LAPORAN TUGAS AUTOPSY PADA MATA KULIAH FORENSIKA DIGITAL

Dosen Pengampu: Rizky Fenaldo Maulana, S.Kom., M.Kom.

Disusun Oleh :

Rayhan Furqoni

1203210139

IF 01-01

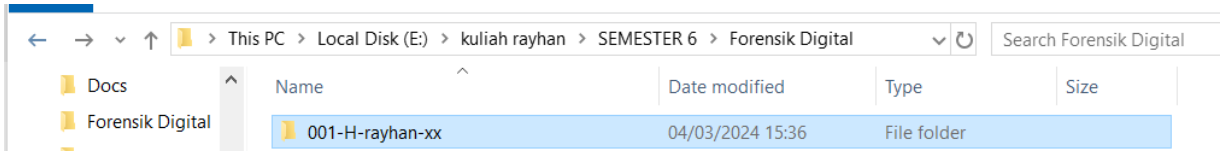
PROGRAM STUDI INFORMATIKA

FAKULTAS INFORMATIKA

TELKOM UNIVERSITY SURABAYA

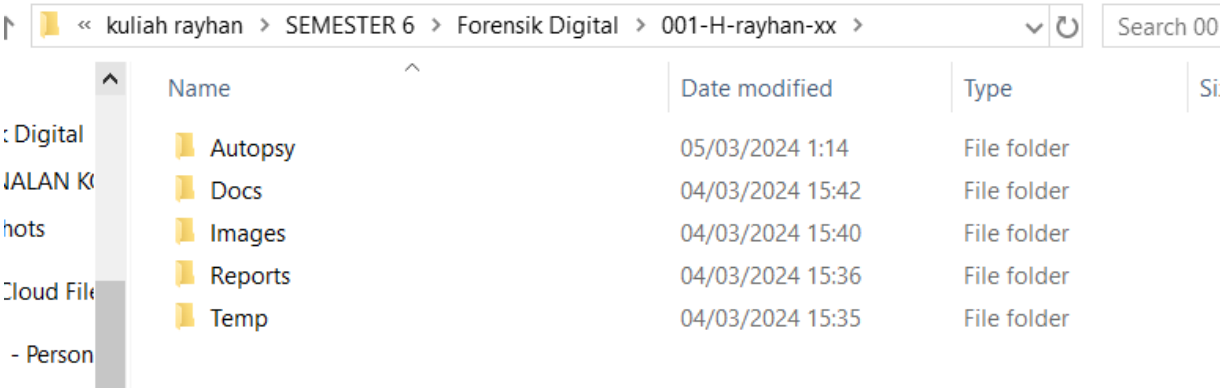
TAHUN AJARAN 2023/2024

1. Mendownload Autopsy 4.21.0
2. Selanjutnya di local disk E dengan nama file 001-H-rayhan-xx.

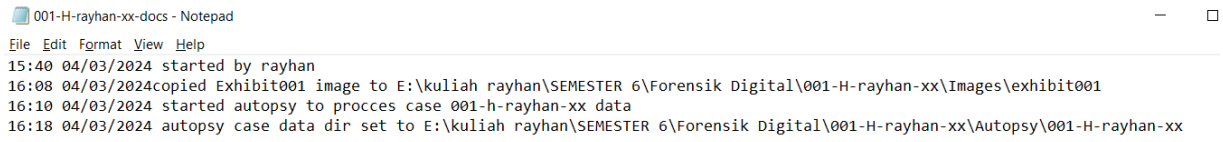


001 adalah nomor kasus , H adalah kategori kasus, rayhan adalah nama penyidik dan XX ini adalah inisialnya anggota penyelidik.

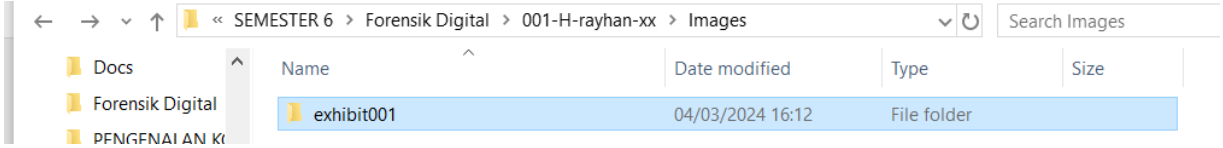
3. kemudiam kits membuat file Docs, Image, temp, Autopsy, Reports didalam file 001- H-rayhan-xx.



