TEORI • FRAMEWORK • METODE • PRAKTIK

DIGITAL FORENSIK PADA MEDIA SOSIAL

FRAMEWORK DAN METODE INVESTIGASI DIGITAL

- Prinsip dan Konsep Digital Forensik
- Akuisisi dan Preservasi Bukti Digital
- Analisis Artefak Media Sosial
- Chain of Custody dan Dokumentasi
- Aspek Hukum dan Etika Investigasi
- Pelaporan dan Presentasi Bukti Digital

Nukman Sn, S.Kom., M.Kom.

ITKA Media

DIGITAL FORENSIK PADA MEDIA SOSIAL • FRAMEWORK DAN METODE INVESTIGASI DIGITAL
Nukman Sn, S.Kom., M.Kom.
ITKA Media

DIGITAL FORENSIK PADA MEDIA SOSIAL: FRAMEWORK DAN METODE INVESTIGASI DIGITAL

Nukman Sn

ITKA Media

DIGITAL FORENSIK PADA MEDIA SOSIAL: FRAMEWORK DAN METODE INVESTIGASI DIGITAL

Penerbit : Nukman Sn

Editor : Lalu Amrullah
Layout & Desain Sampul : Tim Media ITKA
Halaman : 84
Ukuran : 14 x 20

Diterbitkan oleh : ITKA Media

Redaksi :
Jl. Anjani-Suralaga Desa Suralaga
Kec. Suralaga Kab. Lombok Timur
Prov. Nusa Tenggara Barat KP. 83654

Cetakan Pertama, Agustus 2026

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga buku yang berjudul ***Digital Forensik pada Media Sosial: Framework dan Metode Investigasi Digital*** ini dapat diselesaikan dan diterbitkan. Kehadiran buku ini diharapkan dapat memberikan kontribusi bagi pengembangan pengetahuan dan praktik di bidang digital forensik, khususnya dalam memahami proses investigasi terhadap aktivitas, informasi, dan artefak digital yang terdapat pada media sosial.

Perkembangan teknologi informasi dan komunikasi telah menjadikan media sosial sebagai bagian yang tidak terpisahkan dari kehidupan masyarakat. Berbagai bentuk komunikasi, pertukaran informasi, dokumentasi aktivitas, hingga transaksi digital berlangsung melalui berbagai platform media sosial. Kondisi tersebut menghasilkan sejumlah besar jejak digital yang dapat memiliki nilai informasi maupun nilai pembuktian dalam suatu proses investigasi. Oleh karena itu, diperlukan pendekatan yang sistematis, terstruktur, dan dapat dipertanggungjawabkan untuk melakukan identifikasi, pengumpulan, pemeriksaan, analisis, dokumentasi, serta penyajian bukti digital.

Buku ini disusun untuk memberikan pemahaman mengenai konsep dasar digital forensik, karakteristik bukti digital pada media sosial, prinsip-prinsip investigasi digital, serta framework yang dapat digunakan dalam proses **Digital Forensics Investigation**. Pembahasan juga diarahkan pada bagaimana investigator memahami sumber bukti, melakukan preservasi terhadap artefak digital, menganalisis informasi yang diperoleh, menjaga integritas barang bukti, dan menghasilkan dokumentasi investigasi yang sistematis. Dengan demikian, buku ini tidak hanya membahas aspek teknis, tetapi juga menekankan pentingnya prosedur dan metodologi dalam menjaga validitas hasil investigasi.

Secara khusus, buku ini diharapkan dapat menjadi referensi bagi mahasiswa, dosen, peneliti, praktisi teknologi informasi, investigator digital, aparat penegak hukum, maupun pihak lain yang memiliki ketertarikan terhadap bidang **digital forensics** dan investigasi media sosial. Materi yang disajikan berupaya menghubungkan konsep teoritis dengan kebutuhan investigasi digital sehingga pembaca dapat memperoleh pemahaman yang lebih komprehensif mengenai proses penanganan bukti digital pada lingkungan media sosial yang terus berkembang.

Penulis menyadari bahwa perkembangan teknologi digital berlangsung sangat cepat. Platform media sosial, mekanisme penyimpanan data, sistem keamanan, serta pola interaksi pengguna terus mengalami perubahan. Oleh sebab itu, buku ini bukan merupakan akhir dari pembahasan mengenai digital forensik, melainkan bagian dari proses pengembangan pengetahuan yang perlu terus diperbarui melalui penelitian, praktik investigasi, dan perkembangan teknologi. Kritik, saran, serta masukan konstruktif dari para pembaca sangat diharapkan untuk penyempurnaan buku pada edisi berikutnya.

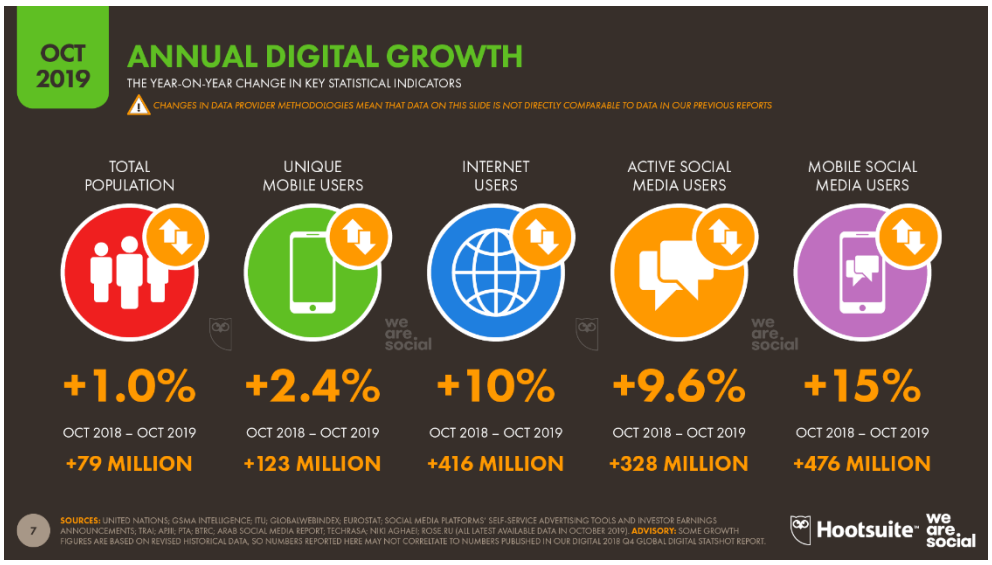
Akhirnya, penulis menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan, pemikiran, motivasi, dan kontribusi selama proses penyusunan hingga terbitnya buku ini. Semoga ***Digital Forensik pada Media Sosial: Framework dan Metode Investigasi Digital*** dapat memberikan manfaat bagi pengembangan keilmuan, pendidikan, penelitian, serta praktik investigasi digital di Indonesia.

DAFTAR ISI

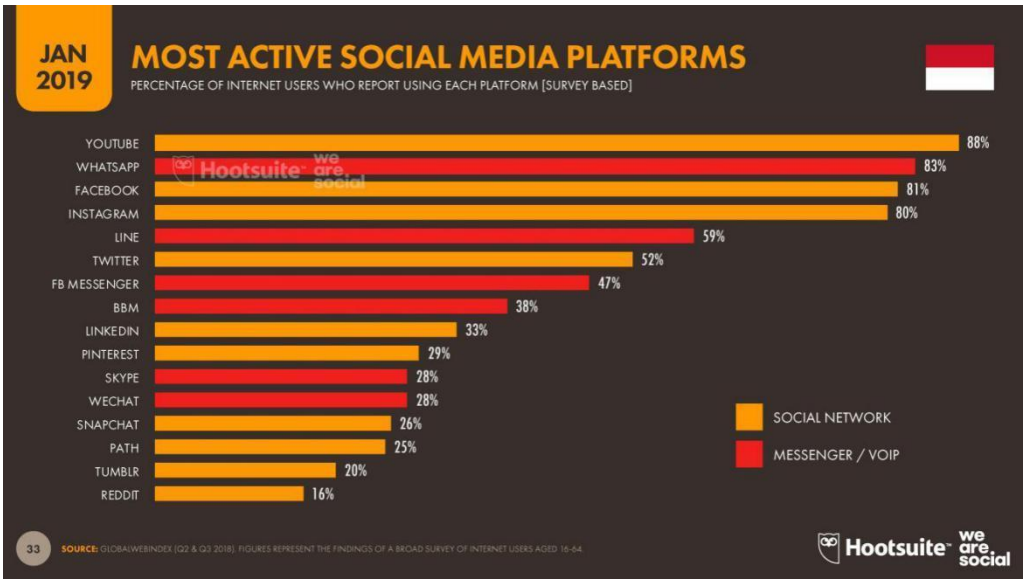
BAB I
PENDAHULUAN

1.1 Latar Belakang : Perkembangan Internet

Perkembangan media sosial pada saat ini adalah sangat berkembang apalagi di era teknologi 4.0 sumber daya *social* media semakin meningkat baik itu digunakan dalam keperluan *private* maupun organisasi. Berdasarkan data dari *We Are Social*, per Januari 2019 jumlah pengguna media sosial aktif di Indonesia ada sebanyak 56% dari total populasi, atau sebesar 150 juta orang. Dari jumlah ini ada sebanyak 130 juta orang aktif menggunakan perangkat *mobile* untuk mengakses media *social*. Youtube adalah *platform* yang paling banyak penggunanya (88%), dikutip *whatsapp* (83%), *Facebook* (81%), *Instigram* (80%) , *Line* (59%) dan *Twitter* hanya (27%), jadi tahun ini naik hamper dua kali lipat. (Ismail Fahmi, 2019). Kalau kita lihat peningkatan penggunaan media sosial di dunia semakin meningkat lebih tinggi lagi. Tingginya pengguna media sosial saat ini maka banyak yang tidak mengerti tentang percakapan mereka baik itu menggunakan gambar, audio, video maupun text, karena dari percakapan mereka di media sosial akan terekam oleh database.



Gambar 1. 1 Data Pengguna sosial di dunia. (wearesocial.com)



Gambar 1. 2 Data Platforms aktif di social media. (websindo.com)

(Supratman 2018) Perkembangan internet pada dasarnya banyak penggunaan media sosial untuk kebutuhan sehari-hari masyarakat pada umumnya, sehingga dalam media sosial banyak permasalahan yang muncul seperti halnya menyalahgunakan account media yang membuat account palsu untuk berbuat kejahatan dan bisa menggunakan media untuk penyebaran berita bohong sehingga membuat keresahan masyarakat.

(Yudhana, Riadi, and Zuhriyanto 2019) Dalam penyelidikan forensik digital, bukti yang diambil dari sebagian besar di dalam media sosial untuk dijadikan sebagai barang bukti. Banyaknya informasi berupa data-data pribadi yang secara tidak sadar dipublikasikan di media sosial baik itu informasi pribadi, perilaku, maupun kegiatan lainnya dapat digunakan penyidik sebagai barang bukti potensial untuk melacak kejahatan di media sosial.

Forensik sering kali dibutuhkan dalam penanganan kejahatan di media sosial karena banyak pelaku kejahatan menduplikat identitas seseorang. (Kurniawan and Prayudi 2014) Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kejahatan dan permasalahan hukum lainnya. Digital forensik merupakan bagian dari ilmu forensik yang menemukan penemuan dan investigasi materi/data yang ditemukan pada perangkat digital (komputer, *handphone*, tablet, PDA, *net-working devices*, *storage*, dan sejenisnya). (Raharjo 2013)

Permasalahan yang sering terjadi pada pengguna media sosial adalah menyalahgunakan hak akses media sehingga bisa membuat berita bohong yang tidak benar dasar informasinya. (Mukti, Masruroh, and Khairani 2018) Informasi atau berita di media sosial sering kali kita mendapatkan yang tidak benar sehingga bisa menjerumuskan ke dalam pelanggaran undang-undang ITE tentang penyebaran berita bohong dengan pasal 28 ayat 1.

Informasi di media sosial sering tidak disadari oleh pengguna media sosial baik itu di *facebook, twitter* maupun di *instagram*, maka dalam proses analisis media sosial ini membutuhkan *framework* untuk menyelesaikan permasalahan tersebut untuk mencari identitas si pengguna media sosial. Dari framework sosial media yang sudah pernah di kembangkan oleh (Al Jumah, Sugiantoro, and Prayudi 2019) dalam prosesnya menerapkan *composite logic* untuk pengumpulan bukti digital pada media sosial. Maka proses ini pengembangan dari *framework* yang sudah diterapkan sebelumnya, sehingga nanti beberapa perbedaan dan manfaat yang akan didapatkan di report nya. Dari problem yang ada maka peneliti mengambil kesimpulan untuk mencarikan solusi untuk investigasi sosial media dalam mengembangkan sebuah *framework* menggunakan metode *System Development Life Cycle (SDLC)* dengan Proses-Proses yang digunakan *planning, analysis, design, maintenance, dan implementation.*

Pemanfaatan *framework* dalam proses ini adalah sebagai kerangka pengumpulan data di media sosial serta dalam bidang manajemen untuk menggambarkan suatu konsep yang memungkinkan penanganan dalam berbagai jenis identitas seseorang. (Ibrahim, Li, and Wang 2018). Pengembangan *framework* ini akan membantu mempermudah pencarian data identitas pelaku kejahatan memanipulasi akun pada media sosial, mempermudah penyidik untuk menganalisis sebuah kasus dalam *cybercrime* khusus nya pada media sosial. Di dalam pengumpulan data di media sosial, proses ini akan mengembangkan *framework* sebagai pendukung kesuksesan dalam penyidikan *cybercrime* pada khususnya di media sosial.

Dari segi banyak proses dalam mengembangkan investigasi untuk membangun sebuah *framework* dari beberapa metode yang digunakan seperti halnya proses dari (Al Jumah, Sugiantoro, and Prayudi 2019) mengenai tentang pengumpulan data media sosial menggunakan metode *composite logic* untuk mengkolaborasikan *framework* digital forensik investigasi model supaya menghasilkan *framework* pengumpulan bukti digital di media sosial. Untuk proses yang saya angkat disini adalah untuk mengembangkan sebuah *Framework Digital Forensics Investigation (FDFI)* dengan menggunakan metode *System Development Life Cycle (SDLC). Framework* yang akan dibuat ini adalah pengembangkan dari *framework* yang sudah dikembangkan sebelumnya, akan tetapi dari jenis-jenis problem dan proses pengembangannya berbeda dengan metode yang digunakan juga berbeda, sehingga pada hasil akhirnya akan dibandingkan dengan *framework* yang sudah ada sebelumnya dengan hasil proses yang baru.

System Development Life Cycle (SDLC) yang akan membantu dalam proses pembuatan sebuah *framework* untuk berjalannya sebuah investigasi digital di sosial media.

Dalam rekayasa sistem dan rekayasa perangkat lunak dapat mengembangkan sebuah proses pembuatan *framework* dan pengubahan sistem serta model dan metodelogi yang digunakan untuk mengembangkan sistem-sistem tersebut. SDLC ini juga merupakan pola yang diambil dari sistem perangkat lunak dengan tahap-tahap yang ada pada proses ini yaitu *planning, analysis, design, maintenance, dan implementation.* Konsep dari SDLC mendasari beberapa jenis metodelogi pengembangan perangkat lunak.

BAB II
KONSEP DIGITAL FORENSIK

2.1 Digital Forensik

Menurut (Raharjo 2013) Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Sebagai ilmu yang masih baru, masih dibutuhkan pemahaman dan kemampuan untuk menguasai ilmu ini. Penguasaan ilmu ini tidak hanya ditujukan pada kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hukum.

Menurut (Firdaus 2016) Forensik secara umum adalah suatu proses ilmiah untuk mengumpulkan, menganalisis, dan menyajikan bukti pada pengadilan. Pada umumnya, sebuah tahap forensik dilakukan dengan asumsi bahwa data-data yang telah dikumpulkan akan digunakan sebagai bukti di pengadilan. Oleh karena itu, setelah pengumpulan barang bukti, para praktisi forensik menjaga dan mengontrol bukti tersebut untuk mencegah terjadinya modifikasi

Menurut Prof (Dr) SC Gupta, dan (Wicaksono and Prayudi 2013) forensik digital didefinisikan sebagai penggunaan metode ilmiah yang berasal dan terbukti terhadap pelestarian, koleksi, validasi, identifikasi, analisis, interpretasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi peristiwa ditemukan pidana atau membantu untuk mengantisipasi tindakan yang tidak sah terbukti mengganggu operasi yang direncanakan.

Forensik dikenal juga dengan (ilmu forensik digital) yang artinya salah satu cabang ilmu forensik terutama untuk penyelidikan dan penemuan konten perangkat digital dan seringkali dikaitkan dengan kejahatan komputer. (Afuan Lasmedi 2020) Istilah dari digital forensik adalah pada awalnya identik dengan digital komputer tapi kini sudah diperluas penyelidikan untuk penyimpanan semua perangkat dalam media digital forensik. Landasan forensik digital adalah praktik pengumpulan, analisis, dan pelaporan data digital, investigasi forensik memiliki peranan yang sangat beragam, pengguna yang paling umum adalah untuk pendukung atau penyangga asumsi criminal dalam pengadilan pidana atau perdata.

Di Dalam media digital mencakup dalam undang-undang nasional maupun internasional, khususnya penyelidikan perdata undang-undang dapat membatasi kemampuan analisis untuk melakukan pemeriksaan. Pembatasan penentuan jaringan atau pembacaan komunikasi pribadi sering kali terjadi. Dalam penyelidikan pidana, undang-

undang nasional membatasi beberapa informasi yang dapat disita. Selama pada awalnya di bidang ini *"International Organization on Computer Evidence (IOCE)* adalah salah satu lembaga yang bekerja dalam menetapkan standar internasional yang kompatibel terhadap penyitaan barang bukti.

2.1.1. Bukti Digital

Bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi digital dapat menjadi subjek penyidikan, dan setiap pembawa informasi yang ditargetkan untuk pemeriksa harus diperlukan sebagai barang bukti. Menurut (Akses, Elektronik, and Akses 2008) pasal 5 UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyebutkan bahwa "informasi elektronik dan atau dokumen elektronik dan hasil cetaknya merupakan alat bukti hukum yang sah", contoh barang bukti digital seperti alamat *Email*, berkas *word processor/spreadsheet*, kode sumber perangkat lunak, berkas gambar (JPEG, PNG, dll), *bookmarks* penjelajah web, *cookies,* kalender, *to do list* dan lain-lain.

2.1.2. Alat Forensik Digital

Para penegak hukum memanfaatkan peralatan seperti perangkat keras dan perangkat lunak khusus untuk penyelidikan forensik digital alat-alat ini digunakan untuk membantu. Alat-alat ini digunakan untuk membantu pemulihan dan pelestarian bukti digital. (Artha, Winarko, and Ilmu 2016)

a. Perangkat Keras

   Perangkat keras dalam forensik merupakan untuk penyimpanan alat bukti digital dan untuk menjaga agar perangkat target tidak berubah demi menjaga integritas bukti. *Forensik disk controller* atau pencacah perangkat keras merupakan perangkat *read-only* yang memungkinkan pengguna untuk membaca data di perangkat tersangka tanpa mengambil resiko memodifikasi atau menghapus konten di dalamnya. Sedangkan *disk write-protector* atau *write-brocker* berfokus pada pelestarian bukti di perangkat target dan berfungsi untuk mencegah konten dalam perangkat penyimpanan termodifikasi atau terhapus. *Hard-drive duplicator* adalah perangkat pencitraan *(Imaging)* yang berfungsi untuk menyalin semua file cakram keras yang di curigai didalam cakram yang bersih, alat ini juga dapat menduplikasi data dalam cakram lepas atau kartu digital (SD) secara aman.

Gambar 2. 1 Alat Perangkat keras Forensik

b. Perangkat Lunak

Untuk penyelidikan dan investigasi yang lebih baik maka para pengembang telah membuat beberapa perangkat lunak forensik, seperti (*Windows, Linux)* sistem operasi ini di modifikasi menjadi multi-tujuan serta dapat melakukan berbagai tugas dalam satu aplikasi sehingga penyelidik sangat mudah menggunakan pengungkapan dalam sebuah kasus kejahatan. Perangkat lunak forensik komputer melengkapi perangkat keras yang tersedia untuk penegak hukum untuk memperoleh menganalisis barang bukti yang dikumpulkan dari perangkat tersangka. Alat-alat forensik ini juga dapat diklasifikasikan kedalam berbagai kategori.

- Alat perekam cakram dan data
- Penampilan berkas
- Alat analisis berkas
- Alat analisis *registry*
- Alat analisis internet
- Alat analisis surat elektronik
- Alat analisis peranti bergerak
- Alat analisis macOS
- Alat forensik jaringan
- Alat forensik basis data

Berikut ada beberapa alat forensik yang digunakan oleh lembaga penegak hukum dalam melakukan investigasi kejahatan.

Tabel 2. 1 Alat-alat Forensik Digital

Alat	Keterangan	Lisensi
Digital Forensics Framework	Digunakan oleh profesional atau non-ahli, ini digunakan untuk lacak balak digital, untuk mengakses perangkat jarak jauh atau local, *forensik system windows* atau *linux*, pemulihan berkas yang dihapus, pencarian cepat untuk mendata berkas.	GPL
Open Computer Forensics Architecture	Dibagun di platform linux dan menggunakan basis dat *postgreSQL* untuk penyimpanan datanya. Dibangun oleh Badan Kepolisian Nasional Belanda untuk mengotomatisasi proses forensik digital.	GPL
CAINE	*Computer Aided Investigative Environment* adalah distro linux yang dibuat untuk forensik digital. *CAINE* menawarkan lingkungan untuk mengintegrasikan perangkat lunak yang ada sebagai modul .	GPL
X-Ways Forensics	*Platform* canggih untuk memeriksa forensik digital, yang berjalan pada semua versi *windows* yang tersedia dan bekerja secara efisien.	Komersial
SAINS Investigative Forensics Toolkit-SIFT	*System operasi forensik* multi-tujuan berbasis Ubuntu, dilengkapi semua alat yang diperlukan yang digunakan dalam proses forensik digital.	Sumber terbuka dan berbayar
EnCase	*Platform* forensik multiguna dengan banyak peralatan untuk beberapa area dalam proses forensik digital. Alat ini dapat dengan cepat untuk mengumpulkan data dari berbagai perangkat dan menggali bukti potensial. *EnCase* juga dapat menghasilkan laporan berdasarkan bukti.	Komersial
Registry Recon	Alat analisis *registry* , alat ini mengekstrak informasi *registry* dari barang bukti dan kemudian membangun kembali representasi *registry*.	Komersial
The Sleuth Kit	Alat yang berbasis *Unix* dan *Windows* dengan berbagai alat-alat yang membantu dalam forensik digital. Alat-alat ini membantu dalam menganalisis image cakram, melakukan analisis mendalam dari file system dan berbagai hal lainnya.	*IBM Open Source Licence Common Public License* GPL
Libforensics	Pustaka untuk mengembangkan aplikasi forensik digital dikembangkan dengan alat *python* dan dilengkapi dengan berbagai alat demo untuk mengekstrak berbagai informasi dari berbagai jenis barang bukti digital.	LGPL
Volatility	*Framework* forensik memori digunakan dalam respon insiden dan analisis malware	GPL

Masih banyak alat yang lain belum masuk dalam tabel tersebut seperti *windowsSCOPE, The Coroner's Toolkit, Oxygen Forensics Suits, Xplico, Mandiant RedLine, Computer Online Forensic Evidence Extractor, P2 eXplorer, Plain Sight, XRY, HELIX 3, dan Cellebrite UFED.*

2.1.3. Bagian-Bagian Forensik

Penyelidikan forensik digital tidak hanya terbatas hanya pada mengambil data pada komputer, karena perangkat digital kecil seperti (tablet, ponsel dan *flash drive*) sekarang banyak digunakan (Huizen, Jayanti, and Hostiadi 2016). Beberapa perangkat ini ada yang memiliki memori volatile dan nada yang tidak. Metodologi yang menandai telah tersedia untuk mengambil data dari memori volatile namun terdapat kekurangan metodologi atau kerangka kerja yang mengambil data dari sumber memori non volatil. Ada lima cabang utama forensik digital dan mereka dikategorikan berdasarkan tempat data disimpan atau bagaimana data ditransmisikan.

