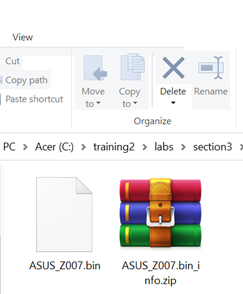
**Pengambilan Image menggunakan Magnet Axiom**

**7.5. Data logikal Ponsel Asus Z007**

Analisis data logikal dari ponsel Asus seri Z007 akan melakukan ekstraksi terhadap data di dalam perangkat tanpa harus melakukan modifikasi terhadap perangkat keras. Perlu diketahui sebelumnya bahwa proses pembuatan image dari perangkat tidak dijelaskan pada bagian ini, melainkan langsung melakukan analisis forensika digital erhadap image yang telah dibuat sebelumnya.

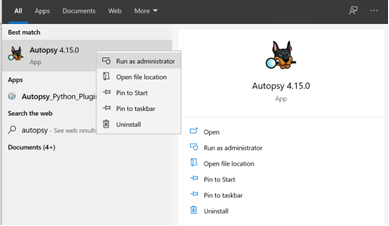
|  |
| --- |
| * Software Autopsy yang dapat diunduh di url: https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.21.0/autopsy-4.21.0-64bit.msi * File image yang ada di: \labs\bab7\images\. |



Gambar 7.2 File image perangkat Z007

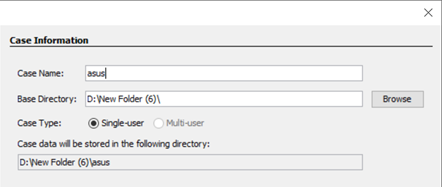
Terdapat dua (2) file yaitu ASUS\_Z007.bin dan ASUS\_Z007.bin\_info.zip dimana ahli akan menggunakan file .bin dalam tahap analisis.

* Jalankan Autopsy dengan Privilege Administrator untuk memberikan akses penuh ke aplikasi, yang nantinya akan berguna untuk pengenalan hard drive dan fungsi lain dari sistem operasi.



Gambar 7.3. Menjalankan aplikasi Autopsy

* Mulai menjalanankan aplikasi Autopsy, dan pilih new case.  
    
  Gambar 7.4. Tampilan awal autopsy
* Konfigurasikan informasi kasus, termasuk nama kasus dan direktori dasar untuk menyimpan hasilnya. Ahli mengatur bagian ini berdasarkan harddisk.



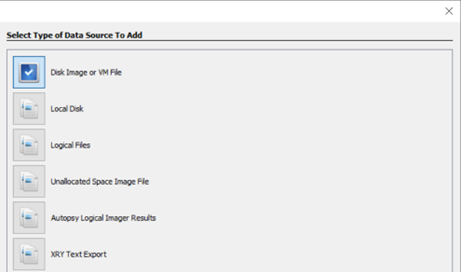
Gambar 7.5. Informasi kasus

* Bagian ini bersifat opsional untuk dilengkapi, karena berisikan nomor kasus, identitas ahli, catatan,dan informasi terkait lainnya.



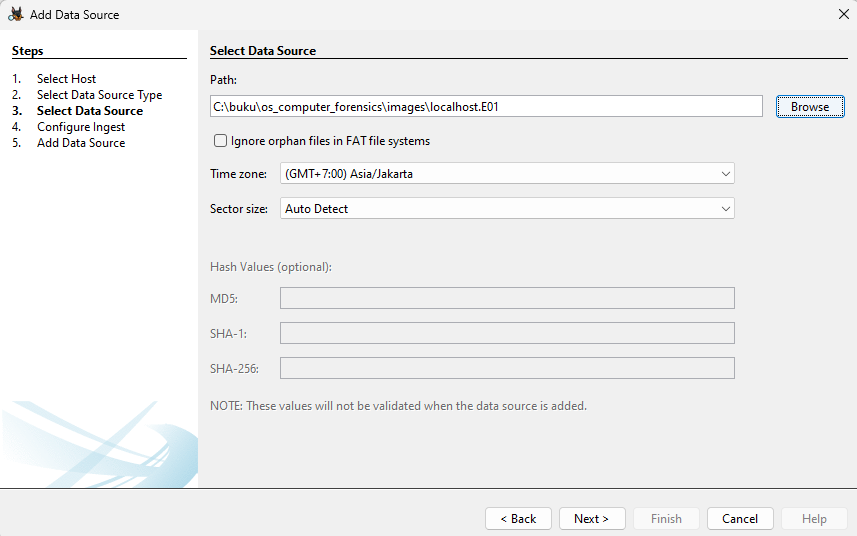
Gambar 7.6. Informasi tambahan

* Pilih jenis sumber data yang akan ditambahkan. Untuk tahap ini, ahli memilih Disk Image atau VM File untuk menambahkan image ponsel yang berhasil dibuat sebelumnya.

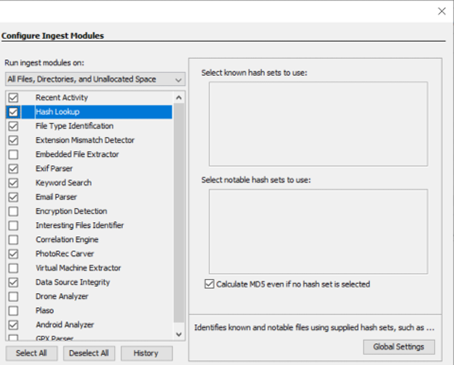


Gambar 7.7. Tipe data source

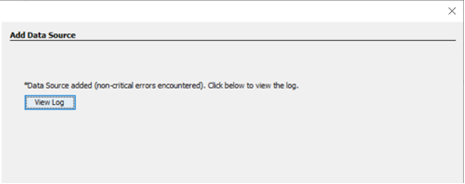
* Mulai tambahkan file gambar bukti (ASUS\_Z007.bin) dari direktori \labs\bab7\images\

Gambar 7.8. Input data source

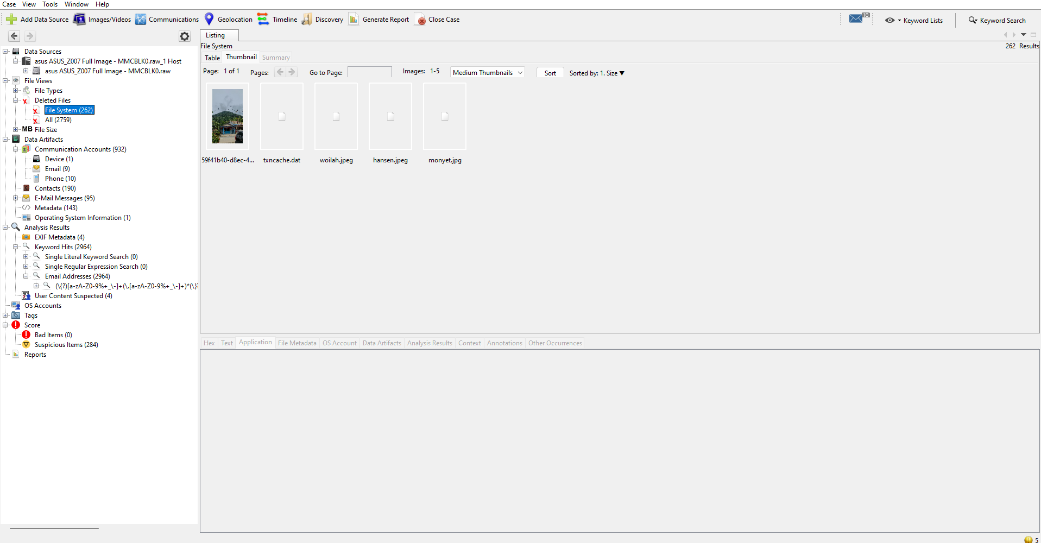
* Centang semua ingest modules dari daftar berikut ini:
  + Recent activity
  + Hash Lookup
  + File type identification
  + Extension Mismatch Detector
  + Exif parser
  + Keyword search
  + Email parser
  + Photorec carver
  + Android analyzer

