**Pengambilan: Data menggunakan Guymager pada Linux**

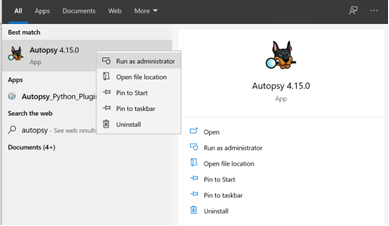
**A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated  
3.4 Kasus: analisis image menggunakan autopsy**

|  |
| --- |
| * Semua image yang digunakan untuk bagian ini disimpan dalam lokasi \labs\bab3\images\. |

* 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.



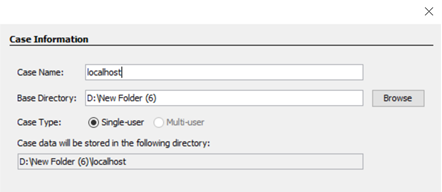
Gambar 3.12. Tampilan Aplikasi Autopsy

* Mulai Autopsy, dan pilih New Case



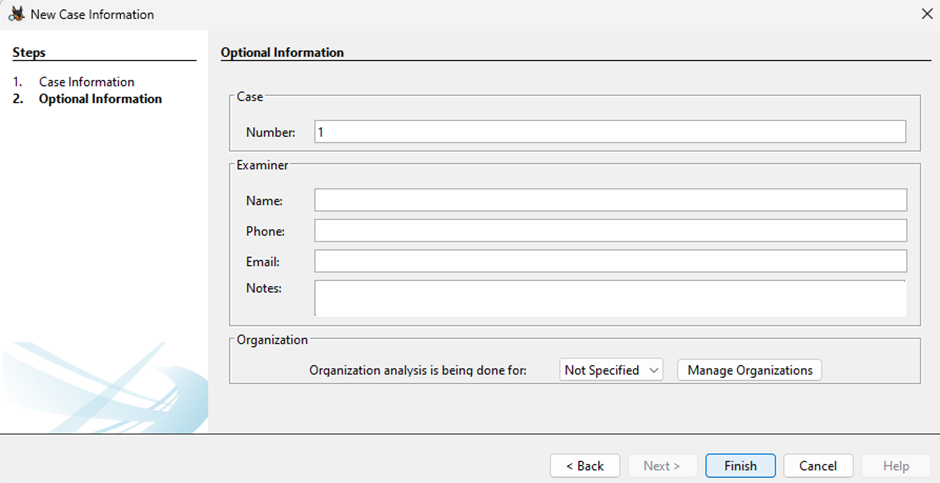
Gambar 3.13. Pemilihan Menu New Case

* Menambahkan informasi kasus, termasuk nama kasus dan direktori dasar untuk menyimpan hasilnya. ahli mengatur bagian ini berdasarkan harddisk.



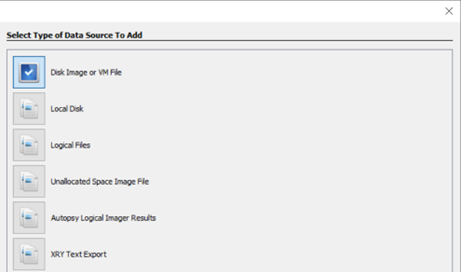
Gambar 3.14. Menambahkan informasi kasus

* Tambahan untuk informasi kasus. Menambahkan informasi nomor, nama, telepon, email-catatan dari ahli.

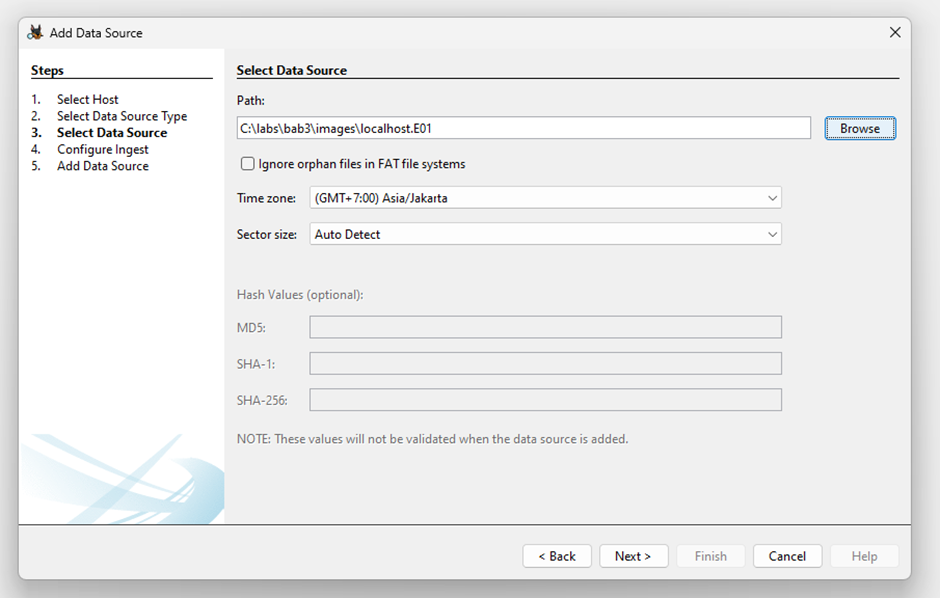


Gambar 3.15. Menambahkan informasi biodata dari Ahli

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

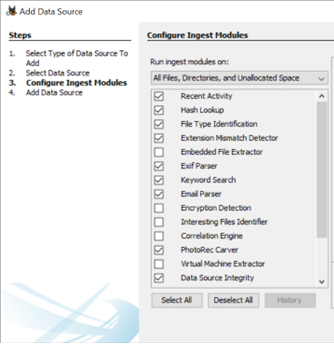
Gambar 3.16. Pemilihan sumber data

* Menambahkan file image contoh bukti (localhost.E01) dari direktori os\_computer\_forensics di \labs\bab3\images\



