

Forensik Digital

SEMESTER GENAP T.A 2023/2024

LAB 2

Windows OS Forensic (Data Carving)



**Program Studi Informatika
Fakultas Teknologi Industri
Universitas Atma Jaya Yogyakarta**



REQUIREMENT

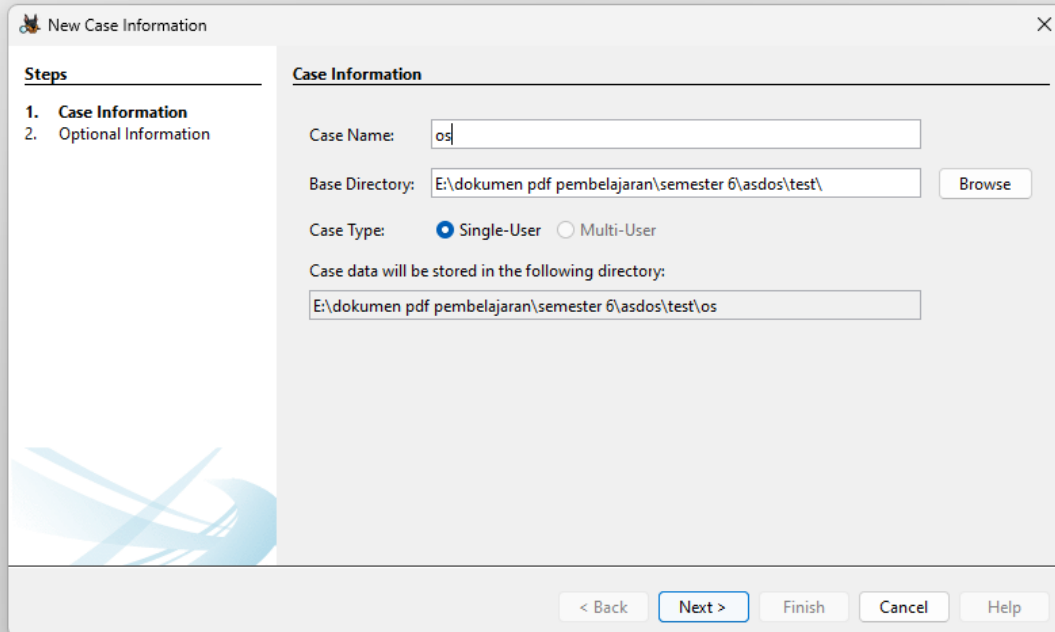
1. Autopsy (instalasi dapat dilihat di tutorial instalasi yang ada di situs kuliah)
2. Disk Image: [Disk Image](#)

PENJELASAN

Windows OS Forensic adalah cabang dari Forensik Digital yang mengacu pada proses pengumpulan, analisis dan interpretasi bukti digital yang berasal dari sistem operasi windows. Dalam praktiknya, Windows OS Forensic melibatkan pemahaman tentang bagaimana windows berinteraksi dengan perangkat keras, sistem file, registri dan aplikasi yang berjalan di dalamnya. Teknik dan alat yang digunakan dalam Windows OS Forensic mencakup berbagai macam, mulai dari alat bawaan Windows seperti Event Viewer dan PowerShell hingga perangkat lunak khusus forensik digital seperti EnCase, FTK (Forensic Toolkit), Autopsy, dan banyak lagi. Pada lab work kali ini, kita akan membahas tentang Data Carving, dimana Data carving adalah proses yang digunakan dalam bidang forensik digital untuk mendapatkan kembali atau merekonstruksi file yang hilang atau terhapus dari media penyimpanan, seperti hard disk, USB drive, atau kartu memori.