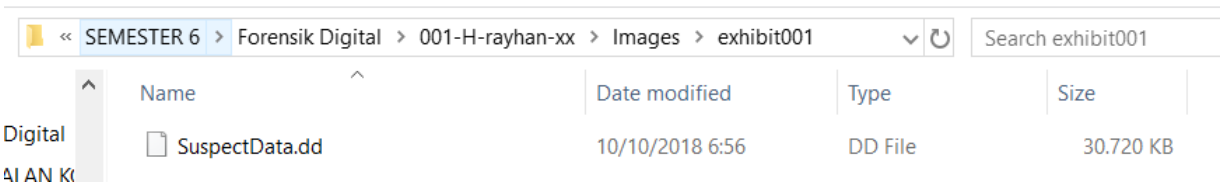
4. masuk kedoc dan membuat dokumen txt yang judulnya sesuai case yaitu 001-H-jij-XX-doc.txt, untuk mencatat waktu dan apa yang kita lakukan terhadap file yang diautopsi



5. buat file exhibit001 di folder image. Folder exhibit untuk data yang dicurigai

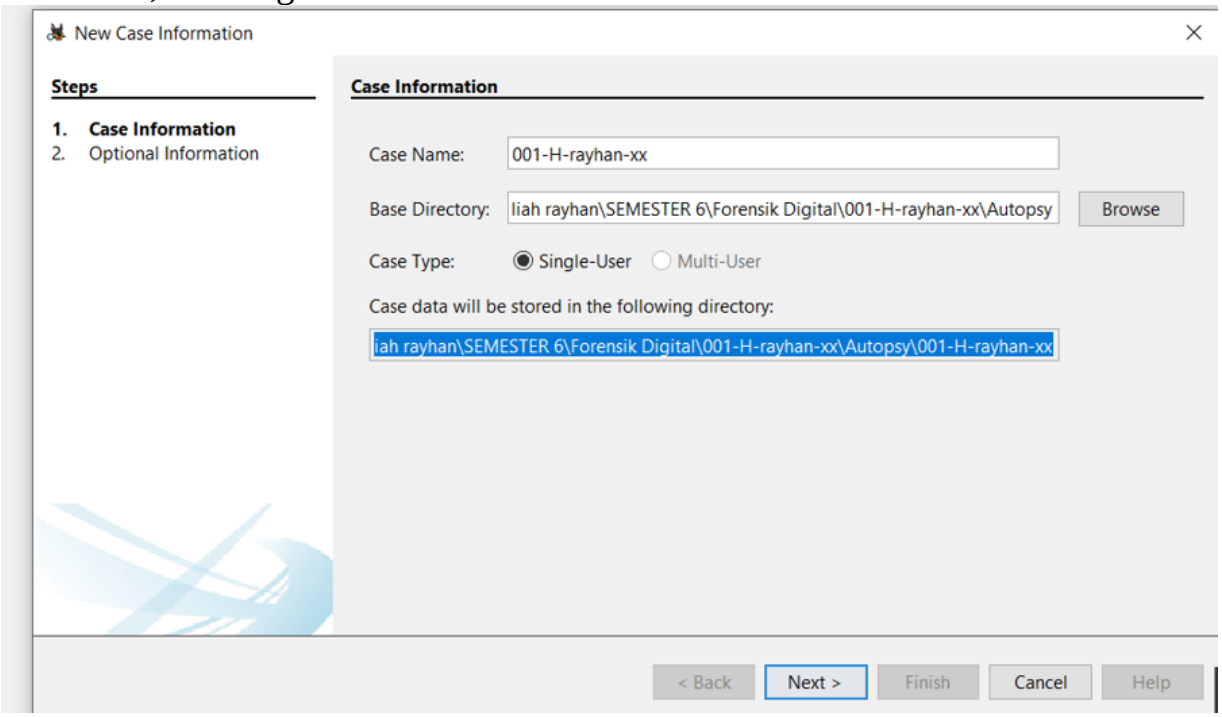


setelah itu memasukkan case suspect yaitu folder suspectdata.dd

