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

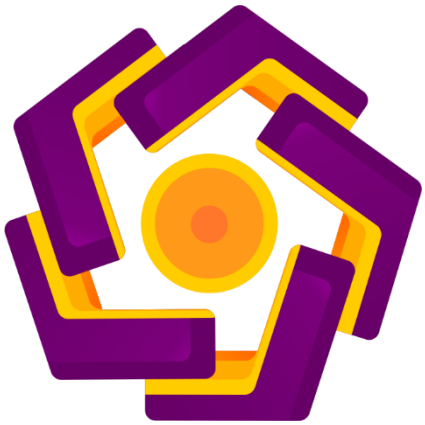
2022

INVESTIGASI ANTI FORENSIC KASUS CYBERTERRORISM PADA TOR BROWSER DAN INCOGNITO MODE MENGGUNAKAN 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 MENGGUNAKAN 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 Incogniton 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 brsyukur dalam setiap proses.

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

(Mahatma Gandhi)

HALAMAN PERSEMBAHAN

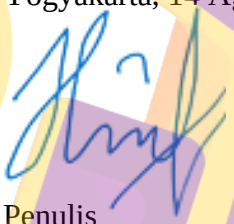
Alhamdulillah, segala puji bagi Allah SWT, kita memuji-Nya, dan meminta pertolongan, pengampunan serta petunjuk kepada-Nya. Kita berlindung kepada Allah dari kejahatan diri kita dan keburukan amal kita. Barang siapa yang mendapat petunjuk dari Allah, maka tidak akan ada yang menyesatkannya dan barang 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 lancer 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

DAFTAR TABEL

DAFTAR GAMBAR

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.