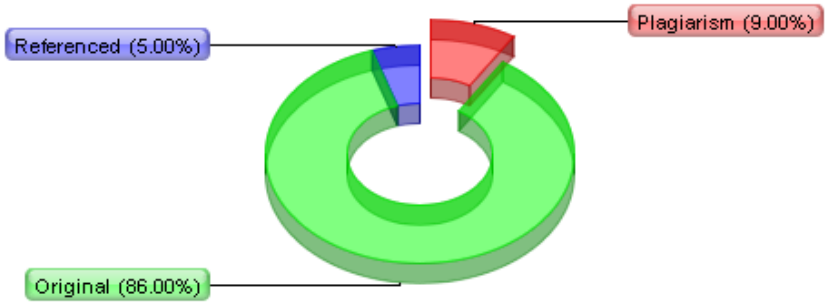
Plagiarism Detector v. 1092 - Originality Report:

Analyzed document: 2/11/2019 1:38:37 PM

"Review Pencarian Bukti Digital dengan Metode Live dan Static Forensics pada Aktivitas Web Browser.doc"

Licensed to: **Heru Priyanto_License14**

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 4	wrds: 161	http://www.academia.edu/36566880/Live_Forensics_Analysis_Method_for_Random_Access_Memory_o...
% 4	wrds: 161	https://www.researchgate.net/publication/251702906_Advanced_evidence_collection_and_analys...
% 4	wrds: 143	https://www.researchgate.net/publication/315513425_Forensic_analysis_and_evidence_collecti...

[Show other Sources:]

Processed resources details:

71 - Ok / 14 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:

[not detected]	[not detected]	[not detected]	[not detected]

Excluded Urls:

https://teknologi.id/tekno/jumlah-perangkat-yang-saling-terhubung-oleh-internet-of-things-...
https://teknologi.id/tekno/jumlah-perangkat-yang-saling-terhubung-oleh-internet-of-things-...
http://jnte.ft.unand.ac.id/index.php/jnte/article/viewFile/120/138
https://journal.uniku.ac.id/index.php/buffer/article/download/597/pdf
https://journal.uniku.ac.id/index.php/buffer/article/download/597/pdf
http://jnte.ft.unand.ac.id/index.php/jnte/article/viewFile/120/138
https://journal.uniku.ac.id/index.php/buffer/article/view/590/451
https://docobook.com/iot-jurnal-umj.html

Included Urls:

Detailed document analysis:

Review Bukti Digital dengan Teknik Live dan Static pada Web Browser Forensics

Muhammad Fajar Sidiq1*), Muhammad Nur Faiz2
1, 2Program Studi Informatika, Fakultas Teknologi Industri dan Informatika, IT Telkom Purwokerto
1,2Jln. D. I. Panjaitan No. 128, Purwokerto 53147, Indonesia
email: 1fajar@ittelkom-pwt.ac.id, 2faiz@ittelkom-pwt.ac.id

Abstract The increasing development of internet usage every year has resulted in the use of web browsers also increasing. This impacts crime

Plagiarism detected: **0.92%** https://www.researchgate.net/public... + 3 more resources! id: **1**

by using a web browser also increasing. This research shows the importance of recognizing the activity of using a web browser in terms of victims and perpetrators. The use of a web browser

will determine the direction of using the web browser. This will help the investigator in analyzing the evidence quickly and can reveal the type of crime that is happening well. Thisresearchprovides a detailed explanation of what can be searched, the location of web browser activity storage, the time format used up to tools to investigation web activity.

Abstrak (Perkembangan penggunaan internet yang semakin banyak setiap tahunnya mengakibatkan penggunaan web browser juga meningkat. Hal ini berdampak kejahatan dengan menggunakan web browser juga meningkat. Penelitian ini menunjukkan pentingnya mengenali aktivitas penggunaan web browser dari sisi korban dan pelaku. Penggunaan web browser akan menentukan arah penggunaan web browser tersebut. Hal ini akan membantu penyidik dalam menganalisis bukti secara cepat dan dapat mengungkap jenis kejahatn yang terjadi secara baik. Penelitian ini memberikan penjelasan secara detail dari apa saja yang dapat dicari, lokasi penyimpanan aktivitas web browser, format waktu yang digunakan sampai dengan tools untuk menginvestigasi aktivitas web.

