JEPIN
(Jurnal Edukasi dan Penelitian Informatika)
ISSN(e): 2548-9364 / ISSN(p) : 2460-0741

Vol. 5
No. 1
April 2019

Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital

Muhammad Fajar Sidiq[#1], Muhammad Nur Faiz[#2]

[#]*Program Studi Informatika, Fakultas Teknologi Industri dan Informatika, IT Telkom Purwokerto*
Jln. D. I. Panjaitan No. 128, Purwokerto 53147, Indonesia

[1]fajar@ittelkom-pwt.ac.id

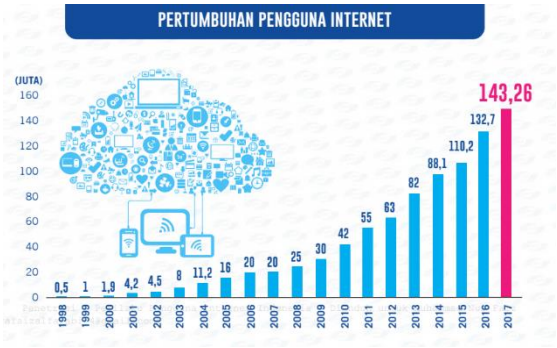
[2]faiz@ittelkom-pwt.ac.id

Abstrak— **Perkembangan penggunaan internet yang semakin banyak setiap tahunnya mengakibatkan penggunaan *web browser* juga meningkat. Hal ini berdampak pada kejahatan dengan menggunakan *web browser* juga meningkat seperti penyalahgunaan email, *hoax, hate speech*, penipuan dan lainnya. Penelitian ini menunjukkan pentingnya mengenali aktivitas penggunaan *web browser* dari sisi korban dan pelaku. Penggunaan *web browser* ini akan menentukan pola atau alur kejahatan pada suatu insiden kejahatan. Hal ini akan membantu penyidik dalam menganalisis bukti digital secara cepat dan dapat mengungkap jenis kejahatan yang terjadi secara baik. Bukti digital yang dianalisis seperti akun, kata kunci pencarian, kunjungan web, dan lainnya. Penelitian ini memberikan penjelasan lokasi penyimpanan bukti digital, format waktu yang digunakan dan 10 *tools* yang digunakan penyidik dalam mengungkap kejahatan dengan media *web browser* seperti Google Chrome, Mozilla Firefox, Internet Explorer, Safari dan Opera.**

Kata kunci*— Bukti, *Web Browser*, Teknik *Forensics

I. 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 Gambar 1 [1].



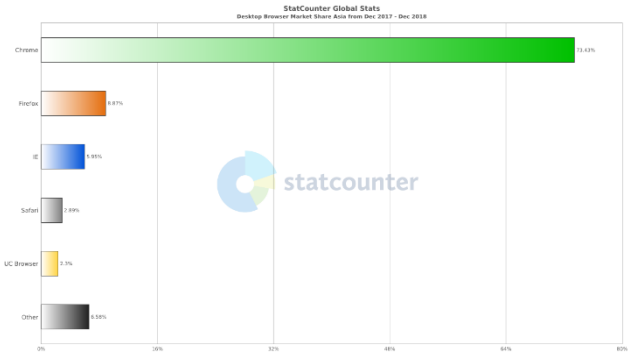
Gambar. 1 Pertumbuhan Pengguna Internet di Indonesia

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 diperlukan suatu prosedur untuk menangani kejahatan pada dunia siber, salah satunya adalah *digital forensics*.

Pada *digital forensics* terdapat dua teknik yang umumnya digunakan, yaitu *live* dan *static*. Teknik *live forensics* membutuhkan data dari sistem yang sedang berjalan atau data *volatile* yang biasanya terdapat pada *Random Access Memory* (RAM) atau transit pada jaringan seperti Internet [5]. Sedangkan teknik *static forensics* merupakan teknik dimana mendapatkan data atau bukti digital dari penyimpanan permanen (non-volatile) seperti hardisk, SSD, flashdisk, CD, dan lainnya [6].

Web browser merupakan aplikasi yang digunakan untuk mencari informasi, melakukan transaksi email, berkomunikasi dengan *instant messenger* atau jejaring

sosial, berbelanja melalui situs *web e-commerce* [7]. *Web browser* yang digunakan umunya : 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 [8].



