ANALISIS FORENSIK SMARPHONE ANDROID PADA APLIKASI TIKTOK MENGGUNAKAN METODE NIST

Faul Isnaeni, Fahmi Fachri
Teknik Informatika, Universitas Nadhlatul Ulama Kebumen
Jalan Raya Kutoarjo Km 5 Jatisari, Kebumen, Kebumen, Jawa Tengah 54317, Indonesia
faulisnaeni@gmail.com

ABSTRAK

Indonesia adalah negara yang sedang mengalami perkembangan pesat dalam pemanfaatan teknologi, termasuk penggunaan *smartphone* berbasis Android. Perkembangan teknologi internet dan smarphone yang semakin meningkat membuka peluang terjadinya kasus kejahatan di media sosial. Tindak kejahatan tersebut akan meninggalkan *history* yang dapat dijadikan barang bukti pada suatu kasus kejahatan teknologi komputer. *Digital forensik* adalah disiplin ilmu yang digunakan untuk membantu penegak hukum dalam menangani kejahatan digital. Tujuannya adalah untuk membuktikan tindak kejahatan tersebut dan mengumpulkan bukti digital yang sah. Penelitian ini menginvestigasi pencemaran nama baik di tiktok dengan memulihkan video, *hashtag*, serta pesan teks kemudian dihapus dari perangkat *smartphone* Android dengan menggunakan motode NIST sebagai langkah penelitian. Tahapan dari penelitian ini yaitu *Collection, Examination, Analysis,* dan *Reporting* untuk mendapatkan bukti digital pada aplikasi tiktok menggunakan *tools mobiledit* dan *FTK Imager*. *Hasil yang diperoleh* presense dengan tools *mobiledit* sebesar 25,5 % berhasil menemukan 11 data dari 43 data awal. Dan hasil presense dengan *tools FTK Imager* sebesar 74,4% berhasil menemukan sejumlah 32 data dari 43 data awal.

Kata kunci : *Bukti Digital, Digital Forensik, Media Sosial, NIST, Tools Forensik*

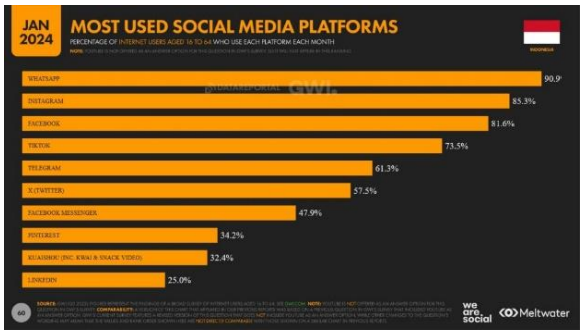
1. PENDAHULUAN

Indonesia adalah negara yang sedang mengalami perkembangan pesat dalam pemanfaatan teknologi, termasuk penggunaan *smartphone* berbasis Android. Setiap hari, para pengembang sistem Android terus berinovasi untuk memberikan kenyamanan bagi pengguna dan pelanggan [1]. Dampak negatif dari perkembangan *smartphone* bagi pengguna terkait dengan pencurian dan penghapusan data untuk menghilangkan barang bukti kejahatan yang dilakukan oleh pelaku. Barang bukti digital ini bisa berupa data di *smartphone*, seperti rincian kontak, *log* panggilan, pesan, video, gambar, dan file dokumen, yang dapat digunakan sebagai alat bukti di pengadilan [2].

Dengan memanfaatkan internet, masyarakat dapat mengeksplorasi berbagai hal dalam waktu singkat. Kemudahan yang ditawarkan oleh internet sangat mendukung komunikasi jarak jauh, yang sebelumnya memerlukan surel atau surat dan bisa memakan waktu berhari-hari. Kini, komunikasi dapat dilakukan secara *real-time*. Internet juga mempermudah akses bagi semua lapisan masyarakat, dari yang muda hingga tua, baik sebagai media untuk mencari informasi pendidikan maupun untuk transaksi bisnis. Beragam kegunaan internet telah melahirkan berbagai *platform* yang tidak hanya sebagai media hiburan, tetapi juga sebagai sumber penghasilan. *Platform* media sosial berfungsi untuk memfasilitasi interaksi dan pengembangan kreativitas penggunanya. Oleh karena itu, media sosial dapat dilihat sebagai wadah online yang memperkuat hubungan antar pengguna serta membentuk ikatan social.

