UNSW SYDNEY | Australia's Global University

sec edu

security
engineering
capability

COMP6445 – Digital Forensics

Term 3 2019 - Week 1 part 1

17 September 2019

Topics for this lecture

1. Course Introduction
2. Introduction to a career in digital forensics (CBA guest lecturer)
3. The digital forensic expert

Introducing your lecturer

HB171: Guidelines for the Management of IT Evidence (above)
HB231: Guidelines for Information Security Risk Management (below)

- Ajoy Ghosh (ajoy.ghosh@unsw.edu.au)

- Lecture in cyberlaw, electronic evidence and digital forensics at Australian and international universities
  - UTS, Sydney Uni, Macquarie, UNSW/ADFA and now UNSW/SECedu
  - Up until now, postgraduate and predominantly Law and Engineering students

- Australian and international standards:
  - Author of Australian handbook on Management of IT Evidence (now incorporated into ISO 27037)
  - Co-author of Australian standard on Information Security Risk Management (now ISO 27005)
  - Contributor to Australian standard on Corporate Governance of IT (now ISO 38500)
  - On Standards Australia committee that oversees IT security, IT Governance and related standards

- Expert witness in complex and high profile cases:
  - Complex technical crimes: hacking, cyber stalking, cyber bullying, child pornography, fraud and forgery, circumvention
  - Politically sensitive and high profile e.g. Sef Gonzales, James Hardie, Sydney terrorism trials, Simon Gittany, B4L and Bra Boys
  - Precedent setting cases e.g. large e-discovery, expert “hot-tubbing”, fabrication of PDF documents

- Advisor to Government and industry:
  - IRAP Assessor with Australian government clearance NV2. IRAP and cyber assessments of significant critical infrastructure and safety-critical systems
  - ACS Cyber Security technical committee

Imagine…

- You have been asked to help solve a crime by examining the victims computer
  - What sort of things would you be looking for?
  - You've, managed to recover some data – how do explain what you've done to the detective, lawyer and eventually judge and jury?

Course outline, lectures and tutorial

- I will presume that you have read the course outline which lays out weeks 1 to 10

- Lectures 3 hrs on Tuesday evening
  - For first 5 weeks
    - 1 hr - about the discipline of being a digital forensic expert
    - 1 hr - about a technical capability
  - Discussion and explain weekly tutorial/lab and assessments
  - Most lectures will be recorded:
    - Not disturbing cases and self-care (week 5)
    - Not all guest lecturers

- Tutorial/labs
  - On Wednesday supervised by tutors
  - Usually a technical activity accompanied by short quiz
  - Week 10 is for presentations

Assessments

- 10% = week 1 activity
  - Hand out today and due next week (online submission)
- 10% = mid term quiz
  - 45 mins during class in week 6
  - Multiple choice and short answers
- 20% (i.e. 8×2.5%) = tutorials/labs
  - Combination of tutors observation, short quiz and reflections
- 30% = major assignment
  - Hand out week 2 and due week 8 (online submission)
  - Scenario based
  - Hands on forensic examination + write expert's report + reflection
  - Only extensions by special consideration
- 30% = exam
  - TBA in Term 3 exam period
  - Multiple choice, short answers and short essay (about 2 pages)

Some rules/expectations

- From next week onwards, I will presume you have read the ”required” reading for each week’s lecture prior to the lecture
- Interactive lectures
  - Ask questions
  - Stimulate discussion by offering your own experiences
- I and guest lectures can only discuss what has already been made public for individual cases
  - We will let you know what we can and can’t discuss
- If you are already working on a real case or one comes up during this semester, let’s discuss it early to avoid any conflict of interest. I don’t need or want to know the details, merely:
  - Case reference (if allocated)
  - Parties and their solicitors

Some rules/expectations (cont)

- Be minful of the SECedu "*good faith policy*"
  - This means we expect you to act in good faith at all times. We expect you to be a good citizen. To not invade, alter or damage the property of others including the university , invade the privacy of others, break any laws or regulations, annoy other people, deprive others of access to resources, breach or weaken the security of any system, or do or omit to do anything else which you know or suspect we would not be happy about. Furthermore you are not to do anything which appears OK by a loophole or a strict interpretation of "the letter of the law" but which is not consistent with the spirit. Basically you must not act in any way so as to bring disrepute to the reputation of the course, the course staff, fellow students, the school, the university, or the ICT profession. Don't be a bad person.

