DIGITAL FORENSICS

Lecture 3:
Digital Evidence

Dr. Arghir-Nicolae Moldovan
arghir.moldovan@ncirl.ie

National College of Ireland

AGENDA

- Sources of Digital Evidence and the Investigation Process
- Developing an understanding of the computer forensic examination process, including
  - Types of information to look for
  - Locations where to look for this information
  - Procedures that need to be observed

National College of Ireland

RECAP TYPES OF COMPUTER-BASED CRIME

- Computer intrusion (hacking, activism, etc..)
- Fraud
- Policy violation
- Copyright infringements
- Identity theft
- Child abuse / Paedophilia
- Stalking and Harassment
- Crime of violence
- Drug offences
- Trafficking
- Terrorism
- Plus everything we haven't thought of yet

PROPERTIES OF EVIDENCE

- Admissible
  - Reflects on the requirement to meet certain conditions of acquisition, retention, etc.
- Authentic
  - All relevant; not have been tampered with in any way
- Complete
  - Representing the entirety of the relevant material in relation to an incident
- Reliable
  - All tests and experiments are reproducible and result to the same conclusions
- Believable
  - The jury shouldn't need the 'Anomalous Technobabble Conundrum Guide'

National College of Ireland

DIGITAL EVIDENCE

- Challenges for Investigators
  - Accountability
    - Authentication
    - Access control
  - Relevance
    - Which materials can be attributed to a user's actions
  - Presentation to a jury
    - De-material
    - Jargon

PRINCIPLES OF COMPUTER-BASED ELECTRONIC EVIDENCE

- **Principle 1**: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

- **Principle 2**: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

nhtcu ACPO Guide v3.0

PRINCIPLES OF COMPUTER-BASED ELECTRONIC EVIDENCE (CONT'D)

- **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.

- **Principle 4:** The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

nhtcu ACPO Guide v3.0

EXAMPLES OF DIGITAL EVIDENCE – COMPUTER INTRUSION

- System logs
- Internet activity logs
- IP addresses and user name(s) recorded
- Hacking tools
- Configuration files
- E-mails, notes
- Text files
- Source code
- Etc.

EXAMPLES OF DIGITAL EVIDENCE – COPYRIGHT INFRINGEMENTS

- Address books and contact lists
- CD-DVD/RW h/w
- Cloning software
- Original media (music, films, etc.)
- Scanners and/or printers
- Access to distribution networks (e.g., peer-to-peer)
- Etc.

