ANALISIS FORENSIK BROWSER KONTEN HOAX PADA LAYANAN MEDIA SOSIAL TIKTOK MENGGUNAKAN METODE *DIGITAL FORENSICS RESEARCH WORKSHOP*

Indah Rafni Yunipratiwi [1], **Imam Riadi** [2], **Abdul Fadlil** [3]
[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2] Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
[3] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
Jln. Ahmad Yani,Tamanan, Banguntapan, Bantul, Special Region of Yogyakarta.
2408048015@webmail.uad.ac.id

ABSTRAK

Perkembangan teknologi informasi telah mendorong masifnya penggunaan media sosial seperti TikTok, yang di Indonesia mencapai 108 juta pengguna. Namun, kemudahan ini juga memicu peningkatan penyebaran informasi palsu atau hoaks. Penelitian ini bertujuan menganalisis artefak digital pada browser yang digunakan untuk mengunggah konten hoaks di TikTok dengan menerapkan metode Digital Forensic Research Workshop (DFRWS). Penelitian dilakukan melalui empat tahap DFRWS: identifikasi dan pengumpulan data kasus hoaks di TikTok, akuisisi artefak browser (history, cache, cookies, metadata) menggunakan Autopsy dan Browser History Examiner, analisis artefak secara sistematis, serta interpretasi hasil untuk merekonstruksi kronologi penyebaran hoaks. Hasil analisis menunjukkan bahwa FTK Imager memperoleh 27,27% dari total temuan, dengan data berupa 1 teks keterangan, 1 nama pengguna, dan 1 tautan, Browser History Examiner memperoleh 18,18% dengan data berupa 1 username dan 1 link, Browser History Viewer mencatatkan 36,36% dengan 2 foto (1 foto profil dan 1 thumbnail video), 1 nama pengguna, dan 1 tautan, sementara Video Cache Viewer memperoleh 18,18% dengan 1 video dan 1 tautan. Hasil ini menunjukkan efektivitas metode DFRWS dalam mengidentifikasi dan menelusuri jejak digital aktivitas penyebaran hoaks di TikTok dengan akurasi yang mendukung pembuktian forensik. Penelitian ini memberikan kontribusi dalam penegakan hukum siber terkait hoaks di Indonesia.

Kata kunci : *Forensik Digital, DFRWS, Hoax, TikTok Browser*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam cara manusia berinteraksi dan memperoleh informasi. Kemajuan ini memungkinkan masyarakat untuk berbagi informasi secara cepat dan efisien melalui berbagai media digital. Salah satu perkembangan signifikan yang terjadi adalah hadirnya media sosial, yang kini telah menjadi platform utama dalam distribusi informasi. [1]. Media sosial, termasuk TikTok, telah digunakan oleh jutaan orang di seluruh dunia, termasuk Indonesia, sebagai sarana untuk berbagi berbagai jenis informasi [2] [3].

Namun, kemudahan ini juga memunculkan dampak negatif berupa penyebaran informasi palsu atau hoaks. Hoaks adalah informasi yang sengaja dibuat untuk menipu atau memanipulasi opini publik, dan sering kali sulit dibedakan dari informasi yang valid karena disajikan dengan cara yang meyakinkan [4]. Fenomena ini menimbulkan tantangan besar dalam menjaga literasi informasi dan mempertahankan kepercayaan publik terhadap sumber informasi digital [5].

TikTok, sebagai salah satu platform media sosial yang sangat populer, menjadi salah satu saluran utama untuk berbagi informasi. Dengan lebih dari 108 juta pengguna aktif di Indonesia, TikTok memiliki pengaruh besar dalam penyebaran informasi baik yang bersifat edukatif maupun yang menyesatkan [6]. Namun, platform ini juga menghadirkan tantangan tersendiri terkait penyebaran hoaks, terutama pada versi berbasis web yang memiliki keterbukaan lebih besar untuk dianalisis secara forensik digital. Berbeda dengan aplikasi mobile yang memiliki pengamanan lebih ketat, TikTok berbasis web memungkinkan pelacakan aktivitas pengguna melalui browser, yang menjadikannya fokus utama dalam penelitian ini [7][8].

Penyebaran hoaks melalui TikTok tidak hanya membingungkan masyarakat, tetapi juga dapat menyebabkan dampak negatif lebih lanjut seperti konflik sosial dan pengambilan keputusan yang keliru [9][10]. Hal ini diperburuk oleh minimnya literasi digital di sebagian besar kalangan masyarakat, yang menjadikan mereka lebih rentan terhadap informasi palsu [11]. Oleh karena itu, penting untuk melakukan upaya dalam mendeteksi dan menganalisis penyebaran hoaks, salah satunya dengan pendekatan forensik digital [12].

Forensik digital, sebagai ilmu yang berfokus pada identifikasi, pengumpulan, dan analisis bukti digital, menjadi salah satu metode yang relevan dalam menganalisis konten hoaks. Salah satu pendekatan yang dapat digunakan adalah metode DFRWS (*Digital Forensic Research Workshop*), yang terdiri dari enam tahapan: *identification*, *preservation/maintenance*, *collection*, *examination*, *analysis*, dan *presentation*. Metode ini dirancang untuk memastikan bukti digital tetap utuh, sah, dan dapat dipertanggungjawabkan secara hukum [13][14][15]. Pendekatan ini telah terbukti efektif dalam menganalisis berbagai kasus

kejahatan digital, termasuk penyebaran hoaks di media sosial dan aplikasi perpesanan [16].

