

**INVESTIGASI ANTI FORENSIC KASUS CYBERTERRORISM  
PADA TOR BROWSER DAN INCOGNITO MODE  
MENGUNAKAN TEKNIK LIVE FORENSIC**

**SKRIPSI**

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



disusun oleh

**DHAFIT BAGASTARA**

**17.83.0040**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2022**

**INVESTIGASI ANTI FORENSIC KASUS CYBERTERRORISM  
PADA TOR BROWSER DAN INCOGNITO MODE  
MENGUNAKAN TEKNIK LIVE FORENSIC**

**SKRIPSI**

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



disusun oleh

**DHAFIT BAGASTARA**

**17.83.0040**

Kepada

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**

**2022**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**INVESTIGASI ANTI FORENSIC KASUS CYBERTERRORISM  
PADA TOR BROWSER DAN INCOGNITO MODE  
MENGUNAKAN TEKNIK LIVE FORENSIC**

yang disusun dan diajukan oleh

**Dhafit Bagastara**

**17.83.0040**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 24 Agustus 2022

**Dosen Pembimbing,**

**Dony Ariyus, M.Kom**

**NIK. 190302128**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**INVESTIGASI ANTI FORENSIC KASUS CYBERTERRORISM**  
**PADA TOR BROWSER DAN INCOGNITO MODE**  
**MENGGUNAKAN TEKNIK LIVE FORENSIC**

yang disusun dan diajukan oleh

**Dhafit Bagastara**

**17.83.0040**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 24 Agustus 2022

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Mulia Sulistyono, M.Kom**  
**NIK. 190302248**

**Jeki Kuswanto, M.Kom**  
**NIK. 190302456**

**Dony Ariyus, M.Kom**  
**NIK. 190302128**

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 24 Agustus 2022

**DEKAN FAKULTAS ILMU KOMPUTER**

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

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Dhafit Bagastara  
NIM : 17.83.0040

Menyatakan bahwa Skripsi dengan judul berikut:

**Investigasi Anti Forensic Kasus Cyberterrorism pada Tor Browser dan Incognito Mode Menggunakan Teknik Live Forensic**

Dosen Pembimbing : Dony Ariyus, 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, 28 Agustus 2022

