

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



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

**Disusun Oleh :**

**Aisyah Dwi Azahra**

**1203210127**

**IF 01-01**

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

- Di drive lokal D membuat folder CASES lalu di folder CASES membuat folder dengan nomor kasus 001 dan menambahkan semacam indikator jenis investigasi sehingga saya dapat melihat kasus saya yang mungkin tidak mengenali kasus tersebut tetapi saya dapat mengidentifikasi tagnya jadi saya akan memberi tanda H, sedangkan jji mewakili tag penyelidik dan XX ini adalah inisial anggota penyelidik.
- Selanjutnya saya membuat folder lain pada folder 001-H-jji-XX yang terdiri dari dokumen, gambar, temp, otopsi dan laporan.
- Lalu pergi ke dokumen dan saya membuat dokumen teks baru bernama 001-H- jji-XX-doc.txt, kemudian saya akan membuat dokumentasi kasus yang akan terbuka di notepad, tekan f5 untuk memasukkan stempel waktu dan jangan lupa untuk menyimpan sebelum keluar.
- Membuat file di folder gambar dan membuat data mencurigakan bernama Exhibit001. Selanjutnya, klik dua kali Exhibit001 dan memindahkan data ke folder (tersedia dari link YouTube). Lalu menambahkan informasi ke SuspectData.dd-hashes.txt.
- Selanjutnya membuka aplikasi autopsy.
- Lalu memilih kasus baru.
- Memasukkan nama kasus : 001-H-jji-XX
- Mengisi folder root : D:\CASES\001-H-jji-XX\Autopsy (alasan menggunakan nomor kasus adalah agar siapapun yang membaca catatan ini akan melihat bahwa catatan tersebut selalu berada di folder yang sama.
- Pilih Single User.
- Lalu klik Berikutnya.
- Lalu memasukkan nomor : 001 Name : nama  
Telepon : memasukkan nomor ponsel (agar sistem kontrol mengetahui siapa yang harus dihubungi)  
Email: isi email  
Organization analysis is being done for : untuk CIA (menambahkan organisasi), kemudian mengklik tombol selesai.
- Memilih specify new host name : Exhibit001 lalu klik Berikutnya.
- Mengklik disk image or VM file : terletak di folder gambar sedangkan itu ada di disk lokal untuk membaca data secara langsung, jadi
- Selanjutnya pilih path gambar : D:\CASES\001-H-jji-XX\Image\SuspectData.dd.
- Memilih zona waktu wilayah Asia/Jakarta.
- Mengisi Hash Value.  
md5 : efbf30672c4eb3713b7f639f16944fd3  
SHA-256 :  
6baed29520499d2d5c44c32a0f3a8a08cbe9247b4e00101b1041d14f9a579e2
- File yang bagus dapat dicari dan diketahui jika kita tahu dapat menggunakan file yang bagus dan jika kita tahu kita dapat menggunakan file yang bagus file yang bagus. Hash database untuk memfilter file-file yang kita tahu bagus, sehingga

kita tidak perlu lagi melihat-lihat di autopsy. Hash juga dapat ditambahkan ke database hash buruk yang diketahui, di mana jika ditemukan file yang cocok dengan hash buruk yang diketahui, file tersebut secara otomatis ditandai untuk kami periksa, membuat penelitian lebih mudah.

Kemudian mengklik pada jenis file deteksi yang dapat menentukan jenis file yang akan dipasang di pengaturan umum.

- Lalu klik Berikutnya.
- Selanjutnya kita melihat gambar dan data mentah dari gambar tersebut ditampilkan pada layar heksadesimal (layar ascii) pada pameran 001.
- Mengklik Mulai di Hxd untuk menginstall/mengunduh hxd. Mencari penjelasannya, misalnya kita masuk ke kata kunci tersangka data dan mencari CAT maka akan memunculkan beberapa kemungkinan warna. Setelah kita memilih kata kunci yang cocok, klik salah satu keywords hits pada pencarian kata kunci data yang mencurigakan (di sini akan mengembalikan apa yang kita cari sebelumnya).
- Lalu, klik kanan istilah pencarian, klik Tambahkan Ekstensi File, yaitu menambahkan ekstensi file, lalu klik Bookmark.
- Memilih tag, lalu pilih bookmark, klik file tag disana, maka akan muncul yang kita tandai sebelumnya. Klik kanan file gambar yang di-bookmark, lalu pilih ekstrak file, dan file akan muncul di penyimpanan gambar internal dan eksternal.
- Mengklik tombol Buat Laporan untuk membuat laporan dan menjalankan beberapa jenis laporan berbeda. Kemudian klik pada html laporan dan akan memproses data yang dicurigai (suspectdata.dd) dan kemudian klik pada hasil target dari data yang dilaporkan yang dapat memberikan hasil yang spesifik. tag, itu akan menambahkan tag khusus ke hasil, lalu klik Periksa bookmark dan klik untuk menyelesaikan. Lalu ada link yang menghasilkan laporan tentang data yang diberi tag. Jika Anda mengklik tautan itu, Anda akan melihat file laporan dan memiliki metadata yang kami gunakan untuk memulai kasus forensik otopsi untuk semua lokasi yang harus cocok dengan dokumentasi, dan kemudian di sisi kiri kami melihat file yang diberi tag dan kami memiliki bookmark yang merupakan salah satu gambar kucing. metadata dan kemudian item penting juga ditandai dengan metadata tersebut. Ketika saya mengklik salah satu tautan ini, saya dapat melihat file secara langsung, sehingga file tersebut diekspor bersama laporannya.

Kesimpulan : Jadi setelah menguji aplikasi autopsy saya menyimpulkan bahwa semua yang ingin kita lakukan dalam aplikasi autopsy seperti pengeditan, bookmark, tag dan sejenisnya masuk ke file di folder autopsy.