Kata Kunci (Aktivitas, Web Browser, Bukti Digital, Live Forensics, Static Forensics.

PENDAHULUAN

Perkembangan teknologi yang kompleks dan canggih mengakibatkan tingkat dan variasi tindak kriminal yang semakin canggih juga. Tindak kriminal tersebut tidak hanya dilakukan pada dunia nyata tetapi juga pada dunia maya, Internet merupakan salah satu fasilitas yang digunakan untuk kejahatan pada dunia maya (cybercrime). Menurut data survei tahun 2017 yang dikeluarkan oleh Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII), bahwa 143,26 juta masyarakat Indonesia telah terhubung dengan internet. Jumlah Pengguna media internet di Indonesia terus bertambah setiap tahunnya. Hal ini dapat dilihat pada Gbr. 1 [1].

Gbr.

Plagiarism detected: **0.17%** http://hadirukiyah.blogspot.com/201... id: **2**

1 Pertumbuhan Pengguna Internet di Indonesia.

Cybercrime merupakan istilah kejahatan di dunia maya atau internet. Setiap tahun selalu meningkat baik dari sisi jumlahnya maupun variasi kejahatannya. Internet dahulu hanya untuk mengirimkan email saja, tetapi sekarang internet telah digunakan diberbagai aktivitas pekerjaan dan kehidupan manusia seperti mengirim gambar, video, data dapat dikirimkan dengan mudah dan cepat [2]. Kejahatan di internet muncul karena adanya komunikasi dan hubungan antara satu komputer dengan komputer yang lain melalui suatu jaringan [3]. Berdasarkan data dari Diektorat Tindak Pidana Kejahatan siber (Dit Tipidsiber) Bareskrim Polri Tahun 2017 menangani kasus cybercrime sebanyak 5.061, angka itu naik 3% dibandingkan tahun 2016, yang berjumlah 4.931 kasus [4]. Berdasarkan data tersebut maka untuk membuat jera pelaku dan menanggulanginya diperlukan prosedur penanganan apabila insiden telah terjadi dan mengakibatkan pelanggaran hukum, dimana salah satu prosedurnya adalah digital forensik.
Pada digital forensik ada dua teknik yang digunakan, yaitu live dan static forensic. Static forensic merupakan Teknik dimana mendapatkan data atau bukti digital dari penyimpanan permanen (non-volatile) seperti hardisk, SSD, flashdisk, CD, dan lainnya [5] [6].

Plagiarism detected: **0.7%** https://www.researchgate.net/public... id: **3**

Sedangkan, live forensic membutuhkan data dari sistem yang sedang berjalan atau data volatile yang biasanya terdapat pada Random Access Memory (RAM) atau transit pada jaringan

seperti Internet [7].
Internet muncul sebagai alat penting untuk membantu kegiatan manusia. Web Browser, aplikasi yang digunakan untuk terhubung ke Internet [8]. Mereka umumnya digunakan untuk mencari informasi di World Wide Web. Web browser, aplikasi yang memungkinkan pengguna untuk mencari informasi, melakukan transaksi email, berkomunikasi dengan instant messenger atau jejaring sosial, berbelanja melalui situs web e-commerce [9][10]. Web browser yang umum digunakan, seperti Mozilla Firefox, Google Chrome, Opera dan Apple Safari. Setiap web browser menawarkan fitur dan kehebatanya sendiri. Penggunaan jenis web browser di Asia ditunjukkan pada Gambar 2 [11].

Gbr. 2 Pasar Web Browser Desktop di Asia.

