

**ANALISA DAN PENCARIAN BUKTI FORENSIK DIGITAL
PADA APLIKASI MEDIA SOSIAL FACEBOOK DAN
TWITTER MENGGUNAKAN METODE STATIK FORENSIK**

SKRIPSI

*Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau*



OLEH:

GUSRA MISHARDILA
153510355

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2020**

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama : Gusra Mishardila
NPM : 153510355
Jurusan : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Judul Skripsi : Analisa dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria - kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak dapat disetujui untuk disidangkan dalam ujian komprehensif.

Pekanbaru, 17 April 2020

Disetujui Oleh :
PEKANBARU

Dosen Pembimbing



YUDHI ARTA, ST., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik



Dr. Eng. MUSLIM, ST., MT
NPK. 09 11 02 374

Ketua Prodi Teknik Informatika



AUSE LABELLAPANSA, ST., M.Cs., M.Kom

**LEMBAR PENGESAHAN
TIM PENGUJI UJIAN SKRIPSI**

Nama : Gusra Mishardila
NPM : 153510355
Jurusan : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Judul Skripsi : Analisa dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah, serta telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 17 April 2020** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang **Ilmu Teknik Informatika.**

Pekanbaru, 17 April 2020

Tim Penguji

- | | | |
|--|------------------------|---------|
| 1. Dr. Arbi Haza Nasution, M.IT | Sebagai Tim Penguji I | (.....) |
| 2. Panji Rachmat Setiawan, S.Kom.,MMSI | Sebagai Tim Penguji II | (.....) |

**Disetujui Oleh :
Dosen Pembimbing**



YUDHIARTA, ST., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik



Dr. Eng. MUSLIM, ST., MT
NPK. 09 11 02 374

Ketua Prodi Teknik Informatika



AUSE LABELLAPANSA, ST., M.Cs., M.Kom

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama : Gusra Mishardila
Tempat/TglLahir : Pulau Binjai, 01 Agustus 1998
Alamat : Jl. Srikandi Perum Wadya Graha 1 Blok B No:5
Kelurahan Delima, Kec. Tampan, Pekanbaru

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada :

Fakultas : Teknik
Jurusan : Teknik Informatika
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul“ **Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik**”. Apabila dikemudian hari ada yang merasa dirugikan dan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karya ilmiah ini **bukan** karya saya sendiri atau **plagiat** hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya.

Pekanbaru, 18 April 2020
Yang membuat pernyataan,



(Gusra Mishardila)

HALAMAN IDENTITAS PENULIS

Nama : Gusra Mishardila

NPM : 153510355

Tempat/Tgl Lahir : Pulau Binjai, 01 Agustus 1998

Alamat Orang Tua : Jl. Srikandi Perum Wadya Graha 1
Blok B No:5 Kelurahan Delima Kec.
Tampan, Pekanbaru

Nama Orang Tua : 1. Harni Nela
2. Abu Khari

No.Hp / Telp : 081390842700

Jurusan : Teknik Informatika

Fakultas : Teknik

Email : gusramishardila@student.uir.ac.id

Masuk Th. Ajaran : 2015

Wisuda Th. Ajaran : 2020

Judul Penelitian : Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi
Media Sosial Facebook dan Twitter Menggunakan Metode
Statik Forensik

Pekanbaru, 18 April 2020

Gusra Mishardila

DAFTAR RIWAYAT HIDUP

a. Data Personal

NPM : 153510355
Nama : Gusra Mishardila
Tempat/Tgl Lahir : Pulau Binjai, 01 Agustus 1998
Jenis Kelamin : Laki-laki
Agama : Islam
Jenjang : Sastra-1 (S1)
Program Studi : Teknik Informatika
Alamat : Jl. Srikandi Perum Wadya Graha 1 Blok B No:5
Kelurahan Delima, Kec. Tampan, Pekanbaru
No. Handphone : 081390842700
E-mail : gusramishardila@student.uir.ac.id

b. Pendidikan

Jenjang	Nama Lembaga	Tahun
SD	SDN 016 Pulau Binjai	2003-2008
SMP	SMPN 1 Kuantan Mudik	2009-2012
SMK	SMKN 1 Kuantan Mudik	2012-2015
Universitas	Universitas Islam Riau	2015-2020

Demikian daftar riwayat hidup ini dibuat dengan sebenarnya.

Pekanbaru, 18 April 2020
Mahasiswa Ybs,

Gusra Mishardila

HALAMAN PERSEMBAHAN

Assalamu'alikum Warahmatullahi Wabarakatuh.

Alhamdulillah, puji syukur penulis panjatkan kehadirat Allah SWT karena atas limpahan rahmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan. Tak lupa pula penulis mengirimkan salam dan shalawat kepada Nabi Besar Muhammad SAW yang telah membawa umat Islam ke jalan yang diridhoi Allah SWT.

Skripsi yang berjudul **"Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik"** merupakan salah satu syarat untuk mencapai gelar sarjana teknik informatika. Terwujudnya skripsi ini tidak lepas dari partisipasi dan bantuan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih yang setulus-tulusnya kepada :

1. Nesi Syafitri, S.Kom., M.Cs selaku penasehat akademik yang senantiasa memberikan masukan dan motivasi kepada penulis.
2. Yudhi Arta, S.T., M.Kom sebagai dosen pembimbing skripsi yang telah meluangkan waktu untuk memberikan masukan, bimbingan, dan motivasi yang membangun kepada penulis hingga skripsi ini terselesaikan dengan baik.

3. Rizdqi Akbar Ramadhan, S.Kom., M.Kom., CHFI Selaku Dosen Digital Forensik Universitas Islam Riau yang rela meluangkan waktunya untuk penulis konsultasi tentang digital forensik yang menjadikan penulis yang pertama mengangkat judul digital forensik ini di Universitas Islam Riau.
4. Kepada seluruh dosen dan staff Prodi Teknik Informatika Fakultas Teknik Universitas Islam Riau yang memberikan ilmu dan pengalaman selama masa perkuliahan.
5. Kepada Orangtua Penulis, Ibunda tercinta yang penulis sayangi dan hormati yang selalu tulus memberikan kasih sayang dan kesabarannya dalam mendidik penulis sampai detik ini, semua berkat doa dan harapannya jua lah penulis meraih semua ini. Meski secarik kertas persembahan ini tak ada apa-apanya dibanding pengorbanannya semoga ini langkah awal untuk bisa membuat orang yang melahirkanku bahagia dunia dan akhirat.
6. Kepada para pahlawan hidupku Atuk, Acik, Oom, Tante, Mamak, Amay, Abang, uni yang senantiasa membantu penulis dengan ikhlas dan kasih sayangnya menghantarkan penulis dalam menyelesaikan studi ini. Semoga doa dan semua hal yang terbaik yang diberikan menjadikanku orang yang baik pula.

7. Kepada Saudaraku Bang Afry, Junda, Prilly, Annisa, Dwi, Rizky, Zaza, Ikhzam yang menyemangati penulis dalam proses meraih gelar Sarjana Teknik ini.
8. Kepada Koncok Arek Otun Cipuik Reza, Ardo, Hengki, Dhea, Ipik, Delfi, Ana, Yana yang memberikan canda tawa dan ejekan kepada penulis dalam menyelesaikan penelitian ini.
9. Kepada, Deni, Restu, Yoga, Jhody, Jakfar, Maulana, Riduan, Imam, Wawan, Hana, Danti, yang telah banyak membantu dan memotivasi penulis pada masa berat semester tua yang berujung manis ini. Suka-duka, semuanya kita lewati bersama dan saling menguatkan.
10. Kepada sahabat-sahabatku Teknik Informatika angkatan 2015 khususnya kelas E yang tidak bisa disebutkan satu persatu, terima kasih atas kebersamaan yang membangun semangat dan dukungan yang diberikan hingga saat ini.
11. Serta seluruh pihak yang ikut membantu, baik secara langsung maupun tidak langsung. Penulis hanya bisa berdoa, semoga Allah membalas kebaikan-kebaikan mereka dengan setimpal. Aamiin.

Penulis menyadari sepenuhnya bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, penulis memohon maaf bila ada kesalahan dalam penulisan skripsi ini. Kritik dan saran kami hargai demi penyempurnaan penulisan serupa dimasa yang akan datang. Besar harapan penulis, semoga

skripsi ini dapat bermanfaat dan dapat bernilai positif bagi semua pihak yang membutuhkan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.



Pekanbaru, 18 April 2020

Penulis

Gusra Mishardila

KATA PENGANTAR

Assalamu'alaikum Warahmatulahi Wabarakatuh.

Dengan segala kerendahan hati Penulis haturkan rasa syukur dalam kehadiran Allah SWT,yang telah memberikan limpahan rahmat dan karunia-Nya yang berupa kemampuan, kesehatan dan juga kesempatan kepada Penulis untuk menyelesaikan proposal tugas akhir “Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik”.

Pada kesempatan ini Penulis juga ingin menyampaikan rasa hormat dan terima kasih kepada berbagai pihak yang telah memberikan bantuan, dorongan, dan bimbingan selama menyelesaikan proposal tugas akhir ini.

Penulis sangat menyadari bahwa masih terdapat kekurangan didalam penulisan laporan ini. Untuk itu Penulis mengharapkan kritik dan saran yang membangun guna kebaikan dan kesempurnaan proposal skripsi ini. Penulis berharap proposal ini bisa bermanfaat bagi pembaca nantinya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Pekanbaru, 18 April 2020

Penulis

ANALYSIS AND SEARCH OF DIGITAL FORENSIC EVIDENCE ON SOCIAL MEDIA APPLICATIONS FACEBOOK AND TWITTER USING THE STATIC FORENSIC METHODS

Gusra Mishardila
Faculty of Engineering
Informatics Engineering Study Program
Islamic University of Riau
Email: gusramishardila@student.uir.ac.id

ABSTRACT

The development of internet technology which is rapidly increasing followed by the increase in social media users has resulted in crime in social media that has increased one of them on the Facebook and Twitter applications. Freedom of expression on social media such as Facebook and Twitter makes users victims or perpetrators of crime on social media. Not a few crimes that occur on social media such as Facebook and Twitter. Among them the spread of hoaxes, which we know for ourselves Indonesian people in general are very easy to believe lies that are unclear sources have resulted in division between several parties. Pornographic content, hate speech, cases of kidnapping, and other crimes that could have occurred on the internet. But basically there is no crime that does not leave a trace, for that there needs to be a research to be built namely "Analysis and search for digital forensic evidence on social media applications Facebook and Twitter using forensic static methods" in assisting legal processes based on applicable laws to expose the crime that is on the internet.

Keywords: *Forensic Digital, Forensic Evidence, Social Media, Facebook, Twitter*

**ANALISA DAN PENCARIAN BUKTI FORENSIK DIGITAL PADA
APLIKASI MEDIA SOSIAL FACEBOOK DAN TWITTER
MENGUNAKAN METODE STATIK FORENSIK**

Gusra Mishardila
Fakultas Teknik
Program Studi Teknik Informatika
Universitas Islam Riau
Email : gusramishardila@student.uir.ac.id

ABSTRAK

Perkembangan teknologi internet yang semakin pesat diikuti pula meningkatnya pengguna media sosial mengakibatkan kejahatan di media sosial semakin meningkat salah satunya pada aplikasi facebook dan twitter. Kebebasan berekspresi di media sosial seperti facebook dan twitter membuat para pengguna menjadi korban atau pelaku kejahatan di media sosial. Tidak sedikit tindak kejahatan yang terjadi di media sosial seperti facebook dan twitter. Diantaranya penyebaran hoax, yang kita tau sendiri masyarakat indonesia pada umumnya mudah sekali mempercayai berita bohong yang tidak jelas sumbernya mengakibatkan terpecah belahnya antara beberapa pihak. Konten pornografi, ujaran kebencian, kasus pembunuhan, dan kejahatan lainnya yang bisa saja terjadi di internet. Namun pada dasarnya tidak ada kejahatan yang tidak meninggalkan jejak, untuk itu perlu adanya sebuah penelitian yang akan dibangun yakni “Analisa dan pencarian bukti forensik digital pada aplikasi media sosial facebook dan twitter menggunakan metode statik forensik” dalam membantu proses hukum berdasarkan undang-undang yang berlaku untuk mengungkap kejahatan yang ada di internet.

Kata Kunci : *Digital Forensik, Bukti forensik, Media Sosial, Facebook, Twitter*

DAFTAR ISI

HALAMAN PERNYATAAN BEBAS PLAGIARISME

HALAMAN IDENTITAS PENULIS

HALAMAN PERSEMBAHAN

KATA PENGANTAR..... i

ABSTRAK ii

DAFTAR ISI..... iv

DAFTAR TABEL vii

DAFTAR GAMBAR..... viii

BAB I PENDAHULUAN 1

1.1 Latar Belakang..... 1

1.2 Identifikasi Masalah 2

1.3 Batasan Masalah 3

1.4 Rumusan Masalah 3

1.5 Tujuan Penelitian..... 3

1.6 Manfaat Penelitian..... 4

BAB II LANDASAN TEORI 5

2.1 Studi Kepustakaan 5

2.2 Dasar Teori 6

2.2.1 Digital Forensik 6

2.2.2 *Chain of Custody* 7

2.2.3 *Pre Acquisition* 8

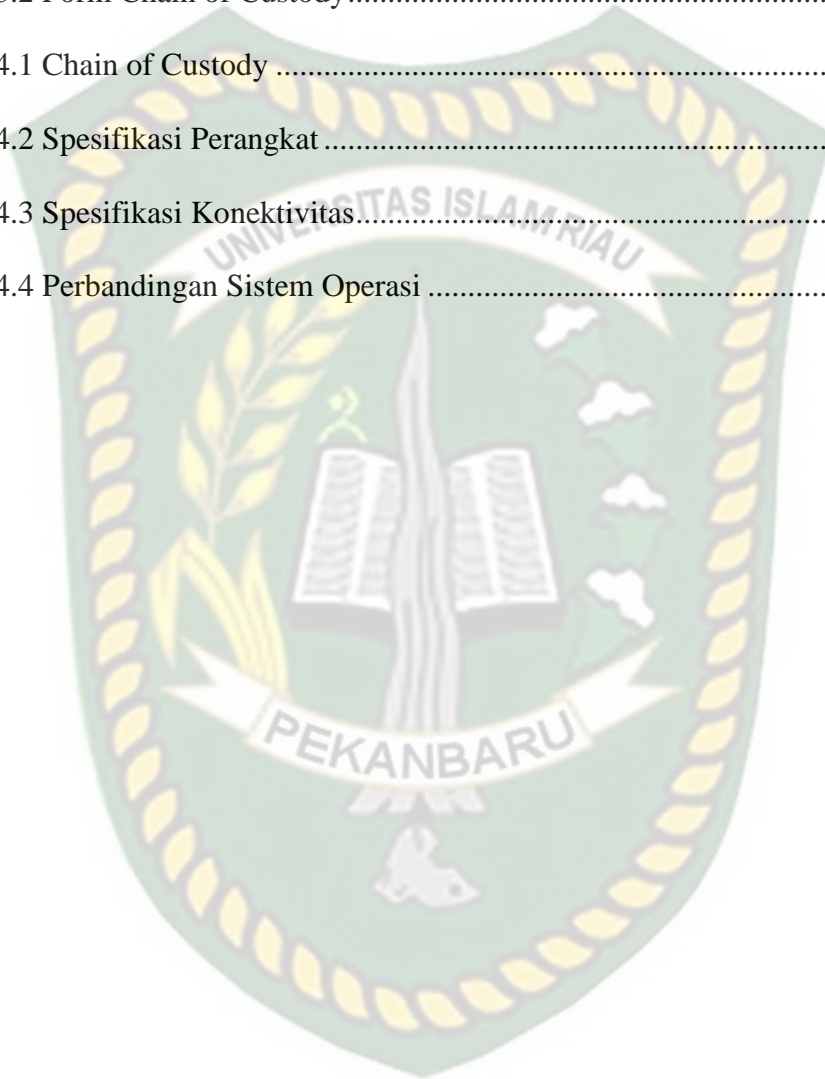
2.2.4 *Core Acquisition* 8

2.2.5	Akuisisi	8
2.2.6	Bukti Digital (<i>Digital Evidence</i>).....	9
2.2.7	<i>Cybercrime</i>	10
2.2.8	<i>Data Recovery</i>	10
2.2.9	Facebook.....	10
2.2.10	Twitter.....	11
2.2.11	Statik Forensik	11
BAB III METODOLOGI PENELITIAN		12
3.1	Tahapan Penelitian	12
3.1.1	Persiapan Sistem.....	12
3.1.2	Bahan dan Alat Penelitian	12
3.1.3	Skenario Simulasi Penelitian	13
3.2	Pra Akuisi	15
3.3	Akuisisi Inti	18
3.3.1	<i>Investigation</i> (Pemeriksaan)	18
3.3.2	<i>Collection</i> (Pengumpulan).....	19
3.3.3	Reporting (Laporan)	20
BAB IV HASIL DAN PEMBAHASAN		21
4.1	Skenario Kasus	21
4.2	Pra Akuisisi	23
4.2.1	Mencari Barang Bukti.....	23
4.2.2	Kasus pada Perangkat	23
4.2.3	Perangkat dan Konfigurasi	28

4.2.4	Konektivitas dan Penyimpanan	29
4.3	Akuisisi Inti	30
4.3.1	Proses <i>Imaging</i> Barang Bukti (Pencitraan)	30
4.3.2	Analisa Menggunakan Aplikasi Autopsy	35
4.4	Result	43
4.5	Laporan	43
4.6	Perbandingan Sistem Operasi	43
4.6.1	Proses <i>Imaging</i> Barang Bukti (Pencitraan) pada Windows.....	43
4.6.2	Proses Analisa pada Windows	43
4.6.3	Proses <i>Imaging</i> Barang Bukti (Pencitraan) pada Linux	43
4.6.4	Proses Analisa pada Linux	43
BAB V KESIMPULAN DAN SARAN		73
5.1	Kesimpulan	73
5.2	Saran	73
DAFTAR PUSTAKA		74
LAMPIRAN		

DAFTAR TABEL

Tabel 3.1 Pra Akuisisi	14
Tabel 3.2 Form Chain of Custody	18
Tabel 4.1 Chain of Custody	23
Tabel 4.2 Spesifikasi Perangkat	30
Tabel 4.3 Spesifikasi Konektivitas	30
Tabel 4.4 Perbandingan Sistem Operasi	30



DAFTAR GAMBAR

Gambar 3.1 Tahapan Penelitian	12
Gambar 3.2 Ilustrasi Simulasi Kasus	14
Gambar 3.3 Pra Akuisisi	15
Gambar 3.4 Akuisisi Inti	19
Gambar 3.5 Tampilan Awal Aplikasi Autopsy	21
Gambar 4.1 Barang bukti yang ditemukan	23
Gambar 4.2 Kasus konten pornografi di facebook.....	24
Gambar 4.3 Kasus <i>Hatespeech</i> di facebook.....	25
Gambar 4.4 Kasus <i>Hatespeech</i> di Twitter.....	25
Gambar 4.5 Kasus <i>Bullying</i> di Fcaebook.....	26
Gambar 4.6 Kasus <i>Bullying</i> di Twitter.....	27
Gambar 4.7 Kasus Penyebaran Hoax di facebook.....	28
Gambar 4.8 Kasus penyebaran Hoax di Twitter.....	28
Gambar 4.9 Tampilan awal FTK Imager.....	30
Gambar 4.10 Pilihan tipe barang bukti	31
Gambar 4.11 Pilihan penyimpanan yang akan di imaging	31
Gambar 4.12 Lokasi penyimpanan imaging	32
Gambar 4.13 Pilihan format imaging.....	32
Gambar 4.14 Informasi item barang bukti	33
Gambar 4.15 Alamat penyimpanan imaging	33
Gambar 4.16 Proses imaging sedang berjalan	34
Gambar 4.17 Laporan kode Hash.....	37

