

**INVESTIGASI ANTI FORENSIC KASUS PENGEDARAN
NARKOTIKA PADA CHROME BROWSER DENGAN INCOGNITO
MODE MENGGUNAKAN TEKNIK LIVE FORENSIC**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana Program Studi S1
Teknik Komputer



disusun oleh

ABDUL FAYYED

17.83.0030

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA**

2024

**INVESTIGASI ANTI FORENSIC KASUS PENGEDARAN
NARKOTIKA PADA CHROME BROWSER DENGAN INCOGNITO
MODE MENGGUNAKAN TEKNIK LIVE FORENSIC**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana Program Studi S1
Teknik Komputer



disusun oleh

ABDUL FAYYED

17.83.0030

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA**

2024

HALAMAN PERSETUJUAN

SKRIPSI

INVESTIGASI ANTI FORENSIC KASUS PENGEDARAN
NARKOTIKA PADA CHROME BROWSER DENGAN
INCOGNITO MODE MENGGUNAKAN TEKNIK LIVE
FORENSIC

Abdul Fayyed

17.83.0030

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 08 Mei 2024

Dosen Pembimbing,



Joko Dwi Santoso, M.Kom

NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

INVESTIGASI ANTI FORENSIC KASUS PENGEDARAN
NARKOTIKA PADA CHROME BROWSER DENGAN
INCOGNITO MODE MENGGUNAKAN TEKNIK LIVE
FORENSIC

yang disusun dan diajukan oleh

Abdul Fayyed

17.83.0030

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Juni 2024

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Anggit F. Nugraha, S.T., M.Eng.
NIK. 190302480

Ali Mustopa, M.Kom
NIK. 190302192

Joko Dwi Santoso, M.Kom
NIK. 190302181



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Juni 2024

DEKAN FAKULTAS ILMU KOMPUTER



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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama Mahasiswa : Abdul Fayyed
NIM : 17.83.0030

Menyatakan bahwa Skripsi dengan judul berikut:
Investigasi Anti Forensic Kasus Pengedaran Narkotika Pada Chrome Browser Dengan Incognito Mode Menggunakan Teknik Live Forensic

Dosen Pembimbing : Joko Dwi Santoso, 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, 26 Juni 2024 Yang

Menyatakan,



Abdul Fayyed

HALAMAN PERSEMBAHAN

Puji syukur kita panjatkan ke hadirat Allah SWT, Tuhan Yang Maha Esa, atas rahmat, hidayah, dan karunia-Nya yang tiada terhingga. Shalawat serta salam semoga tercurah kepada junjungan kita, Nabi Muhammad SAW, keluarganya, dan para sahabat yang mulia, yang telah membawa cahaya petunjuk bagi umat manusia hingga akhir zaman.

