27-05-2026 02:36:05 PM

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Programme Name/s	**: Artificial Intelligence/ Cloud Computing and Big Data/ Computer Technology/ Computer Engineering/ Computer Software Technology/ Computer Science & Engineering/ Data Sciences/ Computer Hardware & Maintenance/ Information Technology/ Computer Science & Information Technology/ Computer Science**
Programme Code	**: AI/ BD/ CM/ CO/ CST/ CW/ DS/ HA/ IF/ IH/ SE**
Semester	**: Sixth**
Course Title	**: DIGITAL FORENSIC AND HACKING TECHNIQUES**
Course Code	**: 316315**

I. RATIONALE

Digital forensics helps analyze and preserve digital evidence to investigate cybercrimes, using specialized tools and procedures. Digital forensic experts play a pivotal role in defending against and responding to cyber threats. Hacking teaches how to identify and fix system vulnerabilities before malicious hackers exploit them. Ethical hacking is a legal way to secure information systems. This course prepares students to safeguard systems from cyber threats and malicious users.

II. INDUSTRY / EMPLOYER EXPECTED OUTCOME

The aim of this course is to help the students to attain the following industry identified outcomes through various teaching learning experiences:

- Apply Digital Forensic methodology to carry out investigations and penetration tests.

III. COURSE LEVEL LEARNING OUTCOMES (COS)

Students will be able to achieve & demonstrate the following COs on completion of course based learning

- CO1 - Explain digital forensics investigation process.
- CO2 - Apply various Digital Forensic Investigation Models.
- CO3 - Apply digital Evidence collecting and handling techniques.
- CO4 - Identify various types of cyber attacks.
- CO5 - Apply Tools and Techniques for Ethical Hacking.

IV. TEACHING-LEARNING & ASSESSMENT SCHEME

Course Code	Course Title	Abbr	Course Category/s	Learning Scheme					Credits	Assessment Scheme											
				Actual Contact Hrs./Week			SLH	NLH		Paper Duration	Theory				Based on LL & TL				Based on SL		Total Marks
															Practical						
				CL	TL	LL					FA-TH	SA-TH	Total		FA-PR		SA-PR		SLA		
											Max	Max	Max	Min	Max	Min	Max	Min	Max	Min	
316315	DIGITAL FORENSIC AND HACKING TECHNIQUES	DFH	DSE	3	-	2	1	6	3	3	30	70	100	40	25	10	25#	10	25	10	175

Total IKS Hrs for Sem. : 0 Hrs
Abbreviations: CL- ClassRoom Learning , TL- Tutorial Learning, LL-Laboratory Learning, SLH-Self Learning Hours, NLH-Notional Learning Hours, FA - Formative Assessment, SA -Summative assessment, IKS - Indian Knowledge System, SLA - Self Learning Assessment
Legends: @ Internal Assessment, # External Assessment, *# On Line Examination , @$ Internal Online Examination
Note :

1. FA-TH represents average of two class tests of 30 marks each conducted during the semester.
2. If candidate is not securing minimum passing marks in FA-PR of any course then the candidate shall be declared as "Detained" in that semester.
3. If candidate is not securing minimum passing marks in SLA of any course then the candidate shall be declared as fail and will have to repeat and resubmit SLA work.
4. Notional Learning hours for the semester are (CL+LL+TL+SL)hrs.* 15 Weeks
5. 1 credit is equivalent to 30 Notional hrs.
6. * Self learning hours shall not be reflected in the Time Table.
7. * Self learning includes micro project / assignment / other activities.

