Program Structure and Syllabus
for
M.Sc. Digital Forensics and Information Security

2021-22 Onwards

ADIKAVI NANNAYA UNIVERSITY

RAJAMAHENDRAVARAM

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM
BOARD OF STUDIES MEETING – FORENSIC SCIENCE
Date: 28-10-2021

AGENDA:

1. Eligibility and Entrance Examinations
2. Syllabus finalization
3. Syllabus for practicals
4. Number of teaching hours / Periods theory / Practicals
5. Model Question Papers
6. Credits / Evaluation
7. Scheme of Valuation
8. List of Examiners for paper setting
9. List of Practical Examiners

Members:

1. Dr. D. Kalyani, Asst. Prof.,
   Dept. of Zoology, AKNU, RJY, - **Chairman**

2. Mr.E.Mohan, Principal,
   Aditya Degree College, Surampalem - **Convener**

3. Dr. N. Kala Bhaskar, Asst. Prof.
   University of Madras, Chennai - **Member**

4. Dr. Komal Saini, Professor,
   Panjabi University - **Member**

5. Dr. P. Uma Maheshwara Rao, Prof. & Head,
   Forensic Medicine & Toxicology,
   Rangaraya Medical College, Kakinada - **Member**

6. Dr. Satyan, Scientist (Retd),
   CFSL Hyderabad - **Member**

RESOLUTIONS:

The common Board consisting of the above members have met on blended mode in the O/o Dean, Academic Affairs, Adikavi Nannaya University, Rajamahendravaram on 28/10/2021 and considered the enclosed agenda. After thorough deliberations and discussions, the Board members have resolved the following.

1. A B.Sc. graduate with “Chemistry or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Forensic Science-Questioned Documents and Fingerprints.

2. A B.Sc. graduate with “Chemistry or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Forensic Science - Chemistry and Toxicology.

3. A B.Sc. graduate with “Biology or Forensic Science” as one of the subjects is eligible to apply for admission into M. Sc. Forensic Science - DNA Finger Printing.

4. A B.Sc. graduate with “Computer Science or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Cyber Security.

5. A B.Sc. graduate with “Computer Science or Forensic Science” as one of the subjects is eligible to apply for admission into M.Sc. Digital Forensics and Information Security.

6. The members formulated the syllabus for M.Sc Forensic Science, a 2 year program on par with other Universities in the Country to be implemented from academic year 2021-22.

7. The syllabus for practicals of the above courses was formulated on par with UGC model curriculum.

8. There shall be 4 to 5 hours per week for each theory paper & 3 hrs for each practical.

9. I & II Semesters are common for M.Sc Forensic Science - Questioned Documents & Fingerprints, M.Sc Forensic Science - Chemistry and Toxicology, M.Sc Forensic Science - DNA Finger Printing

10. III Semester is having specialization i.e, Questioned Documents & Fingerprints in M.Sc Forensic Science - Questioned Documents & Fingerprints, Chemistry and Toxicology in M.Sc Forensic Science - Chemistry and Toxicology, DNA Finger Printing in M.Sc Forensic Science - DNA Finger Printing.

11. IV Semester will be project cum Internship for all M.Sc. Programs M.Sc Forensic Science - Questioned Documents & Fingerprints, M.Sc Forensic Science - Chemistry and Toxicology, M.Sc Forensic Science - DNA Finger Printing, M.Sc. Cyber Security, M.Sc. Digital Forensics and Information Security.

12. Marks and credits are allotted to theory & practical papers in each semester. There will be 100 marks for each theory, and 200 marks for 2 practicals each 100 marks and total marks for each semester 600 x 4 semester 2400 marks.

13. Examination pattern will be as follows.

a) Each theory paper will be evaluated for 100 marks out of which75% of marks, for Semester End Examination (SEE) while the remaining 25% marks for Continuous Internal Assessment (CIA)

Continuous Internal Assessment		
S. No	Scheme of Evaluation	Marks
1	Mid-Semester Examination	10M
2	Assignment/Seminar Presentation	5M
3	Attendance	5M
4	Swachhata Activity	5M
Total		25M

Details of Attendance Marks		
S.No	Attendance	Marks Allotted
1	95% above	5
2	85-94%	4
3	75-84%	3
4	65-74%	2
5	55-64%	1
6	< 54%	0
Total		25M

b) The Semester End Examination question paper comprises of two sections –Section A & B, Section A consists of 4 questions one question from each unit of syllabus with internal choice ‘a’ or ‘b’. Section-B consists of 8 short questions two from each unit of the syllabus, with internal choice out of which only 5 are to be attempted

c) Similarly, each practical will be evaluated for a total of 100 marks, out of which 75% of marks for Semester End Examination (75 Marks) and 25% (25 Marks) for Continuous Internal Assessment.

14. A comprehensive viva-voce will be conducted for students at the end of IV Semester for 100 marks carrying 4 credits.

15. IV Semester Students should do their project cum internship at Forensic Science Laboratories, Police Stations, Cyber cells, Fingerprint Bureau, National Crime Records Bureau, National Forensic Sciences University, Rashtriya Raksha University, Directorate of Forensic Science Services, Centre for Development of Advanced Computing (C-DAC), National Institute of Nutrition, Centre for DNA Fingerprinting and Diagnostics – CDFD, Council of Scientific And Industrial Research–Centre for Cellular and Molecular Biology (CSIR–CCMB), Indian Institute of Chemical Technology (CSIR-IICT), Central Detective Training Institute, etc. and thesis must be submitted to the college and University.

M.Sc. Forensic Science
SEMESTER END EXAMINATION
Theory Model Question Paper pattern

Time: 3 hrs **Max. Marks: 75**

Section-A

Answer all questions. Each question carries 15 marks. **4x15=60**

Q1. Unit-1

a or b

Q2. Unit-2

a or b

Q3. Unit-3

a or b

Q4. Unit-4

a or b

Section-B **5x3=15**

Q5. It contains 8 short questions with at least two from each unit, carrying 3 marks.

5 questions are to be answered.

M.Sc. Digital Forensics and Information Security

Scheme of Examination

Code	Title of the Paper	L	P	Total (Hrs)/ Week	Duration of Exam (hrs)	External Marks	Internal Marks	Total Marks	Credits
I Semester									
MSFS121	Cyber Laws and Intellectual Property Rights	4	3	7	3	75	25	100	4
MSFS122	Forensic Application Development and Networking Concepts	4	3	7	3	75	25	100	4
MSFS123	Modern Cryptography and Steganography	4	3	7	3	75	25	100	4
MSFS124	Network Security and Forensics	4	3	7	3	75	25	100	4
Lab Course									
MSFS125	Forensic Application Development and Networking Concepts Lab				3	75	25	100	4
MSFS126	Network Security and Forensic Lab				3	75	25	100	4
II Semester									
MSFS221	Digital Forensics Part-1	4	3	7	3	75	25	100	4
MSFS222	Vulnerability Assessment and Penetration Testing	4	3	7	3	75	25	100	4
MSFS223	Forensics of Embedded Systems	4	3	7	3	75	25	100	4
MSFS224	Fundamentals of E-Discovery	4	3	7	3	75	25	100	4
Lab Course									
MSFS225	Digital Forensics -1 & E-Discovery Lab				3	75	25	100	4
MSFS226	VAPT & Forensics of Embedded Systems Lab				3	75	25	100	4
III Semester									
MSFS321	Digital Forensics Part-2	4	3	7	3	75	25	100	4
MSFS322	Mobile Security and Forensics	4	3	7	3	75	25	100	4
MSFS323	Cloud security and Forensics	4	3	7	3	75	25	100	4
MSFS324	Malware Analysis	4	3	7	3	75	25	100	4
Lab Course									
MSFS325	Digital Forensics-2 & Mobile Security Lab				3	75	25	100	4
MSFS326	Malware Analysis & Cloud security Lab				3	75	25	100	4
IV Semester									
MSFS421	Comprehensive viva-voce							100	4
MSFS422	Project					500	100	600	24
Total								**2500**	**100**

