ROCHESTON® CERTIFIED CYBERCRIME INVESTIGATOR

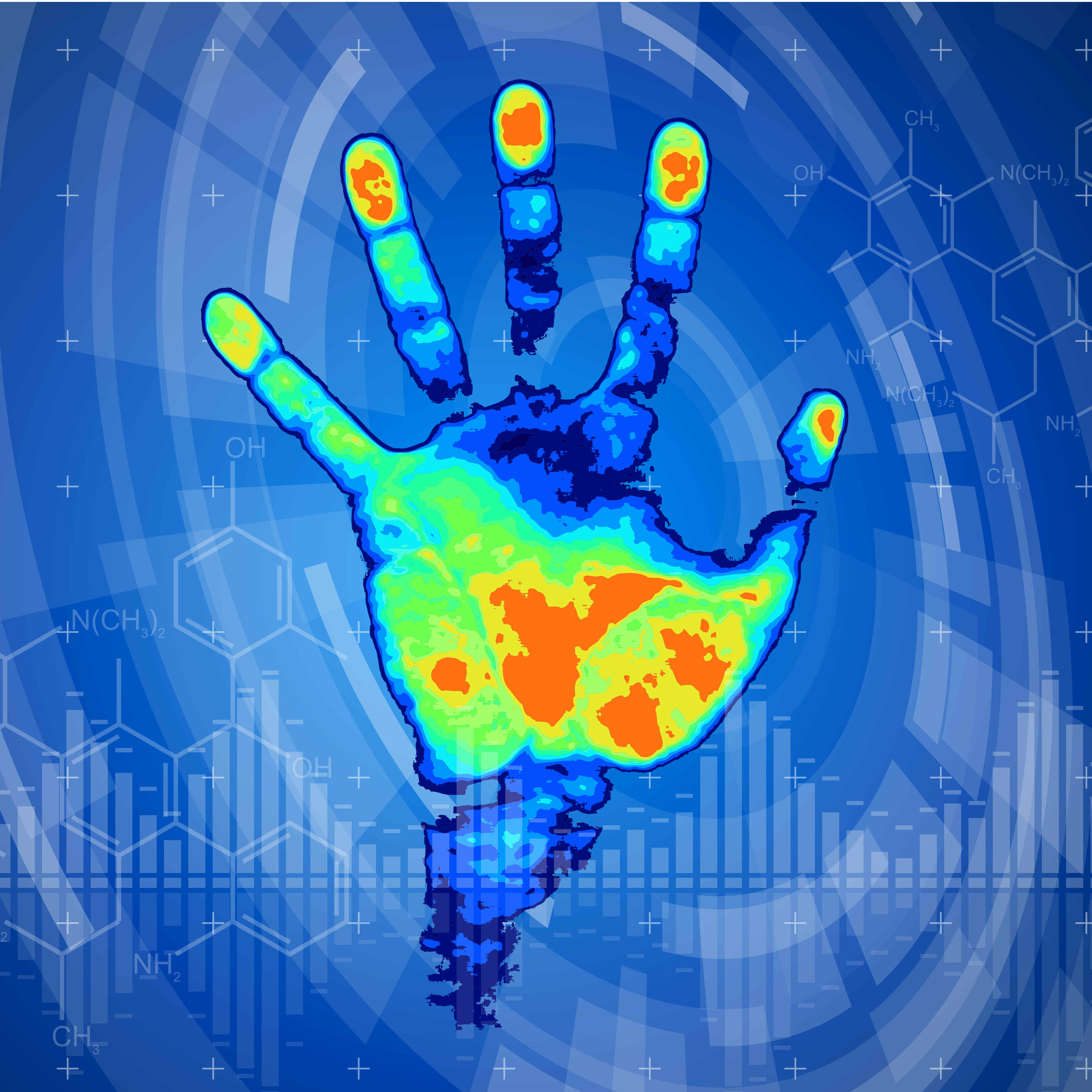
Certified by Rocheston®

RCCI® Certification Program Guide

What is RCCI?

