Maharashtra State Board of Technical Education, Mumbai **K2-A (PRACT)**

LABORATORY PRACTICAL PLANNING

Institute Name: K. K. Wagh Polytechnic, Nashik **Date:** 15/12/2025
Academic Year: 2025-26 (EVEN) **Programme:** Information Technology (IF)
Course: Digital Forensic and Hacking Techniques (DFH) **Course Code:** 316315
Semester: Sixth **Scheme:** K **Name of Faculty:** Ms. S. S. Shinde
Class: TYIF-CRAY Batch: A/B/C

• Teaching-Learning & Assessment Scheme:

Course Code	Course Title &Abbr	Course Category	Learning Scheme					Credits	Paper Duration (Hrs.)	Assessment Scheme										
			Actual Contact Hrs/Week			SLH	NLH			Theory				Based on LL & TSL Practical				Based on SL		Total Marks
			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	3	-	2	1	6	3	3	30	70	100	40	25	10	25#	10	25	10	175

Abbreviations: CL- Class Room 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

- **COURSE LEVEL LEARNING OUTCOMES (COS)**
  By learning course Digital Forensic and Hacking Techniques (DFH-316315) Third Year 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.

• COs, Practical Laboratory Learning Outcome (LLOs) and Mapping:

Sr. No	LLO	Practical Title	Planned Date	Performance Date	Remarks	Related self-learning (if any)
1.	LLO 1.1	* a. Monitor CPU Utilization and Memory Utilization for detecting unauthorized process activations. b. Create complete memory dump using windows c. Read Memory Dump Using Windows Driver toolkit	A- 18/12/25 B- 20/12/25 C- 17/12/25	A- B- C-		
2.	LLO 2.1	* Study the DFRWS Investigative Model and apply it in a simulated digital forensic investigation a. Investigate according to phases of model. b. Prepare report detailing the steps taken during the investigation.	A-01/01/26 B-27/12/25 C-24/12/25	A- B- C-		
3.	LLO 3.1	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				

Institute Name: K. K. Wagh Polytechnic, Nashik **Date:** 15/12/2025
Academic Year: 2025-26 (EVEN) **Programme:** Information Technology (IF)
Course: Digital Forensic and Hacking Techniques (DFH) **Course Code:** 316315
Semester: Sixth **Scheme:** K **Name of Faculty:** Ms. S. S. Shinde
Class: TYIF-CRAY Batch: A/B/C

Sr. No	LLO	Practical Title	Planned Date	Performance Date	Remarks	Related self-learning (if any)
		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	A-08/01/26 B-03/01/26 C-31/12/25	A- B- C-		
4.	LLO 4.1	* 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	A-15/01/26 B-10/01/26 C-07/01/26	A- B- C-		
5.	LLO 6.1	Create Forensic Images with any Imager Tool like Exterro FTK Imager	A-22/01/26 B-17/01/26 C-14/01/26	A- B- C-		
6.	LLO 7.1	* 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.	A-28/01/26 B-24/01/26 C-21/01/26	A- B- C-		
7.	LLO 8.1	Recover deleted or corrupted files from a storage device and perform file carving (e.g., photos, documents) using any data recovery tool	A-05/02/26 B-07/02/26 C-04/02/26	A- B- C-		

Maharashtra State Board of Technical Education, Mumbai

K2-A (PRACT)

LABORATORY PRACTICAL PLANNING

Institute Name: K. K. Wagh Polytechnic, Nashik **Date:** 15/12/2025
Academic Year: 2025-26 (EVEN) **Programme:** Information Technology (IF)
Course: Digital Forensic and Hacking Techniques (DFH) **Course Code:** 316315
Semester: Sixth **Scheme:** K **Name of Faculty:** Ms. S. S. Shinde
Class: TYIF-CRAY Batch: A/B/C

Sr. No	LLO	Practical Title	Planned Date	Performance Date	Remarks	Related self-learning (if any)
8.	LLO 9.1	* Read and Interpret Operating Systems logs on Windows file system	A-12/02/26 B-14/02/26 C-11/02/26	A- B- C-		
9.	LLO 11.1	* 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	A-12/02/26 B-21/02/26 C-18/02/26	A- B- C-		
10.	LLO 13.1	* 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	A- 26/02/26 B- 28/02/26 C- 25/02/26	A- B- C-		
11.	LLO 14.1	Collect information of IP addresses, domain names and emails using any information gathering tool like Recon-ng	A-05/03/26 B- 7/03/2026 C- 11/03/26	A- B- C-		
12.	LLO 15.1	* Use Social-Engineer Toolkit (SET) tool for Simulating phishing attacks to test human vulnerabilities	A-12/03/26 B-14/03/26 C-18/03/26	A- B- C-		

LABORATORY PRACTICAL PLANNING

Institute Name: K. K. Wagh Polytechnic, Nashik **Date:** 15/12/2025
Academic Year: 2025-26 (EVEN) **Programme:** Information Technology (IF)
Course: Digital Forensic and Hacking Techniques (DFH) **Course Code:** 316315
Semester: Sixth **Scheme:** K **Name of Faculty:** Ms. S. S. Shinde
Class: TYIF-CRAY Batch: A/B/C

ASSESSMENT METHODOLOGIES/TOOLS

A. Formative assessment (Assessment for Learning) (FA-TH)

- Continuous assessment based on process and product related performance indicators.
- Each practical will be assessed considering 60% weightage is to process and 40% weightage to product

B. Summative Assessment (Assessment of Learning) (SA-TH)

- End semester Examination, Lab performance, Viva-Voce

C. Suggested micro project / assignment/ activities for specific learning / skills development (self-learning)

1. Arrange Visit to cyber cell or Digital Forensic Laboratory. OR Organize Expert Lecture of Cyber Expert.
2. Complete any one course related to Digital Forensic and Hacking Techniques on MOOCs such as Infosys Springboard/udemy/any other online platform to enhance their learning.

Ms. S. S. Shinde
(Name & Signature of Staff)

Ms. M. S. Karande
(Name & Signature of HOD)