Global Horizon
TRAINING CENTER

Training Course:
FOCAL POINT - ENDPOINT LIVE FORENSICS

17 - 21 March 2025
Kuala Lumpur (Malaysia)
Royale Chulan Kuala Lumpur

Training Course:
FOCAL POINT - ENDPOINT LIVE FORENSICS

Training Course code: IT235173 From: 17 - 21 March 2025 Venue: Kuala Lumpur (Malaysia) - Royale Chulan Kuala Lumpur Training Course Fees: 5775 Euro

Introduction

In today's digital landscape, the ability to conduct real-time forensic analysis on endpoints is critical for organizations to proactively respond to security incidents and mitigate potential threats. Focal Point - Endpoint Live Forensics is a comprehensive training program designed to equip cybersecurity professionals, digital forensic investigators, IT administrators, and incident response teams with the essential skills and knowledge needed to perform live forensics on endpoints effectively.

Objectives

Upon completing this 5-day training program, participants will:

- Understand Live Forensics: Gain a deep understanding of live forensics, its principles, and how it differs from traditional forensics.
- Legal and Ethical Proficiency: Familiarize themselves with the legal and ethical considerations involved in live endpoint forensics, ensuring compliance with relevant laws and ethical standards.
- Tools and Software Mastery: Become proficient in the use of live forensics tools and software, allowing for effective data acquisition and analysis.
- Endpoint Identification and Collection: Learn to identify and collect data from target endpoints, ensuring a systematic and secure approach.
- Secure Environment Setup: Establish a secure forensic environment to prevent contamination of evidence and maintain the chain of custody.
- Documentation Skills: Develop strong documentation skills for maintaining a clear and credible chain of custody throughout the investigative process.
- RAM Acquisition and Analysis: Acquire and analyze volatile memory to identify running processes and uncover potential threats.
- Live Data Acquisition Techniques: Master techniques for collecting live data without altering the system, ensuring minimal disruption.
- Process Analysis: Identify and analyze suspicious processes to isolate and contain threats effectively.
- File System Investigation: Gain expertise in examining file systems, recovering deleted files, and handling encrypted data.
- Forensic Reporting: Create comprehensive forensic reports that effectively communicate findings to stakeholders.
- Best Practices and Future Trends: Embrace best practices in live endpoint forensics and stay informed about emerging trends and technologies.

Target Audience

This training program is designed for the following professionals:

- Cybersecurity Professionals: Security analysts, engineers, and managers responsible for endpoint security and incident response.
- Digital Forensic Investigators: Professionals involved in digital forensic investigations, including those who need to extend their skills to live endpoint forensics.
- IT Administrators: System administrators and IT staff responsible for maintaining and securing endpoint devices.
- Incident Response Teams: Members of incident response teams looking to enhance their ability to assess and mitigate security incidents in real time.
- Any individuals interested in acquiring in-depth knowledge and skills in endpoint live forensics to enhance their career prospects in the field of cybersecurity and digital forensics.

Training Program Outline

Day 1: Introduction and Fundamentals

- Course Overview and Objectives
- What is Live Forensics?
- Legal and Ethical Considerations
- Live Forensics Tools and Software
- Setting Up a Forensic Environment

Day 2: Live Data Acquisition

- Endpoint Identification and Collection
- Secure Environment Setup
- Documentation and Chain of Custody
- RAM Acquisition and Analysis
- Live Data Acquisition Techniques

Day 3: Investigating Active Processes

- Identifying Suspicious Processes
- Isolating and Containing Threats
- File System Basics NTFS, Ext4, HFS+
- Live File System Analysis

Day 4: File System Investigation

- Recovering Deleted Files
- Handling Encrypted Files
- Practical Exercises: Analyzing Real-Life Scenarios

Day 5: Reporting and Final Assessments

- Creating Forensic Reports
- Best Practices and Future Trends

Registration form on the Training Course:
FOCAL POINT - ENDPOINT LIVE FORENSICS

Training Course code: IT235173 From: 17 - 21 March 2025 Venue: Kuala Lumpur (Malaysia) - Royale Chulan Kuala Lumpur Training Course Fees: 5775 Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

☐ Please find enclosed a cheque made payable to Global Horizon

☐ Please invoice me

☐ Please invoice my company

Easy Ways To Register

Telephone: +201095004484 to provisionally reserve your place.	Fax your completed registration form to: +20233379764	E-mail to us : info@gh4t.com or training@gh4t.com	Complete & return the booking form with cheque to:Global Horizon 3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.