Digital Forensics

Subject: Career and Technical Education
Grade: 09
Expectations: 74
Breakouts: 138

(a) Introduction.

1. Career and technical education instruction provides content aligned with challenging academic standards, industry relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and emerging professions.
2. The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services, such as laboratory and testing services and research and development services.
3. Digital forensics is a critical discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the expansion of a globally connected digital society. As computing has become more sophisticated, so too have the abilities to access systems and sensitive information. Digital forensics professionals investigate and craft appropriate responses to disruptions to governments, organizations, and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.
4. Digital Forensics introduces students to the knowledge and skills of digital forensics. The course provides a survey of the field of digital forensics and incident response.
5. Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.
6. Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.

(b) Knowledge and Skills Statements

(1) Employability skills. The student identifies necessary skills for career development and employment opportunities. The student is expected to:

(A) investigate the need for digital forensics

(i) investigate the need for digital forensics

(B) research careers in digital forensics along with the education and job skills required for obtaining a job in both the public and private sector;

(i) research careers in digital forensics

(ii) research the education required for obtaining a job [in digital forensics] in both the public and private sector

(iii) research the job skills required for obtaining a job [in digital forensics] in both the public and private sector

(C) identify job and internship opportunities and accompanying job duties and tasks and contact one or more companies or organizations to explore career opportunities;

(i) identify job opportunities

(ii) identify internship opportunities

(iii) identify accompanying job duties

(iv) identify accompanying tasks

(v) contact one or more companies or organizations to explore career opportunities

(D) identify and discuss certifications for digital forensics careers;

(i) identify certifications for digital forensics careers

(ii) discuss certifications for digital forensics careers

(E) explain ethical and legal responsibilities in relation to the field of digital forensics;

(i) explain ethical responsibilities in relation to the field of digital forensics

(ii) explain legal responsibilities in relation to the field of digital forensics

(F) identify and describe businesses and government agencies that use digital forensics;

(i) identify businesses that use digital forensics

(ii) identify government agencies that use digital forensics

(iii) describe businesses that use digital forensics

(iv) describe government agencies that use digital forensics

(G) identify and describe the kinds of crimes investigated by digital forensics specialists; and

(i) identify the kinds of crimes investigated by digital forensics specialists

(ii) describe the kinds of crimes investigated by digital forensics specialists

(H) solve problems and think critically.

(i) solve problems

(ii) think critically

(2) Employability skills. The student communicates and collaborates effectively. The student is expected to:

(A) apply effective teamwork strategies;

(i) apply effective teamwork strategies

(B) collaborate with a community of peers and professionals;

(i) collaborate with a community of peers

(ii) collaborate with a community of professionals

(C) create, review, and edit a report summarizing technical findings; and

(i) create a report summarizing technical findings

(ii) review a report summarizing technical findings

(iii) edit a report summarizing technical findings

(D) present technical information to a non-technical audience.

(i) present technical information to a non-technical audience

(3) Ethics and laws. The student recognizes and analyzes ethical and current legal standards, rights, and restrictions related to digital forensics. The student is expected to:

(A) develop a plan to advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;

(i) develop a plan to advocate for ethical behaviors both online and offline among peers, family, community, and employers

(ii) develop a plan to advocate for legal behaviors both online and offline among peers, family, community, and employers

(B) research and discuss local, state, national, and international law such as the Electronic Communications Privacy Act of 1986, Title III (Pen Register Act); USA PATRIOT Act of 2001; and Digital Millennium Copyright Act;

(i) research local law

(ii) research state law

(iii) research national law

(iv) research international law

(v) discuss local law

(vi) discuss state law

(vii) discuss national law

(viii) discuss international law

(C) research and discuss historic cases or events regarding digital forensics or cybersecurity;

(i) research historic cases or events regarding digital forensics or cybersecurity

(ii) discuss historic cases or events regarding digital forensics or cybersecurity

(D) analyze ethical and legal behavior when presented with confidential or sensitive information in various scenarios related to cybersecurity activities;

(i) analyze ethical behavior when presented with confidential or sensitive information in various scenarios related to cybersecurity activities

(ii) analyze legal behavior when presented with confidential or sensitive information in various scenarios related to cybersecurity activities

(E) analyze case studies of computer incidents;

(i) analyze case studies of computer incidents

(F) use the findings of a computer incident investigation to reconstruct a computer incident;

