ANALISIS PERBANDINGAN DATA RECOVERY MENGGUNAKAN TOOLS FORENSIK BERBASIS OPEN SOURCE PADA LINUX

MUHAMMAD FAHMI ABDILLAH
20917024

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Digital Forensik
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2021-2022

Lembar Pengesahan Pembimbing

Analisis Perbandingan Data Recovery Menggunakan Tools Forensik berbasis Open Source Pada Linux

MUHAMMAD FAHMI ABDILLAH
20917024

Yogyakarta, 10 Januari, 2023

Pembimbing I

Dr. Yudi Prayudi,S.Si., M.Kom.

Lembar Pengesahan Penguji

Analisis Perbandingan Data Recovery Menggunakan Tools Forensik berbasis Open Source Pada Linux

MUHAMMAD FAHMI ABDILLAH

20917024

Yogyakarta, {Bulan pengesahan, Tahun Pengesahan}

Tim Penguji,

Dr. Yudi Prayudi,S.Si., M.Kom.
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom
Anggota I

Irving Vitra Paputunga, S.T., M.Sc., Ph.D.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

Irving Vitra Paputunga, S.T., M.Sc., Ph.D.

Abstrak

Analisis Perbandingan Data Recovery Menggunakan Tools Forensik berbasis Open Source Pada Linux

Cyber Crime adalah salah satu kejahatan dunia maya yang sering terjadi di era teknologi sekarang ini. Banyak kasus yang terjadi di seluruh dunia seperti pencemaran nama baik, manipulasi data, pencurian data pribadi, perusakan data, dan lain sebagainya. Dampak yang diterima sangatlah besar karena data pribadi bisa disalahgunakan oleh pelaku yang tidak bertanggung jawab. Hal ini disebabkan karena kurangnya penanganan khusus yang merugikan perusahaan atau perorangan pada data pribadi. Untuk mengatasi masalah tersebut pemerintah membuat undang – undang ITE yang akan mengakibatkan pelaku pencurian informasi pribadi dapat dikenakan sanksi pasal 30 ayat (2) undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berbunyi "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik". Jika data tersebut telah hilang atau dihapus bahkan dirusak maka seorang ahli forensik mempunyai beberapa cara untuk mengembalikan data yang telah hilang atau rusak. Salah satunya adalah dengan menggunakan metode recovery data secara utuh menggunakan tools forensic yaitu Autopsy, FTK Imager, Foremost Recover & Testdisk Recover. Metode ini banyak digunakan oleh seorang ahli forensik untuk mencari kebenaran apakah benar data pribadi di ambil dan disalahgunakan. Sayangnya tools Autopsy dan FTK imager mempunyai kelemahan yaitu beberapa file data yang rusak atau corrupt tidak bisa dikembalikan secara utuh, hanya bisa di recovery tetapi tidak bisa dibuka. Akan tetapi tools Autopsy dan FTK Imager masih sering digunakan oleh ahli forensik sebagai alat bantu mereka untuk menemukan sebuah temuan temuan file. Maka dari itu penelitian ini memakai pendekatan metode menggunakan foremost recover dan testdisk recover, hanya saja metode ini tidak bisa di pakai menggunakan Graphic user interface (GUI) tetapi menggunakan CLI (Command Line) yang ada di system oprasi LINUX. Sebagai ahli forensik harus memahami cara untuk menggunakan metode tersebut seperti perintah – perintah yang akan dijalankan nantinya.

Kata kunci

cyber crime, teknologi, recovery, autopsy, ftk imager, foremost, testdisk

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 09 Januari 2022

Muhammad Fahmi Abdillah, S.Kom.

iv

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Muhammad Fahmi dan Yudi Prayudi (2022). Data Recovery Comparative Analysis Using Open-Based Forensic Tools Source on Linux. Article Published in International Journal of Advanced Computer Science and Applications (IJACSA), Volume 13 Issue 9, 2022.

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Muhammad Fahmi	Mendesain eksperimen (60%) Menulis *paper* (70%)
Dr. Yudi Prayudi, S.Si., M.Kom	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**".}

Halaman Persembahan

Alhamdulillah segala puji hanya Milik Allah Subhana Wa Ta'ala yang selalu memberikan rahmatnya kepada setiap makhluk,

Alhamdulillah, hasil dari kerja keras ini saya persembahkan untuk keluarga:

"Kedua orang tua"

Bapak Abdillah Taqwa dan Siti Fatimah

"Yayasan Airlangga Balikpapan"

Terkhusus Ibu Mulia Deviantie dan Ibu Elli Nur Amalia

Kata Pengantar

{Halaman ini merupakan bagian yang dipergunakan oleh penulis untuk menyampaikan kata pengantar dari laporan tesis ini.}

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

GUI	- Graphical User Interface
CLI	- Command Line Interface
SSD	- Solid State Drive
HDD	- Hard Disk
ITE	- Informasi dan Transaksi Elektronik
RAR	- Roshal Archive
PDF	- Portable Dokument Format
JPEG	- Joint Photographic Expert Groub

BAB 1
Pendahuluan

1.1 Latar Belakang

Data loss adalah kondisi dimana data yang telah dimiliki menjadi terkorupsi atau terhapus. Dari beberapa peneiliti banyak sekali perusahaan atau perorangan yg tidak sengaja menghilangkan data pribadinya. Sangat penting bagi analis forensik digital untuk memiliki tools yang tepat untuk memulihkan data. Semua perangkat menyimpan banyak data dan informasi penting yang selalu digunakan untuk kepentingan pribadi maupun perusahaan. Tool forensik digunakan oleh ribuan profesional forensik digital. Fungsionalitas tool forensik sangat bervariasi.

Saat ini, ada banyak tools recovery data yang sederhana beberapa fitur sudah disediakan secara konsisten hingga ekstraksi forensik yang lebih efektif, untuk mendapatkan data keseluruhan. Termasuk penyimpanan gambar, hashing data file, visualisasi data dan data carving pada gambar yang rusak. Akan tetapi tool seperti itu kebanyakan berbayar. Karena fitur pemeriksaan terbatas, data yang diekstraksi tidak dapat di porting langsung dengan sirkuit untuk mengekstrak bukti tambahan. Dalam penelitian ini saya menyajikan beberapa tools gratis yang bisa melakukukan recovery file data yang rusak berbasis open source pada Linux.

Pemulihan data adalah proses pemulihan sistem yang bermasalah atau hilang agar bisa pulih seperti sedia kala. Pemulihan data juga salah satu teknik forensik yang sering digunakan untuk mencari suatu artefak digital yang telah di hilang atau dihapus dari sebuah perangkat seperti handphone, komputer, dan laptop. Berbeda dengan backup data yang merupakan tindakan preventif yang sengaja dilakukan untuk melindungi data dengan cara mengcopy atau menyalin data ke media penyimpanan lainya.

Pada penelitian ini bertujuan untuk mengetahui tools forensik yang berguna saat ini dan masa yang akan datang. Untuk mengatasi terjadinya kehilangan data, seorang ahli forensika digital sangat dibutuhkan. Pengembalian data/recovery data adalah salah satu teknik yang harus dikuasai oleh ahli digital forensic. Jika terjadi suatu kerusakan data atau hilangnya data maka itu menjadi tugasnya seorang forensik untuk memulihkan kembali data yang telah hilang atau rusak. Beberapa kasus rusaknya data atau hilangnya data adalah salah satu tantangan yang harus dihadapi oleh ahli digital forensik. Ada beberapa tools recovery

data yang digunakan oleh ahli digital forensik seperti Autopsy, FTK imager, TSK recover, Foremost & Testdisk.

Pada kasus penelitian sebelumnya banyak ahli forensik menggunakan tools ini sebagai alat bantu untuk menemukan barang bukti. Tools ini sangat membantu untuk merecovery data yang telah hilang atau rusak, akan tetapi tools ini mempunyai suatu kelemahan tertentu, saat pengembalian data atau recovery data, yaitu data yang sudah rusak hanya bisa di recovery tetapi tidak bisa di buka secara utuh, maka dari itu solusi yang dibutuhkan adalah recovery secara utuh, data yang telah diambil / rusak bias direcovery dan dibuka kembali sama seperti sebelumnya. Untuk mengatasi masalah tersebut dengan itu seorang ahli forensik menggunakan tools recovery pada sebuah storage.

Recovery pada data yang akan di pulihkan berada di allocated space dan unallocated space. ruang tersebut menyimpan semua file yang masih tersedia dan bisa dibaca secara logical dan menyimpan semua file yang sudah tidak tersedia lagi bahkan sudah dihapus dari penyimpanan dan tidak bisa dibaca secara logical.

Dari beberapa referansi penelitian yang ditemukan bisa disimpulkan bahwa penelitian sebelumnya yang terkait dengan tema yang dibahas adalah banyak studi kasus yang menggunkan tools forensik dan memakai beberapa metode untuk memulihkan data yang telah hilang. Data tersebut tersimpan didalam storage yang berbeda-beda seperti : FlasDrive, HDD, SSD, RAM. Storage tersebut ada pada mobile device, komputer bahkan server. Metode recovery data juga berbeda-beda tergantung dari storage yang akan diproses. Salah satunya adalah menggunakan tools Autopsy atau tools forensik lainya. Tools ini sangat membantu ahli forensik untuk mencari file data yang hilang, seperti file JPG, MP4, PDF, PNG, Doc, Zip, Rar dan lain sebagainya. Hanya saja tools ini mempunyai kelemahan tertentu, saat pengambilan data atau recovery data yaitu data yang sudah rusak hanya bisa di recovery tetapi tidak bisa dibuka secara utuh, maka dari itu solusi yang dibutuhkan adalah recovery secara utuh, data yang telah hilang/rusak bisa direcovery dan dibuka kembali sama seperti sebelumnya.

Upaya untuk memberikan solusi pemulihan data untuk penanganan bukti digital pada suatu storage device seperti smartphone sudah pernah dibahas oleh (Wilson & Chi, 2017) menggunakan alat forensik digital agar mempermudah mengakuisisi data. Hal tepenting dari memulihkan data adalah metode recovery tersebut karena banyak cara untuk Mengakuisisi dan merecovery data.

Namun demikian ada beberapa peneliti yang memberikan ulasan tentang recovery data dengan Teknik yang berbeda dan device berbeda seperti yang dibahas oleh (Povar &

Bhadran, 2011) Teknik carving adalah yang dimaksud, Teknik ini yang membantu dalam 4 menemukan file yang disembunyikan atau dihapus dari media digital. Atau dengan Teknik akuisisi data yang sudah dibahas oleh (Jo et al., 2016) tentang akuisisi data dengan menggunakan tools forensik yaitu Autopsy. Teknik ini sangat membantu seorang ahli forensik untuk mengumpulkan data atau barang bukti.

Untuk mendukung pemecahan masalah tersebut maka dari beberapa data yang akan digunakan adalah beberapa video, dan gambar berupa file JPG, MP4 dan PNG yang sudah rusak atau corrupt. Dan nantinya akan diolah menggunakan beberapa tools forensik seperti Sleuth Kit Autopsy, Foremost, dan Testdisk recover. Data ini akan dimasukan ke dalam tools tersebut dan akan di proses recovery. Pada tahap akhir bisa dilihat perbandingan dari beberapa tools yang efektif untuk melakukan recovery secara utuh. Upaya untuk memberikan solusi pemulihan data untuk bukti digital pada suatu storage device seperti smartphone sudah pernah dibahas oleh Wilson & Chi menggunakan alat forensik digital agar mempermudah mengakuisisi data. Hal terpenting dari memulihkan data adalah metode recovery tersebut karena banyak cara untuk mengakuisisi dan merecovery data. Solusi yang ditawarkan untuk pemulihan data yang sempurna adalah dengan memakai metode live forensik dengan menggunakan tool formost recovery atau testdisk recover. Tools ini bisa melakukan akuisisi dat dari storage seperti HDD, SSD, FD, CD/DVD, zip, rar.

