

# **LAPORAN TUGAS AUTOPSY PADA MATA KULIAH FORENSIKA DIGITAL**



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

**Disusun Oleh :**

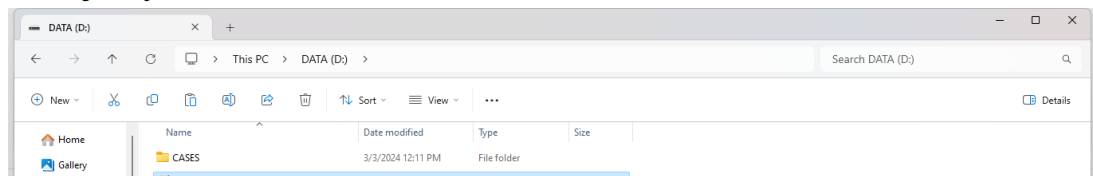
**Emilia Ramona**

**1203210017**

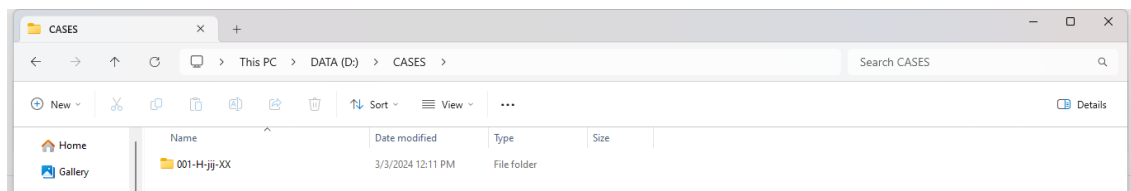
**IF 01-01**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS INFORMATIKA  
TELKOM UNIVERSITY SURABAYA  
TAHUN AJARAN 2023/2024**

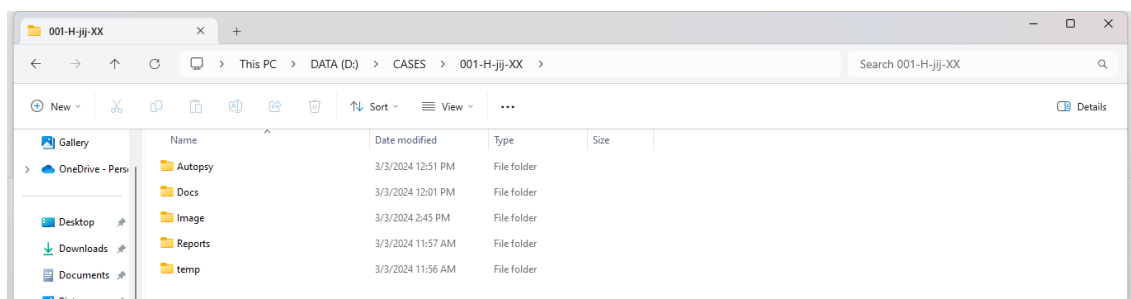
1. Mendownload Autopsy 4.21.0
2. Selanjutnya di local disk D Membuat folder Cases.



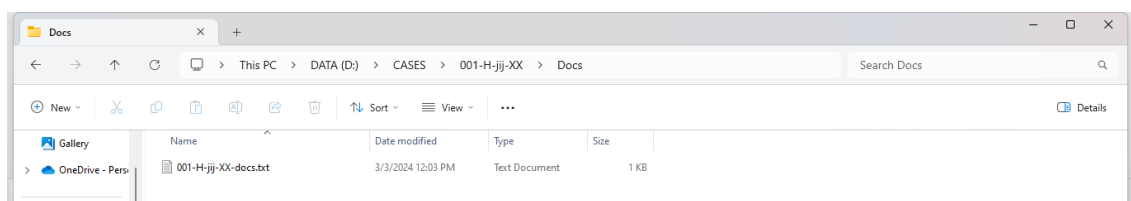
3. Selanjutnya di dalam folder cases, membuat folder dengan nomor kasus 001 dan menambahkan semacam indikator jenis investigasi, dengan cara itu saya bisa melihat kasus saya yang mungkin tidak mengenali nomor kasusnya tetapi saya dapat mengenali tagnya jadi saya akan memberi tanda H, sedangkan jij ini yaitu tentang tag penyelidik dan XX ini adalah inisialnya anggota penyelidik.