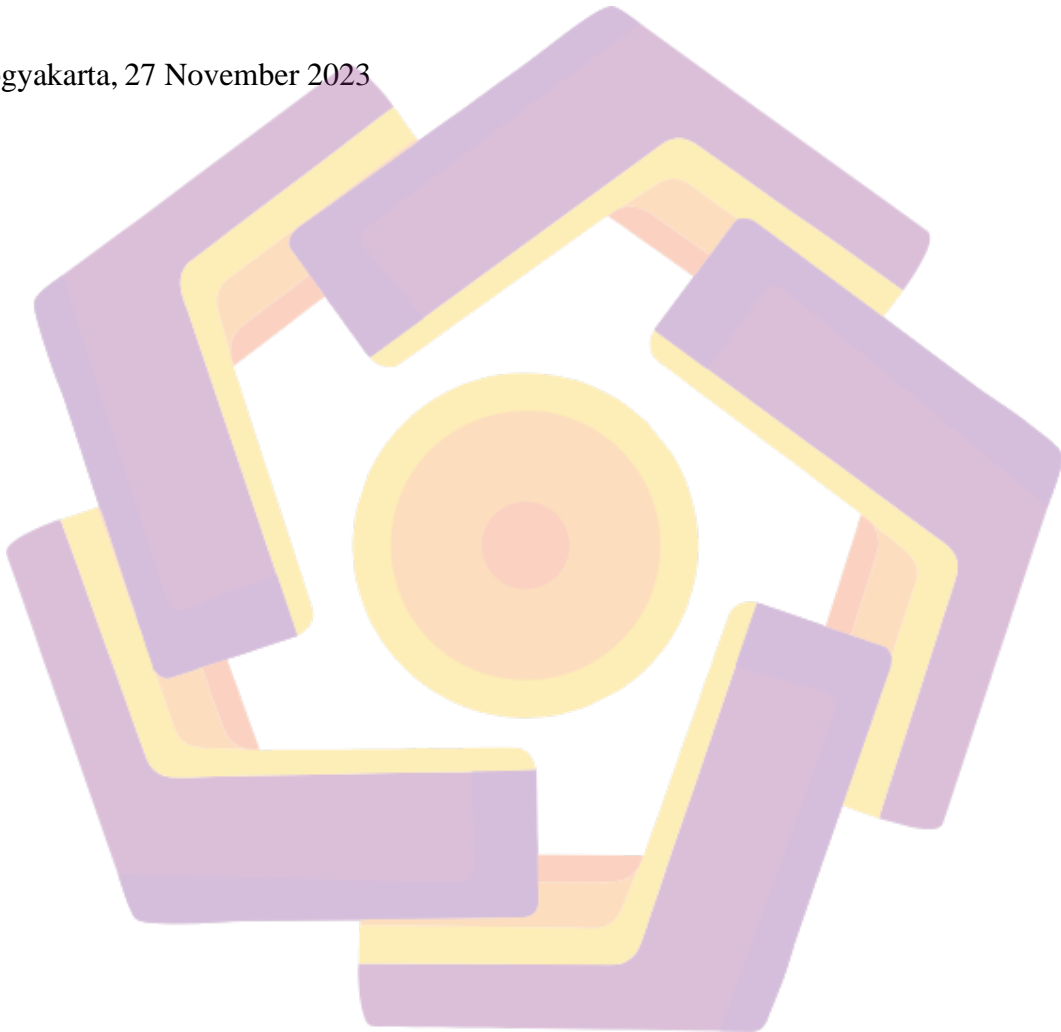
Dengan izin dan pertolongan Allah SWT, skripsi ini berhasil diselesaikan sebagai bagian dari upaya kami untuk menambah wawasan dan mengabdikan diri dalam bidang ilmu pengetahuan. Skripsi ini berjudul "*Investigasi Anti Forensic Kasus Pengedaran Narkotika Pada Chrome Browser Dengan Incognito Mode Menggunakan Teknik Live Forensic*" dan telah disusun dengan dedikasi serta kerjakeras yang tidak terlepas dari bimbingan dan dukungan dari berbagai pihak.

1. Allah SWT, atas rahmat, hidayah, dan kekuatan-Nya dalam menyelesaikan skripsi ini.
2. Keluarga penulis, yang selalu memberikan dukungan, cinta, dan doa untuk kesuksesan penulis dalam menyelesaikan skripsi ini.
3. Pembimbing skripsi, Joko Dwi Santoso, M.Kom. atas bimbingan, saran, dan pengarahan yang berharga dalam penyusunan skripsi ini.
4. Dosen-dosen di S1 Teknik Komputer, atas ilmu, pengajaran, dan dukungan yang telah diberikan kepada penulis selama perkuliahan.
5. Teman-teman penulis, yang selalu hadir dalam suka dan duka, serta memberikan semangat dan motivasi dalam menyelesaikan skripsi ini.

6. Orang-orang yang tidak bisa disebutkan satu per satu, yang memberikan dukungan dan bantuan dalam berbagai bentuk selama proses penulisan skripsi ini.

