

# **Analisis Dampak Pengaturan Mode Keamanan Browser Terhadap Kelengkapan Data Forensik**

**Tugas Akhir**

**diajukan untuk memenuhi salah satu syarat**

**memperoleh gelar sarjana**

**pada Program Studi S1 Informatika**

**Fakultas Informatika**

**Universitas Telkom**

**1301174693**

**Bahtiar Cahyo Nugroho**



**Program Studi Sarjana Informatika**

**Fakultas Informatika**

**Universitas Telkom**

**Bandung**

**2024**

# LEMBAR PENGESAHAN

## **Analisis Dampak Pengaturan Mode Keamanan Browser Terhadap Kelengkapan Data Forensik**

**Analysis the Impact of Browser Security Mode Settings on Forensic Data Completeness**

**NIM :1301174693**

**Bahtiar Cahyo Nugroho**

Tugas akhir ini telah diterima dan disahkan untuk memenuhi sebagian syarat  
memperoleh gelar pada Program Studi Sarjana Informatika  
Fakultas Informatika Universitas Telkom

Bandung, 19 Juli 2024

Menyetujui

Pembimbing 1



Niken Dwi Wahyu Cahyani, S.T., M.Kom, Ph.D.

NIP: 00750052

Pembimbing 2



Satria Akbar Mugitama, S.Kom., M.Kom.

NIP: 20910043

Ketua Program Studi

Sarjana Informatika



Dr. Erwin Budi Setiawan, S.Si., M.T.

NIP: 00760045

## Analisis Dampak Pengaturan Mode Keamanan Browser Terhadap Kelengkapan Data Forensik

Bahtiar Cahyo Nugroho<sup>1</sup>, Niken Dwi Wahyu Cahyani<sup>2</sup>, Satria Akbar Mugitama<sup>3</sup>

<sup>1,2,3</sup>Fakultas Informatika, Universitas Telkom, Bandung

<sup>1</sup>bahtiar@student.telkomuniversity.ac.id,

<sup>2</sup>nikencahyani@telkomuniversity.ac.id, <sup>3</sup>satriamugitama@telkomuniversity.ac.id

---

### Abstrak

Internet sudah menjadi kebutuhan pokok manusia di zaman modern ini. Web browser menjadi salah satu program yang banyak dipakai untuk mengakses internet. Web browser juga menawarkan berbagai macam fitur seperti privasi, keamanan, kinerja penjelajahan internet dan pembersihan data. Dari beberapa fitur tersebut memungkinkan pengguna untuk menjelajahi internet tanpa menyimpan informasi apa pun di dalam web browser. Hal ini akan menjadi masalah jika pengguna melakukan suatu tindakan kriminal melalui web browser dengan fitur yang dirancang untuk tidak meninggalkan jejak digital. Sedangkan pencarian bukti digital dari aktivitas web *browsing* merupakan satu komponen penting dari penyelidikan digital forensik. Pada tugas akhir ini membahas tentang sejauh mana mode pengaturan keamanan browser memengaruhi data forensik yang didapatkan dengan menerapkan teknik akuisisi memori *live forensics* pada simulasi kasus yang melibatkan dua web browser yaitu Brave dan Opera GX. Serta dilakukan analisis terhadap data yang dapat dijadikan bukti digital dari hasil kegiatan simulasi. Dari tugas akhir ini berhasil diperoleh informasi jejak digital dari simulasi yang dilakukan terhadap tiga mode pengaturan keamanan browser.

**Kata Kunci:** web browser, live forensics, bukti digital.

---

### Abstract

The internet has become a basic human need in this modern era. Web browsers are one of the programs that are widely used to access the internet. Web browsers also offer a variety of features such as privacy, security, internet browsing performance and data cleaning. Some of these features allow users to browse the internet without saving any information in the web browser. This will be a problem if the user commits a crime through a web browser with features designed not to leave a digital traces. While searching for digital evidence from web browsing activities is an important component of digital forensic investigations. This final project discusses the extent to which browser security setting modes affect forensic data obtained by applying live forensics memory acquisition techniques to case simulations involving two web browsers, namely Brave and Opera GX. And an analysis of data that can be used as digital evidence from the results of simulation activities is carried out. From this final project, digital traces information was successfully obtained from simulations carried out on three browser security setting modes.

**Keywords:** web browser, live forensics, digital evidence.

---

## 1. Pendahuluan

### Latar Belakang

Internet saat ini sudah menjadi kebutuhan manusia karena internet sangat membantu manusia dalam berbagai aspek, mulai dari sumber informasi, bersosialisasi hingga berbisnis bisa dilakukan melalui internet. Salah satu alat untuk mengakses internet adalah dengan menggunakan web browser. Web browser merupakan salah satu program aplikasi untuk mengakses layanan yang tersedia pada situs web[1]. Pengguna dapat melakukan banyak aktivitas di internet melalui browser seperti mencari suatu informasi dari web, mengakses sosial media, mengunduh *file* dan sebagainya. Saat ini banyak sekali browser internet yang dirilis dengan berbagai nama seperti Google Chrome, Mozilla Firefox, Opera, Brave, dan lain-lain.

Selain itu web browser menyediakan berbagai fitur untuk menjaga keamanan penggunanya ketika menjelajahi internet, seperti mode *private* atau *incognito*, pencegahan pelacakan, anti *phishing*, pembersihan data, dan lain – lain. Namun fitur tersebut juga bisa dimanfaatkan oleh pengguna yang melakukan tindakan kriminal di internet dan melakukan kegiatan anti forensik untuk meminimalkan atau menghilangkan jejak digital. Salah satunya fitur mode *private* atau *incognito*, pada mode normal semua aktivitas yang dilakukan pengguna di dalam browser direkam dan disimpan disistem browser. Aktivitas yang telah dilakukan tersebut dapat dilihat pada riwayat penelusuran atau riwayat unduhan jika pengguna mengunduh suatu *file*. Sedangkan untuk mode *private*, aktivitas yang dilakukan pengguna di dalam browser tidak disimpan sehingga fitur ini memungkinkan pengguna untuk menjelajahi internet tanpa menyimpan informasi apa pun di dalam browser[2]. Pencarian bukti digital dari aktivitas browsing merupakan komponen penting dari penyelidikan digital forensik[3]. Sehingga diperlukan suatu metode penyidikan untuk mendapatkan data atau bukti digital dari web browser.

Pada tugas akhir ini membahas tentang analisis terhadap data artefak yang didapatkan dari tiga mode keamanan web browser dengan menerapkan teknik akuisisi memori *live forensics* yang melibatkan beberapa *tools* forensik. Penerapan teknik akuisisi *live forensics* ini dipilih karena teknik ini dinilai paling sesuai untuk kasus yang diuji. Lalu pada simulasi kasus melibatkan dua web browser yaitu Brave, dan Opera GX. Brave merupakan salah satu *secure* browser populer yang mengutamakan privasi dan keamanan penggunanya. Statistik pengguna aktif bulanan Brave browser pada bulan Januari 2024 mencapai 67,18 juta pengguna[5]. Selain itu Brave browser juga terus melakukan pengembangan fiturnya hingga saat ini. Dan Opera GX adalah varian khusus dari browser Opera yang dikhususkan untuk *gamers*. Browser ini juga dilengkapi dengan fitur privasi yang saat ini belum diteliti sampai mendalam. Pada simulasi, kedua browser tersebut disimpan pada *internal storage (hard disk)* komputer. Selanjutnya hasil akuisisi data dari simulasi tersebut dilakukan analisis untuk mengetahui seberapa banyak data bukti digital yang bisa didapatkan serta untuk menguji efektivitas dari metode yang dijalankan dalam tugas akhir ini.

### **Topik dan Batasannya**

Perumusan masalah tugas akhir ini adalah untuk mencari tahu sejauh mana pengaturan mode keamanan browser memengaruhi kelengkapan data forensik yang didapatkan serta bagaimana metode *live forensics* bisa mengakuisisi data forensik tersebut seperti data histori penelusuran internet dan akun untuk melakukan *login*. Batasan pada penelitian ini adalah simulasi pada penelitian ini dilakukan di dalam lingkungan yang terkontrol, semua perangkat yang digunakan sudah ditentukan. Serta simulasi melibatkan dua *secure* browser yaitu Brave dan Opera GX dengan tiga mode keamanan yaitu mode normal, mode *secure* dan mode *private* untuk masing-masing browser pada simulasi.

### **Tujuan**

Tujuan dari tugas akhir ini adalah melakukan analisis terhadap hasil akuisisi data seperti data histori penelusuran dan akun yang digunakan untuk *login* untuk mengetahui dampak dari pengaturan mode keamanan pada browser terhadap informasi jejak digital yang bisa didapatkan.