4. Selanjutnya didalam folder 001-H-jij-XX ini akan membuat folder lagi yang terdiri Docs, Image, temp, Autopsy, Reports.



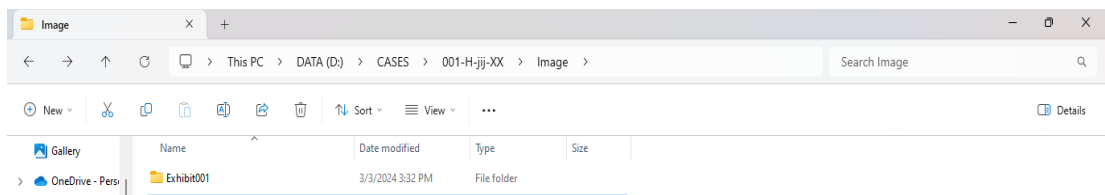
5. Selanjutnya masuk ke dokumen (docs) dan saya akan membuat dokumen teks baru yang berjudul 001-H-jij-XX-doc.txt,



Selanjutnya membuat dokumentasi kasus yang dibuka di notepad. untuk memasukkan stempel waktu tekan f5, dan sebelum keluar jangan lupa untuk disimpan.

```
File Edit View
12:01 PM 3/3/2024 Case 001-jij-XX started by JIJ
12:19 PM 3/3/2024 Copied Exhibit001 image to D:\CASES\001-H-jij-XX\Image
12:21 PM 3/3/2024 Exhibit001 image SHA356
12:22 PM 3/3/2024 Started Autopsy4.19.3 to process case 001-H-jij-XX data
12:47 PM 3/3/2024 Autopsy case data dir set to D:\CASES\001-H-jij-XX\Autopsy\001-H-jij-XX\
```

6. Membuat file di dalam folder image, jadi membuat data yang dicurigai yaitu Exhibit001. selanjutnya klik dua kali pada Exhibit001.



Kemudian memindahkan data ke direktori yang berjudul SuspectData.dd (ada di link youtube) dan selanjutnya menambahkan data SuspectData.dd-hashes.txt.

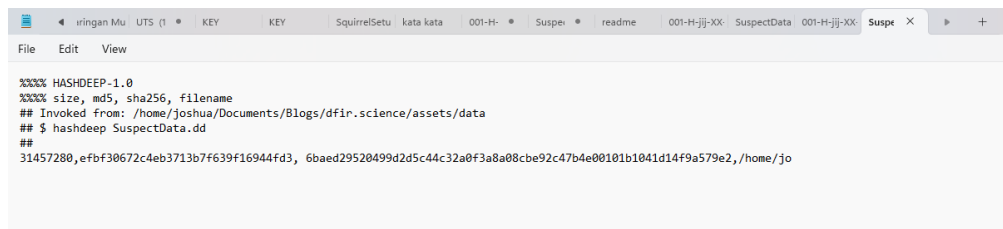
Name	Date modified	Type	Size
SuspectData.dd	3/3/2024 12:14 PM	DD File	30,720 KB
SuspectData.dd-hashes.txt	3/3/2024 12:14 PM	Text Document	0 KB
Top-30-Funny-Cat-Memes-Hilarious.jpg...	3/3/2024 2:45 PM	JPG-SLACK File	2 KB

7. Selanjutnya open aplikasi autopsy.
8. Selanjutnya pilih yang new case.
9. Isi case name : 001-H-jij-XX
10. Isi base directory : D:\CASES\001-H-jij-XX\Autopsy (alasan menggunakan nomor kasus adalah siapa pun yang membaca catatan ini melihat bawa catatan itu selalu berada di direktotri yang sama.
11. Pilih sigle user.
12. Selanjutnya klik next.
13. Selanjutnya isi number :001
  - Name : nama (emilia ramona)
  - Phone : isi nomor hp (agar sistem management tau akan menghubungi kesiapa kasus tersebut )
  - Email : isi email
  - Pilih organization analysis is being done for : CIA (sebelum nya saya menambahkan organisasi dulu yaitu CIA)\
  - Klik finish

