CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 4, No. 1, Mei 2021, hlm. 24-32

ANALISIS *LIVE FORENSIC* PADA *WHATSAPP* WEB UNTUK PEMBUKTIAN KASUS PENIPUAN TRANSAKSI ELEKTRONIK

Syaza Dyah Utami[1], Carudin[2], Azhari Ali Ridha[3]

[123]Program Studi Teknik Informatika Universitas Singaperbangsa Karawang
Email: [1]syaza.dyah17015@student.unsika.ac.id, [2]carudin@staff.unsika.ac.id, [3]azhari.ali@unsika.ac.id

(Naskah masuk: 13 April 2021, diterima untuk diterbitkan: 31 Mei 2021)

Abstrak

Internet tidak hanya memberikan manfaat bagi masyarakat, namun juga dapat menimbulkan dampak negatif. Salah satunya yaitu kejahatan dunia maya. Sosial media yang sering digunakan oleh masyarakat dapat disalahgunakan untuk dijadikan sebagai media kejahatan. Salah satunya melalui sosial media yang popular di Indonesia, yaitu *Whatsapp.* Kasus penipuan melalui aplikasi *Whatsapp* sering terjadi di Indonesia, sehingga memerlukan penanganan lebih lanjut agar kasus kejahatan tersebut dapat diselesaikan dan pelaku dapat mempertanggungjawabkan perbuatannya. *Live forensic* sebagai cabang ilmu *Digital Forensic* dapat digunakan untuk mencari bukti digital terkait kasus penipuan dari perangkat bukti yang masih dalam kondisi menyala (*on*). Tujuan penelitian ini adalah untuk membuktikan kasus penipuan transaksi elektronik pada *Whatsapp* web dengan menggunakan metode *Live forensic*. Metodologi NIST (*National Institute of Standards and Technology*) dengan tahapan koleksi, pemeriksaan, analisis, dan reporting digunakan pada penelitian ini. Pencarian bukti digital dilakukan pada laptop pelaku, sedangkan *smartphone* korban dijadikan sebagai pembanding. Bukti digital yang dianalisis berupa teks percakapan, gambar, dan video. *Live forensic* dilakukan dengan RAM *imaging* serta akuisisi *log file*, *cache*, dan riwayat *browser* dengan menggunakan FTK *Imager* dan *Browser History Viewer*. Hasil penelitian yaitu teks percakapan, *filename* gambar, *filename* video, *timestamp*, *history*, nomor rekening pelaku, dan nomor *handphone* korban yang merupakan bukti digital untuk pembuktian kasus. Bukti digital dari proses *Live Forensic* merupakan bukti yang sah berdasarkan UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Kata kunci: *digital forensik, live forensik, penipuan, whatsapp web*

LIVE FORENSIC ANALYSIS ON WHATSAPP WEB TO PROVE CASE OF ELECTRONIC TRANSACTION FRAUD

Abstract

Internet not only provides benefits to society, but also have negative impacts. One of them is cybercrime. Social media that often used by the public can be misused to serve as a crime's medium. One of them is social media which is popular in Indonesia, namely Whatsapp. Fraud cases through Whatsapp often occur in Indonesia, so that requires further handling so that crime cases can be resolved and the perpetrators can be held accountable for their actions. Live forensic as a branch of Digital Forensic can be used to search digital evidence related to fraud cases from evidence devices that are still on. The purpose of this research is to prove cases of electronic transaction fraud on Whatsapp web using Live forensic. NIST (National Institute of Standards and Technology) methodology with stages of collection, examination, analysis and reporting was used in this research. The search for digital evidence was carried out on the perpetrator's laptop, while the victim's smartphone was used as comparison. Digital evidence that was analyzed was in the form of conversational text, pictures, and videos. Live forensics is performed with RAM imaging and acquisition of log files, cache, and browser history using the FTK Imager and Browser History Viewer. The results of research are conversational text, image filename, video filename, timestamp, history, perpetrator's account number, and victim's cellphone number which are digital evidence to prove the case. Digital evidence from Live Forensic is legal evidence based on Law Number 11 of 2008 concerning Electronic Information and Transactions.

Keywords: *digital forensic, live forensic, fraud, whatsapp web*

1. PENDAHULUAN

Penipuan merupakan bentuk kejahatan yang dilakukan dengan berbagai kebohongan atau tipu muslihat dengan tujuan untuk menguntungkan diri sendiri sebagaimana dijelaskan pada pasal 378 KUHP (Wirasila, Darmadi dan Purwani, 2017). Salah satu jenis penipuan yaitu penipuan transaksi elektronik yang merupakan penipuan yang memanfaatkan internet untuk melakukan modus penjualannya secara *online* (Mulyadi, 2017). Tahun 1970-an menjadi tahun pertama kali terjadinya kasus penipuan transaksi elektronik yang berkaitan dengan penipuan keuangan (Sudyana, 2016). Kasus tersebut terus terjadi dan semakin meningkat disebabkan oleh kemajuan teknologi internet di Indonesia berdasarkan data berikut ini. Survei *We Are Social* pada Januari 2021 yang dikutip dari situs Data Reportal menyatakan bahwa pengguna internet di Indonesia yaitu sebanyak 202,6 juta jiwa atau setara dengan 73,7% dari total penduduk Indonesia. Data tersebut mengalami peningkatan sebanyak 27 juta jiwa atau 15,5% dibandingkan tahun 2020 (Kemp, 2021).

