

**ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC
DAN DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL
WHATSAPP WEB**

SKRIPSI

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



Disusun oleh:

RACHMAT WAHYUDI

18.83.0233

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

**ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC
DAN DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL
WHATSAPP WEB**

SKRIPSI

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



disusun oleh

RACHMAT WAHYUDI

18.83.0233

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC DAN DISK
FORENSIK PADA INVESTIGASI BUKTI DIGITAL WHATSAPP WEB**

Yang disusun dan diajukan oleh

Rachmat Wahyudi

18.83.0233

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 21 Februari 2024

Dosen Pembimbing,



Banu Santoso, S.T., M.Eng.

NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

**ANALISA PERBANDINGAN EFEKTIFITAS LIVE FORENSIC DAN
DISK FORENSIK PADA INVESTIGASI BUKTI DIGITAL WHATSAPP
WEB**

yang disusun dan diajukan oleh

Rachmat Wahyudi

18.83.0233

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Februari 2024

Susunan Dewan Penguji

Nama Penguji

Jeki Kuswanto, M.Kom
NIK. 190302456

Joko Dwi Santoso, M.Kom
NIK. 190302181

Banu Santoso, S.T., M.Eng
NIK. 190302327

Panda Vangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Februari 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 : Rachmat Wahyudi

NIM : 18.83.0233

Menyatakan bahwa Skripsi dengan judul berikut:

Analisa Perbandingan Efektifitas Live Forensic dan Disk Forensic pada Investigasi Bukti Digital Whatsapp Web

Dosen Pembimbing : Banu Santoso, S.T., M.Eng.

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

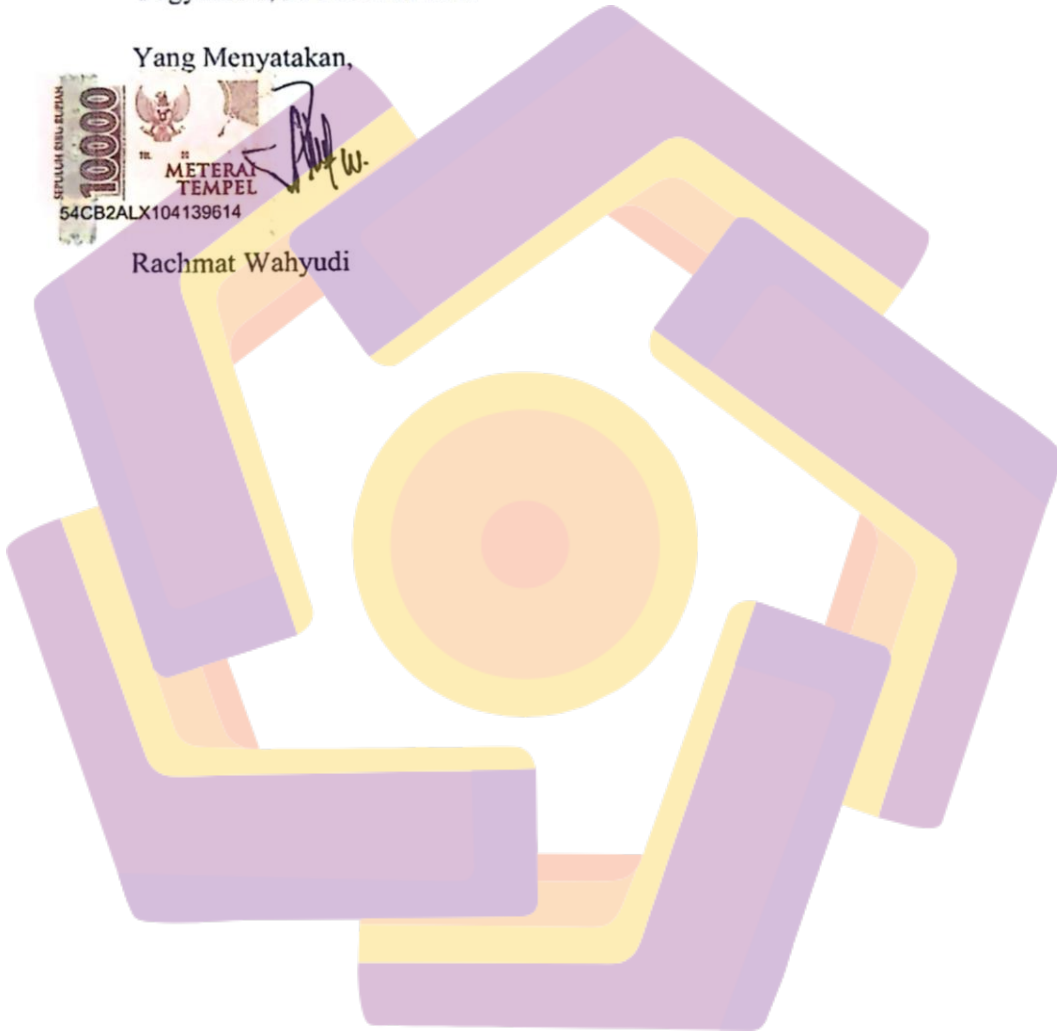
yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 Februari 2024