RCCI is a unique credential on cyber forensic investigation. Rocheston's courseware is designed to ensure industry relevance. SMEs deliver the course content in a five-day learning capsule

Cybercrime will be worth 411M US$ in a few years. Its global nature will necessitate an evolving standard to fight it. Threat neutralization will require best practices and protocol that are common across borders. This is where Rocheston's RCCI steps in.


CH_3
OH
$N(CH_3)_2$
NH_2
$N(CH_3)_2$
NH_2
CH_3
OH
$N(CH_3)_2$
OH
NH_2
CH_3

Benefits of RCCI certification

- **Learn the art and science of cybercrime fighting**

Phishing, online scams, identity theft, malware, virus dissemination, and email bombing. These are just a few of the menaces that a student will learn to neutralize.

- **Obtain knowledge on cyber forensic procedures**

RCCI provides extensive insight on cyber forensics investigations and teaches various strategies to optimize and streamline the course of an investigation.

- **Cybercrime investigators will be in demand**

Job vacancies for cybercrime investigators is expected to increase by 22% in 10 years. RCCI is the perfect platform for budding cyber sleuths.

- **Specialist certification that isn't too technical**

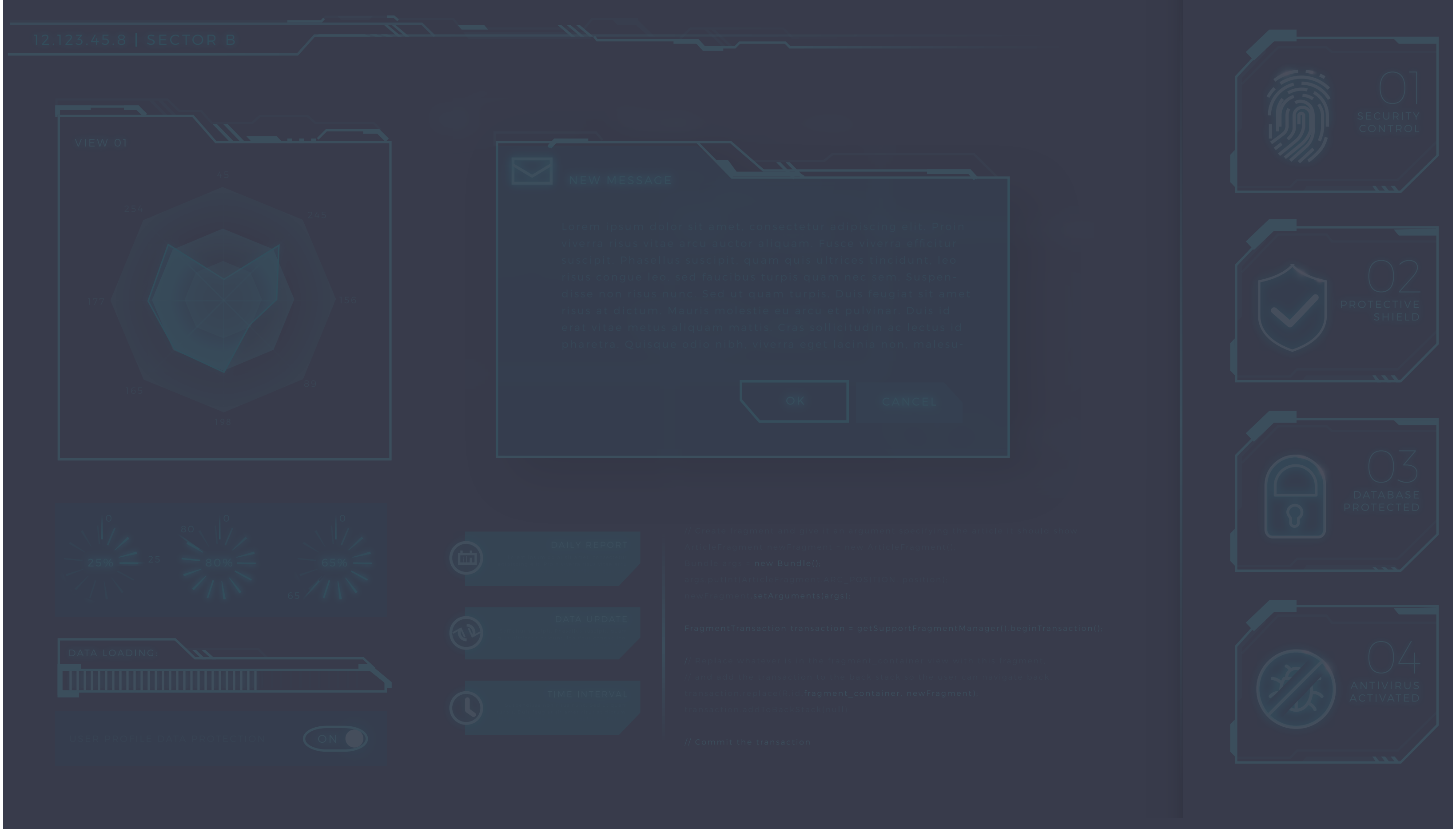
RCCI has the perfect balance. It is a niche and specialist certification that isn't overly technical. Therefore, it is easily accessible to students who aren't tech geniuses. Sophistication, accessibility, and utility.

