Féidearthachtaí as Cuimse
Infinite Possibilities

Case Management & Report Writing and Tools of the Digital Investigator

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Forensics - Week 4 – 11th Oct 2024

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Case Management and Report Writing

What's the Big Deal?

- Each case is a project
- Any misstep will be pounced upon by the opposition
- Managing the case as a project helps avoid errors in procedure
- Good reporting allows you to demonstrate good process

Managing a Case

- Case flow can be divided into three stages
  - Preparation
  - Investigation
  - Presentation
- These three stages map well to the Investigative Model

Preparation

- Done outside the scope of a conventional investigation
- Involves “creating” the case investigation team/department
- Policies and procedures are defined
- Team roles are defined

Investigation

- Triage
- First response
- Scene management
- Lab preparation
- Evidence handling
- Evidence examination

Triage

- Assess any risks (to people, systems, or data)
- Mitigate as many risks as possible
- Determine priorities
- Is saving the data more important than nabbing the culprit?
- Is identifying the culprit worth a financial loss?

First Response

- Use the crime scene first-response protocols whenever possible
- Determine the best method for collecting evidence
- Perform live-response if necessary
- Collect evidentiary materials in a forensically sound manner

Crime Scene Management

- Preserve the scene for other investigators
- Survey the scene
- Document the scene (with photos and videos)
- Search the scene
- Try to virtually reconstruct the crime

Lab Preparation

- Prepare a repository for digital evidence
- Sufficient storage
- Sufficient security
- Ensure proper tools are ready
- Ensure personnel are ready to receive evidentiary materials

Evidence Handling

- Prevent environmental contamination
- Block electromagnetic transmissions
- Maintain excellent chain of custody logs
- Have a way to keep devices powered during transport
- Don’t damage anything!

Evidence Examination

- Use the right tool for the job
- Document everything you do
- Never touch the originals

Presentation Stage

- Avoid interpretation of results
- Present all evidence, both incriminating and exculpatory
- Be prepared to back up any statements or findings in the reports

Report Writing

- Contents of the final report
  - Case summary
  - Authorizations, warrants, and subpoenas
  - Procedural documentation
  - All case notes
  - All photographs and videos
  - A conclusion

Case Summary

- Who requested the investigation?
- Who are the principles involved?
- When did the incident occur?
- When was the report filed?
- What allegedly happened?

Procedural Documentation

- An inventory of items examined
- A list of tools used
- A time line of procedures performed
- A list of people who performed these procedures
- Before/after hash values of each evidence image

Findings

- Details of how findings were obtained (tools used, search strings, etc.)
- Results of each action described in the procedural documentation
- A time line that puts the activities in perspective

Report Conclusion

- Ties all of the other parts of the report together
- Presents evidence either supporting or refuting the initial claim
- Does NOT support or refute the claim

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

How to Write a Digital Forensics Report

What is a digital forensics report?

- A digital forensics report is a formal document that presents the findings of a digital investigation, often related to cybercrime, internal audits, or data breaches.
- The report must be clear, structured, and contain all relevant details necessary for non-technical readers such as legal professionals or management, as well as technical experts.

Structure of a report

- There really isn't a de-facto standard or format for forensics report writing.
- Formatting and layout options are up to the examiner/analyst or they may be required to follow a template for organizational policies or jurisdictional court rules.
- The following slide goes through a sample structure.

Structure of a report (sample)

- Title Page
- Table of Contents
- Overview / Case
- Evidence
- Objectives
- Forensic Analysis (Steps Taken)
- Relevant Findings
- Conclusion

Structure of a report

- **Title Page**
  - Basic details of the case name, name of report writer / investigators, contact info
- **Table of Contents**
  - Apply a structure to the report and offer a ToC at the top of the report.
- **Overview**
  - Overview and a summary of the case
  - What has been asked for with respect to the investigation (what are we doing?)

Continued….