M.Sc. Digital Forensics and Information Security

I Semester, Paper I

MSFS121- Cyber Laws and Intellectual Property Rights

Aim and Objectives of Course: Understanding Cyber Space, Defining Cyber Laws, Scope and jurisprudence and the I.T. Act with its Amendments. Also covering the Intellectual Property Rights, Income Tax Act, Indian Penal Code, and Indian Evidence Act.

Learning Outcomes

1. Overview of Indian Legal System
2. IT Act 2000, and its Amendments in IT Act (till date)
3. Income Tax Laws
4. Indian Penal Code and Indian Evidence Act
5. Intellectual Property Rights
6. Copyright Infringements

Unit I- Introduction

Basics of Law, Understanding Cyber Space, Defining Cyber Laws, Scope and jurisprudence, Concept of Jurisdiction, Cyber Jurisdiction, Overview of Indian Legal System, Introduction to IT Act 2000, and its Amendments in IT Act (till date), Cyber Laws of EU-USA-Australia-Britain, other specific Cyber laws, Indian Penal Code, Indian Evidence Act.

Unit II- Significance of I.T. Act

E-signature and E-governance legality under I.T. Act, 2000, Cyber Contraventions, Compensation & Crimes under I.T. Act,2000. ISPs and Websites Legal Liability under I.T. Act, 2000.

Corporate Legal Liability, Adjudication Process for Recovery of Losses under I.T. Act,2000, Adjudication Process For Recovery of Losses under I.T. Act, 2000.

Policy, Law and Cyber Security community; Indian IT Act, Indian Penal Code, Income Tax Law; International Standards - IPR, COBIT, security audit.

UNIT III- Income Tax Laws, IPC & IEA

Taxation Issues in Cyber Space, IT Act, and its relation with Income Tax Law. IT Act and its relation with Indian Penal Code, Case Studies and Case Laws, Relevant section of other Acts such as IPC, Indian Evidence Act, etc.

Blocking websites, telephone tapping, packet sniffing, Dark web monitoring, social media monitoring.

UNIT IV- Intellectual Property Rights (IPR) & Copyright Infringement

IPR & Cyber Space, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO, Intellectual Property Rights, Understanding Patents, Understanding Trademarks, Trademarks in Internet, Domain name registration, Software Piracy, Legal Issues in Cyber Contracts, Authorship, Document Forgery.

Reference Books:

1. Information Security and Laws by Saurabh Sharma
2. Cyber Frauds, Cybercrimes and Law in India by Pavan Duggal
3. The Internet Law of India: Indian Law Series by Shubham Sinha
4. Cyber Laws – Indian and International Perspectives on Key topics including Data Security, Commerce, Cloud Computing and Cyber Crimes by Aparna Vishwanathan

M.Sc. Digital Forensics and Information Security

I Semester, Paper II

MSFS122- Forensic Application Development and Networking Concepts

Aim and Objectives of Course: Understanding the different programming languages along with Link Layer Devices and Protocols, Firewalls and Network Defence.

Learning Outcomes

1. Python Programming
2. Perl Programming
3. Link Layer Devices
4. Firewalls
5. Intrusion Detection Systems

Unit I- Python Basics

Python Setup, debugging, Variables, Strings, Lists, Dictionaries, Networking, Selection, Exception Handling, Function, Iteration, File I/O, Sys Module, OS Module, Comments And Pound Characters, Numbers And Math, Variables And Names, Conditional Statements, Classes and Objects (OOP) Is-A, Has-A, Inheritance and Composition.

Unit II- Introduction to Perl programming and Bash Scripting

Introduction, Data types, Conditional and iteration statements, Array and Lists, Subroutines, Regular Expressions, File Handling, Introduction to Bash Scripting.

Unit III- Link Layer Devices and Protocols

Link Layer Devices, MAC Addresses, IP and MAC Addresses, Broadcast MAC Addresses, Switches: Multi-switch Networks Segmentation, Multi-switch Example, Multi-switch and Router Example, Forwarding Tables, CAM Table Population, ARP, Hubs, TCP and UDP Ports, Ports Examples, Well-knows Ports, TCP And UDP Headers, TCP Header, UDP Header, Netstat Command, TCP Three-way Handshake.

Unit IV- Firewalls and Network Defence

Firewalls, Packet Filtering Firewalls, Packet Filtering vs. Application Attacks, Packet Filtering vs. Trojan horse, Application Layer Firewalls, IDS: NIDS, HIDS, IPS, NAT and Masquerading. DNS, DNS Structure, DNS Name Resolution, DNS Resolution Example, Resolvers and Root Servers, Reverse DNS Resolution, More about the DNS. Wireshark, NIC Promiscuous Mode, Configuring Wireshark, The Capture Window, Filtering, Capture Filters, Display Filters.

Reference Books:

1. Violent Python: A Cookbook for Hackers, Forensic Analysis, Penetration Testers and Security Engineers Import by TJ O’Connor
2. Learning Perl by Randal L. Schwartz, O’Reilly Media
3. Penetration Testing: A Hands-On Introduction to Hacking, 1st Edition by Georgia Weidman
4. Computer Security Principles and Practice by William Stallings Pearson.

M.Sc. Digital Forensics and Information Security

I Semester, Paper III

MSFS123- Modern Cryptography and Steganography

Aim and Objectives of Course: Understanding Cryptographic Keys and Algorithms and solving Steganography using different techniques.

Learning Outcomes

1. Communication using Symmetric Cryptography
2. Pseudo Random Sequence Generators
3. Cryptographic Algorithms
4. Steganography Techniques
5. Cryptanalysis Techniques

Unit I- Introductions

Basic Terminology, Protocols, Communication using Symmetric Cryptography, Introduction to One-way Functions, Public-Key Cryptography, Introduction to Digital Signatures, Random ad Pseudo Random Sequence Generators. Introduction to Basic, Intermediate, Advanced and Esoteric Protocols.

Unit II- Cryptographic Keys

Introduction, Key Length: Symmetric Key, Public-Key, Key Management: Generating, Transferring, Verifying, Using, Updating, Storing, Destroying, Lifetime, Backup, Compromised Keys. Algorithms: Types, Modes and Use.

Unit III- Cryptographic Algorithms

Mathematical Background: Introduction to information Theory, Number Theory, Factoring, Prime Number Generation, DES: Background, Description, Security, Cryptanalysis, Variants, One-Way Hash Functions: MD, SHA, Other one-way functions. Public-Key Algorithms: RSA, DSA, and others like ECDSA and Introduction to Quantum Computing.