Gambar 4.18 Form <i>Case Information Information</i>	35
Gambar 4.19 Form <i>Additional information</i> Aplikasi Autopsy	35
Gambar 4.20 Form menentukan tipe data yang akan dianalisis	37
Gambar 4.21 Form mengambil data yang akan dianalisis	38
Gambar 4.22 Form penentuan <i>ingest modules</i> aplikasi Autopsy	39
Gambar 4.23 Data <i>Source</i> dalam Aplikasi Autopsy	40
Gambar 4.24 Partisi data <i>Source</i> Aplikasi Autopsy	40
Gambar 4.25 Detail data <i>Source</i> dalam Aplikasi Autopsy(10%)	42
Gambar 4.26 Isi Konten Data <i>Source</i> dalam Aplikasi Autopsy	43
Gambar 4.27 Isi konten Results	44
Gambar 4.28 Metadata barang bukti yang akan dianalisis	44
Gambar 4.29 Username pelaku	45
Gambar 4.30 Metadata Username pelaku	46
Gambar 4.31 Foto penyebaran konten pornografi di facebook	46
Gambar 4.32 Metadata Foto penyebaran konten pornografi di facebook	47
Gambar 4.33 Foto ujaran kebencian pada korban di facebook	47
Gambar 4.34 Metadata Foto ujaran kebencian pada korban di facebook	48
Gambar 4.35 Status Twitter Korban	48
Gambar 4.36 Metadata Status Twitter Korban	49
Gambar 4.37 Tampilan awal FTK Imager	52
Gambar 4.38 Pilihan tipe barang bukti	52
Gambar 4.39 Pilihan penyimpanan yang akan di Imaging	53
Gambar 4.40 Lokasi penyimpanan Imaging	54

Gambar 4.41 Pilihan Format Imaging.....	54
Gambar 4.42 Informasi Item Barang Bukti.....	55
Gambar 4.43 Alamat penyimpanan Imaging	55
Gambar 4.44 Proses Imaging sedang berjalan	56
Gambar 4.45 Laporan hasil Akuisisi.....	57
Gambar 4.46 Form <i>Case Information</i>	58
Gambar 4.47 Form <i>Additional Information</i> Aplikasi Autopsy	58
Gambar 4.48 Form menentukan tipe yang akan dianalisis	59
Gambar 4.49 Form Penentuan <i>ingest modules</i> Aplikasi Autopsy.....	60
Gambar 4.50 Data <i>Source</i> dalam Aplikasi Autopsy	61
Gambar 4.51 List barang bukti yang ditemukan	61
Gambar 4.52 Barang bukti yang dihapus pelaku	62
Gambar 4.53 Metadata barang bukti yang dihapus pelaku	62
Gambar 4.54 Tampilan awal Aplikasi Guymager.....	63
Gambar 4.55 Format yang akan diakuisisi.....	64
Gambar 4.56 Akuisisi barang bukti sedang berjalan	64
Gambar 4.57 Laporan Hasil Akuisisi.....	65
Gambar 4.58 Tampilan Awal Aplikasi Autopsy pada Linux.....	66
Gambar 4.59 Form membuat kasus baru pada Aplikasi Autopsy.....	66
Gambar 4.60 Form penambahan <i>Host</i>	67
Gambar 4.61 Lokasi penyimpanan Analisa	67
Gambar 4.62 Form Input barang bukti.....	68
Gambar 4.63 Form Detail kode Hash	68

Gambar 4.64 Laporan barang bukti berhasil diimport..... 69

Gambar 4.65 Barang bukti yang didapatkan..... 69

Gambar 4.66 Format file barang bukti yang akan dianalisa 70

Gambar 4.67 Tampilan Metadata Format file barang bukti..... 70



BAB I

PENDAHULUAN

1.1 Latar Belakang

Media sosial adalah suatu interaksi sosial antara individu dalam berbagai dan bertukar informasi. Media sosial dapat mencakup berbagai ide, pendapat, gagasan dan konten dalam komunitas virtual serta mampu menghadirkan dan mentranslasikan cara berkomunikasi baru dengan teknologi yang sama sekali berbeda dari media tradisional (Watson. 2009).

Media sosial yang sangat populer sampai dengan saat ini adalah facebook. Di indonesia sendiri pengguna Facebook mencapai 130 juta pengguna, diikuti Instagram 62 juta pengguna dan Twitter 6,4 juta pengguna. Facebook merupakan jejaring sosial yang terkenal di dunia yang membantu pengguna untuk menjalin pertemanan yang sangat luas. Pengguna facebook dapat menjalin pertemanan dengan ratusan bahkan ribuan teman, baik yang dikenal maupun yang tidak. Dari anak-anak, pejabat, orang tua bahkan siapapun berhak menggunakan facebook. Kebanyakan dari mereka memakai facebook untuk menjalin pertemanan dan berkomunikasi dengan banyak orang, baik itu saudara, teman dekat bahkan teman jauh.

Media sosial yang serupa dengan Facebook ialah Twitter. Dimana Facebook dan Twitter ada layanan membuat status dan penyebaran informasi, yang artinya pengguna bebas mengekspresikan pikiran mereka dalam bentuk teks, gambar maupun video. Namun perkembangan teknologi ini dimanfaatkan sebagian orang untuk melakukan tindak kejahatan.

Tidak sedikit tindak kejahatan dilakukan di media sosial facebook dan twitter. Diantaranya penyebaran Hoax, yang kita tau sendiri masyarakat indonesia pada umumnya mudah sekali mempercayai berita bohong yang tidak jelas sumbernya mengakibatkan terpecah belahnya antara beberapa pihak. konten pornografi, sebagai contoh video asusila Ariel dengan Cut Tari dan Luna Maya pada tahun 2010 silam tersebar luas di internet dan facebook salah satunya yang bebas diakses umur berapapun yang mengakibatkan efek buruk yang diterima di masyarakat. *Hatespeech*, atau ujaran kebencian yang mengakibatkan karakter atau watak seseorang yang berkesan tak sopan atau menyudutkan suatu pihak yang bersifat mengadu domba dan menimbulkan perpecahan. *Cyberbully*, segala bentuk kekerasan seperti ejekan atau menghina yang dialami anak atau remaja yang berdampak pada frustrasi, gangguan mental dan bisa berujung bunuh diri atau kematian dan kejahatan internet lainnya.

Berdasarkan pernyataan di atas, penulis melakukan penelitian untuk skripsi dengan judul “Analisa dan Pencarian Bukti Forensik Digital pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik”.

1.2 Identifikasi Masalah

Adapun identifikasi masalah yang dapat diambil dari latar belakang tersebut sebagai berikut :

1. Banyaknya pengguna Facebook dan Twitter mengakibatkan banyaknya tindak kejahatan di media sosial.

2. Kebebasan berekspresi di media sosial sosial facebook dan twitter membuat para pengguna menjadi korban atau pelaku kejahatan di media sosial.

1.3 Batasan Masalah

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

1. Analisis yang dilakukan adalah pembacaan item. Sesuai dengan skenario kasus.
2. Pengembalian/pemulihan(recovery) barang bukti digital yang dicurigai hanya pada aplikasi facebook dan twitter.

1.4 Rumusan Masalah

Dengan berdasarkan latar belakang masalah dan hubungannya dengan pemilihan judul tersebut, maka penulis merumuskan pokok permasalahan yaitu:

1. Bagaimana Penulis menemukan bukti digital yang dapat dijadikan artefak barang bukti kasus kejahatan *cybercrime* dan dapat menemukan file tertentu yang sudah dihapus oleh tersangka?
2. Bagaimana penulis mengimplementasikan metode statik forensik sewaktu pelaku kejahatan media sosial menghilangkan jejaknya?

1.5 Tujuan Penelitian

1. Mengidentifikasi barang bukti. Serta mempelajari bagaimana melakukan teknik identifikasi digital *forensic* yang tepat dengan menggunakan tools yang dipilih.
2. Memahami konsep pengembalian data facebook dan twitter .

1.6 Manfaat Penelitian

Penelitian ini bermanfaat untuk, antara lain :

1. Menambah Pengetahuan dan lebih memahami ilmu *forensic* .
2. Memberikan pemahaman dalam penggunaan tools *forensic*.
3. Menambah pengetahuan *recovery* data melalui Aplikasi yang dipakai.



BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Penelitian lain yang dijadikan acuan adalah penelitian Ruci Meiyanti (2015), Pada penelitian dengan judul Perkembangan digital forensik Saat ini dan Mendatang, yang berisi bahwa ilmu forensik adalah ilmu yang digunakan untuk tujuan hukum, bersifat tidak memihak yang merupakan bukti ilmiah untuk digunakan dalam kepentingan peradilan dan penyelidikan. Digital forensik atau sering disebut juga sebagai komputer forensik adalah salah satu cabang dari ilmu forensik yang berkaitan dengan bukti legal yang masih terdapat pada sebuah atau lebih komputer dan media penyimpanan digital lainnya sebagai bukti-bukti digital yang digunakan dalam kejahatan komputer dan dunia maya. Seorang Pakar digital forensik harus benar-benar terlatih dan berpengalaman dalam menggunakan cara untuk mengumpulkan semua data-data yang diperlukan sehingga bisa dijadikan bukti legal yang semuanya sudah diatur dalam undang-undang informasi dan transaksi elektronik. Dengan pesatnya perkembangan teknologi dewasa ini dalam informatika dan komunikasi yang dapat digunakan untuk aktifitas kejahatan di dunia maya maka dapat diupayakan peralatan investigasi dan aplikasi-aplikasi yang dapat digunakan di dunia sekuriti dan berguna untuk digital forensik pada saat ini dan mendatang.

Berdasarkan penelitian terdahulu yaitu penelitian dari Anton Yudhana (2018) dengan judul Facebook Messenger menjadi media sosial yang populer kedua setelah Whatsapp di tahun 2017. Meningkatnya jumlah pengguna Facebook

Messenger tentu membawa dampak positif dan negatif, salah satu efek negatifnya adalah beberapa orang yang menggunakan Facebook Messenger melakukan kejahatan digital. Jika sebuah smartphone android menjadi bukti dalam kasus pidana dan Facebook Messenger terinstall di smartphone tersebut, maka pada aplikasi ini bukti digital dapat diidentifikasi dan dapat diharapkan menjadi pilihan untuk membantu penegakan hukum dalam mengungkap kejahatan digital. Proses identifikasi berdasarkan proses forensic mobile yang berdasarkan metode NIST (National Institute of Standards Technology). NIST memiliki panduan kerja baik itu kebijakan dan standar untuk menjamin setiap examiner mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat di ulang (repeatable) dan dapat dipertahankan (defendable). Penelitian ini menjelaskan gambaran umum bagaimana teknik-teknik yang dapat digunakan untuk mengembalikan bukti digital berupa text, gambar, dan audio pada Facebook Messenger yang ada di Smartphone Android.

2.2 Dasar Teori

2.2.1 Digital Forensik

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 di perangkat target dikunci, dihapus, atau disembunyikan. Berawal dari bangkitnya revolusi komputasi personal pada akhir 1970-an dan awal 1980-

an, disiplin ini berkembang secara alami selama tahun 1990-an, dan baru pada awal abad ke-21 negara-negara secara bertahap membentuk kebijakannya terhadap disiplin ini.

Landasan forensik digital ialah 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. Forensik juga dapat dilakukan di sektor swasta; seperti penyelidikan internal perusahaan (*in-house*) atau penyelidikan intrusi (penyelidikan khusus mengeksplorasi sifat dan dampak intrusi jaringan yang tidak sah).

Penguasaan ilmu forensik digital tidak hanya menuntut kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hukum. Aspek teknis dari penyelidikan dapat dibagi menjadi beberapa subcabang, sesuai dengan jenis perangkat digital yang terlibat; forensik komputer, forensik jaringan, analisis data forensik dan forensik peranti bergerak. Proses forensik umumnya meliputi penyitaan, *forensic imaging* (akuisisi) dan analisis media digital dan penyusunan laporan berdasarkan bukti yang dikumpulkan.

2.2.2 Chain of Custody

CoC adalah sebuah proses yang menunjukkan bahwa segala bukti terjamin telah dikendalikan dan ditangani dengan benar setelah proses pengumpulan. bermacam forensik digital dilakukan dengan menjaga CoC. Seperti contoh, forensik komputer biasanya berkaitan dengan pencarian file baik yang masih ada ataupun yang telah dihapus sebagai barang bukti digital. CoC forensik komputer

membutuhkan kehati-hatian karena sifat data digital adalah volatile dan mudah berubah. Perbedaan time stamp (*created-modified-access*) pada file log misalnya, dapat merusak bukti digital dan tidak dapat diterima oleh pengadilan. Penanganan awal terhadap bukti elektronik berupa komputer yang didapatkan saat mati atau menyala juga berbeda.

2.2.3 Pre Acquisition

Pra Akuisi ialah segala sesuatu yang mempersiapkan segala bentuk persiapan dalam mencari, mengidentifikasi dan mengakuisisi barang bukti dalam menangani kasus seperti peralatan yang akan dipakai dan juga perangkat keras dan perangkat lunak komputer yang akan digunakan dalam mengakuisisi.

2.2.4 Core Acquisition

Core Akuisi ialah inti dari mengakuisisi dimana proses digital forensik berjalan dimana ketika persiapan untuk mengakuisisi telah terpenuhi maka ahli forensik mulai menjalani tugas nya sesuai prosedur yang berlaku seperti *Collection, Examination, Analysis dan Reporting*.

2.2.5 Akuisisi

Menurut dokumen SNI 27037:2014, akuisisi merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktivitas yang dilakukan. Petugas yang melakukan akuisisi harus memilih metode yang paling sesuai berdasarkan situasi, biaya dan waktu, dan mendokumentasikan keputusan yang dipilih untuk menggunakan metode tertentu dan tool yang sesuai. Metode yang dipilih juga harus dapat dipraktekkan, dapat

diulang kembali prosesnya dengan hasil yang sama, dan dapat diverifikasi bahwa hasil salinan sama persis dengan barang bukti yang asli. Dalam keadaan dimana proses verifikasi tidak dapat dilakukan, sebagai contoh ketika proses akuisisi yang sedang berjalan, tiba-tiba salinan asli yang sedang dibuat mengalami *error sectors* maka dalam kasus seperti ini petugas investigasi yang melakukan akuisisi harus memilih metode yang paling memungkinkan untuk melakukan proses akuisisi ulang dan mendokumentasikannya, lalu dapat menjelaskan kenapa dilakukan akuisisi ulang dan dapat mempertahankan argumennya. (Badan Standarisasi Nasional, 2014).

2.2.6 Bukti Digital (*Digital Evidence*)

Digital Evidence ialah istilah untuk menjelaskan Informasi atau Dokumen Elektronik yang bisa dijadikan sebagai alat bukti yang disimpan dalam dan bisa diambil kembali dari penyimpanan data disebuah komputer atau media penyimpanan lainnya. Menurut Shinder (2002) digital evidence dapat diklarifikasikan menjadi: – bukti digital asli (*original digital evidence*) yaitu barang secara fisik dan objek data yang berkaitan dengan barang-barang tersebut pada saat bukti disita; dan – bukti digital duplikat (*duplicate digital evidence*), yaitu reproduksi digital yang akurat dari seluruh objek data yang tersimpan didalam benda mati yang asli. Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain, dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya.

2.2.7 *Cybercrime*

Cyber crime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalamnya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit (*carding*), *confidence fraud*, penipuan identitas, pornografi anak, dll. *Cyber crime* sebagai tindak kejahatan dimana dalam hal ini penggunaan komputer secara ilegal (Andi Hamzah, 1989).

2.2.8 *Data Recovery*

Recoveri Data atau sering disebut Data Recovery merupakan proses mengembalikan data atau system dari kondisi yang rusak, gagal, korup, atau tidak bisa diakses ke kondisi awal yang normal. Data yang dikembalikan bisa dari hard disk, flash disk dan media simpan lainnya seperti kamera digital, dan camcorder.

2.2.9 Facebook

Facebook adalah sebuah layanan jejaring sosial berkantor pusat di Menlo Park, California, Amerika Serikat yang diluncurkan pada bulan Februari 2004. Hingga September 2012, Facebook memiliki lebih dari satu miliar pengguna aktif, lebih dari separuhnya menggunakan telepon genggam. Pengguna harus mendaftar sebelum dapat menggunakan situs ini. Setelah itu, pengguna dapat membuat profil pribadi, menambahkan pengguna lain sebagai teman, dan bertukar pesan, termasuk pemberitahuan otomatis ketika mereka memperbarui profilnya. Selain itu, pengguna dapat bergabung dengan grup pengguna dengan ketertarikan yang sama, diurutkan berdasarkan tempat kerja, sekolah atau perguruan tinggi,

atau ciri khas lainnya, dan mengelompokkan teman-teman mereka ke dalam daftar seperti "Rekan Kerja" atau "Teman Dekat".

2.2.10 Twitter

Twitter adalah layanan jejaring sosial dan mikroblog daring yang memungkinkan penggunanya untuk mengirim dan membaca pesan berbasis teks hingga 140 karakter. Akan tetapi pada tanggal 07 November 2017 bertambah hingga 280 karakter yang dikenal dengan sebutan kicauan (*tweet*). Twitter didirikan pada bulan Maret 2006 oleh Jack Dorsey, dan situs jejaring sosialnya diluncurkan pada bulan Juli. Sejak diluncurkan, Twitter telah menjadi salah satu dari sepuluh situs yang paling sering dikunjungi di Internet, dan dijuluki dengan "pesan singkat dari Internet. Di Twitter, pengguna tak terdaftar hanya bisa membaca kicauan, sedangkan pengguna terdaftar bisa menulis kicauan melalui antarmuka situs web, pesan singkat (SMS), atau melalui berbagai aplikasi untuk perangkat seluler.

2.2.11 Statik Forensik

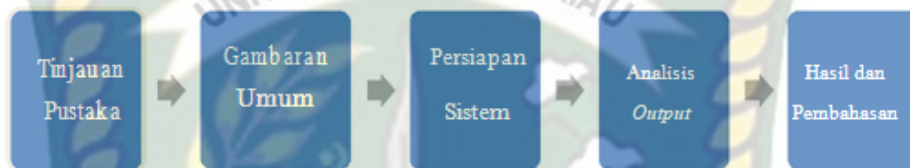
Menggunakan prosedur dan pendekatan konvensional dimana barang bukti elektronik diolah secara *bit-by-bit image* untuk melakukan proses forensik. Proses forensik sendiri berjalan pada sistem yang tidak dalam keadaan menyala atau *running(off)*. Statik forensik difokuskan pada pemeriksaan hasil *imaging* untuk menganalisis isi dari bukti digital, seperti file yang dihapus, history web browsing, berkas fragmen, koneksi jaringan, file yang diakses, history login user, dll.

BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Tahapan Penelitian yang dilakukan adalah menggunakan pendekatan metodologi statik forensik yang akan digambarkan pada gambar 3.1 dibawah ini :



Gambar 3.1 Tahapan Penelitian

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

3.1.1 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 skenario, serta mengimplementasikan Forensika digital.

3.1.2 Bahan dan Alat Penelitian

Pada saat melakukan penelitian ini Penulis menggunakan beberapa *software* dan *hardware* sebagai penunjang penelitian yang akan dilakukan oleh penulis. Untuk spesifikasi alat yang digunakan penelitian adalah sebagai berikut:

1. Kebutuhan perangkat keras.
 - a. Laptop Lenovo Ideapad 320 *Processor intel Core i5*, Memori 4 GB
 - b. Sistem operasi *Windows 10*.
2. Kebutuhan perangkat lunak.
 - a. Software FTK Imager (untuk Imaging barang bukti).
 - b. Software Autopsy

3.1.3 Skenario Simulasi Penelitian

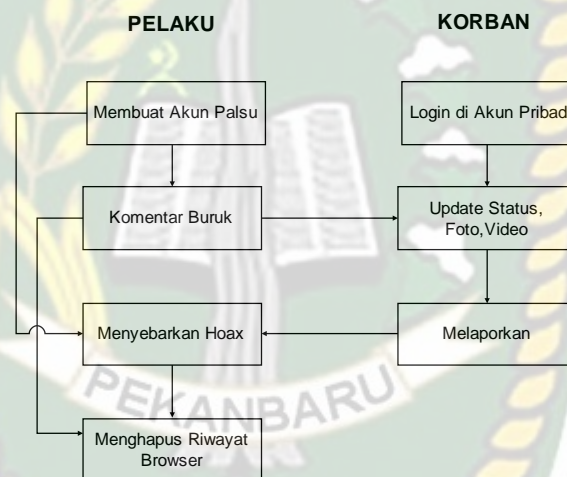
Pada penelitian ini diilustrasikan sebuah skenario kasus tindak kejahatan *cyber*, yaitu seorang pelaku kejahatan di sosial media dengan menyerang korban dengan tindakan ujaran kebencian (*hatespeech*), *bullying*, *body shamming*, dan menyebarkan konten Hoax yang menyangkut korban di media sosial facebook dan twitter.