Gambar 7.9. Ekstensi tambahan

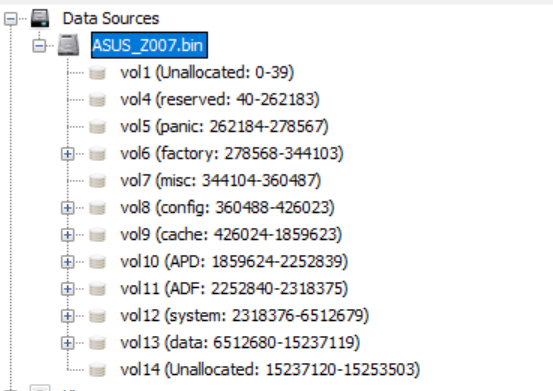
* Setelah itu tinggal menunggu proses analisis hingga selesai.

Gambar 7.10. Data berhasil ditambahkan

* Berikut merupakan tampilan awal dari autopsy. Sambil menunggu selesainya proses pemeriksaan, ahli dapat melihat artefak dan informasi lain yang terkait dengan barang bukti. Perlu diingat, proses pemeriksaan di bagian kanan bawah harus selesai agar dapat melakukan analisa lebih lanjut.

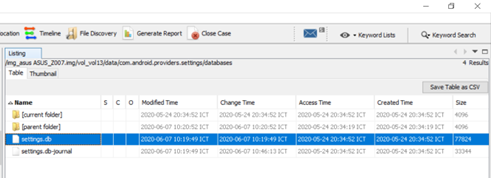
Gambar 7.11. Tampilan data pada autopsy

* Menampilkan semua partisi setelah tahap ekstraksi dari image. Dari penelusuran, diketahui data disimpan pada vol13.

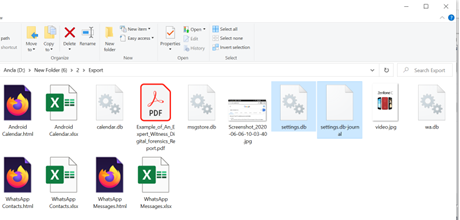


Gambar 7.12. Partisi pada android

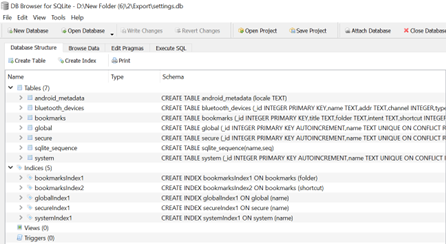
* Menemukan lokasi semua database yang disimpan dalam image. Diketahui pula bahwa file database berada di lokasi  
  /img\_asus ASUS\_Z007.img/vol\_vol13/data/com.android.providers.  
  Settings/databases/

Gambar 7.13 Database pada android

* Perhatikan file "settings.db" dan ekstrak file tersebut ke direktori yang diekspor untuk dianalisis dengan alat lain.

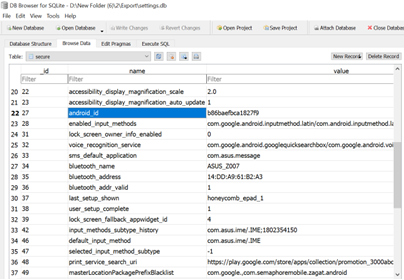
Gambar 7.14 Isi file export android

* Jelajahi database dengan alat DB Browser SQLite. Dan tampilkan daftar struktur database.



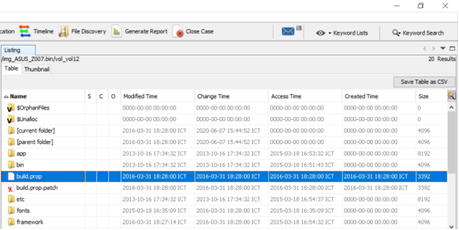
Gambar 7.15 Struktur database

* Pindah ke tab browse data dan pilih tabel ”secure”. Diperoleh pula informasi tambahan mengenai perangkat, yaitu:
  + Android\_id: b86baefbca1827f9
  + Nama\_Bluetooth: ASUS\_Z007
  + Alamat\_Bluetooth: 14: DD: A9: 61: B2: A3

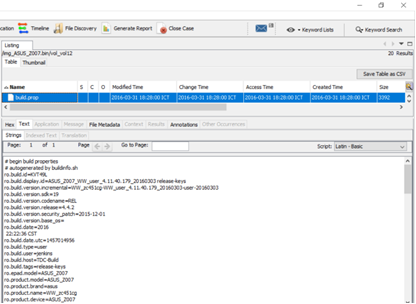


Gambar 7.16 Tab browse pada sqlite

* Cari file /system/build.prop dan ekstrak semua informasi berharga tentang perangkat seluler. Lihat pada daftar partisi dan pilih vol12.

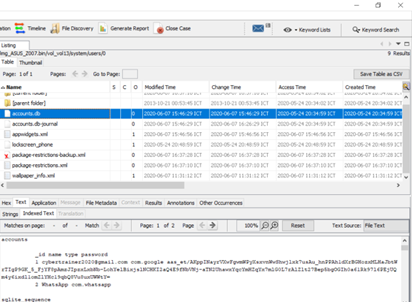
Gambar 7.17 Daftar partisi

* tekan nama "build.prop" pada daftar tabel. Lalu lihatlah detail pada teks Tab di bawah ini. Temukan semua informasi penting tentang perangkat sebagai contoh:
  + build.version.release = 4.4.2
  + product.model=ASUS\_Z007



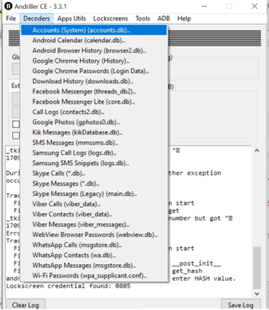
Gambar 7.18 Informasi perangkat android

* Ekstrak file account.db dan account.db-journal dari gambar dan simpan dalam direktori ekspor default di dalam direktori kasus. File tersebut berada di lokasi direktori: /img\_ASUS\_Z007.bin/vol\_vol13/system/users/0



Gambar 7.19 File account db

* Menggunakan Andriller untuk mengekstrak dan menerjemahkan data dari file accounts.db

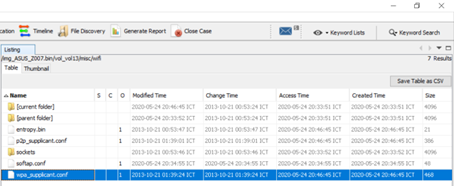


Gambar 7.20 Aplikasi Andriller

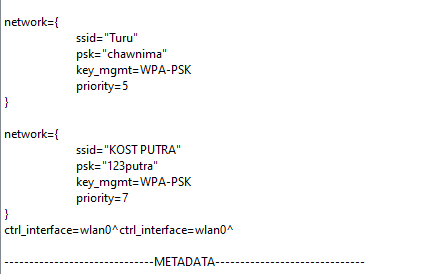
* Browser saat ini akan secara otomatis terbuka dan menunjukkan hasilnya. Lihatlah kolom Kata Sandi, teks kata sandi masih terenkripsi

Gambar 7.21 Hasil Andriller

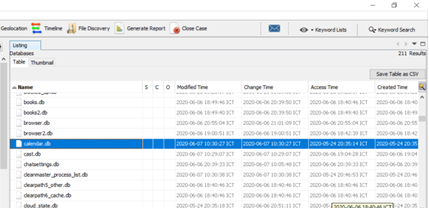
* Temukan berkas ini, "wpa\_supplicant.conf" di lokasi direktori: /img\_ASUS\_Z007.bin/vol\_vol13/misc/wifi/

Gambar 7.22 Wpa\_supplicant.conf

* Buka wpa\_supplicant.conf dengan pindah ke tab Teks di bawah daftar tabel. Bagian ahli adalah membuat daftar semua informasi berharga dari berkas tersebut.

