ANALISA BUKTI DIGITAL TOR BROWSER MENGGUNAKAN METODE *LIVE FORENSIC*

SKRIPSI

Disusun oleh:

Lisa Naomi
17.83.0013

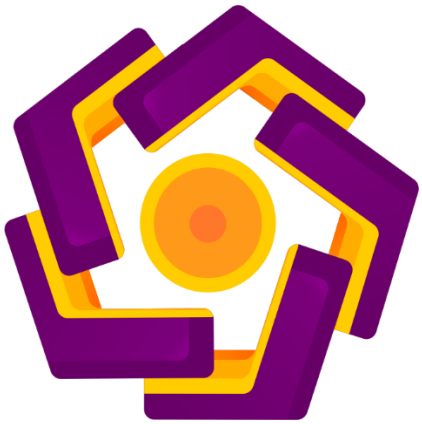
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

ANALISA BUKTI DIGITAL TOR BROWSER MENGGUNAKAN METODE *LIVE FORENSIC*

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Lisa Naomi
17.83.0013

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

ANALISA BUKTI DIGITAL TOR BROWSER MENGGUNAKAN METODE *LIVE FORENSIC*

yang dipersiapkan dan disusun oleh

Lisa Naomi

17.83.0013

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 juni 2021

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISA BUKTI DIGITAL TOR BROWSER MENGGUNAKAN METODE *LIVE FORENSIC*

yang dipersiapkan dan disusun oleh

Lisa Naomi

17.83.0013

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Juni 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Joko Dwi Santoso, M.Kom **NIK. 190302181**	_____
Erni Seniwati, S.Kom, M.Cs **NIK. 190302231**	_____
Andriyan Dwi Putra, M.Kom **NIK. 190302270**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 juni 2021

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Lisa Naomi
NIM : 17.83.0013

Menyatakan bahwa Skripsi dengan judul berikut:

Analisa Bukti Digital Tor Browser Menggunakan Metode *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, 22 Juni 2021

Yang Menyatakan,

Lisa Naomi

HALAMAN MOTTO

“ Usaha dan keberanian tidak cukup tanpa tujuan dan arah perencanaan”
(Jhon F. Kennedy)

“Bermimpilah seakan kau akan hidup selamanya. Hiduplah seakan kau akan mati hari ini”
(James Dean)

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. Kedua orang tua, Bapak Purnanto dan Ibu Parsinah yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Joko Dwi Santoso, M.kom. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada kakak saya Yayah yang selalu memberikan semangat dan dukungan.
4. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

KATA PENGANTAR

Puji dan syukur kami panjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisa Bukti digital Tor Browser Menggunakan Metode *Live Forensic*".

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 mamfaat 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 Santoro, M.kom. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan 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, 22 Juni 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Saat ini tor network melalui media Tor Browsernya menjadi akses dan sarana pelaku cybercrime dalam melakukan aktivitas ilegal di deep web. 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 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.

Fokus penelitian ini akan mengevaluasi dan menganalisis bukti potensial memori ram dengan studi kasus TOR Browser Bundle menggunakan metode National Institute of Standards Technology (NIST). 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.

Mekanisme atau metode live forensics yang digunakan untuk mendapatkan bukti digital ada 4 (empat) proses yang efektif, yaitu akuisisi, eksaminasi, analisis, dan laporan. Skenario aktifitas browsing pada penelitian terbatas pada pencarian search engine, pengiriman email, mengunjungi website dan mendownload gambar. Berdasarkan teknik analisa live forensic dengan barang bukti memori ram, hasil akhir yang diperoleh peneliti mampu membuktikan scenario aktifitas-tersebut.

Kata kunci: Live Forensic, TOR Browser, Anti Forensic

ABSTRACT

Currently, the Tor network has access to many cybercriminals and terrorists doing illegal activities on the dark web. For this reason, various digital forensic techniques continue to evolve to gather important evidence in investigating cybercrime cases effectively. One method is live forensic, which allows investigators to obtain volatile data stored in random access memory, pagefile, or hibernation files. Data on memory ram becomes a valuable source of forensic evidence because it stores a lot of critical information when the system is on (real-time activity) such as running programs, chat logs, network connections, user password, or cryptographic keys.

This research focuses on evaluating and analyzing potential evidence of memory ram image with the TOR Browser Bundle case study using the National Institute of Standards Technology (NIST) method. The results of this research prove the findings of various important artifacts from scenario experiments that become valid digital evidence in the process of uncovering the cybercrime cases.

There are 4 (four) effective processes or live forensics methods used to obtain digital evidence, namely acquisition, examination, analysis, and reports. The scenario of browsing activity in research is limited to search engine searches, sending e-mails, visiting websites and downloading images. Based on the live forensic analysis technique with ram memory evidence, the final results obtained by the researcher were able to prove the activity scenario.

Keyword: Live Forensic, TOR Browser, Anti Forensic