Digital Forensics Technician Skill Standards

TEXAS WORKFORCE
INVESTMENT COUNCIL

DIGITAL FORENSICS TECHNICIAN SKILL STANDARDS

Critical Work Function	Key Activity	Key Activity	Key Activity	Key Activity	Key Activity	Key Activity	Key Activity
1. Manage Risk in Digital Forensics Investigations	1.1 Plan investigation to comply with legal, ethical and pre-examination procedures	1.2 Evaluate software and hardware tool reliability	1.3 Construct reliable and documented test images	1.4 Produce repeatable and verifiable findings	1.5 Encode/ Encrypt investigation data	1.6 Confirm operating system defaults and standard functionality	1.7 Validate reliability of findings
2. Manage Acquisition of Data from Storage Media	2.1 Perform shutdown procedures on operating systems	2.2 Determine scope and acquisition methods	2.3 Evaluate complex storage configurations	2.4 Prepare and sanitize storage media	2.5 Perform remote acquisition	2.6 Perform basic data recovery	2.7 Perform data acquisition from virtual machines
3. Analyze Data from Mobile and Embedded Devices	3.1 Determine collection method for device	3.2 Research device characteristics	3.3 Collect and investigate device specific data				
4. Analyze Windows Based Artifacts	4.1 Investigate file and file system related artifacts	4.2 Investigate application specific artifacts	4.3 Investigate system specific artifacts	4.4 Investigate device specific artifacts	4.5 Process Windows registry analytics		
5. Analyze Mac Based Artifacts	5.1 Process file system	5.2 Evaluate partition configurations	5.3 Investigate configured services	5.4 Investigate Internet related artifacts	5.5 Investigate user history related artifacts		

DIGITAL FORENSICS TECHNICIAN SKILL STANDARDS

6. Analyze Linux Based Artifacts	6.1 Process file system	6.2 Evaluate partition configurations	6.3 Investigate configured services	6.4 Investigate Internet related artifacts	6.5 Investigate user created artifacts		
7. Analyze Network Based Data Acquisitions	7.1 Investigate network log files	7.2 Establish secure file transfer and network communication	7.3 Investigate network packet captures	7.4 Determine status of network based sensors	7.5 Investigate SCADA specific artifacts		
8. Manage Digital Forensics Laboratory Environments	8.1 Perform system configuration, hardening, and maintenance	8.2 Configure network storage devices	8.3 Maintain laboratory equipment	8.4 Configure acquisition/ investigation system			
9. Manage Recovery and Extraction of Big Data	9.1 Inventory big data	9.2 Catalog stored big data	9.3 Restore big data	9.4 Extract mailboxes from big data	9.5 Filter relevant big data	9.6 Prepare data sets in required formats	

Occupational Title: Digital Forensics Technician			
Critical Work Function 1. Manage Risk in Digital Forensics Investigations		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
1.1 Plan investigation to comply with legal, ethical and pre-examination procedures	1.1.1 Keyword searches are appropriately designed and accurately performed. 1.1.2 Procedures for the reservation of evidence are followed. 1.1.3 Computer crimes are accurately described according to Texas and Federal codes and statutes. 1.1.4 Legal rules of evidence and court procedures in Texas are followed. 1.1.5 Standard computer crime reporting methods are used. 1.1.6 Ethical conduct is applied to forensics examination procedures. 1.1.7 Pre-processing analytics are applied in forensics examination procedures. 1.1.8 Texas and Federal agencies are engaged in their specialized roles.	Knowledge of tools used to fight against corporate espionage Ability to utilize different search engines Ability to create customized search queries Knowledge of plagiarism detection tools Ability to seize evidentiary image of a USB device Ability to seize evidentiary Image from a hard drive Knowledge of computer crime, fraud and sexual offense terminology	Texas Constitution and Statutes www.statutes.legis.state.tx.us/ Federal Criminal Code and Rules Internet browsers (Examples: Firefox, Chrome, I.E.,Opera) Computer forensics and information assurance software and hardware tools Regular Expressions SQL language Search engines Customized search queries

Occupational Title: Digital Forensics Technician			
Critical Work Function 1. Manage Risk in Digital Forensics Investigations		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
1.2 Evaluate software and hardware tool reliability	1.2.1 NIST forensics tool testing (CFTT) is used to locate and evaluate hardware. 1.2.2 NIST Forensics Tool Testing (CFTT) is used to locate and evaluate software. 1.2.3 Documentation of updates is maintained. 1.2.4 Forensic testing control samples are created according to standard criteria. 1.2.5 Authenticity of evidence is evaluated according to standard criteria. 1.2.6 Procedures to ensure protection of computer components and stored data are followed. 1.2.7 Procedures to ensure protection of volatile data are followed.	Ability to use software and hardware tools for analysis Ability to analyze and confirm forensics software and hardware Ability to test and verify reliability of available updates to hardware and software tools Ability to verify write blocker device reliability Ability to construct scripts to automate and standardize test procedures	NIST CFTT - http://www.cftt.nist.gov/ Computer forensics and information assurance software and hardware tools
1.3 Construct reliable and documented test images	1.3.1 Test image demonstrates tool effectiveness and performance. 1.3.2 Test images are created and documented according to standard criteria.	Ability to perform tests using command line tools Ability to interpret utility's help documentation without external aid Ability to document all steps in image creation Ability to maintain integrity of monitored data Ability to create images in various formats Ability to construct scripts for consistent deployment of data into base images Knowledge of structural understanding of file systems Knowledge of common forensics artifacts	Computer forensics and information assurance software and hardware tools (Examples: OVAL, Microsoft, Baseline Analyzer)