Gambar. 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 [8].

Penggunaan *web browser* yang terus mengalami peningkatan sehingga dibutuhkan cara menanggulangi atau menyelesaikan suatu kasus yang melibatkan *web browser*. Penelitian ini bertujuan menjelaskan apa saja yang dapat dijadikan bukti digital seperti kata kunci, *username*, kunjungan web, lokasi penyimpanan, format waktu yang digunakan dan juga menjelaskan 10 *tools* yang digunakan penyidik dalam mencari bukti digital pada *web browser* seperti Google Chrome, Mozilla Firefox, Internet Explorer, Safari dan Opera.

II. KAJIAN PUSTAKA

Beberapa penelitian yang telah dilakukan terkait dengan bukti digital pada *web browser forensics* diantaranya penelitian yang 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. Penelitian ini menghasilkan model atau metode baru untuk meningkatkan proses *digital forensics*. Analisis aktivitas *web browser* harus diperiksa secara rinci. Jika metode atau model kesuksesan ini dijalankan maka membutuhkan mesin pencari data untuk komputer *forensics* [9]. Penelitian ini mengusulkan model baru untuk mempercepat proses analisis *forensics* terutama pada aktivitas *web browser* yang banyak lingkupnya, akan tetapi tidak menjelaskan *tools* yang digunakan dan cara mendapatkan bukti digital tersebut.

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. Beberapa tools hanya dapat digunakan pada *web browser* tertentu dengan Teknik tertentu [10]. Penelitian ini membandingkan 5 *tools* yang lebih ke teknik *live forensics*, tidak membahas *tools* untuk teknik *static forensics.*

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* [11]. Penelitian ini hanya membahas teknik *live forensics* tidak membahas *static forensics*.

III. ANALISIS BUKTI DALAM *WEB BROWSER*

A. *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 *digital forensics*. 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 [12].

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

B. *Lokasi File pada Web Browser*

Pada *Web Browser* lokasi penyimpanan catatan pengguna letaknya berbeda. Karena berbeda sistem operasi juga mempengaruhi lokasi filenya. Dalam hal ini yang dikaji adalah *Cache Records, 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 [13].

TABEL III
AKTIVITAS PENGGUNA PADA WEB BROWSER

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

C. *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, penyidik harus menerapkan zona waktu, jika tidak, maka bukti bisa tidak valid. Misal, jika penyidik mengekstraksi file log untuk tersangka di New York (UTC / GMT), penyidik 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 [13].

TABEL IIIII
FORMAT WAKTU YANG DIGUNAKAN PADA WEB BROWSER

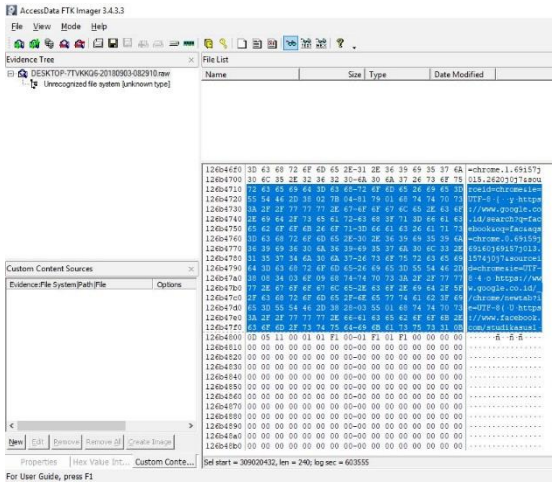
Web Browser	**Format Waktu**
Internet Explorer	FILETIME: 100-ns (10^{-9}) Since January 1, 1601 00:00:00 (UTC)
Firefox	PRTime: microsecond(10^{-6}) Since January 1, 1970 00:00:00 (UTC)
Safari	CF Absolute Time: second Since January 1, 2001 00:00:00 (UTC
Opera	UNIX Time: second Since January 1, 1970 00:00:00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

IV. *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*:

A. *FTK Imager*

FTK Imager (Forensic Toolkit Imager) merupakan aplikasi *digital forensics* 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 [14]. FTK Imager ini produk dari Access Data. Pada Gambar 3 pada kolom biru sebelah kiri menunjukkan bilangan hex pada media penyimpanan sedangkan kolom kanan menjelaskan tentang aktivitas penggunaan *web browser* seperti pengguna menggunakan Google Chrome kemudian mencari pada search engine google dengan kata kunci "Facebook" yang selanjutnya login dengan username studikasus1. Hal ini dapat dijadikan sebagai salah satu bukti digital.

