Janardan Bhagat Shikshan Prasarak Sanstha's

CHANGU KANA THAKUR ARTS, COMMERCE & SCIENCE COLLEGE, NEW PANVEL (AUTONOMOUS)

Re-accredited 'A+' Grade by NAAC
'College with Potential for Excellence' Status Awarded by UGC
'Best College Award' by University of Mumbai

Program: M.Sc.

Revised Syllabus of M.Sc. Information Technology (Part –II)
Choice Based Credit System (60:40)
w.e.f. Academic Year 2022-2023

Sr. No.	Heading	Particulars
1	Title of Course	M.Sc. (Information Technology) Part II
2	Eligibility for Admission	A candidate for being eligible for admission to the M.Sc. I.T. Part-II, shall have passed M.Sc. I.T. Part-I and should have secured not less than 40%.
3	Passing marks	40%
4	Ordinances/Regulations (if any)	-
5	No. of Semesters	Two years – Four Semesters
6	Level	P.G.
7	Pattern	Semester, Choice Based
8	Status	Revised
9	To be implemented from Academic year	From the Academic Year **2022 – 2023**

Preamble:

The M.Sc. Information Technology programme is started with an aim to make the learners employable and impart industry oriented training.

The main objectives of the course are:

- To think analytically, creatively and critically in developing robust, extensible and highly maintainable technological solutions to simple and complex problems.
- To apply their knowledge and skills to be employed and excel in IT professional careers and/or to continue their education in IT and/or related post graduate programmes.
- To be capable of managing complex IT projects with consideration of the human, financial and environmental factors.
- To work effectively as a part of a team to achieve a common stated goal.
- To adhere to the highest standards of ethics, including relevant industry and organizational codes of conduct.
- To communicate effectively with a range of audiences both technical and non-technical.
- To develop an aptitude to engage in continuing professional development.

S. N.	OUTCOMES FOR M. SC. PROGRAM After completion of M.Sc. program students will acquire	Graduate Attribute
PO1	The ability to identify and describe broadly accepted methodologies of science, and different modes of reasoning. Disciplinary knowledge	Disciplinary knowledge
PO2	An ability to demonstrate proficiency in various instrumentation, modern tools, and advanced techniques to meet industrial expectations and research outputs	Disciplinary knowledge
PO3	Ability to identify problems, formulates, and prove hypotheses by applying theoretical knowledge and skills relevant to the discipline.	Problem-solving
PO4	The ability to articulate thoughts, research ideas, information, scientific outcomes in oral and in written presentation to range of audience.	Communication skills
PO5	A capacity for independent, conceptual, and creative thinking, and critical analysis through the existing methods of enquiry.	Critical thinking
PO6	Acquisition of skills required for cutting edge research, investigations, field study, documentation, networking, and ability to build logical arguments using scholarly evidence.	Research skills
PO7	An ability to portray good interpersonal skills with the ability to work collaboratively as part of a team undertaking a range of different team roles.	Teamwork
PO8	The ability to understand ethical responsibilities and impact of scientific solutions in global, societal, and environmental context and contribute to sustainable development.	Moral and ethical awareness/ multicultural competence
PO9	An openness to and interest in, life-long learning through directed and self-directed study.	self-directed learning
PO10	The ability to translate the knowledge and demonstrate the skills required to be employed and successful professional development.	Life-long learning

Program Specific outcomes

Name of the Programme: M.Sc.I.T.	
	After completing the programme in Information Technology, Student will be able to:
PSO1	Apply IT in the field of Data Science, AI, Networking, Security and Cloud Computing.
PSO2	Design solutions for complex IT problems.
PSO3	Develop research, investigation skills and achieve professional competency in the field of I.T.

Semester - III

[Under CBCS Scheme]

Course	**Course code**	**Hrs. / week**	**Internal assessment**	**Semester-end examination**	**Total**	**Credits**
Technical Writing and Entrepreneurship Development	PIT3TED	4	40	60	100	4
Security Breaches and Countermeasures	PIT3SBC	4	40	60	100	4
Malware Analysis	PIT3MWA	4	40	60	100	4
Robotic Process Automation	PIT3RPA	4	40	60	100	4
Project Documentation and Viva	PIT3PDP	4	40	60	100	2
Security Breaches and Countermeasures Practical	PIT3SBP	4	-	50	50	2
Malware Analysis Practical	PIT3MAP	4	--	50	50	2
Robotic Process Automation Practical	PIT3TED	4	--	50	50	2

Semester - IV
[Under CBCS Scheme]

Course	Course code	Hrs/ week	Internal assessment	Semester-end examination	Total	Credits
Blockchain	PIT4BLC	4	40	60	100	4
Digital Image Forensics	PIT4DIF	4	40	60	100	4
Security Operations Center	PIT4SOC	4	40	60	100	4
Human Computer Interaction	PIT4HCI	4	40	60	100	4
Blockchain Practical	PIT4BCP	4	40	60	100	2
Digital Image Forensics Practical	PIT4DFP	4	40	60	100	2
Security Operations Center Practical	PIT4SOP	4	--	50	50	2
Project Implementation and Viva	PIT4PIP	4	--	50	50	2

Examination Scheme

Choice Based Credit System (CBCS)

- **Revised Scheme of Examination**

The performance of the learners shall be evaluated into two components. The learner's Performance shall be assessed by Internal Assessment with 40% marks in the first component by conducting the Semester End Examinations with 60% marks in the second component. The allocation of marks for the Internal Assessment and Semester End Examinations are as shown below:-

A) Internal Assessment: 40 % 40 Marks

Sr. No.	Particular		Marks
01	One periodical class test examination to be conducted in the given semester		20 Marks
02	One case study/ project with presentation based on curriculum to be assessed by the teacher concerned		15 Marks
	Presentation	10 Marks	
	Written Document	05 Marks	
03	Active participation in routine class instructional deliveries and overall conduct as a responsible learner, mannerism and articulation and exhibit of leadership qualities in organizing related academic activities		05 Marks

- Maximum Marks: 20
- Duration: 40 Minutes

Particular	Marks
Match the Column / Fill in the Blanks / Multiple Choice Questions/ True/False/Answer in One or Two Lines (Concept based Questions) (1 Marks each)	20 Marks

Question Paper Pattern for Semester End Examination

(Periodical Class Test/ online examination for the Courses at Under Graduate Programmes)

- **Postgraduate Programmes for M.Sc. in Information Technology**
  - Duration: The examination shall be of 2.5 hours duration.

Question Paper Pattern

Theory question paper pattern
1. There shall be five questions each of 12 marks. 2. All questions shall be compulsory with internal options. 3. Question may be subdivided into sub-questions a, b, c… and the allocation of marks depends on the weightage of the unit.

Passing Standard

The learners to pass a course shall have to obtain a minimum of 40% marks in aggregate for each course where the course consists of Internal Assessment and Semester End Examination. The learners shall obtain minimum of 40% marks (i.e. 16 out of 40) in the Internal Assessment and 40% marks in Semester End Examination (i.e. 24 Out of 60) separately, to pass the course and minimum of Grade D, wherever applicable, to pass a particular semester. A learner will be said to have passed the course if the learner passes the Internal Assessment and Semester End Examination together.

Question Paper Pattern for Practical Examination

Sr. No.	Particular		Marks
01	Practical		50 Marks
	Practical Question	40 Marks	
	Journal	5 Marks	
	Viva	5 Marks	

Semester III

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Technical Writing and Entrepreneurship Development
Course Code	PIT3TED
Credit	4
Hours	4 Hrs per week

Course Objectives	• The objective of this course to provide conceptual understanding of developing strong foundation in general writing, including research proposal and reports. • It covers the technological developing skills for writing Article, Blog, E-Book, Commercial web Page design, Business Listing Press Release, E-Listing and Product Description. • This course aims to provide conceptual understanding of innovation and entrepreneurship development.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Develop technical documents that meet requirement with standard guidelines.
	2. Build effective blogs and social media pages.
	3. Explain effectiveness of innovation and entrepreneurship.
	4. Make use of graphic functions for writing different types of research proposals.