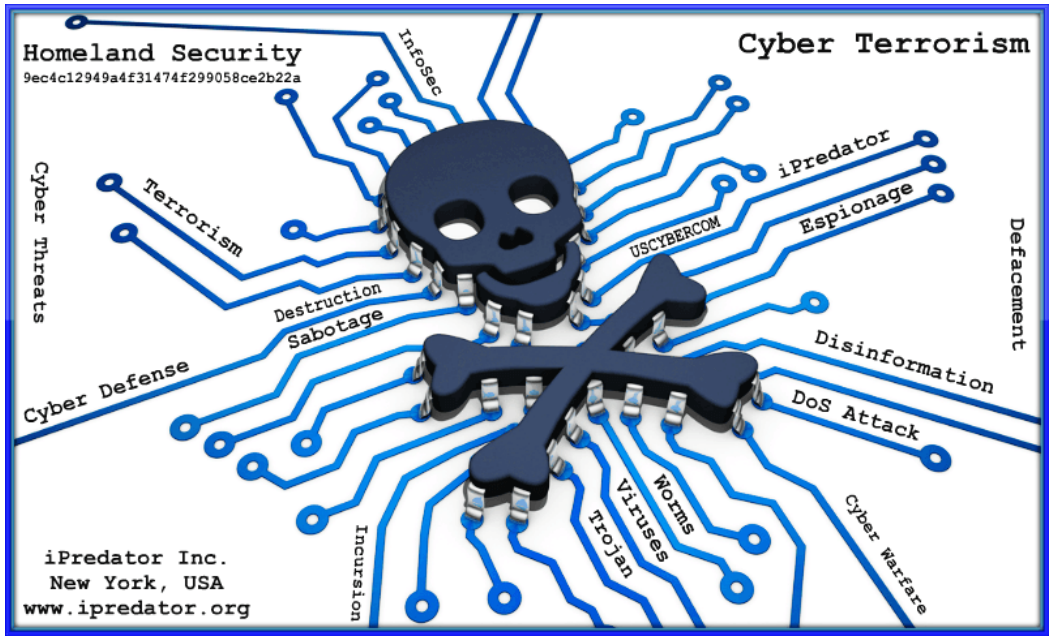
National College of Ireland

EXAMPLES OF DIGITAL EVIDENCE – CHILD ABUSE

- Images
- Other media files (e.g., mpegs)
- Messaging logs
- Digital camera
- Internet activity logs
- Text and word documents
- Graphics editing software
- Games
- Etc.

EXAMPLES OF DIGITAL EVIDENCE – TERRORISM

- Address Books, Contact lists
  - Co-operatives
  - Targets
- Calendars/diaries
- E-mails, notes
- Internet activity logs
- IRC logs
- Social media sites
- Text files
- Databases
- Funding details, Financial templates/forms
- 'Strategic' plans or operational manuals



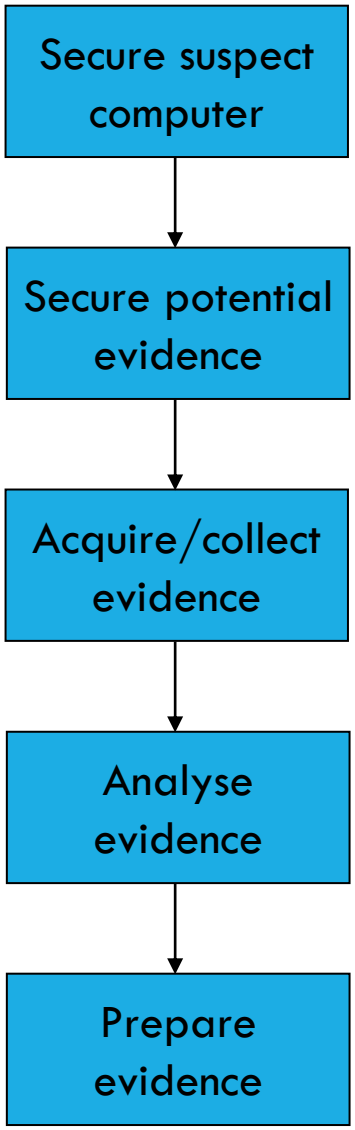
APPROPRIATE HANDLING OF EVIDENCE

- Contaminated or improperly collected electronic evidence has been criticised in many crime cases, civil litigations and corporate internal investigations
- Chain-of-custody
  - Log of whoever had access to the evidence & what they did

INVESTIGATION PROCESS AND PROCEDURES

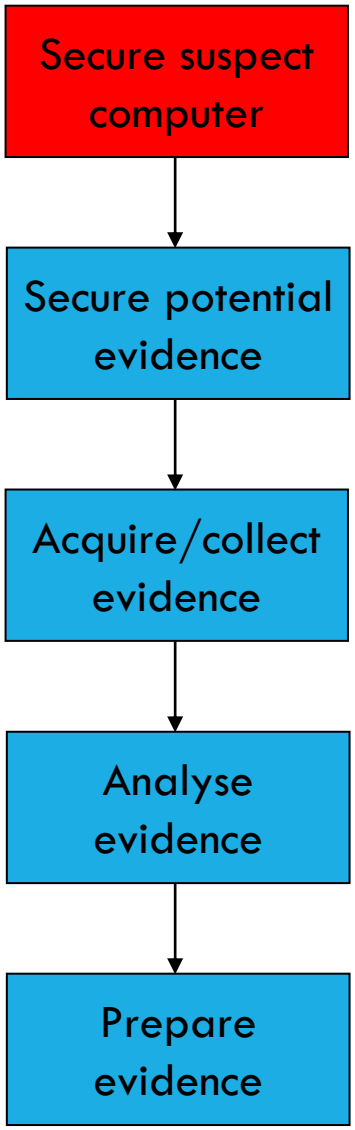
- No single standardised methodology exists for digital investigations