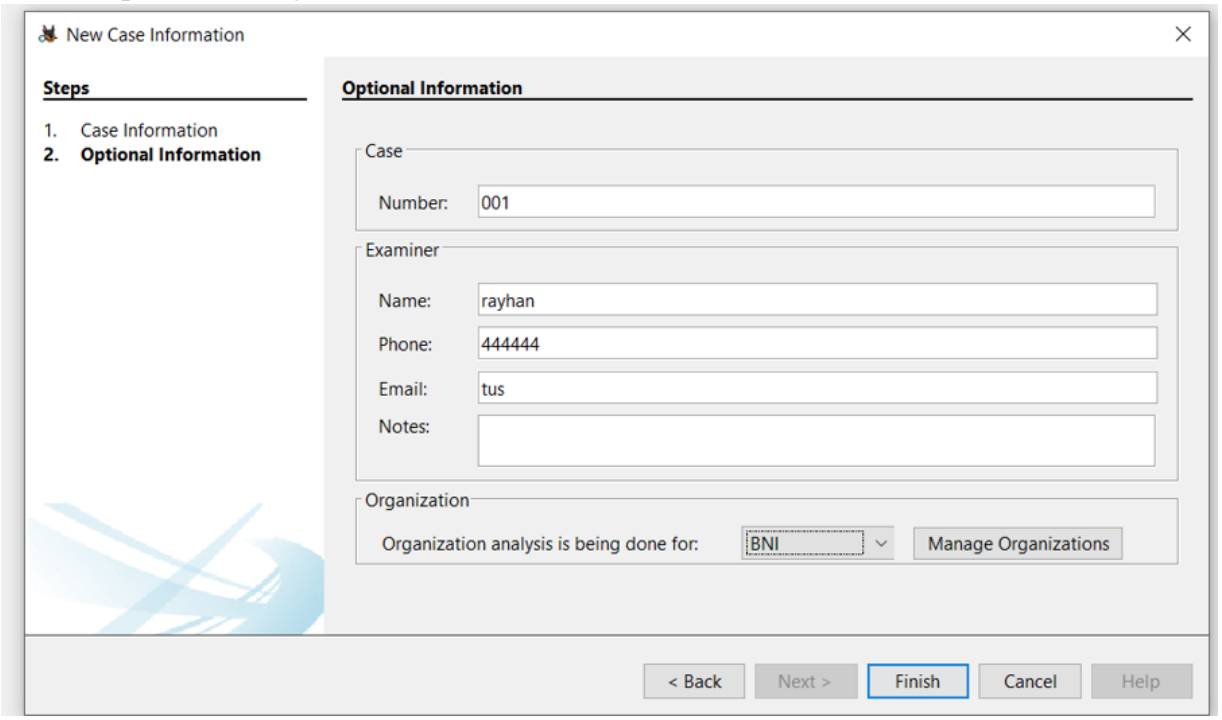


6. membuka aplikasi autopsy,dan membuat file baru dan mengisi file case

lokasi file,dam single user.



7. mengisi optional information untuk mengetahui harus kemana jika terjadi sesuatu pada case nya



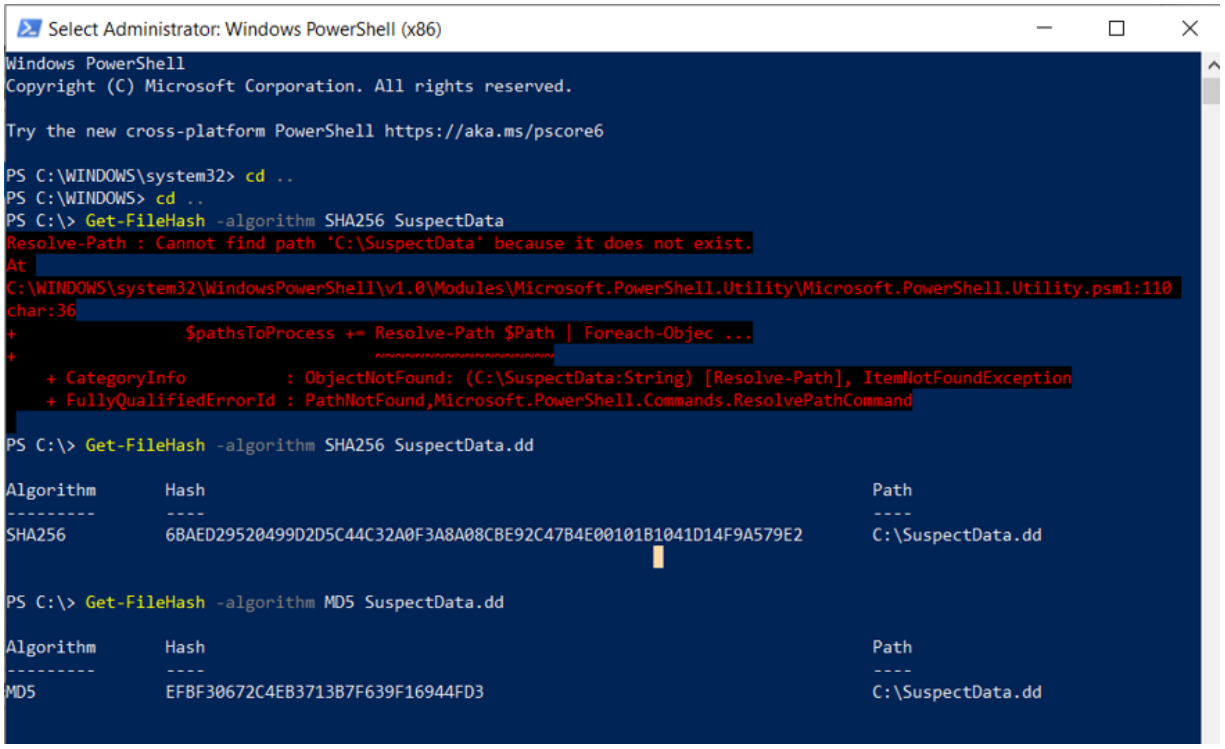
- case number: 001
- Name : rayhan
- Phone : 444444
- Email : tus
- Pilih organization analysis is being done for : BNI