Increasing Costs of Cybercrime

Versatility is the name of the game. Certified individuals have a plethora of options available. RCCIs are expected to be in demand in the following industries:

- 500 billion US$ is the potential cost of cybercrime to the world community, as of 2016.
- 14 billion US$ is the amount of money the U.S.A. Government spent on cybersecurity measures in the year 2017.
- 2.1 trillion US$ is the complete global annual cost of data breaches in 2019, as suggested by Juniper Research.
- 1.5 trillion US$ is the amount that cybercriminals stole from their victims in the year 2017.
- 600 billion US$ is the total global cost of cybercrime in the year 2017.
- 50 million US$ is the complete cost of cybercrime across 237 corporate entities in 6 countries.

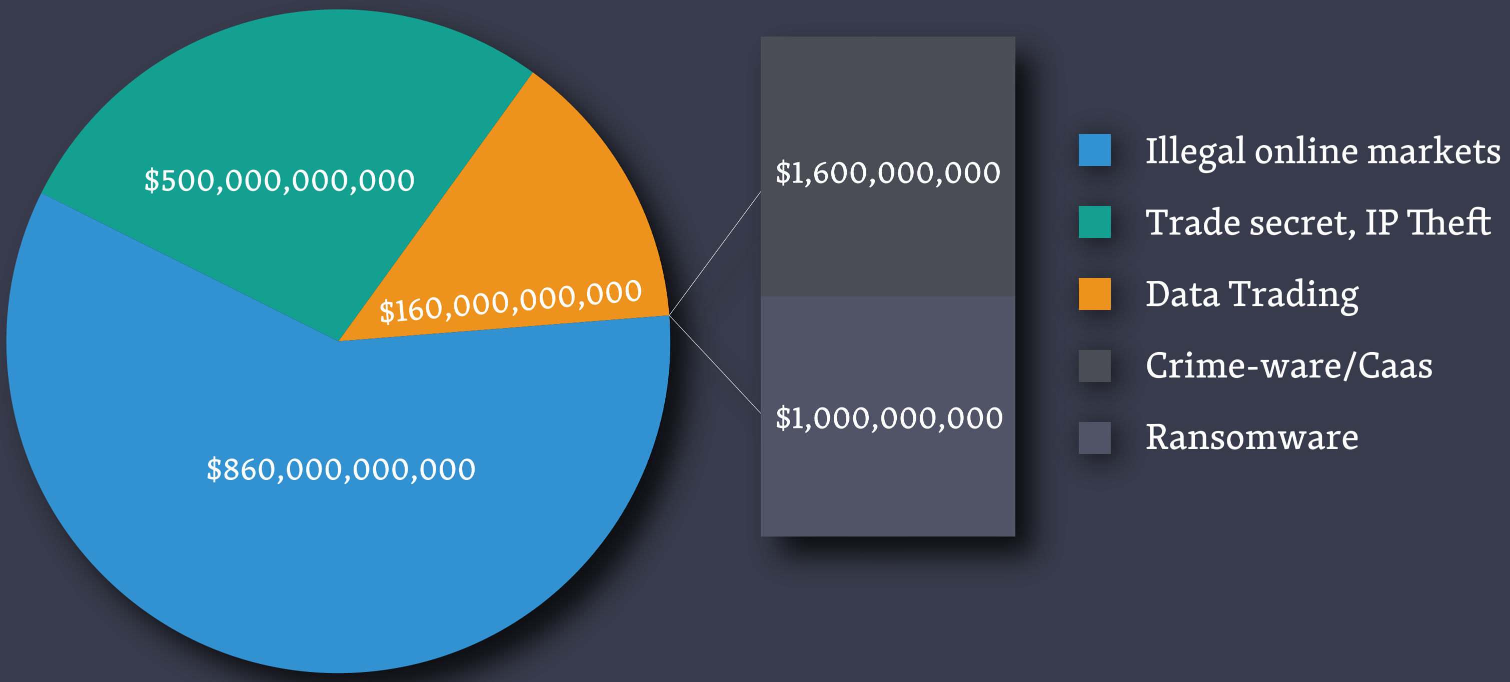
- 530 million US$ is the damage caused by the Coincheck hack, the largest cryptocurrency heist till date.
- 3.8 million US$ is the average damage caused by a data breach to a corporate entity.
- 158 billion US$ the cumulative amount of money customers lost in total in 2015 because of cybercrime activities.
- 2 million US$ is the average damages caused by a DDoS attack on an enterprise in the year 2017.



