DIGITAL FORENSIC DAN IMAGING PADA MEDIA PENYIMPANAN EKSTERNAL UNTUK MENJAMIN KEASLIAN FILE SETELAH RECOVERY MENGGUNAKAN METODE STATIC FORENSIC

SKRIPSI

Diajukan Oleh :

ANDRIE FADHLULLAH WAHBY

NIM. 170212026

Bidang Peminatan : Teknik Komputer dan Jaringan

Mahasiswa Fakultas Tarbiyah dan Keguruan

Program Studi Pendidikan Teknologi Informasi

UNIVERSITAS ISLAM NEGERI AR-RANIRY

FAKULTAS TARBIYAH DAN KEGURUAN

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI

2023 M/1445 H

SKRIPSI

DIGITAL FORENSIC DAN IMAGING PADA MEDIA PENYIMPANAN EKSTERNAL UNTUK MENJAMIN KEASLIAN FILE SETELAH RECOVERY MENGGUNAKAN METODE STATIC FORENSIC

Oleh:

ANDRIE FADHLULLAH WAHBY

NIM. 170212026

Bidang Peminatan : Teknik Komputer dan Jaringan
Mahasiswa Fakultas Tarbiyah dan Keguruan
Program Studi Pendidikan Teknologi Informasi

Disetujui Oleh:

Pembimbing 1	Pembimbing 2
Ridwan, M.T	Firmansyah, S.Kom., M.T
NIP. 198402242019031004	NIP. 198704212015031002

DIGITAL FORENSIC DAN IMAGING PADA MEDIA PENYIMPANAN EKSTERNAL UNTUK MENJAMIN KEASLIAN FILE SETELAH RECOVERY MENGGUNAKAN METODE STATIC FORENSIC

SKRIPSI

Telah diuji oleh Panitia Ujian Munaqasyah Skripsi Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus serta diterima sebagai salah satu beban studi Program Sarjana (S-1) dalam Pendidikan Teknologi Informasi

Pada :

Rabu, 26 Agustus 2023
08 Muharram 1445 H

Darussalam – Banda Aceh
Panitia Ujian Munaqasyah Skripsi

Ketua	Sekretaris
Ridwan, M.T	Firmansyah, S.Kom., M.T
NIP. 198402242019031004	NIP. 198704212015031002
Penguji 1	**Penguji 2**
Sarmi Vita Dewi, S.T., M.Eng	Nazaruddin Ahmad, M.T
NIP. 197312222022032001	NIP. 198206052014031002

Mengetahui,
Dekan Fakultas Tarbiyah Dan Keguruan UIN Ar-Raniry
Darussalam, Banda Aceh

Prof. Safrul Muluk, S.Ag., M.A., M.Ed., P.Hd
NIP. 197301021997031003

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan dibawah ini:

Nama : Andrie Fadhlullah Wahby
NIM : 170212026
Program Studi : Pendidikan Teknologi Informasi
Fakultas : Tarbiyah dan Keguruan
Judul Skripsi : DIGITAL FORENSIC DAN IMAGING PADA MEDIA PENYIMPANAN EKSTERNAL UNTUK MENJAMIN KEASLIAN FILE SETELAH RECOVERY MENGGUNAKAN METODE STATIC FORENSIC

Dengan ini menyatakan bahwa dalam penulisan Skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggung jawabkan.
2. Tidak melakukan plagiat terhadap Naskah karya orang lain
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya
4. Tidak memanipulasi dan memalsukan data
5. Mengerjakan sendiri karya ini dan mampu bertanggung jawab atas karya ini

Bila di kemudian hari ada tuntutan dari pihak lain atas karya saya dan telah melalui pembuktian yang dapat dipertanggung jawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh

Demikian Pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh, 26 Agustus 2023
Yang Menyatakan

Andrie Fadhlullah Wahby

ABSTRAK

Nama : Andrie Fadhlullah Wahby
NIM : 170212026
Fakultas/Prodi : Tarbiyah dan Keguruan/Pendidikan Teknologi Informasi

Judul : Digital Forensic dan Imaging pada Media Penyimpanan Eksternal untuk Menjamin Keaslian File Setelah Recovery Menggunakan Metode Static Forensic
Bidang Peminatan : Teknik Komputer Jaringan (TKJ)
Pembimbing I : Ridwan, M.T
Pembimbing II : Firmansyah, S.Kom, M.T

Kata Kunci : Autopsy, Digital Forensic, FTK Imager, Hardisk, USB Flash Drive

Kehilangan data merupakan kejadian yang sering terjadi baik secara disengaja ataupun tidak disengaja, hilangnya data yang yang penting disaat yang tidak terduga, atau sengaja menghilangkan data untuk menutup-nutupi sesuatu sehingga data tersebut tidak dapat diakses karena terhapus atau dihapus. Umumnya ketika data yang kita miliki tidak sengaja terhapus, biasanya karena perangkat pentimpanannya yang bermasalah dan tindakan yang tidak disengaja untuk menghapus data. Dalam penelitian ini, peneliti melakukan simulasi kasus pada 3 (tiga) jenis *USB flash drive* dengan kapasitas yang berbeda, dan 1 hardisk. Metode yang digunakan adalah metode *static forensic*, dan juga dua aplikasi yaitu Autopsy dan juga FTK Imager karena sesuai dengan studi kasus yang telah disekenariokan yaitu *post incident case* dimana pengembalian data dilakukan setelah penghapusan data terjadi dengan cara mengekstrak hasil dari file-file yang telah dihapus menjadi metadata kemudian mengekspor metada data tersebut menjadi file yang sama seperti file sebelum dihapus. Pengembalian data dilaukan dengan men-imaging terlebih dahulu perangkat penyimpanan yang ingin di analisis, untuk menjaga keaslian file, lalu setelahnya barulah hasil dari Imaging tersebut diubah menjadi metadata dengan aplikasi Autopsy kemudian baru bisa diekstrak menjadi file yang disa dibaca. Berdasarkan dari hasil bukti digital yang telah dianalisis dengan menggunakan bantuan FTK Imager dan aplikasi Autopsy pada tiga USB yang berbeda dan satu hard disk, di dapatkan hasil yang berupa file-file yang telah terhapus dengan masing-masing waktu untuk imaging dan conversi datanya pada device 1 sebesar kurang lebih 49 menit dengan bukti sebanyak 12 file. Untuk device 2 didapatkan hasil waktu imaging kurang lebih 57 menit dengan bukti sebanyak 15 file. Sedangkan pada device 3 di dapatkan hasil waktu imaging 273 menit dengan bukti sebanyak 35 file, dan pada device ke-4 didapatkan hasil kurang lebih dalam waktu 840 menit dengan 170 file.

KATA PENGANTAR

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

Segala puji beserta syukur kita ucapkan atas kehadirat Allah SWT. dengan segala rahmat dan hidayah-Nya sehingga kita dapat meraskaan nikmatnya Iman dan Islam dalam kehidupan saat ini, tak lupa pula shalawat beriring salam kepada Baginda Rasulullah Muhammad SAW yang menjadi penerang dalam kehidupan, menjadi purnama yang hangat ditengah sejuknya malam, dan menjadi suri tauladan sebagai sebaik-baik tauladan bagi umat manusia, sehingga penulis dapat menyelesaikan Skripsi yang berjudul **"Digital Forensic dan Imaging pada Media Penyimpanan Eksternal untuk Menjamin Keaslian File Setelah Recovery Menggunakan Metode Static Forensic"** dengan sebaik-baiknya.

Penulisan skripsi ini merupakan salah satu syarat penting yang harus diselesaikan untuk mendapatkan gelar sarjana oleh setiap mahasiswa Program Studi Pendidikan Teknologi Informasi Fakultas Tarbiyah dan Keguruan Universitas Islam Negeri Ar-Raniry Banda Aceh. Dengan segala upaya yang telah dilakukan dalam menyelesaikan skripsi ini, penulis juga menyadari sepenuhnya bahwa masih terdapat beberapa kekurangan baik dari hal penyusunan dan aspek lainnya. Dalam proses penulisan skripsi ini, tentunya terdapat banyak kesulitan dan tantangan yang dihadapi, baik dari segi penulisan, ekstraksi file, penyusunan data dan proses analisis data yang memakan waktu lama. Berkaitan hal tersebut,

proses penulisan skripsi ini juga adanya dukungan dan bantuan dari dari berbagai pihak.

Berkenaan dengan hal tersebut, maka penulis menyampaikan ucapan terima kasih kepada:

1. Kedua orang tua beserta keluarga yang selalu memberikan dukungan serta senantiasa mendoakan yang terbaik.
2. Rektor UIN Ar-Raniry Banda Aceh, Bapak Prof. Dr. Mujiburrahman, M.Ag.
3. Dekan Fakultas Tarbiyah dan Keguruan Universitas Islam Negeri Ar-Raniry Banda Aceh, Bapak Safrul Muluk, S.Ag., M.A., M.Ed., PhD.
4. Ketua Program Studi Pendidikan Teknologi Informasi Ibu Mira Maisura, M.Sc.
5. Sekretaris Program Studi Pendidikan Teknologi Informasi Bapak Ridwan, M.T.
6. Pembimbing 1 yaitu Bapak Ridwan, M.T dan juga Pembimbing 2 yaitu Bapak Firmansyah, S.Kom., yang telah meluangkan waktu dan memberikan saran serta motivasinya dan membimbing penulis dalam menyelesaikan penulisan skripsi ini.
7. Penguji 1 Ibu Sarini Vita Dewi, S.T., M.Eng., serta Penguji 2 Bapak Nazaruddin Ahmad, M.T., yang telah memberikan banyak masukan dan saran demi tercapainya kesempurnaan skripsi ini.

8. Staf Program Studi Pendidikan Teknologi Informasi yang telah membantu proses pelaksanaan penelitian untuk penulisan skripsi ini.
9. Dan semua pihak, secara langsung maupun tidak langsung, yang tidak dapat disebutkan di sini. Atas bantuan dan perhatiannya selama penyusunan Skripsi ini.

Berbagai upaya yang telah dilakukan dalam menyelesaikan skripsi ini, penulis menyadari sepenuhnya dalam penulisan skripsi ini masih banyak terdapat kekurangan baik dalam penulisan maupun isi.

Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun agar dapat dijadikan masukan dan referensi untuk perbaikan skripsi lanjutan di masa berikutnya. Semoga Allah SWT meridhai segala penulisan skripsi ini dan dapat bermanfaat bagi kita semua. Aamiin

Banda Aceh, 26 Agustus 2023

Penulis,

Andrie Fadhlullah Wahby

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi yang meningkat pesat dapat memberikan dampak yang besar tergantung dari pengguna teknologi tersebut. Salah satu yang sering terjadi di sekitar kita diantaranya kehilangan data, baik disengaja ataupun tidak. Sehingga data-data penting tersebut harus dikembalikan atau di-*recovery*. Kehilangan data merupakan kejadian hilangnya data sehingga berakibat fatal apabila data yang hilang itu penting sehinga tidak dapat diakses karena terhapus atau dihapus. Umumnya ketika data yang kita miliki tidak sengaja terhapus, biasanya misalnya pada perangkat penyimpan data eksternal seperti *USB flash drive* atau hardisk karena tindakan yang disengaja untuk menghapus data ataupun tidak disengaja[1]. Penggunaan *USB flash drive* ataupu hardisk sebagai media transfer data sangat mendunia, dan merupakan hal yang lumrah di zaman sekarang, namun penggunaan *USB flash drive* dan hardisk dapat juga disalah gunakan untuk kejahatan, seperti transaksi informasi pribadi yang bersifat privasi, pornografi, transaksi illegal, penipuan dan sebagainya. Menghapus data di dalam *USB flash drive* ataupu hardisk secara permanen membuat data tidak dapat diakses kembali oleh pengguna, sehingga diperlukan *recovery* untuk pemulihan data yang dilakukan untuk mengembalikan data dengan bantuan aplikasi forensik. Disini

Peneliti berperan untuk melakukan forensik digital pada perangkat penyimpanan dan melakukan pengembalian data-data yang telah dihapus secara permanen.

Penghapusan data-data penting secara tidak sengaja menyebabkan permasalahan yang serius, apalagi jika data tersebut terhapus secara permanen artinya data tersebut tidak dapat ditemukan didalam *recycle bin* yang merupakan tempat atau brangkas penampungan file-fle yang telah kita hapus. Sehingga proses pengembalian data-daa penting ini memerlukan bantuan dari aplikasi pihak ke-3, salah satu yang paling umum digunakan ialah Autopsy. Dalam dunia digital forensic, keaslian data dari file sangat krusial dan rentan rusak, oleh karena itu, peneliti juga menggunakan FTK Imager dari Access Data untuk menjamin keaslian data [2]. Kedua apliksi ini sering digunakan untuk mendukung proses *digital forensic* dalam kasus-kasus pemalsuan data. Di dalam dunia digital forensic khususnya yang berkecimpung di dunia *cyber crime* dalam kasus penipuan, pengajuan untuk bukti elektronik dapat diterima untuk menjadi barang bukti yang dapat digunakan sebagai acuan oleh penyidik untuk menjerat pelaku kejahatan *cyber* dengan hukum yang berlaku setelah tim forensik menganalisis data dari barang bukti tersebut[3].

Salah satu cara untuk mengembalikan data yang secara permanen telah terhapus tersebut, maka dapat menggunakan aplikasi *Autopsy* sebagai tools untuk menganalisis data kemudian mengekstraknya menjadi file yang bisa dibaca, tetapi karena sifat dari data yang rentan rusak sehingga keaslian filenya juga terancam,

maka sebelum menganalisis data dari perangkat yang akan digunakan, para forensika menggunakan aplikasi *FTK Imager from Access Data* sebagai alat bantu untuk enjaga keaslian file tersebut dengan melakukan imaging pada peragkatyang akan dilakukan proses forensik. *Digital forensic* memeiliki tujuan untuk membantu menemukan dan menganalisis fakta-fakta berupa data, serta menganalisa bukti digital yang berkaitan tentang suatu insiden sebagaimana yang juga telah diuraikan pada jurnal yang berjudul *Static Forensic pada USB Mass Storage menggunakan Forensic Imager* oleh Pradipta Mahardika Sulaksosno, dan Bayu Santoso[4]. Oleh karena itu, setelah mengamati bagaimana pentingnya mengembalikan data-data penting yang hilang secara permanen bagi seseorang, maka peneliti berinisiatif melakukan penelitian dengan judul "Digital Forensic Pada Media Penyimpanan Eksternal Dengan Cara Imaging Untuk Menjamin Keaslian File Menggunakan Metode Static Forensic".

1.2 Rumusan Masalah

Berdasarkan latar belakang dan hubungannya dengan pemilihan judul tersebut, maka penulis merumuskan pokok permasalahan diantaranya sebagai berikut:

a. Bagaimana cara menemukan file digital yang telah dihapus baik secara disengaja atau tidak?
b. Bagaimana cara menjaga keaslian file yang telah dihapus sehingga format file tetap terjamin keasliannya?

1.3 Batasan Masalah

Dalam pembuatan proposal skripsi ini, penulis membatasi masalah yang akan dianalisis yaitu:

a. Menjelaskan Tahapan-tahapan mulai dari imaging hingga mengekstrak data kedalam bentuk file.
b. Analisis yang dilakukan hanya sebatas imaging dan pengembalian data yang hilang.