- However most approaches in the literature follow a pattern of
  - Acquisition & Authentication
  - Analysis
  - Preparation & Presentation



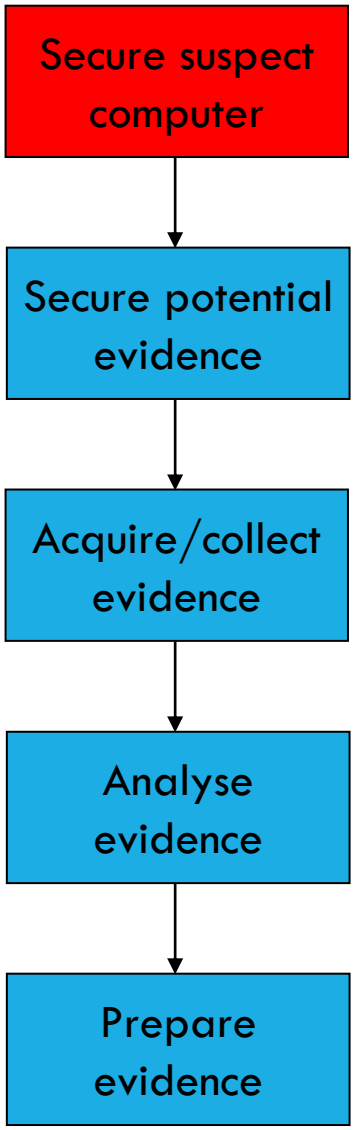
SECURE SUSPECT COMPUTER

- The first step is to identify and physically approach the suspect computer, including equipment
  - Ask the witnesses/suspects if there are any other computers at the premises
- Do not attempt to move a computer if it is switched on
- There is ongoing debate about how to shut a computer down
  - Preventing potential evidence-destructive processes from running further, vs.
  - Corruption of system (or evidence)



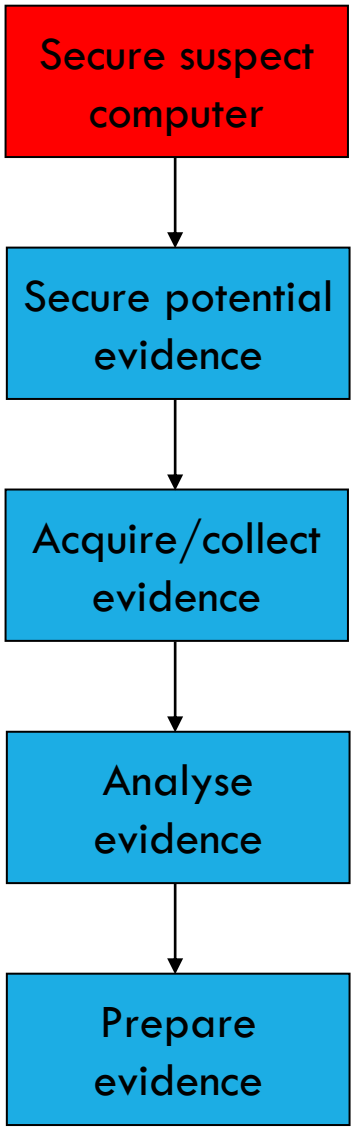
SECURE SUSPECT COMPUTER

- A certain thing is not to reboot the system
  - File slack and swap spaces will probably alter states
- Take photographs or make detailed sketches of the environment
  - Very helpful for when you try and reconnect the peripherals



