COMPUTER FORENSICS
ACTIVITY/COURSE CODE: 5374

COURSE DESCRIPTION: In the Computer Forensics course, students gain a fundamental knowledge of computer forensics and investigation of computer-related crimes. They will learn to collect, preserve, present, and prepare computer-based evidence for the purposes of criminal law enforcement or civil litigation. Students will have the opportunity to present digital evidence to both business and legal audiences. Students will learn to use tools to locate and analyze digital evidence on a variety of devices, how to keep up to date with changing technologies, and laws and regulations in digital forensics.

OBJECTIVE: Given the necessary equipment, supplies, and appropriate software, the student will be prepared to successfully complete the standards.

COURSE CREDIT: 1 (120 hours) or 2 (240 hours) units

RECOMMENDED PREREQUISITE: IT Fundamentals **or**
Computer Repair and Service 1

RECOMMENDED GRADE LEVELS: 10–12

COMPUTER ACCESS REQUIRED: 1 Computer per student with Internet access

RECOMMENDED MAXIMUM ENROLLMENT: 25

RESOURCES: Instructional Materials

A. SAFETY

Effective professionals know the academic subject matter, including safety as required for proficiency within their area. They will use this knowledge as needed in their role. The following accountability criteria are considered essential for students in any program of study.

1. Review school safety policies and procedures.
2. Review classroom safety rules and procedures.
3. Review safety procedures for using equipment in the classroom.
4. Identify major causes of work-related accidents in office environments.
5. Demonstrate safety skills in an office/work environment.

B. STUDENT ORGANIZATIONS

Effective professionals know the academic subject matter, including professional development, required for proficiency within their area. They will use this knowledge as needed in their role. The following accountability criteria are considered essential for

students in any program of study.

1. Identify the purpose and goals of a Career and Technology Student Organization (CTSO).
2. Explain how CTSOs are integral parts of specific clusters, majors, and/or courses.
3. Explain the benefits and responsibilities of being a member of a CTSO.
4. List leadership opportunities that are available to students through participation in CTSO conferences, competitions, community service, philanthropy, and other activities.
5. Explain how participation in CTSOs can promote lifelong benefits in other professional and civic organizations.

C. TECHNOLOGY KNOWLEDGE

Effective professionals know the academic subject matter, including the ethical use of technology as needed in their role. The following accountability criteria are considered essential for students in any program of study.

1. Demonstrate proficiency and skills associated with the use of technologies that are common to a specific occupation.
2. Identify proper netiquette when using e-mail, social media, and other technologies for communication purposes.
3. Identify potential abuse and unethical uses of laptops, tablets, computers, and/or networks.
4. Explain the consequences of social, illegal, and unethical uses of technology (e.g., piracy; illegal downloading; cyberbullying; licensing infringement; inappropriate uses of software, hardware, and mobile devices in the work environment).
5. Discuss legal issues and the terms of use related to copyright laws, fair use laws, and ethics pertaining to downloading of images, photographs, documents, Creative Commons, video, sounds, music, trademarks, and other elements for personal use.
6. Describe ethical and legal practices of safeguarding the confidentiality of business-related information.
7. Describe possible threats to a laptop, tablet, computer, and/or network and methods of avoiding attacks.

D. PERSONAL QUALITIES AND EMPLOYABILITY SKILLS

Effective professionals know the academic subject matter, including positive work practices and interpersonal skills, as needed in their role. The following accountability criteria are considered essential for students in any program of study.

1. Demonstrate punctuality.
2. Demonstrate self-representation.
3. Demonstrate work ethic.
4. Demonstrate respect.
5. Demonstrate time management.
6. Demonstrate integrity.

7. Demonstrate leadership.
8. Demonstrate teamwork and collaboration.
9. Demonstrate conflict resolution.
10. Demonstrate perseverance.
11. Demonstrate commitment.
12. Demonstrate a healthy view of competition.
13. Demonstrate a global perspective.
14. Demonstrate health and fitness.
15. Demonstrate self-direction.
16. Demonstrate lifelong learning.

E. PROFESSIONAL KNOWLEDGE

Effective professionals know the academic subject matter, including positive work practices and interpersonal skills, as needed in their role. The following accountability criteria are considered essential for students in any program of study.

