## Rocheston Certified Cybercrime Investigator (RCCI)

# Rocheston Certified Cybercrime Investigator (RCCI) training program

The Rocheston Certified Cybercrime Investigator (RCCI) training program is designed to provide participants with the knowledge and skills to identify and investigate cybercrime. The program is designed to help participants gain a comprehensive understanding of cybercrime, its impact, and the methods and techniques used to detect and investigate it. The program is suitable for a range of professionals, including law enforcement officers, intelligence agents, cyber security professionals, and legal professionals.

## Why you Need to Attend?

The program consists of several modules, including an introduction to cybercrime and its impact, understanding digital evidence and its role in cybercrime investigations, and the use of digital forensics tools and techniques. Participants will also learn about the legal aspects of cybercrime investigation, including the laws and regulations governing digital evidence and its collection and use.

## Practical Exercises

The program also includes practical exercises and simulations, which will help participants gain hands-on experience in investigating cybercrime. Participants will be taught how to identify cybercrime victims and perpetrators, how to access digital evidence, how to analyze digital evidence, and how to write a successful investigation report.

At the end of the program, participants will be able to demonstrate their understanding of cybercrime investigations, as well as their ability to identify, collect, and analyze digital evidence. They will also have the knowledge and skills necessary to recognize cyber threats, respond to cyber incidents, and produce a successful investigation report.

## Who Should Attend?

The RCCI training program is beneficial for anyone interested in cyber security, forensics, and cybercrime investigation. It provides participants with the skills and knowledge necessary to detect, investigate, and prevent cybercrime. By completing the program, participants gain a comprehensive understanding of cybercrime and its impact, as well as the methods and techniques used to detect and investigate it.

## Course Outline

- Ethics and Legal Issues
- Definition of Cybercrime and Digital Forensics
- Types of Cybercrimes
- Identifying Cybercrimes
- Cybercrime Investigation Process
- Understanding Privacy Laws
- Examining Intellectual Property Rights
- Ensuring Compliance with Regulatory Standards
- Understanding Professional Conduct
- Investigating cybercrime through digital forensics
- Gathering evidence from digital sources
- Analyzing digital evidence
- Understanding the limitations of digital evidence
- Investigative Strategies
- Identification of Victims
- Gathering Evidence
- Analysis of Digital Evidence
- Interviewing Witnesses
- Cybercrime Laws
- Legal Issues in Cybercrime Investigations
- Privacy and data protection laws
- Intellectual property laws
- Electronic communications laws
- International law considerations
- Ethical Considerations in Cybercrime Investigations
- Overview of Ethical Standards

- Role of the Investigator
- Protecting Personal Privacy
- Respect for the Law
- Reporting Requirement
- Respect for privacy
- Respect for civil liberties
- Use of force and coercion
- Accuracy and truthfulness
- Professional codes of conduct
- Prosecuting Cybercrimes
- Collecting and presenting evidence in court
- Strategies for successful prosecution
- Digital Forensics Concepts
- Gathering and Preserving Digital Evidence: Utilizing appropriate methods and best practices
- Digital Forensic Investigation Process
- Assessing the crime scene, setting up a command center, and obtaining search warrants
  Collection of Evidence
- Gaining Access to Digital Evidence: Searching, seizing, and analyzing digital evidence
- Preservation of Evidence
- Analysis of Evidence
- Reporting of Findings
- Authentication of Digital Evidence
- Chain of Custody
- Integrity of Data
- Evidence Tampering
- Digital Evidence Types
- Volatile Data
- Non-Volatile Data
- Network Evidence
- Data Acquisition Strategies
- Digital Evidence Preservation Strategies
- Image File Formats
- Data Acquisition
- Imaging and Cloning

- Documenting Evidence
- Verifying Evidence
- Data Recovery
- Recovering Deleted Files
- Recovering Fragmented Files
- Recovering Encrypted Files
- Data Analysis
- File System Analysis
- Logical Analysis
- Network Analysis
- Digital Forensic Tools and Techniques
- Acquisition Methods
- Examination and Analysis
- Computer Forensics Report Writing
- Purpose of the Report
- Structure of the Report
- Quality Assurance
- Legal Issues with Digital Evidence
- Admissibility of Evidence
- Spoliation
- Relevance of Evidence
- Preparing for Court: Documenting the investigation, preparing reports and legal documents
- Investigative Cellular Network Analysis
- Investigating Online Fraudulent Activity: Scams, Identifying Patterns of Fraudulent Behavior
- Investigating Money Laundering
- Investigating Online Gambling
- Investigating Webcam and Video Surveillance Abuse
- Investigating Fake News and Online Reputation Damage
- Investigating Online Censorship and Propaganda
- Investigating Cyberstalking and Online Extortion
- Investigating System Backdoors and Rootkits
- Investigating Digital Privacy Violations
- Investigating Information Warfare and Cyberwarfare
- Investigating Website Defacement and Destruction