8. Ketika sudah mengisi klik finish , dan Pilih specify new host name : Exhibit001,sesuai dengan file sebelumnya.
9. selanjutnya klik next. Klik disk image or VM file
10. Selanjutnya mengisi select data source

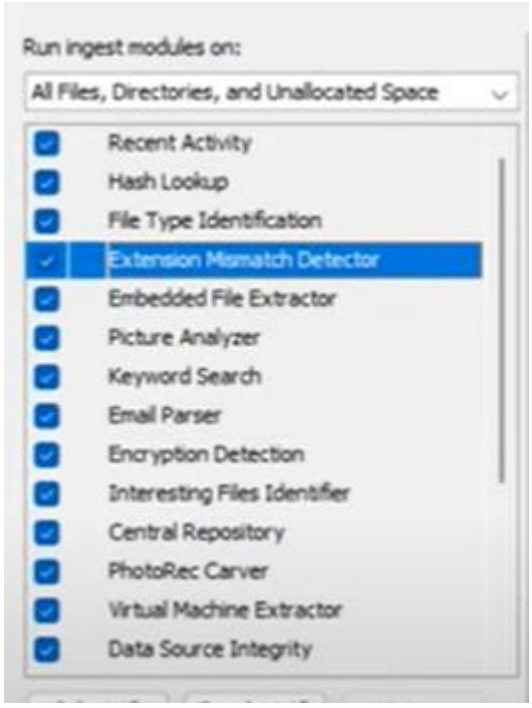
Path image: 001-H-jij- XX\Image\SuspectData.dd,

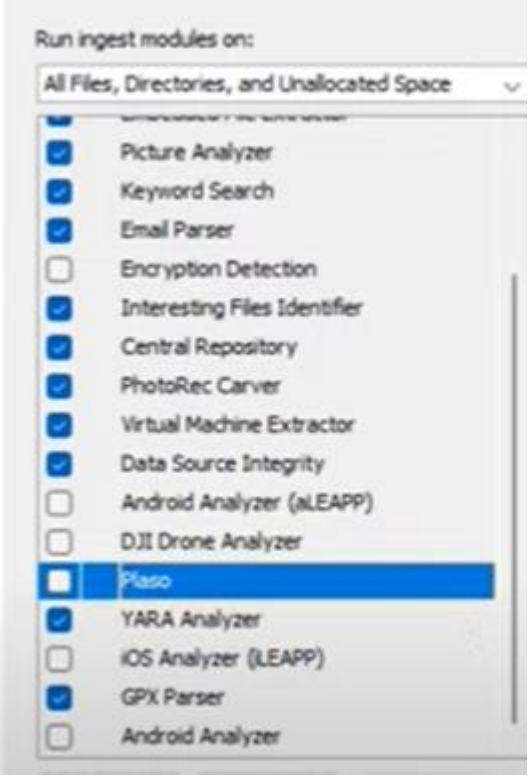
Pilih time zone wilayah : pilih zona waktu sesuai dengan lokasi file dibuat, jika tidak tau pilih gmt 0:00 utc

Isi hash value:



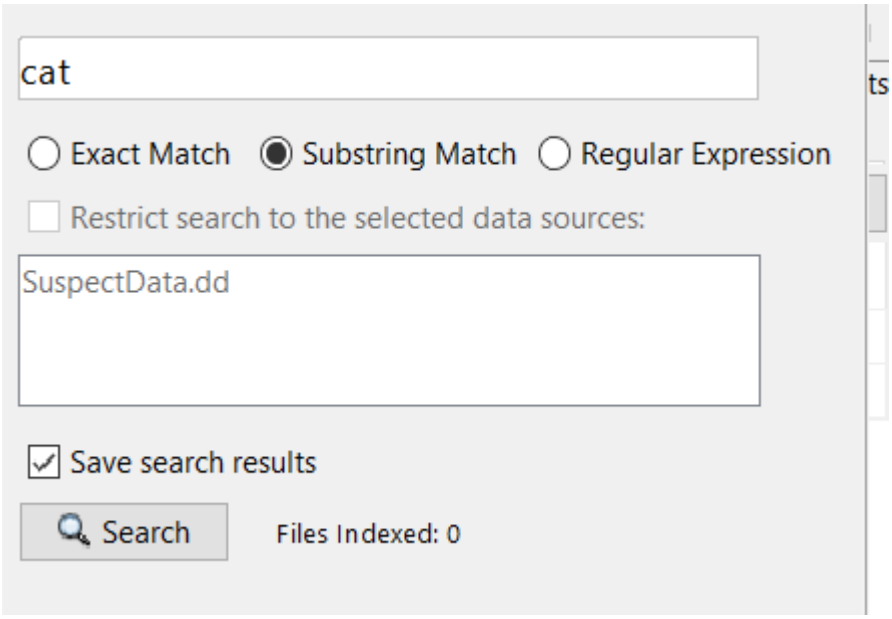
Selanjutnya klik next, dan centang yang diperlukan untuk identifikasi





