Institute of Business Administration

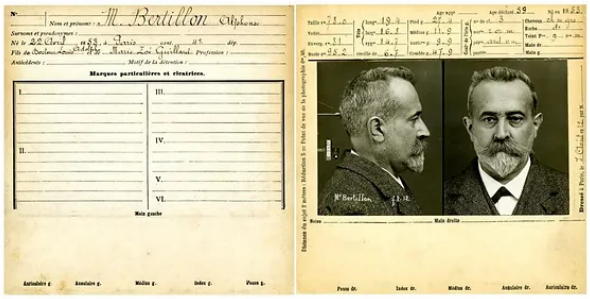
CSE XXX: Digital Forensics

(Course Outline and Syllabus)

IBA SMCS

School of Mathematics and Computer Science

Fall 2023



Institute of Business Administration

School of Mathematics and Computer Science

CSE XXX: Digital Forensics

"The evidence never lies" – **Alphonse Bertillon**

1 Logistics

Course:	CSE XXX: Digital Forensics
Class timings:	Mon/Wed 2:30pm to 3:45pm
Class room:	TBD
Instructor(s):	Faisal Iradat PhD
Email:	f i r a d a t at i b a . e d u . p k
Phone:	YSSSSNRDERD Crack it and win a prize [Hint: Vernam Cypher]
Office:	TR Lab / Room 210, Tabba Building
Office hours:	Thr 1:00 pm to 2:15 pm
LMS:	Digital Forensics (Class:98641) - Spring 2025
TA:	Searching
TA email:	

2 Course Description/Objectives

The Digital Forensics course offers a specialized focus on the analysis, preservation, and examination of digital evidence to uncover cyber incidents. While related courses such as Network Security, Computer Security, and Essentials of Information Security emphasize proactive security measures to protect systems, data, and networks, Digital Forensics delves into post-incident response, working to identify and analyze breaches, cybercrimes, and other malicious activities after they have occurred.

1. Network Security: Primarily focuses on protecting network infrastructure, ensuring secure data transfer, and preventing unauthorized access. Students learn to configure and monitor firewalls, intrusion detection systems, and network protocols to maintain a secure communication environment. In contrast, Digital Forensics emphasizes examining network traffic post-incident to uncover how breaches or unauthorized access occurred.

2. Computer Security: Aims to protect individual devices and systems from malware, unauthorized access, and data breaches, often focusing on encryption, authentication, and access control. Digital Forensics, however, goes beyond protection, training students to investigate

compromised systems, recover deleted or tampered data, and trace malicious activity to understand the attack's origin and methodology.
3. Essentials of Information Security: Offers an overview of fundamental principles like confidentiality, integrity, and availability, along with basic protection techniques across various systems and data types. Digital Forensics provides a more specialized application, concentrating on gathering digital evidence and maintaining the chain of custody in legal or organizational investigations. In essence, this Digital Forensics course is designed for students interested in the investigative side of cybersecurity, equipping them with the tools and methodologies to collect and analyze evidence, trace incidents, and present findings in legal or organizational contexts. It complements the skills gained in security-focused courses by adding a crucial forensic investigation layer, preparing students for roles in cybersecurity that require a deeper understanding of incident response and digital evidence handling.

3 Program Learning Outcomes/Graduate Attributes

Graduate attributes (program learning outcomes - PLO's) taken from `https://www.seoulaccord.org/document.php?id=79`.

PLO-1. **Academic Education**

[Educational depth and breadth]

Completion of an accredited program of study designed to prepare graduates as computing professionals

PLO-2. **Knowledge for Solving Computing Problems**

[Breadth and depth of education and type of knowledge, both theoretical and practical]

Apply knowledge of computing fundamentals, knowledge of a computing specialization, and mathematics, science, and domain knowledge appropriate for the computing specialization to the abstraction and conceptualization of computing models from defined problems and requirements

PLO-3. **Problem Analysis**

[Complexity of analysis]

Identify, formulate, research literature, and solve complex computing problems reaching substantiated conclusions using fundamental principles of mathematics, computing sciences, and relevant domain disciplines

PLO-4. **Design / Development of Solutions**

[Breadth and uniqueness of computing problems, i.e., the extent to which problems are original and to which solutions have previously been identified or codified]

Design and evaluate solutions for complex computing problems, and design and evaluate systems, components, or processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal, and environmental considerations

PLO-5. **Modern Tool Usage**

[Level and appropriateness of the tool to the type of activities performed]

Create, select, adapt and apply appropriate techniques, resources, and modern computing tools to complex computing activities, with an understanding of the limitations

PLO-6. **Individual and Team Work**

[Role in, and diversity of, the team]

Function effectively as an individual and as a member or leader in diverse teams and in multi-disciplinary settings

PLO-7. **Communication**

[Level of communication according to type of activities performed]

Communicate effectively with the computing community and with society at large about complex computing activities by being able to comprehend and write effective reports, design documentation, make effective presentations, and give and understand clear instructions

PLO-8. **Computing Professionalism and Society**

[No differentiation in this characteristic except level of practice]

Understand and assess societal, health, safety, legal, and cultural issues within local and global contexts, and the consequential responsibilities relevant to professional computing practice

PLO-9. **Ethics**

[No differentiation in this characteristic except level of practice]

Understand and commit to professional ethics, responsibilities, and norms of professional computing practice

PLO-10. **Life-long Learning**

[No differentiation in this characteristic except level of practice]

Recognize the need, and have the ability, to engage in independent learning for continual development as a computing professional

4 Course Learning Outcomes

The cognition levels are based on Bloom's revised taxonomy.[1]

Course Learning Outcome		
CLO	**Description**	**Cognition**
CLO-1	**Knowledge**: Demonstrate a thorough understanding of digital forensics principles, including evidence handling, preservation, and analysis.	
CLO-2	**Analyze**: Analyze digital evidence from diverse platforms, such as file systems, networks, mobile devices, and cloud environments.	
CLO-3	**Solve**: Develop effective strategies for solving forensic challenges, including data recovery, malware analysis, and anti-forensics countermeasures.	

