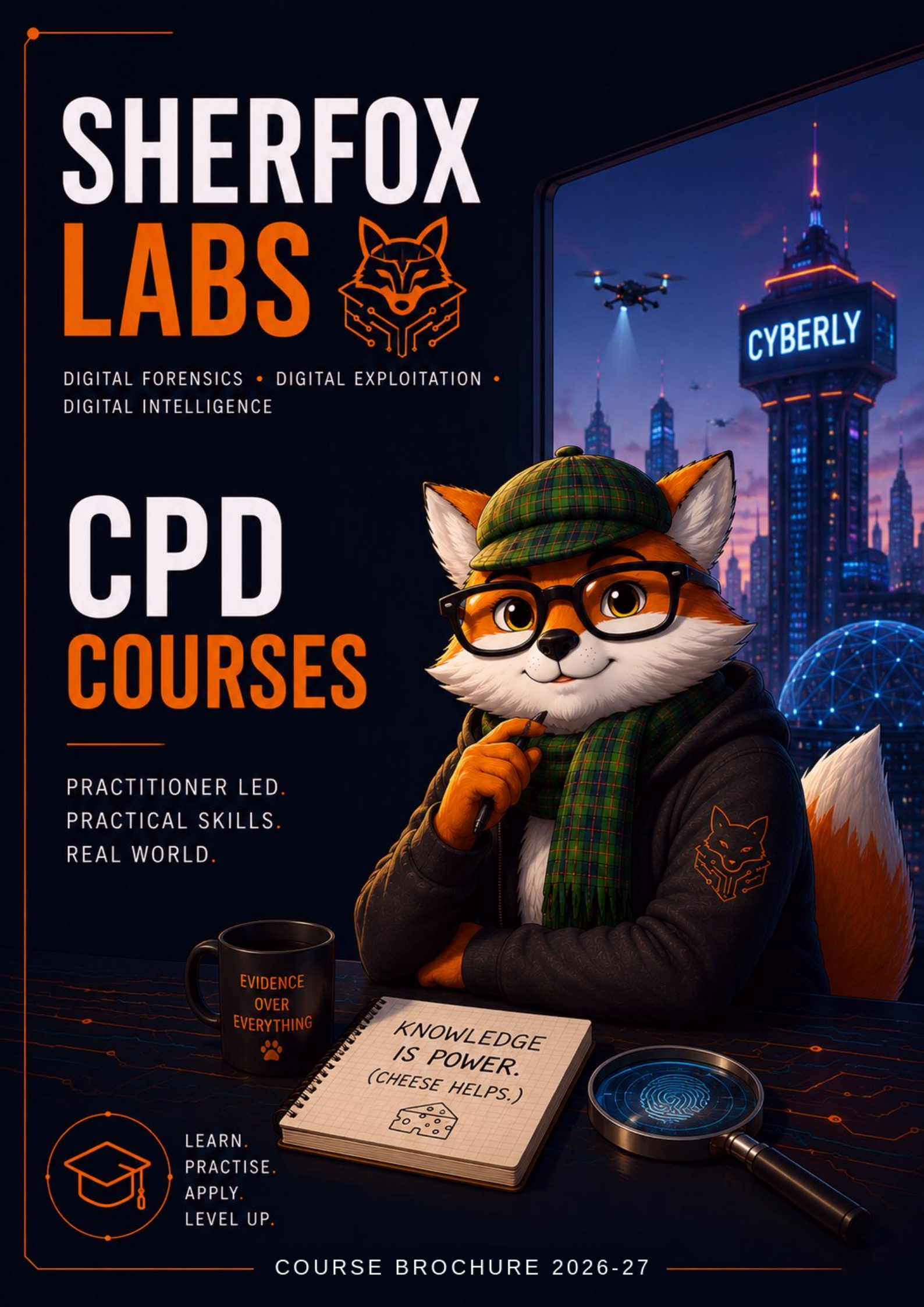
SHERFOX LABS

DIGITAL FORENSICS • DIGITAL EXPLOITATION • DIGITAL INTELLIGENCE

CPD COURSES

PRACTITIONER LED.
PRACTICAL SKILLS.
REAL WORLD.



LEARN.
PRACTISE.
APPLY.
LEVEL UP.

COURSE BROCHURE 2026-27

COURSE BROCHURE 2026–27

What's inside.

SIX SECTIONS · FIFTEEN COURSES · ONE FICTIONAL CITY

01 · WELCOME TO CYBERLY

The city, the Bureau, and the villains who keep us interesting

Pages 04 → 09

02 · HOW WE TEACH

First principles, by hand, with the people who do the work

Pages 10 → 12

03 · THE COURSES

Fifteen courses across six clusters. Pick one, stack a few, or build a pathway

Pages 13 → 28

04 · WHERE YOU'LL LEARN

Labs, scene rooms, Faraday cages, and the rest of the ECS estate

Pages 29 → 30

05 · LOOKING AFTER YOU

Trauma-informed teaching, adjustments, and where to turn if it gets heavy

Pages 31 → 32

06 · GET IN TOUCH

Booking, pricing, FAQs, and the four steps from email to enrolled

Pages 33 → 36

SECTION ONE

01

WELCOME TO CYBERLY.

A purpose-built fictional city where every device has a story, every case lands in context, and nobody ever has to learn forensics on someone's worst day. This is where you'll spend the next fifteen courses.

04 The City

05 Town Map

06 B.Y.T.E.

07 A Letter from Pixelington

08 Rogues' Gallery

09 Marmalade's Note

01

WHO WE ARE

THE FICTIONAL CITY

Cyberly World.

