

Savitribai Phule Pune University (Formerly University of Pune)



**Board of Studies, Department of Technology
Electronics & Electrical (EE) Technology
Curriculum Structure for
Professional Certification Programme in Cyber Crime Investigator**

Course Name: Professional Certification Programme in Cyber Crime Investigator

Compulsory Modules – 12

Duration: 260 Hours (6 Months)

Course Intake: - 30

Course Mode: - Class Room (Hybrid)

Eligibility Criteria: Graduate from Any Discipline.

Students in penultimate year of graduation or pursuing graduation in any field can also apply.

Working professionals & law enforcement personnel.

Course Contents-

Sr. No.	Subject Code	Subject Name	Credits	Teaching Scheme (Theory)	Teaching Scheme (Practical)
1	CPCCI1	Computer & Internet Fundamentals	2	√	√
2	CPCCI2	Understanding the Internet & Network	2	√	
3	CPCCI3	(a)Fundamentals of Cyber Crime, Cyber Security & Hacker Methodologies & (b) Acquisition & Investigation of Digital Evidence	2	√	√
4	CPCCI4	Cyber Forensics & Cyber Crime Investigation	2	√	√
5	CPCCI5	Ethical Wireless Hacking	2	√	
6	CPCCI6	Encryptions & Cryptography	2	√	
7	CPCCI7	Dark Web the Complete Understanding	2	√	
8	CPCCI8	Cyber Terrorism in Indian Subcontinent	2	√	
9	CPCCI9	Cyber Crime & Social Media	2	√	
10	CPCCI10	(a) Online Extremism & Hate Crime & (b) Forensic Science & Criminology	2	√	
11	CPCCI11	Cyber Laws	2	√	
12	CPCCI12	Final Independent Research Project (Dissertation Submission)	6		
		Total Course Credits	28		

TAKE AWAY'S AFTER COMPLETION OF (CCI) COURSE

Students develop a thorough detail understanding of how the Cyber world works. They get to know all the important aspects of this virtual world & how to secure the digital environment. After completion of the course students are able to conduct Cyber Crime Investigations, they can take up jobs offering various roles in the

Cyber Security arena specially with the law enforcement units handling Cyber Security or working within IT industry offering different Cyber Security job roles or in roles protecting Critical National Infrastructure. Students also gain complete knowledge of digital forensics & how it is conducted using various tools. Students also learn how to present this valuable piece of critical evidence in the court of law.

CPCCI1 Computer & Internet Fundamentals

Learning Outcomes

Students will have in-depth knowledge of computers, its components, systems & devices. They will also learn how World Wide Web works & performs all its actions.

Syllabus

The Basics, Internal Components, External Components, System Care and Troubleshooting

Reference:

1. PC Hardware: A Beginner's Guide RON GILSTER
2. The Step-by-step Guide to Understanding Computers By Kevin Wilson
3. COMPUTER ARCHITECTURE : FUNDAMENTALS AND PRINCIPLES OF COMPUTER DESIGN, SECOND EDITION by Joseph D. Dumas II
4. Principles of Computer Hardware by Clements
5. Introduction Computer Hardware Data Comm by Goupille (Author)

CPCCI2 Understanding the Internet & Network

Learning Outcomes

Students will understand the broad concept of internet all of its terminologies, topologies, protocols & functioning. They will also gain knowledge about networking & its significance in real world.

Syllabus

Connecting to the Internet, Exchanging E-mail, Chatting and Conferencing on the Internet, Viewing the World Wide Web, Creating and Maintaining Web Sites, File Transfer and Downloading, Other Internet Topics.

Reference:

1. Internet: The Complete Reference, Millennium Edition Margaret Levine Young
2. The Internet Complete Reference by Harley Hahn
3. Fundamentals of The Internet And The World Wide Web Ellen Hepp Reaymond Green
law
4. Internet And World Wide Web Simplified by Maran Graphics
5. Internet & World Wide Web: How to Program: International Edition 5th Edition, by Harvey M. Deitel (Author), Paul Deitel (Author), Abbey Deitel (Author)
6. Complete Book of the Internet and World Wide Web (Usborne Computer Guides) by Philippa Wingate (Author), Asha Kalbag (Author), Andy Griffin (Author)

CPCCI3 (a) Fundamentals of Cyber Crime, Cyber Security & Hacker Methodologies

Learning Outcomes

Students will develop complete understanding about cybercrimes. Various types, terminologies & methods of cybercrimes. How it all functions & propagate along the internet.

Syllabus

Understanding How Hackers & Cyber Criminals work, Web Hacking, E-Mail Hacking, Spoofing Attacks, Computer Worms & Computer Trojans, Computer Viruses.

Reference:

1. Mastering Information Security Acquisition & Investigation of Digital Evidence Essential Guide for CCI, CERT, DFIR, CSA, CSE By Transcendental Technologies
2. Cyber Crimes and Cyber Security (GTU)
3. Introduction to Cyber Security : Guide to the World of Cyber Security by Anand Shinde
4. Beginners Guide To Ethical Hacking and Cyber Security by Abhinav Ojha

CPCCI3 (b) Acquisition & Investigation of Digital Evidence

Learning Outcomes

Students will learn in detail about cyber security incidence breaches. How to investigate cyber-crimes & ways to prevent security breaches. Students develop a complete understanding of how to prevent, detect, investigate & report incidences & security breaches.

