REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SURAT PENCATATAN
CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202230276, 18 Mei 2022
Pencipta		
Nama	:	**Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU. dan Faradias Izza Azzahra Faisal**
Alamat	:	BTN Tabaria Tower E10/23 Kelurahan Mannuruki, Kecamatan Tamalate, Makassar, SULAWESI SELATAN, 90221
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU. dan Faradias Izza Azzahra Faisal**
Alamat	:	BTN Tabaria Tower E10/23 Kelurahan Mannuruki, Kecamatan Tamalate, Makassar, SULAWESI SELATAN, 90221
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Program Komputer**
Judul Ciptaan	:	**Analisis Mobile Forensic Android Menggunakan Autopsy**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	10 Mei 2022, di Makassar
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000345849

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n Menteri Hukum dan Hak Asasi Manusia
Direktur Jenderal Kekayaan Intelektual
u.b.
Direktur Hak Cipta dan Desain Industri

Anggoro Dasananto
NIP.196412081991031002

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.

PROGRAM KOMPUTER

ANALISIS *MOBILE FORENSIC* ANDROID MENGGUNAKAN *AUTOPSY*

Pengusul

Drs. Ir. Faisal Syafar, M.Si., M.InfTech., Ph.D., IPU
Faradias Izza Azzahra Faisal

Mei 2022

ANALISIS MOBILE FORENSIC ANDROID BERBASIS AUTOPSY

Atopsy adalah tool berbasis GUI open-source yang dapat digunakan untuk memeriksa dan memulihkan bukti dari komputer serta ponsel. Tool ini dapat berjalan di Windows, Linux dan OS X. Ini dapat digunakan sebagai alat utama, ekstensi tool saat ini atau juga untuk memvalidasi hasil dari tool lain. Auopsy menganalisis gambar disk, drive atau folder lokal dan sering digunakan dengan The Sleuth Kit (Brian Carrier, 2020) untuk menganalisis data pada sistem yang dicurigai. Tool ini banyak digunakan oleh berbagai lembaga seperti Akademik & Penelitian, Investigasi Perusahaan, Militer & Pemerintah, dan Penegakan Hukum.

Saat ini, telah tersedia banyak forensik mobile komersial.untuk tujuan seperti analisss Forensik Oksigen dan Detektif, Cellebrite UFED, MSAB XRY dan lain-lain. Aplikasi ini sangat robust dan mampu mengekstrak dataset besar dari berbagai perangkat seluler termasuk Android. Autopsy adalah sebuah antarmuka grafis untuk tool-tool didalam sleuth kit, yang memudahkan pengguna dalam melakukan investigasi. Mereka dapat menganalisis disk dan file system windows dan unix (NTFS, FAT, UFS1/2, EXT2/3). Autopsy menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci, dan operasi lainnya. Autopsy menggunakan perl untuk menjalankan program-program sleuth kit dan mengubah hasilnya ke HTML, oleh karena itu pengguna autopsy membutuhkan web client untuk mengakses fungsi-fungsinya.

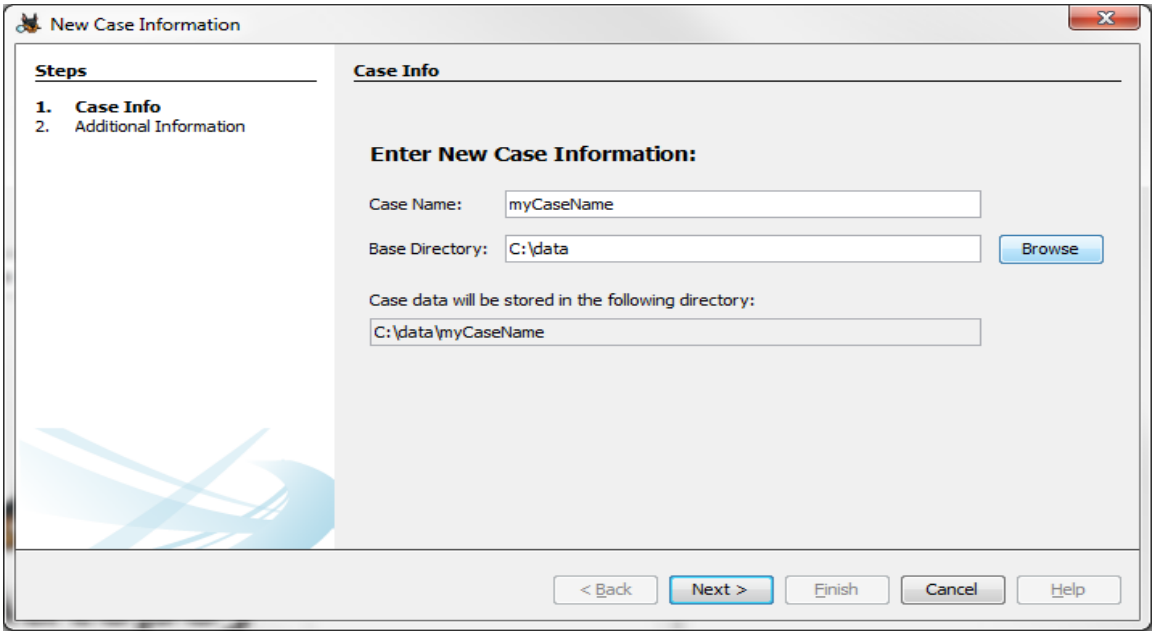
Autopsy adalah platform forensik digital dan antarmuka grafis untuk the sleuthkit dan alat-alat forensik digital lainnya. Hal ini digunakan oleh penegak hukum, militer, dan pemeriksa perusahaan untuk menyelidiki apa yang terjadi pada komputer.

