RECON

CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco · python · EY · Red Hat · CompTIA · Microsoft

OVERVIEW

In this course, students will learn the about Cyber Forensics and Cyber defence techniques. Topics include OS Forensics, Malware, Storage Media, Memory Forensics and more.

PRE-REQUISITES

Students should already be familiar with how to operate the Linux Operating system.

WHO WE ARE

We promise to offer the best training and certification programs to our students. We provide the programs and resources you need to succeed if you are just beginning your Cyber security career or are an experienced expert wishing to develop your skills. Contact us today to learn more about our training and certification options!

WHY CHOOSE US

Welcome to our Cyber Security Training Institute, where we are committed to giving individuals and organisations who want to protect their digital assets thorough training and certification programmes. Our knowledgeable Trainers will bring you through the complexities of cyber security with their cutting-edge expertise and practical experience. You will learn useful methods and abilities to protect yourself from online dangers, such as ethical hacking, network security, incident response, and other things. Our programmes give you the opportunity to hone your skills and grow your profession through practical lab experiences and individualised coaching.

CYBER FORENSICS BOOTCAMP TRAINING

COURSE DURATION: 40 hrs

- Lesson 01 : Introduction to Digital Forensics
  - Overview of Digital Forensics
  - Importance and Applications
  - Legal and Ethical Considerations
- Lesson 02 : Inevitability During computer forensics
  - Investigation Techniques
  - Maintaining Integrity of Evidence
  - Chain of Custody Procedures
    Use of Write Blockers
- Lesson 03 : Data Acquisition - copying and imaging with FTK Imager
  - Introduction to FTK Imager
  - Step-by-Step Imaging Process
  - Validating and Verifying Images
- Lesson 04 : OS Forensics
  - Understanding RAM Dumps
  - Techniques for RAM Dump Analysis
  - Case Studies of OS Forensics
- Lesson 05 : Checking the integrity or files using the concept of Hash value
  - Hash Functions and Algorithms
  - Practical Hash Value Calculation
  - Verifying Data Integrity
- Lesson 06 : Browser Forensics
  - Analyzing Browser History
  - Recovering Deleted Browsing Data
  - Investigating Cookies and Cache
- Lesson 07 : Multimedia Forensics
  - Analyzing Digital Media Files
  - Metadata Extraction
  - Techniques for Detecting Media Manipulation
- Lesson 08 : Investigation methodology and digital devices
  - Methodologies for Digital Investigations
  - Types of Digital Devices
  - Case Studies and Practical Applications
- Lesson 09 : Storage Media
  - Understanding Logical Structure
  - GUID and Partition Tables
  - File Systems and Their Forensic Relevance
- Lesson 10 : Network forensics Cont.
  - Analyzing Network Traffic
  - Network Protocols and Their Forensics
  - Investigating Network Attacks
- Lesson 11 : Malware
  - Types of Malware
  - Techniques for Malware Analysis
  - Case Studies of Malware Incidents

- Lesson 12 : Memory forensics
  - Introduction to Memory Forensics
  - Analyzing Volatile Memory
  - Tools and Techniques for Memory Analysis
- Lesson 13 : Digital forensics tools
  - Creating and Analyzing Disk Images
  - Recovering Deleted Data
  - Extracting Files from Unallocated Space
- Lesson 14 : Cryptanalysis
  - Encryption and Decryption Tools
  - Forensic Data Analysis Tools
  - Techniques for Cryptanalysis
- Lesson 15 : Process of Investigation
  - Roles and Responsibilities in Forensics
  - Identifying and Containing Security Breaches
  - Collection and Preservation of Digital Evidence
  - Investigating and Reporting Incidents
- Lesson 16 : Lab Sessions
  - Installing and Configuring Caine
  - Using USB Packet Sniffers
  - Encryption Practical Exercises
  - Event Viewer for Windows Forensics
  - Memory Forensics Labs