14. Pilih specify new host name : Exhibit001, selanjutnya klik next.
15. Klik disk image or VM file : ini itu berada di folder image.
16. Selanjutnya pilih path image : D:\CASES\001-H-jij-XX\Image\SuspectData.dd
17. Pilih time zone wilayah posisi saya sekarang : saya pilih asia Jakarta.
18. Isi hash value

- md5 : efbf30672c4eb3713b7f639f16944fd3
- SHA-256 :  
6baed29520499d2d5c44c32a0f3a8a08cbe92c47b4e00101b1041d14f9a579e2

Ini ada di SuspectData.dd-hashes.txt



```

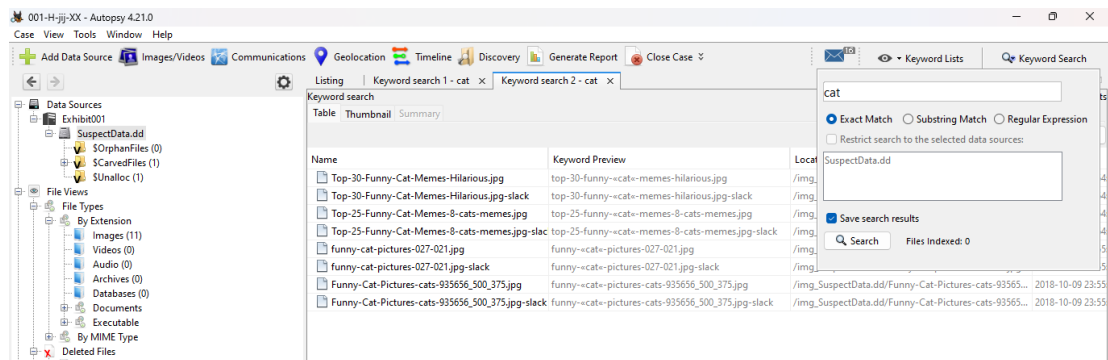
HASHDEEP-1.0
size, md5, sha256, filename
## Invoked from: /home/joshua/Documents/Blogs/dfir.science/assets/data
## $ hashdeep SuspectData.dd
##
31457280,efbf30672c4eb3713b7f639f16944fd3, 6baed29520499d2d5c44c32a0f3a8a08cbe92c47b4e00101b1041d14f9a579e2, /home/jo

