



CRIMINAL INVESTIGATION, ANALYSIS AND DIGITAL TRACING TRAINING COURSE

REF: #LAW85228835



COURSE INTRODUCTION / OVERVIEW:

Modern crime no longer leaves its traces only at a physical scene; it also leaves digital footprints across phones, computers, cloud accounts, financial systems, social media platforms, and communication networks. This intensive five-day program equips investigators and analysts with an integrated approach that connects classic criminal investigation methods with advanced crime analysis and digital tracing techniques. Participants learn how to plan an investigation from the first report, manage a crime scene, collect and preserve physical and digital evidence, maintain a defensible chain of custody, and convert raw data into reliable intelligence that supports sound decisions in court. The course draws on the work of Eoghan Casey, whose book *Digital Evidence and Computer Crime* remains a foundational reference for digital forensics, as well as the investigative reasoning principles of Brent E. Turvey in *Criminal Profiling*. Through realistic scenarios, attendees practice link analysis, timeline reconstruction, open source intelligence (OSINT) investigation, mobile and network forensics, cryptocurrency and financial flow tracing, and suspect behavior analysis. Delivered by BIG BEN Training Center, the program balances legal, ethical, and procedural requirements with hands-on analytical skills, helping professionals build cases that are accurate, lawful, and persuasive. By the end, participants will be able to follow a crime from the scene to the screen and from the screen to the courtroom with confidence, precision, and professional integrity.

TARGET AUDIENCE / THIS TRAINING COURSE IS SUITABLE FOR:

- Criminal investigators and detectives.
- Crime analysts and intelligence analysts.
- Digital forensic examiners and cybercrime investigators.
- Police officers and law enforcement supervisors.
- Public prosecutors and legal investigators.
- Fraud examiners and financial crime investigators.
- Internal audit and compliance investigators.
- Security managers and corporate investigators.
- Crime scene officers and evidence custodians.
- Anti-money laundering analysts.
- Newly appointed investigators seeking structured professional development.



TARGET SECTORS AND INDUSTRIES:

- Government agencies, ministries of interior, public prosecution offices, and equivalent public authorities.
- Police, border security, and customs authorities.
- Banking, insurance, and financial services institutions.
- Telecommunications and internet service providers.
- Judicial and legal institutions.
- Defense and national security organizations.
- Energy, oil, and gas companies with high-value assets.
- Retail and e-commerce companies facing fraud risks.
- Healthcare institutions handling sensitive personal data.
- Aviation, ports, and logistics organizations.

TARGET ORGANIZATIONS DEPARTMENTS:

- Criminal investigation departments.
- Crime analysis and intelligence units.
- Digital forensics and cybercrime units.
- Legal affairs and prosecution departments.
- Internal audit and investigations departments.
- Compliance and anti-money laundering departments.
- Corporate security departments.
- Risk management departments.
- Information security departments.



COURSE OFFERINGS:

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

- Plan and manage a criminal investigation from the initial report to case closure.
- Apply professional crime scene procedures for physical and digital evidence.
- Preserve evidence integrity and maintain a legally defensible chain of custody.
- Use crime analysis techniques such as link analysis, pattern analysis, and timeline reconstruction.
- Conduct lawful and ethical open source intelligence (OSINT) investigations.
- Trace digital footprints across devices, networks, email, and social media.
- Follow financial and cryptocurrency transactions to identify hidden suspects and assets.
- Analyze suspect behavior and apply structured interviewing techniques.
- Recognize and reduce cognitive bias in investigative reasoning.
- Prepare clear investigation reports and present evidence convincingly in court.

COURSE METHODOLOGY:

This course follows a practical, case-driven methodology that mirrors the real workflow of a criminal investigation. Each day combines short expert presentations with guided exercises, so participants immediately apply what they learn rather than simply hearing about it. Realistic case studies drawn from fraud, cybercrime, organized crime, and violent crime investigations form the backbone of the program, allowing participants to analyze evidence, identify leads, and test hypotheses in a safe learning environment. Teamwork plays a central role: participants work in investigation teams that receive a developing case file, divide responsibilities, share findings, and build a coherent picture of events, just as task forces do in practice. Interactive sessions include crime scene simulations, link analysis charting, timeline reconstruction exercises, OSINT search challenges, and role-play interviews with suspects and witnesses. Group discussions encourage participants to compare investigative decisions, debate legal and ethical dilemmas, and learn from the experience of colleagues from different sectors. Throughout the program, the trainers at BIG BEN Training Center provide continuous, constructive feedback on analytical reasoning, evidence handling, and report writing, helping each participant strengthen weak points and refine strong ones. The course concludes with an integrated capstone exercise in which teams investigate a complete case and present their findings as they would before a prosecutor or court panel.



