Jurnal Algoritma
P-ISSN: 1412-3622; E-ISSN:2302-7339
Sekolah Tinggi Teknologi Garut

Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST

Sarjimin[1], Herman[2], Anton Yudhana[3]

Jurnal Algoritma
Sekolah Tinggi Teknologi Garut
Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151 Indonesia
Email : jurnal@sttgarut.ac.id

[1]sarjiminkbm@gmail.com
[2]hermankaha@mti.uad.ac.id
[3]eyudhana@ee.uad.ac.id

Abstrak - Penggunaan System Operasi Linux yang didistribusikan secara *open source* menjadikannya *operating system* yang dapat didistribusikan secara masif oleh banyak perusahaan. PC/Notebook maupun perangkat pintar yang berbasiskan Linux semakin diminati oleh *user* karena dalam proses distribusinya tidak dipungut biaya apapun. Memberikan layanan *browsing* internet kepada para user secara privat dan tidak meninggalkan jejak digital merupakan salah satu upaya yang dilakukan oleh *web browser* sebagai upaya invovasi web browser mendapatkan pengguna layanan sebanyak-banyaknya. Metode investigasi *forensic web browser private mode* menjadi hal yang perlu guna menjadi acuan dalam melakukan *forensic* terhadap kasus/kejadian kejahatan yang melibatkan layanan *browsing* secara privat. Ada banyak tools yang dapat dimanfaatkan untuk melakukan *live forensics* dan analisis data. Penelitian ini berhasil mengungkap bahwa layanan browsing secara privat yang disediakan oleh Mozilla Firefox nyata-nyata tidak privat secara menyeluruh. Artefak digital masih dapat ditemukan dalam RAM dan dianalisa dengan menggunakan berbagai macam tools untuk forensic, tools Autopsy berhasil mendapatkan data log browser sebesar 83%. Hasil artefak investigasi tersebut dapat menjadi acuan permulaan para investigator dalam penegakan hukum untuk mencari tersangka lain dan mendalami sebuah kasus yang melibatkan banyak pihak.

Kata Kunci - Browser; Live Forensic; Mozilla Firefox; NIST; Private Mode.

I. PENDAHULUAN

Web browser telah menjadi suatu keharusan untuk diinstal pada setiap perangkat pintar karena *Web browser* user dapat mengakses seluruh layanan yang disediakan oleh internet, dari membuka email, *searching*, *chatting*, membuka aplikasi penerima dan pengirim pesan (Whatsapp Web, Facebook Messenger, Telegram for web, internet banking, dll). Web browser merupakan peranti lunak yang dibuat untuk menjelajahi internet dan menyimpan informasi seperti URL history, *search keyword*, timestamp, password, dan segala sesuatu yang dilakukan pengguna saat menjelajah di internet [1], sejalan dengan itu Mahaju dan Atkinson [2] menyatakan bahwa web browser menyimpan data dan history untuk memudahkan pengguna dalam pengoperasian, seperti rekomendasi situs web atau akses yang lebih cepat ke situs yang dikunjungi sebelumnya hal ini menjadikan *web browser forensic* menjadi bagian penting dalam disiplin ilmu *digital forensic*.

Penelitian [3] tentang *forensic anti-forensic* mengungkapkan bahwa *history* penelusuran, timestamp dan password masih mungkin ditemukan jika data dalam RAM *computer* tidak dihapus (*anti forensic*), namun jika data dalam RAM telah dihapus dengan tool Clean After Me maka sulit ditemukan data yang dapat dianalisis. Penelitian Tri Rochmadi [4] mendapatkan artefak bukti digital dari web browser Browzar pada

sistem operasi Windows 7 menggunakan tool DumpIt dan dianalisis menggunakan Forensic Memory Volatility dan Winhex sehingga mendapatkan 3 bukti digital potensial terkait kasus kriminal di internet, bukti digital tersebut adalah URL atau alamat situs web yang dikunjungi oleh pelaku. *timestamp*, yaitu waktu mengakses URL oleh pelaku, dan *password* yang merupakan akun pelaku dan digunakan untuk masuk ke akun Google Mail.

