SPEC/4/COMSC/HP3/ENG/TZ0/XX/CS

International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

COMPUTER SCIENCE
CASE STUDY: HIDDEN FILES – COMPUTER FORENSICS

SPECIMEN PAPER

INSTRUCTIONS TO CANDIDATES

- Case study booklet required for higher level paper 3.

4 pages

Introduction

Computer forensics is a branch of computer security which specializes in the analysis of computer systems, in order to provide evidence of computer misuse or attacks on computers.

The ordinary desk top computer stores a considerable amount of data that was never consciously put there by its user. This can range from cookies, to print and email logs and browsing history. These will be stored in files (some hidden) which can be reasonably easily accessed. However, it can also preserve data that has supposedly been deleted or even previous versions of files which have subsequently been updated. The fact that data should be so resistant to deletion should concern not only the cyber-criminal but also businesses and individuals who wish to permanently delete data or recycle their computers. Users should be aware that only a "forensic wipe" will effectively erase all data on their hard drives.

The rest of the case study investigates the work of John Martin, a fictitious computer forensic scientist.

Your Secrets Revealed Inc.

John Martin is employed by the computer security company *Your Secrets Revealed Inc*. This company has two divisions: one which acts as security consultants to advise on computer security systems, and one which specializes in computer forensics. John is employed in the forensics division, and although he was already an experienced computer user, he had to undergo extensive training both in the techniques and the software tools used to locate and identify incriminating evidence, and in procedures that had to be rigorously followed in order that evidence might be accepted in court.

One training exercise involved investigating the following scenario:

"The home of a person suspected of organizing the illegal distribution of drugs was raided and the suspect apprehended. The suspect's PC, which was still switched on, was equipped with both an internet connection and a web cam. The information that led to the house being raided had come about from the interception of a telephone call which had made reference to certain names associated with the illegal drug trade."

John's task was to search the computer system and the surrounding area for electronic information that might incriminate the suspect. He was provided with various tools supplied by the company. His tasks included securing and evaluating the scene, conducting preliminary interviews, documenting the incident, collecting the evidence and packaging and transporting the evidence. His first action was to turn all equipment off and then carefully remove the computer's hard drive ready for transport to the company's laboratories.

John has since been involved in various investigations including:

- employee Internet abuse
- criminal fraud
- industrial espionage
- unauthorized disclosure
- child pornography
- identity fraud.

The industrial espionage case was of particular interest as the company was convinced that a rival firm had stolen their ideas, but had no concrete evidence that would show this. The company's main server was subsequently analysed by *Your Secrets Revealed Inc*. who found that "back-door" remote access had been installed. Further to this the forensics team discovered keystroke loggers had been installed which could relay data entered into the system via the Internet to a third party. The third party was identified and found to indeed be one of their rivals who were trying to steal intellectual property from the company.

The company *Your Secrets Revealed Inc*. was then contracted to update their security system, particularly with respect to preventing unauthorized outside access.

John's current investigation involves the search for illegal images on a computer. The suspect's computer was found switched off. Also, no network hardware was found in the house. A typical hard disk can contain thousands of files so after taking an exact copy of the suspect hard disk, John's first task was to filter out all known files (on the copy) using a hash analysis. It is essential not to manipulate the original disk in any way.

Files with the usual image extensions were located using the computer's file manager in the normal way (the operating system was found to be Windows XP), but no incriminating evidence was found.

As the files that he was looking for did not immediately appear, a more complicated analysis would now have to be made which would involve searching for files that had been disguised in some way. Criminals will often attempt to hide files. A further step that might reveal evidence would be to investigate both unallocated space and slack space that is present on the disk.

Challenges Faced

John and his team must focus on the following challenges:

- To ensure that they follow all the correct procedures so that any evidence discovered would be admissible in subsequent legal proceedings.

- To discover all relevant files on a computer system that the user may have attempted to delete.

- To discover all relevant files on a computer system that the user may have attempted to hide or disguise in some way.

Additional Terminology to the Guide

Back-door access
Bit-stream image
Cluster
Cookies
FAT
File signature
Forensic wipe
Hash analysis
Hidden files
Intellectual property
Logical analysis
Keyboard loggers
MAC times
Message digest (Hash)
Metadata
Mirror image
Physical analysis
Root directory
Slack file space
Write blocker

Companies, products, or individuals named in this case study are fictitious and any similarities with actual entities are purely coincidental.