1.4 Tujuan Penelitian

a. Untuk mengimplementasikan metode static forensic dalam recovery data.
b. Untuk menemukan File yang terhapus baik secara sebgaja ataupun tidak disengaja.

1.5 Manfaat Penelitian

a. Manfaat Teoritis :

   Memberikan literasi dan panduan tambahan tentang bagaimana tahapan-tahapan dalam pengembalian data atau *recovery* dengan proses imaging terlebih dahulu.

b. Manfaat Praktis

   Memberikan panduan dalam men-image data sebagai jaminan untuk keaslian data yang akan di *recovery* dan memberikan panduan dalam proses *recovery* menggunakan Autopsy.

1.6 Penelitian Terdahulu

Table 1: Jurnal-jurnal yang membahas tentang digital forensic

No.	Penelti/ Tahun	Judul	Metode Penelitian	Kelemahan
1.	Syifa Rizki Ardiningtias, dkk./2021	Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National	Penyelidikan dalam penelitian nimenggunakan metode*National Institute of Justice* (NIJ) yang menyediakan beberapa tahap*dentification, preservation, collection, examination,*	Hanya menampilkan perbandingan hasil kerja dari dua aplikasi yang berbeda, sehingga tidak berfokus pada file yang dikembalikan.

		Institute of Justice.”	*analysis*, dan *p resentation.*	
2.	Wisnu Ari Mukti/ 2018	Analisa dan Perbandinga n Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android”.	Menggunakan metode simulasi dengan menjalankan 11 skenario diantaranya adalah pengembalian file yang dihapus, pencarian bukti forensik berupa nama akun, lokasi, nomor telpon, tanggal lahir, photo profile, cover	Hanya mencari data dari file forensik pada aplikasi yang diteliti, dan tidak mengekstrak file dari data yang didapatkan.

			photo, posting berupa teks, posting berupa gambar, isi private message berupa teks dan isi private message berupa gambar.	
3.	Gusra Mishardila /2020	Analisa Bukti Forensik Digital pada Apliksi Media Sosial facebook dan Twitter Menggunak	Menggunakan metode studi kasus pada memori eksternal yang digunakan, dan pengumpulan data dilakukan dengan cara deskriptif.	Tidak menjelaskan kerangka kerja yang digunakan dalam melakukan pengolahan data menggunakan metode static forensic dan juga tidak ada penjelasan tentang tahap pengerjaannya, dan tidak ada penjelasan mengenai metode yang digunakan.

		an Metode Static Forensic		
4.	Muhammad Fajar Sidiq, , Muhammad Nur Faiz/ 2019	Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital.	Menggunakan metode studi kasus terhadap web yang diserang oleh cybercrime.	Hanya sebatas mereview saja, tidak mengekstrak dan mengembalikan file yang telah hilang

1.7 Sistematika Penulisan

Bab 1 : Pendahuluan

Bab ini menjelaskan tentang dasar-dasar masalah serta gambaran umum mengenai perancangan penelitian ini.

Bab 2 : Landasan Teoretis

Bab ini menjelaskan tentang berbagai landasan teori yang digunakan untuk mendukung penelitian ini, serta juga menjadi referensi toritis dalam menjalan penelitian.

Bab 3 : Metodologi Penelitian

Bab ini menjelaskan tentang tahapan-tahapan yang digunakan dalam penelitian ini.

Bab 4 : Hasil dan Pembahasan

Bab ini menjelaskan tentang proses dan hasil dari penelitian yang dilakukan.

Bab 5 : Penutup

Bab ini menjelaskan tentang kesimpulan yang dapat diambil dari proses penelitian.

BAB II

LANDASAN TEORI

2.1 Digital Forensic

Kata forensik berasal dari bahasa Yunani yaitu *forensis* yang memilki arti debat atau perdebatan. Sedangkan menurut istilah kata forensik memiliki makna salah satu bidang ilmu pengetahuan yang digunakan untuk membantu menegakkan proses keadilan melalui proses penerapan ilmu atau sains[5].

Digital forensik adalah salah satu cabang ilmu forensik terutama untuk penyelidikan dan penemuan konten perangkat digital dan seringkali dikaitkan dengan kejahatan komputer. Istilah forensik digital pada awalnya identik dengan forensik komputer tetapi kini telah diperluas untuk menyelidiki semua perangkat yang dapat menyimpan data digital. Forensik digital diperlukan karena biasanya data diperangkat target dikunci, dihapus dan disembunyikan.

Landasan forensik digital adalah praktik pengumpulan, analisis dan pelaporan data digital. Investigasi forensik digital memiliki penerapan yang sangat beragam. Penggunaan paling umum adalah untuk mendukung atau menyanggah asumsi kriminal dalam pengadilan pidana atau perdata. Penguasaan ilmu forensik digital tidak hanya menuntut kemampuan teknis saja tetapi juga terkait dengan bidang lain seperti bidang hukum. Proses forensik umumnya meliputi penyitaan, *forensik imaging* (akuisisi) dan analisis media digital dan penyusunan laporan berdasarkan bukti yang dikumpulkan.

2.2 Static Forensic

Static Forensic yaitu salah satu jenis metode dari forensik digital yang memperoleh bukti digital dengan melakukan ekstraksi serta analisis setelah insiden terjadi ataupun setelah sistem komputer dimatikan *(post incident).* Sedangkan menurut Mamoona, *static forensic* merupakan pendekatan secara tradisional untuk melakukan proses forensik setelah diperolehnya *dump memory* pada sistem yang telah dimatikan sebelumnya. Metode ini digunakan untuk menganalisa *external device* berbasis penyimpanan seperti *USB Flash Drive*[4].

2.3 Framework NIST

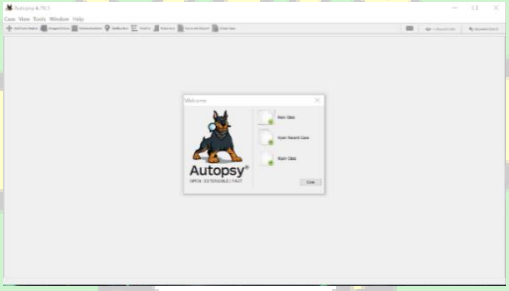
Framework NIST merupakan framework yang diciptakan serta dikembangkan oleh lembagaNational Institute of Standards and Technology yang digunakan untuk proses pengambilan serta pengolahan bukti digital[6]. Framework NIST terdiri dari empat tahapan yaitu *Collection, Examination, Analysis, dan Report.*

a. *Collection/Storage* (Pengumpulan/penyimpanan Bukti Digital)

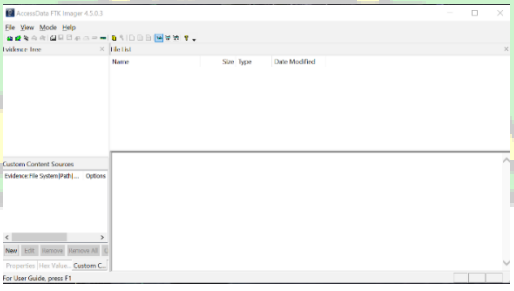
Pada tahap pengumpulan semua file yang telah selesai proses pencitraan akan dikumpulkan dan kemudian akan diurutkan. Tahap ini juga merupakan tahap yang paling penting dalam forensik digital. Tahapan ini termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Barang bukti harus benar-benar steril yang berarti belum mengalami proses apapun ketika diserahkan pada ahli forensik untuk diteliti.

Untuk *software* yang digunakan adalah Autopsy untuk mengembalikan data dan mengekstrak data menjadi file dan FTK Imager untuk men-*imaging* data agar keaslian data terjamin. Kedua aplikasi ini dapat menganalisis disk dan file pada sistem windows dan unix.

Autopsy menyediakan fungsi management kasus, integritas gambar, pencarian kata kunci dan operasi lainnya. FTK Imager membuat salinan yang sama persis yang dikenal sebagai *bit-to-bit*. FTK Imager memungkinkan praanalis data, pencarian informasi, dan pengumpulan data yang mudah menghilang seperti di RAM. Berikut adalah tampilan awal Autopsy dan FTK Imager untuk windows.



Gambar 1 : Tampilan awal aplikasi Autopsy



Gambar 2: Tampilan awal aplikasi FTK Imager

b. *Examination* (Pemeriksaan Bukti Digital)

Tahapan ini, berkaitan dengan proses pengecekan data yang telah diperoleh dari tahap sebelumnya dengan mengikuti prosedur untuk tetap menjaga integritas data. Proses ini bisa dilakukan dengan cara otomatis maupun manual. Semua bukti yang dapat mendukung penyidik telah dikumpulkan sebelumnya, kemudian media penyimpanan yang dijadikan sebagai barang bukti seperti (flash disk, hard disk, dll) dilakukan pemeriksaan secara komprehensif dengan maksud untuk mendapatkan data digital dan sesuai dengan investigasi, artinya analisis forensik harus mendapatkan gambaran fakta kasus yang lengkap dari investigator, sehingga apa yang dicari akhirnya ditemukan oleh analisis forensik adalah sama *(matching)* seperti yang diharapkan oleh investigator untuk pengembangan investigasinya. Setelah mendapatkan gambaran tentang fakta kasusnya, kemudian analisis forensik melakukan pencarian *(searching)* terhadap *image file* untuk mendapatkan fila atau data yang diinginkan[17].

c. *Analysis* (Analisa Bukti Digital)

Tahapan ini dilaksanakan dengan melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Termasuk pengecekan terhadapat metadataselanjutnya melakukan recovery dengan mengembalikan file yang terhapus.

d. *Reporting* (Laporan)

Pada tahap pelaporan isi terlampir berisi penyelidikan dari awal sampai ahir, bentuk bukti, metodologi dan kesimpulan dari awal sampai akhir kasus yang diselesaikan serta Metadata yang telah diperoleh dalam melakukan penelitian[18].

2.4 Bukti Digital

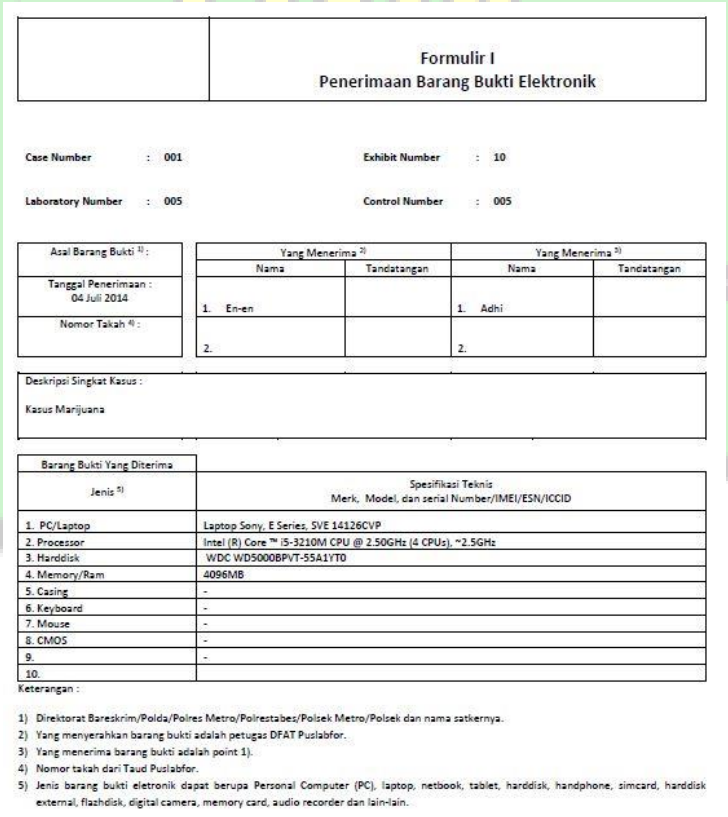
Digital forensik dan bukti digital memiliki keterkaitan, namun keduanya memiliki definisi yang berbeda. Barang bukti digita adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang memiliki subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi digital dapat menjadi subjek penyelidikan, setiap pembawa informasi yang ditargetkan untuk pemeriksaan harus diperlakukan sebagai bukti[7]. Tujuan dari aktifitas forensika digital ini adalah untuk menjaga, mengumpulkan, mengidentifikasi dan menyajikan bukti digital yang terdokumentasi dalam bentuk *chain of custody* untuk dipresentasikan dipengadilan[8].

2.5 Cyber Crime

Cyber crime adalah kejahatan yang lahir sebagai dampak negative dari perkembangan aplikasi internet. *Cyber crime* mencakup semua jenis kejahatan beserta semua modus yang dilakukan sebagai dampak negative aplikasi internet. *Cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital[9].

2.6 Chain of Custody (CoC)

Chain of custody (CoC) adalah sebuah proseduryang secara kronologis melakukan dokumentasi terhadap barang bukti serta pencatatan interaksi terhadap barang bukti tersebut, yang menunjukkan bahwa segala bukti terjamin telah dikendalikan dan ditangani dengan benar setelah proses pengumpulan. Bermacam forensik digital dilakukan dengan menjaga CoC. CoC pada forensik komputer membutuhkan kehati-hatian karena sifat data digital mudah berubah. Pada *file log* dapat merusak bukti digital dan tidak dapat diterima sebagai barang bukti. Contoh gambar chain of custody adalah sebagai berikut :



Formulir I
Penerimaan Barang Bukti Elektronik

Case Number : 001 **Exhibit Number** : 10

Laboratory Number : 005 **Control Number** : 005

Asal Barang Bukti 1) :	Yang Menerima 2)		Yang Menerima 3)	
	Nama	Tandatangan	Nama	Tandatangan
Tanggal Penerimaan : 04 Juli 2014	1. En-en		1. Adhi	
Nomor Takah 4) :	2.		2.	

Deskripsi Singkat Kasus :

Kasus Marijuana

Barang Bukti Yang Diterima	
Jenis 5)	Spesifikasi Teknis Merk, Model, dan serial Number/IMEI/ESN/ICCID
1. PC/Laptop	Laptop Sony, E Series, SVE 14126CVP
2. Processor	Intel (R) Core ™ i5-3210M CPU @ 2.50GHz (4 CPUs), ~2.5GHz
3. Harddisk	WDC WD5000BPVT-55A1YT0
4. Memory/Ram	4096MB
5. Casing	-
6. Keyboard	-
7. Mouse	-
8. CMOS	-
9.	-
10.	

Keterangan :

1) Direktorat Bareskrim/Polda/Polres Metro/Polrestabes/Polsek Metro/Polsek dan nama satkernya.
2) Yang menyerahkan barang bukti adalah petugas DFAT Puslabfor.
3) Yang menerima barang bukti adalah point 1).
4) Nomor takah dari Taud Puslabfor.
5) Jenis barang bukti eletronik dapat berupa Personal Computer (PC), laptop, netbook, tablet, harddisk, handphone, simcard, harddisk external, flazhdisk, digital camera, memory card, audio recorder dan lain-lain.

Gambar 3: Contoh Chain of Custody yang merujuk pada report U.S Departement of Justice

2.7 Data Recovery

Data Recovery adalah proses mendapatkan kembali data yang hilang, terhapus, tidak dapat diakses atau tidak dapat dibuka (*corrupted*), serta data-data yang hilang atau tidak dapat digunakan karena hal-hal yang lain dalam konteks masalah pada *software*. Proses recovery data bukan hanya mengembalikan data yang hilang, namun ada satu hal utama yang sering dilupakan yaitu bagai mana menyelamatkan data-data yang rusak atau *corrupted*. Pada dasarnya proses hilangnya data disebabkan oleh berbagai hal yang berbeda, sehingga untuk memperoleh kembali data tersebut juga dapat dilakukan dengan berbagai macam cara. Namun secara garis besar proses hilangnya data dikelompokkan ke dalam dua kategori berdasarkan penyebabnya, yaitu *software* dan *hardware*[10].

