# Training Course on Automating Forensic Artifact Collection

Professional Development Training Course Outline

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

## Course Introduction

**Introduction**

In the rapidly evolving landscape of cybersecurity, the sheer volume and complexity of digital investigations demand more efficient and scalable solutions. Traditional manual methods of forensic artifact collection are increasingly proving time-consuming, prone to human error, and inadequate for large-scale incidents or proactive threat hunting. Training Course on Automating Forensic Artifact Collection is meticulously designed to empower digital forensic investigators, incident responders, and security analysts with the cutting-edge skills to automate evidence acquisition across diverse endpoints and cloud environments. Participants will learn to leverage scripting, open-source tools, and commercial platforms to streamline the collection process, ensuring comprehensive, consistent, and forensically sound data acquisition at an unparalleled speed.

This intensive program goes beyond basic scripting, delving into advanced techniques for orchestrated artifact gathering, remote acquisition, and integration with existing security information and event management (SIEM) systems and threat intelligence platforms. By mastering automation, attendees will significantly reduce investigation timelines, enhance the accuracy of their findings, and free up valuable human resources to focus on critical analysis rather than repetitive collection tasks. Elevate your forensic capabilities by transforming your approach to evidence collection from reactive and manual to proactive and automated, positioning your organization at the forefront of digital defense.

# Programme Curriculum

## Training Course on Automating Forensic Artifact Collection

### Introduction

In the rapidly evolving landscape of cybersecurity, the sheer volume and complexity of digital investigations demand more efficient and scalable solutions. Traditional manual methods of forensic artifact collection are increasingly proving time-consuming, prone to human error, and inadequate for large-scale incidents or proactive threat hunting. Training Course on Automating Forensic Artifact Collection is meticulously designed to empower digital forensic investigators, incident responders, and security analysts with the cutting-edge skills to automate evidence acquisition across diverse endpoints and cloud environments. Participants will learn to leverage scripting, open-source tools, and commercial platforms to streamline the collection process, ensuring comprehensive, consistent, and forensically sound data acquisition at an unparalleled speed.

This intensive program goes beyond basic scripting, delving into advanced techniques for orchestrated artifact gathering, remote acquisition, and integration with existing security information and event management (SIEM) systems and threat intelligence platforms. By mastering automation, attendees will significantly reduce investigation timelines, enhance the accuracy of their findings, and free up valuable human resources to focus on critical analysis rather than repetitive collection tasks. Elevate your forensic capabilities by transforming your approach to evidence collection from reactive and manual to proactive and automated, positioning your organization at the forefront of digital defense.

### Course Duration

5 Days

### Course Objectives

1. Master Automated Acquisition Principles: Understand the core concepts and methodologies behind automated forensic collection.
2. Develop Custom Collection Scripts: Create and deploy robust scripts for targeted artifact acquisition using Python, PowerShell, or Bash.
3. Utilize Open-Source Automation Tools: Proficiency in tools like Velociraptor, KAPE, OSQuery, and their application in automated forensics.
4. Implement Remote Collection Strategies: Execute forensically sound artifact collection from remote endpoints across networks.
5. Orchestrate Large-Scale Data Collection: Design and manage automated collection workflows for hundreds or thousands of endpoints.

6. Integrate with SIEM & SOAR Platforms: Connect automated collection pipelines with existing security operational tools.
7. Handle Diverse Operating Systems: Automate collection from Windows, Linux, macOS, and cloud environments.
8. Automate Cloud Artifact Collection: Develop strategies for acquiring forensic data from AWS, Azure, and GCP.
9. Ensure Forensic Soundness & Integrity: Maintain chain of custody and data integrity during automated processes.
10. Mitigate Anti-Forensics in Automation: Identify and counter techniques designed to hinder automated collection.
11. Develop Proactive Threat Hunting Scripts: Create automated routines for continuous monitoring and early threat detection.
12. Containerize & Deploy Automation Tools: Utilize Docker/Kubernetes for scalable and consistent deployment of collection agents.
13. Measure & Optimize Automation Performance: Evaluate the efficiency and effectiveness of automated collection workflows.

**Organizational Benefits**

1. Reduced Investigation Timelines: Significantly decrease the time required for data collection in incidents.
2. Enhanced Scalability: Ability to collect artifacts from vast numbers of endpoints simultaneously.
3. Improved Data Consistency: Standardized collection processes reduce human error and ensure uniformity.
4. Cost Efficiency: Lower operational costs by automating repetitive and time-consuming tasks.
5. Faster Incident Response: Quicker data acquisition leads to more rapid threat containment and remediation.
6. Proactive Threat Detection: Enable continuous monitoring and early identification of malicious activities.
7. Resource Optimization: Free up skilled analysts to focus on complex analysis rather than collection.
8. Comprehensive Coverage: Ensure no critical artifacts are missed during investigations.
9. Compliance & Audit Readiness: Maintain well-documented and consistent collection procedures.
10. Competitive Advantage: Position the organization as a leader in advanced forensic capabilities.

