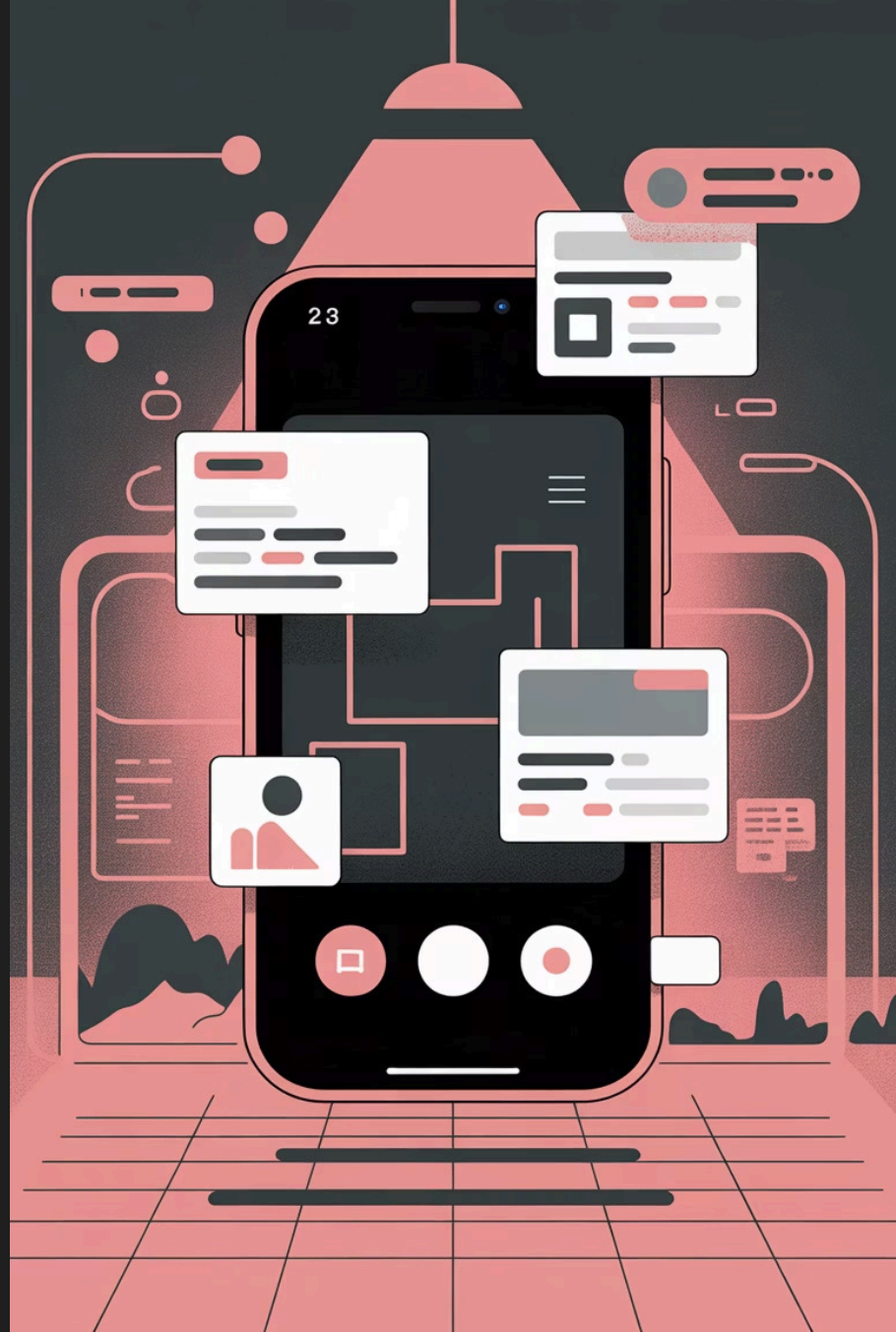
Mobile Forensics: Investigasi Perangkat iOS & Android

Modul komprehensif tentang teknik akuisisi, analisis artefak digital, dan penanganan tantangan keamanan pada perangkat mobile dalam konteks investigasi forensik digital.



