e-Issn: 2745-375
p-Issn: 2776-8546
Djtechno: Journal of Information Technology Research
Vol. 3, No. 2 Desember 2022

Analisis Keamanan Browser Dalam Bersosial Media Menggunakan Metode Institute Of Justice (NIJ)

Zikri Sulthoni Daulay[1)], Rini Indrayani[2)]

1)Prodi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, Indonesia

2) Prodi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, Indonesia

*Coresponding Email: rini.i@amikom.ac.id

Abstrak

Pengguna aktif media sosial di Indonesia terus meningkat di setiap tahunnya. Tetapi masih banyak pengguna yang tidak memahami keamanan dalam mengakses media sosial khususnya ketika mengakses dengan browser. Untuk itu browser yang dianalisis dalam penelitian ini yaitu browser google chrome dan mozilla firefox dengan dua mode yaitu mode publik dan mode incognito. Penelitian ini bertujuan agar dapat mengenal tingkat keamanan browser dalam menggunakan media sosial di browser. Untuk metodenya menggunakan metodologi NIJ (National Institute of Justice). Tool yang digunakan untuk mendapatkan data tersebut menggunakan aplikasi FTK Imager 4.5.0.3. Hasil dari penelitian ini adalah ketika mengakses media sosial facebook, instagram, twitter tidak aman menggunakan browser Google Chrome dan Mozilla Firefox dengan mode publik maupun mode incognito karena user_id, email dan beberapa password masih terdeteksi pada tools FTK Imager. Untuk hasil persentase yang diperoleh dalam penelitian yaitu 89% data user_id, password, email yang ditemukan pada browser Google Chrome mode publik, 67% data yang ditemukan pada browser Google Chrome mode incognito, 78% data yang ditemukan pada browser Mozilla Firefox mode publik, dan 89% data yang ditemukan pada browser Mozilla Firefox mode incognito.

Kata Kunci: Live Forensics; Institute of Justice; Browser; Media Sosial; FTK Imager.

Abstract

Active users of social media in Indonesia continue to increase every year. But there are still many users who do not understand the security of accessing social media, especially when accessing with a browser. For this reason, the browsers analyzed in this study are the Google Chrome and Mozilla Firefox browsers with two modes, namely public mode and incognito mode. This study aims to identify the level of browser security in using social media in the browser. The method used is the NIJ (National Institute of Justice) methodology. The tool used to get the data is using the FTK Imager 4.5.0.3 application. The results of this study are when accessing social media Facebook, Instagram, Twitter is not safe using Google Chrome and Mozilla Firefox browsers with public mode and incognito mode because user_id, email and some passwords are still detected in the FTK Imager tool. For the percentage results obtained in the study, namely 89% of user_id data, passwords, emails found in public mode Google Chrome browsers, 67% data found in incognito mode Google Chrome browsers, 78% data found in public mode Mozilla Firefox browsers, and 89% of data found in Mozilla Firefox browser incognito mode..

Keywords: Live Forensics; Institute of Justice; Browser; Media Sosial; FTK Imager .

1. PENDAHULUAN

Saat ini teknologi mempunyai peran penting dalam masyarakat untuk tujuan pembangunan kemajuan bangsa. Misalnya internet yang mempunyai pengetahuan informasi yang lengkap. Salah satu tool yang dibutuhkan untuk mencari informasi pada internet tersebut adalah browser. Era modern ini browser telah berkembang pesat dari segi fitur maupun segi keamanannya. Browser tersebut memiliki beberapa fitur yaitu mode publik dan mode incognito. Pada mode publik semua aktifitas yang dilakukan pada browser mulai dari histori, cookies, email, password dan lain-lain akan tersimpan pada sistem. Sedangkan mode incognito merupakan fitur khusus yang berguna untuk menjaga privasi ketika beraktifitas di browser. Fungsi mode incognito ini berguna untuk tidak menyimpan cookies, histori browser serta informasi yang diketik ketika mengisi formulir pada halaman web browser (Mu'Minin & Anwar, 2020).

