UNSW SYDNEY | Australia's Global University

sec edu

security engineering capability

COMP6445 – Digital Forensics

Term 3 2019 - Week 2 part 1

24 September 2019

Topics for this lecture

- Expert opinion in the Australian jurisdiction
  - Factual and Opinion Evidence
    - Admissibility
    - Weighting
  - The Expert Witness
    - The Expert
    - The Expert's Report (or Certificate)
    - In the Courtroom

Recap

STANDARDS OF PROOF

Criminal

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

Civil

- Balance of probability
- Some matter require higher e.g. forgery

Criminal and Civil

- Admissibility is always on the balance of probability

TYPES OF EVIDENCE

Testimony

- Given by a witness

Documentary

- Part 4.3 (i.e. §146 and§147) of Evidence Act relates to documents, including: evidence produced by processes, machines and other devices.

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

Types of witnesses

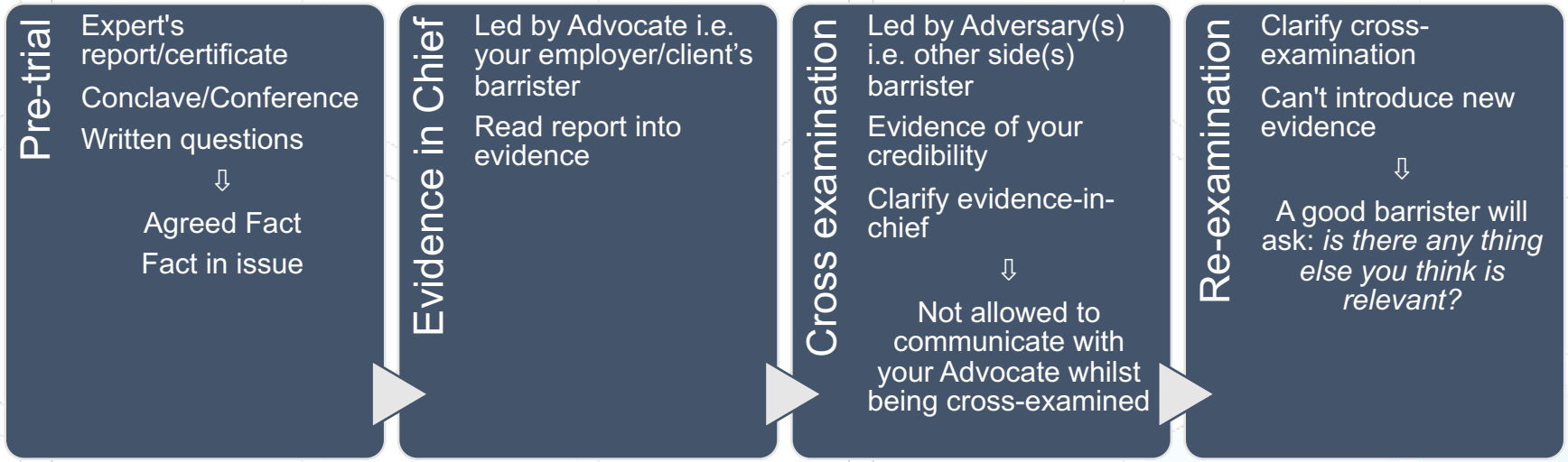
- Lay Witness
  - Merely to recall facts based on their own sensual experience (i.e. I saw…, I heard…) and strictly adhering to the rules of evidence. Of course, the lay witness is not expected to understand these rules of evidence and evidentiary process relies on the objection of opposing counsel.
- Investigator
  - Discover facts i.e. undertake investigation. In evidence, the investigator may also merely recall fact however Courts have come to expect that the investigator has attempted to discover as much **incriminating** and **exculpatory** evidence as reasonable.
- Expert
  - 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 specialized 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)

Types of witnesses

- Who can recap each of these?