Versi terbaru adalah 4.19.3 for Windows Sangat penting untuk dicatat bahwa ia memiliki Modul Analyzer Android, yang memungkinkan untuk mengekstrak artefak berikut: Pesan teks (SMS / MMS); Log panggilan Kontak Pesan Tango Kata-kata dengan Teman pesan GPS dari browser dan GOOGLE Maps GPS dari cache.wifi dan cache.cell file Tapi ini bukan satu-satunya modul yang cocok untuk forensik Android. Ada juga modul penting seperti Exif Parser Module, Keyword Search Module, PhotoRec Carver Module dan beberapa lainnya. Mari kita buat kasus dan tambahkan gambar fisik Android. Mulai suite dan Anda akan melihat jendela Selamat Datang:

Menganalisis data menggunakan Autopsi pada Telpon Android, menggunakan alur kerja berikut:

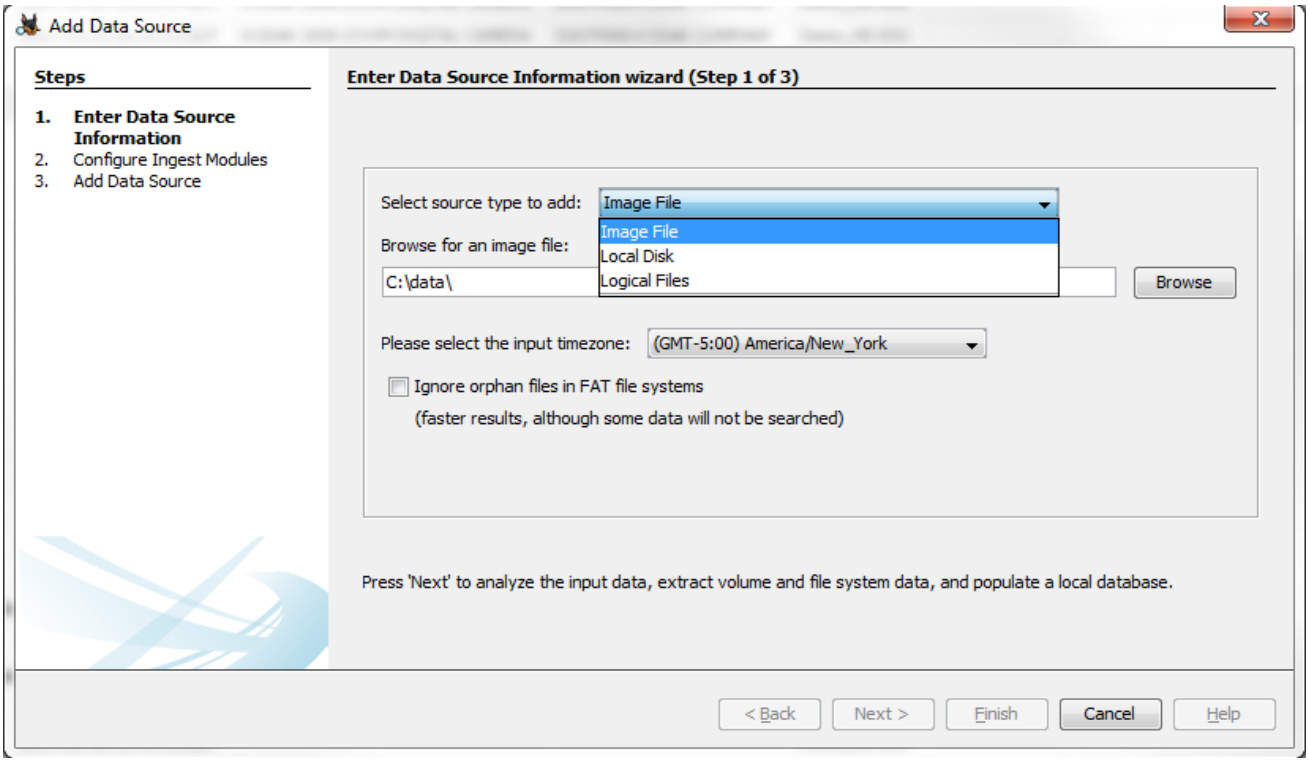
Step 1: **Make a Case**

Kasus adalah "wadah untuk satu atau lebih sumber data. Kasus harus dibuat sebelum data dianalisis."



