ANALISIS DIGITAL FORENSIK PADA DIGITAL FOOTPRINT UNTUK IDENTIFIKASI PELAKU CYBERCRIME DENGAN FRAMEWORK FDFI

Bunga Islamiya Putri[1], Deni Suprihadi[2]

bungaislamiyah02@gmail.com[1], deni.suprihadi99@gmail.com[2]

Program Studi Teknik Informatika, Universitas Kebangsaan Republik Indonesia, Bandung

ABSTRAK

Banyaknya pengguna media sosial pada saat sekarang ini, mengakibatkan banyaknya tindakan kejahatan (cybercrime), dan sulitnya mengidentifikasi pelaku cybercrime di media sosial karena kebanyakan dilakukan dengan cara anonym (menggunakan akun palsu). Namun dengan adanya digital footprint (jejak digital) yang ditinggalkan oleh pengguna dapat mempermudah proses identifikasi pelaku. Penelitian ini menggunakan Metode Social Network Analysis (SNA) untuk mengumpulkan data dan melakukan pendekatan terhadap media sosial kemudian menggunakan Framework Digital Forensik Investigation (FDFI) dalam melakukan analisis investigasi. Penelitian ini akan menganalisis pencarian bukti digital pada aplikasi Twitter. Temuan utama penelitian ini adalah bahwa pendekatan ini mampu mengidentifikasi jejak digital dengan akurasi tinggi dan mengaitkannya dengan identitas pelaku. Hasil penelitian ini memeiliki dampak penting dalam penegakan hukum dan pencegahan kejahatan dunia maya. Identifikasi pelaku yang efektif melalui analisis jejak digital dapat membantu lembaga penegak hukum dalam mengambil tindakan yang cepat dan akurat. Selain itu, penelitian ini juga dapat menjadi dasar bagi perkembangan metode analisis digital forensik yang lebih canggih dan adaptif dalam menghadapi perkembangan teknologi dan metode kejahatan baru di dunia maya.

Kata Kunci : Analisis Digital Forensik, Digital Footprint, Framework FDFI, Media Sosial, Social Network Analysis

ABSTRACT

The large number of social media users at this time, resulting in many crimes (cybercrime), and the difficulty of identifying cybercrime perpetrators on social media because most of them are done anonymously (using fake accounts). However, the digital footprint left by users can facilitate the process of identifying perpetrators. This study uses the Social Network Analysis (SNA) Method to collect data and approach social media then uses the Digital Forensics Investigation Framework (FDFI) in conducting investigative analysis. The study will analyze digital evidence searches on the Twitter app. The main finding of the study is that this approach is able to identify digital traces with high accuracy and associate them with the identity of the perpetrator. The results of this study have an important impact on law enforcement and cyber crime prevention. Effective perpetrator identification through digital footprint

analysis can assist law enforcement agencies in taking swift and accurate action. In addition, this research can also be the basis for the development of more sophisticated and adaptive forensic digital analysis methods in the face of technological developments and new crime methods in cyberspace.
Keywords : *Digital Forensics Analysis, Digital Footprint, FDFI Framework, Social Media, Social Network Analysis*

1. PENDAHULUAN

Prakarsa media sosial dengan semua keunggulannya telah menjadi aspek integral kehidupan manusia. Perkembangan zaman menghasilkan berbagai jenis media, termasuk media sosial. Media sosial merupakan platform komunikasi yang menitikberatkan pada kehadiran pengguna, memungkinkan mereka untuk berinteraksi dan berkolaborasi dalam berbagai aktivitas (Van Dijk, 2016).

