

Forensic Investigator

The Digital Forensic Investigator is responsible for collecting and investigating digital forensics artifacts to assist investigations and/or perform evidence management. When investigating, they focus on the forensics capture and analysis of media and network artifacts to reconstruct timelines associated with an identified attack or breach.

Key Responsibilities

- Analyzing requests, and planning and executing forensic support for both simple and complex investigations.
- Providing recommendations for identification, collection and preservation of digital evidence.
- Determining tools and procedures required for preservation.
- Collecting, processing and analyzing electronically stored information (ESI) obtained from network, cloud and end user digital sources in accordance with industry standards.
- Providing required documentation demonstrating chain of custody of evidence.
- Generating formal forensic analysis reports in a clear and concise manner to a non-technical audience, e.g. senior management.
- Working with other team members to provide guidance and assistance.
- Using industry standard digital forensic tools (e.g. FTK, Xium) during the course of investigation.
- Conducting research into project-related issues.
- Maintaining forensic credentials and ability to provide expert testimony.

Recommended Qualifications

- Bachelor degree in a related field such as information security, management or computer engineering.
- Experience in digital forensics.
- Active CISSP, CISM and CCE or similar certifications are required.
- Other relevant certifications (such as GCIH, GCIA) are desirable.
- Strong attention to detail, concern for data accuracy and high personal integrity.
- In depth experience with industry standard digital forensics methodologies, including: evidence handling, chain of custody procedures, and commonly used forensic toolsets.
- Experience using physical, local and remote acquisition tools across multiple OS systems.
- Ability to clearly document and communicate findings, opinions, and recommendations to both technical and non-technical audiences.