



Model Ontologi Forensik Metadata Media Sosial

Ibnu Rohan Tuharea

19917027

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensik Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2024

Lembar Pengesahan Pembimbing

Model Ontologi Forensik Metadata Media Sosial

Ibnu Rohan Tuharea

19917027



Yogyakarta, Juni 2024

Pembimbing I


Dr. Ahmad Luthfi, S.Kom., M.Kom

Pembimbing II

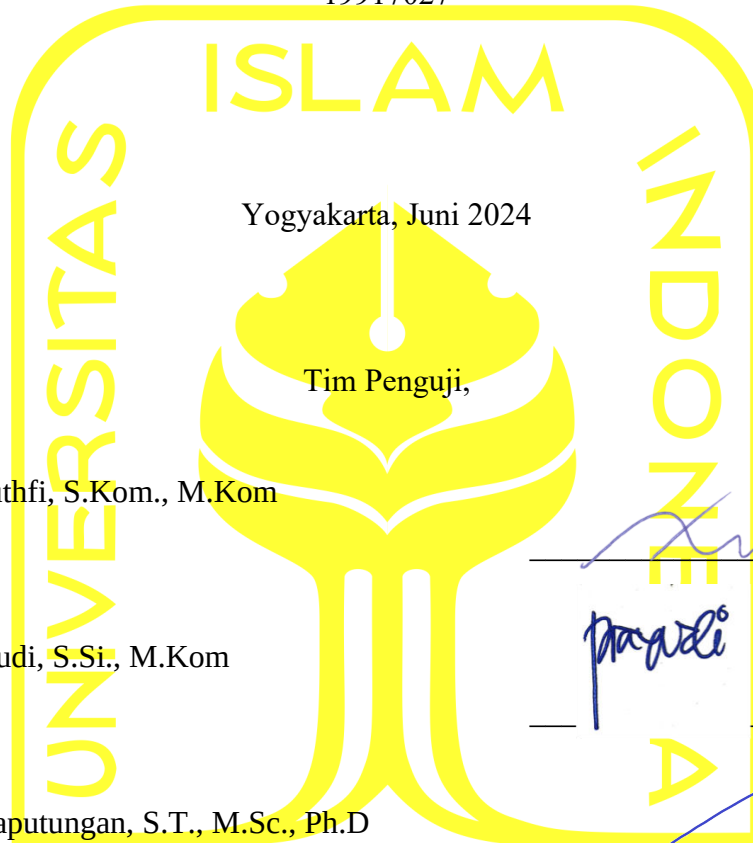

Erika Ramadhani, S.T., M.Eng

Lembar Pengesahan Penguji

Model Ontologi Forensik Metadata Media Sosial

Ibnu Rohan Tuharea

19917027



Yogyakarta, Juni 2024

Tim Penguji,

Dr. Ahmad Luthfi, S.Kom., M.Kom

Ketua

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

Anggota I

Irving Vitra Paputungan, S.T., M.Sc., Ph.D

Anggota II

10/09/2024

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Model Ontologi Forensik Metadata Media Sosial

Maraknya perangkat elektronik portabel, seiring dengan meluasnya penggunaan media sosial, telah membuka era baru aktivitas kriminal. Pada saat yang sama, bidang forensik digital, yang didedikasikan untuk penyelidikan bukti digital, menjadi semakin menonjol. Dalam makalah ini, kami memperkenalkan *Small-Scale Digital Device Forensics* (SSDDF), subbidang khusus yang berpusat pada pemeriksaan perangkat digital mini yang sering terlibat dalam aktivitas kriminal. SSDDF mengatasi tantangan unik yang terkait dengan perangkat ringkas ini. Lebih jauh lagi, penelitian ini menggarisbawahi kegunaan ontologi dalam forensik media sosial, mengeksplorasi potensi bukti digital yang dapat diterima oleh pengadilan dengan menguraikan struktur sistem operasi Android yang terkait dengan media sosial. Hal ini memungkinkan identifikasi dan ekstraksi berbagai kategori data digital, termasuk akun pengguna, pesan, dan gambar. Penelitian ini sangat diperlukan untuk investigasi forensik media sosial. Namun, perlu dicatat bahwa investigasi dalam makalah ini terutama berkonsentrasi pada bukti digital yang tersedia di platform media sosial, dan mengabaikan peran penting perangkat yang digunakan baik oleh penjahat maupun korban. Proses penggalian data digital dari perangkat-perangkat ini tetap penting dalam mengamankan bukti-bukti yang relevan dari media sosial. Meskipun demikian, integrasi SSDDF bersamaan dengan penjelasan struktur sistem Android telah memberikan kontribusi besar dalam memajukan metodologi forensik digital. Peningkatan ini berpotensi mendukung proses investigasi secara signifikan, memungkinkan pengumpulan dan analisis bukti digital penting dari perangkat elektronik kompak dan platform media sosial. Kesimpulannya, kemunculan SSDDF bersamaan dengan klarifikasi struktur sistem Android dan pemanfaatan ontologi dalam forensik media sosial memberikan wawasan yang sangat berharga di bidang forensik digital. Perkembangan ini menjanjikan peningkatan efisiensi dan efektivitas investigasi forensik, khususnya ketika mengumpulkan bukti digital substansial dari perangkat elektronik kecil dan platform media sosial. Hal ini, pada gilirannya, membuka jalan bagi penanganan bukti digital yang lebih baik di masa depan.

Kata kunci

Ontologi, RDF, OWL, Media Sosial , Digital Forensik, Ponsel Pintar

Abstract

Social Media Metadata Forensic Ontology Model

The prevalence of portable electronic devices, along with widespread social media use, has ushered in a new era of criminal activity. Simultaneously, the field of digital forensics, dedicated to the investigation of digital evidence, has gained significant prominence. In this paper, we introduce Small-Scale Digital Device Forensics (SSDDF), a specialized subfield that centers on the examination of miniature digital devices frequently involved in criminal activities. The SSDDF addresses the unique challenges associated with these compact devices. Furthermore, this research underscores the utility of ontology in social media forensics, exploring the potential for court-admissible digital evidence by deciphering Android operating system structures related to social media. This enables the identification and extraction of various categories of digital data, including user accounts, messages, and images. The research is indispensable for social media forensic investigations. However, it is worth noting that the investigations in this study primarily concentrate on digital evidence available on social media platforms, overlooking the crucial role of devices utilized by both criminals and victims. The process of extracting digital data from these devices remains pivotal for securing relevant evidence from social media. Nonetheless, the integration of SSDDF, along with the elucidation of Android system structures, has made substantial contributions to advancing digital forensic methodologies. These enhancements have the potential to significantly bolster the investigative process by enabling collection and analysis of vital digital evidence from compact electronic devices and social media platforms. In conclusion, the emergence of SSDDF alongside the clarification of Android system structures and the utilization of ontology in social media forensics provides invaluable insights to the field of digital forensics. These developments hold promise for enhancing the efficiency and effectiveness of forensic investigations, particularly when gathering substantial digital evidence from small electronic devices and social media platforms. This, in turn, paves the way for a more robust handling of digital evidence in the future.

Keywords

Ontology, RDF, OWL, Social Media, Digital Forensic, Smartphone

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, 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, Juni/2024



Ibnu Rohan Tuharea, S.Kom.

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari Bab 3

Rohan Tuharea, I., Luthfi, A., & Ramadani, E. (2023). Enhancing Digital Forensic Investigation: A Focus on Compact Electronic Devices and Social Media Metadata. *Journal of Information Systems and Informatics*, 5(4). <https://doi.org/10.51519/journalisi.v5i4.594>

Kontributor	Jenis Kontribusi
Ibnu Rohan Tuharea	Mendesain eksperimen (60%) Menulis <i>paper</i> (70%)
Ahmad Luthfi	Mendesain eksperimen (40%) Menulis dan mengedit <i>paper</i> (30%)
Erika Ramadani	Melakukan evaluasi dan analisis

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

Alhamdulillah Robbil ‘Alamin. Segala puji dan syukur atas kehadiran Allah Subhanahu Wa Ta’ala yang telah memberikan rahmat, ridho, dan karunia-Nya kepada saya. Shalawat serta salam kepada Nabi Muhammad Shallallahu ‘Alaihi Wasallam, sebagai pembawa risalah Allah terakhir dan penyempurna seluruh risalah-Nya. Tesis ini kupersembahkan kepada:

1. Allah Subhanahu Wa Ta’ala yang telah memberikan nikmat iman dan Islam, serta kepada Rasulullah Muhammad Shallallahu ‘Alaihi Wasallam yang senantiasa menuntun umatnya ke jalan yang penuh berkah,
2. kedua Orang tua yang selalu memberikan dukungan melalui doa, motivasi, serta mengarahkan hal baik dalam kehidupan,
3. dosen dan seluruh pengurus Akademik Magister Informatika UII yang bersedia memberikan waktu dan ilmu pengetahuan selama menempuh masa studi magister sehingga saya bisa sampai di titik ini,
4. teman-teman yang selalu memberikan semangat dan motivasi selama menempuh pendidikan.

Kata Pengantar

Puji syukur saya panjatkan kehadiran Allah Subhanahu Wa Ta'ala, karena atas berkat rahmat, taufik serta hidayahnya sehingga saya dapat menyelesaikan Laporan Tesis di Fakultas Teknologi Industri, Universitas Islam Indonesia Yogyakarta. Tidak lupa, shalawat serta salam saya haturkan kepada junjungan Nabi Muhammad Shallallahu 'Alaihi Wasallam yang telah membimbing Ummat manusia ke jalan yang baik.

Laporan Tesis yang berjudul “MODEL ONTOLOGI FORENSIK METADATA MEDIA SOSIAL” disusun dengan tujuan memenuhi salah satu syarat akademik untuk menempuh kelulusan Program Studi Informatika Program Magister pada Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta.

Ucapan terima kasih yang sebesar-besarnya kepada pihak yang telah membantu dalam menyelesaikan laporan ini kepada yang terhormat:

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., sebagai Rektor Universitas Islam Indonesia Yogyakarta,
2. Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D., sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta.
3. Bapak Yudi Prayudi, S.Si., M.Kom., selaku Ketua PUSFID Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta,
4. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom., selaku Pembimbing I yang telah memberikan arahan dalam membimbing dan membantu penulis selama penulisan Tesis ini,
5. Ibu Erika Ramadhani, S.T., M.Eng., selaku Pembimbing II yang telah meluangkan banyak waktunya dalam membimbing dan membantu penulis selama penulisan Tesis ini,
6. Segenap Dosen dan Staf Universitas Islam Indonesia Yogyakarta, khususnya Fakultas Teknologi Industri, yang telah mendukung dalam proses penyelesaian Tesis ini.

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	x
Daftar Tabel.....	xii
Daftar Gambar	xiii
Glosarium	xiv
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan masalah	4
1.3 Tujuan	5
1.4 Ruang Lingkup dan Batasan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Metode Penelitian	6
1.7 Sistematika Penulisan	6
BAB 2 Tinjauan Pustaka	8
2.1 Pendahuluan.....	8
2.2 Konsep Pengetahuan.....	12
2.2.1 Fenomena media sosial	12
2.2.2 Kasus pada Media Sosial.....	12
2.2.3 Forensik Digital dan Metadata Media Sosial	13

2.2.4	Ontologi.....	14
2.2.5	Web Semantik	15
2.2.6	RDF	15
2.2.7	OWL.....	15
BAB 3 Metodologi		17
3.1	Pendahuluan.....	17
3.2	Implementasi Studi Kasus	18
3.3	Tahapan Validasi dalam Implementasi Studi Kasus.....	19
3.4	Kondisi dan Batasan Perangkat	19
3.5	Akuisisi Data.....	20
3.6	Tantangan dan Keterbatasan	20
3.7	Pemetaan Ontologi.....	21
BAB 4 Hasil dan Pembahasan.....		23
4.1	Penerapan Praktis Ontologi SSDDF	23
4.2	Pengembangan Ontologi SSDDF	24
4.3	Implementasi Pertanyaan Kompetensi.....	27
4.4	Penerapan Praktis Ontologi Social Media Evidence (SMOnt)	29
4.5	Pengembangan Ontologi Social Media Evidence (SMOnt)	31
4.6	Keseluruhan Ontologi	42
4.7	Struktur Kelas	44
4.8	Struktur Properti Objek.....	44
4.9	Struktur Properti Data	45
4.10	Hasil Analisis	45
BAB 5 Kesimpulan dan Saran.....		48
5.1	Kesimpulan	48
5.2	Saran	49

Daftar Tabel

Tabel 2.1 Daftar penelitian terdahulu	9
Tabel 3.1 Peta perangkat dan pengguna dalam studi kasus	19
Tabel 4.1 Temuan bukti digital.....	25
Tabel 4.2 Temuan barang bukti digital dari sisi server.....	31
Tabel 4.3 Aspek-aspek dalam Efektifitas.	45

Daftar Gambar

Gambar 3.1 Skema pelaksanaan studi kasus.....	18
Gambar 4.1 Ontologi SSDDF	23
Gambar 4.2 Blok penyimpanan internal (mmcblk0) dan penyimpanan eksternal (mmcblk1) pada perangkat Samsung Galaxy J1 Ace	24
Gambar 4.3 Struktur partisi data pengguna dan daftar paket aplikasi Facebook.....	25
Gambar 4.4 Penambahan kelas pada soal kompetensi pertama pada ontologi SSDDF	27
Gambar 4.5 Penambahan kelas pada soal kompetensi kedua pada ontologi SSDDF	28
Gambar 4.6 Penambahan kelas pada soal kompetensi ketiga pada ontologi SSDDF.....	28
Gambar 4.7 Ontologi SSDDF	28
Gambar 4.8 Ontologi SMOnt.....	29
Gambar 4.9 Contoh berkas data pribadi dari penyedia layanan (Server)	31
Gambar 4.10 Ontologi SMOnt.....	41
Gambar 4.11 Keseluruhan ontologi	43

Glosarium

{Berisi daftar istilah-istilah beserta definisinya atau singkatan beserta kepanjangan yang spesifik/khusus terkait tema yang diambil dan dipergunakan dalam tesis ini. Jika sudah dituliskan di sini, maka dalam tesis tidak perlu dituliskan lagi kepanjangan atau definisinya. *Catatan: daftar ini dapat dihapus jika tidak diperlukan*}

BPM	- Business Process Management
BPMS	- Business Process Management System
CFC	- Control Flow Complexity
EDL	- Experience Driven Learning
MCDM	- Multi-Criteria Decision-Making
SAW	- Simple Additive Weighting
WP	- Weighted Product
XES	- eXtensible Event Stream

BAB 1

Pendahuluan

1.1 Latar Belakang

Penggunaan Internet dan media sosial semakin meningkat dari tahun ke tahun. Data *We Are Social* terkait penggunaan sumber daya digital di Indonesia pada Februari 2022 yang dikutip dari *datareportal.com* yaitu total populasi di Indonesia 277.7 juta dengan pengguna internet 73.7% (204.7 juta) serta 68.9% (191.4) juta merupakan pengguna media sosial dari total populasi, naik 12.6% dari Januari 2021. Selain itu, 93.5% pengguna media sosial dari total pengguna internet dengan rata-rata alokasi waktu penggunaan 3 jam 17 menit. Penggunaan platform media sosial paling banyak dari umur 16 sampai 64 tahun yaitu Whatsapp 88.7%, Instagram 84.8%, Facebook 81.3%, Tiktok 63.1%, Telegram 62.8%, Twitter 58.3% (*We Are Social*, 2022). Kondisi ini diikuti dengan munculnya berbagai macam fenomena pada penggunaan media sosial dari waktu ke waktu. Fenomena-fenomena seperti keterbukaan diri dengan mengunggah informasi terkait kegiatan yang mereka lakukan dan permasalahan pribadi yang dialami (Qurrota Ayun, 2015), perilaku-perilaku baru yaitu swafoto (*selfie*), *cyberwar*, belanja daring, personalisasi diri pengguna (*personalize*), dan budaya berbagi (*share*) (Mulawarman & Nurfitri, 2017), *self disclosure* (Sagiyanto & Ardiyanti, 2018), *phubbing* (Aditia, 2021), penggunaan media sosial sebagai hiburan (Bulele & Wibowo, 2020). Hingga *cyberbullying* (Rifauddin, 2016), penyebaran *hoax* (Pakpahan, 2017), narasi terorisme dan radikalisme (Rustandi, 2020), serta kasus kriminal lain yang berkaitan dengan media sosial.

Kasus-kasus yang berkaitan dengan media sosial banyak bermunculan di luar maupun dalam negeri. Beberapa kasus bahkan memberikan bukti bahwa media sosial dapat menjadi alat untuk pembuktian dalam persidangan. Kasus penangkapan seorang anggota geng dan pengedar narkoba di Bronx, New York, Amerika Serikat. Diawali dengan informasi dan data yang diberikan oleh informan (teman tersangka) terkait postingan foto dan percakapan pesan pada media sosial Facebook kepada polisi (Roberts, 2012). Adapun seorang ibu ditangkap bersama pacarnya di Arkansas, Amerika Serikat, dengan tuduhan penganiayaan anak perempuan berusia 3 tahun dan saudara laki-lakinya yang berusia 2 tahun hingga terluka setelah ada laporan yang masuk pada Polisi berdasarkan bukti foto-foto yang beredar di media sosial Facebook. Keduanya dipenjara dengan dakwaan kekerasan dalam rumah tangga tingkat pertama dan mengizinkan penyalahgunaan anak di bawah umur. Kasus

lain terkait pembunuhan yaitu seorang wanita warga negara Kanada ditangkap dan terbukti bersalah atas pembunuhan temannya sendiri setelah mengunggah foto di media sosial menunjukkan tersangka mengenakan sabuk, yang mana sabuk tersebut ditemukan dekat dengan tubuh dari korban dan disinyalir merupakan alat untuk menghilangkan nyawa korban di TKP (Schladebeck, 2018). Kasus terkait hilangnya seorang gadis berumur 21 tahun yang mengarahkan pacar dari korban ditetapkan sebagai tersangka. Bukti yang dijadikan sebagai petunjuk adalah dokumentasi foto-foto kedua pasangan itu pada Instagram dan Facebook saat melakukan perjalanan wisata ke Taman Nasional Grand Teton, Wyoming, Amerika Serikat, sebelum gadis tersebut menghilang serta dokumentasi video Youtube dari wisatawan lain yang melakukan perjalanan wisata ke tempat yang sama dan memperlihatkan adanya mobil yang sering dipakai korban dan pelaku beserta topi dan sandal dari korban yang ada pada mobil tersebut (Wandt, 2021). Selain dari luar negeri, adapun sumber dari dalam negeri yang lebih banyak terkait ujaran kebencian yang pada media sosial Facebook (Faisol, 2017; Zebua, 2017) dan Twitter (Nailufar, 2017).

Dalam forensik digital, terdapat beberapa tahapan atau proses yang harus dilakukan agar bukti yang dihasilkan dapat diterima di pengadilan (Nur Faiz et al., 2018). Tahapan ini dalam beberapa kasus dan menurut beberapa pendapat bisa menjadi tiga tahap atau pun lebih. Namun empat diantaranya yang menjadi sangat penting yaitu akuisisi (*acquisition*), pencarian (*searching*), analisa (*analysis*) dan presentasi (*presentation*) (Randelović & Stojković, n.d.). Jika berkaitan dengan media sosial, ada dua sumber yang bisa menjadi sarana untuk mendapatkan barang bukti digital yaitu perangkat yang dimiliki korban dan atau pelaku (klien) serta penyedia layanan (server), proses ini akan masuk pada tahapan akuisisi sesuai dengan tahapan forensik digital sebelumnya. Pada tahapan selanjutnya para penyidik akan melakukan pencarian dan analisa untuk mencari temuan barang bukti sebelum menyusun laporan dan presentasi terkait hasil temuan barang bukti.

