

Credits: 4

## Digital Forensics and Incident Response

Year: 1

Part: II

### Course Objectives

This course provides a comprehensive overview of digital forensics and incident response, focusing on the methodologies, tools, and techniques used to investigate and respond to cybersecurity incidents. Students will learn to systematically gather, analyze, and preserve digital evidence for legal admissibility and effectively manage and mitigate security breaches. The course integrates theoretical concepts with practical exercises to equip students with the skills to conduct thorough forensic investigations and implement robust incident response strategies.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
<ul style="list-style-type: none"><li>• Understand the fundamentals of digital forensics and incident</li><li>• Understand the essential legal aspects related to digital forensics</li><li>• Grasp a basic understanding of Nepal's legal provisions related to digital forensics</li><li>• Build familiarity with the basics of incident response Frameworks.</li><li>• Apply NIST and SANS Framework for Incident</li></ul>	<b>1. Introduction</b> <ul style="list-style-type: none"><li>1.1. Introduction to digital forensics</li><li>1.2. Digital evidence and legal admissibility</li><li>1.3. Burden of proof</li><li>1.4. Chain of custody of digital evidence</li><li>1.5. Provisions related to digital evidence in the Evidence Act of Nepal.</li><li>1.6. Introduction to Incident Response, phases of incident response.</li><li>1.7. Reporting</li><li>1.8. Common incident response frameworks NIST, SANS</li><li>1.9. Incident response plan, Incident response team</li></ul>	12	<ul style="list-style-type: none"><li>• Lectures: Overview of foundational concepts related to digital forensics and incident response.</li><li>• Lectures: Overview of global and Nepal's law associated with Digital Evidence, Chain of custody, and legal admissibility</li><li>• Interactive Discussion: Nepal's evidence law and its provisions related to digital evidence</li><li>• Case Studies: Application</li></ul>

Response.			of SANS and NIST Framework for Incident Response
<ul style="list-style-type: none"> <li>• Understanding storage and file system layout</li> <li>• Learning forensic imaging and acquisition techniques</li> <li>• Apply tools and techniques to recover deleted data</li> <li>• Application of standard tools for disk-based forensics analysis</li> </ul>	<b>2. Disk and Filesystem Forensics</b> <ol style="list-style-type: none"> <li>2.1. Understanding storage devices and filesystem layout</li> <li>2.2. Forensic imaging and acquisition techniques</li> <li>2.3. Maintaining the integrity of media under analysis</li> <li>2.4. Locating and recovering deleted data</li> <li>2.5. Usage of common tools like Autopsy, SleuthKit, FTK</li> </ol>	8	<ul style="list-style-type: none"> <li>• Lectures: Overview of storage layout for filesystem</li> <li>• Hands-on: Basics of Digital Forensics Image acquisition and analysis</li> <li>• Interactive discussion: Relevant disk-based forensics cases</li> </ul>
<ul style="list-style-type: none"> <li>• Understanding the importance of memory contents, their acquisition, and analysis in digital forensics</li> <li>• Apply tools to analyze memory contents and equip to infer the output of the tools used for analysis</li> </ul>	<b>3. Memory Forensics</b> <ol style="list-style-type: none"> <li>3.1. Analyzing memory (RAM) contents</li> <li>3.2. Importance of analyzing memory contents in digital forensics</li> <li>3.3. Memory dump analysis with Volatility and Rendell</li> </ol>	8	<ul style="list-style-type: none"> <li>• Lectures: Overview of importance, acquisition, and analysis of memory contents in digital forensics</li> <li>• Hands-on: Using tools to capture and analyze memory contents in digital forensics</li> </ul>
<ul style="list-style-type: none"> <li>• Understanding the usage of various network data-capturing tools in different scenarios</li> <li>• Differentiate IPS and IDS and understand their role</li> </ul>	<b>4. Network Forensics</b> <ol style="list-style-type: none"> <li>4.1. Network traffic capture and analysis with PCAP, Wireshark</li> <li>4.2. IDS, IPS systems for forensic analysis</li> <li>4.3. Detecting network attacks and traces and documenting for legal admissibility</li> </ol>	6	<ul style="list-style-type: none"> <li>• Lectures: Overview of capturing, collection, and analysis of network forensics artifacts</li> <li>• Interactive discussion: IPS vs. IDS and their</li> </ul>