Skenario kasus yang terjadi bermula saat pelaku merasa iri, dengki ataupun benci dengan korban sehingga sang pelaku membuat akun palsu di media sosial facebook dan twitter guna untuk berbuat perilaku tidak terpuji di media sosial pada korban dengan tujuan agar korban malu ataupun terganggu dengan serangan yang diperbuat pelaku.

Serangan yang dimaksud ialah ketika korban mengupdate status, foto, maupun video di media sosial facebook dan twitter miliknya sang pelaku mengomentari dengan kata-kata kasar (*Hatespeech*), mengejek atau menghina (*Bullying*), dan mengupdate status di akun miliknya memakai foto korban dengan status yang menyudutkan atau mempermalukan korban dengan

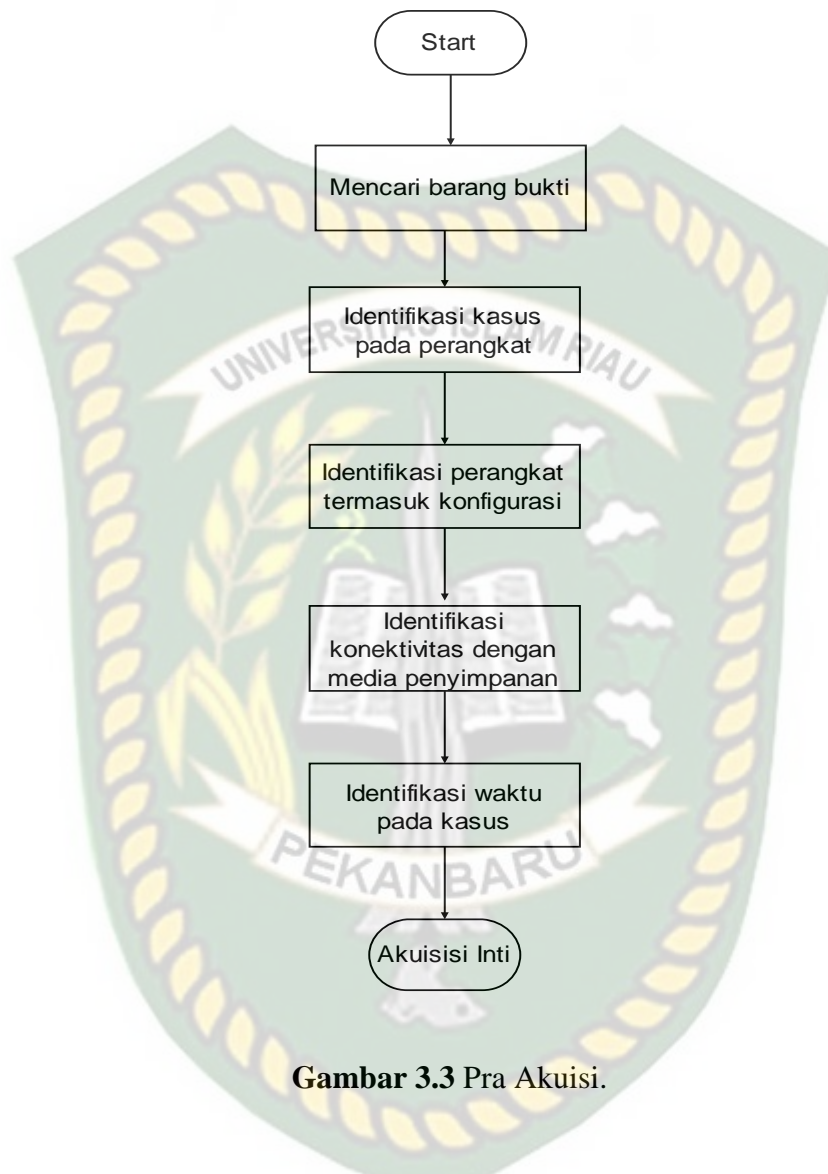
berita yang tidak sebenarnya(Hoax). Karena merasa sangat terganggu dengan pelaku, korban pun membawa kasus tindakan kejahatan di dunia sosial ini ke Ranah Hukum.

Dalam Penelitian ini Diskenariokan pelaku adalah teman korban yang tidak suka dengannya kemudian membuat akun palsu di media sosial untuk menyerang korban menggunakan Laptop dengan Web Browser Mozilla Firefox. Dan untuk menghilangkan jejaknya pelaku menghapus Riwayat di Browser.



Gambar 3.2 Ilustrasi Simulasi Kasus

3.2 Pra Akuisi



Gambar 3.3 Pra Akuisi.

Tabel 3.1 Pra Akuisisi

Tahapan	Tindakan
Mencari barang bukti	Mencari semua barang bukti yang terkait pada kasus yang telah dilaporkan sebelumnya oleh korban. Sesuai dengan SOP surat perintah ataupun arahan dari pihak berwajib.

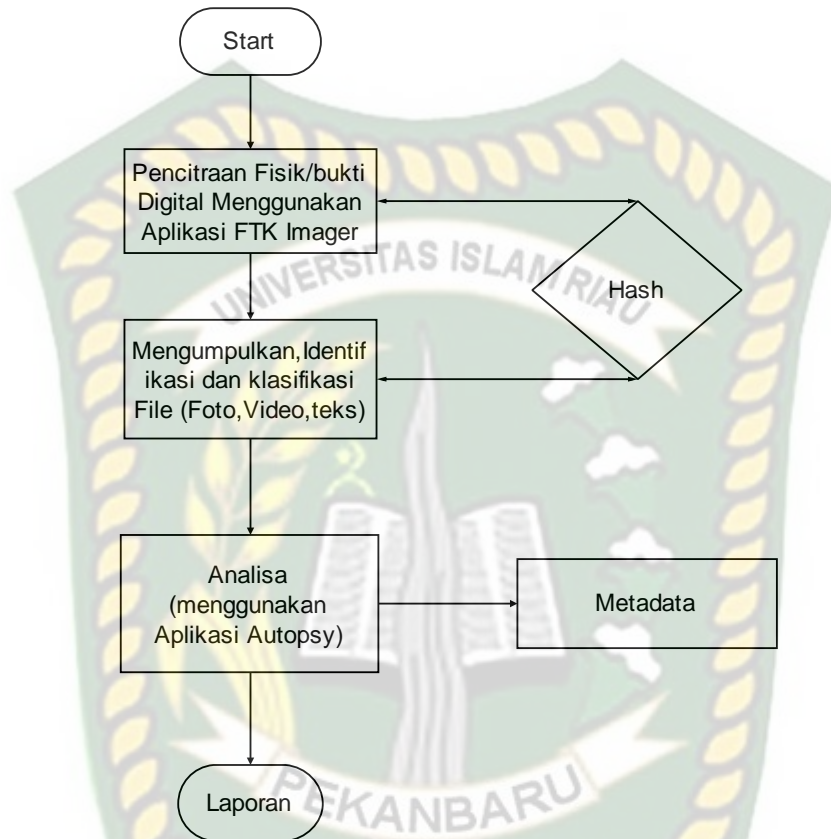
Tahapan	Tindakan
Identifikasi kasus	Menemukan dan mengumpulkan Bukti fisik digital pada kasus serta menyangdingkan kasus tersebut pada UU ITE dalam langkah hukum.
Identifikasi perangkat dan konfigurasi	Menyimpulkan Organisasi dan Arsitektur perangkat barang bukti yang digunakan dalam kasus yang akan di analisa.
Identifikasi konektivitas dengan media penyimpanan	Menentukan Arsitektur dalam USB yang akan digunakan nantinya dalam proses penelitian.
Identifikasi waktu pada kasus	Menampilkan seluruh waktu pada kasus yang akan ditangani. Mulai dari proses pencarian barang bukti sampai dengan barang bukti dikembalikan setelah selesai diperiksa. Selengkapnya pada Tabel 3.2 (<i>Chain of Custody</i>).

Tabel 3.2 Form Chain of Custody

FORM CHAIN OF CUSTODY

A. INFORMASI KASUS			
No Kasus			
Nama Kasus			
Tanggal Kasus			
B. PENANGGUNG JAWAB			
Nama		Alamat:	
Instansi		No.Telp:	
Jabatan		Email:	
C. PENGUMPULAN BARANG BUKTI			
Tanggal Penyitaan			
Waktu Penyitaan			
Lokasi Penyitaan			
DESKRIPSI KASUS			

3.3 Akuisisi Inti



Gambar 3.4 Akuisi Inti.

3.3.1 Investigation (Pemeriksaan)

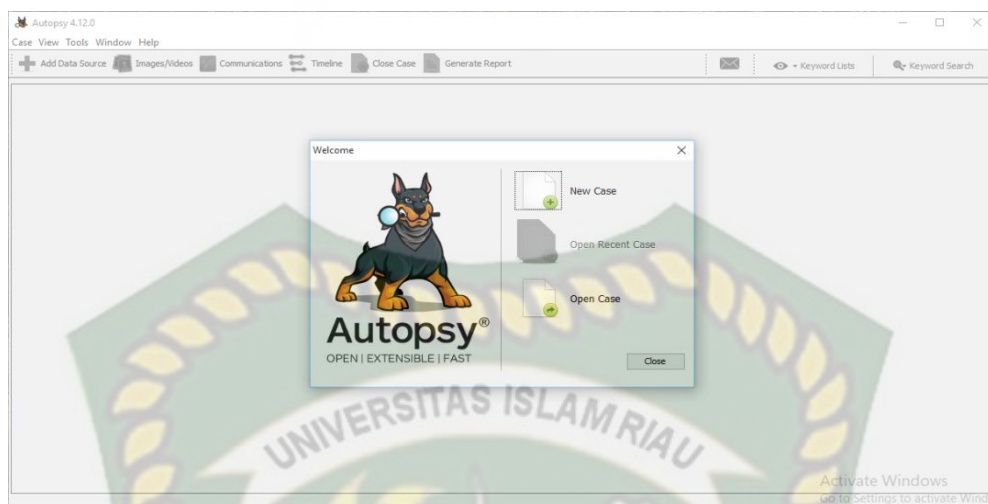
Pada tahapan ini, terhadap *image file* dilakukan pemeriksaan secara komprehensif dengan maksud untuk mendapatkan data digital yang sesuai dengan investigasi, ini artinya analisis forensik harus mendapatkan gambaran fakta kasus yang lengkap dari investigator, sehingga apa yang dicari dan akhirnya ditemukan oleh analisis forensik adalah sama (*matching*) seperti yang diharapkan oleh investigator untuk pengembangan investigasinya. Setelah mendapatkan gambaran

fakta kasusnya, kemudian analisis forensik melakukan pencarian(*searching*) terhadap *image file* untuk mendapatkan file atau data yang diinginkan.

3.3.2 Collection (Pengumpulan)

Pada tahap pengumpulan semua file yang telah selesai proses pencitraan akan dikumpulkan dan kemudian diurutkan. Tahap ini juga merupakan tahap penting dalam forensik digital.

Setelah mendapat file atau data digital yang diinginkan dari proses pemeriksaan diatas, selanjutnya data tersebut dianalisis secara detail dan komprehensif untuk dapat membuktikan kejahatan apa yang terjadi dan kaitannya pelaku dengan kejahatan tersebut. Hasil analisis terhadap data digital tadi selanjutnya disebut barang bukti digital yang harus dapat dipertanggungjawabkan secara ilmiah dan hukum di pengadilan. Untuk *software* yang digunakan adalah Autopsy, adalah sebuah antarmuka grafis untuk tool-tool didalam sleuth kit, yang memudahkan pengguna dalam melakukan investigasi. Mereka dapat menganalisis disk dan file system windows dan unix (NTFS, FAT, UFS1/2, EXT2/3). Autopsy menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci dan operasi lainnya. Autopsy menggunakan perl untuk menjalankan program-program sleuth kit dan mengubah hasilnya ke HTML, oleh karena itu pengguna autopsy membutuhkan web client untuk mengakses fungsi-fungsinya. Berikut adalah tampilan awal aplikasi autopsy pada windows.



Gambar 3.5 Tampilan awal Aplikasi Autopsy

3.3.3 Reporting (Laporan)

Pada tahap pelaporan isi terlampir berisi berupa penyelidikan dari awal sampai akhir, bentuk bukti, metodologi dan kesimpulan dari awal sampai akhir kasus yang akan diselesaikan Serta Metadata yang telah diperoleh dalam melakukan penelitian.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Skenario Kasus

Dalam Penelitian ini sesuai dengan metode yakni Statik Forensik maka diskenariokan dalam suatu adegan dalam Facebook dan Twitter, akun Facebook bernama “Tersang Kha” sebagai pelaku dan “Chor ban” sebagai korban, dan akun Twitter @kha_tersang sebagai pelaku dan @ban_chor sebagai korbannya melakukan aktivitas di dunia maya facebook dan twitter miliknya. Seketika korban update status maupun foto sang pelaku lalu mengomentari korban dengan perkataan yang tidak mengenakan dan di wall profil pelaku juga beredar berita hoax dan konten pornografi. Lalu korban merasa resah dengan pelaku maka korban melakukan tindakan yakni melaporkan pelaku kepada pihak yang berwajib dalam kasus UU ITE pencemaran nama baik dan berita bohong serta konten pornografi. Dan sang pelaku pun merasa takut lalu pelaku menghapus seluruh riwayat browser nya.

Begitu juga dalam proses penyelidikan dilakukan sesuai dengan surat perintah sesuai prosedur dalam *chain of custody* yang telah dilaporkan dengan mengumpulkan barang bukti yang terduga terlibat dalam kasus kemudian dilakukan dokumentasi dari awal penangkapan hingga bukti pelaporan yang dilengkapi oleh korban.

Tabel 4.1 Chain of Custody

B. INFORMASI KASUS			
No Kasus	001/026		
NamaKasus	Tindak kejahatan media sosial (Facebook danTwitter)		
TanggalKasus	19 November 2019		
B. PENANGGUNG JAWAB			
Nama	GusraMishardila	Alamat:	Panam, Pekanbaru
Instansi	UIR	No.Telp:	081390842700
Jabatan	Investigator	Email:	Gusramishardila@gmail.com
C. PENGUMPULAN BARANG BUKTI			
Tanggal penyitaan	22 November 2019		
Waktu Penyitaan	02:46 PM ketika pelaku sedang tidur siang di kediamannya		
Lokasi Penyitaan	Kediaman pelaku komplek dokagu		
DESKRIPSI KASUS			
Telah terjadi kasus <i>Cybercrime</i> di media sosial Facebook dan Twitter antara korban bernama “Chorban” dan pelaku bernama “Tersangkha” dalam kasus <i>Cyberbullying, HateSpeech, Hoax</i> dan konten pornografi.			

4.2 Pra Akuisisi

4.2.1 Mencari Barang Bukti

Setelah mendapat laporan dengan kasus UU ITE sang investigator melakukan penangkapan dan mengamankan barang bukti yang dicurigai digunakan oleh pelaku untuk melakukan tindakan kejahatan di facebook dan twitter tersebut. Didalam kediaman pelaku ditemukan sebuah laptop Acer Aspire dan Flashdisk Thosiba 4GB. Kemudian barang bukti tersebut disita dan dibawa ke laboratorium digital foresik untuk di investigasi.



Gambar 4.1 Barang bukti yang ditemukan

4.2.2 Kasus pada Perangkat

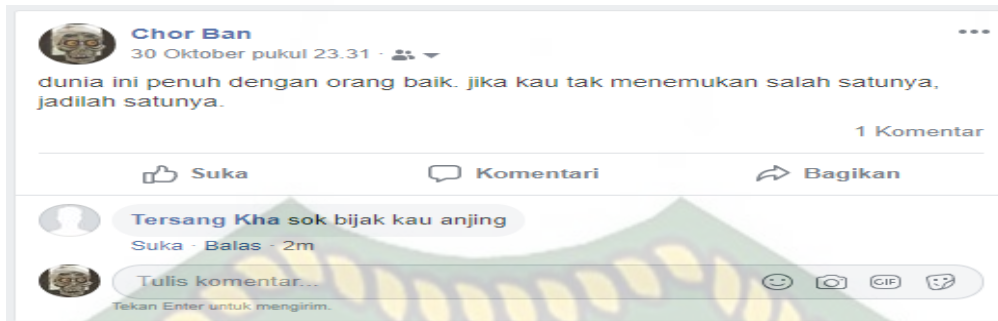
Kasus yang menjerat tersangka dengan perangkat personal komputer nya yakni penyebaran Hoax, Konten Pornografi,ujaran kebencian dan bullying. Dan dalam pelaporan dilampirkan hasil screenshot tindak kejahatan yang diperbuat pelaku. Kemudian dikaitkan dengan undang-undang yang berlaku.



Gambar 4.2 Kasus konten pornografi di facebook

Dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU ITE”) Sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU 19/2016”). Pada Pasal 27 ayat (1) UU ITE adalah sebagai berikut:

Setiap orang dengan sengaja tanpa dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen elektronik yang memiliki muatan yang melanggar kesusilaan dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000 (satu milyar rupiah).



Gambar 4.3 Kasus *HateSpeech* di facebook



Gambar 4.4 Kasus *HateSpeech* di Twitter

Pada Pasal 27 ayat (2) UU ITE adalah: Setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antargolongan (SARA) sebagaimana dimaksud dalam pasal 28 ayat(2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000 (satu milyar rupiah).



Gambar 4.5 Kasus *Bullying* di Facebook



chor ban
@ban_chor

namamu adalah jawaban dari setiap doaku

[Translate Tweet](#)

More replies



tersang kha @KhaTersang · Nov 7, 2019

Replying to @ban_chor

sok bijak kau



tersang kha @KhaTersang · Nov 7, 2019

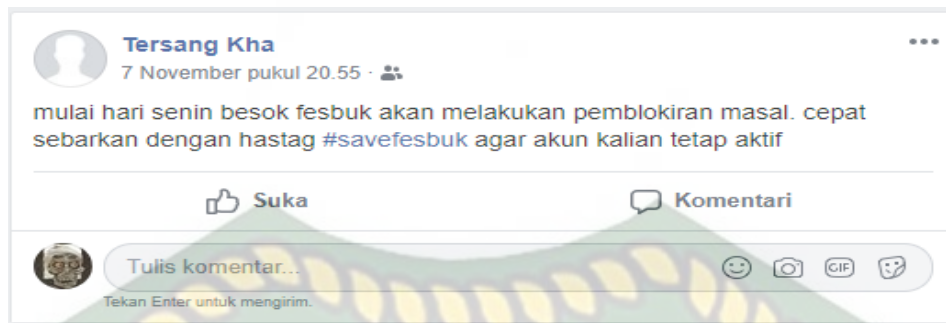
Replying to @ban_chor

badan kurus kayak tiang bendera aja belagu

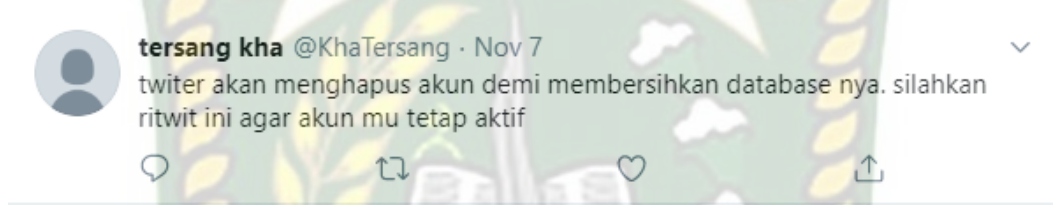


Gambar 4.6 Kasus *Bullying* di Twitter

Pada Pasal 27 ayat (3) UU ITE adalah: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. Ancaman pidana bagi orang yang melanggar diatur dalam pasal 45 ayat (3) UU 19/2016 yang berbunyi: dipidana dengan pidana penjara paling lama 4(empat) tahun dan/atau denda paling banyak Rp750.000.000(tujuh ratus lima puluh juta rupiah).