Web browser yang digunakan oleh penggunanya di wilayah Asia periode Desember 2017 - Desember 2018. Pengguna web browser jenis Chrome paling banyak sampai 73,43% dari jumlah pengguna web browser di Asia. Pada posisi berikutnya ada Firefox dengan 8,87%, Internet Explorer (5,95%), Safari, UC Browser dan yang lainnya.
PENELITIAN YANG TERKAIT
Beberapa penelitian yang telah dilakukan diantaranya penelitian dilakukan oleh Varol dan Sonmez bahwa setiap aktivitas pada web adalah data yang dapat mengungkap pikiran dan niat pengguna seperti kata pencarian, kunjungan web, file yang diunduh semua itu merupakan cerminan dari kecenderungan pengguna. Penelitian ini akan menjadi model baru untuk meningkatkan proses forensik komputer yang ada dengan memulai dengan tinjauan literatur. Ketika studi literatur diperiksa maka analisis aktivitas web browser juga harus diperiksa secara rinci. Jika kesuksesan yang diinginkan tercapai dengan model ini, mungkin bidang studi baru seperti mesin pencari data komputer forensik akan dapat diproduksi [12].
Penelitian selanjutnya dilakukan oleh Nalawade, Bharne dan Mane pada tahun 2016, penelitian ini menunjukkan tools yang digunakan oleh penyidik dalam mengungkap kejahatan pada web browser seperti WebHistorian 1.3, Index.dat Analyzer 2.5, ChromeAnalysis plus, NetAnalysis 1.52 dan WEFA. Penelitian ini juga membandingkan dan menjelaskan manfaat serta Batasan dari tools. Ada beberapa tools yang hanya dapat digunakan untuk web browser tertentu, ada yang hanya untuk mengetahui Indexnya dan lainnya [13].
Penelitian lainnya yang terkait dengan aktivitas web browser forensics dilakukan oleh Oh, Lee dan Lee pada tahun 2011. Penelitian ini menghasilkan bahwa melacak bukti penggunaan web browser merupakan proses penting untuk penyelidikan digital forensic. Penyelidikan web browser diperlukan analisis terintegrasi pada berbagai browser secara bersamaan dan menggunakan analisis garis waktu untuk mendeteksi pergerakan online tersangka dari waktu ke waktu. Selain itu, kata-kata pencarian yang digunakan oleh tersangka harus diselidiki karena dapat membantu menyimpulkan karakteristik dan tujuan tersangka. Jika kata kunci penelitian ini disandikan, proses decoding diperlukan. Investigasi berdasarkan aktivitas pengguna juga diperlukan dari sudut pandang forensik digital. Alat WEFA yang diusulkan akan berguna dalam penyelidikan forensik untuk melakukan analisis cepat dan untuk mengevaluasi kegiatan kriminal tersangka secepat mungkin. Pada penelitian ini, web browser yang berjalan pada Windows [14].
Penelitian selanjutnya dilakukan oleh Umar, Yudhana, dan Faiz pada tahun 2018. Penelitian ini menunjukkan beberapa web browser seperti Chrome dan Mozilla Firefox dengan mode private serta mode public. Eksprerimen

pada penelitian ini menguji fitur private dan public dari kedua web browser tersebut. Hasil penelitian ini menunjukkan bahwa dengan fitur private dan public masih terlihat daftar kunjungan web, kata kunci pencarian, username email, username Facebook dengan Teknik Live forensics [9].
Penelitian lainnya dilakukan oleh Akbal, Fatma Güneş, dan Ayhan Akbal pada tahun 2016. Penelitian ini menunjukkan bagaimana seharusnya dilakukan analisis web browser pada sumber daya digital yang dikenai tindak pidana. bagaimana browser web yang paling umum digunakan menyimpan data, informasi apa yang dapat dipulihkan. Cara menganalisis dan bagaimana berbagai sistem operasi menyimpan catatan. Selain itu, memperkenalkan aplikasi yang dapat digunakan oleh para ahli yang melakukan analisis pada web browser [15].
Penelitian terkait lainnya dilakukan oleh Flowers, Mansour dan Al-Khateeb pada tahun 2016. Penelitian ini menjelaskan bagaimana analisis forensik sistem file memulihkan bukti dari IE saat berjalan dalam mode private sedangkan browser lain tampaknya menjaga privasi pengguna yang lebih baik. Penelitian ini juga menganalisis bagaimana memori yang mudah menguap dan mendemonstrasikan bagaimana memori fisik dengan cara membuang file, hibernate, dan file halaman adalah bidang utama di mana bukti dari semua web browser masih dapat dipulihkan terlepas dari mode atau lokasi asalnya [16].

ANALISIS BUKTI DALAM WEB BROWSER

Aktivitas pada Web Browser

Banyak aktivitas dan informasi yang dilakukan menggunakan web browser. Semua aktivitas itu direkam dalam database web browser itu sendiri. Informasi aktivitas ini bisa seperti daftar kunjungan URL, kata kunci pencarian, hal ini dapat dijadikan bukti yang berpotensi untuk mengungkap kejahatan yang terjadi oleh para ahli forensik digital. Selain itu, penggunaan berbagai web browser juga dapat dianalisis untuk mengetahui alur dari pengguna web tersebut. Daftar aktivitas web browser yang dapat digunakan untuk penggalian kejahatan dapat dilihat pada Tabel 1 [14].