TUTORIAL

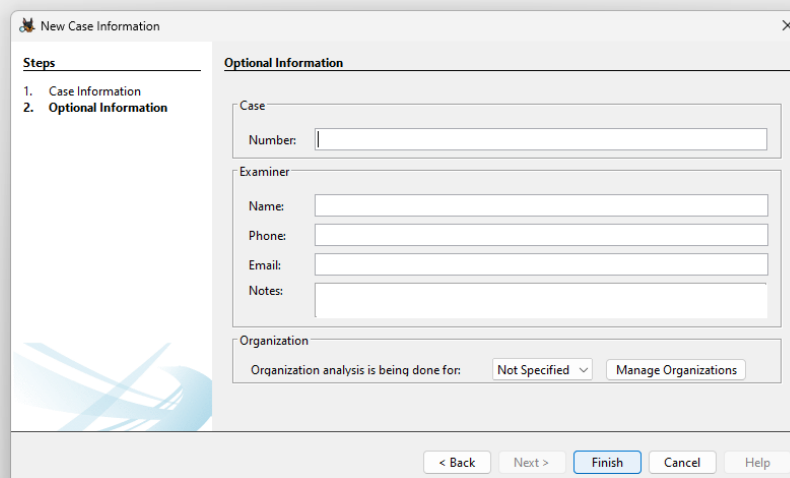
buka autopsy teman-teman dan buatlah sebuah case baru dengan penamaan bebas.



The screenshot shows the 'New Case Information' dialog box with the 'Case Information' tab selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Case Information' section contains the following fields:

- Case Name:** A text box containing 'os'.
- Base Directory:** A text box containing 'E:\dokumen pdf pembelajaran\semester 6\asdos\test\'. A 'Browse' button is to the right.
- Case Type:** Two radio buttons: 'Single-User' (selected) and 'Multi-User'.
- Case data will be stored in the following directory:** A text box containing 'E:\dokumen pdf pembelajaran\semester 6\asdos\test\os'.

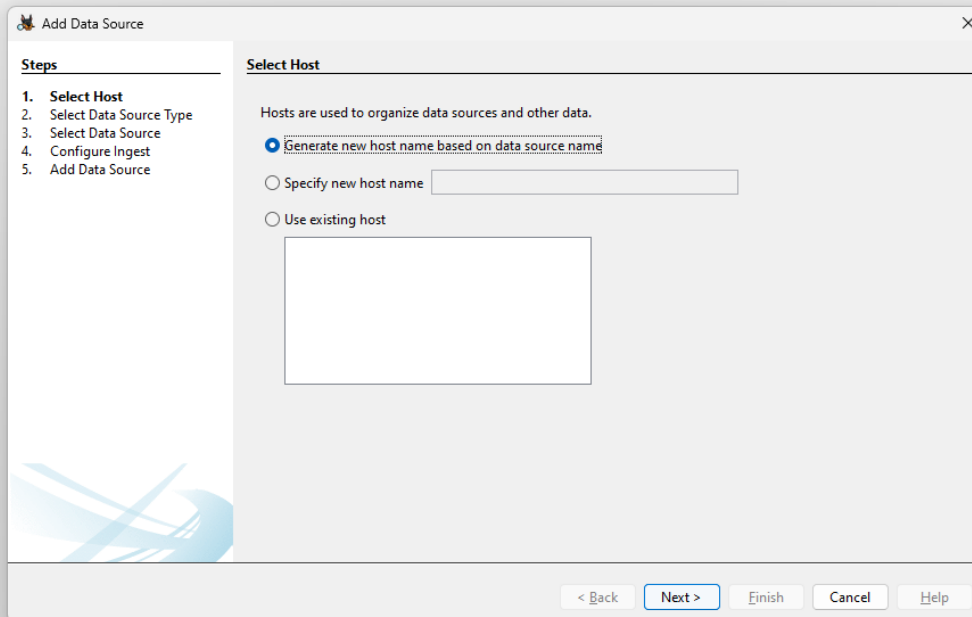
At the bottom, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted.



