CAREER PATHWAY LAW ENFORCEMENT COUNTERINTELLIGENCE FORENSICS ANALYST (211)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 211- LAW ENFORCEMENT COUNTERINTELLIGENCE FORENSICS ANALYST

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 211-Law Enforcement Counterintelligence Forensics Analyst.

Table 1. 211-Law Enforcement Counterintelligence Forensics Analyst Work Role Overview

NICE Role Description	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
OPM Occupational Series	Personnel performing the 211-Law Enforcement Counterintelligence Forensics Analyst work role are most commonly aligned to the following Occupational Series: (Top 5 Shown) - 1811-Criminal Investigation – 83% - 510-Accounting – 7% - 2210-Information Technology – 3% - 1550 – Computer Science – 2% - 1801 – General Inspection, Investigation, Enforcement, and Compliance Series – 1%
Work Role Pairings	Personnel performing the 211 Law Enforcement Counterintelligence Forensics Analyst - work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 132-Target Network Analyst- 79% - 212-Cyber Defense Forensics Analyst- 15% - 221-Cyber Crime Investigator – 4% - 422-Data Analyst – <1% - 461-Systems Security Analyst – <1%
Functional Titles	Personnel performing the 211-Law Enforcement Counterintelligence Forensics Analyst work role may unofficially or alternatively be called: - Computer Crime Forensics Investigator - Forensic Analyst / Technician - Digital Forensic Examiner - Digital Media Collector - Network Forensic Examiner - Insider Threat Analyst

Distribution of GS-Levels	Personnel performing the 211-Law Enforcement Counterintelligence Forensics Analyst work role are most commonly found within the following grades on the General Schedule.* - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☐ GS-10 – redacted** - ☐ GS-11 – redacted** - ☒ GS-12 – 4% - ☒ GS-13 – 13% - ☒ GS-14 – 65% - ☒ GS-15 – 15% *.4% of all 211s are in non-GS pay plans and excluded from this section **Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 211-Law Enforcement Counterintelligence Forensics Analyst work role: - 212-Cyber Defense Forensics Analyst - 221-Cyber Crime Investigator - 531-Cyber Defense Incident Responder
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 211-Law Enforcement Counterintelligence Forensics Analyst. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 212-Cyber Defense Forensics Analyst - 221-Cyber Crime Investigator *Note: Leveraging the knowledge, skills, abilities, and tasks of the 211-Law Enforcement Counterintelligence Forensics Analyst work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711-Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *732-Privacy Compliance Manager / Officer* - *751-Cyber Workforce Developer and Manager* - *752-Cyber Policy and Strategy Planner* - *802-IT Project Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 211-Law Enforcement Counterintelligence Forensics Analyst work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 211-Law Enforcement Counterintelligence Forensics Analyst Core Tasks

Task ID	Task Description	Core or Additional
T0027	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion.	Core
T0048	Create a forensically sound duplicate of the evidence (i.e., 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 diskettes, CD, PDA, mobile phones, GPS, and all tape formats.	Core
T0439	Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data.	Core
T0471	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	Core
T0087	Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Core
T0103	Examine recovered data for information of relevance to the issue at hand.	Core
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Core
T0165	Perform 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.	Core
T0167	Perform file signature analysis.	Core
T0286	Perform file system forensic analysis.	Core
T0168	Perform hash comparison against established database.	Core
T0287	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	Core
T0179	Perform static media analysis.	Core
T0285	Perform virus scanning on digital media.	Core
T0190	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Core
T0212	Provide technical assistance on digital evidence matters to appropriate personnel.	Core
T0075	Provide technical summary of findings in accordance with established reporting procedures.	Core
T0532	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	Core
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Core
T0289	Utilize deployable forensics tool kit to support operations as necessary.	Core
T0240	Capture and analyze network traffic associated with malicious activities using network monitoring tools.	Additional

Task ID	Task Description	Core or Additional
T0432	Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Additional
T0253	Conduct cursory binary analysis.	Additional
T0036	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.	Additional
T0238	Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).	Additional
T0120	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.	Additional
T0172	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	Additional
T0288	Perform static malware analysis.	Additional
T0182	Perform tier 1, 2, and 3 malware analysis.	Additional
T0173	Perform timeline analysis.	Additional
T0193	Process crime scenes.	Additional
T0216	Recognize and accurately report forensic artifacts indicative of a particular operating system.	Additional
T0246	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	Additional

