Introduction to Computer Forensics and Security

6G7Z1009

“Digital Evidence”

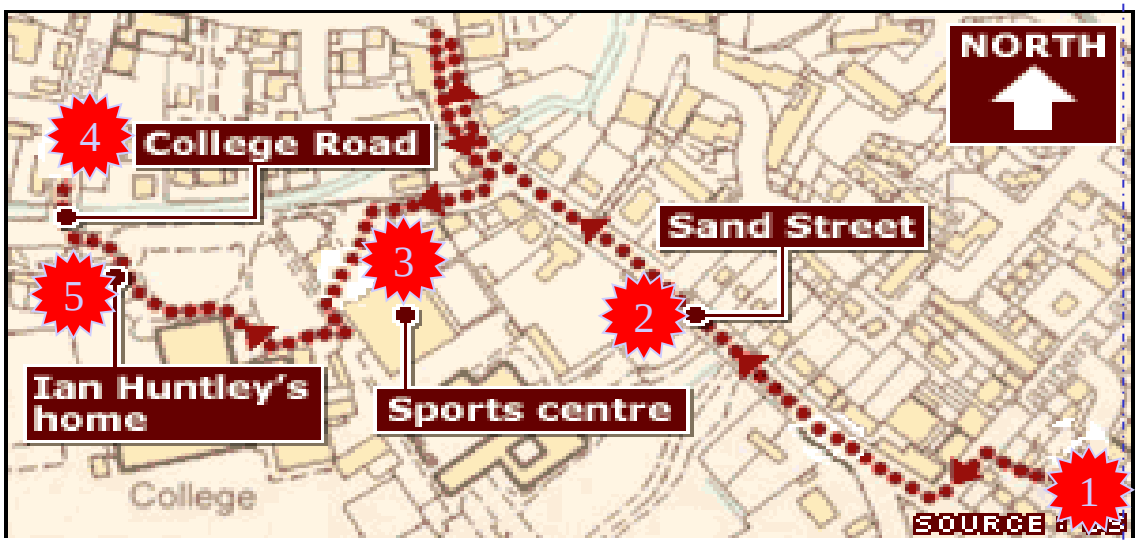
Introduction

Computer forensics investigators are "detectives of the digital world."

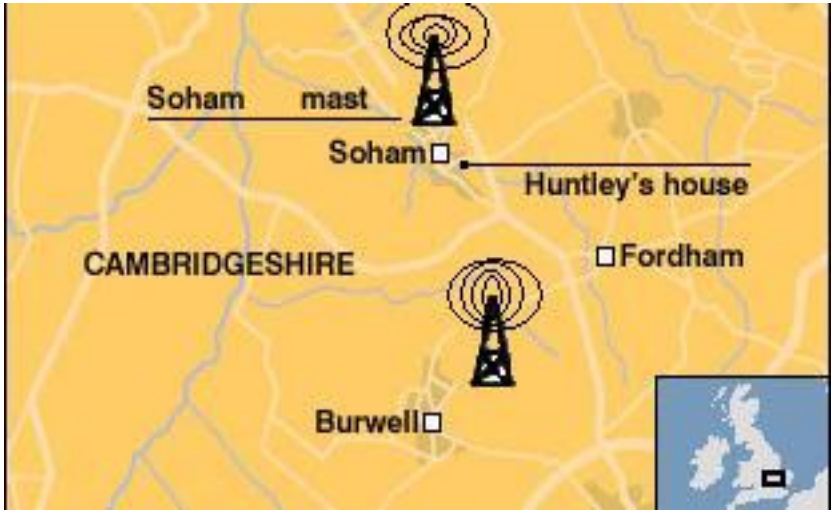
Objectives

- Critical analysis of a real crime scene scenario
- Explain the different types of evidence
- Identify how electronic evidence differs from physical evidence
- Identify different types of electronic evidence
- Identify issues related to the Admissibility of Evidence

Case Study



1. 18:15 Holly & Jessica left Holly's house.
2. 18:25 The girls seen in sand street.
3. 18:28 CCTV photographs the girls crossing the sport centre car park.
4. 18:32 Last sighting of the girls on college road.
5. **18:46 Jessica's mobile phone switched off.**



Evidence Basics

- Evidence is proof of a fact about what did or did not happen
- Three types of evidence can be used to persuade someone:
  - Testimony of a witness
  - Physical evidence
  - Electronic evidence
- Both cybercrimes and traditional crimes can leave cybertrails of evidence.

Types of Evidence (Cont.)