Berdasarkan survei *We Are Social* pada tahun 2021 yang dikutip dari situs Data Reportal juga menyatakan bahwa pengguna aktif sosial media di Indonesia yaitu sebanyak 170 juta jiwa atau setara dengan 61,8% dari total penduduk Indonesia. Data ini pun mengalami peningkatan sebanyak 10 juta jiwa atau 6,3% dibandingkan dengan tahun 2020. Salah satu sosial media yang populer digunakan di Indonesia yaitu aplikasi *Whatsapp*. Survei *We Are Social* pada Januari 2021 menyatakan bahwa Whatsapp berada di posisi kedua pada urutan sosial media yang paling banyak digunakan di Indonesia yaitu sebanyak 87.7% dari total pengguna internet. Survei tersebut pun dilakukan pada aktivitas yang dilakukan oleh pengguna internet, yaitu aktivitas *e-commerce*. Tercatat pada survei tersebut bahwa salah satu aktivitas *e-commerce* yang dilakukan oleh pengguna internet di Indonesia yaitu 79.1% pengguna internet membeli produk *online* melalui perangkat *mobile* dan sebanyak 87.1% pengguna internet menggunakan berbagai perangkat lain (Kemp, 2021).

Tingginya aktivitas pengguna internet dalam kegiatan *e-commerce* menyebabkan angka kejahatan penipuan meningkat sebagaimana data yang dipublikasikan oleh Direktorat Tindak Pidana Siber Bareskrim Polri pada situs resminya, Patroli Siber. Total laporan kejahatan yang dilaporkan oleh masyarakat melalui situs Patroli Siber selama tahun 2021 (Januari s.d. Desember) yaitu sebanyak 12.197 laporan. Berdasarkan laporan tersebut, kejahatan yang paling banyak dilaporkan oleh masyarakat yaitu penipuan/fraud dengan jumlah 7.124 laporan. Adapun *platform* yang dilaporkan sebagai platform yang paling banyak digunakan untuk melakukan tindak kejahatan adalah Whatsapp dengan jumlah 4.888 laporan. Data laporan kejahatan pada Patroli Siber selama 2021 (Januari s.d. Maret) pun menyatakan bahwa penipuan/fraud merupakan kejahatan yang paling banyak dilaporkan dengan jumlah 2.145 dari total 4.453 laporan. Platform yang paling banyak dilaporkan oleh masyakarat sebagai platform kejahatan pun sama dengan tahun sebelumnya, yaitu Whatsapp dengan jumlah 2.062 laporan (Mabes Polri, 2021).

Tingginya angka kejahatan penipuan dan platform Whatsapp sebagai media kejahatan sebanding dengan tingkat pengguna internet, aktivitas media sosial, serta Whatsapp sebagai media sosial populer di Indonesia. Berdasarkan permasalahan tersebut, maka diperlukan penanganan untuk menindaklanjuti kejahatan yang dilakukan oleh pelaku. Digital forensik merupakan salah satu ilmu forensik yang memanfaatkan metode ilmiah untuk memperoleh bukti digital yang dapat digunakan untuk kepentingan di pengadilan (Sudyana, 2016). Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 5 Ayat 1 dijelaskan bahwa bukti digital berupa informasi atau dokumen elektronik dapat termasuk alat bukti hukum yang sah (Al-Azhar, 2012). Salah satu metode yang dapat digunakan untuk membantu proses penyelidikan yaitu metode *live forensic*, yang dapat digunakan untuk pencarian bukti digital ketika perangkat sedang dalam keadaan menyala. *Live forensic* dapat digunakan untuk mencari bukti digital dari data *Random Access Memory* (Riadi, Sunardi dan Rauli, 2018).

Terdapat beberapa penelitian mengenai *live forensic* yang telah dilakukan sebelumnya. Penelitian (Riadi, Sunardi dan Rauli, 2018) menggunakan metode *live forensic* untuk mencari bukti digital yang berkaitan dengan kasus penipuan *online* pada Whatsapp versi desktop. *Tools* yang digunakan pada penelitian tersebut yaitu FTK Imager untuk mencari bukti digital pada data RAM. Hasil penelitian tersebut berupa bukti digital teks percakapan dan *filename* gambar yang digunakan untuk pembuktian kasus penipuan *online*. Adapun penelitian (Zuhriyanto, Yudhana dan Riadi, 2018) menerapkan metode *live forensic* untuk mencari bukti digital pada aplikasi Twitter yang digunakan untuk mendukung penanganan kejahatan. Penelitian tersebut menggunakan tahapan penelitian NIJ (*National Institute of Justice*) yang terdiri dari lima tahapan. Analisis bukti digital dilakukan pada *log file* dan *cache* dengan menggunakan *tools* FTK Imager. Hasil yang diperoleh pada penelitian tersebut yaitu bukti digital berupa ID user dan *file* gambar. Selain itu, penelitian (Umar, Riadi dan Muthohirin, 2019) menerapkan metode *live forensic* untuk memperoleh bukti digital dari email yang berkaitan dengan penipuan pada email. *Tools* yang digunakan pada penelitian tersebut yaitu Wireshark dan Networkminer, sedangkan tahapan penelitian menggunakan metodologi NIST (*National Institute of Standards and Technology*) yang terdiri dari empat tahap. Hasil penelitian tersebut berhasil memperoleh bukti digital berupa *timestamp* pengiriman email,

timestamp penerimaan email, port protokol pengirim, port protokol penerima, serta alamai IP asal dan tujuan.

