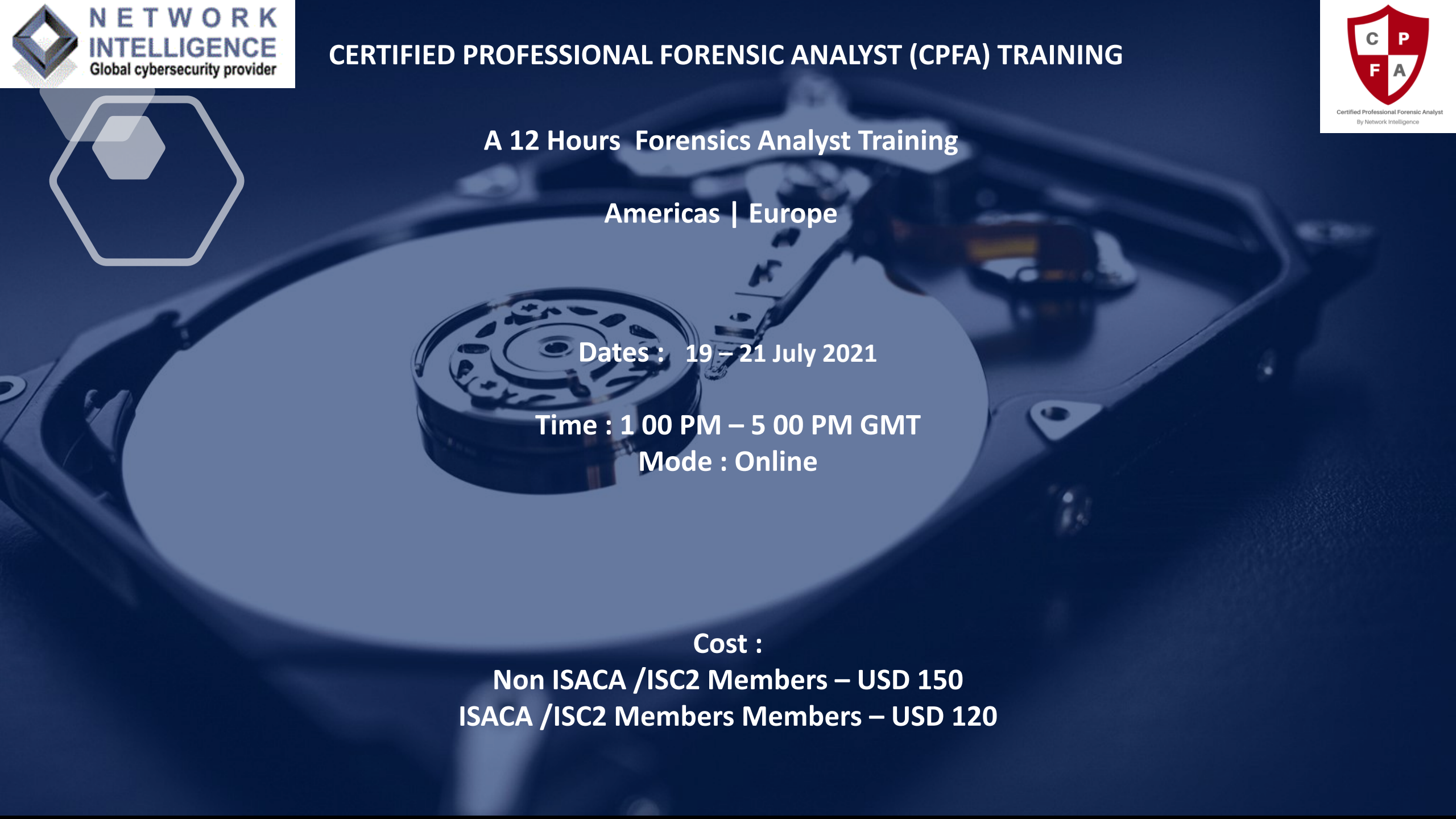
NETWORK INTELLIGENCE
Global cybersecurity provider

CERTIFIED PROFESSIONAL FORENSIC ANALYST (CPFA) TRAINING

Certified Professional Forensic Analyst
By Network Intelligence

A 12 Hours Forensics Analyst Training

Americas | Europe



Dates : 19 – 21 July 2021

Time : 1 00 PM – 5 00 PM GMT
Mode : Online

Cost :
Non ISACA /ISC2 Members – USD 150
ISACA /ISC2 Members Members – USD 120

Introduction

Cyber security threats continue to grow in volume and sophistication. While organizations are adopting the Work from home culture and getting adapted to the new normal, the WFH has significantly increased the attack surface which attackers are taking advantage of to target organizations.