Occupational Title: Digital Forensics Technician			
Critical Work Function 1. Manage Risk in Digital Forensics Investigations		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
1.4 Produce repeatable and verifiable findings	1.4.1 Heuristic hypotheses are formed. 1.4.2 The scientific method is applied to testing methodology. 1.4.3 False positives and false negatives are identified. 1.4.4 Integrity of control image is maintained. 1.4.5 Findings are validated.	Ability to monitor file system changes with approved tools Ability to monitor registry changes with approved tools Ability to evaluate relevant changes Ability to use multiple operating systems	Computer forensics and information assurance software and hardware tools (Examples: PERL, Python, C++, or C#)
1.5 Encode/Encrypt investigation data	1.5.1 Potential problems that might affect later forensic processes are identified. 1.5.2 Application flaws related to data protection are identified. 1.5.3 Compression methods are determined. 1.5.4 Password cracking methodology is applied. 1.5.5 EFS file recovery is performed. 1.5.6 Basic stego analysis is performed.	Ability to configure and decrypt evidence Ability to use and detect encrypted volumes Knowledge of strengths and weaknesses of encoding and encryption Knowledge of detecting and decoding Base64, URL, UNICODE, ASCII, HTML Knowledge of lossy and lossless compression types and methods Ability to use password cracking tools Ability to use EFS recovery key to recover data Ability to use various stego tools Ability to evaluate the method to use in a case for the quickest results	Computer forensics and information assurance software and hardware tools (Examples: TrueCrypt, PRTK/DNA, Hex Workshop, BitlLocker) Encoding and encryption tools (Examples: DES, 3DES, AES, NTLM, LM, CRC, XOR, ROT-13) Password cracking tools (Examples: PRTK/DNA, Ophcrack, John the Ripper, Passware)

Occupational Title: Digital Forensics Technician			
Critical Work Function 1. Manage Risk in Digital Forensics Investigations		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
1.6 Confirm operating system defaults and standard functionality	1.6.1 NIST hardening procedures on Windows client and server operating systems are installed and performed. 1.6.2 Forensically sound boot devices are created. 1.6.3 Windows policy and security settings are determined. 1.6.4 Deviations from expected Windows defaults prior to launching into the examination process are visually identified. 1.6.5 Basic storage area artifacts are identified.	Knowledge of operating system default installation process, folder virtualization, and default settings and security features Knowledge of boot order and process Knowledge of default folder structure and fully qualified paths Knowledge of use of folder virtualization in Windows Knowledge of default settings Knowledge of various security features	Computer forensics and information assurance software and hardware tools (Examples: Secpol.msc, Certmgr.msc)

Occupational Title: Digital Forensics Technician			
Critical Work Function 1. Manage Risk in Digital Forensics Investigations		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
1.7 Validate reliability of findings	1.7.1 System changes are monitored. 1.7.2 Findings are validated by reproducing case scenario. 1.7.3 Operating system is configured to match case settings. 1.7.4 Methodology used is evaluated and reviewed. 1.7.5 Detailed reports are prepared and maintained. 1.7.6 Relevant supporting evidence items are extracted. 1.7.7 Virtual environments are used.	Knowledge of common file structures (e.g., bmp, jpg, evt, pst, MBR, VBR, MFT, DE) Ability to monitor applications for user interaction and changes Ability to establish a base system and reliably recreate hypothesis Ability to export reports Ability to filter interference from local and network sources Ability to implement NIST Software testing metrics Ability to create report based on requirements	Computer forensics and information assurance software and hardware tools(Examples: HexWorkshop, HxD, hexdump)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 1:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 1. Manage Risk in Digital Forensic Investigations																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
3	3	5	5	5	5	5	3	4	3	3	3	5	5	5	5	5

Statement of Assessment for Critical Work Function 1:

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event.
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 2. Manage Acquisition of Data from Storage Media		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
2.1 Perform shutdown procedures on operating systems	2.1.1 Operating system version is determined. 2.1.2 Possible encryption in use on live system is determined. 2.1.3 Common file systems associated with digital evidence are identified. 2.1.4 File system characteristics are identified. 2.1.5 Shutdown is documented.	Ability to use command line tools Knowledge of operating system built-in utilities to perform shutdown Ability to determine if the Operating System has any active connections before shutdown Ability to perform remote operations Ability to keep detailed documentation of all actions performed (sketches, pictures, cable locations) Ability to consider risks associated with losing volatile data and effects of non-forensic tools Knowledge of the structure of VBR and file system signatures Ability to determine file system cluster size from VBR Ability to extract and verify volume serial number Ability to identify anomalies related to file systems	Digital camera Computer forensics and information assurance software and hardware tools(Example: Sysinternals-psexec) Imager