Berdasarkan penelitian-penelitian yang telah dilakukan, dapat diketahui bahwa metode *live forensic* dapat digunakan dalam pencarian bukti digital untuk mendukung penanganan kasus kejahatan. Penelitian ini bertujuan menerapkan metode *live forensic* untuk mencari bukti digital pada Whatsapp web, membuktikan kasus penipuan transaksi elektronik dengan bukti digital yang telah diperoleh, serta mengevaluasi hasil bukti digital yang diperoleh. *Live forensic* dilakukan dengan RAM *imaging* serta analisis *log file, cache,* dan *history browser* menggunakan *tools* FTK Imager dan Browser History Viewer. Metode tersebut digunakan berdasarkan referensi dari penelitian sebelumnya. Tahapan penelitian ini mengikuti *framework* investigasi forensik NIST yang berdasarkan penelitian (Syahib, Riadi dan Umar, 2018), tahapan NIST terdiri dari tahap *collection*, *examination, analysis,* dan *reporting*.

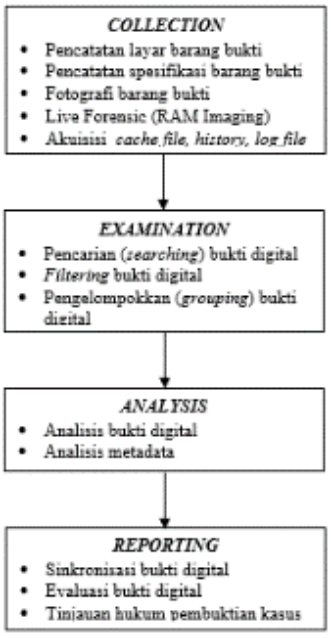
2. METODE PENELITIAN

Penelitian ini menerapkan metode studi literatur untuk mencari data sekunder yang berupa teori dan penelitian sebelumnya yang berkaitan. Data primer pada penelitian ini yaitu data digital yang diperoleh dengan melakukan simulasi dari skenario kasus penipuan transaksi elektronik yang kemudian data tersebut dicari menggunakan metode *live forensic*.

2.1. Metodologi Penelitian

Penelitian ini menerapkan matodologi atau *framework* investigasi *digital forensic* NIST (*National Institute of Standards and Technology*). Alur atau tahapan penelitian berdasarkan metodologi NIST ditunjukkan pada Gambar 1 berikut ini.

.



Gambar 1. Alur penelitian

1. *Collection*

Tahap *collection* atau pengumpulan yaitu tahap yang terdiri dari persiapan, pengumpulan, dokumentasi, dan isolasi barang bukti (Nasirudin, Sunardi dan Riadi, 2020). Hal yang dilakukan pada penelitian ini di antaranya mencatat layar dan spesifikasi barang bukti, mendokumentasikan (memotret) barang bukti, serta melakukan proses *live forensic* (RAM *imaging*, akuisisi *cache file*, *history*, dan *log file*). Pencatatan layar barang bukti dilakukan pada laptop pelaku untuk mengetahui waktu dan program yang sedang berjalan ketika perangkat bukti tersebut ditemukan. Pencatatan spesifikasi barang bukti dilakukan pada semua barang bukti yang terlibat, yaitu laptop pelaku dan *smartphone* korban. Akuisisi data digital dilakukan dengan metode *live forensic*. RAM *imaging* dilakukan menggunakan *tools* FTK Imager, sedangkan *tools* Browser History Viewer digunakan untuk mengakuisisi *cache file*, *history*, dan *log file*.

2. *Examination*

Tahap *examination* tahap pemeriksaan dilakukan setelah data digital diperoleh (Faiz, Prabowo dan Sidiq, 2018). Kemudian pada penelitian ini masing-masing data digital akan dimasukkan ke dalam *tools forensic*. *Tools* tersebut akan mencari (*searching*), mem-*filter*, dan mengelompokkan (*grouping*) setiap data.

3. *Analysis*

Tahap analisis yaitu analisis bukti digital yang telah diperiksa untuk mendapatkan informasi yang berkaitan dengan kasus (Syahib, Riadi dan Umar, 2018). Bukti digital pada penelitian ini dianalisis dengan menggunakan *tools* FTK Imager dan Browser History Viewer. Bukti digital dianalisis bukan hanya untuk mengetahui isi percakapan antara korban dan pelaku, tetapi juga untuk mengetahui metadata serta *timestamp* (keterangan waktu) waktu kejadian.

4. *Reporting*

Uraian hasil analisis bukti digital dan kasus kejahatan yang telah diperoleh kemudian dilaporkan pada tahap *reporting* (Syahib, Riadi dan Umar, 2018). Tahap *reporting* pada penelitian ini meliputi sinkronisasi bukti digital, evaluasi bukti digital, dan tinjauan hukum. Sinkronisasi bukti digital dilakukan dengan membandingkan bukti digital yang diperoleh dari laptop pelaku dengan percakapan pada aplikasi Whatsapp pada smartphone korban. Evaluasi bukti digital dilakukan untuk mengetahui bukti digital apa saja yang diperoleh dan kemampuan dari setiap *tools* yang digunakan. Tinjauan hukum yaitu berupa aturan hukum yang berkaitan dengan kasus penipuan transaksi elektronik.

2.2. Alat dan Bahan

Alat dan bahan yang digunakan pada penelitian ini yaitu berupa *software* atau *tools forensic* serta *hardware* yang merupakan barang bukti milik pelaku dan korban. Berikut ini adalah spesifikasi dari setiap alat dan bahan yang digunakan.

