

DIGITAL FORENSICS SPECIALIST

TYPE	TYPE 1	TYPE 2
DESCRIPTION	Same as Type 2	The National Incident Management System (NIMS) Type 2 Digital Forensics Specialist: 1. Collects, processes, and preserves computer-related evidence in support of network vulnerability mitigation and criminal fraud counterintelligence or law enforcement investigations 2. Works under the technical direction of the NIMS Type 1 Digital Forensics Specialist
CATEGORY	CRITERIA	CRITERIA
EDUCATION	Not Specified	Not Specified
	NOTES: Not Specified	
TRAINING	Same as Type 2	Completion of the following: 1. IS-100: Introduction to Incident Command System, ICS-100 2. IS-200: Incident Command System for Single Resources and Initial Action Incidents 3. IS-700: National Incident Management System, An Introduction 4. IS-800: National Response Framework, An Introduction
	NOTES: Any use of the term "forensics" is descriptive of a skill or capability and does not imply a law enforcement role.	

Superseded

TYPE	TYPE 1	TYPE 2
EXPERIENCE	<p>Same as Type 2, PLUS: Knowledge, Skills, and Abilities:</p> <ol style="list-style-type: none"> 1. Security event correlation tools 2. Debugging procedures and tools 3. Reverse engineering concepts 4. Network security architecture concepts, including topology, protocols, components, and principles 5. Basic system administration, network, and operating hardening techniques 6. Malware analysis tools 7. Conducting forensic analyses in multiple operating system environments 8. Analysis of captured malicious code 9. Using binary analysis tools 10. Identifying abnormal or irregular code and determining whether it is a threat 11. Identifying obscure threats and techniques 12. Interpreting results of debugger to ascertain tactics, techniques, and procedures 13. Developing, testing, and implementing network infrastructure contingency and recovery plans 14. Packet-level analysis using appropriate tools 15. Decrypting digital data collections <p>AHJ-validated experience demonstrated in the following:</p> <ol style="list-style-type: none"> 1. Collecting and analyzing intrusion artifacts and using discovered data to enable mitigation of potential computer network defense (CND) incidents within the enterprise 2. Confirming intrusion and discovering new information, if possible, after identifying intrusion via dynamic analysis 3. Decrypting seized data using technical means 4. Providing technical summary of findings in accordance with established reporting procedures 5. Examining recovered data for information of relevance to the issue at hand 6. Performing CND incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation 7. Performing dynamic analysis to boot an image of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it in a native environment 8. Analyzing life forensic <p>(Continued)</p>	<p>Agency Having Jurisdiction (AHJ)-validated knowledge, skills, and abilities demonstrated in the following areas:</p> <ol style="list-style-type: none"> 1. Electronic evidence law 2. Legal rules of evidence and court procedure 3. Recognizing different types of digital forensics data 4. Deployable forensics 5. Anti-forensic tactics, techniques, and procedures 6. Common forensic tool configuration and support applications from the leading industry tools 7. Data carving tools and technique 8. Computer Fraud and Abuse Act 9. Virtual machine aware malware, aware debugger malware, and packing 10. Basic concepts and practices of processing digital forensic data 11. Encryption algorithms 12. Incident response and handling methodologies 13. Desktop, server, mainframe operating systems including Windows, Unix, Linux, Mac OS 14. Server diagnostics tools and fault identification techniques 15. Basic physical computer component and architectures, including the functions of various components and peripherals 16. File system implementations 17. Processes for seizing and preserving digital evidence 18. Hacking methodologies for common operating systems 19. Legal governance related to admission into systems 20. Processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data 21. Types and collection of data 22. Webmail collection, searching/analyzing techniques, tools, and cookies 23. System files (such as log files, registry files, configuration files) that contain relevant information 24. Forensic tool suites 25. Physically disassembling personal computers and servers 26. Identifying and extracting data of forensic interest in diverse media 27. Identifying, modifying, and manipulating applicable system components 28. Setting up a forensic workstation 29. One way hash functions 30. Analyzing volatile data <p>(Continued)</p>

Superseded

TYPE	TYPE 1	TYPE 2
EXPERIENCE	(Continued) 9. Analyzing timeline 10. Analyzing static media and 1, 2, and 3 malware 11. Recognizing and accurately reporting forensic artifacts indicative of a particular operating system 12. Reviewing forensic images and other data sources for recovery of potentially relevant information 13. Using network monitoring tools to capture and analyze network traffic associated with malicious activity 14. Writing and publishing CND guidance and reports on incident findings to appropriate constituencies 15. Conducting a cursory binary analysis 16. Virus scanning on digital media 17. Analyzing file system forensic analysis 18. Analyzing to mount an "image" of a drive (without necessarily having the original drive) 19. Using deployable forensics toolkit to support operations as necessary	(Continued) 31. Identifying obfuscation techniques AHJ-documented and validated experience demonstrated in the following areas: 1. Conducting analysis of log files, evidence, and other information in order to determine best methods for identifying additional sources of evidence 2. Transportation and storage of data evidence 3. Tamper proofing packaging 4. Creating a forensically sound duplicate of the evidence that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes 5. Documenting original condition of all evidence 6. Ensuring chain of custody is followed for all digital media acquired in accordance with applicable state and federal rules of evidence 7. Identifying digital evidence for examination and analysis in such a way as to avoid unintentional alteration 8. Analyzing file signature 9. Comparing against established database 10. Capturing live forensic data 11. Preparing digital media for imaging for ensuring data integrity 12. Providing technical assistance on digital evidence matters to appropriate personnel
	NOTES: The knowledge, skills, and abilities align with the National Institute of Standards and Technology's National Initiative for Cyber Education (NICE) National Cybersecurity Workforce Framework.	
PHYSICAL/MEDICAL FITNESS	Not Specified	Not Specified
	NOTES: Not Specified	
CURRENCY	Same as Type 2	1. Participates in exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires 3. Active security clearance
	NOTES: Provider must carry out and use any background checks as applicable law specifies. This may include a background check completed within past 12 months; sex-offender registry check; and a local, state, and a local, state, and national criminal history.	
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	Same as Type 2, PLUS: 1. Certified Digital Forensic Examiner (CDFE) 2. Certified Computer Crime Investigator (CCCI) 3. Information Assurance Certification (IAC) 4. Certified Forensic Examiner (CFE) 5. Certified Computer Hacking Forensic Investigator (CCHFI)	1. Technical qualifications equivalent to Department of Defense Directive (DoDD) 8570 Level 2 2. Certified Digital Media Collector (CDMC)
	NOTES: Not Specified	

Superseded

ORDERING SPECIFICATIONS OR DESIGNATIONS

1. (X) Can be ordered as an individual asset
2. (X) Can be ordered in conjunction with a NIMS typed team (Cyber Incident Response Team)
3. () Can be ordered in conjunction with a NIMS typed unit
4. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment
5. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

REFERENCES

1. FEMA, NIMS 508: Cyber Incident Response Team
2. National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014
3. Department of Defense Directive (DoDD), 8570 and Global Assurance Information Certification (GAIC), January 2014

NOTES

Nationally typed resources represent the minimum criteria for the associated category.

Superseded