1. Forensik Komputer

   Tujuan dari forensik komputer adalah untuk menjelaskan keadaan artefak digital saat ini, seperti sistem komputer, media penyimpanan, atau dokumen elektronik. Disiplin ini biasanya mencakup komputer sistem benam (perangkat digital dengan kemampuan komputasi belum sempurna dengan memori *onboard*) dan memori statis seperti (USB *penDrive*).

2. Forensik Peranti Bergerak

   Forensik peranti bergerak adalah subcabang forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat seluler. Berbeda dengan forensik komputer karena perangkat seluler memiliki sistem komunikasi yang terintegrasi (GSM) dan biasanya dengan mekanisme penyimpanan *proprietary,* investigasi biasanya lebih berfokus pada data sederhana seperti data panggilan dan komunikasi (SMS/Email) daripada pemulihan mendalam dari data yang dihapus.

3. Forensik Jaringan

   Forensik jaringan berkaitan dengan pengamatan dan analisis lalu lintas jaringan komputer baik lokal maupun WAN/internet untuk keperluan pengumpulan informasi, pengumpulan bukti, atau deteksi intrusi. Lalu lintas biasa nya disadap ditingkat paket baik disimpan untuk analisis nanti atau disaring secara *real-time.*

4. Analisi Data Forensik

   Analisis data forensik adalah cabang forensik digital. Ini menguji data terstruktur dengan tujuan untuk menemukan dan menganalisis pola kegiatan penipuan yang dihasilkan dari kejahatan keuangan.

5. Forensik Basis Data

   Forensik basis data adalah cabang forensik digital yang berkaitan dengan studi forensik basis data dan metadatanya. Investigasi menggunakan isi basis data, berkas *log* dan data dalam RAM untuk membuat garis waktu atau memulihkan informasi yang relevan.

2.2. *Framework* Forensik

Framework ini pada dasarnya yang arti dari bahasa indonesianya sebuah kerangka kerja, dan framework ini sering digunakan oleh penyidik forensik sebagai alat untuk menyelesaikan permasalahan. Menurut kamus oxford mengartikan *framework* ini sebagai struktur pendukung untuk mensukseskan dalam penyelidik forensik.

Menurut (Al-Azhar Nuh 2011) *framework* forensik meliputi :

1. *Preparation*

   Persiapan *(preparation)* merupakan persiapan awal dari investigasi. Pada tahap ini di persiapkan segala kebutuhan untuk melakukan proses investigasi kebutuhan peralatan baik perangkat lunak maupun perangkat keras yang dibutuhkan dalam proses investigasi.

2. *Collection*

   Pengumpulan Data *(collection)* proses mengumpulkan dan memastikan informasi pada variable of interest (subjek yang akan dilakukan uji coba).

3. *Examination*

   Pemeriksaan *(examination)* tahap pemeriksaan merupakan Proses pemeriksaan secara komprehensif terhadap barang bukti digital sehingga analisis forensik mendapat gambaran fakta-fakta tentang kasus yang ditangani.

4. *Analysis*

   Analisis *(analysis)* merupakan tahap pemeriksaan secara lebih mendetail dari fakta-fakta yang didapatkan pada proses pemeriksaan. Analisis ini bertujuan untuk membuktikan kejahatan yang terjadi dan kaitannya dengan pelaku.

5. *Investigation Report*

   Laporan hasil Investigasi *(investigation report)* merupakan bentuk tertulis dari proses analisis yang dilakukan dan juga berisi temuan-temuan dari proses analisis yang sesuai

dengan aturan penulisan laporan hasil investigasi. Laporan yang dibuat harus dapat dipahami oleh pihak-pihak terkait seperti Hakim, Jaksa, dan lain-lainnya.

2.3. System Development Life Cycle (SDLC)

SDLC adalah rekayasa sistem dan rekayasa perangkat lunak sebuah proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sistem-sistem tersebut. Konsep ini pada umumnya ditujukan kepada sistem komputer dan sebuah informasi. *System development life cycle (SDLC)* ini dapat juga diimplementasikan dengan pengembangan sistem perangkat lunak yang terdiri dari beberapa Proses yang sering digunakan yaitu, *planning* (rencana), *analysis* (analisis), *design* (desain), *implementation* (implementasi), dan *maintence* (pengelolaan). Ada 12 jenis model *System Development Life Cycle (SDLC)*

1. *Waterfall Development* Model (Model Sekuensial Linier)

   Model ini sering disebut dengan model pengembangan Air terjun, karena merupakan paradigma model pengembangan perangkat lunak paling tua dan paling banyak dipakai. Model ini mengusulkan sebuah pendekatan perkembangan perangkat lunak yang sistematik dan sekuensial yang yang dimulai pada tingkat dan kemajuan sistem pada seluruh Proses yaitu, analisis, desain, kode, pengujian, dan pemeliharaan.

2. Model *Prototype*

   Model ini merupakan suatu paradigma baru dalam metode pengembangan perangkat lunak dimana metode ini hanya sekedar evolusi dalam dunia pengembangan perangkat lunak, tetapi juga merevolusi metode pengembangan perangkat lunak yang lama yaitu sistem sekuensial yang biasa dikenal dengan nama SDLC atau *waterfall* development model. Dalam metode prototype dari perangkat lunak yang dihasilkan kemudian dipresentasikan kepada pelanggan, dan pelanggan tersebut diberikan kesempatan untuk memberikan masukan sehingga perangkat lunak yang dihasilkan nantinya betul-betul sesuai dengan keinginan dan kebutuhan pelanggan.

3. Model *Rapid Application Development* (RAD)

   Model ini proses pengembangan perangkat lunak sekuensial linier yang menekankan siklus perkembangan yang sangat pendek (60-90) hari. Model RAD ini merupakan sebuah adaptasi kecepatan tinggi dari model sekuensial linier dimana perkembangan dapat dicapai dengan menggunakan pendekatan konstruksi berbasis komponen.

4. Model *Evolutionary Development* (Evolutionary Software Process Model)

   Model ini bersifat *iteratif* (mengandung perulangan). Hasil proses nya berupa produk yang semakin lama semakin lengkap sampai versi terlengkap dihasilkan sebagai produk akhir dari proses. Model ini dibagi menjadi 2 yaitu, model *incremental* dan model *spiral (model boehm)*

5. Model *Agile*

   Model ini merupakan pengembangan jangka pendek yang memerlukan adaptasi cepat dan pengembangan terhadap perubahan dalam bentuk apa pun. Dalam agile ini terdapat beberapa poin penting diantaranya sebagai berikut :

   a. Interaksi antar personal lebih penting dari proses dan alat
   b. Software yang berfungsi lebih penting daripada dokumentasi yang lengkap.
   c. Kolaborasi dengan klien lebih penting daripada negosiasi kontrak.
   d. Sikap tanggap lebih penting daripada mengikuti rencana/plan.

6. Model *Fountain* (Air Mancur)

   Model ini merupakan perbaikan logis dari model *waterfall*, langkah dan urutan prosedurnya masih sama. Namun pada model ini kita dapat mendahulukan sebuah *step* atau melewati *step* tersebut, akan tetapi ada yang tidak bisa dilewati stepnya seperti memerlukan design sebelum melakukan coding jika itu dilewati maka akan ada kesalahan dalam siklus SDLC.

7. Model *Synchronize and Stabilize*

   Model ini yang digunakan oleh *Microsoft.* Secara garis besar, model *Synchronize and Stabilize* ini sama dengan model incremental akan tetapi, Cusamano dan Selby tahun 1997 menyebutnya sebagai model *Synchronize and Stabilize* karena ada beberapa proses manajemen yang ditekankan oleh *microsoft*.

8. Model *Rational Unified Process*

   Model ini sebagai metodologi pengembangan sistem berbasis objek. Metode ini juga sudah menjadi salah satu metode yang banyak digunakan dalam pengembangan sistem berorientasi objek. RUP ini mempunyai 4 Proses yaitu : *inception, elaboration, construction,* dan *transition*.

9. Model *Build* dan *Fix Method*

   Model ini merupakan metode yang paling lemah diantara model SDLC yang lain, tetapi menjadi acuan pengembangan untuk metode SDLC yang lain. *Build & fix* ini bertujuan untuk memberikan kepercayaan terhadap pelanggan dengan cara

memberikan pelayanan perbaikan dan perawatan secara terus menerus terhadap produk yang digunakan oleh user.

10. Model Pengembangan *Extreme Programming*

    Model ini merupakan suatu pendekatan yang paling banyak digunakan untuk pengembangan perangkat lunak cepat. Dengan alasan menggunakan metode ini karena sifat dari aplikasi yang dikembangkan dengan cepat melalui Proses-Proses sperti : *Planning, Design, Coding* dan *Testing*.

11. SDLC *Big Bang* Model

    Model ini tidak mengikuti proses tertentu. Perkembangan hanya dimulai dengan uang dan usaha yang dibutuhkan sebagai masukan, dan hasilnya adalah perangkat lunak yang dikembangkan yang mungkin tidak sesuai dengan kebutuhan pelanggan.

12. The V-Model

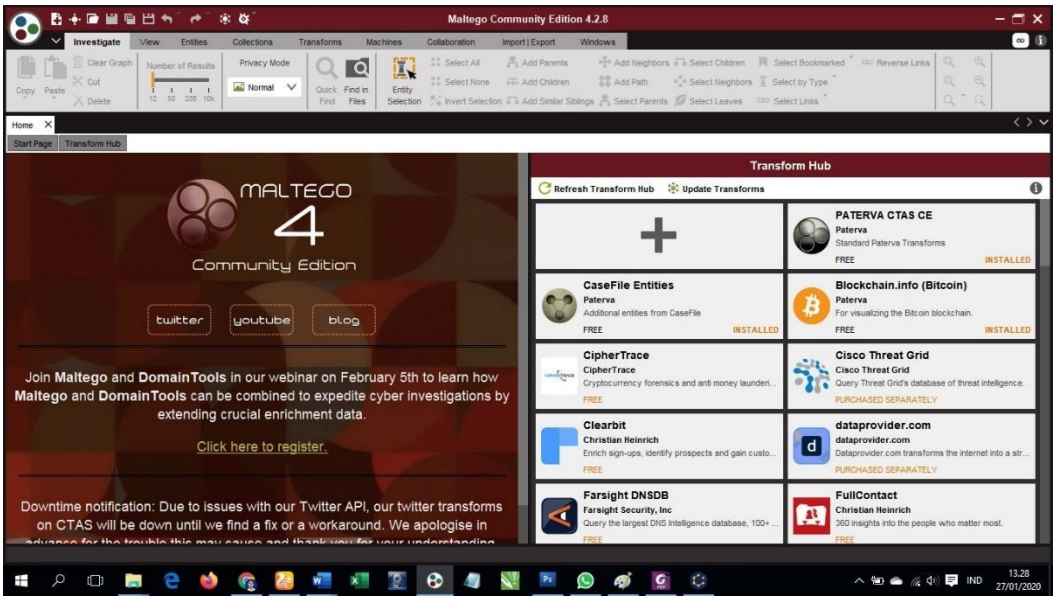
    Model SDLC ini pelaksanaan proses yang terjadi secara berurutan dalam bentuk V. Dikenal juga sebagai model *Verifikasi* dan *Validasi.*

2.4. Maltego

Maltego adalah alat penambangan data interaktif yang menyajikan grafik terarah untuk analisis tautan. Alat ini digunakan dalam penyelidikan online untuk menemukan hubungan antara potongan-potongan informasi dari berbagai sumber yang berlokasi di Internet. Maltego menggunakan ide transformasi untuk mengotomatiskan proses kueri sumber data yang berbeda. Informasi ini kemudian ditampilkan pada grafik berbasis simpul yang cocok untuk melakukan analisis tautan. Saat ini ada empat versi klien Maltego yaitu:

1. Maltego CE - bebas, penggunaan non komersial .
2. Maltego Classic - berbayar, penggunaan komersial.
3. Maltego XL - berbayar, penggunaan komersial.
4. Maltego CaseFile - gratis, komersil, tanpa Transform .

Tiga klien Maltego pertama datang dengan akses ke perpustakaan transformasi standar untuk penemuan data dari berbagai sumber publik yang biasanya digunakan dalam penyelidikan online dan forensik digital. Karena Maltego dapat berintegrasi dengan hampir semua sumber data, banyak vendor data telah memilih untuk menggunakan Maltego sebagai platform pengiriman untuk data mereka. Ini juga berarti Maltego dapat disesuaikan dengan kebutuhan yang unik.

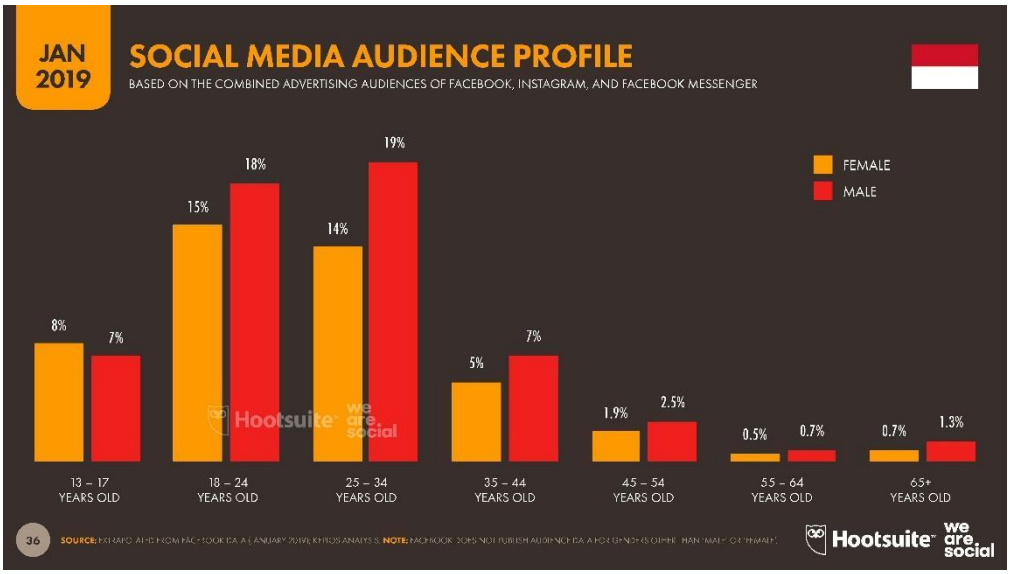


Gambar 2. 2 Tampilan Awal Maltego

2.5. Media Sosial

Media sosial pada saat ini sangat berkembang di kehidupan masyarakat dunia pada umumnya dan masyarakat indonesia pada khususnya. Media sosial adalah kebutuhan sehari-hari dalam keperluan bisnis ataupun informasi, sehingga sangat bermanfaat bagi masyarakat. Tetapi ada juga yang memanfaatkan dalam kejahatan karena di dalam media sosial ini secara umum identitas pengguna terdaftar pada server jaringan. Media sosial ini bukan hanya sekedar facebook, twitter, ataupun instagram, tetapi juga mencakup pada website, blogger, dan youtube karena ini juga sangat dibutuhkan oleh banyak masyarakat dalam mengambil informasi.

Dari hasil proses (Zuhriyanto et al. 2018) mengatakan media sosial yang pada khususnya facebook dan twitter salah satu bagian yang digunakan sebagai penghubung komunikasi antar manusia di dunia *cyber*, karena terpengaruhnya perkembangan teknologi informasi semakin maju dan memudahkan manusia berkomunikasi antar jarak jauh. Selain dari dampak positif ada juga dampak negatif yang terjadi pada penyalahgunaan media sosial sehingga menyebabkan kerugian pada pengguna.



Gambar 2. 3 Perkembangan media sosial antara gender dan umur (websindo.com)

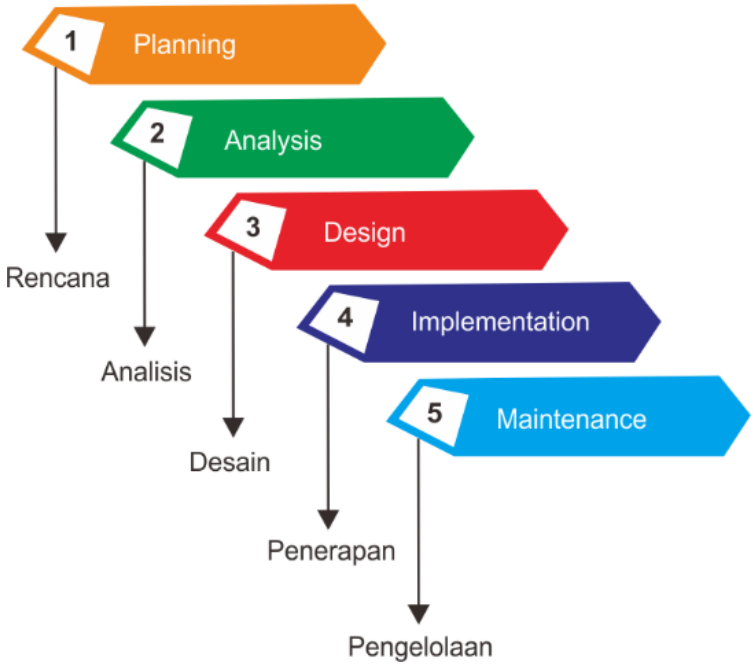
Kalau dilihat dari perkembangan pada gambar 2.3 merupakan tingkat perkembangan dari gender dan umur, terlihat penggunaan media sosial paling banyak 18 - 34 tahun, baik itu laki-laki maupun perempuan, dan ini adalah masa-masa yang sangat aktif menggunakan media sosial setiap waktu.

BAB III

PLANING SDLC *(System Development Life Cycle)*

3.1 SDLC Untuk Framework

SDLC *(System Development Life Cycle)* atau Siklus hidup pengmbangan system adalah proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sebuah sistem. SDLC juga merupakan pola yang diambil untuk mengembangkan sistem perangkat lunak, yang terdiri dari tahap-tahap: rencana *(planning)*,analisis *(analysis)*, desain *(design)*, penerapan *(implementation)*, dan pengelolaan *(maintenance)*.



Gambar 3. 1 Proses Penerapan SDLC *(System Development Life Cycle)*

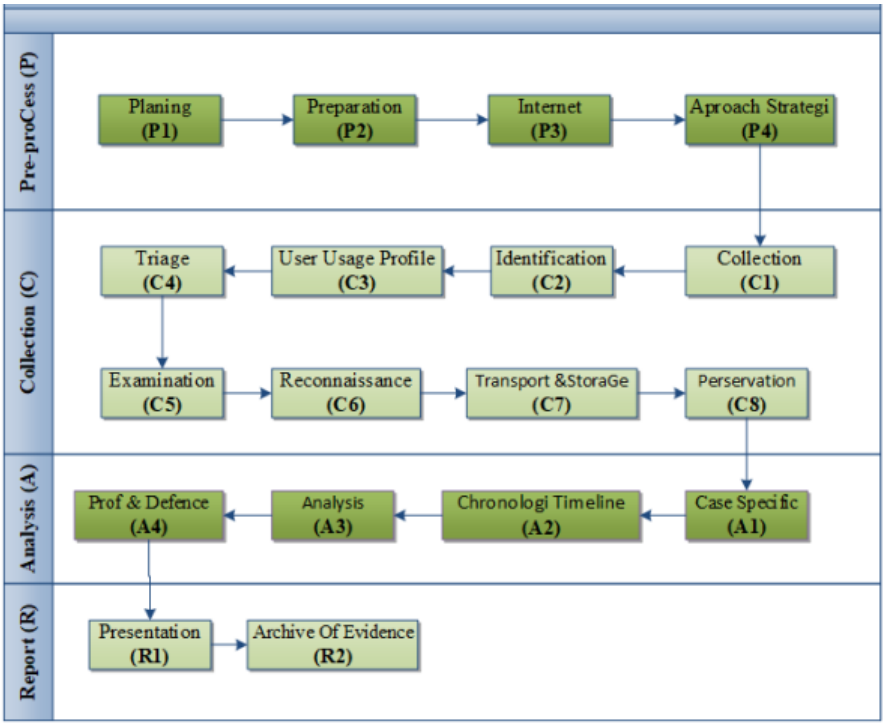
Tabel 3. 1 Proses Pengembangan *framework* pada SDLC

Proses Proses	Uraian Penerapan Proses	Keterangan	Output
Planning	Proses perencanaan awal yang mana Proses ini akan melakukan identifikasi terhadap *framework*	Mengidentifikasi *framework* terkait forensik sosial media	Tabel identifikasi *framework*

	sebelumnya yang berkaitan dengan forensik sosial media		
Analysis	Proses analisis dengan melakukan identifikasi terhadap Proses-Proses *framework* yang akan dikembangkan	Mengidentifikasi Proses-Proses *framework* sebelumnya	Tabel identifikasi Proses-Proses *framework*
Design	Proses dilakukannya normalisasi terhadap Proses yang memiliki makna yang sama setelah itu akan dilakukan penambahan baru yang belum ada pada *framework* sebelumnya untuk mendukung proses investigasi pada sosial media forensik	Melakukan proses normalisasi dan menambahkan Proses baru	Tabel normalisasi *framework*
Implementation	Proses pengembangan *framework* berdasarkan Proses-Proses dari *framework* dan teknik investigasi sosial media forensik sebelumnya. Proses pengembangan *framework* akan gambarkan dalam bentuk state chart diagram.	Proses pengembangan *framework* dari hasil design pada Proses sebelumnya.	Pengembangan *framework*
Maintenance	Proses pemeliharaan *framework* yang telah dikembangakan selama penggunaan *framework*	Proses pemeliharaan	Pengecekan/pemeliharaan kembali *framework* yang sudah dikembangkan

3.2 Planning Pelaksanaan

Planning adalah bertujuan untuk mengidentifikasi apa saja yang akan dikembangkan dan sasaran-sasaran yang akan dicapai untuk pembuatan *framework* baru dalam forensik media sosial. Dari hasil kolaborasi beberapa model yang digunakan oleh pengembang untuk menjadikan sebuah *framework,* adapun *framework* yang sudah ada pada pengembang sebelumnya adalah seperti gambar dibawah ini.



Gambar 3. 2 Hasil kolaborasi *framework* pengembang sebelumnya

Dari gambar 3.2 menjelaskan rancangan awal pengembang *framework* pengumpulan bukti digital pada sosial media dengan beberapa Proses-Proses diantaranya *Pre-Process*, *Collection, Analysis*, dan *Report*

1. *Pre-process* (P) Proses awal dalam pengumpulan barang bukti digital
   - *Planning* (P1) Proses mempersiapkan segala kebutuhan untuk proses penyelidikan baik itu pengumpulan informasi, surat perintah penyelidikan dan penggeledahan, peralatan pendukung lainnya.
   - *Preparation* (P2) Proses menyiapkan alat, teknik, surat perintah penggeledahan, serta memantau otorisasi dan dukungan manajemen.
   - *Internet* (P3) Proses menghubungkan perangkat komputer dan tools yang digunakan dengan internet sehingga dapat memulai proses investigasi.

- *Aproach Strategy* (P4) Proses melakukan pendekatan, pengamatan, dan pemanfaatan teknologi secara spesifik sehingga dapat memaksimalkan proses investigasi yang dilakukan.

2. *Collection* (C) merupakan Proses untuk mengumpulkan bukti-bukti awal dan bukti pendukung.
   - *Collection* (C1) Proses mengumpulkan bukti-bukti yang relevan dengan menggunakan alat maltego dan kunci API sehingga dapat memperoleh informasi yang berasal dari media sosial .
   - *Identification* (C2) Proses melakukan deteksi dan identifikasi terhadap barang bukti yang di temukan.
   - *User Usage Profile* (C3) Proses untuk menemukan hubungan antara bukti digital yang telah dikumpulkan dan di identifikasi dengan pelaku kejahatan.
   - *Triage* (C4) Proses melakukan identifikasi barang bukti dan prorioritas barang bukti berdasarkan kriteria bukti yang potensial dan relevan.
   - *Examination* (C5) Proses pelacakan barang bukti secara sistematis serta melakukan validasi terhadap barang bukti yang telah di temukan.
   - *Reconnaissance* (C6) Proses eksplorasi untuk mendapatkan bukti-bukti yang mendukung.
   - *Transport & Storage* (C7) Proses menyiapkan semua bukti yang telah dikumpulkan, kemudian ditempatkan ditempat aman sehingga dapat menjaga integritas barang bukti.
   - *Perservation* (C8) Proses mengamankan barang bukti dari yang tidak berkepentingan.
3. *Analysis* (A) merupakan Proses untuk melakukan analisa terhadap barang yang telah dikumpulkan
   - *Case Specific* (A1) Proses dimana penyidik dapat menyesuaikan fokus pemeriksaan terhadap bukti yang ditemukan.
   - *Chronology Timeline* (A2) Proses menjelaskan kronologi kejadian yang telah terjadi.
   - *Analysis* (A3) Proses melakukan analisa, merekontruksi dan menarik kesimpulan terhadap barang bukti yang telah ditemukan.
   - *Prof & Defence* (A4) Proses untuk penyidik membuktikan validasi kasus dengan temuan yang ada .
4. *Report* (R) merupakan Proses akhir untuk perancangan *framework* pengumpulan bukti digital di media sosial.

