Southeast Missouri State University

Department of Industrial and Engineering Technology — Course No. CY620

Title of Course: Computer Forensics — Revision

New F12

I. Catalog Description and Credit Hours of Course:

Tools for computer forensics for hardware, software and networking. Ability to use debuggers to understand security issues. Strategies to recreate attack scenarios, evidence collection and analysis of data from different storage locations. Creation of observation strategies for a networked computing infrastructure to adapt to threats to the system. Implement an incidence response system. 3 credit hours.

II. Prerequisite (s): CY320 and CY310 or consent of instructor.

III. Purposes or Objectives of the Course:

A. Identify tools for computer forensics for hardware software and networking.

B. Ability to use debuggers for security analysis.

C. Ability to collect evidence from different storage locations.

D. Implement observation strategies for assets in a computing system.

E. Implementation of an incidence response process.

IV. Student Learning Outcomes:

A. Students will be able to use debuggers for security analysis.

B. Students will be able to collect evidence from different storage locations.

C. Students will be able to implement observation strategies for assets in a computing system.

V. Expectations of Students:

A. Students are expected to read assigned materials.

B. Students are expected to complete all assignments. Assignments will ONLY be accepted on the due dates provided, unless previous arrangements are made or student provides a written medical doctor's excuse.

C. Students are expected to participate in class and group discussions.

D. Student work will be completed in accordance with Code of Student Conduct (http://www6.semo.edu/judaffairs/code.html).

E. In a professional environment, work areas are kept clean. In keeping with a professional attitude towards fellow students, always clean your area before leaving.

F. All laboratory work must be completed during the regularly scheduled lab time.

VI. Course Content or Outline: (*4 contact hours per week*)

A.	1.	Tools for Computer Forensics	4 Weeks
	2.	Debugging strategies for security threats	3 Weeks
	3.	Evidence collection using tools and stored data	3 Weeks
	4.	Attack scenarios and threat modeling	2 Weeks
	5.	Observation strategies for security attacks	2 Weeks
	6.	Incidence response process and systems	2 Weeks

VII. Textbook(s) and/or Other Required Materials or Equipment:

A. Textbook to be announced.

B. Supplemental materials will be provided by the instructor.

VIII. Basis for Student Evaluations

A.
Homework	15%
Labs	10%
Class Participation*	5%
Mid-term Exam	25%
Final Exam	30%
Project	15%

B. Grading Policy:

90-100	A
80-89.9999	B
70-79.9999	C
<70	F

C. The weight of evaluation criteria may vary at the discretion of the instructor and will be indicated at the beginning of each course.

D. * Participation to class discussions, taking labs, homework, and exams on the assigned time slots. The instructor reserves the right, acting within the policies and procedures of the university, to make changes in course content or instructional techniques without notice or obligation. No late assignments will be accepted. “Emergencies” require that YOU contact the instructor ASAP. Request for a late submission after the due time will not be granted.