Mobile forensic

Pengantar Komputer Forensik Teknologi Informasi

UNIVERSITAS GUNADARMA
Fakultas Teknologi Industri
Jurusan Teknik Informatika

Handheld devices

- Cellular Phone – GSM, CDMA
- Personal Digital Assistance (PDA)
- Smart phone (hybrid)

Tablet PC

- Menggunakan WiFi atau modem

Mobile Storage Devices

- SIM Card

- Memory card
  - MMC (Multi-MediaCard)
  - SD (Secure Digital) Card
  - Memory Stick
  - TransFlash atau MicroSD

Mobile Storage Devices

- USB Flash disk
- External hard disk

Digital Evidence in Mobile Device

- Handset Memory
- SIM Card
- USIM (3G SIM)
- Memory Card

Data in Handset Memory

- Audio Files (Music and Voice)
- Calendar Entries
- Call History (Inbound and Outbound)
- Contacts/Phonebook
- Email
- Internet History
- Instant Messaging (IM) chat
- Memos
- Multimedia Messages (MMS)
- Pictures
- Short Message Service (SMS) or Text Messages
- System Firmware Information
- T9 Dictionaries
- Telecommunication Settings
- Videos
- Voice Mail

Data in SIM Card

- Last Number Dialed (LDN)
- Phonebook/Contacts (ADN)
- Text Messages (SMS), including deleted text messages
- Location information (LOCI) from position of last usage
- Service Related Information

Data in USIM Card

- PIN1, PIN2 (Personal Identification Number)
  - PIN1 akses ke handset
  - PIN2 melindungi network setting
- PUK1, PUK2 codes (Personal Unlocking Key)

Data in Memory Card

- Pictures
- Movies
- Audio Files
- Documents

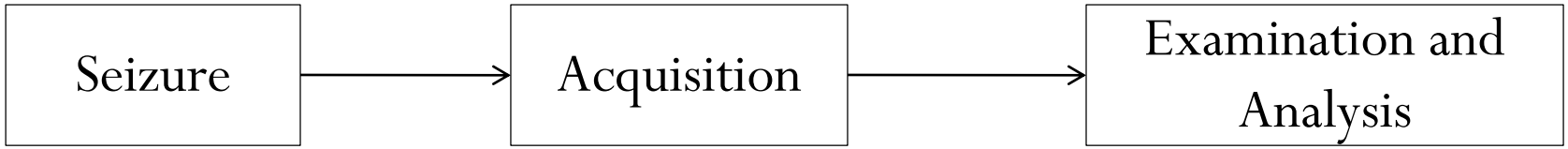
Data from NSP

- Network Service Provider
  - Subscriber Information
  - Call Data Records - related to phone calls and text messages
  - Subscriber Location - this relates to geo location of the
  - physical device, in an effort to track the subscriber

Mobile Operating System

- Google's Android
- Apple's iOS
- RIM's BlackBerry OS
- Microsoft's Windows Phone
- Linux
- HP's webOS
- Samsung's Bada
- Nokia's MeeGo

Mobile Forensic Process



- Seizure → Penyitaan barang bukti
- Acquisition → Mengambil data dari barang bukti
- Examination and Analysis → Pemeriksaan data dan analisis dengan tools

Data Acquisition Types

- **Physical acquisition**
  - Menyalin setiap bit dari keseluruhan penyimpanan fisik (memory chip)
  - Akses langsung ke flash memory
  - Dapat melihat file yang telah dihapus dan sisa-sisa data untuk diperiksa.

