SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Department of Information Technology	LP: IT18013 Rev. No: 00 Date: 22.07.2021
B.E/B.Tech/M.E./M.Tech : B.Tech Regulation: R2018 PG Specialisation : - Sub. Code / Sub. Name : IT18013 / Digital Forensic Tools and Techniques Unit : I	

Unit Syllabus: BASICS OF DIGITAL FORENSICS

The Role of Digital Forensics - the history and purpose, criminal investigations and cybercrime, civil investigations and the nature of e-discovery , The role and challenges of digital forensic practitioners , case studies, Digital Forensics Environment – Nature of digital information, Operating systems , Describing and locating evidence in file systems , password security, encryption, and hidden files , linking the evidence to the user.

Objective:

Students will have an understanding of fundamental concepts and applications of digital forensics.

Session No *	Topics to be covered	Ref	Teaching Aids
1	Role of Digital Forensics	1-Ch 1; pg 1-7	BB/LCD
2	The history and purpose digital forensics	1- Ch 1; pg 8-11	BB/LCD
3	Criminal investigations and cybercrime, civil investigations and the nature of e-discovery	1- Ch 1; pg 12- 14	BB/LCD
4	The role and challenges of digital forensic practitioners	1- Ch 1; pg 15- 20	BB/LCD
5	Case studies	1- Ch 1; pg 21- 22	BB/LCD
6	Digital Forensics Environment – Nature of digital information	1- Ch 2; pg 25- 29	BB/LCD
7	Operating systems	1- Ch 2; pg 30 -41	BB/LCD
8	Describing and locating evidence in file systems	1- Ch 2; pg 42-47	BB/LCD
9	Password security, encryption, and hidden files , linking the evidence to the user	1- Ch 2; pg 48 -53	BB/LCD

Content beyond syllabus covered (if any):

* Session duration: 50 minutes

Sub. Code / Sub. Name: IT18013 / Digital Forensic Tools and Techniques

Unit : II

Unit Syllabus : INTRODUCTION TO DIGITAL EVIDENCE

Digital evidence – Usage, Characteristics, technical complexities, determining the value and admissibility of digital evidence, Recovering and Preserving Digital Evidence - chain of custody, physical acquisition and safe keeping, Recovery - forensic imaging process, live recovery process.

Objective: Students will understand the digital evidence handling procedures.

Session No *	Topics to be covered	Ref	Teaching Aids
10	Digital evidence – Usage	1- Ch 3; pg 55-63	LCD
11	Characteristics	1- Ch 3; pg 64-70	LCD
12	Technical complexities	1- Ch 3; pg 71-75	LCD
13	Determining the value and admissibility of digital evidence	1- Ch 3; pg 76-82	LCD
14	Determining the value and admissibility of digital evidence	1- Ch 3; pg -83-88	LCD
15	Recovering and Preserving Digital Evidence - chain of custody-case studies	1- Ch 4; pg 91-98	LCD
16	Physical acquisition and safe keeping	1- Ch 4; pg 99-104	LCD
17	Recovery - forensic imaging process	1- Ch 4; pg 105-114	LCD
18	Live recovery process	1- Ch 4; pg 115-119	LCD

Content beyond syllabus covered (if any):
Different case studies related to chain of custody.

* Session duration: 50 mins

Sub. Code / Sub. Name: IT18013 / Digital Forensic Tools and Techniques

Unit : III

Unit Syllabus : TOOLS

Forensic Tools - Standards, Need, forensic imaging tools, Enhanced forensic tools - The Event Analysis tool ,The Cloud Analysis tool ,The Lead Analysis tool, Analyzing e-mail datasets ,Detecting scanned images ,Volume Shadow Copy analysis tools ,Timelines and other analysis tools, Case study : Interrogating large datasets , Selecting and Analyzing Digital Evidence- Structured processes to locate and select digital evidence ,Locating digital evidence, Selecting digital evidence , Case study : recovery of deleted evidence held in volume shadows.

Objective: Students will be able to make use of digital forensic tools in appropriate cases.

