# Analisis Keamanan *Browser* Menggunakan Metode *National Institute of Justice* (Studi Kasus: *Facebook* dan *Instagram*)

**Ratri Ayunita Kinasih[1*], Arif Wirawan Muhammad[2], Wahyu Adi Prabowo[3]**

[1,2,3]Program Studi Teknik Informatika, Fakultas Informatika, Institut Teknologi Telkom Purwokerto

[1,2,3]Jl. D.I Panjaitan No.128, Purwokerto Kidul, Kec. Purwokerto Selatan, Kabupaten Banyumas

**e-mail:** [1]ratri.ayunita22@gmail.com, [2]arif@ittelkom-pwt.ac.id, [3] wahyuadi@ittelkom-pwt.ac.id

***Abstrak***

*Pencurian data digital sangat meresahkan pengguna media sosial, terlebih pengguna Facebook dan Instagram yang memiliki jumlah pengguna terbanyak. Browser yang digunakan untuk mengakses media sosial harus terjamin keamanannya. Mengetahui browser yang aman digunakan dalam mengakses media sosial sangat penting, agar pengguna tidak perlu khawatir terjadi pencurian data. Browser yang akan dianalisis yaitu Google Chrome, Mozilla Firefox, dan Microsoft Edge. Penelitian ini menggunakan skenario dengan teknik live forensics agar data volatile masih terekam dalam Random Access Memory (RAM). Metode yang digunakan yaitu metode National Institute of Justice yang memiliki lima tahapan yaitu identification, collection, examination, analysis, dan reporting. Hasil dari penelitian ini yaitu Google Chrome, Mozilla Firefox, dan Microsoft Edge tidak aman untuk mengakses media sosial Facebook. Sedangkan, untuk mengakses media sosial Instagram lebih aman menggunakan Mozilla Firefox. Data yang didapatkan pada penelitian ini diakuisisi menggunakan FTK Imager.*

***Kata kunci:*** *Browser, Facebook, FTK Imager, Instagram, Live Forensics*

***Abstract***

*The theft of digital data is very troubling for social media users, especially Facebook and Instagram users who have the largest number of users. The browser used to access social media must be guaranteed security. Knowing which browsers are safe to use in accessing social media is very important, so that users don't have to worry about data theft. The browser that will be analyzed are Google Chrome, Mozilla Firefox, and Microsoft Edge. This research using a scenario with live forensics techniques so that volatile data is still recorded in Random Access Memory (RAM). The method used is the National Institute of Justice method which has five stages, namely identification, collection, examination, analysis, and reporting. The result of this research are that Google Chrome, Mozilla Firefox, and Microsoft Edge are not safe for accessing Facebook. Meanwhile, accessing Instagram is safer using Mozilla Firefox. The data obtained in this study were acquired using the FTK Imager.*

***Keywords:*** *Browser, Facebook, FTK Imager, Instagram, Live Forensics*

## 1. Pendahuluan

Potensi pencurian data digital sudah menjadi ancaman global. Sudah banyak kasus pencurian data di dunia. Contohnya kebocoran data nasabah supermarket di Amerika Serikat, serta pencurian data pengguna *marketplace* di Indonesia. Semakin banyak pengguna internet maka semakin banyak pula pengguna media sosial. Media sosial berfungsi untuk memudahkan pengguna berinteraksi sosial menggunakan teknologi internet sehingga informasi dapat diterima

oleh banyak penggunya[1]. *Facebook* merupakan media sosial yang menyediakan privasi dan fitur yang lengkap gabungan dari *social networking, chatting, blogging, multimedia, photo sharing*, serta *email*[2]. *Instagram* merupakan aplikasi untuk membagikan foto, mengambil foto, dan menerapkan *filter* foto untuk penggunanya[3].

*Browser* yaitu aplikasi yang digunakan untuk mengakses media sosial. *Browser* selalu mengembangkan fitur keamanannya karena informasi pada internet sangat rentan. Semua pertukaran informasi terjadi di internet termasuk pada media sosial untuk berkomunikasi. Oleh karena itu, informasi dan internet saling berkaitan.[4]. *Browser* harus meningkatan keamanan di sisi pengguna agar informasi yang diakses oleh pengguna tidak dapat diketahui oleh pengguna lain[5].

Digital forensik merupakan ilmu pengetahuan dan teknologi komputer yang digunakan untuk pembuktian hukum. Dalam hal ini digunakan untuk membuktikan kejahatan teknologi komputer untuk mendapatkan bukti digital[6]. Menurut Pasal 5 Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Ayat 1 berbunyi, Informasi dan Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetakan merupakan alat bukti hukum yang sah. Terlepas dari pasal 184 KUHP yang membuat penggolongan alat bukti yang sah, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Pada Pasal 5 Ayat 2 Undang-undang No. 11 Tahun 2008 Tentang ITE menjelaskan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti lain selain alat bukti yang sebagaimana dimaksud dalam ketentuan perundang-undangan[7].

