Acquiring Challenging Computer Devices

CLASSROOM COURSE

SECURE DATA FROM SURFACE PRO, MAC AND CHROMEBOOK DEVICES

The forensic acquisition of computer devices has been made more challenging through the shift from removable hard disk and solid-state drives to "soldered on" flash memory storage. The inability to remove (and image) the storage is further compounded in some devices by the presence of encryption and dedicated security chips, both of which can hamper acquisition via bootable media.

This situation presents multiple challenges to those tasked with forensically acquiring computers. If active encryption is not identified and addressed at seizure, it may be impossible to subsequently decrypt data held on the device. Without the necessary knowledge and specialist tools, "secure boot" features within Windows, Mac and Chromebook devices may prevent any data from being recovered from the device. Even worse, failing to follow correct procedures when acquiring a Chromebook can lead to irretrievable loss of data from the device.

> "GREAT COMPANY...
> GREAT TRAINERS!
> REPUTATION WELL DESERVED.
> LOVE COMING HERE."

Course Aims

Acquiring Challenging Computer Devices is a 2 day course designed to teach delegates how to acquire Microsoft Surface Pro, Apple Mac and Chromebook devices. Fundamental to successful acquisition is not only the accurate identification of the device type, but in the case of Apple Mac devices, determining which specific security platform the device utilises (notably T2 and M1 chips). Once the security platform has been confirmed, appropriate steps can be taken to enable data acquisition.

Delegates will learn how to identify the presence of active BitLocker encryption on Surface Pro devices, perform live acquisitions of powered-on devices and take appropriate action to capture BitLocker recovery keys (which may be essential to subsequent analysis). During what is a highly practical course, delegates will create and use bootable media to recover data from both Chromebook and Surface Pro devices.

What delegates will learn

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

- Recognise if BitLocker is enabled on a Microsoft Surface Pro and use bootable media to acquire it
- Capture decrypted logical backups of Chromebook devices
- Distinguish between T2 and M1 series Apple computers and perform forensic acquisitions of both
- Explain & justify their actions in court

Who should attend?

This intermediate level course is targeted at personnel responsible for forensically acquiring computer devices within a lab environment as well as those tasked with securing digital evidence "at scene". Delegates should have at least 6 months experience in computer acquisition and have previously attended the Control-F Foundation in Securing Computer Evidence (or equivalent).

contact

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

Control-F®
DIGITAL FORENSICS

'We make it make sense'