Tabel I
AKTIVITAS PENGGUNA PADA WEB BROWSER

Aktivitas Pengguna	Istilah pada URL
Pencarian	Search, Katakunci Google, bing
E-mail	Mail, E-mail
Social Media	Facebook, Twitter, Istagram, etc
Shopping	Bukalapak, Tokopedia, Shopee, etc
Video	Youtube, etc
Banking	Bank, credit, payment, etc
Kunjungan Web	Artikel, blog, wordpress, etc

Lokasi File pada Web Browser

Pada Web Browser lokasi penyimpanan catatan pengguna letkanya berbeda. Karena berbeda sistem operasi juga mempengaruhi lokasi filenya. Dalam hal ini yang dikaji adalah Cache Records, History History, Cookies, Registry, dan File yang Diunduh.

Lokasi yang merupakan browser web

menyimpan data pada sistem operasi Windows 7 ditunjukkan pada Tabel II. Pada proses analisis letak ini sangat penting untuk memeriksa data dalam folder yang berbeda. Folder harus dicari dalam 4 jenis rekaman berbeda [15].

Tabel II
LOKASI FILE PENGGUNAAN WEB BROWSER PADA SISTEM OPERASI WINDOWS 7

Web Browser	File Path Internet

Explorer C:\Users\%username%\AppData\Local
\Microsoft\Windows\Temporary
Internet Files\

C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\ Firefox
C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite Safari
C:\Users\%username%\AppData\Roaming\Apple Computer\Safari\

C:\Users\%username%\AppData\Local\Apple Computer\Safari\ Opera
C:\Users\%username%\AppData\Roaming\Opera\Opera\ Google Chrome
C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\

Preferences

Format Waktu pada Web Browser

Analisis bukti pada web browser juga menghubungkan pergerakan penggunaan web browser sepanjang garis waktu. Dengan melakukan analisis garis waktu, penyidik dapat melacak aktivitas kriminal yang terjadi secara

keseluruhan. Analisis ini memberikan timeline dari satu situs ke situs yang lainnya dan apa saja yang dilakukan pada web tersebut. Selain itu, informasi zona waktu harus dipertimbangkan. Kelima web browser terebut menggunakan waktu UTC. Akibatnya, informasi waktu yang diekstrak dari file log bukan waktu lokal. Untuk alasan ini, penyelidik harus menerapkan koreksi zona waktu ke informasi waktu. Kalau tidak, penyelidik tidak bisa tahu waktu setempat yang tepat dari perilaku Internet tersangka. Misalnya, jika penyelidik mengekstraksi file log untuk tersangka di New York (UTC / GMT setiap 5 jam), penyelidik harus menerapkan koreksi ke zona waktu lokalnya, jika di Indonesia (WIB) menggunakan +7 jam. Hal ini sangat bergantung dengan format waktu dari data yang diperoleh dari bukti harus konsisten dengan pemeriksaan pengguna terhadap format waktunya. Hal ini ditunjukkan pada tabel III [15].

Tabel III
FORMAT WAKTU YANG DIGUNAKAN PADA WEB BROWSER

Web Browser	Format Waktu
Internet Explorer	FILETIME: 100-ns (10-9) Since January 1, 1601 00:00:00 (UTC)
Firefox	PRTime: microsecond(10-6) Since January 1, 1970 00:00:00 (UTC)
Safari	CF Absolute Time: second Since January 1, 2001 00:00:00 (UTC
Opera	UNIX Time: second Since January 1, 1970 00:00:00 (UTC)
Google Chrome	WEBKIT Time: microsecond(10-6) Since January 1, 1601 00:00:00 (UTC

)

TOOLS LIVE & STATIC PADA WEB FORENSICS

Beberapa macam tools untuk membantu penyidik dalam mengungkap kejahatan dengan media web browser seperti FTK Imager, Autopsy, WinHex, Encase, Nirsoft browser pass viewer, MyLastSearch, WebHistorian, NetAnalysis, WEFA, Internet Evidence Finder. Berikut penjelasan masing-masing tools:

FTK Imager

FTK Imager (Forensic Toolkit Imager) merupakan aplikasi digital forensik yang terkenal dengan paket lengkap, aplikasi yang bisa dioperasikan saat penyidik menggunakan teknik live atau static bahkan keduanya, aplikasi ini dapat menangkap citra, menyimpan dan menganalisisnya [17]. FTK Imager ini produk dari Access Data. Gambar 3 menunjukan jendela kerja dari FTK Imager.