Structure of a report

- **Evidence**
  - Present the details of the evidence in our chain of custody
  - Description of the hardware, make, model, serial numbers, description, condition, hash values etc...
- **Objectives**
  - Describe in detail what you were specifically being asked to do for this investigation
- **Forensic Analysis (Steps Taken)**
  - This is what you did as part of your forensics investigation
  - What tools you used (make, model, and version of software etc...).
  - The steps taken, thoroughly documenting what you have done
  - This section is very important, try describe everything in granular detail

Continued….

Structure of a report

- **Relevant Findings**
  - This will be a very detailed section of the report
  - Include all artifacts and relevant findings that you found as part of your investigation
  - Analysis and Interpretation:
    - Data Recovery: Mention any data recovered (e.g., deleted files, artifacts, chat logs).
    - User Actions: Identify any actions taken by users (e.g., file access, external drive connections).
    - Indicators of Compromise (IoCs): List any signs of compromise, such as malware, unauthorized logins, or suspicious activity.
  - Each piece of evidence must offer a description that a layperson would understand

Continued….

Structure of a report

- **Timeline**
  - Create a timeline based on the forensic analysis (e.g., access times, login attempts, file modifications etc..).
- **Conclusion**
  - Summary of the investigation, process followed and the findings
  - Any recommendations for further investigation

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Tools of the Digital Investigator

What's Soft and What's Hard?

- Hardware tools are physical devices
  - Computing tools
  - Data capture tools
- Software tools run on physical devices
  - OS utilities
  - Forensic suites
  - Open source tools