Yang Menyatakan,



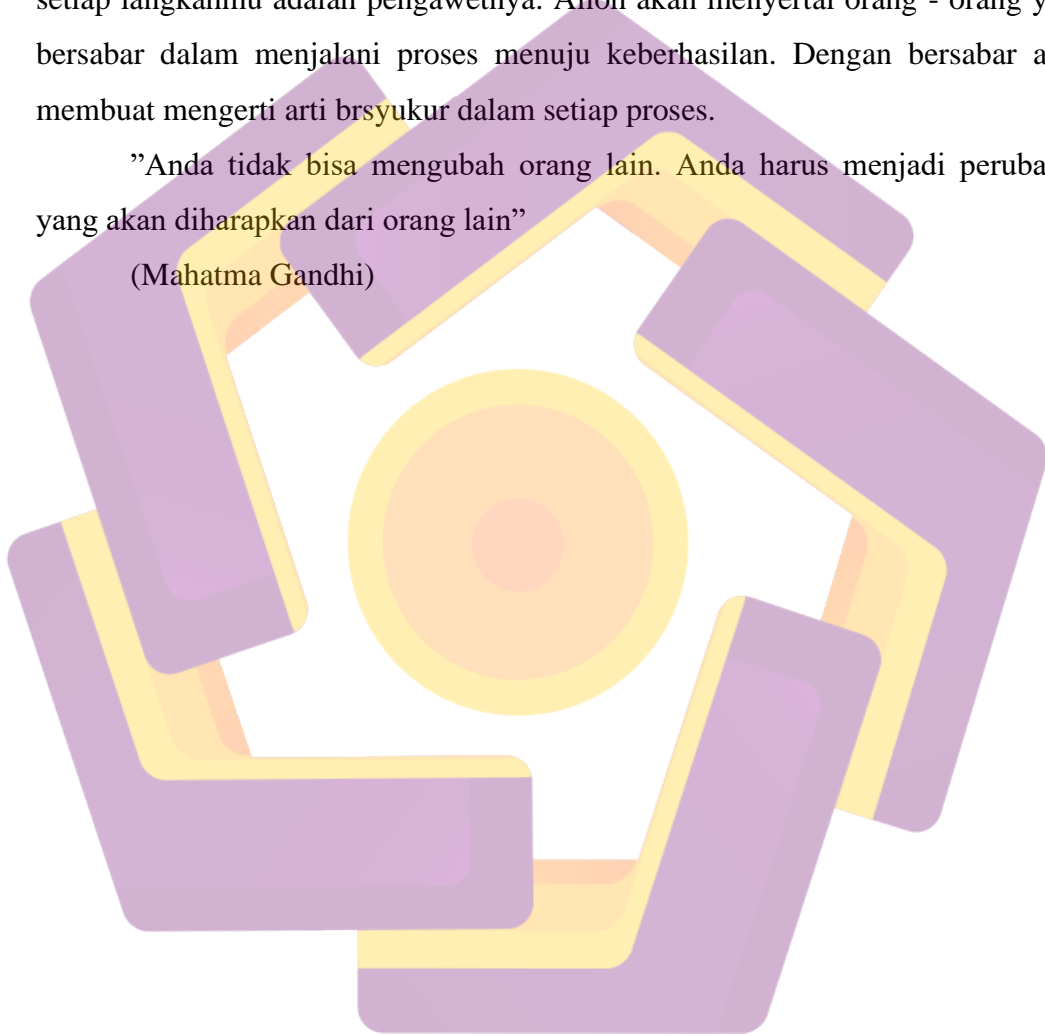
Dhafit Bagastara

## HALAMAN MOTO

Dalam pepatah, keberhasilan adalah sebuah prose. Niat adalah awal keberhasilan. Peluh keringatmu adalah penyedapnya. Doa orangtua dan doa orang-orang disekitar adalah bara api yang akan mematangkannya. Kegagalan di setiap langkahmu adalah pengawetnya. Alloh akan menyertai orang-orang yang bersabar dalam menjalani proses menuju keberhasilan. Dengan bersabar akan membuat mengerti arti bersyukur dalam setiap proses.

”Anda tidak bisa mengubah orang lain. Anda harus menjadi perubahan yang akan diharapkan dari orang lain”

(Mahatma Gandhi)



## HALAMAN PERSEMBAHAN

Alhamdulillah, segala puji bagi Allah SWT, kita memuji-Nya, dan meminta pertolongan, pengampunan serta petunjuk kepada-Nya. Kita berlindung kepada Allah dari kejahatan diri kita dan keburukan amal kita. Barang siapa yang mendapat petunjuk dari Allah, maka tidak akan ada yang menyesatkannya dan barang siapa yang sesat maka tidak akan ada pemberi petunjuk baginya. Aku bersaksi bahwa tidak ada Tuhan selain Allah dan bahwa Muhammad adalah hamba dan Rasul-Nya. Semoga doa, shalawat tercurah pada junjungan dan suri tauladan kita Nabi Muhammad SAW, keluarganya, dan sahabat serta siapa saja yang mendapat petunjuk hingga hari kiamat. Aamiin. Dalam penulisan Skripsi ini, penulis banyak mendapat bantuan dari berbagai pihak. Oleh Karena itu, ucapkan terima kasih penulis sampaikan kepada:

1. Allah SWT atas segala rahmat dan hidayahnya hingga Tugas Akhir ini dapat terselesaikan dengan baik.
2. Keluargaku tersayang, kedua orang tuaku serta kedua kakak ku yang telah memberikan kasih sayang, do'a, dukungan serta motivasi baik secara moril maupun materil untuk selalu terikat dengan hukum syara' dan menjadi orang yang bahagia di dunia maupun di akhirat.
3. Bapak Prof Dr M Suyanto MM. selaku Rektor Universitas Amikom Yogyakarta.
4. Bapak Dony Ariyus, M.Kom selaku Ketua Prodi S1 Teknik Komputer Universitas Amikom Yogyakarta.
5. Bapak Dony Ariyus, M.Kom selaku Dosen Pembimbing yang telah meluangkan waktu serta dengan penuh kesabaran telah memberikan bimbingan dalam penyusunan Skripsi.
6. Segenap Ibu dan Bapak Dosen Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta atas didikan dan bimbingannya selama ini. (Bila ada) Halaman ini berisi kepada siapa skripsi dipersembahkan. Ditulis dengan singkat, resmi, sederhana, tidak terlalu banyak, serta tidak



7. menjurus ke penulisan informal sehingga mengurangi sifat resmi laporan ilmiah.
8. Terimakasih kepada teman -teman Program Studi ahli jenjang S1 Teknik Komputer angkatan 2017 yang banyak memberikan saran, motivasi, dan kenangan, terimakasih atas dukungan selama ini.
9. Semua pihak yang tidak bisa penulis sebutkan satu persatu, terima kasih atas bantuan dan dukungannya.

