

National Forensic Sciences University

An Institution of National Importance
(Ministry of Home Affairs, Government of India)
Sector – 9, Gandhinagar, Gujarat – 382007



School of Cyber Security & Digital Forensics **Gujarat Campus**

M. Sc. Digital Forensics & Information Security

(Syllabus, Teaching & Examination Schemes)

(W.E.F. Academic Year 2021 -22)



Teaching Scheme

Semester I							
Sr. No.	Subject Code	Subject Name	L	T	P	C	TCH
1	CTMSDFIS SI P1	Computer Forensics	3	0	0	3	3
2	CTMSDFIS SI P2	Cyber Security Audit and Compliance	3	1	0	4	4
3	CTMSDFIS SI P3	Incident Response Management	3	0	0	3	3
4	CTMSDFIS SI P4	Python & Scripting	3	0	0	3	3
5	CTMSDFIS SI P5	Introduction to Forensic Science and Law	4	0	0	4	4
6	CTMSDFIS SI L1	Computer Forensics Laboratory	0	0	1	1	2
7	CTMSDFIS SI L2	Incident Response Management Laboratory	0	0	1	1	2
8	CTMSDFIS SI L3	Python & Scripting Laboratory	0	0	1	1	2
Total Credit & Total Credit Hours							20 23
Semester II							
Sr. No.	Subject Code	Subject Name	L	T	P	C	TCH
1	CTMSDFIS SII P1	Mobile Forensics	3	0	0	3	3
2	CTMSDFIS SII P2	Web Application Security	3	0	0	3	3
3	CTMSDFIS SII P3	Malware Analysis & Forensics	3	0	0	3	3
4	CTMSDFIS SII P4	Artificial Intelligence	3	0	0	3	3
5	CTMSDFIS SII P5	Minor Project	0	2	2	4	6
6	CTMSDFIS SII L1	Mobile Forensics Laboratory	0	0	1	1	2
7	CTMSDFIS SII L2	Web Application Security Laboratory	0	0	1	1	2
8	CTMSDFIS SII L3	Malware Analysis & Forensics Laboratory	0	0	1	1	2
9	CTMSDFIS SII L4	Artificial Intelligence Laboratory	0	0	1	1	2
Total Credit & Total Credit Hours							20 26
Semester III							
Sr. No.	Subject Code	Subject Name	L	T	P	C	TCH
1	CTMSDFIS SIII P1	Network Security & Forensics	3	0	0	3	3
2	CTMSDFIS SIII P2	IoT Security & Forensics	3	0	0	3	3
3	CTMSDFIS SIII P3	Blockchain & Cryptocurrency	3	0	0	3	3
4	CTMSDFIS SIII P4	Program Elective 1	3	0	0	3	3
5	CTMSDFIS SIII P5	Program Elective 2	3	0	0	3	3
6	CTMSDFIS SIII L1	Network Security & Forensics Laboratory	0	0	1	1	2
7	CTMSDFIS SIII L2	IoT Security & Forensics Laboratory	0	0	1	1	2
8	CTMSDFIS SIII L3	Blockchain & Cryptocurrency Laboratory	0	0	1	1	2
9	CTMSDFIS SIII L4	Program Elective 1 Laboratory	0	0	1	1	2
10	CTMSDFIS SIII L5	Program Elective 2 Laboratory	0	0	1	1	2
Total Credit & Total Credit Hours							20 25
Semester IV							
Sr. No.	Subject Code	Subject Name	L	T	P	C	TCH
1	CTMSDFIS SIV P1	Major Project	0	10	10	20	30
Total Credit & Total Credit Hours							20 30
List of Program Elective 1 & 2							
Sr. No.	Subject Code	Subject Name					
1	CTMSDFIS SIII P4 EL1	Critical Infrastructure Security and Forensics					
2	CTMSDFIS SIII P4 EL2	Advance Computer Forensics					
3	CTMSDFIS SIII P4 EL3	Cloud Security & Forensics					
4	CTMSDFIS SIII P4 EL4	Mobile Phone Security					
5	CTMSDFIS SIII P5 EL1	Database Forensics					
6	CTMSDFIS SIII P5 EL2	Social Network Analysis					
7	CTMSDFIS SIII P5 EL3	Drone Forensics					
8	CTMSDFIS SIII P5 EL4	Research Methodology					

Total Credits: 80 **L:** Lecture **T:** Tutorial **P:** Practical 1 C = 1 Hour of Lecture / Tutorial and 1 C = 2 Hours of Practical / Project.
Note: TA-2 will be in form of assignments or workshops.



National Forensic
Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

विद्या अमृतं अस्तु

SEMESTER- I



CTMSDFIS SI P1: Computer Forensics

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

* Note: TA-2 will be in the form of assignments or workshops.

Objectives:

1. To learn how computers, work and handle data.
2. To understand electronic evidence and various computer artefacts.
3. To learn electronic evidence acquisition techniques.
4. To learn how to analyze windows, Linux and Mac OS machines.

UNIT – I

Fundamentals of Computer Systems

Number Systems: Binary, Octal, Decimal and Hexadecimal, Conversion and Operations on Binary Number Systems, Representing Information in Hexadecimal and Binary, Little Endian and Big-Endian Formats. Computer Architecture: Input Devices, Central Processing Unit, Storage Devices and Output Devices. Secondary Storage Devices: Understanding Disk, Volume and Partition, HDD and SSD Structures, Introduction to MBR, GPT and VBR. Basics of Operating Systems: Role of Operating System, Boot Process, Introduction to Process and Memory Management.

UNIT-II

Introduction to Computer Forensics Investigations and Electronic Evidence

Digital Forensics: Definition, Process, Lockard's Principle of Exchange, Branches of Digital Forensics, Handling Digital Crime Scene, Important Documents and Electronic Evidences. Introduction to Evidence Acquisition: Identification, Acquisition, Labelling and Packaging, Transportation, Chain-of-Custody, Importance of Documentation and Preservation. Acquisition Process: Write-Blockers, Imaging Techniques, Evidence Integrity, Standard Operating Procedures for Acquisitions and Preservation of Evidences. Introduction to Data Recovery and Carving: Importance of Data Recovery in Forensic Investigation, Carving Methods, Difference between Data Recovery and Carving

UNIT-III

Windows OS Forensics

Windows OS Architecture, File System Analysis: Understanding and Analyzing FAT and NTFS File Systems, Recreating FAT and NTFS Partitions, Analyzing Unallocated Partitions. Registry Analysis: Understanding Windows Registry, Analyzing Windows

Registry, Finding Important Artefacts Related to User Activities, User/Application Configurations and Preferences; Attached Devices, Shared Locations, Recently Accessed Documents, Programs and Locations; Installed Applications and Others from Windows Registry. Event and Log Analysis: Introduction to Windows Events, Understanding Windows Events (Evt and Evtx Files). Analyzing Logs of Third-party Applications.

UNIT - IV

Linux OS Forensics

Linux OS Architecture, File System Analysis: Understanding and Analyzing EXT File System, Recreating EXT Partitions, Analyzing Unallocated Partitions. Log Analysis: Understanding Various Logs, Analyzing Important Logs to Find Important Artefacts Related to User Activities, User/Application Configurations and Preferences; Attached Devices, Shared Locations, Recently Accessed Documents, Programs and Locations; Installed Applications.

UNIT - V

MAC OS Forensics

MAC OS Architecture, File System Analysis: Understanding and Analyzing HFS and HFS+ File System, Recreating HFS Partitions, Analyzing Unallocated Partitions. Log Analysis: Understanding Various Logs, Analyzing Important Logs to Find Important Artefacts Related to User Activities, User/Application Configurations and Preferences Attached Devices, Shared Locations, Recently Accessed Documents, Programs and Locations Installed Applications.

Reference Books: -

1. Practical Guide to Computer Forensics Investigations, A (Pearson IT Cybersecurity Curriculum (ITCC)) 1st Edition by Darren R. Hayes
2. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence 1st Edition by William Oettinger
3. Investigating Windows Systems 1st Edition by Harlan Carvey.
4. Practical Linux Forensics: A Guide for Digital Investigators by Bruce Nikkel
5. Linux Forensics Kindle Edition by Philip Polstra
6. Computer Systems_ Digital Design, Fundamentals of Computer Architecture and Assembly Language
7. Digital Forensics with Open-Source Tools 1st Edition by Cory Altheide, Harlan Carvey
8. Operating Systems: Internals and Design Principles, 9/e by William Stallings
9. Linux Bible 10th Edition by Christopher Negus
10. Linux Pocket Guide: Essential Commands 3rd Edition by Daniel J. Barrett



CTMSDFIS SI P2: CYBER SECURITY AUDIT AND COMPLIANCE

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	01	00	04	04	25	00:45	50	01:30	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To learn Security Audit and Compliance
2. To understand the process of security audit
3. To understand the industry standard practices for auditing
4. To learn various security standards
5. To learn the policy making and organizational structure
6. To understand the Risk and Continuity planning

UNIT – I

The need for information system security compliance

What is IT security assessment? What is an IT security audit? What is compliance? How does an audit differ from an assessment? Why are governance and compliance important? What if an organization does not comply with compliance laws? What is the scope of an IT compliance audit? What does your organization do to be in compliance? What are you auditing within the IT infrastructure? Maintaining IT compliance.