Occupational Title: Digital Forensics Technician			
Critical Work Function 2. Manage Acquisition of Data from Storage Media		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
2.2 Determine scope and acquisition methods	2.2.1 Logical, physical, sparse and volatile data acquisition steps are followed. 2.2.2 Collected images are protected. 2.2.3 Detailed documentation of collection process is maintained. 2.2.4 Collected images are verified. 2.2.5 Forensics image type methods are verified. 2.2.6 Physical size of drive is compared to physical label. 2.2.7 Logical partition sizes are compared to physical drive size. 2.2.8 Forensically sound procedures are followed. 2.2.9 Safe handling of evidence is maintained. 2.2.10 Write blocker verification is performed. 2.2.11 Software write blockers are configured. 2.2.12 Investigative workstation is configured to access connected evidence in a forensically sound manner.	Ability to determine the proper acquisition method based on scope of case Knowledge of encryption methods Ability to identify various hardware devices and interfaces Ability to hash individual files and/or forensics image files Ability to use forensics imaging software	Computer forensics and information assurance software and hardware tools (Examples: Tableau, FTK Imager, LinEn, Helex)
2.3 Evaluate complex storage configurations	2.3.1 SCSI configuration is documented before disassembly. 2.3.2 RAID acquisition is managed. 2.3.3 Storage devices for acquisition are configured.	Knowledge of SCSI storage device configurations Knowledge of RAID configurations Knowledge of SAN technology Knowledge of NAS technology Knowledge of VM and Cloud storage concepts	Computer forensics and information assurance software and hardware tools(Example: ipconfig)

Occupational Title: Digital Forensics Technician			
Critical Work Function 2. Manage Acquisition of Data from Storage Media		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
2.4 Prepare and sanitize storage media	2.4.1 Storage devices are configured in most common operating systems. 2.4.2 Storage devices are managed from the command line. 2.4.3 Accountability of sanitized devices is verified and managed. 2.4.4 Media is properly erased when preparing for disposing of storage media. 2.4.5 Full drive encryption is prepared.	Ability to use mount utility with major file systems Ability to mount file systems in Read-only or Read-Write configurations Ability to use utilities for media sanitization Ability to determine storage device identification in most common operating systems Knowledge of HPA and DCO areas and ability access them if needed Ability to verify and document sanitization results Ability to deploy storage device encryption	Computer forensics and information assurance software and hardware tools (Examples: eraser, EnCase, Tableau, Wipe, Cipher)
2.5 Perform remote acquisition	2.5.1 Remote connection to storage device is established. 2.5.2 Write blocking to storage device is determined. 2.5.3 Reliability of data transfer is determined. 2.5.4 Image is verified.	Ability to use F-Response Ability to use netcat and dd/dcfldd Ability to use LinEn Ability to use secure media and configure networking manually	Computer forensics and information assurance software and hardware tools (Examples: F-Response, netcat/dcfldd/dd, LinEn, NTFS Explorer, HDhost)
2.6 Perform basic data recovery	2.6.1 Existing and deleted files and folders are recovered and exported with the use of manual and automated software tools. 2.6.2 Common file headers and file extensions and related mismatches are recognized. 2.6.3 Deleted, hidden, and encrypted partitions/volumes and files are recovered. 2.6.4 Typical objects from Windows operating systems are recovered and exported. 2.6.5 Search strategies or keywords for digital evidence are developed and applied.	Knowledge of directories, sub-directories, filenames and file slack Knowledge of the rules of a FAT volume to assist in locating and recovering evidence Knowledge of key components of the $MFT Knowledge of file creation and deletion on an NTFS volume Knowledge of different uses of hashing in computer forensics analysis	Computer forensics and information assurance software and hardware tools (Examples: FTK Imager, PhotoRec, scalpel, foremost, HxD, HexWorkshop, FTK, EnCase, Autopsy)

Occupational Title: Digital Forensics Technician			
Critical Work Function 2. Manage Acquisition of Data from Storage Media		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
2.7 Perform data acquisition from virtual machines	2.7.1 Virtual machine storage devices are acquired. 2.7.2 Virtual machine memory is acquired. 2.7.3 Type of virtual machine used is determined. 2.7.4 External storage device connections to virtual machines are determined.	Ability to acquire virtual disks Ability to take snapshot of current system state Ability to determine the type and location of external storage devices	Computer forensics and information assurance software and hardware tools (Examples: FTK Imager, EnCase)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 2:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 2. Manage Acquisition of Data from Storage Media																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
2	3	5	3	4	4	4	3	3	3	3	2	4	4	3	4	5

Statement of Assessment for Critical Work Function 2:

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event.
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 3. Analyze Data from Mobile and Embedded Devices		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
3.1 Determine collection method for device	3.1.1 Possible connection support on device is determined. 3.1.2 Cable for acquisition is selected. 3.1.3 Supported Bluetooth connection is determined. 3.1.4 Device settings are changed for connection success. 3.1.5 Forensic tool supports and device mode are determined.	Knowledge of connection methods specific for mobile devices Ability to use Bluetooth to connect to device Ability to use cable to connect to mobile devices Ability to use Sync software to connect to devices Ability to use IEEE 802.X to connect devices	Internet browsers (Examples: Internet Explorer, Firefox, Chrome, Opera) Computer forensics and information assurance software and hardware tools
3.2 Research device characteristics	3.2.1 Device characteristics are researched from reliable source. 3.2.2 Technical information related to acquisition is interpreted. 3.2.3 Possible storage locations and communication technology support are evaluated. 3.2.4 Tool supports and level of support are researched. 3.2.5 Supporting tool report features and their completeness as it relates to requested data are determined. 3.2.6 Precautions and procedures in device seizure are followed. 3.2.7 Integrity of data on mobile device is maintained. 3.2.8 Technology creates physical signal protection. 3.2.9 Flight mode protection for device is determined.	Ability to search and maintain reliable database of device features Ability to selectively eliminate irrelevant information Ability to determine the proper tool for analysis Ability to triage the device based on examination request requirements Ability to use Faraday bags and strong hold boxes Ability to document procedures Ability to maintain power without outside interference with device Knowledge of the characteristics of RFID systems Ability to avoid remote interference with device acquisition	Internet browsers Computer forensics and information assurance software and hardware tools (Examples: BlackBag, Faraday bag, Faraday cage, Tag and Bag, airplane mode, Excel, Access, CaseNotes)