### **1. Studi Terkait**

Pada penelitian sebelumnya, Mahlous dan Mahlous (2020) melakukan penelitian pada mode *private* dari web browser Brave dengan mempelajari *private* browsing mode, memeriksa penjagaan privasi data dan akuisisi data forensik, serta menguraikan lokasi direktori dan jenis bukti yang tersedia melalui analisis *live* dan *post-mortem*. Dalam penelitian ini dilakukan pengambilan data dari RAM (Random Access Memory) dan hard disk dengan memanfaatkan tools seperti FTK Imager, WinHex, Internet Evidence Finder (IEF), dan Autopsy. Kesimpulan dari penelitian ini adalah *live memory analysis* dari memori RAM lebih efektif karena beberapa jenis artefak seperti URL, email, dan gambar dapat ditemukan. Sebaliknya, *post-mortem analysis* membawa ke jalan buntu bagi peneliti karena Brave berhasil menghapus semua data dan informasi terkait *private* browsing sessions dari hard disk[4].

## 2.1 Live Forensics

*Live forensics* merupakan metode yang memerlukan sebuah komputer dalam keadaan menyala. Semua data dari proses yang berjalan di dalam komputer berada pada memori RAM (Random Access Memory), dan data dari proses yang berjalan tersebut bersifat *volatile*[6].

## 2.2 Web Browser Forensics

Web browser *forensics* adalah cabang dari digital forensik yang bertujuan untuk mengidentifikasi dan mengumpulkan bukti dan informasi penting terkait suatu tindak kejahatan dari penemuan jejak pada sesi penjelajahan internet yang akan digunakan untuk investigasi forensik[4]. Browser dapat menyimpan informasi penting dari data pengguna dan aktivitas *browsing* dari *cached files* dan URL yang dikunjungi sampai *username* dan *password* yang dipakai saat sesi browsing. Artefak penting dari web browser pada web browser forensics antara lain adalah histori browser, downloads, login data, autofill data, bookmarks, cookies, dan cache.

## 2.3 Private Browsing

*Private browsing* merupakan istilah umum yang mereferensi pada mekanisme pada browser yang dirancang untuk mencegah pengguna menyimpan rekaman informasi aktivitas yang dilakukan selama menjelajahi internet. Sehingga browser tidak merekam data penelusuran internet yang dilakukan oleh pengguna.

## 2.4 Data Volatile

Data yang bersifat *volatile* merupakan data yang hilang atau terhapus jika perangkat komputer dimatikan[8]. RAM menyimpan data yang bersifat *volatile* dan data tersebut berperan penting untuk proses investigasi forensik karena data tersebut mengandung fragmen dari *file* yang terenkripsi, daftar proses aplikasi yang berjalan, dan koneksi jaringan[9].

## 2.5 Bukti Digital

Pencarian bukti digital yang ditinggalkan oleh aktivitas penelusuran internet pada web browser merupakan komponen penting dalam penyelidikan digital forensik. Hampir setiap kegiatan yang dilakukan di dalam web browser meninggalkan jejak di komputer. Bukti digital dapat memberikan informasi yang berguna untuk menunjukkan semua aktivitas yang dilakukan di dalam web browser[10].

## 2. Sistem yang Dibangun

### 3.1 Metode Akuisisi dan Analisis

Metode penelitian pada tugas akhir ini mengacu pada empat langkah dasar investigasi digital forensik dari NIST 800-86[11]. Metode tersebut ditunjukkan pada Gambar 1 berikut.



Gambar 1. Empat Tahap Dasar NIST 800-86.

Pada tahap pertama *Collection* ada beberapa kegiatan yang dilakukan, yang pertama kali dilakukan adalah mengidentifikasi potensial sumber data dan mendapatkan data dari situ. Dari kasus ini yang akan menjadi sumber data utama adalah memori RAM, karena banyak data penting dari program yang berjalan bisa didapatkan dari memori RAM[4]. Selain memori RAM, akan dilakukan pengambilan *file* yang berada di dalam folder browser tersebut, yaitu *file* History, Login Data, dan Web Data. Selanjutnya dilakukan *hashing* dengan tipe *hash* MD5 terhadap semua *file* data tersebut untuk memverifikasi integritas dari data tersebut, dengan memanfaatkan aplikasi Hashtool.

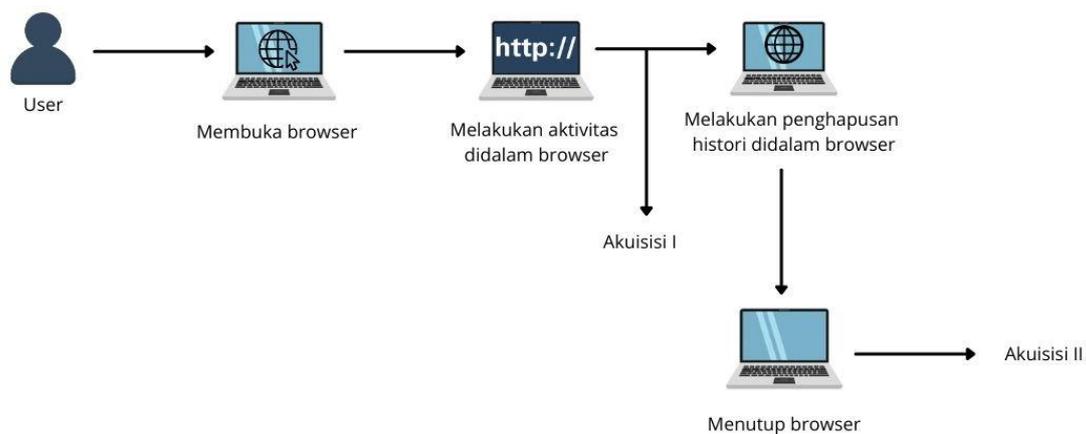
Tahap kedua *Examination*, yaitu dilakukannya pemeriksaan terhadap data yang sudah didapatkan. Pemeriksaan ini dilakukan untuk menilai dari semua data yang sudah dikumpulkan, mana data yang dapat diekstrak menjadi informasi yang relevan. Tahap ketiga *Analysis*, setelah informasi yang relevan berhasil

diekstrak, selanjutnya data tersebut dipelajari dan dilakukan analisis agar bisa ditarik kesimpulan. Tahap keempat *Reporting*, yaitu kegiatan untuk mempersiapkan dan menyajikan informasi akhir yang dihasilkan dari tahap analisis.

Tahap analisis dilakukan setelah skenario alur simulasi selesai dijalankan. Proses analisis dilakukan terhadap data dari hasil kegiatan *Collection* pada tahap akuisisi I yaitu ketika browser dalam keadaan masih terbuka dan akuisisi II yaitu setelah dilakukan penghapusan data histori dan browser sudah dalam keadaan tertutup dalam simulasi. Akuisisi I dan akuisisi II dilakukan untuk mengetahui perbedaan data yang mungkin didapatkan ketika browser dalam keadaan masih terbuka dan adanya kegiatan penghapusan data histori lalu browser ditutup. Nantinya hasil analisis akan memaparkan semua informasi bukti digital yang didapat dari proses simulasi tersebut dan dilakukan perbandingan terhadap informasi bukti digital yang didapatkan pada kedua browser tersebut.

### 3.2 Skenario Simulasi

Pada skenario alur simulasi kasus ini melibatkan dua browser yaitu Brave dan Opera GX. Skenario alur simulasi tersebut ditunjukkan pada Gambar 2 berikut.



Gambar 2. Skenario Alur Simulasi.

Skenario alur simulasi tersebut dilakukan terhadap kedua browser yaitu Brave dan Opera GX dengan tiga mode *browsing*, yaitu mode normal, mode *private* atau *incognito*, dan mode *secure*. Sehingga simulasi tersebut dilakukan sebanyak tiga kali untuk masing-masing browser. Penjelasan mengenai tahapan skenario dari alur simulasi untuk kedua browser adalah sebagai berikut.

1. *User* menyalakan laptop dan membuka browser yang disimpan di dalam komputer.
2. *User* melakukan aktivitas di dalam browser, berikut merupakan tabel aktivitas yang dilakukan *user* di dalam browser.

Tabel 1. Tabel Aktivitas User Di dalam Browser.