Session No *	Topics to be covered	Ref	Teaching Aids
19	Forensic Tools - Standards	1- Ch 5; pg 120 - 127	LCD
20	Need, forensic imaging tools, Enhanced forensic tools	1- Ch 5; pg 129-149	LCD
21	The Event Analysis tool ,The Cloud Analysis tool ,The Lead Analysis tool	1- Ch 6; pg 193-201	LCD
22	Analyzing e-mail datasets ,Detecting scanned images ,Volume Shadow Copy analysis tools ,Timelines and other analysis tools	1- Ch 6; pg 202 - 206	LCD
23	Case study : Interrogating large datasets	1- Ch 5; pg 157 - 162	LCD
24	Selecting and Analyzing Digital Evidence- Structured processes to locate and select digital evidence	1- Ch 6; pg 165-167	LCD
25	Locating digital evidence	1- Ch 6; pg 168-181	LCD
26	Selecting digital evidence	1- Ch 6; pg 182-192	LCD
27	Case study : recovery of deleted evidence held in volume shadows.	1-Ch 6; pg 207-209	

Content beyond syllabus covered (if any):

* Session duration: 50 mins

Sub. Code / Sub. Name: IT18013 / Digital Forensic Tools and Techniques
Unit : IV

Unit Syllabus : **EVIDENCE SOURCE AND EXAMINATION**

Sources of Evidence -The Windows Registry and system files and logs as resources of digital evidence , Apple and other operating system structures, Remote access and malware threats ,Case study – corroborating evidence using Windows Registry, Examining Evidence - Locating evidence from Internet browsing ,Messaging systems , E-mail analysis and the processing of large e-mail databases , evidence recovery from mobile phones and handheld devices Case study – mobile phone evidence in a bomb hoax.

Objective: Students will be able to examine the digital evidence ..

Session No *	Topics to be covered	Ref	Teaching Aids
28	Sources of Evidence -The Windows Registry and system files and logs as resources of digital evidence	1- Ch 7; pg 211 - 227	LCD
29	Apple and other operating system structures	1- Ch 7; pg 228 - 232	LCD
30	Remote access and malware threats	1- Ch 7; pg 233 - 235	LCD
31	Case study – corroborating evidence using Windows Registry	1- Ch 7; pg 236 - 239	LCD
32	Examining Evidence - Locating evidence from Internet browsing	1- Ch 8; pg 241 -252	LCD
33	Messaging systems , E-mail analysis and the processing of large e-mail databases	1- Ch 8; pg 253-264	LCD
34	Evidence recovery from mobile phones and handheld devices	1- Ch 8; pg 265-278	LCD
35	Managing evidence contamination and Concealing illegal activities	1- Ch 8; pg 279-282	LCD
36	Case study – mobile phone evidence in a bomb hoax	1-Ch 8; pg 283-290	LCD

Content beyond syllabus covered (if any):
Managing evidence contamination and Concealing illegal activities in Mobile phones

* Session duration: 50 mins

Sub. Code / Sub. Name: IT18013 / Digital Forensic Tools and Techniques

Unit :V

Unit Syllabus : VALIDATING THE EVIDENCE

The nature and problem of unsound digital evidence , Impartiality in selecting evidence ,The structured and balanced analysis of digital evidence ,Formalizing the validation of digital evidence ,The presentation of digital evidence, Ethical issues confronting digital forensics practitioners, Case study – presumed unauthorized use of intellectual property Solutions to the challenges posed by new hardware and software ,Challenges posed by communication media and the cloud , Mobile phone evidence recovery ,The cloud - convenient for users but problematic for practitioners ,The need for effective evidence processing and validation ,Contingency planning

Objective: Students will be able to appropriately validate and present the digital evidence. .

Session No *	Topics to be covered	Ref	Teaching Aids
37	The nature and problem of unsound digital evidence	1-Ch 9; pg 291-296	LCD
38	Impartiality in selecting evidence ,The structured and balanced analysis of digital evidence	1-Ch 9; pg 297-302	LCD
39	Formalizing the validation of digital evidence-	1-Ch 9; pg 303-308	LCD
40	Applying Bayesian reasoning to the analysis of validation	1-Ch 9; pg 309-319	LCD
41	The presentation of digital evidence, Ethical issues confronting digital forensics practitioners	1-Ch 9; pg 320-325	LCD
42	Case study – presumed unauthorized use of intellectual property	1-Ch 9; pg 326-330	LCD
43	Solutions to the challenges posed by new hardware and software	1-Ch 10; pg 333-336	LCD
44	Challenges posed by communication media and the cloud , Mobile phone evidence recovery ,The cloud - convenient for users but problematic for practitioners ,The need for effective evidence processing and validation ,Contingency planning .	1-Ch 10; pg 337-340	LCD
45	Revision		
Content beyond syllabus covered (if any):			

* Session duration: 50 mins

Sub Code / Sub Name: IT18013 / Digital Forensic Tools and Techniques

Text Books:

1. Richard Boddington, "Practical Digital Forensics", Packt Publishing, 2016

References:

1. Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Syngress, April 2011
2. Harlan Carvey, "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7", Syngress Publishing, 2012.

	Prepared by	Approved by
Signature		
Name	Dr G.SUMATHI	Dr.V.VIDHYA
Designation	Professor	HOD-IT
Date	22/07/2021	22/07/2021
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