```

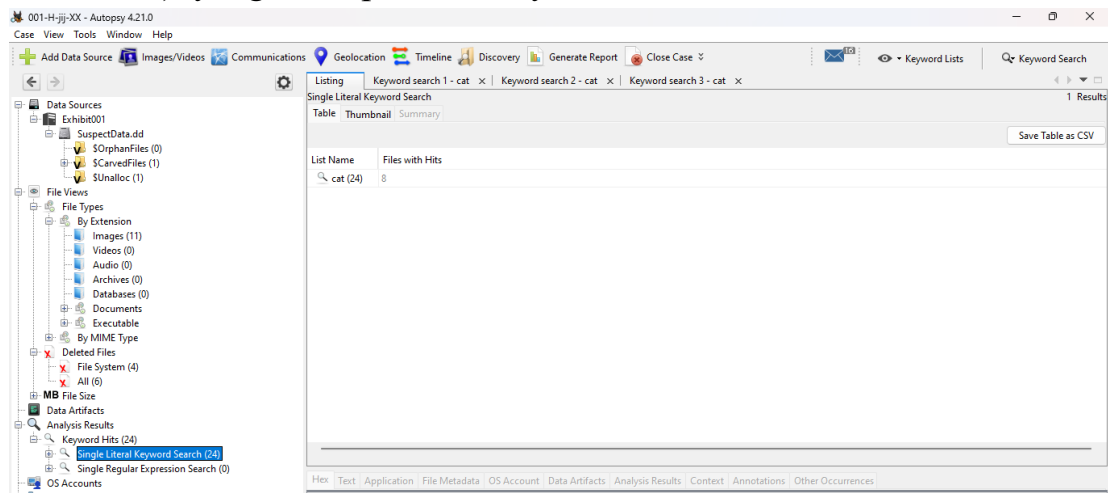
- Selanjutnya klik next

19. 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.
20. Selanjutnya klik 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.
21. Selanjutnya klik next.
22. Selanjutnya di exhibit001 kita dapat melihat gambar dan data mentah dimana dari gambar yang dapat kita lihat tampilan hex (tampilan ascii).
23. Klik launch in Hxd untuk menginstall (Jadi harus dowlod Hxd).

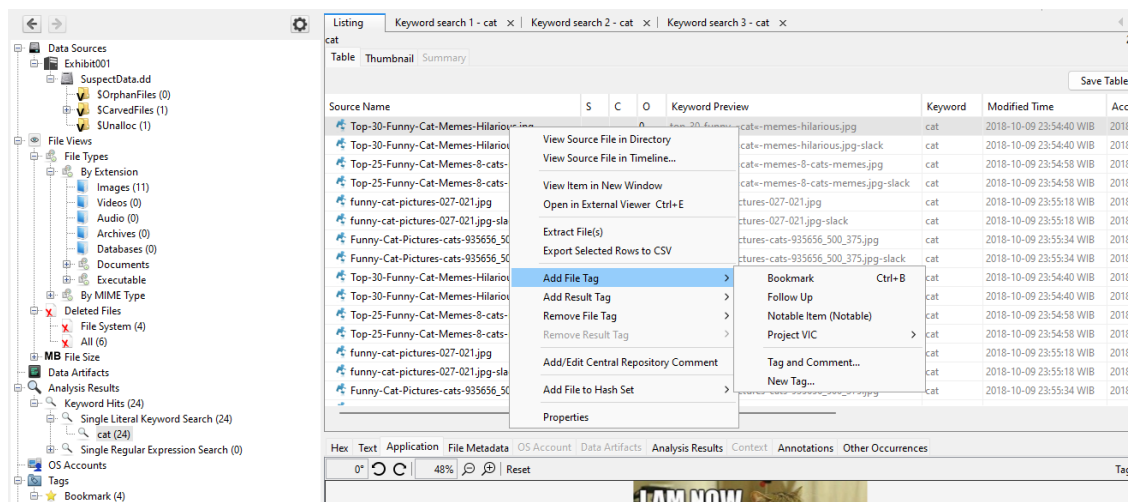
24. Penjelasan mengenai search misal kita ke suspectdata keyword lalu search CAT dia akan memunculkan beberapa pilihan cat.



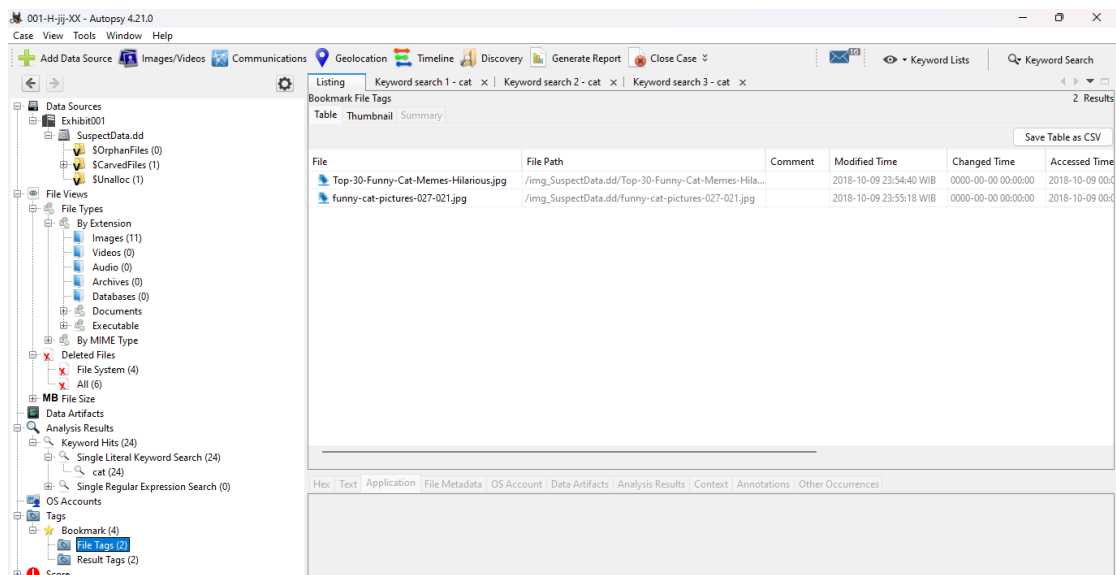
25. Jika sudah kita pilih keyword hits lalu selanjutnya klik single literal keyword search (disitu akan memunculkan kembali apa yang sudah kita search tadi) yang di suspectdata keyword search.