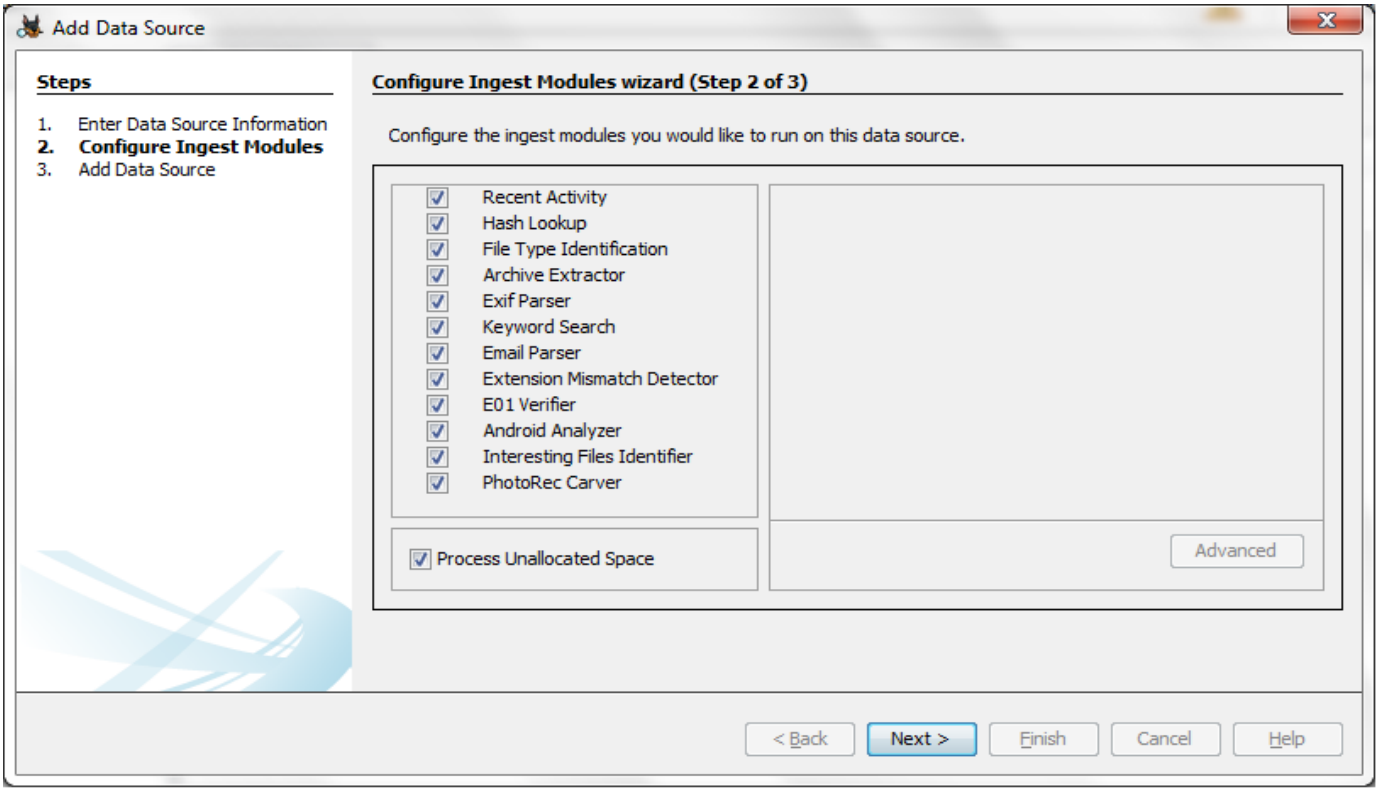
Step 2: Add a Data Source

Satu atau lebih sumber data ditambahkan ke kasing. Sumber data termasuk gambar disk dan file lokal.

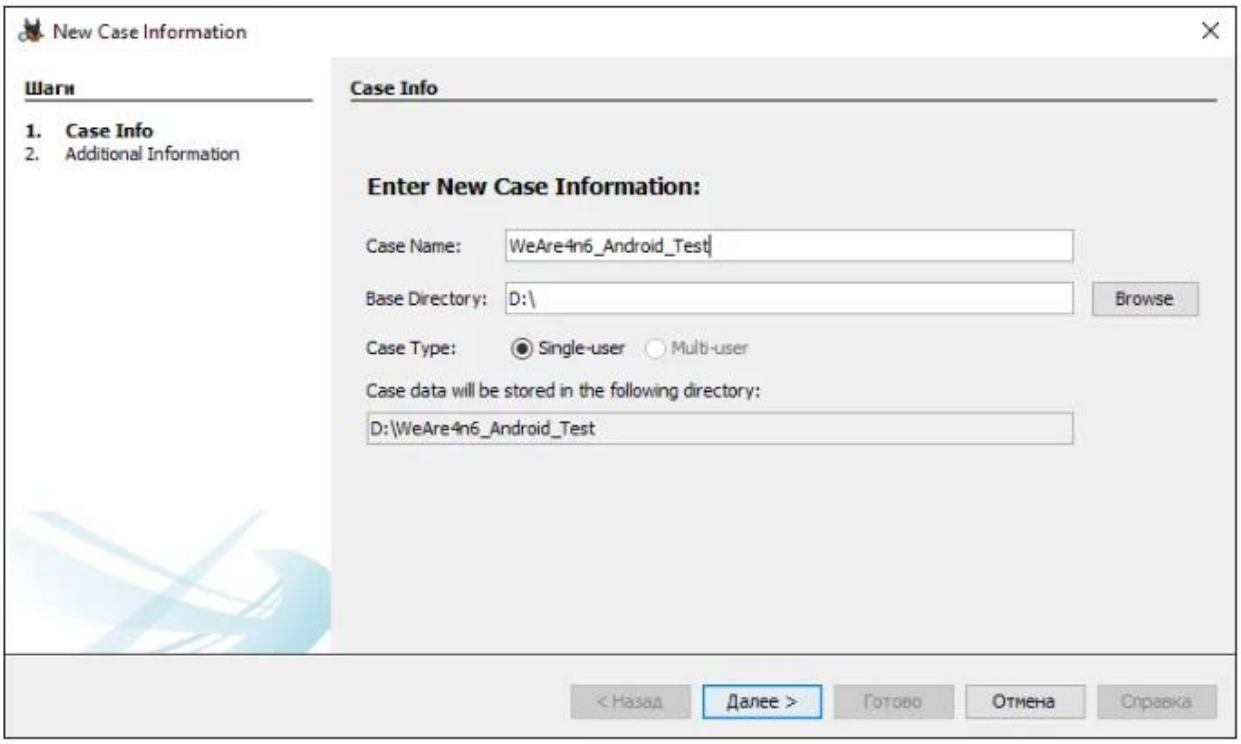


Step 3: Configure Ingest Modules

Setelah sumber data disertakan, modul bekerja untuk memecah informasi. Hasilnya disajikan pada antarmuka terus menerus dan memberikan peringatan penting bila diinginkan oleh user. Modul model ingests menggabungkan jumlah hash dan kueri, pencarian kata kunci, dan ekstraksi relik web. Modul pihak ketiga dapat dibuat dan ditambahkan ke alur.