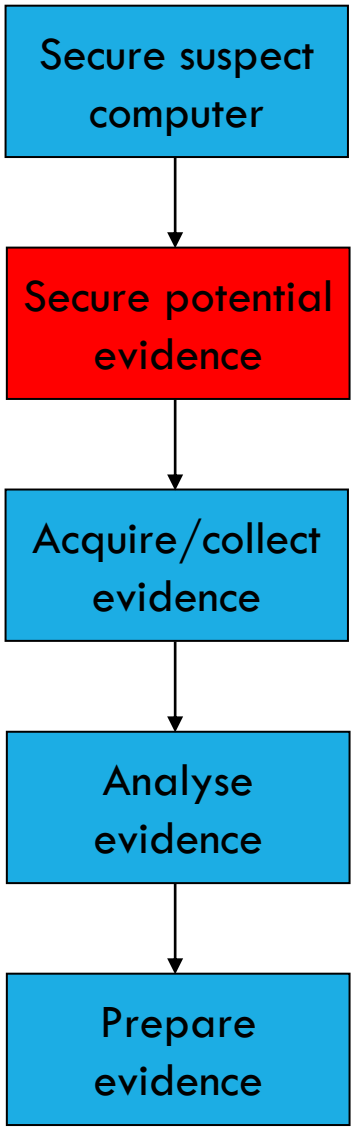
SECURE SUSPECT COMPUTER

- A decision then can be made depending on the circumstances
  - Inspect interfaces or other connections (e.g. modems) and unplug connectivity cables
  - Allow printers to finish jobs
- And maybe eventually… switch off, however
  - Follow the handbook for your organisation on the way to proceed (most of the relevant organisations have produced them)



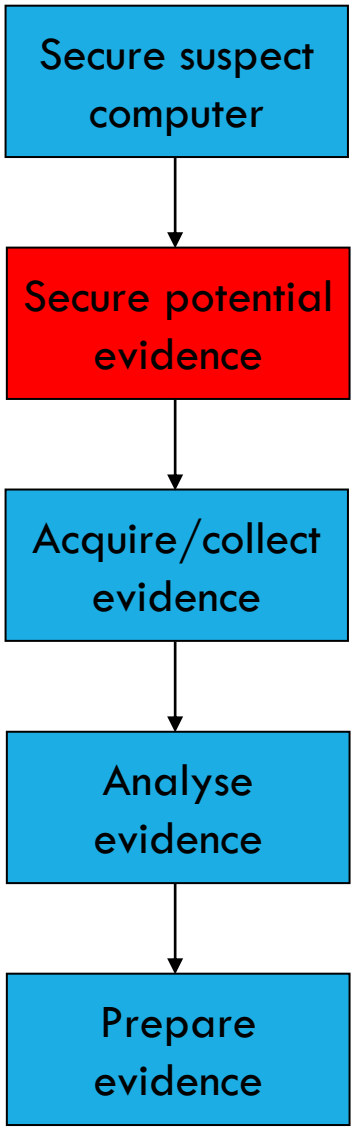
SECURE POTENTIAL EVIDENCE

- Record any 'on screen' messages
- Record details of:
  - Make & Model
  - Any serial numbers for the items of hardware
  - Operating system type in use (if possible)
- If possible try to determine
  - Who supplied the computer
  - Who owns the computer
  - Who has access to the computer
  - What is it used for
  - What software is installed on the computer
  - Is there a BIOS or power on password
  - Are there any File or Application passwords
  - Are there any encrypted areas with passwords



SECURE POTENTIAL EVIDENCE

- An exact copy (image) of the contents of any seized storage media needs to be produced for further analysis purposes
  - This is not a mere file-copying exercise, it is an exact reproduction of the information at the suspect media, as stored at low level
  - All contents need to be examined, including deleted files, slack and swap space and unallocated areas
- Forensic imaging is required

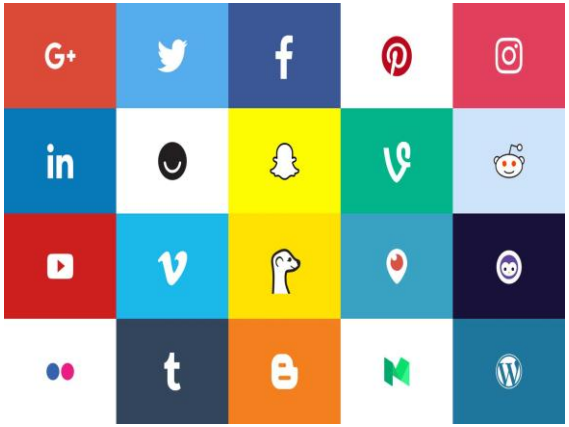


FURTHER SOURCES OF ELECTRONIC EVIDENCE

- When collecting the electronic evidence – Do you have it all?