Tab	Aktivitas	Rincian
1	Pencarian Google dengan kata kunci "bookie7"	Dilanjutkan membuka web www.globalnewsnusantara.co.id. web tersebut merupakan situs judi online
2	Pencarian Google dengan kata kunci "judi online", "mobil", "motor", "togel"	Melakukan pencarian pada mesin pencari Google dengan kata kunci
3	Melakukan login pada mail.google.com	Email: radzigkob@gmail.com Password: KingdomC0me11
4	Mengunjungi situs www.detik.com	Situs media online
5	Melakukan login pada x.com	Username: @radzigkoby_la_ Password: KingdomSk411tz
6	Mengunjungi situs www.kompas.com	Situs media online
7	Mengunjungi situs saritotoasli.com	Situs judi online

8	Melakukan login pada www.instagram.com	Username: @ kingradzig Password: Deliv3r3nC
9	Mengunjungi situs www.cnbcindonesia.com	Situs media online

Tabel 2 untuk aktivitas *user* dibuat berdasarkan data artefak yang signifikan untuk *web browser forensics*. Pada *web browser forensics* bertujuan untuk mengidentifikasi dan mengumpulkan bukti serta informasi penting terkait kejahatan dari jejak yang ditemukan pada sesi penelusuran internet[4]. Pada tabel 2 terdapat keyword, url, serta akun untuk melakukan login, dan data tersebut merupakan informasi penting untuk proses *web browser forensics*.

3. Dilakukan akuisisi I, yaitu menjalankan metode *Collection* saat browser dalam keadaan masih terbuka.
4. Khusus untuk simulasi dengan browser pada mode normal dan *secure*, *user* melakukan penghapusan browsing di dalam browser sebelum *user* menutup browser. Untuk mode *private*, *user* tidak melakukan penghapusan histori di dalam browser karena pada mode *private* browser tidak merekam histori penjelajahan internet.
5. *User* menutup browser.
6. Dilakukan akuisisi II, yaitu menjalankan metode *Collection* forensik saat browser dalam keadaan sudah tertutup.

### 3. Evaluasi

#### 4.1 Data Hasil Simulasi

Pada simulasi yang dijalankan terdapat dua tahap akuisisi untuk pengambilan data, yaitu tahap akuisisi I dan akuisisi II. Tahap akuisisi tersebut dilakukan terhadap dua browser yaitu Brave dan Opera GX dengan tiga mode *browsing* yaitu mode normal, *private* dan *secure*. Pada tahap tersebut menjalankan *collection* atau pengumpulan data saat browser dalam keadaan masih terbuka untuk akuisisi I dan dilanjutkan penghapusan history di dalam browser (untuk mode normal dan *secure*) lalu menutup browser untuk akuisisi II. Data yang didapatkan pada tahap ini berupa *image memory* dari memori RAM dan beberapa *file* dari internal folder browser tersebut. Berikut uraian untuk data yang dikumpulkan.

##### 1. RAM Image Memory

Pengambilan data *image memory* RAM dilakukan dengan menggunakan aplikasi Magnet RAM Capture untuk kedua tahap akuisisi dari tersebut. Berikut merupakan tabel dari data *image memory* RAM yang didapatkan.

Tabel 2. File data image memory RAM.

Browser	Tahap	Nama File	Ukuran File	Hash MD5
Brave	Akuisisi I	brave_normal_1.raw	16,7 GB	49531bd64e625f408c859cfb8f8e9439
		brave_private_1.raw	16,7 GB	b74c41ba96bda714e1336b7a62072f5c
		brave_secure_1.raw	16,7 GB	0df7cca4ba4de57dd19aeb087725b11b
	Akuisisi II	brave_normal_2.raw	16,7 GB	142dd08b89a96a3e56e745618df97778
		brave_private_2.raw	16,7 GB	d3864389e86a5be6376bcf72a5880a
		brave_secure_2.raw	16,7 GB	897b60ad4924645580b0b4745f5ad299
Opera Gx	Akuisisi I	operagx_normal_1.raw	16,7 GB	3bbd45eabb3b65f75fe1679a45405aea
		operagx_private_1.raw	16,7 GB	0882c981060eb2b7c5ea68d9adc57767
		operagx_secure_1.raw	16,7 GB	3e3019d469e98a496311d566d35306ae

	Akuisisi II	operagx_normal_2.raw	16,7 GB	10252d3e3d41bf5b7dc2becec7e5f15d
		operagx_private_2.raw	16,7 GB	2715a8600a0d1ae66c3f67c551d30767
		operagx_secure_2.raw	16,7 GB	fc732773136609fef195f32fad1175f3

Semua *file* tersebut disimpan dalam *usb drive* yang sudah disediakan. Selain itu juga dilakukan *hashing* pada setiap *file image memory RAM* yang didapatkan untuk menjaga integritas data dari *file* tersebut.

2. *File* pada Internal Folder

Browser membuat sebuah folder di dalam penyimpanan sistem lokal komputer untuk menyimpan data. Untuk browser Brave dan Opera GX masing-masing memiliki internal folder dengan alamat direktori yang berbeda. Berikut merupakan alamat direktori untuk *file* data dari masing-masing browser.

Tabel 3. Direktori file data artefak.

File	Brave	Opera GX
History	C:\Users\<(namauser)\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default	C:\Users\<(namauser)\AppData\Roaming\Opera Software\Opera GX Stable
Login Data	C:\Users\<(namauser)\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default	C:\Users\<(namauser)\AppData\Roaming\Opera Software\Opera GX Stable
Web Data	C:\Users\<(namauser)\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default	C:\Users\<(namauser)\AppData\Roaming\Opera Software\Opera GX Stable

Di dalam direktori ini diambil tiga data atau *file*, yaitu History, Login Data, dan Web Data pada masing-masing tahap akuisisi I dan II.

4.2 Analisis Hasil Akuisisi

Setelah data dari tahap akuisisi I dan akuisisi II berhasil dikumpulkan, selanjutnya dilakukan *examination* atau pemeriksaan terhadap data tersebut untuk mencari artefak atau rekam jejak dari aktivitas yang dilakukan di dalam simulasi. Serta dilakukan analisis terhadap data tersebut. Berikut merupakan perbedaan pengaturan pada Brave browser dan Opera GX.

4.2.1 Akuisisi I

1) Brave browser mode normal

Pertama dilakukan pemeriksaan histori penelusuran internet. Data di dalam *file* History yang merupakan *database sql*. Namun *timeline* dalam data tersebut memiliki format *webkit time* sehingga perlu dilakukan konversi ke dalam format waktu lokal dengan *query*:

```
SELECT url, title,datetime((last_visit_time/1000000)-11644473600, 'unixepoch', 'localtime') AS time FROM urls;
```

Berikut merupakan gambar dari data histori penelusuran internetnya.

	url	title	time
1	https://www.google.com/search?...	bookie7 - Google Search	2024-07-09 19:28:03
2	https://www.globalnewsnusantara.co.id/	BOOKIE7 Slot Judi Online Server Thailand Super ...	2024-07-09 19:28:10
3	https://www.google.com/search?...	judi online - Google Search	2024-07-09 19:28:57
4	https://www.google.com/search?...	mobil - Google Search	2024-07-09 19:29:04
5	https://www.google.com/search?...	motor - Google Search	2024-07-09 19:29:09
6	https://www.google.com/search?...	togel - Google Search	2024-07-09 19:29:15
7	https://mail.google.com/	Gmail: Private and secure email at no cost   Goo...	2024-07-09 19:29:32
8	https://mail.google.com/mail/	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:29:58
9	https://mail.google.com/mail/u/0/	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:29:58
10	https://accounts.google.com/ServiceLogin?...	Gmail: Private and secure email at no cost   Goo...	2024-07-09 19:29:32
11	https://www.google.com/intl/en-US/gmail/about/	Gmail: Private and secure email at no cost   Goo...	2024-07-09 19:29:32
12	https://accounts.google.com/AccountChooser/signinchooser?...	Gmail	2024-07-09 19:29:34
13	https://accounts.google.com/AccountChooser?...	Gmail	2024-07-09 19:29:34
14	https://accounts.google.com/ServiceLogin?...	Gmail	2024-07-09 19:29:34
15	https://accounts.google.com/InteractiveLogin?continue=https://...	Gmail	2024-07-09 19:29:34
16	https://accounts.google.com/v3/signin/identifier?...	Gmail	2024-07-09 19:29:35
17	https://accounts.google.com/v3/signin/challenge/pwd?...	Gmail	2024-07-09 19:29:44
18	https://accounts.google.com/CheckCookie?continue=https://...	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:29:58
19	https://mail.google.com/accounts/SetOSID?...	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:29:58
20	https://accounts.youtube.com/accounts/SetSID?...	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:29:58
21	https://accounts.google.co.id/accounts/SetSID?...	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:29:58
22	https://mail.google.com/mail/u/0/#inbox	Kotak Masuk (24) - radzigkob@gmail.com - Gmail	2024-07-09 19:30:07
23	https://mail.google.com/mail/u/0/#inbox/...	Notifikasi keamanan - radzigkob@gmail.com - ...	2024-07-09 19:30:02
24	https://www.detik.com/	detikcom - Informasi Berita Terkini dan Terbaru ...	2024-07-09 19:45:30
25	https://connect.detik.com/token/me.html?autoLogin=1&clientId=2		2024-07-09 19:45:32
26	https://x.com/	X. It's what's happening / X	2024-07-09 19:32:06
27	https://twitter.com/x/migrate?...	x.com	2024-07-09 19:32:04
28	https://x.com/?mx=2	x.com/?mx=2	2024-07-09 19:32:34
29	https://x.com/login	X. It's what's happening / X	2024-07-09 19:32:08
30	https://x.com/i/flow/login	Log in to X / X	2024-07-09 19:32:08
31	https://x.com/home?mx=2	X	2024-07-09 19:32:34
32	https://x.com/home	(18) Home / X	2024-07-09 19:32:43
33	https://x.com/radzigkobylya_	(18) Radzig Kobyla (@radzigkobylya_) / X	2024-07-09 19:32:40
34	https://www.kompas.com/	Berita Terkini Hari Ini, Kabar Akurat Terpercaya - ...	2024-07-09 19:49:56
35	http://saritotoasli.com/	SARITOTO - Game Slot Togel Online & Platform ...	2024-07-09 19:34:38
36	https://saritotoasli.com/	SARITOTO - Game Slot Togel Online & Platform ...	2024-07-09 19:34:53
37	https://www.instagram.com/	Instagram	2024-07-09 19:35:45
38	https://www.instagram.com/accounts/onetap?next=%2F	Instagram	2024-07-09 19:35:35
39	https://www.instagram.com/kingradzig/	Radzig Kobyla (@kingradzig) • Instagram photos ...	2024-07-09 19:35:43
40	https://www.cnbcindonesia.com/	CNBC Indonesia - Berita Ekonomi & Bisnis Terkini...	2024-07-09 19:56:19