UNIT - II

Planning and implementation of an IT Infrastructure Audit for compliance:

Defining the scope for audit, Identifying critical requirements for the audit, assessing IT security, Obtaining Information, Documentation and Resources, Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure, Identifying and Testing Monitoring Requirements **What Are Controls and Why Are They Important?:** Goal- Based Security Controls, Implementation-Based Security Controls, The Security Control Formulation and Development Process, Setting the Stage for Control Implementation through Security Architecture Design, Implementing a Multitiered Governance and Control Framework in a Business **The IT Audit Process:** Audit Plan, Audit Process, Types of IT Audits, Computer-Assisted Audit Techniques (CAATs), CAATs for Sampling, CAATs for Application Reviews, CAATs for Auditing Application Controls.



UNIT – III

Conducting an IT Infrastructure Audit for Compliance:

Identifying the Minimum Acceptable Level of Risk and Appropriate Security Baseline Definitions, Seven Domains of a Typical IT Infrastructure, Writing the IT Infrastructure Audit Report **Compliance within User Domain:** Compliance law requirements and business drivers, Items Commonly Found in the User Domain, **Compliance within the workstation domain:** Compliance law requirements and business drivers, devices and components commonly found in the workstation domain, Maximizing C-I-A, **Compliance within the LAN Domain:** Compliance law requirements and business drivers, devices and components commonly found in the LAN domain, Maximizing C-I-A, **Compliance within LAN and WAN Domain:** Devices and Components Commonly Found in the Domain , Penetration Testing and Validating Configurations, **Compliance within Remote Access and Application Domain:** Devices and Components Commonly Found in the Domain, Application Server Vulnerability Management, Application Patch Management.

UNIT – IV

Risk Assessment and BCP, DR Planning:

Introduction to Risk Analysis, Risk Identification, Risk Assessment, Risk Response and Mitigation, Risk Reporting, Introduction to Business Continuity Planning (BCP), Overview of BCP Life Cycle, Need for BCP, Identifying and Selecting Business Continuity Strategies, Introduction to Disaster Recovery (DR) planning, Identification of potential disaster status, DR Strategies, Plans for Business Resumption.

UNIT-V

Cyber Law and Auditing Standards/Frameworks:

Indian IT ACT with Amendments, Adjudication under Indian IT ACT, Auditing Standards and Frameworks: ISO/IEC 27001/2, COBIT, SOC Compliance, HIPAA, GDPR and PCIDSS.

Reference Books: -

1. Auditing IT Infrastructures for Compliance By Martin M. Weiss, Michael G.Solomon, Jones & Bartlet Learning, 2015
2. The IT Regulatory and Standards Compliance Handbook by Craig S. Wright, Syngress, 2015
3. Information Technology Control and Audit 5th Edition by Angel R. Otero, 2019
4. (Internal Audit and IT Audit Series) The Complete Guide to Cyber Security Risks and Controls by Anne Kohnke, Dan Shoemaker, Ken Sigler, 2016

-
5. PCI DSS An Integrated Data Security Standard Guide- APress By Jim Seaman, 2020
 6. AICPA - Guide_ SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy-Wiley, 2018
 7. The EU General Data Protection Regulation (GDPR) A Practical Guide by Paul Voigt and Axel von dem Bussche, 2017
 8. PCI DSS, SAQ Instructions and Guidelines (Available online)
 9. Bob Hayes, Kathleen Kotwica, “Business Continuity 2nd Edition”, Elsevier Pub.2013.
 10. Governance, risk, and compliance by Microsoft, 2019.



CTMSDFIS S1 P3: Incident Response Management

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand concept of Incident Response Management
2. To learn various Incident Response Management Techniques
3. To understand fundamental of Digital Forensics
4. To learn various Digital Forensics Techniques

UNIT-I

Introduction to Incident Response

Cyber Incident Statistics, Computer Security Incident, Information Warfare, Key Concepts of Information Security, Types of Computer Security Incidents, Examples of Computer Security Incidents, How to Identify an Incident, Need for Incident Response, Goals and Purpose of Incident Response, Signs of an Incident, Incident Categories

UNIT-II

Incident Management

Incident Prioritization, Use of Disaster Recovery Technologies, Impact of Virtualization on Incident Response and Handling, Estimating Cost of an Incident, Incident Reporting, Incident Reporting Organizations, Vulnerability Resources, Incident Management, Incident Response Team Roles, Incident Response Team Responsibilities, Dependencies.

UNIT – III

Incident Handling

Incident Handling Process, Real-time log capture and analysis, Botnet identification and counteraction, Enterprise Solutions for Incident Response and Recovery, Timeline Analysis, Malware Handling: Safety; Documentation; Distribution, Report Writing: Reporting Standards; Report Style and formatting; Report Content, Quality Assurance.

UNIT-IV

Data Collection

When to perform a live response, selecting a live response tool, what to collect, collection best practices, live data collection on Microsoft windows systems, Live data collection



on Unix-based systems, understanding network monitoring, Types of network monitoring, setting up a network monitoring system, network data analysis, collect logs generated from network events.

UNIT-V

Data Analysis

Analysis methodology: Define Objectives; Where the data is stored? Outline an approach; select methods; evaluate results, investigating windows systems: NTFS and file system analysis; Prefetch; Event Logs; Scheduled tasks; the windows registry, investigating applications: What is application data; where is application data stored; general investigation methods; web browsers; email clients; instant message clients, Analysis of application data

Reference Books

1. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson
2. Incident Handling and Response: A Holistic approach for an efficient security incident management by Jithin Aby Alex
3. Blue Team Handbook: Incident Response Edition by Don Murdoch
4. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk by N. K. McCarthy
5. Critical Incident Management: A Complete Response Guide, Second Edition by John McNall, Thomas T. Gillespie, Vincent F. Faggiano
6. Applied Incident Response by Steve Anson
7. Security Operations Centre – SIEM Use Cases and Cyber Threat Intelligence by Arun E Thomas
8. Incident Response & Computer Forensics by Jason T. Lutgens, Kevin Mandia and Matthew Pepe
9. Incident Management for Operations by Chris Hawley, Rob Schnepf and Ron Vidal
10. Digital Forensics and Incident Response: Incident Response Techniques and Procedures to Respond to Modern Cyber Threats, 2nd Edition by Gerard Johansen



CTMSDFIS SI P4: Python and Scripting

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To learn the concept of scripting for cyber security
2. To Learn Python basics for scripting
3. To Learn PowerShell scripting for information security concept
4. To learn Bash Scripting for cyber security related task
5. To Learn the concept related secure development and threat hunting

UNIT – I

Scripting Part 1

What Is "The Shell", Understanding the File System Tree and its Navigation, Exploring the System, Manipulating Files and Directories, Manipulating Files and Directories, I/O Redirection, Expansion, Permissions, Job Control, Configuration and The Environment, Introduction To vi, Customizing the Prompt

UNIT – II

Scripting Part 2

Package Management, Storage Media, Networking, Searching for Files, Archiving and Backup, Regular Expressions, Text Processing, Formatting Output, Printing, Compiling Programs. Writing Shell Scripts: Starting A Project, Top-Down Design, Flow Control: Branching With if, Reading Keyboard Input, Flow Control: Looping With while / until & for, Troubleshooting, Strings and Numbers, Arrays

UNIT – III

Basic Python Scripting

Python Setup, Debugging, Variables, String, Lists, Dictionaries, Networking, Selection, Function, Iteration, Classes and Objects (OOP), Inheritance and Composition, Comments and Pound Character, Numbers and Math, Variables and Names, Conditional statements

UNIT – III

Advance Python Scripting

Exception Handling File I/O, Sys Module, OS Module, Long-Tail/Short-Tail Analysis, Geolocation Acquisition, Blacklists and Whitelists, Packet Analysis, Packet Reassembly,

Payload Extraction. **Forensic Python:** Acquiring Images from Disk, Image Forensics and PIL, SQL Queries, HTTP Communications with Python Built in Libraries, Web Communications with the Requests Module.

UNIT – V

PowerShell Essential and Scripting

Overview PowerShell, Environment Setup, PowerShell Integrated Script Environment (ISE), Working with PowerShell scripts, cmdlets, files and folders, dates and timers, file I/O, Advanced Cmdlets, PowerShell Scripting: special variables, operators, looping, conditions, array, hash tables, regex, blackets, alias, WMIC & PowerShell. PowerShell providers and drives, \$Args variable, param statement, Passing data by value and by reference, PowerShell Advance Functions, Using PowerShell remoting capabilities: emoting concepts Invoking remote commands, processing output, Objects in Windows PowerShell: Error handling concepts, terminating and non- terminating errors, Handling errors using \$?, \$Error and \$lastExitCode variables, Error Record object anatomy, Working with textual files : Saving information into textual and csv files, Reading information from textual and csv files, Example implementation of error handling code.

