Forensik Digital

SEMESTER GENAP T.A 2023/2024

LAB 1

Memory Image Forensic

Program Studi Informatika
Fakultas Teknologi Industri
Universitas Atma Jaya Yogyakarta

REQUIREMENT

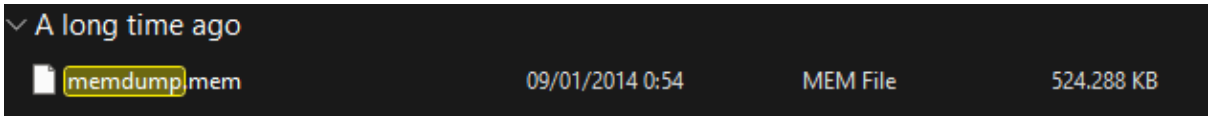
1. Autopsy (instalasi dapat dilihat di tutorial instalasi yang ada di situs kuliah)
2. Memory Image: klik disini untuk mendowload memory image

PENJELASAN

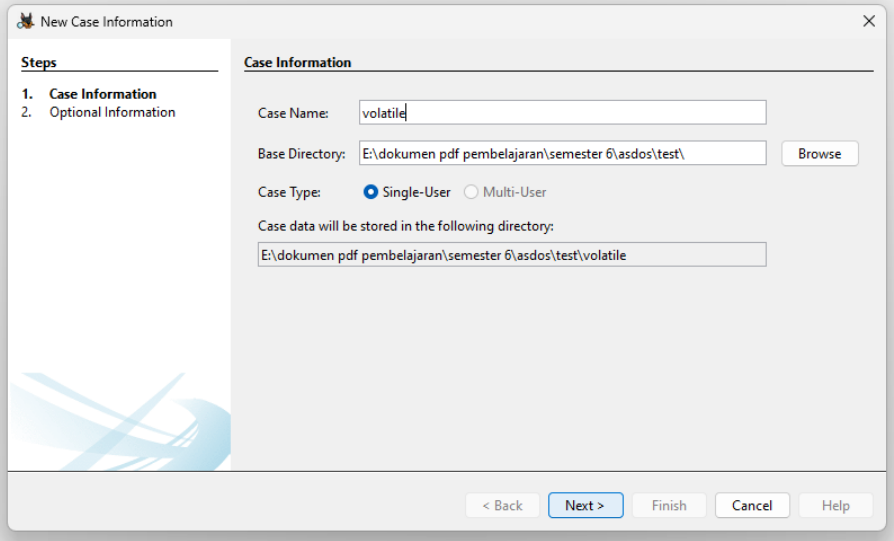
Memory Image adalah proses pengambilan snapshot dari memori yang volatile pada sebuah sistem komputer pada titik waktu tertentu. Tujuan dari Memory Image sendiri adalah meekam kondisi memori sistem pada waktu tertentu, yang kemudian dapat digunakna untuk analisis atau investigasi. Dalam kesempatan kali ini kita akan menggunakan autopsy untuk melakukan Memory Image Forensic.