Module /Unit	**Course Description**	**Hrs**.
I	**Introduction to Technical Communication**: What Is Technical Communication? The Challenges of Producing Technical Communication, Characteristics of a Technical Document, Measures of Excellence in Technical Documents, Skills and Qualities Shared by Successful Workplace Communicators, How Communication Skills and Qualities Affect Your Career? **Understanding Ethical and Legal Considerations:** A Brief Introduction to Ethics, Your Ethical Obligations, Your Legal	**12**

	Obligations, The Role of Corporate Culture in Ethical and Legal Conduct, Understanding Ethical and Legal Issues Related to Social Media, Communicating Ethically Across Cultures, Principles for Ethical Communication **Writing Technical Documents:** Planning, Drafting, Revising, Editing, Proofreading **Writing Collaboratively:** Advantages and Disadvantages of Collaboration, Managing Projects, Conducting Meetings, Using Social Media and Other Electronic Tools in Collaboration, Importance of Word Press Website, Gender and Collaboration, Culture and Collaboration.	
II	**Introduction to Content Writing:** Types of Content (Article, Blog, E-Books, Press Release, Newsletters Etc), Exploring Content Publication Channels. Distribution of your content across various channels. **Blog Creation:** Understand the psychology behind your web traffic, Creating killing landing pages which attract users, Using Landing Page Creators, Setting up Accelerated Mobile Pages, Identifying UI UX Experience of your website or blog. **Organizing Your Information:** Understanding Three Principles for Organizing Technical Information, Understanding Conventional Organizational Patterns, **Emphasizing Important Information:** Writing Clear, Informative Titles, Writing Clear, Informative Headings, Writing Clear Informative Lists, Writing Clear Informative Paragraphs.	**12**
III	**Creating Graphics:** The Functions of Graphics, The Characteristics of an Effective Graphic, Understanding the Process of Creating Graphics, Using Color Effectively, Choosing the Appropriate Kind of Graphic, Creating Effective Graphics for Multicultural Readers. **Researching Your Subject:** Understanding the Differences Between Academic and Workplace Research, Understanding the Research Process, Conducting Secondary Research, Conducting Primary Research, **Research and Documentation:** Literature Reviews, Interviewing for Information, Documenting Sources, Copyright, Paraphrasing, Questionnaires. **Report Components:** Abstracts, Introductions, Tables of Contents, Executive Summaries, Feasibility Reports, Investigative Reports, Laboratory Reports, Test Reports, Trip Reports, Trouble Reports	**12**
IV	**Writing Proposals:** Understanding the Process of Writing Proposals, The Logistics of Proposals, The ―Deliverables‖ of Proposals, Persuasion and Proposals, Writing a Proposal, The Structure of the Proposal. **Writing Informational Reports:** Understanding the Process of Writing Informational Reports, Writing Directives, Writing Field Reports, Writing Progress and Status Reports, Writing Incident Reports, Writing Meeting Minutes. **Writing Recommendation Reports:** Understanding the Role of Recommendation Reports, Using a Problem-Solving Model for Preparing Recommendation Reports, Writing Recommendation Reports. **Reviewing, Evaluating, and Testing Documents and Websites:** Understanding Reviewing, Evaluating, and Testing, Reviewing	**12**

	Documents and Websites, Conducting Usability Evaluations, Conducting Usability Tests, Using Internet tools to check writing Quality, Duplicate Content Detector, What is Plagiarism?, How to avoid writing Plagiarism content? **Innovation management: an introduction:** The importance of innovation, Models of innovation, Innovation as a management process. **Market adoption and technology diffusion:** Time lag between innovation and useable product, Innovation and the market Innovation and market vision ,Analysing internet search data to help adoption and forecasting sales ,Innovative new products and consumption patterns, Crowd sourcing for new product ideas, Frugal innovation and ideas from everywhere, Innovation diffusion theories.	
V	**Managing innovation within firms:** Organisations and innovation, The dilemma of innovation management, Innovation dilemma in low technology sectors, Dynamic capabilities, Managing uncertainty, Managing innovation projects **Operations and process innovation:** Operations management, The nature of design and innovation in the context of operations, Process design, Process design and innovation **Managing intellectual property:** Intellectual property, Trade secrets, An introduction to patents, Trademarks, Brand names, Copyright **Management of research and development:** What is research and development?, R&D management and the industrial context, R&D investment and company success, Classifying R&D, R&D management and its link with business strategy, Strategic pressures on R&D, Which business to support and how?, Allocation of funds to R&D, Level of R&D expenditure **Managing R&D projects:** Successful technology management, The changing nature of R&D management, The acquisition of external technology, Effective R&D management, The link with the product innovation process, Evaluating R&D projects.	**12**

Reference Books:

1. Technical Communication Mike Markel Bedford/St. Martin's 11 2014.
2. Innovation Management and New Product Development Paul Trott Pearson 06 2017.
3. Handbook of Technical Writing Gerald J. Alred , Charles T. Brusaw , Walter E. OliuBedford/St. Martin's 09 2008.
4. Technical Writing 101: A Real-World Guide to Planning and Writing Technical ContentAlan S. Pringle and Sarah S. O'Keefe scriptorium 03 2009.
5. Innovation and Entrepreneurship Peter Drucker Harper Business 03 2009

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Project Documentation and viva
Course Code	PIT3PDP
Credit	2
Hours	4 Hrs per week

Course Objectives	• The objective of this course is to understand some problem and concern of software project manager, learners will able to cost estimation of project.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Apply relevant knowledge & abilities within the main field of study
	2. Analyze larger problems on the advanced level within the main field of study .
	3. Estimate system requirement.
	4. Design data flow diagram & phases in SDLC.

Module/ Unit	**Course Description**
	The learners are expected to develop a project beyond the undergraduate level. Normal websites, web applications, mobile apps are not expected. Preferably, the project should be from the elective chosen by the learner at the post graduate level. In semester three. The learner is supposed to prepare the synopsis and documentation. The same project has to be implemented in Semester IV. More details about the project is given is Appendix 1.

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Security Breaches and Countermeasures
Course Code	PIT3SBC
Credit	4
Hours	4 Hrs per week

Course Objectives	• To get the insight of the security loopholes in every aspect of computing. • To understand the threats and different types of attacks that can be launched on computing systems. • To know the countermeasures that can be taken to prevent attacks on computing systems. • To test the software against the attacks

Course Outcomes	**After completing the course, Student will be able to:**
	1. Classify different security breaches that can occur.
	2. Identify vulnerabilities in the systems, breach the security of the system, and threats due to malware.
	3. Develop social engineering and educate people to be Careful from attacks due to it.
	4. Evaluate vulnerabilities in the Web Servers, Applications and newer technologies like mobiles, IoT and computing

Module/ Unit	**Course Description**	**Hrs**
I	**Introduction to Security Breaching**: Overview of Information Security, Threats and Attack vectors, Concepts of Hacking – Ethical and Unethical, Information Security Controls, Concepts of penetration Testing, Information Security Laws and Standards. **Evaluation Security of IT Organisation:** Concepts, Methodology, Tools, Countermeasures, Penetration Testing. **Network Scanning:** Concepts, Scanning beyond IDS and firewalls, Tools, Banner Grabbing, Scanning Techniques, Network Diagrams, penetration testing.	**12**

	Enumeration: Concepts, Different types of enumeration: Netbios, SNMP, LDAP, NTP, SMTP, DNS, other enumeration techniques, Countermeasures, Penetration Testing	
II	**Analysis of Vulnerability:** Concepts, Assessment Solutions, Scoring Systems, Assessment Tools, Assessment Reports. **Breaching System Security:** Concepts, Cracking passwords, Escalating privileges, Executing Applications, Hiding files, covering tracks, penetration testing. **Threats due to malware:** Concepts, Malware Analysis, Trojan concepts, countermeasures, Virus and worm concepts, anti-malware software, penetration testing. **Network Sniffing:** Concepts, countermeasures, sniffing techniques, detection techniques, tools, penetration testing.	**12**
III	**Social Engineering:** Concepts, Impersonation on networking sites, Techniques, Identity theft, Insider threats, countermeasures, Pen testing. **Denial of Service and Distributed Denial of service:** Concepts, techniques, botnets, attack tools, countermeasures, protection tools, penetration testing. **Hijacking an active session:** Concepts, tools, application level session hijacking, countermeasures, network level session hijacking, penetration testing. **Evasion of IDS, Firewalls and Honeypots:** Introduction and concepts, detecting honeypots, evading IDS, IDS and Firewall evasion countermeasures, evading firewalls, penetration testing.	**12**
IV	**Compromising Web Servers:** Concepts, attacks, attack methodology, attack tools, countermeasures, patch management, web server security tools, penetration testing. **Compromising Web Applications:** Concepts**,** threats, methods, tools, countermeasures, testing tools, penetration testing. **Performing SQL Injection:** Concepts, types, methodology, tools, techniques, countermeasures. **Compromising Wireless Networks:** Concepts, wireless encryption, threats, methodology, tools, compromising Bluetooth, countermeasures, wireless security tools, penetration testing.	**12**
V	**Compromising Mobile Platforms:** Attack vectors, Compromising Android OS, Compromising iOS, Mobile spyware, Mobile Device Management, Mobilesecurity, penetration testing. **Compromising IoT:** Concepts, attacks,compromising methodology, tools,countermeasures,penetration testing. **Cloud Security:** Concepts, Security, threats, attacks,tools, penetration testing. **Cryptography:** Concepts, email encryption,algorithms, disk encryption, tools, cryptanalysis,Public key infrastructure, countermeasures.	**12**

