



Analisis Anti Forensik pada Portable Web Browser Mode Private Menggunakan Metode Live Forensik

Tri Rochmadi

14917161

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2017

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, April, 2017

Tri Rochmadi, S.Kom



Lembar Pengesahan Pembimbing

**Analisis Anti Forensik pada Portable Web Browser Mode Private
Menggunakan Metode Live Forensik**

Nama: Tri Rochmadi

NIM: 14917161

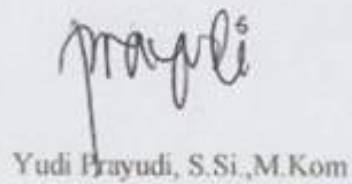
Yogyakarta, April, 2017

Pembimbing I

Pembimbing II



Dr. Imam Riadi, M.Kom



Yudi Prayudi, S.Si., M.Kom

Lembar Pengesahan Penguji

**Analisis Anti Forensik pada Portable Web Browser Mode Private
Menggunakan Metode Live Forensik**

Nama: Tri Rochmadi

NIM: 14917161

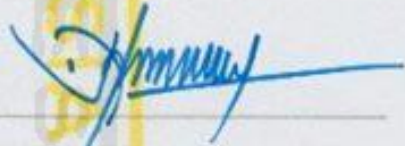
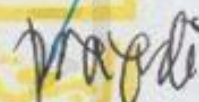
Yogyakarta, April, 2017

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.Si., M.Kom
Anggota I

Dr. Bambang Sugiantoro
Anggota II



Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia



Dr. R. Teduh Dirgahayu, ST, M.Sc

Abstrak

Hampir semua aspek kehidupan sudah menggunakan internet, untuk dapat mengakses Internet salah satunya menggunakan web browser. Untuk keamanan, beberapa fitur web browser mengembangkan mode private. Sayangnya dari fitur ini, oleh beberapa oknum digunakan untuk kegiatan kriminal dengan proses anti-forensik. Proses Anti-forensik tersebut seperti dengan menggunakan web browser portabel dan menghapus registry. Motivasi penggunaan anti-forensik adalah untuk meminimalkan atau menghambat penemuan bukti digital dalam kasus kejahatan. Sehingga, menjadi hambatan bagi penyidik untuk mengungkap kejahatan internet yang telah dilakukan. Makalah ini mengusulkan sebuah kerangka tahapan untuk analisis web browser pada mode private dan anti-forensik. Tujuan dari penelitian ini adalah untuk memberikan solusi dalam investigasi forensik secara efektif dan efisien menggunakan metode live forensik. Penelitian ini menggunakan live forensik untuk mendapatkan informasi lebih detail yang ada di komputer dengan kondisi masih menyala. Jadi metode ini cocok diterapkan untuk penanganan insiden yang lebih cepat dan memungkinkan mendapatkan data dalam RAM.

Kata kunci

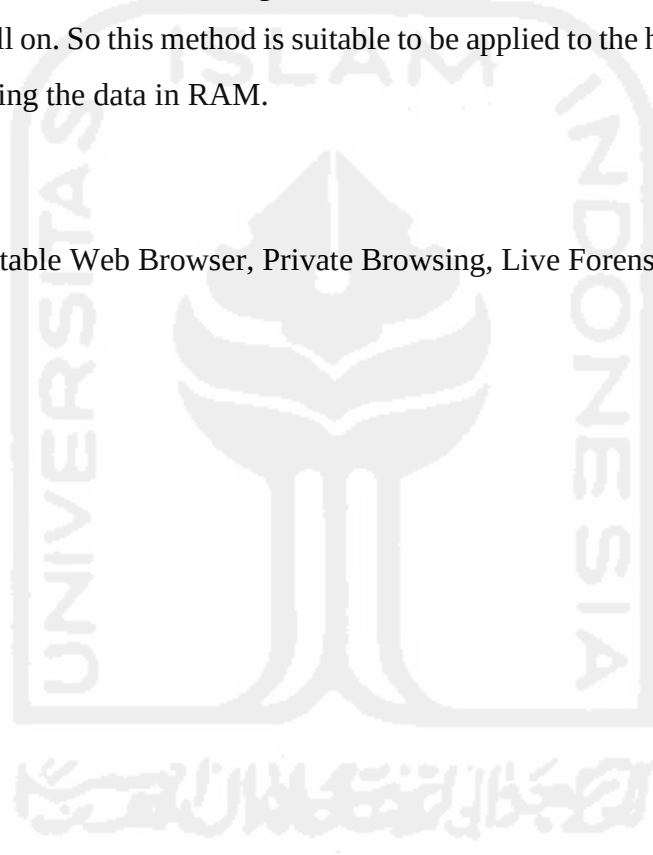
Browser Forensics, Portable Web Browser, Private Browsing, Live Forensics, Anti Forensics

Abstract

Almost all aspects of life already use the internet, to be able to access the Internet one of them using a web browser. For security, some web browser features to develop private mode. Unfortunately, from this feature, by some unscrupulous used for criminal activities by the anti-forensics. An anti-forensics process such as by using a portable web browser and delete registry. Motivation use of anti-forensics is to minimize or inhibit the discovery of digital evidence in criminal cases. So that, be an obstacle for investigators to uncover internet crimes that have been carried out. This paper proposes a framework for analysis phases of the web browser in private mode and anti-forensics. The purpose of this study is to provide solutions in forensic investigations effectively and efficiently using live forensics. This study uses a live forensics to get more detailed 3 evidence information on the computer with the condition is still on. So this method is suitable to be applied to the handling of incidents more quickly and allows getting the data in RAM.

Keywords

Browser Forensics, Portable Web Browser, Private Browsing, Live Forensics, Anti Forensics.



Pernyataan keaslian tulisan

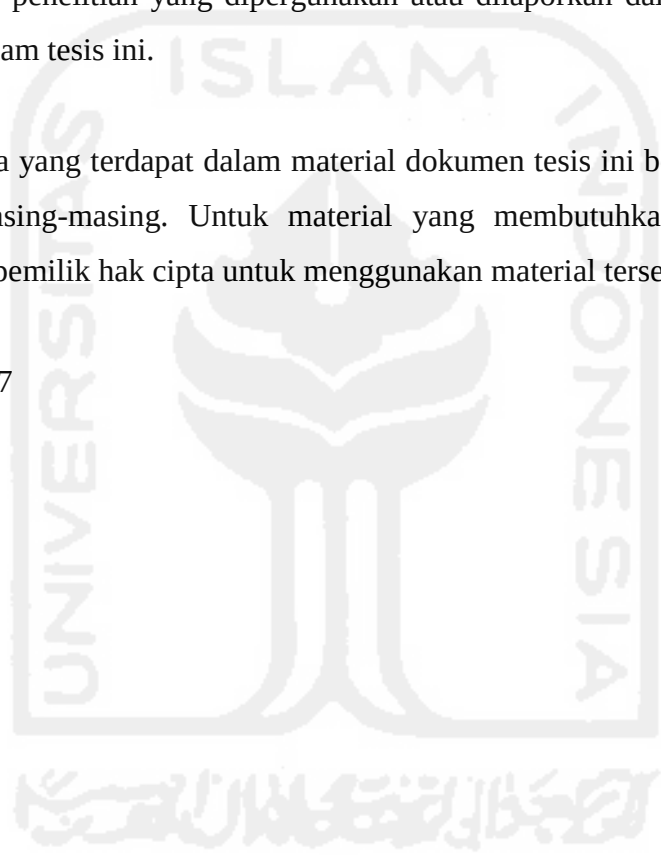
Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, April, 2017

Tri Rochmadi, S.Kom



Publikasi selama masa studi

Publikasi yang menjadi bagian dari tesis

Dear Tri Rochmadi, Imam Riadi, Yudi Prayudi,

The board of International Journal of Computer Applications is pleased to inform that your manuscript is published in **IJCA April 2017 Edition** with effect from **April 18, 2017**.

Manuscript Title : Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser

Digital Library URI : <http://www.ijcaonline.org/archives/volume164/number8/27505-2017913717>

ISBN : 973-93-80896-12-8

T. Rochmadi, I. Riadi, and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. J. Comput. Appl.*, vol. 164, no. 8, pp. 31–37, 2017.

Publikasi tersebut menjadi bagian dari tesis ini dari awal sampai akhir.

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Tri Rochmadi	Menulis <i>paper</i> (60%)
Imam Riadi	Menulis dan mengedit <i>paper</i> (20%)
Yudi Prayudi	Menulis dan mengedit <i>paper</i> (20%)

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain.



Halaman Persembahan

إِنَّا نَحْنُ نُحْيِي الْمَوْتَىٰ وَنَكْتُبُ مَا قَدَّمُوا وَءِثَارَهُمْ وَكُلَّ شَيْءٍ أَحْصَيْنَاهُ فِي إِمَامٍ مُّبِينٍ

Sesungguhnya Kami menghidupkan orang-orang yang mati dan Kami menuliskan apa yang telah mereka kerjakan dan bekas-bekas yang mereka tinggalkan. Dan segala sesuatu Kami kumpulkan dalam Kitab induk yang nyata (Lauh Mahfuzh). (Q.S Yaasin : 12)

PERSEMBAHAN

Alhamdulillah, atas rahmat dan hidayah-Nya, saya dapat menyelesaikan tesis ini dengan baik.

Karya sederhana ini ku persembahkan untuk:

- Alm Bapak Satimin dan Ibu Poniym, yang telah mendukung, memberi motivasi dalam segala hal serta memberikan kasih sayang yang teramat besar yang tak mungkin bisa terbalas dengan apapun.
- Bapak H. Ir. Slamet Prayitno, M.T dan Ibu Hj. Ir. Endang Rismunarsi, M.T yang senantiasa memberikan support, baik moril maupun materiil hingga terselesaikannya tesis ini dengan hasil yang baik.
- Istriku yang tercinta dhek Rita Mulyandari, S.T yang selalu menemani dan memberi support lahir batin dalam mengerjakan tesis ini. Kata-kata penyemangat dan kerelaannya dalam membantu suami dalam meraih cita-citanya.
- Kakak-kakak dan Adik-adikku, Mas Fendy-Mbak Mulyani, Mas Akhir-Mbak Umi, Dhek Bakti, Dhek Erni, dan Dhek Rohmat.
- Teman-teman Teknik Informatika Universitas Islam Indonesia.

Kata Pengantar

Alhamdulillah, segala puji syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan ridho-NYA, sehingga tesis dengan judul “Analisis Anti Forensik pada Portable Web Browser Mode Private Menggunakan Metode Live Forensik” ini dapat diselesaikan.

Rasa syukur dan terima kasih bahwa beberapa kendala dan hambatan yang dijumpai dalam penulisan tesis ini telah dapat diatasi baik, disamping itu penulis menyadari bahwa penulisan tesis ini masih jauh dari sempurna dan masih banyak kekurangan lainnya, maka dari itu saran dan kritik yang membangun dari semua pihak akan menjadi masukan yang sangat diharapkan.

Tesis ini disusun untuk memenuhi salah satu persyaratan memperoleh gelar Magister Komputer (M.Kom) dalam bidang keahlian Forensika Digital pada program studi Teknik Informatika Universitas Islam Indonesia.

Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa hormat dan menghaturkan terima kasih yang sebesar-besarnya, kepada :

1. Ayahanda (Alm) Satimin, Ibunda Poniyeem, Ayah Mertua Ir. Slamet Prayitno, M.T, dan Ibu Mertua Ir. Endang Rismunarsi, M.T yang senantiasa memberi dorongan lahir dan batin hingga terselesaikannya penyusunan tesis ini.
2. Istriku Rita mulyandari, S.T yang senantiasa memberikan motivasi, perhatian, doa dan kesabaran menemani menyusun Tesis ini hingga terselesaikan.
3. Segenap keluarga besar (Alm) Satimin dan Ir. Slamet Prayitno, M.T atas segala dukungan moril dan materiil serta semangat yang telah diberikan untuk menyelesaikan Tesis ini.
4. Dr. R. Teduh Dirgahayu, ST.,M.Sc, sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri atas fasilitas dan sarana prasarana dalam melaksanakan kegiatan perkuliahan dari awal sampai akhir.
5. Dr. Imam Riadi, M.Kom dan Yudi Prayudi, S.Si., M.Kom, sebagai Dosen Pembimbing I dan II yang banyak memberikan ide, saran, bimbingan dan dorongan bagi penulis untuk terus maju dalam mengatasi hambatan yang ada serta memberikan masukan dan motivasi yang memacu penulis dalam menyusun tesis ini.
6. Dr. Bambang Sugiantoro, sebagai Dosen Penguji yang memberikan saran dan masukan pada saat sidang progress tesis.
7. Teman-teman Magister Teknik Informatika UII umumnya dan angkatan X khususnya yang memberikan dorongan semangat bagi penulis.
8. Semua teman yang tidak bisa kami sebutkan satu per satu, terima kasih atas semua dorongannya.

Penulis menyadari bahwa masih banyak kekurangan yang terdapat dalam tulisan ini, namun dalam segala keterbatasannya semoga tulisan ini dapat bermanfaat. Akhir kata, penulis mengharapkan kritik dan saran agar Tesis ini lebih sempurna serta sebagai masukan bagi penulis untuk penelitian dan penulisan karya ilmiah di masa yang akan datang.

Sleman, 26 April 2017

Tri Rochmadi