Jika dalam investigasi ada tahapan untuk mencari dan menganalisa barang bukti digital, banyak peneliti yang mengembangkan model ontologi guna membangun basis data pengetahuan yang dapat dipakai kembali dan mendukung proses analisa dalam forensik digital. David Christopher Harrill dan Richard P. Mislan mengajukan ontologi yang bernama *Small Scale Digital Device Forensics* (SSDDF) (Harrill & Mislan, 2007). Kemudian pada penelitian Nickson M. Karie, M.Sc dan Hein S. Venter, Ph.D, ontologi SSDDF dimasukkan ke dalam sub ontologi yaitu *Device Forensic* (Karie & Venter, 2014). Selain ontologi yang telah disebutkan, terdapat beberapa penelitian ontologi digital forensik untuk media sosial. Salah satu ontologi yang membahas hal tersebut yaitu penelitian yang dilakukan oleh Edlira

Kalemi dan Sule Yildirim-Yayilgan. Perspektif yang mereka gunakan adalah barang bukti digital apa saja yang ada dalam metadata media sosial dan dapat dijadikan sebagai alat bukti yang sah di pengadilan. Berbeda dengan kebanyakan bidang forensik digital lain, forensik media sosial memberikan banyak informasi karena data yang diambil memiliki beragam entitas seperti profil pengguna, pesan, postingan status, foto, teman, grup dan lain-lain (Kalemi & Yildirim-yayilgan, 2016). Namun penelitian tersebut tidak membahas keterkaitan antara barang bukti digital dengan perangkat elektronik yang digunakan.

Metadata yang dihasilkan dari media sosial bisa beragam tergantung dari platformnya. Misalnya, Facebook memiliki properti *User*, *Post*, *Status* dan *Place*, sementara Twitter memiliki properti *User*, *Profile*, *Tweet*, *Geo* dan *Place* (Arshad et al., 2019). Metadata tersebut dapat diunduh dalam format XML, JSON, atau TXT (Flickr, YouTube, Twitter, dll (Abebe et al., 2020). Tidak banyak yang mengaitkan media sosial dengan perangkat elektronik dalam ontologi. Dalam forensik digital, salah satu dari tiga tahapan penting yang harus dilakukan dalam investigasi adalah akuisisi (Randelović & Stojković, 2012), sehingga perangkat dari pelaku dan/atau korban bisa dijadikan sebagai barang bukti yang kemudian dilakukan akuisisi ke dalam barang bukti digital.

Peningkatan penggunaan internet dan media sosial telah menimbulkan berbagai tantangan dalam konteks investigasi forensik digital. Fokus penelitian ini adalah mengembangkan ontologi yang mengintegrasikan *Small Scale Digital Device Forensics* (SSDDF) dan ontologi *Social Media Evidence*. Peneliti bertujuan untuk memetakan hubungan antara perangkat elektronik berskala kecil, seperti ponsel pintar, dengan metadata media sosial. Dengan menguraikan hirarki kelas dan objek dalam ontologi, penelitian ini berharap dapat meningkatkan pemahaman tentang interaksi kompleks antara perangkat bergerak dan data media sosial dalam konteks forensik digital.

Keberhasilan investigasi forensik digital sangat bergantung pada kemampuan memperoleh dan menganalisis bukti digital. Dalam konteks ini, pengembangan ontologi yang mengaitkan media sosial dengan perangkat elektronik berskala kecil menjadi krusial. Ontologi ini diharapkan dapat memberikan landasan yang kokoh untuk memahami dan mengorganisir bukti digital dari kedua sumber tersebut, membantu penyidik forensik dalam menghadapi kompleksitas kasus terkait media sosial (Arshad et al., 2019; Nikolaidou et al., 2019). Langkah ini diambil dengan tujuan meningkatkan integrasi antara sisi perangkat, memungkinkan analisis yang lebih mendalam terhadap bukti digital yang ditemukan. Dengan demikian, penelitian ini tidak hanya merespons perubahan dinamika penggunaan

internet dan media sosial, tetapi juga berupaya menghadirkan kontribusi positif dalam bidang forensik digital di era digital ini (Mohan & Venkataraman, 2017).

Selain itu, pentingnya membangun ontologi dalam penelitian ini terletak pada peran ontologi sebagai representasi yang memungkinkan penyusunan struktur dan hubungan konsep di dalam suatu domain tertentu. Dalam konteks penelitian ini, ontologi berperan sebagai kerangka kerja yang memfasilitasi pemahaman dan pengorganisasian informasi terkait metadata media sosial dan perangkat bergerak skala kecil. Ontologi membantu menciptakan suatu struktur yang jelas dan terstandarisasi, memungkinkan peneliti untuk merepresentasikan entitas, properti, dan hubungan antar kelas atau objek dengan cara yang kohesif dan dapat diinterpretasikan (Jadhao & Agrawal, 2016). Dalam konteks metadata media sosial, ontologi dapat membantu dalam pengorganisasian dan kategorisasi informasi terkait, seperti data pengguna, postingan, atau interaksi. Sementara itu, pada domain perangkat bergerak skala kecil, ontologi dapat memberikan kerangka kerja untuk memahami struktur folder, aplikasi, atau data yang dihasilkan oleh perangkat. Dengan membangun ontologi pada dua domain ini, peneliti menciptakan landasan untuk mengambil barang bukti dan menginterpretasikan informasi dari dua sumber yang berbeda. Ontologi membantu memudahkan pemahaman terhadap struktur data, memberikan konteks yang diperlukan untuk analisis forensik, serta keberlanjutan dalam pengelolaan informasi di dalam penelitian ini (Turnbull & Randhawa, 2015). Dengan kata lain, ontologi menjadi fondasi yang mendasar untuk mencapai pemahaman yang mendalam dan terstruktur di dalam domain metadata media sosial dan perangkat bergerak berskala kecil.

Urgensi ilmiah dalam penelitian ini terletak pada kebutuhan mendesak untuk memiliki metode yang efektif dan terstruktur dalam mengelola dan menganalisis data dari media sosial, khususnya *Facebook*. Dengan jumlah pengguna yang terus meningkat dan kompleksitas data yang dihasilkan, pengembangan ontologi menjadi sangat penting untuk meningkatkan efektivitas dan efisiensi investigasi forensik digital. Penelitian ini tidak hanya memberikan kontribusi teoretis, tetapi juga aplikasi praktis yang relevan dengan kebutuhan saat ini, membantu penyidik dalam mengumpulkan dan menganalisis bukti dari media sosial dengan cara yang dapat diterima di pengadilan.

1.2 Rumusan masalah

Berdasarkan permasalahan yang telah diuraikan pada latar belakang di atas, adapun rumusan masalah dari penelitian ini yaitu:

- a. Bagaimana membangun model ontologi untuk analisis metadata media sosial?
- b. Bagaimana memetakan perangkat bergerak dalam ontologi forensik media sosial?

1.3 Tujuan

Membuktikan apakah ontologi forensik digital pada media sosial dapat membantu proses investigasi dan analisis bukti digital.

1.4 Ruang Lingkup dan Batasan Penelitian

Untuk lebih fokus dan terarahnya penelitian yang dilakukan dan berdasarkan rumusan masalah yang telah diuraikan sebelumnya, maka peneliti memberikan batasan dalam penelitian ini:

- a. Platform media sosial yang menjadi fokus penelitian yaitu Facebook.
- b. Perangkat smartphone Samsung J1 Prime.

1.5 Manfaat Penelitian

Manfaat penelitian yang dapat diambil dan diharapkan dari penelitian ini adalah sebagai berikut:

1. Meningkatkan efektivitas dan efisiensi investigasi forensik digital. Penelitian ini mengembangkan ontologi yang mengintegrasikan *Small Scale Digital Device Forensics* (SSDDF) dengan *Social Media Evidence*, yang dapat meningkatkan efisiensi investigasi. Dengan pemetaan hubungan antara perangkat elektronik skala kecil dan metadata media sosial, penyidik forensik dapat menghemat sumber daya dalam proses akuisisi, pencarian, dan analisis bukti digital.
2. Memfasilitasi analisis bukti digital yang lebih mendalam. Ontologi yang dihasilkan dari penelitian ini memungkinkan penyidik forensik untuk memahami interaksi yang kompleks antara perangkat elektronik dan data media sosial. Ini membantu dalam pengelolaan dan pengorganisasian data yang lebih baik, yang dapat meningkatkan akurasi dan keandalan dalam analisis forensik.
3. Meningkatkan standarisasi dan keteraturan data. Pengembangan ontologi dalam penelitian ini memberikan landasan untuk standarisasi data yang diambil dari media sosial dan perangkat bergerak. Hal ini memungkinkan penyusunan struktur data yang lebih jelas, mempermudah pemahaman dan pengelolaan informasi, serta mendukung interoperabilitas di berbagai domain forensik digital.
4. Menyediakan solusi inovatif untuk investigasi kriminal. Ontologi yang dikembangkan dalam penelitian ini menawarkan pendekatan inovatif untuk menghadapi tantangan dalam pengumpulan dan pengelolaan bukti digital dari media sosial. Penelitian ini berpotensi menjadi kontribusi yang signifikan bagi dunia

forensik digital, terutama dalam menghadapi kejahatan yang berkaitan dengan media sosial.

5. Mendukung keberterimaan bukti di pengadilan. Dengan mengacu pada standar-standar forensik digital yang dapat diterima di pengadilan, penelitian ini membantu memastikan bahwa bukti digital yang dihasilkan dari media sosial dan perangkat elektronik dapat diolah dan dipresentasikan dengan cara yang sesuai dengan kebutuhan hukum.

1.6 Metode Penelitian

Secara garis besar penelitian ini tergolong sebagai jenis penelitian *exploratory* atau eksplorasi, yang mana penelitian jenis ini terdiri dari upaya untuk menemukan sesuatu yang baru dan menarik, dengan mengerjakan topik penelitian (Colin Elman, 2020). Metode penelitian ini berfokus pada pengembangan dan validasi ontologi forensik digital melalui studi kasus penipuan *online* di media sosial, khususnya Facebook.

Dalam penelitian ini, dua perangkat Android digunakan: *Samsung Galaxy Mega 2* dan *Samsung Galaxy J1 Ace*, masing-masing merepresentasikan pelaku dan korban fiktif. Studi kasus ini mencerminkan skenario interaksi penipuan antara kedua akun di platform Facebook, dari komunikasi awal hingga terjadinya penipuan. Data dikumpulkan melalui metode *rooting* menggunakan *Magisk* dan akuisisi berbasis *dd* untuk mengekstraksi bukti digital dari perangkat yang terlibat. Proses akuisisi data meliputi ekstraksi komunikasi digital, seperti pesan teks, gambar, dan berkas multimedia.

Data hasil dari akuisisi perangkat dianalisis dengan pemetaan ontologi *Small-Scale Digital Device Forensic* (SSDDF) dan *Social Media Ontology* (SMOnt). Hasil akuisisi ini juga digunakan untuk mengarahkan pengembangan kedua ontologi tersebut, yang kemudian digabungkan menjadi kerangka kerja baru. Kerangka ini dirancang untuk pemetaan kasus yang berkaitan dengan media sosial. Penggabungan kedua ontologi ini bertujuan untuk membangun kerangka kerja holistik yang dapat memfasilitasi pemahaman menyeluruh tentang bukti digital dalam konteks perangkat skala kecil dan media sosial. Tahapan validasi diterapkan untuk mengukur relevansi ontologi yang dikembangkan terhadap skenario penipuan yang dianalisis.

1.7 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuatlah urutan penulisan sebagai berikut:

BAB I Pendahuluan

Pendahuluan berisi uraian pengantar mengenai masalah yang akan diteliti, di dalamnya menguraikan tentang bagaimana gambaran dari suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Pada bab ini menjelaskan mengenai teori-teori yang melandasi dan berkaitan dengan penelitian terkait guna memecahkan masalah dalam penelitian ini.

BAB III Metodologi Penelitian

Bab metodologi penelitian membahas tentang langkah-langkah atau prosedur jalannya penelitian dari awal sampai akhir, sehingga mampu menyelesaikan masalah secara sistematis.

BAB IV Pembahasan

Pada bab ini berisi hasil atau temuan dan pembahasan dari penelitian terkait penyelesaian masalah yang diangkat, serta uraian analisis mengenai hasil dari temuan tersebut.

BAB V Kesimpulan dan Saran

Bab ini merupakan bab terakhir yang menjelaskan mengenai kesimpulan akhir yang didapat dari hasil analisis penelitian untuk menjawab rumusan masalah serta saran yang perlu diperhatikan mengenai penelitian lanjutan yang diharapkan dapat dilakukan di masa depan.

BAB 2

Tinjauan Pustaka

2.1 Pendahuluan

Sebagaimana penjelasan dalam latar belakang, ontologi dalam forensika digital sudah mulai berkembang. Dari bidang atau domain umum (utama) yaitu forensika digital atau *Digital Forensic* (Karie & Venter, 2014), yang dalamnya terpetakan disiplin ilmu atau sub bidang forensika perangkat atau *Device Forensic*, semakin menelusur kedalam ontologi tersebut terdapat sub bidang atau sub disiplin ilmu forensika perangkat berskala kecil atau *Small Scale Digital Device Forensic* (Harrill & Mislan, 2007) yang memiliki beberapa objek penelitian tablet, embedded device, GPS device, PDA device, Smart/Cell phones, dan lain-lain. Bagan dari ontologi sub bidang forensika digital yang telah dijelaskan dapat dilihat pada **Lampiran 1 - BIDANG ILMU FORENSIKA DIGITAL ATAU DIGITAL FORENSIC** dan **LAMPIRAN 2 - PENGELOMPOKAN OBJEK DALAM FORENSIKA PERANGKAT BERSKALA KECIL ATAU SMALL SCALE DEVICE DIGITAL FORENSIC**.

Disisi lain penelitian lebih lanjut telah dilakukan terkait media sosial yang memetakan barang bukti apa saja yang bisa didapatkan dari akun sosial media seseorang (Kalemi & Yildirim-yayilgan, 2016). Bagan dari ontologi barang bukti digital media sosial dapat dilihat pada **LAMPIRAN 3 - ONTOLOGI FORENSIKA BARANG BUKTI DIGITAL MEDIA SOSIAL ATAU SOCIAL MEDIA DIGITAL EVIDENCE ONTOLOGY**.

Adapun review penelitian lain yang berkaitan dengan tema penelitian ini akan dibahas dalam tabel berikut:

Tabel 2.1 Daftar penelitian terdahulu

No.	Peneliti	Metode penelitian	Hasil penelitian
1	(Harrill & Mislan, 2007)	Mengajukan sub ontologi yang bernama <i>Small Scale Digital Device Forensics</i> (SSDDF).	Ada 18 perangkat berskala kecil yang teridentifikasi dalam kategori ontologi ini. Selanjutnya masing-masing perangkat tersebut dipetakan berdasarkan cara menyimpan data yaitu secara magnetik, secara optikal, menggunakan <i>solid-state flash memory</i> dan perangkat yang dapat menambah kegunaan komputer. Kemudian pengelompokan perangkat berdasarkan kemampuan menyimpannya. Lihat lampiran 1
2	(Karie & Venter, 2014)	Menggabungkan beberapa ontologi ke dalam sub ontologi <i>Digital Forensic</i> .	Ontologi SSDDF dimasukan ke dalam sub ontologi yang lebih besar yaitu <i>Device Forensic</i> .
3	(Kalemi & Yildirim-yayilgan, 2016)	“ <i>Social Media Digital Evidence Ontology</i> ”, perspektif yang mereka gunakan yaitu dari sisi barang bukti digital yang ada dalam media sosial dan dapat dijadikan sebagai alat bukti yang sah di pengadilan.	Menghasilkan model ontologi untuk membantu penyelidikan forensik digital dalam domain media sosial
4	(Mohan & Venkataraman, 2017)	Ontologi dalam media sosial seperti pengembangan analisis media sosial menggunakan ontologi web.	Informasi terkait film yang ditonton oleh pengguna dapat diambil dan dikonstruksikan berdasarkan linimasa menggunakan OWL pada aplikasi Protégé. Data yang diekstrak menggunakan Graph API Explorer versi 1.

5	(Kalemi et al., 2017)	Pengembangan “Social Media Ontology” atau SMONT dengan teknologi web semantic yaitu OWL dan RDF.	Dengan ontologi ini dapat dilakukan analisa dari perpaduan antara data yang ada pada media sosial dan data yang ada pada repositori dari pihak berwajib sehingga dapat dilakukan penarikan kesimpulan yang berkaitan dalam relasi yang ada.
6	(Arshad et al., 2019)	Pengembangan semantic framework berlapis untuk akuisisi yang berkaitan dengan media sosial.	Pada penelitian ini dikembangkan model ontologi yang universal atau global yang dapat berkolaborasi dengan ontologi media sosial lain seperti Facebook dan ontologi Twitter. Ontologi-ontologi media sosial tersebut diekstrak beberapa properti yang memiliki kesamaan dalam ontologi global seperti properti Post dan Status pada ontologi Facebook serta properti Tweet pada ontologi Twitter yang dimasukkan ke dalam properti Object dalam ontologi global. Selain itu ada properti User, Place, created_at / created_time pada masing-masing ontologi media sosial yang dimasukkan ke dalam properti yang relevan pada ontologi global. Sehingga dapat diekstrak grafis interaksi sebagai contoh interaksi subjek atau pengguna dengan pengguna lain.
7	(Bratsas et al., 2021)	The use of national strategic reference framework data in knowledge graphs and data mining to identify red flags	Hasil penelitian ini menggambarkan pengembangan platform <i>RedFlags</i> yang menggunakan <i>National Strategic Reference Framework</i> (NSRF) Open Data, teknologi <i>semantic web</i> , dan teknik <i>data mining</i> untuk mengidentifikasi " <i>Red Flags</i> " pada proyek-proyek fiskal. Dengan memanfaatkan ontologi, <i>RDF triples</i> , dan <i>SPARQL queries</i> , penelitian ini berhasil menghadirkan sistem berbasis

			<p>pengetahuan yang menghitung indikator kinerja dan menggunakan algoritma DBSCAN untuk mengenali potensi masalah dalam implementasi proyek. Skenario penggunaan yang melibatkan auditor dalam memeriksa proyek-proyek NSRF menunjukkan bahwa platform RedFlags lebih cenderung mengidentifikasi kegagalan proyek dan tidak menimbulkan "<i>Red Flags</i>" pada proyek yang tidak ditolak, sesuai dengan permintaan pengguna. Dengan andil proyek yang ditolak sebanyak 3.8% dari total proyek, penelitian ini menyimpulkan bahwa <i>RedFlags</i> menggunakan open data dapat membantu auditor mengorganisir proses pemantauan dengan lebih efisien, memberikan kontribusi pada deteksi potensi risiko pada proyek fiskal, dan meningkatkan efektivitas sistem manajemen fraud.</p>
8	Ibnu Rohan Tuharea, 2022	Model Ontologi Forensik Metadata Media Sosial	<p>Pada penelitian ini penulis mengembangkan ontologi forensik metadata media sosial yang memetakan perangkat kecil (mobile) dengan metadata media sosial.</p>

2.2 Konsep Pengetahuan

2.2.1 Fenomena media sosial

Penggunaan Internet dan media sosial semakin meningkat dari tahun ke tahun. Data *We Are Social* terkait penggunaan sumber daya digital di Indonesia pada Februari 2022 yang dikutip dari datareportal.com yaitu total populasi di Indonesia 277.7 juta dengan pengguna internet 73.7% (204.7 juta) serta 68.9% (191.4 juta) merupakan pengguna media sosial dari total populasi, naik 12.6% dari Januari 2021. Selain itu, 93.5% pengguna media sosial dari total pengguna internet dengan rata-rata alokasi waktu penggunaan 3 jam 17 menit. Penggunaan platform media sosial paling banyak dari umur 16 sampai 64 tahun yaitu Whatsapp 88.7%, Instagram 84.8%, Facebook 81.3%, Tiktok 63.1%, Telegram 62.8%, Twitter 58.3% (We Are Social, 2022).

