Sherfox Brochure 2026

Sherfox Digital Investigation Labs

CPD COURSES

CONTENTS

WHO ARE SHERFOX?

Sherfox Labs was officially created in 2022, but if you add up the experience across our team you get more than a century of digital forensics know-how. We are built on casework, powered by curiosity, and held together by a love of teaching, research, and occasionally very questionable cheese jokes.

Our team now numbers more than twenty, with backgrounds that stretch across computer science, electronics, policing, law, and corporate investigations. What unites us is a focus on real operational problems and a shared belief that digital forensics should be taught and practised in a way that looks after people. The work can be heavy, so we balance it with humour, colour, and more than a hint of cheesiness. That is why our training world of Cyberly is deliberately fun and safe, why we research and teach in trauma-informed ways, and why mental health in our field is something we openly advocate for.

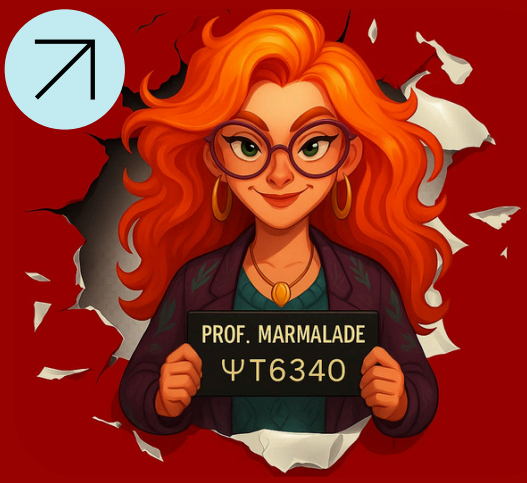
UNIVERSITY OF SOUTHAMPTON

Where we started...

Sherfox Labs, founded by Professor Sarah Morris, sits within the School of Electronics and Computer Science (ECS) at the University of Southampton (UoS), one of the UK's leading centres for cyber security and digital innovation. In short, Southampton is epic, and Sherfox is where the digital forensics magic happens.

CYBERLY

Cyberly is the colourful training and research world brewed by Sherfox Labs, part of the School of Electronics and Computer Science (ECS), University of Southampton.



It brings together data, hardware, and story-driven spaces designed to keep learning lively and forensic. Expect cutting edge tech, steady tea, and many cheesy jokes.

Wherever possible, our datasets are built inside Cyberly, our fictional teaching and research world. This keeps research trauma informed and mentally healthy, giving our team and collaborators the chance to tackle serious problems without unnecessary exposure to distressing material.

ALL COURSES

FOUNDATIONAL KNOWLEDGE

1 Course

- Digital Forensic Essentials (8 days)

DEVICE FOCUSED

3 Courses

- Data Capture Wizard: Acquisition & Storage Media (5 days)
- Mobile Sleuth: Mobile Device Investigations (3 or 5 days)
- IoT Inspector: Unusual Devices and IoT Forensics (5 days)

SCENE ANALYSIS

3 Courses

- Scene Specialist: Conducting Scene Investigations (3 or 5 days)
- Guardian Eye: CCTV Analysis (5 days)
- Security Sentinel: Corporate Security and Incident Response (5 days)

TECHNICAL MASTERCLASS

6 Courses

- AppTracker: Browser and App Forensics (5 days)
- Comms Data Analyser: Analysing Communication Data (3 or 5 days)
- Cyber Sleuth: Network and Corporate Investigations (5 days)
- Document Detective: Analysing Digital Documents (5 days)
- Multimedia Marvel: Multimedia Forensics (5 days)
- Open Source Intel Operative: OSINT Techniques (5 days)

ADVANCED SKILLS

1 Course

- Digital Forensics Masterclass (5 days)

PRESENTATION

1 Course

- Evidence Articulator: Communicating Digital Evidence (3 or 5 days)

DIGITAL FORENSICS ESSENTIALS

Digital Forensics Essentials (8 days)

This course provides a comprehensive introduction to the fundamentals of digital forensics, covering key concepts and methodologies.
Perfect for beginners, it lays the groundwork for all further forensic investigations.

Enrich our growing community.

Digital Forensic Essentials is our only foundational course, and for good reason. In just eight days it gives you everything you need to conduct a basic technical investigation from first principles, building a solid platform for all further forensic work. By the end you will not only understand the language and structures of digital evidence but also have the confidence to explore data directly, interpret artefacts, and apply core investigative strategies. This is the course that sets you up for everything that follows.

Duration: 8 days

Course Aim: To provide a comprehensive foundation in digital forensics, introducing the key principles, terminology, and investigative strategies that underpin all future forensic investigative work.

/1

Intended Learning Outcomes

- Understand core digital forensic terminology and concepts.
- Recognise and explain common data constructs and storage media.
- Identify key filesystem and operating system artefacts relevant to investigations.
- Apply structured investigative strategies to basic forensic problems.