Reference Books:

1. CEHv10, Certified Ethical Hacker Study Guide Ric Messier Sybex - Wiley - 2019
2. All in One, Certified Ethical Hacker Matt Walker Tata McGraw Hill - 2012
3. CEH V10: EC-Council Certified Ethical Hacker Complete Training Guide I.P. Specialist IPSPECIALIST – 2018

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Security Breaches and Countermeasures Practical
Course Code	PIT3SBP
Credit	2
Hours	4 Hrs per week

Course Objectives	• To make the learners capable using of various network information gathering tools. • To make the learners capable of using various network security tools

Course Outcomes	**After completing the course, Student will be able to:**
	1. Make use of tools to perform footprinting and reconnaissance
	2. Determine use of Enumeration and network scanning tools.
	3. Test social engineering toolkits and web application scanning.
	4. Apply different tools for cryptography.

Module/ Unit	**Course Description**	**Hrs**
1	a. Use the following tools to perform footprinting and reconnaissance i. Recon-ng (Using Kali Linux) ii. FOCA Tool iii. Windows Command Line Utilities • Ping • Tracert using Ping • Tracert • NSLookup iv. Website Copier Tool – HTTrack v. Metasploit (for information gathering) vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile vii. Smart Whois viii. eMailTracker Pro ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network	**2Hrs.**

	Discovery Tool, Port Droid Tool b. Scan the network using the following tools: i. Hping2 / Hping3 ii. Advanced IP Scanner iii. Angry IP Scanner iv. Masscan v. NEET vi. CurrPorts vii. Colasoft Packet Builder viii. The Dude	
2	c. Use Proxy Workbench to see the data passing through it and save the data to file. d. Perform Network Discovery using the following tools: i. Solar Wind Network Topology Mapper ii. OpManager iii. Network View iv. LANState Pro e. Use the following censorship circumvention tools: i. Alkasir ii. Tails OS f. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool	**2Hrs**
3	a. Perform Enumeration using the following tools: i. Nmap ii. NetBIOS Enumeration Tool iii. SuperScan Software iv. Hyena v. SoftPerfect Network Scanner Tool vi. OpUtils vii. SolarWinds Engineer's Toolset viii. Wireshark b. Perform the vulnerability analysis using the following tools: i. Nessus ii. OpenVas	**2Hrs**
4	a. Perform mobile network scanning using NESSUS. b. Perform the System Hacking using the following tools: i. Winrtgen ii. PWDump iii. Ophcrack iv. Flexispy v. NTFS Stream Manipulation vi. ADS Spy vii. Snow viii. Quickstego ix. Clearing Audit Policies x. Clearing Logs	**2Hrs**
5	a. Use wireshark to sniff the network. b. Use SMAC for MAC Spoofing. c. Use Caspa Network Analyser. d. Use Omnipeek Network Analyzer	**2Hrs**

6	a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux. b. Perform the DDOS attack using the following tools: i. HOIC ii. LOIC iii. HULK iv. Metasploit c. Using Burp Suite to inspect and modify traffic between the browser and target application.	**2Hrs**
7	a. Perform Web App Scanning using OWASP Zed Proxy. b. Use droidsheep on mobile for session hijacking c. Demonstrate the use of the following firewalls: i. Zonealarm and analyse using Firewall Analyzer. ii. Comodo Firewall d. Use HoneyBOT to capture malicious network traffic. e. Use the following tools to protect attacks on the web servers: i. ID Server ii. Microsoft Baseline Security Analyzer iii. Syhunt Hybrid	**2Hrs**
8	a. Protect the Web Application using dotDefender. b. Demonstrate the following tools to perform SQL Injection: i. Tyrant SQL ii. Havij iii. BBQSQL	**2Hrs**
9	Use Aircrack-ng suite for wireless hacking and countermeasures.	**2Hrs**
10	Use the following tools for cryptography i. HashCalc **ii.** Advanced Encryption Package **iii.** MD5 Calculator **iv.** TrueCrypt **v.** CrypTool	**2Hrs**

Reference Books:

1. CEHv10, Certified Ethical Hacker Study Guide Ric Messier Sybex - Wiley - 2019
2. All in One, Certified Ethical Hacker Matt Walker Tata McGraw Hill - 2012
3. CEH V10: EC-Council Certified Ethical Hacker Complete Training Guide I.P. Specialist IPSPECIALIST – 2018

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Malware Analysis
Course Code	PIT3MWA
Credit	4
Hours	4 Hrs per week

Course Objectives	• Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques. • Have an intimate understanding of executable formats, Windows internals and API, and analysis techniques. • Extract investigative leads from host and network-based indicators associated with a malicious program. • Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples. • Achieve proficiency with industry standard tools including IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon etc.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Define Malware Analysis , Basic Static & Dynamic Analysis Techniques
	2. Explain IDA Pro, C code construct in assemble & Advance Dynamic Analysis
	3. Classify OLLYDBG , WINDBG & Malware Functionality
	4. Elaborate Data encoding , Anti disassembly, debugging , Virtual Machine techniques, Shellcode Analysis

Module/ Unit	Course Description	Hrs
I	**Malware Analysis:** Introduction, Techniques, Types of malware, General rules for Malware Analysis. **Basic Static Techniques:** Antivirus Scanning, Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executable Malware, Portable executable File Format, Linked Libraries and Functions, Static Analysis, The PE file headers and sections. **Malware Analysis in Virtual Machines:** Structure of VM, Creating and using Malware Analysis machine, Risks of using VMware for malware analysis, Record/Replay. **Basic Dynamic Analysis:** Sandboxes, Running Malware, Monitoring with process monitor, Viewing processes with process explorer, Comparing registry snapshots with regshot, Faking a network, Packet sniffing with Wireshark, Using INetSim, Basic Dynamic Tools. x86 Disassembly	**12**
II	**IDA PRO:** Loading an executable, IDA Pro Interface, Using cross references, Analysing functions, Using graphing options, Enhancing disassembly, Extending IDA with plug-ins. **Recognising C Code constructs in assembly:** Globalv/s local variables, Disassembling arithmetic operations, recognizing if statements, recognizing loops, function call conventions, Analysing switch statements, Disassembling arrays, Identifying structs, Analysing linked list traversal. **Analysing Malicious Windows Programs:** The windows API, The Windows Registry, Networking APIs, and Understanding running malware. Kernel v/s user mode, Native API. **Advanced Dynamic Analysis – Debugging:** Sourcelevel v/s Assembly-level debugging, kernel v/s user mode debugging, Using a debugger, Exceptions, Modifying execution with a debugger, modifying program execution.	**12**
III	**Advanced Dynamic Analysis – OLLYDBG:** Loading Malware, The Ollydbg Interface, Memory Map, Viewing threads and Stacks, Executing code, Breakpoints, Loading DLLs, Tracing, Exception handling, Patching, Analysing shell code, Assistance features, Plug-ins, Scriptable debugging. **Kernel Debugging with WINDBG:** Drivers and kernel code, Using WinDbg, Microsoft Symbols, kernel debugging and using it, Rootkits, Loading drivers, kernel issues with windows. **Malware Functionality – Malware Behavior:** Downloaders and launchers, Backdoors, Credential stealers, Persistence mechanisms, Privilege escalation, covering the tracks. **Covert Malware Launching:** Launchers, Process injection, Process replacement, Hook injection, detours, APC injection.	**12**