Menurut laporan data yang diterbitkan oleh *We Are Social*, pada bulan Januari 2022, tercatat sekitar 191 juta orang di Indonesia yang aktif menggunakan media sosial, mengalami peningkatan sebesar 12,35% dibandingkan tahun sebelumnya yang mencapai 170 juta orang. Sementara itu, jumlah pengguna Twitter di Indonesia pada tahun 2022 mencapai 18,45 juta pengguna. Pemanfaatan media sosial yang tidak benar pada saat ini mengakibatkan banyak tindakan kriminal (cybercrime), termasuk perdagangan manusia, intimidasi siber, praktik penipuan, pemerasan, penyebaran informasi palsu, dan variasi lainnya. Saat ini, terjadi peningkatan kasus penipuan yang menggunakan akun-akun palsu berkedok bank terkenal di platform media sosial Twitter. Kelompok penipu ini menggunakan nama-nama bank ternama di Indonesia dan menargetkan nasabah-nasabah dari bank tersebut. Akun penipu ini memiliki *bot* atau semacam program otomatis yang memonitor semua percakapan di twitter.

Tindakan *cybercrime* ini sering kali sulit untuk diidentifikasi pelakunya, karena kebanyak *cybercrime* dilakukan dengan cara *anonym* atau menggunakan akun palsu. Namun dengan adanya *digital footprint,* yaitu jejak digital yang ditinggalkan dapat mempermudah proses identifikasi pelaku. Jejak digital atau *digital footprint* merujuk pada rangkaian aktivitas, tindakan, partisipasi, dan interaksi digital yang tercatat dan terekspos di internet atau dalam perangkat digital (Niken Bestari, 2022).

Dalam forensik digital, bukti yang diperoleh dari media sosial sangat bermanfaat. Banyaknya informasi yang berupa data-data pribadi yang dipublikasikan di media sosial dapat digunakan penyidik sebagai barang bukti yang kuat untuk melacak pelaku dari kejahatan. Selain itu, data-data yang berada dalam ruang lingkup media sosial menawarkan informasi yang cukup banyak untuk mengetahui tentang motif dari setiap tindakan kejahatan yang dilakukan(Arshad et al., 2019).

Forensik sangat diperlukan dalam menginvestigasi kejahatan pada sosial media disebabkan pelaku kejahatan sering melakukan duplikasi terhadap identitas seseorang (Kurniawan & Prayudi, 2014). Forensik adalah upaya dalam menginvestigasi serta memastikan kenyataan terkait insiden kriminal dan isu hukum lainnya. Digital forensik merujuk pada cabang ilmu forensik yang bertujuan memperoleh dan menyelidiki

informasi dan data yang ada dalam perangkat digital seperti komputer, ponsel, tablet, PDA, perangkat jaringan, penyimpanan data, dan lain sebagainya (Raharjo, 2013).

Pada tahun 2019, sebuah penelitian dilakukan mengenai pengembangan kerangka kerja untuk mengumpulkan bukti digital dari platform media sosial dengan menerapkan metode *composite logic*. Dari hasil penelitian ini, berhasil mengumpulkan data mengenai identitas individu yang terlibat dalam tindakan pencemaran nama baik di platform media sosial Twitter. Pendekatan *composite logic* ini digunakan sebagai metode untuk mengumpulkan data dan mengidentifikasi rentang waktu yang relevan. Model yang diterapkan dalam penelitian ini membantu dalam menjelajahi hubungan antara berbagai aktivitas yang memiliki tujuan serupa.(Al Jumah et al., 2019).

Penelitian ini menggunakan metode *social network analysis (SNA)* dalam pendekatan pada media sosial, dan framwork FDFI untuk investigasi akun. Framework FDFI merupakan hasil sinergi berbagai kerangka kerja sebelumnya, dan nilai unggul dari framework ini adalah kesederhanaannya yang sangat cocok untuk memenuhi kebutuhan analisis investigatif di platform media sosial (Nukman, 2022).

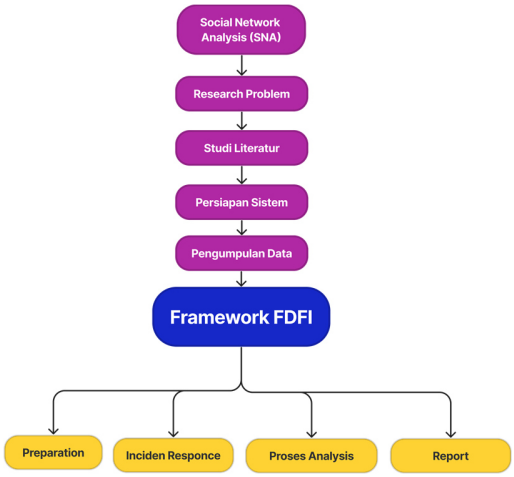
Penggunaan framework dalam studi ini digunakan sebagai struktur untuk menghimpun informasi di media dan juga dalam konteks manajemen, dengan tujuan mengilustrasikan suatu konsep yang memfasilitasi penanganan beragam aspek identitas individu (Ibrahim et al., 2018) .

