Lesson Plan

Branch: All Branches
Semester: VI **Year: 2022-23**

Course Title: Digital Forensic (HCSC601)	SEE: 4 Hours – Theory
Total Contact Hours: 45 Hours	Duration of SEE: 4 Hrs
SEE Marks: 80 (Theory) + 20 (IA)	
Lesson Plan Author: Prof. Unik Lokhande	Date:
Checked By:	Date:

Syllabus:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	**Prerequisite**	**Computer Hardware**: Motherboard, CPU, Memory: RAM, Hard Disk Drive (HDD), Solid State Drive (SSD), Optical drive **Computer Networks:** Introduction CN Terminology: Router, Gateway, OSI and TCP/IP Layers **Operating Systems:** Role of OS in file management, Memory management utilities, Fundamentals of file systems used in Windows and Linux.	**2**	--
I	**Introduction to Cybercrime and Computer-crime**	**Definition and classification of cybercrimes:** Definition, Hacking, DoS Attacks, Trojan Attacks, Credit Card Frauds, Cyber Terrorism, Cyber Stalking. **Definition and classification of computer crimes:** Computer Viruses, Computer Worms. **Prevention of Cybercrime**: Steps that can be followed to prevent cybercrime, Hackers, Crackers, Phreakers. **Self-learning Topics:** Steps performed by Hacker	**4**	CO1
II	**Introduction to Digital Forensics and Digital Evidence**	**Introduction to Digital Forensics:** Introduction to Digital Forensics and lifecycle, Principles of Digital Forensic. **Introduction to Digital Evidence:** Challenging Aspects of Digital Evidence, Scientific Evidence, Presenting Digital Evidence. **Digital Investigation Process Models:** Physical Model, Staircase Model, Evidence Flow Model. **Self-learning Topics:** Digital Investigation Process Models comparison and its application, Rules of Digital Evidence.	**5**	CO2
III	**Computer Forensics**	**OS File Systems Review:** Windows Systems- FAT32 and NTFS, UNIX File Systems, MAC File Systems **Windows OS Artifacts:** Registry, Event Logs **Memory Forensics :** RAM Forensic Analysis, Creating a RAM Memory Image, Volatility framework, Extracting Information **Computer Forensic Tools:** Need of Computer Forensic Tools, Types of Computer Forensic Tools, Tasks performed by Computer Forensic Tools **Self-learning Topics:** Study of 'The Sleuth Kit' Autopsy tool for Digital Forensics	**7**	CO3

Sr. No.	Module	Detailed Content	Hours	CO Mapping
IV	**Incident Response Management, Live Data Collection and Forensic Duplication**	**Incidence Response Methodology:** Goals of Incident Response, Finding and Hiring IR Talent **IR Process:** Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information. **Live Data Collection:** Live Data Collection on Microsoft Windows, **Forensic Duplication:** Forensic Duplicates as Admissible Evidence, Forensic Duplication Tools: Creating Forensic evidence, Duplicate/Qualified Forensic Duplicate of a Hard Drive. **Self-learning Topics:** Live Data Collection on Unix-Based Systems	**10**	CO4
V	**Forensic Tools and Report Writing**	**Forensic Image Acquisition in Linux:** Acquire an Image with dd Tools, Acquire an Image with Forensic Formats, Preserve Digital Evidence with Cryptography, Image Acquisition over a Network, Acquire Removable Media **Forensic Investigation Report Writing:** Reporting Standards, Report Style and Formatting, Report Content and Organization. **Self-learning Topics:** Case study on Report Writing	**10**	CO5
VI	**Network Forensics and Mobile Forensics**	**Network Forensics:** Sources of Network-Based Evidence, Principles of Internetworking, Internet Protocol Suite, Evidence Acquisition, Analyzing Network Traffic: Packet Flow and Statistical Flow, Network Intrusion Detection and Analysis, Investigation of Routers, Investigation of Firewalls **Mobile Forensics:** Mobile Phone Challenges, Mobile phone evidence extraction process, Android OS Architecture, Android File Systems basics, Types of Investigation, Procedure for Handling an Android Device, Imaging Android USB Mass Storage Devices. **Self-learning Topic:** Elcomsoft iOS Forensic Toolkit, Remo Recover tool for Android Data recovery	**14**	CO6

Course Outcomes (CO):

On successful completion of course learner will be able to:

HSC601.1	Identify and define the classes for various computer and cyber-crimes in the digital world.
HSC601.2	Discuss the need of digital forensics and the role of digital evidence.
HSC601.3	Analyze the role of File systems in computer forensics.
HSC601.4	Demonstrate the incident response methodology with the best practices for incidence response with the application of forensics tools.
HSC601.5	Generate as well as Write the report on application of appropriate computer forensic tools for investigation of any computer security incident.
HSC601.6	Investigate forensic evidence in network and mobile.