Yang Menyatakan,



Rachmat Wahyudi



HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Orang tua saya, yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak, Banu Santoso, S.T., M.Eng. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Investigasi Anti Forensic Terhadap Bukti Digital USB Flashdisk dengan Metode NIST”. Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

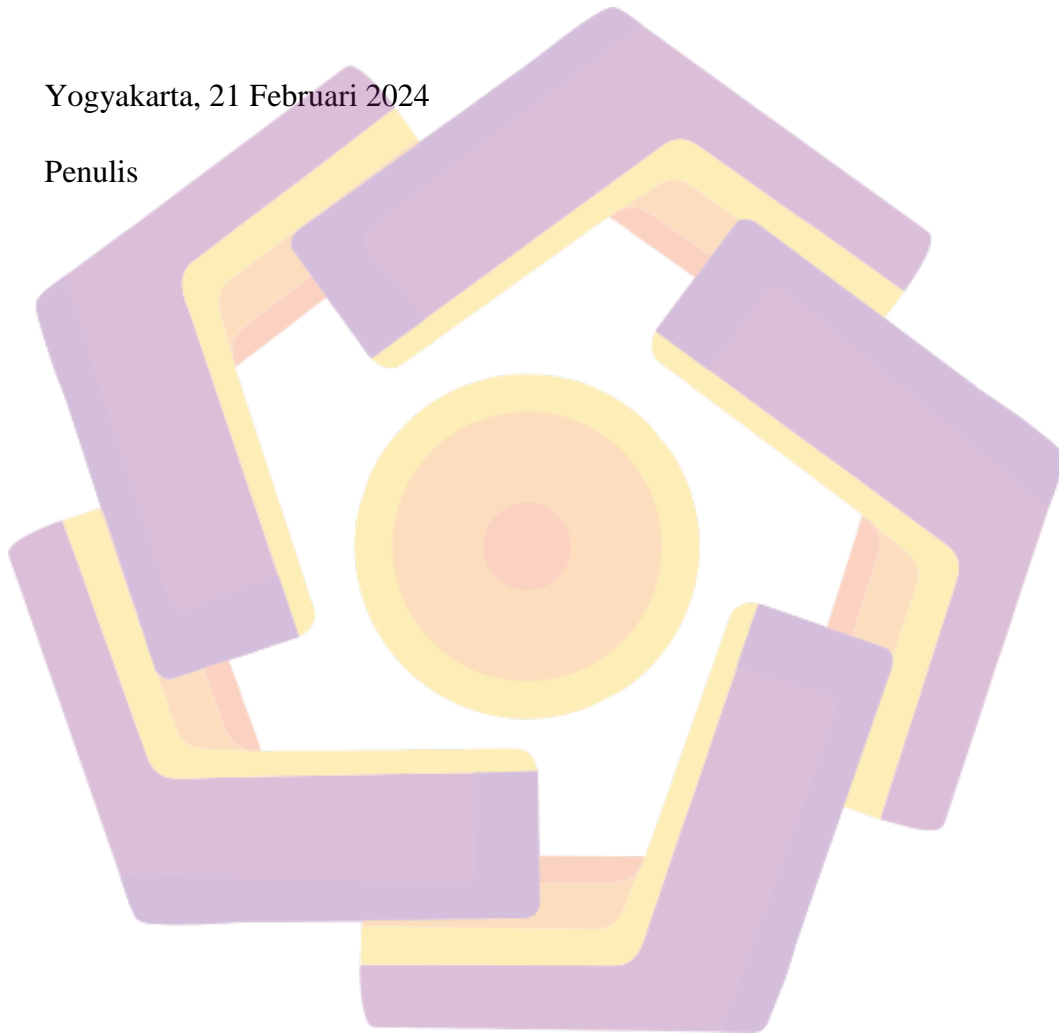
Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada :

1. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat 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. Banu Santoso, S.T., M.Eng. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahannya dan bimbingan dalam penyusunan Skripsi ini.
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.
7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 21 Februari 2024

Penulis

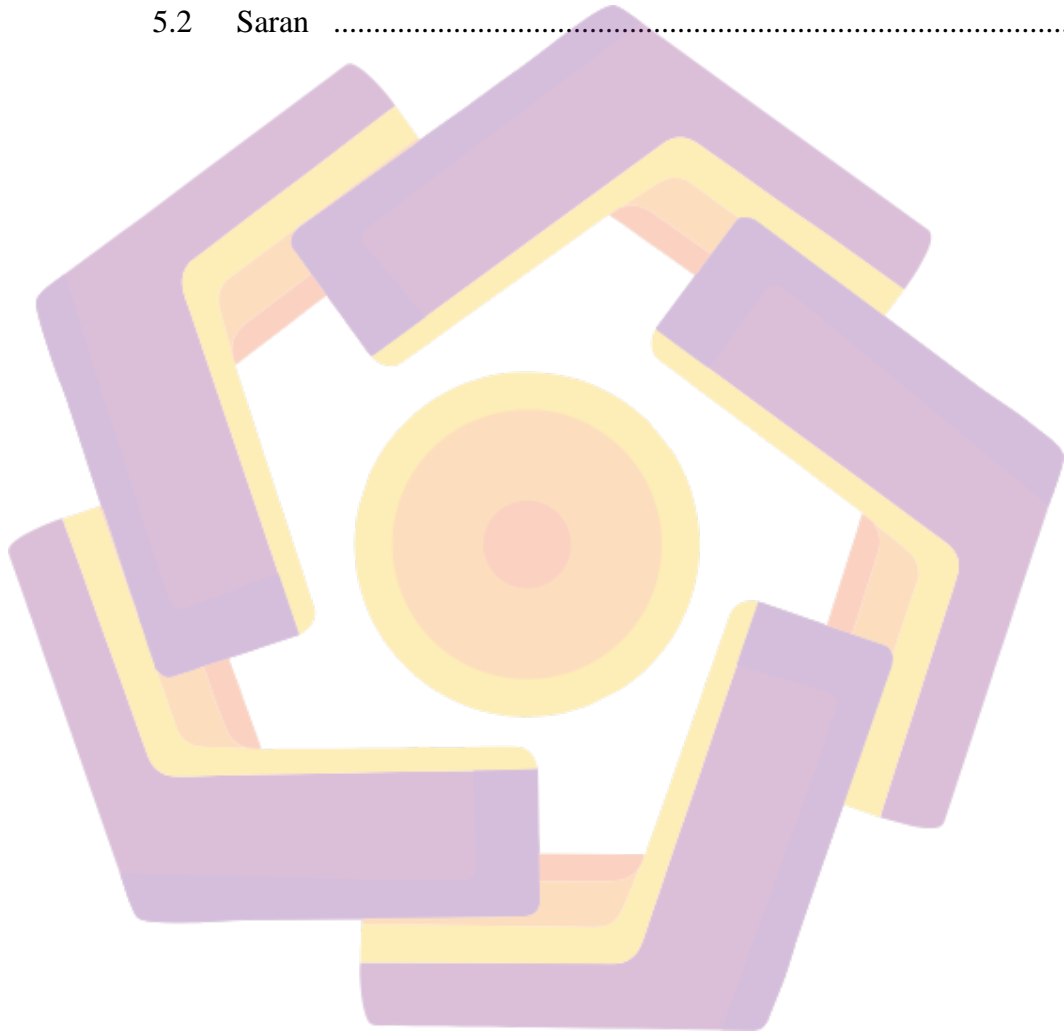


DAFTAR ISI

HALAMAN PERSETUJUAN.....	ii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	vi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	6
2.1 Studi Literatur	6
2.2 Dasar Teori.....	10
2.3 <i>Standard Operating Procedure (SOP)</i>	11
2.3 Artefak Bukti Digital	11
2.4 <i>NIJ Framework</i>	11
2.5 Dead Forensic	14
2.5.1 Disk Forensic.....	14
2.6 Live Forensic	15
2.7 Hashing	15
2.8 Kebutuhan Tool Investigasi	16
2.8.1 MD5 Checker	16
2.8.2 FTK Imager	16
2.8.3 Autopsy	17
2.8.4 Volatility.....	17
2.8.5 Foremost.....	17
2.8.6 Bulk Extractor	18

2.8.7 File Carving.....	18
2.8.8 String Filtering	18
BAB III METODOLOGI PENELITIAN	19
3.1 Objek Penelitian.....	19
3.2 Alur Penelitian	20
3.3 Persiapan Alat dan Bahan Penelitian	21
3.3.1 Lingkungan Simulasi.....	21
3.3.2 Software (Perangkat Lunak).....	22
3.4 Skenario dan Simulasi Kasus.....	23
3.5 Metode Penelitian	25
3.5.1 National Institute of Justice (NIJ)	25
BAB IV PEMBAHASAN.....	28
4.5 Persiapan	28
4.5.1 Persiapan Environment VM Pelaku	28
4.5.2 Pemasangan Environment dan Tools Investigator	29
4.5.3 Pemasangan Environment dan Tools Investigator.....	31
4.6 Penerapan Skenario Penelitian.....	33
4.6.1 Chrome Kondisi Normal	36
4.6.2 Chrome Hapus History + Cookies + Cache	37
4.6.3 Chrome Incognito.....	39
4.6.3 Chrome VPN	40