1.3 CORE KNOWLEDGE, SKILLS, AND ABILITIES

The table below provides a ranking of KSAs that represent the Core, or baseline, expectations for performance in the 211-Law Enforcement Counterintelligence Forensics Analyst work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 211-Law Enforcement Counterintelligence Forensics Analyst Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity principles.	Information Systems/Network Security	Foundational to all work roles.
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to all work roles.
K0003	Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	Legal, Government, and Jurisprudence	Foundational to all work roles.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to all work roles.
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to all work roles.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to all work roles.
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics	Core
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics	Core
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics	Core
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics	Core
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics	Core
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	Computer Forensics	Core
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics	Core
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics	Core
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics	Core

KSA ID	Description	Competency	Importance to Work Role
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics	Core
S0074	Skill in physically disassembling PCs.	Computers and Electronics	Core
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption	Core
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Core
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence	Core
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence	Core
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence	Core
K0060	Knowledge of operating systems.	Operating Systems	Core
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems	Core
S0062	Skill in analyzing memory dumps to extract information.	System Administration	Core
K0021	Knowledge of data backup and recovery.	Business Continuity	Additional
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	Business Continuity	Additional
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics	Additional
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics	Additional
K0128	Knowledge of types and collection of persistent data.	Computer Forensics	Additional
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics	Additional
K0134	Knowledge of deployable forensics.	Computer Forensics	Additional
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics	Additional
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics	Additional
S0069	Skill in setting up a forensic workstation.	Computer Forensics	Additional

KSA ID	Description	Competency	Importance to Work Role
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics	Additional
S0091	Skill in analyzing volatile data.	Computer Forensics	Additional
A0005	Ability to decrypt digital data collections.	Computer Forensics	Additional
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense	Additional
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	Computer Network Defense	Additional
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption	Additional
K0145	Knowledge of security event correlation tools.	Information Systems/Network Security	Additional
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Additional
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence	Additional
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence	Additional
K0077	Knowledge of server and client operating systems.	Operating Systems	Additional
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems	Additional
K0186	Knowledge of debugging procedures and tools.	Software Development	Additional
K0078	Knowledge of server diagnostic tools and fault identification techniques.	System Administration	Additional
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration	Additional
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).	System Administration	Additional
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis	Additional
K0183	Knowledge of reverse engineering concepts.	Threat Analysis	Additional

KSA ID	Description	Competency	Importance to Work Role
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	Threat Analysis	Additional
K0189	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).	Threat Analysis	Additional
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	Threat Analysis	Additional
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	Threat Analysis	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	Additional
K0119	Knowledge of hacking methodologies.	Vulnerabilities Assessment	Additional
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment	Additional
S0046	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment	Additional
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	Web Technology	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 211-Law Enforcement Counterintelligence Forensics Analyst work role, and their associated importance. Listed competencies are collections of three or more similar Knowledge, Skills, or Abilities aligned to the Work Role. *These competencies originate from the NICE Framework Competency Pivot Tool.*