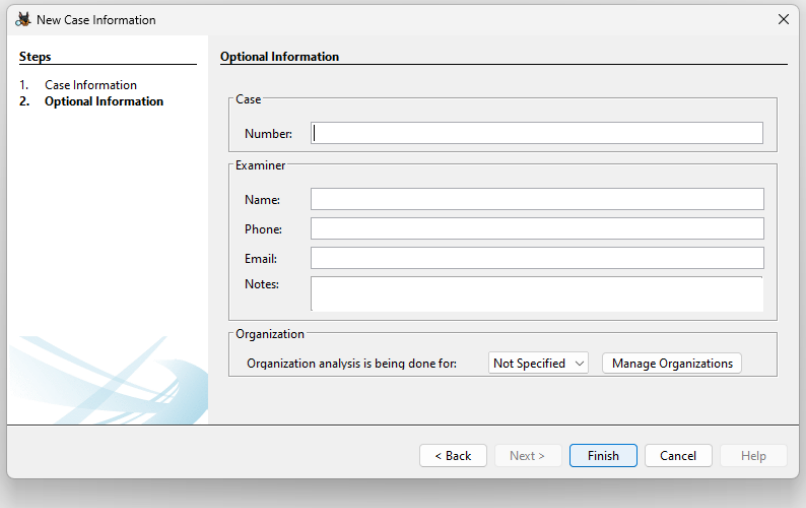
TUTORIAL

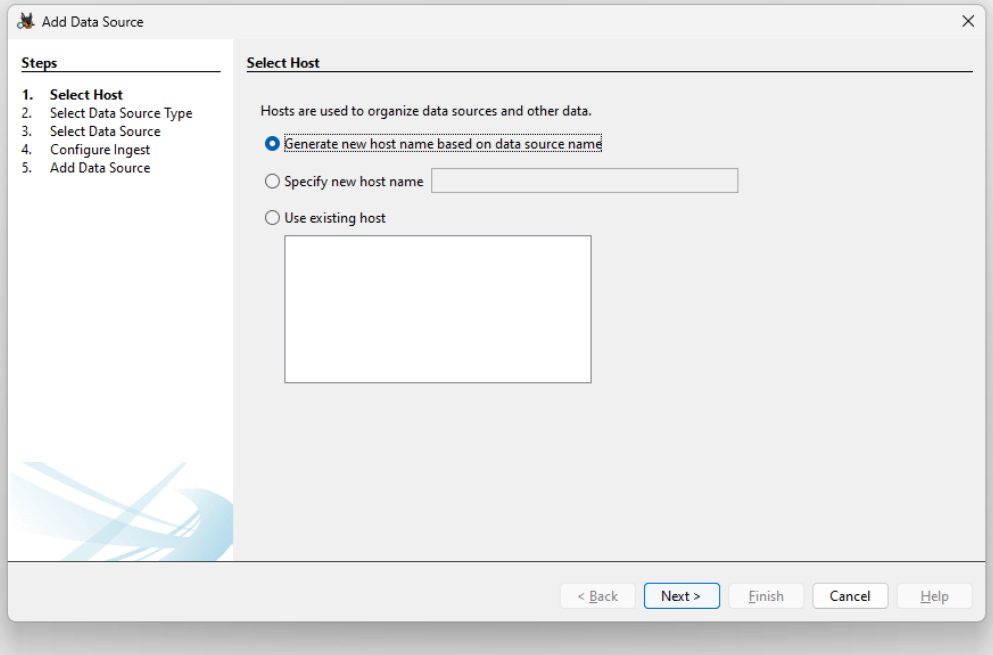
Extract lah file yang sudah didownload pada requirement diatas.



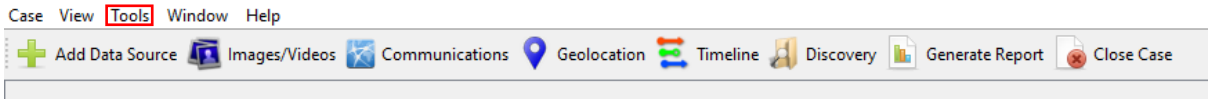
File akan memiliki extensi mem file, setelah itu buka autopsy teman-teman dan buatlah sebuah case baru dengan penamaan bebas.