Penelitian ini bertujuan membandingkan parameter pada tools forensik yang akan digunakan untuk recovery data yang telah rusak atau terhapus berupa format file data yang akan dijadikan sebagai barang bukti untuk menyelesaikan kasus kejahatan Cybercrime. Recovery data pada penelitian ini yaitu dengan menggunakan metode live forensik pada Linux. Hasil dari penelitian ini diharapkan akan menambah ilmu di bidang digital forensik khususnya pada recovery data.

Live Forensik merupakan metode forensik yang digunakan ketika sistem dalam kondisi running. Hal ini karena data yang akan diambil kemungkinan bisa hilang ketika sistem dimatikan. Implementasi metode live forensik ini biasanya digunakan pada kasus memori yang datanya dapat ditulis atau dihapus atau bisa disebut volatile memory / non-volatile memory.

1.2 Rumusan Masalah

Merujuk pada latar belakang yang telah dipaparkan, dapat merumuskan masalah penelitian sebagai berikut :

1. Apakah data yang sudah hilang bisa di kembalikan?
2. Tools forensik apa yang bisa melakukan recovery secara utuh?
3. Apakah nilai hash MD5 berubah pada file yang rusak?
4. Bagaimana cara recovery data yang tidak terdeteksi di sebuah storage, seperti unallocated space?

1.3 Batasan Masalah

Agar penelitian ini fokus pada pokok permasalahan yang telah dirumuskan pada bagian sebelumnya, maka ruang pambahasan penelitian akan diteteap sebagai berikut:

1. Dalam penelitian yang akan dilakukan nantinya hanya menggunakan tools forensik FTK Imager, TSK Recover, Foremost, dan TestDisk saja
2. Dalam penelitian ini proses recovery hanya menggunakan file data berupa .rar yang berisi file JPG, PDF, dan MP4

1.4 Tujuan Penelitian

Tujuan penelitian yang diharapkan dari penelitian sebagai berikut:

1. Tujuan penelitian ini untuk memulihkan data file yang sudah terhapus dan rusak pada suatu penyimpanan
2. Mengetahui tools forensik yang bisa mengembalikan data file secara utuh dan tidak
3. Untuk mengetahui nilai hashing pada file yang rusak berubah atau tidak
4. Untuk mengetahui file yg akan di recovery pada allocated space dan unallocated space

1.5 Sistematika Penulisan

Dalam penyusuan penulisan ini untuk memberikan gambaran terkait dengan penjelasan maka digunakan sebuah sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Pada Bab ini menjelaskan Pendahuluan yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian.

BAB II LANDASAN TEORI

Pada Bab ini menjelaskan teori-teori yang terkait yang berhubungan dengan recovery data dan tools forensik yang digunakan.

BAB III METODOLOGI PENELITIAN

Pada Bab ini membahas tentang langkah-langkah penelitian recovery data dari persiapan sistem tools, akuisisi data, workflow metode recovery, analisis data, hingga hasil pembahasan laporan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan tentang cara recovery data pada setiap tools forensik yang digunakan dengan menggunakan metode live forensic dan analisis pengujian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan saran, berisi kesimpulan dari penelitian dan saran yang memerhatikan keterbatasan temuan dalam penelitian dan rekomendasi untuk penelitian selanjutnya

BAB 2
Tinjauan Pustaka

2.1 Permasalahan Umum Pemulihan Data

Dari beberapa referensi penelitian yang ditemukan bisa disimpulkan bahwa penelitian sebelumnya yang terkait dengan tema yang dibahas adalah banyak studi kasus yang menggunakan tools forensik dan memakai beberapa metode untuk memulihkan data yang telah hilang. Data tersebut tersimpan didalam storage yang berbeda beda seperti : FlashDrive, HDD, SSD, RAM. Storage tersebut ada pada mobile device, komputer bahkan server. Metode recovery data juga berbeda beda tergantung dari storage yang akan di proses. Salah satunya adalah menggunakan tools Autopsy atau FTK imager. Tools ini sangat membantu ahli forensik untuk mencari file data yang hilang, seperti file JPG, MP4, pdf, png, doc, zip, rar dan lain sebagainya. Hanya saja tools Autopsy atau FTK imager ini mempunyai suatu kelemahan tertentu, saat pengembalian data atau recovery data, yaitu data yang sudah rusak hanya bisa di recovery tetapi tidak bisa di buka secara utuh, maka dari itu solusi yang dibutuhkan adalah recovery secara utuh, data yang telah diambil / rusak bisa di recovery dan dibuka kembali sama seperti sebelumnya.

Untuk mendukung pemecahan masalah maka dari beberapa data yang akan di gunakan adalah beberapa video dan gambar yang berupa file JPG, MP4 dan PNG yang sudah rusak atau corrupt. Dan nantinya akan diolah menggunakan beberapa tools forensik seperti Sleuth Kit Autopsy, FTK Imager, Foremost dan Testdisk Recover. Data ini akan dimasukan ke dalam semua tools tersebut dan akan di proses recovery pada data tersebut. Lalu pada tahap akhir bisa dilihat perbandingan dari beberapa tools forensik, Yang nantinya bisa disimpulkan bahwa ada beberapa tools yang efektif untuk melakukan recovery secara utuh walaupun data tersebut telah hilang atau rusak.

File corrupt merupakan file yang tidak bisa di akses karena mengalami kerusakan. File bisa mengalami corrupt ketika berada dalam proses penyimpanan di memori komputer. Kemungkinan penyebab dari file corrupt berasal dari :

1. Aplikasi atau software yang bermasalah ketika meyimpan atau membuat sebuah file.
2. Tidak menutup file dengan benar
3. Hardisk yang bermasalah
4. virus

2.2 Penelitian Sejenis

Upaya untuk memberikan solusi pemulihan data untuk penanganan bukti digital pada suatu storage device seperti smartphone sudah pernah dibahas oleh (Wilson & Chi, 2017) menggunakan alat forensik digital agar mempermudah mengakuisisi data. Hal tepenting dari memulihkan data adalah metode recovery tersebut karena banyak cara untuk
Mengakuisisi dan merecovery data.

Namun demikian ada beberapa peneliti yang memberikan ulasan tentang recovery data dengan Teknik yang berbeda dan device berbeda seperti yang dibahas oleh (Povar & Bhadran, 2011) Teknik carving adalah yang dimaksud, Teknik ini yang membantu dalam menemukan file yang disembunyikan atau dihapus dari media digital. Dengan Teknik akuisisi data yang sudah dibahas oleh (Jo et al., 2016) tentang akuisisi data dengan menggunakan tools forensik yaitu Autopsy. Teknik ini sangat membantu seorang ahli forensik untuk mengumpulkan data atau barang bukti.

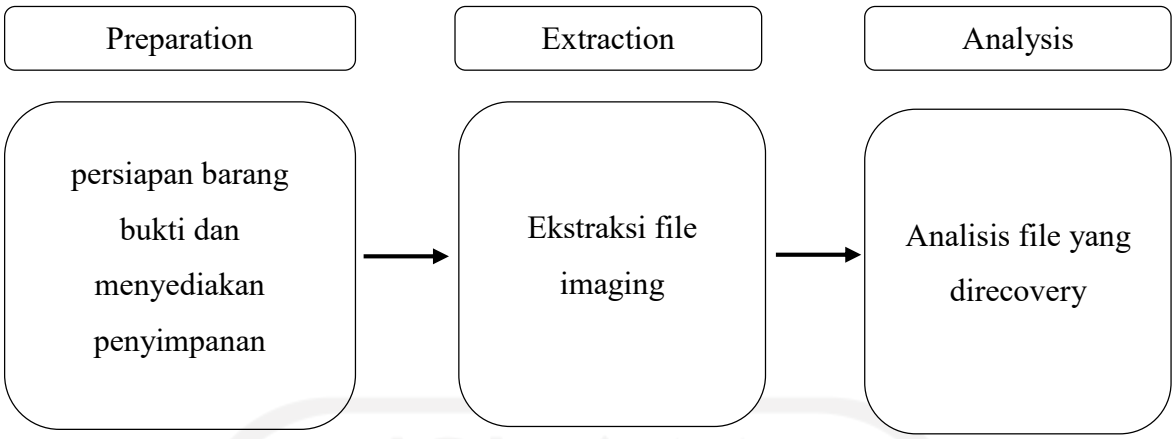
Solusi yang ditawarkan untuk pemulihan data yang sempurna adalah dengan memakai metode pemulihan data foremost (foremost recovery) atau metode pemulihan disk data (test disk recover). Metode ini juga bisa melakukan akuisisi data dari storage seperti : HDD, SSD, Flashdisk, CD/DVD, zip, rar dsb.

Penelitian ini bertujuan membandingkan parameter pada tools forensik yang akan digunakan untuk recovery data yang telah rusak atau terhapus berupa format file data yang akan dijadikan sebagai barang bukti untuk menyelesaikan kasus kejahatan Cyber Crime. Recovery data pada penelitian ini yaitu dengan menggunakan metode live forensik pada Linux. Hasil dari penelitian ini diharapkan akan menambah ilmu di bidang digital forensik khususnya pada recovery data.

2.3 Konsep Pengetahuan

2.3.1 Recovery

Recovery merupakan proses pemulihan sistem yang bermasalah atau hilang agar bisa pulih seperti sedia kala. Pemulihan data juga salah satu teknik forensik yang sering digunakan untuk mencari suatu artefak digital yang telah di hilang atau dihapus dari sebuah perangkat seperti handphone, komputer, dan laptop. Berbeda dengan backup data yang merupakan tindakan preventif yang sengaja dilakukan untuk melindungi data dengan cara mengcopy atau menyalin data ke media penyimpanan lainya. Tahapan dasar recovery dalam proses forensik digital yaitu Preparation, Ekstraction, dan Analysis.



Gambar 2.1 Tahapan dasar recovery

1. Preparation : Melakukan persiapan dengan menyediakan ruang penyimpanan untuk menyimpan data yang akan direcovery serta di ekstrak.
2. Extraction : Melakukan ekstraksi file dengan mengidentifikasi dan merecovery file yang telah terhapus. Ekstraksi file juga akan mengungkapkan karakterisitik struktur file, data yang telah terhapus, nama file, time stamps, ukuran dan lokasi file.
3. Analysis : Tahapan menganalisis hasil file yang telah dilakukan pemeriksaan. Sehingga dapat mengukur atau membandingkan tingkat efektifitas dari ekstraksi file data. serta dapat rekomendasi tools mana yang tepat untuk recovery file pada penelitian ini.

