CHAIN OF CUSTODY UNTUK ARTEFAK SOSIAL MEDIA FORENSIK

Virjayanti Lazinu
19917038

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2023

Lembar Pengesahan Pembimbing

***Chain Of Custody* untuk Artefak Sosial Media Forensik**

Virjayanti Lazinu
19917038

Yogyakarta, 06 Mei 2023

Pembimbing 1	Pembimbing 2
Dr. Bambang Sugiantoro, S.Si., MT	Dr. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

***Chain Of Custody* untuk Artefak Sosial media Forensik**

VIRJAYANTI LAZINU

19917038

Yogyakarta, 18 Mei 2023

Tim Penguji,

Dr. Ir. Bambang Sugiantoro, S.Si., MT.
Ketua

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

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

Mengetahui,

Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

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

Abstrak

Chain Of Custody Untuk Artefak Sosial Media Forensik

Sosial media menjadi sangat populer dikalangan masyarakat saat ini, dan semakin banyaknya penggunaan sosial media tentu saja berdampak baik atau buruk bagi jalannya kehidupan manusia, misalnya dampak buruknya adalah melakukan penipuan, *cyberbully* atau mengobrol di sosial media yang biasa disebut kejahatan siber. Tren kejahatan siber yang melibatkan internet, komputer atau ponsel sebagai media atau target kejahatan terus mengalami peningkatan, Untuk itu barang bukti pada kasus siber dibagi menjadi dua jenis yaitu barang bukti fisik (elektronik) dan barang bukti digital. Forensik digital merupakan salah satu ilmu untuk menangkap pelaku kejahatan secara digital yang akan dibutuhkan dalam pembuktian di pengadilan selama proses investigasi, Agar dapat digunakan dalam proses penegakan hukum, barang bukti harus terjaga dan sama persis seperti ketika pertama kali ditemukan. Salah satu pembuktian ilmiah yang dapat digunakan adalah memastikan informasi kronologis barang bukti dalam dokumen *Chain Of Custody*. Selama ini belum terdapat standar/regulasi yang menjadi acuan utama bagi organisasi/instansi penegak hukum dalam melakukan aktivitas dan menentukan kebutuhan informasi *Chain Of Custody* untuk barang bukti digital.

Penelitian ini, bertujuan untuk menghasilkan dokumentasi *Chains of Custody* dari hasil investigasi *cyber crime* dengan menggunakan *software* Hunchly dan metode *National Institute Standard and Technology* (NIST). Untuk mengidentifikasi dan memodelkan informasi, pendekatan normalisasi diterapkan terhadap beberapa formulir *Chain Of Custody* untuk kejahatan siber atau kejahatan komputer. Sehingga diharapkan dengan adanya konsep *Chain Of Custody* untuk Artefak Sosial media Forensik dapat membantu penyelidikan dalam penanganan bukti digital yang terjadi di sosial media agar terjaga dan sama persis seperti ketika pertama kali ditemukan

Kata kunci

Sosial media, Bukti Digital, Chain Of Custody, Forensik, Metode National Institute Standard and Technology

Abstract

Chain Of Custody For Forensic Sosial Artefects

Sosial media is becoming very popular among this society, and the more and more use of sosial media alone has a good or bad impact on human life, for example the bad impact is committing fraud, or committing crimes on sosial media which are commonly called cyber crimes. The trend of cyber crime involving the internet, computers or mobile phones as media or crime targets continues to increase. For this reason, evidence in cyber cases is divided into two types, namely physical evidence (electronic) and digital evidence. Digital forensics is one of the sciences for capturing crimes digitally which will be needed in evidence in court during the investigation process. In order to be used in the law enforcement process, evidence must be preserved and is the same as when it was first found. One of the scientific evidences that can be used is to ensure the chronological information of the evidence in the *Chain Of Custody* document. So far, there are no standards/regulations that become the main reference for law enforcement organizations/agencies in carrying out activities and determining the need for information chains for digital evidence. This study aims to produce Chains of Custody documentation from the results of cyber crime investigations using Hunchly software and the National Institute Standard and Technology (NIST) method. To identify and model information, a normalized approach is applied to multiple *Chain Of Custody* forms for cybercrimes or computer crimes. It is hoped that with the *Chain Of Custody* concept for Forensic Sosial Artifacts, media can assist investigations in handling digital evidence that occurs on sosial media so that they are maintained and are the same as when they were first discovered.

Keywords

Sosial media, Digital Evidence, *Chain Of Custody*, Forensics, Methods National Institute of Standards and Technology

Pernyataan Keaslian Tulisan

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

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

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

Yogyakarta, 18 Mei 2023

Virjayanti Lazinu

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Lazinu, V, Sugiantoro, B, Prayudi, Y. 2023. *Chain Of Custody* untuk Artefak Sosial media Forensik. JUSTI (Jurnal Sains Terapan Teknologi Informasi)

Kontributor	Jenis Kontribusi
Virjayanti Lazinu	Mendesain eksperimen (60%) Menulis *paper* (70%)
Dr. Bambang Sugiantoro, S.Si., MT	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)
Yudi Prayudi, S.Si., M.Kom	Melakukan evaluasi dan analisis

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

بسم الله الرحمن الرحيم

"Dengan rahmat Allah yang Maha Pengasih lagi Maha Penyayang,"

Persembahan sujud syukur hanya kepada Engkau pencipta alam semesta. Tesis ini saya persembahkan untuk :

Kedua orang tua saya, Bapak H. Jamal dan Ibu Hj. Samria yang telah sabar & berkorban lebih dari segala apapun demi anaknya.

Kakak saya yang selalu memberikan masukan dan arahan untuk adiknya ini.

Adik-adik saya yang selalu mendukung dan mendorong kakaknya untuk menjadi seseorang yang sukses, beserta dengan keluarga besar saya almarhum kake Lazinu.

نمحرال كرابت

Sebuah persembahan untuk keluarga tercinta, sebagai bukti kesungguhan penulis dalam menimba ilmu, sekaligus motivasi bagi para penerus.

Kata Pengantar

Assalamu'alaikum warahmatullahi wabarakatuh

Alhamdulillah, puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, serta kasih sayang-Nya. Sholawat dan salam senantiasa tercurah kepada junjungan dan uswatun hasanah kita, Nabi Muhammad SAW. Atas rahmat Allah SWT yang Maha Pemurah, penulis dapat menyelesaikan thesis dengan judul "*Chain Of Custody* Untuk Artefak Sosial Media Forensik". Tesis ini disusun untuk memenuhi persyaratan guna mencapai derajat Magister (Strata II/ S2) Program Studi Magister Informatika di Universitas Islam Indonesia. Penulis menyadari sepenuhnya jika tanpa adanya bantuan dari berbagai pihak, maka penulis tidak akan menyelesaikan tesis ini dengan baik. Oleh karena itu, selain rasa syukur yang tiada henti tercurah, izinkan penulis dengan tulisan ini untuk menyampaikan segenap terimakasih kepada :

1. Allah SWT, atas segala kesempatan, kekuatan dan seluruh hal yang diberikan kepada penulis hingga detik ini.
2. Kedua orang tua tercinta serta seluruh keluarga kami. Terimakasih atas do'a, bimbingan dan nasehat yang tiada pernah ada habisnya.
3. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., selaku Rektor Universitas Islam Indonesia yang memberikan kesempatan pada penulis untuk menempuh Pendidikan serta memberikan motivasi di Universitas Islam Indonesia.
4. Bapak Prof. Dr. Ir. Hari Purnomo, MT., selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan motivasi dalam proses menempuh Pendidikan di Universitas Islam Indonesia.
5. Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D., selaku Ketua Program Studi Informatika Program Magister Fakultas Industri Universitas Islam Indonesia yang selaku memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
6. Bapak Dr. Ir. Bambang Sugiantoro, S.Si.,MT selaku dosen pembimbing sekaligus Dewan Penguji yang selalu memberikan arahan, motivasi semangat dan do'a selama kegiatan penelitian dan penyusunan tesis.
7. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. dan Bapak, Dr. Yudi Prayudi, S.Si., M.Kom. selaku Anggota Dewan Penguji I dan II yang telah memberikan kritik dan saran yang membangun, dukungan, serta nasihat yang amat berarti. Terimakasih atas ilmu dan pengetahuan yang telah diberikan

8. Bapak dan Ibu Dosen Program Studi Magister Informatika Universitas Islam Indonesia yang telah mendidik dan memberikan bekal pengetahuan selama kegiatan perkuliahan atau praktikum. Semoga menjadi amal jariyah di akhirat kelak.
9. Kakak dan Adik-adik Tercinta, Kakak Syahrul Layali Lazinu, S.M dan Adik Serda Muh. Munawir Lazinu, Zikra mayada Lazinu, Lutfiatul Isyara Lazinu.
10. Seluruh teman teman seperjuangan Keluarga Besar Mahasiswa Program Studi Magister Informatika Universitas Islam Indonesia atas semua dukungan dan doa.
11. Kepada seluruh sahabat, teman dan orang-orang yang mengenal penulis - baik hanya singgah maupun bertahan hingga sekarang yang tidak bisa kami sebutkan satu persatu. Terimakasih sudah hadir dan memberikan banyak pelajaran dalam kehidupan.
12. Serta tidak lupa untuk mengucapkan terima kasih kepada diri sendiri, karena telah mampu menyelesaikan masa studi dengan baik.

Penulis ucapkan terima kasih. Semoga Allah SWT membalas kebaikan dari berbagai pihak yang kami sebutkan dengan berkah-Nya. Penulis berharap tesis ini dapat bermanfaat untuk para pembaca sekalian. Apabila ada kekurangan dalam penulisan, penulis menyampaikan permohonan maaf yang sebesar besarnya. Oleh karena tidak sempurnanya tesis ini, penulis berharap kritik dan saran yang membangun untuk perbaikan penulis selanjutnya.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Yogyakarta, 18 Mei 2023

Hormat Saya

Virjayanti Lazinu

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

COC	- *Chain Of Custody*
UU ITE	- Undang-undang Informasi dan Transaksi Elektronik
SOP	- Standar Operasioanl Prosedur
EDI	- Electronic Data Interchange
TKP	- Tempat Kejadian Perkara
PPBB	- Petugas Pengelolah Barang Bukti
CRC	- Checksum Redundancy Check
NIST	- National Institute of Standart Technology
URL	- Uniform Resource Location

BAB 1
Pendahuluan

1.1 Latar Belakang

Sosial media adalah sebuah media online, yang penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, wiki, forum dan dunia virtual. Blog, jejaring sosial dan wiki merupakan bentuk sosial media yang paling umum digunakan oleh masyarakat di seluruh dunia. Dampak positif dari sosial media adalah memudahkan kita untuk berinteraksi dengan banyak orang, memperluas pergaulan, jarak dan waktu bukan lagi masalah, lebih mudah dalam mengekspresikan diri, penyebaran informasi dapat berlangsung secara cepat, biaya lebih murah. Sedangkan dampak negatif dari sosial media adalah menjauhkan orang-orang yang sudah dekat dan sebaliknya, interaksi secara tatap muka cenderung menurun, membuat orang-orang menjadi kecanduan terhadap internet, menimbulkan konflik, masalah privasi, rentan terhadap pengaruh buruk orang lain (Hadiah et al., 2016). Salah satu permasalahan yang tak luput dari sosial media adalah tindak kejahatan dunia maya yang memanfaatkan sosial media, karena pada dasarnya tidak ada kejahatan yang tidak meninggalkan jejak. Hal tersebut menimbulkan sebuah tren kejahatan baru yang melibatkan internet dan komputer atau *smartphone* baik sebagai media maupun sebagai sasaran dari tindak kejahatan yang dikenal dengan istilah *cyber crime*..

Saat ini *cyber crime* memiliki dua jenis barang bukti, yaitu: bukti fisik dan bukti digital. Barang bukti fisik (elektronik) adalah semua perangkat elektronik yang dapat digunakan untuk kepentingan aktivitas *cyber crime* atau perangkat lain yang dapat merekam jejak dari kegiatan *cyber crime* tersebut, misalnya harddisk, CD, pendrive, cctv, komputer, RAM, handphone dll. Sedangkan barang bukti digital adalah konten digital hasil akuisisi dan ekstraksi dari barang bukti fisik (elektronik). Bukti digital juga dapat berupa file bukti digital hasil ekstraksi (full copy) bit per bit dari media penyimpanan yaitu *hard drives*, *flash drives*, *floppy disk* dan optical media yang dikenal dengan istilah Disk Image. Sehingga pada bukti fisik membutuhkan sebuah ruang khusus yang dapat menampung bukti fisik tersebut. Sedangkan pada bukti digital tidak membutuhkan ruang khusus, namun dibutuhkan sebuah sistem yang dapat menyimpan dan mengelola bukti digital tersebut.

Aspek penting dalam penanganan barang bukti adalah apa yang disebut dengan *Chain Of Custody* (rantai barang bukti), yaitu kronologis pendokumentasian barang bukti. Barang bukti harus dijaga integritas tingkat keasliannya sesuai dengan kondisi ketika

pertama kali ditemukan hingga kemudian nantinya dipresentasikan dalam proses persidangan. Lingkup dari *Chain Of Custody* meliputi semua individu yang terlibat dalam proses akuisisi, koleksi, analisis bukti, catatan waktu serta informasi kontekstual meliputi labeling kasus, unit dan laboratorium yang memproses barang bukti (Prayudi, 2014).

Salah satu *issue* dalam *Chain Of Custody* adalah masalah integritas data. Dalam hal ini menurut Vanstode dalam (Ćosić & Bača, 2011), digital integrity adalah sebuah property di mana data digital tidak mengalami perubahan oleh pihak yang tidak memiliki wewenang otorisasi melakukan perubahan. Perubahan dan kontak kepada barang bukti digital hanya dilakukan oleh mereka yang memiliki otorisasi saja. Integritas barang bukti digital menjamin bahwa informasi yang dipresentasikan adalah lengkap dan tidak mengalami perubahan dari sejak pertama kali ditemukan sampai akhir digunakan dalam proses persidangan.

Dalam kasus hukum, ketika dalam proses persidangan diperlukan untuk menunjukkan secara fisik barang bukti, maka pihak penegak hukum harus dapat menunjukkan dengan kondisi yang sesuai dengan penjelasan pada materi dalam tuntutan. *Chain Of Custody* juga harus memuat dokumentasi terkait dengan perjalanan dan penggunaan dari barang bukti, misalnya ketika barang bukti dikeluarkan dari tempat penyimpanannya untuk kepentingan analisis atau proses penyidikan harus terekam dalam catatan *Chain Of Custody* yang menyertai barang bukti tersebut.

Chain Of Custody akan mendokumentasikan persyaratan yang terkait dengan tempat, kapan, mengapa, siapa, bagaimana dalam penggunaan bukti pada setiap tahap proses investigasi. Masalah Chain Of Custody menjadi sangat penting sebagai keaslian bukti yang harus dipertahankan sesuai dengan kondisi ketika pertama kali ditemukan sampai kemudian disajikan di pengadilan. Lingkup Chain Of Custody mencakup semua individu yang terlibat dalam proses akuisisi, pengumpulan, analisis bukti, catatan waktu serta informasi kontekstual, yang mencakup pelabelan kasus, dan unit dan laboratorium yang memproses bukti.

Dalam forensik digital, bukti digital yang diperoleh dari sosial media akan sangat bermanfaat. Banyaknya informasi berupa data-data pribadi yang secara tidak sadar dipublikasikan di sosial media dapat digunakan penyidik sebagai barang bukti potensial untuk melacak kejahatan di media sosial. Data yang dipublikasikan tersebut dapat digunakan sebagai bukti langsung untuk menunjukkan keterlibatan seseorang dalam pelanggaran. Selain itu, data-data yang berada dalam ruang lingkup sosial media menawarkan informasi yang cukup banyak untuk mengetahui tentang motif dari setiap tindakan kejahatan yang dilakukan (Arshad et al., 2019).

Informasi di sosial media yang berasal dari pengguna sosial media yang telah tersebar luas, sering kali tidak disadari oleh pengguna sosial media. Informasi-informasi berupa profil dari pengguna sosial media sangat mudah untuk diakses seperti jejaring sosial Twitter, Facebook, Instagram, Linkedin dan lain-lain. Dalam proses analisis sosial media melibatkan empat langkah berbeda yaitu penemuan data, pengumpulan, persiapan, dan analisis (Stieglitz et al., 2018). Selain itu data yang beredar di sosial media dapat dibagi menjadi empat kategori, yaitu pengguna, aktivitas, jaringan dan konten (Arshad et al., 2019). Jejak informasi digital di sosial media, jika dieksplorasi dengan benar, dapat memberikan informasi yang luar biasa dalam penyelidikan kriminal. Namun, mengeksplorasi sosial media untuk bukti potensial dan menghadirkan bukti-bukti ini di pengadilan bukanlah tugas yang mudah. Pencarian barang bukti dari sosial media memiliki tantangan karena perkembangan perangkat teknologi dan efektivitas forensik digital yang terus berkembang (Garfinkel, 2010). Bukti digital yang berasal dari sosial media harus dikumpulkan sesuai dengan aturan hukum yang berlaku serta ilmiah, sehingga tidak bertentangan dengan hak privasi individu. Tantangan yang muncul dalam pengumpulan bukti dari sosial media adalah autentikasi dari bukti digital yang telah dikumpulkan

Sementara itu, Penelitian yang dilakukan oleh (Putra & Prayudi, 2021) membuktikan bahwa penerapan *multi smart contract* ditemukan bahwa bukti digital memiliki karakteristik berbeda-beda dan detail informasi yang berbeda-beda antara satu jenis bukti digital gambar, audio, video, dan dokumen atau jenis bukti digital lainnya. Informasi yang detail mampu meningkatkan integritas bukti digital. Otomatisasi dalam membuat hash dan ekstraksi informasi dari suatu bukti digital dapat mengurangi waktu *first responder* dalam penginputan form isian pada sistem *multi smart contract*. Penyimpanan bukti digital di luar blok dapat meningkatkan performa sistem *multi smart contract*. Penyimpanan bukti digital yang hanya berupa alat bukti persidangan mampu mengoptimalkan media penyimpanan bukti digital.

Penelitian tentang solusi *Chain Of Custody* dilakukan oleh (Cosic, 2017b) Solusi yang diberikan masih belum sepenuhnya sesuai dengan kebutuhan penanganan *Chain Of Custody*, terutama sekali dalam hal model untuk meniru konsep pencatatan dan dokumentasi barang bukti. Untuk itu, maka masih terbuka peluang penelitian lainnya dalam mengatasi permasalahan *Chain Of Custody*. Oleh sebab itu, penulis ini memberikan salah satu solusi yang diusulkan untuk memberikan kontribusi bagi penanganan dan penyimpanan bukti digital.

Ada banyak tools lainnya yang bisa digunakan untuk proses akuisisi bukti digital pada penelitian ini dokumentasi *Chain Of Custody* pada sosial media Facebook untuk barang

bukti fisik dan barang bukti digital karena untuk membatasi tujuan pada penelitian ini. Pada suatu kasus kejahatan teknologi komputer yang terjadi pada umumnya akan meninggalkan jejak aktivitas kejahatan. Jejak aktivitas yang terkait dengan tindak kejahatan tersebut dapat dijadikan sebagai barang bukti. Barang bukti kejahatan komputer dapat berupa barang bukti elektronik dan barang bukti digital. Barang bukti elektronik dapat berupa bentuk fisik dari perangkat elektronik tersebut atau dapat berupa media simpan, sedangkan barang bukti digital dapat berupa file dokumen, file history, atau file log yang berisikan data-data terkait yang dapat dijadikan sebagai informasi pendukung pengambil keputusan. Barang bukti elektronik dan barang bukti digital menjadi hal terpenting dalam suatu kasus kejahatan komputer, karena aktivitas tindak kejahatan komputer yang dilakukan terekam oleh sistem komputer pada media penyimpanan utama perangkat komputer

Dokumentasi *Chain Of Custody* untuk barang bukti fisik dan barang bukti digital seharusnya memiliki konsep dan informasi yang sama. Sedangkan pada prakteknya, mekanisme dokumentasi *Chain Of Custody* untuk barang bukti digital berbeda dengan barang bukti fisik karena adanya perbedaan karakteristik (Luthfi & Prayudi, 2016). Praktek dokumentasi *Chain Of Custody* untuk barang bukti fisik pada Perkap (Peraturan Kepala Kepolisian Indonesia) No 10 Tahun 2010 selama ini dilakukan dengan menggunakan berita acara, buku kontrol dan buku register. Selanjutnya untuk melakukan dokumentasi barang bukti digital, salah satu konsep yang dapat digunakan untuk mendukung dokumentasi *Chain Of Custody* bukti digital adalah menggunakan konsep metadata (Prayudi & SN, 2015b)

Sejumlah penelitian telah dilakukan sebagai upaya untuk mengimplementasikan konsep *digital Chain Of Custody*. Namun demikian mengingat karakteristik barang bukti digital terus berkembang dan semakin kompleks maka penelitian untuk memberikan solusi bagi konsep digital *Chain Of Custody* masih merupakan sebuah *challenge* dan *open problem* pada bidang *forensika digital*.

Permasalahan yang selama ini muncul adalah barang bukti tersebut tidak terdokumentasi dan terkordinir dengan baik sesuai dengan kasus yang dihadapi. Hal ini dapat melemahkan pembuktian suatu kasus berdasarkan bukti digital tersebut di Pengadilan. Beberapa hal yang bisa menyebabkan barang bukti menjadi tidak diterima yaitu proses ekstraksi atau pengambilan barang bukti yang tidak profesional, tidak ada kesesuaian antara perkara dengan alat bukti yang ditampilkan, atau tidak terdokumentasinya dengan baik antara kasus yang sedang ditangani dengan bukti-bukti yang didapatkan di TKP (Efendi, 2019b).

Pembuatan *framework Chain Of Custody* bukti digital dengan konsep digital cabinet oleh (Prayudi & SN, 2015b), *framework Chain Of Custody* proses investigasi bukti digital oleh Ćosić, (2010) penjabaran kebutuhan informasi manajemen *Chain Of Custody* menggunakan pendekatan ontology oleh (Luthfi & Prayudi, 2016) dan lain-lain. Namun solusi tersebut masih belum sesuai dengan kebutuhan *Chain Of Custody* untuk barang bukti digital. Dengan pendekatan metadata ada sebagai salah satu solusi yang akan diusulkan untuk memperkaya solusi digital *Chain Of Custody* yang sudah ada. Pendekatan metadata akan menghasilkan model metadata yang cocok untuk kepentingan digital *Chain Of Custody* dalam penanganan studi kasus sosial media.

Selanjutnya solusi yang diberikan adalah *Chain Of Custody* untuk Artefak Sosial media Forensik dengan tujuan dapat menyesuaikan ketidaksesuaian pada konsep *Chain Of Custody* untuk sosial media. Sehingga dengan konsep tersebut dapat menjadi solusi terhadap kebutuhan penyidik.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah yang akan dibahas yaitu bagaimana membangun konsep dokumentasi *Chain Of Custody* untuk artefak sosial media *facebook*. Konsep *Chain Of Custody* yang selama ini diterapkan sifatnya sangat umum untuk artefak digital yang sifatnya fisik, sementara untuk arefak digital sosial media konsep yang ada perlu penyesuaian. Ketiadaan konsep *Chain Of Custody* pada sosial media menyebabkan tidak terdokumemtasinya proses pemeriksaan sosial media sehingga akan menyebabkan integritas proses penyidikan menjadi diragukan. Adanya konsep *Chain Of Custody* untuk artfeak digital diharapkan akan menjadi solusi terhadap kebutuhan penyidik dalam melakukan pemeriksaan kasus-kasus sosial media *facebook*.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini yang terfokus pada dokumentasi *Chain Of Custody* dengan proses pencarian bukti digital melalui sosial media *facebook* dengan menggunakan aplikasi Hunchly.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah dapat membantu proses investigasi pada sosial media *facebook* yaitu untuk menghasilkan dokumentasi *Chain Of Custody*.