Gbr. 3 Tampilan FTK Imager

Autopsy

Autopsy adalah perangkat lunak forensik digital open source yang mendukung tipe sistem file NTFS, FAT, Ext2 / 3/4, HFS / HFS + dan UFS, untuk menyelidiki dari input (file gambar, disk lokal atau file logis). Autopsy memiliki antarmuka pengguna yang mudah untuk dioperasikan dan plugin yang digunakan dalam koleksi Sleuth Kit. Autopsy menggunakan pakar atau ahli untuk membantu penyidik langkah-langkah dalam menyelesaikan suatu kasus. Autopsy lebih sering digunakan penyidik untuk melakukan static forensics karena aplikasi ini hanya membutuhkan citra gambar untuk menganalisisnya. Autopsy menyediakan alur kerja yang intuitif untuk pengguna di Penegakan Hukum, Militer, Agen Intelijen, keamanan Cyber dan komunitas Respon Insiden [18].

Gbr. 4 Tampilan Autopsy

WinHex

WinHex adalah hex editor universal, sangat membantu dalam forensik komputer, pemulihan data, pengeditan data tingkat rendah [19]. Aplikasi ini untuk analisis pada keadaan static forensics.

Fungsi Utama WinHex [20]:

Kloning dan pencitraan disk
Tampilan Hex File.
Perhitungan hash massal untuk file (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, ...)
Mengumpulkan ruang kendur, ruang kosong, ruang antar-partisi, dan teks umum dari drive dan gambar
Pembuatan katalog file dan direktori untuk semua media komputer
Menggabungkan dan memisahkan file, menyatukan dan membagi byte dan kata / bahkan ganjil
Menganalisa dan membandingkan file
Fungsi pencarian dan penggantian yang sangat fleksibel
Mudah deteksi dan akses ke aliran data alternatif NTFS
Kemampuan pencarian fisik dan logis yang kuat dan kuat untuk banyak istilah pencarian secara bersamaan

Gbr. 5 Tampilan WinHex

Encase

Aplikasi digital forensic untuk melakukan pengambilan data, pemulihan file, penguraian file, dan pemulihan format hard disk. Aplikasi ini merupakan aplikasi sistem respons insiden yang diaktifkan jaringan yang menawarkan analisis forensik cepat dan lengkap data volatile dan static pada server dan workstation, tanpa mengganggu operasi. Hal ini digunakan untuk verifikasi data, setelah memverifikasi kemudian memberikan nilai hash. Aplikasi ini bias digunakan pada teknik static dan live forensics. 3 komponen pada Encase [21]:
Kompten pertama pengujian, perangkat lunak ini diinstal pada sistem yang aman untuk dilakukan Investigasi dan audit.
Komponen kedua disebut SAFE, yang merupakan singkatan dari Secure Authentication of EnCase. SAFE adalah server yang digunakan untuk mengautentikasi pengguna, mengelola hak akses, memelihara log transaksi EnCase, dan menyediakan transmisi data yang aman.
Komponen terakhir adalah Servlet, komponen efisien yang diinstal pada workstation jaringan dan server untuk membangun konektivitas antara Penguji, SAFE, dan workstation, server, atau layanan jaringan yang sedang diselidiki.

Gbr. 6 Tampilan Encase

WebBrowserPassView
Aplikasi forensik web browser open source untuk menampilkan semua URL yang dikunjungi, dan penampil riwayat web browser. Itu juga digunakan untuk mengumpulkan kata sandi yang disimpan. Tetapi itu tidak mendukung versi setelah 48.0.2564, karena chrome mengubah algoritma enkripsi untuk menyimpan

kata sandi WebBrowserPassView adalah alat pemulihan kata sandi yang mengungkapkan kata sandi yang disimpan oleh browser Web berikut: Internet Explorer (Versi 4.0 - 11.0), Mozilla Firefox (Semua Versi), Google Chrome, Safari, dan Opera. Alat ini dapat digunakan untuk memulihkan kata sandi Anda yang hilang / terlupakan dari situs web apa pun, termasuk situs web populer, seperti Facebook, Yahoo, Google, dan GMail, selama kata sandi disimpan oleh web browser.