COURSE AGENDA (COURSE UNITS):

UNIT ONE: FOUNDATIONS OF CRIMINAL INVESTIGATION AND CASE MANAGEMENT

- The role and objectives of modern criminal investigation.
- Legal frameworks, jurisdiction, and the rights of suspects and victims.
- Types of investigations: reactive, proactive, and intelligence-led.
- Developing an investigation plan and setting lines of inquiry.
- Case management, task allocation, and documentation standards.
- The investigative mindset and the scientific method in investigation.
- Recognizing cognitive bias, tunnel vision, and confirmation bias.
- Ethics, integrity, and accountability in investigative work.

UNIT TWO: CRIME SCENE MANAGEMENT, EVIDENCE COLLECTION, AND CHAIN OF CUSTODY

- Securing and assessing the crime scene.
- Systematic search patterns and scene documentation.
- Identifying, collecting, and packaging physical evidence.
- Identifying and seizing digital devices at the scene.
- Principles of digital evidence preservation and forensic imaging.
- Chain of custody procedures and evidence integrity.
- Admissibility of evidence and common legal challenges.
- Working with forensic laboratories and specialist experts.



UNIT THREE: CRIME ANALYSIS AND INVESTIGATIVE INTELLIGENCE

- The intelligence cycle and its application to investigations.
- Link analysis and mapping criminal networks.
- Timeline reconstruction and event sequencing.
- Crime pattern analysis and hotspot identification.
- Communication data and call detail record analysis.
- Hypothesis development and the analysis of competing hypotheses.
- Source evaluation and information reliability grading.
- Presenting analytical products to decision makers.

UNIT FOUR: DIGITAL TRACING AND OPEN SOURCE INTELLIGENCE (OSINT)

- Understanding digital footprints and digital identities.
- Lawful and ethical OSINT investigation principles.
- Investigating social media accounts and online profiles.
- Tracing IP addresses, domains, and email headers.
- Mobile device forensics and location data analysis.
- Network and cloud evidence for investigators.
- Tracing financial flows, money laundering, and cryptocurrency transactions.
- Dark web awareness and emerging cybercrime trends.

UNIT FIVE: SUSPECT INTERVIEWING, REPORTING, AND COURTROOM PRESENTATION

- Behavioral analysis and understanding offender motivation.
- Planning and conducting investigative interviews.
- Interviewing witnesses, victims, and suspects ethically.
- Detecting inconsistencies and evaluating statements.
- Writing clear, accurate, and structured investigation reports.
- Preparing evidence files for prosecution.
- Giving testimony and presenting digital evidence in court.
- Capstone exercise: investigating a complete case from scene to courtroom.



FAQ:

QUALIFICATIONS REQUIRED FOR REGISTERING TO THIS COURSE?

There are no requirements.

HOW LONG IS EACH DAILY SESSION, AND WHAT IS THE TOTAL NUMBER OF TRAINING HOURS FOR THE COURSE?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

SOMETHING TO THINK ABOUT:

When a digital trace points strongly to a suspect while the physical evidence remains silent or contradictory, how should an investigator decide which story the evidence is really telling, and how can that decision stay free from the bias created by the first strong lead?

WHAT UNIQUE QUALITIES DOES THIS COURSE OFFER COMPARED TO OTHER COURSES?

This course stands apart because it treats criminal investigation, crime analysis, and digital tracing as one connected discipline rather than three separate specialties. Many programs teach crime scene work without digital evidence, or digital forensics without investigative reasoning; this program shows participants how a single case moves between the physical and digital worlds and how every piece of evidence must fit into one coherent, lawful narrative. The focus is on insight and judgment rather than on tools: participants learn how to ask the right questions, test competing hypotheses, recognize their own cognitive biases, and evaluate the reliability of every source. Practical examples, such as tracing a fraud network through communication records and financial flows, or reconstructing a timeline from mobile location data and witness statements, help participants see how theory becomes action. The program also places strong emphasis on legal admissibility, chain of custody, and ethical OSINT practice, ensuring that the intelligence produced is not only accurate but also usable in court. Delivered by BIG BEN Training Center in an interactive, case-based format, the course ends with a full investigation exercise that brings every skill together, allowing participants to leave with a tested, structured investigative approach they can apply immediately in their own organizations.