Tabel 1. Alat dan bahan penelitian

No.	Kategori	Spesifikasi
1	*Hardware*	Laptop ASUS VivoBook X409DAP M409DA
2	*Software*	*Smartphone Android* Vivo Y91C
3		Sistem Operasi Windows 10 *Home Single Language* 64-*bit*
4		FTK Imager versi 4.3.1.1
5		Browser History Viewer versi 1.3.2

Barang bukti laptop pelaku digunakan untuk mencari bukti digital yang berkaitan dengan kasus penipuan transaksi elektronik yang terjadi. Barang bukti *smartphone* milik korban hanya dijadikan sebagai pebanding antara bukti digital yang telah diperoleh dari laptop pelaku dengan percakapan Whatsapp pada *smartphone* korban.

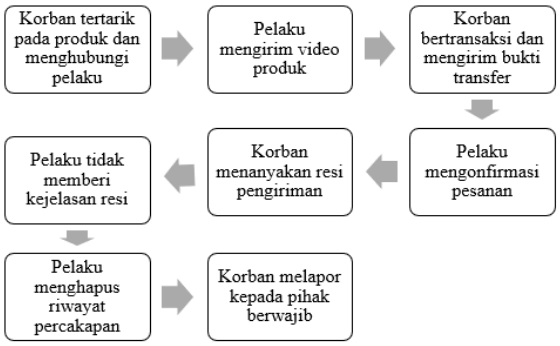
2.3. Simulasi Kasus

Simulasi kasus penipuan transaksi elektronik melalui percakapan Whatsapp dilakukan karena didasari pada aturan berikut ini.

1. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 5 huruf a.
2. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 6 huruf a.
3. Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 7 ayat 1.

Aturan tersebut menyatakan bahwa terdapat kriteria informasi publik yang salah satunya yaitu informasi yang dikecualikan untuk dipublikasikan. Informasi yang dimaksud ialah informasi yang menghambat proses penyelidikan dan penyidikan suatu tindak pidana seperti identitas saksi atau tersangka, barang bukti yang berkaitan, isi berkas perkara, dan modus operandi pada kasus tersebut.

Simulasi pada penelitian ini dilakukan antara korban dan pelaku. Korban menggunakan aplikasi Whatsapp pada *smartphone* miliknya, sedangkan pelaku menggunakan aplikasi Whatapp web pada laptop miliknya yang dijalankan melalui *browser* Google Chrome mode normal. Berikut ini merupakan gambaran simulasi kasus penipuan transaksi elektronik.



Gambar 2. Simulasi kasus penipuan transaksi elektronik

3. HASIL DAN PEMBAHASAN

Hasil penelitian yang telah dilakukan yaitu meliputi penggalian, pembuktian, dan pengevaluasian bukti digital pada kasus penipuan transaksi elektronik dengan metode *live forensic*. Skenario kasus penipuan transaksi elektronik melalui percakapan Whatsapp web antara pelaku dan korban dilakukan pada 31 Januari 2021 dan 1 Februari 2021. Urutan hasil penelitian mengikuti tahapan *framework digital forensic* NIST yang digunakan.

3.1. Collection

Tahap *collection* menghasilkan beberapa catatan dan dokumentasi barang bukti yang terlibat dalam kasus penipuan transaksi elektronik. Catatan yang pertama yaitu mengenai spesifikasi perangkat bukti (laptop pelaku dan *smartphone* korban) yang ditunjukkan pada Tabel 2 berikut ini.

Tabel 2. Spesifikasi perangkat bukti

Jenis	Spesifikasi
Laptop	- LAPTOP-0CT76EIL ASUS - Processor AMD Athlon Silver 3050U - Operation System Windows 10 Home Single Language 64-bit - RAM 4GB
Smartphone	- Vivo Y91C - Android 8.1.0 - Processor 2.0 GHz Octa-core - RAM 2GB

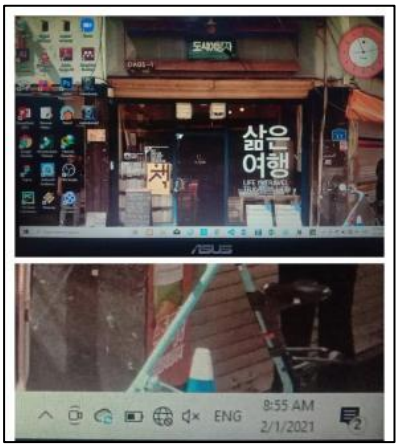
Seluruh perangkat bukti yang terlibat pada penelitian harus dicatat dan didokumentasikan, meskipun pada penelitian ini *smartphone* korban hanya dijadikan sebagai pembanding dan tidak dianalisis lebih lanjut.

Pencatatan selanjutnya dilakukan pada layar barang bukti laptop pelaku yang meliputi *program* yang sedang berjalan dan keterangan waktu pada layar. Hasil pencatatan layar barang bukti ditunjukkan pada Tabel 3 di bawah ini.

Tabel 3. Catatan layar perangkat bukti

No.	Program Running	Timestamp
1	File Explorer	01 Februari 2021
2	Google Chrome	08:55 AM

Pendokumentasian barang bukti yang pertama dilakukan dengan memotret layar barang bukti laptop pelaku seperti pada Gambar 3 berikut.



