BAB II
TINJAUAN PUSTAKA

A. Landasan Teori

1. Keamanan Siber (*Cyber Security*)

a. Definisi Keamanan Siber

Menurut Aji (2023), definisi keamanan siber merupakan sebuah rangkaian tindakan yang memiliki arti untuk melindungi sistem dari ancaman, gangguan, serta serangan terhadap jaringan komputer, baik dari sisi perangkat keras ataupun perangkat lunak, terkait informasi yang ada didalamnya serta hal lainnya dalam ruang siber. Selain itu keamanan siber juga memiliki tugas dalam mencegah dan melindungi dari pengawasan yang tidak di harapkan, seperti aktivitas intelijen. Oleh karena itu, keamanan siber mencakup berbagai mekanisme perlindungan yang dirancang untuk mengurangi risiko gangguan terhadap ketersediaan, integritas, dan kerahasiaan suatu informasi.

b. Ancaman keamanan siber

Keamanan siber menghadapi berbagai macam ancaman yang semakin canggih dengan adanya kemajuan dan perkembangan seiring digitalisasi ini, salah satu ancaman tersebut adalah *ramsomware*, *malware* yang mengenkripsi file dan meminta bayaran dari perilaku tersebut untuk memberikan pemulihan. Selain itu, *Advance Persistent Threat* (APT) adalah serangan canggih yang berlangsung lama untuk melakukan pencurian data *privat* tanpa terdeteksi. Kebocoran data (*data breach*) juga menjadi masalah serius, seperti disebabkan oleh adanya celah keamanan atau serangan *phishing*, di mana pelaku mengelabui korban agar memberikan informasi pribadi. Ancaman lain pada keamanan siber adalah web defacement, yang mengubah tampilan situs aplikasi atau website dengan mengekspoitasi kelemahan pada sistem, adapula serangan bruteforce, di mana penyerang mencoba berbagai kombinasi kata sandi untuk

mendapatkan akses yang tidak resmi atau illegal. malware dan botnet juga menjadi salah satu ancaman, di mana perangkat yang telah diretas digunakan untuk aktivitas illegal seperti serangan DDoS (it.telkomuniversity.ac.id, 2023).

2. Forensik Digital

Menurut Hariyadi *et al.* (2023), forensik digital adalah bidang ilmu yang berfokus pada pemeriksaan barang bukti elektronik atau digital dengan tujuan mengidentifikasi serta mengungkap fakta sebagai bagian dari Upaya penegakan hukum atau peraturan yang berlaku. Metode ini menggunakan pendekatan ilmiah untuk menginvestigasi bukti digital guna mendukung penyelesaian suatu permasalahan yang kompleks serta memastikan kepatuhan terhadap regulasi yang berlaku.

Menurut Carroll *et al.* (2008), forensik digital merupakan penggunaan metode yang telah dibuktikan secara ilmiah untuk menangani bukti digital dengan maksud mendukung investigasi suatu kejadian, terutama yang berkaitan dengan Tindakan kejahatan digital. Proses pada forensik digital mencakup pelestarian, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi, dan penyajian bukti digital yang berasal dari berbagai penyedia. Tujuan pokoknya adalah merekonstruksi kejadian yang terjadi serta memberikan informasi yang dapat digunakan pada proses penegakan hukum.

Pengertian dari Fitriana *et al.* (2020) tentang forensik digital, yaitu ilmu yang membahas atau menjelaskan tentang temuan bukti digital setelah terjadi insiden yang berkaitan dengan keamanan komputer. Forensik digital juga adalah penerapan ilmu pengetahuan yang bertujuan memulihkan dan mengumpulkan bukti digital dari perangkat seperti komputer, smartphone atau perangkat lainnya dengan metode tertentu, sehingga data yang diperoleh dapat digunakan sebagai alat bukti yang sah di pengadilan.

3. Autopsy (perangkat lunak forensik digital)

a. Definisi dan fungsi Autopsy

Menurut Rosita (2023), autopsy merupakan sebuah perangkat lunak forensik sumber terbuka (*open source*) yang digunakan untuk menganalisis perangkat lunak, perangkat keras, serta data digital. Dikembangkan oleh basis technology corp dan terus diperbarui oleh komunitas pengembang terbuka, autopsy dapat dijalankan pada berbagai sistem operasi diantaranya windows, linux, dan MacOS. Perangkat lunak ini sangat membantu bagi professional forensik, seperti penegak hukum, tim investigasi keamanan siber, maupun individu yang ingin melakukan analisis forensik terhadap data digital. Selain itu, autopsy mendukung berbagai plugin yang memungkinkan pengguna memperluas fungsinya sesuai dengan kebutuhan seperti untuk pemulihan data yang telah hilang dalam investigasi forensik tersebut.

b. Fitur autopsy dalam investigasi

Autopsy memiliki berbagai fitur yang mendukung analisis forensik digital, seperti pemulihan data untuk mengembalikan file yang telah dihapus, memungkinkan penyidik menemukan informasi yang seharusnya tidak dapat diakses. Selain itu, perangkat lunak ini dapat menganalisis metadata file, sehingga informasi penting seperti tanggal pembuatan, jenis file, dan perubahan yang dilakukan dapat diketahui. Autopsy juga dilengkapi dengan kemampuan pencarian dan pengumpulan data yang efektif, membantu penyidik menemukan informasi relevan dalam media digital. Fitur visualisasi data mempermudah pemahaman struktur serta hubungan antara berbagai jenis data yang ditemukan, sementara fungsi pelaporan memungkinkan pembuatan laporan terperinci yang dapat digunakan sebagai bukti dalam proses hukum. Selain itu, Autopsy mendukung analisis jaringan dan komunikasi digital, memberikan wawasan lebih dalam untuk keperluan investigasi (Badri, 2023; Dasmen *et al.*, 2024).

4. Server dan virtual server

a. Server

Menurut Yulvianda dan Ismail (2023), server merupakan sistem komputer yang memiliki peran untuk pusat layanan utama dalam suatu jaringan, dimana perangkat ini mampu menyimpan, mengelola, dan mendistribusikan berbagai sumber daya, seperti data, aplikasi, serta layanan khusus lainnya, sehingga memungkinkan pengguna untuk mengakses informasi secara mudah dan terorganisir. Selain itu, server memiliki fungsi penting dalam menjaga kelancaran operasional sistem dengan menyediakan dukungan terhadap berbagai kebutuhan komputasi, termasuk menyimpan data dalam jumlah besar, pemrosesan traksaksi secara real time, serta pengelolaan komunikasi antar perangkat dalam lingkungan digital yang semakin maju. Seiring dengan adanya kemajuan teknologi, server saat ini menjadi bagian utama dalam infrastruktur jaringan, baik dalam skala kecil seperti perusahaan maupun dalam skala besar seperti pusat data global, yang beroperasi secara terus-menerus guna mendukung berbagai aktivitas digital yang terus meningkat dari waktu ke waktu.

b. Virtual Server

Firmansyah dan Riadi (2014), menjelaskan bahwa Virtual server merupakan sistem komputer berbasis perangkat lunak yang memungkinkan untuk mengerjakan beberapa sistem operasi di atas sistem operasi inti, memungkinkan juga bagi pengguna mengoperasikan aplikasi yang didesain untuk sistem operasi lain. Dengan menggunakan teknologi virtualisasi, virtual server membuat sebuah lingkungan sistem yang terisolasi, di mana setiap sistem operasi yang bekerja tidak memiliki keterkaitan langsung dengan sistem operasi inti, sehingga memberikan fleksibilitas dalam pengelolaan sumber daya dan kompatibilitas lintas platform.

5. VirtualBox

Menurut Zhang (2015), VirtualBox merupakan sebuah perangkat lunak virtualisasi sumber terbuka (*open Source*) yang memiliki sifat lintas platform. Perangkat lunak dengan fungsi seperti VirtualBox disebut sebagai perangkat lunak mesin virtual, sedangkan program utama yang mengelola mesin virtual disebut sebagai manajer mesin virtual. Karena pengguna biasanya hanya berinteraksi dengan manajer mesin virtual ini, maka sering kali perangkat lunak ini juga dianggap sebagai perangkat lunak mesin virtual (antarmuka perangkat lunak). VirtualBox awalnya dikembangkan oleh perusahaan Jerman Innotek dan diterbitkan oleh Sun Microsystems. Setelah Sun diakuisisi oleh Oracle, perangkat lunak ini secara resmi berganti nama menjadi Oracle VM VirtualBox, yang sekarang dikelola dan diperbarui oleh Oracle sebagai bagian dari teknologi platform virtualisasi Oracle xVM.

6. Investigasi log dalam forensik digital

a. Definisi Log

Menurut Aji (2022) dan Ariana (2016), log adalah sebuah catatan yang memiliki informasi tentang peristiwa yang terjadi dalam sistem dan jaringan organisasi. Log dihasilkan dari berbagai event pada sistem operasi, aplikasi, serta pesan yang dihasilkan oleh dua pengguna yang berbeda dalam aplikasi komunikasi, sehingga berperan penting dalam pemantauan dan analisis keamanan.

b. Jenis jenis log

Menurut Yogi *et al.* (2019), Dalam proses memonitor kegiatan web server, terdapat tiga jenis log utama yang harus diperhatikan. Log ini berperan penting dalam mencatat berbagai aktivitas yang terjadi pada server, membantu dalam analisis performa, deteksi masalah, serta upaya peningkatan keamanan sistem. Tiga log yang perlu diperhatikan yaitu terdapat access log, server log, dan error log. access log memiliki fungsi untuk mencatat semua akses yang dilakukan terhadap web server, sehingga dapat dipergunakan untuk menganalisis

kegiatan pengguna. Server log mencatat kejadian-kejadian tertentu pada web server, namun file ini biasanya hanya diperiksa ketika terjadi kesalahan pada server. Sementara itu, error log berperan dalam mencatat setiap kesalahan yang terjadi pada web server, baik kesalahan pada file konfigurasi maupun pada proses pembuatan website, sehingga membantu dalam identifikasi dan perbaikan masalah.

7. Protokol Keamanan SSH

   a. Pengertian SSH

      Menurut Desmira & Wiryadinata (2022), SSH atau *Secure Shell* merupakan protokol keamanan jaringan yang digunakan untuk mengirimkan data secara aman antara dua perangkat dalam suatu jaringan. Protokol keamanan jaringan ini terutama digunakan pada sistem berbasis linux dan unix untuk mengakses shell secara remote. SSH dikembangkan sebagai alternatif yang lebih aman dibandingkan telnet dan protokol remote shell lainnya, yang mengirimkan informasi terutama kata sandi dalam bentuk teks biasa sehingga rentan terhadap penyadapan.

   b. Kegunaan SSH

      Pengertian dari Jusuf (2015), SSH digunakan untuk mengendalikan komputer dari jarak yang tidak dekat, mengirimkan file, serta membuat terowongan terenkripsi dan fungsi lainnya. Port forwarding dalam SSH memungkinkan konversi koneksi TCP yang tidak aman menjadi koneksi yang terenkripsi, sehingga dapat mengalihkan koneksi dari satu IP ke IP lainnya, dengan demikian, klien seolah-olah tersambung langsung kepada IP tujuan. Nelalui SSH, port forwarding menciptakan koneksi yang aman antara komputer lokal dan komputer remote, memastikan perpindahan data yang terenkripsi.

B. Penelitian Terdahulu

1. Penelitian yang dilakukan oleh Latif *et al*. (2021)**,** memberikan kontribusi penting dalam bidang forensik digital, khususnya terkait dengan analisis aplikasi komunikasi yang populer seperti whatsapp. Di tengah peningkatan yang jelas pada penggunaan smartphone di indonesia, serta dominasi penggunaan platform media sosial, terdapat kebutuhan mendesak untuk mengembangkan metodologi yang efektif dalam penyelidikan digital. Dengan pertimbangan, penelitian ini bertujuan untuk melakukan eksplorasi penerapan metode *Association of Chief Police Officers* (ACPO) dalam konteks live forensik digital untuk analisis di perangkat simulator android, yaitu pada bluestacks. Penelitian ini menyusun kerangka kerja yang terstruktur berdasarkan metode ACPO dengan 4 tahapan yang terdiri dari *plan* (perencanaan), *capture* (pengambilan bukti), *analysis* (analisis), *dan present* (presentasi). Pada tahap capture, teknik live forensik digunakan untuk mengumpulkan bukti dari aplikasi whatsapp yang berjalan di BlueStacks. Hasil penelitian ini membuktikan dengan mengikuti standarisasi ACPO, proses pengolahan bukti digital dapat dilakukan dengan cara yang sistematis dan terjamin keasliannya. Informasi yang diperoleh tidak hanya pasti, tetapi juga diberikan secara jelas menggunakan aplikasi WhatsApp viewer, yang memberikan kemudahan dalam pemahaman kepada hasil analisis dan laporan data.
2. Sunde (2022) melakukan penelitian yang berfokus terhadap objektivitas pemeriksa dan kepastian bukti dalam forensik digital melalui survei terhadap banyak partisi, dalam konteks forensik digital, di mana perangkat digital dapat menyimpan informasi yang pasti untuk investigasi, penting untuk memastikan bahwa proses analisis dilakukan dengan objektivitas dan teliti. Penelitian ini menyoroti beberapa temuan yang menunjukan tentang bagaimana para praktisi menangani hipotesis dan informasi kontekstual sebelum dan sesudah analisis. Salah satu temuan penting adalah bahwa 45% dari praktisi yang disurvei tidak memulai analisis dengan hipotesis tidak bersalah. Selain itu, 34% praktik tidak menerapkan

teknik untuk mempertahankan objektivitas, dan 38% tidak menggunakan teknik untuk menguji atau mengontrol keandalan bukti. Penelitian ini menggarisbawahi bahwa kesalahan dari analisis forensik sering terjadi dari bias teknik maupun non-teknis, yang dapat mengarah pada kesimpulan yang salah. Pentingnya memastikan dengan menggunakan alat ganda muncul sebagai cara utama untuk memastikan keaslian bukti.penelitian ini menggunakan prinsip bahwa setiap orang dianggap tidak bersalah hingga terbukti sebaliknya. Ini berarti bahwa setidaknya satu hipotesis dibuat oleh para praktisi harus mencakup kemungkinan bahwa orang tersebut tidak bersalah. Meskipun para praktisi menyadari adanya risiko bias dalam analisis mereka, hanya 34% dari mereka yang mengaplikasikan teknik untuk tetap objektif. Temuan ini sangat penting untuk memahami praktik di bidang forensik digital, dan menunjukkan bahwa ada kebutuhan untuk mengembangkan prosedur yang lebih baik dalam mengurangi kesalahan dan meningkatkan manajemen kualitas. Dengan mengetahui cara para praktisi mengelola informasi yang ada dan menjaga objektivitas serta keaslian selama analisis, penelitian ini memberikan pandangan berharga untuk praktik forensik.

3. Dalam penelitian yang dilakukan oleh Aji (2022), membahas tentang cara hacker melakukan serangan *Brute Force* terhadap web server Nginx dengan memanfaatkan metode investigasi forensik untuk melakukan analisis log serangan yang dihasilkan, serta menggunakan Wazuh sebagai alat pemantauan untuk membangun dan memperbarui sistem dasbor monitoring website, metode investigasi forensik kuantitatif yang memiliki 5 tahapan yaitu identifikasi, problem scope, pengumpulan pemeriksaan, analisis, dan presentasi digunakan dalam penelitian ini untuk menganalisis log yang dihasilkan dasbor sistem. Fokus pada analisis log dalam penelitian ini memberikan pengatahuan tentang pola dan karakteristik serangan, sehingga membantu administrator dalam melakukan Tindakan mitigasi yang lebih tepat. Pada penelitian ini memberikan saran untuk peneliti selanjutnya dengan mengusulkan metode baru dengan irisan

keilmuan mengenai investigasi forensik dan cyber security atau metode investigasi forensik yang berbeda.

4. Achmad dan Muntasiroh (2024) melakukan penelitian yang berfokus pada forensik digital sebagai alat penting dalam investigasi pasca kejadian serangan siber, dengan berfokus khusus pada analisis serangan Denial of Service (DoS) dan Brute force. Dalam penelitian ini, tim investigasi menggunakan metode analisis jaringan dengan alat seperti Wireshark, yang bertujuan untuk mengamati atau mengawasi lalu lintas data dan mendeteksi anomali yang menunjukan adanya serangan. Hasil dari pembelajaran ini menunjukan identifikasi beberapa varian serangan DoS, seperti SYN Flood, UDP Flood, dan DNS Amplification, serta bukti pasti dari serangan *Brute Force* yang di kelompokan sebagai Hybrid Attack, yaitu kombinasi dari dictionary attack dan brute force. Meskipun penelitian ini memberikan hasil yang signifikan dalam hal mendeteksi serangan dan menunjukkan beragam teknik yang digunakan oleh penyerang, tim juga menghadapi kendala seperti keterbatasan perangkat keras dan waktu yang membatasi kedalaman analisis. Ketidakmampuan untuk mendeteksi aktivitas malware selama investigasi menjadi area yang menarik dan relevan, menyoroti pentingnya penggunaan alat dan teknik yang lebih canggih untuk memastikan semua potensi ancaman dapat diidentifikasi. Dengan demikian, studi ini tidak hanya memberikan kontribusi terhadap pemahaman tentang serangan siber yang umum terjadi, tetapi juga menggarisbawahi kebutuhan untuk penguatan infrastruktur dan sumber daya yang mendukung proses investigasi forensik yang lebih efektif. Temuan ini menjadi landasan penting bagi penelitian lebih lanjut, termasuk studi ini yang berfokus pada digital forensik dalam konteks simulasi serangan *Brute Force* terhadap server virtual, berusaha untuk mengimplementasikan temuan sebelumnya dan memperluas teknik analisis forensik dalam lingkungan yang terstandarisasi.

5. Dalam penelitian sebelumnya yang dilakukan oleh Rahman (2019), penelitian ini secara komprehensif mengeksporasi metode logika fuzzy dalam konteks analisis forensik untuk mendeteksi dan membuktikan serangan *Brute Force* pada sebuah sistem cloud publik. Penelitian ini menjadikan tanda perkembangan dalam teknologi cloud sebagai latar belakang, sekaligus menyoroti masalah serta tantangan keamanan yang dihadapi oleh infrastruktur cloud, terutama dengan adanya peningkatan serangan cyber yang semakin canggih dan tertata. Penelitian ini mengemukakan pentingnya pemahaman mengenai karakteristik dari serangan brute force, yang dimana serangan tersebut merupakan metode serangan yang mencoba semua kombinasi kemungkinan kata sandi untuk mendapatkan akses ke sistem. Dalam pembahasannya, penelitian ini menyebutkan hasil yang tertuju bahwa serangan *Brute Force* memiliki kemungkinan berhasil yang tinggi apabila terdapat jumlah kemungkinan kata sandi yang besar, meskipun estimasi waktu yang diperlukan dalam melakukan Tindakan ini juga akan meningkat seiring dengan kompleksitas kata sandi yang dituju. Penelitian ini tidak hanya tertuju pada pembahasan tentang masalah teknis yang dihadapi saat mengidentifikasi serangan, tetapi juga memberikan bayangan tentang metodologis yang jelas tentang bagaimana logika fuzzy dapat diimplementasikan analisis data forensik. Penelitian ini juga menjelaskan secara rinci tahapan-tahapan yang dilakukan dalam penelitian ini, mulai dari perumusan masalah yang berfokus pada keamanan cloud, pengumpulan referensi ilmiah, hingga Langkah-langkah pengujian yang meliputi intalasi server cloud dan alat pemantau jaringan. Dengan menggunakan aplikasi seperti wireshark untuk menangkap trafik jaringan dan IDS snort untuk memvalidasi serangan, penelitian ini membuat pendekatan yang sistematis dalam mendeteksi pola serangan secara berulang yang dapat merugikan. Penelitian ini dapat menjadi acuan dalam pemahaman mengenai forensik digital dan pemahaman mengenai *Brute Force* yang terjadi pada cloud public.

6. Penelitian dari Hidayah dan fachri (2025), mengeksplorasi penggunaan pada aplikasi MiChat dalam sebuah tindak kegiatan yang illegal khususnya prostitusi online yang marak terjadi pada negara ini. Dengan melakukan penerapan metode *Association of Chief Police Officers* (ACPO), penelitian ini menandai bahwa pentingnya akuisisi bukti digital yang sah guna memastikan bahwa semua bukti yang telah terkumpul dapat dipertanggungjawabkan secara hukum. Focus utamanya adalah untuk menjaga keaslian atau integritas bukti digital dari awal mulai pengakuisisian hingga penggunaannya dalam proses hukum, mencangkup pengelolaan bukti yang cukup ketat dan dokumentasi yang menyeluruh. Penelitian ini melibatkan penggunaan tools forensik seperti FTK imager dan MOBILedit forensik yang pada masing masing tools mencatat Tingkat keberhasilan akuisisi bukti diatas 60%. Proses tersebut berhasil digunakan untuk mengidentifikasi beragam jenis bukti digital, termasuk adanya pesan, gambar, vidio, dan log aktivitas yang sangat membantu dalam penguatan argument di laporan nantinya. Hasil dari penelitian ini menekankan betapa pentingnya perkembangan metode sistematis dalam akuisisi bukti digital, serta menandai perlunya tahapan-tahapan preventif yang lebih konprehensif dalam menghadapi kejadian prostitusi online yang terus berkembang.
7. Riadi *et al.* (2019) melakukan penelitian yang mengeksporasi investigasi forensik dan diterapkan pada sebuah aplikasi instant messaging berbasis web yang cukup populer seperti WhatsApp, Telegram, dan LINE, dengan focus pada aktor kejahatan digital. Penelitian ini menggunakan metodologi ACPO sebagai pedoman dan kerangka kerjanya untuk membantu menguraikan tahapan-tahapan investigasi secara sistematis dan terencana. Dalam prosesnya, alat forensik seperti FTK Imager, NetWitness Investigator, dan Wireshark digunakan untuk mengumpulkan artefak digital dan memastikan semua bukti digital dicatat dengan baik. Penelitian ini menunjukan bahwa whatsapp memiliki Tingkat keberhasilan investigasi yang lebih tinggi dibandingkan investigasi terhadap LINE dan

Telegram. Hasilnya menyoroti pentingnya memahami spesifik dari setiap aplikasi dalam konteks kejahatan siber dan menggarisbawahi keperluan untuk pengembangan pada metode akuisisi bukti yang tepat dan lebih lanjut. Dengan demikian, pada penelitian ini menggarisbawahi pentingnya pengetahuan tentang cara kerta pada masing-masing aplikasi bagi penyidik, serta mendorong peningkatan fitur keamanan pada platform komunikasi tersebut sebagai tahapan pencegahan terhadap kejahatan digital yang semakin meluas.

8. Penelitian yang dilakukan oleh Aziz *et al.* (2021), memiliki focus terhadap evaluasi kemampuan anti forensik dari aplikasi instant messaging yang paling banyak digunakan, yaitu skype, whatsapp, dan telegram. Mengingat meningkatnya jumlah pengguna aplikasi tersebut, penelitian ini memiliki tujuan unutk mengukur kerentanan masing-masing aplikasi terhadap Teknik anti forensik yang dapat digunakan oleh pelaku kejahatan siber untuk menghindari deteksi. Dengan menggunakan metodologi ACPO (*Association of Chief Police Officers*), penelitian ini terdiri dari 4 tahap perencanaan, peneliti menyusun sebuah rencana yang mendetail mengenai alat dan perangkat lunak yang akan digunakan untuk menguji kerentanan aplikasi- aplikasi tersebut. Penelitian ini memiliki sebuah hasil bahwa aplikasi skype memiliki Tingkat kerentanan yang sangat signifikan, dengan nilai kerentanan berada di angka 97%. Hal ini mengindikasikan bahwa skype rentan terhadap Teknik anti forensik yang dapat merusak integritas bukti digital. Di sisi lain, baik whatsapp maupun telegram menunjukkan nilai kerentanan yang sama yaitu di angka 66%, yang menuju pada indicator bahwa meskipun aplikasi ini lebih aman dibandingkat dengan skype, masih terdapat celah yang bisa di ekspoitasi oleh pihak yang tidak bertanggung jawab. Penelitian ini juga menggambarkan pentingnya pembaharuan aplikasi untuk memahami potensi kerentanan pada perangkat lunak tersebut serta tetap dengan Tindakan pengembahan evaluasi dan perbaikan terhadap fitur keamanan. Dengan meningkatnya perhatian pengguna terhadap privasi dan keamanan

data, penelitian ini memberikan saran berharga kepada pihak yang bersangkutan tentang mitigasi risiko dan penguatan keamanan.

9. Prasongko *et al.* (2022) melakukan penelitian yang berfokus pada pengungkapan bukti forensik dari aplikasi whatsapp yang terkait dengan praktik cyberbullying, yang semakin marak terjadi di indonesia. Menggunakan metode ACPO, penelitian ini meliputi empat fase penting yaitu perencanaan, akuisisi, analisis, presentasi atau report, yang dirancang untuk memberikan striktur yang jelas dalam proses investigasi. Pada fase perencanaan ini peneliti mengidentifikasi perangkat keras dan perangkat lunak yang sesuai seperti belkasoft evidence center dan hashmyfile, untuk digunakan dalam proses akuisisi dan analisis bukti digital. Penelitian ini menunjukan hasil bahwa alay belkasoft evidence center memiliki Tingkat efektivitas akuisisi bukti cukup besar dibandingkan dengan hashmyfile. Kedua alat tersebut berhasil mendeteksi berbagai jenis bukti digital termasuk pesan, media, dan informasi kontak. Proses analisis dikerjakan dengan mensimulasikan beberapa scenario untuk mengidentifikasi artefak digital yang relevan, kemudian digunakan untuk melakukan rangkaian laporan analisis. Temuan ini menandakan pentingnya penerapan protokol forensik yang ketat untuk memastikan akurasi dalam pengambilan dan analisis bukti yang krusial dalam konteks hukum. Penelitian ini sangat tepat dalam memberikan pedoman bagi penyidik dan akademisi untuk lebih memahami tantangan dan Teknik yang ada pada analisis forensik digital di aplikasi komunikasi yang banyak digunakan.
10. Giovani (2024) melakukan studi yang membahas dalam literatur forensik digital, khususnya berhubungan dengan aplikasi komunikasi yang banyak digunakan seperti Discord pada platform Android. Dengan menggunakan metode ACPO, penelitian ini mensimulasikan beberapa skenario kejahatan untuk mengidentifikasi dan mengakuisisi bukti digital dari aplikasi. Penelitian ini menunjukkan bahwa penggunaan virtual machine Android yang telah di-root dilakukan, meskipun prosesnya mirip dengan melakukan forensik pada perangkat asli. Dalam analisis ini, dua alat

tersebut, MOBILedit dan Autopsy, sangat penting dalam mengumpulkan data. Hasil penelitian menunjukkan bahwa simulasi di dua dari empat skenario yang diujicobakan berhasil menghasilkan bukti digital, dengan tingkat keberhasilan akuisisi mencapai 57.8%. Meskipun satu skenario tidak menghasilkan bukti, penelitian ini menunjukkan pentingnya eksplorasi dan penggunaan pendekatan sistematis dalam investigasi digital, yang berfokus pada pengumpulan bukti dari aplikasi komunikasi yang banyak digunakan.