Kondisi ini diikuti dengan munculnya berbagai macam fenomena pada penggunaan media sosial dari waktu ke waktu. Fenomena-fenomena seperti keterbukaan diri dengan mengunggah informasi terkait kegiatan yang mereka lakukan dan permasalahan pribadi yang dialami (Qurrota Ayun, 2015), perilaku-perilaku baru yaitu swafoto (*selfie*), *cyberwar*, belanja daring, personalisasi diri pengguna (*personalize*), dan budaya berbagi (*share*) (Mulawarman & Nurfitri, 2017), *self disclosure* (Sagiyanto & Ardiyanti, 2018), *phubbing* (Aditia, 2021), penggunaan media sosial sebagai hiburan (Bulele & Wibowo, 2020). Hingga *cyberbullying* (Rifauddin, 2016), penyebaran *hoax* (Pakpahan, 2017), narasi terorisme dan radikalisme (Rustandi, 2020), serta kasus kriminal lain yang berkaitan dengan media sosial.

2.2.2 Kasus pada Media Sosial

Kasus-kasus yang berkaitan dengan media sosial banyak bermunculan di luar maupun dalam negeri. Beberapa kasus bahkan memberikan bukti bahwa media sosial dapat menjadi alat untuk pembuktian dalam persidangan. Kasus penangkapan seorang anggota geng dan pengedar narkoba di Bronx, New York, Amerika Serikat. Diawali dengan informasi dan data yang diberikan oleh informan (teman tersangka) terkait postingan foto dan percakapan pesan pada media sosial Facebook kepada polisi (Roberts, 2012).

Adapun seorang ibu ditangkap bersama pacarnya di Arkansas, Amerika Serikat, dengan tuduhan penganiayaan anak perempuan berusia 3 tahun dan saudara laki-lakinya yang berusia 2 tahun hingga terluka setelah ada laporan yang masuk pada Polisi berdasarkan bukti foto-foto yang beredar di media sosial Facebook. Keduanya dipenjara dengan dakwaan kekerasan dalam rumah tangga tingkat pertama dan mengizinkan penyalahgunaan anak di bawah umur (Jones, 2018).

Kasus lain terkait pembunuhan yaitu seorang wanita warga negara Kanada ditangkap dan terbukti bersalah atas pembunuhan temannya sendiri setelah mengunggah foto di media sosial menunjukkan tersangka mengenakan sabuk, yang mana sabuk tersebut ditemukan dekat dengan tubuh dari korban dan disinyalir merupakan alat untuk menghilangkan nyawa korban di TKP (Schladebeck, 2018).

Kasus terkait hilangnya seorang gadis berumur 21 tahun yang mengarahkan pacar dari korban ditetapkan sebagai tersangka. Bukti yang dijadikan sebagai petunjuk adalah dokumentasi foto-foto kedua pasangan itu pada Instagram dan Facebook saat melakukan perjalanan wisata ke Taman Nasional Grand Teton, Wyoming, Amerika Serikat, sebelum gadis tersebut menghilang serta dokumentasi video Youtube dari wisatawan lain yang melakukan perjalanan wisata ke tempat yang sama dan memperlihatkan adanya mobil yang sering dipakai korban dan pelaku beserta topi dan sandal dari korban yang ada pada mobil tersebut (Wandt, 2021).

Selain dari luar negeri, adapun sumber dari dalam negeri yang lebih banyak terkait ujaran kebencian. Gara-gara menulis status di media sosial, warga Desa Sukokerto, Kecamatan Pajarak, Kabupaten Probolinggo, Jawa Timur, diciduk tim cyber Polres Probolinggo. Tersangka dijerat pasal 27 ayat (3) juncto pasal 45 ayat (1) UU RI tahun 2008 tentang Informasi dan Transaksi Elektronik (Faisol, 2017). Seorang pegawai negeri sipil dan seorang satuan pengamanan pada sebuah perusahaan pegadaian di Kota Tarakan, Kalimantan Utara, harus berurusan dengan Kepolisian Resor Tarakan akibat ujaran kebencian karena tersangka tidak terima ditilang karena berhenti ditanda larangan parkir di media sosial (Zebua, 2017). Ada juga artis dan musikus Ahmad Dhani dilaporkan kepada polisi terkait dengan penyebaran informasi yang menimbulkan kebencian oleh kelompok pendukung Ahok-Djarot. Dhani membuat kicauan di akun Twitter, yang nadanya menghasut dan penuh kebencian (Nailufar, 2017).

2.2.3 Forensik Digital dan Metadata Media Sosial

Dalam forensik digital, terdapat beberapa tahapan atau proses yang harus dilakukan agar bukti yang dihasilkan dapat diterima di pengadilan (Nur Faiz et al., 2018). Tahapan ini dalam beberapa kasus dan menurut beberapa pendapat bisa menjadi tiga tahap atau pun lebih. Namun empat diantaranya yang menjadi sangat penting yaitu akuisisi (*acquisition*), pencarian (*searching*), analisa (*analysis*) dan presentasi (*presentation*) (Randelović & Stojković, n.d.).

Jika berkaitan dengan media sosial, ada dua sumber yang bisa menjadi sarana untuk mendapatkan barang bukti digital yaitu perangkat yang dimiliki korban dan atau pelaku (klien) serta penyedia layanan (server), proses ini akan masuk pada tahapan akuisisi sesuai dengan tahapan forensik digital sebelumnya. Pada tahapan selanjutnya para penyidik akan melakukan pencarian dan analisa untuk mencari temuan barang bukti sebelum menyusun laporan dan presentasi terkait hasil temuan barang bukti.

Adapun metadata yang dihasilkan dari media sosial bisa beragam tergantung dari media sosial. Seperti dalam Facebook ada properti User, Post, Status dan Place, sedangkan Twitter ada properti User, Profile, Tweet, Geo dan Place (Arshad et al., 2019). Properti yang dihasilkan akan diunduh dengan format metadata yang berbeda seperti XML, JSON, atau TXT (Flickr, YouTube, Twitter, dll (Abebe et al., 2020).

2.2.4 Ontologi

Ontologi sebagai cabang filsafat menurut Barry Smith dalam buku *The furniture of the world*, merupakan ilmu tentang apa adanya, tentang jenis dan struktur objek, sifat, peristiwa, proses, dan hubungan dalam setiap bidang realitas (Hurtado, 2012). Tidak hanya hanya khusus dalam filsafat, ontologi menjadi sarana dalam memetakan berbagai pengetahuan. Nicola Guarino, Daniel Oberle dan Steffen Staab pada bagian “*What Is an Ontology?*” dalam buku “*Handbook on Ontologies*”, mengatakan bahwa ontologi digunakan dengan arti yang berbeda dalam komunitas yang berbeda (Staab & Studer, 2009). Dalam buku tersebut, para penulis mencoba untuk menggolongkan ontologi menjadi dua berdasarkan kata benda. Yaitu ontologi sebagai kata benda yang tidak dapat dihitung dan ontologi sebagai kata benda yang dapat dihitung.

Ontologi sebagaimana yang dimaksud pada golongan yang pertama yaitu studi tentang atribut-atribut yang dimiliki oleh benda karena sifat-sifatnya, meskipun benda tersebut tidak memiliki keberadaan yang jelas. Sehingga jika benda tersebut masih memiliki sifat dan strukturnya dapat dijelaskan dalam kategori dan hubungan umum, maka masih memungkinkan untuk masuk dalam studi ontologi.

Untuk golongan yang kedua atau ontologi yang memiliki wujud, merupakan penggunaan paling umum dalam ilmu komputer, para penulis merujuk pada ontologi sebagai jenis khusus dari objek informasi atau artefak komputasi. Sehingga ontologi pun dapat dihitung atau dapat dikomputasikan. Para peneliti menjelaskan, ontologi yang dikomputasikan ini merupakan sarana untuk secara formal memodelkan struktur suatu

sistem, yaitu entitas dan hubungan yang relevan yang muncul dari pengamatannya, dan yang berguna untuk tujuan berbagai orang.

Dalam sistem informasi, ontologi menjadi salah satu metode representasi pengetahuan penting yang telah diadopsi secara luas di bidang fusi data dan integrasi sistem informasi karena interoperabilitas semantik dan terbaca mesin yang tinggi (Ma & Molnár, 2020).

2.2.5 Web Semantik

Pada awal kemunculannya, website dibuat dalam arsitektur kumpulan beberapa berkas HTML dalam tempat penyimpanan yang dapat diakses dari manapun. Setiap berkas ini memiliki data dan/atau informasi yang akan ditampilkan kepada pengguna. Berkas-berkas tersebut juga saling terhubung satu sama lain layaknya jaringan.

Web Semantik atau *Semantic Web* adalah jaringan yang dapat dibaca mesin. Seperti yang telah dijelaskan, jaringan yang dapat dibaca mesin memfasilitasi kerjasama manusia dan komputer. Jika sesuai dan diperlukan, beberapa tugas tertentu dapat didelegasikan ke mesin dan diproses secara otomatis. Tentu saja, kemungkinan desain untuk website yang dapat dibaca mesin sangat besar, dan sejumlah keputusan desain diambil dalam mengembangkan *Semantic Web* seperti yang terlihat saat ini (John Domingue, Dieter Fensel, 2011).

2.2.6 RDF

Resource Description Framework (RDF) adalah kerangka kerja untuk membuat pernyataan di Web tentang apapun (John Domingue, Dieter Fensel, 2011). Hal ini memungkinkan siapa saja untuk menggambarkan sumber daya, terutama sumber daya Web, seperti penulis, tanggal pembuatan, subjek, dan hak cipta dari suatu gambar. RDF pertama kali diterbitkan oleh W3C pada tahun 1999 tak lama setelah rekomendasi pertama XML Syntax pada tahun 1998.

Ide utama RDF adalah untuk mendefinisikan kerangka kerja baru untuk melihat, memanipulasi, dan mengasosiasikan kumpulan jaringan informasi terdistribusi. Dengan demikian, ini memberikan interoperabilitas antar aplikasi yang bertukar informasi yang dapat dimengerti mesin. Visi ini awalnya dijelaskan dalam *Semantic Web Roadmap* oleh Tim Berners-Lee (<http://www.w3.org/DesignIssues/Semantic.html>).

2.2.7 OWL

OWL adalah bahasa ontologi yang direkomendasikan oleh W3C. OWL sangat didasarkan pada bahasa representasi pengetahuan yang disebut Logika Deskripsi, yang menyediakan

fitur representasi dasar OWL. OWL juga mencakup fasilitas yang mengintegrasikannya ke dalam arus utama Web, termasuk penggunaan *Internationalized Resource Identifiers* (IRIs) sebagai nama, tipe data Skema XML, dan ontologi sebagai dokumen Web, yang kemudian dapat mengimpor ontologi OWL lainnya melalui Web. Karena OWL didasarkan pada Logika Deskripsi, konstruksinya memiliki arti yang jelas dan ada alat yang melakukan inferensi di OWL, memungkinkan penemuan informasi yang tidak secara eksplisit dinyatakan dalam ontologi OWL (John Domingue, Dieter Fensel, 2011).

OWL juga terintegrasi penuh ke dalam Semantic Web dan menggunakan rekomendasi W3C lainnya. Sintaks transfer resmi untuk ontologi OWL adalah RDF/XML, sintaks untuk mentransfer grafik RDF. Nama (individu, dll.) di Web Semantik adalah *International Resource Identifier* (IRI), jadi nama di OWL adalah IRI. OWL menggunakan tipe data XML *Schema* untuk mendefinisikan dan mengetik nilai data yang digunakannya. Ontologi OWL adalah dokumen Web dan disimpan dan diambil seperti dokumen Web lainnya. OWL termasuk konstruksi untuk mengidentifikasi ontologi dan mengimpor satu ontologi ke yang lain. Ontologi OWL juga dapat digabungkan dengan aturan menggunakan standar W3C *Rule Interchange Format* (RIF) baru.

BAB 3

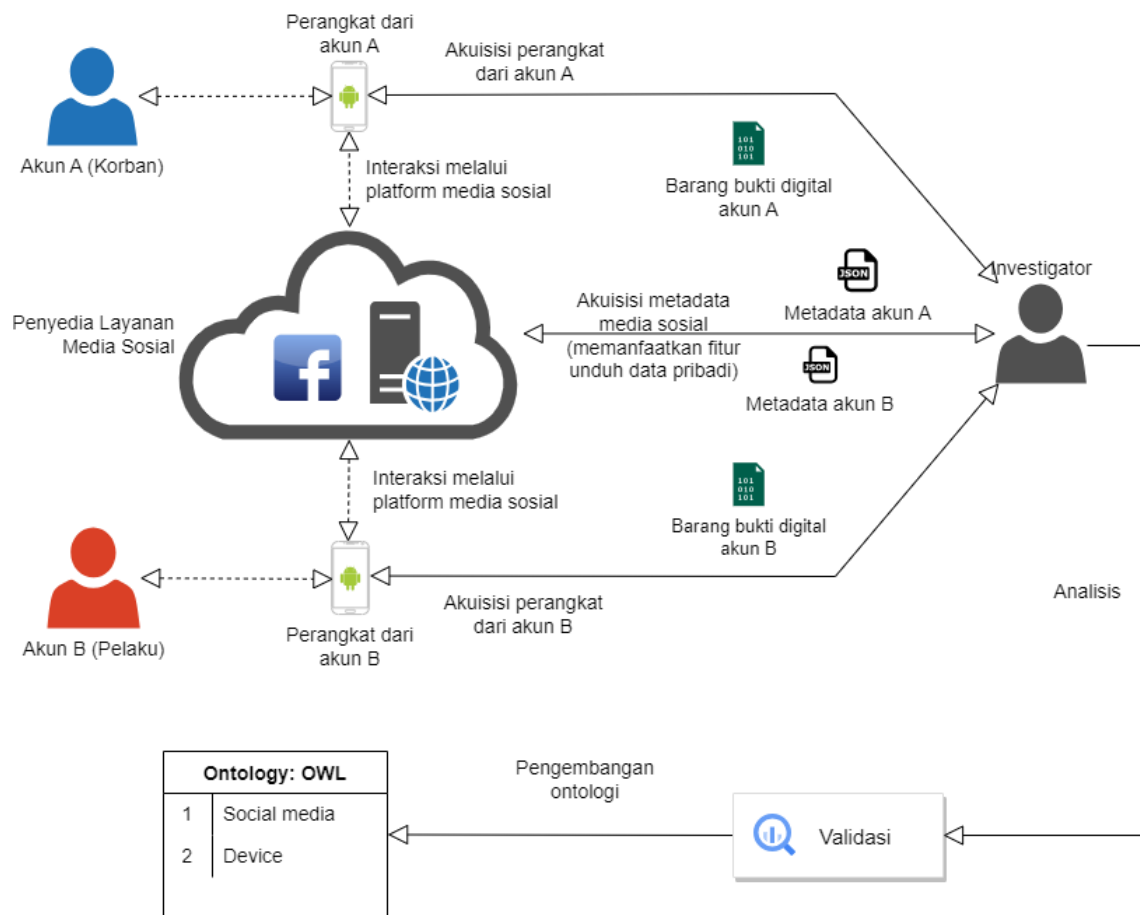
Metodologi

3.1 Pendahuluan

Penelitian ini menggunakan metodologi eksperimental untuk mengembangkan dan memetakan ontologi, serta mengimplementasi studi kasus yang komprehensif yang mengeksplorasi interaksi antara akun tersangka (**Garry Swihart**) dengan perangkat *Android Samsung Galaxy Mega 2* dan akun korban (**Norah Nolan**) yang dilengkapi dengan perangkat *Android Samsung Galaxy J1 Ace*.

Pada implementasi studi kasus, penelitian ini mengeksplorasi kasus penipuan yang melibatkan dua akun, yaitu Akun A (Norah Nolan) sebagai korban dan Akun B (Garry Swihart) sebagai pelaku penipuan. Awalnya, Akun A bergabung dalam sebuah grup yang menawarkan barang-barang mewah, dan Akun B, sebagai anggota grup yang sama, menciptakan grup baru dengan tawaran yang lebih menjanjikan. Strategi pelaku melibatkan penciptaan daya tarik melalui profil yang meyakinkan dan postingan menarik, dengan tujuan memperoleh kepercayaan Akun A. Interaksi dimulai dengan undangan grup baru yang diterima oleh Akun A, yang tertarik dengan tawaran eksklusif. Akun B memberikan informasi palsu dan memposting barang palsu untuk memancing minat Akun A. Setelah berhasil menarik perhatian, Akun B memberikan informasi rekening transfer sebagai media pembayaran *online*, dan Akun A mengirim sejumlah dana. Pelaku kemudian menghilang dan tidak aktif lagi, meninggalkan Akun A sebagai korban dengan kerugian finansial. Studi kasus ini mengungkapkan taktik pelaku penipuan di media sosial dan menjadi dasar untuk pengembangan ontologi yang mencakup kategori-kategori khusus terkait penipuan *online*. Dengan menganalisis interaksi antara korban dan pelaku secara mendalam, penelitian ini bertujuan meningkatkan pemahaman terhadap skenario penipuan di platform media sosial.

3.2 Implementasi Studi Kasus



Gambar 3.1 Skema pelaksanaan studi kasus

Seperti yang disebutkan sebelumnya dan diilustrasikan pada Gambar 3.1:

1. Perangkat dan Akun

- Akun A (Korban – Fiktif):** Norah Nolan, karakter fiksi yang digambarkan sebagai pengguna media sosial biasa, menggunakan perangkat Android Samsung Galaxy J1 Ace sebagai sarana utamanya untuk mengakses dan terlibat dengan konten online.
- Akun B (Tersangka – Fiktif):** Garry Swihart, karakter fiksi lainnya yang digambarkan memiliki potensi aktivitas mencurigakan di media sosial, menggunakan perangkat Android Samsung Galaxy Mega 2 sebagai alat utamanya untuk interaksi digital.

- Interaksi dalam Platform Facebook:** Kontak awal terjadi ketika tersangka fiktif (Garry Swihart) mengajukan permintaan pertemanan kepada korban fiktif (Norah Nolan) di platform Facebook. Selanjutnya, ia menyampaikan undangan untuk bergabung dengan

grup bertajuk "Tas & Aksesori Bermerek", di mana ia menjabat sebagai administrator grup. Ini menandai dimulainya komunikasi mereka dalam ekosistem media sosial ini.