Reference book

1. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers by TJ O' Connor (Author)
2. Shell Scripting: How to Automate Command Line Tasks Using Bash Scripting and Shell Programming by Jason Cannon
3. Mastering PowerShell Scripting - Fourth Edition: Automate and manage your environment using PowerShell by Chris Dent



CTMSDFIS SI P5: Introduction to Forensic Science and Law

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives:

1. About the significance of forensic science to human society and criminal investigation.
2. The fundamental principles of forensic science.
3. The divisions in a forensic science laboratory.
4. The working of the forensic establishments in India and abroad.
5. Legal aspects of forensic investigations

UNIT-I

History of Development of Forensic Science in India. Functions of forensic science. Historical aspects of forensic science. Definitions and concepts in forensic sciences. Scope of forensic science. Various contemporary disciplines of forensic sciences and their applications in different approaches with theoretical concepts Need of forensic science. Basic principles of forensic science.

UNIT-II

Contemporary development in the academic and practices in forensic sciences-advantage of scientific investigations- Tools and Techniques in Forensic Science- Branches of forensic science. Forensic science in international perspectives, including set up of INTERPOL, and FBI. Duties of forensic scientists. Code of conduct for forensic scientists. Qualifications of forensic scientists. Data depiction. Report writing.

UNIT-III

Academic institutions involvement -Organizational set up of Forensic Science Laboratories in India Hierarchical set up of Central Forensic Science Laboratories, State Forensic Science Laboratories, Government Examiners of Questioned Documents, Fingerprint Bureaus, National Crime Records Bureau, Police & Detective Training Schools, NIA, CCNTS, Bureau of Police Research & Development, Directorate of Forensic Science and Mobile Crime Laboratories. Police Academies. National investigation agency and other agencies involved in the criminal investigations- agencies referred for the additional information and requisite examinations

UNIT-IV



Definition of Law, Court, Judge, Basic Terminology in Law, Introduction to Criminal Procedure Code, FIR, Difference between civil and Criminal Justice, Object of Punishment, Kinds of Punishment, Primary and Sanctioning Rights Primary and Secondary functions of Court of Law. Law to Combat Crime-Classification – civil, criminal cases. Essential elements of criminal law. Constitution and hierarchy of criminal courts. **Criminal Procedure Code:** Cognizable and non-cognizable offences. Bailable and nonbailable offences. Sentences which the court of Chief Judicial Magistrate may pass. **Laws specific to Forensic Science:** Indian Penal Code pertaining to offences against persons – Section 121A, 299, 300, 302, 304A, 304B, 307, 309, 319, 320, 324, 326, 351, 354, 359, 362. Sections 375 & 377 and their amendments. **Indian Evidence Act** – Evidence and rules of relevancy in brief. Expert witness. Cross examination and re-examination of witnesses. Sections 32, 45, 46, 47, 57, 58, 60, 73, 135, 136, 137, 138, 141. CrPC – Sections 291, 291A, 292 & 293 in the code of criminal procedure.

UNIT-V

Introduction to Computer and its components, different types of storage media, Category to Cyber-crime, Cyber Law, IT Act 2000 and its amendments, International Cyber Laws, Cyber Ethics, Child Sexual Abuse Material related to cyber domain, various acts related to social media, privacy and security on cyber domain, case studies.

References:

1. B.B. Nanda and R.K. Tiwari, *Forensic Science in India: A Vision for the Twenty First Century*, Select Publishers, New Delhi (2001).
2. M.K. Bhasin and S. Nath, *Role of Forensic Science in the New Millennium*, University of Delhi, Delhi (2002).
3. S.H. James and J.J. Nordby, *Forensic Science: An Introduction to Scientific and Investigative Techniques*, 2nd Edition, CRC Press, Boca Raton (2005).
4. W.G. Eckert and R.K. Wright in *Introduction to Forensic Sciences*, 2nd Edition, W.G. Eckert (ED.), CRC Press, Boca Raton (1997).
5. R. Saferstein, *Criminalistics*, 8th Edition, Prentice Hall, New Jersey (2004).
6. W.J. Tilstone, M.L. Hastrup and C. Hald, *Fisher's Techniques of Crime Scene Investigation*, CRC Press, Boca Raton (2013)
7. Tallinn Manual on The International Law Applicable To Cyber Warfare, International Group of Experts and NATO by Michael N. Schmitt
8. IT Act 2000 and 2008 bare acts documents
Cyber Law in India, Satish Chandra (2017)



CTMSDFIS SI L1: Computer Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SI L2: Incident Response Management Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs		Marks	Hrs		
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SI L3: Python & Scripting Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



National Forensic
Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

SEMESTER- II



CTMSDFIS SII P1: Mobile Forensics

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand concept of Mobile and wearable device forensics.
2. To learn various Techniques in Mobile Forensics.
3. To understand fundamental of mobile device architecture.
4. To learn various Digital Forensics Techniques

UNIT –I

Introduction to Android

The Android architecture: The Linux kernel, Libraries, Dalvik virtual machine, The application framework, The applications layer, Android security, Security at OS level through Linux Kernel: Permission model, Application sandboxing, SELinux in Android, Application Signing. Secure inter process communication, Android hardware components, Core components: Central processing unit, Baseband processor, Memory, SD Card, Display, Battery; Android boot process: Boot ROM code execution, The boot loader, The Linux kernel, The init process, Zygote and Dalvik, System server. Setting Up an Android Forensic Environment: The Android forensic setup with Android Virtual Device, Connecting and accessing an Android device from the workstation, Identifying the device cable, installing device drivers, Accessing the device.

UNIT –II

Android OS internals

Android Debug Bridge, Using adb to access the device, Detecting a connected device, Directing commands to a specific device, Issuing shell commands, Basic Linux commands, Installing an application, Pulling data from the device, Pushing data to the device, Restarting the adb server, Viewing log data, Rooting Android, What is rooting?, Why root?, Recovery and fast boot, Recovery mode, Accessing the recovery mode, Custom recovery, Fast boot mode, Locked and unlocked boot loaders, How to root, Rooting an unlocked boot loader, Rooting a locked boot loader, ADB on a rooted device. Understanding Data Storage on Android DAndroid partition layout, Common partitions in Android, boot loader, boot, recovery, userdata, system cache, radio, Identifying partition layout, Android file hierarchy, An overview of directories, acct, cache, d, data,



dalvik-cache, data, dev, init, mnt, proc, root, sbin, misc, sdcard, system, build.prop, app, framework, ueventd.goldfish.rc and ueventd.rc, Application data storage on the device, Shared preferences, Internal storage, External storage, SQLite database, Network, Android filesystem overview, Viewing filesystems on an Android device, Common Android filesystems, Flash memory filesystems, Media-based filesystems, Pseudo filesystems.

UNIT-III

Data Extraction in Android Device

Introducing Android Forensics: Mobile forensics, The mobile forensics approach: Investigation Preparation, Seizure and Isolation, Acquisition, Examination and Analysis, Reporting; Challenges in mobile forensics, Extracting Data Logically from Android Devices, Logical extraction overview, What data can be recovered logically?, Root access, Manual ADB data extraction, USB debugging, Using ADB shell to determine if a device is root, ADB pull, Recovery mode, Fastboot mode, Determining bootloader status, Booting to a custom recovery image, ADB backup extractions, Extracting a backup over ADB, Parsing ADB backups, Data locations within ADB backups, ADB Dumpsys, Dumpsys battery stats, Dumpsys procstats, Dumpsys user, Dumpsys App Ops, Dumpsys Wi-Fi, Dumpsys notification, Dumpsys conclusions, Android SIM card extractions, Acquiring SIM card data, SIM security, SIM cloning, Issues and opportunities with Android Lollipop. Extracting Data Physically from Android Devices.

UNIT-IV

Logical and Physical Extraction

Physical extraction overview, What data can be acquired physically?, Root access, Extracting data physically with dd, Determining what to image, Writing to an SD card, Writing directly to an examiner's computer with netcat, Installing netcat on the device, Using netcat, Extracting data physically with nanddump, Verifying a full physical image, Analyzing a full physical image, Autopsy, Issues with analyzing physical dumps, Imaging and analyzing Android RAM, What can be found in RAM?, Imaging RAM with LiME, Imaging RAM with mem, Output from mem, Acquiring Android SD cards, What can be found on an SD card?, SD card security, Advanced forensic methods, An overview of data recovery, How can deleted files be recovered?, Recovering data deleted from an SD card, Recovering data deleted from internal memory, Recovering deleted data by parsing SQLite files, Recovering deleted data through file carving techniques, Analyzing backup.

