CRAW
ACADEMY

# Forensics 667

Cracking Codes, Solving Crimes, Explore the World of Cyber Forensics


## Cyber Forensics Investigation

+91 951 380 5401
training@craw.in
https://www.craw.in

# Table of **Content:**



# Program **Overview:**

The Cyber Forensics Investigation Course offers an in-depth exploration of the techniques and tools required for conducting successful cyber investigations. Covering a wide range of topics from basic concepts to advanced analytical methods, this program combines theoretical knowledge with practical hands-on experience, ensuring students are well-prepared to tackle real-world challenges in the cyber forensics domain.

# Program **Features:**

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in cyber forensics and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Stay abreast with our latest cyber forensics curriculum under the prime guidance of world-class training professionals.
- ✓ Explore real-world scenarios to understand the complexities of cyber investigations in our Case Studies section.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

# Delivery **Mode:**

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

# Prerequisites of **Cyber Forensics Investigation:**

- ✓ Basic understanding of computer systems and networks.
- ✓ Familiarity with operating systems such as Windows and Linux.
- ✓ No prior experience in cyber forensics is required, making this course suitable for beginners.

# Target **Audience:**

- ✓ IT professionals looking to specialize in cyber forensics.
- ✓ Law enforcement personnel involved in digital investigations.
- ✓ Legal professionals seeking to understand cyber forensics.
- ✓ Students and recent graduates aspiring to build a career in cyber security and forensics, and
- ✓ Anyone who is willing to learn more about cyber forensics investigation.

# Key Learning **Outcomes:**

This Cyber Forensics Investigation Course will help you:

- ✓ **Fundamental Understanding of Cyber Forensics:** Gain a solid foundation in the principles of cyber forensics, including the importance of ethical practices, legal considerations, and the role of forensics in cybersecurity.
- ✓ **Digital Evidence Management:** Develop the ability to identify, collect, preserve, and document digital evidence while maintaining its integrity and the chain of custody, ensuring it remains admissible in legal proceedings.

- ✓ **Forensic Analysis Techniques:** Master a range of techniques for the forensic analysis of digital data. This includes the ability to work with various types of digital evidence, such as files, emails, and images, across different platforms and devices.
- ✓ **Use of Forensic Tools and Software:** Become proficient in using leading forensic tools and software to analyze and extract valuable information from digital devices, including computers, smartphones, and networks.
- ✓ **Network and Mobile Forensics:** Acquire specialized knowledge in network forensics, including the analysis of network traffic and logs, as well as mobile device forensics, focusing on the retrieval and analysis of data from smartphones and tablets.
- ✓ **Incident Response and Handling**: Learn to effectively respond to cybersecurity incidents with a forensics-focused approach. Understand how to conduct initial assessments, mitigate threats, and implement strategies to prevent future incidents.
- ✓ **Reporting and Presentation of Findings:** Develop the skills necessary to prepare comprehensive forensic reports and present findings in a clear, concise manner that is understandable to non-technical stakeholders, including legal teams and courtrooms.
- ✓ **Preparation for Certification:** Prepare for globally recognized certifications in cyber forensics, enhancing professional credibility and marketability in the cybersecurity field.

## Certification **Alignment:**

Our Cyber Forensics Investigation Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

## Certification **Details & Criteria:**

**Certification Details -**
Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply digital forensics techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

## About the **Exam:**

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

## Craw Security **Certification Criteria:**

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

## 100% Placement with **1 Year Cyber Security Course:**

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.

- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  1. Documentation
  2. Offer Letter
  3. Joining Date/ Timeline of Joining

## What to Choose After this **Course:**

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

## Course **Curriculum:**

### Module 01: Computer Forensics in Today's World

- ✓ Lesson 01: Understanding the cyber crime
- ✓ Lesson 02: Understanding cyber law
- ✓ Lesson 03: Common attack
- ✓ Lesson 04: Digital evidence
- ✓ Lesson 05: Types Digital forensic
- ✓ Lesson 06: Challenge in cybercrime investigation

### Module 02: Computer Forensics Investigation Process

- ✓ Lesson 01: Rules of Digital forensic investigation
- ✓ Lesson 02: Chain of custody, (SOP) standard operating procedure
- ✓ Lesson 03: Lab work, (CSI) crime scene investigation, about Raids, Incident response
- ✓ Lesson 04: Checklist to prepare before the investigation.
- ✓ Lesson 05: Precaution during search and seizure
- ✓ Lesson 06: Equipment's and tools software/hardware based

### Module 03: Understanding Hard Disks and File Systems

- ✓ Lesson 01: Hard disk design and architecture
- ✓ Lesson 02: Various Filesystems
- ✓ Lesson 03: Understanding booting process
- ✓ Lesson 04: Window & Linux Filesystem

### Module 04: Data Acquisition and Duplication

- ✓ Lesson 01: Understanding the concept of data acquisition
- ✓ Lesson 02: Rules of data acquisitions

- ✓ Lesson 03: Types of data acquisitions
- ✓ Lesson 04: Live & Dead acquisitions
- ✓ Lesson 05: Data acquisition Format
- ✓ Lesson 06: Live and dead acquisition on window & Linux

