SORINTEQ

INTERMEDIATE DIGITAL FORENSICS

A 5-Day Intensive specialist course for the Government and commercial sectors

- 5 Day Programme
- Specialist Training for Law Enforcement
- All Training Equipment Provided
- In Association With the University of Buckingham

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Course Overview

Modern investigations increasingly require digital forensic examiners to operate in live environments, where critical evidential opportunities exist before a device can be seized, powered down, or removed for traditional laboratory examination.

The Intermediate Digital Forensics Course builds on the foundations of forensic examination and focuses on the recovery, preservation, and analysis of digital evidence from live systems and active operational environments.

This practical 5-day intensive programme equips learners with the skills required to support live investigations such as cyber attacks, ransomware incidents, insider threats, fraud investigations, and urgent operational deployments where immediate examination must be conducted without removing devices from service.

Participants will develop the capability to recover volatile data, support operational decision-making, preserve evidential integrity, and respond effectively to live crime scenes while maintaining forensic defensibility.

Who is the course for?

This course is designed for professionals who already have a foundation in digital forensic examination and require enhanced capability in live operational environments, including:

- Digital forensic examiners
- Cybercrime investigators
- Incident response and ransomware investigators
- Law enforcement investigators supporting live scenes
- Cyber security and cyber incident response teams
- Intelligence and technical recovery specialists

Participants should have completed a **Fundamentals in Digital Forensics Course** or possess equivalent practical forensic experience.

SORINTEQ

Course Content

The course delivers practical, investigator-led training across key operational areas, including:

- Introduction to Live Digital Forensics
- Understanding live forensic opportunities and operational considerations
- Live Scene Assessment and Triage
- Identifying priorities, preserving volatile evidence, and managing urgent decision-making
- Recovery of Volatile Data
- Memory capture, running processes, active sessions, encryption status, and live artefacts
- Live Network and Connectivity Analysis
- Capturing active connections, sessions, remote access indicators, and threat activity
- Responding to Cyber Attacks and Ransomware
- Supporting incident response teams during active compromise investigations
- Cloud and Virtual Environment Recovery
- Identifying opportunities where evidential recovery extends beyond physical devices
- Live Device Examination Techniques
- Safe recovery from systems that cannot be powered down or seized immediately
- Compiling Live Forensic Strategies
- Planning examinations, prioritising intelligence opportunities, and supporting operational outcomes
- Maintaining Evidential Integrity in Live Environments
- Documentation, continuity, chain of custody, and professional defensibility
- Supporting Interviews and Operational Decision-Making
- Using live forensic findings to support investigators and suspect interviews
- Case Studies and Practical Exercises
- Real-world scenarios including ransomware, insider threat, and live compromise investigations

SORINTEQ

Final Exercise Phase

- Live Incident Response Scenario
- Participants respond to a simulated cyber incident requiring immediate forensic action
- Volatile Data Recovery and Investigative Support
- Applying triage, recovery, and reporting under operational pressure
- Debrief and Professional Review
- Structured feedback on methodology, scene decisions, and evidential handling

Aims and Objectives of the Course

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

- Conduct forensic recovery safely within live digital environments
- Identify and preserve volatile evidence before system shutdown or disruption
- Support live investigations involving cyber attacks, ransomware, and active incidents
- Recover and analyse memory, active sessions, network artefacts, and cloud-linked evidence
- Make informed decisions around live triage and forensic prioritisation
- Apply forensic methodology to minimise contamination and maintain evidential integrity
- Support incident response teams and operational investigators in real time
- Produce defensible reporting suitable for evidential and intelligence purposes

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations. Our Intermediate Digital Forensics course develops practical operational capability, ensuring forensic examiners can confidently support live investigations, preserve critical evidence, and provide immediate value during fast-moving incidents.

Students undertaking courses provided by Sorinteq may earn credits towards formal academic qualifications such as Post Graduate Certificate, Diploma or MSc at the university of Buckingham.

For further enquiries please email info@sorinteq.com or call Sorinteq on +44 (0)333 0063248.

Sorinteq provide all necessary training equipment including laptop computers, internet connectivity, mobile devices and training material.