Gambar 4.7 Kasus penyebaran Hoax di facebook



Gambar 4.8 Kasus penyebaran Hoax di Twitter

Pada Pasal 28 UU ITE adalah: Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik sebagaimana dimaksud dalam pasal 28 ayat (1) dipidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1 milyar.

4.2.3 Perangkat dan Konfigurasi

Setelah barang bukti berupa perangkat laptop acer investigator melakukan penelitian konfigurasi dalam perangkat tersebut.

Tabel 4.2 Spesifikasi Perangkat

Nama perangkat	Acer Aspire 4739
Prosesor	Intel Core i3 (3MB L3 Cache, 2,4 Ghz)
Layar	14"HD Acer cineCristal LED backlight TFT LCD
RAM	2GB DDR3
Hardisk	320 GB SATA
Jaringan	Wifi link 802.11b/g
OS	Windows 10

4.2.4 Konektivitas dan Penyimpanan

Untuk dilakukannya penelitian diperlukan konektivitas dan penyimpanan dalam barang bukti berupa hardisk yang memerlukan *Case Hardisk external* untuk mendukung nya proses penelitian.

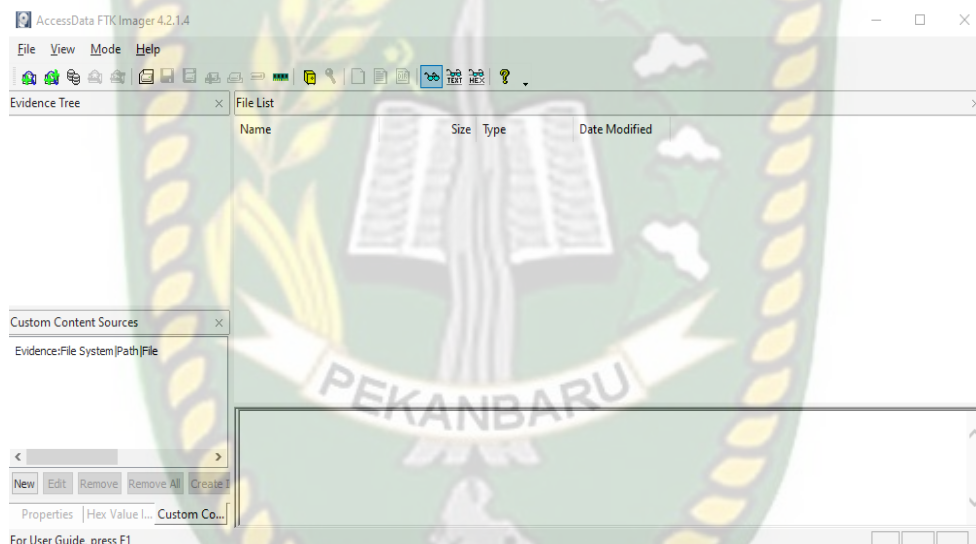
Tabel 4.3 Spesifikasi Konektivitas

Nama	ORICO 219U3
Compatible Drive	SATA 2.5 inch HDD/SSD-7mm dan 9.5mm
Output	USB 3.0 – Micro B
Controller	JMSS78
Capacity	250GB up to 2TB
Dimensions	124.5 x 79 x 13mm
Material	ABS Transparan
Transmission Rate	5GBps

4.3 Akuisisi Inti

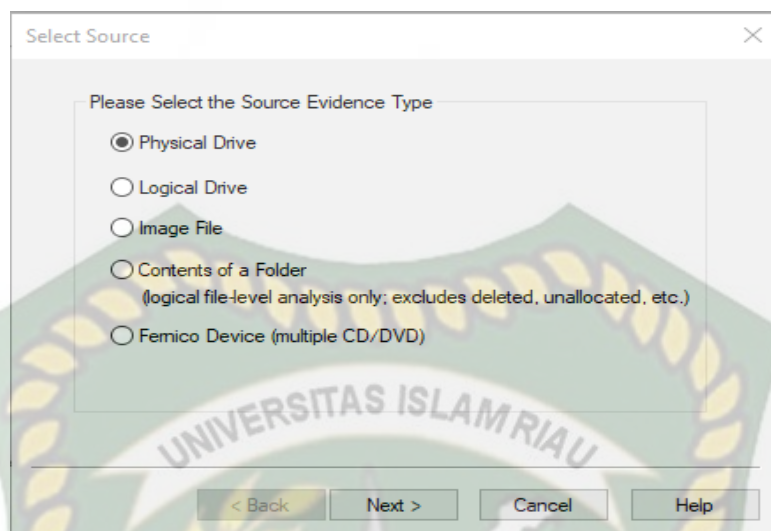
4.3.1 Proses *Imaging* Barang Bukti (Pencitraan)

Disaat persiapan akuisisi telah lengkap dan saatnya kita mulai mengakuisisi barang bukti tersebut dengan cara imaging atau pencitraan terhadap barang bukti agar barang bukti tersebut terjaga keasliannya dan bisa dipertanggungjawabkan. Aplikasi yang digunakan yaitu FTK Imager. Tampilan awal seperti pada gambar 4.9 berikut:



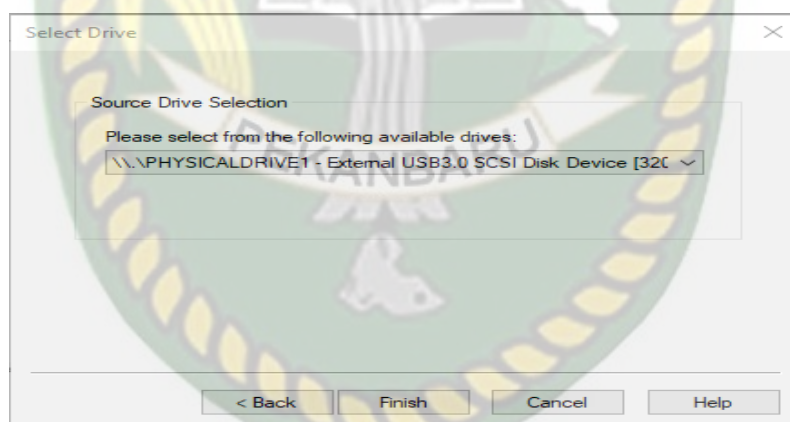
Gambar 4.9 Tampilan Awal Aplikasi FTK Imager

Setelah USB sudah dikoneksikan ke komputer dan sudah terdeteksi maka kita bisa langsung saja memulai proses imaging yaitu 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.



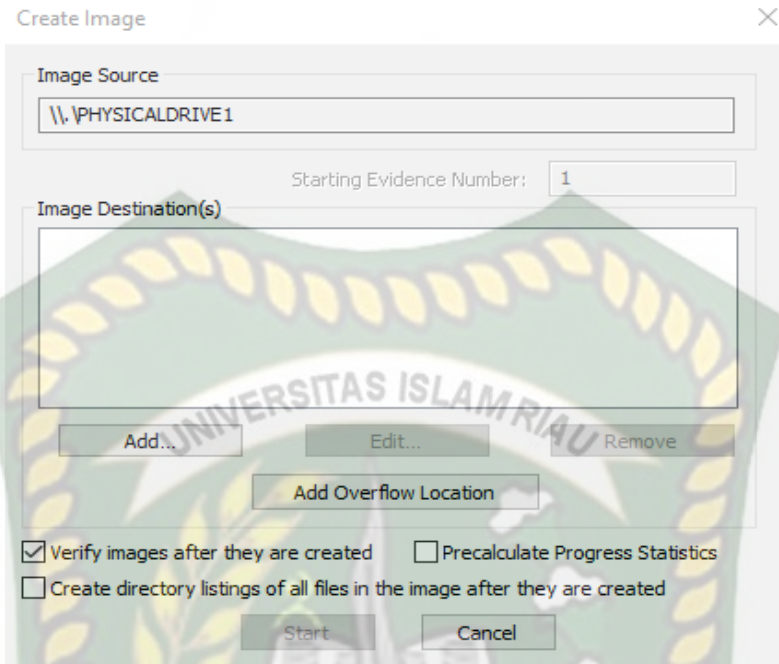
Gambar 4.10 Pilihan tipe barang bukti

Kemudian klik Next, setelah itu pilih Hardisk yang telah kita hubungkan melalui case yakni external memori 3.0



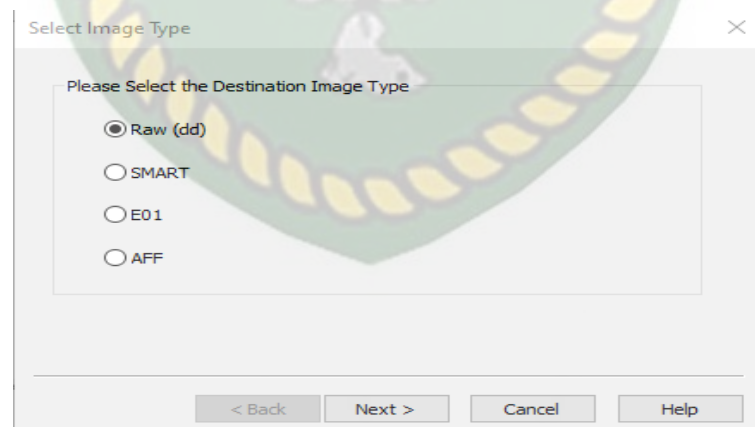
Gambar 4.11 Pilihan Penyimpan yang akan di imaging

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



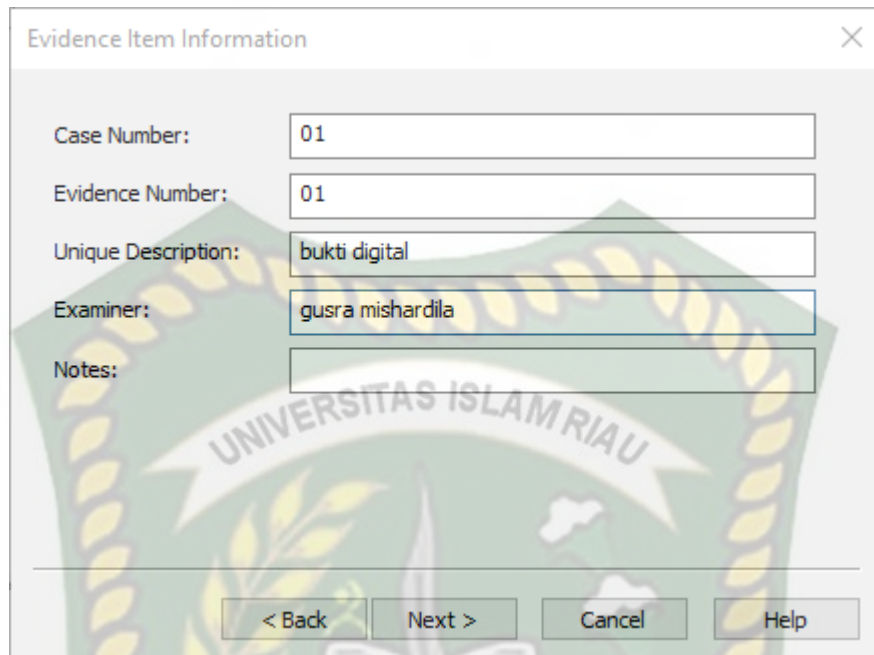
Gambar 4.12 Lokasi penyimpanan Imaging

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 4.13 Pilihan format imaging

Kemudian pilih lokasi folder yang diinginkan dan buat nama file imaging. Lalu klik Next.



Evidence Item Information

Case Number: 01

Evidence Number: 01

Unique Description: bukti digital

Examiner: gusra mishardila

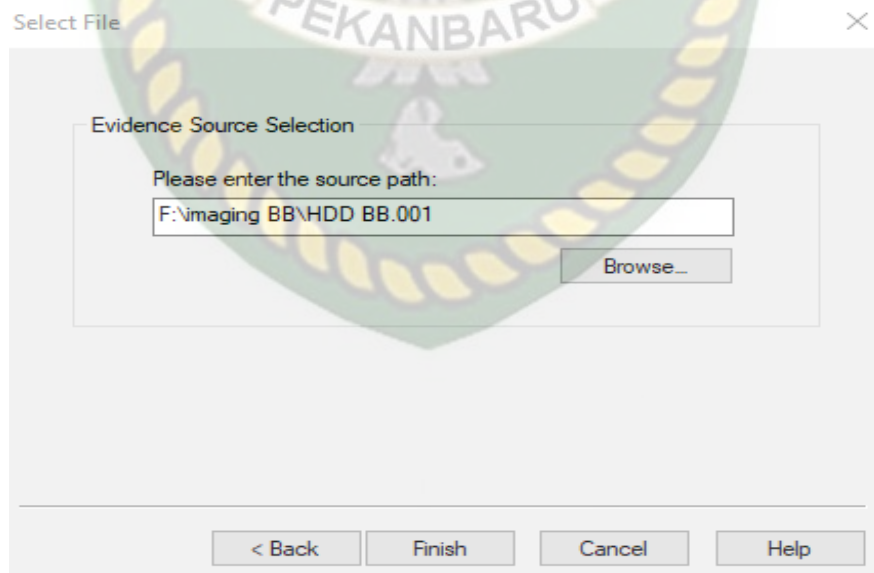
Notes:

< Back Next > Cancel Help

Gambar 4.14 Informasi item batang bukti

Kemudian pilih lokasi folder yang diinginkan dan buat nama file imaging.

Lalu klik finish.



Select File

Evidence Source Selection

Please enter the source path:

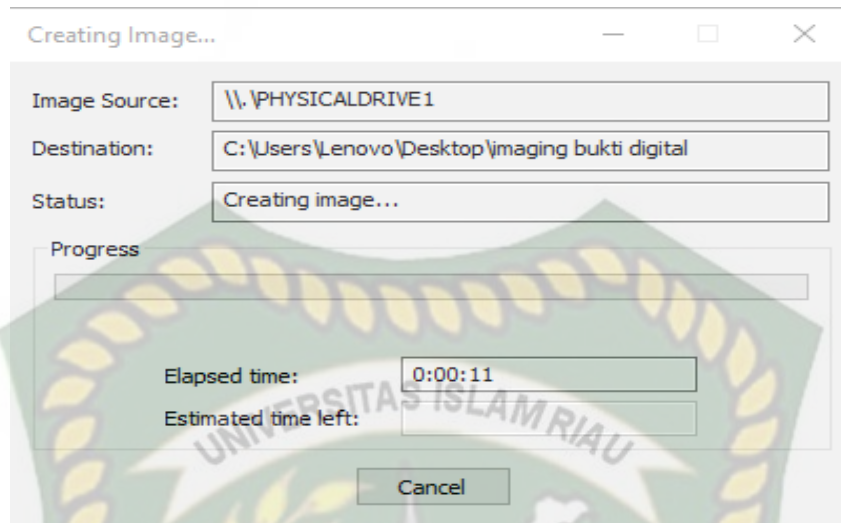
F:\imaging BB\HDD BB.001

Browse...

< Back Finish Cancel Help

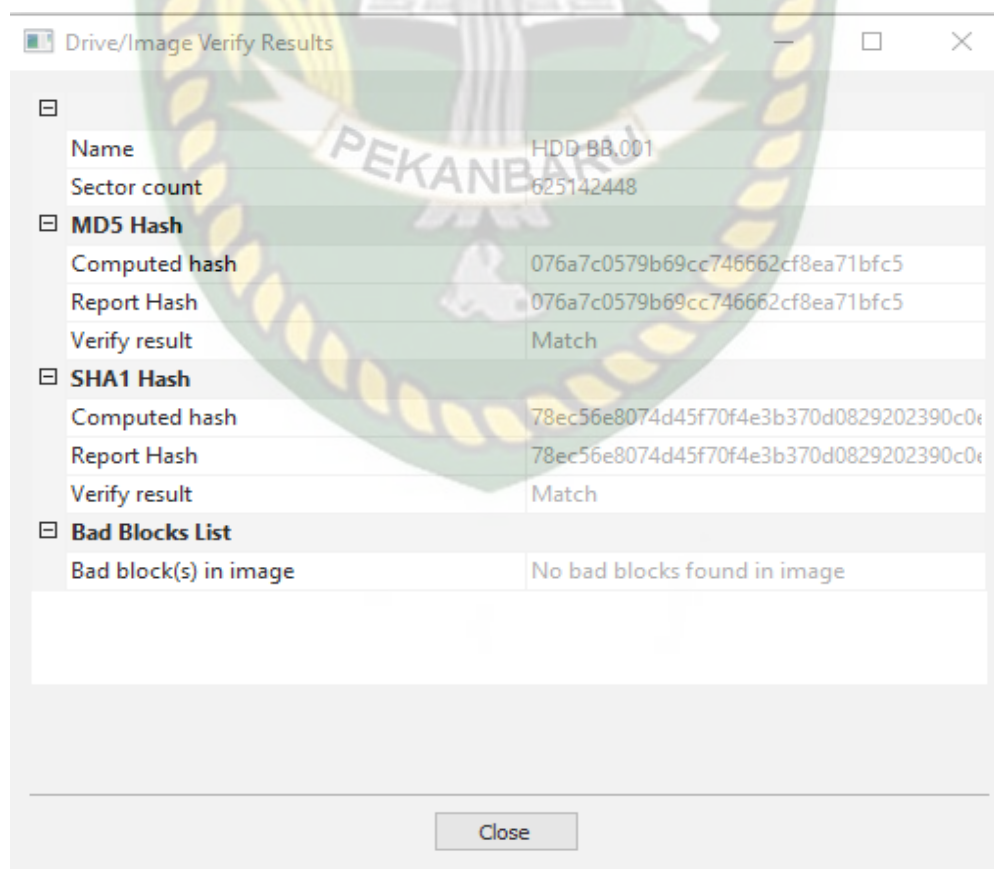
Gambar 4.15 Alamat penyimpanan imaging

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



Gambar 4.16 Proses Imaging sedang berjalan

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



Gambar 4.17 Laporan kode Hash

4.3.2 Analisa Menggunakan Aplikasi Autopsy

Tahap ini adalah untuk menganalisis *file image* yang dihasilkan dengan menggunakan *tools* Autopsy dalam *platform* Windows. Saat membuka aplikasi Autopsy pertama yang dilakukan adalah mengisi beberapa form yaitu *form case info* untuk penamaan dan tata letak kasus yang dianalisis dan *additional information* untuk memberi urutan kasus dan siapa investigator dalam melakukan analisis. Untuk melihat kedua *form* dilihat pada gambar 4.18 dan gambar 4.19.

