



RAM & Registry Analysis

Uncovering volatile and system evidence that others miss

Specialist Capability Course | Reboot Digital Forensic Training

COURSE DETAILS

Duration:	4.5 Days (Classroom Based)
Level:	Intermediate
Max Class Size:	12 Delegates (2 Trainers)
Certification:	Reboot RAM & Registry Analysis Certificate
Pre-requisites:	A basic understanding of digital forensics or completion of the Data Acquisition course
Equipment:	All devices, tools and materials provided
Location:	Hosted at our Reboot training facility at the Electronics Group, Leeds, UK

WHY RAM & REGISTRY ANALYSIS?

When a device is powered off, volatile memory is lost — and with it, evidence that can never be recovered from a disk image alone. Running processes, open network connections, encryption keys, user credentials and recently accessed files all exist in RAM and disappear the moment power is removed. If you are not capturing memory at the point of seizure, you may be missing the most significant evidence on the device.

The Windows Registry is one of the richest sources of forensic artefacts available to an investigator. It records user activity, program execution, connected devices, network history, recently accessed files and a great deal more — much of it invisible to a standard file system review.

This course teaches delegates how to capture volatile memory correctly and analyse both RAM and Registry data to surface evidence that would otherwise remain hidden.

WHO WILL BENEFIT FROM THIS COURSE?

This course is designed for digital forensic analysts and investigators who want to extend their capability beyond traditional disk forensics. It is suitable for practitioners with a basic understanding of digital forensics who are ready to work with volatile and system-level evidence.

- Digital forensic examiners and analysts
- Law enforcement digital forensic units
- Cyber incident response professionals
- Corporate and HR investigation teams
- IT security and threat intelligence teams

PRE-COURSE REQUIREMENTS

Delegates should have a basic familiarity with digital forensics concepts before attending this course. Completion of the Reboot Forensic Computing Data Acquisition course, or equivalent experience, is recommended. No prior knowledge of memory forensics or Registry analysis is required — the course builds from first principles. Delegates should be prepared for hands-on work throughout.

WHAT WILL WE TEACH ON THIS COURSE

This course delivers practical training in the capture and analysis of volatile memory and Windows Registry data. Delegates will work through structured exercises covering real investigative scenarios. Topics covered include:

- Understanding volatile memory and why it matters
- RAM capture tools and correct acquisition methodology
- Analysing RAM: running processes, open connections and artefacts
- Introduction to the Windows Registry: structure and purpose
- Key Registry hives and their forensic significance
- User activity artefacts: recently accessed files and programs
- Program execution evidence: UserAssist, ShimCache and Prefetch, identification of deleted apps and user activity
- Connected devices: USB history and device identification
- Registry analysis tools and practical examination techniques
- Continuity: documentation and exhibit handling
- Good practice to comply with ISO accreditation requirements

OTHER REBOOT COURSES

- **DIGITAL FIRST RESPONDER**
Identifying, securing, seizure and documenting of digital evidence at crime scenes across all common device types.
- **DIGITAL EVIDENCE ACQUISITION**
Imaging of digital media, host based data capture, verification, data basics, partitioning and formatting.
- **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