/2

Indicative Content

- Introduction to digital forensic principles and methodology
- Data structures, storage media and partitioning
- Filesystems and their artefacts
- Operating system core artefacts and their evidential value
- Number systems and conversion between binary, decimal, and hexadecimal
- Use of a hexadecimal editor in forensic analysis
- General investigative strategies and case workflows

Prior knowledge

No prior digital forensics experience is required. A general familiarity with computers is helpful. This course involves converting between number systems and working in a hexadecimal editor. Whilst no prior knowledge is presumed, pre-course materials are provided and are strongly recommended if you are new to the field.

DATA CAPTURE WIZARD

Acquisition & Storage Media

Our Device Focused courses let you dive deep into the areas of digital forensics that matter most. You can take just one, or combine them as a set, with no need to follow a fixed order. Each course gives you extensive time in our electronics and computer labs, with access to the latest forensic hardware and practical exercises that mirror real investigations. Whether you want to master acquisition and storage media, unlock the secrets of mobile devices, or push the boundaries with IoT and unusual hardware, these courses give you the flexibility to specialise while building a powerful toolkit of complementary skills.

Data Capture Wizard (5 days)

Learn how to accurately acquire and preserve data from various storage media, Digital Devices, and Network Data, with advanced techniques.
Essential for ensuring data integrity in forensic investigations

Duration: 5 days

Course Aim: To develop practical expertise in acquiring and preserving data from a wide range of digital storage media and devices, using advanced techniques that ensure evidential integrity.

/1

Intended Learning Outcomes

- Apply forensic principles to the acquisition of diverse storage media.
- Use advanced acquisition methods including hardware-level techniques.
- Evaluate and verify data integrity across acquisition processes.
- Analyse challenges and solutions in wireless and network data acquisition.

/2

Indicative Content

- Forensic principles of acquisition and chain of custody
- Acquisition of common, historic, emerging, and unusual storage media
- Mobile device acquisition considerations
- Wireless data acquisition and validation
- Hardware-based approaches including chip-off and JTAG
- Managing legacy and unusual formats
- Data integrity checks and verification strategies

Prior knowledge

Confidence with hexadecimal editors and command line tools is expected. A solid understanding of digital forensic fundamentals is required.

MOBILE SLEUTH

Mobile Device Investigations

Our Device Focused courses let you dive deep into the areas of digital forensics that matter most. You can take just one, or combine them as a set, with no need to follow a fixed order. Each course gives you extensive time in our electronics and computer labs, with access to the latest forensic hardware and practical exercises that mirror real investigations. Whether you want to master acquisition and storage media, unlock the secrets of mobile devices, or push the boundaries with IoT and unusual hardware, these courses give you the flexibility to specialise while building a powerful toolkit of complementary skills.

Mobile Sleuth (3 or 5 days)

This course covers the forensic investigation of mobile devices, from data extraction to app analysis. Common, bespoke and adapted OS' and hardware are considered.
Ideal for those looking to master the intricacies of mobile forensics.

Duration: 3 days (general) – 5 days (advanced)

Course Aim: To equip investigators with the skills to acquire, analyse, and interpret data from mobile devices across multiple operating systems and hardware platforms.

/1

Intended Learning Outcomes

- Conduct forensic acquisition and extraction from a range of mobile devices.
- Interpret core artefacts across common and bespoke mobile operating systems.
- Analyse applications, messaging, and communications data.
- Apply investigative strategies to both legacy and current mobile devices.

/2

Indicative Content

- Mobile device architecture and evidence sources
- Acquisition methods for historical and modern devices
- Devices with SIM cards and associated metadata
- App data and communication artefact analysis
- Bespoke and adapted operating systems
- Hardware approaches including JTAG and chip-off where appropriate
- Reporting and evidential considerations in mobile forensics

Prior knowledge

Confidence with hexadecimal editors and command line tools is expected. A solid understanding of digital forensic fundamentals is required.

IOT INSPECTOR

Unusual Devices and IoT Forensics

Our Device Focused courses let you dive deep into the areas of digital forensics that matter most. You can take just one, or combine them as a set, with no need to follow a fixed order. Each course gives you extensive time in our electronics and computer labs, with access to the latest forensic hardware and practical exercises that mirror real investigations. Whether you want to master acquisition and storage media, unlock the secrets of mobile devices, or push the boundaries with IoT and unusual hardware, these courses give you the flexibility to specialise while building a powerful toolkit of complementary skills.

IoT Inspector (5 days)

Dive into the world of IoT and other unconventional devices, learning how to investigate and interpret data from these sources.
Crucial for staying ahead in the rapidly evolving field of digital forensics

Duration: 5 days

Course Aim: To explore forensic methods for Internet of Things devices and other unconventional sources, teaching participants how to investigate, interpret, and research data from a wide spectrum of modern technologies.

