

Implementasi Model Digital Forensik Proses (DFD) Untuk Sosial Media Investigation Dengan Tools Hunchly

Muhammad Na'im Al Jum'ah¹, Hamid Wijaya², Rima Ruktiari Ismail³

¹ Ilmu Komputer Fakultas Teknologi Informasi, Universitas Sembilanbelas November Kolaka

^{2,3}Sistem Informasi Fakultas Teknologi Informasi, Universitas Sembilanbelas November Kolaka

Email: ¹muhnaimaljumah@usn.ac.id, ²hamidwijaya@usn.ac.id, ³rimaruktiarii@usn.ac.id

Abstrak

Perkembangan teknologi yang semakin pesat dapat menjadi dampak positif dan dapat negatif. Dampak positifnya adalah proses penyebaran informasi yang semakin cepat, namun dampak negatifnya adalah banyaknya informasi hoax dan hate space yang terjadi di media sosial akibat tidak adanya filter dan pengecekan keabsahan informasi. Hal ini juga mengakibatkan banyaknya tindak kejahatan yang terjadi di media sosial. Salah satu pemecahan masalah dengan banyaknya kasus yang terjadi akibat penyalahgunaan media sosial adalah dengan melakukan proses investigasi forensik pada social media. Proses investigasi forensik ini dilakukan dengan metode live investigation menggunakan metode digital forensik proses yang terdiri dari proses Collection, Examination, Analysis dan Reporting. Proses pengumpulan barang bukti dengan menggunakan tools hunchly sehingga dapat dilakukan proses investigasi secara langsung. Hasil dari penelitian ini adalah dengan memanfaatkan metode digital forensik proses dan penggunaan tools hunchly untuk melakukan teknik live investigation untuk melakukan pengumpulan bukti digital dari akun-akun media sosial yang melakukan tindak kejahatan di media sosial sehingga dapat di proses sesuai dengan peraturan hukum yang telah berlaku

Kata kunci: Bukti Digital, Media Sosial, Digital Forensik, Hunchly

Implementation of the Digital Forensic Process (DFD) Model for Social Media Investigation Using Hunchly Tools

Abstract

The increasingly rapid development of technology can have both positive and negative impacts. The positive impact is that the process of disseminating information is getting faster, but the negative impact is the large amount of hoax information and hate space that occurs on social media due to the absence of filters and checking the validity of the information. This also results in many crimes occurring on social media. One solution to the problem with the many cases that occur due to misuse of social media is to carry out a forensic investigation process on social media. This forensic investigation process is carried out using the live investigation method using a digital forensic process method consisting of Collection, Examination, Analysis and Reporting processes. The process of collecting evidence uses powerful tools so that the investigation process can be carried out directly. The results of this research are by utilizing digital forensic process methods and using hunchly tools to carry out live investigation techniques to collect digital evidence from social media accounts that commit crimes on social media so that it can be processed in accordance with applicable legal regulations.

Keywords: Sosial Media, Digital Forensics, Hunchly

1. PENDAHULUAN

Teknologi saat ini berkembang sangat pesat. Jika dilihat survei dari APPJI data penetrasi pengguna internet di Indonesia tahun 2023 mencapai 78,19%. Banyaknya pengguna internet di Indonesia dapat menjadi hal positif maupun hal negatif. Hal positifnya adalah masyarakat dapat lebih cepat mendapatkan informasi. Sedangkan hal negatifnya adalah banyaknya tindak kejahatan sehingga mengakibatkan kerugian akibat transaksi internet mencapai 95,17%. Untuk pengguna media sosial juga mencapai presentasi tertinggi yaitu Youtube 65,41% dan

Instagram 60,24%. (APPJI 2023). Penggunaan sosial media dengan presentasi yang tinggi ini akan menyebabkan banyaknya kasus kejahatan akibat penyalahgunaan media sosial. Media sosial telah Masyarakat secara umum dan organisasi karena banyaknya keuntungan yang dimilikinya, namun fakta dari bukti menunjukkan bahwa teknologi ini dapat diambil alih dan dimanfaatkan untuk keuntungan para penjahat untuk melakukan kekacauan dan kejahatan berskala luas di dunia cyber (Mustapha and Ahmad 2022).

Hal ini juga akan mengakibatkan tingkat kejahatan di sosial media juga akan semakin tinggi.