Tujuan Pembelajaran Modul

Teknik Akuisisi Data

Memahami dan menerapkan berbagai metode akuisisi data dari perangkat mobile, mulai dari logical hingga physical acquisition dengan prosedur yang aman dan legal.

Identifikasi Artefak Digital

Mengidentifikasi dan menganalisis artefak digital penting seperti SMS, call logs, app data, dan metadata dari perangkat Android dan iOS.

Tantangan Keamanan

Menangani hambatan teknis seperti enkripsi full-disk, device locking, dan sandboxing dengan pendekatan forensik yang tepat dan etis.

Praktik Forensik

Melakukan ekstraksi dan analisis data secara hands-on menggunakan tools standar industri dengan memperhatikan aspek legalitas dan chain of custody.

Peran Mobile Forensics dalam Investigasi Modern

Mengapa Mobile Forensics Krusial?

Perangkat mobile telah menjadi repositori utama data pribadi dan profesional. Smartphone menyimpan komunikasi, lokasi, transaksi keuangan, dan aktivitas digital yang menjadi bukti kunci dalam investigasi kriminal, korporat, dan litigasi sipil.

Dengan lebih dari 6 miliar pengguna smartphone global, hampir setiap kasus investigasi modern melibatkan analisis perangkat mobile sebagai sumber bukti digital primer.

Konteks Investigasi

- Kejahatan siber dan penipuan digital
- Kasus kriminal dan terorisme
- Investigasi korporat dan insider threats
- Litigasi perdata dan e-discovery
- Kasus kehilangan data dan kebocoran informasi

Arsitektur Sistem Mobile: Android vs iOS

Android Architecture

File System: Menggunakan ext4 atau F2FS dengan struktur direktori Linux. Data aplikasi tersimpan di /data/data/ dengan permission berbasis UID.

Sandboxing: Setiap aplikasi berjalan dalam proses terpisah dengan user ID unik, membatasi akses ke data aplikasi lain.

Enkripsi: Full-disk encryption (FDE) atau File-based encryption (FBE) sejak Android 7.0, menggunakan kunci yang terikat pada lock screen credentials.

iOS Architecture

File System: Menggunakan APFS (Apple File System) dengan enkripsi built-in dan snapshot capabilities untuk backup efisien.

Sandboxing: Aplikasi terisolasi ketat dalam container sendiri, hanya dapat mengakses data melalui API yang diizinkan sistem.

Enkripsi: Hardware-based encryption menggunakan Secure Enclave, dengan kunci yang tidak dapat diekstrak dari device tanpa passcode.

Prosedur Standar Penanganan Perangkat Mobile

01

Chain of Custody

Dokumentasikan setiap perpindahan bukti dengan mencatat waktu, lokasi, dan pihak yang menangani. Gunakan formulir chain of custody yang lengkap dengan tanda tangan dan seal.

02

Isolasi Sinyal

Tempatkan perangkat dalam Faraday bag atau aktifkan mode pesawat untuk mencegah remote wipe, sinkronisasi cloud, atau komunikasi yang dapat mengubah bukti.

03

Dokumentasi Visual

Foto perangkat dari semua sudut, catat kondisi fisik, nomor IMEI/serial, status baterai, dan tampilan layar sebelum melakukan prosedur forensik.

04

Preservasi Daya

Jaga perangkat tetap hidup dengan charger atau power bank forensik. Jangan biarkan perangkat mati karena dapat memicu enkripsi tambahan atau kehilangan volatile data.

Teknik Akuisisi Data Mobile

Memilih metode akuisisi yang tepat adalah keputusan strategis yang bergantung pada kondisi perangkat, kebutuhan investigasi, dan constraint legal. Setiap teknik memiliki trade-off antara kelengkapan data, kompleksitas, dan risiko.

