ATTACHMENT
Text of Proposed Repeal and New 19 TAC

Chapter 126. Texas Essential Knowledge and Skills for Technology Applications

Subchapter C. High School

§126.36. Digital Forensics (One Credit), Beginning with School Year 2019-2020.

(a) General requirements. Students shall be awarded one credit for successful completion of this course. The prerequisite for this course is proficiency in the knowledge and skills relating to Technology Applications, Grades 6-8. This course is recommended for students in Grades 9-12.

(b) Introduction.

(1) Digital forensics is an evolving discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the emergence of a globally-connected digital society. As computing has become more sophisticated, so too have the abilities of malicious agents to access systems and private information. By evaluating prior incidents, digital forensics professionals have the ability to investigate and craft appropriate responses to disruptions to corporations, governments, and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.

(2) 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.

(3) 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.

(c) Knowledge and skills.

(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;

(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;

(C) identify job and internship opportunities as well as accompanying duties and tasks;

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

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

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

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

(H) solve problems and think critically.

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

(A) apply effective teamwork strategies;

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

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

(D) 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;

(B) research 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;

(C) research historic cases or events regarding digital forensics or cyber;

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

(E) analyze case studies of computer incidents;

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

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

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

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

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

(K) 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;

(B) use digital tools responsibly;

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

(D) 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;

(B) analyze and report data collected;

(C) maintain data integrity;

(D) examine metadata of a file; and

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

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

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

(D) describe how application logs and metadata are used for investigations;

(E) describe digital forensics tools;

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

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

(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;

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

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

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

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

(F) 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;

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

(C) 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

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

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

(A) define the principle of least privilege;

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

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

(D) 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;

(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

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

(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;

(B) describe incident response preparation;

(C) discuss incident response detection and analysis;

(D) discuss containment and eradication of and 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;

(F) develop an incident response plan; and

(G) 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;

(B) describe safe data handling procedures;

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

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

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

(F) identify events of interest and 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; and

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

[~~§126.36. Digital Forensics (One-Half to One Credit), Beginning with School Year 2012-2013.~~]

[~~(a) General requirements. Students shall be awarded one-half to one credit for successful completion of this course. The prerequisite for this course is proficiency in the knowledge and skills relating to Technology Applications, Grades 6-8. This course is recommended for students in Grades 9-12.~~]

[(~~b) Introduction.~~]

[~~(1) The technology applications curriculum has six strands based on the National Educational Technology Standards for Students (NETS•S) and performance indicators developed by the International Society for Technology in Education (ISTE): creativity and innovation; communication and collaboration; research and information fluency; critical thinking, problem-solving, and decision making; digital citizenship; and technology operations and concepts.~~]

[~~(2) Digital Forensics will foster students' creativity and innovation by presenting opportunities to investigate simulations and case studies of crimes, reconstructing computer security incidents, troubleshooting operational problems, and recovering from accidental system damage. Students will collaborate to develop forensic techniques to assist with computer security incident response. Students will learn methods to identify, collect, examine, and analyze data while preserving the integrity of the information and maintaining a strict chain of custody for data. Students will solve problems as they study the application of science to the law. Students will learn digital citizenship by researching current laws and regulations and by practicing integrity and respect. Students will gain an understanding of computing and networking systems that transmit or store electronic data.~~]

[~~(3) 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.~~]

[~~(c) Knowledge and skills.~~]

[~~(1) Creativity and innovation. The student develops products and generates new understanding by extending existing knowledge. The student is expected to:~~]

[~~(A) explain the need for digital forensics, staffing requirements, and team interactions;~~]

[~~(B) develop policies to define staff roles and responsibilities;~~]

[~~(C) develop guidelines, procedures, and recommendations for digital forensics tool use; and~~]

[~~(D) investigate simulations and case studies of crimes to reconstruct computer security incidents.~~]

[~~(2) Communication and collaboration. The student communicates and collaborates with peers to contribute to his or her own learning and the learning of others. The student is expected to:~~]

[~~(A) describe the characteristics and behaviors of a given system;~~]

[~~(B) justify and describe the impact of selecting a given system;~~]