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, 14 Agustus 2022



Penulis



## 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 Cyber Terrorism pada Tor Browser dan 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 Dony Ariyus, M.Kom selaku dosen pembimbing yang telah bersedia meluangkan waktunya untuk membimbing dan mengarahkan dalam penyusunan Skripsi ini.
5. Ibu Rina Permatasari. M.Kom., 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.

Kedua orang tua dan keluarga yang senantiasa memberikan semangat, mendoakan dan orang-orang tercinta yang selalu memberikan dukungan dalam proses menyelesaikan Skripsi.

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, 16 Agustus 2022

  
Dhafit Bagastara

## DAFTAR ISI

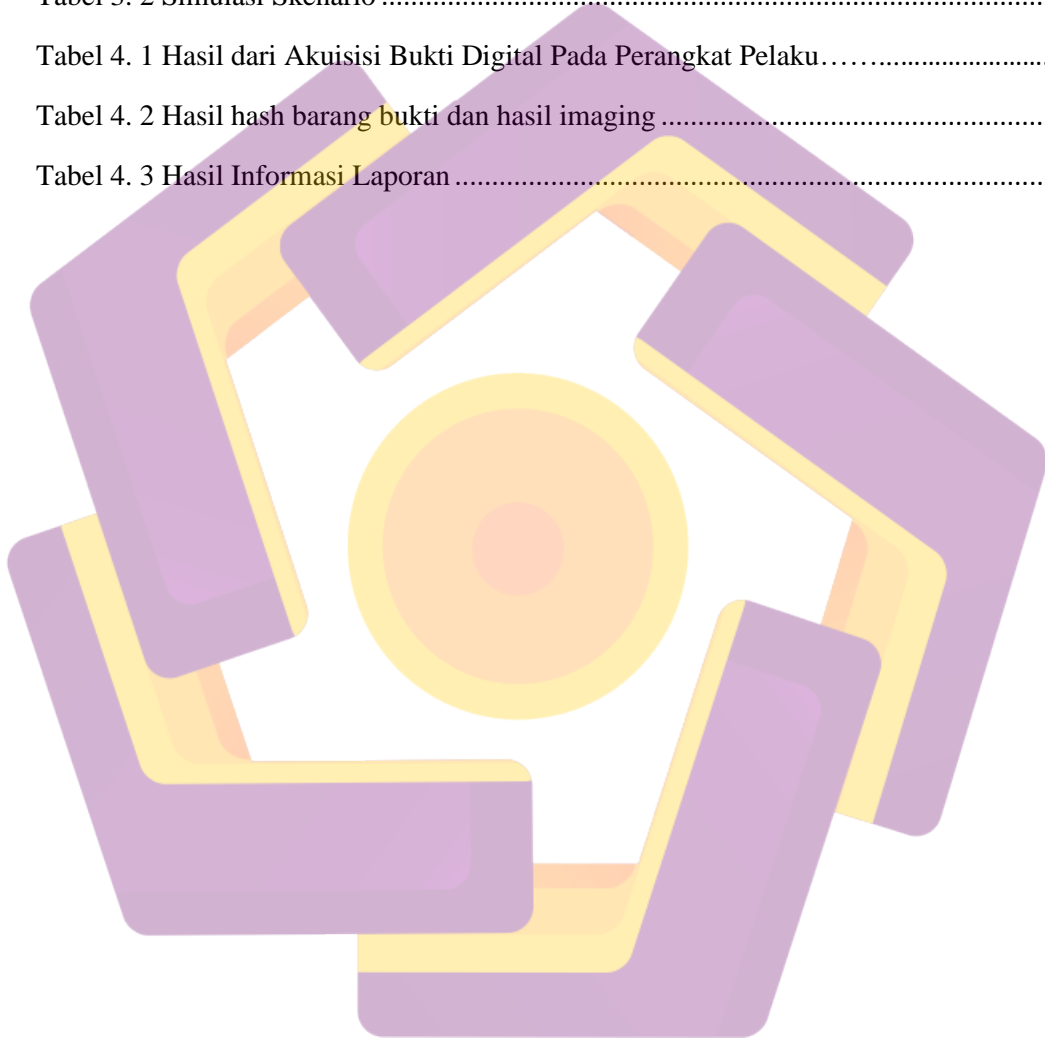
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	v
HALAMAN MOTO .....	vi
HALAMAN PERSEMBAHAN .....	vii
KATA PENGANTAR .....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR .....	xv
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	1
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA.....	4
2.1 Tinjauan Pusataka.....	4
2.2 Forensik Digital.....	7
2.3 Bukti Digital.....	7
2.4 National Institute of Justice (NIJ) .....	8
2.5 Live Forensics .....	8
2.6 Instant Messaging.....	8
2.7 Cyberterrorism.....	9
2.8 Telegram.....	9
2.9 FTK Imager .....	9
2.10 MD5.....	9