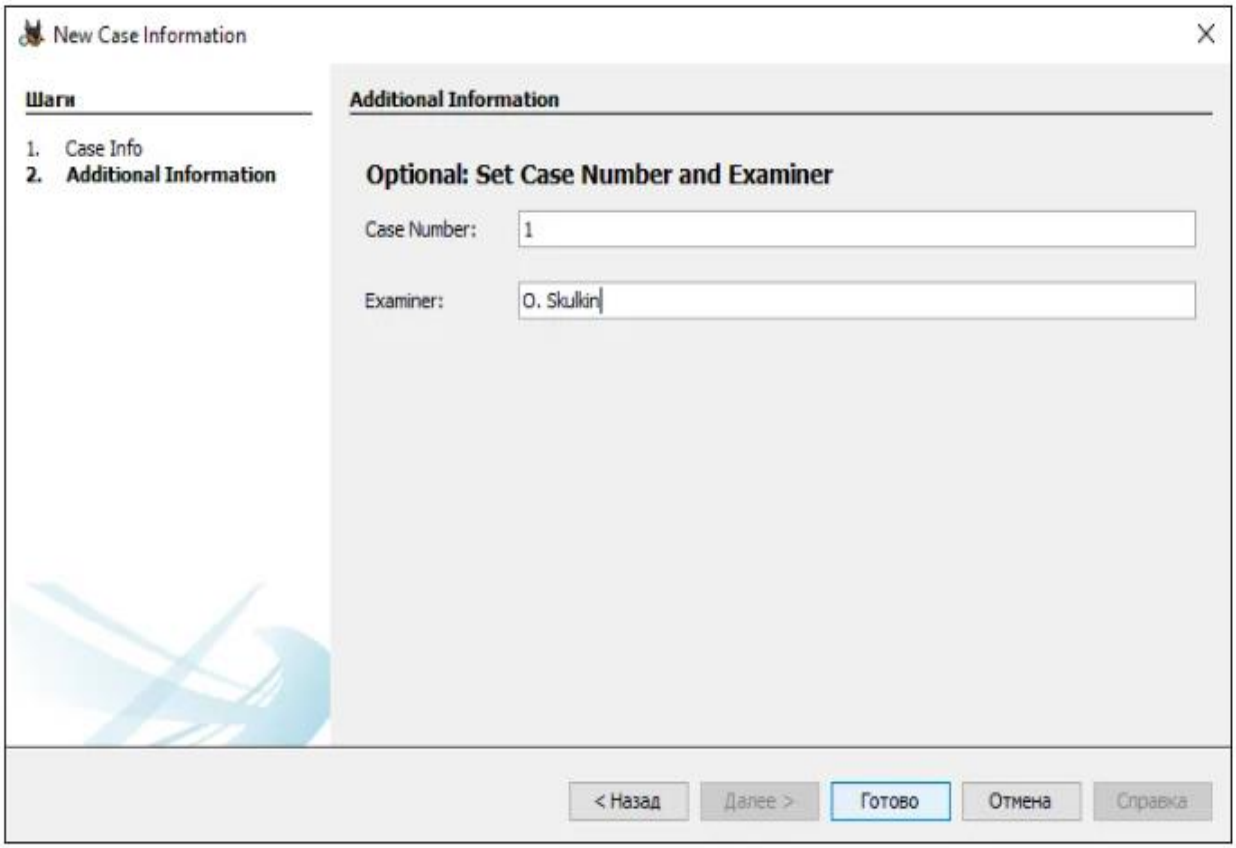


Selanjutnya perlu membuat kasus baru, dengan cara memilih opsi yang sesuai.