National College of Ireland

DON'T FORGET... ONLINE ACTIVITY



GOOGLE ARTIFACTS

ONLINE ARTIFACTS

MAY NO LONGER BE ON THE SUSPECT MACHINE

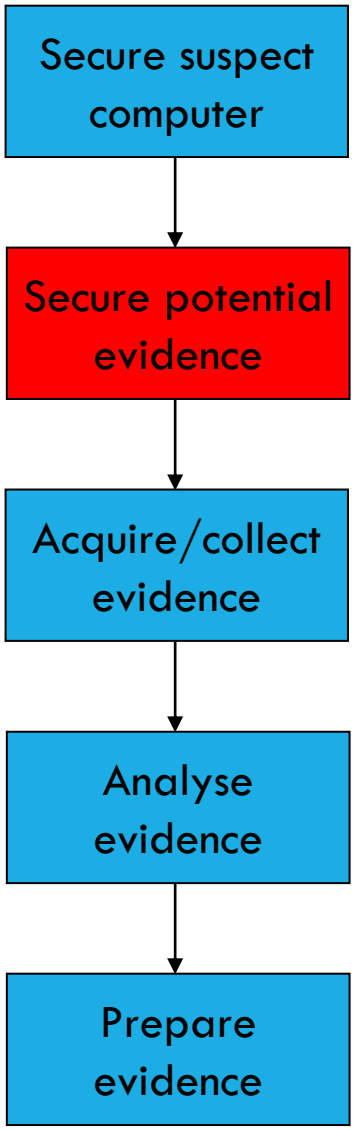
Microsoft Azure

amazon web services

Google Cloud Platform

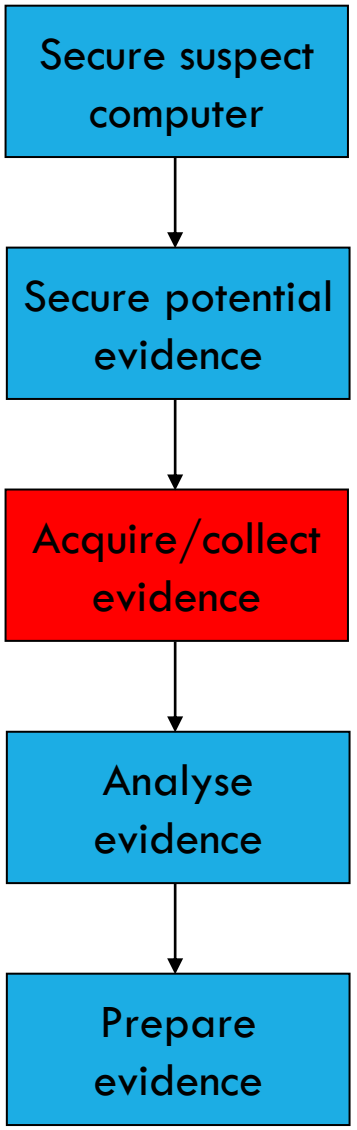
SECURE POTENTIAL EVIDENCE

- Requirements for authenticity and preservation of evidential integrity are met through the application of one-way hash functions
  - Algorithms that compute a unique fingerprint for a message, file, or entire hard drive
  - A change of a single bit of the original data will cause the function to produce a different 'message digest'
- Most widely used algorithms are
  - the Message Digest version 5 (MD5) developed by Rivest at Massachusetts Institute of Technology (1992),
  - the Secure Hash Algorithm version 1 (SHA-1) developed by the National Institute of Standards and Technology (1993)



