River Valley Community College
One College Place
Claremont, NH 03743

March 2012

DIGITAL FORENSICS

CURRICULUM AND COURSE NUMBER:	CYBS 250R
DEPARTMENT:	Business/Computer Technology
CREDIT HOURS:	3
SEMESTER HOURS:	**CLASS:** 2 **LAB:** 2
PREREQUISITES/COREQUISITES:	CYBS 140R

COURSE DESCRIPTION

Students will learn procedures on tracking, analyzing, and patching security holes after an incident has occurred. This will include seizure of equipment, analysis of confiscated materials, and follow up procedures relating to the incident.

Course Competencies:
Upon successful completion of this course, the student will be able to:

1. Computer Forensics and Investigations as a Profession: This topic introduces you to computer forensics and investigations and discusses some of its problems and concerns.
   a. Define digital forensics.
   b. Describe how to prepare for digital evidence investigations and explain the differences between law enforcement agency and corporate investigations.
   c. Explain the importance of maintaining professional conduct.
2. Understanding Computer Investigations: This topic explains how to manage a computing investigation. You will learn about the problems and challenges that examiners face when preparing and processing investigation, including the ideas and questions they must consider.
   a. Explain how to prepare a computer investigation.
   b. Apply a systematic approach to an investigation.
   c. Describe procedures for corporate high-tech investigations.
   d. Explain requirements for data recovery workstations and software.
   e. Describe how to conduct an investigation.
   f. Explain how to complete and critique a case.
3. The Investigator's Office and Laboratory: This topic details what you need to set up an effective computing-forensics laboratory, which is where you examine most of the evidence data that you acquire for an investigation.
   a. Describe certification requirements for computer forensics labs.
   b. List physical requirements for a computer forensics lab.
   c. Explain the criteria for selecting a basic forensic workstation.
   d. Describe components used to build a business case for developing a forensics lab.
4. Data Acquisition: In this topic, you will learn how to acquire digital evidence from electronic media.
   a. List digital evidence storage formats.

   b. Explain ways to determine the best acquisition method.
   c. Describe contingency planning for data acquisitions.
   d. Explain how to use acquisition tools.
   e. Describe how to validate data acquisitions.
   f. Describe RAID acquisition methods.
   g. Explain how to use remote network acquisition tools.
   h. List other forensics tools available for data acquisitions.
5. Processing Crime and Incident Scenes: This topic describes the differences between the needs and concerns of a business and a law enforcement organization, and then discusses incident-scene processing for both the corporate investigator and the law enforcement investigator.
   a. Explain the rules for digital evidence.
   b. Describe how to collect evidence at private-sector incident scenes.
   c. Explain guidelines for processing law enforcement crime scenes.
   d. List the steps in preparing for an evidence search.
   e. Describe how to secure a computer incident or crime scene.
   f. Explain guidelines for seizing digital evidence at the scene.
   g. List procedures for storing digital evidence.
   h. Explain how to obtain a digital hash.
   i. Review a case to identify requirements and plan your investigation.
6. Working with Windows and DOS Systems: This topic reviews how data is stored and managed on Microsoft operating systems. In this chapter, you examine the tasks each operating system performs when it starts so you can avoid altering evidence when you examine data on a disk.
   a. Explain the purpose and structure of file systems.
   b. Describe Microsoft file structures.
   c. Explain the structure of NTFS disks.
   d. List some options for decrypting drives encrypted with whole disk encryption.
   e. Explain how the Windows Registry works.
   f. Describe Microsoft startup tasks.
   g. Describe MS-DOS startup tasks.
   h. Explain the purpose of a virtual machine.
7. Current Computer Forensics Tools: This topic explores the software and hardware tools you use during computing investigations and forensic analysis.
   a. Explain how to evaluate needs for computer forensics tools.
   b. Describe available computer forensics software tools.
   c. List some considerations for computer forensics hardware tools.
   d. Describe methods for validating and testing computer forensics tools.
8. Macintosh and Linux Boot Processes and File Systems: In addition to Linux and Macintosh operating systems, this topic discusses media and hardware such as CDs, Integrated Device Electronics (IDE) hard drives, small computer system interface (SCSI) hard drives, SATA drives, and the redundant array of independent disks (RAID) configuration.
   a. Explain Macintosh file structures and the boot process.
   b. Explain UNIX and Linux disk structures and boot processes.
   c. Describe other disk structures.
9. Computer Forensic Analysis and Validation: This topic explains how to apply your computer forensics skills and techniques to a computing investigation, including what

