Training Course on Deep Dive into Browser Forensics

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 nearly every digital investigation, web browser activity serves as a crucial window into user intent, online behaviors, and potential malicious actions. From cybercrime and data breaches to insider threats and harassment cases, understanding a user's digital footprint left within their browsers is paramount. Training Course on Deep Dive into Browser Forensics offers a deep dive into browser forensics, moving beyond superficial data extraction to equip digital forensic investigators, incident responders, and security analysts with the advanced techniques needed to uncover hidden artifacts, reconstruct complex Browse timelines, and identify sophisticated evasion attempts. Participants will gain mastery over the intricate data structures, storage mechanisms, and privacy features of popular browsers, transforming raw data into powerful actionable intelligence.

This intensive program explores the nuances of artifact collection and analysis across major browsers like Chrome, Firefox, Edge, and Safari, including their often-overlooked derivatives and private Browse modes. Through hands-on labs and real-world case studies, attendees will learn to forensically examine cache, cookies, history, downloads, session data, extensions, and more, correlating these disparate sources to paint a comprehensive picture of user activity. Elevate your investigative capabilities by becoming an expert in web intelligence gathering, providing undeniable evidence crucial for legal proceedings, internal investigations, and robust cybersecurity defences.

Programme Curriculum

Training Course on Deep Dive into Browser Forensics

Introduction

In nearly every digital investigation, web browser activity serves as a crucial window into user intent, online behaviors, and potential malicious actions. From cybercrime and data breaches to insider threats and harassment cases, understanding a user's digital footprint left within their browsers is paramount. Training Course on Deep Dive into Browser Forensics offers a deep dive into browser forensics, moving beyond superficial data extraction to equip digital forensic investigators, incident responders, and security analysts with the advanced techniques needed to uncover hidden artifacts, reconstruct complex Browse timelines, and identify sophisticated evasion attempts. Participants will gain mastery over the intricate data structures, storage mechanisms, and privacy features of popular browsers, transforming raw data into powerful actionable intelligence.

This intensive program explores the nuances of artifact collection and analysis across major browsers like Chrome, Firefox, Edge, and Safari, including their often-overlooked derivatives and private Browse modes. Through hands-on labs and real-world case studies, attendees will learn to forensically examine cache, cookies, history, downloads, session data, extensions, and more, correlating these disparate sources to paint a comprehensive picture of user activity. Elevate your investigative capabilities by becoming an expert in web intelligence gathering, providing undeniable evidence crucial for legal proceedings, internal investigations, and robust cybersecurity defences.

Course Duration

5 Days

Course Objectives

1. Master Browser Architecture: Understand the internal structures, databases (SQLite, ESE, LevelDB), and file formats used by leading web browsers (Chrome, Firefox, Edge, Safari).
2. Conduct Comprehensive History Analysis: Extract and interpret detailed Browse history, including URLs, titles, visit counts, and critical timestamps, even from deleted records.
3. Perform In-depth Cache Forensics: Recover images, scripts, and other web resources from browser caches to reconstruct visited web pages and identify suspicious content.
4. Analyze Cookies & Session Data: Understand various cookie types, their purpose, and their forensic value in tracking user sessions, login status, and website interactions.
5. Investigate Download Activities: Reconstruct file downloads, including source URLs, download paths, timestamps, and completion status.
6. Uncover Search Query Artifacts: Extract explicit search terms from browser history and search engine-specific artifacts to reveal user intent and information seeking.

7. Examine Browser Extensions & Add-ons: Identify installed extensions, their permissions, and potential malicious activities or data leakage.
8. Address Private Browse & Incognito Mode: Understand the limitations and residual artifacts left by private Browse modes across different browsers.
9. Correlate Browser Data with System Artifacts: Link browser activity to operating system logs, Prefetch files, jump lists, and other system-level evidence.
10. Detect Anti-Forensic Browser Techniques: Identify and counter methods used to clear history, manipulate timestamps, or otherwise obfuscate browser activity.
11. Leverage Specialized Browser Forensic Tools: Utilize both commercial and open-source tools for efficient and thorough browser artifact extraction and parsing.
12. Investigate Sync & Cloud-Based Browser Data: Understand and acquire forensic data from browser synchronization services (e.g., Chrome Sync, Firefox Sync).
13. Generate Actionable Forensic Reports: Produce clear, concise, and legally defensible reports based on detailed browser forensic findings.

Organizational Benefits

1. Enhanced Insider Threat Detection: Quicker identification of unauthorized web usage, data exfiltration, or policy violations.
2. Improved Data Breach Investigations: Pinpoint initial compromise vectors and malicious web activity leading to breaches.
3. Stronger Cybercrime Attribution: Develop compelling evidence for legal proceedings involving online fraud, phishing, or harassment.
4. Accelerated Incident Response: Rapidly identify and analyze malicious web-based threats, including command & control communications.
5. Comprehensive Digital Evidence Collection: Ensures no crucial web-related evidence is overlooked in investigations.
6. Reduced Litigation Risk: Provide robust, admissible digital evidence derived from browser artifacts.
7. Proactive Security Posture: Insights from browser forensics can inform and strengthen web filtering and security policies.
8. Cost Efficiency: Streamlined processes for extracting valuable web intelligence.
9. Upskilled Forensic Team: Elevate the expertise of internal cybersecurity and forensic staff in a critical area.
10. Protection of Critical Business Data: Safeguard sensitive information by understanding how it may be accessed or leaked via web browsers.