Gambar 3. History Brave browser.

Selain dari file History, *username* juga dapat ditemukan di dalam file Web Data. Dan sama seperti *file* History, waktu dalam data tersebut memiliki format *unix epoch time* sehingga perlu dilakukan konversi dengan *query*:

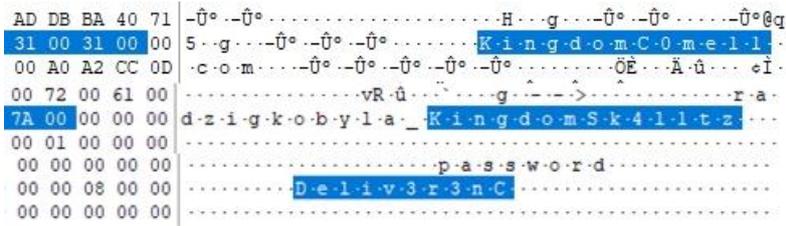
```
SELECT value, DATETIME(date_created, 'unixepoch', 'localtime') AS date_created,
DATETIME(date_last_used, 'unixepoch', 'localtime') AS date_last_used FROM autofill;
```

Berikut merupakan gambar dari data pada *file* Web Data

	value	date_created	date_last_used
1	radzigkob@gmail.com	2024-07-09 19:29:44	2024-07-09 19:29:44
2	@radzigkobylya_	2024-07-09 19:32:19	2024-07-09 19:32:19
3	@kingradzig	2024-07-09 19:35:34	2024-07-09 19:35:34

Gambar 4. Username Brave browser.

Selanjutnya dilakukan pencarian data *password* yang digunakan untuk melakukan *login*, cara untuk mencari data *password* dengan melalui *file image memory* RAM brave\_normal\_1.raw dengan memanfaatkan FTK Imager.



Gambar 5. Password Brave browser.

2) Brave browser mode private

Pertama dilakukan pemeriksaan histori penelusuran internet. Untuk data histori penelusuran serta akun dan *password* didapatkan melalui *file image memory* RAM dengan nama *file* *brave\_private\_1.raw* dengan memanfaatkan FTK Imager.



Gambar 6. History, username, dan password Brave browser.

3) Brave browser mode secure

Pertama dilakukan pemeriksaan histori penelusuran internet. Sama seperti pada mode normal, data ini bisa didapatkan melalui *file* History.

	url	title	time
1	https://www.google.com/search?...	bookie7 - Penelusuran Google	2024-07-13 20:45:51
2	https://www.google.com/sorry/index?...	https://www.google.com/search?...	2024-07-13 20:45:38
3	https://www.google.com/search?...	bookie7 - Penelusuran Google	2024-07-13 20:45:48
4	https://www.globalnewsusantara.co.id/	BOOKIE7 Slot Judi Online Server ...	2024-07-13 20:46:06
5	https://www.google.com/search?...	judi online - Penelusuran Google	2024-07-13 20:46:24
6	https://www.google.com/search?...	mobil - Penelusuran Google	2024-07-13 20:46:30
7	https://www.google.com/search?...	motor - Penelusuran Google	2024-07-13 20:46:38
8	https://www.google.com/search?...	togel - Penelusuran Google	2024-07-13 20:46:46
9	https://mail.google.com/	Gmail: Private and secure email at no ...	2024-07-13 20:47:10
10	https://mail.google.com/mail/	Kotak Masuk (25) - ...	2024-07-13 20:47:32
11	https://mail.google.com/mail/u/0/	Kotak Masuk (25) - ...	2024-07-13 20:47:32
12	https://accounts.google.com/ServiceLogin?...	Gmail: Private and secure email at no ...	2024-07-13 20:47:10
13	https://www.google.com/intl/en-US/gmail/about/	Gmail: Private and secure email at no ...	2024-07-13 20:47:10
14	https://accounts.google.com/AccountChooser/...	Gmail	2024-07-13 20:47:13
15	https://accounts.google.com/AccountChooser?...	Gmail	2024-07-13 20:47:13
16	https://accounts.google.com/ServiceLogin?...	Gmail	2024-07-13 20:47:13
17	https://accounts.google.com/InteractiveLogin?...	Gmail	2024-07-13 20:47:13
18	https://accounts.google.com/v3/signin/identifier...	Gmail	2024-07-13 20:47:13
19	https://accounts.google.com/v3/signin/challenge...	Gmail	2024-07-13 20:47:20
20	https://accounts.google.com/CheckCookie?...	Kotak Masuk (25) - ...	2024-07-13 20:47:32
21	https://mail.google.com/accounts/SetOSID?...	Kotak Masuk (25) - ...	2024-07-13 20:47:32
22	https://accounts.youtube.com/accounts/SetSID?...	Kotak Masuk (25) - ...	2024-07-13 20:47:32
23	https://accounts.google.co.id/accounts/SetSID?...	Kotak Masuk (25) - ...	2024-07-13 20:47:32
24	https://mail.google.com/mail/u/0/#inbox	Kotak Masuk (25) - ...	2024-07-13 20:47:33
25	https://www.detik.com/	detikcom - Informasi Berita Terkini da...	2024-07-13 21:02:52
26	https://connect.detik.com/token/me.html?...		2024-07-13 21:02:54
27	https://x.com/	X. It's what's happening / X	2024-07-13 20:48:07
28	https://twitter.com/x/migrate?...	x.com	2024-07-13 20:48:05
29	https://x.com/?mx=2	x.com/?mx=2	2024-07-13 20:48:34
30	https://x.com/login	X. It's what's happening / X	2024-07-13 20:48:09
31	https://x.com/i/flow/login	Log in to X / X	2024-07-13 20:48:09
32	https://x.com/home?mx=2	X	2024-07-13 20:48:34
33	https://x.com/home	(20) Home / X	2024-07-13 20:48:47
34	https://x.com/radzigkobylya_	(20) Radzig Kobyla (@radzigkobylya_) ...	2024-07-13 20:48:44
35	https://www.kompas.com/	Berita Terkini Hari Ini, Kabar Akurat ...	2024-07-13 20:49:00
36	https://saritotoasli.com/	SARITOTO - Game Slot Togel Online &...	2024-07-13 20:49:35
37	http://saritotoasli.com/	SARITOTO - Game Slot Togel Online &...	2024-07-13 20:49:35
38	https://saritotojamin.com/	SARITOTO - Game Slot Togel Online &...	2024-07-13 20:49:35
39	https://www.instagram.com/	Instagram	2024-07-13 20:50:09
40	https://www.instagram.com/accounts/onetap/?...	Instagram	2024-07-13 20:50:32
41	https://www.instagram.com/accounts/...	Instagram	2024-07-13 20:50:32
42	https://www.cnbcindonesia.com/	CNBC Indonesia - Berita Ekonomi & ...	2024-07-13 21:00:59

Gambar 7. History Brave browser.