(i) use the findings of a computer incident investigation to reconstruct a computer incident

(G) identify and discuss intellectual property laws, issues, and use;

(i) identify intellectual property laws

(ii) identify intellectual property issues

(iii) identify intellectual property use

(iv) discuss intellectual property laws

(v) discuss intellectual property issues

(vi) discuss intellectual property use

(H) contrast legal and illegal aspects of information gathering;

(i) contrast legal and illegal aspects of information gathering

(I) contrast ethical and unethical aspects of information gathering;

(i) contrast ethical and unethical aspects of information gathering

(J) analyze emerging legal and societal trends affecting digital forensics; and

(i) analyze emerging legal trends affecting digital forensics

(ii) analyze emerging societal trends affecting digital forensics

(K) discuss how technological changes affect applicable laws.

(i) discuss how technological changes affect applicable laws

(4) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding digital technology, safety, digital hygiene, and cyberbullying. The student is expected to:

(A) identify and use digital information responsibly;

(i) identify digital information responsibly

(ii) use digital information responsibly

(B) use digital tools responsibly;

(i) use digital tools responsibly

(C) identify and use valid and reliable sources of information; and

(i) identify valid sources of information

(ii) identify reliable sources of information

(iii) use valid sources of information

(iv) use reliable sources of information

(D) gain informed consent prior to investigating incidents.

(i) gain informed consent prior to investigating incidents

(5) Digital forensics skills. The student locates, processes, analyzes, and organizes data. The student is expected to:

(A) identify sources of data;

(i) identify sources of data

(B) analyze and report data collected;

(i) analyze data collected

(ii) report data collected

(C) discuss how to maintain data integrity such as by enabling encryption;

(i) discuss how to maintain data integrity

(D) examine and describe metadata of a file; and

(i) examine metadata of a file

(ii) describe metadata of a file

(E) examine and describe how multiple data sources can be used for digital forensics, including investigating malicious software (malware) and email threats.

(i) examine how multiple data sources can be used for digital forensics, including investigating malicious software (malware)

(ii) examine how multiple data sources can be used for digital forensics, including investigating email threats

(iii) describe how multiple data sources can be used for digital forensics, including investigating malicious software (malware)

(iv) describe how multiple data sources can be used for digital forensics, including investigating email threats

(6) Digital forensics skills. The student understands software concepts and operations as they apply to digital forensics. The student is expected to:

(A) compare software applications as they apply to digital forensics;

(i) compare software applications as they apply to digital forensics

(B) describe the purpose of various application types such as email, web, file sharing, security applications, and data concealment tools;

(i) describe the purpose of various application types

(C) identify the different purposes of data formats such as pdf, wav, jpeg, and exe;

(i) identify the different purposes of data formats

(D) describe how application logs and metadata are used for investigations such as Security Information and Event Management (SIEM) reports;

(i) describe how application logs are used for investigations

(ii) describe how metadata are used for investigations

(E) describe digital forensics tools;

(i) describe digital forensics tools

(F) select the proper software tool based on appropriateness, effectiveness, and efficiency for a given digital forensics scenario;

(i) select the proper software tool based on appropriateness for a given digital forensics scenario

(ii) select the proper software tool based on effectiveness for a given digital forensics scenario

(iii) select the proper software tool based on efficiency for a given digital forensics scenario

(G) describe components of applications such as configurations settings, data, supporting files, and user interface; and

(i) describe components of applications

(H) describe how the "as a service" model applies to incident response.

(i) describe how the "as a service" model applies to incident response

(7) Digital forensics skills. The student understands operating systems concepts and functions as they apply to digital forensics. The student is expected to:

(A) compare various operating systems;

(i) compare various operating systems

(B) describe file attributes, including access and creation times;

(i) describe file attributes, including access

(ii) describe file attributes, including creation times

(C) describe how operating system logs are used for investigations;

(i) describe how operating system logs are used for investigations

(D) compare and contrast the file systems of various operating systems;

(i) compare and contrast the file systems of various operating systems

(E) compare various primary and secondary storage devices; and

(i) compare various primary and secondary storage devices

(F) differentiate between volatile and non-volatile memory.

