AX-MVFS Mobile Virus Forensic System

Product Introduction

The AX-MVFS (Mobile Virus Forensic System) is a **cutting-edge mobile security solution** designed for forensic detection and analysis of malicious code on mobile devices. Leveraging **advanced behavioral analysis** and static/dynamic inspection techniques, it identifies and documents common and sophisticated threats, including spyware, data theft tools, remote access trojans (RATs), and covert surveillance malware. Ideal for cybersecurity teams and law enforcement, it delivers actionable intelligence with court-admissible reporting.

Key Features

1. APK & IPA Static Analysis

- **Automated APK Metadata Extraction**:
  - Retrieve app name, version, package name, file hashes (MD5/SHA1/SHA256).
  - **Signature Analysis**: Certificate details (algorithm, public key type, validity period), signature serial number.
- **Static Permission Profiling**:
  - Categorize permissions by risk level (critical, normal, others) for threat assessment.
- **Third-Party SDK Mapping**:
  - Identify SDK vendors, service types, and regulatory compliance flags.

2. Dynamic & Network Analysis

- **Network Traffic Capture**:
  - **Proxy Mode** or **On-Device Packet Capture** to extract URLs, IPs, response codes, timestamps, and host data.
  - Auto-detect third-party SDK communications (e.g., ad libraries, analytics).
- **Sensitive Data Detection**:
  - Scan source code for URLs, IPs, phone numbers, emails, hash strings, and custom keywords.

3. Reverse Engineering & Recovery

- **One-Click Unpacking**: Bypass obfuscation to decompile APK/IPA files into readable source code.

- **iOS Support**: Static analysis of IPA files for hidden payloads or suspicious entitlements.

4. Reporting & Compliance

- **Multi-Format Reports**: Export findings in **HTML, Word, or PDF** with technical details and evidence summaries.
- **Chain-of-Custody Logs**: Generate MD5/SHA hashes for all analyzed files and network captures.

Technical Highlights

- **Behavioral AI Engine**: Detects zero-day malware by monitoring API calls, process injection, and anomalous network activity.
- **Forensic-Grade Tools**:
  - **ADB Integration**: Built-in command-line tools for advanced device control.
  - **Screen Recording**: Capture tamper-proof video logs of malware behavior.
- **Cross-Platform Support**: Analyze Android APKs and iOS IPAs with unified workflows.

Use Cases

- **Law Enforcement**: Investigate mobile devices involved in cybercrime (e.g., spyware, financial fraud).
- **Enterprise Security**: Audit employee devices for unauthorized data exfiltration tools.
- **Threat Intelligence**: Reverse engineer malware to identify command-and-control (C2) infrastructure.

Why AX-MVFS?

- **Precision**: AI-driven detection for advanced persistent threats (APTs).
- **Speed**: One-click workflows reduce analysis time by 70%.
- **Compliance**: Meets **ISO 27037** and **NIST SP 800-86** standards for digital evidence.

Ansion Intelligence
Innovating Digital Forensics Solutions for Justice and Enterprise

Ansion Intelligence

Ansion Intelligence is a leading provider of cutting-edge digital forensics products and technical services, dedicated to empowering judicial authorities and enterprises with reliable solutions for electronic evidence collection, analysis, and management.