# Certified Digital Forensic Investigator

## Median Salary

**$70,00**

## Job Growth

**+28%**

## Soft Skills

**Curiosity & Insight**

**Strong Communication**

**Creative Problem Solver**

**Ability to Write Reports**

**Ability to Explain Evidence**

## Common Job Duties

- Conduct data breach and security incident investigations
- Recover and examine data from computers and electronic storage devices
- Dismantle and rebuild damaged systems to retrieve lost data
- Identify additional systems/networks compromised by cyber attacks
- Compile evidence for legal cases
- Draft technical reports, write declarations and prepare evidence for trial
- Give expert counsel to attourneys about electronic evidence in a case
- Advise law enforcement on the credibility of acquired data
- Keep abreast of emerging technologies and threats

## Mile2 Cybersecurity Certification's Suggested Course Progression

| C)SP | C)DFE | C)NFE | C)CSA |
|---|---|---|---|
| Security Principles | Digital Forensics Examiner | Network Forensics Examiner | Cybersecurity Analyst |

A Master Forensics Investigator will have the knowledge, skills, and abilities to examin intrusions for both large and small organizations as well as performing detailed analysis of systems, networks and servers for intrusion discovery purposes. These highly trained and flexible digital forensic specialists are often called as expert witnesses in trial scenarios to present their findings, so a deep knowledge of investigative report writing and some understanding of the legalities surrounding cyber crime is valuable.


10213 Wilsky Blvd, Tampa, FL 33625 Phone: +1-813-920-6799 Toll Free: +1 800-816-4532

# Certified Digital Forensic Investigator

**ABILITIES**

- Decrypt digital data collections.
- Conduct forensic analyses in and for both Windows and Unix/Linux environments.

**KNOWLEDGE**

- Computer networking concepts and protocols, and network security methodologies.
- Risk management processes
- Cybersecurity and privacy laws, regulations, and policies
- Cyber threats and vulnerabilities.
- Operational impacts of cybersecurity lapses.
- Encryption algorithms
- Data backup and recovery.
- Incident response and handling methodologies.
- Operating systems.
- System and application security threats and vulnerabilities
- Server and client operating systems.
- Server diagnostic tools and fault identification techniques.
- Physical computer components and architectures
- File system implementations
- Processes for seizing and preserving digital evidence.
- Hacking methodologies.
- Investigative implications of hardware, Operating Systems, and network technologies.
- Legal governance related to admissibility
- Processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
- Types and collection of persistent data.
- Which system files contain relevant information and where to find those system files.
- Digital forensics data and how to recognize them.
- Deployable forensics.
- Security event correlation tools.
- Electronic evidence law.
- Legal rules of evidence and court procedure.
- System administration, network, and operating system hardening techniques.
- Applicable laws, statutes Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
- Network security architecture concepts
- Data carving tools and techniques
- Reverse engineering concepts.
- Anti-forensics tactics, techniques, and procedures.
- Forensics lab design configuration and support applications
- Debugging procedures and tools.
- File type abuse by adversaries for anomalous behavior.
- Malware analysis tools
- Malware with virtual machine detection
- System administration concepts for operating systems
- Binary analysis.
- Network architecture concepts including topology, protocols, and components.
- Packet-level analysis using appropriate tools
- Concepts and practices of processing digital forensic data.
- Operational design.
- Application Security Risks

**SKILLS**

- Developing, testing, and implementing network i nfrastructure contingency and recovery plans.
- Preserving evidence integrity according to standard operating procedures or national standards.
- Analyzing memory dumps to extract information.
- Identifying and extracting data of forensic interest in diverse media
- Identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux
- Collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.
- Setting up a forensic workstation.
- Using forensic tool suites
- Using virtual machines.
- Physically disassembling PCs.
- Conducting forensic analyses in multiple operating system environments
- Deep analysis of captured malicious code
- Using binary analysis tools
- One-way hash functions
- Analyzing anomalous code as malicious or benign.
- Analyzing volatile data.
- Identifying obfuscation techniques.
- Interpreting results of debugger to ascertain tactics, techniques, and procedures.
- Analyzing malware.
- Conducting bit-level analysis.
- Processing digital evidence, to include protecting and making legally sound copies of evidence.
- Performing packet-level analysis.

**TASKS**

- Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
- Confirm what is known about an intrusion
- Create a forensically sound duplicate of the evidence
- Decrypt seized data using technical means.
- Provide technical summary of findings in accordance with established reporting procedures.
- Ensure that chain of custody is followed for all digital media
- Examine recovered data for information of relevance to the issue at hand.
- Identify digital evidence for examination and analysis
- Perform dynamic analysis to boot an "image" of a drive to see the intrusion as the user may have seen it, in a native environment.
- Perform file signature analysis.
- Perform hash comparison against established database.
- Perform timeline analysis.
- Perform real-time cyber defense incident handling tasks to support deployable Incident Response Teams (IRTs).
- Perform static media analysis.
- Perform tier 1, 2, and 3 malware analysis.
- Prepare digital media for imaging by ensuring data integrity
- Provide technical assistance on digital evidence matters t
- Recognize and accurately report forensic artifacts
- Extract data using data carving techniques
- Capture and analyze network traffic associated with malicious activities using network monitoring tools.
- Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
- Conduct cursory binary analysis.
- Serve as technical expert and liaison to law enforcement personnel
- Perform virus scanning on digital media.
- Perform file system forensic analysis.
- Perform static analysis to mount an "image" of a drive
- Perform static malware analysis.

If a person holds the Master Forensic Investigator Badge from Mile2, we certify that they have passed the four certification exams in the role-based progression and thereby has adequate KSA's listed above to complete the applicable tasks required for the job role of Cyber Forensic Investigator.