<ul style="list-style-type: none"> <li>in forensic analysis</li> <li>• Understand documenting requirements of network forensics regarding legal admissibility</li> </ul>			suitability in forensic analysis <ul style="list-style-type: none"> <li>• Hands-on: Using Wireshark to capture and analyze memory forensics-related artifacts</li> </ul>
<ul style="list-style-type: none"> <li>• Understanding the basic concepts and challenges of mobile data acquisition techniques</li> <li>• Exploring the value mobile forensics adds to forensic investigation</li> <li>• Evaluate the capability of tools regarding the acquisition, analysis, and usage of data obtained in mobile forensics</li> </ul>	<b>5. Mobile Device Forensics</b> <ul style="list-style-type: none"> <li>5.1. Mobile device acquisition techniques (iOS, Android)</li> <li>5.2. Recovering SMS, call logs, GPS data, application data</li> <li>5.3. Usage of tools like Andriller, Cellebrite, Oxygen Forensics suite</li> </ul>	8	<ul style="list-style-type: none"> <li>• Lectures: Overview of the importance of mobile data acquisition, analysis in digital forensics</li> <li>• Interactive discussion: Usage of mobile devices and usefulness of forensic data acquired from mobile devices</li> <li>• Lectures and Demonstrations: Mobile forensics tools and analysis of data acquired using these tools</li> </ul>
<ul style="list-style-type: none"> <li>• Understand the changing landscape of data centers to cloud infrastructure</li> <li>• Understand the challenges in the cloud in the acquisition and analysis of digital artifacts.</li> <li>• Explore legal constraints in acquiring digital forensics artifacts in a</li> </ul>	<b>6. Cloud Forensics</b> <ul style="list-style-type: none"> <li>6.1. Introduction to digital forensics in the cloud environment.</li> <li>6.2. Challenges in analyzing digital evidence in the cloud environment</li> <li>6.3. Common practices and tools for digital forensic analysis in aws, azure, and GCP.</li> </ul>	6	<ul style="list-style-type: none"> <li>• Lectures: Changing data infrastructure, landscape to cloud, and challenges it poses on digital forensics.</li> <li>• Presentation: Legal and privacy constraints in collecting digital forensics artifacts in the cloud.</li> <li>• Group discussions: Common practices and</li> </ul>

cloud computing environment. <ul style="list-style-type: none"> <li>Understand standard practices and tools for digital forensics in major cloud providers</li> </ul>			tools for digital forensics for the cloud
<ul style="list-style-type: none"> <li>Understand the importance of malware analysis in digital forensics</li> <li>Differentiate various approaches utilized for the analysis</li> <li>Explore multiple tools used for dynamic analysis</li> </ul>	<b>7. Malware analysis</b> 7.1. Introduction and importance of malware analysis in digital forensics 7.2. Static, dynamic, and hybrid analysis 7.3. Using tools like Cuckoo Sandbox, Ghidra, and Volatility for malware analysis	6	<ul style="list-style-type: none"> <li>Lectures: Overview, Importance of malware analysis in digital forensics</li> <li>Presentation: Various approaches to malware analysis and</li> <li>Group Discussion: usefulness of information obtained from static, dynamic, and hybrid analysis.</li> <li>Hands-on: sample analysis of malware using static and dynamic malware analysis tools</li> </ul>
<ul style="list-style-type: none"> <li>Understand various types of logs</li> <li>Evaluate the possibility of a correlation between logs and other system information for forensics analysis</li> <li>Understand practices</li> </ul>	<b>8. Log Analysis</b> 8.1. Analyzing system, application, and access logs 8.2. Correlating logs with other system information for digital forensics 8.3. Storing and retrieving logs for legal admissibility 8.4. Common log formats, logging applications,	6	<ul style="list-style-type: none"> <li>Lectures: Overview of collection, analysis, retrieval, and storing of logs from various log sources</li> <li>Hands-on: develop a SIEM system based on open-source tools</li> </ul>

regarding storage and retrieval of logs for legal and admissibility. <ul style="list-style-type: none"> <li>Analyze standard log formats, applications, and tools</li> </ul>	and tools		<ul style="list-style-type: none"> <li>Group discussion: legal aspects of storage and retrieval of log data</li> <li>Presentation: Common formats, tools configuration for logging</li> </ul>
--	-----------	--	---

### Practical:

Students will engage in practical hands-on using open source tools for chapters 2, 3, 4, 7, and 8 and submit their findings as assignments. Practical for Chapter 5 will depend on the availability of tools.

### Evaluation Schemes

#### a. Internal Evaluation

Type	Weightage
Minor tests	70%
Assignments	30%

#### b. Final Examination

The questions will cover all chapters of the syllabus. The evaluation scheme will be as indicated in the table.

Chapter	Hours	Marks Distribution*
1	12	12

2	8	8
3	8	8
4	6	6
5	8	8
6	6	6
7	6	6
8	6	6
Total	60	60

\*There may be a minor deviation in mark distribution.

## References

1. Johansen, G. (2022). *Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response*. Packt Publishing Ltd.
2. Oettinger, W. (2022). *Learn Computer Forensics–2nd edition: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence*. Packt Publishing Ltd.
3. Luttgens, J. T., Pepe, M., & Mandia, K. (2014). *Incident response & computer forensics*. McGraw-Hill Education Group.
4. Boddington, R. (2016). *Practical digital forensics*. Packt Publishing Ltd.