Training Course on Scripting for Digital Forensics and Incident Response Automation (Python, PowerShell)

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's rapidly evolving cyber threat landscape, organizations face an unprecedented volume and sophistication of cyberattacks. Traditional manual approaches to Digital Forensics and Incident Response (DFIR) are no longer sufficient to effectively combat these threats, leading to delayed investigations, increased dwell times, and significant financial and reputational damage. Training Course on Scripting for Digital Forensics and Incident Response Automation (Python, PowerShell) addresses this critical need by empowering cybersecurity professionals with advanced **scripting and automation skills** using **Python** and **PowerShell**. By harnessing the power of these versatile languages, participants will learn to streamline forensic data collection, automate incident triage, enhance threat hunting capabilities, and orchestrate rapid incident containment and remediation, ultimately building a more resilient and proactive security posture.

This intensive program delves into practical, hands-on applications, moving beyond theoretical concepts to equip participants with the ability to develop custom tools and scripts that directly address real-world DFIR challenges. From automating evidence acquisition across diverse endpoints to parsing complex log data and integrating with security orchestration platforms, this course emphasizes efficiency, accuracy, and scalability. Participants will gain the expertise to transform their DFIR workflows, minimizing human error, accelerating response times, and significantly improving an organization's ability to **detect, analyze, contain, and recover from cyber incidents** with unparalleled speed and precision.

Programme Curriculum

Training Course on Scripting for Digital Forensics and Incident Response Automation (Python, PowerShell)

Introduction

In today's rapidly evolving cyber threat landscape, organizations face an unprecedented volume and sophistication of cyberattacks. Traditional manual approaches to Digital Forensics and Incident Response (DFIR) are no longer sufficient to effectively combat these threats, leading to delayed investigations, increased dwell times, and significant financial and reputational damage. Training Course on Scripting for Digital Forensics and Incident Response Automation (Python, PowerShell) addresses this critical need by empowering cybersecurity professionals with advanced **scripting and automation skills** using **Python** and **PowerShell**. By harnessing the power of these versatile languages, participants will learn to streamline forensic data collection, automate incident triage, enhance threat hunting capabilities, and orchestrate rapid incident containment and remediation, ultimately building a more resilient and proactive security posture.

This intensive program delves into practical, hands-on applications, moving beyond theoretical concepts to equip participants with the ability to develop custom tools and scripts that directly address real-world DFIR challenges. From automating evidence acquisition across diverse endpoints to parsing complex log data and integrating with security orchestration platforms, this course emphasizes efficiency, accuracy, and scalability. Participants will gain the expertise to transform their DFIR workflows, minimizing human error, accelerating response times, and significantly improving an organization's ability to **detect, analyze, contain, and recover from cyber incidents** with unparalleled speed and precision.

Course Duration

5 days

Course Objectives

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

1. Automate Digital Forensics processes using Python and PowerShell scripting.
2. Develop scripts for efficient incident response (IR) and threat hunting.
3. Implement automated data acquisition from various endpoints (Windows, Linux, macOS).
4. Parse and analyze forensic artifacts including logs, memory dumps, and disk images.
5. Create custom tools for malware analysis automation and indicator of compromise (IOC) extraction.
6. Orchestrate incident containment and eradication actions through scripting.
7. Integrate scripting with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.
8. Utilize PowerShell for live response and Windows forensic investigations.
9. Apply Python for advanced data analysis and visualization in DFIR.
10. Develop cross-platform automation scripts for diverse IT environments.
11. Enhance evidence preservation and chain of custody through automated procedures.
12. Build a foundational understanding of API integrations for DFIR tool interaction.
13. Leverage scripting for proactive security measures and vulnerability assessment automation.

Organizational Benefits

- Automate repetitive tasks, leading to faster detection, analysis, and containment of cyber incidents.
- Minimize human error in forensic investigations and incident response procedures.
- Efficiently handle a larger volume of incidents and data across diverse IT infrastructures.

- Free up highly skilled DFIR professionals to focus on complex analysis and strategic initiatives.
- Develop automated scripts to continuously monitor for anomalous activities and emerging threats.
- Improve overall organizational resilience against cyberattacks through rapid and effective response capabilities.
- Reduce the financial impact of breaches by accelerating recovery and minimizing downtime.
- Ensure meticulous and consistent collection of digital evidence for legal and compliance purposes.