Data Acquisition Types

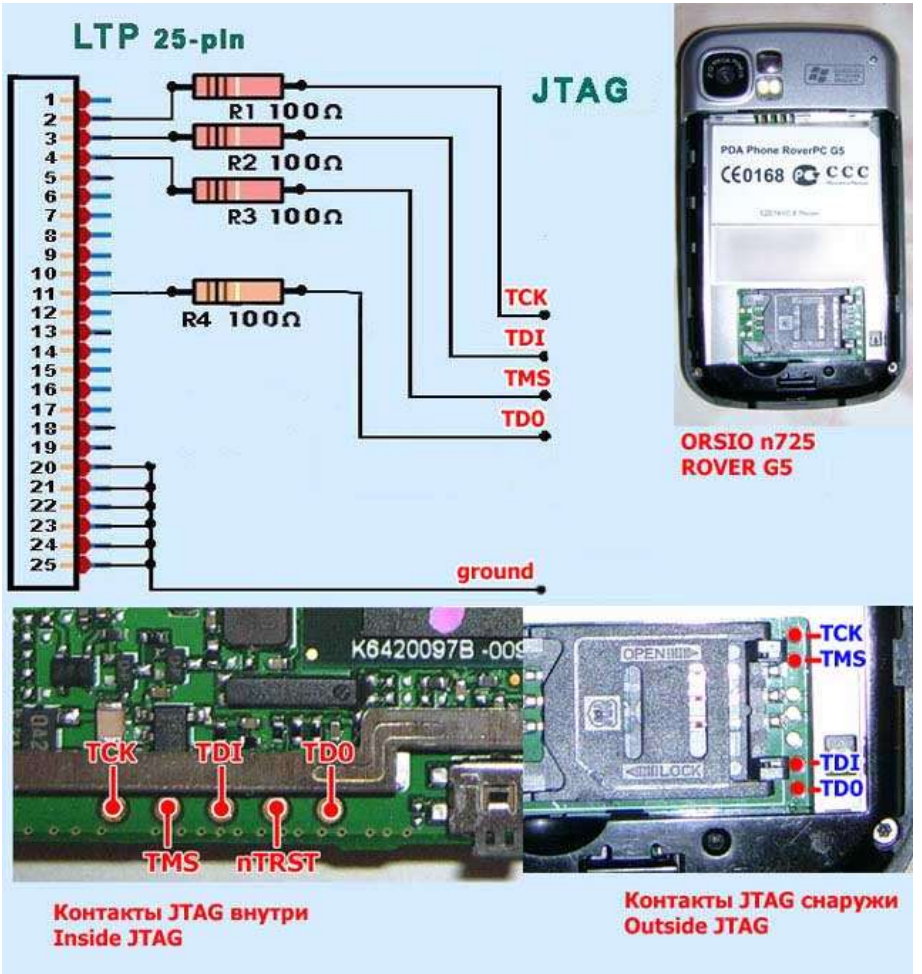
- **Logical acquisition**
  - Menyalin setiap bit dari objek penyimpanan logika (direktori dan file)
  - Butuh interface dari vendor untuk sinkronisasi isi device dengan PC.
  - Sistem file lebih mudah untuk diekstrak dan dikelola
  - Tidak dapat melihat data yang telah dihapus

Data Acquisition Types

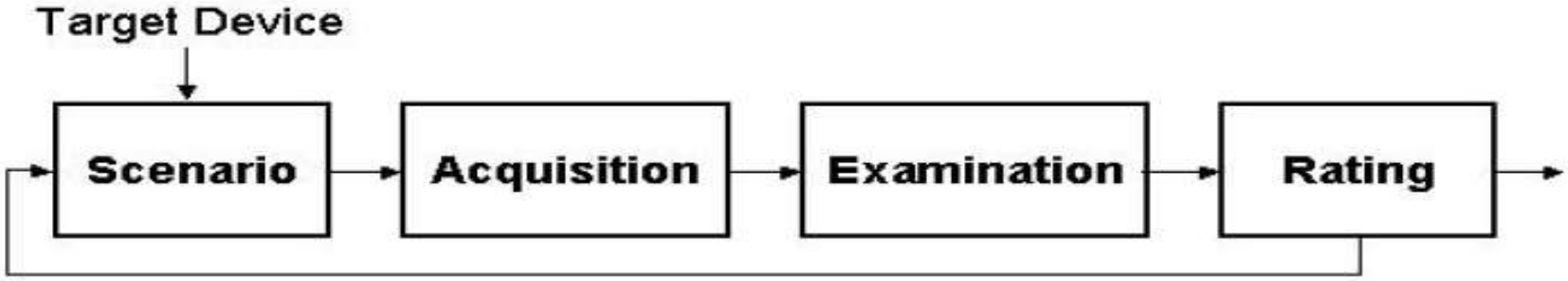
- **Manual acquisition**
  - Menggunakan user interface untuk menginvestigasi isi dari memory
  - Transformasi data mentah menjadi informasi yang dapat dibaca manusia
  - Hanya data yang terlihat oleh sistem operasi yang dapat diperoleh kembali