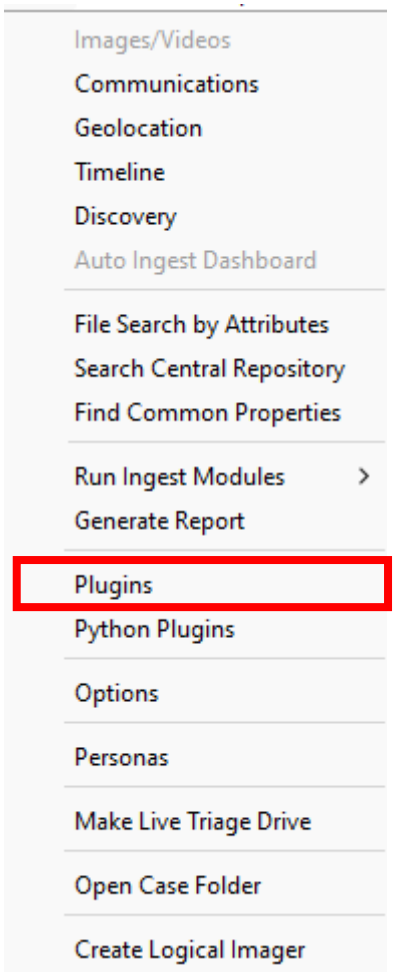


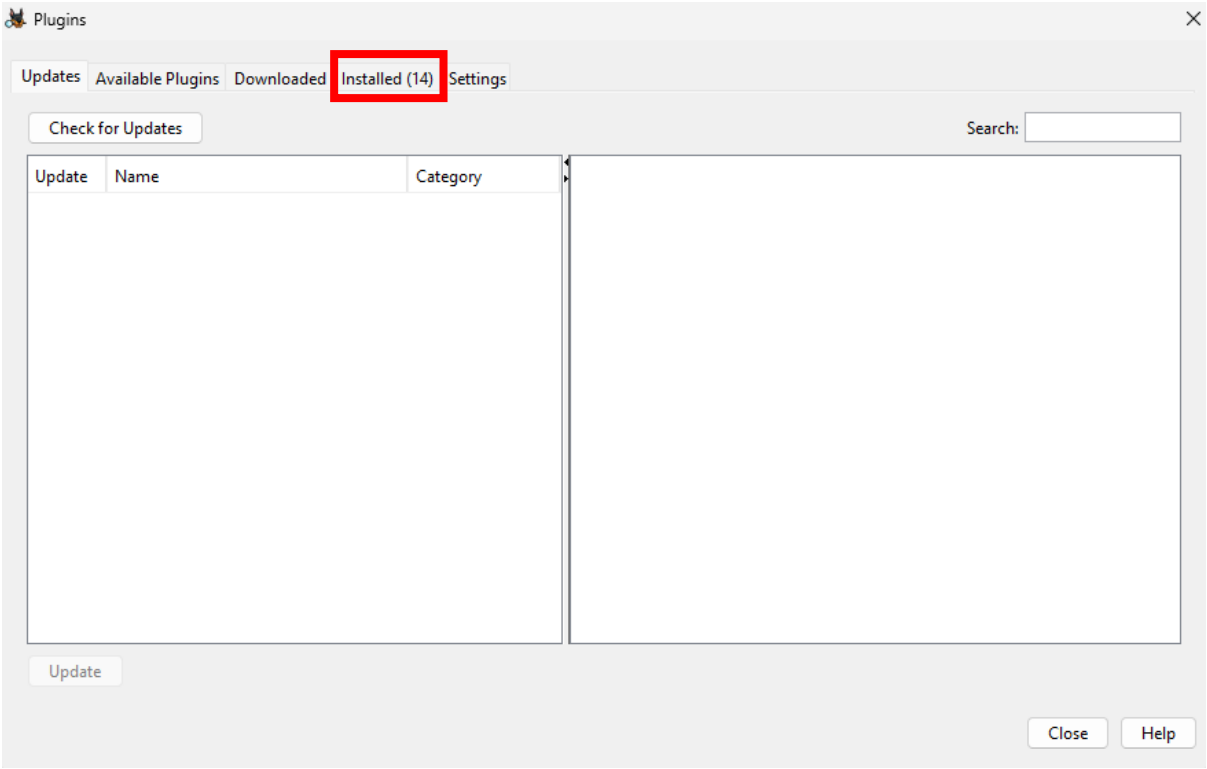


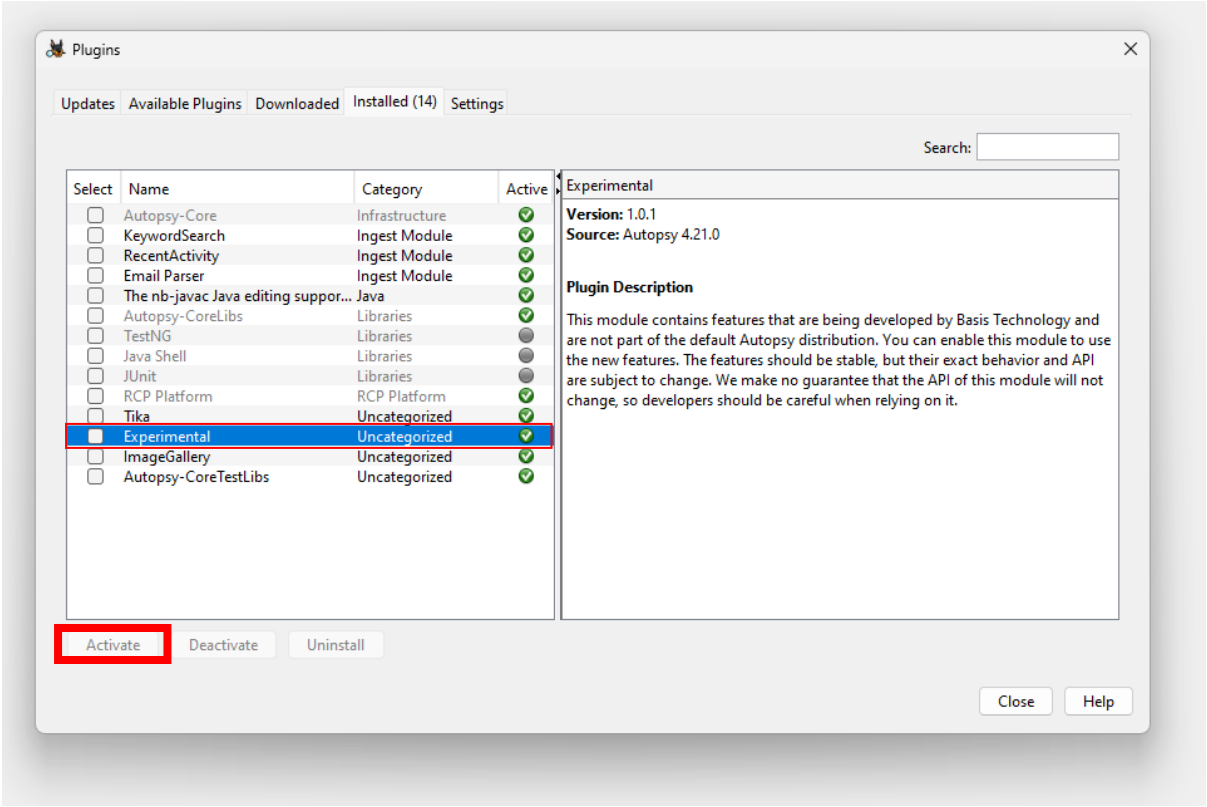


Setelah itu, pada bagian “Select Data Source Type” pilih Memory image disk(Volatility). Jika tidak ada opsi tersebut, teman-teman dapat mengatur nya di tool->Plugin->installed->experimental->Active