- Circumstantial evidence: shows circumstances that logically lead to a conclusion of fact.
- Hearsay evidence: secondhand evidence.
- Material evidence: evidence relevant and significant to lawsuit.
- Immaterial evidence: evidence that is not relevant or significant.

Knowing What to Look For

- Technical knowledge of how data and metadata are stored will determine what e-evidence is found.
- For this reason, technical knowledge of investigators must keep pace with evolving data storage devices

Categories of Stored Data

- Courts recognize five categories of stored data:
  - Active, online data (Volatile Information)
  - Near-online data (Nonvolatile Information)
  - Offline storage/archives
  - Backup tapes
  - Erased, fragmented, or damaged data

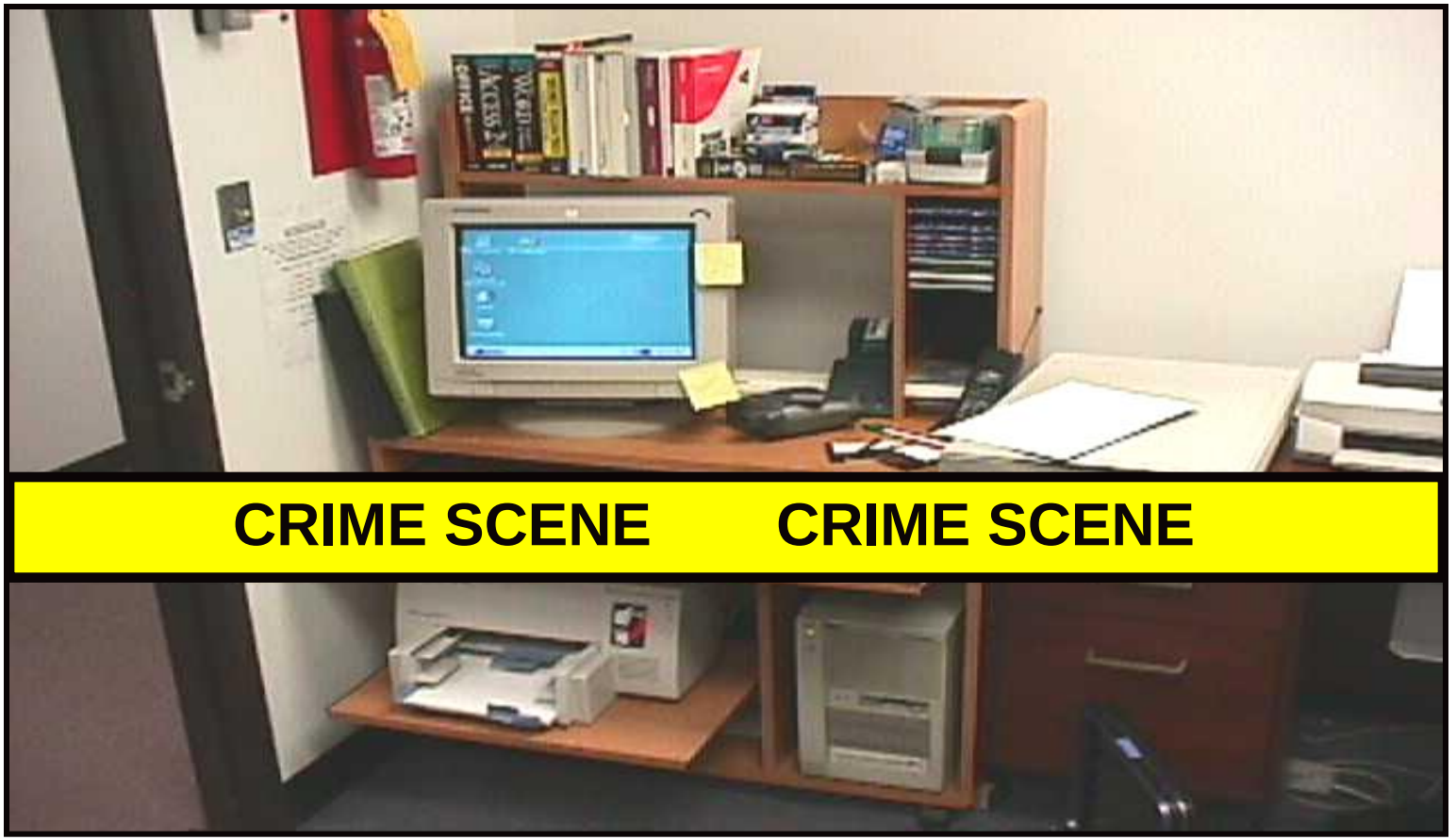
Volatile Information

- Volatile information is data that is lost once the system is rebooted
  - Currently logged-on users
  - The command –line histories of any open windows
  - The contents of clipboard when cut and paste is used
  - Currently open network connections to other systems
  - The current time and date
  - Currently running processes
  - Currently loaded DLLs, drivers, and other modules
  - Background processes and services that are running
  - Last boot time/system uptime
  - Some registry values
  - Currently open network ports
  - Mapped drives and printers