IV	**Data Encoding:** Goal of Analysing algorithms, Simple ciphers, Common cryptographic algorithms, Custom encoding, decoding. **Malware – focused network signatures:** Network countermeasures**,** Safely investigating attacker online, Content-Based Network Countermeasures, Combining Dynamic and Static Analysis Techniques, Understanding the Attacker's Perspective**.** **Anti-disassembly:** Concepts, Defeating disassembly algorithms, anti-disassembly techniques, Obscuring flow control, Thwarting stack-frame analysis. **Anti-debugging:** Windows debugger detection, debugger behavior, Interfering with debugger functionality, Debugger vulnerabilities.	**12**
V	**Anti-virtual machine techniques:** VMWare artifacts, Vulnerable functions, Tweaking settings, Escaping the virtual machine. **Packers and unpacking:** Packer anatomy, Identifying Packed Programs, Unpacking options, Automated Unpacking, Manual Unpacking, Common packers, Analysing without unpacking, Packed DLLs, **Shellcode Analysis:** Loading shellcode for analysis, Position-independent Code, Identifying Execution Location, Manual Symbol Resolution, Shellcode encoding, NOP Sleds, Finding Shellcode. **C++ Analysis:** OOP, Virtual and Non-virtual functions, Creating and destroying objects. **64-bit Malware:** Why 64-bit malware? Differences in x64 architecture, Windows 32-bit on Windows 64-bit, 64-bit hints at malware functionality.	**12**

Reference Books:

1. Practical Malware Analysis – The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig No Scratch Press - 2013
2. Mastering Malware Analysis Alexey Kleymenov, Amr ThabetPackt Publishing - 2019
3. Windows Malware Analysis Essentials Victor MarakPackt Publishing 2015

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Malware Analysis Practical
Course Code	PIT3MAP
Credit	2
Hours	4 Hrs per week

Course Objectives	• To enable the learners to create basic software automation using UIPath Studio. • To make the learners capable of building applications for automating the operations on excel file

Course Outcomes	**After completing the course, Student will be able to:**
	1. Identify the Malware Using Basic & Static Techniques.
	2. Examine the Malware using IDA Pro.
	3. Find Malware effect on .exe & .dll file using OLLYDBG.
	4. Test the Malware Using Advanced Dynamic Technique.

Module/ Unit	Course Description	Hrs
1	a. Files: Lab01-01.exe and Lab01-01.dll. b. Analyze the file Lab01-02.exe. c. Analyze the file Lab01-03.exe. d. Analyze the file Lab01-04.exe. e. Analyze the malware found in the file Lab03-01.exe using basic dynamic analysis tools. f. Analyze the malware found in the file Lab03-02.dll using basic dynamic analysis tools. g. Execute the malware found in the file Lab03-03.exe while monitoring it using basic dynamic analysis tools in a safe environment h. Analyze the malware found in the file Lab03-04.exe using basic dynamic analysis tools.	2Hrs
2	a. Analyze the malware found in the file Lab05-01.dll using only IDA Pro. The goal of this lab is to give you hands-on experience with IDA Pro. If you've already worked with IDA Pro, you may choose to ignore these questions and focus on reverseengineering the malware b. analyze the malware found in the file Lab06-01.exe. c. Analyze the malware found in the file Lab06-02.exe. d. analyze the malware found in the file Lab06-03.exe. e. analyze the malware found in the file Lab06-04.exe	2Hrs
3	a. Analyze the malware found in the file Lab07-01.exe b. Analyze the malware found in the file Lab07-02.exe. c. For this lab, we obtained the malicious executable, Lab07-03.exe, and DLL, Lab07- 03.dll, prior to executing. This is important to note because the mal- ware might change once it runs. Both files were found in the same directory on the victim machine. If you run the program, you should ensure that both files are in the same directory on the analysis machine. A visible IP string beginning with 127 (a loopback address) connects to the local machine. (In the real version of this malware, this address connects to a remote machine, but we've set it to connect to localhost to protect you.) d. Analyze the malware found in the file Lab09-01.exe using OllyDbg and IDA Pro to answer the following questions. This malware was initially analyzed in the Chapter 3 labs using basic static and dynamic analysis techniques. e. Analyze the malware found in the file Lab09-02.exe using OllyDbg f. Analyze the malware found in the file Lab09-03.exe using OllyDbg and IDA Pro. This malware loads three included DLLs (DLL1.dll, DLL2.dll, and DLL3.dll) that are all built to request the same memory load location. Therefore, when viewing these DLLs in OllyDbg versus IDA Pro, code may appear at different memory locations. The purpose of this lab is to make you comfortable with finding the correct location of code within IDA Pro when you are looking at code in OllyDbg	2Hrs
4	a. This lab includes both a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\ System32 directory where it was origi- nally found on the victim computer. The executable is Lab10-01.exe, and the driver is Lab10-01.sys.	2Hrs

	b. The file for this lab is Lab10-02.exe c. This lab includes a driver and an executable. You can run the executable from anywhere, but in order for the program to work properly, the driver must be placed in the C:\Windows\System32 directory where it was originally found on the victim computer. The executable is Lab10-03.exe, and the driver is Lab10-03.sys	
5	a. Analyze the malware found in Lab11-01.exe b. Analyze the malware found in Lab11-02.dll. Assume that a suspicious file named Lab11-02.ini was also found with this malware c. Analyze the malware found in Lab11-03.exe and Lab11-03.dll. Make sure that both files are in the same directory during analysis	2Hrs
6	a. Analyze the malware found in the file Lab12-01.exe and Lab12-01.dll. Make sure that these files are in the same directory when performing the analysis. b. Analyze the malware found in the file Lab12-02.exe. c. Analyze the malware extracted during the analysis of Lab 12-2, or use the file Lab12-03.exe d. Analyze the malware found in the file Lab12-04.exe.	2Hrs
7	a. Analyze the malware found in the file Lab13-01.exe. b. Analyze the malware found in the file Lab13-02.exe. c. Analyze the malware found in the file Lab13-03.exe	2Hrs
8	a. Analyze the malware found in file Lab14-01.exe. This program is not harmful to your system. b. Analyze the malware found in file Lab14-02.exe. This malware has been configured to beacon to a hard-coded loopback address in order to prevent it from harming your system, but imagine that it is a hard-coded external address. c. This lab builds on Practical 8 a. Imagine that this malware is an attempt by the attacker to improve his techniques. Analyze the malware found in file Lab14-03.exe. d. Analyze the sample found in the file Lab15-01.exe. This is a command-line program that takes an argument and prints “Good Job!” if the argument matches a secret code. e. Analyze the malware found in the file Lab15-02.exe. Correct all anti-disassembly countermeasures before analyzing the binary in order to answer the questions. f. Analyze the malware found in the file Lab15-03.exe. At first glance, this binary appears to be a legitimate tool, but it actually contains more functionality than advertised	2Hrs
9	a. Analyze the malware found in Lab16-01.exe using a debugger. Thisisthe same malware as Lab09-01.exe, with added anti-debugging techniques b. Analyze themalware found in Lab16-02.exe using a debugger. The goal ofthis lab is to figure out the correct password. The malware does not drop a malicious payload. c. Analyze the malware in Lab16-03.exe using a debugger. This malware is similar to Lab09-02.exe, with certain modifications,	2Hrs

	including the introduction of antidebugging techniques. d. Analyze the malware found in Lab17-01.exe inside VMware. This is the same malware as Lab07-01.exe, with added anti-VMware techniques. e. Analyze the malware found in the file Lab17-02.dll inside VMware. After answering the first question in this lab, try to run the installation exports using rundll32.exe and monitor them with a tool like procmon. The following is an example command line for executing theDLL: rundll32.exe Lab17-02.dll,InstallRT (or InstallSA/InstallSB) f. Analyze the malware Lab17-03.exe inside VMware	
10	a. Analyze the file Lab19-01.bin using shellcode_launcher.exe b. The file Lab19-02.exe contains a piece of shellcode that will be injected into another process and run. Analyze thisfile c. Analyze the file Lab19-03.pdf. If you get stuck and can't find the shellcode, just skip that part of the lab and analyze file Lab19-03_sc.bin using shellcode_launcher.exe. d. The purpose of this first lab is to demonstrate the usage of the thispointer. Analyze the malware in Lab20-01.exe. e. Analyze the malware In Lab20-02.exe. f. Analyze the malware in Lab20-03.exe. g. Analyze the code in Lab21-01.exe. h. Analyze the malware found in Lab21-02.exe on both x86 and x64 virtual machines.	2Hrs

Reference Books:

1. Practical Malware Analysis – The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig No Scratch Press - 2013
2. Mastering Malware Analysis Alexey Kleymenov, Amr ThabetPackt Publishing - 2019
3. Windows Malware Analysis Essentials Victor MarakPackt Publishing 2015

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Robotic Process Automation
Course Code	PIT3RPA
Credit	4
Hours	4 Hrs per week

Course Objectives	• To make the students aware about the automation today in the industry. • To make the students aware about the tools used for automation. • To help the students automate a complete process

Course Outcomes	**After completing the course, Student will be able to:**
	1. Define the scope and techniques of robotic process automation using UIPath Studio.
	2. Explain the concept of sequence, flowchart and control flow used to manipulate data.
	3. Make use of Exception Handling, Debugging and logging to handle user events and Assistant bots.
	4. Elaborate the deployment and maintenance of bot along with maintaining the code.

