

**UNIT - I****Chapter 1 : Introduction to Cybercrime and Hacking 1-1 to 1-24****Syllabus :**

- 1.1 Cybercrime, Categories of Cybercrime (Cybercrime against people, Cybercrime Against property, Cybercrime Against Government), Types of cybercrime (Violent- Cyber terrorism, Assault by Threat, Cyberstalking, Child Pornography, Non-violent - Cybertrespass, Cyber Theft, Cyberfraud, Destructive Cybercrimes), Computers' role in crimes
- 1.2 Hacking, Life cycle of Hacking, Types of Hackers (White Hat hackers, Black Hat hackers, Grey Hat hackers), Hacking techniques, Passive and Active Attacks, Social Engineering, Attacks vs Vulnerabilities, Prevention of Cybercrime.

<b>1.1 Cybercrime.....</b>	<b>1-1</b>
1.1.1 Categories of Cybercrime (Cybercrime against People, Cybercrime against property, Cybercrime against Government) .....	1-2
1.1.2 Types of Cybercrime.....	1-5
1.1.3 Computers' Role in Crimes .....	1-8
<b>1.2 Hacking.....</b>	<b>1-9</b>
1.2.1 Life cycle of Hacking .....	1-10
1.2.2 Types of Hackers (White Hat hackers, Black Hat hackers, Grey Hat hackers) .....	1-12
1.2.3 Hacking Techniques .....	1-13
<b>1.3 Passive and Active Attacks.....</b>	<b>1-16</b>
1.3.1 Difference between Active attack and Passive Attack .....	1-18
<b>1.4 Social Engineering.....</b>	<b>1-18</b>
<b>1.5 Attacks vs Vulnerabilities.....</b>	<b>1-20</b>
<b>1.6 Prevention of Cybercrime .....</b>	<b>1-21</b>
<b>1.7 Self-learning topics : Distinction between Computer Crimes and Conventional Crimes.....</b>	<b>1-22</b>

**UNIT II****Chapter 2 : Introduction to Digital Forensics 2-1 to 2-26****Syllabus :**

- 2.1 Objectives of digital forensics, Process of digital forensics, Types of digital forensics, Challenges faced by digital forensics
- 2.2 Introduction to Incident - Computer Security Incident, Goals of Incident Response, CSIRT, Incident Response Methodology, Phase after detection of an incident

<b>2.1</b>	<b>Objectives of digital forensics</b> .....	<b>2-1</b>
2.1.1	Process of Digital Forensics .....	2-2
2.1.2	Types of Digital Forensics .....	2-4
2.1.3	Challenges Faced by Digital Forensics .....	2-6
<b>2.2</b>	<b>Introduction to Incident</b> .....	<b>2-7</b>
2.2.1	Computer Security Incident.....	2-7
2.2.2	Goals of Incident Response .....	2-7
2.2.3	CSIRT .....	2-8
2.2.3(A)	The CSIRT Core Team .....	2-8
2.2.3(B)	Technical Support Personnel .....	2-11
2.2.3(C)	Organizational support personnel.....	2-12
2.2.3(D)	External Resources.....	2-13
2.2.4	Incident Response Methodology .....	2-14
2.2.5	Phase After Detection of an Incident.....	2-15
<b>2.3</b>	<b>Distinction between Computer Virus, Worm, Trojan Horse and Trap Door</b> .....	<b>2-24</b>

**UNIT III**

**Chapter 3 : Digital Evidence and Forensics Duplication**

**3-1 to 3-24**

**Syllabus :**

- 3.1 Digital evidence, Admissibility of evidence, Challenges in evidence handling, collecting digital evidence, Preserving digital evidence, Documenting evidence
- 3.2 Necessity of forensic duplication, Forensic duplicates as admissible evidence, Forensic image formats, Forensic duplication techniques, Disk imaging, Analysis of forensic images using FTK Imager

<b>3.1</b>	<b>Digital evidence</b> .....	<b>3-1</b>
3.1.1	Types of Evidence .....	3-2
3.1.2	Evidence Characteristics.....	3-3
3.1.3	Admissibility of Evidence.....	3-3
3.1.4	Challenges in Evidence Handling.....	3-4
3.1.5	Collecting Digital Evidence .....	3-6
3.1.6	Preserving Digital Evidence .....	3-10
3.1.7	Documenting Evidence.....	3-11

**3.2 Necessity of Forensic Duplication ..... 3-12**

    3.2.1 Forensic Duplicates as Admissible Evidence..... 3-12

    3.2.2 Forensic Image Formats..... 3-13

    3.2.3 Forensic Duplication Techniques ..... 3-15

    3.2.4 Disk imaging ..... 3-16

**3.3 Digital Evidence Investigation Using Autopsy ..... 3-17**

**UNIT -IV**

**Chapter 4 : System Investigation 4 - 1 to 4 - 49**

<b>Syllabus :</b>	
4.1	Live/volatile data collection from Windows and Unix Systems
4.2	Investigating Windows systems, Investigating UNIX systems, Investigating applications, Web browsers, Email tracing
4.3	Recovering digital evidence, Acquiring, Analyzing and duplicating data: dd, dcfldd, foremost, scalpel