Unit IV- Steganography

Introduction and History, Need of Data Hiding, Cryptography V/S Steganography, Steganography Techniques, Network Steganography, Steganography Tools, Steganography in Smart Phones, Various Steganography Algorithms.

Introduction to Cryptanalysis and Steganalysis, Introduction to tools used, technologies used in Cryptanalysis, Steganalysis, Different Attacks and their outcome.

Reference Books:

1. Applied Cryptography by Bruce Schneier
2. Cryptology Unlocked by Reinhard Wobst
3. Break the Code: Cryptography for Beginners by Bud Johnson
4. Modern Cryptography: Applied Mathematics for Encryption and Information Security by Chuck Easttom
5. Cryptography Engineering: Design Principles and Practical Applications by Niels Ferguson, Bruce Schneier and Tadayoshi Kohno
6. Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell
7. Modern Cryptography: Theory and Practice by Wenbo Mao
8. Steganography in Digital Media: Principles, Algorithms, and Applications by Jessica Fridrich
9. Investigator's Guide to Steganography by Gregory Kipper
10. Hiding in Plain Sight: Steganography and the Art of Covert Communication by Eric Cole
11. Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols by Michael T. Raggo and Chet Hosmer
12. Noiseless Steganography: The Key to Covert Communications by Abdelrahman Desoky
13. Digital Watermarking and Steganography by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich and Ton Kalker
14. Steganalysis by means of Artificial Neural Networks: Steganography detection in JPEG files by means of Artificial Neural Networks using Huffman coding by Jiri Holoska and Zuzana Kominkova Opiatkova
15. Security to Images - Steganalysis Algorithms by Yogesh Daga

M.Sc. Digital Forensics and Information Security

I Semester, Paper IV

MSFS124- Network Security and Forensics

Aim and Objectives of Course: Understanding Practical Investigative Strategies and working with Network Intrusion Detection and Analysis

Learning Outcomes

1. Wireless Network Forensics
2. Investigate Switches, Routers, Firewalls and Web Proxies
3. Sniffing, Higher-Layer Protocol Awareness
4. Comprehensive Packet Logging

Unit I- Practical Investigative Strategies

Real-World Cases: Hospital Laptop Goes Missing, Catching a Corporate Pirate, Hacked Government Server, Footprints, Concepts in Digital Evidence, Real Evidence, Best Evidence. Direct Evidence, Circumstantial Evidence, Hearsay, Business Records, Digital Evidence, Network-Based Digital Evidence, Challenges Relating to Network Evidence, Network Forensics investigative Methodology (OSCAR), Obtain Information, Strategize, Collect Evidence, Analyze Report.

Unit II- Wireless Network Forensics

Wireless Network Forensics Unplugged. The IEEE Layer 2 Protocol Series, Why So Many Layer 2 Protocols? The 802.11 Protocol Suite, 802.1X, Wireless Access Points (WAP's), Why Investigate Wireless Access Points? WAP Evidence, Wireless Traffic Capture and Analysis, Spectrum Analysis, Wireless Passive Evidence Acquisition, Analyzing 802.11 Efficiently, Common Attacks, Sniffing, Rogue Wireless Access Points, Evil Twin, WEP Cracking, Locating Wireless Devices, Gather Station Descriptors, Identify Nearby Wireless Access Points, Signal Strength, Skyhook.

Unit III- Switches, Routers, and Firewalls

Storage Media, Switches, Why Investigate Switches?, Content-Addressable Memory Table Address Resolution Protocol, Types of Switches, Switch Evidence, Routers, Why Investigate Routers?, Router Evidence, Why Investigate Firewalls?, Firewall Evidence, Interfaces, Simple Network Management Protocol (SNMP), Proprietary Interface, Logging, Local Logging, Simple Network Management Protocol, syslog Authentication, Authorization, and Accounting Logging 355.

Web Proxies: Why Investigate Web Proxies?, Web Proxy Functionality, Caching URL Filtering, Content Filtering, Distributed Caching, Evidence, Types of Evidence, Obtaining Evidence, Squid, Squid Configuration, Squid Access Logfile, Squid Cache, Web Proxy

Analysis, Web Proxy Log Analysis Tools, Example: Dissecting a Squid Disk Cache, Encrypted Web Traffic, Transport Layer Security (TLS), Gaining Access to Encrypted Content, Commercial TLS SSL Interception Tools.

Unit IV- Network Intrusion Detection and Analysis

Why Investigate NIDS/NIPS? Typical NIDS/NIPS Functionality, Sniffing, Higher-Layer Protocol Awareness, Alerting on Suspicious Bits, Modes of Detection, Signature-Based Analysis, Protocol Awareness, Behavioral Analysis, Types of NIDS/NIPSs, Commercial, Roll-Your-Own NIDS/NIPS Evidence Acquisition, Comprehensive Packet Logging, Snort, Basic Architecture, Configuration, Snort Rule Language.

Reference Books:

1. Introduction to Security and Network Forensics by William J. Buchanan CRC Press
2. Network Forensics: Tracking Hackers through Cyberspace by Person

I SEMESTER PRACTICALS

MSFS 125 – Forensic Application Development and Networking Concepts Lab

1. Write and Implement Python Programs.
2. Write and Implement Perl Programs.
3. Write and execute Bash Scripts.
4. Implement Packet Filtering Firewalls.
5. Perform the following operations using Wireshark:
    - Configuring Wireshark,
    - The Capture Window, Filtering,
    - Capture Filters,
    - Display Filters

MSFS 126 – Network Security and Forensic Lab

1. Investigate Switches, Routers.
2. Investigate Firewalls, Web Proxies.
3. Perform the Web Proxy Log Analysis using different tools.
4. Implement the Comprehensive Packet Logging.
5. Install an IDS and use the Snort Rule Language on the host system.

M.Sc. Digital Forensics and Information Security

II Semester, Paper I

MSFS221- Digital Forensics Part-1

Aim and Objectives of Course: Understating the Phases of digital/computer forensics investigation and Imaging/acquisition & data recovery processes.

Learning Outcomes

1. Collection/Acquisition and preservation of digital evidence.
2. Compilation of findings & Reporting.
3. Acquisition of stand-alone machine (both physical & logical).
4. Acquisition or triage collection of live system.
5. Deleted data recovery techniques.
6. Analysis of registry in various operating systems.
7. Log analysis of standalone machine and server.

Unit I- Introduction

Introduction to Digital Forensics, Locard's Principle of Exchange in Digital Forensics, Branches of Digital Forensics, Phases of digital/computer forensics investigation, Identification of digital evidences, necessary documentations such as Chain of Custody, pre-acquisition forms etc., Digital evidence handling at crime scene as per standards, Collection/Acquisition and preservation of digital evidences, Processing & analysis, Compilation of findings & Reporting, Pre-requisite for setting up Digital Forensic lab and global standards.

Unit II- Imaging/acquisition & data recovery

Acquisition of stand-alone machine, peripheral device, other storage media, CCTV, systems (both physical & logical), Acquisition or triage collection of live system, Acquisition of mobiles, PDA's, Tablets, Navigation systems etc., Acquisition over the network i.e. remote acquisition, Understanding of various acquisition software/hardware device, details of various file formats of forensic image, Deleted data recovery techniques.