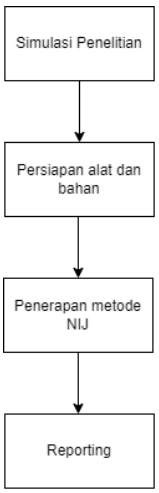
Browser saat ini digunakan bukan hanya untuk sekedar mencari informasi, tetapi juga digunakan untuk bermedia sosial. Media sosial saat ini tidak hanya menjadi sarana pengiriman dan penerimaan informasi, tetapi juga tempat untuk menyimpan informasi. Media sosial yang biasa digunakan masyarakat indonesia yaitu Whatsapp, Instagram, Twitter, Facebook dan sebagainya (Bintang et al., 2018). Saat ini semakin banyak jenis browser, antara lain Mozilla Firefox, Microsoft Edge, Google Chrome. Oleh karena itu, browser harus terus meningkatkan aspek keamanan aplikasinya agar terhindar dari berbagai kejahatan di dunia maya. Kejahatan di dunia maya merupakan suatu bentuk kejahatan virtual menggunakan komputer yang terkoneksi internet (Antoni, 2018). Oleh karena itu, teknik digital forensik sangat dibutuhkan untuk mencari bukti-bukti digital yang valid agar kejahatan tersebut dapat dibawa ke meja persidangan. Forensik digital melibatkan menemukan bukti digital yang dapat disimpan pada RAM, hard drive, CD, dan lain-lain. Forensik digital telah menjadi bagian penting dari keamanan informasi (Nabilla & Rini, 2022). Analisis forensik digital terdiri dari dua jenis yaitu traditional forensik dan live forensik. Perbedaan dari traditional forensik dan live forensik terdapat pada keadaan media penyimpanan saja, apakah sistem sedang hidup atau mati (Mustafa & Umar, 2018). Username dan password adalah elemen terpenting dari akun jejaring sosial, sehingga termasuk dalam data volatile

yang tersimpan di RAM saat komputer dihidupkan dan jika dimatikan data tersebut akan hilang.

Penelitian ini bertujuan agar dapat mengenal tingkat keamanan browser dalam menggunakan jejaring sosial di browser. Browser yang ingin dianalisa pada penelitian ini adalah mozilla firefox dan google chrome. Metode yang digunakan adalah metodologi National Institute of Justice (NIJ) (Kinasih et al., 2020), agar menghasilkan barang bukti harus melalui 5 tahap seperti Identification, Collection, Examination, Analysis dan Reporting.

2. METODE PENELITIAN

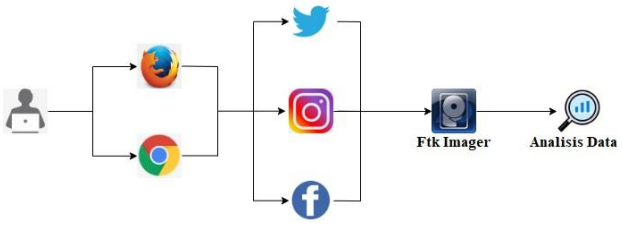
Metode yang digunakan pada penelitian ini yaitu menggunakan teknik live forensic. Ada beberapa tahapan yang dilakukan pada waktu melaksanakan penelitian ini, dapat dilihat pada Gambar 1.



Gambar 1. Tahapan penelitian

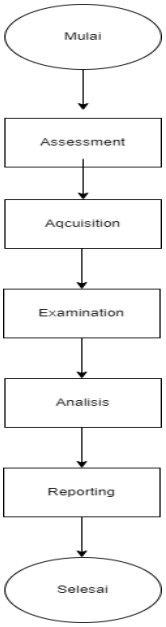
Tahap pertama pada gambar 1 adalah simulasi penelitian. Simulasi penelitian yang digunakan merupakan sebuah scenario dimana pengguna akan melakukan akses login menggunakan basic authentication seperti username dan password ke akun twitter, instagram, dan facebook melalui dua browser berbeda yaitu, mozilla firefox dan google chrome. Pengujian ini juga dilakukan dengan fitur mode incognito yang terdapat pada kedua browser tersebut. Setelah berhasil login, pengguna melakukan capture memory di setiap mode yang ada pada kedua browser tersebut. Proses capture memory ini dilakukan satu per satu, sehingga nantinya penelitian ini melakukan empat kali capture memory, yaitu pada mozilla firefox mode publik, mozilla firefox mode incognito, google chrome mode publik, dan google chrome mode incognito. Pengujian ini juga melakukan pembersihan riwayat pada masing-masing browser seperti history, cookie, cache dan lainnya ketika proses capture memory berhasil dan kemudian melakukan restart pada laptop yang digunakan untuk pengujian. Tahap terakhir yaitu melakukan analisis dari hasil capture memory tersebut yang didapatkan melalui tools FTK imager.