"EVERY BYTE HAS A STORY" · CYBERLYHQ.CO.UK

Cyberly is the fictional investigation universe we built ourselves. Founded in 1842 somewhere in the heart of England. Quietly innovative, fond of tea, suspiciously well-supplied with clever cats. Now home to one of the country's most active digital forensics ecosystems, several questionable AI experiments, and a holding company that pretends to be a consultancy.

Every CPD course you'll find in this brochure is set inside Cyberly. So is much of our research, our student work, and our outreach. Visiting researchers borrow from it. Practitioners come back to it. It is, quietly, the most important thing this lab has built.

WHY IT EXISTS

Forensics training and research usually means exposing learners and staff to real distressing material. We refused that trade-off. Cyberly lets us teach hard skills, push deep into research questions, and never compromise the rigour or the wellbeing of the people doing the work.

WHAT IT ACTUALLY IS

A mapped, populated, plausible city with its own laws, institutions, and recurring characters. Synthetic devices that behave like real ones. Cases that evolve. IoT environments that mirror our physical scene room. A research-grade sandbox.

🏛 B.Y.T.E.

Bureau of Yotta-byte Technical Examination. Cyberly's elite digital investigation agency, led by Lord Pixelington. When you train with us, you train as B.Y.T.E.

😈 V.V.I.

Villainous Ventures Inc. Officially a consultancy. Actually a chaotic collective of cohorts led by Professor Phoenix Marmalade. Servers buried beneath Biscuit Borough.

1842	15	16+	404	∞
FOUNDED	CPD COURSES	CHARACTERS	FM RADIO	TEAPOTS

01

THE MAP

A SHORT TOUR OF TOWN

The Map.

A WORKING CITY, DRAWN TO SCALE (MOSTLY)

Cyberly has districts, landmarks, and a public transport system that occasionally tells the truth. The map below is a starting point. Names will become familiar over the course of any training week you spend with us.

1 BISCUIT BOROUGH

Old town. Cobbled. Suspicious number of bakeries. Reputedly conceals VVI's primary server farm beneath the high street.

2 B.Y.T.E. HQ

High-tech but cosy. Headquarters of the Bureau. Visitors arrive via the polished brass lifts; investigators via the back stairs.

3 VVI HQ

Glass-walled, suspiciously well-funded. Hosts an annual gala that always coincides with a major incident elsewhere.

4 CYBERLY UNI

Run by Professor Normal. Publishes papers. Provides VVI with a steady supply of plausibly-deniable interns.

5 404 FM STUDIO

Barely-regulated radio. Broadcasts on every known frequency and several unknown ones. Soundtrack for every late-night USB recovery.

6 MAYOR'S OFFICE

Mayor Dina Brave. Suspiciously close to the train station. Maintains a working firewall and an open biscuit policy.

The full interactive map lives at cyberlyhq.co.uk. The version above is the one you'll see on the wall during training.

01

B.Y.T.E.

THE GOOD SIDE

B.Y.T.E. Detective Agency.

BUREAU OF YOTTA-BYTE TECHNICAL EXAMINATION · EST. 1842

Where tradition meets technology in the heart of Cyberly. Led by Lord Pixelington, the agency specialises in untangling the kind of digital mysteries that nobody else can quite get their head around. Old-school detective savvy. Cutting-edge tech. A surprisingly good biscuit cupboard.

Every case is treated as a puzzle. No villain, not even the notorious Professor Marmalade, has yet outsmarted the collective wit. When you train with us, you don't train towards B.Y.T.E. You join it. Every course adds a stamp on the digital ID card, and every case file you close earns a place in the agency archives.

THE DIRECTOR

Lord Pixelington runs B.Y.T.E. with old-fashioned courtesy and a frankly modern grasp of cryptography. Believes every case can be cracked given enough biscuits and proper note-taking. Has signed off on every recruit reading this brochure.

THE MISSION

Safeguard Cyberly's future, one byte at a time. Solve the rogue AI cases. Untangle the smart-fridge extortion rings. Catch Marmalade red-handed (eventually). Document everything. Train the next generation.

THE CYBERLY OATH

"Analyse with context. Brew tea before panic. Keep biscuits for morale, not evidence. And foil Villainous Ventures before they get the last laugh."

— MAYOR DINA BRAVE, ON THE DAY B.Y.T.E. WAS FORMALLY FOUNDED

01

LETTER

FROM THE DESK OF

A letter from Pixelington.

B.Y.T.E.

BUREAU OF YOTTA-BYTE TECHNICAL EXAMINATION · CYBERLY

Office of the Director

REF: BYTE/2026/IN-001

Dear Investigator,

If you are reading this, the recruitment process has flagged you. Good. We need you.

Cyberly is, broadly speaking, a wonderful city. Trams that mostly run on time. Tea shops on every corner. Cats with the soft, suspicious confidence of small spies. We also have a persistent problem in the shape of a holding company called **Villainous Ventures Incorporated**, and the woman who runs it, Professor Phoenix Marmalade.

She is clever. Her cohorts are cleverer than they look. Their devices are weirder than anything you've seen, their data destruction is more imaginative than the textbooks cover, and their corporate paperwork is, frustratingly, almost in order. Almost.

That is where you come in. Over the coming pages you will find fifteen courses. Each one is taught by a working practitioner, from first principles, with you at the keyboard for more than half the time. Every one of them unfolds inside Cyberly, which means real rigour, fictional victims, and a B.Y.T.E. badge waiting at the end.

Marmalade thinks she is untouchable. We know better. We know you'll crack the case.

Pixelington

Lord Reginald Pixelington III

DIRECTOR · BUREAU OF YOTTA-BYTE TECHNICAL EXAMINATION

01

ROGUES

AGENTS OF MAYHEM · VVI LINE-UP

The Rogues' Gallery.