Statistik terkini menunjukkan bahwa meskipun TikTok memiliki jangkauan pengguna yang sangat besar, efektivitasnya dalam menjangkau audiens melalui iklan mengalami penurunan signifikan. Data dari KEPIOS mengindikasikan bahwa jangkauan iklan TikTok turun sebesar 34,8% secara kuartalan dan 15,1% secara tahunan. Penurunan ini bisa jadi merupakan indikasi pergeseran perilaku pengguna, perubahan algoritma platform, atau peningkatan kesadaran publik terhadap konten hoaks yang disebarkan.

Melihat urgensi permasalahan ini, penelitian ini bertujuan untuk menganalisis penyebaran konten hoaks pada platform TikTok berbasis web melalui pendekatan forensik digital. Dengan menggabungkan metode DFRWS, diharapkan dapat dihasilkan model analisis yang lebih komprehensif, efektif, dan dapat digunakan dalam investigasi ke depan. Penelitian ini tidak hanya memberikan kontribusi akademik dalam bidang forensik digital, tetapi juga memberikan manfaat praktis bagi lembaga penegak hukum, analis siber, serta pihak-pihak yang berkepentingan dalam menjaga keamanan informasi di ruang digital.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian terdahulu menunjukkan bahwa penerapan metode forensik digital yang terstruktur berperan penting dalam mengungkap bukti digital. Akbar [17] mengkaji deteksi dan analisis steganografi pada berbagai jenis file menggunakan model GCFIM dan tools forensik, yang terbukti efektif dalam mengidentifikasi serta mengekstraksi pesan tersembunyi. Pendekatan serupa dikembangkan oleh Hamad dan Jazzar [18] melalui Improved GCFIM, yang mampu meningkatkan efektivitas investigasi steganografi pada beragam media digital. Selain itu, investigasi forensik terhadap media penyimpanan eksternal yang mengandung file steganografi juga menunjukkan bahwa proses akuisisi, preservasi, dan analisis yang tepat dapat menghasilkan bukti digital yang valid dan dapat dipertanggungjawabkan secara hukum [19].

Penerapan model forensik digital tidak hanya terbatas pada steganografi, tetapi juga pada analisis multimedia dan perangkat mobile. Nugraha [20] membuktikan bahwa model GCFIM efektif digunakan dalam analisis rekaman CCTV untuk mengidentifikasi pelaku kejahatan melalui teknik analisis visual secara mendalam. Pada konteks forensik mobile, beberapa penelitian menerapkan kerangka kerja DFRWS untuk mengekstraksi data dari aplikasi komunikasi dan finansial. Yudhana [21] serta Fadillah [22] menunjukkan bahwa metode DFRWS mampu mengungkap aktivitas pengguna dan memverifikasi keaslian bukti digital secara akurat. Namun, tantangan masih ditemukan pada aplikasi pesan dengan tingkat keamanan tinggi. Penelitian oleh Ichsan dan Riadi [23] serta Riadi [24] menegaskan bahwa akses root perangkat dan keterbatasan tools forensik menjadi faktor utama dalam keberhasilan ekstraksi data pada aplikasi yang menggunakan enkripsi end-to-end, sehingga diperlukan pengembangan alat dan metode forensik digital yang lebih canggih.

2.2. Forensik Digital

Forensik digital merupakan salah satu cabang dari ilmu forensik yang berfokus pada penanganan dan analisis bukti digital yang berkaitan dengan tindak kejahatan komputer maupun kejahatan siber. Bukti-bukti tersebut biasanya tersimpan dalam satu atau lebih perangkat komputer serta media penyimpanan digital lainnya [19]. Forensik digital merupakan salah satu bidang dalam ilmu forensik yang berfungsi untuk mengungkap tindak kejahatan di ranah digital atau dunia maya. Menurut Jessica, Theodorus, dan Carlo, digital forensik bertujuan untuk mengekstraksi data dari perangkat elektronik yang berfungsi sebagai barang bukti, kemudian mengolahnya menjadi informasi intelijen yang dapat digunakan dalam proses hukum. Melalui proses ini, penyidik forensik memiliki kemampuan untuk penelusuran, pemulihan, atau rekonstruksi data digital yang telah rusak maupun dihapus, sehingga dapat disajikan sebagai temuan dalam proses penegakan hukum[20].

2.3. Web Browser

Web browser adalah perangkat lunak yang digunakan untuk berselancar dalam dunia internet [25]. Pada awalnya, *browser* hanya dapat menampilkan teks, tetapi seiring perkembangannya, *browser* juga dapat memutar file multimedia seperti video dan audio, menerima dan mengirim email, mengurai kode HTML sebagai input, dan menampilkan lebih dari sekadar teks. berselancar dan halaman web sebagai output data adalah dua contohnya. Web juga dapat melacak kebiasaan berselancar pengguna, termasuk URL yang dikunjungi, foto yang diunduh, file yang disimpan, cookie yang dipasang, dan banyak lagi.[26] Selain itu, *Mozilla Firefox*, Google *Mozila*, Opera dan *Apple Safari* adalah *browser* yang paling umum digunakan [27].

