BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terkait

2.1.1 Penelitian oleh Feryan Lutfie Nafila, dan Yudi Prayudi (2022)

Penelitian yang berjudul Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android dengan metode NIST, dilakukan oleh Feryan Lutfie Nafila, dan Yudi Prayudi pada tahun 2022. Penelitian ini bertujuan untuk melakukan pengujian dan analisa forensik terhadap aplikasi Signal Messenger berbasis android. Hasil penelitian dapat disimpulkan bahwa penelitian ini penerapan metode NIST berjalan dengan baik. Akusisi dengan menggunakan software Magnet AXIOM 4.10 dan hasil Akuisisi terbaca dengan baik oleh software Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 namun *software* tersebut tidak dapat membaca database dari aplikasi Signal Messenger yang ter *decrypt* sehingga informasi mengenai pesan, media, video, file tidak dapat diperoleh. Analisis data backup dengan menggunakan software Signal-back mampu menampilkan media yang tersimpan dalam data backup seperti gambar, video, file sedangkan untuk software Signalbackup-tools file database dapat di *decrypt* dan diektrak dan kemudian data pada pada database dapat ditampilkan dan menyimpan informasi seperti pesan teks, pesan gambar, pesan video serta informasi file dokumen namun tidak ditemukan data mengenai panggilan suara maupun panggilan video. Dari beberapa software yang telah diuji beberapa digital artifak yang berhasil didapat dan kemudian bisa dijadikan sebagai barang bukti adalah data pesan teks, media gambar, media video, dan file dokumen. Pada penelitian ini beberapa *software* yang digunakan seperti Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 belum mampu untuk membaca database aplikasi Signal Messenger yang terenkripsi. Kemudian software Signal-back dan Signalbackup-tools yang digunakan untuk melakukan decrypte pada data backup tidak mampu menampilkan panggilan suara dan panggilan video. Oleh karena itu diharapkan untuk penelitian berikutnya mampu melakukan analisis lebih lanjut

dengan file akuisisi serta data backup yang dapat menampilkan informasi lebih lengkap [13].

2.1.2 Penelitian oleh Ratri Ayunita Kinasih, dkk. (2020)

Penelitian yang berjudul Analisis Keamanan Browser Menggunakan Metode *National Institute Of Justice* (NIJ) (Studi Kasus: Facebook Dan Instagram), dilakukan oleh Ratri Ayunita Kinasih, dkk. pada tahun 2020. Penelitian ini menggunakan metode *National Institute of Justice* (NIJ) yaitu *identification*, *collection*, *examination*, *analysis*, dan *reporting*. Banyaknya kasus pencurian akun di media sosial menjadi permasalahan dilakukan penelitian ini. Alasan dilakukan penelitian ini yaitu mengetahui browser yang aman digunakan untuk mengakses Facebook dan Instagram dari bukti digital yang didapatkan. Tujuan penleitian ini yaitu menerapkan *live forensics* pada keamanan browser untuk mengakses media sosial Facebook dan Instagram serta menemukan bukti digital dari analisis Facebook dan Instagram pada browser. Berdasarkan hasil penelitian yang ada dapat disimpulkan bahwa Google Chrome, Mozilla Firefox, dan Microsoft Edge tidak aman digunakan unutk mengakses facebook, karena email dan password yang digunakan untuk proses login dapat terdeteksi pada penelitian ini. Mozilla Firefox lebih aman digunakan untuk mengakses Instagram dibandingkan dengan Google Chrome dan Microsoft Edge, karena password yang digunakan untuk login tidak dapat terdeteksi. Teknik *live forensics* dilakukan ketika sistem dalam keadaan menyala, sehingga data volatile masih terekan pada *Random Access Memory* (RAM). Dalam analasis digital *forensics* harus dilakukan secara berulang agar data yang didapatkan lebih baik. Keterbatasan dalam penelitian hanya menggunakan tiga browser dan dua media sosial, dapat dikembangkan lagi dengan menggunakan browser dan media sosial yang lebih banyak lagi agar hasil penelitian yang didapatkan lebih baik [14].

2.1.3 Penelitian oleh Imam Riadi, dkk. (2020)

Penelitian yang berjudul Investigasi *Cyberbullying* pada WhatsApp Menggunakan *Digital Forensics Research Workshop* (DFRWS), dilakukan oleh Imam Riadi, dkk. pada tahun 2020. Penelitian melakukan proses akuisisi

menggunakan aplikasi forensik yaitu MOBILedit yang digunakan untuk mengangkat barang bukti yang kemudian akan dilakukan analisis lebih lanjut mengenai tindakan *cyberbullying*. Penelitian ini menggunakan metode *Digital Forensics Research Workshop* (DFRWS) yang meliputi pemeliharaan, pengumpulan, validasi, identifikasi, analisis, interprestasi, dokumentasi, dan presentasi bukti digital. Hasil yang didapat menggunakan metode DFRWS membantu proses akuisisi untuk mengungkap bukti digital pada pelaku di fitur Group berupa teks. Hasil identifikasi tindakan yang mengarah pada cyberbullying didapatkan dengan nilai hasil tertinggi memiliki tingkat *cyberbullying* sebesar 0,05 dan nilai hasil terendah memiliki tingkat *cyberbullying* dengan nilai ISC sebesar 0,02 dari persentase tersebut didapat nilai kata *cyberbullying* pada percakapan terhadap *query*. Data tersebut membuktikan bahwa metode DFRWS dapat mengangkat barang bukti berupa teks dalam *group* dan metode *Improved Sqrt-Cosine* dapat mengidentifikasi *cyberbullying* seseorang yang akan melakukan tindakan *cyberbullying* dengan tingkat yang berbeda-beda [15].

