Metode Offline Forensic Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux

Wisnu Sanjaya, S.Kom
12917206

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Teknik Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2020

Lembar Pengesahan Pembimbing

Metode Offline Forensic Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux

Wisnu Sanjaya, S.Kom
12917206

Yogyakarta, Mei, 2020

Pembimbing

Dr. Bambang Sugiantoro

Lembar Pengesahan Penguji

Metode Offline Forensic Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux

Wisnu Sanjaya, S.Kom

12917206

Yogyakarta, Mei, 2020

Tim Penguji,

Dr. Imam Riadi, M.Kom.
Ketua

Dr. Yudi Prayudi, M.Kom.
Anggota I

Dr. Bambang Sugiantoro, M.T
Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Izzati Muhimmah, ST., M.Sc., Ph.D

NIK.085240102

Abstrak

Metode Offline Forensic Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux

Perkembangan dunia IT yang begitu pesat telah meliputi seluruh aspek kehidupan dan diantara produk teknologi IT adalah dibuatnya Sistem Operasi dan aplikasi Web browser. Privasi dalam pemanfaatan IT di jaman yang serba terbuka sekarang sangat diharapkan, oleh karena itu sekarang banyak dikembangkan Sistem Operasi dan aplikasi Web browser yang mempunyai fasilitas untuk melindungi privasi pengguna. Linux dan TOR Browser merupakan paduan yang banyak digunakan dalam bidang security, akan tetapi sayangnya banyak disalah gunakan oleh oknum dalam sebuah tindak kriminal. Motivasi penggunaan keduanya adalah untuk menghilangkan atau meminimalkan jejak digital dari aktivitas browsing sehingga akan mempersulit pencarian barang bukti digital dalam sebuah tindak kejahatan. Penelitian ini mengusulkan kerangka tahapan untuk analisis TOR Browser di Sistem Operasi linux yang bertujuan untuk memberikan solusi dalam investigasi forensik menggunakan metode offline forensic. Penggunaan metode offline forensic untuk memperoleh informasi yang detail dari sebuah bukti digital pada computer dalam kondisi tidak menyala.

Kata kunci

Browser Forensics, TOR, Linux,Offline Forensic

Abstract

Offline Forensic Method For TOR Browser Digital Artefacs Analisys On Linux Operating System

The rapid development of the IT world has covered all aspects of life and among IT technology products is the creation of Operating Systems and Web browser applications. Privacy in the use of IT in the open era is now highly expected, therefore now widely developed Operating Systems and Web browser applications that have facilities to protect user privacy. Linux and TOR Browser is a combination that is widely used in the field of security, but unfortunately many are misused by the person in a crime. The motivation to use both is to eliminate or minimize the digital footprint of the browsing activity so that it will complicate the search of digital evidence in a crime. This research proposes a framework of stages for TOR Browser analysis in Linux Operating System which aims to provide solution in forensic investigation using offline forensic method. The use of offline forensic methods to obtain detailed information from a digital proof on a computer in a off state.

Keywords

Browser Forensics, TOR, Linux,Offline Forensic

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 ciptayang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Mei, 2020

Wisnu Sanjaya, S.Kom

DaftarPublikasi

Publikasi selama masa studi

Amelia, R., Bahri, S., & Sanjaya, W. (2018). PERANCANGAN APLIKASI E-VOTE BERBASIS MOBILE ANDROID PADA PEMILIHAN KETUA RT NGESTIHARJO RT 02/15 SISWODIPURAN BOYOLALI. *JITU : Journal Informatic Technology And Communication*, *2*(3), 1 - 9. Retrieved from https://ejournal.uby.ac.id/index.php/jitu/article/view/18

Sanjaya, W., Sugiantoro, B., & Prayudi, Y. (2020). Metode Offline Forensik Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux. *JITU : Journal Informatic Technology And Communication*, *4*(2), 41-51. https://doi.org/10.36596/jitu.v4i2.345

Publikasi yang menjadi bagian dari tesis

Sanjaya, W., Sugiantoro, B., & Prayudi, Y. (2020). Metode Offline Forensik Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux. *JITU : Journal Informatic Technology And Communication*, *4*(2), 41-51. https://doi.org/10.36596/jitu.v4i2.345

Publikasi berikut menjadi bagian tesis dari awal hingga akhir

Penulis Wisnu Sanjaya et al. (2020).

Kontributor	**Jenis Kontribusi**
Wisnu Sanjaya	Menulis *paper* (60%)
Bambang Sugiantoro	Menulis dan mengedit *paper* (20%)
Yudi Prayudi	Menulis dan mengedit *paper* (20%)

Halaman Kontribusi

Tidak ada kontribusi dari pihak lain

Halaman Persembahan

Alhamdulillah, atas rahmat dan hidayah Allah S.W.T, saya dapat menyelesaikan tesis ini dengan baik.

Karya sederhana ini aku persembahkan untuk:

1. Alm Bapak Uskadi dan Ibu Sri Mulyani, yang telah mendukung, memberi motivasi dalam segala hal serta memberikan kasih sayang yang teramat besar yang tak mungkin bisa terbalas dengan apapun.
2. Bapak H. Rahmat Suyatno dan Ibu Hj. Sugiyem yang senantiasa memberikan support, baik moril maupun materiil hingga terselesaikannya tesis ini dengan hasil yang baik.
3. Istriku yang tercinta Nur Handayani, S.Pd yang selalu menemani dan memberi support lahir batin dalam mengerjakan tesis ini. Kata-kata penyemangat dan kerelaannya dalam membantu suami dalam meraih cita-citanya.
4. Keluarga Besar Bapak Uskadi dan Bapak H. Rahmat Suyatno
5. Teman-teman Teknik Informatika Universitas Islam Indonesia.

Kata Pengantar

بِسْمِ اللهِ الرَّحْمنِ الرَّحِيمِ

Alhamdulillah, segala puji syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan ridho-Nya, sehingga tesis dengan judul "Metode Offline Forensic Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux " 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) Uskadi, Ibunda Sri Mulyani, Ayah Mertua H. Rahmat Suyatno dan Ibu Mertua Hj. Sugiyem yang senantiasa memberi dorongan lahir dan batin hingga terselesaikannya penyusunan tesis ini.
2. Istriku Nur Handayani, S.Pd yang senantiasa memberikan motivasi, perhatian, doa dan kesabaran menemani menyusun Tesis ini hingga terselesaikan.
3. Ibu Izzati Muhimmah, ST.,M.Sc.,Ph.D sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri atas fasilitas dan sarana prasarana dalam melaksanakan kegiatan perkuliahan dari awal sampai akhir.
4. Dr. Bambang Sugiantoro, M.T dan Dr. Yudi Prayudi, 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 motivas yang memacu penulis dalam menyusun tesis ini.
5. Dr. Imam Riadi, M.Kom, sebagai Dosen Penguji yang memberikan saran dan masukan pada saat sidang progress tesis.

6. Teman-teman Magister Teknik Informatika UII yang memberikan dorongan semangat bagi penulis.

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.

Daftar Isi

Daftar Tabel

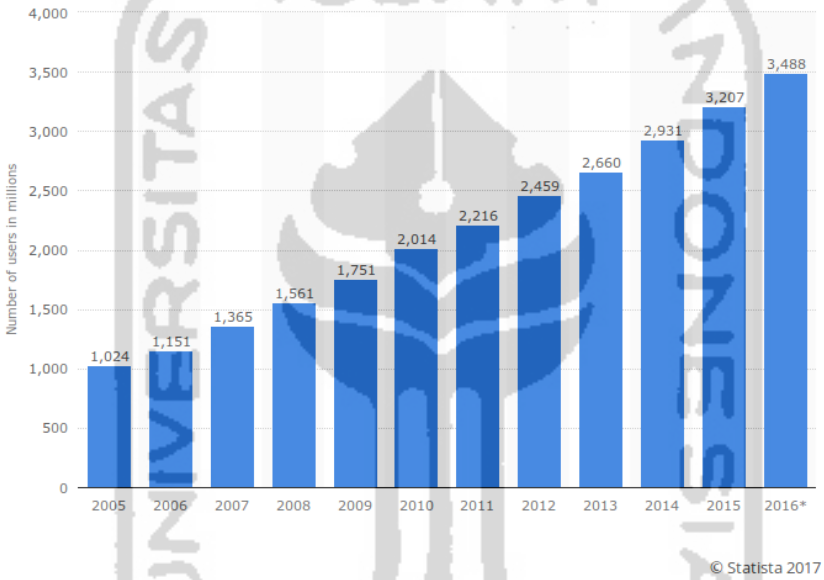
Daftar Gambar

BAB 1

Pendahuluan

1.1 Latar Belakang

Ditemukanya internet berdampak terhadap kehidupan manusia yg cukup drastis, dimana internet digunakan untuk menghubungkan antar individu yg berbeda secara geografi dalam hampir seluruh aktivitas keseharian. Web browser merupakan program yang diinstal pada sistem operasi untuk yang digunakan untuk mengakses, melihat, dan berkomunikasi dengan Situs web, pengguna lain serta berkas lainnya yang berada dalam server web.



Gambar 1.1 Statistik Pengguna Internet

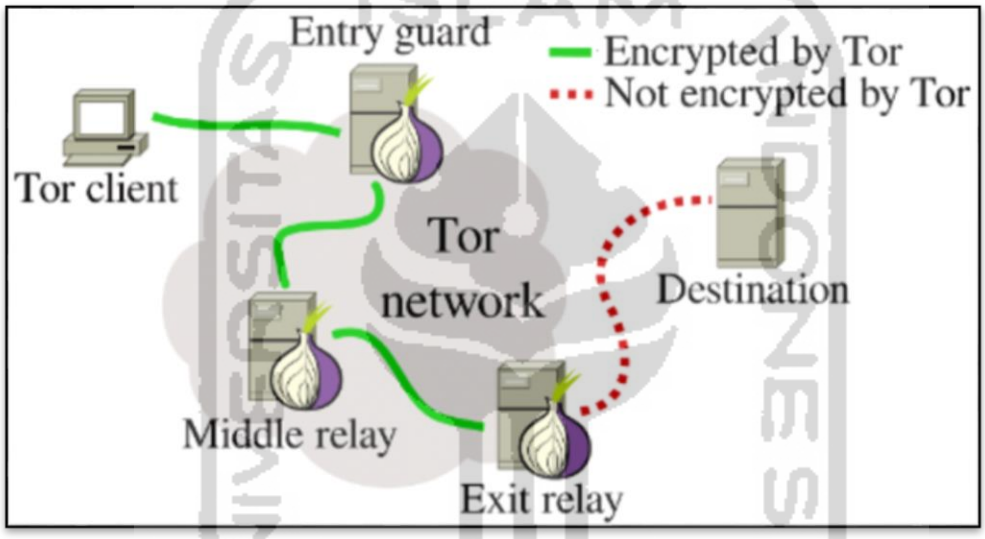
(Sumber: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/)

Web browser merupakan sebuah aplikasi software penting yang biasa digunakan untuk mengakses internet baik untuk mencari informasi, bersosial media dan bertransaksi internet (Oh, Lee, & Lee, 2011). Web Browser adalah sebuah aplikasi software yang paling banyak digunakan oleh pengguna komputer atau laptop (Chivers, 2013).

