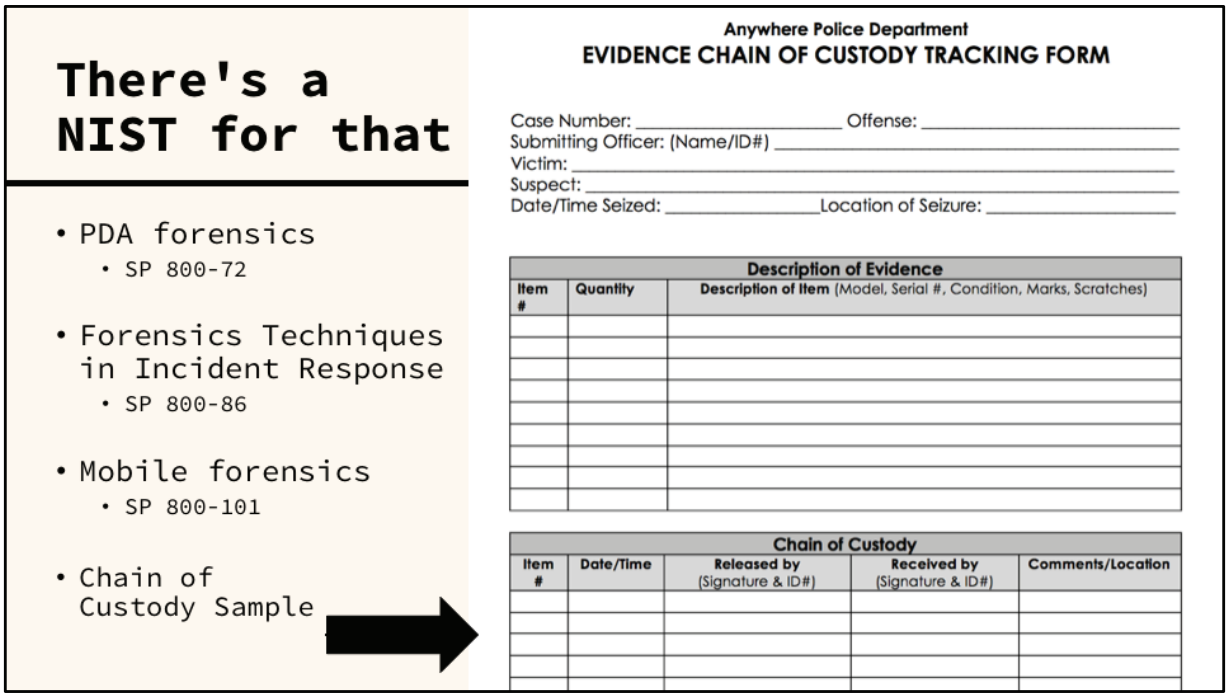
https://arxiv.org/abs/1807.10359

Handling Evidence

- Always work on a copy, never with the original...
  - Usually an image
- Hash everything
  - Why?
  - **INTEGRITY!**
- Timestamp everything
- Record everything

There's a NIST for that

- PDA forensics
  - SP 800-72
- Forensics Techniques in Incident Response
  - SP 800-86
- Mobile forensics
  - SP 800-101
- Chain of Custody Sample



Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

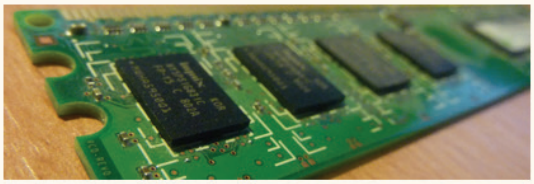
Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

https://www.nist.gov/document/sample-chain-custody-formdocx

What are we looking for?