2. METODE PENELITIAN

Penelitian ini menggunakan metode pendekatan *Social Network Analysis pada Framework Digital Forensik Investigation.* Untuk mengumpulkan data dari media sosial, digunakan aplikasi Maltego, kemudia untuk melacak domain menggunakan WHOIS Domain, dan untuk menjaga intergrity bukti digunakan SHA-256. Data dan informasi yang diambil dalam penelitian ini adalah data pada digital footprint yang meliputi data email, alias akun media sosial, dan aktivitas pada media sosial.

Data yang dipakai dalam penelitian ini diambil dari media sosial twitter. Pengambilan data dilakukan melalui aplikasi maltego dengan pendekatan pada media sosial menggunakan metode *Social Network Analysis.*

Berikut tahapan yang akan dilakukan pada penelitian ini.

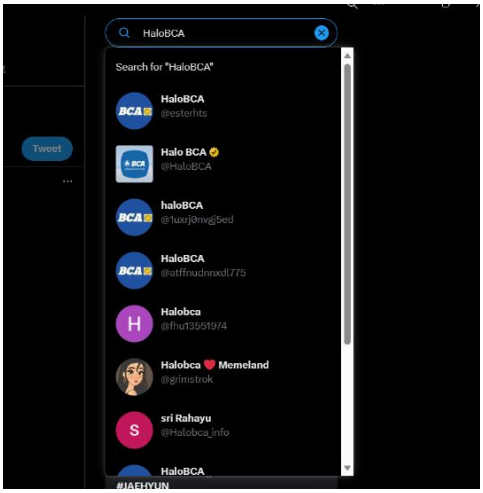


Gambar 1. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

3.1. *Social Network Analyis*

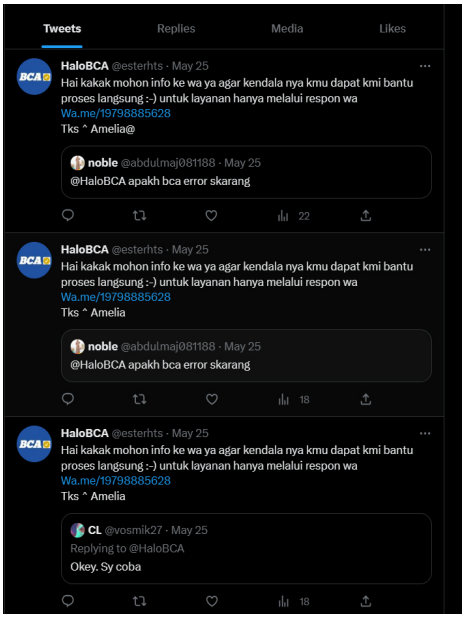
Social Network Analysis (SNA) dalam investigasi forensik digital dapat membantu dalam memahami hubungan sosial dan jaringan komunikasi antara entitas yang terlibat dalam kasus tersebut. Penggunaan metode SNA ini adalah untuk langkah awal sebagai pendekatan pada media sosial untuk mendapatkan bukti awal dari kejahatan. Berikut adalah akun-akun palsu dari BCA yang ditemukan pada aplikasi twitter.



Gambar 2. Akun-akun Palsu BCA

Untuk bukti awal, berikut adalah bukti komentar dari akun palsu pada nasabah yang mengalami permasalahan dan menyampaikan keluhannya melalui twitter, kemudian

akun palu HaloBCA merespon keluhan dari nasabah tersebut agar menghubungi No. WhatsApp dari pelaku.