(i) differentiate between volatile and non-volatile memory

(8) Digital forensics skills. The student understands networking concepts and operations as they apply to digital forensics. The student is expected to:

(A) examine networks, including Internet Protocol (IP) addressing and subnets;

(i) examine networks, including Internet Protocol (IP) addressing

(ii) examine networks, including subnets

(B) describe the Open Systems Interconnection (OSI) model;

(i) describe the Open Systems Interconnection (OSI) model

(C) describe the Transmission Control Protocol/Internet Protocol (TCP/IP) model;

(i) describe the Transmission Control Protocol/Internet Protocol (TCP/IP) model

(D) use network forensic analysis tools to examine network traffic data from sources such as firewalls, routers, intrusion detection systems (IDS), and remote access logs; and

(i) use network forensic analysis tools to examine network traffic data from sources

(E) identify malicious or suspicious network activities such as mandatory access control (MAC) spoofing and rogue wireless access points.

(i) identify malicious or suspicious network activities

(9) Digital forensics skills. The student explains the principles of access controls. The student is expected to:

(A) define the principle of least privilege;

(i) define the principle of least privilege

(B) describe the impact of granting access and permissions;

(i) describe the impact of granting access

(ii) describe the impact of permissions

(C) identify different access components such as passwords, tokens, key cards, and biometric verification systems;

(i) identify different access components

(D) explain the value of an access log to identify suspicious activity;

(i) explain the value of an access log to identify suspicious activity

(E) describe the risks of granting third parties access to personal and proprietary data on social media and systems;

(i) describe the risks of granting third parties access to personal data on social media

(ii) describe the risks of granting third parties access to personal data on systems

(iii) describe the risks of granting third parties access to proprietary data on social media

(iv) describe the risks of granting third parties access to proprietary data on systems

(F) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements; and

(i) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements

(G) identify various access control methods such as mandatory access control (MAC), attribute-based access control (ABAC), role-based access control (RBAC), and discretionary access control (DAC).

(i) identify various access control methods

(10) Incident response. The student follows a methodological approach to prepare for and respond to an incident. The student is expected to:

(A) define the components of the incident response cycle, including preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity;

(i) define the components of the incident response cycle, including preparation

(ii) define the components of the incident response cycle, including detection and analysis

(iii) define the components of the incident response cycle, including containment, eradication, and recovery

(iv) define the components of the incident response cycle, including post-incident activity

(B) describe incident response preparation;

(i) describe incident response preparation

(C) discuss incident response detection and analysis;

(i) discuss incident response detection

(ii) discuss incident response analysis

(D) discuss containment and eradication of and recovery from an incident;

(i) discuss containment of an incident

(ii) discuss eradication of an incident

(iii) discuss recovery from an incident

(E) describe post-incident activities such as reflecting on lessons learned, using collected incident data, and retaining evidence of an incident;

(i) describe post-incident activities

(F) develop an incident response plan; and

(i) develop an incident response plan

(G) describe ways a user may compromise the validity of existing evidence.

(i) describe ways a user may compromise the validity of existing evidence

(11) Incident response. The student objectively analyzes collected data from an incident. The student is expected to:

(A) identify the role of chain of custody in digital forensics;

(i) identify the role of chain of custody in digital forensics

(B) describe safe data handling procedures;

(i) describe safe data handling procedures

(C) explain the fundamental concepts of confidentiality, integrity, availability, authentication, and authorization;

(i) explain the fundamental [concept] of confidentiality

(ii) explain the fundamental [concept] of integrity

(iii) explain the fundamental [concept] of availability

(iv) explain the fundamental [concept] of authentication

(v) explain the fundamental [concept] of authorization

(D) identify and report information conflicts or suspicious activity;

(i) identify information conflicts or suspicious activity

(ii) report information conflicts or suspicious activity

(E) identify events of interest and suspicious activity by examining network traffic; and

(i) identify events of interest by examining network traffic

(ii) identify suspicious activity by examining network traffic

(F) identify events of interest and suspicious activity by examining event logs.

(i) identify events of interest by examining event logs

(ii) identify suspicious activity by examining event logs

(12) Incident response. The student analyzes the various ways systems can be compromised. The student is expected to:

(A) analyze the different signatures of cyberattacks;

(i) analyze the different signatures of cyberattacks

(B) identify points of weakness and attack vectors such as online spoofing, phishing, and social engineering; and

(i) identify points of weakness

(ii) identify attack vectors

(C) differentiate between simple versus multistage attacks.

(i) differentiate between simple versus multistage attacks