 ISSN: 2721-0901

Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito)

Mu'Minin[a,1,*] dan Nuril Anwar[a,2]

[a]*Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan*
Jl. Ringroad Selatan, Kragilan, Tamanan, Banguntapan, Bantul 55191, Yogyakarta, Indonesia
[1] *mu1400018190@webmail.uad.ac.id;* [2] *nuril.anwar@tif.uad.ac.id*

INFORMASI ARTIKEL

Diterima : 28 – 07 – 2020
Direvisi : 15 – 08 – 2020
Diterbitkan : 31 – 08 – 2020

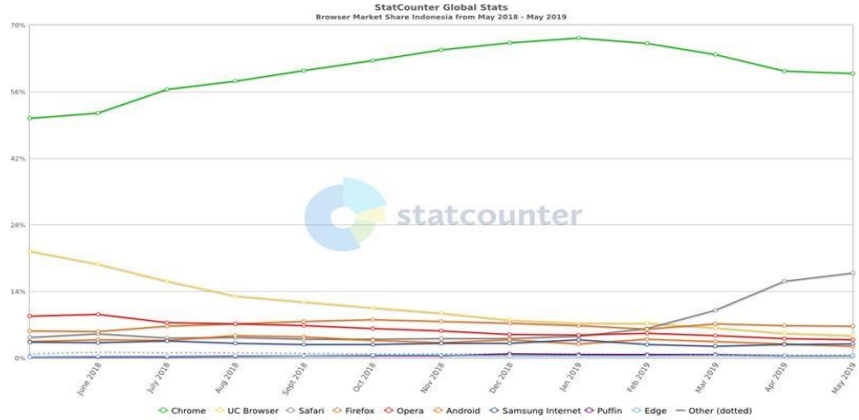
Kata Kunci:
Browser
Digital Evidence
Digital Forensic
Incognito
Live Forensic

ABSTRAK

Browser merupakan program aplikasi perangkat lunak yang digunakan untuk mengakses internet baik dari perangkat *desktop* maupun *mobile*. *Browser* tersebut digunakan untuk mencari segala macam informasi yang tersedia di dunia internet. *Browser* terdapat fitur mode *incognito* yang digunakan dalam menjelajah informasi di internet. Fitur ini diklaim tidak menyimpan data penelusuran pribadi, seperti riwayat penelusuran, *cookies, cache*, dan kata sandi, di penyimpanan *browser*. Namun *browser mode incognito* dapat meninggalkan barang bukti digital di sistem. Hal ini menjadi tantangan bagi forensik investigator untuk melakukan investigasi forensik dan mencari barang bukti digital *(digital evidence)* dari *browser mode incognito*. Investigasi forensik yang dilakukan investigator dilakukan sesuai dengan prosedur forensik digital dalam mencari barang bukti. Investigasi forensik terdapat metode yang digunakan dalam mencari barang bukti yaitu *live forensic* dan *post morterm analytic*. *Post morterm analytic* merupakan metode investigasi yang dilakukan setelah terjadi tindak kejahatan sedangkan *live forensic* yaitu metode investigasi yang dilakukan saat tindak kejahatan berlangsung. Dalam penelitian ini, investigator menggunakan metode *live forensic.* Penelitian yang dilakukan menggunakan metode *live forensic* mampu mendapatkan dan membuktikan bahwa penggunaan *browser mode incognito* masih meninggalkan informasi berupa barang bukti digital dari pengguna. Barang bukti yang ditemukan yaitu berupa *browsing history, web search, password, username, visited url*. Barang bukti kemudian digunakan dipengadilan untuk menentukan proses tindak pidana pada pelaku.

I. Pendahuluan

Browser adalah perangkat lunak yang berfungsi untuk menerima dan menyajikan sumber informasi dari internet. Browser menjadi sangat penting dalam dunia internet karena tanpa adanya browser, user tidak bisa mengakses ke internet. Browser di era sekarang telah banyak berkembang baik dari segi kualitas maupun kuantitas. Browser yang digunakan oleh user memiliki Persentase penggunaan yang berbeda. Berdasarkan statistik yang di diungkapkan oleh media survei statcounter dari periode mei 2018 s/d mei 2019 google chrome menjadi browser yang paling banyak digunakan dengan presentase tertinggi diikuti UC Browser, Safari, Firefox, Opera seperti Gambar 1 ;



Gambar 1. Statistik Penggunaan Browser

Data pada Gambar 1 menunjukan bahwa chrome merupakan browser ter-populer bagi pengguna internet. Browser-browser tersebut menyediakan fitur penjelajahan mode normal dan penjelajahan pribadi atau disebut juga mode incognito. Pada fitur penjelajahan mode normal semua aktifitas yang dilakukan di browser tersebut terekam dan disimpan disistem. Aktifitas-aktifitas yang telah dilakukan bisa dilihat di riwayat browser atau bisa melalui sistem windows-nya. Sedangkan pada mode incognito, memiliki fungsi untuk tidak menyimpan session apapun di dalam penggunaannya. Fitur mode incognito memungkinkan pengguna untuk menjelajah web tanpa menyimpan data pada sistem mereka yang dapat diambil oleh penyelidik. Mode privasi juga menonaktifkan penyimpanan data di cookies dan menelusuri basis riwayat data. Perlindungan ini hanya tersedia untuk perangkat lokal karena masih mungkin untuk mengidentifikasi situs web yang dikunjungi dengan mengaitkan alamat IP (Internet Protocol) di situs web.

