Digital Forensics

TRAINING

Unlock the Secrets of Digital Evidence: Discover the Art of Digital Forensics

Facilitated by
MOHAMED ELGHAZOULY

Online
Day 1: Monday, June 10, 2024
Day 2: Monday, June 17, 2024

Overview

In an era marked by a surge in cybersecurity incidents, digital forensics assumes a pivotal role in countering and alleviating the escalating threats. By unraveling the complexities of cyber incidents, digital forensics aids organizations in comprehending vulnerabilities, fortifying security measures, and enhancing incident response capabilities. It not only contributes to the pursuit of justice but also facilitates proactive risk management, empowering organizations to maintain resilience in the face of evolving cybersecurity challenges.

Primarily, this course empowers participants with essential skills to combat the expanding menace of cybercrime. As organizations and individuals confront heightened risks to their sensitive information, proficiency in digital forensics becomes paramount for investigating and combating these crimes. Furthermore, the course addresses legal and investigative requirements by furnishing participants with the knowledge and techniques to adeptly identify, collect, preserve, and analyze digital evidence. This ensures that investigations align with legal and regulatory standards, ensuring the admissibility of digital evidence in legal proceedings.

Through a blend of expert-led presentations, group discussions, practical exercises, and case studies, participants undergo a hands-on learning experience in applying digital forensics concepts and principles. This interactive approach guarantees that participants exit the course equipped with the tools to pinpoint vulnerabilities, implement preventive measures, and respond effectively to security incidents. The course endows them with the skills and knowledge necessary to navigate the intricate realm of digital forensics, safeguard valuable data, and fortify organizations in the contemporary digital age.

Why Attend

- **Gain** essential skills in digital forensics, enabling you to investigate and analyze digital evidence effectively.

- **Stay updated** with the latest techniques and best practices in digital forensics to stay ahead in the evolving field of cybersecurity.

- **Improve** investigation outcomes by learning to navigate digital environments, recover data, and accurately present findings.

- **Enhance** your career prospects with in-demand skills sought after by organizations needing digital forensics expertise.

Learning Objectives

This course will give participants a strong foundation in digital forensics principles, practices, and tools, enabling them to gain a solid foundation in the art of digital forensics. Upon completion, participants will be able to:

- Understand the fundamental concepts and principles of digital forensics.

- Apply industry best practices for identifying, collecting, and preserving digital evidence

- Utilize specialized tools and techniques to analyze digital data and recover deleted or hidden information.

- Conduct investigations involving various digital devices, including computers, mobile phones, and networks.

- Present findings and evidence in a clear, concise manner.

Who Attends

This course is ideal for professionals interested in cyber security, information technology, risk management, compliance, or digital forensic investigations. It is recommended for individuals with some knowledge of IT concepts and operating systems, including:

- **IT Security -** Strengthen incident response and data protection through digital forensics knowledge

- **Incident Response -** Effective handling, analysis, and containment of cybersecurity incidents

- **Digital Forensic Analyst -** Identify, collect, preserve, and analyze data from various digital devices, such as computers, mobile phones, and networks

- **Network administrators -** Identify threats, investigate incidents, and implement network protective controls

- **Security Managers -** Informed decision-making, incident management, and compliance through digital forensics

Meet Your **Facilitator**

MOHAMED ELGHAZOULY

Mohamed is a cyber security Expert, Professor, trainer, executive coach and Security Architect, with extensive forensics and privacy expertise in different industries. He has advised and trained in a wide range of industries from energy, healthcare, banking and finance, education and training, telecom and government.

His most recent roles were as graduate and undergraduate professor for different technical offensive security and forensics.

He established a boutique advisory firm "Galvorn Dome Inc." who is along with the right professionals to be the trusted advisors for clients worldwide.
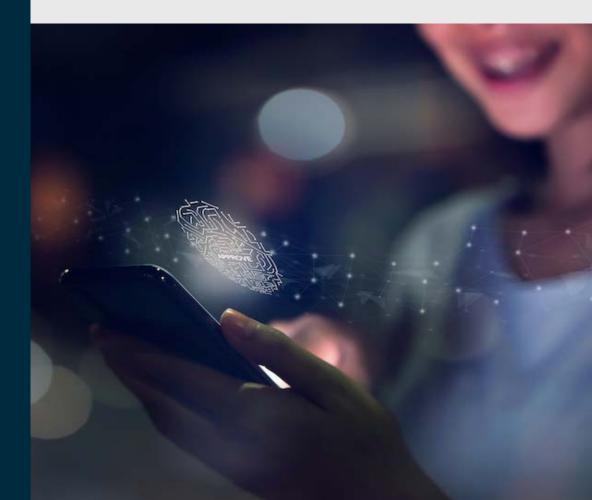
Qualifications and Certifications:

- M.Sc. and B.Sc. Electronics and Communication Engineering
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Data Privacy Solutions Engineer (CDPSE)
- GIAC Systems and Network Auditor (GSNA)
- Certified Third Party Risk Professional (CTPRP)
- ITIL Foundations Exam Certified (ITIL Foundation Certified)
- OneTrust Professional and Expert
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified System Engineer (MCSE)
- Expired-PCI SSC Payment Card Industry Professional (PCIP)
- Revenue Assurance Practitioner's Accreditation, TM Forum
- Oracle8i Certified Database Administration Master

Preparation

This workshop is highly interactive with group activities and discussions throughout. Come prepared with some current challenges you face in your organization.

To participate you'll need:

- A computer with camera and microphone
- Strong internet connection
- Quiet, well-lit space
- Current product or service challenges you facing

Explore the Agenda

DAY 1 | Monday, June 10, 2024

11:00am EST — **Introduction to Digital Forensics**
- Understanding the digital forensic process
- Legal and ethical considerations in digital investigations
- Role of digital forensics in law enforcement and corporate environments

12:45pm EST — **Digital Evidence Identification and Collection**
- Understanding the digital forensic process
- Legal and ethical considerations in digital investigations
- Role of digital forensics in law enforcement and corporate environments

2:00pm EST — **Break**

3:00pm EST — **File Systems and Data Storage Analysis**
- Understanding file systems and their structure
- Recovering deleted or hidden data
- Analyzing data storage media

4:00pm EST — **Forensic Imaging and Data Acquisition**
- Principles of forensic imaging
- Creating and verifying forensic images
- Tools and techniques for data acquisition

5:00pm EST — **End of Day 1**

DAY 2 | Monday, June 17, 2024

11:00am EST — **Digital Forensic Analysis Techniques**
- File system analysis and keyword searching
- Timeline analysis and reconstruction
- Data carving and recovery of fragmented files

12:45pm EST — **Mobile and Network Forensics**
- Investigating mobile devices and applications
- Network traffic analysis and log examination
- Internet and social media investigations

2:00pm EST — **Break**

3:00pm EST — **Malware Analysis and Incident Response**
- Analyzing malicious software and malware behavior
- Incident response procedures and tools
- Live forensics and volatile data collection

4:00pm EST — **Reporting and Presentation of Findings**
- Writing forensic reports and documenting findings
- Presenting evidence in court or other legal proceedings
- Quality Control and peer review in digital forensics

5:00pm EST — **End of Day 2**