Gambar 3. Komentar Akun Palsu HaloBCA

3.2. Analysis Framework

1. *Preparation*

a. Notification, Tahap ini merupkana langkah awal yang melibatkan persiapan berkas laporan mengenai kasus kejahatan di platform media sosial, contohnya adalah menyiapkan laporan pengaduan yang akan disampaikan kepada pihak jaksa hukum.

b. *Authorization,* Tahapa ini mengharuskan adanya keabsahan dalam melaksanakan proses investigasi sesuai dengan hukum yang berlaku.

c. *Preparation,* Tahap ini menyediakan semua kebutuhan yang diperlukan dalam proses investigas, seperti mempersiapkan perangkat keras, perangkat lunak/alat, dan koneksi internet.

Tabel 1. Detail 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 CE	 Windows 10 V 4.4.2

	c. SHA-256 d. Who is Domain c. Sosial Media	 Twitter

2. *Incident Response*

a. Sucuring Documentation, Sebuah penyelidikan dilakukan dengan tujuan mengumpulkan Bukti digital, contohnya akun media sosial Twitter, tangkapan layar insiden kasus, serta unsur-unsur terkait lainnya. Dapat dilihat pada gambar 4. dan gambar 5. berikut.

Gambar 4. barang Bukti Akun Palsu HaloBCA

b. *Event Triggering,* Penelusuran terhadap bukti digital lainnya untuk mengidentifikasi keterkaitannya dengan pelaku kejahatan, dapat dilihat pada gambar 6. Berikut.

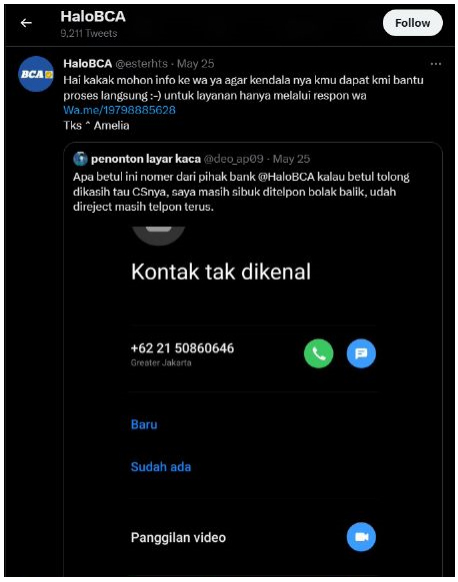
Gambar 5. Ikatan Kejahatan dengan Orang Lain

3. *Proses Analysis*

a. Preservation, Bukti-bukti digital yang berhasil ditemukan akan dijaga dengan baik agar terhindar dari kontaminasi atau perubahan yang dapat mempengaruhi barang bukti lainnya. Untuk menyimpan barang bukti digital yang telah diproses melalui analisis Maltego, akan diterapkan format penyimpanan khusus yang dikenal sebagai (*mtgl), dan ini akan dijelaskan menggunakan metode enkripsi AES-128.

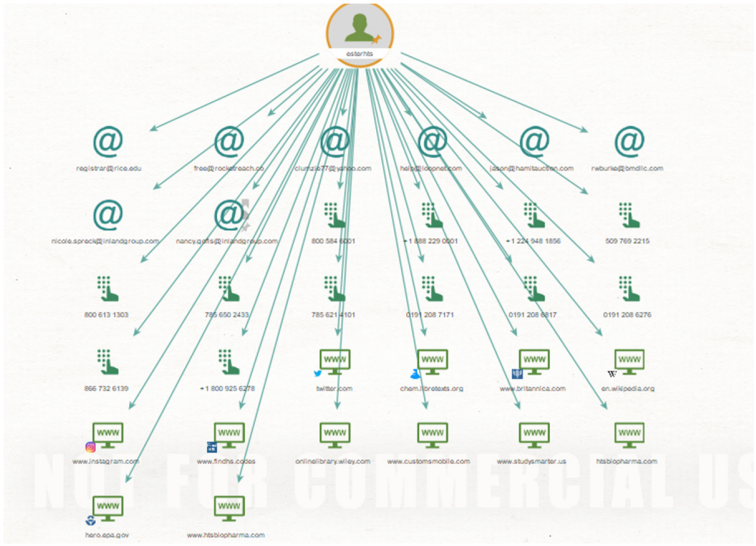
b. *Examination,* Dalam usaha melacak bukti dengan pendekatan yang terstruktur, validasi juga diterapkan pada bukti yang telah ditemukan untuk mengidentifikasi sejauh mana hubungannya dengan akun pelaku..