JTAG

- Joint Test Action Group (JTAG)
- Untuk me-recover memory



Tool Assessment



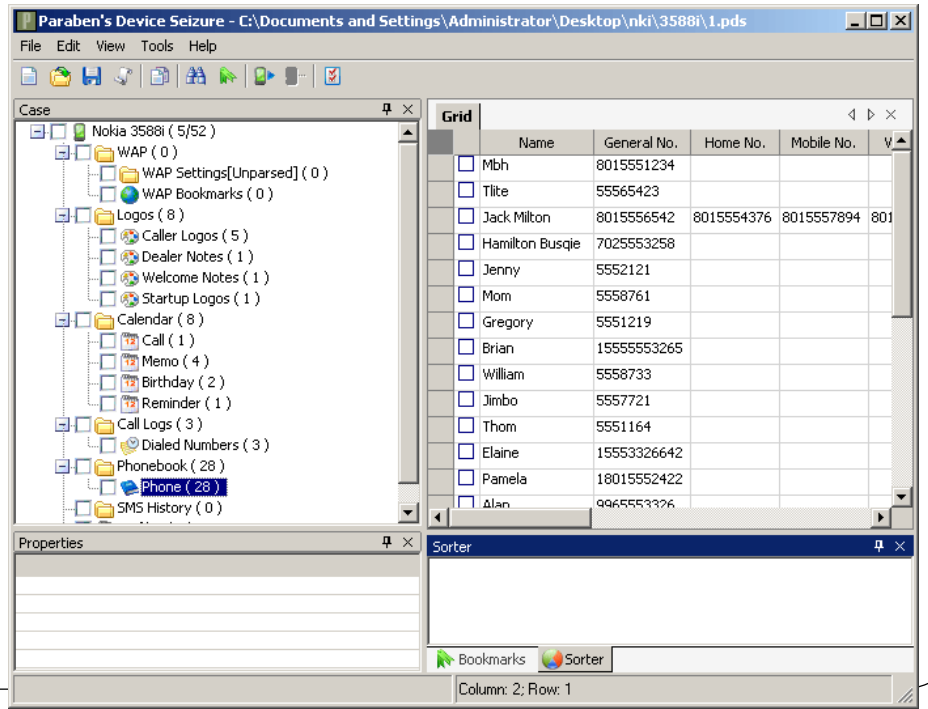
- Skenario → dipisahkan antara simple dan smart phone, serta aktivitasnya
- Pengumpulan data → konten dari device dan/atau SIM card terkait serta memory
- Pemeriksaan data
- Rating → apakah hasil sesuai yang diharapkan

Mobile Forensic Tools

- Tools untuk device
- Tools untuk simcard

Paraben mobile forensic

- http://www.paraben.com
- **Device Seizure**
  Mobile Field
  DS Box
  SIM Card Seizure
  StrongHold Bag
  StrongHold Box
  Project-A-Phone



XRY forensic tools

- Program + Cable
- Terlengkap untuk berbagai handphone
- Dari MicroSystemation
- http://www.msab.com
- Dengan program XACT dapat memeriksa mobile devices yang filenya dihapus

Mobile Device Forensic Tools

	Fungsi	Fitur
pilot-link	**Acquisition**	• Palm OS phones • Open source non-forensic software • Tidak support recovery informasi SIM • Hanya dengan cable interface
Oxygen PM (forensic version)	**Acquisition, Examination, Reporting**	• GSM phones tertentu • Supports only internal SIM acquisition
MOBILedit! For nsic	**Acquisition, Examination, Reporting**	• GSM phones tertentu • Internal and external SIM support • Support cable dan IR interfaces

Mobile Device Forensic Tools

	Fungsi	Fitur
BitPIM	**Acquisition, Examination**	• CDMA phones tertentu • Open source software with write-blocking capabilities • No support for recovering SIM information
TULP 2G	**Acquisition, Reporting**	• GSM and CDMA phones that use the supported protocols to establish connectivity • Internal and external SIM support • Requires PC/SC-compatible smart card reader for external SIM cards • Cable, Bluetooth, and IR interfaces supported

SIM toolkit

- Ada JVM di dalam SIM
- Operator dapat menginstal program melalui OTA – Over The Air (secara remote tanpa diketahui)
- Standard yang "vulnerable" invisible flags, binary updates, call-control, proprietary

XRY SIM ID cloner

- Memungkinkan menggunakan handphone dengan SIM terkunci
- Memungkinkan memeriksa cell phone tanpa koneksi

SIM Card Forensic Tools

	Fungsi	Fitur
ForensicSIM	**Acquisition, Examination, Reporting**	• External SIM cards only • Produces physical facsimiles of SIM for prosecutor and defense, and as a storage record
Forensic Card Reader	**Acquisition, Reporting**	• External SIM cards only
SIMCon	**Acquisition, Examination, Reporting**	• External SIM cards only
Mobiledit! Forensic	**Acquisition, Examination, Reporting**	• Also recover information from SIM card, when inserted in handset
SIMIS	**Acquisition, Examination, Reporting**	• External SIM cards only