



الجامعة الإسلامية
INDONESIA

**Pengembangan *Framework* Digital Forensics Investigation
(FDFI) Pada Sosial Media Dengan Metode *System Development
Life Cycle (SDLC)***

N u k m a n
18917216

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2022

Lembar Pengesahan Pembimbing

Pengembangan *Framework Digital Forensic Investigation (FDFI)*
Pada *Sosial Media* Dengan Metode *System Development Life Cycle (SDLC)*



Dr. Yudi Prayudi, S.Si., M.Kom

Fietyata Yuda S.Kom., M.Kom

Lembar Pengesahan Penguji

Pengembangan *Framework Digital Forensic Investigation (FDFI)* Pada *Sosial Media* Dengan Metode *System Development Life Cycle (SDLC)*

N u k m a n

18917216

Yogyakarta, Maret 2022

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom

Ketua

Dr. Ir. Bambang Sugiantoro, S.Si., M.T

Anggota I

Ahmad Luthfi, S.Kom., M.Kom., Ph.D

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia



Izzati Muhammadiyah, S.T., M.Sc., Ph.D.

Abstrak

Pengembangan *Framework Digital Forensic Investigation (FDFI)* Pada *Sosial Media* Dengan Metode *System Development Life Cycle (SDLC)*

Dari perkembangan teknologi yang begitu semakin bersaing dan semakin diperlukan dalam kehidupan masyarakat untuk keperluan sehari-harinya di *media social* seperti yang sering digunakan oleh masyarakat yaitu *Twitter, Facebook, Instagram, Youtube, WhatsApp* dan *social media* lainnya. Tapi di masyarakat umum tidak tahu bahwa data yang dikirim tersebut tersimpan didalam server pusat sehingga orang lain bisa menggunakan data tersebut untuk berbuat kejahatan seperti mengambil identitas sehingga dapat digunakan sebagai alat untuk berbuat untuk menyebarkan informasi yang tidak valid kejahatan lainnya yang bisa merugikan orang banyak. Maka dari itu peneliti mengembangkan sebuah *Framework* investigasi di dalam *social media* sebagai pengumpulan data dengan metode *System Development Life Cycle (SDLC)*. dalam pengembangan *framework* pengambilan data ini peneliti menggunakan tool Maltego sebagai alat pembuktian identitas pelaku. *Framework* yang dirancang akan menghasilkan lima tahapan yaitu *planning, analysis, design, dan implementation, maintenance*. Adapun bukti digital yang akan diperoleh dari tools tersebut diantaranya akun *twitter, email address, phone number, DNS, website* dan *social media*.

Kata kunci

framework, sosial media, maltego FDFI, system development life cycle (SDLC)

Abstract

Development of Digital Forensic Investigation (FDFI) Framework On Social Media Using the System Development Life Cycle (SDLC) Method

From technological developments that are so increasingly competitive and increasingly needed in people's lives for their daily needs on social media as is often used by the community, namely Twitter, Facebook, Instagram, Youtube, WhatsApp and other social media. But the general public does not know that the data sent is stored on a central server so that other people can use the data to commit crimes such as taking identities so that it can be used as a tool to act to spread information that is not infallible for other crimes that can harm many people. Therefore, the researcher developed an investigative framework in social media as data collection using the System Development Life Cycle (SDLC) method. In developing this data collection framework, researchers used the Maltego tool as a means of proving the identity of the perpetrator. The designed framework will produce five stages, namely planning, analysis, design, maintenance, and implementation. The digital evidence that will be obtained from these tools includes twitter accounts, email addresses, phone numbers, DNS, websites and social media.

Keywords

framework, social media, maltego, FDFI, system development life cycle (SDLC)

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Maret 2022


Nukman, S.Kom



Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari tesis ini

Kontributor	Jenis Kontribusi
Nukman	Mendesain eksperimen (70%) Menulis <i>paper</i> (100%)
Yudi Prayudi	Mendesain eksperimen (30%) Mereview artikel
Fietyata Yudha	Mendesain eksperimen (30%) Mereview artikel

Halaman Kontribusi

Penelitian ini tidak terlepas dari berbagai saran maupun bimbingan dari berbagai pihak, mulai dari pra penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Yudi Prayudi, S.Si., M.Kom dan Fietyata Yudha S.Kom., M.Kom



Halaman Persembahan

Bismillahirrahmanirrahim.

Alhamdulillah, atas ridho Allah Subhanahu Wa Ta'ala karya ini Saya persembahkan kepada kedua orang tua dan teman-teman yang selama ini telah mendukung, memberikan semangat dan motivasi dalam menyelesaikan pendidikan magister komputer saya ini, secara khususnya kepada:

1. Ayahanda (Sahnan) dan Ibunda (Rusni), yang selalu mendo'akan anaknya baik tengah malam maupun pagi hari, supaya anaknya menjadi orang yang sukses seperti yang diharapkan, begitu juga dengan do'a material yang dikeluarkan selama menjalani pendidikan tidak tanggung-tanggung pinjam sana pinjam sini untuk menyelesaikan pendidikan anaknya selama menjalankan perkuliahan.
2. Saudariku satu-satunya (khaesuanah) Terima kasih atas semua bantuan dan do'a yang telah diberikan kepada saya selama menempuh perkuliahan.
3. Joharatul Fitri, S.E. Terimakasih atas dorongan, bantuan dan dukungannya yang tidak henti-hentinya memberi dan menyemangati saya supaya pendidikan yang saya tempuh ini cepat terselesaikan.
4. Tidak lupa juga teman-teman seperjuangan forensika digital angkatan 18 yang telah memberikan support selama menempuh pendidikan ini.

Kata Pengantar

Assalamualaikum Warahmatullahi Wabarokatuh.

Puji syukur penulis panjatkan kepada Allah SWT atas limpahan dan karunia yang diberikan kepada penulis sehingga dapat menyelesaikan laporan penelitian tesis dengan judul “Pengembangan *Framework Digital Forensik Investigasi (FDFI)* Pada Sosial Media Dengan Metode *System Development Life Cycle (SDLC)*”. Adapun maksud dari penulisan laporan penelitian ini adalah sebagai persyaratan dalam mencapai jenjang pendidikan Magister Informatika konsentrasi Forensika Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia. Dalam proses penyelesaian tesis ini penulis tidak dapat menyelesaikannya bila tidak ada turut serta pihak lain yang juga ikut membantu baik secara langsung maupun tidak langsung dalam menyelesaikan penelitian ini, untuk itu penulis ingin menyampaikan rasa terima kasih kepada beberapa pihak yang telah mendukung dalam penyusunan tesis ini, antara lain:

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D, selaku rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk menimba ilmu di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D, selaku Ketua Program Studi Informatika Program Magister Fakultas Teknologi Industri, Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Yudi Prayudi S.SI., M.Kom, dan Bapak Fietyata Yudha S.Kom.,M.Kom. selaku dosen pembimbing yang telah banyak meluangkan waktunya dalam memberikan berbagai saran selama proses bimbingan.
5. Seluruh Dosen, staff administrasi dan civitas Magister Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
6. Seluruh keluarga baik Bapak, Ibu, dan Adik yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungan baik moril maupun materil.
7. Rekan-rekan mahasiswa MTI khususnya konsentrasi Forensika Digital angkatan 18 yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
8. Joharatul Fitri, S.E. yang turut membantu dan memberikan semangat dan motivasi dalam penyusunan laporan tesis.

Adapun yang masih ada kekurangan maupun kesalahan dalam laporan ini, penulis membuka lebar kritik dan sarannya agar dapat diperbaiki supaya kedepannya lebih maksimal sesuai yang diinginkan. Akhir kata dari penulis, terimakasih sebesar-besarnya semoga laporan ini bermanfaat dan bisa membantu rekan-rekan yang membutuhkan khususnya mahasiswa/mahasiswi Universitas Islam Indonesia.

Wassalamu'alaikum Warahmatullahi Wabarokatuh.



Daftar Isi

Lembar Pengesahan Pembimbing	i
Lembar Pengesahan Penguji.....	ii
Abstrak	iii
Abstract.....	iv
Pernyataan Keaslian Tulisan	v
Daftar Publikasi	vi
Halaman Kontribusi.....	vii
Halaman Persembahan	viii
Kata Pengantar.....	ix
Daftar Isi	xi
Daftar Tabel.....	xiv
Daftar Gambar	xv
Glosarium	xvii
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
1.6 Literature Review	5
BAB 2 Tinjauan Pustaka	14
2.1 Digital Forensik	14
2.1.1. Bukti Digital.....	15
2.1.2. Alat Forensik Digital.....	15
2.1.3. Bagian-Bagian Forensik.....	18

2.2.	<i>Framework Forensik</i>	19
2.3.	<i>System Development Life Cycle (SDLC)</i>	20
2.4.	Maltego	22
2.5.	Media Sosial	23
BAB 3 Metodologi Penelitian		25
3.1.	Research Problem	26
3.2.	Study Literatur	26
3.3.	Proses SDLC untuk Framework	26
3.4.	<i>Framework Digital Forensics Investigation (FDFI)</i>	27
3.5.	<i>Testing Framework</i>	27
3.6.	<i>Examination</i>	28
3.7.	<i>Report</i>	29
BAB 4 Hasil dan Pembahasan		30
4.1	SDLC untuk Framework	30
4.1.1	Planning	32
4.1.2	Analysis	34
4.1.3	Design	35
4.1.4	Implementation	41
4.1.4.1	Problem	42
4.1.4.2	Barang Bukti Digital	43
4.1.4.3	Identifikasi	44
4.1.4.3.1	Pencarian Identitas	44
4.1.4.3.2	Sosial Media	45
4.1.4.3.3	<i>Analysis</i>	45
4.1.4.4	Report	46
4.1.4.5	Hasil Analisa Framework	46
4.1.5	Maintenance	47

4.2	SDLC (System Development Life Cycle)	47
4.3	Testing Framework.....	47
4.3.1	Simulasi <i>framework</i>	47
4.3.2	Analysis <i>framework</i>	49
BAB 5 Kesimpulan dan Saran.....		58
5.1	Kesimpulan.....	58
5.2	Saran	58
Daftar Pustaka		59



Daftar Tabel

Tabel 1. 1 Rangkuman Literatur Review Penelitian Investigasi Sosial Media	8
Tabel 2. 1 Alat-alat Forensik Digital	17
Tabel 3. 1 Perbandingan framework	28
Tabel 4. 1 Proses Pengembangan framework pada SDLC	30
Tabel 4. 2 Identifikasi framework	34
Tabel 4. 3 Perbandingan pengembang yang sudah ada dan pengembang baru.....	35
Tabel 4. 4 Identifikasi Tahapan-Tahapan Framework.....	35
Tabel 4. 5 Normalisasi Framework tahap awal	35
Tabel 4. 6 Proses Normalisasi Tahapan.....	36
Tabel 4. 7 Perbedaan Framework	38
Tabel 4. 8 Normalisasi Framework FDFI.....	39
Tabel 4. 9 Analisa Framework	46
Tabel 4. 10 Input, Proses dan Output Pemeliharaan.....	47
Tabel 4. 11 Spesifikasi Perangkat.....	50
Tabel 4. 12 Perbedaan Hasil Investigasi Akun.....	56

Daftar Gambar

Gambar 1. 1 Data Pengguna sosial di dunia. (wearesocial.com)	1
Gambar 1. 2 Data Platforms aktif di social media. (websindo.com).....	2
Gambar 1. 3 Tahapan-tahapan Penelitian.....	12
Gambar 2. 1 Alat Perangkat keras Forensik	16
Gambar 2. 2 Tampilan Awal Maltego	23
Gambar 2. 3 Perkembangan media sosial antara gender dan umur (websindo.com).....	24
Gambar 3. 1 Alur Metode Penelitian.....	25
Gambar 3. 2 Tahapan System Development Life Cycle (SDLC)	26
Gambar 3. 3 Tahapan Testing Framework	27
Gambar 3. 4 Proses Simulasi Framework	28
Gambar 4. 1 Proses Penerapan SDLC (System Development Life Cycle).....	30
Gambar 4. 2 Hasil kolaborasi framework pengembang sebelumnya	32
Gambar 4. 3 Framework FDFI Investigation Digital	39
Gambar 4. 4 Flowchart alur kerja investigasi.....	41
Gambar 4. 5 Akun-akun Palsu CustomerCare BNI di twitter	42
Gambar 4. 6 Barang Bukti Digital postingan Akun Palsu Customercare BNI.....	43
Gambar 4. 7 Hasil Pencarian Data 1.....	44
Gambar 4. 8 Hasil Pencarian Data 2.....	45
Gambar 4. 9 Ilustrasi publikasi akun twitter.....	48
Gambar 4. 10 Bukti screen balasan pesan BNIcustomer care	48
Gambar 4. 11 Framework yang dikembangkan.....	49
Gambar 4. 12 Barang bukti akun twitter	50
Gambar 4. 13 Ikatan kejahatan dengan orang lain	51

Gambar 4. 14 Penyimpanan Barang Bukti Digital	52
Gambar 4. 15 Keterkaitan akun twitter	52
Gambar 4. 16 Hasil temuan investigasi	53
Gambar 4. 17 Detail view dan Layout entity	54
Gambar 4. 18 Hasil temuan investigasi BNICustomerCare	54
Gambar 4. 19 Detail view dan Layout entity BNICustomerCare	55
Gambar 4. 20 Screen Dokumentasi barang bukti digital 1	55
Gambar 4. 21 Screen Dokumentasi barang bukti digital 2	56



