LAPORAN TUGAS AUTOPSY PADA MATA KULIAH FORENSIKA DIGITAL

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

Disusun Oleh :

Nurul Azizi Hasibuan

1203210090

IF 01-01

PROGRAM STUDI INFORMATIKA

FAKULTAS INFORMATIKA

TELKOM UNIVERSITY SURABAYA

TAHUN AJARAN 2023/2024

1. pada percobaan aplikasi Autopsy digital forensic ini saya menggunakan penyimpanan eksternal (flashdisc) lalu tahap pertamanya adalah membuat folder Cases di dalam folder cases membuat folder dengan nomor kasus 001 dan menambahkan semacam indikator jenis investigasi, agar dapat melihat kasus saya yang mungkin tidak menegenali nomor kasusnya tetapi saya dapat mengenali tagnya jadi saya akan memberi tanda H,sedangkan jij sebagai tag penyelidik dan XX adalah inisialnya aggota penyelidik.
2. pada folder 001-H-jij-XX ini nantinya akan membuat folder lagi yang terdiri dari Docs, Image, temp, Autopsy, dan Reports
3. Selanjutnya masuk kedokumen dan saya akan membuat dokumen teks baru yang berjudul 001-H-jij-XX-doc.txt, selanjutnya membuat dokumentasi kasus yang dibuka di notepad tekan f5 untuk memasukkan waktu saat berjalannya membuat folder. dan sebelum keluar jangan lupa untuk disimpan.
   12:02 03/03/2024 Case 001-H-jij-XX started by JIJ
   12:18 03/03/2024 Copied Exhibit001 Image to E:\CASES\001-H-jij-XX\Images\Exhibit001
   12:20 03/03/2024 Exhibit001 image SHA256 (tidak ada hash dari folder/file)
   12:22 03/03/2024 Started Autopsy 4.19.3 to process case 001-H-jij-XX data
   12:44 03/03/2024 Autopsy case data dir set dir E:\CASES\001-H-jij-XX\Autopsy\001-H-jij-XX
4. 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 terdapat pada link youtube. dan selanjutnya menambahkan data 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
5. Membuka aplikasi autopsy yang telah di install pada windows
6. Pilih new case
7. Isi case name : 001-H-jij-XX sesuai dengan nama folder yang ada pada direktori penyimpanan yang akan dilakukan uji coba
8. Isi base directory : D:\CASES\001-H-jij-XX\Autopsy (alasan menggunakan nomor dan nomor phone agar sistem management ini dapat mengetahui melalui siapa menghubunginya dan kepada yang membaca catatan ini melihat bahwa catatan itu selalu berada di direktotri yang sama.
9. Pilih sigle user
10. Selanjutnya klik next
11. Selanjutnya isi number :001
    name : nama user
    phone : phone user (agar sistem management tau akan menghubungi kesiapa kasus tersebut)
    email : email user
12. organization analysis is being done for : CIA (menambahkan organisasi) setelah menambahkan seperti diatas maka klik finish

13. Pilih specify new host name : Exhibit001 selanjutnya klik next
14. Pilih disk image or VM file : adalah yang berada di folder image sedangkan local disk untuk membaca data secara langsung
15. Selanjutnya pilih path image : KIOXIA(E):\CASES\001-H-jij-XX\Image\SuspectData.dd
16. Pilih time zone wilayah yaitu pada asia/jakarta
17. Isi hash value
    md5 : efbf30672c4eb3713b7f639f16944fd3
    SHA-256 :
    6baed29520499d2d5c44c32a0f3a8a08cbe92c47b4e00101b1041d14f9a579e2
18. jika sudah mengisi hash values seperti diatas lalu next pada apk Autopsy
19. Pencarian pada hash lookup adalah agar dapat mengatur database hash dari file yang diketahui baik dan file buruk yang diketahui, serta dimana file yang diketahui baik kita dpat menggunakan database hash untuk memfilter file yang kita tahu bagus sehingga tidak perlu lagi melihat di autopsy. hash juga dapat menambahkan database hash buruk yang diketahu dimana jika ada file yang cocok dengan hash buruk yang diketahui, maka file tersebut secara otomatis ditandai umtuk kita mininjau sehingga membuat penyelidikan menjadi sangat mudah lalu, klik file type identification yang dapat mengatur jenis file yang ingin dicocokkan dalam pengaturan global, selanjutnya klik next.
20. Pada folder exhibit001 kita dapat melihat gambar dan data mentah dari gambar yang dapat dilihat ditampilan hex (tampilan ascii)
21. Klik launch in Hxd untuk menginstall / dowlod hxd
    Penjelasan mengenai search misal kita ke suspectdata keyword lalu search CAT maka disana akan muncul beberapa pilihan cat. jika sudah kita pilih keyword hits lalu klik single literal keyword serch (disitu akan memunculkan kembali apa yang sudah kita search tadi) di suspectdata keyword search
22. Selanjutnya pada keyword search di cat klik kanan klik add file tag yaitu untuk menambahkan tag file lalu klik bookmark
23. Pilih tags, selanjutnya pilih bookmark, klik file tags disitu akan muncul yang telah kita bookmark tadi
24. Klik kanan pada file gambar yang telah di bookmark lalu pilih ekstract file maka file akan muncul pada penyimpanan image internal dan eksternal
25. Klik generate report untuk membuat laporan dan apa yang dilakukan pada beberapa jenis laporan yang berbeda selanjutnya klik html report kemudian akan memproses data yang dicurigai (suspectdata.dd) 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 dan 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 kami memulai kasus forensik Aoutopsy semua lokasi yang harus sesuai dengan dokumentasi, dan kemudian di sisi kiri kami dapat melihat file yang diberi tags dan kami memiliki bookmart yang merupakan salah satu 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.

kesimpulan yang saya dapat setelah melakukan uji coba Autopsy adalah setiap apa yang ingin dilakukan pada aplikasi autopsy contohnya seperti edit,bookmark,tags an lain sebaigainya, maka akan masuk ke file folder autopsy.