Nonvolatile Information

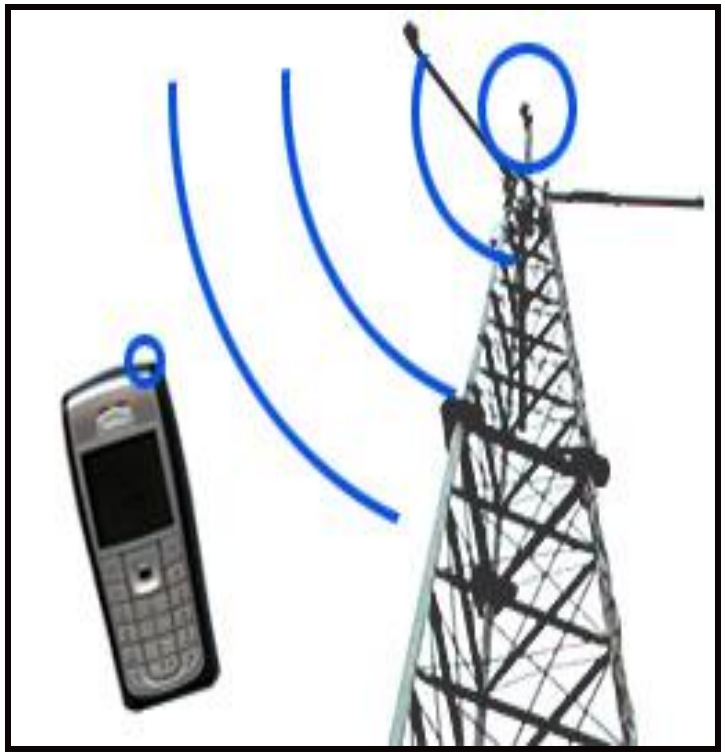
- Nonvolatile information is information that will survive a reboot of the machine and still be available.
  - Most of the registry
  - File system objects
  - Items queued in the printer (interface to the print device)
  - Event Logs
  - Scheduled tasks
  - Application logs
- Nonvolatile information can be damaged by activity triggered by shutdown.
  - Script designed toerase log files on shutdown
  - Normal processing of the system with registry keys like run once
  - Batch files that remove or uninstall programs quietly on shutdown
- Power off boxes instead of running shut down

Knowing What to Look for



Knowing What to Look for (Cont.)

Knowing What to Look for (Cont.)



Knowing What to Look for (Cont.)

Knowing What to Look for (Cont.)

Admissibility of Evidence

- Goal of an investigation: collect evidence using accepted methods so that the evidence is accepted in the courtroom and admitted as evidence in the trial.
- Judge's acceptance of evidence is called *admission of evidence*

Admissibility of Evidence (Cont.)

- Evidence admissibility requires legal search and seizure and chain of custody.
- Chain of custody must include:
  - Where the evidence was stored
  - Who had access to the evidence
  - What was done to the evidence
- In some cases, it may be more important to protect operations than obtain admissible evidence

Search Warrant for Admissible Evidence

- A *search warrant* is issued only if law enforcement provides sufficient proof that there is *probable cause* a crime has been committed.
- Law officer must have a reasonable belief that a person has committed a crime
- The law officer must specify what premises, things, or persons will be searched.
- Evidence discovered during the search can be seized.

Search Warrants (Cont.)

- Two reasons a search can take place without a search warrant:
  - The officer may search for and remove any weapons that the arrested person may use to escape or resist arrest.
  - The officer may seize evidence in order to prevent its destruction.

Forensics Investigation Methods

- Methods used by investigators must achieve these objectives:
  - Protect the suspect system
  - Discover all files
  - Recover deleted files
  - Reveal contents of hidden files
  - Access protected or encrypted files
  - Use steganalysis to identify hidden data
  - Analyze data in unallocated and slack space
  - Print an analysis of the system
  - Provide an opinion of the system layout
  - Provide expert testimony or consultation

The Five Ws

- Answering the 5 Ws helps in criminal investigations:
  - Who
  - What
  - Where
  - When
  - Why

Questions?

m.owda@mmu.ac.uk