SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Department of Information Technology	LP: Sub Code Rev. No: 01
~~B.E~~/B.Tech/~~M.E/M.Tech~~ : Information Technology Regulation: 2018 PG Specialisation : -- Sub. Code / Sub. Name : IT18701 / Cyber Forensics Unit : I	Date: 23/08/2021

Unit Syllabus: INTRODUCTION

The Scope of Computer Forensics - Windows Operating and File Systems –Handling Computer Hardware –Anatomy of Digital Investigation.

Objective:

Students will understand the fundamentals of Computer Forensics and computing Investigations.

Session No *	Topics to be covered	Ref	Teaching Aids
1	The Scope of Computer Forensics – Introduction	2- Ch 1; pg 1-5	BB/LCD
2	Types of Computer Forensics Evidence Recovered – What skills must a computer Forensics Investigator Possess?	2- Ch 1; pg 6-11	BB/LCD
3	The importance of computer forensics – A History of computer forensics – Training and Education	2- Ch 1; pg 12-24	BB/LCD
4	Windows Operating and File Systems – Physical and Logical Storage	2- Ch 2; pg 32- 41	BB/LCD
5	File Conversion and Numbering Formats – Operating Systems	2- Ch 2; pg 41- 49	BB/LCD
6	Windows Registry – Microsoft Windows features	2- Ch 2; pg 50- 72	BB/LCD
7	Handling Computer Hardware – Hard Disk Drives – Cloning a PATA or SATA Hard disk	2- Ch 3; pg 80- 92	BB/LCD
8	Removable memory	2- Ch 3; pg 93- 108	BB/LCD
9	Anatomy of Digital Investigation	1- Ch 1; pg 1 -5	BB/LCD
10	A Basic Model for Investigators	1- Ch 1; pg 6 -8	BB/LCD
11	Understanding the scope of the Investigation	1- Ch 1; pg 8 -13	BB/LCD
12	The Art of Documentation	1- Ch 1; pg 13 -20	BB/LCD
Content beyond syllabus covered (if any): Digital Investigation			

* Session duration: 50 minutes

Sub. Code / Sub. Name: IT18701 / Cyber Forensics

Unit : II

Unit Syllabus : INVESTIGATIVE SMART PRACTICES
Forensics Investigative Smart Practices –Time and Forensics –Incident closure

Objective: Students will understand the fundamentals of Computer Forensics and computing Investigations.

Session No *	Topics to be covered	Ref	Teaching Aids
13	Forensics Investigative Smart Practices - The Forensic process –	3- Ch 10; pg:211-222	BB/LCD
14	Forensic Investigative smart practices - Time	3- Ch 10; pg 223-238	BB/LCD
15	Time and Forensics - What is time? - Network Time Protocol	3- Ch 11; pg:241-243	BB/LCD
16	Timestamp data – Keeping track of time	3- Ch 11; pg:244-246	BB/LCD
17	Clock models and time bounding: The foundations of Forensic time - MS-DOS 32 -bit Timestamp: Date and Time	3- Ch 11; pg :247-249	BB/LCD
18	Clock models and time bounding: The foundations of Forensic time – MS-DOS 32 -bit Timestamp: Date and	3- Ch 11; pg :247-249	BB/LCD
19	Date Determination – Time Determination – Time Inaccuracy	3- Ch 11; pg :250-258	BB/LCD
20	Incident closure – Forensic Investigative smart practices	3- Ch 12; pg :264-265	BB/LCD
21	Investigation – Communicative Findings Characteristics of a good Cyber forensic report contents	3- Ch 12; pg:265-268	BB/LCD
22	Retention and Curation of Evidence	3- Ch 12; pg:269-272	BB/LCD
23	Retention and Curation of Evidence	3- Ch 12; pg:269-272	BB/LCD
24	Investigation Wrap – up and Conclusion Investigator's role as an expert witness summary	3- Ch 12; pg:273-279	BB/LCD
Content beyond syllabus covered (if any):			

* Session duration: 50 mins

Sub. Code / Sub. Name: IT18701 / Cyber Forensics

Unit : III

Unit Syllabus : LAWS AND PRIVACY CONCERNS

Laws Affecting Forensic Investigations –Search Warrants and Subpoenas–Legislated Privacy Concerns –The admissibility of Evidence –First Response and Digital Investigator

Objective: Students will recognize the legal underpinnings and critical laws affecting forensics.

Session No *	Topics to be covered	Ref	Teaching Aids
25	Laws Affecting Forensic Investigations – Constitutional Implications	1- Ch 2; pg 23 -27	BB/LCD
26	Forensic Investigation – The right to privacy – The expert witness	1- Ch 2; pg 28 -31	BB/LCD
27	Search Warrants and Subpoenas – Distinguishing between warrants and Subpoenas	1- Ch 3; pg 35-39	BB/LCD
28	What is a search and when is it legal? - basic elements of obtaining a warrant	1- Ch 3; pg 40-42	BB/LCD
29	The plain view doctrine – The Warrantless search - Subpoenas	1- Ch 3; pg 43-50	BB/LCD
30	Legislated Privacy Concerns – General Privacy – Financial Legislation	1- Ch 4; pg 55 - 61	BB/LCD
31	Privacy in Health Care Education – Privileged Information	1- Ch 4; pg 62 - 66	BB/LCD
32	The admissibility of Evidence – What makes evidence admissible? – keeping evidence authentic	1- Ch 5; pg 71-83	BB/LCD
33	The admissibility of Evidence – What makes evidence admissible? – keeping evidence authentic	1- Ch 5; pg 71-83	BB/LCD
34	Defining the scope of the search – when the constitution doesn't apply	1- Ch 5; pg 84-88	BB/LCD
35	First Response and Digital Investigator-Forensics and Computer Science – Controlling the scene of the crime	1- Ch 5; pg 91-99	BB/LCD
36	Handling evidence	1- Ch 5; pg 100- 108	BB/LCD