V. THEORY LEARNING OUTCOMES AND ALIGNED COURSE CONTENT

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
1	TLO 1.1 Explain rules of Digital Forensics. TLO 1.2 Describe the given type of Digital Forensics. TLO 1.3 Explain Digital Forensics process.	**Unit - I Digital Forensics** 1.1 Overview of Digital forensics, Rules of digital forensic, Digital forensics investigation and its goal 1.2 Introduction to Cyber Crime and attack 1.3 Types of Digital Forensics- Computer Forensics, Network Forensics, Cloud Forensics, Mobile Forensics and Database Forensics 1.4 Digital Forensics process 1.5 Areas of Applications of computer forensics- Public Sector, Private Sector	Lecture using Chalk-Board Flipped Classroom Demonstration
2	TLO 2.1 Describe the given model of digital forensic investigation. TLO 2.2 Explain General ethical norms for investigators.	**Unit - II Digital Forensic Investigation Models** 2.1 Models of Digital Forensic Investigation: DFRWS Investigative Model, Abstract Digital Forensics Model (ADFM), Integrated Digital Investigation Process (IDIP), End-to-End digital investigation process (EEDIP), An extended model for cybercrime investigation, UML modeling of digital forensic process model (UMDFPM) 2.2 Challenges in Digital Forensics: Encryption, Volume of Data, Anti-Forensics Techniques, Legal and Ethical Issues, Emerging Technologies 2.3 Legal and Ethical Considerations in Digital Forensics: General ethical norms for investigators, Unethical norms for investigation	Lecture Using Chalk-Board Flipped Classroom Demonstration

27-05-2026 02:36:05 PM

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
3	TLO 3.1 Describe the given rule for digital evidence. TLO 3.2 Explain the given type of digital evidence. TLO 3.3 Describe the evidence handling procedure. TLO 3.4 Explain various challenges in evidence handling. TLO 3.5 Explain Hashing and hashing algorithms.	**Unit - III Digital Evidences** 3.1 Crime Scenes and Collecting Evidence-Removable Media, Cell Phones, Order of Volatility 3.2 Documenting the Scene-Photography, Notes 3.3 Chain of Custody-Marking Evidence 3.4 Cloning-Purpose of Cloning, The Cloning Process, Forensically Clean Media, Forensic Image Formats, Risks and Challenges 3.5 Live System versus Dead System-Live Acquisition Concerns, Advantage of Live Collection, Principles of Live Collection, Conducting and Documenting a Live Collection 3.6 Hashing-Types of Hashing Algorithms, Hashing Example, Uses of Hashing	Lecture Using Chalk-Board Flipped Classroom Demonstration
4	TLO 4.1 Explain ethical hacking principles. TLO 4.2 Explain the symptoms of the given type of attack on computer system. TLO 4.3 Explain the process of ethical hacking for the given situation.	**Unit - IV Basics of Hacking** 4.1 Ethical Hacking: How Hackers Beget Ethical Hackers, Defining hacker, Malicious users 4.2 Understanding the need to hack your own systems 4.3 Understanding the dangers your systems face: Nontechnical attacks, Network-infrastructure attacks, Operating-system attacks, Application and other specialized attacks 4.4 Obeying the Ethical hacking Principles: Working ethically, Respecting privacy, Not crashing your systems 4.5 Ethical hacking Process: Formulating plan, Selecting tools, Executing the plan, Evaluating results	Lecture Using Chalk-Board Flipped Classroom Demonstration
5	TLO 5.1 Define Ethical Hacking and Penetration Testing. TLO 5.2 Describe Phases of Ethical Hacking. TLO 5.3 Describe the characteristics of the given type of Network Infrastructure Vulnerability. TLO 5.4 Explain the given social engineering attack.	**Unit - V Hacking Techniques** 5.1 Overview of Ethical Hacking and Penetration Testing 5.2 Phases of Ethical Hacking: Reconnaissance, Scanning, Exploitation, Post-Exploitation 5.3 Network Hacking: Network Infrastructure Vulnerabilities, Scanning-Ports, Ping swiping, Scanning SNMP, Grabbing Banners, Analysing Network Data and Network Analyzer, MAC-daddy attack 5.4 Introduction to Social Engineering, Types of social engineering attacks- Phishing, Watering hole attacks, Physical social engineering	Lecture Using Chalk-Board Flipped Classroom Demonstration

VI. LABORATORY LEARNING OUTCOME AND ALIGNED PRACTICAL / TUTORIAL EXPERIENCES.

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 1.1 Monitor CPU and Memory Utilization.	1	* a. Monitor CPU Utilization and Memory Utilization for detecting unauthorized process activations. (Hint: More CPU utilization as compared to Memory is an indicator of anomaly) b. Create complete memory dump using windows c. Read Memory Dump Using Windows Driver toolkit	2	CO1

