Analisa Live Forensik Pada *Session Portable* Browser Brave Menggunakan Metode *National Institute of Standards and Technology* (NIST)

SKRIPSI

Disusun oleh:

Edward Tansen
17.83.0060

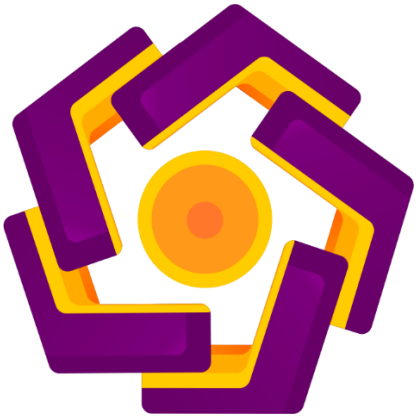
PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

Analisa Live Forensik Pada *Session* Portable Browser Brave Menggunakan Metode *National Institute of Standards and Technology* (NIST)

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:

Edward Tansen
17.83.0060

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

HALAMAN PERSETUJUAN

SKRIPSI

Analisa Live Forensik Pada *Session* Portable Browser Brave Menggunakan Metode *National Institute of Standards and Technology* (NIST)

yang dipersiapkan dan disusun oleh

Edward Tansen

17.83.0060

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Juli 2021

Dosen Pembimbing,

Dony Ariyus, M.Kom
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

Analisa Live Forensik Pada *Session* Portable Browser Brave Menggunakan Metode *National Institute of Standards and Technology* (NIST)

yang dipersiapkan dan disusun oleh

Edward Tansen

17.83.0060

Telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Juli 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Banu Santoso, S.T.,M.Eng **NIK. 190302327**	
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Dony Ariyus, M.Kom **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Juli 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Edaward Tansen
NIM : 17.83.0060

Menyatakan bahwa Skripsi dengan judul berikut:

Analisa Live Forensik Pada *Session* Portable Browser Brave Menggunakan Metode *National Institute of Standards and Technology* (NIST)

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, 27 Juli 2021

Yang Menyatakan,

Edward Tansen

HALAMAN MOTTO

"Hidup Mengalir Layaknya Air Di Sungai Amazon Yang Tenang Namun Mematikan :v"
(Edward Tansen 2021)

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 Irpan dan Ibu Rosidah yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Dony Ariyus, M.kom. Selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada Kakak Saya Rz. Ricky Satria Wiranata dan Istrinya Kiki Melita yang selalu memberikan semangat serta dukungannya.
4. Kepada sahabat Andrian, Alfat, Deris, Hardi, Setiawan, Waode, Hazri, Wildan, Lisa, Ansuri dan teman-teman lainnya yang ada disaat suka maupun duka selama masa perkuliahan saya.
5. Kepada Pak Tri Hariyanto yang telah Membangun P-Store.net karena berkat platform beliau memberikan banyak manfaat untuk saya saat masa sulit

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 *Live Forensic* Pada *Session* Portable Browser Brave Menggunakan Metode *National Institute of Standards and Technology* (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 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 Dony Ariyus, 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, 27 Juli 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Perkembangan teknik atau metode *anti forensic* terhadap penggunaan *browser* saat ini sudah memiliki berbagai macam varian mulai dari menggunakan portable *apps*, menggunakan mode *private* sampai memanipulasi *registry* pada computer. Hal ini menjadi tantangan tersendiri terhadap investigator dalam mengumpulkan bukti digital saat analisa *forensic* dilakukan, dan memaksa para investigator untuk mengimprovisasi teknik analisa yg mereka gunakan, salah satu teknik analisa *forensic* yaitu *live forensic* dimana dengan teknik ini investigator memungkinkan untuk mendapat data *volatile* yang tersimpan pada *ram*, *pagefile* ataupun *hibernation file*. Dengan teknik ini investigator dapat mengimprovisasi teknik analisanya lebih jauh untuk mendapatkan bukti terhadap data pada memori *ram* yang 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*.

Focus pada penelitian ini yaitu mengevaluasi dan menganalisis bukti yang potensial dari memori *ram* dengan studi kasus Portable Brave *Browser* dengan connectivitas tor menggunakan teknik *live forensic* dan metode *National Institute of Standards Technology* (NIST). Hasil dari penelitian ini adalah pembuktian terhadap termuan berbagai artefak penting dari skenario yang telah di buat sehingga dapat menjadi bukti digital yang valid dalam proses mengungkap tindak kejahatan.

Metode *live forensics* yang digunakan pada penelitian ini ada 4 (empat) proses sesuai metode NIST, yaitu akuisisi, eksaminasi, analisis, dan laporan. Skenario yang di siapkan peneliti berupa aktifitas *browsing* pada search engine, kunjungan website, dan *chatting* menggunakan platform whatsapp web. Berdasarkan teknik analisa *live forensic* dengan barang bukti memori ram, hasil akhir yang diperoleh peneliti mampu membuktikan scenario aktifitas tersebut.

Kata Kunci : Forensics, Digital Forensics, RAM, Brave Browser, NIST

ABSTRACT

The development of anti-forensic techniques or methods for using browsers currently has various variants ranging from using portable applications, using private mode to manipulating the registry on the computer. This poses a challenge for investigators to collect digital evidence when forensic analysis is carried out, and forces investigators to improvise the analytical techniques they use, one of the forensic analysis techniques is live forensics where with this technique investigators allow investigators to obtain volatile data stored in ram , pagefile or hibernation file. With this technique investigators can improve their analysis techniques further to obtain evidence against data in RAM memory which 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 a cryptographic key.

The focus of this research is to analyze the potential evidence of ram memory by studying the case of Portable Brave Browser with connectivity using direct forensic techniques with the National Institute of Standards Technology (NIST) method. The result of this research is proof of various important artifacts from the scenarios that have been made so that they can become valid digital evidence in uncovering evidence of crime.

The live forensic method used in this study to obtain digital evidence has 4 (four) processes according to the NIST method, namely acquisition, examination, analysis, and report. The scenarios visited by the researchers were in the form of browsing search engines, websites, and chatting using the WhatsApp web platform. Based on the live forensic analysis technique with ram memory evidence, the final results obtained by the researchers were able to prove the scenario of the activity.

Keyword: Forensics, Digital Forensics, RAM, Brave Browser, NIST