1. Demonstrate effective speaking and listening skills.
2. Demonstrate effective reading and writing skills.
3. Demonstrate mathematical reasoning.
4. Demonstrate job-specific mathematics skills.
5. Demonstrate critical-thinking and problem-solving skills.
6. Demonstrate creativity and resourcefulness.
7. Demonstrate an understanding of business ethics.
8. Demonstrate confidentiality.
9. Demonstrate an understanding of workplace structures, organizations, systems, and climates.
10. Demonstrate diversity awareness.
11. Demonstrate job acquisition and advancement skills.
12. Demonstrate task management skills.
13. Demonstrate customer-service skills.

F. INTRODUCTION TO COMPUTER FORENSICS

Proficient IT professionals demonstrate knowledge in Computer Forensics as needed in their role. The following accountability criteria are considered essential for students Computer and Information Systems Security/Information Assurance program of study.

1. Define terms related to forensics and computer forensics, e.g., data, information, device, cloud, evidence, etc.
2. Investigate the origins and history of computer forensics and its impact on society.
3. Describe the role that computer forensics plays in the private or public sector.
4. Discuss and develop a code of ethics as related to the field of computer forensics.
5. Evaluate the types of visible and hidden data.
6. Compare and contrast the hardware and software essential for computer forensic investigation, e.g., hot swappable bays and operating systems.

G. INVESTIGATIVE PROCESS

Proficient IT professionals demonstrate knowledge and skills in investigative process as needed in their role. The following accountability criteria are considered essential for students Computer and Information Systems Security/Information Assurance program of study.

1. List the four basic phases of working a case, i.e., physical crime scene investigation, digital crime scene investigation, reconstruction, and communication.
2. Describe the process for starting a new case.
3. Discuss the purpose of previewing a device.
4. List the steps needed to acquire an image.
5. List the variants that must be taken into account before searching for a person's name, e.g., name spellings, nicknames, alias.
6. Describe the forensic examination process, i.e., seizure, acquisition, analysis, and reporting of evidence.
7. Create and maintain a case log.
8. Construct a report on findings from the investigation.

H. PHYSICAL EVIDENCE COLLECTION AND CONTROL

Proficient IT professionals demonstrate knowledge and skills in physical evidence collection and control as needed in their role. The following accountability criteria are considered essential for students Computer and Information Systems Security/Information Assurance program of study.

1. Describe the purpose of search and seizure laws.
2. Compare and contrast a voluntary consent to search versus a search warrant.
3. Demonstrate proper procedures for collecting and documenting evidence.

I. DATA ACQUISITION AND RECOVERY

Proficient IT professionals demonstrate knowledge and skills in data acquisition and recovery as needed in their role. The following accountability criteria are considered essential for students Computer and Information Systems Security/Information Assurance program of study.

1. Compare and contrast data storage, e.g., storage media, internal/external hard drives, disk arrays, cloud.
2. Compare and contrast common methods for erasing, recovering, and analyzing data.
3. Describe the need for hardware and software write-blocking protection.
4. Analyze the different types of write-blocking, e.g., USB forensic bridge.
5. Demonstrate proper use of write-blocking.
6. Analyze the information contained in a data acquisition log.

J. DIGITAL EVIDENCE ANALYSIS

Proficient IT professionals demonstrate knowledge and skills in digital evidence analysis as needed in their role. The following accountability criteria are considered essential for students Computer and Information Systems Security/Information Assurance program of study.

1. Distinguish between the values of data versus information.
2. Implement procedures for analyzing files and file systems, e.g., information searches, keyword searches, cryptology.
    a. Image/graphic
    b. Document
    c. Compressed
    d. Password
    e. Web activity/internet history
    f. E-mail
    g. Malware scans
3. Differentiate the multiple types of encoding, e.g. ASCII, Unicode, UTF-8, and UTF-16.
4. Define and distinguish between different numbering systems, i.e., binary coded decimal, hexadecimal, and binary.
5. Analyze the properties of endianness, big-endian, little-endian, and middle-endian.

Course Materials and Resources

Course Academic Standards and Indicators

Computer Science Academics Standards and Indicators