Week 3

Computer Forensics
Semester 2 -2024

Lecturer : Dr. Mbemba HYDARA

Week 3

Forensic Computer Investigation At the Crime Scene

2

Lecture Objectives

- Understand the importance of decision making at the crime scene
- Understand important ACPO principles
- Understand the process involved in securing, documenting, photographing and transportation at the crime scene.

First steps at the scene

ACPO - Principles

Principle 1:

No action taken by law enforcement agencies or their agent s should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to acces s original data held on a computer or on storage media, that person must be competent to do so and be able to give evi dence explaining the relevance and the implications of their actions.

ACPO Principles Contd.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved.

An independent third party should be able to examine those processes and achieve the same result.

ACPO Principles Contd.

Principle 4:

The person in charge of the investigation (the cas e officer) has overall responsibility for ensuring t hat the law and these principles are adhered to.

Seizure of Equipment

- ACPO guidelines state that : “a computer or associated media should not seized because it is there.
- The person in charge of the search must make a consciou s decision to remove property and
- There must be justifiable reasons for doing so”,
- It proceeds to state that: “officers should ensure they are a cting within the terms of the search warrant”.

The Crime Scene

Note: Most investigation is done away from the crime scene.

- Our involvement with the crime scene will be for two reasons.
  - ‘capture’ what might otherwise have been lost (live data –Live forensics)
  - Seize the evidence (off-line investigation

Crime Scene Contd.

- Must ensure that we do not compromise or corrupt the evidence
- ‘Traditional’ forensic science techniques may apply Visual inspection of environment or devices (faulty?)
- Perimeters may have to be defined to limit access to authorized personnel
  - Device and power supply
- Identify people who normally have access to the system as the investigator may need passwords

Video and Photography

- The room, equipment, layout
- Connection of devices (leads)
- Running OS programs
- Running network processes
- Do not use the Windows screen capture
- RAM overwriting
- Insertion of external devices (to save the screen
- shot) modifies the registry
- If no camera, draw a sketch of the scene

Periphery Search

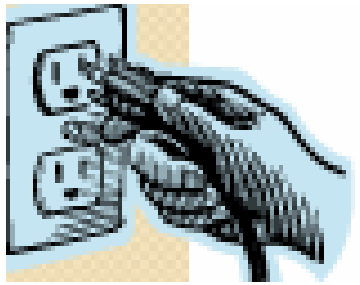
Search the area around the sus

pect machine for

- Diaries
- Notepads
- Post-its
- Passwords…

Power on/Power of

Should a machine be unplugged?



- Graceful power down or power up
- Graceful power-down or power up…
- Crucial servers…
- Network enabled forensic software
- Allow printers to complete
- Always remove power from the back of machine not wall
- UPS systems

Is it really switched off

Fans , Hard disk lights, Power lights, Screen savers

- Determine whether to bring machine out of screen saver mode
- Note that moving the mouse touching keyboard

may inadvertently bring the machine out of screen saver mode

- Photograph/video screen when brought out of screensaver mode
- Screen may be password protected. Take note

Laptops

- If turned off, remove battery
- Opening the lid might power on a
- ‘hibernated’ laptop
- Is the laptop in ‘standby mode’ – how can
- you tell?
- Removing battery in these circumstances

  you will lose ‘hibernated data’.

Networks

Network Cables and Wireless Devices

- Do we disconnect network cables?
- Is there a network process taking place?
- Is there a network process taking place?
- Do we need to take photos of it?
- Could the machine be ‘hacked’ over the network if we do not act?
- Do we disconnect wireless devices?
- Can we analyze wireless network traffic?

Network Configuration

- Switches, hubs, routers, firewalls (or devices which
- combine all three)
- These will indicate network activity
- Embedded network cards (e.g. Intel Centrino).
- Access Points.
- Printers and digital cameras.
- Bluetooth devices –PDAs, mobile phones, dongles
- etc.

Network Configuration contd.

- Hard drives both wired and wireless (may not be on site). site).
- Trace back connections, tally port numbers with machines
- Investigate configuration of routers/firewalls
- May require cooperation of IT staff

Documentation at the Crime Scene

Documentation at Crime Scene

Note: There are two levels of documentation that we complete when we arrive at a scene giving an overview and that

- Which we complete when we seize equipment for investigation. They are not always the same thing...

Documentation on arrival at a crime scene…

- Sketch map of scene.
- Details of all persons present where computers are located.
- Remarks/comments/information offered by user(s) of computer(s).
- Actions taken at scene showing exact g time.

Document the crime scene contd.

- Locate all evidence to be seized (use forms)
- Record a general description of the room:
- Type of media found
- What types of media devices are located in, near the computer
- What did we do with the device, i.e. pull the plug.

Note down Technical Details

Labelling

- Label each lead with each port so that you can p reconstruct later on

Description

- Make, model and serial number.
  Hard disk doesn't have to be removed at the site.
- MAC/IP addresses (if still on)
- Operating System/service pack (if still on)
- Time on the machines (for benchmarking) (if still on)

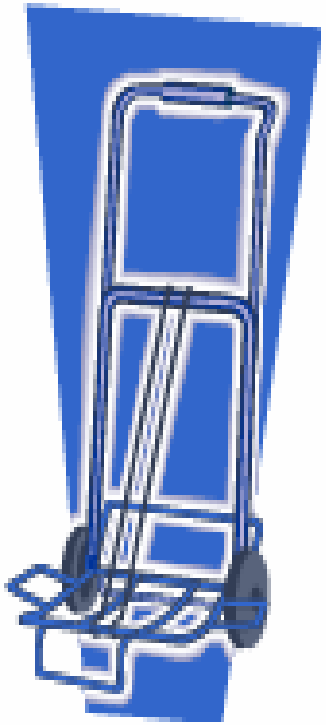
Transportation and Storage

Seize, Store, Tag and Transport

- Allow machines to cool down before transporting.
- Evidence stored in plastic/antistatic bags/boxes
- Tagged with information previously discussed
- Transported to site where investigation will take place,
- ensure this is done in a safe and secure manner
- Store items at room temperature

Useful Transporting Equipment

- Luggage cart
- Handcart Hand cart
- Bungee cords with hooks or clamps
- Duct tape
- Small cargo net
- Leather gloves Leather gloves
- Twist ties
- Plastic cable ties/Plastic Cuffs



End of Lecture...