27-05-2026 02:36:05 PM

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 2.1 Investigate the given Digital Forensic scenario and prepare report.	2	*Study the DFRWS Investigative Model and apply it in a simulated digital forensic investigation (Consider digital forensic scenario like a case involving a potential data breach or unauthorized access to a computer system). a. Investigate according to phases of model. b. Prepare report detailing the steps taken during the investigation.	2	CO2
LLO 3.1 Analyze the given real world case and prepare the report based on the ethical issues arose.	3	Analyze a real-world or hypothetical case where ethical issues arose in a digital forensics investigation Task to be performed by students: a. Select a real-world case of a digital forensics investigation where ethical issues played a significant role (e.g., the case of the FBI's investigation of the San Bernardino iPhone, The Ashley Madison Hack (2015)) b. Analyze the case based on following points: • Ethical issues involved in the investigation • Situation handling procedure followed by Investigator • Does the investigation based on professional ethical norms • Or what Ethical guidelines should be followed c. Prepare Report on ethical issues, their impact on the investigation and a conclusion on how the situation could have been managed ethically	2	CO2
LLO 4.1 Investigate data in a cloud environment focusing on issues like data privacy and security breaches.	4	*Investigate data in a cloud environment, focusing on issues like data privacy and security breaches a. Conduct a forensic analysis of cloud storage (e.g., Dropbox, Google Drive) for potential data breaches or misuse b. Retrieve access logs and analyze activities that suggest unauthorized access or tampering (Hint: Use Cloud storage APIs, AWS CloudTrail, Google Cloud Platform logs.)	2	CO2
LLO 5.1 Run given commands on Windows/Linux OS to collect live data.	5	Collect live data on Windows\Linux: a. Create a response toolkit on windows having utility cmd.exe, PsLoggedOn, netstat b. Establish TCP connection between forensic workstation and the target system using netcat c. Run trusted cmd.exe, identify logged users and remote access users, Record creation, access times and all the modifications made to the files	2	CO3

27-05-2026 02:36:05 PM

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 6.1 Create Forensic Images with any Imager Tool.	6	Create Forensic Images with any Imager Tool like Exterro FTK Imager	2	CO3
LLO 7.1 Perform Hashing to verify the authenticity of digital evidence.	7	*Perform Hashing to verify the authenticity of digital evidence a. Create a file and generate a hash (MD5, SHA-256) using hashing tools b. Alter the file slightly and generate the hash again to observe how the hash changes (Use HashCalc, MD5 & SHA Checksum Utility, Python's hashlib or any such tool)	2	CO3
LLO 8.1 Recover deleted or corrupted files from a storage device.	8	Recover deleted or corrupted files from a storage device and perform file carving (e.g., photos, documents) using any data recovery tool	2	CO3
LLO 9.1 Read and Interpret Operating Systems logs on Windows file system.	9	*Read and Interpret Operating Systems logs on Windows file system Hint: Check whether the log gives information about file systems. Any such entry indicates some malicious activity	2	CO4
LLO 10.1 Configure Kali Linux.	10	Install Kali Linux Hint: Students can install Kali Linux on VMware Workstation/Virtual Box	2	CO4
LLO 11.1 Use nmap utility for scanning.	11	*Use nmap utility to perform following tasks: a. Install Nmap on Linux or Windows OS b. Detect which devices are live on your local network. Identify the services and their versions running on a particular host c. Detect the operating system of a target host d. Perform a port scan on a specific set of ports e. Perform an aggressive scan to gather as much information as possible about a target host f. Use Nmap's scripting engine to search for vulnerabilities in a target system	2	CO4
LLO 12.1 Establish DoS attack using TCP/ICMP flooding.	12	Establish DoS attack using TCP/ICMP flooding: a. Ping continuously a particular machine at a time from different machines and observe the machine behavior on Network b. Write shell script for continuously flooding a Machine with ping and observe the machine behavior on Network	2	CO4
LLO 13.1 Use Wireshark tool to analyze network traffic.	13	* Capture Network traffic using Wireshark tool a. Install Wireshark tool on Windows/Kali Linux b. Use Wireshark tool to capture network traffic and to understand three-way handshaking concept/Analyze the packet c. Examine HTTP, FTP, or other protocols for evidence of cybercrime	2	CO5