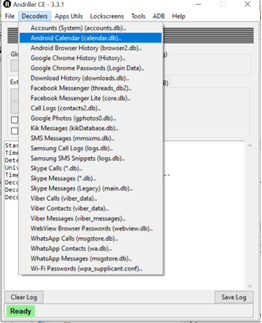
Gambar 7.23 Isi file wpa\_supplicant

* + serial\_number=F5AZB7029588
  + device\_type=10-0050F204-5
  + ssid="turu" dan “kost putra”
  + psk="chawnima" dan “123putra”
  + key\_mgmt=WPA-PSK
* Membaca agenda tersembunyi dari pemilik ponsel. Fungsi kalender dan semua data akan disimpan di "calendar.db". Temukan lokasi file calendar.db pada gambar. Lokasi db kalender ada di: /img\_asus ASUS\_Z007.img/   
  vol\_vol13/data/com.android.providers.calendar/databases/



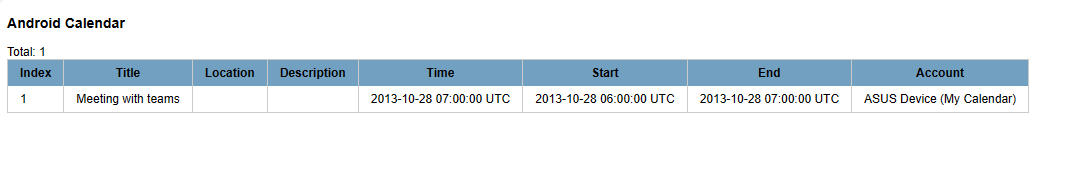
Gambar 7.24 Memeriksa calender.db

* Ekstrak file calendar.db ke direktori ekspor autopsy. Dan buka dengan Andriller untuk menganalisis

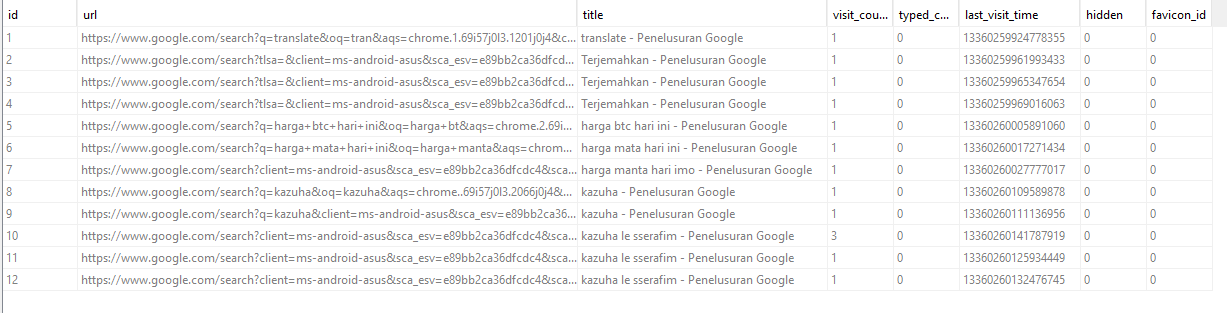


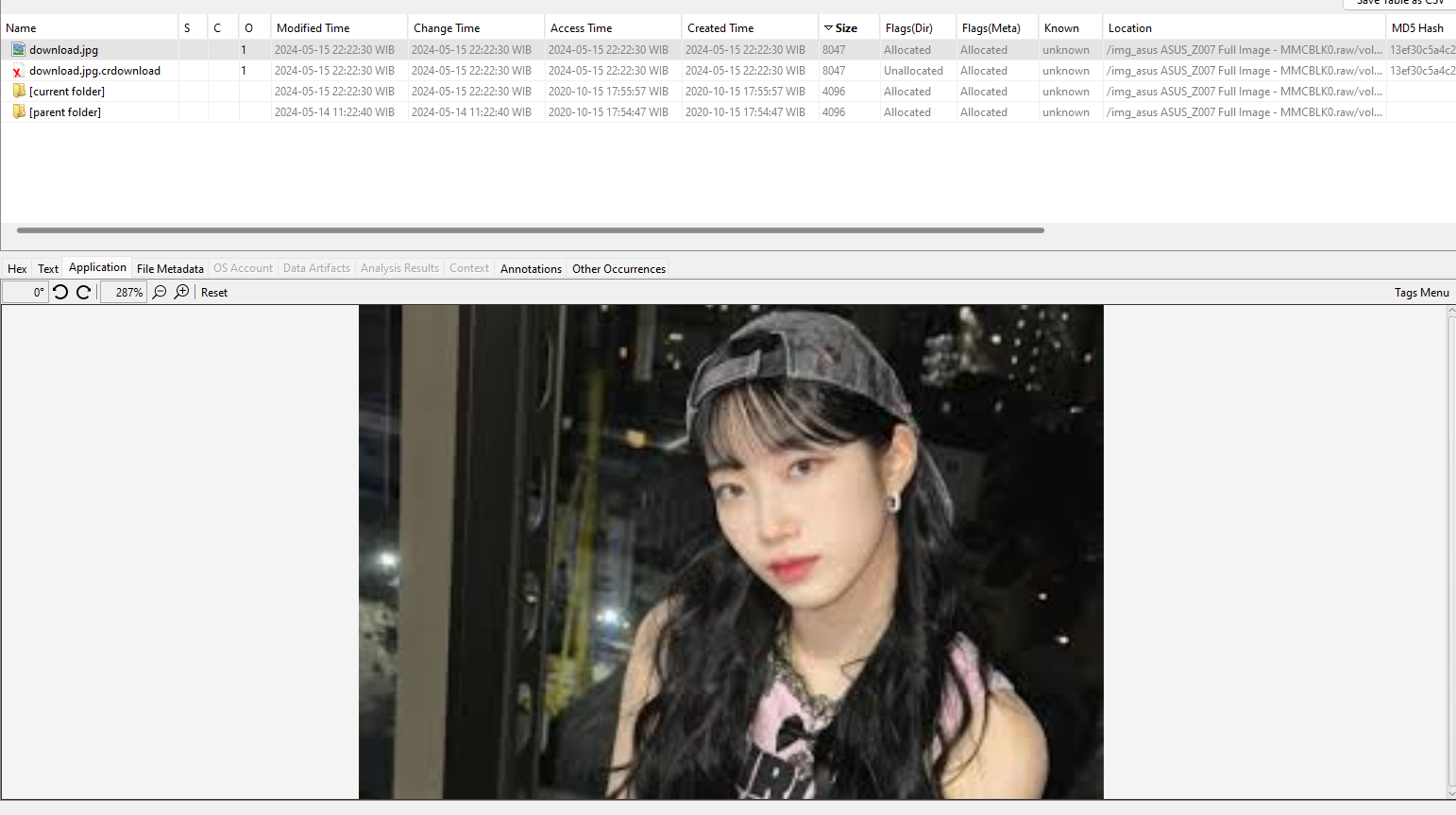
Gambar 7.25 Proses Ekstraksi calendar

* Andriller dapat memecahkan kode data dari "calendar.db" dengan lancar. Dengan membuka browser, ahli dapat melihat agenda tersembunyi dari pemilik ponsel dengan seseorang di luar. Informasi yang diperoleh seperti berikut:
  + Judul: Meeting with teams
  + Tanggal Mulai: 2013-19-28 06:00:00 UTC
  + Tanggal berakhir: 2013-19-28 07:00:00 UTC
  + Akun: ASUS Device