/1

Intended Learning Outcomes

- Identify forensic opportunities within IoT and non-traditional devices.
- Acquire and analyse data from a variety of IoT ecosystems.
- Apply wireless data acquisition and interpretation techniques.
- Use research-led approaches to access and interpret novel devices.

/2

Indicative Content

- IoT device fundamentals and forensic challenges
- Wireless protocols and data acquisition methods
- Investigating vehicles, washing machines, alarms, and home assistants
- Research approaches for accessing undocumented or unusual devices
- Security, privacy, and ethical considerations in IoT forensics
- Hardware-level approaches where applicable (chip-off, JTAG)
- Case studies of IoT investigations and lessons learned

Prior knowledge

Confidence with hexadecimal editors and command line tools is expected. A solid understanding of digital forensic fundamentals is required.

SCENE SPECIALIST

Scene Specialist (3 or 5 days)

Focuses on the critical aspects of managing and investigating digital evidence at a physical scene.
A must for professionals involved in on-site forensic investigations.

Conducting Scene Investigations

The Scene Analysis courses bring digital forensics into the real world. These are practical, immersive programmes designed for anyone who needs to manage evidence at a scene, analyse surveillance material, or respond to live security incidents. You can take each course on its own or combine them to build a broader skillset. Two of the courses make use of our immersive scene room, giving you realistic practice in handling devices and evidence under pressure. Whether you are first on-site, reviewing CCTV footage, or leading corporate incident response, these courses prepare you to work with confidence where the digital and physical worlds meet.

Duration: 3 days (general) – 5 days (advanced)

Course Aim: To equip participants with the skills to identify, preserve, and recover digital evidence at physical scenes while maintaining evidential integrity.

/1

Intended Learning Outcomes

- Plan and manage digital evidence handling at a physical scene.
- Apply recognised methods for identifying and preserving evidence.
- Document and maintain chain of custody under operational conditions.
- Conduct hands-on recovery and interpretation exercises in live environments.

/2

Indicative Content

- Scene management principles and first response
- Identifying digital devices and potential evidence sources
- Handling, documenting, and transporting evidence
- Live scene practicals in our immersive crime scene room
- Reporting and evidential continuity

Prior knowledge

Knowledge of digital forensic fundamentals is expected. Experience with investigative environments is beneficial but not required.

GUARDIAN EYE

CCTV Analysis

The Scene Analysis courses bring digital forensics into the real world. These are practical, immersive programmes designed for anyone who needs to manage evidence at a scene, analyse surveillance material, or respond to live security incidents. You can take each course on its own or combine them to build a broader skillset. Two of the courses make use of our immersive scene room, giving you realistic practice in handling devices and evidence under pressure. Whether you are first on-site, reviewing CCTV footage, or leading corporate incident response, these courses prepare you to work with confidence where the digital and physical worlds meet.

Guardian Eye (5 days)

Teaches the techniques for analysing CCTV footage and other video evidence in forensic investigations.
Essential for those involved in cases with video surveillance evidence.

Duration: 5 days

Course Aim: To provide practical and technical expertise in analysing CCTV and video evidence for forensic purposes.

/1

Intended Learning Outcomes

- Identify evidential opportunities within CCTV and video systems.
- Extract, convert, and preserve video evidence without data loss.
- Analyse and interpret footage in forensic contexts.
- Apply best practices in reporting, continuity, and presentation of video evidence.

/2

Indicative Content

- CCTV system types and evidential considerations
- Recovery and preservation of digital video footage
- File formats, conversion, and compatibility issues
- Analytical techniques for reviewing footage
- Hands-on exercises in the immersive scene room
- Evidential continuity and courtroom presentation

Prior knowledge

Knowledge of digital forensic fundamentals is expected. Familiarity with handling digital files is helpful.

SECURITY SENTINEL

Security Sentinel (5 days)

Provides insights into corporate security, focusing on incident response and mitigating digital threats.
Key for professionals tasked with protecting organisational digital assets

Corporate Security and Incident Response

The Scene Analysis courses bring digital forensics into the real world. These are practical, immersive programmes designed for anyone who needs to manage evidence at a scene, analyse surveillance material, or respond to live security incidents. You can take each course on its own or combine them to build a broader skillset. Two of the courses make use of our immersive scene room, giving you realistic practice in handling devices and evidence under pressure. Whether you are first on-site, reviewing CCTV footage, or leading corporate incident response, these courses prepare you to work with confidence where the digital and physical worlds meet.

Duration: 5 days

Course Aim: To develop practical and strategic skills in incident response and corporate security, enabling professionals to protect organisational assets from digital threats.