Gambar 6. Keterkaitan Akun Twitter

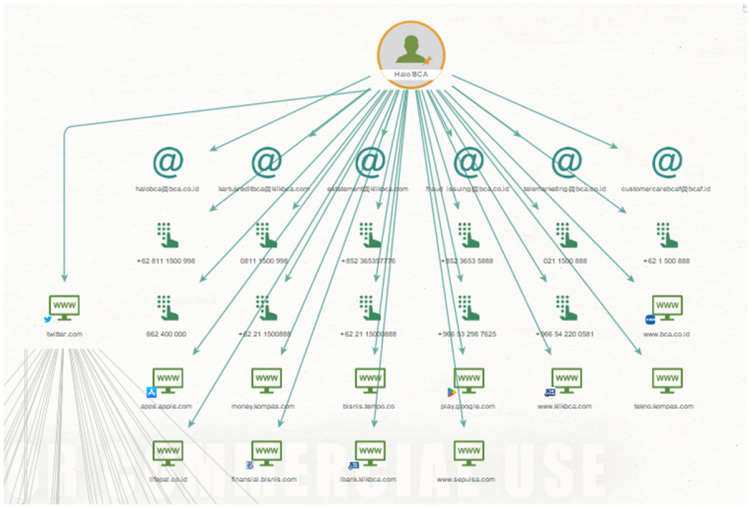


Gambar 7. Hasil Validasi keterkaitan Akun Twitter

c. *Analysis,* Tindakan selanjutnya adalah melakukan analisis danmenarik kesimpulan berdasarkan barang bukti yang telah ditemukan.

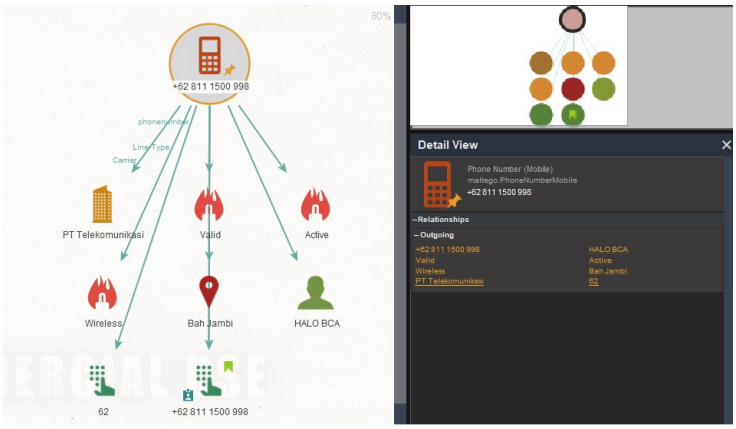


Gambar 8. Hasil temuan Investigasi Akun Palsu HaloBCA

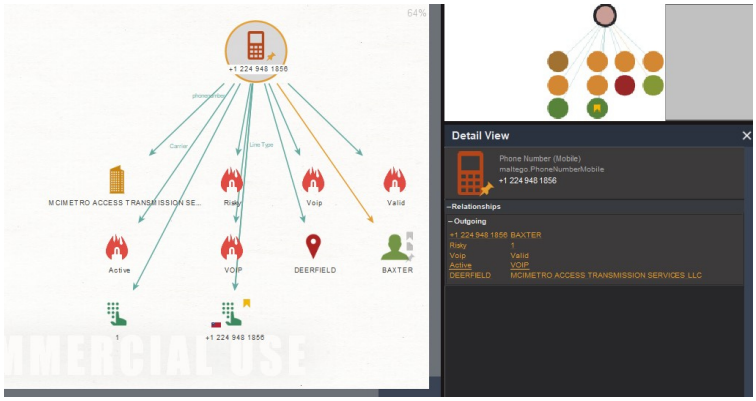


Gambar 9. Hasil Temuan Investigasi Akun Asli HaloBCA

Berdasarkan analisis pada gambar 9. dan gambar 10. Beberapa entity yang ditemukan seperti lamat email, domain, no. Telephone, dan lainnya terdapat perbedaan yang sangat siginifikan. Kemudian selanjutnya untuk memastikannya, maka dilakukan juga analisis terhadap no. Telephone yang ditemukan.



