BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian mengenai implementasi *dead forensic* yang telah dilakukan oleh peneliti terdahulu. Penelitian yang dilakukan menghasilkan berbagai hasil yang berbeda-beda pastinya. Berikut merupakan beberapa penelitian terhadulu :

1. **Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode *National Institute Of Justice* (NIJ)., Imam Riadi, Rusydi Umar, Imam Mahfudl Nasrulloh, Jurnal ELINVO 2018.**

   Penelitian ini bertujuan untuk implementasi salah satu *software* pembeku *drive* yaitu *Shadow Defender* yang dapat membeukan suatu Drive (frozen solid state driver) terbukti berpengaruh terhadap analisa forensik yang didapatkannya bukti-bukti digital. Tidak semua *file* dapat di restorasi karena struktur *file* dan data sudah rusak, dan juga catatn pengguna komputer (*recent activity*) dan sejarah *internet* (*history internet*) tercatat ketika fitur pembeku drive diaktifkan. Nilai 28,7% dari total keberhasilannya yaitu dari sebanyak 85 *file* yang disiapkan untuk implementasi dan pengujian dan hasil *file* yang berhasil direstorasi hanya sebanyak 25 *file* saja. Sehingga dapat menyebabkan hambatan dalam proses forensik digital yang dilakukan oleh penyidik dan hasil dari penyidikan masih sangat sedikit informasi yang didapatkan dari barang bukti digital. Dalam penelitian ini menggunakan metode *National Institute Of Justice* dengan alur nya yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*.

   Hasil analisis yang telah dilakukan didapatkan data-data proses akuisisi menggunakan *tool software* OSForensics, Autopsy, dan Winhex yang berguna untuk menemukan bukti digital. Dengan bukti digital yang diharapkan ditemukan adalah *file* dokumen seperti *.doc*, *.xls*, *.ppt*, *.pdf*, *file* gambar seperti *.jpg*, *.png*, *file* aplikasi seperti *.exe*, *file* multimedia

seperti *.mp3*, *.mp4*, *history internet* dan catatan terbaru penggunaan komputer.[5]

Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan sosial media *instagram*, *facebook*, *twitter*, *whatsapp*, *pinterest*, *linkedin* dengan menggunakan metode *National Institute Standards and Tecnology* untuk proses mendapatkan hasil bukti digital.

2. Analisis *Live Forensic* Untuk Perbandingan Keamanan *E-mail* Pada Sistem Operasi *Proprietary*., Muhammad Nur Faiz, Rusydi Umar, Anton Yudhana, Jurnal ILKOM 2016.

Penelitian ini bertujuan dengan menggunakan Sistem Operasi yang telah banyak sekali digunakan perusahaan atau diseluruh dunia. Email merupakan hal pendukung kinerja suatu perusahaan atau penggunanya dalam segala bidang termasuk untuk bisnis dan bertukar informasi.Gmail merupakan E-mail terbaik saat ini dengan dukungan keamanan yang tinggi pada *mode browser private*. Hasil eksperimen yang dilakukan dengan menggunakan PC Sistem Operasi Windows 10 64bit, *Browser* Mozilla Firefeox 49.0.1, MicrosoftEdge 20.10240.17146.0, Google Chrome 54.0.2840.59, capture dan analisis pada FTK Imager 3.4.2.6. Penelitian ini juga membuat akun email latihancoba1@gmail.com login pada Google Chrome, latihancoba1@yahoo.com login pada Mozilla Firefox , latihancoba1@live.com login pada Microsoft Edge.[6] Dalam penelitian ini menggunakan metode *National Institute Of Justice* (NIJ) dengan alur nya yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*.

Hasil analisis yang telah dilakukan didapatkan data-data proses akuisisi menggunakan *Personal Computer* Sistem Operasi Windows 10 64bit dan *tool* yang digunakan FTK Imager. Dengan menggunakan *browser* Microsoft Edge dengan *type public* pada *Outlook* terlihat dengan jelas *username* dan *password* yaitu dengan *username* latihancoba1@live.com dan *password* mtiuad2016.

Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian

menggunakan dua *tools* yang pertama Autopsy dan FTK Imager dan juga berbeda analisis dalam penelitian milik penulis menganalisis *dead forensic* sedangkan penelitian ini menggunakan *live forensics*.