Penulis menyadari Skripsi ini masih jauh dari sempurna, karena hal tersebut tidak lepas dari kelemahan dan keterbatasan penulis. Akhirnya penulis berharap agar Skripsi ini berguna sebagian tambahan ilmu pengetahuan serta dapat memberikan manfaat bagi semua pihak dan dijadikan implementasi selanjutnya bagi mahasiswa.

Yogyakarta, 27 November 2023



KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa atas segala petunjuk, rahmat, pertolongan serta kekuatan yang berikan kepada penulis dalam menyelesaikan skripsi dengan judul “ *Investigasi Anti Forensic Kasus Pengedaran Narkotika Pada Chrome Browser Dengan Incognito Mode Menggunakan Teknik Live Forensic.*”

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih kepada seluruh pihak yang terlibat dalam memberikan dukungan, arahan, bimbingan dan semangat sehingga penulis dapat menyelesaikan skripsi ini dan berjalan lancar, untuk itu penulis mengucapkan terima kasih kepada :

1. Allah SWT atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan lancar dan semoga dapat bermanfaat di kemudian hari.
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. Bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang telah bersedia meluangkan waktunya untuk membimbing dan mengarahkan dalam penyusunan Skripsi ini.
5. Bapak Banu Santoso, S.T., M.Eng. 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 kepada penulis di bangku perkuliahan dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.