Cybercrime Statistics

- Cybercrime is estimated to have created profits in excess of 1.5 trillion US$ in 2018.

Cybercrime Annual Revenues



Cybercrime revenue can be defined as money that is earned due to crimes where computers and other electronic devices played a direct role. However, certain scams such as mobile scams were not included in this figure.

High profile ransomware were curiously enough, not big earners. This is particularly interesting as Petya/NotPetya gained huge publicity in the media and was very rampant during its heyday. But it is worth noting that ransomware is designed for either profit, or disruption. Petya/NotPetya comes under the second category.

Cybercrime operations are also structured in a rather interesting way. The larger operations mirror multi-national corporations and the smaller operations resemble single proprietorship businesses. Bigger cybercrime operations rake in revenue in excess of 1 billion per year, while the more humble operations bring in about US$ 30k to US$ 50k.

Objectives of RCCI

The RCCI program is tailored for students of cybercrime, investigation, and law enforcement methodology. RCCIs can be game changers both in corporate and other environments. The objective of the RCCI course is to provide students with a solid foundation in cybercrime deterrence and identification, and law enforcement methodology.

CONTRACT

Role of an RCCI

The next 10-years will see a 22% increase in the demand for cybercrime investigators.

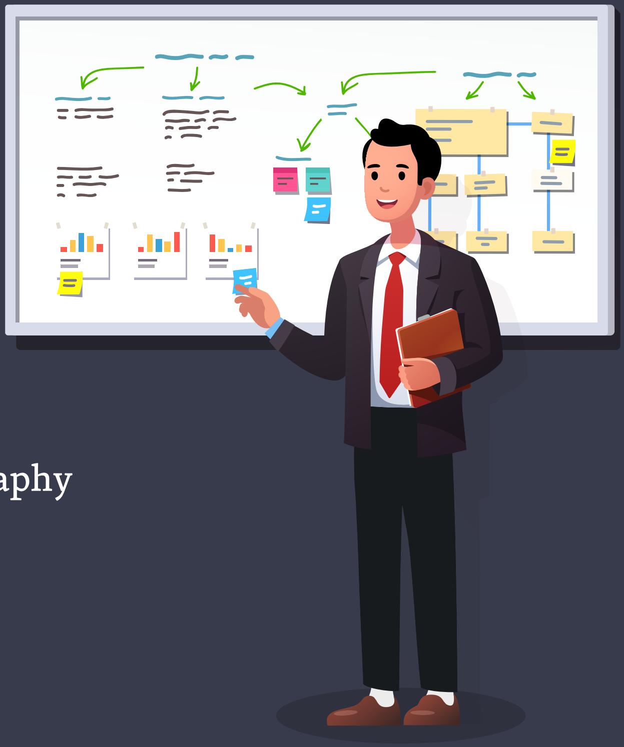
The following are some of the functionalities of a cybercrime investigator:

