Cyber Security/Forensics Infusion Units

CYBR Any

Table of Contents

Acknowledgments

The components of this instructional framework were revised by a combined group of industry experts and teachers:

Glenn S. Dardick, Ph.D., CCE (ISFCE), CCFP (ISC2), Director, Longwood Center for Cyber Security, Longwood University, Farmville
Shawn Gross, Educational Specialist for Pre-Engineering and Industrial Careers, Henrico County Public Schools
Lauren-Anne Sledzinski, Teacher, Trade and Industrial Education, Hermitage Technical Center, Henrico County Public Schools
Keisha Leonard, Teacher, Business and Information Technology, Hermitage Technical Center, Henrico County Public Schools
Shirley Bazdar, Director, Career and Technical and Adult Education, Loudoun County Public Schools
Ken Shade, Teacher, Cyber Security, Chantilly Academy, Fairfax County Public Schools
Michael E. Miklich, President, iForCE, Institute for Cyber Security Education, Haymarket
Stephanie Holt, Program Manager, Business and Information Technology, Fairfax County Public Schools
Ray Kinard, Director, Cyber Academy, Northrop Grumman
General Bernard K. Skoch, Commissioner, AFA CyberPatriot

The framework was edited and produced by the CTE Resource Center:

Margaret L. Watson, Administrative Coordinator
Darren E. Morris, Writer/Editor

Judith P. Sams, Specialist, Business and Information Technology and Related Clusters
Office of Career and Technical Education Services
Virginia Department of Education

Edward Sullivan, Specialist, Trade and Industrial Education and Related Clusters
Office of Career and Technical Education Services
Virginia Department of Education

B. Anne Rowe, Coordinator, Curriculum & Instruction
Office of Career and Technical Education Services
Virginia Department of Education

Lolita B. Hall, Director
Office of Career and Technical Education Services
Virginia Department of Education

Course Description

Suggested Grade Level: 9 or 10 or 11 or 12

The need for personal and professional cyber security skills has never been greater. The Cyber Security/Forensics infusion units are comprised of three main pieces: Cyber Security Foundations, Social Engineering and Personal Cyber Security, and Cyber Forensics. All tasks are listed as optional so that instructors may customize the units as they wish.

Task Essentials Table

- Tasks/competencies designated by plus icons (⊕) in the left-hand column(s) are essential
- Tasks/competencies designated by empty-circle icons (○) are optional
- Tasks/competencies designated by minus icons (⊖) are omitted
- Tasks marked with an asterisk (*) are sensitive.

Task Number	CYBR	Tasks/Competencies
Unit 1: CYBER SECURITY FOUNDATIONS		
Exploring the Foundations of Cyber Security		
001	○	Define *cyber system* and industry-specific terminology.
002	○	Provide background on fundamental information technology security concepts.
003	○	Create a framework to protect information systems.
004	○	Describe information technology ethics and an acceptable use policy (AUP).
005	○	Act upon AUP infractions.
Working with Virtual Machines		
006	○	Define components of and terminology related to virtual machines.
007	○	Identify advantages and disadvantages of using virtual machines.
008	○	Determine software downloading and installation procedures for virtual machines.
009	○	Perform common tasks, using a virtual machine.
Exploring Cyber Careers		
010	○	Research career opportunities for cyber security/forensics professionals.
011	○	Identify the educational pathways for emerging cyber security and cyber forensics professionals.
012	○	Identify career paths and job titles within the cyber security/forensics industry and related Career Clusters.
Unit 2: SOCIAL ENGINEERING AND PERSONAL CYBER SECURITY		
Establishing Passwords		

013	○	Verify that Web sites are secure before submitting personal or corporate information.	
014	○	Describe vulnerabilities associated with using automated teller machines (ATM).	
015	○	Describe keylogging vulnerabilities.	
016	○	Establish a password protocol and policy.	
Maintaining Endpoint Security			
017	○	Install an operating system and components.	
018	○	Install service packs and updates.	
019	○	Update installed applications.	
020	○	Install and update anti-virus/anti-spyware utilities.	
021	○	Configure critical operating system parameters.	
022	○	Enable security and auditing logs.	
023	○	Back up a system.	
024	○	Restore a system from a backup.	
025	○	Secure a router connection.	
026	○	Secure other personal/mobile devices.	
027	○	Secure a game console.	
Maintaining Network Security			
028	○	Describe network topologies.	
029	○	Identify network vulnerabilities.	
030	○	Describe methods for strengthening network security.	
031	○	Identify components of physical security.	
032	○	Identify common network devices.	
033	○	Identify protocols.	
034	○	Describe the fundamentals of domain names.	
035	○	Describe network configuration tools.	

Implementing Threat Mitigation			
036	○	Set up a schedule for anti-virus scans.	
037	○	Run an anti-virus scan.	
038	○	Respond to results from an anti-virus scan.	
039	○	Research the nature (i.e., motivations) and scope (i.e., prevalence) of current and past threats.	
040	○	Report system anomalies.	
Unit 3: CYBER FORENSICS			
Exploring Ethical and Legal Issues			
041	○	Identify laws applicable to cyber.	
042	○	Describe the rule of law and its impact on cyber forensics.	
043	○	Identify rules of evidence relevant to cyber forensics.	
Applying Legal Procedures			
044	○	Describe ISO/IEC-27037 and its relevance to cyber forensics.	
045	○	Describe the importance of using a write blocker or best effort to preserve evidence.	
046	○	Create a forensic image and establish hash code, using a write blocker.	
047	○	Establish and maintain the chain of custody.	
Identifying Media			
048	○	Identify types of media hardware.	
049	○	Identify types of hardware interfaces.	
Exploring Media Forensics			
050	○	Identify common file systems.	
051	○	Identify types of artifacts.	
052	○	Identify geometry parameters of physical media.	
053	○	Recover artifacts from physical media.	
Conducting Mobile Devices Forensics			

054	○	Change EXIF (exchangeable image file format).	
055	○	Extract text messages.	
056	○	Extract call logs.	
057	○	Extract unique identifiers from components.	

Legend: ⊕Essential ○Non-essential ⊖Omitted

Curriculum Framework

Unit 1: CYBER SECURITY FOUNDATIONS

Exploring the Foundations of Cyber Security

Task Number 001

Define *cyber system* and industry-specific terminology.

Definition

Definitions should include

- cyber system—a system of collaborating computational elements controlling physical entities
- information technology— the development, implementation, and maintenance of computer hardware and software systems to organize and communicate information electronically
- cyber security—the processes and mechanisms by which computer-based equipment, information, and services are protected from unintended or unauthorized access, change, or destruction, including protection from unplanned events and natural disasters
- password—a basic security mechanism that consists of a secret phrase to restrict access to a system, application, or service
- spam—unsolicited bulk electronic messages
- copyright law and plagiarism—legal protections for the creator of information or original work, including plagiarism, the wrongful use of another person’s or entity’s original expressions or ideas, typically without crediting the originator
- network computing—working within a system of connected devices or computers

Task Number 002

Provide background on fundamental information technology security concepts.

Definition

Provision should include

- authentication
- access control
- data integrity
- confidentiality
- accountability
- loss prevention and recovery.

Task Number 003

Create a framework to protect information systems.

Definition

Creation should include identifying

- the type of organization the system serves
- the existing components of the system
- data used and how it is used
- the individuals who have system access
- the users and the purpose of the system
- existing policies, standards, and procedures and how they might need to change
- the enforcement of policy
- monitoring procedures, network audit trails.

Task Number 004

Describe information technology ethics and an acceptable use policy (AUP).

Definition

Description should include the following:

- Information technology ethics are legally interpreted through an AUP, a written set of rules that governs the use of computer equipment and network access and provides the framework and consequences for any end-user violations.
- The purpose or rationale of an AUP is to ensure that there is proper use of technology within the entity (e.g., business, school, organization) to promote productivity and limit liability.

AUP laws pertaining to information technology and ethics include the following:

- Computer Fraud and Abuse Act (CFAA)
- Electronic Communications Privacy Act (ECPA)
- Digital Millennium Copyright Act (DMCA)
- No Electronic Theft Act (NET)
- Prioritizing Resources and Organization for Intellectual Property Act of 2008 (Pro-IP Act)

Task Number 005

Act upon AUP infractions.

Definition

Actions should include

- alerting appropriate parties of unethical behavior
- determining the consequences of unethical behaviors, based on related court decisions.