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 14.1 Use any information gathering tool to collect information of IP addresses, domain names and emails.	14	Collect information of IP addresses, domain names and emails using any information gathering tool like Recon-ng	2	CO5
LLO 15.1 Simulate phishing attacks using Social-Engineer Toolkit.	15	*Use Social-Engineer Toolkit (SET) tool for Simulating phishing attacks to test human vulnerabilities	2	CO5

Note : Out of above suggestive LLOs -

- '*' Marked Practicals (LLOs) Are mandatory.
- Minimum 80% of above list of lab experiment are to be performed.
- Judicial mix of LLOs are to be performed to achieve desired outcomes.

VII. SUGGESTED MICRO PROJECT / ASSIGNMENT/ ACTIVITIES FOR SPECIFIC LEARNING / SKILLS DEVELOPMENT (SELF LEARNING)

Activity

- Find Job opportunities in Government sector in Digital Forensics and Ethical Hacking. Prepare detailed report on any Job Role. (e.g. Forensic Computer Analyst, Digital Forensics Experts, Forensic Investigator, Security Auditor)
- Arrange Visit to cyber cell or Digital Forensic Laboratory. OR Organize Expert Lecture of Cyber Expert.

Assignment

- Simulate a penetration testing environment and identify vulnerabilities in a network. Write a detailed penetration testing report that outlines vulnerabilities found, how they were exploited, and recommended mitigation strategies.
- Capture and analyze network traffic to detect malicious activities. Write a report detailing the network traffic analysis and identify malicious behavior. Also write how network forensics can help identify cyber-attacks and the importance of packet analysis.

Note

- Teacher should give more such assignments covering all COs.

Micro project

- Study any Trojan attack. Identify the Trojan attack:
  i. State the way trojan got installed on particular Machine.
  ii. State the effects of the Trojan.
  iii. Elaborate/Mention/State protection/Blocking mechanism for this specific Trojan, example specification of any anti-threats platform which filters the Trojan.
- Study Credit card fraud as an identity threat. Identify:
  i. Use of digital media in carrying out fraud.
  ii. Vulnerability Exploited.
  iii. Effect of fraud.
  iv. Protection/Precaution to be taken against such frauds.
- Study any case of forgery /falsification crime case solved using digital forensics:
  i. Identify the model used for Digital Investigation.
  ii. Was investigation done ethically or unethically?
  iii. Where does digital evidence found for crime establishment?
  iv. State the punishment meted.
- Study any case of fake profiling. Identify
  i. The way digital forensics was used in detecting the fraud.
  ii. Where was digital evidence located?
  iii. Effects.

27-05-2026 02:36:05 PM

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Other

- Students are encouraged to register themselves in various MOOCs such as NPTEL/Infosys Springboard/udemy/any other online platform to enhance their learning.

Note :

- Above is just a suggestive list of microprojects and assignments; faculty must prepare their own bank of microprojects, assignments, and activities in a similar way.
- The faculty must allocate judicial mix of tasks, considering the weaknesses and / strengths of the student in acquiring the desired skills.
- If a microproject is assigned, it is expected to be completed as a group activity.
- SLA marks shall be awarded as per the continuous assessment record.
- For courses with no SLA component the list of suggestive microprojects / assignments/ activities are optional, faculty may encourage students to perform these tasks for enhanced learning experiences.
- If the course does not have associated SLA component, above suggestive listings is applicable to Tutorials and maybe considered for FA-PR evaluations.