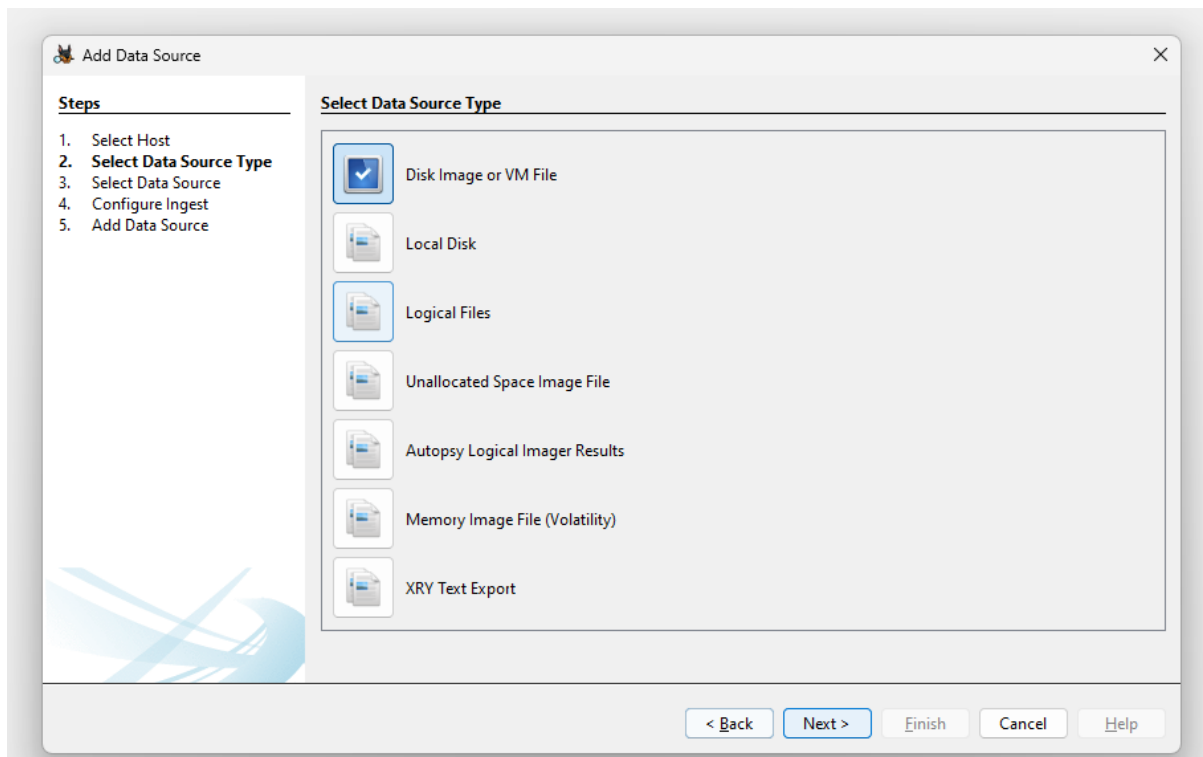
The screenshot shows the 'New Case Information' dialog box with the 'Optional Information' tab selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Optional Information' section contains the following fields:

- Case:** A text box containing 'Number:'.
- Examiner:** A section containing four text boxes: 'Name:', 'Phone:', 'Email:', and 'Notes:'.
- Organization:** A section containing a dropdown menu for 'Organization analysis is being done for:' (set to 'Not Specified') and a 'Manage Organizations' button.

At the bottom, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Finish' button is highlighted.



