Digital Forensics

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

(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

(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)
o(i)

(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

(D)

(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)

(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