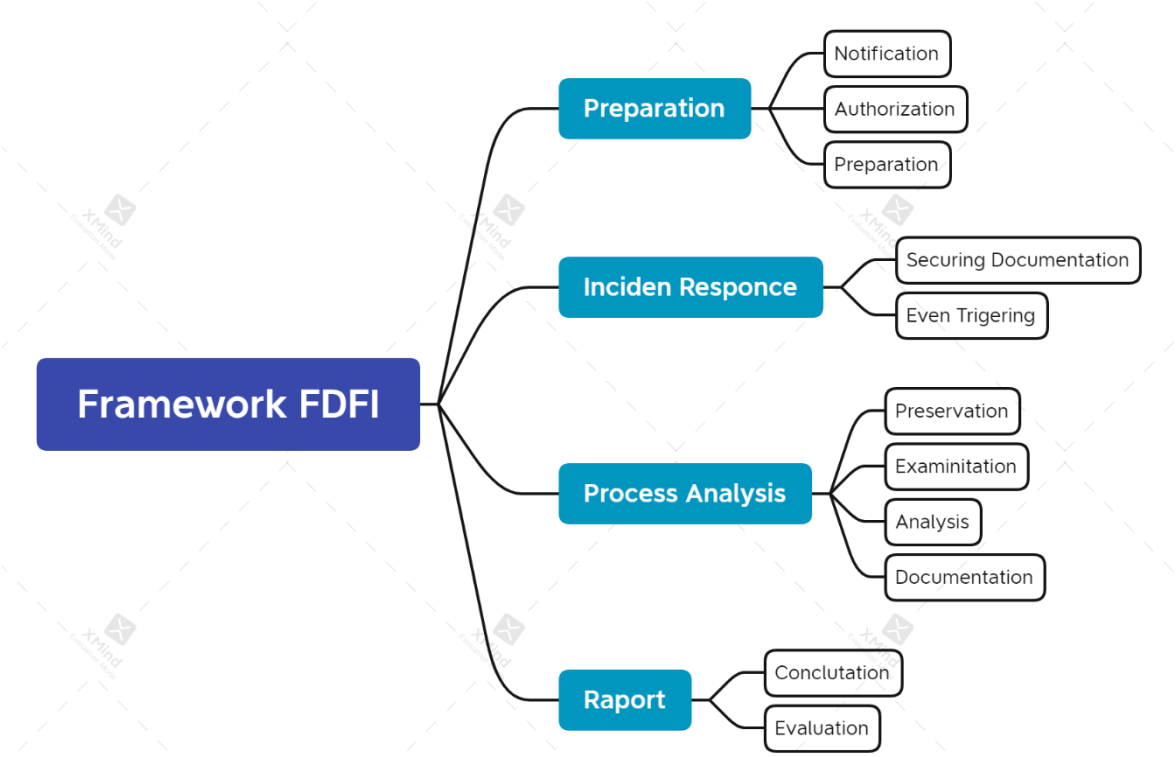
- *Presentation* (R1) Proses meringkas dan memberikan kesimpulan, pelaporan serta melakukan dokumentasi
- *Archive Of Evidence* (R2) Proses penyimpanan barang bukti yang telah dilakukan analisa dan telah di proses di pengadilan.

Dari hasil penjelasan framework di atas ada beberapa Proses yang seharusnya masuk pada 1 bagian seperti Proses *pre-process* di bagian internet bisa masuk di bagian preparation dan pada Proses *collection* ini tidak sesui dengan problem yang peneliti kembangkan baik itu di sub *trage*, dan *Transport & Storage*. Maka dari itu sesuai dengan problem yang akan di kembangkan perlu *framework* yang baru untuk memecahkan permasalahan tersebut.

Tabel 3.2 Normalisasi *Framework* FDFI

No	Tahap Normalisasi *Framework FDFI*	ID
Preparation		**1**
1.	Notification	1.1
2.	Authorization	1.2
3.	Preparation	2.3
Incident Response		**2**
4.	Securing Documentation	2.1
5.	Event Triggering	2.2
Process Analysis		**3**
6.	Preservation	3.1
7.	Examination	3.2
8.	Analysis	3.3
9.	Documentation	3.4
Report		**4**
10.	Conclusion	4.1
11.	Evaluation	4.2

Adapun tabel normalisasi *framework FDFI* di atas adalah olahan atau gabungan *framework* sebelumnya sehingga peneliti lebih mudah dan singkat dalam proses analisis investigasi digital.



Gambar 3. 3 *Framework* FDFI *Investigation* Digital

3.3 *Framework FDFI*

Framework FDFI adalah *framework* baru dari hasil kolaborasi *framework* yang sudah ada sebelumnya dan kelebihan dari *framework* ini sangat simpel dan sederhana sesuai dengan kebutuhan analisis investigasi pada social media. *Framework FDFI* ini menggunakan empat tahap proses investigasinya mulai dari *preparation, incident response, process analysis dan report*.

1) *Preparation*

Proses ini merupakan persiapan yang dilakukan dalam penanganan investigasi social media dalam pada pencarian barang bukti digital mulai dari perkara sampai dengan laporan akhir.

a. *Notification:* Tahap ini merupakan dalam pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum.
b. *Authorization:* Proses untuk mendapatkan hak akses terhadap barang bukti dan status hukum proses penyidikan.
c. *Preparation:* Persiapan yang meliputi ketersediaan alat, personel dan berbagai hal kebutuhan penyelidikan.

2) *Incident Response*

Proses ini merupakan kegiatan perkara kejadian untuk mengamankan barang bukti digital sehingga tidak terjadi terkontaminasi dengan kejadian lain.

a. *Securing Documentation:* Melakukan sebuah mekanisme untuk mengamankan dokumentasi dan mengolah tempat kejadian perkara, mencari sumber pemicu kejadian, mencari sambungan komunikasi atau jaringan dan mendokumentasikan tempat kejadian dengan mengambil barang bukti digital.
b. *Event Triggering:* Melakukan analisa awal terhadap sebuah proses kejadian yang terjadi

3) Proses Analysis

Tahap ini akan melakukan proses analisis data barang bukti yang sudah didapatkan sebelumnya sehingga dapat ditemukan jenis kejahatan yang terjadi.

a. *Preservation:* Menjaga integritas temuan yang didapatkan dari hasil proses sehingga tidak terjadi permasalahan.
b. *Examination:* Pengolahan barang bukti digital untuk menentukan keterkaitan dengan kejadian.
c. *Analysis:* Merupakan kajian teknis dan merangkai keterkaitan dengan temuan yang ada.
d. Documentation: Melakukan dokumentasi terhadap semua proses kegiatan dari awal penyidikan sampai proses analisis laporan kegiatan.

4) Report

Proses ini merupakan proses pembuatan laporan hasil analisa yang dilakukan pada tahap sebelumnya dan memastikan sudah sesuai dengan aturan hukum yang berlaku.

a. *Conclusion:* Menyimpulkan hasil dari investigasi yang dilakukan
b. Evaluation: proses analisa dan evaluasi keseluruhan terhadap hasil investigasi dan mencatat proses penyelidikan yang sudah dilakukan.

BAB VI
INVESTIGASI

Mode investigasi dalam menjalankan aksi untuk memperoleh barang bukti merupakan pendekatan sistematis yang digunakan dalam proses penyelidikan atau penyidikan untuk mengungkap suatu peristiwa pidana berdasarkan fakta yang dapat diverifikasi. Investigasi tidak semata-mata berorientasi pada menemukan barang bukti, tetapi juga bertujuan memastikan hubungan antara bukti, peristiwa, korban, dan pihak yang diduga terlibat. Dalam praktiknya, kegiatan investigasi perlu dilakukan berdasarkan prosedur hukum agar bukti yang diperoleh memiliki nilai pembuktian dan tidak diperoleh melalui cara yang melanggar hak seseorang. Penanganan tempat kejadian perkara menjadi salah satu tahap penting karena kondisi dan benda di lokasi dapat memberikan informasi awal mengenai suatu peristiwa.

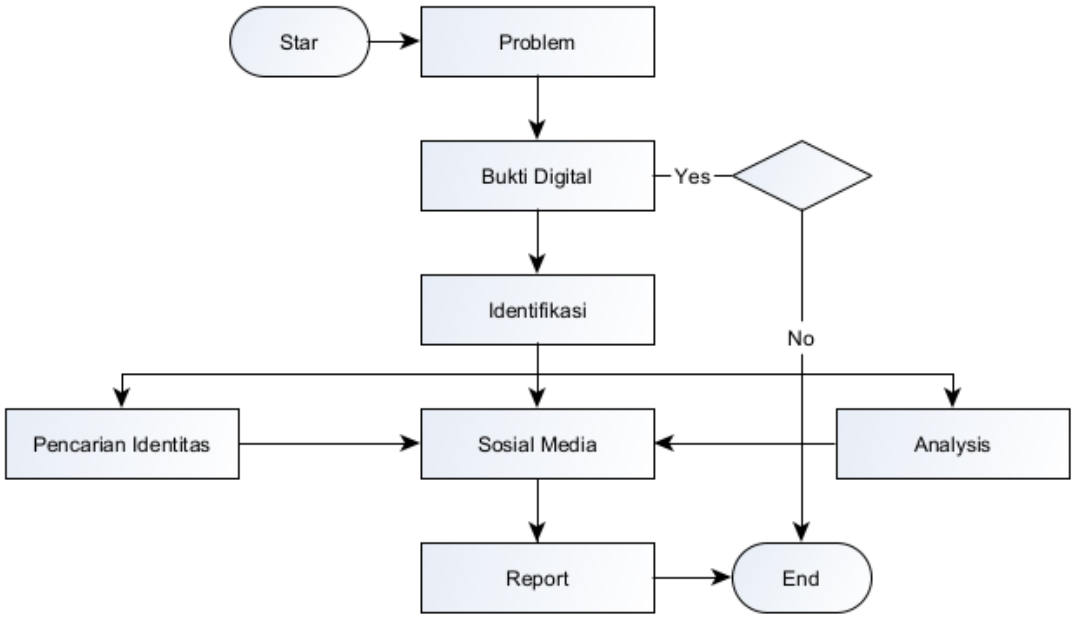
Dalam memperoleh barang bukti, investigator terlebih dahulu melakukan identifikasi terhadap informasi dan objek yang memiliki keterkaitan dengan perkara. Tahap ini dapat mencakup pengamatan lokasi, pemeriksaan dokumen, wawancara, serta penelusuran terhadap objek yang diduga berkaitan dengan tindak pidana. Tujuannya adalah menentukan bukti apa yang relevan dan bagaimana bukti tersebut dapat mendukung konstruksi perkara. Investigasi yang sistematis diperlukan agar proses pencarian tidak dilakukan secara sembarangan dan agar setiap barang atau informasi yang ditemukan dapat dikaitkan dengan konteks peristiwa secara objektif.

Setelah barang bukti ditemukan, tahap berikutnya adalah pengumpulan dan pengamanan barang bukti. Dalam proses ini, kondisi awal barang bukti perlu dijaga sehingga tidak mengalami perubahan, kerusakan, atau kontaminasi yang dapat memengaruhi hasil pemeriksaan. Pada barang bukti digital, misalnya, proses identifikasi, pengumpulan, akuisisi, dan preservasi perlu dilakukan secara terstruktur karena perubahan terhadap data dapat memengaruhi keabsahan dan keandalan hasil pemeriksaan. Proses mengenai forensik digital menunjukkan bahwa penggunaan kerangka investigasi tertentu dapat membantu investigator memperoleh bukti secara sistematis dan menjaga integritas data yang diperoleh.

Barang bukti yang telah dikumpulkan kemudian dianalisis untuk mengetahui informasi yang terkandung di dalamnya serta keterkaitannya dengan perkara. Analisis dapat dilakukan melalui pemeriksaan forensik terhadap benda fisik maupun perangkat dan data digital.

Sebagai contoh, proses forensik digital menunjukkan bahwa data yang tersisa pada perangkat dapat memberikan informasi yang relevan meskipun pengguna telah menggunakan fitur tertentu yang dirancang untuk mengurangi penyimpanan riwayat aktivitas. Oleh karena itu, hasil investigasi tidak cukup hanya berupa penemuan suatu benda, tetapi harus disertai analisis yang mampu menjelaskan relevansi benda atau informasi tersebut terhadap peristiwa yang sedang diselidiki.

Proses ini akan menjelaskan bagaimana cara menjalankan sebuah *framework* baru yang sudah dibangun dan langsung akan diimplementasikan melalui *flowchart* yang tersusun sesuai dengan kinerja investigasi.



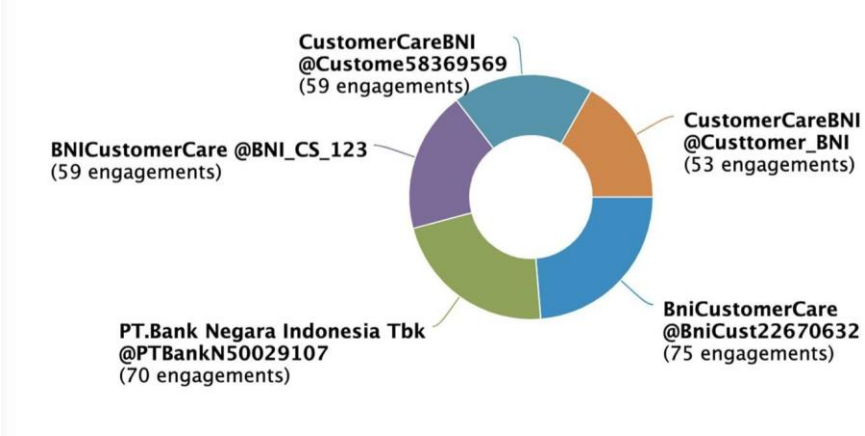
Gambar 4.1 *Flowchart* alur kerja investigasi

Dari gambar 4.1 menjelaskan tentang alur kinerja investigasi pada social media mulai dari masalah yang ada sampai ke laporan. Dalam suatu investigasi maka harus jelas permasalahan yang akan ditelusuri dan mempunyai barang bukti yang jelas dan akurat, barang bukti tersebut baik itu berbentuk digital ataupun dokumentasi, dan kalau barang buktinya tidak jelas atau tidak kuat maka proses pemecahan masalah tersebut tidak bisa ditindak lanjuti tapi kalau barang buktinya sudah jelas maka selanjutnya akan diidentifikasi sesuai dengan barang bukti tersebut. Pada investigasi ini yang akan dicari adalah identitas akun social media yang digunakan baik itu nama, alamat, email dan banyak yang lainnya yang mencakup dari akun tersebut, kalau sudah didapatkan identitas tersebut dan sesuai dengan permasalahan yang ada maka dibuatkan laporan yang akan dilaporkan ke badan hukum untuk di sidang sesuai

dengan undang-undang ITE tahun 2008 pasal 30 ayat (2) yang berbunyi “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik”.

4.1 Problem

Banyaknya kejadian telah terjadi di social media berbagai macam penipuan berdalih mengaku sebagai reseller instansi perusahaan yang akan bisa mengambil data targetnya. Sehingga mengakibatkan nasabah memberikan identitas dan pin yang ada pada rekening pemiliknya. Seperti masalah pada gambar dibawah ini salah satu instansi bank banyak akun-akun palsu yang meresahkan nasabah.



Gambar 4.2 Akun-akun Palsu *CustumerCare* BNI di *twitter*

Pada gambar diatas yang dikutip dari proses (DronEmperit) banyaknya akun-akun palsu yang mengaku *CostumerCare* BNI untuk menipu nasabah tiada lain adalah untuk menjerumuskan targetnya baik itu dalam bentuk pengambilan data ataupun pemerasan dan pada akhirnya akan merugikan nasabah.

Adapun telah terjadi penipuan akun yang mengatasnamakan CostumerCareBNI online menghubungi target supaya bisa berkomunikasi sampai target menyerahkan identitasnya seperti pin, nomor rekening dan lain sebagainya yang bisa dimanfaatkan oleh si pelaku.

4.2 Barang Bukti Digital

Barang bukti sudah diambil dari hasil komunikasi lewat social media twitter yang bagaimana akun tersebut memberikan nomor whatsapp pribadinya sebagai komunikasi lanjutannya.

Gambar 4.3 Barang Bukti Digital postingan Akun Palsu *Custumercare* BNI

Dari gambar 4.3. menjelaskan tentang percakapan akun palsu *CostumerCareBNI (@Costumer17214490)* dengan akun atas nama *@andrybrew*. Percakapan tersebut mulai dari antrian panjang di kantor resmi BNI sehingga mengambil jalan pintas melalui media, sehingga akun palsu tersebut memberi arahan dengan menghubungi nomor whatsapp pribadinya.

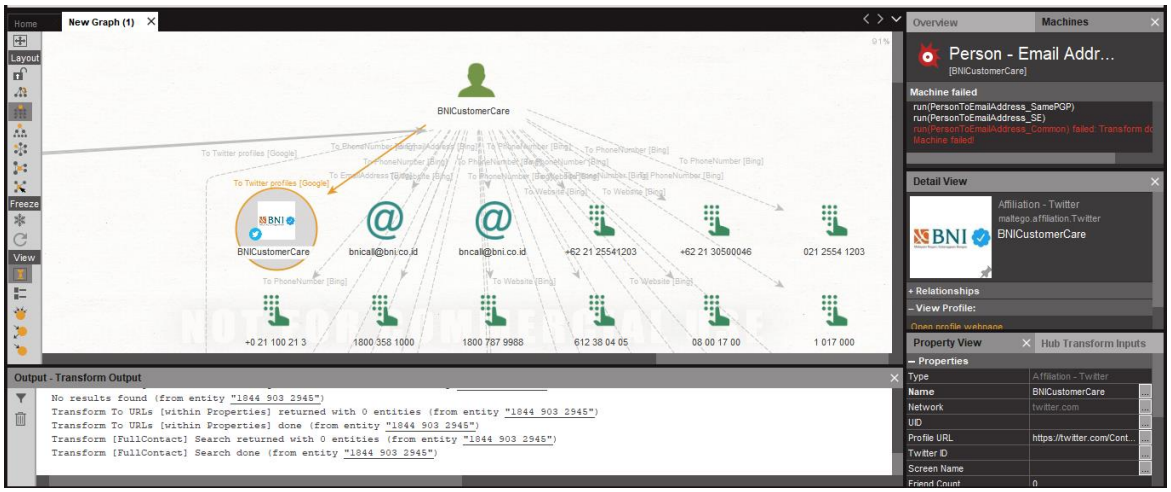
Adapun barang bukti digital yang didapatkan dari postingan tersebut adalah sebuah akun palsu atas nama *CostumerCareBNI (@Costumer17214490)* dan Bnicotumercare *(@Bnicust81490598*) dan tanggal pengirimannya.

4.3 Identifikasi

Sesuai dengan permasalahan dan barang bukti diatas maka dari itu perlu ditindaklanjuti dengan mencari kebenaran akun tersebut, apakah memang benar dari pihak instansi atau orang lain yang mengaku customer BNI.

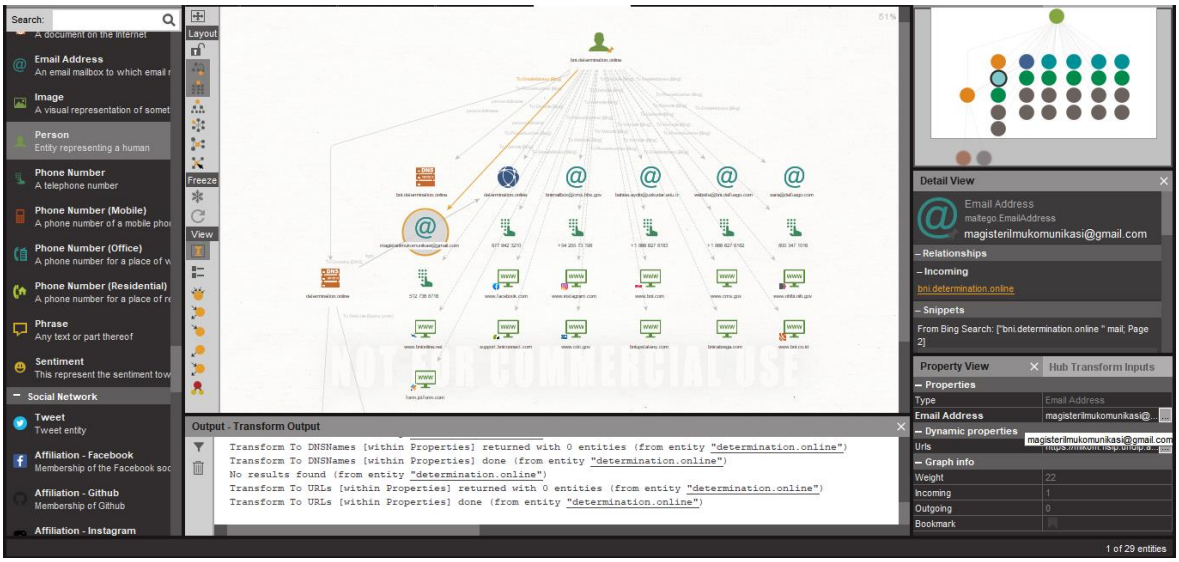
4.4 Pencarian Identitas

Dari permasalahan diatas tentang akun yang mengatasnamakan instansi pemerintah yang meresahkan masyarakat akan menimbulkan penipuan untuk pengambilan entitas orang lain ataupun pemerasan sehingga perlu di ketahui keaslian akun tersebut supaya bisa di laporkan ke pihak hukum untuk diproses. Adapun kasus ini peneliti ambil dari permasalahan nasabah yang sudah tertipu sama akun *twitter CostumerCareBNI (@Costumer17214490)* dan Bnicotumercare *(@Bnicust81490598)*. Maka akan dicari keaslian akun tersebut dengan cara mengclosing datanya melalui aplikasi maltego sehingga nama, akun, lokasi dan tanggal pengirimannya kita bisa verifikasi sesuai dengan data yang didapatkan.



Gambar 4.4 Hasil Pencarian Data 1

pada gambar 4.4. di atas menjelaskan hasil pencarian data pada media digital akun BNICustomerCare yang asli dari instansi bank, hasil yang didapatkan dari identifikasi *detail view adalah email address, twitter, phone number* dan *website* resminya.



Gambar 4.5 Hasil Pencarian Data 2

Dari hasil pencarian data di atas menjelaskan tentang pencarian data akun bni.determination.online, data yang didapatkan dari hasil investigasi akun tersebut adalah *email address, dns, website,* dan *facebook.* Dari barang bukti yang didapatkan tidak sesuai dengan keaslian datanya, seperti halnya *email addres* dan *websitenya* menggunakan tidak resmi.

4.5 Sosial Media

Pada social media yang digunakan sesuai dengan masalah ini adalah twitter yang dimana twitter tersebut adalah platform jaringan social masa kini yang digunakan banyak orang. Jaringan sosial ini banyak manfaatnya baik itu digunakan sebagai media informasi, media komunikasi dan membuat story yang bisa dilihat secara umum dan berbentuk terbuka, begitu juga dengan segi negatifnya, bisa membuat akun banyak baik personal maupun kelompok sehingga orang bisa memanfaatkan untuk menipu orang lain memakai dengan akun mengatasnamakan pihak instansi atau pemerintah. Secara setandar media twitter ini bisa dilihat oleh umum namun pengguna dapat membatasi pengiriman hanya bagi pengikutnya saja.