Working with Virtual Machines

Task Number 006

Define components of and terminology related to virtual machines.

Definition

Definitions should include the following components:

- Hardware with virtual machine support

- Programs (i.e., applications) running on virtual machines
- The operating system

Definitions should include the following terminology:

- Virtual machine
- System virtual machine
- System platform
- Operating system (OS)
- Hardware virtualization
- Cloud computing
- Process virtual machine
- Single program
- Single process
- Program portability
- Program flexibility
- Virtual memory
- Kernel SamePage Merging (KSM)
- Embedded systems
- Real-time operating system
- Sandbox
- Application virtual machine
- Managed runtime environment (MRE)
- Operating system-level (server virtualization)

Task Number 007

Identify advantages and disadvantages of using virtual machines.

Definition

Identification should include

- advantages—
  - Server consolidation
  - Many applications on each server
  - Maximum server utilization, minimum server count
  - Faster, easier application and resource provisioning
  - High application availability
  - Wizard-based guides for ease of installation
  - Simple, streamlined management
  - Higher reliability and performance
  - Superior security
  - Greater savings
  - Affordability
- disadvantages—

    - Magnified physical failures
    - Degraded performance
    - New skills and training required
    - Complex root-cause analysis
    - New management tools needed
    - Virtual machine sprawl
    - Virtual habits

Task Number 008

Determine software downloading and installation procedures for virtual machines.

Definition

Determination should be made by following

- manufacturer guidelines
- instructor specifications.

Task Number 009

Perform common tasks, using a virtual machine.

Definition

Performance should include

- system virtual machine tasks
- process virtual machine tasks
- operating system-level virtualization (server virtualization) tasks.

Exploring Cyber Careers

Task Number 010

Research career opportunities for cyber security/forensics professionals.

Definition

Research should include using online job research and job posting sites (e.g., Virginia Employment Commission) to locate entry-level cyber security and cyber forensics opportunities at the local, state, national, and international levels.

Task Number 011

Identify the educational pathways for emerging cyber security and cyber forensics professionals.

Definition

Identification should include

- online resources that specialize in providing this type of information (e.g., O*Net online, Bureau of Labor Statistics, Virginia Wizard)
- common pathways based on industry requirements
- academic goals
- career and technical education goals
- postsecondary options.

Task Number 012

Identify career paths and job titles within the cyber security/forensics industry and related Career Clusters.

Definition

Identification should include

- related Career Clusters (e.g., Government and Public Administration; Information Technology; Law, Public Safety, Corrections and Security; Science, Technology, Engineering and Mathematics)
- Career Pathways related to selected Career Clusters
- job titles related to selected paths.

Unit 2: SOCIAL ENGINEERING AND PERSONAL CYBER SECURITY

Establishing Passwords

Task Number 013

Verify that Web sites are secure before submitting personal or corporate information.

Definition

Verification should include

- checking the uniform resource locator (URL)
- applying the Web browser’s security features
- applying third-party security software features.

Task Number 014

Describe vulnerabilities associated with using automated teller machines (ATM).

Definition

Description should include vulnerabilities in

- physical security—the hardware that prevents the actual break-in of an ATM
- logical security—protection from malware
- fraud protection—techniques used to prevent theft of money or information (e.g., skimming) related to authorized account access and user identification.

Task Number 015

Describe keylogging vulnerabilities.

Definition

Description should include

- a definition of keylogging and the type of information that can be recorded or copied
- hidden keystroke logging devices
- flawed encryption techniques
- vulnerabilities in browsers, applications, and scripts.

Task Number 016

Establish a password protocol and policy.

Definition

Establishment should include

- describing the rationale of password security
- identifying the vulnerabilities of password security
- researching models for protocols and policies
- writing specific protocol and policy, based on a system scenario.

Maintaining Endpoint Security

Task Number 017

Install an operating system and components.

Definition

Installation should include

- hardware drivers

- system services.

Task Number 018

Install service packs and updates.

Definition

Installation should include adhering to secure operating procedures, along with the following:

- Describing the philosophy behind these procedures—the reasons for installing service packs and updates
- Searching for service packs and updates, or setting the operating system to automatically search and notify the user, and ensuring that the installation is legitimate and secure
- Using both standard and custom installation procedures, following an automatic installation interface
- Setting and following a systematic schedule for these actions

---

Task Number 019

Update installed applications.