Ada beberapa kasus terjadi akibat dari penggunaan media sosial yang kurang baik, seperti kasus pencemaran nama baik, penyebaran informasi hoax hingga kasus penipuan di media sosial. Penyebab lain kejahatan di media sosial adalah karena kurangnya pemahaman masyarakat mengenai literasi digital serta banyaknya informasi yang dapat diakses dengan mudah di media sosial. Literasi digital akan membantu masyarakat dalam bertindak di media sosial (Setyaningsih et al. 2021).

Media sosial memiliki banyak jenis di antaranya LinkedIn, facebook, Instagram, twitter, youtube dan lain sebagainya. media sosial juga banyak digunakan sebagai sarana penyebaran informasi, kepada pelanggan, partisan pemilu dan lain sebagainya penyebaran informasi tersebut, kadang kala terdapat beberapa informasi yang menyesatkan atau hoax dan *hate speech*. Karena dengan penyebaran informasi yang begitu cepat, penerima informasi kadang tidak melakukan filter awal dan sangat gampang percaya dengan informasi yang telah di sebarakan (Palupi 2019).

Hoax dan *hate speech* adalah bentuk kejahatan yang sangat berbahaya. Banyaknya kejahatan yang terjadi di media sosial, maka proses investigasi di media sosial juga sangat penting dilakukan. Proses investigasi untuk memperoleh data berupa bukti digital di media sosial ini akan menjadi solusi pemecahan kasus yang terjadi akibat dari penyalahgunaan media sosial. Pengumpulan data untuk investigasi di media sosial terdiri dari 4 macam yaitu pengguna, aktifitas, jaringan dan konten (Arshad, Jantan, and Omolara 2019).

Selain itu penggunaan tools yang baik akan memudahkan investigator dalam mengumpulkan barang bukti di media sosial (Stodelov and Miloslavskaya 2022). Bukti digital tersebut yang akan digunakan penyidik dalam proses persidangan. Penelitian dengan metode analisis bibliometric juga dapat membantu memetakan para pelaku berdasarkan sumber sosial media yang digunakan (Kusuma et al., 2021).

Dalam investigasi di media sosial, tentu membutuhkan metode dan tools yang sesuai agar bukti digital yang dikumpulkan dapat di terima dan dipertanggung jawabkan di persidangan. Proses investigasi forensik terdiri atas empat fase yaitu *collection*, *Examination*, *Analysis*, dan *Reporting*. (Kent et al. 2006).

Ada beberapa penelitian yang berkaitan dengan penelitian ini. Seperti yang dilakukan oleh (Pomalingo, Sugiantoro, and Prayudi 2019). Penelitian ini memanfaatkan data visualisasi sebagai pendukung invstigasi media sosial. hasil dari penelitian ini didapatkan informasi yang penting untuk melakukan investigasi media sosial, seperti informasi tentang profil pengguna, postingan, komentar, halaman sosial media yang disukai, lokasi, serta time stamp yang semuanya itu dihubungkan oleh sebuah garis yang memiliki arah yang

menunjukkan hubungan antara node. Penelitian lain juga dilakukan oleh (David 2020) tentang dua tahap untuk investigasi sosial jaringan di forensik digital. Dari penelitian ini menyoroti perlunya pendekatan yang memungkinkan penyidik digital memprioritaskan artefak jaringan sosial untuk dianalisis lebih lanjut; menentukan hubungan sosial dalam konteks penyelidikan, misalnya. hubungan sosial pengguna, bagaimana artefak tersebut ditemukan, dan bagaimana artefak tersebut dapat digunakan sebagai bukti di pengadilan.

Penelitian lain juga dilakukan oleh (Montasari et al. 2018) Investigasi forensik digital media sosial, akuisisi dan analisis bukti digital. Hasil dari penelitian ini adalah penelitian ini berhasil menguraikan langkah-langkah proses investigasi forensik digital yang harus dilakukan untuk memperoleh bukti digital yang autentik dan sah secara forensik. Penelitian lain juga dilakukan oleh (Sanduni and Perera 2020). Berbeda dengan penelitian sebelumnya, penelitian ini melakukan tinjauan kritis tentang Investigasi keamanan media sosial. Hasil dari penelitian ini adalah media sosial memiliki risiko keamanan yang tinggi serta risiko terhadap privasi. Karena infrastruktur mereka yang terpusat, arsip mereka yang sangat besar yang berisi semua data pengenalan pribadi yang dibutuhkan seorang peretas, dan ketidaktahuan masyarakat umum tentang cara menggunakan pengaturan privasi dengan benar untuk meningkatkan keamanan.

