DIGITAL FORENSIK FACEBOOK MESSENGER SEBAGAI BARANG BUKTI MENGGUNAKAN METODE NIST SP 800-101

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

Disusun oleh:

Erlina Ekawati

18.83.0230

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

DIGITAL FORENSIK FACEBOOK MESSENGER SEBAGAI BARANG BUKTI MENGGUNAKAN METODE NIST SP 800-101

SKRIPSI

Untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

Disusun oleh:

Erlina Ekawati

18.83.0230

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

DIGITAL FORENSIK FACEBOOK MESSENGER SEBAGAI BARANG BUKTI MENGGUNAKAN METODE NIST SP 800-101

yang disusun dan diajukan oleh

Erlina Ekawati

18.83.0230

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 15 Agustus 2023

Dosen Pembimbing,

Subektiningsih, M.Kom
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

DIGITAL FORENSIK FACEBOOK MESSENGER SEBAGAI BARANG BUKTI MENGGUNAKAN METODE NIST SP 800-101

yang disusun dan diajukan oleh

Erlina Ekawati

18.83.0230

Telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Agustus 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	
Majid Rahardi, S.Kom., M.Eng. **NIK. 190302393**	
Subektiningsih, M.Kom **NIK. 190302413**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Erlina Ekawati
NIM : 18.83.0230

Menyatakan bahwa Skripsi dengan judul berikut:

Digital forensik Facebook Messenger Sebagai Barang Bukti Menggunakan Metode NIST SP 800-101

Dosen Pembimbing : Subektiningsih, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 15 Agustus 2023

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan karunia-Nya, yang telah memberikan saya kesehatan dan kelancaran sehingga saya dapat menyelesaikan skripsi saya dengan lancar dan sebaik-baiknya. Skripsi ini saya persembahkan umtuk:

1. Ibu saya tercinta Ibu Diana Ahmad dan Bapak saya selaku cinta pertama saya Asrul Alha serta yang selalu menyemangati, mendoakan dan memfasilitasi saya apapun yang saya butuhkan.
2. Kepada ketiga adik saya Yulvi Aisyh, Nurartalita dan Ahmad Alveratti terima kasih telah menjadi penyemangat saya selama pengerjaan skripsi.
3. Untuk diri saya sendiri Erlina Ekawati, karena telah berjuang untuk sampai pada titik sekarang.
4. Terima kasih kepada Ibu Subektiningsih, M.Kom selaku dosen pembimbing saya sangat baik dan selalu sabar dalam membimbing saya serta memberikan masukkan dalam menyusun skripsi ini.
5. Terima kasih seluruh dosen Teknik Komputer atas ilmu yang diberikan, motivasi, cerita serta kenangan selama masa perkuliahan.
6. Terima kasih kepada Fitra Rizky Bustami, yang menjadi support system saya yang telah memberikan dorongan untuk menyelesaikan skripsi ini dan juga selalu ada ketika saya butuhkan dan mendengarkan saya disaat berkeluh kesah tentang dunia perskripsian ini.
7. Kepada saudara-saudara saya, sahaba-sahabat dan teman-teman saya yang tidak bisa disebutkan satu per satu terima kasih karena sudah membantu dan memberi semangat dalam proses pengerjaan skripsi ini.
8. Kepada teman kelas saya 18-S1TK-02 yang telah membantu saya selama masa perkuliahan.

KATA PENGANTAR

Puji syukur penulis penjatkan kepada Allah SWT atas rahmat dan karunia-Nya serta nikmat kesehatan dan kesempatan sehingga penulis dapat menyelesaikan skripsi yang berjudul "Digital Forensik Facebook Messenger Sebagai Barang Bukti Menggunakan Metode National Institute of Standard Technology (NIST) 800-101.

Skripsi ini merupakan hasil dari upaya penelitian dan dedikasi yang dilakukan dalam rangka pemenuhan tugas akhir guna meraih gelar Sarjana Komputer dari Universitas Amikom Yogyakarta.

Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang mendalam kepada semua pihak yang telah memberikan dukungan, motivasi, serta ilmu selama perjalanan akademik sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan lancar, untuk itu penulis mengucapkan terima kasih kepada:

1. Allah SWT karena atas karunia-Nya penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat disuatu hari nanti.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta.
4. Ibu Subektiningsih, M. Kom. Selaku Dosen Pembimbing atas bimbingan, arahan, serta masukan berharga yang telah diberikan dalam penulisan skripsi ini.
5. Ibu Rina Pramitasari, S.Si., M.Cs Selaku Dosen Wali yang selalu memberikan pengarahan dan dukungan selama penulis menempuh masa perkuliahan.
6. Segenap Dosen, Staff, dan karyawan Universitas Amikom Yogyakarta yang telah memberikan ilmu dan juga membantu penulis dalam kelancaran segala administrasi sampai terselesaikannya skripsi ini.
7. Orang tua tercinta yang telah memenuhi segala kebutuhan penulis dari awal kuliah hingga sekarang penulis telah menyelesaikan skripsi.

8. Keluarga, saudara-saudara, pacar beserta teman-teman yang membantu dalam penyusunan skripsi ini dan memberikan dukungan kepada penulis yang tidak bisa penulis sebutkan satu per satu.

Ketika menyusun skripsi ini, penulis mengakui bahwa skripsinya masih jauh dari kesempurnaan, sebab terbatasnya pengalaman dan pengetahuan. Penulis berharap bahwa skripsi ini suatu hari nanti akan memberikan manfaat bagi semua yang memerlukannya serta dapat menjadi pedoman bagi penelitian di masa depan. Penulis juga mengundang saran, kritik, serta masukan yang berguna untuk menyempurnakan karya ini.

Yogyakarta, 9 Agustus 2023

Erlina Ekawati

DAFTAR ISI

HALAMAN JUDUL i
SKRIPSI i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI viii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR LAMBANG DAN SINGKATAN xiv
INTISARI xv
ABSTRACT xvi
BAB I PENDAHULUAN 17
1.1 Latar Belakang 17
1.2 Rumusan Masalah 20
1.3 Batasan Masalah 20
1.4 Tujuan Penelitian 21
1.5 Manfaat Penelitian 21
1.6 Sistematika penulisan 22
BAB II TINJAUAN PUSTAKA 23
2.1 Studi Literatur 23
2.2 Dasar Teori 29
2.2.1 Mobile Forensik 29
2.2.2 Smartphone 29
2.2.3 Facebook Messenger 30
2.2.4 Magnet Axiom 31

2.2.5 Mobiledit Forensik 31
2.2.6 National Institute of standards and Technology (NIST) SP 800-101. 32
1. Preservation 32
2. Acquisition 32
3. Examination & Analysis 33
4. Reporting 33
BAB III METODE PENELITIAN 34
3.1 Alat dan Bahan 34
3.2 Alur Penelitian 36
3.3 Skenario Kasus 37
3.4 Analisis Mobile Forensik Menggunakan NIST SP 800-101 38
3.4.1 Preservation 38
3.4.1.1 Mengamankan dan Mengevaluasi Perangkat Seluler 39
3.4.1.2 Mendokumentasikan Adegan 39
3.4.1.3 Isolasi 40
3.4.1.4 Pengemasan, Pengangkutan dan Penyimpanan barang bukti 40
3.4.2 Acquisition 41
3.4.2.1 Identifikasi perangkat seluler 41
3.4.2.2 Pemilihan Alat dan Ekspektasi 41
3.4.2.3 Akuisisi Memori Perangkat Seluler 42
3.4.3 Examination & Analysis 42
3.4.3.1 Bukti Potensial 42
3.4.3.2 Menerapkan Alat Forensik Perangkat Seluler 43
3.4.4 Reporting 43
BAB IV HASIL DAN PEMBAHASAN 44
4.1 Preservation 44

4.1.1 Mengamankan dan Mengevaluasi Perangkat Seluler 46
4.1.2 Mendokumentasikan Adegan 46
4.1.3 Isolasi 48
4.1.4 Pengemasan, Pengangkutan dan Penyimpanan barang bukti..... 48
4.2 Acquisition *49*
4.2.1 Identifikasi Perangkat Seluler 50
4.2.2 Pemilihan Alat dan Ekspektasi..... 51
4.2.3 Akuisisi Memori Perangkat Seluler 51
4.3 Examination & Analysis 59
4.4 Reporting..... 69
BAB V PENUTUP..... 71
5.1 Kesimpulan 71
5.2 Saran 71
REFERENSI 72