2.11	DD .....	10
2.12	HxD .....	10
2.13	Browser Google Chrome .....	10
2.14	Tor Browser .....	10
2.15	Firefox Mozilla .....	10
2.16	Mode Incognito .....	11
<b>BAB III METODE PENELITIAN .....</b>		<b>12</b>
3.1	Gambaran Umum Penelitian .....	12
3.2	Metode Penelitian .....	12
3.2.1	Identification .....	13
3.2.2	Collection .....	13
3.2.3	Examination .....	13
3.2.4	Analysis .....	13
3.2.5	Reporting .....	13
3.3	Alat dan Bahan Penelitian .....	14
3.4	Tahapan Persiapan Penelitian .....	15
3.5	Skenario Kasus .....	15
3.5.1	Eksperimen Pertama .....	16
3.5.2	Eksperimen Kedua .....	17
3.5.3	Eksperimen Ketiga .....	18
3.5.4	Eksperimen Keempat .....	18
3.5.5	Eksperimen Kelima .....	19
3.6	Alur Penelitian .....	19
3.7	Teknik Analisa .....	20
3.7.1	Teknik String Filtering .....	20
<b>BAB IV PEMBAHASAN .....</b>		<b>22</b>
4.1	Persiapan Sistem .....	22
4.1.1	Instalasi Tool Akuisisi pada Perangkat Pelaku .....	22
4.1.2	Instalasi Tools pada Perangkat Investigator (Peneliti) .....	24
4.1.2.1	Proses Instalasi tools DD .....	25
4.1.2.2	Proses Instalasi HxD Editor .....	25
4.2	Implementasi Skenario .....	27
4.2.1	Skenario (Browser Tor) .....	27

4.2.2	Skenario (Browser Chrome) .....	28
4.2.2.1	Chrome mode normal .....	28
4.2.2.2	Chrome mode incognito .....	28
4.2.3	Skenario (Browser Firefox) .....	29
4.2.3.1	Chrome mode normal .....	29
4.2.3.1	Chrome mode incognito .....	29
4.3	Identifikasi .....	30
4.4	Collection .....	30
4.4.1	Imaging .....	34
4.4.2	Validasi Kecocokan Hash .....	36
4.5	Examination dan Analysis .....	38
4.5.1	Analisa Skenario (Browser Tor) .....	38
4.5.1.1	Analisa Skenario Browser Tor Normal .....	38
4.5.2	Analisa Skenario (Browser Chrome) .....	39
4.5.2.1	Analisa Skenario Browser Chrome Normal .....	40
4.5.2.2	Analisa Skenario Browser Chrome Incognito .....	40
4.5.2	Analisa Skenario (Browser Firefox) .....	41
4.5.3.1	Analisa Skenario Browser Firefox Normal .....	41
4.5.3.2	Analisa Skenario Browser Firefox Incognito .....	42
4.6	Reporting .....	42
<b>BAB IV PENUTUP</b> .....		<b>45</b>
5.1	Kesimpulan .....	45
5.2	Saran .....	46
<b>DAFTAR PUSTAKA</b> .....		<b>48</b>

## DAFTAR TABEL

Tabel 2. 1 Tabel Tinjauan Pustaka.....	5
Tabel 3. 1 Alat dan bahan penelitian .....	14
Tabel 3. 2 Simulasi Skenario .....	16
Tabel 4. 1 Hasil dari Akuisisi Bukti Digital Pada Perangkat Pelaku.....	32
Tabel 4. 2 Hasil hash barang bukti dan hasil imaging .....	37
Tabel 4. 3 Hasil Informasi Laporan .....	43