Logical Acquisition: Metode Cepat dan Aman

Karakteristik

Logical acquisition mengekstrak data yang dapat diakses melalui interface sistem operasi normal, seperti kontak, SMS, call logs, dan backup aplikasi.

Kecepatan tinggi dan risiko minimal menjadikannya pilihan pertama dalam banyak investigasi, terutama ketika waktu menjadi faktor kritis.

Kelebihan

- Tidak memerlukan rooting atau jailbreaking
- Proses cepat, biasanya selesai dalam menit
- Risiko kerusakan data minimal
- Legal defensibility tinggi karena non-invasive

Keterbatasan

- Tidak dapat mengakses data yang telah dihapus
- Terbatas pada data yang diizinkan OS untuk diakses
- Tidak mendapat app data yang dilindungi sandbox

File System Extraction: Akses Mendalam

1

Akses Root/Jailbreak

Memerlukan elevated privileges melalui rooting (Android) atau jailbreaking (iOS) untuk mengakses seluruh file system termasuk area yang dilindungi.

2

Ekstraksi File System

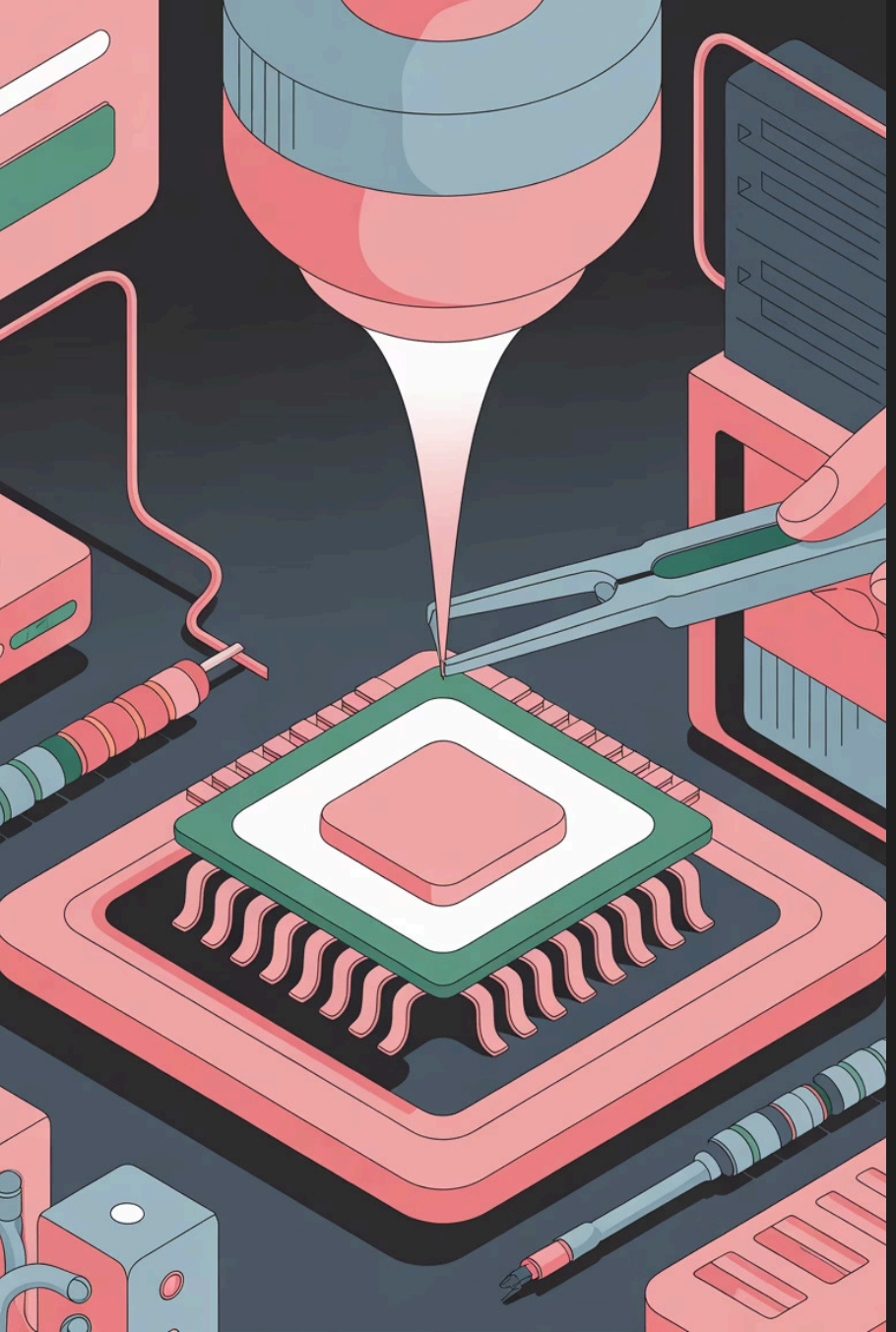
Menyalin seluruh struktur direktori termasuk folder /data/, /system/, dan hidden directories yang berisi database SQLite, cache, dan log aplikasi.