Pada tahun 2016 yakni dari kepolisian melalui CNN (Cable News Network) Indonesia mengungkapkan bahwa jumlah kejahatan di Indonesia mencapai 1627 kasus yang ditangani polisi. Kasus- kasus tersebut 1207 merupakan kejahatan dunia maya atau dikenal dengan sebutan cybercrime, yang berupa provokasi, penipuan, penyebaran berita hoax, pembobolan situs, pronografi, hingga pencurian data atau informasi penting oleh pihak ketiga yang dapat merugikan pihak lain. Tindak kriminal yang dilakukan pelaku kriminal cybercrime tersebut dilakkukan dengan penjelajahan dengan mode incognito.

Kondisi ideal browser, catatan website yang dikunjungi ketika dalam mode incognito tidak boleh ditinggalkan pada komputer pengguna. Namun, terdapat kelemahan pada mode incognito yaitu seputar jejak yang ditinggalkan pada memori. Riwayat- riwayat dari penjelelajahan yang dilakukan melalui browser mode incognito masih bisa ditemukan dengan dilakukan aksi atau penyelidikan forensik terhadap cache dari aplikasi tersebut [1].

Forensik dalam pendekatannya untuk menemukan suatu barang bukti digunakan metode live data forensic dan post mortem analysis. Karena live data forensic lebih baik dari pada post mortem analysis terutama di bagian keamanan, maka di penelitian ini penulis menggunakan metode live data forensic [2].

Analisis menggunakan live data forensic pada volatile memori mengurangi terjadinya hal yang membahayakan pada barang bukti. Hal tersebut dikarenakan kita mencapture RAM (Random Access Memory) yang berisi semua data-data pada sistem yang dapat berupa process, registry, file dan system atau aplikasi tertentu pada system [3]. RAM dalam sistem berfungsi sebagai jembatan antara hardisk dengan processor jadi seluruh proses yang ada pada sistem akan tercatat di memori sehingga meminimalisir terjadinya hal yang membahayakan barang bukti. Bahkan dalam keadaan mati peneliti tetap dapat melakukan proses analisis dari hasil capture RAM tersebut. Proses capture RAM, investigator dalam melakukan investigasi menggunakan forensic sleuth kit seperti RAM Capturer, winhex sedangkan untuk proses autopsy menggunakan tool autopsy.

Penelitian yang dilakukan oleh [4] dengan judul penelitiannya *A Study of the Internet Privacy in Private Browsing Mode.* Penelitian ini dilakukan dengan skenario pengguna menyediakan informasi pribadi dengan kehendaknya, dan atau informasi diakses tanpa kesadaran pengguna. Pengguna melakukan pengiriman e-mail dengan proxy tertentu. Hasil penelitiannya yaitu baik dilakukan dengan kehendaknya atau dengan user yang lalai data bisa ditemukan dari komputer pengguna maupun dari sumber eksternal.

Penelitian lainnya [5]dengan judul "*On the Privacy of Private Browsing –A Forensic Approach".* Penelitian yang dilakukan mendapatkan beberapa data dari aktifitas yang dilaukandi dalam *web browser* diantaranya *bookmark, sqlite database, extension, crossmade interference, hyperlink, cookie timing, external element, memory, file timestamp*. Penelitian menyimpulkan bahwa apabila mengunakan browser, seharusnya di buka dengan single mode guna menghindari hal yang telah disebutkan diatas disalahgunakan oleh pihak lain.

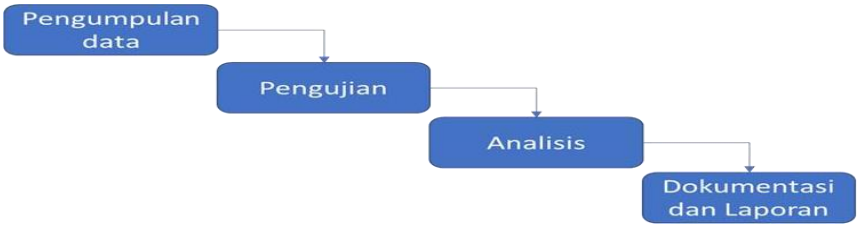
Penelitian lainnya yang dilakukan [6] dengan judul *Forensics Analysis of Residual Artefacts Acquired During Normal and Private Web Browsing Sessions.* Hasil penelitiannya yaitu aktifitas yang dilakukan di dalam web browser berupa nama pengirim *e-mail*, nama penerima *e-mail* dan *URL* yang dikunjungi oleh pelaku serta *keyword* yang menjadi kata pencarian ditemukan. Aktifitas tersebut ditemukan dari file yang sudah terhapus. Penelitian berikutnya oleh [7] yang berjudul *Private web browser forensic : a case study of the epic privacy browser* menghasilkan barang bukti berupa *history, chache, cookies, download.*

