Savitribai Phule Pune University, Pune

(Formerly University of Pune)

Three Year B.Sc. Degree Program in
Cyber and Digital Science
(Faculty of Science & Technology)

T.Y.B.Sc.(Cyber and Digital Science)

Choice Based Credit System Syllabus

To be implemented from

Academic Year **2022-2023**

T.Y.B.Sc. (Cyber and Digital Science)

Semester V

Course Type	Paper Code	PaperTitle	Credits		Evaluation		
			T	P	CA	UA	Total
DSEC-I	CDS-351	Digital Forensics-1	4		30	70	100
	CDS-354	Lab on CDS-351		2	15	35	50
DSEC-II	CDS-352	Cyber Threat Intelligence	4		30	70	100
	CDS-355	Lab on CDS-352		2	15	35	50
DSEC-III	CDS-353	Information Security policy and Audit	4		30	70	100
	CDS-356	Lab on CDS-353		2	15	35	50
SECC-I	CDS-357	Professional Elective-I	2		15	35	50
SECC-II	CDS-358	Professional Elective-II		2	15	35	50

Semester VI

Course Type	Paper Code	PaperTitle	Credits		Evaluation		
			T	P	CA	UA	Total
DSEC-I	CDS-361	Digital Forensics-2	4		30	70	100
	CDS-364	Lab on CDS-361		2	15	35	50
DSEC-II	CDS-362	Cyber Law (Information Security Policies and Strategies)	4		30	70	100
	CDS-365	Lab on CDS-362		2	15	35	50
DSEC-III	CDS-363	Web Science	4		30	70	100
	CDS-366	Lab on CDS-363		2	15	35	50
SECC-III	CDS-367	Professional Elective-III	2		15	35	50
SECC-IV	CDS-368	Professional Elective-IV		2	15	35	50

*CC:Core Course
*DSE:Discipline Specific Elective
*AECC:Ability Enhancement Compulsory Course
*SECC:Skill Enhancement Compulsory Course

Professional Electives

** Note: There is a one to one mapping from the sets of SECC. A student will have to select acoursefor CDS-357andits appropriatemappingforCDS-358.

SECC (Any one for CDS-357 and CDS -367)	SECC (Any one for CDS-358 and CDS -368)
Mobile forensics	Lab Course on Mobile Forensics
Malware Analysis	Lab Course on Malware Analysis
Fin tech- Cybersecurity	Lab Course on Fin-tech Cybersecurity
Cloud security	Lab Course on cloud security

Savitribai Phule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-351
Title: Digital Forensics-1

Teaching Scheme	No. of Credits	Examination Scheme
4hours / week	4	CA :30 marks UA: 70 marks

Prerequisites: -

1. Knowledge of Cryptography and Security
2. Basic knowledge Operating Systems and Computer Networks

Course Objectives: -

1. To understand underlying principles and many of the techniques associated with the digital forensic practices and cyber crime
2. To explore practical knowledge about digital forensic methodology.
3. To learn the importance of evidence handling and storage for various devices
4. To develop an excellent understanding of current cyber security issues and analyzed the ways that exploits in securities.
5. To investigate attacks, Intrusion Detection System technical exploits and router attacks and "Trap and Trace" computer networks.
6. To apply digital forensic knowledge to use computer forensic tools and investigation report writing.

Course Outcomes: -

After completion of the course student will be able to :-

1. Describe Forensic science and Digital Forensic concepts
2. Determine various digital forensic Operandi and motive behind cyber attacks
3. Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective.
4. Demonstrate various forensic tools to investigate the cybercrime and to identify the digital pieces of evidence
5. Analyze the digital evidence used to commit cyber offences.

Course Contents

Chapter 1	**Introduction: Digital Forensics**	**12 hours**
1.1.	What Is Digital Forensics?	
1.2.	Digital Forensics Goals	

1.3. Cybercrime

1.3.1 Cybercrime Attack Mode How Are Computers Used in Cybercrimes?

1.3.2 Example of Cybercrime

1.4. Types of Digital Forensics

1.4.1 Computer Forensics

1.4.2 Mobile Forensics Network Forensics

1.4.3 Database Forensics

1.4.4 Forensics Data Analysis

1.5. Digital Forensics Users

1.5.1 Law Enforcement

1.5.2 Civil Ligation

1.5.3 Intelligence and Counterintelligence

1.6. Types of Digital Forensics Investigation

1.7. Forensics Readiness

1.7.1 The Importance of Forensic Readiness for Organizations

Reference book 1 and 2

Chapter 2	**Essential Technical Concepts**	**10 hours**

2.1 Data Representation

2.1.1 Decimal (Base-10)

2.1.2 Binary

2.1.3 Hexadecimal (Base-16)

2.1.4 Computer Character Encoding Schema

2.2 File Structure

2.3 Digital File Metadata

2.4 Timestamps Decoder (Tool)

2.5 Hash Analysis

2.6 How to Calculate File Hash

2.7 Memory Types

2.7.1 Volatile Memory

2.7.2 Nonvolatile Memory

2.8 Types of Computer Storage

2.8.1 Primary Storage

2.8.2 Secondary Storage

2.9 HPA and DCO

2.10 Data Recovery Considerations

2.11 File Systems

2.11.1 NTFS

2.11.2 FAT

Reference book 1 and 2

Chapter 3	**Initial Response and First Responder Tasks**	**16 hours**

3.1 Digital Evidence

3.1.1 Digital Evidence Types

3.1.2 Locations of Electronic Evidence

3.1.3 Challenge of Acquiring Digital Evidence

3.1.4 Who Should Collect Digital Evidence?

3.1.5 Chain of Custody

3.1.6 Cloning, and Live vs Dead System

3.1.7 Hashing, and Final Report

3.2 Digital Forensics Examination Process

3.2.1 Seizure

3.2.2 Acquisition

3.2.3 Analysis

3.2.4 Reporting

3.3 Digital Forensics vs. Other Computing Domain

3.4 Search and Seizure

3.1.1 Consent to Search

3.1.2 Subpoena

3.1.3 Search Warrant

3.5 First Responder Toolkit

3.6 First Responder Tasks

3.7 Order of Volatility

3.8 Documenting the Digital Crime Scene

3.9 Packaging and Transporting Electronic Devices

3.10 Conducting Interview

3.7.1 First Responder Questions When Contacted by a Client

3.7.2 Witness Interview Questions

3.7.3 Witness Signature

Reference Book 1 and 2

Chapter 4	**Network Forensic**	**12 hours**

4.1 What Is Network Forensics?

4.2 Computing Environment

4.2.1 Personal Computing Environment

4.2.2 Client Server Computing Environment

4.2.3 Distributed Computing Environment

4.3 Introduction to the Incident Response Process

4.4 Investigative and Forensics Methodologies

4.5 Where Network Forensics Fits In

4.6 Capturing Network Traffic

4.6.1 The Importance of DHCP Logs

4.6.2 Using tcpdump/WinDump

4.6.3 Using Wireshark

4.6.4 Using SPAN Ports or TAPS

4.6.5 Using Fiddler

4.6.6 Firewalls

Reference Book 3

Chapter 5	**Digital Forensics Tools**	**10 hours**

5.1 Evaluating Digital Forensics Tool Needs

5.1.1 Types of Digital Forensics Tools

5.1.2 Tasks Performed by Digital Forensics Tools

5.1.3 Tool Comparisons

5.1.4 Other Considerations for Tools

5.2 Digital Forensics Software Tools

5.2.1 Command-Line Forensics Tools

5.2.2 Linux Forensics Tools

5.2.3 Other GUI Forensics Tools

5.3 Digital Forensics Hardware Tools

5.3.1 Forensic Workstations

5.3.2 Using a Write-Blocker

5.3.3 Recommendations for a Forensic Workstation

5.4 Validating and Testing Forensics Software

5.4.1 Using National Institute of Standards and Technology Tools

5.4.2 Using Validation Protocols

Reference Book 4 and 6

Reference Books:

1. John Sammons, "The Basics of Digital Forensics - The Primer for Getting Started in Digital Forensics" *Syngress* is an imprint of Elsevier
2. Nihad A. Hassan, "Digital Forensics Basics - A Practical Guide Using Windows OS" Apress
3. Clint P Garrison "Digital Forensics for Network, Internet, and Cloud Computing A forensic evidence guide for moving targets and data , Syngress Publishing, Inc. 2010
4. Bill Nelson Amelia Phillips Christopher Steuart , Guide to Computer Forensics and Investigations: Processing Digital Evidence, Cengage Learning
5. Nilakshi Jain, Dhananjay Kalbande, "Digital Forensic : The fascinating world of Digital Evidences " Wiley India Pvt Ltd 2017.
6. Cory Altheide, Harlan Carvey "Digital forensics with open source tools "Syngress Publishing, Inc. 2011.

