How to Become a CyberCop / Cyber Crime Investigator

(Designed for learners who commented “CCI” — from the desk of @ankurdecodes)

1. Introduction: The Rise of Cyber Crime & Digital Policing

Online fraud, scams, digital identity theft, hacking, ransomware, financial fraud, and online harassment are increasing every day. Because of this, the demand for Cyber Crime Investigators has exploded in both government and private sectors.

A “CyberCop” is someone who:

- Tracks online criminals
- Investigates digital evidence
- Prevents cyber fraud
- Works with police, government, and corporate security teams
- Protects people and organizations from online threats

Salary Expectations (Beginner → Pro):

- Beginner: ₹3.5 – ₹6 LPA
- Mid-Level: ₹7 – ₹15 LPA
- Expert / Government / Corporate: ₹18 – ₹40 LPA+
- Freelance / Private Forensics: Even higher depending on cases

If you want to be an online cop or catch online fraudsters, this roadmap is for you

2. Step-by-Step Roadmap to Become a CyberCop

STEP 1: Build Core Foundations (1 Month)

Before investigating cyber crimes, understand how systems work.
Learn Basics Of:

- Computers & operating systems
- Networking fundamentals (IP, DNS, Ports, Protocols)
- Linux basics (important for investigations)
- Internet technologies

Tools to Explore:

- Wireshark
- Packet analyzers
- Browser developer tools

This forms your base as a cyber investigator.

STEP 2: Learn Cybersecurity Fundamentals (1–2 Months)

To catch criminals, you must understand how attacks happen.

Learn:

- Malware basics
- Phishing
- Ransomware
- Password attacks
- Web vulnerabilities (SQLi, XSS)
- Social engineering

Practice On:

- TryHackMe (Beginner labs)
- HackTheBox (Beginner tracks)

This builds your "attacker mindset" — crucial for investigations.

STEP 3: Learn Digital Forensics (The Most Important Skill!) (1–2 Months)

Digital forensics helps you collect, analyze, and present digital evidence.

Learn:

- Disk forensics
- Mobile forensics
- Network forensics
- Log analysis
- Memory forensics
- Evidence collection & chain of custody

Important Tools:

- Autopsy
- FTK Imager
- Cellebrite (mobile forensics)
- Volatility (memory forensics)
- EnCase

This skill makes you capable of solving real cases.

STEP 4: Learn OSINT (Open-Source Intelligence) (1–2 Months)

OSINT is used to track criminals online.

Learn:

- Social media tracking
- Website footprinting
- Email tracing
- Image forensics
- Phone number investigation
- Dark web basics

Popular Tools:

- Maltego
- Shodan
- Sherlock
- SpiderFoot
- WhatsMyName

OSINT is a must-have for cyber policing.

STEP 5: Learn Indian Cyber Laws (Very Important!)

To work with government or police, you must know the laws.

Study:

- IT Act 2000
- IPC sections for cyber crime
- Cyber safety laws
- Digital evidence laws
- Privacy and data protection

This helps you handle cases legally and professionally.

STEP 6: Recommended Certifications

These certifications increase the chances of getting government/private cyber investigation roles.

Beginner Certifications:

- Google Cybersecurity Certificate
- EC-Council CEH (Ethical Hacking)
- CompTIA Security+

Forensics Certifications:

- CHFI (Computer Hacking Forensic Investigator)
- CCE (Certified Computer Examiner)
- GCFA (GIAC Forensic Analyst)

OSINT Certifications:

- OSINT Foundation
- Practical OSINT Training

These boost your credibility.

3. Career Opportunities for Cyber Cops

Cyber Crime Investigators are needed in:

Government Sector:

- State Cyber Crime Cells
- CBI Cyber Crime Division
- Intelligence agencies
- Police digital forensics labs
- CERT-In

Private Sector:

- Banks & FinTech companies
- Cybersecurity companies
- Digital forensics firms
- Fraud detection teams
- IT security departments

Freelance Opportunities:

- Private investigation
- Cyber fraud case consulting
- OSINT investigations
- Forensic analysis services

4. Projects You Should Build (Portfolio Boosters)

Build a portfolio to get hired faster.

Project Ideas:

- A complete digital forensics case study
- Network traffic investigation report
- OSINT-based missing person investigation
- Phishing investigation dashboard
- Malware analysis report
- Fake profile investigation using OSINT

Upload to:

- GitHub
- Portfolio website
- LinkedIn

5. 6-Month CyberCop Learning Timeline

- Month 1: Basics + networking + Linux
- Month 2: Cybersecurity fundamentals
- Month 3: Digital forensics
- Month 4: OSINT + cyber laws
- Month 5: Projects + forensic tools
- Month 6: Apply for govt/private roles

6. Tools Every CyberCop Should Know

- Wireshark
- Autopsy
- Burp Suite
- Shodan
- Nmap
- Volatility
- Metasploit

Bonus Tip:

To explore trending cybersecurity, OSINT & AI tools quickly, check platforms like Techyuni.com or install their Chrome extension — gives access to hundreds of tools in a single click.

7. Tips from @ankurdecodes

- Small daily practice > long weekend study
- Focus on digital forensics & OSINT — highest demand
- Read real case studies of cyber crime
- Learn to write professional investigation reports
- Stay updated — new attacks appear daily

8. Your Next Step

You received this roadmap because you commented “CCI”.
If you sincerely follow this roadmap, you can become a skilled cyber investigator and build a career that is high-paying, respected, and impactful.
For more insights on cybersecurity, OSINT, AI, and powerful tech tools — follow @ankurdecodes.
Stay sharp. Stay alert. Your CyberCop journey begins today. 🔐🚓🚀

ANKUR CHANDRAKANT

For more such Valuable Resources

Follow @ankurdecodes