Gambar 10. Pengecekan Pada No. Telephone Akun Asli BCA



Gambar 11. Pengecekan Pada No. Telephone Akun Palsu BCA

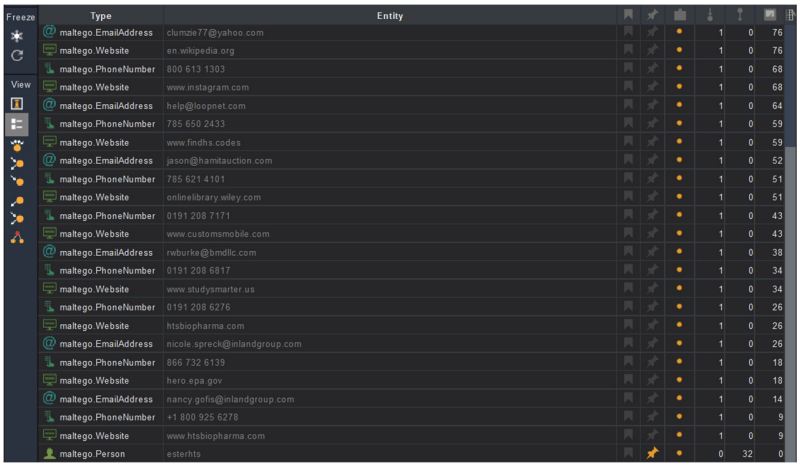
Dari hasil dan data yang ditampilkan pada gambar 11. Dan gambar 12. Dapat diambil kesimpulan bahwa No. Telephone dari akun HaloBCA (@esterhts) adalah bukan dari No. Telephone Bank BCA.

Kemudian selanjutnya dilakukan juga pengecekan pada domain antara akun HaloBCA (@esterhts) dan akun HaloBCA (@halobca).


```
sferProhibited https://icann.org/epp#clientTransferProhibited', 'clientUpdatePro
hibited https://icann.org/epp#clientUpdateProhibited']
Name Servers: ['mnet.mevzuat.net', 'infosql2013.infosoft.com.tr']
Creation Date: 2015-09-17 16:53:06
Expiry Date: 2023-09-17 16:53:06
Updated Date: 2023-06-24 06:12:18
Registrant: None
Organization: Domains By Proxy, LLC
Country: US
State: Arizona
City: REDACTED FOR PRIVACY
Emails: abuse@godaddy.com
Name Server IPs: None
Name Server IPs: {
  "domain_name": "findhs.codes",
  "registrar": "GoDaddy.com, LLC",
  "whois_server": "whois.godaddy.com/",
  "referral_url": null,
  "updated_date": "2023-06-24 06:12:18",
  "creation_date": "2015-09-17 16:53:06",
  "expiration_date": "2023-09-17 16:53:06",
  "name_servers": [
    "mnet.mevzuat.net",
    "infosql2013.infosoft.com.tr"
```


Gambar 12. Informasi Domain Akun Palsu BCA

d. *Documentation,* Setelah menganalisis bukti yang telah diidentifikasi, langkah selanjutnya adalah menjaga keamanan bukti tersebut sebagai dokumen yang akan disertakan dalam laporan yang akan diserahkan kepada otoritas yang berwenang..



Gambar 13. Dokumentasi Barang Bukti Akun Palsu HaloBCA

e. *Report,* Tahapan proses penyusunan laporan akhir berdasarkan temuan yang ditemukan selama proses investigasi. Tabel 2 dibawah adalah hasil pemeriksaan SHA-256 pada barang bukti yang telah terkumpul, pemeriksaan SHA-256 ini bertujuan untuk menjaga keaslian barang bukti, agar nanti jika ada pemalsuan atau manipulasi barang bukti kita kita memeriksa nilai dari SHA-256 yang telah diperiksa pada masing-masing barang bukti pada saat awal ditemukan.