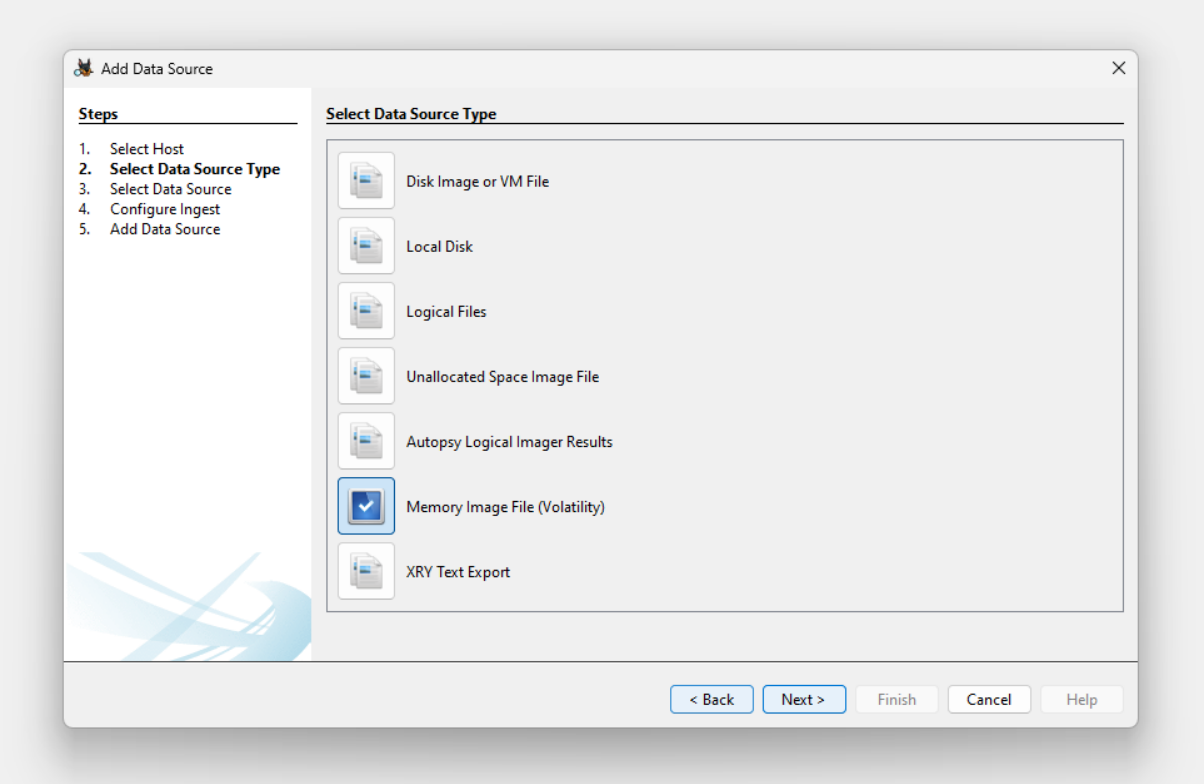

Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case


Images/Videos
Communications
Geolocation
Timeline
Discovery
Auto Ingest Dashboard
File Search by Attributes
Search Central Repository
Find Common Properties
Run Ingest Modules
Generate Report
Plugins
Python Plugins
Options
Personas
Make Live Triage Drive
Open Case Folder
Create Logical Imager





Setelah itu, maka Memory image disk(Volatility).

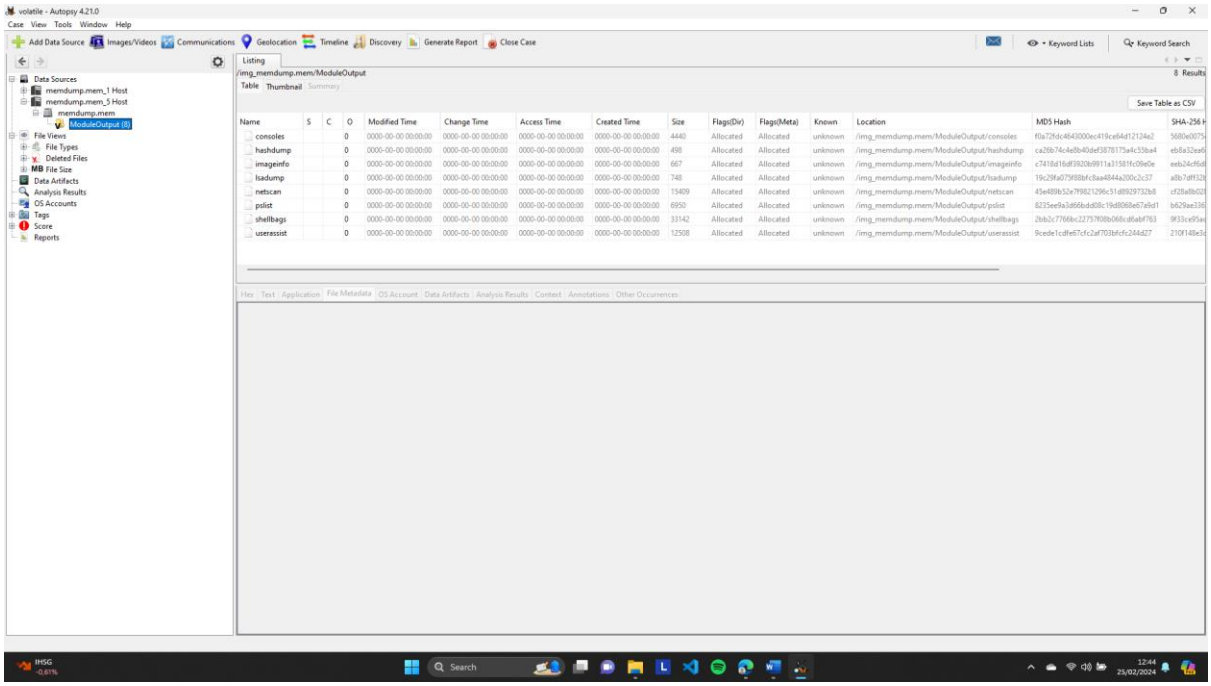


Klik next, lalu browse tempat dimana teman-teman menyimpan file memdump.mem tadi yang sudah di extract. Lalu pada plugin. Cukup ceklis beberapa plugin dibawah ini:

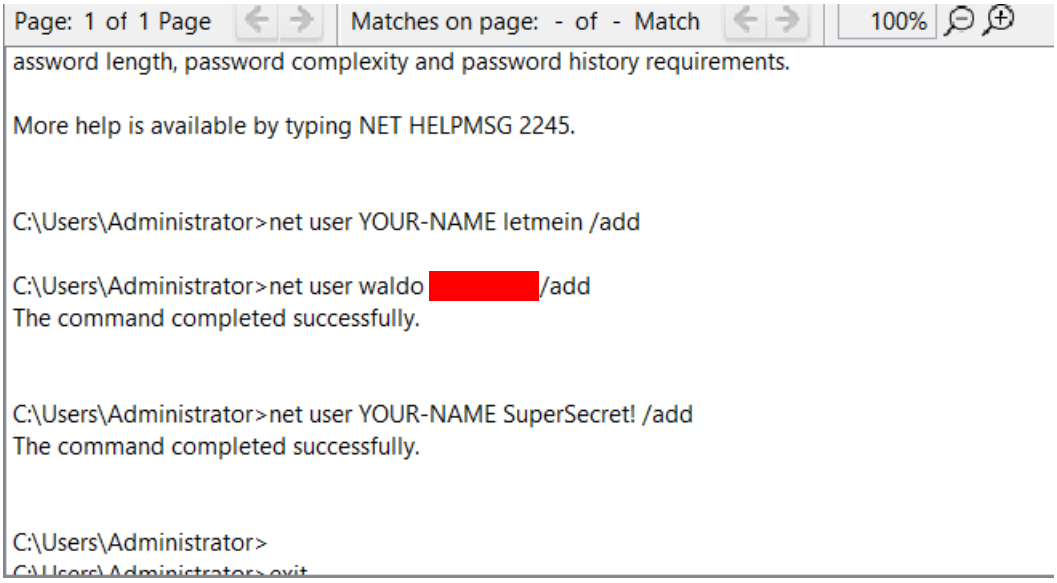
- Consoles (untuk mengekstrak informasi konsol yang berjalan)
- Hashdump (untuk mengekstrak nilai hash dari password pengguna)
- Isadump (untuk mengekstrak informasi ruang alamt ISA)
- Netscan (untuk pemindaian jaringan pada memori sistem)
- Pslist (untuk mengekstrak daftar proses yang berjalan pada sistem)
- Shellbags (untuk mengekstrak informasi tentang shellbags dalam sistem)
- Userassist (untuk mengekstrak informasi tentang penggunaan aplikasi)

Setelah itu tinggal next dan finish.