- Assessing/investigating crimes committed using electronic devices
- Retrieving affected or damaged data
- Drafting case documentation
- Understanding and reconstructing crime scenes/scenarios
- Developing forensic/criminology skills via research
- Identifying methods for processing digital evidence
- Testifying in court if necessary
- Making evidence and case documentation comprehensible to the jury/court

Skills You Will Learn

The following are a few essential skills for cybercrime investigators:

- Web programming
- A functional understanding of web tech
- Strong awareness of web hacking
- Proficiency in interviewing suspects
- Comprehensive knowledge of documentation
- Knowledge of the dark web
- Working knowledge of virtual payment systems
- Understanding of the ISO/IEC 27037 standard
- Working knowledge of Steganography & Cryptography



Job Prospects

An RCCI-certified individual can expect to be employed in the following capacities:

- Cyberforensic Computer Analyst
- Cyber Intelligence Analyst
- Incident Response Investigator
- Cyberforensic Investigator
- Computer Forensics Specialist
- Computer Forensics Technician

SYLLABUS

Module 1: Investigation Process, Procedures, and Protocol

- Investigating victims, witnesses, and suspects
- Investigating strategy for violations
- Conducting forensic analysis and investigations
- Data retrieval investigations
- Investigate and detect evidence
- Investigating computer network attack analysis
- Investigating the behaviour of individuals
- Investigating computer generated vulnerabilities
- Investigating the magnitude of threats
- Investigating crisis events
- Investigating crime scenes
- Establishing proof of crime in investigations
- Investigating computer-generated vulnerabilities
- Investigating evidence for conclusions

Syllabus

- Investigating and developing leads
- Investigating insider threats
- Investigating dynamics of attackers
- Reading individuals in investigations
- Investigating using scientific methods
- Investigating the dark web
- Investigating digital media
- Investigating data for trends
- Investigating a compromised system
- Investigating with a cyber defence toolkit
- Investigating hardware/software implications
- Investigative tools in detail
- Investigating suspect code
- Investigating volatile data
- Investigating an intrusion
- Investigating intrusions in their native environment
- Handle and manage events in investigations
- Investigating forensic artefacts
- Investigating with data carving techniques
- Investigating analysis of file systems
- Investigating static malware

Module 2: Evidence Procedures and Protocol

- Protecting evidence in investigations
- Investigating physical evidence
- Processing and tagging evidence
- Investigate, compile and preserve evidence utilized in the prosecution of computer crimes.
- Securing the source of info in investigations
- Documenting evidence in investigations
- Digital evidence protocol
- Evidence and the chain of custody
- Evidence integrity in investigations
- Investigating cyberforensic data
- Investigating anti-forensics
- Investigating diverse media
- Setting up forensic workstations for investigations
- Forensic tool suites in investigations
- Investigating hardware/software implication
- Investigating seized malicious code
- Backing up evidence in investigations
- Decrypting seized evidentiary data
- Summarizing findings in investigations

- Evidence and the chain of custody
- Execute real-time forensic analysis in investigations
- Analysing timelines in investigations
- Technical assistance in investigations
- Investigating suspect network traffic
- Investigating with a cyber defence toolkit
- Investigating an intrusion
- Investigating information sources

Module 3: Legalities, Prosecution and Court Procedures

- Furnish criminal investigative assistance to the trial counsel during the judicial process
- Investigating security events
- Team relationships in investigations
- Documenting the investigation
- Privacy and cybersecurity in investigations
- Admissibility in investigations
- Digital Evidence Protocol
- Awareness of the legalities with regards to cyber/digital evidence in investigations.

