Upon completion of the training, the participant would have an in-depth knowledge of the Digital forensics and incident response, its importance and implementation. The 12 hours of online course is spread across 3 days 4 hours each which includes 11 hours of training session followed by 1-hour online examination Below is the Table of Contents for the training. Below is the course outline of the training for your reference.

<table>
<tr><th colspan="2">3 Days (Professional Forensics Analyst (CPFA) Training Course</th></tr>
<tr><td>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</td><td>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</td></tr>
<tr><td>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</td><td>Session 5: Finding IOC’s & Forensic Report Writing
Gathering Indicators of Compromise (IOC’s)
Report Writing Skills
Sample Report
Common Mistakes in Reports</td></tr>
</table>