Setelah itu, pada bagian “Select Data Source Type” pilih Disk Image or VM

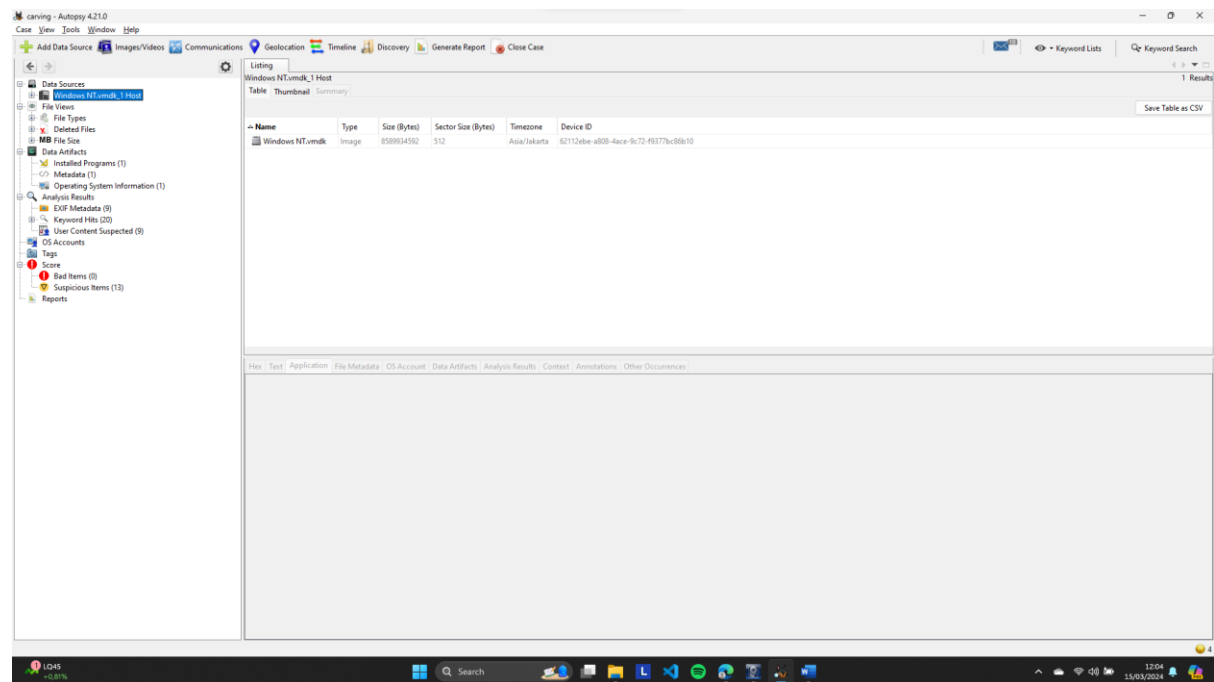


Klik next, lalu browse tempat dimana teman-teman menyimpan file disk image tadi yang sudah di extract. Lalu Configure Ingest, ceklis saja semua.

Setelah itu tinggal next dan finish dan tunggu hingga analyzing file (pojok kanan bawah) selesai.

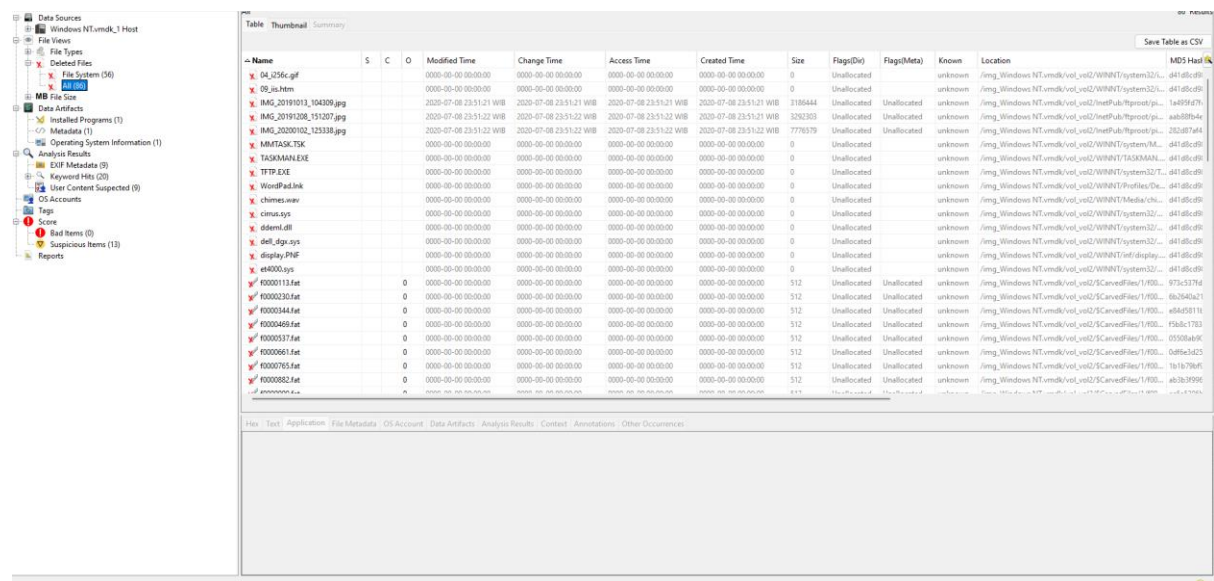


Berikut adalah tampilan awal dari autopsy jika teman-teman sudah melakukannya dengan benar.