Web browser memiliki kemampuan untuk menyimpan aktivitas browsing dari sesi pengguna yang berupa informasi url yg dikunjungi, berkas dan gambar yang disimpan, pencariaan, cokie dan informasi lainya. Informasi tersebut tersimpan dalam komputer dan bisa diakses atau diambil oleh pengguna lainya. (Said, Mutawa, Awadhi, & Guimaraes, 2011).

Semakin pedulinya pengguna terhadap privasi aktivitas browsing, maka mereka menghendaki web browser mampu untuk tidak meninggalkan jejak informasi terkait aktifitas browsing sesi pengguna (Satvat, Forshaw, Hao, & Toreini, 2014)

TOR Browser adalah Web browser yang secara default sdh mempunyai kemampuan menjaga privasi, sehingga keberadaan dan identitas pengguna tidak terekpos ke internet. Perute onion dikembangkan lebih jauh oleh DARPA pada tahun 1997. Versi alpha dari TOR, yang dikembangkan oleh ilmuwan Syverson dan komputer Roger Dingledine dan Nick Mathewson dan kemudian disebut proyek Onion Routing, atau proyek TOR, diluncurkan pada tanggal 20 September 2002 (Syverson, 2005)



Gambar 1.2 Jaringan TOR

(Sumber: https://mybroadband.co.za/news/internet/165690-tor-network-what-it-is-and-how-it-works.html)

Kali Linux adalah salah satu distro linux yg dikenal cukup populer untuk kegunaan uji keamanan jaringan dan digital forensic. Kali linux memiliki kurang lebih tools uji keamanan dan mampu berjalan di beberpa arsitektur komputer (Shree Krishna Lamichhane, 2016)

1.2 Rumusan Masalah

Merujuk dari latar belakang di atas maka dalam penelitian merumuskan beberapa masalah antara lain:

1. Bagaimana karakteristik bukti digital dari keberadaan dan penggunaan TOR Browser di system operasi kali linux?

2. Bagaimana tahapan offline forensic untuk melakukan investigasi TOR Browser di system operasi kali linux?

1.3 Batasan Masalah

Dalam melaksanakan kegiatan penelitian ini, supaya penelitian akan lebih spesifik dan maksimal maka dibuat batasan masalah. Berikut batasan masalah yang terdapat pada penelitian ini :

1. Penelitian akan dilakukan dengan mensimulasikan penggunaan TOR Browser di Sistem Operasi Kali Linux, yang dijalankan diatas aplikasi virtualisasi Virtualbox dan fokus pada bahasan analisa TOR browser terutama di System Operasi Kali Linux.
2. Proses investigasi forensik menggunakan metode offline forensik, disesuaikan dengan kasus akuisisi data pada media penyimpan, sehingga diharapkan dapat mencari bukti digital yang diklaim sudah tidak ada dalam sistem computer.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang dibuat di atas maka tujuan dari penelitian ini antara lain:

1. Mengetahui karakteristik bukti digital dari penggunaan TOR browser di sistem operasi kali linux.
2. Melakukan tahapan offline forensic untuk melakukan investigasi TOR browser di sistem operasi kali linux.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari hasil penelitian ini adalah sebagai berikut :

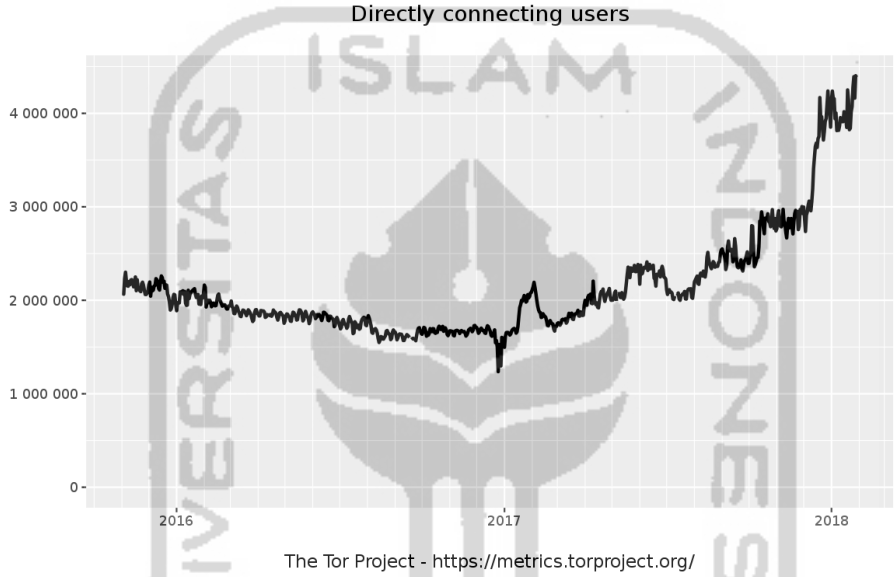
1. Pengetahuan tentang bagaimana TOR browser bekerja.
2. Memberikan pengetahuan dasar kali linux dalam dunia keamanan informasi
3. Dapat mengetahui proses untuk mendapatkan bukti digital dari TOR Browser
4. Melengkapi penelitian-peneltian sebelumnya dan mengembangkan dari saran penelitian sebelumnya tentang forensik web browser di TOR browser dan bagaimana pengumpulan barang buktinya.

BAB 2

Landasan Teori

2.1 Penelitian Terdahulu

Penelitian sejenis tentang Private browser telah banyak dilakukan, diera yang serba terbuka saat ini pengguna internet yang menginginkan privasinya terlindungi. Dari sisi aplikasi TOR Browser adalah salah satu aplikasi perambah web yang mempunyai kemampuan untuk melindungi privasi penggunanya dan cukup banyak penggunanya.



Gambar 2.1 Statistik pengguna TOR

Tabel 2.1 Literatur Review

Paper Utama	Offline Forensic	Private Browser	Kali Linux	Pengujian
(Rochmadi, 2017)		√		Pencarian bukti digital dari portable private browser metode live forensic
(Hassan & Jaber, 2017)	√			Komparasi ektrasi data metode Online dengan Offline pada layanan cloud
(Kolhe & Ahirao, 2017)	√			Analisis malware dengan

				akuisisi image menggunakan perbandingan dua buah metode
(Shree Krishna Lamichhane, 2016)			√	Penggunaan Kali Linux tools untuk uji keamanan Jaringan
(Babincev & Vuletic, 2016)			√	Pengujian Keamanan aplikasi web menggunakan Kali Linux
(Keller, 2016)		√		Pencarian jejak digital dari tor browser
(Adautin & R, 2015)	√			Metode offline diterpakan pada google portable browser private session
(Al-Khaleel, Bani-Salameh, & Al-Saleh, 2014)		√		Pencarian tor browser artefacs secara online forensic pada memory
(Mulazzani, 2014)		√		Pencarian jejak digital dari tor browser dengan metode online forensic
(Noorulla, 2014)		√		Melakukan forensik file sistem dan memori pada computer dengan hasil Bukti digital masih tersisa pada memori dan di sebagian browser bukti digital terdapat di file sistem
(Sandvik, 2013)		√	√	Menguji forensic browser pada beberapa jenis

				browser dan system operasi
Usulan Penelitian				
Solusi yang diusulkan	Mengingat Masih sangat jarangnnya penelitian Browser Forensic pada system operasi kali linux dimana distro linux tersebut sangan popular dan banyak digunakan professional dibidang security yang disana sangat dimungkinkanya penggunaan aplikasi anti forensic utk menghilangkan jejak, maka penulis berusaha meneliti Jejak digital dari browser pd system operasi kali linux dengan metode offline.			

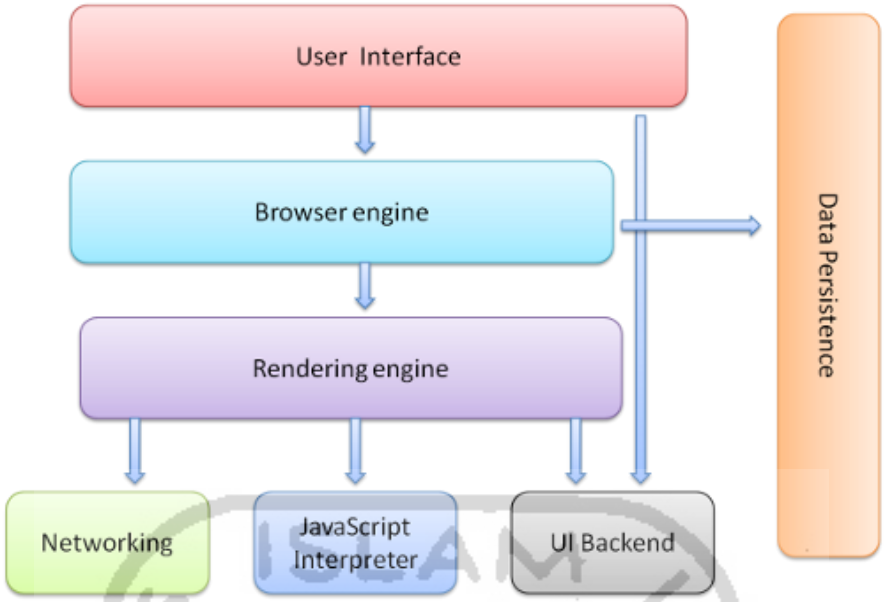
Tabel 2.2 Penelitian yang Diusulkan

Judul	Uraian Singkat Masalah Penelitian	Solusi	Hasil Yang diharapkan
Metode Offline Forensic Untuk Analisis Digital Artefacs Pada TOR Browser Di Sistem Operasi Linux	Bagaimana cara memperoleh bukti digital dari keberadaan dan aktivitas TOR Browser di system operasi Linux dalam kondisi computer off	Membuat duplikat dari barang bukti dan melakukan hashing Mengakuisisi bukti digital dengan autopsy	Memberi gambaran tahapan-tahapan akusisi dengan metode offline Memperoleh Bukti digital

2.2 Web Browser

Web browser adalah aplikasi perangkat lunak untuk mengambil, penyajian, dan melintasi sumber informasi di World Wide Web. Sebuah sumber informasi diidentifikasi dengan *Uniform Resource Identifier (URI)* dan mungkin menjadi halaman web, gambar, video, atau bagian lain dari konten (Jain 2011).

