Montgomery County Community College
CIS 207
Introduction to Computer Forensics
3-2-2

COURSE DESCRIPTION:
This course will teach a student the knowledge and skills required to identify, track, and prevent cybercrimes. Students will also learn about the cyber security and investigation techniques, safeguarding of information and enhancing network and data security, while performing basic troubleshooting to identify and establish steps to prevent future attacks. The course will also cover the objectives of the EC-Council Computer Hacking Investigator (CHFI) certification examination.

PREREQUISITE(S):
CIS 275 Network Security Fundamentals or
CIS 208 Implementing Network Security

CO-REQUISITE(S):
CIS 275 Network Security Fundamentals or
CIS 208 Implementing Network Security

Upon successful completion of this course, the student will be able to:

LEARNING OUTCOMES	LEARNING ACTIVITIES	EVALUATION METHODS
1. Describe Computer Forensics and the Investigation Process.	Lecture/Discussion Homework Assignments Assigned readings Research	Discussion/Questions Research presentations Chapter Quiz
2. Interpret Digital Evidence.	Lecture/Discussion Hands on Labs Homework Assignments Assigned readings Research	Discussion/Questions Research presentations Chapter Quiz
3. Describe Hard Disks, File Systems and Windows Forensics.	Lecture/Discussion Hands on Labs Homework Assignments Assigned readings Research	Discussion/Questions Research presentations Chapter Quiz
4. Utilize Network Forensics to interpret Logs and Network Traffic.	Lecture/Discussion Hands on Labs Homework Assignments Assigned readings Research	Discussion/Questions Research presentations Chapter Quiz

LEARNING OUTCOMES	LEARNING ACTIVITIES	EVALUATION METHODS
5. Investigate Wireless Attacks, Web Attacks, Email Crimes and Mobile Forensics.	Lecture/Discussion Hands on Labs Homework Assignments Assigned readings Research	Discussion/Questions Research presentations Chapter Quiz Final Skills based assessment and written final exam.

At the conclusion of each semester/session, assessment of the learning outcomes will be completed by course faculty using the listed evaluation method(s). Aggregated results will be submitted to the Director of Educational Effectiveness. The benchmark for each learning outcome is that *70% of students will meet or exceed outcome criteria.*

SEQUENCE OF TOPICS:

Computer Forensics in Today's World

- Computer Forensics Investigation Process
- Searching and Seizing Computers and Digital Evidence
- First Responder Procedures

Understanding Hard Disks and File Systems

- Windows Forensics
- Data Acquisition and Duplication
- Recovering Deleted Files and Deleted Partitions
- Steganography and Image File Forensics

Forensics Investigation Using Software Tools

- Software Tools
- Application Password Crackers

Network Forensics

- Log Capturing and Event Correlation
- Investigating Logs and Investigating Network Traffic
- Investigating Wireless Attacks
- Investigating Web Attacks
- Tracking Emails and Investigating Email Crimes
- Mobile Forensics

Investigative Reports

LEARNING MATERIALS:
Nelson et all. (2018). Guide to Computer Forensics and Investigations (6th ed.) Cengage Brain, ISBN# 9781337685863

COURSE APPROVAL:
Prepared by: Anil Datta Date: 9/6/2013
VPAA/Provost or designee Compliance Verification:
Victoria L. Bastecki-Perez, Ed.D. Date: 12/2014

Prepared by: Marie Hartlein Date: 12/20/2019
VPAA/Provost or designee Compliance Verification: Date: 2/26/2020

This course is consistent with Montgomery County Community College's mission. It was developed, approved and will be delivered in full compliance with the policies and procedures established by the College.