UNIT-V

Android Application Forensics

Forensic Analysis of Android Applications, Application analysis, Why do app analysis?,

The layout of this chapter, Determining what apps are installed, Understanding Linux epoch time, Wi-Fi analysis, Contacts/call analysis, SMS/MMS analysis, User dictionary analysis, Gmail analysis, Google Chrome analysis, Decoding the Web Kit time format, Google Maps analysis, Google Hangouts analysis, Google Keep analysis, Converting a Julian date, Facebook analysis, Facebook Messenger analysis, Skype analysis, Recovering video message-es from Skype, Snapchat analysis, Viber analysis, Tango analysis, WhatsApp analysis, Decrypting WhatsApp backups.

Reference Books

1. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, Second Edition by Lee Reiber, McGraw-Hill Education Publication (2018).
2. Android Hacker's Handbook by Joshua J. Drake, Zach Lanier, Georg Wicherski, Pau Oliva Fora, Stephen A. Ridley, Collin Mulliner, Wiley Publication (2014).
3. Android Forensics Investigation, Analysis and Mobile Security for Google Android by Andrew Hoog, Elsevier Science Publication (2011).
4. Learning Android Forensics by Rohit Tamma, Donnie Tindall, Packt Publication (2015).
5. Practical Mobile Forensics, A Hands-on Guide to Mastering Mobile Forensics for the IOS, Android, and the Windows Phone Platforms, 3rd Edition by Heather Mahalik, Satish Bommisetty, Oleg Skulkin, Rohit Tamma, Packt Publication (2018)



CTMSDFIS SII P2: Web Application Security

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To learn the concept of web application technology
2. Learn various aspects of web application security
3. Learn to vulnerability assessment of web application security
4. Exploitation of potential found vulnerability
5. Learn industry standard techniques to exploit advanced vulnerability

UNIT – I

Introduction to web technology and information Gathering

TCP, HTTP/S Protocol Basics, Encoding, Origin, Cookies, Sessions, Fingerprinting the web server, Subdomain's enumeration, finding virtual hosts, fingerprinting custom applications, Enumerating resources, Relevant information through misconfigurations, Google hacking.

UNIT – II

Web Application Security Vulnerability Terminology

Introduction to Vulnerability Assessment, Life cycle of Vulnerability Assessment, Vulnerability Scanners, Unknown Vulnerability, False Positive, CVE, CWE, Common Vulnerability Scoring System (CVSS), STRIDE, DREAD, Secure Source Code Review.

UNIT – III

Proxy and Interception

Burp Suite / OWASP Zed Attack Proxy (ZAP): Logging and monitoring, learning tools to spider a website, analyzing website content, Brute forcing unlinked files and directories via ZAP and ffuf, Web authentication mechanisms, Fuzzing with Burp Intruder, Username harvesting and password guessing, Burp sequencer, Session management and attacks, Authentication and authorization bypass.

UNIT – IV

Attack Landscape - Web Application Security

OWASP 10 Ten – Injection, Broken Authentication, Sensitive Data Exposure, XML

External Entities, Broken Access Control, Security Misconfiguration, Cross Site Scripting, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring, Cross Site Request Forgery, File Inclusion, Click Jacking, File Inclusion, File Upload, Insecure Captcha, SSRF/XSPA.

UNIT – V

Advanced Web Security Pen-Testing

Web Service concepts, REST concepts, SQL Injection - Vulnerable code, Sensitive data in GET, Weak Auth tokens & IDOR, Leaky APIs, Automated Scanning with FuzzAPI / Astra / other industry standard tools, Introduction to CMS and Docker containers security.

Reference Books

1. Web Application Security, A Beginner's Guide by Bryan Sullivan, Vincent Liu, McGraw-Hill Education Publication (2011).
2. Hands-On Bug Hunting for Penetration Testers A Practical Guide to Help Ethical Hackers Discover Web Application Security Flaws by Joseph Marshall, Packt Publication (2018).
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard, Marcus Pinto, 2nd Edition, Wiley Publication (2007).
4. The Penetration Tester's Guide to Web Applications by Serge Borso, Artech House Publication (2019).
5. Web Application Security Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman, O'Reilly Media Publication (2020)



CTMSDFIS SII P3: Malware Analysis and Forensics

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To learn the various malware types
2. To learn the internals of executable files
3. To learn various malware analysis techniques
4. To learn the signature creation for malware detection
5. To learn the reverse engineering of malware
6. To learn about malware forensics.

UNIT – I

Introduction to Malware and Malware Analysis:

Malware Definition and Types, Malware Analysis, Forensic Importance of Malware Analysis, Introduction to different analysis techniques, Malware Behavior, Setting up malware analysis laboratory. Static Analysis: Hashing, Finding Strings, Decoding Obfuscated Strings Using FLOSS, PE Files Headers and Sections, PE View, Linked Libraries and Functions, Dependency Walker, CFF Explorer, Resource Hacker, Malware signature and Clam AV Virus Signature, YARA Signatures, Dynamic Analysis: Sandboxes, Running and Monitoring a Malware, Process Monitor, Process Explorer, RegShot, faking a network, Using Wireshark for Packet Analysis.

UNIT – II

Assembly and Reverse Engineering

Introduction to x86 Assembly and CPU registers, Overview of the Stack, IDA Pro with its functions and features, Understanding of C code construct in Assembly, Analyzing Malicious Windows Programs, Live Memory Analysis using Volatility.

UNIT – III

Debugging

Difference between Source level v/s Assembly level debugger, Kernel mode v/s User mode debugger, Debugger common features, Breakpoints, Exceptions, Modification of Program Execution, Working with OllyDbg and Immunity Debugger, Kernel Debugging with WinDBG

UNIT – IV

Behaviors of Malware

Common behavior of the malwares, Process Injection, Process Replacement, Hook Injection, Data Encoding, Anti- Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques, Packers and Unpacking.

UNIT - V

Volatile Data

Examination from Windows and Linux Systems: Understanding processes, threads, ports, handles etc. Identifying services and drivers, determining scheduled tasks. Discovering and extracting malware and associated artifacts from Windows and Linux Systems.

Reference Books

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig.
2. Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware by Monappa K A (2018)
3. Mastering Malware Analysis: The Complete Malware Analyst's Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks by Alexey Kleymenov, Amr Thabet (2019)
4. Malware Analysis Cookbook: Tools and Techniques for Fighting Malicious Code by Matthew Richard, Blake Hartstein, Michael Hale Ligh, Steven Adair.
5. Practical Reverse Engineering: X86, X64, ARM, Windows Kernel, Reversing Tools, and Obfuscation by Alexandre Gazet, Bruce Dang, and Elias Bachaalany
6. The IDA Pro Book: The unofficial guide to the world's most popular disassembler by Chris Eagle
7. Android Malware and Analysis by Tim Strazzere, Manu Quintans, Jose Andre Morales, Shane Hartman, Ken Dunham
8. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy and Aaron Walters
9. Malware Forensics: Investigating and Analyzing Malicious Code by James M. Aquilina, Eoghan Casey, Cameron H. Malin
10. Sockets, Shellcode, Porting and Coding: Reverse Engineering Exploit and Tool Coding for Security Professionals by James C. Foster and Mike Morgan Price



CTMSDFIS SII P4: Artificial Intelligence

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand concept of Artificial Intelligence, Machine Learning and Deep Learning
2. To learn various Machine Learning and Deep Learning techniques
3. To create models to understand applications of AI
4. To learn role of ML/DL in Information Security

UNIT-I

Introduction to Mathematics for ML and Python

Python: Setting up Environment, Basic Python Commands, Creating Python Scripts, Conditions, Loops, List, Dictionary, User Defined Functions, Introduction to Anaconda, Working with NumPy, Pandas and Matplotlib. Mathematics for ML: Vectors, Matrices, Linear Equations, Mean, Median, Mod, Standard Deviation and Variance, Probability, Correlation, Regression, Handling and Representing Data.

UNIT-II

Machine Learning (ML)

Definition and History of AI, Defining Machine Learning, Applications of ML, Issues and Challenges in ML, Types of ML. Basics of Supervised Learning, Prediction, Classification, Understanding Datasets, Feature Selection, Feature Normalization, Data Cleaning, Training, Testing & Validation Sets, Different Models of Supervised Learning, Hyperparameters, Measuring Performance, Accuracy and Loss Underfitting & Overfitting, Basics of Unsupervised Learning, Different Models of Unsupervised Learning.

UNIT-III

Neural Network

Understanding Biological Brain, Defining Artificial Neural Network (ANN), Applications of ANN & DL. Defining & Building a Perceptron, Feed Forward, Back propagation, Single-layer & Multi-layer ANNs, building an ANN Model, Activation & Loss Functions, Compiling & Evaluating a Model. Convolutional Neural Networks



(CNN): Understanding Convolutions, Pooling, Building & Fitting CNN Models, Evaluating Model Performance. Recurrent Neural Networks (RNN): Basic RNN Architecture, Applications of RNN, Building & Fitting RNN Models, Evaluating Model Performance. Long Short-Term Memory Networks (LSTM): LSTM Network Architecture, Understanding LSTM, Building LSTMs

UNIT-IV

Computer Vision and Natural Language Processing

Computer Vision: Introduction, Object Detection and Image Segmentation, Detecting and Recognizing Faces, Tracking Objects, Pattern Recognition. Natural Language Processing (NLP): Introduction, Language as Data, Building Custom Corpus, Text Vectorization & Transformation, Classification for Text Analysis, Clustering for text Similarity, Context-Aware Text Analysis, Text Visualization.