Module/ Unit	**Course Description**	**Hrs**
I	**Robotic Process Automation:** Scope and techniques of automation, About UiPath **Record and Play:** UiPath stack, Downloading and installing UiPath Studio, Learning UiPath Studio, Task recorder, Step-by-step examples using the recorder.	**12**
II	**Sequence, Flowchart, and Control Flow:** Sequencing the workflow, Activities, Control flow, various types of loops, and decision making, Step-by-step example using Sequence and Flowchart, Step-by-step example using Sequence and Control flow **Data Manipulation:** Variables and scope, Collections, Arguments – Purpose and use, Data table usage with examples, Clipboard management, File operation with step-by-step example, CSV/Excel to data table and vice versa (with a step-by-step example)	**12**

III	**Taking Control of the Controls :** Finding and attaching windows, Finding the control, Techniques for waiting for a control, Act on controls – mouse and keyboard activities, Working with UiExplorer, Handling events, Revisit recorder, Screen Scraping, When to use OCR, Types of OCR available, How to use OCR, Avoiding typical failure points **Tame that Application with Plugins and Extensions:** Terminal plugin, SAP automation, Java plugin, Citrix automation, Mail plugin, PDF plugin, Web integration, Excel and Word plugins, Credential management, Extensions – Java, Chrome, Firefox, and Silverlight	**12**
IV	**Handling User Events and Assistant Bots:** What are assistant bots?, Monitoring system event triggers, Hotkey trigger, Mouse trigger, System trigger ,Monitoring image and element triggers, An example of monitoring email, Example of monitoring a copying event and blocking it, Launching an assistant bot on a keyboard event **Exception Handling, Debugging, and Logging:** Exception handling, Common exceptions and ways to handle them, Logging and taking screenshots, Debugging techniques, Collecting crash dumps, Error reporting	**12**
V	**Managing and Maintaining the Code:** Project organization, Nesting workflows, Reusability of workflows, Commenting techniques, State Machine, When to use Flowcharts, State Machines, or Sequences, Using config files and examples of a configfile, Integrating a TFS server **Deploying and Maintaining the Bot:** Publishing using bpublish utility, Overview of Orchestration Server, Using Orchestration Server to control bots, Using Orchestration Server to deploy bots, License management, Publishing and managing updates	**12**

Reference Books:

1. Learning Robotic Process Automation Alok Mani TripathiPackt 1st 2018
2. Robotic Process Automation Tools, Process Automation and their benefits: Understanding RPA and Intelligent Automation Srikanth Merianda Createspace Independent Publishing 1st 2018
3. The Simple Implementation Guide to Robotic Process Automation (Rpa): How to Best Implement Rpa in an Organization Kelly Wibbenmeyeri Universe 1st 2018

Course Description: M.Sc. (Information Technology)	
Semester	III
Course Name	Robotic Process Automation Practical
Course Code	PIT3RAP
Credit	2
Hours	4 Hrs per week

Course Objectives	• To make the students aware about the automation today in the industry. • To make the students aware about the tools used for automation. • To help the students automate a complete process

Course Outcomes	**After completing the course, Student will be able to:**
	1. Create simple sequence and flowchart based projects in UIPath Studio.
	2. Develop Automation of any process using basic and Desktop recording.
	3. Build applications for automating the operations on excel file.
	4. Demonstrate the UIPath automation of activities such as MouseClick, Hotkey Trigger.

Module/ Unit	**Course Description**	**Hrs**
1	a. Create a simple sequence based project. b. Create a flowchart-based project. c. Create an UiPath Robot which can empty a folder in Gmail solely on basis of recording.	2Hrs
2	a. Automate UiPath Number Calculation (Subtraction, Multiplication, Division of numbers). b. Create an automation UiPath project using different types of variables (number, datetime, Boolean, generic, array, data table)	2Hrs
3	a. Create an automation UiPath Project using decision statements. b. Create an automation UiPath Project using looping statements.	2Hrs
4	a. Automate any process using basic recording. b. Automate any process using desktop recording. c. Automate any process using web recording.	2Hrs
5	a. Consider an array of names. We have to find out how many of	2Hrs

	them start with the letter "a". Create an automation where the number of names starting with "a" is counted and the result is displayed.	
6	a. Create an application automating the read, write and append operation on excel file. b. Automate the process to extract data from an excel file into a data table and vice versa	2Hrs
7	a. Implement the attach window activity. b. Find different controls using UiPath. c. Demonstrate the following activities in UiPath: i. Mouse (click, double click and hover) ii. Type into iii. Type Secure text	2Hrs
8	a. Demonstrate the following events in UiPath: i. Element triggering event ii. Image triggering event iii. System Triggering Event b. Automate the following screen scraping methods using UiPath i. Full Test ii. Native iii. OCR c. Install and automate any process using UiPath with the following plug-ins: i. Java Plugin ii. Mail Plugin iii. PDF Plugin iv. Web Integration v. Excel Plugin vi. Word Plugin vii. Credential Management	2Hrs
9	a. Automate the process of send mail event (on any email). b. Automate the process of launching an assistant bot on a keyboard event. c. Demonstrate the Exception handing in UiPath. d. Demonstrate the use of config files in UiPath	2Hrs
10	a. Automate the process of logging and taking screenshots in UiPath. b. Automate any process using State Machine in UiPath. c. Demonstrate the use of publish utility. d. Create and provision Robot using Orchestrator.	2Hrs

Reference Books:

1. Learning Robotic Process Automation Alok Mani TripathiPackt 1st 2018
2. Robotic Process Automation Tools, Process Automation and their benefits: Understanding RPA and Intelligent Automation Srikanth Merianda Createspace Independent Publishing 1st 2018
3. The Simple Implementation Guide to Robotic Process Automation (Rpa): How to Best Implement Rpa in an Organization Kelly Wibbenmeyeri Universe 1st 2018

Semester IV

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Blockchain
Course Code	PIT4BLC
Credit	4
Hours	4 Hrs per week

Course Objectives	• To provide conceptual understanding of the function of Blockchain as a method of securing distributed ledgers, how consensus on their contents is achieved, and the new applications that they enable.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Define the structure of blockchain system such as bitcoin and ethereum.
	2. Elaborate the use of different components in Solidity Programming.
	3. Explain concepts of Hyperledger, Smart Contracts & tokens, Mining Ether and cryptoeconomics.
	4. Elaborate the development of blockchain, EthereumD, Dapp applications.

Module/ Unit	**Course Description**	**Hrs**
I	**Blockchain:** Introduction, History, Centralised versus Decentralised systems, Layers of blockchain, Importance of blockchain, Blockchain uses and use cases. **Working of Blockchain:** Blockchain foundation, Cryptography, Game Theory, Computer Science Engineering, Properties of blockchain solutions, blockchain transactions, distributed consensus mechanisms, Blockchain mechanisms, Scaling blockchain **Working of Bitcoin:** Money, Bitcoin, Bitcoin blockchain, bitcoin network, bitcoin scripts, Full Nodes and SVPs, Bitcoin wallets.	12