*Username* dan *password* merupakan hal yang penting dalam suatu akun dan termasuk data *volatile* atau data sementara yang ada saat komputer menyala dan jika komputer mati maka data akan hilang[1]. Untuk mendapatkan *username* dan *password* yang tersimpan di *Random Access Memory* (RAM) dibutuhkan teknik yang bersifat *voletile*, yang mana akuisisi informasi hanya dapat dilakukan ketika sistem berjalan. Data *voletile* yang tersimpan di RAM menggambarkan semua kegiatan yang sedang berjalan di komputer. Oleh karena itu digunakan teknik *live forensics* karena mampu menjamin integritas data *volatile* tanpa menghilangkan data yang berpotensi menjadi barang bukti[8]. *Live foresics* dilakukan saat system sedang berjalan, karena hampir keseluruhan penggunaan sistem tersimpan di RAM, *page file, hibernation file* dan *crash dump file*[9]. *Live forensics* bertujuan untuk menganalisis barang bukti tanpa mempengaruhi kinerja sistem, melakukan forensik pada memori, *file swap*, jaringan dan proses system yang sedang berjalan untuk mendapatkan informasi, serta untuk menjamin integritas data[10][11][12].

*Forensic Toolkit Imager (FTK Imager)* merupakan aplikasi *digital forensic* yang dioperasikan saat proses penyidikan menggunakan teknik *live* atau *static* atau bahkan keduanya[13]. FTK Imager berfungsi untuk melakukan akuisisi data, dimana sistem akuisisi itu merupakan suatu sistem yang berfungsi untuk mengambil, mengumpulkan dan menyiapkan data, hingga memprosesnya untuk menghasilkan data yang dikehendaki. Jenis serta metode yang dipilih bertujuan untuk menyederhanakan setiap langkah yang dilakukan pada keseluruhan proses[14].

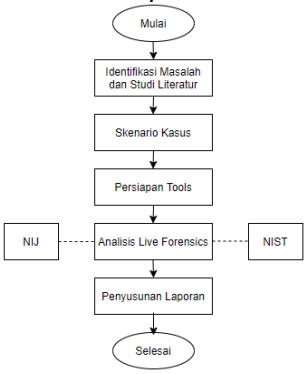
Pada penelitian yang dilakukan oleh Muhammad Nur Faiz, dkk yang berjudul "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Emai"l[4], masalah yang diangkat yaitu keamanan *email* pada beberapa *browser* secara umum seiring dengan banyaknya pelanggaran *cybercrime.* Penelitian Tri Rochmadi yang berjudul "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar"[5]. *Cybercrime* terus meningkat dan berinovasi seiring dengan perkembangan internet yang cepat dan lebih mudah diakses di mana-mana. Sehingga browser juga menyesuaikan untuk meningkatkan keamanan di sisi pengguna sehingga informasi yang diakses oleh pengguna tidak dapat diketahui oleh pengguna lain. Penelitian Muhammad Nur Faiz, dkk yang berjudul "Experimental Analysis of Web Browser Sessions Using Live Forensics Method"[15]. Penelitian ini menunjukkan penggunaan kata kunci ganja dan sabu dalam percobaan yang dilakukan, semua kata kunci dicatat dalam RAM. Sementara itu, kunjungan web yang ditemukan untuk bukti digital adalah planetdrugsdirect.com serta *Facebook ID* dan *Email ID* yang ditemukan berdasarkan percobaan

yang dilakukan. *Facebook ID* menggunakan Eksperimen sedangkan untuk *Email ID* adalah latihancoba1@gmail.com. Simulasi Eksperimen dilakukan dengan menggunakan *browser web Google Chrome* dan *Mozilla Firefox* dalam mode privat. Setelah memperoleh hasil akuisisi dengan DumpIt pada media penyimpanan, kemudian mengkloning dan memeriksa nilai *hash* pada *file* asli dan mencocokan hasil kloning. Analisis lebih lanjut tentang penggunaan *browser web* selama komputer aktif. Proses analisis dengan metode forensik langsung dilakukan dengan mencari bukti seperti kata kunci pencarian, kunjungan *web*, *ID email* dan *ID Facebook* dari kedua *browser.*

Penelitian ini dibuat dengan memperhatikan penelitian-penelitian yang sudah ada sebelumnya. Perbedaan dari penelitian sebelumnya yaitu penelitian ini mengangkat media sosial sebagai studi kasus, menggunakan teknik *live forensics* untuk mendapatkan data yang terekam pada *Random Access Memory* (RAM), serta menggunakan FTK Imager sebagai *tools forensics.* Banyaknya kasus pencurian akun di media sosial menjadi permasalahan dilakukan penelitian ini. Alasan dilakukan penelitian ini yaitu mengetahui *browser* yang aman digunakan untuk mengakses *Facebook* dan *Instagram* dari bukti *digital* yang didapatkan. Tujuan penleitian ini yaitu menerapkan *live forensics* pada keamanan *browser* untuk mengakses media sosial *Facebook* dan *Instagram* serta menemukan bukti *digital* dari analisis *Facebook* dan *Instagram* pada *browser.*