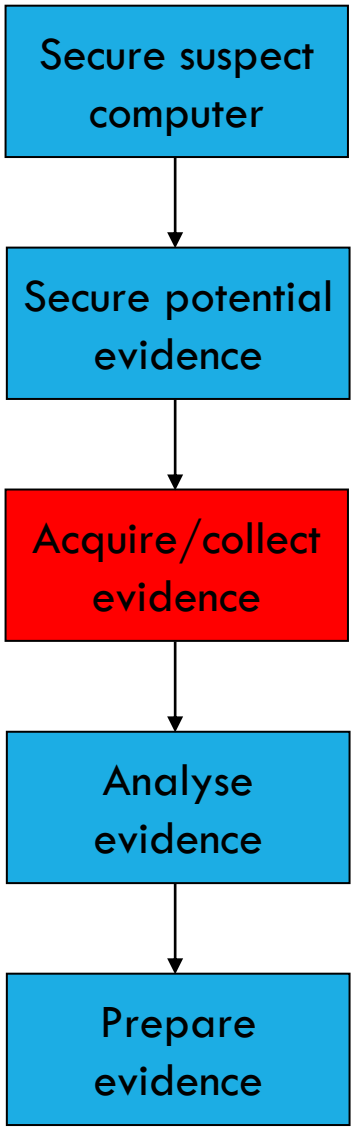
ACQUIRE/COLLECT EVIDENCE

- Ensure that forensically sterile conditions are established
  - All media to be used must be freshly prepared and completely wiped
  - All media to be used must be virus checked and verified
  - All forensic software must be properly licensed for use by the examining body
  - All media should be marked for future identification
- Use of the cloned data to extract evidence in relation to the case
  - No original source can be used for this purpose



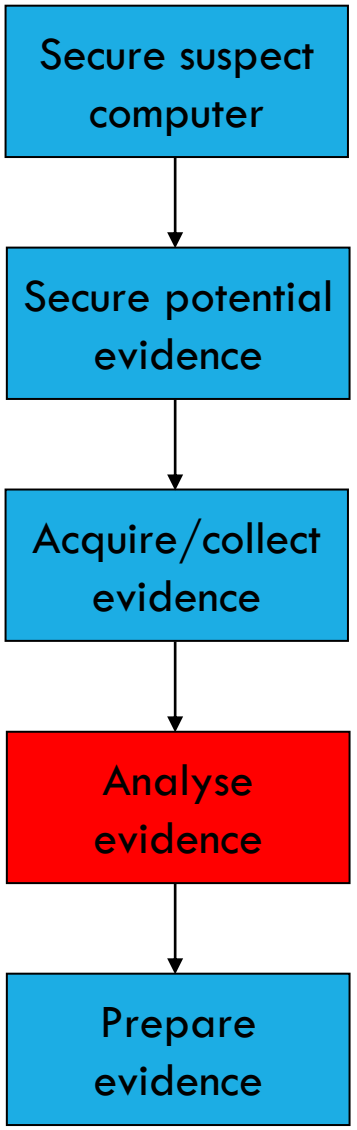
ACQUIRE/COLLECT EVIDENCE

- Evidence can be hiding anywhere
  - Files and folders in good standing
  - Deleted but recoverable files
  - Deleted but partially overwritten files
  - References to files that are no longer there
  - Logs, internet histories, cookies, configuration settings, etc.
- Challenges of acquisition
  - Volume of imaged data (order of magnitude of TB)
  - Investigations of multiuser environments (servers with multiple user settings/data)
  - Target machine power status
  - Encryption
  - Time



ANALYSE EVIDENCE

- Various techniques can be applied in order to correlate evidence and provide an interpretation of a crime scene or incident (we will discuss those in detail later)
  - Log parsing/ Transactional analysis
  - Timeline of events
  - Contextual reasoning
- The instructing party should provide guidance on what it could be retrieved
  - Keywords to run raw searches against the entire contents
  - Types of possible evidence files, e.g. Excel spreadsheets



WHAT CAN BE RECOVERED

- File Carving - Recover Deleted documents and fragments of documents
- Keyword Searching
- Email analysis
  - Webmail traces on hard drive
  - Deleted mails
- Document analysis
  - Timestamps
  - Metadata Information
  - MD5 Hashing
- Password cracking
- Internet usage analysis
- Analyse file fragments in unallocated space or file slack
- Analyse data by using date-ranges
- File type searches

