**Pengambilan: Data menggunakan Guymager pada Linux**

**A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated**

**4.6. Analisis Image Localhost**

Menggunakan studi kasus merupakan cara yang paling tepat dan cepat untuk mengetahui implementasi forensik digital. Untuk itu telah disiapkan sebuah gambar logika pada mesin yang menggunakan sistem operasi Windows, yang dapat digunakan oleh ahli dalam mengeksplorasi dan terlibat dalam kegiatan simulasi analisis digital forensik.

Alat FTK Imager membantu ahli untuk mengumpulkan memori volatil (RAM) lengkap dari sebuah komputer. Memori akses acak atau RAM adalah sistem penyimpanan data komputer yang memungkinkan informasi disimpan dan diambil pada komputer. Karena informasi diakses secara acak dan bukan secara berurutan seperti pada hard drive, komputer dapat mengakses data dengan lebih cepat. Namun, salah satu kelemahan RAM adalah membutuhkan daya untuk menjaga agar data tetap dapat diakses.

Semua informasi yang disimpan dalam RAM akan hilang apabila kehilangan sumber daya. Semua program yang berjalan di sistem menyimpan data dalam RAM, dan ini berarti seberapa banyak bukti yang dapat ditampung oleh RAM. Beberapa contoh informasi yang mungkin disimpan dalam RAM meliputi:

* Percakapan
* Riwayat penggunaan internet
* Email
* Nama Pengguna dan kata sandi

Berikut langkah-langkah untuk analisis.

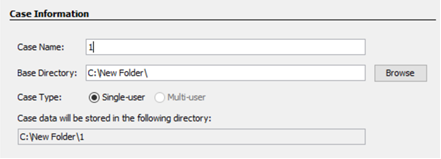
|  |
| --- |
| * Image analisis yang digunakan pada bagian ini disimpan dalam direktori \labs\bab3\images\ |

* Jalankan Autopsy dengan Privilege Administrator untuk memberikan akses penuh ke aplikasi, yang nantinya akan berguna untuk pengenalan harddrive dan fungsi lain dari sistem operasi. Pilih menu New Case untuk memulai analisis.



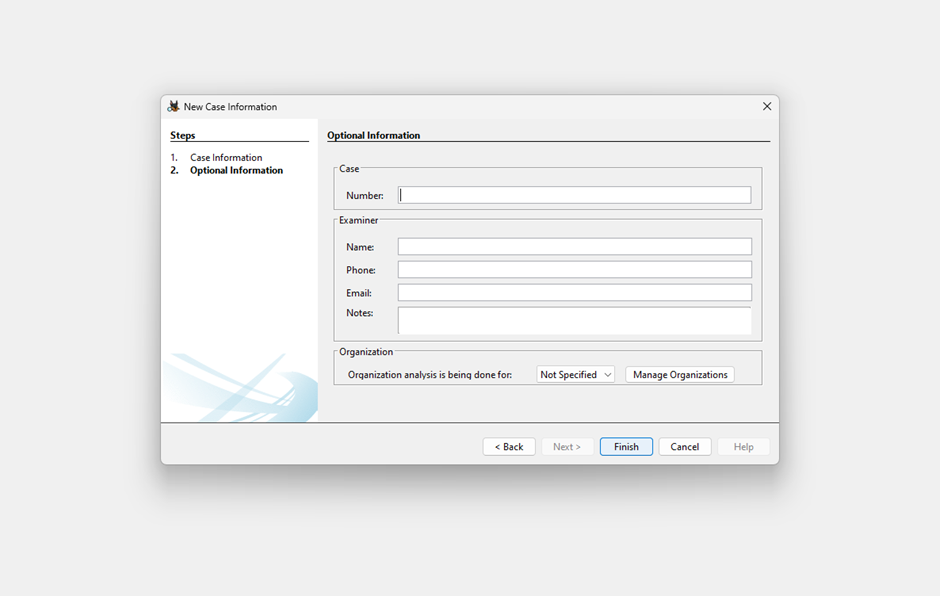
Gambar 4.68. Tampilan Aplikasi Autopsy

* Konfigurasikan informasi kasus, termasuk nama kasus dan direktori dasar untuk menyimpan hasilnya. ahli mengatur bagian ini berdasarkan hard disk.