Aplikasi cocok digunakan saat di TKP atau live forensics.

Gbr. 7 Tampilan WebBrowserPassView
MyLastSearch
Aplikasi ini berfungsi untuk memindai file cache dan histori web browser, dan menemukan semua permintaan pencarian dibuat dengan mesin pencari paling populer (Google, Yahoo dan MSN) dan dengan situs jejaring sosial populer (Twitter, Facebook, MySpace). Aplikasi ini umumnya digunakan pada Teknik live forensics. Query pencarian yang dibuat ditampilkan dalam tabel dengan kolom berikut: Teks Pencarian, Mesin Pencari, Waktu Pencarian, Jenis Pencarian (Umum, Video, Gambar), Browser Web, dan URL pencarian [22].

Gbr. 8 Tampilan MyLastSearch

WebHistorian
Web Historian adalah alat yang memungkinkan penyelidik untuk mengumpulkan, menampilkan, dan menganalisis data riwayat web. Ini mendukung windows dan sebagian besar browser [13]. Aplikasi ini umumnya digunakan pada Teknik live forensics.

Gbr. 9 Tampilan WebHistorian

NetAnalysis
NetAnalysis adalah tools yang dikembangkan oleh Digital Detective company untuk pemeriksaan digital web browser.

Aplikasi ini dapat digunakan untuk Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari dan

Opera bowsers. Aplikasi ini bertujuan untuk pemeriksaan riwayat Internet, cache, cookie, dan komponen lainnya. NetAnalysis memiliki fitur pelaporan yang efektif yang memungkinkan pengumpulan bukti dengan cepat sesuai dengan perilaku pengguna. Perangkat lunak ini juga memiliki alat analitis yang efektif untuk memecahkan kode dan memahami data. Pada saat yang sama, NetAnalysis memiliki kemampuan untuk menggunakan query SQL untuk mengidentifikasi bukti terkait. Juga dapat digunakan untuk memulihkan komponen browser web yang dihapus [15].

Gbr. 10 Tampilan NetAnalysis

WEFA

WEFA merupakan aplikasi yang memberikan peningkatan pada titik lemah alat lainnya dan memberikan analisis yang efektif untuk web browser. Alat ini menyediakan fungsi analisis terintegrasi untuk semua lima web browser di berbagai zona waktu, selain itu menyediakan aktivitas pengguna online, kata-kata pencarian, dan parameter URL, semua itu adalah informasi penting untuk digital forensics. Alat ini juga memberikan fungsi decoding, ketika informasi kata pencarian dikodekan dalam karakter yang tidak dikenal atau jika kata-kata pencarian dalam bahasa yang berbeda [13].

Gbr. 11 Tampilan WEFA

IEF (Internet Evidence Finder)

MAGNET IEF digunakan untuk menemukan, menganalisis, dan melaporkan bukti digital dari komputer, smartphone, dan tablet. Internet Evidence Finder (IEF) dapat menemukan dan mengambil setiap dan semua artefak terkait internet yang didukung, menguntungkan penyelidikan dengan mempercepat proses penguraian data. Hal ini memberikan informasi artefak

Plagiarism detected: **0.14%** https://makinrajin.com/pengertian-w... id: **9**

untuk: browser web (Google Chrome

, Mozilla Firefox, Internet Explorer, dll.); program obrolan (AIM, Google Talk, Yahoo Messenger); email (Gmail, Hotmail, Yahoo Mail); dan program torrent (Ares, Frostwire, emule) antara lain. Mencari informasi ini secara manual seringkali terbukti menjadi tugas yang sulit dan menghabiskan waktu. Banyak file artefak diisi dengan apa yang mungkin tampak seperti data yang tidak penting dan tidak mudah dibaca. File-file ini, meskipun mereka mungkin menyimpan data penting, mengandung banyak huruf, simbol, dan kata-kata yang tampaknya acak yang mungkin tidak banyak berarti, kecuali jika orang yang melihatnya tahu apa yang dia lihat, seperti Digital Forensic Examiner. Karena data sulit untuk ditafsirkan, Pemeriksa Forensik Digital harus mengkonfirmasi setiap dan semua hasil dari IEF dengan artefak yang sebenarnya terletak pada bukti [23].