/1

Intended Learning Outcomes

- Understand incident response processes in corporate contexts.
- Apply forensic principles to organisational security incidents.
- Detect, contain, and mitigate digital threats in real time.
- Implement effective reporting and recovery strategies.

/2

Indicative Content

- Incident response frameworks and policies
- Identifying and triaging digital incidents
- Corporate security tools and technologies
- Mitigating and containing active threats
- Forensic approaches to insider and external incidents
- Communication and reporting in organisational environments

Prior knowledge

Knowledge of digital forensic fundamentals is expected. Familiarity with IT or security operations is beneficial.

APPTRACKER

Browser and App Forensics

The Technical Masterclass courses are where digital forensics gets detailed and powerful. Each one focuses on a core evidence type or investigative approach, giving you low-level skills that transfer across devices, tools, and cases. From browser traces to corporate networks, from documents to multimedia files, from comms data to OSINT, these courses combine fundamentals with the latest emerging techniques. You can take them individually or as a set, and whichever route you choose you will leave with sharper, novel skills that give you the confidence to tackle complex digital investigations head-on.

AppTracker (5 days)

Explore the forensic analysis of web browsers and applications to uncover user activity and data trails.
Vital for those specialising in internet and app-based investigations.

Duration: 5 days

Course Aim: To develop the skills required to identify, recover, and analyse artefacts from web browsers and applications, providing insight into user activity across platforms.

/1

Intended Learning Outcomes

- Recognise and interpret browser artefacts and cached data.
- Extract and analyse application data from common and bespoke apps.
- Identify patterns of user behaviour and online activity.
- Present browser and app evidence in a forensic context.

/2

Indicative Content

- Web browser architecture and evidence sources
- Cache, history, cookies, and log file analysis
- Mobile and desktop app data recovery
- SQLite databases, JSON, and log artefacts
- Linking to wider system activity
- Cross-platform challenges and solutions
- Reporting and evidential presentation

Prior knowledge

Confidence with hex editors and command line tools is expected. Knowledge of digital forensic fundamentals is required.

COMMS DATA ANALYSER

Comms Data Analyser (3 or 5 days)

This course covers the forensic analysis of communication data, including data packets, emails, messaging apps, and call logs. Crucial for investigations involving communication records.

Analysing Communication Data

The Technical Masterclass courses are where digital forensics gets detailed and powerful. Each one focuses on a core evidence type or investigative approach, giving you low-level skills that transfer across devices, tools, and cases. From browser traces to corporate networks, from documents to multimedia files, from comms data to OSINT, these courses combine fundamentals with the latest emerging techniques. You can take them individually or as a set, and whichever route you choose you will leave with sharper, novel skills that give you the confidence to tackle complex digital investigations head-on.

Duration: 3 days (general) – 5 days (advanced)

Course Aim: To equip participants with the skills to extract, analyse, and interpret communication data from telecoms providers, devices, and messaging applications.

/1

Intended Learning Outcomes

- Interpret call detail records and telecoms data sets.
- Extract and analyse communication artefacts from devices.
- Evaluate instant messaging and VoIP data sources.
- Present communication data as part of a forensic timeline.

/2

Indicative Content

- Structure and interpretation of call detail records (CDRs)
- Telecoms data acquisition and validation
- Instant messaging, SMS, and VoIP artefacts
- Correlating multiple sources of communication data
- Challenges with modern encrypted messaging services
- Evidential reporting and courtroom use

Prior knowledge

Knowledge of digital forensic fundamentals is expected. Familiarity with basic telecoms data structures is beneficial.

CYBER SLEUTH

Network and Corporate Investigations

The Technical Masterclass courses are where digital forensics gets detailed and powerful. Each one focuses on a core evidence type or investigative approach, giving you low-level skills that transfer across devices, tools, and cases. From browser traces to corporate networks, from documents to multimedia files, from comms data to OSINT, these courses combine fundamentals with the latest emerging techniques. You can take them individually or as a set, and whichever route you choose you will leave with sharper, novel skills that give you the confidence to tackle complex digital investigations head-on.

Cyber Sleuth (5 days)

Learn about network forensics and corporate investigations, focusing on cyber threats, incident response techniques and internal security breaches.
Essential for professionals in corporate security.

Duration: 5 days

Course Aim: To provide participants with the skills to investigate digital incidents within corporate and networked environments, tracing evidence through traffic and systems.

/1

Intended Learning Outcomes

- Monitor and interpret network traffic for investigative purposes.
- Apply forensic techniques to corporate system incidents.
- Detect and triage intrusions and malicious activity.
- Develop effective investigative reports for corporate stakeholders.

/2

Indicative Content

- Network traffic capture and analysis fundamentals
- Investigating corporate infrastructure and logs
- Identifying intrusions and APT activity
- Incident triage and evidence preservation
- Correlating multiple data sources across networks
- Corporate communication and reporting requirements

Prior knowledge

Knowledge of digital forensic fundamentals is required. Familiarity with networking concepts and corporate IT environments is recommended.