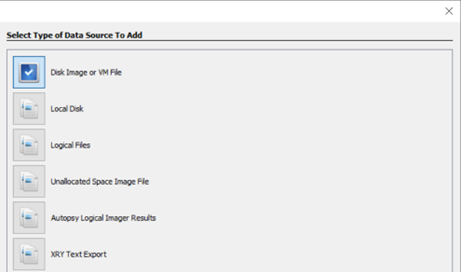


Gambar 4.69. Konfigurasi Nama kasus

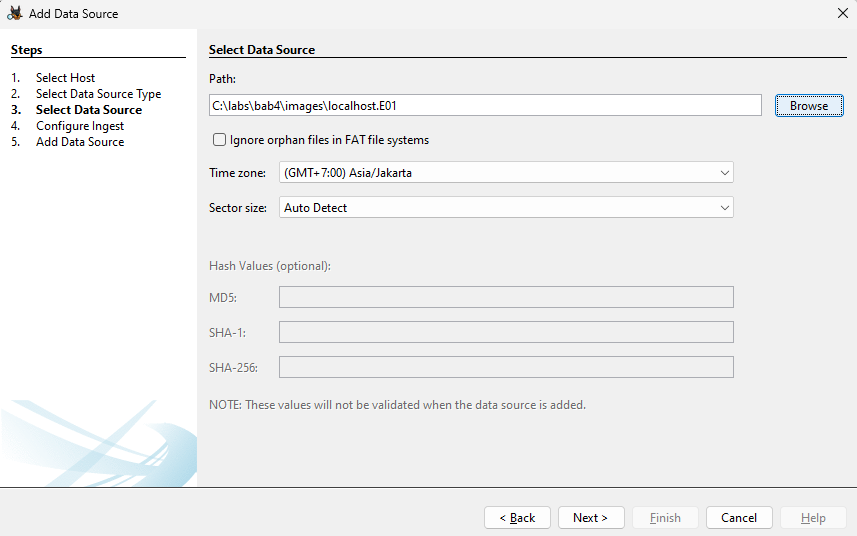
* Tambahan untuk informasi kasus. konfigurasikan nomor, nama, telepon dan email-catatan.

  
Gambar 4.70. Konfigurasi Identitas Ahli

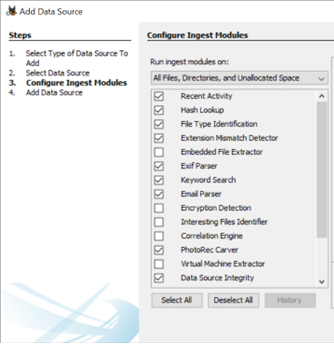
* Pilih jenis sumber data yang akan ditambahkan. Untuk tahap ini, ahli memilih Disk Image atau VM File untuk menambahkan gambar perangkat seluler yang berhasil dibuat sebelumnya.

Gambar 4.71. Pemilihan Sumber Data

|  |
| --- |
| * Mulai menambahkan file image bukti (localhost.E01) dari direktori \labs\bab3\images\ |

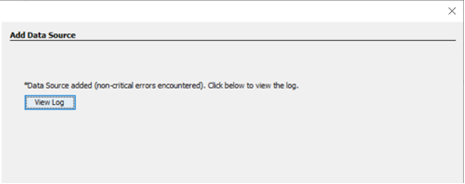
  
Gambar 4.72. Konfirmasi Pemilihan Sumber Data

* Aktifkan semua semua ingest modules di bawah ini:
  + Recent Activity
  + Hash Lookup
  + File Type Identification
  + Extension Mismatch Detector
  + Exif Parser
  + Keyword Search
  + Email Parser
  + PhotoRec Carver
  + Data Source Integrity