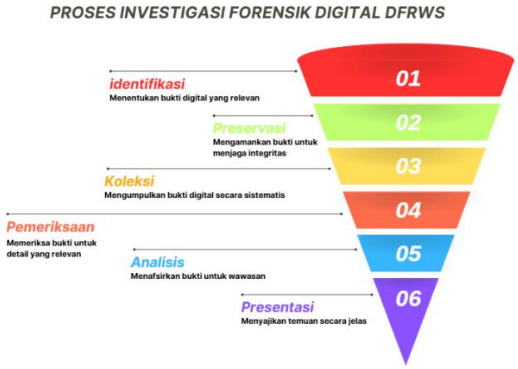
2.4. DFRWS (Digital Forensic Research Workshop)

DFRWS merupakan sebuah proses dalam disiplin ilmu forensik digital yang memiliki peran penting dalam membantu penyidik memperoleh bukti digital secara valid, sekaligus menyediakan mekanisme terpusat untuk mendokumentasikan dan menyimpan informasi yang telah dikumpulkan secara sistematis [28]. Kerangka kerja DFRWS dikenal sebagai metodologi yang banyak diadopsi oleh praktisi dan peneliti dalam melakukan investigasi forensik digital di berbagai platform, mulai dari perangkat komputer, aplikasi, hingga layanan berbasis web dan *cloud*. Biasanya, metodologi DFRWS mencakup enam

tahapan utama yang saling berkesinambungan, yaitu tahap identifikasi sumber bukti, tahap pelestarian agar integritas bukti tetap terjaga, tahap pengumpulan data, tahap pemeriksaan mendetail, tahap analisis untuk mengungkap fakta dari data, serta tahap penyajian hasil analisis dalam bentuk laporan yang dapat dipertanggungjawabkan di pengadilan. Dengan struktur yang terorganisir ini, DFRWS menjadi salah satu metode yang efektif untuk mendukung keabsahan dan keterpercayaan hasil investigasi digital.

3. METODE PENELITIAN

Penelitian ini akan menerapkan metode DFRWS yang berfungsi penting dalam proses investigasi guna mendapatkan bukti digital yang sah serta menyediakan sistem dokumentasi terpusat yang rapi dan sistematis [28]. Sebagaimana dijelaskan pada Gambar 1.



Gambar 1. Proses investigasi forensik

Pada Gambar 1 diatas menunjukkan tahap-tahap dari metode yang kita gunakan, untuk penjelasan setiap tahap, sebagai berikut:

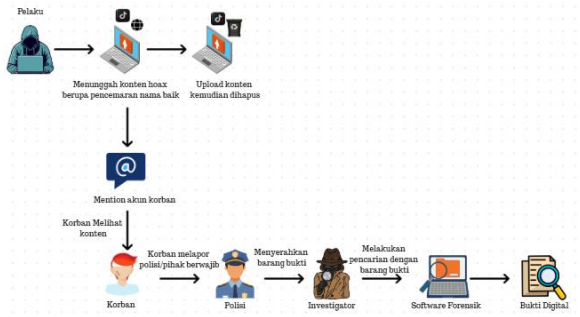
a. Identifikasi
   Langkah pertama dalam proses forensik digital adalah tahap identifikasi bukti yang relevan dengan kasus. Tahap ini mencakup pencarian dan penentuan data atau informasi yang berpotensi mendukung jalannya investigasi. Tim forensik perlu menetapkan perangkat keras, perangkat lunak, serta sistem yang akan dianalisis, dan mengidentifikasi jenis bukti apa saja yang perlu didokumentasikan. Selain itu, pemahaman mendalam mengenai konteks kasus juga diperlukan agar bukti yang ditemukan benar-benar mendukung penyidikan.
b. Pelestarian *(Preservasi)*
   Setelah bukti berhasil diidentifikasi, tahap berikutnya adalah menjaga bukti tersebut tetap utuh agar tidak mengalami perubahan, kerusakan, atau kontaminasi. Ini dilakukan dengan membuat salinan data dan memastikan bukti disimpan dalam keadaan yang tidak dapat dimodifikasi. Pada tahap ini, sangat penting untuk tidak menggunakan perangkat asli secara langsung karena dapat mengakibatkan perubahan data. Oleh karena itu, penggunaan perangkat lunak dan alat forensik yang mampu menghasilkan salinan bit-per-bit sangat diperlukan untuk menjaga keaslian bukti.
c. Pengumpulan (*Collection*)
   Pengumpulan bukti dilakukan dengan cara yang legal, terstruktur, dan sesuai prosedur. Data yang dianggap penting akan diambil dari berbagai sumber, seperti komputer, perangkat seluler, server, media penyimpanan (USB, kartu memori), maupun file digital lainnya yang berhubungan dengan insiden. Selama proses ini, pengumpulan harus dilakukan dengan hati-hati untuk menghindari kerusakan atau perubahan data, serta semua tahapan pengumpulan perlu dicatat secara detail agar bukti sah di mata hukum.
d. Pemeriksaan (*Examination*)
   Pada tahap pemeriksaan, data yang sudah dikumpulkan akan dianalisis secara menyeluruh untuk menemukan bukti yang berkaitan langsung dengan kasus. Proses ini meliputi ekstraksi file tersembunyi, pengecekan metadata, analisis file log, dan penelusuran jejak digital lainnya yang bisa mengarah pada temuan penting. Tujuan pemeriksaan adalah memastikan bahwa data yang diperoleh benar-benar relevan, akurat, dan dapat mendukung pertanyaan atau hipotesis penyelidikan.
e. Analisis (*Analysis*)
   Tahap analisis merupakan fase di mana data yang telah diperiksa dievaluasi secara mendalam untuk mengungkap pola, hubungan antar data, serta indikasi aktivitas ilegal atau pelanggaran yang terjadi. Di sini, forensik digital akan menafsirkan informasi secara detail untuk mendapatkan kesimpulan yang mendukung kasus. Selain itu, analisis juga memastikan bahwa bukti yang ditemukan dapat diterima sebagai barang bukti di pengadilan dan memiliki keterkaitan langsung dengan perkara yang diselidiki.
f. Penyajian (*Presentation*)
   Tahap terakhir adalah menyusun hasil investigasi dalam bentuk laporan yang rapi, sistematis, dan mudah dipahami. Laporan ini memuat ringkasan temuan utama, detail bukti yang berhasil dikumpulkan, serta metode yang digunakan pada setiap tahapan penyelidikan. Penyajian bukti ini penting karena laporan yang dihasilkan akan menjadi dokumen resmi yang digunakan dalam proses hukum, baik di pengadilan maupun dalam penyelidikan internal, sehingga harus dapat dipertanggungjawabkan secara hukum