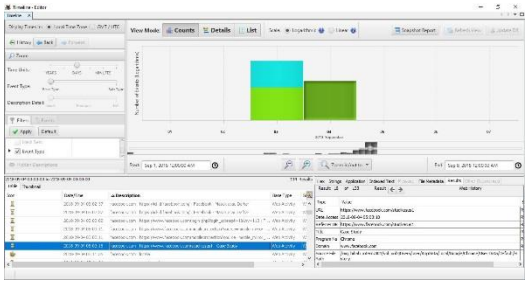


Gambar. 3 Tampilan FTK Imager

B. *Autopsy*

Autopsy adalah perangkat lunak *digital forensics 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 *plug in* yang digunakan dalam koleksi Sleuth Kit. 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 [15]. Pada gambar 4 menunjukkan berapa kali pengguna mengakses suatu halaman web, waktu akses, alamat webnya, *web browser* yang digunakannya.



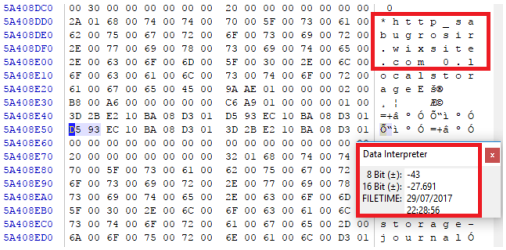
Gambar. 4 Tampilan Autopsy

C. *WinHex*

WinHex adalah hex editor universal, sangat membantu dalam *digital forensics*, pemulihan data, pengeditan data tingkat rendah [16]. Aplikasi ini untuk analisis pada keadaan *static forensics*. Fungsi Utama WinHex [17] :

- Kloning dan pencitraan disk
- Tampilan Hex File.
- Perhitungan hash massal untuk file (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, ...)
- 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

Pada gambar 5 menunjukkan bahwa pengguna pernah mengunjungi alamat web “sabugrosir.wixsite.com” pada tanggal 29 Juli 2017 jam 22:28:56. Hal ini dapat dijadikan sebagai salah satu bukti digital



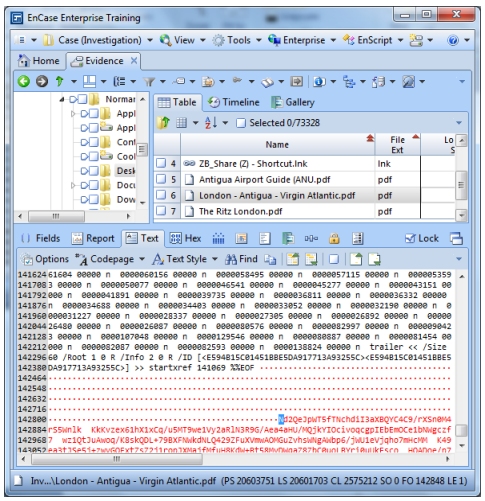
Gambar. 5 Tampilan WinHex.

D. *Encase*

Aplikasi *digital forensic* untuk melakukan pengambilan data, pemulihan file, penguraian file, dan pemulihan format harddisk. Aplikasi ini merupakan aplikasi sistem insiden respons yang diaktifkan jaringan yang menawarkan analisis secara cepat dan lengkap data *volatile* dan static pada server dan workstation, tanpa mengganggu operasi. Hal ini digunakan untuk verifikasi data, kemudian memberikan nilai hash. Aplikasi ini bisa digunakan pada teknik *static* dan *live forensics*. 3 komponen pada Encase [18].

1. Komponen pertama pengujian, perangkat lunak ini diinstal pada sistem yang aman untuk dilakukan Investigasi pengujian dan audit.
2. 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.
3. 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.