Glosarium

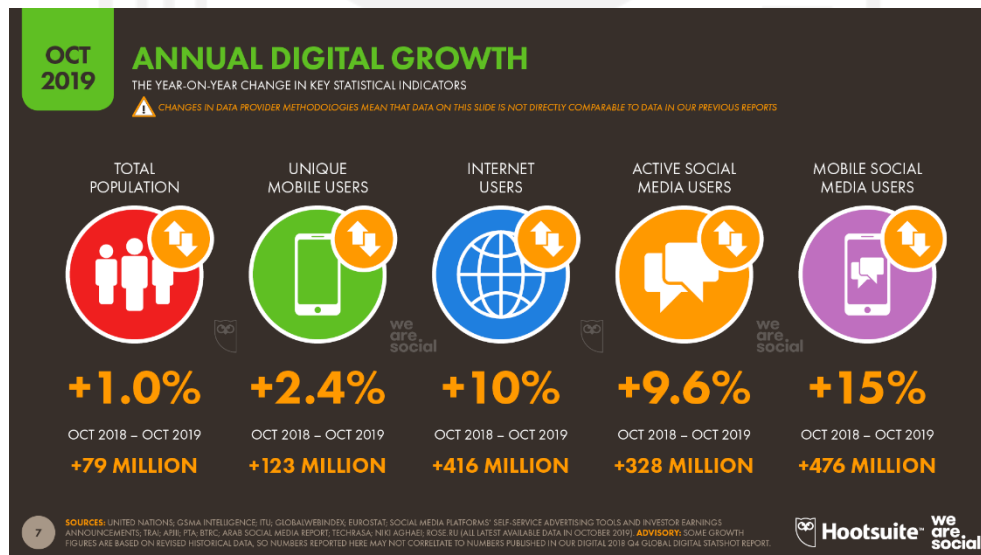
FDFI	- Framework Digital Forensic Investigation
FDIM	- Digital Forensics Investigation Model
DFAT	- Digital Forensics Analysis Team
SDLC	- System Development Life Cycle
ITE	- Informasi dan Transaksi Elektronik
PNG	- Portable Network Graphics
GPL	- General Public License
UFED	- Universal Forensic Extraction Device
USB	- Universal Serial Bus
GSM	- Global System for Mobiles
RAD	- Rapid Application Development
CE	- Community Edition
OSINT	- Open Source Intelligence
BNI	- Bank Negara Indonesia
VGA	- Video Graphics Array
ATM	- Automated Teller Machine

BAB 1

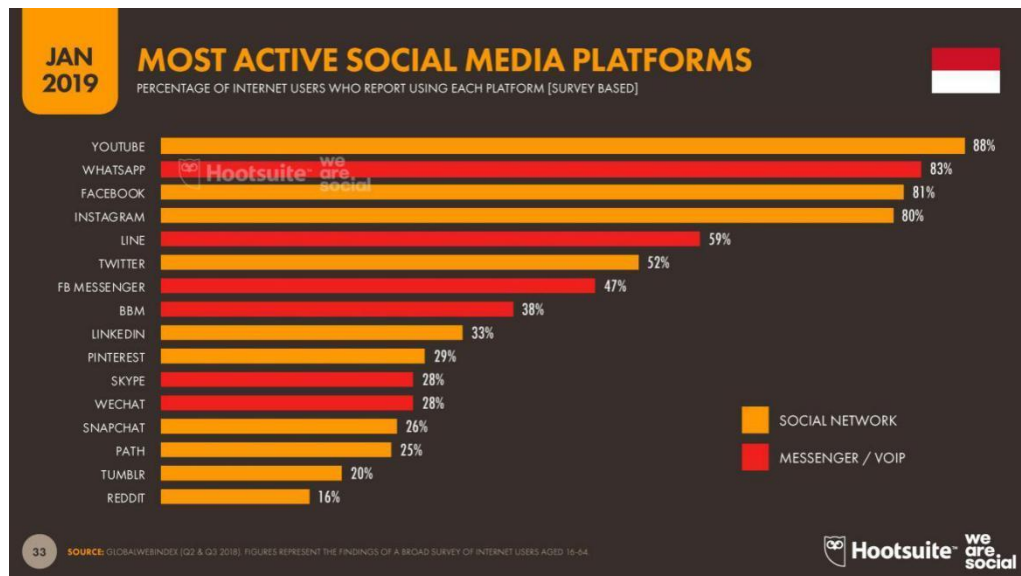
Pendahuluan

1.1 Latar Belakang

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 penggunaannya (88%), dikutip *whatsapp* (83%), *Facebook* (81%), *Instagram* (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 dikembangkan oleh (Al Jumah, Sugiantoro, and Prayudi 2019) dalam penelitiannya menerapkan *composite logic* untuk pengumpulan bukti digital pada media sosial. Maka penelitian 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 mencari solusi untuk investigasi sosial media dalam mengembangkan sebuah *framework* menggunakan metode *System Development Life Cycle (SDLC)* dengan tahapan-tahapan yang digunakan *planning, analysis, design, maintenance, dan implementation*.

Pemanfaatan *framework* dalam penelitian 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, penelitian ini akan mengembangkan *framework* sebagai pendukung kesuksesan dalam penyidikan *cybercrime* pada khususnya di media sosial.

Dari segi banyak penelitian dalam mengembangkan investigasi untuk membangun sebuah *framework* dari beberapa metode yang digunakan seperti halnya penelitian 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 penelitian 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 pengembangan 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 penelitian 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 metodologi yang digunakan untuk mengembangkan sistem-sistem tersebut. SDLC ini juga merupakan pola yang diambil dari sistem perangkat lunak dengan tahap-tahap yang ada pada penelitian ini yaitu *planning, analysis, design, maintenance, dan implementation*. Konsep dari SDLC mendasari beberapa jenis metodologi pengembangan perangkat lunak.

1.2 Rumusan Masalah

Dari latar belakang diatas, maka rumusan masalah yang diuraikan adalah :

- a. Bagaimana cara mengembangkan sebuah *framework* berdasarkan *framework* yang sudah ada sebelumnya.
- b. Bagaimana cara menggunakan *System Development Life Cycle (SDLC)* untuk pengembangan *framework* investigasi.
- c. Bagaimana cara melakukan identifikasi terhadap akun yang menyebarkan informasi palsu di media sosial.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

- a. Penelitian ini hanya mengembangkan sebuah *framework* sudah ada sebelumnya tentang sosial media.
- b. Simulasi kasus yang akan dikembangkan dalam penelitian ini kasus penyebaran akun palsu di sosial media.
- c. Sosial media yang dituju dalam pengumpulan data ini hanya twitter saja.

1.4 Tujuan Penelitian

Dari rumusan masalah diatas maka tujuan dari penelitian ini adalah :

- a. Untuk membangun sebuah *Framework* dalam pengumpulan data digital pada sosial media dengan mengembangkan penelitian sebelumnya.
- b. Untuk mendapatkan barang bukti digital pada akun media sosial.
- c. Menerapkan *System Development Life Cycle (SDLC)* sebagai pengembangan sistem investigasi khususnya di sosial media .

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dalam penelitian ini adalah :

- a. Menghasilkan pengembangan sebuah *framework* baru untuk investigasi social media

- b. Supaya mempermudah penyidikan didalam permasalahan pada social media.
- c. Mudah-mudahan penelitian ini bisa membantu dan memberikan kontribusi pada peneliti selanjutnya.

1.6 Literature Review

Forensika digital program yang sudah lama digunakan dalam penyidikan tetapi dalam perkembangan yang sekarang ini di era semua digital dan berbasis media social maka forensika digital ini dikembangkan dan menjadi terpopuler banyak digunakan pada investigasi di media social. Adapun hasil penelitian dari (Pomalingo, Sugiantoro, and Prayudi 2019) tentang Data Visualisasi Sebagai Pendukung Investigasi Media Sosial dengan metode *Social Network Analysis* di penelitiannya menggunakan metode graf berarah yang dapat digunakan untuk melakukan analisa investigasi pada berbagai media sosial sehingga mendapatkan satu kesatuan visualisasi, dimana simpul atau mode menggambarkan entitas seperti person, postingan, komentar, dan lainnya, dan sisi menggambarkan sebuah garis berarah yang menyatakan hubungan setiap simpul. Penggunaan graf berarah dapat membantu menyederhanakan proses investigasi pada berbagai media sosial.

Hasil penelitian juga dari (Ahmadi and Supriyono 2019) tentang Analisis Strategi Implementasi Media Sosial menggunakan metode *Miles* dan *Huberman* dari penelitiannya menyatakan bahwa studi kasus yang diartikan sebagai proses menginvestigasi terhadap peristiwa-peristiwa yang aktual sebagai unit analisis. dan juga dapat mengemukakan alasan memilih rancangan jenis penelitian studi kasus adalah (1) karena peneliti berminat untuk menyelidiki proses, dan (2) karena fenomena yang diselidiki itu sangat unik. Studi kasus juga bertujuan untuk mengembangkan pengetahuan secara mendalam guna mengenal objek yang akan diteliti, sehingga sifat penulisnya lebih banyak eksploratif dan deskriptif. Selain itu penelitian deskriptif berusaha menggambarkan suatu gejala sosial. Dengan kata lain, peneliti terjun langsung ke lapangan dan kemudian menggambarkan sifat atau sesuatu yang sedang terjadi.

Penelitian selanjutnya dari (Anwar and Riadi 2017) tentang Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web menggunakan metode *WhatsApp Evidence*, *Riset Goal Investigation Methode*, *Forensics Tools Investigator*, *Digital Evidence Risk* hasil dari penelitiannya telah menunjukkan bahwa seseorang dapat memperoleh akses lengkap ke semua informasi di *WhatsApp* baik itu *WhatsApp Smartphone* maupun *WhatsApp Web*. Sebagian besar aplikasi *chat* mengikuti pola sinkronisasi pesan, kontak dan data pengguna yang sama saat *sync* dan memperbarui data

percakapan secara berkala. Pendekatan yang diambil memberi garis besar umum untuk semua aplikasi serupa yang berjalan di perangkat ber-*platform Android* maupun *Windows* seperti *Telegram* dan sejenisnya. Penelitian ini dapat bermanfaat untuk *Mobile Forensik Analysis* dan *Investigation* pada *smartphone Android* dan aplikasi ganda berbasis *web browser*. *Database QR Code* membutuhkan autentikasi terhadap *smartphone* hanya sekali setiap saat *login* pertama kali sehingga dibutuhkan kewaspadaan penggunaanya seperti penggunaan *pattern lock* pada *smartphone* dan *login user password* pada komputer penggunaanya. Proses akuisisi langsung terhadap *smartphone* korban dan analisis *web browser* pada komputer. Diharapkan kedepan lebih banyak penelitian yang dapat dilakukan pada interpretasi data percakapan *WhatsApp* dalam bentuk jurnal atau naskah lain sebagai literatur selanjutnya.

Penelitian selanjutnya dari (Mukti, Masruroh, and Khairani 2018) tentang Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial *Facebook* Dan *Twitter* Pada *Smartphone Android* menggunakan metode simulasi untuk bukti-bukti dari penelitiannya dan Berdasarkan hasil dari tahapan-tahapan metode simulasi yang telah dilakukan, proses pencarian dan analisa bukti forensik pada aplikasi media sosial *Facebook* dan *Twitter* yang diakses pada *smartphone Android* dapat disimpulkan bahwa data-data pada media sosial *Facebook* dan *Twitter* tidak sepenuhnya disimpan pada *server*. Data tersebut juga tersimpan pada memori internal perangkat *Android* yang hanya dapat diakses setelah perangkat *Android* melalui proses *root*.

Penelitian selanjutnya oleh (Al Jumah, Sugiantoro, and Prayudi 2019) tentang perancangan *framework* pengumpulan bukti digital pada sosial media dengan metode dengan penerapan metode *composite logic*. Dari hasil penelitian ini mendapatkan data identitas pelaku yang berbuat pencemaran nama baik yang ada di sosial media *twitter*. Data yang didapatkan dari hasil pengumpulan data identitas yaitu, location, phone number, email, profil sosial media dll. *Composite logic* ini membantu sebagai metode yang digunakan dalam pengumpulan datanya untuk identifikasi *timeframe* yang akan dibuat. Pemodelan yang digunakan membantu penelitian dalam mengeksplorasi keterhubungan dari aktivitas berbeda dengan tujuan yang sama. Sehingga memudahkan peneliti dalam melakukan klasifikasi dan kolaborasi beberapa *framework* yang pada akhirnya akan menghasilkan satu set *framework*.

Penelitian selanjutnya oleh (Saidi 2017) tentang pengembangan *framework* untuk investigasi email menggunakan metode *system development life cycle (SDLC)*, penelitian ini

menggunakan 4 tahapan untuk melakukan pengembangan *framework* yang akan di bangun yaitu, *identifying research problem*, *study literatur*, *SDLC* untuk *framework*, dan *testing framework*, di dalam penelitiannya mengaitkan antara *framework* dengan *system development life cycle* dan dari hasil penelitiannya menghasilkan memiliki karakteristik yang sama yaitu memiliki elemen-elemen yang saling berhubungan antara satu dengan yang lainnya yaitu membentuk *framework*. Pengembangan *framework* dengan metode SDLC ini memerlukan 5 tahapan yaitu, *planning*, *analysis*, *design*, *maintenance*, dan *implementation* sehingga *framework* yang dihasilkan bisa menganalisis investigasi email yang maksimal.

