BAB II

TINJAUAN PUSTAKA

2.1 Kajian Pustaka

Penelitian Imam Riadi, Anton Yudhayana, Muhamad Ceaser Febriansyah Putra yang berjudul "Akuisisi Bukti Digital Pada *Instagram Masengger* Berbasis *Android* Menggunakan Metode *National Institute of Justice* (NIJ)". Mendapatkan bukti digital dari dua *smartphone* berbeda menggunakan *tools* yaitu oxygen forensik pada aplikasi *instagram* menggunakan metode *National Institute of Justice* (NIJ) menjadi tujuan penelitian ini. Hasil akhir dari penelitian tersebut ditemukan bahwa barang bukti digital pada aplikasi instagram diperoleh dalam kondisi *smartphone* telah di *root* yakni berupa gambar dan percakapan sedangkan untuk *smartphone* tidak dalam kondisi *root* barang bukti digital tidak didapatkan [16].

Penelitian selanjutnya berjudul Metode NIST Untuk Analisis Forensik Bukti Pada Perangkat *Android* oleh Rusydi Umar dan Sahirrudin. Penelitian ini berfokus kepada pengembalian data sebagai bukti digital berupa data kontak, dan pesan yang telah terhapus sebelumnya pada sebuah *smartphone* menggunakan dua buah *tools* yakni Oxygen Forensics Suite 2014 dan wondershare dr. fone for Android. Pengembalian barang bukti digital pada penelitian ini yaitu dengan menggunakan metode yang dikembangkan oleh National Institute of Standard and Tecnology (NIST) dan didapatkan hasil Wondershare dr. Fone for Android data yang dihapus berhasil dikembalikan dengan keberhasilan 30%, sementara Oxygen Forensics Suite 2014 keberhasilan mencapai 73% [17].

Penelitian selanjutnya berjudul analisis perbandingan *tools* forensic pada aplikasi twitter menggunakan metode digital forensics research workshop oleh imam riadi, ikhsan zuhriyanto, dan anton yudhana. Penelitian ini dilakukan dengan metode Digital Forensics Research Workshop (DFRWS) untuk memeperoleh bukti forensik pada aplikasi media sosial Twitter pada

smartphone. Mobiledit forensic express dan belkasoft evidence center dijadikan *tools* pada penelitian ini. Terdapat 16 skenario pencarian bukti digital dengan hasil akhir *tools* mobiledit forensic express memperoleh data sebesar yaitu 85,75% dengan 14 bukti yang berhasil diperoleh dari 16 skenario sedangkan belkasoft evidence center mendapatkan akurasi 43,75% dengan 7 bukti dari 16 skenario [18].

Penelitian selanjutnya berjudul analisis live forensic pada whatsapp web untuk pembuktian kasus penipuan transaksi elektronik oleh syaza dyah utami, carudin, dan azhari ali ridha. Penelitian ini secara Live Forensic dengan NIST sebagai metodelogi yang digunakan dan *tools* forensik yaitu ftk imager dan browser history viewer untuk mengungkap kasus penipuan pada whatsapp web. Ditemukan teks percakapan, gambar, video, timestamp, history, nomor rekening pelaku, dan nomor handphone korban yang merupakan bukti digital untuk pembuktian kasus itulah hasil akhir dari penelitian ini [19].

Penelitian selanjutnya berjudul *forensic tools comparison on instagram digital evidence based on android with the nist method* oleh Imam Riadi, Anton Yudhana, Dan Muhamad Caesar Febriansyah Putra. Dalam penelitian ini mencari bukti digital pada aplikasi Instagram dan mengkomparasi hasil bukti digital yang ditemukan oleh dua *tools* yaitu Oxygen forensics dan Axiom Magnets. Untuk hasil akhir dari penelitian ini adalah data yang didapat *tools* Axiom Magnet mencapai 100% sedangkan Forensic Oxygen sebesar 84%[20].

Penelitian selanjutnya yang di lakukan oleh Imam Riadi, Sunardi, dan Sahiruddin pada penelitian "*Perbandingan Tools Forensik Data Recovery Berbasis Android Menggunakan Metode NIST*". Pada penelitian ini membahas tentang bagaimana cara mengembalikan data berupa log panggilan, kontak, dan pesan pada dua *smartphone* dengan jumlah data yang berbeda, pada penelitian ini menggunakan metode NIST dengan dua *tools* forensic yaitu wondershare dr. fone for android dan oxygen forensic suite 2014. Hasil akhir yang didaptkan *tools* Wondershare hanya mencapai 31% data terhapus dapat dikembalikan, sedangkan hasil kinerja dengan Oxygen forensik mencapai 67% pada

smartphone 1 hasil kinerja. Pada *smartphone* 2 Wondershare 35% , sedangkan dengan Oxygen forensik mencapai 69% data dapat dikembalikan [21].

Pada penelitian selanjutnya yang diteliti oleh Imam Riadi dan Tomi Pandela mengenai "Browser Forensics on Web-based Tiktok Applications". Mereka melakukan analisis mengenai forensik pada aplikasi web TikTok dengan skenario melakukan posting video pada aplikasi dan menghapusnya. Dilakukan pengembalian data yang dihapus dengan *tools* forensik FTK Imager, Browser History Capture dan Video Cache Viewer. Dan hasil akhir dari penelitian ini yaitu FTK Imager mampu mendapakan bukti teks berupa info akun dan link, untuk browser history capture foto, username, dan link, dan terakhir video cache viewer hanya link saja [6].

Untuk penelitian selanjutnya yang dilakukan oleh Ilhami Algi Plianda dan Rini Indrayanti dengan tema "Analisa dan Perbandingan Performa *Tools* Forensik Digital pada *Smartphone* Android menggunakan Instant Messaging Whatsapp". Di dalam penelitian mereka ini memilik tujuan untuk menguji peforma software forensik yaitu Mobiledit Forensik dan Oxygen Forensik *tools*. Untuk skenario mereka memiliki 19 skenario hasil akhir yang mereka buat, Mobiledit memiliki keunggulan dalam menemukan bukti dibanding Oxygen dalam kasus aplikasi IM Whatsapp [22].

Penelitian yang dilakukan oleh Maghvirna Rafika Dhewi Qibriya, Awalludiyah Ambarwati, Kunto Eko Susilo mengenani "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di *Smartphone* Berbasis Android Untuk Bukti Digital". Dengan tujuan penelitian yaitu membuktikan kasus penipuan yang dilakukan dalam aplikasi IM yaitu whatsapp dan telegram dibantu oleh *tools* forensik mobiledit sebagai imaging dan untuk analisis menggunakan *tools* FTK imager dan autopsy dengan hasil akhir pada penelitian ini yaitu untuk aplikasi whatsapp ini dapat mengembalikan dan menemukan semua data setelah dianalisa oleh kedua *tools*, sedangkan untuk telegram hanya file media saja yang dapat ditemukan untuk riwayat percakapan tidak dapat ditemukan atau di kembalikan [23].

Tabel 2.1 Kajian Pustaka

No	Judul	Objek	Metode	Hasil	Perbedaan
1.	Akuisisi Bukti Digital Pada Instagram Masengger Berbasis Android Menggunakan Metode National Institute of Justice (NIJ). (2018). [16].	Objek pada penelitian ini yaitu mengungkapkan kasus *cyberbullying* pada aplikasi *Instagram*.	Penelitian dilakukan menggunakan *National Institute of Justice* (NIJ).	Hasil penelitian ini yaitu proses akuisisi bukti digital menggunakan *tools OXYGEN Forensic* pada saat *smartphone* dalam keadaan sudah di *root* dapat menemukan bukti.	Fokus pada penelitian ini yaitu berfokus pada fitur *Direct Message* pada aplikasi *Instagram*.
2.	Metode NIST Untuk Analisis Forensik Bukti Pada Perangkat Android. (2019). [17].	Objek pada penelitian ini yaitu *Recovery Data* log panggilan, pesan, dan kontak pada *smartphone*.	Metode yang digunakan pada penelitian ini *National Institute of Standard Techonlogy* (NIST).	Hasil penelitian ini yaitu Wondershare dr. Fone for Android berhasil mengembalikan data terhapus 30%, Oxygen Forensics Suite 2014 mencapai 73%.	Penelitian ini berfokus pada *recovery* data log panggilan, kontak, dan pesan pada *smartphone* berbasis *android*.

No	Judul	Objek	Metode	Hasil	Perbedaan
3.	Analisis Perbandingan *Tools* Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop. (2020). [18].	Objek pada penelitian ini yaitu menemukan bukti *forensic* pada aplikasi media sosial *Twitter* yang diakses menggunakan aplikasi *smartphone*	Penelitian ini menggunakan yaitu *Digital Forensics Research Workshop* (DFRWS).	Hasil penelitian ini menunjukan software digital forensik MOBILedit Forensic Express lebih baik dengan tingkat akurasi 85,75% sedangkan Belkasoft Evidence Center 43,75%.	Fokus penelitian ini yaitu menemukan bukti digital berdasarkan skenario 16 variabel pada aplikasi *mobile Twitter*.
4.	Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus penipuan Transaksi Elektronik. (2021). [19].	Objek pada penelitian ini yaitu mendapatkan barang bukti digital kasus penipuan pada Aplikasi *Whatsapp Web.*	Metode yang digunakan dalam penelitian ini yaitu *Live Forensic* dengan Metodelogi *National Institute of Standard Techonlogy* (NIST).	Hasil dari penelitian ini berhasil mendapatkan bukti digital berupa teks percakapan, filename gambar, filename video, timestamp, history, nomor rekening pelaku	Fokus dalam penelitian ini yaitu pengungkapan bukti digital pada Aplikasi *Whatsapp Web*.

No	Judul	Objek	Metode	Hasil	Perbedaan
5.	Forensic *Tools* Comparison on Instagram Digital Evidence Based on Android with The NIST Method. (2018). [20].	Objek pada penelitian ini yaitu menemukan bukti digital berupa *chat* dan *image* pada aplikasi *Instagram*	Metode penelitian ini menggunakan *National Institute of Standard Techonlogy* (NIST).	Hasil dari penelitian ini yaitu hasil dari mendapatkan data *chat* dan *image* sesuai skenario yang dibuat dengan menggunakan dua *tools* dengan hasil untuk Oxygen Forensic Magnets 87% sedangkan Axiom Magnet 100%	Fokus dalam penelitian ini yaitu menemukan bukti berupa *chat, image* pada kasus *cyberbullying* pada *instagram*
6.	Perbandingan *Tools* Forensik Data *Recovery* Berbasis Android Menggunakan Metode NIST. (2020). [21]	Objek pada penelitian ini yaitu *recovery* data log panggilan, pesan, dan kontak pada dua *smarphone* yang berbeda	Metode penelitian ini menggunakan *National Institute of Standard Techonlogy* (NIST)	*Smartphone* 1 Wondershare 31% Oxygen forensik 67%. Pada *smartphone* 2 Wondershare 35%, Oxygen forensik mencapai 69%.	Fokus pada penelitian ini yaitu *recovery* data pada log panggilan, pesan, dan kontak pada dua buah *smartphone*.

No	Judul	Objek	Metode	Hasil	Perbedaan
7.	Browser Forensics on Web-based Tiktok Applications. (2020). [6].	Melakukan *recovery* data posting yang di hapus pada Aplikasi Tik Tok berbasis Website	Metode penelitian ini menggunakan *National Institute of Standard Techonlogy* (NIST)	Mendapatkan hasil pada setiap *tools* forensik yang digunakan yaitu untuk *FTK Imager* untuk analisis data bersifat text, *Browser History Capture* untuk mencari *Link/URL* yang di akses, dan *Video Cache View*.	Dalam penelitian ini hanya berfokus pada pengembalian data posting dan ini bersifat *Live Forensic*
8.	Analisa dan Perbandingan Performa *Tools* Forensik Digital pada *Smartphone* Android menggunakan Instant Messaging Whatsapp. (2022). [22].	Melakukan analisis perbandingan *tools* forensik pada aplikasi *IM Whatsapp* dalam *recovery*	Metode penelitian ini menggunakan *National Institute of Standard Techonlogy* (NIST)	Untuk hasil akhir *Mobiledit Forensik* lebih unggul dengan berhasil mendapatkan data keseluruhan dibandingkan dengan *OXYGEN Forensik*	Untuk objek penelitian sendiri hanya aplikasi *IM Whatsapp*

No	Judul	Objek	Metode	Hasil	Perbedaan
9.	Analisis Forensik Digital Pada Aplikasi Instant Messaging Di *Smartphone* Berbasis Android Untuk Bukti Digital. (2021). [23].	Mengembalikan dan Menemukan bukti kasus kejahatan penipuan pada aplikasi *instant mesaging* Whatsapp dan Telegram	Metode penelitian ini menggunakan *National Institute of Standard Techonlogy* (NIST) *SP 800-101 RI*	Analisis menggunakan *tools* FTK Imager dan Autopsy untuk Whatsapp sendiri dapat menemukan semua file sedangkan untuk telegram hanya dapat mengembalikan file media saja	Objek pada penelitian ini whatsapp dan telegram

2.2 Landasan Teori

2.2.1 Digital Forensik

Ilmu penerapan pengetahuan di bidang komputer dalam hal dalam pembuktian di bidang hukum, guna untuk membuktikan kejahatan dengan *smartphone* atau kejahatan komputer secara ilmiah maka dari itu bukti-bukti digital didapatkan digunakan untuk menghukum pelaku kejahatan. Pada dasarnya ilmu ini dapat mencari bukti digital yang biasa tersimpan pada penyimpanan perangkat digital sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan, dan lainya [17].

2.2.2 Mobile Forensik

Merupakan ilmu turunan dari ilmu pengetahuan digital forensik adalah mobile forensik. Metode ilmiah dari digital forensik yang mempelajari tentang cara pemeliharaan, pengumpulan, validasi, analisis, interprestasi, dokumentasi dan presentasi bukti digital dari

sumber-sumber digital untuk tujuan membuktikan peristiwa kejahatan yang terjadi. Bisa dikatakan mobile forensik merupakan ilmu yang melakukan proses pemulihan bukti digital dari perangkat mobile menggunakan cara sesuai proses investigasi forensik [24].

2.2.3 Sosial Media

Media sosial menjadi fasilitas yang digunakan untuk mengutarakan identitas dan suasana hati bagi perorangan maupun kelompok secara daring dengan menunggah gambar, video, serta artikel. Seriap pengguna mempunyai tujuan serta kegiatan tersendiri yang menjadi alasan bermedia sosial, sebagai contoh swafoto, *cyberwar*, mencari informasi. [25].

2.2.4 *Smartphone*

Smartphone atau sering disapa gadget sebuah perangkat yang didalamnya terdapat mikroprosesor, media peyimpanan, layar dan modem. *Smartphone* merupakan perangkat pintar dengan fungsionalitas sama dengan komputer dalam bentuk yang kecil. Fitur yang dimiliki *smartphone* diantaranya, pesan teks, kamera, pemutar music dan video, game, akses e-mail, tv digital, *search engine*, pengelola informasi pribadi, fitur GPS, jasa telepon internet.

Pertama kali dikenalkan *smartphone* dengan sistem operasi android sebagai platform perangkat mobile open source yang dikembangkan kernel Linux 2.6 dan dikelola oleh Open Handset Alliance, sekelompok operator, produsen, perangkat dan komponen mobile, dan vendor perangkat lunak [17].

2.2.5 National Institute of Standards and Technology (NIST) 800-86

Pengaplikasian metode guna mengetahui prosedur dan alur penelitian secara sistematis, dan menerangkan bagaimana langkah-langkah penelitian yang akan dilaksanakan sehingga dapat dijadikan landasan pada investigas penelitian ini. *Collection, Examination, Analysis dan Reporting* adalah tahapan dari metode ini [7]. Untuk prosedur metode bisa dilihat pada gambar dibawah ini:

Gambar 2.1 Skema Metode NIST 800-86

Keterangan lebih lanjut dari proses dari metode (NIST) 800-86 adalah sebagai berikut [21]:

2.2.5.1 *Collection/Preservation*

Langkah pertama dalam proses forensik adalah mengidentifikasi sumber data potensial dan memperoleh data darinya. menjelaskan berbagai sumber data yang tersedia dan membahas tindakan yang dapat dilakukan organisasi mengambil untuk mendukung pengumpulan data yang sedang berlangsung untuk tujuan forensik. Memperoleh Data Setelah mengidentifikasi sumber data potensial, analis perlu memperoleh data dari sumber tersebut. Data akuisisi harus dilakukan dengan menggunakan proses tiga langkah

Dapatkan datanya. Jika data belum diakuisisi oleh alat keamanan, alat analisis, atau cara lain, proses umum untuk memperoleh data melibatkan penggunaan alat forensik untuk mengumpulkan data volatil, menduplikasi sumber data non-volatil untuk mengumpulkan data mereka, dan mengamankan yang asli sumber data yang tidak mudah menghilang.

2.2.5.2 *Examination*

Setelah data terkumpul, tahap selanjutnya adalah menguji data, yang meliputi penilaian dan mengekstrak informasi yang relevan dari data yang dikumpulkan. Fase ini mungkin juga melibatkan melewati atau mengurangi fitur OS atau aplikasi yang mengaburkan data dan kode, seperti kompresi data,

enkripsi, dan mekanisme kontrol akses. Hard drive yang diperoleh mungkin berisi ratusan ribu dari file data; mengidentifikasi file data yang berisi informasi yang menarik, termasuk informasi disembunyikan melalui kompresi file dan kontrol akses, bisa menjadi tugas yang menakutkan. Selain itu, file data dari bunga mungkin berisi informasi asing yang harus disaring.

Misalnya, log firewall kemarin mungkin menyimpan jutaan catatan, tetapi hanya lima catatan yang mungkin terkait dengan peristiwa yang menarik. Untungnya, berbagai alat dan teknik dapat digunakan untuk mengurangi jumlah data yang harus diayak melalui. Pencarian teks dan pola dapat digunakan untuk mengidentifikasi data terkait, seperti menemukan dokumen yang menyebutkan subjek atau orang tertentu, atau mengidentifikasi entri log email untuk alamat email tertentu. Teknik lain yang bermanfaat adalah dengan menggunakan alat yang dapat menentukan jenis konten dari setiap file data, seperti: teks, grafik, musik, atau arsip file terkompresi. Pengetahuan tentang tipe file data dapat digunakan untuk mengidentifikasi file yang perlu dipelajari lebih lanjut, serta untuk mengecualikan file yang tidak menarik untuk pemeriksaan. Di sana juga database yang berisi informasi tentang file yang diketahui, yang juga dapat digunakan untuk menyertakan atau mengecualikan file dari pertimbangan lebih lanjut. Informasi khusus tentang alat dan teknik pemeriksaan

2.2.5.3 *Analysis*

Kesimpulan berdasarkan data yang tersedia atau menentukan bahwa belum ada kesimpulan yang dapat ditarik. Analisis harus mencakup mengidentifikasi orang, tempat, barang, dan peristiwa, dan menentukan bagaimana elemen-elemen ini berhubungan sehingga dapat ditarik suatu kesimpulan.

Seringkali, upaya ini akan mencakup data yang menghubungkan antara beberapa sumber. Misalnya, log sistem deteksi intrusi jaringan (IDS) dapat menautkan suatu peristiwa ke a host, log audit host dapat menautkan acara ke akun pengguna tertentu, dan log IDS host dapat menunjukkan tindakan apa yang dilakukan pengguna. Alat seperti logging terpusat dan manajemen acara keamanan perangkat lunak dapat memfasilitasi proses ini dengan mengumpulkan dan menghubungkan data secara otomatis. Perbandingan karakteristik sistem ke baseline yang diketahui dapat mengidentifikasi berbagai jenis perubahan yang dilakukan pada sistem.

2.2.5.4 *Reporting*

Tahap reporting merupakan proses akhir yaitu pelaporan hasil analisis yang meliputi informasi data barang bukti yang berhasil ditemukan Tahap terakhir adalah pelaporan, yaitu proses penyusunan dan penyajian informasi yang dihasilkan dari tahap analisis. Banyak faktor yang mempengaruhi pelaporan, termasuk yang berikut ini.

a) Penjelasan Alternatif. Ketika informasi mengenai suatu acara tidak lengkap, mungkin tidak mungkin untuk sampai pada penjelasan definitif tentang apa yang terjadi.
b) Pertimbangan Audiens. Mengetahui audiens yang akan ditampilkan data atau informasinya penting. Sebuah insiden yang membutuhkan keterlibatan penegak hukum membutuhkan laporan yang sangat rinci dari semua informasi yang dikumpulkan, dan mungkin juga memerlukan salinan dari semua data bukti yang diperoleh.
c) Informasi yang Dapat Ditindaklanjuti. Pelaporan juga mencakup mengidentifikasi informasi yang dapat ditindaklanjuti yang diperoleh dari data yang

memungkinkan seorang analis mengumpulkan sumber informasi baru [26].

2.2.6 Bukti Digital

Bukti digital menurut ahli yaitu "The Scientific Working Group on Digital Evidence" (SWGDE) adalah "*Information of probative value stored or transmitted in digital form*". Segala sesuatu yang memilliki sifat menguak sebuah kasus kejahatan dalam bentuk digital. definisi tersebut dapat diartikan lagi, bukti digital tidak hanya sebuah bukti yang diperoleh dalam jaringan komputer saja, akan tetapi juga termasuk perangkat audio, video bahkan telpon selular [27].

2.2.7 Instagram

Sosial media yang memberi layanan berbagi foto yang memungkinkan pengguna untuk berfoto dan memberi filter lalu menyebarluaskannya di jejaring sosial adalah instagram. Instagram sebagai aplikasi yang memiliki banyak pengguna *smartphone* saat ini. Kebanyakan tujuan menggunakan instagram selain unggah foto, yaitu mengirim *chatting* yang mereka lakukan kesesama pengguna Instagram [6].

2.2.8 MOBILedit Forensic Express

MOBILedit Forensic Express merupakan *tools* forensik yang memungkinkan penyidik memperoleh secara logic. melacak dan memeriksa ponsel dengan beberapa mekanisme konektivitas terutama nirkabel, cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lain seperti kontak dan pesan [18].

2.2.9 Autopsy

Platform forensik open source besutan Basis Technology dalam situs resminya autopsy sebagai aplikasi mudah digunakan, dan mampu menganalisis semua jenis perangkat seluler dan media digital. Sedangkan menurut situs resmi CGSecurity, PhotoRec menjadi perangkat lunak multi-platform open source yang dirancang untuk memulihkan file yang hilang pada berbagai macam sistem file [28].

2.2.10 *Cybercrime*

Perbuatan melanggar hukum dengan menggunakan teknologi komputer dengan memakai kecanggihan teknologi internet. *Cybercrime* adalah istilah kejahatan melalui jaringan komputer untuk dijadikan alat, sasaran, atau tempat kejadian perkara. Beberapa kejahatan *cybercrime* yaitu hatespeech, lelang online, cek pemalsuan, penipuan kredit/kartu, penipuan kepercayaan, hatespeech identitas, pornografi. *Cybercrime* dapat terjadi di semua perangkat elektronik, seperti *smartphone android* [24].

2.2.11 Tik Tok

Tiktok salah satu *software* mobile yang menyediakan fitur visual effect video yang dapat membuat video pendek dengan hasil yang keren serta dapat dipamerkan kepada teman teman atau pengguna lainnya. Sosial media video pendek ini mendukung musik yang banyak sehingga penggunanya menciptakan kreatifitas lewat tarian, gaya bebas, dan masih banyak lagi [29].

2.2.12 FTK Imager

Forensic *Tools*kit Imager (FTK Imager) yakni salah satu *tools* digital forensik yang dijalankan pada saat proses penyidikan menggunakan teknik live atau static bisa keduanya. fungsi dari *tools* ini melakukan akuisisi data, dimana sistem berfungsi untuk mengambil, mengumpulkan dan menyiapkan data salah satu fungsi akuisisi, untuk menghasilkan data yang diinginkan [17].