DOCUMENT DETECTIVE

Analysing Digital Documents

The Technical Masterclass courses are where digital forensics gets detailed and powerful. Each one focuses on a core evidence type or investigative approach, giving you low-level skills that transfer across devices, tools, and cases. From browser traces to corporate networks, from documents to multimedia files, from comms data to OSINT, these courses combine fundamentals with the latest emerging techniques. You can take them individually or as a set, and whichever route you choose you will leave with sharper, novel skills that give you the confidence to tackle complex digital investigations head-on.

Document Detective (5 days)

Focuses on the forensic examination of digital documents, including metadata analysis, embedded objects, corrupt document recovery, timelining, and document verification.
Perfect for cases where document integrity is critical.

Duration: 5 days

Course Aim: To build expertise in analysing digital documents, uncovering metadata, hidden content, and artefacts that reveal creation, modification, and usage history.

/1

Intended Learning Outcomes

- Identify and extract metadata from common document formats.
- Detect hidden content, revisions, and versioning information.
- Correlate document artefacts with wider investigative data.
- Produce forensic reports on document analysis findings.

/2

Indicative Content

- Document file formats (Word, PDF, spreadsheets, presentations)
- Metadata structures and evidential value
- Hidden content, version history, and embedded artefacts
- Watermarks, authoring information, and timestamps
- Document correlation in larger investigations
- Presentation of document evidence

Prior knowledge

Knowledge of digital forensic fundamentals is required. Familiarity with common office software is beneficial.

MULTIMEDIA MARVEL

Multimedia Forensics

The Technical Masterclass courses are where digital forensics gets detailed and powerful. Each one focuses on a core evidence type or investigative approach, giving you low-level skills that transfer across devices, tools, and cases. From browser traces to corporate networks, from documents to multimedia files, from comms data to OSINT, these courses combine fundamentals with the latest emerging techniques. You can take them individually or as a set, and whichever route you choose you will leave with sharper, novel skills that give you the confidence to tackle complex digital investigations head-on.

Multimedia Marvel (5 days)

Dive into the analysis of multimedia files, including images, audio, and video, to extract and interpret forensic evidence. Learn how to identify media which is computer generated, or manipulated, as well as using media for intelligence. Ideal for those dealing with media-rich investigations.

Duration: 5 days

Course Aim: To provide technical and practical skills for analysing images, video, and audio, validating authenticity, and extracting evidential value.

/1

Intended Learning Outcomes

- Identify evidential opportunities within multimedia files.
- Apply forensic techniques to detect manipulation or tampering.
- Extract metadata and contextual information from media.
- Present findings with clarity and evidential rigour.

/2

Indicative Content

- Multimedia file structures and formats
- Image analysis, EXIF data, and hidden artefacts
- Video recovery, conversion, and validation
- Audio analysis and metadata extraction
- Detecting manipulation, splicing, and editing
- Reporting and evidential presentation

Prior knowledge

Knowledge of digital forensic fundamentals is required. Familiarity with multimedia formats is helpful.

OPEN SOURCE INTEL OPERATIVE

Open Source Intel Operative (5 days)

Teaches the techniques for gathering and analysing open-source intelligence (OSINT) for forensic or intelligence gathering purposes.
Key for professionals looking to leverage public data in investigations.

OSINT Techniques

The Technical Masterclass courses are where digital forensics gets detailed and powerful. Each one focuses on a core evidence type or investigative approach, giving you low-level skills that transfer across devices, tools, and cases. From browser traces to corporate networks, from documents to multimedia files, from comms data to OSINT, these courses combine fundamentals with the latest emerging techniques. You can take them individually or as a set, and whichever route you choose you will leave with sharper, novel skills that give you the confidence to tackle complex digital investigations head-on.

Duration: 5 days

Course Aim: To introduce safe, ethical, and effective methods for gathering and analysing intelligence from open sources to support digital investigations.

/1

Intended Learning Outcomes

- Apply OSINT techniques across social media and online platforms.
- Use advanced search and filtering strategies to locate intelligence.
- Evaluate reliability and evidential weight of OSINT findings.
- Integrate OSINT into broader digital forensic investigations.

/2

Indicative Content

- Introduction to OSINT frameworks and ethics
- Search engine operators and advanced filtering
- Social media investigations and metadata recovery
- Monitoring and archiving open source material
- Combining OSINT with device or comms data
- Evidential and legal considerations

Prior knowledge

Knowledge of digital forensic fundamentals is required. No prior OSINT experience is necessary.