Syllabus

Introduction, Understanding Networks, Foot-printing & Reconnaissance, Google Hacking, Scanning, System Hacking, Android & I-phone Hacking, Malwares, SQL Injection, Cross Site Scripting, Sniffing, Social Engineering, Identity Theft Fraud, DoS, Session Hijacking, Penetration Testing, Exploit Writing & Buffer Overflow, Cryptography & Steganography, Firewall & Honeypots, IDS & IPS, Hacking Web Server, Wireless Hacking, Physical Security, Reverse Engineering, E-Mail Hacking, Security, Compliance & Auditing, Incident Handling & Counter Majors.

Reference:

1. Mastering Information Security Acquisition & Investigation of Digital Evidence Essential Guide for CCI , CERT, DFIR, CSA, CSE By Transcendental Technologies
2. ASCL Cyber Crime Investigation Manual
3. Blackstone's Handbook of Cyber Crime Investigation by Andrew Staniforth (Author), Police National Legal Database (PNLD) (Author), Professor Babak Akhgar (Author), Francesca Bosco (Author)
4. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors by Anthony Reyes (Author), Richard Britton (Author), Kevin O'Shea (Author), James Steele (Author)
5. Cyber Crime Investigator's Field Guide by Bruce Middleton (Author)
6. Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition By Albert Marcella, Jr., Doug Menendez

CPCC14 Cyber Forensics & Cyber Crime Investigation

Learning Outcomes

Students develop a thorough understanding of how to collect & present digital forensic evidence. They learn various tools & software's used to conduct Digital forensics & how to present the same in the court of law .

Syllabus

Introduction, Computer Forensics, Forensic Examination of Digital Evidence, Internet Fraud, Memory Forensics.

Reference:

1. Cyber Forensics & Cyber Crime Investigation By Transcendental Technologies
2. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes by Albert Marcella Jr. (Editor), Robert S. Greenfield (Editor)
3. Cyber and Digital Forensic Investigations: A Law Enforcement Practitioner's Perspective: 74 (Studies in Big Data) by Kim-Kwang Raymond Choo (Editor), Nhien-An Le-Khac (Editor)
4. Digital Forensics and Cyber Crime by Daryl Johnson (Editor), Makan Pourzandi (Editor), Pavel Gladyshev (Editor), Sanjay Goel (Editor), Suryadipta Majumdar (Editor)
5. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives (Advances in Digital Crime, Forensics, and Cyber Terrorism) by Raghu Santanam

CPCCI5 Ethical Wireless Hacking

Learning Outcomes

Students learn about the Wi-Fi networks & how to secure & protect them from being hacked. They develop a complete understanding of how securing & protecting networks from attacks & build strategies to protect networks.

Syllabus

Introduction, WI-Fi Hacking, How is Wireless Network Secured?, Understanding the Hacking System, Hardware Requirements, Attacking the Network, Attacking the WPA Protected Network, Bridging the Airgap, Cracking.

Reference:

1. Ethical Wireless Hacking By Transcendental Technologies
2. Hacking Wireless Networks for Dummies by Kevin Beaver (Author), Peter T. Davis (Author), Devin K. Akin (Foreword)
3. Hacking: Wireless Hacking: 3 by Alex Wagner (Author)

CPCCI6 Encryptions & Cryptography

Learning Outcomes

Students learn about encryption techniques & cryptography. They also learn about digital signatures & different Hash values

Syllabus

The Basics of Cryptography, Classic Cryptology, Modern Cryptology,P.G.P .

Reference:

1. Secret History The Story of Cryptology By Craig P. Bauer
2. Secret History: The Story of Cryptology (Chapman & Hall/CRC Cryptography and Network Security Series) by Craig Bauer (Author)
3. Real-World Cryptography by David Wong
4. Introduction to Modern Cryptography (2nd edition) Jonathan Katz and Yehuda Lindell
5. Introduction to Cryptography Sahadeo Padhye, Rajeev A. Sahu, Vishal Saraswat

CPCCI7 Dark Web the Complete Understanding

Learning Outcomes

Students will develop a complete understanding of how Dark web exists & operate on the World Wide Web. How illicit activities & organize crime & terrorists operate in the Dark Net. They will also develop skills to tackle the challenges & handle issues arising from dark web.

Syllabus

Introduction to Cyber Security & Dark Web, Threat landscape in Dark Net, Malicious Dark Net / TOR Network, Malware, Cyber criminal Activities in Dark Web, Evolution of the Web and its Hidden Data, Dark Web Content Analyzing Techniques, Extracting Information from Dark Web contents / LOGS, Dark Web Forensics, Open-Source Intelligence, Immerging trends in the Dark Web & Mitigation Techniques.