[1] Anderson, Lorin W.; Krathwohl, David R., eds. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Allyn and Bacon

4.1 CLO's to PLO's Mapping

An example CLO-PLO mapping.

	PLO-2	PLO-3
CLO-1	✓	
CLO-2	✓	
CLO-3		✓

5 Format and Procedures:

The LMS site will be used to share the syllabus, give out assignments, and to share other course resources.

The University's standard policies on attendance, inclusivity, office hours, and academic integrity apply in this course. These are described in later sections below.

6 Course Requirements

- Class participation policy: Background reading for next session and active participation in class discussions.
- **Textbooks:**
  - There are no textbooks, however, students may refer to the following and my lecture slides.
- **References:**
  - *Digital Forensics and Incident Response: Incident Detection and Response by Gerard Johansen (2nd Edition, 2022).*
  - *Practical Forensic Imaging by Bruce Nikkel (2nd Edition, 2023).*

7 Grading Procedures

Grades will be computed as follows.

Tentative	
Activities / Homework	30%
Project	20%
Midterm	20%
Final	30%

- Each topic includes an activity.
- There will be a research project in the field of Digital Forensics. Projects will typically be done in groups of 3-4 students. Students will have the option to either write a survey paper or work on a practical project.

Start thinking of ideas early – it's never too soon to get started! And be ambitious, the goal is to get something to the point where it is a summer school publication, or a stepping stone toward a conference-quality paper, like the ones you are given to read.

8 Makeup Policy

There will be no makeup exams in general. Makeup exams may be given to students under extreme circumstances, such as hospitalization, serious injury, death in the family, etc, with prior notification and valid documents. Subject to approval from Department and Examinations.

9 Attendance Policy

IBA attendance policy applies.

10 Academic Integrity

Each student in this course is expected to abide by the IBA Code of Conduct. Scholastic dishonesty shall be considered a serious violation of these rules and regulations and is subject to strict disciplinary action as prescribed by IBA regulations and policies. Scholastic dishonesty includes, but is not limited to, cheating on exams, plagiarism on assignments, and collusion.

Kindly refer to `https://examination.iba.edu.pk/CheatingPlagiarism.php` for more details.

- **PLAGIARISM:** Plagiarism is the act of taking the work created by another person or entity and presenting it as ones own for the purpose of personal gain or of obtaining academic credit. Plagiarism includes the submission of or incorporation of the work of others without acknowledging its provenance or giving due credit according to established academic practices. This includes the submission of material that has been appropriated, bought, received as a gift, downloaded, or obtained by any other means. Students must not, unless they have been granted permission from all faculty members concerned, submit the same assignment or project for academic credit for different courses.
- **CHEATING:** The term cheating shall refer to the use of or obtaining of unauthorized in- formation in order to obtain personal benefit or academic credit.
- **COLLUSION:** Collusion is the act of providing unauthorized assistance to one or more person or of not taking the appropriate precautions against doing so.

  Any student violating academic integrity a second time in this course will receive a failing grade for the course, and additional disciplinary sanctions may be administered.
- **SHARING CREDENTIALS:** It has been observed that some students share their credentials (log in id's and passwords) of LMS, portal, email, etc., with with other students. These credentials are private and confidential and not to be shared with anyone. Any violation will be considered as aiding in plagiarism/collusion/cheating and appropriate action might be taken against such students.

11 Office hours

I will be available in my office on Thr from 1:00 pm to 2:15 pm for any queries / questions. Please schedule an appointment.

12 Weekly breakdown of classes

Week 1: Introduction to Digital Forensics
Overview of digital forensics in cybersecurity. Key concepts such as evidence types, preservation, and legal considerations.
Week 2: Legal and Ethical Considerations
Understanding digital evidence laws, chain of custody, and legal compliance. Ethical considerations in forensic investigation.
Week 3: File Systems and Data Storage
In-depth understanding of file systems (NTFS, FAT, ext4).
Week 4: Data Acquisition and Imaging
Methods and tools for data acquisition and disk imaging.
Week 5: Volatile Memory and RAM Forensics
Techniques for RAM analysis, capturing volatile data.
Week 6: File Carving and Data Recovery
Techniques to recover deleted files and hidden data
Week 7: Network Forensics and Intrusion Detection
Basics of network traffic analysis and intrusion detection.
Week 8: Mobile Device Forensics
Challenges in mobile device data collection and analysis.
Week 9: Malware Forensics
Techniques for identifying and analyzing malware on compromised devices
Week 10: Cloud Forensics
Cloud-specific challenges and methodologies for forensics in cloud environments.
Week 11: Email and Social Media Forensics
Investigating digital communication platforms for evidence collection.
Week 12: Forensic Report Writing and Presentation
Writing forensic reports, presenting findings, and defending in legal settings.
Week 13: Advanced Topics and Research Methodology in Digital Forensics
Anti-forensics, AI in forensics, and new trends in digital investigation.
Week 14: Research in Digital Forensics
Students finalize and present a research paper exploring a current issue in digital forensics, simulating a real-world forensic analysis research study. Peer review and presentations to simulate academic conference-style sharing of research insights. .