Acquiring Challenging & Encrypted Devices

CLASSROOM COURSE - 4½ days

SECURE DATA FROM ENCRYPTED COMPUTER DEVICES

Increasingly robust security on desktop and laptop computers presents challenges for Digital Forensic Units. TPMs on Windows and Chromebook devices protect encryption keys, with similar mechanisms used on Apple Mac devices. Restrictions on the use of bootable media further complicate imaging when storage cannot be removed.

This has driven a shift towards live acquisition of decrypted data. While valuable, live acquisition offers limited options and increased risk. Without the necessary knowledge and skills, opportunities may be missed; worse still, device security mechanisms may be triggered, rendering data inaccessible.

> “FINALLY, A TRAINING COMPANY THAT UNDERSTANDS THE SCIENCE OF LEARNING!”

Course Aims

Acquiring Challenging & Encrypted Devices is a 4½-day course that teaches delegates how to secure decrypted data from Macs, Chromebooks, Windows PCs, and Microsoft Surface devices.

Underpinning the course is the process of accurately identifying the device and confirming its security configuration. Based on this, delegates can choose the most suitable acquisition method.

Delegates will learn to image devices to external media where possible and apply best-practice video capture techniques in situations where a live examination of the device is the only option.

Given the prevalence of BitLocker encryption, the course includes hands-on experience in exploiting software vulnerabilities to recover Volume Master Keys and hashed user credentials. Delegates will use these techniques to decrypt protected data and crack user passwords without disassembling the device, thereby preventing the activation of BitLocker Recovery Mode.

What delegates will learn

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

- Use video capture techniques to record manual examinations of Macs, Chromebooks and Surface devices
- Use bootable media to acquire ‘Secure boot’ enabled devices and extract Windows account password hashes
- Crack passwords for Windows accounts, ZIP files and PDF documents using free tools
- Use free tools to decrypt BitLocker encrypted volumes on TPM-protected devices
- Explain and justify their actions in court

Who should attend?

This intermediate level course is targeted at personnel responsible for securing digital evidence from computer devices, either in a lab environment or at-scene. Delegates should have at least 6 months’ experience in computer acquisition and have previously attended the Control-F course ‘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