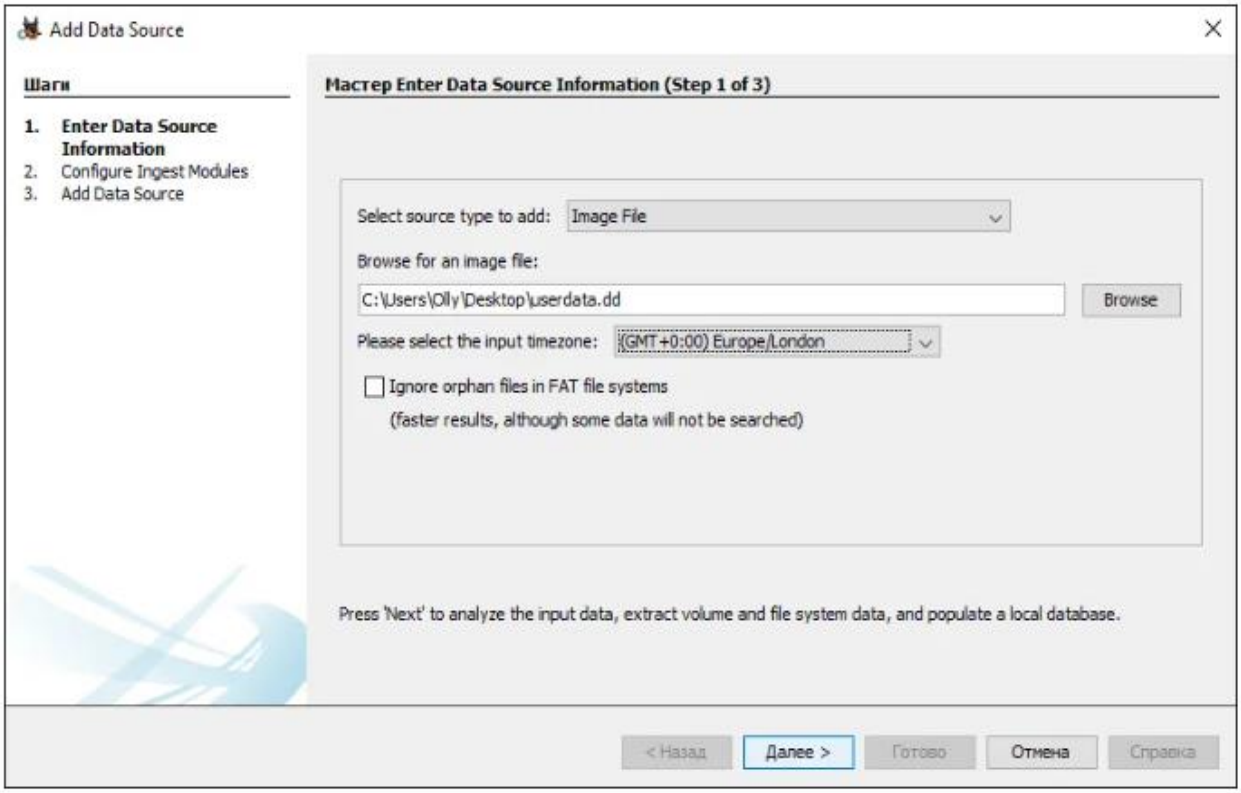


Mulai dengan pemberian nama kasus, pilih WeAre4n6_Android_Test – our base directory is D:\, (atau terserah memilih folder), jadi data akan disimpan di drive D:\ WeAre4n6_Android_Test.

Mengatur nomor kasus dan nama pemeriksa hanya opsional, sehingga Anda dapat melewati langkah ini:

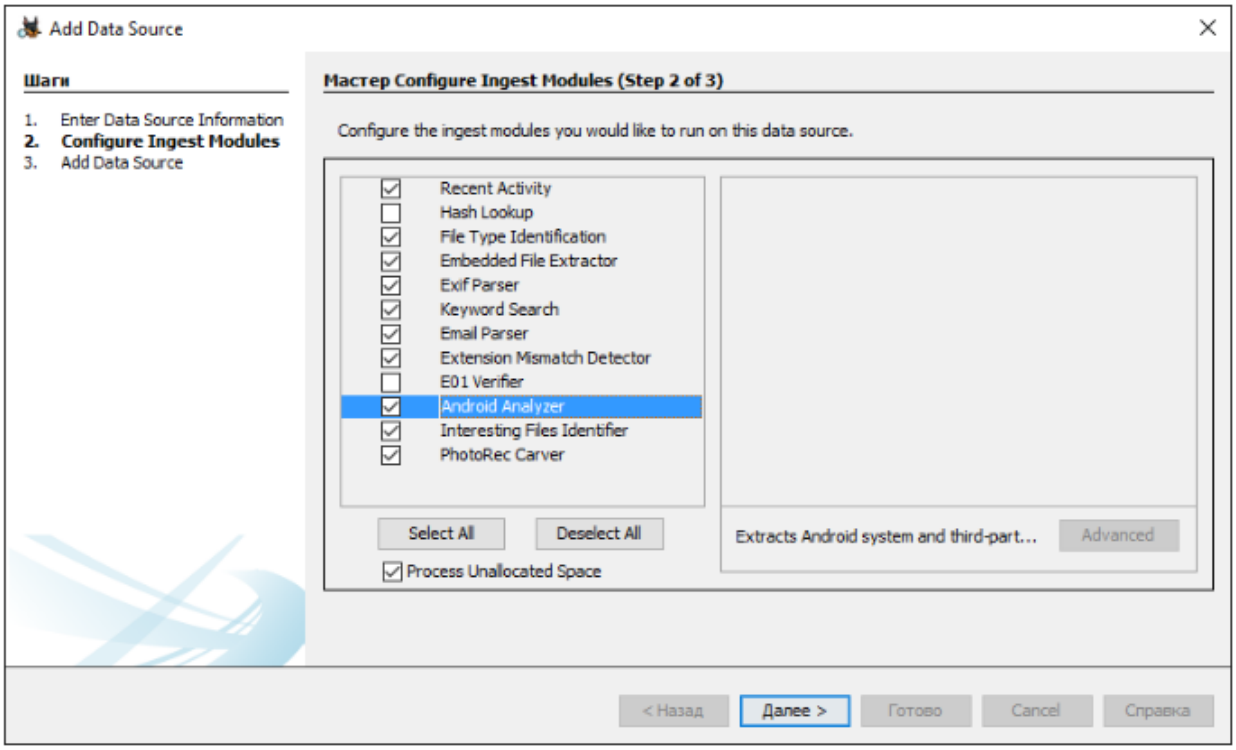


Pilih sumber data:



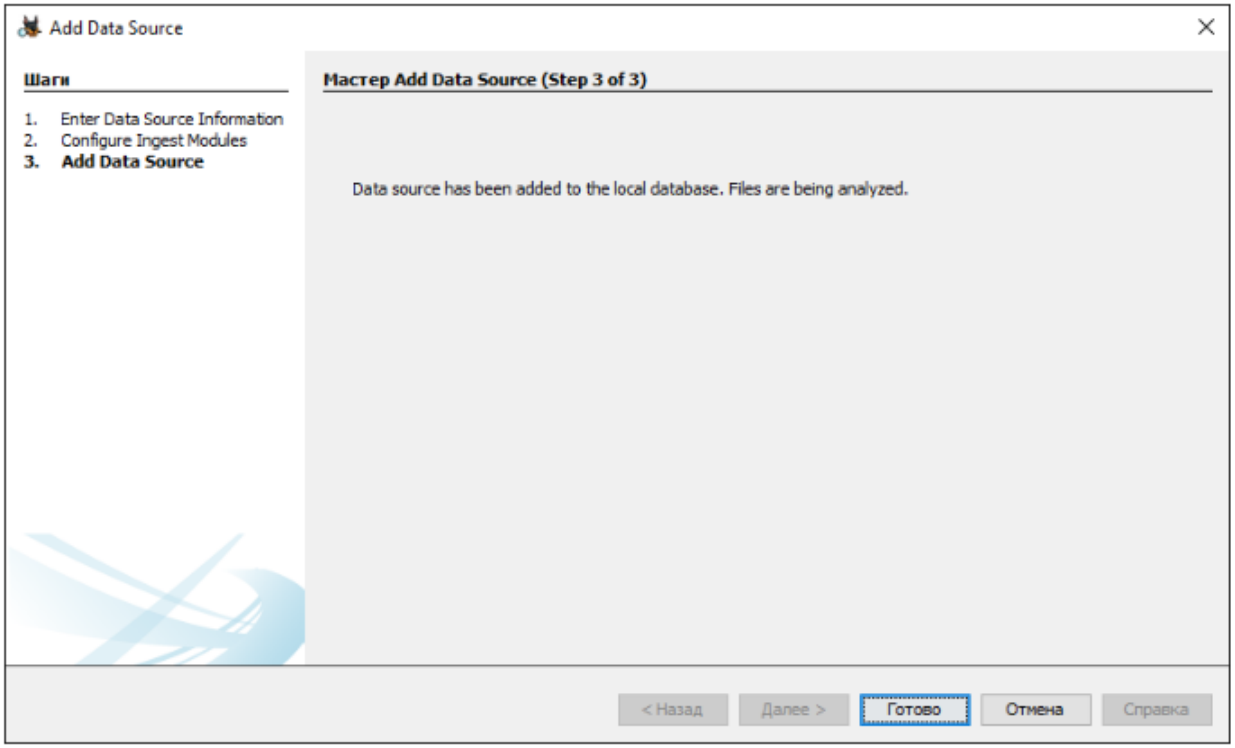
Pada kasus (contoh) ini, (userdata.dd), berada di drive C:\Users\Olly\Desktop. Jangan lupa mengatur time zone yang sesuai.

Sekarang pilih modul ingest yang ingin dijalankan seperti terlihat pada gambar:

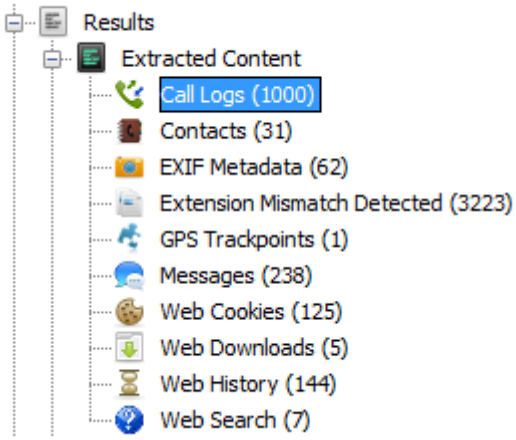


Jangan lupa untuk memilih Android Analyzer! Exif Parser, Keyword Search dan PhotoRec Carver. Selain itu, pastikan Anda memeriksa opsi Process Unallocated Space – itu akan dieksekusi secara otomatis dengan PhotoRec.

Selanjutnya, gambar sedang dianalisis oleh Autopsy Ingest Modules:



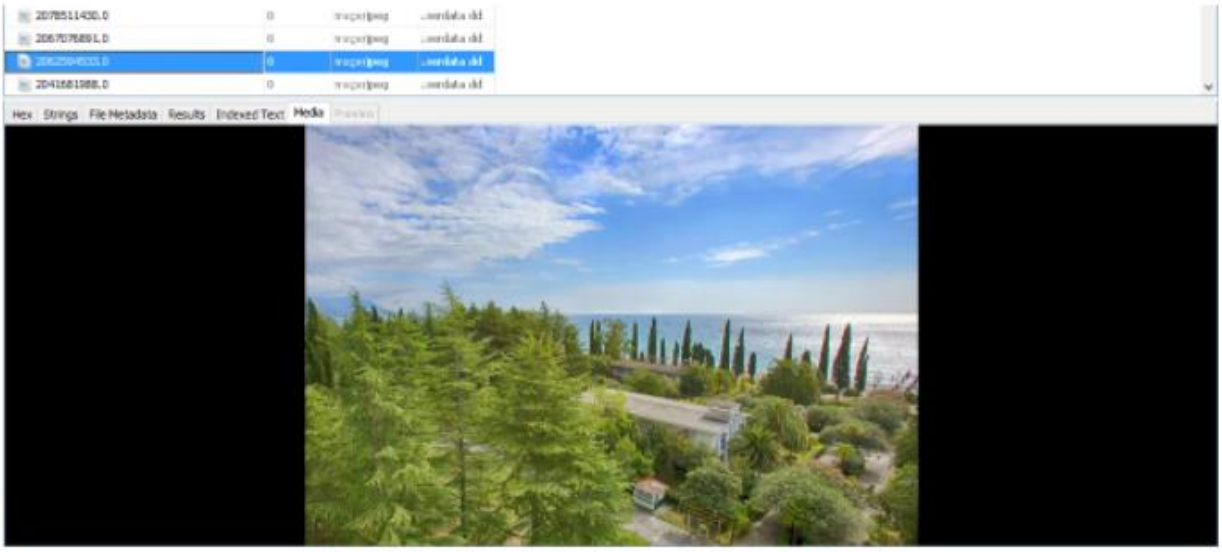
Berikut adalah hasil yang didapatkan dari modul Android Analyzer:



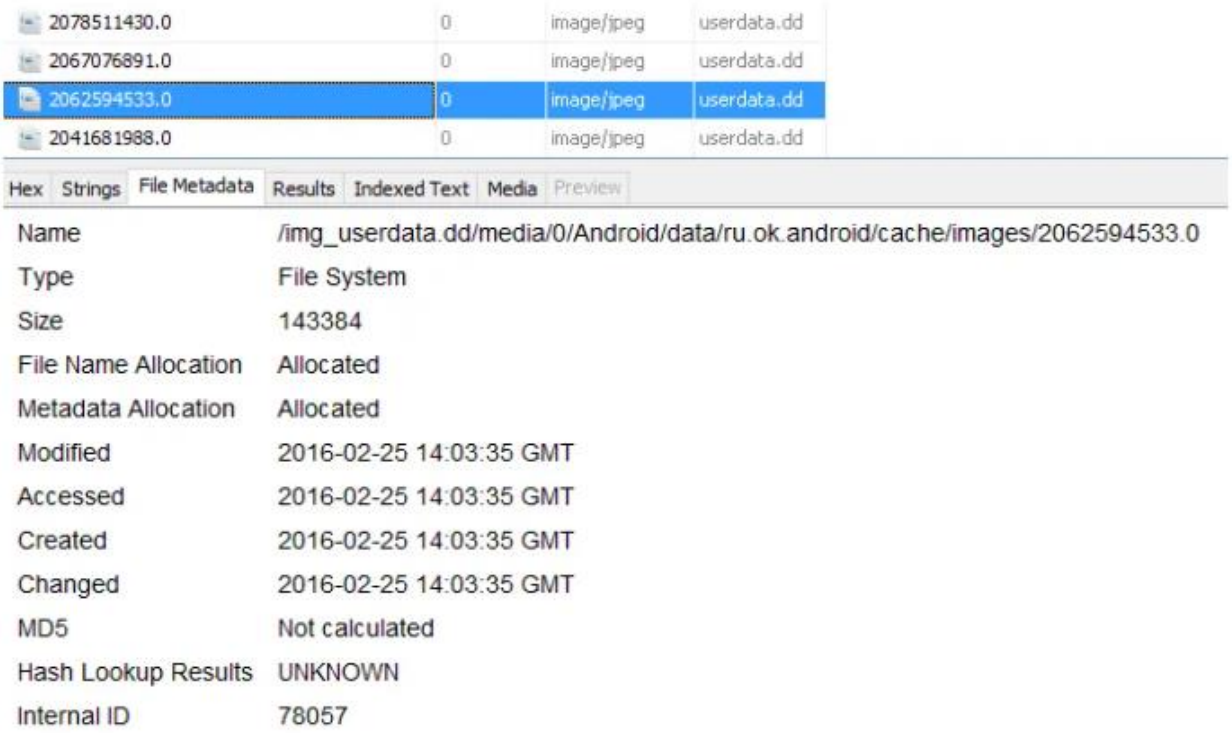
Seperti yang Anda lihat, cukup banyak data yang diekstraksi secara otomatis. Log panggilan, kontak, trackpoint GPS, dan pesan diekstraksi dengan modul Android Analyzer, metadata EXIF diekstraksi oleh modul Parser EXIF, file dengan ekstensi yang salah terdeteksi oleh modul

Extension Mismatch Detector, dan cookie web, unduhan web, riwayat web/pencarian web diekstraksi oleh modul Aktivitas Terbaru.

Modul Extension Mismatch Detector sangat berguna untuk forensik Android, misalnya, dapat digunakan untuk menemukan gambar yang di-cache, seperti terlihat pada gambar dibawah:

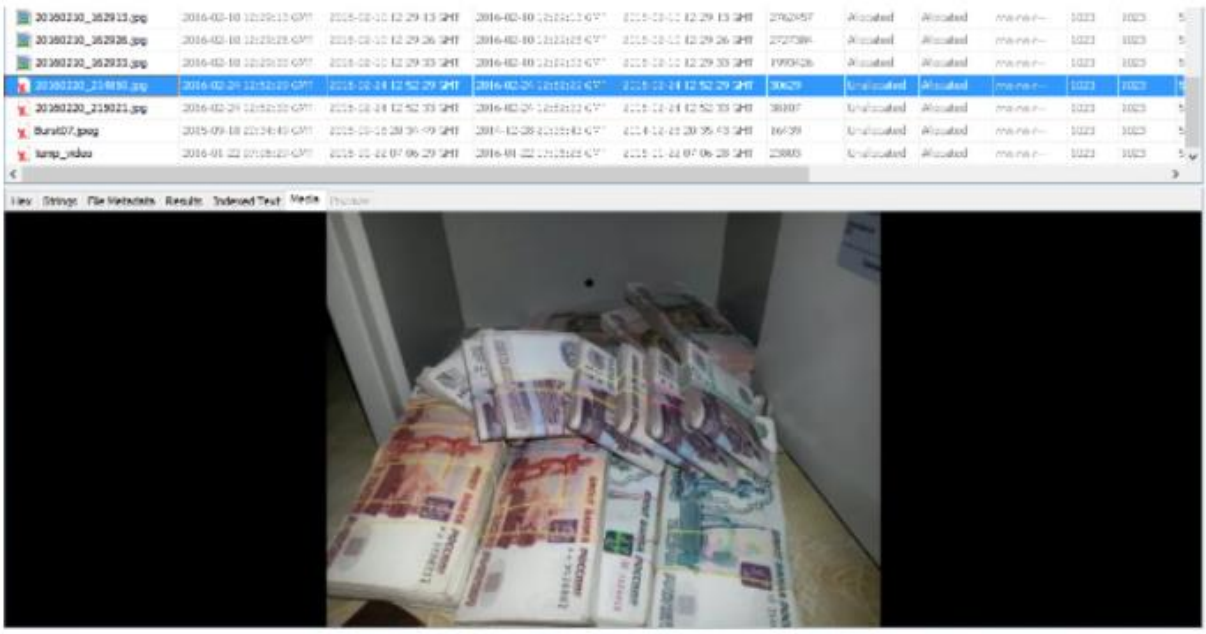


Seperti yang terlihat pada gambar cache ini memiliki ekstensi "0" bukan "jpg":

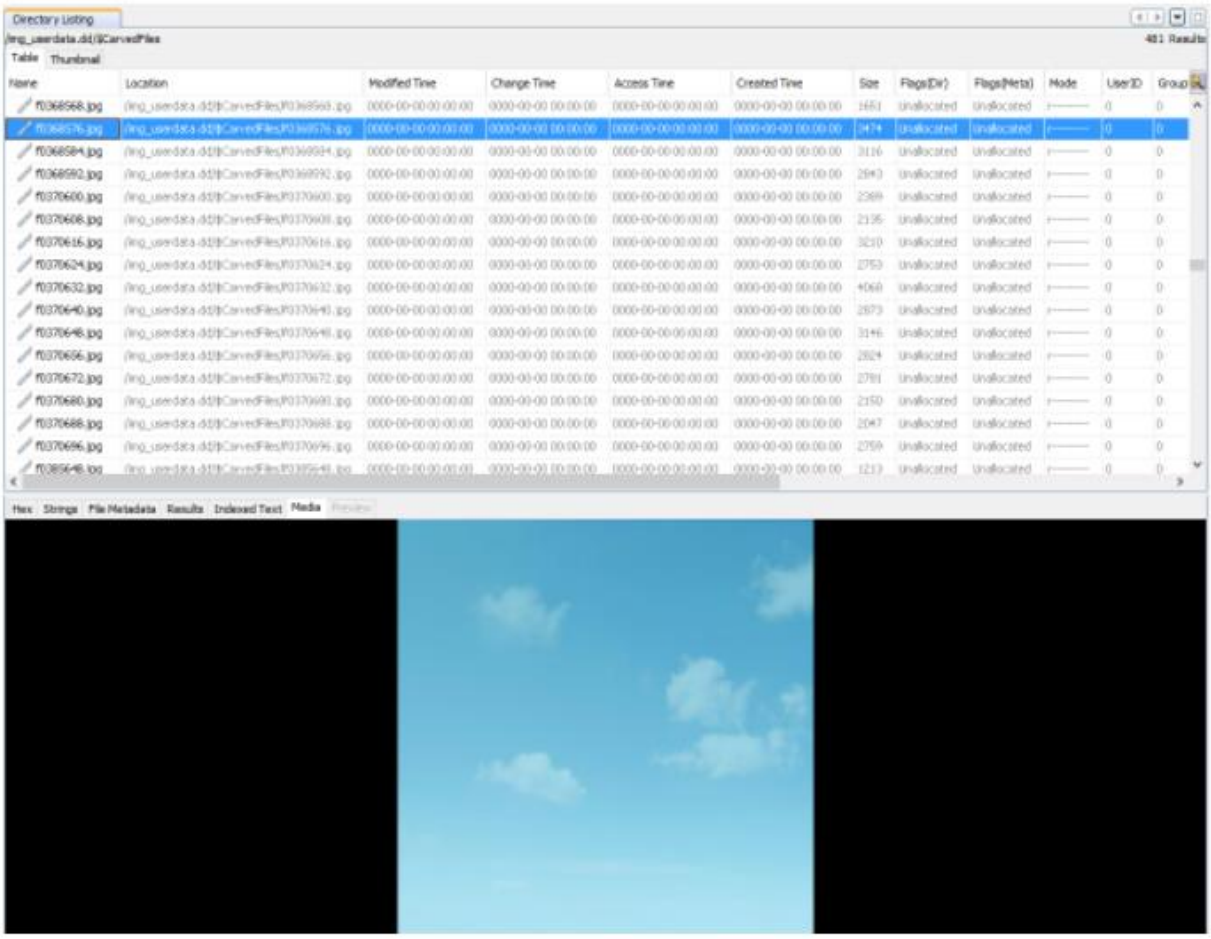


Hasil analisa lokasi menunjukkan bahwa gambar ini di-cache oleh Odnoklassniki - aplikasi media sosial Rusia.

Selain itu, Autopsy mendukung pemulihan file yang dihapus otomatis dari sistem file Ext4, seperti terlihat pada gambar di bawah:



Akhirnya, dapat disimpulkan bahwa modul PhotoRec Carver membantu pemeriksa forensik seluler untuk mengekstrak data dari ruang unallocated melalui teknik ukiran (curving):



Analisis ini telah menunjukkan bahwa Autopsy adalah alat open source yang cukup kuat untuk forensik Android dengan sejumlah modul yang mampu mengurai dan memulihkan data.