Penelitian selanjutnya oleh (Juliswara 2017) tentang Mengembangkan Model Literasi Media yang Berkebhinekaan dalam Menganalisis Informasi Berita Palsu (*Hoax*) di Media Sosial dengan metode *Empowering Eight* Ujaran kebencian (*hate speech*) mengiringi kebebasan berpendapat di media sosial. Sejak pilpres 2014 lalu, istilah ‘hater’ pun dikenal luas, yang menandai banyak orang membuat pesan ujaran kebencian pada suatu kelompok tertentu. Kebhinekaan sebagai pengikat sosial diuji karena kecenderungan praktik ujaran kebencian yang lakukan melalui media sosial. keadaan itu diperparah oleh penyalahgunaan media sosial seperti penyebaran berita bohong atau informasi palsu (*hoax*) yang mengakibatkan menimbulkan permusuhan dan tidak sesuai dengan budaya bangsa Indonesia yang mengutamakan toleransi. Dalam rangka merespon berkembangnya ujaran kebencian, kajian ini mencoba untuk mengembangkan suatu model literasi media yang berkebhinekaan dalam menganalisis informasi palsu (*hoax*) dalam berita di media sosial. Melalui pengembangan model kajian literasi media sebagai pendekatan yang memberdayakan pengguna media sosial (*netizen*) maka diasumsikan para netizen akan lebih mampu mengkonstruksi muatan yang positif dalam memanfaatkan media sosial.

Tabel 1. 1 Rangkuman Literatur Review Penelitian Investigasi Sosial Media

Literatur	Latar Belakang	Issue Business Model	Konsep Storage	Konsep Pencatatan Informasi	Konsep Akses Kontrol dan Secure Platform	Framework
(Pomalingo, Sugiantoro, and Prayudi 2019)	Penggunaan graf berarah dapat membantu menyederhanakan proses investigasi pada berbagai media social.	sebuah visualisasi berupa graf berarah yang merepresentasikan data dari berbagai media sosial	-	Data Visualisasi Sebagai Pendukung Investigasi Media Sosial dengan metode <i>Social Network Analysis</i>	-	-
(Zuhriyanto et al. 2018)	Pengambilan bukti digital tindak kejahatan pada penelitian ini dilakukan dengan tahapan penelitian dan analisa mengadaptasi metode forensik dari National Institute of Justice (NIJ)	Kejahatan pada media sosial Facebook dan Twitter sangat meningkat	-	Pengaruh teknologi memberikan kemudahan kepada manusia dalam hal komunikasi	-	-
(Riadi et al. 2016)	Cara pembuktian untuk mendapatkan bukti yang valid adalah dengan melakukan investigasi menggunakan pendekatan penanganan bukti digital yang	Smartphone merupakan salah satu bentuk teknologi yang digunakan untuk melakukan penipuan melalui fasilitas Short Message Service (SMS)	-	persiapan(pre-process), olah TKP (proactive process), pemeriksaan barang bukti di laboratorium digital forensics(reactive process) dan laporan hasil pemeriksaan	-	Integrated Digital Forensics Investigation Framework versi 2 (IDFIF v2)

Literatur	Latar Belakang	Issue Business Model	Konsep Storage	Konsep Pencatatan Informasi	Konsep Akses Kontrol dan Secure Platform	Framework
	dikenal dengan istilah Framework			barang bukti digital(post-process)		
(Rahayu and Prayudi 2014)	Kajian ilmiah forensika digital bertujuan untuk membuktikan sebuah peristiwa di depan persidangan yang jelas, tidak ambigu dan dapat dipertanggungjawabkan di mata hukum		-	Penggunaan metode ilmiah turunan dan pembuktian melalui tahapan collection, validation, identification, analysis, interpretation, documentation, and presentation	-	Integrated Digital Forensics Investigation Framework (IDFIF)
(Inggi, Prayudi, and Sugiantoro 2018)	mengembangkan framework audio forensik dengan menerapkan Systems Development Life Cycle (SDLC) dalam melakukan proses pengembangan framework audio forensik.	Salah satu barang bukti elektronik yang ditemukan di TKP atau yang berkaitan dengan kasus pidana maupun perdata adalah barang bukti alat perekam suara (audio reorder) yang dengan orang lain	-	planning, analysis, design, implementation, dan maintenance	<i>System Development Life Cycle (SDLC)</i>	Framework Audio Forensik

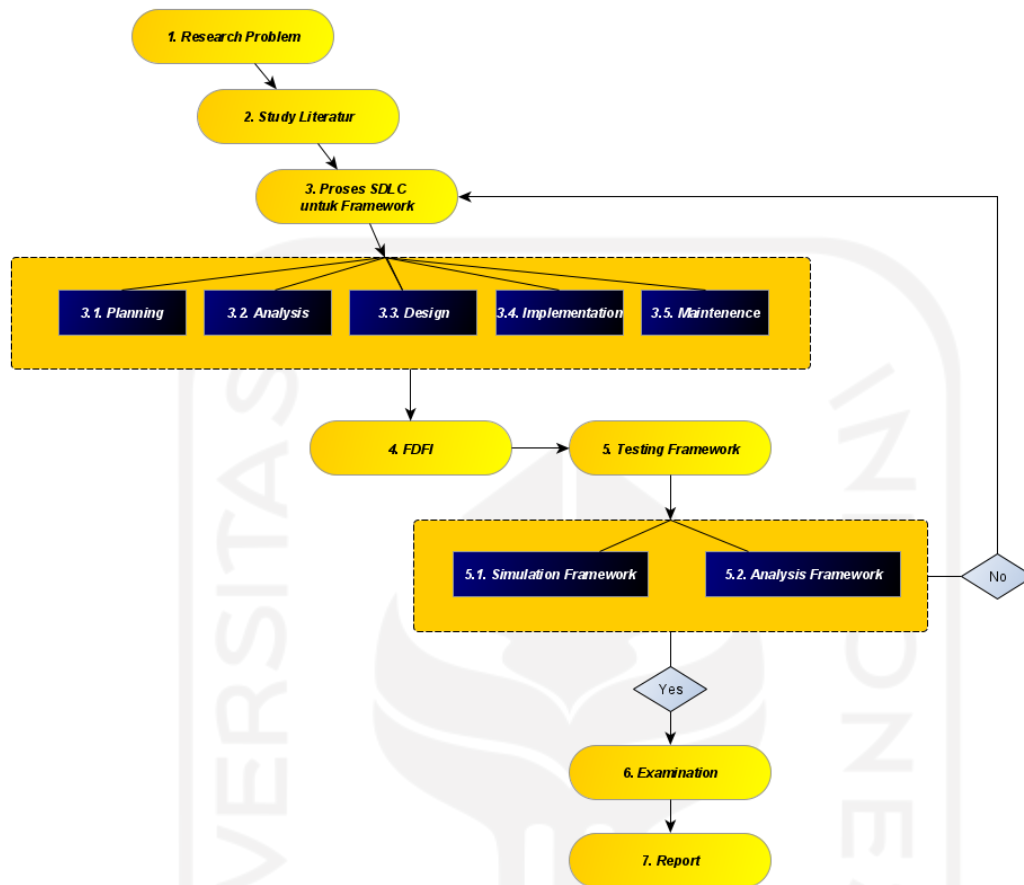
Literatur	Latar Belakang	Issue Business Model	Konsep Storage	Konsep Pencatatan Informasi	Konsep Akses Kontrol dan Secure Platform	Framework
		File rekaman suara (Audio) sangat mudah dimanipulasi dan untuk penanganannya berbeda dengan komputer forensik secara umum				
(Saidi 2017)	Electronic Mail atau biasa disingkat juga email yang dalam bahasa Indonesia diartikan sebagai “surat elektronik” merupakan sebuah sistem yang bertujuan untuk mengirim dan menerima pesan elektronik berupa file gambar, audio, video, dan lain-lain dari satu orang ke orang lain di belahan dunia melalui jaringan internet	investigasi metadata, pencarian kata kunci, port scanning, dll untuk penulis atribusi dan identifikasi penipuan e-mail.	-	header analysis, bait tactics, server investigation, network device investigation, software embedded identifiers, dan sender mailer fingerprints.	<i>System Development Life Cycle (SDLC)</i>	framework investigasi email forensics
(Al Jumah, Sugiantoro, and Prayudi 2019)	Media sosial telah menjadi media yang populer untuk masyarakat, namun	Beberapa pihak juga memanfaatkan media sosial untuk	-	Pre-process, Collection, Analysis dan Report	metode Digital Forensic Intelligence + Open Source	Framework social media digital

Literatur	Latar Belakang	Issue Business Model	Konsep Storage	Konsep Pencatatan Informasi	Konsep Akses Kontrol dan Secure Platform	Framework
	dengan popularitas media sosial saat ini banyak pengguna akun media sosial tanpa sadar telah menyebarkan informasi berupa data pribadi seperti alamat email, foto, nomor telepon, lokasi, tempat tinggal dan perilaku mereka setiap hari.	melakukan tindak kejahatan seperti penipuan, cyber bullying, perdagangan anak, prostitusi online, ujaran kebencian, sara dan lain-lain			Intelligence (DFINT + OSINT). DFINT + OSINT memungkinkan Composite Logic	
Usulan	Mebutuhkan <i>framework</i> untuk menyelesaikan permasalahan tersebut untuk mencari identitas si pengguna media sosial	Informasi di media sosial sering tidak disadari oleh pengguna media sosial baik itu di <i>facebook</i> , <i>twitter</i> maupun di <i>instagram</i> .	-	<i>planning, analysis, design, maintenance, dan implementation</i>	<i>System Development Life Cycle (SDLC)</i>	<i>Framework Digital Forensics Investigation (FDFI)</i> pada media sosial



1.1. Metode Penelitian

Tahap-tahap yang akan dilakukan untuk proses penelitian ini lihat pada Gambar 1.3.



Gambar 1. 3 Tahapan-tahapan Penelitian

1.2. Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas, didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan tentang teori-teori dari berbagai bahan referensi yang terkait guna memecahkan masalah dalam penelitian ini.

BAB III METODOLOGI PENELITIAN

Pada bab ini membahas tentang langkah-langkah atau prosedur penelitian, sehingga mampu menyelesaikan masalah secara sistematis.

BAB IV PEMBAHASAN

Pada bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis, dan evaluasi dari penelitian yang diangkat.

BAB V PENUTUP

Bab ini merupakan bab terakhir yang memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama penelitian dan rekomendasi untuk pengembangan penelitian selanjutnya



BAB 2

Tinjauan Pustaka

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

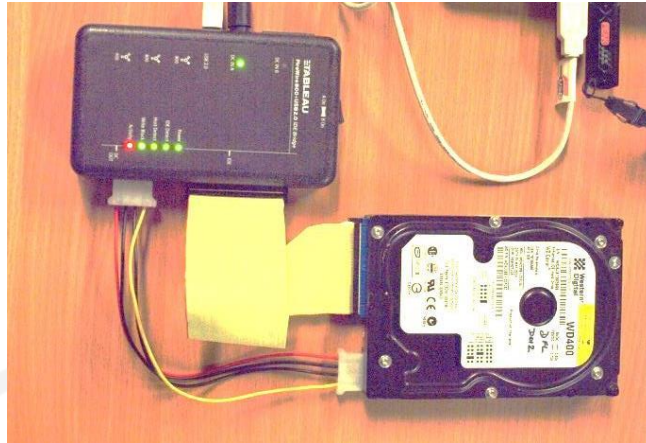
Bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi digital dapat menjadi subjek penyidikan, dan setiap pembawa informasi yang ditargetkan untuk diperiksa harus diperlukan 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 penyidik 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
<i>Digital Forensics Framework</i>	Digunakan oleh profesional atau non-ahli, ini digunakan untuk lacak balak digital, untuk mengakses perangkat jarak jauh atau local, <i>forensik system windows</i> atau <i>linux</i> , pemulihan berkas yang dihapus, pencarian cepat untuk mendata berkas.	GPL
<i>Open Computer Forensics Architecture</i>	Dibangun di platform linux dan menggunakan basis dat <i>postgreSQL</i> untuk penyimpanan datanya. Dibangun oleh Badan Kepolisian Nasional Belanda untuk mengotomatisasi proses forensik digital.	GPL
<i>CAINE</i>	<i>Computer Aided Investigative Environment</i> adalah distro linux yang dibuat untuk forensik digital. <i>CAINE</i> menawarkan lingkungan untuk mengintegrasikan perangkat lunak yang ada sebagai modul .	GPL
<i>X-Ways Forensics</i>	<i>Platform</i> canggih untuk memeriksa forensik digital, yang berjalan pada semua versi <i>windows</i> yang tersedia dan bekerja secara efisien.	Komersial
<i>SAINS Investigative Forensics Toolkit-SIFT</i>	<i>System operasi forensik</i> multi-tujuan berbasis Ubuntu, dilengkapi semua alat yang diperlukan yang digunakan dalam proses forensik digital.	Sumber terbuka dan berbayar
<i>EnCase</i>	<i>Platform</i> 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. <i>EnCase</i> juga dapat menghasilkan laporan berdasarkan bukti.	Komersial
<i>Registry Recon</i>	Alat analisis <i>registry</i> , alat ini mengekstrak informasi <i>registry</i> dari barang bukti dan kemudian membangun kembali representasi <i>registry</i> .	Komersial
<i>The Sleuth Kit</i>	Alat yang berbasis <i>Unix</i> dan <i>Windows</i> 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.	<i>IBM Open Source Licence Common Public License GPL</i>
<i>Libforensics</i>	Pustaka untuk mengembangkan aplikasi forensik digital dikembangkan dengan alat <i>python</i> dan dilengkapi dengan berbagai alat demo untuk mengekstrak berbagai informasi dari berbagai jenis barang bukti digital.	LGPL
<i>Volatility</i>	<i>Framework</i> 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 penyelidikan 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 tahapan 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 tahapan yang sering digunakan yaitu, *planning* (rencana), *analysis* (analisis), *design* (desain), *implementation* (implementasi), dan *maintenance* (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 sistematis dan sekuensial yang dimulai pada tingkat dan kemajuan sistem pada seluruh tahapan 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 mendahului 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 tahapan 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 tahapan-tahapan seperti : *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

