SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1, 2014

Outline solutions for 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.

CF Process and Steps

1. **Identify – before a “raid” determine what is likely to be present at the scene and how much time it is likely to take. At the scene, physically search for relevant devices, storage devices etc that need to be copied. Take still photos and video footage to cover chain of custody issues**
2. **Secure – copy data from the identified devices. Copies must be bit streams from the devices preserving the partition tables and file systems. Hash values must be calculated as data is copied to ensure accurate copying. Write blockers must be used to prevent the original data from being altered in any way.**
3. **Analyse – find data relevant to the case that helps to prove or disprove the case. Keyword searching, browsing files, looking for deleted and/or hidden data, building a timeline of events from email, web browsing, chat sessions, file usage etc.**
4. **Report – Prepare report on the case. Must be relevant to the case, must be understandable by non-technical people (judge and jury), must outline the process undertaken in the analysis stage so that findings can be replicated if necessary**

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.

Technique	**Ability Required**	**Tools Required**
Change file extension	Basic file handling	File browser or command line
Embedding a file in another	File handling	Editor capable of copying one file's contents into another file
Changing magic numbers in file headers	Knowledge of file header magic numbers e.g. JFIF in .jpg files	Hex or text editor
Placing data into sector and cluster slack	Knowledge of file systems	Hex editor capable of writing to disk
Placing data into inter-partition gaps	Knowledge of disk systems	Hex editor capable of writing to disk
Steganography	Basic knowledge of technique	Specialist tools are available from the Internet
Encryption	Basic knowledge of encryption	Encryption tools are readily available
Change font colour to background colour	Basic knowledge of using documents	Any document editing tools (Office, OpenOffice etc)

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?

Hash values (also called checksums) are used:

- **during the copying of a disk or device to ensure a true and accurate record of the device has been captured**
- **within analysis tool suites**
    - **all files located are hashed**
    - **hash values can be compared to database of known file hash values for**
        - **exclusion – operating system files, applications etc**
        - **inclusion – known illegal files**
- **any time any portion of a disk/device is extracted from the main image to show that portions have not been altered during investigative processes**

QUESTION 4

The legal case of Sony versus University of Tasmania was one of the first computer forensic cases in Australia. The attached PDF 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 were the MP3 files were stored. 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?

In summary, Sony wanted full access to the disk systems to see what was there. They were fishing for proof. Full access would allow analysis of the file system and for detection of deleted files if the relevant sectors had not been overwritten.

However, the file system did not just contain illegal MP3 files. University of Tasmania documents were also on the file system. UTas argued there was no need for anyone to have access to those files. They were concerned about the loss of confidentiality of University files which were completely unrelated to the music file sharing.

One concern regarding UTas' provision of file listings is that it would not have included any metadata about file creation and accessed times or the actual contents of the files.

The outcome was somewhere in between (read the relevant pdf!).

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 may be found there?

a) Difference between a sector and a cluster:

- **A sector is a basic unit of storage on a disk. Typically 512 bytes.**

- **A cluster is a group of sectors – 1, 2, 4, 8, 16 up to 64 – and is the minimum amount that can be read/written in one read/write**

operation. Cluster size is a function of disk size and partitioning. Larger disks have larger cluster sizes.

b) **The operation of writing to a cluster can result in wasted space, especially for small files or for files which when broken into clusters only occupy a small amount of the final cluster. The left over space is the slack space. Unless a file fills a sector exactly there will be sector slack (some portion of the last sector will contain what was there before) and cluster slack (not all clusters will be filled – so again, what was there before will still be accessible to analysis tools).**

c) **Slack space can be searched for keywords relevant to an investigation, resulting in partial recovery of file contents.**