Occupational Title: Digital Forensics Technician			
Critical Work Function 3. Analyze Data from Mobile and Embedded Devices		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
3.3 Collect and investigate device specific data	3.3.1 Android logical, physical and file system images are processed. 3.3.2 Apple IOS logical, physical and file system images are processed. 3.3.3 BlackBerry logical, physical and file system images are processed. 3.3.4 Relevant data from SIM cards are extracted. 3.3.5 Relevant evidence from GPS devices is extracted. 3.3.6 Digital media players are processed. 3.3.7 String searches, data carving, and email forensics are performed. 3.3.8 Mobile devices are collected and investigated for backup.	Ability to use standard mobile forensic file systems and tools Ability to query and extract mobile data Ability to draw conclusions based on examined data Knowledge of other digital media and related technologies Ability to interpret SIM file system Knowledge of mobile device wireless communication technologies	Computer forensics and information assurance software and hardware tools (Examples: CelleBrite, Device Seizure, XRY, *Oxygen Forensic* Suite, SQLite viewer, plist viewer, FTK Imager, EnCase)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 3:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 3. Analyze Data from Mobile and Embedded Devices																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
3	2	5	4	4	4	5	3	4	3	3	3	4	4	4	5	5

Statement of Assessment for Critical Work Function 3:

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event.
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 4. Analyze Windows Based Artifacts		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
4.1 Investigate file and file system related artifacts	4.1.1 File download activities are conducted according to established criteria. 4.1.2 File manipulation activities are conducted according to established criteria. .	Ability to search and analyze email, deleted files, file access dates and time, registry artifacts, recent files Ability to open/save MRU and artifacts related to Office or other applications in the Cloud	Computer forensics and information assurance software and hardware tools (Examples: Regripper, Registry Viewer, Windows File Analyzer, rifiuti, FTK, EnCase, SIFT, Kaspersky, AVG, BitDefender, virustotal.com) Various open source tools
4.2 Investigate application specific artifacts	4.2.1 Program execution activities are investigated. 4.2.2 Account usage facts are determined. 4.2.3 Internet browser usage artifacts are determined.	Ability to search and analyze LNK files and MRU Ability to search and analyze account settings Ability to search and analyze internet history	Computer forensics and information assurance software and hardware tools (Examples: Notepad++, UserAssistView, UserAssist, Regripper, FTK, EnCase, SIFT)
4.3 Investigate system specific artifacts	4.3.1 Physical location related artifacts are determined. 4.3.2 Volatile data is collected and analyzed. 4.3.3 Logs are analyzed. 4.3.4 Language used on device (real or symbolic) is determined.	Ability to analyze registry settings Ability to analyze network history Ability to analyze running process Ability to analyze event logs	Computer forensics and information assurance software and hardware tools (Examples: Volatility, log2timeline, Regripper, Registry Viewer, Pasco, Web Historian, Net Analysis, CacheBack, Memoryze, Redline)

Occupational Title: Digital Forensics Technician			
Critical Work Function 4. Analyze Windows Based Artifacts		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
4.4 Investigate device specific artifacts	4.4.1 External storage device connection related artifacts are determined. 4.4.2 File/partition related artifacts are determined.	Ability to examine registry for attached USB devices Ability to identify and examine standard file systems and partitions	Computer forensics and information assurance software and hardware tools (Examples: Regripper, FTK , EnCase, SIFT, AnalyzeMFT, Ntfswalk, and/or NDXParse.py, LogParser, Kaspersky, AVG, BitDefender)
4.5 Process Windows registry analytics	4.5.1 Profile users and group related information are extracted. 4.5.2 Registry data located in unallocated space is recovered. 4.5.3 Relevant data about software no longer installed on the system is gathered using the Windows registry.	Ability to extract key information from registry files Ability to identify and capture registry files	Computer forensics and information assurance software and hardware tools (Examples: Regripper, Registry Viewer, Registry Decoder, Reglookup, YARU)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 4:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 4. Analyze Windows Based Artifacts																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
2	3	5	5	5	4	4	3	4	3	3	3	4	4	4	5	5

Statement of Assessment for Critical Work Function 4:

