Miami Dade College

Course Description

CET2880C | Digital Forensics | 4.00 Credits

This is an introductory digital forensics course for students who are studying cybersecurity, electronics or computer engineering technologies. In this course, students will learn the setup and use of an investigator's laboratory, how to perform data acquisition, web forensics, email forensics, mobile forensics, network analysis, and file recovery

Course Competencies

Competency 1: The student will demonstrate an understanding of methods of data acquisition and preservation by:

1. Identifying the aspects of digital systems that are volatile versus nonvolatile
2. Prioritizing relevant digital storage in terms of volatility
3. Enumerating the different locations valuable data may be stored (e.g. memory, processes, hard drives, cloud storage, etc)
4. Using appropriate tools to capture and store memory images (e.g. WinDD, DD, etc)
5. Identifying and using appropriate file formats for preserving disk images (e.g. dd, EWF, ISO, etc)
6. Demonstrating basic proficiency using Windows and Linux based operating systems

Competency 2: The student will demonstrate an understanding of recovering deleted, hidden, and lost files by:

1. Demonstrating a basic understanding of common file system types (e.g. FAT31, NTFS, EXT4, etc.)
2. Describing and acquiring various forms of meta- data from files (e.g. owner, permissions, file size, modification date, etc)
3. Explaining the purpose and role of slack space in file systems
4. Demonstrating an understanding of unallocated space and information that may be hidden in such regions
5. Using common tools to sift through large numbers of files looking for specific information (e.g., grep and String)
6. Using common tools to perform recovery of deleted files

Competency 3: The student will demonstrate a basic understanding of file and Document Analysis by:

1. Enumerating basic file types and their common extensions
2. Explaining why the file extension alone is not enough to identify the file type with certainty
3. Exploring the basic structure of several different file types (e.g. bmp, txt, exe, etc)
4. Identifying files located within the temporary directory
5. Finding data and metadata within the Windows registry system
6. Using common steganography tools to hide and recover data within images
7. Opening a file within a hex editor

Competency 4: The student will demonstrate an understanding of email forensics by:

1. Describing the process by which email is transferred across the internet
2. Identifying the common protocols used for email exchange (e.g SMTP, POP3, IMAP)
3. Identifying and using common email clients (e.g. Gmail, Outlook, Thunderbird, etc)
4. Describing the basic anatomy of the email header (e.g. To, From, Subject, Date)
5. Identifying the basic anatomy of the MIME header including IP address
6. Tracing the source of anonymous email using the IP address and tools such as tracert
7. Using common methods of email encryption such as GPG

Competency 5: The student will demonstrate an understanding of web forensics by:

1. Describing the process that occurs when a web address is typed into a web browser

2. Analyzing the current web browsers settings to locate relevant historical data
3. Using domain name service providers to locate the registrant and geographic location of web services
4. Enumerating the various URL schemes currently in use (e.g. http, https, ftp, nntp, mail to, telnet, etc)
5. Using the browser history and temporary files to analyze user activity
6. Setting up a basic web server (e.g. apache, httpd, IIS, etc)
7. Parsing and analyzing log files from common web servers
8. Describing the purpose of and demonstrating use of proxy servers to hide location records
9. Describing how onion routing (e.g. TOR) can be used to hide the location of users and servers
10. Using TOR to explore websites located on the dark net

Competency 6: The student will demonstrate an understanding of networks forensics by:

1. Identifying physical threats such as keyloggers that may be attached to the network
2. Accessing the network auditing features of Windows and Linux systems
3. Using a tool such a NMAP to map out devices attached to a network
4. Using a tool such as Wireshark to capture and analyze network packets
5. Using a tool such as netstat to determine current network connections
6. Enumerating the basic router operations such as DHCP, port forwarding, DNS, etc
7. Using who is to determine the owner/registrant of various IP ranges
8. Describing the methodologies used in network forensics (e.g. interlacing of device and network forensics, Log-file Analysis, Forensic Imaging and Analysis)
9. Describing the methodologies used in host forensics (e.g. File Systems and File System Forensics, Hypervisor Analysis, Cryptanalysis, Rainbow Tables, Known File Filters, Steganography, File Carving, Live System Investigations, Timeline Analysis)

Course Competency 7: The student will demonstrate an understanding of device forensics by:

1. Describing methods for the acquisition/analysis of widespread, non-PC devices (e.g. embedded devices, IoT)
2. Describing the basic operation of cell phones and cellular networks (e.g. CMDA, GSM, etc)
3. Describing the process of triangulation using cell phone towers to determine the location of an active cellular signal
4. Identifying the SIM card, and additional hardware identifiers used to identify the user on the cellular network (e.g. IMEI, SIM, ESN, ICCID, etc)
5. Locating data stored in various locations on the cellular device (e.g. SIM Card, SD Cards, Internal Storage, Cache, etc)
6. Using tools such as screen capture to log the forensics investigation process
7. Explaining the legal issues related to non-PC device forensic activities

Competency 8: The student will demonstrate an ability to circumvent common anti-forensics techniques by:

1. Identifying the four categories of anti-forensics behavior (i.e. artifact destruction, data hiding, trail obfuscation, and attacks against forensic tools)
2. Locating lost files by extracting history from the Windows Registry
3. Locating the metadata contained within the Device Configuration Overload (DCO) and the Host Protected Area (HPA)
4. Locating previously deleted files using the logs of the master file table
5. Examining the temporary files on the system for relevant data
6. Implementing and using basic methods of covert channels
7. Locating data stored in obscure/hidden locations (e.g. slack, bad clusters, hidden partitions, etc)

Competency 9: The student will demonstrate understanding of tasks related to the casework process by:

1. Describing methods and approaches for forensic analysis and examination on specified media

2. Processing image evidence (authentication, acquisition, sparse vs full imaging)
3. Maintaining evidence integrity
4. Processing forensic image.
5. Managing document examination process
6. Controlling/securing and accessing logs for image media
7. Discussing the rules, laws, policies, and procedures that affect digital forensics
8. Describing the steps in performing digital forensics from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, through the completion of legal proceedings
9. Using one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Formulate strategies to locate, evaluate, and apply information
- Use computer and emerging technologies effectively
- Describe how natural systems function and recognize the impact of humans on the environment

Updated: Fall 2025