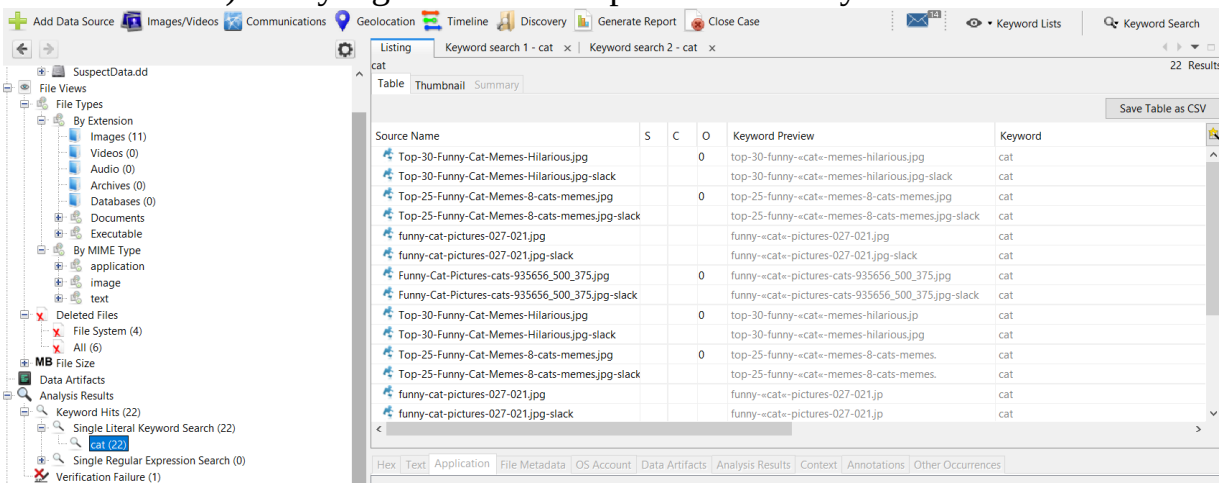
11. Penjelasan singkat pencarian
    - **hash lookup** memungkinkan pengaturan database hash dari file yang diketahui baik dan file buruk yang diketahui. Database hash tersebut dapat digunakan untuk memfilter file yang diketahui baik sehingga tidak perlu diperiksa lagi di Autopsy. Selain itu, hash juga dapat menambahkan database hash file-file buruk yang diketahui, sehingga jika ada file yang cocok dengan hash buruk yang terdaftar, file tersebut secara otomatis ditandai untuk diperiksa lebih lanjut. Hal ini memudahkan proses penyelidikan.
    - file type identification adalah langkah yang memungkinkan pengguna untuk mengatur jenis file yang ingin dicocokkan dalam pengaturan global, sehingga Autopsy dapat mengenali dan mengklasifikasikan file dengan lebih akurat selama proses penyelidikan. Dengan mengatur jenis file yang ingin dicocokkan, pengguna dapat mempersempit atau memperluas ruang lingkup pencarian, meningkatkan efisiensi dalam menemukan bukti digital yang relevan.
    - photorec carver untuk menambah data atau mengembalikan data
    - android dan drone analyzer tidak digunakan karena kita tidak menggunakan android, dan drone analysis
    - plaso tidak dicentang karena terlalu lama untuk identifikasi, jika ingin lebih detail bisa di centang
    - yara dicentang untuk analisis struktur file
    - ios analyzer tidak digunakan karena tidak memakai ios
    - gpx dicentang karena untuk menemukan informasi lokasi potensial

12. Selanjutnya klik next, dan data diproses untuk ditampilkan isinya
13. Selanjutnya di exhibit001 kita dapat melihat gambar dan data mentah dimana dari gambar yang dapat kita lihat ditampilan hex (tampilan ascii).\
14. Klik launch hxd
15. Kita bisa mencari data berdasarkan exach match dan substring match/

