CSN10102 Assessment Specification

Details

Module name:	Advanced Security and Digital Forensics
Module number:	CSN10102
Session:	Semester 2, 2011
Weighting:	50%
Submission:	Week 13

Coursework Assignment

Title:	Investigation of Criminal Peer-to-Peer Sharing

Outline Requirements

A company (MyComp) has had a security breach where it is alleged that there has been illegal file sharing on the corporate server. The company has managed to get a virtual image of the computer, which contains traces of evidence that could be used for the investigation (this includes both host activity on the system and network traces). It is thus your objective to investigate the virtual image, and produce a fair and unbiased report on the findings. The VM image exists on with the Napier Cloud at http://lm2003.napier.ac.uk, which also contacts the network trace, which can also be downloaded from:

http://www.dcs.napier.ac.uk/~bill/cw_capture.rar

The analysis should involve analysing the network trace for the connections from the hosts which connected to the host-under-suspicion (HUS). Along with this you should analyse and cross-correlate the activity within the logs on the HUS, and the trace of files left on the system. Evidence should also be gained from the applications which were used within the time window of interest. Please note that all other activity outside this window-of-interest should be ignored.

Marking schedule

The coursework should be submitted via Web-CT, in a PDF format, if possible. It will be marked as follows:

- **Investigation Procedure** [20%]. This should outline your procedures for analysing the virtual image.
- **Findings** [45%]. This should outline the trail of evidence produced, and the findings from it.
- **Conclusions** [20%]. This should reflect the methods you have used in the report, and to assess their strengths and weaknesses, and any observations that you have gained.
- **References/Presentation** [15%]. All references must be defined in an APA/Harvard format, and should be integrated in the report.

The report should use the APA/Harvard format for all of the references, and, if possible, should include EVERY reference to material sourced from other places. Also, the report should be up to 15 pages long (where appendices do not count in the page count number).