Sebuah *web browser* pada umumnya menggunakan arsitektur browsernya seperti gambar berikut ini.



Gambar 2.2 Arsitektur Web Browser (Grosskurth & Godfrey, 2005)

2.3 TOR Browser

Tor Browser adalah salah satu browser yang mampu menjaga anonimitas dan digunakan oleh mereka yang ingin terjaga privasi dan menghindari sensor saat browsing internet. Seiring waktu, TOR Browser terus dikembangan menjadi sangat baik dalam hal ini. Hal ini membuat keamanan, stabilitas, dan kecepatan jaringan meningkat.

Konsep Onion Routing (TOR) pertama kali diusulkan pada tahun 1995, di mana pertama kali didanai oleh Office of Naval Research (ONR) dan kemudian dibantu oleh DARPA pada tahun 1997. Sejak itu, pendanaan untuk TOR Proyek telah disediakan oleh sejumlah sponsor.

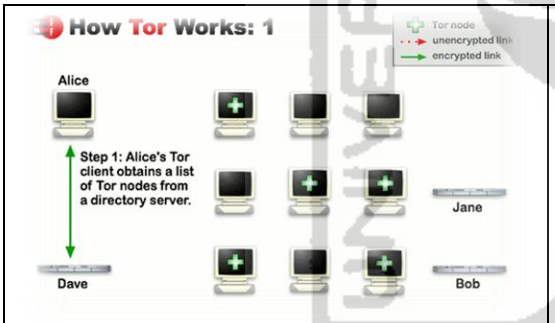
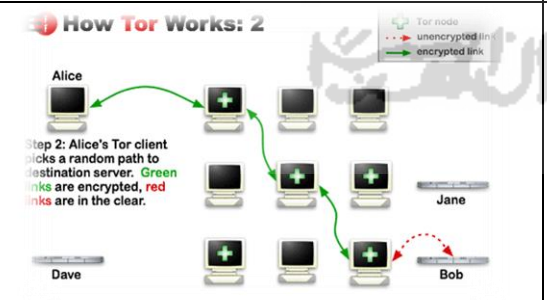
Perangkat lunak TOR seperti yang kita ketahui hari ini awalnya dirilis pada bulan Oktober tahun 2003, dan merupakan perangkat lunak Onion Routing generasi ke-3. Gagasan tentang Onion Routing ini adalah bahwa kita dapat membungkus lalu lintas di lapisan terenkripsi (seperti bawang) untuk melindungi isi data dan juga anonimitas pengirim dan penerima.

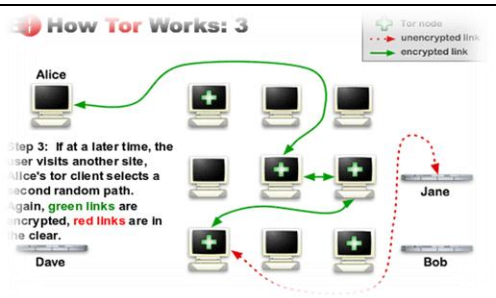
Perkembangan browser Tor dimulai pada tahun 1995 dengan gagasan Onion Routing, yang dimaksudkan untuk melindungi komunikasi Internet di antara Intelijen Amerika Serikat Komunitas (Goldschlag, Reed, & Syverson, 1996). David Goldschlag, Michael Reed, dan Paul Syverson digambarkan dalam "Menyembunyikan Informasi Perutean", arsitektur Bawang yang diusulkan Metodologi routing, yang akan membatasi kerentanan jaringan dan analisis lalu lintas. Ide ini adalah sebuah proyek penelitian di

Laboratorium Penelitian Angkatan Laut A.S., yang didanai oleh DARPA yang slogannya adalah, "menciptakan teknologi terobosan untuk keamanan nasional" (DARPA, 2016). Padahal United Lembaga pemerintah negara bagian pada awalnya menciptakan dan mendanai Tor untuk tujuan keamanan nasional, organisasi seperti FBI percaya bahwa hal itu berkontribusi pada masalah "Going Dark" (Comey, 2015).

Pada tahun 1998, generasi pertama jaringan Onion Routing sedang setup, dengan, "didistribusikan jaringan dari node pada NRL, NRAD, dan UMD "(Syverson, n.d.). Sebuah makalah berjudul, "Anonymous Connections and Onion Routing "dirilis oleh David Goldschlag, Michael Reed, dan Paul Syverson dan memenangkan Alan Berman Research Publication Award (1998). Penelitian tersebut menjelaskan apa jaringan bawang dan bagaimana ia beroperasi untuk kebaikan yang lebih besar berkaitan dengan privasi dan keamanan. Ketiga individu ini adalah pencipta asli browser Tor. Tujuan mereka, digariskan di koran, adalah menggunakan Onion Routing untuk komunikasi anonim dan pribadi bidirectional melalui jaringan publik (Goldschlag, Reed, & Syverson, 1998).

Tabel 2.3 Cara Kerja TOR (https://www.torproject.org/about/overview.html.en)

	TOR Client mencari dan mendapatkan daftar computer pemakai TOR yang aktif dari server untuk dijadikan router nantinya untuk komunikasi
	TOR Client menggunakan jalur acak melalui computer pengguna aktif sebagai router untuk menuju server tujuan. Dimana warna hijau menunjukan jalur yang terenkripsi sedang warna merah jalur yang tdk terenkripsi

	Disaat lain jika client hendak menujuk website lain maka akan memilih jalur acak lagi yang berbeda dari jalur pertama.

2.4 Kali Linux

Kali Linux adalah salah satu distro linux yg dikenal cukup populer untuk kegunaan uji keamanan jaringan dan digital forensic. Kali linux memiliki banyak tools uji keamanan dan mampu berjalan di beberpa arsitektur komputer (Shree Krishna Lamichhane, 2016)

Gambar 2.3 Kali Linux Timeline

2.5 Digital Forensik

Digital forensik adalah cabang dari forensik yang berhubungan dengan pemulihan, investigasi dan analisis bukti yang ditemukan di perangkat digital yang dapat disajikan dalam pengadilan hukum. Saat melakukan penyelidikan harus mengikuti prosedur yang tepat dan protokol dan juga mendokumentasikan dari setiap tahapan saat mencari bukti digital (Noorulla, 2014).

Ungkapan forensik digital dan komputer forensik keduanya sering digunakan secara bergantian yang berarti ilmu memperoleh, mengambil, melestarikan, dan penyajian data yang telah diproses secara elektronik dan disimpan di media komputer (Kruse & Heiser, 2001). Sebagaimana yang disampaikan dalam penelitiannya oleh (Lowman & Ferguson, 2010).

Dari pengertian di atas, maka digital forensik juga dapat dibagi menjadi forensik komputer, forensik multimedia, forensik selular, forensik jaringan, forensik browser dan lainnya. Forensik web browser menjadi penting dalam forensik digital karena meningkatnya jumlah penipuan internet dan aktifitas ilegal lainnya seperti perjudian, prostitusi, perdagangan anak dan lainnya. Forensik web browser adalah kegiatan investigasi atau penyelidikan untuk menggali informasi yang dihasilkan dari web browser dan dapat dideteksi dari informasi yang diperoleh seperti history browser web, cache, cookie, temporary internet file dan bukti digital lainnya yang dihasilkan oleh sebuah web browser (Dharan, 2014).

Dalam proses forensik seperti pengertian dalam digital forensik di atas, maka harus ada prosedur yang harus dilakukan, menurut (Ashcroft, 2001) ada 5 tahapan yaitu:

1. Preparation

   Persiapan yaitu penyidik harus menyadari masalah ini sepenuhnya mulai dari memperoleh izin untuk mengakses informasi pada saat proses investigasi dan perlengkapan pendukung untuk mendokumentasikan kegiatan investigasi.
2. Collection (data)

   Proses mengumpulkan data yang dibutuhkan untuk penyelidikan. Tindakan pencegahan yang tepat harus diambil saat mengumpulkan informasi. Semua data harus dikumpulkan sesuai dengan rencana penyelidikan.
3. Examination

   Pemeriksaan dengan seksama dan harus dilakukan dengan menggunakan beberapa tool/software yang dapat digunakan untuk memastikan dan memberikan hasil yang akurat
4. Analysis

   Analisis hasil untuk mencapai kesimpulan dari apa yang telah dilakukan dan harus jelas. Pada proses analisa bisa juga dengan wawancara sebagai hasil dari kesimpulan jika memungkinkan untuk dilakukan supaya hasil lebih akurat.
5. Reporting

Laporan harus dilaporkan kepada pihak yang berwenang dan harus memenuhi rules of evidence. Laporan harus diarsipkan dan disimpan untuk referensi jika sewaktu-waktu diperlukan di kemudian hari.

Supaya barang bukti dapat diterima di pengadilan maka harus sesuai Rules of Evidence (Cyber Crime Investigators) sesuai modul CHFI yaitu :

1. Dapat diterima

   Barang bukti harus dapat digunakan/diterima di pengadilan atau ditempat lain, jika sewaktuwaktu digunakan oleh pihak lain untuk keperluan tertentu.

2. Otentik/asli

   Barang bukti tersebut harus berhubungan dengan kejadian yang sebenarnya dengan cara yang relevan, jika tidak, maka bukti tersebut tidak bisa membuktikan apa-apa.

3. Lengkap

   Barang bukti yang digunakan haruslah lengkap, tidak hanya menunjukkan satu perspektif dari suatu kejadian. Semua barang bukti yang ditemukan harus di evaluasi.

4. Dapat diandalkan

   Kumpulan barang bukti dan SOP yang telah dijalankan tidak boleh meragukan pada keaslian dan kebenaran barang bukti.

5. Dapat dipercaya

   Barang bukti yang dihadirkan harus jelas mudah dipahami oleh hakim, jaksa dan orang-orang yang berkaitan. Tidak ada gunanya menghadirkan bukti dalam bentuk biner, nilai hash ataupun tulisan asli dari hasil analisis, namun saksi ahli harus mampu menjelaskan antara bukti yang berbentuk naskah yang mudah dipahami dengan bukti asli hasil uji laboratorium dan apakah bukti itu masih asli atau sudah dipalsukan. Semua itu adalah tantangan bagi seorang saksi ahli untuk dapat membuktikan kebenarannya

2.6 Web Browser Forensik

Web browser forensic adalah kegiatan forensik untuk mendapatkan informasi yang tersimpan dari sebuah web browser. Bukti digital yang terdapat pada web browser setidaknya ada caches, history, cookies, download file list, dan sessions. (Ran & Jin, 2012) adapun deskripsi masing-masing sebagai berikut:

1. Cache

   Cache browser adalah sebuah file yang diambil dari situs-situs yang dikunjungi disimpan (sementara) pada lokasi tertentu pada hard disk. Tujuan utama dari ini adalah

bahwa (bagian dari) halaman web yang dikunjungi sebelumnya dapat dimuat lebih cepat ketika halaman web ini dikunjungi lagi di tahap selanjutnya (Schaap, 2013).