Content beyond syllabus covered (if any):

* Session duration: 50 mins

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Sub. Code / Sub. Name: IT18701 / Cyber Forensics
Unit : IV

Unit Syllabus : DATA ACQUISITION AND REPORT WRITING
Data Acquisition –Finding Lost Files –Document Analysis –Case Management and Report Writing –Building a Forensics Workstation.

Objective: Students will recognize the legal underpinnings and critical laws affecting forensics.

Session No *	Topics to be covered	Ref	Teaching Aids
37	Data Acquisition- Order of Volatility	1- Ch 7; pg 111-122	BB/LCD
38	Memory and Running Processes – Acquiring media	1- Ch 7; pg 121-127	BB/LCD
39	Finding Lost files- File recovery	1- Ch 8; pg 131-141	BB/LCD
40	The deleted file – data carving	1- Ch 8; pg 141-148	BB/LCD
41	Document Analysis – File identification – understanding metadata	1- Ch 9; pg 151-171	BB/LCD
42	Mining the temporary files – identifying alternate hiding places of data	1- Ch 9; pg 172-182	BB/LCD
43	Mining the temporary files – identifying alternate hiding places of data	1- Ch 9; pg 172-182	BB/LCD
44	Case Management and Report Writing	1- Ch 17; pg 379-388	BB/LCD
45	Managing a case – Writing reports	1- Ch 17; pg 389-392	BB/LCD
46	Managing a case – Writing reports	1- Ch 17; pg 389-392	BB/LCD
47	Building a Forensics Workstation– What is a forensic workstation? - Commercially available forensic	1- Ch 19; pg 423-428	BB/LCD
48	Building a Forensics Workstation from scratch	1- Ch 19; pg 429-239	BB/LCD

Content beyond syllabus covered (if any):

* Session duration: 50 mins

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Sub. Code / Sub. Name: IT18701 / Cyber Forensics
Unit :V

Unit Syllabus : TOOLS AND CASE STUDIES

Tools of the Digital Investigator-Licensing and Certification –Case Studies: E-mail Forensics –Web Forensics –Searching the Network –Excavating a Cloud –Mobile device Forensics.

Objective: Students will apply the tools and methods to uncover hidden information in digital systems. Students will learn about current licensing and certification requirements to build the career in digital forensic.

Session No *	Topics to be covered	Ref	Teaching Aids
49	Tools of the Digital Investigator – Software tools – Working with "Court-Approved" tools	1- Ch 18; pg 395-412	BB/LCD
50	Hardware tools – nontechnical tools	1- Ch 18; pg 413-420	BB/LCD
51	Licensing and Certification – Digital Forensic Certification- Vendor Licensing Requirements	1- Ch 20; pg 441-448	BB/LCD
52	Neutral Certification Programs - Vendor – Neutral Specific Programs – Digital Forensic	1- Ch 20; pg 448-453	BB/LCD
53	Case Studies: E-mail Forensics – Email technology – Information Stores – the Anatomy of an E-mail – An approach to Email analysis	1- Ch 10; pg 185-209	BB/LCD
54	Web Forensics –Internet Addresses – Web browsers – Web servers – Proxy servers	1- Ch 11; pg 213-242	BB/LCD
55	Searching the Network- An eagle's eye view – Initial response – Proactive collection of evidence	1- Ch 12; pg 247-252	BB/LCD
56	Post – incident Collection of evidence – Router and switch forensics	1- Ch 12; pg 253-274	BB/LCD
57	Excavating a Cloud - What is cloud computing? Shaping the cloud	1- Ch 13; pg 277-293	BB/LCD
58	The implications of cloud forensics – on virtualization –Constitutional issues	1- Ch 13; pg 294-302	BB/LCD
59	Mobile device Forensics – Challenges of mobile device forensics – how cell phone works – data storage on cell	1- Ch 14; pg 307-316	BB/LCD
60	Acquisition and storage – legal aspects of mobile device forensics	1- Ch 14; pg 317-323	BB/LCD

Content beyond syllabus covered (if any):

* Session duration: 50 mins

TEXT BOOKS:

1. Michael Graves, —Digital Archaeology: The Art and Science of Digital Forensics, Addison-Wesley Professional, 2014.
2. Darren R. Hayes, —Practical Guide to Computer Forensics Investigation, Pearson, 2015.

REFERENCES:

3. Albert J. Marcella and Frederic Guillossou, —Cyber Forensics: From Data to Digital Evidence, Wiley, 2015.
4. Bill Nelson, Amelia Phillips and Christopher Steuart, —Guide to Computer Forensics

	Prepared by	Approved by
Signature	G. 23/8/2021.	23/8/21
Name/ Designation	Ms.G.Sangeetha / Assistant Professor Mr. AR. Gurugokul / Assistant Professor	Dr.V.VIDHYA HOD-INT
Date	23/08/2021	23/08/2021
Remarks *:		
Remarks *:		

* If the same lesson plan is followed in the subsequent semester/year it should be mentioned and signed by the Faculty and the HOD