Professional Diploma in Cyber Investigations and Law

Curriculum and Syllabus
2020

(Applicable to the students admitted from the Academic year 2020 onwards)

INSTITUTE OF TECHNOLOGY MANAGEMENT & RESEARCH
(Division of Mamta Trust)
2/850, Mugalivakkam Main Road, Mugalivakkam, Chennai – 600 125

Eligibility Criteria for this program

TO be filled up

Enrollment process:

1. Filled up applications are received for scrutiny
2. All applicable eligibility credentials are validated (Graduation, proof of employment , proof of experience as defined in eligibility criteria)
3. A **personal interview** by a Panel of professionals will be carried out to evaluate the candidate, his knowledge of computers and understand the submitted credentials to complete the enrollment.

Codification:

The codification of the courses of this program will be in consonance with the existing codes for similar subjects and for all other courses, they will be defined de novo.

INSTITUTE OF TECHNOLOGY MANAGEMENT & RESEARCH

Diploma in Cyber Investigations & Laws

CURRICULUM 2013-2014

Sl. No	Course Code	Course Title	L	T	P	C	TCH
SEMESTER I							
Theory							
1.	DCE201	Cyber Risk Management	3	0	0	3	3 45
2.	DCE202	Cyber Investigation Management	3	0	0	3	3
3	DCE203	Cyber forensics	4	0	0	4	4 60
4.	DCE204	Cyber Law	4	0	0	4	4
5.	DCE205	SIEM & log trails	3	0	0	3	3
Practical							
6.	DCE206	Forensics and VA lab	0	0	4	2	2
7.	DCE207	Project	0	0	7	4	4
		Total Credits	23				

	Cyber RISK Management	L T P C 3 0 0 3

Goal	To introduce the principles of Cyber Risk management and expose the various techniques of Risk evaluation

Objective:	Outcome :
• Understand the components of IT Systems • Understand the IT assets and Asset evaluation techniques • Understand the Threat modeling methods • Understand the elements of Risk assessment • Understand Business Continuity	• Differentiate the IT components • Apply Asset evaluation methods • Apply threat modelling methods • Apply the elements of Risk Assessment techniques • Apply business continuity components

Unit 1: IT Systems: Information Systems - System components - network components - Risk management - What is Risk - profile - identification -assessment -Analysis -Response -Tolerance - Risk types - inherent risk - control risk - audit risk. -Security risk analysis - Advantages

Unit 2: IT Assets: Assets management - Identify Assets - Asset classification - Asset valuation - Binary Asset Valuation -Rank-Based Asset Valuation - Consensus Asset Valuation - Classification-Based Asset Valuation - others

Unit 3: Cyber Threat: Threat management - Identifying Threats -Threat model - Threat attributes - Attack tree - STRIDE - DREAD - OCTAVE - CAPEC- Threat Statements- Technical Threats and Safeguards - Physical Threats and Safeguard - Human Threats to Physical Security -The RIIOT Method: Physical Data Gathering - Test Physical Security Safeguard.

Unit 4: Risk Assessment: Security Risk Assessment - Quantitative vs. Qualitative Analysis - Determining Risk - Creating Risk Statement - Security Risk Mitigation - Selecting Safeguard - Security Risk Assessment Reports - Report Structure.

Unit 5: Business Continuity: Principles of Business continuity - Business Interruption Events – Business impact assessment – fire exposure analysis – functional analysis –compliance issues – Pre-Planning - Initial Response - Recovery - Identification of Recovery environment - Identification of Recovery Point - site and structures – Equipment and technology – documents and records electronic equipment and process equipment - Business continuity plans – crisis management plans –function restoration plans – disaster recovery plans – Incident Response Plan

Text Book

1. Thomas L Norman., Risk analysis and Security counter measure selection , CRC press, 2010
2. Ariel Evans, Managing Cyber Risk, Routledge, 2019
3. Lee T Ostrom, Risk Assessment: Tools, Techniques, and Their Applications, Wiley 2019
4. Christopher Hodson,, Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls, Kogan, 2019
5. Richard.E Cascarino., Auditors guide to information system auditing, John Wiley and Sons, 2007

	Cyber Forensics	L T P C 3 0 0 3

Goal	To introduce concepts of cybercrime and Cyber Forensics with a focus on disk forensics network forensics and software forensics
Objective: •	**Outcome :** •

Unit I: Cyber Crime: Cyber world - Data - Information – cyber threat - cybercrime – White collar crimes – economic offense – cyber stalking - cyber extortion – insider threat - Hacker - types– cyber terrorism - cyber espionage - cyber warfare -weapons - Professional Ethics: Characteristics - system of professions - computing profession - professional relationships - code of ethics and professional conduct - Ethical dilemmas – Ethical decision making - Cyber Forensic Evidence Management