Gambar 3. Dokumentasi layar barang bukti

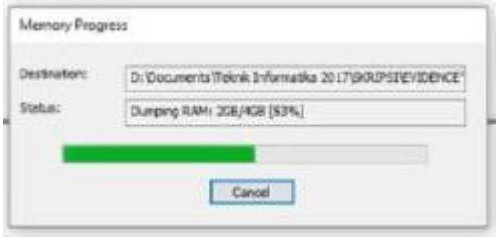
Pemotretan layar seperti pada gambar di atas dilakukan secara keseluruhan dan pada bagian yang menunjukkan keterangan waktu. Selain itu, Gambar 4 di bawah ini merupakan hasil pemotretan perangkat bukti, yaitu laptop milik pelaku.

Gambar 4. Dokumentasi perangkat bukti laptop pelaku

Pemotretan perangkat bukti juga dilakukan pada *smartphone* milik korban yang ditunjukkan pada Gambar 5 di bawah ini.

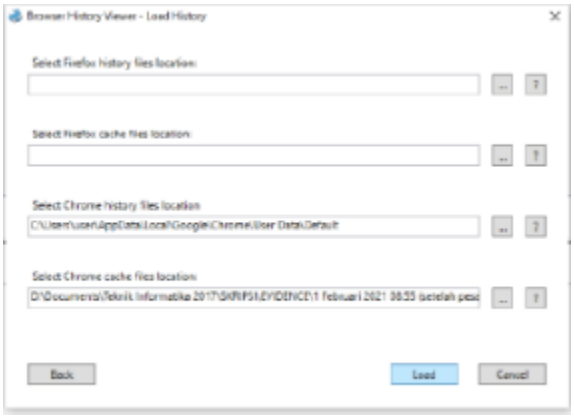
Gambar 5. Dokumentasi perangkat bukti *smartphone* korban

Setelah pencatatan dan dokumentasi barang bukti, selanjutnya dilakukan proses *live forensic* pengumpulan bukti digital. Proses RAM *imaging* untuk mendapatkan bukti digital RAM *image* dilakukan menggunakan *tools* FTK Imager seperti Gambar 6 berikut.



Gambar 6. Proses RAM *imaging*

Bukti digital *log file* diperoleh dari folder C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb. Bukti digital *cache* diperoleh dari folder C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache. Bukti digital *history* diperoleh dari folder *Default* Google Chrome. *Cache* dan *history browser* dikumpulkan menggunakan *tools* Browser History Viewer yang ditunjukkan pada Gambar 7 berikut.



Gambar 7. Proses pengumpulan bukti digital *cache* dan *history*

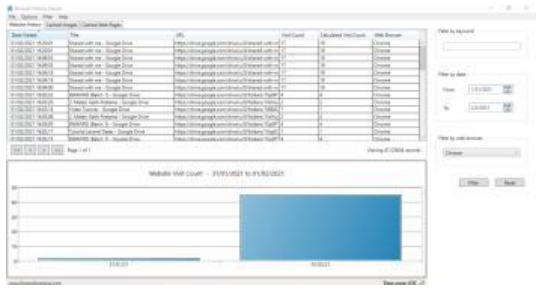
3.2. Examination

Hasil dari tahap *examination* (pemeriksaan) yaitu berupa bukti digital yang telah dicari, dikelompokkan, dan di-*filter*. Gambar 8 di bawah ini menunjukkan proses pengelompokkan RAM *image* menggunakan FTK Imager.

Gambar 8. Pengelompokkan bukti digital RAM Image

Berdasarkan gambar di atas, RAM *image* pada FTK Imager dikelompokkan berdasarkan tipe barang bukti (*evidence type*), yaitu *Forensic Disk Image.* Bukti digital *log file* juga dikelompokkan menggunakan FTK Imager dan termasuk ke dalam tipe barang bukti *Contents of Folder.*

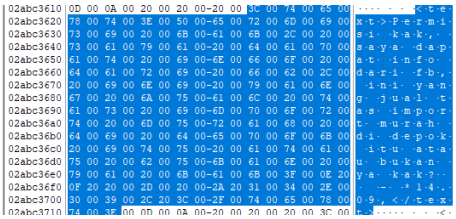
Browser History Viewer pada tahap ini digunakan untuk melakukan pencarian secara *default* pada *history browser*. Selain itu, *history* serta *cache browser* juga di-*filter* menggunakan *tools* yang sama. *Filtering* dilakukan berdasarkan tanggal kejadian (31 Januari 2021 s.d. 2 Februari 2021) dan *browser* (Google Chrome). Pengelompokkan bukti digital pada Browser History Viewer dilakukan secara otomatis meliputi *Website History*, *Cached Images*, dan *Cached Web Pages.*



Gambar 9. Pengelompokka dan *filtering* bukti digital *cache* dan *history browser*

3.3. Analysis

Analisis bukti digital yang pertama yaitu RAM *image* menggunakan FTK Imager. Analisis RAM *image* dilakukan untuk menemukan teks percakapan pada *Whatsapp* web antara pelaku dan korban. Salah satu hasil analisis RAM *image* yang berupa teks percakapan dan *timestamp* (keterangan waktu) ditunjukkan pada Gambar 10 di bawah ini.



Gambar 10. Bukti digital hasil analisis RAM *image*

Analisis pada RAM *image* manghasilkan 22 bukti digital yang meliputi teks percakapan, keterangan waktu, nomor *handphone* pengirim (korban), nomor rekening pelaku, *filename* gambar, dan *filename* video. Seluruh bukti digital yang ditemukan pada RAM *image* disajikan pada Tabel 4 berikut.