DIGITAL FORENSICS MASTERCLASS

Digital Forensics Masterclass (5 days)

An advanced course that deepens your understanding of digital forensics, focusing on complex investigative approaches and cutting-edge techniques.
A must for experienced practitioners aiming to refine their expertise.

Advanced Technical Challenges and Approaches

For those who already have strong technical knowledge and want to push further, our Advanced Skills course takes you into the most complex areas of digital forensics. This is where experienced practitioners refine their expertise, tackle advanced challenges, and explore cutting-edge investigative approaches.

Duration: 5 days

Course Aim: To challenge and extend the knowledge of experienced forensic practitioners by exploring advanced techniques, complex investigations, and innovative approaches to digital forensics.

/1

Intended Learning Outcomes

- Tackle complex forensic problems using advanced methods and tools.
- Evaluate and apply cutting-edge research and emerging techniques.
- Integrate multiple sources of evidence into cohesive case narratives.
- Adapt investigative strategies to unusual or highly technical scenarios.

/2

Indicative Content

- Advanced acquisition and recovery techniques
- Complex filesystem and operating system artefacts
- Correlation of diverse datasets across multiple devices
- Emerging challenges in encryption, anti-forensics, and volatile data
- Integrating OSINT, comms, and device artefacts in advanced cases
- Case studies from unusual and high-profile investigations

Prior knowledge

Significant prior experience in digital forensics is essential. Participants should already be confident with hex editors, command line tools, and core forensic processes..

EVIDENCE ARTICULATOR

Communicating Digital Evidence

Even the strongest investigation can fail if the evidence is not communicated clearly. This cluster is dedicated to building the skills you need to explain complex technical findings in ways that are accurate, persuasive, and accessible to your audience.

Evidence Articulator (3 or 5 days)

Learn how to effectively present and communicate digital evidence in legal and professional settings.
Essential for ensuring that your findings are clearly understood and impactful.

Duration: 3 days (general) – 5 days (advanced)

Course Aim: To equip participants with the ability to present and communicate digital evidence effectively in legal, investigative, and professional contexts.

/1

Intended Learning Outcomes

- Translate complex technical findings into clear and accurate narratives.
- Develop written and oral communication skills tailored to different audiences.
- Apply best practices for courtroom and investigative reporting.
- Demonstrate confidence in articulating digital evidence under scrutiny.

/2

Indicative Content

- Principles of effective communication in digital forensics
- Writing reports that are clear, accurate, and legally sound
- Preparing and delivering expert testimony
- Explaining complex technical findings to non-technical audiences
- Communication strategies for courts, clients, and investigators
- Practical exercises with simulated evidence presentations

Prior knowledge

Knowledge of digital forensic fundamentals is required. Some prior exposure to reporting or professional communication is beneficial but not essential.

BOOKING.

Because our courses are practitioner focused, we do not openly advertise dates or locations online for security and safety reasons. If you would like further details, please email us from a corporate email address. If you are contacting us from a free email service, please note that limited information will be provided until your identity has been verified.
Once your identity is confirmed, you will complete a short online skills check (around five minutes). After this you will be able to book onto courses directly.

KEY INFORMATION.

Access to materials
All course participants receive access to online materials for 12 months after their course, plus a downloadable take-away pack for permanent reference.

Virtual delivery
Some courses have virtual versions available, please ask if this is an option for your chosen course.

Booking options
You can book as an individual, in bulk, or request for us to run a course at your organisation for groups of six or more.

Pricing
Courses range from £2600 – £4500 depending on content and duration. Bursaries are available for those not currently employed or for those with an existing relationship with ECS.

We are committed to keeping our training secure, accessible, and practitioner led. If you have any additional queries or concerns, please get in touch and our team will be happy to help.

NEXT STEPS

So you found a course you liked! Here's what happens next...

GET IN TOUCH

Email us with your enquiry. Use a corporate email if possible (free email addresses will be verified before we can share full details.)

IDENTITY CHECK

For security, we confirm who you are before giving access to course information.

SKILLS CHECK

Complete a short five-minute online skills check so we can recommend the right course level for you.

BOOK YOUR PLACE

Book individually, in bulk, or request a dedicated course at your location for groups of six or more.

GET PREPARED

After booking, you'll receive joining instructions, pre-course materials, and everything you need to get the most out of your training.

FAQs

SHERFOX LABS.

Sherfox Labs operates a suite of dedicated specialist laboratories designed specifically for digital forensics, investigation, and applied research.

Operational Laboratory

The Sherfox operational laboratory is fully equipped to handle evidential material and supports a wide range of global casework across multiple investigation types.
It contains current digital forensic hardware and software for computer-based analysis, as well as specialist capabilities for electronic and embedded investigations, including chip-off, JTAG, and vehicle forensics. The lab operates under established evidential handling and provenance principles.

