

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



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

Disusun Oleh :

Tifanni Diva Auliya

1203210027

IF 01-02

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

- Membuat folder dengan nama "CASES" pada local disk D. Di dalamnya, saya membuat folder kasus 001 dan tambahan tanda khusus untuk membedakan jenis penyelidikan. Jadi, meskipun ada kasus yang tidak jelas, tetapi masih diketahui kasusnya dari tanda yang sudah ditetapkan. Misalnya, diberi tanda "H" untuk jenis penyelidikan tertentu, "jij" untuk penanda penyelidik, dan "XX" untuk inisial anggota tim. Selanjutnya saya membuat folder lain pada folder 001-H-jij-XX yang terdiri dari dokumen, gambar, temp, otopsi dan laporan.
- Kemudian, saya menuju ke dokumen dan buat dokumen teks baru dengan nama 001-H-jij-XX-doc.txt. Selanjutnya, saya mulai membuat dokumentasi kasus yang akan terbuka di Notepad. Saya tekan tombol F5 untuk menambahkan stempel waktu, dan pastikan untuk menyimpan sebelum keluar.
- Membuat sebuah file di dalam folder gambar dan beri nama Exhibit001 untuk menampung data mencurigakan. Setelah itu, saya klik dua kali Exhibit001 dan transfer data ke folder yang sudah disediakan melalui link YouTube. Setelah pemindahan selesai, saya tambahkan informasi ke dalam SuspectData.dd-hashes.txt. Langkah berikutnya, saya buka aplikasi autopsy dan pilih opsi untuk membuat kasus baru.
- Memasukkan nama kasus sebagai "001-H-jij-XX" dan mengatur folder root di lokasi "D:\CASES\001-H-jij-XX\Autopsy". Selanjutnya, memilih opsi Single User.
- Kemudian, saya klik tombol Berikutnya dan memasukkan nomor "001" dengan informasi nama, nomor telepon, dan alamat email yang relevan, agar sistem kontrol dapat mengetahui kontak yang harus dihubungi. Selanjutnya, mengisi bagian "Organization analysis is being done for" dengan CIA, menambahkan informasi organisasi, dan terakhir, menyelesaikan proses dengan mengklik tombol selesai.
- Menentukan host name baru sebagai "Exhibit001" dan melanjutkan dengan mengklik tombol Berikutnya. Setelah itu, memilih opsi "disk image or VM file" yang berada di folder gambar di disk lokal untuk membaca data secara langsung. Kemudian, menentukan path gambar sebagai "D:\CASES\001-H-jij-XX\Image\SuspectData.dd." Selanjutnya, memilih zona waktu wilayah Asia/Jakarta.
- Mengisi Hash Value.
md5 : efbf30672c4eb3713b7f639f16944fd3
SHA-256 :
6baed29520499d2d5c44c32a0f3a8a08cbe9247b4e00101b1041d14f9a579e2
- Menggunakan file hash dapat mempermudah identifikasi dan filtrasi file yang telah diketahui baik atau buruk dalam database hash. Hal ini meminimalkan kebutuhan untuk secara manual menelusuri file di autopsy. Jenis file deteksi dapat diatur dalam pengaturan umum untuk memudahkan proses penelitian. Selanjutnya, klik tombol berikutnya.
- Kemudian, kita melihat gambar dan data mentah dari gambar tersebut ditampilkan dalam layar heksadesimal (layar ASCII) pada Exhibit001. Selanjutnya, saya klik "Mulai" di Hxd untuk menginstal atau mengunduh Hxd. Saat mencari penjelasan, contohnya dengan memasukkan kata kunci "tersangka data" dan mencari "CAT", akan muncul beberapa kemungkinan warna. Setelah memilih kata kunci yang sesuai, klik salah satu hasil pencarian kata kunci yang mencurigakan untuk melihat apa yang telah dicari 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.

- Klik tombol "Buat Laporan" untuk membuat dan menjalankan beberapa jenis laporan yang berbeda. Setelah itu, saya pilih laporan HTML untuk memproses data mencurigai (SuspectData.dd). Klik pada hasil target dari data yang dilaporkan untuk mendapatkan hasil yang spesifik dengan menambahkan tag khusus.
- Selanjutnya, klik "Periksa bookmark" dan selesaikan. Terdapat link yang menghasilkan laporan tentang data yang diberi tag, memungkinkan melihat metadata yang digunakan untuk memulai kasus forensik otopsi. Pada sisi kiri, file yang diberi tag terlihat dengan bookmark yang berupa gambar kucing dan item penting lainnya ditandai dengan metadata tersebut. Saat mengklik tautan ini, saya dapat melihat file secara langsung, sehingga file tersebut diekspor bersama laporannya.

Kesimpulan : Dalam proses investigasi forensik, saya membuat dan mengorganisir struktur folder, menciptakan dokumen kasus, dan menyimpan data mencurigakan. Penggunaan aplikasi Autopsy, database hash, dan Hxd memfasilitasi analisis dan ekstraksi informasi dari file. Hasilnya, saya berhasil menghasilkan laporan terstruktur dengan tag khusus, memudahkan identifikasi dan dokumentasi kasus forensik secara efisien.