

LAPORAN TUGAS AUTOPSY PADA MATA KULIAH FORENSIKA DIGITAL



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

Disusun Oleh :

M RAIHAN KANJUL

ADHIM

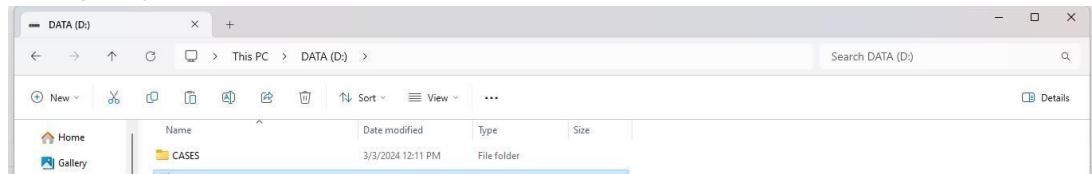
1203210097

IF 01-01

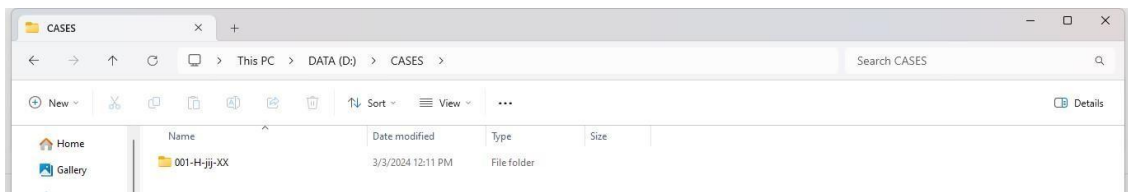
**PROGRAM STUDI INFORMATIKA
FAKULTAS INFORMATIKA TELKOM
UNIVERSITY SURABAYA TAHUN**

AJARAN 2023/2024

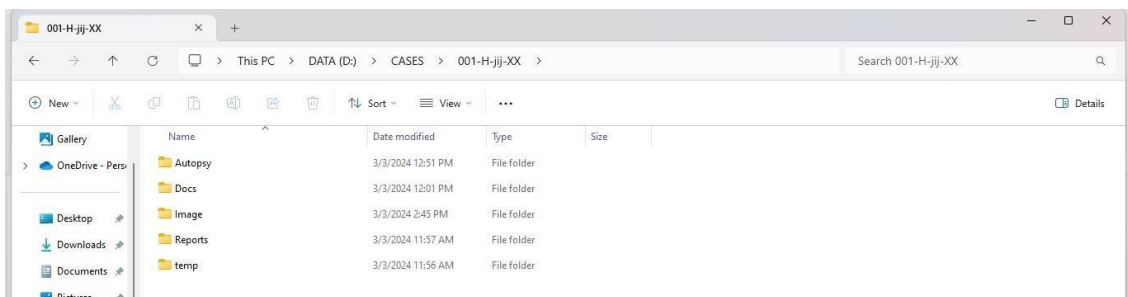
1. Download Autopsy 4.21.0
2. Selanjutnya di local disk D Membuat folder Cases.



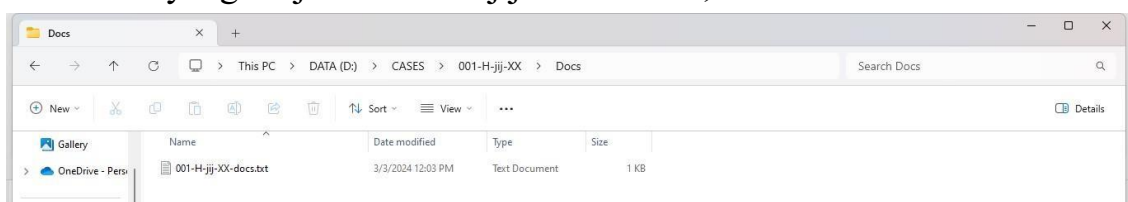
3. Selanjutnya di dalam folder cases, membuat folder dengan nomor kasus 001 dan menambahkan semacam indikator jenis investigasi, dengan cara itu saya bisa melihat kasus saya yang mungkin tidak mengenali nomor kasusnya tetapi saya dapat mengenali tagnya jadi saya akan memberi tanda H, sedangkan jij ini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



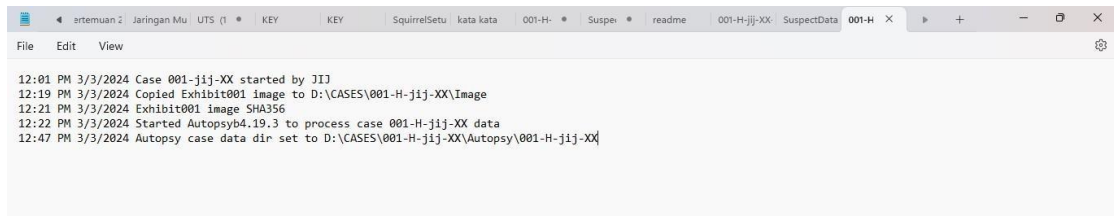
4. Selanjutnya didalam folder 001-H-jij-XX ini akan membuat folder lagi yang terdiri Docs, Image, temp, Autopsy, Reports.