Private mode browsing telah dikenal dalam banyak *web browser*, Google Chrome menyebutnya *Incognito Mode* [5], Google Chrome tidak akan menyimpan riwayat penelusuran, cookie, dan data situs, atau informasi yang dimasukkan dalam formulir. Mozilla Firefox menyebutnya *Private Browsing* [6] yaitu Mozilla Firefox tidak menyimpan informasi penjelajahan yang dilakukan oleh *user*, seperti riwayat dan cookie, *user* tidak meninggalkan jejak setelah user mengakhiri sesi atau menutup browser. Microsoft Edge menyebut fitur *browsing* secara private sebagai *InPrivate mode* [7], Microsoft Edge tidak menyimpan data riwayat penjelajahan, cookie dan pencarian dalam media penyimpanan primer (*harddisk*). Apple Safari menyebut fitur private browsing sebagai *Private Browsing* [8] yaitu saat user menggunakan jendela Penelusuran Pribadi, detail penelusuran user tidak disimpan, dan situs web yang user kunjungi tidak dibagikan dengan perangkat user lainnya.

Reza Montasari dan Pekka Peltolla [9] dalam penelitiannya menyatakan fitur *private mode* pada empat browser yang paling umum digunakan Incognito – Google Chrome Version 26.0.1410.43., Private Browsing – Mozilla Firefox Version 20.0., InPrivate – Internet Explorer Version 9.0.8112.16421., Private Browsing – Apple Safari Version 5.1.7 (7534.57.2). Percobaan yang dilakukan dalam penelitian ini mengungkapkan kenyataan bahwa *browser* dalam *private mode* dari Mozilla Firefox, Internet Explorer dan Apple Safari tidak dapat menjaga aktivitas penelusuran yang dilakukan oleh user secara privat. Ketiganya meninggalkan berbagai jenis data penelusuran di lokasi *"common"* dan *"uncommon"* pada *hard drive*. Mode *private mode* dari Mozilla Firefox, Internet Explorer dan Apple Safari mungkin menawarkan privasi pada pengguna tertentu pada tingkat tertentu dibandingkan pengguna biasa dari mesin yang sama. Sebaliknya, percobaan penelitian pada mode penjelajahan "Incognito Mode" Google Chrome mengungkapkan bahwa penelusuran secara privat sepenuhnya prvat, tidak meninggalkan artefak penjelajahan di lokasi *"common"* dan *"uncommon"* pada hard drive. Penelitian diatas menyimpulkan bahwa keempat browser yang diteliti tidak meninggalkan artefak penelusuran *private mode* dalam media penyimpanan primer (*harddisk*).

A. Review Literatur

Penelitian Rathod [10] menyatakan bahwa pada browser mode standar menunjukkan bahwa sebagian besar peneliti menggunakan log browser, file lokal atau analisis RAM sebagai sumber informasi untuk mengekstraksi artefak terkait penggunaan internet, penelitian ini mendapatkan data akses terakhir diantaranya tanggal dan waktu yang diakses dari Google Chrome, item pencarian, URL yang dikunjungi, dan cara memulihkan data yang dihapus.

Penelitian Ohana & Shashidhar [11] pada *operating system* Microsoft Windows 7 Professional (64 bit) dan *browser* Internet Explorer, Firefox, Safari dan Chrome menyatakan mayoritas file residu pencarian ditemukan dalam RAM. Google Chrome Portable meninggalkan paling banyak residu artefak pada mesin host. Penelitian ini menunjukkan dengan jelas bahwa data lebih lanjut masih dapat dipulihkan pada mesin host tanpa kehadiran perangkat penyimpanan primer (*harddisk*) maupun portable (*flashdisk*) yaitu dengan metode *live forensic*.

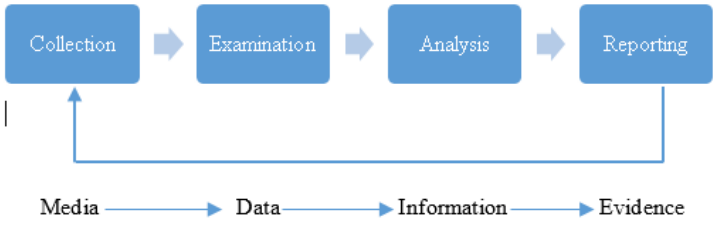
Penelitian Yudhana, et al [12] metode *live forensic* dengan langkah kerja DFRWS dan tool FTK imager pada system operasi Windows berhasil mendapatkan bukti *log* hasil posting dalam *social media* twitter meskipun postingan tersebut telah dihapus dari twitter, hasil posting ini dapat ditemukan melalui forensic *memory* (RAM).