1.5 Manfaat Penelitian

Manfaat dalam penelitian ini untuk mengetahui cara dalam penanganan bukti digital yang terjadi di sosial media *facebook* dalam proses investigasi menggunakan aplikasi Hunchly.

1.6 Metode Penelitian

Langkah-langkah yang akan ditempuh selama melakukan penelitian ini adalah sebagai berikut :

1. Studi Pustaka

   Penelitian ini melakukan studi pustaka dengan langkah awal mengumpulkan referensi yang relevan dengan objek penelitian melalui buku, makalah, literatur maupun jurnal ilmiah yang membahas mengenai bukti fisik- bukti fisik, formulir *Chain Of Custody* barang bukti, dan aplikasi Hunchly serta sumber- sumber informasi lainnya yang dapat diperoleh melalui *internet.*

2. Membangun Konsep COC untuk Artefak Sosial media *Facebook*

   Konsep yang akan dibangun pada penelitian ini yaitu merupakan suatu aktifitas yang akan merekam informasi bukti digital untuk dokumentasi *Chain Of Custody* dengan menggunakan aplikasi Hunchly yang akan merekam atau men*capture* jejak bukti digital dalam browser chrome sehingga dapat membantu penyidik dalam menemukan bukti digital pada sosial media *facebook.*

3. Implementasi Konsep

   Implementasi pada penelitian ini adalah menerjemahkan konsep COC dengan kebutuhan aplikasi yang akan digunakan dalam penelitian meliputi proses-proses apa saja yang akan menganalisis halaman-halaman web untuk mendukung investigasi kejahatan pada sosial media *facebook*, dalam hal ini peneliti menggunakan aplikasi Hunchly berbasis dekstop yang dapat dijalankan pada browser chrome dan membuat program aplikasi *digital Chain Of Custody* untuk dokumentasi investigasi kejahatan sosial media *facebook*

4. Pengujian Konsep

   Pengujian konsep *chains of custody* adalah menggunakan pendekatan pengujian secara konseptual dan fungsional. Konsep *chains of custody* akan diuji kualitasnya secara konseptual berdasarkan aspek-aspek dokumentasi. Sedangkan pengujian secara

fungsional ialah dengan melakukan studi kasus untuk *proof of concept*. Studi kasus yang akan dianalisis menggunakan aplikasi Hunchly untuk investigasi kejahatan pada sosial media *facebook.* Dan dokumentasi *Chain Of Custody* bukti digital merupakan hasil dari *proof of concept*.

1.7 Struktur Penulisan

Tahapan yang menjelaskan secara umum terkait sistematika penulisan yang berisi penjelasan secara ringkas terhadap kerangka penulisan yang digunakan.

BAB I : PENDAHULUAN

Tahap awal dari penelitian berisi penjelasan terkait dengan latar belakang penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode serta struktur penulisan yang digunakan. Dalam bagian ini juga dijelaskan mengenai temuan paling relevan dengan penelitian sebelumnya dan kontribusi ilmiah yang diharapkan.

BAB II : KAJIAN PUSTAKA

Tahap ini menjelaskan tentang kajian atas pustaka yang relevan dengan penelitian dan rumusan masalah berupa konsep dokumentasi *Chain Of Custody* untuk artefak sosial media *facebook*, dokumentasi bukti digital, aplikasi Hunchly untuk mendukung investigasi pada sosial media *facebook*.

BAB III : METODOLOGI PENELITIAN

Menguraikan metode penelitian yang digunakan untuk memperoleh data dan informasi sesuai dengan topik penelitian. Pada penelitian ini, metodologi yang diguanakan adalah berbasis penelitian desain (*design research*).

BAB IV : ANALISIS DAN HASIL

Menjelaskan kebutuhan informasi *Chain Of Custody* bukti digital , analisis informasi dokumentasi yang digunakan serta aplikasi/sistem sebagai wujud implementasi dokumetasi *chainc of custody* untuk sosial media *facebook*. Dan hasil berisi tentang pembahasan dan penyelesaiaan masalah yang dianalisis dengan cara pengujian yang akan dilakukan dalam menjawab permasalahan yang diusulkan.

BAB V : IMPLEMENTASI DAN PEMBAHASAN

Menjelaskan penerapan atau implementasi dari artefak sosial media terkait proses investgasi studi kasus disosial media *facebook.*. Dengan memaparkan hasil analisis dan pembahasan proses invesstigasi kasus sosial media *facebook* menggunakan aplikasi Hunchly untuk menemukan bukti digital. Sehingga dengan adanya konsep *Chain Of*

Custody untuk artefak sosial media *facebook* dapat memenuhi kebutuhan penyidik dalam mendokumentasikan *Chain Of Custody* sesuai dengan kebutuhan.

BAB VI : PENUTUP

Berisi simpulan dari hasil penelitian disertai dengan beberapa saran

DAFTAR PUSTAKA

BAB 2
Tinjauan Pustaka

2.1 Penelitian Terdahulu

Penelitian terkait merupakan proses untuk memetakan penelitian antara penelitian sebelumnya dan penelitian terbaru. Penelitian yang dilakukan oleh (Naufal Bahreisy et al., 2021) tentang Analisis Halaman Darkweb Untuk Mendukung Investigasi Kejahatan Berdasarkan hasil penelitian bahwa menganalisis halaman-halaman Dark Web menggunakan Hunchly dapat digunakan untuk melakukan analisis investigasi pada halaman Dark Web, di mana dari analisis halaman Dark Web ditemukan salah satu produk yang paling sering dijual yaitu "drugs" serta profil vendor. Data selector yang terinput pada aplikasi Hunchly, dapat dijadikan sebagai dasar untuk mendapatkan informasi dari halaman Dark Web. Selanjutnya dilakukan analisis untuk mendapatkan informasi lebih mendalamdari tiap-tiap halaman Dark Web. Berdasarkan hasil penelitian, didapatkan informasi yang penting untuk melakukan investigasi pada halaman Dark Web, seperti informasi tentang profil pegguna, vendor level, trust level, membersince, jabber, email, website,

Penelitian yang dilakukan oleh (Efendi, 2019a) membahas tentang Manajemen Barang Bukti Fisik Dan *Chain Of Custody* (CoC) Pada Penyimpanan Laboratorium Forensika Digital, yang diharapkan dengan adanya konsep manajemen barang bukti dan dokumentasi *Chain Of Custody* segala aktivitas yang berkaitan dengan penyimpanan barang bukti dapat terjaga serta terdokumentasi dengan baik. Hasil penelitian ini diperoleh proses penyimpanan keaslian bukti digital sebagai panduan untuk melakukan dokumentasi secara terstruktur. Namun pada konsep ini belum terdapat penanganan barangbukti digital dengan metode live forensik dengan dokumentasi *Chain Of Custody*.

Penelitian lain dilakukan oleh (Widatama & Yudi Prayudi, 2017) membahas tentang konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML. Pada pendekatan XML untuk membangun LPBD memudahkan dalamproses implementasi dan interoperabilitas penyimpanan bukti digital. Selain itu konsep LPBD juga dapat menjadi solusi terhadap mekanisme penyimpanan bukti digital sebagaimana analogi sebuah lemari yang digunakan untuk penyimpanan bukti fisik, LPBD memiliki 4 struktur bagian untuk menyimpan sebuah file bukti digital, yaitu:warehouse, cabinet, rack dan bag. File yang dapat disimpan memiliki format RAW (DD) dan Advanced Forensics Format (AFF). Hasil dari penelitian ini berupa pendekatan yang telah mampu menyelesaikan solusi perlunya penyimpanan bukti digital, namun belum terdokumentasi dengan baik.

Penelitian yang dilakukan oleh (Minin, 2020) dengan konsep Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito). Browser terdapat fitur mode incognito yang digunakan dalam menjelajah informasi di internet. Fitur ini diklaim tidak menyimpan data penelusuran pribadi, seperti riwayat penelusuran, cookies, cache, dan kata sandi, di penyimpanan browser. Namun browser mode incognito dapat meninggalkan barang bukti digital di sistem. Hal ini menjadi tantangan bagi forensik investigator untuk melakukan investigasi forensik dan mencari barang bukti digital (digital evidence) dari browser mode incognito. Penelitian yang dilakukan menggunakan metode live forensic mampu mendapatkan dan membuktikan bahwa penggunaan browser mode incognitomeninggalkan informasi berupa barang bukti digital dari pengguna. Barang bukti yang ditemukan yaitu berupa browsing history, web search, password, username, visited url.

Penelitian yang dilakukan oleh (Anwar & Riadi, 2017) yang berjudul "Analisis Investigasi Forensik Whatsapp Messenger Smartphone Terhadap WhatsappBerbasis Web" Dengan diterapkannya metode investigasi WhatsApp forensik yang melibatkan skema proses yaitu pentest WhatsApp attack dan flowchart penyadapan WhatsApp maka akan diperoleh hasil perbandingan investigasi terhadap dua devices mencakup WhatsApp on Smartphone dengan sistem operasi Android dan WhatsApp Webon komputer yang ber-platform Windows sehingga nantinya terdapat tabel normalisasi perbandingan akan eksplorasi temuan digital evidence yang menyatakan tindak kejahatan kaitannya dengan pesan layanan *WhatsApp messenger*. Penelitian ini telah menunjukkan bahwa seseorang dapat memperoleh akses lengkap ke semua informasi di WhatsApp baik itu WhatsApp Smartphone maupun WhatsApp Web.

Penelitian yang dilakukan oleh (Larasati & Hidayanto, 2017) Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10. Penelitian ini dilakukan untuk aplikasi Instant Messenger popular yaitu Facebook, LINE dan Telegram pada platform windows 10. Dari analisis ingin diketahui aplikasi yang mudah dan sulit untuk memperoleh data sebagai bukti digital. Dilakukan pengujian skenario dengan cara eksperimen berupa data percakapan biasa dan penghapusan pesan atau percakapan. Menggunakan tools Winhex dan Belkasoft Evidence Center digunakan untuk menganalisis data digital. Jenis data berupa data primer percakapan dan data media yang memiliki karakteristik unik sehingga data yang didapatkan juga berbeda bergantung struktur data yang disusun pada aplikasi.

Tabel 2.1 Penelitian Terkait

Paper Utama	Metode	Tools	Objek	Hasil
(Bahreisy et al., 2021)	Live Forensic	Hunchly	Dark Web	Hasil pada penelitian ini, didapatkan informasi yang penting untuk melakukan investigasi pada halaman Dark Web, seperti informasi tentang profil pegguna, vendor level, trust level, membersince, jabber, email, website, PGPyang semuanya dapat memberikan informasi terkait data yang dapat dijadikan sebagian salahsatu barang bukti dalam mendukung investigasi kejahatan.Dari hasil penelitian, ditemukannya emailvendor pada akun terkait sehingga perlu dilakukan investigasi yang kebih jauh terhadap akun untuk mendaatkan informasi yang relevan.
(Efendi, 2019b)	Studi Pustaka	MySql Dan DBMS	*Chain Of Custody*	Konsep manajemen barang bukti dan dokumentasi *Chain Of Custody* segala aktivitas yang berkaitan dengan penyimpanan barangbukti dapat terjaga serta terdokumentasi dengan baik. Kontribusi dalam penelitian ini adalah proses penyimpanan keaslian bukti digital sebagai panduan untuk melakukan dokumentasi secara terstruktur. Namun pada konsep ini belum terdapat penanganan barang bukti digital dengan metode live forensik dengan dokumentasi *Chain Of Custody*
(Widatama & Prayudi, 2017)	Pendekatan XML	Lemari Penyimpanan Bukti Digital(LPBD)	Warehouse, Cabinet, Rack Dan Bag.	Pada pendekatan XML untuk membangun LPBD memudahkan dalamproses implementasi dan interoperabilitas penyimpanan bukti digital. Selain itu konsep LPBD juga dapat menjadi solusi terhadap mekanisme penyimpanan bukti digital sebagaimana analogi sebuah lemari yang digunakan untuk penyimpanan bukti fisik, LPBD memiliki 4 struktur bagian untuk menyimpan sebuah file bukti digital, yaitu: warehouse, cabinet, rack dan bag. File yang dapat disimpan memiliki format RAW (DD) dan Advanced Forensics Format (AFF). Hasil berupa pendekatan yang mampu menyelesaikan solusi perlunya penyimpanan bukti digital, namun belum terdokumentasi dengan baik

Tabel 2.2 Penelitian Terkait (Lanjutan)

Paper Utama	Metode	Tools	Objek	Hasil
(Minin & Anwar, 2020)	Live Forensic	AccesData FTK Imager Dan Autopsy	Browser Mode Incognito	Dengan menggunakan metode live forensic mampu mendapatkan dan membuktikan bahwa penggunaanbrowser mode incognito masih meninggalkan informasi berupa barang bukti digital dari pengguna.
(Anwar et al., 2017)	Pentest	SQLite Database	WhatsApp Web	Dengan diterapkannya metode investigasi WhatsApp forensik yang melibatkan skema proses yaitu pentest WhatsApp attack dan flowchart penyadapan WhatsApp maka akan diperoleh hasil perbandingan investigasi terhadap dua devices mencakup WhatsApp on Smartphone dengan sistem operasi Android dan WhatsApp Web on komputer yang ber-platform Windows.
(Larasati et al., 2017)	Live Forensic	Winhex Dan Belkasoft	LINE Messenger, Facebook Messenger dan Telegram Messenger	Berdasarkan hasil penelitian pada analisis forensika digital pada aplikasi instant IM yaitu LINE Messenger, Facebook Messenger dan Telegram Messenger, pengimplementasian teknik live forensics untuk mendapatkan bukti digital dari aktivitas penggunaan aplikasi IM membutuhkan tools dan teknik yang berbeda untuk mendapatkan analisis yang sesuai dengan yang diinginkan, terlebih terdapatnya kekurangan dari teknik live forensics yaitu tidak semua data yang didapatkan sesuai dengan yang telah direncanakan
Usulan	Live Forensic	Hunchly	Facebook	-
Ulasan	membangun konsep dokumentasi *Chain Of Custody* untuk artefak sosial media *facebook*. Konsep *Chain Of Custody* yang selama ini diterapkan sifatnya sangat umum untuk artefak digital yang sifatnya fisik, sementara untuk arefak digital sosial media konsep yang ada perlu penyesuaian. Ketiadaan konsep *Chain Of Custody* pada sosial media menyebabkan tidak terdokumemtasinya proses pemeriksaan sosial media sehingga akan menyebabkan integritas proses penyidikan menjadi diragukan. Adanya konsep *Chain Of Custody* untuk artfeak digital diharapkan akan menjadi solusi terhadap kebutuhan penyidik dalam melakukan pemeriksaan kasus-kasus sosial media *facebook*			

2.2 Landasan Teori

Penelitian ini memiliki fokus pada dokumentasi *Chain Of Custody*. Sedangkan objek utama dari penelitian ini adalah barang bukti digital dan tools yang akan digunakan untuk menemukan bukti digital yaitu Hunchly.

2.2.1. Facebook

Facebook adalah sebuah layanan jejaring sosial dan situs web yang diluncurkan pada 4 *Februari* 2004 yang dioperasikan dan dimiliki oleh Facebook, Inc. Facebook lahir atas usaha seorang mantan mahasiswa Harvard bernama Mark Zuckerberg. Mark Zuckerberg menciptakan Facemash, pendahulu Facebook, tanggal 28 Oktober 2003 ketika berada di Harvard sebagai mahasiswa tahun kedua. Facemash menarik 450 pengunjung dan 22.000 tampilan foto pada empat jam pertama mengudara. Situs ini langsung diteruskan ke beberapa server group kampus, namun dimatikan beberapa hari kemudian oleh administrasi Harvard. Zuckerberg dihukum karena menembus keamanan kampus, melanggar hak cipta, dan melanggar privasi individu, dan terancam dikeluarkan. Namun, hukuman tersebut dibatalkan.

Pengguna dapat membuat profil pribadi, menambahkan pengguna lain sebagai teman dan bertukar pesan, termasuk pemberitahuan otomatis ketika memperbarui profilnya. Selain itu, pengguna dapat bergabung dengan grup pengguna yang memiliki tujuan tertentu, diurutkan berdasarkan tempat kerja, sekolah, perguruan tinggi, atau karakteristik lainnya.

Menurut Ginting (2012), Facebook diartikan sebagai mesin yang sangat pintar, canggih, serba komplit, namun justru sangat user friendly. Dari segi teknis, Facebook juga bersifat open source sehingga pengguna bisa menambahkan sendiri aplikasi yang disukai. Sedangkan dari segi sosial, Facebook bisa dikatakan sebagai identitas di dunia maya.

Facebook menyediakan fitur gabungan antara aplikasi Sosial Networking, Chatting, Blogging, Multimedia, Photo Sharing, dan bahkan Email. Beberapa bagian dalam Facebook adalah Profil, News Feed, Wall, Applications, Photo, Video, Poke, Group, Events, Marketplace, Post, Notes, dan Gift. Dalam satu akun Facebook seseorang dapat melakukan beragam aplikasi tersebut.

Facebook memberikan beberapa manfaat diantaranya memudahkan seseorang dalam menjalin hubungan pertemanan dan penyampaian informasi. Dengan fitur yang terdapat pada Facebook para pengguna dapat membagikan informasi diri melalui biodata maupun status yang diperbaharui. Namun tidak jarang informasi yang disampaikan hanya fiktif atau

bukan yang sebenarnya. Ada pula yang memberikan informasi terlalu terbuka tanpa memperhatikan situasi dan keadaan baik dari pihak pemberi maupun penerima informasi, yang akhirnya memberikan penggunaan fitur Facebook memberikan dampak negatif pada salah satu pihak.

2.2.2. Definisi dan Contoh Bukti Digital

Pada buku Digital Forensic: Panduan Praktis Investigasi Komputer, barang bukti digital forensik diklasifikasikan menjadi dua, yaitu: barang bukti elektronik dan barang bukti digital. Barang bukti elektronik ini bersifat fisik dan dapat dikenali secara visual, sehingga investigator dan analis forensik harus sudah memahami serta mengenali masing-masing barang bukti elektronik ini ketika sedang melakukan proses pencarian (searching) barang bukti di TKP. Barang bukti elektronik ini contohnya: PC, handphone, hard disk, router, kamera digital, dan lain-lain. Sedangkan barang bukti digital adalah barang bukti yang bersifat digital yang diekstrak atau di-recover dari barang bukti elektronik. Barang bukti ini dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah "informasi elektronik" dan "dokumen elektronik". Jenis barang bukti ini yang harus dicari oleh analis forensik untuk kemudian dianalisis secara teliti keterkaitan masing-masing file dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik. Contoh barang bukti digital: logical file, deleted file, log file, video file, image file, email, dan lain sebagainya (Nuh Al-Azhar, 2012). Bukti digital adalah obyek digital yang mengandung informasi handal dalam mendukung atau menolak terkait kasus kejahatan dalam proses investigasi

Sedangkan yang dimaksud dengan Informasi Elektronik dalam Pasal 1 ayat (1) UU ITE, bahwa Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data *interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Yang dimaksud dengan Dokumen Elektronik dalam Pasal 1 ayat (2) UU ITE adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda,

angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Berikut beberapa contoh barang bukti digital yaitu: *Logical file, Deleted File, Lost File, File slack, Log File, Encrypted File,Steganography file, Office file, Audio File, video File, Image file, Email, User ID* dan *Password, Short Message Service (SMS), Multimedia Message Service (MMS), Call Logs*. Bukti digital juga adalah *file* bukti digital hasil ekstraksi (*full copy*) bit per bit dari media penyimpanan yaitu *hard drives, flash drives, floppy disk* dan *optical media* yang dikenal dengan istilah *Disk Image*.

2.2.3 Karakter Bukti Digital

Menurut (Kuntze et al., 2017) untuk dapat diterima di persidangan barang bukti digital harus memenuhi karakteristik bukti digital yaitu *Admissible* (layak), *Authentic* (Asli), *Complete* (Lengkap), *Reliable* (Dapat dipercaya) dan *Believable* (terpercaya).

1. Admissible

   Barang bukri digital harus sesuai dengan fakta dan masalah yang terjadi dan dapat diterima serta digunakan secara hukum mulai dari proses penyidikan sampai ke pengadilan.
2. Authentic

   Bahwa barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan barang bukti bukan hasil rekayasa. Barang bukti adalah masih asli dan tidak pernah diubah-ubah.
3. Complete

   Barang bukti harus lengkap dan dapat membuktikkan tindakan jahat yang dilakukan pelaku kejahatan. Barang bukti yang dikumpulkan, tidak cukup hanya berdasarkan satu perspektif dari sebuah kejadian yang berlangsung.
4. Reliable

   Barang bukti yang dikumpulkan harus dapat dipercayai. Pengumpulan barang bukti dan analisis yang dilakukan harus sesuai prosedur dan dilakukan dengan jujur. Selain itu barang bukti tidak boleh meragukan dan benar benar harus dapat dipercayai serta sesuai dengan prosedur yang SOP yang berlaku.

2.2.4 Chain Of Custody

Chain Of Custody adalah prosedur pencatatan / dokumentasi kronologis barang bukti sejak barang bukti ditemukan, proses duplikasi, penyimpanan barang bukti baik itu secara fisik ataupun digital hingga sampai pada presentasi dan keputusan akhir terhadap barang bukti. *Chain Of Custody* digunakan untuk memastikan integritas dan orisinalitas dari barang bukti (Prayudi & SN, 2015a).

Dokumentasi *Chain Of Custody* selama ini tidak memiliki standar yang baku. Sehingga setiap penegak hukum dapat memiliki form dokumentasi *Chain Of Custody* yang berbeda-beda. Namun untuk dapat diterima di persidangan, sebuah form *Chain Of Custody* setidaknya mencakup informasi "5W dan 1 H" untuk mencatat setiap proses investigasi diantaranya (Cosic, 2017a):

- Siapa yang terlibat dalam penanganan barang bukti
- Kapan waktu setiap proses penanganan barang bukti dilakukan
- Bagaimana proses penanganan yang dilakukan terhadap barang barang bukti
- Kemana saja alur perjalanan proses penanganan barang bukti itu dibawa dan dimana disimpan
- Mengapa pihak tersebut menanganinya
- Apa saja barang bukti yang telah dikumpulkan

Dalam melakukan *Chain Of Custody*, ada hal-hal yang harus diperhatikan diantaranya (Leintz, n.d.) :

1. *Security and Trust*

   Proses *Chain Of Custody* seharusnya mampu menjamin keamanan dan tingkat kepercayaan di persidangan. Menciptakan dan memelihara *Chain Of Custody* artinya menjaga *log* detail terkait dimana barang bukti ditemukan dan *log* seluruh aktivitas yang terjadi pada barang bukti.

2. *Documentation*

   Proses *Chain Of Custody* dimulai di Tempat Kejadian Perkara (TKP) yaitu pada saat proses investigasi dan ketika barang bukti pertama kali diperoleh. Dokumentasi yang dilakukan di TKP umumnya dilakukan dengan menggunakan foto-foto TKP dan catatan investigasi awal sampai selesai kasus.