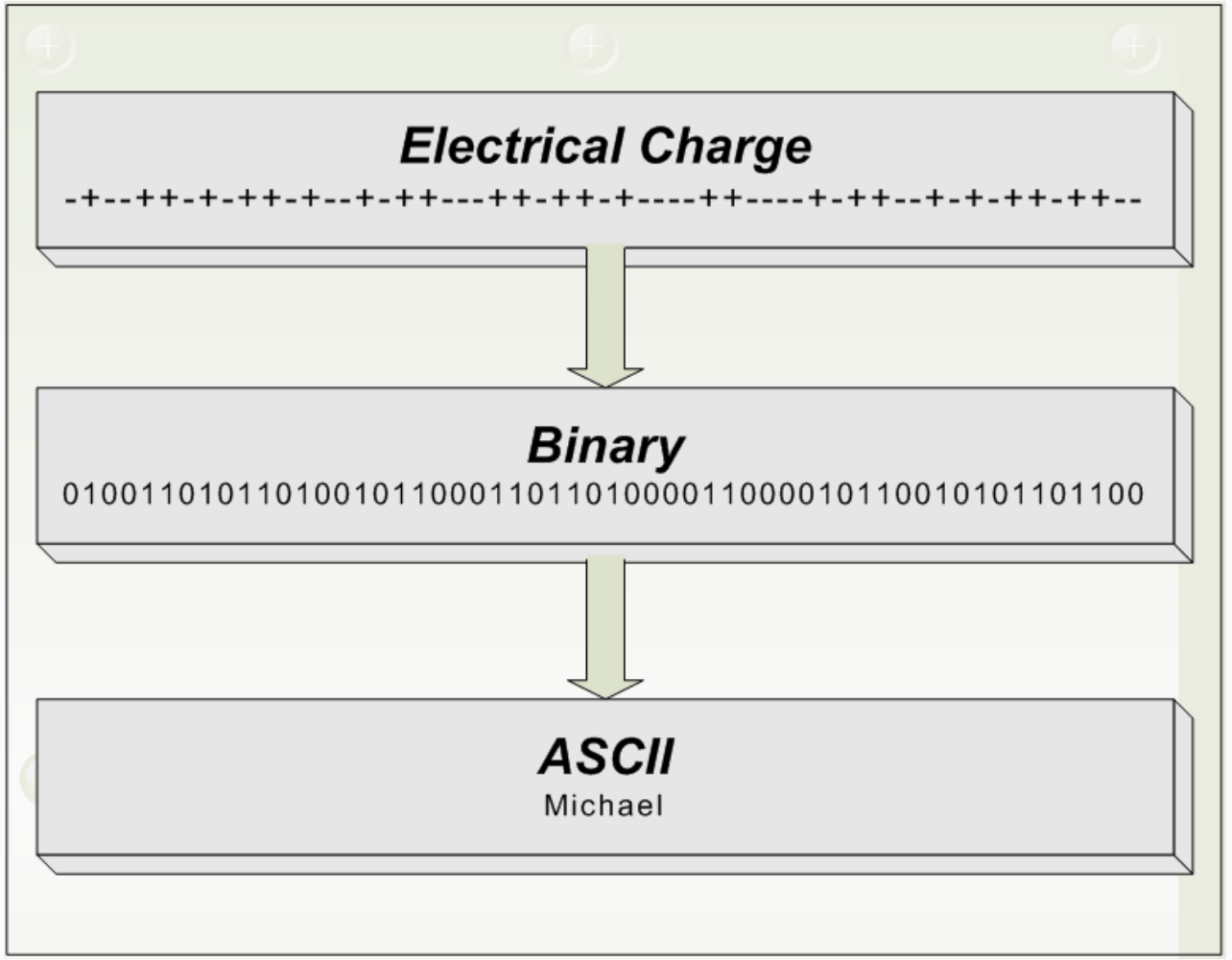
Tool Types

- Media capture and analysis
- Memory capture and analysis
- Application analysis
- Network capture and analysis

Data Abstraction Layers

- Moving information from thought to electronic impulse and back goes through a number of doors
- On an electronic level, data is not humanly readable
- On the human level, the CPU can’t function
- Abstraction layers move up and down the spectrum

Data Abstraction Layers



Measuring Suitability of Tools

- Four necessary traits
  - Accuracy
  - Verification capabilities
  - Consistency
  - Usability
- If even one trait is lacking the tool is unsuitable

The Daubert Test

- From the court case Daubert v. Merrell Dow Pharmaceuticals
  - Can the evidence presented be or has it been tested empirically and can it be falsified?
  - Has the approach or technique been the subject of peer review and publication?
  - Is the technique generally accepted within the scientific or professional community?
  - Does the technique or procedure contain a high known or potential rate of error?

OS Utilities

- Windows
- Linux/Unix
- Macintosh (a Unix derivative)

Windows Utilities

- Regedit (Windows Registry Editor)
- Event Viewer
- Task Manager
- Powershell
- Command Prompt
- Windows Sysinternals Suite
- Prefetch and Superfetch
- Volume Shadow Copy Service (VSS)
- File History and System Restore
- Windows Memory Dump Files
- Backup Utilities
- BitLocker Encryption Tools

Linux Utilities

- Disk Dump (DD)
- dcfldd
  - A forensic-enhanced version of dd
- GREP
- Linux Disk Editor
- PhotoRec
- fdisk, gparted
- hexdump
- grep / find
- stat
- netstat
- wireshark / tcpdump
- auditd
- Log files
- Foremost

Commercial Suites

- EnCase Forensic (by OpenText)
- FTK (Forensic Toolkit) by Exterro
- Magnet AXIOM (by Magnet Forensics)
- X-Ways Forensics
- Cellebrite UFED
- OS Forensics
- Paladin Forensic Suite

This is just a sample…
There are many more…

Open Source Applications

- Autopsy
- Sleuthkit
- SafeCopy
- Metaviewer
- Disk Investigator
- Directory Snoop
- WinHex

This is just a sample…
There are many more…

Court Approved Tools

- There is no such thing
  - Many tools have been acknowledged by individual courts or precincts
  - National Institute of Standards and Testing performs independent tests
- To be accepted in court: test, verify, understand, and be able to explain the tool

Hardware Tools

- A standard tool kit
- Write-protect interfaces for making images
- External storage for archiving images
- Forensic workstations for analyzing data

Non-Technical Tools

- Digital camera
- Video camera
- Audio recorder
- Anti-static bags
- Faraday shield
- Evidence bags
- Labeling material

Questions