CDS-352
Title: Cyber Threat Intelligence

Teaching Scheme	**No. of Credits**	**Examination Scheme**
4hours / week	4	CA :30 marks UA: 70 marks

Prerequisites

1. Cyber Security Fundamentals
2. Basics of Python
3. Good Programming skills

Course Objectives: -

1. To understand the fundamentals of Cyber threats.
2. To understand the basic techniques to defend against the threats.
3. To apply appropriate tool for ensuring security of any system.

Course Outcomes: - Student will be able to :-

1. Detecting and Responding to Advanced Cyber Attacks
2. to defend against the cyber-attacks.
3. to understand to use appropriate technique for the cyber-attacks.

Course Contents

Chapter 1	**Introduction to Threat Intelligence**	**4 hours**

1.1 An Introduction to Threat Intelligence and Cross-Organizational Information Sharing
1.2 Benefit of Threat Information Sharing
1.3 Challenges of Threat Information Sharing
1.4 Creating Cyber Threat Information
1.5 Types of Cyber Threat Information
1.6 Cornerstones of Threat Information Sharing Activities
1.7 Establish Cyber Threat Intelligence Sharing Capabilities
1.8 Participating in Threat Information Sharing Relationships
1.9 The Role of Nation-States as Enablers of Information Sharing

Chapter 2	**Attack Scenarios and Involved Threat Actors**	**8 hours**

2.1 Introduction
2.2 The Definitions of Cybersecurity in a Nutshell.
2.3 On Cyber Attacks, Cybercrime, and Cyberwar: Emerging Trends and Threats
2.3.1 Emerging Technologies and Threat Trends in Cyberspace
2.3.2 APT Characteristics
2.3.3 Cyber Kill Chain
2.3.3.1 Step 1: Reconnaissance
2.3.3.2 Step 2: Weaponization
2.3.3.3 Step 3: Delivery

2.3.3.4 Step 4: Exploitation and Initial Intrusion 2.3.3.5 Step 5: C2 and Lateral Movements 2.3.3.6 Step 6: Actions of Intent		
Chapter 3	**Monitoring, Logging, and Network Analysis to Threat Intelligence Extraction**	**4 hours**
3.1 Introduction 3.2 An Overview of Concepts in Cyber Threat Intelligence 3.3 Raw Monitoring Data: Origin, Structure, and Insights 3.4 Evaluation and Analysis of Monitoring Data to Derive Cyber		
Chapter 4	**Information Sharing**	**8 hours**
4.1 Introduction 4.2 The Dimensions of Information Sharing 4.3 Dimension I: Efficient Cooperation and Coordination 4.4 Dimension II: Legal and Regulatory Landscape 4.5 Dimension III: Standardization Efforts 4.6 Dimension IV: Regional and International Implementations 4.7 Dimension V: Technology Integration into Organizations. 4.8 Review of Cyber Incident Information-Sharing Aspects		
Chapter 5	**Cyber Threat Intelligence**	**10 hours**
5.1 Introduction 5.2 The Promise of Intelligence Communities 5.3 CTI Community Structures 5.4 Organizational Context of a CTI Community 5.5 Tooling and Infrastructure 5.6 Case Studies 5.7 Community Enrichment and Enhancements		
Chapter 6	**Situational Awareness for Strategic Decision Making**	**6 hours**
6.1 Introduction 6.2 An Overview of National and International Cybersecurity Strategies 6.3 Cybersecurity Centres and Their Responsibilities and Tasks 6.4 Situational Awareness Models Supporting Strategic Decision-Making Processes 6.5 Information and Sources for Situational Awareness at the National Level.		
Chapter 7	**Legal Implications of Information Sharing**	**4 hours**
7.1 Introduction 7.2 Mapping the EU Cybersecurity Legal Framework 7.3 Information Sharing: Breaches, Threats, and Best Practices 7.4 Legal Certainty, Information Sharing, and Potential Legal Barriers to Data Transfer		
Chapter 8	**Legal Implications of Information Sharing**	**4 hours**
8.1 Introduction 8.2 Case Study 1: Distribution of Security-Relevant Information Containing Personal Data and Anonymization 8.3 Case Study 2: Harm to Reputation of Third Parties 8.4 Case Study 3: Information Leakage of Threat Intelligence, Incident Data, and Status Data 8.5 Case Study 4: Harm due to Disproportionate Mitigation Measures 8.6 Case Study 5: Legal Implications of the Involvement of Service Providers		

Chapter 9	Real-World Implementation of an Information Sharing Network	4 hours
9.1 Introduction 9.2 Overall Architecture and Technologies to Implement a National TI Framework 9.3 Roles, Responsibilities, and Processes within the National TI Framework 9.4 Description of Application Cases for the EU FP7 Project ECOSSIAN 9.5 Lessons Learned and Recommendations for a Large-Scale Rollout		
Reference Books: **1. Collaborative Cyber Threat Intelligence edited By Florian Skopik** **2. Cyber Threat! How to Manage the Growing Risk of Cyber Attacks By N. MACDONNELL ULSCH**		

CDS-353 **Title: Information Security Policy and Audit**		
Teaching Scheme **4 hours / week**	**No. of Credits** **4**	**Examination Scheme** **CA :30 marks** **UA: 70 marks**
Prerequisites: 1.Basics of ethical hacking 2.Knowledge of Network Security and Cryptography		
Course Objectives: **1.** To introduce the fundamental concepts and techniques in Information and Network security **2.** To give students an overview of Information security and Auditing **3.** To expose students to the concepts in Organization Security and Controls		
Course Outcomes: 1. Students will be able to describe fundamental concepts of information security and systems auditing 2. Analyze the latest trend of computer security threats 3. Identify security weaknesses in information systems and find appropriate solution for security mechanism 4. Explain the security controls in the aspects of physical, logical and Operational security control 5. Critically evaluate the security of information systems and audit		
Course Contents		

Chapter 1	Introduction to Information Security and IS Auditing	6 hours

1.1 Objectives of IS audit and control
1.2 The structure of an IS audit and audit reports
1.3 IS auditing standards
1.4 Computer assisted audit tools

Chapter 2	Organization Security and Controls	12 hours

2.1 Physical security controls
2.1.1Contingency plan
2.1.2 Disaster recovery and reconstruction
2.2 Logical security controls
2.2.1 Operating system security and access control
2.3 Operating controls
2.3.1. Segregation of duties
2.3.2. Monitoring and logging controls
2.4 Personnel security and management practices
2.4.1 User training and incident reporting
2.4.2 Third-party access and outsourcing
2.5 Application software control
2.5.1 Software development control
2.5.2 Input, processing and output control

Chapter 3	Domains of IT Security	6 hours

3.1 User/ accepted usage/access, data access, physical access, Internet access, e-mail, digital signature, outsourcing
3.2 Software development and acquisition, hardware acquisition
3.3 Domains related security based Case studies

Chapter 4	Basics of Cryptographic Technologies	6 hours

4.1 Symmetric encryption
4.2 Asymmetric encryption
4.3 Basics of message authentication and cryptographic hash functions
4.4 Digital signatures and digital certificates
4.5 Public-key Infrastructure & Web of Trust

Chapter 5	IT Governance	8 hours

5.1 Concept of IT Governance
5.2 Features of Good governance
5.3 Objectives and dimensions
5.4 Introduction to IT governance framework: COBIT, ISO/IEC 27001/27002

Chapter 6	Host Security & Network Security– Attack & Defense	10 hours

6.1 Virus, Worm, Trojan Horse, Rootkit, Stealth

6.2 Network Attacks
6.2.1 Host based attacks
6.2.2 Network attacks
6.2.3 Web based attacks
6.3 Network Defense
6.3.1 Intrusion detection systems & firewall
6.3.2 IPSec and DNSSec
6.3.3 IPv6
6.3.4 Cloud computing

Chapter 7	**Information System Security Auditing and Other Security Technologies**	**12 hours**

7.1 Auditing concepts a need, standards, performance
7.2 Security auditing and security standards
7.3 Incident handling and computer forensic
7.4 Other security technologies including blockchain

Reference Books:

1. S. Khilari, Information Security and Audit, Everest Publishing house, 2015
2. Mark Stamp, Information Security: Principles and Practice, Wiley Publication, 2018
3. William Stallings and Lawrie Brown, Computer Security Principles and Practice, (3rd Edition), Pearson, 2014
4. Bruce Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, 2015
5. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno,Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, 2010.
6. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Software Security Engineering: A Guide for Project Managers, Addison-Wesley, 2008.
7. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley, 2008.
8. Eric Cole, Network Security Bible, 2nd Edition, Wiley, 2009.

eBooks:
https://www.academia.edu/26365341/_2_2_Full_Book_Information_Security_and_Audit_

Savitribai Phule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-354
Title: Lab on CDS-351

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	**2**	**CA:15 marks** **UA: 35 marks**

Course Objectives: -

The course should enable the student:

- Describe digital forensics and relate it to an investigative process.
- Practice the basic digital forensic investigations.
- Understand and use different digital forensic tools.
- Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.

