MURDOCH UNIVERSITY

ICT378 Cyber Forensics

Assignment Information

You should **submit your assignment online using the Assignment course tool**.

Late submissions will be penalised at the rate of 10 marks per day late or part thereof.

You should submit your assignment as ONE word-processed document containing **all** of the required question answers.

You **must** keep a copy of the final version of your assignment as submitted and be prepared to provide it on request.

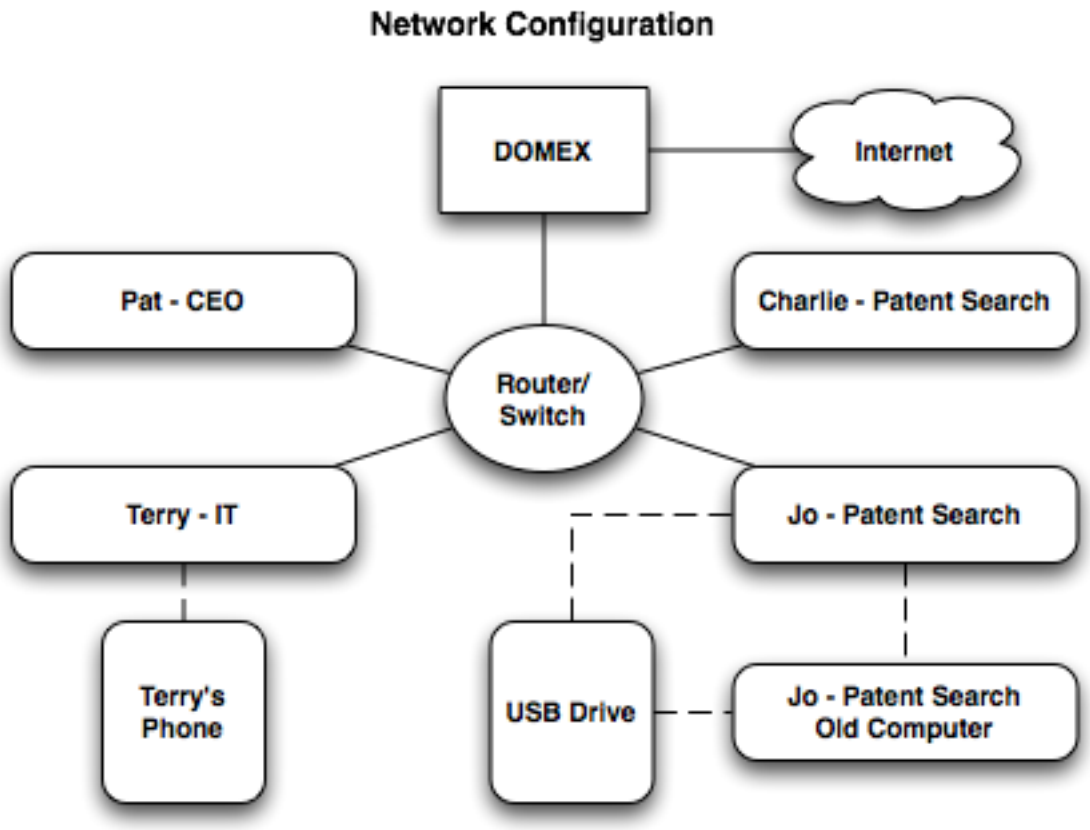
The University treats plagiarism, collusion, theft of other students' work and other forms of dishonesty in assessment seriously. This is an INDIVIDUAL assignment. For guidelines on honesty in assessment including avoiding plagiarism, see: http://www.murdoch.edu.au/teach/plagiarism

M57 Patents

Founded by Pat McGoo, m57.biz is a new patent search company that researches patent information for their clients.

Specifically, the business of patent search is to generally verify the novelty of a patent (before the patent is granted), or to invalidate an existing patent by finding prior art (proof that the idea existed before the patent). At the start of the scenario, the firm has four employees: CEO (Pat McGoo), IT Administrator (Terry), and two patent researchers (Jo, Charlie). The firm is planning to hire additional employees at a later date once further clients are booked. Since the company is looking to hire additional employees, they have an abundant amount of technology in the inventory that is not being used.

Employees work onsite, and conduct most business exchanges over email. All of the employees work in Windows environments, although each employee prefers different software (e.g. Outlook vs. Thunderbird).



The Case: Illegal materials - Methamphetamine

• A functioning workstation originally belonging to m57.biz was purchased on the secondhand market. The buyer (Aaron Greene) realizes that the previous owner of the computer had not erased the drive, and finds suspicious documents and videos on it, related to drug use, specifically Methamphetamine. This drug is a very real problem in Australia and Singapore. Aaron reports this to the police, who take possession of the computer.

• Police forensics investigators determine the following:
    • The computer originally belonged to m57.biz
    • The computer was used by Jo, an M57 employee, as a work machine.
• Police contact Pat McGoo (the CEO). Pat authorizes imaging of all other computer equipment onsite at

M57 to support additional investigation. Police further pursue a warrant to seize a personal thumb drive belonging to Jo.

You are given disk images from all of the computers and USB devices found onsite at M57. Additionally you are given two more images, clearly in a different format, which are supposed to be of the same computers. The first images were given in *expert witness* data format (used by EnCase software) – E01 extensions. The second images have the extension AD1..AD*n*. There does seem to be an issue with the logging of evidence, and it is even brought to your attention in passing that a police staff member is suspected of negligence or even “foul-play” - but that has yet to be determined.

The Materials: Drive images

The materials you will use for your investigations are:

- Hard drive image 2009-11-19.E01 (of the original sold computer) – E01
- Second drive image purporting to be of the same computer – AD1, AD2
- Hard drive image 2009-12-01.E01 (of the suspect's replacement computer seized from M57) – E01
- Second drive image purporting to be of the same computer – AD1, AD2, AD3

To submit: Forensic report

Given the above suspicion and seized data files, it is your role as investigator to uncover any evidence to prove or disprove the allegations – of drug involvement - but also of evidence tampering. The brief above has highlighted what in particular you are looking for, so the scope of the investigation is limited to this particular suspected crime.

Your report should follow the structure detailed in Chapter 14 of the textbook, there is no limitation on size of the report although you are urged to state the facts clearly and not bury them in pages of irrelevant content.

Your report should highlight the following areas (these will be assessed):

a) Discuss if there is there any evidence of illegal drug activity (Methamphetamine). Explain your position on this. What evidence did you find if any? How sound / reliable do you believe your evidence collection to be? **[20 marks]**

b) Present any evidence in a time line format, signposting the points where you believe any offence may have occurred and other significant dates/times in the case. Compare any evidence found and timeline information side by side with the different tools available to you (e.g. ProDiscover/ OSFOrensics/ FTK Imager) and highlight any differences. Be sure to state the pros and cons of using one tool over the other. **[20 marks]**

c) You were provided with two sets hard drive images. Are there any differences between them, considering they are purported to be of the same computers. What do you think has occurred here? What are the differences between the sets of the drive images? Which images do you think are the originals and why? How do you think the sets of drive images were created? **[20 marks]**

d) A common defence is that the actions were committed unintentionally or that the perpetrator did not know the actions were illegal. With these possible defences in mind, address how you would respond to these defences. Are there any clues that indicate intent or knowledge of criminal activity? **[20 marks]**

e) Conduct some research into ways that image files could be "tampered with". Are there ways that are undetectable, or difficult to detect? Present your findings in a short section – written in a formal referenced style. You are only expected to have approximately 5 references (good quality: reputable journal or conference papers). **[20 marks]**