Hidden Files—A Computer Forensics Case Study

Question Paper

1. Outline the meaning of the following terms:

(a) cookie, [2 marks]

A cookie is data stored locally that is used by some websites for data that needs to be kept between sessions, for example, remembering the details of the active user.

2

(b) slack file space. [2 marks]

Slack file space occurs when a file is smaller than the total size of the clusters allocated to it. Slack file space is the space between the end of the data of the file and the next cluster.

2

2. Companies who recycle their computers by selling them on to someone else will aim to erase all data on their hard drive. However, this may not always be successful.

(a) Outline how formatting the disk may not in fact achieve this aim [4 marks]

A file is stored on a hard drive as both the information contained within the file, but also any meta-information about the file such as creation times and the location of the contents of the file on the disk. [Kept in the root directory and FAT] Normally, when deleting a file the space occupied by the contents are marked as available and so will be overwritten when needed. [Explanation] When a disk is formatted the exact process will depend on the tool used. [This needed a little more detail. Normal formatting (e.g. under Windows or DOS) would erase the data in the root directory and FAT. A "forensic wipe", however, will typically write a series of identical characters (e.g. zeros) to every sector]. It is likely that only the reference to the file will be removed, similar to deleting, and so the contents of the file will still remain. [To gain the 4th mark the student needs to differentiate between the different types of formatting (his reference to the "tool" used) as the choice of formatting would lead to different results].

3

(b) Outline the possible effects on privacy if all of the data is **not** erased. [4 marks]

It is likely that the user of a computer will have recorded sensitive company information, such as client details, marketing strategies etc. If this data is not fully erased then it may be available to the new owners of the hard drive. Privacy is generally assumed to be a right and so the loss of privacy by unintentional revealing of data is an ethical issue. [Not adding value to answer] If client information is passed to another company for example, the new company could have access to information that could compromise the client, such as health records or legal records.

4

3. In the training exercise, John focused on securing the hard drive of the suspect's computer.

Explain why other file evidence may have been missed in concentrating solely on the hard drive. [6 marks]

The data contained in a computer does not entirely reside on the hard drive as the main memory of the computer (RAM) also contains temporary data. If the hard drive is taken as the focus of the investigation then any evidence that is stored in the RAM would be lost when the system is powered down. The programs currently open may prove to be relevant to the investigation as may any data contained in any open programs. This information is likely only stored in the memory of the computer and so by focusing on the hard disk alone evidence could be missed. [The answer is correct, but care must be taken not to alter any important evidence such as time stamps when interacting with the computer]

If the user of the system had taken anti-forensic countermeasures such as encrypting the data on the hard drive then concentrating solely on the hard disk would result in the loss of any data usable as evidence. If the hard drive is encrypted then the key to decrypt it may only be stored in RAM and so would be lost by not investigating the contents of the system memory. The surrounding area may contain flash drives or optical media that could also contain encryption keys. If these sources of data were not investigated then evidence could also be missed in the form of files or data stored within. [The answer is correct, but care must be taken not to alter any important evidence such as time stamps when interacting with the computer].

The hard drive is the most logical place to find evidence and so if the user had taken basic anti-forensic measures then any data on the hard drive might be hidden and so searching for files might be more time consuming and searching the memory and surrounding area might produce any incriminating (or exonerating) evidence more easily.

The response demonstrates a very good level of understanding and develops a number of ideas thoroughly. The length of the response (267 words) is appropriate.

6

4. Discuss the methods used by criminals to hide or disguise certain files. For each method identify the countermeasures that can be taken by a computer forensic scientist. [12 marks]

If a criminal is aware of computer forensics and the techniques used they may attempt to make some effort to hide or disguise their incriminating activities or data. In order to locate these activities further efforts must be made.

From independent research based on Anti-Forensics and the schools visit to Dr McBride at De Montfort University [evidence of research], one possible way of hiding incriminating information is to encrypt the data on the hard drive, either encrypting individual files or the whole hard drive. This makes the contents of the file unreadable without the encryption key however this may be seen as preventing access rather than hiding data and may draw attention to it. [Off course, no value added to the response]

From research on Forensics Wiki, [research – URL not required, information goes beyond the case study so is considered research] Steganography **[M1]** is the act of hiding information or files inside other innocent appearing files, such as hiding a text file within an image. Images usually contain information about the image itself such as the camera that took the photo, this space can be used to store unconnected data, such as a text file. As long as the hidden file is stored in plain text than a string based search for keywords relevant to the investigation should find the information. If the information is, however, encrypted then finding it is made much more difficult. It may also be possible to search for irregularities in files that show the use of common steganographic software **[CM1]** such as large amounts of redundant data which are not related to the image and could be encrypted information, for example 'stegdetect' looks for common signatures of steganographic programs. [Excellent knowledge based on research going well beyond the information in the case study]

Changing the file extension **[M2]** may also help to hide files, as they will be hidden from a simple search for files of a particular type. For example, in the case study, a search for images could be stopped by changing the extension of any incriminating images, for example, a jpg file to a doc file. A suitable countermeasure for this would be to instead search for images by the contents of the file **[CM2]**. As file types usually have a standard header identifying them as images a search can be conducted for this header which would be a more reliable way of locating images but also more time consuming.

Also, renaming files **[M3]** can obscure the contents by making it harder to find files relevant to the investigation, such as giving relevant files innocent names so the contents are not suspected to contain any information relevant to the case. A countermeasure **[CM3]** to this is to not focus on the names of files but instead focus on the contents by using searches designed to find keywords relevant to the investigation regardless of their placement on the hard drive.

There are many way that criminals can use to hide any incriminating evidence however most can be easily defeated by searching for expected strings across the entire hard drive. [Good summary] Information on Anti-Forensics and the schools visit to Dr McBride at De Montfort University showed how this would find most information regardless of how it is disguised with different file names or extensions. [Conclusion linked to analysis and research] If, however, encryption is used then the encryption key must be found through other means in order to get at any contained data. There are simple countermeasures to the basic methods of hiding or disguising files and in most cases it is not likely that encryption would be used. Even in the cases where it was it is quite likely that evidence could be found elsewhere in activity logs which would be unnoticed and left unencrypted.

A very thorough and well researched response that addresses three measures and countermeasures in appropriate depth. The final paragraph ties the response together and provides a suitable conclusion. The response clearly extends beyond the information in the case study and provides clear evidence that extensive research has been undertaken.

There is a slight confusion within the response about encryption and that it does not hide or disguise files, merely makes them more difficult to access, but the candidate would have scored full marks without it, so does not self penalize by going off course.

12

Sources – for information only

http://archive.cabinetoffice.gov.uk/e-government/resources/handbook/html/4-7.asp

- In depth look at cookies, provides too much detail but introduction gives a good summary of cookies and discusses privacy.

http://www.anti-forensics.com/

- Provides the opposite point of view and is useful for showing some of the techniques used to defeat computer forensics.

http://en.wikipedia.org/wiki/Computer_forensics#The_Forensic_Process

- Not reliable as it's from Wikipedia but gives an overview of the forensic process and helps to understand how an investigation unfolds.

http://www.forensicswiki.org/wiki/Main_Page

- Mostly useful for finding the meaning of keywords, didn't provide as much information about the forensic process.

http://www.daemon.be/maarten/forensics.html

- Provides information about the forensic process but also gives specific examples of techniques used.

http://www.outguess.org/detection.php

- A program used to detect steganographic information in image files