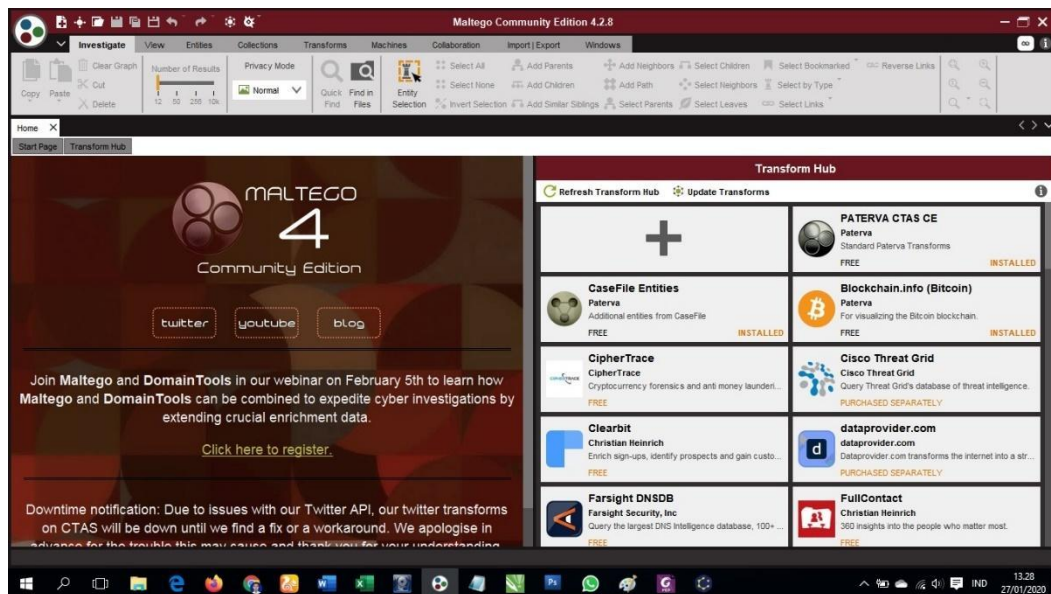
Model SDLC ini pelaksanaan proses yang terjadi secara berurutan dalam bentuk V. Dikenal juga sebagai model *Verifikasi* dan *Validasi*.

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.

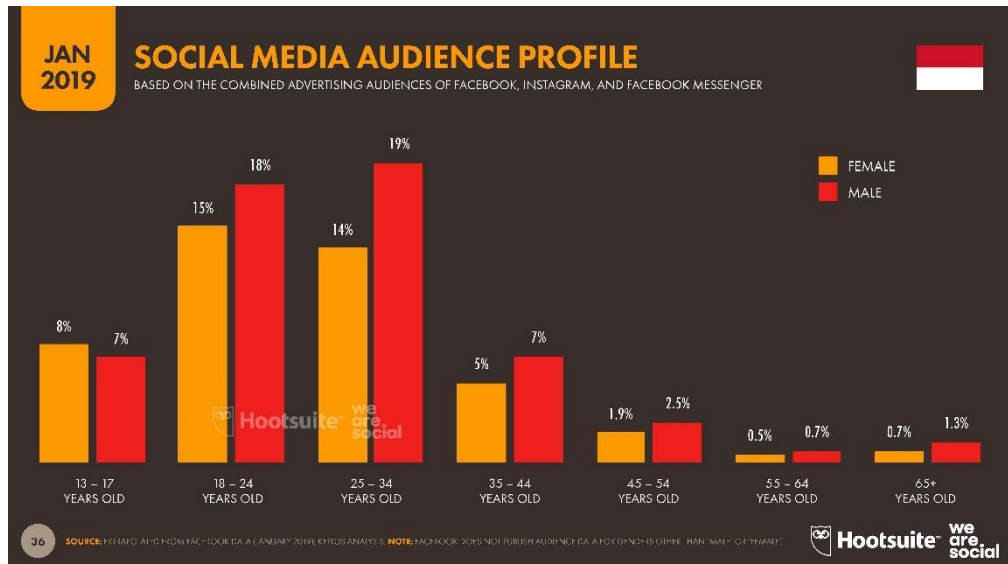


Gambar 2. 2 Tampilan Awal Maltego

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 penelitian (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.



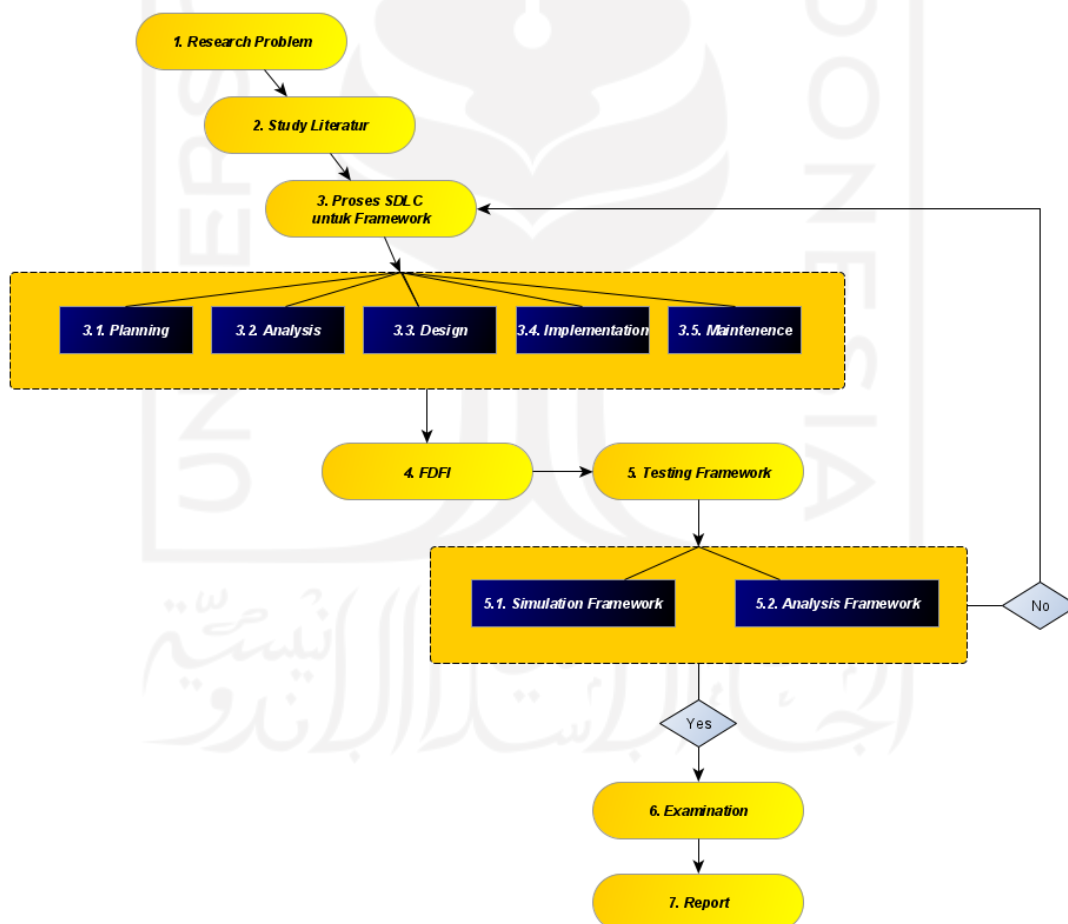
Gambar 2. 3 Perkembangan media sosial antara gender dan umur (websindo.com)

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 3

Metodologi Penelitian

Metode yang akan digunakan dalam pengambilan data pada penelitian ini adalah *System Development Life Cycle (SDLC)* yang bagaimana untuk membangun sebuah *Framework* Investigasi pada Media Sosial dan pada akhirnya menghasilkan *Reporting* yang maksimal. Metode penelitian ini meliputi ada 4 tahapan sebagai proses investigasi masalah yang ada, yaitu *research problem*, *study literatur*, *framework digital forensics investigation (FDFI)* dengan metode *system development life cycle (SDLC)* dalam pengembangan *framework* ini dibagi menjadi lima bagian diantaranya, *planning*, *analysis*, *design*, *implementation*, dan *maintenance*, dalam *testing framework* ini dibagi 2 lagi diantaranya *simulation framework*, dan *analysis framework*.



Gambar 3. 1 Alur Metode Penelitian

Dari gambar 3.1 adalah alur dari metodologi penelitian yang menerangkan berdasarkan hasil dari review dari penelitian. Pada grafik ini menjelaskan secara singkat tentang pembangunan *framework* digital forensik investigasi pada media sosial dengan menggunakan metode *System Development Life Cycle (SDLC)*.

3.1. Research Problem

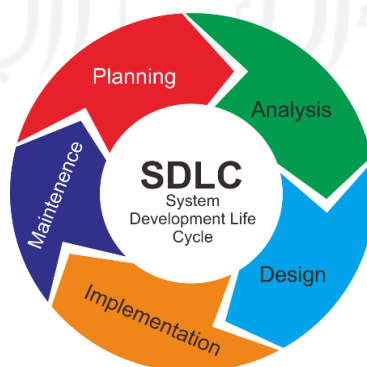
Tahap ini adalah tahap awal dalam penelitian untuk mencari barang bukti digital forensik yang akan menentukan berjalannya sebuah sistem. Penelitian ini dilakukan sesuai dengan masalah yang ada, seperti halnya pada kasus yang peneliti ambil disini adalah membangun *framework digital forensics investigasi* dan kasus ini menggunakan metode *System Development Life Cycle (SDLC)* sehingga bisa menjadi acuan bagi para penyidik *forensics* digital.

3.2. Study Literatur

Sebelum melakukan penelitian maka perlu mencari dokumen, buku, artikel, jurnal makalah ataupun di situs-situs yang membutuhkan informasi mengenai permasalahan yang akan diteliti. Pencarian informasi dari berbagai sumber ini adalah untuk mencari problem yang ada dan yang belum diteliti oleh orang lain, ataupun masalah yang ada tetapi untuk pengembangan lebih lanjut yang sudah diteliti oleh orang lain sehingga dapat di publikasikan ke penyidik forensik. Maka terkait dengan penelitian ini problem yang akan diteliti adalah pembuatan *framework digital forensics investigation* pada media sosial.

3.3. Proses SDLC untuk Framework

Pada tahapan ini penelitian akan mengembangkan sebuah *framework* dengan menggunakan metode *System Development Life Cycle (SDLC)*. Dalam membangun *framework Digital Forensics Investigation (FDFI)* ini ada 5 tahap proses yaitu *planning*, *analysis*, *design*, *implementation*, dan *maintenance*.



Gambar 3. 2 Tahapan *System Development Life Cycle (SDLC)*

Adapun tahap diatas menerangkan sebagai berikut :

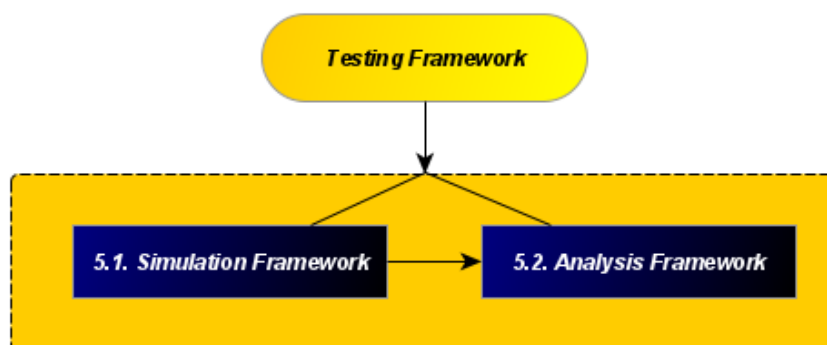
1. *Planning* tahapan yang bertujuan untuk mengidentifikasi sistem yang akan dikembangkan dan sasaran yang akan dicapai.
2. *Analysis* merupakan tahap penelitian atas sistem yang sudah digunakan dan melakukan aktifitas literatur untuk menentukan suatu kasus yang bisa ditangani oleh sistem, dan akan mengidentifikasi terhadap sistem sebelumnya yang sudah dikembangkan.
3. *Design* tahap ini untuk menentukan proses tahapan-tahapan dan teknik yang akan menerapkan sistem baru yang sudah dikembangkan dari sistem sebelumnya.
4. *Implementation* tahapan ini mengimplementasikan rancangan dari tahap-tahap sistem yang sudah dibangun dan akan dikembangkan beserta akan melakukan *testing* terhadap sistem tersebut.
5. *Maintenance* tahapan ini akan melakukan proses pemeliharaan sistem selama penggunaan agar tetap beroperasi secara teratur.

3.4. *Framework Digital Forensics Investigation (FDFI)*

Setelah melakukan proses dalam pembuatan *framework* menggunakan *system development life cycle (SDLC)* maka akan menghasilkan *framework digital forensics investigation (FDFI)*

3.5. *Testing Framework*

Testing ini adalah tahap untuk percobaan *framework* yang sudah di rancang dan bertujuan untuk memastikan kelayakan apakah sudah bisa diterapkan atau belum. Dalam percobaan ini diperlukan beberapa tahapan-tahapan sehingga supaya bisa menghasilkan yang maksimal dalam investigasi di media sosial. Adapun tahapan-tahapan dari *testing* untuk *framework* ini yaitu, simulasi *framework*, *analysis framework*.



Gambar 3. 3 Tahapan *Testing Framework*

3.5.1. Simulasi *Framework*

Pada tahap simulasi *framework* ini adalah skenario proses kasus terhadap kejahatan yang ada pada sosial media khususnya di twitter, kemudian akan di analisis menggunakan *framework* yang sudah dibuat, maka proses analisis juga akan diidentifikasi melalui tahapan-tahapan investigasi pada *framework* yang ada.



Gambar 3. 4 Proses Simulasi *Framework*

3.5.2. *Analysis Framework*

Proses analisis ini adalah tahapan untuk melihat perbandingan antara *framework* yang sudah dikembangkan sebelumnya. Berdasarkan hasil simulasi yang diterapkan maka akan dibandingkan dengan *framework* yang sudah ada sebelumnya.

Tabel 3. 1 Perbandingan *framework*

No.	<i>Framework</i> yang sudah dikembangkan	<i>Framework</i> yang baru	Analisis <i>framework</i> digital forensik investigasi
1	Tahapan ¹	Tahapan ¹	Tahapan ¹
2	Tahapan ²	Tahapan ²	Tahapan ²
3	Tahapan ³	Tahapan ³	Tahapan ³

3.6. *Examination*

Pada tahap ini adalah melakukan analisa proses yang sudah di sudah di *testing* sehingga *framework* yang sudah dirancang dapat menghasilkan yang sempurna. Didalam pemeriksaan ini untuk memastikan keberhasilan *framework* yang sudah dirancang. Untuk tahap evaluasi terhadap *framework* yang digunakan bisa melihat kekurangan-kekurangan proses prosedur yang telah dibuat dan diuji coba sebelumnya.

3.7. *Report*

Tahap report ini berisi tentang laporan dari hasil *framework* yang dibuat dan hasil dari perbandingan dengan *framework* sebelumnya, sehingga hasil akhir dari investigasi pada media sosial bisa didapatkan serta sudah di analisis dan mendapatkan perbandingan yang sesuai, maka hasil tersebut akan dibuatkan laporan barang bukti digital ataupun document tentang kesimpulan penelitian tersebut.

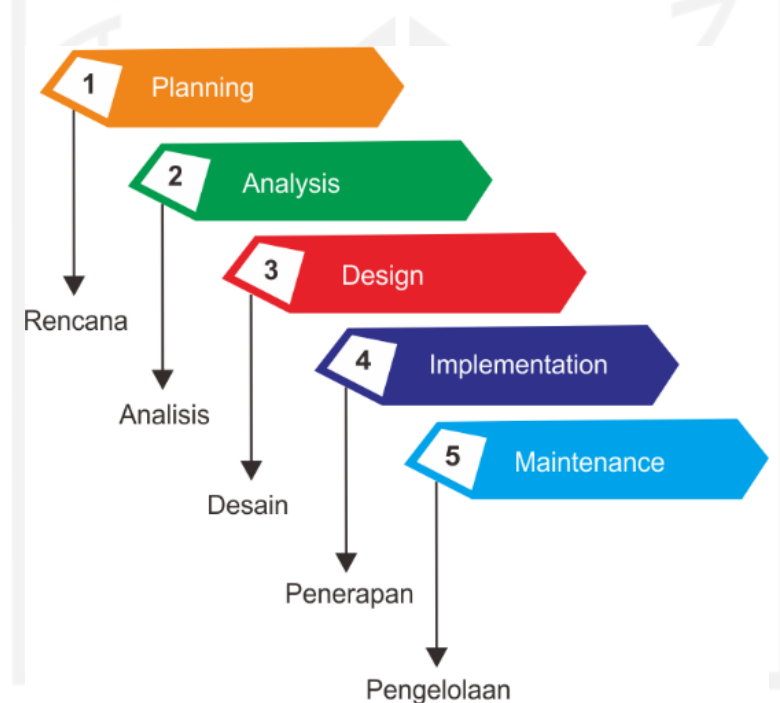


BAB 4

Hasil dan Pembahasan

4.1 SDLC untuk Framework

SDLC (*System Development Life Cycle*) atau Siklus hidup pengembangan 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 4. 1 Proses Penerapan SDLC (*System Development Life Cycle*)

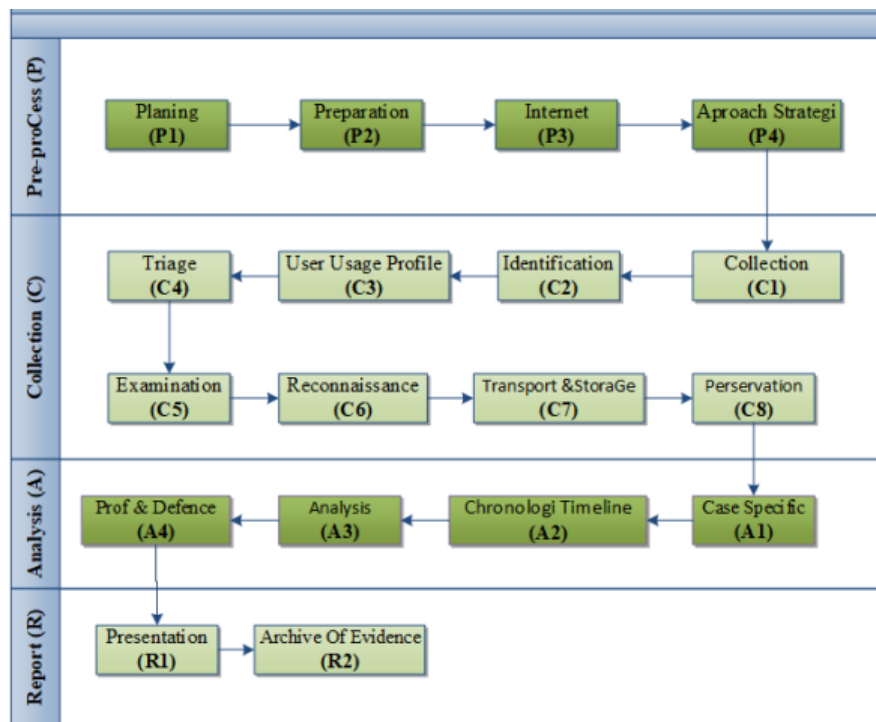
Tabel 4. 1 Proses Pengembangan *framework* pada SDLC

Tahapan Proses	Uraian Penerapan Proses	Keterangan	Output
<i>Planning</i>	Tahapan perencanaan awal yang mana tahapan ini akan melakukan identifikasi terhadap <i>framework</i>	Mengidentifikasi <i>framework</i> terkait forensik sosial media	Tabel identifikasi <i>framework</i>

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

4.1.1 Planning

Pada tahapan awal ini 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 4. 2 Hasil kolaborasi *framework* pengembang sebelumnya

Dari gambar 4.2 menjelaskan rancangan awal pengembang *framework* pengumpulan bukti digital pada sosial media dengan beberapa tahapan-tahapan diantaranya *Pre-Process*, *Collection*, *Analysis*, dan *Report*

1. *Pre-process* (P) tahapan awal dalam pengumpulan barang bukti digital

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

- *Approach Strategy* (P4) tahapan melakukan pendekatan, pengamatan, dan pemanfaatan teknologi secara spesifik sehingga dapat memaksimalkan proses investigasi yang dilakukan.
2. *Collection* (C) merupakan tahapan untuk mengumpulkan bukti-bukti awal dan bukti pendukung.
- *Collection* (C1) tahapan mengumpulkan bukti-bukti yang relevan dengan menggunakan alat maltego dan kunci API sehingga dapat memperoleh informasi yang berasal dari media sosial .
 - *Identification* (C2) tahapan melakukan deteksi dan identifikasi terhadap barang bukti yang di temukan.
 - *User Usage Profile* (C3) Tahapan untuk menemukan hubungan antara bukti digital yang telah dikumpulkan dan di identifikasi dengan pelaku kejahatan.
 - *Triage* (C4) tahapan melakukan identifikasi barang bukti dan prorioritas barang bukti berdasarkan kriteria bukti yang potensial dan relevan.
 - *Examination* (C5) tahapan pelacakan barang bukti secara sistematis serta melakukan validasi terhadap barang bukti yang telah di temukan.
 - *Reconnaissance* (C6) tahapan eksplorasi untuk mendapatkan bukti-bukti yang mendukung.
 - *Transport & Storage* (C7) tahapan menyiapkan semua bukti yang telah dikumpulkan, kemudian ditempatkan ditempat aman sehingga dapat menjaga integritas barang bukti.
 - *Perservation* (C8) tahapan mengamankan barang bukti dari yang tidak berkepentingan.
3. *Analysis* (A) merupakan tahapan untuk melakukan analisa terhadap barang yang telah dikumpulkan
- *Case Specific* (A1) tahapan dimana penyidik dapat menyesuaikan fokus pemeriksaan terhadap bukti yang ditemukan.
 - *Chronology Timeline* (A2) tahapan menjelaskan kronologi kejadian yang telah terjadi.
 - *Analysis* (A3) tahapan melakukan analisa, merekontruksi dan menarik kesimpulan terhadap barang bukti yang telah ditemukan.
 - *Prof & Defence* (A4) tahapan untuk penyidik membuktikan validasi kasus dengan temuan yang ada .

4. *Report (R)* merupakan tahapan akhir untuk perancangan *framework* pengumpulan bukti digital di media sosial.
 - *Presentation (R1)* tahapan meringkas dan memberikan kesimpulan, pelaporan serta melakukan dokumentasi
 - *Archive Of Evidence (R2)* tahapan penyimpanan barang bukti yang telah dilakukan analisa dan telah di proses di pengadilan.

Dari hasil penjelasan *framework* di atas ada beberapa tahapan yang seharusnya masuk pada 1 bagian seperti tahapan *pre-process* di bagian internet bisa masuk di bagian preparation dan pada tahapan *collection* ini tidak sesuai 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 4. 2 Identifikasi *framework*

No	Digital Forensics Investigation Model (DFIM)	Digital Forensics Analysis Team (DFAT)
1	<i>Pre-Process</i>	<i>Pre-Process</i>
2	<i>Collection</i>	<i>Proactive</i>
3	<i>Analysis</i>	<i>Reactive</i>
4	<i>Report</i>	<i>Recoding</i>
5		<i>Analysis</i>
6		<i>Presentation</i>

Ada 2 jenis *framework* ini akan dijadikan bahan perbandingan dari pengembang-pengembang sebelumnya yaitu :

1. *Digital Forensics Investigation Model (DFIM)* dari pengembang (Al Jumah, Sugiantoro, and Prayudi, 2019)
2. *Digital Forensics Analysis Team (DFAT)* dari pengembag (Inggi, Prayudi, and Sugiantoro, 2018)

4.1.2 Analysis

Pada tahap analisis ini akan melakukan analisa barang bukti sehingga dapat menemukan barang bukti pendukung sesuai dengan *framework* yang akan dikembangkan dan mengidentifikasi perbedaan sistem sebelumnya yang sudah dikembangkan.

Tabel 4. 3 Perbandingan pengembang yang sudah ada dan pengembang baru

No	Tahapan <i>framework</i> yang digunakan	Metode	Analysis	Keterangan
1.	<ul style="list-style-type: none"> - <i>Pre-Process</i> - <i>Colection</i> - <i>Analysis</i> - <i>Report</i> 	<i>Composite Logic</i>	<i>Social Media Forensics</i>	Pengembang yang sudah ada
2.	<ul style="list-style-type: none"> - <i>Pre-Process</i> - <i>Proactive</i> - <i>Reactive</i> - <i>Recoding</i> - <i>Analysis</i> - <i>Presentations</i> 	<i>System Development Life Cycle</i>	<i>Audio Forensics</i>	Pengembang yang sudah ada
3	<ul style="list-style-type: none"> - <i>Planning</i> - <i>Analysis</i> - <i>Design</i> - <i>Implementation</i> - <i>Maintenance</i> 	<i>System Development Life Cycle</i>	<i>Social Media Forensics</i>	Pengembang baru

Dari tabel 4.2 menerangkan tentang tahapan *framework* yang sudah dikembangkan sebelumnya mulai dengan *framework* yang akan dikembangkan saat ini dengan perbedaan metode dan sistem analisis yang masing-masing terapkan.