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event.
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 5. Analyze Mac Based Artifacts		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
5.1 Process file system	5.1.1 iOS file system files are recognized. 5.1.2 Logical and physical acquisition steps are followed. 5.1.3 Users' home directory is analyzed. 5.1.4 Version of operating system is established. 5.1.5 Slack space types and their location are differentiated.	Ability to use tools and Intel based systems Ability to use SIFT Ability to identify and recover lost, damaged, and deleted files Ability to disable disk arbitration and manual mount file system as Read-Only Ability to examine Apple Mac HFS+ computers Knowledge of purpose of inodes	Computer forensics and information assurance software and hardware tools (Examples: BlackBag, SIFT, Sumuri, PALA, Raptor)
5.2 Evaluate partition configurations	5.2.1 Partition schemes and their characteristics are distinguished. 5.2.2 Logical partition is mounted as Read-Only. 5.2.3 Malware is identified by scanning. 5.2.4 Hard drive is forensically imaged.	Ability to identify GUID (Globally Unique Identifier) Partition Table, Apple Partition Map, and Master Boot Record Ability to use investigative software and related open source tools Ability to boot into Single User or Target mode if it is available Ability to distinguish between PowerPC and Intel Macintosh models	Computer forensics and information assurance software and hardware tools (Examples: The Sleuth Kit (TSK), Autopsy Forensic Browser)
5.3 Investigate configured services	5.3.1 Forensically safe acquisition is performed. 5.3.2 Verification is performed. 5.3.3 Detailed documentation of service states and configurations are prepared. 5.3.4 Command history is examined. 5.3.5 Boot process is controlled. 5.3.6 Timeline of events is created. 5.3.7 Metadata is extracted. 5.3.8 FileVault in activation is determined.	Ability to physically secure evidence or conduct on-site preview (Collection) Ability to acquire, verify, and archive digital media data Ability to report results Knowledge of the Macintosh Keychain utility works Ability to decode .plist files Knowledge of common Apple operating system logs and the data they contain Ability to identify artifacts of usage, access, existence and execution	Computer forensics and information assurance software and hardware tools (Examples: BlackBag, The Sleuth Kit (TSK), X-Ways, plist viewer)

Occupational Title: Digital Forensics Technician			
Critical Work Function 5. Analyze Mac Based Artifacts		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
5.4 Investigate Internet related artifacts	5.4.1 Mac Office suites installed on suspect media are identified, and files are viewed and their metadata created by the applications. 5.4.2 Email storage location on Macintosh system is located. 5.4.3 Mechanics and attributes of Time Machine are determined. 5.4.4 Application data display in the native Macintosh environment is determined. 5.4.5 DropBox user i.d. is determined. 5.4.6 Bundled applications are investigated.	Knowledge of artifacts related to applications Ability to create timeline from log files Ability to examine appropriate applications (e.g., iCal, Address Book, Mail, .Mac, Safari, iChat), and logs related to application activities Ability to view Time Machine volumes	Computer forensics and information assurance software and hardware tools (Examples: BlackBag, The Sleuth Kit (TSK) X-Ways, plist viewer)
5.5 Investigate user history related artifacts	5.5.1 Command history is examined. 5.5.2 User home directory is examined. 5.5.3 File access rights owned by user are determined.	Ability to interpret history contents Ability to identify and extract file metadata conforming to scope of case Ability to evaluate file access rights and determine validity	Computer forensics and information assurance software and hardware tools Command line tools (Examples: umask, chmod, ls), log2timeline, vi, emacs, BlackBag, The Sleuth Kit (TSK), X-Ways, plist viewer)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 5:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

<table>
<tr><th colspan="17">Occupational Title: Digital Forensics Technician</th></tr>
<tr><th colspan="17">CWF 5. Analyze Mac Based Artifacts</th></tr>
<tr><td>Listening</td><td>Speaking</td><td>Using Information and Communication Technology</td><td>Gathering and analyzing Information</td><td>Analyzing and Solving Problems</td><td>Making Decisions and Judgments</td><td>Organizing and Planning</td><td>Using Social Skills</td><td>Adaptability</td><td>Working in Teams</td><td>Leading Others</td><td>Building Consensus</td><td>Self and Career Development</td><td>Writing</td><td>Reading</td><td>Mathematics</td><td>Science</td></tr>
<tr><td>3</td><td>3</td><td>5</td><td>5</td><td>5</td><td>4</td><td>4</td><td>3</td><td>4</td><td>3</td><td>3</td><td>3</td><td>5</td><td>4</td><td>5</td><td>5</td><td>5</td></tr>
</table>