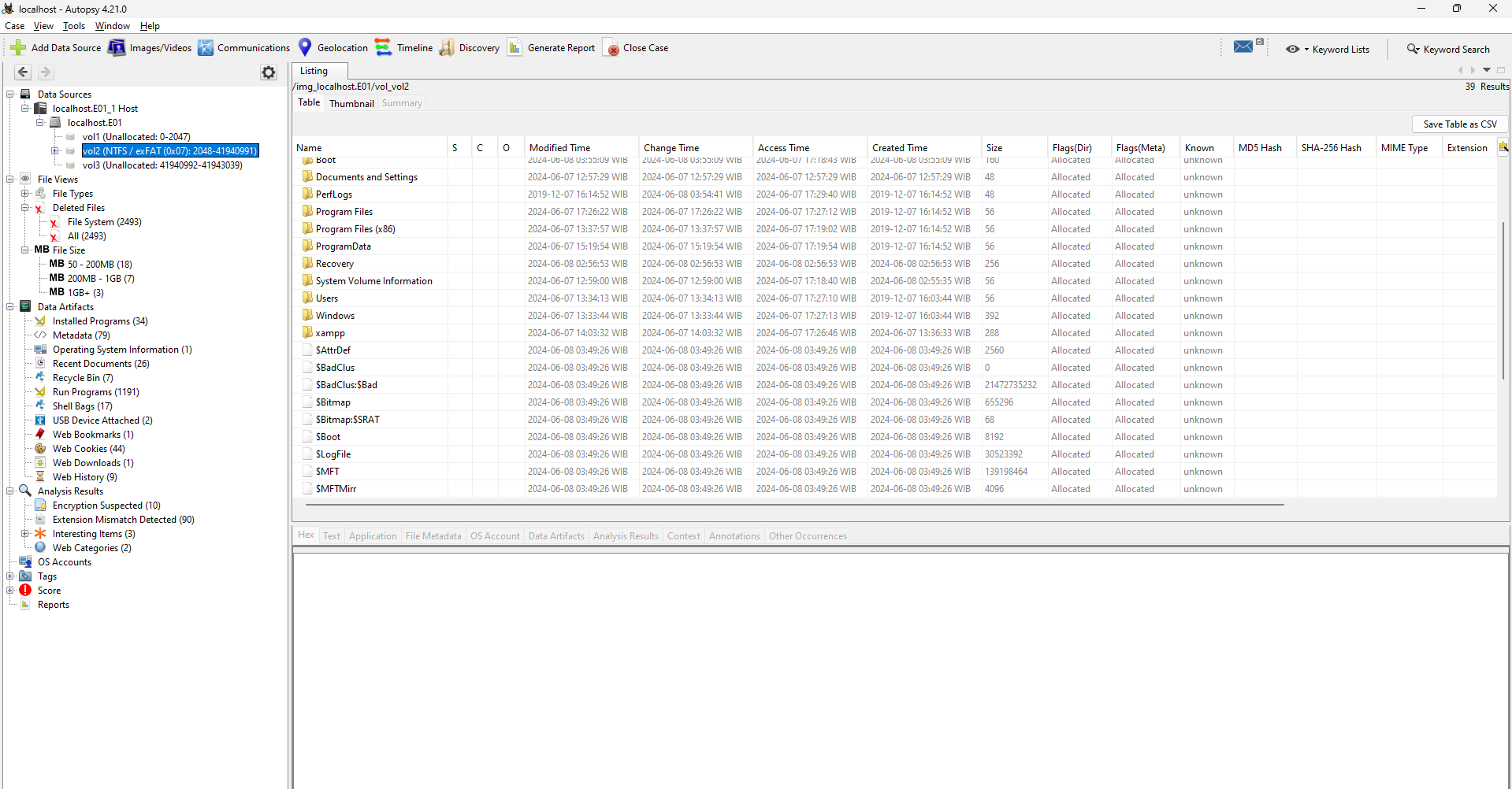
Gambar 3.17. Pemilihan Lokasi Penyimpanan dari Image

* Centang atau aktifkan seluruh Ingest modul di bawah ini:
  + Recent Activity
  + Hash Lookup
  + File Type Identification
  + Extension Mismatch Detector
  + Exif Parser
  + Keyword Search
  + Email Parser
  + PhotoRec Carver
  + Data Source Integrity

