48436/32309

Tutorial Week 10 Law Report

Name: Huynh Lam Student ID: 13264763 Date: 17/10/2021 Activity No.: Cmp1/03

Reading	Questions
Week 10 Reading document **1) Evidence ACPO.pdf** **2) Forensic Legal issues.pdf**	Examine the documents below in this week's readings and answer the questions provided. **1) Evidence ACPO.pdf** What are the four 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 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. • 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. Give examples of how to enforce these principles What items of information should be recovered using a scripted approach (running a set of command line tools via a script)? • process listings. • service listings. • system information. • logged on & registered users. • network information including listening ports, open ports, closing ports. • ARP (address resolution protocol) cache • auto-start information. • registry information. • a binary dump of memory What is the difference between the examination process and the analysis phase? • The examination process is to make evidence visible and explain it's original and significance. First, it should document the content and state of evidence in totality. Documentation allows all parties to discover what is contained in evidence. Finding hidden and obscured data is also part of the process. Once all the information is visible the process of data reduction

3) Exclusionary rule	begins. Finally filtering out what evidence would prove useful for the investigation. • This phase differs from examination in that it looks at the product of the examination for its significance and probative value to the case. The examination is a technical review that is the province of the forensic practitioner.
	2) Forensic Legal issues.pdf **Jurisdiction of case.** Does a Texas Court have the right to assert its jurisdiction over a British Columbian resident? • The Texas Court had no right to assert its jurisdiction over a British Columbian resident
4) D F-issues-in-civil-proceedings.pdf	**Search and seizure of digital evidence** Explain how the forensic investigator needs to consider the privacy of a culprit in any search. • During the initial process of forensic investigation, the use of an improper methodology or unlawful search and seizure can negatively affect the admissibility of the evidence. The forensic investigator must therefore ensure that the privacy of a culprit is not infringed in any search. The legal procedure for searching and seizing computers with a warrant largely mirrors the legal framework for other forensic investigations. How can you detect when a plaintiff fabricates an email by pasting a legitimate header and altering the Subject line? • To find if the emails have been fabricated, you need to look at the email header. The header contains critical components of every email: From, To, Date, and Subject, as well as detailed information about where the email came from and how it was routed to you. Importantly, it also contains the results of the verification process your email provider used to determine if the sending server has permission to send using that domain.
	3) Exclusionary rule Explain the Fruit of the Poisoned Tree' principle used to exclude certain evidence. • In strict cases, when an illegal action is used by police/prosecution to gain any incriminating result, all evidence whose recovery stemmed from the illegal action.

	Now the evidence acquired illegally can be thrown out from a jury An illegal (not done properly) step in an investigation may void all following evidence. How can you minimise this? • The team that is doing the investigation should follow the regulations and guidelines when submitting and obtaining evidence. As investigators are quite good at their jobs and assumptions made tend to be quite correct they will need to obtain evidence legally. By obtaining warrants and proper consent to recording they are able to achieve obtaining evidence legally. A person may track their spouse's activity to gain evidence for divorce proceedings. Name two activities that would be of interest and the type of malware used to gain the evidence. • (GPS) tracking information and malware would be spyware • Text messages and the malware of interest would be keylogging How would the tracked person suspect such a tracker was being used? • The person being tracked could potentially take it to a digital forensic officer and they can perform their analysis such as memory analysis to find hidden programs silently running in the background. There could be a hint of spying as unusual programs installed or browser history/file history being accessed without the primary user opening these applications. How could the victim's attorney gain corroborating evidence of this tracking activity? • The person could look into the person tracking information such as monitoring site's logs or user records to show use by the perpetrator, or the credit card history to show the purchase of the monitoring application. • This may include remotely activating web cameras that are built into computers and mobile devices. Some cameras have an activation light, which indicates when a camera is being used. • The device that is suspected to have tracking activity can be presented to a digital forensic officer where that person can perform malware analysis on the device.