3. **Kasus:** Dalam grup Facebook "Tas & Aksesori Bermerek", tersangka fiktif (Garry Swihart) secara strategis memposting konten yang dirancang untuk menarik perhatian korban fiktif (Norah Nolan). Postingan ini bertujuan untuk membangkitkan minatnya, sehingga mengarah pada keterlibatan lebih lanjut melalui komentar. Interaksi awal dalam grup ini akhirnya berkembang menjadi pesan pribadi.
4. **Investigasi:** Menanggapi meningkatnya interaksi antara korban fiktif (Norah Nolan) dan tersangka fiktif (Garry Swihart) melalui pesan pribadi, penyidik memulai proses pengumpulan bukti. Hal ini melibatkan pengumpulan dan pelestarian semua komunikasi digital terkait dengan cermat, termasuk pesan teks, file multimedia, dan stempel waktu terkait. Investigasi ini bertujuan untuk menyusun garis waktu interaksi yang komprehensif, mengidentifikasi bukti potensial dari aktivitas terlarang, dan meneliti niat dan tindakan kedua pihak fiktif.

3.3 Tahapan Validasi dalam Implementasi Studi Kasus

Dalam pembahasan Implementasi Studi Kasus di atas peneliti menambahkan tahapan validasi terhadap kedua ontologi yang digunakan dalam penelitian ini. Untuk sisi klien menggunakan SSDDF dan untuk sisi server menggunakan SMONT. Tujuan dari tahapan ini adalah menemukan relevansi dari setiap ontologi dengan struktur data terbaru dari implementasi study kasus.

3.4 Kondisi dan Batasan Perangkat

Penelitian ini menggunakan dua smartphone Android Samsung yaitu **Samsung Galaxy Mega 2** dan **Samsung Galaxy J1 Ace**. Perangkat ini berbeda dalam spesifikasi perangkat lunak. **Samsung Galaxy Mega 2** berjalan pada Android versi 4.4.4 (KitKat), sedangkan **Samsung Galaxy J1 Ace** beroperasi pada Android versi 5.1.1 (Lollipop). Gambaran rinci tentang spesifikasi perangkat disajikan pada **Tabel 3.1**.

Tabel 3.1 Peta perangkat dan pengguna dalam studi kasus

Merek & Tipe	Kode	Versi Android	Nama belakang	Peran
Perangkat				
Samsung Galaksi Mega 2	luas3g	4.4.4 (Kitkat)	Norah Nolan	Korban
Samsung Galaxy J1 Ace	j1acevelte	5.1.1 (Lolipop)	Garry Swihart	Pelaku

Kondisi yang diamati untuk kedua perangkat:

- 1) untuk versi Android KitKat (digunakan korban): Aplikasi Facebook (**com.facebook.katana** atau **FB**) tidak tersedia di Play Store. Sebaliknya, Facebook Lite (**com.facebook.lite** atau **FBL**) berfungsi sebagai alternatif instalasi yang ringan,
- 2) untuk versi Android Lollipop (digunakan tersangka): Aplikasi Facebook tersedia di *Play Store* tanpa kendala yang ditemui, berbeda dengan versi Android sebelumnya.

3.5 Akuisisi Data

Setelah pelaksanaan studi kasus, perolehan data dilakukan dengan menggunakan metode sebagai berikut:

- 1) *rooting* kedua perangkat menggunakan **Magisk**, Magisk, serangkaian perangkat lunak sumber terbuka, digunakan untuk akses komprehensif ke data perangkat dan aplikasi hampir semua versi Android dengan lebih dari 260 kontributor dalam pengembangan proyek (*Download Magisk Manager Latest Version 26.3 For Android 2023*, n.d.; *GitHub - Topjohnwu/Magisk: The Magic Mask for Android*, n.d.). Rooting memungkinkan peningkatan hak istimewa, memungkinkan ekstraksi data bermakna yang mungkin tidak dapat diakses (Boueiz, 2020)
- 2) melakukan akuisisi kedua perangkat menggunakan metode **dd**, metode dd digunakan untuk membuat salinan penyimpanan perangkat sedikit demi sedikit, memastikan perolehan data yang luas [19], termasuk pesan teks, gambar, data aplikasi, dan file sistem
- 3) mentransfer data yang diperoleh dari shell **Android Debug Bridge (ADB)** ke komputer host menggunakan perintah **nc (Netcat)** yang diinstal oleh **Busybox**. Data yang diperoleh ditransfer dari shell ADB ke komputer host menggunakan perintah Netcat (nc) yang diinstal oleh Busybox. ADB, sebuah alat sumber terbuka, memungkinkan operasi baris perintah, termasuk menginstal dan melakukan debug aplikasi pada perangkat Android (*Android Debug Bridge (Adb) | Android Studio | Android Developers*, n.d.), alat umum seperti (Almehmadi & Batarfi, 2019; Boueiz, 2020; Lwin et al., n.d.). kotak sibuk (*BusyBox*, n.d.) digunakan untuk menginstal dan menjalankan perintah Netcat di kedua perangkat untuk operasi jaringan
- 4) hasil perolehan data yang ditransfer berbentuk file berekstensi **.dd**. Data yang ditransfer, dalam bentuk file '.dd', mewakili data yang diperoleh dalam format gambar disk mentah, ekstensi standar dalam forensik digital.

3.6 Tantangan dan Keterbatasan

Studi kasus ini mengungkapkan beberapa tantangan dan keterbatasan:

- 1) **Keterbatasan Data untuk FB dan FBL** , Salah satu tantangannya adalah terbatasnya cakupan data yang diperoleh dari Facebook (FB) dan Facebook Lite (FBL). Meskipun FB menyediakan data kontak dan media lokal sebagai bukti, FBL memiliki akses data yang lebih terbatas, hanya menawarkan data kontak.
- 2) **Penyertaan Messenger (FBM)** , Tantangan lainnya melibatkan integrasi aplikasi tambahan, Messenger (*com.facebook.orca* atau FBM). Mengekstraksi data mengenai pesan pribadi atau percakapan antara kedua akun menghadirkan tantangan meskipun Messenger menawarkan fungsi khusus untuk mengirim pesan antar pengguna FB.

Tantangan dan keterbatasan ini sangat mempengaruhi proses pengumpulan data dan harus dipertimbangkan ketika menafsirkan temuan penelitian. Tantangan dan keterbatasan tersebut menggaris bawahi kompleksitas dalam forensik digital dan perolehan data dari platform media sosial.

3.7 Pemetaan Ontologi

Pada tahapan ini, dilakukan pemetaan ontologi dengan mengintegrasikan Ontologi Small-Scale Digital Device Forensic (SSDDF) dan Social Media Ontology (SMOnt) ke dalam ontologi yang holistik. Proses ini diarahkan pada pembangunan hubungan antara konsep dan istilah dari kedua ontologi tersebut, dengan menggabungkannya dalam kelas yang lebih umum, yaitu **Thing**.

1. Penggabungan Ontologi.

Ontologi SSDDF dan SMOnt digabungkan langsung dalam kelas **Thing**. Integrasi ini bertujuan untuk menciptakan keselarasan yang menyeluruh, memungkinkan representasi ontologi yang lebih komprehensif terhadap bukti digital dari perangkat skala kecil dan data media sosial.

2. Penambahan Kelas pada SSDDF.

Untuk memperluas cakupan ontologi SSDDF, beberapa kelas tambahan ditambahkan dengan fokus pada struktur folder hasil akuisisi perangkat. Kelas-kelas ini mencakup entitas yang merepresentasikan struktur penyimpanan data, seperti **FolderPelaku** dan **FolderKorban**.

3. Penambahan Kelas pada SMOnt.

Ontologi SMOnt diperkaya dengan menambahkan kelas-kelas yang mencerminkan kategori data pada hasil unduhan berkas data pribadi dari akun pelaku dan korban, terutama yang berformat **.json**. Kelas-kelas ini mencakup entitas seperti **DataPribadiPelaku** dan **DataPribadiKorban**.

4. Langkah Pemetaan

Langkah-langkah pemetaan melibatkan identifikasi konsep kunci dari data yang diperoleh, seperti struktur folder, kategori data, spesifikasi perangkat, dan bukti digital lainnya. Selanjutnya, dilakukan pembuatan kelas dan properti yang sesuai dalam ontologi gabungan, mengaitkan kelas dan properti dengan konsep yang setara atau terkait dalam data yang diperoleh.

5. Manfaat Pemetaan Ontologi.

Pemetaan ontologi memungkinkan analisis forensik digital, memungkinkan penyelidik untuk menavigasi dan memahami struktur data kompleks dari perangkat digital dan data media sosial. Integrasi ontologi SSDDF dan SMOnt memberikan kerangka kerja yang kuat untuk analisis kontekstual bukti digital dari dua sisi, memfasilitasi pemahaman menyeluruh terhadap interaksi yang terjadi pada perangkat Android dalam skenario penelitian ini.

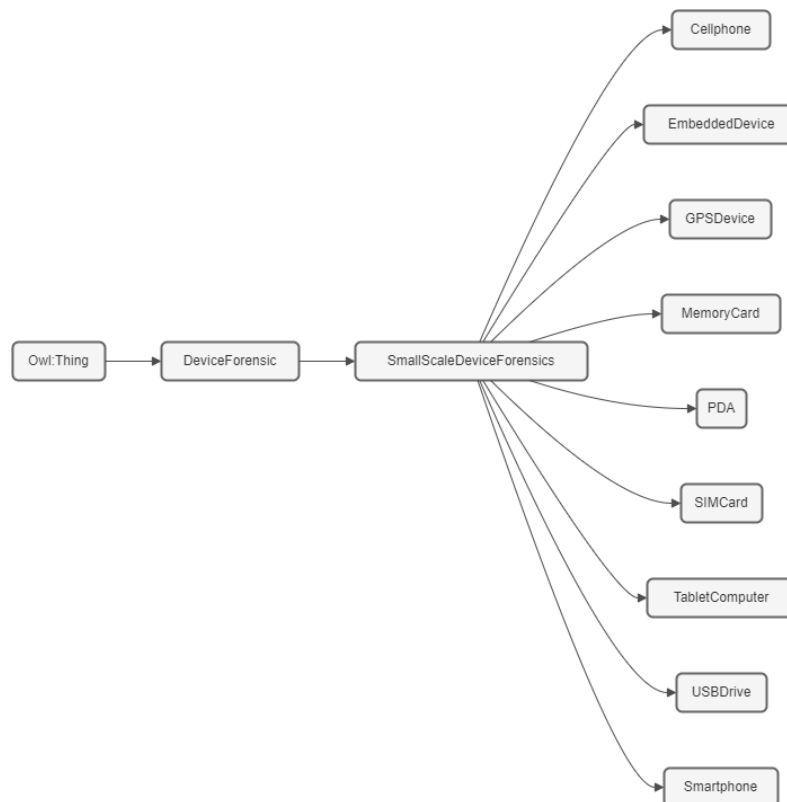
Langkah-langkah dan prinsip-prinsip ini menjadi pedoman dalam menyusun ontologi gabungan yang dapat mendukung investigasi forensik digital.

BAB 4

Hasil dan Pembahasan

4.1 Penerapan Praktis Ontologi SSDDF

Ontologi *Small-Scale Digital Device Forensics (SSDDF)*, digambarkan pada **Gambar 4.1**, memainkan peran sentral dalam mengkategorikan dan mengatur bukti digital dari perangkat digital skala kecil. Ontologi ini berfungsi sebagai landasan untuk mengeksplorasi investigasi forensik digital pada perangkat seperti *smartphone*, *memory card*, dan *embedded device*.



Gambar 4.1 Ontologi SSDDF

Pada bagian ini, kami mengilustrasikan kegunaan praktis dari ontologi SSDDF dalam investigasi forensik digital dunia nyata. Ontologi SSDDF berfungsi sebagai alat yang berharga bagi lembaga penegak hukum dan ahli forensik, meningkatkan kemampuan mereka dengan cara berikut:

- 1) Analisis Data: Ontologi SSDDF menawarkan kerangka kerja terstruktur untuk mengatur dan menggolongkan bukti digital dari perangkat digital berskala kecil. Kelas dan hubungannya yang telah ditentukan sebelumnya memfasilitasi analisis data, memungkinkan penyelidik memperoleh wawasan lebih cepat.
- 2) Korelasi Lintas Perangkat: Dalam investigasi multi-perangkat, ontologi SSDDF memungkinkan korelasi data dari berbagai sumber. Hal ini memungkinkan penyelidik

untuk menghubungkan bukti dari ponsel pintar, kartu memori, dan perangkat yang tertanam, sehingga dapat merekonstruksi garis waktu kejadian secara komprehensif.

- 3) Pengambilan Data yang Ditingkatkan: Dengan kelas dan properti yang terdefinisi dengan baik, ontologi SSDDF menyederhanakan pengambilan data. Penyidik dapat dengan cepat menemukan informasi yang relevan, seperti riwayat obrolan, file media, atau profil pengguna, sehingga menghasilkan penyelesaian kasus.
- 4) Integrasi dengan Alat yang Ada: Ontologi SSDDF dirancang untuk diintegrasikan secara mulus dengan alat dan perangkat lunak forensik digital yang ada. Integrasi ini meningkatkan aksesibilitas bagi para ahli forensik, menyederhanakan proses investigasi tanpa memerlukan pelatihan ulang yang ekstensif.

4.2 Pengembangan Ontologi SSDDF

Dalam pengembangan ontologi SSDDF, eksplorasi difokuskan pada blok penyimpanan sistem Android, khususnya mmcblk0 untuk penyimpanan internal dan mmcblk1 untuk penyimpanan eksternal. **Gambar 4.2** mengilustrasikan blok-blok tersebut pada perangkat Samsung Galaxy J1 Ace.

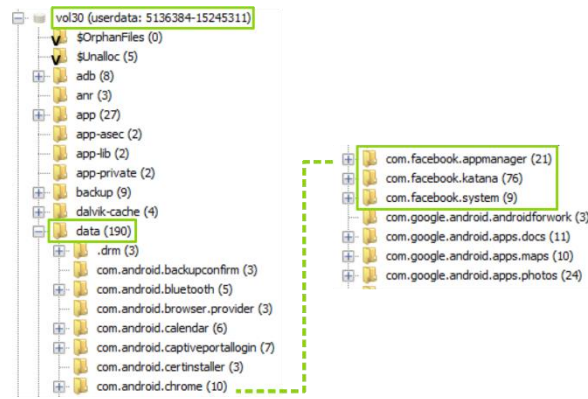
```

root@jlacevelte: / # cd /dev/block/
root@jlacevelte: /dev/block # ls
loop0      mmcblk0boot1  mmcblk0p18    mmcblk0p27    mmcblk1p1
loop1      mmcblk0p1     mmcblk0p19    mmcblk0p3     param
loop2      mmcblk0p10    mmcblk0p2     mmcblk0p4     persistent
loop3      mmcblk0p11    mmcblk0p20    mmcblk0p5     platform
loop4      mmcblk0p12    mmcblk0p21    mmcblk0p6     vswap0
loop5      mmcblk0p13    mmcblk0p22    mmcblk0p7     vold
loop6      mmcblk0p14    mmcblk0p23    mmcblk0p8
loop7      mmcblk0p15    mmcblk0p24    mmcblk0p9
mmcblk0    mmcblk0p16    mmcblk0p25    mmcblk0rpm
mmcblk0boot0 mmcblk0p17    mmcblk0p26    mmcblk1
root@jlacevelte: /dev/block #

```

Gambar 4.2 Blok penyimpanan internal (**mmcblk0**) dan penyimpanan eksternal (**mmcblk1**) pada perangkat **Samsung Galaxy J1 Ace**

Dalam partisi data pengguna penyimpanan internal, yang mencakup folder "data", "media", dan "sistem", penyelidikan mencari temuan terkait aplikasi Facebook (FB, FBL, dan FBM). **Gambar 4.3** menyajikan struktur partisi data pengguna dan daftar paket aplikasi Facebook.



Gambar 4.3 Struktur partisi data pengguna dan daftar paket aplikasi Facebook

Berdasarkan struktur folder dan file, ditemukan banyak data terkait aktivitas kedua akun. Tabel 2 menguraikan beberapa temuan utama bukti digital yang diperoleh dari implementasi studi kasus.

Tabel 4.1 Temuan bukti digital

Kode Aplikasi	Mengajukan	Jalur File	Keterangan
Samsung Galaxy Mega 2 (luas3g)			
com.facebook. lite	fblite_databas e.db	/vol_vol30/data/com.faceboo k.lite/databases/fblite_databa se.db	Basis data ini berisi data penting dari Facebook Lite, termasuk profil pengguna, pesan, dan log aktivitas.
com.facebook .orca	msys_databas e_100090534 141448	/vol_vol30/data/com.faceboo k.orca/databases/msys_datab ase_100090534141448	Basis data sistem Messenger, yang menyimpan riwayat obrolan, lampiran, dan informasi kontak.
Samsung Galaxy J1 Ace (j1acevelte)			
com.facebook. katana	app_uploads	/vol_vol30/data/com.faceboo k.katana/app_uploads	Direktori tempat aplikasi Facebook mengunggah file media, termasuk foto dan video yang dibagikan oleh pengguna.
com.facebook. katana	kontak_db2	/vol_vol30/data/com.faceboo k.katana/databases/contacts_ db2	Basis data yang menyimpan informasi kontak dari aplikasi Facebook, membantu pelacakan kontak dan analisis koneksi.

com.facebook.katana	lokal_media_db	/vol_vol30/data/com.facebook.k.katana/databases/local_media_db	Basis data ini menampung file media yang disimpan secara lokal dan dibagikan di Facebook, yang menawarkan wawasan tentang preferensi media pengguna.
com.facebook.katana	autentikasi	/vol_vol30/data/com.facebook.k.katana/app_light_prefs/com.facebook.katana/authentication	Data preferensi autentikasi, penting untuk memahami pola login pengguna dan langkah-langkah keamanan sistem
system	accounts.db	/vol _vol30/system/users/0/akun.db	Basis data akun tingkat sistem yang menyimpan informasi tentang akun pengguna di perangkat.

Dari temuan ini, jelas bahwa ontologi SSDDF memerlukan kelas terstruktur tambahan untuk memetakan data yang ditemukan. Kompleksitas struktur data yang ada dalam perangkat menimbulkan pertanyaan kompetensi: *"Bagaimana memetakan ontologi Forensik Perangkat Digital Skala Kecil?"* Pertanyaan ini membentuk asumsi awal mengingat sifat rumit dari struktur data di dalam perangkat.

Kehadiran blok penyimpanan (**mmcblk0** dan **mmcblk1**) menunjukkan bahwa fokus utama eksplorasi harus pada penyimpanan internal, dengan penyimpanan eksternal sebagai pilihan. Dalam penyimpanan internal, folder data, media, dan sistem menunjukkan perlunya kelas terpisah untuk memetakan direktori ini untuk identifikasi dan kategorisasi yang lebih jelas.

Dari hasil temuan maka di validasi bahwa ontologi yang sudah ada masih belum memenuhi struktur yang ditemukan dalam studi kasus. Oleh karena itu, pertanyaan kompetensi dapat disempurnakan menjadi sub-pertanyaan berikut:

1) Bagaimana cara memetakan berdasarkan sifat penyimpanan Internal dan Eksternal?

Justifikasi: Membedakan antara elemen penyimpanan internal dan eksternal sangat penting untuk kategorisasi data yang tepat. Diferensiasi ini membantu peneliti dalam memfokuskan analisis mereka pada sumber data yang relevan dan memastikan bahwa ontologi secara akurat mencerminkan sifat media penyimpanan.

2) Bagaimana cara memetakan struktur penting yang ada di penyimpanan internal?