7. Kedua orang tua dan keluarga yang senantiasa memberikan semangat, mendoakan dan orang-orang tercinta yang selalu memberikan dukungan dalam proses menyelesaikan Skripsi.
8. Untuk teman-teman Teknik Komputer 01 yang telah memberikan dukungan kepada penulis dalam menyelesaikan Skripsi.

Penyusunan skripsi ini masih jauh dari kata sempurna karena terbatasnya pengetahuan dan pengalaman penulis, untuk itu segala saran dan kritik yang membangun sangat penulis harapkan guna menyempurnakan skripsi ini dimasa mendatang. Semoga skripsi ini dapat bermanfaat dan menjadi acuan bagi penelitian serupa dan semua pihak yang terkait.

Yogyakarta, 27 November 2023

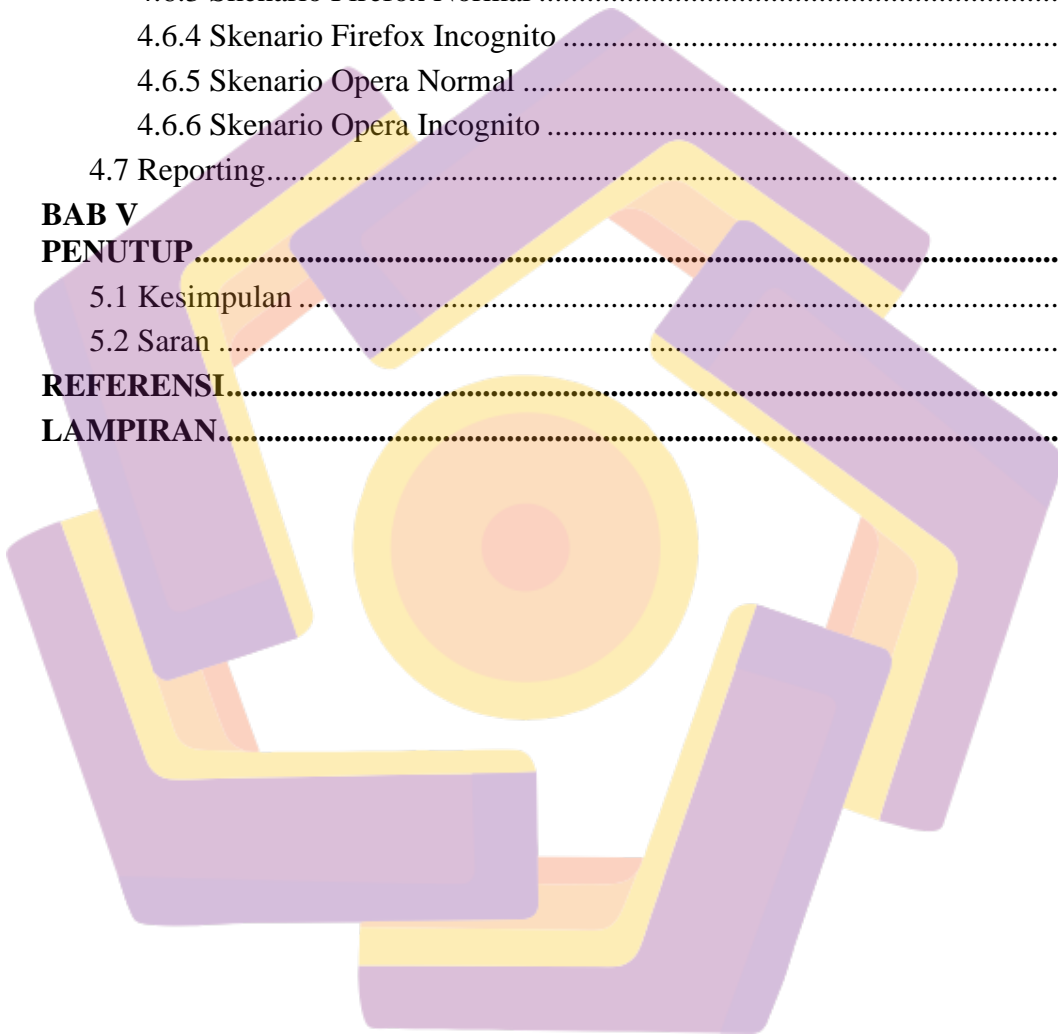
Abdul Fayyed

DAFTAR ISI

COVER	2
HALAMAN PERSETUJUAN.....	3
HALAMAN PENGESAHAN	4
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	5
KATA PENGANTAR	8
DAFTAR ISI.....	10
DAFTAR TABEL.....	14
DAFTAR GAMBAR	15
INTISARI	18
ABSTRACT.....	19
BAB I	
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB II	
TINJAUAN PUSTAKA	5
2.1 Studi Literatur	5
2.2 Forensik Digital.....	11
2.3 Bukti Digital.....	11
2.4 National Institute of Justice (NIJ)	12
2.5 Live Forensics	12
2.6 Telegram	13
2.7 Narkotika.....	13
2.8 FTK Imager.....	14
2.9 MD5 Checker	14
2.10 DD.....	14
2.11 HxD Editor	15
2.12 Browser	15
2.13 Chrome.....	15