CO-PO Mapping: (BL – Blooms Taxonomy, C – Competency, PI – Performance Indicator)

CO	BL	C	PI	PO	Mapping
HSC601.1	1, 2, 3	1.3	1.3.1	PO1	1
		6.1	6.1.1	PO6	1
		8.2	8.2.2	PO8	1
HSC601.2	2, 4	1.3	1.3.1	PO1	1
		2.1 2.3	2.1.1 2.3.1	PO2	2
		4.1	4.1.1	PO4	1
HSC601.3	2	1.3 1.4	1.3.1 1.4.1	PO1	2
		2.1	2.1.2	PO2	1
		4.3	4.3.3	PO4	1
		5.2	5.2.2	PO5	1
HSC601.4	2	1.3 1.4	1.3.1 1.4.1	PO1	2
		2.2	2.2.3	PO2	1
		4.1 4.1 4.3	4.1.1 4.1.3 4.3.1	PO4	3
		5.1 5.3	5.1.1 5.3.1	PO5	2
		10.1	10.1.2	PO10	1
HSC601.5	2	1.3	1.3.1	PO1	1
		2.4	2.4.2	PO2	1
		4.1 4.3	4.1.1 4.1.3 4.3.1 4.3.4	PO4	3
		5.1 5.3	5.1.1 5.3.1	PO5	2
		8.1	8.1.1	PO8	1
		10.1	10.1.2	PO10	1
HSC601.6	4	1.3	1.3.1	PO1	1
		2.2 2.4	2.2.2 2.4.2	PO2	2
		4.1 4.3	4.1.1 4.3.1	PO4	2
		5.1 5.3	5.1.1 5.3.1	PO5	2
		10.1	10.1.2	PO10	1

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
HSC601.1	1					1		1				
HSC601.2	1	2		1								
HSC601.3	2	1		1	1							
HSC601.4	2	1		3	2					1		
HSC601.5	1	1		3	2			1		1		
HSC601.6	1	2		2	2					1		

CO-PSO Mapping:

CO	BL	C	PI	PSO	Mapping
HSC601.1	1, 2, 3	2.2 2.3	2.2.2 2.3.1	PSO2	2
HSC601.3	2, 4	2.4	2.4.1	PSO2	1
HSC601.4	2	2.4	2.4.1	PSO2	2
HSC601.5	2	2.4	2.4.1	PSO2	2
HSC601.6	4	2.2 2.4	2.2.2 2.4.1	PSO2	2

	PSO1	PSO2
HSC601.1	--	2
HSC601.2	--	--
HSC601.3	--	1
HSC601.4	--	1
HSC601.5	--	1
HSC601.6	--	2

CO Measurement Weightages for Tools:

Course Outcomes	***Direct Method (80%)***					***Indirect Method (20%)***
	Unit Tests		Quizzes		End Sem Exam	Course exit survey
	1	2	1	2		
HSC601.1	30%	--	10%	--	60%	100%
HSC601.2	30%	--	10%	--	60%	100%
HSC601.3	30%	--	10%	--	60%	100%
HSC601.4	--	30%	--	10%	60%	100%
HSC601.5	--	30%	--	10%	60%	100%
HSC601.6	--	30%	--	10%	60%	100%

Attainment:

CO HSC601.1:

Direct Method

$$A_{\mathrm{HSC601.1}D} = 0.3 * Test1 + \ 0.1 * Quizzes + 0.6 * SEE_{T}heory$$

Final Attainment:

$$A_{\mathrm{CSC602.1}} = 0.8 * A_{\mathrm{HSC601.1}D} + 0.2 * A_{\mathrm{HSC601.1}I}$$

CO HSC601.2:

Direct Method

$$A_{\mathrm{HSC601.2}D} = 0.3 * Test1 + 0.1 * Quizzes + 0.6 * SEE_{T}heory$$

Final Attainment:

$$A_{\mathrm{HSC601.2}} = 0.8 * A_{\mathrm{HSC601.2}D} + 0.2 * A_{\mathrm{HSC601.2}I}$$

CO HSC601.3:

Direct Method

$$A_{\mathrm{HSC601.3}D} = 0.3 * Test1 + 0.1 * Quizzes + 0.6 * SEE_{T}heory$$

Final Attainment:

$$A_{\mathrm{CSC602.3}} = 0.8 * A_{\mathrm{HSC601.3}D} + 0.2 * A_{\mathrm{HSC601.3}I}$$