Definition

Updates should be performed for common applications (e.g., Adobe Reader, Flash Player) and include the following secure operating procedures:

- Describing the philosophy behind these procedures—the reasons for installing updates
- Searching for application updates through the applications themselves or receiving notifications from those applications that updates are available and ensuring the installation is legitimate and secure
- Using both standard and custom installation procedures, following an automatic installation interface
- Setting and following a systematic schedule for these actions
- Automating these procedures

Task Number 020

Install and update anti-virus/anti-spyware utilities.

Definition

Installation and updates should include

- distinguishing among available anti-virus/anti-spyware utilities
- scanning for malware by following secure operating procedures and identifying results.

Task Number 021

Configure critical operating system parameters.

Definition

Configuration should include establishing or following

- password policy
- access control
- audit policy
- kernel-mode driver configuration procedures.

Task Number 022

Enable security and auditing logs.

Definition

Enabling security and auditing logs should be completed according to the specific operating system and computer manufacturer specifications and include

- establishing the number of security events to be recorded, including common types, such as
    - any changes to user account and resource permissions
    - any failed attempts for user logon
    - any failed attempts for resource access
    - any modification to the system files
- configuring auditing to customize the process
- recording selected types of events in the security log of the Web server.

Task Number 023

Back up a system.

Definition

Backup of a system should be completed according to the specific operating system and computer manufacturer specifications and include

- verifying that the operation was performed to specifications
- setting a schedule for performing these operations in the future
- describing why such operations are necessary.

Task Number 024

Restore a system from a backup.

Definition

Restoration of a system should be completed according to the specific operating system and computer manufacturer specifications and include

- verifying that the operation was performed to specifications
- setting a schedule for performing these operations in the future
- describing why such operations are necessary.

Task Number 025

Secure a router connection.

Definition

Security procedures should be completed according to the specific operating system and computer manufacturer specifications and include

- encrypting network passwords
- turning off broadcasting
- disabling guest networks
- adding media access control (MAC) filtering
- acquiring a network monitoring application (e.g., Fing).

Task Number 026

Secure other personal/mobile devices.

Definition

Security procedures should be completed according to the specific operating system and computer manufacturer specifications and include

- keeping the system updated
- installing a security application
- applying safe browsing techniques
- avoiding making personal, private transactions (e.g., shopping, banking) on a public network
- acquiring applications from trusted sources
- checking (periodically) data usage for each application.

Task Number 027

Secure a game console.

Definition

Security procedures should be completed according to the specific operating system and computer manufacturer specifications and include

- ensuring that all Internet-enabled devices are updated and protected from malware and other threats, including installing the latest operating system and applications, anti-virus protection, and browsers
- using a strong online password
- reporting but refusing to engage cyberbullies
- documenting and reporting inappropriate behaviors
- omitting any personal information (e.g., name, location, gender, age, actual appearance)
- disguising or not using one's actual voice or appearance when gaming, and withholding all private information
- limiting playing time
- avoiding downloads offered from other players
- avoiding meeting other gamers in person
- assessing risks and practicing good judgment.

Maintaining Network Security

Task Number 028

Describe network topologies.

Definition

Description should include a comparison of the features, functions, characteristics, and financial considerations of local area network (LAN) topologies.

Task Number 029

Identify network vulnerabilities.

Definition

Identification should include

- network map analysis
- threat map analysis.

Task Number 030

Describe methods for strengthening network security.

Definition

Description should include

- prioritizing remediation by identifying hosts that are directly exposed to untrusted networks
- determining the actions that would provide the greatest impact to improving security.

Task Number 031

Identify components of physical security.

Definition

Identification should include

- facility characterization
- undesired events/critical assets identification
- consequence determination
- threat definition; likelihood of an attack
- protection system effectiveness analysis: detection, delay, response
- risk estimation upgrades and impacts: system

- upgrades, upgrade impact, methodology summary.

Task Number 032

Identify common network devices.

Definition

Identification should include

- hub
- repeater
- modem
- network interface card (NIC)
- media converters
- basic switch
- bridge
- wireless access point (WAP)
- basic router
- basic firewall
- basic dynamic host configuration protocol (DHCP) server.