Evidence



Having your report become an agreed fact (instead of fact in issue) is the best outcome for you and your client. That is why we will spend so much time on this

This is where many technical experts fail:

- Take the test of credibility as a personal attack
- Not familiar enough with their evidence
- Let their ego trap them into answering beyond the scope of their expertise

Factual and opinion evidence

FACT

Something the person saw, heard or otherwise perceived

Something that is self-evident or common knowledge

OPINION

Hearsay

Specialised knowledge based on the person's training, study or experience

There is a grey area that relates to business records, tags and labels and electronic communications. These happen to be what we are often asked to give evidence on

Factual and opinion evidence (cont)

ADMISSIBILITY

- Will the evidence be allowed?
  - If so, which parts?

⇩

This is the first hurdle

1. Fact in issue
2. Agreed fact

WEIGHTING

- How persuasive is the evidence?
  - If there are opposing views, which one will the decision-maker rely on

⇩

Written report

+

Testimony in Court

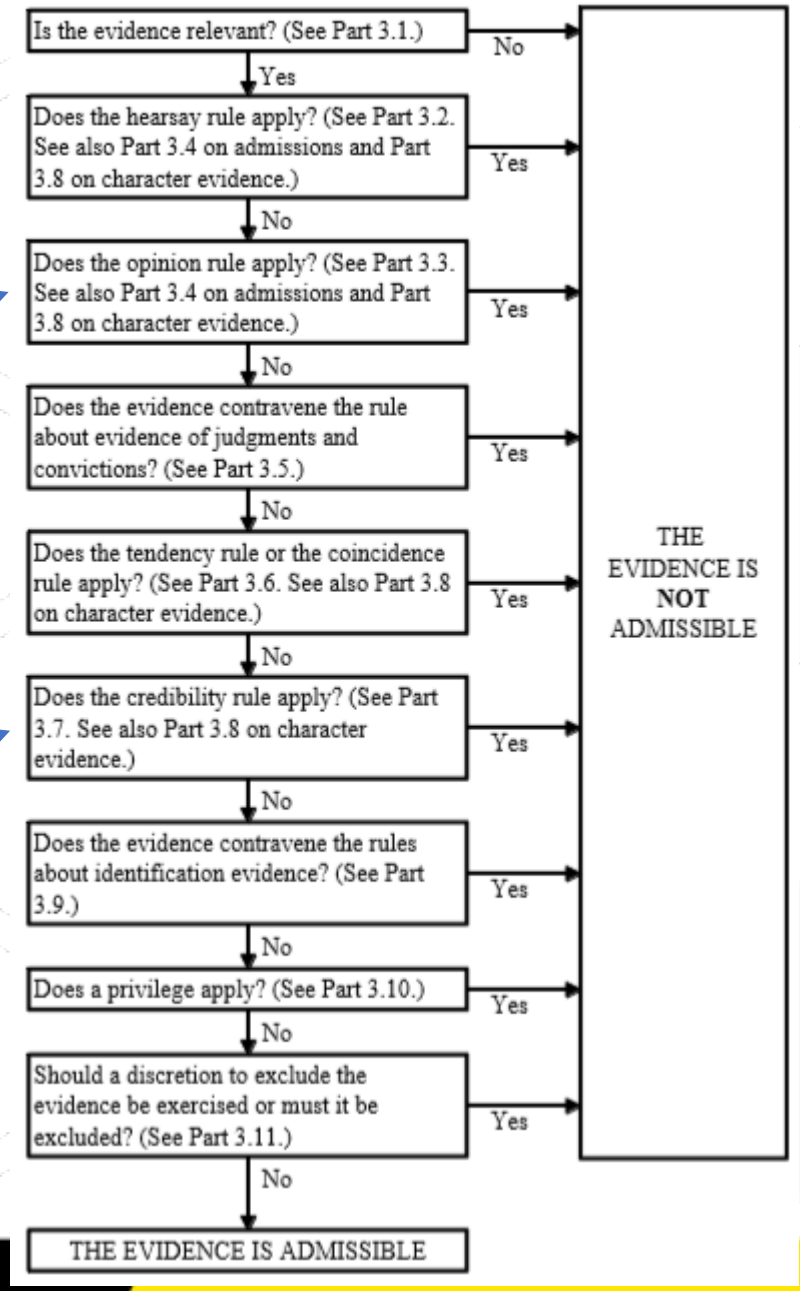
(often referred to as ”*the theatre of Court*”)