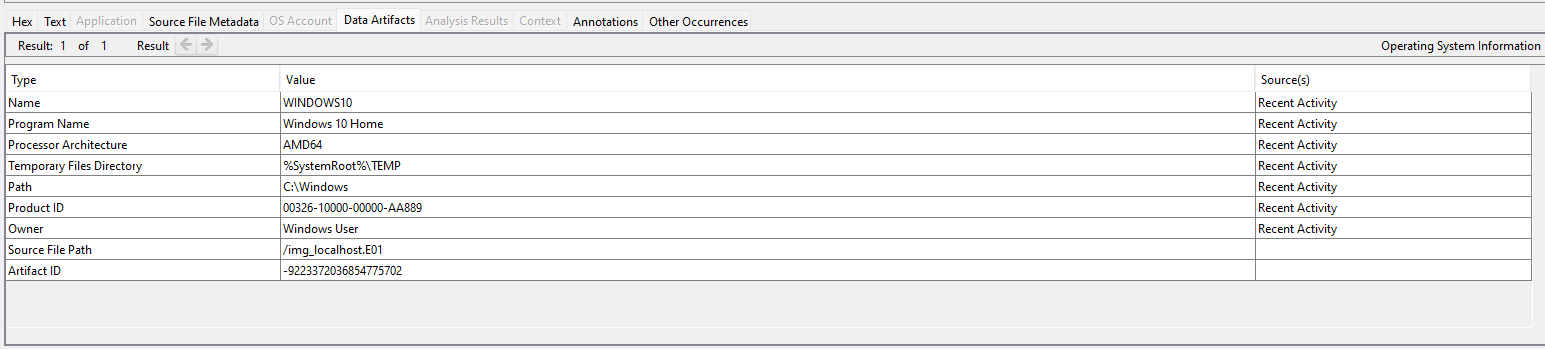


Gambar 3.18. Pemilihan Ingest Module

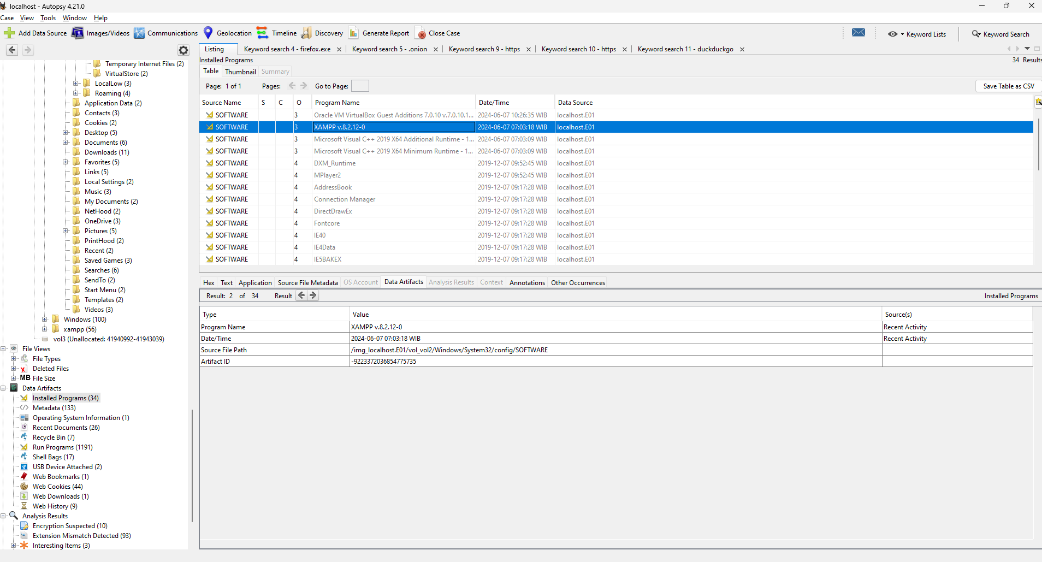
* Tunggu hingga selesai lalu klik pada bagian silang.
* Berikut adalah tampilan awal dari autopsy. Sambil menunggu selesainya proses pemeriksaan, ahli dapat melihat artefak dan informasi lain yang terkait dengan barang bukti. Perlu diingat, proses pemeriksaan di bagian kanan bawah harus selesai agar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

Gambar 3.19. Dashboard Aplikasi Autopsy

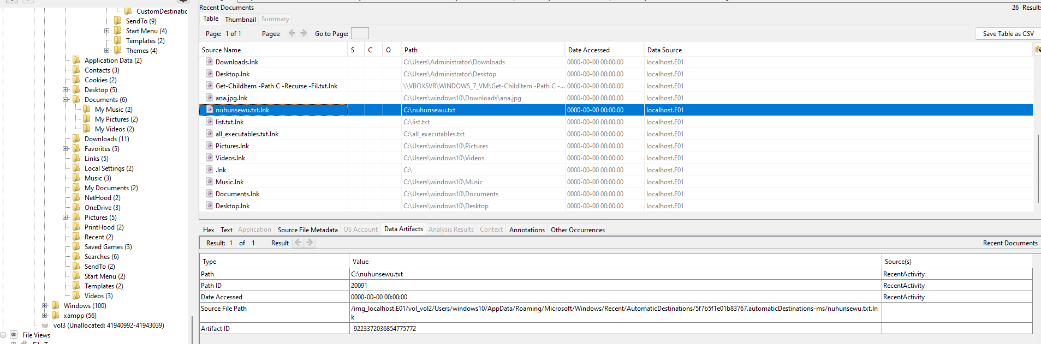
* Jelajahi direktori artifak dan buka bagian “operating system information” untuk mengetahui informasi dasar mengenai sistem operasi dari image.  
  Dapar terlihat bahwa file image ini menggunakan sistem operasi windows 10 Home.

Gambar 3.20. Operating System Information

* Dari konten yang diekstrak, Ahli menemukan semua daftar perangkat lunak yang terinstal di dalam bukti yang terdapat di artefak.

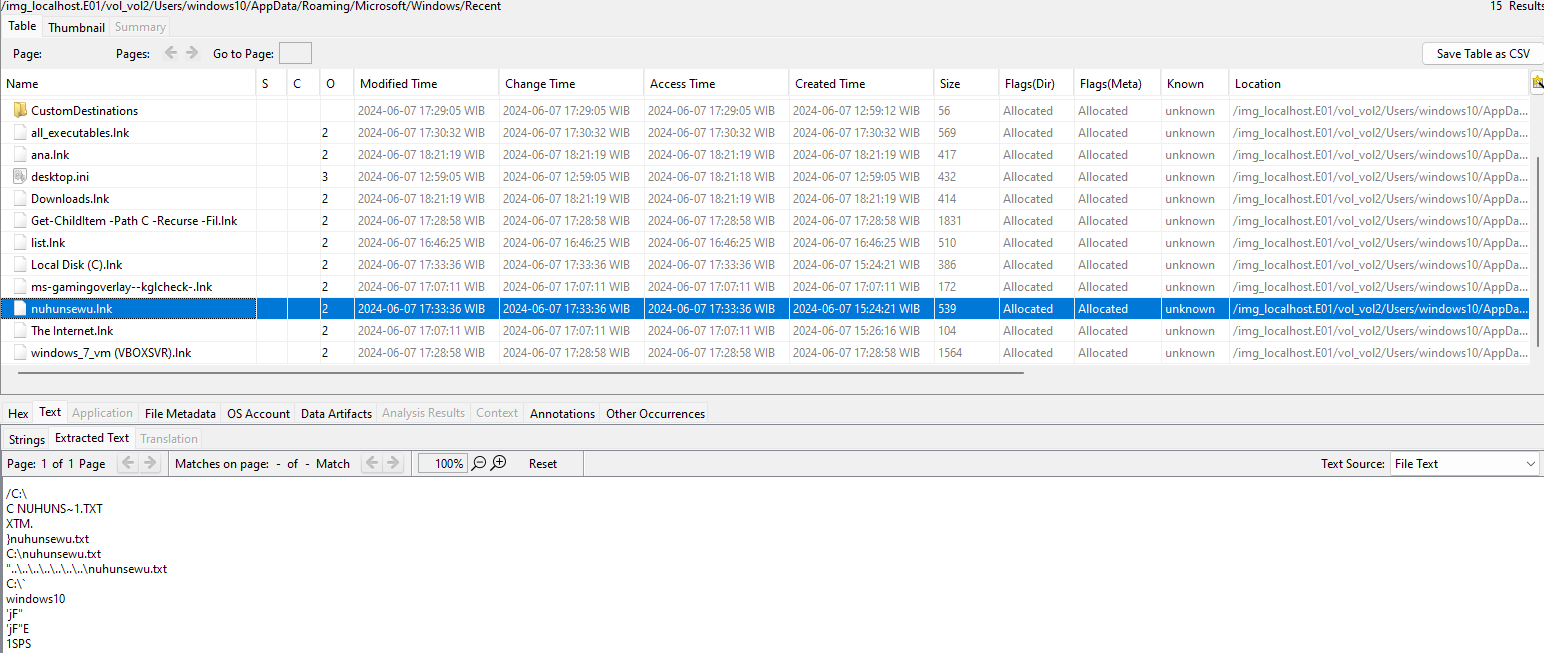
Gambar 3.21. Tampilan detail

* Lanjut, ahli membuka bagaian Recent Documents yang terdapat di artifak. Ahli menemukan file bernama “nuhunsewu.Ink”