2.1.4 Penelitian oleh Rauhulloh Ayatulloh Khomeini Noor Bintang, dkk. (2020)

Penelitian yang berjudul Analisis Media Sosial Facebook Lite dengan aplikasi Forensik menggunakan Metode *National Institute of Standards and Technology* (NIST), dilakukan oleh Rauhulloh Ayatulloh Khomeini Noor Bintang, dkk. pada tahun 2020. Penelitian ini menggunakan *National Institute of Standards and Technology* (NIST), metode ini dapat mempermudah proses investigasi mulai dari pengangkatan barang bukti sampai dengan tahap pelaporan barang bukti dengan tahapan *Collection, Examination, Analysis* dan *Reporting*. Hasil dari *scenario* dengan menggunakan Smartphone Android Galaxy J2, dengan melakukan *Rooting*, dan menginstall aplikasi Facebook Lite, membuat postingan, dan melakukan proses investigasi menggunakan aplikasi forensik yang bernama MOBILedit Forensik, kemudian melakukan analisis menggunakan aplikasi forensik tersebut dan mendapatkan hasil analisis yang akan menjadi barang bukti digital. Hasil yang telah didapatkan dalam penggunaan aplikasi forensik berikut

yaitu Akun ID, Images, Audio, Video [12].

2.1.5 Penelitian oleh Panggah Widiandana, dkk. (2020)

Penelitian yang berjudul Implementasi Metode *Jaccard* pada Analisis Investigasi *Cyberbullying* WhatsApp *Messenger* Menggunakan Kerangka Kerja *National Institute of Standards and Technology* (NIST), dilakukan oleh Panggah Widiandana, dkk. pada tahun 2020. Penelitian ini menggunakan dua metode yaitu metode *Jaccard* dan metode *National Institute of Standards and Technology* (NIST). Metode *Jaccard* digunakan untuk mengidentifikasi barang bukti digital dengan tahapan *prepocessing*, pembobotan kata, dan identifikasi *bullying*. Sedangkan metode *National Institute of Standards and Technology* (NIST) dapat mempermudah proses investigasi dalam pengangkatan barang bukti sampai dengan tahap pelaporan barang bukti dengan tahapan *Collection, Examination, Analysis* dan *Reporting*. Hasil penelitian ini, metode *Jaccard* mampu mengidentifikasi *bullying* dengan tingkat yang berbeda, nilai presentasi pelaku tertinggi yang didapat yaitu 21% kata teridentifikasi 79% lainnya kata tidak teridentifikasi, dan pelaku dengan nilai terendah yang didapat 13% kata teridentifikasi 87% lainnya kata tidak teridentifikasi. Perhitungan menggunakan aplikasi dan perhitungan secara manual didapatkan kesamaan 100% [3].

2.1.6 Penelitian oleh Vindy Arista Yuliani, dan Imam Riadi (2019)

Penelitian yang berjudul *Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Frame*work, dilakukan oleh Vindy Arista Yuliani, dan Imam Riadi pada tahun 2019. Penelitian ini bertujuan untuk mencari bukti forensik kejahatan kriminal di aplikasi WhatsApp. Penelitian ini menggunakan aplikasi oxygen forensic dan andriller. Sedangkan untuk metode analisisnya menggunakan metode *National Institute of Standard and Technology* (NIST) versi 800-101, memiliki tahapan seperti *Preservation, Acquisition, Examination & Analysis,* dan *Reporting.* Penelitian ini berhasil mendapatkan bukti artefak berupa eksplorasi laporan data ponsel cerdas seperti sesi obrolan, avatar, kontak di aplikasi whatsapp, status on whatsapp, dan juga mendapatkan file media whatsapp dan file database cadangan

terenkripsi [16].

2.1.7 Penelitian oleh Imam Riadi, dkk. (2018)

Penelitian yang berjudul Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode *National Institute Of Justice* (NIJ), dilakukan oleh Imam Riadi, dkk. pada tahun 2018. Penelitian yang dilakukan untuk mendapatkan barang bukti digital dari sebuah *smartphone* yang menjadi barang bukti elektronik dari kejahatan yang terindikasi *cyberbulling*. Proses akuisisi data menggunakan metode *National Institute Of Justice* (NIJ) yang merekomendasikan beberapa macam tahapan seperti persiapan, koleksi, pemeriksaan, analisis dan pelaporan. Proses akuisisi yang dilakukan menggunakan aplikasi OXYGEN forensik sehingga mendapatkan hasil sesuai dengan yang diinginkan yakni barang bukti digital berupa gambar/foto dan percakapan/*chatting* dari sosial media Instagram yang terpasang pada smartphone tersebut. Proses akuisisi barang bukti digital yang berhasil didapatkan pada Instagram pada *smartphone* dalam kondisi *Root* didapatkan data yang diharapkan yakni berupa gambar/foto dan percakapan/*chatting* sedangkan untuk smartphone tidak dalam kondisi *Root* tidak didapatkan barang bukti digital [17].

Tabel 2. 1 Penelitian Terkait

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
1.	Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android dengan metode NIST Oleh Feryan Lutfie Nafila, dan Yudi prayudi.	2022	*National Institute of Standard and Technology* (NIST) 800-101	Beberapa pengguna aplikasi pesan singkat menjadi khawatir dengan data pesan yang mereka kirimkan akan disalahgunakan oleh perusahaan aplikasi pesan tersebut. Kekhawatiran ini semakin tinggi setelah aturan baru yang dikeluarkan oleh perusahaan aplikasi tersebut dimana data dari aplikasi pesan akan dihubungkan dengan aplikasi lain untuk keperluan bisnis perusahaan, beberapa pengguna aplikasi tersebut merasa khawatir akan privasi mereka memilih untuk beralih ke aplikasi pesan lain yang dirasa lebih aman dan menawarkan privasi. Salah satu aplikasi yang menjadi pilihan adalah Signal Messenger karena aplikasi ini dianggap lebih aman dalam	Pada penelitian ini beberapa *software* yang digunakan seperti Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 belum mampu untuk membaca database aplikasi Signal Messenger yang terenkripsi. Kemudian *software* Signal-back dan Signalbackup-tools yang digunakan untuk melakukan *decrypte* pada data backup tidak mampu menampilkan panggilan suara dan panggilan video.	• Studi kasus media sosial yang di teliti pada penelitian ini yaitu Signal Messenger. • Menggunakan *tool* Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18. • Menggunakan *tool software* Signal-back dan Signalbackup-tools untuk melakukan *decrypte* pada data backup

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
				menjaga privasi.		
2.	Analisis Keamanan Browser Menggunakan Metode *National Institute Of Justice* (Studi Kasus: Facebook Dan Instagram) Oleh Ratri Ayunita Kinasih, dkk.	2020	*National Institute Of Justice* (NIJ)	Media sosial Facebook mengalami kebocoran data pengguna sejumlah 87 juta data pada tahun 2018. Pada April 2019 UpGuard menemukan bahwa Cultura Colectiva sebuah perusahaan media digital di Meksiko meninggalkan lebih dari 540 juta arsip pengguna Facebook di basis data publik. Bahkan di Indonesia data pengguna marketplace dicuri oleh pihak yang tidak bertanggung jawab. Facebook berada di peringkat ketiga sebagai social media yang banyak digunakan dengan jumlah pengguna sebanyak 82% dari jumlah pengguna internet di Indonesia sedangkan Instagram berada di urutan keempat dengan jumlah pengguna 79% dari	Google Chrome, Mozilla Firefox, dan Microsoft Edge tidak aman digunakan untuk mengakses facebook, karena email dan password yang digunakan untuk proses login dapat terdeteksi pada penelitian ini. Mozilla Firefox lebih aman digunakan untuk mengakses Instagram dibandingkan dengan Google Chrome dan Microsoft Edge, karena password yang digunakan untuk login tidak dapat terdeteksi. Teknik *live forensics* dilakukan ketika sistem dalam keadaan menyala, sehingga data volatile masih terekan pada *Random Access Memory* (RAM). Dalam analasis digital *forensics* harus dilakukan	• Studi kasus media sosial menggunakan dua media sosial yaitu Facebook dan Instagram. • Menggunakan metode *National Institute Of Justice* (NIJ).

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
				jumlah pengguna internet di Indonesia. Semakin banyak pengguna internet yang ada di Indonesia memungkinkan semakin banyak pengguna Facebook dan Instagram di waktu yang akan datang. Tidak sedikit pengguna media sosial yang menyalahgunakan media sosial untuk melakukan kejahatan-kejahatan elektronik seperti membuat akun media sosial palsu.	secara berulang agar data yang didaptakan lebih baik. Keterbatasan dalam penelitian hanya menggunakan tiga browser dan dua media sosial, dapat dikembangkan lagi dengan menggunakan browser dan media sosial yang lebih banyak lagi agar hasil penelitian yang didapatkan lebih baik.	
3.	Investigasi *Cyberbullying* pada WhatsApp Menggunakan *Digital Forensics Research Workshop* (DFRWS) Oleh Imam Riadi, dkk.	2020	*Digital Forensics Research Workshop* (DFRWS)	Banyaknya pengguna media sosial khususnya WhatsApp membuka peluang adanya kejahatan siber (*cybercrime*). Kasus-kasus kejahatan di Indonesia yang melibatkan aplikasi WhatsApp banyak menjadi rujukan dalam forensika digital. WhatsApp *Group* (WAG) merupakan salah satu	Hasil yang didapat menggunakan metode DFRWS membantu proses akuisisi untuk mengungkap bukti digital pada pelaku di fitur Hasil identifikasi tindakan yang mengarah pada *cyberbullying* didapatkan dengan nilai hasil tertinggi memiliki tingkat *cyberbullying*	• Studi kasus media sosial yang di teliti pada penelitian ini hanya satu yaitu WhatsApp. • Menggunakan *Digital Forensics Research Workshop* (DFRWS).

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
				fitur yang dapat membantu komunitas untuk melakukan komunikasi secara intensif, disisi lain fitur tersebut juga membuka peluang adanya *bully* dalam *group* tersebut.	sebesar 0,05 dan nilai hasil terendah memiliki tingkat *cyberbullying* dengan nilai ISC sebesar 0,02 dari persentase tersebut didapat nilai kata *cyberbulying* pada percakapan terhadap query. Data tersebut membuktikan bahwa metode forensics DFRWS dapat mengangkat barang bukti berupa teks dalam *group* dan metode *Improved Sqrt-Cosine* dapat mengidentifikasi *cyberbullying* seseorang yang akan melakukan tindakan *cyberbullying* dengan tingkat yang berbeda-beda.	
4.	Analisis Media Sosial Facebook Lite dengan *tool* Forensik menggunakan Metode *National Institute of Standards and*	2020	*National Institute of Standards and Technology* (NIST)	Tindakan kejahatan pada media sosial contohnya penipuan jual beli *online* maupun *Cyberbully* atau tindakan merendahkan derajat orang lain. Pada kejehatan digital yang dapat	Hasil dari *scenario* dengan menggunakan Smartphone Android Galaxy J2, dengan melakukan *Rooting*, dan menginstall aplikasi Facebook Lite, Membuat Postingan, dan	• Penelitian ini memiliki objek penelitian yaitu *cybercrime.* • Studi kasus media sosial yang digunakan pada

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
	Technology (NIST) Oleh Rauhulloh Ayatulloh Khomeini Noor Bintang, dkk.			dilakukan melalui platform media sosial Facebook Lite dengan bertujuan untuk kriminal kejahatan dengan melakukan penipuan jual beli *online*, melakukan kegiatan perdagangan narkoba, melakukan jual beli PSK online maupun melakukan tindakan kriminal lainnya.	melakukan proses investigasi menggunakan *tool* Forensik yang bernama MOBILedit Forensik, kemudian melakukan analisis menggunakan *tool forensic* tersebut dan mendapatkan hasil analisis yang akan menjadi barang bukti digital. Hasil yang telah didapatkan dalam penggunaan *tool forensic* berikut yaitu Akun ID, Image, Audio, Video dengan menggunakan suatu metode *National Institute Of Standards Technology* (NIST).	penelitian ini yaitu Facebook Lite. • Menggunakan metode NIST 800-86
5.	Implementasi Metode *Jaccard* pada Analisis Investigasi *Cyberbullying* WhatsApp *Messenger* Menggunakan Kerangka Kerja *National Institute of Standards and*	2020	Metode *Jaccard* dan *National Institute of Standards and Technology* (NIST)	Pengguna aplikasi WhatsApp bertambah sangat pesat, tahun 2015 terdapat 900 juta pengguna dan pada Maret 2020 naik menjadi 2 Miliar pengguna. Data tersebut membuka peluang bagi tindakan *cybercrime* dalam aplikasi WhatsApp.	Berdasarkan hasil analisis dan percobaan pada penelitian yang telah dilakukan membuktikan bahwa metode NIST dapat mempermudah proses investigasi mulai dari pengangkatan barang bukti sampai dengan tahap pelaporan	• Studi kasus media sosial yang di teliti pada penelitian ini hanya satu yaitu WhatsApp. • Pada penelitian ini menggunakan dua metode yaitu Metode

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
	Technology (NIST) Oleh Panggah Widiandana, dkk.			*Cyberbullying* menurut Taskin Tanrikulu (2015) mencakup perilaku teknik relasional berbahaya diarahkan kepada individu, kelompok menggunakan teknologi informasi dan komunikasi. *Cyberbullying* dapat melalui perantara seperti pesan yang mengandung kata-kata negatif, kata-kata yang dapat mengarah pada tindakan bullying seperti abnormal, pengecut, aneh, banci, bodoh, buruk, gila, jelek, khianat, dan munafik.	barang bukti. Metode *Jaccard* mampu mengidentifikasi *bullying* dengan tingkat yang berbeda, nilai presentasi pelaku tertinggi yang didapat yaitu 21% kata teridentifikasi 79% lainnya kata tidak teridentifikasi, dan pelaku dengan nilai terendah yang didapat 13% kata teridentifikasi 87% lainnya kata tidak teridentifikasi. Perhitungan menggunakan aplikasi dan perhitungan secara manual didapatkan kesamaan 100%.	*Jaccard* dan *National Institute of Standards and Technology* (NIST) versi 800-86.
6.	*Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology* (NIST)	2019	*National Institute of Standard and Technology* (NIST) versi 800-	Aplikasi Whatsapp adalah alternatif untuk bertukar pesan karena kemudahan penggunaannya. Itu jumlah pengguna dan fitur keamanan WhatsApp adalah tersedia, memungkinkan	Penelitian ini berhasil mendapatkan bukti artefak berupa eksplorasi laporan data ponsel cerdas seperti sesi obrolan, avatar, kontak di aplikasi whatsapp, status on whatsapp, dan juga	• Penelitian ini memiliki objek penelitian yaitu kejahatan pada WhatsApp. • Studi kasus media sosial yang di teliti pada

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
	Framework Oleh Vindy Arista Yuliani, dan Imam Riadi.		101	WhatsApp untuk digunakan sebagai media komunikasi untuk tujuan kriminal seperti: penipuan jual beli online, teroris kegiatan, perencanaan pembunuhan, dan kriminal lainnya kegiatan.	mendapatkan file media whatsapp dan file database cadangan terenkripsi	penelitian ini hanya satu yaitu WhatsApp. • Menggunakan *tool* oxygen forensic dan andriller.
7.	Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ) Oleh Imam Riadi, dkk.	2018	*National Institute Of Justice* (NIJ)	Aktivitas yang dapat dilakukan pada fitur Instagram Messenger yakni melakukan komunikasi antar sesama pengguna dalam bentuk pesan teks percakapan (*Chatting*) dan dapat juga membagikan gambar atau foto ke sesama pengguna Instagram. Hal ini bisa berdampak negatif pada penggunaan Instagram Messenger karena dapat memberikan peluang penyalagunaan fitur ini untuk melakukan suatu tindak kejahatan yang paling berpotensi adalah *cybercrime* khususnya kejahatan *cyberbullying*, untuk	Penelitian yang dilakukan untuk mendapatkan barang bukti digital dari sebuah *smartphone* yang menjadi barang bukti elektronik dari kejahatan yang terindikasi *cyberbullying*. Proses akuisisi data menggunakan metode *National Institute Of Justice* (NIJ) yang merekomendasikan beberapa macam tahapan seperti persiapan, koleksi, pemeriksaan, analisis dan pelaporan. Proses akuisisi yang dilakukan menggunakan aplikasi OXYGEN forensik sehingga mendapatkan hasil	• Menggunakan *tools* OXYGEN forensik. • Menggunakan metode *National Institute Of Justice (NIJ).*

No.	Judul	Tahun	Metode	Masalah	Hasil	Perbedaan dengan penelitian yang dilakukan
				mengatasi kejahatan tersebut maka perlunya suatu analisis dan metode forensik agar dapat membantu menyelesaikan kejahatan *cyberbullying* yang terjadi pada sosial media Instagram.	sesuai dengan yang diinginkan yakni barang bukti digital berupa gambar/foto dan percakapan/*chatting* dari sosial media Instagram yang terpasang pada *smartphone* tersebut. Proses akuisisi barang bukti digital yang berhasil didapatkan pada Instagram pada *smartphone* dalam kondisi Root didapatkan data yang diharapkan yakni berupa gambar/foto dan percakapan/ *chatting* sedangkan untuk *smartphone* tidak dalam kondisi Root tidak didapatkan barang bukti digital	

2.2 Dasar Teori

2.2.1 Digital Forensik

Ilmu forensik adalah bidang yang sangat luas karena ilmu pengetahuan apapun yang digunakan untuk membantu menyelesaikan masalah atau kasus hukum dapat menikmati kata sifat 'forensik' dalam konteks seperti itu (Robertson, 2002). Forensik adalah penerapan ilmu pengetahuan untuk hukum pidana dan perdata, terutama - pada sisi kriminal selama penyelidikan pidana, sebagaimana diatur oleh standar hukum bukti yang dapat diterima dan prosedur pidana. Forensik juga berarti bidang pengetahuan yang digunakan untuk membantu proses menegakkan keadilan. Digital forensik memiliki arti adalah cabang ilmu forensik yang membahas pemulihan dan investigasi materi yang terkandung dalam perangkat digital, yang terkait dengan kejahatan komputer [18]. Digital forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat dipertanggungjawabkan secara hukum [19].

2.2.2 Mobile Forensics

Digital forensik memiliki banyak cabang diantaranya adalah *mobile forensics*. *Mobile Forensics* adalah ilmu yang melakukan proses memulihkan bukti digital dari perangkat seluler menggunakan metode yang sesuai dengan kondisi forensik [20]. Penggunaan mobile seperti *smartphone* dengan berbagai macam tipe dan sistem operasi untuk kejahatan sudah semakin tinggi jumlahnya, tetapi dengan adanya forensik untuk perangkat mobile dapat membantu untuk mengatasi kasus kejahatan yang berhubungan dengan perangkat mobile khususnya *smartphone* [17].

2.2.3 Cyberbullying

Cyberbullying merupakan bentuk baru dari *bullying* yang biasa dialami di dunia nyata namun dengan karakteristik dan efek yang sama. *Cyberbullying* mencakup perilaku teknik relasional berbahaya diarahkan kepada individu,

kelompok menggunakan teknologi informasi dan komunikasi. *Cyberbullying* tidak hanya dilakukan oleh perorangan, namun bisa jadi dilakukan oleh kelompok atau institusi, baik resmi atau tidak. Dibandingkan di dunia nyata (*offline*), *cyberbullying* di dunia maya menjadi mudah dilakukan dan cenderung aman karena menyembunyikan identitas asli. Artinya, perangkat media siber memungkinkan seseorang untuk membangun identitas lain (*anonymous*) atau relitas diri palsu sehingga pengguna lain tidak mengetahui identitas sebenarnya[2] .

Cyberbullying yang berkepanjangan bisa mematikan rasa percaya diri anak, membuat anak menjadi murung, khawatir, selalu merasa bersalah atau gagal karena tidak mampu mengatasi sendiri gangguan yang menimpanya. Bahkan ada pula korban *Cyberbullying* yang berpikir untuk mengakhiri hidupnya karena tak tahan lagi diganggu. Motivasi pelaku *cyberbullying* beragam, ada yang melakukannya karena marah dan ingin balas dendam, frustrasi, ingin mencari perhatian bahkan ada pula yang menjadikannya sekedar hiburan pengisi waktu luang [21].

Willard dalam bukunya Novan Ardy Wiyani yang berjudul *Save Our Children From School Bullying*, menyebutkan macam-macam jenis *cyberbullying* sebagai berikut [8] :

1. *Flaming* (pertengkaran) : Mengirimkan pesan teks yang isinya merupakan kata-kata yang penuh amarah dan frontal. Istilah “flame” ini pun merujuk pada kata-kata di pesan yang berapi-api.
   Contoh : Orang berdebat dan ngomong kasar di kolom komentar.
2. *Harassment* (pelecehan) : Pesan yang buruk, kejam dan menghina di jejaring sosial dilakukan secara terus menerus.
   Contoh : Mengejek seseorang dengan pesan buruk berulang-ulang.
3. *Denigration* (pencemaran nama baik) : Proses mengumbar keburukan seseorang di internet dengan maksud merusak relasi, reputasi dan nama baik orang tersebut.
   Contoh : Akun-akun gosip yang sering membawakan berita palsu seseorang.
4. *Impersonation* (peniruan) : Berpura-pura menjadi orang lain dan mengirim atau memuat sesuatu yang dapat membuat orang lain berada dalam masalah atau merusak reputasi atau relasinya.

Contoh : Akun palsu (*fake*) yang berisi postingan buruk.

5. *Outing* (penyebaran) : Menyebarkan rahasia, informasi atau gambar orang lain secara *online*.

   Contoh : Membagikan atau menyebarkan luaskan foto memalukan orang lain.

6. *Trickery* (tipu daya) : Tindakan membujuk seseorang dengan tipu daya agar mendapatkan rahasia atau foto pribadi orang tersebut. Berawal dengan berbicara sama orang lain, kemudian mengungkap rahasia atau informasi memalukan miliknya tanpa izin.

   Contoh : Mengirim *screenshot* curhatan seseorang.

7. *Exclusion* (pengucilan) : Pengabaian secara sengaja dan kejam kepada orang lain dalam satu forum *online.*

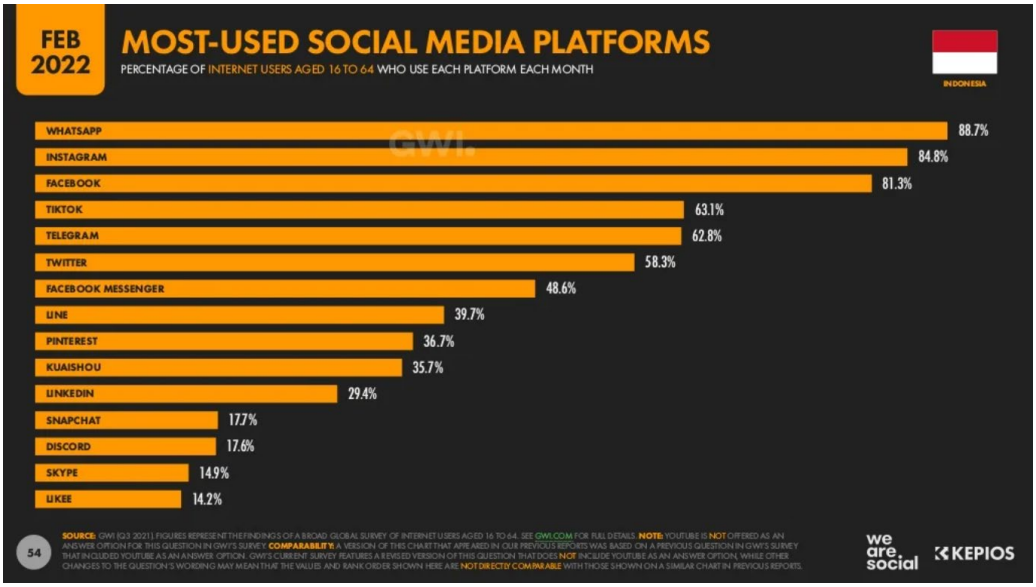
   Contoh : Sengaja hanya membaca diskusi/ pendapat seseorang dalam forum *online*.

8. *Cyberstalking* (penguntitan): penguntitan atau pelecehan kepada seseorang secara intens dan berulang sehingga menimbulkan rasa takut.

   Contoh Menguntit akun media sosial seseorang, lalu mengancam orang tersebut dengan hasil *stalking*-annya [8].

2.2.4 Media sosial

Media sosial termasuk kedalam salah satu sarana teknologi informasi dan komunikasi sangat di gemari oleh masyarakat di dunia. Riset terbaru dari *Hootsuite (We Are Social)* menyebut bahwa hingga bulan Februari 2022, jumlah pengguna media sosial yang aktif di dunia telah mencapai 4,62 milyar orang (58,4 persen dari jumlah populasi di dunia), sedangkan untuk di Indonesia jumlah pengguna media sosial yang aktif telah mencapai 191,4 juta orang, jumlah tersebut meningkat 12,6 persen dari tahun 2021 yang berjumlah 170 juta orang. Jumlah pengguna media sosial aktif di Indonesia menjadi 68.9 persen dari total populasi Indonesia pada tahun 2022 yang sebesar 277,7 juta orang. Banyaknya pengguna media sosial aktif ini kemungkinan besar dapat menimbulkan beberapa kasus *cyberbullying* di dunia ataupun di Indonesia [5].



Gambar 2. 1 *Presentase platforms* media sosial yang sering digunakan di Indonesia [5]

Riset dari *Hootsuite* dan *We Are Social* menyebutkan juga *platforms* media sosial yang sering digunakan di Indonesia. Pada gambar 2.1 menunjukkan bahwa WhatsApp menduduki peringkat pertama sebesar 88.7 persen, sedangkan peringkat kedua diduduki oleh Instagram sebesar 84.8 persen [5].

a. Instagram

Instagram merupakan sebuah aplikasi layanan berbagi foto yang memungkinkan pengguna untuk mengambil foto, menerapkan filter digital dan membagikannya ke berbagai layanan jejaring sosial. Sistem sosial di Instagram adalah dengan mengikuti akun pengguna lainnya, atau memiliki pengikut Instagram. Dengan demikian komunikasi antara sesama pengguna Instagram dapat terjalin dengan memberikan tanda suka dan mengomentari foto yang telah diunggah oleh pengguna lainnya. Instagram juga dapat menampilkan video dengan durasi yang cukup lama dan dipenuhi fitur pelengkap lainnya [14].

Instagram secara resmi mengumumkan peluncuran fitur resmi bernama Instagram Messenger pada tahun 2013, fitur ini menyerupai *Instant Messaging* atau pesan singkat yang ada pada sosial media seperti whatsapp dan lainnya. Satu hal yang kurang dimiliki media sosial Instagram yakni kemampuan untuk menjaga

percakapan bersifat pribadi dengan satu orang atau kelompok kecil sesama pengguna Instagram, maka fitur Instagram *Messenger* ini merupakan fitur yang dikembangkan oleh media sosial Instagram untuk memberikan keamanan kepada penggunanya dalam melakukan komunikasi yang lebih bersifat pribadi. Aktivitas yang dapat dilakukan pada fitur Instagram *Messenger* yakni melakukan komunikasi antar sesama pengguna dalam bentuk pesan tesk percakapan (*Chatting*) dan dapat juga membagikan gambar atau foto ke sesama pengguna Instagram. Hal ini bisa berdampak negatif pada penggunaan Instagram *Messenger* karena dapat memberikan peluang penyalagunaan fitur ini untuk melakukan suatu tindak kejahatan yang paling berpotensi adalah *cybercrime* khususnya kejahatan *cyberbullying* [17].

b. WhatsApp

WhatsApp adalah sebuah aplikasi layanan pesan cepat lintas *platform* untuk smartphone yang mengandalkan internet untuk pengiriman pesan. Berdasarkan model berlangganan berbiaya rendah, WhatsApp adalah alternatif yang murah untuk mengirim pesan teks melalui SMS, terutama untuk pesan internasional atau grup. Aplikasi perpesanan *mobile* memungkinkan pengguna berbagi pesan teks, gambar dan video. Aplikasi WhatsApp *Messenger* menggunakan koneksi data mobile serta WiFi untuk melangsungkan komunikasi data, dengan menggunakan WhatsApp, seseorang dapat melakukan obrolan online, berbagi file, bertukar foto dan fitur lainnya yang menarik penggunanya [22].

2.2.5 National Institute Of Standard And Technology (NIST)

National Institute of Standards and Technology (NIST) merupakan metode yang digunakan untuk melakukan forensik analisis [23]. Metode berikut menjelaskan bagaimana alur tahapan penelitian sehingga dapat dilakukan suatu langkah penelitian secara terstruktur agar dapat digunakan untuk pedoman dalam menyelesaikan suatu persoalan yang ada [12].

Pada penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST) dengan panduan *Special Publication 800-101 Revision 1* yang berjudul "*Guidelines on Mobile Device Forensics*" diterbitkan pada tahun 2014.

Panduan tersebut khusus untuk forensik perangkat seluler (*mobile*). Panduan ini berfungsi untuk menjembatani kesenjangan dengan memberikan pandangan mendalam ke perangkat seluler dan menjelaskan teknologi yang terlibat dan hubungannya dengan prosedur forensik [24]. Berikut tahapan dari metode NIST *Special Publication 800-101 Revision 1*, yaitu:

Gambar 2. 2 Tahapan Metode NIST Special Publication 800-101 Revision 1.

Penjelasan dari tahapan metode NIST adalah sebagai berikut :

a. Preservation

Tahap awal adalah tahap *preservation* atau penjagaan. Dalam tahap ini dilakukan penjagaan pada perangkat yang menjadi kebutuhan untuk melakukan proses analisa forensik [13], seperti mempersiapkan barang bukti yang akan dianalisa, mengamankan perangkat seluler yang akan diinvestigasi dan mempersiapkan peralatan dokumentasi [25]. Tahap *preservation* melibatkan pencarian, pengenalan, dokumentasi dan pengumpulan barang bukti berbasis elektronik. Berdasarkan NIST *Special Publication 800-101 Revision 1*, ini adalah langkah pertama dalam pemulihan digital [24].

b. Acquisition

Tahap *acquisition* atau akusisi data, adalah proses *imaging* atau pengkloningan terhadap perangkat seluler yang menjadi barang bukti [26]. Tujuan dari proses ini adalah untuk melindungi keutuhan dari barang bukti, sehingga dapat melakukan pemeriksaan lebih lanjut dengan baik terhadap barang bukti tersebut [13].

c. Examination & Analysis

Tahap ini adalah tahap *examination* dan *analysis* dilakukan. Tahap *examination* atau pemeriksaan data, proses ini diperlukan untuk mengungkap bukti digital, termasuk yang mungkin disembunyikan atau dikaburkan. Selain itu, tahap

ini berguna untuk mengidentifikasi keterkaitan suatu barang bukti dengan kasus yang sedang ditangani [13]. Kemudian tahap Analysis atau analisis data, setelah dilakukan pemeriksaan maka hasil pemeriksaan akan dikumpulkan untuk dilakukan proses Analisa secara detail dan komprehensif dengan menggunakan metode yang dibenarkan secara teknik dan hukum [27], sehingga dapat ditarik kesimpulan data yang diinginkan berkaitan dengan kasus penyidikan [26].

d. Reporting

Tahap terakhir adalah tahap *reporting* atau tahap pelaporan, digunakan untuk melaporkan hasil analisis dan kesimpulan yang didapatkan dalam penyelidikan suatu kasus [24]. Tahap ini mencakup deskripsi tindakan yang digunakan, menjelaskan alat dan prosedur yang dipilih, dan menentukan tindakan lanjutan jika diperlukan [28].

2.2.6 Smartphone

Smartphone memiliki perkembangan teknologi yang sangat pesat yang mana dahulu hanya dapat digunakan untuk berkomunikasi via suara maupun pesan singkat (*Short Message Service*). *Smartphone* kini telah berkembang dengan fitur yang disesuaikan dengan perkembangan zaman dan kebutuhan dari penggunanya. Teknologi *smartphone* android tersebut memberikan peluang bagi pengembang aplikasi untuk meluaskan penggunaan aplikasi khususnya sosial media Instagram dan WhatsApp di sistem operasi Android [17].

2.2.7 MOBILedit Forensic

MOBILedit Forensic adalah pengekstrak ponsel, penganalisis data, dan pembuat laporan semuanya dalam satu solusi. Sebuah aplikasi 64-bit yang kuat menggunakan metode akuisisi data fisik dan logis. MOBILedit sangat bagus untuk penganalisis aplikasi tingkat lanjut, pemulihan data yang dihapus, pembaruan langsung, berbagai ponsel yang didukung termasuk sebagian besar ponsel berfitur, laporan yang disesuaikan, pemrosesan ponsel secara bersamaan, dan antarmuka pengguna yang mudah digunakan. MOBILedit Forensic banyak digunakan oleh para profesional di bidang penegakan hukum, militer serta di sektor perusahaan dan

swasta. Dengan menghubungkan telepon melalui kabel USB, Wi-Fi atau Bluetooth, dapat melakukan pemeriksaan individual pada sebagian besar perangkat seluler dan menghasilkan laporan dalam berbagai format (PDF, HTML, Excel, dll.) untuk berbagai kebutuhan. MOBILedit Forensic dapat mengekstrak semua data dari ponsel termasuk data yang dihapus, riwayat panggilan, kontak, pesan teks, pesan multimedia, foto, video, rekaman, item kalender, pengingat, catatan, file data, kata sandi, dan data dari aplikasi seperti Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Sinyal, WeChat, dan banyak lainnya [29].

2.2.8 Autopsy

Autopsy adalah aplikasi yang dapat mengetahui informasi-informasi tersembunyi dari suatu file, mulai dari kapan file itu dibuat, kapan file itu terakhir kali dirubah, kapan file terakhir kali di akses, kapan file itu di hapus, aplikasi ini menggunakan enskripsi apa, dan passwordnya apa. Aplikasi ini menyediakan alur kerja yang intuitif untuk pengguna di penegakan hukum, militer, agen intelijen, keamanan *cyber* dan pemeriksa perusahaan. Aplikasi ini hanya membutuhkan *disk image* dari perangkat yang akan dianalisis [30].

2.2.9 Access Data FTK Imager

Access Data Forensic Tool Kit Imager atau biasa disebut “AD FTK Imager” merupakan salah satu aplikasi yang digunakan dalam dunia forensik digital untuk melakukan sistem akuisisi data yang dikembangkan oleh perusahaan Access Data. Dimana sistem akuisisi itu sendiri merupakan suatu sistem yang berfungsi untuk mengambil, mengumpulkan dan menyiapkan data, hingga memprosesnya untuk menghasilkan data yang dikehendaki [14].