REGIS UNIVERSITY

COLLEGE OF COMPUTER & INFORMATION SCIENCES

Syllabus

Course Title: Cyber Forensics
Course Number: CIT 435

Course Description:

Introduces the principles and practices of digital forensics including digital investigations, data and file recovery methods, and digital forensics analysis and invalidation. Topics include data acquisition, digital forensics tools, virtual machines, network, mobile device, and cloud forensics.

Prerequisite Courses:

Prerequisite(s): CIT 331.

Course Overview

Many people do not know that the scientific discipline of computer forensics is gaining prominence, and rapidly becoming essential to recovering evidence that is so vital to pursuing justice for all persons. This course focuses on the use of the most popular forensics tools and provides specific guidance on dealing with civil and criminal matters relating to the law and technology. Includes discussions on how to manage a digital forensics operation in today's business environment.

Key concepts to be covered in this course include:

- Understanding the Digital Forensics Profession and Investigations.
- The Investigator's Office and Laboratory.
- Data Acquisition.
- Processing Crime and Incident Scenes.
- Working with Windows and CLI Systems.
- Current Computer Forensics Tools.
- Macintosh and Linux Boot Processes and File Systems.
- Recovering Graphics Files.
- Computer Forensics Analysis and Validation.
- Virtual Machine and Cloud Forensics.

- Live Acquisitions and Network Forensics.
- Email Investigations.
- Cell Phone and Mobile Device Investigations
- Report Writing for High Tech Investigations.
- Expert Testimony in High Tech Investigations.
- Ethics for the Investigator and Expert Witness.

Course Outcomes:

Upon completion of this course, learners should be able to:

- Explain how to prepare a digital forensics investigation by taking a systematic approach
- Analyze how the advent of computer technologies changes the nature of cybercrime.
- Determine what data to collect and analyze
- Explain standard procedures for conducting forensic analysis
- Apply different computer forensic tools to a given cybercrime scene
- Apply current practices to data recovery and acquisition.

Course Materials:

Required Texts:

Nelson, B., Phillips, A., & Steuart, C. (2016). *Guide to Computer Forensics and Investigations* (5th ed.). Boston, MA: CENGAGE Learning. ISBN 1-285-06003-2, 978-1-285-06003-3.

American Psychological Association. (2010). *Publication Manual of the American Psychological Association (6th ed.).* Washington, DC: American Psychological Association. ISBN 1433805618, 978-1433805615. Companion website: http://www.apastyle.org.

Technology Requirements:

The labs are designed to run as a virtualized computer using a software package such as VMware, Parallels, or VirtualBox.

You must have up to date virus protection software on your computer. If your computer does not meet any of these requirements, please contact the instructor immediately.

Minimum Requirements for Virtualization

- 1 GHz processor (2 GHz or higher recommended)
- 1 GB RAM (2 GB or higher recommended)
- 10 GB available hard disk space (30 GB recommended)
- Cable or DSL Internet connection

Pre-Assignment:

Online Format: Sign on to D2L (Home Page) and become familiar with the course navigation of the Web Curriculum. Read chapters 1 & 2 from the textbook,

Classroom-based Format: Read chapters 1 & 2 from the textbook,

Pre-Assignment Due Dates:

Classroom-based Format: This assignment is due the first night of class.

Online Format: The instructor will specify the due date for this assignment.

Course Assignments and Activities:

Wk	Topics	Readings	Activities Assignments and Associated Points
1	Introduction to Cyber Forensics	Text: Ch. 1 & 2	Class Discussion: • Introductions • Weekly Discussion Forum (25 pts)
2	Processing Crime and Incident Scenes	Text: Ch. 3 &4	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • When Search Warrants are Not Required for Searches and Seizures - Paper (100 pts)
3	File Systems	Text: Ch. 5 & 7	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • Hidden and Deleted Evidence - Paper (100 pts)
4	Cyber Forensics Tools	Text: Ch.6 & 8	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • Examination Processes and Validated Tools in Cyber Forensics - Paper (100 pts)
5	Digital Forensics Analysis and Validation	Text: Ch. 9	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • Best Practices for Cyber Forensics - Paper (100 pts) • Lab (50 pts)

6	Network and Cloud Forensics	Text: Ch.10 & 13	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • Network Types and Forensic Artifacts and Tools - Paper (100 pts)
7	Email, Social Media, and Mobile Device Forensics	Text: Ch.11 & 12	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • Mobile Phone Forensics - Paper (100 pts)
8	The Professional Cyber Forensics Expert	Text: Ch. 14, 15 & 16	Class Discussion: • Weekly Discussion Forum (25 pts) Written Assignment: • Cyber Forensics Critical Elements : Final Written Paper (250 pts)
			Maximum Points Possible: 1100

Course Policies and Procedures:

CC&IS Grading Scale

Letter Grade	Percentage	Grade Point
A	93 to 100	4.00
A–	90 to less than 93	3.67
B+	87 to less than 90	3.33
B	83 to less than 87	3.00
B–	80 to less than 83	2.67
C+	77 to less than 80	2.33
C	73 to less than 77	2.00
C–	70 to less than 73	1.67
D+	67 to less than 70	1.33
D	63 to less than 67	1.00
D-	60 to less than 63	.67
F	Less than 60	0

Additional information about grading can be found in the latest edition of the University Catalog, available at http://www.regis.edu/Academics/Course%20Catalog.aspx.

CC&IS Policies and Procedures

Each of the following CC&IS Policies & Procedures is incorporated here by reference. Students are expected to review this information each term, and agree to the policies and procedures as identified here and specified in the latest edition of the University Catalog, available at http://www.regis.edu/Academics/Course%20Catalog.aspx or at the link provided.

- The CC&IS Academic Integrity Policy.
- The Student Honor Code and Student Standards of Conduct.
- Incomplete Grade Policy, Pass / No Pass Grades, Grade Reports.
- The Information Privacy policy and FERPA. For more information regarding FERPA, visit the U.S. Department of Education.
- The HIPPA policies for protected health information. The complete Regis University HIPAA Privacy & Security policy can be found here: http://www.regis.edu/About-Regis-University/University-Offices-and-Services/Auxiliary-Business/HIPAA.aspx.
- The Human Subjects Institutional Review Board (IRB) procedures. More information about the IRB and its processes can be found here: http://regis.edu/Academics/Academic-Grants/Proposals/Regis-Information/IRB.aspx.

The CC&IS Policies & Procedures Syllabus Addendum summarizes additional important policies including, Diversity, Equal Access, Disability Services, and Attendance & Participation that apply to every course offered by the College of Computer & Information Sciences at Regis University. A copy of the CC&IS Policies & Procedures Syllabus Addendum can be found here: https://in2.regis.edu/sites/ccis/policies/Repository/CCIS%20Syllabus%20Addendum.docx.