Unit II : Types of Cyber Crime: Data frauds - data diddling - scavenging - data theft - data leakage – data hiding - Information theft – cybersquatting - Id theft - Password theft – key logger - Child Pornography - obscene messages - Job Racketing - Marketing and Advertisement Rackets - Nigerian frauds- pay per click scams – web defacement - Accounting Frauds - Fraud Schemes - ATM frauds - credit, debit card crimes - Card Cloning - salami techniques - IP spoofing - email & ip address – Telecommunication Fraud - Software piracy

Unit 3: Disk Forensics : Digital data – digital device – Hard disk – Types – Disk characteristics – SSD - File systems - NTFS – MFT Structure - fragmentation -MFT fragmentation – Files and attributes - File hashing - Slack space – Disk Forensics tools - Win Hex – Disk imaging – write blockers – types of blockers - Data Carving – techniques - Scalpel - Registry Forensics - Registry – registry data types – RegEdit -concept of timeline – Anti forensics.

Unit 4: Software Forensics : Volatile Live Vs Offline Forensics - Artefacts - System Information - Linux ~ Windows – System commands - Network information – Network commands - proc file system - Software Program - source code - types of software - Source code repository - software license - commercial piracy - soft lifting - structures & versions - Analysis Tools - Objects of analysis - Obfuscation – code Obfuscation - Stylometric - author characteristics - Software Forensic challenges – Principles of Steganography

Unit 5: Network Forensics: Network components - Port scans – SYN flood -Key Loggers - Email Forensics - email spoofing – Phishing – mail header analysis - Network protocols – Protocols Susceptible to Sniffing - Active and Passive Sniffing - Wireshark – Capture and Display Filters - pcap analysis – Problems - Trojans and Backdoors, Overt and Covert Channels, Types of Trojans - Botnets - types of botnet- Structure of bots – Crime bots - Spamming bots - DoS – DDoS Attacks – types - Honey Pots - Forensic evidences.

Text Books

1. Dejey, Cyber forensics, Oxford, 2018
2. Gerard Johanses, Digital forensics and incident response, 2017
3. Harlon Carvey, Windows Registry forensics, Syngress, 2011
4. Sherri Davidoff et al, Network forensics, Prentice Hall, 2012
5. Albert J Marcella, et al, Cyber forensics, 2nd edition, Auerbach, 2008
6. George Mohay et al, Computer and intrusion forensics, Artech house, 2003
7. Mani , legal Framework on Cyber Crimes Lawmann’s, Kamal Publishers, New Delhi, 2011
8. Tommie Singleton, Fraud Auditing and Forensic Accounting, John Wiley, 3rd Ed, 2006

	Cyber Investigation Management	L T P C 4 0 0 4

Goal	Introduce the concept of Cyber investigation and prepare the individual for cyber investigation profiles
Objective: • Understand the basics of Cyber Investigation • Understand the concepts of Profiling • Understand the concepts of Crime Scene Management • Understand the evidence types and management needs • Define the Case management needs	**Outcome :** • Differentiate between Investigation and cyber investigation • List the profiling traits • Working knowledge on Intrusion investigation • Manage evidences • Manage Case and address the requirements

Unit 1: Investigation: Concepts of Investigation - types of investigation - Digital Investigation – Intrusion investigation – Criminal investigation – forensic investigation – Network investigation - Observation skills - the investigate process – Investigation Unit - Role of investigator – Electronic Discovery – Hypothesis creation - Legal Context - Professional Ethics: Characteristics - system of professions - code of ethics and professional conduct.

Unit 2: Cyber Investigation : Warrant – Types of warrant - Search warrant - concept of search – home search – computer search - cyber investigation - Network Investigation - Investigating audit logs - Investigating Web attacks - Investigating Computer Intrusions - Profiling - criminal profiling - deviant behaviour - Motive - stylometric

Unit 3: Cyber Crime Scene: Elements of a cyber-case – Scene of cyber-crime - Surveying and preserving digital crime scene - Chain of custody –challenges – Admissibility.

Unit 4: Evidence Management: Evidence – Digital Evidence - Types of evidence – physical evidence – real evidence – circumstantial evidence – network evidence- digital evidence– Evidence collection – Evidence Analysis - Contextual Information – Timing - Evidence Management –- Investigative Reconstruction with Digital Evidence. - The Process of Elimination - Tools

Unit 5 Case Management : case life cycle - Identification of a cyber-crime –code of criminal procedure - Jurisdiction –types of jurisdiction – Handling a Digital Crime Scene - Cyber Crime Case filing procedures – Lodging a complaint – Registering case - Filing F.I.R. – Contents of F.I.R - Tracking of FIR - correlation & corroboration - Cyber Crime in Court - Role of court appointed experts.

Text book

1. Rory J McMahon, Practical handbook for Private investigators, CRC, 2nd Ed 2007
2. Christopher, L.T. Brown, Computer Evidence Collection and Preservation, Cengage, 2010
3. Tom Bazley, Investigating White collar crime, Pearson 2008
4. H.K.Saharay, Law of Evidence, Eastern Law House, 2008

Reference

1. Bruce Middleton, Cyber Crime Investigators Field Guide, Auerbach,2002
2. Thomas A Johnson, Forensic Computer Crime Investigation, CRC, 2005
3. Barry A.J. Fisher, Techniques of Crime Scene Investigation, CRC, 2004
4. Peter Stephenson, Investigating Computer Related Crime A handbook for Corporate Investigators, CRC 2000
5. Gerald R McMenamin, Forensic Linguistics Advances in Forensic stylistics, CRC,2002

DCE204	**Cyber Law**	L T P C 4 0 0 4
Goal	To enable a prospective student to understand the various types of cybe and associated legal implications.	

Objective:	**Outcome :**
• Understand the concept of cyber crime • Understand & differentiate types of cyber crime • Understand network crime and techniques • Understand IT ACT and role • Correlate IT ACT with related acts	• Differentiate the various types of cyber crime • Differentiate the various types of virus and BOTS and their crime ware capabilities • Differentiate the various elements of IT act and related amendments • IT acts influence on Related acts

Unit 1 CrPC: Constitution of criminal courts - power of courts - arrest of persons - process to compel appearance - summons - warrant of arrest - summons to product - search warrants - general provisions relating to search - maintenance of public order - jurisdictions of criminal courts - conditions requisite for initiating of proceedings - complaints to magistrates - charge - trial -evidence in inquiries and trials - transfer of cases - provisions of bails and bonds

Unit 2 IT Act-Digital Signature: Information Technology Act 2000 – Digital signature - Electronic Governance - Secure electronic records - Regulation of certifying authorities - Electronic signature certificates - Penalties compensation –

Unit-3: IT Act- Offences: Adjudication - Offenses - Examiner of electronic evidence - Amended IT Act - Provisions of other Acts amended by I.T. Act

Unit 4 Intellectual Property: Intellectual Property - Types of IP - Copyright Act – Ownership – Duration Registration - Originality of Material - Fixation of Material - Exclusions from Copyright Protection - Compilations – Collections - Derivative Works. Patents: Patents Act - Patentability - Design Patents - Double Patenting - Direct Infringement - Inducement to Infringe - Contributory Infringement.

Unit 5 Trade Mark act: Trademark classes - What can be trademarked - Trademark Registration Process - Post-registration Procedures- Legal rights - obligations - infringement of trade mark - trade marking cyber world - trade mark and website registration - case studies

Text book

1. V.K.Ahuja, Law relating to Intellectual Property rights. LexisNexis, 2017
2. V.K.Ahuja, Intellectual Property rights in India. Vol 1 and Vol 2 LexisNexis, 2009

Reference

3. N.R.Subbaram, Demystifying Intellectual Property Rights, LexisNexis, 2009
4. Deepak Gogia, Intellectual Property Law, Ashoka Law House, 2010

<table>
<tr><td></td><td colspan="2"><b>SIEM AND LOG TRAILS</b></td><td>L T P C
3 0 0 3</td></tr>
<tr><td><b>Goal</b></td><td colspan="3">To expose the learner on the relevance of various types of Logs generated from different systems and expose the concept of SIEM which is used for Log correlation and alerts</td></tr>
<tr><td colspan="2"><b>Objective:</b>
• Understand the relevance of MIB and RMON
• Understand the Concept of Log formats and log correlation
• Understand the relevance and working of Syslog server
• Understand the relevance and working of SNORT</td><td colspan="2"><b>Outcome :</b>
• Differentiate the MIBs, OIDs and RMON capabilities
• Differentiate the Log formats
• Understand the configurations of Syslog server
• Understand SNORT configuration and SNORT rules.</td></tr>
</table>

Unit 1: Introduction: Concepts of Log, What Should the Logs Log? Everything - The 5 Ws (Who, What, When, Where, and Why) - Unix Logs – Windows Logs - Events and Event Lifecycle - Linux Logs - Types of logs - Security logs - Application logs – System Logs – WMI – WMI Architecture

Unit 2: SNMP: Simple Network Management Protocol – Structure – Basic commands – get get next,…Management Information Base (MIB) – V1, V2 and V3, RMON - OID notation - OID Trees - SNMP Tools, Case Studies

Unit 3: Log Formats And Log Collection: Log files – Log formats – application specific Log Formats - Apache Logs - Mail logs - Firewall Logs – vendor Specific Logs - Event Correlation - Event Normalization, Correlation Rules Log Collection - Push Log Collection - Pull Log Collection - Prebuilt Log Collection - Custom Log - Parsing/Normalization of Logs - Rule Engine/Correlation Engine - Correlation Engine, Case Studies

Unit 4: Managing Log Files: Log tools – SYSLOG – Open source Log analyzers - Log File Conversion -Standardizing Log Formats - Using XML for Reporting -Correlating Log File Data -Log Rotation and Archival -Determining an Archiving Methodology -Separating Logs, Case Studies

Unit 5: Investigating Intrusions: Intrusion detection system - NIDS, HIDS - Locating Intrusions - Monitoring Logons - Monitoring IIS - Reconstructing Intrusions – concepts of SNORT - Rules - Rule headers - Rule options - Pre- processors - Stream4 - Frag2 - Frag3 - HTTP inspect - plugins - Alerts Detail Report, Case Studies.

TEXT BOOKS

1. David Miller, Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2010
2. Client P Garrison, Digital forensics for network internet and cloud computing, , Elsevier, 2010
3. Jacob Babbin et al, Security Log Management-Identifying patterns in chaos, Syngress, 2006
4. Vivek Chopra, et al, Professional Apache Tomcat, Wrox, 2004
5. Gabriele Giuseppini, et al, Microsoft Log Parser Toolkit, Syngress, 2004
6. Toby Kohlenberg, Snort IDS and IPS toolkit, Syngress, 2007
7. Al-Sakib Khan Pathan, The State of the Art in Intrusion Prevention and Detection, CRC 2014
8. John R.Vacca, Scott Ellis, Firewalls Jumpstart for Network and Systems Administrators, Elsevier,2005

	FORENSICS LAB	L T P C 0 0 4 2
Goal	To understand the use of tools to manage forensics and system and application level vulnerability	
Objective: 1. Understand the technique of collecting live forensic information 2. Understand the use of disk forensic tools 3. Understand the use of mobile forensic tools 4. Understand the use of Network forensic tools	**Outcome :** 1.Exhibit live forensic data collection 2.Exhibit the use of disk forensic tool to collect and manage evidence 3.Exhibit SIM data collection techniques 4. Use network tools to collect VA and exploits data	

1. Use NMAP as your tool and try out the various scan types with different flag combinations. With a single IP address and multiple IP address combinations.

2. Load a single IP address in Nessu**s** and carry out a light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Extend the exercise for a range of addresses in Nessus and repeat the light scan, and intensive scan of the identified machines. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Also list out the block range of Filters available for SCAN as a part of your report

3. Load a single IP address in OPENVAS and carry out a light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Extend the exercise for a range of IP addresses in OPENVAS and repeat the light scan, and intensive scan of the IP address. Generate the reports for both types of SCAN. Compare the scan and generate a report on the observed changes. Also list out the block range of Filters available for SCAN as a part of your report.

4. Use the password cracker tool (**SALT** or equivalent) and with a given encrypted / or shadowed password file, try to identify the username and the respective passwords.

5. Using Wireshark as a tool capture the network traffic and reconstruct the data flowing through the network for an Identified HTTP traffic.

6. Using Wireshark as a tool, load an captured pcap file and analyse the same with respect to given problem. Isolate the evidences from the captured traffic file, construct a forensic report describing the incidents in a time line view.

7. Live Forensics: Identify the following details from the target machine using live analysis tool. List loaded programs, List current network connections, List running processes, List open share files, list of routing table entries, list of ARP entries.

8. Using Nikto as a web application analysis tool, scan a given website for web vulnerabilities at the web server level and the application level

9. Using Wapiti as a web application analysis tool scan a given website for web vulnerabilities at the web server level and the application level

10. For a given email header, carry out the header analysis, identify the domains, and reconstruct the mail traffic flow from the sender to the receiver. Differentiate between internal and external IP addresses if available in the header and try to reconstruct the network.

11. In a given machine Identifiy the list of visited websites with respect to Internet explorer and Firefox. Generate the output as a timeline entry. Mark observed deviations in browsing based on the timeline and describe the person's activity at that point in time.

12. Take a USB stick which has a few jpeg images. Delete a few JPEG images. and create an disk image of USB. Mount the disk image and using Scalpel tool retrieve the deleted images.

13. With a sample apache attack log, analyse the shared log and try to identify the attacker along with the steps in identifying the method of entry.

14. For the given Asset inventory, identify the threat and risk matrix and hence calculate the exposure risk for the shared assets. Propose a risk mitigation plan.

15. With the given windows system, use a suitable disk explorer tool and identify the directory structure and windows specific hidden file locations especially, the event and security log entry locations and system32 locations with file size entries,

16. With the given windows system, identify the various registry entries and generate a report on the current configuration and current user permissions. With the given configuration and the permissions, try to reconstruct the users, and their privileges.

17. **Demonstration only**: Load a SIM card and analyze the various folders available as a part of the SIM.

DCE 207 Project

As per university Guidelines