## 2. Metode Penelitian

Tahapan penelitian dalam melakukan analisis *live forensics* oleh penulis adalah sebagai berikut:



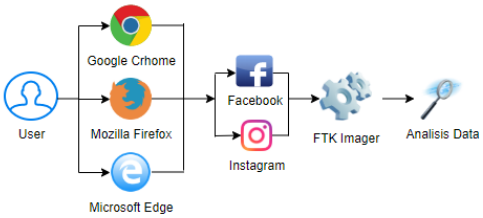

Gambar 1. Tahapan Penelitian

### 2.1 Identifikasi Masalah dan Studi Literatur

Pada tahapan ini dilakukan identifikasi terhadap masalah yang ada. Masalah yang diambil pada penelitian ini yaitu keamanan *browser.* Identifikasi dilakukan berdasarkan banyak terjadinya penipuan identitas di media sosial. Kejahatan yang dilakukan dalam penipuan identitas yaitu dengan mencuri data pribadi seseorang untuk melakukan kejahatan. Permasalahan ini cocok diangkat menjadi objek penelitian. Setelah proses identifikasi, selanjutnya dilakukan studi literatur dari penelitian terdahulu. Kata kunci pencarian pada FTK Imager yaitu *email, password*, nama pengguna, kiriman pengguna, *private message*, dan lain-lain.

### 2.2 Skenario Kasus

Dalam penelitian ini digunakan skenario yang dibuat untuk menjelaskan langkah-langkah dalam melakukan penelitian ini. Skenario pada gambar 2 yang dibuat yaitu *user* akan *login* akun *facebook* dan *Instagram* di ketiga *browser* dengan menggunakan akun yang berbeda. Setelah *user* berhasil *login* selanjutnya *user* akan melakukan aktivitas pada media sosial tersebut. Kemudian *user* akan mengakuisisi data aktivitas di media sosial pada ketiga *browser* tersebut dengan menggunakan FTK Imager. Setelah data berhasil di akuisisi, maka *user* akan menganalisis hasil dari akuisisi data tersebut.




Gambar 2. Skenario Kasus

### 2.3 Persiapan Tools

Mempersiapkan *tools* yang akan digunakan untuk menganalisis keamanan *browser*. Pada penelitian ini digunakan beberapa *tools* bseperti Tabel 1 berikut:

Tabel 1. Tabel Tools

| No | Alat dan Bahan | Spesifikasi | Keterangan |
|---|---|---|---|
| 1 | AccessData FTK Imager | Versi 4.3.1.1 | Perangkat Lunak |
| 2 | Akun Simulasi *Facebook* | analisisforensik@gmail.com<br>ayunitaratri@gmail.com<br>fitrianiazizah24.fa@gmail.com | Akun yang akan digunakan dalam skenario penelitian. Masing-masing *browser* akan *login* menggunakan satu akun. |
| 3 | Akun Simulasi *Instagram* | ratriayu22<br>azrahasna15<br>bigbosswh | Akun yang akan digunakan dalam skenario penelitian. Masing-masing *browser* akan *login* menggunakan satu akun. |
| 4 | *Browser Google Chrome* | Versi 84.0.4147.89 | *Browser* yang akan digunakan dalam simulasi skenario penelitian. |
| 5 | *Browser Mozilla Firefox* | Versi 78.0.2 | *Browser* yang akan digunakan dalam simulasi skenario penelitian. |
| 6 | *Browser Microsoft Edge* | Versi 83.0.478.64 | *Browser* yang akan digunakan dalam simulasi skenario penelitian. |

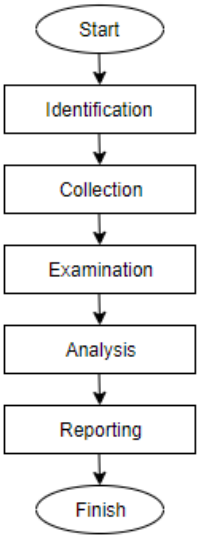
### 2.4 Analisis Live Forensics

Metode yang digunakan dalam analisis *live forensics* yaitu metode *National Institute of Justice* (NIJ), tahapan dari metode NIJ yaitu:

Berdasarkan Gambar 3 metode *National Institute of Justice* (NIJ) dapat dijelaskan sebagai berikut[16]:

a. *Identification*, yaitu melakukan identifikasi dan menyiapkan skenario penelitian serta *tools* yang akan digunakan dalam penelitian ini.
b. *Collection*, yaitu mengumpulkan data yang dapat dijadikan sebagai barang bukti digital pada ketiga *browser* yang digunakan dalam penelitian ini dengan menggunakan FTK Imager.
*c.* *Examination*, yaitu mengecek nilai *hash* dari setiap *file capture memory* pada proses sebelumnya menggunakan FTK Imager.

d. *Analysis,* yaitu menganalisis data yang dapat dijadikan bukti digital sesuai dengan skenario penelitian.
e. *Reporting,* yaitu membandingkan hasil analisis pada ketiga *browser* agar mendapatkan kesimpulan *browser* yang lebih aman untuk mengakses *facebook* dan *Instagram.*




Gambar 3. Tahapan NIJ

## 3. Hasil dan Pembahasan

### *3.1 Identification*

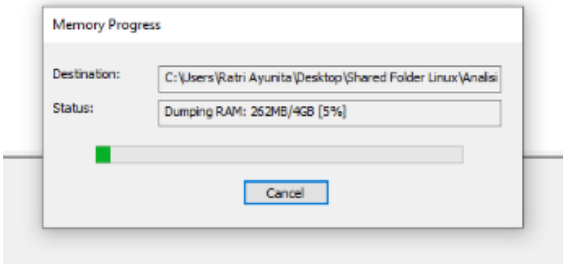
Menyiapkan *tools* dan skenario penelitian, *tools* yang akan digunakan dalam penelitian ini dapat dilihat pada Tabel 2.

Tabel 2 Spesifikasi *Tools*

| No | Alat dan Bahan | Spesifikasi | Keterangan |
|---|---|---|---|
| 1 | Laptop | Komputer *name:* DESKTOP-J17MKE5<br>*Operating System:* Windows 10 64-bit<br>*Processor:* AMD Ryzen 3 with Radeon Vega Mobile Gfx 2.50 GHz<br>*Memory:* 4,00 GB | Alat investigasi |
| 2 | AccessData FTK Imager | Versi 4.3.1.1 | Perangkat Lunak |
| 3 | *Google Chrome* | *Instagram* diakses pada 21 Juli 2020<br>*Facebook* diakses pada 23 Juli 2020 | *Browser* yang akan dianalisis |
| 4 | *Mozilla Firefox* | *Instagram* diakses pada 22 Juli 2020<br>*Facebook* diakses pada 23 Juli 2020 | Media sosial yang akan dianalis |
| 5 | *Microsoft Edge* | *Instagram* diakses pada 22 Juli 2020<br>*Facebook* diakses pada 23 Juli 2020 | Media sosial yang akan dianalisis |

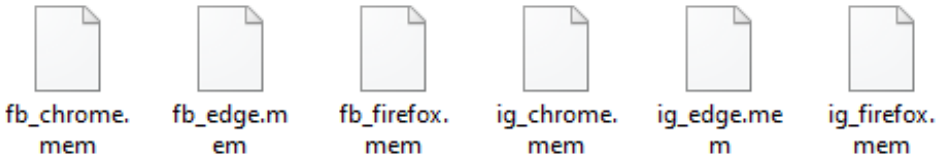
### *3.2 Collection*

Mengumpulkan data daari aktivitas yang dilakukan di media sosial dengan menggunakan FTK Imager. Dilakukan *capture memory* saat membuka media sosial pada *browser* yang akan dianalisis untuk mengakuisisi proses yang sedang berjalan pada sistem.




Gambar 4. *Memory Progress*

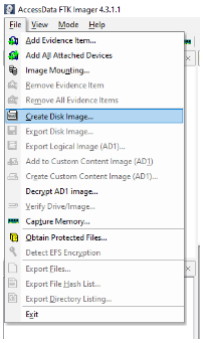
Hasil dari *memory progress* akuisisi yaitu *file* dengan ekstensi.mem yang dapat dilihat pada Gambar 5.




Gambar 5. *File* Hasil *Capture Memory*

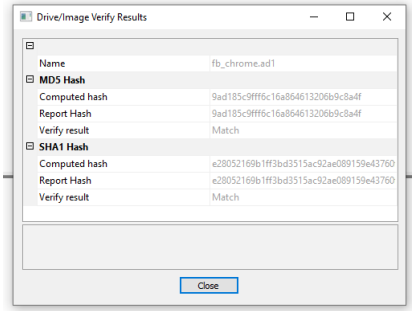
### 3.3 *Examination*

Setelah dilakukan *capture memory* atau proses akuisis data pada RAM yang menghasilkan *file* dengan ektensi .mem, kemudian dilakukan pengecekan nilai *hash* dari *file* hasil *capture memory.* Untuk mengecek nilai *hash* maka pilih *create disk image* pada FTK Imager seperti pada Gambar 6.