- Whilst we will discuss disturbing and illegal things, whilst in class or for class:
  - If you think this will affect you, please raise it early (and well before week 5)
  - You are not to access illegal material e.g. child pornography, jihadist, etc or do illegal things e.g. unauthorised access, circumvention, etc
  - Take reasonable care when doing activities – VMs may have malware and sensitive material (we have intentionally chosen old malware which should be detected by common antivirus software)

Some rules/expectations (cont)

- This is an introductory course. The hands-on activities have been simplified and structured for a learning experience
- You are not to distribute or publish learning materials including slides and activities
  - Students can access then on WebCMS
  - They are only to be used for UNSW purposes
- The specific methods and tools described in the course are general advice. You need to make your decision regarding what methods and tools you use based on the circumstances for each particular case

What is forensics?

- The adjective forensic comes from the Latin word *forensis*, meaning “in open court” or “public.”

- Forensic science (often shortened to forensics) is the application of a broad spectrum of sciences to answer questions of interest to the legal system. The study and application of science to matters of law.

Some definitions

From ISO 27037

- Digital evidence
  - Information or data stored or transmitted in binary form that may be relied upon as evidence
- Digital evidence first responder (DEFR)
  - a person authorized and qualified to act first on the scene, performing digital evidence collection and acquisition
- Digital evidence specialist (DES)
  - has specialized knowledge and skills to handle specialized tasks
- Most jurisdictions refer to ISO 27037 as a guide and the forensic laboratory accreditations go to some length to point this out
  - e.g. UK Forensic Science Regulator – Code of Practice and Conduct 2014[1]

From McKemmish[2]

- The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable
- Primary activities:
  - Media and electronic device analysis
  - Data communication analysis
  - Research and development

1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/351220/2014.08.28_FSR-C-107_Digital_forensics.pdf
2. What is forensic computing? AIC Trends and Issues #118 1999 see https://aic.gov.au/publications/tandi/tandi118

Another definition of Digital Forensics

- The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purposes of facilitating or furthering the reconstructions of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations.[1]

1. A roadmap for Digital Forensic Research DFRWS 2001. See http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

Digital forensics curriculum development

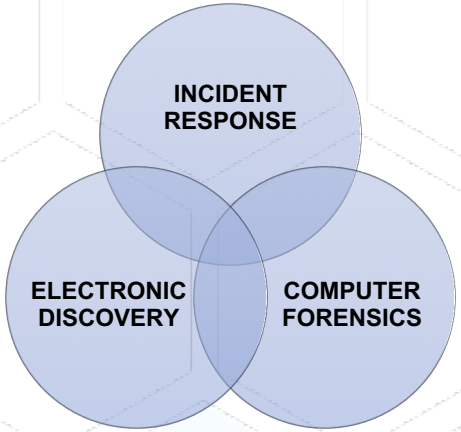
- Ultimately, we are learning how to persuade a decision-maker that our conclusion, based on our interpretation of data (evaluate, critique, synthesise), is the right one.

- Electronic evidence special advisory group – part of ANZ Policing Advisory Agency (ANZPAA)

- Capability framework[1]:
  - Level 1 – Define (Knowledge)
  - Level 2 – Apply (Comprehension)
  - Level 3 – Explain (Application) — **Graduate level**
  - Level 4 – Evaluate (Analysis) — **Graduate level**
  - Level 5 – Critique (Synthesis) — **Postgraduate level**
  - Level 6 – Synthesis (Evaluation) — **Postgraduate level**

1. Valli *Establishing a vendor neutral skills based framework for digital forensics curriculum development and competence assessment 2011*

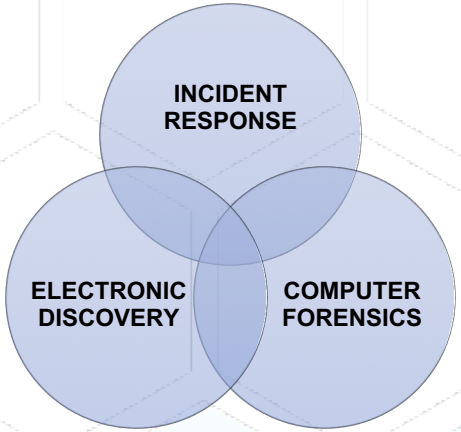
Response versus Forensics



- Incident Response
  - Immediate
  - Primary objective is to limit damage and protect the victim
    - Collecting evidence is secondary
  - Produce contemporaneous artefacts
    - Best effort in the time and with the tools available
  - Responder may be a witness but is not expected to know the rules of evidence
  - Generally not regulated in Australia
    - May be specific industry-based requirements