WHAT CAN BE RECOVERED

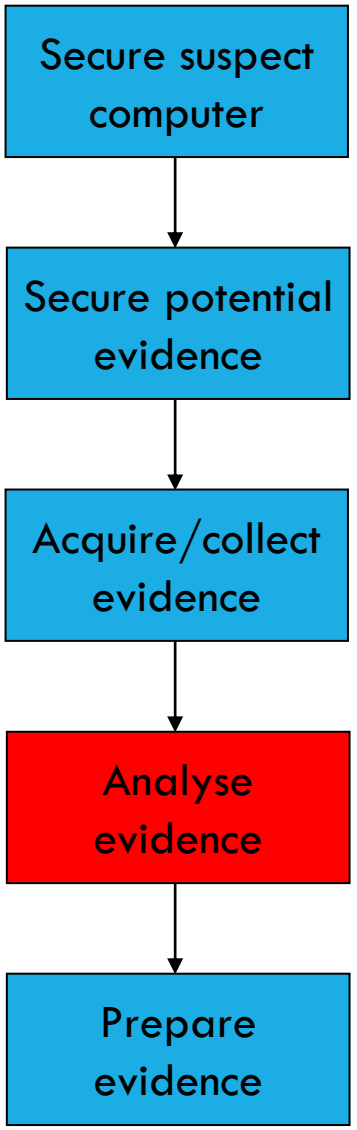
Examples of traces of data that can be found on your PC or digital media?

- Printing docs
- Burnings CDs
- Log-in logs to Networks
- Internet histories
- Application Traces
- Accessing Documents
- Link files
- Deleted files

"Remember Everything you do on a PC leaves traces behind"

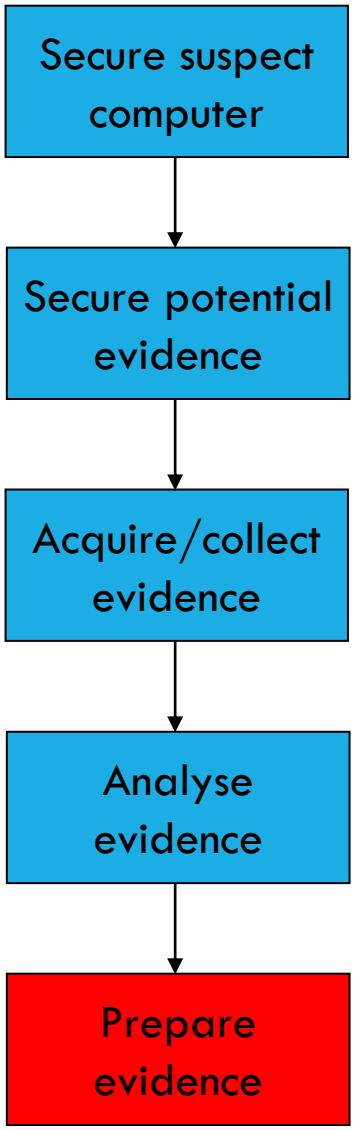
ANALYSE EVIDENCE

- The analysis includes a review of areas of the storage media that do not contain 'rigid' data…
  - File slack or slack space
  - Unallocated areas
- …challenging against the fundamental principles of evidence
  - E.g., how can we know who was responsible for data found in unallocated space



PREPARE EVIDENCE

- To support any investigation findings submitted as evidence, a number of conditions should have been met throughout
  - Authenticity and integrity of evidence
  - Reliability of tests
- Vital role in this plays the documentation of interactions, evidence processing and any other handling



National College of Ireland

IN CONCLUSION…

- Remember the challenging nature of digital evidence
  - Not DNA
- Requirement for detailed documentation and adherence to the code of practice and a disciplined approach
  - We outlined a generic methodology

National College of Ireland

SOURCES

- Backhouse, J. and Dhillon, G. (1995), "Managing computer crime: a research outlook", Computers & Security, 14, 645-651.
- Culley, A. (2003), "Digital Forensics: past, present and future", Information Security Technical Report. Vol. 8, No. 2, pp. 33-36.
- Kruse, W.G. and Heiser, J.G. (2002), Digital Forensics: Incident Response Essentials, Addison-Wesley.
- Wang, Y., Cannady, J. and Rosenbluth, J. (2005), "Foundations of Digital Forensics: A technology for the fight against computer crime", Computer Law & Security Report, 21, 119-127.