Note:

Course content may be changed, term to term, without notice. The information below is provided as a guide for course selection and is not binding in any form, and should <u>not</u> be used to purchase course materials.

COURSE SYLLABUS

CSCI 511
DIGITAL FORENSICS

COURSE DESCRIPTION

This course covers the basics of digital forensics, including the technical aspects of evidence gathering for legal testimony and usage of digital forensics tools.

RATIONALE

Computing systems are increasingly involved in criminal activity, motivating the need for forensics specialists who understand the tools and techniques required to acquire, examine, and interpret digital evidence. Students interested in cyber security must understand the technical and legal implications of today's digital world in order to competently promote justice when computer systems are misused. This course will introduce students to this field of computer forensics and provide a comprehensive foundation for investigating and responding to cyber crime.

I.   PREREQUISITE

For information regarding prerequisites for this course, please refer to the Academic Course Catalog.

II.   REQUIRED RESOURCE PURCHASE

Click on the following link to view the required resource(s) for the term in which you are registered: http://bookstore.mbsdirect.net/liberty.htm

III.   RECOMMENDED RESOURCE PURCHASE

American Psychological Association. *Publication manual of the American Psychological Association* (Current ed.). Washington, DC: Author.

IV.   ADDITIONAL MATERIALS FOR LEARNING

A.   Computer with basic audio/video output equipment

B.   Internet access (broadband recommended)

C.   Blackboard recommended browsers

D.   Microsoft Office

V.   MEASURABLE LEARNING OUTCOMES

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

A.   Use forensic technology and tools in order to collect, recover, preserve, and prepare digital evidence in a forensically sound manner from a variety of digital systems.

B.   Evaluate typical forms of computer crime or attack to determine evidentiary value.

C.   Explain the legal issues and rules of evidence that apply in performing digital forensic analyses.

D.   Prepare a forensics report in an administrative, civil, or criminal context to defend investigative findings in the role of an expert witness.

E.   Integrate biblical principles within the field of digital forensics.

VI.   **COURSE REQUIREMENTS AND ASSIGNMENTS**

A.   Textbook readings and lecture presentations

B.   Course Requirements Checklist

After reading the Course Syllabus and Student Expectations, the student will complete the related checklist found in Module/Week 1.

C.   Discussion Board Forums (3)

Discussion boards are collaborative learning experiences. Therefore, the student is required to provide a thread in response to the provided prompt for each forum. Each thread must be at least 300 words and demonstrate course-related knowledge. In addition to the thread, the student is required to reply to 2 other classmates' threads. Each reply must be at least 150 words. All assertions in the student's thread and replies must be supported by Reading & Study materials, good examples, thoughtful analysis, and at least 1 scholarly resource.

D.   Labs (8)

The student will complete labs associated with the course material. Each lab will have specific instructions for tasks, along with deliverables, to be completed in the virtual lab environment.

E.   Quizzes (6)

Each quiz will cover the Reading & Study material for the module/week in which it is assigned. Each quiz will be open-book/open-notes, contain 8 multiple-choice and/or true/false questions and 2 short answer questions, and have a 20-minute time limit.

F.   Midterm Exam

The Midterm Exam will cover the Reading & Study material for Modules/Weeks 1–4. The Midterm Exam will be open-book/open-notes, contain 48 multiple-choice and/or true/false questions and 2 short answer questions, and have a 1-hour and 30-minute time limit.

G.   Final Exam

The Final Exam will cover all of the Reading & Study material for the entire course. The Final Exam will be open-book/open-notes, contain 48 multiple-choice and/or true/false questions and 2 short answer questions, and have a 1-hour and 30-minute time limit.

VII.   COURSE GRADING AND POLICIES

A.   Points

Course Requirements Checklist		10
Discussion Board Forums (1 at 40 pts; 2 at 50 pts ea)		140
Labs (8 at 75 pts ea)		600
Quizzes (6 at 10 pts ea)		60
Midterm Exam	(Modules 1–4)	100
Final Exam	(Modules 1–8)	100
	Total	1010

B.   Scale

A = 940–1010   A- = 920–939   B+ = 900–919   B = 860–899   B- = 840–859

C+ = 820–839   C = 780–819   C- = 760–779   F = 0–759

C.   Disability Assistance

Students with a documented disability may contact Liberty University Online's Office of Disability Academic Support (ODAS) at LUOODAS@liberty.edu to make arrangements for academic accommodations. Further information can be found at www.liberty.edu/disabilitysupport.

COURSE SCHEDULE

CSCI 511

MODULE/ WEEK	READING & STUDY	ASSIGNMENTS	POINTS
1	Easttom: chs. 1, 3 Maras: chs. 1–2 1 presentation 1 worksheet	Course Requirements Checklist Class Introductions DB Forum 1 Lab 1: Documenting a Workstation Configuration Using Common Forensic Tools Quiz 1	10 0 40 75 10
2	Easttom: chs. 4–5 Maras: chs. 3–4 1 presentation 1 worksheet	Lab 2: Creating a Forensic System Case File for Analyzing Forensic Evidence Quiz 2	75 10
3	Easttom: chs. 6–7 Maras: chs. 8, 11 1 presentation 1 worksheet	Lab 3: Uncovering New Digital Evidence Using Bootable Forensic Utilities Quiz 3	75 10
4	Easttom: ch. 8 Maras: ch. 5 1 presentation 1 worksheet	DB Forum 2 Lab 4: Automating E-Mail Evidence Discovery Using P2 Commander Midterm Exam	50 75 100
5	Easttom: chs. 9–10 Maras: ch. 6 1 presentation 1 worksheet	Lab 5: Recognizing the Use of Steganopgraphy in Image Files Quiz 4	75 10
6	Easttom: ch. 11 Maras: chs. 9, 13 1 presentation 1 worksheet	DB Forum 3 Lab 6: Analyzing Images to Identify Suspicious or Modified Files Quiz 5	50 75 10
7	Easttom: ch. 12 Maras: ch. 12 1 presentation 1 worksheet	Lab 7: Decoding an FTP Protocol Session for Forensic Evidence Quiz 6	75 10
8	Easttom: chs. 13–15 Maras: chs. 7, 10, 14 1 presentation 1 worksheet	Lab 8: Conducting an Incident Response Investigation for a Suspicious Login Final Exam	75 100

TOTAL		**1010**

DB = Discussion Board

NOTE: Each course module/week begins on Monday morning at 12:00 a.m. (ET) and ends on Sunday night at 11:59 p.m. (ET). The final module/week ends at 11:59 p.m. (ET) on **Friday**.