- Awareness of court protocol and legalities of evidence from investigations.
- Investigation protocol
- Presenting evidence from investigations
- Judicial process
- Investigating exploitation and cyber targeting
- Investigating conflicts in procedure
- Constitutional issues in investigations
- Organizational cyber policy in investigations
- Digital Evidence Laws and Protocol
- Assisting law enforcement in investigations
- Disseminating investigation information
- Cyber defence recommendations

Module 4: Skills and Knowledge that a Certified Cybercrime Investigator Will Have

- Networking in investigations
- Risk management in investigations
- Investigating intrusions
- Investigating threats and vulnerabilities
- Investigating adversarial behaviour
- Investigating devices

Syllabus

- Investigating covert communication
- Using scripts for/in investigations
- Reverse engineering in investigations
- Processing cyber forensic info in investigations
- Operating systems in investigations
- Server diagnostics and fault identification in investigations.
- Computer parts and architectures in investigations
- Investigating different file systems
- Investigating with hacking
- Persistent data in investigations
- Investigating system files
- Deployable forensics in investigations
- Hardening techniques in investigations
- Network security architecture theories in investigations
- Data carving in investigations
- Forensics labs and support apps in investigations
- Debugging protocol/tools in investigations
- Malware analysis in investigations
- Investigating and understanding malware

Syllabus

- Obfuscation in investigations
- Application security risks in investigations
- Network infrastructure recovery in investigations
- Contingency plans for investigations
- Packet-level analysis in investigations
- Analysing memory dumps in investigations
- System manipulation and handling in investigations
- Virtual machines in investigations
- Binary analysis utilities in investigations
- One-way hash functions in investigations
- Debugger results in investigations
- File signature analysis in investigations
- Hash comparisons in investigations
- Analysing static media in investigations
- Malware analysis in investigations
- Imaging digital media in investigations
- Investigating digital media
- Windows registry analysis in investigations
- Image processing in investigations
- Processing evidence
- Cyber defence reports in investigations

Module 5: Cyberforensics Evidence

- Preservation of cyber forensics evidence
- Preparation of cyberforensics evidence
- Packaging and storage of cyberforensics evidence
- Collecting evidence for cybercrimes
- Evidence collection, equipment, and bags

Module 6: Technology and Troubleshooting

- Investigating viruses and malware infected documents
- Investigating malware in mobile phones

Module 7: Cybercrime and Mobile Phones (7)

- Investigating threats using mobile phones
- Tracking GPS location and cell tower location in mobile threats
- Spying on children using mobile agents and spyware
- Investigating cybercrimes committed using a mobile phone
- Decrypting data stored in mobile phones
- Eavesdropping on a live mobile phone call

Module 8: Cybercrime, Cyberforensics, and The Law

- Reporting cybercrime to law enforcement agencies
- Investigating defamation of a person's good character in the cyber world
- International Cybercrime Laws
- Investigating credit card fraud
- Chain of custody
- Cyberforensics concepts and theories
- How to conduct cyberforensics investigations
- Creating and managing a cyberforensics lab in organizations
- Cyberforensics tools, devices, and technologies
- Investigating cyberforensic crimes committed with USB, hard disks, and media analysis
- Cybercrime prosecution steps and procedures
- Cybercrime extradition treaty
- Setting up a police cyber cell unit
- Setting up honeypots and entrapments to capture cyber criminals
- Setting up of cybercrime taskforces
- Investigating denial-of-service attacks
- Identifying cyber criminals hiding behind VPNs and proxy servers
- The role of cyberforensics in virtualization
- Reverse tracking an IP address to locate a cyber criminal

Syllabus

- Investigating pornographic images on laptops, computers, and mobile phones
- Investigating child pornography crimes
- Use of cyberforensics in criminal cases
- Cyberforensics and image analysis
- How to obtain arrest warrants to capture a cybercriminal
- Expert witnesses in cyberforensics
- Court procedures with regards to prosecution
- Best practices to be followed in cyberforensics
- Ethical code of a cybercrime investigator
- How to setup a cybercrime and cyberforensics awareness website
- Creating awareness about cybercrime among the public
- How to trace stolen phones, laptops, and computers
- Various types of cybercrimes
- Investigating theft of corporate data
- Investigating software piracy and theft
- Investigating cyber stalking
- Investigating cyber fraud in accounting systems
- Investigating money laundering
- Investigating election tampering
- Investigating computer crimes using extortion
- Investigating cyber bullying
- Investigating cyber sexual harassment
- Investigating breach of contract

Module 9: Investigating Various Types of Espionage

- Investigating cyber espionage
- Investigating corporate espionage
- Investigating government espionage