2.8 Media Penyimpanan (jenis-jenis media penyimpanan)

2.8.1 Penyimpanan magnetik *(magnetic* disk*)*

Penyimpanan magnetik merupakan media penyimpanan yang termasuk ke dalam penyimpanan sekunder *(secondary storage)* yang paling banyak dipakai pada sistem komputer modern. Adapun kelebihannya adalah kapasitas penyimpanannya lebih besar dari media penyimpanan lainnya bahkan sudah mencapai petabyte dengan kecepatan tinggi. Sedangkan kekurangannya adalah harganya lebih mahal dibandingkan yang lainnya, macam-macam media penyimpanan magnetik disk antara lain: disket, hardisk, flash disk, memori card dan lainnya.

2.8.2 Penyimpanan Optikal *(Optical disk)*

Penyimpanan optikal adalah media yang menyimpan data komputer yang dapat ditulis dan dibaca dengan menggunakan laser bertenaga rendah. Adapun kelebihannya adalah beratya lebih ringan dari beberapa media penyimpanan magnetik disk. Sedangkan kekurangannya kapasitas memorinya lebih kecil dari magnetik disk dan jika tergores maka beresiko data yang terdapat di dalamnya tidak dapat dibaca. Macam-macam media dari optikal penyimpanan antara lain: CD *(Compact Disk)*, DVD *(Digital Video Disk)* dan sejenisnya.

2.8.3 Penyimpanan Awan *(Cloud Storage)*

Cloud Storage merupakan media yang masih tergolong baru, media ini bersifat online dan tidak menggunakan kapasitas data memori pada perangkat kerena mereka menggunakan penyimpanan yang terdapat pada internet. Adapun kelebihannya adlah tidak memerlukan perangkat untuk menyimpan data, sedangkan kekurangannya yaitu sering terjadi kesalahan pada server dengan resiko data akan hilang dan juga dikenakan akses koneksi data[11].

2.9 USB Flash Drive dan Hardisk

USB merupakan singkatan dari *Universal Serial Bus* dengan makna lain dapat dikatakan standar antarmuka sebuah penyimpanan.[12] USB Flash drive atau flash disk adalah perangkat yang paling mudah untuk menyimpan dan mentransfer informasi. Flash disk tersedia dalam ukuran dan kapasitas yang

berbeda, mulai dari 2GB sampai 1TB. Flash drive atau flash disk tidak memiliki bagian yang bergerak tetapi hanya berisi chip memori sirkuit terpadu yang digunakan untuk menyimpan data. Flash disk biasanya memiliki selubung plastic atau aluminium yang mengelilingi chip memori dan konektor USB untuk digunakan pada kebanyakan komputer modern[11]. Sedangkan hardisk adalah komponen perangkat keras yang menyimpan semua konten digital. Dokumen, foto, music, video, program, preferensi aplikasi, dan sistem operasi maupun konten digital tersimpan di hardisk. Hardisk dapat berupa eksternal dan internal.

2.10 Autopsy

Autopsy adalah platform forensik digital dengan *open source* menggunakan mekanisme *end-to-end.* Dibangun menggunakan basis teknologi dengan fitur inti yang diperlukan dalam *software* forensik, Autopsy juga merupakan aplikasi yang dapat menampilkan hasil dari pencarian forensik dari volume mendasar sehingga memudahkan untuk menandai bagian data yang bersangkutan[13]. Adapun *end-to-end encryiption* yaitu suatu mekanisme komunikasi dimana orang yang bisa membaca pesannya hanyalah orang yang sedang berkomunikasi tersebut[14]. Sehingga Autopsy bisa digunakan untuk mencari dan mengembalikan file yang telah terhapus dari sistem.

2.11 FTK Imager from Access Data

FTK Imager adalah *software* gratis yang dapat diunduh dari *Accessdata* di situs resminya, FTK Imager digunakan untuk melakukan akuisisi media digital.

Untuk memastikan integritas dari data yang dikumpulkan, FTK Imager membuat salinan yang sama persis (gambar forensik) yang dikenal sebagai *bit-to-bit* atau aliran bit. FTK Imager adalah *software* yang kuat dan ju*ga* gratis, hal ini memungkinkan praanalis data, pencarian informasi, dan pengumpulan data yang mudah menghilang seperti di RAM dan lainnya[15].

2.12 File Extention

File Ectention adalah karakteristik dari sebuah file yang berfungsi sebagai tanda pengenal dan memberutahu pengguna tentang bagaimana cara menggunakan file tersebut, biasanya *file extention* ini terdiri dari 3-4 huruf diikuti tanda titik di sebelahnya. Adapun output yang dikeluarkan oleh Autopsy nantinya akan berupa berbagai macam jenis file dalam berbagai bentuk extensi, ada beberapa yang paling familiar digunakan seperti : .txt, .mp3, png, dll.

BAB III

METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Dalam penelitian ini, peneliti melakukan simulasi kasus pada 4 (empat) jenis *USB flash drive* dan 1 Hard Disk dengan kapasitas yang berbeda, yaitu : dua *USB flash drive* dengan kapsitas 8GB, 1 Hard Disk dengan kapasitas 1TB, dan satu *USB flash drive* dengan kapasitas 2GB. Metode penelitian yang digunakan dalam proposal skripsi ini adalah metode statik forensik, alasan penulis mengambil motede ini karena sesuai dengan studi kasus yang peneliti lakukan yaitu *post incident case* dimana peneliti berkerja setelah penghapusan data terjadi dan harus mengekstrak hasil dari file-file yang telah dihapus menjadi metadata kemudian mengekspor menjadi file yang persis sebelum dihapus dari metadata yang didapatkan.

Penelitian ini merupakan penelitian yang berbasis studi kasus yaitu metode dalam mengetahui dan memahami sesuatu menggunakan praktek inklusif (berbagai sudut pandang) dan menyeluruh (komprehensif), pada salah satu barang bukti yang telah diamankan yaitu *USB flash drive* yang bertujuan untuk mengidentifikasi bukti dari data-data yang diperlukan dengan menggunakan aplikasi FTK imager from Access Data dan Autopsy.

3.2 Tahapan Penelitian

Tahapan yang dilakukan dalam penelitian ini adalah tahapan dasar dalam digital forensic. Terdapat 4 tahapan dalam digital forensic yaitu: *Assessment, Acquisition, Examination, Report.*

3.2.1. *Assessment*

Assessment adalah pemeriksa atau auditor dari digital forensik yang harus menilai bukti-bukti digital yang ada dengan memberikan penilaian yang netral.

3.2.2. *Aqcuisition*

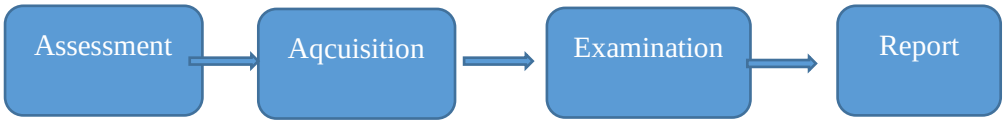
Aqcuisition adalah pemeriksaan terhadap bukti secara hati-hati, maka dari itu untuk menjaga keaslian file yang rentan rusak akibat akifitas forensik, digunakanlah FTK Imager untuk men-image data dari file bukti.

3.2.3. *Examination*

Examination adalah untuk mengambil serta menganalisis data kemudian di ekstrak atau di recovery menjadi file-file hasil *recovery*.

3.2.4. *Report*

Report adalah pelaporan mengenai prosedur dan tahapan yang dilakukan agar dapat menjadi acuan dan bahan penelitian mengenai kefektifitasan metode yang digunakan.



Gambar 4: Tahapan Penelitian[16]

3.3 Tahapan Pengumpulan

Metodologi ini dikaji serta dijabarkan untuk menjelaskan bagaimana tahapan penelitian diakukan sehingga dapat diketahui kerincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan solusi dari permasalahan yang ada dalam penelitian ini.

3.4.1 Persiapan Sistem

Persiapan sistem merupakan tahap dalam melakukan analisa dan pencarian bukti forensik digital. Langkah pertama yang harus dilakukan dalam penelitian ini adalah mempersiapkan perangkat *hardware* dan *software*, merancang scenario, serta mengimplementasikan forensika digital.

3.4.2 Bahan dan Alat Penelitian

Pada saat melakukan penelitian ini penulis menggunakn beberapa *software* dan *hardware* sebagai penunjang penelitian yang akan dilakukan oleh penulis. Untuk spesifiksi alat yang digunkan dalam penelitian adalah sebagai berikut :

a. Kebutuhan Perangkat Keras

1) Laptop DELL Inspirion 3493, *Processor Intel Core i5*, Memori 8GB RAM
2) Flash Disk Corsair.D.K 2GB, Flash Disk Toshiba 8GB, Flash Disk ScanDisk Cruzer Blade 8GB.
3) Hard Disk Toshiba Portable Storage 1TB.

b. Kebutuhan Perangkat Lunak

1) Window 10 Home Single
2) FTK Imager from Accessdata
3) Autopsy

Gambar 5: Alat-alat yang digunakan

3.4 Tahapan Analisis Data

3.4.1 Kasus yang Mendasari Penelitian

Pada penelitian ini diilustrasikan sebuah scenario kasus tindak kejahatan *cyber* yang marak terjadi, yaitu pemalsuan data diri atau Ijazah palsu, yang diterbitkan oleh instansi-instansi yang tidak bertanggung jawab dengan menrima

sogokan sejumlah uang. Sehingga data orang tersebut tidak tercatat didapodik atau dengan katalain secara resmi tidak pernah mengeyam Pendidikan di instansi terkait secara resmi, sehingga kejadian-kejadian seperti ini dapat merugikan perusahaan atau tempat bekerja Ketika ijazah palsu ini digunakan untuk melamar kerja dang dimintai sebagai bukti telah mengeyam Pendidikan.

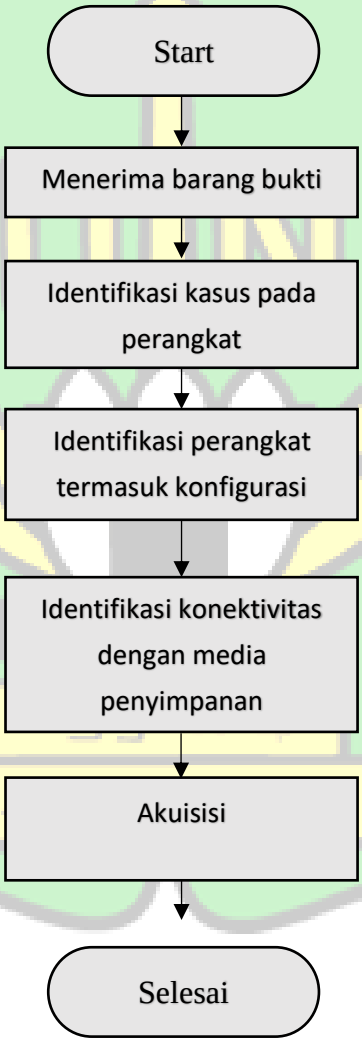
Tak hanya merugikan diri sendiri dan juga instansi terkait dalam penggunaan ijazah palsu ini, tetapi juga merugikan pencatatan data tentang informasi diri yang tercatat di pencatatan sipil sehingga harus berurusan dengan pengadilan.

Adapun menurut undang-undang administrsi kependudukan ditegaskan:

a. Pasal 93 : Setiap Penduduk yang dengan sengaja memalsukan surat dan/atau dokumen kepada Instansi Pelaksana dalam melaporkan Peristiwa Kependudukan dan Peristiwa Penting dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 50 juta.
b. Pasal 94 : Setiap orang yang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi Data Kependudukan dan/atau elemen data Penduduk sebagaimana dimaksud dalam Pasal 77 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp75.000.000,00 (tujuh puluh lima juta rupiah).
c. Pasal 96A : Setiap orang atau badan hukum yang tanpa hak mencetak, menerbitkan, dan/atau mendistribusikan Dokumen Kependudukan

sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf c dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

3.4.2 Tahapan Kejadian Sebelum Akuisisi:



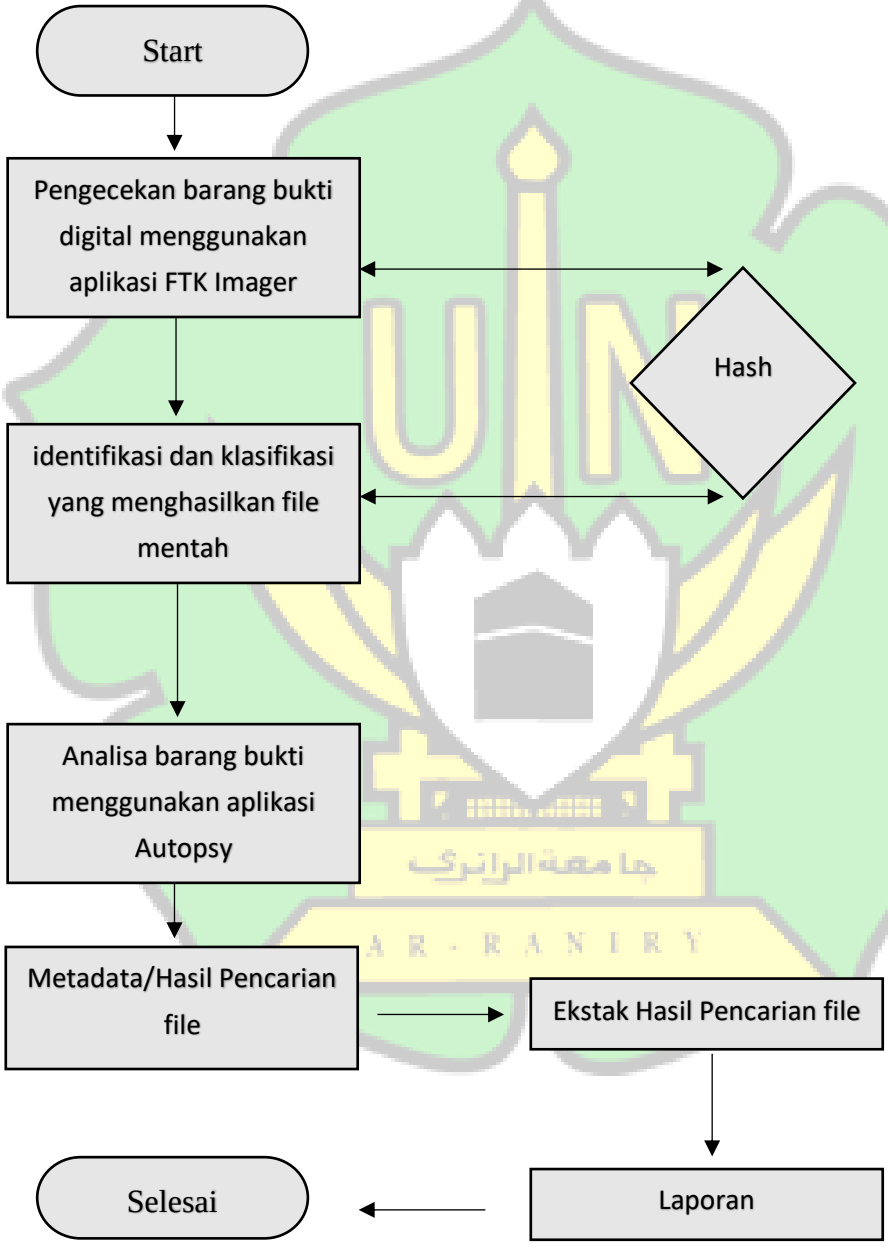
Gambar 6: Pra Akuisisi[16]

Table 2 : Pra Akuisisi[16]

Tahapan	Tindakan
Menerima barang bukti	Penyidik memberikan barang bukti yang telah disita untuk dianalisa
Identifikasi kasus	Penyidik meminta untuk menemukan file-file yang bersangkutan
Identifikasi perangkat dan konfigurasi	Menyimpulkan organisasi dan arsitektur perangkat barang bukti yang digunakan dalam kasus yang akan dianalisa
Identifikasi konektivitas dengan media penyimpanan	Menentukan tersambungnya USB dan Hardisk yang akan digunakan nantinya

3.4.3 Akuisisi:

Merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktivitas yang dilakukan.



