Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan Framework D4I (Studi Kasus: CekResi SiCepat Express .apk)

LAPORAN TUGAS AKHIR

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang

Alfin Zahrotun Nasuhah
202010370311037

Bidang Minat:
Sistem Keamanan Jaringan

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2024

LEMBAR PERSETUJUAN

Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan Framework D4I (Studi Kasus: CekResi SiCepat Express .apk)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *22 Januari 2025*

Dosen Pembimbing 1	Dosen Pembimbing 2
Ir Denar Regata Akbi S.Kom., M.Kom.	**Bashor Fauzan Muthohirin S.Kom., M.Kom**
NIP. 10816120591PNS.	**NIP. 20230126071994PNS.**

LEMBAR PENGESAHAN

Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan Framework D4I (Studi Kasus: CekResi SiCepat Express .apk)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

Alfin Zahrotun Nasuhah
202010370311037

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 22 Januari 2025

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Diah Risqiwati ST., MT.	**Briansyah Setio Wiyono S.Kom., M.Kom**
NIP. 10814100545PNS.	**NIP. 190913071987PNS.**

Mengetahui,
Ketua Jurusan Informatika

Ir. Galih Wasis Wicaksono S.kom. M.Cs.
NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : **Alfin Zahrotun Nasuhah**

NIM : **202010370311037**

FAK./JUR. : **Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan Framework D4I (Studi Kasus: CekResi SiCepat Express .apk)"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Ir Denar Regata Akbi S.Kom., M.Kom.

Malang, 22 Januari 2025
Yang Membuat Pernyataan

Alfin Zahrotun Nasuhah

ABSTRAK

Tingginya penggunaan media sosial di Indonesia, khususnya WhatsApp, meningkatkan risiko kejahatan siber seperti penipuan berbasis rekayasa sosial. Penelitian ini menganalisis kasus pelanggaran data menggunakan *framework* forensik digital D4I dengan studi kasus file APK CekResi SiCepat Express. *Framework* D4I mengoptimalkan proses investigasi melalui pemetaan artefak ke dalam model *Cyber-Kill-Chain* untuk menjawab pertanyaan 5W1H. Penelitian ini menggunakan alat seperti MOBILedit Forensic, MobSF, dan JADX-GUI untuk mengidentifikasi malware dan pola serangan. Hasil menunjukkan bahwa pelaku menggunakan file APK berbahaya untuk memperoleh data korban melalui bot Telegram. *Framework* D4I terbukti efektif dalam mengidentifikasi jalur serangan dan motif penyerangan dari pelaku.

Kata kunci: *digital forensic*, *framework* D4I, *Cyber-Kill-Chain*, *malware*

ABSTRACT

The widespread use of social media in Indonesia, particularly WhatsApp, has increased the risk of cybercrimes such as social engineering-based fraud. This study analyzes a data breach case using the D4I digital forensic framework with a case study of the CekResi SiCepat Express APK file. The D4I framework optimizes the investigation process by mapping artifacts into the Cyber-Kill-Chain model to answer the 5W1H questions. This study utilizes tools such as MOBILedit Forensic, MobSF, and JADX-GUI to identify malware and attack patterns. The findings reveal that the perpetrator used a malicious APK file to extract victim data through a Telegram bot. The D4I framework has proven effective in identify the path of the attack and the motives of the perpetrators.

Keywords: digital forensic, framework D4I, Cyber-Kill-Chain, malware

LEMBAR PERSEMBAHAN

Segala puji syukur dipanjatkan kepada Allah SWT atas seluruh rahmat, ridho, dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini yang berjudul "Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan *Framework* D4I (Studi Kasus: CekResi SiCepat Express .apk)".

Dalam penyusunan tugas akhir ini penulis mendapat dukungan dari berbagai pihak. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Allah SWT, Tuhan Yang Maha Esa, atas rahmat dan hidayah-Nya sehingga penulis bisa menjalani dan menempuh fase perkuliahan sampai pada penyelesaian tugas akhir ini.
2. Kedua Orang Tua, adik-adik dan seluruh keluarga penulis yang selalu memberi dukungan baik motivasi, materi, dan spiritual selama penulis menempuh pendidikan. Terima kasih telah membesarkan, membimbing, dan memberikan kasih sayang kepada penulis sehingga penulis sampai pada fase akhir perkuliahan menuju perwujudan mimpi dan cita-cita penulis.
3. Bapak Ir. Denar Regata Akbi, S.Kom, M.Kom dan Bapak Bashor Fauzan Muthohirin, S.Kom., M.Kom., sebagai dosen pembimbing beserta seluruh dosen pengajar yang telah memberikan arahan, ilmu, bimbingan dan motivasi selama proses perkuliahan sampai kepada penulisan tugas akhir ini.
4. Sahabat seperjuangan selama perkuliahan, Putri Intan Ashuri, Diah Maulida Akil dan Audina Bebasari, beserta seluruh teman-teman yang tidak dapat penulis sebutkan satu persatu yang selalu ada membantu, memberi motivasi, dan semangat kepada penulis selama menjalani studi di perguruan tinggi.
5. Bapak Jenderal TNI (Purn.) (HOR) H. Prabowo Subianto Djojohadikusumo, beserta keluarga Hambalang, yang selalu memberikan inspirasi dan motivasi kepada penulis untuk selalu bangkit dan berjuang dalam mewujudkan apa yang dicita-citakan