UNIT-V

ML/DL for Cyber Security

Introduction to Role of ML in Cyber Security, Malware Detection & Classification, Anomaly Detection, Pen Testing using ML, Social Engineering, ML based Intrusion Detection and other Applications of ML in Cyber Security.

Reference Books

1. Mathematics for Machine Learning 1st Edition by Marc Peter Deisenroth
2. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd Edition by AurélienGéron
3. Python Machine Learning: Machine Learning and Deep Learning with Python, scikit- learn, and TensorFlow 2, 3rd Edition by Sebastian Raschka and Vahid Mirjalili
4. Hands-On Neural Networks with Keras: Design and create neural networks using deep learning and artificial intelligence principles 1st Editionby NiloyPurkait
5. Deep Learning with Keras: Implementing deep learning models and neural networks with the power of Python by Antonio Gulli, Sujit Pal
6. Practical Machine Learning for Computer Vision 1st Edition by Valliappa Lakshmanan, Martin Görner and Ryan Gillard
7. Learning OpenCV 4 Computer Vision with Python 3: Get to grips with tools, techniques, and algorithms for computer vision and machine learning, 3rd Edition by Joseph Howseand Joe Minichino
8. Natural Language Processing in Action: Understanding, analyzing, and generating text with Python 1st Editionby Hobson Lane, Hannes Hapke and Cole Howard.
9. Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to

implement machine learning algorithms for building security systems using Python by Emmanuel Tsukerman.

10. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem by Soma Halder (Author), Sinan Özdemir



CTMSDFIS SII P5: Minor Project

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
00	02	02	04	06	25	00:45	50	01:30	100	03:00	---	---	200

Students will need to work on a minor project under guidance of an internal faculty member. The students will need to submit a regular progress report for internal evaluation. A project report will need to be submitted and presented at the end of the semester for final evaluation.



CTMSDFIS SII L1: Mobile Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SII L2: Web Application Security Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs		Marks	Hrs		
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SII L3: Malware Analysis & Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SII L4: Artificial Intelligence Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



National Forensic
Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

SEMESTER- III



CTMSDFIS SIII P1: Network Security

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

UNIT-I

Basics of Networking

ISO/OSI, TCP-IP, Networking devices: Host, Hub, Bridge, Switch, Router and its functioning, Perimeter devices: IDS, IPS, Firewall and its functioning. NOC, SOC, SIEM, Servers: DNS, DHCP, Proxy, Mail and Application servers. Threat, vulnerability, attack surface, attack vector, exploit. Common attacks and countermeasures: Phishing attack, ARP poising, MAC flooding, DoS and DDoS.

UNIT-II

Penetration Testing

Penetration testing life cycle: Scope, SOW, Reconnaissance, target enumeration, vulnerability identification, assessment, exploitation, and reporting. Information gathering starting at source scrutinizing key employees, Dumpster diving, War driving, analyzing the web, exploring domain ownership- whois, Regional internet registries, server location, Scanning: active and passive, ICMP (Ping), OS and server fingerprinting, scanning tools and port status, TCP and UDP scan. SNMP services enumeration, and countermeasures. Routing devices enumeration and countermeasures. Advanced enumeration: Password cracking, sniffing password hashes and password protection. Vulnerability exploitation, Buffer overflow, vulnerability assessment tools, source code assessment tools, application assessment tools, system assessment tools, exploit tools.

UNIT-III

Cryptography

Introduction to Security: need for security, principle of security, security approaches. Encryption Techniques: plaintext, cipher text, substitution & transposition techniques, encryption & decryption, key range & size. Symmetric and Asymmetric encryption. Public Key Cryptography and Message Authentication: Public key cryptographic principles, digital signatures, key management, hash function and message digest. Types of attacks and countermeasures.

UNIT-IV

Wireless Network Security

802.11 Protocols, WAP and inherent security issues, promiscuous and monitor mode, Sniffing wireless packets, management, control, and data frames, WLAN authentication and encryption, WEP, WPA and WPA 2. WLAN authentication and security flaws. WLAN based attacks and countermeasures. WLAN Pen testing tools.

UNIT-V

Network Forensics

Digital evidence, Network based digital evidence, Network Forensic investigation methodology, Sources of network-based evidence, Evidence acquisition, Network traffic capture and analysis, Traffic capture and analysis tools, Event log aggregation, correlation, and analysis. Data in motion investigation

Reference Books

1. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
2. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
3. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, 2010 2.
4. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed., 2009.
5. Michael Gregg, Build Your Own Security Lab: A Field Guide for Networking Testing.
6. Sherri Davidoff and Jonathan Ham, Network Forensics Tracking Hackers through Cyberspace.
7. Mastering Wireless Penetration Testing for Highly Secured Environments by Aaron Johns
8. Chris McNab, Network Security Assessment: Know Your Network 9. Cameron Buchanan and Vivek Ramachandran, Kali Linux Wireless Penetration Testing Beginner's Guide



CTMSDFIS SIII P2: IoT Security & Forensics

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives:

1. To understand the basic concept and architecture of IoT.
2. To understand the IoT communication and messaging protocols.
3. To understand the IoT enabling technologies.
4. To understand the IoT security aspects.
5. To understand the basics of IoT security.

UNIT – I

Introduction to IoT

Definition & Characteristics of IoT; Evolution of IoT; Physical Design of IoT – IoT Components; Logical Design of IoT; IoT Levels and Deployment Techniques; IoT Applications & Domains; IoT Enabling Technologies; Challenges in IoT

UNIT – II

M2M & System Management

M2M; Difference between IoT and M2M; Software Defined Networking (SDN); Network Function Virtualization (NFV); Simple Network Management Protocol (SNMP); Limitation of SNMP, Network Operator Requirements; H/W and S/W Communications in IoT (UART, SPI, I2C, JTAG)

UNIT – III

IoT Communication and Messaging Protocols

IoT Protocol Design – Protocol Stack for IoT; IoT Communication Protocol – HTTP Basics, HTTP Architecture; MQTT Basics, MQTT Architecture; XMPP Basics, XMPP Architecture; COAP Basics, COAP Architecture

UNIT – IV

IoT Security

IoT Interoperability; Need for IoT Security; Privacy & Threat to Data in IoT, IoT Attack Vectors & IoT Attack Surfaces; IoT Pen testing Approaches; Understanding OWASP Top 10 for IoT; Threat Modeling in IoT; IoT Cloud Security Architecture; Case Study

UNIT – V

IoT Forensics, Standards & Guidelines

Introduction to IoT Forensics; Forensic Investigation of IoT Devices & Components; IoT Forensic Tools & Techniques; IoT Standards and Guidelines; Case Study

Reference Books

1. Internet of Things_ A Hands-On Approach by Arshdeep Bahga, Vijay Madisetti - Universities Press (India) Private Limited (2015)
2. A Beginner's Guide to Internet of Things Security-Attacks, Applications, Authentication, and Fundamentals - by B. B. Gupta (Author)_ Aakanksha Tewari (Author) - CRC Press (2020).
3. IoT Penetration Testing Cookbook_ Identify vulnerabilities and secure your smart devices – by Aaron Guzman, Aditya Gupta - Packt Publishing (2017)
4. Practical IoT Hacking_ The Definitive Guide to Attacking the Internet of Things – by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods - No Starch Press (2021)
5. Practical Internet of Things Security, by Brian Russell and Drew Van Duren, 2016.
6. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, by Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, 1st Edition, Academic Press, 2014.
7. Securing the Internet of Things, by Shancang Li and Li Da Xu, Elsevier, 2017
8. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, by David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017.
9. Digital Forensic Investigation of Internet of Thing Devices, Reza Montasari, Hamid Jahankhani, Richard Hill, Simon Parkinson, Springer; 1st ed. 2021 edition



CTMSDFIS SIII P3: Blockchain and Cryptocurrencies

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand concept of Blockchain
2. To learn various Use-Cases of Blockchain
3. To understand fundamental of Blockchain Security
4. To learn various Blockchain Security Techniques

UNIT-I

Introduction to Cryptography and Cryptocurrencies

Introduction, Cryptography, Hash Function, Hash Pointers and One-Way Functions, Data Structures, Digital Signatures – ECDSA, Memory Hard Algorithm, Zero Knowledge Proof, Distributed Database, Two General Problem, Byzantine General Problem and Fault Tolerance, Memory Hard Algorithm – Hashcash Implementation, Direct Acyclic Graph, Introduction to Quantum Computing and How it will break existing methods

