

[Creative Commons License](http://creativecommons.org/licenses/by/3.0/deed.en_US)

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](http://creativecommons.org/licenses/by/3.0/deed.en_US).

Authoring Organization: Moraine Valley Community College

Written by: David Rigor

Copyright: © National Information Security, Geospatial Technologies Consortium (NISGTC)

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

**Digital Forensics Syllabus**

Please provide a complete syllabus. All elements of the syllabus are required unless noted as “if applicable.”

|  |  |
| --- | --- |
| **Course Title:** Digital Forensics: Processing, Tools, File Systems, and Analysis | **Course Number** (If applicable): LAN143AB |
| **COURSE DESCRIPTION:** This course instructs students in the preservation, identification, extraction, documentation and interpretation of computer data. Students will learn about processing the crime scene, computer forensic tools, file systems, and forensics analysis.  **Note:** Companion Courses (LAN143AA Digital Forensics: Introduction, Investigative Methodology, Forensics, and Data Acquisition and LAN143AC Digital Forensics: Mobile, Email, Recovering Graphics, Networks, and Reporting) bookend the sequence of topics to include, the basics of digital forensics, investigative methodology, the forensics lab, and data acquisition, mobile devices & email, recovering graphics, network forensics, and testimony & report writing. | |
| **PREREQUISITES:** LAN143AA | |
| **REQUIRED MATERIALS: None** | |
| **ADDITIONAL RESOURCES** (if applicable): | |
| **LEARNING OUTCOMES/COMPETENCIES:**  **Computer Network Defense**  1.3 Knowledge of unix command line (e.g., mkdir, mv, ls, passwd, grep, etc.) (CND342)  **Digital Forensics**  2.1 Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures) (DF786)  2.2 Provide technical assistance on digital evidence matters to appropriate personnel (DF817)  2.4 Knowledge of Forensic Chain of Evidence (DF290)  2.5 Assist in the gathering and preservation of evidence used in the prosecution of computer crimes (DF429)  2.8 Use an array of specialized computer investigative techniques and programs to resolve the investigation (DF872)  2.9 Skill in seizing and preserving digital evidence (DF217)  2.10 Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise (DF438)  2.12 Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes hard drives, floppy diskettes, CD, PDA, mobile phones, GPS, and all tape formats (DF480)  2.13 Decrypt seized data using technical means (DF482)  2.15 Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.) (DF564)  2.16 Ensure chain of custody is followed for all digital media acquired (e.g., indications, analysis, and warning standard operating procedures) (DF573)  2.17 Examine recovered data for items of relevance to the issue at hand (DF613)  2.18 Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration (DF636)  2.19 Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment (DF749)  2.21 Perform hash comparison against established database (DF753)  2.22 Perform live forensic analysis (e.g., using Helix in conjunction with LiveView) (DF758)  2.23 Perform MAC timeline analysis on a file system (DF759)  2.24 Perform static media analysis (DF768)  2.25 Perform tier 1, 2, and 3 malware analysis (DF771)  2.28 Review forensic images and other data sources for recovery of potentially relevant information (DF839)  2.29 Update hash comparison databases from various libraries (e.g., National Software Reference Library, National Security Agency/Central Security Service Information Systems Incident Response Team) (DF867)  2.32 Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence (DF871)  2.34 Knowledge of binary analysis (DF268)  2.35 Knowledge of file system implementations (DF287)  2.39 Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files (DF346)  2.40 Skill in analyzing memory dumps to extract information (DF350)  2.41 Skill in identifying, modifying, and manipulating applicable system components (Windows and/or Unix/Linux) (e.g., passwords, user accounts, files) (DF364)  2.42 Skill in processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data (DF369)  2.44 Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK) (DF381)  2.46 Knowledge of types of digital forensics data and how to recognize them (DF888)  2.47 Knowledge of forensics in multiple operating system environments (DF890)  2.48 Ability to decrypt digital data collections (DF908)  2.49 Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property (DF620)  **Incident Response**  3.1 Skill in seizing and preserving digital evidence (IR217)  3.2 Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems (IR755) | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **COURSE ASSESSMENT:**  **Grading Scale**   |  |  | | --- | --- | | **Category** | **Points** | | Labs | 90 | | Quizzes | 50 | | Case Studies/Assignments | 20 | |  |  | | **Total** | 160 |  |  |  |  | | --- | --- | --- | | **Total Points** | **Percentage** | **Grade** | | 148-160 | 92-100 | A | | 136-147 | 85-91 | B | | 124 | 135 | C | | 110-123 | 69-76 | D | | 0-109 | 0-68 | F | |

**COURSE SCHEDULE:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson** | **Module/Lesson Title & description** (if applicable) | **Learning Outcomes** | **Assignment (w/category & point value)** |
|  | Processing the Crime Scene | 1. Describe how to secure a computer, incident or crime scene. 2. List procedures for storing digital evidence. 3. Identify hashing algorithms used for forensic purposes. | Quiz 1 (5 pts)  Case Study 1  Lab 6 – Introduction to Single Purpose Forensic Tools |
|  | Computer Forensics Tools | 1. Describe how to evaluate needs for computer forensic tools. 2. Identify available computer forensic software tools. 3. Identify methods for validating and testing computer forensic tools. 4. List considerations for computer forensic hardware tools. | Quiz 2 (15 pts)  Lab 7 – Introduction to Autopsy Forensic Browser  Lab 8 – Introduction to PTK Forensics Basic Edition |
|  | File Systems | 1. Describe Microsoft file structures. 2. Explain the structure of NTFS disks. 3. Describe the Mac file structure and boot process. 4. Identify the Linux disk structure. | Quiz 3 (15 pts)  Lab 9 – Analyzing a FAT Partition with Autopsy  Lab 10 – Analyzing an NTFS Partition with PTK |
|  | Computer Forensics Analysis | 1. Determine data to be analyzed. 2. Explain tools utilized to validate data. 3. Explain common data hiding techniques. 4. Describe methods of performing a remote acquisition. | Quiz 4 (15 pts)  Case Study 2  Lab 11 – Browser Artifact Analysis |