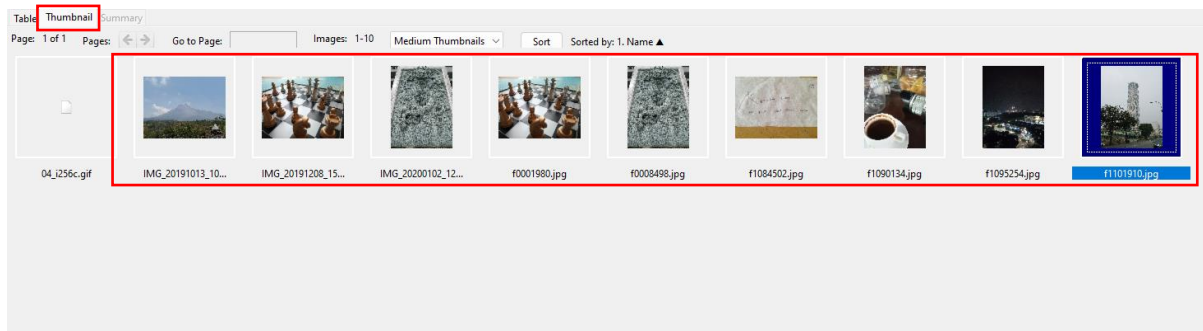


Buka deleted files dan teman-teman dapat melihat file-file yang sudah terhapus.

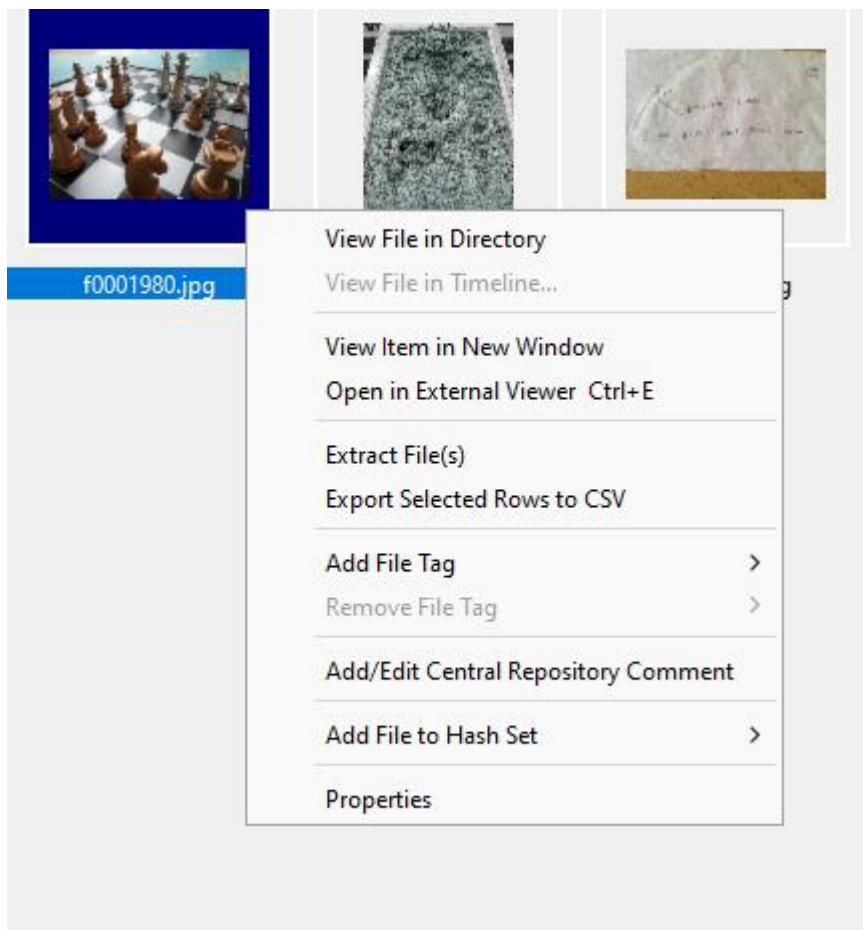
*tidak semua file yang terhapus dapat dipulihkan secara sempurna