The students should be able to:

- Perform basic digital forensics.
- Demonstrate use of digital forensics tools.
- Guide a digital forensics exercise.
- Recognize the state of the practice and the gaps in technology, policy, and legal issues.

Practical List

Assignment No. 1: (2 slots)

- Creating a Forensic Image using FTK Imager/Encase Imager :
  - Creating Forensic Image
  - Check Integrity of Data
  - Analyze Forensic Image

Assignment No. 2: ((2 slots)

- Data Acquisition:
  - Perform data acquisition using:
  - USB Write Blocker + FTK Imager

Assignment No. 3: (2 slots)

- Forensics Case Study: Solve the Case study (image file) provide in lab using Encase Investigator.
- Forensics Case Study: Solve the Case study (image file) provide in lab using Autopsy.

Assignment No. 4: (2 slots)

- Recovering and Inspecting deleted files
  - Check for Deleted Files
  - Recover the Deleted Files
  - Analyzing and Inspecting the recovered files

Assignment No. 5: (2 slots)

- Web Browser Forensics.
  - Web Browser working
  - Forensics activities on browser
  - Cache / Cookies analysis

- Last Internet activity

Assignment No. 6: (2 slots)

- Capturing and analyzing network packets using Wireshark (Fundamentals) :
  - Identification the live network
  - Capture Packets
  - Analyze the captured packets

Assignment No. 7: (2 slots)

- Analyze the packets provided in lab and solve the questions using Wireshark :
  - What web server software is used by www.snopes.com?
  - About what cell phone problem is the client concerned?
  - According to Zillow, what instrument will Ryan learn to play?
  - How many web servers are running Apache?

Assignment No. 8: (2 slots)

- Using Sysinternals tools for Network Tracking and Process Monitoring :
  - Check Sysinternals tools
  - Monitor Live Processes
  - Capture RAM
  - Capture TCP/UDP packets
  - Monitor Hard Disk
  - Monitor Virtual Memory
  - Monitor Cache Memory

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS-355
Title: Lab on CDS-352

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CA:15 marks UA: 35 marks

Prerequisites

1. Cyber Security Fundamentals
2. Basics of Python
3. Good Programming skills
-

Course Objectives: -

1. To understand the fundamentals of Cyber threats.
2. To understand the basic techniques to defend against the threats.
3. To apply appropriate tool for ensuring security of any system.

Course Outcomes: - Student will be able to :-

1. Detecting and Responding to Advanced Cyber Attacks
2. to defend against the cyber-attacks.
3. to understand to use appropriate technique for the cyber-attacks.

Assignment No. 1:
- Threat Intelligence using search engines
- Google Dork

Assignment No. 2:
- Introduction to Threat analysis
- Threatcrowd.org
- Netcraft

Assignment No. 3:
- Threat Intelligence using amass OWASP

Assignment No. 4:
- IP and Domain reputation check
- MX Toolbox • AbuseDb

The harvester • Recon-ng

Assignment No. 5:
- Introduction to Dark Web
- Dark web search
- TOR

Assignment No. 6:
- Introduction to OSINT • Shodan
- OSTrICa - Open-Source Threat Intelligence Collector
- Maltego

Assignment No. 7:
- Introduction to email header search

- Manual search for email header
- https://mha.azurewebsites.net/ Microsoft email header analysis

Assignment No. 8:

- Introduction to DNS info • WHOIS
- Nslookup

Assignment No. 9:

- Introduction to Social engineering
- SE Tool Kit

Savitribai Phule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-356
Title: Lab on CDS-353 (Information Security Policy and Audit)

Teaching Scheme	No. of Credits	Examination Scheme
2hours / week	2	CA:15 marks UA: 35 marks

Course Objectives: -The course should enable the student:

- To obtain practical knowledge of Information Security
- To learn IS Auditing standards
- To understand the different domains of IT Security
- To gain knowledge about Cryptographic Technologies

The students should be able to:

1. Solve Case studies related to Information Security and Audit
2. Analyze Security controls
3. Apply cryptographic technologies
4. Perform basic level Information Security Audit

Practical List

Assignment No. 1: (1 slot)
Case study on IS Auditing standards
https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=2261&context=masters-theses

Assignment No. 2: (1 slot)
Case study on Security controls
https://cyphra.com/case-studies/professional-services-case-study-security-controls/

Assignment No. 3: (2 slots)
Case study on domains of IT security
https://journals.sagepub.com/doi/full/10.1177/0972150917721836

Assignment No. 4: (2 slots)
Case study on Cryptographic Technologies
https://www.cryptomathic.com/customers/case-studies

Assignment No. 5: (2 slots)
Case study on IT Governance
https://www.itgovernanceusa.com/case-studies
.

Assignment No. 6: (2 slots)
Case study on Host Security and Network Security
https://www.ouritdept.co.uk/wp-content/uploads/2017/09/Antivirus-Case-Study.pdf

Assignment No. 7: (2 slots)
Case study on Information Security Audit
https://www.altiusit.com/casestudies.htm

Savitribai Phule Pune University
T.Y.BSc Cyber and Digital Science
CDS-357A
Title: Mobile Forensics

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CA:15 marks UA:35 marks

Prerequisites
1. Knowledge of Networking and its Techniques

Course Objectives:-

1. To identify the unique challenges involved in mobile forensics.
2. Explain and apply the procedures of the validation, preservation, acquisition, examination, analysis and reporting of digital information from a mobile device.
3. Explain and compare thehardware, OS architectures and file systems.
4. Explain and compare various data acquisition and analysis techniques used in mobile forensics.
5. Analyze the extracted data to identify and examine important case data such as contacts, call logs, SMS, images, audio and video files, web history, passwords, application data.
6. Apply industry best practices to evidence collection and analysis with hands-on exercises using current tools.

Course Outcomes:- Student will be able to :-
1. understand the cellular network and mobile device hardware
2. Learn mobile forensics process in detail
3. Understand mobile devices and its forensics
4. Understand and use mobile forensics tools

Course Contents

Chapter 1	**Fundamentals of Mobile Devices and Cellular Network**	**5 hours**

1.1. Cellular Network
1.1.1. Evolution of Cellular Network and its History
1.1.2. Cellular Network Architecture and Technologies
1.2. Mobile Device Hardware
1.2.1. Evolution of Mobile Device and its History
1.2.2. Mobile Device Architecture and Technologies
1.2.3. Mobile Operating Systems
1.3. Smart Cards
1.3.1. Subscriber Identification Module (SIM/USIM)
1.3.2. SIM/USIM File Management
1.3.3. SIM/USIM Security

Chapter 2	Mobile Forensics Process	**14 hours**

2.1.Mobile Forensic and its Challenges
2.2. Mobile Forensics Process
2.1.1. Preservation

2.1.2. Acquisition
2.1.3. Examination and Analysis
2.1.4. Reporting
2.3. Acquisition Methods
2.2.1. Manual Acquisition
2.2.2. Logical Acquisition
2.2.3. Physical Acquisition
2.2.4. File-System Acquisition
2.2.5. JTAG and Chip-Off Acquisition
2.4. Emerging Techniques in Mobile Forensics

Chapter 3	Mobile Device Forensics	**8 hours**

3.1. Android, BlackBerry, iOS and Windows Mobile Forensics
3.2. Artefacts Extraction
- 3.2.1. Contacts and Phone Call Artefacts
- 3.2.2. SMS Artefacts
- 3.2.3. Network and Location Artefacts
- 3.2.4. System Artefacts
- 3.2.5. Multimedia Files Artefacts

3.3. Data and File Carving
3.4. Deleted Files Recovery
3.5. Bypassing Security Controls2

Chapter 4	Mobile Forensics Tools	**9hours**

4.1.Cellebrite
- 4.1.1. Features of Cellebrite UFED Physical Analyser
- 4.1.2. Usage
- 4.1.3. Supported devices