data to collect and analyze. Validation with hex editors and forensics software is explained.
   a. Determine what data to analyze in a computer forensics investigation.
   b. Explain tools used to validate data.
   c. Explain common data-hiding techniques.
   d. Describe methods of performing a remote acquisition.
10. Recovering Graphics Files: This topic begins with brief introductions to computer graphics and data compressions, and then explains how to locate and recover image files based on information stored in image file headers.
    a. Describe types of graphics file formats.
    b. Explain types of data compression.
    c. Explain how to locate and recover graphics files.
    d. Describe how to identify unknown file formats.
    e. Explain copyright issues with graphics.
11. Network Forensics: This topic covers tools and methods for conducting network investigations, performing live acquisitions, and reviewing network logs for evidence. It also examines using UNIX/Linux tools and the Honeynet Project's resources.
    a. Describe the importance of network forensics.
    b. Explain standard procedures for performing a live acquisition.
    c. Explain standard procedures for network forensics.
    d. Describe the use of network tools.
    e. Describe the goals of the Honeynet Project.
12. E-mail Investigations: This topic explains how e-mail works to send and retrieve messages via the Internet. It also reviews some specialized forensics tools.
    a. Explain the role of e-mail in investigations.
    b. Describe client and server roles in e-mail.
    c. Describe tasks in investigating e-mail crimes and violations.
    d. Explain the use of e-mail server logs.
    e. Describe some available e-mail computer forensics tools.
13. Cell Phone and Mobile Device Forensics: This topic covers investigation techniques and acquisition procedures for recovering data from cell phones and mobile devices.
    a. Explain the basic concepts of mobile device forensics.
    b. Describe procedures for acquiring data from cell phones and mobile devices.
14. Report Writing for High-Tech Investigations: This topic discusses the importance of report writing in examinations and offers guidelines on report content, structure, and presentation. Generating reports with forensics software tools is explored.
    a. Explain the importance of reports.
    b. Describe guidelines for writing reports.
    c. Explain how to use forensics tools to generate reports.
15. Expert Testimony in High-Tech Investigations: This topic explains how to become an expert witness and how to avoid problems when giving testimony.
    a. Explain guidelines for giving testimony as a technical/scientific or expert witness.
    b. Describe guidelines for testifying in court.
    c. Explain guidelines for testifying in dispositions and hearings.
    d. Describe procedures for preparing forensics evidence for testimony.
16. Ethics for the Expert Witness: This topic provides guidance in the principles and practice of ethics for computer forensics investigators and examines other codes of ethics.
    a. Explain how ethics and codes apply to expert witnesses.
    b. Explain how other organizations' codes of ethics apply to expert testimony.

c. Describe ethical difficulties in expert testimony.

17. Scenario-based Projects: This topic provides the student with practical application of the knowledge and skills covered in the previous topics and courses.

a. Complete a scenario-based project based on a corporate incident.
b. Complete a scenario-based project based on a data recovery incident.
c. Complete a scenario-based project based on a law enforcement incident.

Course Outline:

Computer Forensics investigation techniques
Investigation techniques for Windows and DOS Systems
Investigation techniques for Macintosh and Linux Systems
Computer Forensics Tools
Digital Evidence Controls
Processing Crime and Incident Scenes
Data Acquisition
Computer Forensic Analysis
E-mail Investigations
Recovering Image Files
Writing Investigation Reports
Becoming an Expert Witness

Learning/Instructional Methods:

Lectures
PowerPoint Presentations
Lab and Reading Assignments
Discussions
Term Papers

Performance Evaluation:

Midterm and Final Exams
Term Paper
Quizzes
Weekly written assignments
Discussion participation

Suggested Text(s): Please refer to syllabus

Origination date:

Revisions:
March 2012