Browser merupakan salah satu aplikasi yang berguna untuk menerjemahkan *HTML* menjadi Bahasa yang dapat dipahami oleh *user* [8]. Contoh *browser*-nyaadalah *google chrome, mozilla firefox, internet explorer, opera* dan lain-lain. *Browser-browser* tersebut mempunyai fitur diantaranya : (a) *Normal Browsing* merupakan kegiatan menjelajahi internet dimana *cache,cookies, history* dan yang lainnya masih tersimpan di dalam browser. (b) Incognito Browsing merupakan kegiatan menjelajahi internet dimana cache dan history-nya tidak tersimpan di dalam browser. (2) Browser Forensik. Browser forensik adalah proses investigasi forensik yang dilakukan terhadap browser untuk menemukan informasi atau barang bukti digital yang tersimpan didalam web browser saat atau setelah digunakan. Barang bukti digital yang dapat ditemukan pada browser antara lain *cache, history, download, video, dan session* [9]. Sedangkan menurut [10] terdapat ketentuan tertantu dari barang bukti digital yang dapat ditemukan didalam *browser mode incognito* yaitu : (a) *false sense of security* merupakan suatu keadaan atau ketika menggunakan logika dimana browser mode normal membuat perintahuntuk me-*write* data di partisi *disk* maka *mode incognito* juga me-*write* data

di partisi *disk*. Kesimpulannya browser benar-benar tidak menjamin kerahasiaan dan privasi aktifitas browsing pengguna. (b) Deteksi *Incognito Mode* yaitu Ekstraksi barang bukti dari mode *private/incognito* berbeda dengan mode normal sehingga investigator harus bisa mengetahui apakah investigasi mengunanakan mode private atau tidak. Indikasi sederhananya untuk *private mode* yaitu adanyaincognito sign dan tidak adanya bar tab sebelumnya. Ketika browser ditutup investigator bisa menjalankan *Cross-mode Interference inspector* untuk melihat apakah mode private diaktifkan dan dimana data disimpan [11]. Jadi sebelum percobaan, *browser* sebaiknya di *uninstall* dan di *re-install* agar tidak terjadi kesalahan untuk menentukan mana barang bukti yang berasal dari mode normal dan mode private. (3) Komputer forensik. Komputer forensik merupakan salah satu cabang ilmu digital forensik yang berhubungan dengan bukti digital yang ditemukan didalam komputer maupun media penyimpanan digital [7].

II. Metode

Bidang ilmu yang dimanfaatkan dan dilibatkan pada suatu tindak kejahatan atau kriminal bisa dimanfaatkan untuk kepentinganhukum dan keadilan, dimana ilmu tersebut dikenal dengan ilmu forensik. Menurut [8] tahapan komputer forensik meliputi indetifikasi, persiapan, ekstraksi, dan interprestasi dari data yang terdapat pada komputer untuk dijadikan barang bukti digital dari *cybercrime*. Sedangkan menurut *National Institute of Standard and Technology* (NIST), terdapat 4 fase dalam komputer forensik yaitu seperti pada Gambar 2 berikut ;



Gambar 2. Tahapan Komputer Forensik

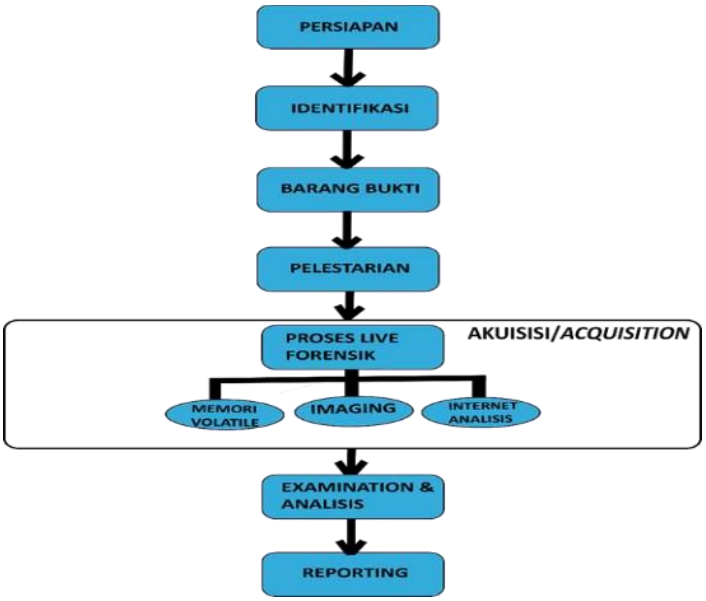
Menurut [12] didalam pengangkatan barang bukti dapat dilakukan dengan 2 cara yaitu *post morterm analysis* dan *live forensic*. Post morterm analysis merupakan suatu teknik yang membutuhkan data yang tersimpan secara permanen dalam perangkat media penyimpanan umumnya hardisk. *Live forensic* yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada system atau data volatile yang umumnya tersimpan pada *Random Access Memory* (RAM) atau transit pada jaringan analisa dilakukansaat sistem belum shut down. Investigasi secara live forensic lebih terjamin dalam mendapatkan barang bukti digital. [4] Digital forensik. Digital Forensik merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital[13]. Pada saat melakukan investigasi digital forensik memerlukan tahapan-tahapan untuk memperoleh barang bukti, menurut [14] tahapan tersebut meliputi *preservation, collection, examination, analysis dan reporting* yang mengacu dan sesuai dengan tahapan National Institute of Standard and Technology (NIST) seperti Gambar 3 berikut ;