Gambar 6. *Create Disk Image*

Hasil dari proses *create diski image* akan didapatkan informasi *MD5 Hash* dan *SHA1 Hash.* Nilai *hash* berfungsi untuk menunjukkan keaslian *file*, bahwa saat dilakukan penngujian *file* tidak berubah.




Gambar 7. Nilai *Hash File fb_chrome.ad1*

Hasil akuisisi *create disk image* berupa *file* dengan ekstensi .ad1. Nilai *hash* menunjukan keaslian *file* bukti *digital*, sehingga akan terlihat bahwa *file* masih sama atau tidak di modifikasi. Pada penelitian ini nilai *hash* yang didapatkan *file* fb_chrome.ad1 yaitu

9ad185c9fff6c16a864613206b9c8a4f MD5 dan e28052169b1ff3bd3515ac92ae089159e43760 SHA1.

Tabel 3. Nilai *Hash*

| Nama *file image* | MD5 | SHA1 |
|---|---|---|
| fb_chrome.ad1 | 9ad185c9fffc16a864613206b9c8a4f | e28052169b1ff3bd3515ac92ae089159e43760 |
| fb_firefox.ad1 | 46088e0b6c86a3c3e0b3144c0965300e | 2ff91da6c8bf03c7af0a4e43113ecab253ae8a5 |
| fb_edge.ad1 | Bedd534c30c0b4c5026ae738648af558 | 8a759c67b96053524e80cac8350e00946148fb |
| ig_chrome.ad1 | 16717d4accfbdc8c77940413ec56f32d | 88ac1b0d2952f0adc583b263d0b440066d719 |
| ig_firefox.ad1 | 06ce177fca27e4e97273c24b47987d96 | 79af0a83e23beaf91506cea1f728f7771f575a43 |
| ig_edge.ad1 | 689995f4c0eb3fff663cfe826a939a69 | C4c847ebab1573df0213bf53e2b1b38389ab66 |

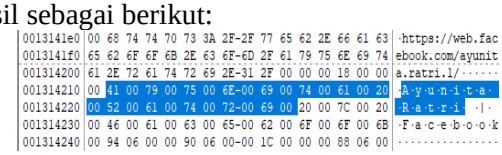
### 3.4 *Analysis*

Tahap selanjutnya yaitu analisis, pada tahap ini dilakukan analisis media sosial *Facebook* dan *Instagram* pada *Google Chrome, Mozilla Firefox,* dan *Microsoft Edge.*

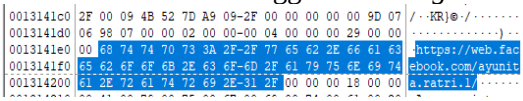
**1. Hasil Analisis Facebook**

**a. Analisis *Facebook* pada *Google Chrome***

Setelah melakukan *capture memory* maka didapatkan *file* fb_chrome.mem. Analisis yang dilakukan mendapatkan hasil sebagai berikut:

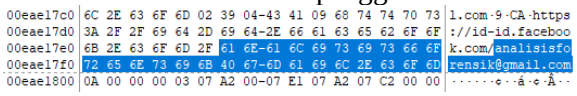



Gambar 8. Nama Pengguna di *Google Chrome*

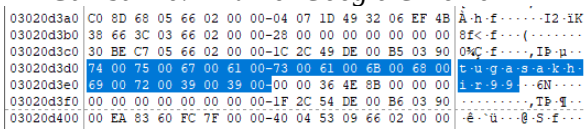



Gambar 9. Situs Pengguna di *Google Chrome*

Pada Gambar 8 terlihat bahwa di *offset* 001314210 sampai 001314220 terlihat nama *Facebook* yang digunakan oleh pengguna yaitu Ayunita Ratri. Pada Gambar 9 *offset* 0013141d0, 0013141e0, dan 001314f0 terlihat situs pengguna *Facebook.*




Gambar 10. *Email* di *Google Chrome*

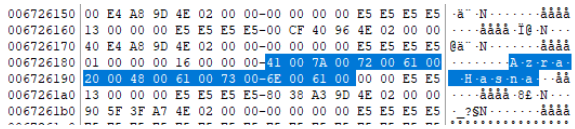



Gambar 11. *Password* di *Google Chrome*

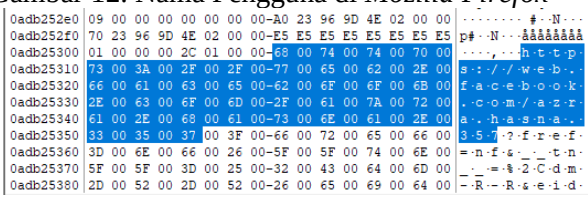
Pada Gambar 10 di *offset* 00eae17e0 dan 00eae17f0 serta Gambar 11 di *offset* 03020d3d0 dan 03020d3e0 terlihat *email* yaitu analisisforensik@gmail.com dan *password* yang digunakan oleh pengguna untuk *login Facebook* di *google chrome.*