Selain dari file History, username juga dapat ditemukan di dalam file Web Data.

	value	date_created	date_last_used
1	radzigkob@gmail.com	2024-07-13 20:47:20	2024-07-13 20:47:20
2	@radzigkobylya_	2024-07-13 20:48:20	2024-07-13 20:48:20
3	@kingradzig	2024-07-13 20:50:31	2024-07-13 20:50:31

Gambar 8. Username Brave browser.

Selanjutnya dilakukan pencarian data password yang digunakan untuk melakukan login, cara untuk mencari data password dengan melalui file image memory RAM brave\_secure\_1.raw dengan memanfaatkan FTK Imager.

```

0A 40 72 61 64 sia.com...radzigkob@gmail.com..KingdomC0mell...@rad
33 72 33 6E 43 zigkobyla_..KingdomSk4lltz...@kingradzig..Deliv3r3nC
00 00 00 00 00 ..yÿÿÿ-yG.....
00 00 00 00 00 .....
    
```

Gambar 9. Password Brave browser.

4) Opera GX mode normal

Pertama dilakukan pemeriksaan histori penelusuran internet. Data ini bisa didapatkan di dalam file History.

	url	title	time
1	https://gxcorner.games/	GX Corner	2024-07-07 18:16:56
2	https://www.google.com/search?client=opera-...	bookie7 - Penelusuran Google	2024-07-07 18:18:05
3	https://www.google.com/url?...	BOOKIE7 Slot Judi Online Server Thailand Super ...	2024-07-07 18:18:15
4	https://www.globalnewsusantara.co.id/	BOOKIE7 Slot Judi Online Server Thailand Super ...	2024-07-07 18:18:15
5	https://www.google.com/search?client=opera-...	judi online - Penelusuran Google	2024-07-07 18:18:52
6	https://www.google.com/search?q=mobil&client=opera-...	mobil - Penelusuran Google	2024-07-07 18:19:03
7	https://www.google.com/search?q=motor&client=opera-...	motor - Penelusuran Google	2024-07-07 18:19:10
8	https://www.google.com/search?q=togel&client=opera-...	togel - Penelusuran Google	2024-07-07 18:19:21
9	https://mail.google.com/	Gmail: Private and secure email at no cost   Goo...	2024-07-07 18:19:33
10	https://mail.google.com/mail/	Kotak Masuk (23) - radzigkob@gmail.com - Gmail	2024-07-07 18:20:02
11	https://mail.google.com/mail/u/0/	Kotak Masuk (23) - radzigkob@gmail.com - Gmail	2024-07-07 18:20:02
12	https://accounts.google.com/ServiceLogin?...	Gmail: Private and secure email at no cost   Goo...	2024-07-07 18:19:33
13	https://www.google.com/intl/en-US/gmail/about/	Gmail: Private and secure email at no cost   Goo...	2024-07-07 18:19:33
14	https://accounts.google.com/AccountChooser/signinchooser...	Gmail	2024-07-07 18:19:37
15	https://accounts.google.com/AccountChooser?...	Gmail	2024-07-07 18:19:37
16	https://accounts.google.com/ServiceLogin?...	Gmail	2024-07-07 18:19:37
17	https://accounts.google.com/InteractiveLogin?...	Gmail	2024-07-07 18:19:37
18	https://accounts.google.com/v3/signin/identifier?...	Gmail	2024-07-07 18:19:37
19	https://accounts.google.com/v3/signin/challenge/pwd?...	Gmail	2024-07-07 18:19:46
20	https://accounts.google.com/CheckCookie?continue=https:/...	Kotak Masuk (23) - radzigkob@gmail.com - Gmail	2024-07-07 18:20:02
21	https://mail.google.com/accounts/SetOSID?...	Kotak Masuk (23) - radzigkob@gmail.com - Gmail	2024-07-07 18:20:02
22	https://accounts.google.co.id/accounts/SetsID?...	Kotak Masuk (23) - radzigkob@gmail.com - Gmail	2024-07-07 18:20:02
23	https://mail.google.com/mail/u/0/#inbox	Kotak Masuk (23) - radzigkob@gmail.com - Gmail	2024-07-07 18:20:12
24	https://mail.google.com/mail/u/0/#inbox/...	Notifikasi keamanan - radzigkob@gmail.com - ...	2024-07-07 18:20:11
25	https://www.detik.com/	detikcom - Informasi Berita Terkini dan Terbaru ...	2024-07-07 18:35:27
26	https://x.com/	X. It's what's happening / X	2024-07-07 18:21:16
27	https://twitter.com/x/migrate?...	x.com	2024-07-07 18:21:12
28	https://x.com/?mx=2	x.com/?mx=2	2024-07-07 18:21:45
29	https://x.com/login	X. It's what's happening / X	2024-07-07 18:21:22
30	https://x.com/flow/login	Log in to X / X	2024-07-07 18:21:22
31	https://x.com/home?mx=2	X	2024-07-07 18:21:45
32	https://x.com/home	(14) Home / X	2024-07-07 18:21:56
33	https://x.com/radzigkobyla_	(14) Radzig Kobyla (@radzigkobyla_) / X	2024-07-07 18:21:53
34	https://www.kompas.com/	Berita Terkini Hari Ini, Kabar Akurat Terpercaya -...	2024-07-07 18:22:08
35	https://saritotoasli.com/	SARITOTO - Game Slot Togel Online & Platform ...	2024-07-07 18:23:11
36	https://www.instagram.com/	Instagram	2024-07-07 18:24:19
37	https://www.instagram.com/accounts/onetap/?next=%2F	Instagram	2024-07-07 18:24:06
38	https://www.instagram.com/kingradzig/	Radzig Kobyla (@kingradzig) • Instagram photos ...	2024-07-07 18:24:17
39	https://www.cnbcindonesia.com/	CNBC Indonesia - Berita Ekonomi & Bisnis Terkini...	2024-07-07 18:34:40

Gambar 10. History Opera GX.

Berikut merupakan gambar dari data pada file Web Data dan Login Data.

	value	date_created	date_last_used
1	radzigkob@gmail.com	2024-07-07 18:19:47	2024-07-07 18:19:47
2	@radzigkobyla_	2024-07-07 18:21:33	2024-07-07 18:21:33
3	@kingradzig	2024-07-07 18:24:05	2024-07-07 18:24:05

Gambar 11. Web Data pada Opera GX.





6) Opera GX mode secure

Pertama dilakukan pemeriksaan histori penelusuran internet. Data di dalam *file* History, berikut merupakan gambar dari data histori penelusuran internetnya.

	url	title	time
1	https://gxcorner.games/	GX Corner	2024-07-07 23:31:52
2	https://www.google.com/search?client=opera-...	bookie7 - Penelusuran Google	2024-07-07 23:35:08
3	https://www.google.com/url?...	BOOKIE7 Slot Judi Online Server Thailand Super Lin...	2024-07-07 23:35:14
4	https://www.globalnewsusantara.co.id/	BOOKIE7 Slot Judi Online Server Thailand Super Lin...	2024-07-07 23:35:15
5	https://www.google.com/search?client=opera-...	judi online - Penelusuran Google	2024-07-07 23:35:52
6	https://www.google.com/search?q=mobil&client=opera...	mobil - Penelusuran Google	2024-07-07 23:35:43
7	https://www.google.com/search?q=mobil&client=opera...	mobil - Penelusuran Google	2024-07-07 23:35:59
8	https://www.google.com/search?q=motor&client=oper...	motor - Penelusuran Google	2024-07-07 23:36:04
9	https://www.google.com/search?q=togel&client=opera...	togel - Penelusuran Google	2024-07-07 23:36:09
10	https://mail.google.com/	Gmail: Private and secure email at no cost   Google...	2024-07-07 23:36:20
11	https://mail.google.com/mail/	Kotak Masuk (22) - radzigkob@gmail.com - Gmail	2024-07-07 23:36:43
12	https://mail.google.com/mail/u/0/	Kotak Masuk (22) - radzigkob@gmail.com - Gmail	2024-07-07 23:36:43
13	https://accounts.google.com/ServiceLogin?...	Gmail: Private and secure email at no cost   Google...	2024-07-07 23:36:20
14	https://www.google.com/intl/en-US/gmail/about/	Gmail: Private and secure email at no cost   Google...	2024-07-07 23:36:20
15	https://accounts.google.com/AccountChooser/...	Gmail	2024-07-07 23:36:23
16	https://accounts.google.com/AccountChooser?...	Gmail	2024-07-07 23:36:23
17	https://accounts.google.com/ServiceLogin?...	Gmail	2024-07-07 23:36:23
18	https://accounts.google.com/InteractiveLogin?...	Gmail	2024-07-07 23:36:23
19	https://accounts.google.com/v3/signin/identifier?...	Gmail	2024-07-07 23:36:24
20	https://accounts.google.com/v3/signin/challenge/pwd?...	Gmail	2024-07-07 23:36:31
21	https://accounts.google.com/CheckCookie?...	Kotak Masuk (22) - radzigkob@gmail.com - Gmail	2024-07-07 23:36:43
22	https://mail.google.com/accounts/SetOSID?...	Kotak Masuk (22) - radzigkob@gmail.com - Gmail	2024-07-07 23:36:43
23	https://accounts.google.co.id/accounts/SetSID?...	Kotak Masuk (22) - radzigkob@gmail.com - Gmail	2024-07-07 23:36:43
24	https://mail.google.com/mail/u/0/#inbox	Kotak Masuk (22) - radzigkob@gmail.com - Gmail	2024-07-07 23:36:54
25	https://mail.google.com/mail/u/0/#inbox/...	Notifikasi keamanan - radzigkob@gmail.com - Gmail	2024-07-07 23:36:53
26	https://www.detik.com/	detikcom - Informasi Berita Terkini dan Terbaru Har...	2024-07-07 23:37:03
27	https://x.com/	X. It's what's happening / X	2024-07-07 23:37:24
28	https://twitter.com/x/migrate?...	x.com	2024-07-07 23:37:20
29	https://x.com/?mx=2	x.com/?mx=2	2024-07-07 23:37:51
30	https://x.com/login	X. It's what's happening / X	2024-07-07 23:37:27
31	https://x.com/i/flow/login	Log in to X / X	2024-07-07 23:37:27
32	https://x.com/home?mx=2	X	2024-07-07 23:37:52
33	https://x.com/home	(16) Home / X	2024-07-07 23:38:02
34	https://x.com/radzigkobylya_	(16) Radzig Kobyla (@radzigkobylya_) / X	2024-07-07 23:38:00
35	https://www.kompas.com/	Berita Terkini Hari Ini, Kabar Akurat Terpercaya - ...	2024-07-07 23:38:11
36	https://saritotoasli.com/	SARITOTO - Game Slot Togel Online & Platform ...	2024-07-07 23:38:44
37	https://www.instagram.com/	Instagram	2024-07-07 23:40:30
38	https://www.instagram.com/accounts/onetap?...	Instagram	2024-07-07 23:40:17
39	https://www.instagram.com/kingradzig/	Radzig Kobyla (@kingradzig) • Instagram photos a...	2024-07-07 23:40:28
40	https://www.cnbcindonesia.com/	CNBC Indonesia - Berita Ekonomi & Bisnis Terkini ...	2024-07-07 23:50:51