Evaluation of evidence

Evidence Act Part 3

Here is where “opinion” is tested

Here is where “legally obtained” is tested



Hearsay

- Hearsay generally excluded - Evidence Act §59
  - Referred to as an *asserted fact*
  - *A person has personal knowledge of the asserted fact if his or her knowledge of the fact was, or might reasonably be supposed to have been, based on something that the person saw, heard or otherwise perceived, other than a previous representation made by another person about the fact* (Evidence Act S62(2))

- Relevant exceptions
  - Business records (§ 69)
  - Tags and labels (§70)
  - Electronic communications (§71)

Opinion

- Evidence Act §76
  - *Evidence of an opinion is not admissible to prove the existence of a fact about the existence of which the opinion was expressed*
- *Expert opinion* is an exception
  - *If a person has specialised knowledge based on the person's training, study or experience, **the opinion rule does not apply** to evidence of an opinion of that person that is wholly or substantially based on that knowledge* (Evidence Act §79(1))

- Uniform Civil Procedure Rules (§31.18)
  - ***expert**, in relation to any issue, means a person who has such knowledge or experience of, or in connection with, that issue, or issues of the character of that issue, that his or her opinion on that issue would be admissible in evidence.*
  - ***expert witness** means an expert engaged or appointed for the purpose of:*

    (a) providing an expert's report for use as evidence in proceedings or proposed proceedings, or

    (b) giving opinion evidence in proceedings or proposed proceedings.

Evidence produced by processes, machines and other devices (S146)

(1) This section applies to a document or thing—

> *(a) that is produced wholly or partly by a device or process; and*
>
> *(b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.*

*(2) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (**unless evidence sufficient to raise doubt about the presumption is adduced**) that, in producing the document or thing on the occasion in question, the device or process produced that outcome.*

- Presumption that a document or thing produced by a machine/device is reliable
  - Onus is on person claiming it is unreliable
  - Example given is photocopier
  - Computer produced documents may fall into that category
- Only applies to the document…not the interpretation of the document
- Also S147…in the course of business i.e. *business records rule*

Meaning of document

document[1] 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.

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

- As an expert, you will be giving evidence to refute or support the presumption
  - Document was an *ordinarily produced outcome*?
  - The machine was *properly used*?
- When creating documents, you should consider the same
- **DISCUSSION** – what sorts of things should you do to establish the presumption? In other words to pre-empt the other sides arguments refuting reliability

R..R..S..P

RELEVANT

- Fact
- Opinion

Is it a piece of the right puzzle?

RELIABLE

- Evidence
- Witness

Are they the right pieces? …or a ring-in or a cheap knock-off

Do you have the skill and expertise to find the pieces and put them together?

SUFFICIENT

- Standard of proof
- Prove the right thing(s)

Are there enough pieces of the puzzle?

PERSUASIVE

- Understood by the decision-maker(s)
- Know the audience

Can you persuade a decision-maker that your thesis is the right one?

Relevant

- *…could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding*
  - Evidence Act §55

- Depends on the case and its circumstances. Includes:
  - Credibility of a witness
  - Admissibility of other evidence
  - Failure to adduce evidence

⇩

  - Decision-maker has broad discretion in deciding to admit evidence (or not), including provisionally admitting evidence

Reliable

- The witness
  - Appropriately qualified for the evidence they want to give?
  - Truthful and unbiased?
  - Compromised?

The adversary may go to some length to test this.