Gambar 7: Akuisisi [16]

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pembahasan

Dalam penelitian ini sesuai dengan metode yaitu *static forensic*, dimana peneliti akan mengembalikan file yang telah terhapus atau *recovery* dengan menjamin terjaganya keaslian dari file tersebut.

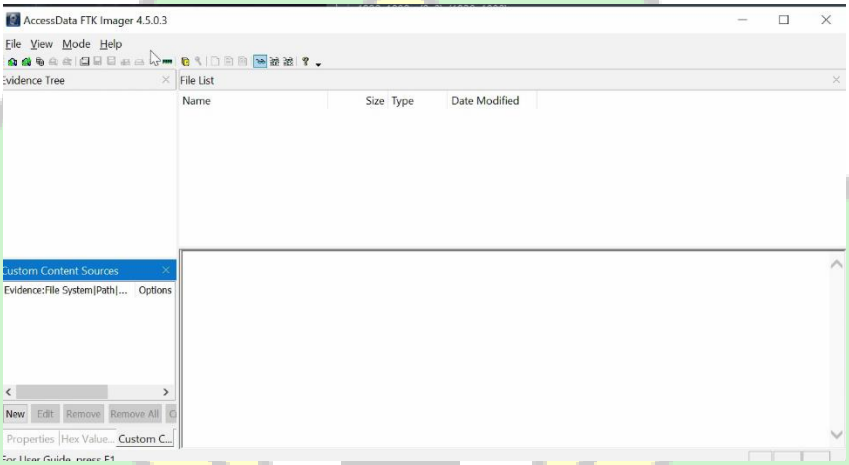
Adapun dalam penelitian ini, ada 4 media penyimpanan yang akan dilakukan proses imaging dan analisis untuk menjada keaslian file yang nantinya akan direcovery, yaitu tiga *USB Flash Drive*, dengan kapasitas dan merek yang berbeda, satu yang berkapasitas 2 GB dan dua lainnya berkapasitas masing-masing 8 GB dan sebuah hardisk berkapastitas 1 TB.

4.2 Proses Imaging dan Analisis Perangkat Penyimpanan

Pada kasus-kasus yang berkaitan dengan aktifitas cyber crime, biasanya ada file-file yang dibutuhkan untuk proses forensik tetapi sayangnya telah dihapus. Parahnya lagi, file tersebut sudah tidak ada di dalam recycle bin sehingga tidak bisa di restrore karena memang telah dihapus dari recycle bin. Mengembalikan file yang telah dihapus merupakan salah satu kemampuan yang penting untuk dimiliki bagi seorang investigaror forensik. Untuk mengatasi hal tersebut kita memerlukan program tambahan untuk menyelamatan file yang sudah menghilang dari recycle bin. Yaitu dengan menggunakan aplikasi salah satunya FTK Imager dan Autopsy.

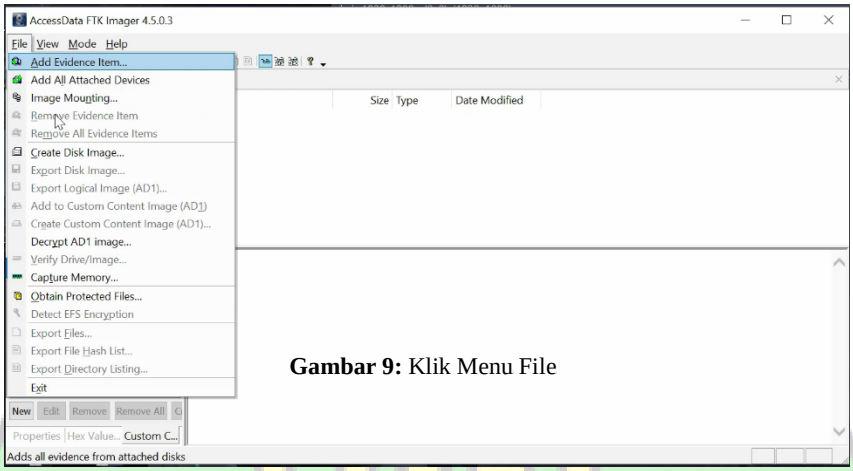
4.2.1 *Imaging* dengan FTK Imager

Disaat Persiapan telah lengkap dan saatnya kita mulai proses awal cara *imaging* terhadap barang bukti agar barang bukti tersebut terjaga keasliannya dan bisa dipertanggung jawabkan. Aplikasi yang digunakan yaitu FTK Imager. Tampilan awal pada aplikasi FTK Imager adalah sebagai berikut:

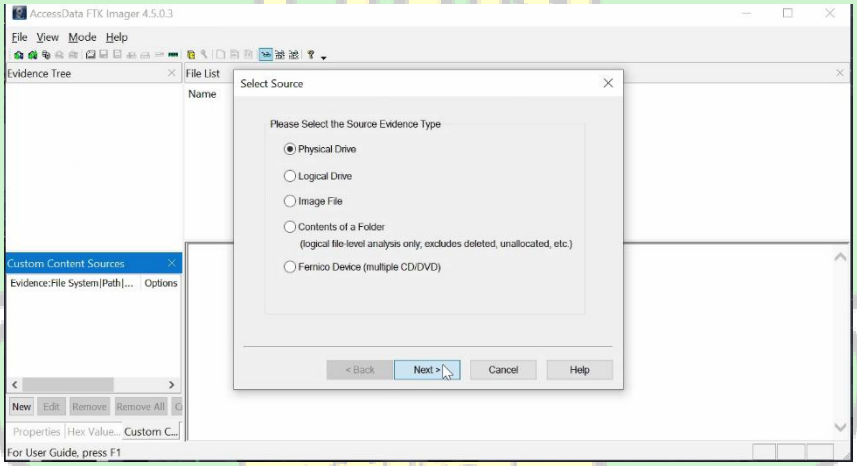


Gambar 8: Tampilan Awal Aplikasi FTK Imager

Setelah *USB* sudah dikoneksikan ke komputer atau laptop dan sudah terdeteksi maka kita bisa langsung saja memulai proses *imaging* dengan klik menu *File*, kemudian pilih *Create Disk Image*. Kemudian akan muncul dialog box yang baru, pilih *Physical Drive* karena akan dilakukan *imaging* terhadap fisik dari *harddisk*.

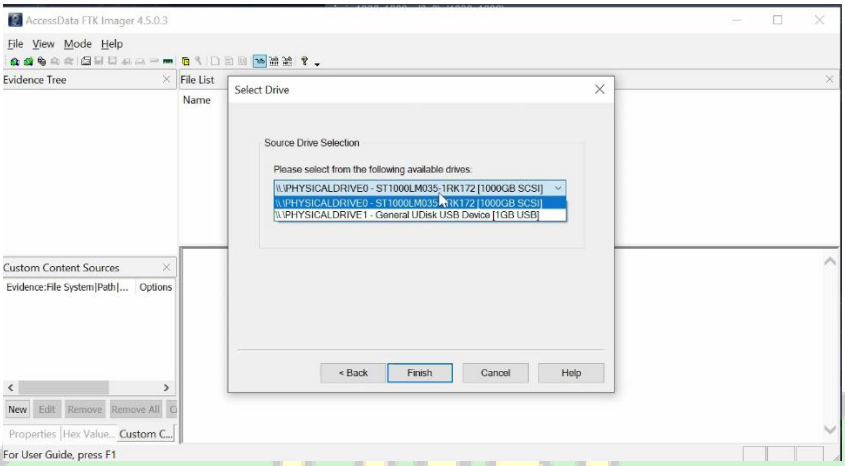


Gambar 9: Klik Menu File



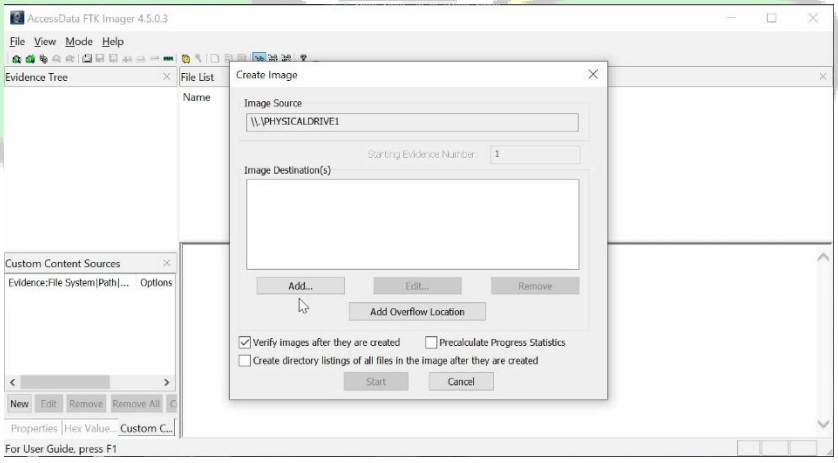
Gambar 10: Pilihan Type Barang Bukti

Kemudian klik *next*, setelah itu pilih *harddisk* yang telah sambungkan melalui *case* yaitu eksternal memori 3.0.



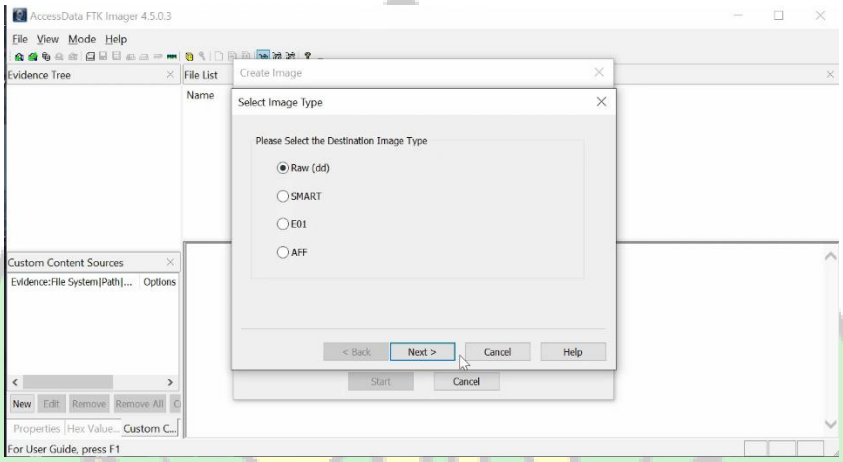
Gambar 11: Pilihan Media Penyimpanan yang akan di Imaging

Setelah itu klik add untuk memilih lokasi hasil *imaging*, dan juga mencontreng pilihan *verify images after they are created*. Pilihan tersebut adalah *untuk* menghitung kode hash barang bukti dan hasil *imaging*, kemudian mencocokkan keduanya.



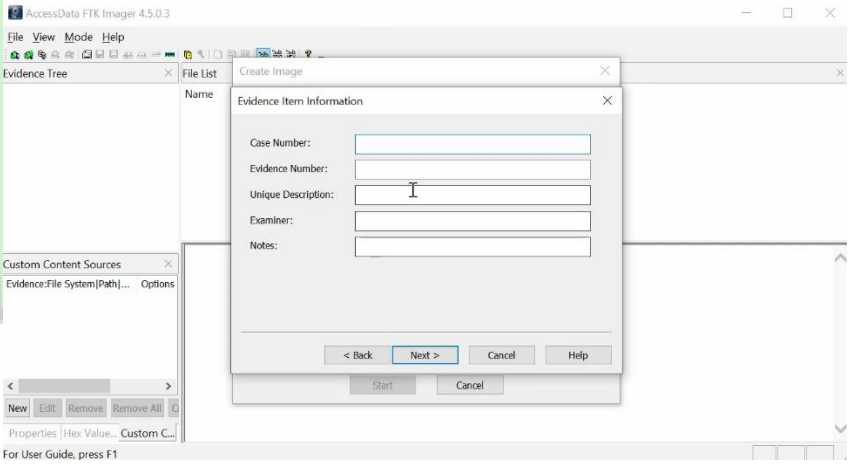
Gambar 12: Lokasi Penyimpanan Imaging

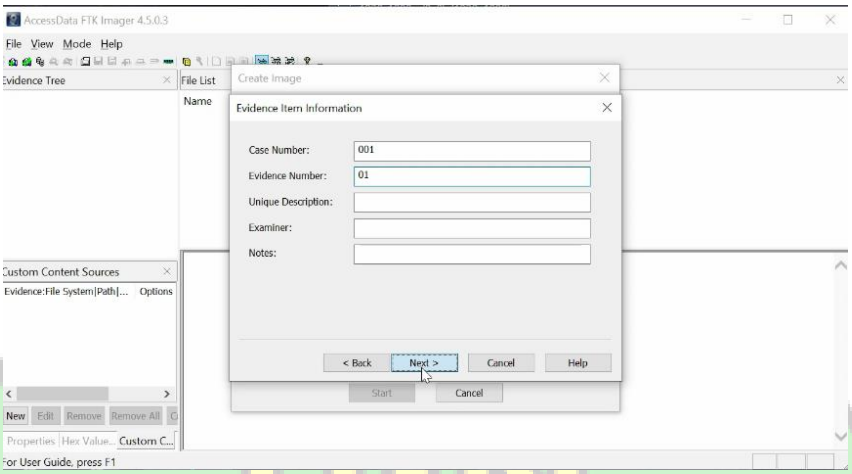
Karena untuk data yang asli pilih *raw DD* untuk format hasil *imaging.* Setiap data hash disimpan dalam file log terpisah yang umumnya dengan file gambar.