Justifikasi: Penyimpanan internal berisi berbagai struktur penting (misalnya data, media, sistem) yang memerlukan pemetaan terpisah. Struktur ini adalah kunci untuk mengatur dan mengkategorikan bukti digital.

3) *Bagaimana cara memetakan struktur yang ada di penyimpanan eksternal?*

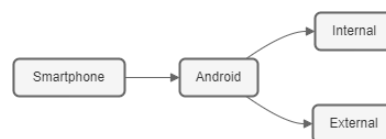
Justifikasi: Meskipun fokus utamanya adalah pada penyimpanan internal, penyimpanan eksternal tetap menjadi sumber bukti digital yang potensial. Memasukkan kelas untuk memetakan penyimpanan eksternal memastikan penyelidik dapat memperhitungkan dan menganalisis data yang disimpan di media yang dapat dipindahkan bila relevan.

Dengan menawarkan pembenaran ini, tujuan kami adalah untuk menjelaskan alasan dibalik pemilihan dan penggabungan kelas dan properti tertentu ke dalam ontologi SSDDF. Penambahan ini dirancang khusus untuk menyelaraskan dengan kebutuhan praktis analisis forensik digital dan menyederhanakan investigasi.

4.3 Implementasi Pertanyaan Kompetensi

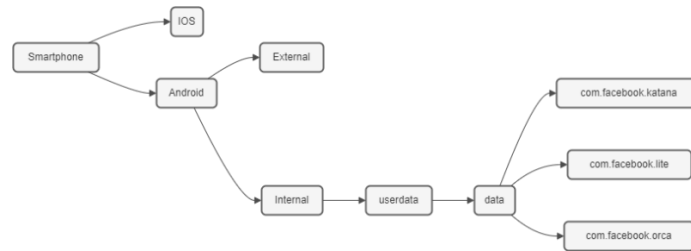
Pertanyaan kompetensi memainkan peran penting dalam membentuk ontologi SSDDF. Mereka memandu proses pengembangan untuk memastikan ontologi menjawab kebutuhan analisis forensik perangkat digital. Struktur kelas asli berfungsi sebagai landasan, dengan struktur kelas tambahan dibuat berdasarkan pertanyaan kompetensi untuk meningkatkan relevansi dan kegunaan.

Untuk pertanyaan kompetensi pertama **"Bagaimana cara memetakan berdasarkan sifat penyimpanan Internal dan Eksternal?"**, Gambar 5 memberikan representasi visual kelas tambahan untuk penyimpanan internal dan eksternal.



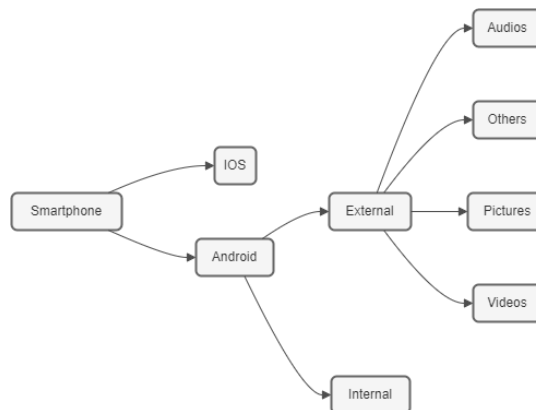
Gambar 4.4 Penambahan kelas pada soal kompetensi pertama pada ontologi SSDDF

Untuk pertanyaan kompetensi kedua **"Bagaimana memetakan struktur penting yang ada di penyimpanan internal?"**, Gambar 4.5 mengilustrasikan kelas yang ditambahkan.



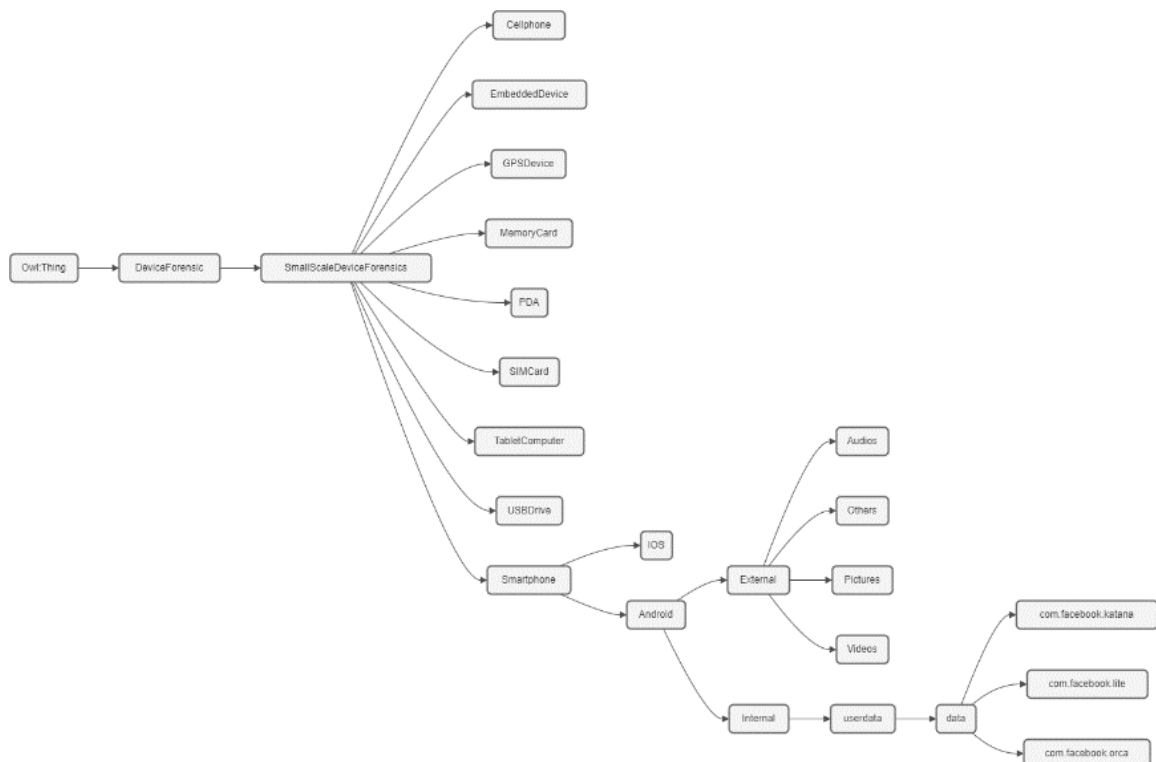
Gambar 4.5 Penambahan kelas pada soal kompetensi kedua pada ontologi SSDDF

Untuk pertanyaan kompetensi ketiga "**Bagaimana memetakan struktur yang ada di penyimpanan eksternal?**", **Gambar 4.6** menampilkan kelas yang ditambahkan.



Gambar 4.6 Penambahan kelas pada soal kompetensi ketiga pada ontologi SSDDF

Ontologi SSDDF lengkap hasil implementasi soal kompetensi divisualisasikan pada **Gambar 4.7**.

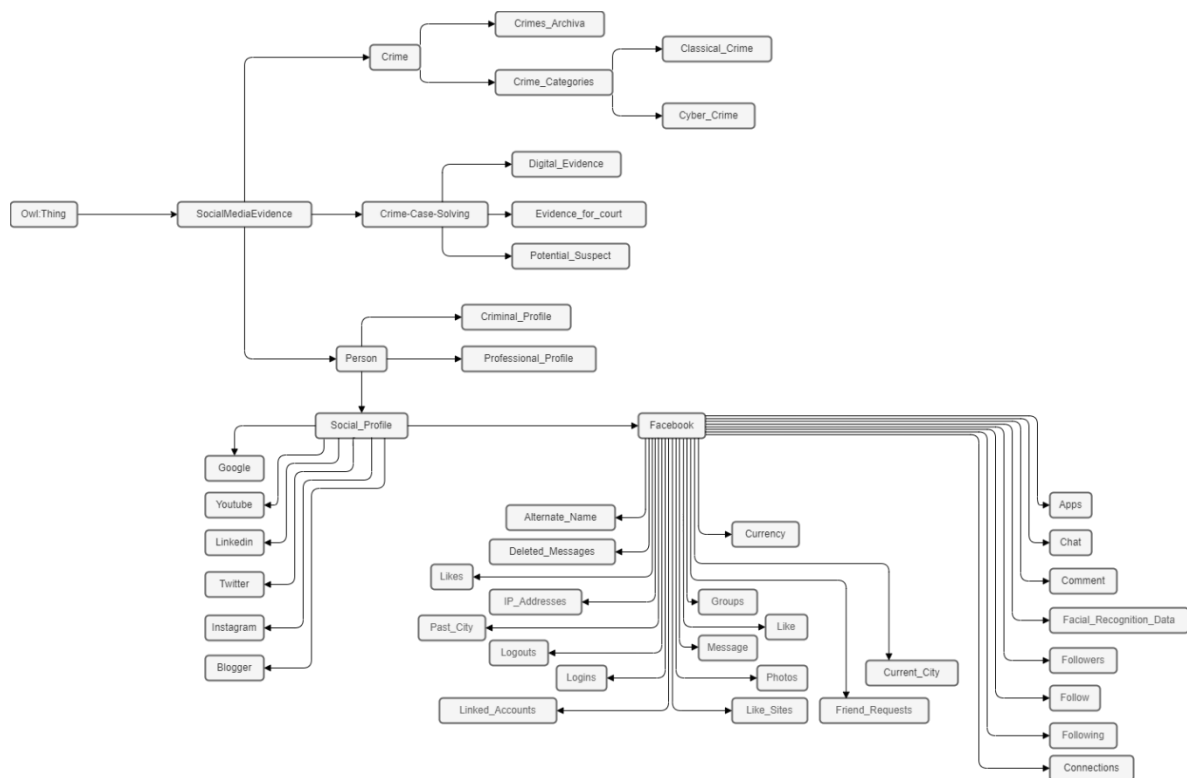


Gambar 4.7 Ontologi SSDDF

Integrasi dengan ontologi yang ada, seperti ontologi Bukti Media Sosial, berkontribusi pada pendekatan holistik terhadap analisis forensik perangkat digital. Ontologi SSDDF menyatu secara mulus dengan ontologi Bukti Media Sosial yang sudah ada, sehingga menciptakan kerangka pengetahuan terpadu. Integrasi ini memanfaatkan kekuatan kedua ontologi, dengan SSDDF yang berfokus pada penataan data forensik perangkat digital dan Bukti Media Sosial yang berspesialisasi dalam menangkap metadata dan informasi kontekstual dari platform media sosial.

4.4 Penerapan Praktis Ontologi Social Media Evidence (SMOnt)

Ontologi *Social Media Ontology (SMOnt)*, digambarkan pada Gambar 3, memainkan peran sentral dalam mengkategorikan dan mengatur bukti digital dari penyedia layanan (server). Ontologi ini berfungsi sebagai landasan untuk mengeksplorasi investigasi forensik digital pada domain khususnya platform *Facebook*.



Gambar 4.8 Ontologi SMOnt

Pada bagian ini, kami mengilustrasikan kegunaan praktis dari ontologi SMOnt dalam investigasi forensik digital dunia nyata. Ontologi SSDDF berfungsi sebagai alat yang berharga bagi lembaga penegak hukum dan ahli forensik, meningkatkan kemampuan mereka dengan cara berikut:

- 1) Analisis Bukti Digital dari Media Sosial: SMOnt dapat digunakan untuk mengorganisir dan menganalisis bukti digital yang ditemukan di platform media sosial. Ini melibatkan

identifikasi, kategorisasi, dan hubungan antar berbagai entitas seperti profil pengguna, aktivitas, dan pesan.

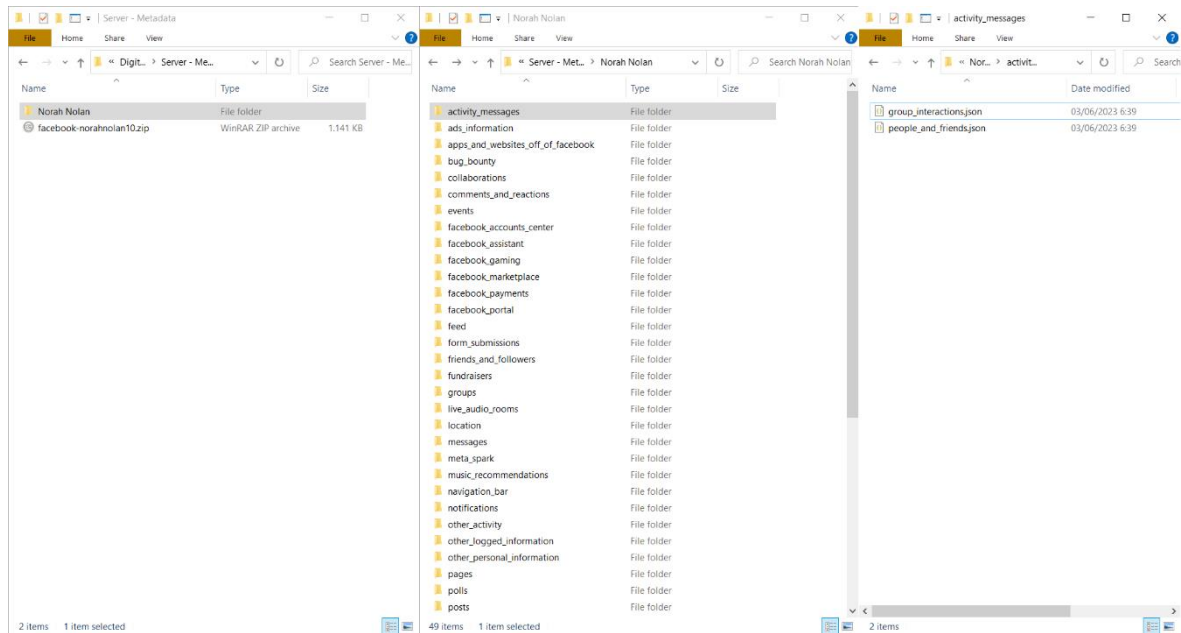
- 2) Rekonstruksi Kejadian dan Interaksi: Dengan memanfaatkan SMOnt, forensik digital dapat merekonstruksi kejadian dan interaksi yang terjadi di media sosial. Ini termasuk memahami hubungan antar pengguna, aktivitas yang dilakukan, serta evolusi kejadian seiring waktu.
- 3) Penelusuran Kejahatan Digital dan Identifikasi Pelaku: SMOnt dapat membantu dalam penelusuran kejahatan digital dengan menyajikan bukti-bukti terkait kejahatan, mengidentifikasi pelaku, dan memahami metode yang digunakan oleh pelaku kejahatan dalam lingkungan media sosial.
- 4) Pengumpulan dan Integrasi Bukti dari Berbagai Sumber: Ontologi dapat membantu dalam pengumpulan dan integrasi bukti digital dari berbagai sumber media sosial. Ini termasuk data dari platform seperti Facebook, Twitter, Instagram, dan lainnya, sehingga menyediakan pandangan yang holistik.
- 5) Pendukung Penyidikan Hukum: SMOnt dapat digunakan sebagai alat pendukung penyidikan hukum dengan menyediakan struktur yang jelas untuk menyajikan bukti-bukti digital di pengadilan. Ini membantu dalam mengkomunikasikan temuan forensik dengan lebih sistematis.
- 6) Analisis Tren dan Pola Perilaku: Dengan menggunakan ontologi, analis forensik dapat melakukan analisis tren dan pola perilaku di media sosial. Ini termasuk memahami bagaimana individu atau kelompok berinteraksi dan berkomunikasi di platform tersebut.
- 7) Keamanan dan Pencegahan Kejahatan: SMOnt dapat mendukung langkah-langkah keamanan dengan memahami pola perilaku yang mungkin menandakan ancaman atau kegiatan ilegal di media sosial. Ini dapat membantu dalam pencegahan kejahatan lebih lanjut.
- 8) Pelatihan dan Pengembangan Kapabilitas Forensik: Ontologi dapat digunakan sebagai dasar untuk melatih analis forensik digital dan mengembangkan kapabilitas dalam memahami serta menangani bukti digital dari media sosial.

Penerapan praktis ini memberikan pandangan lebih dalam dan terstruktur terhadap kejadian di dunia media sosial, yang dapat mendukung penyelidikan, analisis forensik, dan tindakan keamanan. Penting untuk terus mengembangkan dan memperbarui ontologi sesuai dengan perubahan dalam platform media sosial dan tren kejahatan digital.

4.5 Pengembangan Ontologi Social Media Evidence (SMOnt)

Dalam pengembangan ontologi SMOnt, eksplorasi difokuskan pada metadata yang diakuisisi dari kedua akun pelaku dan korban menggunakan fitur “Unduh Data Pribadi” pada masing-masing akun.

Dari metadata yang diakuisisi pada kedua akun, sejumlah data dikategorikan dalam bentuk Folder dan berkas JSON. Dari seluruh folder yang ada, beberapa data tidak memiliki representasi kelas dalam ontology yang sudah ada.



Gambar 4.9 Contoh berkas data pribadi dari penyedia layanan (Server)

Temuan barang bukti dalam sisi server bisa dijabarkan sebagai berikut:

Tabel 4.2 Temuan barang bukti digital dari sisi server.

No	Nama Berkas	Nama Folder	Deskripsi
Norah Nolan (Korban)			
1	<i>group_interactions.json,</i> <i>people_and_friends.json</i>	<i>activity_messages</i>	Berisi metadata terkait interaksi di dalam Group dan akun lain. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 3 .
	<i>likes_and_reactions_1.json</i>	<i>comments_and_reactions</i>	Berisi daftar aktifitas Like pada akun.