Berbeda dengan beberapa penelitian sebelumnya, penelitian ini akan berfokus pada proses pengumpulan bukti digital yang dilakukan secara live investigation dengan memanfaatkan tools Hunchly. Dengan memanfaatkan tools hunchly ini lebih memudahkan investigator dalam melakukan pengumpulan digital untuk proses persidangan.

2. TINJAUAN PUSTAKA

Langkah ini memuat beberapa teori yang mendukung metode usulan untuk menyelesaikan masalah dan/atau mengembangkan metode, didukung dengan referensi serta sumber yang jelas dan referensi yang terbaru.

2.1. Media Sosial

Perbedaan pertama yang harus dibuat adalah antara situs web atau situs media sosial dan layanan media sosial. Pada dasarnya semua media sosial dapat diakses melalui web browser, namun beberapa perusahaan menawarkan layanan lain seperti android. Ada beberapa jenis media sosial di antaranya (Golbeck 2015):

1. Facebook sudah memiliki 1,2 miliar pengguna aktif. Ini pada dasarnya adalah situs jejaring sosial, tetapi menawarkan banyak fitur mulai dari bermain game hingga mengobrol hingga email, menjadikannya tujuan utama banyak orang di internet.

2. Twitter merupakan halaman microblogging yang sudah memiliki sekitar 300 juta pengguna. Orang membangun hubungan sosial dengan mengikuti orang yang kontennya menarik bagi mereka. Pesan disebut "tweet".
3. YouTube adalah situs web berbagi video paling populer. YouTube dimiliki oleh Google, yang pada gilirannya memiliki sistem masuk tunggal untuk semua layanannya. Selain itu, pengguna dapat menonton video di YouTube meskipun tidak memiliki akun. Oleh karena itu, peringkat pengguna tidak masuk akal di sini
4. Instagram - Situs berbagi foto yang sangat populer di kalangan remaja saat ini. Itu tidak dimiliki oleh Facebook dan tidak terintegrasi dengan platform Facebook. Instagram memiliki sekitar 85 juta pengguna.

2.2. Digital Forensik

Forensik digital adalah bidang ilmu forensik yang menggunakan pengetahuan ilmiah untuk mengumpulkan, menganalisis, mencatat, dan menyajikan bukti digital terkait kejahatan komputer untuk digunakan dalam proses peradilan. Tujuan utamanya adalah mengetahui apa yang dilakukan, kapan dilakukan dan siapa yang melakukannya. Istilah "forensik digital" secara luas digunakan sebagai sinonim untuk forensik komputer, namun telah diperluas untuk mencakup penyelidikan semua perangkat yang mampu menyimpan data digital, seperti perangkat jaringan, ponsel, tablet, kamera digital, , perangkat Internet of Things (IoT) dan lainnya. Digital forensik juga bertanggung jawab untuk menyelidiki hampir semua serangan dalam kejahatan cyber terhadap sistem komputer seperti ransomware, phishing, SQL injection, DDoS, pencurian data, spionase yang merugikan bisnis atau reputasi (Hassan 2019).

Proses digital forensik terdiri dari 4 fase yaitu *collection*, *Examination*, *Analysis*, dan *Reporting* (Kent et al. 2006).



Gambar 1. Digital Forensik Proses

2.3. Hunchly

Hunchly adalah alat penangkap web yang dirancang khusus untuk investigasi online. Hunchly secara diam-diam berjalan di browser web Anda dan secara otomatis mengumpulkan,

mendokumentasikan, dan memberi anotasi pada setiap situs web yang Anda kunjungi. Dengan menggunakan alat ini, Anda tidak akan pernah lupa mengambil screenshot, cut and paste a URL, atau menyimpan dokumen saat menjelajah (Hunchly 2023).

3. PEMBAHASAN

Metode penyelesaian kasus untuk proses investigasi forensic pada penelitian ini menggunakan digital Forensik proses. Proses awal sampai akhir akan menggunakan metode ini.