4.6.4 Uninstall Chrome	43
4.6.5 Identification dan Collection	44
4.6.6 Akuisisi RAM (Live Forensic).....	44
4.6.7 Akuisisi Disk (Dead Forensic)	50
4.6.8 Duplikat Hasil Akuisisi	53
4.6.9 Eksaminasi dan Analisa.....	55

4.7.0	Analisa Menggunakan Disk Forensic.....	55
4.7.1	Analisa menggunakan Live Forensic	59
4.8	Laporan Akhir Investigasi.....	67
BAB V PENUTUP		72
5.1	Kesimpulan	72
5.2	Saran	73



DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian	6
Tabel 2.2 Penelitian yang Diusulkan	10
Tabel 3.1 Spesifikasi PC Investigator	23
Tabel 3.2 Spesifikasi Virtual Machine Pelaku	23
Tabel 3.3 Kebutuhan Perangkat Lunak Investigator.....	23
Tabel 3.4 Implementasi Teknik Menghilangkan Jejak Digital	25
Tabel 4.1 Implementasi Skenario Penghapusan Jejak Digital	34
Tabel 4.2 Detail Ukuran File (Bytes) Artefak Gambar.....	35
Tabel 4.3 Implementasi Skenario Pertama Penghapusan Jejak.....	37
Tabel 4.4 Implementasi Skenario Kedua Penghapusan Jejak Digital.....	39
Tabel 4.5 Implementasi Skenario Ketiga Penghapusan Jejak Digital	41
Tabel 4.6 Implementasi Skenario Keempat Penghapusan Jejak Digital.....	43
Tabel 4.7 Implementasi Skenario Kelima Penghapusan Jejak Digital	45
Tabel 4.8 Hasil Akuisisi Memory RAM.....	49
Tabel 4.9 Hasil Akuisisi Memory DISK VM	54
Tabel 4.10 MD5 Hash Dari Hasil Imaging Memori RAM	56
Tabel 4.11 Penggunaan Fungsi Tool dalam Analisa RAM	60
Tabel 4.12 Perintah Volatility Yang Penulis Gunakan dalam Analisa Memori RAM	61
Tabel 4.13 Process ID Browser Chrome.....	63
Tabel 4.14 Hasil Analisa Skenario Pertama.....	68
Tabel 4.15 Hasil Analisa Skenario Kedua	69
Tabel 4.16 Hasil Analisa Skenario Ketiga	69
Tabel 4.17 Hasil Analisa Skenario Keempat	70
Tabel 4.18 Hasil Analisa Skenario Kelima.....	70