Statement of Assessment for Critical Work Function 5

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 6. Analyze Linux Based Artifacts		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
6.1 Process file system	6.1.1 Disk Image in read-only mode is mounted. 6.1.2 Raw, E01, AFF disk images are acquired and mounted. 6.1.3 Inodes are examined for possible deleted files.	Ability to mount images as a loopback device Ability to distinguish appropriate types of file systems (e.g., ext2, ext3, ext4) Ability to acquire file system in forensically sound manner Ability to protect file system by providing software write blocking Ability to verify collection Ability to access Linux file system from Windows Knowledge of LVM identification and modification	Computer forensics and information assurance software and hardware tools (Examples: ssdeep & md5deep,FTK, Explore2fs (Read-only Access), Ext2 IFS (Installable File System), DiskInternals Linux reader (Read-only Access),Ext2 FSD (File System Driver), Ext2Read,SIFT))
6.2 Evaluate partition configurations	6.2.1 Software RAID configuration is determined. 6.2.2 MBR is investigated. 6.2.3 Partition information is displayed using native tools. 6.2.4 Specific partitions utilizing command line tools are manually mounted.	Ability to troubleshoot Linux boot process Ability to use fdisk, cfdisk, mount, and other native tools Ability to mount partition as read-only Ability to dissect MBR using GUI and command line hex viewers Ability to configure Linux MD service	Computer forensics and information assurance software and hardware tools (Examples: FTK Imager, EnCase, FTK, fdisk, cfdisk, mount, md)
6.3 Investigate configured services	6.3.1 Basic Memory Image is analyzed. 6.3.2 Configuration of services is analyzed. 6.3.3 Volatile data based on order of volatility are captured.	Ability to examine the /etc/init.d/ folder and interpret contents Ability to determine non-standard services Ability to determine running services and open ports Ability to analyze and interpret configuration files Ability to analyze proc structure and access	Computer forensics and information assurance software and hardware tools (Examples: WireShark, Volatility, Framework, Memoryze, vi, emacs, hexdump,dd, dcfldd, natstat)

Occupational Title: Digital Forensics Technician			
Critical Work Function 6. Analyze Linux Based Artifacts		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
6.4 Investigate Internet related artifacts	6.4.1 Open Office suites installed on suspect media are identified and files and their metadata created by applications are viewed. 6.4.2 E-mail stored on Linux system is located. 6.4.3 Mechanics and attributes of encryption software are determined. 6.4.5 Application data in native Linux environment are displayed. 6.4.6 DropBox is identified. 6.4.7 Bundled applications are investigated.	Knowledge of the artifacts related to email, Knowledge of Internet browsers, and types of web applications Ability to decode log files Ability to create timeline from log files Ability to examine chat room software and logs related to application activities	Computer forensics and information assurance software and hardware tools (Examples: The Sleuth Kit, DFLabs PTK/ Autopsylog2timeline, EnCase, FTK, Pasco)
6.5 Investigate user created artifacts	6.5.1 Command history is examined. 6.5.2 User home directory is examined. 6.5.3 File access rights owned by user are analyzed. 6.5.4 Timeline of user activity is created.	Ability to interpret history contents Ability to identify and extract file metadata conforming to scope of case Ability to evaluate file access rights and determine validity Ability to identify files of interest for timeline generation Ability to analyze and report on syslog, utmp, wtmp	Computer forensics and information assurance software and hardware tools (Examples: The Sleuth Kit, DFLabs PTK/ Autopsy, log2timeline, Pivot Table in MS Excel and OO Calc, EnCase, FTK, Vinetto, Rifiuti, Foremost/Scalpel, PhotoRec)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 6:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 6. Analyze Linux Based Artifacts																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
2	2	5	5	4	3	4	3	4	3	3	4	5	3	3	4	4

Statement of Assessment for Critical Work Function 6

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 7. Analyze Network Based Data Acquisitions		**Occupational Skills, Knowledge & Conditions**	
Key Activity	Performance Criteria *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
7.1 Investigate network log files	7.1.1 Types of information that may be contained within remote log servers are determined. 7.1.2 Relevant evidence that can be found on IDS or sniffer is determined. 7.1.3 Physical and logical layout of analyzed network is visualized. 7.1.4 IP addresses and GPS coordinates are map captured. 7.1.5 Logs related to VoIP are determined. 7.1.6 System log files are investigated. 7.1.7 Format of log files is identified.	Ability to recognize various types of network topologies and their properties/attributes Knowledge of Intrusion Detection Systems (IDSs) Knowledge of Active Directory and how it is used in Windows networked environment Ability to determine importance of switch and switch types during network investigation Knowledge of data transfer protocols Ability to analyze various network logs	Computer forensics and information assurance software and hardware tools (Examples: Wireshark, nmap, kismet, hydra, netstat, arp, route, BackTrack, Network Miner, LogParser, log2timeline, SNORT, Barnyard, Snorby)
7.2 Establish secure file transfer and network communication	7.2.1 File transfer over network is utilized. 7.2.2 Best method of file transfer is determined. 7.2.3 Licenses and certificates are configured and managed. 7.2.4 Network credentials are protected. 7.2.5 Anonymity and minimal footprint are maintained. 7.2.6 Secure wireless networks are connected.	Ability to use. ftp and sftp Ability to configure, use, and manage SSH Ability to maintain and secure credentials Ability to establish secure wireless connection Ability to utilize anonymizers Ability to use tunneling and TOR	Computer forensics and information assurance software and hardware tools (Examples: WinSCP, Putty, TOR)

