Training Course on Smart TV and Streaming Device 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

This specialized training course is designed for digital forensic investigators, law enforcement professionals, cybersecurity analysts, and privacy advocates grappling with the increasingly significant role of Smart TVs and streaming devices in digital investigations. Modern households are replete with these connected entertainment hubs, from Smart TVs running Android TV, Tizen, or webOS, to dedicated streaming sticks like Roku, Amazon Fire TV, and Apple TV. While offering unparalleled access to content, these devices are also rich repositories of user activity, viewing habits, application usage, network connection data, and even voice commands, making them critical, yet often overlooked, sources of digital evidence in a wide array of cases, including cybercrime, child exploitation, intellectual property infringement, and even homicides.

Training Course on Smart TV and Streaming Device Forensics provides a deep dive into the diverse operating systems, memory architectures, and data storage mechanisms employed by various Smart TVs and streaming devices. Through intensive hands-on labs and real-world case studies, participants will gain practical proficiency in forensically sound data acquisition techniques, ranging from logical extractions via developer modes and ADB, to advanced hardware-based methods like JTAG, ISP, and Chip-Off when direct access is limited. The course also critically addresses the significant privacy implications of the vast data collected by these devices and the complex legal frameworks (including Kenya's Data Protection Act 2019) governing their forensic examination, ensuring that all acquired evidence is admissible in court and ethically handled, empowering investigators to unlock crucial intelligence from these pervasive consumer electronics.

Programme Curriculum

Training Course on Smart TV and Streaming Device Forensics

Introduction

This specialized training course is designed for digital forensic investigators, law enforcement professionals, cybersecurity analysts, and privacy advocates grappling with the increasingly significant role of Smart TVs and streaming devices in digital investigations. Modern households are replete with these connected entertainment hubs, from Smart TVs running Android TV, Tizen, or webOS, to dedicated streaming sticks like Roku, Amazon Fire TV, and Apple TV. While offering unparalleled access to content, these devices are also rich repositories of user activity, viewing habits, application usage, network connection data, and even voice commands, making them critical, yet often overlooked, sources of digital evidence in a wide array of cases, including cybercrime, child exploitation, intellectual property infringement, and even homicides.

Training Course on Smart TV and Streaming Device Forensics provides a deep dive into the diverse operating systems, memory architectures, and data storage mechanisms employed by various Smart TVs and streaming devices. Through intensive hands-on labs and real-world case studies, participants will gain practical proficiency in forensically sound data acquisition techniques, ranging from logical extractions via developer modes and ADB, to advanced hardware-based methods like JTAG, ISP, and Chip-Off when direct access is limited. The course also critically addresses the significant privacy implications of the vast data collected by these devices and the complex legal frameworks (including Kenya's Data Protection Act 2019) governing their forensic examination, ensuring that all acquired evidence is admissible in court and ethically handled, empowering investigators to unlock crucial intelligence from these pervasive consumer electronics.

Course Duration

5 Days

Course Objectives

1. Identify diverse Smart TV and streaming device platforms (Android TV, Tizen, webOS, Roku OS, tvOS) and their unique forensic characteristics.
2. Understand the types of digital artifacts recoverable from Smart TVs and streaming devices, including viewing history, app usage, network data, and voice commands.
3. Perform forensically sound data acquisition using various methods: logical, physical (JTAG, ISP, Chip-Off), and network-based.
4. Utilize developer modes and debugging interfaces (e.g., ADB for Android TV) to extract data from accessible devices.
5. Analyze proprietary file systems and data formats common to Smart TV and streaming device operating systems.

6. Extract and interpret application-specific data from popular streaming services (Netflix, YouTube, Hulu, etc.) and other installed apps.
7. Investigate network connection logs (Wi-Fi SSIDs, MAC addresses, IP addresses, timestamps) to establish device presence and activity.
8. Recover and analyze browser history, search queries, and content download logs from integrated web browsers.
9. Identify and interpret voice command data and associated recordings from Smart TVs with AI assistants.
10. Reconstruct user activity timelines by correlating various data artifacts from the device.
11. Navigate data privacy concerns and legal requirements (e.g., Kenya's Data Protection Act 2019) related to Smart TV data.
12. Employ specialized forensic tools and open-source utilities for Smart TV and streaming device analysis.
13. Generate comprehensive forensic reports detailing findings from Smart TV and streaming device investigations for legal admissibility.

Organizational Benefits

1. Expanded Investigative Scope: Access crucial evidence from previously overlooked digital sources in various case types.
2. Enhanced Case Resolution: Corroborate alibis, establish viewing habits, or identify illegal content access through device data.
3. Proactive Threat Intelligence: Understand vulnerabilities and data collection practices of Smart TVs and streaming devices.
4. Reduced Reliance on External Experts: Build in-house capability for specialized Smart TV and streaming device forensics.
5. Improved Evidence Admissibility: Ensure data acquisition and analysis comply with legal and forensic standards.
6. Faster Incident Response: Quickly extract relevant data in cases involving device compromise or misuse.
7. Cost Savings: Optimize investigations by leveraging this increasingly common source of digital evidence.
8. Comprehensive Digital Footprint Analysis: Integrate Smart TV data with other digital evidence for a holistic view of user activity.
9. Compliance Assurance: Train personnel on the latest privacy laws, especially relevant for user-generated content and viewing habits.
10. Cutting-Edge Expertise: Position the organization at the forefront of emerging digital forensic challenges.