DAFTAR GAMBAR

Gambar 2.1 Tahapan Metodologi NIJ	13
Gambar 3.1 Alur Investigasi Forensik menggunakan Metodologi NIJ	21
Gambar 3.2 Implementasi Simulasi dan Skenario	24
Gambar 3.3 Tahapan Penanganan Forensik Metode NIJ.....	26
Gambar 4.1 Instalasi Virtual Mesin Pelaku	28
Gambar 4.2 Sharing Folder PC Asli dengan VM	29
Gambar 4.3 Tool FTK Imager Siap Diinstall	30
Gambar 4.4 Pilih Opsi Accept atau Terima	30
Gambar 4.5 FTK Imager Berhasil Terinstall	31
Gambar 4.6 File Executable DD	32
Gambar 4.7 Lokasi Tool DD sudah Ditambahkan ke Path Environment.....	32
Gambar 4.8 Tool DD Siap Digunakan.....	33
Gambar 4.9 Bahan Barang Bukti Gambar	35
Gambar 4.10 MD5 Hash Checksum dari Kelima File.....	36
Gambar 4.11 Impementasi Skenario Pertama.....	37
Gambar 4.12 Implementasi Skenario Kedua	38
Gambar 4.13 Skenario Kedua Melakukan Hapus History dan Cache	39
Gambar 4.14 Penggunaan Incognito Browser Skenario Ketiga	40
Gambar 4.15 Aktivitas Percakapan Dilakukan	40
Gambar 4.16 Skenario Keempat Menggunakan VPN	41
Gambar 4.17 VPN Menggunakan Server US	42
Gambar 4.18 Aktivitas Percakapan Skenario Keempat Dilakukan	42
Gambar 4.19 Pengiriman Bukti Pesan Skenario Kelima	44
Gambar 4.20 Melakukan Uninstall Browser Chrome.....	44
Gambar 4.21 Akuisisi RAM akan Dilakukan	46
Gambar 4.22 Pemilihan Destination Path Akuisisi.....	46
Gambar 4.23 Akuisisi RAM Sedang Berlangsung	47
Gambar 4.24 Proses Akuisisi RAM Selesai dilakukan.....	47
Gambar 4.25 Output Hasil Akuisisi.....	48
Gambar 4.26 Size File Akuisisi RAM	48