Gambar 7.26 Hasil andriller

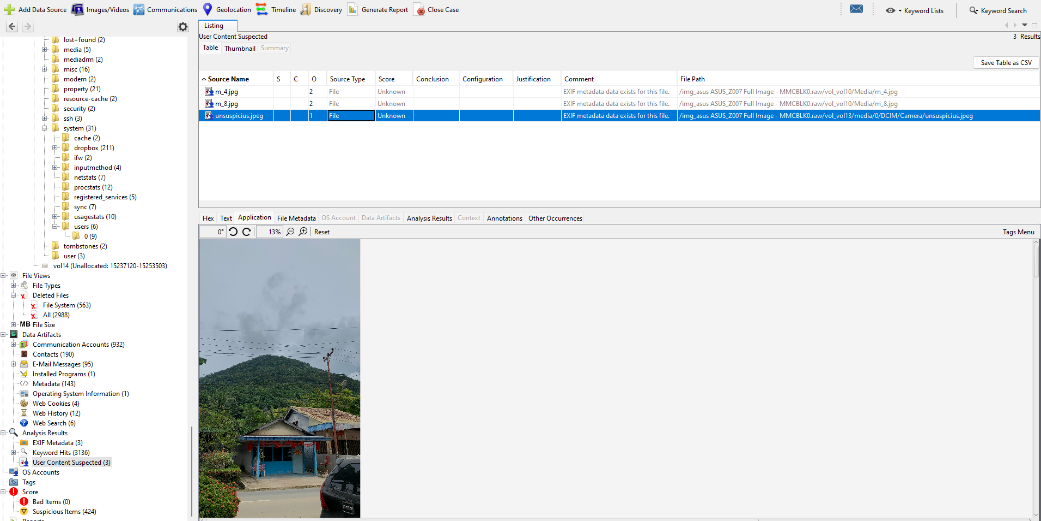
* Buat daftar semua pencarian kata kunci yang diketik di browser oleh pemilik ponsel dengan membuka: /img\_ASUS\_Z007.bin/vol\_vol13/  
  data/com.android.chrome/app\_chrome/Default/History

Gambar 7.27 Daftar browser yang diakses

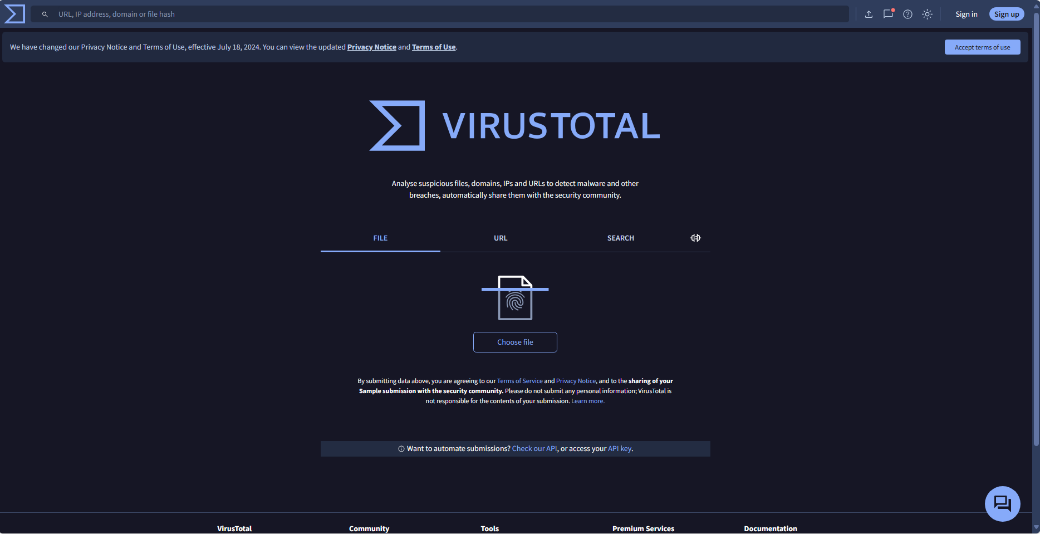
* Ahli juga melihat file apa saja yang diunduh pada browser pada lokasi: /img\_ASUS\_Z007.bin/vol\_vol13/media/0/Download  
  

Gambar 7.28 File unduhan dari android

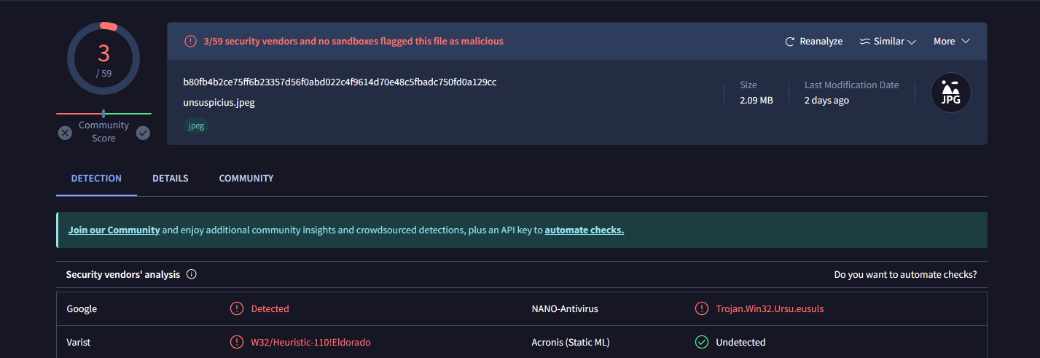
* Selanjutnya bukalah “user content suspected” dan extract lah file bernama “unsuspicius.jpeg”

Gambar 7.29 File gambar pada android

* Bukalah website <https://www.virustotal.com/gui/home/upload> untuk melakukan analisis terhadap gambar tersebut

Gambar 7.30 Website virustotal

* Masukan gambar ke website tersebut dan tunggu proses selesai, dapat terlihat bahwa file tersebut teridentifikasi sebagai virus.