Module 10: Understanding Surveillance (Techniques and Tools)

- Investigating cameras, recording devices, scanners, and other electronics used in surveillance
- Analyzing and investigating footage from a surveillance camera
- Investigating instant messaging phone calls, messages, photographs
- Investigating email messages
- Identifying and investigating bugs planted in offices
- Investigating the authenticity of a recorded conversation
- Investigating videos uploaded to Youtube

Module 11: Crimes Committed using Technology

- Investigating threats using internet-of-things
- Investigating crimes committed using embedded systems
- Investigating network intrusions
- Investigating intrusions using digital locks
- Investigating crimes committed using Bluetooth
- Investigating hijacking of social media accounts
- Investigating hijacking of email accounts
- Investigating DNS intrusions
- Investigating crimes committed using satellite tracking systems
- Investigating phishing attacks
- Investigating hacking of GPS systems in vehicles
- Investigating computer crimes using Facebook
- Investigating computer crimes committed with ransomware
- Setting up of an incident response team
- Setting up and management of emergency response in organizations

Module 12: Cracking, Decrypting, and Encrypting

- Cracking passwords with the help of automated tools
- Cracking passwords in an iPhone
- Cracking biometrics authentication
- Cracking facial recognition authentication
- Decrypting data being transmitted over the network
- Cracking and decrypting password-protected word/excel documents
- Cracking and decrypting password-protected PDF documents
- Decrypting an encrypted email message
- Cracking two-factor authentication
- Investigating data encoded with steganography techniques

Module 13: Investigating System Logs and System Software

- Investigating web server audit logs
- Investigating intrusion detection system audit logs
- Investigating firewall audit logs
- Investigating Windows event viewer audit logs
- Investigating Linux syslog

- Investigating network logs
- Investigating browser data
- Investigating web browser history
- Investigating web browser cookies
- Investigating search engine history

Module 14: Investigating Electronic Communication

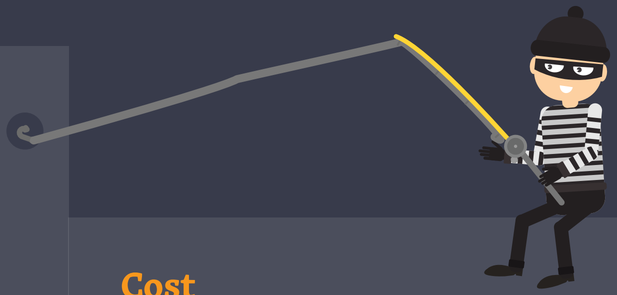
- Investigating Gmail messages
- Investigating Microsoft Outlook
- Investigating SMS messages
- Photography and image analysis
- Investigating email attachments
- Identifying the source of email messages, with geo-location
- Investigating fake news
- Investigating leakage of sensitive information in organizations

Module 15: Investigating Technology

- Investigating virtualization snapshot images
- Investigating virtualization hyper-VVHDs
- Investigating cloud firewalls

- Investigating Microsoft active directory
- Investigating and analyzing windows file systems
- Investigating and analyzing Linux file systems
- Investigating and analyzing MacOS file systems
- Investigating routers, switches, and gateways
- Managing centralized login systems
- Investigating digital printers, fax machines, and copier machines
- Investigating point-of-sale terminals
- Investigating cybercrime with desktops
- Investigating cybercrime with laptops
- Investigating cybercrime with tablets
- Investigating online scams
- Investigating and analyzing network traffic

What will be the course structure?