3.1. Skenario Penelitian

Pada Gambar 2 merupakan skenario kejadian yang mengsimulasikan kasus berita hoax pada TikTok Web, dengan penjelasan sebagai berikut:

Skenario ini dibuat untuk menjabarkan tahapan-tahapan *forensic* web browser. Skenario penelitian ini menggunakan sebuah laptop yang di gunakan untuk mendeteksi konten *hoax* yang menyebar pada layanan

TikTok web. Kasus ini di skenariokan bagaimana pelaku mengupload konten *hoax* yang menyebar pada layanan *TikTok* yang berjalan pada browser *mozila.* Pihak yang merasa di rugikan kemudian melaporkan konten tersebut kepada pihak aparat yang berwajib. Laptop yang di gunakan oleh tersangka menjadi barang bukti untuk dilakukan i*maging* menggunakan aplikasi *forensic*. Kemudian kasus diselidiki oleh *investigator* degan menggunakan *software forensic* digital. Hasil penyelidikan yaitu berupa barang bukti digital.



Gambar 2. Skenario Kasus Penelitian

Parameter uji secara terprogram. Dalam kasus ini, *smartphone* dan laptop pelaku menggunakan proses forensik digital untuk menemukan barang bukti. Selain sebagai parameter uji, tujuan dari pembuatan skenario penelitian ini adalah untuk menentukan tindakan yang akan dilakukan selama proses penelitian. Skenario ini dibuat untuk menggambarkan berbagai tahapan forensik web browser. Skenario ini menggunakan laptop untuk mendeteksi penyebaran konten *hoax* di web browser TikTok. Pada tahap ini, menjelaskan proses identifikasi barang bukti dalam kasus ini gambar. Pihak yang di rugikan melaporakan konten tersebut ke polisi, dan laptop yang digunakan tersangka menjadi barang bukti digital menggunakan aplikasi forensik, yang kemudian diselidiki oleh investigator menggunakan perangkat lunak forensik digital.

4. HASIL DAN PEMBAHASAN

Studi ini berhasil mendapatkan bukti digital melalui proses analisis dan ekstraksi data pada media social TikTok. Hasil analisis akan disajikan menggunakan skema DFRWS

4.1. *Identification*

Tahap Plan ini disebut juga tahap perencanaan. Pada tahap ini, perangkat keras dan perangkat lunak yang akan digunakan dan tindakan yang akan diambil selama investigasi direncanakan. Perencanaan diperlukan agar proses penelitian dapat berjalan dengan lancar, termasuk menentukan alat-alat yang akan digunakan dalam proses penelitian sehingga dapat diperoleh hasil penelitian yang valid, selain memiliki rancangan tahap investigasi dan rencana simulasi uji pada tahap ini.

Tahap identifikasi ini juga mencakup penentuan skenario penelitian yang digunakan sebagai parameter uji, yaitu simulasi penyebaran video hoaks oleh akun TikTok pelaku melalui browser Mozilla Firefox. Skenario ini membantu peneliti memahami konteks kasus, menentukan titik-titik penting dalam sistem yang berpotensi menyimpan bukti digital, serta mempersiapkan proses akuisisi pada tahap selanjutnya. Tahap identifikasi berperan penting dalam memastikan seluruh langkah investigasi forensik dilakukan secara terencana, terarah, dan sesuai standar prosedur forensik digital yang berlaku dalam kerangka metode DFRWS.

4.2. *Preservation*

Tahap ini bertujuan untuk menjaga keaslian, integritas, dan keandalan bukti digital agar tetap autentik serta dapat diterima secara hukum sesuai dengan prinsip-prinsip forensik digital. Pada penelitian ini, proses pelestarian dilakukan terhadap laptop Lenovo *AMD Ryzen 7 4800U with Radeon Graphics 8.00 GB RAM* yang digunakan pelaku untuk mengunggah konten hoaks melalui TikTok Web. Proses akuisisi data dilakukan menggunakan FTK Imager untuk membuat salinan bit-per-bit (*forensic image*) dari media penyimpanan asli tanpa mengubah struktur atau isi data. Langkah ini mencakup pencadangan file sistem, *cache*, riwayat penelusuran, dan artefak digital lainnya yang tersimpan di browser Mozilla Firefox. Selama proses pelestarian, investigator memastikan penerapan rantai pengawasan (*chain of custody*) dengan melakukan dokumentasi lengkap atas setiap tindakan, mulai dari pengambilan hingga penyimpanan salinan forensik. Semua proses pemeriksaan dan analisis selanjutnya dilakukan pada salinan hasil imaging, bukan pada perangkat asli, untuk mencegah modifikasi atau kerusakan data. Dengan demikian, tahap pelestarian berfungsi sebagai mekanisme perlindungan hukum yang menjamin bahwa bukti digital yang diperoleh tetap utuh, dapat diverifikasi, dan memiliki kredibilitas tinggi dalam konteks penyelidikan forensik digital berbasis metode DFRWS.