[~~(C) apply effective teamwork practices;~~]

[~~(D) collaborate with multiple participants;~~]

[~~(E) document use, functionality, and implementation;~~]

[~~(F) seek and respond to advice from peers and professionals; and~~]

[~~(G) describe considerations required for incident response.~~]

[~~(3) Research and information fluency. The student locates, analyzes, processes, and organizes data. The student is expected to:~~]

[~~(A) identify possible sources of data;~~]

[~~(B) acquire data;~~]

[~~(C) analyze and report data collected;~~]

[~~(D) collect files by copying files from media while maintaining data file integrity;~~]

[~~(E) examine data files by locating files, extracting data, and using a digital forensics toolkit;~~]

[~~(F) examine and analyze operating system data;~~]

[~~(G) collect volatile and non-volatile operating system data;~~]

[~~(H) collect, examine, and analyze application data;~~]

[~~(I) use traffic data sources, including firewalls and routers, packet sniffers and protocol analyzers, intrusion detection systems, remote access, security event management software, and network forensic analysis tools;~~]

[~~(J) describe how a file scan can be accessed and modified;~~]

[~~(K) collect, examine, and analyze data from multiple sources; and~~]

[~~(L) provide examples of how multiple data sources can be used during digital forensics, including investigating worm infections, viruses, and email threats.~~]

[~~(4) Critical thinking, problem solving, and decision making. The student uses appropriate strategies to analyze problems and design algorithms. The student is expected to:~~]

[~~(A) resolve information conflicts and validate information through data acquisition, research, and comparison; and~~]

[~~(B) examine and analyze network traffic data, including identifying events of interest, examining data sources, and identifying attacks.~~]

[~~(5) Digital citizenship. The student explores and understands safety, legal, cultural, and societal issues relating to the use of technology and information. The student is expected to:~~]

[~~(A) identify and use digital information appropriately;~~]

[~~(B) identify and use appropriate methods for citing sources;~~]

[~~(C) identify and discuss intellectual property laws, issues, and use;~~]

[~~(D) identify intellectual property stakeholders and their needs and perspectives;~~]

[~~(E) identify and describe the kinds of crimes investigated by digital forensics specialists;~~]

[~~(F) identify legal, illegal, ethical, and unethical aspects of information gathering;~~]

[~~(G) compare and contrast legal, illegal, ethical, and unethical information gathering methods and identify possible gray areas;~~]

[~~(H) identify and describe ways in which developing laws and guidelines affect digital forensics practices;~~]

[~~(I) identify and describe legal considerations and technical issues related to collecting network traffic data;~~]

[~~(J) identify and describe ways in which technological changes affect applicable laws; and~~]

[~~(K) identify and describe businesses and government agencies that use digital forensics.~~]

[~~(6) Technology operations and concepts. The student understands technology concepts, systems, and operations as they apply to computer science. The student is expected to:~~]

[~~(A) demonstrate knowledge of and appropriately use operating systems, software applications, and communication and networking components;~~]

[~~(B) compare, contrast, and appropriately use various input, processing, output, and primary and secondary storage devices;~~]

[~~(C) make decisions regarding the selection, acquisition, and use of software, including its quality, appropriateness, effectiveness, and efficiency;~~]

[~~(D) demonstrate knowledge of data formats;~~]

[~~(E) demonstrate knowledge of networks, including the Internet, intranets, and extranets;~~]

[~~(F) compare and contrast non-volatile and volatile data;~~]

[~~(G) describe file basics, including file storage, file systems, and other types of storage media;~~]

[~~(H) describe file modification, including access and creation times;~~]

[~~(I) describe operating systems, including terminology and functions;~~]

[~~(J) describe technical procedures related to collecting operating system data;~~]

[~~(K) describe the significance to digital forensics of the Transmission Control Protocol/Internet Protocol (TCP/IP) model, including application, transport, IP, and hardware layers;~~]

[~~(L) describe the function and use of application components, including configurations settings, authentications, logs, application data, supporting files, and application architecture; and~~]

[~~(M) describe the functions and use of application types, including email, web usage, interactive communications, file sharing, document usage, security applications, and data concealment tools.~~]