

Common Course Outline
DCOM 250
Digital Forensics II
4 Credits
The Community College of Baltimore County

Description

DCOM 250 – Digital Forensics II enables students to implement a methodological digital forensics analysis. This course covers major forensic investigation techniques such as password cracking, encryption technology, in-depth imaging analysis, and investigate browser history. Students will perform hands-on digital forensic exercises using various forensics tools.

4 Credits

Pre-requisite: DCOM 150

Overall Course Objectives

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

1. Define digital forensics and describe how to take a systematic approach when preparing a digital investigation;
2. Acquire evidence and validate the evidence;
3. Process evidence using forensics tools;
4. Compare and contrast various files system supported by different operating systems;
5. Create and conduct key searches to extract evidence;
6. Perform signature analysis and hash analysis;
7. Extract data from Windows artifacts;
8. Examine e-mail files, internet history, cache content, and internet artifacts from evidence file;
9. Extract data from web browser artifacts;
10. Perform password recovery;
11. Identify encryption algorithms;
12. Extract and analyze forensic evidence; and
13. Write a forensic report.

Major Topics

- I. Overview of digital forensics profession and investigation
- II. Process and validate evidence from various media using forensic tools.
- III. Data acquisition and validation
- IV. File systems
- V. Keyword searches

- VI. File signature analysis and hash Analysis
- VII. Windows artifacts
- VIII. Recovering deleted partition
- IX. Password recovery
- X. Mac operating system (OS) artifacts
- XI. CD/DVD file system
- XII. Digital forensics analysis, documentation and report writing

Course Requirements

Grading/Exams: Grading procedures will be determined by the individual faculty member and at a minimum will include the following:

- five laboratory projects
- two exams

Writing: The individual faculty member will determine specific writing assignments. Writing assignment should conform to Acceptable Usage Policy.

Other Course Information

This course is a program elective for the following programs:

Network Technology A.A.S Degree with Cisco Options
Information Systems Security, A.A.S Degree
Network Technology for Cisco Certificate
Information Systems Security Certificate

This course is the second course in a three -course sequence.
This course is taught in a computerized environment.

Revised: 04/26/16