DAFTAR TABEL

Tabel 2. 1 Tinjauan Pustaka 25
Tabel 3. 1 Kebutuhan perangkat keras 34
Tabel 3. 2 Kebutuhan perangkat lunak 34
Tabel 4. 1 Form Chain Of Custody 45
Tabel 4. 2 Identifikasi Perangkat Seluler 50
Tabel 4. 3 Laporan barang bukti yang berhasil diangkat 69

DAFTAR GAMBAR

Gambar 2. 1 Tahapan NIST Special Publication 800-101 Revision 1 32
Gambar 3.1 Alur Penelitian 36
Gambar 3. 2 Skenario Kasus 37
Gambar 3.4.1 Form Chain of Custody 38
Gambar 4. 1 TKP 46
Gambar 4. 2 Smartphone & charger 47
Gambar 4. 3 Smartphone 47
Gambar 4. 4 Mode Pesawat 48
Gambar 4.5 Proses Penyimpanan Barang Bukti dalam Evidence Bag. 49
Gambar 4. 6 Proses Pelabelan 49
Gambar 4. 7 Identifikasi Perangkat Seluler Bagian Depan, Samping dan Belakang. 50
Gambar 4. 8 Tampilan Tool Mobiledit Forensik 52
Gambar 4. 9 Pemilihan akuisisi Application analysis pada Mobiledit Forensik .. 52
Gambar 4. 10 Pemilihan Application Facebook Messenger 53
Gambar 4. 11 Proses Akuisisi Berlangsung 53
Gambar 4. 12 Hasil Akuisisi 54
Gambar 4. 13 Input Case Information 54
Gambar 4. 14 Pemilihan Acquire Evidence 55
Gambar 4. 15 Pemilihan Device 55
Gambar 4. 16 Pemilihan *Logical Image* 56
Gambar 4. 17 Proses Akusisi Logical Berlangsung 57
Gambar 4. 18 Hasil Akuisisi Logical Magent Axiom 57
Gambar 4. 19 Pemilihan *Physical Image* 58
Gambar 4. 20 Proses Akusisi Physical Berlangsung 58
Gambar 4. 21 Hasil Akuisisi Physical Image 59
Gambar 4. 22 Hasil Pemeriksaan Facebook Messenger 60
Gambar 4. 23 Hasil Repot Mobiledit 60
Gambar 4. 24 Hasil Pemeriksaan Gambar di Facebook Messenger 61

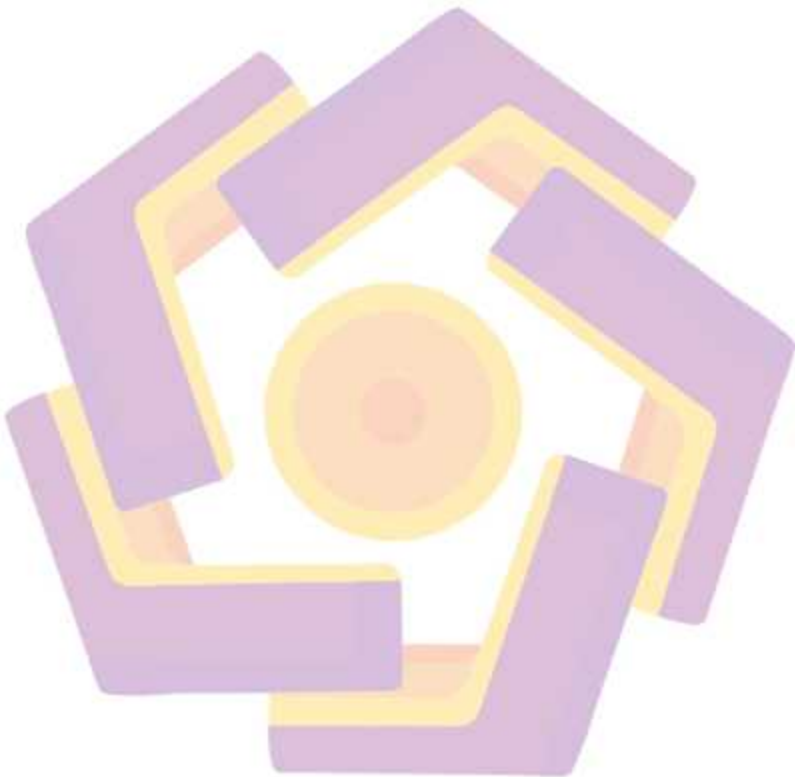
Gambar 4. 25 Hasil Report Mobiledit 62
Gambar 4. 26 Informasi Pemilik Akun Facebook Messenger 62
Gambar 4. 27 Gambar Yang Terdapat Pesan Pembelian Narkoba 63
Gambar 4. 28 Bukti Chat Pemesanan Narkoba Pembeli Ke Pengedar 63
Gambar 4. 29 Gambar Yang Terdapat Pesan Pembelian Narkoba 63
Gambar 4. 30 Bukti Chat Pemesanan Narkoba Pengedar Ke Pembeli 64
Gambar 4. 31 Analysis Data Akuisisi Physical 64
Gambar 4. 32 Hasil Analysis Akuisisi Physical 65
Gambar 4. 33 Database Akuisisi Logical pada Magnet Axiom 65
Gambar 4. 34 Hasil Gambar Pada Magnet Axiom 66
Gambar 4. 35 Analysis Data Akuisisi Logical 66
Gambar 4. 36 Hasil Analysis Akuisisi Logical 67
Gambar 4. 37 Database Akuisisi Logical Gambar pada Magnet Axiom 68
Gambar 4. 38 Hasil Gambar Pada Magnet Axiom 68