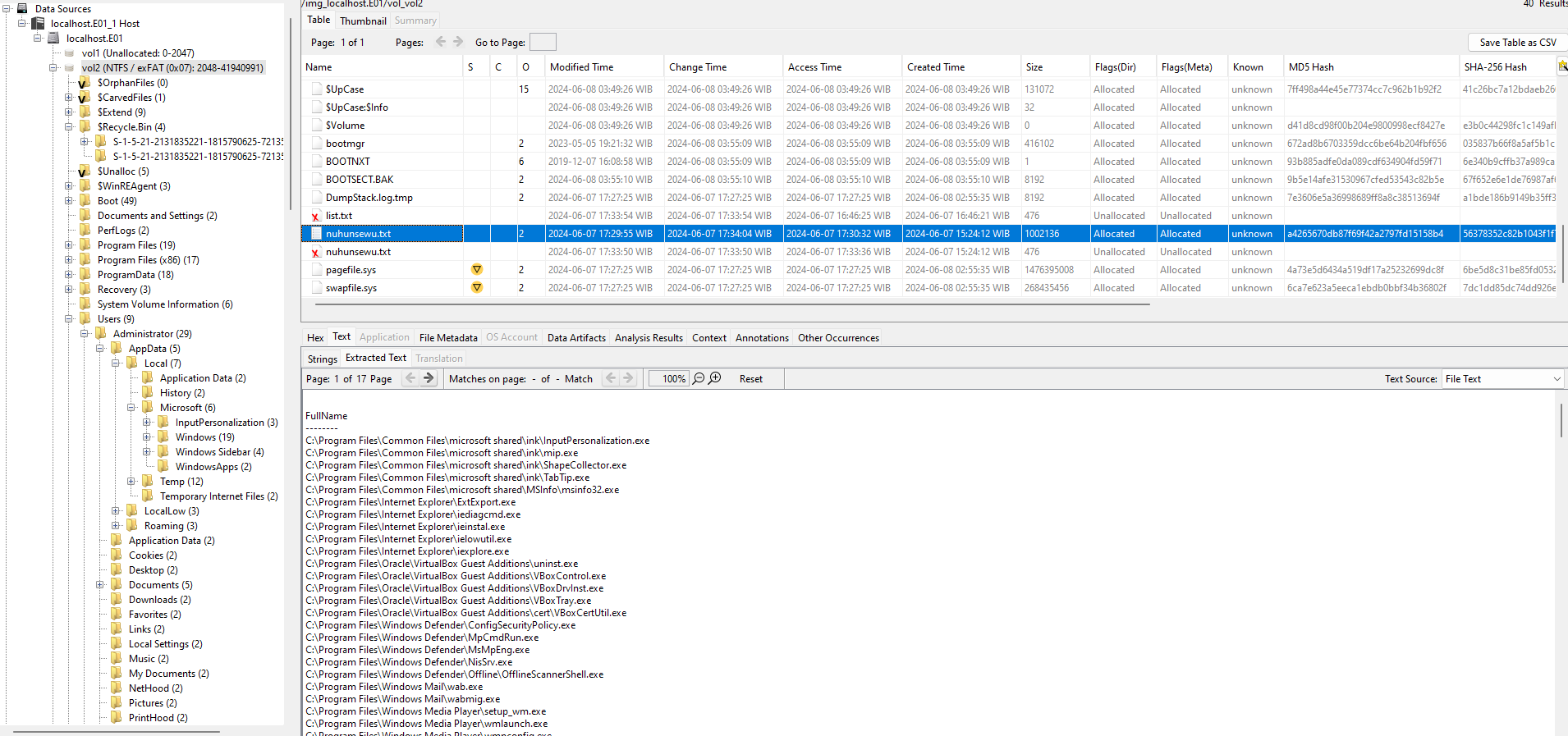


Gambar 3.22. Detail File nuhunsewu.Ink

* Ahli langsung menelusuri lokasi tempat file tersebut disimpan yaitu:  
  vol\_vol2/Users/windows10/AppData/Roaming/Microsoft/Windows/Recent/