SIXTEEN COHORTS. EVERY ONE A TEACHABLE MOMENT.

Villainous Ventures Inc. claims to be a consultancy. It is, in fact, a flat-structured collective of remarkably specialised people. You will meet them, gradually, across the fifteen courses ahead. Each one's specialism connects to a teachable forensic skill.

VVI · 01 · THE SCIENTIST

Prof. Phoenix Marmalade

"It's not a trap. It's a teaching moment with mild fire risks."

SPECIALISM

Forensic metadata weaponised. Dollhouse crime scenes. Glitter-trail incident response.

VVI · 02 · THE HACKER

Silent Si

"I don't lift for strength. I lift for access."

SPECIALISM

CCTV image analysis. Server-squatting. Spotting compression artefacts at fifty feet.

VVI · 03 · THE DEMOLITIONIST

Explosive Anne

"Oh fluff it, just hand me the taser and stand back."

SPECIALISM

Improvised EMPs. Creative taser deployment. Performance-art entry techniques.

VVI · 04 · THE MAGICIAN

Fidget Fingers

"It's not stealing if I use my magic wand."

SPECIALISM

Lockpicks. Sleight of hand. Reverse-shoplifting. Smartwatch swaps with biscuit trackers.

VVI · 05 · THE ARCHITECT

Blueprint Betty

"Why would I want my secrets wafting about with the weather?"

SPECIALISM

Architectural mischief. Corridor confusion. Hides things "somewhere obvious but not too obvious."

VVI · 06 · THE COUNSEL

Savvy Steph

"Technically, morally, and alphabetically... I win."

SPECIALISM

Cyberlaw loopholes. Regulatory misdirection. Emotionally persuasive PowerPoint.

VVI · 07 · THE FINANCIER

Data Dave

"I just encouraged the leaderboard to reflect reality."

SPECIALISM

Data integrity manipulation. Pivot tables of sabotage. Beautiful, statistically-sound charts.

VVI · 08 · THE DETECTOR

Pulse Reader Paul

"I made the data too intelligent to be found."

SPECIALISM

Regex sorcery. Pattern detection. Behavioural analysis. Codes in Perl by candlelight (allegedly).

Continued on the next page ⟶

01

ROGUES

AGENTS OF MAYHEM · CONTINUED

...and friends.

VVI · 09 · THE ENIGMA

Mr. Scott

"Just because we're villains doesn't mean we don't have feelings. Or anxiety."

SPECIALISM

Mental health in high-stress environments. Burnout-proofing teams. Compassionate incident response.

VVI · 10 · THE PLANNER

Clue-Hoarder Chris

"So many vulnerabilities hiding in plain logic."

SPECIALISM

Multi-layered strategy. Scriptable sabotage. Recursive to-do lists that work.

VVI · 11 · THE ORACLE

Just John

"I joined for the pension and the rooftop BBQ permissions."

SPECIALISM

Data acquisition. Evidence recovery. Slow-smoked brisket. Teaching Labs to fetch USBs.

VVI · 12 · THE MECHANIC

Trickster V

"If it has wheels, wires or warnings, I can break it."

SPECIALISM

Vehicle tech. National infrastructure. Once jail-broke a bus. Cannot pass a broken escalator.

VVI · 13 · THE IMPERSONATOR

Chameleon Charles

"Did I arrive, or did I sell you a convincing replica?"

SPECIALISM

Social engineering. Biometric bypass. Blending into corporate events like a well-dressed spreadsheet.

VVI · 14 · THE DECEPTOR

Decoy Diana

"Truth is a narrative without a good stylesheet."

SPECIALISM

Digital illusions. Synthetic logs. Rewriting reality one pixel at a time.

VVI · 15 · THE APPRENTICE

Circuitbreaker Josh

"If I solder this, does it count as work or sabotage?"

SPECIALISM

Microcontroller mischief. Wireless wizardry. Villain-tech bootstrapped from IKEA lamps.

VVI · 16 · THE FIXER

CodeMac Jimbob

"Wait, did that hex dump just make sense?"

SPECIALISM

Hex analysis. Command-line sorcery. Quietly carrying the entire team and never claiming credit.

+1

PROFESSOR NORMAL

Head of Cyberly Uni · Honorary VVI. Technically the most powerful academic in town. Funds half their experiments. Always publishes just before they explode.

TOP SECRET

To whom it may concern.

(And by "concern", I mean **deeply**, **personally**, and ***permanently***.)

So. You've signed up to chase me, have you? How darling. How *persistent*. How very **SherFox** of you.

Let me save you some time, sweetheart. I have devices you've never heard of. I have data destruction techniques your tools weren't built for. I have a cohort of accomplices, a perfectly-laundered corporate structure, and a tea blend that would soften you up if you'd just ***sit down***.

You'll be told my henchpeople are sneaky. They are. You'll be told the cases get harder. They do. You'll be told Cyberly's Bureau of Yotta-byte Technical Examination is the finest agency in the city. **Frankly**, well, frankly they're alright I suppose, if you like that sort of thing.

But you, in particular, are going to be a ***problem***. I can tell. Pixelington always picks the irritatingly capable ones.

Enjoy your training. Crack a case or two. Enjoy your little fox mascot and your little hexadecimal editor. Just know that I'll be watching from somewhere very comfortable, sipping something expensive, and plotting something **extraordinary**.

— and do mind the cheese.

P. Marmalade

Professor Phoenix Marmalade

CEO · Chaos Architect-in-Chief · Villainous Ventures Inc.

SECTION TWO

02

HOW WE TEACH.