4.3. *Collection*

Pada Tahapan ini merupakan tahapan awal, dimana tahap pengumpulan dilakukan dengan proses mencari dan mengumpulkan barang-barang yang diidentifikasi sebagai barang bukti untuk mendukung penyidikan kasus penyebaran konten *hoax* Pada skenario ditemukan laptop yang terhubung dengan internet yang diduga sebagai alat penyebaran konten *hoax* melalui aplikasi *TikTok.* Laptop tersebut adalah laptop dengan *merk* Lenovo. Berikut merupakan barang bukti yang dapat dilihat pada

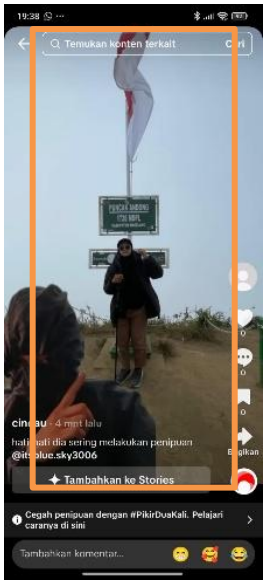
Tabel **1** di bawah ini.

Tabel 1. Contoh barang bukti

No	Barang Bukti	Gambar
1	Laptop Pelaku	
2	Kabel Pengisi Daya	

Pada

Tabel **1** menampilkan dokumentasi barang bukti yang di dapatkan dari tempat kejadian perkara yaitu sebuah laptop lenovo *ideapad slim* 5 dengan *AMD Ryzen 7 4000U with Radeon Graphics* dan RAM 8GB serta penyimpanan SSD 512 GB dengan sebuah *OS* windows 11 yang di temukan menyala dan masih terhubung ke internet. Berikut merupakan gambar bukti laporan dari korban yang dapat dilihat pada Gambar 3 di bawah ini.



Gambar 3. Bukti Laporan Korban

Pada Gambar 3 terlihat sebuah video dari akun TikTok dengan user "@cincau" yang menampilkan caption provokatif "hati-hati diaa sering melakukan penipuan @itsblue.sky3006". Data yang diperoleh dapat dilihat pada Tabel 2.

Tabel 2. Jenis data yang diperoleh

No	Data Obtained
1	User Pelaku
2	Caption Pelaku

Pada Tabel 2 menunjukkan jenis data yang diperoleh selama proses pengumpulan data dari ponsel korban. Korban memberikan ponselnya beserta bukti-bukti lain, seperti informasi akun pelaku, lokasi terakhir pelaku, riwayat chat sebelum dihapus oleh pelaku, dan riwayat chat setelah dihapus oleh pelaku. Bukti-bukti yang didapatkan dari smartphone korban nantinya akan digunakan untuk membandingkan dengan bukti-bukti yang didapatkan dari *smartphone* pelaku.

4.4. *Examination*

Pada tahapan ini dilakukan proses pemeriksaan terhadap data yang telah diperoleh sebelumnya. Pemeriksaan dilakukan pada data hasil capture RAM (*Random Access Memory*) dan hasil capture riwayat penelusuran pada web browser yang digunakan. Untuk membaca data yang telah diperoleh digunakan *tools* forensik yaitu *tools FTK Imager, Browser History Examiner, Browser History Viewer* dan Video Cache.Analysis.

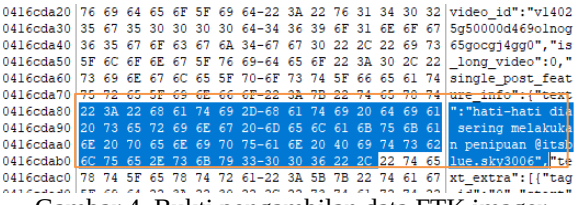
a. *FTK Imager* berhasil menemukan bukti berupa Username Pelaku, dan Caption yang di posting pelaku yang tersimpan pada direktori D:\FORENSIK 1\bukti.mem dengan nama file bukti.mem.
b. *Browser History Examiner* menemukan tanggal penguploadan, jam, url dan riwayat history yang tersimpan pada folder di direktori D:\FORENSIK 1\Capture\Firefox\Profiles\am22dfuy.default-release-1635777173628.
c. *Browser History Viewer* menemukan foto profile dan thumbnail yang tersimpan pada folder dengan nama Profiles\am22dfuy.default-release-1635777173628.
d. *Video Cache View* menemukan video yang tersimpan di folder direktori C:\Users\LENOVO\AppData\Local\Mozilla\Firefox\Profiles\am22dfuy.default-release-1635777173628\cache2\entries\1C9DB69353B06A95C7B760942610E5E783DC3532.