3

Analisis Database

Mengakses database SQLite dari aplikasi populer seperti WhatsApp (msgstore.db), browser (history.db), dan sistem (contacts2.db) untuk ekstraksi data detail.

Pertimbangan Legal: Rooting/jailbreaking dapat mengubah kondisi bukti original. Selalu dokumentasikan prosedur dan pertimbangkan implikasi legal di yurisdiksi Anda.



Physical Acquisition: Ekstraksi Bit-by-Bit

Metode Paling Komprehensif

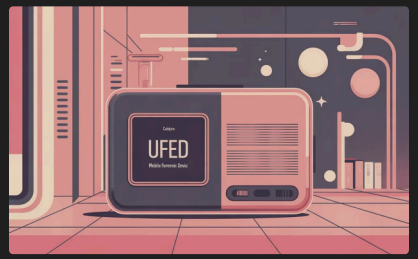
Physical acquisition membuat salinan bit-by-bit dari seluruh memori perangkat, termasuk unallocated space yang dapat berisi data terhapus dan artifacts tersembunyi.

Teknik ini menggunakan exploit atau hardware interface (JTAG, Chip-Off) untuk bypass sistem operasi dan mengakses raw memory.

Kompleksitas dan Risiko

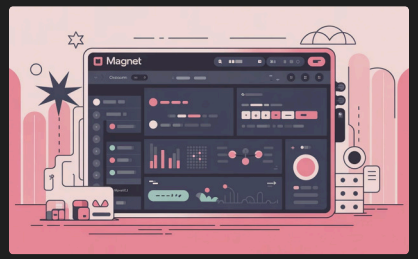
- Memerlukan tools dan expertise tingkat lanjut
- Proses lambat, dapat memakan waktu berjam-jam
- Risiko kerusakan hardware pada metode invasif
- Tergantung pada device support dan security features
- Dapat memulihkan deleted files dan hidden data

Tools Forensik Mobile Standar Industri



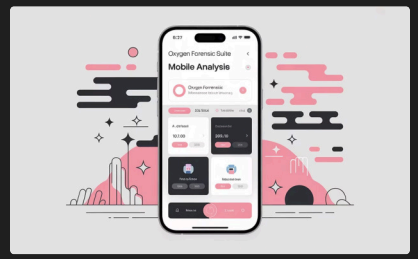
Cellebrite UFED

Platform forensik mobile paling populer dengan dukungan ekstensif untuk ribuan device model. Menyediakan logical, file system, dan physical extraction dengan interface intuitif.