Tabel 4. 4 Identifikasi Tahapan-Tahapan *Framework*

No	Teknik Tahapan Akuisisi	Teknik Investigasi	Forensik Analysis Media Sosial
1	Pengecekan keaslian	Pengumpulan	<i>Preparation</i>
2	Akuisisi	Pengujian	<i>Collection</i>
3	Pengumpulan barang bukti	Analisis	<i>Examination</i>
4	Identifikasi	Laporan	<i>Analysis</i>
5	Hasil/Laporan		<i>Reporting</i>

4.1.3 Design

Proses ini dilakukannya normalisasi terhadap tahapan sebelumnya yang memiliki makna sama setelah itu akan dilakukan transisi sesuai dengan tahapan yang digunakan sekarang dengan alasan tahapan sebelumnya tidak sesuai dengan problem yang digunakan sekarang.

Tabel 4. 5 Normalisasi *Framework* tahap awal

No	Tahapan <i>Framework</i>	ID
	Pre-Process	P
1.	Planning	P1
2.	Preparation	P2

3.	Internet	P3
4.	Approach strategy	P4
Collection		C
5.	Collection	C1
6.	Identification	C2
7.	User usage profil	C3
8.	Triage	C4
9.	Examination	C5
10.	Reconnaissance	C6
11.	Transport & storage	C7
12.	Verservation	C8
Analysis		A
13.	Case Spesifik	A1
14.	Chronology Timeline	A2
15.	Analysis	A3
16.	Prof & Defence	A4
Report		R
17.	Presentation	R1
18.	Archive Of Evidence	R2

Dari tabel 4.5 menerangkan beberapa tahapan yang sudah diterapkan pada peneliti *framework* sebelumnya, maka *framework* yang baru ini peneliti kembangkan menjadi *framework FDFI* dimana FDFI itu adalah nama metode yang digunakan sebagai bentuk perbedaan *framework* yang sudah ada sebelumnya dengan *framework* yang pengembangan sekarang.

Tabel 4. 6 Proses Normalisasi Tahapan

ID	Tahapan dikembangkan	ID	Tahapan sebelumnya	Keterangan
1	Preparation	P	Pre-Process	Pada tahap <i>pre-process</i> di ganti dengan <i>preparation</i> adalah makna arti yang sama yaitu tahap persiapan awal kegiatan investigasi tapi kalimat <i>preparation</i> lebih tepat karena menurut (Saidi 2017) lebih ke awal investigasi secara umum, begitu juga dengan <i>notification</i> dengan <i>planning</i> yaitu mempersiapkan surat perintah dan perijinan tetapi pada sub tahapan <i>internet</i> dan <i>aproach strategy</i> makna yang sama sehingga bisa di satukan menjadi <i>preparation</i> yaitu untuk ketersediaan alat yang digunakan pada investigasi.
1.1	Notification	P1	Planning	
1.2	Authorization	P2	Preparation	
1.3	Preparation	P3	Internet	
		P4	Aproach Strategy	
2	Incident Response	C	Collection	

2.1	Securing Documentation	C1	Collection	Pada tahapan <i>collection</i> pada peneleti sebelumnya yang dimana proses ini alokasikan sebagai pengumpulan barang bukti awal dan pendukung lainnya sehingga ada sun tahap <i>identification, user usage profil, triage, examination, reconnaissance, tranport & storage</i> dan <i>perservation</i> , dimana sub tahapan ini menyesuaikan dengan problem yang di analisa seperti mencari data identitas pelaku dan mencari keterkaitan yang terhubung dengan pelaku, tapi pada pengembang menggunakan tahapan incident response dan sub tahapan ini adalah tahapan <i>securing documentation, event triggering</i> pada tahapan ini proses pengambilan data yang ada pada saat kejadian seperti bukti pengiriman akun, tempat tanggal kejadian dan data entitas akun pelaku.
2.2	Event Triggering	C2	Identification	
		C3	User usage profil	
		C4	Triage	
		C5	Examination	
		C6	Reconnaissance	
		C7	Transport & Storage	
		C8	Perservation	
3	Process Analysis	A	Analysis	Tahapan <i>analysis</i> ini tidak jauh beda dengan pengembang sebelumnya yaitu proses menganalisa problem terjadi seperti pemeriksaan di akun twitter pelaku akan tetapi pada pengembang sebelumnya ada sub tahap <i>chronology timeline</i> yaitu menampilkan kronologi kejadian dan tidak menampilkan hasil dokumetasinya kalau yang di kembangkan sekarang tidak ada sub tahap kronologi karena kronologinya berada pada tahap simulasi <i>framework</i> dan untuk <i>documentation</i> menampilkan hasil screen entity yang didapatkan.
3.1	Preservation	A1	Case Specific	
3.2	Examination	A2	Chronology Timeline	
3.3	Analysis	A3	Analysis	
3.4	Documentation	A4	Prof & Defence	
4	Report	R	Report	Pada tahapan <i>report</i> ini adalah sama-sama menampilkan hasil analisa yang di dapatkan akan tetapi pada pengembangan ini ada sub <i>conclusion</i> dan <i>evaluation</i> untuk mengkosultasikan hasil yang di dapatkan ke pihak hukum dan mengevaluasi hasil data yang ditemukan sebagai bahan pertimbangan dan di simpan dengan aman.
4.1	Conclusion	R1	Presentation	
4.2	Evaluation	R2	Archive Of Evidence	

Tabel 4.6 menjelaskan tentang normalisasi tahapan pengembang sebelumnya dengan tahapan yang dikembangkan sekarang karena perbedaan tahapan sesuai dengan kebutuhan

permasalahan yang akan di analisa. Sesuai tabel 4.6 pada kolom keterangan menerangkan dengan jelas masing-masing sub tahapan yang di normalisasikan.

Tabel 4. 7 Perbedaan *Framework*

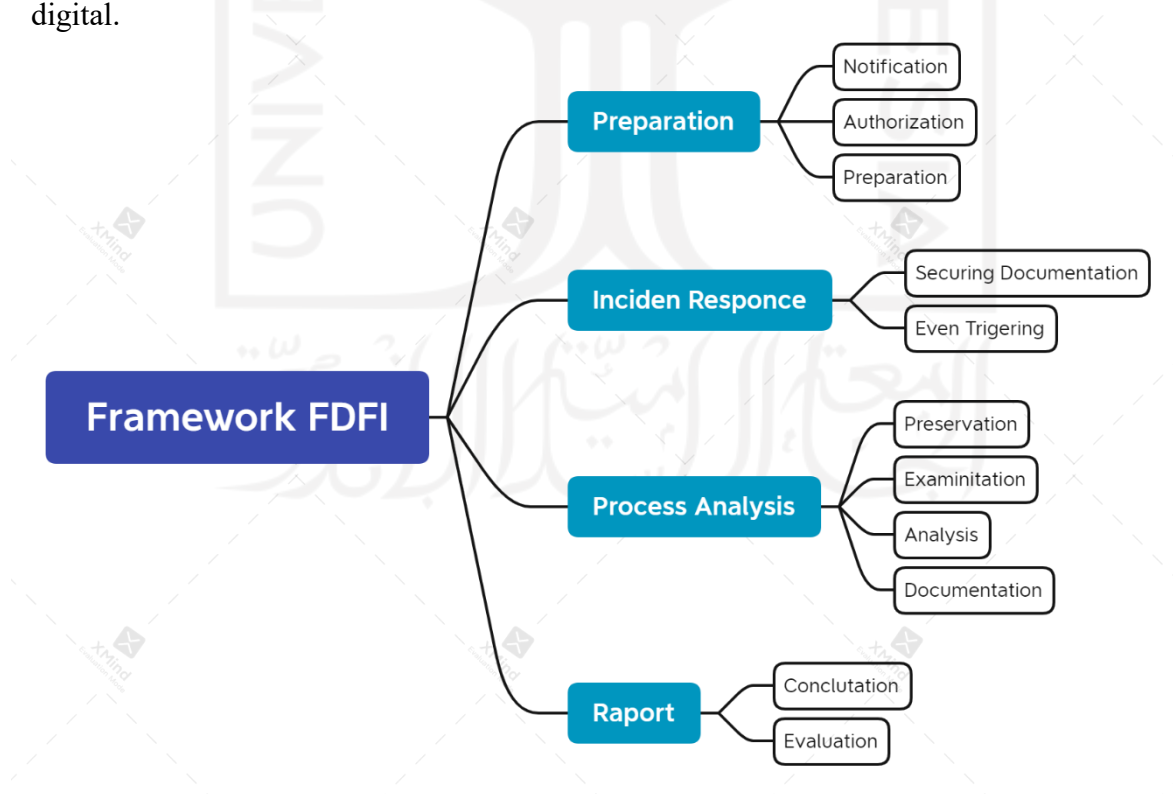
ID	Tahapan	Framework		Keterangan
		Lama	Baru	
P1	Planning	√		
P2	Preparation	√		
P3	Internet	√		
P4	Approach Strategy	√		
	1.1	Notification	√	Sub tahapan awal persiapan proses pengumpulan bukti digital.
	1.2	Authorization	√	
	1.3	Preparation	√	
C1	Collection	√		
C2	Identification	√		
C3	User usage profil	√		
C4	Triage	√		
C5	Examination	√		
C6	Reconnaissance	√		
C7	Transport & Storage	√		
C8	Perservation	√		
	2.1	Securing Documentation	√	Sub tahapan mempersiapkan bukti pendukung
	2.2	Event Triggering	√	
A1	Case Specific	√		
A2	Chronology Timeline	√		
A3	Analysis	√		
A4	Prof & Defence	√		
	3.1	Preservation	√	Sub tahapan melakukan analisa terhadap barang bukti yang ditemukan
	3.2	Examination	√	
	3.3	Analysis	√	
	3.4	Documentation	√	
R1	Presentation	√		
R2	Archive Of Evidence	√		
	4.1	Conclusion	√	Sub tahap akhir proses pelaporan hasil investigasi barang bukti
	4.2	Evaluation	√	

Pada tabel 4.7 menerangkan tentang perbedaan sub tahapan *framework* yang sudah dikembangkan sebelumnya dengan sub tahapan yang akan dikembangkan sekarang. Dari hasil ceklis (√) menandakan perbedaan *framework* lama dan *framework* yang baru, pada kolom keterangan menjelaskan masing-masing fungsi sub tahapan tersebut.

Tabel 4. 8 Normalisasi *Framework FDFI*

No	Tahap Normalisasi <i>Framework FDFI</i>	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 4. 3 *Framework FDFI Investigation Digital*

4.1.3.1. *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*: Tahapan 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*

Tahapan 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 penelitian 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

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

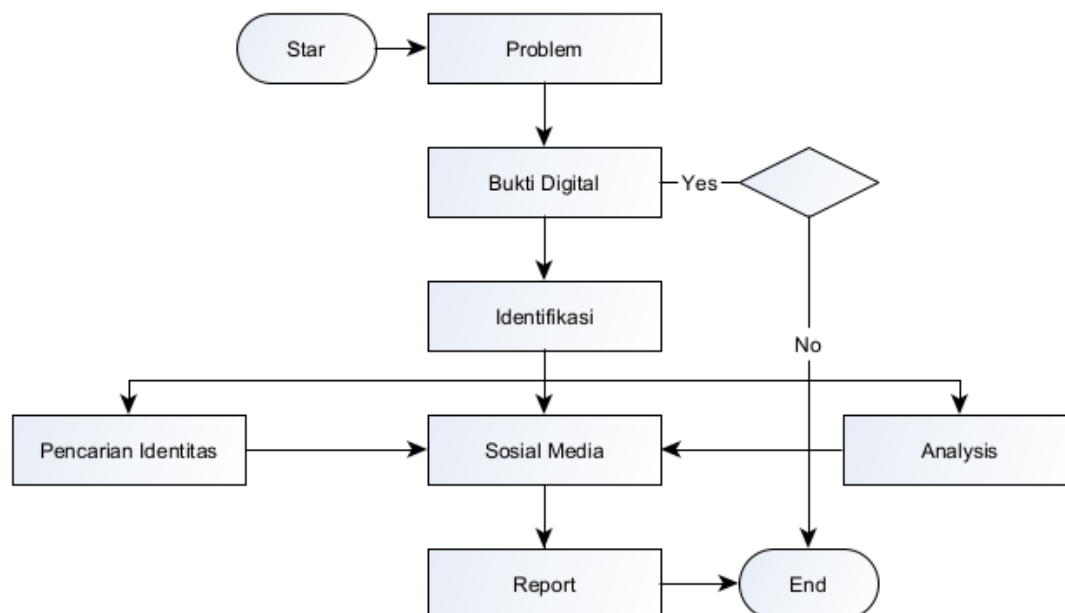
- a. *Conclusion*: Menyimpulkan hasil dari investigasi yang dilakukan
- b. *Evaluation*: proses analisa dan evaluasi keseluruhan terhadap hasil investigasi dan mencatat proses penyelidikan yang sudah dilakukan.

4.1.3.2. Metode Framework FDFI

Metode yang digunakan pada *framework FDFI* ini menggunakan *System Development Life Cycle (SDLC)* untuk mengolah data perangkat lunak yang akan di investigasi di media social.