3. *Preventing Contamination*

   Merupakan aspek pencegahan barang bukti dari adanya kontaminasi, perubahan dan kerusakan selama proses penanganan. Hal ini berkaitan dengan nilai integritas dan

keaslian dari barang bukti. Pihak-pihak yang berwenang dalam mengakses barang bukti, mendokumentasikan, dan menyerahkan merupakan pihak yang bertanggung jawab. Menurut (Cosic & Baca, 2010) dalam dunia forensika digital, nilai integritas barang bukti digital adalah memastikan bahwa informasi yang terkandung dalam bukti yang dihadirkan lengkap dan tidak mengalami perubahan oleh pihak yang tidak memiliki wewenang otorisasi mulai pada saat diciptakan, penanganan hingga selesai persidangan. Salah satu metode yang dapat digunakan untuk memastikan integritas bukti digital adalah tidak berubahnya nilai fungsi MD5/hash barang bukti digital. MD5 merupakan fungsi hash yang paling umum digunakan dan merupakan pengembangan dari MD4. Fungsi MD5 memiliki panjang 128 bit. MD5 bekerja dengan membawa setiap pesan yang ada dan menghitung total bit yang terdapat pada pesan dan melakukan *message diggest* dengan langkah penambahan *padding bit*, penambahan nilai panjang semula, inisialisasi buffer, pengolahan buffer dan pengolahan pesan dalam blok 512 bit .

2.2.5 Hunchly

Hunchly adalah alat tangkap web yang dirancang khusus untuk investigasi online. Hunchly diam-diam berjalan di browser web dan secara otomatis mengumpulkan, mendokumentasikan, dan membuat anotasi setiap situs web yang kunjungi. Dengan menggunakan alat ini, pengguna tidak perlu mengingat untuk mengambil tangkapan layar, memotong dan menempelkan URL, atau menyimpan dokumen saat menjelajah. (Michael Kissiah, 2020)

- Halaman situs web
    - Dokumen
    - Hasil mesin pencari
    - Posting forum diskusi
    - Posting dan diskusi media sosial
    - Penelitian web gelap
    - pengajuan pengadilan
    - URL dan stempel waktu

1. Buat Jejak Audit

Hunchly secara otomatis membuat jejak audit dari semua langkah yang lalui selama sesi penelitian. Hal ini memungkinkan untuk melacak di mana pengguna telah dan apa yang telah lihat di sepanjang jalan.

2. Dokumentasi Cepat

Hunchly secara otomatis mengunduh dan menyimpan salinan laporan, dokumen, dan materi lainnya ke komputer. Ini sangat mengurangi berapa kali harus menghentikan apa yang sedang lakukan. Plus, ini membantu menandai dan mengkategorikan konten di sepanjang jalan.

3. Pencarian yang Kuat

Hunchly memiliki fitur pencarian yang kuat yang memungkinkan untuk mencari melalui semua dokumen, tanpa harus mengunjungi kembali situs web. Ini adalah fitur penghemat waktu yang hebat, terutama ketika harus bekerja secara offline.

4. Pelaporan Cepat

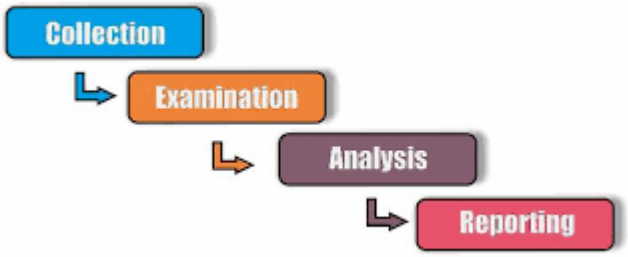
Buat laporan dengan cepat dan mudah di Hunchly untuk dikirim langsung ke klien. Bangun paket bukti siap-sidang dalam hitungan menit. Ini menghemat waktu dalam waktu dokumentasi sehingga memiliki lebih banyak waktu untuk melakukan pekerjaan investigasi. Hemat waktu, dan tingkatkan akurasi pelaporan.

2.2.6 Live Forensics

Live forensics pada dasarnya memiliki kesamaan pada teknik forensik tradisonal dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja live forensics merupakan respon dari kekurangan teknik forensik tradisonal yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktifitas memory, network proses, swap file, running system proses, dan informasi dari file sistem. Teknik *live forensics* memerlukan kecermatan dan ketelitian, dikarenakan data volatile pada RAM dapat hilang jika sistem mati, dan adanya kemungkinan tertimpanya data penting yang ada pada RAM oleh aplikasi yang lainnya. Karena itu diperlukan metode live forensics yang dapat menjamin integritas dan keaslian data volatile tanpa menghilangkan data yang berpotensial menjadi barang bukti. Pada metode *Live forensics* bertujuan untuk penanganan insiden lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibuka dan kapasitas memori yang lebih rendah bila dibandingkan dengan metode forensik tradisional. Banyak *tools* untuk digunakan *live forensics* untuk analisis data. Tools yang dibandingan pada metode live forensics yaitu dari kemampuan penggunaan *memory*, waktu, jumlah langkah dan akurasi paling baik dalam melakukan *live forensic*. (Larasati & Hidayanto, 2017)

2.2.7 Alur Proses Digital Forensik

Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST *(National Institute of Standards Technology).* Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis. Akhirnya, transformasi informasi menjadi bukti analogi dengan mentransfer pengetahuan ke dalam tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan. Dalam *National Institute Standard and Technology* (NIST) oleh (Kent, Chevalier, Grance, & Dang, 2006) secara umum proses forensik dibagi ke dalam empat tahapan, yaitu *collection*, *examination*, *analysis* dan *reporting* seperti pada gambar 2.1.



Gambar 2.1 Proses Digital Forensik

Tahap *Collection* (Pengumpulan Data) meliputi aktivitas identifikasi sumber data yang relevan terkait kasus, pelabelan dan pencatatan. Dalam tahapan ini seluruh prosedur yang dilakukan harus sesuai dengan pedoman dan Standar Operasional Prosedur yang berlaku untuk menjaga integritas barang bukti digital.

Tahap *Examination* (Pemeriksaan) meliputi aktivitas penggunaan *tools* atau perangkat lunak dan teknik tertentu untuk melakukan identifikasi dan ekstraksi informasi yang relevan. Tahap pemeriksaan dapat menggunakan *tools* otomatis atau melalui proses manual.

Tahap *Analysis* (Analisis) merupakan aktivitas analisis terhadap hasil pemeriksaan untuk mendapatkan informasi yang berguna sehingga diperoleh kesimpulan.

Tahap *Reporting* (Pelaporan) merupakan aktivitas yang memuat tindakan, prosedur, alat yang digunakan dan memberikan rekomendasi perbaikan kebijakan dan petunjuk dalam aspek proses forensik.

2.2.8 Karakteristik Sosial Media Facebook

Proses investigasi di sosial media facebook di lakukan untuk mengumpulkan bukti-bukti digital. Proses ini dapat dilakukan secara live forensik, karena data-data yang dibutuhkan sebagai bukti digital harus dilakukan secara langsung. Dalam proses investigasi artefak sosial media ini membutuhkan akses internet dan tools pendukung untuk mengumpulkan data-data sebagai bukti digital.

Platform sosial media memiliki karakteristik tersendiri. Beberapa karakteristik sosial media serta informasi yang dapat ditemukan dari sosial media Facebook diantaranya adalah adding friends, status update, like, comment, share, dan liking pages. Pencarian seseorang melalui facebook dapat dilakukan dengan melakukan pencarian berdasarkan nama, email address, organisasi, ataupun berdasarkan like terhadap suatu postingan di media sosial. Setelah target personal ditemukan di facebook, beberapa informasi yang dapat diperoleh dari pengguna facebook tersebut adalah diantaranya profil pengguna, hubungan sosial, aktifitas dan informasi lokasi pengguna. (Golbeck, Klavans, & Editor, 2015)

Data pengguna sosial media dapat dikelompokkan menjadi dua macam yaitu data primer dan data sekunder. Data primer ini terdiri dari data yang berasal dari akun profil pengguna sedangkan data sekunder berasal dari metadata postinggan yang dilakukan oleh akun pengguna. Data primer terdiri dari Nama Lengkap, tanggal Lahir, Lokasi Geografis, Kerabat, Pendidikan & Riwayat Pekerjaan, Alamat Email, Nama Samaran, Nomor telephone, dan Foto. Sedangkan data sekunder adalah informasi dari suatu file misalkan, kapan file dibuat, kapan file di edit, kapan file di akses, nilai hash file, dan lain-lain.

Data dan informasi yang dapat kita temukan di berbagai sosial media facebook, pada umumnya sebagai berikut (Golbeck et al., 2015) :

1. Aktivitas Facebook
    - Menambah pertemanan sehingga pengguna dapat melihat setiap pembaruan yang dimiliki pengguna lainnya.
    - Pembaruan status dimana pengguna dapat membagikan informasi ke pengguna lain melalui status. Pembaruan status biasanya berupa teks, tautan, foto, video, 37 dan lokasi informasi. Serta pengguna dapat me-mention pengguna lain dengan namanya.

- Likes, komentar, dan share yang dilakukan pengguna untuk berinteraksi dengan pengguna lainnya. Menyukai sesuatu di facebook adalah salah satu cara paling umum pengguna berinteraksi. Selain itu pengguna juga dapat berkomentar sehingga setiap pengguna dapat saling berdiskusi. Sedangkan aktivitas share memungkinkan pengguna dapat memposting ulang sesuatu sehigga teman dari pengguna tersebut bisa melihatnya.
- Liking "Pages" atau menyukai "halaman" pada facebook yang dikelola oleh perusahaan, selebriti, atau entitas public lainnya.
- Integrasi pihak ketiga dimana fasilitas ini memungkinkan pengguna ketika mengklik tautan pada sebuah situs web, secara otomatis pengguna tersebut membagikan tautan pada halaman facebooknya.

2. Komponen Facebook
   - Facebook dipecah menjadi dua bagian utama yaitu *News Feed* dan *Timeline*. *News Feed* merupakan kumpulan pembaruan status atau aktivitas pada facebook. Sedangkan *Timeline* mengandung semua postingan dari setiap pengguna.
3. Informasi Demografi
   - Hampir setiap sosial media memiliki beberapa halaman profil penggunanya. Halaman tersebut memiliki beberapa informasi demografis seperti foto profil, usia, jenis kelamin, lokasi, dan deskripsi singkat tentang pengguna.
4. Mencari Pengguna Lainnya

   Ada beberapa cara yang dapat dilakukan untuk melakukan pencarian terhadap pengguna lain, yakni:

   - Pencarian menggunakan nama dengan memasukkan nama pengguna lain pada bagian atas halaman facebook.
   - Pencarian berdasarkan alamat email. Namun hal ini tergantung pada pengaturan profil pengguna. Jika pengguna mengijinkan untuk memunculkan alamat email pada halam profil mereka, maka pencarian dapat dilakukan.
   - Pencarian berdasarkan asosiasi yang diketahui. Dengan mencari rekan dari pengguna facebook yang memiliki asosiasi yang sama, kita dapat menemukan pengguna facebook yang kita cari.
   - Pencarian menggunakan "likes" dimana ketika seseorang menyukai sebuah halaman atau postingan di facebook, biasanya akan muncul di daftar orang yang menyukai halaman atau postingan tersebut.

BAB 3
Metodologi Penelitian

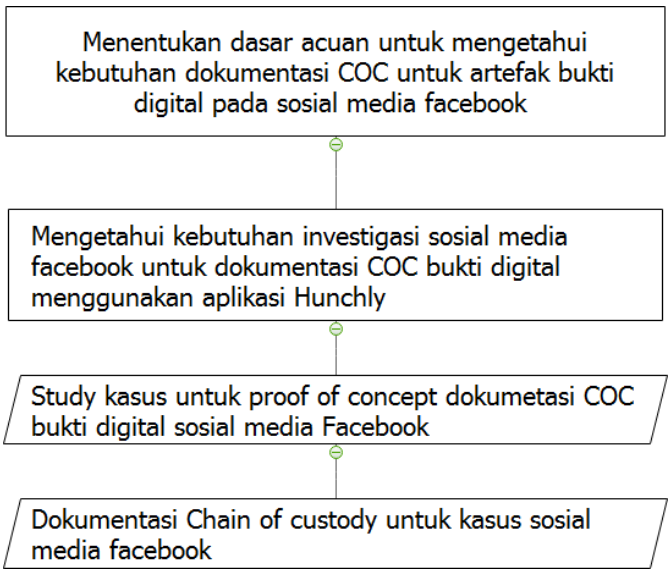
Bab ini menjelaskan tentang metodologi penelitian ini menggunakan metode komparatif yang bersifat eksperimental yang akan penulis gunakan, berdasarkan literatur dan landasan teori pada bab sebelumnya. Penelitian ini memfokuskan pada proses investigasi kejahatan untuk menemukan bukti digital dari hasil *record/capturing* sosial media *facebook* berdasarkan fakta forensik.

3.1 Studi Pustaka

Data yang digunakan pada penelitian ini diperoleh dari berbagai studi pustaka yang relevan terkait dengan bukti digital, *Chain Of Custody* bukti digital, sosial media, dan Hunchly.

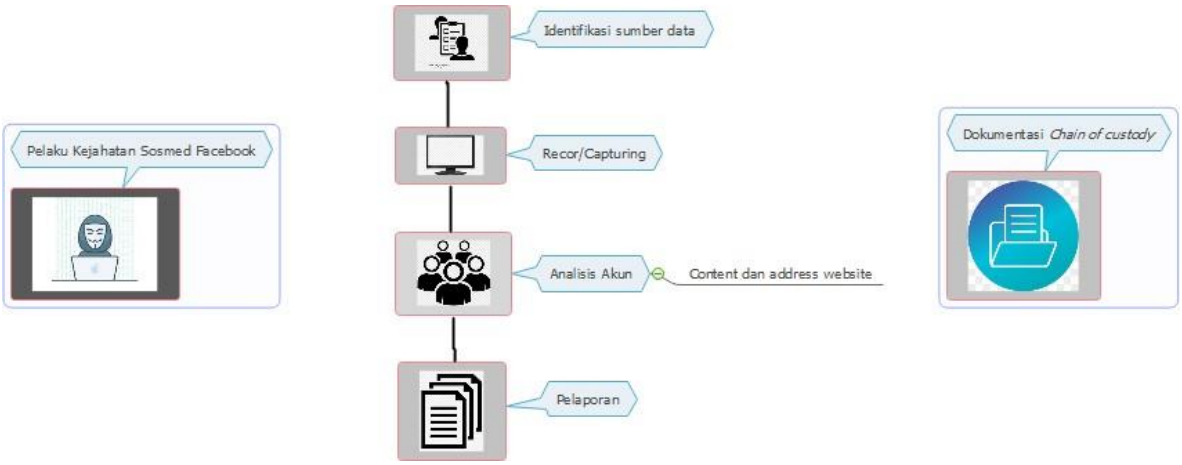
3.2 Membangun Konsep COC Untuk Artefak Sosial Media Forensik

Penelitian ini akan membangun konsep *Chain Of Custody* untuk artefak sosial media *facebook* dengan melakukan investigasi pada sosial media untuk mendukung proses dokumentasi *Chain Of Custody* bukti digital. Untuk dapat melakukan dokumentai *Chain Of Custody*, tahapan penting yang harus dilakukan adalah investigasi dalam menemukan bukti digital pada sosial media *facebook*. Tahapan untuk melakukan proses investigasi sosial media *facebook* dapat ditunjukkan pada gambar 3.1.



Gambar 3.1 Tahapan Kebutuhan investigasi Sosial media *Facebook*

Tahap pertama dari penelitian ini adalah menentukan dasar yang digunakan sebagai acuan untuk identifikasi kebutuhan dokumentasi *Chain Of Custody* untuk artefak bukti digital pada sosial media facebook. Tahap selanjutnya adalah identifikasi kebutuhan investigasi sosial media *facebook* untuk dokumentasi *Chain Of Custody* bukti digital berdasarkan acuan yang telah ditentukan. Dasar acuan dan daftar kebutuhan informasi untuk *Chain Of Custody* bukti digital dapat diperoleh dari beberapa sumber diantaranya; referensi penelitian terdahulu dan standar operasional prosedur atau aturan resmi yang telah ada yang mengatur tentang mekanisme pelaksanaan *Chain Of Custody*. Dokumen tersebut seperti dalam NIST, NIJ, Perkap dan dokumen formulir *Chain Of Custody*. Daftar kebutuhan informasi ini nantinya akan digunakan untuk membantu dalam identifikasi studi kasus sosial media *facebook* untuk *Chain Of Custody* bukti digital. Proses identifikasi kasus kejahatan sosial media facebook dapat ditunjukkan pada gambar 3.2.

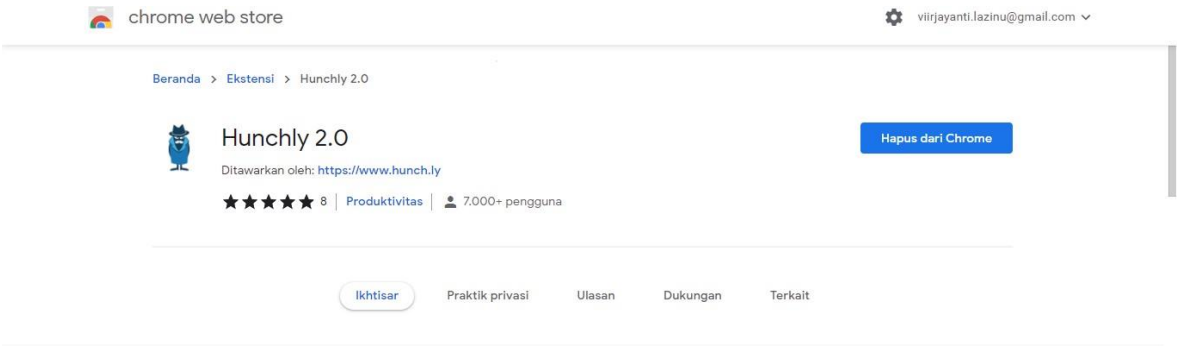


Gambar 3.2 Proses identifikasi kasus kejahatan sosial media *facebook*

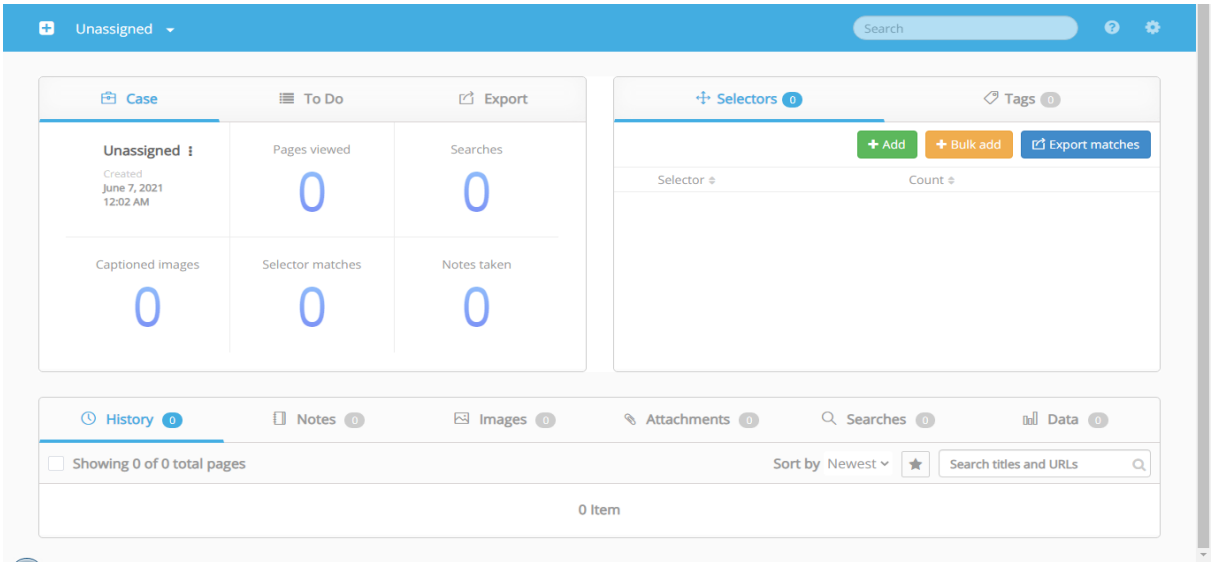
Proses identifikasi kasus kejahatan pada sosial media *facebook* dilakukan dengan 4 tahap yaitu tahap pertama identifikasi sumber data terkait dengan pengumpulan data yang relevan pada kasus kejahatan sosial media *facebook*, tahap kedua yaitu proses pemeriksaan berupa *record*/*capturing* yang dihasilkan pada aplikasi Hunchly sebagai proses investigasi, selanjutnya tahapan ketiga analisis terkait dengan hasil dari pemeriksaan akun pelaku kejahatan, dan tahapan terakhir yaitu pelaporan dari hasil analisis *capturing* kejahatan sosial media *facebook*.

3.3 Implementasi Konsep *Chain Of Custody*

Implementasi pada penelitian ini adalah menerjemahkan konsep *Chain Of Custody* dalam proses investigasi kejahatan sosial media *facebook* dengan menggunakan tools yang dapat membantu penyidik dalam menemukan bukti digital pada sosial media *facebook*. Tools yang digunakan dalam penelitian ini adalah Hunchly sebagai *record/capturing* dalam menemukan bukti digital pada proses investigasi. *facebook*. Adapun instalasi aplikasi Hunchly seperti pada Gambar 3.3 dan Gambar 3.4 sebagai tampilan awal aplikasi Hunchly.



Gambar 3.3 *addons* Hunchly di*chrome*



Gambar 3.4 Tampilan *Desktop* Hunchly

Aplikasi Hunchly digunakan dalam *record/capturing* sosial media *facebook* yang kemudian dianalisis untuk mendukung investigasi kejahatan, Selanjutnya untuk hasil dari proses investigasi diperlukan sebuah program aplikasi untuk dokumentasi *Chain Of Custody* yang merujuk pada kejahatan sosial media. Dokumentasi *Chain Of Custody* barang bukti merujuk pada bahasa pemrograman *javaScript* serta referensi pustaka lainya.

3.4 Pengujian Konsep *Chain Of Custody*

Pengujian konsep *chains of custody* adalah menggunakan pendekatan pengujian secara konseptual dan fungsional. Pengujian secara konseptual dilakukan untuk mengetahui kualitas dan kuantitas informasi dokumentasi *Chain Of Custody*. Mekanisme yang digunakan dalam pengujian secara konseptual adalah dengan memetakan informasi terhadap kebutuhan informasi *Chain Of Custody* dalam dokumen ISO/IEC 27037. Dokumen ISO/IEC 27037 sendiri merupakan dokumen standar nasional yang digunakan sebagai pedoman dalam melakukan identifikasi, pengumpulan, akuisisi dan preservasi bukti digital. Sedangkan pengujian secara fungsional ialah dengan melakukan percobaan Simulasi kasus dalam dengan *recording/capturing* halaman-halaman web menggunakan aplikasi Hunchly, dengan *recording/capturing* beberapa halaman web yang kemudian akan dianalisis. Simulasi kasus ini bertujuan untuk mengetahui proses investigasi kasus sosial media *facebook* sampai dengan dokumentasi *Chain Of Custody* bukti digital.

