

**ANALISIS FORENSIK APLIKASI TELEGRAM BERBASIS WEB
MENGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE***

Skripsi

**Disusun untuk memenuhi Sebagian persyaratan
mencapai derajat Sarjana**



Disusun Oleh :

Larassaty Chandra Pakaya

1900018216

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS AHMAD DAHLAN

YOGYAKARTA

2023

LEMBAR PERSETUJUAN PEMBIMBING

SKRIPSI

**ANALISIS FORENSIK APLIKASI TELEGRAM BERBASIS WEB MENGGUNAKAN METODE
NATIONAL INSTITUTE OF JUSTICE**

Dipersiapkan dan disusun oleh :
Larassaty Chandra Pakaya
1900018216



Disetujui oleh :

Pembimbing

Dr. Ir. Imam Riadi, M.Kom.
NIPM. 198008102002201110915675

LEMBAR PENGESAHAN SKRIPSI

SKRIPSI

ANALISIS FORENSIK APLIKASI TELEGRAM BERBASIS WEB MENGGUNAKAN METODE
NATIONAL INSTITUTE OF JUSTICE

Dipersiapkan dan disusun oleh :
Larassaty Chandra Pakaya
1900018216

Telah dipertahankan didepan Dewan Penguji
Pada hari Senin, 11 September 2023
Dan dinyatakan telah memenuhi syarat

Susunan Dewan Penguji

Ketua : Dr. Ir. Imam Riadi, M.Kom.
Penguji 1 : Guntur Maulana Zamroni, B.Sc, M.Kom.
Penguji 2 : Ir. Nuril Anwar, S.T., M.Kom.



[Handwritten signatures and dates]
5/10/23
27/9/23
21/9-2023

Yogyakarta, 11 September 2023
Dekan Fakultas Teknologi Industri
Universitas Ahmad Dahlan



[Handwritten signature]
Sunardi, S.T., M.T., Ph.D.
NIPM.197405212000021110862028

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini :

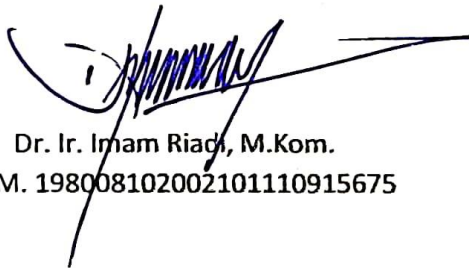
Nama : Larassaty Chandra Pakaya
NIM : 1900018216
Prodi : S1 Informatika
Judul TA/Skripsi : Analisis Forensik Aplikasi Telegram Berbasis Web Menggunakan Metode National Institute Of Justice

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat yang karya pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar Pustaka.

Yogyakarta, 11 September 2023

Mengetahui,
Dosen Pembimbing

Yang menyatakan



Dr. Ir. Imam Riadi, M.Kom.
NIPM. 198008102002101110915675



Larassaty Chandra Pakaya
1900018216

SURAT TIDAK PLAGIAT

Saya yang bertanda tangan dibawah ini :

Nama : Larassaty Chandra Pakaya
NIM : 1900018216
Email : larassaty1900018216@webmail.uad.ac.id
Program Studi : Informatika
Fakultas : Teknologi Industri

Dengan ini menyatakan bahwa :

- 1 Hasil karya yang saya serahkan ini adalah asli dan belum pernah mendapatkan gelar keserjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
- 2 Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian dan implementasi saya sendiri, tanpa bantuan pihak lain kecuali arahan pembimbing akademik dan narasumber penelitian.
- 3 Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan di setujui oleh pembimbing.
- 4 Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 11 September 2023
Yang Menyatakan



Larassaty Chandra Pakaya

PERYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini :

Nama : Larassaty Chandra Pakaya
NIM : 1900018216
Email : larassaty1900018216@webmail.uad.ac.id
Program Studi : S1 Informatika
Fakultas : Teknologi Industri
Judul Penelitian : Analisis Forensik Aplikasi Telegram Berbasis Web Menggunakan Metode National Institute Of Justice

Dengan ini saya menyerahkan hak sepenuhnya kepada Pusat Sumber Belajar Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengolahan terhadap karya saya ini dengan mengacu pada ketentuan akses skripsi elektronik sebagai berikut (beri tanda pada kotak) :



Saya mengizinkan karya tersebut diunggah ke dalam aplikasi Repository Pusat Sumber Belajar Universitas Ahmad Dahlan

Demikian pernyataan ini saya buat dengan sebenarnya.

Mengetahui,
Yang Menyatakan,
Dosen Pembimbing


Dr. Ir. Imam Riadi, M.Kom.
NIPM. 198008102002101110915675

Yogyakarta, 11 September 2023
Yang Menyatakan,


Larassaty Chandra Pakaya
1900018216

MOTTO

“Sesungguhnya sesudah kesulitan itu ada kemudahan. Maka apabila kamu telah selesai (dari sesuatu urusan), kerjakanlah dengan sungguh-sungguh (urusan) yang lain.”

