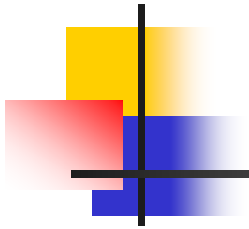
Computer Forensics:
Legal & Evidentiary Issues

Dr Rita Esen

Visiting Reader

northumbria UNIVERSITY

Searching for Digital Evidence



- Search must be lawful
  - All searches must meet legal requirements
- Unlawful search may
  - Result in evidence being rejected in court
- Types of search:
    - Searches with consent
    - Searches with warrants
    - Searches without warrants

Search With Consent

- A person's premises or workplace may be
  - Searched with consent
- Consent to search:
  - In writing
- There should be a clear statement of:
    - Purpose of search

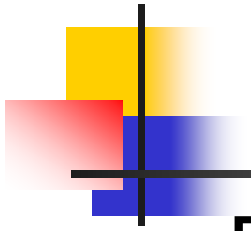
Search With Warrant

- To search for evidence of an offence:
  - A warrant must be obtained
  - The offence must be:
    - A serious crime, or
    - An indictable offence
- Reasonable force to exercise the warrant
- Entry and search must be carried out:
    - Within one month of warrant issue date

Search Without a Warrant

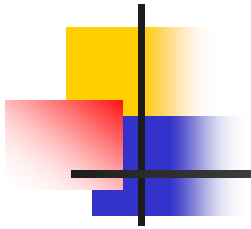
- Police can search without warrant:
  - To execute a warrant of arrest
  - To arrest someone for an offence
  - To re-capture a person who escaped from lawful custody
  - To save life or limb or prevent serious damage to property

Documenting the Scene (1)



- Documentation of the scene should:
  - Create a permanent historical record
- Documentation should reflect:
  - The location & condition of:
    - All electronic devices and paper evidence
- Observe & document the physical scene:
  - Location of computer systems
  - Location of other components
  - Power status (off, on, sleep mode)

Documenting the Scene (2)



- Document irregularities encountered
- Document all aspects of:
  - Operating system
  - Installed patches
- Document the condition of:
  - Collected evidence
- Take legible photographs of:
  - Screen, front & back
- Document pre-existing damage to evidence

Seizure of Digital Evidence

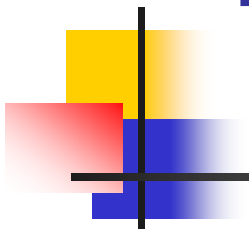
- The right to search computers & networks is:
  - Normally accompanied by the right to seize
- During such searches anything can be seized
  - If there is reasonable grounds to believe that:
    - It is evidence of an offence
    - If not seized it may be:
      - Damaged, concealed or modified


POLICE LINE DO NOT CROSS


RIME SCENE DO NOT CRO
CRIME


CROSS
CRIME SCENE

Packaging Digital Evidence

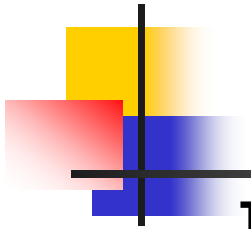


- All collected evidence must be:
  - Properly labelled to:
    - Enable re-assembly of system
- Use antistatic packaging
- Do not use plastic bags as they:
  - Produce static electricity
  - Allow the development of humidity
  - Produce condensation

Transporting Digital Evidence

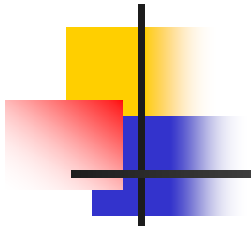
- When transporting digital evidence:
  - Keep evidence away from magnetic sources:
    - Radio transmitters, speaker magnets
    - Heated seats
  - Protect evidence from extremes of temperature
  - Use anti-shock packing materials
    - Bubble wrap

Chain of Custody (1)