3. **Analisis Bukti Digital Pada Flash Disk Drive Menggunakan *Generic Computer Forensic Investigation Model* (GCFIM)., Muh. Hajar Akbar, Sunardi, Imam Riadi, Jurnal Seminar Nasional Teknologi Fakultas Teknik Universitas Krinadwipayana 2019.**

   Penelitian ini untuk menganalisis barang bukti digital menggunakan metode forensik. Pada Proses cloning menjadi langkah awal yang penting pada saat akan melakukan analisis pada barang bukti digital. Teknik hash MD5 dapat digunakan untuk menjaga integritas barang bukti digital sehingga dapat dipastikan barang bukti hasil cloning identik dengan yang asli. Tools Winhex sangat membantu dalam penelitian ini terutama pada proses cloning maupun hashing *file*, tools Autopsy digunakan untuk menganalisis *file cloning* serta dapat memberikan informasi mengenai hex, *strings*, *file metadata*, *results*, maupun *indexted text*. Pada penelitian ini akan dilakukan analisis pada barang bukti berupa satu buah flashdisk yang dicurigai terdapat bukti kejahatan.[7] Dalam penelitian ini menggunakan metode *Generic Computer Forensic Investigation Model* (GCFIM) dengan alur nya yaitu *Pre-Process*, *Acquisition & Preservation*, *Analysis*, *Presentation*, dan *Post-Process*.

   Hasil Analisis yang telah dilakukan didapatkan data-data akuisisi menggunakan WinHex dengan kebutuhan proses *cloning* yang dijalankan. Dengan media penyimpanan yang digunakan adalah *flashdisk*. Dengan *flashdisk* tersebut berisikan berupa barang bukti digital Setelah proses *identification* telah selesai lanjut memulai dengan Analisis menggunakan autopsy.

   Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan media penyimpanan nya berupa *harddisk*. *Harddisk* yang sebagai media penyimpanan tersebut akan di *cloning* dan di analisa menggunakan kedua *tools* yaitu Autopsy dan FTK Imager. *Framework*

yang digunakan yaitu *National Intitute Standards Of Technology*.

4. **Implementasi Live Forensics Untuk Perbandingan *Browser* Pada Keamanan E-mail., Muhammad Nur Faiz, Rusydi Umar, Anton Yudhana, JISKa 2017.**

   Browser merupakan salah satu aplikasi yang berguna untuk menerjemahkan *Hypertext Markup Language* (HTML) menjadi bahasa yang dapat dipahami oleh user. Keamanan pada *browser* merupakan suatu tantangan tersendiri untuk mengembangkan *browser* default dari windows 10 dengan berbagai fitur kemanan dan kemudahan dalam menggunakan *browser*. Microsoft Edge merupakan *browser* default dari Windows 10 dengan beberapa fitur lebih baik dari Internet Explorer akan tetapi untuk keamanan lebih lama jika dibandingkan oleh *browser* Mozilla firefox, dan juga Google chrome lebih kuat akan passwordnya. Hasil eksperimen yang telah dilakukan dengan menggunakan Personal *Computer* Sistem Operasi nya ialah windows 10 64 bit. Dengan versi *browser* Mozilla Firefox 49.0.1, Microsoft Edge 20.10240.17146.0, Google chrome 54.0.2840.59, dengan capture dan analisis pada *software* FTK Imager 3.4.2.6. Penelitian ini juga terlebih dahulu membuat akun email latihancoba1@gmail.com yang login pada Google chrome.[8] Dalam penelitian ini menggunakan metode *National Institute Of Justice* (NIJ) dengan alur nya yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*.

   Hasil Analisis yang telah dilakukan didapatkan data-data berupa *e-mail* dan *password*. *E-mail* yang didapatkan yaitu latihancoba1@gmail.com dan *password* nya yaitu mtiuad2016 dengan menggunakan *tool* FTK Imager. Dengan kebutuhan analisa nya menggunakan *Personal Computer* Sistem Operasi Windows 64 bit.

   Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan kedua *tools* yaitu FTK Imager dan Autopsy. Dengan media sosial *facebook*, *twitter*, *instagram*, *pinterest*, *whatsapp*, dan *linkedin*. Dengan teknik analisa menggunakan *dead forensic*.

5. **Rancangan Investigasi Forensik Email Dengan Menggunakan Metode Nasional Institute Of Standards And Technology (*NIST*)., Mustafa, Imam Riadi, Rusydi Umar SNST 2018.**

Penelitian ini ialah menggunakan metode *National Institut Of Standards And Technology* (NIST) dengan pendekatan kepada Header Analisis yang telah menghasilkan pola pemalsuan email yang menggunakan subjek, tanggal email yang palsu juga. Selain dari itu juga investigasi email forensic ini juga menghasilkan 1 alamat email pengirim, email palsu 2 yang memeriksa protocol inisiasi pesan berupa Http, smtp, memeriksa Id pesan sebanyak 4 dan juga alamat IP pengirim. Metode ini juga telah digunakan pada tahapan analisis email palsu, dengan tahapan sebagai berikut Header analisis, dimana pada seiap bagian header email memuat field-field seperti from, subject, date, received. Selanjutnya di scenario dalam pembuatan email palsu yang baru, dilakukan dengan cara memanipulasi field pada header email dan berupa pesan yang sangat meyakinkan bahwa emailnya merupakan yang asli dan juga sah. Pada saat sama juga dikirimkan email yang sah dan asli dari akun yang benar. Pada tahapan teakhir dilakukan juga pelaporan atau juga biasa disebut reporting yaitu hasil analisis yang berupa barang bukti yang valid atau sah berupa konten dari email itu. Pada pelaporan juga akan dijelaskan proses yang telah digunakan dalam mendapatkan barang bukti.[2] Dalam penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) dengan alur nya yaitu *collection*, *examination*, *analysis*, dan *reporting*.