4.1.4 Implementation

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

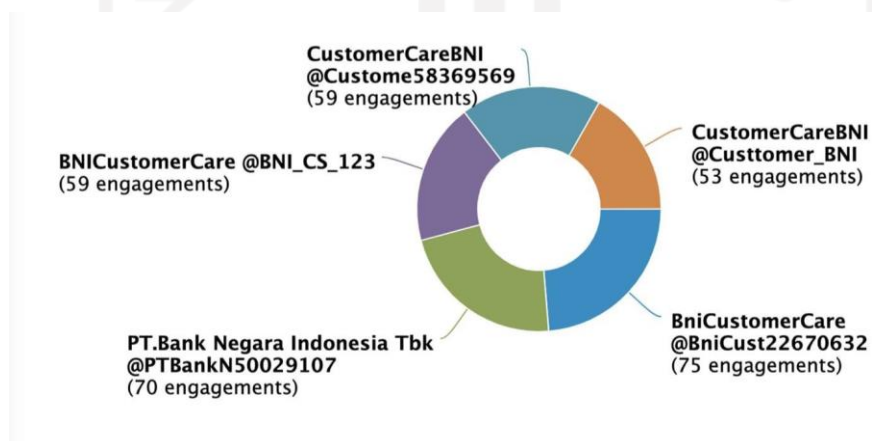


Gambar 4. 4 *Flowchart* alur kerja investigasi

Dari gambar 4.3 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”.

4.1.4.1 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. 5 Akun-akun Palsu *CustomerCare* BNI di *twitter*

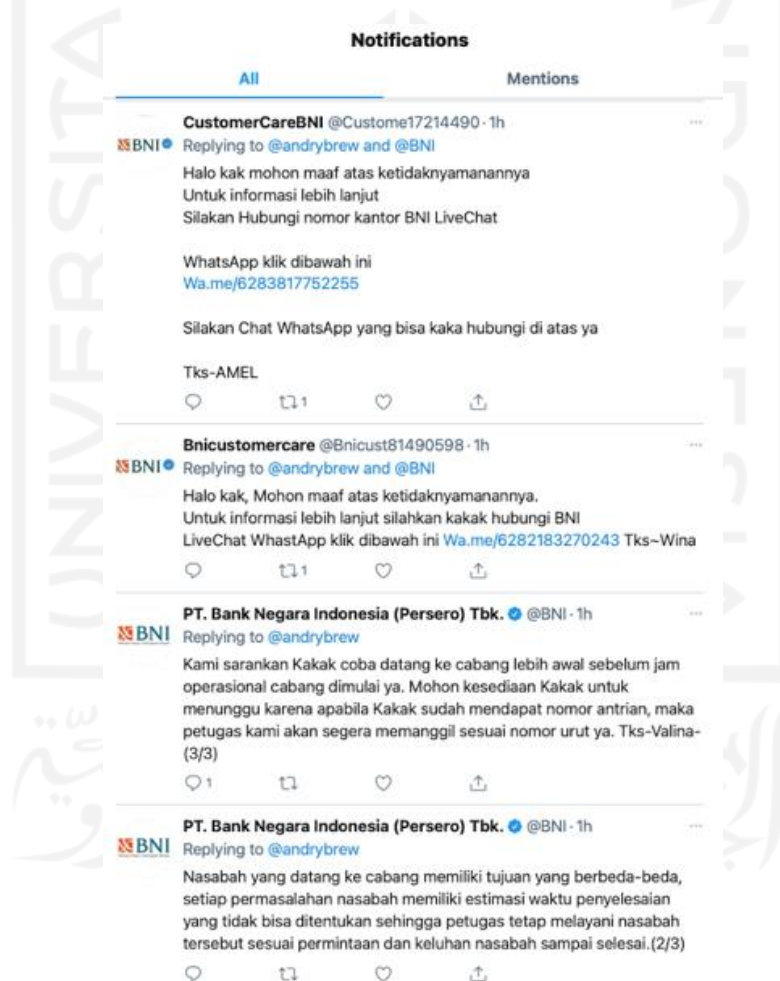
Pada gambar diatas yang dikutip dari penelitian (DronEmperit) banyaknya akun-akun palsu yang mengaku *CostumerCare* BNI untuk menipu nasabah tiada lain adalah untuk

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.

4.1.4.2 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. 6 Barang Bukti Digital postingan Akun Palsu *Custumercare* BNI

Dari gambar 4.5. 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.

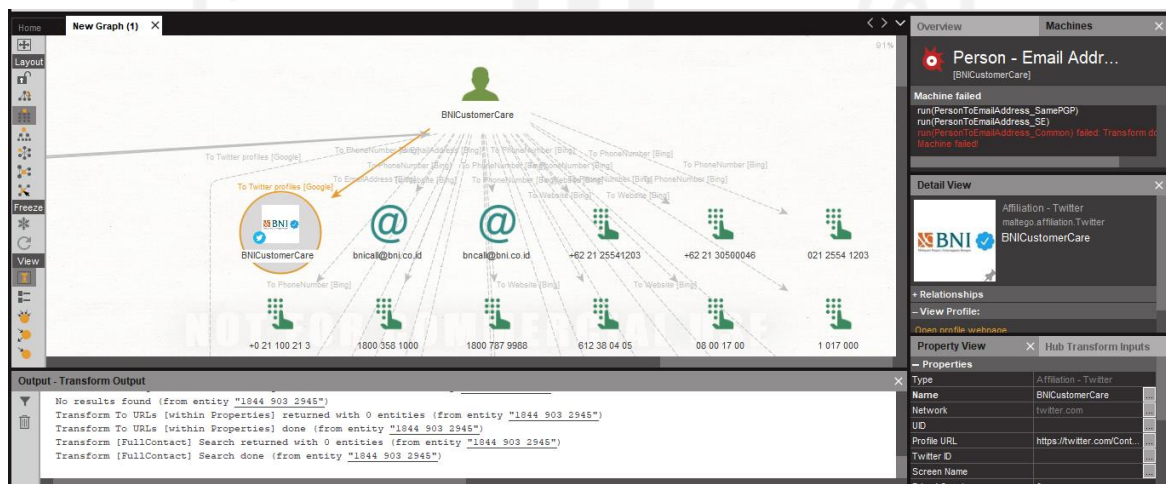
Adapun barang bukti digital yang didapatkan dari postingan tersebut adalah sebuah akun palsu atas nama *CostumerCareBNI* (@Costumer17214490) dan *Bnicotumercare* (@Bnicust81490598) dan tanggal pengirimannya.

4.1.4.3 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.

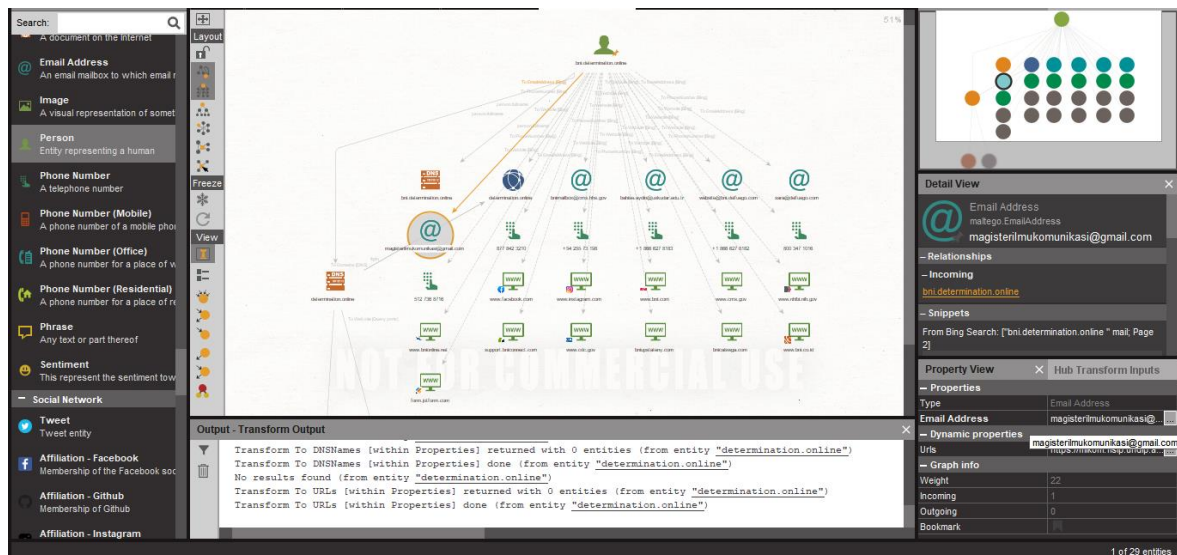
4.1.4.3.1 Pencarian Identitas

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. 7 Hasil Pencarian Data 1

pada gambar 4.6. 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. 8 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 address* dan *websitenya* menggunakan tidak resmi.

4.1.4.3.2 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.

4.1.4.3.3 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.

4.1.4.4 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.

4.1.4.5 Hasil Analisa *Framework*

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

Tabel 4. 9 Analisa *Framework*

No	Tahapan <i>Framework</i>	<i>Framework Digital Forensic Investigation (FDFI)</i>	<i>Digital Forensics Investigation Model (DFIM)</i>	<i>Digital Forensics Analysis Team (DFAT)</i>
1	<i>Notification</i>	√	x	√
2	<i>Authorization</i>	√	x	√
3	<i>Preparation</i>	√	x	√
4	<i>Securing Documentation</i>	√	x	x
5	<i>Event Triggering</i>	√	x	x
6	<i>Preservation</i>	√	√	√
7	<i>Examination</i>	√	√	√
8	<i>Analysis</i>	√	√	√
9	<i>Documentation</i>	√	x	√
10	<i>Conclusion</i>	√	x	√
11	<i>Evaluation</i>	√	x	x

Tabel 4.9 menerangkan bahwa tahapan-tahapan yang digunakan pada pengambilan bukti digital berdasarkan hasil eliminasi *framework* sebelumnya. Tahapan FDFI tersebut tahapan yang akan di kembangkan pada penelitian ini dan tahapan DFIM, DFAT adalah tahapan *framework* yang sudah dikembangkan sebelumnya, maka kesimpulannya adalah tahapan

yang mempunyai hasil ceklis (√) tahapan yang bisa digunakan yang yang bertanda silang (x) tahapan yang tidak bisa digunakan atau tidak sesuai dengan problem peneliti kembangkan.

4.1.5 Maintenance

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

Tabel 4. 10 Input, Proses dan Output Pemeliharaan

Input	Proses	Output
<i>Framework FDFI</i>	SDLC	Pemeliharaan dan pengecekan kembali <i>framework</i> yang sudah jadi.

4.2 SDLC (System Development Life Cycle)

Siklus yang digunakan dalam pembuatan atau pengembangan sistem informasi yang bertujuan untuk menyelesaikan masalah investigasi secara efektif. Konsep ini umumnya ditujukan pada sistem komputer atau informasi yang diambil untuk mengembangkan perangkat lunak yang terdiri dari tahapan *planning, analysis, design, implementation, and maintenance*.

4.3 Testing Framework

Testing *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 :

4.3.1 Simulasi *framework*

Pada tahapan 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 4. 9 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 4. 10 Bukti screen balasan pesan *BNIcustomercare*

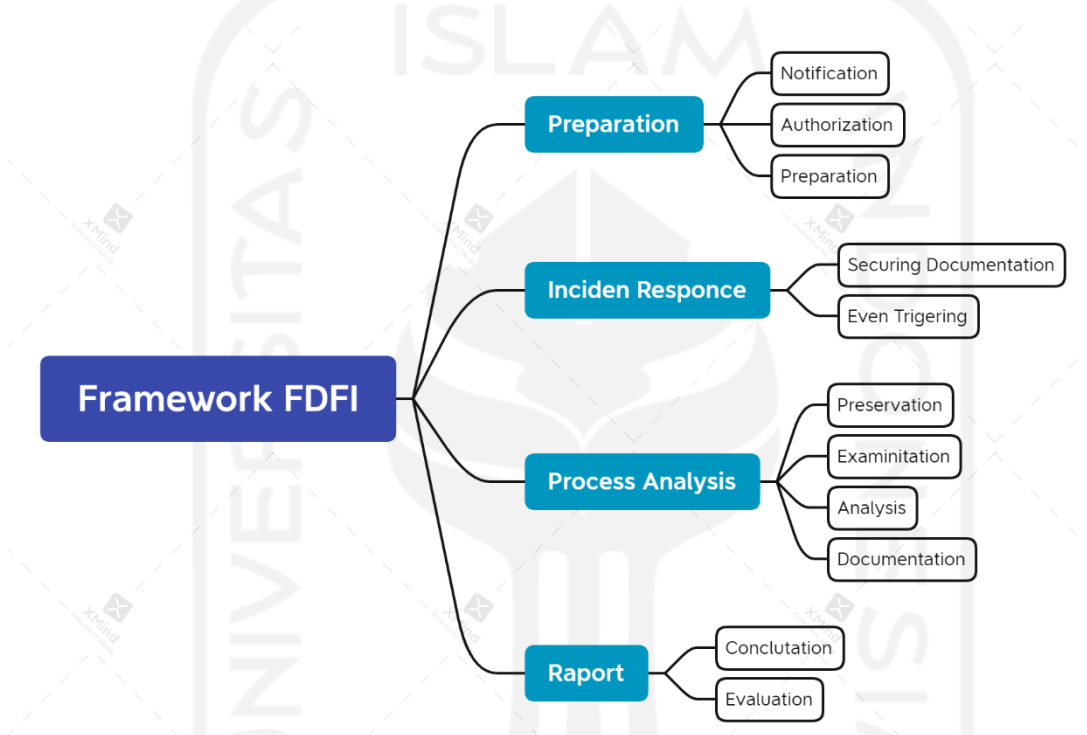
➤ Bukti digital yang didapatkan

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

4.3.2 Analysis framework

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



Gambar 4. 11 *Framework* yang dikembangkan

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

1. *Preparation*

Tahapan pertama yang dilakukan dalam investigasi ini adalah menyiapkan segala sesuatu kebutuhan dalam penyidikan social media, adapun beberapa tahapan yang siapakan adalah :

- 1.1. *Notification*, tahap ini tahapan 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 4. 11 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 <i>free</i> Twitter

2. Incident Response

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

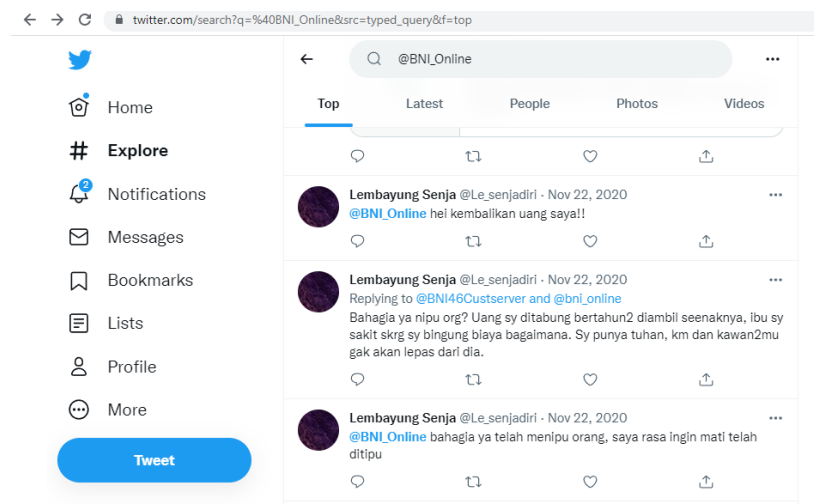
2.1. *Securing Documentation*, sebuah proses investigasi melakukan pengamanan barang bukti digital seperti akun media sosial twitter, screen kasus kejadian dan lain-lain yang bersangkutan dengan lokasi kejadian.