4.2.Oxygen Forensics Suite
- 4.2.1. Features of Oxygen ForensicsSuite
- 4.2.2. Usage
- 4.2.3. Supported devices

4.3. Paraben iRecovery Stick
- 4.3.1. Features of Paraben iRecovery Stick
- 4.3.2. Usage
- 4.3.3. Supported devices

4.4. Open-Source Mobile Forensic Tools

Reference Books:

7. Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing Ltd, 2014
8. Mobile Forensics, link : https://ec.europa.eu/programmes/erasmus-plus/project-result-content/9d82c6b2-d28c-441a-b165-e73b1a87736f/FORC%20Book%207.pdf

CDS-357B
Title: Cloud Security

Teaching Scheme	No. of Credits	Examination Scheme
3 hours / week	3	CA :15 marks UA: 35 marks

Prerequisites

1. CDS-121 Fundamentals of Cyber Security
2. CDS-123 Computer Networks
3. CDS-231 Basics of Ethical Hacking
4. CDS-243 Network Security and Cryptography

Course Objectives:

1. To understand the concepts of cloud computing
2. To know the data assets in cloud and its protection
3. To know various cloud assets and security
4. To apply the Identity Asset Management (IAM) concept in cloud

Course Outcomes: Student will be able to

1. learn the fundamentals of cloud computing and its models
2. learn data, storage and network security mechanism in cloud environment

Course Contents

Chapter 1	**Cloud Computing Fundamentals**	**5 hours**

1.1. What is Cloud Computing?
- 1.1.1 Definition
- 1.1.2 Essential Characteristics

1.2. SPI Framework for Cloud Computing
- 1.2.1. Relevant Technologies in Cloud Computing
- 1.2.2. Cloud Services Delivery Model - Software as a Service(SaaS), Platform as a Service(PaaS), Infrastructure as a Service(IaaS)
- 1.2.3. Cloud Deployment Models - Public Clouds, Private Clouds, Hybrid Clouds, Community Clouds

Chapter 2	**Data Asset Management and Protection**	**8 hours**

2.1 Data Identification and Classification
2.2 Example data classification levels
2.3 Data Asset Management in Cloud - Tagging cloud resources
2.4 Protecting Data in the Cloud
- 2.4.1 Tokenization
- 2.4.2 Encryption – In motion, In use, At rest

Chapter 3	**Cloud Asset Management and Protection**	**8 hours**

3.1 Type of Cloud Assets
- 3.1.1 Compute Assets
- 3.1.2 Storage Assets
- 3.1.3 Network Assets

3.2 Asset Management Pipeline
- 3.2.1 Procurement Leaks
- 3.2.2 Processing Leaks

3.2.3 Tooling Leaks 3.2.4 Finding Leaks 3.3 Tagging Cloud Assets		
Chapter 4	**Identity and Assess Management (IAM)**	**9 hours**
4.1 Life Cycle for Identity and Access 4.2 Request, Approve 4.3 Create, Delete, Grant, Revoke 4.4 Authentication 4.5 Authorization 4.6 Revalidate		

Reference Books:

9. **Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance**
   Authors: Tim Mather, Subra Kumaraswamy, Shahed Latif
   Publisher: O'Reilly Publication
10. **Cloud Security: A Comprehensive Guide to Secure Cloud Computing**
    Authors: Ronald L. Krutz and Russell Dean Vines
    Publisher: Wiley Publishing, Inc.
11. **Practical Cloud Security: A Guide for Secure Design and Deployment**
    Author: Chris Dotson
    Publication: O'Reilly Publication

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS-358A
Title:Lab on CDS-357A(Mobile Forensic)

Teaching Scheme	No. of Credits	Examination Scheme
2hours / week	2	CA:15 marks UA: 35 marks

Course Objectives: -The course should enable the student:

- To present the concepts of mobile forensics
- To Learn the mobile forensics tools

The students should be able to:

5. Find the 5G technologies affects in mobile forensics
6. Understand to explain the technical terms to a non-technical person
7. Use the mobile forensics tools and try various usages of them in real life

Practical List

Assignment No. 1: (1 slot)

- Identify two implications that might affect mobile forensic in the future as a result of the advancement in 5G technology.

Assignment No. 2: (2 slots)

- Record a video explaining what Sim cards are in non-technical terms (5 minutes maximum). Imagine that you are explaining them to ateacherwith no technical background

Assignment No. 2: (2 slots)

- Compare between the different data acquisition methods explained in the textbook in terms of the data that each method can recover, complexity, requirements, supports by forensics tools, and when it should be used.

Assignment No. 3: (2 slots)

- Use Oxygen Forensics Suite and extracts the following data: phonebook with assigned photos, calendar events and notes, call logs, messages, camera snapshots, video and music

Assignment No. 4: (2 slots)

- Use Oxygen Forensics Suite and extracts the following data: phonebook with assigned voice mail, passwords, dictionaries, and coordinates, IP connections, locations, navigation applications, device data, factory installed, third-party applications data

Assignment No. 5: (2 slots)

- Use Paraben iRecovery Stick and recover the following data: deleted data from SQLite databases, messages, contacts, call history

Assignment No. 6: (3 slots)

- Use Paraben iRecovery Stick and extracts the following data: deleted data from Internet history and calendar events

Savitribai Phule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-358B
Title: Lab course on Cloud Security (CS-357B)

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CA:15 marks UA: 35 marks

Course Objectives: -The course should enable the student:

- To understand the mechanism to setup virtual machines/servers instances cloud platform
- To acquire the knowledge of how to setup security on own virtual instances in cloud

The students should be able to:

8. Setup own Amazon EC2 instances on cloud
9. Setup infrastructure and data security
10. Apply Identity and Access Management (IAM) policies on cloud instances
11. Define customized security groups

Practical Assignment List

Following Lab Assignments are to be performed on Amazon EC2 (Elastic Compute Cloud) platform to learn Cloud Services and Security

Assignment No. 1: Setup Amazon EC2 (2 slots)

- Understand Amazon EC2 and Services
- Signup for AWS (Amazon Web Services)
- Create Key Pair
- Create Security Group

Assignment No. 2: Amazon EC2 Linux Instances (2 slots)

- Launch, Connect and Cleanup Instances
- Perform Best Practices on Instances
  - Security, Storage, Resource Management, Backup and Recovery, Networking
- Use and Create AMI (Amazon Machine Images)

Assignment No. 3: Infrastructure and Data Security in Amazon EC2 (2 slots)

- Setup Infrastructure Security
- Setup Data Resilience and Protection

Assignment No. 4: Identity and Access Management (IAM) (2 slots)

- Define Network access to instance
- Setup Permissions
- Define IAM policies roles

Assignment No. 5: Key Pairs (2 slots)

- Create key pairs
- Tag and Describe public key
- Add and Remove public keys on instances

Assignment No. 6: Security Groups (2 slots)

- Setup default and custom security groups

- Connection tracking
- Work with security groups

Reference Books:

- **AWS Cookbook**
  Authors: John Culkin, Mike Zazon
  Publisher: O'Reilly
- **Mastering AWS Security**
  Author: Albert Anthony
  Publisher: Packt Publishing

Amazon EC2 Documentation:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf#concepts

SavitribaiPhule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-361
Title:Digital Forensics-2

Teaching Scheme	No. of Credits	Examination Scheme
4hours / week	4	CA :30 marks UA: 70 marks

Prerequisites:-

3. **Knowledge of Computer Networks**
4. **Knowledge of Cryptography and Network Security**
5. **Basic concepts of Digital Forensics**

Course Objectives:-

7. To understand underlying principles behind email and social media investigation
8. To understand basic concepts and procedures for mobile forensics.
9. To learn techniques behind multimedia forensics
10. To apply digital forensic knowledge to investigate cloud, network and virtual machine data.

Course Outcomes:-

After completion of the course student will be able to :-

6. Explain how to apply digital forensics methods to investigating email and social media communications
7. Trace, recover, and analyze e-mail messages by usingforensics tools
8. Describe procedures for acquiring data from mobile devices
9. Retrieve information from mobile devices
10. To examine and recover graphics files
11. Explore procedures for virtual machine forensics, live acquisitions, and network forensics.