2.3.2 Hashing

Menurut (Deepakumara et al., 2001) Hash adalah kode alfanumerik dengan panjang tetap yang digunakan untuk mewakili kata, pesan, atau data. Hash pada dasarnya mempunyai dua karateristik yaitu :

1. Satu input yang sama akan selalu menghasilkan output yang sama
2. Tidak ada fungsi atau cara untuk mengembalikan output kemabali menjadi input

Hashing adalah proses menghasilkan fixed-size output dari variabel-sized yang dilakukan dengan penggunaan rumus matematika yang dikenal sebagai hash function. Setiap aset kripto menggunakan berbagai algoritma hashing yang berbeda untuk membuat berbagai jenis kode hash. Algoritma ini bertugas untuk menghasilkan alfanumerik acak. Kode alfanumerik ini sebenarnya adalah angka yang ditulis dalam notasi hexadecimal yang penulisanya sebagai berikut :

Hexadecimal : 0 1 2 3 4 5 6 7 8 9 A B C D E F

Decimal : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

2.3.3 MD5 Hash

Menurut (Kumar & Gupta, 2014) MD5 merupakan singkatan dari Message Digest algoritma yaitu fungsi hash kriptografi. Algoritma ini digunakan untuk melakukan pemeriksaan integritas file dalam berbagai situasi. Kerap digunakan bersama *hash value* 128-bit, MD5 merupakan fungsi *hash* yang dimanfaatkan dalam sejumlah aplikasi keamanan, salah satunya Internet standar (RFC 1321). MD sendiri adalah singkatan dari *message digest* dan MD5 yang sekarang sering digunakan adalah pengganti MD4 yang dikembangkan Profesor Ronald Rovest dari MIT. pada tahun 1991 sebagai fungsi hash kriptografik untuk keperluan keamanan data (hingga saat ini masih banyak tabel "user" yang menggunakan MD5 untuk mengacak password agar tidak disimpan sebagai plaintext di database), dan bisa juga digunakan untuk mengecek integritas file.

2.3.4 Digital Forensik

Digital Forensik adalah proses ilmiah atau upaya ilmiah yang didasarkan pada ilmu mengumpulkan, menganalisis, dan menyajikan bukti dalam proses pengadilan untuk membantu pengungkapan kejahatan melalui pengungkapan bukti yang disahkan oleh hukum dan peraturan.

Digital forensik merupakan salah satu sarana untuk membantu penyidik dalam kewenangannya melakukan penyelidikan dan penyidikan yang diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Kitab Undang-undang Hukum Acara Pidana (KUHAP). Untuk dapat melakukan penerapan ilmu digital forensik dalam proses penyidikan perlu pemahaman yang lebih dalam mengenai ilmu teknologi selain daripada ilmu hukum yang biasa diterapkan dalam proses pengadilan pidana. Penerapan ilmu digital forensik dibagi menjadi 4 (empat) yaitu

1. Forensik Komputer yaitu penyidikan yang dilakukan terkait dengan data aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas log
2. Forensik Jaringan yaitu penyidikan yang dilakukan kepada data yang diperoleh berdasarkan pengamatan jaringan.

3. Forensik aplikasi yaitu penyidikan yang dilakukan dengan penggunaan aplikasi tertentu. Aplikasi tersebut memiliki fungsi audit karena aplikasi tersebut terdapat fitur untuk meninggalkan jejak suatu perangkat.
4. Forensik perangkat merupakan penyidikan dengan tujuan untuk mendapatkan serta mengumpulkan data dan jejak log tertentu dalam suatu perangkat digital seperti smart phone.

2.3.5 Forensik komputer

Penyidikan yang dilakukan terkait dengan data aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas log. Forensika digital pada awalnya lebih dikenal dengan sebutan forensik komputer hal ini disebabkan bukti yang dikumpulkan terbatas hanya pada sebuah perangkat komputer. Pertumbuhan teknologi membawa sebuah variasi kemampuan penyimpanan dan pengiriman data hingga meningkatnya kejahatan siber mendorong proses digital forensik untuk menjawab permasalahan siber. Tahapan dasar recovery dalam proses forensik digital yaitu Preparation, Ekstraction, dan Analysis.

2.3.6 Forensik Jaringan

Forensik jaringan adalah salah satu sub-cabang forensik digital di mana data yang dianalisis adalah lalu lintas jaringan yang menuju dan dari sistem yang sedang diamati. Definisi forensika jaringan adalah proses menangkap, merekam, dan menganalisis aktivitas jaringan untuk menemukan bukti digital adanya penyerangan atau kejahatan yang dilakukan yang dilakukan dengan menggunakan jaringan komputer. Secara umum, proses forensika jaringan berupa CIA (Capture, Identify and Analyze).

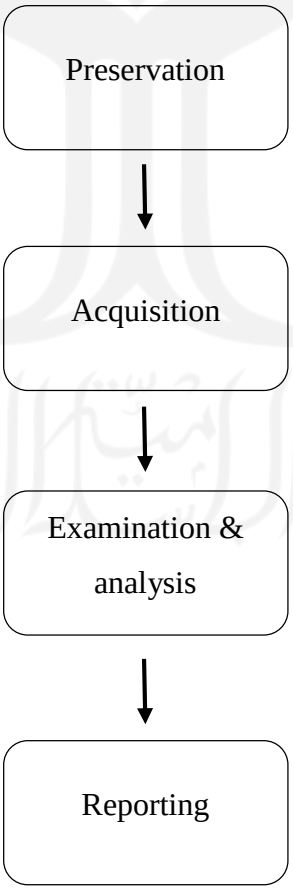
2.3.7 Forensik Aplikasi

Forensik aplikasi adalah kegiatan investigasi yang dilakukan untuk menemukan bukti digital yang memperkuat atau memperlemah bukti fisik suatu kasus dengan media perangkat komputer.digital. Metode penelitian yang mengacu pada pedoman forensik perangkat mobile yang dibuat oleh National Institute of Standards and Technology (NIST) dengan langkah-langkah sebagai berikut :

1. Preservation : Tahap ini merupakan awal dalam metode mobile forensik, yaitu mencari, mengumpulkan dan mendokumentasikan barang bukti. Selain itu pada tahapan ini dilakukan persiapan dan perencanaan bagaimana smartphone yang

menjadi barang bukti akan di analisis beserta tools yang diperlukan untuk membantu proses analisis forensik.

2. Acquisition : Tahap ini melakukan proses imaging atau pengkloningan perangkat mobile, baik memori internal maupun external berdasarkan prosedur yang sudah ditentukan. Proses pengambilan data pada setiap perangkat smartphone bisa berbeda-beda caranya, hal ini dipengaruhi seperti asal vendor smartphone, jenis protokol transfer data yang digunakan, dan versi operating system yang di pakai pada smartphone. Pada umumnya jenis perangkat mobile dan data yang akan di ekstrak menentukan tools dan teknik yang akan digunakan pada proses penyelidikan.
3. Examination & analysis : Tahap ini bertujuan mengangkat atau mengungkap sebuah bukti digital dan melakukan proses analisa terhadap hasil acquisition untuk mendapatkan data yang di inginkan berkaitan dengan kasus penyidikan.
4. Reporting : Tahap ini merupakan proses mempersiapkan laporan dan menyimpulkan hasil analisis mencakup deksripsi tindakan yang diambil, menjelaskan tools dan prosedur yang dipilih dalam proses analisis, menentukan tindakan lanjutan jika diperlukan.



Gambar 2.2 Tahapan NIST

2.3.8 Live forensik

Suatu teknik analisis dimana menyangkut data yang berjalan pada system atau data volatile yang umumnya tersimpan pada Random Access Memory (RAM) atau transit pada jaringan. Teknik live forensics ini sangat bergantung pada keadaan komputer yang sedang menyala, karena membutuhkan data yang berjalan pada Random Access Memory (RAM). Data pada RAM disebut juga data volatile atau data sementara yaitu data yang hanya terdapat saat komputer menyala jika komputer mati maka data itu akan hilang. Data volatile ini berisi data penting seperti username, password, file akses, file modifikasi, aplikasi yang digunakan, kata kunci pencarian.

2.3.9 Tools Forensik

Tools forensik merupakan alat bantu penyidik untuk mencari jejak digital pada sebuah kasus. Biasanya tools forensik yang sering digunakan penyidik seperti :

1. Autopsy
2. FTK Imager
3. Winhex
4. Mobiledit
5. Helix forensic

Tabel 2.1 Review Penelitian

No	Paper Utama	Keywords	Isu	Metode	Storage yang digunakan			Tools yang digunakan	Target
					HDD	SSD	ROM		
1	(Wilson & Chi, 2017)	App; Digital forensics; IOS; Open source tools; Smartphone	Akuisisi data dari tools forensik pada smartphone IOS	Analisis akuisisi data atau pengembalian data	-	-	√	IBackup extraktor	Storage ROM pada IOS
2	(Baek et al., 2021)	Ransomware; data recovery; flash-based SSDs; malware detection	Sistem pertahanan ransomeware pada SSD	Signature Base detection & Content base detection	-	√	-	SSd Assisted Recovery	Invariant Features of Ransomware
3	(Winter, 2013)	recovery; HDDs; SSDs;	Proses recovery pada HHD dan SSD	Recovery secara utuh pada HHD dan SSD	√	√	-	RAID Arrays	Physical Media destruction

4	(Jo et al., 2016)	Digital Forensics; Metadata; Recovery; UFS	Analisis struktur UFS	Metode pemulihan data yang dihapus dengan Teknik baru	√	√	-	UFS Explorer, FTK(Forensic ToolKit)	data onto Linux or Android smartphone's file system which is called Ext 2/3/4 [2~4]
5	(Na et al., 2014)	Video file restoration; corrupted video data; frame-based recovery; video file specifications	recovery video rusak menggunakan video codec spesifikasi	mengekstrak video dari Sebagian video yang di pulihkan sesuai dengan spesifikasi codec	√	-	-	The sleuth kit Autopsy	corrupted video files irrespective of a file system
6	(Campos et al., 2016)	Autopsy Forensic Browser; Foremost; data	Pengambilan Informasi untuk menganalisis alat forensik	Memulihkan data penyimpanan pada perangkat	√	√	-	The sleuth kit Autopsy	Storage file pada HHD / SSD

		recovery; phases of computer forensics; storage device	komputasi (autopsy forensic						
7	(Putra & Widiatedja, 2008)	criminal act of theft; cyber crimes; legal protection; restitution	Dampak negative dari perkembangan teknologi dan Hukum bagi korban pencurian informasi pribadi melalui dunia cyber	-	-	-	-	-	Bukan penelitian eksperimental
8	(Povar & Bhadran, 2011)	criminal act of theft; cyber crimes; legal	Data carving	Metode ekstraksi yang harus memiliki	√	√	-	Disk analysis tool	digital images (jpeg, gif, bmp, png), html,

		protection; restitution		header dan footer agar bisa di analisis					zip, compound documents (doc, ppt, excel, thumbs.db), pdf, video (avi, dat, mp4, mov, wmv, 3gp)
9	(Ryu et al., 2014)	Content-aware image resizing; Image forensics; Seam carving; Seam insertion	trace of seam carving	Metode yang di gunakan adalah detektor yang menyelidiki hubungan antara piksel atau disebut dengan novel forensik technique	√	√	-	Seam carving detection	Seam carved

10	(Al-Sabaawi et al., 2019)	Android Forensics; Digital Forensics; Mobile Forensics; Mobile Security	Akuisisi data file pada android	Analisis pengambilan data	-	-	√	AFLogical application, FTK imager, Autopsy	data pada storage android
11	(Dibb & Hammoudeh, 2013)	Android OS Forensics; Mobile Forensics	Recovery data pada smartphone android dengan menggunakan toolkit open source	Analisis Pemulihan data pada Smartphone Android	-	-	√	Sleuthkit Autopsy	data pada storage android
12	(Breeuwsma & Jongh, 2007)	embedded systems; flash memory;	Recovery data pada Flash Memory	Analisis metode pemulihan data pada flash memory	√	-	-	Flasher tool	Data pada flash memory

		physical analysis							
13	(Guo & Slay, 2010)	data recovery; digital forensic tools; validation; verification	Recovery data function	Analisis sistematis forensik digital dengan memetakan fungsi fundamental	√	-	-	Electronic Evidence (EE)	Data pada Komputer
14	(Buchanan-Wollaston et al., 2013)	Digital forensic tools; data recovery; testing	Data recovery	Analisis terhadap hashing data dari seluruh gambar disk	√	-	-	FTK Imager	Data pada Komputer
15	(Pratama, 2021)	computer forensics; data; industry photorec; secure data recovery	Data recovery computer forensic	Memulihkan data dari penyimpanan media	√	-	-	Photorec	Storage data dari komputer