VIII. LABORATORY EQUIPMENT / INSTRUMENTS / TOOLS / SOFTWARE REQUIRED

Sr.No	Equipment Name with Broad Specifications	Relevant LLO Number
1	Computer with Kali Linux Operating system/ Kali Linux/any open source OS installed on Virtual Box/VMware workstation	4,5,6,7,8,10,11,13,14
2	Digital Forensic and Hacking Freeware tools mentioned in practicals.	6,7,8,9,11,13,14,15
3	Computer system with basic configuration	All

IX. SUGGESTED WEIGHTAGE TO LEARNING EFFORTS & ASSESSMENT PURPOSE (Specification Table)

Sr.No	Unit	Unit Title	Aligned COs	Learning Hours	R-Level	U-Level	A-Level	Total Marks
1	I	Digital Forensics	CO1	8	6	4	2	12
2	II	Digital Forensic Investigation Models	CO2	8	4	6	2	12
3	III	Digital Evidences	CO3	9	6	8	2	16
4	IV	Basics of Hacking	CO4	10	4	8	2	14
5	V	Hacking Techniques	CO5	10	4	8	4	16
Grand Total				**45**	**24**	**34**	**12**	**70**

X. ASSESSMENT METHODOLOGIES/TOOLS

Formative assessment (Assessment for Learning)

- Laboratory Performance, Unit Tests, Midterm Exam, Term Work, Seminar/ Presentations.
- Continuous assessment based on process and product related performance indicators.
- Each practical will be assessed considering 60% weightage to process and 40% weightage to product.

Summative Assessment (Assessment of Learning)

- End Semester Exam, Practical exam, viva voce.

XI. SUGGESTED COS - POS MATRIX FORM

27-05-2026 02:36:05 PM

DIGITAL FORENSIC AND HACKING TECHNIQUES **Course Code : 316315**

Course Outcomes (COs)	Programme Outcomes (POs)							Programme Specific Outcomes* (PSOs)		
	PO-1 Basic and Discipline Specific Knowledge	PO-2 Problem Analysis	PO-3 Design/ Development of Solutions	PO-4 Engineering Tools	PO-5 Engineering Practices for Society, Sustainability and Environment	PO-6 Project Management	PO-7 Life Long Learning	PSO-1	PSO-2	PSO-3
CO1	2	2	1	-	1	-	-			
CO2	2	2	2	-	2	1	1			
CO3	2	3	3	2	2	1	2			
CO4	2	3	2	2	2	2	2			
CO5	1	2	2	3	2	2	2			

Legends :- High:03, Medium:02,Low:01, No Mapping: -
*PSOs are to be formulated at institute level

XII. SUGGESTED LEARNING MATERIALS / BOOKS

Sr.No	Author	Title	Publisher with ISBN Number
1	Pachghare V. K.	Cryptography and Information Security	PHI Learning Pvt. Ltd, Delhi ISBN-978-93-89347-11-1 ISBN- 978-93-89347-10-4
2	John Sammons	The Basics of Digital Forensic	Elsevier, Netherlands ISBN 978-1-59749-661-2
3	Kevin Beaver CISSP	Hacking for Dummies	Wiley Publishing, New Delhi ISBN: 978-81-265-6554-2
4	Mark D. Spivey CISSP	Practical Hacking Techniques and Countermeasures	Auerbach Publication, Taylor and Francis Group ISBN-13: 978-0-8493-7057-1

XIII . LEARNING WEBSITES & PORTALS

Sr.No	Link / Portal	Description
1	https://resources.infosecinstitute.com/digital-forensics-models/#gref.	Introduction to Digital forensics models
2	https://docs.kali.org/introduction/download-official-kali-linux-images	Download Kali Linux and its installation steps
3	www.openwall.com/passwords/windows-pwdump	Hash Suite-auditing tool for Windows password hashes.
4	https://www.techtarget.com/searchsecurity/tutorial/How-to-use-Social-Engineer-Toolkit	How to use Social-Engineer Toolkit
5	https://www.youtube.com/watch?v=GZMUYqjAS6k	How to make a Forensic Image with FTK Imager
6	https://www.youtube.com/watch?v=qTaOZrDnMzQ	Wireshark Tutorial for Beginners

Note :

- Teachers are requested to check the creative common license status/financial implications of the suggested online educational resources before use by the students