Skema skenario tersebut dapat dilihat pada Gambar 2.



Gambar 2. Simulasi Penelitian

Tahap selanjutnya yaitu persiapan alat dan bahan dimana peneliti menyiapkan seluruh kebutuhan penelitian yaitu berbagai hardware, software, serta informasi akun yang akan digunakan sebagai informasi dasar aktivitas login di simulasi penelitian. Kemudian setelah simulasi semua persiapan dan simulasi dilakukan, maka diterapkan metode National Institute of Justice). Alur metode NIJ yang digunakan untuk mendapatkan data-data dari aktifitas browser yang tersimpan pada RAM dapat dilihat pada Gambar 3.



Gambar 3. Alur National Of Justice (NIJ)

Berdasarkan Gambar 3, penjelasan dari metode tersebut adalah sebagai berikut :

a) Assessment, merupakan tahapan pemeriksaan atau evaluasi terhadap alat dan bahan yang dibutuhkan dalam penelitian ini.
b) Aqcuisition, merupakan tahapan akuisi untuk mengumpulkan data digital pada kedua browser menggunakan tools FTK Imager yang nantinya data tersebut akan dianalisis.
c) Examination, Tahapan untuk pengecekan nilai hash dari seluruh file hasil capture memory.
d) Analysis, merupakan tahapan menganalisis data media sosial Facebook, Instagram, dan Twitter

pada browser Mozilla Firefox dan Google Chrome sesuai dengan simulasi yang telah dijelaskan sebelumnya menggunakan tools FTK Imager.

e) Reporting, merupakan tahapan yang dilakukan untuk membandingkan hasil dari analisis kedua browser tersebut yang disajikan dalam tabel dan grafik agar mendapatkan suatu kesimpulan rekoimendasi browser yang lebih aman ketika pengguna melakukan mengakses media sosial.

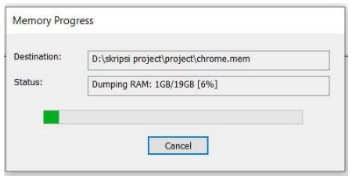
3. HASIL DAN PEMBAHASAN

3.1 Tahapan Assessment

Pada tahapan assessment ini melakukan proses pemeriksaan atau evaluasi terhadap alat penelitian berupa Laptop Acer Nitro AN515-52 dan tools FTK Imager 4.5.0.3.

3.2 Tahapan Aqcuisition

Tahap ini melakukan akuisisi pada RAM Laptop Acer Nitro AN515-52 untuk mengumpulkan data-data dari kedua browser tersebut. Dilakukan dengan cara capture memory pada tools FTK Imager yang nantinya akan meng-capture seluruh proses yang sedang berjalan pada memory.



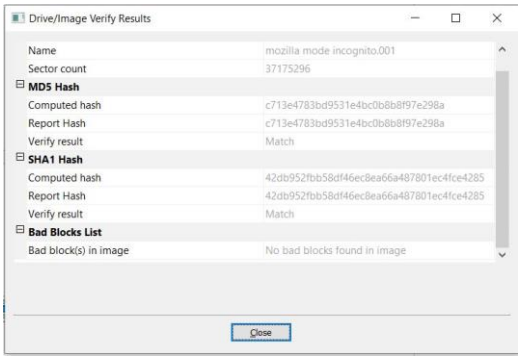
Gambar 4. Memory Progress

Setelah proses capture memory selesai akan menghasilkan file dengan ekstensi .mem yang selanjutnya akan dianalisis untuk mendapatkan data-data digital.

