**NorthWest Arkansas Community College**
**Business & Computer Information Systems Division**

# Computer Information Department Course Outline

# NTWK 2253 COMPUTER FORENSICS (On Demand)

## *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. Instructional methods to include: lecture, discussion, reading assignments, projects, hands-on labs and Canvas components. This course will require additional outside lab time.

## *Prerequisites*

| | |
|---|---|
| NTWK 2014 | Networking & Information Systems (CCNA1) or |
| CMJS 2363 | Introduction to Cybercrime |

## *Credit Hours/Contact Hours/Load Hours*

3/3/3

## *Target Audience/Transferability:*

The target audience includes, but is not necessarily limited to, the following:

- Students pursuing a career in Networking or other computer-related field
- Students who wish to enhance their understanding of computer forensic investigations
- Community members or networking professionals who wish to expand their understanding of computer forensic investigation.

## *Student Learning Outcomes:*

Students will:

- Understand computer forensics and its history
- Understand and apply concepts of computer forensics
- Understand 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)
- Understand evidence control and chain of evidence
- Acquire data from a suspect hard drive

## *Topics*

- Legal Compliance
- Ethics and Professional issues in forensics
- Search and Seizure
- Chain of Custody
- Evidence verification and validation
- Using Virtual Machines
- Authentication of Evidence
- E-Discovery
- Digital Investigations
- Steganography
- Cryptanalysis
- Registry Files
- File Systems
- File System forensicsMetadata
- 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 Machines
- Court room testimony
- Report writing

## *Forms of Assessment:*

Written assignments, discussions, hands-on activities, projects, quizzes, and exams.
Students will demonstrate proficiency by scoring 70% or above on all homework, quizzes, tests and lab assignments.

Rev. 7/2019