Computer Forensics
Semester 2 -2024

Lecturer : Dr. Mbemba HYDARA

Computer Forensics
Case Administration

2

Lecture Objective

- Understand Organizational policies and response Strategy to Computer Crime

Incident Response policy/strategy

Questions an organization must ask itself

- What do we as an organization do if a member of staff is suspected of illegal/inappropriate activity?
  - Have we defined what such activity is?
  - Do we conduct an internal investigation/contract out?
  - What about suspension?

Why an organization need strategy?

- Employee made false ‘allegations’ (damage of character, unfairly suspended)
- Mishandled the investigation
- Information about an allegation ‘leaking’ out, this can have an impact on our reputation
- Potential police involvement because the organization is seen as trying to ‘cover up’ a criminal matter
- Embarrassment and legal issues as a result of an employee stealing data and selling to competitors Liability

Analyzing the Scope

Some terms...

- The case
- Evidence

Some terms...

- Documentation:
- General case intake form
- Chain of custody form
- The log
- Report

Questions to be asked before embarking on a Case

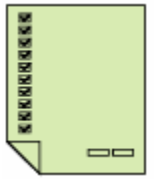
- What is the background (what has happened)?
- What is to be investigated?
- What are the timescales?
- What hardware/operating systems are we likely to be encounter?

Questions Contd.

Reason for establishing the scope and remit:

- Time pressures (member of staff about to leave or currently suspended)
- Potential victims, such as cases of children as victims
- Time scales, amount of time before the court date
- The age of the case
- Is it a criminal or civil case

General Case Intake Form



- This is not standard practice*, but good practice nevertheless
- Checks for conflict of interest in the case
- Defines the remit of the case

Initial Assessment

Collect Preliminary Data

Questions	Considerations
What types of e-evidence am I looking for?	Are you being tasked to look for photographs, documents, databases, spreadsheets, financial records, or e-mail?
What is the skill level of the user in question?	The more sophisticated the user, the more likely that he has the capability to alter or destroy evidence.
What kind of hardware is involved?	Is it an IBM-compatible computer or a Macintosh computer?
What kind of software is involved?	To a large degree, the type of software you are working with determines how you extract and eventually read the information.
Do I need to preserve other types of evidence?	Will you need to worry about fingerprints, DNA, or trace evidence?
What is the computer environment like?	Are you dealing with a network? If so, what are the physical/logical topology, OS, usernames and passwords?

Chain of Custody

Chain of Custody

What is ‘the evidence

- **The Media & the Data**.

The media because it belongs to or was in the possession of the suspect

- Typical forensic investigative procedures and concepts apply)

The data because this is ‘THE’ evidence required by the court to administer justice

Property Record Number: _____

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**

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

Importance of Implementing Forensically Sound Techniques

Responsibility and negligence

- Gates Rubber co vs. Bando Chemical Industries
- Court criticized one of the forensic experts for not making an image copy and stated that
- They had a “duty to utilize the method which would yield the most complete and accurate results

Chain of custody and the 3Cs of Evidence Management

- Evidence not handled correctly can result in it being dismissed from the case.

Requires proving that:

- Data has not been added, deleted, or altered in the imaging process or during analysis
- A complete copy of the evidence was made and verified.

Chain of custody and the 3Cs of Evidence Management Contd.

- A reliable copying process was used
- All media containing the evidence were secured
- All data that should have been copied has been copied
- Chain of custody is a process through which you can prove that the evidence was handled with care, control and consistency.

What do we record in the log?

- When evidence was seized, received by us, where it was located (sketch)
- Record dates if it is released to anyone else
- Details of ‘what’ the evidence is, i.e. make,
- models, serial numbers).
- Access Points.
- Printers and digital cameras.
- Bluetooth devices –PDAs, mobile phones, dongles etc.

What do we record in the log? Contd.

- The legal team (on both sides) should be
- Able to 'retrace' every step in in the investigation through the report and log.

Note: the report is produced by the software, the log by us the team.

Handling Evidence

- Restrict access to evidence,
- Ensure that we have secure premises
- Place original hard drive in an evidence Locker
- Perform all forensics on a image copy, never on the original data.

Investigation Objectives and Chain of Custody Practices

Investigation Objectives	Chain of Custody Practices
Document the scene, evidence, activities, and findings	Document everything that is done; keep detailed records and photographs, etc.
Acquire the evidence	Collect and preserve the original data, and create an exact copy
Authenticate the copy	Verify that the copy is identical to the original
Analyze and filter the evidence	Perform the technical analysis while retaining its integrity
Be objective and unbiased	Ensure that the evaluation is fair and impartial to the person or people being investigated
Present the evidence/evaluation in a legally acceptable manner	Interpret and report the results correctly

End of Lecture...