4. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, “Computer Networks: An Open Source Approach”, McGraw Hill, 2012.

CO’s- PO’s & PSO’s MAPPING

CO’s	PO’s												PSO’s	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	-	2	-	-	-	-	-	-	-	-	-	-	3	-
2	-	-	-	-	2	-	-	-	-	-	-	2	-	2
3	-	2	-	-	3	-	-	-	-	-	-	-	-	3
4	-	-	-	1	2	-	-	-	-	3	-	-	-	-
5	-	3	2	-	-	-	-	-	-	-	-	-	-	-
AVg.	-	2	-	-	2	-	-	-	-	1	-	-	1	1

1 - low, 2 - medium, 3 - high, ‘-' - no correlation

CB3601 CYBER FORENSICS L T P C
3 0 2 4

COURSE OBJECTIVES:

- To learn cyber crime and forensics
- To become familiar with forensics tools
- To learn to analyze and validate forensics data
- To understand cyber laws and the admissibility of evidence with case studies
- To learn the vulnerabilities in network infrastructure with ethical hacking

UNIT I INTRODUCTION TO CYBER CRIME AND FORENSICS 9

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Role of ECD and ICT in Cybercrime - Classification of Cyber Crime. The Present and future of Cybercrime - Cyber Forensics -Steps in Forensic Investigation - Forensic Examination Process - Types of CF techniques - Forensic duplication and investigation - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

UNIT II EVIDENCE COLLECTION AND FORENSICS TOOLS 9

Processing Crime and Incident Scenes – Digital Evidence - Sources of Evidence -Working with File Systems. - Registry - Artifacts - Current Computer Forensics Tools: Software/ Hardware Tools - Forensic Suite - Acquisition and Seizure of Evidence from Computers and Mobile Devices - Chain of Custody- Forensic Tools

UNIT III ANALYSIS AND VALIDATION 9

Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics - Analysis of Digital Evidence - Admissibility of Evidence - Cyber Laws in India - Case Studies

UNIT IV ETHICAL HACKING 9

Introduction to Ethical Hacking - Footprinting and Reconnaissance - Scanning Networks - Enumeration - System Hacking - Malware Threats – Sniffing – Email Tracking

UNIT V ETHICAL HACKING IN WEB 9

Social Engineering - Denial of Service - Session Hijacking - Hacking Web servers - Hacking Web Applications – SQL Injection - Hacking Wireless Networks - Hacking Mobile Platforms.

45 PERIODS

PRACTICAL EXERCISES: 30 PERIODS

1. Study and Explore the following forensic tools:

(a) FTK Imager
(b) Autopsy
(c)EnCase Forensic Imager
(d) LastActivityView
(e) USBDeview

2. Recover deleted files using FTKImager

3. Acquire forensic image of hard disk using EnCase Forensics Imager and also perform integrity checking/validation

4. Restore the Evidence Image using EnCase Forensics Imager.

5. Study the following:

(a) Collect Email Evidence in Victim PC.

(b) Extract Browser Artifacts (ChromeHistory view for Google Chrome)

6. Use USBDeview to find the last connected USB to the system

7. Perform Live Forensics Case Investigation using Autopsy

8. Study Email Tracking and EmailTracing and write a report on them.

COURSE OUTCOMES:

CO1: Understand the basics of cyber crime and computer forensics
CO2: Apply a number of different computer forensic tools to a given scenario
CO3: Analyze and validate forensics data
CO4: Understand Admissibility of evidence in India with Cyber laws and Case Studies
CO5: Identify the vulnerabilities in a given network infrastructure
CO6: Implement real-world hacking techniques to test system security

TEXT BOOKS

1. Bill Nelson, Amelia Phillips, Christopher Steuart, — Guide to Computer Forensics and Investigations‖, Cengage Learning, India Sixth Edition, 2019.
2. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, Version 11, 2021.
3. Dejey, S. Murugan - Cyber Forensics, Oxford University Press, India, 2018

REFERENCE BOOKS

1. John R.Vacca, "Computer Forensics ", Cengage Learning, 2005
2. MarjieT.Britz, "Computer Forensics and Cyber Crime: An Introduction 3rd Edition, Prentice Hall, 2013.
3. AnkitFadia " Ethical Hacking, Second Edition, Macmillan India Ltd, 2006
4. Kenneth C.Brancik "Insider Computer Fraud‖ Auerbach Publications Taylor &Francis Group– 2008.

CO's- PO's & PSO's MAPPING

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	-	-	-	-	-	-	1	1	-	-	-	2	-	3
2	2	1	1	2	-	-	-	-	-	-	-	2	2	1

3	2	2	1	1	2	-	-	-	-	-	-	1	3	-
4	-	-	-	-	-	-	1	2	-	-	-	1	-	2
5	-	3	-	2	-	-	1	1	-	-	-	2	2	1
AVg.	2	2	1	2	2	-	1	1	-	-	-	2	2	2

1 - low, 2 - medium, 3 - high, '-' - no correlation

CB3602 NETWORK SECURITY L T P C
3 0 2 4

COURSE OBJECTIVES:

- To understand the basic concepts of security
- To understand the concept of authentication protocols and digital signatures.
- To learn various methods and protocols to understand the cryptography.
- To learn various network security attacks.
- To understand the IP and Web security.

UNIT I FUNDAMENDALS OF NETWORKING SECURITY 9

Overview of networking security- Security Services -Confidentiality, Authentication, Integrity, Non-repudiation, access Control - Availability and Mechanisms- Security Attacks -Interruption, Interception ,Modification and Fabrication.

UNIT II AUTHENTICATION AND SECURITY 9

Authentication overview - Authentication protocols - Authentication and key establishment - key exchange - mediated key exchange - User Authentication –password based authentication - password security - Certificate Authority and key management - digital signatures - digital Certificates.

UNIT III PUBLIC-KEY CRYPTOGRAPHY AND MESSAGE AUTHENTICATION 9

Basics of cryptography -cryptographic hash functions - symmetric and public-key encryption - public key cryptography principles & algorithms - cipher block modes of operation - Secure Hash Functions – HMAC

UNIT IV SECURITY ATTACKS 9

Buffer overflow attacks & format string vulnerabilities - Denial-of-Service Attacks -Hijacking attacks : exploits and defenses - Internet worms – viruses – spyware –phishing – botnets - TCP session hijacking - ARP attacks - route table modification - UDP hijacking - man-in-the-middle attacks.

UNIT V IP SECURITY AND WEB SECURITY 9

Network defense tools: Firewalls,VPNs, Intrusion Detection, and filters - Email privacy: Pretty Good Privacy (PGP) and S/MIME - Network security protocols in practice- Introduction to Wireshark – SSL - IPsec, and IKE -DNS security- Secure Socket Layer (SSL) and Transport Layer Security (TLS) - Secure Electronic Transaction (SET)

45 PERIODS

PRACTICAL EXERCISES:

1. Using Wireshark explore the different layer protocol headers.
2. Demonstrate two different Certificates producing the same MD5 hash
3. Computing MACs, HASH and HMAC for messages