CO HSC601.4:
Direct Method

$$A_{\text{HSC601.}4D} = 0.3 * Test2 + 0.1 * Quizzes + 0.6 * SEE_Theory$$

Final Attainment:

$$A_{\text{HSC601.4}} = 0.8 * A_{\text{HSC601.}4D} + 0.2 * A_{\text{HSC601.}4I}$$

CO HSC601.5:
Direct Method

$$A_{\text{HSC601.}5D} = 0.1 * Test2 + 0.1 * Quizzes + 0.6 * SEE_Theory$$

Final Attainment:

$$A_{\text{HSC601.5}} = 0.8 * A_{\text{HSC601.}5D} + 0.2 * A_{\text{HSC601.}5I}$$

CO HSC601.6:
Direct Method

$$A_{\text{HSC601.}6D} = 0.3 * Test2 + 0.1 * Quizzes + 0.6 * SEE_Theory$$

Final Attainment:

$$A_{\text{HSC601.6}} = 0.8 * A_{\text{HSC601.}6D} + 0.2 * A_{\text{HSC601.}6I}$$

Course Level Gap (if any): Nil

Content beyond Syllabus: Nil

Lecture Plan:

Module No	**Lecture No**	**Planned date**	**Actual Date**	**Content Covered**	**Delivery Mechanism/ Remark**
0	1	10-01-2023	10-01-2023	Prerequisite: Basics of hardware/ software, Networks, OS	PPT & Board
1	2	11-01-2023	11-01-2023	Definition and classification of cybercrimes	PPT & Board
	3	12-01-2023	12-01-2023	Hacking, Hackers, Crackers, Phreakers, DoS Attacks	PPT & Board
	4	13-01-2023	12-01-2023	Credit Card Frauds, Cyber Terrorism, Cyber Stalking	PPT & Board
	5	17-01-2023	13-01-2023	Computer Viruses, Computer Worms, Trojan Attacks	PPT & Board
2	6	18-01-2023	17-01-2023	Introduction to Digital Forensics and lifecycle, Principles of Digital Forensic.	PPT & Board
	7	19-01-2023	18-01-2023	Challenging Aspects of Digital Evidence, Scientific Evidence, Presenting Digital Evidence	PPT & Board
	8	20-01-2023	19-01-2023	Digital Investigation Process Models: Physical Model	PPT & Board
	9	24-01-2023	20-01-2023	Staircase Model, Evidence Flow Model.	PPT & Board

3	10	25-01-2023	24-01-2023	Windows Systems- FAT32 and NTFS	PPT & Board
	11	27-01-2023	25-01-2023	UNIX File Systems, MAC File Systems	PPT & Board
	12	31-01-2023	27-01-2023	Windows OS Artifacts: Registry, Event Logs	PPT & Board
	13	01-02-2023	31-01-2023	Memory Forensics: RAM Forensic Analysis, Creating a RAM Memory Image	PPT & Board
	14	02-02-2023	01-02-2023	Volatility framework, Extracting Information	PPT & Board
	15	03-02-2023	02-02-2023	Need of Computer Forensic Tools, Types of Computer Forensic Tools	PPT & Board
	16	07-02-2023	03-02-2023	Tasks performed by Computer Forensic Tools	PPT & Board
4	17	09-02-2023	07-02-2023	IR Process- I	PPT & Board
	18	10-02-2023	09-02-2023	IR Process- II	PPT & Board
	19	14-02-2023	10-02-2023	Live Data Collection: Live Data Collection on Microsoft Windows	PPT & Board
	20	15-02-2023	14-02-2023	Forensic Duplicates as Admissible Evidence, Forensic Duplication Tools	PPT & Board
	21	16-02-2023	15-02-2023	Creating a Forensic, Duplicate/ Qualified Forensic Duplicate of a Hard Drive.	PPT & Board
	22	17-02-2023	16-02-2023	DEMO on data collection	PPT & Board
5	23	21-02-2023	17-02-2023	Forensic Image Acquisition in Linux	PPT & Board
	24	22-02-2023	18-02-2023	Acquire an Image with dd Tools, Acquire an Image with Forensic Format	PPT & Board
	25	23-02-2023	21-02-2023	Acquire an Image with Forensic Formats	PPT & Board
	26	24-02-2023	22-02-2023	Preserve Digital Evidence with Cryptography,	PPT & Board
	27	02-03-2023	23-02-2023	Image Acquisition over a Network, Acquire Removable Media	PPT & Board
	28	03-03-2023	24-02-2023	Forensic Investigation Report Writing	PPT & Board
	29	08-03-2023	08-03-2023	Reporting Standards	PPT & Board
	30	09-03-2023	14-03-2023	Report Style and Formatting, Report Content and Organization.	PPT & Board
	31	10-03-2023	15-03-2023	Case study on Report Writing	PPT & Board
	32	14-03-2023	16-03-2023	Demo on dd tool	PPT & Board
6	33	15-03-2023	17-03-2023	Network Forensics	PPT & Board
	34	16-03-2023	21-03-2023	Sources of Network-Based Evidence	PPT & Board