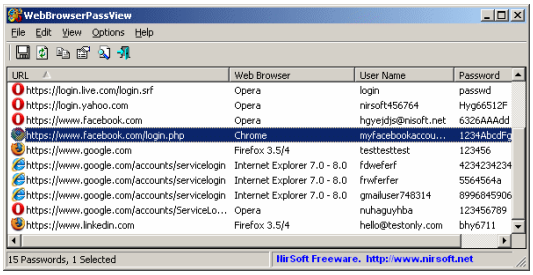
Pada gambar 6 terlihat beberapa file unduhan yang berekstensi pdf, file ini dapat dijadikan salah satu pendukung bukti digital



Gambar. 6 Tampilan EnCase

E. WebBrowserPassView

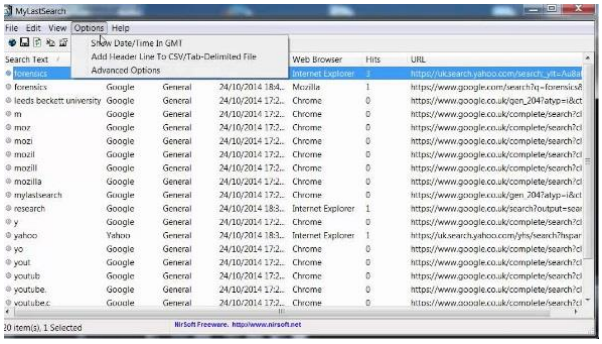
Aplikasi *digital forensics* pada *web browser* untuk menampilkan semua URL yang dikunjungi, dan penampil riwayat *web browser*. Itu juga digunakan untuk mengumpulkan kata sandi yang disimpan. WebBrowserPassView adalah alat pemulihan kata sandi yang mengungkapkan kata sandi yang disimpan oleh browser 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 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 7 [19]. Aplikasi cocok digunakan saat di TKP atau *live forensics*. *username* dan *password* yang digunakan pada beberapa *web browser* dapat terlihat dan ditunjukkan pada gambar.



Gambar. 7 Tampilan WebBrowserPassView

F. MyLastSearch

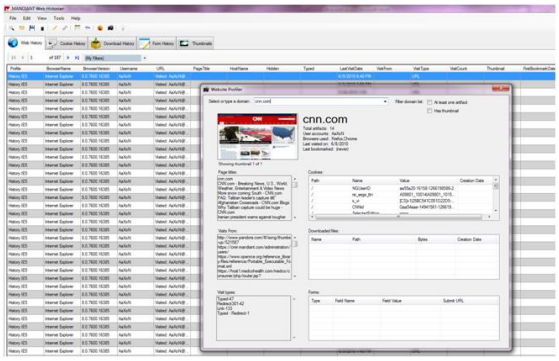
Aplikasi ini berfungsi untuk memindai file *cache* dan histori *web browser*, dan menemukan semua permintaan pencarian dibuat dengan mesin pencari paling populer (Google, Yahoo dan MSN) dan dengan situs jejaring sosial populer (Twitter, Facebook, MySpace). Aplikasi ini umumnya digunakan pada Teknik *live 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 [20]. Pada gambar 8 ditunjukkan bahwa pengguna menggunakan kata kunci pencarian "*forensics*" pada Internet Explorer dengan *search engine* yahoo.com. Hal ini dapat memperkuat bukti dan melengkapi timeline penggunaan *web browser*.



Gambar. 8 Tampilan MyLastSearch

G. WebHistorian

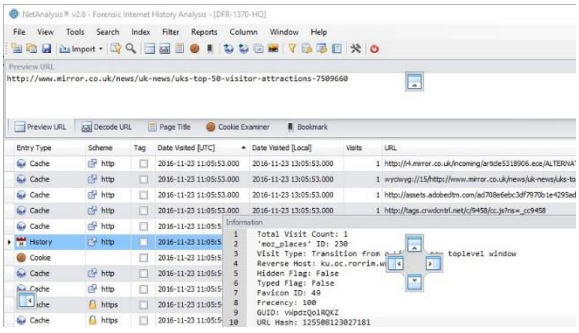
Web Historian adalah aplikasi yang memungkinkan penyidik untuk mengumpulkan, menampilkan, dan menganalisis data kunjungan web [10]. Aplikasi ini umumnya digunakan pada Teknik *live forensics.* Pada gambar 9 terlihat daftar kunjungan web pada waktu tertentu, kemudian dapat melihat profil web yang pernah dikunjunginya. Hal ini dapat memperkuat bukti digital bahwa pengguna telah mengunjungi alamat web dengan profil web cnn.com.