Course Contents

Chapter 1	**E-Mail and Social Media Investigation**	**10 hours**
1.8.	Exploring the role of email investigation	
1.9.	Exploring the role of client and server in email	
1.10.	Investigating E-mail crimes and violations	
	1.3.1 Examining E-mail Messages	
	1.3.2 Viewing E-mail headers	

1.3.3 Examining E-mail headers

1.3.4 Examining additional E-mail files

1.3.5 Tracing an e-mail message

1.3.6 Using network E-mail logs

1.11. Understanding E-mail servers

1.3.1 Examining Unix and Microsoft email server logs

1.12. Applying Digital Forensics Methods to Social Media Communications

1.13. Social Media Forensics on Mobile Devices

1.14. Forensics Tools for Social Media Investigations

Reference book 1

Chapter 2	**Mobile Device Forensics**	**16 hours**

2.12 Why do we need mobile forensics?

2.13 Challenges in mobile forensics

2.14 The mobile phone evidence extraction process

2.15 Understanding mobile device forensics

2.1.5 Mobile phone basics

2.1.6 Inside mobile devices

2.2 Understanding acquisition procedures for cell phones and mobile devices

2.2.1 Mobile Forensics Equipment

2.2.2 Mobile Forensics Tools

2.3 The Android model, file system and hierarchy

2.4 Android Data Extraction Techniques

2.4.1 Manual data extraction

2.4.2 Logical data extraction: ADB pull data extraction , Using SQLite Browser to view the data, Extracting device information , Extracting call logs , Extracting SMS/MMS , Extracting browser history , Analysis of social networking/IM chats

2.4.3 Physical data extraction: Imaging an Android Phone, Imaging a memory (SD) card

2.5 Android data analysis and recovery

2.5.1 Analyzing an Android image using Autopsy

2.5.2 Recovering deleted data from external SD card

2.5.3 Recovering data deleted from internal memory

2.5.4 Recovering deleted files by parsing SQLite files

2.5.5 Recovering files using file carving techniques

2.5.6 Recovering contacts using your Google account

Reference book 1 and 2

Chapter 3	**Multimedia Forensics**	**12 hours**

3.11 Graphics File formats

i. Understanding Bitmap and Raster Images

ii. Understanding Vector Graphics

iii. Understanding Metafile Graphics

iv. Understanding Graphics File Formats

v. Understanding Digital Photograph File Formats

3.12 Understanding Data Compression

3.2.1 Lossless and Lossy Compression

3.2.2 Locating and Recovering Graphics Files

3.2.3 Identifying Graphics File Fragments

3.2.4 Repairing Damaged Headers

3.2.5 Searching for and Carving Data from Unallocated Space

3.2.6 Rebuilding File Headers

3.2.7 Reconstructing File Fragments

3.13 Identifying Unknown File Formats

3.3.1 Analyzing Graphics File Headers

3.3.2 Tools for Viewing Images

3.14 Understanding Steganography in Graphics Files

3.4.1 Using Steganalysis Tools

3.15 Understanding Copyright Issues with Graphics

Reference Book 1

Chapter 4	**Cloud Forensics**	**12 hours**

4.7 An Overview of Cloud Computing

4.1.1 Cloud Service Levels and Deployment Methods

4.1.2 Cloud Vendors

4.1.3 Basic Concepts of Cloud Forensics

4.8 Legal Challenges in Cloud Forensics

4.2.1 Service Level Agreements

4.2.2 Jurisdiction Issues

4.2.3 Accessing Evidence in the Cloud

4.9 Technical Challenges in Cloud Forensics

4.3.1 Architecture, Analysis of Cloud Forensic Data

4.3.2 Anti-Forensics, Incident First Responders, Role Management

4.4 Encryption in the Cloud

4.4.1 Conducting a Cloud Investigation

4.4.2 Investigating CSPs

4.4.3 Investigating Cloud Customers

4.4.4 Understanding Prefetch Files

4.4.5 Examining Stored Cloud Data on a PC

4.4.6 Windows Prefetch Artifacts

4.5 Tools for Cloud Forensics

Reference Book 1

Chapter 5	**Virtual Machine Forensics, Live Acquisitions, and Network Forensics**	**10hours**

5.5 An Overview of Virtual Machine Forensics

i. Type 2 Hypervisors

ii. Conducting an Investigation with Type 2 Hypervisors

iii. Working with Type 1 Hypervisors

5.6 Performing Live Acquisitions

5.2.1 Performing a Live Acquisition in Windows

5.7 Network Forensics Overview

5.3.1 The Need for Established Procedures

5.3.2 Securing a Network

5.3.3 Developing Procedures for Network Forensics

5.3.4 Investigating Virtual Networks

5.3.5 Examining the Honeynet Project

Reference Book 1

Reference Books:

12. Bill Nelson Amelia Phillips Christopher Steuart , Guide to Computer Forensics and Investigations: Processing Digital Evidence, Sixth Edition, Cengage Learning

13. Heather Mahalik, RohitTamma, Satish Bommisetty, Practical Mobile Forensics,

Second Edition, Packt Publishing

14. John Sammons,"The Basics of Digital Forensics - The Primer for Getting Started in Digital Forensics"*Syngress,* Elsevier
15. Nihad A. Hassan, "Digital Forensics Basics - A Practical Guide Using Windows OS" Apress
16. Clint P Garrison "Digital Forensics for Network, Internet, and Cloud Computing A forensic evidence guide for moving targets and data , Syngress Publishing, Inc. 2010
17. Nilakshi Jain, DhananjayKalbande, "Digital Forensic : The fascinating world of DigitalEvidences " Wiley India Pvt Ltd 2017.
18. Cory Altheide, Harlan Carvey "Digital forensics with open source tools "Syngress Publishing,Inc. 2011.

.

SavitribaiPhulePuneUniversity

T.Y.Cyber and Digital ScienceSemester–VI

CourseCode: CDS 362

SubjectName:Cyber Law(Information Security Policies and Strategies)

TotalHours:60 lectures

Teaching Scheme 4 hours/ week	**Number of Credits 4**	**Examination Scheme** **CA : 30 Marks** **UA : 70 Marks**

Prerequisites: -

- Fundamentals of Cyber Securities.

Course Objectives:

- To understand the fundamentals of cyber security.
- To understand the computer security issues
- To Understand Information secure system planning and Security Policies.

Course Outcome: -

- Have a good understanding of Cyber Security and the Tools
- Develop The Understanding of, how to make secure system planning,
- Make Learner to develop standard and policies

Chapters	Topic	No ofHours
1	**Chapter1:-Introductionto CyberCrimeand CyberSecurity** 1.1 Introduction 1.2 Cybercrime: DefinitionandOriginoftheWord 1.3 CybercrimeandInformationSecurity 1.4 WhoareCybercriminals? 1.5 ClassificationsofCybercrimes: E-MailSpoofing, Spamming, Cyber defamation, Internet Time Theft,Salami Attack/Salami Technique, Data Diddling,Forgery, Web Jacking,Newsgroup,Spam/CrimesEmanatingfromUsenetNewsgroup,IndustrialSpying/IndustrialEspionage, Hacking,OnlineFrauds,ComputerSabotage,EmailBombing/MailBombs, Computer Network Intrusions, PasswordSniffing,CreditCardFrauds,IdentityTheft 1.6 DefinitionofCyberSecurity 1.7 Vulnerability,ThreatsandHarmfulacts 1.8 CIATriad 1.9 CyberSecurityPolicyand DomainsofCyberSecurityPolicy	10
2	**Chapter2 :-Cybercrimesand Cybersecurity:TheLegalPerspectives** 2.1 Introduction 2.2 cCybercrimeandtheLegalLandscapearoundtheWorld 2.3 WhyDoWeNeedCyberlaws:TheIndianContext 2.4 TheIndianIT Act 2,5 ChallengestoIndianLawandCybercrimeScenarioinIndia 2.6 ConsequencesofnotAddressingtheWeakness inInformationTechnologyAct 2.7 DigitalSignaturesandtheIndianITAct 2.8 AmendmentstotheIndianITAct 2.9 CybercrimeandPunishment 2.10 Cyberlaw,TechnologyandStudents:IndianScenario	10