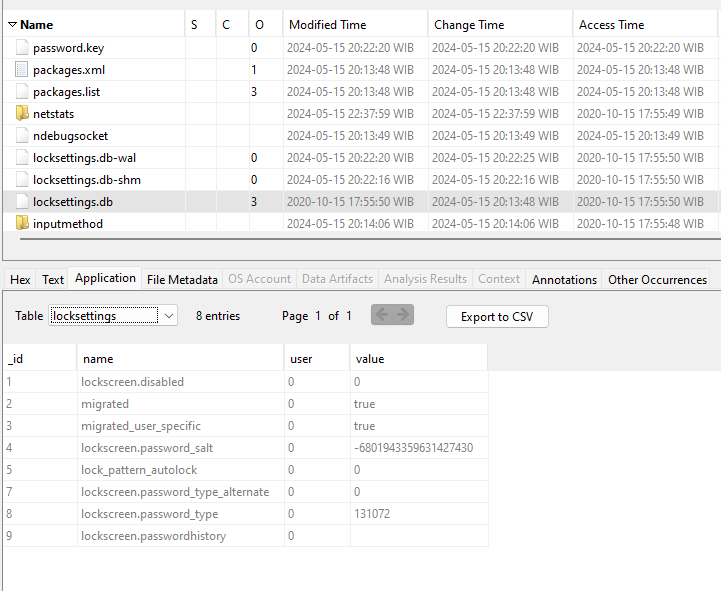
Gambar 7.31 Hasil scan virustotal

Cara untuk meretas perangkat Android adalah dengan melewati layar kunci. Pengguna sering menggunakan pola, pin, atau kunci pintar seperti wajah tepercaya untuk mengamankan perangkat mereka

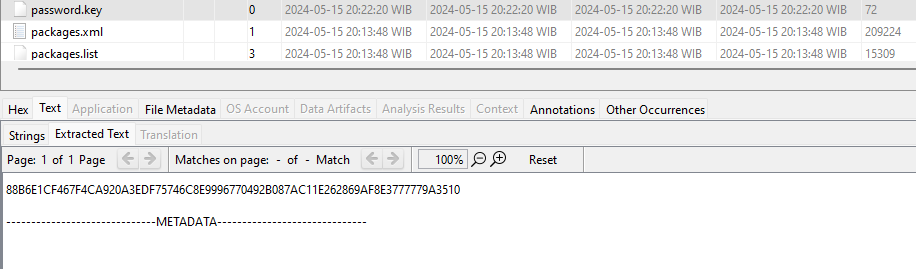
* Android menyimpan kunci pola di /data/system/gesture.key.
* OS meng-hash pin dan kata sandi di /data/system/password.key.
* Android menyimpan salt hash tersebut dan menyimpannya di /data/system/locksettings.db.

Alat seperti Andriller dapat mencoba dan memecahkan kunci PIN. Ahli menggunakan cara yang sama untuk mendapatkan kode PIN pembuka kunci untuk mendekripsi file gambar.

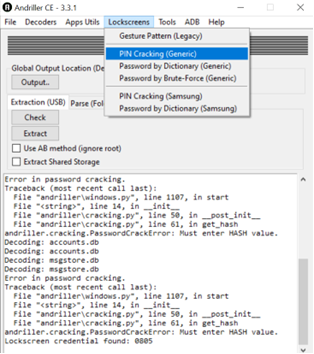
* Metode buka kunci PIN/kata sandi juga bergantung pada hash yang tersimpan dari otorisasi pengguna; namun, metode ini juga menggunakan salt acak 64-bit per pengguna sebagai basis data SQLite, bersama dengan pengaturan lain yang terkait dengan layar kunci.
* Salt disimpan di lokasi: img\_ASUS\_Z007.bin/vol\_vol13/system/locksettings.db.

Gambar 7.33 Informasi dari file locksettings.db

* Hash kata sandi disimpan dalam file /img\_ASUS\_Z007.bin/vol\_vol13/system/password.key, yang berisi gabungan nilai hash SHA-1 dan MD5 kata sandi. Isi file mungkin terlihat seperti ini:

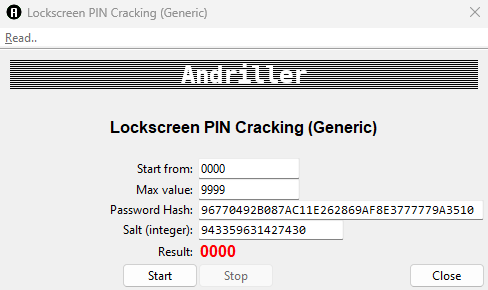
Gambar 7.33 Metadata

* Ahli menggunakan Andriller untuk memecahkan PIN/kata sandi dari perangkat seluler.



Gambar 7.34 Andriller untuk password cracking

* Dengan informasi sebelumnya tentang salt kata sandi layar kunci dan kunci kata sandi, ahli lanjutkan dengan memecahkan pin/kata sandi.
  + Salt kata sandi layar kunci: 943359631427430
  + Kunci kata sandi: 88B6E1CF467F4CA920A3EDF75746C8E9996770492B087AC11E262869AF8E3777779A3510
  + Ahli berhasil mendapatkan hasil PIN/kata sandi dari barang bukti yang dicurigai. Nomor kode PIN pembuka kunci adalah 0000.