Target Audience

1. Incident Responders.
2. Digital Forensics Analysts.
3. Security Operations Center (SOC) Analysts
4. Cybersecurity Engineers.
5. IT Administrators.
6. Threat Hunters
7. Penetration Testers
8. Security Consultants

Course Outline

Module 1: Introduction to DFIR Automation & Scripting Fundamentals

- Understanding the need for automation in modern DFIR workflows.
- Introduction to Python and PowerShell for cybersecurity applications.
- Setting up the DFIR scripting environment
- Basic scripting concepts: variables, data types, control flow, functions.
- **Case Study:** Automating basic file system artifact collection on a suspect workstation using a simple Python script.

Module 2: Automated Data Acquisition & Evidence Preservation

- Scripting disk imaging and volatile data collection
- Automating evidence integrity verification
- Collecting network connection data and open ports with PowerShell.
- Scripting remote data acquisition from multiple endpoints.
- **Case Study:** Developing a PowerShell script to automatically collect system information, running processes, and network connections from 100 Windows servers, ensuring hash verification of collected data.

Module 3: Log Analysis Automation

- Parsing and normalizing various log formats (Windows Event Logs, Syslog, Apache, IIS) using Python.
- Filtering and searching large log datasets for specific events or IOCs.
- Automating correlation of logs from different sources to identify attack patterns.
- Developing scripts to ingest log data into analytical tools or SIEM platforms.
- **Case Study:** Building a Python script to parse firewall logs, identify anomalous outbound connections, and alert the SOC team via API integration.

Module 4: Process & Memory Forensics Automation

- Automating memory acquisition and analysis using tools like Volatility and PowerShell.
- Scripting the extraction of running processes, loaded DLLs, and network sockets from memory dumps.
- Identifying hidden or malicious processes through automated anomaly detection.
- Extracting credentials and sensitive data from memory using custom Python scripts.
- **Case Study:** Using Python and Volatility to automatically scan memory images for known malware signatures and extract suspicious process command lines.

Module 5: File System & Registry Forensics Automation

- Scripting the analysis of file system artifacts (MFT, prefetch, jump lists).
- Automating Windows Registry analysis for persistence mechanisms and configuration changes.
- Identifying recently accessed files and programs.
- Developing scripts to extract metadata and categorize files based on type or content.
- **Case Study:** Creating a PowerShell script to enumerate common persistence locations in the Windows Registry and generate a report of suspicious entries for review.

Module 6: Malware Analysis & IOC Extraction Automation

- Automating static and dynamic malware analysis sandbox interactions.
- Scripting the extraction of IOCs (hashes, domains, IPs, file paths) from suspicious samples.
- Developing Python scripts to interact with threat intelligence platforms for IOC enrichment.
- Automating YARA rule creation and application for malware detection.
- **Case Study:** Building a Python-based pipeline that takes a suspicious file, submits it to a sandbox for analysis, extracts IOCs from the sandbox report, and pushes them to a threat intelligence platform.

Module 7: Incident Containment & Remediation Automation

- Scripting network isolation and host quarantine actions using PowerShell.
- Automating account disablement and password resets.
- Developing scripts for automated file deletion and patch deployment.
- Orchestrating multi-step remediation playbooks using scripting.
- **Case Study:** Implementing a PowerShell script that, upon detection of a specific ransomware activity, automatically isolates the infected host, disables the compromised user account, and triggers a system rollback.

Module 8: Advanced DFIR Scripting & Integrations

- Working with REST APIs for integrating with SIEM, SOAR, and other security tools.
- Developing custom forensic tools and utilities with Python and PowerShell.
- Error handling, logging, and best practices for robust DFIR scripts.
- Exploring advanced topics like cloud forensics automation and machine learning applications in DFIR.
- **Case Study:** Designing and implementing a Python script that integrates with a SOAR platform to automatically enrich an incident alert with threat intelligence data, then initiates a PowerShell script to collect relevant forensic artifacts from the affected endpoint.

Training Methodology

This training course employs a highly **interactive and hands-on methodology**, combining theoretical concepts with extensive practical application. Key components include:

- **Instructor-Led Sessions:** Engaging lectures and demonstrations by experienced DFIR and scripting experts.
- **Hands-on Labs:** Practical exercises and real-world scenarios performed in a dedicated lab environment, allowing participants to write and execute scripts.
- **Case Studies:** In-depth analysis of real-world cyber incidents and how scripting solutions can be applied.
- **Live Coding Demonstrations:** Instructors will walk through the process of building scripts from scratch.
- **Group Discussions & Problem Solving:** Collaborative sessions to discuss challenges and share solutions.
- **Practical Assignments:** Take-home exercises to reinforce learning and encourage independent practice.
- **Q&A Sessions:** Dedicated time for participants to ask questions and clarify concepts.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
03 Aug 2026	07 Aug 2026	Online	$1,100
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100

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

Register Online Now

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