4.5. *Analysis*

Tahap analysis, peneliti dapat menganalisis barang bukti secara manual atau dengan bantuan software yang di gunakan. Analisis secara manual dilakukan dengan cara mengamati, mengelompokkan, dan mencatat informasi penting dari barang bukti secara langsung berdasarkan kriteria yang telah ditentukan.

4.6. *FTK Imager*

Bukti yang diperoleh pada tahap selanjutnya dari pemeriksaan akan dianalisis untuk menemukan bukti digital atau data yang dapat menjadi petunjuk. Alat FTK imager akan digunakan untuk menganalisis hasil pemeriksaan sebelumnya yang akan di lakukan menggunakan alat FTK Imager. Berkas pengambilan data kemudian akan dianalisis. Proses pengumpulan data atau bukti digital juga akan dilakukan dengan fitur alat yang sama untuk pengumpulan bukti, seperti yang ditunjukkan pada Gambar 4.



Gambar 4. Bukti pengambilan data FTK imager

Pada Gambar 4 adalah hasil pencarian pertama dengan kata kunci "@itsblue.sky3006". Hasilnya adalah caption di TikTok dengan caption pengguna. Caption "Hati-hati dia sering melakukan penipuan @itsblue.sky3006". Tabel 3 hasil analisis yang temukan menggunakan FTK Imager.

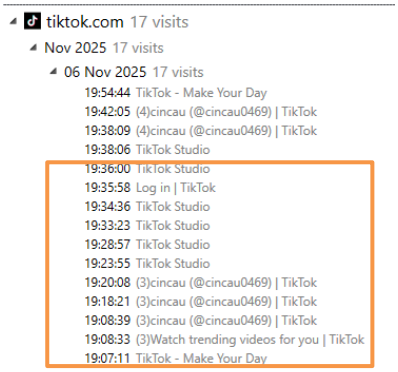
Tabel 3. Hasil FTK imager

No	Perangkat	Hasil	Keterangan
1	Username	@cincau	Ditemukan
2	Caption	"hati-hati dia sering melakukan penipuan @itsblue.sky3006"	Ditemukan

Pada Tabel 3 menunjukkan hasil FTK Imager yang ditemukan yaitu informasi Username dan Caption yang di buat oleh pelaku. Dengan Caption yang berisikan "hati-hati dia sering melakukan penipuan @itsblue.sky3006" dan ditemukan Username pelaku yaitu "@cincau".

4.7. *Browser History Examiner*

Browser History Examiner digunakan untuk membuka dan menganalisis hasil tangkapan riwayat penelusuran browser web. Alat ini menampilkan grafik aktivitas pengguna serta menyediakan fitur filter berdasarkan kata kunci dan rentang waktu untuk mempermudah pencarian data yang relevan. Data yang dianalisis meliputi URL yang dikunjungi, tanggal dan waktu akses, email, browser yang digunakan, gambar yang dimuat, serta halaman web yang pernah diakses. *Browser History Examiner* mendukung analisis riwayat web pada browser Chrome, Firefox, dan Internet Explorer di platform Windows. Contoh hasil analysis dengan *Browser History Examiner* pada Gambar 5.



Gambar 5 Hasil *Analysis Browser History Examiner*

Pada Gambar 5 terbukti pada *tools browser history examiner* pelaku mengunggah sebuah video pada pukul 19.08 tanggal 06/11/2025.

4.8. *Browser History Viewer*

Tabel 4. Hasil bukti analysis browser history viewer

Informasi	Hasil
Foto Profil	
Thumbnail Video	

Pada Tabel 4 yaitu berisikan hasil bukti analysis menggunakan *browser history viewer* yang di mana di temukan bukti berupa foto profil dan thumbnail dari postingan pelaku.

4.9. *Video Cache View*

Video Cache Viewer Adalah alat yang digunakan untuk mengambil video dari aplikasi browser Firefox, Chrome, Internet Explorer. Proses pengambilan melibatkan ekstraksi bertahap berkas video dari cache video dibrowser. Semua *cache* dari browser yang merupakan browser akan secara otomatis dibaca oleh alat ini.

4.10. *Presentation*

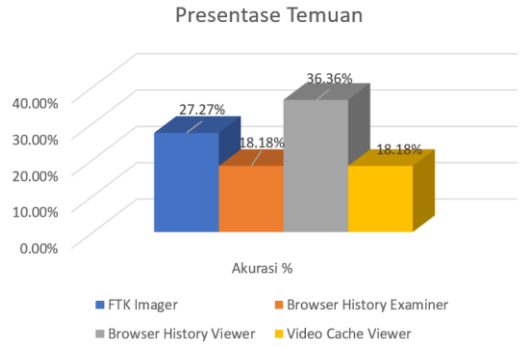
Tahap pelaporan merupakan bagian akhir dari proses presentation dalam kerangka metode DFRWS. Pada tahap ini, seluruh hasil analisis forensik digital terhadap web browser Mozilla Firefox yang digunakan dalam tindak penyebaran konten hoaks melalui TikTok Web didokumentasikan secara sistematis dan komprehensif. Laporan ini mencakup hasil temuan dari berbagai alat forensik yang digunakan selama proses investigasi, yaitu *FTK Imager, Browser History Examiner, Browser History Viewer*, dan *Video Cache View*. Tujuan dari tahap ini adalah menyajikan hasil analisis secara terukur serta memperlihatkan perbandingan kemampuan setiap alat forensik dalam mengekstraksi artefak digital yang relevan dengan kasus. Hasil Perbandingan antar alat forensik pada Tabel 5.