Gambar 7.35 Proses password cracking Andriller

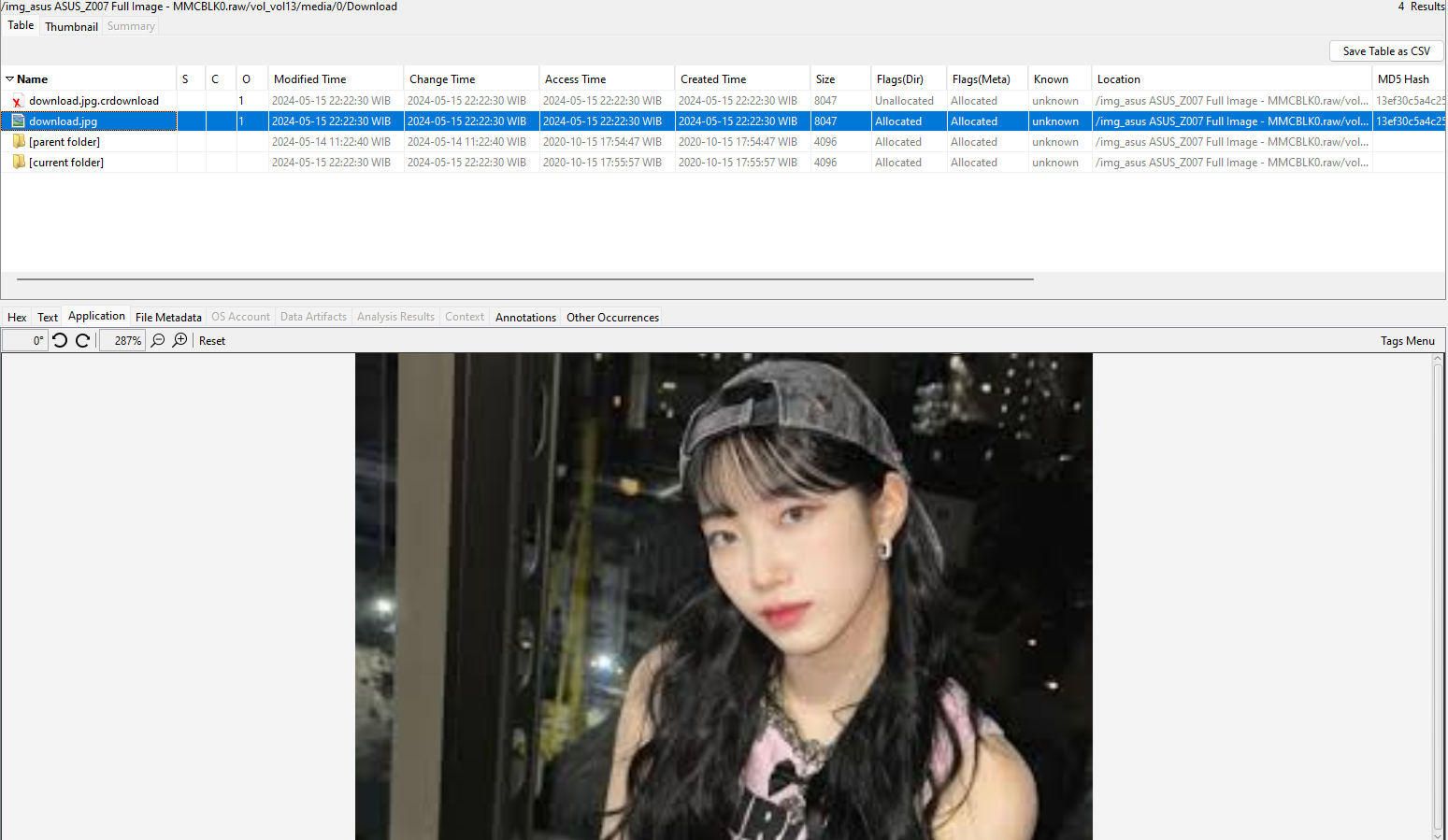
**7.6. Fitur Tambahan Autopsy**

Menggunakan fitur lain dari Autopsy memberikan pengalaman dan Menggunakan fitur lain dari Autopsy memberikan pengalaman dan pengetahuan kepada ahli tentang barang bukti. Tentu saja, hal ini dapatsemakin menambah kelengkapan laporan investigasi yang dibuat, dan berguna dalam menyelesaikan investigasi dari suatu kasus. Dibutuhkan beberapa jam untuk mendapatkan artefak data lengkap dari barang bukti.

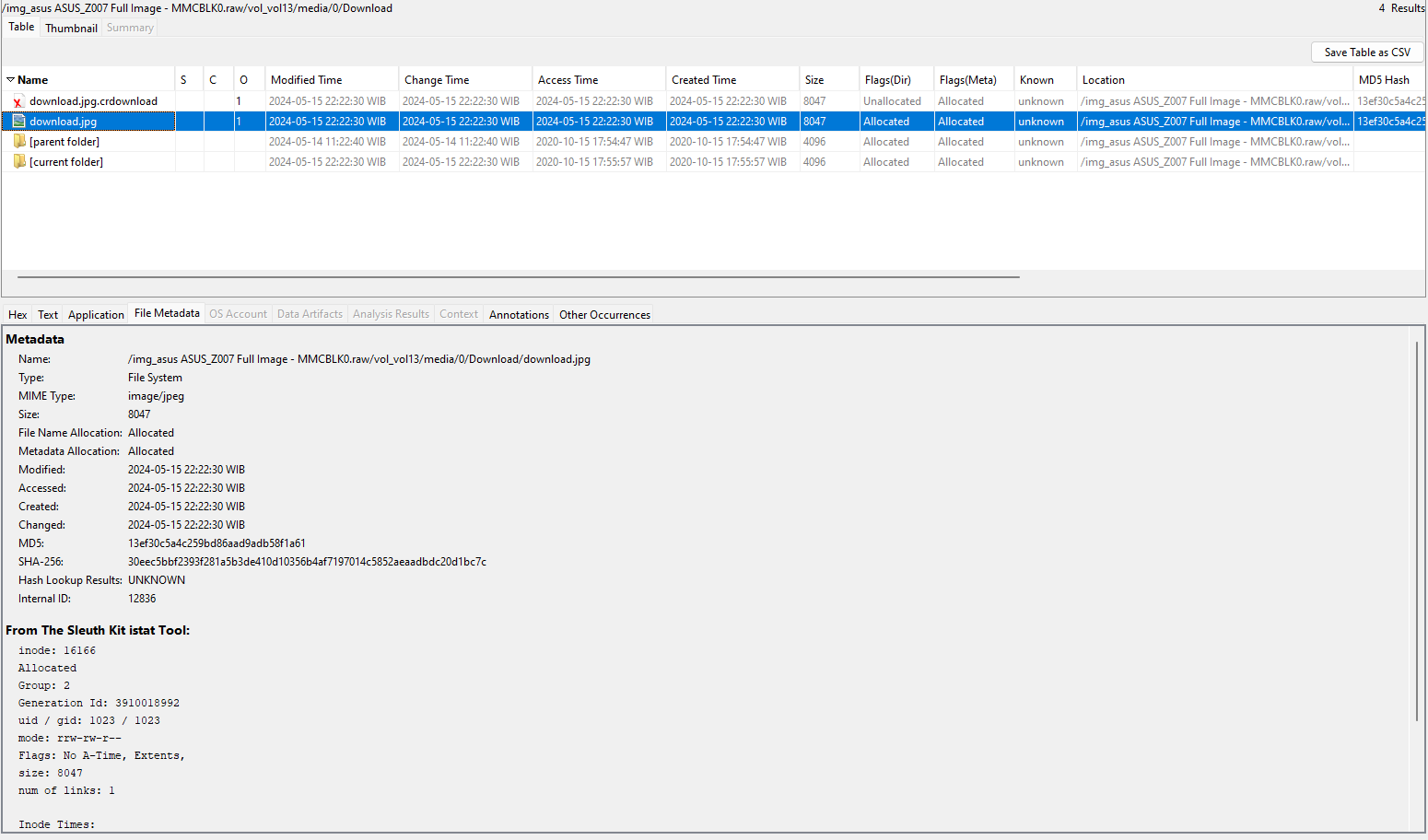
**7.6.1. Galeri Gambar/video**

Mengumpulkan banyak artefak berupa file gambar, dan file video yang dapat dibuka seluruhnya setelah proses pemeriksaan selesai. Tampilan galeri gambar yang baru telah dibuat secara eksplisit dengan digunakan untuk berbagai jenis investigasi lain yang mencakup gambar dan video. Ini merekomendasikan fitur yang dihasilkan di luar daftar panjang thumbnail tradisional yang saat ini disediakan oleh Autopsy dan alat lainnya. Pada setiap partisi (vol) dalam struktur direktori barang bukti, ahli dapat melihat informasi lengkap dari sebuah artefak. Sebagai contoh:

* Atribut dan nilai
* Kategori

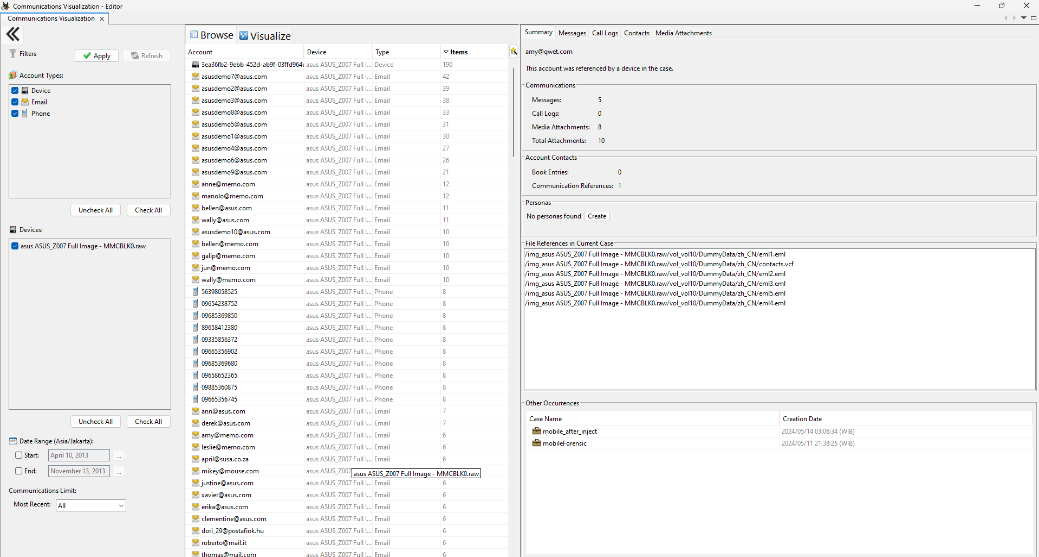
Gambar 7.36 Gambar diunduh

* Dari gambar-gambar tersebut juga dapat mengakses menu Content Viewer, dengan melakukan Klik Kanan pada media tersebut.