Gambar 5. Hasil Capture Memory

3.3 Tahapan Examination

Tahapan ini dilakukan untuk pengecekan nilai hash dari seluruh file yang telah didapatkan melalui capture memory. Untuk pengecekan nilai hash dapat dilakukan dengan cara Create Disk Image pada tools FTK Imager. Setelah proses dari create disk image berhasil, akan menghasilkan informasi MD5 Hash dan SHA1 Hash. Tujuan dari create disk image ini untuk dapat mengetahui nilai hash dari file tersebut guna untuk menghindari perubahan pada nilai hash dapat dilihat pada Gambar 6.



Gambar 6. Hasil Create Disk

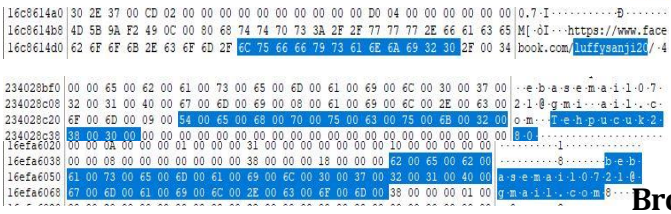
3.4 Tahapan Analysis

Tahapan ini melakukan analisis data media sosial yang didapatkan pada browser Google Chrome dan Mozilla Firefox.

3.4.1 Hasil Analisis Media Sosial pada Browser Google Chrome Mode Public

a. Hasil Analisis Facebook

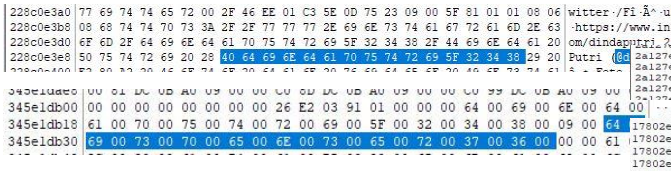
Dari hasil analisis pada file *chrome.mem* telah didapatkan sebuah user_id, password, dan email seperti pada gambar 7.



Gambar 7. Penemuan User_id dan Password Facebook

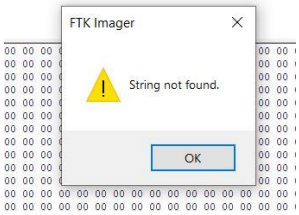
b. Hasil Analisis Instagram

Dari hasil analisis pada file *chrome.mem* telah didapatkan sebuah user_id dan password akun instagram, ditunjukkan pada gambar 8.



Gambar 8. User_id dan Password Instagram

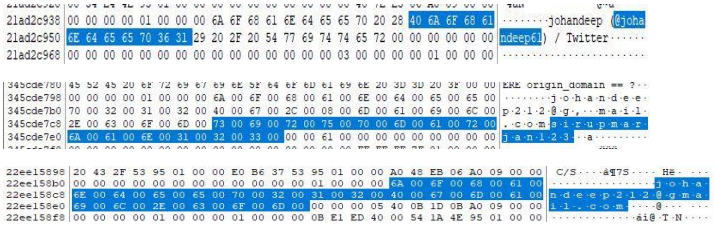
Selanjutnya pada Gambar 9 ketika melakukan analisis atau mencari alamat email pada akun instagram tersebut, hasil yang didapatkan tidak ada.



Gambar 9. Email instagram tidak ditemukan

c. Hasil Analisis Twitter

Hasil analisis pada file *chrome.mem* telah didapatkan sebuah user_id, password, dan email akun Twitter, ditunjukkan pada gambar 10.

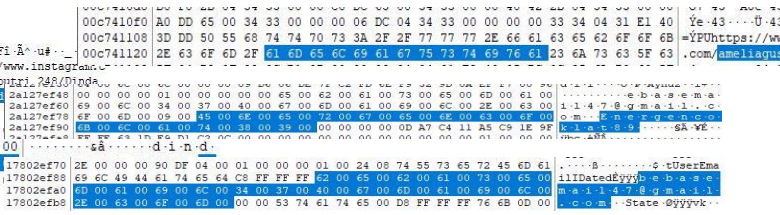


Gambar 10. User_id, Password, dan Email Twitter

3.4.2 Hasil Analisis Media Sosial pada Browser Google Chrome Mode Incognito

a. Hasil Analisis Facebook

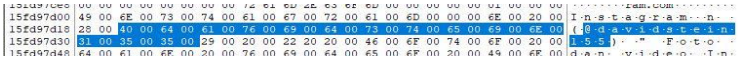
Hasil analisis pada file *incognito.mem* telah didapatkan sebuah user_id, password, dan email akun Facebook, ditunjukkan pada gambar 11.