Gambar 1. Metode Penelitian

3.1. Collection

Proses awal forensik digital adalah mengidentifikasi sumber data yang potensial untuk memperoleh data lainnya. Proses ini akan mengumpulkan data dari sumber yang tersedia, Sumber data yang paling jelas dan umum adalah komputer desktop, server, perangkat penyimpanan jaringan, dan laptop. Sistem ini biasanya memiliki drive internal yang menerima media, seperti CD dan DVD, dan juga memiliki beberapa jenis port (misalnya, Universal Serial Bus [USB], Firewire, Personal Computer Memory Card International Association [PCMCIA]) tempat penyimpanan data eksternal media dan perangkat dapat dilampirkan. Dalam kasus media sosial, sumber data yang dimaksud adalah akun media sosial dan meta data yang terdapat dari akun tersebut.

3.2. Examination

Setelah proses pengumpulan data selesai, langkah selanjutnya yaitu proses verifikasi data yang menjadi bukti digital, yang meliputi proses evaluasi dan penggalian informasi yang memiliki relevansi dari data atau bukti yang dikumpulkan. Proses ini melibatkan penghapusan atau minimalisasi fitur

sistem operasi atau aplikasi yang mengaburkan data dan kode, seperti kompresi data, enkripsi, dan mekanisme akses kontrol.

Mengidentifikasi file data yang berisi informasi penting, termasuk informasi yang dikaburkan oleh proses compress file dan akses control, salah satu tugas yang sulit. File data yang terpengaruh mungkin akan berisi informasi tidak relevan yang perlu disaring, seperti log firewall yang berisi jutaan catatan, namun hanya beberapa yang memiliki keterkaitan dengan peristiwa atau data yang telah dikumpulkan. Namun, berbagai tools dan teknik dapat digunakan oleh penyidik untuk mengurangi jumlah data yang perlu disortir. Pencarian teks dan pola dapat digunakan untuk mengidentifikasi data terkait, misalnya, untuk menemukan dokumen yang merujuk pada topik atau orang tertentu, atau untuk mengidentifikasi entri log email untuk alamat email secara spesifik.

3.3. *Analysis*

Setelah informasi yang relevan telah diekstraksi, analis harus mempelajari dan menganalisis data untuk menarik kesimpulan dari data yang telah di kumpulkan. Fondasi forensik harus menggunakan pendekatan metodis untuk mencapai kesimpulan yang tepat berdasarkan dari data yang tersedia atau menentukan bahwa belum ada kesimpulan yang dapat ditarik. Proses analisis akan mencakup proses identifikasi orang, tempat, barang, dan peristiwa, dan menentukan bagaimana komponen tersebut memiliki keterkaitan satu sama lain sehingga kesimpulan dapat dicapai dan dapat dipertanggung jawabkan dalam proses persidangan.

3.4. *Report*

Tahap terakhir yang dilakukan adalah proses pelaporan, yaitu proses penyusunan serta penyajian informasi yang dihasilkan dari tahap analisis. Banyak faktor yang memengaruhi pelaporan, termasuk yang berikut:

1. Pelaporan Alternatif. Ketika informasi tentang suatu peristiwa tidak lengkap, tidak mungkin untuk sampai pada penjelasan yang pasti tentang apa yang terjadi. Ketika suatu peristiwa memiliki dua atau lebih penjelasan yang masuk akal, masing-masing harus dipertimbangkan dalam proses pelaporan. Analis harus menggunakan pendekatan metodis untuk mencoba membuktikan atau menyangkal setiap kemungkinan penjelasan yang diajukan.
2. Pertimbangan Audiens. Audiens yang memahami data atau informasi akan ditampilkan adalah penting. Kejadian yang membutuhkan keterlibatan penegak hukum membutuhkan laporan yang sangat detail dari semua informasi yang dikumpulkan, dan mungkin juga memerlukan salinan dari semua data bukti yang diperoleh. Administrator sistem mungkin ingin melihat lalu lintas jaringan dan

statistik terkait dengan sangat detail. Manajemen senior mungkin hanya menginginkan tinjauan tingkat tinggi tentang apa yang terjadi, seperti representasi visual yang disederhanakan tentang bagaimana serangan itu terjadi, dan apa yang harus dilakukan untuk mencegah insiden serupa.