First principles, by hand, taught by people who still do the work. We teach the why before the tool. We expect you at the keyboard. We don't hide behind automation and we don't pretend a vendor parser is a substitute for understanding.

12 Our Approach

02
APPROACH

WHAT MAKES OUR TRAINING DIFFERENT

First principles. By hand.

NO TOOL-TOUR SHORTCUTS · NO VENDOR SCRIPTS · NO BLACK BOXES

Most digital forensics training teaches you a tool. We teach you the underlying science. The artefacts, file structures, binary, the why. When the tool changes, when the parser breaks, when the vendor pulls support, you still know what you're looking at.

🔬 FIRST PRINCIPLES

Knowledge that survives the next OS update, vendor pivot, parser discontinuation. You'll learn what is happening inside the device, not how to click through somebody else's wizard.

✋ BY HAND, NOT BY AUTOMATION

Hex editor, small scripts, manual timestamp cross-referencing. Automated suites have their place, but they don't build practitioners. Doing the work does.

⌨️ OVER HALF THE TIME AT THE KEYBOARD

Live practicals on real evidence with fictional victims. Small cohorts. Instructors stand behind you and watch what you actually type.

👩‍💻 PRACTITIONER-LED

Every course taught by someone with active casework experience. They know why a step matters because they watched it matter on a real case last week.

🧠 TRAUMA-INFORMED

Every course runs inside Cyberly. Realistic technical challenge, fictional victims, zero exposure to real distressing material. Rigour without the cost.

🗓 12 MONTHS ACCESS

You leave with the take-away pack and 12 months online access to materials, datasets and practice environments. Forensics knowledge sticks when you can practise it again three months later.

WHY WE STILL BUILD IT BY HAND

"Automation is useful, but it leaves a trace. We want our evidence to feel like it came from a bad day in a real life. So we build it ourselves, timestamp by timestamp."

— PROF. SARAH MORRIS, FOUNDER, SHERFOX LABS

SECTION THREE

03

THE COURSES.

Fifteen practitioner-led CPD courses across six clusters, three to eight days each. Set inside Cyberly. Taught from first principles. Designed to be stacked, sequenced, or taken on their own. Pricing from £2,600 to £4,500.

14 Course Map

15 Foundation

16 Device

19 Scene

22 Technical

28 Advanced

03
COURSES

FIFTEEN COURSES · SIX CLUSTERS

At a glance.

FOUNDATION · DEVICE · SCENE · TECHNICAL · ADVANCED · COMMUNICATION

Every course set inside Cyberly. Every course taught by a working practitioner. Every course built from first principles, by hand. Stack them into a pathway or take one to fix a gap.

🏗 FOUNDATION

Digital Forensic Essentials · 8 days · p15

💾 DEVICE FOCUSED

Data Capture Wizard · 5 days · p16
Mobile Sleuth · 3 or 5 days · p17
IoT Inspector · 5 days · p18

🏛 SCENE ANALYSIS

Scene Specialist · 3 or 5 days · p19
Guardian Eye (CCTV) · 5 days · p20
Security Sentinel · 5 days · p21

🌐 TECHNICAL MASTERCLASS

AppTracker · 5d · p22
Comms Data Analyser · 3 or 5d · p23
Cyber Sleuth · 5d · p24
Document Detective · 5d · p25
Multimedia Marvel · 5d · p26
Open Source Intel Operative · 5d · p27

🎓 ADVANCED SKILLS

Digital Forensics Masterclass · 5 days · p28

🎤 COMMUNICATION

Evidence Articulator · 3 or 5 days · p28

Pricing £2,600–£4,500 · bursaries available for independents, alumni, SMEs and unemployed practitioners · see page 33 for booking.

03

FOUNDATION

🏗 FOUNDATION CLUSTER — 8 DAYS

THE ONE COURSE EVERY INVESTIGATOR NEEDS FIRST

Digital Forensic Essentials.

FROM HEX TO HISTORIES · THE SCIENCE BEFORE THE TOOLCHAIN

If you do one course with us, do this one first. Eight days that take you from "I think I know what a partition is" to running a basic technical investigation yourself, from acquisition through to writing it up. By the end of week two you'll be reading raw hex with confidence and tracing a filesystem artefact back to the user behaviour that produced it.

"It was where everything else started to make sense." — past learner, returning for the masterclass

YOU'LL LEAVE ABLE TO

- Speak fluent digital forensics: terminology, concepts, the lot
- Read raw hex and walk it back to filesystem artefacts
- Recognise common data constructs and storage media in the wild
- Identify key operating system artefacts of evidential value
- Apply structured investigative strategies to first-cut forensic problems
- Write a clean, defensible case note that survives review

WHAT YOU'LL WORK THROUGH

- Forensic principles and methodology, end-to-end
- Data structures, storage media, partitioning by hand
- Filesystems, their quirks, their artefacts
- Operating system artefacts that matter most
- Binary, decimal, hexadecimal conversion at the keyboard
- Investigative strategy and case workflow
- Live practicals throughout, fresh Cyberly case files each day

PRIOR KNOWLEDGE None required. General computer familiarity is helpful. Pre-course materials cover number-system conversion and basic hex editing, recommended if either is new to you.

03
DEVICE

💾 DEVICE FOCUSED · COURSE 1 OF 3 — 5 DAYS

ACQUISITION DONE PROPERLY THE FIRST TIME

Data Capture Wizard.

STORAGE MEDIA · COMMON, HISTORIC, EMERGING, UNUSUAL

Acquisition is where every case stands or falls. Get it wrong here and nothing downstream can rescue it. This course makes sure you don't. Five days of hands-on work across common storage, legacy formats, emerging media, and the awkward edge cases that the textbooks gloss over. By the end of the week you'll know exactly what to do when a colleague hands you a device and says "we've never imaged one of these before."