2.14 Opera.....	16
2.15 Firefox.....	16
2.16 Mode Incognito	17

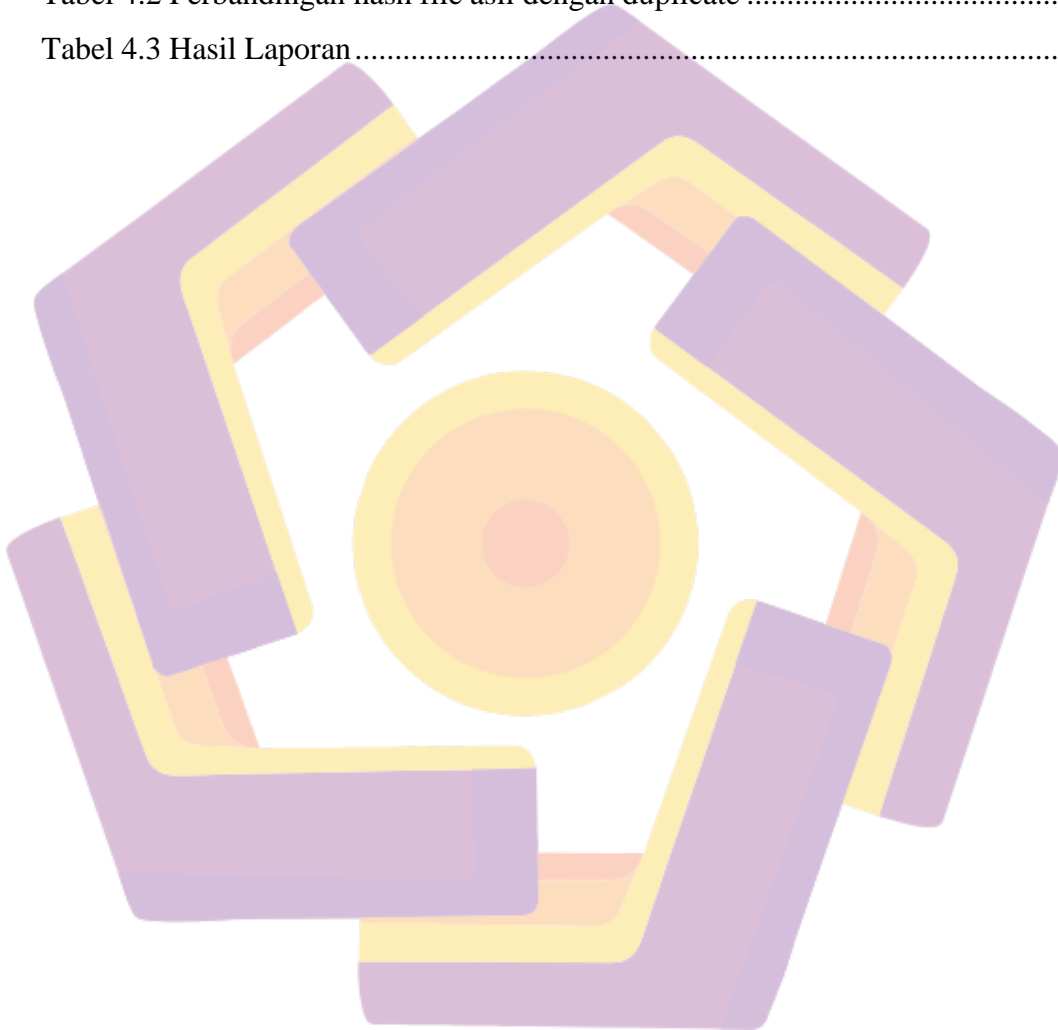
BAB III	
METODE PENELITIAN	18
3.1 Objek Penelitian	18
3.2 Alur Penelitian	18
3.2.1 Identification	18
3.2.2 Collection	19
3.2.3 Examination	19
3.2.4 Analysis.....	19
3.2.5 Reporting.....	19
3.3 Alat dan Bahan.....	20
3.4 Tahapan Persiapan Penelitian	21
3.5 Skenario Kasus.....	21
3.5.1 Eksperimen pertama, Skenario chat pada Browser Chrome.....	23
3.5.2 Eksperimen pertama, Skenario chat pada Browser Firefox.....	24
3.5.3 Eksperimen pertama, Skenario chat pada Browser Opera.....	25
3.6 Alur Penelitian	25
3.7 Teknik Analisis	27
3.7.1 Teknik String Filtering.....	27
BAB IV	
HASIL DAN PEMBAHASAN	28
4.1 Persiapan Sistem Pelaku	28
4.1.1 Mempersiapkan Virtual Machine.....	28
4.1.2 Install Windows 7	32
4.1.3 Install tools FTK Imager	34
4.2 Persiapan Sistem Investigator	37
4.2.1 Tools HDD	37
4.2.2 Install tools HxD	37
4.3 Implementasi Skenario.....	40
4.3.1 Skenario dengan browser Chrome	40
4.3.1.1 Chrome mode Normal.....	40
4.3.1.2 Chrome mode Incognito	41
4.3.2 Skenario dengan browser Firefox	42
4.3.2.1 Firefox mode Normal.....	42
4.3.2.2 Firefox mode Incognito.....	43
4.3.3 Skenario dengan browser Opera	44
4.3.3.1 Opera mode Normal.....	44
4.3.3.2 Opera mode Incognito.....	45
4.4 Identifikasi	46