Malang, 15 November

Penulis

KATA PENGANTAR

Dengan memanjatkan segala puji syukur atas hadirat Tuhan Yang Maha Esa yang telah memberikan hidayat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul :

"Analisis Digital Forensik Kasus Pelanggaran Data Pada Media Sosial Whatsapp dengan Framework D4I (Studi Kasus: CekResi SiCepat Express .apk)"

Penelitian ini membahas tentang analisa digital forensik menggunakn framework D4I pada kasus pelanggaran data melalui media sosial Whatsapp dengan studi kasus CekResi SiCepat Express .apk., dengan tujuan yang diharapkan adalah hasil analisa digital forensic yang lebih komprehensif untuk menjawab pertanyaan 5W1H.

Penulis menyadari bahwa tugas akhir ini masih banyak kekurangan dan keterbatasan ilmu. Oleh karena itu atas kesalahan dan kekurangan dalam penulisan tugas akhir ini penulis memohon maaf dan mengaharapkan kritik dan saran yang bersifat membangun. Harapan penulis, semoga tugas akhir memberikan manfaat bagi siapa saja pembacanya

Malang, 15 November

Penulis

DAFTAR ISI

LEMBAR PERSETUJUAN ii
LEMBAR PENGESAHAN iii
LEMBAR PERNYATAAN iv
ABSTRAK v
ABSTRACT vi
LEMBAR PERSEMBAHAN vii
KATA PENGANTAR viii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR PUSTAKA 1
BAB I 3
PENDAHULUAN 3
1.1 Latar Belakang 3
1.2 Rumusan Masalah 5
1.3 Tujuan Masalah 5
1.4 Batasan Masalah 6
BAB II 7
TINJAUAN PUSTAKA 7
2.1 Penelitian Terdahulu 7
2.2 Kajian Pustaka 20
2.2.1 Digital Forensik 20
2.2.2 Artefak Digital 20
2.2.3 *Malware* 21
2.2.4 MOBILedit Express Forensic Tools 21
2.2.5 MobSF 21
2.2.6 Jadx GUI 21
BAB III 22
METODOLOGI PENELITIAN 22
3.1 Alur Penelitian 22
3.1.1 Pengumpulan barang bukti 22
3.1.2 Identifikasi Artefak dan Korelasi 23

3.1.3 Analisa 23
3.1.4 Pembuatan kesimpulan dengan pelaporan 5W1H yang lengkap 24
3.2 Metode Penelitian 24
3.2.1 Framework D4I 24
3.2.2 CKC (Cyber-Kill-Chain) 26
3.2.3 Rancangan Kebututuhan Alat Penelitian 27
3.2.4 Rancangan Lembar Kerja Penelitian 27
3.2.5 Rancangan Skenario Kasus 31
3.2.6 Rancangan Metode Pengukuran Data Analisa Digital Forensik 31
BAB IV 35
HASIL DAN PEMBAHASAN 35
4.1 Implementasi analisis digital forensik 35
4.2 Pengukuran Data Analisa Digital Forensik 51
BAB V 55
PENUTUP 55
5.1 Kesimpulan 55
5.2 Saran 57

DAFTAR TABEL

Tabel 2. 1 *Journal Mapping* 7
Tabel 3. 1 Alat Penelitian 27
Tabel 3. 2 Tools Forensik 27
Tabel 3. 3 Lembar Kerja Informasi Kasus 28
Tabel 3. 4 Lembar Kerja Perangkat Seluler 28
Tabel 3. 5 Lembar Kerja Chain of Artifacts 29
Tabel 3. 6 Lembar Kerja Laporan Hasil 30
Tabel 3. 7 Metode Pengukuran Data Analisa Digital Forensik 32
Tabel 4. 1 Lembar Informasi Kasus Saat Laporan Diterima 35
Tabel 4. 2 Lembar Informasi Barang Bukti Perangkat Seluler 37
Tabel 4. 3 Lembar Chain of Artefact (CoA) 48
Tabel 4. 4 Lembar Laporan Hasil Analisa 49
Tabel 4. 5 Implementasi pengukuran data analisa digital forensik 51
Tabel 5. 1 Artefak digital yang berkorelasi 55