Unit III- Registry and Logging

Understanding and in-depth analysis of registry in various operating systems, Log analysis with respect to standalone machine and server, which includes system logs, kernel logs, event logs, ftp/sftp, application Web Servers/ Proxy logs.

Unit IV- Computer and Mobile Forensic Analysis

Introduction to DFF, Working with Autopsy and other tools to solve a Cyber Crime, Introduction to Digital forensic tools, various features of these tools, solving a case using various digital forensic tools, Understanding of other intermediate tools for data processing, keyword search & analysis etc, Encryption handling techniques.

Reference Books:

1. The Basics of Digital Forensics: The Primer for getting started in Digital Forensics by Sammons
2. Digital Forensics Workbook: Hands-on Activities in Digital Forensics by Michael K Robinson
3. Computer Forensics and Cyber Crime: An Introduction by Marjie T. Britz
4. Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey
5. Forensic Computing -A Practitioner's Guide by Tony Sammes, Brian Jenkinson
6. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher Steuart
7. Handbook of Digital Forensics and Investigation by Eoghan Casey
8. Digital Forensics Explained by Greg Gegolin
9. Windows Registry Forensics (WRF) with Volatility Framework: Quick Startup Guide for Beginners by Kapil Soni
10. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Windows Registry by Harlan Carvey
11. File System Forensic Analysis by Brian Carrier
12. EnCase Computer Forensics- The Official EnCE: EnCase Certified Examiner Study Guide by Steve Bunting
13. Computer Forensics and Digital Investigation with EnCase Forensic v7 by Suzanne Widup
14. Computer Forensics with FTK by Fernando Carbone
15. Digital Forensics with the AccessData Forensic Toolkit (FTK) by John Sammons
16. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management by Anton A. Chuvakin and Kevin J. Schmidt

M.Sc. Digital Forensics and Information Security

II Semester, Paper II

MSFS222- Vulnerability Assessment and Penetration Testing

Aim and Objectives of Course: Understanding about Vulnerability Assessment and Web Application Pentesting using different tools.

Learning Outcomes:

1. Vulnerability using W3uf and Nikto, Nessus tools.
2. Fingerprinting with netcat, OpenSSL, httprint.
3. Exploiting Misconfigured HTTP Verbs.
4. Implementing different Password Attacks.
5. Implementing various Buffer Overflow Attacks.
6. Understanding the Overflows in the Stack.

Unit I- Vulnerability Assessments and Social Engineering

Introduction to Vulnerability Assessment, Life cycle of Vulnerability Assessment, Vulnerability Scanners, Manual Testing, Vulnerability using W3uf and Nikto, Nessus, Architecture, Introduction to Unknown Vulnerability Assessment.

Unit-2: Footprinting and Scanning

Footprinting: Mapping a Network: Why Map a (Remote) Network, Ping Sweeping: Fping, Nmap Ping Scan, OS Fingerprinting: Fingerprinting with Nmap Port Scanning: Under the Hood of a Port Scanner: TCP Three Way Handshake, Scanning with Nmap: Nmap Scan Types, TCP Connect Scan with Nmap, TCP SYN Scan with Nmap, Version Detection with Nmap, Specifying the Targets: By DNS Name, With an IP Addresses List, By Using CIDR Notation, By Using Wildcards, Specifying Ranges, Octets Lists, Combining the Previous Methods, Choosing the Ports to Scan, Nmap Examples, Port Scanning. Service Detection, Vulnerabilities Database Lookup.

Unit III- Web Application Pentesting

Fingerprinting: Introduction, Web Server Fingerprinting: Fingerprinting with Netcat, Fingerprinting with Netcat Examples, Common Mistakes, Fingerprinting with OpenSSL, Limits of Manual Fingerprinting, Fingerprinting with Httprint, HTTP Verbs: GET, POST, HEAD, PUT, DELETE, OPTIONS, Using HTTP 1.0 Syntax, Exploiting Misconfigured HTTP Verbs: Enumeration with OPTIONS, Exploiting DELETE, Exploiting PUT, Uploading a PHP Shell with PUT, Directories and File Enumeration: Brute-force, Dictionary-based Enumeration. Cross Site Scripting, XSS Actors, Vulnerable Web Applications, Users, Attackers, Finding an XSS, Reflected XSS Attacks, Reflected XSS Filters, Persistent XSS Attacks, Persistent XSS Attack Examples, Cookie Stealing via XSS, DOM XSS SQL Injections: SQL Statements, SELECT Example, UNION Example, SQL Queries Inside Web Applications, Vulnerable Dynamic Queries, Finding SOL Injections, Example - Finding SQL Injections, From Detection to Exploitation, Boolean Based SQL Injections, Exploiting a Boolean Based SQL Injection, Scripting Boolean Based SQL

Injections, UNION Based SQL Injections, Exploiting UNION SQL Injections, SQL Injection (Blind), SOL Map with all options.

Password Attacks- Brute Force Attacks: A Brute Force Algorithm, Brute Force Weaknesses, Dictionary Attacks, Performing a Dictionary Attack, Weaknesses of Dictionary Attacks, Mangling Words, John the Ripper, Unshadow, Brute Force with John the Ripper, Dictionary Attacks with John the Ripper, Installing Password Dictionaries, Rainbow Tables, Rainbow Tables Limitations, Ophcrack, Burp Suite: Intercepting Proxies, Intercepting Proxy Example, Proxy Server Example, Burp Proxy, Burp Proxy Configuration, Burg Repeater, Buffer Overflow Attacks: Buffers, Buffer Overflow Example, The Stack, Push Operation, Pop Operation, Allocating Space on the Stack.

Unit IV- Metasploit

Introduction, MSFConsole, identifying a Vulnerable Service, Searching, Configuring an Exploit. Configuring a Payload, Running an Exploit, Meterpreter: Bind and Reverse, Launching Meterpreter, Session, Information Gathering with Meterpreter, System Information, Network Configuration, Routing Information, Current User, Privilege Escalation, Bypassing UAC, Dumping the Password Database, Exploring the Victim System Uploading and Downloading files, Running JOS Shell.

Overflows in the Stack, The Stack and Applications, How Buffer Overflow Attacks works, Null Session Vulnerability, Command Execution, Cross Site Request Forgery, File Inclusion, File Upload, Insecure Captcha, SSRF/XSPA, OWASP top ten vulnerability, Common Vulnerability Scoring System (CVSS), Pentesting process i.e., format of a vulnerability report (OSCP report). Lifecycle of a penetration test and the process involved in pentesting.

Reference Books:

1. Social Engineering: The Science of Human Hacking by Christopher Hadnagy
2. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert by Dr. Erdal Ozkaya
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto
4. Metasploit: The Penetration Tester's Guide by David Kennedy, Jim O'Gorman, et al.
5. Metasploit for Beginners: Create a threat-free environment with the best-in-class tool by Sagar Rahalkar
6. The Complete Metasploit Guide: Explore effective penetration testing techniques with Metasploit by Sagar Rahalkar and Nipun Jaswal
7. Hands-On Web Penetration Testing with Metasploit: The subtle art of using Metasploit 5.0 for web application exploitation by Harpreet Singh and Himanshu Sharma
8. Mastering Metasploit: Exploit systems, cover your tracks, and bypass security controls with the Metasploit 5.0 framework, 4th Edition by Nipun Jaswal

M.Sc. Digital Forensics and Information Security

II Semester, Paper III

MSFS223- Forensics of Embedded Systems

Aim and Objectives of Course: Understanding Embedded Systems and its forensic analysis using various Smart Devices and Gadgets Forensics.