Magnet AXIOM

Suite analisis forensik komprehensif yang mendukung mobile, computer, dan cloud data. Powerful artifact parsing dan timeline visualization untuk investigasi kompleks.



Oxygen Forensic Suite

Tool all-in-one untuk ekstraksi dan analisis data mobile dengan fokus pada cloud extraction dan social media artifacts. Mendukung lebih dari 20.000 device models.

Tools open-source seperti **Android Debug Bridge (ADB)**, **iTunes/iMazing**, dan **Autopsy** juga menjadi pilihan penting untuk investigator dengan budget terbatas.

Artefak Digital Utama dalam Investigasi Mobile

SMS & MMS

Database: mmssms.db (Android), sms.db (iOS)

- Isi pesan lengkap dengan thread conversation
- Timestamp pengiriman dan penerimaan
- Nomor telepon pengirim/penerima
- Status pesan (terkirim, gagal, dibaca)

Call Logs

File: calls.db, calllog.db

- Panggilan masuk, keluar, dan tidak terjawab
- Durasi panggilan dalam detik
- Timestamp dengan timezone information
- Contact name jika tersimpan

Contact List

Database: contacts2.db

- Nama, nomor telepon, email addresses
- Metadata: last contacted, times contacted
- Sinkronisasi dengan akun cloud (Google, iCloud)
- Photo dan custom fields

App Data: Sumber Bukti Digital Kaya

WhatsApp Forensics

Database: msgstore.db, wa.db

- Chat messages dengan enkripsi end-to-end
- Media files: foto, video, audio, dokumen
- Group chat metadata dan participant lists
- Call logs untuk voice dan video calls
- Status updates dan broadcast messages

Key backup terenkripsi memerlukan decryption key yang tersimpan di device atau backup.

Browser & Email Artifacts

Browser: history.db, cookies.sqlite

- URL browsing history dengan timestamps
- Search queries dan form autofill data
- Cookies dan session tokens
- Downloaded files dan cache

Email: mailbox.db, attachments

- Email content (inbox, sent, drafts)
- Attachment files dan metadata
- Account credentials (hashed/encrypted)

Location & GPS Artifacts: Tracking Pergerakan

1

Location Database

File location.db dan cache.cell menyimpan koordinat GPS, cell tower information, dan WiFi access points yang terdeteksi dengan timestamps presisi tinggi.

2

Google Timeline / Apple Maps

Cloud-synced location history dalam format JSON atau KML yang merekam pergerakan user dengan detail rute, moda transportasi, dan tempat yang dikunjungi.

3

App Location Logs

Aplikasi seperti Uber, Gojek, Google Maps, dan social media menyimpan location metadata dalam database masing-masing untuk fitur ride history dan geotagging.

Media Files: Metadata EXIF dan Forensik Visual

Tipe Media

- Foto dan screenshots
- Video recordings
- Audio files dan voice memos
- Downloaded media dari apps

Informasi Metadata Krusial

EXIF Data pada Foto:

- Timestamp pembuatan dan modifikasi
- GPS coordinates (latitude, longitude)
- Device make, model, dan camera settings
- Software yang digunakan untuk edit

Metadata ini dapat divalidasi untuk mendeteksi manipulasi gambar dan memverifikasi authenticity dalam investigasi. Tools seperti ExifTool dapat parsing metadata lengkap dari ribuan file sekaligus.

Tantangan Teknis dalam Mobile Forensics

Enkripsi dan Device Security: Hambatan Utama

Full-Disk Encryption (FDE)

Mengenkripsi seluruh partisi data menggunakan kunci yang derived dari user passcode. Tanpa credentials, physical extraction hampir mustahil pada device modern dengan hardware encryption.

Secure Boot & TEE

Trusted Execution Environment (TEE) dan Secure Enclave menyimpan kunci kriptografi di hardware terpisah yang tidak dapat diakses bahkan dengan physical access.