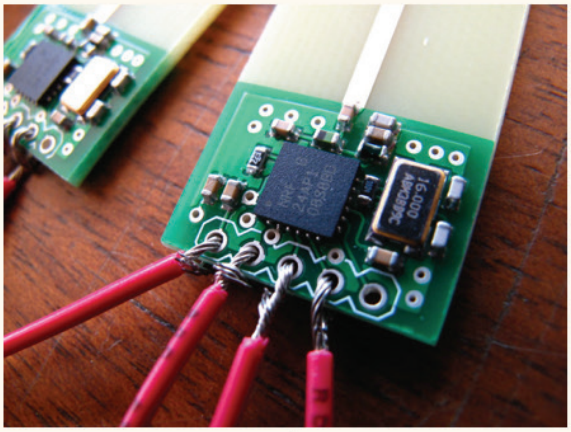
- Storage mediums (HD, USB, SD)
  - Regular data (mounting old drives)
  - Hidden data (obfuscation, steganography)
  - Deleted files
- Memory
  - Malware signatures
  - Browsing history
  - Network connections

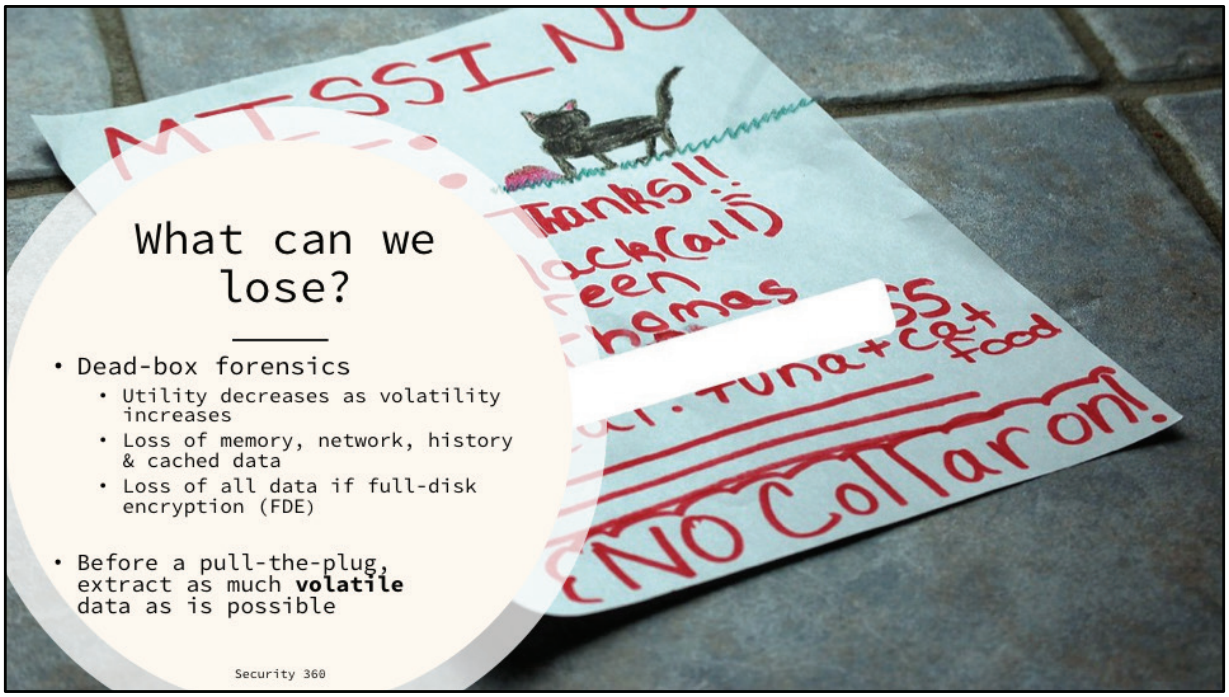


What else are we looking for?

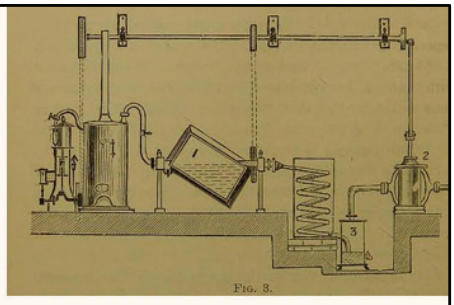
- Network
  - Packet analysis
  - Netflow analysis
  - Log analysis

look a bit like a blue team analyst?



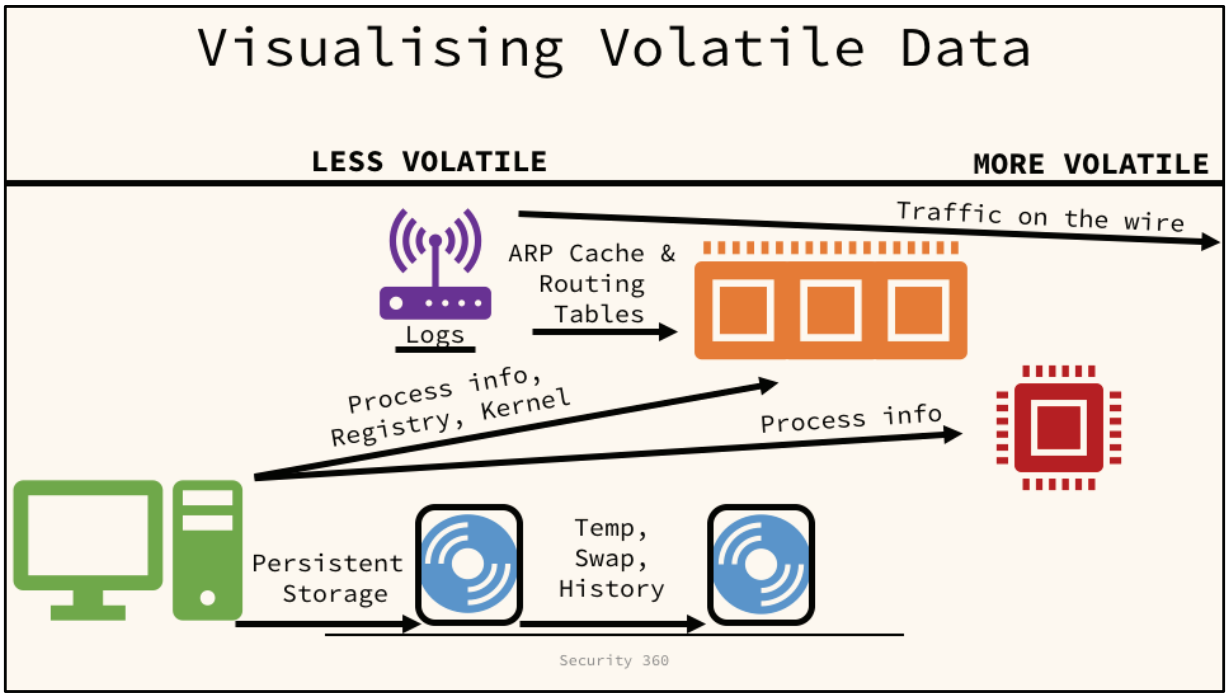


Volatile Data



- Order of Volatility (OOV)
  - CPU registers & cache
  - Network traffic
  - Network routing tables, ARP cache
  - RAM, running processes, registry, kernel data
  - Temporary files & swap space
  - Command history
  - Clipboard data, users logged in
  - Decrypted FDE

David Watson, Andrew Jones, in Digital Forensics Processing and Procedures, 2013


Visualising Volatile Data
LESS VOLATILE
MORE VOLATILE
Traffic on the wire
ARP Cache & Routing Tables
Logs
Process info, Registry, Kernel
Process info
Persistent Storage
Temp, Swap, History
Security 360

Dumps

- Gathering data during live forensics
  - Extracting data that does not persist on shutdown
  - Used in later analyses
- Dumping specific processes
- Full memory dumps
- Capturing temporary data & swap
- Drive Imaging with decrypted FDE

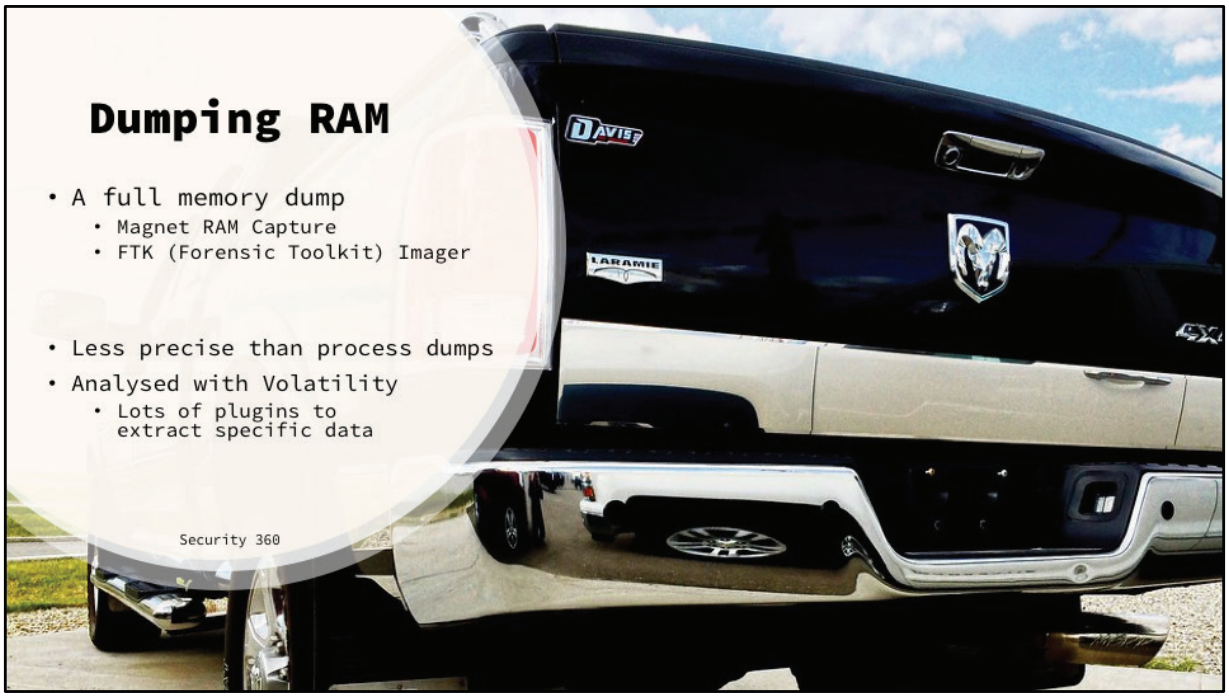
Dumping process state

- A process memory dump
  - Linux Core files
    - gcore
  - Windows user dumps
    - Userdump.exe

- Associated memory dump of a specific process
  - Also contains CPU register values
  - CPU cache is lost

Learning from the process

- Analyse with gdb, objdump / WinDbg, CBD
- The core / userdata file gives info on system calls, what the process did
  - Malware analysis
- Elsewhere in memory
  - Current browser page
  - Browsing history



Learning from memory (Memory Forensics)

- Network info
  - ARP cache
  - Routing tables
  - Connected users
- System info
  - Open windows
  - Local time
  - Logged in user
- General process info
  - Malware threats
- Kernel info
  - Rootkit threats

Security 360

Ligh, M.H., Case, A., Levy, J. and Walters, A., 2014. *The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory*. John Wiley & Sons

Capturing tmp & swap & history

- Temporary files kept on disk
  - Sometimes in own partition (/tmpfs)
- Swap
  - "virtual memory" on-disk
  - A partition in Linux
  - A file (Pagefile) in Windows
- What can we learn depends...
  - If swap is active, if history is active
  - What has been allocated to swap space
  - What tmp files / history is saved

"Dumping the Drive" (FDE)

- Full disk is usually decrypted on first log-in
- Not encrypted again until log-out / shut-down

- Get a live system, check for FDE
- If enabled, image the drive first
  - So, not quite a dump
  - Just regular imaging
  - FDE makes it volatile

Security 360

Casey, E. and Stellatos, G.J., 2008. The impact of full disk encryption on digital forensics. *ACM SIGOPS Operating Systems Review*, *42*(3), pp.93-98.