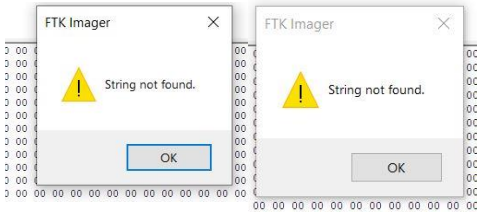
Gambar 11. User_id, Password, dam Email Facebook

b. Hasil Analisis Instagram

Hasil analisis pada file *chrome mode incognito.mem* telah ditemukan user_id yang digunakan untuk login ke akun instagram seperti pada gambar 12. Sedangkan informasi mengenai password dan email tidak dapat ditemukan seperti pada gambar 13.



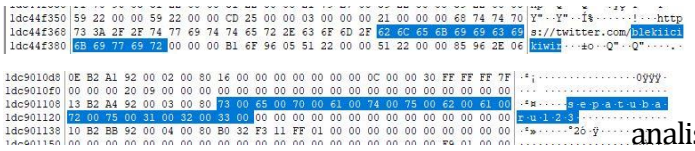
Gambar 12. User_id Instagram



Gambar 13. Password dan Email instagram tidak ditemukan

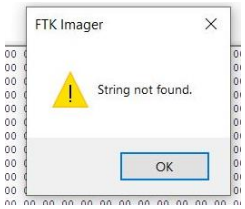
c. Hasil Analisis Twitter

Hasil analisis pada file *chrome incognito.mem* telah didapatkan user_id dan password yang digunakan untuk login ke akun Twitter, ditunjukkan pada gambar 14.



Gambar 14. User_id dan Password Twitter

Selanjutnya pada Gambar 15 hasil yang didapatkan ketika melakukan analisis atau mencari alamat email pada akun twitter tersebut tidak ditemukan.

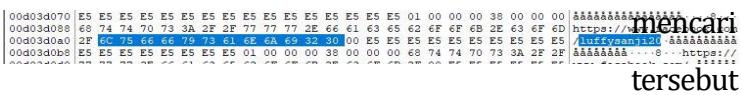


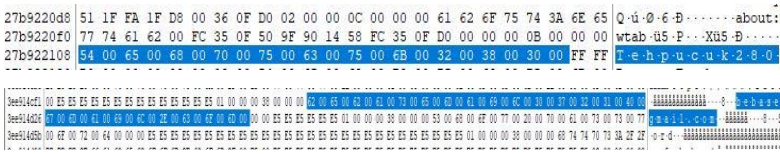
Gambar 15. Email Twitter Tidak Ditemukan

3.4.3 Hasil Analisis Media Sosial pada Browser Mozilla Firefox Mode Public

a. Hasil Analisis Facebook

Hasil analisis pada file *mozilla.mem* telah ditemukan sebuah user_id, password, dan email akun Facebook, ditunjukkan pada gambar 16.

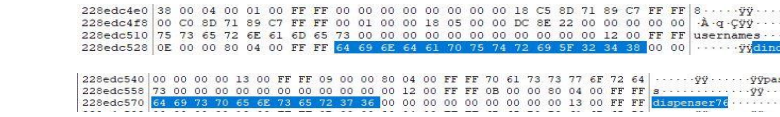




Gambar 16. User id, Password dan Email Facebook

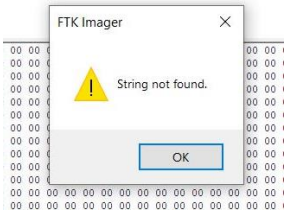
b. Hasil Analisis Instagram

Hasil analisis pada file *mozilla.mem* telah ditemukan user_id dan pasword yang digunakan untuk login ke akun instagram, ditnjukkan pada gambar 17.