Task Number 033

Identify protocols.

Definition

Identification should include brief descriptions of the following:

- Transmission control protocol (TCP)—a network communication protocol designed to send data packets over the Internet
- User Datagram Protocol (UDP)—part of the Internet protocol suite used by programs running on different computers on a network; UDP is used to send short messages called datagrams, but it is an unreliable, connectionless protocol
- HyperText Transfer Protocol (HTTP)—an application-layer protocol used primarily on the Internet; a stateless and connectionless protocol
- Hypertext Transfer Protocol Secure (HTTPS)—a variant of HTTP that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection
- File Transfer Protocol (FTP)—a client/server protocol used for transferring files to or exchanging files with a host computer. FTP is also the Internet standard for moving or transferring files from one computer to another using TCP or IP networks.

- Post Office Protocol (POP)—a type of computer networking and Internet standard protocol that extracts and retrieves e-mail from a remote mail server for access by the host machine

Task Number 034

Describe the fundamentals of domain names.

Definition

Description should include the following:

- Domain names are broken down into top-level domain names where the entire address in the cloud (network architecture) is considered to be the fully qualified domain name (FQDN).
- There is a need for top-level domain (TLD) names that can be used by a root server for creating names without fear of conflicts with current or future actual TLD names in the global Domain Name System (DNS).
- DNS—a hierarchical, distributed naming system for computers, services, or any resource connected to the Internet/cloud or a private network/private cloud. DNS associates information with domain names assigned to each of the partaking bodies and translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services attached to the Internet/cloud.
- FQDN is the complete domain name for a specific computer, or host, on the Internet, consisting of two parts: the hostname and the domain name.

Task Number 035

Describe network configuration tools.

Definition

Description should include brief explanations of the following:

- Active directory—the active directory database, designed to handle a large number of read and search operations and a significantly smaller number of changes and updates, consists of objects and attributes and is hierarchical, replicated, and extensible.
- Dynamic Host Configuration Protocol (DHCP)—a standardized protocol that enables clients to be dynamically assigned with various configuration parameters, such as an IP address, subnet mask, default gateway, and other critical network configuration information. DHCP servers centrally manage such configuration data and are configured by network administrators with settings that are appropriate for a given network environment. DHCP servers, in turn, communicate with DHCP clients through the use of DHCP messages.
- Application Programming Interface (API)—also referred to as DHCP client options, enables Microsoft Windows clients to query specific options from DHCP servers.

Implementing Threat Mitigation

Task Number 036

Set up a schedule for anti-virus scans.

Definition

Setting up a schedule should include the dates and times to scan

- local hard disks
- floppy disks or removable drives
- CD drives.

Task Number 037

Run an anti-virus scan.

Definition

Running a scan should include addressing the scan itself and the cleanup. The scan should include

- scanning inside archive files
- scanning for Macintosh viruses
- scanning system memory
- running scan at lower priority
- scanning for root kits
- scanning for adware and potentially unwanted applications (PUAs)
- scanning for suspicious files on individual computers at the host-based intrusion prevention system (HIPS) level

If cleanup is not automatically handled after the scan, a manual cleanup should include

- disabling adware/PUA files
- denying access to suspicious files.

Task Number 038

Respond to results from an anti-virus scan.

Definition

Response should include

- interpreting results; determining whether threats are real or misidentified
- containing and/or deleting identified/verified threats
- repeating steps 1 and 2 until no threats are found.

Task Number 039

Research the nature (i.e., motivations) and scope (i.e., prevalence) of current and past threats.

Definition

Research should include accessing the top Web sites that publish this type of information, such as

- virustotal.com (see "statistics")
- datalossDB.org (provides data on daily breaches).

Task Number 040

Report system anomalies.

Definition

Reporting should include

- identifying system anomalies
- adhering to the elements of the report and additional formatting issues
- providing further summary and analysis, as requested
- submitting the report to the appropriate personnel in a timely fashion.

Unit 3: CYBER FORENSICS

Exploring Ethical and Legal Issues

Task Number 041

Identify laws applicable to cyber.