## DAFTAR GAMBAR

Gambar 3. 1 Tahapan metode National Institute of justice.....	12
Gambar 3. 2 Tahapan Persiapan Penelitian .....	15
Gambar 3. 3 Skenario chat pada browser Tor.....	17
Gambar 3. 4 Skenario chat pada browser Chrome normal .....	17
Gambar 3. 5 Skenario chat pada browser Chrome incognito.....	18
Gambar 3. 6 Skenario chat pada browser Firefox normal .....	18
Gambar 3. 7 Skenario chat pada browser Firefox incognito.....	19
Gambar 3. 8 Alur Penelitian .....	20
Gambar 3. 9 Proses Analisa String Filtering .....	21
Gambar 4. 1 Proses pertama install FTK Imager.....	22
Gambar 4. 2 Menu install persetujuan license .....	23
Gambar 4. 3 Tool FTK Imager di dalam laptop pelaku.....	23
Gambar 4. 4 Proses terakhir install .....	24
Gambar 4. 5 Tool FTK Imager di dalam laptop pelaku.....	24
Gambar 4. 6 Tampilan DD.....	25
Gambar 4. 7 Tampilan awal instal HxD .....	25
Gambar 4. 8 Proses terakhir install HxD .....	26
Gambar 4. 9 Tampilan tool HxD Editor .....	26
Gambar 4. 10 Skenario a1 Tor mode normal.....	27
Gambar 4. 11 Skenario b1 Chrome mode normal .....	28
Gambar 4. 12 Skenario b2 Chrome mode incognito.....	28
Gambar 4. 13 Skenario c1 Firefox mode normal.....	29
Gambar 4. 14 Skenario c1 Firefox mode incognito .....	30
Gambar 4. 15 Proses akuisisi Pada memory ram.....	31
Gambar 4. 16 Pengaturan Output Nama dan Path Pada Akuisisi Memory Ram .....	31
Gambar 4. 17 Proses akuisisi ram saat sedang berjalan.....	32



Gambar 4. 18 Proses Imaging File Skenario a1 (Tor) .....	34
Gambar 4. 19 Proses Imaging File Skenario b1 (Chrome normal).....	35
Gambar 4. 20 Proses Imaging File Skenario b2 (Chrome incognito).....	35
Gambar 4. 21 Proses Imaging File Skenario c1 (Firefox normal) .....	35
Gambar 4. 22 Proses Imaging File Skenario c2 (Firefox incognito) .....	35
Gambar 4. 23 Salah satu hasil duplicate dari proses tool DD.....	35
Gambar 4. 24 Output Nilai Hash dari Hasil Akuisisi Skenario a1.....	36
Gambar 4. 25 Output Nilai Hash dari Hasil Akuisisi Skenario b1 .....	36
Gambar 4. 26 Output Nilai Hash dari Hasil Akuisisi Skenario b2 .....	36
Gambar 4. 27 Output Nilai Hash dari Hasil Akuisisi Skenario c1.....	37
Gambar 4. 28 Output Nilai Hash dari Hasil Akuisisi Skenario c2.....	37
Gambar 4. 29 Bukti chat dari analisa pada web Browser Tor (Normal).....	39
Gambar 4. 30 Bukti chat dari analisa pada web Browser Chrome (Normal) .....	40
Gambar 4. 31 Bukti chat dari analisa pada web Browser Chrome (Incognito) .....	40
Gambar 4. 32 Bukti chat dari analisa pada web Browser Firefox (Normal).....	41
Gambar 4. 33 Bukti chat dari analisa pada web Browser Firefox (Incognito) .....	42

## INTISARI

Saat ini *tor network* melalui media Tor Browser-nya menjadi akses dan sarana pelaku *cybercrime* dalam melakukan aktivitas ilegal di *deep web*. Tor diambil dari singkatan kata “*The Onion Router*” yang merupakan sebuah jaringan virtual untuk meningkatkan keamanan dan kerahasiaan data di dunia maya. Berbagai teknik digital forensik terus berkembang dalam upaya mengumpulkan bukti kritikal dalam proses mengungkap kasus *cybercrime*. Salah satu teknik nya adalah *live forensic*, dimana dengan teknik ini investigator memungkinkan mendapat data *volatile* yang tersimpan pada *memori* RAM, *page file* 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 TOR 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:** Tor, Live Forensik, Digital Forensik, Telegram, RAM.

## ABSTRACT

*Currently, the tor network through its Tor Browser media is an access and means for cybercrime perpetrators to carry out illegal activities on the deep web. Tor is taken from the abbreviation of the word "The Onion Router" which is a virtual network to increase the security and confidentiality of data in cyberspace. Various digital forensic techniques continue to develop in an effort to collect critical evidence in the process of uncovering cybercrime cases. One of the techniques is live forensics, where with this technique it is possible for investigators to obtain volatile data stored in RAM memory, pagefiles or hibernation files. Data in RAM memory is a sensitive source of digital evidence because it stores a lot of important information while the system is on (real time) such as running programs, chat logs, network connections or even cryptographic keys. The focus of this research will be to examine and analyze the evidence for potential RAM memory by studying the TOR Browser case using the NIJ methodology. The result of this research is the proof of various important artifacts from several scenarios and experiments that have been prepared so that valid digital investigations can be carried out in crime investigations.*

**Keyword:** Tor, Live Forensik, Digital Forensik, Telegram, RAM.