Occupational Title: Digital Forensics Technician			
Critical Work Function 7. Analyze Network Based Data Acquisitions		**Occupational Skills, Knowledge & Conditions**	
Key Activity	Performance Criteria *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
7.3 Investigate network packet captures	7.3.1 Chat conversations from packet captures are extracted. 7.3.2 Multimedia from packet captures are extracted. 7.3.3 Application specific activity from packet captures is extracted. 7.3.4 Source and destination of communication are identified. 7.3.5 Domain name and server (DNS) records and attributes are analyzed. 7.3.6 Pattern searches are performed. 7.3.7 GUI and command line tools are utilized. 7.3.8 Patterns are identified. 7.3.9 Anomalies are identified.	Ability to investigate pcap files Ability to use automated tools to analyze packet captures Ability to export artifacts in required format and metadata intact Ability to create and use custom filters Ability to construct custom filters for .pcap files Ability to determine false positives and minimize false negatives Ability to recognize "abnormal" communication pattern Ability to use regular expressions	Computer forensics and information assurance software and hardware tools (Examples: NetworkMiner, NetWitness, tshark, ngrep, Wireshark)
7.4 Determine status of network based sensors	7.4.1 Operation of network sensors at intrusion is verified. 7.4.2 Reliability of network captures is determined. 7.4.3 Sensor configuration on client operating system is determined. 7.4.4 Sensors on network and local operating systems are deployed.	Ability to deploy and configure appropriate sensors Ability to determine anomalies in packet captures Ability to deploy and determine client sensor functionality	Computer forensics and information assurance software and hardware tools (Examples: SNORT, Netwitness, ping, nmap)
7.5 Investigate SCADA specific artifacts	7.5.1 Challenges associated with control systems are identified. 7.5.2 Commands specific to control systems are captured. 7.5.3 Command anomalies are identified.	Knowledge of appropriate protocol command set (e.g., Modbus) Ability to identify patterns of reconnaissance Ability to perform signature based analysis	Computer forensics and information assurance software and hardware tools (Examples: Wireshark, WinHex, Hex Workshop, HxD, PLC) Various tools used to design ladder logic (Example: NIST SP800-32)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 7:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 7. Analyze Network Based Data Acquisitions																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
2	2	5	4	5	4	4	2	3	3	3	2	5	3	3	5	5

Statement of Assessment for Critical Work Function 7

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 8. Manage Digital Forensics Laboratory Environments		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
8.1 Perform system configuration, hardening, and maintenance	8.1.1 System to prevent malicious code propagation is configured. 8.1.2 Trust backup for quick restore is created. 8.1.3 Virtual machine is configured. 8.1.4 Server hardening and maintenance are performed. 8.1.5 Operating system and application hardening are performed. 8.1.6 Patch management is configured.	Ability to utilize ghosting software Ability to configure virtual machine and vm networking Ability to follow NIST's Security Configuration Checklists Ability to maintain patching manually and automatically	Various client/server operating systems from Microsoft, Apple, and Linux NIST reference guide for ladder logic tools (e.g. SP800-83, SP800-53)
8.2 Configure network storage devices	8.2.1 SAN is maintained. 8.2.2 NAS is maintained. 8.2.3 Cloud computing environment is utilized.	Ability to replace hardware Ability to perform scheduled maintenance Ability to monitor available storage resources	Various client/server operating system tools from Microsoft, Apple, and Linux (Examples: Ubuntu, ReadyNAS)
8.3 Maintain laboratory equipment	8.3.1 Hardware and firmware upgrades are performed. 8.3.2 Components are organized and maintained. 8.3.3 Licensing is maintained. 8.3.4 Forensic field kits are utilized. 8.3.5 Secure storage and communication are configured.	Ability to perform firmware upgrades Ability to maintain organized and properly labeled components Ability to track and plan for license upgrades Ability to use laptops/handheld imagers Ability to use and maintain ftp and sftp Ability to configure RAID0, RAID1, RAID2, RAID1+0, RAID5 and RAID10 Ability to maintain SSH	Various client/server operating systems from Microsoft, Apple, and Linux (Examples: TrueCrypt, Putty)
8.4 Configure acquisition/ investigation system	8.4.1 Fastest and most reliable bust type is determined. 8.4.2 Multiboot operating system is installed. 8.4.3 Software based write blockers are maintained. 8.4.4 Internal hardware write blocker is installed. 8.4.5 Forensics software is installed. 8.4.6 Reliable case management is provided.	Ability to keep updated attack vectors on servers Ability to track IIS log format changes Ability to update knowledge on Web attacks Knowledge of the latest methods of Web page defacement Ability to follow internal procedures to case management	Various client/server operating systems from Microsoft, Apple, and Linux (Examples: FTK/UTK, EnCase, SleuthKit, SIFT, Helix, CAINE, BackTrack, BitDefender, Kaspersky, WinFE)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 8:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 8. Manage Digital Forensics Laboratory Environments																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
2	3	5	5	5	4	4	3	4	3	3	3	4	3	3	3	3

Statement of Assessment for Critical Work Function 8

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question

Occupational Title: Digital Forensics Technician			
Critical Work Function 9. Manage Recovery and Extraction of Big data		**Occupational Skills, Knowledge & Conditions**	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
9.1 Inventory big data	9.1.1 Evidence is securely transported and stored. 9.1.2 Chain of Custody is maintained. 9.1.3 Standard operating procedures for media management are followed.	Ability to use barcode scanners Ability to lift and carry physical devices Knowledge of potential risks of handling evidence Ability to verify device identifications and document unique characteristics Ability to identify visual damage before receiving	Computer forensics and information assurance software and hardware tools (Examples: Access, Excel, CaseNotes), Barcode readers
9.2 Catalog stored big data	9.2.1 Header scans are performed. 9.2.2 System scans are performed. 9.2.3 Scanned data is indexed. 9.2.4 Data relevancy is identified.	Ability to use indexing tools Ability to manage database tools Ability to configure and apply noise reduction filters Ability to configure encoding types and needs (e.g. ASCII, UNICODE, BASE-64) Ability to process complex file types (e.g., zip, rar, 7z)	Barcode readers Computer forensics and information assurance software and hardware (Examples: dtSearch, Mount Image Pro, OCR, EnCase, FTK)
9.3 Restore big data	9.3.1 Data is restored from tapes and other storage media. 9.3.2 Non-native restorations are performed. 9.3.3 Data restoration without need of native backup is performed. 9.3.4 Data that is inaccessible by native tools or damaged is recovered. 9.3.5 E-discovery acquisition is performed.	Ability to perform tasks accurately in a timely manner Knowledge of technology changes and reliable tools Knowledge of tool configuration settings and consequences Ability to select tool for task at hand Ability to reconstruct damaged data if needed Ability to evaluate file headers for manual reconstruction Knowledge of multi-threaded restoration methods and tools Ability to preserve all metadata while processing	Computer forensics and information assurance software and hardware (Examples: EnCase, FTK)