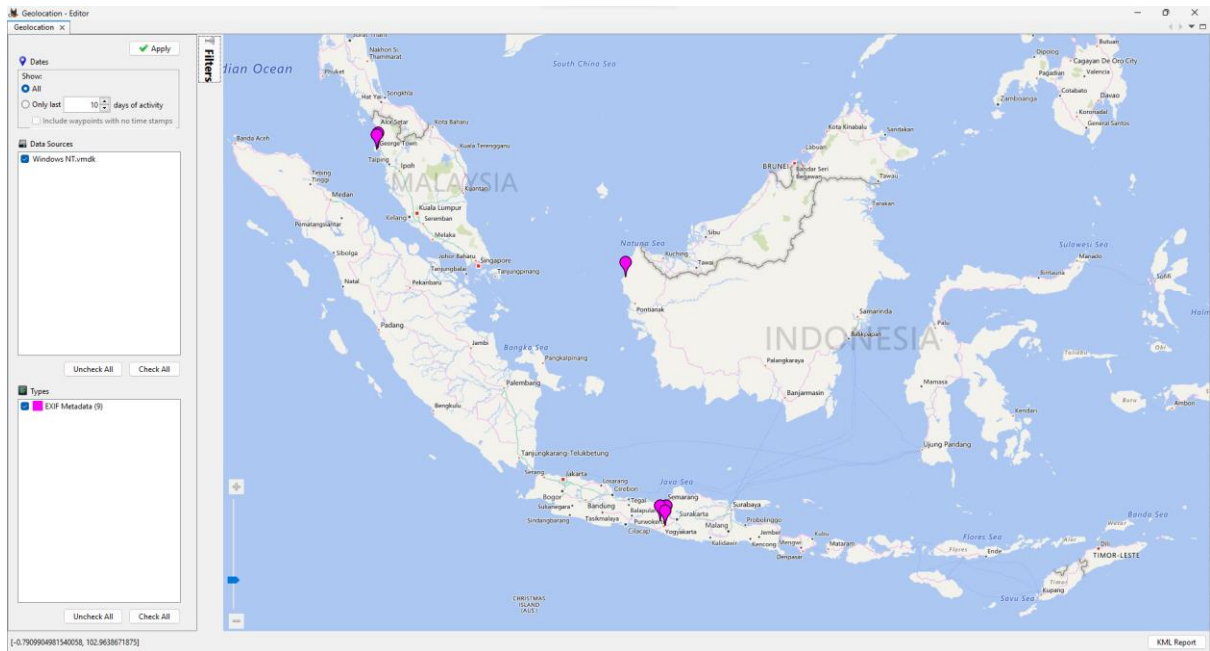
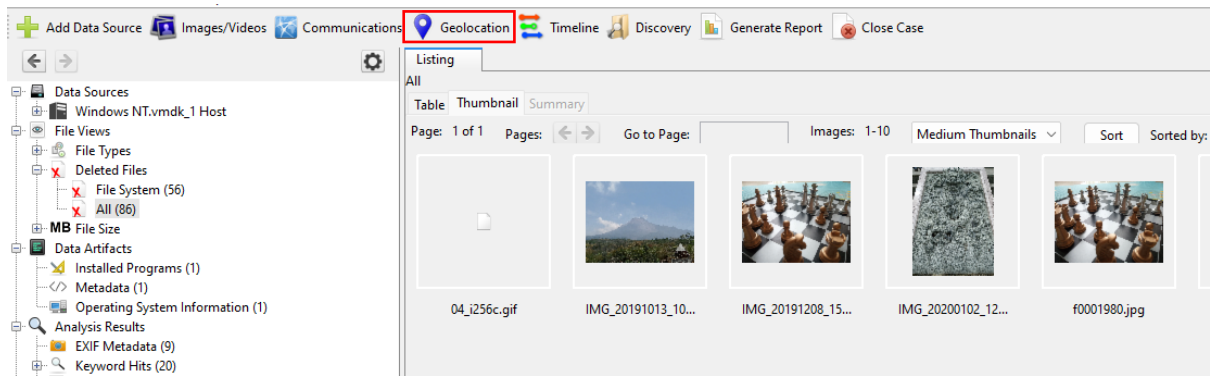
Klik pada Thumbnail dan teman-teman dapat melihat file mana saja yang dapat direcovery tanpa adanya corrupted data.



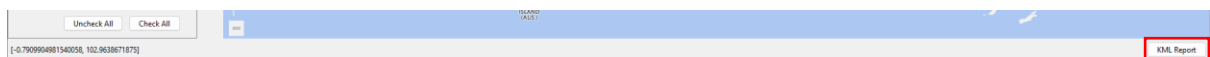
Lakukanlah restore pada satu buah foto dengan cara klik kanan pada mouse dan pilih extract file(s). lalu, pilih lokasi yang teman-teman inginkan



Setelah itu teman-teman juga dapat melihat lokasi pengambilan foto di geolocation



Setelah itu teman-teman dapat membuat laporan dengan mengklik “KML” Report pada bagian kiri bawah.



Teman-teman juga bisa mengetahui kapan gambar-gambar tersebut ditambahkan dengan membuka timeline.