	35	17-03-2023	23-03-2023	Principles of Internetworking, Internet Protocol Suite	PPT & Board
	36	21-03-2023	24-03-2023	Evidence Acquisition	PPT & Board
	37	23-03-2023	24-03-2023	Analyzing Network Traffic: Packet Flow and Statistical Flow	PPT & Board
	38	24-03-2023	28-03-2023	Network Intrusion Detection and Analysis	PPT & Board
	39	28-03-2023	05-04-2023	Investigation of Routers, Investigation of Firewalls	PPT & Board
	40	29-03-2023	06-04-2023	Mobile Forensics: Mobile Phone Challenges	PPT & Board
	41	31-03-2023		Mobile phone evidence extraction process	PPT & Board
	42	05-04-2023		Android OS Architecture, Android File Systems basics	PPT & Board
	43	06-04-2023		Types of Investigation, Procedure for Handling an Android Device	PPT & Board
	44	11-04-2023		Imaging Android, USB Mass Storage Devices.	PPT & Board
	45	12-04-2023		Demo Data recovery toolkits	PPT & Board

Textbooks:

1. Digital Forensics by Dr. Dhananjay R. Kalbande Dr. Nilakshi Jain, Wiley Publications, First Edition, 2019.
2. Digital Evidence and Computer Crime by Eoghan Casey, Elsevier Academic Press, Third Edition, 2011.
3. Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe and Kevin Mandia, McGraw-Hill Education, Third Edition (2014).
4. Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham, Pearson Edu,2012
5. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma, Heather Mahalik, PACKT publication, Open-source publication, 2014 ISBN 978-1-78328-831-1
6. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh (Author), Andrew Case (Author), Jamie Levy (Author), AAron Walters (Author), Publisher: Wiley; 1st edition (3 October 2014),

Reference Books:

1. Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002.
2. Digital Forensics with Open-Source Tools by Cory Altheide and Harlan Carvey, Syngress Publication, First Edition, 2011.
3. Practical Forensic Imaging Securing Digital Evidence with Linux Tools by Bruce Nikkel, NoStarch Press, San Francisco, (2016)
4. Android Forensics: Investigation, Analysis, and Mobile Security for Google Android by Andrew Hogg, Elsevier Publication,2011

Web References:

1. https://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2
2. https://flylib.com/books/en/3.394.1.51/1/

3. https://www.sleuthkit.org/autopsy/
4. http://md5deep.sourceforge.net/md5deep.html
5. https://tools.kali.org/
6. https://kalilinuxtutorials.com/
7. https://accessdata.com/product-download/ftk-imager-version-4-3-0
8. https://www.amazon.in/Art-Memory-Forensics-Detecting-Malware/dp/1118825098

Research Papers: Mobile Forensics/Guidelines on Cell Phone Forensics:

1. Computer Forensics Resource Center: NIST Draft Special Publication 800-101: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final
2. https://cyberforensicator.com/category/white-papers
3. https://www.magnetforensics.com/resources/ios-11-parsing-whitepaper/
4. Samarjeet Yadav, Satya Prakash, Neelam Dayal and Vrijendra Singh, "Forensics Analysis WhatsApp in Android Mobile Phone", Electronic copy available at: https://ssrn.com/abstract=3576379

Evaluation Scheme

CIE Scheme

Internal Assessment: 20 (Average of two tests)

Internal Assessment Scheme

Module		Lecture Hours	No. of questions in		No. of questions in SEE
			Test 1	Test 2	
1	Introduction to Cybercrime and Computer- crime	4	01 (5 marks)	--	1
2	Introduction to Digital Forensics and Digital Evidence	4	01(5 Marks each)	--	2
3	Computer Forensics	7	02 (10 Marks)	--	3
4	Incident Response Management, Live Data Collection and Forensic Duplication	6	--	01 (5 Marks)	1
5	Forensic Tools and Report Writing	10	--	01 (5 Marks)	2
6	Network Forensics and Mobile Forensics	14	--	02 (10 Marks)	3

Verified by:

Programme Coordinator Subject Expert