Reference:

1. Inside the Dark Web by Erdal Ozkaya (Author), Rafiqul Islam (Author)
2. The Dark Web... Mystery Untold Kindle Edition by Prakash Prasad
3. TOR: Access the Dark Net, Stay Anonymous Online and Escape NSA Spying (Darknet,Tor Browsing, Dark Web, Hacking Book 1) by Evan Lane (Author),
4. Dark Web Investigation (Security Informatics and Law Enforcement) by Babak Akhgar (Editor), Marco Gercke (Editor), Stefanos Vrochidis (Editor), Helen Gibson (Editor)

CPCCI8 Cyber Terrorism in Indian Subcontinent

Learning Outcomes

Students learn in detail about cyber terrorism, the concept & its use by various criminal organisations & terrorist groups across subcontinent. They develop an understanding about how it poses a significant threat & how to tackle the menace of cyber terrorism.

Syllabus

Definitional Issues Relating to Cyberterrorism, The Challenges Faced by International Organizations in Curbing Cyberterrorism, Application of Legal Provisions in the Case of Cyberterrorism, Issues of Enforcement in Cyberterrorism, Issues of Jurisdiction for Cyberterrorism, Conclusion and Recommendations.

Reference:

1. Cyberterrorism: The Legal and Enforcement Issues by PARDIS MOSLEMZADEH TEHRANI
2. Cyber Crime and Cyber Terrorism Investigator's Handbook by Babak Akhgar (Editor), Andrew Staniforth (Editor), Francesca Bosco Dr. (Editor)
3. New Threats and Countermeasures in Digital Crime and Cyber Terrorism (Advances in Digital Crime, Forensics, and Cyber Terrorism) by Maurice Dawson (Editor), Marwan Omar (Editor)
4. Cyber Warfare and Cyber Terrorism Lech Janczewski, Andrew Colarik

CPCCI9 Cyber Crime & Social Media

Learning Outcomes

Students understand the complete chronology & importance of social media. How we can develop safe practices to protect our critical important data & ensure safe social practices.

Syllabus

What is Social Media?, Opportunities of Social Media, Employment and Social Media, Considerations for setting up social media, Being Bold versus being overlooked, Risks of Social Media, The Dark Side, Risk Management, Policies and Privacy, Security, Future Aspects of Social Media.

Reference:

1. Social Media Security: Leveraging Social Networking While Mitigating Risk by Michael Cross MD (Author)
2. Online Social Networks Security: Principles, Algorithm, Applications, and Perspectives by Brij B. Gupta (Author), Somya Ranjan Sahoo (Author)

CPCCI10 (a) Online Extremism & Hate Crime

Learning Outcomes

Students learn about how online environment can largely affect radicalization & extremist ideology. Students also learn about the importance & power of internet & how it can affect our real world adversely if we don't follow safe net use practices. They also learn about what different factors harbor the divide in the society mainly demographic, political, social & economic.

Syllabus

Concept of Radicalization & Extremism, Causes and Drivers of Radicalization and Extremism, Violence as a solution OR Response to grievance and problems, The efficiency of Democratic process to address political grievances, Perused links between Islam, Extremism, Terrorism, The role of media within discourses of radicalization and extremism, Preventing or mitigating the threat of radicalization and violent extremism.

Reference:

1. Today's Crime and Punishment Issues: Democrats and Republicans by Angela D. Madden (Editor)
2. Fanaticism, Racism, and Rage Online: Corrupting the Digital Sphere by Adam Klein (Author)
3. Hate Crime (Crime and Society Series) by Nathan Hall (Author)

CPCCI10 (b) Forensic Science & Criminology

Learning Outcomes

Students will gain an additional knowledge of forensic science & criminology; which give them an advantage while handling complex criminal investigations as a Cyber Crime Investigator.

Syllabus

Introduction & Basic Concepts, Microscopy & Death Causes, Toxicology, Forensics Psychology.

Reference:

1. Forensic Science in Court: Challenges in the Twenty First Century (Issues in Crime and Justice) by Donald Shelton (Author)
2. Forensic Science In Criminal Investigation And Trials 6Th Edition by B R Sharma (Author)
3. Forensic Criminology by Brent E. Turvey (Editor), Claire E. Ferguson (Editor), Wayne Petherick (Editor)
4. Encyclopedia of Crime Criminology and Forensic Science by Ashok Kumar Choudhary (Author)

CPCCI11 Cyber Laws

Learning Outcomes

Students will gain complete knowledge about cyber laws in India. They will learn the significance, importance of following procedures & guidelines & how to present digital evidence in the court of law.

Syllabus

Indian Evidence Act 1872, The Information Technology Act 2000, Indian Penal Code (IPC) 1860, Code of Criminal Procedure (CRPC) 1973

Reference:

1. Cyber Laws an Indian Perspective By Transcendental Technologies
2. CYBER LAW AND CYBER CRIMES by DR JN BAROWALIA (Author), Dr Aarushi jain (Author)
3. Cyber Laws by Justice Yatindra Singh (Author)