4.6 Analysis

Akun social media yang menjadi target investigasi akan dianalisis lebih lanjut untuk memastikan kesalahan yang dilakukan oleh pelaku kejahatan dengan cara crawling data

menggunakan aplikasi maltego untuk mencari identitas pelaku. Sehingga pelaku dipastikan bersalah dari hasil analisis dan barang bukti yang riil dan lengkap terstruktur.

Pada akun twitter yang akan di analisa disini ada 2 akun yang pertama akun palsu dan akun asli milik Bank BNI Customer Care, sehingga hasilnya bisa diketahui sesuai dengan data yang didapatkan.

4.7 Report

Dari hasil penyelidikan investigasi maka akun tersebut memang bukan dari bank BNI hanya orang yang tidak bertanggung jawab membuat akun tersebut, karena dari hasil perbandingan data yang didapatkan baik dari akun bank BNI asli ataupun akun BNI palsu banyak perbedaan.

4.8 Hasil Analisa Framework

Dari analisa pengembangan *framework* sebelumnya dengan *framework* yang dibuat sekarang, maka hasil kesimpulan perbandingan didapatkan dari Prosesnya pada tabel 4.9.

Tabel 4.1 Analisa *Framework*

No	Proses *Framework*	*Framework Digital Forensic Investigation (FDFI)*	*Digital Forensics Investigation Model (DFIM)*	*Digital Forensics Analysis Team (DFAT)*
1	*Notification*	√	x	√
2	*Authorization*	√	x	√
3	*Preparation*	√	x	√
4	*Securing Documentation*	√	x	x
5	*Event Triggering*	√	x	x
6	*Preservation*	√	√	√
7	*Examination*	√	√	√
8	*Analysis*	√	√	√

9	*Documentation*	√	x	√
10	*Conclusion*	√	x	√
11	*Evaluation*	√	x	*x*

Tabel 4.1 menerangkan bahwa Proses-Proses yang digunakan pada pengambilan bukti digital berdasarkan hasil eliminasi framework sebelumnya. Proses FDFI tersebut Proses yang akan di kembangkan pada proses ini dan Proses DFIM, DFAT adalah Proses framework yang sudah dikembangkan sebelumnya, maka kesimpulannya adalah Proses yang mempunyai hasil ceklis (√) Proses yang bisa digunakan yang yang bertanda silang (x) Proses yang tidak bisa digunakan atau tidak sesuai dengan problem peneliti kembangkan.

4.9 Maintenance

Proses pemeliharaan ini merupakan proses pemeliharaan *framework* selama penggunaan investigasi. Tahap ini juga merupakan tahap pengecekan terhadap *framework* untuk terus memberikan dukungan terhadap penggunanya agar tetap mampu beroperasi secara benar melalui Proses-Proses dalam *framework* yang telah dikembangkan sesuai dengan kebutuhan. Adapun input dan output pada pemeliharaan ini terdapat pada tabel dibawah ini.

Tabel 4.2 Input, Proses dan Output Pemeliharaan

Input	Proses	Output
Framework FDFI	SDLC	Pemeliharaan dan pengecekan kembali *framework* yang sudah jadi.

BAB V
FRAMEWORK

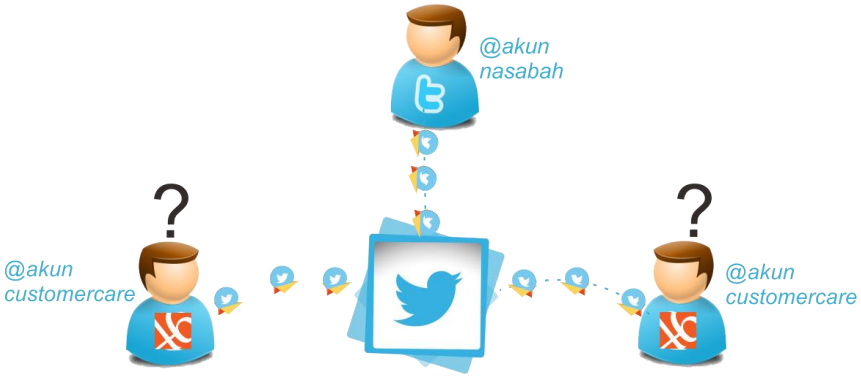
framework ini akan melihat keberhasilan kinerja dari *framework* dalam investigasi social media untuk mendapatkan barang bukti digital pada twitter. Adapun testing *framework* ini dibagi menjadi 2 bagian yaitu :

5.1 Simulasi *framework*

Pada Proses ini peneliti akan uji coba *framework* yang sudah jadi dan akan dikembangkan dengan menggunakan tools maltego.

- Kronologi

Adapun kronologi masalahnya adalah salah satu akun twitter yang mengatasnamakan instansi pemerintah yaitu Bank BNI sebagai Customer care dan melayani nasabah secara online. Adapun akun yang digunakan pada customer online ini sangat mirip dengan akun asli milik bank BNI.



Gambar 5.1 Ilustrasi publikasi akun *twitter*

- Pengiriman Pesan Nasabah

Pengiriman pesan dilakukan oleh nasabah BNI ke twitter dengan mention salah satu akun BNI Customer Care meminta bantuan dalam penyelesaian ATM yang terblokir maka pesan tersebut dibalas dengan cepat oleh akun customer BNI tersebut dengan melampirkan nomor WA untuk menghubunginya lebih lanjut.

Gambar 5.2 Bukti screen balasan pesan *BNIcustomercare*

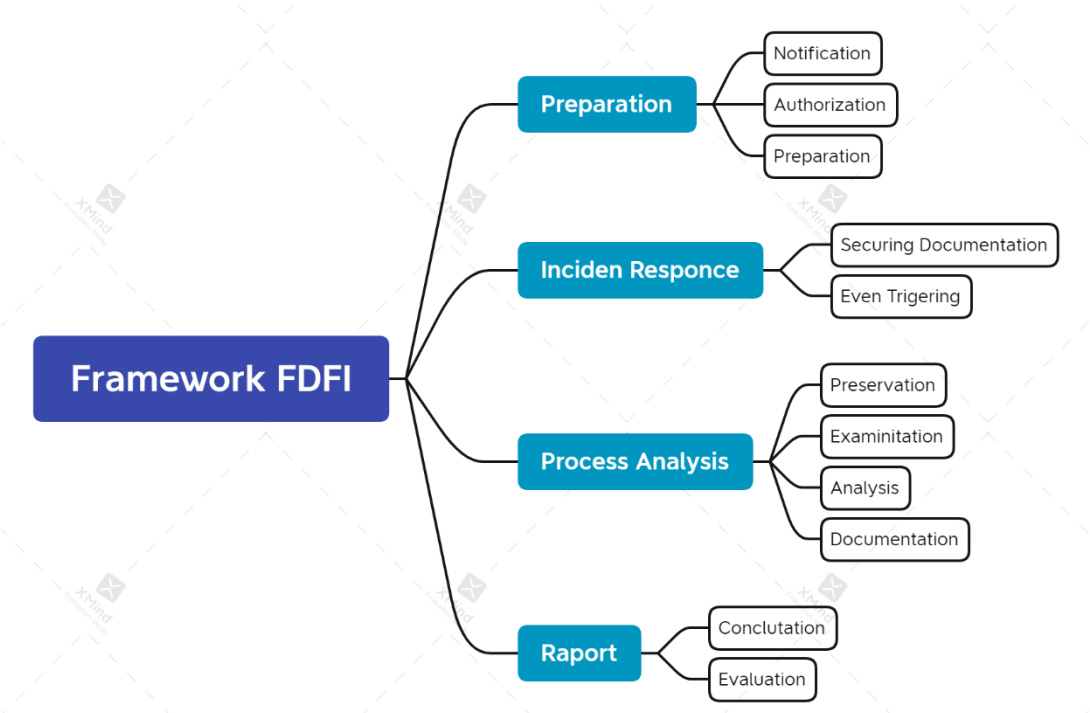
- Bukti digital yang dapatkan

  Bukti digital ini diambil dari screen pesan tersebut adalah :

  - ✓ Akun twitter : *@BNIcutomercare*
  - ✓ Nomor WA : 083817752223
  - ✓ Nama : bayu
  - ✓ Waktu pengirim : 8:24 AM
  - ✓ Tanggal : 10 Maret 2021

5.2 Analysis *framework*

Penanganan barang bukti digital yang sudah ditemukan, maka akan diproses dengan menggunakan *framework* yang akan di kembangkan.



Gambar 5.3 *Framework* yang dikembangkan

Berikut penjelasan proses penanganan investigasi social media terhadap studi kasus dengan menggunakan *framework* yang akan dikembangkan.

1. ***Preparation***

Proses pertama yang dilakukan dalam investigasi ini adalah menyiapkan segala sesuatu kebutuhan dalam penyidikan social media, adapun beberapa Proses yang siapkan adalah :

1.1. *Notification,* tahap ini Proses yang mempersiapkan berkas laporan tentang adanya kasus kejahatan di media sosial, misalnya menyiapkan laporan pengaduan ke pihak jaksa hukum. Laporan pengaduan bertujuan sebagai bahan dasar tentang adanya tindak kejahatan sehingga perlu diadakan investigasi sesuai kejadian perkara dalam mekanisme penyidikan.

1.2. *Authorization,* tahap ini harus memiliki hak dalam melakukan proses investigasi secara sah menurut hukum yang berlaku, misalnya memiliki surat perintah penyidikan dari pihak yang berwenang dan memiliki API Key developer twitter dengan meminta ke pihak admin developer twitter, adapun surat perintah harus sesuai dengan konten penyidikan yang akan dilakukan, misalnya menyita barang bukti atau melakukan hak akses untuk menganalisa akun sosial media yang akan didapatkan.

1.3. *Preparation*, menyiapkan segala kebutuhan dalam proses investigasi misalnya menyiapkan alat perangkat keras, software/tools dan jaringan internet.

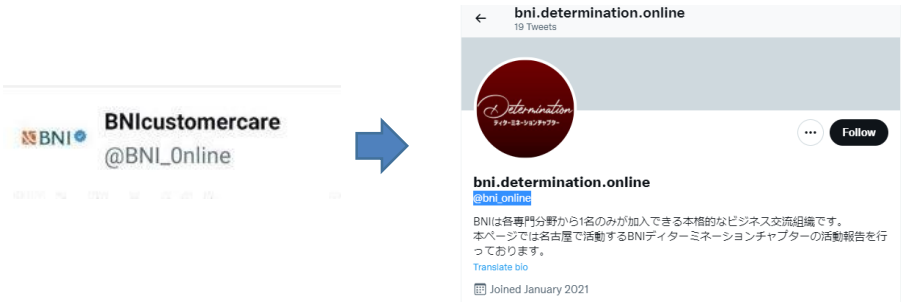
Tabel 5.1 Spesifikasi Perangkat

No	Nama Perangkat	Spesifikasi Minimal
1.	Komputer / Laptop a. Processor b. VGA Card c. Memory	 Core i3 AMD A4 4144 MB
2.	Software a. Sistem Operasi b. Maltego c. Sosial Media	 Windows 10 Pro 64 V 4.3.0 *free* Twitter

2. *Incident Response*

Pada Proses ini adalah aktivitas yang dilakukan disaat investigasi dalam kejadian perkara, maka ada beberapa Proses yang akan dilakukan didalam kejadian yaitu :

a. *Securing Documentation,* sebuah proses investigasi melakukan pengamanan barang bukti digital seperti akun media sosial twitter, screen kasus kejadian dan lain-lain yang bersangkutan dengan lokasi kejadian.



Gambar 5.4 Barang bukti akun *twitter*

Barang bukti digital diatas menjelaskan tentang akun twitter yang digunakan oleh pelaku, akun tersebut sudah melakukan perubahan sejak kejadian tersebut tapi dari nama usernya masih sama yaitu *@bni_online* .

b. *Event Triggering* pada saat kejadian maka akan di cari hubungan antara bukti digital lainnya sebagai bahan identifikasi dengan pelaku kejahatan, adapun barang bukti digital lainnya yang sudah dilakukan oleh pelaku ada pada gambar 4.13.

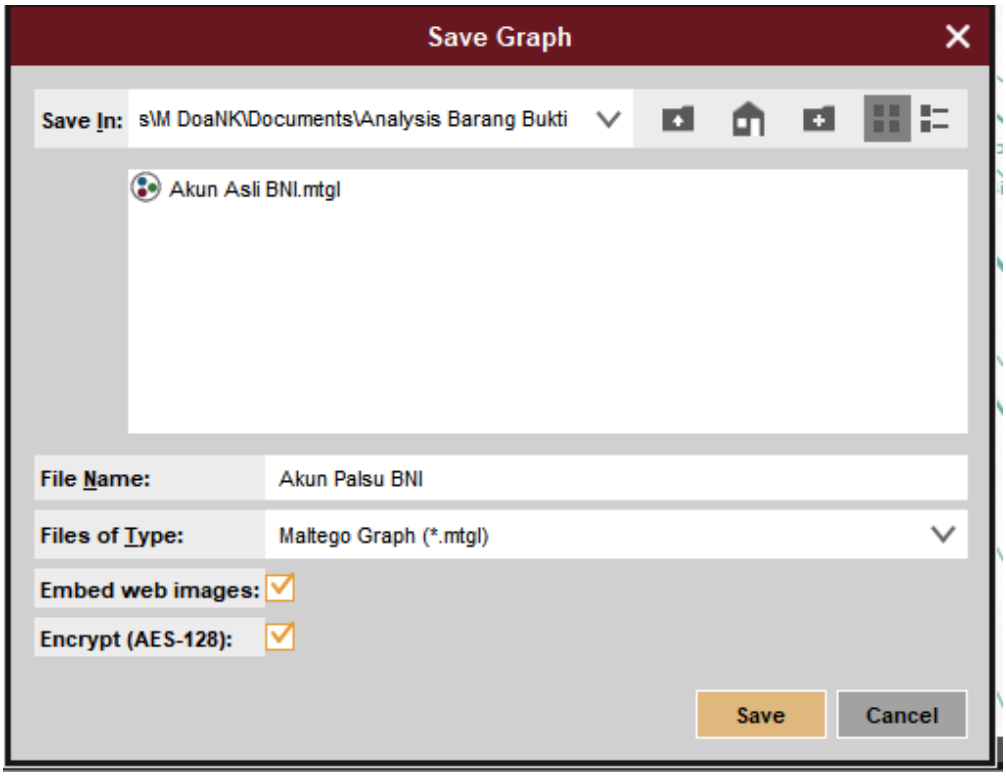
Gambar 5.5 Ikatan kejahatan dengan orang lain

Gambar diatas menerangkan banyak orang menjadi korban penipuan oleh akun tersebut sehingga dapat menjadi barang bukti tambahan untuk investigasi lebih lanjut.

3. *Process Analysis*

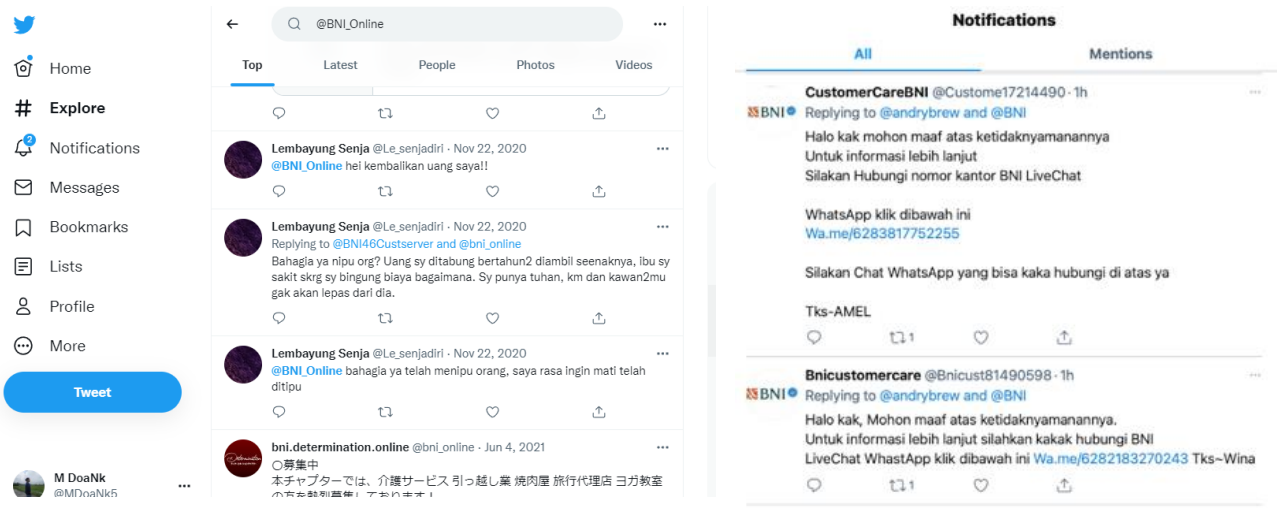
Proses ini akan menganalisis dari barang bukti yang sudah didapatkan pada Proses sebelumnya sesuai dengan permasalahan yang ada menggunakan tools maltego.

a. *Preservation* barang bukti digital yang telah ditemukan akan diamankan supaya barang bukti yang diperoleh tidak terkontaminasi atau perubahan pada barang bukti yang lain. Untuk penyimpanan barang bukti digital yang sudah dianalisis dengan maltego maka akan diamankan dengan baik dan aman sesuai type maltego yaitu (*mtgf) dan ter enkripsi AES-128. Dari hasil penyimpanan tersebut sehingga bisa terhindar dari pihak yang tidak memiliki kepentingan.



Gambar 5.6 Penyimpanan Barang Bukti Digital

b. *Examination* pelacakan barang bukti secara sistematis serta melakukan validasi terhadap barang bukti yang telah ditemukan seperti keterkaitannya barang bukti dengan akun pelaku. Dari hasil yang ditemukan cuitan yang bisa jadi barang bukti bahwa akun pelaku dapat dinyatakan penggunaan akun tindak kejahatan karena korban adalah lebih dari satu orang melainkan beberapa orang jadi korban tindak penipuan terhadap akun tersebut.

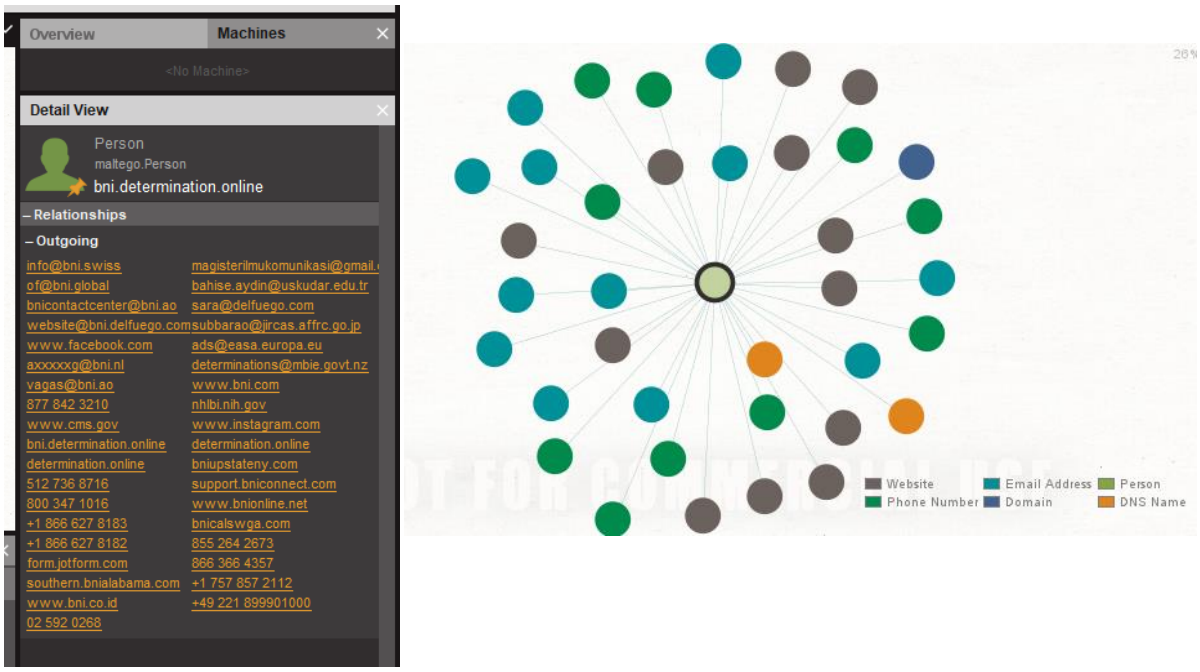


Gambar 5.7 Keterkaitan akun *twitter*

c. *Analysis* akan dilakukan analisa merekonstruksikan dan menarik kesimpulan terhadap barang bukti yang sudah ditemukan sehingga dapat menemukan bukti pendukung lainnya untuk mengembangkan proses investigasi yang dapat menjerat pelaku kejahatan atas akun palsu yang disebarkan.

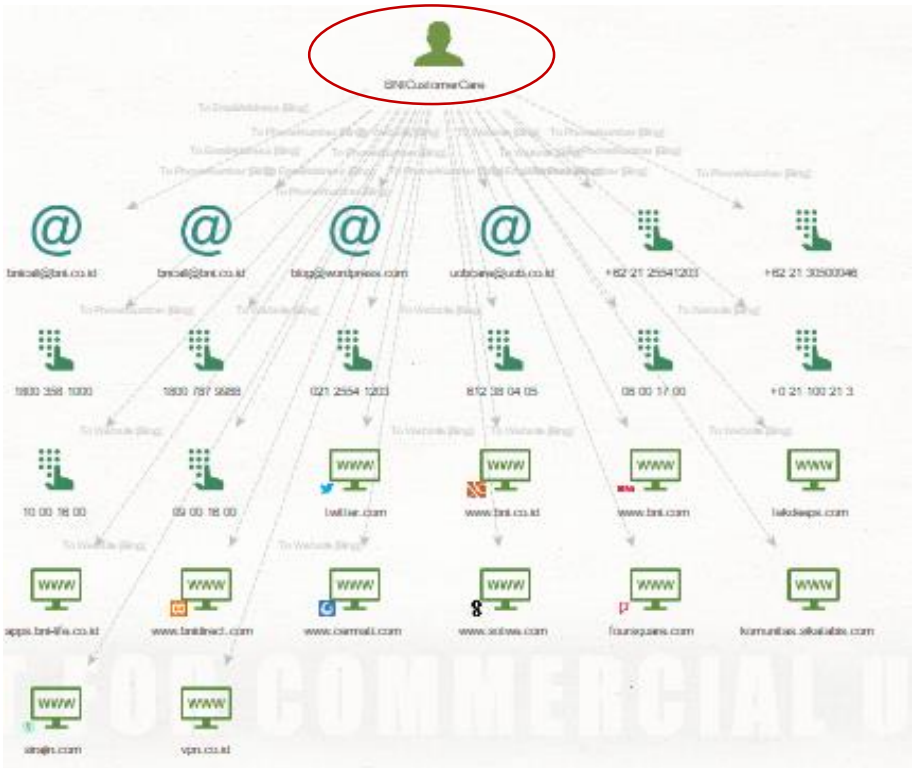
Gambar 5.8 Hasil temuan investigasi

Pada gambar 4.16 di atas menerangkan tentang hasil penemuan investigasi akun twitter yang bernama **bni.determination.online** dengan user ***@bni_online*** telah mendapatkan beberapa *entity* terkait penelusuran menggunakan tools maltego menggunakan *entitas person* dengan kata kunci *bni.determination.online.* adapun hasil yang didapatkan ada pada gambar 4.8.