Tabel 5. Hasil perbandingan antar alat forensik

Bukti Digital	FTK Imager	Browser History Examiner	Browser History Viewer	Video Cache Viewer
Foto/Thumbnail	0	0	2	0
Video	0	0	0	1
Caption	1	0	0	0
Username	1	1	1	0
Link	1	1	1	1

Pada Tabel 5 merupakan hasil perbandingan antar alat forensik tersebut menunjukkan bahwa setiap perangkat lunak memiliki kemampuan berbeda dalam mengungkap artefak digital, pada tools FTK Imager unggul dalam menemukan data berbasis teks dan struktur file, sedangkan *Browser History Examiner* dan *Viewer* efektif untuk menelusuri artefak visual serta histori aktivitas. Adapun *Video Cache View* berfungsi memperkuat pembuktian dengan menampilkan konten video asli dari *cache browser*. Dengan demikian, laporan akhir ini memberikan gambaran menyeluruh mengenai integrasi antar alat

forensik dalam memastikan keakuratan, validitas, dan konsistensi bukti digital yang ditemukan selama proses investigasi forensik pada kasus penyebaran hoaks di TikTok Web, ditunjukan pada Gambar 6.



Gambar 6. Presentasi Temuan

Pada Gambar 6 menunjukkan presentasi jumlah temuan pada empat alat pengumpulan data, yaitu *FTK Imager*, *Browser History Examiner*, *Browser History Viewer*, *Video Cache View*. Dari presentasi tersebut, dapat dilihat perbandingan signifikan antara ketiga alat dalam proses pengumpulan data, seperti caption, gambar, video, file, dan sebagainya. *FTK imager* memiliki total 27,27% presentasi, dengan data di peroleh dari 1 teks keterangan, 1 nama pengguna, dan 1 tautan, *Browser History Examiner* memiliki total 18,18% presentasi, dengan data di peroleh 1 username dan 1 link, *Browser History Viewer* memiliki jumlah presentasi tersebar dengan 36,36% mengumpulkan 2 foto (1 foto profil dan 1 *thumbnail video*), 1 nama pengguna, dan 1 tautan. Sementara itu, *video cache viewer* memiliki 18,18% dan total presentasi dari 1 video dan 1 tautan.

5. KESIMPULAN DAN SARAN

Penerapan metode DFRWS terbukti efektif dalam mengidentifikasi dan menganalisis artefak digital yang terkait dengan penyebaran konten hoaks pada TikTok Web melalui browser Mozilla Firefox. Proses forensik dilakukan secara sistematis melalui enam tahapan utama, yaitu identifikasi, pelestarian, pengumpulan, pemeriksaan, analisis, dan penyajian. Hasil analisis menunjukkan bahwa alat forensik *FTK Imager*, *Browser History Examiner*, *Browser History Viewer*, dan *Video Cache Viewer* mampu mengungkap berbagai jenis bukti digital, seperti *username*, *caption*, foto profil, thumbnail video, riwayat tautan (URL), serta cache video. Integrasi hasil dari keempat alat tersebut berhasil merekonstruksi kronologi aktivitas digital pelaku secara akurat, yang mendukung proses pembuktian forensik. Berdasarkan alat yang digunakan dalam penyelidikan ini, 90% bukti berhasil diperoleh, sementara 10% tidak berhasil diperoleh, yaitu kata sandi tersangka. Presentasi jumlah temuan menunjukkan bahwa *FTK Imager* memperoleh 27,27% dengan data berupa 1 teks keterangan, 1 nama pengguna, dan 1 tautan, *Browser History Examiner* memperoleh 18,18% dengan data berupa 1 username dan 1 link, *Browser History Viewer* mencatatkan 36,36% dengan 2 foto (1 foto profil dan 1 thumbnail video), 1 nama pengguna, dan 1 tautan, sedangkan *Video Cache Viewer* memperoleh 18,18% dengan 1 video dan 1 tautan. Oleh karena itu, metode DFRWS terbukti relevan dan dapat dijadikan pedoman yang efektif dalam penyelidikan forensik digital terkait kasus penyebaran hoaks di media sosial berbasis web.

DAFTAR PUSTAKA

[1] I. Fauziah, S. A. Saputri, and Y. Herlambang, "Teknologi Informasi: Dampak Media Sosial pada Perubahan Sosial Masyarakat," *Indo-MathEdu Intellectuals Journal*, p., 2024, doi: 10.54373/imeij.v5i1.645.

[2] A. Anuashok, V. Gupta, T. Tyagi, T. Agarwal, R. Reddy, and A. Rout, "A Study on the Impact of Social Media on Modern Communication," *International Journal For Multidisciplinary Research*, p., 2024, doi: 10.36948/ijfmr.2024.v06i02.15980.

[3] E. H. Lee, T. Lee, and B.-K. Lee, "Understanding the role of new media literacy in the diffusion of unverified information during the COVID-19 pandemic," *New Media Soc.*, vol. 26, pp. 5195–5218, 2022, doi: 10.1177/14614448221130955.

[4] M. Ulfa Batoebara and B. S. Hasugian, "Isu Hoaks Meningkat Menjadi Potensi Kekacauan Informasi," vol. 4, no. 2, 2023, [Online]. Available: https://www.kominfo.go.id/content/detail/51727/siaran-pers-no

[5] P. Majerczak and A. Strzelecki, "Trust, Media Credibility, Social Ties, and the Intention to Share towards Information Verification in an Age of Fake News," *Behavioral Sciences*, vol. 12, p., 2022, doi: 10.3390/bs12020051.