	<i>your_friends.json</i>	<i>friends_and_followers</i>	Berisi metadata daftar akun teman.
	<i>your_comments_in_groups.json,</i> <i>your_contributions.json,</i> <i>your_group_membership_activity.json</i>	<i>groups</i>	Berisi metadata aktifitas dalam Group dimana akun tergabung.
	<i>device_location.json,</i> <i>primary_location.json,</i> <i>timezone.json</i>	<i>location</i>	Berisi metadata berkaitan dengan lokasi perangkat yang digunakan. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 4.
	<i>photos/341908888_263920606074157_8665723289328886533_n_263920599407491.jpg,</i> <i>photos/341925658_774604704194071_262001010521499161_n_774604700860738.jpg,</i> <i>photos/341931857_917589472631686_4171382839539476541_n_917589465965020.jpg,</i> <i>photos/343264468_262189196343280_2796060366579876393_n_262189193009947.jpg,</i> <i>photos/343932198_228727459845524_7458925843766544275_n_228727453178858.jpg,</i> <i>photos/343975509_920775105876782_4298509330563293551_n_920775102543449.jpg,</i> <i>message_1.json</i>	<i>messages/inbox/garrys wihart_149101114772495</i>	Berisi metadata untuk seluruh percakapan pada akun korban kepada akun pelaku.
	<i>notifications.json</i>	<i>notifications</i>	Berisi metadata notifikasi yang ada dalam akun. Isi metadata untuk kelas ini berdasarkan implementasi

			studi kasus bisa dilihat pada LAMPIRAN 5.
	<i>album/0.json,</i> <i>media/Profilepictures_K8aW16J</i> <i>TaA/341876194_717996013438</i> <i>176_7356421892100952360_n_</i> <i>140686952292442.jpg,</i> <i>media/Profilepictures_K8aW16J</i> <i>TaA/342036025_182154067992</i> <i>929_9019974005907382537_n_</i> <i>140686645625806.jpg,</i> <i>photo_effects.json,</i> <i>your_posts_1.json</i>	<i>posts</i>	Berisi metadata terkait dengan postingan.
	<i>your_search_history.json</i>	<i>search</i>	Berisi metadata informasi profil akun. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 6.
	<i>account_activity.json,</i> <i>browser_cookies.json,</i> <i>email_address_verifications.jso</i> <i>n,</i> <i>ip_address_activity.json,</i> <i>login_protection_data.json,</i> <i>logins_and_logouts.json,</i> <i>mobile_devices.json,</i> <i>record_details.json,</i> <i>where_you're_logged_in.json,</i> <i>your_facebook_activity_history.j</i> <i>son</i>	<i>security_and_login_in</i> <i>formation</i>	Berisi metadata riwayat pencarian.
	<i>recently_viewed.json,</i> <i>recently_visited.json</i>	<i>your_interactions_on_</i> <i>facebook</i>	Berisi metadata aktivitas umum pada akun.
Garry Swihart (Pelaku)			
2	<i>group_interactions.json,</i> <i>people_and_friends.json</i>	<i>activity_messages</i>	Berisi metadata terkait interaksi di dalam Group dan

			akun lain. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 3.
	<i>your_friends.json</i>	<i>friends_and_followers</i>	Berisi metadata daftar akun teman.
	<i>group_posts_and_comments.json,</i> <i>your_badges.json,</i> <i>your_comments_in_groups.json,</i> <i>your_contributions.json,</i> <i>your_group_membership_activity.json,</i> <i>your_groups.json</i>	<i>groups</i>	Berisi metadata aktifitas dalam Group dimana akun tergabung.
	<i>device_location.json,</i> <i>primary_location.json,</i> <i>timezone.json</i>	<i>location</i>	Berisi metadata berkaitan dengan lokasi perangkat yang digunakan. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 4.
	<i>photos/341908888_263920606074157_8665723289328886533_n_263920599407491.jpg,</i> <i>photos/341925658_774604704194071_262001010521499161_n_774604700860738.jpg,</i> <i>photos/341931857_917589472631686_4171382839539476541_n_917589465965020.jpg,</i> <i>photos/343264468_262189196343280_2796060366579876393_n_262189193009947.jpg,</i>	<i>messages/inbox/norah nolan_149101114772495</i>	Berisi metadata untuk seluruh percakapan pada akun pelaku kepada akun korban.

	<p><i>photos/343932198_228727459845524_7458925843766544275_n_228727453178858.jpg,</i></p> <p><i>photos/343975509_920775105876782_4298509330563293551_n_920775102543449.jpg,</i></p> <p><i>message_1.json</i></p>		
	<i>notifications.json</i>	<i>notifications</i>	Berisi metadata notifikasi yang ada dalam akun. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 5 .
	<p><i>album/0.json,</i></p> <p><i>media/Profilepictures_BfqvV-dp9g/341502178_621608466384388_3570839881280430957_n_143690311980242.jpg,</i></p> <p><i>media/your_posts/342806956_164357476258211_838988183220333483_n_149085934774013.jpg,</i></p> <p><i>media/your_posts/343214792_770564751118270_8904959228994077209_n_149089061440367.jpg,</i></p> <p><i>media/your_posts/343215435_1307373346842489_4987611659705133777_n_149088998107040.jpg,</i></p> <p><i>media/your_posts/343217795_195558869944921_3359819746399149962_n_149090008106939.jpg,</i></p> <p><i>media/your_posts/343221958_1192847264763121_3272801911</i></p>	<i>posts</i>	Berisi metadata terkait dengan postingan.

383521207_n_14909119144015 4.jpg, media/your_posts/343327436_6 19428329706034_65067472845 93569827_n_149074011441872 .jpg, media/your_posts/343379763_9 26480881885150_11298856292 75696714_n_149088901440383 .jpg, media/your_posts/343427986_5 80714444125474_40925311226 74333516_n_149088934773713 .jpg, media/your_posts/343640356_6 28495558698252_39262569784 42302466_n_149091778106762 .jpg, your_posts_1.json, your_uncategorized_photos.json		
profile_information.json, profile_update_history.json	profile_information	Berisi metadata informasi profil akun.
your_search_history.json	search	Berisi metadata riwayat pencarian. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada LAMPIRAN 6.
account_activity.json, browser_cookies.json, email_address_verifications.json, ip_address_activity.json, login_protection_data.json, logins_and_logouts.json, mobile_devices.json,	security_and_login_information	Berisi metadata aktivitas umum pada akun.

	<i>recognized_devices.json,</i> <i>record_details.json,</i> <i>where_you're_logged_in.json,</i> <i>your_facebook_activity_history.j</i> <i>son</i>		
	<i>recently_visited.json</i>	<i>your_interactions_on_</i> <i>facebook</i>	Berisi metadata aktifitas akun.

Berdasarkan hasil temuan pada studi kasus yang melibatkan akun **Norah Nolan** (Korban) dan **Garry Swihart** (Pelaku) pada sisi server, ditemukan beberapa kelas yang belum tercakup dalam ontologi yang sudah ada. Hasil temuan ini mencakup berbagai aspek metadata yang terkait dengan interaksi di dalam grup, aktivitas teman, postingan, percakapan, notifikasi, riwayat pencarian, informasi keamanan dan login, serta aktivitas umum pada akun.

Penambahan kelas-kelas ini diperlukan untuk memperluas cakupan ontologi dan mengakomodasi aspek-aspek spesifik yang muncul dalam hasil temuan. Dengan demikian, dapat disimpulkan bahwa ontologi yang ada perlu dikembangkan lebih lanjut dengan menambahkan kelas-kelas seperti **Activity_Messages**, **Location**, **Notifications**, **Search**.

Selain itu, hasil temuan juga menunjukkan adanya kebutuhan untuk menambahkan kelas-kelas baru yang mencerminkan fitur-fitur khusus dari Facebook, seperti **Bug_Bounty**, **Facebook_Assistant**, **Facebook_Accounts_Center**, **Facebook_Marketplace**, **Facebook_Payments**, **Facebook_Portal**, dan sebagainya. Penambahan kelas-kelas ini akan memberikan representasi yang lebih komprehensif terhadap fitur-fitur spesifik yang ada dalam konteks forensik digital.

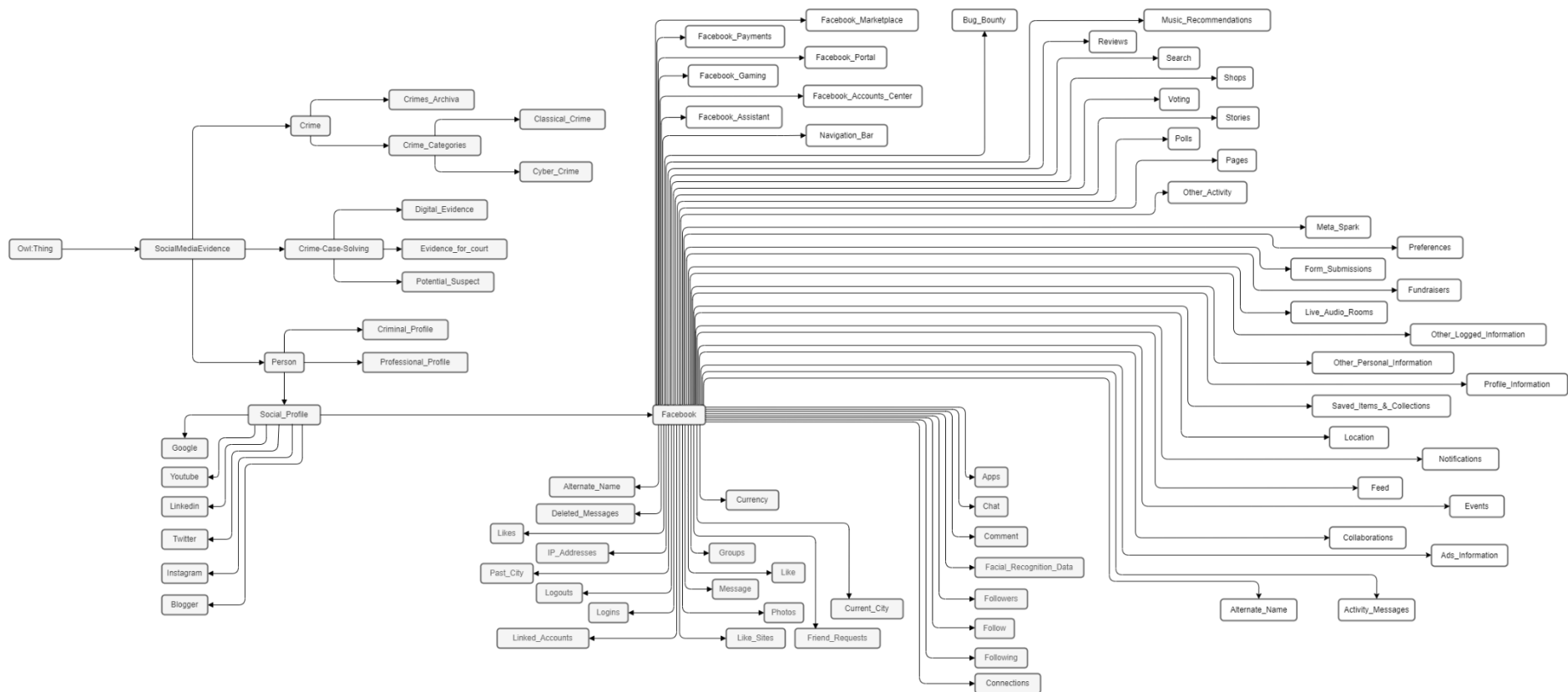
Penjelasan lebih lengkap untuk setiap kelas yang ditambahkan dapat dijelaskan sebagai berikut:

1. **Activity_Messages:** Merepresentasikan pesan atau komunikasi yang terkait dengan aktivitas pengguna di platform. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada **LAMPIRAN 3**.
2. **Location:** Merepresentasikan informasi lokasi yang terkait dengan aktivitas pengguna. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada **LAMPIRAN 4**.

3. **Notifications:** Merepresentasikan notifikasi yang diterima atau dibuat oleh pengguna. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada **LAMPIRAN 5**.
4. **Search:** Merepresentasikan aktivitas pencarian yang dilakukan oleh pengguna di platform. Isi metadata untuk kelas ini berdasarkan implementasi studi kasus bisa dilihat pada **LAMPIRAN 6**.
5. **Bug_Bounty:** Merepresentasikan informasi terkait program *bug bounty* di Facebook, termasuk laporan bug dan imbalan yang mungkin terkait.
 - *Laporan_Bug:* Menyimpan detail laporan bug yang diajukan, termasuk informasi tentang kerentanan atau kelemahan yang dilaporkan.
 - *Imbalan:* Menyimpan informasi tentang imbalan yang diberikan sebagai penghargaan atas laporan bug yang valid.
6. **Facebook_Assistant:** Merepresentasikan interaksi dengan asisten virtual di Facebook, seperti chatbot atau fitur bantuan otomatis.
 - *Jenis_Assistant:* Menyimpan informasi tentang jenis asisten virtual yang terlibat.
 - *Riwayat_Interaksi:* Menyimpan log interaksi dengan asisten virtual.
7. **Facebook_Accounts_Center:** Merepresentasikan fitur terkait manajemen akun di Facebook, seperti pengaturan keamanan atau perubahan informasi profil.
 - *Pengaturan_Keamanan:* Menyimpan informasi tentang pengaturan keamanan akun.
 - *Perubahan_Profil:* Menyimpan catatan tentang perubahan informasi profil.
8. **Facebook_Marketplace:** Merepresentasikan interaksi dan aktivitas di Marketplace Facebook, termasuk penjualan, pembelian, atau pertukaran barang.
 - *Produk:* Menyimpan informasi produk yang dijual atau dibeli.
 - *Transaksi:* Menyimpan detail tentang transaksi yang terjadi di Marketplace.
9. **Facebook_Payments:** Merepresentasikan informasi terkait pembayaran yang dilakukan di Facebook, termasuk metode pembayaran dan riwayat transaksi.
 - *Metode_Pembayaran:* Menyimpan informasi tentang metode pembayaran yang digunakan.
 - *Riwayat_Transaksi:* Menyimpan catatan transaksi keuangan.

10. **Facebook_Portal:** Merepresentasikan interaksi dan fitur terkait dengan perangkat Facebook Portal, seperti panggilan video atau penggunaan fitur kamera.
 - *Aktivitas_Portal:* Menyimpan log aktivitas terkait penggunaan Portal.
11. **Facebook_Gaming:** Merepresentasikan aktivitas dan interaksi dalam platform gaming di Facebook, termasuk permainan dan interaksi komunitas gaming.
 - *Permainan:* Menyimpan informasi tentang permainan yang dimainkan.
 - *Komunitas_Gaming:* Menyimpan interaksi dalam komunitas gaming.
12. **Form_Submissions:** Merepresentasikan data terkait dengan pengisian formulir atau formulir yang diajukan di platform Facebook.
 - *Formulir:* Menyimpan informasi tentang formulir yang diisi atau diajukan.
 - *Data_Submission:* Menyimpan data yang diajukan melalui formulir.
13. **Fundraisers:** Merepresentasikan informasi terkait penggalangan dana atau kampanye amal di Facebook.
 - *Kampanye:* Menyimpan informasi tentang kampanye penggalangan dana.
 - *Kontribusi:* Menyimpan data kontribusi dan sumbangan.
14. **Live_Audio_Rooms:** Merepresentasikan aktivitas dan interaksi dalam fitur Live Audio Rooms di Facebook.
 - *Percakapan_Audio:* Menyimpan log percakapan audio yang terjadi di Live Audio Rooms.
15. **Navigation_Bar:** Merepresentasikan informasi terkait dengan navigasi dalam antarmuka pengguna Facebook.
16. **Meta_Spark:** Merepresentasikan aktivitas atau entitas terkait Meta Spark di Facebook.
17. **Preferences:** Merepresentasikan preferensi atau pengaturan yang dikonfigurasi oleh pengguna di platform Facebook.
18. **Other_Activity:** Merepresentasikan aktivitas lain yang tidak termasuk dalam kategori kelas tertentu.
19. **Music_Recommendations:** Merepresentasikan rekomendasi musik yang diberikan atau dihasilkan oleh platform Facebook.

20. **Other_Logged_Information:** Merepresentasikan informasi log atau data lain yang tidak termasuk dalam kategori kelas tertentu.
21. **Other_Personal_Information:** Merepresentasikan informasi pribadi lain yang tidak termasuk dalam kategori kelas tertentu.
22. **Profile_Information:** Merepresentasikan informasi profil pengguna di Facebook.
23. **Saved_Items_&_Collections:** Merepresentasikan barang atau koleksi yang disimpan oleh pengguna di platform.
24. **Shops:** Merepresentasikan informasi terkait toko atau tempat berbelanja di Facebook.
25. **Reviews:** Merepresentasikan ulasan atau penilaian yang diberikan oleh pengguna.
26. **Voting:** Merepresentasikan aktivitas pemungutan suara atau voting yang dilakukan di platform.
27. **Stories:** Merepresentasikan cerita atau konten berbasis cerita yang dibagikan oleh pengguna.
28. **Polls:** Merepresentasikan jajak pendapat atau survei yang dilakukan oleh pengguna.
29. **Pages:** Merepresentasikan halaman atau profil khusus yang dibuat di Facebook.
30. **Feed:** Merepresentasikan aktivitas atau konten yang muncul di feed atau beranda pengguna.
31. **Events:** Merepresentasikan acara atau kegiatan yang diikuti atau dibuat oleh pengguna.
32. **Collaborations:** Merepresentasikan kolaborasi atau kerjasama antara pengguna di platform.
33. **Ads_Information:** Merepresentasikan informasi terkait dengan iklan yang dilihat atau diinteraksi oleh pengguna.



Gambar 4.10 Ontologi SMOnt

4.6 Keseluruhan Ontologi

Integrasi metodologis melibatkan pemetaan kelas dan properti yang relevan dari setiap ontologi untuk memastikan kompatibilitas dan interoperabilitas data. Meskipun ada tantangan seperti menyelaraskan perbedaan dalam definisi kelas dan menangani properti yang tumpang tindih, manfaatnya jauh lebih besar daripada tantangan tersebut. Gambar 9 memberikan gambaran ontologi terintegrasi yang dihasilkan.

4.7 Struktur Kelas

Ontologi terdiri dari dua kelas utama: DeviceForensic dan SocialMediaEvidence , masing-masing dengan subkelasnya. Ontologi DeviceForensic mengatur data yang diperoleh dari perangkat digital skala kecil, mencakup penyimpanan, file, dan karakteristik perangkat. Sebaliknya, ontologi SocialMediaEvidence menangani bukti dari platform media sosial, termasuk profil pengguna, pesan, koneksi, dan aktivitas online. Masing-masing dari mereka memiliki sub- kelasnya:

1) **DeviceForensic:** *SmallScaleDeviceForensics, Cellphone, EmbeddedDevice, GPSDevice, MemoryCard, PDA, SIMCard, Smartphone, Android, External, Audios, Others, Pictures, Videos, Internal, userdata, data, com.facebook.katana, com.facebook.lite, com.facebook.orca, media, system, IOS, TabletComputer, and USBDrive.*

2) **SocialMediaEvidence:** *Crime, Crime_Categories, Classical_Crime, Cyber_Crime, Crimes_Archiva, Crime-Case-Solving, Digital_Evidence, Evidence_for_court, Potential_Suspect, Person, Criminal_Profile, Professional_Profile, Social_Profile, Blogger, Facebook, Alternate_Name, Apps, Chat, Comment, Connections, Currency, Current_City, Deleted_Messages, Facial_Recognition_Data, Follow, Followers, Following, Friend_Requests, Groups, IP_Addresses, Like, Like_Sites, Likes, Linked_Accounts, Logins, Logouts, Message, Past_City, Photos, Photos_Metadata, Place, Post, Privacy_Setting, Share, Subscribings, Text, Video, Google, Instagram, Linkedin, Twitter, Youtube.*

Pendekatan ontologi ganda ini menawarkan solusi komprehensif untuk investigasi forensik digital, memfasilitasi analisis kontekstual bukti digital yang komprehensif dan diperkaya.

4.8 Struktur Properti Objek

Banyak properti telah ditambahkan untuk memperkaya pengetahuan dalam ontologi. Properti ini mencakup berbagai hubungan, seperti: *administrator, advocate_of, as_account_in, author_of, bank_account_of, check_in, co_author, comment, current_work, dislike, education, eyewitness_of, family_relations, followed, geolocation, going_to, has_additional_item, has_advocate, has_attended, has_author, has_bank_account, has_blocked, has_brother, has_cousin, has_criminal_profile, has_device, has_eyewitness, has_father, has_husband, has_juror, has_mother, has_officer, has_political_status, has_religion, has_sister, has_wife, has_witness, hash_value, inspector_of, interested_in, is_closed, is_open, is_part_of, is_private, is_public, juror_of, like, location, member,*

mentioned, mentioned_by, officer_of, ownedby, owns, participate_same_riot, past_work, photo_of, published_emotions, published_status, same_organisation, share_via, stored_in, subscribe, tagged, tagged_by, talking_about, transferred_amount, transferred_by, transferred_to, uses_app, vality_url, video_of, visited, witness_to.

4.9 Struktur Properti Data

Pada struktur properti data telah ditambahkan beberapa properti, seperti *directory*, *has_app*, dan *parent_directory*. Properti ini berkontribusi pada pemetaan individu yang terkait dengan *DeviceForensic*.