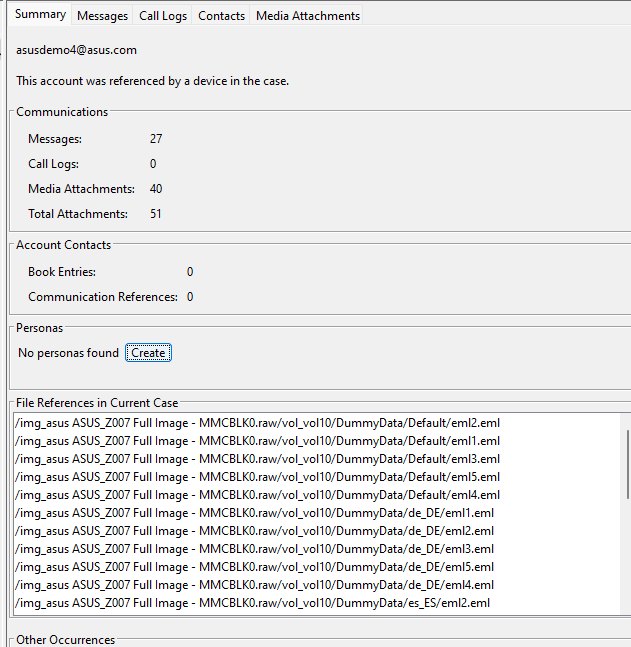
Gambar 7.37 Menu content viewer

**7.6.2. Communication**

* Communications Visualization Tool memberikan tampilan gabungan dari semua peristiwa komunikasi untuk kasus tersebut dan memungkinkan ahli untuk melihat data komunikasi dengan cepat seperti akun yang paling sering digunakan Komunikasi dalam jangka waktu tertentu.

Gambar 7.38 Log komunikasi pada android

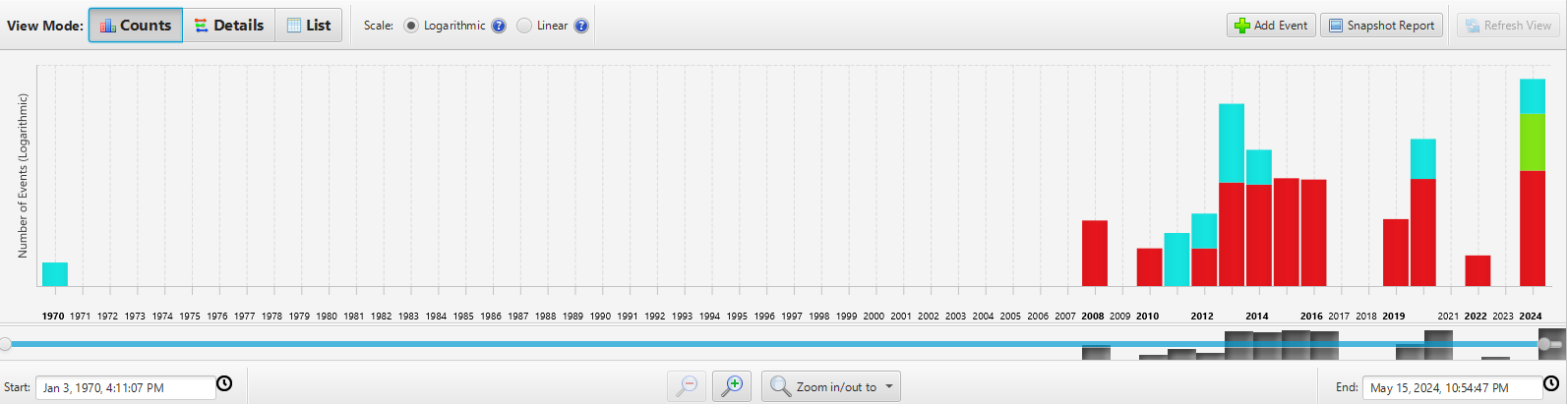
Menampilkan beberapa informasi dari menu tab di sisi kanan jendela alat. Ahli dapat menjelajahi informasi yang lebih rinci dari Ringkasan, Pesan, Log Panggilan, Kontak, dan Lampiran Media.



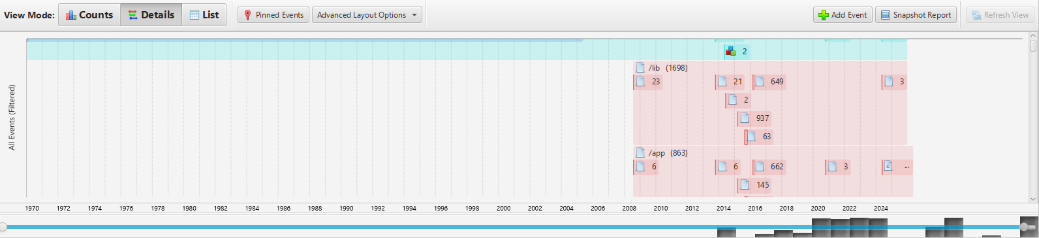
Gambar 7.39 Ringkasan lengkap proses log

**7.6.3. Timeline**

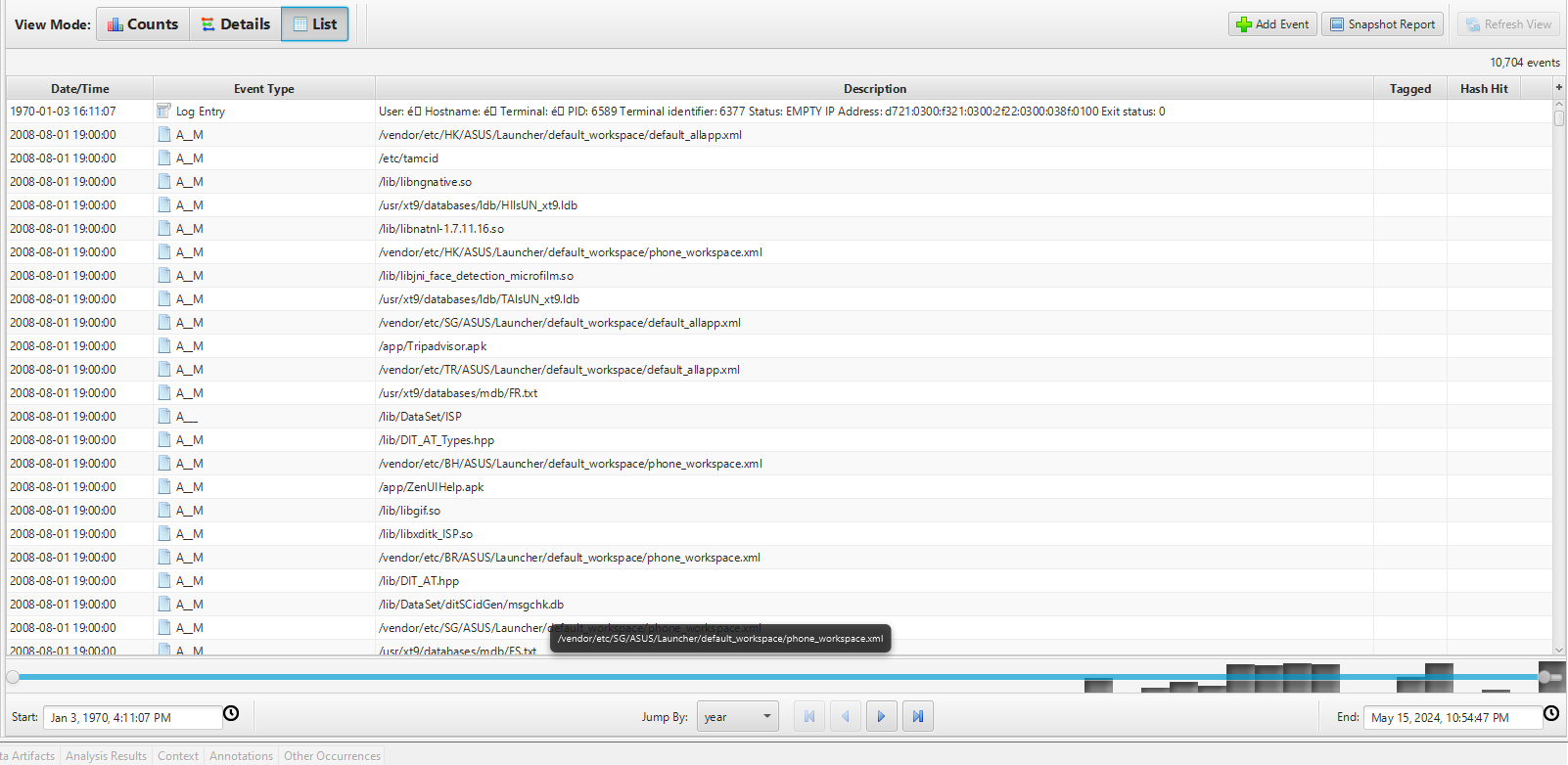
* Analisis timeline sangat berguna untuk berbagai jenis pemeriksaan, yang sering kali digunakan untuk menanggapi permintaan tentang kapan peristiwa komputer terjadi. Memiliki tiga jenis mode tampilan, membuat fitur timeline memberikan pengetahuan yang berbeda kepada ahli dalam menemukan informasi detail artefak.
  + View Mode: Counts