**Target Participants**

- Digital Forensic Investigators

- Incident Responders
- Security Operations Center (SOC) Analysts
- Threat Hunters
- Cybersecurity Engineers
- Security Architects
- IT Security Managers
- DevSecOps Engineers
- Malware Analysts
- Penetration Testers with defensive interests

**Course Outline**

**Module 1: Introduction to Automated Forensic Collection**

- **The Need for Automation:** Challenges of manual collection, benefits of automation.
- **Core Concepts:** Definition of forensic artifacts, types of data to collect.
- **Automation Methodologies:** Scripting, tools, and orchestration approaches.
- **Forensic Soundness in Automation:** Maintaining integrity, chain of custody, and admissibility.
- **Case Study: The Cost of Manual Collection in a Large Breach**

**Module 2: Scripting for Automated Collection (Python & PowerShell)**

- **Fundamentals of Python for Forensics:** File I/O, process interaction, data structures.
- **PowerShell for Windows Forensics:** WMI, event logs, registry access, and system commands.
- **Bash Scripting for Linux/macOS:** Common commands, piping, and system interactions.
- **Error Handling and Logging:** Robustness in automated scripts.
- **Case Study: Automating User Profile Artifact Collection**

**Module 3: Open-Source Tools for Artifact Automation**

- **Velociraptor:** Advanced endpoint visibility and collection framework.
- **KAPE (Kroll Artifact Parser and Extractor):** Targeted artifact collection and parsing.
- **OSQuery:** SQL-based operating system analytics for live forensics.
- **GRR Rapid Response:** Agent-based forensic collection and analysis.
- **Case Study: Deploying Velociraptor for Enterprise-Wide Hunts**

**Module 4: Remote & Network-Based Collection Automation**

- **Remote Execution Techniques:** PsExec, SSH, WinRM, and agent-based solutions.
- **Network Artifact Collection:** Automating packet capture, flow data, and proxy logs.
- **Centralized Collection Architectures:** Designing scalable infrastructure for remote acquisition.
- **Security Considerations for Remote Access:** Secure channels, authentication, and authorization.
- **Case Study: Remotely Collecting Evidence from Dozens of Compromised Servers**

**Module 5: Cloud Forensic Artifact Automation**

- **AWS CloudTrail & GuardDuty Automation:** Collecting logs and security findings.

- **Azure Log Analytics & Sentinel Integration:** Automating data collection from Azure services.
- **GCP Logging & Security Command Center:** Scripting for Google Cloud Platform artifact acquisition.
- **Serverless Functions for Collection:** AWS Lambda, Azure Functions for event-driven collection.
- **Case Study: Automating Collection from a Compromised Cloud Instance**

**Module 6: Orchestration & Integration with Security Platforms**

- **SOAR (Security Orchestration, Automation, and Response) Integration:** Playbooks for automated collection.
- **SIEM (Security Information and Event Management) Feeds:** Sending collected data to Splunk, ELK, etc.
- **API-Driven Automation:** Interacting with security tools via their APIs.
- **Workflow Design for Incident Response:** Automating the full cycle from alert to initial collection.
- **Case Study: Building an Automated Ransomware Incident Response Playbook**

**Module 7: Advanced Automation & Anti-Forensics Mitigation**

- **Memory Acquisition Automation:** Automated RAM capture and analysis.
- **Container & Orchestration Forensics:** Docker, Kubernetes artifact collection.
- **Identifying & Bypassing Anti-Forensic Techniques:** Rootkits, wipers, obfuscation.
- **Automated Timeline Creation:** Generating event timelines from collected artifacts.
- **Case Study: Automated Response to a Sophisticated APT Attack**

**Module 8: Best Practices & Future Trends**

- **Testing and Validation of Automation Scripts:** Ensuring reliability and accuracy.
- **Maintenance & Version Control:** Managing automated collection tools and scripts.
- **Legal & Ethical Considerations in Automation:** Data privacy, scope, and consent.
- **Emerging Technologies:** AI/ML in forensic automation, blockchain for integrity.
- **Case Study: Implementing a Continuous Forensic Monitoring Program**

**Training Methodology**

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.com 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 |
|---|---|---|---|
| **07 Sep 2026** | 11 Sep 2026 | Physical | $1,500 |
| **14 Sep 2026** | 18 Sep 2026 | Physical | $1,500 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $1,500 |
| **28 Sep 2026** | 02 Oct 2026 | Physical | $1,500 |
| **05 Oct 2026** | 09 Oct 2026 | Physical | $1,500 |
| **12 Oct 2026** | 16 Oct 2026 | Physical | $1,500 |
| **19 Oct 2026** | 23 Oct 2026 | Physical | $1,500 |

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **26 Oct 2026** | 30 Oct 2026 | Physical | $1,500 |

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

**Register Online Now**

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