3.5 Perangkat Pendukung Penelitian

3.5.1 Perangkat Keras

Dalam proses penelitian beberapa perangkat pendukung digunakan agar penelitian dapat berjalan sesuai rencana. Kebutuhan perangkat ini terbagi menjadi perangkat keras dan perangkat lunak, Adapun perangkat keras yang digunakan adalah:

a. Processor Intel (R) Celeron (R) CPU N3060 @ 1.60GHz
b. Memory (RAM) 4,00 GB
c. System type 64-bit Operating System

3.5.2 Perangkat Lunak

Perangkat lunak merupakan aplikasi komputer yang digunakan dalam mendukung penelitian. Adapun perangkat lunak yang digunakan adalah :

a. Sistem Operasi : Micros*o*ft Windows 7 Ultimate
b. Pengolah Kata : Micros*o*ft *Of*fice Word 2019
c. Bahasa Pemrograman :JavaScript, HTML
d. Desain sistem : Micros*o*ft *Of*fice Visio / MindMaster

BAB 4
Hasil dan Pembahasan

Pada bab ini akan membahas terkait proses penelitian, analisis serta hasil yang ditemukan dalam penelitian ini. Pembahasan dalam bab ini meliputi proses penemuan bukti digital dan analisis bukti digital. Tahapan analisis digunakan untuk menganalisis data terpilih untuk dilakukan analisis *record/capturing* penemuan bukti digital untuk mendukung investigasi kejahatan.

4.1 Membangun Konsep COC Untuk Artefak Sosial Media Forensik

Digital *Chain Of Custody* di bidang forensik digital merupakan bagian penting dari proses investigasi digital. Agar alat bukti dapat diterima oleh pengadilan sebagai sah, *Chain Of Custody* untuk barang bukti digital harus disimpan, atau harus diketahui siapa sebenarnya, kapan, di mana, mengapa dan bagaimana kontak dengan barang bukti dalam setiap tahap penyidikan digital. Proses (Ćosić & Bača, 2011). Hal yang esensial dalam forensik digital adalah *Chain Of Custody*, yang merupakan upaya untuk menjaga integritas bukti digital serta prosedur untuk melakukan dokumentasi secara kronologis terhadap bukti. Karakteristik barang bukti digital menyebabkan penanganan lacak balak menjadi lebih rumit dan kompleks (Prayudi & SN, 2015b).

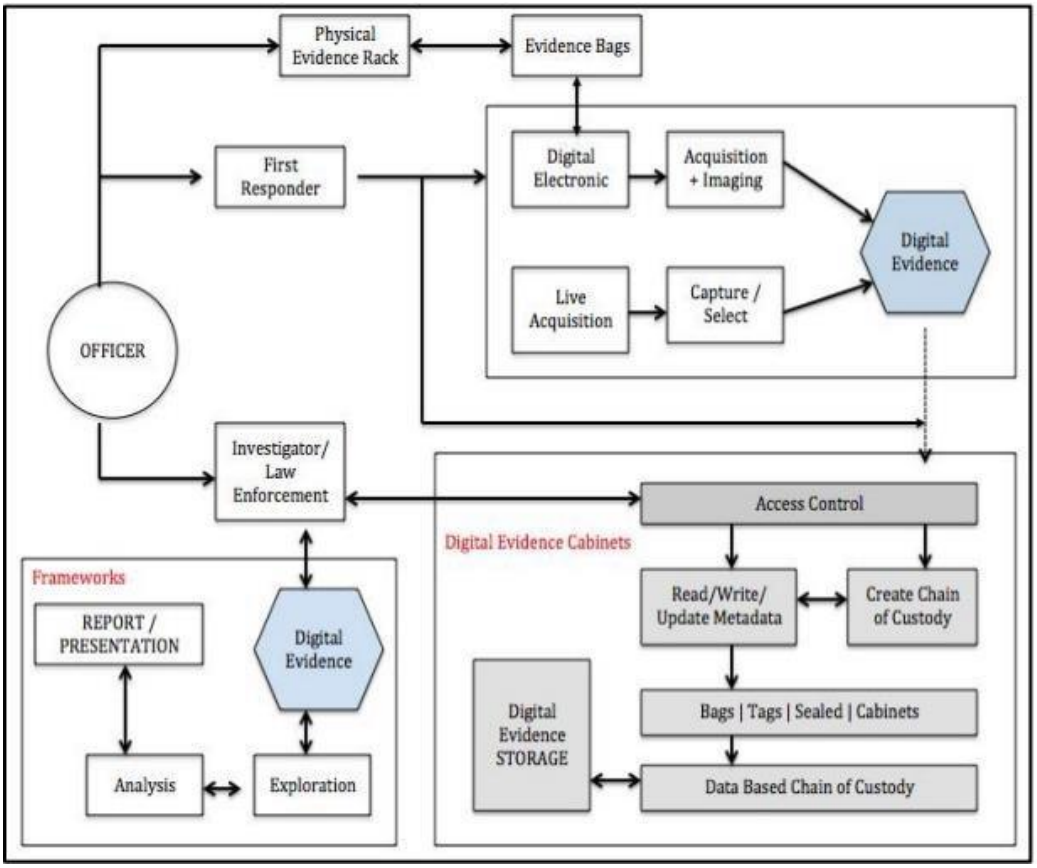
Ada lima elemen penting dalam proses digital *Chain Of Custody* (DCoC) (Sadiku et al., 2017):

1. Characteristics: Ini termasuk sumber-sumber seperti PC, perangkat digital, dan cloud.
2. Dynamics: Ini termasuk orang-orang yang terlibat dalam proses, yaitu tersangka, korban, profesional hukum, penyidik forensik. Rantai pengawasan selalu menjadi proses orang.
3. Factors: Ini menjawab pertanyaan berikut: Apa bukti digitalnya? Mana bukti digitalnya? Siapa yang mengelola dengan bukti digital? Mengapa melakukannya? Kapan bukti digital ditangani? Bagaimana penanganan dengan bukti digital? Pertanyaan-pertanyaan ini dapat dijawab menggunakan sidik jari, biometrik, cap waktu, pencari GPS, serangkaian prosedur, dan praktik terbaik.
4. Institutions: Ini akan mencakup penegakan hukum, militer, agen keamanan, bank, asuransi, institusi perusahaan, dan individu.

5. Integrity: Teknik untuk memastikan integritas bukti digital termasuk CRC (Checksum Redundancy Check), tanda tangan digital, enkripsi, timestamp, dan watermarking.

Metadata menjadi artefak penting dalam media sosial. Metadata merupakan Informasi berupa postingan dari sosial media berisi informasi yang disematkan. Metadata memberikan informasi tentang suatu file, misalnya informasi waktu file tersebut dibuat, waktu terakhir file diakses atau diubah, lokasi, atau maupun nama pengguna akun (Brill, Pollitt, & Morgan Whitcomb, 2007). Ada tiga jenis metadata: deskriptif, struktural, dan administratif. (Salama, Varadharajan, & Hitchens, 2012). Selain itu metadata mampu memberikan informasi untuk menjawab pertanyaan utama: siapa, apa, kapan, bagaimana, di mana, dan mengapa. Metadata yang dikelola oleh situs sosial media adalah aspek kontribusi lain untuk membantu penyelidikan dan untuk mengotentikasi bukti (Arshad et al., 2019). Informasi mengenai metadata dari informasi media sosial ini dapat dijadikan sebagai acuan untuk mengumpulkan bukti digital di media sosial facebook.

Penelitian ini akan mengadopsi model bisnis *Chain Of Custody* untuk bukti digital (Prayudi et al., 2015). Dalam model ini petugas yang bertanggung jawab terhadap *Chain Of Custody* barang bukti adalah *First Responder*, investigator, dan petugas pengelola yang bertanggung jawab penuh terhadap akses dan pengelolaan barang bukti. Terkait dengan apa saja aktivitas yang terdapat pada *Chain Of Custody* dalam manajemen barang bukti, di Indonesia telah diatur di dalam Peraturan Kepala Kepolisian Republik Indonesia No 10 Tahun 2010 tentang tata cara pengelolaan barang bukti di lingkungan kepolisian. Aktivitas pengelolaan barang bukti meliputi; penerimaan dan penyimpanan barang bukti, pengamanan dan perawatan barang bukti, serta pengeluaran barang bukti baik untuk keperluan pemeriksaan, peminjaman, pemusnahan dan lain-lain dari ruang penyimpanan khusus barang bukti. Seluruh aktivitas pengelolaan barang bukti tersebut dicatat dan didokumentasikan oleh petugas PPBB (Petugas Pengelola Barang Bukti).



Gambar 4.1 Model Manajemen *Chain Of Custody* Bukti Digital

(Sumber : Prayudi, Ashari, & Priyambodo, (2015))

4.1.1 Dasar Acuan Kebutuhan Dokumentasi Chain Of Custudy untuk Artefak Bukti Digital Pada Sosial Media Facebook

Di beberapa organisasi dan institusi, *Chain Of Custody* pada prakteknya dilakukan berbasis kertas (*paper based*) yaitu menggunakan formulir *Chain Of Custody*. Formulir *Chain Of Custody* berisi *field* catatan informasi mengenai barang bukti dan perjalanan barang bukti. Informasi yang terdapat di dalam formulir tersebut merupakan informasi penting yang diperlukan di dalam persidangan. Selama ini belum terdapat regulasi atau aturan baku yang menjadi acuan utama bagi organisasi dalam melakukan aktivitas dan menentukan kebutuhan informasi *Chain Of Custody* untuk barang bukti. Hal ini menyebabkan masing-masing organisasi memiliki aturan tersendiri dan mekanisme pelaksanaan *Chain Of Custody* menjadi berbeda-beda sesuai dengan peraturan dan kebutuhan dari setiap organisasi.

Panduan atau standart operasional yang membahas tentang kebutuhan informasi di dalam dokumen *Chain Of Custody* barang bukti digital saat ini masih sangat sedikit. Namun

ada beberapa penelitian yang membahas mengenai kebutuhan umum informasi manajemen *chain of custudy*. Seperti yang dilakukan (Ashcroft et al., 2004) dalam laporan *National Institute of Justice* dokumentasi *Chain Of Custody* setidaknya dapat merekam informasi terkait tindakan, tahapan atau aktivitas maupun perpindahan barang bukti serta subyek/personel/organisasi yang terlibat dengan aktivitas tersebut. Selain itu detail tanggal/waktu dari setiap aktivitas terhadap barang bukti tersebut juga perlu diperhatikan. Terkait dengan keamanan barang bukti digital *Chain Of Custody* seharusnya juga dapat memberikan informasi tentang bagaimana barang bukti disimpan dan dianalisis. Informasi yang berkaitan dengan penyimpanan barang bukti meliputi deskripsi lokasi penyimpanan beserta nilai MD5/SHA-1 apabila barang bukti tersebut adalah barang bukti digital. Sedangkan untuk informasi yang berkaitan dengan analisis barang bukti meliputi metode dan tools atau perangkat yang digunakan selama proses analisis. Informasi penting lain yang seharusnya ada di dalam dokumen *Chain Of Custody* adalah berkaitan dengan informasi bagaimana barang bukti tersebut didapatkan (*collection*).(Dahiya & Sangwan, 2014), (Thomson, 2011), (Anderson & ENISA, 2014, Cosic et al., 2011, Gayed et al., 2013, Graves, 2013, Ryder, 2021, dan Woods et al., 2013). Selain itu informasi kasus juga diperlukan dalam dokumen *Chain Of Custody* (Ashcroft et al., 2004).

Secara garis besar informasi *Chain Of Custody* seharusnya dapat menjawab pertanyaan tentang 5W+1H (Cosic et al., 2011). *Chain Of Custody* minimal dapat memberikan informasi yang berkaitan dengan aktivitas barang bukti dan subyek yang terlibat di dalamnya. Namun dokumen *Chain Of Custody* yang baik adalah dokumen yang memiliki informasi lengkap. Semakin detail dan lengkap informasi yang dicatat maka semakin baik *Chain Of Custody* (Coons, 2015). Pada prinsipnya, informasi pada formulir *Chain Of Custody* untuk barang bukti digital seharusnya memiliki kebutuhan yang hampir sama dengan formulir *Chain Of Custody* untuk barang bukti fisik. Namun karena barang bukti digital memiliki karakteristik yang berbeda dengan barang bukti fisik, maka perlu beberapa informasi pada formulir *Chain Of Custody* yang harus disesuaikan. Untuk lebih mudah mengetahui kebutuhan informasi *Chain Of Custody* dan sesuai dasar acuan identifikasi pada Gambar 4.1, Tabel 4.3 dapat menunjukkan pemetaan kebutuhan informasi *Chain Of Custody* dari beberapa sumber.

Tabel 4.1 Ekstraksi Kebutuhan Informasi *Chain Of Custody* Barang Bukti

NO	Kebutuhan informasi COC	Penjelasan	(Ashcroft et al., 2004)	(Dahiya & Sangwan, 2014)	(Thomson, 2011)	(Woods et al., 2013)	(Gayed et al., 2013)	(Giova, 2011)	(Anderson & ENISA, 2014)	(Ryder, 2021)	(Cosic et al., 2011)	(Graves, 2013)	(Coons, 2015)
1	Bukti Elektronik	Deskripsi perangkat atau spesifikasi temuan barang bukti elektronik, seperti model, manufaktur, tipe, kapasitas, kondisi pada saat ditemukan dan perangkat yang tersambung.	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗
2	Personel yang terlibat	Petugas atau individu yang melakukan interaksi atau terlibat secara langsung dengan barang bukti	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓
3	Lokasi penyimpanan barang bukti	Tempat atau ruang dimana barang bukti disimpan	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗
4	Kondisi lokasi penyimpanan barang bukti	Kondisi keamanan tempat penyimpanan barang bukti	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗
5	Bukti digital	Deskripsi *file* image hasil akuisisi seperti; nama *file*, ukuran dan format	✓	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗

Tabel 4.2 Ekstraksi Kebutuhan Informasi *Chain Of Custody* Barang Bukti Lanjutan

NO	Kebutuhan informasi COC	Penjelasan	(Ashcroft et al., 2004)	(Dahiya & Sangwan, 2014)	(Thomson, 2011)	(Woods et al., 2013)	(Gayed et al., 2013)	(Giova, 2011)	(Anderson & ENISA, 2014)	(Ryder, 2021)	(Cosic et al., 2011)	(Graves, 2013)	(Coons, 2015)
6	Proses mendapatkan barang bukti elektronik	Deskripsi aktivitas koleksi (*collection*) oleh petugas. Disebut juga sebagai proses olah Tempat Kejadian Perkara	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
7	Proses Akuisisi bukti elektronik	Deskripsi aktivitas ekstraksi atau *imaging* bukti elektronik untuk mendapatkan *file* digital di dalamnya	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓
8	Nilai Hash/MD5/SHA-1	Nilai hashing *file* hasil ekstraksi atau *imaging*	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓
9	Tanggal/Waktu	Informasi waktu terjadinya aktivitas forensik, interaksi dan perpindahan barang bukti	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓
10	Lokasi ditemukan bukti elektronik	Alamat dimana barang bukti diperoleh	✓	✓	✗	✗	✗	✓	✗	✗	✓		✓
11	Kasus	Deskripsi tentang kasus kejahatan yang melibatkan barang bukti	✓	✓	✓	✗	✓		✗	✗	✗	✗	✓
12	Korban dan pelaku	Nama lengkap dari pelaku dan korban kejahatan	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗

Tabel 4.3 Ekstraksi Kebutuhan Informasi *Chain Of Custody* Barang Bukti Lanjutan

NO	Kebutuhan informasi COC	Penjelasan	(Ashcroft et al., 2004)	(Dahiya & Sangwan, 2014)	(Thomson, 2011)	(Woods et al., 2013)	(Gayed et al., 2013)	(Giova, 2011)	(Anderson & ENISA, 2014)	(Ryder, 2021)	(Cosic et al., 2011)	(Graves, 2013)	(Coons, 2015)
13	Interaksi dan perpindahan	Catatan interaksi dan perpindahan seperti peminjaman dan pengeluaran barang bukti dari ruang penyimpanan	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗
14	*Role of evidence*	Alasan mengapa barang bukti dipilih sebagai barang bukti di dalam sebuah kasus dan catatan informasi yang diharapkan (*potensial sought*) sebagai bukti pendukung dalam mengungkap kasus	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
15	Akses	Individu yang melakukan interaksi dengan barang bukti adalah individu yang memiliki hak akses atau diberikan hak akses kepadanya	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗	✗
16	Perangkat yang digunakan	Nama perangkat yang digunakan selama proses mendapatkan barang bukti	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓

Berdasarkan pemetaan pada Tabel 4.1 sampai Tabel 4.3, kebutuhan informasi *Chain Of Custody* untuk barang bukti digital dapat disederhanakan menjadi beberapa kelompok informasi diantaranya :

1. Informasi kasus (*Case Information*), memuat informasi terkait identitas kasus yang dimiliki dari setiap barang bukti digital.
2. Informasi mendapatkan bukti elektronik (*Collection Information*), memuat informasi penting selama proses mendapatkan barang bukti elektronik dari tempat kejadian perkara.
3. Informasi mendapatkan bukti digital (*Acquisition Information*), memuat informasi proses akuisisi untuk mendapatkan *file* digital dari barang bukti elektronik.
4. Informasi deskripsi bukti Elektronik (*Electronic Evidence Description*), memuat informasi deskripsi baik secara fisik maupun spesifik dari barang bukti elektronik.
5. Informasi hasil akuisisi (*Image Description*), memuat informasi tentang deskripsi dari *file* image barang bukti termasuk nilai hash atau MD5/SHA-1 dari *file* image bukti digital setelah didapatkan dari barang bukti elektronik.
6. Informasi lokasi penyimpanan (*Storage Information*), memuat informasi lokasi dan kondisi penyimpanan barang bukti digital.
7. Informasi personel yang terlibat (*Personel Information*), memuat informasi mengenai siapa saja subyek / individu yang memiliki keterlibatan dengan barang bukti digital. Subyek tersebut dapat meliputi *first responder*, investigator forensik, saksi ahli, penegak hukum, petugas yang menangani manajemen barang bukti, dan pihak-pihak yang dapat terlibat dengan barang bukti apabila diberikan hak akses.
8. *Role of evidence*, memuat informasi mengenai alasan mengapa bukti elektronik dipilih sebagai barang bukti dalam kasus dan informasi apa saja yang diharapkan dapat diperoleh dari barang bukti tersebut
9. Interaksi dan perpindahan *(Chain Of Custody)*, memuat informasi mengenai apapun aktivitas / tindakan yang dikenakan terhadap barang bukti, kapan dan alasan mengapa aktivitas tersebut perlu dilakukan.

4.1.2 Identifikasi Field Informasi *Chain Of Custody*

Pada tahap ini, identifikasi *field* informasi untuk metadata *Chain Of Custody* adalah dengan melakukan ekstraksi dari beberapa model formulir *Chain Of Custody* barang bukti yang ada di internet. Selanjutnya, *field* informasi hasil dari identifikasi yang telah dilakukan

akan digunakan di dalam formulir usulan *Chain Of Custody* serta menentukan definisi dan relasi dari masing-masing *field* informasi.

1. Ekstraksi Model Informasi Formulir *Chain Of Custody*

   Field informasi untuk metadata *Chain Of Custody* didapatkan dengan melakukan ekstraksi *field* informasi dari beberapa contoh formulir *Chain Of Custody* yang sudah ada. Formulir yang digunakan dalam ekstraksi adalah formulir *Chain Of Custody* barang bukti untuk kasus *computer crime*. Meskipun memiliki tujuan yang sama, namun formulir ini memiliki karakteristik dan perbedaan. Perbedaan dapat terlihat dari jenis barang bukti dan jumlah item barang bukti yang dapat diakomodasi dalam satu formulir *Chain Of Custody*, informasi yang disimpan dan jumlah *field* informasi yang disediakan di dalam formulir. Diantara formulir yang digunakan untuk melakukan ekstraksi *field* informasi adalah formulir *Chain Of Custody* dari University *of* Pennsylvenia, Audit West, NIST (National Institute *of* Standards and Technology), Digital Forensic Lab dan PVL Forensics.

   Tabel 4.4 sampai Tabel 4.7 merupakan tabel Ekstraksi *field* informasi dari kelima formulir *Chain Of Custody* diatas. Berikut dapat dijabarkan perbedaan dari masing-masing formulir *Chain Of Custody* yang digunakan :

   - Formulir *Chain Of Custody* dari University *of* Pennsylvenia

     Merupakan formulir yang dapat digunakan untuk menyimpan catatan informasi barang bukti digital. Selain itu, formulir ini hanya dapat digunakan untuk mencatat satu item barang bukti yaitu satu formulir *Chain Of Custody* adalah untuk satu item barang bukti digital. Dalam formulir ini memuat beberapa kelompok informasi diantaranya; informasi bukti dan kasus, deskripsi barang bukti digital, histori *copy* dan histori transfer barang bukti.

   - Formulir *Chain Of Custody* dari Audit West

     Merupakan formulir yang digunakan untuk menyimpan catatan *Chain Of Custody* untuk barang bukti komputer elektronik. Dalam satu formulir ini hanya dapat digunakan untuk mencatat satu item barang bukti. Untuk informasi yang dicatat di dalam formulir ini adalah informasi deskripsi barang bukti, informasi penyitaan barang bukti dan informasi *Chain Of Custody*.

   - Formulir *Chain Of Custody* dari Digital Forensics Lab

     Merupakan formulir yang dapat digunakan untuk menyimpan catatan informasi barang bukti fisik/elektronik dan *file* digital hasil akuisisi dari bukti elektronik tersebut. Satu formulir *Chain Of Custody* Digital Forensics Lab digunakan

untuk mencatat satu item bukti fisik dan satu item bukti digital. Di dalam formulir ini, informasi yang dicatat adalah; nomor kasus dan nomor barang bukti, informasi proses mendapatkan barang bukti, detail informasi barang bukti elektronik, detail informasi barang bukti digital, *remarks*, informasi disposal penyerahan barang bukti dan tabel *Chain Of Custody*.

- Formulir *Chain Of Custody* dari NIST (*National Institute of Standards and Technology*)

  Merupakan formulir yang dapat digunakan untuk mencatat informasi lebih dari satu barang bukti elektronik dalam satu kasus kejahatan yang ditangani. Informasi di dalam formulir ini diantaranya; nomor kasus, petugas, nama korban, nama pelaku dan informasi penyitaan, deskripsi barang bukti, tabel *Chain Of Custody* dan tabel *final disposal* untuk informasi penyerahan atau pemusnahan barang bukti.

- Formulir *Chain Of Custody* dari PVL Forensics

  Merupakan formulir yang juga dapat digunakan untuk menyimpan catatan informasi lebih dari satu barang bukti. Informasi barang bukti yang dicatat di dalam formulir ini adalah untuk barang bukti digital, di antaranya; nama kasus dan nomor kasus, deskripsi barang bukti digital dan transfer *Chain Of Custody* dari barang bukti digital.