Biometric Protection

Fingerprint dan Face ID menambah layer security yang sulit bypass. Investigator harus obtain biometric sample atau legal order untuk unlock dalam golden hour.

Golden Hour: Periode kritis setelah device seizure dimana perangkat masih unlocked atau dalam AFU (After First Unlock) state sebelum masuk BFU (Before First Unlock) dengan enkripsi penuh aktif.

App Sandboxing dan Cloud Sync: Data Tersebar

Sandboxing Limitations

Arsitektur sandbox modern membatasi akses inter-app dan memerlukan privilege escalation untuk ekstraksi data aplikasi yang dilindungi.

Pada iOS, sandboxing sangat ketat hingga membuat extraction tanpa jailbreak hanya dapat mengakses data melalui backup iTunes yang terbatas.

Android memberikan sedikit lebih banyak fleksibilitas dengan ADB backup, namun banyak app modern menggunakan flag ALLOW_BACKUP=false yang prevent backup access.

Cloud Synchronization

Data penting semakin banyak tersimpan di cloud:

- iCloud: photos, contacts, notes, backups
- Google Drive: backup, photos, documents
- WhatsApp backup ke cloud storage
- Social media: messages, photos, videos

Forensic cloud acquisition memerlukan credentials atau legal process untuk data request ke service providers dengan response time bervariasi.

Aspek Legal dan Chain of Custody

Legal Authorization

Pastikan investigasi didukung warrant, persetujuan tertulis, atau legal basis sesuai yurisdiksi. Bukti tanpa proper authorization dapat ditolak di pengadilan.

Chain of Custody

Dokumentasi lengkap setiap tahap handling bukti dari seizure hingga analisis. Setiap gap dalam custody chain dapat mempertanyakan integrity bukti.

Reporting Standards

Laporan forensik harus memenuhi standar seperti SWGDE/IOCE dengan methodology transparency, tool validation, dan reproducible results.

Praktik Lab: Hands-on Mobile Forensics

Skenario Investigasi

Peserta akan melakukan ekstraksi dan analisis data dari backup perangkat Android dan iOS (non-rooted/jailbroken) untuk menemukan bukti komunikasi dan aktivitas digital.

Android Logical Backup (ADB)

Aktifkan USB debugging, hubungkan device, jalankan: `adb backup -apk -shared -all -f backup.ab` untuk create full backup file.

iOS Backup (iTunes/iMazing)

Connect iOS device ke computer, create unencrypted backup menggunakan iTunes atau iMazing. Backup akan tersimpan di lokasi default system.

Analisis dengan Forensic Tools

Import backup files ke Autopsy atau Magnet AXIOM. Tools akan parsing database dan extract artifacts secara otomatis dengan categorization.

Investigasi Artefak Target

Navigate ke modules: Messaging (SMS, WhatsApp), Call Logs, Contacts, Browser History. Extract relevan artifacts dan build timeline investigasi.

Forensic Reporting

Compile findings dalam format report standar: Executive Summary, Methodology, Findings dengan screenshots, Timeline Analysis, dan Conclusions dengan evidence references.

Key Takeaways: Mobile Forensics Essentials

3

Metode Akuisisi

Logical, File System, dan Physical acquisition—masing-masing dengan trade-off kompleksitas vs kelengkapan data

8

Artefak Krusial

SMS, calls, contacts, app data, location, media—sumber bukti digital primer dalam investigasi

5

Tantangan Utama

Enkripsi, device lock, sandboxing, cloud sync, dan legal constraints yang harus dinavigasi

---

Mobile forensics adalah bidang yang terus berkembang seiring evolusi teknologi smartphone dan security features. Forensic investigator harus continuously update knowledge tentang tool capabilities, OS updates, dan legal frameworks untuk conduct investigations yang effective dan legally defensible.

Remember: Proper methodology, documentation, dan adherence to legal standards adalah foundation dari every successful mobile forensic investigation.