II	**Ethereum:** three parts of blockchain, Ether as currency and commodity, Building trustless systems, Smart contracts, Ethereum Virtual Machine, The Mist browser, Wallets as a Computing Metaphor, The Bank Teller Metaphor, Breaking with Banking History, How Encryption Leads to Trust, System Requirements, Using Parity with Geth, Anonymity in Cryptocurrency, Central Bank Network, Virtual Machines, EVM Applications, State Machines, Guts of the EVM, Blocks, Mining's Place in the State Transition Function, Renting Time on the EVM, Gas, Working with Gas, Accounts, Transactions, and Messages, Transactions and Messages, Estimating Gas Fees for Operations, Opcodes in the EVM. **Solidity Programming:** Introduction, Global Banking Made Real, Complementary Currency, Programming the EVM, Design Rationale, Importance of Formal Proofs, Automated Proofs, Testing, Formatting Solidity Files, Reading Code, Statements and Expressions in Solidity, Value Types, Global Special Variables, Units, and Functions,	12
III	**Hyperledger:** Overview, Fabric, composer, installing hyperledger fabric and composer, deploying, running the network, error troubleshooting. **Smart Contracts and Tokens:** EVM as Back End, Assets Backed by Anything, Cryptocurrency Is a Measure of Time, Function of Collectibles in Human Systems, Platforms for High-Value Digital Collectibles, Tokens as Category of Smart Contract, Creating a Token, Deploying the Contract, Playing with Contracts.	12
IV	**Mining Ether:** Why? Ether's Source, Defining Mining, Difficulty, Self-Regulation, and the Race for Profit, How Proof of Work Helps Regulate Block Time, DAG and Nonce, Faster Blocks, Stale Blocks, Difficulties, Ancestry of Blocks and Transactions, Ethereum and Bitcoin, Forking, Mining, Geth on Windows, Executing Commands in the EVM via the Geth Console, Launching Geth with Flags, Mining on the Testnet, GPU Mining Rigs, Mining on a Pool with Multiple GPUs. **Cryptoecnomics:** Introduction, Usefulness of cryptoeconomics, Speed of blocks, Ether Issuance scheme, Common Attack Scenarios.	12
V	**Blockchain Application Development:** Decentralized Applications, Blockchain Application Development, Interacting with the Bitcoin Blockchain, Interacting Programmatically with Ethereum—Sending Transactions, Creating a Smart Contract, Executing Smart Contract Functions, Public vs. Private Blockchains, Decentralized Application Architecture, **Building an EthereumDApp:** The DApp, Setting Up a Private Ethereum Network, Creating the Smart Contract, Deploying the Smart Contract, Client Application, **DApp deployment:** Seven Ways to Think About Smart Contracts, Dapp Contract Data Models, EVM back-end and front-end communication, JSONRPC, Web 3, JavaScript API, Using Meteor with the EVM, Executing Contracts in the Console, Recommendations for Prototyping, Third-Party Deployment Libraries, **Creating Private Chains.**	12

Reference Books:

1. Beginning BlockchainA Beginner's Guide to Building Blockchain Solutions Bikramaditya Singhal, GautamDhameja, PriyansuSekhar Panda Apress 2018
2. Introducing Ethereum and Solidity Chris DannenApress 2017
3. The Blockchain Developer EladElromApress 2019
4. Mastering Ethereum Andreas M. Antonopoulos Dr. Gavin Wood O'Reilly First 2018
5. Blockchain Enabled Applications Vikram Dhillon David Metcalf Max Hooper Apress 2017

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Blockchain Practical
Course Code	PIT4BCP
Credit	2
Hours	4 Hrs per week

Course Objectives	• Blockchain is an emerging technology platform for developing decentralized applications and data storage, over and beyond its role as the technology underlying the cryptocurrencies. • The basic tenet of this platform is that it allows to create a distributed and replicated ledger of events, transactions, and data generated through various IT processes with strong cryptographic guarantees of tamper resistance, immutability, and verifiability

Course Outcomes	**After completing the course, Student will be able to:**
	1. Design programs for blockchain in Python.
	2. Create blockchain and exhibit its use.
	3. Build Apps with angular.
	4. Develop different functions in Solidity Programming.

Module/ Unit	**Course Description**	**Hrs**
1	Write the following programs for Blockchain in Python: a. A simple client class that generates the private and public keys by using the builtin Python RSA algorithm and test it. b. A transaction class to send and receive money and test it. c. Create multiple transactions and display them. d. Create a blockchain, a genesis block and execute it. e. Create a mining function and test it. f. Add blocks to the miner and dump the blockchain.	2Hrs
2	Install and configure Go Ethereum and the Mist browser. Develop and test a sample application.	2Hrs

3	Implement and demonstrate the use of the following in Solidity: a. Variable, Operators, Loops, Decision Making, Strings, Arrays, Enums, Structs, Mappings, Conversions, Ether Units, Special Variables. b. Functions, Function Modifiers, View functions, Pure Functions, Fallback Function, Function Overloading, Mathematical functions, Cryptographic functions.	2Hrs
4	Implement and demonstrate the use of the following in Solidity: a. Withdrawal Pattern, Restricted Access. b. Contracts, Inheritance, Constructors, Abstract Contracts, Interfaces. c. Libraries, Assembly, Events, Error handling.	2Hrs
5	Install hyperledger fabric and composer. Deploy and execute the application.	2Hrs
6	Write a program to demonstrate mining of Ether.	2Hrs
7	Demonstrate the running of the blockchain node.	2Hrs
8	Demonstrate the use of Bitcoin Core API.	2Hrs
9	Create your own blockchain and demonstrate its use.	2Hrs
10	Build Dapps with angular.	2Hrs

Reference Books:

1. Beginning BlockchainA Beginner's Guide to Building Blockchain Solutions Bikramaditya Singhal, GautamDhameja, PriyansuSekhar Panda Apress 2018
2. Introducing Ethereum and Solidity Chris DannenApress 2017
3. The Blockchain Developer EladElromApress 2019
4. Mastering Ethereum Andreas M. Antonopoulos Dr. Gavin Wood O'Reilly First 2018
5. Blockchain Enabled Applications Vikram Dhillon David Metcalf Max Hooper Apress 2017

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Digital Image Forensics
Course Code	PIT4DIF
Credit	4
Hours	4 Hrs per week

Course Objectives	• To understand describe the origin of computer forensics and the relationship between law enforcement and industry. • Describe electronic evidence and the computing investigation process. • Extracting Digital Evidence from Images and establishing them in court of Law. • Enhancing images for investigation and various techniques to enhance images. • Interpret and present Evidences in Court of Law.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Define the origin of Computer Forensics & relationship between law enforcement & industry
	2. Distinguish Digital Still & Digital Video Camera , Color Mode & Channel Blending
	3. Classify Multiple Image Techniques, Contrast adjustment Techniques & Advanced Processing Techniques
	4. Elaborate Enhancement Strategies for Image Intended for Analysis.

Module/ Unit	**Course Description**	**Hrs**
I	History of Forensic Digital Enhancement, Establishing Integrity of Digital Images for Court,	**12**
II	Digital Still and Video Cameras, Color Modes and Channel Blending to Extract Detail.	**12**
III	Multiple Image Techniques, Fast Fourier Transform (FFT) – Background Pattern Removal.	**12**

IV	Contrast Adjustment Techniques, Advanced Processing Techniques, Comparison and Measurement	**12**
V	The Approach – Developing Enhancement Strategies for Images Intended for Analysis, Digital Imaging in the Courts, Interpreting and Presenting Evidence	**12**

Reference Books:

1. Forensic Digital Image Brian Dalrymple, Jill CRC 2018 Processing: Optimization of impression Evidence Smith Press
2. Forensic Uses of Digital Imaging John C. Russ, Jens Rindel, P. Lord Taylor & Francis Group 2nd2016

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Digital Image Forensics Practical
Course Code	PIT4DFP
Credit	2
Hours	4 Hrs per week

Course Objectives	• To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices. • The main goal of Digital Image forensics is to identify, collect, preserve, and analyse data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Apply basic Image Forensics Techniques to establish their integrity
	2. Categorize different technique for extracting details from images
	3. Measure various parameters associated with digital Images
	4. Apply various enhancement strategies for digital image

Module/ Unit	**Course Description**	**Hrs**
1	Finding image raw data by using Data Acquisition tools.	2Hrs
2	Fake photo Identification using Forensically.	2Hrs
3	Understand the Apply image in Photoshop.	2Hrs
4	Use Image subtraction technique on image.	2Hrs

5	Understand calculation dialogue box using Photoshop Focus Stacking.	2Hrs
6	Do HDR pro procedure on image.	2Hrs
7	Understand the Channel Subtraction in Photoshop.	2Hrs
8	Understand different tools in Photoshop.	2Hrs
9	Making adjustments in curves using Photoshop	2Hrs
10	Understand Shadow/Highlight dialogue box.	2Hrs

Reference Books:

1. Forensic Digital Image Brian Dalrymple, Jill CRC 2018 Processing: Optimization of impression Evidence Smith Press
2. Forensic Uses of Digital Imaging John C. Russ, Jens Rindel, P. Lord Taylor & Francis Group 2nd2016

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Security Operations Centre
Course Code	PIT4SOC
Credit	4
Hours	4 Hrs per week

Course Objectives	• To get the insight of the security loopholes in every aspect of computing. • To understand the threats and different types of attacks that can be launched on computing systems. • To know the countermeasures that can be taken to prevent attacks on computing systems. • To test the software against the attacks

Course Outcomes	**After completing the course, Student will be able to:**
	1. Classify different security breaches that can occur.
	2. Identify vulnerabilities in the systems, breach the security of the system, and threats due to malware.
	3. Develop social engineering and educate people to be Careful from attacks due to it.
	4. Evaluate vulnerabilities in the Web Servers, Applications and newer technologies like mobiles, IoT and computing.