DAFTAR GAMBAR

Gambar 3. 1 Flowchart Alur Penelitian 22
Gambar 3. 2 Framework D4I 25
Gambar 3. 3 Skenario Kasus 31
Gambar 4. 1 Barang Bukti Ponsel Korban 36
Gambar 4. 2 Nomor IMEI pada MOBILedit Forensic 37
Gambar 4. 3 Folder hasil proses backup MOBILedit Forensic 38
Gambar 4. 4 Proses deteksi awal *malware* 38
Gambar 4. 5 Pesan untuk membuka resi pada Whatsapp 39
Gambar 4. 6 Fase *Cyber-Kill-Chain* yang dipilih 40
Gambar 4. 7 File Android XML dari hasil *decompile* APK SiCepat Express 41
Gambar 4. 8 File class *SmsEyeSmsListener* 42
Gambar 4. 9 File class *SmsEyeNetwork* 42
Gambar 4. 10 File Builder dari instance TelegramBot 43
Gambar 4. 11 File-file dalam *folder assets* 43
Gambar 4. 12 ID dari BOT telegram 44
Gambar 4. 13 Artefak digital pesan yang ditemukan pada Whatsapp 44

DAFTAR PUSTAKA

[1] C. M. Annur, "Ini Media Sosial Paling Banyak Digunakan di Indonesia Awal 2024," databoks.katadata.co.id. Accessed: Mar. 01, 2024. [Online]. Available: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/66ea436ab12f2/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024

[2] E. Suryowati, "BSSN: Sektor keuangan Peringkat Ketiga Paling Rentan Kejahatan Siber Setelah Administrasi Pemerintahan dan Energi," jawapos.com. Accessed: Dec. 29, 2023. [Online]. Available: https://www.jawapos.com/ekonomi-digital/013669836/bssn-sektor-keuangan-peringkat-ketiga-paling-rentan-kejahatan-siber-setelah-administrasi-pemerintahan-dan-energi

[3] D. Ryan Triwahono *et al.*, "Pencegahan Penipuan Social Engineering pada Massa 4.0," *J. Ilmu Multidisplin*, vol. 2, no. 1 SE-Articles, pp. 68–74, Jun. 2023, doi: 10.38035/jim.v2i1.232.

[4] A. Tanujaya, "Statistik Kejahatan Siber di Indonesia Selama 2023," inet.detik.com. Accessed: Nov. 24, 2023. [Online]. Available: https://inet.detik.com/security/d-7054249/statistik-kejahatan-siber-di-indonesia-selama-2023

[5] A. R. Hakim, K. Ramli, T. S. Gunawan, and S. Windarta, "A Novel Digital Forensic Framework for Data Breach Investigation," *IEEE Access*, vol. 11, no. May, pp. 42644–42659, 2023, doi: 10.1109/ACCESS.2023.3270619.

[6] I. Riadi, R. Umar, and M. I. Syahib, "Akusisi Bukti Digital Viber Messenger Android Menggunakan Metode NIST," vol. 1, no. 10, pp. 45–54, 2021.

[7] M. Marzuki and T. Sutabri, "Analisis Forensik Media Sosial Michat Metode Digital Forensik Integrated Investigation Framework (IDFIF)," *Blantika Multidiscip. J.*, vol. 2, no. 1, pp. 56–70, 2023, doi: 10.57096/blantika.v2i1.11.

[8] A. El Hafidy, D. Relikson, and M. L. P. Sopian, "Analisis Bukti Digital pada Fitur Edit WhatsApp Desktop menggunakan Metode Digital Forensic

Research Workshop (DFRWS)," *JRIIN J. Ris. Inform. dan Inov.*, vol. 1, no. 8 SE-, Apr. 2024, [Online]. Available: https://jurnalmahasiswa.com/index.php/jriin/article/view/831

[9] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4I - Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, no. October 2019, p. 100015, 2020, doi: 10.1016/j.array.2019.100015.

[10] N. Lefkovitz and K. Boeckl, "Indonesian Translation of the NIST Privacy Framework Version 1.0," Gaithersburg, MD, Sep. 2021. doi: 10.6028/NIST.CSWP.01162020id.

[11] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th Editio. 2018.

[12] Y. D. Puji Rahayu and Nanang Trianto, "Analisis *Malware* Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1," *Info Kripto*, vol. 15, no. 3, pp. 105–111, 2021, doi: 10.56706/ik.v15i3.30.

[13] B. A. Saputro, L. I. Alfitra, and R. B. Oktaviaji, "Analisis *Malware* Android Menggunakan Metode Reverse Engineering," *J. Repos.*, vol. 2, no. 10, Jan. 2024, doi: 10.22219/repositor.v2i10.31842.

[14] A. Kartono, A. Sularsa, and S. Ismail, "Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf," in *e-Proceeding of Applied Science*, 2019, pp. 146–151.

[15] A. R. Q. Syahwidi, S. Cahyono, and R. N. Yasa, "Analisis Aplikasi Cryptowallet Tiruan Terhadap Indikasi Android *Malware*," *Info Kripto*, vol. 17, no. 1, pp. 23–31, 2023.

[16] H. Try Sulistyono, "Prosedur Autentifikasi Alat Bukti Elektronik Pada Pemeriksaan Persidangan," 2020.