Understanding Mobile Forensic Data

ONLINE ON-DEMAND COURSE

WHAT'S RECOVERABLE? WHERE DID IT COME FROM? HOW CAN WE USE IT?

Data recovered from mobile devices plays a vital role in an increasing number of investigations. Our mobile devices contain an imprint of how we live our lives: who we know, where we go, what we think and what we do. Being able to explore and analyse the data behind that imprint gives investigators a unique insight into the whereabouts, actions and opinions of both victims and defendants.

Yet mobile forensics is far from simple. The types and volume of data which can be recovered depend upon a host of factors. Not only that, the data which can be recovered has origins in multiple sources – some reliable, some less so. Mobile forensic data can seem bewildering or overwhelming, meaning that there is a real risk that valuable data may be overlooked or misinterpreted.

Course Aims

Understanding Mobile Forensic Data is an on-demand (self-paced) online course designed to teach delegates how data is recovered from mobile devices, the origins and reliability of such data and its relevance within an investigation.

Delegates will learn about the differences between logical, physical and full filesystem extractions as well as why some of those techniques may not be available in some situations. Through the use of engaging and interactive visual content, delegates will learn where location data and time and date information present in mobile devices originate from. Crucially, the course will highlight data which once recovered from a mobile device should be corroborated or enriched with data from other sources (for example, a Communications Service Provider).

Who should attend?

This entry-level course is targeted at anyone who needs to understand the origins, scope and relevance of data recovered from mobile devices. This will include frontline police officers, investigators, analysts, case officers, senior police officers, lawyers, judges and more.

Successful completion of this course is a prerequisite for attendance of our classroom training course 'Reviewing Mobile Forensic Data'.

What you will learn

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

- Explain what a digital forensic artefact is and provide three examples

- Explain how logical and 'full filesystem' extractions of the same device might differ

- Give two examples of mobile forensic data which require corroboration via a Communications Service Provider

- Evaluate competing strategies for progressing an investigation using digital forensic data

Course Access & Duration

This online course can be accessed from a desktop or laptop PC with an appropriate Internet connection and comprises approximately 1½ days content. Our on-demand delivery allows learners to save their progress at any point, thus providing flexibility in both where and when they undertake the course.

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'