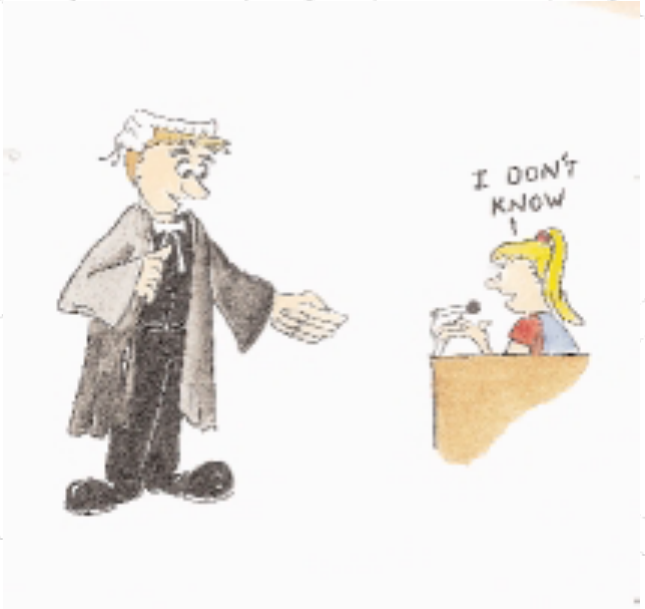
Advocacy 101 is:

1. Attack the evidence
2. Attack the process
3. Attack the witness

If they get to here, you should feel good because they are struggling with (1) and (2)

- The process
  - The administrative process
    - Lawfully acquired
    - Opportunity for spoilage or tampering ⇨ Chain of custody
  - The scientific process
    - Appropriate training and experience
    - Equipment calibrated and operating correctly
    - Predictable
    - Repeatable
    - Can quantify errors
    - Broad practice base i.e. used by peers, standardised
    - Supported by published research – avoid vendor ”research”

An increasingly common scenario



Barrister: So Mr Ghosh, are you in the habit of lying?
Mr Ghosh: No.

Barrister: Then how do you explain these....
PRODUCES POSTINGS FROM INTERNET (evidence regarding the credibility of a witness in relevant)

Although remember, just because someone publishes something it does not always mean it is so (including pictures and video)

There is also a lesson here in moderating your own behaviour – online and in the real world

Pip V. • 2nd
Contributing to Civic, Local Community & K-12 School Cyber Resiliency
17h • Edited

Your digital footprints and why you really need to keep your birthday and other identifying info safe. Especially your childrens!!!!
#security #K12 #education #privacy #community #cyber #resil ...see more

Frank Abagnale: Never do these 2 things because 'that's 98% of me stealing your identity'

finance.yahoo.com

2 · 2 Comments

Like Comment Share Top Comments

Add a comment...

[redacted] 9h ···

Hilariously every year I have several internet birthdays where I randomly get a few happy birthdays before people remember it wouldn't actually be my birthday because that's not in the

· 1 Like · 1 Reply

REFLECTION ACTIVITY - Are you truthful?

- Don’t wait for the adversary to find this – have your speech prepared

- Working in pairs (5 mins interview and 5 mins reflection)

- Interview
  1. Interview your partner
  2. **The questioner**: Ask questions to elicit their digital personas
  3. **The answerer**: Be co-operative in your answer
  4. Have they been truthful?

- Reflection
  1. **The questioner**: How would you go about demonstrating they have not been truthful?
  2. **The liar**: How would you explain the untruth(s)?

What does this mean for cloud services?

- Consider how you access cloud services when you use someone else's credentials or fake credentials or assumed credentials

- Is your access lawful?
  - which is different to complying with the service-provider's contract
  - consider this in the context of a search warrant or a controlled operation

1. Who can use Facebook

When people stand behind their opinions and actions, our community is safer and more accountable. For this reason, you must:

- Use the same name that you use in everyday life.
- Provide accurate information about yourself.
- Create only one account (your own) and use your timeline for personal purposes.
- Not share your password, give access to your Facebook account to others or transfer your account to anyone else (without our permission).

