



DIGITAL FIRST RESPONDER

Getting scene data right - securing & seizure of digital evidence

Specialist Capability Course | Reboot Digital Forensic Training

COURSE DETAILS

Duration:	3 Days (Classroom Based)
Level:	Foundation
Max Class Size:	12 Delegates (2 Trainers)
Certification:	Reboot Digital First Responder Certificate
Pre-requisites:	None — suitable for staff with no prior digital forensic training
Equipment:	All devices, tools and materials provided
Location:	Hosted at our Reboot training facility at the Electronics Group, Leeds, UK (This course can be hosted on-site)

WHY DIGITAL FIRST RESPONDER?

Digital evidence is now present at almost every crime scene. Decisions made in the first minutes at the scene can determine whether that evidence is identified, secured, recovered, preserved, changed or lost - forever! A powered-on device left unattended, a missed network connection or an incorrect seizure decision can render critical data unusable or unrecoverable before it is seized.

This course gives first responders, investigators and forensic staff the knowledge and confidence to make the right decisions at the scene. Delegates will learn to recognise, secure, seize and document digital evidence correctly across all common device types, from mobile phones and laptops to smart home devices, dashcams and CCTV systems. Or when to request assistance when they realise they can't act properly or legally.

Our teaching and scenarios are grounded in current legislation, best practice guidelines and evidential requirements, ensuring your team can act decisively at the scene and that what they recover will be usable in court and comply with required standards.

WHO WILL BENEFIT FROM THIS COURSE?

This course is designed for anyone who may encounter digital devices or digital evidence at a crime scene, regardless of their current level of digital forensic knowledge. It is equally valuable as a standalone course or as an entry point into further forensic training.

- Digital forensic analysts and forensic support staff
- Police first responders and crime-scene investigators
- Detectives and investigating officers
- Corporate security and HR investigation teams
- Intelligence and surveillance teams

PRE-COURSE REQUIREMENTS

There are no formal pre-course requirements for this course. It is designed to be accessible to delegates with no prior digital forensic experience. A general familiarity with mobile phones and computers as everyday devices is all that is needed. Delegates should come prepared for practical, scenario-based activities throughout the course with a willingness to develop and learn.

WHAT WILL WE TEACH ON THIS COURSE

This course delivers practical, scenario-driven training in the identification, securing and seizure of digital evidence at crime scenes along with its documentation. Delegates will work through realistic scenarios covering a wide range of device types and scene conditions. Topics covered include:

- Legal framework around actions and evidence admissibility
- Recognising digital evidence sources at a crime scene
- Scene photography, seizure and documentation of digital devices
- Powered-on vs powered-off seizure decisions and risks
- Dealing with volatile data; RAM, encryption and cloud based data
- Network isolation: when, why and how to use it correctly
- Mobile phone, tablet, computer and laptop seizure procedures
- Smart home devices, IoT and wearables as evidence sources
- Introduction to vehicle telematics, dashcams and GPS device recovery
- Network evidence: routers, logs and preserving Wi-Fi artefacts
- Scene debrief: common mistakes and how to avoid them

OTHER REBOOT COURSES

- **DIGITAL EVIDENCE ACQUISITION**
Imaging of digital media, host based data capture, verification, data basics, partitioning and formatting.
- **APP DATA FORENSICS**
App-level forensic analysis for iOS and Android — SQLite, plist, messaging apps, social media and other artefacts.
- **DEVICE REPAIR MODULES 1, 2 & 3**
Progressive repair training from foundation component replacement through to expert-level chip and NAND recovery techniques.

CONTACT DETAILS & OTHER INFORMATION

Email: enquiries@rebootforensic.co.uk

Web: <https://rebootforensic.co.uk>

Phone: 0203 879 1746

Social: LinkedIn