Module/ Unit	**Course Description**	**Hrs**
I	**Introduction to Security Operations Management:** Foundation Topics Introduction to Identity and Access Management Phases of the Identity and Access Lifecycle Registration and Identity Validation Privileges Provisioning Access Review Access Revocation Password Management Password Creation Password Storage and Transmission Password Reset Password Synchronization Directory Management Single Sign-On Kerberos Federated SSO Security Assertion Markup Language OAuth OpenID Connect Security Events and Logs Management Logs Collection, Analysis, and Disposal Syslog Security Information and Event Manager Assets Management Assets Inventory Assets	**12**

	Ownership Assets Acceptable Use and Return Policies Assets Classification Assets Labeling Assets and Information Handling Media Management Introduction to Enterprise Mobility Management Mobile Device Management Configuration and Change Management Configuration Management Change Management Vulnerability Management Vulnerability Identification Finding Information about a Vulnerability Vulnerability Scan Penetration Assessment Product Vulnerability Management Vulnerability Analysis and Prioritization Vulnerability Remediation Patch Management References and Additional Readings **Fundamentals of Cryptography and Public Key Infrastructure** (PKI): Cryptography Ciphers and Keys Ciphers Keys Block and Stream Ciphers Symmetric and Asymmetric Algorithms Symmetric Algorithms Asymmetric Algorithms Hashes Hashed Message Authentication Code Digital Signatures Digital Signatures in Action Key Management Next-Generation Encryption Protocols IPsec and SSL IPsec SSL Fundamentals of PKI Public and Private Key Pairs RSA Algorithm, the Keys, and Digital Certificates Certificate Authorities Root and Identity Certificates Root Certificate Identity Certificate X.500 and X.509v3 Certificates Authenticating and Enrolling with the CA Public Key Cryptography Standards Simple Certificate Enrollment Protocol Revoking Digital Certificates Using Digital Certificates PKI Topologies Single Root CA Hierarchical CA with Subordinate CAs Cross-certifying CAs Exam Preparation Tasks Review All Key Topics Complete Tables and Lists from Memory **Introduction to Virtual Private Networks (VPNs)** What Are VPNs? Site-to-site vs. Remote-Access VPNs An Overview of IPsec IKEv1 Phase 1 IKEv1 Phase 2 IKEv2 SSL VPNs SSL VPN Design Considerations User Connectivity VPN Device Feature Set Infrastructure Planning Implementation Scope	
II	**Windows-Based Analysis:** Process and Threads Memory Allocation Windows Registration Windows Management Instrumentation Handles Services Windows Event Logs Exam Preparation Tasks **Linux- and Mac OS X–Based Analysis:** Processes Forks Permissions Symlinks Daemons UNIX-Based Syslog Apache Access Logs **Endpoint Security Technologies:** Antimalware and Antivirus Software Host-Based Firewalls and Host-Based Intrusion Prevention Application-Level Whitelisting and Blacklisting System-Based Sandboxing	**12**
III	**Threat Analysis:** What Is the CIA Triad: Confidentiality, Integrity, and Availability? Confidentiality Integrity Availability Threat Modeling Defining and Analyzing the Attack Vector Understanding the Attack Complexity Privileges and User	**12**

	Interaction The Attack Scope Exam Preparation Tasks **Forensics:** Introduction to Cybersecurity Forensics The Role of Attribution in a Cybersecurity Investigation The Use of Digital Evidence Defining Digital Forensic Evidence Understanding Best, Corroborating, and Indirect or Circumstantial Evidence Collecting Evidence from Endpoints and Servers Collecting Evidence from Mobile Devices Collecting Evidence from Network Infrastructure Devices Chain of Custody Fundamentals of Microsoft Windows Forensics Processes, Threads, and Services Memory Management Windows Registry The Windows File System Master Boot Record (MBR) The Master File Table (MFT) Data Area and Free Space FAT NTFS MFT Timestamps, MACE, and Alternate Data Streams EFI Fundamentals of Linux Forensics Linux Processes Ext4 Journaling Linux MBR and Swap File System Exam Preparation Tasks **Fundamentals of Intrusion Analysis:** Common Artifact Elements and Sources of Security Events False Positives, False Negatives, True Positives, and True Negatives Understanding Regular Expressions Protocols, Protocol Headers, and Intrusion Analysis Using Packet Captures for Intrusion Analysis Mapping Security Event Types to Source Technologies	
IV	**Introduction to Incident Response and the Incident Handling Process Introduction to Incident Response:** What Are Events and Incidents? The Incident Response Plan The Incident Response Process The Preparation Phase The Detection and Analysis Phase Containment, Eradication, and Recovery Post- Incident Activity (Postmortem) Information Sharing and Coordination Incident Response Team Structure The Vocabulary for Event Recording and Incident Sharing (VERIS) **Incident Response Teams:** Computer Security Incident Response Teams (CSIRTs) Product Security Incident Response Teams (PSIRTs) Security Vulnerabilities and Their Severity Vulnerability Chaining Role in Fixing Prioritization Fixing Theoretical Vulnerabilities Internally Versus Externally Found Vulnerabilities National CSIRTs and Computer Emergency Response Teams (CERTs) Coordination Centers Incident Response Providers and Managed Security Service Providers (MSSPs) **Compliance Frameworks:**Payment Card Industry Data Security Standard (PCI DSS) PCI DSS Data Health Insurance Portability and Accountability Act (HIPAA) HIPAA Security Rule HIPAA Safeguards Administrative Safeguards Physical Safeguards Technical Safeguards Sarbanes-Oxley (SOX) Section 302 Section 404 Section 409 SOX Auditing Internal Controls **Network and Host Profiling:** Network Profiling Throughput Measuring Throughput Used Ports Session Duration Critical Asset Address Space Host	**12**

	ProfilingListening Ports Logged-in Users/Service Accounts Running Processes Applications	
V	**The Art of Data and Event Analysis:** Normalizing Data Interpreting Common Data Values into a Universal Format Using the 5-Tuple Correlation to Respond to Security Incidents Retrospective Analysis and Identifying Malicious Files Identifying a Malicious File Mapping Threat Intelligence with DNS and Other Artifacts Deterministic Versus Probabilistic Analysis **Intrusion Event Categories** Diamond Model of Intrusion Cyber Kill Chain Model Reconnaissance Weaponization Delivery Exploitation Installation Command and Control Action and Objectives **Types of Attacks and Vulnerabilities:** Types of Attacks Reconnaissance Attacks Social Engineering Privilege Escalation Attacks Backdoors Code Execution Man-in-the Middle Attacks Denial-of-Service Attacks Direct DDoS Botnets Participating in DDoS Attacks Reflected DDoS Attacks Attack Methods for Data Exfiltration ARP Cache Poisoning Spoofing Attacks Route Manipulation Attacks Password Attacks Wireless Attacks Types of Vulnerabilities **Security Evasion Techniques:** Key Encryption and Tunneling Concepts Resource Exhaustion Traffic Fragmentation Protocol-Level Misinterpretation Traffic Timing, Substitution, and Insertion Pivoting	**12**

Reference Books:

1. CCNA Cyber Ops SECOPS 210-255 Official Cert Guide Omar Santos, Joseph Muniz CISCO 1st 2017
2. CCNA Cyber Ops SECFND 210-250 Official Cert Guide Omar Santos, Joseph Muniz CISCO 1st 2017
3. CCNA Cyber security Operations Companion Guide CISCO 1st 2018

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Security Operations Centre Practical
Course Code	PIT4SOP
Credit	2
Hours	4 Hrs per week

Course Objectives	• To make the learners capable using of various network information gathering tools. • To make the learners capable of using various network security tools.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Make use of tools to perform footprinting and reconnaissance
	2. Determine use of Enumeration and network scanning tools.
	3. Test social engineering toolkits and web application scanning.
	4. Apply different tools for cryptography.