We try to make Facebook broadly available to everyone, but you cannot use Facebook if:

- You are under 13 years old (or the minimum legal age in your country to use our Products).
- You are a convicted sex offender.
- We've previously disabled your account for breaches of our Terms or Policies.
- You are prohibited from receiving our products, services or software under applicable laws.

https://www.facebook.com/terms.php

Sufficient

- "Sufficient" is subjective and depends on the fact you are trying to prove and the particular circumstances, bearing in mind the standard of proof
- Courts generally react badly to experts who cast doubt through "mere speculation" e.g.
  - A hacker could have done it
  - The machine mightn't have been working properly
- Often limited by time/budget
  - Say so in the limitations section or your report
- Consider having more than what is sufficient e.g.
  - If you are relying on a record that is an ordinarily produced outcome, are you able to demonstrate the machine was operating properly and being properly operated?
  - Can you produce the same outcome in a different way?
  - Is your thesis supported by your peers – present the supporting research

SOMETIMES YOU JUST HAVE TO RELY ON THE SNIPPET YOU HAVE, HOPE YOU ARE PERSUASIVE AND LET THE CIRCUMSTANCES FALL INTO PLACE

Persuasive

- Experts have to overcome somewhat sceptical decision-makers (see the 2001 Magistrate's Survey on next slide)

- Barristers and judges can be
  - Demanding, time-poor and somewhat direct
  - Limited understanding of technology (or think they know it all)

- Establishing transcripted obiter (judge's remarks in passing) is a great way to establish credibility for the next case, and the next case…

I was impressed with Mr Ghosh as a witness. He did not at all appear to be an advocate, but rather he gave the appearance throughout his evidence of being an objective expert with full mastery of the subject to be examined for the purpose of these proceedings. His evidence analysed in an objective and methodical way the facts and issues that led him to conclude that the alleged email of April 2005 was fabricated.

The making of a finding of fabrication requires very cogent evidence that satisfies the requisite standard, having regard to the seriousness of the allegations…

- Kelly v Australia and New Zealand Banking Group Limited 2014] NSWSC 426

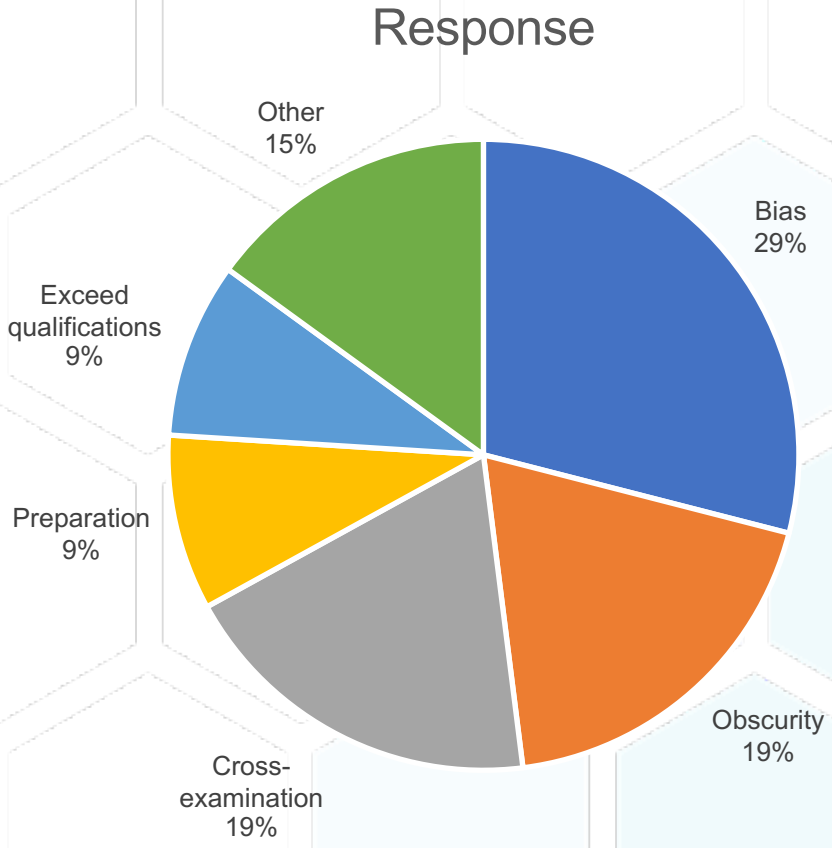
2001 Magistrate's Survey

Magistrates and judges were asked their experience of experts who gave evidence in their Court