Gambar 3. Tahapan Forensik Digital

Tahapan pada Gambar 3 mempunya penjelasan sebagai berikut : (a) Pelestarian atau *freezing the crime scene* merupakan tahap untuk menghentikan atau mencegah aktifitas yang dapat merusak informasi digital yang dikumpulkan. Pelestarian melibatkan operasi seperti mencegah orang menggunakan komputer selama pengumpulan bukti, menghentikan proses penghapusan yang sedang berlangsung dan memilih cara teraman untuk mengumpulkan informasi. (b) Koleksi merupakan tahap pengumpulan terdiri dari temuan dan pengumpulan informasi digital yang mungkin relevan dengan peyelidikan. Karena informasi digital tersimpan di komputer, kumpulan informasi digital berarti pengumpulan peralatan yang berisi informasi, atau merekam informasi pada beberapa media. Pengumpulan data dilakukan dengan melakukan pengamanan barang bukti yang digunakan pelaku baik itu hardware maupun software. (c) Pemeriksaan terdiridari pencarian bukti yang sistematis dengan kejadian yang sedang diselidiki. Hasil pemeriksaan adalah data yang ditemukan dalam

informasi yang dikumpulkan, termasuk file log, file data, times stamps dan lainnya. (d) Analisa bertujuan untuk menarik kesimpulan dari barang bukti yang ditemukan berdasarkan kasus yang terjadi. (e) Proses mempersiapkan laporan secaraterperinci, dan menyimpulkan hasil dari investigasi untuk disajikan secara detil dari semua artefak yang berkaitan dengan penggunaan browser mode incognito untuk mengungkap kasus yang sudah diskenariokan

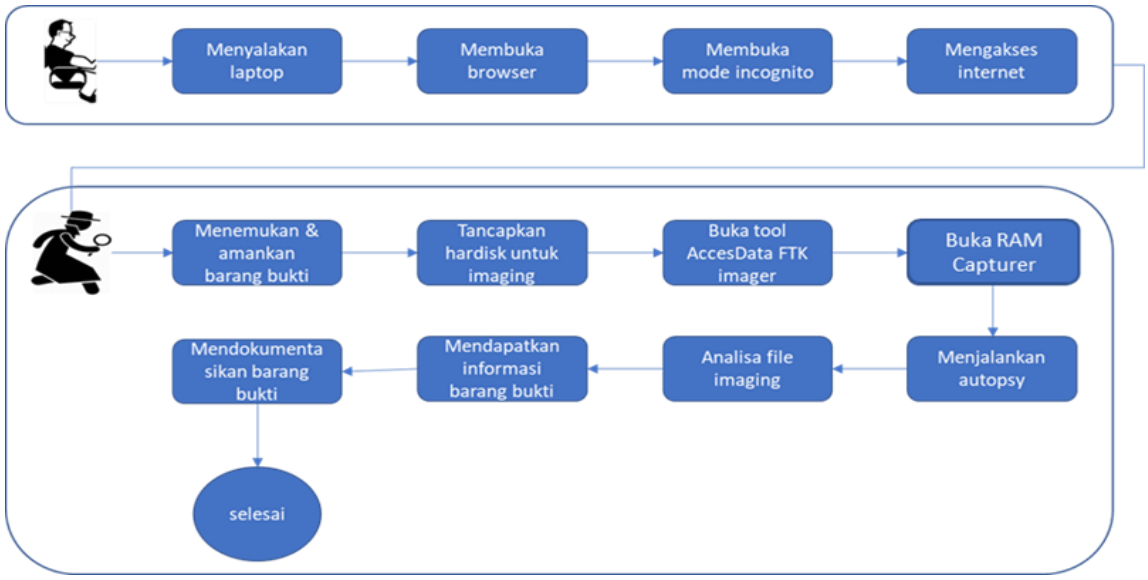
Metode yang digunakan dalam penelitian adalah metode investigasi dengan *live forensic*. Metode *live forensic* merupakan metode investigasi forensik yang dilakukan ketika barang bukti masih keadaan menyala. Tahapannya seperti Gambar 4 berikut ;



Gambar 4. Tahapan Investigasi Live Data Forensik

Tahap pada Gambar 4 merupakan proses dilakukannya metode live forensic yang penjelasannya sebagai berikut : (1) Persiapan merupakan tahapan paling awal yaitu mempersiapkan keperluan investigasi baik itu perangkat keras (*hardware*) maupun perangkat lunak (*software*). (2) Identifikasi merupakan tahap mencari tahu barang bukti apa yang didapat dimana dan bagaimana cara penyimpanannya agar dapat diketahui cara penanganannya. (3) Barang bukti utama yang didapat berupa komputer/laptop yang digunakan pelaku. (4) Pelestarian merupakan proses dimana investigator melakukan pemeliharaan, pengumpulan data, pendokumentasian barang bukti, dan pengamanan baik itu lokasi maupun evidence. (5) Akuisisi yaitu proses dimana barang bukti yang diakuisisi berdasarkan keadaan di lokasi kejadian barang bukti ditemukan. Apabila laptop yang digunakan pelaku masih dalam keadaan hidup/turn on akan dilakukan metode investigasi live forensic namun bila dilokasi kejadian laptop sudah dalam keadaan mati/turn off maka dilakukan tahapan dead forensic khususnya flashdrive yangdigunakan pelaku. Penjelasan secara terperinci dari proses akuisisi sebagai berikut : (a) *memory volatile* merupakan tahap *imaging* terhadap *random access memori* (RAM) untuk mendapatkan informasi, menggunakan bantuan *tools forensic* Belkasoft RAM *capture memory*. (b) *Imaging* Merupakan proses akuisisi dari isi *flashdrive* untuk diamankan yang akan dianalisa ke proses selanjutnya. (c) internet analisis merupakan Analisa aktifitas internet yang dijalankan pelaku pengunaan browser mode incognito. (6) *Examination* dan *Analysis* merupakan prosesinvestigator dapat melakukan eksplorasi, analisa secara mendalam dan mengungkap apa yang didapat dari hasil serangkaian olah investigasi dari kasus yang sudah diskenariokan hingga memperoleh informasi penting. (7) Pelaporan/reporting adalah tahapan dimana investigator melaporkan secara terperinci dari hasil analisis yang sudah dilakukan dan melakukan penyimpulan dari rangkaian investigasi yang sudah dilakukan.