Dapat disimpulkan bahwa log web browser mode standar masih dapat diperoleh dengan proses forensic static karena log browser tercatat dalam harddisk yaitu pada "*common files"* dan *"uncommon files*. Log web browser mode private maupun log hasil posting social media Twitter pada system operasi Windows masih mungkin didapatkan meskipun log web browser tidak tersimpan dalam media penyimpanan primer (*harddisk*) namun masih mungkin didapatkan pada *secondary memory* (RAM) yaitu dengan metode *live forensic*.

Berdasarkan *review literature* datas penelitian ini bertujuan untuk mendapatkan bukti log browser pada System Operasi yang umum digunakan selain Windows yaitu Linux dengan metode *live forensic*, sehingga dapat memberikan gambaran yang lebih komprehensif pada artefak digital *pada web browser private mode*.

II. METODE PENELITIAN

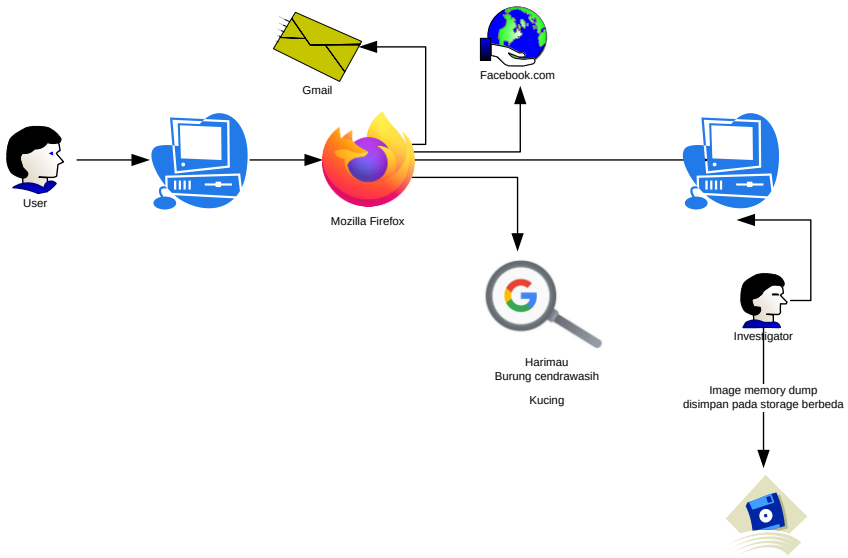
Penelitian menggunakan metode *forensic live forensic* dimana proses forensik dilakukan pada sistem yang sedang berjalan. Langkah kerja yang digunakan adalah National Institute of Standar and Technology (NIST) yang menerapkan empat tahap penelitian. Gambar 1 mengilustrasikan keempat tahap tersebut yang meliputi *data collection, examination, analysis* dan *reporting*. NIST memiliki kerangka kerja dan proses forensik yang terstruktur sehingga menjamin investigator mengikuti langkah penelitian agar hasil yang didapatkan dapat dipertanggung jawabkan.



Gambar 1 : langkah kerja metode NIST

Metode NIST dimulai dengan pengumpulan data (*collection*) yaitu mengumpulkan barang bukti termasuk didalamnya membuat *image* dari alat bukti yang ditemukan di tempat kejadian perkara (TKP). Penelitian ini akan meng-capture data yang terdapat di *Random Access Memory* atau yang biasa dikenal dengan istilah *RAM acquisition*. Proses selanjutnya yaitu pengujian hasil image terhadap alat bukti tersebut (*examination*) pada proses ini hasil imaging dilakukan pemeriksaan dengan berbagai tool/aplikasi *forensic*. Langkah selanjutnya adalah *analisys*, langkah ini untuk mengetahui keseluruhan apa yang telah dilakukan oleh *user*, tahap ini investigator mencari bukti pelanggaran/kejahatan yang dilakukan. Proses data *collection, examination, dan analysis* akan dilakukan dengan menggunakan beberapa alat bantu yang standar digunakan dalam forensik (*forensic tools*). Tahap terakhir yaitu pelaporan (*reporting*), yaitu membuat catatan dan dokumentasi keseluruhan aktivitas dari awal pengumpulan data sampai dengan tahap analisis, proses laporan ini harus dilakukan secara rinci dan menjelaskan apa yang telah dianalisis kemudian memaparkan alat bukti yang telah ditemukan.