Gambar 13: Pilihan Format Imaging

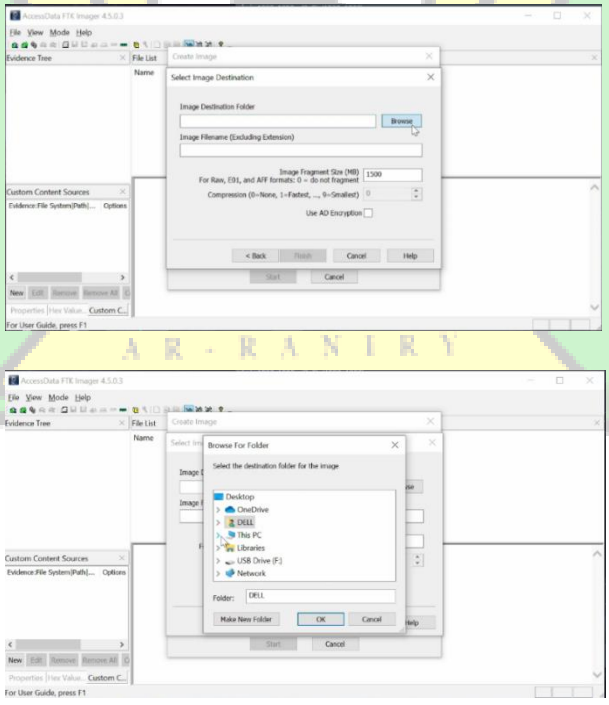
Selanjutnya pilih lokasi folder yang diinginkan dan buat nama file imaging, lalu klik *next.*

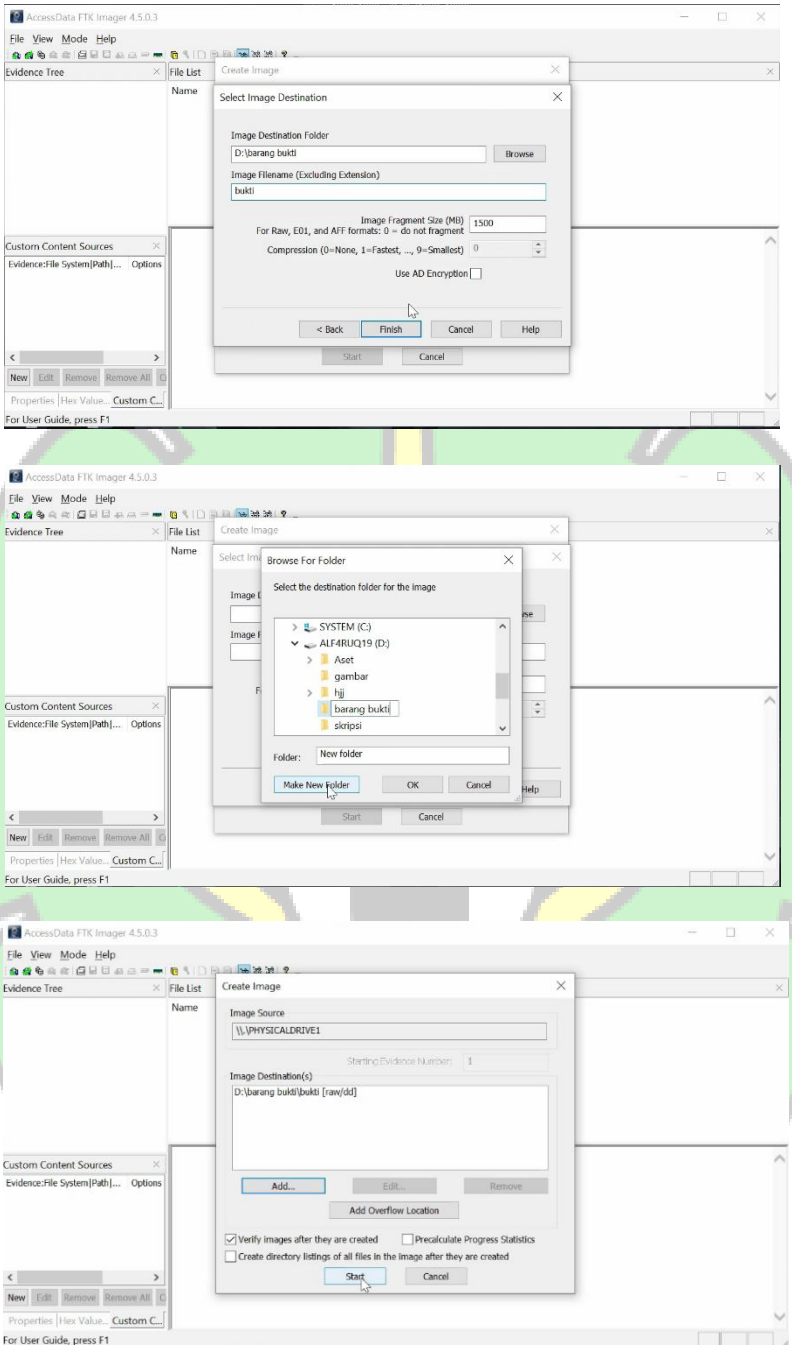




Gambar 14: Informasi Item Barang Bukti

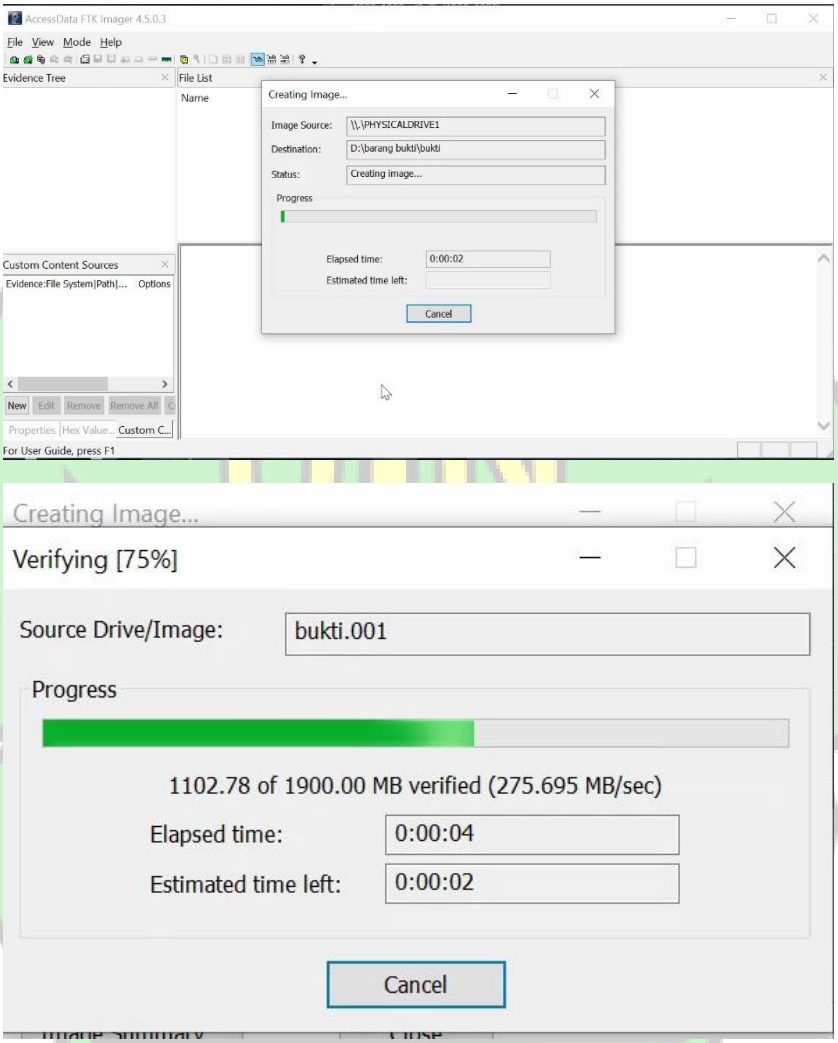
Kemudian pilih lokasi folder yang diinginkan dan buat nama file imaging, lalu klik finish.





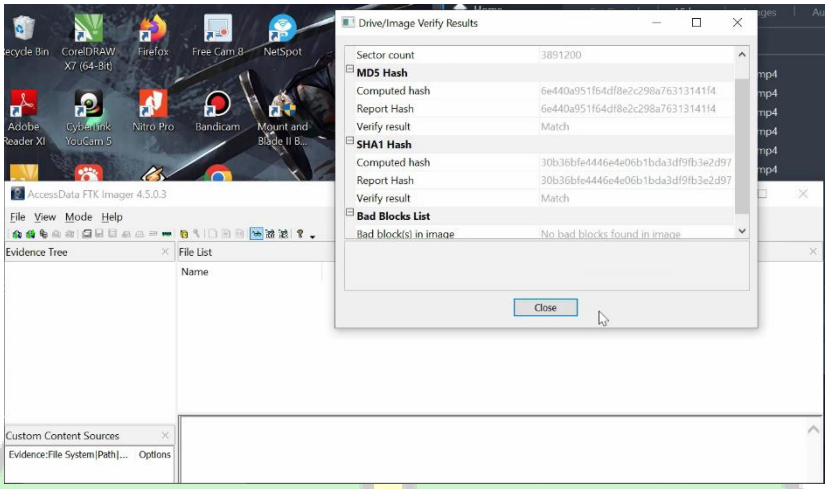
Gambar 15: Menentukan Alamat Penyimpanan Imaging

Langkah terakhir, klik start untuk memulai imaging, gambar dibawah ini menunjukkan proses yang sedang berlangsung.



Gambar 16: Proses yang Sedang Berjalan

Setelah proses imaging selesai, FTK akan memberikan kode dan laporan hash MD5 dan SHA 1 serta hasil prosesnya.

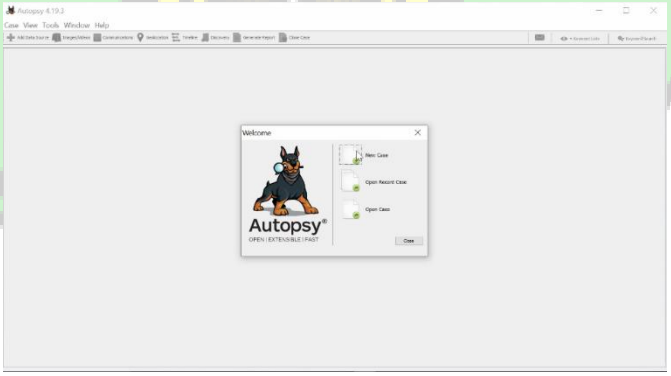


Gambar 17: Laporan Kode Hash

4.2.2 Mengembalikan File dengan Aplikasi Autopsy

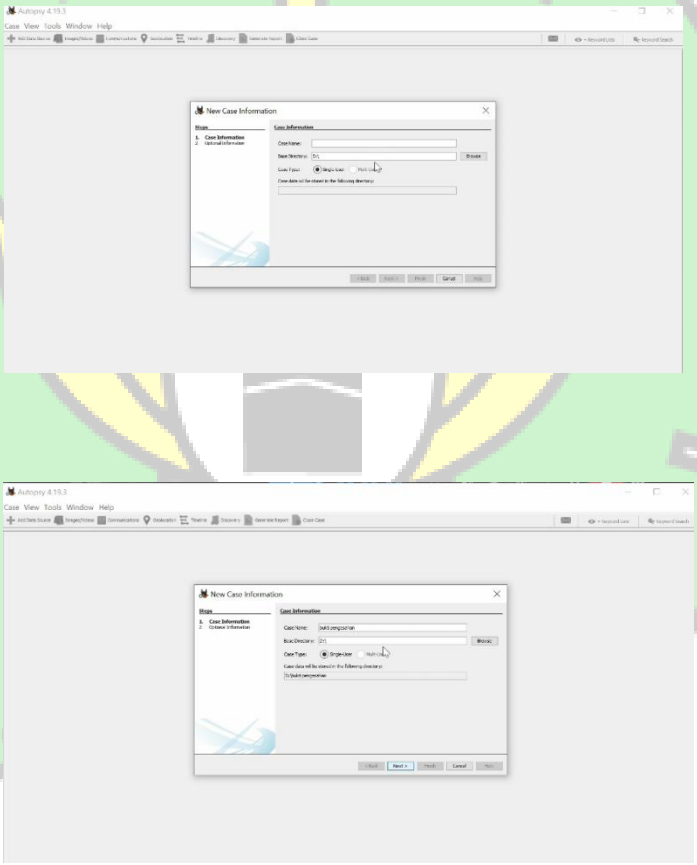
Sebenarnya ada cukup banyak aplikasi yang bisa digunakan untuk mengembalikan file yang telah dihapus, salah satunya adalah Autopsy. Kelebihan dari apliksi ini adalah selain bisa membaca file yang telah terhapus dari dalam local hardisk, juga bisa mencari dari file image yang kita miliki.

Adapun tampilan awal dari aplikasi Autopsy ini adalah seperti gambar dibawah ini:



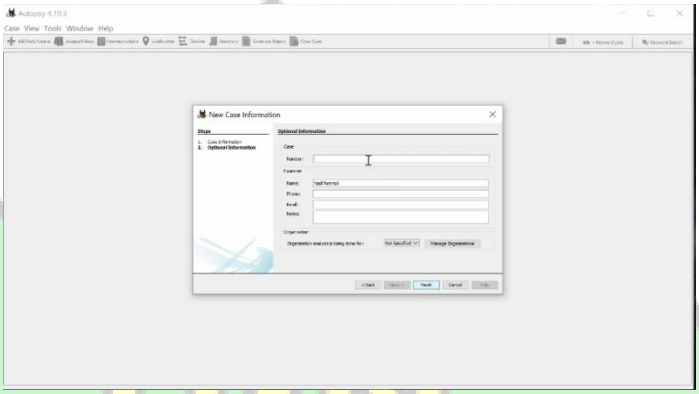
Gambar 18: Tampilan Awal Autopsy

Untuk memulai kegiatan forensik, klik pada create new case yang terdapat pada kotak dialog welcome seperti yang terlihat pada gambar dalam kotak dialog new case information, pada bagian case name isikanlah dengan nama kasus forensik yang sedang ditangani, selanjutnya pada bagian base directory tentukanlah lokasi folder untuk menaruh file yang didapatkan dengan cara mengklik tombol browse. Setelah semua peraturan selesai, klik tombol next.



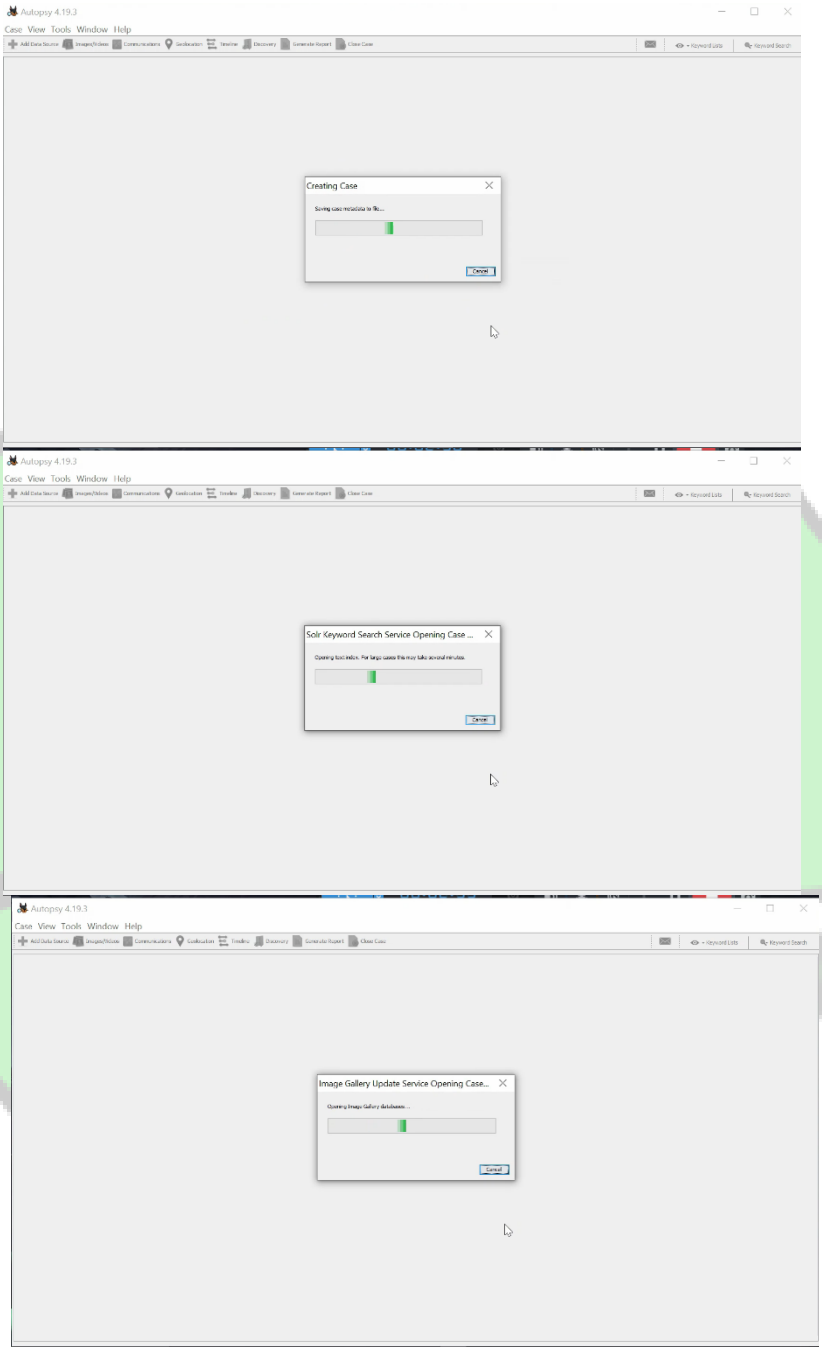
Gambar 19: Case Information

Dari tampilan berikutnya yang mumcul, masukkan lah nomor kasus pada bagian case number, serta nama investigator forensik pada bagian *Examiner* kemudian klik tombol finish.