Hasil Analisis yang telah dilakukan didapatkan data-data dengan pendekatan *header analysis* menghasilkan pemalsuan berupa email dengan subjek, alamat, dan tanggal email yang palsu dan aspek lain yaitu format penyimpanan alamat email ketersediaan beberapa email untuk proses menganalisis email.[2]

Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan kedua *tools* yaitu Autopsy dan FTK Imager yang berguna

untuk proses analisis nanti nya. Dengan metode yang digunakan *National Institute Of Standards and Technology*. Sosial media yang digunakan yaitu *facebook, twitter, instagram, linkedin, whatsapp,* dan *pinterest*.

6. **Perancangan Perbandingan Live Forensic Pada keamanan Media Sosial Instagram, Facebook dan Twitter di Windows 10., Rauhulloh Ayatulloh Khomeini Noor Bintang, Rusydi Umar, Anton Yudhana, SNST 2018.**

   Penelitian ini ialah melakukan berupa *forensic* media sosial pada laptop ataupun komputer yang memerlukan sebuah metode dan tools yang akan membantu peneliti untuk mencari atau mendapatkan data yang akan di investigasi forensik nantinya. Dengan diawali membuat akun sosmed *facebook, Instagram,* dan juga *twitter*. Dengan pemilihan tools yang akan digunakan untuk mengambil data pada akun media sosial, dengan tools yang dinamakan FTK Imager sebagai pengelola pada data yang akan di analisis. Selanjutnya pada saat pembuatan akun media sosial tersebut, dilakukan dengan cloning data dan hashing data fungsi nya yaitu meyakinkan akun media sosial tersebut menjadi nilai yang merepresentasikan string asli ataupun akun asli. Dengan tahapan terakhir dilakukan laporan hasil penelitian mengenai data pada medsos berupa barang butki data yang sah pada media sosial tersebut, dalam pelaporan nya juga menjelaskan tahapan-tahapan atau proses yang digunakan untuk memperoleh barang bukti yang akan dibutuhkan supaya data tersebut asli.[9] Dalam penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) dengan alur nya yaitu *collection, examination, analysis,* dan *reporting*.

   Hasil Analisis yang telah dilakukan didapatkan data-data dari media sosial seperti *facebook, twitter, instagram*. Memanfaatkan *tool* FTK Imager dengan kegunaan nya untuk proses analisis dan mengetahui keamanan dari masing-masing media sosial tersebut nanti nya.

   Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan *tools* FTK Imager dan Autopsy dengan sosial media

facebook, *twitter*, *instagram*, *pinterest*, *linkedin*, *whatsapp*. Dan untuk metode yang digunakan *National Institue Of Standards and Technology*(NIST).