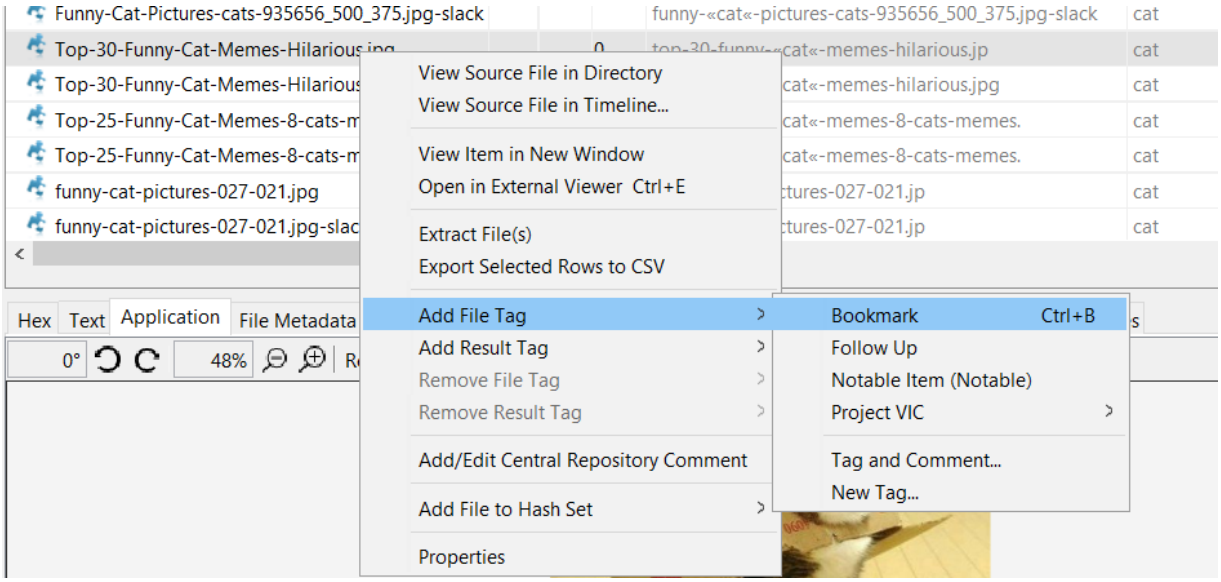


Exach match untuk memilih kata yang sesuai dengan yang kita cari contoh cat maka kata yang ada kata cat akan ditampilkan lebih spesifik, kalau substring match untuk mencari kata yang ada cat tidak terlalu spesifik lebih luas contoh kata cats akan tampil karena ada kata cat.

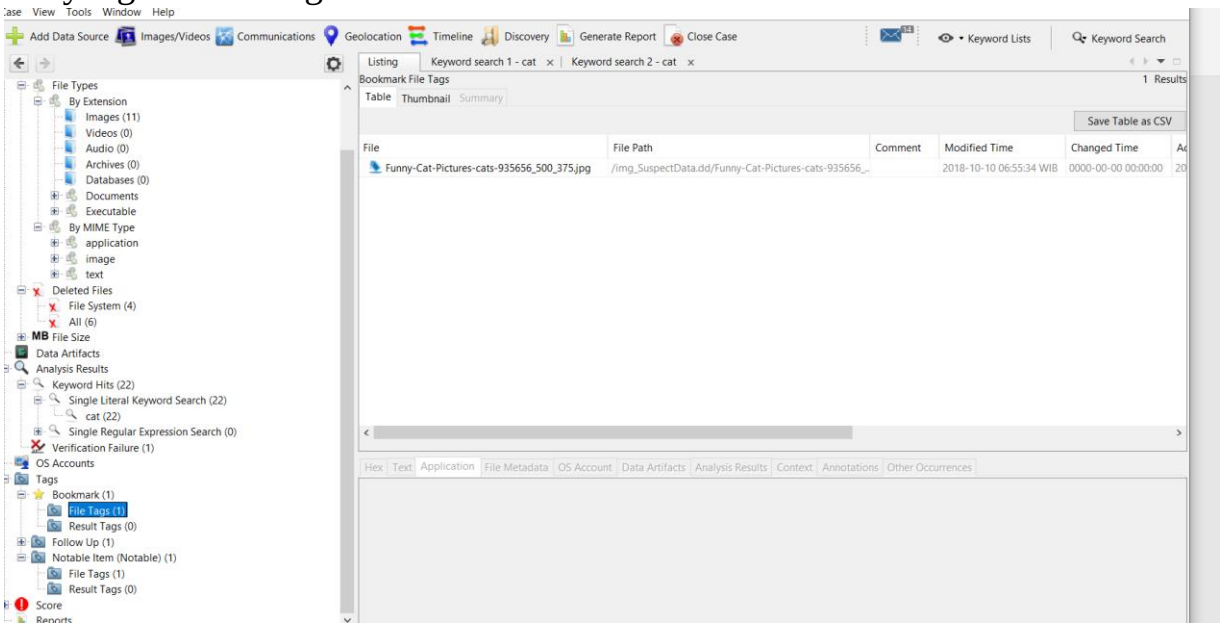
16. Jika sudah kita pilih keyword hits lalu selanjutnya klik single literal keyword serch (disitu akan memunculkan kembali apa yang sudah kita search tadi) yang di suspectdata keyword search.