Includes chip-off, JTAG, integrity verification, and what to do with the drive that nobody else could image.

YOU'LL LEAVE ABLE TO

- Apply forensic acquisition principles to a wide range of media
- Choose the right hardware approach for the device in front of you
- Use chip-off and JTAG techniques where appropriate
- Acquire wireless and networked data without losing the evidential thread
- Verify integrity across the acquisition process and report it cleanly
- Handle legacy and unusual formats with confidence

WHAT YOU'LL WORK THROUGH

- Acquisition principles and chain of custody
- Common, historic, emerging and unusual storage media
- Mobile device acquisition considerations
- Wireless data acquisition and validation
- Hardware-level approaches: chip-off, JTAG
- Legacy and unusual formats; integrity verification

PRIOR KNOWLEDGE Confidence with hex editors and command line tools is expected. A solid grounding in digital forensic fundamentals is required (Digital Forensic Essentials covers it).

03
DEVICE

💾 DEVICE FOCUSED · COURSE 2 OF 3 — 3 OR 5 DAYS

PHONES ARE WHERE MOST MODERN CASES LIVE

Mobile Sleuth.

MOBILE DEVICES · SIM-ERA THROUGH TO CURRENT GENERATION

Phones change every six months. We keep up so you can. Mobile is where most modern investigations end up sooner or later, and it's the area where vendor tools struggle most. Three-day general or five-day deep dive, both built around hands-on extraction, manual artefact analysis, and the kind of work that makes you the person colleagues call when their commercial parser gives up.

"Three-day general" for incident responders. "Five-day deep" for those who'll be reviewing the tricky cases.

YOU'LL LEAVE ABLE TO

- Conduct forensic acquisition and extraction across modern mobile devices
- Read core artefacts across common and bespoke mobile operating systems
- Analyse application data, messaging and communications
- Apply investigative strategies to legacy and current generation devices
- Recognise when hardware approaches are warranted, and use them safely

WHAT YOU'LL WORK THROUGH

- Mobile device architecture and evidence sources
- Acquisition methods for historical and modern devices
- SIM-card devices and associated metadata
- App data and communication artefact analysis
- Bespoke and adapted operating systems
- Hardware approaches where appropriate (JTAG, chip-off)
- Reporting and evidential considerations

PRIOR KNOWLEDGE Confidence with hex editors and command line tools is expected. Solid understanding of digital forensic fundamentals required.

03
DEVICE

💾 DEVICE FOCUSED · COURSE 3 OF 3 — 5 DAYS

FOR WHEN NOBODY HAS IMAGED ONE OF THESE BEFORE

IoT Inspector.

UNUSUAL DEVICES · UNDOCUMENTED HARDWARE · THE EDGE OF WHAT'S KNOWN

Vehicles. Washing machines. Doorbells. Fridges. The genuinely-weird-and-undocumented. When the device in your evidence bag has no manual, no commercial parser, and no community write-up, you need a research method, not a wizard. This course teaches that method. Five days of hands-on work with the kit, the wireless protocols, and the lateral thinking that finds the firmware nobody else thought to extract.

If it plugs in and nobody's written the manual yet, this is the course that gets you in anyway.

YOU'LL LEAVE ABLE TO

- 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

WHAT YOU'LL WORK THROUGH

- IoT fundamentals and the forensic challenges they present
- Wireless protocols and data acquisition methods
- Vehicles, washing machines, alarms, home assistants
- Research approaches for undocumented or unusual devices
- Security, privacy and ethical considerations
- Hardware-level approaches where applicable
- Case studies from the genuinely strange end of the spectrum

PRIOR KNOWLEDGE Confidence with hex editors and command line tools is expected. Solid understanding of digital forensic fundamentals required.

03
SCENE

🏛 SCENE ANALYSIS · COURSE 1 OF 3 — 3 OR 5 DAYS

WHAT YOU DO IN THE FIRST HOUR SHAPES THE WHOLE CASE

Scene Specialist.

IDENTIFYING, PRESERVING AND RECOVERING DIGITAL EVIDENCE AT A PHYSICAL SCENE

Decisions made in the first hour echo through the rest of the case. Get the scene wrong and your lab work has to swim upstream forever after. Three days for first-responders covering scene management essentials, or five days for those leading scenes and managing teams. Built around our immersive, dressed, instrumented scene room so you spend most of the week on your feet, in the room, making the calls.

Sensible shoes. Evidence bags. We'll provide the rest, including the suspect device that pings at three in the morning.

YOU'LL LEAVE ABLE TO

- 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 pressure
- Conduct hands-on recovery in live environments
- Brief colleagues, communicate decisions, and write up cleanly

WHAT YOU'LL WORK THROUGH

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

PRIOR KNOWLEDGE Digital forensic fundamentals expected. Experience in investigative environments is beneficial but not required.

03
SCENE

🏛 SCENE ANALYSIS · COURSE 2 OF 3 — 5 DAYS

CCTV IS EVERYWHERE, IN ALMOST NO SENSIBLE FORMAT

Guardian Eye.

CCTV RECOVERY AND ANALYSIS FROM SYSTEM TO COURTROOM

Proprietary codecs. Locked exporters. Players that crash silently. The world of CCTV evidence is a minefield of incompatibility and quiet corruption. This course cuts through it. Five days of recovering footage cleanly, converting it without losing a frame, analysing it forensically, and presenting it as evidence that holds up under cross-examination. Everything from a domestic ring doorbell to a 64-channel commercial DVR.