[6] S. Kemp, "TikTok Users, Stats, Data & Trends for 2025," Datareportal, Kepios. Accessed: May 11, 2025. [Online]. Available: https://datareportal.com/essential-tiktok-stats

[7] F. Zahrah and I. Riadi, "Browser Forensics on Web-based Tiktok Applications using Digital Forensic Research Workshop Method," *Int. J. Comput. Appl.*, p., 2023, doi: 10.5120/ijca2023923009.

[8] Y. Keim, S. Hutchinson, A. Shrivastava, and U. Karabiyik, "Forensic Analysis of TikTok Alternatives on Android and iOS Devices: Byte, Dubsmash, and Triller," *Electronics (Basel).*, p., 2022, doi: 10.3390/electronics11182972.

[9] D. Surjatmodjo, A. Unde, H. Cangara, and A. F. Sonni, "Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience," *Soc. Sci.*, p., 2024, doi: 10.3390/socsci13080418.

[10] D. A. H. Hakim and I. Riadi, "Forensic Analysis of Instagram Application Against Case of Spreading Hoax Content using National Institute

of Justice Method," *Int. J. Comput. Appl.*, p., 2025, doi: 10.5120/ijca2025925637.

[11] I. Isnaini, T. N. Nasyiriyah, N. A. Istighfari, and S. R. Rohmah, "The Role of Digital Literacy in Social Media," *MIMESIS*, p., 2025, doi: 10.12928/mms.v6i1.12242.

[12] I. Riadi, H. Herman, and I. A. Rafiq, "Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework," *International Journal of Artificial Intelligence Research*, p., 2022, doi: 10.29099/ijair.v6i2.311.

[13] Sonasri.S and B. P. Niranjana. M, "Cyber Forensics: Investigating Digital Crimes," *International Journal on Science and Technology*, p., 2025, doi: 10.71097/ijsat.v16.i2.3389.

[14] A. S. S. Hamed, "Digital Forensic: Techniques, Challenges, and Future Direction," *Int. J. Res. Appl. Sci. Eng. Technol.*, p., 2025, doi: 10.22214/ijraset.2025.71562.

[15] K. A. Arifin and I. Riadi, "Forensic Analysis of Online Fraud on Telegram Web using Digital Forensics Workshop Method," *Int. J. Comput. Appl.*, p., 2025, doi: 10.5120/ijca2025925515.

[16] D. Rohmah and I. Riadi, "Mobile Forensic Analysis of Child Pornography Cases on Twitter using Digital Forensic Research Workshop Method," *Int. J. Comput. Appl.*, p., 2025, doi: 10.5120/ijca2025925711.

[17] M. Hajar Akbar, Sunardi, and I. Riadi, "Steganalysis Bukti Digital pada Media Storage Menggunakan Metode GCFIM," 2020.

[18] N. Hamad and M. Jazzar, "An Improved GCFIM Framework for Analyzing Digital Evidence Steganography," 2024. [Online]. Available: https://www.researchgate.net/publication/380154459

[19] M. Hajar Akbar, Sunardi, and I. Riadi, "Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework," 2020. [Online]. Available: www.ijacsa.thesai.org

[20] A. Nugraha, E. I. Alwi, and A. W. M. Gaffar, "Penerapan Model Investigasi Forensik Komputer Umum dalam Analisis Forensik Video CCTV," *Jurnal Minfo Polgan*, vol. 13, no. 1, pp. 1130–1137, Aug. 2024, doi: 10.33395/jmp.v13i1.13963.

[21] A. Yudhana, I. Riadi, R. Yudhi Prasongko, A. Dahlan, J. Ahmad Yani Tamanan, and J. Soepomo, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," vol. 7, no. 1, 2022.

[22] M. N. Fadillah, R. Umar, A. Yudhana, A. Dahlan, Y. Jalan, and S. H. Soepomo, "Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan Metode DFRWS," 2022.

[23] A. N. Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, Feb. 2021, doi: 10.5120/ijca2021921076.

[24] I. Riadi, Herman, and N. H. Siregar, "Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework," *Ingenierie des Systemes d'Information*, vol. 27, no. 6, pp. 903–913, Dec. 2022, doi: 10.18280/ISI.270606.

[25] A. D. Abdiati, S. Setiawan, and H. Supendar, "Pemilihan web browser pada mobile menggunakan metode analytical hierachy process," *Jurnal Infortech*, vol. 3, no. 1, pp. 26–32, 2021.

[26] H. HARIANI, "EKSPLORASI WEB BROWSER DALAM PENCARIAN BUKTI," vol. 6, no. April, pp. 66–74, 2021.

[27] M. F. Sidiq and M. N. Faiz, "Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital," *J. Edukasi dan Penelit. Inform*, vol. 5, no. 1, pp. 67–73, 2019.

[28] E. Satriya Wijaya and F. Tyas Pramesti, "Analisis Bukti Digital Forensik Pada Aplikasi Facebook Messenger Dan Twitter Berbasis Android Menggunakan Proses DFRWS (Studi Kasus: Pencemaran Nama Baik)," *Jurnal Media Pratama*, vol. 18, 2024.

[29] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, no. 1, pp. 43–48, Jan. 2022, doi: 10.30591/jpit.v7i1.3639