Syllabus

CYB 205 – Digital Forensics (Credit Units: 3)

Department of Cyber Security
Faculty of Computing
University of Delta, Agbor, Nigeria

Lecturer: Dr. Okpako Abugor Ejaita
Office Location: FOC Room 2
Email: ejaita.okpako@unidel.edu.ng
Phone: +234 08163239516
Office Hours: Monday, Tuesday, Wednesday, Thursday & Friday 8:00 am - 4:00 pm

There are many ways to reach me. There is no substitute for face-to-face communication which often leads to more refined and focused questions resulting in your improved understanding. I strongly encourage you to take advantage of my office hours. Questions during class or immediately after class are always welcomed. Email is an easy way to ask questions outside of class but is not productive as face-to-face communication.

Meeting Time and Place: Wednesday, 10:00am to 12:00pm, FOC LH 4

Attendance

You are expected to attend every class. If you must miss a class, it is your responsibility to make up for the work that you missed. If you are going to be absent from any class, you must please notify the instructor in advance.

Methods of Instruction

This syllabus contains an overview of what will be covered in class; for specific information, students are referred to the class web page maintained on the University website. Assignments will be posted on University of Delta LMS or given in the class and should be submitted through University of Delta LMS. Class attendance, doing all your practical and homework will help the borderline cases.

Overview

Computer forensics cannot be divorced from the law. A computer forensics investigator needs knowledge of the law to effectively do his or her job. Meanwhile, legal professionals working on cybercrimes must have knowledge of the hardware, software, and technology involved in computer forensics to effectively do their jobs. This course presents an overview of the principles and practices of digital investigation. The objective of this class is to emphasize the fundamentals and importance of digital forensics. Students will learn different techniques and procedures that enable them to perform a digital investigation. This course focuses mainly on the analysis of physical storage media and volume analysis and covers the major phases of digital investigation such as preservation, analysis and acquisition of artifacts that reside in hard disks, random access memory, mobile devices, email, and network devices.

Objectives

The objectives of this course are to: (i) describe the world of computer forensics; (ii) discuss digital investigation and digital evidence; (iii) laws regulating access to electronic evidence; (iv) examine open-source forensics tools to perform digital investigation; (v) discuss file system analysis & file recovery on Windows & Linux operating systems; (vi) describe file carving & document analysis; (vii) discuss email and network; and (viii) explain mobile devices in computer forensics investigations.

Learning outcomes

Upon completion of this course, should be able to: (i) explain and properly document the process of digital forensics analysis; (ii) discuss the trade-offs and differences between various forensic tools; (iii) describe the representation and organization of data and metadata within modern computer systems; (iv) describe the inner workings of file systems; (v) create disk images, recover deleted files and extract hidden information; (vi) define the current research problems in computer forensics and develop effective solutions.

Course Contents

Cybercrime defined. Cybercrime vs traditional crime. Cybercrime categories. Combating cybercrime. Digital investigation and digital evidence. Laws regulating access to electronic evidence. Searches and seizures of computers and electronic evidence. Cybercrime laws. Computer-networking environment. Cybercrime incident scene. Data Acquisition of physical storage devices. File system analysis & file recovery on Microsoft Windows & Linux Systems. File carving & document analysis. Email forensics. Network forensics. Mobile devices in computer forensics investigations. The pretrial and courtroom experiences of a computer forensics investigator

Lecture Schedules

Week	Content	Lecture notes/slides
1.	Cybercrime defined. Cybercrime vs traditional crime. Cybercrime categories. Combating cybercrime.	
2.	Digital investigation and digital evidence.	
3.	Laws regulating access to electronic evidence	
4.	Searches and seizures of computers and electronic evidence & Cybercrime laws	
5.	Computer Forensics Tools	
6.	Cyberterrorism & Networking environment	
7.	Mid-semester break	
8.	Data Acquisition of physical storage devices	
9.	Test	
10.	File System Analysis & file recovery	
11.	File carving & document analysis	
12.	Email & Network forensics	
13.	Mobile devices in computer forensics	
14.	Revisions	
15.	Final Exam	

Examination schedule

- Attendance
- Homework
- Class Test
- Practical exercises
- End of Semester Exam

Practical Exercises

1: International cybercrime case
2: Court case and computer forensics tool
3: Admitting hearsay evidence in criminal or civil court
4: Using Internet resources & review of scientific papers
5: Computer forensics workstation
6: Forensic examination using TSK
7: Digital forensic investigation
8: Volume Analysis

9: File carving
10: Log analysis
11: Exploring SIMcon mobile forensics software tool
12: Mounting a VM as a drive in the OSForensics tool

Grading

- Homework: 10% of grade
- Practical: 10% of grade
- Midterm Exam: 10% of grade
- Final Exam: 70% of grade

Text & References

Lin X. (2018), introductory computer forensics: a hands-on practical approach, Springer

Maras M-H (2015), Computer forensics: cybercriminals, laws, and evidence 2/e, Jones & Bartlett Learning

Britz M. T. (2013), Computer Forensics and Cyber Crime: An Introduction 3/e, https://ec.europa.eu › project-result-content, February 2023

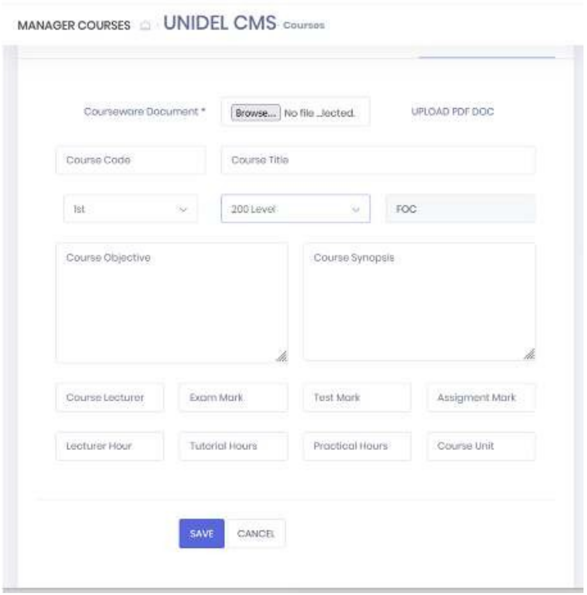
Sammons J. (2012), The basics of digital forensics, Elsevier

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behaviour conducive to a positive learning environment. The code of student conduct is described in detail in the student handbook or University website.

Academic Honesty

"All students enrolled at the University shall follow the tenets of common decency and acceptable behaviour conducive to a positive learning environment." It is the policy of the University, that no form of plagiarism or cheating will be tolerated. Plagiarism is defined as the deliberate use of another's work and claiming it as one's own. This means ideas as well as text or code, whether paraphrased or presented verbatim (word-for-word). Cheating is defined as obtaining unauthorised assistance on any assignment. Proper citation of sources must always be utilised thoroughly and accurately. If you are caught sharing or using other people's work in this class, you will receive a 0 grade and a warning on the first instance. A subsequent instance will result in receiving an F grade for the course, and possible disciplinary proceedings. If you are unclear about what constitutes academic dishonesty, ask.



MANAGER COURSES UNIDEL CMS Courses

Courseware Document * No file ..lected.

Course Code | Course Title

1st | 200 Level | FOC

Course Objective | Course Synopsis

Course Lecturer | Exam Mark | Test Mark | Assigment Mark

Lecturer Hour | Tutorial Hours | Practical Hours | Course Unit