Gambar 20: Optional Information

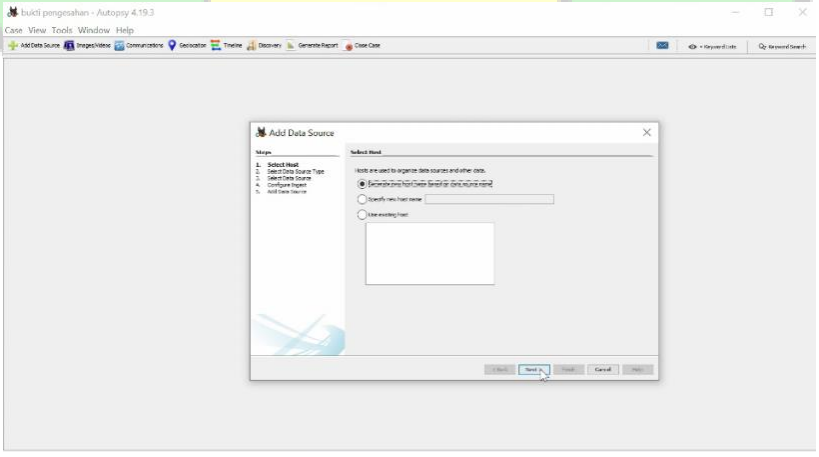
Pada gambar ini 19 merupakan form case information. Pada form ini menjelaskan mengenai kasus yang ingi dianalisis dari mengisikan nama kasus dan pemilihan letak directory untuk menyimpan kasus tersebut yang akan menghasilkan sebuah dokumen. Pada gambar 20 merupakan form additional information menjelaskan mengenai kasus ke berapa dan siapa nama pengguna aplikasi autopsy yang akan melakukan analisis tersebut. Kedua form tersebut berfungsi untuk mendapatkan rekam analisis yang dapat dipertanggung jawabkan. Selanjutnya tunggulah proses persiapan dilakukan hingga selesai.

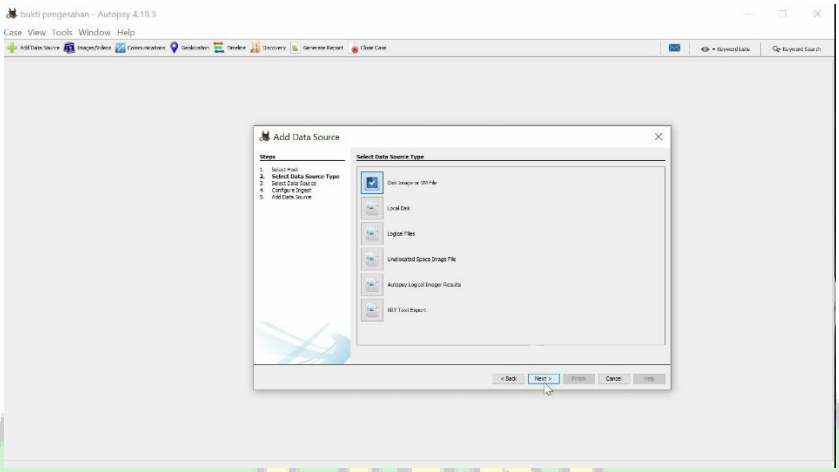


Gambar 21: Membuat Database

Setelah proses persiapan selesai secara otomatis akan muncul kotak dialog untuk menentukan dimana lokasi file yang telah diihapus akan direcover. Umumnya dalam kegiatan forensik adalah mengambil data dari disk image or VM file. Itulah pentingnya pembuatan file image terlebih dahulu dalam proses forensik.

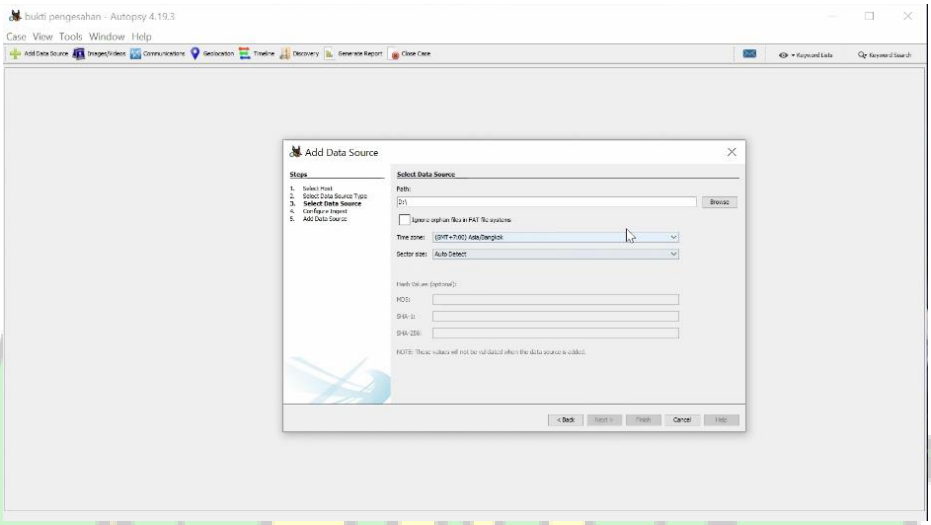
Setelah melakukan penelitian form untuk kepentingan analisis, selanjutnya masuk ke dalam tahap-tahap melakukan proses analisis dari file image yang dihasilkan aplikasi, tahap-tahap tersebut antara lain adalah menentukan data apa yang akan dianalisis yaitu berupa file image, mengambil file image yang ingin dianalisis dari hasil proses akuisisi penyimpanan, memilih modul dalam aplikasi autopsy untuk kepentingan menganalisis, dan data source akan ditampilkan dalam aplikasi autopsy yang sudah teridentifikasi data-datanya. Untuk melihat tahap pertama yaitu menentukan data apa yang ingin dianalisis dapat dilihat pada gambar berikut ini.

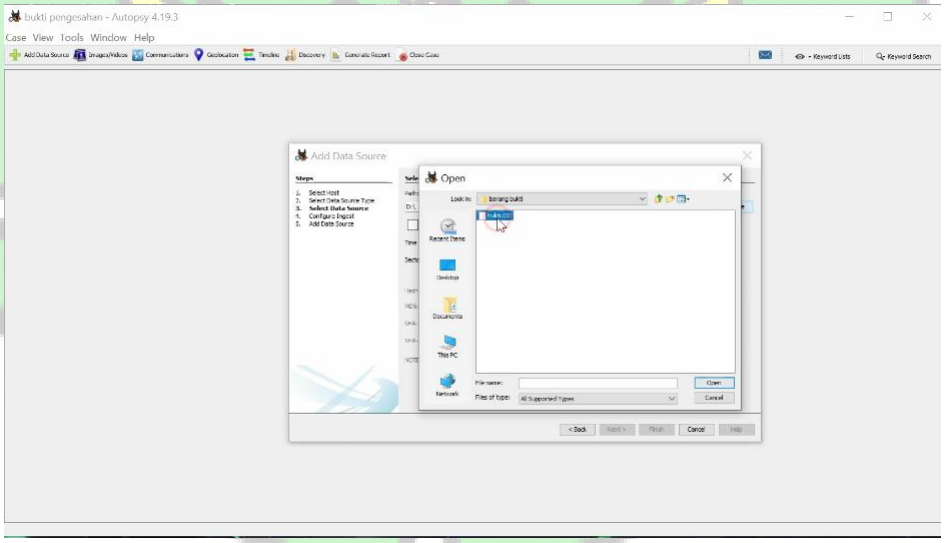


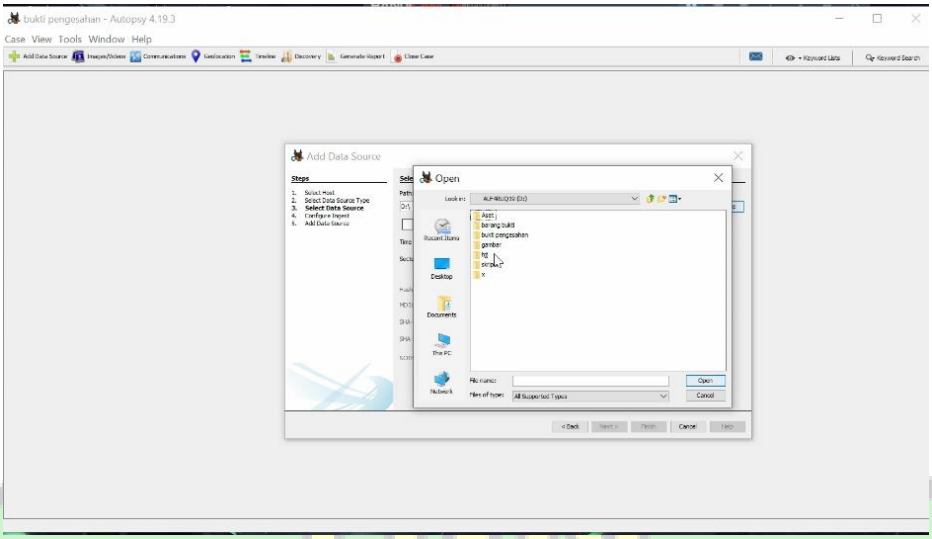


Gambar 22: Form Menentukan Type yang akan dianalisis

Pada gambar ini merupakan form dalam aplikasi Autopsy untuk memilih tipe data yang ingin dianalisis, untuk file yang akan dianalisis adalah file image yang dihasilkan aplikasi. Maka dari file tersebut kita dapat memilih pilihan 1 yaitu disk image karena file yang hasilkan aplikasi bertipe disk image dan juga pilihan 1 memiliki fungsi untuk menganalisis file tersebut secara menyeluruh, untuk pilihan 2 dan 3 adalah pilihan untuk menganalisis file dari localdisk dan logical files, sedangkan pilihan 4 adalah pilihan untuk menganalisis dari file image, namun hanya dalam sector unallocated space dari file image yang akan dianalisis, setelah memilih pilihan 1, selanjutnya aka nada form mengambil file image yang dihasilkan aplikasi untuk dimasukkan dalam aplikasi autopsy dan dapat dilakukan analisis dari file tersebut. Form tersebut seperti yang tertera pada gambar berikut.


bukti pengesahan - Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Steps
Select Data Source
Path:
Browse
Time zone:
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
< Back
Next >
Finish
Cancel
Help

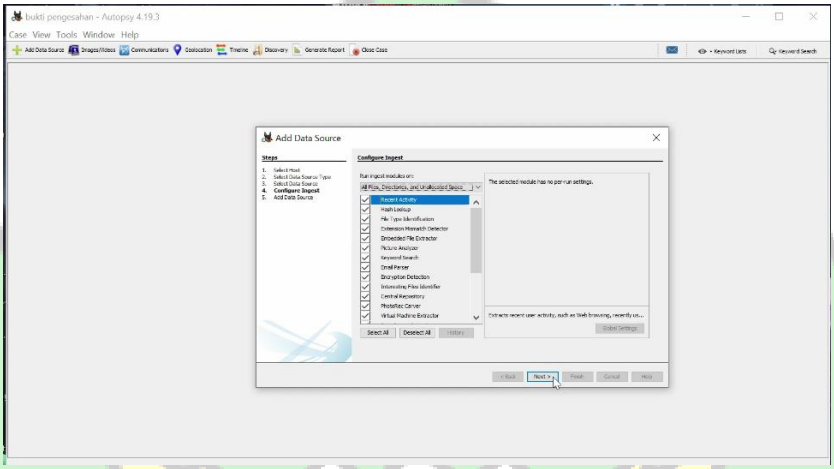

bukti pengesahan - Autopsy 4.19.3
Case View Tools Window Help
Keyword Lists
Keyword Search
Add Data Source
Open
Look in:
Recent Items
Desktop
Documents
This PC
Network
File name:
Open
Files of type:
Cancel
< Back
Next >
Finish
Cancel
Help

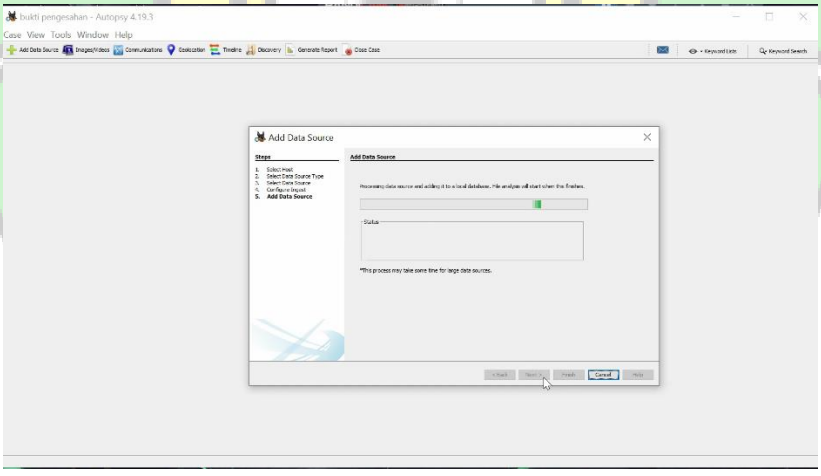


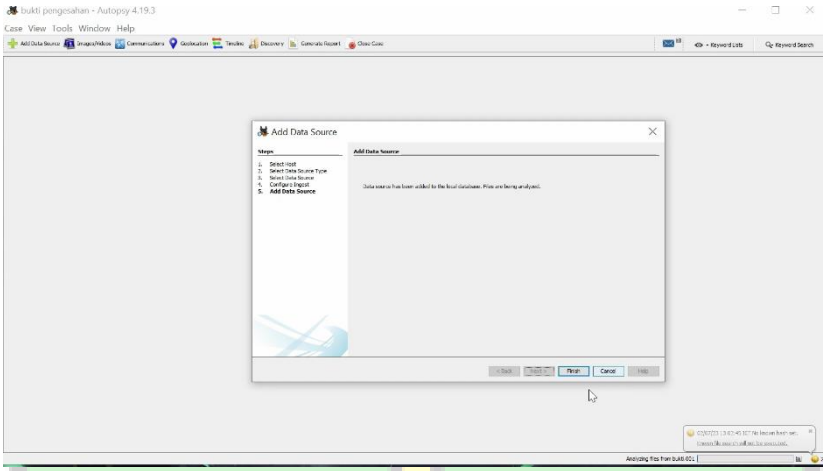
Gambar 23: Mengambil Data yang akan dianalisis

Pada gambar di atas merupakan form penentuan untuk memilih modul dalam aplikasi autopsy yang berfungsi untuk membagi data yang dibutuhkan saat melakukan proses analisis dari file image yang sudah dimasukkan dalam aplikasi autopsy agar tersusun dengan rapi dan dapat dianalisis secara menyeluruh dalam aplikasi autopsy, dari memilih modul dalam aplikasi autopsy banyak pilih yang memiliki fungsi untuk kepentingan analisis agar mudah dilakukan. Setelah penentuan memilih modul, maka aplikasi autopsy menjalankan memilih modul yang telah dipilih dan akan masuk dalam menu utama untuk melakukan analisis dari file image yang telah dimasukkan dalam aplikasi autopsy. Untuk melihat data file image penyimpanan yang sudah terbaca dalam aplikasi autopsy dan menjadi data source untuk proses analisis dengan membagi beberapa komponen data dari

fungsi memilih modul yang dijalankan aplikasi autopsy dapat dilihat pada gambar berikut.