Tabel 4.4 Ekstraksi Model Informasi Formulir *Chain Of Custody*

No	**Kelompok Informasi**	**University of Pennsilvenia**	**Audit West**	**Digital Evidence Lab**	**NIST**	**PVL Forensics**	**Form Usulan**
1	Deskripsi bukti elektronik		Items No	Evidence No	Item No		Model
			Make	Device Type	Quantity		Serial Number
			Model	Manufacturer	Description		Type
			S/N	Capacity			Manufacturer
			Date/Time Computer	Model			Electronic Evidence No
			Attached Devices	Serial Number			Owner
			Notes	Additional Info			
			Name (Discovered Evidence)	Digital image taken?			
			Name (Seized Evidence)				
			Name (Forensic Activity)				
2	Lokasi Penyimpanan	Storage Location		Date/Time Stored			
		Storage Condition		Evidence Storage Location Time Stored			Time Stored
				Image Storage Location			
							Validator
3	Deskripsi Bukti Digital	Evidence Description		File Name		Evidence No	File Name
		Software to open		Size		Image Format	Size
		Item Number		Additional Info			Md5
				MD5 Sum			SHA-1
				SHA-1 Sum			SHA-256
							Degital Evidence
							Status

Tabel 4.5 Ekstraksi Model Informasi Formulir *Chain Of Custody* Lanjutan

No	**Kelompok Informasi**	**University of Pennsilvenia**	**Audit West**	**Digital Evidence Lab**	**NIST**	**PVL Forensics**	**Form Usulan**
4	Mendapatkan bukti elektronik (Collection)	Collection Method	Date	Date/Time Collected	Date/Time		Tools
		Date/Time Collected	Time	Site Address	Location		Date/Time
		Data of Collector	Description				Address
		Date of Collector Signature	Location				
5	Personel yang terlibat (First Responder)	Collector Name		Collector by	Officer Name/ID		First Responder Name
		Collector Signature					Position
							Agency
6	Akuisisi Bukti Elektronik			Date/Time Imageg		Date/Time	Acquisition Time
				Imaged by		Creator	Acquisition Tools
						Method	Acquisition Date
						Device Acquisition	Acquisition Officer
						Notes	Device
7	Identitas Kasus	Case Name	Case No	Case No	Case No	Case Name	Offence
			Page		Offence	Case Number	Suspect
					Victim		Victim
					Suspect		Case Number
8	Handover / Diposal			Date/Time	Item No (disposal)		
				Submited by	Suspect (disposal)		
				Signature	Method (disposal)		
				Received by	Officer (disposal)		
				Signature	Date (disposal)		
				Witnessed by	Signature (disposal)		

Tabel 4.6 Ekstraksi Model Informasi Formulir *Chain Of Custody* Lanjutan

No	**Kelompok Informasi**	**University of Pennsilvenia**	**Audit West**	**Digital Evidence Lab**	**NIST**	**PVL Forensics**	**Form Usulan**
				Signature	Item no (Destruction)		
				Remaks	Custodiao (Destruction)		
					ID (Destruction)		
					Date (Destruction)		
					Wittness (Destruction)		
					Signature (Destruction)		
					Date Sign (Destruction)		
					Item No (Release)		
					Custodian (Release)		
					ID (Release)		
					To Name (Release)		
					Address		
					City		
					State		
					Zip Code		
					Phone No		
					Signature owner		
					Date Sign (Release)		
					Copy attached?		
9	Informasi Interaksi Dan Perpindahan	Date	Registered Mail	Case No	Item No	Evidence No	Autorized by
		Copied By	Date	Evidence No	Date/Time	Date	Received by
		Copy Method	Time	Page No	Released Id	Time	Action

Tabel 4.7 Ekstraksi Model Informasi Formulir *Chain Of Custody* Lanjutan

No	**Kelompok Informasi**	**University of Pennsilvenia**	**Audit West**	**Digital Evidence Lab**	**NIST**	**PVL Forensics**	**Form Usulan**
		Disposition Of Original And All Copy	Released by	Submitter Name	Received by	From	Request time
		Transfered From	Signature	Signature	Comments/Location	Signature	Approve time
		Transfered To	Received by	Receiver Name		To	Received time
		Storage Location Now	Signature	Signature		Signature	
		Security Evidence Condition	Reason	Date/Time Submit		Description/Reason	
				Date/Time Receive			
				Evidence Modified			
10	Role Of Evidence						Reason For Foreclose
							Potential Information
11	Other					Form Dscription	
						Notes	

2. Identifikasi *Field* Informasi Formulir *Chain Of Custody*

Ekstraksi pada Tabel 4.4 Sampai Tabel 4.7 telah dikelompokkan berdasarkan kelompok kebutuhan informasi *Chain Of Custody* bukti digital yang dibutuhkan. Beberapa penelitian lain banyak mengelompokan informasi berdasarkan ontology, namun pada penelitian ini pengelompokan informasi dilakukan berdasarkan kesesuaian terhadap kelompok informasi yang telah diidentifikasi sebelumnya. Untuk memperoleh usulan field informasi dilakukan dengan cara menghapus beberapa field yang kurang sesuai dan menambahkan beberapa field yang dibutuhkan, sehingga tujuan dan kebutuhan informs *Chain Of Custody* dapat tercapai

Dari proses normalisai *field* informasi pada formulir diperoleh sebanyak 42 *field* informasi untuk formulir usulan. Beberapa *field* informasi dipilih dari formulir yang telah ada dan beberapa lainnya merupakan *field* informasi tambahan, diantaranya;

- Kelompok informasi **"Deskripsi bukti elektronik"** terdiri dari *field* informasi *Model, Serial Number, Type, Manufacturer,Electronic Evidence No,* dan *Owner*.
- Kelompok informasi **"Lokasi penyimpanan"** terdiri dari *field* informasi *time stored* dan *validator*.
- Kelompok informasi **"Deskripsi bukti digital"** terdiri dari *field* informasi *File Name, Size, Md5, SHA-1, SHA-256, Degital Evidence,* dan *Status*
- Kelompok informasi **"Mendapatkan bukti elektronik"** terdiri dari *field* informasi *tools, date/time* dan *address*.
- Kelompok informasi **"Perosnel yang terlibat"** terdiri dari *field* informasi *first responder name, position* dan *agency*.
- Kelompok informasi **"Akuisisi bukti elektronik"** terdiri dari *field informasi acquisition time, acquisition tools, acquisition date, acquisition officer* dan *device*.
- Kelompok informasi **"Identitas kasus"** terdiri dari *field* informasi *case number, offense, suspect* dan *victim*.
- Kelompok informasi **"Interaksi dan perpindahan"** terdiri dari *field informasi autorized by, received by, request time, approve time, received time* dan *action*.
- Kelompok informasi **"Role *of* evidence"** merupakan kelompok informasi tambahan yang sebelumnya tidak terdapat di dalam formulir. Informasi ini terdiri dari *field reason for foreclose* dan *potential information*.
- Sedangkan kelompok informasi **"lain-lain"** serta **"final disposal dan penyerahan"** barang bukti tidak digunakan atau dihilangkan di dalam formulir usulan.

Setiap *field* informasi pada formulir usulan merepresentasikan informasi tertentu pada formulir *Chain Of Custody* bukti digital. Berikut merupakan deskripsi dari masing-masing *field* informasi.

Tabel 4.8 *Field* Informasi Formulir Usulan *Chain Of Custody*

No	Nama Field	Keterangan
1	Case Number	Field informasi yang merepresentasikan nomor kasus dari barang bukti digital
2	Offence	*Field* informasi yang merepresentasikan tipe kasus dari tindak kejahatan. Misalnya tipe kejahatan sosial media, pelanggaran UU ITE dan lain-lain.
3	Suspect	*Field informasi yang merepresentasikan nama tersangka/pelaku kasus kejahatan*
4	Victim	*Field informasi yang merepresentasikan nama dari korban tindakan kejahatan*
5	First Responder Name	*Field informasi yang merepresentasikan nama dari Petugas yang melakukan olah TKP barang bukti*
6	Position	*Field* informasi yang merepresentasikan jabatan dan status dari petugas yang melakukan olah TKP barang bukti
7	Agency	*Field* informasi yang merepresentasikan organisasi / instansi yang menaungi petugas olah TKP
8	Tools	*Field* informasi yang merepresentasikan nama perangkat yang digunakan dalam melakukan proses olah TKP BB
9	Date/Time	*Field* informasi yang merepresentasikan tanggal dan waktu dilakukan proses olah TKP
10	Address	*Field* informasi yang merepresentasikan tempat/alamat olah TKP dilakukan
11	Electronic Evidence No	*Field* informasi yang merepresentasikan no register atau no daftar yang diberikan pada bukti elektronik
12	Model	*Field* informasi yang merepresentasikan model/seri dari bukti elektronik
13	Serial Number	*Field* informasi yang merepresentasikan nomor serial bukti elektronik
14	Type	*Field* informasi yang merepresentasikan tipe bukti elektronik. Misalnya komputer atau laptop
15	Owner	*Field* informasi yang merepresentasikan nama dari pemilik barang bukti elektronik
16	Acquisition Time	*Field* informasi yang merepresentasikan waktu dilakukan proses mendapatkan bukti digital dari bukti elektronik
17	Acquisition Tools	*Field* informasi yang merepresentasikan perangkat lunak yang digunakan untuk mendapatkan bukti digital
18	Device	*Field* informasi yang merepresentasikan perangkat keras yang digunakan untuk mendapatkan bukti digital
19	Acquisition Date	*Field* informasi yang merepresentasikan tanggal dilakukan proses akuisisi bukti elektronik
20	Acquisition Officer	*Field* informasi yang merepresentasikan nama petugas yang melakukan akuisisi
21	File Name	*Field* informasi yang merepresentasikan nama dan format dari *file* bukti digital hasil proses akuisisi
22	Size	*Field* informasi yang merepresentasikan ukuran dari *file* bukti digital

Tabel 4.9 *Field* Informasi Formulir Usulan *Chain Of Custody*

No	Nama Field	Keterangan
23	MD5	*Field* informasi yang merepresentasikan nilai MD5 yang dimiliki oleh *file* bukti digital
24	SHA-1	*Field* informasi yang merepresentasikan nilai SHA-1 yang dimiliki oleh *file* bukti digital
25	SHA-256	*Field* informasi yang merepresentasikan nilai SHA-256 yang dimiliki oleh *file* bukti digital
26	Status	*Field* informasi yang merepresentasikan status bukti digital. Terdapat 2 macam status yaitu open dan close. Open menunjukkan bahwa bukti digital masih dapat di akses dan masih digunakan untuk keperluan pengadilan. Close menunjukkan bahwa bukti digital telah selesai digunakan.
27	Storage Location	*Field informasi yang merepresentasikan lokasi (path) tempat dimana file bukti digital disimpan*
28	Time Stored	*Field* informasi yang merepresentasikan tanggal/waktu bukti digital disimpan di dalam lokasi penyimpanan
29	Validator	*Field* informasi yang merepresentasikan nama petugas validasi terhadap informasi *Chain Of Custody*
30	Reason For Foreclose	*Field* informasi yang merepresentasikan alasan mengapa BE ini dipilih sebagai BB dalam kasus, kaitannya dengan suspect dan victim
31	Potential Information	*Field* informasi yang merepresentasikan informasi apa yang diharapkan didapat dari BB ini yang akan mendukung proses investigasi
32	Autorized by	*Field* informasi yang merepresentasikan nama dari petugas pengelola yang memberikan akses terhadap bukti digital
33	Received by	*Field* informasi yang merepresentasikan nama dari petugas/individu/organisasi yang menerima akses bukti digital
34	Request time	*Field* informasi yang merepresentasikan tanggal dan waktu terjadinya permintaan akses terhadap bukti digital
35	Approve time	*Field* informasi yang merepresentasikan tanggal dan waktu disetujuinya permintaan akses terhadap bukti digital
36	Received time	*Field* informasi yang merepresentasikan tanggal dan waktu bukti digital telah diterima atau selesai di *download*
37	Action	*Field* informasi yang merepresentasikan alasan atau tindakan yang dilakukan terhadap bukti digital selama interaksi berlangsung

3. Pemetaan dan Spesifikasi Field Informasi

Dokumentasi *Chain Of Custody* setidaknya dapat memuat informasi perihal pertanyaan 5W+1H yaitu *What, Who, Where, When, Why* dan *How* tentang barang bukti di persidangan (Cosic et al., 2011). Berdasarkan rangkaian informasi pada formulir *Chain Of Custody* yang telah diusulkan, maka dapat dipetakan bagaimana konstruksi informasi dari konten metadata formulir usulan terhadap 5W+1H, sebagai berikut;

Tabel 4.10 Pemetaan Field Informasi

1	Who	:	First Responder, Suspect, Victim, Examiner, Officer, Law Enforcement
2	What	:	Spesifikasi dari Bukti Elektronik dan Bukti Digital yang didapat
3	Where	:	Lokasi olah TKP Bukti Elektronik dan lokasi Bukti Digital
4	When	:	Tanggal dan waktu olah TKP Bukti Elektronik, Akuisisi Bukti Elektronik dan Bukti Digital, Akses terhadap Bukti Digital
5	Why	:	Role of Evidence, Mengapa Bukti Elektronik dan Bukti Digital ini dipilih dalam kasus ini serta mengapa melakukan interaksi Bukti Digital
6	How	:	Bagaimana proses akuisisi dan imaging Bukti Digital, tools dan alatnya, dan bagaimana kondisi lokasi penyimpanan Bukti Elektronik dan Bukti Digital

Untuk lebih jelasnya, pemetaan field informasi formulir usulan *Chain Of Custody* berdasarkan kelompok informasi, konten informasi (*What, Where, When, Who, Why dan How)*, dapat di tunjukan pada Tabel 4.11 dan Tabel 4.12.

Tabel 4.11 Pemetaan Field Informasi Formulir Usulan *Chain Of Custody*

No	**Kelompok Informasi**	***Field* Informasi**	***Who***	***When***	***Where***	***What***	***Why***	***How***
1	Identitas Kasus (*Case*)	*Case Number*				■		
		Offense				■		
		Suspect	■					
		Victim	■					
2	*First Responder*	*First Responder Name*	■					
		Position	■					
		Agency	■					
3	Olah TKP Bukti Elektronik (Collection)	*Tools*				■		
		Date/Time		■				
		Address			■			
4	Bukti elektronik (*Electronic* Evidence)	*Model*				■		
		Serial Number				■		
		Type				■		
		Electronic Evidence No				■		
		Owner	■					
5	Proses Akuisisi	*Acquisition Time*		■				
		Acquisition Tools						■
		Acquisition Date		■				
		Acquisition Officer	■					
		Device				■		

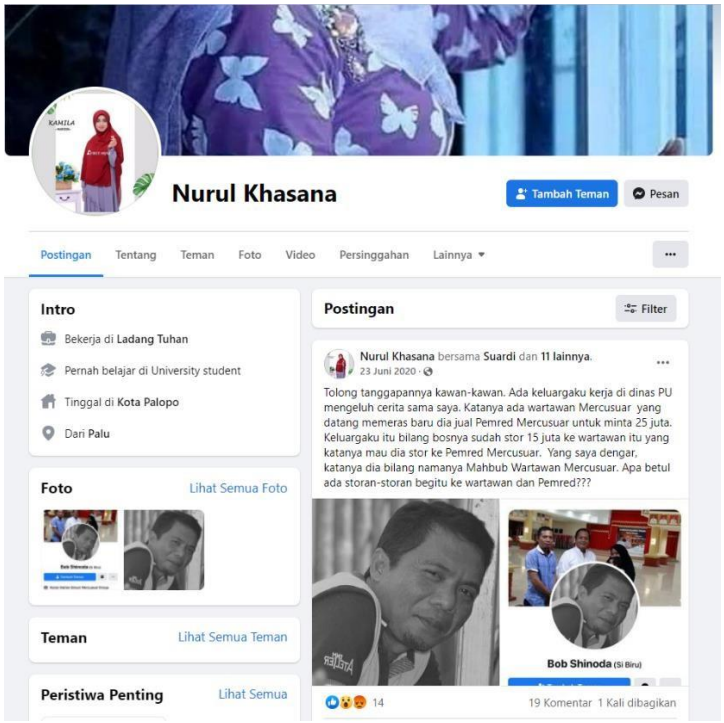
Tabel 4.12 Pemetaan Field Informasi Formulir Usulan *Chain Of Custody*

No	Kelompok Informasi	*Field* Informasi	*Who*	*When*	*Where*	*What*	*Why*	*How*
6	Hasil Imaging BE (ImageFile / Digital Evidence)	*File name*				■		
		Size				■		
		MD5				■		
		SHA-1				■		
		SHA-256				■		
		Status				■		
7	Lokasi Penyimpanan BD (Storage)	*Storage Location*			■			
		Time Stored		■				
		Validator	■					
8	*Role of Evidence*	*Reason For Foreclose*					■	
		Potential Information					■	
9	Interaksi Para Pihak (Interactions)	*Autorized by*	■					
		Received by	■					
		Request time		■				
		Approve time		■				
		Received time		■				
		Action					■	

4.1.3 Kebutuhan Investigasi Sosial Media Facebook Untuk Dokumentasi COC Bukti Digital Menggunakan Aplikasi Hunchly

Kebutuhan investigasi di sosial media facebook ini, akan melakukan investigasi terhadap salah satu akun facebook yang atas nama "Nurul Khasana" dengan menggunakan tools Hunchly. Proses ini dilakukan untuk melakukan simulasi kasus dengan menggunakan tools Hunchly Pada proses ini Akun Facebook atas nama "Nurul Khasana" diduga telah melakukan fitnah terhadap salah satu wartawan yang atas nama Mahbub alias Bob. Dalam dinding akun Facebooknya, akun atas nama Nurul Khasana telah menuliskan sebuah status yang berisi "*Tolong tanggapannya kawan-kawan. Ada keluargaku kerja di dinas PU mengeluh cerita sama saya. Katanya ada wartawan Mercusuar yang datang memeras baru dia jual Pemred Mercusuar untuk minta 25 juta. Keluargaku itu bilang bosnya sudah stor 15 juta ke wartawan itu yang katanya mau dia stor ke Pemred Mercusuar. Yang saya dengar,*

katanya dia bilang namanya Mahbub Wartawan Mercusuar. Apa betul ada storan-storan begitu ke wartawan dan Pemred???".



Gambar 4.2 Halaman Profil Akun Facebook

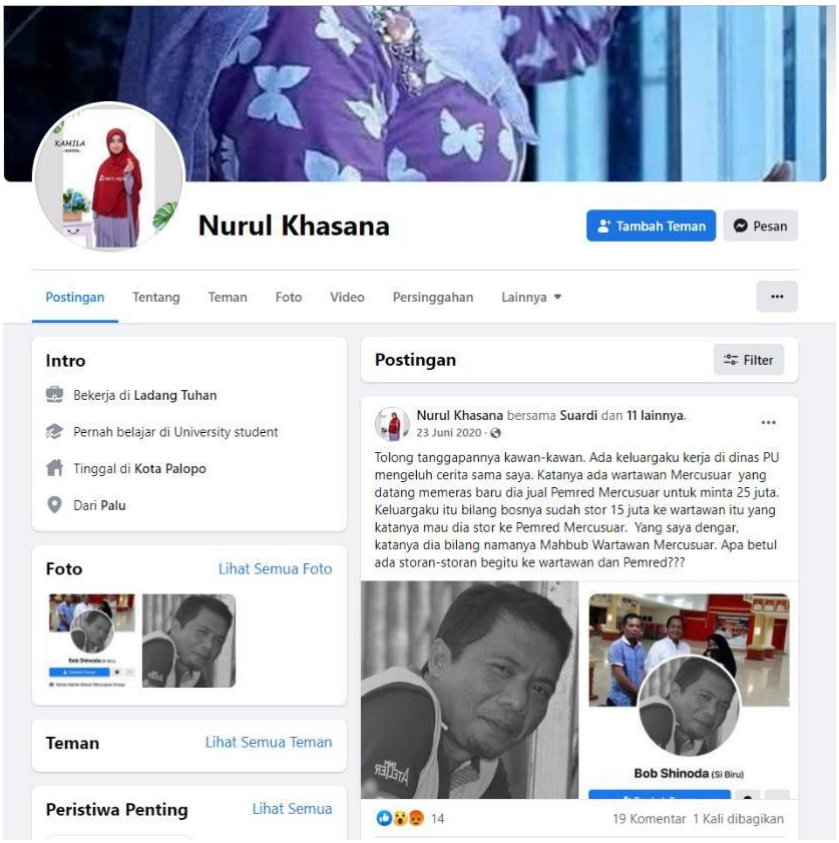
4.1.4 Study Kasus Untuk Proof Of Concept Dukumentasi COC Bukti Digital Sosial Media Facebook

Pada tahapan ini akan dilakukan investigasi pada akun atas nama "Nurul Khasana" dengan menggunakan Tools Hunchly. Pada proses ini akan dilakukan capture pada halaman web google chrome dengan menggunakan tools Hunchly. Proses pengujian ini akan menerapkan proses Chain Of Custudy yang telah di rancang dengan pemanfaatan tools Hunchly. Hal ini dilakukan untuk mengetahui hubungan antara desain *Chain Of Custody* yang telah di rancang dan pemanfaatan tools Hunchly.

Pada proses investigasi ini, ada beberapa data yang akan di kumpulkan, di antaranya Platform apa yang digunakan, di mana postingan tersebut di buat, Mengapa dia membuat postingan tersebut, Kapan postingan di buat, Siapa yang membuat postingan, dan bagaimana isi postinganya. Pada proses investigasi, di temukan bahwa Postingan ini di buat di media sosial facebook. Berikut proses penerapan antara desain *Chain Of Custody* dan penggunaan tools Hunchly.

1. Identifikasi Kasus

- Case Number merupakan informasi yang merepresentasikan nomor kasus dari barang bukti digital. Case Number ini yang akan membedakan nomor dari setiap kasus yang di tangani. Dalam proses inivestigasi ini Case Number yang di berikan adalah Case 001.
- Offense merupakan informasi yang merepresentasikan tipe kasus dari tindak kejahatan. Offense ini akan juga akan menjelaskan tipe dari sosial media apa yang menjadi pelanggaran. Dalam proses investigasi ini jenis Offence adalah sosial media Facebook.
- Suspect merupakan informasi yang mempresentasekan nama tersangka atau pelaku kasus kejahatan, dalam proses investigasi ini dilakukan proses investigasi terhadap salah satu akun media sosial facebook aas nama Nurul Khasana. Hala ini berdasarkan laporan atas nama Bob Shinoda atas dugaan pencemaran nama baik dan pelanggaran UU ITE.

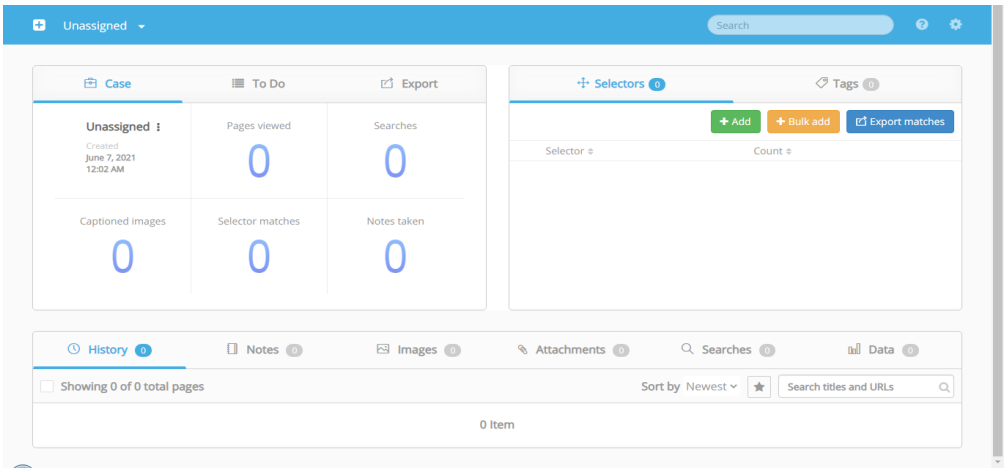


Gambar 4.3 Halaman beranda akun Nurul Khasana

- Victim merupakan informasi yang merepresentasikan nama dari korban tindakan kejahatan. Dalam proses investigasi ini, yang menjadi korban atau pelapor dari tindak kejahatan ini adalah atas nama Bob Shinoda. Dalam proses ini pelapor atas

nama Bob Sinoda ini, pelapor merasa pelaku telah melakukan pencemaran nama baik dan melanggar undang-undang ITE dengan status yang di buat dalam media sosial facebook seperti yang terlihat pada gambar 4.3.