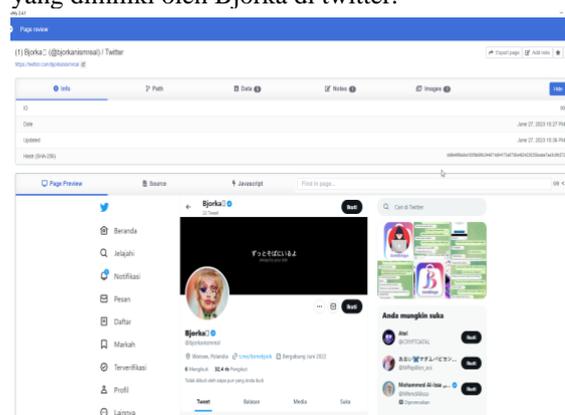
Proses report juga memerlukan identifikasi informasi yang dapat ditindaklanjuti yang diperoleh dari data yang memungkinkan seorang analis untuk mengumpulkan sumber informasi yang terbaru. Misalnya, daftar kontak dapat dikembangkan dari data yang mungkin mengarah pada informasi tambahan tentang suatu insiden atau kejahatan. Selain itu, informasi dapat diperoleh yang dapat mencegah kejadian di masa mendatang, seperti pintu belakang pada sistem yang dapat digunakan untuk serangan di masa mendatang, kejahatan yang sedang direncanakan, worm yang dijadwalkan untuk mulai menyebar pada waktu tertentu, atau kerentanan yang dapat dieksploitasi

4. PEMBAHASAN

Pada penelitian ini, studi kasus untuk proses investigasi di media sosial adalah melakukan proses investigasi akun twitter @bjorka. Akun ini sering melakukan penyerangan terhadap pemerintah dan memberikan informasi terhadap kebocoran data Bank Syariah Indonesia.

4.1. *Collection*

Proses Collection ini merupakan tahap awal dalam melakukan investigasi. Pada proses investigasi ini hal pertama adalah mencari akun media sosial yang dimiliki oleh Bjorka di twitter.



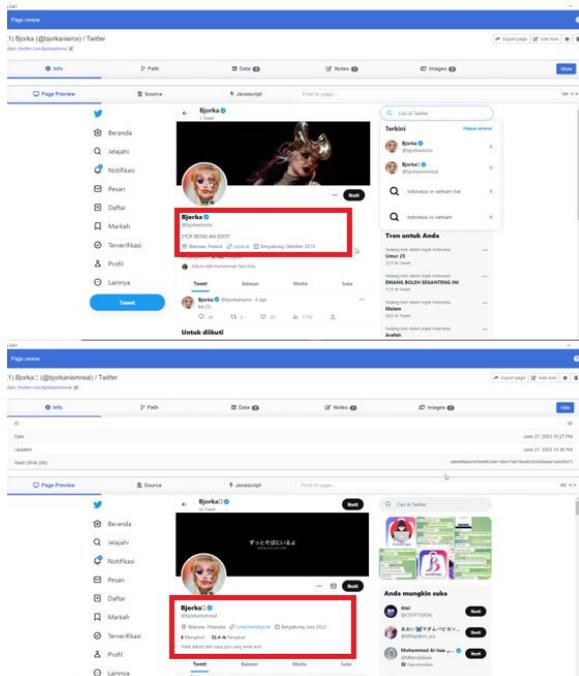
Gambar 3. Akun Bjorka

Dari proses collection data, akun twitter Bjorka ini memiliki nama @bjorkanismreal. Akun ini berlokasi di Warsaw, Polandia dan mulai bergabung dengan twitter pada juni 2022.

4.2. *Examination*

Tahapan selanjutnya adalah melakukan proses Examination. Proses ini akan memeriksa data, yang melibatkan penilaian dan penggalian informasi yang

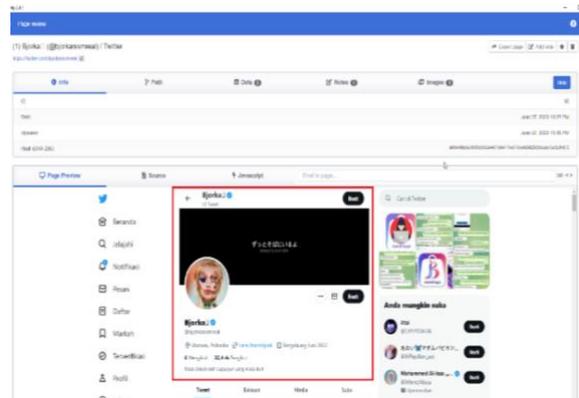
relevan dari data yang dikumpulkan. Dari proses pemeriksaan data akun twitter bjorka ini, terdapat dua akun Bjorka yang ada di twitter. Akun pertama dengan nama @bjorkanismreal dan akun kedua dengan nama @bjorkanismx. Namun dari hasil perbandingan dari dua akun ini, akun Bjorka dengan nama @bjorkanismreal yang paling terbaru dan aktif digunakan. Hal ini terlihat dari postingan pada beranda akun tersebut.