- In criminal law, chain of custody is:
  - Tracking of evidence items
    - From the crime scene
    - To its presentation in court
- It documents how, why, when & by whom
  - Digital evidence was handled
- Chain of custody is a vital part of:
  - Validating integrity of evidence

Chain of Custody (2)



- Chain of custody begins:
  - When an item of evidence is collected
- The chain is maintained:
  - Until the evidence is disposed of
- Where chain of custody:
  - Does not show continuous accountability
    - Evidence will be inadmissible in court

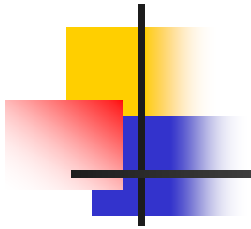
Preparing for Court

- Be familiar with the content of your documents and exhibits
- Prepare an outline of your case
- Be prepared to produce documents that
  - You have referred to in your report
- Find out court location beforehand

Authentication of Digital Evidence

- The evidence must support a finding that:
  - Computer record is what it claims to be.
- Degree of authentication does not vary:
  - Because evidence is in electronic form
- Challenges to authenticity include:
  - Altered or damaged records after creation
  - Reliability of computer program:
  - Identity of author of digital records

Hearsay Issues

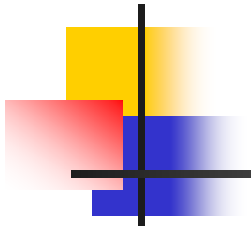


- Computer records:
  - May or may not be ‘hearsay evidence’.
- Contents of records with assertions:
  - Attributed to a third party, and
  - Presented as evidence
    - May be considered hearsay
- Computer generated records where:
  - Humans were not involved
    - Are not hearsay

Expert Witness (1)

- An expert witness is one who:
  - By virtue of education, skills and experience:
    - Has specialist knowledge specific issues
- Expert witnesses are:
  - Required to be independent
- Expert evidence relied on if:
  - Evidence is within scope of case

Expert Witness (2)



- An expert witness should:
  - Address his/her report to the court:
    - Not to commissioning party
- An expert witness may:
  - Give expert opinion if it is:
    - Based on sufficient facts/data
    - The product of reliable methods/principles

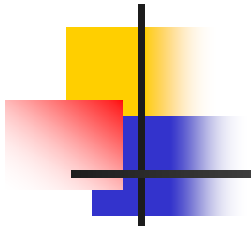
Presenting Digital Evidence

- Explain complex technical issues
  - Powerpoint presentations
    - Text and images
  - Computer animation
    - Showing chronological progression of events
  - Sound recordings
  - Computer simulations
    - Virtual representation of:
      - How events would or could occur

Examination in Chief

- Questioning of a witness by the party who called him/her
- Must not contain leading question
- A leading question is one that:
  - Suggests the answer
  - Contains the information sought after

Cross-Examination



- Questioning of opposing party's witness about:
  - Matters brought up during examination in chief
- Leading questions can be used in cross-examination
- Every party has a right to:
  - Cross-examine opposing witness
- Purposes are to:
  - Attack opposing party's case
  - Discredit opposing party's witness

Re-Examination

- This follows cross examination
- Consists of a second examination:
  - By party that first examined witness
- Addresses issues highlighted during cross-examination
- Re-direct should not open doors for re-cross

Considerations for Jurors

- When presenting digital exhibits to jurors:
  - Avoid using multiple terms to:
    - Describe the same item
      - Computer – desktop, workstation
  - Allow enough time for them to read exhibits
  - Use legible text style
    - Italics and underlines are harder to read
  - Keep visual focus on the evidence
    - Not the presentation technology

Need for International Co-operation

- Cross-border nature
- State assistance to each other
  - Search of digital crime scene
  - Seizure of physical & digital evidence
    - Physical – the container (laptop, desktop, mobile
    - Digital – volatile or at rest
  - Storage, security & chain of custody
  - Analysis, reporting and presentation

Questions