"That file definitely won't play." We'll show you how to make it play.

YOU'LL LEAVE ABLE TO

- Identify evidential opportunities within CCTV and video systems
- Extract, convert and preserve video evidence without data loss
- Analyse and interpret footage in forensic contexts
- Present video evidence under courtroom standards

WHAT YOU'LL WORK THROUGH

- 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 practicals in the immersive scene room
- Evidential continuity and courtroom presentation

PRIOR KNOWLEDGE Digital forensic fundamentals expected. Familiarity with handling digital files is helpful but not essential.

03
SCENE

🏛 SCENE ANALYSIS · COURSE 3 OF 3 — 5 DAYS

FOR WHEN "TAKE IT OFFLINE" ISN'T AN OPTION

Security Sentinel.

CORPORATE SECURITY AND INCIDENT RESPONSE

Incident response in a corporate environment is its own beast. Pressure, politics, a network that absolutely must stay up, and stakeholders who don't speak forensics. Five days on frameworks, triage, containment, and the kind of reporting that lands well with both a board and a barrister. Taught by people who have done it, with the scars to prove it.

By the end of the week you'll write incident reports a regulator can read and a CEO will sign off on.

YOU'LL LEAVE ABLE TO

- 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

WHAT YOU'LL WORK THROUGH

- Incident response frameworks and policies
- Identifying and triaging digital incidents
- Corporate security tools and technologies
- Mitigating and containing active threats
- Insider and external incident approaches
- Communication and reporting in organisational settings

PRIOR KNOWLEDGE Digital forensic fundamentals expected. Familiarity with IT or security operations is beneficial.

03

TECHNICAL

TECHNICAL · COURSE 1 OF 6 — 5 DAYS

MODERN USER BEHAVIOUR LIVES IN APPS AND BROWSERS

AppTracker.

BROWSER AND APPLICATION FORENSICS, BY HAND

Cache, history, cookies, and SQLite databases that change schema every patch. Five days of working through the artefacts manually so you understand what the commercial parser was doing and what it missed. By Friday you'll be reading the SQLite files yourself, mapping the schema, and identifying the rows the vendor tool skipped.

SQLite is your friend. We promise. Eventually.

YOU'LL LEAVE ABLE TO

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

WHAT YOU'LL WORK THROUGH

- 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 app artefacts to wider system activity
- Cross-platform challenges and solutions

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

03
TECHNICAL

TECHNICAL · COURSE 2 OF 6 — 3 OR 5 DAYS

WHO SPOKE TO WHOM, AND WHEN, PROPERLY

Comms Data Analyser.

CDRS, TELECOMS RECORDS, MESSAGING, VOIP, ENCRYPTED SERVICES

Communication data is the timeline backbone of most modern cases. Three days of essentials or five days of depth. You'll build defensible timelines from raw call detail records, pull comms artefacts off devices, correlate them across sources, and write findings that survive scrutiny in court. Modern encrypted messaging has changed the field. We teach what's still possible, what isn't, and how to evidence the difference.

If a barrister asks "and how can you be sure that's the same person on both ends?", you'll have a confident, technically-grounded answer.

YOU'LL LEAVE ABLE TO

- 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

WHAT YOU'LL WORK THROUGH

- Structure and interpretation of call detail records
- 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 expected. Familiarity with basic telecoms data structures is beneficial.

03
TECHNICAL

TECHNICAL · COURSE 3 OF 6 — 5 DAYS

THE PATIENT INTRUSIONS ARE THE HARDEST TO SPOT

Cyber Sleuth.

NETWORK AND CORPORATE INTRUSION INVESTIGATIONS

Traffic captures, log mountains, lateral movement, and the kind of advanced persistent threats that have been sitting quietly in the network since last summer. Five days of finding the thread, pulling it carefully, and writing it up for a non-technical audience without losing technical accuracy. Includes hands-on with realistic Cyberly enterprise environments where you'll triage, contain, and report on a live-ish incident.

By the end of the week you'll have written a report that helps your business actually respond, not just describes what happened.

YOU'LL LEAVE ABLE TO

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

WHAT YOU'LL WORK THROUGH

- 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 Digital forensic fundamentals required. Familiarity with networking concepts and corporate IT environments is recommended.

03
TECHNICAL

TECHNICAL · COURSE 4 OF 6 — 5 DAYS

A DOCUMENT IS ALMOST NEVER JUST A DOCUMENT

Document Detective.

METADATA, HIDDEN CONTENT, REVISIONS, EMBEDDED ARTEFACTS

A Word file is a zip archive with secrets. A PDF is a tree of objects with revision history. A spreadsheet hides macros, named ranges, and that one cell someone forgot to overwrite. Five days inside the file formats — by hand, with hex editors and unzip utilities, not just relying on a parser to tell you what it found. By Friday you'll spot the back-dated draft, the swapped author, and the hidden tab without breaking a sweat.

If you've ever wished a Word file had subtitles, this is the course for you.

YOU'LL LEAVE ABLE TO

- 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

WHAT YOU'LL WORK THROUGH

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

PRIOR KNOWLEDGE Digital forensic fundamentals required. Familiarity with common office software is beneficial.

03
TECHNICAL

TECHNICAL · COURSE 5 OF 6 5 DAYS

WHEN THE IMAGE IS SUSPICIOUSLY PERFECT

Multimedia Marvel.

IMAGE, VIDEO, AUDIO · AUTHENTICATION, MANIPULATION, AI-MEDIA DETECTION

Images, video and audio analysed, authenticated, and questioned. Five days covering EXIF and container metadata, splicing detection, double-compression analysis, and the increasingly important art of spotting AI-generated media before it reaches court. You'll learn the underlying signal-processing concepts, then apply them by hand on Cyberly case files before the toolchain ever opens.