DAFTAR LAMBANG DAN SINGKATAN

Par : Nomor indeks tools forensik yang digunakan

Σar0 : Jumlah total data yang didapatkan

ΣarT : Jumlah total data yang diperlukan



INTISARI

Facebook Messenger menjadi media interkasi sosial dan hubungan antarindividu. Meningkatnya jumlah pengguna facebook tentu membawa dampak positif maupun dampak negatif. Salah satu efek negatifnya yaitu digunakan untuk tindakan kejahatan digital seperti perdagangan narkoba, cara menangkap para pelaku kejahatan perlu adanya barang bukti, maka dari itu dengan adanya teknik digital forensik dapat memudahkan untuk menangkap pelaku kejahatan perdagangan narkoba dan untuk menggali barang bukti pada data berupa gambar, log panggilan, dan akun facebook messenger. Forensik digital dapat dilakukan pada smartphone android atau pada jenis smartphone lainnya. Tujuan dari penelitian ini adalah untuk menerapkan praktik ekstraksi bukti dalam investigasi forensik digital yang terkait dengan situasi kasus perdagangan narkoba. Penelitian ini diharapkan memberikan kontribusi bagi lembaga penegak hukum dalam mengumpulkan bukti digital serta memberikan dampak positif dalam upaya memberantas kasus kejahatan di ranah siber. Dalam upaya ini, digunakan perangkat lunak Mobiledit Forensik dan Magnet Axiom dengan menerapkan metode National Institute of Standards and Technology (NIST) SP 800-101. Hasil dari penggunaan kedua alat tersebut menunjukkan Mobiledit memiliki tingkat akurasi sebesar 100%, sementara Magnet Axiom memiliki tingkat akurasi sebesar 33,33%. Hasil ini memberikan gambaran tentang kemampuan alat-alat tersebut dalam mendeteksi bukti digital pada perangkat smartphone Android.

Kata kunci: Facebook, Mobiledit, Android, Oxygen Forensik, NIST SP 800-101

ABSTRACT

Facebook Messenger is a medium of social interaction and relationships between individuals. The increasing number of Facebook users brings about both positive and negative impacts. One of the negative effects is its use in digital criminal activities such as drug trafficking. To apprehend perpetrators of such crimes, the presence of evidence is crucial. Therefore, the application of digital forensic techniques becomes essential in capturing individuals involved in drug trafficking and uncovering evidence from data like images, call logs, and Facebook Messenger accounts. Digital forensics can be conducted on Android smartphones or other types of smartphones.The objective of this research is to implement evidence extraction practices in digital forensic investigations related to drug trafficking cases. This study is expected to contribute to law enforcement agencies by aiding in the collection of digital evidence and positively impacting efforts to combat cybercrime. In this endeavor, Mobiledit Forensic and Magnet Axiom software tools are employed, utilizing the National Institute of Standards and Technology (NIST) SP 800-101 method. The results obtained from the use of these tools indicate that Mobiledit achieved an accuracy rate of 100%, while Magnet Axiom achieved an accuracy rate of 33.33%. These outcomes provide insights into the capabilities of these tools in detecting digital evidence on Android smartphones.

Keyword: *Facebook, Mobiledit, Android, Oxygen Forensik, NIST SP 800-1*