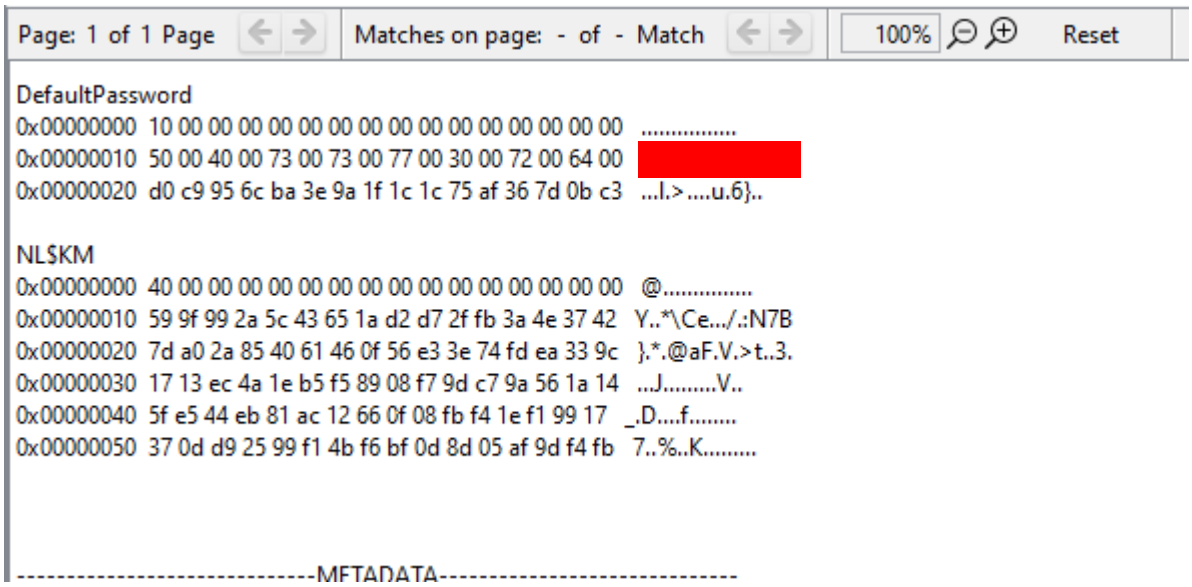
Berikut adalah tampilan awal dari autopsy jika teman-teman sudah melakukannya dengan benar.



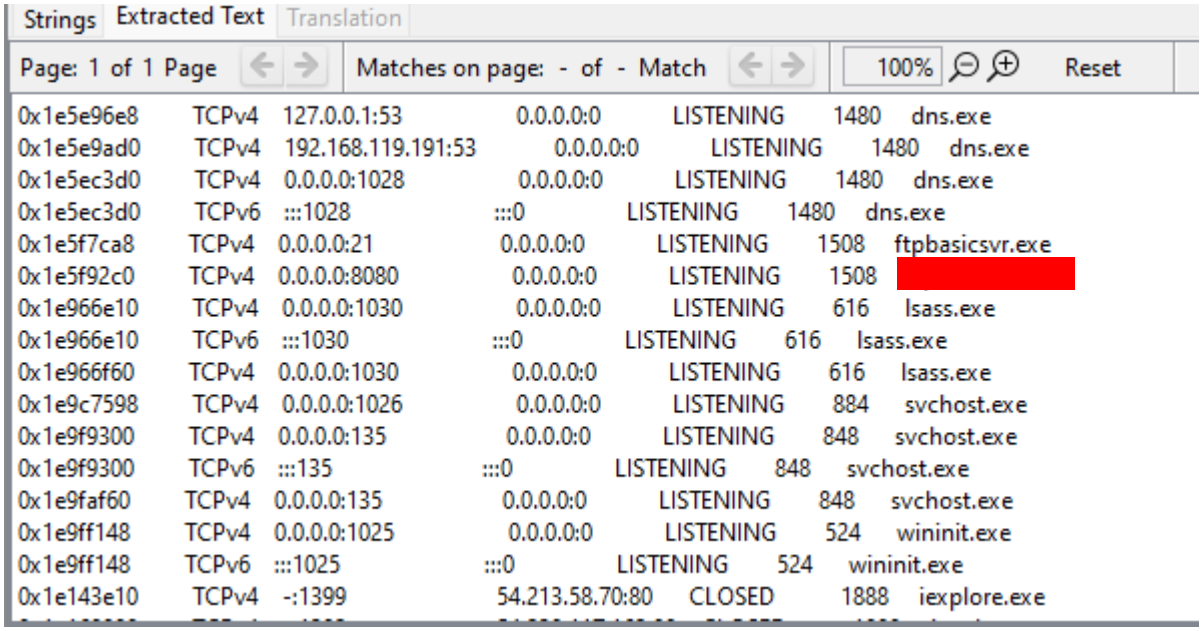
- Buka Consoles dan carilah “waldo’s password” yang tertutup pada gambar dibawah.