Simulasi kasus dirancang untuk menjelaskan proses pengambilan data dimana simulasi kasus ini diharapkan menggambarkan kejadian sebagaimana dalam kenyataan asli. Software dalam simulasi kasus adalah *system operasi* Linux Mint 19.3 Tricia dan web browser Mozilla Firefox 77.0.1 (64-bit), simulasi ini dilakukan menggunakan *web browser* Mozilla Firefox *Private Mode* pada system operasi Linux, setelah mendapatkan hasil akuisisi dengan Lime pada media penyimpanan eksternal. Analisis lebih lanjut tentang penggunaan *web browser* saat komputer dalam kondisi on. Proses analisis dengan metode live forensics dilakukan dengan mencari bukti seperti kata kunci pencarian, kunjungan web, dan ID email.



Gambar 2 : Simulasi Kasus

Simulasi kasus dilakukan dengan mengunjungi mesin pencari google.com dan keyword pencarian : harimau; burung cendrawasih; kucing, mengunjungi situs website https://facebook.com, login https://gmail.com dengan akun sarjiminkbm@gmail.com dan password kebumen123. Proses Live forensic mengharuskan investigator melakukan RAM acquisition pada saat kondisi *host/computer* simulasi tetap menyala. Penyelidikan dilakukan setelah penyidik memperoleh data RAM dan disimpan pada media lain. Investigator harus mendapatkan bukti digital yang berkaitan dengan log dalam RAM. Parameter dalam penelitian ini adalah investigator mampu mendapatkan bukti digital / artefak pencarian google, akun email dan website yang dikunjungi oleh pelaku.

III. HASIL DAN PEMBAHASAN

A. *Collection*

Bukti yang ditemukan di tempat kejadian adalah komputer system operasi Linux mint dalam kondisi menyala. Tahap selanjutnya dilakukan imaging terhadap alat bukti tersebut dengan module Linux Memory Ekstraktor (LIME) pada media penyimpanan eksternal. Hasil imaging terhadap RAM berupa file image (.lime). Lime mendukung pemindahan memori ke SD di telepon atau mengirimkan pada perangkat lain melalui jaringan [13]. Data image hasil selanjutnya dianalisa dengan tool Sleuthkit Autopsy dan Belkasoft Evidence Center.
Perintah akuisi RAM dengan diberi nama lime_20200813.lime dan selanjutnya disimpan dalam folder /home/jimin:

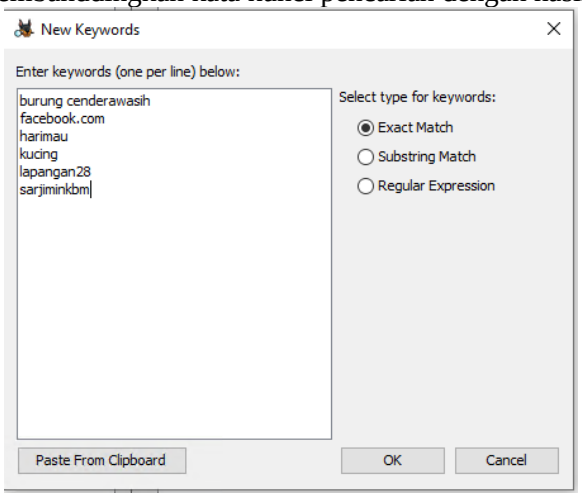
```
# insmod /sdcard/lime.ko "path=/home/jimin/lime_20200813.lime format=lime"
```

Perintah diatas menginstruksikan penambahan module pada Linux (*insmod*) untuk dijalankan dan mencapture memory untuk disimpan pada file lime_20200813 dengan ekstensi dot lime (.lime).