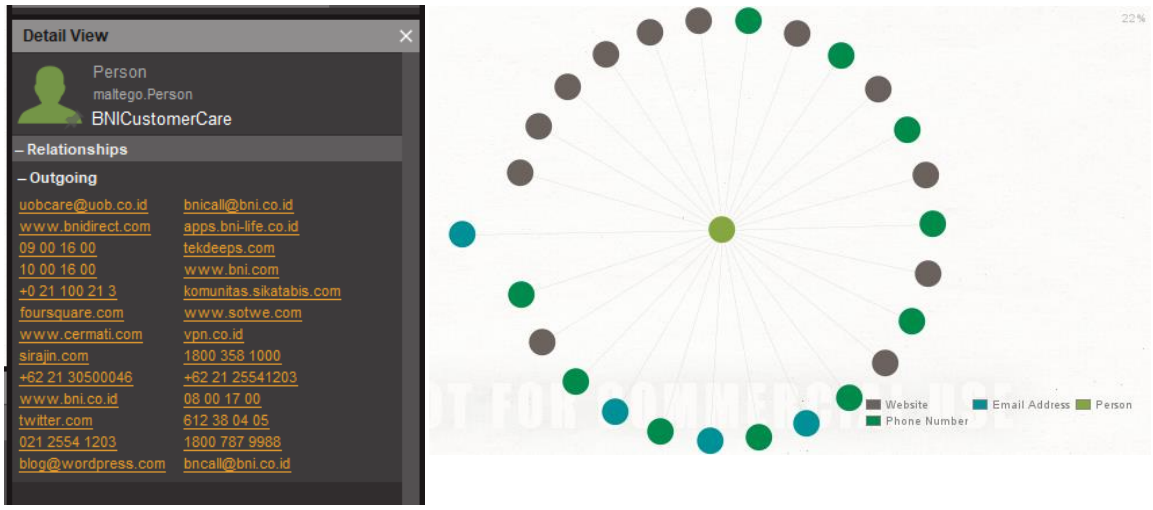
Gambar 5.9 *Detail view* dan *Layout entity*

Sedangkan hasil penelusuran akun dari twitter BNI dengan kata kunci *BNICutomerCare* menggunakan *entitas person* mendapatkan hasil pada gambar 5.10.



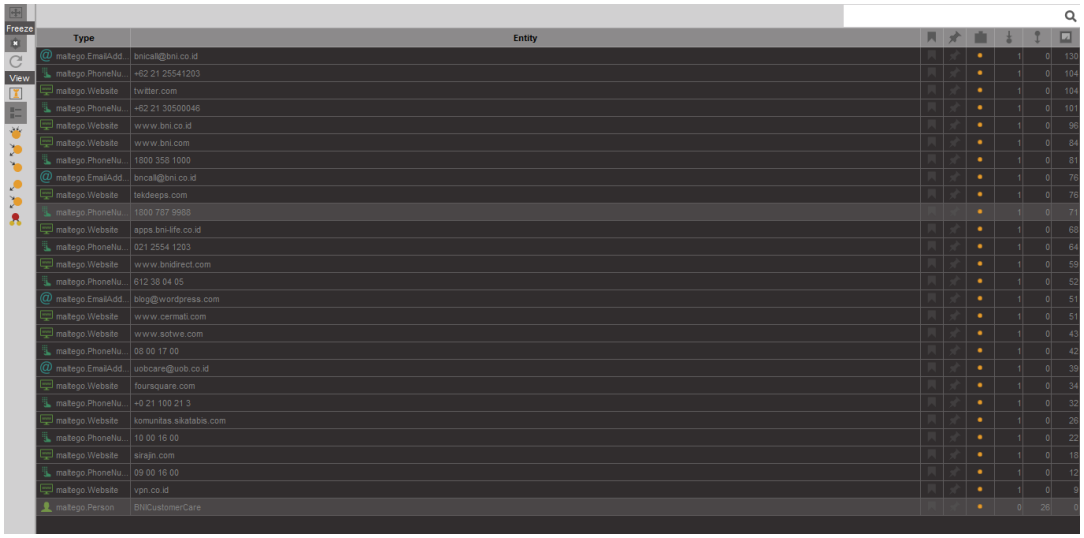
Gambar 5.10 Hasil temuan investigasi *BNICustomerCare*

Dari hasil penelusuran gambar 4.10 bahwa beberapa *entity* yang didapatkan sesuai dengan fakta yang ada yaitu *email address* dan *domain* yang di temukan asli dari pihak instansi BNI. Adapun detail viewnya ada pada gambar 5.11

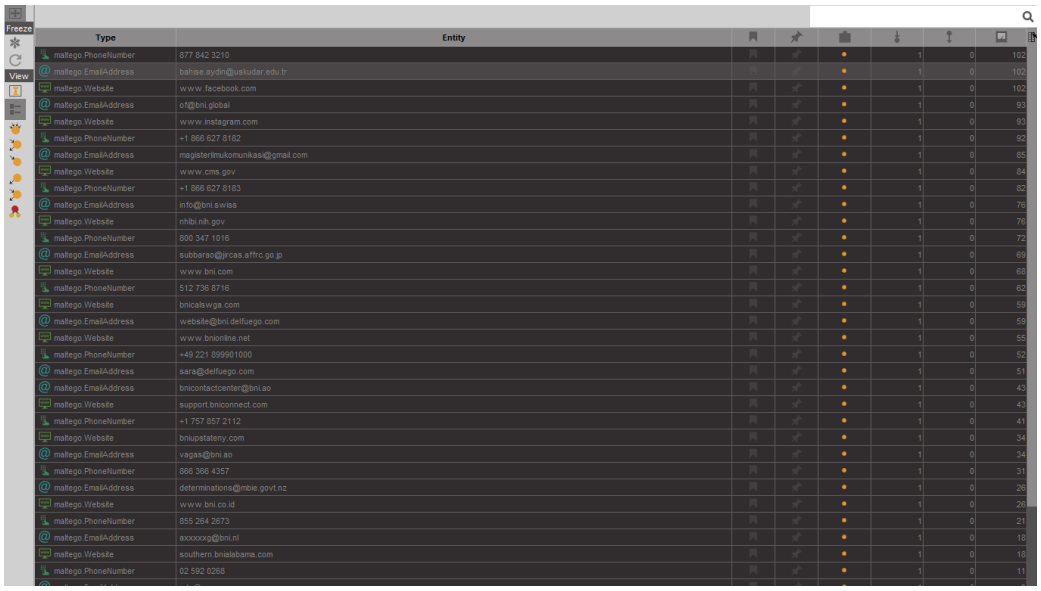


Gambar 5.11 *Detail view* dan *Layout entity BNICustomercare*

d. *Documentation* setelah melakukan analisa terhadap barang bukti yang sudah ditemukan maka tahap selanjutnya adalah mengamankan barang bukti yang telah ditemukan sebagai dokumentasi dalam pelaporan ke pihak hukum.



Gambar 5.12 *Screen* Dokumentasi barang bukti digital 1



Gambar 5.13 *Screen* Dokumentasi barang bukti digital 2

5.3 *Report*

Proses ini adalah Proses untuk penyusunan laporan akhir yang sudah ditemukan dalam investigasi. Barang bukti digital yang ditemukan akan diolah dan disusun untuk dijelaskan sesuai fakta yang ditemukan.

Tabel 5.2 Perbedaan Hasil Investigasi Akun

No	Akun Twitter	Entity	Entity Results	Authenticity
1	CustomerCareBNI	*Akun Twitter*	BNICustomerCare	√
	@ BNICustomerCare	*Website*	www.bni.co.id	√
			www.bni.com	√
			www.bnisekuritas.co.id	√
			www.bnidirect.com	√
		PhoneNumber	+62 21 25541203	√
			+62 21 30500046	√
			+0 21 100 21 3	√
		Email Address	bnicall@bni.co.id	√
2	bni.determination.online	*Email Address*	magisterilmukomunikasi@gmail.com	-
	@BNI_Online		bahise.aydin@uskudar.edu.tr	-
			website@bni.delfuego.com	-
		PhoneNumber	+54 255 73 198	-
			+1 866 627 8183	-
			+1 866 627 8182	-
		DNS	199.59.243.200	-
		Website	determination.online	-
		Facebook	https://www.facebook.com/BNI-Determination-104429321223541/ BNI	-

			Determination - Home | Facebook	

Penjelasan pada tabel 5.2 adalah akun twitter *@BNICustomerCare* mendapatkan entity *akun twitter, website, phone Number*, dan *email address* yang sesuai dengan data asli karena domain-domain yang digunakan *email address* ataupun *website* terbukti keabsahannya ke pemerintah. Adapun akun *@BNI_Online* yang terdiri dari entity yang didapatkan *email address, phone number, website, DNS,* dan *facebook* hampir sama entity yang didapatkan tetapi perbedaan *website* dan *email address* yang ditemukan tidak terbukti keabsahannya karena domain yang digunakan menggunakan *free domain* seperti *@gmail* dan *.online* .

4.1.Conclusion, bukti dan informasi yang ditemukan oleh investigator sudah cukup bukti bahwa akun yang digunakan tersangka adalah palsu, akun tersebut digunakan untuk mempengaruhi nasabah instansi bank BNI supaya data entitas target dapat diungkapkan seperti nomor ATM, PIN dan lain-lain yang mengakibatkan data entitas bisa diambil oleh pelaku.

4.2.Evaluation, Proses ini investigator melakukan evaluasi terhadap hasil temuan yang ditemukan sehingga proses kegiatan pelaku kejahatan dapat diketahui dengan jelas, dan apabila investigator mendapat kasus serupa, proses ini dapat dijadikan sebagai rujukan dalam proses investigasi pada sosial media.

BAB VI
MACAM-MACAM KEJAHATAN MEDIA SOSIAL

6.1 Phishing pada Media Sosial

Phishing merupakan salah satu bentuk kejahatan siber yang paling banyak digunakan untuk mendapatkan informasi sensitif pengguna melalui teknik manipulasi. Pada media sosial, phishing dapat muncul dalam bentuk pesan pribadi, komentar, email, notifikasi palsu, maupun tautan yang menyerupai halaman resmi. Pelaku biasanya membuat komunikasi yang terlihat meyakinkan agar korban memasukkan username, password, kode verifikasi, atau informasi pribadi. Pada Facebook, Instagram, TikTok, WhatsApp, dan Telegram, phishing dapat dilakukan dengan menyamar sebagai teman, administrator, petugas keamanan, atau pihak yang menawarkan hadiah dan layanan tertentu. Dari perspektif digital forensics, investigasi phishing dilakukan dengan mengidentifikasi pesan, waktu komunikasi, akun pengirim, alamat tautan, perangkat korban, serta perubahan aktivitas setelah korban berinteraksi dengan pesan tersebut. Investigator perlu menjaga bukti agar tidak berubah dan membuat kronologi kejadian. Cara mengatasinya adalah tidak membuka tautan mencurigakan, memeriksa alamat situs sebelum memasukkan kredensial, menggunakan autentikasi multifaktor, serta tidak pernah memberikan kode verifikasi kepada pihak lain. Jika korban telah memasukkan kredensial pada situs yang mencurigakan, segera lakukan pengamanan melalui halaman resmi platform, ubah kata sandi, keluarkan sesi yang tidak dikenal, dan amankan email yang terhubung. Dalam lingkungan organisasi, edukasi phishing dan simulasi keamanan dapat dilakukan secara berkala. Dengan demikian, pertahanan terhadap phishing harus menggabungkan teknologi, kewaspadaan pengguna, kebijakan keamanan, serta prosedur respons insiden.

6.2 Social Engineering

Social engineering adalah kejahatan yang mengeksploitasi faktor manusia, bukan semata-mata kelemahan teknis sistem. Pelaku memanfaatkan kepercayaan, rasa takut, rasa ingin tahu, atau tekanan waktu untuk membuat korban melakukan tindakan yang menguntungkan pelaku. Pada media sosial, pelaku dapat membuat identitas palsu, berpura-pura menjadi teman, petugas layanan, rekan kerja, atau orang yang dikenal korban. Pelaku kemudian meminta informasi pribadi, kode autentikasi, uang, atau akses terhadap akun. Kejahatan ini

dapat terjadi pada Facebook, WhatsApp, Instagram, TikTok, maupun Telegram. Investigasi dilakukan dengan menganalisis pola komunikasi, identitas akun, waktu interaksi, perubahan perilaku akun, serta hubungan antara komunikasi dan kejadian keamanan. Investigator harus berhati-hati karena identitas akun media sosial belum tentu sama dengan identitas orang sebenarnya. Cara mengatasi social engineering adalah melakukan verifikasi identitas melalui saluran komunikasi lain sebelum memenuhi permintaan yang sensitif. Pengguna tidak boleh memberikan password, kode OTP, atau kode autentikasi kepada siapa pun. Informasi pribadi yang dipublikasikan juga perlu dibatasi karena dapat digunakan untuk membuat pendekatan yang lebih meyakinkan. Organisasi perlu memiliki prosedur verifikasi untuk permintaan perubahan rekening, password, akses sistem, atau informasi penting. Edukasi keamanan menjadi bagian utama pertahanan karena teknologi keamanan tidak akan efektif apabila pengguna dengan mudah menyerahkan informasi rahasia. Dengan menerapkan prinsip verifikasi dua arah dan least privilege, risiko social engineering dapat dikurangi secara signifikan.

6.3 Account Takeover atau Pengambilalihan Akun

Account takeover adalah kondisi ketika pihak yang tidak berwenang berhasil memperoleh kendali terhadap akun media sosial seseorang. Kejahatan ini dapat terjadi akibat kredensial yang bocor, phishing, social engineering, penggunaan password yang sama, perangkat yang tidak aman, atau penyalahgunaan sesi login. Setelah memperoleh akses, pelaku dapat mengubah informasi akun, mengirim pesan kepada kontak korban, melakukan penipuan, menghapus konten, atau menggunakan identitas korban untuk aktivitas lain. Dalam investigasi digital, indikator account takeover antara lain adanya login dari perangkat tidak dikenal, perubahan email atau nomor telepon, perubahan password, pesan yang tidak dibuat korban, dan aktivitas pada waktu yang tidak sesuai dengan kebiasaan pengguna. Investigator harus menyusun timeline untuk mengetahui kapan aktivitas normal berubah menjadi aktivitas mencurigakan. Cara mengatasinya adalah mengaktifkan autentikasi multifaktor, menggunakan password unik, memeriksa perangkat atau sesi yang sedang aktif, serta mengamankan email dan nomor telepon yang terhubung. Apabila akun telah diambil alih, pemilik harus menggunakan prosedur pemulihan resmi platform dan segera menginformasikan kepada kontak apabila terdapat pesan mencurigakan yang dikirim dari akun tersebut. Jangan melakukan tindakan balasan terhadap pelaku karena dapat memperburuk keadaan dan menghilangkan bukti. Organisasi perlu memiliki prosedur

account recovery dan incident response yang terdokumentasi. Dengan monitoring dan autentikasi berlapis, peluang keberhasilan pengambilalihan akun dapat ditekan.

6.4 Penipuan Online melalui Media Sosial

Penipuan online merupakan kejahatan yang memanfaatkan media sosial untuk memperoleh keuntungan secara tidak sah. Bentuknya sangat beragam, mulai dari toko daring palsu, investasi palsu, giveaway palsu, penjualan barang fiktif, hingga permintaan transfer dengan alasan tertentu. Pelaku dapat menggunakan akun yang terlihat profesional dan memiliki foto, testimoni, serta jumlah pengikut yang dibuat seolah-olah meyakinkan. Facebook, Instagram, TikTok, WhatsApp, dan Telegram sering digunakan sebagai media komunikasi antara pelaku dan korban. Dalam investigasi, informasi penting meliputi identitas akun, nomor telepon, rekening atau metode pembayaran, waktu transaksi, percakapan, bukti transfer, URL, dan konten yang digunakan pelaku. Bukti tersebut perlu disimpan dan didokumentasikan secara sistematis. Cara mengatasi penipuan adalah melakukan verifikasi identitas penjual atau pihak yang menawarkan layanan, memeriksa reputasi, tidak mudah percaya terhadap keuntungan yang tidak masuk akal, dan tidak melakukan transfer hanya berdasarkan tekanan komunikasi. Untuk organisasi, transaksi harus melalui prosedur verifikasi dan persetujuan yang jelas. Apabila seseorang menjadi korban, jangan menghapus komunikasi karena dapat menjadi bukti penting. Simpan bukti transaksi dan laporkan melalui saluran resmi yang tersedia. Dalam perspektif forensik, korelasi antara akun, nomor telepon, rekening, waktu komunikasi, dan transaksi dapat membantu membangun kronologi kejadian. Pencegahan terbaik adalah kombinasi literasi digital, verifikasi identitas, keamanan transaksi, dan dokumentasi bukti.

6.5 Identity Theft atau Pencurian Identitas

Identity theft terjadi ketika informasi identitas seseorang digunakan tanpa izin untuk melakukan aktivitas tertentu. Media sosial menyediakan banyak informasi yang dapat dimanfaatkan untuk membentuk profil seseorang, seperti nama, foto, pekerjaan, sekolah, lokasi umum, hubungan sosial, dan aktivitas sehari-hari. Pelaku dapat menggunakan informasi tersebut untuk membuat akun palsu, melakukan penipuan, atau menyamar sebagai korban. Investigasi digital terhadap pencurian identitas dilakukan dengan membandingkan akun yang diduga palsu dengan akun asli, menganalisis waktu pembuatan akun, konten, pola komunikasi, gambar profil, serta hubungan dengan akun lainnya. Investigator perlu

membedakan antara kesamaan nama dan bukti identitas karena banyak orang dapat memiliki nama yang sama. Pencegahan dilakukan dengan membatasi informasi pribadi yang dipublikasikan secara terbuka, menggunakan pengaturan privasi, dan tidak mengunggah dokumen identitas atau informasi sensitif. Foto profil dan informasi publik juga perlu dipertimbangkan karena dapat digunakan oleh pihak lain untuk membuat akun tiruan. Jika menemukan akun yang menyamar, pengguna dapat menggunakan mekanisme pelaporan resmi platform dan menyimpan bukti sebelum konten berubah atau dihapus. Organisasi juga perlu melakukan verifikasi identitas sebelum memberikan akses berdasarkan permintaan melalui media sosial. Dalam konteks forensik, pencurian identitas harus dianalisis berdasarkan kumpulan bukti, bukan hanya kemiripan visual. Dokumentasi dan korelasi berbagai artefak digital menjadi faktor penting untuk membangun kesimpulan yang dapat dipertanggungjawabkan.

6.6 Cyberbullying dan Pelecehan Digital

Cyberbullying merupakan tindakan intimidasi, penghinaan, ancaman, atau pelecehan yang dilakukan melalui teknologi digital. Media sosial memungkinkan tindakan tersebut dilakukan secara berulang dan dapat menjangkau banyak orang dalam waktu singkat. Bentuknya dapat berupa komentar menghina, penyebaran rumor, pembuatan akun palsu, pengiriman pesan mengganggu, atau penyebaran konten yang mempermalukan korban. Investigasi cyberbullying perlu memperhatikan kronologi, identitas akun, isi komunikasi, frekuensi tindakan, serta hubungan antara pelaku dan korban. Bukti berupa pesan, komentar, tautan, nama akun, waktu kejadian, dan dokumentasi konten dapat membantu proses pemeriksaan. Cara mengatasinya adalah menggunakan fitur block, restrict, report, dan pengaturan privasi yang tersedia pada platform. Korban sebaiknya tidak membalas dengan tindakan agresif karena dapat memperpanjang konflik dan menciptakan bukti tambahan yang merugikan. Jika tindakan mengandung ancaman atau bentuk pelanggaran serius, korban perlu melibatkan orang dewasa tepercaya, institusi yang berwenang, atau pihak profesional sesuai kondisi. Dalam organisasi pendidikan, sekolah atau kampus perlu memiliki kebijakan penanganan cyberbullying. Dari perspektif digital forensics, bukti harus dipreservasi sebelum akun atau konten berubah. Investigator perlu menjaga kerahasiaan informasi korban dan hanya mengumpulkan data yang relevan. Penanganan cyberbullying harus menggabungkan aspek teknologi, perlindungan korban, edukasi, dan mekanisme pelaporan.

6.7 Penyebaran Malware melalui Media Sosial

Malware adalah perangkat lunak berbahaya yang dirancang untuk melakukan tindakan tidak sah pada sistem atau perangkat. Media sosial dapat digunakan sebagai sarana distribusi malware melalui tautan, file, aplikasi palsu, atau pesan yang menarik perhatian korban. Pelaku dapat menyamarkan file atau tautan seolah-olah berupa foto, dokumen, hadiah, aplikasi, atau informasi penting. Ketika korban berinteraksi dengan konten tersebut, perangkat dapat mengalami gangguan keamanan. Dalam investigasi, pemeriksaan dapat mencakup waktu interaksi, perangkat yang digunakan, file yang diterima, aktivitas aplikasi, perubahan sistem, serta komunikasi yang terjadi sebelum dan setelah kejadian. Investigator harus menggunakan lingkungan analisis yang aman dan tidak menjalankan file mencurigakan pada perangkat kerja biasa. Cara mengatasi risiko malware adalah memperbarui sistem operasi dan aplikasi, menggunakan perangkat lunak keamanan, menghindari instalasi dari sumber tidak terpercaya, serta tidak membuka file mencurigakan. Pengguna juga perlu melakukan backup data penting secara berkala. Organisasi harus menerapkan endpoint protection, access control, dan kebijakan instalasi perangkat lunak. Jika perangkat diduga terinfeksi, jangan langsung menghapus seluruh data karena tindakan tersebut dapat menghilangkan bukti investigasi. Perangkat sebaiknya ditangani berdasarkan prosedur incident response. Dengan pertahanan berlapis dan pengelolaan perangkat yang baik, risiko malware melalui media sosial dapat dikurangi.

6.8 Doxxing atau Penyebaran Data Pribadi

Doxxing adalah tindakan menyebarkan informasi pribadi seseorang kepada publik tanpa persetujuan dengan tujuan tertentu, termasuk intimidasi atau pelecehan. Informasi yang dapat disalahgunakan antara lain nomor telepon, alamat, tempat kerja, identitas keluarga, atau informasi pribadi lainnya. Media sosial dapat mempercepat penyebaran informasi tersebut karena konten dapat dibagikan dan disalin oleh banyak pengguna. Dalam investigasi, investigator perlu mengidentifikasi sumber awal informasi, waktu publikasi, akun yang menyebarkan, jaringan penyebaran, serta bukti bahwa informasi tersebut berkaitan dengan korban. Pencegahan dilakukan dengan membatasi informasi pribadi yang dipublikasikan, memeriksa pengaturan privasi, dan menghindari publikasi dokumen yang mengandung informasi sensitif. Pengguna juga perlu berhati-hati ketika membagikan lokasi atau informasi rutinitas secara terbuka. Jika terjadi doxxing, dokumentasikan konten dan gunakan mekanisme pelaporan platform. Jangan menyebarluaskan kembali data pribadi

tersebut karena dapat memperbesar dampak terhadap korban. Organisasi perlu memiliki prosedur untuk menangani kebocoran informasi personal pegawai atau pelanggan. Dalam investigasi, data pribadi yang diperoleh harus disimpan secara aman dan hanya digunakan untuk tujuan yang sah. Prinsip data minimization sangat penting agar investigasi tidak justru memperluas penyebaran informasi. Penanganan doxxing membutuhkan kombinasi keamanan akun, perlindungan privasi, pelaporan, dan respons insiden.

6.9 Impersonation atau Penyamaran Akun

Impersonation merupakan tindakan menggunakan identitas orang atau organisasi lain tanpa izin. Pada media sosial, pelaku dapat membuat profil yang menggunakan nama, foto, logo, dan informasi yang menyerupai akun asli. Tujuannya dapat berupa penipuan, manipulasi reputasi, penyebaran informasi palsu, atau mendapatkan kepercayaan dari korban lain. Facebook, Instagram, TikTok, WhatsApp, dan Telegram dapat menjadi media penyamaran dengan karakteristik berbeda. Investigasi dapat dilakukan dengan membandingkan profil asli dan profil yang diduga palsu, termasuk waktu pembuatan akun, konten, pola komunikasi, hubungan akun, dan informasi publik lainnya. Kesamaan foto atau nama saja tidak cukup untuk memastikan bahwa akun tersebut palsu. Pencegahan dilakukan dengan mengaktifkan fitur keamanan akun, menggunakan identitas organisasi secara konsisten, serta melakukan monitoring terhadap akun yang menggunakan nama dan logo resmi. Organisasi dapat menggunakan kanal resmi untuk mengumumkan akun yang benar. Jika menemukan akun palsu, pengguna dapat menggunakan fitur pelaporan impersonation yang tersedia. Bukti harus didokumentasikan sebelum akun tersebut berubah atau dihapus. Investigator perlu memperhatikan chain of custody ketika menyimpan bukti. Dalam kasus organisasi, akun palsu dapat menimbulkan kerugian reputasi dan finansial sehingga respons harus dilakukan secara cepat tetapi terukur. Edukasi kepada pengikut mengenai akun resmi juga dapat mengurangi keberhasilan penyamaran.