The screenshot shows the 'New Case Information' dialog box with the 'Case Information' step selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Case Information' section contains the following fields:

- Case Name:
- Base Directory:
- Case Type: Single-user Multi-user
- Case data will be stored in the following directory:

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Gambar 4.18 Merupakan case information

The screenshot shows the 'New Case Information' dialog box with the 'Optional Information' step selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Optional Information' section contains the following fields:

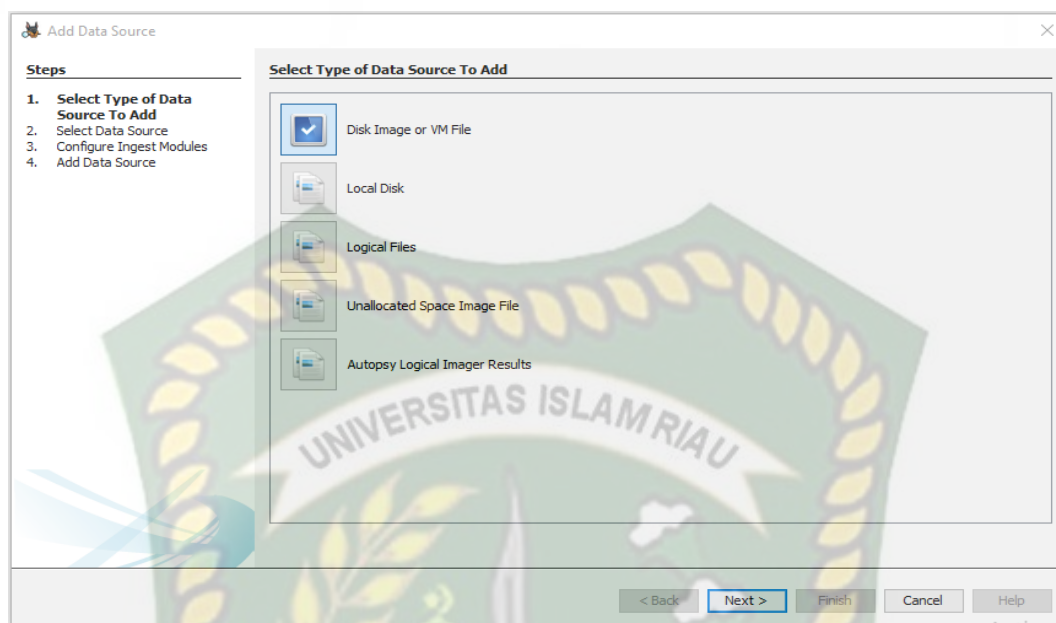
- Case Number:
- Examiner Name:
- Phone:
- Email:
- Notes:
- Organization:

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Gambar 4.19 Form Additional Information Aplikasi Autopsy

Pada Gambar 4.18 Merupakan Form Case Information. Pada form ini menjelaskan mengenai kasus yang ingin dianalisis dari mengisi nama kasus dan pemilihan letak direktori untuk menyimpan kasus tersebut yang akan menghasilkan sebuah dokumen, sedangkan pada gambar 4.19 Merupakan form Additional Information menjelaskan mengenai kasus ke berapa dan siapa nama pengguna aplikasi autopsy yang akan melakukan analisis tersebut. Dari kedua form tersebut berfungsi untuk mendapatkan rekam analisis yang dapat dipertanggung jawabkan.

Setelah melakukan pengisian 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, menentukan ingest modules 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 4.20.



Gambar 4.20 Form Menentukan tipe yang akan dianalisis

Gambar 4.20 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 dihasilkan aplikasi bertipe *disk image* dan juga pilihan 1 memiliki fungsi untuk dapat menganalisis file tersebut secara menyeluruh, untuk pilihan 2-3 adalah pilihan untuk menganalisis file dari *localdisk* dan *logical files*, dan 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 akan ada *form* mengambil *file image* yang dihasilkan aplikasi untuk dimasukkan dalam aplikasi autopsy dan dapat dilakukan analisis dari file tersebut, *form* tersebut dapat dilihat pada [Gambar 4.21](#).

Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: F:\imaging BB\DD BB.001

Ignore orphan files in FAT file systems

Time zone: (GMT+7:00) Asia/Bangkok

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

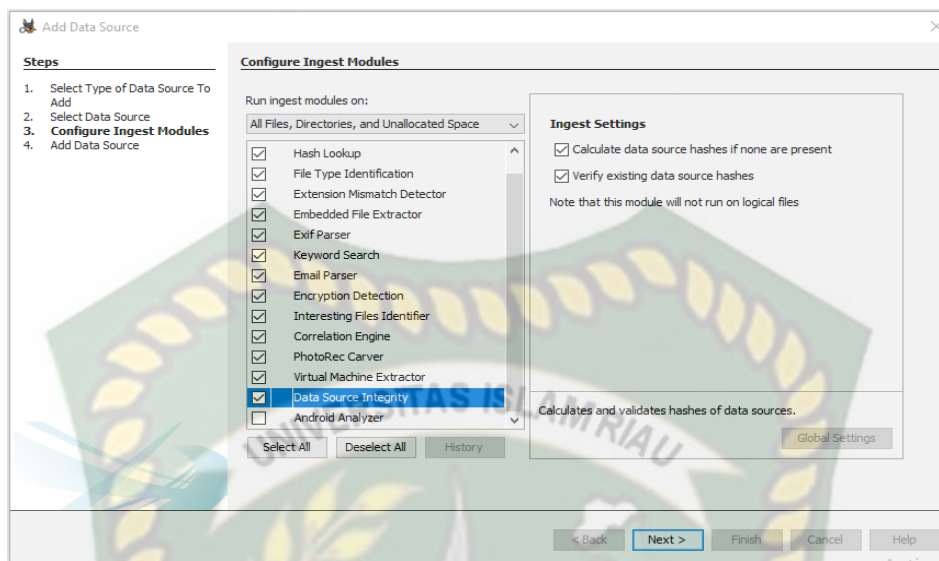
SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help

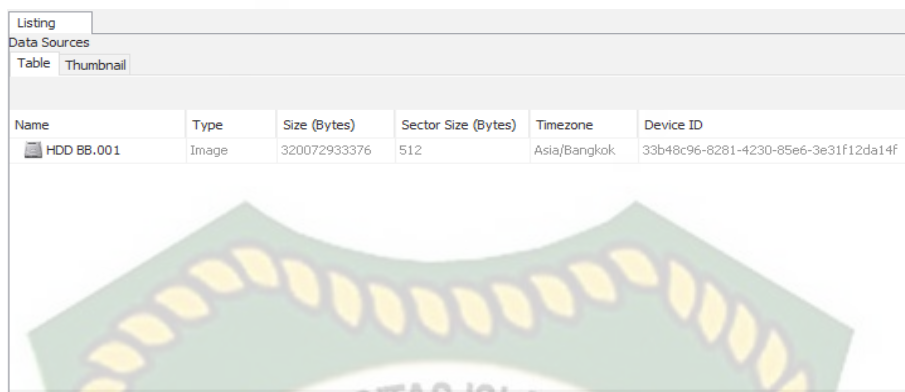
Gambar 4.21 Form Mengambil Data yang ingin Dianalisis.

Pada Gambar 4.21 merupakan *Form* untuk mengambil sebuah data *file image* yang dihasilkan aplikasi yang akan dimasukkan dalam aplikasi autopsy untuk dilakukan analisis dari data tersebut, setelah data sudah dipastikan masuk dan terbaca oleh aplikasi autopsy, maka selanjutnya aplikasi menampilkan *form ingest modules* dan seorang analisis akan mengisi untuk menentukan *form ingest modules* yang dibutuhkan untuk analisis aplikasi autopsy dan dapat dilihat pada Gambar 4.22.



Gambar 4.22 Form penentuan *ingest modules* Aplikasi Autopsy.

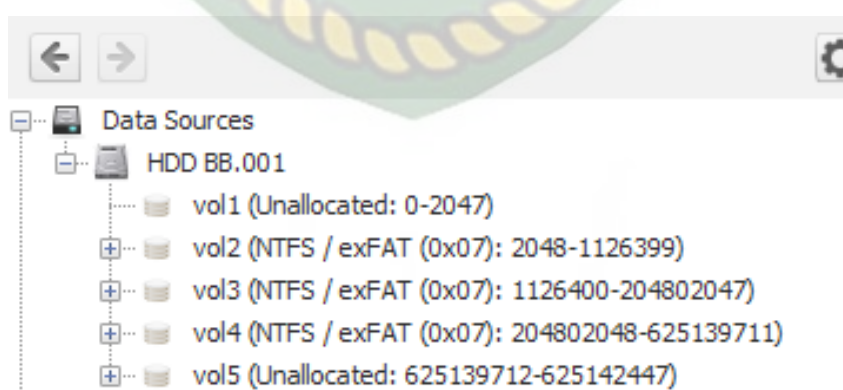
Pada Gambar 4.22 merupakan *form* penentuan untuk memilih *ingest modules* dalam aplikasi autopsy yang berfungsi untuk membagi data yang dibutuhkan saat melakukan proses analisis dari *file image* yang sudah dimasukkan dalam aplikasi autopsy agar tersusun dengan rapi dan dapat dianalisis secara menyeluruh dalam aplikasi autopsy, dari *ingest modules* dalam aplikasi autopsy banyak pilihan yang memiliki fungsi untuk kepentingan analisis agar mudah dilakukan. Setelah penentuan *ingest modules*, maka aplikasi autopsy menjalankan *ingest modules* 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 terbagi beberapa komponen data dari fungsi *ingest modules* yang dijalankan aplikasi autopsy dapat dilihat pada Gambar 4.23



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
HDD BB.001	Image	320072933376	512	Asia/Bangkok	33b48c96-8281-4230-85e6-3e31f12da14f

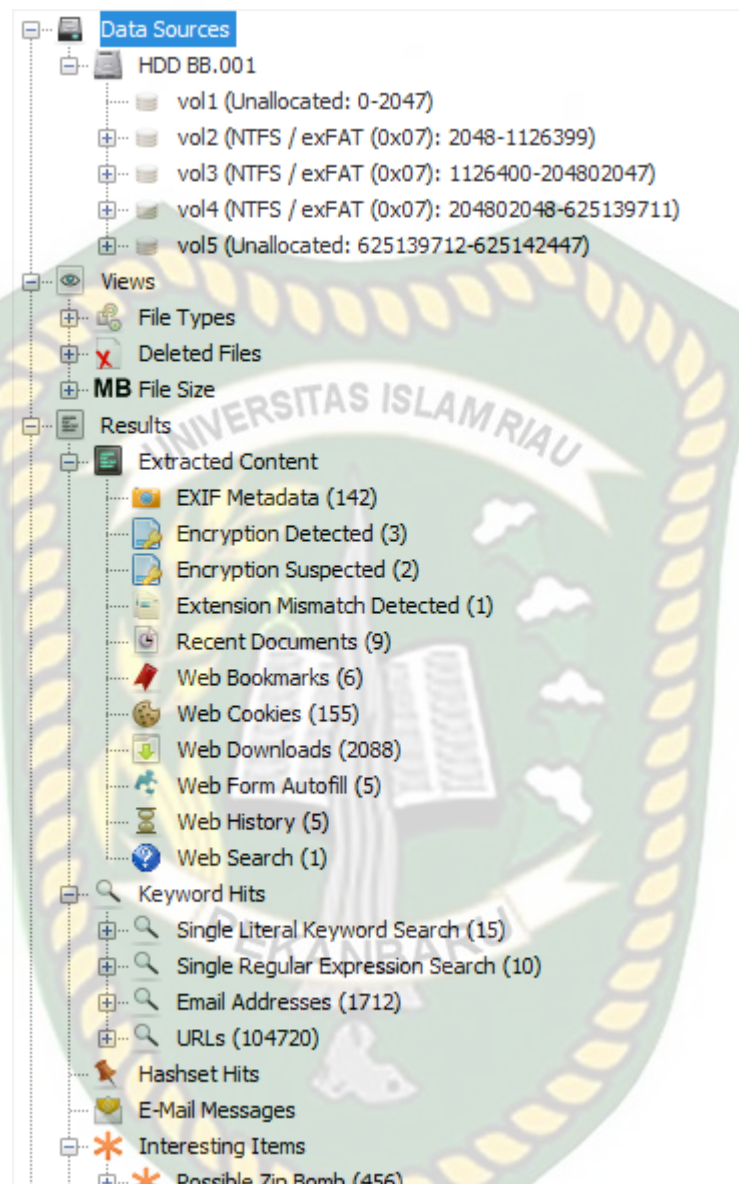
Gambar 4.23 Data Source dalam Aplikasi Autopsy

Pada Gambar 4.23 merupakan data *source* yang dihasilkan aplikasi autopsy dari *file image* yang telah dimasukkan ke dalam 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 4.24



Gambar 4.24 Partisi dalam Data Source aplikasi Autopsy.

Pada Gambar 4.24 merupakan daftar partisi-partisi dari *file image* penyimpanan yang sudah dijadikan *data source* dalam aplikasi autopsy. Dari daftar partisi- partisi tersebut dapat mengetahui semua data-data yang terdapat dalam partisi tertentu yang dihasilkan dari *data source* dalam aplikasi autopsy dan dapat juga data tersebut diekstrak ke perangkat laptop yang akan dijadikan file barang bukti yang dihasilkan dari proses analisis. Dari semua daftar partisi yang terdapat dalam *file image* penyimpanan. Ada beberapa partisi utama yang dijadikan bahan analisis oleh seorang forensika digital, partisi tersebut adalah partisi “system” pada vol 3 yang berfungsi untuk melihat data sistem yang digunakan dalam penyimpanan. kedua adalah partisi “userdata” pada vol 4 yang berfungsi untuk melihat semua data-data yang tersimpan dalam penyimpanan. Setelah melakukan analisis dari kedua partisi utama dalam penyimpanan yang dihasilkan dari *data source* aplikasi autopsy, maka aplikasi juga memberikan fasilitas untuk melihat semua data-data yang memiliki *file type*. untuk melihat semua data (10%) berdasarkan *file type*-nya dan telah tersusun dengan rapi dapat dilihat pada Gambar 4.25

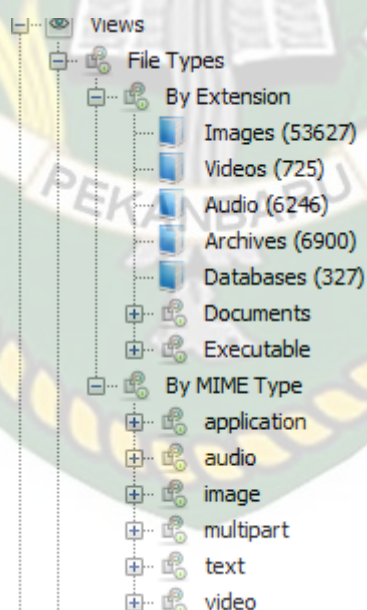


Gambar 4.25 Detail Data Source dari Aplikasi Autopsy(10%)

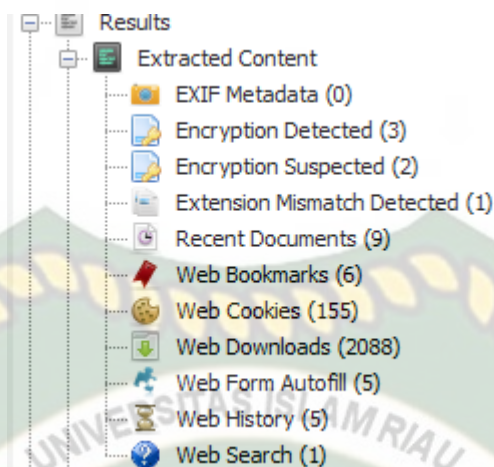
Pada Gambar 4.25 merupakan fasilitas dari autopsy untuk melihat semua detail data-data yang terdapat dalam penyimpanan internal yang telah tersusun dengan rapi dan telah menjadi *data source* dalam aplikasi autopsy, dari detail *data source* tersebut terbagi dari beberapa komponen data dari penyimpanan internal, data tersebut diantaranya berdasarkan dari *file type*, *delete files*, dan *file size* yang terbilang cukup besar.

Data berdasarkan *file types* terbagi menjadi 2 bagian data, bagian data pertama adalah data berdasarkan *extension* yang berfungsi untuk melihat semua data-data yang memiliki format seperti gambar, video, audio dan dokumen yang didapat dari proses analisis dan juga diekstrak ke dalam perangkat laptop untuk dijadikan barang bukti dari hasil proses analisis, sedangkan bagian data kedua adalah data berdasarkan *MIME type* adalah data seperti aplikasi, pesan, dan lainnya.

Data berdasarkan *deleted file* berfungsi untuk melihat data apa saja yang sudah terhapus sebelumnya dalam penyimpanan internal dari data *file system* dan juga data lainnya yang sudah terhapus yang dapat dilihat pada Gambar 4.26.



Gambar 4.26 Isi Konten dalam Data Source Aplikasi Autopsy



Gambar 4.27 Isi Konten Results

Pada Gambar 4.27 Merupakan hasil data dari konten yang terdapat dalam *web cookies*, *web search*, *web history*, dan *web download* dalam *web browser* dan sebagainya dari data tersebut didapatkan hasil dari rekam jejak penggunaan yang dapat di ekstrak untuk dijadikan barang bukti berupa dokumen. dan konten lainnya dari penggunaan email, melihat pesan email.

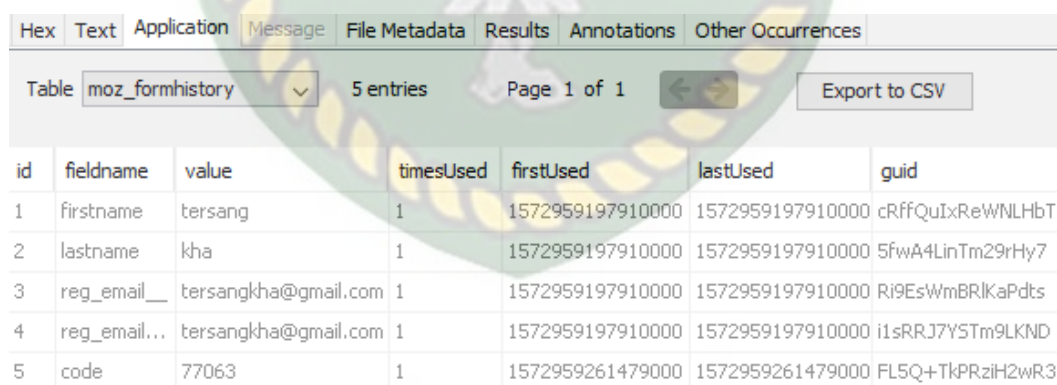
Setelah proses validasi selesai maka data-data yang telah didapatkan akan muncul di halaman data source dalam aplikasi autopsy. Untuk penelitiannya memerlukan banyak waktu untuk validasi data. Untuk lebih lengkap sesuai dengan gambar 4.28 Dibawah ini.

Location:	C:\Users\Lenovo\Documents
Size:	10,5 GB (11.330.837.564 bytes)
Size on disk:	10,6 GB (11.413.991.424 bytes)
Contains:	44.063 Files, 2.166 Folders
<hr/>	
Created:	Rabu, 22 Januari 2020, 21.57.12

Gambar 4.28 Metadata Barang bukti yang dianalisa

Untuk penelitian sendiri terlihat pada gambar diatas dimulai pada 22 Januari 2020 pada pukul 21:57 WIB dan selesai pada 24 Januari 2020 pada pukul 09:00 WIB yang artinya selesai dalam waktu kurang lebih 35 jam hanya untuk 10% data dari keseluruhan dalam barang bukti dan penyimpanan berkapasitas 10.5 GB dengan 44.063 file dalam 2.116 folder.

Dalam barang bukti yang ditemukan dalam penelitian ini apapun yang berhubungan dengan kasus yang akan ditangani agar bisa dipertanggungjawabkan dengan kasus yang sedang berjalan. Salah satunya ditemukan jejak email dari sang pelaku didalam perangkat yang dijadikan barang bukti sama persis dengan usernya di akun facebook milik pelaku yang berasal dari moz history yakni yang ditampilkan pada gambar 4.29 Dan tampilan metadatanya yang berisikan waktu dan rincian mulai dari nama,type,kode hash dan lain sebagainya pada gambar 4.30.



id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	firstname	tersang	1	1572959197910000	1572959197910000	cRffQuIxReWNLHbT
2	lastname	kha	1	1572959197910000	1572959197910000	5fwA4LinTm29rHy7
3	reg_email__	tersangkha@gmail.com	1	1572959197910000	1572959197910000	Ri9EsWmBRlKaPdts
4	reg_email...	tersangkha@gmail.com	1	1572959197910000	1572959197910000	i1sRRJ7YSTm9LKND
5	code	77063	1	1572959261479000	1572959261479000	FL5Q+TkPRziH2wR3

Gambar 4.29 Username pelaku

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Name	/img_HDD BB.001/vol_vol3/Users/User/AppData/Roaming/Mozilla/Firefox/Profiles/9com2xx.default/formhistory.sqlite						
Type	File System						
MIME Type	application/x-sqlite3						
Size	196608						
File Name Allocation	Allocated						
Metadata Allocation	Allocated						
Modified	2019-11-05 20:07:41 WIB						
Accessed	2019-11-18 16:22:16 WIB						
Created	2019-11-05 20:03:27 WIB						
Changed	2019-11-05 20:07:41 WIB						
MD5	39269a54a8135ce97868507e6f60c18a						

Gambar 4.30 Metadata Username pelaku

Kemudian barang bukti yang ditemukan ialah foto yang berasal dari pelaku untuk konten pornografi yang disebarluaskan di akun facebook miliknya.