4.10 Hasil Analisis

Penelitian ini mengimplementasikan studi kasus menggunakan data terbaru dari dua akun Facebook sebagai validasi terhadap ontologi yang dikembangkan. Dalam studi kasus ini, peneliti berhasil mengakuisisi dan menganalisis data dari akun-akun tersebut, menunjukkan bahwa ontologi yang dibangun mencerminkan keadaan nyata dan relevan dengan tantangan investigasi saat ini. Studi kasus ini membuktikan bahwa ontologi yang dikembangkan mampu memberikan struktur yang diperlukan untuk pemahaman yang mendalam serta analisis yang efektif dari data media sosial.

Ontologi yang diimplementasikan menunjukkan keunggulan dari beberapa aspek yang berkontribusi pada efektivitas proses investigasi:

Tabel 4.3 Aspek-aspek dalam Efektifitas.

Aspek	Metode Tradisional	Metode berbasis Ontologi
Kelengkapan	Tidak	Ya
Konsistensi	Tidak	Ya
Interoperabilitas	Tidak	Ya
Fleksibilitas	Tidak	Ya

Pada aspek Kelengkapan, ontologi ini mencakup kelas-kelas yang lengkap dan relevan, sesuai dengan hasil dari implementasi studi kasus media sosial Facebook terbaru. Semua elemen dari data media sosial berhasil diakomodasi dalam ontologi, sehingga mendukung proses investigasi yang komprehensif. Kelengkapan dalam ontologi sangat penting untuk mendukung pemahaman dan komunikasi yang jelas dalam domain yang diteliti. Dengan representasi semantik yang eksplisit dan terstruktur, ontologi membantu mengungkap hubungan yang mendasari data, sekaligus mendukung interoperabilitas semantik antar sistem. Seperti yang diungkapkan dalam sebuah studi, kelengkapan ontologi

memungkinkan terciptanya representasi yang dapat dipercaya dan eksplisit, yang merupakan elemen penting untuk membangun sistem yang dapat diandalkan. Hal ini menjadi pembeda utama antara model konseptual klasik dan model yang digerakkan oleh ontologi, di mana ekspresivitas dan kelengkapan memainkan peran krusial dalam pemahaman domain dan negosiasi makna yang lebih efektif (Guizzardi & Guarino, 2024).

Pada aspek konsistensi, struktur kelas, properti, serta objek yang ada dalam ontologi dapat digunakan kembali dalam investigasi lainnya, menunjukkan bahwa ontologi ini konsisten dan dapat diandalkan dalam skenario investigasi digital pada kasus media sosial. Kemampuan ini mengurangi kebutuhan untuk penyesuaian besar pada ontologi saat diaplikasikan ke kasus-kasus baru. Konsistensi ini sangat penting untuk memastikan bahwa seluruh kelas, objek dan properti dalam ontologi dapat saling berdampingan tanpa adanya konflik. Sebuah ontologi yang konsisten memungkinkan penalaran yang bagus dan penarikan kesimpulan yang valid. Tidak konsisten dalam ontologi dapat mengakibatkan kesimpulan yang salah dan menurunkan kegunaan ontologi dalam aplikasi praktis, termasuk analisis dan pengambilan keputusan yang berbasis data. Dalam konteks ini, penalaran dan inferensi merupakan dua proses yang bergantung pada konsistensi untuk memberikan hasil yang akurat. Penalaran adalah proses logis untuk menghasilkan informasi baru berdasarkan aturan dan hubungan dalam ontologi, sementara inferensi adalah penarikan kesimpulan dari informasi yang diperoleh melalui penalaran tersebut. Oleh karena itu, memastikan konsistensi dalam ontologi adalah kunci untuk mencapai hasil yang dapat dipercaya dan mendukung aplikasi yang efektif (Guizzardi & Guarino, 2024).

Pada aspek interoperabilitas, ontologi ini tidak hanya terbatas pada media sosial tetapi juga memiliki potensi untuk diimplementasikan ke bidang lain yang membutuhkan investigasi digital, seperti forensik perangkat kecil (SSDDF). Kemampuan untuk beradaptasi di berbagai domain ini memperlihatkan fleksibilitas yang tinggi dari ontologi. Interoperabilitas merupakan aspek penting dalam efektivitas ontologi, terutama dalam mendukung standarisasi data di berbagai domain. Ontologi yang dapat diintegrasikan dengan sistem lain memungkinkan kolaborasi yang lebih baik antara berbagai domain, yang sangat penting dalam konteks pengolahan data lintas sektor. Dengan adopsi arsitektur semantik yang semakin luas, interoperabilitas memainkan peran yang kian signifikan dalam meningkatkan kolaborasi dan memfasilitasi integrasi data. Kemampuan ontologi untuk berinteraksi dan berfungsi di berbagai domain memastikan standarisasi data, sehingga memudahkan analisis dan memungkinkan akses yang lebih luas ke informasi yang dibutuhkan oleh berbagai entitas pengguna (Jensen et al., n.d.).

Yang terakhir pada aspek fleksibilitas, ontologi ini mudah beradaptasi dengan perubahan yang terjadi di dalam lingkungan investigasi digital yang dinamis. Kemampuan untuk menyesuaikan ontologi dengan perkembangan teknologi, jenis data baru serta perluasan sesuai kebutuhan, memperkuat daya gunanya dalam jangka panjang. Sebagai contoh, dalam penelitian yang melibatkan ontologi untuk domain diabetes dan obesitas, peningkatan jumlah kelas dan properti objek sebesar 16% dan 18% masing-masing menunjukkan kemampuan ontologi untuk diperluas dan disesuaikan dengan tambahan data dan pengetahuan baru (Quinn et al., 2018). Selain itu, partisipasi dari pengguna dengan latar belakang teknis dan non-teknis dalam pengembangan ontologi menekankan bahwa ontologi tersebut dapat dengan mudah diadaptasi oleh berbagai tipe pengguna, bukan hanya oleh ahli dalam bidang tersebut. Hal ini mencerminkan bahwa ontologi dapat berfungsi dalam berbagai konteks aplikasi dengan adaptasi yang minimal (Quinn et al., 2018).

Selain itu, kemampuan untuk menerapkan ontologi ke berbagai konteks dan bidang lain menunjukkan sifat adaptabilitas yang penting. Sebagai contoh, penyesuaian ontologi untuk domain kesehatan seperti diabetes dan obesitas juga menyoroti bagaimana ontologi dapat diterapkan di berbagai konteks, memfasilitasi pemahaman dan komunikasi yang lebih baik di berbagai domain (Jensen et al., n.d.). Ini menekankan pentingnya fleksibilitas ontologi dalam menghadapi berbagai tantangan dan kebutuhan yang mungkin timbul dalam pengaplikasiannya.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Penelitian ini merupakan penerapan kerangka ontologis sebagai alat penting untuk mengkategorikan bukti digital secara sistematis pada titik akhir server dan klien. Dengan menggunakan Ontologi Bukti Digital Media Sosial dan memperkenalkan *Small Scale Digital Device Forensic* (SSDDF), penelitian ini telah berkontribusi pada metodologi prosedural yang berbeda untuk memeriksa berkas kasus yang terkait dengan insiden media sosial. Kontribusi pertama adalah pengorganisasian data yang cermat dari penyedia layanan sisi server menggunakan *Social-Media Digital Evidence Ontology*, yang terbukti menjadi metodologi prosedural yang kuat untuk meneliti berkas kasus terkait insiden media sosial. Kontribusi kedua, SSDDF, secara eksplisit menggambarkan arsitektur penyimpanan dalam ponsel pintar Android, memainkan peran penting dalam mengkategorikan bukti digital yang diperoleh dari peralatan seluler atau klien.

Implikasi praktis dari penelitian ini sangat besar. Penerapan SSDDF melengkapi penyelidik forensik dan lembaga penegak hukum dengan kerangka terstruktur untuk mengatur dan mengkategorikan bukti digital dari perangkat digital skala kecil. Hal ini menghasilkan analisis data, wawasan yang lebih cepat, korelasi lintas perangkat yang lebih baik, dan pengambilan data yang lebih baik. Selain itu, integrasi SSDDF dengan alat forensik digital yang ada menghilangkan kebutuhan akan pelatihan ulang yang ekstensif, sehingga menyederhanakan proses investigasi.

Dalam penelitian ini, peneliti melakukan implementasi studi kasus untuk memvalidasi ontologi yang dikembangkan menggunakan data terbaru dari Facebook. Langkah ini dimaksudkan untuk menguji sejauh mana ontologi yang dikembangkan mencerminkan struktur dan konsep dalam data aktual dari platform media sosial. Melalui studi kasus ini, peneliti dapat mengevaluasi kesesuaian ontologi dengan data yang diperoleh. Hasil analisis menunjukkan bahwa ontologi mampu menggambarkan dan mengorganisir data media sosial dalam konteks forensik digital dengan baik. Implementasi studi kasus ini menjadi langkah penting dalam memvalidasi ontologi, memastikan bahwa fondasi penelitian tepat dalam merepresentasikan data aktual dalam domain metadata media sosial dan perangkat bergerak berskala kecil.

Selain itu ontologi yang dikembangkan dapat menunjang dalam *Open Source Intelligence* (OSINT) sehingga meningkatkan kapasitas forensik digital, khususnya dalam menganalisis data dari media sosial. Pendekatan ontologi ini dapat menjadi dukungan keamanan dan penyaringan pesan instan di lingkungan media sosial, membantu identifikasi potensi risiko keamanan yang mungkin timbul.

Selain itu, kontribusi ontologi ini tidak hanya terbatas pada analisis saat ini, melainkan melibatkan elemen prediksi aktivitas pengguna di masa depan. Kemampuan ontologi dalam menganalisis perilaku pengguna dapat memberikan wawasan yang berharga dalam mengidentifikasi potensi ancaman dan kejahatan digital yang mungkin terjadi.

Dalam menangani tantangan kompleks forensik media sosial, ontologi mampu mengatasi heterogenitas data dan volume besar, membentuk dasar sistematis untuk mengelola informasi dari berbagai sumber. Penggunaan Ontologi Jaringan Sosial Terpadu (USNO) terbukti berhasil dalam homogenisasi data, memungkinkan analisis lintas sumber yang mendalam, dan pada akhirnya mengurangi biaya penyelidikan.

Di samping itu, ontologi mendukung ekstraksi konten semantik otomatis dan hubungan spasial-temporal, memudahkan analisis forensik dengan memahami makna dan hubungan antar entitas data. Meskipun terdapat tantangan, seperti manajemen provenans, paragraf ini mencerminkan pandangan optimis dengan mengusulkan arah penelitian masa depan, termasuk pengembangan ontologi yang lebih komprehensif dan evaluasi prototipe perangkat lunak.

Secara keseluruhan, ontologi yang telah dikembangkan memberikan landasan yang sistematis untuk pendekatan forensik digital diarahkan OSINT. Kontribusinya dalam menyederhanakan analisis dan memberikan wawasan proaktif menjadikannya elemen kunci dalam mengatasi kompleksitas forensik digital, menggambarkan peran yang penting dalam menghadapi tantangan dunia digital yang terus berkembang.

5.2 Saran

Untuk penelitian ke depan, penting untuk memperluas penelitian tentang pemetaan sistem penyimpanan di berbagai platform perangkat seluler, tidak hanya mencakup Android, tetapi juga mencakup *smartphone* berbasis iOS, *smartwatch*, *Unmanned Aerial Vehicles* (UAV), dan masih banyak lagi. Selain itu, ada kebutuhan untuk mengeksplorasi implementasi praktis SparkQL untuk memperkuat keterkaitan yang rumit antara server dan data klien, sehingga memperjelas dinamika interaksi data yang kompleks dalam ekosistem digital.

Adapun saran terkait kualitas penelitian, pada penelitian ontologi selanjutnya perlu dilakukan validasi yang lebih mendalam dengan mengonfirmasikan ontologi yang

dikembangkan kepada ahli yang berkaitan dengan forensik digital. Hal ini akan memastikan bahwa ontologi yang dikembangkan memiliki integritas dan validitas yang tinggi, serta dapat diandalkan dalam berbagai konteks investigasi forensik. Validasi oleh para ahli akan memberikan masukan yang berharga untuk penyempurnaan ontologi, memastikan bahwa setiap konsep, hubungan, dan struktur yang ada dalam ontologi relevan dan sesuai dengan praktik terbaik dalam forensik digital. Dengan demikian, ontologi yang dihasilkan akan lebih kuat dan efektif dalam mendukung analisis forensik digital yang kompleks.

Daftar Pustaka

- Abebe, M. A., Tekli, J., Getahun, F., Chbeir, R., & Tekli, G. (2020). Generic metadata representation framework for social-based event detection, description, and linkage. *Knowledge-Based Systems*, 188. <https://doi.org/10.1016/j.knosys.2019.06.025>
- Aditia, R. (2021). Fenomena Phubbing: Suatu Degradasi Relasi Sosial Sebagai Dampak Media Sosial. *KELUWIH: Jurnal Sosial Dan Humaniora*, 2(1), 8–14. <https://doi.org/10.24123/soshum.v2i1.4034>
- Almehmadi, T., & Batarfi, O. (2019). Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1–6. <https://doi.org/10.1109/CAIS.2019.8769520>
- Android Debug Bridge (adb) | Android Studio | Android Developers*. (n.d.). Retrieved September 18, 2023, from <https://developer.android.com/tools/adb>
- Arshad, H., Jantan, A., Hoon, G. K., & Butt, A. S. (2019). A multilayered semantic framework for integrated forensic acquisition on social media. *Digital Investigation*, 29, 147–158. <https://doi.org/10.1016/j.diin.2019.04.002>
- Boueiz, M.-R. (2020). Importance of rooting in an Android data acquisition. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–4. <https://doi.org/10.1109/ISDFS49300.2020.9116445>
- Bratsas, C., Chondrokostas, E., Koupidis, K., & Antoniou, I. (2021). The use of national strategic reference framework data in knowledge graphs and data mining to identify red flags. *Data*, 6(1), 1–20. <https://doi.org/10.3390/data6010002>
- Bulele, Y. N., & Wibowo, T. (2020). ANALISIS FENOMENA SOSIAL MEDIA DAN KAUM MILENIAL: STUDI KASUS TIKTOK. *Conference on Business, Social Sciences and Innovation Technology*, 1(1), 565–572. <http://journal.uib.ac.id/index.php/cbssit>
- BusyBox*. (n.d.). Retrieved September 18, 2023, from <https://www.busybox.net/>
- Colin Elman. (2020). *The Production of Knowledge* (C. Elman, J. Gerring, & J. Mahoney, Eds.). Cambridge University Press. <https://doi.org/10.1017/9781108762519>
- Download Magisk Manager Latest Version 26.3 For Android 2023*. (n.d.). Retrieved September 18, 2023, from <https://magiskmanager.com/>

- Faisol, A. (2017, December 19). *Tulis Status soal Tilang di Facebook, Wanita Ini Ditahan Polisi*. Kompas.Com. <https://regional.kompas.com/read/2017/12/19/05495311/tulis-status-soal-tilang-di-facebook-wanita-ini-ditahan-polisi>
- GitHub - topjohnwu/Magisk: *The Magic Mask for Android*. (n.d.). Retrieved September 18, 2023, from <https://github.com/topjohnwu/Magisk>
- Guizzardi, G., & Guarino, N. (2024). Explanation, semantics, and ontology. *Data & Knowledge Engineering*, 102325. <https://doi.org/10.1016/j.datak.2024.102325>
- Harrill, D. C., & Mislán, R. P. (2007). A Small Scale Digital Device Forensics ontology. *Small Scale Digital Device Forensics Journal*, 1(1), 1–7.
- Jadhao, A. R., & Agrawal, A. J. (2016). A digital forensics investigation model for social networking site. *ACM International Conference Proceeding Series*, 04-05-March-2016. <https://doi.org/10.1145/2905055.2905346>
- Jensen, M., De Colle, G., Kindya, S., More, C., Cox, A. P., & Beverley, J. (n.d.). *The Common Core Ontologies*. <https://doi.org/10.48550/arXiv.2404.17758>
- John Domingue, Dieter Fensel, J. A. H. (2011). *Handbook of Semantic Web Technologies* (J. Domingue, D. Fensel, & J. A. Hendler, Eds.). Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-540-92913-0>
- Jones, L. (2018, June 26). *Mother, boyfriend arrested for abuse of 2 and 3-year-old children in Arkansas*. News Channel 3 Wreg Memphis. <https://wreg.com/news/gosnell-police-investigating-severe-child-abuse-case-person-of-interest-in-custody/>
- Kalemi, E., & Yildirim-yayilgan, S. (2016). *Ontologies for Social Media Digital Evidence*. January.
- Kalemi, E., Yildirim-Yayilgan, S., Domnori, E., & Elezaj, O. (2017). SMOnt: An ontology for crime solving through social media. *International Journal of Metadata, Semantics and Ontologies*, 12(2–3), 71–81. <https://doi.org/10.1504/IJMSO.2017.090756>
- Karie, N. M., & Venter, H. S. (2014). Toward a general ontology for digital forensic disciplines. *Journal of Forensic Sciences*, 59(5), 1231–1241. <https://doi.org/10.1111/1556-4029.12511>
- Lwin, H. H., Aung, W. P., & Lin, K. K. (n.d.). *Comparative Analysis of Android Mobile Forensics Tools*.
- Mohan, A. K., & Venkataraman, D. (2017). Forensic future of social media analysis using web ontology. *2017 4th International Conference on Advanced Computing and*

