App Investigator 1

RECOVER EVIDENCE FROM UNSUPPORTED APPS

Smartphone and tablet devices submitted to forensic units present a veritable treasure trove of potential evidence generated through the use of pre-installed "1st party" and user-installed 3rd party apps. Unfortunately the relentless evolution of new and existing 3rd party apps means that commercial forensic tools cannot realistically decode, interpret and report all of the data of interest to investigators.

Course Aims

Android and iOS platforms both make extensive use of SQLite, a free open-source database platform, to store data relating to first and third party apps. Analysis of SQLite databases can recover live and deleted data as well as often overlooked binary data such as thumbnail images. In addition to SQLite databases, iOS devices make use of Property List (plist) files to store application data and mobile forensic examiners need to be skilled in analysing and reporting data from both file formats.

> "THIS WAS AN EXCELLENT COURSE. THE TUTORS WERE VERY SUPPORTIVE AND THE LEVEL OF KNOWLEDGE THEY HAVE IS EVIDENT."

App Investigator 1 is an instructor-led online course designed to teach delegates how to recover evidence from smartphone and tablet applications. This includes first party apps, but the emphasis will be on developing skills and techniques for working with 3rd party apps which are unsupported by commercial forensic tools. Delegates will gain experience of working with data recovered from iOS and Android devices.

Who should attend?

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

What you will learn

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

- Locate, view & recover evidence from SQLite databases used by smartphone applications
- Maximise evidence recovery from SQLite databases through appropriate handling and analysis of associated Write Ahead Logging (WAL) files
- Locate, view & recover evidence from Property List (plist) files used by iOS and associated applications
- Manually decode smartphone apps
- Explain & justify their actions in court

Technical requirements

Delegates will remotely log in to a Control-F PC to undertake the training and as such will require a computer with a minimum 10MB Internet connection

Delegates will also require a webcam, speakers (or headset). Access to dual monitors is highly recommended.

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'