UNIT-II

Blockchain

Introduction, Advantages over Conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain Application, Soft & Hard Fork, Private and Public Blockchain

UNIT-III

Distributed Consensus

Nakamoto Consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy Utilization, Alternate Smart Contract Construction

UNIT-IV

Cryptocurrency

History, Distributed Ledger, Bitcoin Protocols – Mining Strategy and Rewards, Ethereum Construction, Gas Limit, DAO, Smart Contract, GHOST, Vulnerabilities, Attacks, Sidechain, Name coin, Case Study related to – Naïve Blockchain Construction, Play with

Go-Ethereum, Toy Application using Blockchain

UNIT-V

Cryptocurrency Regulation

Stakeholders, Roots of Bitcoin, Legal Aspects-Cryptocurrency Exchange, Black Market and Global Economy, Applications: Internet of Things, Medical Record Management System, Domain Name Service and Future of Blockchain, Case study related to Mining Puzzles

Reference Books

1. Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton University Press, 2016 by Arvind Marayam, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder.
2. Bitcoin and Blockchain Security by Elli Androulaki and Ghassan Karame
3. Blockchain Cybersecurity, Trust and Privacy by Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo
4. Blockchain for Cyber Security and Privacy: Architectures, Challenges and Applications by Mamoun Alazab, Yassine Maleh, Mohammad Shojafar, Imed Romdhani
5. The Truth Machine: The Blockchain and the Future of Everything by Michael Casey and Paul Vigna
6. Blockchain for Distributed Systems Security by Laurent L. Njilla, Charles Kamhoua and Sachin Shetty
7. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
8. The Age of Cryptocurrency by Paul Vigna and Michael Casey
9. The Basics of Bitcoins and Blockchains by Antony Lewis
10. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher



CTMSDFIS SIII P4 EL1: Critical Infrastructure Security and Forensics

Teaching Scheme					Evaluation Scheme									
Th	Tu	Pr	C	TCH	Theory						Practical			Total
					Internal Exams				University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs		
					Marks	Hrs	Marks	Hrs						
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand the concept of ICS/SCADA and Critical Infrastructure.
2. To learn the difference between IT and OT.
3. To learn various protocols of ICS/SCADA.
4. To learn the Programming of PLC.
5. To understand the vulnerabilities of OT verticals.
6. To learn various security standards of ICS/SCADA.

UNIT– I

Introduction to ICS/SCADA system

History of ICS/SCADA, SCADA System Evolution (Industry 1.0 to Industry 4.0), SCADA System Architecture (The Purdue model), Components of ICS/SCADA Systems (Field Devices, Control Devices and Network Devices), Applications of SCADA Systems, IT v/s OT systems, Threats and Attacks in ICS/SCADA systems, Challenges and issues in ICS/SCADA Security, Case Studies.

UNIT– II

ICS/SCADA Protocols & Programming

Evolution of SCADA Protocols, SCADA Communication Protocols, Protocols in Depth (Modbus, DNP3, PROFIBUS), PLC Programming with Ladder Logic.

UNIT– III

ICS / SCADA Protocol Penetration Testing

IT Security v/s OT Security, the need of a Penetration Testing in ICS/SCADA, Asset Identifications, Vulnerabilities of ICS/SCADA, ICS Penetration-Testing Strategies, ICS/SCADA Penetration Testing Tools and Technologies, Hacking ICS Protocols.

UNIT – IV

Hacking ICS Devices and Applications: Exploiting Vulnerabilities



Buffer Overflows, Integer Bugs, Pointer Manipulation, Exploiting Format Strings, Directory Traversal, DLL Hijacking, Cross-Site Scripting, Cross-Site Request Forgery (CSRF), Exploiting Hard-Coded Values, Brute-Force and their relevance in ICS/SCADA.

UNIT-V

Security Standards, Risk and Mitigation

CIA Triad for ICS/SCADA, Common ICS Cybersecurity Standards: NIST System Protection Profile for Industrial Control Systems (SPP ICS), NIST SP 800-82, ISA/IEC 62443 (formerly ISA-99), etc., General ICS Risk Mitigation Considerations: ICS Network Considerations, ICS Host-Based Considerations, ICS Physical Access Considerations. The Risk Mitigation Process: Integrating the Risk Assessment Steps, Integrating the Risk Scenarios, performing a Cost-Benefit Analysis, Establishing the Risk Mitigation Strategy.

Reference Books

1. Industrial Automation with SCADA: Concepts, Communications and Security by K S Manoj Notion Press; 1st edition 2019.
2. Handbook of SCADA/Control Systems Security by Robert Radvanovsky, Jacob Brodsky CRC Press, 2016
3. Securing SCADA Systems by Ronald L. Krutz, Wiley Publication, Inc. 2005
4. Hacking Exposed: Industrial Control Systems by Aaron Shbeeb, Clint Bodungen, Bryan Singer, Stephen Hilt, Kyle Wilhoit, Tata McGraw Hill, 2017.
5. Industrial Cybersecurity Efficiently secure critical infrastructure systems by Pascal Ackerman, Packt Publication, 2017.
6. Cybersecurity for Industrial Control Systems_ SCADA, DCS, PLC, HMI, and SIS (2011, Auerbach Publications, CRC Press)
7. Cyber-security of SCADA and Other Industrial Control Systems (2016, Springer International Publishing)
8. Cybersecurity of Industrial Systems by Jean-Marie Flaus (2019, ISTE, John Wiley & Sons)
9. An Architecture for SCADA Network Forensics by Tim Kilpatrick M.S., Jesus Gonzalez Ph.D., Rodrigo Chandia Ph.D., Mauricio Papa, Sujeet Shenoi



CTMSDFIS SIII P4 EL2: Advanced Computer Forensics

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To Learn about Various Artefacts of Memory.
2. To Understand Windows and Linux Memory Analysis.
3. To Understand various Anti-Forensics Techniques.
4. To get Acquainted with the Emerging Domains of Computer Forensics.

UNIT – I

Introduction to Memory Forensics

Introduction to Primary Storage, Understanding Random Access Memory (RAM) and It's Working, Memory Management, Hibernation, Direct Memory Access (DMA), Address Space, Registers, Segmentation, Paging, Address Translation, Physical Address Extension, Virtual Memory, Demand Paging, Shared Memory, Stacks and Heaps, Privilege Separation, System Calls. Important Artefacts in Memory, Challenges involved in Memory Forensics, Live v/s Dead Forensics.

UNIT – II

Windows Memory Forensics

Acquiring RAM Dump from Windows Machines, Analyzing Windows RAM dump using Open-Source Tools. Understanding Windows Objects and Pool Allocation. Analyzing Processes, Handles, DLLs, Registry, Event Logs, Network Communications Disk Artefacts and Other Important Artefacts. Understanding Event Reconstruction and Timeline, Introduction to Analysis of Memory to Investigate Windows Malware

UNIT – III

Linux Memory Forensics

Understanding ELF Files, Shared Library, Global Offset Table, Procedure Linkage Table, Linux Address Translation. Acquiring RAM Dump from Linux Machines, Analyzing Linux RAM dump using Open-Source Tools. Analyzing Processes, Command-line Arguments, Handles, Bash History, Network Communications, Disk / Filesystem Artefacts and Other Important Artefacts. Understanding Event Reconstruction and Timeline. Introduction to Analysis of Memory to Investigate Linux Malware

UNIT – IV

Handling Anti-Forensic Techniques

Introduction to Cryptography, Encryption Types, Handling Encrypted Evidences, Introduction to Steganography, Handling Stego Content, Detecting Log and Timestamp Manipulations, Analyzing Anonymous Browsers and Communications, Investigating Pluggable Devices and Applications, Detecting Wiping Tools, Identifying Important Artefacts to Support use of Anti-Forensic Techniques / Tools.

UNIT – V

Emerging Domains of Computer Forensics

Introduction to Chip-Off and JTAG. Investigating Containers and Virtual Machines Investigating Cryptocurrencies and Dark web Related Cases using Computer Forensics. Using Artificial Intelligence based Solutions for Effective Forensic Investigation of Computers. Other Emerging Challenges and Domains Related to Computer Forensics.