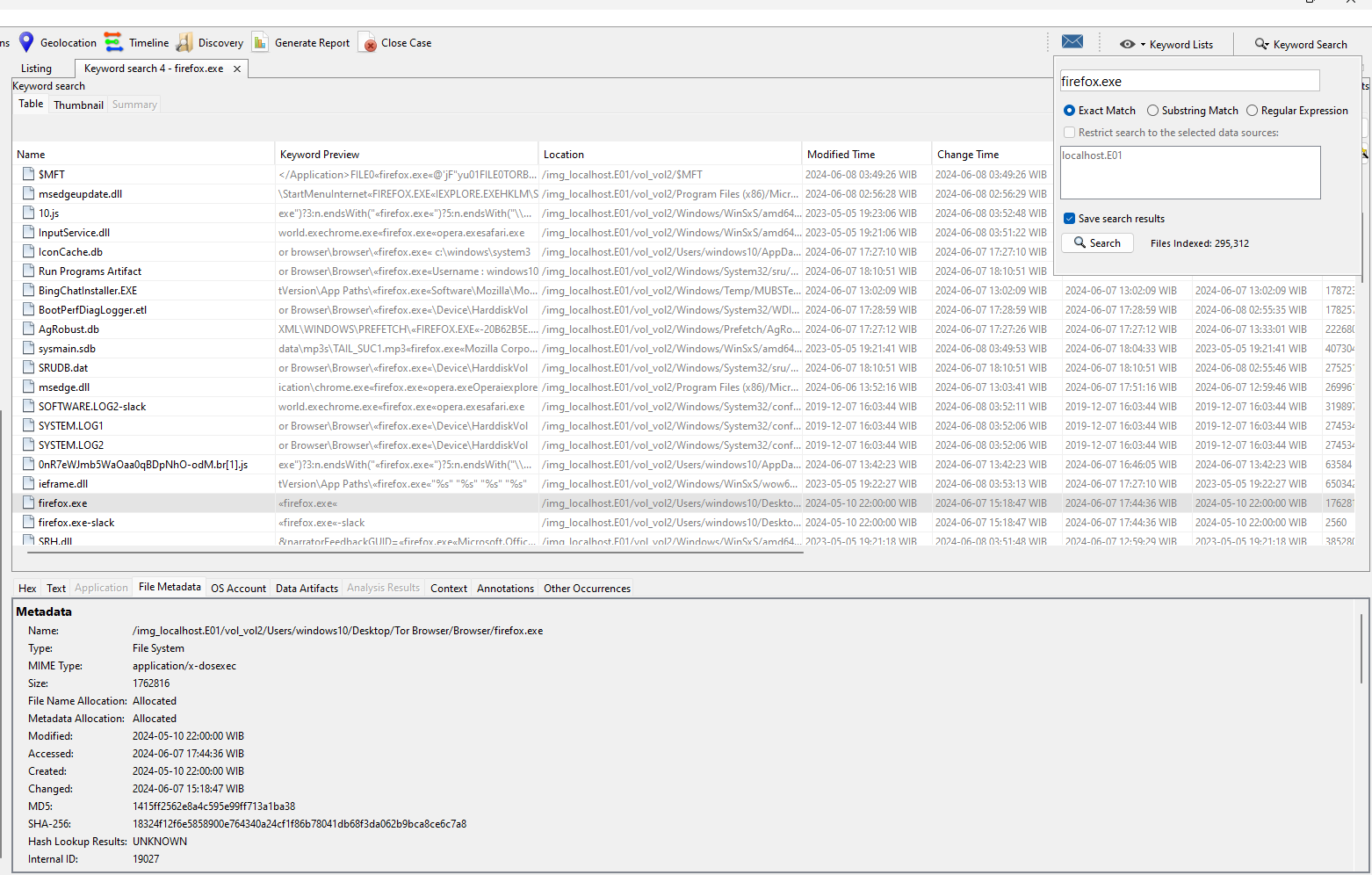
Gambar 3.23. Penelusuran File nuhunsewu.Ink