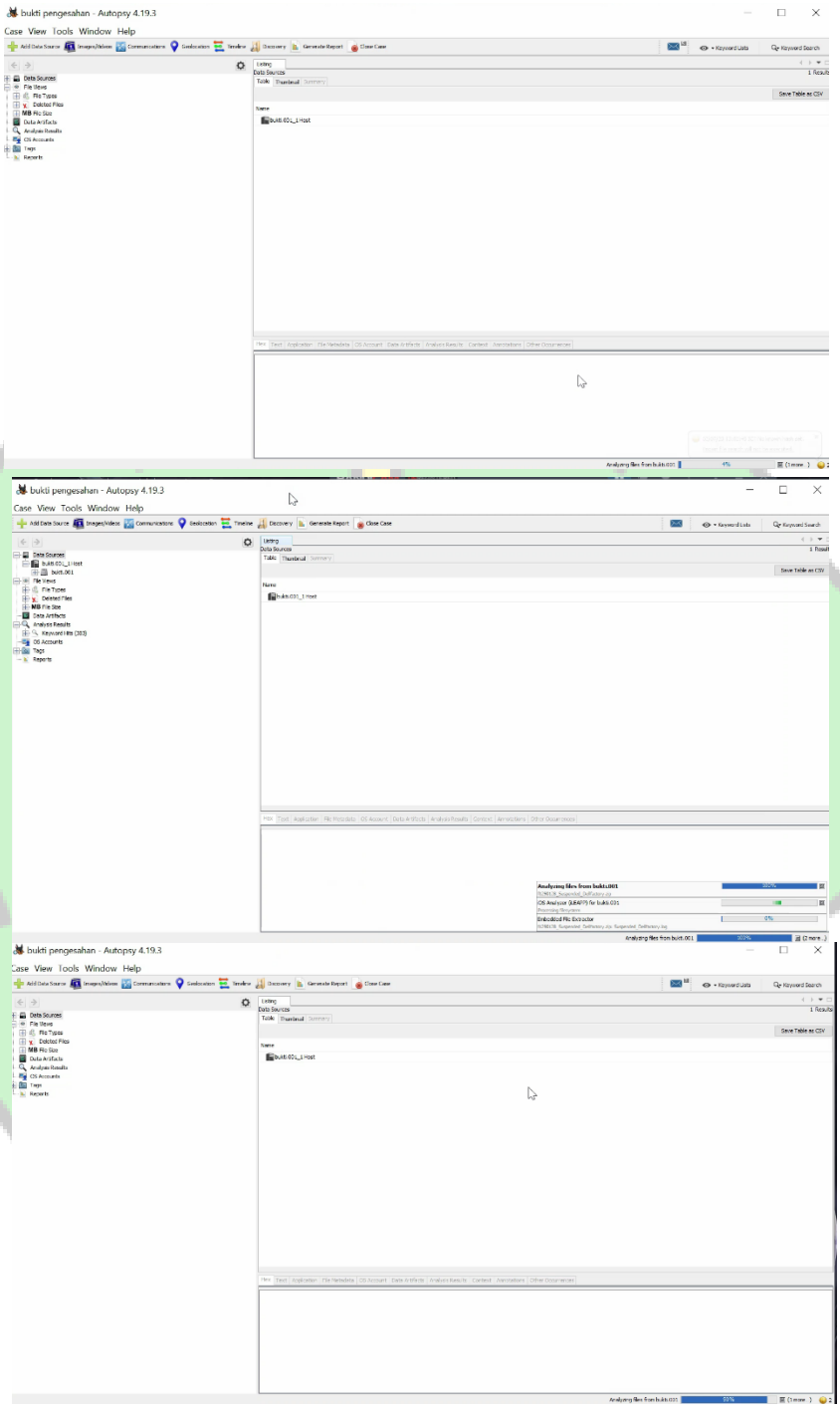


Gambar 24: Menentukan Modul Aplikasi Autopsy

Pada gambar 24 merupakan form penentuan untuk memilih modul dalam aplikasi autopsy yang berfungsi untuk membagi data yang dibutuhkan saat melakukan proses analisis dari file image yang sudah dimasukkan dalam aplikasi autopsy agar tersusun dengan rapi dan dapat dianalisis secara menyeluruh dalam aplikasi autopsy, dari memilih modul dalam aplikasi autopsy banyak pilihan yang memiliki fungsi untuk kepentingan analisis agar mudah dilakukan.

Setelah penentuan memilih modul, maka aplikasi autopsy menjalankan modul yang telah dipilih dan akan masuk dalam menu utama untuk melakukan analisis dari file image yag telah dimasukkan dalam aplikasi autopsy.

Untuk melihat data file image penyimpanan yang sudah terbaca dalam aplikasi autopsy dan menjadi data source untuk proses analisis dengan terbagi beberapa komponen data dari fungsi memilih modul yang dijalankan apikasi autopasy dapat dilihat pada gambar berikut ini:



Gambar 25: Data Source dalam Aplikasi Autopsy

Pada gambar diatas merupakan data source yang dihasilkan aplikasi autopsy dari file image yang telah dimasukkan kedalam aplikasi autopsy untuk melakukan proses analisis file image tersebut, namun setelah masuk dan terbaca sebagai data source aplikasi autopsy, maka aplikasi menjalankan proses untuk membaca semua isi file image agar tersusun dengan baik dan mudah untuk dianalisis.

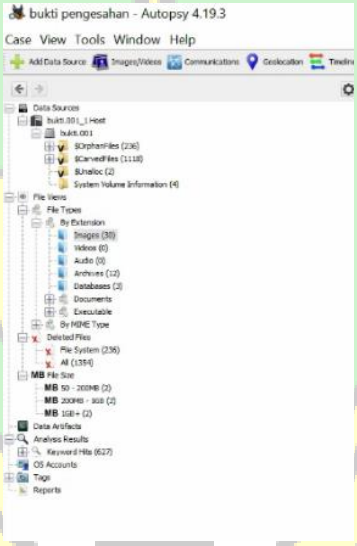
Setelah proses data source dalam aplikasi autopsy telah selesai maka data tersebut sudah dapat dianalisis dan tersusun dengan rapi. Untuk melihat partisi dalam file image penyimpanan yang telah menjadi data source yang dihasilkan aplikasi autopsy untuk dilakukan analisis dapat dilihat pada gambar berikut:

Gambar 26: Part dalam Data Source Aplikasi Autopsy

Gambar di atas merupakan daftar part-part dari file image penyimpanan yang sudah dijadikan data source dalam aplikasi autopsy. Dari daftar part-part tersebut dapat mengetahui semua data-data yang terdapat dalam part tertentu yang

dihasilkan dari data source dalam aplikasi autopsy dan dapat juga data tersebut diekstrak ke perangkat yang akan dijadikan file barang bukti yang akan dihasilkan dari proses analisis.

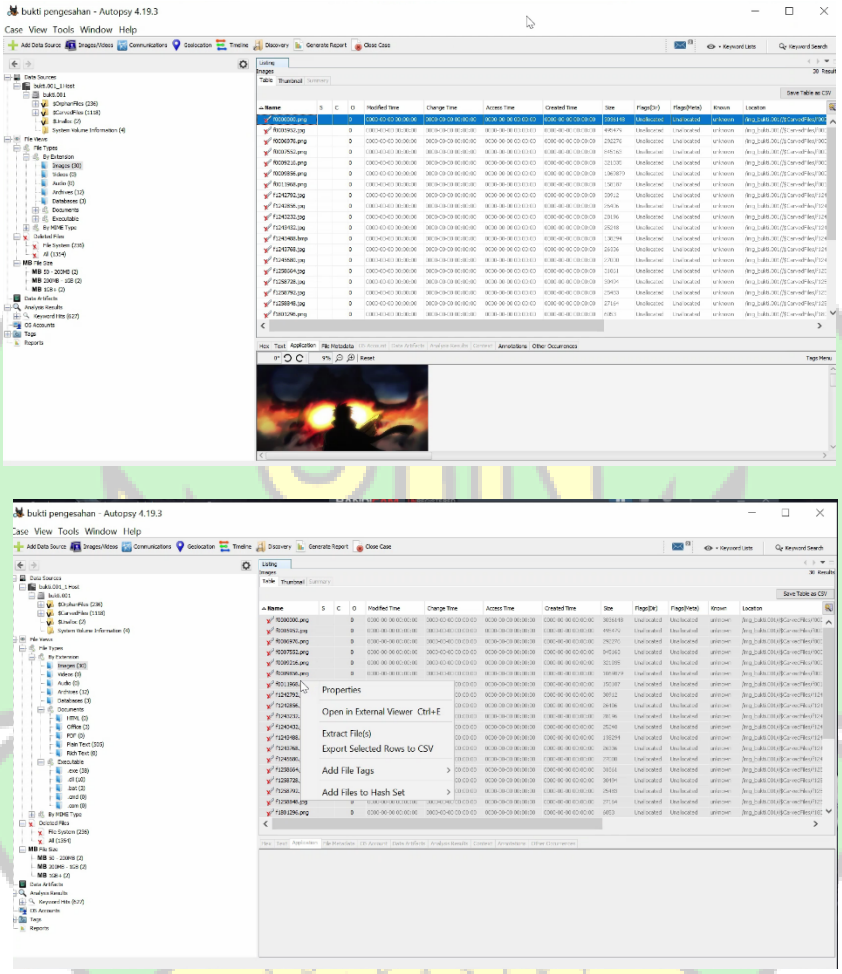
Untuk melihat semua data berdasarkan file yang telah tersusun rapi dapat dilihat pada gambar berikut:



Gambar 27: Detail Data Source dari Autopsy

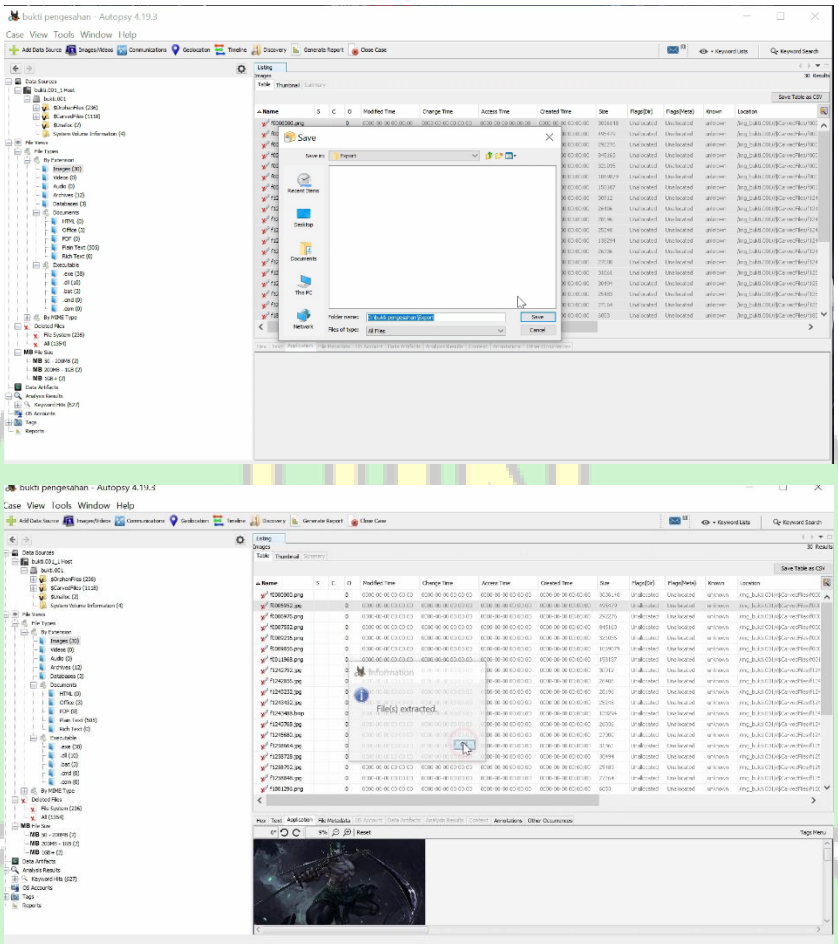
Gambar sebelumnya merupakan fasilitas dari autopsy untuk melihar semua detail data-data yang terdapat dalam penyimpanan internal yang telah tersusun dengan rapi dan telah menjadi data source dalam aplikasi autopsy, dari detail data source tersebut terbagi dari beberapa komponen data dari penyimpanan internal, data tersebut diantaranya berdasarkan dari file type, delete files dan file size yang terbilang cukup besar.

Apabila ada file yang ingin di ekstrak kembali bisa dengan mengklik kanan pada file tersebut kemudian klik file(s).



Gambar 28: Ekstrak File

Jika tidak ada halangan akan muncul pesan file(s) extracted, lalu klik “OK”.