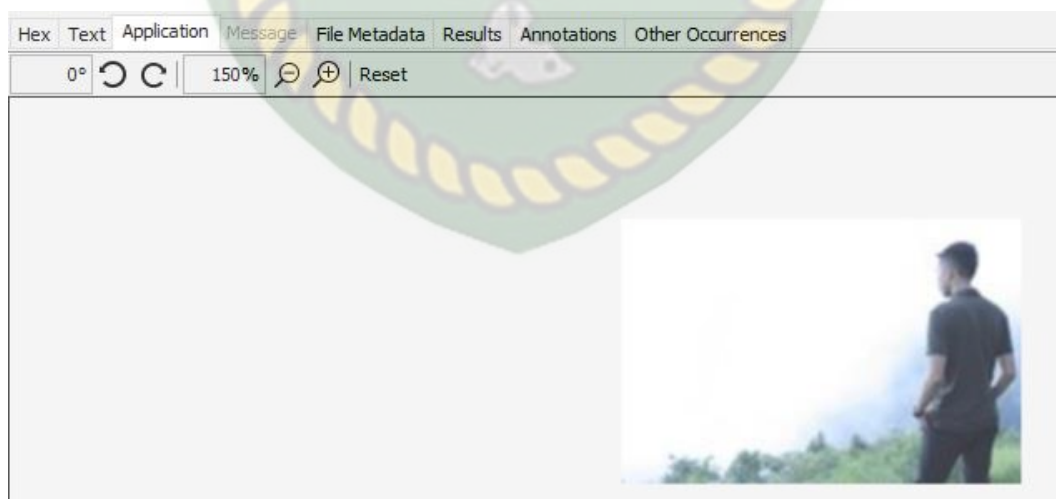


Gambar 4.31 Foto penyebaran konten pornografi di Facebook

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Name	/img_HDD						
	BB.001/vol_vol3/Users/User/AppData/Local/Mozilla/Firefox/Profiles/9com2xxd.default/cach						
Type	File System						
MIME Type	image/jpeg						
Size	15356						
File Name	Allocated						
Allocation	Allocated						
Metadata	Allocated						
Allocation	Allocated						
Modified	2019-11-18 16:36:26 WIB						
Accessed	2019-11-18 16:36:26 WIB						
Created	2019-11-18 16:36:26 WIB						
Changed	2019-11-18 16:36:26 WIB						
MD5	899607c02408d3b8462a72e3d4792b76						
Hash							

Gambar 4.32 Metadata foto penyebaran konten pornografi di Facebook

Selanjutnya yang ditemukan pada perangkat milik pelaku ialah foto dari korban yang pelaku komentari dengan kata-kata tidak seharusnya dikatakan atau ujaran kebencian yang pelaku lontarkan kepada korban di media sosial facebook.



Gambar 4.33 Foto ujaran kebencian korban di facebook

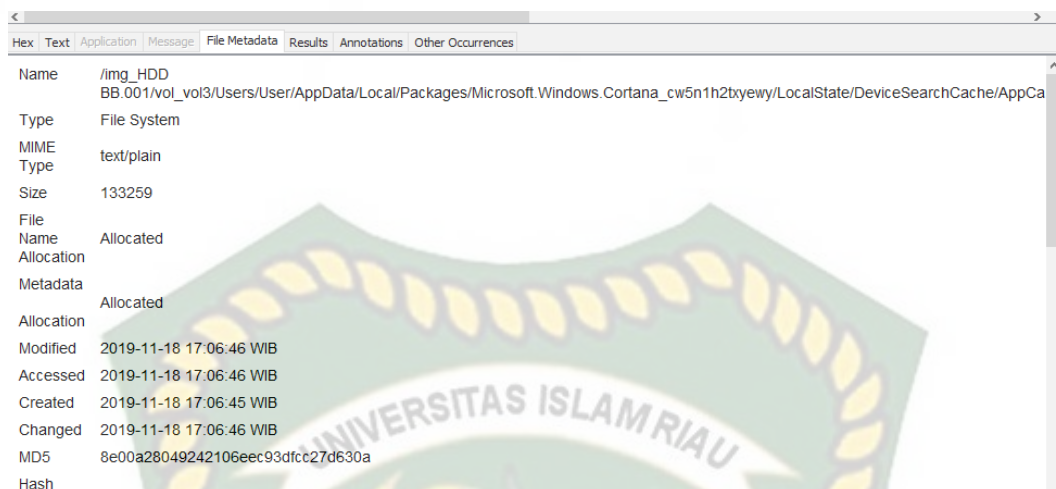
Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Name	/img_HDD						
	BB.001/vol_vol3/Users/User/AppData/Local/Mozilla/Firefox/Profiles/9com2xxd.default/ca						
Type	File System						
MIME Type	image/jpeg						
Size	12810						
File Name Allocation	Allocated						
Metadata Allocation	Allocated						
Modified	2019-11-18 17:01:02 WIB						
Accessed	2019-11-18 17:01:02 WIB						
Created	2019-11-18 16:24:45 WIB						
Changed	2019-11-18 17:01:02 WIB						
MD5 Hash	bb3163d01c24ed2a8708eed546ceaafa						

Gambar 4.34 Metadata Foto ujaran kebencian korban di facebook

Barang bukti selanjutnya yang bisa membuktikan kejahatan korban ialah ditemukan status twitter korban yang dikomentari oleh pelaku dengan kata-kata kasar dan merendahkan korban.

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Strings Indexed Text Translation							
Page: 1 of 9				Page < >		Go to Page:	
						Script: Latin - Basic	
<pre> {"System.FileExtension":{"Value": ".exe", "Type": 12}, "System.Software.ProductVersion":{"Value": "N/A", "Type": 12}, "System.Kind":{"Value": " program", "Type": 12}, "System.ParsingName":{"Value": "E7CF176E110C211B", "Type": 12}, "System.Software.TimesUsed":{"Value": 7, "Type": 5}, " System.Tile.Background":{"Value": 4280291898, "Type": 5}, "System.AppUserModel.PackageFullName":{"Value": "N/A", "Type": 12}, "System. Identity":{"Value": "N/A", "Type": 12}, "System.FileName":{"Value": "firefox", "Type": 12}, "System.ConnectedSearch.JumpList":{"Value": "({\ Name\": \"Frequent\", \"Type\": 4, \"Items\": [{\"Type\": 2, \"Name\": \"chor ban on Twitter: \\\"namamu adalah jawaban dari setiap doaku https://t.co/lqZy5hkFC2\\\" / Twitter\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \"Description\": \" chor ban on Twitter: \\\"namamu adalah jawaban dari setiap doaku https://t.co/lqZy5hkFC2\\\" / Twitter\"}, {\"Type\": 2, \"Name\": \"(1) Chor Ban\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \"Description\": \"(1) Chor Ban\"}, {\"Type\": 2, \" Name\": \"Tersang Kha\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \"Description\": \"Tersang Kha\"}, {\" Type\": 2, \"Name\": \"chor ban (@ban_chor) / Twitter\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \" Description\": \"chor ban (@ban_chor) / Twitter\"}, {\"Type\": 2, \"Name\": \"Facebook\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \"Description\": \"Facebook\"}, {\"Type\": 2, \"Name\": \"chor ban on Twitter: \\\"namamu adalah jawaban dari setiap doaku https://t.co/lqZy5hkFC2\\\" / Twitter\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \" Description\": \"chor ban on Twitter: \\\"namamu adalah jawaban dari setiap doaku https://t.co/lqZy5hkFC2\\\" / Twitter\"}, {\"Type\": 2, \"Name\": \"Notifications / Twitter\", \"Path\": \"C:\\\\Program Files (x86)\\\\Mozilla Firefox\\\\firefox.exe\", \"Description\": \" Notifications / Twitter\"}], \"Type\": 3, \"Items\": [{\"Type\": 2, \"Name\": \"Open new tab\", \"Path\": \"C:\\\\Program Files (x86) \\\\Mozilla Firefox\\\\firefox.exe\", \"Description\": \"Open a new browser tab.\"}, {\"Type\": 2, \"Name\": \"Open new window\", \"Path\": \" </pre>							

Gambar 4.35 Status Twitter korban



Gambar 4.36 Metadata Status Twitter korban

4.4 Result

Pada Hasil dari penelitian ini yang berhasil dianalisa hanya 10% ialah berupa data-data yang terkait berkapasitas 10.5GB dengan 44.063 File dalam 2.116 folder. Berikut data yang terkait dalam kasus *cyber crime* dalam barang bukti yang di analisa. Dapat dilihat pada tabel 4.4

Tabel 4.3 Spesifikasi Konektivitas

Kasus terkait	Lokasi	MIME Type	MD5
Username pelaku	/Img_HDD BB.001/vol_vol3/users/user/ap pData/Roaming/Mozilla/Firefo x/Profiles/9com2xxd.default/fo rmhistory.sqlite	Application/x- sqlite3	39269a54a813 5ce97868507e 61160c18a
Konten pornografi	/Img_HDD BB.001/vol_vol3/users/user/ap pData/Roaming/Mozilla/Firefo x/Profiles/9com2xxd.default/ca che2/entries/9E93E570A4AB5	Image/jpeg	899607c02408 d3b8462a72e3 d4792b76

Kasus terkait	Lokasi	MIME Type	MD5
	B43BBABA6F873F878DA0B0A901E		
Ujaran kebencian	/Img_HDD BB.001/vol_vol3/users/user/ap pData/ Mozilla/Firefox/Profiles/9com 2xxd.default/cache2	Image/jpeg	Bb3163d01c24 ed2a8708eed5 46ceaafa
Bullying status	/Img_HDD BB.001/vol_vol3/users/user/ap pData//Local/Packages/Micros oft.Windows.Cortana_cw5n1h 2txyewy/LocalState/DeviceDe archChace/AppChace	Text/plain	8e00a2804924 2106eec93dfcc 27d630a

4.5 Laporan

Pada Laporan Berdasarkan *Chain of Custody* korban melaporkan tersangka dengan kasus tindak kejahatan media sosial facebook dan twitter pada tanggal 19 November 2019 dan kemudian pihak investigator melakukan penangkapan dan mengamankan serta mengumpulkan barang bukti berupa sebuah Laptop Acer Aspire dan juga mengamankan sebuah Flashdisk berkapasitas 4GB yang juga dicurigai dalam kasus ini dikediaman pelaku pada tanggal 22 November 2019. Selanjutnya hasil yang ditemukan ialah pelaku terbukti bersalah atas perbuatan tak terpujinya di dunia maya sejak tanggal 30 Oktober sampai dengan ditangkapnya barang bukti melakukan kejahatan di dunia maya. Untuk itu pelaku terjerat UU no 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) pasal 27 ayat

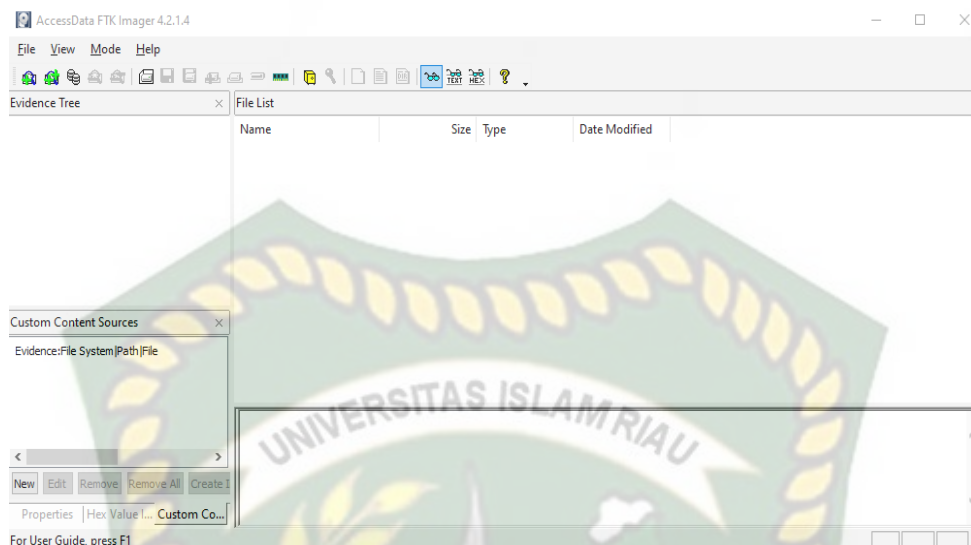
1 tentang konten pornografi, pasal 27 ayat 2 tentang ujaran kebencian, pasal 27 ayat 3 tentang kasus bullying, dan pasal 28 tentang penyebaran Hoax. Dan selanjutnya barang bukti digital pada kasus ini akan diserahkan kepada pengadilan untuk ditindak lanjuti dan bisa dipertanggung jawabkan.

4.6 Perbandingan Sistem Operasi

Pada perbandingan hasil penelitian sistem operasi membandingkan hasil dari proses analisa menggunakan sistem operasi Windows dan sistem operasi Linux dengan media penyimpanan sama yakni sebuah Flashdisk berkapasitas 4 GB yang berisi data 395 MB menjadi barang bukti yang ditemukan.

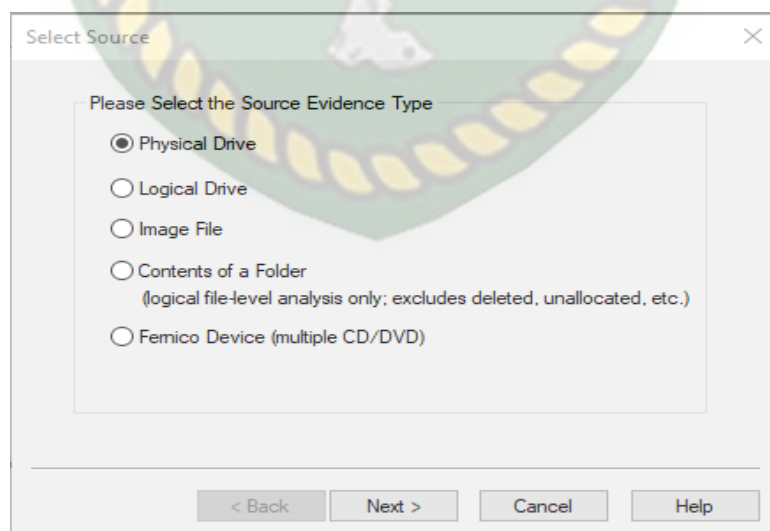
4.6.1 Proses *Imaging* Barang Bukti (Pencitraan) pada Windows

Disaat persiapan akuisisi telah lengkap dan saatnya kita mulai mengakuisisi barang bukti tersebut dengan cara imaging atau pencitraan terhadap barang bukti agar barang bukti tersebut terjaga keasliannya dan bisa dipertanggungjawabkan. Aplikasi yang digunakan yaitu FTK Imager. Tampilan awal seperti pada gambar 4.37 berikut:



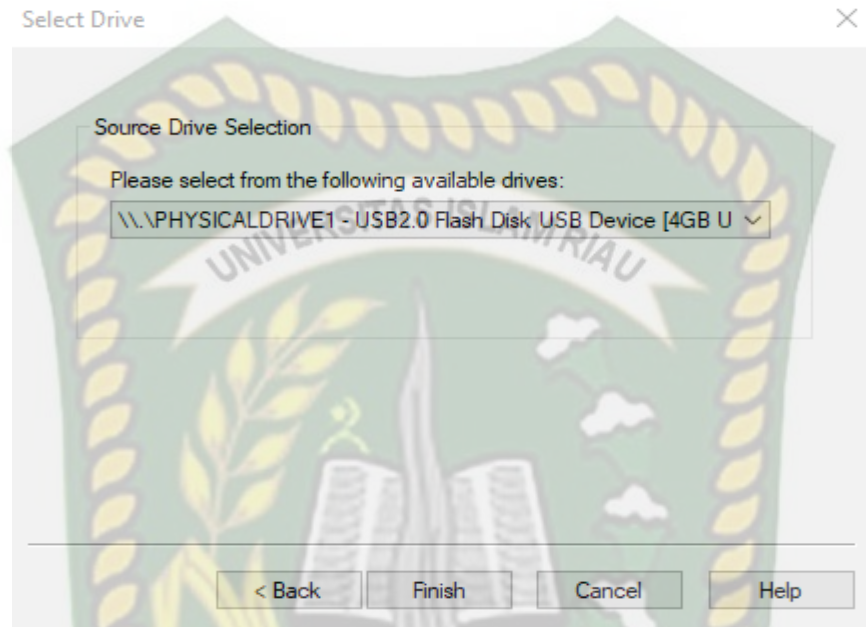
Gambar 4.37 Tampilan Awal Aplikasi FTK Imager

Setelah USB sudah dikoneksikan ke komputer dan sudah terdeteksi maka kita bisa langsung saja memulai proses imaging yaitu 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 Flashdisk seperti pada gambar 4.38 berikut.



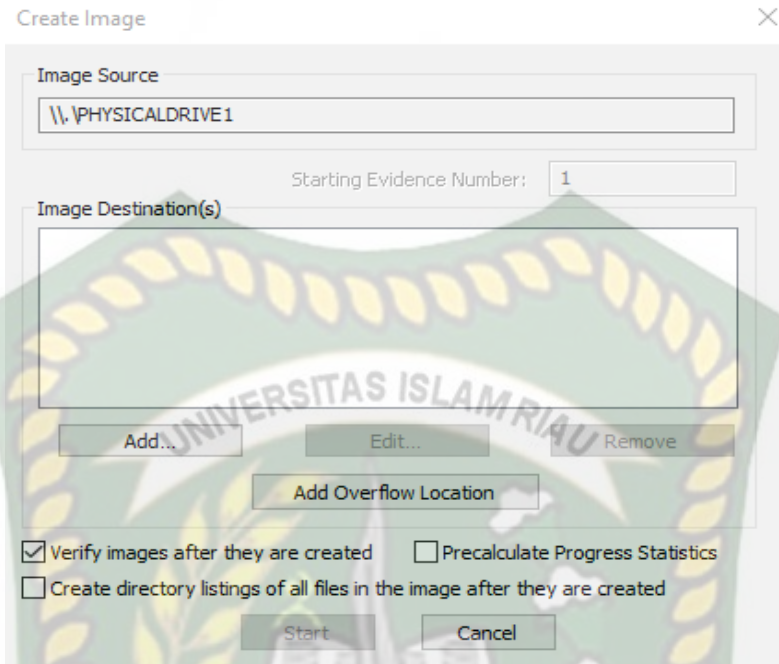
Gambar 4.38 Pilihan tipe barang bukti

Kemudian klik Next, setelah itu pilih PHYSICALDRIVE1 - USB2.0 Flash Disk USB Device seperti pada gambar 4.39 berikut.



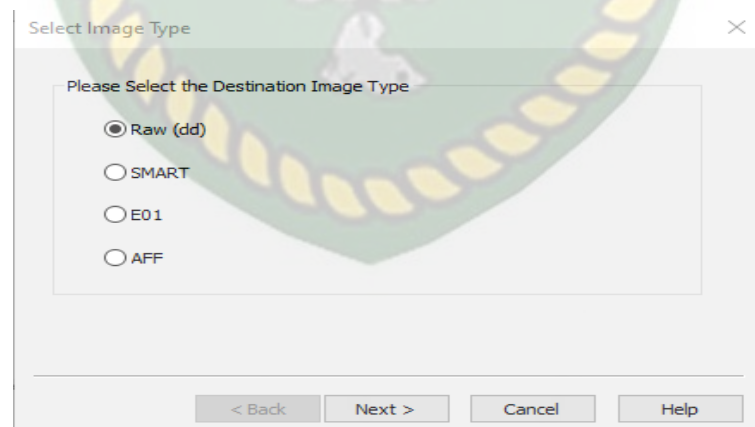
Gambar 4.39 Pilihan Penyimpanan yang akan di imaging

Setelah itu, klik Add untuk memilih lokasi hasil imaging. Dan juga mencontreng pilihan *Verify images after they are created*. Pilihan tersebut berguna untuk menghitung kode hash barang bukti dan hasil imaging kemudian mencocokkan keduanya. Dapat dilihat pada gambar 4.40.