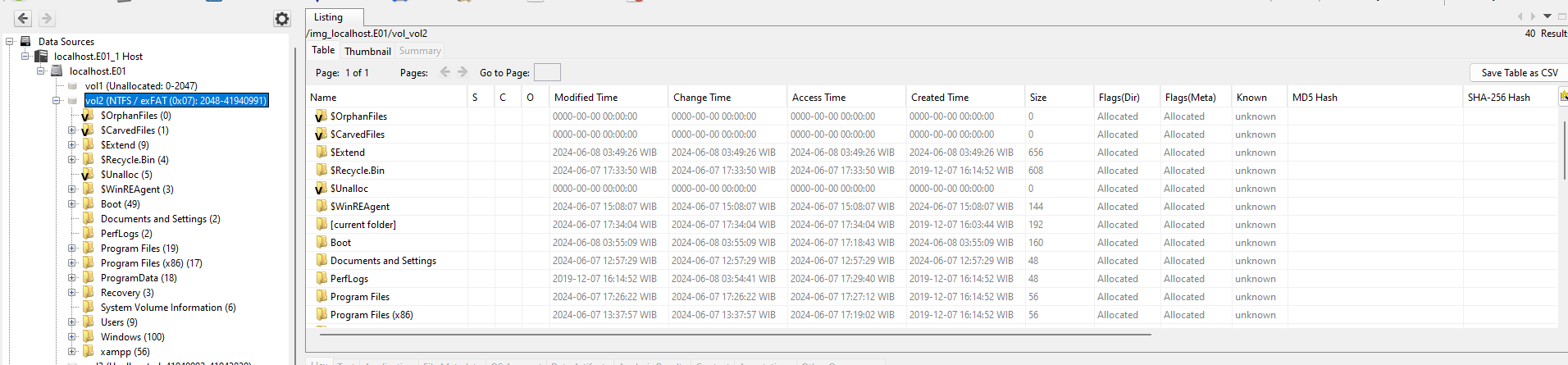


Gambar 4.73. Pemilihan Ingest Module

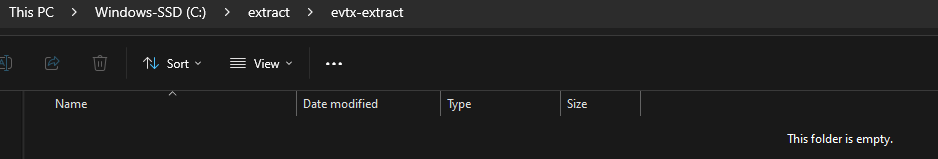
* Tunggu hingga selesai lalu tekan pada bagian silang.