Tabel 2. Hasil Integrity Bukti

No	Nama Barang Bukti	Nilai SHA-256	Tahapan
1	Komentar Akun Palsu HaloBCA	0e0aec0fcc7f687d384b262ebe4688602a98496ec6b1ee8829e3f46296f49c68	4.1.2 barang bukti digital
2	Profile Akun Palsu HaloBCA	b313d6dec1d2671958803651df51c82130685d9415c647e2764d17b694d1dd14	Securing documentation
3	Keterkaitan Akun Twitte	2dbdf8d815cb90fffc14d58c363aaf2fa71e1dccc2a5f6e3a1a50a53e041b236	Examination poin a
4	Validasi Keterkaitan Kejahatan	b7f7bdaf39f5337213a1b0e105c3b3e0c46b4a407570d2e39518f29075974fdfc	Examination poin b

No	Nama Barang Bukti	Nilai SHA-256	Tahapan
5	Hasil Temuan Investigasi Akun Palsu HaloBCA	508b546755bfee2f46b5588436fe1ff635cb3309de15b0f3d0175cd14be641bf	Analysis poin a analysis akun palsu
6	Hasil Temuan Investigasi Akun Asli HaloBCA	ee12c8c4ab01c7630adf7c19189714e86dd14db7b4ab9a79ead4ced3f2c2b241	Analysis poin b analysis akun asli
7	No Telephon Akun Asli HaloBCA	a7851d76be9e7a0b6f475fadee5a3578ef881ae5f654ae5f56bf5deec6ef0296	Analysis poin c penegecekan No Telephon
8	No Telephon Akun Palsu HaloBCA 1	2b569bc45401b3729a7a65f098c5836b9ab74ee0d6c37a145575bf0edd52b52d	Analysis poin c penegecekan No Telephon

Selanjutnya, berikut hasi investigasi akun yang telah di analysis, dapat dilihat pada tabel 3.

Tabel 3. Hasil Investigasi Akun

No	Akun Twitter	Entity	Entity Result	Authenticity (terhadap bukti yang ada)
1	HaloBCA *@HaloBCA*	Akun Twitter	HaloBCA	√
		Website	www.bca.co.id	√
			www.klikbca.com	√
			Ibank.klikbca.com	√
		Phone Number	+62 811 1500 998	√
			+852 3653 5888	√
		Email Address	Halobca@bca.co.id	√
2	HaloBCA @esterhts	Akun Twitter	HaloBCA	-
		Website	www.findhs.codes	
		Phone Number	866 7326 139 19798885628	-
		Email Address	Nicole.spreck@inlandgroup.com	-
			jason@hamitauction.com	-

Di akun Twitter HaloBCA (@HaloBCA), terdapat entitas berupa akun Twitter, situs web, nomor telepon, dan alamat email yang konsisten dengan data resmi, karena domain email dan situs web yang digunakan telah terverifikasi keasliannya oleh pemerintah. Namun, akun Twitter HaloBCA (@esterhts) yang mencakup entitas akun Twitter, nomor telepon, dan alamat email, tidak dapat dianggap valid karena domain yang digunakan tidak sejalan dengan yang dinyatakan oleh pemerintah.Dari semua proses investigasi yang telah dilakukan, terbukti bahwa akun HaloBCA (@esterhts) adalah akun palsu, dan berikut adalah data pemilik dari akun tersebut :

Tabel 4. Data Pemilik Akun Palsu

Keterangan	Data
Nama Pemilik Akun	Risky
Asal	Angleton
No. Handphone/Telephone	+19798885628
Email	Nicole.spreck@inlandgroup.com

a. *Conclusion,* Bukti dan data yang telah berhasil dihimpun oleh penyelidik memberikan indikasi yang sangat meyakinkan bahwa akun yang digunakan oleh tersangka adalah palsu.

b. Evaluation, Pada tahap ini investigator melakukan evaluasi terhadap temuan telah ditemukan guna memperoleh pemahaman yang lebih mendalam mengenai proes kejahatan yang dilakukan oleh pelaku.