16	(Mohite & Ardhapurkar, 2015)	Cloud Computing; Computer Forensic; Digital Evidence; Forensic Investigation	Implementasi pada cloud komputer	Metode pemulihan data pada cloud computing	-	-	-	- AIR (Automated Image Restore) - TSK (The Sleuth Kit) - AFB (Autopsy Forensic Browser	Data pada Cloud
17	(Plum & Dewald, 2018)	APFS; Data recovery; Digital forensics; File systems; Open Source; Tool	Recovery file data pada perangkat apple	Metode pemulihan file data pada APFS	√	-	√	APFS	Storage pada perangkat komputer dan smartphone
18	(Guo et al., 2009)	Computer forensics; Searching; Validation; Verification	Recovery data function	Validasi dan verifikasi pada software komputer	√	-	-	Electronic Evidence (EE)	Data pada Komputer

19	(Hilgert et al., 2017)	File systems; Forensic analysis; Pooled storage; The Sleuth Kit; ZFS	Recovery data storage	Pembaruan model carrier untuk menganalisis sistem file penyimpanan gabungan	√	-	-	Sleuth Kit Autopsy	ZFS - File sistem pada storage, cloud
20	(Riadi et al., 2019)	Forensik, Recovery, Smartphone, Android, NIJ.	Recovery pada smartphone android	Metode ekstraksi pada storage smartphone	-	-	√	- MOBILedit, - Wondershare dr. Fone for Android - Belkasoft Evidence Center	Storage pada android
21	(Simanjuntak & Panjaitan, 2021)	Recovery Data, Komputer Forensik, Winhex, X-Way Forensik	Proses recovery data pada komputer	Metode ekstraksi file cloningan pada image	√	-	-	- X way Forensic - WinHex - FTK - Scalpel - Ddrescue	
22	(Zuhriyanto et al., 2017)	DFRWS; Digital	Perbandingan Tools forensik	Metode Digital	-	-	√	MOBILedit Forensic Express	Smartphone Android

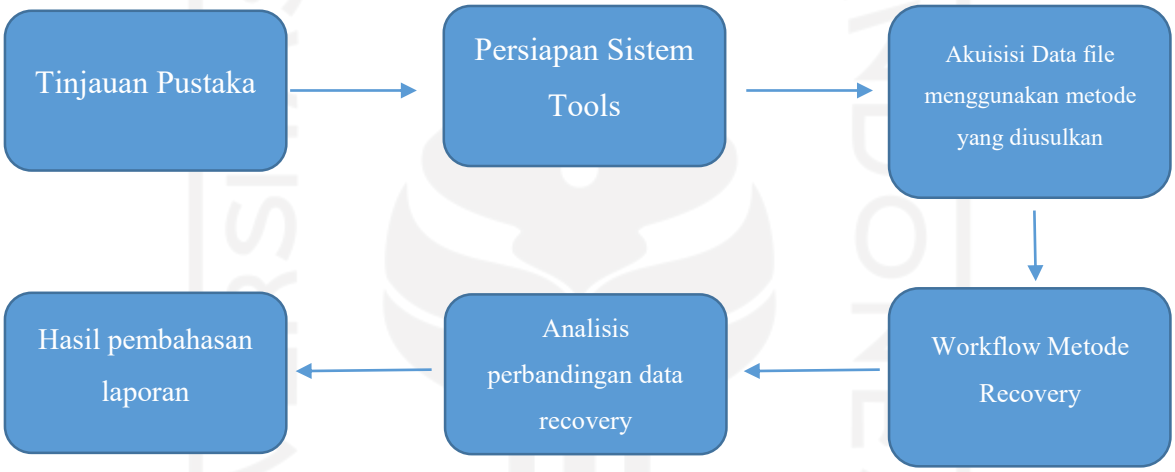
		Forensics; Mobile Forensics; Social Media; Twitter	pada smartphone	Forensics Research Workshop (DFRWS)					
23	(Handrizal, 2017)	data; data recovery; data yang; dihapus; forensik	Recovery data pada USB Flash-Drive	Memulihkan data penyimpanan pada USB Flash-Drive	√	-	-	Puran file recovery, Glary Undelete dan Recuva Data Recovery	FlashDrive
24	(Panjaitan & Sitepu, 2021)	IT Forensic Tools, Imaging File, Forensic Toolkit (FTK) Imager, Encase Imager,	Ekstraksi file imaging	Metode yang digunakan adalah Desktop forensik, live forensik, dan network forensik	√	√	-	- ProDiscover Basic - Encase - Belkasoft	

		Belkasoft Acquisition							
25	(Plianda & Indrayani, 2022)	cybercrime; instan messaging; mobiledit; oxygen forensic; whatsapp	Perbandingan performa tools forensik pada smartphone	Metode akuisisi data atau pengembalian data, NIST	-	-	√	FTK imager dan MOBILedit	Storage pada smartphone

BAB 3
Metodologi Penelitian

3.1 Pendahuluan

Metodologi penelitian adalah langkah-langkah yang harus ditempuh untuk kepentingan penelitian. Langkah-langkah tersebut dibuat supaya menjawab masalah yang muncul secara sistematis dan logis sehingga dilakukan proses ilmiah untuk menyelesaikan masalah yang muncul.



Gambar 3.1 Metodologi Penelitian

3.2 Tinjauan Pustaka

Tujuan dari Tinjauan pustaka ini dilakukan untuk mengumpulkan bahan-bahan informasi mengenai topik penelitian yang dapat bersumber dari artikel, paper, jurnal, makalah, yang berupa teori, laporan penelitian, atau penemuan sebelumnya dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan teori-teori tentang digital forensik, barang bukti, recovery, sehingga dapat menunjang tujuan akhir dilakukannya penelitan ini.

3.3 Persiapan Sistem Tools

Merupakan tahapan dalam mempersiapkan spesifikasi hardware dan software yang digunakan dalam penelitian seperti melakukan perancangan dan implementasi analisis perbandingan recovery data dengan menggunakan flashdisk. seperti melakukan instalasi dan konfigurasi sistem, konfigurasi sistem operasi yang ada dalam komputer fisik yaitu microsoft windows 11 Home. Agar implementasi eksperimental dapat berjalan dengan baik,

maka perlu adanya hardware dan software komputer fisik sebagai alat dan bahan penelitian, berukut ini alat dan bahan yang digunakan dalam melakukan bahan penelitian eksperimen :

1. Laptop MSI Modern 14 dengan spesifikasi :
   a) Processor : Intel® Core™ I7-10510U CPU @1.80GHz
   b) Memory : 512 GB SSD / 8 GB RAM
   c) OS : Windows 11 Home Insider 64-bit
2. FlashDisk 8 GB
3. Oracle VM Virtual Box (CSI Linux)
4. TSK Recover tool
5. FTK Imager
6. Foremost Recover
7. TestDisk Recover

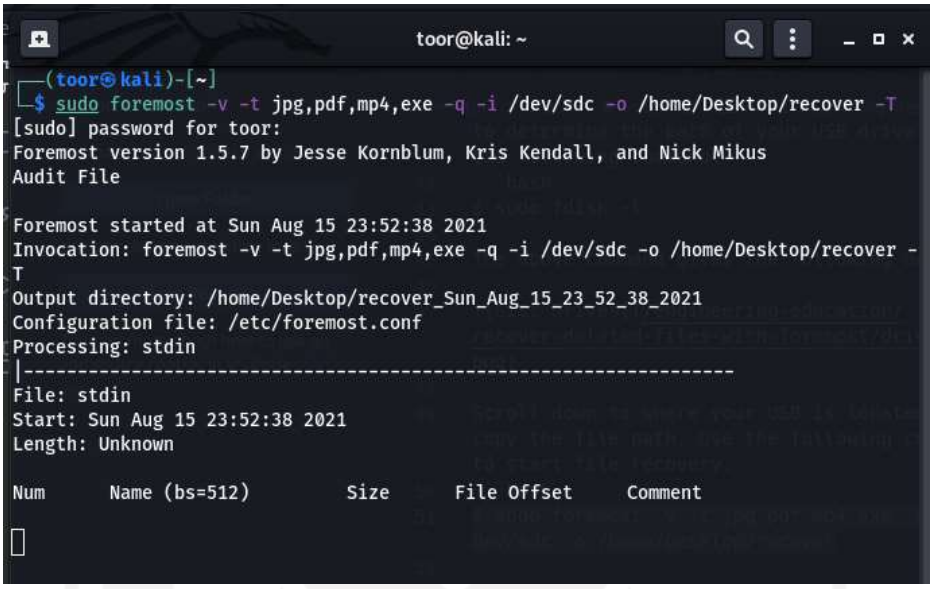
3.4 Metodologi Yang Diusulkan

3.4.1 Metode Foremost Recover

Metode foremost recover ini dibuat pada Maret 2001 untuk menduplikasi fungsionalitas program DOS carving untuk digunakan pada platform Linux. Foremost awalnya ditulis oleh agen khusus kris kendall dan jesse Kornblum dari kantor investigasi khusus Angkatan udara AS. Pada tahun 2005, program ini dimodifikasi oleh Nick mikus, seorang peneliti di pusat studi keamanan informasi dan penelitian sekolah pascasarjana angakatan laut sebagai bagian dari tesis master, modifikasi ini termasuk peningkatan akurasi dan tingkat ekstraksi foremost.

Metode foremost recover ini dirancang untuk mengabaikan jenis sistem file yang mendasari dan langsung membaca dan menyalin bagian dari drive ke dalam memori komputer. Untuk melakukan proses tersebut foremost recover ini menggunakan proses yang dikenal sebagai file carving mencari memori ini untuk jenis file header yang cocok dengan yang ditemukan dalam file konfigurasi foremost. Terutama digunakan dari antarmuka baris perintah, tanpa opsi antarmuka pengguna grafis yang tersedia. Metode foremost ini mampu memulihkan jenis file tertentu seperti JPG, GIF, PNG, BMP, AVI, EXE, MPG, WAV, RIFF, WMV, MOV, PDF PLE, DOC, ZIP, RAR, HTM dan CPP. Ada file konfigurasi biasanya ditemukan di /usr/local/etc/foremost.conf yang dapat digunakan untuk menentukan jenis file tambahan. Terutama dapat digunakan untuk memulihkan data dari file gambar, atau langsung dari

hardrive yang menggunakan sistem file ex3, NTFS, atau FAT. Terutama juga dapat digunakan melalui komputer untuk memulihkan data dari Iphone.