Research Laboratory

The Sherfox research laboratory is available to students and staff who have completed appropriate training. It mirrors the operational laboratory environment and supports high-quality, practice-informed research using professional-grade equipment.

Scene and IoT Environment

The Sherfox scene environment focuses on IoT and connected device ecosystems. It is used for training, education, research, and operational simulation, and also doubles as an immersive escape-room-style environment to support realistic scenario-based activity.

Flexible, High-Quality Infrastructure

Across teaching, research, and operational activity, Sherfox Labs benefits from bespoke, top-of-the-range laboratory infrastructure. Facilities are designed to be flexible and adaptable, enabling us to support a wide range of requirements, from large-scale teaching through to specialist operational and research needs.

UoS FACILITIES AND LABS.

As part of the School of Electronics and Computer Science (ECS) at the University of Southampton, Sherfox Labs has access to a wide range of facilities across the School and the wider University. There has been significant investment in laboratory infrastructure within ECS, resulting in a flexible, powerful, and highly capable environment that supports teaching, research, and operational activity.

Research Laboratories

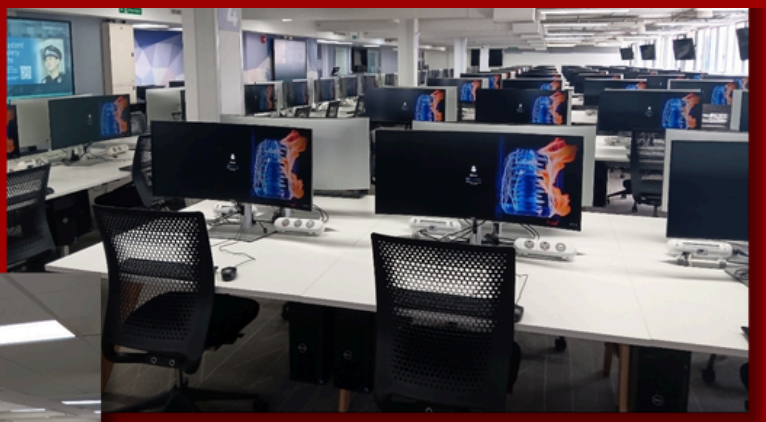
Sherfox Labs offers access to a broad portfolio of custom research laboratories supporting electronics, communications, high-power and high-voltage systems, robotics, materials, sensors, biomedical work, vehicles, and computer science.

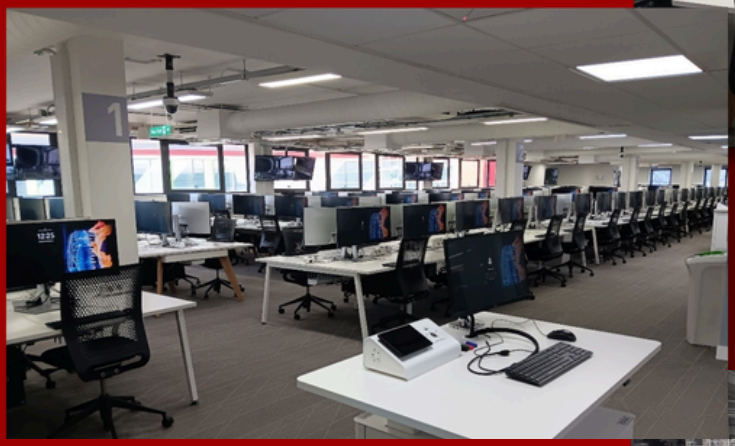
Facilities include Faraday cages and anechoic chambers, both on-site and in dedicated lab spaces, enabling controlled experimental, investigative, and operational work.

Specialist Laboratories

The School hosts purpose-designed teaching laboratories for electronics, computer science, and hybrid delivery. Labs seat approximately 100 to 180 students and support large-scale, technically demanding teaching.

All laboratories are equipped with custom PCs, distributed screens for clear visibility, integrated microphones, and high-quality audiovisual systems, enabling interactive teaching without reliance on a single front focal point.





FAQS.

We want every learner to feel safe, included, and able to succeed. If you have a disability, learning difference, additional needs, or you are new to the field, we will work with you to make the course fit you. The answers below cover common concerns. If you need something not listed here, email us and we will help.

/1 I Have A Disability Or Long-Term Health Condition. Can You Provide Adjustments?

Yes. Typical adjustments include advance access to materials, alternative colour schemes, extra time for tasks, larger fonts, seating preference, step-free access, and frequent rest breaks. We can also provide live captions for virtual delivery and quiet spaces onsite where possible. Tell us what works for you and we will confirm what we can put in place before the course starts.

/2 I Have Dyslexia, ADHD, Or Another Learning Difference. How Is The Course Structured?

Courses use clear step-by-step instructions, short task blocks, and frequent checkpoints. We provide pre-work primers, plain-language glossaries, and templates for note-taking. You can work at your pace during practicals and we avoid surprise timed tests. Assessment is optional and can be done in alternative formats.