"That photograph is suspiciously perfect." Yes. Quite. Now you'll be able to prove it.

YOU'LL LEAVE ABLE TO

- 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

WHAT YOU'LL WORK THROUGH

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

PRIOR KNOWLEDGE Digital forensic fundamentals required. Familiarity with multimedia formats is helpful.

03
TECHNICAL

TECHNICAL · COURSE 6 OF 6 — 5 DAYS

POWERFUL, WHEN DONE WELL · DISASTROUS, WHEN DONE BADLY

Open Source Intel Operative.

OSINT · ETHICS FIRST, TECHNIQUE SECOND, EVIDENCE LAST

OSINT done badly is a privacy disaster and a courtroom liability. OSINT done well is one of the most powerful investigative techniques there is. Five days on the legal frame, the ethical frame, the technical methods, and how to integrate intelligence findings back into a forensic case without contaminating the chain of evidence. Practitioners arrive with curiosity and leave with a defensible methodology.

Ethics first. Always. Including (especially) when you really, really want to keep going.

YOU'LL LEAVE ABLE TO

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

WHAT YOU'LL WORK THROUGH

- OSINT frameworks and ethical principles
- 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 Digital forensic fundamentals required. No prior OSINT experience necessary.

03

ADVANCED

🎓 ADVANCED SKILLS 5 DAYS

FOR PRACTITIONERS WHO ALREADY KNOW WHAT THEY'RE DOING

Digital Forensics Masterclass.

THE DEEP END · WE SUPPLY THE LIFEGUARD

This is the course for experienced practitioners who want to be tested. Encryption, anti-forensics, volatile data, multi-device correlation, the edge cases that publish papers. Five days of complex investigations drawn from the harder reaches of the field, taught by people who handle Marmalade-level cases for a living. Expect to be challenged. That is the point.

Bring your hardest case. We'll bring three harder ones, and the methods that crack them.

YOU'LL LEAVE ABLE TO

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

WHAT YOU'LL WORK THROUGH

- Advanced acquisition and recovery techniques
- Complex filesystem and operating system artefacts
- Correlation across multiple devices and data sources
- Encryption, anti-forensics, volatile data
- Integrating OSINT, comms and device artefacts
- Case studies from unusual and high-profile investigations

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

03

COMMUNICATION

🎤 COMMUNICATION · PRESENTATION

3 OR 5 DAYS

THE STRONGEST INVESTIGATION CAN STILL FAIL IN THE WITNESS BOX

Evidence Articulator.

REPORTS, TESTIMONY, COMPLEX FINDINGS, PLAIN LANGUAGE

A jury cannot convict on what it doesn't understand. This course builds the written and spoken skills that make complex digital evidence accurate, persuasive, and accessible to whoever has to make a decision based on it. Three days for foundations, five for in-depth practical work including a simulated cross-examination. You'll leave with reports a barrister can read out and answers you can give under pressure without losing your technical footing.

We bring real barristers in for the cross-examination. They are very good at their job.

YOU'LL LEAVE ABLE TO

- Translate complex technical findings into clear, accurate narratives
- Develop written and oral communication for different audiences
- Apply best practices for courtroom and investigative reporting
- Articulate digital evidence with confidence under scrutiny

WHAT YOU'LL WORK THROUGH

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

PRIOR KNOWLEDGE Digital forensic fundamentals required. Some prior exposure to reporting or professional communication is beneficial but not essential.

SECTION FOUR

04

WHERE YOU'LL LEARN.

SherFox sits inside the School of Electronics and Computer Science at the University of Southampton. Operational labs, research labs, scene rooms, Faraday cages, anechoic chambers, vehicle bays, and 100-to-180 seat teaching theatres. If a course needs a specialist environment, we have it on campus.

31 Facilities

04
FACILITIES

WHERE THE WORK HAPPENS

UoS Facilities & Labs.

SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE · UNIVERSITY OF SOUTHAMPTON

As part of one of the UK's leading centres for cyber and forensics, SherFox has access to a flexible, powerful and highly capable infrastructure that supports teaching, research and operational activity. Significant ongoing investment by ECS and the University.



OPERATIONAL LABORATORY

Fully equipped to handle evidential material and support global casework. Current digital forensic hardware and software for computer-based analysis. Specialist electronic and embedded capabilities including chip-off, JTAG, and vehicle forensics. Operates under established evidential handling and provenance principles.



RESEARCH LABORATORY

Mirrors the operational lab. Available to trained students and staff for practice-informed research using professional-grade equipment. Where our home-built tools are tested before they touch a real case.



SCENE AND IOT ENVIRONMENT

Immersive, dressed, instrumented scene room used for teaching, research and operational simulation. Doubles as an escape-room-style space for realistic scenario-based training. The CCTV and Scene Specialist courses both live here.



WIDER UNIVERSITY ACCESS

Faraday cages and anechoic chambers, both on-site and in dedicated lab spaces. Vehicle bays, high-power and high-voltage rigs, biomedical and sensor labs. Teaching laboratories seating 100 to 180 students with custom PCs, distributed screens and integrated AV. If a course needs a specialist environment, we have it on campus.

Bespoke. Flexible. Adaptable. From the eight-day Essentials cohort right through to the masterclass weirdness, every room can be re-dressed for the course at hand. Custom requirements welcome.

SECTION FIVE

05

LOOKING AFTER YOU.

The work can be heavy. So we balance it with humour, colour, and more than a hint of cheesiness. We also take adjustments, accessibility, and mental health seriously. Tell us what you need and we'll work with you to make the course fit.