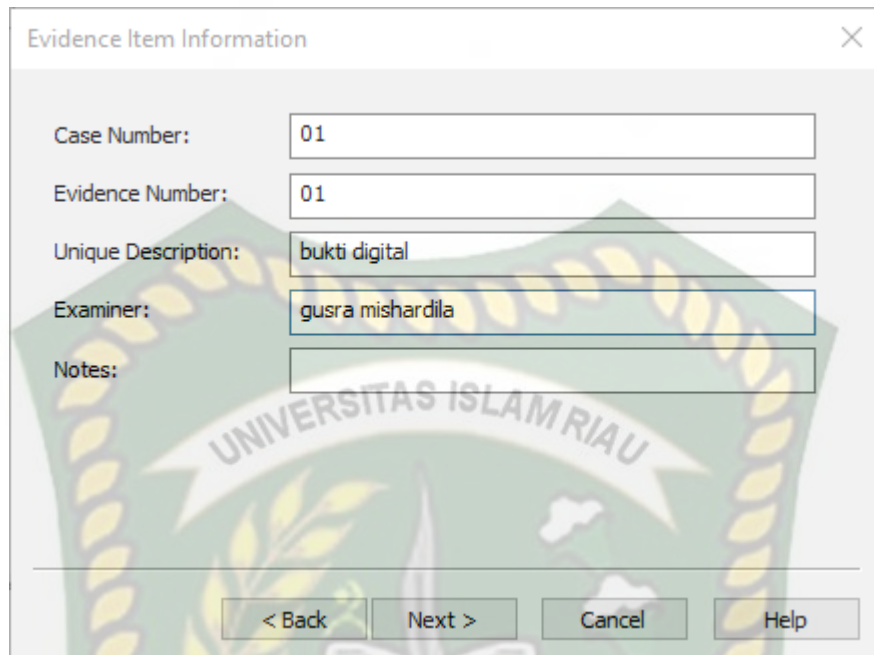
Gambar 4.40 Lokasi penyimpanan Imaging

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 seperti gambar 4.41 berikut.



Gambar 4.41 Pilihan format imaging

Kemudian pilih lokasi folder yang diinginkan dan buat nama file imaging. Lalu klik Next seperti gambar 4.42 berikut.



Evidence Item Information

Case Number: 01

Evidence Number: 01

Unique Description: bukti digital

Examiner: gusra mishardila

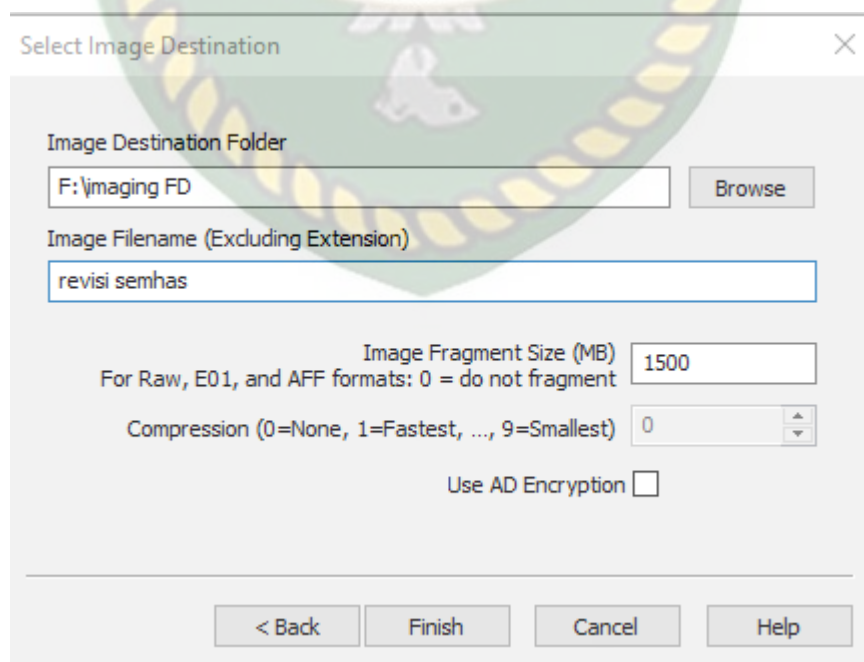
Notes:

< Back Next > Cancel Help

Gambar 4.42 Informasi item batang bukti

Kemudian pilih lokasi folder yang diinginkan dan buat nama file imaging.

Lalu klik finish seperti pada gambar 4.43 berikut.



Select Image Destination

Image Destination Folder: F:\imaging FD Browse

Image Filename (Excluding Extension): revisi semhas

Image Fragment Size (MB): 1500
For Raw, E01, and AFF formats: 0 = do not fragment

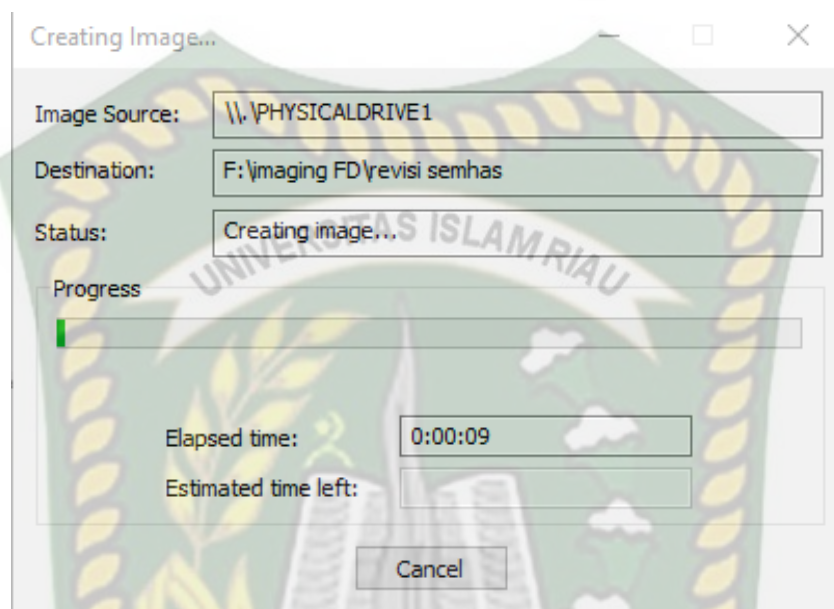
Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption

< Back Finish Cancel Help

Gambar 4.43 Alamat penyimpanan imaging

Langkah terakhir, klik start untuk memulai imaging. Dan gambar 4.44 dibawah ini menunjukkan proses sedang berlangsung.



Gambar 4.44 Proses Imaging sedang berjalan

Setelah proses imaging selesai, FTK akan memberikan laporan informasi dari segala hasil akuisisi lengkap dengan kondisi barang bukti tersebut beserta kode hash MD5 dan SHA1 seperti pada gambar 4.45 berikut.

```

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 509
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 8.192.000
[Physical Drive Information]
Drive Model: USB2.0 Flash Disk USB Device
Drive Serial Number: 2019120517180125
Drive Interface Type: USB
Removable drive: True
Source data size: 4000 MB
Sector count: 8192000
[Computed Hashes]
MD5 checksum: 111dff301f47726942a7e8a37a109171
SHA1 checksum: af80d40d99d12948f68ccc7592ffeb8623dc6ed1

Image Information:
Acquisition started: Sun Apr 19 20:40:08 2020
Acquisition finished: Sun Apr 19 21:02:56 2020
Segment list:
F:\revisi kompre\imagingkompre.001
F:\revisi kompre\imagingkompre.002
F:\revisi kompre\imagingkompre.003

Image Verification Results:
Verification started: Sun Apr 19 21:03:01 2020
Verification finished: Sun Apr 19 21:03:45 2020
MD5 checksum: 111dff301f47726942a7e8a37a109171 : verified
SHA1 checksum: af80d40d99d12948f68ccc7592ffeb8623dc6ed1 : verified

```

Gambar 4.45 Laporan hasil Akuisisi

4.6.2 Proses Analisa pada Windows

Tahap ini adalah untuk menganalisis *file image* yang dihasilkan dengan menggunakan *tools* Autopsy dalam *platform* Windows. Saat membuka aplikasi Autopsy pertama yang dilakukan adalah mengisikan beberapa form yaitu *form case info* untuk penamaan dan tata letak kasus yang dianalisis dan *Additional Information* untuk memberi urutan kasus dan siapa investigator dalam melakukan analisis. Untuk melihat kedua *form* dilihat pada gambar 4.46 dan gambar 4.47.

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: Single-user Multi-user

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

Gambar 4.46 Merupakan case information

New Case Information

Steps

1. Case Information
2. Optional Information

Optional Information

Case Number:

Examiner Name:

Phone:

Email:

Notes:

Organization:

Organization analysis is being done for:

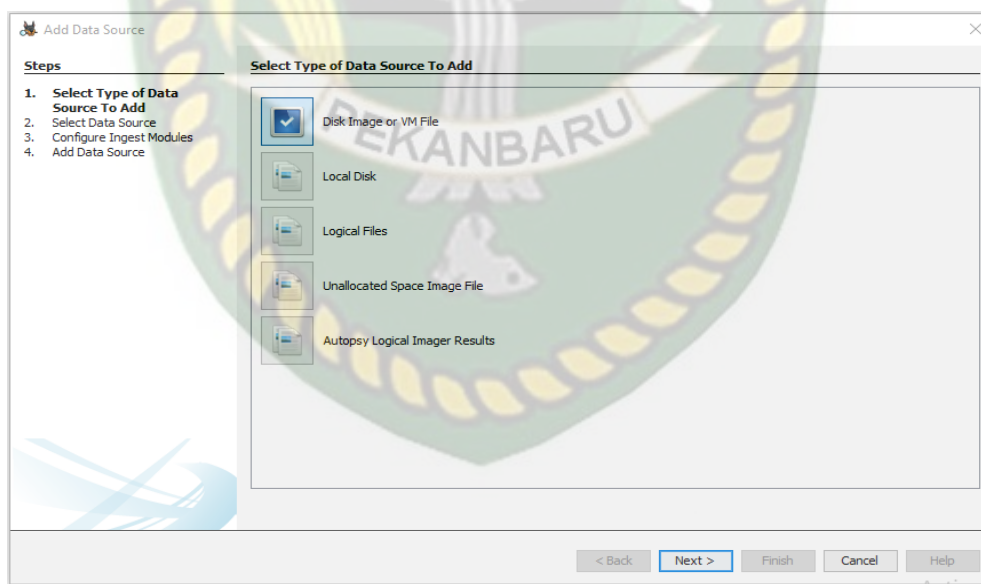
< Back

Gambar 4.47 Form *Additional Information* Aplikasi Autopsy

Pada Gambar 4.46 Merupakan Form *Case Information*. Pada form ini menjelaskan mengenai kasus yang ingin dianalisis dari mengisi nama kasus dan pemilihan letak direktori untuk menyimpan kasus tersebut yang akan menghasilkan sebuah dokumen, sedangkan pada gambar 4.47 Merupakan form *Additional Information* menjelaskan mengenai kasus ke berapa dan siapa nama pengguna aplikasi autopsy yang akan melakukan analisis tersebut. Dari kedua

form tersebut berfungsi untuk mendapatkan rekam analisis yang dapat dipertanggung jawabkan.

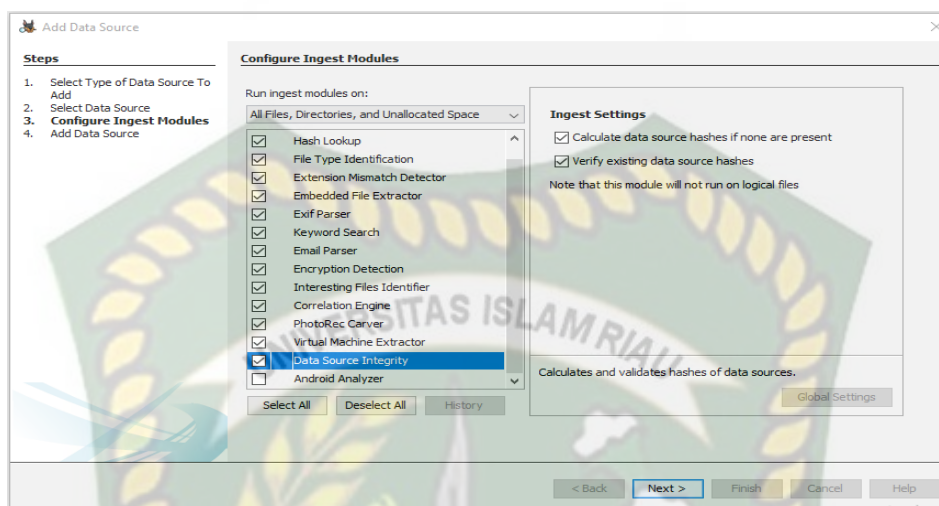
Setelah melakukan pengisian form untuk kepentingan analisis, selanjutnya masuk ke dalam tahap-tahap melakukan proses analisis dari file image yang dihasilkan aplikasi, tahap-tahap tersebut antara lain adalah menentukan data apa yang akan dianalisis yaitu berupa file image, mengambil file image yang ingin dianalisis dari hasil proses akuisisi penyimpanan, menentukan ingest modules 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 4.48.



Gambar 4.48 Form Menentukan tipe yang akan dianalisis


Setelah data sudah dipastikan masuk dan terbaca oleh aplikasi autopsy, maka selanjutnya aplikasi menampilkan *form ingest modules* dan seorang analisis akan mengisi untuk menentukan *form ingest modules* yang dibutuhkan

untuk analisis aplikasi autopsy dan dapat dilihat pada Gambar 4.49.












Gambar 4.49 Form penentuan *ingest modules* Aplikasi Autopsy.

Pada Gambar 4.49 merupakan *form* penentuan untuk memilih *ingest modules* 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 *ingest modules* dalam aplikasi autopsy banyak pilihan yang memiliki fungsi untuk kepentingan analisis agar mudah dilakukan. Setelah penentuan *ingest modules*, maka aplikasi autopsy menjalankan *ingest modules* 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 terbagi beberapa komponen data dari fungsi *ingest modules* yang dijalankan aplikasi autopsy dapat dilihat pada Gambar 4.50.

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
 revisi semhas.001	Image	4194304000	512	Asia/Bangkok	e2ddc8f1-d317-469e-8a53-2f8891648758

Gambar 4.50 Data *Source* dalam Aplikasi Autopsy

Pada Gambar 4.50 merupakan data *source* yang dihasilkan aplikasi autopsy dari *file image* yang telah dimasukkan ke dalam 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 4.51.

Name	S	C	Location	Modified Time	Change Time	Access Time
 IMG_4631.JPG			/img_revisi semhas.001/IMG_4631.JPG	2019-05-03 22:03:30 ICT	0000-00-00 00:00:00	2020-03-19 00:00:00
 LRM_EXPORT_20170225_173135.jpg			/img_revisi semhas.001/LRM_EXPORT_20170225_173135.jpg	2017-02-25 17:31:38 ICT	0000-00-00 00:00:00	2020-03-19 00:00:00
 LRM_EXPORT_20170209_175758.jpg			/img_revisi semhas.001/LRM_EXPORT_20170209_175758.jpg	2017-02-09 17:58:02 ICT	0000-00-00 00:00:00	2020-03-19 00:00:00
 IMG_20161109_013442.jpg			/img_revisi semhas.001/IMG_20161109_013442.jpg	2016-11-09 01:34:44 ICT	0000-00-00 00:00:00	2020-03-19 00:00:00
 f0004784.jpg			/img_revisi semhas.001/CarvedFiles/f0004784.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 f0013008.jpg			/img_revisi semhas.001/CarvedFiles/f0013008.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 thumbnail.jpeg			/img_revisi semhas.001/semproh/hehe.pptx/thumbnail.jpeg	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 image2.png			/img_revisi semhas.001/semproh/BAB 1, 2,3.docx/image2....	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
 image6.png			/img_revisi semhas.001/semproh/BAB 1, 2,3.docx/image6....	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Gambar 4.51 List Barang bukti yang ditemukan

Kemudian tampilan barang bukti yang dihapus pelaku pada aplikasi Autopsy dalam Sistem Operasi windows dapat dilihat tampilannya pada gambar 4.52 berikut serta pada gambar 4.53 metadata dari barang bukti yang dihapus.



Gambar 4.52 Barang bukti yang dihapus pelaku

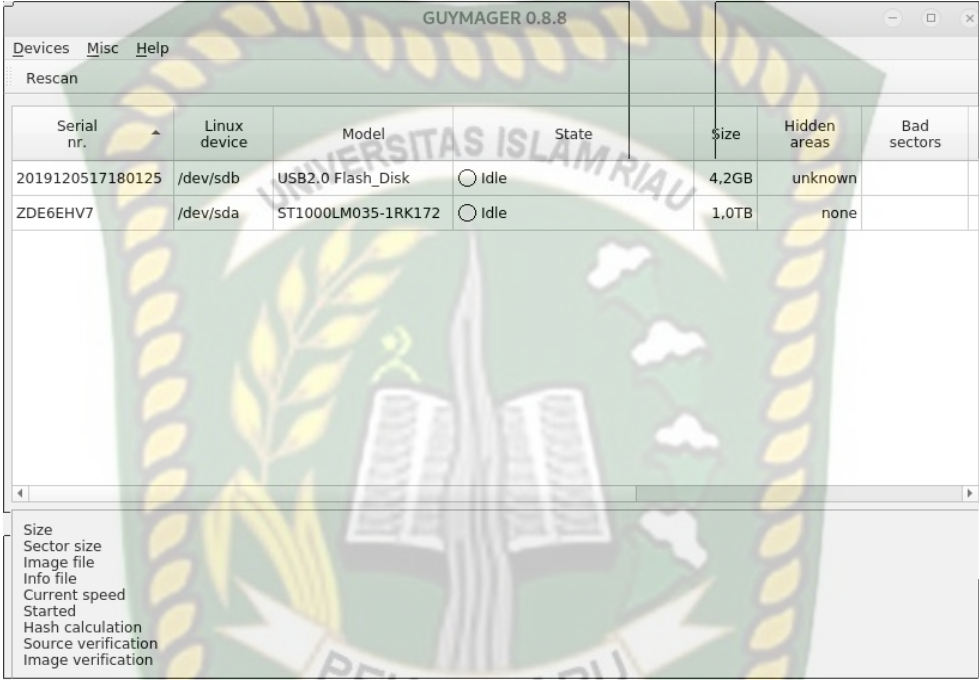
Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Name	/img_revisi semhas.001/LRM_EXPORT_20170209_175758.jpg						
Type	File System						
MIME Type	image/jpeg						
Size	4185351						
File Name Allocation	Unallocated						
Metadata Allocation	Unallocated						
Modified	2017-02-09 17:58:02 ICT						
Accessed	2020-03-19 00:00:00 ICT						
Created	2020-03-19 12:38:39 ICT						
Changed	0000-00-00 00:00:00						
MD5	4f0b392e0e2f3917434ce8718a3ab766						

Gambar 4.53 Metadata Barang bukti yang dihapus pelaku

4.6.3 Proses *Imaging* Barang Bukti (Pencitraan) pada Linux

Guymager ialah aplikasi bawaan dari Linux untuk membantu proses imaging pada perangkat penyimpanan. Aplikasi yang mudah dioperasikan serta open source ini juga menghasilkan data (dd), EWF (E01) dan AFF. Tampilan

pada Aplikasi Guymager berisikan tentang penyimpanan yang terhubung dengan perangkat, beserta status dari penyimpanan tersebut dapat dilihat pada gambar 4.54 dibawah ini.