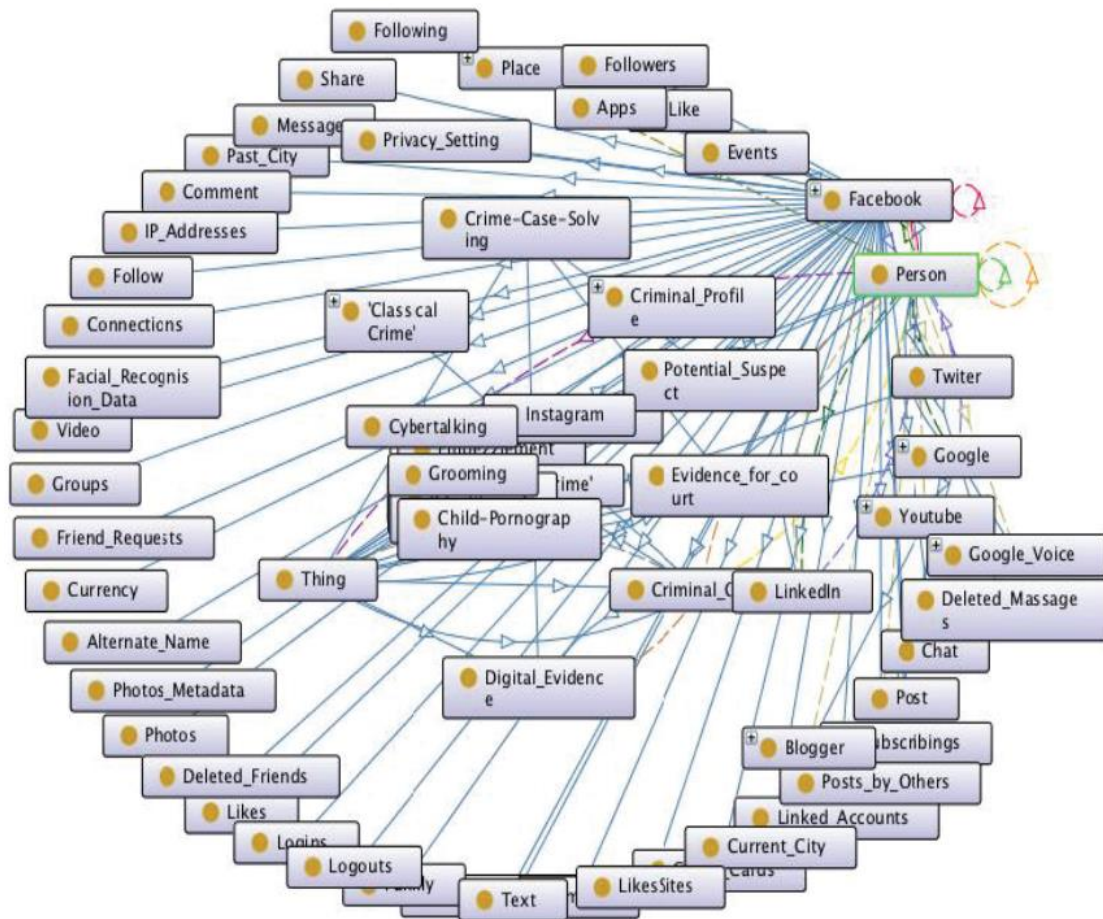
- Communication Systems, ICACCS 2017*.
<https://doi.org/10.1109/ICACCS.2017.8014682>
- Mulawarman, & Nurfitri, A. D. (2017). Perilaku Pengguna Media Sosial beserta Implikasinya Ditinjau dari Perspektif Psikologi Sosial Terapan. *Buletin Psikologi*, 25(1), 36–44. <https://doi.org/10.22146/buletinpsikologi.22759>
- Nailufar, N. N. (2017, March 10). *Ahmad Dhani Dilaporkan ke Polisi karena Kicauan Bernada Kebencian*. Kompas.Com.
<https://megapolitan.kompas.com/read/2017/03/10/09084661/ahmad.dhani.dilaporkan.ke.polisi.karena.kicauan.bernada.kebencian>
- Nikolaidou, A., Lazaridis, M., Semertzidis, T., Axenopoulos, A., & Daras, P. (2019). Forensic analysis of heterogeneous social media data. *IC3K 2019 - Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, 2, 343–350.
<https://doi.org/10.5220/0008347803430350>
- Nur Faiz, M., Adi Prabowo, W., & Fajar Sidiq, M. (2018). *Journal of Informatics, Information System, Software Engineering and Applications Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal*. 1(1), 63–70.
<https://doi.org/10.20895/INISTA.V1I1>
- Pakpahan, R. (2017). ANALISIS FENOMENA HOAX DIBERBAGAI MEDIA SOSIAL DAN CARA MENANGGULANGI HOAX. *Konferensi Nasional Ilmu Sosial & Teknologi (KNiST)*, 1(1), 479–484.
<http://seminar.bsi.ac.id/knist/index.php/UnivBSI/article/view/184>
- Quinn, S., Bond, R., & Nugent, C. (2018). A two-staged approach to developing and evaluating an ontology for delivering personalized education to diabetic patients. *Informatics for Health and Social Care*, 43(3), 264–279.
<https://doi.org/10.1080/17538157.2017.1364246>
- Qurrota Ayun, P. (2015). Fenomena Remaja Menggunakan Media Sosial dalam Membentuk Identitas. *CHANNEL Jurnal Komunikasi*, 3(2), 1–16.
<https://doi.org/10.12928/channel.v3i2.3270>
- Randelović, D., & Stojković, D. (2012). Possibilities of autopsy tool use for forensic purposes. *Nauka, Bezbednost, Policija*, 17(3), 19–33.
- Rifauddin, M. (2016). Fenomena Cyberbullying pada Remaja. *Khizanah Al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, 4(1), 35–44.
<https://doi.org/10.24252/kah.v4i1a3>

- Roberts, J. J. (2012, August 15). *'Friends' can share your Facebook profile with the government, court rules – Old GigaOm*. GigaOm.
<https://old.gigaom.com/2012/08/15/friends-can-share-your-facebook-profile-with-the-government-court-rules/>
- Rustandi, R. (2020). Analisis Framing Kontra Narasi Terorisme dan Radikalisme di Media Sosial (Studi Kasus pada Akun @dutadamaijabar). *Jurnal Komunikatif*, 9(2), 134–153. <https://doi.org/10.33508/jk.v9i2.2698>
- Sagiyanto, A., & Ardiyanti, N. (2018). SELF DISCLOSURE MELALUI MEDIA SOSIAL INSTAGRAM (Studi Kasus Pada Anggota Galeri Quote). *Nyimak (Journal of Communication)*, 2(1), 81–94. <https://doi.org/10.31000/nyimak.v2i1.687>
- Schladebeck, J. (2018, January 18). *Canadian woman convicted in friend's murder after authorities uncover clue in Facebook selfie – New York Daily News*. New York Daily News. <https://www.nydailynews.com/news/world/woman-convicted-friend-murder-posting-facebook-selfie-article-1.3762298>
- Turnbull, B., & Randhawa, S. (2015). Automated event and social network extraction from digital evidence sources with ontological mapping. *Digital Investigation*, 13, 94–106. <https://doi.org/10.1016/j.diin.2015.04.004>
- Wandt, A. S. (2021, October 5). *YouTube, TikTok helped police in Gabby Petito case. How social media can aid in others*. NBC News.
<https://www.nbcnews.com/think/opinion/youtube-tiktok-helped-police-gabby-petito-case-how-social-media-ncna1280522>
- We Are Social. (2022). *Digital 2022: Indonesia - DataReportal - Global Digital Insights*. DataReportal. <https://datareportal.com/reports/digital-2022-indonesia>
- Zebua, D. J. (2017, June 16). *Hina Polisi di Facebook Usai Ditilang, Seorang PNS Dijerat UU ITE*. Kompas.Com.
<https://regional.kompas.com/read/2017/06/16/07040051/hina.polisi.di.facebook.usai.ditilang.seorang.pns.dijerat.uu.ite>

LAMPIRAN 1 - PENGELOMPOKAN OBJEK DALAM FORENSIKA PERANGKAT BERSKALA KECIL ATAU *SMALL SCALE DEVICE DIGITAL FORENSIC*

		Magnetic Devices	Flash Devices	PC Extension Devices	Optical Devices
Device Type					
Super Disk LS-120/240 Drive	✓				
Zip 100/250 Drive	✓				
Modular USB Micro Drive	✓				
Thumb or Keychain USB Drives		✓			
MultiMediaCard (MMC)		✓			
Memory Stick		✓			
ATA cards		✓			
DiskOnChip		✓			
Memory Card		✓	✓		
Cell Phones		✓	✓		
PDA's		✓	✓		
Smart Phone		✓	✓		
Notebook Computer	✓	✓	✓	✓	✓
Tablet Computer	✓	✓	✓	✓	✓
Handheld Game Console		✓	✓	✓	✓
Digital Audio Player (DAP)	✓	✓	✓		
GPS Receiver		✓			
GPS Device			✓		

LAMPIRAN 2 - ONTOLOGI FORENSIKA BARANG BUKTI DIGITAL MEDIA SOSIAL ATAU *SOCIAL MEDIA DIGITAL EVIDENCE*



LAMPIRAN 3 – HASIL TEMUAN METADATA

ACTIVITY_MESSAGES

1. Sisi korban (Norah Nolan).

```
{
  "group_interactions_v2": [
    {
      "name": "",
      "description": "",
      "entries": [
        {
          "data": {
            "name": "Branded Bags & Accessories",
            "value": "5 times",
            "uri": "https://www.facebook.com/groups/789542252783275/"
          }
        }
      ]
    }
  ]
}
```

2. Sisi pelaku (Garry Swihart).

```
{
  "group_interactions_v2": [
    {
      "name": "",
      "description": "",
      "entries": [
        {
          "data": {
            "name": "Branded Bags & Accessories",
            "value": "6 times",
            "uri": "https://www.facebook.com/groups/789542252783275/"
          }
        }
      ]
    }
  ]
}
```

```
{
  "people_interactions_v2": [
    {
      "name": "",
      "description": "",
```

```
"entries": [  
  {  
    "timestamp": 1682867621,  
    "data": {  
      "name": "Norah Nolan",  
      "uri": "https://www.facebook.com/norah.nolan.10"  
    }  
  }  
]  
}  
]
```

LAMPIRAN 4 – HASIL TEMUAN METADATA LOCATION

1. Sisi korban (Norah Nolan).

```
{
  "phone_number_location_v2": [
    {
      "spn": "PT. Telkomsel Selular (Telkom)",
      "country_code": "510"
    }
  ]
}
```

```
{
  "primary_location_v2": {
    "city_region_pairs": [
      [
        "Kejayan, Yogyakarta",
        "Special Region of Yogyakarta"
      ]
    ],
    "zipcode": [
      "55283"
    ]
  }
}
```

2. Sisi pelaku (Garry Swihart).

```
{
  "phone_number_location_v2": [
    {
      "spn": "PT. Telkomsel Selular (Telkom)",
      "country_code": "510"
    }
  ]
}
```

```
{
  "primary_location_v2": {
    "city_region_pairs": [
      [
        "Kejayan, Yogyakarta",
        "Special Region of Yogyakarta"
      ]
    ],
    "zipcode": [
      "55283"
    ]
  }
}
```

LAMPIRAN 5 – HASIL TEMUAN METADATA NOTIFICATIONS

1. Sisi pelaku (Garry Swihart)

```
{
  "notifications_v2": [
    {
      "timestamp": 1685591015,
      "unread": true,
      "href":
"https://www.facebook.com/groups/247716726179834/permalink/1288903445394485/"
,
      "text": "RD Graphics & Signs posted in Things for Sale on Thursday."
    },
    {
      "timestamp": 1684990026,
      "unread": true,
      "href":
"https://www.facebook.com/groups/247716726179834/permalink/1284756602475836/"
,
      "text": "Shannon Wongsodikromo, Jerry Matiskam and 11 others posted in
Things for Sale."
    },
    {
      "timestamp": 1684566743,
      "unread": false,
      "href":
"https://www.facebook.com/dyi/?tab=all_archives&referrer=notif",
      "text": "Your Meta information is ready to download."
    },
    {
      "timestamp": 1684514778,
      "unread": true,
      "href":
"https://www.facebook.com/groups/247716726179834/permalink/1281880276096802/"
,
      "text": "West Mart Shopping & More, Varsha Benie Patjai and 15 others
posted in Things for Sale.: \"Nieuw BINNEN NIKE AIRFORCE BEPERK
VOORRAAD...\"."
    },
    {
      "timestamp": 1684421556,
      "unread": true,
      "href": "https://www.facebook.com/watch/?ref=NOTIFICATIONS",
      "text": "You can watch the latest videos just for you on Facebook
Watch."
    }
  ],
}
```

```

{
  "timestamp": 1684115065,
  "unread": true,
  "href": "https://www.facebook.com/groups/565851308453722/",
  "text": "Norah Nolan joined Luxury - Streetwear Brands PH."
},
{
  "timestamp": 1684003346,
  "unread": false,
  "href": "https://www.facebook.com/groups/565851308453722/",
  "text": "Norah Nolan joined Luxury - Streetwear Brands PH."
},
{
  "timestamp": 1683896864,
  "unread": true,
  "href":
"https://www.facebook.com/groups/247716726179834/permalink/1277500203201476/
",
  "text": "Shivii's Cosm, Casnova FM perfumes and 15 others posted in
Things for Sale."
},
{
  "timestamp": 1683788501,
  "unread": true,
  "href": "https://www.facebook.com/watch/?ref=NOTIFICATIONS",
  "text": "You can watch the latest videos just for you on Facebook
Watch."
},
{
  "timestamp": 1683271960,
  "unread": true,
  "href":
"https://www.facebook.com/groups/247716726179834/permalink/1273516536933176/
",
  "text": "The Phone Center, Audrey Kisman and 14 others posted in
Things for Sale."
},
{
  "timestamp": 1682867710,
  "unread": false,
  "href":
"https://www.facebook.com/groups/789542252783275/?post_id=793713712366129&co
mment_id=793727449031422&reply_comment_id=796597245411109",
  "text": "Norah Nolan mentioned you in a comment in Branded Bags &
Accessories."
},
{
  "timestamp": 1682822351,
  "unread": true,

```

```

    "href": "https://www.facebook.com/watch/?ref=NOTIFICATIONS",
    "text": "You can watch the latest videos just for you on Facebook
Watch."
  },
  {
    "timestamp": 1682423416,
    "unread": true,
    "href":
"https://www.facebook.com/groups/789542252783275/?multi_permalinks=793713712
366129",
    "text": "Norah Nolan likes your post in Branded Bags & Accessories."
  },
  {
    "timestamp": 1682423413,
    "unread": true,
    "href":
"https://www.facebook.com/groups/789542252783275/?multi_permalinks=793714782
366022",
    "text": "Norah Nolan likes your post in Branded Bags & Accessories."
  },
  {
    "timestamp": 1682423410,
    "unread": true,
    "href":
"https://www.facebook.com/groups/789542252783275/?multi_permalinks=793717419
032425",
    "text": "Norah Nolan likes your post in Branded Bags & Accessories."
  },
  {
    "timestamp": 1682423385,
    "unread": true,
    "href":
"https://www.facebook.com/groups/789542252783275/?post_id=793713712366129&co
mment_id=793727449031422",
    "text": "Norah Nolan commented on your post in Branded Bags &
Accessories."
  },
  {
    "timestamp": 1682423132,
    "unread": true,
    "href": "https://www.facebook.com/norah.nolan.10",
    "text": "Norah Nolan accepted your friend request."
  },
  {
    "timestamp": 1682421621,
    "unread": true,
    "href": "https://www.facebook.com/groups/789542252783275/",
    "text": "Your group now has 5 posts. Keep it up by posting again in
Branded Bags & Accessories."
  }
]

```

```

    },
    {
      "timestamp": 1682251205,
      "unread": false,
      "href": "https://www.facebook.com/groups/789542252783275/members/",
      "text": "Branded Bags & Accessories is almost complete. Invite your
friends to get things started."
    },
    {
      "timestamp": 1681590378,
      "unread": true,
      "href": "fb://groups/tab/discover",
      "text": "You aren't in any groups yet. Join groups to find other
people who share your interests."
    },
    {
      "timestamp": 1681437331,
      "unread": true,
      "href": "fb://groups/tab/discover",
      "text": "You aren't in any groups yet. Join groups to find other
people who share your interests."
    },
    {
      "timestamp": 1680900815,
      "unread": true,
      "href": "fb://groups/tab/discover",
      "text": "You aren't in any groups yet. Join groups to find other
people who share your interests."
    },
    {
      "timestamp": 1680805291,
      "unread": true,
      "href": "fb://groups/tab/discover",
      "text": "You aren't in any groups yet. Join groups to find other
people who share your interests."
    },
    {
      "timestamp": 1680714388,
      "unread": true,
      "href": "https://www.facebook.com/watch/?ref=NOTIFICATIONS",
      "text": "You can watch the latest videos just for you on Facebook
Watch."
    }
  ]
}

```

LAMPIRAN 6 – HASIL TEMUAN METADATA SEARCH

1. Sisi pelaku (Garry Swihart)

```
{
  "searches_v2": [
    {
      "timestamp": 1681754009,
      "attachments": [
        {
          "data": [
            {
              "text": "\"branded\""
            }
          ]
        }
      ],
      "data": [
        {
          "text": "branded"
        }
      ],
      "title": "You searched Facebook"
    },
    {
      "timestamp": 1681754032,
      "attachments": [
        {
          "data": [
            {
              "text": "\"luxury pearl\""
            }
          ]
        }
      ],
      "data": [
        {
          "text": "luxury pearl"
        }
      ],
      "title": "You searched Facebook"
    },
    {
      "timestamp": 1681754050,
      "attachments": [
        {
          "data": [
            {
              "text": "\"branded things\""
            }
          ]
        }
      ],
      "data": [
        {
          "text": "branded things"
        }
      ],
      "title": "You searched Facebook"
    }
  ]
}
```

```

    }
  ]
}
],
"data": [
  {
    "text": "branded things"
  }
],
"title": "You searched Facebook"
},
{
  "timestamp": 1681754269,
  "attachments": [
    {
      "data": [
        {
          "text": "\"branded things\""
        }
      ]
    }
  ],
  "data": [
    {
      "text": "branded things"
    }
  ],
  "title": "You searched Facebook"
},
{
  "timestamp": 1681754278,
  "attachments": [
    {
      "data": [
        {
          "text": "\"Branded Things\""
        }
      ]
    }
  ],
  "data": [
    {
      "text": "Branded Things"
    }
  ],
  "title": "You searched Facebook"
},
{
  "timestamp": 1681754318,

```

```

    "attachments": [
      {
        "data": [
          {
            "text": "\"branded things sale point\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "branded things sale point"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754346,
    "attachments": [
      {
        "data": [
          {
            "text": "\"branded things sale point\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "branded things sale point"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754360,
    "attachments": [
      {
        "data": [
          {
            "text": "\"branded things sale point\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "branded things sale point"
      }
    ]
  }

```

```

    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754581,
    "attachments": [
      {
        "data": [
          {
            "text": "\"branded things sale point\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "branded things sale point"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754585,
    "attachments": [
      {
        "data": [
          {
            "text": "\"BRANDED THINGS SALE POINT\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "BRANDED THINGS SALE POINT"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754625,
    "attachments": [
      {
        "data": [
          {
            "text": "\"branded things sale point\""
          }
        ]
      }
    ]
  }
}

```

```

    ],
    "data": [
      {
        "text": "branded things sale point"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754636,
    "attachments": [
      {
        "data": [
          {
            "text": "\"Things for Sale\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "Things for Sale"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754664,
    "attachments": [
      {
        "data": [
          {
            "text": "\"luxury pearl\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "luxury pearl"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754672,
    "attachments": [
      {
        "data": [

```

```

        {
            "text": "\"luxury pearl\""
        }
    ]
},
"data": [
    {
        "text": "luxury pearl"
    }
],
"title": "You searched Facebook"
},
{
    "timestamp": 1681754677,
    "attachments": [
        {
            "data": [
                {
                    "text": "\"Pearl Luxury
\u00e2\u009a\u00ac\u00e2\u009a\u00ab\u00e2\u009a\u00ac\""
                }
            ]
        }
    ],
    "data": [
        {
            "text": "Pearl Luxury
\u00e2\u009a\u00ac\u00e2\u009a\u00ab\u00e2\u009a\u00ac"
        }
    ],
    "title": "You searched Facebook"
},
{
    "timestamp": 1681754682,
    "attachments": [
        {
            "data": [
                {
                    "text": "\"luxury pearl\""
                }
            ]
        }
    ],
    "data": [
        {
            "text": "luxury pearl"
        }
    ],

```

```

    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681754759,
    "attachments": [
      {
        "data": [
          {
            "text": "\"luxury pearl\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "luxury pearl"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681755158,
    "attachments": [
      {
        "data": [
          {
            "text": "\"branded\""
          }
        ]
      }
    ],
    "data": [
      {
        "text": "branded"
      }
    ],
    "title": "You searched Facebook"
  },
  {
    "timestamp": 1681755173,
    "attachments": [
      {
        "data": [
          {
            "text": "\"branded\""
          }
        ]
      }
    ],
  },

```

```
    "data": [  
      {  
        "text": "branded"  
      }  
    ],  
    "title": "You searched Facebook"  
  }  
]
```