2. First Responder
    - First Responden Name merupakan informasi yang mempresentasekan nama dari petugas yang melakukan olah TKP barang bukti. Dalam proses penanganan bukti digital First Responder ini menjadi hal yang sangat penting karena menjadi proses mekanisme awal yang penting untuk menganalisis barang bukti, keahlian tersebut merupakan tanggung jawab untuk melindungi TKP serta mengontrol perubahan yang dilakukan TKP dengan kemampuan terbaik yang dimiliki serta mengidentifikasi dan mengumpulkan bukti yang ada pada TKP. Di mana dalam penentuan barang bukti itu diterima (sah) atau tidak dimata hukum tergantung dari seorang responder jika dalam mekanisme yang dilakukan salah maka bisa mengurangi barang bukti dan mempengaruhi proses analisis. Dalam proses investigasi ini yang menjadi First Responder Name adalah atas nama Virjayanti Lazinu.
    - Position merupakan informasi yang merepresentasikan jabatan dan status dari petugas yang melakukan olah TKP barang bukti. Dalam proses investigasi ini Position yang melakukan identifikasi kasus adalah Penyidik./ First Responder.
    - Agency merupakan informasi yang merepresentasikan organisasi / instansi yang menaungi petugas olah TKP. Dalam proses ini organisasi / instasi yang menaungi penyidik /First Reponder adalah Pusat Digital Forensik UII.
3. Olah TKP Bukti Elektronik (Collection)
    - Tools merupakan informasi merepresentasikan nama perangkat yang digunakan dalam melakukan proses olah TKP BB. Dalam proses investigasi ini tools yang digunakan adalah Huncly.



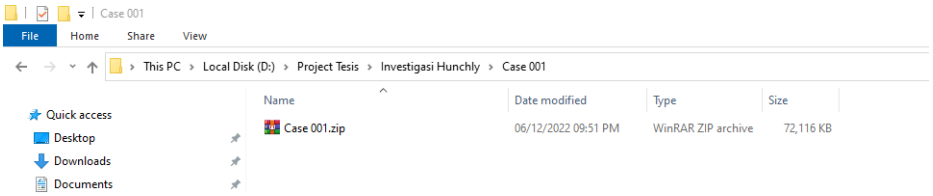
Gambar 4.4 Tampilan Dashboard Hunchly.

- Date/Time merupakan informasi merepresentasikan merepresentasikan tanggal dan waktu dilakukan proses olah TKP. Dalam proses investigasi ini Date/Time saat dilakukan olah TKP barang bukti adalah 12 Juni 2022, 2022 / 3:02 PM.
- Address merupakan informasi merepresentasikan tempat/alamat dilakukanya olah TKP dilakukan. Dalam proses investigasi ini tempat / alamat olah TKP adalah Laboratorium Pusat Digital Forensik UII.

4. Bukti Elektronik (Electronic Evidence)
    - Model merupakan informasi merepresentasikan model/seri dari bukti elektronik. Model seri ini penomoran dari barang bukti yang di tangani. Model ini di tentukan langsung oleh agency yang menangani barang bukti. Model barang bukti dari dari proses investigasi barang bukti ini adalah Case001/XI/22/Pusfid/UII.
    - Serial Number merupakan informasi merepresentasikan nomor serial bukti elektronik. Dari proses investigasi ini Serial Number barang bukti ini adalah Case001120720220302.
    - Type merupakan informasi merepresentasikan tipe bukti elektronik. Misalnya komputer atau laptop. Dalam proses investigasi ini Type dari bukti elektronik adalah Akun sosial media Facebook.
    - Electronic Evidence No merupakan informasi merepresentasikan no register atau no daftar yang diberikan pada bukti elektronik. Dalam proses investigasi ini nomor dari elektonik evidence adalah Reg Case001/DE/XI/22/Pusfid/UII.

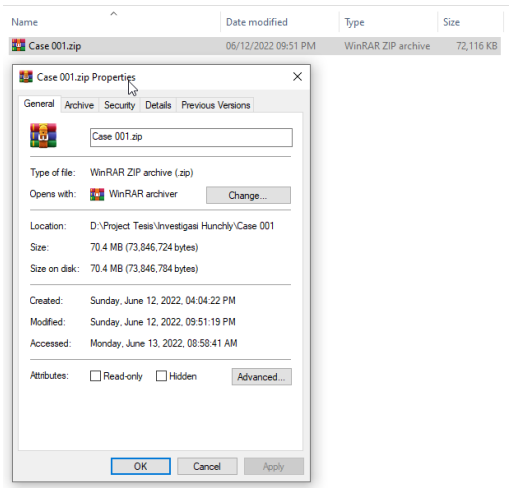
- Owner merupakan informasi merepresentasikan nama dari pemilik barang bukti elektronik. Dalam proses investigasi ini owner dari barang bukti adalah Virjayanti Lazinu.

5. Proses Akuisisi
    - Acquisition Time merupakan informasi merepresentasikan waktu dilakukan proses mendapatkan bukti digital dari bukti elektronik. Dalam proses investigasi ini waktu mendapatkan barang bukti digital adalah pukul 3:02 PM.
    - Acquisition Tools merupakan informasi merepresentasikan perangkat lunak yang digunakan untuk mendapatkan bukti digital. Proses investigasi ini menggunakan tools Hunchly.
    - Acquisition Date merupakan informasi merepresentasikan tanggal dilakukan proses akuisisi bukti elektronik. Dalam proses investigasi ini barang bukti di dapatkan pada tanggal 12 Juni 2022.
    - Acquisition Officer merupakan informasi merepresentasikan nama petugas yang melakukan akuisisi. Dalam proses investigasi ini petugas yang bertanggung jawab melakukan akuisisi untuk mendapatkan barang bukti digital adalah Virjayanti Lazinu.
    - Device merupakan informasi merepresentasikan perangkat keras yang digunakan untuk mendapatkan bukti digital. Pada proses investigasi untuk mendapatkan barang bukti menggunakan perangkat berupa Laptop.
6. Hasil Imaging BE (Image File/ Digital Evidence)
    - File name merupakan informasi merepresentasikan nama dan format dari *file* bukti digital hasil proses akuisisi. Setelah proses melakukan Analisis untuk mendapatkan barang bukti digital dengan menggunakan tools Hunchly, barang bukti yang di dapatkan kemudian di ekspor. Hasil ekspor barang bukti digital ini berupa file Zip dengan nama Case001.zip.



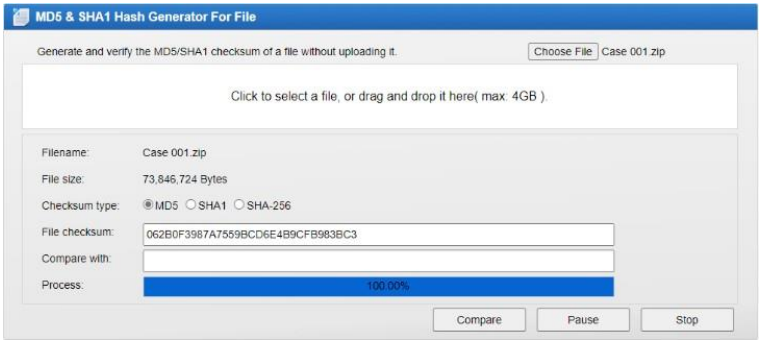
Gambar 4.5 File name barang bukti

- Size merupakan informasi merepresentasikan ukuran dari file bukti digital. Dalam proses investigasi ini ukuran dari file barang bukti yang di dapatkan adalah 70.4 MB (73,846,724 bytes).



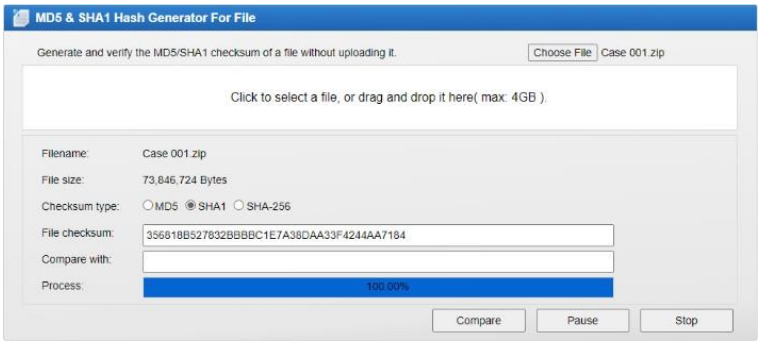
Gambar 4.6 Size barang bukti

- MD5 merupakan informasi merepresentasikan nilai MD5 yang dimiliki oleh *file* bukti digital. Nilai dari MD5 dari bukti digital dengan file name Case001.zip adalah 062B0F3987A7559BCD6E4B9CFB983BC3



Gambar 4.7 Nilai MD5 barang bukti

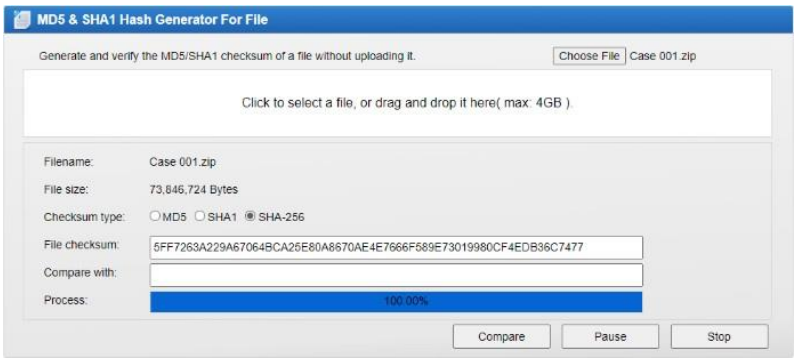
- SHA-1 merupakan informasi merepresentasikan nilai SHA-1 yang dimiliki oleh *file* bukti digital. Nilai SHA-1 dari bukti digital dengan file name Case001.zip adalah 356818B527832BBBBC1E7A38DAA33F4244AA7184



Gambar 4.8 Nilai SHA-1 barang bukti

- SHA-256 adalah informasi merepresentasikan nilai SHA-256 yang dimiliki oleh *file* bukti digital. Nilai SHA-256 dari bukti digital dengan file name Case001.zip

5FF7263A229A67064BCA25E80A8670AE4E7666F589E73019980CF4EDB3
6C7477

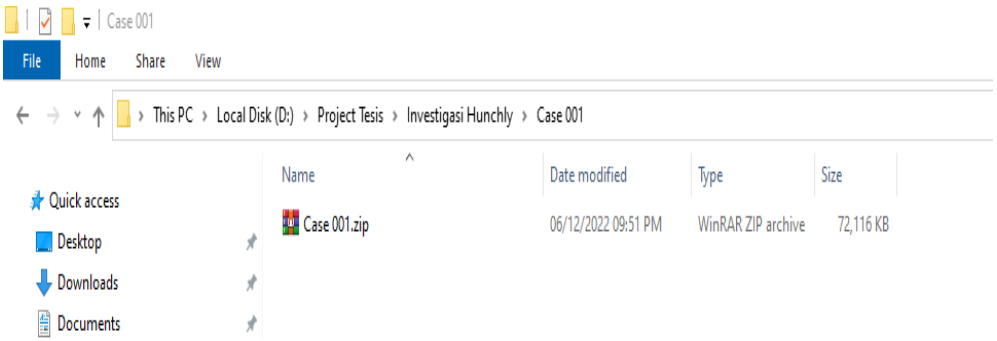


Gambar 4.9 Nilai SHA-256 barang bukti

- Status merupakan informasi merepresentasikan status bukti digital. Terdapat 2 macam status yaitu open dan close. Open menunjukkan bahwa bukti digital masih dapat di akses dan masih digunakan untuk keperluan pengadilan. Close menunjukkan bahwa bukti digital telah selesai digunakan. Dalam proses penyidikan barang bukti ini status dari bukti digital ini adalah open karena bukti digital ini masih dapat di akses dan masih digunakan untuk keperluan pengadilan.

7. Lokasi Penyimpanan BD(Storage)

- Storage Location merupakan informasi merepresentasikan *lokasi (path) tempat di mana file bukti digital disimpan.* Dalam proses investigasi ini lokasi penyimpanan barang bukti adalah D:\Project Tesis\Investigasi Hunchly\Case001



Gambar 4.10 Store Location Barang Bukti

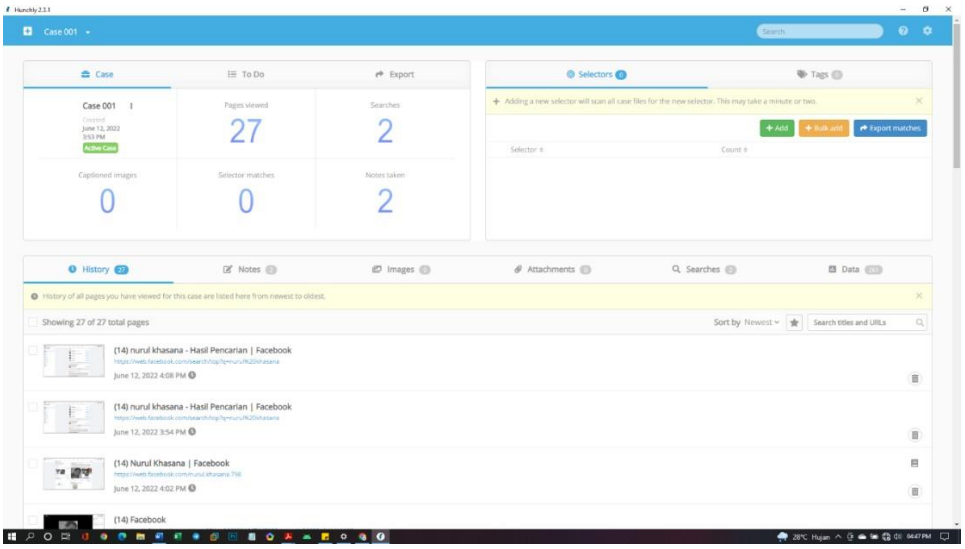
- Time Stored merupakan informasi merepresentasikan tanggal/waktu bukti digital disimpan di dalam lokasi penyimpanan. Tanggal/waktu penyimpanan barang bukti ini adalah Sunday, June 12, 2022, 04:04:22 PM
- Validator merupakan informasi merepresentasikan nama petugas validasi terhadap informasi *Chain Of Custody*. Petugas yang melakukan validasi terhadap informasi *Chain Of Custody* adalah Yudi Prayudi

8. Role Of Evidence

- Reason For Foreclose merupakan informasi merepresentasikan alasan mengapa bukti elektronik ini dipilih sebagai barang bukti dalam kasus, kaitannya dengan suspect dan victim. Dalam proses investigasi kasus ini yang menjadi bukti digital dalam kasus ini adalah Postingan pada halaman dinding beranda Akun Nurul Khasana alasan barang bukti ini dipilih sebagai barang bukti digital adalah karena dari postingan dari akun nurul khasa tersebut diduga telah melakukan fitnah terhadap Bob Shinoda.

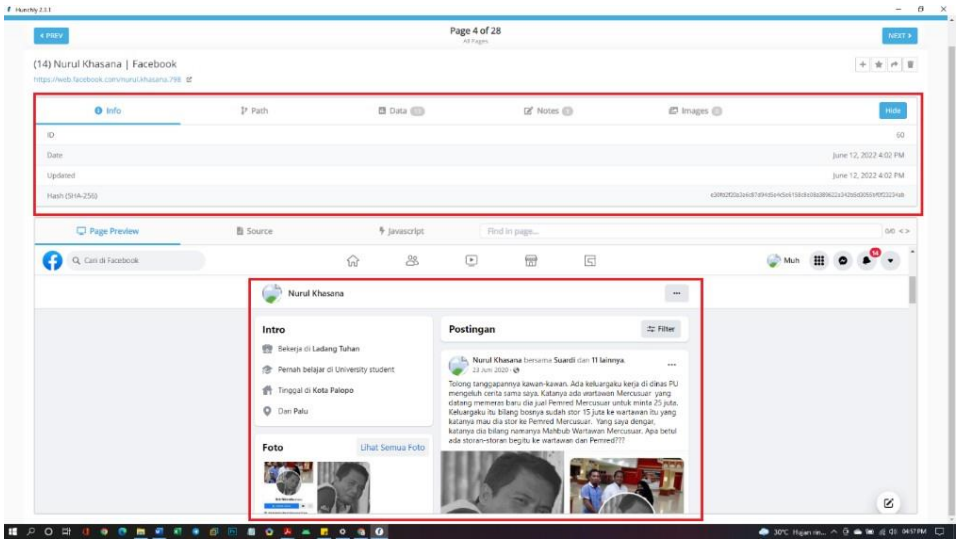
  Pada proses investigasi ini, ada beberapa data yang akan di kumpulkan, diantaranya Platform apa yang digunakan, Di mana postingan tersebut di buat, Mengapa dia membuat postingan tersebut, Kapan postingan di buat, Siapa yang membuat postingan, dan bagaimana isi postinganya.

  Pada proses investigasi, di temukan bahwa Postingan ini di buat di media sosial facebook. Postingan pada dinding facebook ini di buat untuk meminta tanggapan terhadap kawan-kawan tentang adanya dugaan pemerasan yang dilakukan oleh salah satu wartawan Mercusuar. Postingan ini dibuat pada Selasa, 23 Juni 2020 Pukul 20.09 Wita. Postingan dibuat atas nama Nurul Khasana. Isi dari postingan atas nama akun facebook Nurul Khasana adalah "*Tolong tanggapannya kawan-kawan. Ada keluargaku kerja di dinas PU mengeluh cerita sama saya. Katanya ada wartawan Mercusuar yang datang memeras baru dia jual Pemred Mercusuar untuk minta 25 juta. Keluargaku itu bilang bosnya sudah stor 15 juta ke wartawan itu yang katanya mau dia stor ke Pemred Mercusuar. Yang saya dengar, katanya dia bilang namanya Mahbub Wartawan Mercusuar. Apa betul ada storan-storan begitu ke wartawan dan Pemred???*".



Gambar 4.11 Proses pengumpulan data Hunchly

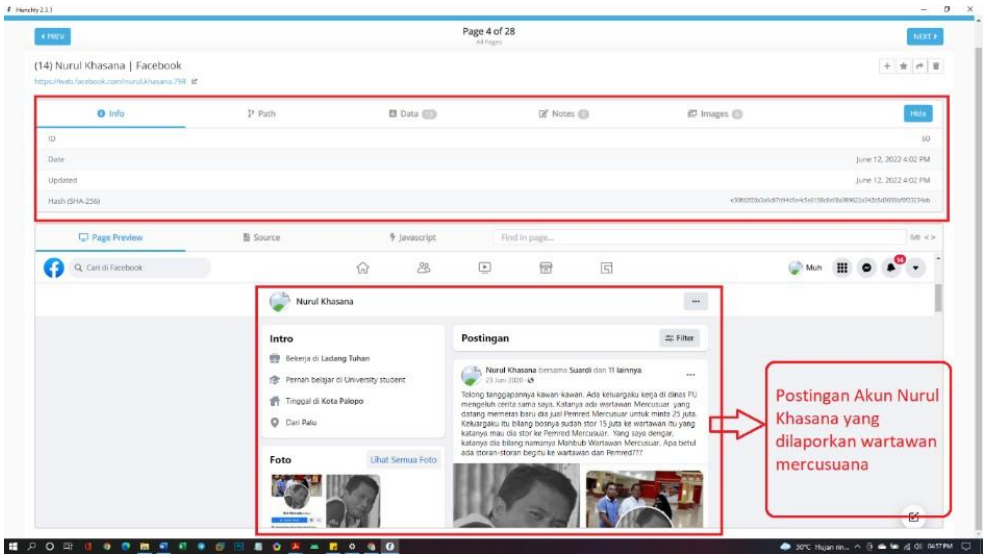
Pada gambar 4.11 di atas, dilakukan proses investigasi dengan melakukan capture menggunakan tools Hunchly. Proses investigasi ini di beri nama Case 001. Proses investigasi dengan menggunakan tools Hunchly ini telah mencapture 27 Page Viewed, 2 Searches, 2 Notes taken, dan 261 Data.



Gambar 4.12 Investigasi Halaman Dinding Akun

Pada gambar 4.12 , dilakukan investigasi halaman dinding akun facebook Nurul Khasana dengan melakukan capture pada tools Hunchly. Proses ini memiliki ID 60, Date June 12, 2022 4:02 PM, June 12, 2022 4:02 PM, Hash (SHA-256) : e30fd2f20a3a6c87d94d5e4c5e6158c8e08a389622a342b5d3055bf0f23234ab.

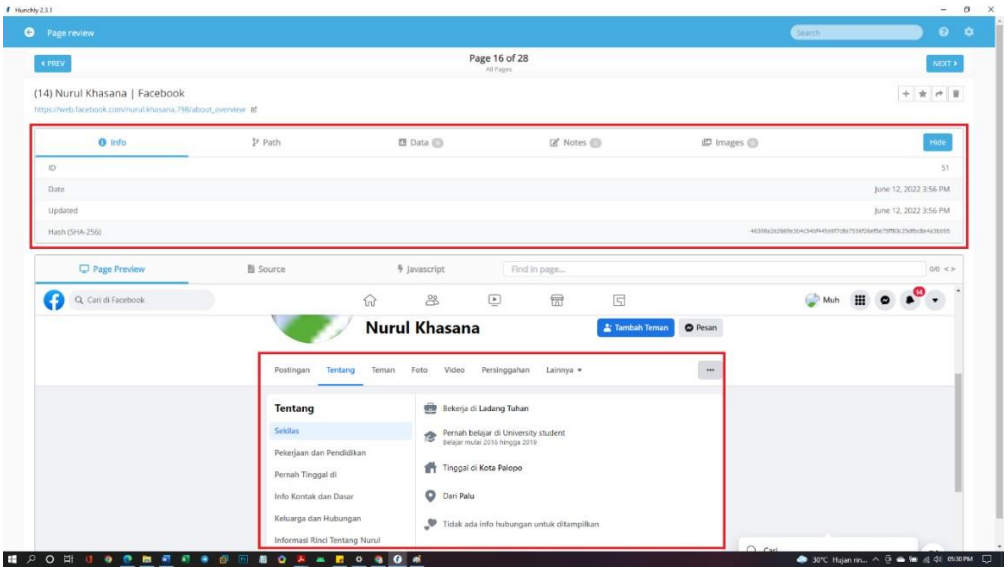
Pada proses ini di temukan isi postingan dari akun Nurul Khasana yang berisi "*Tolong tanggapannya kawan-kawan. Ada keluargaku kerja di dinas PU mengeluh cerita sama saya. Katanya ada wartawan Mercusuar yang datang memeras baru dia jual Pemred Mercusuar untuk minta 25 juta. Keluargaku itu bilang bosnya sudah stor 15 juta ke wartawan itu yang katanya mau dia stor ke Pemred Mercusuar. Yang saya dengar, katanya dia bilang namanya Mahbub Wartawan Mercusuar. Apa betul ada storan-storan begitu ke wartawan dan Pemred???*" Seperti yang terlihat pada gambar 4.13.



Gambar 4.13 Postingan akun sebagai bukti

- Potential Information merupakan informasi merepresentasikan informasi apa yang diharapkan didapat dari barang bukti ini yang akan mendukung proses investigasi.