Gbr. 12 Tampilan WEFA

KESIMPULAN

Plagiarism detected: **0.17%** https://rikuji.wordpress.com/2014/0... + 2 more resources! id: **10**

Analisis web browser merupakan salah satu

proses terpenting dalam investigasi digital forensics. Sebagian besar kejahatan dilakukan melalui sistem komputer dilakukan melalui web browser dan banyak kejahatan yang terungkap oleh analisis ini. Pakar digital forensics harus mengetahui bagaimana web browser menyimpan data dalam sistem operasi yang berbeda untuk dapat mengumpulkan bukti dari browser web. Mendapatkan riwayat pencarian tersangka, kata-kata pencarian, URL yang dikunjungi, riwayat unduhan dan data cache sangat penting untuk mengumpulkan bukti. Informasi yang diperoleh dari file pengguna mengungkapkan apakah pelanggaran terjadi atau tidak. Karena itu, para ahli harus menganalisis data web browser dengan benar. Pada penelitian ini ditunjukkan bagaimana browser web yang paling umum digunakan menyimpan data, informasi apa yang dapat dipulihkan atau dianalisis dan apa saja tools yang digunakan dan diperkenalkan oleh para ahli yang melakukan analisis di bidang ini. Dengan demikian, dikemukakan data mana yang akan diperoleh dan dianalisis oleh pakar di bidang ini.

UCAPAN TERIMA KASIH

Penelitian ini didukung oleh LPPM IT Telkom

Plagiarism detected: **0.22%** https://digilib.uns.ac.id/dokumen/d... + 2 more resources! id: **11**

Purwokerto yang telah membantu dan memberikan dukungan terkait

dengan bantuan fasilitas penelitian, dana hibah, dan lainnya.

DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia,

Quotes detected: **0.17%** in quotes: id: **12**

"Penetrasi & Perilaku Pengguna Internet Indonesia,"

Jakarta, 2017.

[2] M. N. Faiz and W. A. Prabowo,

Quotes detected: **0.22%** in quotes: id: **13**

"Comparison of Acquisition Software for Digital Forensics Purposes,"

Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control, vol. 4, no. 1, pp. 37-44, 2019.
[3] M. Danuri and Suharnawi,

Quotes detected: **0.22%** in quotes: id: **14**

"Trend cyber crime dan teknologi informasi di indonesia,"

INFOKAM, vol. 13, no. 2, pp. 55-64, 2017.
[4] Y. Medistiara,

Quotes detected: **0.25%** in quotes: id: **15**

"Selama 2017 Polri Tangani 3.325 Kasus Ujaran Kebencian,"

2017.
[5] M. Nur Faiz, R. Umar, and A. Yudhana,

Quotes detected: **0.25%** in quotes: id: **16**

"Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email,"

J. Inform. Sunan Kalijaga, vol. 1, no. 3, pp. 108-114, 2017.
[6] I. Riadi, R. Umar, and I. M. Nasrulloh,

Quotes detected: **0.39%** in quotes: id: **17**

"Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods,"

LONTAR Komput., vol. 9, no. 3, pp. 169-181, 2018.
[7] M. N. Faiz, W. A. Prabowo, and M. F.

Plagiarism detected: **0.03%** https://www.researchgate.net/public... id: **18**

Sidiq,

Quotes detected: **0.22%** in quotes: id: **19**

"Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal,"

J. Informatics, Inf. Syst. Softw. Eng. Appl., vol. 1, no. 1, pp. 63-70, 2018.
[8] D. Dharan and N.

Plagiarism detected: **0.03%** http://www.academia.edu/36566880/Li... + 2 more resources! id: **20**

Meeran,

Quotes detected: **0.31%** in quotes: id: **21**

"Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser,"

Int. J. Comput. Appl., vol. 91, no. 4, pp. 32-35, 2014.
[9] R. Umar, A. Yudhana, and M. N.

Plagiarism detected: **0.03%** https://www.researchgate.net/public... id: **22**

Faiz,

Quotes detected: **0.28%** in quotes: id: **23**

"Experimental analysis of web browser sessions using live forensics method,"

Int. J. Electr. Comput. Eng., vol. 8, no. 5, pp. 2951-2958, 2018.
[10] N. Shafqat,

Quotes detected: **0.42%** in quotes: id: **24**

"Forensic Investigation of User ' s Web Activity on Google Chrome using various Forensic Tools,"

IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 16, no. 9, pp. 123-132, 2016.
[11] StatCounter Global Stats,

Quotes detected: **0.11%** in quotes: id: **25**

"Browser Market Share Asia,"

2018.
[12] A. Varol and Y. U.