Gambar 4. 12 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* .

2.2.*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.



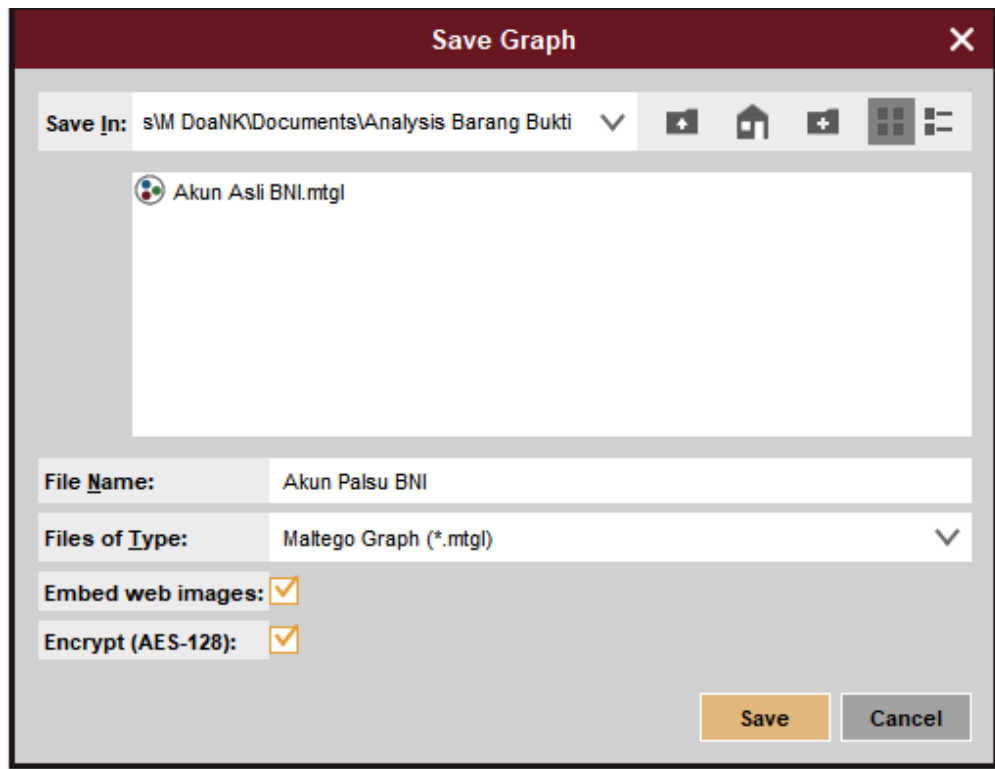
Gambar 4. 13 Ikatan kejahatan dengan orang lain

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

3. *Process Analysis*

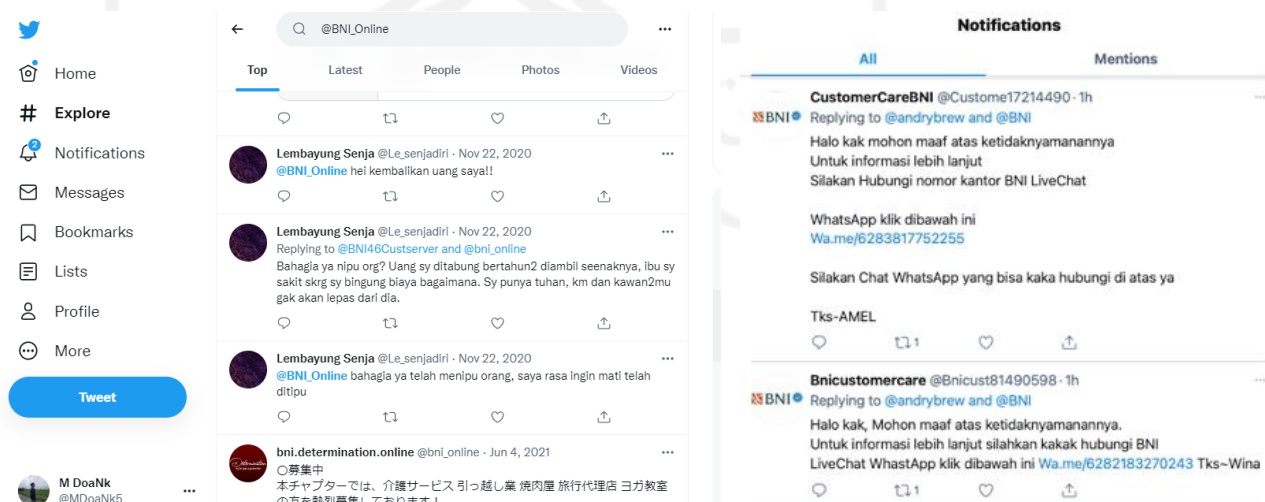
Tahapan ini akan menganalisis dari barang bukti yang sudah didapatkan pada tahapan sebelumnya sesuai dengan permasalahan yang ada menggunakan tools maltego.

3.1.*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.

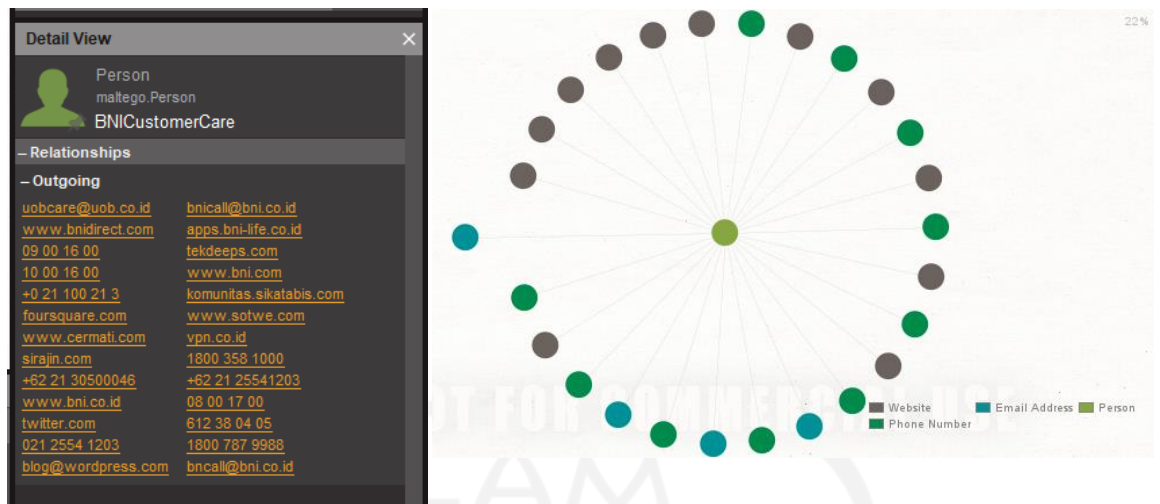


Gambar 4. 14 Penyimpanan Barang Bukti Digital

3.2. *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 4. 15 Keterkaitan akun *twitter*



Gambar 4. 19 *Detail view dan Layout entity BNICustomerCare*

3.4. *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.

Type	Entity	View	Details	Links	Score
maltego.EmailAdd	bnicall@bni.co.id	View	Details	Links	130
maltego.PhoneNu	+62 21 25541203	View	Details	Links	104
maltego.Website	twitter.com	View	Details	Links	104
maltego.PhoneNu	+62 21 30500046	View	Details	Links	101
maltego.Website	www.bni.co.id	View	Details	Links	96
maltego.Website	www.bni.com	View	Details	Links	84
maltego.PhoneNu	1800 358 1000	View	Details	Links	81
maltego.EmailAdd	bnicall@bni.co.id	View	Details	Links	76
maltego.Website	tekdeeps.com	View	Details	Links	76
maltego.PhoneNu	1800 787 9988	View	Details	Links	71
maltego.Website	apps.bni-life.co.id	View	Details	Links	68
maltego.PhoneNu	021 2554 1203	View	Details	Links	64
maltego.Website	www.bnidirect.com	View	Details	Links	59
maltego.PhoneNu	612 38 04 05	View	Details	Links	52
maltego.EmailAdd	blog@wordpress.com	View	Details	Links	51
maltego.Website	www.cermati.com	View	Details	Links	51
maltego.Website	www.sotwe.com	View	Details	Links	43
maltego.PhoneNu	09 00 17 00	View	Details	Links	42
maltego.EmailAdd	uobcare@uob.co.id	View	Details	Links	39
maltego.Website	foursquare.com	View	Details	Links	34
maltego.PhoneNu	+0 21 100 21 3	View	Details	Links	32
maltego.Website	komunitas.sikatabis.com	View	Details	Links	26
maltego.PhoneNu	10 00 16 00	View	Details	Links	22
maltego.Website	sirajin.com	View	Details	Links	18
maltego.PhoneNu	09 00 16 00	View	Details	Links	12
maltego.Website	vpn.co.id	View	Details	Links	9
maltego.Person	BNICustomerCare	View	Details	Links	6

Gambar 4. 20 *Screen Dokumentasi barang bukti digital 1*

Gambar 4. 21 *Screen* Dokumentasi barang bukti digital 2

4. Report

Tahapan ini adalah tahapan 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 4. 12 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/BN I-Determination- 104429321223541/	BNI

Penjelasan pada tabel 4.12 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*, tahapan 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 5

Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan, maka peneliti mendapat kesimpulan bahwa *System Development Life Cycle* (SDLC) dapat diterapkan dalam membangun sebuah *framework* social media dengan cara mengidentifikasi *framework* sebelumnya dan melakukan eliminasi tahapan-tahapan yang memiliki makna yang sama dan melakukan penambahan tahapan sesuai dengan keperluan investigasi. Didalam *framework* yang dikembangkan ini terdapat 4 tahapan dalam penanganan investigasi digital yaitu *preparation, incident response, process analysis, dan report* sehingga dapat menghasilkan barang bukti yang cukup seperti email address, phone number, website, dan DNS pelaku.

Adapun kelebihan *framework FDFI* ini adalah dapat digunakan sebagai pengumpulan barang bukti digital dan *framework* ini juga cukup spesifik dan cepat dalam penanganan investigasi sosial media khususnya ke twitter dan *open source*. Dari hasil yang didapatkan dalam pencarian data untuk membuktikan akun twitter BNICustomerCare (*BNICustomerCare*) dengan akun twitter bukan dari instansi BNI dengan nama *bni.determination.online (@BNI_Online)* email address, website, phone Number, dan DNS, dari perbandingan entity yang didapatkan tidak sesuai dengan data yang aslinya.

Pengembangan *framework* menggunakan metode *System Development Life Cycle* (SDLC) dapat diterapkan pada investigasi media sosial twitter dengan menganalisa sebuah akun mengatasnamakan instansi pihak BNI sehingga dalam proses investigasi tersebut mendapatkan barang bukti akun palsu.

5.2 Saran

Bagi pengguna *framework* ini supaya kedepannya bisa lebih disempurnakan karena *framework* ini hanya dapat digunakan pada social media twitter. Maka kedepannya bisa dikembangkan lagi ke banyak social media lainnya, dan tools yang digunakan dalam investigasi pengumpulan barang bukti juga masih *free* jadi barang bukti yang didapatkan juga tidak banyak. Bagi pengembang selanjutnya supaya bisa menggunakan tools yang *pro* supaya barang bukti yang didapatkan lebih banyak.

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 Messenger 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, CIGED*, 2002:2525–30. <https://doi.org/10.1109/CIGED.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 Umami Masrurroh, 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 Sositelknologi* 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.