Response	
Bias on the part of the expert	29%
Obscurity of the language of expert evidence	19%
Poor cross-examination of expert witnesses by advocates	19%
Poor preparation of the advocate	9%
Tendency of some experts to exceed their proved qualifications	9%

Life in the courts makes one sceptical and demanding about data. It teaches the need for scrutiny, even of apparently honest and well intended evidence, in the knowledge that honest and well intended witnesses can sometimes make serious mistakes with grave personal and economic consequences

– Justice Michael Kirby [1]



Expert's report (or certificate)

- Whilst there is no set format, Australian jurisdictions require the following[1]:
- Summary of expert's qualifications and experience;
- Statement that expert has understood and complied with their duty;
- Statement that expert has made all inquiries that they believe appropriate;
- Statement that opinion is provisional when available information is insufficient;
- Statement that opinion is qualified when available information is incomplete or inaccurate;
- Statement that a particular question or issue is outside the expert's expertise;
- Statement that opinion is genuinely held by the expert;
- Acknowledgement that opinions are based on the expert's specialised knowledge;
- Communications with parties;
- NSW and SA require disclosure of certain fee details e.g. contingent or deferred;
- Report to be signed by the expert.
- Note: SA requires expert's to retain a copy of all drafts of their report(s) communicated with any party

Rules for expert's set out according to jurisdiction

Jurisdiction and evidence law	Evidence Act	Civil Procedure Rules relating to expert evidence	Expert Witness Code of Conduct
Supreme Court of the ACT [ACTSC]	Uniform Evidence Act Evidence Act 2011 (ACT)	ACTSC Procedures Rules 2006 Part 2.12 Expert Evidence Rules 1200—1246	Schedule 1 Expert Witness Code of Conduct
Federal Court of Australia [FCA]	Uniform Evidence Act Evidence Act 1995 (Cth)	FCA Rules 2011 Rule 5.04 and Part 23 Experts RR 23.01—23.15	Practice Note CM7 Expert Witnesses in proceedings in the Federal Court of Australia
Supreme Court of NSW [NSWSC]	Uniform Evidence Act Evidence Act 1995 (NSW)	Uniform Civil Procedure Rules 2005 (NSW) Rules 31.17—31.54	Schedule 7 Expert Witness Code of Conduct
Supreme Court of the NT [NTSC]	Uniform Evidence Act Evidence Act 2011 (NT)	NTSC Rules Order 44 Expert Evidence	N/A
Supreme Court of Queensland [QSC]	Common law Evidence Act 1977 (Qld)	Uniform Civil Procedure Rules 1999 (Qld) Ch 11, Part 5, Division 2 Rules 423—429S	N/A
Supreme Court of SA[SASC]	Common law Evidence Act 1929 (SA)	SASC Civil Rules 2006 Rules 160, 161	Part I Practice Direction 5.4 Expert Witnesses (Rule 160)
Supreme Court of Tasmania [TSC]	Uniform Evidence Act Evidence Act 2001 (Tas)	TSC Rules 2000 Part 19 Division 5 Expert Opinion Evidence Rules 514—517	N/A
Supreme Court of Victoria [VSC]	Uniform Evidence Act Evidence Act 2008 (Vic)	VSC Rules 2005 Order 44 Expert Evidence Rules 44.01—44.06	Form 44A Expert Witness Code of Conduct
Supreme Court of WA (WASC)	Common law Evidence Act 1906 (WA)	Rules of WASC 1971 Order 36A Expert Evidence Rules 1—9	N/A

A format I have found useful

TABLE OF CONTENTS	
PRELIMINARIES	• You • Address if required • Qualifications and expertise
INSTRUCTIONS & SCOPE	• Communications with instruction solicitor • Specific questions you have been asked to answer - and your understanding of them • Scope of your report, if not apparent from the questions
SUMMARY	• If required i.e. report is lengthy
MAIN BODY	• A section for each question • Use sub-sections if needed
DECLARATION	• Required form of wording for declaration • Limitations and qualifications if needed
SIGNATURE	• Only sign final report • Watermark drafts
LIST OF ATTACHMENTS	• Items at "marked and attached" (not annexed)