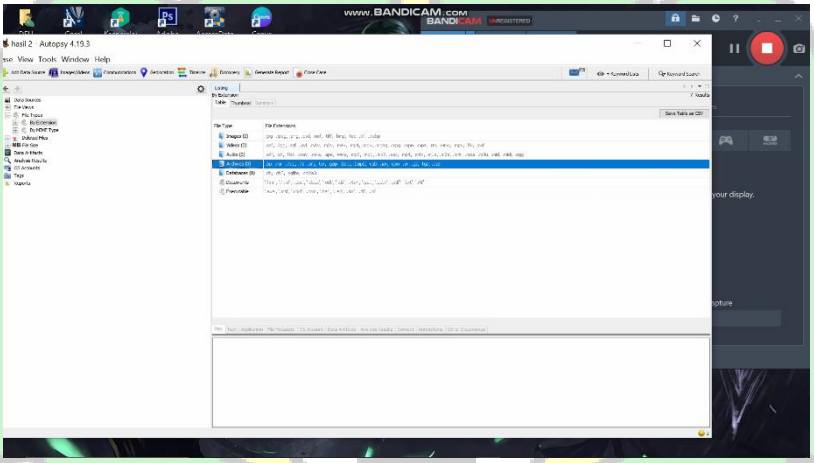


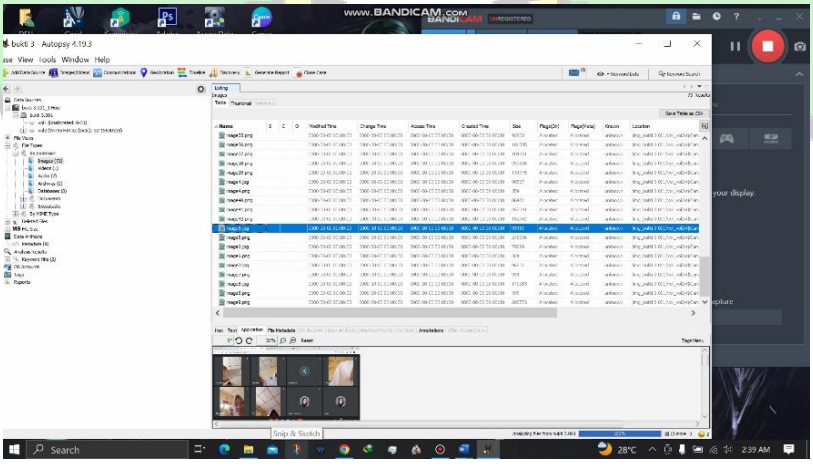
Gambar 29: Ekstrak Selesai

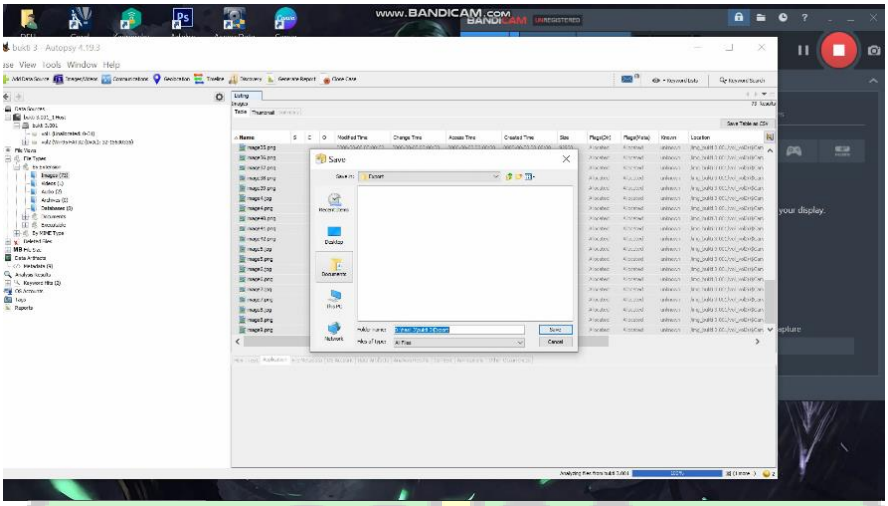
Pengembalian file yang telah hilang telah berhasil dilakukan dan file yang dimaksud dapat ditemukan pada folder tujuan yang telah diekstrak.

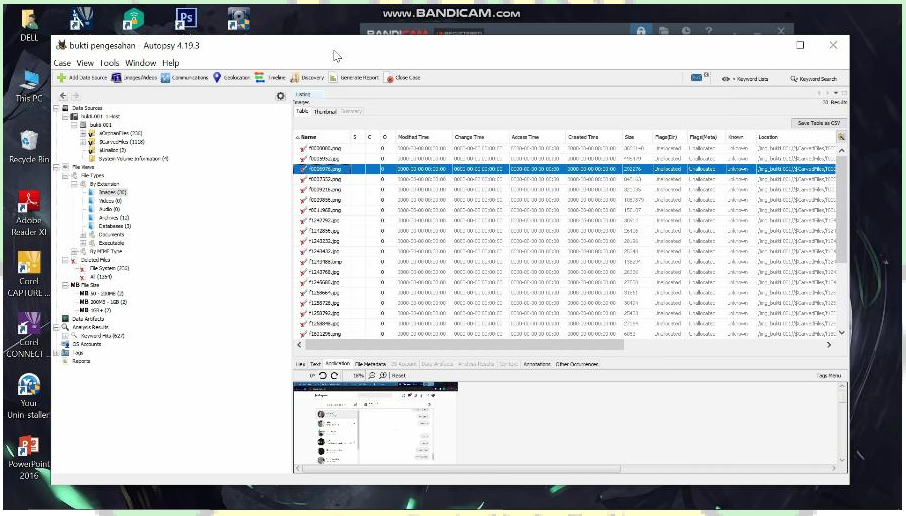
4.3 Hasil

Setelah melakukan pemeriksaan pada 3 barang bukti yang berbeda ditemukan bahwa data yang telah dihapus berisi 15 file dengan 6 jenis ekstensi yang berbeda, dengan keterangan data yang sama seperti file yang sebelumnya dihapus.

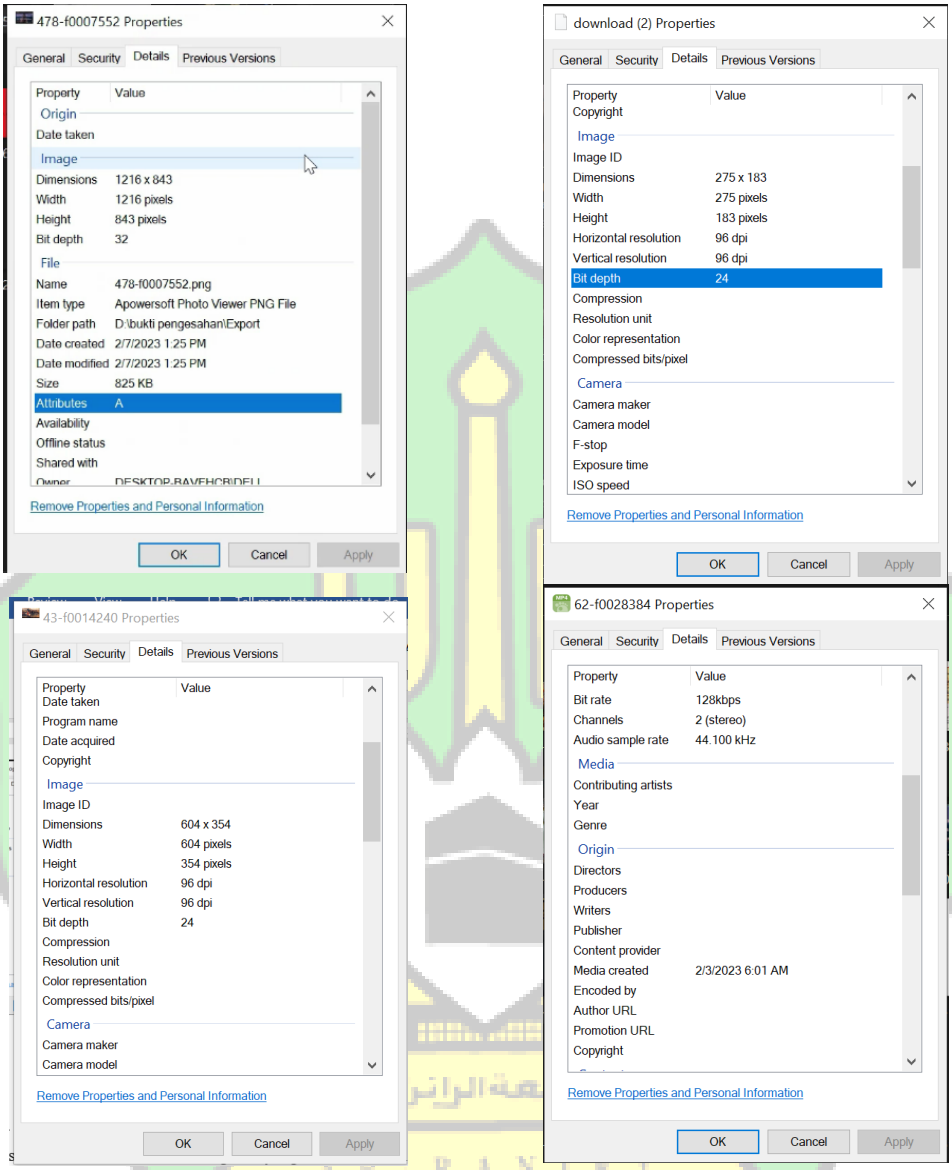








Gambar 30: Hasil pengembaian file yang sudah siap untuk di *extract*



Gambar 31: Contoh details dari beberapa file yang sudah di kebalikan.

4.4 Laporan

Berdasarkan dari hasil bukti digital yang telah dianalisis dengan menggunakan bantuan FTK Imager dan aplikasi Autopsy di 3 USB yang berbeda, di dapatkan hasil waktui imaging pada device 1 sebesar kurang lebih 49 menit dengan bukti sebanyak 12 file. Untuk device 2 didapatkan hasil waktu imaging kurang lebih 57 menit dengan bukti sebanyak 15 file. Sedangkan pada device 3 di dapatkan hasil waktu imaging 273 menit dengan bukti sebanyak 35 file, dan pada device 4 didapatkan hasil waktu imaging 840 menit dengan jumlah file bukti sebanyak 170 file.

Table 3: Rangkuman *Recovery* File

Device	**Ekstensi File**	**Jumlah Pengujian**	**File Bukti**	**File Asli**	**Waktu (menit)**	**Status**
Flash Disk Corsair.D.K 2GB	jpg, png, docx, txt.	4	12	12	49	Berhasil
Flash Disk Toshiba 8GB	jpg, png, docx, txt, xlsx, pptx.	5	15	15	57	Berhasil

Flash Disk ScanDisk Cruzer Blade 8GB	jpg, png, docx, txt, xlsx, pptx, mp3, mov, mp4.	2	35	35	273	Berhasil
Toshiba Portable Storage 1TB	jpg, png, docx, txt, xlsx, pptx, mp3, mov, mp4.	7	170	170	840	Berhasil

BAB V

PENUTUP

5.1.Kesimpulan

Berdasarkan penelitian dan pembahasan skripsi ini mengenai Digital Forensic dengan Metode Static Forensic dapat disimpulkan bahwa:

1. Dalam metode static forensic ini perlunya pengumpulan semua data-data yang akan dianalisa baik dalam bentuk fisik ataupun bukan agar terjaminnya keaslian data dalam penelitian.
2. Aplikasi FTK Imager sebagai tools imaging barang bukti terbukti mampu mengembalikan data-data yang hilang dari barang bukti secara utuh.
3. Aplikasi autopsy sebagai tools Analisa barang bukti mampu mengangkat barang bukti secara terperinci meski proses tidak sempurna 100% validasi.

5.2. Saran

Untuk pengembangan lebih lanjut dibutuhkan alat investigator dengan spesifikasi yang lebih memadai supaya bisa meganalisa barang bukti secara menyeluruh sehingga nantinya juga bisa melakukan penelitian terkait dengan perangkat mobile.

DAFTAR PUSTAKA

[1] F. Fil-Ardh, "Keaslian Pengembalian data pada Flash Drive sebagai Bukti Digital," Universitas Pasundan Bandung, 2019.

[2] Handrizal, "Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete dan Recuva Data Recovery untuk Digital Forensic," *J. Sains Komput. dan Inform.*, vol. 1, p. 85, 2017.

[3] F. Lerian, "USB Flash Drive Data Acquisition for Collecting Evidence by Recovering Delete Data from Unallocated Space According to Digital Forensic Procedures," Universitas Gajah Mada, 2018.

[4] P. M. S. and B. Santoso, "Static Forensic pada USB Mass Storage menggunakan Forensic Imager," *J. Komput. Terap.*, vol. 8, p. 134, 2022.

[5] Z. G. Melda Agnes Manuhutu, Muttaqin Muttaqin, Deci Irmayani, Tomi Tamara, *Pengantar Forensik Teknologi Informasi*, 1st ed. Yayasan Kita Menulis, 2021.

[6] R. A. Ramadhan and D. Mualfah, "Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 183–192, 2020, doi: 10.25299/itjrd.2021.vol5(2).5750.

[7] R. Watrianthos, *Forensik Digital*. Yayasan Kita Menulis, 2021.

[8] T. F. Efendi, "Manajemen Barang Bukti Fisik Dan Chain of Custody (CoC)

Pada Penyimpananan Laboratorium Forensika Digital," *Pros. Semant.*, pp. 242–250, 2019, [Online]. Available: https://journal.uncp.ac.id/index.php/semantik/article/view/1522

[9] Fauzia Amanta,"Jurnal Pendidikam dan Konseling" *J.Penerapan Hukum Pinadana Dalam PEnggunaan IJazah Palsu*, Vol. 5 no. 1, 1023

[10] Muhammad Yusuf, *Komunikasi Bisnis*. Medan: Manhaji, 2019.

[11] Autopsy, "Now Supporting Forensic Team Collaboration." Autopsy, p. 1, 2023. [Online]. Available: www.Autopsy.com

[12] G. Mishardila, "Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Facebook dan Twitter menggunakan metode Statik Forensik," Universitas Islam Riau Pekan Baru, 2020.

[13] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[14] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018, doi: 10.15408/jti.v10i1.6820.

[15] S. R. Ardiningtias, S. Sunardi, and H. Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis

Android Menggunakan Kerangka Kerja National Institute of Justice," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, p. 322, 2021, doi: 10.26418/jp.v7i3.48805.

[16] P. Mahardika Sulaksono and B. Santoso, "Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager," *J. Komput. Terap.*, vol. 8, no. Vol. 8 No. 1 (2022), pp. 132–142, 2022, doi: 10.35143/jkt.v8i1.5334.

[17] I. Artikel, "Kriminalisasi terhadap orang yang memberikan keterangan palsu untuk layanan sertifikat vaksinasi," no. Ciastech, pp. 261–268, 2022.

[18] I. Riadi and I. M. N. Rusydi Umar, "Forensic Analysis of Digital Evidence on Frozen Solid State Drives Using the National Institute of Standards and Technology (NIST) Method," *J. Insa. Comtech*, vol. 2, no. 2, pp. 33–40, 2017.

[19 Carolus Borromeus Mulyatno, "Jurnal Pendidikan dan Konseling ي ع ل م ه م ل ا م ن سن ل ِ ل ق ل ا ِ ب م ل ع ي ِ ل ً ا ِ ا م ل ع ٤ م," *J. Pendidik. dan Konseling*, vol. 4, no. 635, pp. 1349–1358, 2022.

[20] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Exposing Cybercrime," *CyberSecurity dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020.

[21] Y. Nugroho, "Tindak Pidana Terhadap Penggunaan Ijazah Palsu," *Mimb. INTEGRITAS J. Pengabdi.*, vol. 1, no. 2, pp. 168–177, 2020, [Online]. Available:

https://ojs.unars.ac.id/index.php/mimbarintegritas/article/view/2071

[22] M. Prof. Dr. Sarjon Defit, S.Kom, MSc., Efvy Zamirda Zam, M.Kom., *BELAJAR OTODIDAK WINDOWS FORENSIC UNTUK SEMUA VERSI WINDOWS*. Jakarta: PT Elex Media Komputindo Kelompok Gramedia, 2018.