Northwest Arkansas Community College

Business and Computer Information Systems Division

Discipline Code
NTWK

Course Number
2253

Course Title
Computer Forensics

Catalog Description
This course will provide an introduction to digital forensic fundamentals and best practices for incidence response. Students will learn how to obtain and analyze digital information for possible evidence in civil, criminal, and administrative cases. Students will be introduced to the legal and regulatory aspects of computer forensics including an understanding of the judicial system, investigation process, importance of evidence chain of custody, admissibility of expert witness testimony and incident reporting. Topics covered will include the setup of a laboratory, digital evidence, crime scene processing, rules of evidence, report writing, data acquisition, file systems, and forensic analysis and file recovery. (Outside lab time will be required.)

Prerequisites
NTWK 2014 Network & Information Systems (CCNA1), or
CMJS 2363 Introduction to Cybercrime

Credit Hours
3 credit hours

Contact hours
45 lecture/lab contact hours

Load hours
3 load hours

Semesters Offered
Spring, On Demand

ACTS Equivalent
N/A

Grade Mode
A-F

Learning Outcomes

Students will:

- Understand computer forensics and its history
  - Apply concepts of computer forensics to conduct an examination
  - Describe the rules, laws, policies and procedures that affect digital forensics
  - Demonstrate evidence collection methods
  - Describe the steps in performing digital forensics through to the legal proceedings
  - Identify and use multiple computer forensic tools (FTK, ProDiscover, SleuthKit, ect)
  - Explain evidence control and chain of evidence
  - Use forensic methods to acquire data from a suspect hard drive
  - Prepare a forensic report for a scenario

General Education Outcomes Supported

- Students can write clear, coherent, well-organized documents, substantially free of errors.
- Students can use computers proficiently.
- Students can employ a variety of sources to locate, evaluate, and use Information.

Standard Practices

Topics list

- Legal compliance
- Ethics and professional issues in forensics
- Search and seizure
- Chain of custody
- Evidence verification and validation
- Using virtual machines in forensic analysis
- Authentication of evidence
- E-Discovery
- Digital Investigations
- Steganography
- Cryptanalysis
- Cryptography
- Hashing
- Registry files
- Filesystems (Windows, Unix, macOS)
- File system forensics
- Metadata
- Slack space and hidden files/clusters/partitions
- File recovery
- Email investigations
- Live system investigations
- Mobile device analysis
- Network Forensics
- Forensic tools
- Live vs static data acquisition
- Virtual machine forensics
- Court room testimony
- Report writing

Learning activities

- A virtual environment for activities, assignments and projects utilizing a Windows and UNIX operating systems for forensic analysis of evidence.
- This course requires some in class, hands-on work and also additional hands-on work in a virtual or on-campus computer lab.

Assessments

- Written assignments
- Discussions
- Lab assignments
- Hands-on activities
- Projects
- Quizzes
- Exams

Grading guidelines

- A = 90-100
- B = 80-89
- C = 70-79
- D = 60-69
- F = 59 & below

Revision Date

May 20, 2020