***b. Analisis Facebook pada Mozilla Firefox***

Pada *file* fb_firefox.mem didapatkan hasil analisis sebagai berikut:

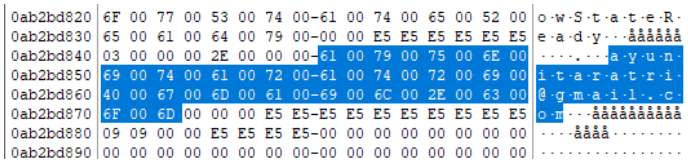


Gambar 12. Nama Pengguna di *Mozilla Firefox*

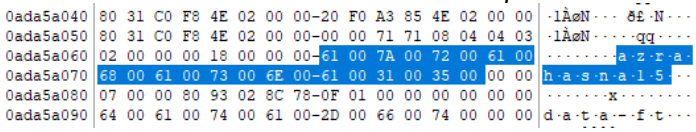


Gambar 13. Situs Pengguna di *Mozilla Firefox*

Pada Gambar 12 terlihat bahwa di *offset* 006726190 dan 0067261990 ada nama pengguna *Facebook* yaitu Azra Hasna. Sedangkan pada Gambar 13 terlihat bahwa di *offset* 0adb25300, 0adb25310, 0adb25320, 0adb25330, 0adb25340, dan 0adb25350 terdapat situs pengguna *Facebook.*



Gambar 14. *Email* di *Mozilla Firefox*

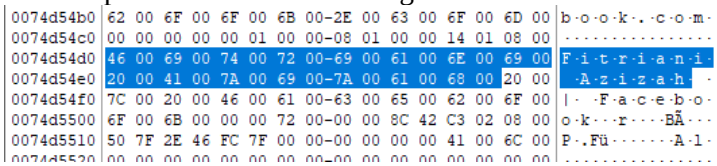


Gambar 15. *Password* di *Mozilla Firefox*

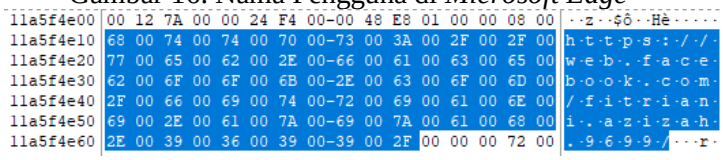
Pada Gambar 14 di *offset* 0ab2bd840, 0ab2bd850, 0ab2bd860, dan 0ab2bd870 terlihat bahwa *email* pengguna, sedangkan Gambar 15 di *offset* 0ada5a060 dan 0ada5a070 terlihat *password* pengguna yang digunakan untuk *login* ke *Facebook.*

### *c. Analisis Facebook pada Microsoft Edge*

Pada *file* fb_edge.mem didapatkan hasil analisis sebagai berikut:

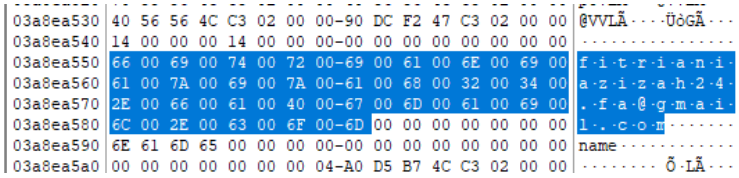


Gambar 16. Nama Pengguna di *Microsoft Edge*

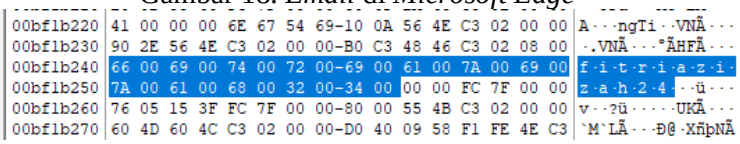


Gambar 17. Situs Pengguna di *Microsoft Edge*

Pada Gambar 16 terlihat bahwa di *offset* 0074d54d0 dan 0074d54e0 terdapat nama pengguna yaitu Fitriani Azizah. Sedangkan di Gambar 17 *offset* 11a5f4e10, 11a5f4e20, 11a5f4e30, 11a5f4e40, 11a5f4e50, dan 11a5f4e60 terdapat situs pengguna *Facebook.*




Gambar 18. *Email* di *Microsoft Edge*



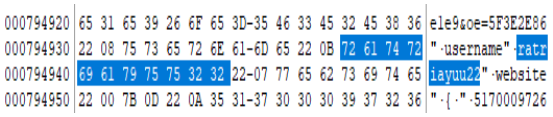

Gambar 19. *Password* di *Microsoft Edge*

Pada Gambar 18 di *offset* 03a8ea550, 03a8ea560, 03a8ea570, dan 03a8ea580 terdapat email pengguna yaitu fitrianiazizah24.fa@gmail.com, sedangkan pada Gambar 19 di *offset* 00bf1b240 dan 00bf1b250 terdapat *password* yang digunakan oleh pengguna untuk *login Facebook.*