Gambar 16. History Opera GX.

Berikut merupakan gambar dari data pada *file* Web Data dan Login Data.

	value	date_created	date_last_used
1	radzigkob@gmail.com	2024-07-07 23:36:31	2024-07-07 23:36:31
2	@radzigkobylya_	2024-07-07 23:37:38	2024-07-07 23:37:38
3	@kingradzig	2024-07-07 23:40:15	2024-07-07 23:40:15

Gambar 17. Web Data pada Opera GX.

	origin_url	date_created
1	https://accounts.google.com/	2024-07-07 23:36:49
2	https://x.com/	2024-07-07 23:37:53
3	https://www.instagram.com/	2024-07-07 23:40:20

Gambar 18. Login Data pada Opera GX.







Tabel 4. Timestamp histori Opera Gx.

	Data	Keterangan	waktu
1	bookie7 - Penelusuran Google	keyword	07 Juli 2024 18:18:03
2	www.globalnewsnusantara.co.id	url	07 Juli 2024 18:18:20
3	judi online - Penelusuran Google	keyword	07 Juli 2024 18:18:52
4	mobil - Penelusuran Google	keyword	07 Juli 2024 18:19:05
5	motor - Penelusuran Google	keyword	07 Juli 2024 18:19:11
6	togel - Penelusuran Google	keyword	07 Juli 2024 18:19:21
7	mail.google.com	url	07 Juli 2024 18:20:12
8	www.detik.com	url	07 Juli 2024 18:35:31
9	x.com	url	07 Juli 2024 18:21:56
10	www.kompas.com	url	07 Juli 2024 18:22:50
11	saritotoasli.com	url	07 Juli 2024 18:23:22
12	www.instagram.com	url	07 Juli 2024 18:24:19
13	www.cnbcindonesia.com	url	07 Juli 2024 18:24:38

5) Opera GX mode private

Pertama dilakukan pemeriksaan histori penelusuran internet. Data histori penelusuran serta akun dan password didapatkan melalui file image memory RAM dengan nama file operagx\_private\_2.raw dengan memanfaatkan FTK Imager.

```

22 3A 6E 75 6C .....opera-touch-recent-tabs- "[{"id":nul
3D 6F 70 65 72 l, "url": "https://www.google.com/search?client=oper
22 2C 5C 22 74 a-gx&q=bookie7&sourceid=operasie=UTF-8&oe=UTF-8", "t
05 D2 1F 15 00 itlH..á...H..2...H..Û...HÇ..Ø.....HÇ..Û.....HÇ..Û...
00 00 00 00 00 ..s...https://www.globalnewsnusantara.co.id/.....
00 78 00 00 00 .....x.....
68 3F 71 3D 6A .....G.....G.....https://www.google.com/search?q=j
38 62 37 36 36 udi+online&client=opera-gx&hs=9LD&asca_esv=5253a18b766
67 6F 6F 67 6C cent-tabs- "[{"id":null, "url": "https://www.googl
65 73 76 3D 31 e.com/search?q=mobil&client=opera-gx&hs=n19&asca_esv=1
5C 22 75 72 6C .....opera-touch-recent-tabsE "[{"id":null, "url
74 3D 6F 70 65 \": "https://www.google.com/search?q=motor&client=ope
53 4B 59 32 4B ra-gx&hs=y19&asca_esv=14ed951b5469336&sei=qXmKZsH5KY2K
22 69 64 5C 22 ¥.....opera-touch-recent-tabsØ "[{"id\
2F 23 69 6E 62 :null, "url": "https://mail.google.com/mail/u/0/#inb
6D 2F 5C 22 2C sú- "[{"id":null, "url": "https://www.detik.com/\",
64 61 6E 20 54 \", "title": "detikcom - Informasi Berita Terkini dan T
CA 03 22 5B 7B 9]]"+YÁ-ñ.....opera-touch-recent-tabsE "[{
3A 5C 22 78 2E \": "https://x.com/\", "title": "x.
32 35 63 34 31 08ccc6191386x-Äc^Ûp-.....xO°...ÿÿ471425c4l
00 00 00 00 00 fe4965ee5&origin=https%3A%2F%2Fwww.kompas.com.....
FF FF 00 00 00 .....kú.....È-içÖÜ"-Á.....ÿÿ-ü*-TpWoY»l...ÿÿ...
00 00 00 00 00 .....
22 74 69 74 6C d":null, "url": "https://saritotoasli.com/\", "titl
72 6D 20 48 69 e": "SARITOTO - Game Slot Togel Online & Platform Hi
6D 2E 63 6F 6D sú- "[{"id":null, "url": "https://www.instagram.com
61 6D 5C 22 2C /accounts/onetap/?next=%2F", "title": "Instagram",
43 20 49 6E 64 https://www.cnbcindonesia.com/\", "title": "CNBC Ind
69 5C 22 2C 5C onesia - Berita Ekonomi & Bisnis Terkini Hari Ini", \
72 61 6E 20 47 le.com/favicon.ico.....".....togel - Penelusuran G
3F 71 3D 74 6F oogle.....".....https://www.google.com/search?q=t
36 61 63 26 73 gel&client=opera-gx&hs=60Y&asca_esv=07cb220601c5e6ács

```

Gambar 28. History Opera Gx.

```

00 36 00 00 00 /ssl.gstatic.com/ui/v1/icons/mail/rfr/gmail.ico-6...
69 6C 00 00 2F ...Kotak Masuk (22) - radzigkob@gmail.com - Gmail.../
00 00 00 00 00 ...'...https://mail.google.com/mail/u/0/#inbox.....
20 00 52 00 61 o-m-p..d-l-l...^#Om-vø-N-øÿüí; #ÿ#çð{-(.l.5.)- R.a
00 6C 00 61 00 -d-z-i-g- K-o-b-y-l-a- (@-r-a-d-z-i-g-k-o-b-y-l-a
00 00 01 00 00 )- /-X-...-O-p-e-r-a...U2...Wá*ÿ{ç7\...
00 00 00 00 00 .....
64 65 6F 73 5C Kobyła (@kingradzig) á-c Instagram photos and videos\

```

Gambar 29. Email dan username Opera Gx.