Plagiarism detected: **0.03%** https://www.researchgate.net/public... + 2 more resources! id: **26**

Sonmez,

Quotes detected: **0.22%** in quotes: id: **27**

"The Importance of Web Activities for Computer Forensics,"

in 2017 International Conference on Computer Science and Engineering (UBMK), 2017, no. December, pp. 1-7.
[13] A. Nalawade, S. Bharne, and V.

Plagiarism detected: **0.03%** http://www.academia.edu/36566880/Li... + 4 more resources! id: **28**

Mane,

Quotes detected: **0.25%** in quotes: id: **29**

"Forensic Analysis and Evidence Collection for Web Browser Activity,"

Plagiarism detected: **0.34%** https://www.researchgate.net/public... id: **30**

in 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT

) International Institute of Information Technology (I2IT), Pun, 2016, pp. 518-522.
[14] J. Oh, S. Lee, and S.

Plagiarism detected: **0.03%** http://www.academia.edu/36566880/Li... + 6 more resources! id: **31**

Lee,

Quotes detected: **0.25%** in quotes: id: **32**

"Advanced Evidence Collection and Analysis of Web Browser Activity,"

Digit. Investig., vol. 8, pp. 63-70, 2011.
[15] E. Akbal, G. Fatma, and A. Akbal,

Quotes detected: **0.2%** in quotes: id: **33**

"Digital Forensic Analyses of Web Browser Records,"

J. Softw., vol. 11, no. 7, pp. 631-637, 2016.
[16] C. Flowers, A. Mansour, and H. M. Al-

Plagiarism detected: **0.03%** https://www.researchgate.net/public... + 5 more resources! id: **34**

Khateeb,

Quotes detected: **0.34%** in quotes: id: **35**

"Web Browser Artefacts in Private and Portable Modes : A Forensic Investigation,"

Int. J. Electron. Secur. Digit. Forensics, vol. 8, no. 2, pp. 1-18, 2016.
[17] D. S. Yudhistira, I. Riadi, and Y.

Plagiarism detected: **0.03%** https://www.researchgate.net/public... + 2 more resources! id: **36**

Prayudi,

Quotes detected: **0.31%** in quotes: id: **37**

"Live Forensics Analysis Method For Random Access Memory On Laptop Devices,"

Int. J. Comput. Sci. Inf. Secur., vol. 16, no. 4, pp. 188-192, 2018.
[18] N. Trivedi and D. Patel,

Quotes detected: **0.14%** in quotes: id: **38**

"Digital Evidence Handling Using Autopsy,"

Int. J. Sci. Adv. Res. Technol., vol. 1, no. 1, pp. 10-18, 2015.
[19] S. Fleischmann,

Quotes detected: **0.03%** in quotes: id: **39**

"WinHex,"

2017.
[20] S. K. K and B. Meshram,

Quotes detected: **0.17%** in quotes: id: **40**

"Digital Forensic Investigation using WinHex Tool,"

Int. J. Comput. Sci. Technol., vol. 8491, no. 1, pp. 547-553, 2012.
[21] J. Kaur and G. Singh,
Quotes detected: **0.14%** in quotes: id: **41**
"Comprehensive Study of Digital Forensics,"
Int. J. Adv. Res. Comput. Eng. Technol., vol. 1, no. 5, pp. 180-184, 2012.
[22] B. V Prasanthi,
Quotes detected: **0.17%** in quotes: id: **42**
"Cyber Forensic Tools : A Review,"
Int. J. Eng. Trends Technol., vol. 41, no. 5, pp. 266-271, 2017.
[23] N. Murray,
Quotes detected: **0.11%** in quotes: id: **43**
"Internet Evidence Finder Report,"
Vermont, 2013.

Jurnal Informatika: Jurnal pengembangan IT (JPIT), Vol.xx, No.xx, Bulan 2018 ISSN: 2477-5126
e-ISSN: 2548-9356

*) penulis korespondensi: Muhammad Fajar Sidiq
Email: fajar@ittelkom-pwt.ac.id