3	Cybersecurity: Organizational Implications 3.1 Organizational Implications: Cost of cybercrimes and IPR issues 3.2 Web threats for organizations 3.3 Security and Privacy Implications from Cloud Computing 3.4 Social media marketing 3.5 Social computing and the associated challenges for organizations, Protecting people's privacy in the organization 3.6 Organizational guidelines for Internet usage and safe computing guidelines and computer usage policy 3.7 Incident handling 3.8Intellectualpropertyinthecyberspaceofcybersecurity.	8
4	INFORMATION SECURITY POLICIES **4.1 Introduction** 4.2 Corporate Policies 4.3 Organizationwide (Tier 1) Policies 4.4 Organizationwide Policy Document 4.5 Legal Requirements 4.6 Duty of Loyalty 4.7Duty of Care 4.8 Other Laws and Regulations 4.9 Business Requirements 4.10 Where to Begin?	8
5	**Planning and Preparation** 5.1 Introduction 5.2 Objectives of Policies, Standards, and Procedures 5.3 Employee Benefits 5.4 Preparation Activities 5.5 Core and Support Teams 5.6 Focus Groups 5.7 What to Look for in a Good Writer and Editor 5.8 Development Responsibilities 5.9 Other Considerations 5.10 Key Factors in Establishing the Development Cost 5.11 Reference Works 5.12 Milestones 5.13 Responsibilities 5.14 Development Checklist	9
6	**Developing Policies** 6.1 Policy Is the Cornerstone 6.2 Why Implement Information Security Policy? 6.3 Some Major Points for Establishing Policies 6.4 What Is a Policy? 6.5 Definitions 6.6 Policy Key Elements 6.7 Policy Format	5

7	**Developing Standards** 7.1 Do Standards Belong? 7.2 What Does a Standard Look Like? 7.3 Where Do I Get the Standards? 7.4 Sample Information Security Manual	5
8	**Developing Procedures** 8.1 Introduction 8.2 Important Procedure Requirements 8.3 Key Elements in Procedure Writing 8.4 Procedure Checklist 8.5 Getting Started 8.6 Procedure Styles 8.7 Procedure Development Review	5

ReferencesBooks:

1. CyberSecurityUnderstandingCyberCrimes,ComputerForensicsandLegal Perspectives–NinaGodbole,SunitBelapure,Wiley:April2011India PublicationsReleased.

2 .Thomas R. Peltier, “Information Security policies and procedures: A Practitioner’s Reference”, 2nd Edition Prentice Hall, 2004.

3. PrinciplesofInformationSecurity,-MichaelEWhitman, HerbertJMattord,3rdEdition, 2011.

Savitribai Phule Pune University

T.Y.B.Sc. (Cyber and Digital Science)

CDS-363

Title: Web Science

Teaching Scheme	No. of Credits	Examination Scheme
4 Hours / week	**4**	**CA :30 marks** **UA: 70 marks**

Prerequisites:

Fundamentals of any programming language like Python, PHP

Fundamentals of internet working

Fundamentals of GNU/Linux Operating System

Course Objectives

1. Understand Web versions
2. Understand the role of web in society and economy
3. Understand Web architecture and its applications
4. Understand basics of web security
5. Understand basics of web analysis

Course Outcomes: On completion of the course, student will be able to

1. Develop a simple web application
2. Access and develop web services
3. Provide security to the web application through authorization and authentication.

Course Contents

Unit 1	**Introduction To Web**	**5 hours**
	1.1 History of Web 1.2 Introduction to Web 1.0, Web 2.0 and Web 3.0 1.3 Building blocks of web 1.4 UniformResource Locator	
Unit 2	**Web Architecture**	**6 hours**
	2.1 Web browser, 2.2 Web Server 2.3 HTTP protocol	

Unit 3	**Approaches to Web Application Development**	**5 hours**
	3.1 Programmatic approaches 3.2 Template Approaches 3.3 Hybrid approaches	
Unit 4	**HTML and XML**	**10 hours**
	4.1 Introduction to HTML 4.2 HTML forms 4.3 Introduction to XML 4.4 Structure of XML 4.5 XML document structure 4.6 XML parser	
Unit 5	**Security Development Lifecycle**	**8 hours**
	5.1 Introduction to SDL 5.2 AGILE SDL	
Unit 6	**Server-Side Web Security**	**6 hours**
	6.1 SQL Injection attacks 6.2 Stored Procedure attack 6.3 SQL column truncation.	
Unit 7	**Authorization and Authentication**	**8 hours**
	7.1 Access control: 7.1.1 Horizontal rights management 7.1.2 Vertical rights management 7.2 Authentication: 7.2.1 Loophole in password security 7.2.2 Complex Password security and password Recovery	
Unit 8	**Web Services**	**12 hours**
	8.1 SOAP 8.2 WSDL 8.3 UDDI 8.4 Demo of Web services	
Reference Books:		
1. Web Application Architecture Principles, protocols and practices by Leon Shklar Richard Rosen, John Wiley and Sons, Ltd 2. WEB SECURITY A WhiteHat Perspective by Hanqing Wu and Liz Zhao, CRC Press.		

SavitribaiPhule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-364
Title:Lab on CDS-361

Teaching Scheme	No. of Credits	Examination Scheme
2hours / week	**2**	**CA:15 marks** **UA: 35 marks**

Course Objectives: -

The course should enable the student:

- Describe digital forensics and relate it to an investigative process.
- Practice advanced digital forensic investigations.
- Understand and use different digital forensic tools.

The students should be able to:

- Perform basic digital forensics.
- Demonstrate use of digital forensics tools.
- Guide a digital forensics exercise.

Practical List

Assignment No. 1: Inspecting Emails (2 slots)

Use any web-based email such as gmail or yahoo and view the email headers. For gmail, Open an e-mail, click the down arrow next to the Reply arrow, and click Show original. Click the Download Original link and inspect the header. Identify various parts of the header such as servers, domain keys, attachment type, etc.

Answer the following questions:

1.What is the name and file type of the base64 encoded attachment?

2. To which email was this file attached?Identify two pieces of data that tell you that.

3. Who was this email sent from, to, and when was it sent?

4. In what time zone does the computer that was used to send the email reside(presuming it corresponds to the time zone setting for the computer)?What data inthe header tells you that?

5.In what time zone does the sender's mail server reside (presuming it corresponds tothe time zone setting for the computer)?What data in the header tells you that?

6.If you believed the source email address information has been spoofed, whichspecific IP address would you resolve, and subsequently contact the owner of, to findout who might have really sent the email?

Assignment No. 2: Accessing mobile data (3 slots)

adb is a command-line tool that helps you communicate with the device to retrieve information. Using adb, you can extract data from all the files on the device or only the relevant files in which you are interested.

Autopsy® is the premier end-to-end open source digital forensics platform.

i. Extracting device information of your android device

ii. Use the SQLite Browser to display call logs

iii. Display all call logs

iv. View browser history information

Assignment No. 3: Extracting social media data (2 slots)
Extract data from any social media application such as facebook/whatsapp etc. an display relevant information

Assignment No. 4:Accessing mobile device data (2 slots)
Create an image of your phone data
Inspect the contents and note your observations.

Assignment No. 5: Recovering deleted files on mobile device (2 slots)
Use autopsy tool to analyze the Android image of your phone
Recover deleted SMS's on your android device
Recover contacts using google

Assignment No. 5:Multimedia forensics (2 slots)

- Use Autopsy and Exif Reader for this assignment
- i. Extract metadata of any jpg, png and bmp image on your computer

Assignment No. 6: Cloud Forensics (2 slots)
Use the WinHex editor to perform the following operations:
Find out the last time you accessed Google Drive on your computer.
Find the number of times this program hasbeen run
Find the detailed list of a user's cloud transactions and list the create, modify, and delete dates and times

Assignment No. 7: Virtual Machine and Network Forensics(3 slots)

Using VMware Workstation Player and FTK Imager Lite, examine
yourown system for evidence of a VM.
Acquire a forensic image of the host computer(the physical machine the VM runs on) as well as network logs
Extract and examineFiles associated with VMs, such as log files to determine the crime or incident's timeline and to findrelevant information, such as Web sites and network files that were accessed as well asdownloads that occurred from the VM's IP address

Examine network traffic using the tcpdump command-line program(www.tcpdump.org),
Using a network analysis tool such as Wiresharkto generate a list of the top 10 Web sites users in the network arevisiting.

SavitribaiPhule Pune University
T.Y.B.Sc. (Cyber and Digital Science)
CDS-365
Title:Lab on CDS-362 (Information Security Policies and Strategies**)**

Teaching Scheme	No. of Credits	Examination Scheme
2hours / week	2	CA:15 marks UA: 35 marks

Course Objectives: -The course should enable the student:

- To obtain practical knowledge of Information Security
- To learnIndian IT Acts.
- To understand the different cybercrimes and cyberLaw

The students should be able to:

12. Solve Case studies related to Information Security Policies and Strategies
13. Study if Indian IT Acts.
14. Study of Security standard.
15. Perform basic level Information Security policies.