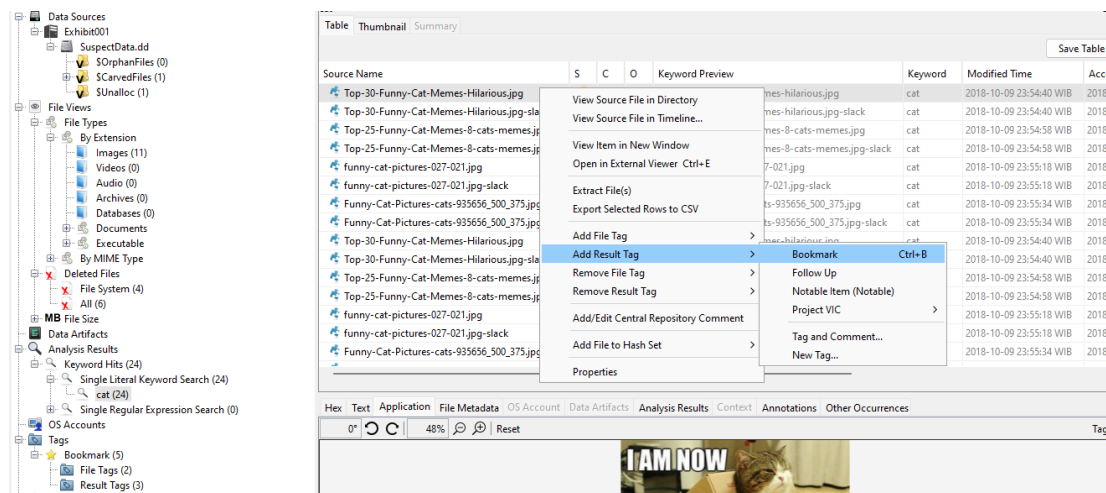
26. Selanjutnya pada keyword search di cat klik kanan klik add file tag yaitu untuk menambahkan tag file lalu klik bookmark.