Gambar 4.74. Konfirmasi Konfigurasi

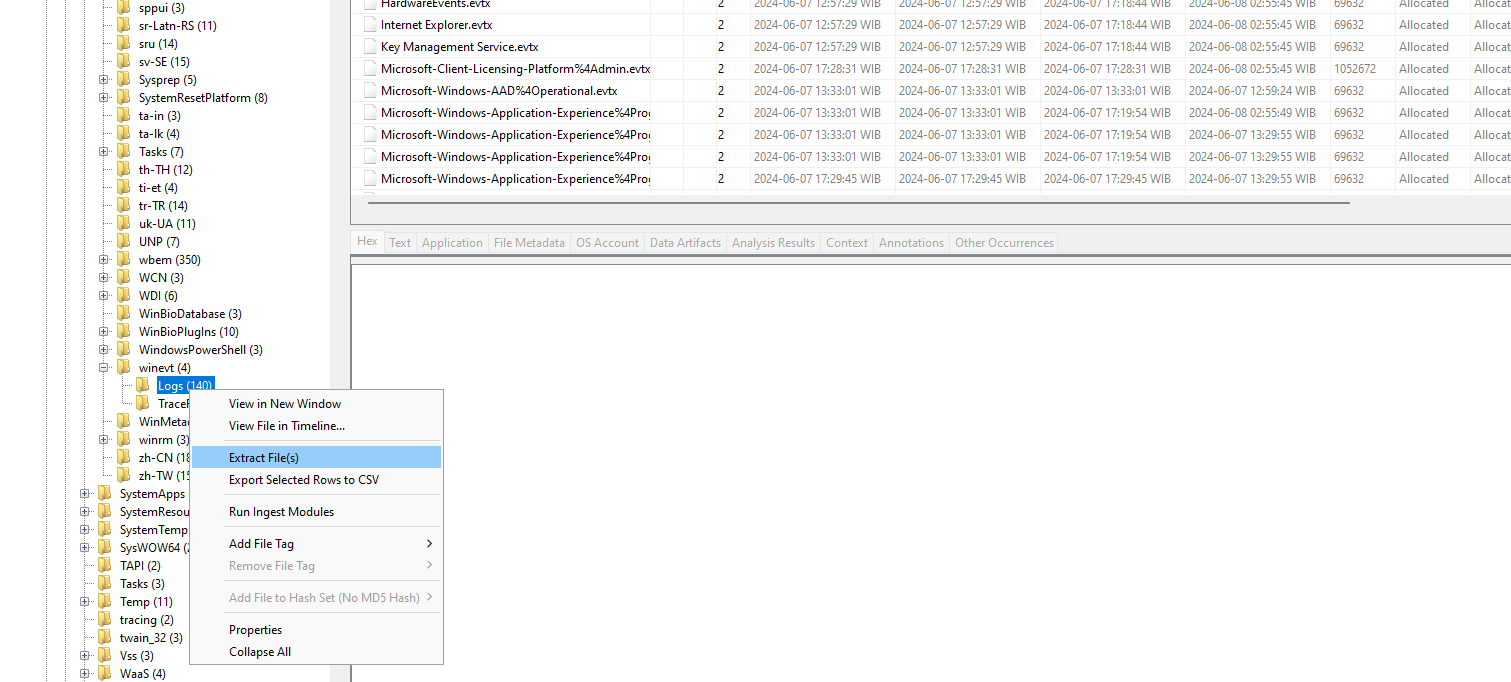
* Berikut adalah tampilan awal dari autopsy. Sambil menunggu selesainya proses pemeriksaan, ahli dapat melihat artefak dan informasi lain yang terkait dengan barang bukti. Perlu diingat, proses pemeriksaan di bagian kanan bawah harus selesai agar dapat melakukan analisis secara optimal dan menyeluruh terhadap image bukti.

  
Gambar 4.75. Tampilan Dashboard

* Eksplorasi drive C dari image logical localhost.E01. Ahli dapat mengekstrak file atau direktori berdasarkan tahap pemeriksaan yang diperlukan. Seluruh struktur dari partisi menunjukkan kondisi nyata dari hard disk bukti
* Autopsy menyediakan fasilitas bagi ahli dalam melakukan ekstraksi data mentah ke dalam hard disk tujuan. Hal ini memudahkan analisis, karena artefak yang dicurigai berada di lokasi lingkungan yang terpisah dari gambar logis. Lanjutkan dengan mengekstrak direktori event log dari Windows yang tersimpan di lokasi direktori C:\windows\system32\winevt\logs\, dan akan disimpan di lokasi direktori baru yang disesuaikan dengan struktur hirarki direktori komputer yang digunakan penguji.
* Buat direktori baru di drive C dengan nama "evtx-extract"