Gambar 17. Password Instagram

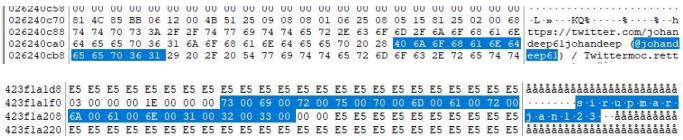
Sedangkan Gambar 18 menunjukkan analisis Email Instagram yang tidak ditemukan.



Gambar 18. Email instagram tidak ada

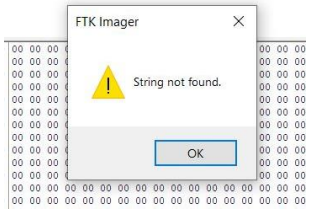
c. Hasil Analisis Twitter

Hasil analisis pada file *mozilla.mem* telah didapatkan user_id dan password yang digunakan untuk login ke akun twitter, ditunjukkan pada gambar 19.



Gambar 19. User_id dan Password Twitter

Gambar 20 menunjukkan hasil yang didapatkan ketika melakukan analisis atau mencari alamat email pada akun twitter tersebut tidak ditemukan.

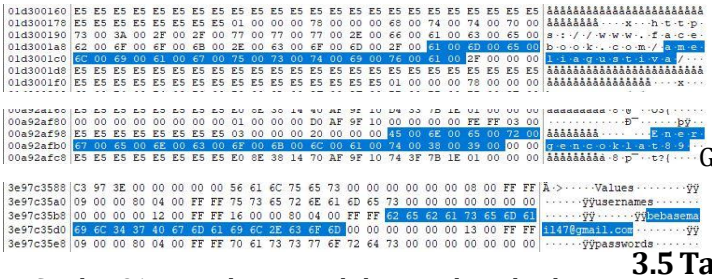


Gambar 20. Email Twitter Tidak Ditemukan

3.4.4 Hasil Analisis Media Sosial pada Browser Mozilla Firefox Mode Incognito

a. Hasil Analisis Facebook

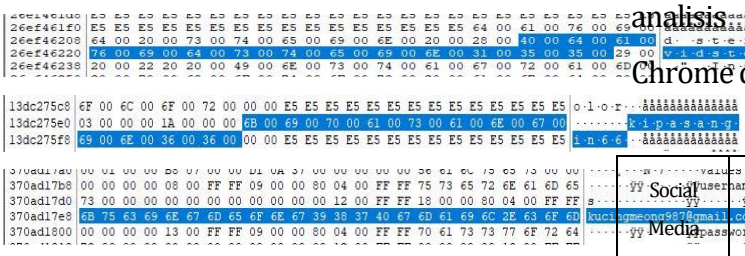
Hasil analisis pada file *mozilla mode incognito.mem* telah ditemukan user_id, password, dan email Facebook yang ditunjukkan pada gambar 21.



Gambar 21. User_id, Password, dan Email Facebook

b. Hasil Analisis Instagram

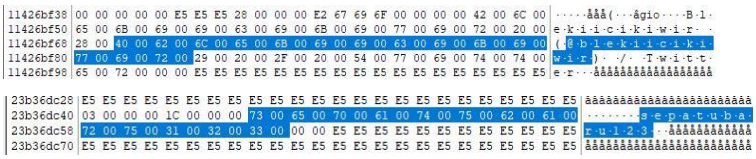
Hasil analisis pada file *mozilla mode incognito.mem* telah ditemukan user_id, password, dan email instagram ditunjukkan pada gambar 22.



Gambar 22. User_id, Password, dan Email Instagram

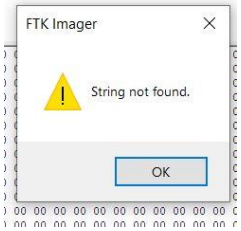
c. Hasil Analisis Twitter

Hasil analisis pada file *mozilla incognito.mem* telah didapatkan user_id dan password Twitter ditunjukkan pada gambar 23.



Gambar 23. Password Twitter

Gambar 24 menunjukkan hasil yang didapatkan ketika melakukan analisis atau mencari alamat email pada akun twitter tersebut tidak ditemukan.