– QS Al-Insyirah [94:6-7] –

"Kebahagiaan bukanlah sesuatu yang harus kamu capai. Kamu masih bisa bahagia selama proses mencapai sesuatu."

– RM –

“Apabila sesuatu yang kau senangi tidak terjadi maka senangilah apa yang terjadi.”

– Ali bin Abi Thalib –

“Tidak ada sesuatu yang mustahil untuk dikerjakan, Hanya tidak ada sesuatu yang mudah”

– Napoleon Bonaparte –

HALAMAN PERSEMBAHAN

Alhamdulillah hirrobbil Alamin. Segala puji kepada Allah SWT yang telah memberikan kemampuan kepada penulis untuk menyelesaikan skripsi ini. Sebagai tanda bakti, hormat, dan rasa terima kasih yang tiada terhingga, dengan penuh ketulusan, saya persembahkan skripsi ini untuk :

1. Mama, Papa, Kakak, Koko, Elma, dan Dea yang selalu mendoakan, membantu dan mendukung selama penyelesaian masa studi.
2. Keluarga besar Pakaya dan keluarga besar Hemuto yang selalu mendukung, memberikan semangat dan motivasi yang tiada henti.
3. Suweg girls: Alviahtu Zakiah, Qoyum Milati Tri Rejeki, Rizky Khairiah, Fakhira Annisatul Zahrah, Bella Saphira, dan Lina Julianti yang sudah kebersamai dari semester 1 sampai akhirnya bisa mendapatkan gelar Sarjana Komputer. Terima kasih telah menjadi rumah kedua dan melewati kehidupan di perantauan.
4. Y girls : Aimmatul Firdausy dan Karimatun Nisa El Husna yang telah menemani dengan canda tawa, dukungan, dan dorongan. Terima kasih selalu ada dan membantu dalam menjalani kehidupan yang tidak mudah ini.
5. Teman-teman seperbimbingan yang berjuang bersama dan saling menyemangati satu sama lain. Terima kasih selalu ada dalam suka dan duka setiap bimbingan bersama.
6. Orang terdekat yang selalu memberikan semangat dalam setiap langkah perjalanan ini. Terima kasih sudah menjadi kekuatan dalam mengerjakan skripsi ini.
7. Seluruh member BTS, yang sudah memberikan banyak motivasi dan semangat melalui karya kalian.
8. Terakhir, terima kasih untuk diri sendiri yang tak pernah berhenti berjuang, terima kasih karena telah melewati rintangan dan tantangan dengan ketabahan dan kegigihan, terima kasih telah melewati malam-malam tanpa tidur, menjaga semangat di tengah kelelahan, dan terus berusaha meski terkadang ingin menyerah, dan juga terima kasih karena tak pernah berhenti bermimpi dan bekerja keras untuk mewujudkannya.

Terima kasih telah menemani dan mendukung penulis di saat pusingnya mencari jalan buntu selama proses penyelesaian skripsi

KATA PENGANTAR

*Bismillahirrahmaanirrahiim,
Assalamua'alaikum Warahmatullahi Wabarakatuh*

Segala puji dan syukur atas kehadiran Allah SWT, karena atas Rahmat dan hidayah-Nya peneliti dapat menyelesaikan skripsi yang berjudul “Analisis Forensik Aplikasi Telegram Berbasis Web Menggunakan Metode National Institute Of Justice”. Skripsi ini disusun sebagai salah satu syarat untuk mencapai derajat sarjana komputer Universitas Ahmad Dahlan. Selama menulis skripsi ini, peneliti menyadari banyak pihak yang memberikan support dan bimbingannya, pada kesempatan ini peneliti ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Prof. Dr. Muchlas Arkanuddin, M.T. Selaku Rektor Universitas Ahmad Dahlan.
2. Dr. Murinto, S.Si., M.Kom. Selaku Ketua Program Studi Informatika
3. Ali Tarmuji, S.T., M.Cs. Selaku Dosen Pendamping Akademik yang telah banyak memberikan bimbingan dan semangat dalam bidang Akademik.
4. Dr. Ir. Imam Riadi, M.Kom. Selaku Dosen Pembimbing Skripsi. Peneliti mengucapkan terimakasih sebesar-besarnya atas segala bimbingan, ilmu, dukungan, serta bantuannya.
5. Guntur Maulana Zamroni, B.Sc, M.Kom. selaku dosen penguji 1
6. Ir. Nuril Anwar, S.T., M.Kom. selaku dosen penguji 2
7. Seluruh Dosen dan Staf Informatika Universitas Ahmad Dahlan yang telah membantu.

Semoga Allah SWT senantiasa melindungi dan membalas segala kebaikan yang telah diberikan. Mohon maaf atas segala kekurangan serta kekhilafan dalam penulisan skripsi ini. Kekurangan dalam skripsi ini semoga dapat disempurnakan dalam penelitian selanjutnya Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Yogyakarta, 11 September 2023

Peneliti



Larassaty Chandra Pakaya

ANALISIS FORENSIK APLIKASI TELEGRAM BERBASIS WEB MENGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE*

Larassaty Chandra Pakaya
1900018216

ABSTRAK

Saat ini, aplikasi pesan instan tidak hanya tersedia dalam bentuk aplikasi pada *smartphone*, melainkan juga dapat diakses melalui web *browser*, salah satunya yaitu *Telegram Web*. Penggunaan Telegram melalui platform web memberikan kemudahan kepada penggunanya. Namun, seiring dengan kemudahan ini, muncul potensi kerentanan yang menarik perhatian pelaku kejahatan digital atau *cybercrime*. Penelitian ini bertujuan untuk memperoleh bukti digital kasus penipuan *freelance* pada Telegram yang berjalan pada web browser *Google Chrome* dengan menggunakan metode *National Institute of Justice* (NIJ).

Tahapan dalam metode NIJ antara lain *Identification, Collection, Examination, Analysis, dan Reporting*. Tahap awal adalah *Identification* di mana persiapan peralatan penyelidikan dilakukan, seperti *FTK Imager, Browser History Capture, Browser History Examiner, dan OSForensics*. Tahap berikutnya, *Collection*, melibatkan pengambilan barang bukti seperti data dan bukti fisik. *Examination* kemudian menganalisis data yang telah dikumpulkan. Tahap *Analysis* menganalisis hasil pemeriksaan secara mendalam. Terakhir, tahap *Reporting* menyusun laporan yang memaparkan hasil analisis yang telah dilakukan.

Hasil dari penelitian ini mencakup berbagai informasi yang ditemukan melalui berbagai *tools* forensik digital. Diantaranya, nomor telepon pelaku berhasil diidentifikasi dengan bantuan *Browser History Examiner*. Selain itu, sebanyak 45 percakapan antara korban dan pelaku yang sebelumnya dihapus berhasil dipulihkan. Akun pelaku juga berhasil ditemukan melalui analisis menggunakan *FTK Imager*. Selanjutnya, berbagai gambar yang termasuk dalam percakapan antara korban dan pelaku, seperti 2 bukti transfer dan 3 tangkapan layar tugas yang diberikan pelaku, berhasil diakses dan diidentifikasi menggunakan *OSForensics*.

Kata Kunci : Bukti Digital, *Cybercrime, Google Chrome, National Institute Of Justice* (NIJ), *Telegram*

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	ii
LEMBAR PENGESAHAN SKRIPSI	iii
LEMBAR PERNYATAAN KEASLIAN	iv
SURAT TIDAK PLAGIAT	v
PERYATAAN PERSETUJUAN AKSES	vi
MOTTO	vii
HALAMAN PERSEMBAHAN	viii
KATA PENGANTAR	ix
ABSTRAK	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xv
BAB I Pendahuluan	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Batasan Masalah	3
1.4 Rumusan Masalah	4
1.5 Tujuan Penelitian	4
1.6 Manfaat Penelitian	4
BAB II Kajian Pustaka	5
2.1 Kajian Terdahulu	5
2.2 Landasan Teori	9
A. Forensik Digital	9
B. Bukti Digital	10
C. NIJ (National Institute Justice)	11
D. Telegram	13
E. Web browser	15
F. Cybercrime	16
G. Tools Forensik	17
BAB III Metode Penelitian	20
3.1 Objek Penelitian	20
3.2 Metode Pengumpulan Data	20
3.3 Spesifikasi Kebutuhan	21

3.4	Tahapan Penelitian.....	21
3.5	Skenario Kasus.....	23
BAB IV Hasil dan Pembahasan.....		25
4.1	Analisis Kebutuhan.....	25
4.2	Skenario Penelitian.....	25
4.3	Hasil dan Pembahasan	29
A.	<i>Identification</i> (Identifikasi)	29
B.	<i>Collection</i> (Koleksi)	30
C.	<i>Examination</i> (Pemeriksaan)	35
D.	<i>Analysis</i> (analisis).....	60
E.	Reporting (Pelaporan)	62
BAB V Penutup		64
5.1	Kesimpulan.....	64
5.2	Saran.....	65
DAFTAR PUSTAKA.....		66