Gambar. 9 Tampilan WebHistorian

H. NetAnalysis

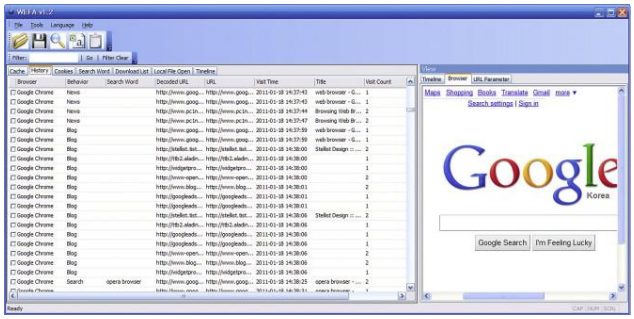
NetAnalysis adalah *tools* yang dikembangkan oleh Digital Detective company untuk pemeriksaan digital *web browser*. Aplikasi ini dapat digunakan untuk Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari dan Opera. Aplikasi ini bertujuan untuk pemeriksaan riwayat Internet, *cache*, *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 *web browser* yang dihapus [13]. Gambar 10 menunjukkan daftar *history* kunjungan web, aplikasi ini dapat melihat *host server*, jumlah kunjungan berapa kali. Daftar *history* serta keterangan lainnya dapat dijadikan bukti digital.



Gambar. 10 Tampilan NetAnalysis

I. *WEFA*

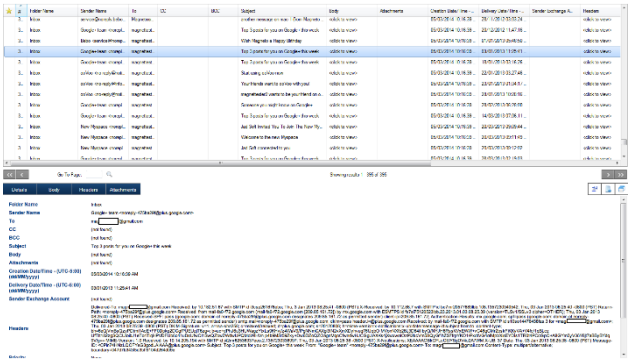
WEFA merupakan aplikasi yang dapat memberikan analisis yang efektif untuk *web browser*. Alat ini menyediakan fungsi analisis terintegrasi untuk semua lima *web browser* di berbagai zona waktu, selain itu menyediakan aktivitas pengguna online, kata-kata pencarian, dan parameter URL, semua itu adalah 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 [10]. Pada gambar 11 aplikasi WEFA ini dapat melihat *history* dari berbagai jenis *web browser*, kata kunci, alamat URL-nya, waktunya dan berapa kali mengunjungi web tersebut. Hal ini dapat memperkuat bukti digital untuk jejak atau aktivitas pengguna pada *web browser*.



Gambar. 11 Tampilan WEFA

J. *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, hal ini sangat membantu proses investigasi karena dapat mempercepat proses penguraian data. Artefak internet yang dapat diurai seperti pada *web browser* (Google Chrome, Mozilla Firefox, Internet Explorer), *Chatting* (AIM, Google Talk, Yahoo Messenger), E-mail (Gmail, Hotmail, Yahoo Mail). Banyak file artefak yang masih susah untuk diartikan atau belum mempunyai makna. Namun, berbeda jika yang melihat adalah penyidik, karakter atau kata-kata yang acak dan tidak beraturan tersebut mempunyai arti tersendiri dan harus dapat ditafsirkan [21]. Gambar 12 menunjukkan aplikasi IEF saat menganalisis email secara lengkap dari pengirimnya, subject, isi, lampiran, waktu pesan dibuat, waktu pesan terkirim. Email merupakan salah satu bukti digital yang cukup banyak digunakan sebagai bukti utama.