Tabel 4. Bukti digital RAM *image*

No.	Bukti RAM Image	Timestamp
1	Permisi kak, saya dapat info dari fb, ini yang jual tas import murah di depok itu atau bukan ya kak?	14:12
2	Saya tertarik sama produk yg baru diposting tadi pagi kak.	14:12
3	Masih ready ngga ya?	14:12
4	C:\Users\user\Videos\real product.mp4	-
5	Kak, produk yang kami jual 100% original	-
6	Isi formar berikut ya kak. Nama No HP Alamat Warna Produk Jumlah	-
7	u mau dikirim hari ini juga bisa langsung transfer ke sini ya kak. BTN 0018101610090714	-
8	Whatsapp Image 2021-01-31 at 14.40.jpg	14:40
9	Oke kak. pesanannya kami proses hari ini juga, mohon ditunggu	-
10	nanti kalau sdh ada saya kirimin ya. blm dikasih dari kurirnya	-
11	Oh gitu, ok deh kak	-
12	blm ada kak, ditunggu aja	-
13	iya kak dari kurirnya blm dikasih	-
14	+6285778883009	08:37
15	Saya biasanya juga kalo beli online begitu barang dikirim langsung ada ko resinya.	08:37
16	iya kak, sabar ya ditunggu aja	-
17	Masalahnya saya udh transfer dan katanya udh dikirim psenan saya. Tapi giliran ditanya resi blm ada terus	-
18	Gimana sih ini tokonya	-
19	Gmn nih uang udh saya transfer tapi pesanan saya ga jelas gini udh dikirim atau belum.	08:43
20	Bales chat saya dong! Tolong kejelasannya ya!!!	08:44
21	DASAR PENIPU KURANG AJAR!!!	08:46
22	Awas lo ya gua laporin ke polisi baru tau rasa!!!	08:47

Analisis *log file* dilakukan menggunakan FTK Imager pada *file* 000631.log dan *file* LOG. Hasil analisis *file* 000631.log yaitu berupa ID pengguna *Whatsapp* web, status *online Whatsapp*, serta *timestamp* pesan terkirim dan pesan diterima yang terdapat pada Tabel 5 di bawah ini.

Tabel 5. Bukti digital hasil analisis *file* 000631.log

No.	Bukti Digital	Keterangan
1	"value""Syaza Dyah Utami"{2‰B 2021-02-01	ID *User* Membuka
2	08:34:25.968:NetworkStatus online"	*Whatsapp* Web
3	2021-02-01 08:35:38.843: send: 3EB07ECB4DDE8D4B5E97, action,message,chat	Pesan Terkirim
4	2021-02-01 08:36:16.521: send: 3EB012C389D065587394, action,message,chat	Pesan Terkirim
5	2021-02-01 08:39:20.064: send: 3EB0BD551DA005469663, action,message,chat	Pesan Terkirim
6	2021-02-01 08:36:04.292:bin-recv: 6144173d577d2153.--c,action,msg,relay,chat	Pesan Diterima
7	2021-02-01 08:37:31.298:bin-recv: 6144173d577d2153.--11,action,msg,relay,chat	Pesan Diterima
8	2021-02-01 08:40:28.408:bin-recv: 6144173d577d2153.--15,action,msg,relay,chat	Pesan Diterima
9	2021-02-01 08:41:45.036:bin-recv: 6144173d577d2153.--17,action,msg,relay,chat	Pesan Diterima
10	2021-02-01 08:41:51.410:bin-recv: 6144173d577d2153.--18,action,msg,relay,chat	Pesan Diterima
11	2021-02-01 08:42:09.936:bin-recv: 6144173d577d2153.--19,action,msg,relay,chat	Pesan Diterima
12	2021-02-01 08:42:22.095:bin-recv: 6144173d577d2153.--1a,action,msg,relay,chat	Pesan Diterima
13	2021-02-01 08:43:41.819:bin-recv: 6144173d577d2153.--1b,action,msg,relay,chat	Pesan Diterima
14	2021-02-01 08:44:20.736:bin-recv: 6144173d577d2153.--1c,action,msg,relay,chat	Pesan Diterima
15	2021-02-01 08:46:46.069:bin-recv: 6144173d577d2153.--1d,action,msg,relay,chat	Pesan Diterima

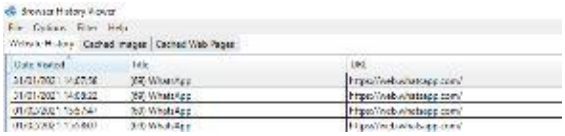
16	2021-02-01 08:47:19.576:bin-recv: 6144173d577d2153.--1e,action,msg,relay,chat	Pesan Diterima

Adapun bukti digital yang diperoleh dari *file* LOG yang menunjukkan penggunaan *Whatsapp* web pada hari pertama kejadian (31 Januari 2021). Bukti digital hasil analisis *file* LOG disajikan pada Tabel 6 di bawah ini.

Tabel 6. Bukti digital hasil analisis *file* LOG

No	Bukti Digital
1	2021/01/31-14:08:02.414 3b50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb/MANIFEST-000001
2	2021/01/31-14:08:02.597 3b50 Recovering log #626
3	2021/01/31-14:08:03.146 3b50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_web.whatsapp.com_0.indexeddb.leveldb/000626.log

Bukti digital hasil analisis *history* menggunakan Browser History Viewer yaitu ditemukan riwayat akses *Whatsapp* web yang sesuai dengan waktu kejadian pada tanggal 31 Januari 2021 pukul 14:07 dan 14:08. Bukti digital *history browser* ditunjukkan pada Gambar 11 berikut ini.



