DIGITAL FORENSICS 101

KARTIKEYA SRIVASTAVA

SANCHAY SINGH

THE INTRODUCTIONS

KARTIKEYA SRIVASTAVA

Currently I am pursuing my Bachelor of technology in computer Science major, I am working in the field of cyber security and cyber forensics from past 4 years.

I have developed an antivirus named mrityunjay, I have worked with cyber crime cell ghaziabad and done various Internships at Cisco, Palo Alto Networks, CDAC etc.

CYBERSECURITY ENTHUSIAST

SANCHAY SINGH

Founding member of HackersVilla CyberSecurity. With over 6-7 years of professional experience in the field, I have worked with many top researchers. Mentored numerous students across the globe. Also working as Subject Matter Expert with UpgradCampus since last 15 months. Have given numerous talks at Null Delhi Chapter and worked with many other security conventions of India.

CYBERSECURITY EXPERT AND TRAINER

sanchayofficial

@sanchayofficial

sanchayofficial@gmail.com

WHAT IS DIGITAL FORENSICS?

EMERGING DISCIPLINE IN COMPUTER SECURITY

INVESTIGATION THAT TAKES PLACE AFTER AN INCIDENT HAS HAPPENED

HELPS IN FINDING THE INTRUDER

TYPES OF INVESTIGATIONS

- Determine what the incident was and get back to a working state
- Internal investigation
  - Should be based on IR policy
  - May lead to criminal investigation
- Criminal investigation
- Support for “real world” investigations

REAL-LIFE CASES WHERE DIGITAL FORENSICS PLAYED A CRUCIAL ROLE

THE SILK ROAD

ASHLEY MADISON HACK

ENRON SCANDAL

THE DIGITAL FORENSICS PROCESS

TYPICAL INVESTIGATION PHASES

ACQUISITION

PRESERVATION

ANALYSIS

PRESENTATION

PHASE 1: ACQUISITION

- Analogous to crime scene in the “real world”
- Goal is to recover as much evidence without altering the crime scene
- Investigator should document as much as possible
- Creating bit-for-bit copy of the og data source and storing in a secure location

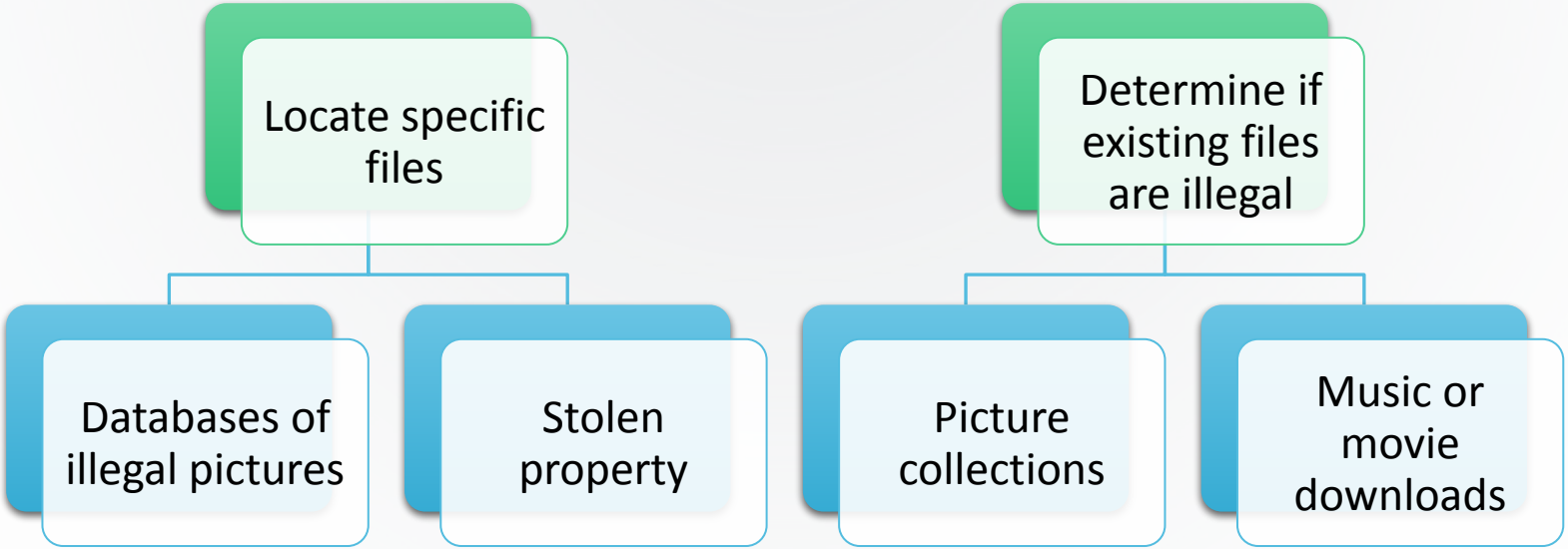
PHASE 2: PRESERVATION

- Ensure that the data remains unchanged
- Goal is to recover as much evidence without altering the crime scene
- Investigator should document as much as possible
- Maintain *Chain of Custody*