Recently, many organizations have been targeted for ransomware attacks and data breaches, which have significantly impacted their businesses. In such circumstance's organizations need to adopt practices that allow them to rapidly identify, respond to, and mitigate these types of incidents while becoming more resilient and protecting against future incidents.

Whether your data has been compromised by a cyber-attack or your files encrypted by a cyber-crime like ransomware, it is important to know how the incident happened in your network, how to contain the incident, how to reduce the cost of the incident and at the same time how to quickly recover from the incident. Organizations also need to conduct post-incident analysis and forensics analysis to gather digital evidence which can be held in the court of law to bring the attackers to justice.

Importance Of Incident Response & Digital Forensics

Protecting your data from falling in the wrong hands or being held for ransom, protecting your reputation, customer's trust & loyalty, protecting your revenue and assisting law enforcement agencies are some critical reasons why organizations need to conduct forensic analysis and have a strong incident response plan today.

Incident response strategies and plans layout what defines a breach, the roles and responsibilities of the CSIRT (Cyber Security Incident Response) team, tools for managing a breach, steps that will need to be taken to address a security incident, how the incident will be investigated and communicated, and the notification requirements following a data breach.

Why CPFA ?

The term cyber-crime no longer refers only to hackers and other external attackers. Almost all cases of financial fraud or employee misuse involves a very strong element of computer-based evidence.

The Certified Professional Forensics Analyst (CPFA) training is focused on comprehensive coverage of all aspects of digital forensics and incident response. It is designed to ensure that all aspects have a real-life scenario-based approach explaining start to end of digital forensics investigation, incident detection and response.

Objectives

- What should one do when there is a suspicion of a computer-based crime?
- What tools and techniques are most likely to yield the right set of clues?
- What is the procedure to deal with incident response and remediation?
- How should the investigation be carried out such that it can be presented in a court of law?
- Demonstration with the worlds' leading forensics tool – Encase

This Course Is Best For :

- Chief Security Officers, Chief Technology Officers, Chief Information Officers.
- Security practitioners and managers.
- Auditors and Fraud Examiners.
- Anyone interested in computer forensics and cyber-crime investigations.

The CPFA program is a hands-on training experience with case studies to explain the digital forensics and incident response process in much detail.

In line with these objectives, we are pleased to announce a 3-day 4-hour online training on "Certified Professional Forensics Analyst (CPFA)

Certified Professional Forensic Analyst (CPFA) Training

Course Content

Session 1: Computer Crimes & Case Studies

- Hacking Incidents
- Financial Theft
- Identity Theft
- Corporate Espionage
- Email Misuse
- Case Studies

Session 2: Introduction to Incident Response

- Pre-incident Preparation
- Detection of Incidents
- Initial Response Phase
- Response Strategy Formulation
- Incident Management Process
- Writing An Incident Response Plan
- Incident Response Runbooks
- SIEM Use Cases – Kill Chain

Session 3: Digital Forensics

- Introduction to Digital Forensic
- Chain of Custody
- Evidence Collection & Analysis
- The 6 A's of Digital Forensics
- Network Forensics
- Live Forensics
- Windows Live Response
- Linux Live response
- Browser Forensics

Session 4: Forensic Imaging

- Introduction to Imaging
- Importance of Imaging
- Integrity of the Evidence
- Disk Imaging using Encase / FTK
- Write Blockers
- Memory Analysis
- Tools for Acquiring RAM Dump
- Volatility Framework
- Email Forensics
- Introduction to Steganography

Session 5: Finding IOC's & Forensic Report Writing

- Gathering Indicators of Compromise (IOC's)
- Report Writing Skills
- Sample Report
- Common Mistakes in Reports

Examination – The participants would need to undergo an online examination after the training. On successfully clearing the examination, the participant would be awarded with the CPFA certificate

"Remember….. you are the Centre of Security"

NETWORK INTELLIGENCE
Global cybersecurity provider

Lead Trainer

KK Mookhey,
Founder & CEO
Network Intelligence

KK provides the vision and direction for the company and has steered it from a one-man consulting firm started in 2001 to a global cybersecurity firm with an expansive portfolio of services. A technologist at heart, he enjoys dealing with complex security problems and developing solutions to client challenges. He is a qualified PCI QSA, CISA and CISSP.

Lionel Faleiro,
Practice Lead - Forensics
Network Intelligence

Lionel is passionate about training and working in DFIR. He comes with an experience of almost 10 years in IT and Cybersecurity. He began as a SysAdmin then a Security Trainer and now leads the Forensic Practice at the firm. He has solved numerous cases during his tenure at Network Intelligence and is an avid gamer as well.