Occupational Title: Digital Forensics Technician			
Critical Work Function 9. Manage Recovery and Extraction of Big data		Occupational Skills, Knowledge & Conditions	
Key Activity	**Performance Criteria** *How do we know when the key activity is performed well or performed successfully?*	**Occupational Skills & Knowledge** *What should the technician know and what skills should the technician have in order to do the activity?*	**Conditions** *What tools must the technician use in order to do the activity?*
9.4 Extract mailboxes from big data	9.4.1 Mailboxes in many types of databases are extracted and restored on forensics system for review. 9.4.2 Types of mailboxes and possible protections are identified. 9.4.3 Email files from a mailbox are collected. 9.4.4 Recovered emails are converted to other formats.	Ability to configure software to extract emails from case (e.g., .PST, .MBX, .DBX) Ability to convert recovered emails to .PST format Knowledge of procedures to recover emails from server storage archives (.EDB, .NSF, .DB) Knowledge of encryption and password protection related to email storage Ability to extract Microsoft Exchange mailboxes Ability to convert emails to given format Ability to perform email analysis and metadata extraction Knowledge of types of email formats Ability to recognize Web based mail	Computer forensics and information assurance software and hardware tools (Examples: EnCase, FTK, NUIX, Clearwell, Recover My Email, big extractor (SIFT))
9.5 Filter relevant big data	9.5.1 Data is de-duplicated across multiple custodians. 9.5.2 Near duplicates are identified. 9.5.3 Filters are applied to data. 9.5.4 Keyword searches are performed. 9.5.5 Data volume is reduced by reliable methods.	Ability to utilize search tools (e.g., dtSearch) Ability to evaluate search results for completeness (e.g., ASCII, UNICODE, Base64, and other common encodings) Ability to construct regular expression based search strings Ability to identify patterns that will result in fastest processing Ability to modify existing search queries Knowledge of appropriate programming language Knowledge of language settings	Computer forensics and information assurance software and hardware (Examples: dtSearch, EnCase, FTK, KFF) Databases: Microsoft, Sequel, Progres, Oracle
9.6 Prepare data sets in required formats	9.6.1 Load files or data loaded to storage media are created. 9.6.2 Procedures to sign off on completed projects are established. 9.6.3 Documentation to maintain Chain of Custody after processing is produced. 9.6.4 Relevant content is delivered in secure and reliable manner.	Ability to create load file headers based on predefined default fields Knowledge of default field mappings in tools Ability to adjust load file parameter modification based on request	Computer forensics and information assurance software and hardware (Examples: Concordance, Summation)

Academic and Employability Knowledge and Skill Matrix for Critical Work Function 9:

On a scale of 1 (lowest) to 5 (highest), identify the level of complexity required in each of these skills for the worker to perform the critical work function. Keep in mind that this scale is not for rating an individual's proficiency. It is intended only for rating the level of complexity required to do the work.

Occupational Title: Digital Forensics Technician																
CWF 9 Manage Recovery and Extraction of Big Data																
Listening	Speaking	Using Information and Communication Technology	Gathering and analyzing Information	Analyzing and Solving Problems	Making Decisions and Judgments	Organizing and Planning	Using Social Skills	Adaptability	Working in Teams	Leading Others	Building Consensus	Self and Career Development	Writing	Reading	Mathematics	Science
2	2	5	5	4	4	4	3	3	3	3	3	2	2	2	4	4

Statement of Assessment for Critical Work Function 9

The statements of assessment can do any of several things:

- *Define tools or strategies that industry could use to assess the level of competency a worker has attained in a particular critical work function.*
- *Define for trainers and educators how to assess the level of competency a student has attained relevant to the critical work function.*
- *Define the level of mastery of the critical work function that indicates that a worker or student has achieved an entry-, intermediate-, or advanced level of mastery of a critical work function.*

A. Tests could include:

1) Multiple choice and essay questions that demonstrate an understanding of knowledge being assessed.
2) Preparation and justification of a reasonable solution to a problem scenario.

B. Hands-on exercises or simulations to demonstrate acquisition of knowledge and skills that could:

1) Apply relevant knowledge or skills
2) Focus on the application of knowledge and skills to a new situation
3) Demonstrate an ability to plan, organize, and create a product, service, or an event
4) Illustrate by individual performance the attained levels of knowledge and skills
5) Include observation of events, groups, and individuals that focuses on the relevant traits of the skill in question