Learning Outcomes

1. Different PCB Concepts.
2. Embedded System analysis.
3. Smart device Acquisition.
4. Smart Device internal memory acquisition and analysis.
5. Firmware Forensics Analysis.
6. Simulation of various Embedded devices.

Unit I- Embedded Systems fundamentals

Introduction to embedded systems: Classification, Characteristics and requirements, embedded device market growth, Gordon Moore's Law, PCB Concepts, PLC Fundamentals, Flash File Systems, Chip-off concepts. Memory Fundamentals of digital forensics.

Unit II- Forensic Analysis

Embedded System analysis, Physical Data Acquisition, Boot Loaders, disordering, Reverse Engineering, Disassembler tools IDA Pro & Practices, Sketching a Forensic Reverse Engineering Methodology

UNIT III- Smart Devices and Gadgets Forensics

Smart Phone device forensics, Smart device Acquisition, Smart Device internal memory acquisition and analysis, Firmware Forensics Analysis, Firmware tools, Gadgets forensics, Basics of SCADA Systems, Stuxnet Analysis Case study.

Unit IV- Simulation & Research

Simulink, Emulation of devices, Router Forensics, Data Card Dongles Firmware analysis, ICS (Industrial Control Systems) concepts, Raspberry Pi, ARM Instruction set & Fundamentals.

Reference Books:

1. Handbook of Digital Forensics and Investigation, By Eoghan Casey, Academic Press.
2. Forensic imaging of embedded systems using JTAG, Ing. M.F. Breeuwsma
3. Forensic analysis of an unknown embedded device, Jarle Eide & Jan Ove Skogheim Olsen
4. Embedded System Design: A Unified Hardware/Software Introduction, Frank Vahid and Tony Givargis, John Wiley & Sons.
5. The Internet of Things by Samuel Greengard
6. Designing the Internet of Things by Adrian McEwen and Hakim Cassimally
7. Internet of Things (A Hands-on-Approach) by Arshdeep Babga and Vijay Madisetti
8. Learning Internet of Things by Peter Waher
9. Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts by Nitesh Dhanjani
10. Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems
11. Development by David Kleidermacher and Mike Kleidermacher 11. Security in Embedded Devices (Embedded Systems) by Catherine H. Gebotys

M.Sc. Digital Forensics and Information Security

II Semester, Paper IV

MSFS224- Fundamentals of E-Discovery

Aim and Objectives of Course: Understanding E-Discovery and its data collection process using different tools and ESI.

Learning Outcomes

1. General framework of e-Discovery.
2. Legal aspects of e-Discovery.
3. Electronic Discovery Reference Model Project.
4. Discovery Tools and E-Discovery Issues.
5. Technical anatomy of e-mail messages e-mail systems.

Unit I- Basics of E-Discovery

History and development of e discovery, Overview of technology issues in e-discovery matters, including distinction between data and metadata, General framework of e-Discovery, Legal aspects of e-Discovery, e-Discovery industry, Electronic Discovery Reference Model Project, Developing "data maps" for enterprises, Technology tools for archiving and retrieving Electronically Stored Information.

Unit II- E-Discovery Data Collection

Data Preservation & Data Collection, Technology and data preservation-issues and means of preservation. Identifying the scope of data collection efforts - sources of data, Technical means of collecting ESI, including the use of forensic and non-forensic means and tools, Preservation of metadata and data during the collection process, International issues and privacy laws.

Unit III- Tools & ESI

Discovery Tools and E-Discovery Issues, Inspection of data collections, including inspection of computers and forensic imaging, Backup tape preservation and processing. Technological impediments to collection and data processing. The role of sampling in ESI production disputes, ESI Processing & Search, Reducing the volume of ESI through de-duplications, system file filtering, or other calling methodologies.

Technical Aspects:
The use of search in e-discovery, including different text search technologies and reaching agreements with opponents, "Keyword" search compared to "concept" search and other search technologies. Quality control measures and risk management for the use of search to filter electronic data, Review & Production of ESI, Producing metadata, Difference

between OCR and extracted text (and accompanying privilege risks), Handling foreign language documents.

Unit IV- E-Discovery investigation

Technical anatomy of e-mail messages e-mail systems, Enterprise class e-mail vs private email systems such as G-Mail, Web 2.0 Technologies, HotMail, Yahoo, etc. Collecting, processing, reviewing, and producing e-mail messages, E-discovery of instant messaging, Discovery of online information assets like Facebook, web sites, wikis and other web 2.0 technologies, Investigatory opportunities using computer forensics (recovering deleted files, retrieving internet activity, file fragment analysis, etc.)

Reference Books:

1. E-Discovery For Dummies by Linda Volonino, Ian Redpath, 2009.
2. Arkfeld on Electronic Discovery and Evidence, 3rd Ed. By Michael R. Arkfeld, Law Partner Publishing.
3. http://ediscoveryservicesinindia.blogspot.in/
4. Techno Security's Guide to E-Discovery and Digital Forensics: A Comprehensive Handbook by Jake Wiles, Syngress 1st edition, 2007.

II SEMESTER PRACTICALS

MSFS225 – Digital Forensics-1 & E-Discovery Lab

1. Acquisition of stand-alone machines, peripheral devices.
2. Retrieving data from different storage media and analyzing the files.
3. Acquisition or triage collection of live system, mobiles, PDA's, Tablets, Navigation systems etc.,
4. Acquisition over the network using remote acquisition tools.
5. Retrieve deleted data using various recovery tools and techniques.
6. Using technology tools, archive and retrieve Electronically Stored Information.
7. Technically collect ESI, including the use of forensic and non-forensic means and tools, and preserving the metadata and data during the collection process.
8. Inspection of data collections, including inspection of computers and forensic imaging, Backup tape preservation and processing.
9. Using search in e-discovery, including different text search technologies, and reaching agreements with opponents.
10. Collect, process, review, and produce e-mail messages using e-discovery tools.
11. Implement the E-discovery of instant messaging, Discovery of online information assets like Facebook, web sites, wikis, and other web 2.0 technologies.

MSFS226 – VAPT & Forensics of Embedded Systems Lab

1. Manual Testing of Vulnerability using W3uf and Nikto, Nessus, and other tools.
2. Perform the following command for Ping Sweeping: Fping, Nmap Ping Scan.
3. Perform OS Fingerprinting with Nmap Port Scanning, Version Detection with Nmap.
4. Perform Fingerprinting with Netcat, OpenSSL, Httprint.
5. Perform the following Exploiting commands: DELETE, PUT, etc.
6. Finding SOL Injections sources and implementing the attacks.
7. How to configure Burp Suite and perform the following operations
    - Spider
    - Intruder
    - Repeater
    - Sequencer
    - Decoder
    - Scanner
8. Implement the following using Metasploit: Cross Site Request Forgery, File Inclusion, File Upload, Insecure Captcha.
9. Implement and understand Embedded System analysis.
10. Perform the Physical Data Acquisition on different devices.
11. Perform Reverse Engineering using Disassembler tools like IDA Pro, etc.
12. Perform Firmware Forensics Analysis using Firmware tools.
13. Practicing the Stuxnet Analysis Case study.
14. Implement Router Forensics involving Data Card Dongles Firmware analysis.