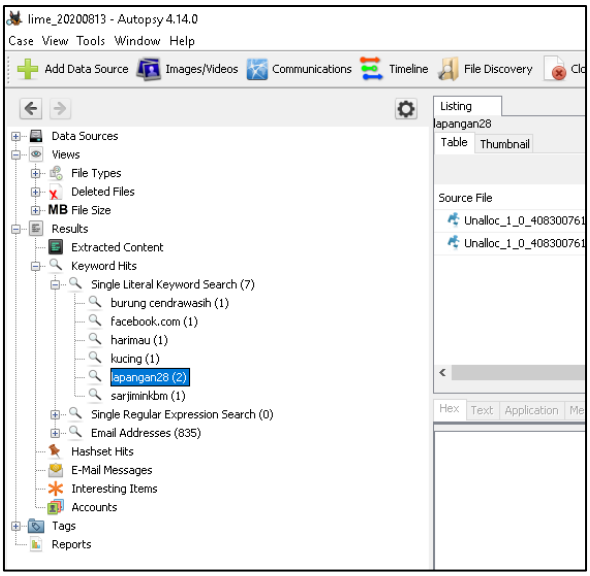
B. *Examination*

Data *capture image* yang telah didapatkan selanjutnya dianalisa dengan tool Sleuthkit Autopsy dan Belkasoft Evidence Center.
Proses pengujian *image* lime dengan *tool* Autopsy:

Pengujian dengan tools Autopsy dimulai dengan menentukan *text* pencarian (*keyword search*) yaitu kata kunci pencarian google, *username* dan *password* facebook serta *username* dan *password* gmail. Menentukan kata kunci dilakukan untuk membanddingkan kata kunci pencarian dengan hasil dari *tool* autopsy.



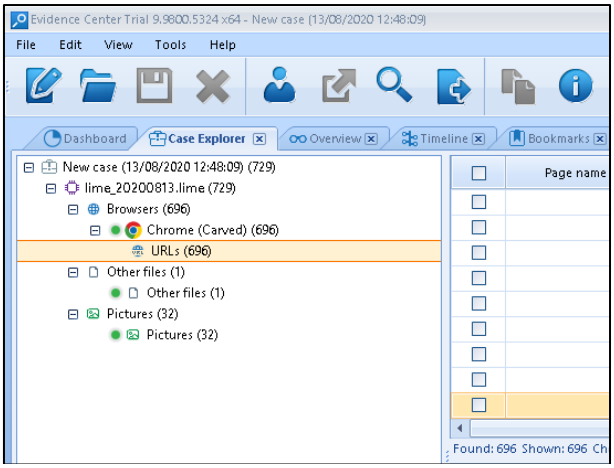
Gambar 3 : Menentukan k*eyword search*



Gambar 4 : Proses pengujian *image* dengan Sleuthkit Autopsy

Gambar 3 menampilkan hasil pengujian Sleuthkit Autopsy yang menunjukkan kunjungan *web* facebook.com ditemukan sebanyak 1 log; pencarian google.com dengan kata kunci harimau ditemukan sebanyak 1 log, kata kunci kucing ditemukan sebanyak 1 log dan kata kunci burung cendrawasih ditemukan sebanyak 1 log, username gmail dengan email sarjiminkbm@gmail ditemukan ditemukan sebanyak 1 log.

Proses pengujian image lime dengan tool Belkasoft Evidence Center:



Gambar 5 : Proses analisa dengan tool Belkasoft Evidence Center

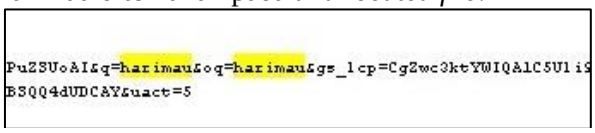
Pengujian dengan menggunakan Belkasoft Evidence Center juga dilakukan dengan menentukan keyword search seperti pada pengujian dengan Autopsy. Pengujian dengan Belkasoft Evidence Center tidak mendapatkan bukti kunjungan web, pencarian dengan google maupun username dan password gmail.

C. *Analysis*

Tools Autopsy menemukan bahwa history pencarian Mozilla Firefox *web browser private mode* dengan kata kunci harimau, burung cendrawasih dan kucing ditemukan seluruhnya dan tidak terenkripsi.

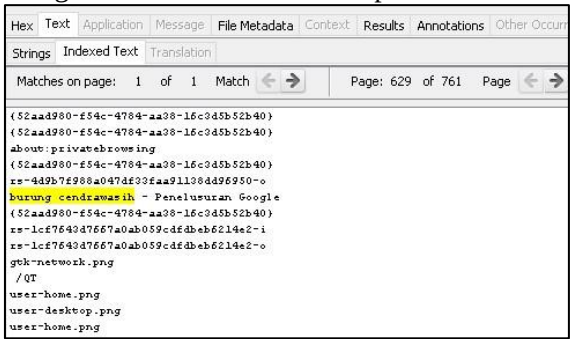
Gambar 6 : Pencarian dengan kata kunci kucing

Pencarian dengan kata kunci harimau ditemukan pada *unallocated file*.



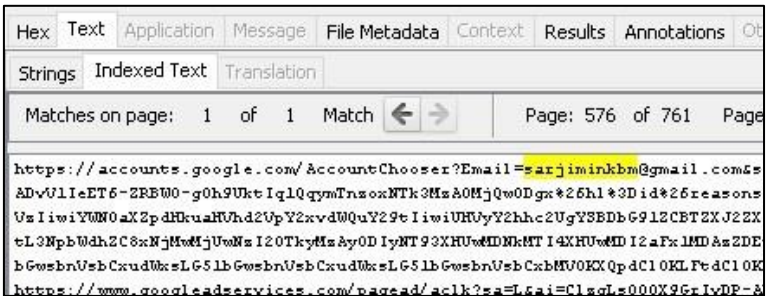
Gambar 7 : Pencarian dengan kata kunci harimau

Pencarian dengan kata kunci burung cenderawasih ditemukan pada *unallocated file*.



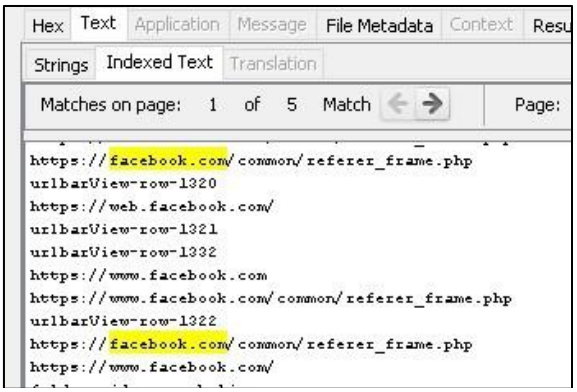
Gambar 8 : Pencarian dengan kata kunci burung cendrawasih

Percobaan login pada https://gmail.com dengan akun sarjiminkbm@gmail.com dan password kebumen123, teks akun email ditemukan dengan tool Sleuthkit Autopsy namun password tidak diemukan dengan tool Autopsy Sleuthkit. Gambar dibawah menunjukkan password Gmail telah terenkripsi dalam memory.



Gambar 9 : Percobaan login pada akun gmail

Percobaan mengunjungi website https://facebook.com dapat ditemukan dengan tool Sleuthkit Autopsy.



Gambar 10 : Percobaan mengunjungi website https://facebook.com

Log kunjungan website facebook.com dapat ditemukan dengan lebih dari satu *record* pada *unallocated file* memory yang diuji.
Pengujian dengan menggunakan Belkasoft Evidence Center tidak mendapatkan bukti kunjungan web, pencarian dengan google maupun username dan password gmail.

D. *Reporting*

Hasil analisis forensic yang dilakukan berdasarkan 4 jenis data yang menjadi focus pencarian (pencarian google, kujungan *web*, *username* dan *password*) tools Autopsy berhasil mendapatkan 3 jenis data namun tools Belkasoft tidak mendapatkan data apapun.
Ringkasan yang didapatkan pada masing-masing alat uji disajikan pada Tabel 1 sebagai berikut:

Tabel 1 : Hasil bukti digital

Item Percobaan	Sleuthkit Autopsy	Belkasoft
Kata kunci kucing	1	0
Kata kunci harimau	1	1
Kata kunci burung cendrawasih	1	1
Kunjungan web Facebook.com	1	0
Akun Gmail	1	0
Password Gmail	0	0

Perbandingan hasil kinerja tool alat analisis log *web browser private mode* menggunakan Autopsy dan Belkasoft adalah Autopsy memiliki hasil kinerja 75% dalam mendapatkan log *web browser private mode*, sedangakan dengan Belkasoft tidak mendapatkan data apapun.

Perhitungan kinerja *tool* Autopsy : $\frac{5}{6} \times 100\% = 83\%$

Perhitungan kinerja *tool* Belkasoft : $\frac{0}{6} \times 100\% = 0\%$

Hasil investigasi ini dapat digunakan sebagai bahan bukti permulaan yang mendukung proses investigasi selanjutnya dalam mendalami suatu kejadian perkara. Temuan bukti digital dalam proses perolehan data secara *live forensic* dapat mengungkap data selain password gmail. Keberhasilan investigasi dalam penelitian *web browser private mode* ini adalah mampu menemukan data bukti digital yang berupa kata kunci, kunjungan web, dan username email. Alat bukti tersebut dapat digunakan untuk meminimalisir penyalahgunaan *web browser private mode* pada tindakan criminal. Pengguna *web browser* pada mode *private* menjadi lebih paham dan berhati-hati dalam menggunakan *fitur ini*. Penelitian ini juga mendukung hasil dari [12], [11] dan [9] serta menyanggah klaim [6].

IV. KESIMPULAN

Berdasarkan hasil penelitian perbandingan tool forensik untuk menemukan bukti digital dalam RAM menggunakan tool Autopsy dan Belkasoft pada Sistem Operasi Linux Mint memberikan kesimpulan bahwa kinerja tool Belkasoft tidak berhasil mendapatkan log yang diharapkan, sedangkan hasil kinerja dengan Autopsy mencapai 83%.

Hasil penelitian ini memberikan kontribusi untuk melengkapi penelitian sebelumnya pada bidang *web browser private mode*. Penelitian ini mengungkap bahwa melalui RAM masih dimungkinkan untuk diambil informasi berharga tentang aktivitas yang dicurigai, seperti situs web yang dikunjungi, kata kunci di Internet, dan jejak email. Artefak ini dapat menjadi penghubung antara data dan tersangka sehingga pihak-pihak yang terlibat dalam sebuah tindakan kriminal dapat ditelusuri secara mendalam. Eksperimen menunjukkan bahwa klaim Website resmi atas privasi dapat disanggah melalui prose *live forensic* sehingga dapat disimpulkan bahwa klaim privasi yang disediakan oleh web browser private mode tidak sepenuhnya benar.

Dapat disimpulkan pula bahwa Tool Sleuthkit Autopsy dapat mengambil banyak artefak dari image RAM yang diambil dengan tool Lime dibandingkan dengan Belkasoft Evidence Center. Harapan peneliti pada penelitian ini adalah merekomendasikan kepada para investigator *tool* terbaik untuk proses investigasi RAM pada sistem operasi Linux.

V. UCAPAN TERIMAKASIH

Terimkasih kepada seluruh rekan-rekan MTI9 Universitas Ahmad Dahlan yang tetap semangat berjuang dan seluruh pihak yang membantu penyelesaian penelitian ini.

DAFTAR PUSTAKA

[1] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," *Digit. Investig.*, vol. 8, pp. S62–S70, 2011.

[2] S. Mahaju and T. Atkison, "Evaluation of firefox browser forensics tools," *Proc. SouthEast Conf. ACMSE 2017*, pp. 5–12, 2017, doi: 10.1145/3077286.3077310.

[3] 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.

[4] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, pp. 32–38, 2018.

[5] Google, "Browse in private," 2020. https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en&oco=0 (accessed Mar. 17, 2020).
[6] M. Firefox, "Private Browsing - Use Firefox without saving history," 2020. https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history (accessed Mar. 17, 2020).
[7] Microsoft, "Browse InPrivate in Microsoft Edge," 2020. https://support.microsoft.com/en-us/help/4026200/microsoft-edge-browse-inprivate (accessed Mar. 17, 2020).
[8] Apple, "Menelusuri secara pribadi di Safari di Mac," 2020. https://support.apple.com/id-id/guide/safari/ibrw1069/mac (accessed Mar. 17, 2020).
[9] R. Montasari and P. Peltola, "Computer forensic analysis of private browsing modes," in *International Conference on Global Security, Safety, and Sustainability*, 2015, pp. 96–109.
[10] D. M. Rathod, "Web browser forensics: google chrome," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 7, 2017.
[11] D. J. Ohana and N. Shashidhar, "Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions," *EURASIP J. Inf. Secur.*, vol. 2013, no. 1, p. 6, 2013, doi: 10.1186/1687-417X-2013-6.
[12] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 20, no. 2, pp. 125–130, 2019.
[13] J. Sylve, A. Case, L. Marziale, and G. G. Richard, "Acquisition and analysis of volatile memory from android devices," *Digit. Investig.*, vol. 8, no. 3–4, pp. 175–184, 2012, doi: 10.1016/j.diin.2011.10.003.