Target Participants

- Digital Forensic Investigators
- Incident Responders

- Cybersecurity Analysts
- Law Enforcement Investigators
- eDiscovery Specialists
- Security Operations Center (SOC) Analysts
- Threat Hunters
- Fraud Investigators
- Internal Audit Professionals
- Legal Professionals (with technical interest)

Course Outline

Module 1: Foundations of Browser Forensics & Common Artifacts

- **Introduction to Web Browser Forensics:** Importance in modern investigations, overview of key evidence types.
- **Browser Architecture & Data Storage:** Understanding SQLite databases (e.g., History, Web Data), ESE databases, JSON, LevelDB.
- **Core Artifacts Overview:** History, Cache, Cookies, Downloads – their location and basic interpretation.
- **File System & Registry Interaction:** How browser activity leaves traces in the OS (e.g., Prefetch, Registry).
- **Case Study: Initial Triage of Browser Artifacts on a Suspect Workstation**

Module 2: Google Chrome Forensics: A Deep Dive

- **Chrome Data Structures:** History, Web Data, Cookies, Login Data, Top Sites files.
- **Detailed History Analysis:** Parsing History database for URLs, titles, visit types, transition types.
- **Cache Exploration:** Recovering images, HTML, scripts from Chrome's cache structure.
- **Download & Search Query Analysis:** Extracting download metadata and explicit search terms.
- **Case Study: Reconstructing User Activity on a Chrome Browser Leading to Malware Download**

Module 3: Mozilla Firefox Forensics: Unique Artifacts & Challenges

- **Firefox Profile Structure:** Understanding places.sqlite, cookies.sqlite, downloads.sqlite, formhistory.sqlite.
- **History & Bookmark Analysis:** Deep dive into places.sqlite for comprehensive Browse history and visited sites.
- **Cache & Session Recovery:** Examining Firefox's cache system and recovering active sessions.
- **Password & Form Data Forensics:** Identifying saved credentials and auto-filled form entries.
- **Case Study: Investigating Credential Theft via Firefox Browser**

Module 4: Microsoft Edge & Internet Explorer Forensics

- **Microsoft Edge (Chromium-based):** Artifact locations, similarities to Chrome, and unique Edge features.

- **Internet Explorer (Legacy):** Analyzing WebCacheV01.dat (ESE database), index.dat, and history/cache folders.
- **Compatibility View & Enterprise Mode Artifacts:** Tracing specific IE configurations.
- **Correlating Edge/IE with Windows Ecosystem:** Integration with Windows Defender, SmartScreen logs.
- **Case Study: Uncovering Activity on an Older System using IE Artifacts**

Module 5: Safari & Other Browser Forensics

- **Safari Forensics (macOS/iOS):** Examining History.db, Cookies.binarycookies, Cache.db, and Downloads.plist.
- **Mobile Browser Forensics Overview:** Key differences and challenges in mobile browser data extraction.
- **Browser Derivatives & Privacy Browsers:** Brief analysis of browsers like Brave, Opera, Tor Browser, and their artifact implications.
- **Cross-Platform Browser Considerations:** Handling browser data consistency across multiple OS.
- **Case Study: Tracing Activity Across a User's Safari and Mobile Browser**

Module 6: Advanced Artifacts & User Intent

- **Session Data & Open Tabs:** Recovering information about active browser sessions and open tabs.
- **Extension & Add-on Forensics:** Identifying installed extensions, their associated data, and potential malicious intent.
- **Web Storage (LocalStorage, SessionStorage, IndexedDB):** Extracting client-side stored data for forensic insights.
- **Service Workers & Push Notifications:** Understanding their forensic value and persistent data.
- **Case Study: Pinpointing Data Exfiltration through a Malicious Browser Extension**

Module 7: Anti-Forensic Techniques & Evasion

- **Private Browse & Incognito Mode:** Understanding the limitations and residual artifacts (e.g., DNS cache, memory, network logs).
- **History Deletion & Cache Clearing:** Techniques for recovering "deleted" browser data.
- **Browser Sync & Cloud Artifacts:** Analyzing data synchronized across devices via cloud services (e.g., Chrome Sync history).
- **Ad-Blockers & Proxy/VPN Usage:** Identifying and analyzing tools used to obscure Browse activity.
- **Case Study: Bypassing Anti-Forensic Measures to Recover Hidden Browse History**

Module 8: Tooling, Automation & Reporting

- **Commercial Browser Forensic Tools:** Magnet AXIOM, X-Ways Forensics, EnCase (focus on browser parsing).
- **Open-Source Tools & Scripts:** SQLite tools, custom Python/PowerShell scripts for browser artifact analysis.
- **Automating Browser Artifact Collection:** Strategies for large-scale data acquisition from multiple endpoints.
- **Correlation & Timeline Generation:** Integrating browser data with other system artifacts for comprehensive timelines.

- **Case Study: Generating a Comprehensive Browser Activity Report for a Legal Case**

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.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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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