Training Course on Developing Custom Forensic Tools

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the rapidly evolving landscape of cyber threats, traditional digital forensic tools often fall short in addressing the complexities of novel attack vectors, emerging technologies, and proprietary systems. Digital forensics professionals increasingly encounter unique challenges that demand tailored solutions beyond the capabilities of off-the-shelf software. Training Course on Developing Custom Forensic Tools empowers participants with the essential programming, scripting, and analytical skills to design, implement, and deploy specialized forensic utilities. By mastering these advanced techniques, investigators can overcome evidentiary bottlenecks, expedite incident response, and unlock deeper insights from complex digital artifacts, ensuring the integrity and admissibility of evidence in legal proceedings.

This course focuses on practical, hands-on application of programming concepts to real-world forensic scenarios. Participants will delve into the underlying mechanisms of operating systems, file systems, and network protocols to identify areas where custom tools can provide a distinct advantage. Emphasizing **Python scripting, reverse engineering, memory forensics, and artifact parsing**, the curriculum is designed to equip forensic examiners, incident responders, and cybersecurity researchers with the ability to innovate and adapt their investigative methodologies to combat sophisticated cybercrime, insider threats, and data breaches effectively. The skills acquired will significantly enhance an organization's capacity for proactive risk management and robust digital evidence acquisition.

Programme Curriculum

Training Course on Developing Custom Forensic Tools

Introduction

In the rapidly evolving landscape of cyber threats, traditional digital forensic tools often fall short in addressing the complexities of novel attack vectors, emerging technologies, and proprietary systems. Digital forensics professionals increasingly encounter unique challenges that demand tailored solutions beyond the capabilities of off-the-shelf software. Training Course on Developing Custom Forensic Tools empowers participants with the essential programming, scripting, and analytical skills to design, implement, and deploy specialized forensic utilities. By mastering these advanced techniques, investigators can overcome evidentiary bottlenecks, expedite incident response, and unlock deeper insights from complex digital artifacts, ensuring the integrity and admissibility of evidence in legal proceedings.

This course focuses on practical, hands-on application of programming concepts to real-world forensic scenarios. Participants will delve into the underlying mechanisms of operating systems, file systems, and network protocols to identify areas where custom tools can provide a distinct advantage. Emphasizing **Python scripting, reverse engineering, memory forensics, and artifact parsing**, the curriculum is designed to equip forensic examiners, incident responders, and cybersecurity researchers with the ability to innovate and adapt their investigative methodologies to combat sophisticated cybercrime, insider threats, and data breaches effectively. The skills acquired will significantly enhance an organization's capacity for proactive risk management and robust digital evidence acquisition.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Identify gaps in commercial forensic tools and pinpoint specific scenarios requiring custom solutions, particularly in **cloud forensics** and **IoT forensics**.
2. Develop proficiency in Python programming for automating forensic tasks, data parsing, and report generation, including advanced **data visualization** techniques.
3. Comprehend the structure and metadata of various file systems (NTFS, EXT4, APFS) to develop tools for advanced **file carving** and **data recovery**.
4. Write custom scripts to extract and analyze volatile data from RAM, focusing on **malware analysis** and **process analysis**.
5. Create specialized utilities for **packet analysis**, protocol dissection, and **network anomaly detection**.
6. Design and build tools to efficiently parse, filter, and correlate large volumes of log data for **threat hunting** and **incident detection**.
7. Develop parsers for proprietary or undocumented digital artifacts from applications, operating systems, and **mobile devices**.
8. Utilize basic reverse engineering techniques to understand the functionality of unknown programs and extract forensic artifacts.
9. Implement best practices for data acquisition, hashing, and chain of custody to maintain the admissibility of digital evidence.
10. Leverage existing open-source forensic libraries and frameworks to accelerate custom tool development.
11. Develop tools to acquire and analyze data from cloud environments, including **SaaS and IaaS platforms**.
12. Design tools and techniques to detect and counter anti-forensic measures employed by adversaries.

13. Understand how to document and potentially share custom tools with the broader digital forensics community for collaborative advancement.

Organizational Benefits

- Faster and more targeted investigations into complex cyber incidents, minimizing dwell time and financial impact.
- Automation of repetitive forensic tasks, freeing up highly skilled analysts for more complex analytical work.
- Reduced reliance on expensive commercial tools by developing in-house solutions for specific needs.
- The ability to quickly develop tools for newly identified threats, proprietary systems, or unique data formats.
- Assurance of evidentiary integrity through custom tools designed with rigorous forensic principles.
- Enhanced capabilities to detect and investigate internal data exfiltration or intellectual property theft.
- Development of bespoke tools to proactively identify anomalies and indicators of compromise within their unique IT environments.
- Fostering an internal culture of innovation and expertise in digital forensics and tool development.