Table 4. 211-Law Enforcement Counterintelligence Forensics Analyst Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Computer Forensics	C005	This area contains KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence.	• Knowledge of concepts and practices of processing digital forensic data. (K0017) • Knowledge of processes for seizing and preserving digital evidence. (K0118) • Knowledge of investigative implications of hardware, Operating Systems, and network technologies. (K0122) • Knowledge of types and collection of persistent data. (K0128) • Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files. (K0132) • Knowledge of types of digital forensics data and how to recognize them. (K0133) • Knowledge of deployable forensics. (K0134) • Knowledge of data carving tools and techniques (e.g., Foremost). (K0182) • Knowledge of anti-forensics tactics, techniques, and procedures. (K0184) • Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark). (K0185) • Skill in preserving evidence integrity according to standard operating procedures or national standards. (S0047) • Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics). (S0065) • Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. (S0068) • Skill in setting up a forensic workstation. (S0069) • Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK). (S0071) • Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems). (S0075) • Skill in analyzing anomalous code as malicious or benign. (S0090) • Skill in analyzing volatile data. (S0091)	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Legal, Government, and Jurisprudence	C030	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.	• Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. (K0003) • Knowledge of legal governance related to admissibility (e.g. Rules of Evidence). (K0123) • Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody. (K0125) • Knowledge of electronic evidence law. (K0155) • Knowledge of legal rules of evidence and court procedure. (K0156) • Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. (K0168)	Core
Operating Systems	C034	This area contains KSAs that relate to computer network, desktop, and mainframe operating systems and their applications.	• Knowledge of operating systems. (K0060) • Knowledge of server and client operating systems. (K0077) • Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]). (K0117) • Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). (S0067)	Core
Vulnerabilities Assessment	C057	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of cyber threats and vulnerabilities. (K0005) • Knowledge of specific operational impacts of cybersecurity lapses. (K0006) • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). (K0070) • Knowledge of hacking methodologies. (K0119) • Knowledge of file type abuse by adversaries for anomalous behavior. (K0187) • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) (K0624) • Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). (S0046)	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Threat Analysis	C055	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.	• Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. (K0107) • Knowledge of reverse engineering concepts. (K0183) • Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro). (K0188) • Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device). (K0189) • Skill in deep analysis of captured malicious code (e.g., malware forensics). (S0087) • Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump). (S0088)	Additional
System Administration	C048	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.	• Knowledge of server diagnostic tools and fault identification techniques. (K0078) • Knowledge of system administration, network, and operating system hardening techniques. (K0167) • Skill in analyzing memory dumps to extract information. (S0062) • Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). (S0073)	Additional
Information Systems/ Network Security	C024	This area contains KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	• Knowledge of cybersecurity and privacy principles. (K0004) • Knowledge of security event correlation tools. (K0145) • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). (K0179)	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 211-Law Enforcement Counterintelligence Forensics Analyst Suggested Qualifications

For indicators of capability for the 511-Cyber Defense Analyst work role, please see Draft NISTR 8193 - National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators.

Section to be populated with updated DoD-8140 Qualification Matrix for 211-Law Enforcement Counterintelligence Forensics Analyst.

2 APPENDIX: 211-LAW ENFORCEMENT COUNTERINTELLIGENCE FORENSICS ANALYST TASK ANALYSIS AND KSA MAPPING

2.1 KEY TO READING THE TASK ANALYSIS AND KSA MAPPING

Table 6. Key to Reading the Task Analysis and KSA Mapping

Proficiency	Task Statement	Importance
As Written	Task as written within the NICE Cybersecurity Workforce Framework (NICE Framework).	Overall Importance to Work Role
Entry	*Example behavioral indicator / task permutation for performing this task at an Entry skills proficiency level.*	
Intermediate	*Example behavioral indicator / task permutation for performing this task at an Intermediate skills proficiency level.*	
Advanced	*Example behavioral indicator / task permutation for performing this task at an Advanced skills proficiency level.*	

Table 7. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
ID of K, S, or A	Knowledge, Skill or Ability needed to perform the task as written within the NICE Framework	Competency mapped to the individual K, S, or A.

2.2 211-Law Enforcement Counterintelligence Forensics Analyst Task Analysis and KSA Mapping

Table 8. T0027 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion.	Core
Entry	*Under supervision, conduct basic analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion. Understand what logs to look for and how to read logs.*	
Intermediate	*Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion.*	
Advanced	*Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion. Develop advanced techniques and processes to automate parsing and prioritizing logs.*	

Table 9. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems

KSA ID	Description	Competency
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0062	Skill in analyzing memory dumps to extract information.	System Administration
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0119	Knowledge of hacking methodologies.	Vulnerabilities Assessment

Table 10. T0048 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Create a forensically sound duplicate of the evidence (i.e., 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 diskettes, CD, PDA, mobile phones, GPS, and all tape formats.	Core
Entry	*Under supervision, assist with or coordinate the creation of forensically sound duplication of evidence.*	
Intermediate	*Independently create a forensically sound duplicate of the evidence (i.e., 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 diskettes, CD, PDA, mobile phones, GPS, and all tape formats.*	
Advanced	*Verify or develop the process to image the device and integrity of the evidence created.*	

Table 11. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics

KSA ID	Description	Competency
S0074	Skill in physically disassembling PCs.	Computers and Electronics
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems

Table 12. T0439 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data.	Core
Entry	*Detect encrypted data, stenography, alternate data streams and other forms of concealed data.*	
Intermediate	*Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data.*	
Advanced	*Develop advanced process/techniques; oversee process improvement activities and serve as quality control.*	

