DIGITAL FORENSIC

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Related Jobs Titles

Persons working in this Specialty area may have job titles similar to:

- Computer Forensic Analyst
- Computer Network Defense Forensic Analyst
- Digital Forensic Examiner
- Digital Media Collector
- Forensic Analyst
- Forensic Analyst (Cryptologic)
- Forensic Technician
- Network Forensic Examiner

Tasks

Professional involved in this Specialty perform the following tasks:

- Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
- Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
- Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion
- Conduct cursory binary analysis
- Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis
- Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy d
- Decrypt seized data using technical means
- Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)
- Employ IT systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
- Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence
- Examine recovered data for information of relevance to the issue at hand
- Formulate a strategy to ensure chain of custody is maintained in such a way that the evidence is not altered (ex: phones/PDAs need a power source, hard drives need protection from shock and strong magnetic fields)
- Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
- Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
- Perform dynamic analysis to boot an
- Perform file signature analysis
- Perform file system forensic analysis
- Perform hash comparison against established database

- Perform live forensic analysis (e.g., using Helix in conjunction with LiveView)
- Perform static analysis to mount an \image\" of a drive (without necessarily having the original drive)"""
- Perform static malware analysis
- Perform static media analysis
- Perform tier 1, 2, and 3 malware analysis
- Perform timeline analysis
- Perform virus scanning on digital media
- Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures)
- Provide consultation to investigators and prosecuting attorneys regarding the findings of computer examinations
- Provide technical assistance on digital evidence matters to appropriate personnel
- Provide technical summary of findings in accordance with established reporting procedures
- Provide testimony related to computer examinations
- Recognize and accurately report forensic artifacts indicative of a particular operating system
- Review forensic images and other data sources for recovery of potentially relevant information
- Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
- Use an array of specialized computer investigative techniques and programs to resolve the investigation
- Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis
- Use network monitoring tools to capture and analyze network traffic associated with malicious activity
- Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence
- Utilize deployable forensics tool kit to support operations as necessary
- Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies

KSAs

Experts in the Specialty Area have the following Knowledge, Skills, and Ability:

- Ability to decrypt digital data collections
- Knowledge of anti-forensics tactics, techniques, and procedures
- Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. ...
- Knowledge of basic concepts and practices of processing digital forensic data
- Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)
- Knowledge of basic system administration, network, and operating system hardening techniques
- Knowledge of common forensics tool configuration and support applications (e.g., VMWare, WIRESHARK)
- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
- Knowledge of data carving tools and techniques (e.g., Foremost)
- Knowledge of debugging procedures and tools
- Knowledge of deployable forensics
- Knowledge of electronic evidence law
- Knowledge of encryption algorithms (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)
- Knowledge of file system implementations (e.g., NTFS, FAT, EXT)
- Knowledge of hacking methodologies in Windows or Unix/Linux environment
- Knowledge of how different file types can be used for anomalous behavior
- Knowledge of incident response and handling methodologies
- Knowledge of investigative implications of hardware, Operating Systems, and network technologies

- Knowledge of legal governance related to admissibility (Federal Rules of Evidence)
- Knowledge of legal rules of evidence and court procedure
- Knowledge of malware analysis tools (e.g., OllyDbg, IDA Pro)
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of Defense-in-Depth)
- Knowledge of operating systems
- Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Knowledge of reverse engineering concepts
- Knowledge of security event correlation tools
- Knowledge of seizing and preserving digital evidence (e.g., chain of custody)
- Knowledge of server and client operating systems
- Knowledge of server diagnostic tools and fault identification techniques
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)
- Knowledge of the common networking protocols (e.g., TCP/IP), services (e.g., web, mail, Domain Name Server), and how they interact to provide network communications
- Knowledge of types and collection of persistent data
- Knowledge of types of digital forensics data and how to recognize them
- Knowledge of virtual machine aware malware, debugger aware malware, and packing
- Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies
- Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files
- Skill in analyzing anomalous code as malicious or benign
- Skill in analyzing memory dumps to extract information
- Skill in analyzing volatile data
- Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems)
- Skill in deep analysis of captured malicious code (malware forensics)
- Skill in developing, testing, and implementing network infrastructure contingency and recovery plans
- Skill in identifying and extracting data of forensic interest in diverse media (media forensics)
- Skill in identifying obfuscation techniques
- Skill in identifying, modifying, and manipulating applicable system components (Windows and/or Unix/Linux) (e.g., passwords, user accounts, files)
- Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures
- Skill in one-way hash functions (e.g., Sha, MDS)
- Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)
- Skill in physically disassembling PCs
- Skill in preserving evidence integrity according to standard operating procedures or national standards
- Skill in setting up a forensic workstation
- Skill in using binary analysis tools (e.g., Hexedit, xxd, hexdump)
- Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK)
- Skill in using virtual machines