**4.1 Live/volatile data collection from Windows and Unix Systems ..... 4-1**

    4.1.1 Volatile Data Collection from Windows System..... 4-1

        4.1.1(A) Creating a Response Toolkit..... 4-1

        4.1.1(B) Storing Information Obtained During the Initial Response..... 4-4

        4.1.1(C) Obtaining Volatile Data..... 4-6

    4.1.2 Volatile Data Collection from UNIX System ..... 4-10

        4.1.2(A) Creating a Response Toolkit..... 4-10

        4.1.2(B) Storing Information Obtained During the Initial Response..... 4-11

        4.1.2(C) Obtaining Volatile Data Prior to Forensic Duplication..... 4-11

**4.2 Investigating Windows systems, Investigating UNIX Systems, Investigating Applications, Web browsers, Email Tracing ..... 4-15**

    4.2.1 Investigating Windows Systems ..... 4-15

        4.2.1(A) Steps for Conducting a Windows Investigation..... 4-16

    4.2.2 Investigating Live Unix System..... 4-26

    4.2.3 Investigating Applications ..... 4-34

    4.2.4 Web Browsers..... 4-36

        4.2.4(A) Cookie Storage and Analysis..... 4-38

4.2.4(B) Analyzing Cache and Temporary Internet Files.....	4-39
4.2.5 Email Tracing.....	4-40
4.2.5(A) Email Clients and Servers.....	4-41
4.2.5(B) E-mail Analysis.....	4-42
4.2.5(C) e-mail Headers and Spoofing.....	4-44
<b>4.3 Recovering digital evidence, Acquiring, Analysing and Duplicating data : dd, dcfldd, foremost, scalpel.....</b>	<b>4-45</b>
<b>4.4 Methods of storing data (RAM and Hard disk).....</b>	<b>4-48</b>

## UNIT V

### Chapter 5 : Network Forensics

**5-1 to 5-56**

#### **Syllabus :**

- |  |
|--|
| 5.1 Introduction to intrusion detection systems, Types of IDS, Understanding network intrusion and attacks |
| 5.2 Analyzing network traffic, collecting network based evidence, Evidence handling. Investigating routers |

<b>5.1 Introduction to Intrusion Detection Systems .....</b>	<b>5-1</b>
5.1.1 Types of IDS.....	5-2
5.1.2 Understanding Network Intrusion and Attacks.....	5-3
5.1.2(A) Identifying and Categorizing Attack Types .....	5-4
<b>5.2 Analyzing Network Traffic .....</b>	<b>5-22</b>
5.2.1 Collecting Network-Based Evidence.....	5-22
5.2.1(A) What is Network Based Evidence?.....	5-23
5.2.1(B) What are the Goals of Network Monitoring ?.....	5-23
5.2.1(C) Types of Network Monitoring.....	5-23
5.2.1(D) Setting up a Network Monitoring System .....	5-24
5.2.1(E) Performing a Trap-and-Trace .....	5-29
5.2.1(F) Using TCPDUMP for Full Content Monitoring.....	5-29
5.2.2 Evidence Handling.....	5-31
5.2.2(A) Shipping/Transporting Evidence Media .....	5-35
5.2.3 Investigating Routers .....	5-37
5.2.3(A) Obtaining Volatile Data Prior to Powering Down .....	5-38

5.2.3(B) Finding the Proof..... 5-39

5.2.3(C) Using Routers as Response Tools..... 5-42

**5.3 Use of Packet Sniffing Tools Like Wireshark ..... 5-45**

**UNIT -VI**

**Chapter 6 : Laws Related to Cyber Crime 6-1 to 6-17**

**Syllabus :** Constitutional law, Criminal law, Civil law, Levels of law: Local laws, State laws, Federal laws, International laws. Levels of culpability: Intent, Knowledge, Recklessness, Negligence. CFAA, DMCA, CAN Spam

**6.1 Constitutional law, Criminal law, Civil law .....6-1**

6.1.1 Criminal Law..... 6-1

6.1.2 Civil Law..... 6-3

6.1.3 Administrative/Regulatory Law..... 6-3

**6.2 Levels of Law .....6-4**

6.2.1 Local Laws..... 6-4

6.2.2 State Laws ..... 6-5

6.2.3 Federal Laws..... 6-5

6.2.4 International Laws..... 6-6

**6.3 Levels of Culpability : Intent, Knowledge, Recklessness, Negligence .....6-6**

6.3.1 Intent..... 6-6

6.3.2 Knowledge..... 6-6

6.3.3 Recklessness..... 6-7

6.3.4 Negligence..... 6-7

**6.4 Level and Burden of Proof.....6-7**

6.4.1 Criminal Versus Civil Cases ..... 6-7

6.4.2 Vicarious Liability ..... 6-8

**6.5 Laws Related to Computers : CFAA, DMCA, CAN Spam .....6-8**

6.5.1 Computer Fraud and Abuse Act (CFAA)..... 6-8

6.5.2 Digital Millennium Copyright Act (DMCA)..... 6-10

6.5.3 The CAN-SPAM Act..... 6-13

**6.6 Relevant law to combat computer crime –Information Technology Act..... 6-15**