Gambar 4. Perbandingan dua akun Bjorka

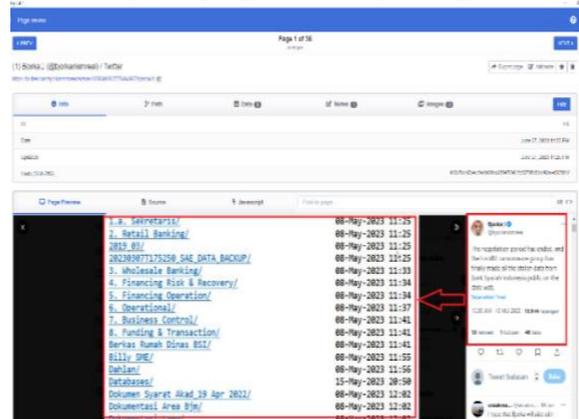
4.3. Analysis

Tahap selanjutnya adalah dilakukan proses analisis terhadap akun Bjorka ini. Proses analisis ini harus mempelajari dan menganalisis data untuk menarik kesimpulan dari data yang telah di kumpulkan. Analisis data awal yang dilakukan adalah melakukan pengecekan meta data dari akun @bjorkanismreal. Dari hasil pengecekan meta data, diperoleh informasi bahwa akun ini di buat pada juni 2022, memiliki lokasi di Warsaw, Polandia dan memiliki grub telegram dengan link <https://t.me/itsmebjork>. Akun ini juga memiliki 32,4 rb Pengikut dan 6 akun yang di ikuti di twitter. Seperti yang terlihat pada gambar 5.



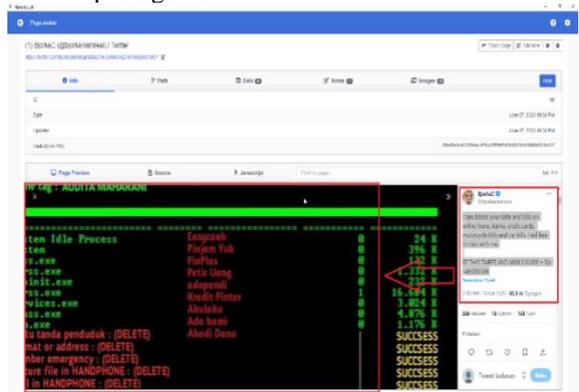
Gambar 5. Metadata akun Bjorka

Dari hasil pemeriksaan terhadap beranda akun @bjorkanismreal ditemukan beberapa postingan akun tentang penjualan data dan pembocoran data dari Bank Syariah Indonesia. Seperti pada tweet nya "The negotiation period has ended, and the LockBit ransomware group has finally made all the stolen data from Bank Syariah Indonesia public on the dark web." Seperti yang terlihat pada gambar 6.



Gambar 6. Negosiasi kebocoran data Bank BSI

Selain itu, akun Bjorka ini juga menawarkan pilihan untuk proses penghapusan data dan tagihan pada pinjaman online, bank, kartu kredit, tagihan motor dan tagihan mobil seperti terlihat pada tweetnya "I can delete your data and bills on online loans, banks, credit cards, motorcycle bills and car bills. Feel free to chat with me. RT THIS TWEET AND WIN \$10.000 = Rp 149.000.000" seperti yang terlihat pada gambar 7.



Gambar 7. Penawaran untuk penghapusan Credit Card

4.4. Report

Tahapan terakhir yang dilakukan adalah report. Proses pelaporan ini dilakukan agar bukti yang telah dikumpulkan itu dapat diterima pada proses pengadilan. Dalam proses report ini barang bukti yang ditemukan harus dijelaskan secara rinci. Salah satu tindakan agar barang bukti dapat diterima di persidangan adalah, barang bukti tersebut harus dicatat secara detail bagaimana cara mendapatkannya dan bagaimana cara pemrosesan dari barang bukti tersebut. Untuk itu perlu dilakukan manajemen barang bukti dengan menerapkan dokumen chain of custody. Dokumen chain of custody ini belum memiliki standarisasi yang baku. Salah satu model dokumen chain of custody yang dapat digunakan dapat terlihat pada gambar 8.