Practical List

Assignment No. 1: (2 slot)
Case study on CybercrimeScenarioinIndia

Assignment No. 2: (2 slot)
Case study on TheIndianIT Act

Assignment No. 3: (2 slots)
Case study on CybercrimeandPunishment

Assignment No. 4: (2 slots)
Case study on Cyberlaw,TechnologyandStudents:IndianScenario

Assignment No. 5: (2 slots)
Case study on Developing Information security Policies

Assignment No. 6: (2 slots)
Case study on Developing security Standards

Guideline to write case study
A case study example

1. Start with a clear headline. This should be gives the most important information. ...
2. Provide a snapshot. ...
3. Introduce the client. ...(if applicable)

4. State the problem, consequences, & hesitations. ...
5. Describe the solution. ...
6. Share the results & benefits. ...
7. Conclude with words of advice

Savitribai Phule Pune University

T.Y.B.Sc. (Cyber and Digital Science)

CDS-366

Title: Lab on CDS-363

Teaching Scheme	No. of Credits	Examination Scheme
4 hrs 20 mins / week	2	CA:15 marks UA: 35 marks

Course Objectives: -The course should enable the student:

- To obtain practical knowledge development of web applications.
- To gain hands-on practical on SQL injection, Web services.
- To grasp the understanding of importance of authorization and authentication in web application.

Course Outcomes: The students should be able to:

- Develop the simple Web applications
- Perform SQL injection attack analysis on web application and database.
- Implement basic web services.

Assignment 1. Use of HTML(2 Slots)

1. Design a webpage for the following layout For Student profile – where student roll number, name, contact, photo, class and area of interestin column 2. In Colum 1 provide the hyperlinks for Home, Contact us and about us.
2. Extend the above question, so that If user clicks on home menu the home page will be displayed, If user click on Contact us the contact of college will be displayed.
3. Create a form to accept student information (name, class, address) and marks (Physics, Biology, Chemistry, Mathematics, Marathi, English).

Assignment 2. Introduction to PHP(2 Slots)

1. Extend the Assignment 1 question number 2 to display the mark sheet for the student that contains name, class, marks of the subject, total and percentage.

2. Create a login form with a username and password. Display “Welcome” message if username and password is same otherwise display “Invalid username or password” message.

Assignment 3.Introduction to XML (2 Slots)

1. Write a script to create XML file named "Subject.xml".Stored at least 3 records containing subject id, subject name, class, semester etc.

2. Write a script to create "cricket.xml" file with multiple elements as given below

```
<Cricket  team>
<Country = India>
        <Player Name >--------    <Player Name >
        <Wickets>--------- </Wickets>
        <Runs>--------</Runs>
</Country>
</Cricket  team>
```

   Add at least 5 records in the file.

Assignment 4. Databases (2 Slots)

1. Using SQL injection attack on Login check whether you can log into another user's account without knowing the correct password.
2. To show the SQL injection attack on UPDATE statement, you need to make an unauthorized modification to the database by modifying another user's profile.

Assignment 5.Authorization and Authentication (2 Slots)

1. Design an application to accept username and password. While accepting password check whether is it made of numbers, alphabets, special symbols and password length should be greater than 8. If password is as per requirement, then print "You entered strong password" else print error message "Enter complex password".

2. Design an application that accept the full name, contact number, email-id, password and confirm password. If password and confirm password matched the store accept data into database while storing password encrypt it.

Assignment 6.Web Services (2 Slots)

1. Write a program to access online weather API.

2. Write a simple web service called Dairy Product Price Service. This keeps a

dairy product price table to record the different kinds of product prices. It will supply 3 services to the client so that clients can add product price, delete product price, update product prize

Assignment 7. Introduction OWASP

1) OWASP Top 10 threats for web introduction
2) OWASP Top 10 threats for API introduction

Assignment 8. Introduction to Web Security audit tools

1) OWASP ZAP scanner
2) Burp Suite Scanner

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS-367A
Title: Malware Analysis

Teaching Scheme	No. of Credits	Examination Scheme
4 hours / week	4	CA :30 marks UA: 70 marks

Prerequisites
1. Basic Python Programming
2. Basic Computer Hardware
3. Basic Assembly Programming

Course Objectives: -
1. Static and Dynamic Analysis of Malwares
2. Study of windows malwares in depth.
3. Study of linux malwares, Mac malwares, Android malware in brief.

Course Outcomes: - Student will be able to:-
1. classify the malwares and analyze them.
2. use the tools for analysis of any type of malware.
3. write own tools/programs for analyzing the malware.

Course Contents

Chapter 1	**Introduction**	**2 hours**

1.1. Malware – Definition, Types , Examples , Malicious Actions of Malwares
1.2. Malware Types (Based on OS)- Windows Malware, Linux Malware, Mac Malware, Android Malware.
1.2. Malware Analysis – Definition, need, Types

Chapter 2	**Static Analysis**	**4 hours**

2.1 Statis Analysis – Definition, techniques.
2.2 Techniques of static Analysis - Determining file type, fingerprinting the malware, Multiple antivirus scanning, extracting strings, Determining file obfuscation, Packers and Cryptors, Inspecting PE Header Information, Comparing And Classifying The Malware

Chapter 3	**Dynamic Analysis**	**4 hours**

3.1 System and network monitoring
3.2 Dynamic Analysis (Monitoring) Tools
3.3 Dynamic Analysis Steps
3.4 Analysing a Malware executable
3.5 Dynamic-Link Library (DLL) Analysis

Chapter 4	**Assembly Language and Disassembly Primer**	**4 hours**

4.1 Computer Basics
4.2 CPU Registers
4.3 Data Transfer Instructions
4.4 Arithmetic Operations

4.5 Bitwise Operations
4.7 Branching And Conditionals
4.8 Loops
4.9 Functions
4.10 Arrays and Strings
4.11 Structures
4.12 X64 Architecture

Chapter 5	**Disassembly Using IDA**	**4 hours**

5.1 Code Analysis Tools
5.2 Static Code Analysis (Disassembly) Using IDA
5.3 Disassembling Windows API
5.4 Patching Binary Using IDA
5.5 IDA Scripting and Plugins

Chapter 6	**Debugging malicious binaries**	**5 hours**

6.1 General debugging concepts
6.2 Debugging a binary using x64dbg
6.3 Debugging a binary using IDA
6.4 writing a debugging script in python
6.5 IDA Scripting and Plugins

Chapter 7	**Malware Functionalities and Persistence**	**5 hours**

7.1 Malware Functionalities:
Downloader, dropper, keylogger, Malware replication using removable media, Malware Command and Control(C2), PowerShell based execution
7.2 Malware Persistence Methods:
Run registry key, scheduled tasks, startup folder, winlogon registry entries, Image File Execution options, Accessibility Program, AppInit_DLLs, DLL Search Order Hijacking, COM hijacking, Service

Reference Books:

1. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, By Monnappa K A , Packt Publishing Limited
2. Android Malware and Analysis, By Ken Dunhum, Shane Hartman, Jose Andre Morales, Manu Quintans, Tim Strazzere
3. Learn Malware Analysis: Explore the Concepts, Tools and Techniques to Analyse and Investigate Malware, Sobia Publication
4. Malware Analysis Techniques: Tricks for the triage of adversarial software by Dylan Barker
5. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig
6. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware by Abhijit Mohanta and Anoop Saldanha
7. Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks by Alexey Kleymenov and Amr Thabet
8. Malware Analysis Techniques: Tricks for the triage of adversarial software by Dylan Barker
9. Windows Malware Analysis Essentials by Victor Marak

10. Cuckoo Malware Analysis by Digit Oktavianto and Iqbal Muhardianto
11. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code

Savitribai Phule Pune University
CDS-367B
Title: Fin tech- Cybersecurity

Teaching Scheme	No. of Credits	Examination Scheme
2hours / week	2	CA :15 marks UA: 35 marks

Prerequisites
1. Knowledge of Banking

Course Objectives:-
1. To understand financial technology management
2. To study the Risk treatment across the financial organizations

Course Outcomes:- Student will be able to :-
1. understand the financial threats and its security
2. monitor the threats and try to find the FinTech Solutions for Small Businesses

Course Contents

Chapter 1	**Introduction to Cyber Security and financial Technology Management**	**6 hours**

1.1. Understanding Threat Environment
1.2. Overview of the risk landscape
1.3. Threat categories for financial organizations
1.4. Threat Intelligence and Threat Modeling
1.5. Technology vulnerabilities in Fintech
1.6. Banking and the E-Book Moment
1.7. Why We're so Excited About FinTech
1.8. Current Trends in Financial Technology
1.9. Lending (Capital) in the 21st Century
1.10. The Next Big Innovation in FinTech – Identity
1.11. Tech Giants Becoming Non-Bank Banks
1.12. Design is No Longer an Option – User Experience (UX) in FinTech