33 Trauma-Informed

34 Adjustments and Access

05

WELLBEING

WHY WE BUILT CYBERLY IN THE FIRST PLACE

Trauma-informed by design.

HARD SKILLS · SAFE SPACE · RESOURCES WHEN YOU NEED THEM

Digital forensics training has traditionally meant exposure to real distressing material. We refused that trade-off. Cyberly lets us teach hard skills and run serious research without compromising on rigour, or on the wellbeing of the people doing the work.

Every CPD course you'll find in this brochure unfolds inside Cyberly. The artefacts are technically representative. The cases are inventive and demanding. The victims are entirely fictional. Nobody real is being harmed for the sake of your learning, and that matters.

WHAT THIS LOOKS LIKE IN PRACTICE

No graphic content. No real victim data. Optional debriefs after harder sessions. Quiet spaces on site. Sensible class sizes. Instructors who know the work and who'll spot when somebody is finding the day heavier than expected. Conversations that stay private if you want them to.

IF THE WORK TAKES A TOLL

Looking after yourself in this field is part of the job, not a sign of weakness. If you need support, the following are good first ports of call. Talk to your supervisor too, and to us during the course if anything is sitting badly.

SAMARITANS

116 123 · samaritans.org · 24/7, free, confidential

MIND

mind.org.uk · mental health charity · information, advice, local services

OSCAR KILO

Police wellbeing services · oscarkilo.org.uk · psychological support for policing

UK COPS

Care of Police Survivors · ukcops.org · support for families of officers who lost their lives

05

ACCESS

EVERY LEARNER MATTERS, EVERY ADJUSTMENT COUNTS

Adjustments & access.

TELL US WHAT YOU NEED · WE'LL MAKE IT WORK

Every learner should feel safe, included, and able to succeed. If you have a disability, learning difference, additional needs, or you're new to the field, we'll work with you to make the course fit. The questions below cover the common ones. If yours isn't here, email us.

Q · I have a disability or long-term condition. Can you provide adjustments?

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

Q · I get anxious in busy spaces or prefer lower sensory environments. What support is there?

Sensible class sizes, daily plans outlined in advance, expectations made clear. Arrive early to settle in. Choose a quieter seat. Take breaks whenever you need. We use Cyberly datasets rather than graphic real-world material. Questions can be submitted privately.

Q · 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.

Q · How do I request an adjustment?

Email us after your identity check with a short description of what you need and what's helped you before. We'll agree a plan in writing

Q · I have dysle

Courses use clea primers, plain-la we avoid surpris

Q · I'm not from

Yes. Many learne first principles ar

Q · Can I attend

Selected course online and what

SECTION SIX

06

GET IN TOUCH.

Courses aren't listed publicly, for security reasons. Every booking starts with an email. Four steps from first contact to confirmed enrolment, and you'll never get an automated reply from us. We're academics. Patterns vary. Tea always available.

36 Booking and Pricing

37 Contact

06

BOOKING

FROM EMAIL TO ENROLLED IN FOUR STEPS

How to book.

IDENTITY CHECK · SKILLS CHECK · BOOK YOUR PLACE

Courses aren't publicly listed. For security and safety reasons, dates and locations are shared after a brief identity check. Corporate email preferred for first contact. Free-email enquiries are verified before we share course details.

GET IN TOUCH 01

Email us with your enquiry and the course(s) you're interested in. Corporate email preferred. A real person reads each one.

IDENTITY CHECK 02

For security, we confirm who you are before sharing dates, locations and details. Quick, friendly, and over by the time the kettle boils.

SKILLS CHECK 03

A short online check, around five minutes, so we can recommend the right course at the right level for you. Honest answers help.

BOOK YOUR PLACE 04

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

KEY INFORMATION

🔒 ACCESS TO MATERIALS

12 months online access after your course, plus a downloadable take-away pack for permanent reference.

💻 VIRTUAL DELIVERY

Available for selected courses. Ask which when you enquire and we'll be honest about what works.

👥 BOOKING OPTIONS

Individual, bulk, or dedicated. Groups of six or more can be delivered at SherFox or on-site at your organisation.

💷 PRICING

£2,600–£4,500 depending on content and duration. Bursaries available for independents, alumni, SMEs, unemployed practitioners, and existing ECS relationships.

06

CONTACT

EVERY ROUTE STARTS WITH AN EMAIL

Start the conversation.

REAL PEOPLE · REAL REPLIES · WRITTEN BY HUMANS, SENT BY HUMANS

Whether it's "I'd like to book Mobile Sleuth for our team," or "we have a weird device and we don't know what to do," or "tell me more about Cyberly," we'd like to hear about it.

✉

EMAIL

hello@sherfoxlabs.com

📞

PHONE

+44 23 8059 3441

🌐

WEB

sherfoxlabs.com · cyberlyhq.co.uk · craftyfoxforensics.com · rolodex.cyberlyhq.co.uk

🔗

LINKEDIN

linkedin.com/company/sherfox-labs

📍

POST

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

⏰ ABOUT OUR HOURS

We're academics, so patterns vary. The shared inbox is normally monitored 10:00–16:00 UK Mon–Fri. Urgent? Put "URGENT" in the subject line.

🔒 ON SECURITY

Please don't send live case data on first contact. Once we know what we're handling we'll arrange SFTP or an encrypted archive.

We like conversations. Send us yours.

"Brains, heart, & a touch of cheese." 

SherFox Labs.

DIGITAL FORENSICS · EXPLOITATION · INTELLIGENCE

UNIVERSITY OF SOUTHAMPTON · ECS · EST. 2022

sherfoxlabs.com · cyberlyhq.co.uk