The Chartered Society of Forensic Sciences

Component Standard

Digital Evidence Analysis, Recovery & Preservation

Purpose

To equip students with an understanding of the theory and application of analytical methods commonly used in digital evidence examination, recovery & preservation and to equip them to provide justified interpretation of the results of analysis.

General Outcomes

Students should be equipped to identify and recover a range of digital devices from typical crime scenes appropriate to the course. They should also be able to produce “forensically sound” copies of stored data using appropriate tools and techniques.

The course should be designed to enable the student to:

1. describe common digital architectures;
2. describe typical device physical and logical characteristics;
3. demonstrate detailed understanding of relevant storage devices, their operation and interfaces;
4. demonstrate detailed understanding of data storage formats (file systems, file formats *etc*.);
5. demonstrate detailed understanding of appropriate operating system and application software behaviours, including user controlled behaviours;
6. understand and demonstrate evaluation and selection of toolsets for data recovery and analysis (*e.g*. data carving, regular expression searches, scripting *etc*.);
7. demonstrate understanding of methods employed by others which are likely to have an adverse impact on the ability analyse & interpret recovered data;
8. understand digital device imaging techniques and tools, including best practice;
9. identify typical and atypical digital devices;
10. identify and describe device functions;
11. demonstrate safe handling of relevant digital devices in the context of seizure and storage;
12. demonstrate identification and handling of devices with live communications channels;
13. demonstrate methods to avoid or minimise alterations to data held on digital devices;

Agreed – June 2011

14. demonstrate awareness of laws affecting device seizure and imaging, data recovery and analysis.