Berdasarkan tahap *Conclusion* dan *Evaluation* maka diperoleh *Report* berbetuk laporan *Chain of Custody,* seperti terilhat pada gambar 17. Dibawah ini .

EVIDENCE CHAIN OF CUSTODY

Case Number: 01 Offense: Melakukan penipuan dengan mengaku sebagai pihak dari bank BCA
Submitting Officer: (Name/ID#)
Victim: Abdulmaj081188
Suspect: Risky
Date/Time Seized 26 May 2023/23:26:42 Pm Location Of Seizue: Twitter

Description of Evidence		
Item #	**Quality**	**Description of Item**
Akun : HaloBCA (@esterhts)	OK	Akun Twitter yang digunakan oleh pelaku
Webisite : www.fidhs.codes	OK	Website yang digunakan oleh pelaku
Phone Number : 866 7326 139 +19798885628	OK	No. Telephon yang digunakan oleh pelaku
Email Address : Nocole.spreak@ilnadgroup.com jason@hamitauction.com	OK	Alamat Email yang digunakan oleh pelaku

Chain of Custody			
Item #	**Date/Time**	**Received by**	**Comments/Location**
Akun : HaloBCA (@esterhts)	23 May 2023	Achmad Syafaat	
Webisite : www.fidhs.codes	27 May 2023	Achmad Syafaat	
Phone Number : 866 7326 139 +19798885628	27 May 2023	Achmad Syafaat	
Email Address : Nocole.spreak@ilnadgroup.com jason@hamitauction.com	23 May 2023	Achmad Syafaat	

Gambar 14. Laporan Chain of Custody Digital Footprint

4. KESIMPULAN

Berdasarkan hasil penelitian yang diperoleh, dapat diambil kesimpulan bahwa :

1. Pemanfaatan Social Network Analysis (SNA) dalam struktur Kerangka Investigasi Digital Forensik dapat digunakan pada analisis penyelidikan pada platform media sosial.

2. Kelebihan dari Kerangka FDFI terletak pada kemampuannya sebagai alat pengumpul bukti digital, serta memiliki tingkat spesifik yang memadai dan kinerja yang cepat dalam menghadapi investigasi media sosial, terutama pada Twitter dan platform open source.

3. Implementasi metode Social Network Analysis dalam Kerangka FDFI dapat diaplikasikan pada penyelidikan media sosial Twitter dengan melakukan analisis terhadap akun yang mengaku sebagai instansi BCA, sehingga hasil investigasi dapat mengungkap bukti-bukti terkait keberadaan akun palsu.

DAFTAR PUSTAKA

Al Jumah, M. N., Sugiantoro, B., & Prayudi, Y. (2019). Penerapan metode composite logic untuk perancangan framework pengumpulan bukti digital pada media sosial. *ILKOM Jurnal Ilmiah*, *11*(2), 135–142.

Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, *28*, 126–138. https://doi.org/10.1016/j.diin.2019.02.001

Ibrahim, M. A., Li, L., & Wang, P. (2018). The Design of 220kV Substation Grounding Grid with Difference Soil Resistivity Using Wenner and Schlumberger Methods. *2018 China International Conference on Electricity Distribution (CICED)*, 2525–2530. https://doi.org/10.1109/CICED.2018.8592188

Kurniawan, A., & Prayudi, Y. (2014). *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics*. https://www.researchgate.net/publication/263847986

Niken Bestari. (2022). *Mengenal Digital Footprint: Penjelasan, Manfaat, dan Bahayanya*.

Nukman. (2022). *Pengembangan Framework Digital Forensics Investigation (FDFI) Pada Sosial Media Dengan Metode System Development Life Cycle (SDLC)*. Universitas Islam Indonesia.

Raharjo, B. (2013). SEKILAS MENGENAI FORENSIK DIGITAL. *Jurnal Sosioteknologi*, *12*(29), 384–387. https://doi.org/10.5614/sostek.itbj.2013.12.29.3

Van Dijk. (2016). *Media Sosial*. Jakarta Bumi Aksara.