Gambar 7.40 View mode counts

* + View Mode: Details

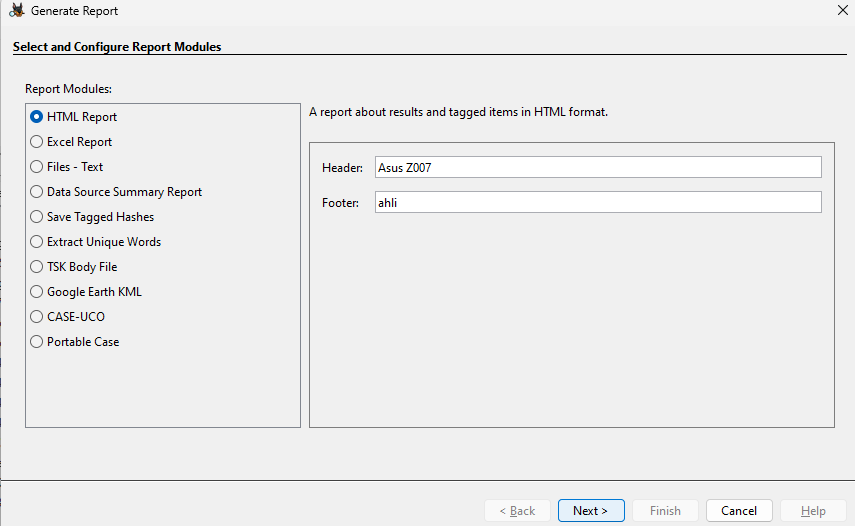
Gambar 7.41 View mode details

* + View Mode: List

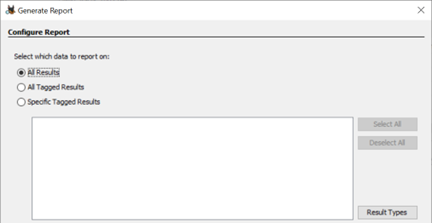
  
Gambar 7.42 View mode details

**7.6.4. Laporan**

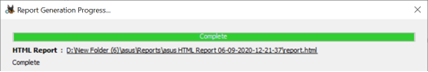
* Fungsi pembuatan laporan pemeriksaan secara otomatis merupakan salah satu fitur yang harus digunakan oleh ahli. Laporan dari alat Forensika digital digunakan sebagai bahan penelitian dari kegiatan investigasi kasus. Untuk beberapa pelaporan kegiatan penanganan perkara pidana, laporan Forensika digital menjadi lampiran dokumen dalam Berita Acara Pemeriksaan untuk mendukung analisis barang bukti digital yang telah diperoleh. Tentunya dokumen tersebut menjadi konfirmasi atas analisis bukti digital dari artefak yang ditemukan.
* Buka menu "Buat Laporan" dari dasbor

Gambar 7.43 Tipe laporan

* Setelah memilih jenis laporan, pilih di antara berikut ini:
  + All results
  + All tagged results
  + Specific tagged results

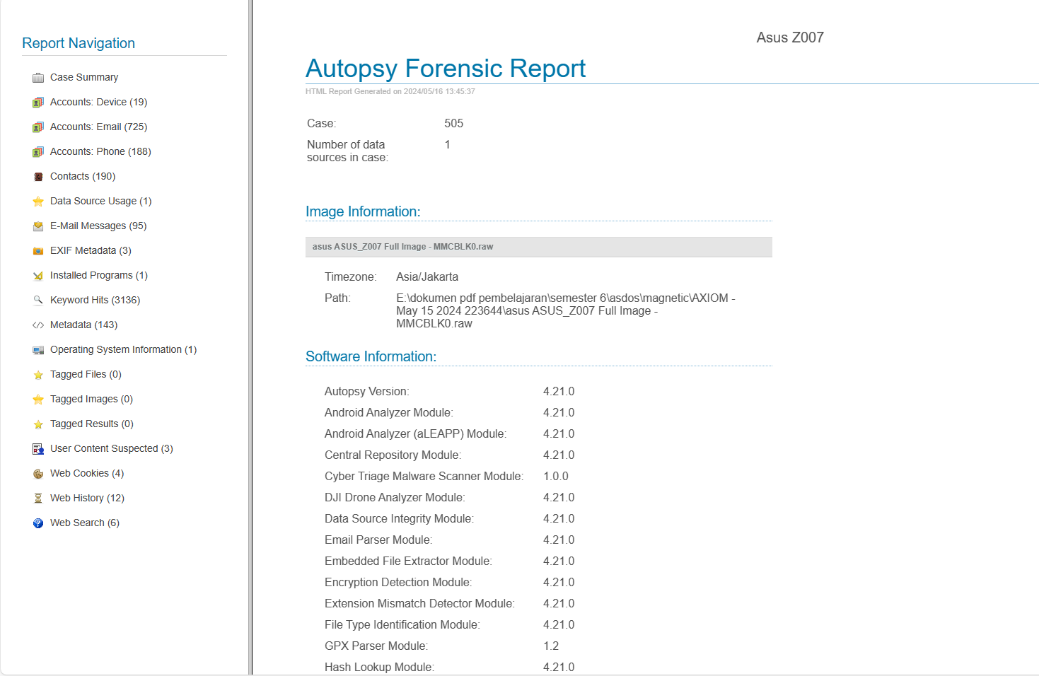
Gambar 7.44 Konfigurasi laporan

* Tampilan saat pembuatan laporan berhasil diselesaikan.



Gambar 7.45 Proses menghasilkan laporan

* Setelah proses pembuatan laporan selesai, lanjutkan dengan membuka tautan yang tersedia dan secara otomatis membuka browser untuk menampilkan laporan.

Gambar 7.46 Hasil laporan