Gambar 3.2 Contoh Metode Foremost Recover

3.4.2 Metode TestDisk Recover

Testdisk adalah alat pemulihan data yang gratis dan opensource, yang dirancang untuk memulihkan data dari partisi yang dihapus atau hilang. Tool ini berbasis CLI tidak ada versi user interfacenya, dengan ini seorang ahli digital forensik bisa menghidupkan kembali partisi – partisi yang tidak dapat di boot yang disebabkan oleh factor-faktor seperti penghapusan tabel partisi secara sengaja maupun tidak sengaja, dan serangan malware tentunya. Selain itu Testdisk ini bisa melakukan beberapa hal lainya seperti :

1. Recover sector boot FAT32 dari cadanganya
2. Recover sector boot FAT12/FAT16/FAT32
3. Recover sector boot NTFS
4. Memulihkan sector boot NTFS dari cadanganya
5. Memperbaiki MFT menggunakan cermin MFT
6. Temukan SuperBlock cadangan ext2/ext3/ext4
7. Membatalkan penghapusan file dari sistem file FAT, exFAT, NTFS, dan ext2
8. Copy file dari partisi FAT,exFat, NTFS dan ext2/ext3/ext4 yang dihapus

Gambar 3.3 Contoh Metode TestDisk Recovery

3.5 Workflow Metode Recovery

Workflow process dari metode foremost recover ini atau biasa disebut dengan Langkah-langkah atau tahapan dari dari metode yang harus diikuti oleh pemeriksa digital dalam menjalankan aktivitas digital. Seperti contoh dibawah ini :

Gambar 3.4 Tahapan Recovery Data

4. Preparation : Melakukan persiapan dengan menyediakan ruang penyimpanan untuk menyimpan data yang akan direcovery serta di ekstrak.
5. Extraction : Melakukan ekstraksi file dengan mengidentifikasi dan merecovery file yang telah terhapus. Ekstraksi file juga akan mengungkapkan karakterisitik struktur file, data yang telah terhapus, nama file, time stamps, ukuran dan lokasi file.

6. Analysis : Tahapan menganalisis hasil file yang telah dilakukan pemeriksaan. Sehingga dapat mengukur atau membandingkan tingkat efektifitas dari ekstraksi file data. serta dapat rekomendasi tools mana yang tepat untuk recovery file pada penelitian ini.

3.6 Analisis Perbandingan Data Recovery

Analisis perbandingan data recovery merupakan tahapan data recovery yang telah di ektraksi menggunakan tools forensik seperti : FTK Imager, TSK recover, Foremost, dan testdisk recovery. File data seperti JPG, PNG, dan MP4 pada flasdisk, HDD, SSD dan penyimpanan lainya yang sudah rusak akan diolah dengan metode recovery file data dengan menggunakan beberapa tools, yang nantinya akan menemukan perbedaan yang berpengaruh dalam recovery data pada tools tersebut Agar bisa dibuka kembali secara utuh. Dari hasil investigasi forensik nantinya akan ada beberapa contoh tabel yang memetakan hasil dari recovery tersebut dapat dilihat pada tabel 3.1

Tabel 3.1 Hasil Recovery data Flasdisk

Storage	Flasdisk	
Tools	TSK recover, FTK imager, Foremost, Testdisk	
Jenis File	JPG, PNG, MP4	
Status recovery	Berhasil	Tidak berhasil
	√	

Tabel 3.2 Hasil Recovery data HDD / SSD

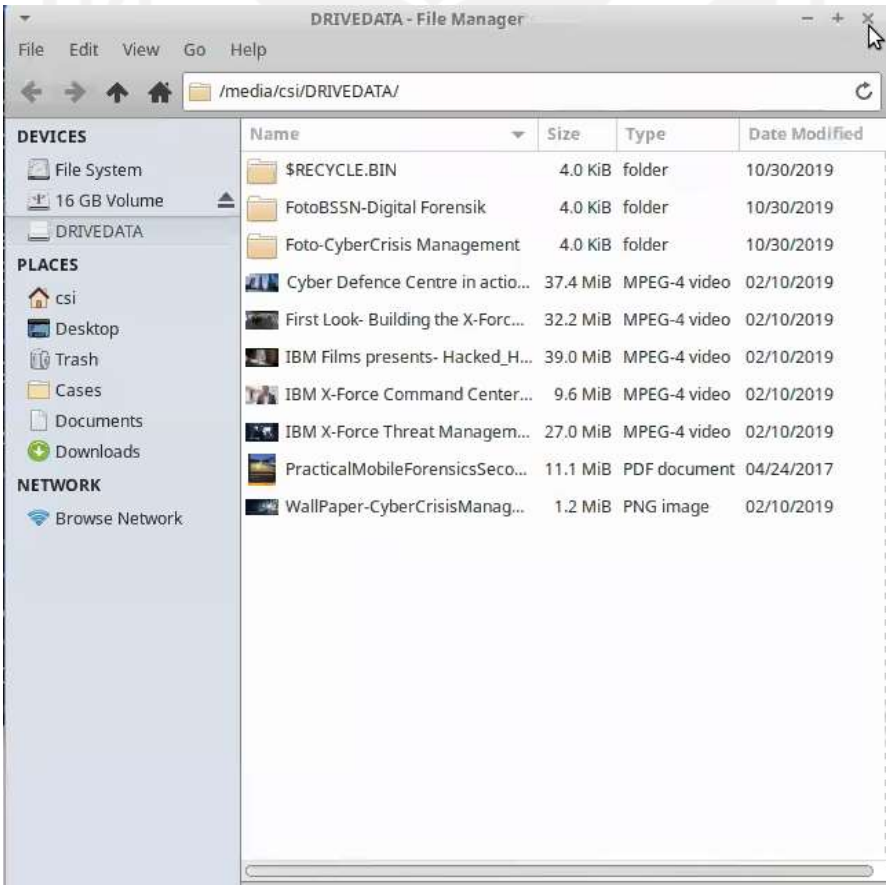
Storage	HHD / SSD	
Tools	TSK recover, FTK imager, Foremost, Testdisk	
Jenis File	JPG, PNG, MP4	
Status recovery	Berhasil	Tidak berhasil
	-	-

BAB 4
Hasil dan Pembahasan

Bab ini membahas secara lengkap tahapan-tahapan recovery dengan menggunakan beberapa tools forensik sebagai metode live forensik. Recovery memiliki 3 tahapan yaitu Preparation, Extraction, dan Analisis yang akan diuraikan secara detail pada bagian pembahasan ini.

4.1 Preparation

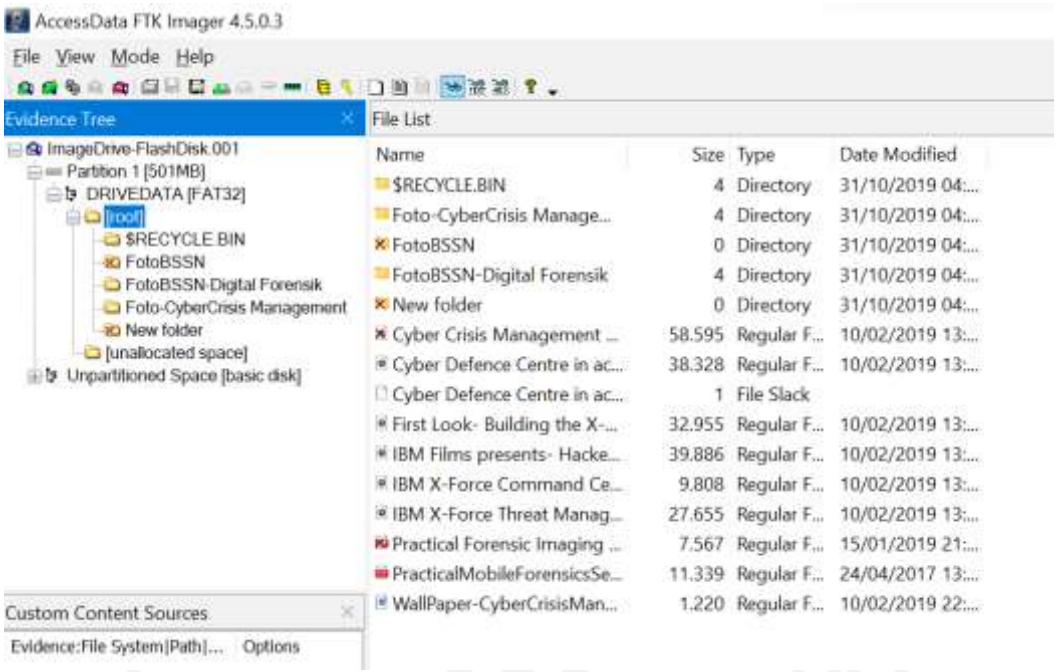
Pada tahap ini dilakukan persiapan dengan menyediakan ruang penyimpanan. untuk menyimpan data yang akan direcovery serta di ekstrak. Persiapan ini menggunakan storage flashdisk yang berisi file image berbentuk rar dengan nama ImageDrive-FlashDisk.001 yang tidak bisa dibuka dan berisi file seperti JPG, PNG, PDF, MP4. Hasil dan pengujian yang dilakukan bertujuan untuk mendapatkan file recovery yang seutuhnya sehingga dapat melihat perbandingan antara tool-tool forensik yang digunakan. File image tersebut akan di mounting terlebih dahulu melalui CSI Linux menggunakan Command Line "sudo losetup -Pf ImageDrive-FlashDisk.001" seperti gambar 4.1



Gambar 4.1 Hasil Mounting ImageDrive-FlashDisk.001

4.2 Extraction

Pada tahap ini, dilakukan ekstraksi file dengan mengidentifikasi dan merecovery file yang telah terhapus. Ekstraksi file juga akan mengungkapkan karateristik struktur file, data yang telah terhapus, nama file, file stamps, ukuran dan lokasi file. Tools yang dipakai untuk membantu proses ekstraksi tersebut menggunakan FTK Imager pada linux. Dan untuk recovery data menggunakan tools Foremost dan TestDisk seperti gambar 4.2



Gambar 4.2 Hasil Ekstraksi ImageDrive-FlashDisk.001dengan menggunakan FTK Imager

Pada gambar diatas diketahui ada beberapa file yg teridentifikasi telah terhapus dan tidak bisa dibuka, Maka akan dilakukan proses recovery terhadap file tersebut.

Tabel 4.1 Hasil File Yang Telah Terhapus

No	File data	QTY	File rusak
1	JPG	12	3
2	PDF	2	1
3	MP4	6	1

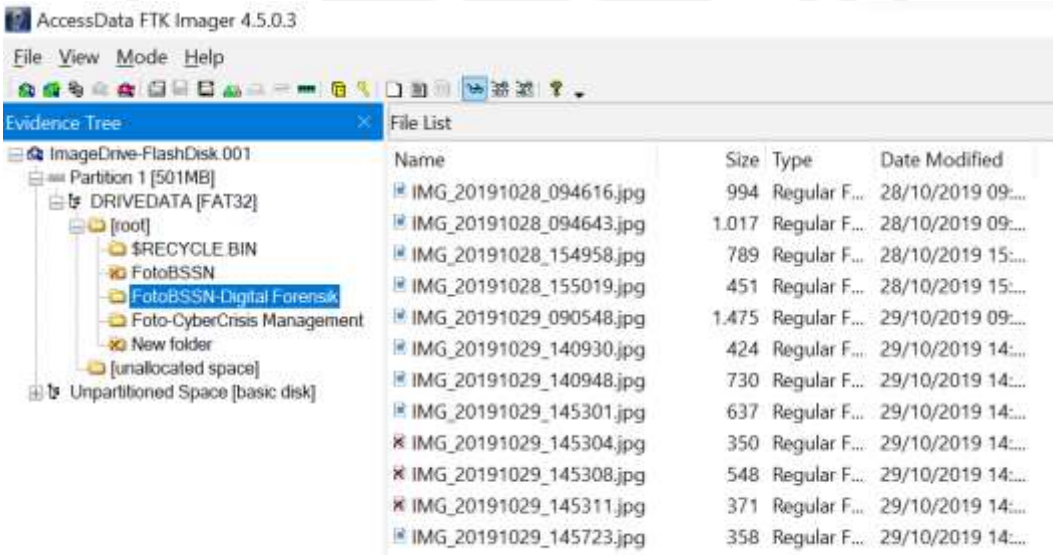
File rusak tersebut akan di check MD5 hash untuk membandingkan file yang rusak apabila cocok maka file tersebut masih utuh dan tidak corrupt. Setelah di check menggunakan MD5 teridentifikasi hashing file seperti pada tabel 4.2