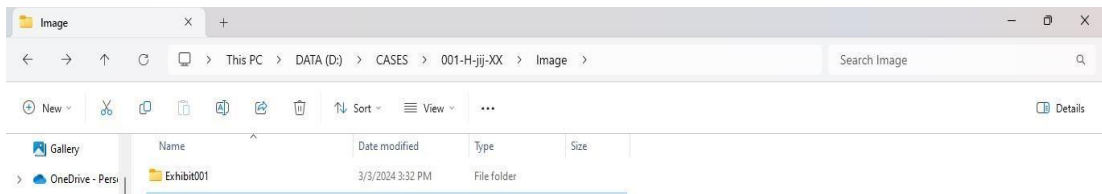
5. Selanjutnya masuk ke dokumen (docs) dan saya akan membuat dokumen teks baru yang berjudul 001-H-jij-XX-doc.txt,



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



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



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



8. Buka aplikasi Autopsy.
9. Pilih opsi new case.
10. Isi nama kasus: 001-H-jij-XX.
11. Isi direktori dasar: D:\CASES\001-H-jij-XX\Autopsy.
12. Pilih mode single user.
13. Klik next.
14. Selanjutnya, isi nomor: 001.
Nama: M Raihan Kanjul Adhim.
Nomor telepon: isi nomor hp.
Email: isi email.
Pilih organisasi yang menganalisis:
Klik selesai.
15. Pilih spesifik nama host baru: Exhibit001, kemudian klik selanjutnya.
16. Klik file gambar disk atau file VM: ini berada di folder gambar (image).
17. Pilih jalur gambar: D:\CASES\001-H-jij-XX\Image\SuspectData.dd.

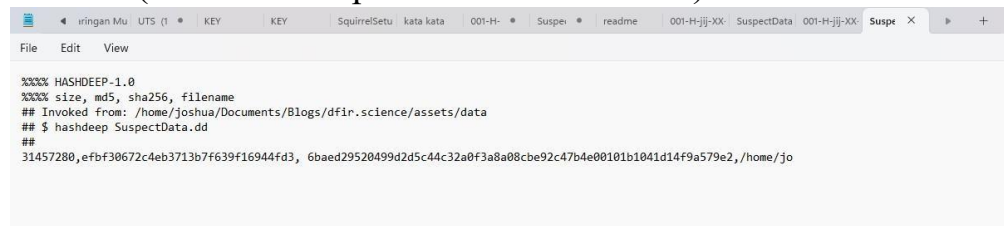
18. Pilih zona waktu sesuai dengan lokasi saat ini, misalnya Asia/Jakarta.

19. Isi nilai hash:

md5: efbf30672c4eb3713b7f639f16944fd3

SHA-256:

6baed29520499d2d5c44c32a0f3a8a08cbe92c47b4e00101b1041d14f9a579e2 (Ini ada di SuspectData.dd-hashes.txt)



```
File Edit View
%% 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
```

20. Selanjutnya klik next

21. Penjelasan singkat tentang 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.

22. Klik identifikasi jenis file 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.

23. Klik selanjutnya.

24. Selanjutnya, di Exhibit001, kita dapat melihat gambar dan data mentah, dimana gambar tersebut dapat kita lihat dalam tampilan hex (ASCII).

25. Klik launch in Hxd untuk menginstall (Harus mendownload Hxd).

26. Penjelasan tentang pencarian, misalnya mencari kata kunci suspectdata lalu mencari CAT yang akan menampilkan beberapa pilihan kucing.

27. Jika sudah, pilih keyword hits, lalu klik single literal keyword search yang ada di pencarian kata kunci suspectdata.

28. Selanjutnya, pada pencarian kata kunci tersebut, klik kanan dan tambahkan tag file untuk menambahkan tag file, lalu klik bookmark.

29. Pilih tag, kemudian pilih bookmark, disitu akan muncul file tag yang telah kita bookmark tadi.
30. Klik kanan pada file gambar yang telah di bookmark, lalu pilih extract file. Terserah nanti ekstraknya mau ditempatkan dimana. Maka nanti gambarnya akan muncul pada folder gambar.
31. Klik generate report untuk membuat laporan tentang apa yang telah dilakukan pada beberapa jenis laporan yang berbeda.
32. Selanjutnya, klik html report, kemudian akan memproses data yang dicurigai (suspect