Data Demystifier 1

ONLINE INSTRUCTOR-LED COURSE

TURN DATA INTO EVIDENCE

Digital forensic software tools extract data from devices and present that data on screen for analysis, typically by means of a simple point-and-click interface. Such tools provide great benefits in simplifying both the acquisition and analysis phases of a mobile device examination, thereby allowing more devices to be processed in less time. However, this simplification has its drawbacks, most notably that forensic examiners are less likely to encounter, and therefore understand, the raw data stored on the device. This lack of understanding fundamentally limits an examiner's ability to present evidence with confidence.

Course Aims

Data Demystifier 1 is a 4½ day online instructor-led course designed to give existing digital forensic examiners a true understanding of the data recovered and decoded by forensic software tools.

Delegates will learn the fundamental encodings used for time and date information, text data (ASCII and Unicode) as well as the vital role played by file signatures in digital forensics.

Students will gain extensive experience in working with raw data within a hex editor: understanding offsets, Endian-ness, using regular expressions to search large device extractions, manually carving data of interest and then making sense of that data.

Developing an in-depth understanding of how electronic devices actually store data enables digital forensic examiners to not only corroborate the evidence presented by commercial forensic tools, but also to recover and present evidence which such tools may have missed.

What you will learn

By the end of the course, students will be able to:

- Confidently navigate raw data within a hex viewer and manually carve data of interest
- Construct regular expressions to search for deleted media files within a physical extraction
- Identify and interpret data encoded using Little Endian and Big Endian byte ordering
- Attempt manual repair of unplayable MP4/3GP/MOV video files
- Explain and justify their actions in court

Who should attend?

This course is targeted at existing digital forensic examiners who have at least 6 months experience. Ideally delegates would have previously attended either of the Control-F Foundation in Mobile Phone Forensics or Foundation in Securing Computer Evidence courses (or equivalent).

Delivery format

Online instructor-led.

Technical requirements

Delegates will require a computer with a minimum 10MB Internet connection, a webcam and speakers (or headset). Delegates are strongly recommended to ensure they have access to dual monitors.

contact
+44 (0)20 8133 8758
info@controlf.net
PO Box 167, Sandy, SG19 9AL
www.controlf.net
Dates & prices are on our website