Tabel 4.2 hasil awal hashing MD5 File Corrupt

No	File data rusak	MD5 Hash
1	JPG 1	459d4d4d38993bb270d9f8d7d5029a5c
2	JPG 2	9c8ea5f8f9886a21398a63b58684f9c6
3	JPG 3	e76cebfd00342d100fb12d5daa9b3443
4	PDF	120695b94e5d3bf867862eb42715a4a4
5	MP4	677f7dca67cdf3741d3f924a668fc2b2

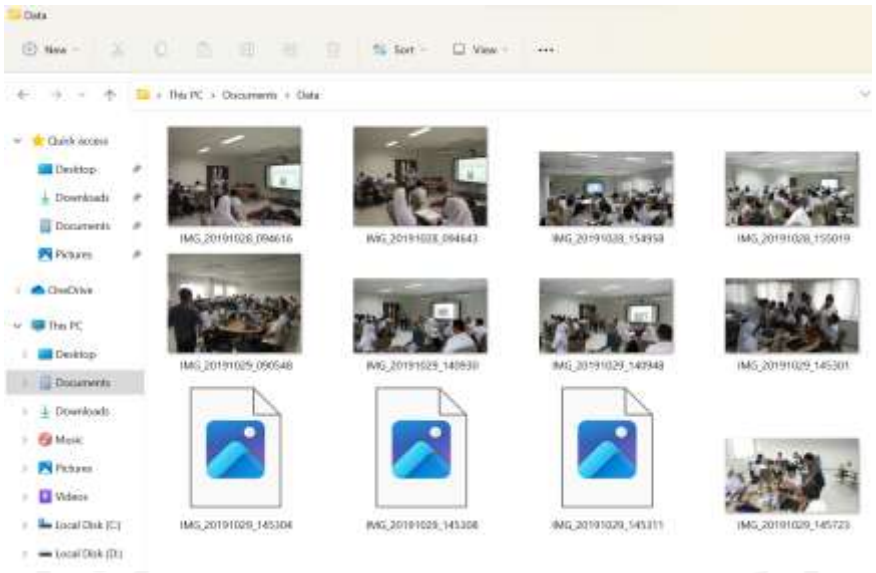
4.2.1 Proses Recovery FTK Imager

Pada tahap ini proses pemulihan data dengan menggunakan beberapa tools untuk perbandingan yaitu FTK Imager, TSK recover, Foremost dan TestDisk recover. File yang telah di ekstrak kemudian akan dilakukan proses recovery. Tool FTK Imager ini adalah salah satu tool recovery open source yang ada di windows, proses recovery dengan menggunakan tool FTK Imager dapat dilihat pada gambar 4.3



Gambar 4.3 Proses Recovery Menggunakan FTK Imager

Terlihat pada gambar 4.3 teridentifikasi ada 12 file JPG, dan semua file tersebut berhasil di recovery dengan cara di eksport, tetapi 3 diantaranya tidak bisa dibuka atau rusak seperti gambar 4.4



Gambar 4.4 Hasil Ekport file JPG dari FTK Imager

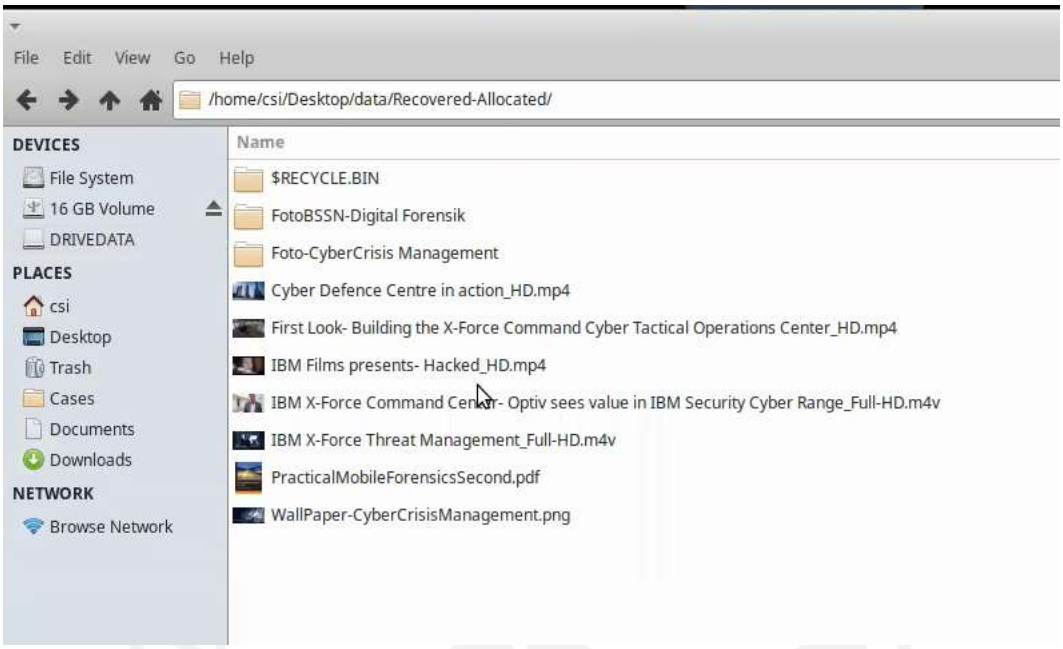
4.2.2 Proses Recovery TSK

Pada tahap recovery TSK recover perlu dilakukan penginstalan tools terlebih dahulu pada CSI Linux dengan menggunakan command " apt install sleuthkit ". Tools TSK ini bisa merecover Allocated file only dan recover all file termasuk UnAllocated, bisa dilihat seperti gambar 4.5

```
oot@csi:/home/csi/Desktop/data# tsk_recover
issing output directory and/or image name
sage: tsk_recover [-vVae] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o sector_offset] [
] image [image] output_dir
        -i imgtype: The format of the image file (use '-i list' for supported types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: The file system type (use '-f list' for supported types)
        -v: verbose output to stderr
        -V: Print version
        -a: Recover allocated files only
        -e: Recover all files (allocated and unallocated)
        -o sector_offset: sector offset for a volume to recover (recovers only that volume)
        -d dir_inum: Directory inum to recover from (must also specify a specific partition
```

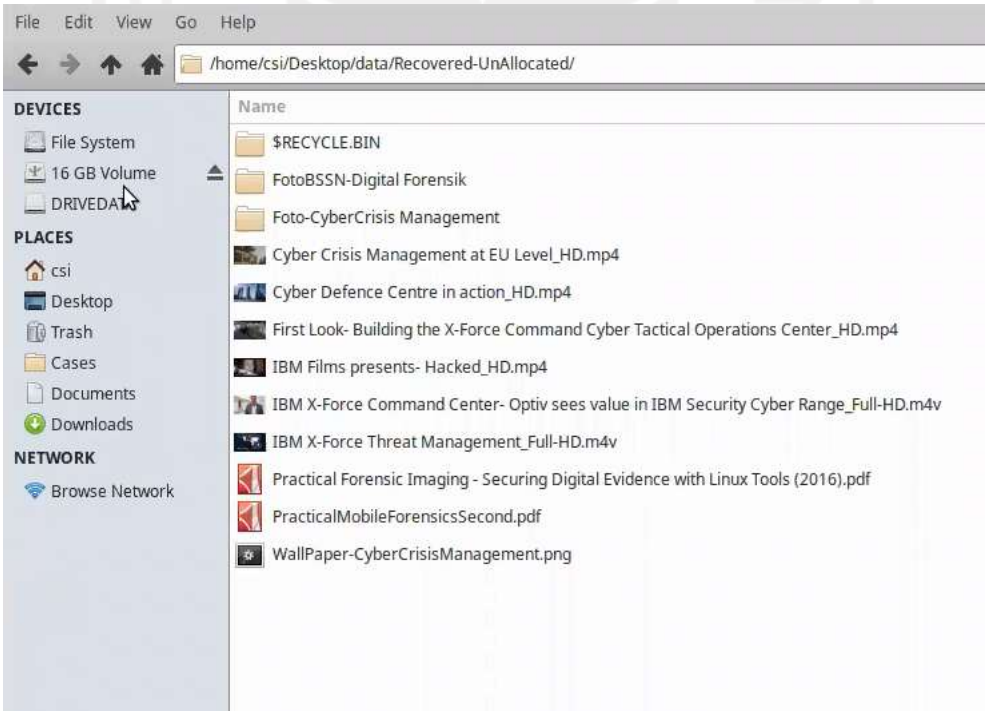
Gambar 4.5 Proses Recovery Menggunakan TSK Recover

Tahap selanjutnya adalah recovery file allocated terlebih dahulu dengan menggunakan command " tsk_recover –a /dev/loop0p1 Recovered-Allocated " dan mendapatkan hasil recovery 52 file seperti pada gambar 4.6



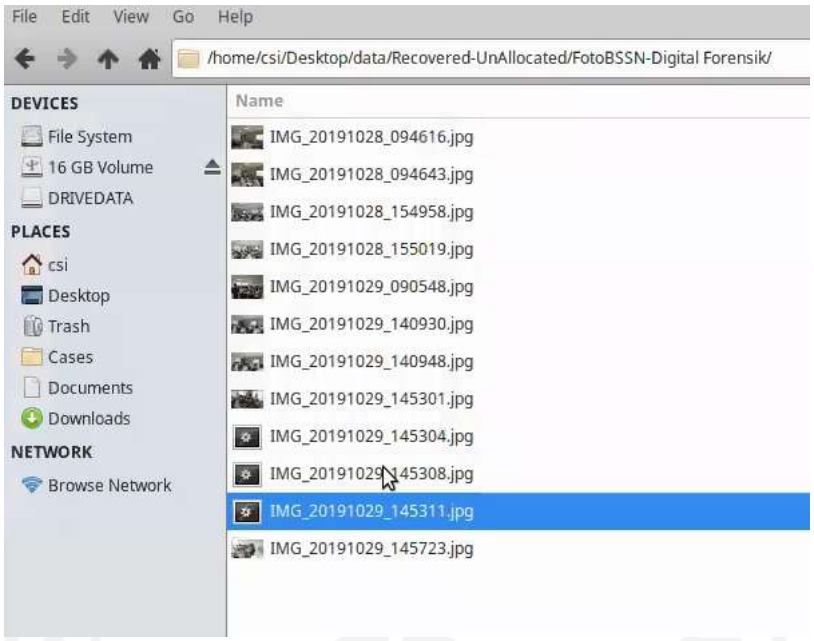
Gambar 4.6 Hasil Recovery Allocated file Menggunakan TSK Recover

Tahap setelah merecover allocated file, maka akan dilanjutkan dengan merecovery file UnAllocated dengan menggunakan command " tsk_recover -e /dev/loop0p1 Recovered-UnAllocated " dan mendapatkan hasil recovery file sejumlah 60 file seperti gambar 4.7



Gambar 4.7 Hasil Recovery UnAllocated file Menggunakan TSK Recover

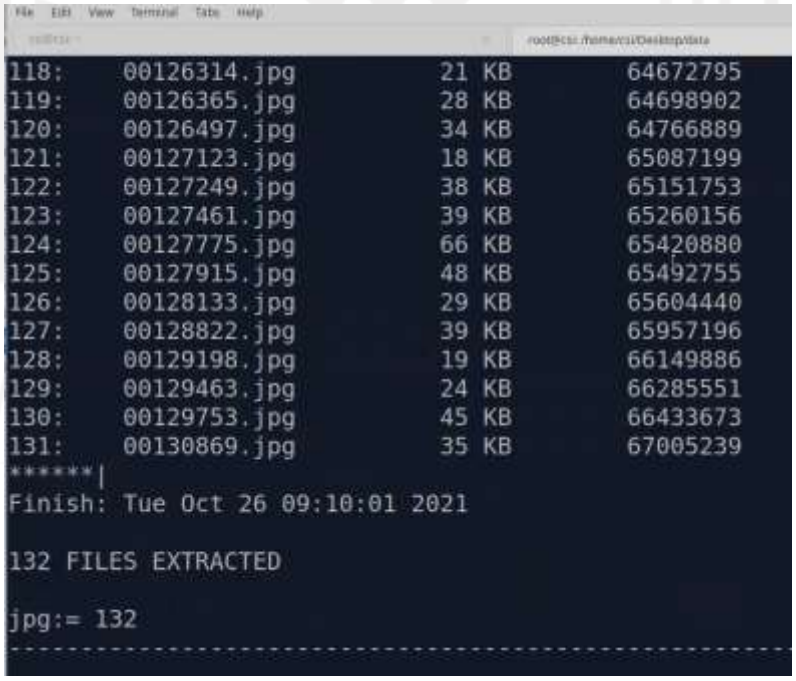
Setelah melakukan proses recovery terlihat pada gambar 4.8 teridentifikasi ada 12 file JPG, dan semua file tersebut berhasil di recovery, tetapi 3 diantaranya tetap tidak bisa dibuka atau rusak.