Reference Books

1. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, et al.
2. The little handbook of Windows Memory Analysis: Just some thoughts about Memory, Forensics and Volatility! by Andrea Fortuna
3. Introduction to Modern Cryptography: Third Edition by Jonathan Katz and Yehuda Lindell
4. Applied Cryptography: Protocols, Algorithms and Source Code in C 20th Edition by Bruce Schneider
5. Codes, Ciphers, Steganography & Secret Messages by Sunil Tanna
6. Digital Watermarking and Steganography: Fundamentals and Techniques, Second Edition by Frank Y. Shih
7. Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments 1st Edition by Diane Barrett and Greg Kipper
8. Data Hiding Techniques in Windows OS: A Practical Approach to Investigation and Defense 1st Edition by Nihad Ahmad Hassan, Rami Hijazi
9. Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols 1st Edition by Michael T. Raggo and Chet Hosmer
10. Tor Darknet_ Master the Art of Invisibility



CTMSDFIS SIII P4 EL3: Cloud Security & Forensics

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. Understand key terms and concepts in cloud security and forensics
2. Understand the underlying principles in how a cloud is built and operated
3. Ability to understand the available cloud infrastructure
4. Ability to identify, analyze and remediate cloud security breaches by learning and implementing the real-world scenarios.
5. Develop policies to strengthen the security of cloud and carry out forensic analysis

UNIT – I

Introduction to cloud computing

Introduction to cloud computing, characteristic of cloud computing, cloud computing models: Service model and deployment model, cloud services and technologies, research challenges, cloud computing reference architecture, network recruitment for cloud computing. Cloud Computing Security Baseline: Overview of computer security, vulnerabilities and attacks, privacy and security in cloud storage services, privacy and security in multi clouds, cloud accountability, Understanding the Threats, Classification and countermeasures: Infrastructure and host threats, service provider threats, generic threats, threat assessment.

UNIT – II

Security Challenges in Cloud Computing

Creating a Safe Environment, Access control, The CIA model : Confidentiality, Integrity, Availability, A real-world example, The principles of security: The Principle of Insecurity, The Principle of Least Privilege, The Principle of Separation of Duties, The Principle of Internal Security, Data center security: Select a good place, Implement a castle-like structure, Secure your authorization points, Defend your employees, Defend all your support systems, Keep a low profile, Server security: The importance of logs, Where to store the logs?, Evaluate what to log, Evaluate the number of logs, The people aspect of security: Simple forgetfulness, Shortcuts, Human error, Lack of information, Social engineering, Evil actions under threats, Evil actions for personal advantage.



UNIT – III

Securing Network in Cloud

The Open Systems Interconnection model: Layer 1 – the Physical layer, Layer 2 – the Data link layer, Address Resolution Protocol (ARP) spoofing, MAC flooding and Content Addressable Memory table overflow attack, Dynamic Host Configuration Protocol (DHCP) starvation attack, Cisco Discovery Protocol (CDP) attacks, Spanning Tree Protocol (STP) attacks, Virtual LAN (VLAN) attacks, Layer 3 – the Network layer, Layer 4 – the Transport layer, Layer 5 – the Session layer, Layer 6 – the Presentation layer, Layer 7 – the Application layer, TCP/IP, Architecting secure networks, Different uses means different network, The importance of firewall, IDS, and IPS, Firewall, Intrusion detection system (IDS), Intrusion prevention system (IPS).

UNIT- IV

Securing Cloud Communications and API

Encryption security, Symmetric encryption, Stream cipher, Block cipher, Asymmetric encryption, Diffie-Hellman, RSA algorithm, Elliptic Curve Cryptography, Symmetric/asymmetric comparison and synergies, Hashing, MD5, SHA, Public key, infrastructure, signed certificates versus self-signed certificates, cipher security, Designing a redundant environment for your APIs. Identification and Authentication System and Its Dashboard identification versus authentication versus authorization, Identification, Authentication: Something you know, something you have, something you are, The multifactor authentication, Authorization: Mandatory Access Control, Discretionary Access Control, Role-based Access Control, Lattice-based Access Control, Session management, Federated identity.

UNIT– V

Securing Cloud Storage

Different storage types,: Object storage, Block storage, File storage, Securing the Hypervisor :Various types of virtualization, Full virtualization, Paravirtualization, Partial virtualization, Comparison of virtualization levels, Hypervisors: Kernel-based Virtual Machine, Xen, VMware ESXi, Hyper-V, BareMetal, Containers, Docker, Linux Containers, Criteria for choosing a hypervisor : Team expertise, Product or project maturity, Certifications and attestations, Features and performance, Hardware concerns, Hypervisor memory optimization, Additional security features, Hardening the hardware management: Physical hardware – PCI passthrough, Virtual hardware with Quick Emulator, virtualization, Hardening the host operating system, Cloud Forensics, Cloud Forensic Frameworks, Digital Forensic Investigation and Cloud Computing, Dimensions

of cloud forensics, cloud crime, challenges in cloud forensics, usages of cloud forensics, Cloud forensics tools.

Reference Books

1. Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Doston
2. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide by Brian T O'Hara
3. OpenStack Cloud Security Paperback by Alessandro Locati Fabio, PacktPub
4. Cloud Computing Security: Foundations and Challenges edited by John R. Vacca, CRC Press
5. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, John Wiley & Sons



CTMSDFIS SIII P4 EL4: Mobile Phone Security

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. Understanding the Architecture of the Mobile Devices Operating Systems like Android.
2. Understanding the security concepts of the Mobile Devices and its OS.
3. Learning the Android Application Security Testing and Auditing.

Unit –I

Introduction Android Security

Introduction to Android, Android's Architecture, Android Run Time, Android Application Framework, Introduction to Android Application component, Sandboxing, Android application inter-process communication, Application permission, Android boot process, Android partitions, File systems.

Unit – II

Android Application Pen-Testing

Configuration of lab using Santoku or Kali Linux or Mobexler or Android Studio or Genymotion, ADB commands, Configuration vulnerable application, Open GApps Project, need of ARM Translator, Mobile application security pen-testing strategy, Android application vulnerability exploitation : Insecure login, hard core issues, insecure data storage issue, input validation issues, access control issues, content provider leakage, path traversal Client-side injection attacks or other latest vulnerability or latest OWASP top 10 vulnerabilities.

Unit – III

Reverse Engineering and Secure Source Code Review

Reverse engineering using Apktool, JADX, JD-GUI, Hex Dump, Dex Dump, Reversing and Auditing Android Apps: Android application teardown and secure source code review.

Unit-IV

Android Application Security Auditing and Pen-Testing

Security auditing using Drozer, MobSF (Mobile Security Framework): Static and Dynamic Analysis, Android application security vulnerability assessment using QARK, Android dynamic instrumentation using Frida and Objection framework. Introduction to Xposed is a framework.

Unit-V

Request Interception and traffic analysis

Traffic Analysis for Android Devices, Android traffic interception, Ways to analyse Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception, Other ways to intercept SSL traffic

Reference Books

1. Android Security Internals: An In-Depth Guide to Android's Security Architecture by Nikolay Elenkov.
2. Android Hacker's Handbook by Joshua J. Drake, Zach Lanier, Georg Wicherski, Pau Oliva Fora, Stephen A. Ridley, Collin Mulliner, Wiley publication.
3. Learning Pentesting for Android Devices by Aditya Gupta, Packt Publication.



CTMSDFIS SIII P5 EL1 Database Forensics

Teaching Scheme						Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical				Total	
					Internal Exams		University Exams		University Exams (LPW)					
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs	Marks	Hrs		
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200	

* Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand the fundamentals of security, and how it relates to information systems
2. To identify assets in your organization and their values
3. To learn good password policies, and techniques to secure passwords in your organization
4. To learn concepts of database forensics.
5. To learn investigative methodology to recover artifacts from database

UNIT-I

Security and Information Technology

Introduction to Database and Database Management Systems; Role of Database in Information Systems; Objectives & Need for Database Security; Attackers and their motives; Security Architecture, Global Policies for Database Environment.

UNIT-II

Database Review

Structural Components of Database (Tuples, Keys, Queries); Models of Database; Types of Database; Database System Architecture – Three Levels of the Architecture; Client/Server Architecture; Introduction to Relational Database; Introduction to Virtual Private Database; Roles and Applications of VPD; Importance of Cryptography in Database.

UNIT-III

Database Architecture

Introduction to Oracle Architecture – Physical & Memory Structure; Introduction to MySQL Architecture – Query & Storage Engine, Database Connection Manager, Transaction & Storage Manager, Introduction to Microsoft SQL Server Architecture - Physical & Memory Structure, Buffer Management, Threads and Processes.

UNIT-IV

Database Forensics – 1

Introduction to Database Forensics; Database Artifacts – Types & Categories, Tables or Views with SQL, Privilege Changes, Changes to Security, Object Changes, ID based searches, Database Dumps, Data files, Database Users, Jobs, Triggers; Non-Database Artifacts – Webserver Logs, Application Logs, Database trace, SQL *Net Trace, Errors Logs, Security Controls and more;

UNIT– V

Database Forensics – 2

Introduction to SQL Server; SQL Server Artifacts – Types & Categories; Residential Artifacts - Data Cache, Active VLFs, Reusable VLFs, Server Logins, Database Users, Jobs, Triggers, Errors Logs, Data Files; Non- Residential Artifacts, System Event Logs, Web Server Logs, Security Controls and more; Collection of Volatile SQL Server Artifacts, Collection of Non-Volatile SQL Server Artifacts, Analysis of Collected Artifacts – Database Server Versioning, Recovering Deleted Data Files, Recovering Transaction Log, Recovering Query Logs and more; Execution of SQL Server Data Collection Scripts.