Skenario penelitian merupakan tahapan awal dalam menggambarkan penelitian yang akan dilakukan. Skenario yang dilakukan memerlukan perlengkapan sebagai berikut : (1) *Software*. (a) sistem operasi, (b) browser, (c) tool autopsy, (d) FTK imager, (e) RAM capturer,
(f) Winhex. (2) Hardware. (a) PC, (b) Processor, (c) RAM. Alat-alat tersbut akan digunakan untuk skenario yang dilakukan seperti Gambar 5 berikut ;



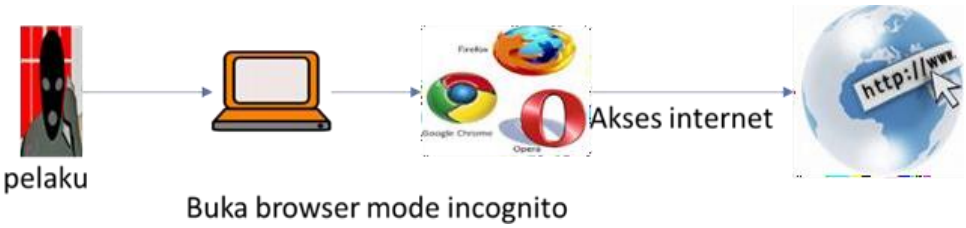
Gambar 5. Skenario Penelitian

Gambar 5 menjelaskan bahwa pelaku menggunakan browser mode incognito dimulai dari menyalakan laptop sampai pengaksesan internet. Dari aktifitas yang dilakukan pelaku, didapatkan informasi penting yang berupa alamat website yang sedang dikunjungi sebagai barang bukti di browser. Sedangkan username, password, e-mail,cache,history serta informasi lain yang bisa didapatkan melalui imaging sistem. Investigator melakukan penyitaan terhadap barang bukti untuk dijadikan sebagai barang bukti di pengadilan. Tujuan dilakukan penyitaan yaitu untuk mengamankan barang bukti digital yang ada agar barang bukti terjaga keasliannya. Kemudian investigator melakukan imaging terhadap barang bukti yang diamankan dengan menggunakan FTK imager. Setelah dilakukan imaging tahap selanjutnya yaitu analisis terhadap hasil imaging dengan autopsy. Ketika autopsy selesai dilakukan, data terkelompokan secara otomatis. Investigasi yang dilakukan investigator terhadap barang bukti menghasilkan informasi yang digunakan untuk laporan investigasi di ranah hukum. Skenario kasus yang diangkat dalam penelitian ini adalah kasus tentang perdagangan bayi ilegal melalui media sosial *twitter* dan *facebook*.

III. Hasil dan Pembahasan

A. Simulasi Browser mode Incognito

Proses simulasi merupakan proses dimana pelaku melakukan aktifitas diinternet dengan *browser mode incognito* seperti Gambar 6 berikut ;

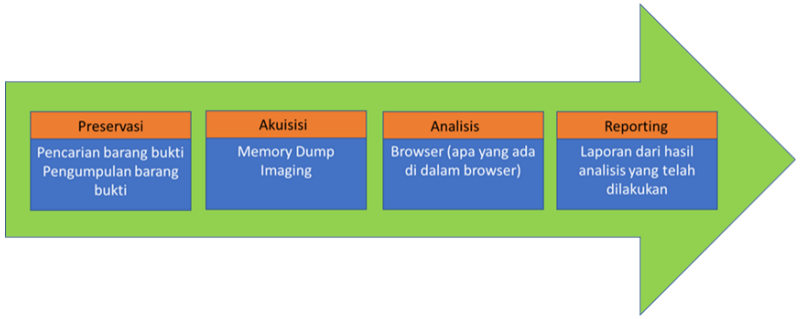


Gambar 6. Simulasi Browser mode Incognito

Gambar 6 menjelaskan skenario bagaimana pelaku menggunakan *browser mode incognito* untuk login ke suatu website dan aktifitas lain yang dilakukan pelaku dimana pelaku pertama membuka laptop kemudian dilanjutkan dengan membuka *browser* dan masuk ke mode incognito setelah itu pelaku melakukan *browsing* ke suatu website.