- Computer Forensic
  - Post event
  - Objective is to investigate i.e. discover the truth
    - Discover Who, What, When, Where, Why and How
    - Disciplined process – some might say “limiting”
  - Benefit of time and hindsight
    - Produce artefacts that are reliable, sufficient and understandable (even persuasive)
  - Is expected to be an expert
    - Expert judgement
    - Know the rules of evidence
  - Regulated across Australia (mostly)
    - Expert witness code of conduct

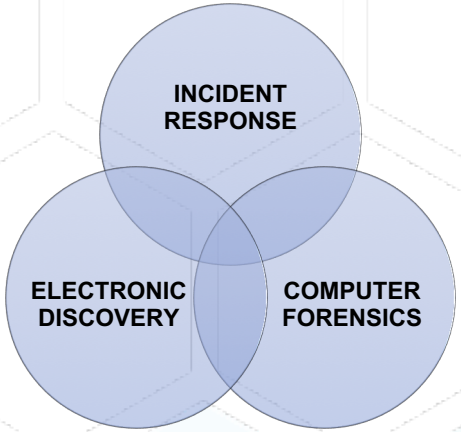
Response versus Forensics



- Incident Response
  - Immediate
  - Primary objective is to limit damage and protect the victim
    - Collecting evidence is secondary
  - Produce contemporaneous artefacts
    - Best effort in the time and with the tools available
  - Responder may be a witness but is not expected to know the rules of evidence
  - Generally not regulated in Australia
    - May be specific industry-based requirements

- Computer Forensic
  - Post event
  - Objective is to investigate i.e. discover the truth
    - Discover Who, What, When, Where, ~~Why~~ and How
    - Disciplined process – some might say “limiting”
  - Benefit of time and hindsight
    - Produce artefacts that are reliable, sufficient and understandable (even persuasive)
  - Is expected to be an expert
    - Expert judgement
    - Know the rules of evidence
  - Regulated across Australia (mostly)
    - Expert witness code of conduct