Module/ Unit	**Course Description**	**Hrs**
1	Encrypting and Decrypting Data Using OpenSSL	2Hrs
2	Demonstrate the use of Snort and Firewall Rules	2Hrs
3	Demonstrate Extract an Executable from a PCAP	2Hrs
4	Demonstrate Analysis of DNS Traffic	2Hrs
5	Create your own syslog Server	2Hrs
6	Configure your Linux system to send syslog messages to a syslog server and Read them	2Hrs
7	Install and Run Splunk on Linux	2Hrs
8	Install and Configure ELK on Linux	2Hrs

9	Install and Configure GrayLog on Linux	2Hrs
10	Demonstrate Conversion of Data into a Universal Format.	2Hrs

Reference Books:

1. CCNA Cyber Ops SECOPS 210-255 Official Cert Guide Omar Santos, Joseph Muniz CISCO 1st 2017
2. CCNA Cyber Ops SECFND 210-250 Official Cert Guide Omar Santos, Joseph Muniz CISCO 1st 2017
3. CCNA Cyber security Operations Companion Guide CISCO 1st 2018

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Human Computer Interaction
Course Code	PIT4HCI
Credit	4
Hours	4 Hrs per week

Course Objectives	• Understand the important aspects of implementation of human-computer interfaces. • Identify the various tools and techniques for interface analysis, design, and evaluation. • Identify the impact of usable interfaces in the acceptance and performance utilization of information systems.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Define HCI principles that influence a system's interface design.
	2. Explain techniques used for any of the proposed systems.
	3. Explain the cognitive models and its design.
	4. Elaborate system resource management techniques and implementing systems.

Module/ Unit	**Course Description**	**Hrs**
I	**The Interaction:** Models of interaction, Design Focus, Frameworks and HCI, Ergonomics, Interaction styles, Elements of the WIMP interface, Interactivity **Paradigms:** Introduction, Paradigms for interaction **Interaction design basics:** What is design?, The process of design, User focus, Cultural probes, Navigation design, the big button trap, Modes, Screen design and layout, Alignment and layout matters, Checking screen colors, Iteration and prototyping **HCI in the software process**: The software life cycle, Usability engineering , Iterative design and prototyping, Prototyping in practice, Design rationale	**12**

II	**Design**: Principles to support usability, Standards, Guidelines, Golden rules and heuristics, HCI patterns **Implementation support:** Elements of windowing systems, Programming the application, Going with the grain, Using toolkits, User interface management systems **Evaluation techniques:** What is evaluation?, Goals of evaluation, Evaluation through expert analysis, Evaluation through user participation, Choosing an evaluation method	**12**
III	**Universal design:** Universal design principles, Multimodal interaction, Designing websites for screen readers, Choosing the right kind of speech, Designing for diversity **User support:** Requirements of user support, Approaches to user support, Adaptive help systems, Designing user support systems **Cognitive models:** Goal and task hierarchies, Linguistic models, The challenge of display-based systems, Physical and device models, Cognitive architectures	**12**
IV	**Socio-organizational issues and stakeholder requirements:** Organizational issues, Capturing requirements **Communication and collaboration models:** Face-to face communication, Conversation, Text-based communication, Group working **Task analysis:** Differences between task analysis and other techniques, Task decomposition, Knowledge based analysis, Entity–relationship-based techniques, Sources of information and data collection, Uses of task analysis	**12**
V	**Dialog notations and design:** What is dialog?, Dialog design notations, Diagrammatic notations, Textual dialog notations, Dialog semantics, Dialog analysis and design **Models of the system:** Standard formalisms, Interaction models, Continuous behavior **Modeling rich interaction:** Status–event analysis, Rich contexts, Low intention and sensor-based interaction	**12**

Reference Books:

1. HUMAN-COMPUTER INTERACTION, Alan Dix, Janet Finlay,Gregory D. Abowd, Russell Beale, Third Edition, Pearson Education

Course Description: M.Sc. (Information Technology)	
Semester	IV
Course Name	Project Implementation and Viva-Voce
Course Code	PIT4PIP
Credit	2
Hours	4 Hrs per week

Course Objectives	The Project Implementation and Viva Voce details are given in Appendix 1.

Course Outcomes	**After completing the course, Student will be able to:**
	1. Design User Interface
	2. Develop Coding for the project
	3. Examine various system testing
	4. Predict the future Scope of Project

Appendix – 1

Project Documentation and Viva-voce (Semester III) and Project Implementation and Viva-Voce (Semester IV)

Goals of the course Project Documentation and Viva-Voce

The student should:

- be able to apply relevant knowledge and abilities, within the main field of study, to a given problem within given constraints, even with limited information, independently analyse and discuss complex inquiries/problems and handle larger problems on the advanced level within the main field of study reflect on, evaluate and critically review one's own and others' scientific results
- be able to document and present one's own work with strict requirements on structure, format, and language usage
- be able to identify one's need for further knowledge and continuously develop one's own Knowledge

To start the project:

- Start thinking early in the programme about suitable projects.
- Read the instructions for the project.
- Attend and listen to other student´s final oral presentations.
- Look at the finished reports.

- Talk to senior master students.
- Attend possible information events (workshops / seminars / conferences etc.) about the related topics.

Application and approval:

- Read all the detailed information about project.
- Finalise finding a place and supervisor.
- Check with the coordinator about subject/project, place and supervisor.
- Write the project proposal and plan along with the supervisor.
- Fill out the application together with the supervisor.
- Hand over the complete application, proposal and plan to the coordinator.
- Get an acknowledgement and approval from the coordinator to start the project.

During the project:

- Search, gather and read information and literature about the theory.
- Document well the practical work and your results.
- Take part in seminars and the running follow-ups/supervision.
- Think early on about disposition and writing of the final report.
- Discuss your thoughts with the supervisor and others.
- Read the SOP and the rest you need again.
- Plan for and do the mid-term reporting to the coordinator/examiner.
- Do a mid-term report also at the work-place (can be a requirement in some work-places).
- Write the first draft of the final report and rewrite it based on feedback from the supervisorand possibly others.
- Plan for the final presentation of the report.

Finishing the project:

- Finish the report and obtain an OK from the supervisor.
- Ask the supervisor to send the certificate and feedback form to the coordinator.
- Attend the pre-final oral presentation arranged by the Coordinator.
- Rewrite the final report again based on feedback from the opponents and possibly others.
- Prepare a title page and a popular science summary for your report.
- Send the completed final report to the coordinator (via plagiarism software)
- Rewrite the report based on possible feedback from the coordinator.
- Appear for the final exam.

Project Proposal/research plan

- The student should spend the first 1-2 weeks writing a 1-2 pages project plan containing:

- Short background of the project
- Aims of the project
- Short description of methods that will be used
- Estimated time schedule for the project

- The research plan should be handed in to the supervisor and the coordinator.
- Writing the project plan will help you plan your project work and get you started in finding information and understanding of methods needed to perform the project.

Project Documentation

The documentation should contain:

- Introduction - that should contain a technical and social (when possible) motivation of the project topic.
- Description of the problems/topics.
- Status of the research/knowledge in the field and literature review.
- Description of the methodology/approach. (The actual structure of the chapters here depends on the topic of the documentation.)
- Results - must always contain analyses of results and associated uncertainties.
- Conclusions and proposals for the future work.
- Appendices (when needed).
- Bibliography - references and links.

For the master's documentation, the chapters cannot be dictated, they may vary According to the type of project. However, in Semester III Project Documentation and Viva Voce must contain at least 4 chapters (Introduction, Review of Literature, Methodology / Approach, Proposed Design / UI design, etc. depending on the type of project.) The Semester III report should be spiral bound.

Examination Pattern

Theory: 100 Marks (60 +40=100)

60 Theory			40 Internal
Q.1	**Solve any 2 (From 4)**	**12 M**	**1) Class Test 20M** **2) Attendance 5M** **3) Presentation 15M** **<u>Semester III (For only 1 subject)</u>** **SWAYAM(Advanced Course) of minimum 20 hours and certification exam should be completed in any one of the course.** **<u>Semester IV (For only 1 subject)</u>** **Research paper to be Published for any of the course.**
Q.2	**Solve any 2 (From 4)**	**12 M**	
Q.3	**Solve any 2 (From 4)**	**12 M**	
Q.4	**Solve any 2 (From 4)**	**12 M**	
Q.5	**Solve any 2 (From 4)**	**12 M**	

Practical: 50 Marks

50 Marks	OR	50 Marks
20 Program1		40 Program1
20 Program 2		
5 Viva		5 Viva
5 Journal		5 Journal