Gambar 4.8 Hasil Recovery File JPG Menggunakan TSK Recover

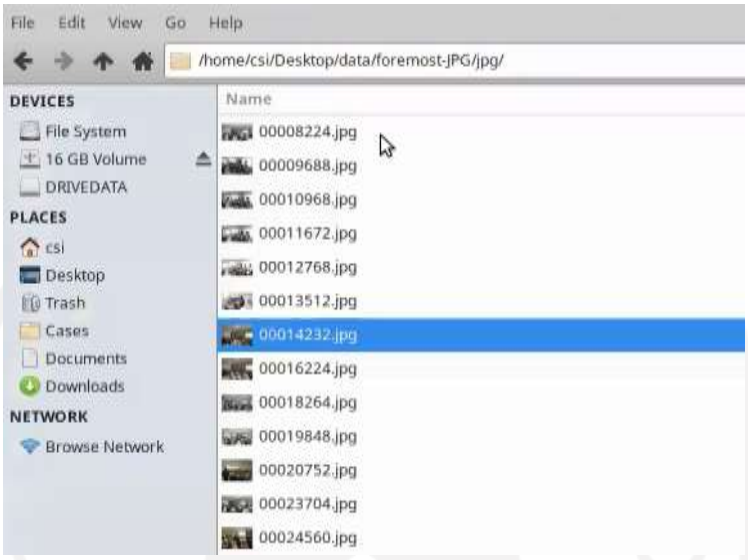
4.2.3 Proses Recovery Foremost

Pada tahap recovery dengan tool Foremost recover pada CSI Linux, akan dilakukan proses recovery untuk file JPG harus dengan menggunakan command " sudo foremost –v –o foremost-JPG –t jpg –i /dev/loop0p1 ". Dan hasilnya bisa dilihat terdapat 132 file JPG yang berhasil di recovery seperti gambar 4.9



Gambar 4.9 Proses Recovery File JPG Menggunakan Foremost

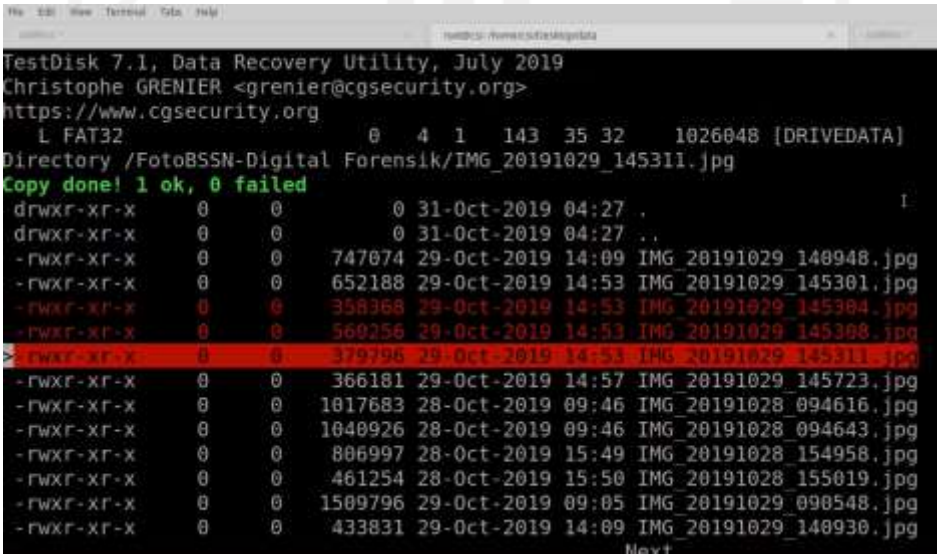
File JPG yang sebelumnya berhasil di recovery dan tidak bisa dibuka oleh tools FTK Imager dan TSK recover, dengan tool foremost file JPG tersebut bisa dibuka secara utuh bisa dilihat seperti gambar 4.10



Gambar 4.10 Hasil Recovery File JPG Menggunakan Foremost

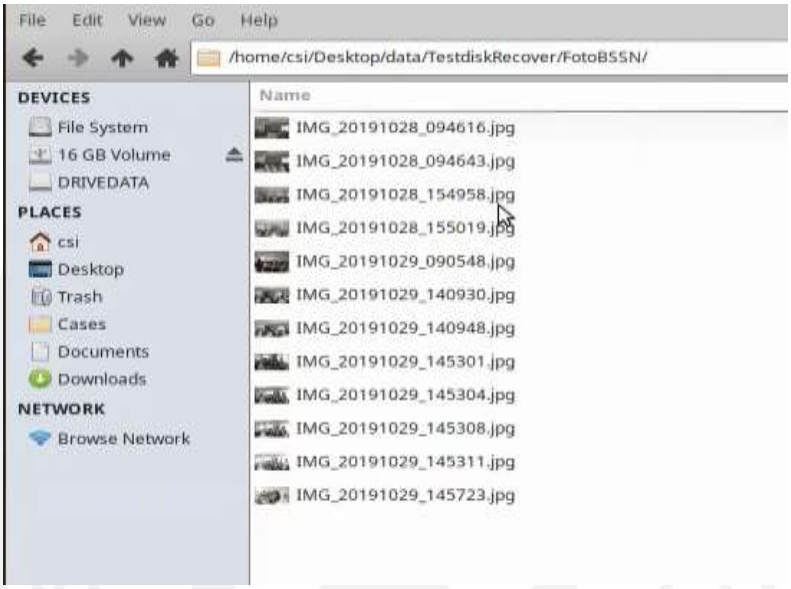
4.2.4 Proses Recovery TestDisk

Pada tahap recovery dengan tool Foremost recover pada CSI Linux, akan dilakukan proses recovery untuk file JPG harus dengan menggunakan command " sudo testdisk ImageDrive-FlashDisk.001 ". Dan hasilnya bisa dilihat terdapat 13 file JPG yang terlihat 3 diantaranya adalah file JPG yg berwarna merah yg tidak bisa dibuka atau rusak seperti gambar 4.11



Gambar 4.11 Proses Recovery File JPG Menggunakan TestDisk

Setelah dilakukan proses recovery dengan menggunakan Testdisk maka file JPG yang sebelumnya berhasil di recovery dan tidak bisa dibuka oleh tools FTK Imager dan TSK recover, dengan tool Testdisk recover, file JPG tersebut bisa dibuka secara utuh seperti tool Foremost, bisa dilihat seperti gambar 4.12



Gambar 4.12 Recovery File JPG Menggunakan TestDisk

4.3 Analysis

Pada tahap ini menganalisis bagian hasil file yang telah dilakukan recovery. Perbandingan dari ke empat tools yang digunakan untuk recovery file data berekstensi JPG, PNG, dan MP4 yang berada pada allocated space dan unallocated space mendapatkan hasil yang berbeda. Seperti pada penelitian ini maka bisa dijelaskan bahwa ada tools yang tidak bisa memulihkan file dengan sepurna dan ada yang berhasil memulihkan file dengan sempurna. Bisa dilihat dari tabel 4.3 dan tabel 4.4

Tabel 4.3 Hasil Status Recovery Allocated Files

No	Tools	Status File Recovery		
		JPG	PDF	MP4
		13 file	2 file	6 file
1	TSK Recover	100%	100%	100%
2	FTK Imager	100%	100%	100%
3	Foremost Recover	100%	100%	100%
4	TestDisk	100%	100%	100%

Allocated space merupakan penyimpanan file yang masih tersedia beserta file didalamnya yang bisa dibaca secara logical. Setelah dilakukan penelitian dengan tools diatas maka semua file yang ada di allocated space bisa di recover secara utuh.

Tabel 4.4 Hasil Status Recovery UnAllocated Files

No	Tools	Status File Recovery		
		JPG	PNG	MP4
		13 file	2 file	6 file
1	TSK Recover	77%	50%	83%
2	FTK Imager	77%	50%	83%
3	Foremost Recover	100%	100%	100%
4	TestDisk	100%	100%	100%

Unallocated space merupakan penyimpanan file yang sudah tidak tersedia atau sudah terhapus dan tidak bisa dibaca secara logical. Setelah dilakukan penelitian terhadap data file pada Unallocated space dengan menggunakan tool diatas maka tidak semua file berhasil di recovery secara utuh dan tidak sempurna.

Hashing adalah proses menghasilkan fixed-size output dari variabel-sized yang dilakukan dengan penggunaan rumus matematika yang dikenal sebagai hash function.

MD5 merupakan singkatan dari Message Digest algoritma yaitu fungsi hash kriptografi. Algoritma ini digunakan untuk melakukan pemeriksaan integritas file dalam berbagai situasi. Setelah melakukan hasing MD5 File rusak tersebut yang sudah di recovery setelah di check menggunakan MD5 teridentifikasi hashing file seperti tabel 4.4

Tabel 4.5 Hasil Akhir Hashing MD5 File Corrupt

No	File data	MD5 Hash
1	JPG 1	802d8d831083f24abc8a35d040d4da84
2	JPG 2	9deabc0cd170c556f4b01ed95607b470
3	JPG 3	67e4764ef793cbca0cb033a7967942b3
4	PDF	7fe0d6d164be3169c3098d32371b2eec
5	MP4	ae20fbeb7ba54be4560524220115acda

4.3.1 Action

Masalah yang sering terjadi pada sebuah storage yang berisi file hilang atau rusak perlu di atasi dengan tindakan dari penelitian ini menjawab beberapa pertanyaan seperti :

1. Apakah data yang sudah hilang bisa di kembalikan?
2. Tools forensik apa yang bisa melakukan recovery secara utuh?
3. Apakah nilai hash MD5 berubah pada file yang rusak?
4. Bagaimana cara recovery data yang tidak terdeteksi di sebuah storage, seperti unallocated space?

