COMPUTER FORENSICS
COURSE CODE: 5374
STUDENT PROFILE

STUDENT'S NAME:	**TEACHER'S NAME:**
School Year/Semester:	**Grade:**
Begin Date:	**Date Completed:**

Directions: Document student's progress using the applicable rating scales below: Enter date of completion under the appropriate column.

0 - Has not received instruction in this area / **no experience or knowledge of this task (N/A)**
1 – Can apply and perform **independently (80-100)**
2 – Can perform the task completely with **limited supervision (70-79)**
3 – Requires additional instruction and or **close supervision (60-69)**

A. SAFETY		**0**	**1**	**2**	**3**
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		**0**	**1**	**2**	**3**
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		**0**	**1**	**2**	**3**
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., cyber bullying; 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, Creative Commons, documents, 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		**0**	**1**	**2**	**3**
1	Demonstrate punctuality.				
2	Demonstrate critical thinking and problem-solving skills				
3	Demonstrate initiative and self-direction.				
4	Demonstrate integrity.				
5	Demonstrate work ethic.				
6	Demonstrate conflict resolution skills.				
7	Demonstrate listening and speaking skills.				
8	Demonstrate respect for diversity.				
9	Demonstrate customer service orientation.				
10	Demonstrate teamwork.				
E. PROFESSIONAL KNOWLEDGE		**0**	**1**	**2**	**3**
1	Demonstrate global or “big picture” thinking.				
2	Demonstrate career and life management skills and goal-making.				
3	Demonstrate continuous learning and adaptability skills to changing job requirements.				
4	Demonstrate time and resource management skills.				
5	Demonstrates information literacy skills.				
6	Demonstrates information security skills.				

7	Demonstrates information technology skills.				
8	Demonstrates knowledge and use of job-specific tools and technologies.				
9	Demonstrate job-specific mathematics skills.				
10	Demonstrates professionalism in the workplace.				
11	Demonstrates reading and writing skills.				
12	Demonstrates workplace safety.				
F. INTRODUCTION TO COMPUTER FORENSICS		**0**	**1**	**2**	**3**
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		**0**	**1**	**2**	**3**
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	Construct a report on findings from the investigation.				
8	Construct a report on findings from the investigation.				
H. PHYSICAL EVIDENCE COLLECTION AND CONTROL		**0**	**1**	**2**	**3**
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		**0**	**1**	**2**	**3**
1	Compare and contrast data storage, e.g., storage media, internal/external hard drives, disk arrays, cloud.				
2	Evaluate the use of large data sets to explore a real-world phenomenon or support a claim.				
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		**0**	**1**	**2**	**3**
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.				