27. Pilih tags, selanjutnya pilih bookmark, klik file tags disitu akan muncul yang telah kita bookmark tadi.

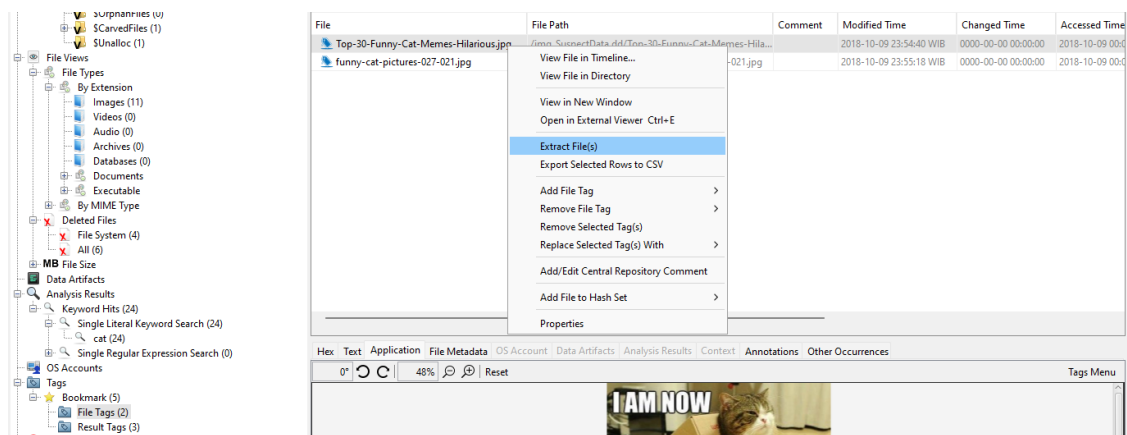


28. Selanjutnya pada keyword search di cat klik kanan klik add result tag yaitu untuk menambahkan tag file lalu klik bookmark.



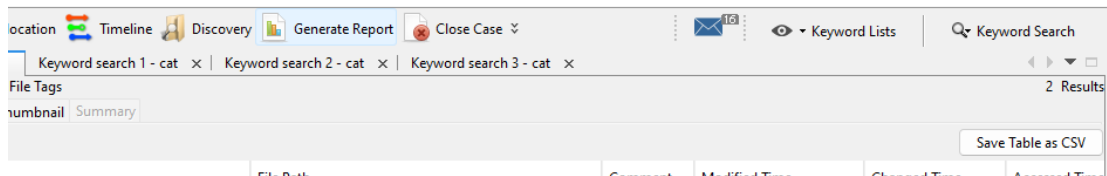
29. Pilih tags, selanjutnya pilih bookmark, klik result tak disitu akan muncul yang telah kita bookmark tadi.

30. Klik kanan pada file gambar yang telah di bookmark lalu pilih extract file.

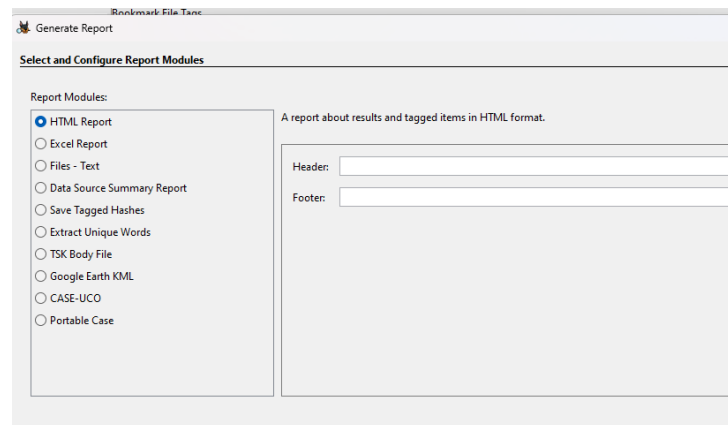


Terserah nanti extract nya mau di tempatkan dimana (kalau saya taruh di folder image) Maka nanti gambarnya akan muncul pada folder image.

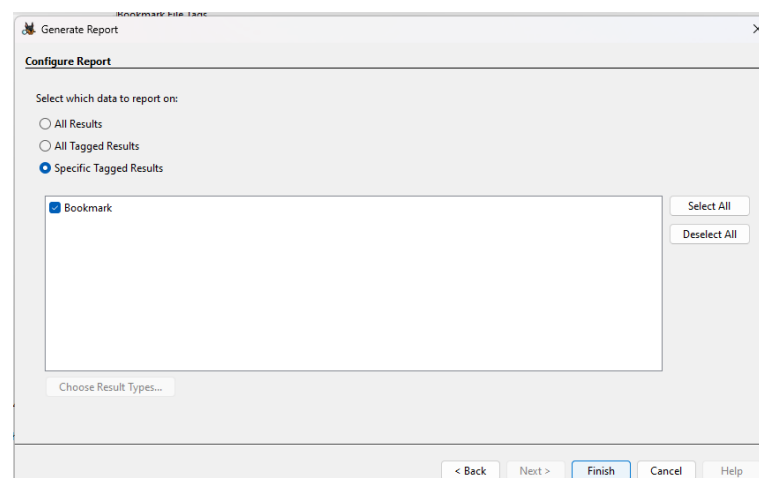
31. Klik generate report untuk membuat laporan dan apa yang dilakukan pada beberapa jenis laporan yang berbeda.