B. Proses Investigasi

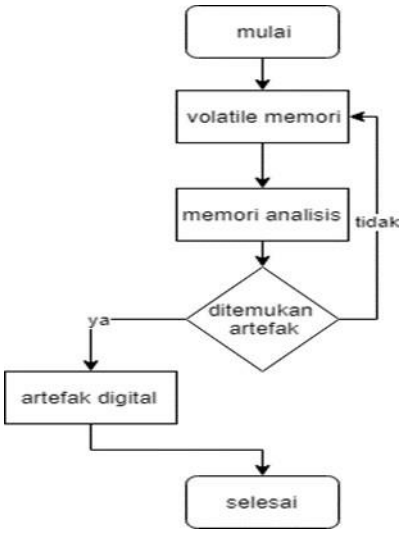
Proses dimana investigasi forensik berlangsung dari mulai sampai selesainya tahapan. Tahapan dari proses investigasi ditunjukan seperti Gambar 7 berikut ;



Gambar 7. Proses Investigasi

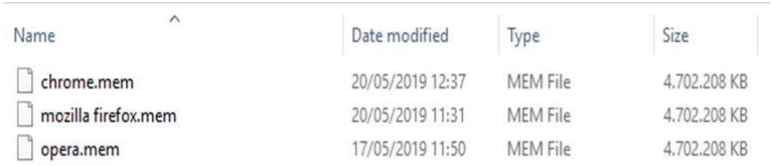
Gambar 7 merupakan alur proses dari investigasi yang dilakukan oleh investigator untuk menemukan barang bukti. Penjelasannya yaitu : (1) Preservasi. merupakan tahapan yang dilakukan investigator untuk mencari dan mengumpulkan barang bukti yang ada di tempat kejadian baik perangkat keras maupun perangkat lunak. Barang bukti yang ditemukan diamankan hingga tidak ada barang bukti yang tertinggal. (2) Akuisisi merupakan tahapan yang sangat penting dalam proses investigasi forensik. Pada proses akuisisi, akan dilakukan proses mengakuisisi atau pengambil alihan informasi yang terdapat pada barang bukti yakni barang bukti digital *(digital evidence)* sebagai penguat bukti di pengadilan. Proses akuisisi dilakukan dengan metode *live forensic* yaitu proses investigasi yang dilakukan dimana barang bukti yang berupa laptop masih dalam keadaan menyala. Akuisisi dilakukan agar barang bukti tersebut terjaga keasliannya dari pihak yang tak berhak. Hal ini dilakukan dengan tujuan karena barang bukti yang asli digunakan dalam sidang pengadilan. Tahapan akuisisi dari proses investigasi adalah sebagai berikut : (a) *Memory Volatile* atau *memory dump* merupakan tahapan yang dilakukan dengan mengakuisisi Random Acces Memory (RAM).

Proses *memory volatile* ini mendapatkan data yang tersimpan pada *memory* RAM yang saat itu sedang digunakan yakni aktifitas yang dilakukan di dalam *browser mode incognito*. Terdapat dua pendekatan untuk melakukan akuisisi memori yaitu berbasis *hardware* dan *software*, Pendekatan yang digunakan dalam akuisisi ini adalah pendekatan berbasis *software*. Terdapat banyak *software* yang digunakan untuk akuisisi memori, tetapi investigor menggunakan *belkasoft* RAM *Capturer* dalam proses investigasinya. Berikut ini merupakan *flowchart* dari *memory volatile* yang dijelaskan pada Gambar 8 berikut ;



Gambar 8. Flowchart Memory Volatile

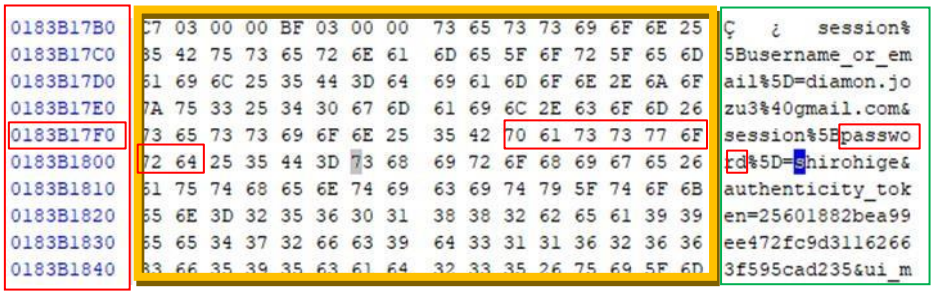
Gambar 8 menjelaskan bagaimana proses *memory volatile* dilakukan yaitu dilakukan akuisisi yang kemudian dari memory volatile tersebut kemudian dilakukan analisis terhadap memori. Jika proses berhasil maka akan ditemukan outputnya kemudian proses memory volatile selesai. Ketika tidak ditemukan output, maka proses memory volatile selesai. Perlu diketahui, proses memory volatile dilakukan ketika laptop sedang dalam keadaan menyala. Proses tersebut menghasilkan data RAM yang tertera pada gambar 9 sebagai berikut ;



Name	Date modified	Type	Size
chrome.mem	20/05/2019 12:37	MEM File	4.702.208 KB
mozilla firefox.mem	20/05/2019 11:31	MEM File	4.702.208 KB
opera.mem	17/05/2019 11:50	MEM File	4.702.208 KB

Gambar 9. Hasil Akuisisi Memori RAM

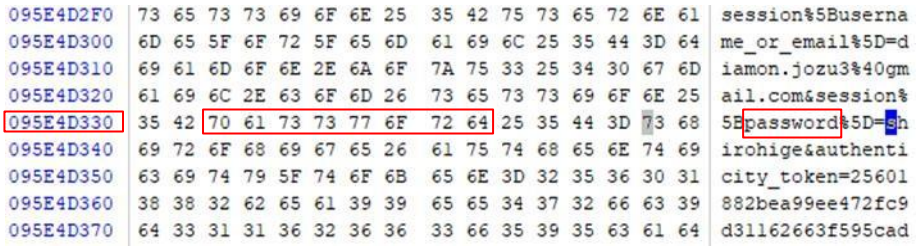
Gambar 9 merupakan hasil dari akuisisi RAM yang menghasilkan file berformat *.mem* dengan ukuran 4GB dari masing-masing browser yang diakuisisi melalui RAM. Hasil dari akuisisi memori RAM kemudian dilakukan proses analisis dengan menggunakan *tool winhex* untuk memperoleh *digital evidence.* File terebut kemudian di eksrak menggunakan *winhex* yang menghasilkan barang bukti dengan kata kunci pencarian "*password*" seperti Gambar 10 berikut ;



```
0183B17B0  C7 03 00 00 BF 03 00 00  73 65 73 73 69 6F 6E 25  Ç   ¿   session%
0183B17C0  35 42 75 73 65 72 6E 61  6D 65 5F 6F 72 5F 65 6D  5Busername_or_em
0183B17D0  61 69 6C 25 35 44 3D 64  69 61 6D 6F 6E 2E 6A 6F  ail%5D=diamon.jo
0183B17E0  7A 75 33 25 34 30 67 6D  61 69 6C 2E 63 6F 6D 26  zu3%40gmail.com&
0183B17F0  73 65 73 73 69 6F 6E 25  35 42 70 61 73 73 77 6F  session%5Bpasswo
0183B1800  72 64 25 35 44 3D 73 68  69 72 6F 68 69 67 65 26  rd%5D=shirohige&
0183B1810  61 75 74 68 65 6E 74 69  63 69 74 79 5F 74 6F 6B  authenticity_tok
0183B1820  65 6E 3D 32 35 36 30 31  38 38 32 62 65 61 39 39  en=25601882bea99
0183B1830  65 65 34 37 32 66 63 39  64 33 31 31 36 32 36 36  ee472fc9d3116266
0183B1840  33 66 35 39 35 63 61 64  32 33 35 26 75 69 5F 6D  3f595cad235&ui_m
```

Gambar 10. Hasil Ekstraksi Browser Chrome

Gambar 10 menunjukan adanya e-mail dan password milik pelaku yang digunakan untuk login ke media sosial yang digunakan dalam tindak kejahatan. *Password* dan *username* tersebut berada di dalam kolom hjiau yaitu kolom *text*, dengan memiliki bilangan *hexadecimal* yaitu 70 61 73 73 77 6F 72 64 pada kolom jingga, dan terletak di memori pada *offset* ke 0183B17F0 pada kolom berwarna merah. E-mail pelaku yang tertera yaitu diamon.jozu3@gmail.com,sedangkan *password*-nya yaitu shirohige. *Browser opera* menampilkan hasil seperti pada Gambar 11 sebagai berikut ;

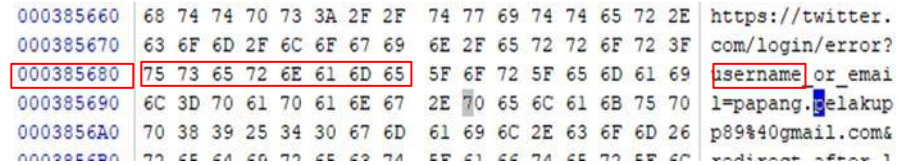


```
095E4D2F0  73 65 73 73 69 6F 6E 25  35 42 75 73 65 72 6E 61  session%5Buserna
095E4D300  6D 65 5F 6F 72 5F 65 6D  61 69 6C 25 35 44 3D 64  me_or_email%5D=d
095E4D310  69 61 6D 6F 6E 2E 6A 6F  7A 75 33 25 34 30 67 6D  iamon.jozu3%40gm
095E4D320  61 69 6C 2E 63 6F 6D 26  73 65 73 73 69 6F 6E 25  ail.com&session%
095E4D330  35 42 70 61 73 73 77 6F  72 64 25 35 44 3D 73 68  5Bpassword%5D=sh
095E4D340  69 72 6F 68 69 67 65 26  61 75 74 68 65 6E 74 69  irohige&authenti
095E4D350  63 69 74 79 5F 74 6F 6B  65 6E 3D 32 35 36 30 31  city_token=25601
095E4D360  38 38 32 62 65 61 39 39  65 65 34 37 32 66 63 39  882bea99ee472fc9
095E4D370  64 33 31 31 36 32 36 36  33 66 35 39 35 63 61 64  d31162663f595cad
```

Gambar 11. Hasil Ekstraksi Browser Opera

Gambar 11 menunjukan adanya barang bukti digital yang berupa *session* yang berisi *username* dan *password* ketika dilakukan analisis oleh investigator menggunakan *tool winhex*. *E-mail* yang didapatkan dari hasil ekstraksi RAM yaitu diamon.jozu3@gmail.com dan *password* : shirohige. Sedangkan *browser Firefox* dengan kata kunci "*username*" menghasilkan informasi seperti gambar 12 berikut ;

Gambar 12 Hasil Ekstraksi Browser Firefox



```
000385660  68 74 74 70 73 3A 2F 2F  74 77 69 74 74 65 72 2E  https://twitter.
000385670  63 6F 6D 2F 6C 6F 67 69  6E 2F 65 72 72 6F 72 3F  com/login/error?
000385680  75 73 65 72 6E 61 6D 65  5F 6F 72 5F 65 6D 61 69  username_or_emai
000385690  6C 3D 70 61 70 61 6E 67  2E 70 65 6C 61 6B 75 70  l=papang.pelakup
0003856A0  70 38 39 25 34 30 67 6D  61 69 6C 2E 63 6F 6D 26  p89%40gmail.com&
```

Gambar 12 menunjukan akun untuk login media sosial yang dilakukan oleh pelaku dalam aktifitas penggunaan *browser*. Kemudian *password* dan *username* yang telah didapatkan kemudian investigator membuka akun tersebut dan membuktikan apakah benar pelaku melakukan tindak kejahatan. *Reporting*

merupakan tahapan akhir dari investigasi yang hasilnya akan disajikan secara detail dari semua barang bukti digital yang didapat dari aktifitas penggunaan *browser mode incognito* oleh pelaku tindak kejahatan seperti Tabel 1 berikut ;

Tabel 1. Hasil Penemuan Barang Bukti Setiap Browser

Evidence	Browser		
	Chrome	Firefox	Opera
Bookmarks	Ada	Ada	Ada
Cookies	Ada	Ada	Ada
E-mail	Ada	Ada	Ada
History	Ada	Ada	Ada
Images	Ada	Ada	Ada
Timestamps	Ada	Ada	Ada
Password	Ada	Ada	Ada
URL	Ada	Ada	Ada
Search History	Ada	Ada	Ada

Tabel 1 menunjukan masing-masing browser memliki hasil seperti yang terlihat pada tabel. Pada tabel, browser chrome, firefox dan opera menemukan semua jenis evidence. Hal ini membuktikan kalau penereapan metode *live forensic* terhadap *browser mode incognito* bisa menemukan barang bukti yang tertingal melalui RAM.

IV. Kesimpulan dan saran

Berdasarkan hasil penelitian "Live Data Forensic : Artefak Internet Browser (Studi Kasus Browser Google Chrome,Mozilla Firefox, Opera Mode Incognito)" dapat ditarik kesimpulan sebagai berikut : (1) Pengimplementasian metode "live forensic" terhadap tindak kejahatan yang menggunakan browser dengan mode incognito berhasil mendapatkan informasi penting dari barang bukti fisik yang ditemukan di TKP dan investigator mendapatakn barang bukti digital yang tersimpan di dalam barang bukti fisik milik pelaku yang sedang melakukan kejahatan transaksi perdagangan bayi melalui media sosial. (2) Penerapan analisis yang dilakukan terhadap barang bukti yang kemudian dilakukan imaging baik akuisisi terhadap RAM maupun terhadap sistem partisi didapatakan barang bukti digital yang penting. Dari hasil ujicoba terhadap 3 browser yaitu Google Chrome, Mozilla Firefox dan Opera hasil yang didapatkan mempunyai kesamaan pada hasil.

Daftar Pustaka

[1] A. Zammouri and A. A. Moussa, "SafeBrowse: A new tool for strengthening and monitoring the security configuration of web browsers," in *2016 International Conference on Information Technology for Organizations Development, IT4OD 2016*, 2016.

[2] G. Horsman, "A process-level analysis of private browsing behavior: A focus on Google Chromes Incognito mode," in *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*, 2017.

[3] C. Hanifurohman, "ANALISA FORENSIK MEMORI VOLATIL DATA BROWSER," vol. IX, no. 02, pp. 1–7, 2017.

[4] J.-C. Liou, M. Logapriyan, T. W. Lai, D. Pareja, and S. Sewell, "A Study of the Internet Privacy in Private Browsing Mode," *Proc. 3rd Multidiscip. Int. Soc. Networks Conf. Soc.2016, Data Sci. 2016 - MISNC, SI, DS 2016*, pp. 1–7, 2016.

[5] K. Satvat, M. Forshaw, F. Hao, and E. Toreini, "On the privacy of private browsing - A forensic approach," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8247 LNCS, pp. 380–389, 2014.

[6] N. A. Alomirah, "Forensics Analysis of Residual Artefacts Acquired During Normal andPrivate Web Browsing Sessions," 2016.

[7] M. Scanlon, "Private Web Browser Forensics : A Case Study of the Epic Privacy Browser Private Web Browser Forensics : A Case Study of the Epic Privacy Browser," no. March, 2018.

[8] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *J. Ilm. Ilk.*, vol. 8, no. 3, pp. 242–247, 2016.

[9] 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.

[10] N. Shafqat, "Forensic Investigation of User 's Web Activity on Google Chrome using Open-source Forensic Tools," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 9, pp. 123– 132, 2016.

[11] A. Nalawade, S. Bharne, and V. Mane, "Forensic analysis and evidence collection for web browser activity," in *International Conference on Automatic Control and Dynamic Optimization Techniques, ICACDOT 2016*, 2017, pp. 518–522.

[12] E. Akbal, F. Güneş, and A. Akbal, "Digital Forensic Analyses of Web Browser Records," *J. Softw.*, vol. 11, no. 7, pp. 631–637, 2016.

[13] B. Raharjo, "Sekilas Mengenai Forensik Digital," *J. Sosioteknologi*, vol. 12, no. 29, pp. 384–387, 2016.

[14] C. Flowers, A. Mansour, and H. M. Al Khateeb, "Web browser artefacts in private and portable modes: a forensic investigation," *Int. J. Electron. Secur. Digit. Forensics*, vol. 8,no.2,p.99,2016.