* Pada detail file, dapat terlihat jika file tersebut utama C:\

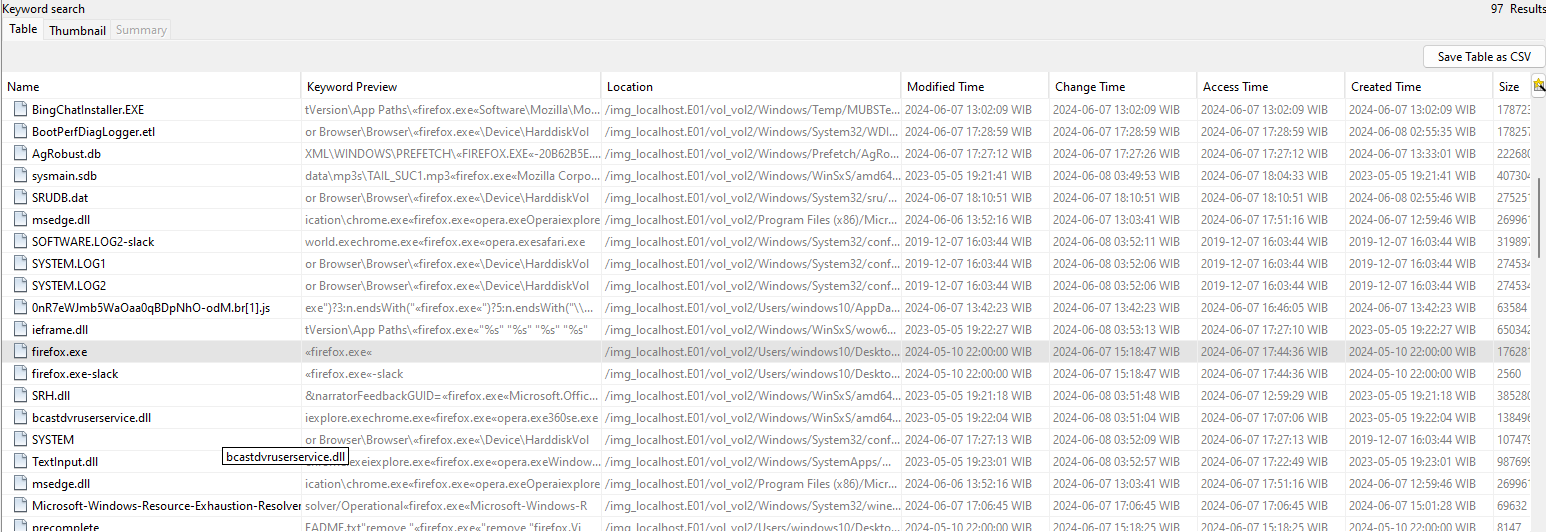


Gambar 3.24. Isi File nuhunsewu.Ink

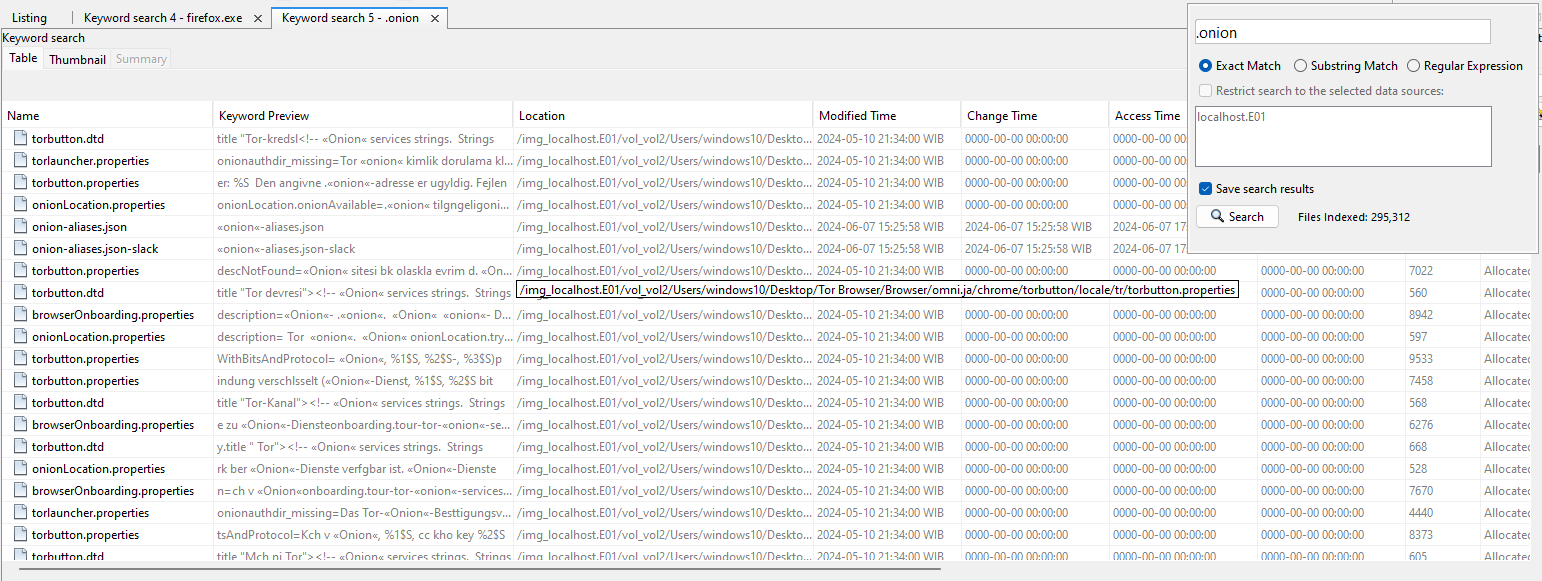
* Dapat terlihat bahwa isi file nuhunsewu merupakan daftar perangkat lunak yang terpasang di perangkat.
* Selanjutnya, temukan aplikasi Tor browser di dalam harddisk. Ahli menggunakan kata kunci "firefox.exe" pada menu Keyword Search untuk mencari lebih dalam pada image logis.

3.25. mencari firefox.exe

* Jelajahi lokasi file firefox.exe yang sebenarnya dengan menggunakan menu tekan kanan " View Source File in Directory." Temukan tautan artefak pada direktori dengan lokasi: /img\_localhost.E01/Users/me/Desktop/Tor Browser/Browser/

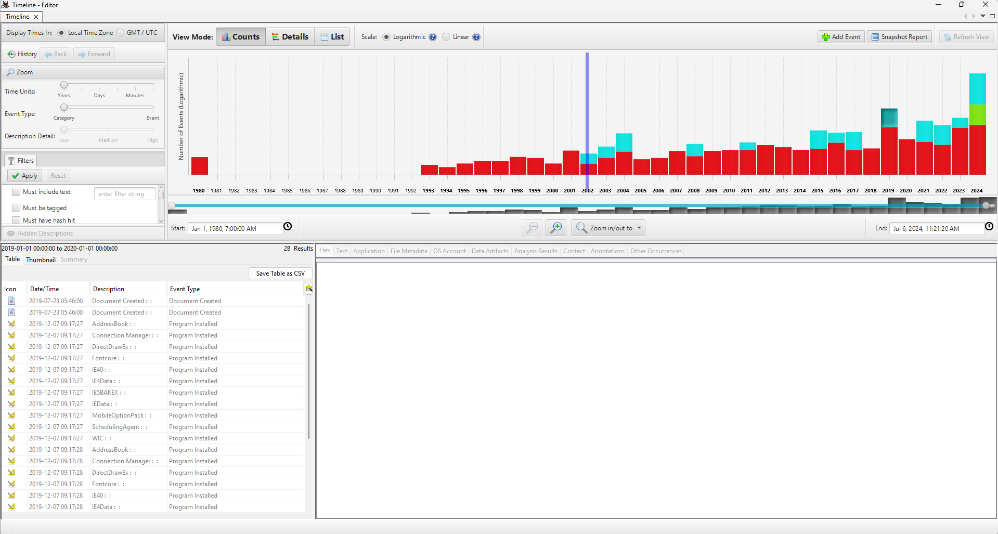
Gambar 3.26. Tampilan lokasi

* Berdasarkan karakteristik Tor, ahli perlu mengekstrak informasi tentang URL yang diakses dari peramban TOR. Alamat situs web menggunakan .onion. Ahli menggunakan menu " keyword search " untuk menemukan artefak