M.Sc. Digital Forensics and Information Security

III Semester, Paper I

MSFS321- Digital Forensics Part-2

Aim and Objectives of Course: Understanding Live Memory Analysis, Windows, Linux, and Mac Forensics and Multimedia Forensics.

Learning Outcomes:

1. Setup of memory forensic environment.
2. Windows artifact analysis using Digital Forensic Tools.
3. CCTV Footage analysis.
4. Understanding of several virtualization platforms.

Unit I- Live Memory Analysis

Importance of live memory analysis in Digital Forensics, Acquisition of volatile memory using various tools, Setup of memory forensic environment, Extraction of various artifacts from memory dump, Analysis of memory dump, Using different tools like Volatility, LiME and others.

Unit II- Windows, Linux, and Mac Forensics

Windows artifact analysis using EnCase and Similar tools which includes MRU, link file, USB analysis, Prefetch analysis, shell bag, web cache etc., Analysis of UNIX based and other operating systems using EnCase, FTK, Autopsy and similar tools.

Unit III- Multimedia Forensics

Forensic analysis of Multimedia Files, CCTV Footage analysis, Introduction to Steganography, Different Steganalysis tools and techniques, Digital Watermarking. Identification of Device, confirming integrity, detecting origin of the multimedia, voice identification, image enhancement.

Unit IV- Forensics in virtual machines and Anti-Forensics

Introduction to Virtualization, understanding of several virtualization platforms, disk emulation techniques etc. In-depth analysis in virtual machines, Introduction to anti-forensics, tools and techniques used in anti-forensics.

Reference Books

1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons
2. Digital Forensics Workbook: Hands-on Activities in Digital Forensics by Michael Robinson
3. Computer Forensics and Cyber Crime: An Introduction by Marjie T. Britz
4. Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey
5. Forensic Computing by Anthony Sammes and Brian Jenkinson
6. Guide to Computer Forensics and Investigations, 6E by Bill Nelson/Amelia Phillips/Christopher Steuart
7. Handbook of Digital Forensics and Investigation by Eoghan Casey BS MA

8. Digital Forensics Explained by Greg Gogolin
9. Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows by Harlan Carvey
10. Linux Forensics by Philip Polstra
11. Computer Forensics and Digital Investigation with EnCase Forensic v7 by Suzanne Widup
12. EnCase Computer Forensics -- The Official EnCE: EnCase Certified Examiner Study Guide by Steve Bunting
13. Computer Forensics with FTK by Fernando Carbone
14. Digital Forensics with the AccessData Forensic Toolkit (FTK) by John Sammons
15. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management by Anton Chuvakin Ph.D. Stony Brook University Stony Brook NY., Kevin Schmidt, et al.
16. Handbook of Digital Forensics of Multimedia Data and Devices (IEEE Press) by Anthony T. S. Ho and Shujun Li
17. Digital Image Forensics: There is More to a Picture than Meets the Eye by Husrev Taha Sencar and Nasir Memon
18. Steganography in Digital Media: Principles, Algorithms, and Applications by Jessica Fridrich
19. Forensic Image Processing (ELECTRONICS) by Marcus Borengasser
20. Forensic Voice Identification by Harry Hollien

M.Sc. Digital Forensics and Information Security

III Semester, Paper II

MSFS322- Mobile Security and Forensics

Aim and Objectives of Course: Understanding Android and iOS Forensics and its Network Traffic Analysis.

Learning Outcomes

1. Setting up the development environment.
2. Reversing and Auditing Android Apps.
3. Traffic Analysis for Android Devices.
4. Understanding iOS Application Security.
5. Intercepting traffic of iOS Simulator.

Unit I- Introduction Android Security

Introduction to Android, Digging deeper into Android, Sandboxing and the permission model, Application signing, Android startup process, Setting up the development environment, Creating an Android virtual device, Useful utilities for Android Pentest, Android Debug Bridge, Burp Suite, APKTool, Reversing and Auditing Android Apps: Android application teardown, Reversing an Android application, Using APKTool to reverse an Android application, Auditing Android applications, Content provider leakage, Insecure file storage, Path traversal vulnerability or local file inclusion, Client-side injection attacks, OWASP top 10 vulnerabilities for mobiles.

Unit II- Traffic Analysis

Traffic Analysis for Android Devices, Android traffic interception. Ways to analyze Android traffic, Passive analysis, Active analysis, HTTPS Proxy interception, Other ways to intercept SSL traffic, Extracting sensitive files with packet capture. Basics of a penetration testing report, Writing the pentest report, Executive summary, Vulnerabilities, Scope of the work, Tools used, Testing methodologies followed, Recommendations.

Unit III- Android Forensics

Types of forensics, Filesystems, Android filesystem partitions, Using dd to extract data, Using a custom recovery image, Using Andriller to extract an application's data, Using AFLogical to extract contacts, calls, and text messages, Dumping application databases manually, Logging the logcat, Using backup to extract an application's data.

Unit IV- iOS Forensics

Introducing iOS Application Security, Basics of iOS and application development, Developing your first iOS app, Running apps on iDevice, iOS MVC design, iOS security model, iOS secure boot chain, iOS application signing, iOS application sandboxing, OWASP Top 10 Mobile Risks, Weak server-side controls, Insecure data storage; Insufficient transport layer protection, Side channel data leakage, Poor authorization and authentication, Broken cryptography, Client-side injection, Security decisions via untrusted input, Improper session handling. Lack of binary protections, Setting up Lab for iOS App Pentesting: Need for jailbreaking. What is jailbreak? Types of jailbreaks, Hardware, and software requirements, Jailbreaking iDevice, Adding sources to Cydia, Connecting and Transferring files to iDevice,

Connecting to Device using VNC, Installing utilities on Device, Installing idb tool. Installing apps on iDevice, Pentesting using iOS Simulator. Identifying the Flaws in Local Storage, Introduction to insecure data storage, Installing third party applications, Insecure data in the plist files, Insecure storage in the NSUserDefaults class. Insecure storage in SQLite database, SQL injection in iOS applications, Insecure storage in Core Data, Insecure storage in keychain, Traffic Analysis for iOS Application: Intercepting traffic over HTTP, Intercepting traffic over HTTPS, Intercepting traffic of iOS Simulator, Web API attack demo, Bypassing SSL pinning. Sealing up Side Channel Data Leakage: Data leakage via application screenshot, Pasteboard leaking sensitive information, Device logs leaking application sensitive data, Keyboard cache capturing sensitive data.

Introducing iOS Forensics, Basics of iOS forensics, The iPhone hardware, The iOS filesystem, Physical acquisition, Data backup acquisition, iOS forensics tools walkthrough, Elcomsoft iOS Forensic Toolkit (EIFT), Open source and free tools.