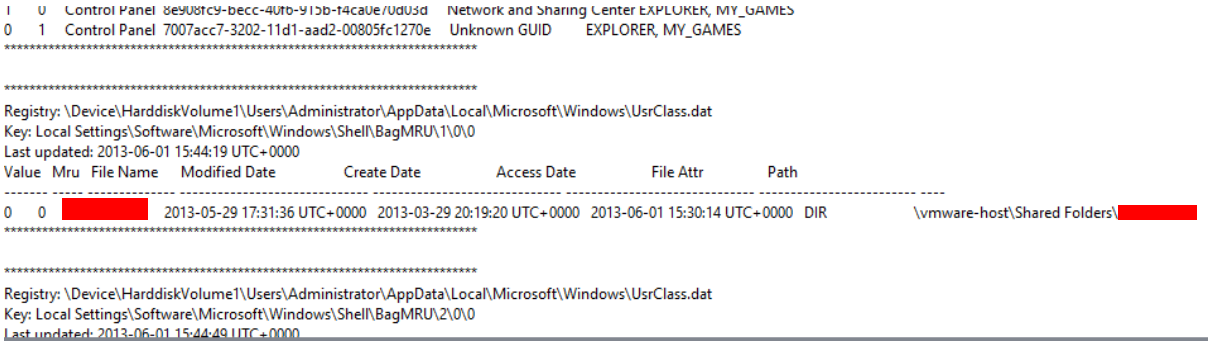
- Buka isadump dan carilah password default, yang tertutup pada gambar dibawah.



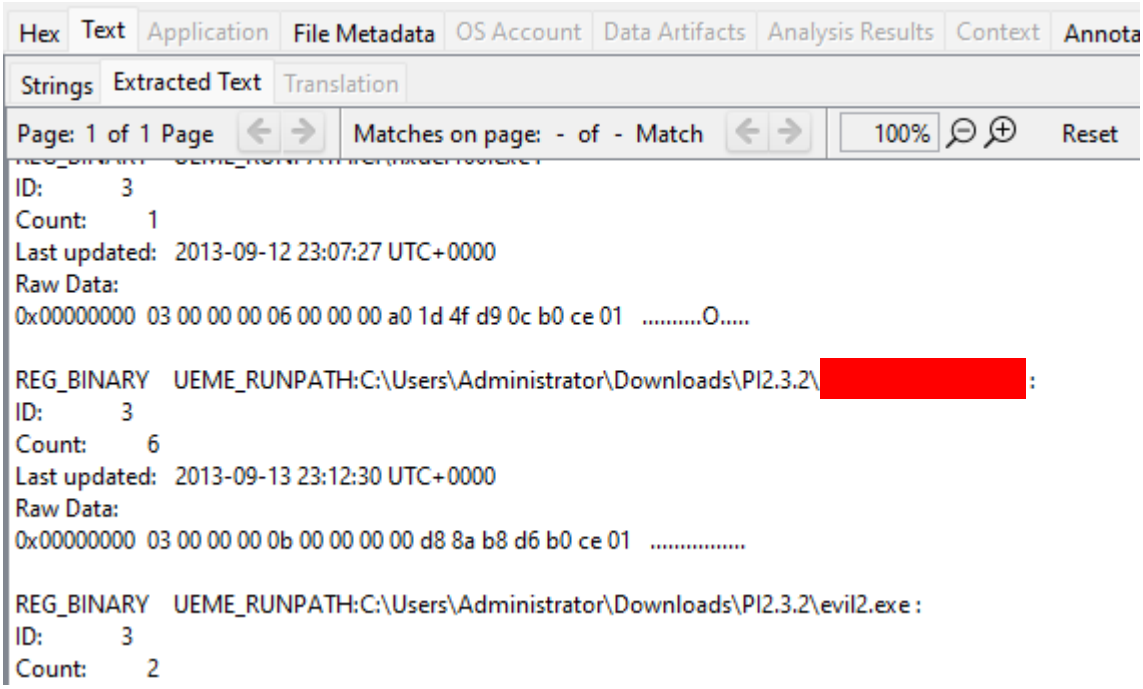
- Buka netscan dan carilah executable listening di port 8080, yang tertutup pada gambar dibawah.



- Pada bagian shellbags carilah shared folder yang terhubung dengan mesin ini, yang tertutup pada gambar dibawah.



- Pada bagian userassist, carilah nama dangerous executable yang berjalan pada 13-09-2013 pukul 23:12:30, yang tertutup pada gambar dibawah.



- Carilah password dari akun probe di bagian hashdump. Setelah ketemu, cobalah untuk melakukan decrypt pada hash code tersebut.