6) Opera GX mode secure

Pertama dilakukan pemeriksaan histori penelusuran internet. Data histori penelusuran serta akun dan password didapatkan melalui file image memory RAM dengan nama file operagx\_secure\_2.raw dengan memanfaatkan FTK Imager.

```

5C 22 3A 5C 22 | \":\bookie7 - Penelusuran Google\,\favIconUrl\:\
72 6C 5C 22 3A | \",\timestamp\":1720370102944},{\id\":null,\url\":
5C 22 74 69 74 | rl\":\https://www.globalnewsnusantara.co.id/\,\tit
53 75 70 65 72 | le\":\BOOKIE7 Slot Judi Online Server Thailand Super
22 74 69 6D 65 | Link Gacor Terbaru 2024\,\favIconUrl\:\",\time
72 61 6E 20 47 | -8&oe=UTF-8\,\title\":\judi online - Penelusuran G
30 31 33 35 33 | oogle\,\favIconUrl\:\",\timestamp\":17203701353
73 6E 75 73 61 | 41},{\id\":null,\url\":\https://www.globalnewsnusa
6F 6E 55 72 6C | \title\":\mobil - Penelusuran Google\,\favIconUri
6C 2C 5C 22 75 | \":\",\timestamp\":1720370159472},{\id\":null,\u
47 6F 6F 6F 6C | =gws-wiz-serp\,\title\":\motor - Penelusuran Googl
37 33 31 7D 2C | e\,\favIconUrl\:\",\timestamp\":1720370164731},
6C 20 2D 20 50 | LjGgB8Qissclient=gws-wiz-serp\,\title\":\toge - P
61 6D 70 5C 22 | enelusuran Google\,\favIconUrl\:\",\timestamp\
77 77 2E 67 6C | :1720370169343},{\id\":null,\url\":\https://www.gl
6C 2F 75 2F 30 | id\":null,\url\":\https://mail.google.com/mail/u/0
69 67 6B 6F 62 | /#inbox\,\title\":\Notifikasi keamanan - radzigkob
74 61 6D 70 5C | @gmail.com - Gmail\,\favIconUrl\:\",\timestamp\
77 77 77 2E 67 | :1720370214661},{\id\":null,\url\":\https://www.g
77 77 77 2E 64 | h-recent-tabs=\{\{\id\":null,\url\":\https://www.d
69 74 61 20 54 | etik.com/\,\title\":\detikcom - Informasi Berita T
22 2C 5C 22 74 | erkini dan Terbaru Hari Ini\,\favIconUrl\:\",\t
22 68 74 74 70 | imestamp\":1720370228218},{\id\":null,\url\":\http
2F 68 6F 6D 65 | 0370298142},{\id\":null,\url\":\https://x.com/home
5F 29 20 2F 20 | \,\title\":\@radzigkobylya (@radzigkobylya) /
36 39 39 7D 5D | X\,\favIconUrl\:\",\timestamp\":1720370282699}}
65 5C 22 3A 5C | :null,\url\":\https://www.kompas.com/\,\title\":\
61 20 2D 20 4B | "Berita Terkini Hari Ini, Kabar Akurat Terpercaya - K
32 30 33 37 30 | ompas.com\,\favIconUrl\:\",\timestamp\":1720370
65 5C 22 2C 5C | 298142},{\id\":null,\url\":\https://x.com/home\,\
49 54 4F 54 4F | \":\https://saritotoasli.com/\,\title\":\SARITOTO
62 61 69 6B 20 | - Game Slot Togel Online & Platform Hiburan Terbaik
00 00 00 00 01 | 2024\,\timestamp\":1720370405414}} 4bPg..R.....
77 2E 69 6E 73 | 1720371111332},{\id\":null,\url\":\https://www.ins
64 7A 69 67 29 | tagram.com/\,\title\":\Radzig Kobylya (@kingradzig
22 3A 5C 22 5C | â-e Instagram photos and videos\,\favIconUrl\:\
00 00 00 00 00 | \",\timestamp\":1720370430760}}.....
00 00 00 00 00 |
2C 5C 22 74 69 | :null,\url\":\https://www.cnbcindonesia.com/\,\ti
20 54 65 72 6B | tle\":\CNBC Indonesia - Berita Ekonomi & Bisnis Terk
69 6E 64 6F 6E | ini Hari Ini\,\favIconUrl\":\https://cdn.cnbcindon
65 73 74 61 6D | esia.com/cnbc/images/favicon.png?v=6.2.6\,\timestam
2F 2F 77 77 77 | p\":1720371052856},{\id\":null,\url\":\https://www
    
```

Gambar 30. History Opera Gx.

```

69 67 6B 6F 62 | /#inbox\,\title\":\Notifikasi keamanan - radzigkob
74 61 6D 70 5C | @gmail.com - Gmail\,\favIconUrl\:\",\timestamp\
3A 5C 22 28 31 | \":null,\url\":\https://x.com/home\,\title\":\@radzigkobylya (@radzigkobylya) / X\,\favIconUrl\
6E 55 72 6C 5C | 4) Radzig Kobylya (@radzigkobylya) / X\,\favIconUrl\
62 79 6C 61 20 | tps://www.instagram.com/\,\title\":\Radzig Kobylya
5C 22 66 61 76 | (@kingradzig) â-e Instagram photos and videos\,\fav
    
```

Gambar 31. Email dan username Opera Gx.

Dari gambar 60 dan gambar 61 bisa ditemukan semua histori penelusuran internet beserta timestamp atau waktu dari histori penelusuran tersebut.

Tabel 5. Timestamp histori Opera Gx.

	Data	Keterangan	waktu
1	bookie7 - Penelusuran Google	keyword	07 Juli 2024 23:35:02
2	www.globalnewsnusantara.co.id	url	07 Juli 2024 23:35:19
3	judi online - Penelusuran Google	keyword	07 Juli 2024 23:35:35

4	mobil - Penelusuran Google	keyword	07 Juli 2024 23:35:59
5	motor - Penelusuran Google	keyword	07 Juli 2024 23:36:04
6	togel - Penelusuran Google	keyword	07 Juli 2024 23:36:09
7	mail.google.com	url	07 Juli 2024 23:36:54
8	www.detik.com	url	07 Juli 2024 23:37:08
9	x.com	url	07 Juli 2024 23:38:02
10	www.kompas.com	url	07 Juli 2024 23:38:18
11	saritotoasli.com	url	07 Juli 2024 23:40:05
12	www.instagram.com	url	07 Juli 2024 23:40:30
13	www.cnbcindonesia.com	url	07 Juli 2024 23:50:52

### 4.3 Rangkuman Hasil Analisis

Setelah dilakukan pemaparan data analisis dari hasil akuisisi yang didapatkan dari simulasi, berikut merupakan rangkuman dari seluruh hasil analisis tersebut.

#### 4.3.1 Akuisisi I

Tabel 6. Data Hasil Akuisisi I.

Tab	Data	Keterangan	Brave Browser			Opera GX		
			Mode Normal	Mode Private	Mode Secure	Mode Normal	Mode Private	Mode Secure
1	'bookie7', www.globalnewsnusantara.co.id	Keyword, url	ada	ada	ada	ada	ada	ada
2	'judi online', 'mobil', 'motor', 'togel'	keyword	ada	ada	ada	ada	ada	ada
3	mail.google.com, Email: radzigkob@gmail.com Password: KingdomC0me11	url, akun	ada	ada	ada	ada	ada	ada
4	www.detik.com	url	ada	ada	ada	ada	ada	ada
5	x.com Username: @radzigkobyala_ Password: KingdomSk411tz	url, akun	ada	ada	ada	ada	ada	ada
6	www.kompas.com	url	ada	ada	ada	ada	ada	ada
7	saritotoasli.com	url	ada	ada	ada	ada	ada	ada
8	www.instagram.com Username: @kingradzig Password: Deliv3r3nC	url, akun	ada	ada	ada	ada	ada	ada
9	www.cnbcindonesia.com	url	ada	ada	ada	ada	ada	ada
	Timeline	waktu dari aktivitas dilakukan	ada	tidak ada	ada	ada	tidak ada	ada

Dari tabel 12 menunjukkan semua jejak digital yang menunjukkan aktivitas *user* di dalam Brave browser berhasil didapatkan di ketiga mode browser. Namun pada mode *private* tidak didapatkan *timeline* dari aktivitas tersebut, karena pada mode *private*, data bersumber dari *file image memory* RAM, dan di dalam *file* tersebut tidak terekam informasi untuk *timeline* dari aktivitas *user*.

Selanjutnya untuk Opera GX semua jejak digital yang menunjukkan aktivitas *user* berhasil didapatkan di ketiga mode browser. Namun pada mode *private* tidak didapatkan *timeline* dari aktivitas tersebut, karena data dari waktu aktivitas tersebut dilakukan tidak terekam di dalam RAM.

4.3.2 Akuisisi II

Tabel 13. Data Hasil Akuisisi II.