Gambar. 12 Tampilan IEF

V. KESIMPULAN

Web browser forensics merupakan salah satu proses terpenting dalam investigasi *digital forensics*. Sebagian besar kejahatan yang dilakukan dengan internet membutuhkan media *web browser* untuk mengaksesnya. Penyidik harus mengetahui dimana *web browser* menyimpan data, menyimpan riwayat kata-kata pencarian, URL yang pernah dikunjungi, riwayat unduhan dan lainnya. Informasi ini dapat dijadikan sebagai bukti digital yang bisa mengungkapkan apakah terjadi pelanggaran atau tidak. Karena itu, para penyidik harus menganalisis data *web browser* dengan rinci dan teliti. Penelitian ini menjelaskan apa saja bukti digital yang dapat dicari, lokasi penyimpanan aktivitas penggunaan kelima *web browser*, dan 10 *tools* yang digunakan untuk mencari bukti digital beserta penjelasannya.

UCAPAN TERIMA KASIH / ACKNOWLEDGMENT

Penelitian ini didukung oleh LPPM IT Telkom Purwokerto yang telah membantu dan memberikan dukungan terkait dengan bantuan fasilitas penelitian, dana hibah, dan lainnya.

REFERENSI

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, “Penetrasi & Perilaku Pengguna Internet Indonesia,” Jakarta, 2017.

[2] M. N. Faiz and W. A. Prabowo, “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, “Trend cyber crime dan teknologi informasi di indonesia,” *INFOKAM*, vol. 13, no. 2, pp. 55–64, 2017.

[4] Y. Medistiara, “Selama 2017 Polri Tangani 3.325 Kasus Ujaran Kebencian,” 2017.

[5] M. N. Faiz, W. A. Prabowo, and M. F. Sidiq, “Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal,” *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, pp. 63–70, 2018.

[6] I. Riadi, R. Umar, and I. M. Nasrulloh, “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] N. Shafqat, “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.

[8] StatCounter Global Stats, “Browser Market Share Asia,” 2018.

[9] A. Varol and Y. U. Sonmez, "The Importance of Web Activities for Computer Forensics," in *2017 International Conference on Computer Science and Engineering (UBMK)*, 2017, no. December, pp. 1–7.

[10] A. Nalawade, S. Bharne, and V. Mane, "Forensic Analysis and Evidence Collection for Web Browser Activity," in *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (I²IT), Pun*, 2016, pp. 518–522.

[11] 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, 2018.

[12] J. Oh, S. Lee, and S. Lee, "Advanced Evidence Collection and Analysis of Web Browser Activity," *Digit. Investig.*, vol. 8, pp. 63–70, 2011.

[13] E. Akbal, G. Fatma, and A. Akbal, "Digital Forensic Analyses of Web Browser Records," *J. Softw.*, vol. 11, no. 7, pp. 631–637, 2016.

[14] D. S. Yudhistira, I. Riadi, and Y. Prayudi, "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.

[15] N. Trivedi and D. Patel, "Digital Evidence Handling Using Autopsy," *Int. J. Sci. Adv. Res. Technol.*, vol. 1, no. 1, pp. 10–18, 2015.

[16] S. Fleischmann, "WinHex," 2017.

[17] S. K. K and B. Meshram, "Digital Forensic Investigation using WinHex Tool," *Int. J. Comput. Sci. Technol.*, vol. 8491, no. 1, pp. 547–553, 2012.

[18] J. Kaur and G. Singh, "Comprehensive Study of Digital Forensics," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 1, no. 5, pp. 180–184, 2012.

[19] T. Y. Yang, A. Deghantanha, K.-K. raymond Choo, M. Conti, and T. Dargahi, "Forensic Investigation of Cooperative Storage Cloud Service : Symform as a Case Study," *J. Forensic Sci.*, vol. 62, no. 3, pp. 641–654, 2017.

[20] B. V Prasanthi, "Cyber Forensic Tools : A Review," *Int. J. Eng. Trends Technol.*, vol. 41, no. 5, pp. 266–271, 2017.

[21] N. Murray, "Internet Evidence Finder Report," Vermont, 2013.