| FORMULIR PENERIMAAN BARANG BUKTI ELEKTRONIK | | | |
|---|-------------------|----------------|-------|
| Informasi Kasus ⁽¹⁾ | | | |
| No. Kasus : | | Hari/Tanggal : | |
| Lokasi Kasus : | | | |
| Yang Menyerahkan ⁽²⁾ | | | |
| Nama Jelas | Hari/Tanggal | Jam | Paraf |
| 1. Muhammad Innuddin | Senin, 25/08/2015 | 14:30:-- WIB | ---- |
| 2. | | | |
| 3. | | | |
| Yang Menerima ⁽³⁾ | | | |
| Nama Jelas | Hari/Tanggal | Jam | Paraf |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| Deskripsi Singkat Kasus ⁽⁴⁾ : | | | |
| | | | |

Gambar 8. Dokumen Chain Of Custody

5. KESIMPULAN DAN SARAN

Hasil yang diperoleh dalam penelitian ini adalah dengan memanfaatkan metode digital forensik proses dan penggunaan tools hunchly untuk melakukan teknik live investigation, berhasil mengumpulkan bukti digital dari akun-akun media sosial yang melakukan tindak kejahatan di media sosial sehingga dapat di proses sesuai dengan prosedur hukum yang ada. Keunggulan dari penelitian ini dari penelitian sebelumnya adalah penelitian ini bisa secara langsung mencapture bukti digital dari akun media sosial dengan metode live investigation.

Saran untuk penelitian selanjutnya, proses pengujian bisa menggunakan tools OSINT lain.

DAFTAR PUSTAKA

APPJI. 2023. *Survei Penetrasi Dan Perilaku Internet 2023*.
 Arshad, Humaira, Aman Jantan, and Esther Omolara. 2019. 'Evidence Collection and Forensics on Social Networks: Research Challenges and Directions'. *Digital Investigation* 28: 126–38.

<https://linkinghub.elsevier.com/retrieve/pii/S1742287618302937>.
 David, Anne. 2020. 'A Two-Stage Model for Social Network Investigations in Digital Forensics'. *The Journal of Digital Forensics, Security and Law*.
 Golbeck, Jennifer. 2015. *Introduction to Social Media Investigation: A Hands-on Approach*. Syngress.
 Hassan, Nihad A. 2019. *Digital Forensics Basics Digital Forensics Basics 'A Practical Guide Using Windows OS'*.
 Hunchly. 2023. 'Hunchly Dark Web Investigation Guide'.
 Kent, K, S Chevalier, T Grance, and H Dang. 2006. 'Guide to Integrating Forensic Techniques into Incident Response'. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>.
 Kusuma, M, D Hariyadi, Fazlurrahman, and M A Nugroho. 2021. 'The Bibliometric Analysis the Digital Forensics Researcher in Indonesia Based on Garba Rujukan Digital: 2008–2020'. In *2021 IEEE Mysore Sub Section International Conference (MysuruCon)*, , 13–17.
 Montasari, Reza, Richard Hill, Victoria Carpenter, and Farshad Montasari. 2018. 'Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence'. *International Journal of Strategic Engineering* 2(1): 52–60.
 Mustapha, Rabi, and Muhammad Aminu Ahmad. 2022. *Digital Forensic Investigation of Cyberstalking and Social Media Harassment Using Network Forensic Analysis PhD Project View Project Knowledge Management in Pandemic View Project*. www.atbuftejoste.com.
 Palupi, Rety. 2019. 'Penyalahgunaan Media Sosial Sebagai Alat Propaganda'. *Jurnal Komunikasi* 10(1): 69–76. <http://ejournal.bsi.ac.id/ejurnal/index.php/jkom>.
 Pomalingo, Suwito, Bambang Sugiantoro, and Yudi Prayudi. 2019. 'Data Visualisasi Sebagai Pendukung Investigasi Media Sosial'. *ILKOM Jurnal Ilmiah* 11(2): 143–51.
 Sanduni, W, and Shashipraba Perera. 2020. *Investigation of Social Media Security: A Critical Review*. <https://www.researchgate.net/publication/349944503>.
 Setyaningsih, Rila et al. 2021. *Model Penguatan Literasi Digital Melalui Pemanfaatan E-Learning*.
 Stodelov, Denis, and Natalia Miloslavskaya. 2022. 'Open Source INTelligence Tools'. In *Procedia Computer Science, Elsevier B.V.*, 83–88.