6.10 Spam dan Scam melalui Media Sosial

Spam merupakan pengiriman komunikasi yang tidak diinginkan dalam jumlah besar, sedangkan scam adalah komunikasi yang dirancang untuk menipu korban. Keduanya dapat muncul dalam bentuk komentar, pesan pribadi, undangan grup, tautan promosi, atau iklan yang mencurigakan. Spam dapat menjadi tahap awal untuk mengarahkan pengguna kepada penipuan atau phishing. Pada platform seperti Facebook, Instagram, TikTok, WhatsApp, dan

Telegram, pelaku dapat memanfaatkan popularitas konten untuk menyebarkan pesan kepada banyak orang. Cara mengatasinya adalah menggunakan filter spam, membatasi siapa yang dapat mengirim pesan, memblokir akun mencurigakan, dan tidak berinteraksi dengan tautan yang tidak jelas. Pengguna juga perlu memahami bahwa jumlah pengikut, komentar, atau tampilan sebuah akun tidak otomatis membuktikan keasliannya. Dalam investigasi, pola pengiriman pesan, akun pengirim, waktu distribusi, URL, dan kesamaan isi pesan dapat digunakan untuk mengidentifikasi pola kampanye spam. Organisasi perlu memiliki sistem monitoring dan prosedur pelaporan untuk komunikasi berbahaya. Apabila terdapat scam, bukti komunikasi dan transaksi harus disimpan. Jangan menghapus percakapan sebelum dokumentasi dilakukan. Dari sisi keamanan, pendekatan paling efektif adalah filtering, user awareness, authentication, dan incident reporting. Spam mungkin terlihat sederhana, tetapi kampanye yang terorganisasi dapat menjadi pintu masuk bagi kejahatan yang lebih serius seperti phishing, pencurian identitas, atau penipuan finansial.

6.11 Penyebaran Berita Palsu dan Disinformasi

Disinformasi merupakan penyebaran informasi yang salah atau menyesatkan yang dapat memengaruhi persepsi publik. Media sosial memungkinkan informasi menyebar dengan cepat melalui fitur berbagi, repost, komentar, grup, dan rekomendasi algoritmik. Pelaku dapat menggunakan akun palsu atau jaringan akun untuk meningkatkan penyebaran suatu narasi. Investigasi disinformasi harus membedakan antara informasi salah yang disebarkan karena ketidaktahuan dan informasi yang sengaja dimanipulasi. Investigator perlu memeriksa sumber awal, waktu publikasi, konteks, bukti pendukung, serta perubahan konten selama penyebaran. Cara mengatasi disinformasi adalah melakukan fact-checking sebelum membagikan informasi, membandingkan beberapa sumber tepercaya, dan tidak menyebarkan konten hanya karena judulnya menarik atau emosional. Organisasi perlu memiliki prosedur komunikasi krisis agar dapat memberikan klarifikasi berdasarkan fakta. Dalam konteks digital forensics, preservation penting karena konten dapat dihapus atau diedit. Screenshot, URL, waktu pengamatan, dan informasi akun dapat menjadi dokumentasi pendukung. Namun, bukti tersebut perlu diverifikasi dan tidak boleh dianggap sebagai fakta tanpa pemeriksaan lebih lanjut. Literasi digital merupakan pertahanan utama terhadap disinformasi. Pengguna perlu memahami bahwa viralitas tidak sama dengan kebenaran. Dengan meningkatkan kemampuan verifikasi sumber dan konteks, dampak informasi palsu terhadap individu maupun organisasi dapat dikurangi.

6.12 Penipuan Investasi melalui Media Sosial

Penipuan investasi menggunakan media sosial untuk menawarkan peluang keuntungan yang terlihat menarik tetapi sebenarnya tidak memiliki dasar yang sah. Pelaku sering menggunakan testimonial, grafik keuntungan, figur publik palsu, atau komunitas online untuk membangun kepercayaan. Komunikasi dapat dilakukan melalui Facebook, Instagram, TikTok, WhatsApp, atau Telegram. Korban kemudian diarahkan untuk melakukan pembayaran atau transfer dana. Dalam investigasi, bukti penting meliputi akun media sosial, komunikasi, materi promosi, identitas pihak yang menawarkan, bukti pembayaran, rekening tujuan, serta kronologi transaksi. Cara mengatasi penipuan investasi adalah melakukan verifikasi legalitas pihak yang menawarkan investasi melalui sumber resmi, tidak percaya pada jaminan keuntungan tanpa risiko, dan tidak melakukan transfer berdasarkan tekanan. Pengguna juga perlu berhati-hati terhadap kelompok diskusi yang menjanjikan keuntungan cepat. Apabila sudah menjadi korban, simpan seluruh bukti komunikasi dan transaksi serta segera gunakan jalur pelaporan resmi yang relevan. Jangan menghapus percakapan karena informasi tersebut dapat membantu investigasi. Organisasi keuangan perlu menerapkan mekanisme monitoring dan edukasi konsumen. Dalam digital forensics, investigator dapat melakukan korelasi antara akun, nomor telepon, rekening, waktu komunikasi, dan transaksi untuk membangun alur kejadian. Pencegahan tetap menjadi strategi utama karena kerugian finansial sering kali sulit dipulihkan sepenuhnya setelah transaksi terjadi.

6.13 Account Cloning

Account cloning adalah pembuatan akun yang meniru akun seseorang dengan menggunakan nama, foto, dan informasi publik yang serupa. Kejahatan ini berbeda dengan account takeover karena pelaku tidak harus memperoleh kendali terhadap akun asli. Tujuan cloning biasanya adalah menipu kontak korban, meminta uang, menyebarkan informasi palsu, atau merusak reputasi korban. Investigasi dapat dilakukan dengan membandingkan waktu pembuatan akun, daftar pertemanan atau pengikut, konten, foto, pola komunikasi, dan hubungan akun. Pengguna dapat mengurangi risiko dengan membatasi informasi profil yang tersedia untuk publik dan mengaktifkan pengaturan privasi. Selain itu, pengguna dapat memberitahukan kepada kontak apabila terdapat akun palsu yang mengatasnamakan dirinya. Organisasi dapat menggunakan branding yang konsisten dan kanal resmi untuk membantu masyarakat membedakan akun asli dari akun tiruan. Jika akun cloning ditemukan, simpan dokumentasi profil tersebut dan gunakan mekanisme pelaporan platform. Dalam konteks

forensik, investigator harus mempertahankan informasi mengenai akun palsu sebelum dilakukan perubahan. Bukti dapat mencakup nama akun, URL, foto profil, waktu pengamatan, konten, dan komunikasi. Investigator tidak boleh mengambil alih akun palsu atau mencoba menyerang pelaku. Analisis harus berorientasi pada dokumentasi dan korelasi bukti. Dengan mekanisme verifikasi identitas yang baik, risiko cloning dapat dikurangi dan dampaknya dapat ditangani lebih cepat.

6.14 Kebocoran Data Pribadi

Kebocoran data terjadi ketika informasi yang seharusnya dilindungi tersedia atau tersebar kepada pihak yang tidak berwenang. Media sosial dapat menjadi tempat terjadinya kebocoran secara langsung maupun tidak langsung. Data dapat berasal dari unggahan pengguna, akun yang dikompromikan, aplikasi pihak ketiga, atau organisasi yang mengelola informasi pengguna. Dampaknya dapat berupa pencurian identitas, penipuan, spam, phishing, dan berbagai bentuk penyalahgunaan lainnya. Investigasi kebocoran data perlu menentukan jenis data yang terdampak, sumber kebocoran, waktu kejadian, pihak yang memiliki akses, serta bagaimana data tersebut tersebar. Cara mengatasinya adalah melakukan data minimization, menerapkan access control, mengenkripsi data sensitif, mengaktifkan MFA, dan melakukan monitoring keamanan. Pengguna harus menghindari publikasi data sensitif secara terbuka. Organisasi perlu memiliki data classification dan incident response plan. Jika kebocoran terjadi, prioritasnya adalah containment, preservation of evidence, assessment, notification sesuai kewajiban yang berlaku, dan remediation. Investigator harus berhati-hati agar proses investigasi tidak menyebabkan data sensitif tersebar lebih luas. Bukti yang mengandung informasi pribadi perlu diberikan perlindungan khusus. Dari sisi keamanan, pencegahan kebocoran membutuhkan kombinasi teknologi, kebijakan, pelatihan, dan kontrol akses. Setiap organisasi perlu memahami bahwa keamanan data merupakan proses berkelanjutan, bukan hanya tindakan ketika insiden sudah terjadi.

6.15 Hijacking Sesi dan Perangkat

Session hijacking merupakan kondisi ketika pihak tidak berwenang memperoleh atau menggunakan sesi autentikasi yang masih aktif. Pengguna dapat tidak menyadari bahwa akunnya masih terbuka pada perangkat lain. Risiko dapat meningkat ketika perangkat digunakan bersama, hilang, atau tidak dilindungi dengan baik. Dalam investigasi, indikator dapat berupa sesi perangkat yang tidak dikenali, aktivitas akun dari perangkat yang tidak

biasa, atau perubahan aktivitas tanpa adanya login password baru. Investigator perlu membandingkan informasi sesi dengan perangkat yang dimiliki pengguna dan kronologi aktivitas. Cara mengatasinya adalah mengakhiri sesi yang tidak dikenal, menggunakan penguncian perangkat, memperbarui sistem operasi, dan mengaktifkan MFA. Pengguna juga sebaiknya tidak meninggalkan akun aktif pada perangkat publik atau perangkat milik orang lain. Organisasi perlu menerapkan endpoint security dan kebijakan penggunaan perangkat. Jika terdapat dugaan kompromi, perubahan password harus dilakukan melalui perangkat yang dipercaya dan diikuti pemeriksaan sesi aktif. Dalam investigasi, bukti sesi harus dicatat sebelum sesi ditutup apabila prosedur memungkinkan. Investigator harus mempertimbangkan bahwa informasi lokasi atau perangkat dapat memiliki tingkat akurasi terbatas. Oleh karena itu, session hijacking perlu dianalisis melalui korelasi berbagai indikator. Pengamanan sesi merupakan bagian penting dari keamanan akun karena password yang kuat saja tidak selalu cukup apabila sesi autentikasi sudah terbuka pada perangkat lain.

6.16 Serangan melalui Aplikasi Pihak Ketiga

Aplikasi pihak ketiga yang terhubung dengan media sosial dapat memperoleh izin tertentu berdasarkan persetujuan pengguna. Risiko muncul ketika pengguna memberikan permission secara berlebihan atau aplikasi tersebut tidak memiliki keamanan yang memadai. Aplikasi dapat memiliki akses terhadap informasi profil, konten tertentu, atau fungsi lain sesuai izin yang diberikan. Dalam investigasi, investigator dapat memeriksa apakah terdapat aplikasi eksternal yang terhubung sebelum muncul aktivitas mencurigakan. Perubahan permission atau koneksi aplikasi dapat dimasukkan ke dalam timeline. Cara mengatasinya adalah melakukan audit aplikasi yang terhubung secara berkala dan mencabut akses yang tidak diperlukan. Pengguna sebaiknya tidak menghubungkan akun media sosial dengan aplikasi yang tidak jelas asal-usulnya. Organisasi perlu menerapkan kebijakan penggunaan aplikasi eksternal dan melakukan review terhadap permission. Dalam digital forensics, aplikasi pihak ketiga menjadi salah satu komponen attack surface yang harus dipertimbangkan ketika mencari akar masalah. Investigator harus membedakan antara izin aplikasi yang sah dan penggunaan izin secara tidak sah. Tidak semua aktivitas setelah aplikasi terhubung berarti aplikasi tersebut adalah penyebab insiden. Korelasi waktu dan bukti lain diperlukan. Pencegahan terbaik adalah prinsip least privilege, yaitu memberikan izin seminimal mungkin sesuai kebutuhan. Dengan melakukan audit permission secara berkala, risiko penyalahgunaan integrasi media sosial dapat dikurangi.

6.17 Kejahatan melalui Grup dan Komunitas Online

Grup dan komunitas media sosial dapat menjadi sarana komunikasi positif, tetapi juga dapat disalahgunakan untuk penipuan, penyebaran malware, perdagangan ilegal, manipulasi informasi, dan berbagai bentuk pelanggaran lainnya. Facebook Groups, Telegram Groups, WhatsApp Groups, dan komunitas pada platform lain memungkinkan banyak pengguna berkomunikasi secara bersamaan. Risiko meningkat ketika administrator tidak melakukan moderasi atau verifikasi anggota. Investigasi terhadap grup perlu memperhatikan struktur komunitas, akun administrator, waktu aktivitas, pola komunikasi, konten, serta hubungan antara anggota. Investigator harus memastikan bahwa pengumpulan bukti dilakukan sesuai kewenangan. Cara mengatasi risiko adalah menerapkan aturan komunitas, moderasi, verifikasi anggota, pembatasan tautan mencurigakan, dan mekanisme pelaporan. Administrator sebaiknya tidak memberikan hak istimewa kepada anggota tanpa kebutuhan. Pengguna perlu berhati-hati terhadap informasi yang diterima dari grup karena identitas anggota tidak selalu dapat diverifikasi. Dalam investigasi, grup dapat dianalisis sebagai social network untuk memahami hubungan antarakun dan pola penyebaran informasi. Namun, analisis harus tetap menghormati privasi dan batas legal. Dokumentasi waktu, akun, pesan, serta perubahan grup penting untuk menjaga kronologi. Dengan governance yang baik, komunitas digital dapat tetap menjadi ruang komunikasi yang aman sekaligus mengurangi peluang penyalahgunaan.

6.18 Serangan Reputasi dan Penyebaran Konten Manipulatif

Serangan reputasi merupakan tindakan yang bertujuan merusak citra individu atau organisasi melalui penyebaran informasi, gambar, video, atau narasi yang menyesatkan. Media sosial membuat serangan semacam ini dapat menyebar dengan sangat cepat. Konten manipulatif dapat berupa potongan komunikasi tanpa konteks, foto yang diedit, video yang dipotong, atau narasi yang menghubungkan seseorang dengan kejadian tertentu tanpa bukti memadai. Investigasi harus menentukan sumber awal konten, konteks, waktu penyebaran, perubahan versi konten, serta akun yang memperluas distribusi. Cara mengatasi serangan reputasi adalah tidak langsung membalas secara emosional. Organisasi perlu melakukan verifikasi fakta, mengamankan bukti, dan memberikan klarifikasi berdasarkan informasi yang dapat diverifikasi. Konten yang melanggar aturan platform dapat dilaporkan melalui mekanisme resmi. Dalam investigasi digital, metadata, salinan konten, URL, timestamp, dan hubungan antarakun dapat membantu membangun kronologi. Namun, investigator harus menghindari

kesimpulan hanya berdasarkan popularitas suatu konten. Banyaknya repost tidak membuktikan kebenaran informasi. Organisasi juga sebaiknya memiliki crisis communication plan sebelum insiden terjadi. Dengan respons yang terukur, bukti yang terdokumentasi, dan komunikasi berbasis fakta, dampak reputational attack dapat diminimalkan. Pendekatan tersebut juga mencegah organisasi memperbesar penyebaran konten bermasalah melalui respons yang tidak terkontrol.

6.19 Serangan terhadap Akun Resmi Organisasi

Akun resmi organisasi memiliki nilai strategis karena digunakan untuk komunikasi publik, pemasaran, pelayanan, dan penyampaian informasi. Pengambilalihan akun tersebut dapat menyebabkan kerugian reputasi, penyebaran informasi palsu, dan kerugian finansial. Risiko meningkat apabila password dibagikan kepada banyak orang atau administrator tidak menggunakan MFA. Investigasi terhadap insiden akun resmi harus mencakup daftar administrator, perubahan permission, perangkat yang digunakan, sesi login, aktivitas publikasi, serta waktu terjadinya perubahan. Cara mengatasi risiko adalah menggunakan role-based access control, MFA, password manager, dan prinsip least privilege. Setiap administrator harus memiliki akun individual apabila platform mendukungnya, bukan menggunakan satu password bersama. Ketika seorang pegawai tidak lagi bertugas sebagai administrator, aksesnya harus segera dicabut. Organisasi juga perlu memiliki backup contact dan prosedur pemulihan akun. Monitoring aktivitas akun dapat membantu mendeteksi perubahan yang tidak biasa. Jika terjadi kompromi, organisasi harus mengamankan bukti sebelum melakukan perubahan yang tidak perlu, kemudian mengikuti prosedur recovery resmi. Setelah akun berhasil dipulihkan, seluruh akses administrator harus diaudit. Post-incident review perlu dilakukan untuk mengetahui akar masalah. Dengan governance akun yang baik, organisasi dapat mengurangi risiko bahwa satu kredensial atau satu kesalahan pengguna menyebabkan kompromi terhadap seluruh kanal komunikasi publik.

6.20 Strategi Umum Mengatasi Kejahatan Media Sosial

Berbagai kejahatan dan serangan pada media sosial memiliki pola yang berbeda, tetapi strategi pertahanannya memiliki beberapa prinsip yang sama. Pertama, pengguna harus menggunakan password unik dan kuat serta mengaktifkan autentikasi multifaktor. Kedua, pengguna harus menjaga keamanan perangkat, sistem operasi, aplikasi, email, dan nomor telepon yang terhubung. Ketiga, kewaspadaan terhadap phishing, social engineering,

penipuan, tautan, file, dan aplikasi yang tidak dikenal harus ditingkatkan. Keempat, pengaturan privasi harus disesuaikan agar informasi pribadi tidak tersedia secara berlebihan. Kelima, pengguna perlu melakukan pemeriksaan terhadap sesi login dan aplikasi pihak ketiga secara berkala. Jika terjadi insiden, jangan langsung menghapus bukti. Dokumentasikan akun, pesan, URL, waktu kejadian, screenshot, dan informasi relevan lainnya sesuai kebutuhan, kemudian gunakan mekanisme pelaporan atau pemulihan resmi. Dalam perspektif **digital forensics**, penanganan insiden idealnya mengikuti siklus identification, preservation, collection, examination, analysis, dan reporting. Bukti harus memiliki provenance yang jelas dan chain of custody yang terdokumentasi. Organisasi perlu melengkapi langkah tersebut dengan security awareness, incident response plan, access control, backup, monitoring, serta evaluasi pascainsiden. Prinsip terpenting adalah bahwa keamanan media sosial bukan hanya masalah teknologi, melainkan kombinasi antara manusia, proses, teknologi, dan tata kelola. Dengan pendekatan berlapis tersebut, risiko kejahatan media sosial dapat ditekan dan apabila insiden terjadi, proses investigasi serta pemulihan dapat dilakukan secara lebih terstruktur dan dapat dipertanggungjawabkan.

BAB VII
KEAMANAN MEDIA SOSIAL

7.1 Investigasi Forensik pada Media Sosial

Investigasi pada media sosial merupakan proses sistematis untuk mengidentifikasi, mengamankan, mengumpulkan, memeriksa, menganalisis, dan menyajikan bukti digital yang berasal dari platform jejaring sosial. Facebook, WhatsApp, TikTok, Instagram, dan Telegram menyimpan berbagai bentuk informasi yang dapat memiliki nilai investigatif, seperti profil pengguna, komunikasi, foto, video, komentar, aktivitas login, hubungan pertemanan, metadata, serta informasi perangkat. Dalam praktik digital forensics, investigator tidak boleh langsung menyimpulkan bahwa suatu akun telah diretas hanya karena terdapat aktivitas yang tidak dikenal. Diperlukan pemeriksaan terhadap indikator kompromi, kronologi aktivitas, perangkat yang digunakan, lokasi login, perubahan kredensial, dan pola komunikasi. Proses investigasi harus mempertahankan integritas bukti sehingga data yang diperoleh dapat dipertanggungjawabkan. Prinsip penting yang digunakan adalah preservation, identification, acquisition, examination, analysis, dan reporting. Setiap tindakan terhadap barang bukti digital harus terdokumentasi secara jelas. Selain itu, investigator perlu memperhatikan kebijakan platform, aturan hukum, privasi, dan kewenangan akses. Dengan pendekatan tersebut, investigasi media sosial tidak hanya bertujuan menemukan pelaku atau sumber kejadian, tetapi juga memahami bagaimana insiden terjadi, data apa yang terdampak, serta bagaimana sistem dapat diperkuat untuk mencegah kejadian serupa.

7.2 Facebook sebagai Objek Investigasi

Facebook merupakan salah satu platform yang dapat menjadi sumber bukti digital dalam suatu investigasi. Informasi yang dapat dianalisis antara lain profil, unggahan, komentar, pesan, daftar pertemanan, aktivitas halaman, grup, foto, video, dan informasi mengenai sesi akses akun. Dalam investigasi, investigator perlu membedakan antara informasi yang tersedia secara publik dengan informasi yang memerlukan kewenangan khusus. Akun Facebook dapat mengalami kompromi akibat penggunaan kata sandi yang lemah, penggunaan kata sandi yang sama pada berbagai layanan, phishing, perangkat yang tidak aman, atau sesi login yang tertinggal pada perangkat lain. Investigator dapat

mengidentifikasi indikator seperti perubahan informasi profil tanpa izin, unggahan yang tidak dibuat pemilik akun, pesan yang tidak pernah dikirim, atau notifikasi login dari perangkat yang tidak dikenal. Namun, indikator tersebut harus diverifikasi melalui beberapa sumber agar tidak menghasilkan kesimpulan yang keliru. Dari sisi antisipasi, pengguna sebaiknya mengaktifkan autentikasi dua faktor, menggunakan kata sandi yang unik, memeriksa perangkat yang memiliki sesi aktif, dan menghindari tautan mencurigakan. Pengguna juga perlu mengaktifkan pemberitahuan keamanan sehingga perubahan penting dapat segera diketahui. Dalam konteks forensik, bukti Facebook harus dicatat bersama waktu pengumpulan, sumber, metode memperoleh data, dan kondisi data ketika ditemukan.

7.3 Investigasi Akun WhatsApp

WhatsApp memiliki karakteristik berbeda karena sebagian besar komunikasi personal dilindungi dengan enkripsi end-to-end. Dalam investigasi, hal tersebut berarti investigator tidak dapat memperlakukan WhatsApp seperti sumber data terbuka biasa. Pemeriksaan dapat mencakup perangkat yang digunakan, informasi akun, konfigurasi aplikasi, keberadaan sesi perangkat tertaut, cadangan yang tersedia secara sah, serta artefak digital yang terdapat pada perangkat sesuai kewenangan investigasi. Risiko kompromi akun dapat muncul ketika pengguna memberikan kode verifikasi kepada orang lain, kehilangan akses terhadap nomor telepon, menggunakan perangkat yang tidak terlindungi, atau membiarkan akun tertaut pada perangkat yang tidak dikenal. Salah satu indikator penting adalah munculnya perangkat tertaut yang tidak dikenali atau aktivitas komunikasi yang tidak dilakukan oleh pemilik akun. Antisipasi dapat dilakukan dengan mengaktifkan verifikasi dua langkah, menjaga keamanan nomor telepon, menggunakan penguncian perangkat, dan tidak pernah membagikan kode autentikasi. Pengguna juga perlu melakukan pemeriksaan secara berkala terhadap perangkat tertaut. Dalam investigasi forensik, investigator harus menghindari tindakan yang dapat mengubah data sumber. Jika perangkat menjadi barang bukti, dokumentasi kondisi perangkat pada saat ditemukan sangat penting. Waktu, kondisi jaringan, status aplikasi, dan metode akuisisi harus dicatat. Dengan demikian, analisis WhatsApp tetap berlandaskan prinsip integritas, legalitas, dan reproducibility.

