SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Tutorial questions for Lecture 10: Computer Forensics

QUESTION 1

a) Identify the four main steps in the Computer Forensics process.
b) Discuss the types of activities that take place in each step.

QUESTION 2

Hiding data on a standard computer hard disk can be done in a large number of ways. These range in complexity from:

- Very simple (for example, formatting the font in a document to be the same colour as the background), to
- Technically difficult (for example, writing directly to a disk in areas not able to be accessed by the operating system).

Use the lecture notes and online search to identify a range of data hiding techniques. For each technique you identify:

a) Discuss the complexity of the technique (what skills do you need to be able to do this?)
b) Identify any tools that may be required to use this technique to hide data.

QUESTION 3

The MD5 and SHA1 hash functions are used extensively in computer forensics to create check sums.

a) What are some of the purposes for using check sums in a computer forensic investigation?
b) Which properties of hash functions are important for these purposes?

QUESTION 4

The legal case of Sony versus University of Tasmania was one of the first computer forensic cases in Australia. The attached PDF (see the separate file) includes some discussion of the difficulties in the case – up to page 8.
2003 *Sony Music Entertainment (Australia) Ltd v University of Tasmania* - Federal Court decision on discovery application by record companies against three universities for alleged use of the universities' computer networks for reproduction and communication of MP3 files, infringing copyright in music and sound recordings.

The companies sought access to university records to identify alleged infringers and to determine whether there are grounds to seek relief for infringement. The universities resisted on a number of grounds that included privacy. The Federal

Court agreed to grant the orders on certain conditions, primarily regarding preservation of confidentiality and privilege.

Sony wanted full access to the disks where the MP3 files were stored. The University of Tasmania only wanted to provide file listings able to be viewed from the operating system level.

a) Why would Sony need access to the disks?
b) What loss of confidentiality could occur if this was granted?

QUESTION 5

With respect to computer disk systems,

a) What is the difference between a sector and a cluster?
b) What is slack space?
c) Why is slack space important in a computer forensic investigation? What useful information might be found there?