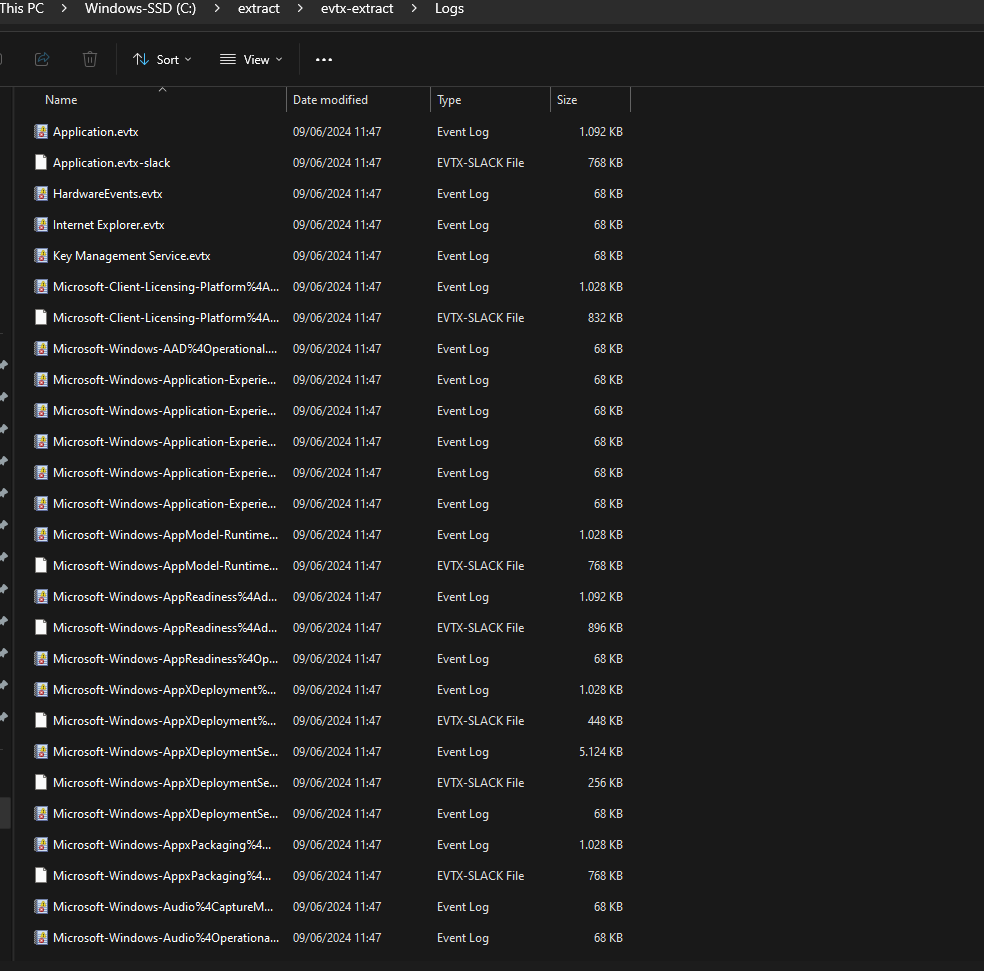
Gambar 4.76. Pembuatan Direktori Penyimpan Hasil Ekstraksi

* Penelusuran direktori yang baru dibuat tersebut dalam file image log, dan klik kanan pada nama direktori log untuk mengekstrak semua ke direktori log C:\evtx-extract



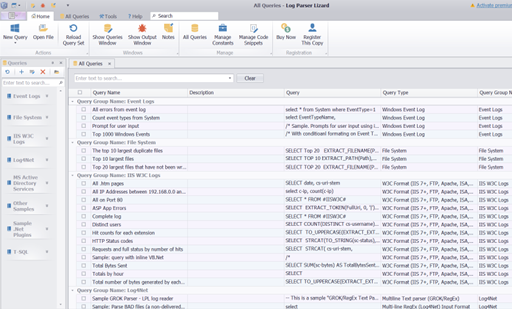
Gambar 4.77. Hasil Ekstraksi di Direktori Evtx-extract

* Hasil dari tahap ekstraksi bukti localhost.E01. ahli mendapatkan 140 data yang disimpan di direktori c:\evtx-extract\Logs\