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

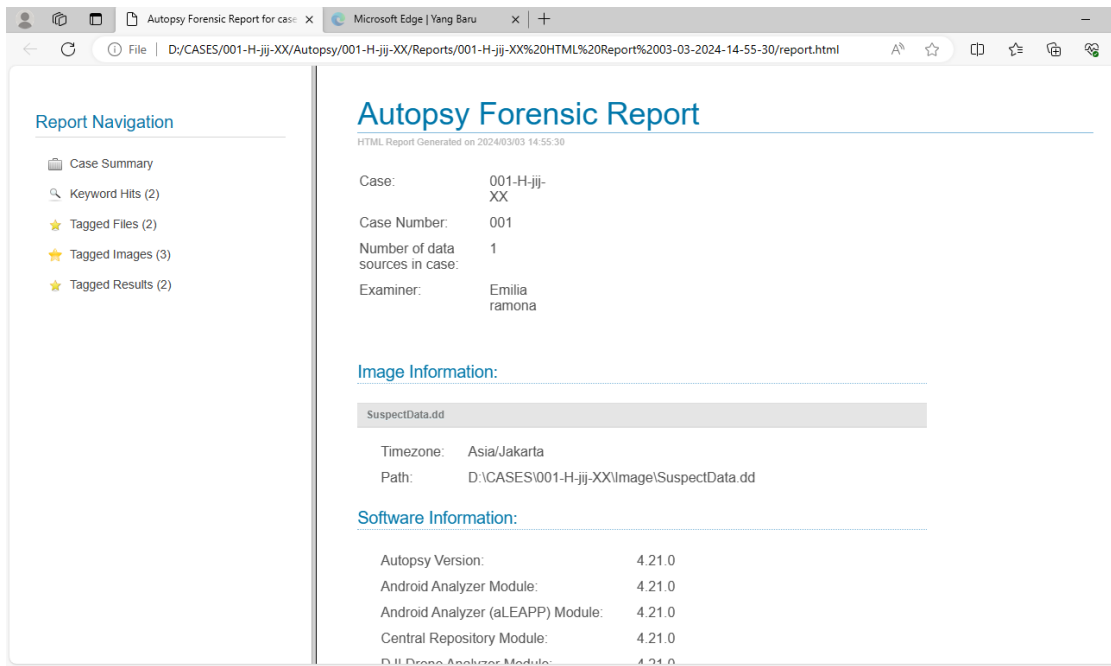


33. Selanjutnya klik spesifik targged result untuk data yang dilaporkan yang dapat melakukan hasil yang diberi tags tertentu selanjutnya akan melakukan hasil yang diberi tags khusus lalu klik centang bookmark dan klik finish untuk mengakhiri.



34. Selanjutnya ada link akan menghasilkan laporan tentang data yang telah di tandai jika tautan di klik maka akan melihat file laporan dan itu memiliki

meta data darimana saya memulai kasus forensik Aoutopsy semua lokasi yang harus sesuai dengan dokumentasi, dan kemudian di sisi kiri saya dapat melihat file yang diberi tags dan kami memiliki bookmart yang merupakan gambar kucing dengan metadatanya dan kemudian item penting juga ditaandai dengan metadatanya jika saya mengklik salah satu tautan itu, maka saya dapat melihat file secara langsung sehingga telah di ekspor dengan laporan kami.



Jadi kesimpulan yang saya dapat setelah melakukan uji coba Autopsy adalah setiap apa yang ingin dilakukan pada aplikasi autopsy contohnya seperti edit,bookmark,tagged image,tagged result dan tagged image dan remove, maka akan masuk ke file folder autopsy yang dibuat awal tadi, di local disk D.