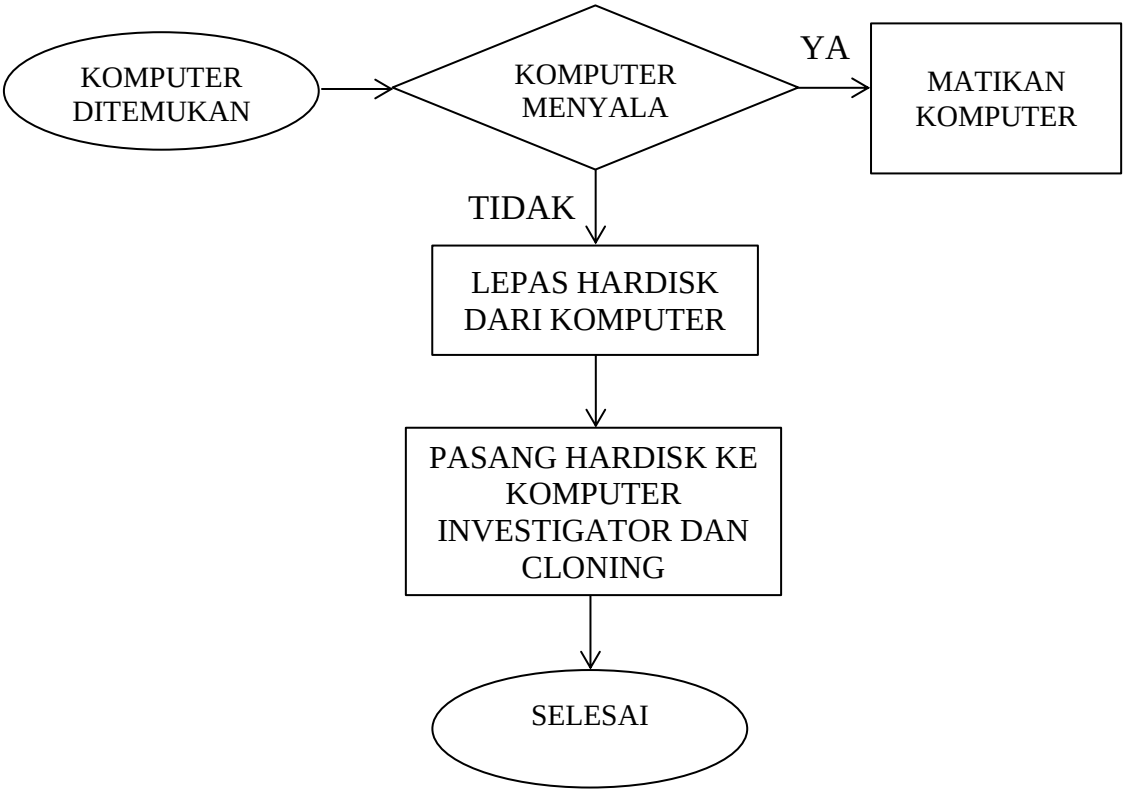
Tabel 2. 1 Penlitian Terdahulu

Judul Penelitian	Nama Peneliti Terdahulu	Tahun	Inti Pembahasan	Metode	Tool	Perbedaan dengan penelitian yang dilakukan
Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ)	Imam Riadi, Rusydi Umar, Imam Mahfudl Nasrulloh.	2018.	Hasil analisis yang telah dilakukan didapatkan data-data proses akuisisi menggunakan *tool software* OSForensics, Autopsy, dan Winhex yang berguna untuk menemukan bukti digital. Dengan bukti digital yang diharapkan ditemukan adalah *file* dokumen seperti .doc, .xls, .ppt, .pdf, *file* gambar seperti .jpg, .png, *file* aplikasi seperti .exe, *file* multimedia seperti .mp3, .mp4, *history internet* dan catatan terbaru penggunaan komputer	National Institute Of Justice (NIJ).	OSForensics, Autopsy dan WinHex.	Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan sosial media instagram, facebook, twitter, whatsapp, pinterest, linkedin dengan menggunakan metode National Institute Standards and Tecnology untuk proses mendapatkan hasil bukti digital
Analisis Live Forensic Untuk Perbandingan Keamanan E-mail Pada Sistem Operasi Proprietary.	Muhammad Nur Faiz, Rusydi Umar, Anton Yudhana.	2016	Hasil analisis yang telah dilakukan didapatkan data-data proses akuisisi menggunakan *Personal Computer* Sistem Operasi Windows 10 64bit dan *tool* yang digunakan FTK Imager. Dengan menggunakan *browser* Microsoft Edge dengan *type public* pada *Outlook* terlihat dengan jelas *username* dan *password* yaitu dengan *username* latihancoba1@live.com dan *password* mtiuad2016	National Institute Of Justice (NIJ).	FTK Imager	Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan dua tools yang pertama Autopsy dan FTK Imager dan juga berbeda analisis dalam penelitian milik penulis menganalisis dead forensic sedangkan penelitian ini menggunakan live forensics.
Analisis Bukti Digital Pada Flash Disk Drive Menggunakan Generic Computer Forensic Investigation Model (GCFIM).	Muh. Hajar Akbar, Sunardi, Imam Riadi	2019	Hasil Analisis yang telah dilakukan didapatkan data-data akuisisi menggunakan WinHex dengan kebutuhan proses *cloning* yang dijalankan. Dengan media penyimpanan yang digunakan adalah *flashdisk*. Dengan *flashdisk* tersebut berisikan berupa barang bukti digital Setelah proses *identification* telah selesai lanjut memulai dengan Analisis menggunakan autopsy	Generic Computer Forensic Investigation Model (GCFIM).	WinHex dan Autopsy	Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan media penyimpanan nya berupa harddisk. Harddisk yang sebagai media penyimpanan tersebut akan di cloning dan di analisa menggunakan kedua tools yaitu Autopsy dan FTK Imager. Framework yang digunakan yaitu National Intitute Of Standards and Technology.
Implementasi Live Forensics Untuk Perbandingan Browser Pada Keamanan E-mail.	Muhammad Nur Faiz, Rusydi Umar, Anton Yudhana.	2017	Hasil Analisis yang telah dilakukan didapatkan data-data berupa *e-mail* dan *password*. *E-mail* yang didapatkan yaitu latihancoba1@gmail.com dan *password* nya yaitu mtiuad2016 dengan menggunakan *tool* FTK Imager. Dengan kebutuhan analisa nya menggunakan *Personal Computer* Sistem Operasi Windows 64 bit.	*National Institute Of Justice* (NIJ).	FTK Imager	Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan kedua tools yaitu FTK Imager dan Autopsy. Dengan media sosial *facebook, twitter, instagram, pinterest, whatsapp*, dan *linkedin*. Dengan teknik analisa menggunakan *dead forensic.*
Rancangan Investigasi Forensik Email Dengan Menggunakan Metode *Nasional Institute Of Standards And Technology* (NIST).	Mustafa, Imam Riadi, Rusydi Umar.	2018.	Hasil Analisis yang telah dilakukan didapatkan data-data dengan pendekatan *header analysis* menghasilkan pemalsuan berupa email dengan subjek, alamat, dan tanggal email yang palsu dan aspek lain yaitu format penyimpanan alamat email ketersediaan beberapa email untuk proses menganalisis email.	*National Institute Of Standards and Technology* (NIST).	Aid4Mail *Forensic*	Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan kedua tools yaitu Autopsy dan FTK Imager yang berguna untuk proses analisis nanti nya. Dengan metode yang digunakan *National Institute Standards Of Technology*. Sosial media yang digunakan yaitu *facebook, twitter, instagram, linkedin, whatsapp,* dan *pinterest*.
Perancangan Perbandingan Live Forensic Pada keamanan Media Sosial Instagram, Facebook dan Twitter di Windows 10.	Rauhulloh Ayatulloh Khomeini Noor Bintang, Rusydi Umar Anton Yudhana.	2018	Hasil Analisis yang telah dilakukan didapatkan data-data dari media sosial seperti facebook, twitter, instagram. Memanfaatkan tool FTK Imager dengan kegunaan nya untuk proses analisis dan mengetahui keamanan dari masing-masing media sosial tersebut nanti nya.	*National Institute Of Justice* (NIJ).	FTK Imager, Media sosial (*facebook, instagram, twitter)*.	Perbedaan penelitian ini dengan milik penulis yaitu dalam penelitian menggunakan tools FTK Imager dan Autopsy dengan sosial media *facebook, twitter, instagram, pinterest, linkedin, whatsapp*. Dan untuk metode yang digunakan *National Institue Of Standards and Technology*(NIST).

2.2. Dasar Teori

2.2.1. *Dead Forensic(*DF)

Dead forensik adalah suatu teknik yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan umumnya ialah harddisk. Bagian yang wajib pada digital forensik ialah keaslian dari barang bukti digital. Melakukan investigasi melalui tahapan pendekatan prosedur pemeriksaan digital forensik, digital forensik sendiri ialah cara yang valid untuk mendapatkan pembuktian. *Internet forensic* adalah suatu penulusuran dan investigasi dari kejahatan dari *internet* dan juga dapat dipelajari hal-hal yang didalamnya. Digital forensik analisis pada umumnya terdapat dua metode, ialah dead forensik dan juga *live* forensik. [7]



Sumber : [10]

Gambar 2. 1 Alur *Dead Forensic*

Metode dead forensic bertujuan untuk penanganan barang bukti digital, dimana penyimpanan barang bukti digital tidak sedang menjalankan *system* atau dalam keadaan komputer sedang mati. Teknik dead forensik ialah dengan cara proses investigasi yang dilakukan untuk mencari barang bukti digital dari sebuah barang elektronik yang sudah mati atau tidak sedang dialiri listrik. Barang bukti tersebut ialah berupa harddisk, hal ini bisa dianalisa dengan harddisk yang terdapat penyimpanan dari aktifitas pengguna[6]

Dead forensik ini ialah bukti digital yang tersimpan pada penyimpanan komputer sementara, penyimpanan permanen, CD, Flashdrive. Digital forensik kemudian berkembang menjadi sesuatu yang penting dalam keamanan informasi. Dalam keterlibatan suatu perangkat atau media dalam kejahatan komputer dibedakan menjadi tiga yaitu :

-Komputer sebagai tujuan.

-Komputer menjadi wadah kejahatan.

-Komputer sebagai penyimpanan segala informasi yang mengandung tindak pidana.[7]

Dengan implementasi dead forensik dilakukan pada saat data sudah tersimpan pada harddisk, dikarenakan penyimpanan diperoleh barang bukti. Barang bukti yang telah didapatkan akan dikembangkan (explore dan exploit) kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan akan didapatkan hasil analisis. Pengambilan bukti digital mengacu pada metode static forensic atau disebut juga metode akuisisi secara tradisional, hal ini berfokus pada memeriksa salinan duplikat.[2]

Dengan menjalankan analisis data pada Harddisk diperangkat laptop berbasis *system* operasi *linux* dan *windows* dengan metode *dead* forensik yang merupakan bagian dari komputer forensik, dengan begitu peneliti berpedoman dengan *framework* NIST 800-86 dengan hal ini untuk penanganan barang bukti yang tersimpan di harddisk adalah sebagai berikut :[1]

Gambar 2. 1 Tahapan *National Institute Of Standards and Technology* (NIST)

1. Collection adalah pelabelan, identifikasi, rekaman, dan pengambilan data dari sumber data yang relevan dengan prosedur yang tepat agar tidak mengubah keaslian data dan untuk menjaga integritas data.[7]
2. Examination adalah pengolahan data yang dikumpulkan, pada tahap ini adalah bagaimana penggunaan forensik kombinasi dari berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sesuai kebutuhan penelitian sambil mempertahankan integritas data.[7]
3. Analysis adalah tahapan dari pemeriksaan hasil dengan menggunakan metode teknis yang dibenarkan sesuai prosedur dan hukum.[7]
4. Reporting adalah melaporkan hasil analisis yang meliputi persiapan, pengujian, penggambaran tindakan yang dilakukan, serta hasil yang diperoleh dari penelitian.[7]

Pengertian Digital forensik adalah cabang dari forensik yang berhubungan dengan pemulihan, investigasi dan analisis bukti yang ditemukan di perangkat digital yang dapat disajikan dalam pengadilan

hukum. Saat melakukan penyelidikan harus mengikuti prosedur yang tepat dan protokol dan juga mendokumentasikan dari setiap tahapan saat mencari bukti digital.[10]

Ungkapan forensik digital dan komputer forensik keduanya sering digunakan secara bergantian yang berarti ilmu memperoleh, mengambil, melestarikan, dan penyajian data yang telah diproses secara elektronik dan disimpan di media computer. Sebagaimana yang disampaikan dalam penelitiannya oleh Lowman & Ferguson yang berjudul Web History *Visualisation for ForensicInvestigations*.[11]

2.2.2. Bukti Digital

Bukti Digital merupakan sumber informasi yang bisa berada didalam *storage devices*.[12] Barang bukti ini bersifat digital yang diekstrak dari barang bukti elektronik. Barang bukti ini dalam Undang-undang Nomor 11 Tahun 2008 dikenal dengan istilah informasi elektronik dan dokumen elektronik. Jenis barang bukti inilah yang harus dicari untuk kemudian dianalisis secara teliti keterkaitan masing-masing *file* dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik.[13] Contoh-contoh barang bukti digital antara lain *Logical file*, *Deleted file*, *Lost file*, *File slack*, *Log file*, *Encrypted file*, *Steganography file*, *Office file*, *Audio file*, *video file*, *image file*, *Email*, *User ID* dan *password*, *Short Message Service* (SMS), *Multimedia Message Service* (MMS), *Call logs*.

Ada beberapa aturan standar agar bukti-bukti digital dapat diterima dalam proses peradilan diantaranya :

- *Valid*: Data harus mampu diterima dan digunakan demi proses hukum
- Asli: Keaslian dari data tersebut.
- Lengkap: Bukti bisa disebut lengkap jika didalamnya terdapat banyak petunjuk yang dapat membantu investigasi.
- Dapat dipercaya: Data tersebut merupakan terbukti dari investigasi dan bukan hasil data rekayasa.[14]

Bukti digital bersifat rapuh, mudah menguap dan rentan jika tidak ditangani dengan benar. Semua jenis perubahan yang mengandung bukti digital akan mengarah pada kesimpulan yang salah, atau bukti tidak akan berguna. Akses ke bukti digital hanya diberikan untuk siapa yang diberi wewenang dan tidak ada yang menggunakan perangkat elektromagnetik dekat dengan bukti digital, dokumentasi kondisi dan konfigurasi media penyimpanan digital. Barang bukti yang telah didapatkan perlu dikembangkan (*Explore and Exploit*) kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan sehingga didapat hasil analisis antara lain: siapa yang telah melakukan, apa yang telah dilakukan (penggunaan *software* apa), hasil proses apa yang dihasilkan, dan waktu melakukan. Pengambilan bukti digital mengacu pada metode static forensic atau disebut juga metode akuisisi secara tradisional, hal ini berfokus pada memeriksa salinan duplikat.[13]

Barang bukti pada dasarnya sama yaitu merupakan informasi dan data, hanya saja kompleksitas dan media penyimpanannya yang mengubah sudut pandang dalam penanganannya. Barang bukti digital dalam komputer forensic secara garis besar terbagi menjadi 3 jenis, yaitu:

- Data aktif, yaitu data terlihat dengan mudah dikarenakan untuk beberapa kepentingan yang telah berkaitan sangat erat dengan kegiatan yang sedang dilakukan, contoh nya yaitu program, *file* gambar, dan dokumen *teks*.
- Data arsip, yaitu data yang sudah tersimpan untuk keperluan *backup*, contoh nya ialah dokumen berupa *file* yang telah terdigitalisasi untuk disimpan dalam format *Temporary Instruction File Format* (TIFF) dengan tujuan agar terjaga kualitas dokumen.
- Data laten, disebut juga data ambient. Data ambient adalah data yang tidak dapat dilihat langsung karena tersimpan pada lokasi yang tidak umum dan dalam format yang tidak umum juga misalnya, *database log* dan *internet log*. Data laten juga disebut sebagi *resudial* data.

Resudial data adalah data sisa ataupun data sementara.[16]

2.2.3. Akuisisi

Akuisisi pada digital forensic ialah sebagai digital forensic ilmu. Dengan suatu pemulihan dan investigasi dari bahan yang telah ditemukan dalam perangkat digital. Akuisisi yaitu suatu proses yang fungsi nya membuat salinan barang bukti digital dan juga mendokumentasikan metodologi yang telah digunakan dan juga aktifitas yang dilakukan.[14]

Pada tahap akuisisi terdapat langkah-langkah akuisisi bukti digital dilakukan dengan memperhatikan, media digital sebagai bukti nya, tata letak fisik media penyimpanan digital, integritas dan keaslian dari bukti digital yang telah menggunakan *write-protect*, *hash*, dan sebagainya. Akses pada bukti digital hanya diberikan untuk siapa yang telah di beri wewenang dan tidak ada yang menggunakan perangkat elektromagnetik dekat dengan bukti digital nya. Dokumentasi kondisi dan juga konfigurasi media penyimapanan digital nya, bukti digital berupa duplikat / pencitraan menggunakan prosedur dan perangkat dibawah standar akuisisi digital forensik.[2]

2.2.4. *Forensic Web Browser*

Forensic Web Browser ialah sebuah aktivitas investigasi untuk menganalisis apa yang dihasil dari penggunaan web browser tersebut. Analisis ini adalah untuk menemukan bukti digital dari aktivitas penggunaan terhadapat *web browser* seperti *cache*, *histori*, *cookie*, *timestamp*, *session*, dan *file downloads*. Bukti digital sangat penting karena dengan bukti digital dapat mengungkapkan kejahatan dan melacak pelaku kejahatan yang terbukti adanya. Seorang investigator setidaknya dalam analisis forensic web *browser* dapat menemukan bukti digital yang terdapat dalam web *browser* tersebut. [15]

2.2.5. *Web Browser*

Web Browser ialah perangkat lunak yang digunakan untuk

mengakses berupa halaman web untuk mendapatkan informasi yang jelas dan mudah dibaca. Sumber dari informasi diidentifikasi dengan *Uniform Resource Identifier* (URI) dan akan menjadi halaman web, gambar, video atau konten lainnya. Saat ini banyak jenis web *browser* dengan berbagai engine *browser* yang ada dalam perangkat lunak. Diantaranya yang paling banyak digunakan adalah Google Chrome, Mozilla Firefox, Opera, UcBrowser, Microsoft Edge. Dalam kondisi *mode private*, semua *vendor browser* mengatakan bahwa history, *cookie*, dan *download file* atau lainnya tidak akan disimpan dikomputer.[15]

2.2.6. *Harddisk* (HDD)

Hard Disk Drive (HDD) atau biasa dikenal dengan Harddisk ialah media penyimpanan sekunder pada sebuah komputer. Harddisk sebagai media penyimpanan sekunder akan tetapi pada kenyataan nya fungsinya sangatlah penting dan juga tidak bisa ditinggalkan lagi untuk kebutuhan sebuah laptop ataupun komputer. Hal ini sangatlah jelas dengan kebutuhan akan *software* berupa program maupun aplikasinya, serta data yang diolah membutuhkan media penyimpanan yang sangat besar, yang tidak cukup hanya ditampung oleh sebuah media penyimpanan utama berupa Read Only Memory (ROM) dan juga Random Acces Memory(RAM). Ada beberapa tipe dari harddisk interface sendiri menurut perkembangannya hingga saat ini ialah :

- *Small Computer System Interface* (SCSI)
- *Integrated drive electronics/enhanced* IDE (IDE/EIDE)
- *Universal Serial Bus* (USB)
- *Advanced Technology Attachment* (ATA)
- *Fiber Channel*[16]

2.2.7. *Software Forensic*

Tools software forensik dipergunakan untuk menganalisa data secara digital dalam proses analisa forensik untuk mendapatkan bukti-bukti digital yang ada. Diantara *software* yang digunakan untuk kepentingan identifikasi untuk memperoleh bukti digital ialah sebagai berikut:[14]

- *FTK Imager*

  Software ini biasa digunakan untuk sebuah acquisition tool digital forensik yang dibuat oleh Accesdata. FTK Imager ini merupakan *software* free atau *software* tidak berbayar. Namun jangan salah, dengan fasilitas yang telah disediakan dan juga kemampuannya tidak kalah hebat dengan *software* acquisition yang berbayar. FTK Imager dapat digunakan untuk membuat suatu image disebuah drive (physical imaging), membuat image isi sebuah folder, maupun membuat custom image yang terdiri atas *file* yang kita pilih saja. Masing-masing pilihan sangat berguna di dalam kondisi lapangan yang berbeda dan jenis *evidence* yang kita ingin investigasikan.[5] *Physical imaging* akan membuat *image* dari *harddisk suspect*, oleh karena itu tentu saja membutuhkan waktu yang lama karena kita harus mengkopikan seluruh konten harddisk ke dalam media eksternal kita yang biasanya menggunakan port usb (Misal HDD eksternal). Dibandingkan dengan hardware clone dan hardware imaging yang menggunakan hardware, kecepatan physical imaging dari FTK Imager ini tentu saja kalah jauh dengan yang berbayar. Namun FTK Imager ini sangat berguna dalam ruang lingkup yang tidak sering melepaskan atau mengambil harddisk yang didalam laptop untuk melakukan suatu tindakan kloning data maupun imaging menggunakan hardware , misalnya di suatu laptop yang masih berlakunya suatu

garansi karena dengan rusaknya segel tersebut akan menghilangkan garansi dari laptop tersebut. Di sinilah peran penting dari FTK Imager dalam data acquisition sekaligus menjaga agar evidence (bukti) tetap dilakukan, karena FTK Imager akan mengkalkulasi hash value, image, dan juga membuat manifest dari image yang dibuatnya.[9]

- *The Sleuthkit* (*Autopsy*)

  Software Autopsy ini ialah kumpulan *file command line* berbasiskan UNIX, sekaligus *tool* analisis forensik volume sistem. Autopsy dibuat dengan menggunakan bahasa C dan Perl, dan menggunakan beberapa kode serta rancangan dari *The Coroner's Toolkit* (TCT). Autopsy secara umum terbagi dari dua bagian yaitu dengan *file system tools* dan media management *tools*. *File system* tool memungkinkan pengguna untuk memeriksa *file system* dari sebuah komputer yang telah dicurigai, secara tersembunyi. Karena tool ini tidak bergantung pada operating *system* untuk mengolah *file system, file* yang telah dihapus atau disembunyikan dengan sengaja dapat ditampilkan. Tool yang termasuk kedalam bagian ini adalah *file system* layer, *file name* layer, meta data layer, data unit layer, dan juga yang terakhir ialah *file* sistem *journal*. Media management tools dapat memungkinkan *user* memeriksa layout dari sebuah disk dan media lainnya. Dengan *tool* ini, pengguna dapat mengidentifikasikan letak dari posisi partisi dan mengekstraknya, sehingga dapat menlakukan analisis dengan *file system* tool. Autopsy *forensic browser* ialah sebuah antarmuka grafis untuk tool-tool yang berada di dalam Sleuth kit, yang memudahkan user dalam menjalankan investigasi. Autopsy juga 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, dengan begitu user akan

membutuhkan web client untuk mengakses fungsi-fungsinya. Sleuth Kit dan Autopsy ini memiliki banyak keunggulan, misalnya ialah kemampuan untuk proses analisis dari berbagai jenis fiile *system* yang beda-beda. Dikarenakan suatu itool open source, keduanya dapat dikembangkan sesuai dengan kebutuhan masing-masing iuser.[5]

2.2.8. Kejahatan Dunia Maya

Untuk memudahkan pemahaman tentang *Cybercrime* yang dimana segala macam bentuk kejahatan virtual dengan memanfaatkan media *computer* berteknologi dengan menyalah gunakan kemudahan teknologi digital dengan mengeksploitasi *computer* lain yang terhubung dengan akses *internet* juga.[17] Dengan memanfaatkan lubang-lubang keamanan pada *system* operasi yang menyebabkan kelemahan dan terbukanya celah yang dapat digunakan para *cracker, hacker* dan *script kiddies* untuk menyusup kedalam komputer tersebut.[15]

Kejahatan komputer sering asosiasikan dengan *hacker*, yang biasanya menimbulkan arti yang negative dimana banyak yang menyatakan bahwa *Hacker* adalah seseorang yang senang memprogam dan percaya bahwa berbagi suatu informasi yang sangat berharga, dan pada umumnya *Hacker* adalah orang pintar dan senang terhadap semua hal yang berbau dengan computer.[18] Sasaran dan Teknik pelaku *CyberCrime* pada biasanya menggunakan *tools* yang sudah ada di *internet*, dimana *tools* tersebut kemudian dijalankan untuk menyerang *system computer*. *Hacker* yang berpengalaman membuat Script atau progam sendiri untuk melakukan *hacking*, dimana yang menjadi sasaran yaitu:

- *Database credit card*
- *Database account bank*
- Data informasi pelanggan seperti *account website*, *gmail* dan lain-lain.

- Pembelian barang dengan *credit* card milik orang lain atau sering disebut *carding*.