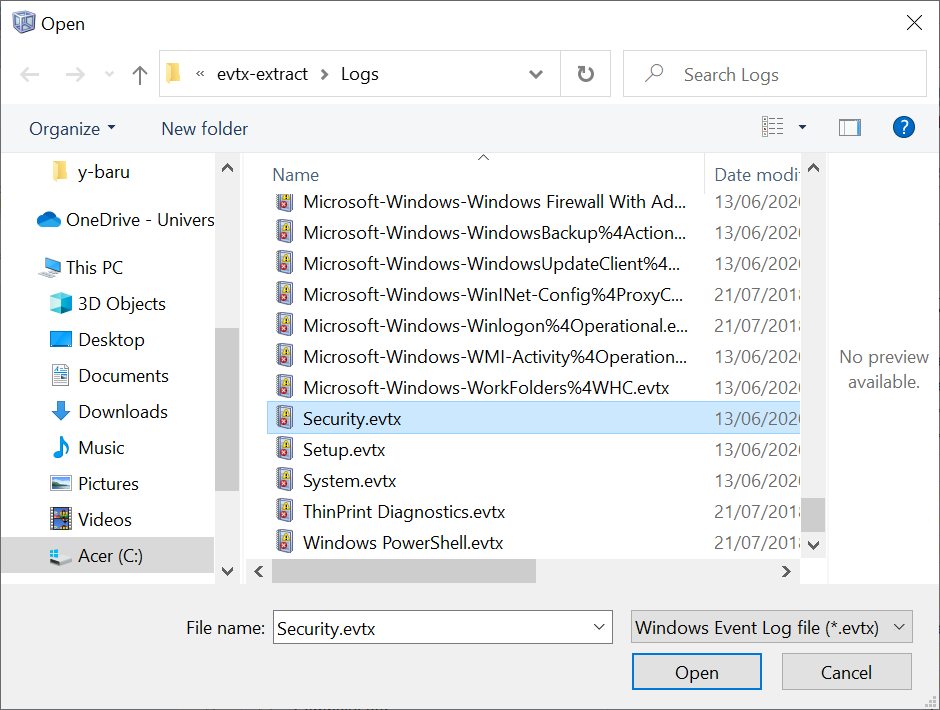
  
Gambar 4.78. Hasil Ekstraksi

**4.6.1. Log Parser Lizard**

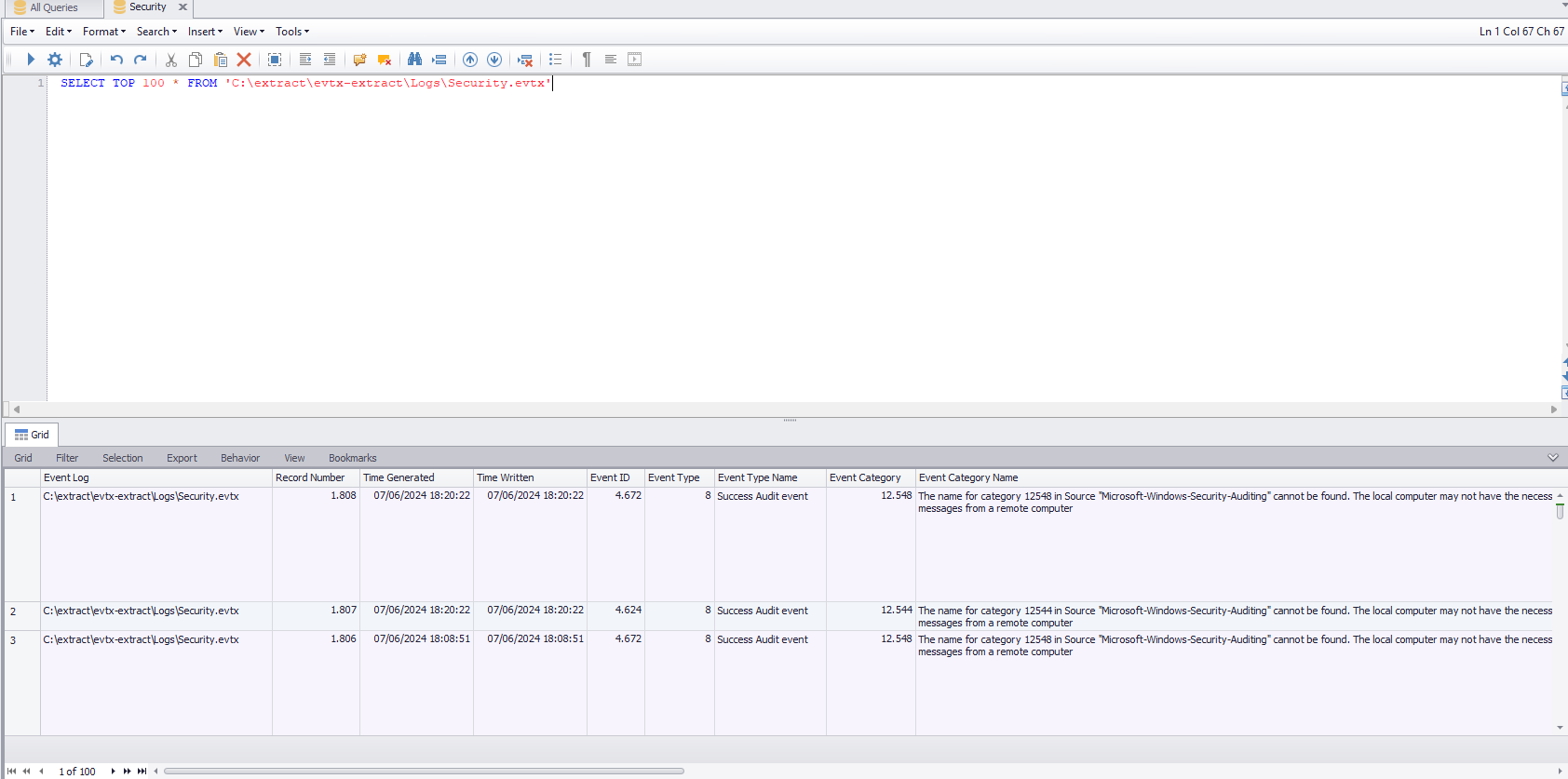
* Mengikuti tutorial sebelumnya yang telah dilakukan dengan tool ini, diharapkan dapat memberikan pengetahuan kepada ahli dalam melakukan query dan mendapatkan hasil dari evtx yang dimaksud dengan alternatif perangkat lunak yang digunakan.