Target Participants

- Digital Forensic Examiners
- Law Enforcement (CID, DCI, Cybercrime Units)
- Cybersecurity Incident Responders
- Internal Corporate Investigators
- Privacy Officers / Legal Professionals (interested in digital evidence)
- Intelligence Analysts
- Mobile Device Forensic Specialists (seeking expansion)
- Hardware Reverse Engineers (interested in consumer electronics)
- e-Discovery Specialists
- Consumer Product Security Teams

Course Outline

Module 1: Smart TV & Streaming Device Fundamentals (Smart TV Basics)

- Overview of Smart TV and Streaming Device Ecosystems (Android TV, Tizen, webOS, Roku OS, tvOS)
- Hardware Components: CPUs, Memory Types (eMMC, NAND), Storage
- Connectivity Options: Wi-Fi, Ethernet, Bluetooth, USB, HDMI
- User Interfaces and Application Stores
- **Case Study**: Identifying the operating system and key hardware features of a common Smart TV model.

Module 2: Data Types and Artifacts on Smart TVs (Smart TV Artifacts)

- Viewing History and Watchlist Data from Streaming Apps
- Application Installation, Usage Logs, and User Preferences
- Network Connection Data (SSIDs, MAC Addresses, IP Addresses, Timestamps)
- Web Browser History, Cookies, and Search Queries
- USB and External Device Connection Logs (e.g., connected hard drives, phones)
- **Case Study**: Identifying key artifacts left behind by a popular streaming application on a Smart TV.

Module 3: Logical Data Acquisition Techniques (Logical Extraction)

- Accessing Data via Developer Modes and Diagnostic Menus

- Utilizing Android Debug Bridge (ADB) for Android TV devices (shell access, `adb pull`)
- Extracting Logs via USB or Network Export Features
- Challenges of Locked Devices and User Passcodes
- **Case Study**: Performing a logical extraction of application data from an Android TV device using ADB.

Module 4: Advanced Hardware-Based Acquisition (Hardware Acquisition)

- Introduction to JTAG, UART, and ISP (In-System Programming) for direct memory access
- Principles of Chip-Off Forensics for eMMC/NAND Flash
- Identifying Test Points and Connection Methods on Device Boards
- Considerations for Physically Damaged or Non-Responsive Devices
- **Case Study**: Discussing the feasibility and challenges of a Chip-Off acquisition from a proprietary Smart TV.

Module 5: Firmware Analysis & Reverse Engineering (Firmware Forensics)

- Extracting Firmware Images (where possible) from Smart TVs/Streaming Devices
- Using Tools like Binwalk for Firmware Analysis and Extraction
- Identifying Configuration Files, Embedded Databases, and Executables within Firmware
- Basic Firmware Reverse Engineering for Proprietary Code Analysis
- **Case Study**: Analyzing a streaming stick's firmware for hidden configuration files.

Module 6: Network and Cloud-Based Evidence (Network & Cloud Forensics)

- Capturing and Analyzing Network Traffic (e.g., Wireshark) for Device Communications
- Identifying Connections to Streaming Services, Ad Servers, and Manufacturer Servers
- Investigating Cloud-Synced Data: Watch History, Preferences linked to User Accounts
- Challenges of Encrypted Traffic and Cloud Service Provider Warrants
- **Case Study**: Analyzing network traffic to identify suspicious outbound connections from a Smart TV.

Module 7: Analysis and Interpretation of Smart TV Data (Data Analysis & Correlation)

- Tools for Parsing and Visualizing Smart TV and Streaming Device Artifacts
- Correlating Data (e.g., viewing history with internet activity, connection logs)
- Reconstructing Timelines of User Activity and Device Usage
- Interpreting Device Settings related to Privacy and Data Collection (ACR, voice assistants)
- **Case Study**: Building a timeline of events based on app usage and network connection logs from a Smart TV.

Module 8: Legal, Ethical & Reporting Considerations (Legal & Reporting)

- Legal Basis for Seizing and Examining Smart TVs and Streaming Devices (Search Warrants, Consent)
- Privacy Concerns: User Expectation of Privacy vs. Data Collection by Manufacturers
- Compliance with **Kenya's Data Protection Act 2019** and other relevant privacy regulations (e.g., GDPR, CCPA).
- Best Practices for Documenting Findings and Presenting Evidence in Court
- **Case Study**: Discussing a scenario where a Smart TV's voice recordings become relevant evidence in a case under the framework of Kenya's privacy laws.

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
26 Oct 2026	30 Oct 2026	Physical	$1,500

Register Online Now

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