Reference Books

1. Learning Pentesting for Android Devices by Aditya Gupta
2. Learning iOS Penetration Testing Paperback by Swaroop Yermalkar

M.Sc. Digital Forensics and Information Security

III Semester, Paper III

MSFS323 - Cloud security and Forensics

Aim and Objectives of Course: Understanding OpenStack and its security challenges and Securing OpenStack Communications and Its API and Storage.

Learning Outcomes

1. Securing authorization points.
2. Evaluate the number of logs.
3. The OpenStack structures.
4. The Open Systems Interconnection model.
5. Configuring OpenStack Keystone to use Apache HTTPd.
6. Making Keystone available to HTTPd.
7. Configuring iptables, firewalld and SELinux.

Unit I- Introduction

Creating a Safe Environment, Access control, The CIA model, 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.

OpenStack Security Challenges

Private cloud versus public cloud security, The private cloud, The public cloud, Private cloud versus public cloud, The different kinds of security threats: Possible attackers, The possible attacks: Denial of Service, 0-day, Brute force, Advanced Persistent Threat, Automated exploitation tools, The ISP intercept, The supply chain attack, Social engineering, The Hypervisor breakout.

The OpenStack structure: OpenStack Compute Service - Nova, OpenStack Object Storage Service - Swift, OpenStack Image Service - Glance, OpenStack Dashboard-Horizon, OpenStack Identity Service – Keystone, OpenStack Networking Service - Neutron, OpenStack Block Storage Service - Cinder, OpenStack Orchestration - Heat, OpenStack Telemetry - Ceilometer, OpenStack Database Service - Trove, OpenStack Data Processing Service - Sahara, Future components: Ironic - bare metal provisioning, Zaqar- cloud messaging, Manila - file sharing, Designate - DNS, Barbican - Key management.

Unit II- Securing OpenStack Networking

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), Generic Routing Encapsulation (GRE), VXLAN, Flat network versus VLAN versus GRE in OpenStack Quantum, Design a secure network for your OpenStack deployment, The networking resource policy engine, Virtual Private Network as a Service (VPNaaS)

Unit III- Securing OpenStack Communications and Its API

Encryption security, Symmetric encryption, Stream cipher, Block cipher, Asymmetric encryption, Diffie-Hellman, RSA algorithm, Elliptic Curve Cryptography, Symmetric/asymmetric comparison and synergies, Hashing, MDS, SHA, Public key Infrastructure, Signed certificates versus self-signed certificates, Cipher security, Designing a redundant environment for your APIs, Secure your OpenStack API with TLS: Apache HTTPd, Nginx, Enforcing HTTPS for future connections. Securing the OpenStack 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, Configuring OpenStack Keystone to use Apache HTTPd: Apache HTTPd configuration, Making Keystone available to HTTPd, Configuring iptables, Configuring firewalld, SELinux, up shared tokens, Setting up the startup properly, Setting up Keystone as an Identity Provider. Configuring Apache HTTPd, Configuring Shibboleth: Configuring OpenStack Keystone.

Unit IV- Securing OpenStack Storage

Different storage types: Object storage, Block storage, File storage, Comparison between storage solutions, Security, Backends: Ceph, GlusterFS, The Logical Volume Manager, The Network File System, Sheepdog, Swift, Z File System (ZFS), Security, Securing OpenStack Swift, Hiding information, Securing ports, Securing the Hypervisor: Various types of virtualization, Full virtualization, Para virtualization, 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, sVirt - SELinux and virtualization, Hardening the host operative system.

Cloud Forensics

Cloud Forensic Frameworks, Digital Forensic Investigation and Cloud Computing, Dimensions of cloud forensics, cloud crime, challenger cloud forensics, usages of cloud forensics, Cloud forensics tools.

Reference Books

1. OpenStack Cloud Security Paperback by Alessandro Locati Fabio, PacktPub
2. Cloud Storage Forensics 1st Edition by Darren Quick, Ben Martini, Raymond Choo Syngress
3. Cybercrime and Cloud Forensics: Applications for Investigation Processes Keyun Ruan (University College Dublin, Ireland)

M.Sc. Digital Forensics and Information Security

III Semester, Paper IV

MSFS324- Malware Analysis

Aim and Objectives of Course: Understanding Malware Analysis and Covent Malware, and Reverse Engineering Techniques.

Learning Outcomes

1. Different Malware analysis techniques and their Behavior.
2. Static and Dynamic Analysis.
3. Analyzing Malicious Windows Programs.
4. Process Injection, Process Replacement, Hook Injections.

Unit I- Introduction to Malware Analysis and Covent Malware

Malware Definition and Types. Malware Analysis, Forensic Importance of Malware Analysis, Introduction to different analysis techniques, Malware Behavior, Setting up malware analysis laboratory.

Unit II- Static and Dynamic Analysis

Static Analysis: Hashing, Finding Strings, PE Files and Headers, Linked Libraries and Functions, Malware analysis in Virtual Machines. Dynamic Analysis: Sandboxes, Running and Monitoring a Malware, Process Monitor, Process Explorer, RegShot, Using Wireshark for Packet Analysis.

Unit III- Debugging and Reverse Engineering

Introduction to x86 Assembly, IDA Pro, Analyzing Malicious Windows Programs, Working with OllyDbg, Kernel Debugging with WinDBG, Live Memory Analysis using Volatility, Anti-Reverse Engineering: Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques.

Covert Malware: Process Injection, Process Replacement, Hook Injections, Data Encoding, Packers and Unpacking, Malware-Focused Network Signatures, Shell Code Analysis, 64-Bit Malware.

Unit IV- Android Malware Analysis

Android Architecture, Google Play Store, Android Permissions, Types of Android Malware, Behavior Analysis, Reverse Engineering, Working with Santoku.

Reference Books

1. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by

Michael Sikorski and Andrew Honig

2. Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code by Michael Ligh, Steven Adair, Blake Hartstein and Matthew Richard
3. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh,
4. Andrew Case, Jamie Levy and Aaron Walters
5. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation by Bruce Dang, Alexandre Gazet, Elias Bachaalany and Sébastien Josse
6. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle
7. Reversing: Secrets of Reverse Engineering by Eldad Eilam
8. Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham
9. Advanced Malware Analysis by Christopher Elisan
10. Christopher Elisan by Ken Dunham, Shane Hartman, Manu Quintans, Jose Andre Morales and Tim Strazzere
11. The Shellcoder's Handbook: Discovering and Exploiting Security Holes by Chris Anley, John Heasman, Felix Lindner and Gerardo Richarte
12. 12, Automatic Malware Analysis: An Emulator Based Approach by Heng Yin and Dawn Song
13. Botnets: The Killer Web App by Craig Schiller and Jim Binkley
14. Cuckoo Malware Analysis by Digit Oktavianto and Iqbal Muhardianto
15. Mastering Reverse Engineering by Ajay Kumar Tiwari
16. Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals by James C Foster

SEMESTER – III PRACTICALS

MSFS325 – Digital Forensics-2 & Mobile Security Lab

1. Acquisition of volatile memory using various tools like Volatility, etc.
2. Setup of memory forensic environment and extract various artifacts from memory dump and analyze the memory dump, Using different tools like Volatility, LiME, etc.
3. Windows artifact analysis using different forensic tools, which includes MRU, link file, USB analysis, Prefetch analysis, shell bag, web cache etc.,
4. Analysis of UNIX based and other operating systems using EnCase, FTK, Autopsy and similar tools.
5. Perform forensic analysis of Multimedia Files and CCTV Footage analysis.
6. Using APKTool to reverse an Android application, Auditing Android applications.
7. Perform the following on different Android Image files:
    - Using a custom recovery android image.
    - Using AFLogical to extract contacts, calls, and text messages.
    - Dumping application databases manually.
    - Logging the logcat and using backup to extract an application's data.
8. Developing your first iOS app and running apps on iDevice.
9. Pentest using iOS Simulator and identifying the Flaws in Local Storage,
10. Perform traffic analysis for iOS Applications by: Intercepting traffic over HTTP, HTTPS, iOS Simulator.
11. Perform physical acquisition of iOS devices physical and Data backup acquisition using Elcomsoft iOS Forensic Toolkit (EIFT), Open source and free tools.