Gambar 11. Bukti digital hasil analisis *history browser*

Analisis pada *cache browser* menggunakan Browser History viewer dilakukan untuk menemukan bukti berupa gambar dan video. Namun, bukti digital tersebut tidak dapat ditemukan.

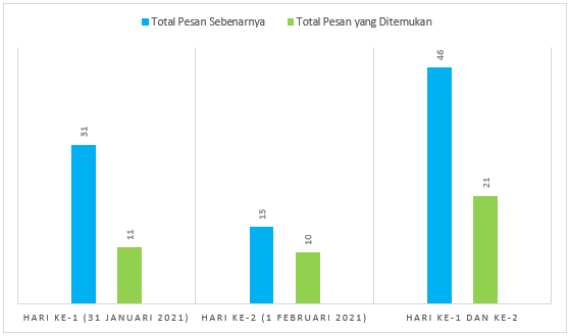
3.4. Reporting

Hasil dari tahap *reporting* (pelaporan) yang pertama berupa evaluasi bukti digital yang telah diperoleh. Tabel 7 berikut ini merupakan evaluasi hasil bukti digital.

Tabel 7. Evaluasi hasil bukti digital

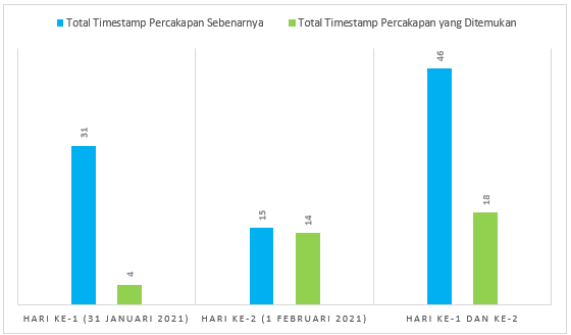
No.	Bukti Digital	Deskripsi	*Tools*
1	Teks percakapan	21 teks dari total 46 pesan (45,6%)	FTK Imager
2	*Filename* gambar	W.h.a.t.s.A.p.p..I.m.a.g.e. .2.0.2.1..0.1..3.1..a.t..1.4. ..4.0...4.1...j.p.e.g	FTK Imager
3	*Filename* video	C.:.\.U.s.e.r.s.\.u.s.e.r.\. V.i.d.e.o.s.\.r.e.a.l. .p.r.o.d.u.c.t...m.p.4	FTK Imager
4	*Timestamp*	18 *timestamp* dari total 46 *timestamp* percakapan (39%)	FTK Imager, Browser History Viewer
5	*History*	Riwayat aktivitas Whatsapp yang sesuai dengan waktu kejadian ditemukan pada *log file* dan *history browser*.	FTK Imager, Browser History Viewer
6	Identitas korban dan pelaku	Nomor *handphone* korban (085778883009) dan nomor rekening pelaku (BTN 0018101610090714) ditemukan pada RAM *image*	FTK Imager

Berdasarkan tabel di atas, bukti digital teks percakapan yang berhasil diperoleh hanya 45,6 %. Jika dihitung berdasarkan waktu kejadian (31 Januari dan 1 Februari 2021), pada hari pertama diperoleh 11 dari 31 pesan (35,5%) dan pada hari kedua diperoleh 10 dari 15 pesan (66,7%). Gambar 12 di bawah ini menggambarkan perbandingan jumlah bukti teks percakapan yang berhasil ditemukan dengan total teks percakapan sebenarnya.



Gambar 12. Diagram Perbandingan Bukti Teks Percakapan yang Ditemukan dengan Total Teks Percakapan Sebenarnya

Persentase perolehan bukti teks percakapan lebih tinggi di hari kedua dibandingkan dengan hari pertama karena dipengaruhi data RAM yang bersifat *volatile* (sementara dan mudah hilang). Bukti digital gambar dan video hanya dapat ditemukan nama *file*-nya saja pada RAM *image*. Bukti keterangan waktu (*timestamp*) pada percakapan antara korban dan pelaku dapat ditemukan pada RAM *image* dan *file* 000631.log sebanyak 18 dari 46 *timestamp* pesan (39%). Jika dihitung berdasarkan waktu kejadian (31 Januari dan 1 Februari 2021), pada hari pertama diperoleh 4 dari 31 *timestamp* pesan (12,9%) dan pada hari kedua diperoleh 14 dari 15 *timestamp* pesan (93,3%). Perbandingan antara bukti *timestamp* percakapan yang berhasil ditemukan dengan total *timestamp* percakapan sebenarnya ditunjukkan pada Gambar 13 berikut ini.



Gambar 13. Diagram Perbandingan Bukti Timestamp Percakapan yang Ditemukan dengan Total Timestamp Percakapan Sebenarnya

History penggunaan Whatsapp web pun ditemukan pada *file* LOG dan *history browser* yang membuktikan bahwa pada hari kejadian kasus tersebut pelaku memang mengakses Whatsapp web. Bukti digital yang berkaitan dengan identitas korban dan pelaku pun ditemukan pada salah satu teks percakapan di dalam RAM *image*, yaitu nomor *handphone* korban dan nomor rekening pelaku.