- Investigating Social Engineering and Predatory Behavior
- Investigating Cyber Espionage and Corporate Sabotage
- Investigating Hacking Incidents: Investigating Unauthorized Access,
- Investigating Denial of Service Attacks
- Investigating Cyberbullying and Harassment: Identifying Digital Abuse, Tracking IP Addresses,
- Investigating Social Media Abuse, Crimes Involving Social Media
- Investigating Insider Threats and Data Leaks
- Investigating Child Exploitation and Trafficking: Locating Victims, Identifying Predators, Documenting Digital Abuse
- Investigating Online Credit Card Fraud
- Investigating Employee Monitoring and Surveillance
- Investigating Online Banking Fraud and Money Laundering
- Investigating Intellectual Property Theft and Copyright Infringement: Identifying Counterfeit Goods, Documenting Piracy, Investigating Software Piracy
- Investigating Phishing, Spam, and Botnets: Detecting Phishing Websites, Investigating Malware Distribution, Identifying Botnet Command and Control Centers
- Investigating Identity Theft and Financial Crimes: Determining Sources of Identity Theft, Investigating Financial Transactions, Locating Assets
- Investigating Cyber Terrorism: Investigating Terrorist Networks, Analyzing Malware, Investigating Ransomware
- Investigating Data Breaches: Identifying Vulnerabilities, Locating Compromised Data, Preparing Breach Reports
- Investigating Mobile Device Use: Analyzing Phone Records, Recovering Deleted Text Messages, Accessing GPS Data
- Investigating Network Traffic: Packet Analysis, Protocols, Investigating Network Intrusions
- Investigating Cloud Storage: Identifying Cloud Services, Accessing Data, Analyzing Logs
- Investigating Web Applications: Application Architecture, Reverse Engineering, Security Testing
- Investigating Database Activity: Database Management Systems, Log Analysis, Querying Databases
- Investigating Social Media: Identifying Accounts, Analyzing Content, Tracking Connections
- Investigating Voice Over IP: Analyzing VoIP Traffic, Intercepting Calls, Investigating Call Forwarding

- Investigating Dark Web Activity: Identifying Dark Web Sites, Analyzing Cryptocurrencies, Investigating Illegal Markets
- Investigating Embedded Devices: Smartphones, Medical Devices, SCADA Systems
- Investigating Automated Systems: Robotics, Autonomous Vehicles, Industrial Automation
- Investigating Cryptocurrency Transactions: Blockchain Analysis, Tracking Wallets, Identifying Illicit Activity
- Investigating Internet of Things Devices: Device Identification, Network Analysis, Data Analysis
- Investigating Smart Contracts: Analyzing Contract Code, Investigating Disputes, Ensuring Compliance
- Investigating Augmented Reality Applications: Analyzing AR Data, Investigating AR Communications, Tracking AR Devices
- Investigating Virtual Reality Applications: Analyzing VR Data, Investigating VR Communications, Tracking VR Devices
- Analyzing Steganography: Image Analysis, Audio Analysis, Document Analysis
- Investigating Wireless Networks: Wi-Fi Analysis, Bluetooth Analysis, Mesh Networks
- Investigating Physical Access Controls: Analyzing CCTV Footage, Biometric Analysis, Investigating Keyloggers
- Investigating Surveillance Cameras: Analyzing Video Feeds, Investigating Spyware, Identifying Surveillance Devices
- Investigating Networked Devices: Analyzing Network Traffic, Locating Rogue Devices, Investigating Network Misconfigurations
- Investigating Videoconferencing: Analyzing Videoconference Traffic, Identifying Misuses, Investigating Video Tampering
- Investigating Location Data: Geolocation Analysis, Mapping Tools, Location Tracking
- Investigating Wearable Technologies: Health Monitors, Smart Watches, Fitness Trackers
- Investigating Robotics: Robot Programming, Artificial Intelligence, Machine Learning
- Investigating Autonomous Vehicles: Vehicle Telematics, Driverless Car Technology, Analyzing Sensor Data
- Investigating Industrial Control Systems: SCADA Systems, Analyzing Control Logic, Identifying Vulnerabilities
- Investigating Building Automation Systems: Analyzing Building Data, Identifying Security Vulnerabilities, Investigating Access Controls
- Investigating Smart Homes: Analyzing Home Data, Tracking Devices, Identifying Security Weaknesses