MSFS326 – Malware Analysis & Cloud security Lab

1. Setting up malware analysis laboratory.
2. Perform the following static analysis operations:
    - Hashing.
    - Finding Strings.
    - PE Files and Headers.
    - Linked Libraries and Functions.
    - Malware analysis in Virtual Machines.
3. Run and Monitor a Malware, including Process Explorer, RegShot and Packet Analysis using Wireshark.
4. Analyze Malicious Windows Programs using OllyDbg and Kernel Debugging with WinDBG.
5. Perform Anti-Reverse Engineering techniques like: Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine techniques.
6. Design a secure network for your OpenStack deployment.
7. Designing a redundant environment for your APIs and securing your OpenStack API with TLS.
8. Configuring OpenStack Keystone to use Apache HTTPd: Setting up Keystone as an Identity Provider.
9. Configuring Apache HTTPd, Configuring Shibboleth: Configuring OpenStack Keystone.
10. Perform the following operations: Physical hardware PCI passthrough and Virtual hardware with Quick Emulator, SVirt – SELinux.

M.Sc. Forensic Science

IV Semester

MSFS421 – Comprehensive viva-voce

M.Sc. Forensic Science

IV Semester, Paper II

MSFS422 – PROJECT

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM

M.Sc. Forensic Science

I-SEMESTER END EXAMINATION

Theory Model Question Paper Pattern: Paper I

MSFS121- Cyber Laws and Intellectual Property Rights

Time: 3 hrs **Max. Marks: 75**

Section - A

Answer All The Following Questions **5X10=50M**

1. a. Define Cyber Law. Why do we need cyber laws?

(Or)

b. What Information Security? When do we need Information Security?

2. a. Explain concept of Jurisdiction and Cyber Jurisdiction.

(Or)

b. Write a note on IT ACT.

3. a. Explain E- Signature and E- Governance.

(Or)

b. Explain Websites Legal Liability under IT act.

4. a. Describe Taxation Issues in Cyber Space.

(Or)

b. Explain WIPO.

5. a. Write a note on Indian Legal System.

(Or)

b. Write in detail about blocking websites, telephone tapping, packet sniffing .

Section-B

Answer Any Five Of The Following Questions **5X5=25M**

a. Write in details about Amendments in IT Act till date.

b. Explain different cyber laws of EU,USA, Australia and Britain.

c. What are the various issues in Cyberspace. Explain various attacks along with the preventive measures.

d. Write a note on IT Act and its relation with IPC.

e. Explain relation of Income Tax Law with IT Act.

f. Explain Adjudication process for recovery of losses under IT Act.

g. Write a note on: a. Document Forgery b. Software Piracy

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM
M.Sc. Forensic Science
I-SEMESTER END EXAMINATION
Theory Model Question Paper Pattern: Paper I
MSFS122- Forensic Application Development and Networking Concepts

Time: 3 hrs **Max. Marks: 75**

Section-A

Answer all questions. Each question carries 15 marks. **4x15=60**

1. a. Discuss in detail about Python setup, debugging and various strings.

(OR)

b. What is OOP? Write in detail.

2. a. Give an introduction of Perl programming and data types.

(OR)

b. Explain the file handling process and introduction to Bash Scripting.

3. a. Explain Multi-switch Networks and their examples.

(OR)

b. what is TCP, ARP and UDP? Discuss in details.

4. a.Explain Firewalls in detail.

(OR)

b. What is Wireshark?

Section-B

Answer any FIVE of the following **5X3=15**

a. Write a note on: i) CID ii) NIA iii) RAW

b. Write duties of Forensic Scientist.

c. Explain about social change and crime relationships.

d. Write about Probation and Parole.

e. What are the powers of Lokayukta?

f. Write about IPC and Sec 171B, 291, and 299 with suitable examples

g. What is meant by the admissibility of expert testimony?

h. Explain examination- in chief, cross-examination, and re-examination.

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM

M.Sc. Forensic Science

I-SEMESTER END EXAMINATION

Theory Model Question Paper Pattern: Paper I

MSFS123- Modern Cryptography and Steganography

Time: 3 hrs **Max. Marks: 75**

Section-A

Answer all questions. Each question carries 15 marks. **4X15=60**

1. a. What is Cryptography? Discuss in detail.

(OR)

b. Explain Digital Signature in details.

2. a. Introduction about Cryptographic keys and Key Length.

(OR)

b. Explain Algorithm, their types, modes and uses.

3. a. Explain Quantum computing and its uses.

(OR)

b. Describe One-Way Hash functions.

4. a. What is Steganography? Discuss its type.

(OR)

b. Define cryptanalysis and steganalysis.

Section-B **5X3=15**

Answer any FIVE of the following

a. What is Public-Key Cryptography?

b. What is Basic and Intermediate protocols?

c. Explain the differences between Advanced and Esoteric protocols.

d. What is symmetric key?

e. Explain RSA and DSA.

f. Write a note on information theory and number theory.

g. Define history and need of Data Hiding technique.

h. Explain Network Steganography.

ADIKAVI NANNAYA UNIVERSITY: RAJAMAHENDRAVARAM

M.Sc. Forensic Science

I-SEMESTER END EXAMINATION

Theory Model Question Paper Pattern: Paper I

MSFS124- Network Security and Forensics

Time: 3 hrs **Max. Marks: 75**

Section-A

Answer all questions. Each question carries 15 marks. **4x15=60**

1. a. Explain Network Forensic investigation methodology.

(OR)

b. What are Network Based Digital Evidences? Explain.

2. a. Define various kind of network attacks.

(OR)

b. Explain Wireless Passive Evidence Acquisition.

3. a. What are web proxies and its functionality?

(OR)

b. Explain Simple Network Management Protocol.

4. a. What is Network Intrusion Detection and Analysis?

(OR)

b. Explain Higher- Layer Protocol Awareness.

Section-B **5X3=15**

Answer any FIVE of the following

a. Explain various challenges relating to network evidence.

b. What is Real evidences, Best Evidence, Direct evidence and circumstantial Evidence?

c. What is WAP? Explain.

d. Explain spectrum analysis?

e. What is syslog authentication?

f. Describe Squid Configuration and Squid Access Logfile.

g. Explain Comprehensive Packet Logging.

h. Explain Snort rule language.