Pembuktian kasus penipuan transaksi elektronik yang terjadi memerlukan tinjauan dari segi hukum agar pelaku dapat mempertanggungjawabkan perbuatannya sesuai dengan hukum yang berlaku. Pertama, pelaku berusaha menipu dan merugikan korban dengan berpura-pura menjual sebuah barang. Tindakan kejahatannya dapat dijerat dengan UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat 1 Juncto Pasal 45a Ayat 1 serta UU Nomor 8 Tahun 1981 Pasal 378 Kitab Undang-Undang Hukum Acara Pidana Ayat 1 dan 2 yang mengatur tentang penipuan.

Selain itu, setelah menipu korbannya pelaku menghapus riwayat percakapan pada Whatsapp web yang berarti bahwa ia berusaha menghilangkan barang bukti. Maka perbuatannya tersebut dapat dijerat dengan UU Nomor 11 Tahun 2008 Tentang ITE Pasal 32 Ayat 1 Juncto Pasal 48 Ayat 1. Adapun metode yang digunakan untuk memperoleh bukti digital pada penelitian ini, yaitu ilmu Digital Forensik, dapat digunakan sebagai alat bukti yang sah di pengadilan karena termasuk keterangan ahli yang disebutkan di dalam UU Nomor 8 Tahun 1981 Pasal 184 Kitab Undang-Undang Hukum Acara Pidana Ayat 1. Bukti digital yang diperoleh pun dinyatakan sebagai alat bukti yang sah karena termasuk informasi/dokumen elektronik berdasarkan UU Nomor 11 Tahun 2008 Tentang ITE Pasal 5 Ayat 1 dan Pasal 6.

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan, pencarian bukti digital pada kasus penipuan transaksi elektronik menggunakan metode *live forensic* dilakukan dengan menganalisis RAM *image, log file, history,* dan *cache browser* menggunakan *tools* FTK Imager dan Browser History Viewer. Pembuktian kasus penipuan transaksi elektronik dilakukan dengan membandingkan/sinkronisasi antara bukti digital teks percakapan yang telah diperoleh dari laptop pelaku dengan percakapan Whatsapp pada *smartphone* korban. Adapun hasil evaluasi bukti digital yang diperoleh dari laptop pelaku di antaranya yaitu teks percakapan Whatsapp sebanyak 45,6% dari total 46 pesan, *timestamp* percakapan Whatsapp sebanyak 39% dari total 46 *timestamp* pada pesan, *filename* gambar dan video, *history browser*, nomor *handphone* korban, dan nomor rekening pelaku.

5. SARAN

Penelitian ini dapat dilakukan lebih lanjut dengan menganalisis perangkat bukti *smartphone* korban. Selain itu, pencarian bukti digital berupa gambar dan video dapat dilanjutkan menggunakan metode *static forensic* pada *hardisk* laptop pelaku dari *filename* yang telah ditemukan. Kemudian bukti digital gambar dan video tersebut dapat dianalisis masing-masing dengan menerapkan metode *image forensic* dan *video forensic.*

DAFTAR PUSTAKA

AL-AZHAR, M.N., 2012. *Digital Forensic Practical Guidlines for Computer Investigation*. Jakarta: Pusat Laboratorium Forensik Polri.

FAIZ, M.N., PRABOWO, W.A. dan SIDIQ, M.F., 2018. Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, 1(1), hal.63–70.

KEMP, S., 2021. *Digital 2021 Indonesia*. [daring] Tersedia pada: <https://datareportal.com/reports/digital-2021-indonesia?rq=indonesia> [Diakses 27 Feb 2021].

Mabes Polri, 2021. *Statistik: Patroli Siber*. [daring] Tersedia pada: <https://patrolisiber.id/statistic> [Diakses 1 Apr 2021].

MULYADI, D., 2017. Unsur-Unsur Penipuan Dalam Pasal 378 Kuhp Dikaitkan Dengan Jual Beli Tanah. *Jurnal Ilmiah Galuh Justisi*, 5(2), hal.206.

NASIRUDIN, N., SUNARDI, S. dan RIADI, I., 2020. Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, 5(1), hal.89.

RIADI, I., SUNARDI, S. dan RAULI, M.E., 2018. Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics. *Jurnal Teknik Elektro*, 10(1), hal.18–22.

SUDYANA, D., 2016. *Belajar Mengenali Forensika Digital*. Yogyakarta: Kelompok Penerbit Diandra.

SYAHIB, M.I., RIADI, I. dan UMAR, R., 2018. Analisis Forensik Digital Aplikasi Beetalk untuk Penanganan Cybercrime Menggunakan Metode NIST. *Seminar Nasional Informatika*, [daring] 2018(November), hal.134. Tersedia pada: <http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629>.

UMAR, R., RIADI, I. dan MUTHOHIRIN, B.F., 2019. Live forensics of tools on android devices for email forensics. *Telkomnika (Telecommunication Computing Electronics*

and Control), 17(4), hal.1803–1809.

WIRASILA, A.. N., DARMADI, A.. N.Y. dan PURWANI, S.P.M.E., 2017. *Buku Ajar Tindak Pidana Tertentu dalam KUHP Kejahatan dan Pelanggaran Terhadap Harta Benda*. Denpasar: Fakultas Hukum Universitas Udayana.

ZUHRIYANTO, I., YUDHANA, A. dan RIADI, I., 2018. Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics. *Seminar Nasional Informatika 2008 (semnasIF 2008)*, 2018(November), hal.86–91.