Demystifying Hex Data

Mobile forensic software tools extract data from mobile 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.

> GREAT COURSE, FULL OF GREAT KNOWLEDGE, EASY TO FOLLOW AND UNDERSTAND

Course Aims

Demystifying Hex Data is a 3½ day course designed to give existing mobile 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.

Delegates 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 mobile devices actually store data enables mobile 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.

Who should attend?

This course is targeted at existing digital forensic examiners who have at least 6 months experience in mobile device or computer forensics. Ideally delegates would have previously attended the Control-F 'Foundation in Mobile Phone Forensics' course (or equivalent).

What you will learn

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

- Confidently navigate raw data within a hex viewer and manually carve data of interest

- Identify and interpret data encoded using Little Endian and Big Endian byte ordering

- Construct regular expressions to search for deleted media files within a physical extraction

- Attempt repair of unplayable MP4/3GP/MOV video files

- Explain & justify their actions in court

Control-F
DIGITAL FORENSICS

'We make it make sense'