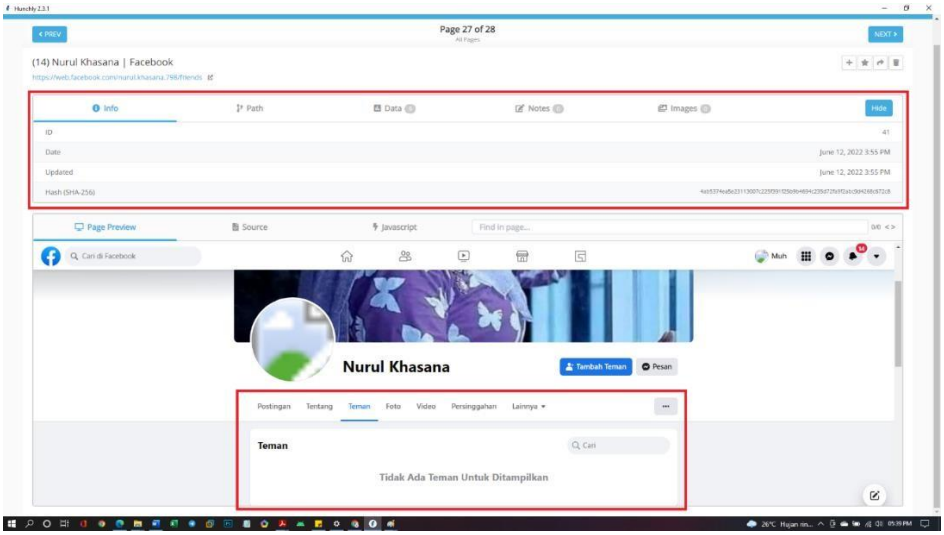
Setelah di temukan isi postingan dari akun facebook Nurul Khasana, dilakukan proses investigasi lanjutan untuk mengumpulkan data-data dari akun Nurul Khasana. Data-data yang dikumpulkan adalah Halaman Tentang, Teman, Foto, Video, Persinggahan. Proses ini dilakukan untuk mendukung bukti artefak digital.



Gambar 4.14 Pencarian bukti di halaman Tentang

Dari informasi pada gambar 4.14 hasil capture dengan tools Hunchly dengan ID 51, Date June 12, 2022 3:56 PM, Updated June 12, 2022 3:56 PM, Hash (SHA-256) 46398a2e2669e3b4c34bf445e6f7c8e7556f26ef5e75ff83c25d fbc8e4a3bb95 di temukan bahwa akun Nurul Khasana Bekerja di Ladang Tuhan, Pernah belajar di University students dari 2016 sampai 2019. Tinggal di kota Palopo, dari Palu.

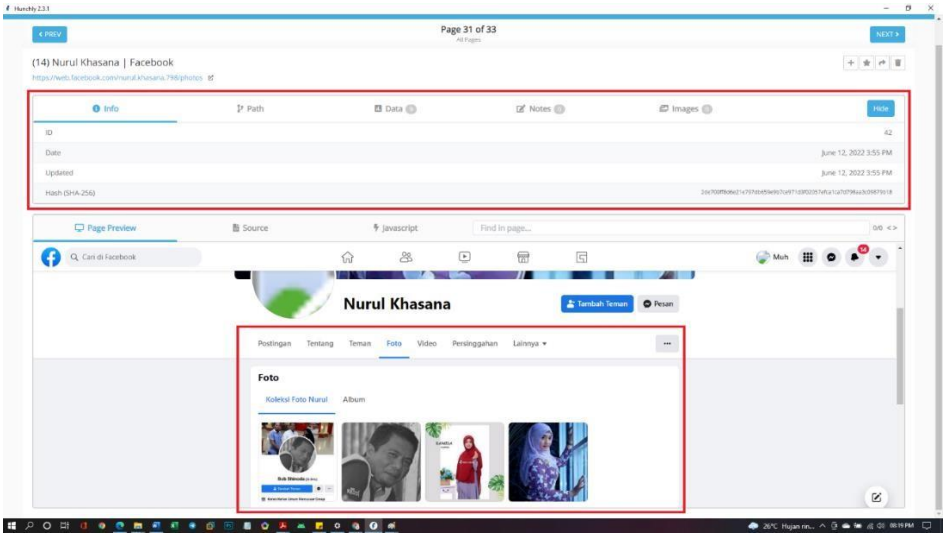
Pada informasi teman di akun facebook Nurul Khasana, tidak di temukan akun facebook yang menjadi teman seperti yang terlihat pada gambar 4.15.



Gambar 4.15 Pencarian bukti di halaman Pertemanan

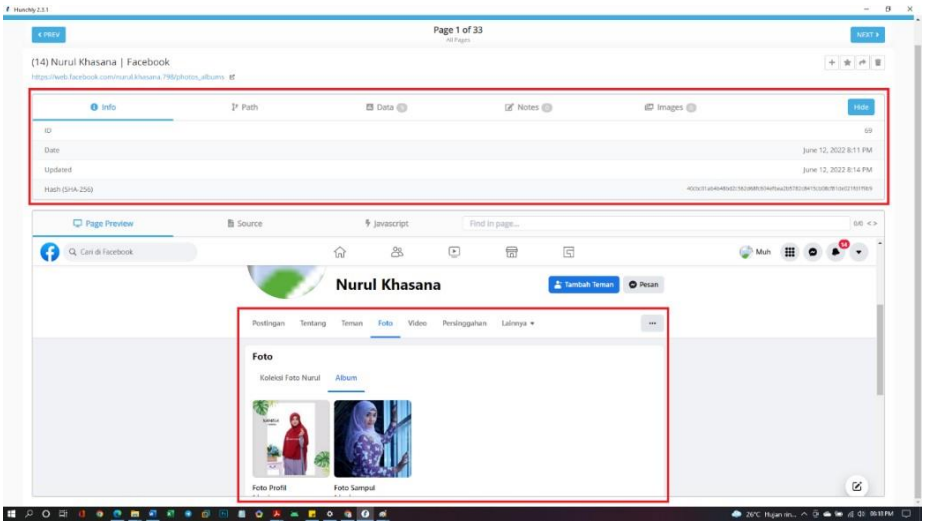
Pada gambar 4.15 hasil capture dengan tools Hunchly dilakukan Analisis terhadap teman facebook akun Nurul Khasana. Dari proses investigasi dengan ID 41, Date June 12, 2022 3:55 PM, Updated June 12, 2022 3:55 PM, Hash (SHA-256) 4ab5374ea5e23113007c225f391f25b9b4694c235d72fa9 f2abc9d4268c67 2c8 tidak ditemukan teman dari akun facebook Nurul Khasana. Akun ini tidak memiliki pertemanan pada akunnya.

Pada proses pengumpulan informasi di akun facebook Nurul Khasana untuk mengecek Foto dan Album pada akun tersebut, ditemukan 4 foto dan 2 album dari akun tersebut seperti yang terlihat pada gambar 4.16 dan 4.17.



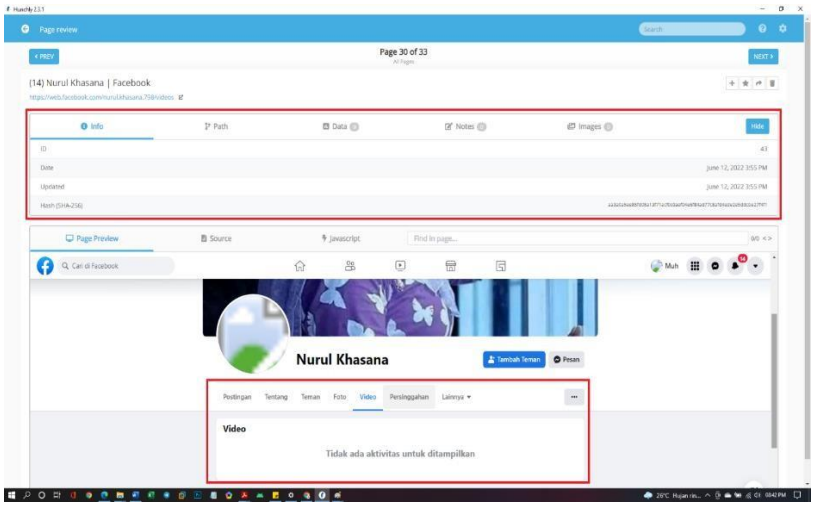
Gambar 4.16 Pencarian bukti di halaman Foto

Dari hasil investigasi seperti pada gambar 4.16 Koleksi foto pada akun facebook milik Nurul Khasana hasil capture dengan tools Hunchly dengan capture ID :42, Date June 12, 2022 3:55 PM, Updated June 12, 2022 3:55 PM, Hash (SHA-256) 2de700ff8d6e21e797db659e9b7ce971d3f02057efca1ca7d7 98aa3c09879b18 ditemukan 4 foto yang dimiliki akun tersebut.



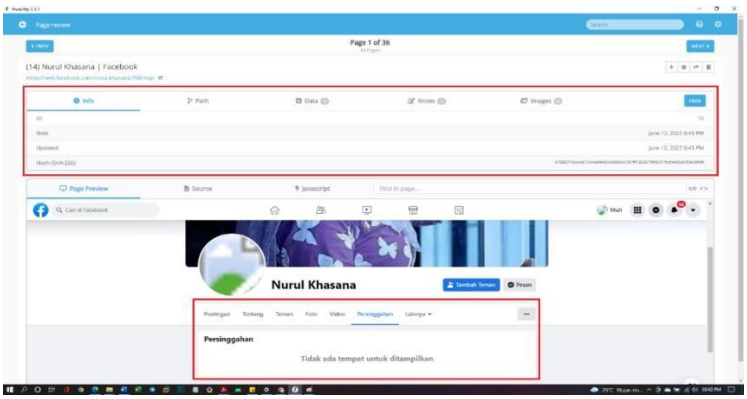
Gambar 4.17 Pencarian bukti di halaman Album

Selain itu pada proses investigasi untuk mengetahui informasi Album yang dimiliki akun Nurul Khasana berdasarkan hasil capture dengan tools Hunchly dengan capture ID: 69, Date: June 12, 2022 8:11 PM, Updated June 12, 2022 8:36 PM, Hash (SHA-256) e1c97dd1f4816ea6cc3ba5ceb5dbf09d97bb9 f215371170fdb44915b31828f69ditemukan 2 album milik akun Nurul Khasana seperti yang terlihat pada gambar 4.17.



Gambar 4.18 Pencarian bukti di halaman Video

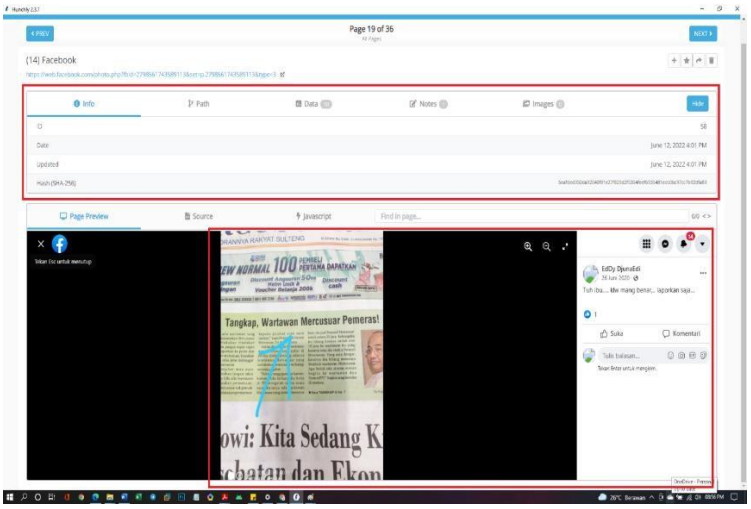
Pencarian informasi pada Video dan Persinggahan dari akun Nurul Khasana, tidak di temukan data seperti yang terlihat pada gambar 4.18 dengan ID: 43, Date: June 12, 2022 3:55 PM, Updated: June 12, 2022 3:55 PM, Hash (SHA-256) aa3a0a5ee85fd08a13f71acf0c0aef04e6f84ad77c8afd4ed e2e5ddc be27f4f1



Gambar 4.19 Pencarian bukti di halaman Persinggahan

Kemudian pada pencarian di halaman persinggahan, capture Persinggahan seperti pada Gambar 4.19 dengan ID: 72, Date: June 12, 2022 8:43 PM, Updated: June 12, 2022 8:43 PM, Hash (SHA-256) 47583716cacc6144 4e9e894a98 865c787ff1353479f0b31fbd0ed5a000e09fd8

Pada proses investigasi juga di temukan gambar yang di sematkan pada kolom komentar akun Nurul Khasana Yang berisi berita koran kasus yang menimpa wartawan Mercusuar seperti yang dapat pada gambar 4.13 dengan ID: 58, Date: June 12, 2022 4:01 PM, Updated: June 12, 2022 4:01 PM, Hash (SHA-256) eafded350da92040f81e27f829d2f5304feef6935481edc0bc97cc7b92dfa89



Gambar 4.20 Berita Koran dari halaman komentar

9. Interaksi Para Pihak (Interaction)
    a. Autorized by merupakan informasi merepresentasikan nama dari petugas pengelola yang memberikan akses terhadap bukti digital. Petugas pengelola yang memberikan akses terhadap bukti digital adalah Yudi Prayudi
    b. Received by merupakan informasi merepresentasikan nama dari petugas/individu/organisasi yang menerima akses bukti digital.

Petugas/Individu/Organisasi yang menerima akses bukti digital adalah Yudi Prayudi

c. Request time merupakan informasi merepresentasikan tanggal dan waktu terjadinya permintaan akses terhadap bukti digital. Tanggal dan waktu terjadinya permintaan akses terhadap bukti digital adalah Sunday, June 12, 2022, 08:01:25 PM
d. Approve time merupakan informasi merepresentasikan tanggal dan waktu disetujuinya permintaan akses terhadap bukti digital. Tanggal dan waktu disetujuinya permintaan akses terhadap bukti digital adalah Sunday, June 12, 2022, 09:04:22 PM
e. Received time merupakan informasi merepresentasikan tanggal dan waktu bukti digital telah diterima atau selesai di *download.* Tanggal dan waktu bukti digital telah diterima atau selesai di *download adalah* Sunday, June 12, 2022, 09:30:02 PM
f. Action merupakan informasi merepresentasikan alasan atau tindakan yang dilakukan terhadap bukti digital selama interaksi berlangsung. Alasan atau tindakan yang dilakukan terhadap bukti digital selama interaksi berlangsung adalah Melakukan pengembangan dan Validasi barang bukti

4.1.5 Dokumentasi *Chain Of Custody* untuk kasus sosial media Facebook

Dokumentasi *Chain Of Custody* di perlukan untuk mencatat segala sesuaitu yang berkaitan dengan barang bukti digital. Proses pencatatan dimulai dari Identifikasi kasus, Informasi Kasus, Pemgambilan Barang Bukti, Petugas Beratnggung Jawab dan pengisian Evidence *Chain Of Custody* Tracking Form dari barang bukti.

Tabel 4.13 Dokumen *Chain Of Custody* dari form usulan

A	**Identitas Kasus (*Case*)**			
	1	*Case Number*	:	
	2	*Offense*	:	
	3	*Suspect*	:	
	4	*Victim*	:	
B	***First Responder***			
	1	*First Responder Name*	:	
	2	*Position*	:	
	3	*Agency*	:	
C	**Olah TKP Bukti Elektronik (Collection)**			
	1	*Tools*	:	
	2	*Date/Time*	:	
	3	*Address*	:	
D	**Bukti elektronik (*Electronic* Evidence)**			
	1	*Model*	:	
	2	*Serial Number*	:	
	3	*Type*	:	
	4	*Electronic Evidence No*	:	
	5	*Owner*	:	
E	**Proses Akuisisi**			
	1	*Acquisition Time*	:	
	2	*Acquisition Tools*	:	
	3	*Acquisition Date*	:	
	4	*Acquisition Officer*	:	
	5	*Device*	:	
F	**Hasil Imaging BE (ImageFile / Digital Evidence)**			
	1	*File name*	:	
	2	*Size*	:	
	3	MD5	:	
	4	SHA-1	:	
	5	SHA-256	:	
	6	*Status*	:	
G	**Lokasi Penyimpanan BD (Storage)**			
	1	*Storage Location*	:	
	2	*Time Stored*	:	
	3	*Validator*	:	
H	***Role of Evidence***			
	1	*Reason For Foreclose*	:	
	2	*Potential Information*	:	

Tabel 4.14 Dokumen *Chain Of Custody* dari form usulan (Lanjutan)

I	**Interaksi Para Pihak (Interactions)**			
	1	*Autorized by*	:	
	2	*Received by*	:	
	3	*Request time*	:	
	4	*Approve time*	:	
	5	*Received time*	:	
	6	*Action*	:	

4.2 Implementasi Konsep *Chain Of Custody*

Pada penelitian ini proses implementasi dari Chain Of Costudy dapat di lihat pada tahapan pengumpulan barang bukti dengan menggunakan tools Hunchly. Proses ini menerjemahkan konsep *Chain Of Custody* dalam proses investigasi kejahatan sosial media *facebook* dengan menggunakan tools yang dapat membantu penyidik dalam menemukan bukti digital pada sosial media *facebook.*

Proses implementasi ini dapat dilihat pada gambar 4.2 sampai gambar 4.13. Proses pengumpulan barang bukti dengan menggunakan tools hancly ini dilakukan dengan menerapkan konsep Chain of Custudy, dimana dari proses proses pencatatan barang bukti dilakukan dari tahapan awal sampai akhir. Proses pencatatan ini meliputi capture dari informasi yang dikumpulkan sebagai pendukung barang bukti digital. Setiap data yang dikumpulkan memiliki ID, Date, Updated, Hash (SHA-256) yang berbeda-beda dari setiap item informasi sebagai pendukung barang bukti digital.

Tabel 4.15 Proses Implementasi Chain Of Custudy

A	**Identitas Kasus (*Case*)**			
	1	*Case Number*	:	Case 001
	2	*Offense*	:	Sosial Media Facebook
	3	*Suspect*	:	Nurul Khasana
	4	*Victim*	:	Bob Shinoda
B	***First Responder***			
	1	*First Responder Name*	:	Virjayanti Lazinu
	2	*Position*	:	Penyidik
	3	*Agency*	:	Pusat Digital Forensik UII
C	**Olah TKP Bukti Elektronik (Collection)**			
	1	*Tools*	:	Hunchly
	2	*Date/Time*	:	12 Juni 2022, 2022 / 3:02 PM
	3	*Address*	:	Laboratorium Pusat Digital Forensik UII

Tabel 4.16 Proses implementasi Chain of Custudy (Lanjutan)

D	**Bukti elektronik (*Electronic* Evidence)**			
	1	*Model*	:	Case001/XI/22/Pusfid/UII
	2	*Serial Number*	:	Case001120720220302
	3	*Type*	:	Sosial Media Facebook
	4	*Electronic Evidence No*	:	Reg Case001/DE/XI/22/Pusfid/UII
	5	*Owner*	:	Virjayanti Lazinu
E	**Proses Akuisisi**			
	1	*Acquisition Time*	:	12 Juni 2022, 2022
	2	*Acquisition Tools*	:	Hunchly
	3	*Acquisition Date*	:	3:02 PM
	4	*Acquisition Officer*	:	Virjayanti Lazinu
	5	*Device*	:	Laptop
F	**Hasil Imaging BE (ImageFile / Digital Evidence)**			
	1	*File name*	:	Case001.zip
	2	*Size*	:	70.4 MB (73,846,724 bytes)
	3	MD5	:	062B0F3987A7559BCD6E4B9CFB983BC3
	4	SHA-1	:	356818B527832BBBBC1E7A38DAA33F4244AA7184
	5	SHA-256	:	5FF7263A229A67064BCA25E80A8670AE4E7666F589E73019980CF4EDB36C7477
	6	*Status*	:	Open
G	**Lokasi Penyimpanan BD (Storage)**			
	1	*Storage Location*	:	D:\Project Tesis\Investigasi Hunchly
	2	*Time Stored*	:	Sunday, June 12, 2022, 04:04:22 PM
	3	*Validator*	:	Yudi Prayudi
H	***Role of Evidence***			
	1	*Reason For Foreclose*	:	Postingan pada halaman dinding beranda Akun Nurul Khasana
	2	*Potential Information*	:	Postingan Akun Nurul Khasanan
I	**Interaksi Para Pihak (Interactions)**			
	1	*Autorized by*	:	Yudi Prayudi
	2	*Received by*	:	Yudi Prayudi
	3	*Request time*	:	Sunday, June 12, 2022, 08:01:25 PM
	4	*Approve time*	:	Sunday, June 12, 2022, 09:04:22 PM
	5	*Received time*	:	Sunday, June 12, 2022, 09:30:02 PM
	6	*Action*	:	Melakukan pengembangan dan Validasi barang bukti

4.3 Pengujian Konsep *Chain Of Custody*

Proses pengujian Konsep *Chain Of Custody* ini dilakukan untuk mengetahui apakah proses pengumpulan bukti digital di media sosial facebook dengan menggunakan tools Hunchly telah memenuhi standar, sesuai dengan standar dokumen ISO/IEC 27037. Proses ini dilakukan agar semua proses yang dilakukan dalam mengumpulkan bukti digital sesuai dengan kaidah yang berlaku dan dapat di pertanggung jawabkan dalam proses pengadilan.

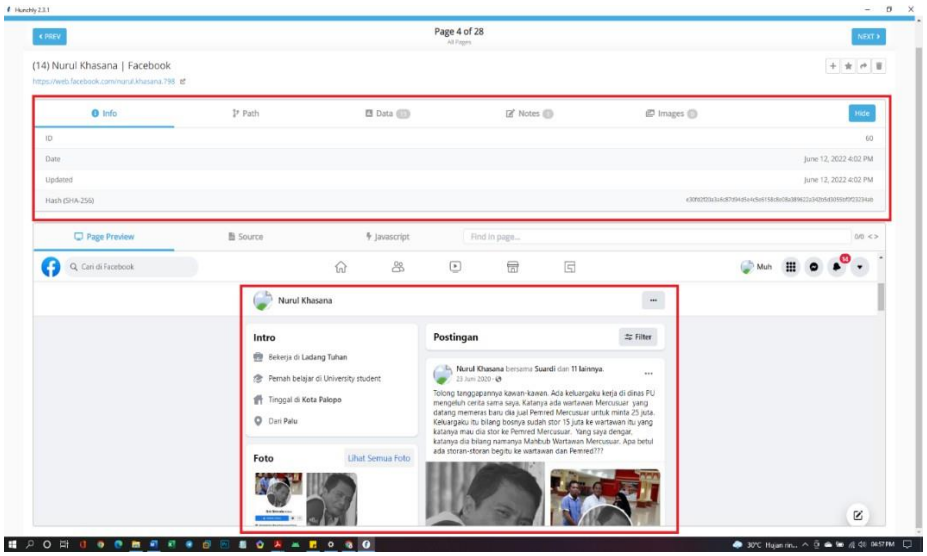
Standar dokumen ISO/IEC 27037 memiliki empat proses utama diantaranya sebagai berikut:

A) Identification

Proses identifikasi meliputi pencarian, pendeteksian dan pendokumentasian bukti digital yang direpresentasikan dalam bentuk bukti physical dan logical. Semua perangkat yang dapat berisi bukti digital harus diidentifikasi selama proses ini. Proses Digital Evidence First Responder harus melakukan penggeledahan sistematis di TKP untuk mencegah mengabaikan perangkat atau bahan kecil yang disamarkan yang tampaknya tidak relevan pada pandangan pertama. Selain itu, Digital Evidence First Responder harus mempertimbangkan kemungkinan adanya bukti tersembunyi dalam bentuk komponen virtual (Chung et al., 2012) . Dalam hal penanganan bukti digital yang bersumber dari media sosial memiliki karakteristik tersendiri, sehingga dalam proses identification harus dilakukan secara Live Investigation yang membutuhkan akses internet dan tools sehingga dapat mengumpulkan bukti digital di media sosial (Golbeck et al., 2015). Pada penelitian ini untuk proses Indentification dilakukan dengan melakukan identifikasi terhadap akun media sosial yang digunakan dan Jenis barang bukti. Jenis barang bukti yang berhasil di identifikasi adalah barang bukti digital dan media sosial yang digunakan adalah media sosial Facebook dengan Username“Nurul Khasana”.