Gambar 24. Email Twitter Tidak Ditemukan

3.5 Tahap Reporting

Tahapan ini membandingkan hasil dari analisis kedua browser agar mendapatkan suatu rekomendasi browser aman ketika pengguna melakukan mengakses media sosial. Berikut adalah tabel reporting dari hasil analisis media sosial pada browser Google Chrome dan Mozilla Firefox.

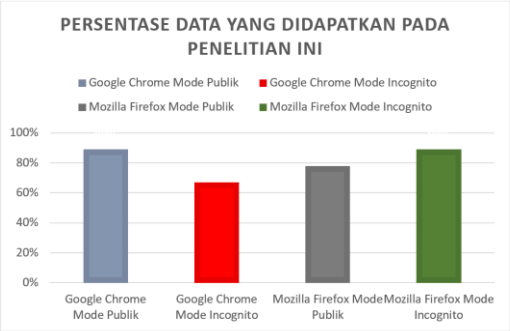
Tabel 2. Hasil Analisis Browser

Social Media	Evidence	Google Chrome		Mozilla Firefox	
		Mode Public	Mode Incognito	Mode Public	Mode Incognito
Facebook	User_id	ada	ada	ada	ada
	Password	ada	ada	ada	ada
	Email	ada	ada	ada	ada
Instagram	User_id	ada	ada	ada	ada
	Password	ada	Tidak ada	ada	ada
	Email	Tidak ada	Tidak ada	Tidak ada	ada

Twitter	User_id	ada	ada	ada	ada
	Password	ada	ada	ada	ada
	Email	ada	Tidak ada	Tidak ada	Tidak ada

Berikut ini adalah persentase data yang didapatkan pada penelitian ini dengan rumus:

$$\frac{Jumlah\ \ data\ yang\ didapat}{Total\ data\ per\ browser} \times 100\% \quad (1)$$



Gambar 43. Persentase Perbandingan Browser

4. SIMPULAN

Berdasarkan hasil penelitian yang sudah dilakukan dapat disimpulkan bahwa mengakses media sosial facebook, twitter tidak aman menggunakan browser Google Chrome dan Mozilla Firefox dengan mode publik maupun mode incognito karena user_id, email dan beberapa password masih terdeteksi pada tools FTK Imager. Dari hasil percobaan kedua browser tersebut, untuk mengakses instagram lebih aman digunakan dengan browser google chrome pada mode incognito karena pada mode tersebut hanya dapat menemukan user_id saja, sedangkan password dan email tidak ditemukan. Keterbatasan dalam penelitian ini hanya menggunakan dua browser dan tiga media sosial saja, diharapkan penelitian berikutnya dapat mengembangkan lagi dengan menggunakan media sosial yang lebih banyak, serta menggunakan tools dan metode yang berbeda agar menghasilkan lebih banyak informasi dari data-data yang diakuisisi karena setiap tools forensik mempunyai kekurangan dan kelebihan masing-masing

DAFTAR PUSTAKA

A. Antoni, "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online," *Nurani J. Kaji. Syari'ah dan Masy.*, vol. 17, no. 2, pp. 261–274, 2018, doi: 10.19109/nurani.v17i2.1192.

Mu'Minin & N. Anwar, "Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome , Mozilla Firefox , Opera Mode Incognito)," *Busiti*, vol. 1, no. 3, pp. 1–9, 2020.

Mustafa, I. Riadi, & R. Umar, "Rancangan Investigasi Forensik E-mail dengan Metode National Institute of Standards and Technology (NIST)," *Snst Ke-9*, vol. 9, pp. 121–124, 2018, [Online]. Available: https://publikasiilmiah.unwahas.ac.id/index.php/PROSIDING_SNST_FT/article/download/2385/2371.

Nabilla F. & Rini I., "P Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics" Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD 5(2) 185-192, 2022.

R. A. K. N. Bintang, R. Umar, & U. Yudhana, "Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.

R. A. Kinasih, A. Wirawan Muhammad, & W. Adi Prabowo, "Analisis Live Forensics Pada Keamanan Browser Untuk Mencegah Pencurian Akun (Studi Kasus: Facebook dan Instagram)," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 174–185, 2020, doi: 10.31849/digitalzone.v11i2.4678.