Reference Books

1. Database Security by Alfred Basta, Melissa Zgola, Dana Bullaboy, Thomas L. Whitlock Sr. (Published by Course Technology, Cengage Learning)
2. Database Security and Auditing: Protecting Data Integrity and Accessibility, by Hassan A. Afyouni (Published by Cengage Learning)
3. Database Forensics: A Clear and Concise Reference by Gerardus Bkijdyk
4. Oracle Incident Response and Forensics – Preparing for and Responding to Data Breaches by Pete Finnigan (Published by Apress)
5. SQL Server Forensic Analysis by Kevvie Fowler (Publication – Addison-Wesley)



CTMSDFIS SIII P5 EL2: Social Network Analysis

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. Students will learn social media working concepts.
2. Students will learn social media based online data investigations and analysis.
3. Students will learn the intelligence gathering concepts from open source available data.

UNIT – I

Social Networking

Fundamentals of Social Networking, Social Networking viral, why social networking is popular, Psychology & Sociology for Online Media, Concepts of Geospatial Information System, How Facebook works?

UNIT – II

Social Media & Legal Implication

Graph Theory and Social Networks, Markets and Strategic Interactions in Networks, Information Networks and the World Wide Web, Network Dynamics: Population and Structural Models, Legal aspects of Privacy in India, Institutions and Aggregate Behavior, Social Media and its impact on Business, Politics, Law and Revolutions, Legal Responsibilities for Social Networking.

UNIT – III

Information Gathering from Resources

Intelligence gathering, People searching, OSINT, Deep Web, Defamatory content analysis, Multimedia forensics over Social Networking, Emerging Trends in Social Networks

UNIT – IV

Social Networking exploitation and hacking

Introduction: hacking on Twitter data Micro formats: semantic Markup and common sense collide, Twitter: friends, followers, and set wise operations, Twitter: the tweet, LinkedIn: clustering your professional network for fun (and profit?), cosine similarity, and collocations, Facebook: the hackers outlook.

UNIT – V

Social Networking Forensics

Twitter GPS & Account Data, Hidden Social Network Content, Cell Phone Owner Information, Hidden Photo GPS & Metadata, Deleted Websites & Posts, Website Owner Information, Alias Social Network Profiles, Additional User Accounts, Sensitive Documents & Photos, Live Streaming Social Content, Videos Uploaded by Location, Newspaper Archives & Scans, Social Content by Location, Text Transcripts of Videos, Historical Satellite Imagery, Duplicate Copies of Photos, Public Government Records, Document Metadata, Voter Registration Records, Facebook Wall Posts

Reference Books

1. Social Network Analysis: Methods and Applications by Katherine Faust and Stanley Wasserman
2. Social network analysis by John Scott
3. Models and Methods in Social Network Analysis by Stanley Wasserman, Peter J. Carrington, John Scott
4. The SAGE Handbook of Social Network Analysis by John Scott, Peter J. Carrington
5. Analysing Social Networks by Jeffrey C. Johnson, Martin G Everett, and Stephen Borgatti
6. Social Network Analysis: Methods and Examples by Franziska B. Keller, Lu Zheng, and Song Yang
7. Social Network Analysis by David Knoke and Song Yang
8. The Development of Social Network Analysis by Linton Freeman
9. Advances in Social Network Analysis: Research in the Social and Behavioural Sciences by Joseph Galaskiewicz, Stanley Wasserman
10. Understanding Social Networks: Theories, Concepts, and Findings by Charles Kadushin



CTMSDFIS SIII P5 EL3: Drone Forensics

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives:

1. To develop understanding of Drones and its architecture.
2. To understand the various protocols used in Drone communication and management.
3. To understand the legal and regulatory aspects related to Drone and its forensics.
4. To understand the principles and procedure involved in Drone forensics.
5. To develop understanding to investigate Drone incidents and conduct Drone forensics

UNIT – I

Introduction to Drones

Introduction to Drones, classification of Drones, Major components of Drones, Capacity and Capability of drones, Drone payloads, Criminal use of Drones, Drone seizure and handling at crime scene, Case studies

UNIT – II

Drone Architecture

Drone hardware and software components, Drone network and communication protocols, Drone Architecture, Drone components and controller identification, Controller options- Mobile and Tablet devices, Bespoke flight controllers, FPV controllers, Drone assembling and flying

UNIT – III

Drone Legal and Regulatory Aspects

Domestic Laws on Drones, Drone Regulations, International Laws on Drones, International guidelines and regulations on Drones, Evidence Integrity, Chain of custody, Presentation of evidence.

UNIT – IV

Drone Forensics part -I

Introduction to digital forensics, digital forensics principles, digital forensic fields/sub-fields applicable to Drone forensics, Evidence integrity and standard forensic practices, Evidence continuity, Identifying makes and models, Initial examination and case review,

identifying damage or customized Drone, Drone adaptability and modifications, Evidence data locations, Extraction techniques and tools, Extracting removable storage mediums, Preservation of evidence.

UNIT – V

Drone Forensics part II

Extraction of data from the aircraft, extraction of data from mobile and tablet device, disassembling techniques, interpretation of data, techniques in using open source and commercial forensic tools to review the evidence, interpretation of data contained on the Drone, Extracting registered user information, Identifying Drone details, Flight log analysis techniques, Flight path recreation, Interpretation of data from portable devices, default folder structures of the controlling App from an Android and iOS device, synchronized logs vs. local logs, Media file examination (Geolocations and dates & times), workflows in combining offline files for further analysis, techniques in the interpretation of additional data on other devices, Corroboration of evidence and Report writing.

Reference Books

1. Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, by Joakim Kävrestad. 2nd ed. 2020.
2. Edition Digital Forensics Explained 2nd Edition by Greg Gogolin, CRC Press; 2nd edition, 2021.
3. Digital Forensics for Drones: A Study of Tools and Techniques, by Sowmya Viswanathan Zubair Baig, Chapter published in Springer International Conference on Applications and Techniques in Information Security. Available: <https://link.springer.com/conference/atis>
4. Interpol Framework for Responding to a Drone Incident for First Responders and Digital Forensics Practitioners.
5. Ministry of Civil Aviation, The Drone Rules, 2021.
6. Information Technology Act 2000 (amendment 2008).



CTMSDFIS SIII P5 EL4: Research Methodology

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
03	01	00	04	04	25	00:45	50	01:30	100	03:00	-	-	200

Objectives:

1. To understand basic concepts of research and its methodologies
2. To identify appropriate research topics
3. To select and define appropriate research problem and parameters
4. To learn how to prepare a project proposal to undertake a project or a grant
5. To learn how to organize and conduct research on advanced projects in a more appropriate manner
6. To learn how to write a research report and thesis based on the research.

UNIT – I

Objectives and types of research: Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, Conceptual vs. Empirical. Research Formulation, Literature review and Development of hypothesis

UNIT – II

Research design and methods, Developing a research plan - Exploration, Description, Diagnosis, Experimentation. Determining experimental and sample designs

UNIT – III

Data Collection and analysis: Methods of data collection – Sampling Methods and Data Processing. Data Analysis: Types of data, Basic concept of frequency distribution, measure of central values – Mean, median and mode, measure of dispersion, range, mean deviation and standard deviation, probability, theory and classical definition of probability, Bayes theorem of probability, conditional probability and coincidence probability, Chi-square test, ANOVA, SPSS. Types of Errors and Interpretation of Findings.

UNIT – IV

Reporting and thesis writing: Structure and components of scientific reports and thesis, Significance and Different steps in the preparation, Illustrations, Bibliography. Presentations: Oral and Poster, Importance of effective communication in scientific research.

UNIT – V

Basics of Ethical issues, Intellectual property rights, Copy right, Reproduction of published material: Plagiarism in scientific research and communications.

Reference

1. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, U.K., 2002. An introduction to Research Methodology, RBSA Publishers.



CTMSDFIS SIII L1: Network Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SIII L2: IoT Security & Forensics Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SIII L3: Blockchain & Cryptocurrency Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SIII L4: Program Elective 1 Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



CTMSDFIS SIII L5: Program Elective 2 Laboratory

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams			University Exams		University Exams (LPW)			
					TA-1/TA-2		MSE		Marks	Hrs			
					Marks	Hrs	Marks	Hrs	Marks	Hrs			
00	00	01	01	02	--	--	--	--	--	--	100	03:00	100

Experiments / Practicals to support the associated theory course.



National Forensic
Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

SEMESTER- IV



CTMSDFIS SIV P1 Major Project

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory				Practical		Total		
					Internal Exams		University Exams		University Exams (LPW)				
					TA-1/TA-2	MSE	Marks	Hrs	Marks	Hrs			
00	10	10	20	30	25	00:45	50	01:30	100	03:00	-	-	200

Students will need to work on a major project under guidance of internal faculty members. The students will need to submit a regular progress report for internal evaluation. A project report will need to be submitted and presented at the end of the semester for final evaluation.