Table 13. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption

KSA ID	Description	Competency
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems

Table 14. T0471 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	Core
Entry	*Under supervision, assist with documentation of original condition and/or associated evidence.*	
Intermediate	*Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).*	
Advanced	*Review, approve, and sign off on documentation; oversee process improvement to find efficiencies and efficacies.*	

Table 15. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics

Table 16. T0087 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Core
Entry	*Under supervision, observe the chain of custody activities and demonstrate understanding about the collection protocols for the Federal Rules of Evidence.*	
Intermediate	*Ensure the chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.*	
Advanced	*Oversight of portfolio of employees/activities to ensure the integrity of chain of custody is intact; quality control/assurance.*	

Table 17. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence

Table 18. T0103 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Examine recovered data for information of relevance to the issue at hand.	Core
Entry	*Be trained and observe others in examining recovered data for information of relevance to the issue at hand.*	
Intermediate	*Examine recovered data for information of relevance to the issue at hand.*	
Advanced	*Validate the results of the examination of recovered data and approve information is relevant to the issue at hand.*	

Table 19. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0060	Knowledge of operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems

Table 20. T0113 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Core
Entry	*Under supervision, identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.*	
Intermediate	*Examine digital evidence for examination and analysis in such a way as to avoid unintentional alteration.*	
Advanced	*Approve the workflow process and develop advanced techniques for digital evidence and examination analysis; ensure compliance with guidelines/protocol.*	

Table 21. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics

KSA ID	Description	Competency
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems

Table 22. T0165 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform 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.	Core
Entry	*Under supervision, use the imaged media to conduct preliminary analyses.*	
Intermediate	*Perform analysis on boot imaged media (derived from original) to determine intrusion activity.*	
Advanced	*Develop the advanced techniques to perform analysis on boot imaged media for intrusion activity.*	

Table 23. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0134	Knowledge of deployable forensics.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
K0060	Knowledge of operating systems.	Operating Systems

Table 24. T0167 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform file signature analysis.	Core
Entry	*Know the sources available and where to find sources for signature analysis; validate against signature database.*	
Intermediate	*Perform file signature analysis; populate database; write new signatures as needed.*	
Advanced	*Oversee/approve file signature analysis.; brief on threats identified.*	

Table 25. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment

Table 26. T0286 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform file system forensic analysis.	Core
Entry	*Under supervision, perform file system forensic analysis.*	
Intermediate	*Perform file system forensic analysis; complete appropriate reports; maintain log.*	
Advanced	*Oversee/approve file system forensic analysis; approve dissemination of finalized reports.*	

Table 27. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0090	Skill in analyzing anomalous code as malicious or benign.	Computer Forensics
S0091	Skill in analyzing volatile data.	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics

KSA ID	Description	Competency
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
K0060	Knowledge of operating systems.	Operating Systems
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0062	Skill in analyzing memory dumps to extract information.	System Administration

Table 28. T0168 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform hash comparison against established database.	Core
Entry	*Consistently demonstrate the accurate application of hash comparisons.*	
Intermediate	*Perform hash comparison and verify against established databases and/or contribute new to database; differentiate among types.*	
Advanced	*Ensure the hashes are accurate and valid; compare hashes against original media; ensure overall integrity of process.*	

Table 29. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption

Table 30. T0287 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	Core
Entry	*Under supervision, use the imaged media to conduct preliminary analyses.*	
Intermediate	*Perform analysis on boot imaged media (derived from original) to determine intrusion activity.*	
Advanced	*Develop the advanced techniques to perform analysis on boot imaged media for intrusion activity.*	

Table 31. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption
K0060	Knowledge of operating systems.	Operating Systems

Table 32. T0179 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform static media analysis.	Core
Entry	*Under supervision, use the imaged media to conduct preliminary analyses.*	
Intermediate	*Perform analysis on boot imaged media (derived from original) to determine intrusion activity.*	
Advanced	*Develop the advanced techniques to perform analysis on boot imaged media for intrusion activity.*	

Table 33. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
S0092	Skill in identifying obfuscation techniques.	Computer Network Defense
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
K0060	Knowledge of operating systems.	Operating Systems