2. Cookies

   Cookie adalah bit data yang tersimpan pada klien oleh browser. Cookies pada browser menyimpan segala macam informasi yang berkaitan tentang apa saja situs yang dikunjungi (Lori MacVittie, 2008).

3. Download File List

   Download file list adalah sebuah fitur dari browser yang berguna untuk menyimpan dan menampilkan daftar dari apa yang didownload menggunakan browser.

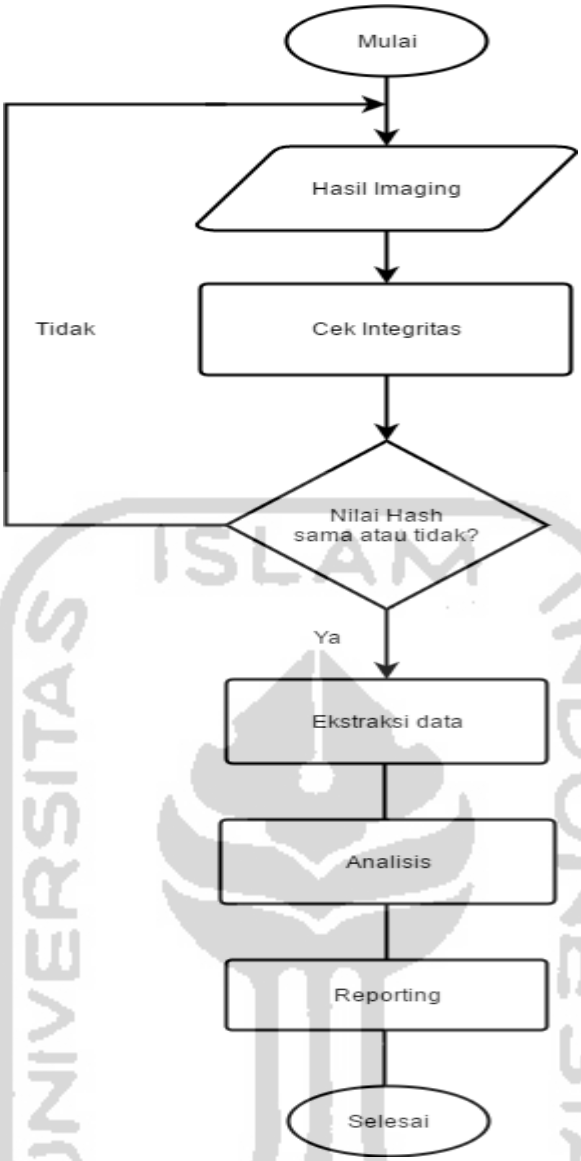
4. Sessions

   Session adalah suatu cara dimana web browser dan server untuk mempertahankan hubungan antara pengguna yang melakukan aktifitas di internet. Session digunakan untuk memelihara informasi akses dari pengguna (Lori MacVittie, 2008). Setidaknya minimal barang bukti digital dari web browser di atas sangat penting dan bagus digunakan oleh investigator untuk menganalisa dalam sebuah kasus yang menggunakan internet (Jones and Belani, 2008).

2.7 Analisis Forensik

Menurut Divyesh G Dharan D, proses pengumpulan barang bukti dalam komputer ada 2 yaitu Offline dan Live (Dharan, 2014)

Proses *forensic* yang dilakukan dalam penelitian ini akan mengambil fokus utama terhadap analisa data *Log sistem operasi, url history, cache, cookie*. *Download file* Komponen-komponen tersebut merupakan informasi yang dapat digabungkan untuk bisa menjawab kebutuhan informasi terkait dari mana sumber tindak kejahatan, dan waktu kejadian kejahatan. Adapun alur kerja forensik yang dilakukan pada penelitian ini.



Gambar 2.4 Alur Analisis Forensik

2.8 File Log

File log adalah file yang berisi daftar acara, yang telah "login" oleh komputer. File log sering dihasilkan selama instalasi perangkat lunak dan dibuat oleh server Web, namun file tersebut juga dapat digunakan untuk berbagai tujuan lain. Sebagian besar file log disimpan dalam format teks biasa, supaya meminimalkan ukuran file dan memungkinkannya dapat dilihat melalui teks editor(Christensson, 2010).

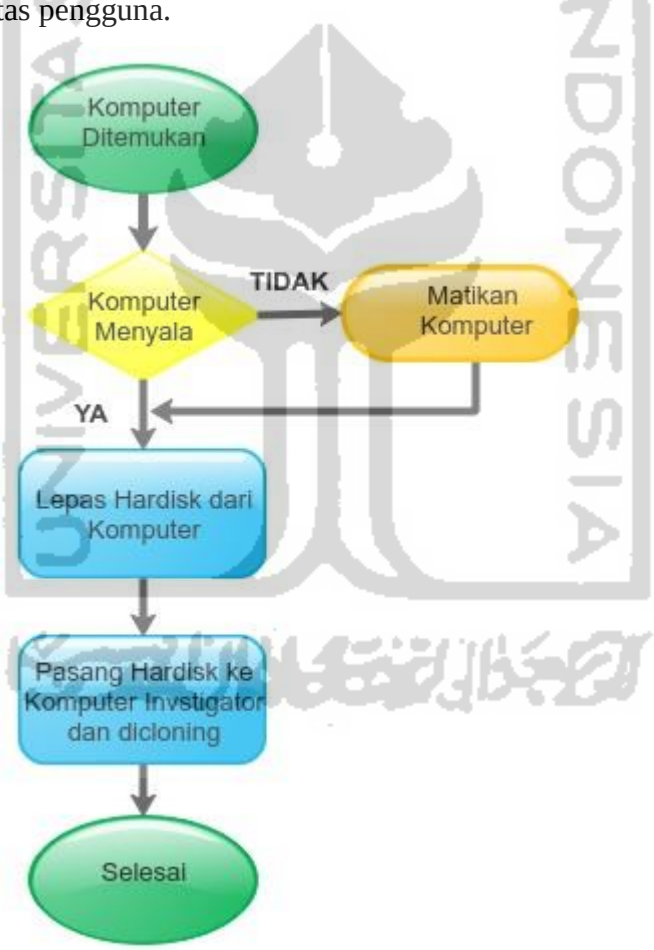
File log yang dibuat oleh perangkat lunak biasanya berisi daftar file yang telah ditambahkan atau disalin ke hard drive selama proses instalasi. File log juga menyertakan tanggal dan waktu file-file itu terpasang, serta direktori tempat setiap file ditempatkan. File log penginstal memungkinkan pengguna melihat file apa yang terinstal di sistem

menggunakan program tertentu. Hal ini berguna saat mengatasi masalah crash program atau saat menguninstall sebuah program(Christensson, 2010).

Log, dalam konteks komputasi adalah dokumentasi kejadian (aktivitas) yang diproduksi secara otomatis dengan pewaktuan (*time-stamps*) yang relevan dengan sistem tertentu. Hampir semua aplikasi dan sistem perangkat lunak menghasilkan file log, log dapat diartikan sebagai file yang berisi daftar tindakan yang telah terjadi.

2.9 Offline Forensik

Analisa offline dalam forensik digital adalah proses investigasi yang dilakukan untuk mencari barang bukti dari sebuah barang elektronik yang sudah mati atau OFF. Dalam hal ini yang bias dianalisa adalah berupa storage atau apapun yang di dalamnya akan menyimpan dari aktifitas pengguna.



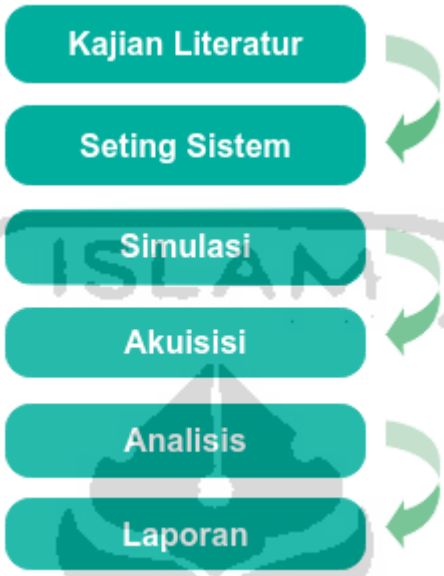
Gambar 2.5 Alur Offline Forensic

BAB 3

Metodologi Penelitian

3.1 Alur Penelitian

Dalam melaksanakan penelitian ini akan dilakukan tahapan-tahapan sesuai gambar berikut



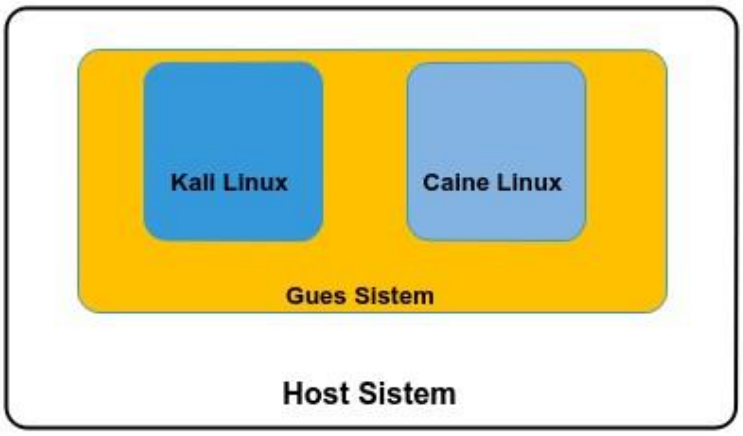
Gambar 3.1 Alur Penelitian

3.2 Kajian Literatur

Studi literatur digunakan untuk memahami tentang konsep, teori, dan hasil temuan penelitian lain yang serumpun dan akan dijadikan acuan sebagai landasan penelitian. Pada review penelitian berisi rangkuman dan hasil penelitian sebelumnya dengan topic yang terkait.