Tab	Data	Keterangan	Brave Browser			Opera GX		
			Mode Normal	Mode Private	Mode Secure	Mode Normal	Mode Private	Mode Secure
1	'bookie7', www.globalnewsnusantara.co.id	Keyword, url	ada	ada	ada	ada	ada	ada
2	'judi online', 'mobil', 'motor', 'togel'	keyword	ada	ada	ada	ada	ada	ada
3	mail.google.com, Email: radzigkob@gmail.com Password: KingdomC0me11	url, akun	ada	ada	ada	url dan email ada, password tidak ada	url dan email ada, password tidak ada	url dan email ada, password tidak ada
4	www.detik.com	url	ada	ada	ada	ada	ada	ada
5	x.com Username: @radzigkobyala_ Password: KingdomSk41ltz	url, akun	ada	ada	ada	url dan username ada, password tidak ada	url dan username ada, password tidak ada	url dan username ada, password tidak ada
6	www.kompas.com	url	ada	ada	ada	ada	ada	ada
7	saritotoasli.com	url	ada	ada	ada	ada	ada	ada
8	www.instagram.com Username: @kingradzig Password: Deliv3r3nC	url, akun	ada	ada	ada	url dan username ada, password tidak ada	url dan username ada, password tidak ada	url dan username ada, password tidak ada
9	www.cnbcindonesia.com	url	ada	ada	ada	ada	ada	ada
	Timeline	waktu dari aktivitas dilakukan	tidak ada	tidak ada	tidak ada	ada	tidak ada	ada

Berbeda dengan akuisisi I pada akuisisi II terdapat kegiatan penghapusan data penelusuran internet di dalam browser dan menutup browser. Dari tabel 13 menunjukkan semua jejak digital yang menunjukkan aktivitas *user* di dalam Brave browser berhasil didapatkan di ketiga mode browser dari mulai histori penelusuran internet, email, *username* dan *password*. Namun untuk *timeline* dari aktivitas *user* tidak ditemukan, berbeda dengan akuisisi I pada akuisisi II *file* yang diambil dari folder browser yang tersimpan di penyimpanan lokal yaitu History dan Web Data kosong karena adanya kegiatan penghapusan data penelusuran internet di dalam browser. Sehingga pada akuisisi II data hanya bersumber dari memori RAM, dan *timeline* untuk aktivitas di dalam Brave browser tidak terekam di dalam RAM.

Selanjutnya untuk Opera GX semua jejak digital yang menunjukkan aktivitas *user* seperti histori penelusuran internet, email, dan *username* berhasil ditemukan berhasil didapatkan. Namun untuk *password* tidak ditemukan di ketiga mode browser. Hal ini dipengaruhi oleh kegiatan penutupan browser. Karena hasil akuisisi data setelah dilakukan penghapusan data penelusuran internet dan Opera GX masih dalam keadaan terbuka, *password* masih bisa ditemukan dalam bentuk *plain text* di dalam *image memory* RAM. Tetapi untuk hasil akuisisi data setelah dilakukan penutupan browser Opera GX tanpa melakukan penghapusan data penelusuran internet, data *password* tidak ditemukan dalam bentuk *plain text* di dalam *image memory* RAM, sehingga data *password* tersebut sudah dalam bentuk *digest* dari fungsi *hash*. Sehingga yang menjadi penyebab data *password* tidak ditemukan pada hasil data akuisisi II di ketiga mode browser pada Opera GX adalah adanya kegiatan menutup browser yang dilakukan oleh *user*. Tetapi berbeda dengan Brave browser pada Opera GX untuk mode normal dan *secure*, waktu dari aktivitas *user* berhasil didapatkan.

#### 4. Kesimpulan

Dari pemaparan hasil analisis data akuisisi menunjukkan bahwa metode *live forensics* dinilai efektif untuk penelitian ini. Pada Brave browser untuk tahap akuisisi I pada mode normal dan mode *secure* semua data yang diujikan di dalam simulasi berhasil ditemukan, namun pada mode *private* untuk informasi *timeline* dari aktivitas yang dilakukan *user* tidak ditemukan sehingga dapat disimpulkan mode *private* dapat memengaruhi kelengkapan data forensik yang didapatkan. Lalu pada akuisisi II semua data penelusuran dan akun untuk melakukan *login* berhasil ditemukan, tetapi informasi *timeline* dari aktivitas yang dilakukan *user* tidak ditemukan di ketiga mode browser.

Sedangkan untuk Opera GX pada tahap akuisisi I pada mode normal dan mode *secure* semua data yang diujikan di dalam simulasi berhasil ditemukan, namun pada mode *private* untuk informasi *timeline* dari aktivitas yang dilakukan *user* tidak ditemukan. Lalu untuk tahap akuisisi II semua data aktivitas histori penelusuran internet, email, dan *username* pada ketiga mode browser berhasil ditemukan, namun data *password* tidak ditemukan di ketiga mode browser. Hal ini dipengaruhi oleh kegiatan penutupan browser. Selain itu pada mode normal dan *secure* informasi *timeline* dari aktivitas yang dilakukan *user* berhasil ditemukan, namun pada mode *private* informasi *timeline* tidak ditemukan. Sehingga dapat disimpulkan mode *private* dapat memengaruhi kelengkapan data forensik yang didapatkan. Untuk penelitian selanjutnya diharapkan dapat dilakukan dengan melibatkan browser yang berbeda. Selain itu bisa ditambahkan artefak browser yang diambil seperti, downloads, bookmarks, cache, dan cookies.

#### Daftar Pustaka

- [1] D. Rathod, "Web Browser Forensics: Google Chrome Available Online at [www.ijarcs.info](http://www.ijarcs.info)," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. December, pp. 5–9, 2017, doi: 10.26483/ijarcs.v8i7.4433.
- [2] 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, doi: 10.5120/ijca2017913717.
- [3] M. R. Jadhav and B. B. Meshram, "Web Browser Forensics for Detecting User Activities," *Int. Res. J. Eng. Technol.*, vol. 5, no. 7, 2018.
- [4] A. R. Mahlous and H. Mahlous, "Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 294–306, 2020, doi: 10.22266/ijies2020.1231.26.
- [5] "9 Brave Browser Stats for 2024: Usage, Market Share, Searches." [Online]. Available: <https://taptwicedigital.com/blog/brave-usage>.
- [6] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental analysis of web browser sessions using live forensics method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018, doi: 10.11591/ijece.v8i5.pp.2951-2958.
- [7] R. Harris, "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem," *Digit. Investig.*, vol. 3, no. SUPPL., pp. 44–49, 2006, doi: 10.1016/j.diin.2006.06.005.
- [8] Rabia Mehmood, "Volatile Data Acquisition and Analysis by Using Memory Forensics Techniques," *Int. J. Electron. Crime Investig.*, vol. 7, no. 4, pp. 81–90, 2024, doi: 10.54692/ijeci.2023.0704169.
- [9] H. Nyholm *et al.*, "The Evolution of Volatile Memory Forensics," *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 556–572, 2022, doi: 10.3390/jcp2030028.
- [10] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity," *Digit. Investig.*, vol. 8, no. SUPPL., 2011, doi: 10.1016/j.diin.2011.05.008.
- [11] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.
- [12] Brave, "Brave Shields - Blocking Ads, Trackers & more | Brave." [Online]. Available: <https://brave.com/shields/>.
- [13] R. Saputra and I. Riadi, "Forensic Browser of Twitter based on Web Services," *Int. J. Comput. Appl.*, vol. 175, no. 29, pp. 34–39, 2020, doi: 10.5120/ijca2020920832.
- [14] F.-K. Hasan, K.-M. Sondas, H. Hussin J, and H. Ale J, "Forensic analysis of private browsing mechanisms: Tracing internet activities," *J. Forensic Sci. Res.*, vol. 5, no. 1, pp. 012–019, 2021, doi: 10.29328/journal.jfsr.1001022.

- [15] S. Berham and S. Morris, "a Critical Comparison of Brave Browser and Google Chrome Forensic Artefacts," *J. Digit. Forensics, Secur. Law*, vol. 17, no. March, 2022, doi: 10.15394/jdfsl.2022.1752.
- [16] G. Choi, J. Bang, S. Lee, and J. Park, "Chracer: Memory analysis of Chromium-based browsers," *Forensic Sci. Int. Digit. Investig.*, vol. 46, no. S, p. 301613, 2023, doi: 10.1016/j.fsidi.2023.301613.
- [17] F. Iqbal, Z. Khalid, A. Marrington, B. Shah, and P. C. K. Hung, "Forensic investigation of Google Meet for memory and browser artifacts," *Forensic Sci. Int. Digit. Investig.*, vol. 43, p. 301448, 2022, doi: 10.1016/j.fsidi.2022.301448.