**INSTITUTE OF HUMAN RESOURCES DEVELOPMENT**
TC.86/1949(2), NH Bypass Junction, Chakka, Petta P.O, Thiruvananthapuram, Kerala, India. Pin-695 024
http://www.ihrd.ac.in

# POST GRADUATE DIPLOMA IN CYBER FORENSICS & SECURITY

(1 Year- Two Semesters)

## Scheme & Syllabus

## 2024

(Effective from January 2024 admission)

**Institute of Human Resources Development**
*(Established by the Govt. of Kerala)*

# Post Graduate Diploma in Cyber Forensics & Security

*(1 Year- Two Semesters)*

## Subjects of Study and Scheme of Assessment

## (Scheme-2024)

## Semester 1

| Code | Subject | No. of Hrs/ week | | Minimum Marks | | | Maximum marks | | |
|---|---|---|---|---|---|---|---|---|---|
| | | T | P | W/P | CE | Total | W/P | CE | Total |
| PGDCF101 | Cyber Forensics and Incident Response | 4 | - | 30 | 10 | 50 | 75 | 25 | 100 |
| PGDCF102 | OS and File System Forensics | 4 | - | 30 | 10 | 50 | 75 | 25 | 100 |
| PGDCF103 | Ethical Hacking & Network Security | 4 | - | 30 | 10 | 50 | 75 | 25 | 100 |
| PGDCF104 | Cyber Forensics Lab** | - | 3 | 30 | 10 | 50 | 75 | 25 | 100 |
| PGDCF105 | Ethical Hacking Lab*** | - | 3 | 30 | 10 | 50 | 75 | 25 | 100 |
| Total Duration : 225 Hrs | | 12 | 6 | Total marks: | | | 375 | 125 | 500 |

* *T- Theory P – Practical W – Written CE–Continuous Evaluation T – Total*

** ***PGDCF104****- Experiments to be carried out based on* ***NSDC*** *Qualification Packs- Forensic Specialist (SSC/Q0922) with the help of a Skill Knowledge provider(SKP)/Training Partner of NSDC*

*** ***PGDCF105****- Experiments to be carried out based on* ***NSDC*** *Qualification Packs- Penetration Tester (SSC/Q0912) with the help of a Skill Knowledge provider(SKP)/ Training Partner of NSDC*

# Subjects of Study and Scheme of Assessment

## (Scheme-2024)

## Semester 2

| Code | Subject | No. of Hrs/ week | | Minimum Marks | | | Maximum marks | | |
|---|---|---|---|---|---|---|---|---|---|
| | | T | P | W/P | CE | Total | W/P | CE | Total |
| PGDCF201 | Malware Analysis using ML and Deep Learning | 4 | - | 30 | 10 | 50 | 75 | 25 | 100 |
| PGDCF202 | Project Work & Internship | - | 16 | 100 | 100 | 200 | 200 | 200 | 400 |
| PGDCF203 | MOOC Course & Certification | - | 10 | To be completed successfully | | | | | |
| Total Duration : 225 Hrs | | 4 | 26 | Total marks: | | | 275 | 225 | 500 |

** T- Theory P – Practical W – Written CE–Continuous Evaluation T – Total*

*[Scheme-2024]*

# PGDCF101 Cyber Forensics and Incident Response

(Duration: 45 Hours)

***Objectives:***

*1. To understand about Computer Forensics and the procedures for investigations and incident response*
*2. To study about data acquisition and to have an understanding of different forensic acquisition tools*
*3. To explore the various cyber threats, attacks and the different anti forensic techniques*
*4. The theory behind Network Forensics, Mobile Forensics and various types of Forensics*

**Module 1.Computer Forensics-Introduction**

Computer Forensics: History of computer forensics, developing computer forensics resources, preparing for computer investigations, understanding law enforcement agency investigations and corporate investigations, maintaining professional conduct Understanding Computer Investigations -Preparing a computer investigation, taking a systematic approach, procedures for corporate high tech investigations, conducting an investigation, completing the case, determining the physical requirements for a CF lab, Incident Response-Stages of incident Response, IR tools (9 Hrs)

**Module 2.Data Acquisition**

Data Acquisition - storage formats for digital evidence, determining the best acquisition method, contingency planning for image acquisitions, using acquisition tools, validating data acquisitions, using remote network acquisition tools, using other forensic acquisition tools, Identifying digital evidence, collecting evidence in private sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene. Seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash.

(9 Hrs)

**Module 3.Data Analysis and Validation**

Analysis and validation -determining what data to collect and analyse, validating forensic data, addressing data -hiding techniques, performing remote acquisitions. Recovering Graphics Files-Recognizing, locating and recovering graphic files, understanding data compression, copy rights issues with graphics, identifying unknown file formats,. (9 Hrs)

**Module 4. Cyber Security**

Cybercrimes, Types of Cybercrimes , Cyber Security Steps taken to protect ICT and prevent Misuse of Internet**-** IT Act 2000**-** Social Cyber Media, –IT Rules 2021-Cyber-attacks -Frameworks-Mitre Frame work, Anti forensics techniques and tools- Case studies, Cryptocurrency. (10 Hrs)

**Module 5. Types of Forensics**

Network Forensics-overview, performing live acquisitions, developing standard procedures for network forensics, using network tools. Email Investigations-role of E-mail in investigations, exploring the roles of the client and server, investigating e-mail crimes and violations, understanding E-mail servers, specialized E-mail forensic tool (8 Hrs)

---

**Text Books:**


- Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Christofer Steuart , Second Indian Reprint 2009, Cengage Learning India Private Ltd.
- Niranjan Reddy, “Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations”, Apress, 2019
- Leighton R. Johnson III, ”Computer Incident Response and Forensics: Team Management Conducting a Successful Incident Response”, Syngress,2014


**Reference Books:**


- Digital Evidence and Computer Crime – Eoghan Casey, Edition 3, Academic Press, 2011
- Computer Forensics and Cyber Crime: An Introduction – MarjieBritz, Edition 2, Prentice Hall, 2008
- Practical guide to Computer Forensics- David Benton and Frank Grindstaff , Book Surge Publishing,2006
- Computer Evidence: Collection & Preservation- Christopher L.T Brown Charles River Media publishing, Edn 1, 05
- Computer Investigation (Forensics, the Science of crime-solving) – Elizabeth Bauchner, Mason Crest , 2005


*******

*[Scheme-2024]*

# PGDCF102 OS and File System Forensics

(Duration: 45 Hours)

**Objectives:**

*1. To understand the foundation of digital investigation and methods of data analysis*
*2. To understand and to familiarize the NTFS,ext2 and ext3 file systems*
*3. To familiarize the UFS1 and UFS2 concepts and to understand the different file s/m structures-Windows/Linux*
*4. To understand how data acquisition is done from a Windows and Linux System*
*5. To analyze windows memory and files including executable files*
*6. To have an overview on concepts implemented in modern operating systems.*

**Module 1.Digital investigation foundation**

Digital investigations and evidence,Digital crime scene investigation process, Data analysis, overview of toolkits, Computer foundations- Data organizations, booting process,Hard disk technology, Hard disk data acquisition- introduction, reading the source data, writing the output data

(9 Hours)

**Module 2.File System analysis-Windows**

What is a file system, exploring Microsoft file structures, examining NTFS disks, whole disk encryption, the windows registry, Microsoft and MS-DOS start up tasks, virtual machines, File system category, Content category, Metadata category, File name category, Application category, Application-level search techniques, Specific file systems, FAT concepts and analysis-, File recovery, determining type, Consistency check. FAT data structure-Boot sector, FAT 32 FS info, directory entries, Long file name directory entries. NTFS (10 Hours)

**Module 3.File System analysis-Linux and Android**

Examining UNIX and LINUX disk structures and boot processes. ext2, ext3 , UFS1, UFS2 file systems - concepts and analysis- File system category, Content category, Metadata category, File name category, File recovery, determining the type, Consistency check. ext2, ext3 data structures. Android File System-Flash memory, Architecture, NAND and NOR, Android Mobile File Systems, Data Organization, YAFFS2,F2FS ( 9 Hours)

**Module 4.Windows Forensic Analysis**

Live Response: Data Collection- Introduction , Locard's Exchange Principle, Order of Volatility ,When to Perform Live Response ,What Data to Collect- Volatile and Non Volatile Data Live-Response Methodologies: Data Analysis- Data Analysis, Agile Analysis, Windows Memory Analysis, Rootkits and Rootkit detection. ( 9 Hours)

**Module 5.Linux Forensics analysis**

Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image, Initial Triage and Live Response: Data Analysis- Log Analysis, Keyword Searches, User Activity, Network Connections, Running Processes, Open File Handlers, The Hacking Top Ten, Reconnaissance Tools (8 Hours)

---

**Text Books:**


- File System Forensic Analysis – Brian Carrier, Addison Wesley, 2005
- Digital Evidence and Computer Crime- Casey, Eoghan , edition 2, Academic Press, 2004.
- Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc. , 2008
- Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc. , 2009


**Reference Books:**


- Guide to Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Thomson Course Technology, 2004
- Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009


* * * * * * *

*[Scheme-2024]*

# PGDCF103 Ethical Hacking and Network Security

(Duration: 45 Hours)

**Objective**

*1. To understand the basics of Ethical Hacking,network and computer attacks*
*2. To study the various OS, Server and Desktop vulnerabilities*
*3. To impart a deeper understanding of network security,cyber security and information security principles and policies and wireless networking security issues and approaches.*

**Module 1.Introduction to Ethical Hacking**

Elements of Information Security, Authenticity and Non-Repudiation, Security Challenges, Effects of Hacking, Hacking Methodologies, Hacker – Types of Hacker, Ethical Hacker ,Role of Security and Penetration Testing, Penetration Testing Methodologies :– OSSTMM, NIST, OWASP, Categories of Penetration Test, Types of Penetration Tests, Vulnerability Assessment- Desktop and Server OS Vulnerabilities (8 Hours)

**Module 2. Foot Printing & Social Engineering**

Tools for Foot Printing, Conducting Competitive Intelligence, Google Hacking, DNS Zone Transfer Scanning, Enumeration, Trojans & Backdoors, Virus & Worms, Proxy & Packet Filtering, Denial of Service, Sniffer, Social Engineering and counter measures–shoulder surfing, Dumpster Diving, Tailgating, Piggybacking. Introduction to Port Scanning-Types of Port Scan-Port Scanning Tools (9 Hours)

**Module 3. Computer Networks and Network attacks**

Classful Internet Addresses- The original Classful Addressing Scheme, Dotted Decimal Notation-Subnetting& Classless Extensions, VLAN. Vulnerability Data Resources – Exploit Databases – Network Sniffing – Types of Sniffing – MITM Attacks – ARP Attacks – Denial of Service Attacks - Hijacking Session with MITM Attack -DNS Spoofing – ARP Spoofing Attack Manipulating the DNS Records – DHCP Spoofing -Remote Exploitation – Attacking Network Remote Services – Overview of Brute Force Attacks – Traditional Brute Force – Attacking SMTP – Attacking SQL Servers – Testing for Weak Authentication (10 Hours)

**Module 4.Network Protection System & Hacking Web servers**

Routers, Firewall & Honey pots, IDS &IPS, Web Filtering, Vulnerability, Session Hijacking, Web Server, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles Phone Hacking.

. (9 Hours)

**Module 5. Wireless Security**

VoIP, The Cellular phone network,Wireless transmission systems,Pervasive Wireless Data Network Technologies, IEEE Wireless LAN specification,War driving,War chalking,War Flying, Wi-Fi Security Recommendations,Bluetooth,WAP (9 Hours)

---

**Text books:**


- Hands on ethical hacking and network defense by Michael T Simpson, Kent Backman, James Corley, Cengage Learning, 2 edition,2010.
- Ed Skoudis and Tom Liston, "Counter Hack Reloaded: A step-by-step guide to computer attacks and effective defenses", Prentice Hall Series in Computer Networking and security, 2nd edition, 2006.
- Rafay Baloch, "Ethical Hacking and Penetration Testing Guide", CRC Press, 2014.
- The Basics of Hacking and Penetration testing - Patrick Engebretson, Syngressedn. 01,2011.
- NoTech Hacking: A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing by Johnny Long,Syngress publishers,1st edition,2008.
- Hacking:The Art of Exploitation,2nd Edition by Jon Erickson,William Pollock publishers,2008.
- Network Security Bible-Eric Cole,RonaldKrutz,James W Conley,Edition 2, Wiley India Pvt Ltd,2010.
- Network Security Essentials- William Stallings, Edition 4,Pearson Education,2011.


* * * * * * *

*[Scheme-2024]*

## PGDCF104 Cyber Forensics Lab
## (Based on NSDC Qualification Pack- Forensic Specialist (SSC/Q0922))

(Duration: 45 Hours)

Various types of forensics analysis include:

- dynamic analysis to boot an image of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it
- file signature analysis
- file system forensic analysis
- hash comparison against established database
- live forensic analysis (e.g., using Helix in conjunction with Live View or Pro Discover Basic)
- timeline analysis
- static media analysis
- static analysis to mount an "image" of a drive (without necessarily having the original drive)
- static malware analysis
- tier 1, 2, and 3 malware analysis
- cursory binary analysis

* * * * * * *

*[Scheme-2024]*

## PGDCF105 Ethical Hacking Lab
## (Based on NSDC Qualification Pack- Penetration Tester (SSC/Q0912))

(Duration: 45 Hours)

- Identify and analyze exposures and weaknesses in applications and their deployments
- Various testing methods for testing applications-
- configuration and deployment management testing
- enumerate all the roles that can be provisioned and explore the permissions that are allowed to be applied to the objects including any constraints
- identity management testing
- authentication testing
- authorization testing
- session management testing
- input validation testing
- business logic testing
- client side testing

* * * * * * *

*[Scheme-2024]*

# PGDCF201 Malware Analysis using ML and Deep Learning

(Duration: 45 Hours)

**Objectives:**

*1. To understand the different ML and Deep learning methods*
*2. To find the malware artifacts from a live Windows and Linux system*
*3. To analyze the suspect files affected by malwares*
*4. To learn how to extract the malware artifacts*

**Module 1. Introduction to Machine Learning**

Distinction between traditional programming and machine learning. Types of Machine Learning- Supervised Learning: Prediction and regression, Unsupervised Learning: Clustering and dimensionality reduction,Reinforcement Learning: Decision-making and autonomous systems. ML Algorithms: -Overview of popular algorithms such as linear regression, decision trees, k-nearest neighbors, and neural networks. (9 Hours)

**Module 2. Deep Learning Concepts**

Understanding Neural Networks, Deep Neural Networks:neural networks and the advantages of deep architectures, The vanishing gradient problem and its implications.Convolutional Neural Networks (CNNs):- Convolutional layers, pooling layers, and their role in feature extraction. Recurrent Neural Networks (RNNs) -Sequential data processing using RNNs - Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) cells. Transfer Learning, Generative Models: - Introduction to generative adversarial networks (GANs) and variational auto encoders (VAEs).Ethical Considerations in Deep Learning (9 Hours)

**Module 3. Malwares**

Introduction to malware, evolution of malware, malware types - viruses,worms, rootkits,Trojans,bots, spyware, adware,logic bombs. Types of malware Analysis – Static Analysis, Dynamic Analysis, Malware Analysis Tools - Static Analysis Tools, Dynamic Analysis Tools. Antivirus Scanning, Fingerprint for Malware. (8 Hours)

**Module 4. Malware Incident Response & Post Mortem Forensics**

Volatile Data Collection and Examination on a Live Windows System, Non-volatile Data collection from a live Windows system, Forensic preservation of Select Data on a Live Windows System, Incident Response Tool Suites for Windows. Post mortem Forensics: Discovering and Extracting Malware and Associated Artifacts from Windows Systems, Forensic Examinations of Compromised Windows, Functional Analysis Resuscitating a Windows Computer, Malware Discovery and Extraction from a Windows System (10 Hours)

**Module 5.File Identification,Profiling and Analysis**

Initial Analysis of a suspect file on a Windows -Overview of the File Profiling process, Working with Executables, File similarity indexing, File signature identification and classification, Embedded artifact extraction, File Obfuscation, ELF file Structure. Guidelines for Examining a Malicious Executable Program, Establishing the Environment Baseline, Pre-execution Preparation, Exploring and verifying specimen functionality and purpose (9 Hours)

---

**Text Books:**


- Malware Forensics Investigating and Analyzing Malicious code-James M. Aquilina, Eoghan Casey, Cameron H. Malin, Syngress Publishing, 2008
- Malware Analyst's Cookbook Tools and Techniques for fighting malicious code- Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley Publishing Inc., 2011
- Malware Analysis Using Artificial Intelligence and Deep Learning Mark Stamp • Mamoun Alazab • Andrii Shalaginov Editors Springer


**Reference Books:**


- Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos
- Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc.,2007
- Windows Forensic Analysis- Harlan Carvey, Dave Kleiman, Syngress Inc., 2007
- File System Forensic Analysis- Brian Carrier, Addison Wesley, edition 1, 2005 *[Scheme-2024]*

## PGDCF 202 Project Work & Internship

(Duration: 150 Hours)

### Course Description

The students can select Cyber Forensics/Security projects. The project can be implemented using suitable CF tools which students have studied and used during the course. A total product or project can be selected. The topics also includes Threat Surface Analysis, Penetration Testing, Vulnerability analysis etc

A Project Evaluation & viva-voce will be conducted along with practical examination for Terminal evaluation of the Project work.

Internship of minimum 2 weeks duration at any Cyber Forensics/Security based Industry/establishments shall be provided.

## PGDCF 203 MOOC Course and Certification

(Duration: 30 Hours)

MOOC Courses and certifications programmes related to Cyber Security /Forensics/Ethical Hacking provided through online platforms by NPTEL/Swayam/ Coursera/Google/IBM/ECCouncil etc to be completed successfully.

* * * * * * *

.

*[Scheme-2024]*

# Post Graduate Diploma in Cyber Forensics and Security

## 1. Question paper pattern

**Duration of Exam. : 3 Hrs.** **Maximum marks:75**

Part - A Short Answer type Questions with answer size up to 1 page per question. 5 Marks each.
Part - BDescriptive type Questions with answer size up to 2 to 3 pages per question. 15 marks each.

**Marks Distribution**

| Part | No. of questions | Need to be answered | Marks/Question | Total |
|---|---|---|---|---|
| A | 5 | 5 | 5 | 25 |
| B | 10 | 5 | 10 | 50 |
| Total | | | | 75 |

**Guidelines for Question paper setters:**

1. In Part A, 5 questions, one short answer question from each module.
In Part B, 10 questions, two questions from each module. Students have choice to opt any one of the two questions from each module. In part B, each question can be have sub divisions, but total mark per questions is 10 marks.
2. The level of difficulty shall be as follows
   i) Easy Questions : 30% -40%
   ii) Intermediate level to difficult: 30% -40%
   iii) Difficult questions: 20% -30%
3. The question paper setters must prepare and submit the question papers as per the following guidelines.
   i) Question paper must be designed and prepared to fit in an A4 size paper with one inch margin on all four sides.
   ii) Prepare the Question in MS-Word/Open office-Writer document format. Use only "TimesNewRoman" font with size 10. Align text to both left and right margins.
   iii) Please leave 5 cm. free area at the top of the front page of each question paper to place examination details/Question paper header by the examination department.
   iv) Avoid placing 1 or 2 questions in the last part in a fresh page, unless it is absolutely necessary. In such case, try to accommodate above questions in the previous page(s) by adjusting top/bottom margins and line spacing, if possible. This will reduce printing expenses.
   v) Specify marks for each question/part clearly.
   vi) Clearly specify the number of questions to be answered for each Part.
   vii) Confirm that no questions in part A is repeated in Part B also.
   viii) Avoid repeating questions in Part B from the immediate previous examination.
   ix) Key for evaluation must be prepared and enclosed in a separate cover and should be submitted along with the question paper set. Key for evaluation must specify evaluation guidelines for each part in the question paper, otherwise the key prepared will be treated as incomplete and will be rejected.
   x) Submit Question paper in Laser print out form only. Hand written and printed in poor quality printers is not acceptable.

**********

*[Scheme 2024]*

## Post Graduate Diploma in Cyber Forensics and Security

### 2. Scheme for Continuous Evaluation.

1. For Theory Papers: Weightage

a). Average of minimum Two test papers : 30%
b). Average of minimum Two Assignments : 30%
c). Score for Seminar : 20%
d). Score for Class Attendance. : 10%
e). Overall performance in the class. : 10%

2. For Practical Papers: Weightage

a). Average of minimum Two Lab tests : 30%
b). Average of minimum Two Lab Assignments : 30%
c). Maintenance of Lab record : 20%
d). Score for Lab Attendance. : 10%
e). Overall performance in the Lab. : 10%

3. Teachers shall submit Mark list for Continuous Evaluation to the Head of Institution in the following format.

Subject code: Subject name:

| Sl No. | Regno | Name | a.Test | b.Assignment | c.Seminar | d.Attendance | e.performance | Total |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

4. Head of Institution/Co-ordinator shall forward Continuous evaluation marks to the Examination Section of IHRD in the following format only.

Centre code: Centre Name:

| Sl No. | Regno | Name | PGDCF101 25 | PGDCF102 25 | PGDCF103 25 | PGDCF104 25 | PGDCF105 25 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

5. Continuous evaluation(CE) marks must be published in the notice board at least one week before the commencement of theory examinations after getting approval from the Head of Institution/Co-ordinator.

* * * * * * *

Thiruvananthapuram
16.02.2024

Sd/-
Director