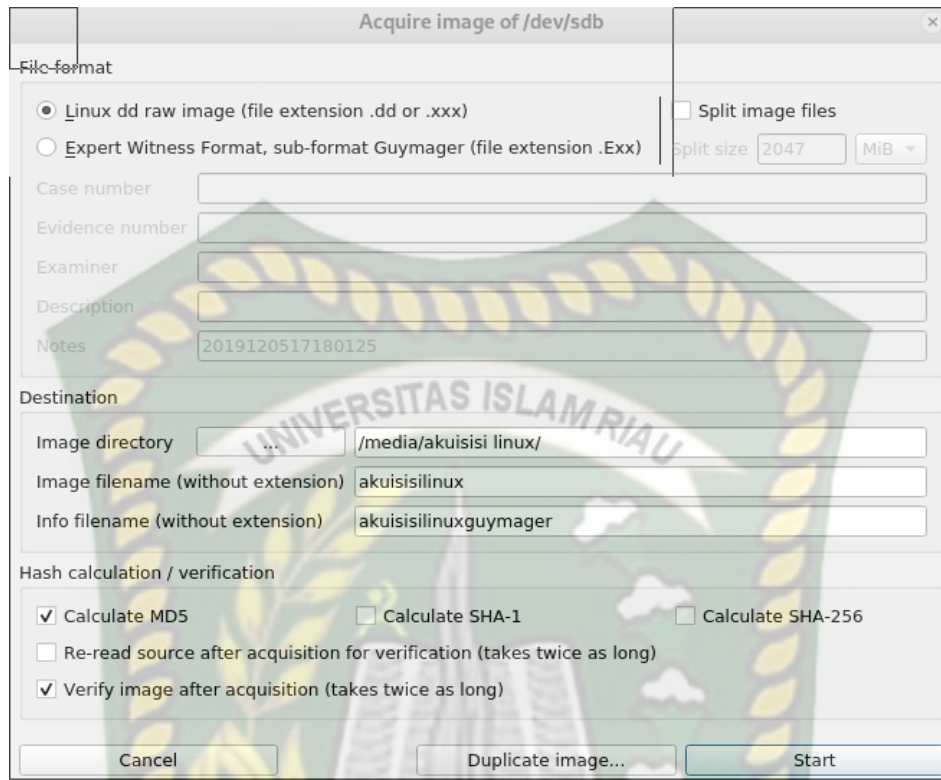
The screenshot shows the GUYMAGER 0.8.8 application window. It has a menu bar with 'Devices', 'Misc', and 'Help'. Below the menu bar is a 'Rescan' button. The main area contains a table with the following data:

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
2019120517180125	/dev/sdb	USB2.0 Flash_Disk	<input type="radio"/> Idle	4,2GB	unknown	
ZDE6EHV7	/dev/sda	ST1000LM035-1RK172	<input type="radio"/> Idle	1,0TB	none	

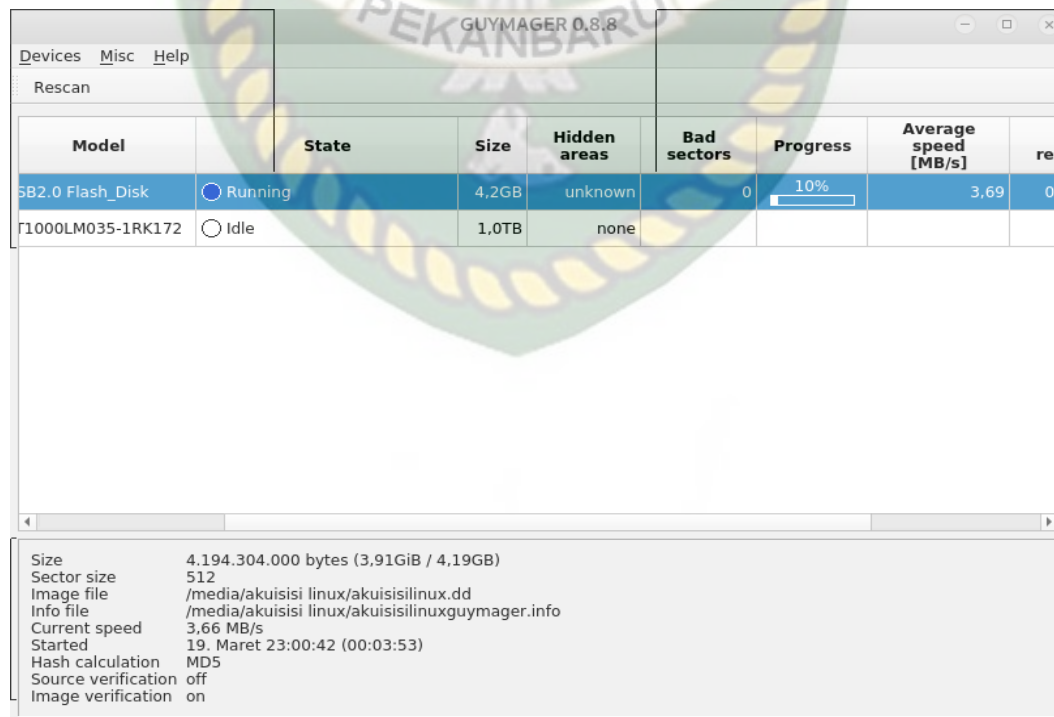
At the bottom of the window, there is a list of options: Size, Sector size, Image file, Info file, Current speed, Started, Hash calculation, Source verification, and Image verification.

Gambar 4.54 Tampilan Awal Aplikasi Guymager.

Kemudian apabila *doubleclick* pada tab kiri maka kita langsung mengakuisi penyimpanan yang akan kita imaging. Serta dihadapkan langsung ke form format imaging serta lokasi penyimpanan dan info dari yang akan kita imaging pada gambar 4.55 serta proses akuisi sedang berjalan pada gambar 4.56.



Gambar 4.55 Format yang akan diakuisisi



Gambar 4.56 Akuisisi barang bukti sedang berjalan

Kemudian setelah berakhir proses imaging aplikasi Guymager menyediakan laporan dari hasil proses imaging detail dari barang bukti yang berhasil diimaging tersebut seperti pada gambar 4.57 berikut ini.

```

Acquisition
-----
Linux device       : /dev/sdb
Device size        : 4194304000 (4,2GB)
Format             : Linux split dd raw image - file extension is .xxx
Image path and file name: /media/New Folder/imagingkompre.xxx
Info path and file name: /media/New Folder/imagingkompre.info
Hash calculation   : MD5 and SHA-1
Source verification : off
Image verification  : on

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash           : e2f59c3ff20d2cd189808bc799a56650
MD5 hash verified source : --
MD5 hash verified image  : e2f59c3ff20d2cd189808bc799a56650
SHA1 hash          : 8511ed56bd10946fbbefed886c6079b99060bc21
SHA1 hash verified source : --
SHA1 hash verified image  : 8511ed56bd10946fbbefed886c6079b99060bc21
SHA256 hash        : --
SHA256 hash verified source : --
SHA256 hash verified image  : --
Image verification OK. The image contains exactly the data that was written.

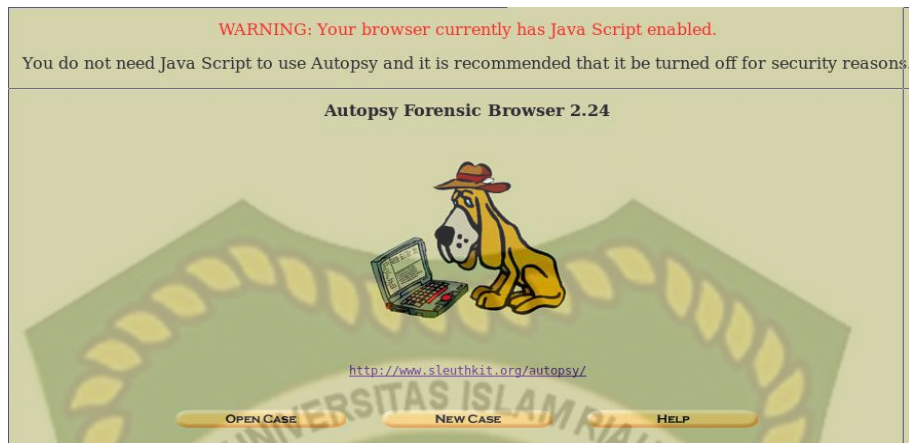
Acquisition started : 2020-04-19 21:14:15 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2020-04-19 21:32:51
Ended               : 2020-04-19 21:34:05 (0 hours, 19 minutes and 50 seconds)
Acquisition speed  : 3.58 MByte/s (0 hours, 18 minutes and 36 seconds)
Verification speed  : 54.05 MByte/s (0 hours, 1 minutes and 14 seconds)

```

Gambar 4.57 Laporan Hasil Akuisisi

4.6.4 Proses Analisa pada Linux

Pada tahap melakukan analisa menggunakan aplikasi Autopsy di Linux segera buka aplikasi Autopsy di desktop kemudian keluar terminal yang mengarahkan link ke browser. Dan berikut pada gambar 4.58 tampilan awal aplikasi Autopsy di Linux.



Gambar 4.58 Tampilan Awal Aplikasi Autopsy pada Linux

Kemudian ketika ingin membuat kasus baru form menyediakan seperti nama kasus, deskripsi kasus dan nama dari investigator yang melakukan analisa. Seperti pada gambar 4.59.

Gambar 4.59 Form membuat kasus baru pada aplikasi Autopsy

Setelah berhasil mengisi form pada pembuatan kasus baru selanjutnya Form Host baru pada aplikasi Autopsy akan muncul seperti pada gambar 4.60 dibawah ini.

ADD A NEW HOST

- Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
- Description:** An optional one-line description or note about this computer.
- Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
- Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

Gambar 4.60 Form penambahan Host

Ketika selesai penambahan Host baru pada gambar 4.61 berisi tentang lokasi penyimpanan data analisa sebelum menambahkan barang bukti yang telah diimaging tadi untuk dianalisa.

```

Adding host: host1gusra to case revisisemhas
Host Directory (/var/lib/autopsy/revisisemhas/host1gusra/) created
Configuration file (/var/lib/autopsy/revisisemhas/host1gusra/host.aut) created
We must now import an image file for this host

  ADD IMAGE

```

Gambar 4.61 Lokasi penyimpanan analisa

Selanjutnya pada gambar 4.62 form penambahan image yang telah diimaging menggunakan aplikasi guymager seperti lokasi dari image yang akan

dianalisa, tipe dari barang bukti yang akan dianalisa dan metode import dari barang bukti dan gambar 4.63 detail kode hash dan selanjutnya pada gambar 4.64 barang bukti selesai diimport.

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/media/akuisisi linux/akuisisilinux.dd

2. Type
Please select if this image file is for a disk or a single partition.

Disk Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink Copy Move

NEXT CANCEL HELP

Gambar 4.62 Form import barang bukti

Image File Details

Local Name: images/revisi.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.

Calculate the hash value for this image.

Add the following MD5 hash value for this image:

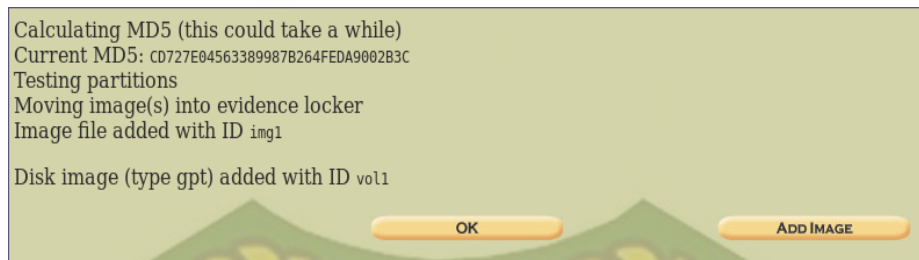
Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

ADD CANCEL HELP

Gambar 4.63 Form detail kode Hash



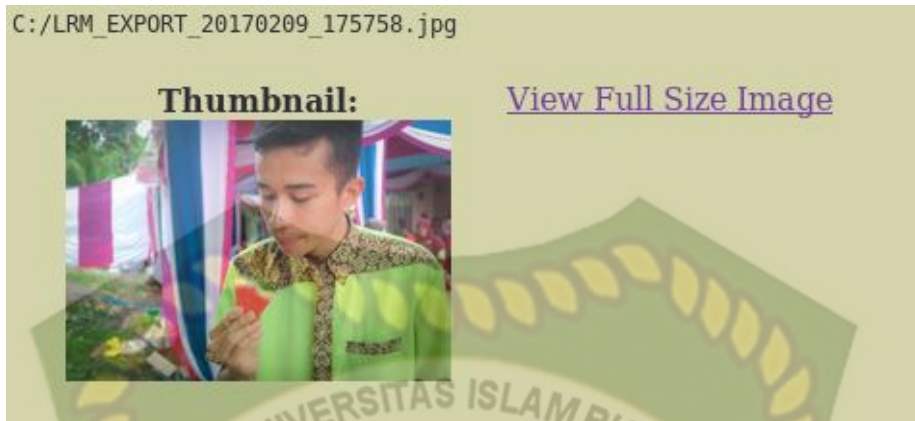
Gambar 4.64 Laporan barang bukti berhasil di import

Pada gambar 4.65 ialah data-data dari barang bukti yang berhasil didapatkan dan siap untuk dianalisa berisi data yang telah dihapus, format pada file, tipe dari file, waktu dan sebagainya.

FILE ANALYSIS	KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP	CLOSE
00:00:00 (UTC)	0000-00-00	00:00:00 (UTC)	0000-00-00	00:00:00 (UTC)	0 0 0	?	X
v / v	\$FAT1		0000-00-00	0000-00-00	0000-00-00		2048000
			00:00:00 (UTC)	00:00:00 (UTC)	00:00:00 (UTC)		
v / v	\$FAT2		0000-00-00	0000-00-00	0000-00-00		2048000
			00:00:00 (UTC)	00:00:00 (UTC)	00:00:00 (UTC)		
v / v	\$MBR		0000-00-00	0000-00-00	0000-00-00		512
			00:00:00 (UTC)	00:00:00 (UTC)	00:00:00 (UTC)		
✓ r / r	IMG_20161109_013442.jpg		2016-11-09	2020-03-19	2020-03-19		90801
			01:34:44 (WIB)	00:00:00 (WIB)	12:43:58 (WIB)		
r / r	IMG_4631.JPG		2019-05-03	2020-03-19	2020-03-19		1997087
			22:03:30 (WIB)	00:00:00 (WIB)	12:42:46 (WIB)		
✓ r / r	LRM_EXPORT_20170209_175758.jpg		2017-02-09	2020-03-19	2020-03-19		4185351
			17:58:02 (WIB)	00:00:00 (WIB)	12:38:39 (WIB)		
r / r	LRM_EXPORT_20170225_175135.jpg		2017-02-25	2020-03-19	2020-03-19		6713419

Gambar 4.65 Barang bukti yang didapatkan

Data yang berhasil didapatkan dari barang bukti yang telah dihapus dapat diangkat kembali dan siap untuk dianalisa seperti pada gambar 4.66.



Gambar 4.66 Format file barang bukti yang akan dianalisa

Dan terakhir berikut gambar 4.67 metadata dan hasil report dari barang bukti yang didapat menjelaskan semua dari sebuah file yang menjadi barang bukti.

```

- Autopsy Hex Report
-----
GENERAL INFORMATION
File: C://LRM_EXPORT_20170209_175758.jpg
MD5 of recovered file: 4f0b392e0e2f3917434ce8718a3ab766 -
SHA-1 of recovered file: 0b59add2da729c0ee0bb184ce942b32603c1fd05
-----
META DATA INFORMATION

Directory Entry: 21
Not Allocated
File Attributes: File, Archive
Size: 4185351
Name: _RM_EX~1.JPG

Directory Entry Times:
Written:      2017-02-09 17:58:02 (WIB)
Accessed:    2020-03-19 00:00:00 (WIB)
Created:     2020-03-19 12:38:39 (WIB)

```

Gambar 4.67 Tampilan Metadata Format file barang bukti

4.6.5 Perbandingan Sistem Operasi

Perbedaan pertama yaitu pada tampilan dari kedua Sistem Operasi ini meski telah sama-sama GUI (*Graphical User Interface*) Aplikasi yang dipakai pada sistem operasi windows tentu saja lebih mudah dipahami dikarenakan telah terbiasanya dengan tampilan tersebut yang berkesan mudah untuk dioperasikan. Selanjutnya pada aplikasi yang digunakan untuk penelitian ini ialah pada aplikasi Autopsy pada Sistem Operasi Kali Linux harus memerlukan koneksi internet untuk menjalankan. Aplikasinya berbeda dengan aplikasi Autopsy pada Windows tetap bisa berjalan meski tidak terhubung ke internet. Namun Linux dari segi waktu lebih efektif dibandingkan sistem operasi Windows dikarenakan sedikit mendahului proses imaging yang dilakukan oleh Guymager dibandingkan FTK Imager. Dan dari segi keamanan sudah pasti sistem operasi *Open Source* ini mengungguli Windows karena menggunakan metode hashing MD5 dan SHA1 sedangkan Autopsy di Windows hanya membaca bilangan hash MD5 saja. Untuk lebih lanjut berikut perbedaan dari kedua Sistem Operasi Windows dan Linux dengan distro Kali pada Tabel 1.1.

Tabel 4.4 Perbandingan Sistem Operasi

NO	PERBEDAAN	WINDOWS	LINUX
1	TAMPILAN	Lebih mudah digunakan, karena tampilan windows lebih dikenal secara umum.	Walaupun pada Sistem Operasi Linux sudah Mendukung <i>Graphical User interface</i> namun masih dianggap susah bagi user untuk

			dioperasikan.
2	JARINGAN	FTK Imager dan Autopsy bisa dijalankan secara <i>Offline</i> .	Pada aplikasi Autopsy harus menggunakan koneksi internet (<i>online</i>).
3	WAKTU	<p>Mulai Akuisisi: 19-04-2020 20:40:08</p> <p>Akuisisi selesai: 19-04-2020 21:02:56 (23 menit 4 detik)</p> <p>Mulai verifikasi: 19-04-2020 21:03:01</p> <p>Verifikasi selesai: 19-04-2020 21:03:45(44 detik)</p> <p>Total: 23 menit 48 detik.</p>	<p>Mulai akuisisi: 19-04-2020 21:14:15</p> <p>Mulai verifikasi: 19-04-2020 21:32:51</p> <p>Kecepatan akuisisi: 3.58 MB/s (18 menit 36 detik)</p> <p>Kecepatan verifikasi: 54.05 MB/s (1 menit 14 detik)</p> <p>Total: 19-04-2020 21:35:05 (19 menit 50 detik).</p>
4	KEAMANAN	Pada aplikasi Autopsy metadata hanya menampilkan kode hash MD5 saja.	Guymager dan Autopsy menampilkan kode hash MD5 dan SHA1.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian dan pembahasan tugas akhir mengenai analisa dan pencarian bukti forensik digital pada aplikasi media sosial facebook dan twitter menggunakan metode statik forensik dapat disimpulkan bahwa:

1. Dalam metode Statik Forensik ini perlunya pengumpulan semua data-data yang akan dianalisa baik dalam bentuk fisik maupun tidak 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 artefak barang bukti secara terperinci meski proses tidak sempurna 100% validasi.
4. Dalam segi keunggulan dalam menganalisa Sistem Operasi Linux lebih mengguli Sistem Operasi Windows.

5.2 Saran

Untuk Pengembangan lebih lanjut dibutuhkan spesifikasi alat investigator yang memadai agar bisa melakukan analisa barang bukti keseluruhan 100%. Serta juga bisa dilakukan penelitian dengan perangkat mobile nantinya.

DAFTAR PUSTAKA

- Agarwal, A., Gupta, M., & Gupta, S.(2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118-134.
- Anton Yudhana, 2017, *Facebook Messenger menjadi media sosial yang populer kedua setelah Whatsapp*, *IT Journal research and Development*, Vol.3
- Casey, Eoghan, 2014, *Digital Evidence and Computer Crime*, United States of America:Academica.
- Dedy, Faulinda, 2014, *Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO, iec 27037:2014*
- Firmansyah Gustav Hikmatyar, 2017, *Analisis Forensika Digital pada Smartphone Android untuk Penangan Kasus Cybercrime*, Skripsi, UIN Sunan Kalijaga, Yogyakarta
- Marcella, Albert J., Jr. Doug Manendez, 2007, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, United States of America:CRC Press LLC
- Ranny Rastati, 2016, *Bentuk Perundungan Siber di Media Sosial dan Pencegahannya bagi korban dan Pelaku*, *Jurnal Sositologi*,Vol.15
- Rizdqi, Desti, 2014, *Acquisition and Analysis on CCTV Digital Evidence Using Static Forensic Method based on SNI ISO,IEC 27037*
- Rizdqi,Yudi, 2017, *Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive*, *Jurnal Teknomatika*, Vol.9
- Ruci Meiyanti, 2015, *Perkembangan Digital Forensik saat ini dan Masa mendatang,*, *Jurnal Ilmu Pengetahuan dan Teknologi Terapan*, Vol.7