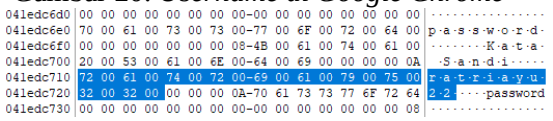
## 2. Hasil Analisis Facebook

### a. *Analisis Instagram pada Google Chrome*

Pada *capture memory* didapatkan *file* ig_chrome.mem yang menghasilkan analisis sebagai berikut:

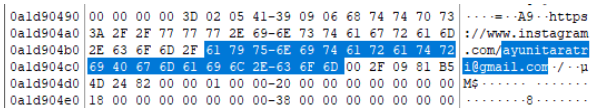



Gambar 20. *Username di Google Chrome*

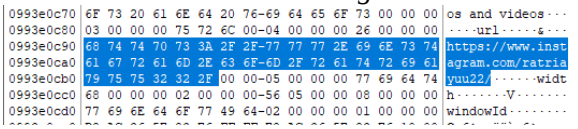



Gambar 21. *Password di Google Chrome*

Berdasarkan Gambar 20 terlihat bahwa di *offset* 000794930 dan 000794940 terdapat *username* pengguna *Instagram* yaitu ratriayuu22. Gambar 21 menunjukkan bahwa di *offset* 041edc710 dan 041edc720 terdapat *password* yang digunakan untuk *login* ke *Instagram* yaitu ratriayu22.




Gambar 22. *Email* di *Google Chrome*

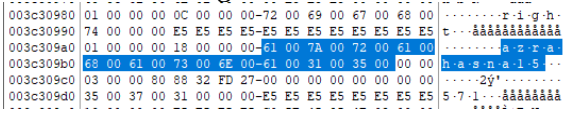



Gambar 23. Situs *Web* di *Google Chrome*

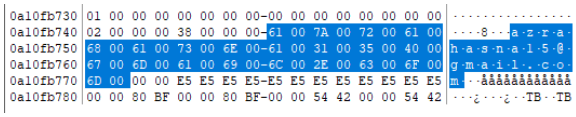
Gambar 22 menunjukkan bahwa di *offset* 0a1d904b0 dan 0a1d904c0 terlihat alamat *email* yang digunakan pengguna yaitu ayunitaratri@gmail.com. Sedangkan di Gambar 23 *offset* 0993e0c90, 0993e0ca0, dan 0993e0cb0 menunjukkan situs *web* pengguna.

### b. *Analisis Instagram pada Mozilla Firefox*

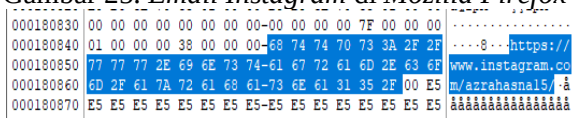
Hasil analisis pada *file* ig_firefox.mem sebagai berikut:




Gambar 24. *Username Instagram* di *Mozilla Firefox*



Gambar 25. *Email Instagram* di *Mozilla Firefox*

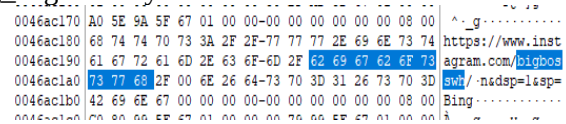


Gambar 26. Situs *Web Instagram* di *Mozilla Firefox*

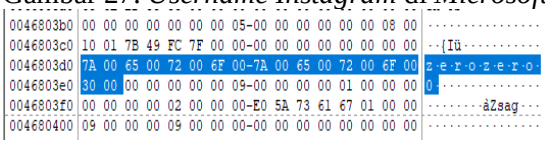
Berdasarkan Gambar 24 terlihat di *offset* 003c309a0 dan 003c309b0 terdapat *username* yaitu azrahasna15. Gambar 25 menunjukkan bahwa di *offset* 0a10fb740, 0a10fb740, dan 0a10fb760 terdapat *email* yang digunakan oleh pengguna yaitu azrahasna15@gmail.com. Sedangkan di Gambar 26 menunjukkan situs *web* yang ada di *offset* 000180840, 000180850, dan 000180860.

### c. *Analisis Instagram pada Microsoft Edge*

Hasil analisis pada *file* ig_edge.mem yaitu:



Gambar 27. *Username Instagram* di *Microsoft Edge*



Gambar 28. *Password Instagram* di *Microsoft Edge*

Berdasarkan Gambar 27 di *offset* 0046ac190 dan 0046ac1a0 terdapat *username* pengguna yaitu bigbosswh. Pada Gambar 28 di *offset* terdapat *password* yang digunakan untuk *login* yaitu zerozero0.