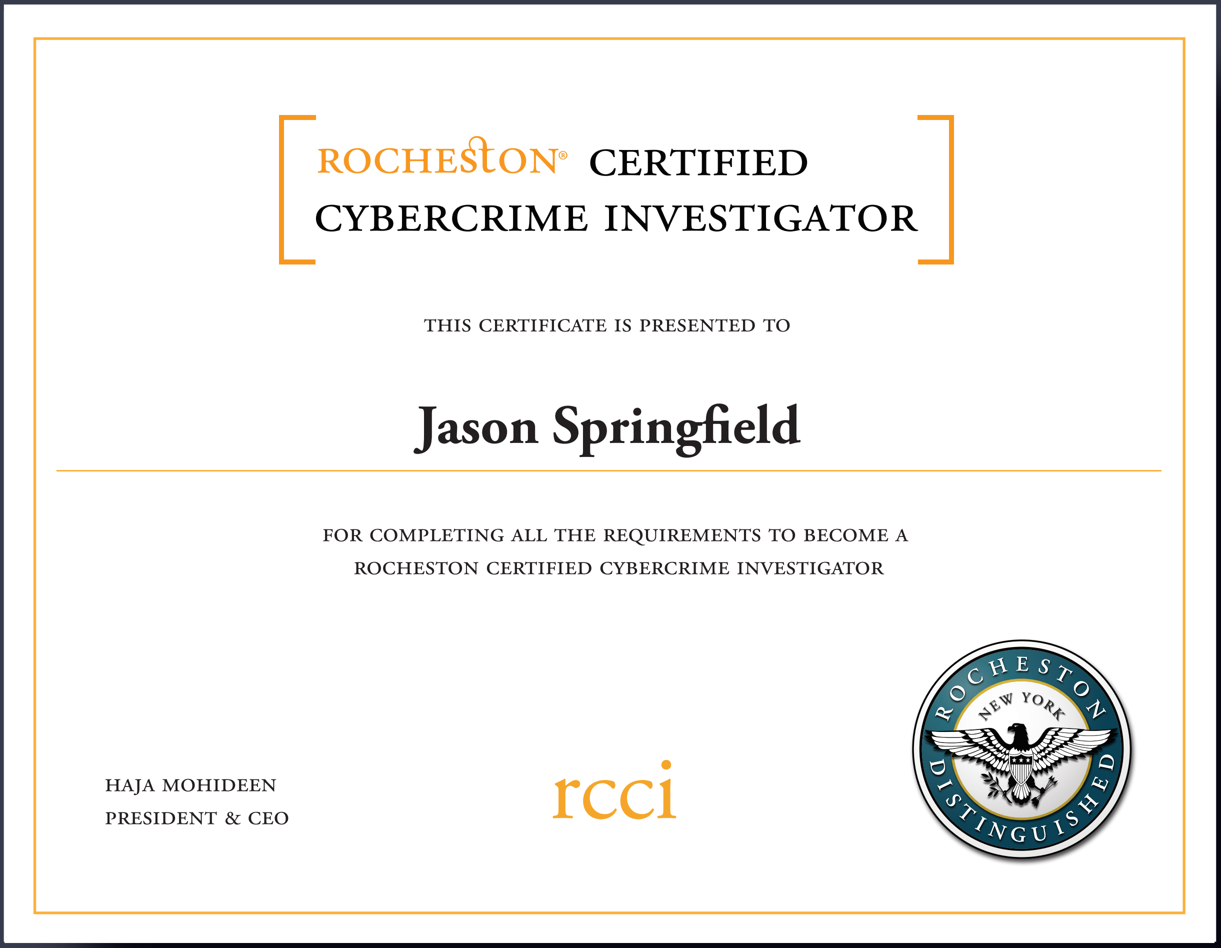
What the course will consist of:

- A 5-day Training Program
- Time: 9:30 AM – 6 PM
- The Provision of an Active Web Portal
- Seminars Conducted by Qualified Engineers
- Best in-class environment
- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.

Cost

For pricing in your region, please contact the local distributor.

RCCI Certificate



ROCHESTON® CERTIFIED
CYBERCRIME INVESTIGATOR

THIS CERTIFICATE IS PRESENTED TO

Jason Springfield

FOR COMPLETING ALL THE REQUIREMENTS TO BECOME A
ROCHESTON CERTIFIED CYBERCRIME INVESTIGATOR

HAJA MOHIDEEN
PRESIDENT & CEO

rcci

ROCHESTON
NEW YORK
DISTINGUISHED

ROCHESTON® CERTIFIED CYBERCRIME INVESTIGATOR

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON® CERTIFIED CYBERCRIME INVESTIGATOR

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON® CERTIFIED CYBERCRIME INVESTIGATOR

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON®

BE EXCEPTIONAL