Drive Imaging

- Byte-for-byte copy of a drive
  - In Linux, dd (**C**opy & **C**onvert), FTK Imager
  - On Windows, dd forks, full FTK (trial-paid)
- A must-do to start/continue any Chain of Custody
  - Hash the image for integrity!
- dd is dangerous
  - Out-of-order commands can wipe a drive:

```
dd if=/dev/null of=/dev/sda2 bs=512
dd if=/dev/sda2 of=/dev/null bs=512
```

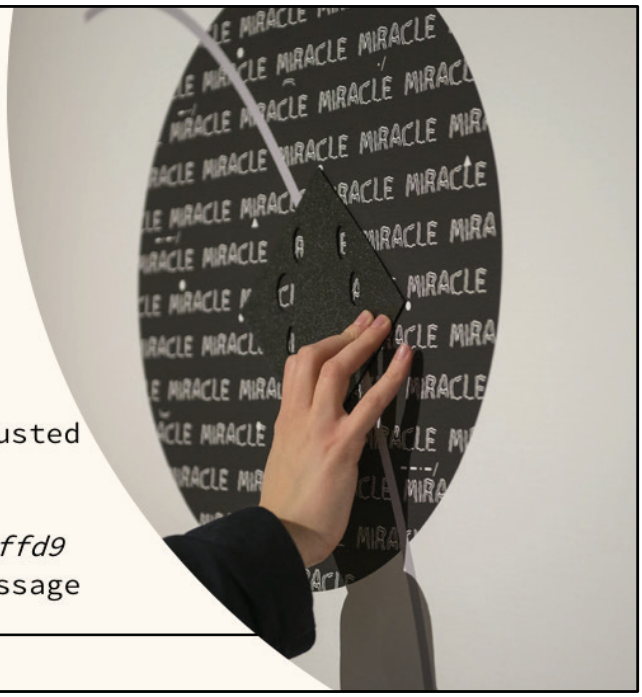
Learning from disk

- Logical analysis
  - Boot the image to OS, analyse through normal use
- Physical analysis
  - Mount the image, low-level disk analysis
- Retrieval
  - Retrieve files
  - Retrieve hidden files
  - Retrieve obfuscated files
  - Retrieve steganographic files
  - Retrieve deleted files

Steganography

- Messages hidden in messages
- Commonly done by hiding secrets in digital images
  - Brightness, hue, colour adjusted
  - New values yield a message

  OR
  - Overflow JPEG end-of-image *ffd9*
  - The overflow is a hidden message



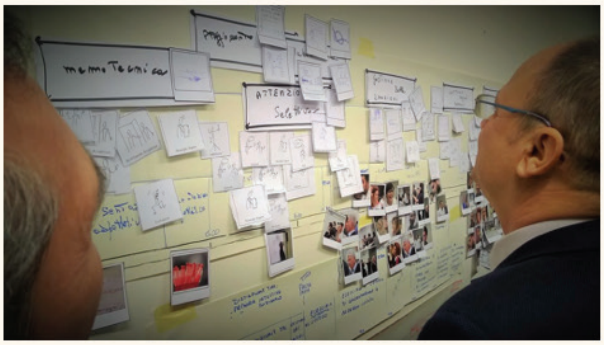
Security 360

Recovering Deleted Files

- Deleting files only removes the "pointer"
  - The record of where the file was stored
- Files are only truly deleted when they are overwritten by other files
  - **OR** by dd if=/dev/null *or* dd if =/dev/random
- Tools can find files with missing pointers
  - These are our deleted files!

Building a Timeline

- Once we have collected and analysed data
- Build a timeline
  - When was it downloaded
  - When was it run
  - When were they connected
  - What happened & when



Forensic Suites

- Help build cases, recover files, store evidence
- Trusted by law enforcement & courts

- Encase, Forensic Toolkit (FTK), X-Ways

€1000-3000

- The Sleuth Kit (TSK) & Autopsy (GUI)

€FREE

In the courtroom

- Digital Forensic Expert Witness
- Q&A on the evidence you collected
  - Methodology
  - Reasoning
  - Chain of Custody
  - Analysis
- Q&A on you
  - Education / Certifications
  - Experience
  - Confidence

Security 360