DAFTAR GAMBAR

Gambar 1.1 Daftar Aplikasi Pesan Instan yang Paling Banyak Dipakai 2022	1
Gambar 2.1 Tahapan Metode NIJ	11
Gambar 2.2 Logo Telegram	13
Gambar 2.3 Cara Kerja Web Browser	15
Gambar 2.4 Jenis- Jenis Web Browser	16
Gambar 3.1 Tahapan Metode NIJ	22
Gambar 3.2 Skenario Kasus yang Terjadi	23
Gambar 4.1 Pre Insiden Kasus Penipuan Freelance	26
Gambar 4.2 Insiden Kasus Penipuan Freelance	26
Gambar 4.3 Pasca Insiden Kasus Penipuan Freelance	27
Gambar 4.4 Kontak Pelaku	28
Gambar 4.5 Fitur Capture Memory pada FTK Imager	32
Gambar 4.6 Proses Saat Capture Memory Di FTK Imager	32
Gambar 4.7 Hasil Capture RAM FTK Imager	33
Gambar 4.8 Tampilan Browser History Capturer	33
Gambar 4.9 Browser History Capturer Sedang Proses Capture	34
Gambar 4.10 Hasil Capture	34
Gambar 4.11 Isi Folder Capture	35
Gambar 4.12 Fitur Load History	36
Gambar 4.13 Tampilan Untuk Load History File	36
Gambar 4.14 Proses Ekstraksi Data	37
Gambar 4.15 Hasil Ekstraksi Data Dari Folder Capture	37
Gambar 4.16 Tampilan Website Visit	38
Gambar 4.17 Tampilan Form History	38
Gambar 4.18 Fitur Add Evidence Item	39
Gambar 4.19 Source Evidence Type	40
Gambar 4.20 Evidence Source Selection	40
Gambar 4.21 Hasil Ekspolarasi Data	41
Gambar 4.22 Fitur Find	41
Gambar 4.23 Akun Pelaku	42
Gambar 4.24 Tampilan Awal Aplikasi OSForensics	47
Gambar 4.25 Fitur Thumbcache Viewer	48
Gambar 4.26 Hasil Scan Drive C	48
Gambar 4.27 Hasil Pencarian Gambar	49
Gambar 4.28 Metadata Gambar	49
Gambar 4.29 Pemeriksaan kedua dengan Browser History Examiner	50
Gambar 4.30 Hasil Akuisisi 2 Riwayat kunjungan Web	51
Gambar 4.31 Hasil Pemeriksaan 2 Form History	51
Gambar 4.32 Proses Dump Memori kedua pada FTK Imager	52
Gambar 4.33 Hasil Pemeriksaan 2 pada FTK Imager	52
Gambar 4.34 Proses Pemeriksaan 2 OSForensics	53
Gambar 4.35 Hasil Pemeriksaan 2 pada OSForensics	53
Gambar 4.36 Cek MD5 File Bukti Tools Browser History Examiner	54

Gambar 4.37 Verifikasi MD5 File Bukti Browser History Examiner	54
Gambar 4.38 Cek MD5 File Bukti Tools FTK Imager	55
Gambar 4.39 Verifikasi MD5 File Bukti FTK Imager	55
Gambar 4.40 Cek MD5 File Bukti Tools OSForensics	56
Gambar 4.41 Verifikasi MD5 File Bukti OSForensics	56
Gambar 4.42 Hasil Scan Fitur User Activity OSForensics	57
Gambar 4.43 Proses Dump Memory OSForensics	58
Gambar 4.44 Hasil Dump Memory Chat Pelaku dengan OSForensics	58
Gambar 4.45 Hasil Dump Memory Akun Pelaku dengan OSForensics	59
Gambar 4.46 File Info Dump Memory OSForensics	59

DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian Terdahulu	8
Tabel 3.1 Kebutuhan Perangkat Keras	21
Tabel 3.2 Kebutuhan Perangkat Lunak	21
Tabel 4.1 Bukti Chat dan Transfer yang Dilakukan antara Korban dan Pelaku	28
Tabel 4.2 Persiapan Tools.....	30
Tabel 4.3 Barang Bukti yang Didapat	31
Tabel 4.4 Spesifikasi Laptop	31
Tabel 4.5 Chat Pelaku ke-1	42
Tabel 4.6 Chat Pelaku ke-2	43
Tabel 4.7 Chat Pelaku ke-3	43
Tabel 4.8 Chat Pelaku ke-4	44
Tabel 4.9 Chat Pelaku ke-5	44
Tabel 4.10 Chat Pelaku ke-6	45
Tabel 4.11 Chat Korban ke-1	45
Tabel 4.12 Chat Korban ke-2	45
Tabel 4.13 Chat Korban ke-3	46
Tabel 4.14 Chat Korban ke-4	46
Tabel 4.15 Chat Korban ke-5	46
Tabel 4.16 Chat Korban ke-6	46
Tabel 4.17 Chat Korban ke-7	47
Tabel 4.18 Detail Bukti yang Ditemukan pada FTK Imager	60
Tabel 4.19 Hasil Temuan Bukti Digital.....	63