DON'T WORRY IF YOU CAN'T READ THIS
A template is in the reading

Some tips on style and wording

DO

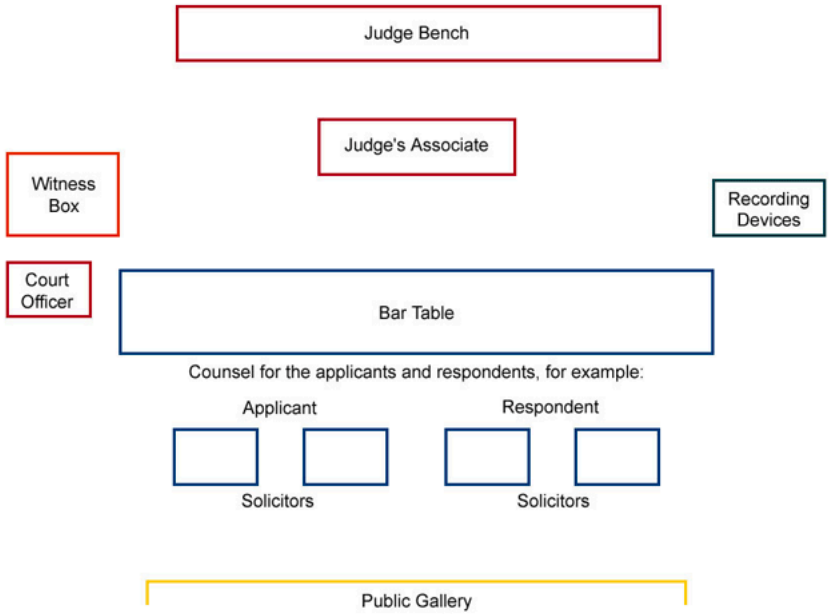
- Be clear about what is fact and what is opinion
- Write clearly, simply and in the first person
  - If you are supervising or working in a team, be clear about who did what
- Write step-by-step and chronologically
  - Consistently with contemporaneous note
- Write using logic and critical reasoning
  - Decompose, answer each bit, synthesise your thesis
  - Lead the reader on a journey of understanding
- Justify, justify, justify
  - Why did I choose that method, tool, etc

DON'T

- Use jargon or complicated explanations
  - If you can't explain it simply, you haven't mastered the subject well enough
- Skip over steps and arrive at a conclusion
  - Someone in a Jury may know more about something than you expect e.g. retired maths professor when presenting encryption
- Be argumentative or attack the other expert(s)
  - Lay out your argument on its merits
- Insist that you are right
  - "I don't know" should be used more often
  - "I was wrong and now I believe…because…" can be used re-state a position

In the Courtroom

- Let’s spend some time discussing Courtroom etiquette and theatre



Expert's given some privileges

- Not expected to know the rules
  - Advised by instructing Counsel
  - Knowing the rules adds to your credibility
- Allowed to stay in Court and listen to other evidence
- Allowed to advise Counsel
  - Except when under examination
- Allowed to address the Court (thru judge)
  - Includes pre-trial and access to documents
- Some of Court's privileges are extended e.g. copyright exemption
  - Use with discretion and ONLY for the Court purposes (may not include your own pre-trial examinations)

Privilege comes with responsibility

- Confidentiality
- Responsibility to the Court
  - Not the engaging party
  - Consistent with purpose
    - *just resolution of disputes according to law as quickly, inexpensively and efficiently as possible* – FCA Central Practice Note
  - Comply with Orders, including standing orders e.g.
    - Time to file documents
    - Retaining documents/material
    - Reporting of illegal conduct e.g. perjury (be aware of rules regarding self-incrimination and privilege), tax avoidance
- Respect privileges – Part 3.10 of Evidence Act
- Limited to instructions
- Court's look dimly on expert's who refuse instructions or refuse to be examined
  - Limited reasons e.g. conflict
  - Fee is limited to "taxation" e.g. $475/hr in NSW – can charge more, but opposing party only has to pay at taxation rate
- ACT is only jurisdiction that offers "immunity" to testifying experts

Short break – 10 mins

And then Week 2b:

- Windows forensics #2