Target Audience

- Digital Forensic Investigators and Analysts
- Incident Response Team Members
- Cybersecurity Professionals and Engineers
- Security Operations Center (SOC) Analysts
- Law Enforcement and Government Agency Investigators
- IT Security Managers and Directors
- Software Developers with an interest in cybersecurity
- Academics and Researchers in Digital Forensics

Course Outline

Module 1: Introduction to Custom Tool Development & Python Fundamentals for Forensics

- Understanding the limitations of commercial tools and the need for custom solutions.
- Setting up the forensic development environment Python basics for scripting: data types, control flow, functions, and modules.
- Handling files and directories programmatically: reading, writing, and manipulating data.
- Introduction to command-line argument parsing for tool usability.
- **Case Study:** Developing a simple Python script to automatically hash all files in a directory for integrity verification.

Module 2: File System Forensics & Data Recovery

- Deep dive into file system structures: NTFS, EXT4, and APFS basics for forensic relevance.
- Identifying and parsing metadata: timestamps, file attributes, and deleted file entries.
- Implementing file carving techniques for various file types
- Developing tools to recover data from unallocated space and damaged file systems.
- Working with disk images (DD, E01) using Python libraries.

- **Case Study:** Building a custom Python script to carve deleted JPEG images from a raw disk image and extract their EXIF data.

Module 3: Memory Forensics Tooling

- Understanding volatile data and its importance in investigations.
- Techniques for memory acquisition (dumping RAM) and volatile data collection.
- Developing parsers for process lists, network connections, loaded modules, and open handles from memory dumps.
- Extracting sensitive information from live memory.
- Integrating with existing memory forensic frameworks
- **Case Study:** Creating a Python tool to extract a list of running processes and their associated network connections from a Windows memory dump to identify suspicious activity.

Module 4: Network Forensics Tool Development

- Fundamentals of network protocols (TCP/IP, HTTP, DNS) and their forensic significance.
- Capturing and analyzing network traffic using Python with libraries like Scapy or dpkt.
- Developing custom parsers for specific network protocols or application-layer data.
- Identifying and reconstructing data streams from packet captures.
- Implementing tools for network anomaly detection and traffic filtering.
- **Case Study:** Building a Python script to analyze a PCAP file, extract HTTP GET/POST requests, and identify potential data exfiltration attempts.

Module 5: Log Analysis & Timeline Reconstruction

- Understanding various log formats
- Developing robust parsers for different log sources using regular expressions and structured parsing.
- Correlating log entries across multiple systems to create comprehensive timelines.
- Automating the identification of suspicious events, authentication failures, and access patterns.
- Visualizing log data for better analytical insights.
- **Case Study:** Designing a Python tool to ingest Apache web server logs and generate a timeline of suspicious login attempts or unusual resource access.

Module 6: Artifact Parsing & Application Forensics

- Identifying common application artifacts
- Developing custom parsers for complex application-specific data structures.
- Extracting user activity, communication records, and system configurations.
- Analyzing mobile device artifacts and developing parsers for mobile applications.
- Handling encrypted or obfuscated application data
- **Case Study:** Creating a Python parser for a specific web browser's history database (e.g., SQLite) to extract visited URLs, download history, and search queries.

Module 7: Introduction to Reverse Engineering for Forensics

- Basic concepts of assembly language and processor architectures.
- Using disassemblers (e.g., IDA Pro Free, Ghidra) for static analysis of executables.
- Introduction to debuggers (e.g., x64dbg, WinDbg) for dynamic analysis.
- Identifying malicious functionality and hidden features in executables.
- Extracting strings, configuration data, and indicators of compromise (IOCs) from binaries.

- **Case Study:** Performing static analysis on a suspected malware sample to identify key functions, network communication patterns, and embedded strings.

Module 8: Advanced Topics, Best Practices & Legal Considerations

- Developing forensic tools for cloud environments
- Exploring IoT device forensics and custom tool needs for embedded systems.
- Implementing robust error handling, logging, and reporting mechanisms in custom tools.
- Ensuring tools adhere to legal and ethical guidelines for evidence admissibility.
- Future trends in digital forensics and the role of AI/ML in custom tool development.
- **Case Study:** Designing a conceptual framework and outlining the development steps for a custom tool to collect and analyze specific forensic artifacts from an AWS EC2 instance.

Training Methodology

This course employs a highly interactive and hands-on training methodology designed to foster practical skill development and critical thinking:

- **Interactive Lectures & Discussions:** Core concepts are delivered through engaging presentations, followed by open discussions to encourage knowledge sharing.
- **Live Demonstrations:** Instructors will showcase the development of custom tools step-by-step, explaining code and rationale.
- **Extensive Hands-on Labs:** Participants will spend a significant portion of the course working on practical exercises and coding challenges, applying learned concepts to real forensic scenarios.
- **Case Study Analysis:** Real-world digital forensic case studies will be dissected to highlight the necessity and application of custom tools.
- **Problem-Based Learning:** Participants will be presented with complex forensic problems that require the design and implementation of custom solutions.
- **Pair Programming & Group Exercises:** Collaborative learning opportunities to enhance problem-solving skills and teamwork.
- **Q&A and Troubleshooting Sessions:** Dedicated time for addressing participant queries and debugging code.
- **Project-Based Assessment:** A final project where participants develop a custom forensic tool to solve a specific challenge.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com