Gambar 4.78. Analisis menggunakan FileParser Lizard

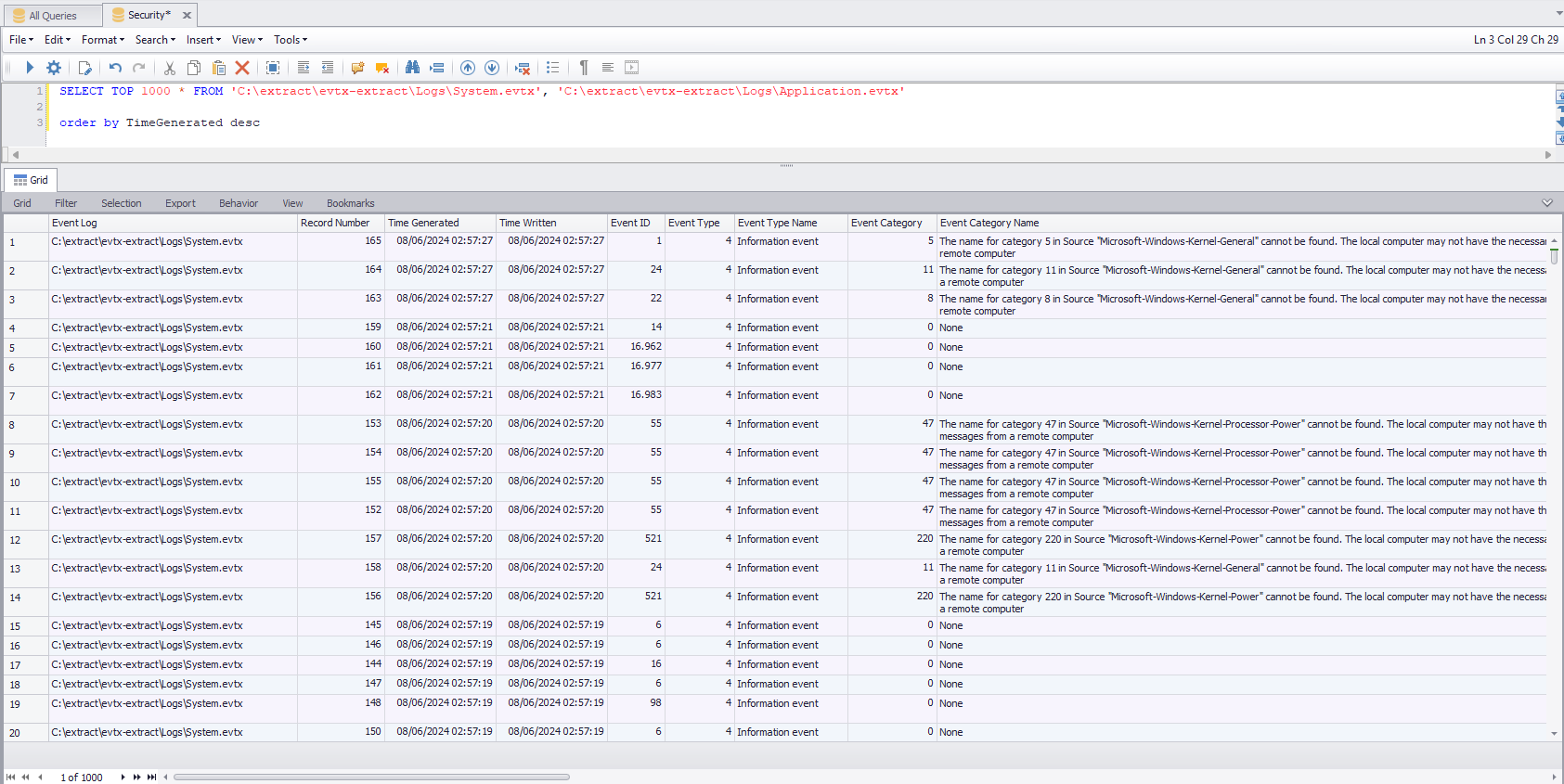
* Buka satu file evtx, yaitu Security.evtx dari direktori gambar logis yang diekstrak. Dari menu File-> Open, untuk selanjutnya mengarahkan ke file Application. Evtx

  
File 4.79. Melakukan analisis file Security.evtx

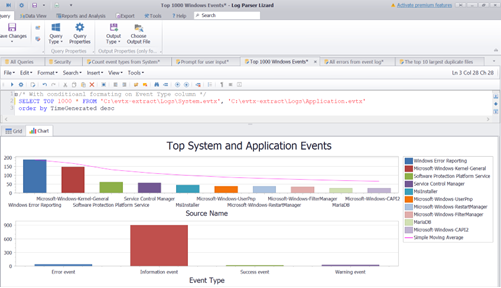
* Setelah file evtx berhasil dibuka oleh aplikasi, aplikasi akan menampilkan kotak untuk melakukan kueri melalui perintah SQL. Jalankan satu fungsi contoh untuk mendapatkan 100 teratas dari file Security.evtx dengan mengetik "run query"
  + SELECT TOP 100 \* FROM 'C:\evtx-extract\Logs\Security.evtx

Gambar 4.80. Fitur Query

* Ahli dapat menggabungkan berbagai perintah SQL untuk memproses data pencarian agar lebih optimal dan lebih cepat. Contoh menunjukkan 1000 Peristiwa Windows teratas. Ahli menggunakan dua file log peristiwa, Sistem dan Aplikasi.
  + SELECT TOP 1000 \* FROM 'C:\evtx-extract\Logs\System.evtx', 'C:\evtx-extract\Logs\Application.evtx'
  + order by TimeGenerated desc

Gambar. 4.81. Penggunaan Query Spesifik

* Salah satu fitur favorit dari alat ini adalah hasil grafik. Sebagai contoh dari perintah SQL di atas, ahli dapat melihat ringkasan grafik dari 1000 kejadian teratas dari log Sistem dan Keamanan



Gambar 4.82. Tampilan Grafik