Definition

Identification should include relevant descriptions of the following:

- Fourth Amendment—"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." This amendment is part of the Bill of Rights and protects an individual's right to privacy.
- Health Insurance Portability and Accountability Act (HIPAA)—protects the privacy of an individual's health records
- Family Educational Rights and Privacy Act (FERPA)—protects the privacy of an individual's educational records and transcripts
- Sarbanes-Oxley Act (SOX)—protects investors from financial fraud by establishing new financial reporting standards for businesses and accounting firms
- Gramm-Leach-Bliley Act (GLBA)—also known as the Financial Services Modernization Act; removed previous legal barriers to allow banks, insurers, and securities companies to merge; institutes new standards on how consumer information is shared and what is disclosed to the consumer
- Computer Fraud and Abuse Act (CFAA)—clarifies the definitions of specific cyber crimes and protects users against certain types of fraud
- Electronic Communications Privacy Act (ECPA)—protects privacy by extending telephone wire taps and transmitted computer data surveillance
- Freedom of Information Act (FOIA)—establishes disclosure standards for government controlled information
- USA PATRIOT Act—terrorism obstruction law that allows law enforcement agencies to gather greater intelligence on individuals within the United States, thereby redefining the standard right to privacy
- Code of Virginia—state interpretations and additions to existing federal cyber security acts and privacy protections (e.g., cyber bullying, online gambling, computer-based obscenity, privacy, fraud)

Task Number 042

Describe the rule of law and its impact on cyber forensics.

Definition

Description should include

- the definition of *rule of law*—procedures that form a legal framework within a legal system
- definition of *jurisdiction*—the authority to administer justice
- Council of Europe and the Convention on Cybercrime—helps protect societies worldwide from the threat of cybercrime through its protocol on xenophobia and racism, the Cybercrime Convention Committee (T-CY), and the technical cooperation program on cybercrime.

Task Number 043

Identify rules of evidence relevant to cyber forensics.

Definition

Identification should include an explanation of the following:

- Daubert standards—establishes a legal standard as to the rule of evidence for the submission of expert witness testimony in federal cases
- Federal Rules for Civil Procedure (FRCP)—standards of civil procedure in federal courts

Applying Legal Procedures

Task Number 044

Describe ISO/IEC-27037 and its relevance to cyber forensics.

Definition

Description should include that ISO/IEC-27037 was created

- as a subset of ISO-27000 series of standards to act as the best practices standard for acquisition and preservation of digital evidence
- as the product of ISO/IEC JTC1 (Joint Technical Committee 1) SC27 (Sub Committee 27), an international body that meets in person twice a year

- by the International Organization for Standardization (IOS).

Task Number 045

Describe the importance of using a write blocker or best effort to preserve evidence.

Definition

Description should include

- hardware write blocking
- software write blocking
- spoliation (the intentional concealment, alteration, or destruction of evidence) or alteration.

Task Number 046

Create a forensic image and establish hash code, using a write blocker.

Definition

Creation should include the following steps:

- Create an imaging plan.
- Connect the device to be imaged to a write blocker.
- Connect or make available a drive to be the destination of the forensic image.
- Create the forensic image on the destination media.
- Identify the hash code of the imaged device.

Task Number 047

Establish and maintain the chain of custody.

Definition

Establishment and maintenance should include

- identifying the rationale, components, and governance of a chain of custody

- describing the operating procedures that ensure the chain of custody.

Identifying Media

Task Number 048

Identify types of media hardware.

Definition

Identification should include brief descriptions of the following:

- Hard disk drives
- Removable drives
- Flash memory

Task Number 049

Identify types of hardware interfaces.

Definition

Identification should include brief descriptions of the following:

- IDE—integrated drive electronics (standard for connecting devices, hard drives, and motherboards)
    - parallel advanced technology attachment (PATA)
    - serial advanced technology attachment (SATA)
- USB—universal serial bus (an external bus standard)
- Firewire—meets the IEEE 1394 standard (a very fast external bus standard)

Exploring Media Forensics

Task Number 050

Identify common file systems.

Definition

Identification should include brief descriptions of the following file systems and the operating systems with which they are associated:

- FAT—file allocation table; OS: Windows
- NTFS—new technology file system; OS: Apple for Windows NT
- ext3—third extended file system; OS: Linux
- HFS—hierarchical file system; OS: Apple
- Types of operating systems where common file systems are used

---

Task Number 051

Identify types of artifacts.