PHASE 3: ANALYSIS

- Methodology differs depending on the objectives of the investigation:
  - Locate contraband material
  - Reconstruct events that took place
  - Determine if a system was compromised
  - Authorship analysis

CONTRABAND MATERIAL



LOCATING MATERIAL

- Requires specific knowledge of file system and OS.
- Data may be encrypted, hidden, obfuscated
- Obfuscation:
  - Misleading file suffix
  - Misleading file name
  - Unusual location

EVENT RECONSTRUCTION

- Utilize system and external information
  - Log files
  - File timestamps
  - Firewall/IDS information
- Establish time line of events

TIME ISSUES

- Granularity of time keeping
  - Can’t order events that occur in the same time interval
- Multiple systems:
  - Different clocks
  - Clock drift

COMPROMISED SYSTEM

- If possible, compare against known good state
  - Tripwire
  - Databases of “good” files
- Look for unusual file MACs
- Look for open or listening network connections (trojans)
- Look for files in unusual locations

AUTHORSHIP ANALYSIS

- Determine who or what kind of person created file.
  - Programs (Viruses, Trojans, Sniffers/Loggers)
  - E-mails (Blackmail, Harassment, Information leaks)
- **If actual person cannot be determined, just determining the skill level of the author may be important.**

PHASE 4: PRESENTATION

- An investigator that performed the analysis may have to appear in court as an expert witness.
- For internal investigations, a report or presentation may be required.
- Challenge: present the material in simple terms so that a jury or CEO can understand it.
- Creation of reports, charts or visualizations

FORENSICS TOOLS

- Acquisition
  - dd, pdd, Encase
  - SafeBack
  - Write-blockers, WiebeTech
- Recovery
  - Encase
  - TCT and SleuthKit
  - Md5sum, sha1sum
- Analysis
  - Wireshark, NetworkMiner - Network Analysis
  - Photorec, Testdisk/Scalpel - Data Carving Tools
  - dtSearch, X-Ways - Keyword search & Indexing
- Presentation
  - Autopsy
  - Tableau

DOCUMENTATION AND CHAIN OF CUSTODY

DOCUMENTATION

- Establishes clear and comprehensive record of the investigation
- Should include details
  - Date and time of investigation
  - Individuals involved in investigation
  - Tools and Techniques used
  - Results of the investigation

CHAIN OF CUSTODY

- Process of tracking the movement of digital evidence from acquisition to presentation phase
- Ensures that the investigation is not compromised
- Establishes Integrity

COMMON TYPES OF DIGITAL FORENSICS METHODS

FILE SYSTEMS

- Get files and directories
- Metadata
  - User IDs
  - Timestamps (MAC times)
  - Permissions, …
- Some deleted files may be recovered
- Slack space

FILE DELETION

- Most file systems only delete directory entries but not the data blocks associated with a file.
- Unless blocks get reallocated the file may be reconstructed
  - The earlier the better the chances
  - Depending on fragmentation, only partial reconstruction may be possible

SLACK SPACE

Unallocated blocks

Mark blocks as allocated to fool the file system

Unused space at end of files if it doesn’t end on block boundaries

Unused space in file system data structures

STEGANOGRAPHY

- Data hidden in other data
- Unused or irrelevant locations are used to store information
- Most common in images, but may also be used on executable files, meta data, file system slack space

ENCRYPTED DATA

- Depending on encryption method, it might be infeasible to get to the information.
- Locating the keys is often a better approach.
- A suspect may be compelled to reveal the keys by law.

RECOVERY (CONT.)

- Locating hidden or encrypted data is difficult and might even be impossible.
- Investigator has to look at other clues:
  - Steganography software
  - Crypto software
  - Command histories

FILE RESIDUE

- Even if a file is completely deleted from the disk, it might still have left a trace:
  - Web cache
  - Temporary directories
  - Data blocks resulting from a move
  - Memory

LEGAL & ETHICAL CONSIDERATIONS

DIFFERENT TYPES OF CASES

CYBERCRIME

INTELLECTUAL PROPERTY THEFT

FRAUD

CONSIDERATIONS

1. Privacy
2. Evidence Integrity
3. Professional Standards
4. Jurisdiction
5. Data Protection

Digital Forensics Professionals must be aware of a range of legal and ethical considerations in order to ensure that their investigations are conducted in a forensically sound manner.

FUTURE IN DIGITAL FORENSICS

FUTURE IN DF

- The need for standards
  - Acquisition procedure: develop step-by-step instructions to be followed
  - Certification
    - Investigators
    - Tools
    - Operating Systems

FUTURE IN DF (2)

- Research
  - Create more meaningful audit data
  - Ensure integrity and availability of audit data
  - Privacy and Digital Forensics
  - Develop detection techniques

THANK YOU !