Table 34. T0285 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform virus scanning on digital media.	Core
Entry	*Perform virus scanning on digital media and follow the organization's standard operating procedures.*	
Intermediate	*Perform virus scanning on digital media, analyze data, determine the type of virus, and isolate for remediation based of organization's standard operating procedures.*	
Advanced	*Coordinate with partners/vendors on remediation; issues Traffic Light Protocol (TLP), as necessary; seek identification.*	

Table 35. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0060	Knowledge of operating systems.	Operating Systems
K0189	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer’s display device).	Threat Analysis
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.	Vulnerabilities Assessment

Table 36. T0190 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Core
Entry	*Under supervision, assist with the preparation of digital media and demonstrate understanding of write blocker concepts/forensic-data capture and the organizations standard operating procedures.*	
Intermediate	*Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures); demonstrate a fundamental understanding of compliance and adherence to Federal, SLTT, D/A regulations.*	
Advanced	*Author and update the standard operating procedures; ensure/oversee compliance and validation with the preparation of digital media for imaging; demonstrate mastery of TTPs implementation and utilization; demonstrate compliance and adherence to Federal, SLTT, D/A regulations.*	

Table 37. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0134	Knowledge of deployable forensics.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics

KSA ID	Description	Competency
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems

Table 38. T0212 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide technical assistance on digital evidence matters to appropriate personnel.	Core
Entry	*Provide technical assistance on basic digital evidence matters to appropriate personnel.*	
Intermediate	*Provide technical assistance on more complex digital evidence matters to appropriate personnel and breakdown to be actionable/informative; report out, as appropriate.*	
Advanced	*Collect information on digital evidence matters and report out, as necessary; author/validate communications; approve dissemination/release of information.*	

Table 39. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics

KSA ID	Description	Competency
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics

Table 40. T0075 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide technical summary of findings in accordance with established reporting procedures.	Core
Entry	*Learn established reporting procedures and requirements for documentation and draft technical summary of findings.*	
Intermediate	*Author technical summary of findings and perform initial quality control management and peer reviews.*	
Advanced	*Approve technical summary of finding, develop new templates/requirements for documentation/playbooks; write white papers; oversee the update lifecycle of reports or documentation.*	

Table 41. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption

Table 42. T0532 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	Core
Entry	*Under supervision, examine forensic media and other data sources, following organization's process/procedures/job aid; use forensic software tools to recover potentially relevant information.*	
Intermediate	*Independently collect and review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.*	
Advanced	*Collect and review complex forensic images and other data sources; define the process for reviewing; approve the report out; ensure compliance agency guidelines (e.g. CIGIE).*	

Table 43. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0133	Knowledge of types of digital forensics data and how to recognize them.	Computer Forensics
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
A0005	Ability to decrypt digital data collections.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics

KSA ID	Description	Competency
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	Encryption
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems

Table 44. T0241 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Core
Entry	*Assist with cataloging, documenting, extracting, collecting, packaging, and preserving digital evidence.*	
Intermediate	*Use specialized software/equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.*	
Advanced	*Develop and approve specialized software/equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.*	

Table 45. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0134	Knowledge of deployable forensics.	Computer Forensics
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	Computer Forensics
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	Computers and Electronics

KSA ID	Description	Competency
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	Operating Systems

Table 46. T0289 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Utilize deployable forensics tool kit to support operations as necessary.	Core
Entry	*Assist with preparations before deployment. Under supervision, utilize deployable forensics tool kit to support operations as necessary.*	
Intermediate	*Identify, prepare, and utilize deployable forensics tool kit to support operations as necessary. Update equipment with the latest hardware and software updates needed.*	
Advanced	*Identify, prepare, and utilize deployable forensics tool kit to support operations as necessary. Validate equipment has latest hardware and software updates needed. Develop processes and SOPs associated with maintaining tool kits. Plan for equipment/software refresh to avoid obsolesce.*	

Table 47. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0017	Knowledge of concepts and practices of processing digital forensic data.	Computer Forensics
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	Computer Forensics
K0134	Knowledge of deployable forensics.	Computer Forensics
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
S0069	Skill in setting up a forensic workstation.	Computer Forensics
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	Computer Forensics
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	Computer Forensics
S0074	Skill in physically disassembling PCs.	Computers and Electronics
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).	Encryption
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0060	Knowledge of operating systems.	Operating Systems

KSA ID	Description	Competency
K0077	Knowledge of server and client operating systems.	Operating Systems
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	Operating Systems
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration