

PG Diploma in Digital Forensic Syllabus

ELIGIBILITY:-

Masters/Graduate – Any science background (Maths / Computer science or application / Chemistry / Physics

BCA, BSc, MSc (Computer science, Cyber Security, Data Science, BTech IT or CSE), LAW, Forensic Science)

DURATION OF COURSE:-

12 Month

COURSE CONTENT:-

Module1 : Python & Hacking tools

Module2 : Networking

Module 3 : Ethical Hacking

Module 4 : Computer Forensic

Module 5 : Mobile Forensic

Module 6 : Project

SL.NO	MODULE TITLE	THEORYHOURS	PRACTICALHOURS (If Applicable)	TOTAL HOURS
Module 1	Python & Hacking tools	20 hours	20 hours	40 hours
Module 2	Networking	20 hours	20 hours	40 hours
Module 3	Ethical Hacking	20 hours	20 hours	40 hours
Module 4	Computer Forensic	20 hours	20 hours	40 hours
Module 5	Mobile Forensic	20 hours	20 hours	40 hours
Module 6	Project	0 hours	40 hours	40 hours
TOTAL HOURS - 240 IN HOURS Total theory hours –100HRS Total Practical Hours-140HRS				

MODULE NUMBER 1: Python & Hacking tools (40Hours)	
THEORY (20 Hours)	
1. Installing Python on Linux and another Operating Systems & Introduction	4 Hrs
2. Using quotes and escape character,String Concatenation and Repeater Operators	2 Hrs
3. Using Mathematical Operators with Numbers,len() with Lists	2 Hrs
4. Deleting List Element, Common list and operations, Accessing Dictionary values	2 Hrs
5.Adding, Replacing and Deleting key-value pairs, Functions: get(), keys(), values() and items()	2 Hrs
6. Using for Loops,Using Sequence Operators and Functions with Strings	4 Hrs
7. Indexing and Slicing Strings,Handling Exceptions	4 Hrs
PRACTICAL (20 Hours)	
8. Lambda Function (filter(), map()),Functions: Recursive function	5 Hrs
9. Importing Modules,Writing Modules	5 Hrs
10. Using Modules in Programs, The open Function, Input from Text Files.	10 Hrs
LEARNING OUTCOME	
<p>1.The course is designed to provide Basic knowledge of Python. Python programming is intended for software engineers, system analysts, program managers and user support personnel who wish to learn the Python programming language. Learning Outcomes: Problem solving and programming capability.</p> <p>2. Understand what a comprehension is and the conditions for use. Translate a loop into a comprehension. Executed nested comprehensions. Integrate comprehensions with a data structure.</p> <p>3.To acquire programming skills in core Python. To acquire Object Oriented Skills in Python To develop the skill of designing Graphical user Interfaces in Python To develop the ability to write database applications in Python</p> <p>4. Through a series of hands-on exercises, students will learn to turn data into actionable information. The world is drowning in data. Each day 2.5 Exabytes of data (250 new Library of Congresses built or 90 years of HD video) is produced. The problem is getting the data into a format which can be used by tools that help in understanding and verifying the data. Python programming is relatively quick to learn and has a great set of tools for importing, transforming, exploring, extracting insights from, making predictions with, and exporting the data. This course introduces the major Python tools used for preparing the data for analysis, the tools available for understanding the data, and using the data for insights and predictions. All class work and exercises are done in Python 3.x.</p> <p>5. To learn how to design and program Python applications. To learn how to use lists, tuples, and dictionaries in Python programs. To learn how to identify Python object types. To learn how to use indexing and slicing to access data in Python programs.</p> <p>6.Its language constructs as well as its object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects. ... It supports multiple programming paradigms, including structured (particularly, procedural), object-oriented and functional programming.</p>	

Reference Books:

1. Python Crash Course (Author: Eric Matthes)
2. Learning Python (Author: Mark Lutz)
3. Python Tricks: A Buffet of Awesome Python Features (Author: Dan Bade)
4. Learn Python the Hard Way (Author: Zed Shaw)
5. Automating Boring Stuff with Python (Author: Al Sweigart)
6. Python for Data Analysis (Author: Wes McKinney)

MODULE NUMBER 2 - Networking (40Hours)	
THEORY (20 Hours)	
1. LAN, MAN, WAN, Topology, Bits, Bytes and Octets	4 Hrs
2. What is Packet Tracer? & Packet Tracer Installation	4 Hrs
3. Introduction to IP and MAC Address, Use of IP and MAC Address	2 Hrs
4. IPv4(Classful Addressing), Public IP Private IP, Loopback Address and APIPA	2 Hrs
5. Default Subnet Mask, Calculate FLSM for Class C Address	2 Hrs
6. Calculate VLSM for 4-6 Network Requirement with variable Host, Brief explanation for TCP Header	2 Hrs
7. Comparison between OSI and TCP/IP Model, DHCP Configuration using 4pcs (Classful & Classless)	4 Hrs
PRACTICAL (20 Hours)	
8. Configure DHCP Snooping with 2 Servers (DHCP Configured inside) and 4 PCs, Configure Port Security (Restrict, Protect, Shutdown Mode) (Sticky, Dynamic MAC Address, Maximum Address)	10 Hrs
9. Explain Different WAN Technologies (Leased Line, Circuit Switching, Packet Switching), Explain and Configure different Point to Point Link Sencapsulation technology (HDLC, PPP --> PAP, CHAP)	5 Hrs
10. Explain AAA and the working, Discuss the differences between TACACS+ and RADIUS	5 Hrs
LEARNING OUTCOME	
1. Build multiple host and network architectures, given business requirements and constraints; student will configure operating systems, network specific services, routing, switching, and remote access solutions	
2. The main emphasis of this course is on the organization and management of local area networks (LANs). The course objectives include learning about computer network organization and implementation, obtaining a theoretical understanding of data communication and computer networks, and gaining practical experience in installation, monitoring, and troubleshooting of current LAN systems. The course introduces computer.	
3. Gain more knowledge. Networking is a great opportunity to exchange best practice knowledge, learn about the business techniques of your peers and stay abreast of the latest industry developments. A wide network of informed, interconnected contacts means broader access to new and valuable information.	
4. Network Analysis has become a widely adopted approach for studying the interactions between agents, information and infrastructures. The strong demand for comprehensive expertise and skills in. Network analysis has been fueled by the widespread acknowledgement that everything is connected, the popularity of social networking services, and advances in computational solutions for collecting, visualizing and analyzing network data.	

5. This interdisciplinary course introduces students to fundamental theories, concepts, methods and applications of network analysis. We will focus on social, socio-technical and information networks. Students learn how to approach network analysis in an informed, systematic and analytically rigorous fashion. At the end of the course, students will be able to design, manage and execute network analysis projects for scholarly and commercial use, and to critically assess network studies.

6. Demonstrate ability to select and apply a network analysis method (qualitative, quantitative, metrics, etc.) that is appropriate and feasible given the research question, dataset and scope of the project.

Reference Books:

1. Network Programmability and Automation.
2. Computer Networking: A Top-Down Approach.
3. Computer Networks.
4. Network Warrior.
5. Networking All-in-One for Dummies.
6. Cisco Networking All-in-One for Dummies.

MODULE NUMBER 3 – Ethical Hacking (40 Hours)	
THEORY (20 Hours)	
1. Brush up Linux (Optional), Brush up networking (Optional), What are the different types of hackers.	4 Hrs
2. Information Gathering, Scanning.	4 Hrs
3. System Hacking, System Hacking (Cont.), Reverse connection in different network using port forwarding.	2 Hrs
4. Show software-based vulnerabilities (Badblue/iceblaster), Explain LDAP	2 Hrs
5. Explain how Kerberos works (Authentication Server, Ticket Granting Server, TGT etc.)	2 Hrs
6. Malware (Different types of Malware, Virus and Trojan)	2 Hrs
7. Man In the Middle Attack using the concept of ARP poisoning, Steganography.	4 Hrs
PRACTICAL (20 Hours)	
8. Wireless Attacks, Website Attacks, Prevention	5 Hrs
9. Explain different kinds of sql injection attacks, explain cookie stealing, session hijacking.	5 Hrs
10. File upload vulnerability, Phishing Attack, DOS and DDOS attacks, Cloud based attacks	10 Hrs

LEARNING OUTCOME

1. Plan a vulnerability assessment and penetration test for a network. Execute a penetration test using standard hacking tools in an ethical manner. Report on the strengths and vulnerabilities of the tested network. Identify legal and ethical issues related to vulnerability and penetration testing.
2. The Certified Ethical Hacker salary in India for freshers starts from ₹3.5 LPA. If you break it down, the average salary of an Ethical Hacker in India turns out to be between ₹29k and ₹41k per month.
3. There is no shortage of ethical hacking jobs in India. As per the 2019/2020 Official Annual Cybersecurity jobs report, the demand for information security personnel will lead to an estimated 3.5 million unfilled jobs being created globally by 2021. The industry will witness a 350% growth by 2021.
4. The CBS article mentioned other major companies, including Square and Google, that also enlist professional hackers' help. Even Apple, whose products are famous for their resistance to viruses, has hired hackers.
5. Employment: The most basic way to make money hacking computers is to work for a company as a penetration tester. ... In return for the hacker disclosing what they found the company gives out a cash reward. Several companies such as Facebook, Intel, Snapchat, Cisco, Dropbox and Apple have bug bounty programs.
6. Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Reference Books:

- 1) Hacking: The Art of Exploitation.
- 2) The Basics of Hacking and Penetration Testing.
- 3) The Hacker Playbook 2: Practical Guide to Penetration Testing.
- 4) Penetration Testing – A Hands-On Introduction to Hacking.
- 5) The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
- 6) Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security

MODULE NUMBER 4 –Computer Forensic (40 Hours)**THEORY (20 Hours)**

1. Computer Forensics in Today's World	4 Hrs
2. Computer Forensics Investigation Process	4 Hrs
3. Understanding Hard Disks and File Systems	2 Hrs
4. Data Acquisition and Duplication	2 Hrs
5. Defeating Anti-Forensics Techniques	2 Hrs
6. Windows Forensics	2 Hrs
7. Linux and Mac Forensics	4 Hrs
PRACTICAL (20 Hours)	
8. Linux and Mac Forensics	5 Hrs
9. Linux and Mac Forensics	5 Hrs

10. Computer Forensics Investigation Process	10 Hrs
<p>LEARNING OUTCOME</p> <p>1. Workforce demand for Computer Hacking Forensic Investigators is on an all-time high across multiple work options; major industries for CHFI hiring include law enforcement, military and defense, enterprise IT, insurance and banking, legal practices, and of course cyber security firms.</p> <p>2. The Certified Ethical Hacker salary in India for freshers starts from ₹3.5 LPA. If you break it down, the average salary of an Ethical Hacker in India turns out to be between ₹29k and ₹41k per month.</p> <p>3. From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.</p> <p>4. This paper proposes a detailed guideline model for digital forensics; the proposed model consists of five main phases, Preparation phase, Physical Forensics and Investigation Phase, Digital Forensics Phase, Reporting and Presentation Phase, and Closure Phase.</p> <p>5. Computer forensics can be a stressful field, as you often need to find information quickly for a criminal investigation and criminals can be highly skilled at technology. On the other hand, a computer forensics career is in a top growing field that has many diverse employment opportunities.</p> <p>6. Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts.</p>	

Reference Books:

1. Fraud, Kenneth C. Brancik, Insider Computer, Edition 2008, Auerbach Publications Taylor & Francis Group.
2. William Oettinger, Learn Computer Forensics: A Beginner's Guide to Searching, Analyzing, and Securing Digital Evidence, Edition 2020, Packet Publishing.
3. Gerard Johansen, Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, Second Edition, Packet Publishing.
4. Joakim Kävrestad, Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, Edition 2018, Springer publications.
5. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, Second Edition, Springer, 2014.

MODULE NUMBER 5 -Mobile Forensic (40 Hours)	
THEORY (20 Hours)	
1. Network Forensics	4 Hrs
2. Investigating Web Attacks	4 Hrs
3. Mobile Data Recovery	2 Hrs
4. Dark Web Forensics	2 Hrs
5. Database Forensics	2 Hrs

6. Cloud Forensics	2 Hrs
7. Investigating Email Crimes	4Hrs
PRACTICAL (20 Hours)	
8. Mobile Data Recovery, IoT Forensics	5 Hrs
9. Dark Web Forensics	5 Hrs
10. Investigating Email Crimes, Malware Forensics	10 Hrs
<p>LEARNING OUTCOME</p> <p>1. Workforce demand for Computer Hacking Forensic Investigators is on an all-time high across multiple work options; major industries for CHFI hiring include law enforcement, military and defense, enterprise IT, insurance and banking, legal practices, and of course cyber security firms.</p> <p>2. The Certified Ethical Hacker salary in India for freshers starts from ₹3.5 LPA. If you break it down, the average salary of an Ethical Hacker in India turns out to be between ₹29k and ₹41k per month.</p> <p>3. From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.</p> <p>4. This paper proposes a detailed guideline model for digital forensics; the proposed model consists of five main phases, Preparation phase, Physical Forensics and Investigation Phase, Digital Forensics Phase, Reporting and Presentation Phase, and Closure Phase.</p> <p>5. Computer forensics can be a stressful field, as you often need to find information quickly for a criminal investigation and criminals can be highly skilled at technology. On the other hand, a computer forensics career is in a top growing field that has many diverse employment opportunities.</p> <p>6. Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts.</p>	

Reference Books:

1. John R. Vacca, Charles River Media, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, 2005
2. Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 2010, Second Edition, Springer's.
3. Ali Jahangiri, Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, First edition, 2009
4. Barkhs and U. Rama Mohan, Cyber Law Crimes, Third Edition, 2017, Asia Law House
5. Viveek Sood, Cyber Laws Simplified, Fourth reprint 2008, McGraw Hill.
6. M. Merkow, & J. Breithaupt, Information security: Principles and practices, Second Edition, 2006, Upper Saddle River, NJ: Prentice Hall

MODULE NUMBER 6 – Project (40 Hours)	
THEORY (0 Hours)	NA
1. NA	Hrs

2. NA	Hrs
3. NA	Hrs
4. NA	Hrs
5. NA	Hrs
6.NA	Hrs
7.NA	Hrs
PRACTICAL (40 Hours)	
8. Report Writing	10 Hrs
9. Industrial training internship for Digital forensic investigation	10 Hrs
10. Client site visit for data recovery work	20 Hrs