LAPORAN TUGAS AUTOPSY
FORENSIKA DIGITAL

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

Disusun Oleh :

Retna Dwi Efriliani

1203210028

IF 01-02

PROGRAM STUDI INFORMATIKA
FAKULTAS INFORMASI
TELKOM UNIVERSITY SURABAYA
TAHUN AJARAN 2021/2022

- Langkah pertama di local disk D buatlah folder bernama Cases kemudian di dalam folder cases buatlah folder menggunakan nomor kasus 001 dan tambahkan semacam indikator jenis investigasi, dengan cara ini saya dapat melihat kasus saya yang mungkin tidak dapat mengenali nomor kasusnya tapi disini saya dapat mengenali tagnya jadi saya akan memberi tanda H,sedangkan jij ini tentang tag penyelidik dan XX ini merupakan inisialnya aggota penyelidik.
- Kemudian pada folder 001-H-jij-XX disini untuk membuat folder lagi yang berisi Docs, Image, temp, Autopsy, Reports
- Selanjutnya masuk kedokumen dan saya akan membuat dokumen teks baru yang bernama 001-H-jij-XX-doc.txt, selanjutnya membuat dokumentasi kasus yang dibuka di notepad tekan fn dan f5 untuk memasukkan stempel waktu. Dan jangan lupa simpan isi file sebelum keluar.
- membuat file dalam folder image, jadi membuat data yang dicurigai yaitu Exhibit001. Kemudian klik 2 kali pada Exhibit001 kemudian pindahkan data ke direktori (ada pada link youtube). Untuk selanjutnya dapat ditambahkan data SuspectData.dd-hashes.txt.
- selanjutnya bukalah aplikasi autopsy yang sudah di download sebelumnya
- klik dan pilih new case
- berilah nama pada bagian seperti ini, case name : 001-H-jij-XX
- base directory mengisi dengan cara salinlah dari path maka akan seperti ini : D:\CASES\001-H-jij-XX\Autopsy (alasan menggunakan nomor kasus berfungsi untuk siapa pun yang membaca catatan ini, melihat bahwa catatan itu selalu berada pada direktotri yang sama.
- Pilihlah single user
- Kemudian klik next
- Selanjutnya isi number :001
- name : nama
- phone : isi nomor hp (agar sistem management tau yang nantinya akan menghubungi kesiapa kasus tersebut)
- email : isi email
- organization analysis is being done for : CIA (untuk menambahkan organisasi)
- kemudian klik finish
- pilih specify new host name : Exhibit001
- selanjutnya klik next
- selanjutnya klik disk image or VM file :yaitu yang berada di folder image
- sedangkan local disk disini untuk membaca data secara langsung jadi
- kemudian pilih path image : D:\CASES\001-H-jij-XX\Image\SuspectData.dd
- pilihlah time zone wilayah

- isi hash value
- md5 : efbf30672c4eb3713b7f639f16944fd3
- SHA-256 : 6baed29520499d2d5c44c32a0f3a8a08cbe92c47b4e00101b1041d14f9a579e2
- Selanjutnya klik next
- pencarian hash lookup yaitu dimana kita dapat mengatur database hash dari file yang diketahui baik bahkan file buruk yang diketahui n dan serta dimana file yang diketahui baik kita dapat menggunakan data base hash berguna untuk memfilter file yang kita tahu bagus sehingga tidak perlu lagi untuk melihat di autopsy. Hash disini juga dapat menambahkan database hash buruk yang diketahui bahwa dimana jika ada file yang cocok dengan hash

buruk yang diketahui, maka file tersebut akan secara otomatis ditandai untuk kita meninjau sehingga dapat membuat penyelidikan menjadi lebih mudah

- klik file type identification yaitu dapat mengatur jenis file yang ingin dicocokkan dalam pengaturan global
- selanjutnya klik next
- selanjutnya pada exhibit001 kita dapat melihat gambar dan juga data mentah dari gambar yang dapat dilihat ditampilan hex (tampilan ascii)
- klik launch in Hxd untuk menginstall atau downloadd hxd
- penjelasan mengenai search, misalnya kita ke suspectdata keyword kemudian search CAT maka akan memunculkan beberapa pilihan cat. jika sudah terpilih keyword hits lalu klik single literal keyword search (disitu dapat memunculkan kembali apa yang sudah kita search sebelumnya) di suspectdata keyword search
- kemudian pada keyword search di cat klik kanan klik, add file tag fungsinya untuk menambahkan tag file lalu klik bookmark
- pilih tags, selanjutnya pilih bookmark, klik file tags maka disitu akan muncul yang telah kita bookmark tadi
- kemudian klik kanan pada file gambar yang telah di bookmark lalu pilih ekstract file maka file akan muncul di penyimpanan image internal dan eksternal
- klik generate report untuk membuat laporan dan apa yang dilakukan pada beberapa jenis laporan yang berbeda dan selanjutnya klik html report yang 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 selanjutnya klik centang bookmark dan klik finish untuk mengakhiri lalu ada link untuk menghasilkan laporan tentang data yang telah di tandai ,jika tautan tersebut di klik maka akan melihat file laporan dan itu memiliki meta data yang darimana kita memulai kasus forensik Aoutopsy semua lokasi yang harus sesuai dengan dokumentasi, kemudian di sisi kiri kami dapat melihat file yang diberi tags dan kita memiliki bookmar yang merupakan salah satu gambar kucing dengan metadatanya dan selanjutnya item penting juga ditandai dengan metadatanya, jika saya mengklik salah satu tautan itu, maka saya dapat melihat file secara langsung sehingga telah di ekspor dengan laporan kita.

- jadi disini kesimpulan yang saya dapat setelah melakukan uji coba Autopsy yaitu setiap apa yang ingin kita lakukan pada aplikasi autopsy contohnya seperti mengedit,bookmark,tags dan yang lain-lain, maka nantinya akan masuk ke file folder autopsy.