3.3 Setting Sistem

Sistem yang digunakan untuk melakukan penelitian semua berjalan dalam lingkungan Virtualisasi Menggunakan Perangkat Laptop dan Software Virtualbox



Gambar 3.2 Desain system

3.3.1 Alat dan Bahan

Untuk mendukung implementasi dalam penelitian ini diperlukan adanya perangkat keras dan perangkat lunak sebagai alat dan bahan penelitian, berikut ini beberapa alat dan bahan

Hardware:

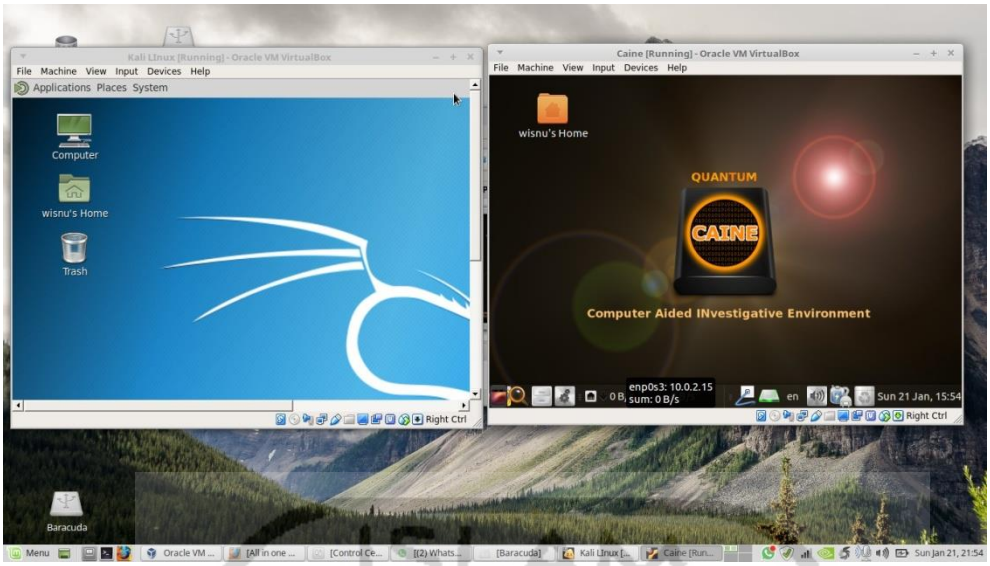
- Laptop Lenovo IdeaPad 310 sebagai komputer untuk melakukan penarikan data dan analisa, dengan spesifikasi Intel Core i5, RAM 8GB

Software:

- Kali Linux
- Caine Linux
- Forensic Tools
- VirtualBox

3.3.2 Instalasi Sistem Operasi dan Aplikasi

Dalam implementasi ini, Sistem Operasi yang digunakan sbg object yaitu Kali Linux dan system operasi sbg Subyek forensic yaitu Caine Linux dipasang dalam lingkungan virtualisasi menggunakan software virtualbox dan sebagai host OSnya Linux Mint



Gambar 3.3 Sistem Software yg Terpasang

Tabel 3.1 Software Pendukung Penelitian

Software	Logo	Keterangan
Linux Mint		Sebagai Host OS atau system operasi utama yg terpasang di lapptop
Virtualbox		Sebagai software virtualisasi untuk menjalankan guest OS
Kali Linux		Guest OS sebagai obyek forensic
Caine Linux		Guest OS sebagai subyek forensic

3.4 Simulasi

Untuk melakukan simulasi maka dibuat skenario dari penggunaan Kali Linux dan TOR Browser. Tahapan skenario diperlukan untuk menggali informasi, melakukan ujicoba sistem, dan pendalaman dalam memahami karakteristik digital artefacs. Berikut ini merupakan topologi yang diterapkan pada penelitian ini.

Simulasi dilakukan untuk menimbulkan jejak aktivitas pada sistem operasi Kali Linux dengan menjalankan aktivitas browsing Menggunakan TOR Browser kemudian akan dicari sebagai temuan dalam proses investigasi forensik. Adapun jenis simulasi yang akan diterapkan adalah Setelah user melakukan aktivitas browsing, maka dilakukan Forensic Secara Offline dengan cara Hardisk dilepas dan dihubungkan dengan Komputer yg sudah terinstall Linux Caine yg digunakan khusus utk Analisi Forensic.

Gambar 3.4 Alur Simulasi

3.5 Akuisisi

Tahap akuisisi pada penelitian ini dilakukan secara *offline forensic*, dimana dilakukan dalam kondisi komputer tidak menyala, dan media penyimpan dilepas. Media penyimpan dihubungkan ke sistem utk forensic dan dilakukan write blocker untuk menghindari adanya perubahan data pada media penyimpan yang akan diakuisisi.

Software Autopsy digunakan untuk melakukan akusisi barang bukti dalam upaya untuk menemukan bukti digital yang bisa menjadi petunjuk dari keberadaan dan aktivitas TOR Browser pada sistem operasi Kali Linux.

3.6 Analisis

Tahapan analisis ini digunakan untuk menganalisa barang bukti yang telah dilakukan akuisisi. Proses *forensic* yang dilakukan dalam penelitian ini akan mengambil fokus utama terhadap analisa data hasil aktivitas browsing menggunakan browser TOR berupa, cache, history, dan cokies.Komponen-komponen tersebut merupakan informasi yang dapat digabungkan untuk bisa menjawab kebutuhan informasi terkait dari mana sumber tindak kejahatan, dan waktu kejadian kejahatan.

3.7 Laporan

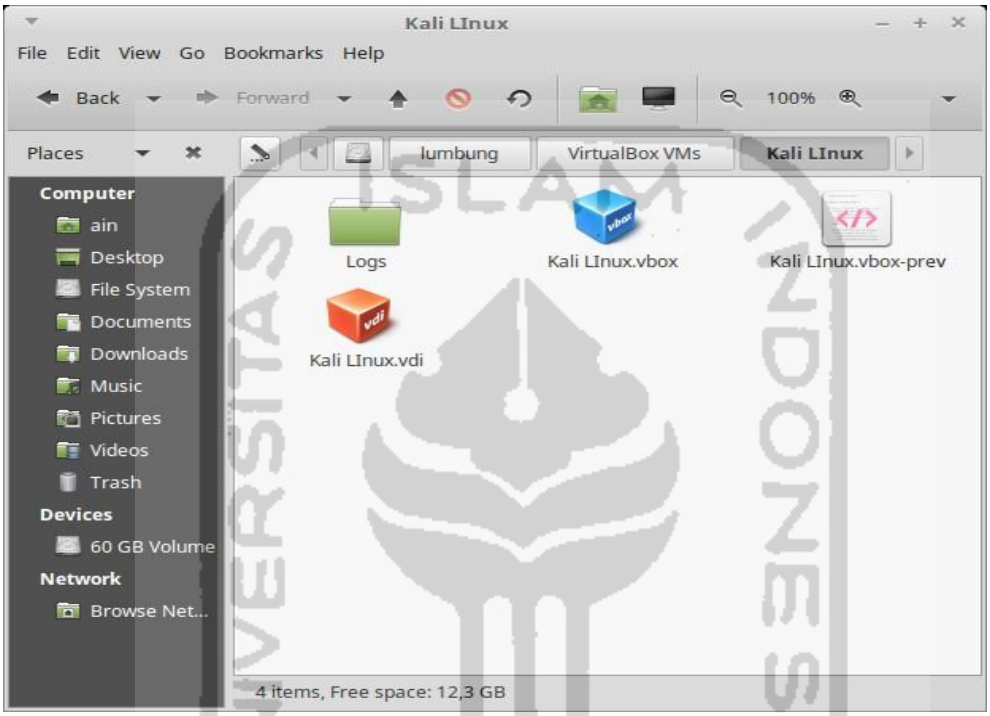
Tahap terakhir dari penelitian adalah membuat dokumentasi terhadap penelitian yang dilakukan secara keseluruhan agar bisa menjadi sebuah karya ilmiah dan memungkinkan sebagai referensi penelitian lain yang topiknya yang berkesesuaian.

BAB 4

Hasil dan Pembahasan

4.1 Data

Dalam proses offline forensic ini barang bukti utama yang ada yaitu storage media berupa hardisk, dikarenakan berasal dari sebuh system virtual maka hardisk yang ada berupa file image sesuai format virtualisasi.



Gambar 4.1 Barang Bukti Image Hardisk

Untuk melakukan analisis digital forensic digunakan system operasi linux caine yang dikhususkan untuk penggunaan Digital forensic dengan tool-tool bawaan yang sudah cukup lengkap.

Jejak Digital Artefak yang mungkin di hasilkan dari kegiatan penelitian TOR Browser forensic kali ini adalah *log system operasi, cache, cookies, file download* dimana file tersebut diperoleh dengan cara explorasi dari media penyimpan yang telah diakuisisi

Dalam Implementasi Forensic Aktivitas dari TOR Browser untuk memperolah jejak-jejak digital maka perludilakukan tahapan-tahapan berikut:

4.1.1 Validasi

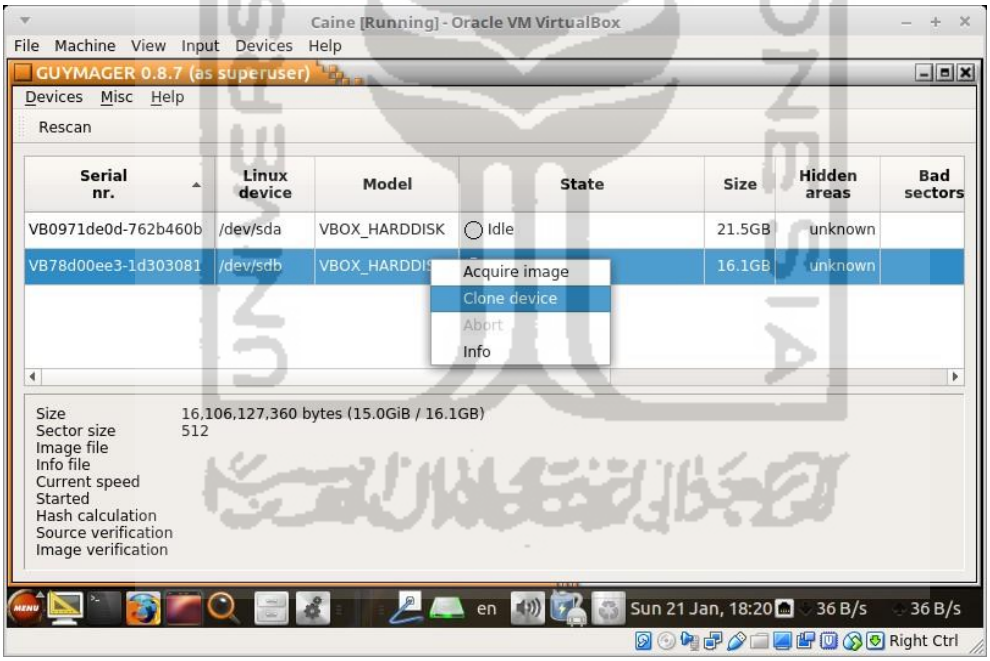
Untuk memastika keaslian dari barang bukti duplikat yang akan dianalisis, maka perlu dilakukan hashing terhadap barang bukti dengan menggunakan standart MD5 sehingga jika

ada kesesuaian nilai hash dari barang bukti asli dan duplikanya maka bisa dipastikan bahwa keduanya identik dan otentik.