/3 I Experience Anxiety Or Prefer Lower Sensory Environments. What Support Is Available?

We keep class sizes sensible, outline each day's plan, and make expectations clear. You can arrive early to settle in, choose a quieter seat, and take breaks whenever you need. We use trauma-informed Cyberly datasets rather than graphic real-world material. You may submit questions privately if you do not want to speak out loud.

/4 I Am Not From A Digital Forensics Background. Will I Keep Up?

Yes. Many learners join us from policing, legal practice, IT support, or adjacent roles. We teach from first principles and give pre-course primers. Practical tasks start simple and build steadily. Instructors are practitioners who explain why a step matters and how it appears in real cases.

/5 Can I Bring Assistive Tech Or A Support Person?

Assistive software and devices are welcome. If you need a support person or interpreter, let us know in advance so we can arrange access and confidentiality agreements where needed.

/6 What If I Need Remote Or Flexible Participation?

Several courses have virtual options. We can offer camera-off participation, captioned sessions, and flexible timings for breaks. Recording is available for some components. Ask during booking and we will advise on the best fit.

/7 How Do I Request An Adjustment?

Email us after your identity check with a short description of what you need and anything that has helped you before. We will agree a plan in writing before the course and share it with your instructors so you do not have to repeat yourself.

WORK WITH US.

Beyond CPD: Other ways to work with us

Sherfox Labs offers a range of ways to collaborate that sit alongside, and beyond, our CPD and training activity. We actively welcome engagement from practitioners, organisations, researchers, and partners who want to work with us operationally, academically, or creatively.

Operational Collaboration

We work with partners across the globe on a wide range of investigation types and operational needs.

You can work with us operationally in several ways:

- Full casework delivery
- Specialist support on existing investigations
- Advisory or second-opinion input
- Targeted technical assistance

Our experience spans civil, criminal, and intelligence investigations, as well as work supporting journalists and complex data recovery efforts. We operate across a wide range of common and bespoke devices, with expertise covering electronics, communications, and computer science.

Engagement can be short-term or ongoing, remote or in person, depending on requirements.

Research Collaboration

Research collaboration with Sherfox Labs is deliberately flexible and partner-friendly.

You can work with us through:

- Direct collaborative research
- Joint funding bids
- Bringing us a real-world problem that needs solving
- Exploratory or pilot work to assess feasibility

Depending on scope, formal funding may not be required. In-kind support, shared data, or practitioner insight may be sufficient for smaller or early-stage problems. Where funding is appropriate, we are experienced in collaborative bids and are always keen to support partners pursuing STAR and similar research funding awards.

Our research is practice-informed, impact-focused, and designed to translate into real operational benefit.

WORK WITH US.

Education and Training Engagement

There are many ways to work with Sherfox Labs through education and skills development.

These include:

- Sponsoring or co-supervising a PhD student
- Providing project ideas for undergraduate, Master's, or group projects
- Guest lectures or specialist teaching sessions
- Contributing to courses or workshops
- Supporting lunch-and-learn sessions or informal knowledge sharing

These opportunities can be delivered online or in person and often require time and expertise rather than funding.

Membership and Community

You can also work with us by becoming part of Sherfox Labs.

We welcome new members who share our values and bring expertise, curiosity, or lived experience relevant to our work. Membership is about contributing to, and benefiting from, a collaborative, supportive, and practice-driven community.

Public Engagement and Outreach

Sherfox Labs is committed to public engagement and outreach, including work with children and young people. We believe in demystifying technology, investigation, and science, and in making them accessible and human.
We are also enthusiastic supporters of science-based comedy as a legitimate engagement and wellbeing tool. This approach reflects our belief that learning, curiosity, and mental health are closely linked.

A Collaborative Ethos

We are not "just after funding". Collaboration with Sherfox Labs can involve:

- Financial support
- In-kind contributions
- Shared expertise
- Time and participation
- Joint bids and co-created research
- Online or in-person engagement

If you have an idea, a challenge, or a curiosity, we are always happy to start a conversation.

CONTACT US.

Need something else? Contact us and we will work it through together.

(+44) 23 8059 3441

hello@sherfoxlabs.com

https://sherfoxlabs.com

ECS Partners Ltd, University of Southampton, University Road, Highfield, Southampton, SO17 1BJ

Contact us via form

We are academics ...

Our working patterns can be ad hoc around teaching, research, and casework.
Shared inbox monitoring: typically 10:00–16:00 UK on office days (Mon–Fri). Triage outside this window may be slower.

Urgent subjects: add “URGENT” at the start of your email subject for quicker triage.

Security notes

Please avoid sending live case data on first contact. We’ll arrange SFTP or an encrypted archive if needed.