4.5 Collection	47
4.5.1 Akuisisi dengan FTK Imager	47
4.5.2 Duplikasi	50
4.5.2.1 Proses duplikat	51
4.5.3 Validasi hash	52
4.6 Examination dan Analysis	55
4.6.1 Skenario Chrome Normal	56
4.6.2 Skenario Chrome Incognito	57
4.6.3 Skenario Firefox Normal	58
4.6.4 Skenario Firefox Incognito	59
4.6.5 Skenario Opera Normal	60
4.6.6 Skenario Opera Incognito	61
4.7 Reporting.....	62
BAB V	
PENUTUP.....	64
5.1 Kesimpulan	64
5.2 Saran	65
REFERENSI.....	67
LAMPIRAN.....	72



DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian.....	7
Tabel 3.1 Alat dan bahan penelitian.....	20
Tabel 3.2 Skenario Chat.....	22
Tabel 4.1 Hasil akuisisi	49
Tabel 4.2 Perbandingan hash file asli dengan duplicate	55
Tabel 4.3 Hasil Laporan.....	62

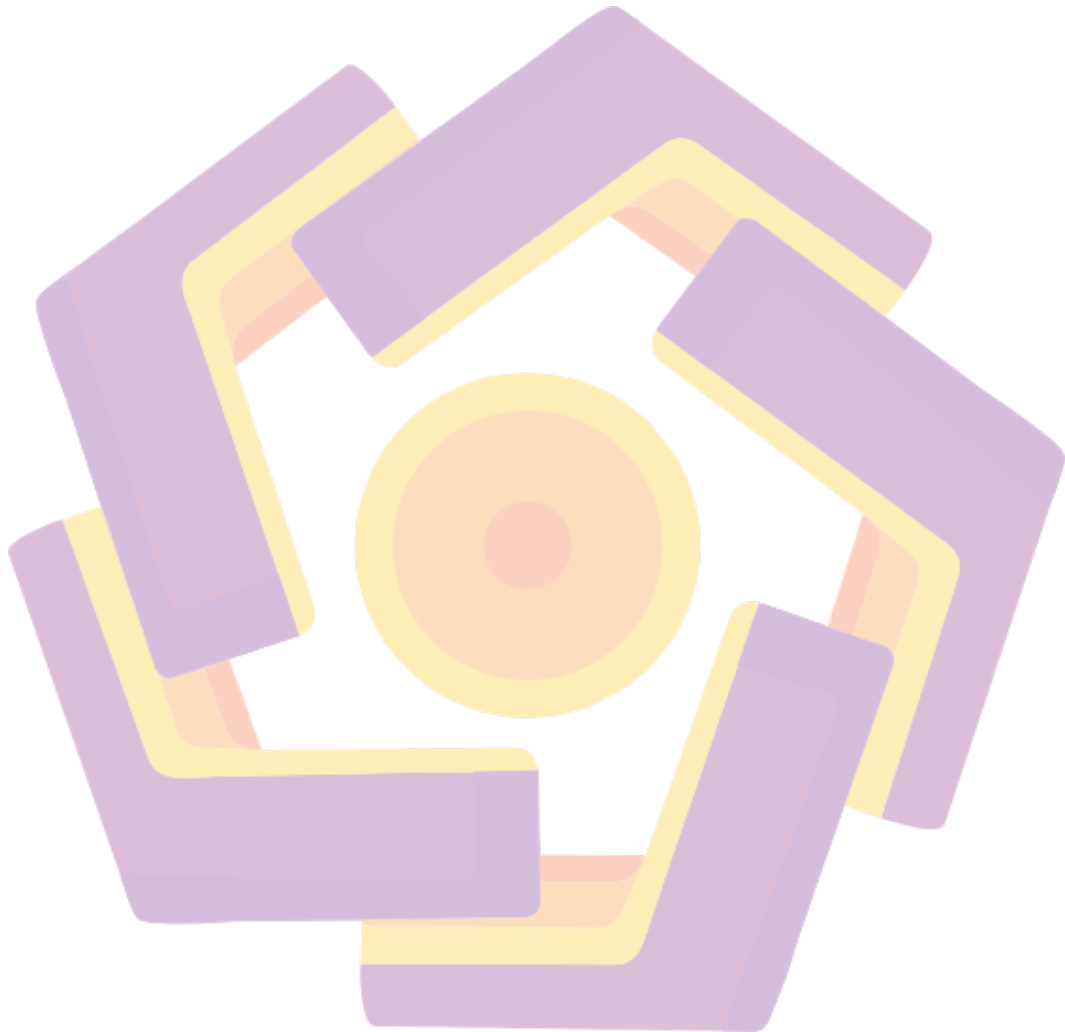


DAFTAR GAMBAR

Gambar 3.1 Tahapan metode National Institute of Justice	18
Gambar 3.2 Tahapan persiapan penelitian	21
Gambar 3.3 Skenario Browser Chrome mode Normal	23
Gambar 3.4 Skenario Browser Chrome mode Incognito	23
Gambar 3.5 Skenario Browser Firefox mode Normal	24
Gambar 3.6 Skenario Browser Firefox mode Incognito	24
Gambar 3.7 Skenario Browser Opera mode Normal	25
Gambar 3.8 Skenario Browser Opera mode Incognito	25
Gambar 3.9 Alur Penelitian	26
Gambar 3.10 Teknik String Filtering	27
Gambar 4.1 Proses persiapan VM	28
Gambar 4.2 Mengatur versi OS dan nama OS	29
Gambar 4.3 Menentukan ukuran RAM	29
Gambar 4.4 Mengatur jenis disk virtual	30
Gambar 4.5 Mengatur tipe file disk	30
Gambar 4.6 Mengatur ukuran disk	31
Gambar 4.7 Memasukkan ISO ke VM	31
Gambar 4.8 Tampilan awal VM dengan OS windows 7	32
Gambar 4.9 Install now untuk memulai	32
Gambar 4.10 Diminta mengikuti ketentuan lisensi	33
Gambar 4.11 Memilih disk yang ada	33
Gambar 4.12 Proses terakhir instalasi	34
Gambar 4.13 Proses awal install FTK Imager	35
Gambar 4.14 Diminta menyetujui lisensi	35
Gambar 4.15 Menentukan penyimpanan system	36
Gambar 4.16 Install FTK Imager selesai	36