Basics of Mail Forensics

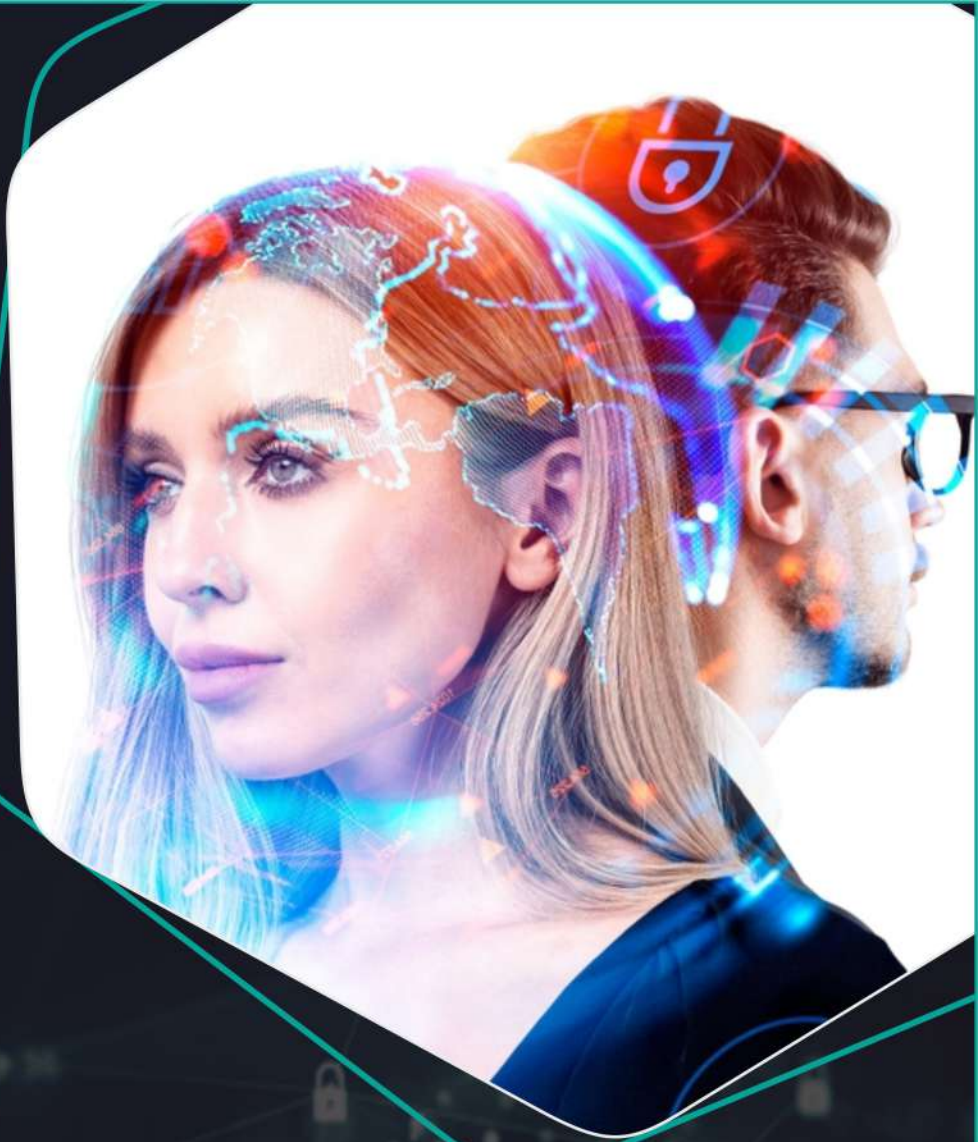
- Lesson 17 : Window forensics
  - Analyzing Windows Artifacts
  - Investigating Windows Registry
  - Case Studies in Windows Forensics
- Lesson 18 : Dark web forensics
  - Understanding the Dark Web
  - Techniques for Investigating Dark Web Activities
  - Tools for Dark Web Forensics
- Lesson 19 : Cloud forensics
  - Overview of Cloud Computing
  - Techniques for Cloud Data Investigation
  - Challenges and Solutions in Cloud Forensics
- Lesson 20 : Email Forensics
  - Analyzing Email Headers
  - Recovering Deleted Emails
  - Investigating Email-Based Attacks
- Lesson 21 : Mobile forensics
  - Mobile Device Data Acquisition
  - Analyzing Mobile Apps and Data
  - Investigating Mobile Device Security Incidents

BOOTCAMP TRAINING HOURS

- **3 HOURS**
- **4 HOURS**
- **6 HOURS**

- **20 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **Certificate after completion**
- **Interview preparation**
- **Live hacking training**
- **Class session recordings**
- **Ebooks tutorials24x7 support**

- Every Class Recordings
- Easy Repetations
- Shareable Content
- Hybrid Classes
- Checkpoint Based Training
- 24x7 Support



RECON CYBER SECURITY PVT. LTD

(HEAD OFFICE | LAXMI NAGAR, NEW DELHI)

2nd Floor, Gali no 1, Shakarpur, Laxmi Nagar New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

RECON CYBER SECURITY PVT. LTD

(BRANCH OFFICE | SANT NAGAR BURARI, NEW DELHI)

Ground Floor, Gali no 8, Main Market, Sant Nagar, Burari, New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

#RECON CYBER SECURITY