Gambar 4.2 Hashing Barang Bukti

4.1.2 Duplikasi

Dalam melakukan akuisisi dan analisis maka sesuai prinsip utama dalam digital forensic untuk tidak melakukan analisis langsung terhadap barang bukti asli. Sehingga perlu adanya salinan dari barang bukti asli yang identik. Dalam melakukan duplikasi maka digunakan aplikasi Guymager yang merupakaan tools bawaan dari distro Linux Caine yang digunakan untuk melakukan analisis forensic.



Gambar 4.3 Proses Duplikasi Hardisk

4.2 Simulasi Kasus

Dalam simulasi Kasus ini, untuk mendapatkan data dengan jumlah dan karakteristik yang variatif serta memadai maka akan dilaksanakan dalam beberapa skenario dari aktifitas pengguna.

Simulasi implementasi forensic TOR Browser secara keseluruhan dijelaskan seperti bagan berikut ini

Gambar 4.4 Bagan Simulasi Kasus

Sekenario tersebut dibagi menjadi tiga dan masing-masing sekenario memiliki aktivitas yang berbeda-beda seperti ditampilkan dalam tabel 4.1 berikut ini:

Tabel 4.1 Skenario Simulasi

Aktifitas Pengguna	Skenario 1	Skenario 2	Skenario 3
Pemasangan TOR Browser	√		
Menjalankan TOR Browser	√	√	√
Menjelajah Web		√	
Mendownload File			√
Menutup TOR Browser	√	√	√

4.2.1 Skenario Pertama

Skenario pertama dilakukan dengan dimulai dari download, instalasi dan menjalankan pertama kali TOR Browser, tanpa melakukan aktivitas menjelajah internet.

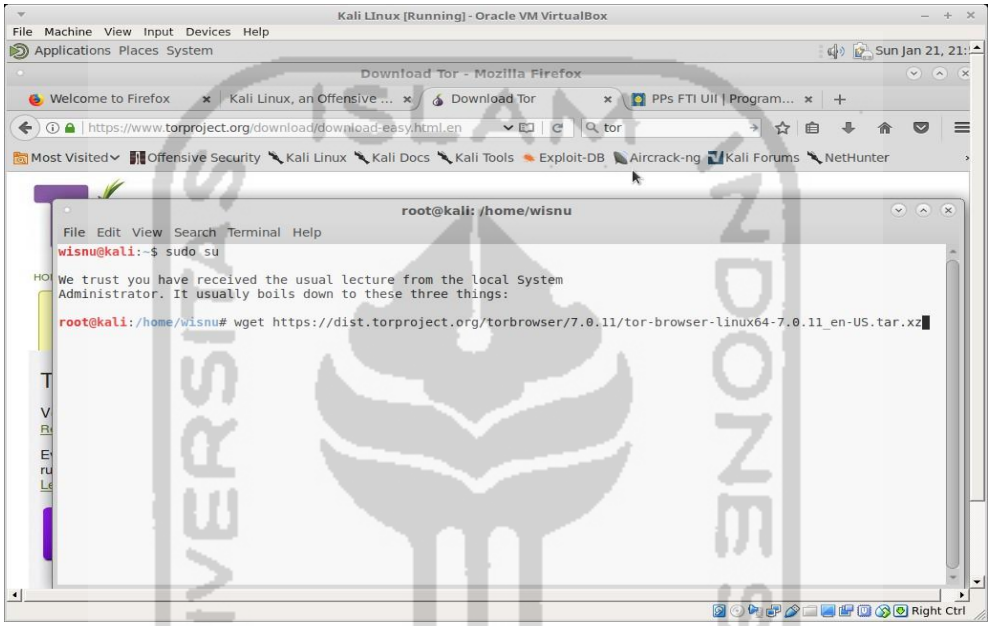
Harapan dari skenario ini akan diperoleh data jejak keberadaan TOR Browser dari log-log pada Sistem Operasi Kali Linux dimana TOR Browser dipasang.

Gambar 4.5 Skenario Pertama

Tahapan-tahapan yang dilakukan dalam sekenario pertama ini dapat dirinci sebagai berikut:

1. Download

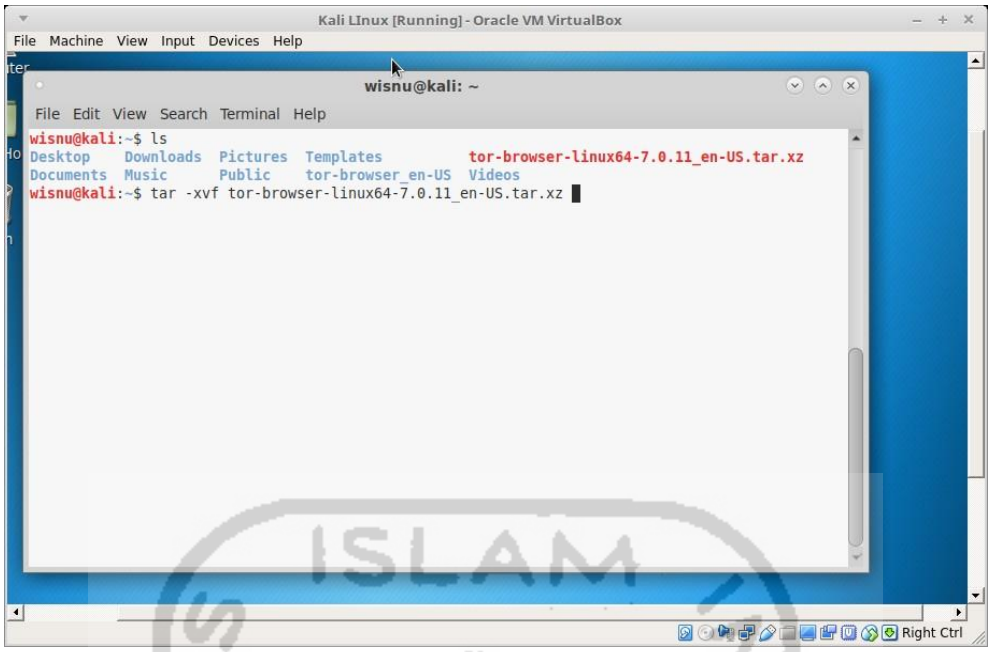
   Pada tahap ini user melakukan download aplikasi TOR Browser dari situs www.torproject.org melalui sistem operasi kali linux baik secara command line maupun dari browser bawaan. Dari aktivitas ini diperoleh file installer dari tor yaitu tor-browser-linux64-7.0.11_en-US.tar.xz yang tersimpan kedalam folder home user.



Gambar 4.6 Proses Download TOR Browser

2. Install

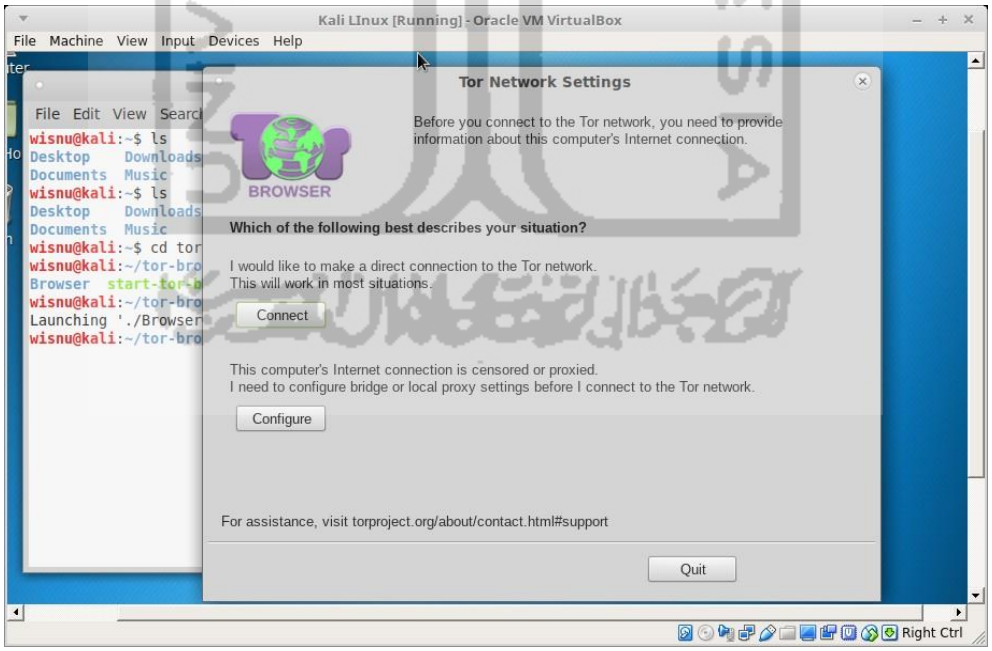
   Pada tahap ini user melakukan pemasangan TOR Browser hasil download kedalam sistem operasi kali linux. Karena paket installernya berupa file binary yang terkompres, maka cara instalasinya cukup dg melakukan ekstrasi saja menggunakan tool tar bawaan dari kali linux



Gambar 4.7 Install TOR Browser

3. Menjalankan

Pada tahap ini user menjalankan TOR Browser untuk pertama kalinya melalui command line. TOR Browser dijalankan tanpa melakukan aktivitas menjelajah web dengan tujuan untuk meninggalakan jejak dalam system operasi kali linux akan aktivitas menjalankan aplikasi TOR Browser.



Gambar 4.8 Menjalankan TOR Browser Pertama Kali

4.2.2 Skenario Kedua

Skenario kedua dilakukan dengan dimulai menjalankan TOR Browser untuk melakukan aktivitas menjelajah interne ke beberapa situs, dan kemudian menutup sesi dari TOR

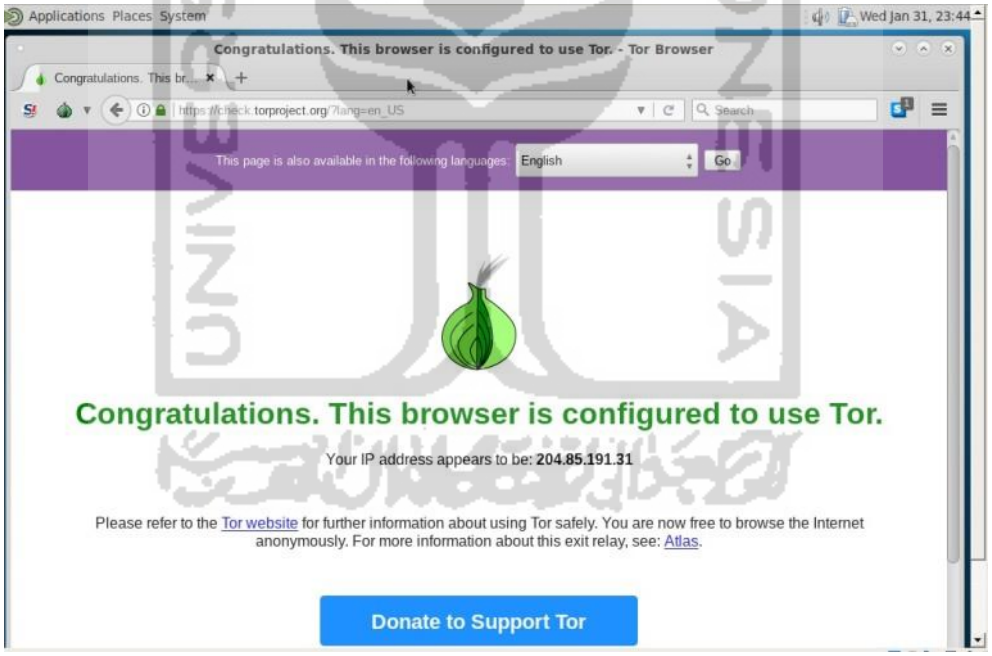
Browser sehingga diharapkan akan adanya jejak digital dari aktivitas penjelajahan internet kebeberapa situs tersebut yang tersimpan kedalam media penyimpanan berupa url history, cache maupun cookies

Gambar 4.9 Skenario Kedua

Tahapan-tahapan yang dilakukan dalam sekenario kedua ini dapat dirinci sebagai berikut:

1. Menjalankan

   Pada tahap ini user menjalankan TOR Browser secara umum melalui commandline



Gambar 4.10 Menjalankan TOR Browser

2. Menjelajah

   Pada tahap ini user menggunakan TOR Browser untuk membuka dan menjelajah ke beberapa website dan sub domainya

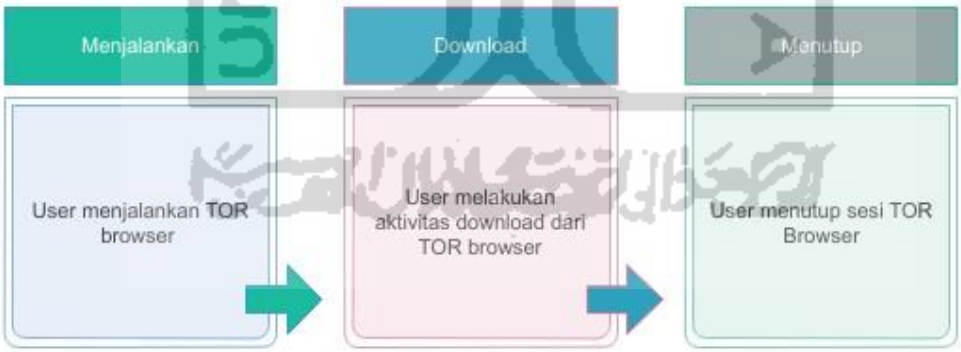
Gambar 4.11 Menjelajah Web dengan TOR Browser

3. Menutup

   Pada tahap ini user mematikan TOR Browser dengan mengklik tombol silang dari windows manager aplikasi tersebut.

4.2.3 Skenario Ketiga

Skenario ketiga dilakukan seperti sekenario kedua yaitu melakukan penjelajahan ke beberapa website namun dengan tambahan aktivitas download sebuah file, sehingga diperoleh tipe jejak digital yang berbeda dari sekenario sebelumnya.

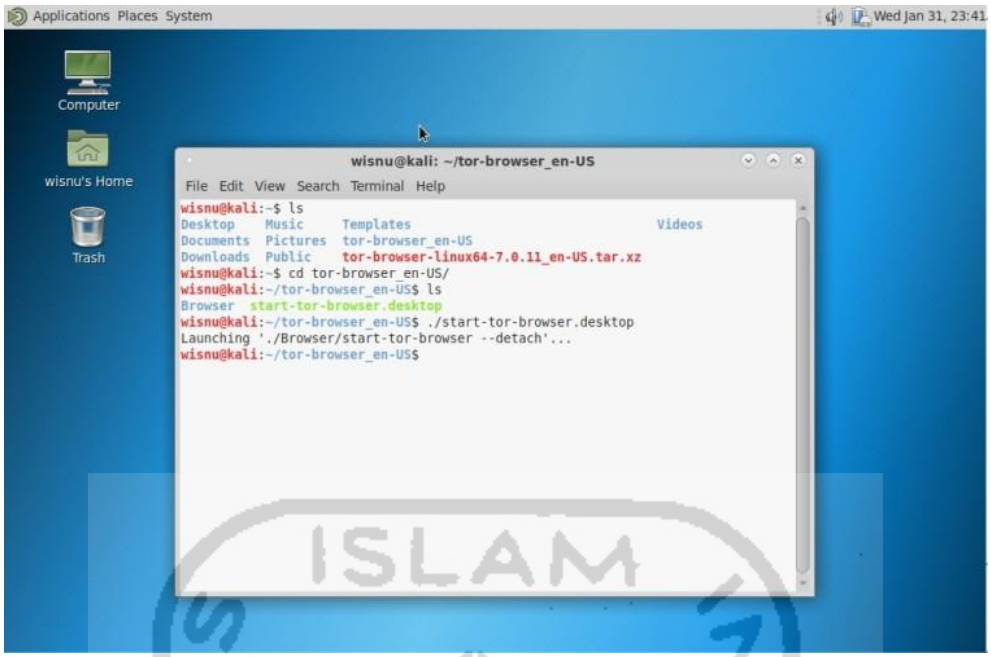


Gambar 4.12 Skenario Ketiga

Tahapan-tahapan yang dilakukan dalam sekenario kedua ini dapat dirinci sebagai berikut:

1. Menjalankan

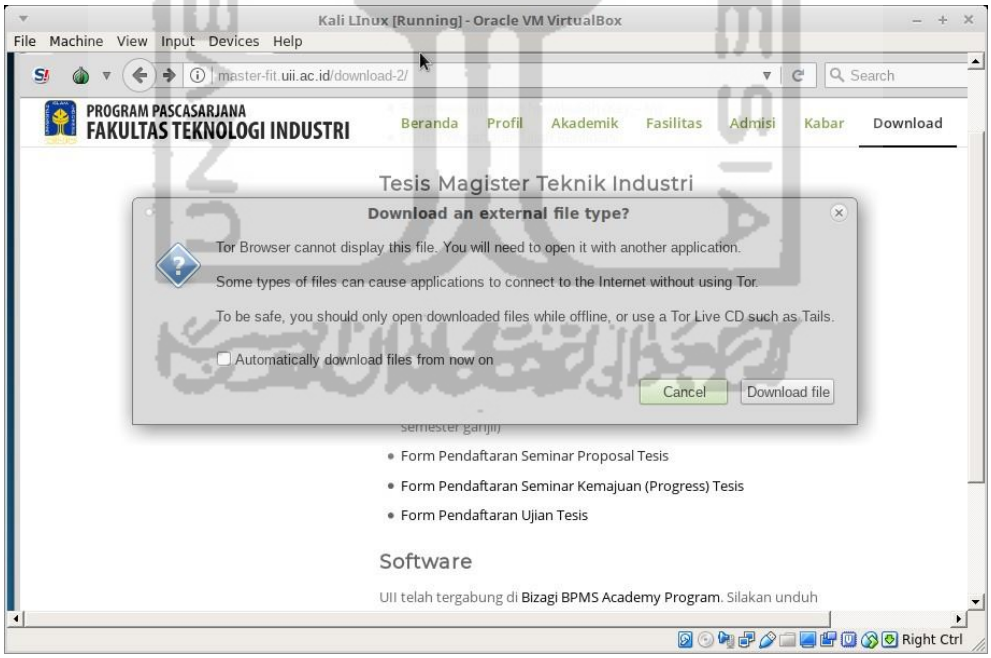
   Pada tahap ini user menjalankan TOR Browser secara umum dengan commandline



Gambar 4.13 Menjalankan TOR Browser

2. Download

Pada tahap ini user berkunjung ke sebuah web site dan melakukan download file menggunakan TOR Browser, dimana file tersebut tersimpan kedalam folder default download dari TOR Browser



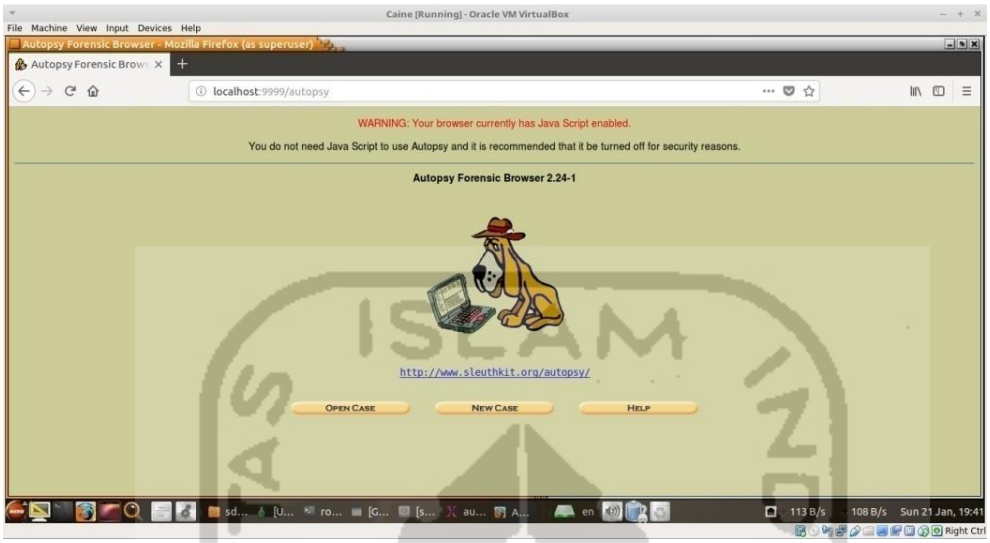
Gambar 4.14 Download pada TOR Browser

3. Menutup

Pada tahap ini user mematikan TOR Browser dengan mengklik tombol silang dari windows manager aplikasi tersebut.

4.3 Akuisisi

Dalam melakukan akuisisi dari barang bukti berupa image disk, peneliti menggunakan tools Autopsy yang berbasis Open sources



Gambar 4.15 Autopsy

Proses Pencarian Bukti Digital dilakukan dengan mengekplorasi image disk secara mendalam kedalam struktur file system dan folder dari image tersebut.

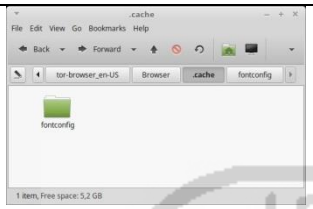
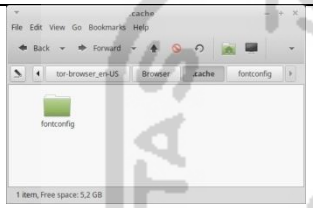
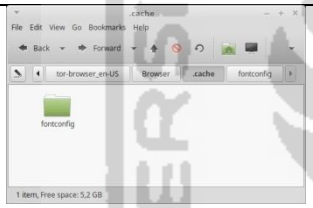
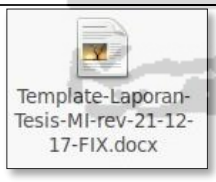
Gambar 4.16 Proses Akuisis Pencarian Bukti Digital

Dari Gambar 4.15 Proses akuisis bisa terlihat jelas hasil dari explorasi bukti digital dimana file-file dan folder yang ada dalam bukti digital bisa terlihat dan ditemukan

4.4 Hasil

Hasil implementasi penelitian diperoleh dari akuisisi media penyimpanan baik berupa file-file log, hasil download maupun pendukung lainya.

Tabel 4.2 Hasil Bukti Digital

Artefac	TOR Browser	Sistem Operasi	Keterangan
Url history		-	Tidak ditemukan
Cache		-	Tidak ditemukan
Cookies		-	Tidak ditemukan
Bash History	-		Ditemukan dalam log file bash_history
Dowloaded File		-	Ditemukan dalam folder Download dari TOR Browser

4.5 Analisis

Analisis dilakukan untuk mencari segala informasi yang dimungkinkan bisa menjadi bukti digital dari keberadaan dan aktivitas penggunaan TOR Browser.

4.5.1 Analisis Url history

Dalam aktifitas penjelajahan internet secara default browser akan menyimpan daftar website yang pernah dikunjungi berupa sebuah database yang tersimpan didalam folder dari browser yang digunakan.

Dalam analisis pencarian jejak digital untuk histori dari website yang telah dikunjungi menggunakan TOR Browser ternyata tidak ditemukan file database dari daftar website yang pernah dikunjungi seperti terlihat dalam gambar 4.16

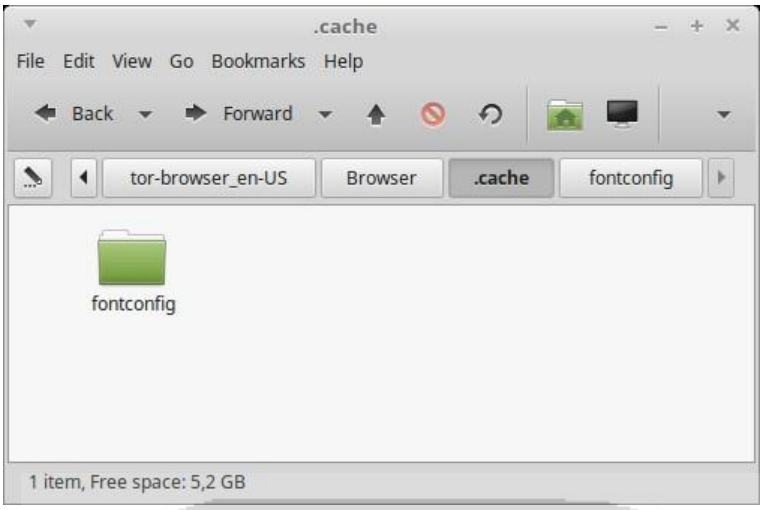
Gambar 4.17 Folder Penyimnpanan URL history

Dari hasil pencarian dengan tidak ditemukanya jejak digital terkait Url histori maka bisa dijelaskan bahwa TOR Browser memang tidak menyimpan daftar website yang telah dikunjungi.

4.5.2 Analisis Cache

Dalam setiap aktivitas membuka sebuah website, browser secara default akan menyimpan file-file dari websiter tersebut yang akan digunakan dikala membuka website yang sama maka tidak perlu langsung mengambil dari website aslinya, cukup dari file cache yang terimpan dalam browser tersebut.

Dalam analisis pencarian jejak digital untuk cache dari website yang telah dikunjungi menggunakan TOR Browser tidak ditemukan seperti terlihat dalam gambar 4.17



Gambar 4.18 Folder Penyimpanan Cache

4.5.3 Analisis Cookies

Cookie sangat penting digunakan dalam website yang ada proses transaksi didalamnya, dimana cookies ini memungkinkan website tetap menjaga koneksi/sesi dari transaksi yang dilakukan.

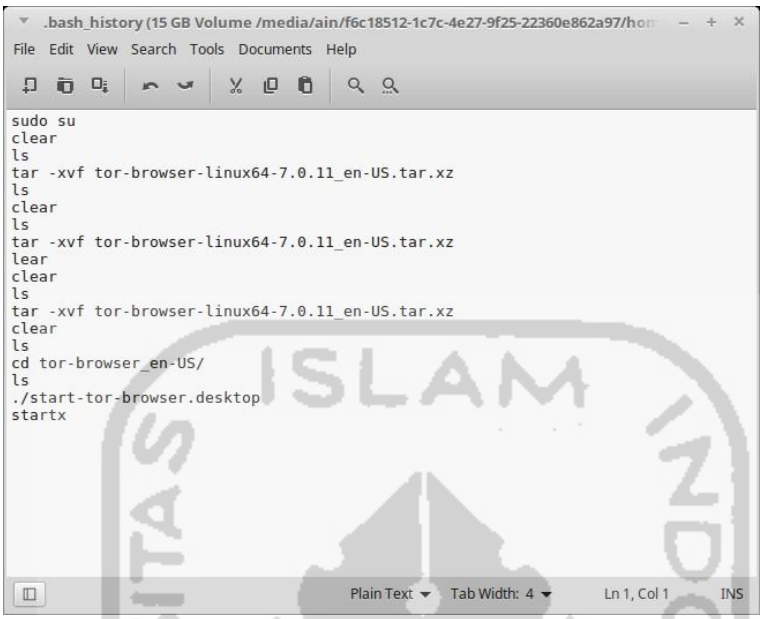
Dalam analisis pencarian jejak digital untuk histori dari website yang telah dikunjungi menggunakan TOR Browser tidak ditemukan

Gambar 4.19 Folder Penyimpanan Cookies

4.5.4 Analisis Bash history

Shell merupakan komponen utama dan sangat penting dalam system operasi linux, dimana shell berfungsi menterjemahkan perintah-perintah user untuk dijalankan oleh system operasi linux. BASH merupakan shell standart bawaan yang banyak digunakan dan shell mempunyai kemampuan untuk merekam dan menyimpan dari perintah-perintaj yang telah dijalankan sehingga aktivitas user bisa terekam.

Dari analisis log bash histori ditemukan bahwa user melakukan pemasangan dan menjalankan TOR Browser



Gambar 4.20 Log Dari Bash History

4.5.5 Analisis Download

Sebuah web browser menyediakan folder tersendiri untuk menyimpan file-file hasil dari melakukan aktifitas download oleh user.

TOR Browser menyimpan hasil downloadnya seperti browser-browser yang lain sehingga file tersebut bisa ditemukan karena tersimpan secara permanen dalam media penyimpanan.

Gambar 4.21 Hasil Pencarian file download

Seperti tampak dalam gambar 4.20 bahwa file hasil download tersimpan dalam folder download dari TOR Browser.

Dari proses ujicoba yang dilakukan dengan beberapa skenario untuk memperoleh bukti digital dan merujuk dari Tabel hasil akuisisi maka bisa diperoleh jawaban dari rumusan masalah terkait dari karakteristik barang bukti yang bisa diperoleh dari penggunaan metode offline forensic untuk analisis digital artefacs pada TOR Browser di Sistem Operasi Kali Linux bahwa ada jejak digital yang tersimpan dalam media penyimpan dan ada jejag digital yang tidak tersimpan dalam media penyimpan.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil analisis forensic yang dilakukan bisa ditarik kesimpulan sebagai berikut:

1. Keberadaan penggunaan TOR Browser untuk aktifitas penjelajahan web bisa diketahui dari analisis log-log dari system operasi dimana TOR Browser tersebut dipasang.
2. Jejak Digital dari TOR Browser ada yang bersifat tersimpan di media penyimpanan dan tidak tersimpan di media penyimpanan
3. Tahapan Dalam melakukan Offline Forensic pada TOR Browser untuk analisis bukti digital meliputi: Imaging, validasi hashing, dan akuisisi

5.2 Saran

Untuk Memperoleh bukti digital yang kuantitasnya sebanyak mungkin dan variatif dan lengkap dalam investigasi forensic maka perlu mencari bukti digital dari banyak media yang dimungkinkan tersimpanya jejak digital dan akusisi bukti digital dilakukan tidak hanya menggunakan satu jenis metode saja.

Karena masing-masing tool forensic memiliki kelebihan dan kekurangan maka perlu digunnakan banyak tools untuk menghasilkan analisis yang lebih lengkap.

DaftarPustaka

Adautin, E. D., & R, N. M. A. (2015). Forensic Reconstruction and Analysis of Residual Artifacts from Portable Web Browser, *128*(18), 19–24.

Al-Khaleel, A., Bani-Salameh, D., & Al-Saleh, M. I. (2014). On the Memory Artifacts of the Tor Browser Bundle. *Proceedings of the International Conference on Computing Technology and Information Management*, 41–46.

Babincev, I., & Vuletic, D. (2016). Web application security analysis using the Kali Linux operating system. *Vojnotehnicki Glasnik*, *64*(2), 513–531. https://doi.org/10.5937/vojtehg64-9231

Christensson, P. (2010). Log File Definition.

Hassan, N. F., & Jaber, H. M. (2017). Offline vs . Online Digital Forensics of Cloud - based Services, *20*(4), 117–124. https://doi.org/10.22401/JUNS.20.4.18

Keller, K. (2016). *The Tor Browser A Forensic Investigation Study*.

Kolhe, M., & Ahirao, P. (2017). Live Vs Dead Computer Forensic Image Acquisition. *International Journal of Computer Science and Information Technologies*, *8*(3), 455–457.

Mulazzani, M. (2014). New challenges in digital forensics: online storage and anonymous communication, *2014*.

Noorulla, E. S. (2014). Web Browser Private Mode Forensics Analysis.

Rochmadi, T. (2017). Analisis Anti Forensik pada Portable Web Browser Mode Private Menggunakan Metode Live Forensik.

Sandvik, R. A. (2013). Forensic Analysis of the Tor Browser Bundle on OS X, Linux, and Windows, 1–13.