Chapter 2	FnTech hubs and FinTech Technologies	**8 hours**

2.1 Nurturing New FinTech Communities
2.2 The Journey Towards an Integrated FinTech Ecosystem – The Netherlands
2.3 Luxembourg, a Future FinTech Hub?
2.4 Vienna as the No 1 FinTech Hub in Mobile Payments?
2.5 India's FinTech Ecosystem
2.6 Introduction to Cryptocurrencies and blockchain technology
    2.6,1 Cryptocurrency, Digital Currency Bitcoin and Ethereum
    2.6.2 Smart Contracts
2.7 Blockchain use cases

Chapter 3	**Emerging Markets and Social Impact**	8 hours

3.1 FinTech – The Not So Little Engine That Can 3.2 Why Am I Not Gonna Be Able to Enter a Bank? 3.3 The Rise of the Rest in FinTech 3.4 Smartphones, FinTech, and Education – Helping the Unbanked Reach Financial Inclusion 3.5 The Social Impact of FinTech in Nigeria 3,6 India and the Pyramid of Opportunity 3.5 cyber security risk as operationsal risk 3.6 Risk treatment across the financial organizations		
Chapter 4	**FinTech Solutions**	8
4.1 Rewiring the Deal – The Path Forward for B2B Supply Chains 4.2 Payments and Point of Sales (POS) Innovation 4.3 Predictive Algorithms – Building Innovative Online Banking Solutions 4.4 Big Data is the Cornerstone of Regulatory Compliance Systems 4.5 FinTech Solutions in Complex Contracts Optimization 4.6 Behavioural Biometrics – A New Era of Security 4.7 Ultra-Fast Text Analytics in Trading Strategies 4.8 Regulated Crowdfunding Ecosystems 4.9 Remittances – International FX Payments at Low Cost 4.10 FinTech Solutions for Small Businesses 4.11 Payment Solutions Including Apple Pay 4.12 FinTech Solutions Benefiting other Sectors 4.13 FinTech Innovation for Wearables 4.14 Cyber security risk appetite and performance objectives 4.15 Architectural views and enterprise capabilities 4.16 Montitoring and Reporting		
Reference Books:		
1. The FINTECH Book. The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries. Edition No. 1(chapters 1,2,3,4,5) 2. Financial cyber security Risk management, Paul Rohmeyer, Jenifer L. Bayuk(Chapter 1, 2,6,7) 3. Inclusive Fintechy, Blockchain, cryptocurrency and ICO ,Devid Lee Kuo Chen, Linda Low (chapters 1,2,5,7) 4. Beginning Blockchain : A Beginner's Guide to Building Blockchain Solutions By Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, ApressMedia		

Savitribai Phule Pune University

S.Y.B.Sc. (Cyber and Digital Science)

CDS-368B

Title:Lab on CDS-367B(Fintech security)

Teaching Scheme	No. of Credits	Examination Scheme
2hours / week	2	CA:15 marks UA: 35 marks

Course Objectives: -The course should enable the student:

- To present the concepts of Fintech technology
- To Learn the blockchain technology.

The students should be able to:

16. Understand the blockchain for payment service.
17. Understand cyber security and risk management..

Practical List

Assignment 1 –Demonstration of Blockchain (2 slots)
https://andersbrownworth.com/blockchain

Assignment No. 2: Case study on cyber security risk management (2 slots)
Explain the control architecture and supporting processes

Assignment No. 3: Case study onInternet and mobile finance:
Alibaba, Alipay to Ant Financial
.

Assignment No. 4: Case study on Fintech in Singapore (2 slots)

Assignment No. 5:
Introduction to Compliance within Fintech • Payment Card Industry Data Security Standard (PCI DSS) • RBI PSS (Reserve Bank of India - Payment and Settlement Systems)

Assignment No. 6:
Introduction of DevSecOPs in Fintech • CICD introduction • SSDLC introduction

Assignment No. 7:
Introduction to Software composition analysis (SCA) - security case study

Assignment No. 8:
Introduction Payment Services Directive (PSD2) - security case study

Assignment No. 9:
Introduction to Electronic Identification and Trust Services (eIDAS) - security case study

Assignment No. 10:
Introduction to Shift Left Principal in Fintech - security case study

Savitribai Phule Pune University
S.Y.B.Sc. (Cyber and Digital Science)
CDS-368A
Title: Lab on CDS-367A

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	**2**	**CA:15 marks** **UA: 35 marks**

Prerequisites
1. Basic C and Python Programming
2. Basic Computer Hardware
3. Basic Assembly Programming

Course Objectives: -
1. Static and Dynamic Analysis of Malwares
2. Study of windows malwares in depth.
3. Study of Linux malwares, Mac malwares, Android malware in brief.

Course Outcomes: - Student will be able to:-
1. classify the malwares and analyze them.
2. use the tools for analysis of any type of malware.
3. write own tools/programs for analyzing the malware.

Assignment No. 1: (1 slot) : Setting up the Malware Lab

Download and Install VMWare/ Virtual Box
Setting Up and Configuring Linux VM
Setting Up and Configuring Windows VM
Setting Up and Configuring Macintosh VM

Assignment No. 2: (2 slots) : Static Analysis of Malwares

1) **Install Required tools :***xxd, file, md5sum, sha256sum, sha1sum,*

2) **Download sample malware and perform static analysis. Print following info for the malwares using tools:**

File type, Cryptographic hash Values,

3) Scan suspicious binary file using VirusTotal/VirScan/Jotti Malware Scan/Metadefender
4) Extract Strings from binary file.

5) **Write Python Script for the following**
   - Print File type of suspicious malware.
   - Print Cryptographic hash Values of suspicious malware.
   - Accept the hash value (MD5/SHA1/SHA256) as input and queries the VirusTotal database.

Assignment No. 3: (2 slots) : Dynamic Analysis of Malwares

1) Setup the lab/machine for dynamic analysis of malwares.
2) Install Process hacker and do analysis of sample malwares.
3) Install Process Monitor and dos analysis of sample malwares.
4) Use noriben tool and do dynamic analysis of sample malwares.
5) Analyzing the DLL Using rundll32.exe

Assignment No. 4: (1 slots) : Disassembly using IDA

1) Installation of IDA tool and IDAPython tool.
2) Do static code analysis of sample malware using IDA
3) Open malicious DLL and change the behaviour and run notepad.exe under it.
4) Do static code analysis of sample malware using IDAPython

.

Assignment No. 4: (2 slots) : Debugging malicious binaries

1) Installation of x64dbg and dnSpy tool.
2) Debug a sample malicious binary using x64dbg.
3) Debug a sample malicious DLL using x64dbg.
4) Debug a sample malware executable using x64dbg.
5) Debug a sample malicious DLL using IDA.
6) Debug malicious .net application using dnSpy.

Assignment No. 5:

7) Introduction to Malware entry points and safeguarding it
8) Emails, SPF, Spam email detection
9) Phishing
10) USB

Assignment No. 6:

- Introduction to REMnux – Toolkit for Malware Analysis

11)

Assignment No.7 : : Introduction to Network Analysis

- Analyzing infected network
- Wireshark

Assignment No. 7: (2 slots)
(Research Paper Writing Activity)

Sample Topics:

- Writing review paper on Static analysis of Malwares.
- Writing review paper on Dynamic analysis of Malwares.
- Writing review paper on Hybrid analysis of Malwares.

Reference Books:

1. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, By Monnappa K A , Packt Publishing Limited
2. Android Malware and Analysis, By Ken Dunhum, Shane Hartman, Jose Andre Morales, Manu Quintans, Tim Strazzere
3. Learn Malware Analysis: Explore the Concepts, Tools and Techniques to Analyse and Investigate Malware, Sobia Publication
4. Malware Analysis Techniques: Tricks for the triage of adversarial software by Dylan Barker
5. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig
6. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware by Abhijit Mohanta and Anoop Saldanha
7. Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks by Alexey Kleymenov and Amr Thabet

Malware Sources

Hybrid Analysis: https:/ / www. hybrid- analysis. com/
KernelMode.info**:** http:/ / www. kernelmode. info/ forum/ viewforum. php? f= 16
VirusBay:https:/ / beta. virusbay. io/
Contagio malware dump:http:/ / contagiodump. blogspot. com/
AVCaesar:https:/ / avcaesar. malware. lu/
Malwr:https:/ / malwr. com/
VirusShare:https:/ / virusshare. com/
theZoo:http:/ / thezoo. morirt. com/
https://zeltser.com/malware-sample-sources/