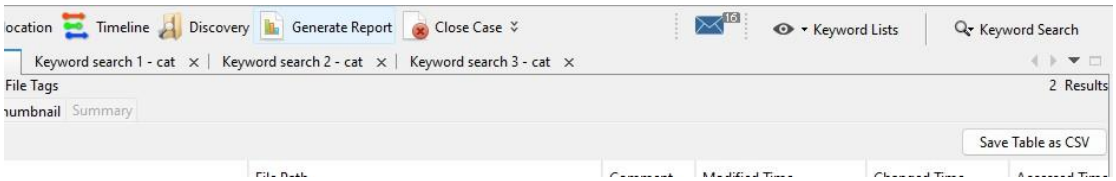
17. Selanjutnya pada keyword search di cat kita bisa menambahkan beberapa tag yaitu bookmark, follow up, notable, dengan cara klik kanan klik add tag, dan pilih antara 3 tag tadi.


Funny-Cat-Pictures-cats-935656_500_375.jpg-slack
funny-«cat«-pictures-cats-935656_500_375.jpg-slack
cat
Top-30-Funny-Cat-Memes-Hilarious.jpg
cat«-memes-hilarious.jp
cat
Top-30-Funny-Cat-Memes-Hilarious
cat«-memes-hilarious.jpg
cat
Top-25-Funny-Cat-Memes-8-cats-m
cat«-memes-8-cats-memes.
cat
Top-25-Funny-Cat-Memes-8-cats-m
cat«-memes-8-cats-memes.
cat
funny-cat-pictures-027-021.jpg
tures-027-021.jp
cat
funny-cat-pictures-027-021.jpg-slac
tures-027-021.jp
cat
Hex
Text
Application
File Metadata
0°
48%
View Source File in Directory
View Source File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)
Export Selected Rows to CSV
Add File Tag
Add Result Tag
Remove File Tag
Remove Result Tag
Add/Edit Central Repository Comment
Add File to Hash Set
Properties
Bookmark Ctrl+B
Follow Up
Notable Item (Notable)
Project VIC
Tag and Comment...
New Tag...

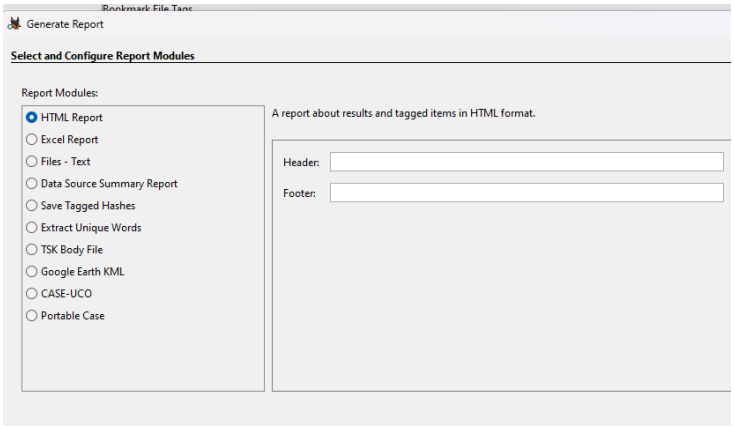
18. Pilih tags, selanjutnya pilih bookmark, klik file tags disitu akan muncul file yang kita beri tag.