Gambar 4.17 Tahap awal install HxD.....	37
Gambar 4.18 Menyetujui license dari HxD	38
Gambar 4.19 Menentukan penyimpanan file system.....	38
Gambar 4.20 Proses install HxD.....	39
Gambar 4.21 Tahap terakhir install HxD.....	39
Gambar 4.22 Chat pada Skenario 1	41
Gambar 4.23 Chat pada Skenario 2	42
Gambar 4.24 Chat pada Skenario 3	43
Gambar 4.25 Chat pada Skenario 4	44
Gambar 4.26 Chat pada Skenario 5	45
Gambar 4.27 Chat pada Skenario 6	46
Gambar 4.28 Tampilan awal FTK Imager	47
Gambar 4.29 Seting nama dan penyimpanan FTK Imager.....	48
Gambar 4.30 Proses Capture FTK Imager.....	48
Gambar 4.31 Proses tool DD pada skenario Chrome Normal	51
Gambar 4.32 Proses tool DD pada skenario Chrome Incognito	51
Gambar 4.33 Proses tool DD pada skenario Firefox Normal	51
Gambar 4.34 Proses tool DD pada skenario Firefox Incognito	52
Gambar 4.35 Proses tool DD pada skenario Opera Normal	52
Gambar 4.36 Proses tool DD pada skenario Opera Incognito	52
Gambar 4.37 Hasil hash pada skenario Chrome Normal.....	53
Gambar 4.38 Hasil hash pada skenario Chrome Incognito.....	53
Gambar 4.39 Hasil hash pada skenario Firefox Normal.....	53
Gambar 4.40 Hasil hash pada skenario Firefox Incognito.....	54
Gambar 4.41 Hasil hash pada skenario Opera Normal	54
Gambar 4.42 Hasil hash pada skenario Opera Incognito.....	54
Gambar 4.43 Hasil Analisis skenario Chrome Normal pada HxD	56

Gambar 4.44 Hasil Analisis skenario Chrome Incognito pada HxD57
Gambar 4.45 Hasil Analisis skenario Firefox Normal pada HxD58
Gambar 4.46 Hasil Analisis skenario Firefox Incognito pada HxD59
Gambar 4.47 Hasil Analisis skenario Opera Normal pada HxD60
Gambar 4.48 Hasil Analisis skenario Opera Incognito pada HxD61



INTISARI

Chrome Browser salah satu *aplikasi* web browser yang paling populer digunakan di seluruh dunia. Chrome Browser juga dikenal sebagai browser yang aman karena memiliki fitur keamanan seperti perlindungan malware dan phishing. Dalam perkembangannya, Chrome Browser terus melakukan pembaruan dan peningkatan untuk meningkatkan kinerja dan pengalaman pengguna.

Berbagai teknik digital forensik terus berkembang dalam upaya mengumpulkan bukti kritikal dalam proses mengungkap kasus peredaran narkoba. Salah satu tekniknya adalah *live forensic*, dimana dengan teknik ini investigator memungkinkan mendapat data volatile yang tersimpan pada memori RAM, pagefile ataupun file hibernasi. Data pada *memory* RAM menjadi sumber bukti digital yang sensitif karena menyimpan banyak informasi penting ketika sistem dalam keadaan hidup (real time) seperti program yang berjalan, chat logs, network connections atau bahkan cryptographic keys.

Fokus penelitian ini akan mengevaluasi dan menganalisis bukti potensial *memory* RAM dengan studi kasus Chrome Browser menggunakan metodologi NIJ. Hasil penelitian ini adalah pembuktian temuan berbagai artefak penting dari beberapa skenario dan eksperimen yang sudah dipersiapkan sehingga dapat menjadi bukti digital yang valid dalam investigasi tindak kejahatan.

Kata kunci: *Chrome, RAM, Digital Forensik, Browser.*

ABSTRACT

The Chrome Browser is one of the most popular web browsers used worldwide. It is also known as a secure browser due to its security features, such as malware and phishing protection. In its development, Chrome Browser continues to update and improve to enhance performance and user experience.

Various digital forensics techniques are continuously evolving in an effort to gather critical evidence in drug trafficking cases. One of these techniques is live forensic analysis, where investigators can retrieve volatile data stored in RAM, pagefile, or hibernation files. Data in RAM is a sensitive digital evidence source because it contains a wealth of important information when the system is running in real-time, such as running programs, chat logs, network connections, or even cryptographic keys.

This research focuses on evaluating and analyzing potential evidence in RAM memory with a case study on Chrome Browser using the NIJ methodology. The research findings provide evidence of various important artifacts from several prepared scenarios and experiments, making them valid digital evidence in crime investigations.

Keywords: *Chrome, RAM, Digital Forensics, Browser.*