Berdasarkan hasil dari bukti file yang telah direcovery maka file yang telah terhapus bisa dipulihkan kembali dengan tools forensik seperti TSK recover, FTK imager, Foremost, dan Testdisk. Tool forensik seperti TSK recover dan FTK imager tidak bisa memulihkan data secara utuh, sedangkan tool Foremost dan Testdisk recover bisa memulihkan file data allocated dan unallocated yang terhapus dan rusak secara sempura.

4.3.2 Metode Investigasi Forensik

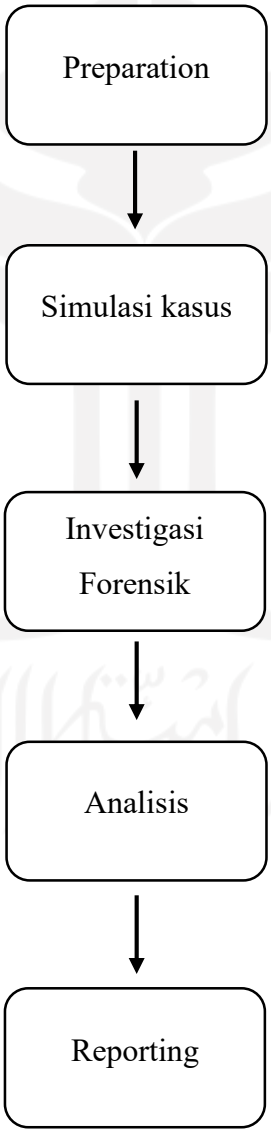
Pengimplementasian metode live forensik sebagai tahapan untuk melakukan investigasi forensik komputer terhadap kerusakan atau kehilangan file data dengan melihat hasil dari investigasi yang dijalankan. Metode live forensik dapat dijalankan untuk proses investigasi dalam mengungkap kasus cyber crime, komputer forensik juga berfungsi untuk mengumpulkan, menyimpan, menampilkan, dan menganalisis barang bukti digital dari sebuah komputer yang berbasis barang digital atau komputer. Terdapat barang bukti yang termasuk dalam digital forensik yaitu :

1. Email
2. Foto digital
3. Dokumen
4. Pesan instan
5. Spreadsheet
6. History internet browser
7. Dan isi memori komputer

Metode live forensik merupakan suatu teknik untuk menemukan barang bukti pada data volatile termasuk username dan password. Volatile sendiri adalah istilah yang digunakan untuk menunjukan bahwa data apapun yang disimpan hanya akan bertahan

selama ada daya listrik yang mengalir di dalam komputer. Sementara data non volatile akan tetap menyimpan data meski komputer dalam keadaan mati.

Metode live forensik pada dasarnya memiliki kesamaan pada teknik forensik tradisional yaitu indentifikasi penyimpanan, analisis dan presentasi. Metode live forensik merupakan respon dari kekurangan teknik forensik tradisional yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktivitas memory, proses jaringan, penukaran file, dan proses berjalanya sistem. Informasi dari file sistem ini menjadi kelebihan dari teknik live forensik. Penelitian ini pada dasarnya menggunakan pendekatan dari metodologi yang digunakan oleh teknik live forensik. Adapun proses tahapan yang harus dilakukan untuk melakukan live forensik ditampilkan pada gambar 4.13



Gamber 4.13 Tahapan Live Forensik

4.3.3 Evaluasi hasil

Bisa disimpulkan bahwa ada beberapa tools forensik yang bisa digunakan saat melakukan proses investigasi seperti autopsy, FTK Imager, Mobiledit dll. Pada penelitian ini terdapat 2 tool forensik yang direkomenasikan bisa digunakan untuk mengatasi investigasi forensik terhadap kehilangan file yang terhapus atau rusak. Foremost recover adalah salah satu tool yang berguna untuk penyidik untuk memulihkan file yang telah terhapus dan rusak. Foremost recover ini menggunakan proses yang dikenal sebagai file carving mencari memori ini untuk jenis file header yang cocok dengan yang ditemukan dalam file konfigurasi foremost. Sama seperti halnya dengan tool Testdisk recover, dengan ini seorang ahli digital forensik bisa memulihkan kembali file-file yang tidak dapat di pulihkan secara utuh disebabkan oleh factor-faktor seperti penghapusan data file secara sengaja maupun tidak sengaja.

setelah dilakukan analisis bisa disimpulkan bahwa file yang rusak/corrupt disebabkan perubahan pada nilai hash.nya. seperti pada tabel 4.2 dan 4.5 mendapatkan hasil hashing MD5 yang berbeda. Maka file file tersebut butuh di recovery dengan menggunakan tool yang bisa memperbaiki nilai hash seperti Foremost dan Testdisk.

BAB 5

Kesimpulan

Berdasarkan hasil penelitian tentang perbandingan data recovery menggunakn tools berbasis open source pada linux adalah hasil dari perbandingan tools ini dengan penelitian sebelumnya sangat berbeda, Dikarenakan terbatasnya fitur fitur yang berada pada tool forensik open source yang ada pada tool TSK recover dan FTK Imager, yang membuat penyidik sulit untuk mendapatkan bukti yg valid. Bisa disimpulkan bahwa diantara tool-tool tersebut ada yang bisa memulihkan file data yang telah rusak dan bisa dibuka kembali secara utuh dan ada yang tidak. Salah satu tools berbasis open source yang bisa digunakan adalah Foremost recover dan Testdisk recover. Tools ini adalah solusi dari permasalahan recovery. Dari tools yang sudah di uji coba hanya 50% yang berhasil di recovery secara utuh. Yaitu TSK recover dan FTK imager. Sementara tool foremost dan Testdisk 100% bisa merecovery secara utuh. Akan tetapi tool-tool yang tidak bisa memulihkan secara utuh ini bukan berarti tidak bagus. Tools tersebut masih direkomendasikan dan bisa digunakan untuk membantu investigator pada proses penyelidikan. investigator bisa mempunyai beberapa opsi pilihan pada tool-tool forensik untuk melakukan proses investigasi. Pada penelitian ini bertujuan untuk mengetahui tools forensik yang berguna saat ini dan masa yang akan datang.

Daftar Pustaka

Al-Sabaawi, A., Foo, E., & Au, E. (2019). A Comparison Study of Android Mobile Forensics for Retrieving Files System Handprint Recognition Technique Based in Image Segmentation for Recognize View project A Comparison Study of Android Mobile Forensics for Retrieving Files System. *International Journal of Computer Science and Security (IJCSS)*, *13*, 2019–2148. https://www.researchgate.net/publication/335422366

Baek, S., Jung, Y., Mohaisen, D., Lee, S., & Nyang, D. H. (2021). SSD-Assisted Ransomware Detection and Data Recovery Techniques. *IEEE Transactions on Computers*, *70*(10), 1762–1776. https://doi.org/10.1109/TC.2020.3011214

Breeuwsma, M., & Jongh, M. De. (2007). Forensic data recovery from flash memory. *Small Scale Digital …*, *1*(1), 1–17. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.5697&rep=rep1&type=pdf%5Cnhttp://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

Buchanan-Wollaston, J., Storer, T., & Glisson, W. (2013). Comparison of the Data Recovery Function of Forensic Tools. *IFIP Advances in Information and Communication Technology*, *410*, 331–347. https://doi.org/10.1007/978-3-642-41148-9_22

Campos, L. M. O., Gomes, E., & Martins, H. P. (2016). Forensic Expertise in Storage Device USB Flash Drive: Procedures and Techniques for Evidence. *IEEE Latin America Transactions*, *14*(7), 3427–3433. https://doi.org/10.1109/TLA.2016.7587651

Deepakumara, J., Heys, H. M., & Venkatesan, R. (2001). FPGA implementation of MD5 hash algorithm. *Canadian Conference on Electrical and Computer Engineering*, *2*, 919–924. https://doi.org/10.1109/ccece.2001.933564

Dibb, P., & Hammoudeh, M. (2013). Forensic data recovery from android os devices: An open source toolkit. *Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013*, *May*, 226. https://doi.org/10.1109/EISIC.2013.58

Guo, Y., & Slay, J. (2010). Chapter 21 DATA RECOVERY FUNCTION TESTING. *Ifip International Federation For Information Processing*, 297–311.

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic

software tools-Searching Function. *Digital Investigation*, *6*(SUPPL.), S12–S22. https://doi.org/10.1016/j.diin.2009.06.015

Handrizal, H. (2017). Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *1*(1), 84. https://doi.org/10.30645/j-sakti.v1i1.31

Hilgert, J. N., Lambertz, M., & Plohmann, D. (2017). Extending the Sleuth Kit and its underlying model for pooled storage file system forensic analysis. *DFRWS 2017 USA - Proceedings of the 17th Annual DFRWS USA*, *22*, S76–S85. https://doi.org/10.1016/j.diin.2017.06.003

Jo, W., Chang, H., & Shon, T. (2016). Digital forensic approach for file recovery in Unix systems: Research of data recovery on Unix file system. *Proceedings of 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2016*, 562–565. https://doi.org/10.1109/ITNEC.2016.7560423

Kumar, S., & Gupta, E. P. (2014). A Comparative Analysis of SHA and MD5 Algorithm. *International Journal of Computer Science and Information Technologies*, *5*(June 2014), 4492–4495.

Mohite, M. P., & Ardhapurkar, S. B. (2015). Design and implementation of a cloud based computer forensic tool. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 1005–1009. https://doi.org/10.1109/CSNT.2015.180

Na, G. H., Shim, K. S., Moon, K. W., Kong, S. G., Kim, E. S., & Lee, J. (2014). Frame-based recovery of corrupted video files using video codec specifications. *IEEE Transactions on Image Processing*, *23*(2), 517–526. https://doi.org/10.1109/TIP.2013.2285625

Panjaitan, J., & Sitepu, A. C. (2021). *Analisis Kinerja Forensic Acquisition Tools Untuk*. *1*(2), 17–25.

Plianda, I. A., & Indrayani, R. (2022). Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp. *Jurnal Media Informatika Budidarma*, *6*(1), 500. https://doi.org/10.30865/mib.v6i1.3487

Plum, J., & Dewald, A. (2018). Forensic APFS file recovery. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3230833.3232808

Povar, D., & Bhadran, V. K. (2011). Forensic data carving. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *53*, 137–148. https://doi.org/10.1007/978-3-642-19513-6_12

Pratama, I. P. A. E. (2021). Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept. *International Journal of Science, Technology & Management*, *2*(4), 1189–1196. https://doi.org/10.46729/ijstm.v2i4.256

Putra, R. C. W., & Widiatedja, I. P. (2008). *Informasi Pribadi Melalui Dunia Cyber Ditinjau Dari Dan Transaksi Elektronik (Uu Ite)*. *11*, 1–5.

Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *3*(1), 87. https://doi.org/10.30872/jurti.v3i1.2292

Ryu, S. J., Lee, H. Y., & Lee, H. K. (2014). Detecting trace of seam carving for forensic analysis. *IEICE Transactions on Information and Systems*, *E96-D*(5), 1304–1311. https://doi.org/10.1587/transinf.E97.D.1304

Simanjuntak, M. S., & Panjaitan, J. (2021). Analisa Recovery Data Menggunakan Software. *Jurnal Teknik Informatika Komputer Universal*, *1*(1), 26–32.

Wilson, R., & Chi, H. (2017). A case study for mobile device forensics tools. *Proceedings of the SouthEast Conference, ACMSE 2017*, 154–157. https://doi.org/10.1145/3077286.3077564

Winter, R. (2013). SSD vs HDD - Data recovery and destruction. *Network Security*, *2013*(3), 12–14. https://doi.org/10.1016/S1353-4858(13)70041-2

Zuhriyanto, I., Yudhana, A., & Riadi, I. (2017). Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop. *Jurnal Resti*, *1*(3), 829–836.