Response versus Forensics

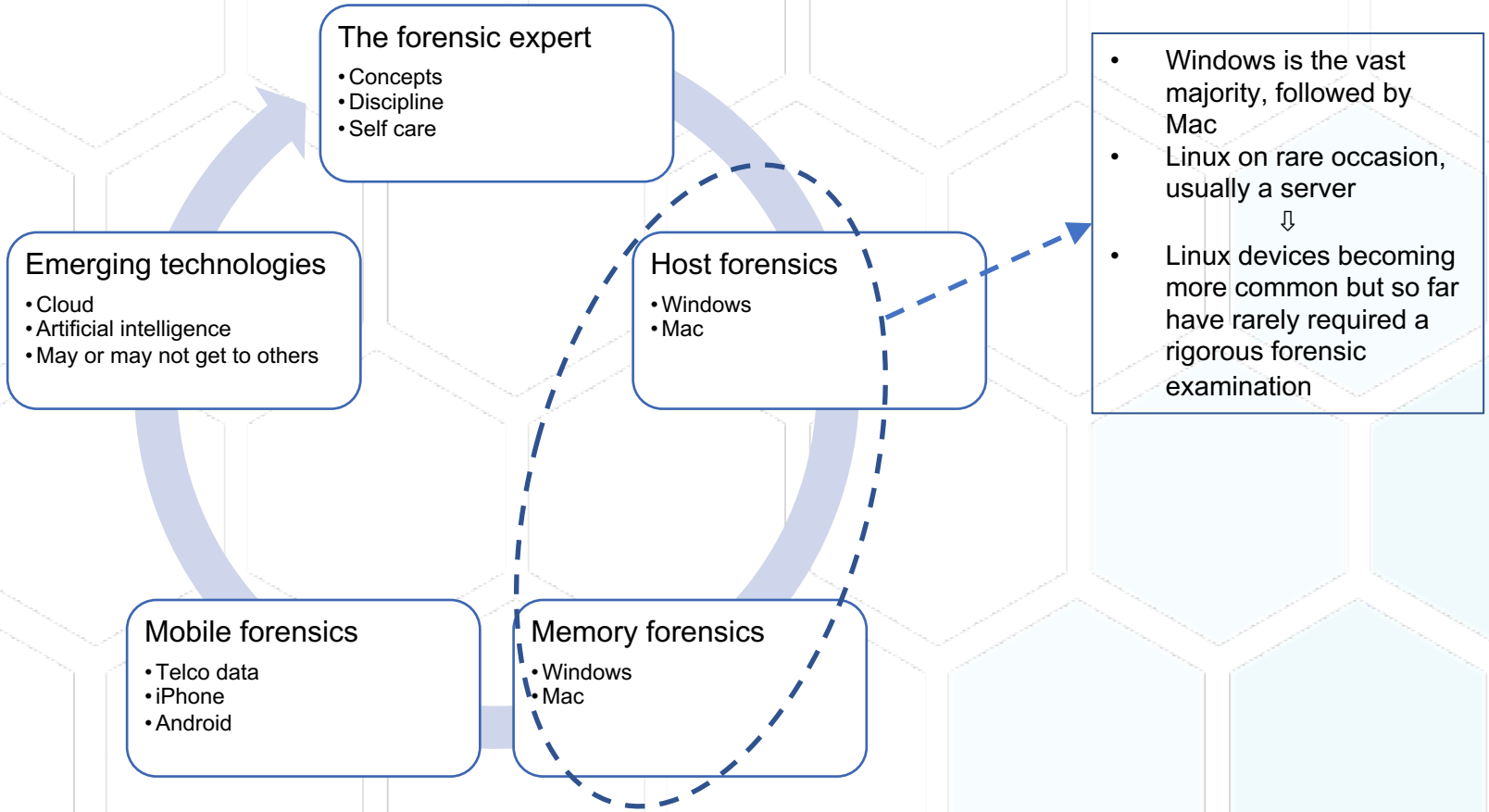


- Incident Response
  - Immediate
  - Primary objective is to limit damage and protect the victim
    - Collecting evidence is secondary
  - Produce contemporaneous artefacts
    - Best effort in the time and with the tools available
  - Responder may be a witness but is not expected to know the rules of evidence
  - Generally not regulated in Australia
    - May be specific industry-based requirements

- Computer Forensic
  - Post event
  - Objective is to investigate i.e. discover the truth
    - Discover Who, What, When, Where, ~~Why~~ and How
    - Disciplined process – some might say “limiting”
  - Benefit of time and hindsight
    - Produce artefacts that are reliable, sufficient and understandable (even persuasive)
  - Is expected to be an expert
    - Expert judgement
    - Know the rules of evidence
  - Regulated across Australia (mostly)
    - Expert witness code of conduct

Why did I strike out the ”Why”?

Our focus areas



A career in digital forensics

Tabitha Bauer & Tim Boyce

CBA guest lecturers

The digital forensic expert

Brief intro to evidence

1. Testimony
   - Given by a witness

2. Documentary
   - See Dictionary at end of Evidence Act
   - Part 4.3 of Evidence Act relates to documents, including: *evidence produced by processes, machines and other devices*.

3. Physical
   - A real thing that is able to be produced in Court
   - Often, documents are used in place of physical evidence e.g. picture, video, etc

document means any record of information, and includes:

(a) anything on which there is writing; or

(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or

(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or

(d) a map, plan, drawing or photograph.

From Evidence Act 1995, § 3, Part 1 i.e. Dictionary

Witnesses

- Lay Witness
  - Merely to recall facts based on their own sensual experience (i.e. I saw…, I heard…) and strictly adhering to the rules of evidence. Of course, the lay witness is not expected to understand these rules of evidence and evidentiary process relies on the objection of opposing counsel.
- Investigator
  - Discover facts i.e. undertake investigation. In evidence, the investigator may merely recall fact (unless deemed an ad-hoc expert). Courts have come to expect that the investigator has attempted to discover as much **incriminating** and **exculpatory** evidence as reasonable.
- Expert (we will examine expert evidence in more detail next week)
  - Answer a particular question, or questions as instructed by legal counsel. In doing so, the expert is allowed to provide an opinion based on their particular expertise.
  - In most Australian jurisdictions, an "expert" is loosely defined as a person who has specialised knowledge based on the person's training, study or experience[1].
- Independent Expert
  - Not formally distinguished, but in practice weighs heavily when assessing credibility
  - As well as demonstrating his or her expertise, an independent expert must demonstrate that, apart from their instructions, they have no other interest in the matter at hand.