Hasil dari penelitian ini adalah ketiga *browser* yang digunakan dalam penelitian ini tidak aman untuk mengakses *Facebook,* dan untuk mengakses *Instagram* lebih aman menggunakan *Mozilla Firefox.* Sedangkan, hasil penelitian[4] adalah membuat tiga akun *email* dan *login* dengan *browser* yang berbeda. *Browser* yang aman digunakan pada *type public* yaitu *Google Chrome* karena tidak terlihat *password email.* Pada *type private* juga *Google Chrome* karena tidak terlihat *username* dan *password.* Hasil penelitian[17] yaitu tidak dapat ditemukan *history, timestamp* dan *password* pada *browser* Browzar. Hasil penelitian[15] memori forensik dapat mengambil informasi penting tentang aktivitas yang dicurigari, seperti situs *web* yang dikunjungi, kata kunci pencarian di internet, jejak *email* dan *id facebook* bahkan setelah *browser* ditutup dan *history* dihapus.

## 4. Kesimpulan

Berdasarkan hasil penelitian yang ada dapat disimpulkan bahwa *Google Chrome, Mozilla Firefox,* dan *Microsoft Edge* tidak aman digunakan unutk mengakses *facebook,* karena *email* dan *password* yang digunakan untuk proses *login* dapat terdeteksi pada penelitian ini. *Mozilla Firefox* lebih aman digunakan untuk mengakses *Instagram* dibandingkan dengan *Google Chrome* dan *Microsoft Edge,* karena *password* yang digunakan untuk *login* tidak dapat terdeteksi. Teknik *live forensics* dilakukan ketika sistem dalam keadaan menyala, sehingga data *volatile* masih terekan pada *Random Access Memory* (RAM). Dalam analasis *digital forensics* harus dilakukan secara berulang agar data yang didaptakan lebih baik. Keterbatasan dalam penelitian hanya menggunakan tiga *browser* dan dua media sosial, dapat dikembangkan lagi dengan menggunakan *browser* dan media sosial yang lebih banyak lagi agar hasil penelitian yang didapatkan lebih baik.

## Daftar Pustaka


[1] R. Ayatulloh, K. Noor, and R. Umar, "Perancangan Prbandingan Live Forensics Pada Keamanan Media Sosial Instagram, Facebook dan Twitter di Windows 10," *SNST ke-9*, pp. 125–128, 2018.

[2] W. Nicolas, "Gaya Komunikasi dan Motif Mahasiswa dalam Penggunaan Facebook (Studi Deskriptif Kualitatif Gaya Komunikasi dan Motif Penggunaan Facebook di Kalangan Mahasiswa Fakultas Ilmu Sosial dan Ilmu Politik)," 2019.

[3] L. S. Maulani and B. Sanawiri, "Pengaruh Social Media Marketing Terhadap Brand Awareness Serta Dampaknya Pada Purchase Decision (Survei Online Pada Followers Aktif Instagram Dan Facebook Vauza Tamma Hijab)," *J. Adm. Bisnis*, vol. 72, no. 2, pp. 148–156, 2019.

[4] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKa*, vol. 1, no. 3, pp. 108–114, 2017.

[5] 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.

[6] I. Riadi, Sunardi, and Sahirudin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice ( NIJ )," *JURTI*, vol. 3, no. 1, pp. 87–95, 2019.

[7] Widodo and B. Sugiantoro, "Penerapan Framework Harmonised Digital Forensic Investigation Process (HDFIP) Untuk Mendapatkan Artifak Bukti Digital Pada Smartphone Tizen," *CyberSecurity dan Forensik Digit.*, vol. 1, no. 2, pp. 67–74, 2018.

[8] D. S. Yudhistira, "Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop," 2018.

[9] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemanan Email Pada Sistem Operasi Proprietary," *J. Ilm. Ilk.*, vol. 8, no. 3, pp. 242–247, 2016.

[10] A. Sah, I. Riadi, and Y. Prayudi, "Deteksi Bukti Digital Online Gambling Menggunakan Live Forensik Pada Smartphone Berbasis Android," *CyberSecurity dan Forensik Digit.*, vol. 1, no. 1, pp. 14–19, 2018.

[11] T. Rochmadi, "Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Live Forensik," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 2, pp. 21–24, 2019.

[12] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *APPPTM*, pp. 207–211.

[13] M. F. Sidiq and M. N. Faiz, "Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital," *JEPIN*, vol. 5, no. 1, pp. 67–73, 2019.

[14] S. Awal *et al.*, "Makalah Digital Forensik ( FTK IMAGER )," 2017.

[15] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *IJECE*, vol. 8, no. 5, pp. 2951–2958, 2018, doi: 10.11591/ijece.v8i5.pp.2951-2958.

[16] A.- Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice ( NIJ )," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, p. 8, 2018, doi: 10.24014/coreit.v4i1.5803.

[17] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.