7.4 TikTok dalam Investigasi Digital

TikTok menghasilkan berbagai artefak digital yang dapat berguna dalam investigasi, termasuk video, komentar, profil, aktivitas interaksi, pesan jika tersedia, serta informasi

mengenai hubungan antara akun dan konten. Investigasi TikTok perlu memperhatikan karakteristik konten yang sangat dinamis. Video dapat dihapus, akun dapat diubah, dan informasi profil dapat diperbarui dalam waktu singkat. Oleh karena itu, preservation menjadi tahap penting. Investigator dapat mendokumentasikan konten yang ditemukan secara sah, mencatat URL atau identitas konten, waktu pengamatan, nama akun, serta konteks interaksi. Risiko keamanan TikTok, seperti platform lainnya, dapat berkaitan dengan phishing, kredensial yang digunakan kembali, perangkat terinfeksi, aplikasi pihak ketiga, atau pengambilalihan sesi. Investigator perlu mencari indikator yang menunjukkan adanya aktivitas tidak normal tanpa mencoba mengambil alih akun. Antisipasi dapat dilakukan dengan menggunakan kata sandi unik, autentikasi multifaktor jika tersedia, memperbarui aplikasi, membatasi aplikasi pihak ketiga, dan menghindari tautan yang meminta informasi login. Pengguna juga perlu memahami bahwa konten publik dapat menjadi sumber informasi bagi pihak lain. Dalam investigasi, konten TikTok tidak boleh langsung dianggap sebagai bukti tunggal. Keaslian, konteks, waktu publikasi, hubungan akun, dan kemungkinan manipulasi harus diperiksa. Pendekatan tersebut membantu memastikan bahwa analisis TikTok menghasilkan temuan yang objektif dan dapat dipertanggungjawabkan.

7.5 Instagram sebagai Sumber Bukti Digital

Instagram dapat menjadi sumber informasi penting dalam investigasi karena aktivitas pengguna menghasilkan berbagai artefak digital. Foto, video, Stories, komentar, pesan, profil, pengikut, mengikuti, dan aktivitas akun dapat memberikan gambaran mengenai hubungan sosial serta kronologi suatu kejadian. Dalam investigasi forensik, investigator perlu memperhatikan bahwa sebagian konten Instagram memiliki sifat sementara atau dapat dihapus oleh pemilik akun. Karena itu, pengamanan bukti harus dilakukan sedini mungkin dengan metode yang sah dan terdokumentasi. Kerentanan akun Instagram dapat dipengaruhi oleh penggunaan kata sandi yang lemah, phishing, penggunaan kredensial yang sama pada layanan lain, perangkat yang tidak aman, atau akses sesi yang tidak lagi dikontrol pengguna. Tanda kompromi dapat berupa perubahan email, nomor telepon, nama pengguna, foto profil, pesan, atau unggahan yang tidak dilakukan pemilik akun. Antisipasi dapat dilakukan dengan menggunakan autentikasi multifaktor, kata sandi unik, pemeriksaan aktivitas login, dan kewaspadaan terhadap pesan yang meminta kode keamanan. Pengguna juga sebaiknya tidak memberikan akses kepada aplikasi pihak ketiga yang tidak dipercaya. Dalam proses investigasi, screenshot saja tidak selalu cukup untuk membuktikan keseluruhan konteks

suatu kejadian. Investigator perlu melakukan korelasi dengan sumber lain, misalnya perangkat, waktu aktivitas, metadata yang tersedia secara sah, atau bukti komunikasi lain. Hal tersebut meningkatkan reliabilitas kesimpulan investigasi.

7.6 Telegram sebagai Objek Forensik

Telegram mempunyai karakteristik teknis yang perlu diperhatikan dalam investigasi digital. Platform ini menyediakan komunikasi berbasis cloud untuk sebagian besar percakapan dan memiliki fitur Secret Chat dengan karakteristik keamanan yang berbeda. Karena itu, investigator harus memahami jenis percakapan yang sedang diperiksa sebelum menentukan metode analisis. Artefak yang relevan dapat mencakup akun, username, grup, channel, pesan, media, perangkat yang digunakan, dan sesi aktif. Risiko kompromi akun dapat berkaitan dengan pengambilalihan nomor telepon, kode autentikasi yang diberikan kepada pihak lain, perangkat yang tidak aman, atau sesi Telegram yang masih aktif pada perangkat lain. Indikator kompromi dapat berupa sesi perangkat asing, pesan yang tidak dibuat pemilik akun, perubahan informasi akun, atau aktivitas pada waktu yang tidak sesuai dengan kebiasaan pengguna. Antisipasi dapat dilakukan melalui verifikasi dua langkah, perlindungan nomor telepon, penguncian aplikasi, serta pemeriksaan sesi aktif secara berkala. Dalam investigasi, investigator harus membedakan antara data yang berasal dari akun, perangkat, dan server. Setiap sumber memiliki karakteristik evidentiary yang berbeda. Investigator juga harus mempertimbangkan kemungkinan sinkronisasi data antarperangkat. Dengan demikian, satu artefak Telegram tidak boleh dianalisis secara terisolasi. Korelasi antara akun, perangkat, waktu, jaringan, dan aktivitas pengguna dapat menghasilkan gambaran investigasi yang lebih akurat.

7.7 Mengapa Akun Media Sosial Dapat Dikompromikan

Istilah “mudah terbobol” sebaiknya dipahami sebagai kondisi ketika keamanan akun relatif lemah atau pengguna mudah menjadi korban rekayasa sosial, bukan berarti platform tersebut dapat ditembus dengan mudah. Sebagian besar insiden pengambilalihan akun justru berawal dari faktor manusia, seperti penggunaan kata sandi yang sama, membagikan kode verifikasi, mengklik tautan phishing, atau menginstal aplikasi yang tidak terpercaya. Serangan juga dapat terjadi melalui perangkat yang telah terinfeksi atau sesi login yang tidak diamankan. Oleh karena itu, investigasi harus memeriksa rantai kejadian secara menyeluruh. Investigator perlu menentukan apakah insiden berasal dari kredensial, perangkat, nomor telepon, sesi

aktif, aplikasi pihak ketiga, atau teknik social engineering. Pendekatan ini penting karena solusi keamanan harus sesuai dengan akar masalah. Misalnya, mengganti kata sandi tidak cukup apabila nomor telepon atau perangkat pengguna masih dikuasai pihak lain. Demikian pula, menghapus aplikasi mencurigakan tidak menyelesaikan masalah apabila kredensial telah diberikan kepada pelaku. Dari perspektif forensik, setiap kemungkinan harus diuji berdasarkan bukti. Investigator tidak boleh membuat kesimpulan hanya berdasarkan asumsi. Dengan melakukan analisis kronologis dan korelasi bukti, penyebab kompromi dapat diidentifikasi secara lebih objektif dan langkah mitigasi dapat dirancang secara tepat.

7.8 Phishing sebagai Ancaman Utama

Phishing merupakan salah satu teknik yang sering digunakan untuk memperoleh informasi autentikasi dengan memanfaatkan manipulasi psikologis pengguna. Korban dapat menerima pesan, email, atau tautan yang tampak seolah-olah berasal dari layanan resmi. Pesan tersebut biasanya mendorong pengguna melakukan tindakan tertentu, misalnya masuk ke akun atau memberikan informasi keamanan. Dalam konteks investigasi, investigator perlu memeriksa sumber pesan, waktu penerimaan, alamat atau identitas pengirim, tujuan tautan, isi komunikasi, dan hubungan pesan tersebut dengan kejadian kompromi. Investigator tidak perlu mencoba mengakses sistem yang menjadi tujuan tautan tersebut karena tindakan tersebut dapat menimbulkan risiko dan melampaui kewenangan. Pencegahan phishing dilakukan dengan memverifikasi sumber komunikasi, tidak memberikan kode autentikasi, menggunakan pengelola kata sandi, dan mengaktifkan autentikasi multifaktor. Pengguna juga harus berhati-hati terhadap pesan yang menggunakan tekanan waktu atau ancaman. Dalam lingkungan organisasi, edukasi keamanan secara berkala sangat penting karena teknologi keamanan tidak dapat sepenuhnya menggantikan kewaspadaan pengguna. Dari sisi investigasi, bukti phishing harus diamankan tanpa mengubah isinya. Pesan, header jika tersedia, waktu penerimaan, informasi pengirim, dan konteks kejadian perlu dicatat. Korelasi antara pesan phishing dan perubahan aktivitas akun dapat membantu investigator menentukan apakah komunikasi tersebut berkaitan dengan insiden keamanan.

7.9 Social Engineering pada Media Sosial

Social engineering merupakan teknik manipulasi manusia yang bertujuan memperoleh akses atau informasi melalui interaksi sosial. Pelaku dapat berpura-pura menjadi teman, petugas layanan, rekan kerja, atau pihak yang dipercaya. Media sosial menjadi lingkungan yang

mendukung teknik tersebut karena banyak informasi pribadi tersedia secara terbuka. Dalam investigasi, investigator perlu memperhatikan pola komunikasi yang tidak biasa, perubahan gaya komunikasi, permintaan informasi sensitif, dan hubungan antara percakapan dengan kejadian keamanan. Namun, investigator harus menghindari kesimpulan hanya berdasarkan gaya bahasa karena akun dapat digunakan oleh orang lain atau konten dapat diterjemahkan secara otomatis. Pencegahan social engineering dilakukan dengan membatasi informasi pribadi yang dipublikasikan, memverifikasi identitas melalui saluran lain, dan tidak memberikan kode keamanan kepada siapa pun. Organisasi juga perlu memiliki prosedur verifikasi untuk permintaan sensitif. Dalam kasus investigasi, komunikasi yang diduga menjadi bagian dari social engineering perlu dipreservasi secara legal dan lengkap. Tanggal, waktu, identitas akun, isi komunikasi, serta perubahan aktivitas setelah komunikasi tersebut harus dianalisis. Investigator kemudian dapat membuat timeline untuk melihat hubungan sebab-akibat yang mungkin. Dengan demikian, investigasi social engineering tidak sekadar mencari pesan mencurigakan, tetapi menganalisis bagaimana manipulasi tersebut berhubungan dengan perubahan keamanan akun.

7.10 Keamanan Kata Sandi

Kata sandi merupakan salah satu komponen penting dalam keamanan akun media sosial. Penggunaan kata sandi yang sama pada banyak platform meningkatkan dampak ketika salah satu layanan mengalami kebocoran kredensial. Jika kombinasi tersebut digunakan kembali pada Facebook, Instagram, TikTok, Telegram, atau layanan lainnya, kompromi satu akun dapat meningkatkan risiko terhadap akun lain. Karena itu, pengguna sebaiknya menggunakan kata sandi unik untuk setiap layanan. Pengelola kata sandi dapat membantu menghasilkan dan menyimpan kredensial yang berbeda tanpa mengharuskan pengguna mengingat semuanya. Dalam investigasi, penggunaan ulang kata sandi dapat menjadi salah satu hipotesis yang perlu diperiksa apabila beberapa akun mengalami kompromi secara berurutan. Namun, investigator tidak boleh mencoba menguji kata sandi pengguna tanpa kewenangan. Pemeriksaan harus dilakukan melalui bukti yang diperoleh secara legal. Antisipasi juga mencakup penggantian kredensial setelah terjadi indikasi kompromi dan pemeriksaan terhadap sesi yang masih aktif. Organisasi dapat menerapkan kebijakan autentikasi yang kuat dan edukasi keamanan bagi pengguna. Prinsip utamanya adalah mengurangi kemungkinan bahwa satu kredensial yang bocor dapat membuka akses ke banyak layanan. Dalam konteks forensik, investigator perlu mencatat kapan pengguna

menyadari insiden, kapan kredensial diubah, dan apakah aktivitas mencurigakan terjadi sebelum atau sesudah perubahan tersebut.

7.11 Autentikasi Multifaktor

Autentikasi multifaktor atau MFA memberikan lapisan keamanan tambahan karena akses tidak hanya bergantung pada kata sandi. Apabila kata sandi diketahui pihak lain, faktor autentikasi tambahan masih dapat menghambat akses tidak sah. Dalam investigasi, penggunaan MFA menjadi aspek penting karena investigator perlu mengetahui apakah MFA aktif, bagaimana metode autentikasinya, dan apakah terdapat perubahan konfigurasi sebelum insiden. Perubahan metode keamanan yang tidak dilakukan pemilik akun dapat menjadi indikator kompromi. Antisipasi terbaik adalah mengaktifkan MFA pada platform yang mendukungnya dan menjaga faktor autentikasi tetap berada dalam kendali pemilik akun. Kode verifikasi tidak boleh diberikan kepada orang lain, termasuk pihak yang mengaku sebagai petugas layanan. Pengguna juga perlu memahami prosedur pemulihan akun karena proses recovery yang lemah dapat menjadi titik risiko. Dalam organisasi, MFA sebaiknya diterapkan terutama untuk akun dengan akses penting. Dari perspektif digital forensics, bukti terkait autentikasi harus diperlakukan sebagai bagian dari timeline. Misalnya, apabila konfigurasi MFA berubah sebelum aktivitas mencurigakan, perubahan tersebut dapat menjadi petunjuk penting. Investigator tetap perlu memverifikasi temuan menggunakan bukti lain. MFA bukan berarti akun tidak mungkin dikompromikan, tetapi dapat mengurangi risiko pengambilalihan berbasis kredensial yang bocor.

7.12 Investigasi Perangkat yang Digunakan

Perangkat seperti smartphone, komputer, dan tablet sering menjadi sumber bukti utama dalam investigasi media sosial. Aplikasi Facebook, WhatsApp, TikTok, Instagram, dan Telegram dapat meninggalkan berbagai artefak pada perangkat, tergantung sistem operasi, versi aplikasi, konfigurasi, dan metode penggunaan. Dalam investigasi forensik, perangkat harus diperlakukan sebagai barang bukti yang memerlukan prosedur pengamanan. Investigator perlu mendokumentasikan kondisi perangkat ketika ditemukan dan menjaga chain of custody. Akuisisi data harus menggunakan metode yang sesuai kewenangan dan tujuan pemeriksaan. Perubahan data sumber harus diminimalkan. Analisis kemudian dapat mencakup aplikasi, database, file media, konfigurasi akun, log, notifikasi, serta informasi lain yang relevan dan dapat diperoleh secara sah. Investigator juga perlu memahami bahwa

beberapa data dapat tersinkronisasi dengan cloud sehingga keberadaan artefak lokal tidak selalu menggambarkan keseluruhan aktivitas akun. Antisipasi dari sisi pengguna dilakukan dengan mengaktifkan penguncian perangkat, memperbarui sistem operasi, memasang aplikasi dari sumber resmi, dan tidak memberikan akses perangkat kepada pihak yang tidak dipercaya. Dalam organisasi, perangkat yang digunakan untuk aktivitas penting sebaiknya memiliki kebijakan keamanan yang jelas. Investigasi perangkat harus dilakukan secara hati-hati karena tindakan yang tidak tepat dapat mengubah bukti dan menyulitkan proses pembuktian.

7.13 Sesi Login sebagai Indikator Kompromi

Sesi login merupakan salah satu informasi penting ketika menyelidiki dugaan pengambilalihan akun. Banyak layanan media sosial memungkinkan pengguna melihat perangkat atau lokasi yang pernah digunakan untuk mengakses akun. Informasi tersebut dapat membantu pengguna dan investigator mengidentifikasi aktivitas yang tidak dikenal. Namun, lokasi yang ditampilkan tidak selalu menunjukkan lokasi fisik pengguna secara tepat karena dapat dipengaruhi oleh jaringan, VPN, operator seluler, atau sistem geolokasi. Oleh sebab itu, informasi lokasi harus diperlakukan sebagai indikator, bukan bukti tunggal. Investigator dapat membandingkan waktu sesi, jenis perangkat, alamat jaringan jika tersedia secara sah, dan aktivitas akun pada periode yang sama. Antisipasi dilakukan dengan memeriksa sesi aktif secara berkala dan mengakhiri sesi pada perangkat yang tidak dikenali. Jika terdapat indikasi kompromi, pengguna dapat melakukan pengamanan akun melalui mekanisme pemulihan resmi platform. Dalam investigasi, perubahan sesi harus dimasukkan ke timeline. Misalnya, muncul sesi perangkat baru kemudian diikuti perubahan profil atau pengiriman pesan yang tidak dikenal. Korelasi tersebut dapat memperkuat hipotesis adanya kompromi. Namun, investigator tetap harus mempertimbangkan kemungkinan perangkat keluarga, komputer publik, atau perangkat lama yang masih memiliki sesi aktif. Dengan demikian, pemeriksaan sesi harus dilakukan secara kontekstual dan tidak menghasilkan tuduhan berdasarkan satu indikator saja.

7.14 Metadata sebagai Informasi Pendukung

Metadata adalah informasi mengenai suatu data, seperti waktu pembuatan, perubahan, jenis file, perangkat, atau karakteristik teknis tertentu. Dalam investigasi media sosial, metadata dapat memberikan informasi pendukung untuk memahami asal-usul dan kronologi suatu

konten. Namun, metadata yang tersedia pada platform dapat berbeda dengan metadata asli pada perangkat karena proses unggah, kompresi, pemrosesan ulang, atau perubahan format. Oleh sebab itu, investigator tidak boleh menganggap metadata media sosial selalu identik dengan metadata file asli. Pemeriksaan metadata sebaiknya dilakukan dengan membandingkan beberapa sumber apabila tersedia secara sah. Misalnya, file asli pada perangkat dapat dibandingkan dengan konten yang dipublikasikan pada platform. Dari perspektif antisipasi, pengguna perlu menyadari bahwa foto dan video dapat mengandung informasi mengenai perangkat atau waktu tertentu jika metadata tersebut tetap dipertahankan. Pengaturan privasi dan kehati-hatian ketika membagikan konten dapat mengurangi paparan informasi. Dalam investigasi, metadata harus diperlakukan sebagai evidence supporting element, bukan selalu sebagai bukti tunggal. Investigator juga perlu mencatat alat yang digunakan untuk memperoleh dan membaca metadata. Setiap proses pemeriksaan harus terdokumentasi agar hasil dapat direplikasi. Dengan pendekatan tersebut, metadata dapat membantu membangun timeline, menghubungkan konten dengan perangkat tertentu, serta memperkuat korelasi antara beberapa sumber bukti.

7.15 Chain of Custody

Chain of custody atau rantai penguasaan barang bukti merupakan elemen penting dalam investigasi digital. Prinsip ini memastikan bahwa setiap perpindahan, penyimpanan, pemeriksaan, dan pengelolaan barang bukti terdokumentasi. Pada investigasi media sosial, bukti dapat berupa perangkat, file hasil akuisisi, screenshot, rekaman layar, dokumen, atau data lain yang diperoleh melalui prosedur yang sah. Investigator harus mencatat siapa yang memperoleh bukti, kapan diperoleh, bagaimana metode pengambilannya, dan di mana bukti disimpan. Tujuannya adalah mempertahankan integritas dan memastikan bahwa bukti tidak mengalami perubahan yang tidak terdokumentasi. Penggunaan hash dapat menjadi salah satu mekanisme untuk memverifikasi integritas file hasil akuisisi, sesuai prosedur dan jenis bukti. Dalam kasus Facebook, WhatsApp, TikTok, Instagram, dan Telegram, chain of custody menjadi semakin penting karena data dapat berubah, dihapus, atau tersinkronisasi secara otomatis. Dokumentasi yang buruk dapat menyebabkan kesulitan ketika hasil investigasi harus dipertanggungjawabkan. Oleh karena itu, investigator perlu memiliki formulir atau sistem pencatatan bukti yang konsisten. Antisipasi dari sisi organisasi dilakukan dengan membuat SOP digital evidence handling. Setiap personel yang menangani barang bukti harus memahami prosedur tersebut. Dengan chain of custody yang baik, hasil

investigasi memiliki dasar dokumentasi yang lebih kuat dan dapat dipertanggungjawabkan secara profesional.

7.16 Penyusunan Timeline Investigasi

Timeline merupakan salah satu teknik penting dalam digital forensics karena membantu investigator memahami urutan kejadian. Pada investigasi media sosial, timeline dapat menghubungkan waktu login, perubahan akun, komunikasi, unggahan, penghapusan konten, dan aktivitas perangkat. Misalnya, apabila terdapat login dari perangkat yang tidak dikenal kemudian terjadi perubahan email dan pengiriman pesan tertentu, rangkaian tersebut dapat menjadi indikasi penting. Namun, waktu yang ditampilkan oleh platform harus dipahami dengan memperhatikan zona waktu dan kemungkinan perbedaan timestamp. Investigator harus melakukan normalisasi waktu jika data berasal dari beberapa sumber. Informasi dari perangkat, aplikasi, platform, dan dokumen eksternal dapat digabungkan untuk membuat timeline yang komprehensif. Timeline tidak hanya digunakan untuk mencari pelaku, tetapi juga menentukan kapan kompromi kemungkinan terjadi dan tindakan apa yang dilakukan setelahnya. Dari sisi antisipasi, pengguna dan organisasi perlu mencatat waktu kejadian ketika menyadari adanya aktivitas mencurigakan. Jangan langsung menghapus semua data karena tindakan tersebut dapat menghilangkan informasi yang diperlukan untuk investigasi. Pengamanan akun sebaiknya dilakukan melalui prosedur pemulihan resmi sambil mempertahankan bukti yang relevan. Dengan timeline yang terstruktur, investigator dapat membedakan aktivitas normal, aktivitas mencurigakan, dan aktivitas setelah pemulihan sehingga analisis menjadi lebih objektif.

7.17 Korelasi Bukti Antarplatform

Salah satu karakteristik investigasi media sosial modern adalah adanya hubungan antara berbagai platform. Seseorang dapat menggunakan nama pengguna yang sama di Instagram, TikTok, Telegram, Facebook, atau platform lainnya. Konten juga dapat dipublikasikan ulang pada beberapa layanan. Korelasi tersebut dapat membantu investigator memahami hubungan antarakun, tetapi harus dilakukan secara hati-hati. Kesamaan username atau foto profil tidak otomatis membuktikan bahwa dua akun dimiliki orang yang sama. Diperlukan indikator tambahan seperti pola waktu aktivitas, konten, hubungan komunikasi, atau informasi lain yang diperoleh secara sah. Dalam investigasi, investigator dapat membangun relationship mapping untuk memvisualisasikan hubungan antara akun, perangkat, konten, dan waktu.

Teknik ini dapat membantu menemukan pola yang tidak terlihat ketika setiap platform dianalisis secara terpisah. Antisipasi bagi pengguna adalah menghindari publikasi informasi pribadi yang terlalu banyak pada berbagai platform. Penggunaan identitas digital yang sama pada banyak layanan dapat meningkatkan risiko profiling. Dari perspektif forensik, korelasi antarplatform harus disertai dokumentasi sumber data. Investigator perlu menjelaskan dasar yang digunakan untuk menghubungkan dua akun atau dua aktivitas. Dengan pendekatan tersebut, analisis menjadi lebih terukur dan mengurangi risiko false attribution atau salah mengidentifikasi pemilik akun.

7.18 Risiko Aplikasi Pihak Ketiga

Aplikasi pihak ketiga dapat memberikan fitur tambahan pada media sosial, tetapi juga dapat menimbulkan risiko keamanan apabila diberikan izin yang berlebihan. Pengguna terkadang memberikan akses kepada aplikasi tanpa membaca jenis permission yang diminta. Jika aplikasi tersebut tidak terpercaya atau mengalami kompromi, informasi akun dapat berpotensi terdampak. Dalam investigasi, pemeriksaan aplikasi pihak ketiga dapat membantu menjelaskan bagaimana suatu akun mengalami perubahan atau aktivitas tidak dikenal. Investigator perlu melihat apakah terdapat aplikasi atau layanan eksternal yang memperoleh akses sebelum insiden. Namun, pemeriksaan harus dilakukan melalui data yang tersedia secara sah dan tidak boleh melibatkan pengambilalihan aplikasi tersebut. Antisipasi dapat dilakukan dengan membatasi penggunaan aplikasi pihak ketiga, mencabut izin yang tidak lagi diperlukan, dan hanya menggunakan aplikasi dari sumber terpercaya. Pengguna juga perlu memperhatikan permintaan akses yang tidak relevan dengan fungsi aplikasi. Dalam organisasi, penggunaan aplikasi eksternal sebaiknya mengikuti kebijakan keamanan informasi. Investigator dapat memasukkan perubahan izin aplikasi ke dalam timeline jika informasi tersebut tersedia. Korelasi antara pemberian izin dan munculnya aktivitas mencurigakan dapat menjadi indikator investigasi. Dengan demikian, keamanan media sosial tidak hanya bergantung pada platform utama, tetapi juga pada ekosistem aplikasi dan layanan yang terhubung dengannya.