## Module 05: Defeating Anti-Forensics Techniques

- ✓ Lesson 01: Insight of anti-forensic technique
- ✓ Lesson 02: Steganography pros & cons
- ✓ Lesson 03: Types of Steganography
- ✓ Lesson 04: Basic stenographic model
- ✓ Lesson 05: Data sanitization by hardware and software tools
- ✓ Lesson 06: Password cracking technique
- ✓ Lesson 07: Deleted data recovery
- ✓ Lesson 08: Encryption methods

## Module 06: Windows Forensics

- ✓ Lesson 01: Methodology of window forensic
- ✓ Lesson 02: Collecting volatile data & non-volatile data
- ✓ Lesson 03: Window forensic analysis
- ✓ Lesson 04: Gathering information by tools
- ✓ Lesson 05: Examine whole file
- ✓ Lesson 06: Examine network information
- ✓ Lesson 07: Examine process information
- ✓ Lesson 08: Examine event logs
- ✓ Lesson 09: Understanding metadata

## Module 07: Linux and Mac Forensics

- ✓ Lesson 01: Methodology of Linux forensics
- ✓ Lesson 02: Collecting file system information
- ✓ Lesson 03: Collecting volatile data & non-volatile data
- ✓ Lesson 04: Collecting login history and currently logged in user
- ✓ Lesson 05: Collecting hostname, data, time, uptime data
- ✓ Lesson 06: Gathering network information
- ✓ Lesson 07: Gathering open port information
- ✓ Lesson 08: Analysing log files in Linux OS
- ✓ Lesson 09: Collecting suspicious information
- ✓ Lesson 10: Collection network information

## Module 08: Network Forensics

- ✓ Lesson 01: Introduction of network forensics
- ✓ Lesson 02: Network forensics process
- ✓ Lesson 03: Analysing different network logs
- ✓ Lesson 04: Log file analysis
- ✓ Lesson 05: Log management challenges
- ✓ Lesson 06: Analysing network traffics
- ✓ Lesson 07: Gathering info through sniffing
- ✓ Lesson 08: Sniffing tools

## Module 09: Investigating Web Forensics

- ✓ Lesson 01: Introduction to web application forensics
- ✓ Lesson 02: Indicators of a web attack

- ✓ Lesson 03: Web application threats
- ✓ Lesson 04: Web attack investigation methodology
- ✓ Lesson 05: Analysing web logs client/admin

## Module 10: Dark Web Forensics

- ✓ Lesson 01: Introduction to dark web forensics
- ✓ Lesson 02: Layers of internet
- ✓ Lesson 03: Tor browser architecture
- ✓ Lesson 04: Investigating tor

## Module 11: Cloud Forensics

- ✓ Lesson 01: Cloud models
- ✓ Lesson 02: Cloud computing threats & attack
- ✓ Lesson 03: Cloud forensics
- ✓ Lesson 04: Cloud crimes

## Module 12: Investigating Email Crimes

- ✓ Lesson 01: Email server architecture
- ✓ Lesson 02: Understanding email structure
- ✓ Lesson 03: Email crime investigation procedure
- ✓ Lesson 04: Analysing email

## Module 13: Malware Forensics

- ✓ Lesson 01: Introduction to malware forensics
- ✓ Lesson 02: What is malware & what can malware do
- ✓ Lesson 03: Type of malware
- ✓ Lesson 04: Different ways malware can get into a system
- ✓ Lesson 05: Components of malware
- ✓ Lesson 06: Types Malware analysis
- ✓ Lesson 07: Tools for malware analysis
- ✓ Lesson 08: Deep study on malware cases

## Module 14: Mobile Forensics

- ✓ Lesson 01: Introduction of mobile forensics
- ✓ Lesson 02: Why do we need mobile forensics
- ✓ Lesson 03: Challenges in mobile forensics
- ✓ Lesson 04: Mobile devices and fundamental component
- ✓ Lesson 05: Mobile phone evidence extraction process
- ✓ Lesson 06: Removable and external data storage
- ✓ Lesson 07: Data Acquisition from iOS Devices & android
- ✓ Lesson 08: Data Acquisition and Analyzing SIM Cards
- ✓ Lesson 09: Examination and analysis
- ✓ Lesson 10: Mobile forensic tools

## Module 15: IoT Forensics

- ✓ Lesson 01: Understanding the IOT forensics
- ✓ Lesson 02: Understanding IOT & IOT issues
- ✓ Lesson 03: IOT architecture
- ✓ Lesson 04: Learning objectives of IOT forensics
- ✓ Lesson 05: IOT security problems
- ✓ Lesson 06: IOT attack surface area

# About us:

Craw Security is India's leading cybersecurity training institute, dedicated to developing the next generation of cybersecurity professionals. With a focus on practical, hands-on training, we offer a wide range of courses tailored to all skill levels. Our mission is to enhance the cybersecurity posture of individuals and organizations worldwide.

For more information, please visit our course page website:
https://www.craw.in/cyber-forensics-investigation-course-in-delhi/

# Contact us:

## Craw Cyber Security Private Limited, India (Head Office)

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

## Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

## Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel