Bab 1Pendahuluan

1.1 Latar Belakang

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

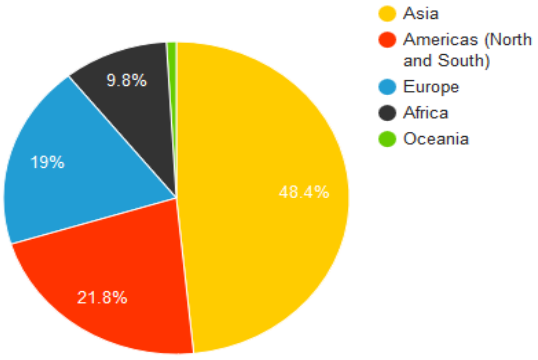
Kegiatan internet dari mulai mencari informasi, berkirim email, blogging, sosial media, menonton video dan aktifitas lain di internet penggunanya selalu bertambah, dan dari pantauan live www.internetlivestats.com menunjukkan traffik internet di estimasikan pada 1 Juli 2016 mencapai 3.424.971.237. Tabel 1.1 menunjukkan statistik pengguna internet seluruh dunia dari tahun 2005.

Tabel 1. 1 Statistik Pengguna Internet Seluruh Dunia

Year	Internet Users**	Penetration (% of Pop)	World Population	Non-Users (Internetless)	1Y User Change	1Y User Change	World Pop. Change
2016*	**3,424,971,237**	46.1 %	7,432,663,275	4,007,692,038	7.5 %	238,975,082	1.13 %
2015*	**3,185,996,155**	43.4 %	7,349,472,099	4,163,475,944	7.8 %	229,610,586	1.15 %
2014	**2,956,385,569**	40.7 %	7,265,785,946	4,309,400,377	8.4 %	227,957,462	1.17 %
2013	**2,728,428,107**	38 %	7,181,715,139	4,453,287,032	9.4 %	233,691,859	1.19 %
2012	**2,494,736,248**	35.1 %	7,097,500,453	4,602,764,205	11.8 %	262,778,889	1.2 %
2011	**2,231,957,359**	31.8 %	7,013,427,052	4,781,469,693	10.3 %	208,754,385	1.21 %
2010	**2,023,202,974**	29.2 %	6,929,725,043	4,906,522,069	14.5 %	256,799,160	1.22 %
2009	**1,766,403,814**	25.8 %	6,846,479,521	5,080,075,707	12.1 %	191,336,294	1.22 %
2008	**1,575,067,520**	23.3 %	6,763,732,879	5,188,665,359	14.7 %	201,840,532	1.23 %
2007	**1,373,226,988**	20.6 %	6,681,607,320	5,308,380,332	18.1 %	210,310,170	1.23 %
2006	**1,162,916,818**	17.6 %	6,600,220,247	5,437,303,429	12.9 %	132,815,529	1.24 %
2005	**1,030,101,289**	15.8 %	6,519,635,850	5,489,534,561	12.8 %	116,773,518	1.24 %

Sumber : http://www.internetlivestats.com/internet-users/#trend

Sumber yang sama juga menyebutkan pengguna internet terbesar berasal dari benua Asia dengan persentase 48,4% seperti pada Gambar 1.1 di bawah ini.



Gambar 1. 1 Grafik Persentase Pengguna Internet
Sumber : http://www.internetlivestats.com/internet-users/#byregion

Semakin merebaknya aktifitas di internet, maka bidang yang lainpun juga ikut berevolusi memanfaatkan internet semisal *e-commerce* ataupun dari cara masyarakat bersosialisasi. Hal demikian juga sudah mulai terasa di Indonesia seperti yang disebutkan dalam statistik pada Tabel 1.2 yang menunjukkan bahwa Indonesia menempati urutan ke 12 dari pengguna internet seluruh dunia.

Tabel 1. 2 Statistik Pengguna Internet Berdasarkan Negara

#	Country	Internet Users (2016)	Penetration (% of Pop)	Population (2016)	Non-Users (internetless)	Users 1 Year Change (%)	Internet Users 1 Year Change	Population 1 Y Change
1	China	721,434,547	52.2 %	1,382,323,332	660,888,785	2.2 %	15,520,515	0.46 %
2	India	462,124,989	34.8 %	1,326,801,576	864,676,587	30.5 %	108,010,242	1.2 %
3	U.S.	286,942,362	88.5 %	324,118,787	37,176,425	1.1 %	3,229,955	0.73 %
4	Brazil	139,111,185	66.4 %	209,567,920	70,456,735	5.1 %	6,753,879	0.83 %
5	Japan	115,111,595	91.1 %	126,323,715	11,212,120	0.1 %	117,385	-0.2 %
6	Russia	102,258,256	71.3 %	143,439,832	41,181,576	0.3 %	330,067	-0.01 %
7	Nigeria	86,219,965	46.1 %	186,987,563	100,767,598	5 %	4,124,967	2.63 %
8	Germany	71,016,605	88 %	80,682,351	9,665,746	0.6 %	447,557	-0.01 %
9	U.K.	60,273,385	92.6 %	65,111,143	4,837,758	0.9 %	555,411	0.61 %
10	Mexico	58,016,997	45.1 %	128,632,004	70,615,007	2.1 %	1,182,988	1.27 %
11	France	55,860,330	86.4 %	64,668,129	8,807,799	1.4 %	758,852	0.42 %
12	Indonesia	53,236,719	20.4 %	260,581,100	207,344,381	6.5 %	3,232,544	1.17 %
13	Viet Nam	49,063,762	52 %	94,444,200	45,380,438	3.3 %	1,564,346	1.07 %
14	Turkey	46,196,720	58 %	79,622,062	33,425,342	5.1 %	2,242,750	1.22 %
15	Philippines	44,478,808	43.5 %	102,250,133	57,771,325	4.4 %	1,855,574	1.54 %

Sumber : http://www.internetlivestats.com/internet-users-by-country/

Dari kenyataan tersebut menurut (Patel, 2014.) kejahatan dengan *web browser* bertambah dan akibatnya dari kejahatan tersebut menimbulkan kerugian sehingga penting untuk mengumpulkan jejak riwayat internet dan password untuk bisa dijadikan sebagai barang bukti.

Setiap aktifitas menggunakan *web browser*, selalu meninggalkan jejak pada komputer seperti *cache, history, cookies* dan daftar download jika pengguna juga mendownload dari internet (Oh et al., 2011). Jejak bukti digital dari suatu *web browser* dibutuhkan untuk menganalisa rekam jejak aktifitas yang dilakukan pengguna apabila terjadi suatu tindakan *cybercrime* (Chivers, 2013). Atas dasar pengetahuan tersebut maka beberapa developer *web browser* berupaya membuat *mode private* pada *web browser* untuk melindungi dan meningkatkan privasi keamanan *web browser* untuk di sisi pengguna supaya ketika pengguna menutup software aplikasi *web browser* sudah tidak meninggalkan jejak digital lagi dalam komputernya (Dharan 2014).

Menurut Chivers (2013) pada *mode private browsing* saat beraktifitas internet menjadi pembatas atau pencegahan dalam analisa forensik digital. Hal ini dikarenakan pada saat menggunakan *web browser* dengan *mode private browsing* jejak digital seperti *history* dan bukti digital lainnya tidak terekam oleh *web browser*, padahal *web browser* didesain untuk menyimpan setiap informasi seperti file *history, URLs*, pencarian dan *password* yang berkaitan dengan aktifitas pengguna *web browser* tersebut (Dharan 2014).

Namun sayangnya, adanya fitur *mode private browsing* ini menjadi momok sendiri bilamana hal tersebut digunakan untuk kejahatan, apalagi dengan adanya browser yang bernama Browzar, dalam website resminya disebutkan bahwa tidak akan meninggalkan jejak dalam artian bukti digital dari browser tersebut.

Browzar merupakan *portable web browser* yaitu *web browser* yang terinstal pada sebuah disk eksternal yang diluar dari perangkat dalam computer yang tujuannya untuk *personalisasi sesi browsing* pengguna. Ditambahkannya penggunaan *mode private* ketika menggunakan *portable web browser*, apabila oleh oknum yang paham kemudian melakukan *anti forensik* dengan menghapus *registry* maka dapat mengurangi interaksi aktivitas *browsing* dengan disk komputer yang berguna untuk menghilangkan jejak dan semakin aman dalam transaksi di internet. Registry adalah sebuah informasi database computer yang merekam setiap aktifitas di computer baik ketika ada hardware baru ataupun aktifitas software yang berjalan. Sehingga hal tersebut menjadi tantangan tersendiri bagi investigator ketika melakukan forensik atau menyelidiki aktifitas internet tersangka dalam kasus cybercrime yang menggunakan web browser (Dharan 2014).

Penelitian tentang bukti digital pada web browser yang sudah dilakukan umumnya adalah seputar instalasi normal dan portable baik normal maupun mode private. Hal ini seperti yang dilakukan oleh (Aggarwal, G. et al., 2010), (Noorulla, E. S., 2014), (Dharan 2014), namun penelitian tersebut lebih fokus pada eksplorasi bukti digital untuk web browser pada instalasi normal, mode private pada instalasi normal, portable pada mode private dan mereka lebih focus di web browser popular yang biasa digunakan oleh kebanyakan pengguna, belum pada tahap anti

forensik penghapusan registry dan browser khusus yang memang dirancang sudah portable dan ada anti forensic didalamnya.

Oleh karena itu perlu dilakukan penelitian untuk mengetahui bagaimana karakteristik bukti digital dari penggunaan anti forensik pada portable web browser dengan mode private tersebut apakah sama dengan web browser pada umumnya ketika menggunakan web browser pada umumnya. Di samping hal itu penelitian yang ada untuk analisa karena menggunakan web browser yang sudah popular digunakan, maka tahapan kerangka investigasi sudah bisa langsung menuju ke tahapan penentuan engine browser atau jenis browser yang digunakan. Kemudian, bagaimana jika web browser tersebut asing terdengar dan belum begitu popular digunakan, maka disini perlu adanya sebuah kerangka tahapan investigasi langkah apa yang seharusnya dilakukan terlebih dahulu sebelum melakukan investigasi live forensik untuk mengefisienkan waktu analisa forensik.

Penelitian yang sudah ada dari (Dharan 2014), membahas tentang analisa live dan offline mencari bukti digital dari browser baik pada instalasi normal pada computer ataupun portable dengan mode normal dan juga mode private. Oleh karena itu, tema yang diajukan dalam penelitian ini adalah dengan live forensik yang terjadi ketika ada proses anti forensik seperti yang telah disebutkan di atas. Live forensik ini juga merupakan solusi yang tepat dalam menganalisa nantinya dan dalam analisa ini adalah dengan mencari bukti digital dari data dalam memori RAM. Tentu saja dalam penerapan live forensik ini juga harus disesuaikan dengan kasus yang ada yaitu dalam penelitian ini adalah web browser. Diharapkan hasil dari penelitian ini dapat mengembangkan kerangka tahapan live forensik untuk melakukan investigasi forensik khususnya untuk kasus web browser dan dapat membantu investigator dalam mencari bukti digital dan menambah ilmu pengetahuan yang terkait tentang live forensik dan analisis browser portable mode private yang ditambah anti forensik pada aktifitas setelah browsingnya.

1.2 Rumusan Masalah

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

1. Bagaimana karakteristik bukti digital dari penggunaan *anti forensik* di *portable web browser* dengan *mode private browsing*?
2. Bagaimana kerangka tahapan *live forensic* untuk melakukan investigasi *anti forensik* di *portable web browser* dengan *mode private browsing*?

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 anti forensik pada saat browsing menggunakan portable web browser mode private.
   a. 1 unit laptop yang digunakan untuk melakukan aktifitas browsing.
   b. 2 unit usb flashdisk, usb flashdisk pertama sebagai media penyimpanan software portable (mozilla firefox, google chrome, internet explorer, browzar dan cleanafterme), dan usb flashdisk kedua sebagai media penyimpanan software procmon dan dumpit yang digunakan sebagai tahap awal langkah investigasi forensik.
2. Membandingkan hasil analisa pada simulasi penelitian yang terdapat 3 simulasi yang akan dilakukan pada penelitian ini.
3. Fokus pada bahasan analisa browser terutama pada Browzar.
4. Objek analisa hanya pada history url, search keyword, password dan timestamp.
5. Proses investigasi forensik menggunakan metode live forensik, disesuaikan dengan kasus akuisisi data pada memori RAM, 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 *anti forensik* di *portable web browser* dengan *mode private browsing*.
2. Melakukan tahapan *live forensic* untuk melakukan investigasi anti forensik pada *portable web browser mode private browsing.*

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari hasil penelitian ini adalah sebagai berikut :

1. Pengetahuan tentang bagaimana menerapkan keamanan dalam transaksi ketika menggunakan browser.
2. Memberikan pengetahuan dasar portable web browser mengenai layanan mode private pada web browser tersebut dan penanganan bagaimana investigasi dilakukan jika ada kejahatan cyber pada kasus tersebut.

3. Dapat mengetahui proses untuk mendapatkan bukti digital pada layanan mode private pada web browser portable.
4. Melengkapi penelitian-peneltian sebelumnya dan mengembangkan dari saran penelitian sebelumnya tentang forensik web browser di portable web browser bagaimana pengumpulan barang buktinya.

1.6 Review Penelitian

Pada penelitian akan difokuskan pada analisa forensik dengan analisa live forensik dari sebuah *portable web browser*. Penelitian sebelumnya oleh (Aggarwal et al. 2010) menyatakan bahwa mereka menganalisis *browser mode private* di empat web browser yang populer dan menyarankan penggunaan *private browsing* yang berbeda pada umumnya karena dari hasil penelitiannya untuk mencapai tujuan *security* masih banyak kelemahan terutama dari sisi jika ada *ektensi* dan *plugin* yang tertanam pada *browser* tersebut.

Soghoian (2010), melakukan penelitian serupa dan menyimpulkan bahwa beberapa pengguna mengabaikan peringatan *browser* tentang pembatasan fitur *private browsing*. Mereka menyimpulkan bahwa *private browsing* tidak terjadi pelacakan online oleh pihak ketiga.

Penelitian di tahun berikutnya oleh (Said, Mutawa, Awadhi, & Guimaraes, 2011) hasil penelitiannya menyatakan bahwa mampu mengembalikan rekam jejak pada histori *browser* di *mode private* yang terdapat pada sistem komputer di tiga jenis *browser*.

Penelitian oleh (Choi et al 2012) menyimpulkan bahwa forensik browser web adalah bagian yang paling penting dalam forensik digital terakhir karena menganalisis kepentingan tersangka atau riwayat penelusuran. *Web browser portabel* dapat dijalankan pada *removable media* agar tidak menyimpan sejarah internet pada sistem operasi. *Portabel web browser* menyimpan sejarah internet di folder diinstal, sementara web browser biasa menyimpan sejarah internet dalam sistem operasi. Sejarah internet dapat dengan mudah dihapus oleh alat optimasi sistem atau alat *anti-forensik.* Karena itu, sulit untuk memutuskan apakah akan digunakan *web browser portabel* di komputer tersangka. Jika tidak ada sejarah internet di komputer tersangka, penyidik harus mengkonfirmasi jejak oleh *web browser portabel.*

Penelitian serupa oleh (Ohana, 2013) mengatakan bahwa pada *browser* internet explorer masih dapat menemukan rekam jejak yang bisa dijadikan bukti digital dari *mode private* pada internet explorer dan itu cukup untuk mereka ulang dan menemukan jejak dari histori dan sesi waktu *browsing*.

Tahun yang sama penelitian (Lerner et al. 2013) mempelajari bagaimana dampak ekstension browser pada mode private browsing. Mereka menciptakan sebuah sistem untuk menganalisis

ekstensi JavaScript dan mengamati di mode private browsing, memantau beberapa kejanggalan pada mode private browsing di ekstensionnya.

Satvat et al. (2013) juga melakukan analisis private browsing di empat browser populer dengan *threat mode* yang lebih rinci yaitu local dan remote attack. Remote attack berkaitan dengan serangan jarak jauh dan kurangnya kontrol yang tepat pada *ekstensi* di *mode private* dan kurangnya pengujian pada kasus tertentu semisal program ketika *crash* ataupun penambahan yang lain semisal bookmark.

Satvat et al. (2014) kembali melanjutkan penelitian yang serupa dari yang sebelumnya tentang pendekatan forensik pada *private web browser*. Mereka menyampaikan bahwa masih banyak kerentanan yang bisa terjadi dari implementasi pada keempat *browser* popular yang pada intinya adalah masalah keamanan, hal ini didasarkan pada vendor *browser* yang bisa saja mengabaikan akan hal ini karena dianggapnya tidak penting keamanan pada sisi browser. Dan pendekatan yang lebih sistematis perlu diujikan khususnya pada *private web browser* dengan beberapa *model threat* untuk mengetahui tolak ukur hal keamanan yang sering dilupakan semisal ketika *aplikasi crash*, penambahan yang lain *bookmark* atau *ekstensi browser* juga harus diujikan.

Gao, Yang, Fu, Lindqvist, & Wang, (2014) juga melakukan penelitian pada *browser mode private* dan menyatakan bahwa masih banyak yang tidak mengetahui tentang mode private dan kegunaannya, namun juga beberapa partisipan juga menggunakannya agar tidak meninggalkan jejak digital saat mereka mengakses internet, oleh sebab itu mereka menyarankan agar *mode private* dibuat lebih menonjol di menu atau ada pop up sebagai pengingat dan memberikan pengertian bahwa *mode private* penting untuk menjaga privasi saat berinteraksi di internet.

Penelitian serupa oleh (Noorulla, 2014) mengatakan bahwa beberapa vendor browser mengungkapkan tidak menyimpan jejak pada *mode private*, namun dari penelitiannya dengan menggunakan metode pengambilan file system dan memori, masih ada beberapa *browser* yang meninggalkan jejak. Dan pada penelitian tersebut pada mode privasi dicondongkan untuk menggunakan Google Chrome dan Firefox daripada browser lainnya.

Penelitian ini termotivasi oleh ulasan dan penelitian dari (Dharan, 2014) yang mana sudah disimpulkan bahwa pemeriksaan dengan secara live lebih banyak untuk mendapatkan informasi lebih daripada secara offline. *Sistem volume information* dan file *prefect* pada windows menjadi informasi utama yang bisa dijadikan dalam proses investigasi. Pada penelitiannya dikembangkan sebuah IR Toolkit untuk analisis live dan dengan mengembangkan metodologi untuk mendapatkan bukti digital sebanyak mungkin. Penelitian tersebut juga mengembangkan sebuah tool yang memiliki tampilan dan penggunaan yang mudah dalam proses investigasi dengan tujuan investigasi menjadi lebih efektif.

Beberapa review terkait penelitian di atas dirangkum dalam Tabel 1.3 dan usulan penelitian yang akan dilakukan.

Tabel 1. 3 Review Penelitian Browser Forensik

Peneliti	Domain Penelitian	Metode/Tools	Keterangan
Aggarwal (2010)	Analisis modern browser mode private	Menggunakan metode otomasi tool untuk pengujian keamanan browsing.	Masih banyak celah untuk mencapai tujuan keamanan.
Soghoian (2010)	Mode private browsing	-	Mode private browsing tidak terjadi pelacakan online oleh pihak ketiga.
Huwida Said, Noora Al Mutawa, Ibtesam Al Awadhi dan Mario Guimaraes (2011)	Analisis artifacts private browsing	Menggunakan tool Cache and History View, Encase dan penelitian ini dalam virtual.	Tidak ada bukti yang ditampilkan saat private browsing, namun masih ada di sistem computer.
Jong-Hyun Choi , Keun-gi Lee , Jungheum Park , Changhoon Lee, dan Sangjin Lee (2012)	Analisis artifact portable web browser	Framework deteksi portable web browser	Membuat framework analisis pendeteksian artifact di portable browser.
Ohana (2013)	Sessions portable web browser	Menggunakan Nirsoft Internet tool, AccessData FTK Imager untuk analisa.	Mengusulkan metodologi untuk menganalisis artefak web browsing pribadi dan portabel
Benjamin S. Lerner, Liam Elberty, Neal Poole, dan Shriram Krishnamurthi (2013)	Ektensi web browser mode private	-	Membuat sebuah sistem tipe statis untuk menganalisis ekstensi JavaScript diamati dari mode penjelajahan pribadi.
Satvat (2013)	Portable private browsing	-	Bukti yang dapat diambil tergantung browser yang digunakan.
Kiavash Satvat, Matthew Forshaw, Feng Hao, Ehsan Toreini (2013)	Privasi private browsing	Pendekatan forensik untuk mengumpulkan dan menganalisis data residual pada komputer	Masih banyak celah keamanan yang belum diketahui.
Xianyi Gao, Yulong Yang, Huiqing Fu, Janne Lindqvist, dan Yang Wang (2014)	Perlindungan privasi private browsing	-	Pengusulan desain untuk pemahaman tentang private browsing di web browser yang berbeda.

Tabel Lanjutan Review Penelitian Browser Forensik

Peneliti	Domain Penelitian	Metode/Tools	Keterangan
Emad Sayed Noorula (2014)	Analisis web browser private browsing	Melakukan forensik file sistem dan memori pada computer.	Bukti digital masih tersisa pada memori dan di sebagian browser bukti digital terdapat di file sistem.
Divyesh G Dharan D (2014)	Rekontruksi artefak di portable web browser	Melakukan forensik analisa live dengan IR Toolkit.	Pembuatan toolkit untuk analisa berupa tampilan GUI yang memudahkan proses investigasi.
Usulan Penelitian	Analisis anti forensik di portable web browser mode private	Analisis forensik dengan metode live forensik	-
	Dari beberapa review penelitian sebelumnya, belum ada yang meneliti terkait usulan penelitian ini, yaitu melakukan analisis pada aktifitas browsing menggunakan portable web browser mode private khususnya Browzar setelah dilakukan proses anti forensic. Diharapkan dari penelitian ini bisa menghasilkan suatu rumusan baru, analisa live forensik untuk menemukan bukti digital yang tersisa di RAM.		

1.7 Metodologi Penelitian



Gambar 1. 2 Alur Metodologi Penelitian

Dari sketsa metodologi penelitian pada Gambar 2.2 menunjukkan proses secara garis besar penelitian ini dari awal sampai akhir yang menggunakan beberapa tahapan metode penelitian yang akan dijelaskan dibawah ini:

1. **Studi Literatur**

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

2. **Persiapan dan Identifikasi Kebutuhan**

Tahapan ini merupakan suatu proses persiapan alat dan bahanyang akan digunakan dalam melakukan penelitian untuk keperluan simulasi sampai dengan investigasi forensik akan dilakukan, seperti toolsbantuan, hadware maupun software yang dapat digunakan dalam penelitian.

3. **Skenario dan Simulasi Studi Kasus**

Pada tahap skenario dan studi kasus dibuat sebuah rencana bagaimana penggunaan web browser portable dengan melakukan aktifitas di internet. Dari skenario tersebut kemudian diimplementasikan pada studi kasus sesuai topik yang akan diteliti yaitu web browser portable yang terdapat pada sebuah flashdisk. Sehingga dari adanya studi kasus dari skenario yang dibuat bisa dilakukan penelitian untuk mensimulasikan bagaimana investigasi dilakukan.

4. **Investigasi Forensik**

Merupakan tahap dilakukannya proses investigasi live forensic terhadap simulasi kasus anti forensik pada browser portable mode private. Investigasi yang dilakukan meliputi pra analisis, analisis dan pasca analisis

5. **Penyusunan Kerangka Investigasi Forensik**

Tahapan dimana berupa rancangan framework yang digunakan untuk menangani kasus yaitu analisa browser portable yang jarang diketahui sehingga diperlukan informasi engine apa yang digunakan browser tersebut dan plugin apa yang nantinya akan sesuai digunakan untuk keperluan analisa.

6. **Laporan**

Tahap terakhir adalah melakukan dokumentasi terhadap penelitian yang dilakukan agar bisa menjadi sebuah karya ilmiah dan memungkinkan sebagai referensi penelitian yang berkaitan di topik yang dibahas.

1.8 Sistematika Penulisan

Untuk memudahkan pembahasan dalam penelitian ini maka dibuat sistematika penulisan pada penelitian ini yaitu:

BAB I PENDAHULUAN

Bab ini merupakan pengantar terhadap permasalahan pada topic penelitian yang akan dibahas. Dalam pendahuluan ini disampaikan tentang gambaran dari penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, review penelitian, metodologi penelitian serta sistematika penulisan.

BAB II KAJIAN PUSTAKA

Bab ini merupakan penjelasan dari teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan Web Browser Portabel, Analisa Live Forensik, Digital Forensik dan Memori Forensik.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langkah-langkah penelitian dan bagaimana proses dalam penyelesaian kasus, sehingga dengan tahapan tersebut diharapkan memudahkan dan memberika hasil yang maksimal.

BAB IV PEMBAHASAN DAN HASIL

Bab ini berisikan tentang pembahasan dan hasil terhadap rumusan masalah, yang mencakup pembahasan penyelesaian masalah yang diangkat, simulasi kasus, dan penentuan hasil analisis.

BAB V KESIMPULAN DAN SARAN

Simpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.