7.19 Keamanan Nomor Telepon

Nomor telepon dapat menjadi komponen penting dalam autentikasi berbagai layanan media sosial. Karena itu, keamanan nomor telepon harus diperhatikan. Pengambilalihan nomor atau penyalahgunaan proses pemulihan akun dapat menyebabkan risiko terhadap akun yang

menggunakan nomor tersebut. Dalam investigasi, perubahan nomor yang terhubung dengan akun, kehilangan akses secara tiba-tiba, atau kode autentikasi yang tidak diminta dapat menjadi indikator yang perlu diperiksa. Pengguna sebaiknya tidak membagikan kode verifikasi kepada siapa pun. Jika menerima kode autentikasi yang tidak diminta, pengguna perlu menganggapnya sebagai peringatan dan memeriksa keamanan akun melalui saluran resmi. Antisipasi juga mencakup penggunaan metode autentikasi tambahan dan perlindungan terhadap informasi pribadi yang berkaitan dengan nomor telepon. Dalam organisasi, nomor yang digunakan untuk akun penting harus dikelola dengan prosedur yang jelas. Investigator yang menangani dugaan pengambilalihan perlu membuat timeline mengenai perubahan nomor, aktivitas autentikasi, dan perubahan akun. Data tersebut harus dikorelasikan dengan bukti lain karena munculnya kode autentikasi saja belum membuktikan bahwa akun telah berhasil diambil alih. Dengan demikian, nomor telepon harus dipandang sebagai bagian dari authentication ecosystem yang membutuhkan perlindungan sama seriusnya dengan kata sandi.

7.20 Keamanan Email yang Terhubung

Email sering menjadi mekanisme pemulihan untuk akun media sosial. Apabila email utama berhasil dikompromikan, beberapa akun media sosial yang terhubung dapat ikut berisiko. Karena itu, investigasi pengambilalihan media sosial perlu mempertimbangkan keamanan email sebagai bagian dari attack surface. Investigator dapat memeriksa secara sah apakah terdapat perubahan alamat email, notifikasi keamanan, atau aktivitas pemulihan akun yang tidak dikenal. Pengguna harus menggunakan kata sandi unik dan MFA pada email utama. Email pemulihan juga harus diamankan. Antisipasi penting lainnya adalah memeriksa alamat email yang digunakan untuk akun penting dan menghindari penggunaan email yang sama untuk terlalu banyak kebutuhan sensitif tanpa perlindungan yang memadai. Dalam investigasi, urutan kejadian sangat penting. Jika email mengalami aktivitas mencurigakan terlebih dahulu kemudian akun Instagram atau Facebook berubah, terdapat kemungkinan hubungan antara kedua kejadian tersebut. Namun, hubungan tersebut harus dibuktikan melalui bukti yang tersedia. Investigator tidak boleh langsung menganggap email sebagai sumber serangan. Analisis harus mempertimbangkan alternatif seperti phishing langsung terhadap media sosial, perangkat terinfeksi, atau penyalahgunaan sesi. Dengan pendekatan attack-chain analysis, investigator dapat memahami jalur kompromi secara lebih komprehensif dan menentukan titik pengamanan yang paling efektif.

7.21 Investigasi Konten yang Dihapus

Konten media sosial dapat dihapus oleh pemilik akun atau menjadi tidak tersedia karena perubahan kebijakan platform. Dalam investigasi, keberadaan konten yang sudah tidak dapat diakses secara langsung tidak selalu berarti bahwa seluruh jejak digitalnya hilang. Bukti pendukung mungkin terdapat pada perangkat, notifikasi, salinan yang sah, komunikasi terkait, atau sumber lain. Namun, investigator harus memastikan bahwa sumber tersebut diperoleh secara legal dan dapat diverifikasi. Dokumentasi terhadap konten yang ditemukan ketika masih tersedia menjadi salah satu alasan pentingnya preservation. Investigator perlu mencatat waktu pengamatan, identitas akun, konteks konten, dan sumber bukti. Screenshot dapat menjadi dokumentasi pendukung, tetapi keandalannya meningkat jika dikombinasikan dengan sumber lain dan metode verifikasi. Antisipasi bagi organisasi adalah memiliki prosedur preservation ketika insiden pertama kali diketahui. Jangan melakukan tindakan yang tidak perlu terhadap perangkat atau akun karena dapat mengubah bukti. Dari sisi pengguna, jika menjadi korban penyalahgunaan akun, dokumentasikan aktivitas mencurigakan sebelum melakukan tindakan pemulihan yang dapat mengubah kondisi bukti. Investigasi konten terhapus membutuhkan kehati-hatian karena data dapat memiliki konteks yang berbeda setelah dipisahkan dari sumber aslinya. Oleh karena itu, investigator perlu menjelaskan provenance setiap bukti yang digunakan.

7.22 Analisis Foto dan Video

Foto dan video merupakan jenis bukti yang sering ditemukan pada Facebook, Instagram, TikTok, Telegram, dan platform lainnya. Dalam investigasi, analisis tidak hanya melihat isi visual, tetapi juga mempertimbangkan sumber file, waktu, metadata yang tersedia, konteks publikasi, dan hubungan dengan aktivitas akun. Investigator harus mempertimbangkan kemungkinan bahwa suatu foto atau video telah diedit, dipotong, dikompresi, atau dipublikasikan ulang. Karena itu, visual evidence perlu diverifikasi menggunakan sumber lain apabila tersedia. Analisis dapat membantu menentukan hubungan antara konten dan timeline suatu kejadian. Namun, kemampuan teknis untuk menemukan manipulasi tidak berarti bahwa setiap perubahan otomatis menunjukkan niat jahat. Kompresi platform juga dapat mengubah karakteristik file tanpa adanya manipulasi oleh pengguna. Dari sisi antisipasi, pengguna perlu memahami bahwa konten visual dapat mengungkapkan informasi pribadi atau lokasi. Pengaturan privasi dan selektivitas dalam membagikan foto dapat mengurangi risiko. Dalam investigasi, setiap file sebaiknya disimpan melalui prosedur yang

menjaga integritasnya. Hash dan dokumentasi sumber dapat digunakan sesuai prosedur forensik. Investigator juga harus mencatat apakah file diperoleh dari perangkat, platform, atau sumber lain. Dengan pendekatan tersebut, foto dan video dapat digunakan sebagai evidence yang lebih kuat tanpa mengabaikan kemungkinan manipulasi atau perubahan teknis.

7.23 Analisis Pesan dan Komunikasi

Pesan merupakan sumber informasi penting karena dapat menunjukkan hubungan, waktu komunikasi, konteks, dan perkembangan suatu peristiwa. WhatsApp, Telegram, Facebook Messenger, Instagram, dan platform lain memiliki karakteristik penyimpanan dan keamanan yang berbeda. Dalam investigasi, investigator perlu menentukan sumber pesan, kondisi data, waktu, identitas pengirim dan penerima, serta kemungkinan adanya perubahan atau penghapusan. Pesan tidak boleh dipisahkan dari konteks percakapan karena satu kalimat dapat memiliki arti berbeda ketika tidak melihat rangkaian komunikasi secara lengkap. Investigator juga perlu membedakan antara akun asli dan akun yang mungkin telah diambil alih. Antisipasi dilakukan dengan mengamankan akun, perangkat, dan kode autentikasi. Pengguna sebaiknya tidak meneruskan informasi sensitif melalui percakapan yang tidak diperlukan. Dalam organisasi, kebijakan penyimpanan komunikasi harus memperhatikan kebutuhan bisnis dan perlindungan privasi. Jika pesan menjadi barang bukti, metode akuisisi harus terdokumentasi. Investigator harus menghindari perubahan terhadap data sumber. Korelasi pesan dengan waktu login, perangkat, dan aktivitas lainnya dapat membantu menentukan apakah komunikasi benar-benar berkaitan dengan suatu insiden. Dengan demikian, analisis pesan harus memperhatikan content, context, provenance, dan chronology agar hasil investigasi tidak menyesatkan.

7.24 Perlindungan Privasi dalam Investigasi

Investigasi media sosial harus dilaksanakan dengan memperhatikan prinsip privasi dan proporsionalitas. Tidak semua informasi yang dapat ditemukan secara teknis boleh dikumpulkan atau dianalisis tanpa batas. Investigator harus memiliki dasar kewenangan yang jelas dan hanya mengambil data yang relevan dengan tujuan investigasi. Pengumpulan data berlebihan dapat meningkatkan risiko pelanggaran privasi. Dalam investigasi Facebook, WhatsApp, TikTok, Instagram, dan Telegram, batas antara informasi publik dan informasi privat harus diperhatikan. Data komunikasi pribadi memiliki tingkat sensitivitas

tinggi dan memerlukan perlindungan yang sesuai. Investigator juga harus menerapkan kontrol akses terhadap barang bukti agar hanya personel berwenang yang dapat mengaksesnya. Penyimpanan bukti harus menggunakan mekanisme keamanan yang memadai. Setelah kebutuhan investigasi berakhir, organisasi perlu memiliki kebijakan retensi dan pemusnahan data yang jelas. Dari sisi pengguna, privasi dapat diperkuat melalui pengaturan visibilitas profil, pembatasan informasi pribadi, dan pengelolaan daftar aplikasi yang memiliki akses. Dalam laporan investigasi, informasi yang tidak relevan sebaiknya tidak dicantumkan. Prinsip minimization membantu menjaga fokus investigasi sekaligus mengurangi risiko penyalahgunaan data. Dengan demikian, investigasi digital yang baik bukan hanya mampu menemukan bukti, tetapi juga mampu melindungi hak dan privasi pihak yang terlibat.

7.25 Penggunaan OSINT secara Bertanggung Jawab

Open-Source Intelligence atau OSINT merupakan proses pengumpulan dan analisis informasi yang tersedia secara terbuka. Dalam investigasi media sosial, OSINT dapat digunakan untuk memahami akun, hubungan antarprofil, konten publik, dan perkembangan informasi. Facebook, TikTok, Instagram, Telegram, dan platform lainnya dapat menjadi sumber informasi publik, tetapi investigator harus memperhatikan batas legal dan etika. OSINT bukan berarti investigator bebas mengumpulkan semua informasi tentang seseorang. Data harus relevan dengan tujuan investigasi dan diperoleh melalui cara yang sah. Investigator juga harus memperhitungkan kemungkinan akun palsu, informasi tidak akurat, konten yang dimanipulasi, serta identitas yang menggunakan nama serupa. Verifikasi silang menjadi prinsip penting dalam OSINT. Informasi sebaiknya dikonfirmasi menggunakan beberapa sumber independen sebelum digunakan sebagai dasar kesimpulan. Antisipasi bagi pengguna adalah menyadari bahwa informasi yang dipublikasikan secara terbuka dapat dikumpulkan dan dikorelasikan oleh pihak lain. Karena itu, pengaturan privasi dan pembatasan informasi sensitif sangat penting. Dalam laporan forensik, investigator perlu mencatat sumber informasi, waktu pengumpulan, metode dokumentasi, dan konteks. Dengan pendekatan tersebut, OSINT dapat menjadi komponen investigasi yang efektif tanpa berubah menjadi aktivitas pengumpulan data pribadi secara berlebihan.

7.26 Peran Investigator Digital Forensics

Investigator digital forensics memiliki tanggung jawab untuk memastikan bahwa proses pemeriksaan dilakukan secara sistematis, objektif, dan dapat dipertanggungjawabkan. Dalam investigasi media sosial, investigator tidak hanya mencari informasi yang mendukung suatu dugaan, tetapi juga harus mempertimbangkan bukti yang dapat menyangkal dugaan tersebut. Prinsip objektivitas sangat penting karena data media sosial dapat memiliki konteks yang kompleks. Investigator harus memahami karakteristik masing-masing platform, sistem operasi, aplikasi, mekanisme autentikasi, dan metode penyimpanan data. Kemampuan teknis perlu disertai pemahaman hukum, etika, chain of custody, dan evidence handling. Investigator juga harus mendokumentasikan setiap prosedur yang dilakukan. Apabila menggunakan perangkat lunak forensik, versi dan konfigurasi alat sebaiknya dicatat. Hasil analisis harus dapat dijelaskan sehingga pihak lain memahami bagaimana kesimpulan diperoleh. Investigator tidak boleh mengubah barang bukti hanya untuk mendapatkan hasil tertentu. Dalam kasus Facebook, WhatsApp, TikTok, Instagram, dan Telegram, investigator harus menyadari bahwa setiap platform memiliki batasan data yang berbeda. Oleh karena itu, metode investigasi harus disesuaikan dengan sumber bukti. Profesionalisme investigator ditunjukkan melalui ketelitian, dokumentasi, verifikasi, dan kemampuan membedakan fakta dari interpretasi.

7.27 Model Investigasi Berbasis Framework

Investigasi media sosial akan lebih efektif apabila menggunakan framework yang memiliki tahapan jelas. Salah satu pendekatan umum dapat terdiri atas identification, preservation, collection, examination, analysis, dan reporting. Identification bertujuan menentukan akun, perangkat, konten, dan kejadian yang relevan. Preservation bertujuan menjaga agar bukti tidak berubah. Collection dilakukan berdasarkan kewenangan dan metode yang sesuai. Examination digunakan untuk mengekstraksi artefak yang relevan. Analysis bertujuan menghubungkan artefak dan membangun kronologi. Reporting menyajikan temuan secara sistematis. Framework tersebut dapat diterapkan pada Facebook, WhatsApp, TikTok, Instagram, dan Telegram dengan penyesuaian terhadap karakteristik masing-masing platform. Penggunaan framework mengurangi risiko investigator melewatkan tahapan penting. Selain itu, framework membantu memastikan setiap bukti memiliki provenance dan dokumentasi yang jelas. Dalam pengembangan framework, aspek teknis, legal, etika, keamanan informasi, dan validasi hasil perlu diperhatikan. Antisipasi juga dapat dimasukkan

ke dalam framework melalui tahap lessons learned. Setelah investigasi selesai, investigator dapat menentukan kelemahan yang menyebabkan insiden dan menyusun rekomendasi perbaikan. Dengan demikian, digital forensics tidak berhenti pada menemukan bukti, tetapi menghasilkan pengetahuan yang dapat digunakan untuk memperkuat keamanan organisasi dan pengguna.

7.28 Strategi Antisipasi untuk Pengguna

Antisipasi terhadap kompromi akun media sosial harus dilakukan secara berlapis. Pengguna sebaiknya menggunakan kata sandi unik, mengaktifkan MFA, memperbarui sistem operasi dan aplikasi, serta menghindari tautan yang mencurigakan. Pemeriksaan perangkat yang memiliki akses ke akun juga perlu dilakukan secara berkala. Aplikasi pihak ketiga yang tidak diperlukan harus dicabut aksesnya. Informasi pribadi seperti nomor telepon, email, tanggal lahir, alamat, atau informasi keluarga sebaiknya tidak dipublikasikan secara berlebihan. Pengguna juga perlu berhati-hati ketika menerima pesan yang meminta kode verifikasi atau informasi keamanan. Jika terjadi aktivitas mencurigakan, pengguna harus menggunakan mekanisme pemulihan resmi platform dan mengamankan email serta nomor telepon yang terkait. Dalam kasus yang diduga serius, dokumentasi aktivitas mencurigakan perlu dilakukan sebelum data berubah atau hilang. Namun, pengguna tidak dianjurkan melakukan tindakan investigasi teknis yang berisiko atau mencoba menyerang balik pihak yang diduga sebagai pelaku. Untuk organisasi, edukasi keamanan, kebijakan penggunaan media sosial, MFA, monitoring, dan prosedur incident response perlu diterapkan. Pendekatan ini membuat keamanan tidak hanya bergantung pada kemampuan teknis individu. Dengan kombinasi technology, policy, awareness, dan incident response, risiko kompromi dapat dikurangi secara signifikan.

7.29 Strategi Antisipasi untuk Organisasi

Organisasi yang menggunakan media sosial sebagai sarana komunikasi dan pemasaran perlu memiliki kebijakan keamanan khusus. Akun resmi Facebook, Instagram, TikTok, WhatsApp, dan Telegram dapat menjadi target karena memiliki nilai reputasi dan akses publik yang besar. Organisasi harus menggunakan akun khusus dengan kredensial yang dikelola secara terpusat, MFA, pembatasan hak akses, dan prosedur pergantian administrator. Tidak semua pegawai perlu memiliki akses penuh terhadap akun organisasi. Prinsip least privilege dapat diterapkan untuk mengurangi risiko. Organisasi juga perlu

memiliki prosedur ketika administrator keluar dari organisasi agar seluruh akses segera ditinjau dan diperbarui. Monitoring terhadap perubahan profil, unggahan, pesan, dan aktivitas login dapat membantu mendeteksi kejadian lebih cepat. Jika terjadi kompromi, organisasi harus memiliki incident response plan yang menentukan siapa yang bertanggung jawab, bagaimana akun dipulihkan, bagaimana bukti diamankan, dan bagaimana komunikasi publik dilakukan. Dokumentasi insiden harus dilakukan secara sistematis. Setelah insiden selesai, organisasi perlu melakukan post-incident review untuk menemukan akar masalah. Hasil evaluasi kemudian digunakan untuk memperbarui kebijakan dan meningkatkan kesadaran pengguna. Dengan pendekatan tersebut, keamanan media sosial menjadi bagian dari information security governance, bukan hanya tanggung jawab administrator akun.

7.30 Kesimpulan Investigasi dan Antisipasi

Investigasi terhadap Facebook, WhatsApp, TikTok, Instagram, dan Telegram menunjukkan bahwa keamanan media sosial tidak dapat dilihat hanya dari kemampuan teknis platform. Banyak insiden kompromi berkaitan dengan kredensial, phishing, social engineering, perangkat yang tidak aman, sesi login yang terlupakan, aplikasi pihak ketiga, atau lemahnya prosedur pemulihan akun. Karena itu, istilah "mudah terbobol" lebih tepat dipahami sebagai adanya kondisi atau faktor yang dapat meningkatkan risiko kompromi. Dalam digital forensics, investigator harus menggunakan pendekatan sistematis mulai dari identification, preservation, acquisition, examination, analysis hingga reporting. Bukti harus dijaga integritasnya, dicatat melalui chain of custody, dan dianalisis dengan memperhatikan konteks. Antisipasi dilakukan melalui kombinasi kata sandi unik, MFA, pembaruan perangkat lunak, pengamanan perangkat, pengelolaan sesi, pembatasan aplikasi pihak ketiga, serta peningkatan literasi keamanan digital. Pengguna juga harus memahami bahwa informasi yang dipublikasikan di media sosial dapat menjadi sumber intelligence bagi pihak lain. Organisasi perlu melengkapinya dengan SOP, incident response, kontrol akses, dan edukasi keamanan. Dengan demikian, investigasi media sosial tidak hanya berorientasi pada menemukan pihak yang bertanggung jawab, tetapi juga menghasilkan pemahaman mengenai akar masalah dan rekomendasi untuk mencegah insiden berulang. Pendekatan preventif dan forensik harus berjalan secara berkesinambungan.

DAFTAR PUSTAKA

Afuan Lasmedi. 2020. "Pemanfaatan Framework Codeigniter Dalam Pengembangan Sistem Informasi Pendataan Laporan Kerja Praktek Mahasiswa Program Studi Teknik Informatika Unsoed (Codeigniter Framework Used in Information System Development for Student's Report Data Collection Prac." *Juita* I: 39–44. Web engineering , framework, CodeIgniter.

Ahmadi, H Abu, and Widodo Supriyono. 2019. "Analisis Strategi Implementasi Media Sosial." *Jurusan Manajemen, Fakultas Bisnis, Universitas Presiden [2] Jurusan Manajemen Universitas Budi Luhur E-Mail:Pandu.Cakranegara@president.Ac.Id,* 1–16.

Akses, Kode, Sistem Elektronik, and Kode Akses. 2008. "Electronic Data Interchange (EDI),."

Al-Azhar Nuh, Muhammad. 2011. "Audio Forensics : Theory and Analysis," 1–38.

Anwar, Nuril, and Imam Riadi. 2017. "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web." *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika* 3 (1): 1. https://doi.org/10.26555/jiteki.v3i1.6643.

Artha, Komang Sidhi, Edi Winarko, and Departemen Ilmu. 2016. "Perbandingan Eros , Euclidean Distance Dan Dynamic Time Warping Dalam Klasifikasi Data Multivariate Time Series Menggunakan KNN," no. Senapati.

Firdaus, Vipkas Al Hadid. 2016. "Forensik Audio Pada Rekaman Suara." *School of Electrical Engineering and Informatics Institute Technology of Bandung Bandung, Indonesia*. Bandung.

Huizen, Roy Rudolf, Ni Ketut Dewi Ari Jayanti, and Dandy Pramana Hostiadi. 2016. "Model Acquisisi Rekaman Suara Di Audio Forensik." *Semnasteknomedia Online*.

Ibrahim, Mohammed Abdaldaim, Lin Li, and Ping Wang. 2018. "The Design of 220kV Substation Grounding Grid with Difference Soil Resistivity Using Wenner and Schlumberger Methods." In *China International Conference on Electricity Distribution, CICED*, 2002:2525–30. https://doi.org/10.1109/CICED.2018.8592188.

Inggi, Rahmat, Yudi Prayudi, and Bambang Sugiantoro. 2018. "Penerapan System Development Life Cycle (Sdlc) Dalam Mengembangkan Framework Audio Forensik." *SemanTIK* 4 (2): 193–200.

Juliswara, Vibriza. 2017. “Mengembangkan Model Literasi Media Yang Berkebhinnekaan Dalam Menganalisis Informasi Berita Palsu (Hoax) Di Media Sosial.” *Jurnal Pemikiran Sosiologi* 4 (2): 142. https://doi.org/10.22146/jps.v4i2.28586.

Jumah, Muhammad Naim Al, Bambang Sugiantoro, and Yudi Prayudi. 2019. “Penerapan Metode Composite Logic Untuk Perancangan Framework Pengumpulan Bukti Digital Pada Media Sosial.” *ILKOM Jurnal Ilmiah* 11 (2): 135. https://doi.org/10.33096/ilkom.v11i2.442.135-142.

Kurniawan, Aan, and Yudi Prayudi. 2014. “Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics.” *HADFEX (Hacking and Digital Forensics Exposed)*, 1–5.

Mukti, Wisnu Ari, Siti Ummi Masruroh, and Dewi Khairani. 2018. “Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android.” *Jurnal Teknik Informatika* 10 (1): 73–84. https://doi.org/10.15408/jti.v10i1.6820.

Pomalingo, Suwito, Bambang Sugiantoro, and Yudi Prayudi. 2019. “Data Visualisasi Sebagai Pendukung Investigasi Media Sosial.” *ILKOM Jurnal Ilmiah* 11 (2): 143–51. https://doi.org/10.33096/ilkom.v11i2.443.143-151.

Raharjo, Budi. 2013. “Sekilas Mengenai Forensik Digital.” *Jurnal Sosioteknologi* 12 (29): 384–87. https://doi.org/10.5614/sostek.itbj.2013.12.29.3.

Rahayu, Yeni Dwi, and Yudi Prayudi. 2014. “Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic.” *Seminar Nasional SENTIKA* 2014 (Sentika).

Riadi, Imam, Yudi Prayudi, Jl Prof Soepomo, and S H Janturan Yogyakarta. 2016. “Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) Pada Proses Investigasi Smartphone” 2.

Saidi, La Ode Muhammad. 2017. “Pengembangan Framework Untuk Investigasi Email Forensics Menggunakan Metode Systems Development Life Cycle (SDLC).” *ILKOM Jurnal Ilmiah* 117: 14917145.

Supratman, Lucy Pujasari. 2018. “Penggunaan Media Sosial Oleh *Digital Native*.” *Jurnal ILMU KOMUNIKASI* 15 (1): 47–60. https://doi.org/10.24002/jik.v15i1.1243.

Wicaksono, Galieh, and Yudi Prayudi. 2013. “Teknik Forensika Audio Untuk Analisa Suara Pada Barang Bukti Digital.” *Semnas Unjani* 11 (2087–1716).

Yudhana, Anton, Imam Riadi, and Ikhsan Zuhriyanto. 2019. “Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research

Workshop (DFRWS).” *Jurnal TECHNO* 20 (2): 125–30.

Zuhriyanto, Ikhsan, Anton Yudhana, Program Studi, Teknik Informatika, Universitas Ahmad Dahlan, Program Studi, Sistem Informasi, Universitas Ahmad Dahlan, and Live Forensic. 2018. “Perancangan Digital Forensik Pada Aplikasi.” *Seminar Nasional Informatika* 2018 (November): 86–91.