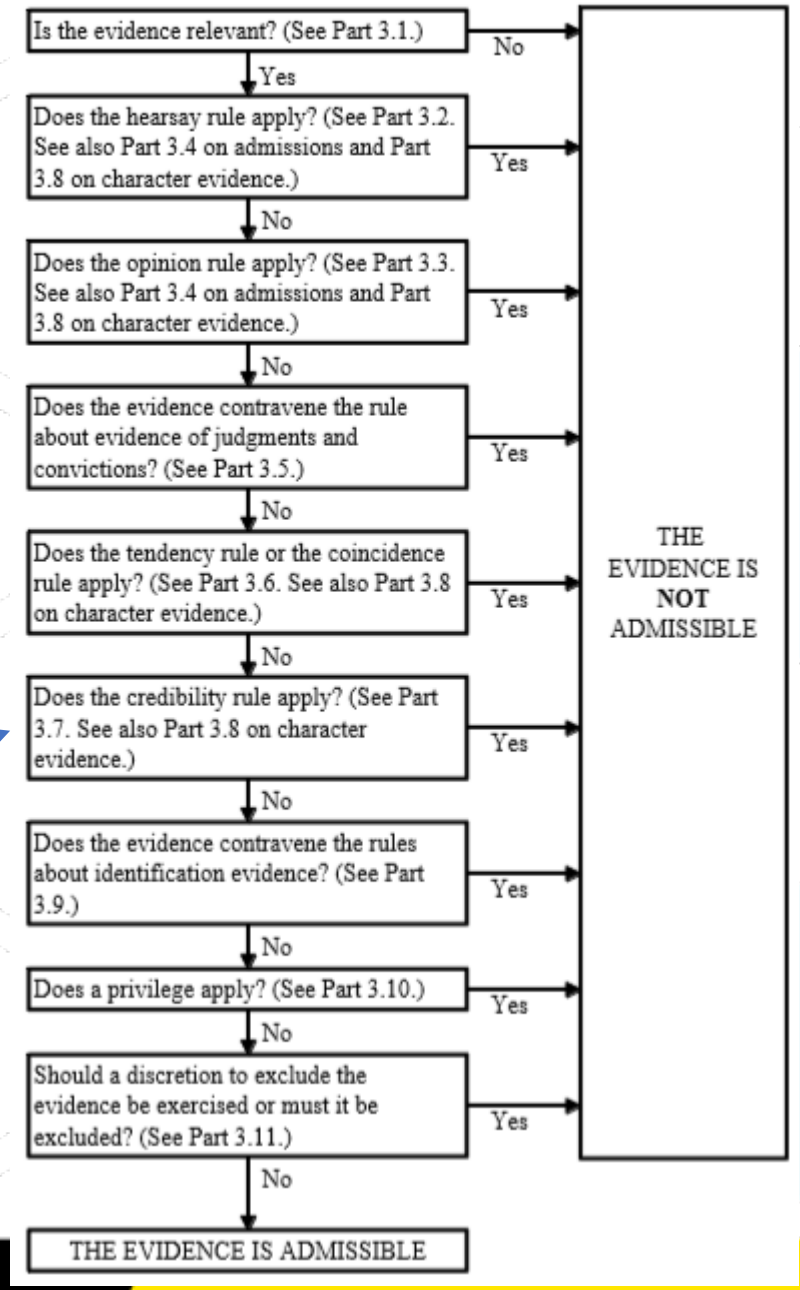
1. See for example s1.8 Supreme Court Rules 1970 (NSW)

Evaluation of evidence

Evidence Act Part 3

BTW, this is a good example why you should look at Acts as they are published and not rely on text-only versions e.g. AustLII (although AustLII is a great starting point)

Here is where "legally obtained" is tested



The Evidence Act is included in the Reading materials for the course

Standards of proof

Civil

- Balance of probability
- In practice, some matters have come to require higher e.g. forgery

Criminal

- Prosecution – beyond reasonable doubt
- Defendant – on the balance of probabilities

In both civil and criminal

- Admissibility of evidence is always on the balance of probability

In other words…

We'll come back to evidence in more detail next week

Short break – 10 mins

And then Week 1 part 2:

- Forensic copying
- Windows forensics #1