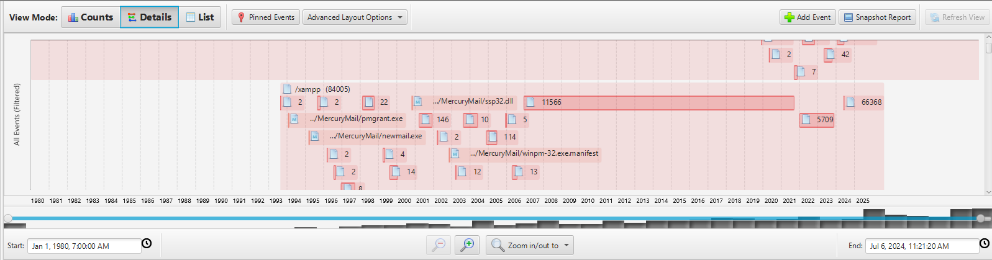
Gambar 3.27. Hasil ekstraksi

**3.4.1. Timeline**

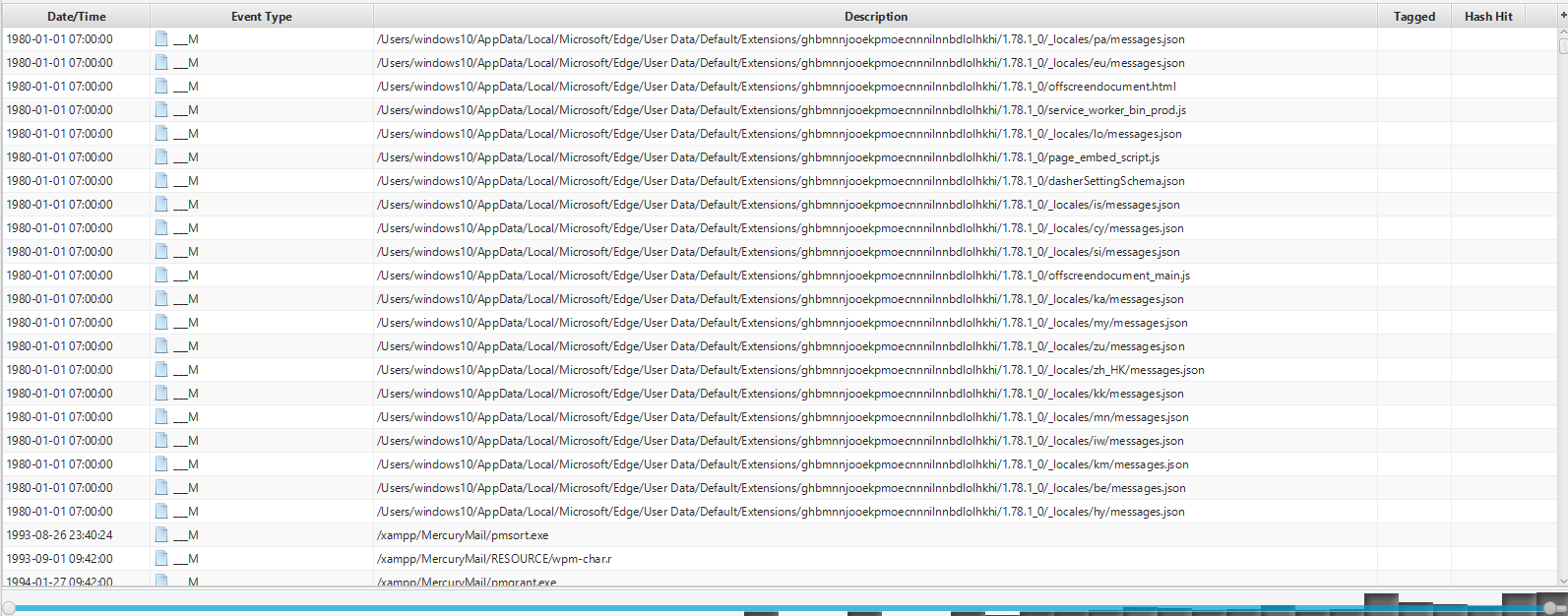
* Autopsy menyediakan fitur bawaan berupa timeline, dimana fitur ini pengguna dapat melihat timeline image yang sedang di analisis. Ahli dapat melihat data, dengan tiga jenis mode untuk dilihat, yaitu, Hitungan, Detail, dan Daftar.
  + Counts mode