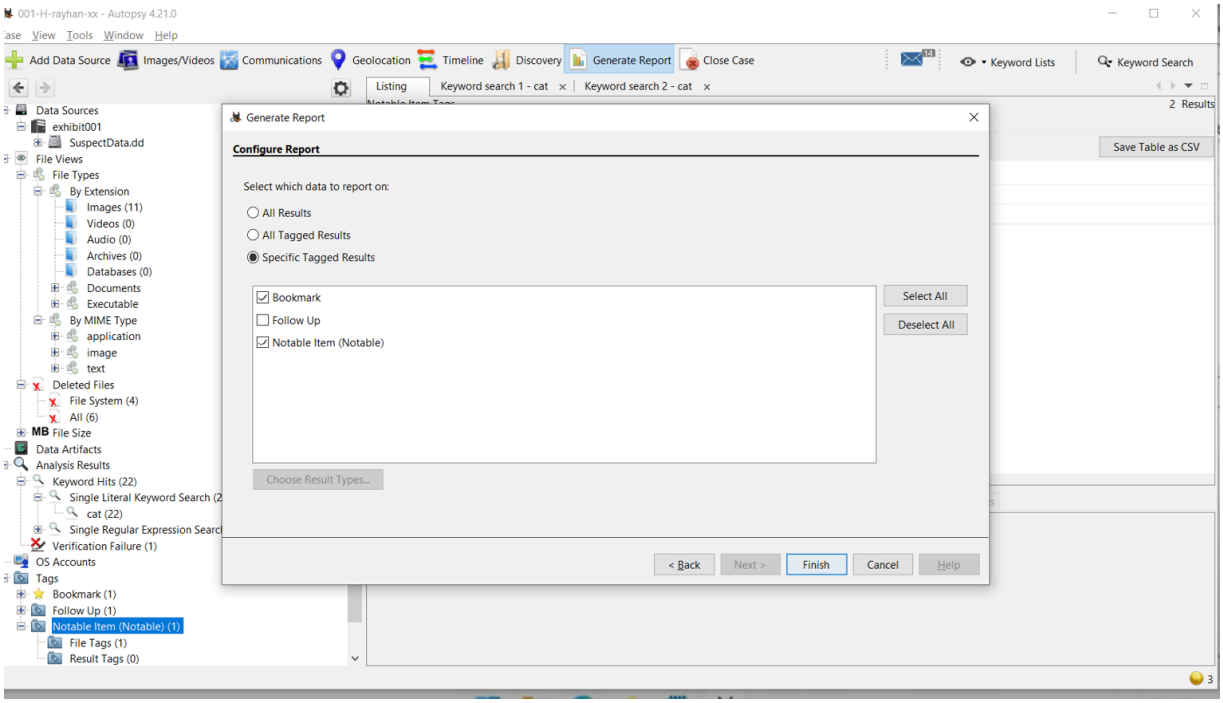
19. Klik generate report untuk membuat laporan dan apa yang dilakukan pada beberapa jenis laporan yang berbeda.



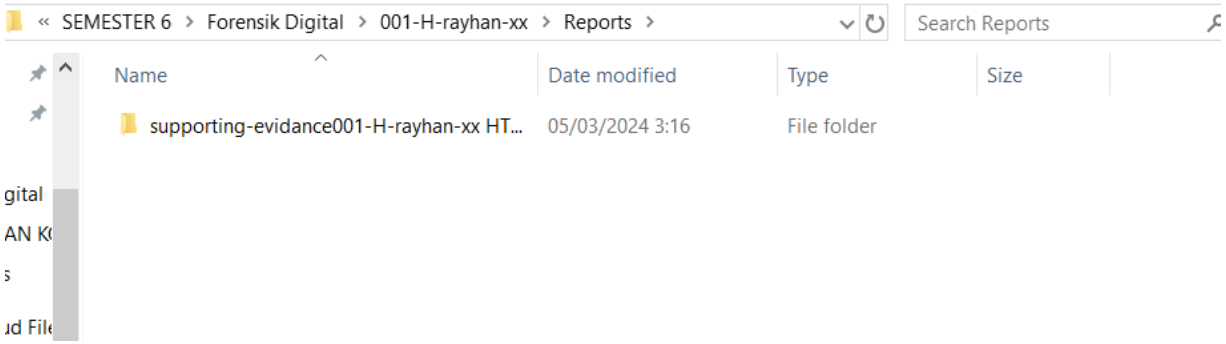
20. Selanjutnya klik html report kemudian akan memproses data yang dicurigai (suspectdata.dd).



21. Selanjutnya klik spesifik tagged result untuk data yang dilaporkan yang dapat melakukan hasil yang diberi tags tertentu selanjutnya akan melakukan hasil yang diberi tags khusus lalu klik centang bookmark dan notable, dan klik finish



22. Setelah diproses kita masukkan data report ke file kasus kita


« SEMESTER 6 › Forensik Digital › 001-H-rayhan-xx › Reports ›
Search Reports
Name
Date modified
Type
Size
supporting-evidance001-H-rayhan-xx HT...
05/03/2024 3:16
File folder

Jadi kesimpulan yang saya dapat mengidentifikasi file yang sudah tidak tau bentuknya/terhapus kita dapat mengembalikan dan identifikasi menjadi file sebenarnya/semula