B) Collection

Setelah identifikasi perangkat yang mungkin berisi bukti digital, perangkat ini dipindahkan dari lokasi aslinya dan dipindahkan ke laboratorium untuk dianalisis dan diproses sebagai langkah berikutnya. Proses pengumpulan selalu didokumentasikan, termasuk pengemasan dan pengangkutan ke laboratorium. Pada proses Collection, pengumpulan bukti digital dari akun Facebook Nurul Khasana ini dilakukan secara Live Investigation dengan menggunakan Tools Hunchly. Proses pengumpulan bukti digital ini telah mendapatkan data-data yang bisa di jadikan sebagai bukti digital diantaranya Salah Satu status Facebook Nurul Khasana yang diduga Telah melakukan fitnah terhadap terlapor.



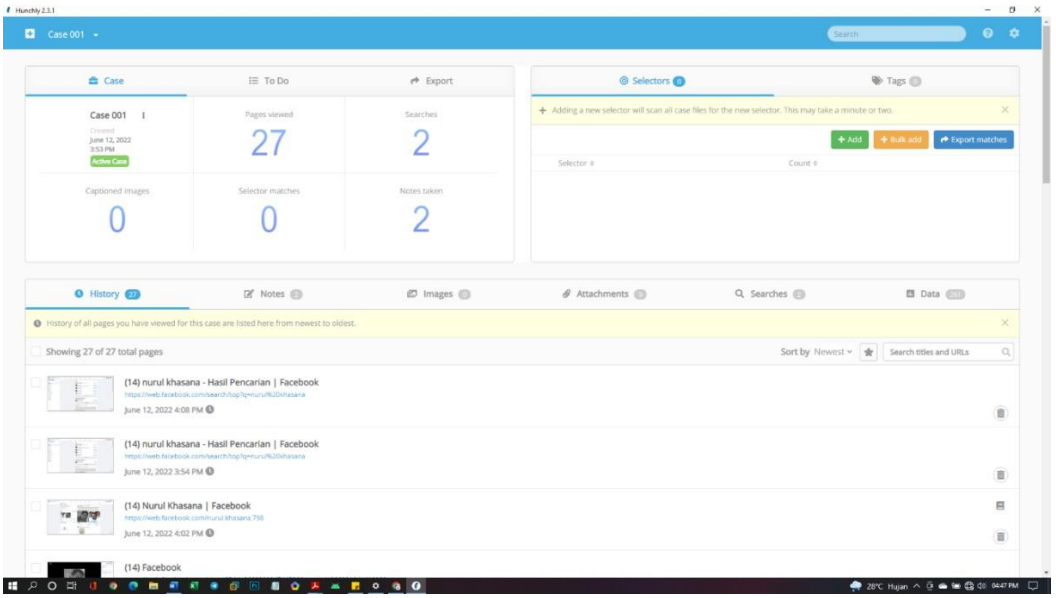
Gambar 4.21 Unggahan jendela facbook milik Nurul Khasana

C) Acquisition

Pemrosesan awal bukti digital terutama terdiri dari pembuatan salinan bukti (misalnya konten seluruh hard drive) dan mendokumentasikan metode yang digunakan. Jika perlu, ruang yang dialokasikan dan juga tidak terisi (termasuk file yang dihapus) harus diperoleh. Umumnya, yang asli dan salinannya harus menghasilkan keluaran (hash) yang sama dari fungsi verifikasi yang sama (terbukti akurat pada saat itu). Tergantung pada keadaan (situasi, waktu, harga), Digital Evidence First Responder harus memilih prosedur dan metode yang paling tepat untuk memperoleh data. Jika proses ini menghasilkan perubahan yang tak terhindarkan dalam salinan yang dibuat, dibandingkan dengan aslinya, perlu untuk mendokumentasikan data apa yang diubah. Dalam kasus-kasus di mana proses verifikasi tidak dapat dilakukan (misalnya saat memperoleh data dari sistem yang sedang berjalan, ketika yang asli mengandung bad sector, atau ketika waktu untuk memperoleh data terbatas), Digital Evidence First Responder harus menggunakan cara terbaik dan kemudian dapat untuk membenarkan dan membenarkan pilihannya metode. Jika salinan digital yang dibuat tidak dapat diverifikasi, maka ini harus didokumentasikan dan dibenarkan. Jika sumber bukti digital (data) terlalu besar untuk ditangani, DEFR hanya dapat memperoleh bagian yang relevan (file, folder, atau jalur yang dipilih). Semua langkah lain dari analisis forensik dilakukan pada salinan bukti digital (Sindhu & Meshram, 2012).

Pada penelitian ini tidak dilakukan proses akuisisi seperti halnya dilakukan pada bukti digital yang bersifat physical dan logical. Proses pengambilan data dalam penelitian ini dilakukan secara live investigation dengan menggunakan akses internet dan menggunakan tools Hunchly. Penggunaan tools Hunchly pada penelitian ini di lakukan

untuk mengumpulkan data-data pendukung bukti digital. Hasil yang di dapatkan dari penelitian ini, data-data sebagai pendukung bukti digital berhasil di capture dengan menggunakan tools Hunchly.

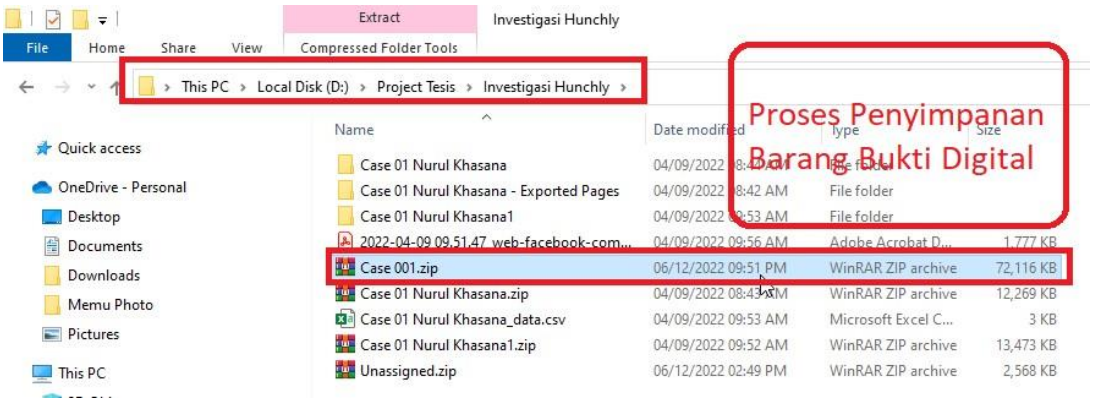


Gambar 4.22 Hasil Capture dari tools Hunchly

Hasil capture dari tools Hunchly, berhasil merekan beberapa postingan yang ada pada beranda facebook milik Nurul Khasana. Hasil setiap hasil capture ini berhasil memiliki ID dan Nilai hash yang berbeda beda pada setiap hasil capturenya.

D) Preservation

Dalam hal Preservation barang bukti digital, integritas dari barang bukti perlu dijaga agar dapat digunakan untuk keperluan investigasi. Digital Evidence First Responder harus dapat menunjukkan bahwa bukti tidak berubah sejak pengumpulannya dan untuk memberikan dokumentasi dan pembenaran atas semua tindakan yang menyebabkan perubahannya. Profesional yang melakukan kegiatan tersebut biasanya polisi atau ahli forensik. Proses preservation ini Barang bukti yang telah di kumpulkan akan di amankan. Proses pengamanan barang bukti ini dengan mencatumkan nilai MD5, SHA- 1 dan SHA-256 sehingga dapat mencegah perubahan yang terjadi pada barang bukti yang ada.



Gambar 4.23 Penyimpanan bukti digital

4.4 Analisis penerapan Tools pada Chain Of Costudy

Setelah proses implementasi konsep dan pengujian model *Chain Of Custody* di lakukan dapat terlihat bahwa pengumpulan barang bukti dari sosial media menggunakan tools Hunchly dengan menerapkan model *Chain Of Custody* telah berhasil dilakukan. Berdasarkan desain *Chain Of Custody* yang telah dirancang maka model pengumpulan bukti digital dengan tools Hunchly telah mengikuti desain *Chain Of Custody* yang telah di buat, seperti yang telihat pada table 4.15 dan table 4.16. Dari table tersebut implementasi *Chain Of Custody* telah dilakukan dari tahapan awal yaitu Identitas Kasus, First Responder, Olah TKP Bukti Elektronik, Bukti Elektronik, Proses Akuisis, Hasil Imaging Bukti Elektronik, Lokasi Penyimpanan Barang Bukti, Role Of Evidence, Serta Interaksi Para Pihak. Proses penggunaan tools Huncly pada model *Chain Of Custody* yang di buat lebih mendalam terlihat pada proses Hasil Imaging Bukti Elektronik, Lokasi Penyimpanan Barang Bukti, sampai Role Of Evidence. Hal ini karena pada proses ini tools Huncly sangat berperan penting dan proses pengumpulan barang bukti.

Pada proses Hasil Imaging Bukti Elektronik, dilakukan pencatatan terhadap File Name dari barang bukti, kemudian dilakukan pengecekan ukuran atau kapasitas dari barang bukti, serta dilakukan pengecekan nilai MD5, SHA-1, SHA-256 untuk memastikan keaslian dari Bukti Elektronik yang telah di akuisis menggunakan Tools huncly. Selanjutanya pada tahapan Lokasi Penyimpanan BD (Storage) dari Bukti Elektronik dalam model *Chain Of Custody*, dilakukan proses penyimpanan bukti elektronik yang ada dengan tiga proses tahapan yaitu Storage Location untuk penentuan lokasi dari barang bukti, time stored untuk pencatatan waktu dari penyimpanan barang bukti, serata proses validator untuk melakukan validasi terhadap Bukt Elektronik yang telah di simpan dari hasil akuisisi dari tools Hunchly.

Proses selanjutnya adalah Role Of Evidence, pada tahapan ini dilakukan dua proses penting yaitu Reason For Fereclose untuk mengetahui informasi yang merepresentasekan

alasan mengapa barang bukti elektronik ini di pilih serta proses kedua adalah Potential Information untuk mencari informasi yang merepresentasekan informasi apa yang diharapkan dapat ditemukan pada bukti elektronik yang ada. Dari proses analisis dengan menggunakan tools Hunchly diperoleh banyak informasi dari analisis barang bukti di media sosial pelaku, seperti informasi akun, Informasi Postingan, maupun Timestamp dari akun dan posting yang menjadi barang bukti. Dari uraian-uraian tersebut dapat menjelaskan bahwa data yang telah di kumpulkan dengan tools Hunchly dan model *Chain Of Custody* yang telah di rancang telah bersesuaian, sesuai dengan kebutuhan untuk mengumpulkan barang bukti yang ada di media sosial.

4.5 Analisis dan Pembahasan

Berdasarkan data dan fakta yang telah di peroleh dalam penelitian ini perancangan konsep dokumentasi *Chain Of Custody* untuk artefak sosial media *facebook* telah memenuhi kriteria untuk dapat digunakan. Berdasarkan hasil Ekstraksi Model Informasi Formulir *Chain Of Custody* pada table 4.4 sampai 4.7 dapat terlihat bahwa form usulan untuk Formulir *Chain Of Custody* ini merupakan hasil dari gabungan beberapa formulir diantaranya formulir University of Pennsylvenia, Audit West, Digital Forensics Lab, NIST (National Institute of Standards and Technology), dan PVL Forensics. Kelima macan formulir ini kemudian di ekstarksi berdasarkan deskripsi dan relasi dari setiap form sesuai dengan kebutuhan untuk penanganan bukti digital di sosial media facebook. Hasil ekstraksi tersebut yang dijadikan sebagai form usulan untuk *Chain Of Custody* dalam penanganan bukti artefak dari media sosial facebook.

Selain itu model usulan dari form *Chain Of Custody* dalam penanganan bukti artefak dari media sosial facebook ini telah memuat informasi perihal pertanyaan 5W+1H yaitu *What, Who, Where, When, Why* dan *Ho*w tentang barang bukti di persidangan. Proses ini dapat terlihat pada table 4.11 dan 4.12. Dalam proses penanganan barang bukti digital ini pertanyaan 5W+1H ini sangat penting untuk dipenuhi sehingga barang bukti yang diperoleh dapat dijelaskan sumbernya (Cosic et al., 2011).

Dari proses pengujian menggunakan studi kasus berupa akun media sosial facebook milik Nuruk Khasana dengan menggunakan tools Hunchly, telah ditemukan bukti digital berupa hasil capture dengan menggunakan tools Hunchly. Proses pengumpulan barang bukti dengan menggunakan tools Hunchly ini harus dilakukan secara Live Investigation karena membutuhkan akses internet dan tools ini berjalan di browser web dan secara otomatis mengumpulkan, mendokumentasikan, dan membuat anotasi setiap situs web yang kunjungi. Dengan memanfaatkan tools ini secara otomatis akan melakukan capture layar,

memotong dan menempelkan URL, atau menyimpan dokumen saat menjelajah. Dari hasil capture tersebut juga ditemukan beberapa informasi mengenai artefak media sosial milik Nurul Khasana.

Pada proses implementasi dari Form usulan *Chain Of Custody* untuk penanganan artefak media sosial facebook dapat dilihat pada table 4.15 dan 4.16. Proses ini telah berhasil dilakukan, di mana dari setiap proses pengisian form usulan ini merupakan hasil dari proses pengumpulan barang bukti menggunakan tools Hunchly. Proses *Chain Of Custody* ini mencatat setiap detail dari proses penanganan barang bukti digital dengan menggunakan tools Hunchly.

Pada proses penelitian ini masih memiliki keterbatasan dalam hal proses pengumpulan bukti digital. Dalam proses pengumpulan bukti digital menggunakan tools Hunchly ini memiliki keterbatasan ketika barang bukti digital dari postingan media sosial Facebook tersebut telah di hapus. Data dari postingan yang telah di hapus tersebut tidak bisa dilakukan capture dengan menggunakan tools Hunchly ini. Keterbatasan tools ini bisa dikolaborasikan menggunakan beberapa tools lain sehingga dapat mengantisipasi kelemahan dari tools Hunchly. Selain itu media sosial yang menjadi fokus penelitian ini adalah Facebook. Untuk proses pengujian di media sosial lainya bisa dikembangkan untuk penelitian selanjutnya.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Adapun kesimpulan yang dapat ditarik dari penelitian ini yaitu:

1. Proses perancangan *Chain Of Custody* untuk penanganan bukti artefak dari media sosial facebook telah berhasil di lakukan. Proses perancangan *Chain Of Custody* ini dilakukan dengan melakukan ekstraksi dari form *Chain Of Custody* yang telah ada sebelumnya. Proses ekstraksi ini menghasilkan Form Usulan baru untuk penanganan bukti artefak dari media sosial facebook yang dapat di gunakan untuk proses pengumpulan Bukti digital di media sosial.
2. Dalam proses perancangan *Chain Of Custody* yang di usulkan telah memuat informasi perihal pertanyaan 5W+1H yaitu *What, Who, Where, When, Why* dan *Ho*w. Informasi perihal pertanyaan 5W+1H ini kemudian dilakukan proses pemetaan berdasarkan kelompok informasi dan konten informasi.
3. Proses penerapan dari desain *Chain Of Custody* dengan penggunaan tools Hunchly dalam proses pengujian telah berhasil dilakukan. Penggunaan tools Hunchly telah berhasil mencapture bukti digital dari postingan akun milik Nurul Khasana. Selain berhasil melakukan capture dari postingan akun tersebut sebagai bukti digital. Selain itu data lain yang telah di dapatkan adalah platform digunakan, di mana postingan tersebut di buat, Mengapa dia membuat postingan tersebut, Kapan postingan di buat, Siapa yang membuat postingan, dan bagaimana isi postinganya.

5.2 Saran

Adapun saran untuk penelitian selanjutnya adalah sebagai berikut :

1. Dalam penelitian ini hanya menggunakan satu tools yaitu tools Hunchly dalam proses pengumpulan bukti digital. Untuk penelitian selanjutnya bisa menggunakan tools lain dalam pengumpulan bukti digital, sehingga bisa dilakukan perbandingan.
2. Dalam penelitian ini hanya berfokus pada satu media sosial yaitu facebook untuk proses pengujianya. Penelitian selanjutnya dapat melakukan pengujian terhadap media sosial lainya.

Daftar Pustaka

Anderson, Philip., & ENISA. (2014). *Electronic evidence, a basic guide for first responders : good practice material for CERT first responders.* ENISA.

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

Anwar, N., Riadi, I., Dahlan Jalan Soepomo, A., & Janturan Yogyakarta, S. (2017). Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web. In *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)* (Vol. 3, Issue 1).

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

Ashcroft, J., Daniels, D. J., & Hart, S. v. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. http://www.ojp.usdoj.gov/nij

Bahreisy, M. N., Rahmadi, R., & Prayudi, Y. (2021). Analisis Halaman Darkweb Untuk Mendukung Investigasi Kejahatan. *Jurnal Informatika Dan Komputer) Akreditasi KEMENRISTEKDIKTI*, *4*(1), 2614–8897. https://doi.org/10.33387/jiko

Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. *Digital Investigation*, *9*(2), 81–95. https://doi.org/10.1016/J.DIIN.2012.05.015

Coons. (2015). How to Document Your *Chain Of Custody* and Why It's Important. *Https://Www.Lhh.Com/Us/En/Insights/How-to-Document-Your-Chain-of-Custody-and-Why-Its-Important/*.

Cosic, J. (2017a). Formal Acceptability of Digital Evidence. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-44270-9

Cosic, J. (2017b). Formal acceptability of digital evidence. *Intelligent Systems Reference Library*, *115*, 327–348. https://doi.org/10.1007/978-3-319-44270-9_14

Cosic, J., & Baca, M. (2010). *Do We Have Full Control Over Integrity in Digital Evidence Life Cycle ?* 429–434.

Ćosić, J., & Bača, M. (2011). An Ontological Approach to Study and Manage Digital *Chain Of Custody* ofDigital Evidence. In *Article in Journal of Information and Organizational Sciences* (Vol. 35, Issue 1). https://www.researchgate.net/publication/279174939

Cosic, J., Cosic, Z., & Baca, M. (2011). An Ontological Approach to Study and Manage Digital *Chain Of Custody* of Digital Evidence. In *Preliminary Communication Article JIOS* (Vol. 35, Issue 1).

Dahiya, Y., & Sangwan, M. S. (2014). Developing and Enhancing the Security of Digital Evidence Bag. In *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)* (Vol. 1, Issue 2). www.arcjournals.org

Efendi, T. F. (2019a). Manajemen Barang Bukti Fisik Dan *Chain Of Custody* (CoC) Pada Penyimpananan Laboratorium Forensika Digital. *Prosiding Semantik*.

Efendi, T. F. (2019b). Manajemen Barang Bukti Fisik Dan *Chain Of Custody*(CoC) Pada Penyimpananan Laboratorium Forensika. *SEMANTIK 2019*.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*(SUPPL.). https://doi.org/10.1016/j.diin.2010.05.009

Gayed, T. F., Bari, M., & Nicolas, R. (2013). *Representing and Managing Tangible Chain Of Custody Using the Linked Data Principles*.

Giova, G. (2011). Improving *Chain Of Custody* in Forensic Investigation of Electronic Digital Systems *Chain Of Custody* View project Digital education View project Improving *Chain Of Custody* in Forensic Investigation of Electronic Digital Systems. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 11, Issue 1). https://www.researchgate.net/publication/267400650

Golbeck, J., Klavans, J. L., & Editor, T. (2015). *Introduction to* Sosial *Media Investigation Introduction to* Sosial *Media Investigation A Hands-on Approach*. https://doi.org/10.1016/B978-0-12-801656-5.09993-5

Graves, M. W. (2013). *The Anatomy of a Digital Investigation*.

Hadiah, U. S., Jurusan, F. E., & Syariah, P. (2016). *Pengaruh Media Sosial terhadap Perubahan Sosial Masyarakat di Indonesia*. https://www.coursehero.com/file/61625603/Pengaruh-Media-Sosial-terhadap-Perubahan-Sosial-Masyarakat-di-Indonesiadocx/

Kuntze, N., Rudolph, C., Richter, J., Kuntze, N., & Rudolph, C. (2017). *Securing Digital Evidence . Securing Digital Evidence*. *July*. https://doi.org/10.1109/SADFE.2010.31

Larasati, T. D., Bekti, D., & Hidayanto, C. (2017). Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10. In *Seminar Nasional Sistem Informasi Indonesia*.

Larasati, T. D., & Hidayanto, B. C. (2017). Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10. *Sesindo*, *6*(November), 456–256.

Leintz, R. (n.d.). *What is the Chain Of Custody - Definition, Procedures & Importance*.

Luthfi, A., & Prayudi, Y. (2016). Process Model of Digital Forensics Readiness Scheme (DFRS) as a Recommendation of Digital Evidence Preservation. *Proceedings - 4th International Conference on Cyber Security, Cyber Warfare, and Digital Forensics, CyberSec 2015*, 117–122. https://doi.org/10.1109/CyberSec.2015.31

Minin, M. (2020). *LIVE DATA FORENSIC ARTEFAK INTERNET BROWSER (STUDI KASUS GOOGLE CHROME , MOZILLA FIREFOX , OPERA MODE INCOGNITO)*. *1*(3), 1–9.

Minin, M. ’, & Anwar, N. (2020). *Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito)*. *1*(3), 1–9.

Naufal Bahreisy, M., Rahmadi, R., & Prayudi, Y. (2021). Analisis Halaman Darkweb Untuk Mendukung Investigasi Kejahatan. *JIKO (Jurnal Informatika Dan Komputer)*, *4*(1), 1–7. https://doi.org/10.33387/jiko.v4i1.1817

Nuh Al-Azhar, M. (2012). *digital forensics*. 302.

Prayudi, Y. (2014). *Problema Dan Solusi Digital Chain Of Custody Dalam Proses Investigasi Cybercrime*.

Prayudi, Y., Ashari, A., & K Priyambodo, T. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security*, *7*(11), 1–8. https://doi.org/10.5815/ijcnis.2015.11.01

Prayudi, Y., & SN, A. (2015a). Digital *Chain Of Custody*: State of The Art. *International Journal of Computer Applications*, *114*(5), 1–9. https://doi.org/10.5120/19971-1856

Prayudi, Y., & SN, A. (2015b). Digital *Chain Of Custody*: State of The Art. *International Journal of Computer Applications*, *114*(5), 1–9. https://doi.org/10.5120/19971-1856

Putra, A. S., & Prayudi, Y. (2021). *Implementasi Multi Smart Contract pada Bukti Digital dan Chain Of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital*. *6*(2). http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

Ryder, K. (2021). *Computer Forensics-We’ve Had an Incident, Who Do We Get to Investigate?*

Sadiku, M. N. O., Shadare, A. E., & Musa, S. M. (2017). Digital *Chain Of Custody*. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(7), 117. https://doi.org/10.23956/ijarcsse.v7i7.109

Sindhu, K. K., & Meshram, B. B. (2012). Digital Forensic Investigation Tools and Procedures. *International Journal of Computer Network and Information Security*, *4*(4), 39–48. https://doi.org/10.5815/ijcnis.2012.04.05

Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Sosial media analytics – Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*, *39*(October 2017), 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Thomson, L. L. (2011). *Admissibility Of Electronic Documentation As Evidence In U. S. Court. United State of America*. http://blog.witness.org/2011/01/cameraseverywhere.

Widatama, K., & Prayudi, Y. (2017). *Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML*.

Widatama, K., & Yudi Prayudi. (2017). Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML. *Seminar Nasional Informatika Dan Aplikasinya Ke-3*, *September*, 23.

Woods, K., Chassanoff, A., & Lee, C. A. (2013). *Managing and Transforming Digital Forensics Metadata for Digital Collections*. http://www.forensicswiki.org/wiki/Category:Digital_Fo