Gambar 3.28. Mode Counts pada Timeline

* + Details mode

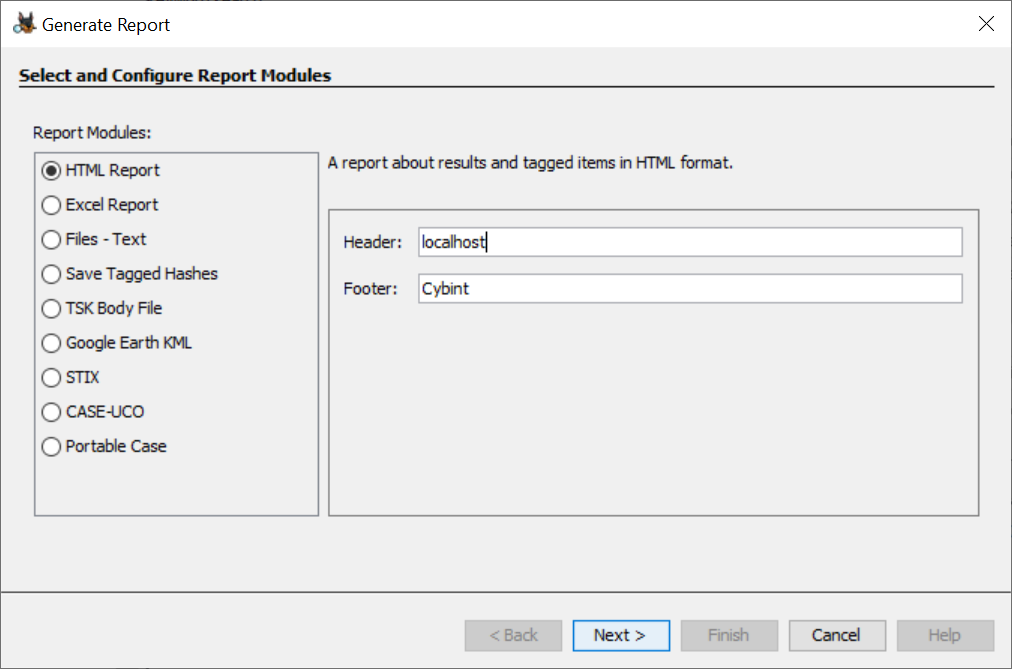
Gambar 3.29. Mode Details pada Timeline

* + List mode

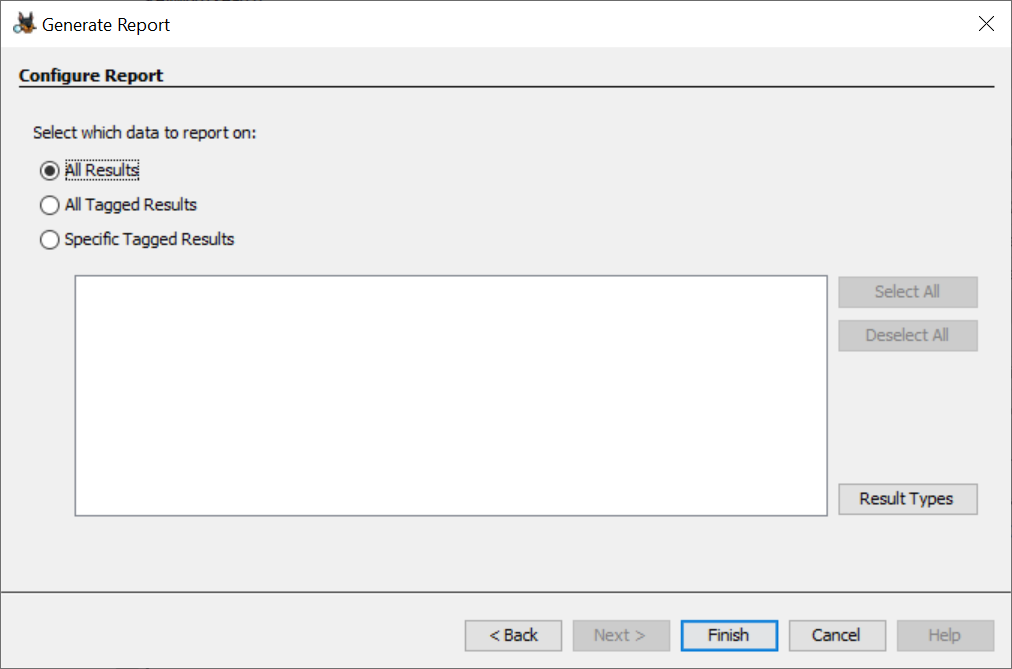
Gambar 3.30. Mode list pada Timeline

**3.4.2. Laporan**

* Membuat laporan sebagai ringkasan dari aktivitas analisis logical image yang telah dilakukan dengan menggunakan Autopsy. Ahli dapat langsung menekan menu "Generate Report", lalu mengonfigurasi menu Pilih dan konfigurasikan basis data laporan(Pada kasus ini ahli memilih laporan dengan format HTML). Langkah selanjutnya adalah melakukan konfigurasi pada laporan yang mungkin tentang hasil dan item yang ditandai dalam format HTML. Isi informasi yang sesuai pada Header dan Footer.

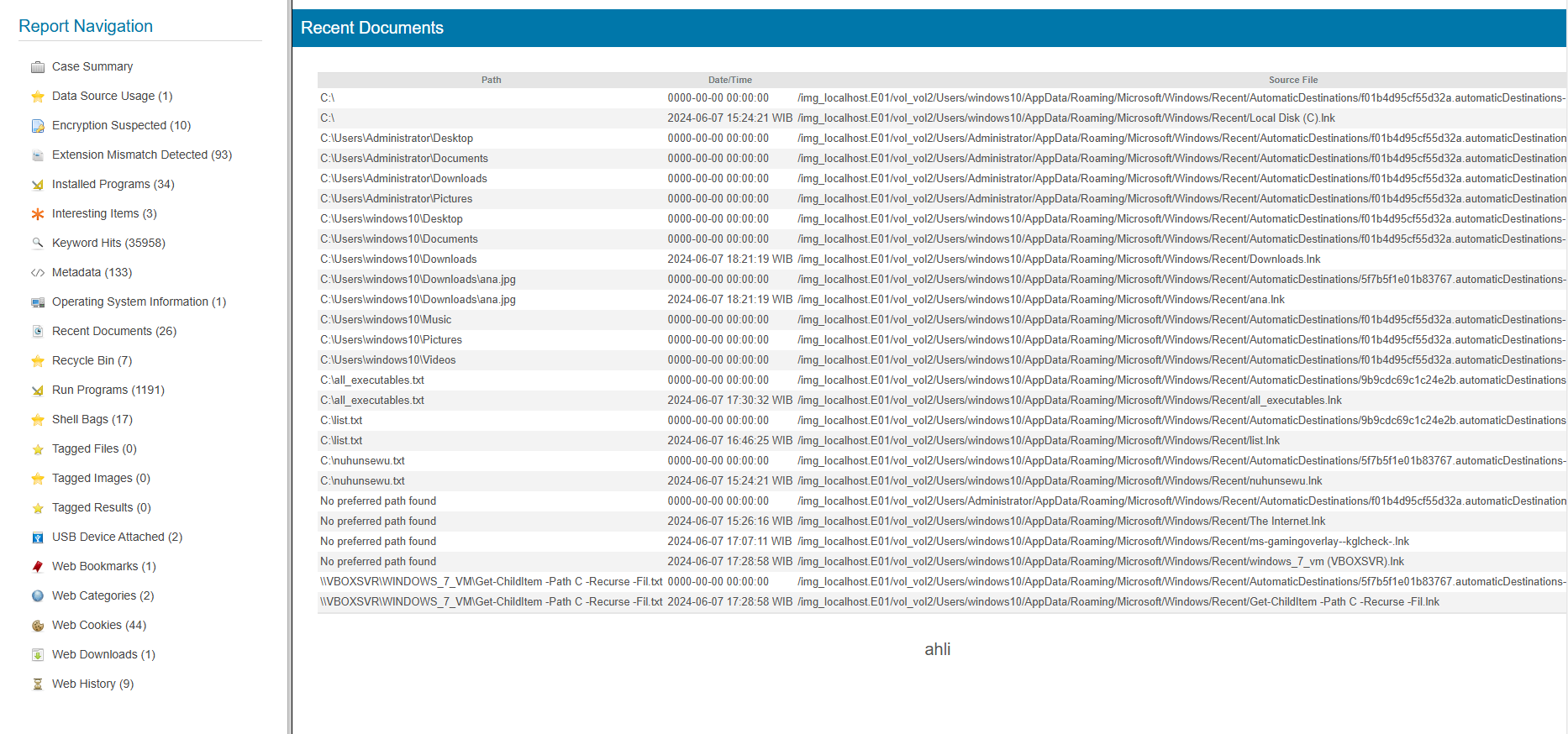
  
Gambar 3.31. Tampilan Generate Report

* Konfigurasikan format laporan dengan memilih data mana yang akan dilaporkan. ahli memilih "Semua Hasil”.



Gambar 3.32. Pilihan report

* Hasil akhir akan disimpan dalam direktori Reports di dalam default case. pengguna perlu menunggu beberapa menit hingga prosesnya selesai. Browser akan terbuka secara otomatis ketika pembuat laporan selesai. ahli dapat menelusuri semua informasi tentang bukti logical image. Namun, format laporan yang dipilih tergantung pada kebutuhan gaya laporan.

Gambar 3.33. Hasil dari Report