- Investigating 3D Printing: Analyzing 3D Objects, Identifying Intellectual Property Theft, Investigating Printer Tampering
- Investigating Biometrics: Analyzing Fingerprint Data, Investigating Facial Recognition Systems, Analyzing Iris Data
- Investigating Radio Frequency Identification: RFID Analysis, Tracking Tags, Investigating Tampering
- Investigating Artificial Intelligence: Analyzing AI Algorithms, Evaluating AI Performance, Investigating Abnormal Outputs
- Investigating Digital Rights Management: Analyzing DRM Solutions, Investigating DRM Violations, Identifying Counterfeit Products
- Investigating Voice Recognition: Analyzing Voice Data, Identifying Anomalies, Investigating Misuses
- Investigating Speech Recognition: Analyzing Speech Data, Identifying Anomalies, Investigating Misuses
- Investigating Mobile Applications: Analyzing Application Data, Identifying Anomalies, Investigating Misuses
- Investigating Email Use: Analyzing Email Logs, Identifying Anomalies, Investigating Misuses
- Investigating Cloud Storage: Analyzing Cloud Logs, Identifying Anomalies, Investigating Misuses
- Investigating Web Browsers: Analyzing Browser Logs, Identifying Anomalies, Investigating Misuses
- Investigating Operating Systems: Analyzing OS Logs, Identifying Anomalies, Investigating Misuses
- Investigating Online Payment Systems: Analyzing Payment System Logs, Identifying Anomalies, Investigating Misuses
- Investigating Social Media: Analyzing Social Media Logs, Identifying Anomalies, Investigating Misuses
- Investigating Network Traffic: Analyzing Network Traffic Logs, Identifying Anomalies, Investigating Misuses
- Investigating Database Activity: Analyzing Database Logs, Identifying Anomalies, Investigating Misuses
- Investigating Fake Passports, Identity Cards and Government Issued Documents
- Investigating Fake Currency
- Investigating Deepfake Videos and Artificial Generated Images

- Investigating Malware: Analyzing Malware Logs, Identifying Anomalies, Investigating Misuses
- Investigating Encryption: Analyzing Encryption Logs, Identifying Anomalies, Investigating Misuses
- Investigating Intrusion Detection Systems: Analyzing IDS Logs, Identifying Anomalies, Investigating Misuses
- Investigating Endpoints: Analyzing Endpoint Logs, Identifying Anomalies, Investigating Misuses
- Investigating Network Security: Analyzing Network Security Logs, Identifying Anomalies, Investigating Misuses
- Investigating Proxies: Analyzing Proxy Logs, Identifying Anomalies, Investigating Misuses
- Investigating Firewalls: Analyzing Firewall Logs, Identifying Anomalies, Investigating Misuses
- Investigating Router Activity: Analyzing Router Logs, Identifying Anomalies, Investigating Misuses
- Investigating Internet of Things (IoT): Analyzing IoT Logs, Identifying Anomalies, Investigating Misuses
- Investigating Virtual Private Networks (VPN): Analyzing VPN Logs, Identifying Anomalies, Investigating Misuses
- Investigating Packet Sniffing: Analyzing Packet Sniffer Logs, Identifying Anomalies, Investigating Misuses
- Investigating DDoS Attacks: Analyzing DDoS Attack Logs, Identifying Anomalies, Investigating Misuses
- Investigating Botnets: Analyzing Botnet Logs, Identifying Anomalies, Investigating Misuses
- Investigating Phishing Attacks: Analyzing Phishing Attack Logs, Identifying Anomalies, Investigating Misuses
- Investigating Ransomware Attacks: Analyzing Ransomware Attack Logs, Identifying Anomalies, Investigating Misuses
- Investigating Spam: Analyzing Spam Logs, Identifying Anomalies, Investigating Misuses
- Investigating Spyware: Analyzing Spyware Logs, Identifying Anomalies, Investigating Misuses
- Investigating Keyloggers: Analyzing Keylogger Logs, Identifying Anomalies, Investigating Misuses
- Investigating Adware: Analyzing Adware Logs, Identifying Anomalies, Investigating Misuses
- Investigating Exploit Kits: Analyzing Exploit Kit Logs, Identifying Anomalies, Investigating Misuses

- Investigating Password Cracking: Analyzing Password Cracking Logs, Identifying Anomalies, Investigating Misuses
- Investigating Cryptojacking: Analyzing Cryptojacking Logs, Identifying Anomalies, Investigating Misuses
- Investigating Zero-Day Vulnerabilities: Analyzing Zero-Day Logs, Identifying Anomalies, Investigating Misuses
- Cybercrime Prosecution in Court
- Cybercrime and the Legal System
- Definition, scope, and types of cybercrime
- Understanding the legal system and its role in cybercrime prosecutions
- Overview of local, state, federal, and international laws related to cybercrime
- Understanding the Roles of the Prosecutor and Defense Counsel
- Establishing Elements of the Offense and Building a Case
- Presenting Digital Evidence in Court: Expert witnesses and cross-examination techniques
- Strategies for Defending Against Cybercrime Charges