Definition

Identification should include brief descriptions of the following:

- Registry
- Log files
- MAC timestamps
- File types
- File slack space
- RAM slack space
- Unallocated space

Task Number 052

Identify geometry parameters of physical media.

Definition

Identification should include brief descriptions of the following:

- Cylinders—a three-dimensional structure to which data can be written and stored
- Heads—reads and writes data in a hard drive
- Sectors—smallest storage unit that is addressable by a hard drive

- Disk size using sectors, cylinders, and heads

Task Number 053

Recover artifacts from physical media.

Definition

Recovered artifacts should include examples of the following:

- Registry entries describing the system hardware and software
- System and Internet history log files
- MAC time stamps
- Data from different file types from allocated space, file slack space, RAM slack space, and unallocated space

---

Conducting Mobile Devices Forensics

Task Number 054

Change EXIF (exchangeable image file format).

Definition

Procedures should include

- changing the date and time
- changing the location label identifying where a picture was taken.

Task Number 055

Extract text messages.

Definition

Procedures should include documentation of all text messages from the systems management server (SMS), including

- those on a cellphone, using a camera
- deleted messages on a cellphone by forensically acquiring the logical data from the cellphone
- deleted messages, on a cellphone by examining the logical data forensic image acquired from the cellphone.

Task Number 056

Extract call logs.

Definition

Extraction should include

- forensic acquisition of the logical data from the cellphone
- documentation of all call logs on a cellphone by examining the logical data forensic image acquired from the cellphone
- documentation of all call logs on a cellphone by examining and photographing the cellphone.

Task Number 057

Extract unique identifiers from components.

Definition

Extraction should include

- documentation of unique identifiers by examining the logical data forensic image acquired from a cellphone
- documentation of unique identifiers by visually examining a cellphone. Unique identifiers include the following:
    - IMEI (International Mobile Equipment Identity)
    - Serial numbers
    - FCC-ID (Federal Communications Commission Identification)

SOL Correlation by Task

001	Define *cyber system* and industry-specific terminology.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5
002	Provide background on fundamental information technology security concepts.	
003	Create a framework to protect information systems.	
004	Describe information technology ethics and an acceptable use policy (AUP).	History and Social Science: GOVT.1, GOVT.11
005	Act upon AUP infractions.	History and Social Science: GOVT.1, GOVT.11
006	Define components of and terminology related to virtual machines.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5
007	Identify advantages and disadvantages of using virtual machines.	
008	Determine software downloading and installation procedures for virtual machines.	
009	Perform common tasks, using a virtual machine.	
010	Research career opportunities for cyber security/forensics professionals.	English: 9.8, 10.8, 11.8, 12.8 History and Social Science: GOVT.1, GOVT.15
011	Identify the educational pathways for emerging cyber security and cyber forensics professionals.	History and Social Science: GOVT.1
012	Identify career paths and job titles within the cyber security/forensics industry and related Career Clusters.	History and Social Science: GOVT.1
013	Verify that Web sites are secure before submitting personal or corporate information.	
014	Describe vulnerabilities associated with using automated teller machines (ATM).	
015	Describe keylogging vulnerabilities.	
016	Establish a password protocol and policy.	
017	Install an operating system and components.	
018	Install service packs and updates.	
019	Update installed applications.	
020	Install and update anti-virus/anti-spyware utilities.	
021	Configure critical operating system parameters.	History and Social Science: GOVT.1
022	Enable security and auditing logs.	History and Social Science: GOVT.1
023	Back up a system.	History and Social Science: GOVT.1
024	Restore a system from a backup.	History and Social Science: GOVT.1
025	Secure a router connection.	History and Social Science: GOVT.1
026	Secure other personal/mobile devices.	History and Social Science: GOVT.1
027	Secure a game console.	History and Social Science: GOVT.1
028	Describe network topologies.	
029	Identify network vulnerabilities.	
030	Describe methods for strengthening network security.	
031	Identify components of physical security.	
032	Identify common network devices.	
033	Identify protocols.	
034	Describe the fundamentals of domain names.	

035	Describe network configuration tools.	
036	Set up a schedule for anti-virus scans.	
037	Run an anti-virus scan.	
038	Respond to results from an anti-virus scan.	
039	Research the nature (i.e., motivations) and scope (i.e., prevalence) of current and past threats.	English: 9.8, 10.8, 11.8, 12.8
040	Report system anomalies.	
041	Identify laws applicable to cyber.	History and Social Science: GOVT.1, GOVT.9, GOVT.11, GOVT.15
042	Describe the rule of law and its impact on cyber forensics.	History and Social Science: GOVT.1, GOVT.11, GOVT.13, GOVT.15
043	Identify rules of evidence relevant to cyber forensics.	History and Social Science: GOVT.1, GOVT.9, GOVT.15
044	Describe ISO/IEC-27037 and its relevance to cyber forensics.	
045	Describe the importance of using a write blocker or best effort to preserve evidence.	
046	Create a forensic image and establish hash code, using a write blocker.	History and Social Science: GOVT.1
047	Establish and maintain the chain of custody.	History and Social Science: GOVT.1
048	Identify types of media hardware.	
049	Identify types of hardware interfaces.	
050	Identify common file systems.	
051	Identify types of artifacts.	
052	Identify geometry parameters of physical media.	Mathematics: G.11, COM.16
053	Recover artifacts from physical media.	
054	Change EXIF (exchangeable image file format).	
055	Extract text messages.	
056	Extract call logs.	
057	Extract unique identifiers from components.	

Cyber Security/Forensics Resources

For additional resources teachers should use the links below and go to the Cyber Explorations website. Once there, teachers and students can log in to the high school club program.

The Cyber Explorations Pilot Program is "a collaboration between Longwood University, the Longwood Center for Cyber Security, Hanover County Public Schools, Superior Document Services, community mentors, and experts from around the Globe."

Unit 1, Cyber Security Foundations

Virginia Laws Related to Computer/Internet-related Offense
https://virginiarules.org/resources-and-publications/juvenile-law-handbook/

Virginia Guidelines and Resources for Internet Safety in Schools
www.doe.virginia.gov/support/safety_crisis_management/internet_safety/index.shtml
https://www.doe.virginia.gov/support/safety_crisis_management/internet_safety/guidelines_resources.pdf

Critiquing Acceptable Use Policies
http://www.prismnet.com/~kinnaman/aupessay.html

Unit 2, Social Engineering and Personal Cyber Security

Step-by-Step Procedure for Backup System Restore
http://windows.microsoft.com/en-us/windows7/products/features/system-restore

How DNS Works
http://technet.microsoft.com/en-us/magazine/2005.01.howitworksdns.aspx

Active Directory
http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492%28v=vs.85%29.aspx

DHCP
http://msdn.microsoft.com/en-us/library/windows/desktop/aa363383%28v=vs.85%29.aspx

Verify that websites are secure
http://info.ssl.com/article.aspx?id=10068

Describe vulnerabilities associated with using automated teller machines (ATMs).
http://www.bankinfosecurity.com/interviews/atm-security-3-key-vulnerabilities-i-1027
http://www.bankinfosecurity.com/search.php?keywords=ATM+Security

Describe keylogging vulnerabilities.
http://www.securelist.com/en/analysis?pubid=204791931

Install service packs and updates.
http://windows.microsoft.com/en-us/windows/service-packs-download#sptabs=win7

Update installed applications.
http://lifehacker.com/5495501/the-definitive-guide-to-keeping-your-pc-up-to-date

Secure a router connection.
http://www.pcmag.com/article2/0,2817,2409751,00.asp

Secure a game console.
http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips#sthash.3zLlXSRF.dpuf

Run an anti-virus scan.
http://www.sophos.com/en-us/support/knowledgebase/63985.aspx

Unit 3, Cyber Forensics

Spoliation and/or alteration
http://civilprocedure.uslegal.com/discovery/spoliation-of-evidence/

Create an imaging plan
http://en.wikipedia.org/wiki/Digital_forensic_process#Acquisition

Types of operating systems where common file systems are used
http://en.wikipedia.org/wiki/Comparison_of_file_systems
http://en.wikipedia.org/wiki/File_system

Artifacts/Registry
http://support.microsoft.com/kb/256986
http://en.wikipedia.org/wiki/Windows_Registry

Rule of Law
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG
http://en.wikipedia.org/wiki/Convention_on_Cybercrime