Gambar 4.27 Informasi Lain Hasil File Akuisisi RAM.....	49
Gambar 4.28 Pilih Add Evidence Item	50
Gambar 4.29 Physical Drive Evidence Type	51
Gambar 4.30 Pemilihan Drive VBOX HARDDISK	51
Gambar 4.31 Image Type dipilih raw (dd)	52
Gambar 4.32 Mengatur Detail Penyimpanan Akuisisi	52
Gambar 4.33 Proses Akuisisi Disk VM Sedang Berlangsung	53
Gambar 4.34 Output Hasil Akuisisi.....	53
Gambar 4.35 Imaging File Memori Image RAM	54
Gambar 4.36 Output File Hasil Imaging.....	55
Gambar 4.37 File Asli dan Hasil Duplikat Memiliki Hash yang Sama.....	55
Gambar 4.38 Pemilihan Data Source	57
Gambar 4.39 Proses Scanning Data Autopsy pada Disk Image	57
Gambar 4.40 Barang Bukti Terbaca di Autopsy.....	58
Gambar 4.41 Melihat Berbagai Jenis File dengan Autopsy.....	59
Gambar 4.42 Runtutan Riwayat Aktifitas Browsing	59
Gambar 4.43 Aktivitas Pelaku Mengakses Whatsapp	60
Gambar 4.44 Profile Volatility dari RAM bisa Terlihat	62
Gambar 4.45 Informasi Chrome yang Berjalan pada RAM Pelaku	63
Gambar 4.46 Kata Kunci GANJA Berhasil ditemukan Pada Analisa RAM.....	64
Gambar 4.47 Ekstraksi Informasi Penting Lain dengan bulk extractor.....	64
Gambar 4.48 Output File hasil Ekstraksi Bulk_extractor	65
Gambar 4.49 Carving Url dari Memory Image	66
Gambar 4.50 Ekstraksi Carving Menggunakan Foremost	66
Gambar 4.51 Ekstraksi Carving Menggunakan Foremost.....	67
Gambar 4.52 Perolehan File Gambar dari Proses File Carving.....	67

INTISARI

Internet tidak hanya memberikan manfaat bagi masyarakat, namun juga dapat menimbulkan dampak negatif. Salah satunya yaitu kejahatan dunia maya. Sosial media yang sering digunakan oleh masyarakat dapat disalahgunakan untuk dijadikan sebagai media kejahatan. Salah satunya melalui sosial media yang populer di Indonesia, yaitu Whatsapp. Kasus peredaran narkoba melalui aplikasi Whatsapp sering terjadi di Indonesia, sehingga memerlukan penanganan lebih lanjut agar kasus kejahatan tersebut dapat diselesaikan dan pelaku dapat mempertanggungjawabkan perbuatannya.

Salah satu teknik nya adalah live forensic, dimana dengan teknik ini investigator memungkinkan mendapat data volatile yang tersimpan pada ram, pagefile ataupun hibernation file. Data pada memori ram menjadi sumber bukti digital yang sangat 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. Tidak hanya live forensic, penelitian ini juga menggabungkan analisa disk forensik sebagai acuan perbandingan efektifitas. Fokus penelitian ini akan mengevaluasi dan menganalisis bukti potensial memori ram dan disk menggunakan metode National Institute of Justice (NIJ). Hasil penelitian ini adalah pembuktian temuan berbagai artefak penting dari skenario dan eksperimen sehingga dapat menjadi bukti digital yang valid dalam proses mengungkap tindak kejahatan. Berdasarkan teknik analisa live forensic dan disk forensik, hasil akhir yang diperoleh peneliti mampu membuktikan scenario aktivitas tersebut.

Kata kunci: *Digital Forensic, Disk Forensic, Live Forensic, Whatsapp Forensic*

ABSTRACT

The internet not only provides benefits to society, but can also have negative impacts. One of them is cyber crime. Social media that is often used by the public can be misused to be used as a medium for crime. One of them is through the popular social media in Indonesia, namely Whatsapp. Cases of drug trafficking through the Whatsapp application often occur in Indonesia, so that further handling is required so that these crime cases can be resolved and the perpetrators can be held accountable for their actions.

One of the techniques is live forensic, where with this technique it is possible for investigators to obtain volatile data stored in RAM, pagefile or hibernation file. Data in RAM memory is a very sensitive source of digital evidence because it stores a lot of important information when the system is on (real time) such as running programs, chat logs, network connections or even cryptographic keys. Not only live forensics, this study also incorporates disk forensic analysis as a reference for comparing effectiveness. The focus of this research will be to evaluate and analyze the potential evidence of ram and disk memory using the National Institute of Justice (NIJ) method. The result of this research is to prove the findings of various important artifacts from scenarios and experiments so that they can become valid digital evidence in the process of uncovering crimes. Based on live forensic and disk forensic analysis techniques, the final results obtained by the researcher are able to prove the activity scenario.

Keyword: *Digital Forensic, Disk Forensic, Anti Forensic*