Salah satu aplikasi media sosial adalah TikTok. Aplikasi ini dikembangkan oleh perusahaan teknologi asal Cina dan diluncurkan pada bulan September 2016 [3]. TikTok adalah platform media sosial yang berfokus pada pembuatan dan berbagi video musik pendek, berdurasi 15 hingga 60 detik. Pada Juni 2021, durasi video diperpanjang menjadi 3 menit, dan kemudian hingga 10 menit pada Februari 2022. Namun, dengan popularitasnya, juga terjadi peningkatan kejahatan dunia maya, seperti pencemaran nama baik, *bullying*, dan penipuan [2].

Berdasarkan survei yang dikutip dari *We Are Social*, sebanyak 49,9 persen atau sekitar 139 juta dari total populasi Indonesia aktif menggunakan media sosial per Januari 2024. Tiktok menempati urutan ke empat seperti gambar 1.



Gambar 1. Urutan penggunaan media sosial 2024

Perkembangan sosial media saat ini banyak disalah gunakan untuk tindak kejahatan. Tindak kejahatan tersebut akan meninggalkan *history* yang dapat dijadikan barang bukti pada suatu kasus kejahatan teknologi komputer. *Digital forensik* adalah disiplin ilmu yang digunakan untuk membantu penegak hukum dalam menangani kejahatan digital. Tujuannya adalah untuk membuktikan tindak

kejahatan tersebut dan mengumpulkan bukti digital yang sah [4]. *Mobile forensics* adalah cabang dari *digital forensics*, yang lebih dikenal sebagai *komputer forensic* berkaitan dengan pemulihan bukti digital [5]. *Mobile forensics* merupakan langkah yang penting dalam menangani kejahatan digital, karena proses ini memungkinkan penemuan bukti digital yang telah dihapus dari perangkat *mobile* [6]. Analisis barang bukti digital melibatkan pengumpulan dan pembacaan data untuk mengungkapkan bukti penting. Bukti digital diperoleh dari ekstraksi data mencangkup dokumen, gmail, kontak, obrolan teks, dan file media.[7].

Penelitian ini menggunakan *Tools Mobiledit dan FTK Imager*. *Mobiledit Forensic* adalah perangkat lunak forensik digital yang dirancang untuk mengekstraksi, menganalisis, dan membuat laporan data dari perangkat seluler seperti ponsel pintar dan ponsel fitur. Menurut (Yana Safitri et al., 2022) *Mobiledit Forensic* lebih cocok digunakan untuk melakukan investigasi terhadap kasus forensika digital terhadap aplikasi *Facebook Messenger* karena langsung melakukan reporting gambar dan video sehingga tidak diperlukan tools yang lain untuk melakukan deskripsi gambar dan video [8].

Sedangkan pada *Forensic Toolkit Imager* (*FTK Imager*) adalah perangkat lunak forensik digital yang digunakan dalam penyelidikan kejahatan s*yber*. Menurut (M.Ali Diko Putra et al., 2024) Penelitian dengan menggunakan *FTK Imager* sebagai alat forensik digital untuk mengakses data yang telah dihapus pada aplikasi TikTok berbasis web. Hasil analisis menunjukkan bahwa *FTK Imager* mampu memperoleh berbagai bukti digital, termasuk informasi akun, riwayat penelusuran, dan konten visual. [9].

Penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST). Metode ini bertujuan untuk menjelaskan langkah-langkah dan alur penelitian secara sistematis serta tahapan-tahapan yang akan dilaksanakan, sehingga dapat menjadi panduan dalam menyelesaikan masalah yang dihadapi. Metode NIST terdiri dari beberapa tahap, yaitu *Collection, Examination, Analysis*, dan *Reporting* [9]. Penelitian ini merupakan kelanjutan dari penelitian-penelitian sebelumnya, seperti studi Nasirudin yang berjudul "Analisis *Forensik Smartphone* Android Menggunakan Metode NIST dan Alat *MOBILedit Forensik Express"*. Dalam penelitiannya, Nasirudin berhasil melakukan proses *recovery* data pada *smartphone* Samsung Galaxy A8 pada aplikasi telegram dengan bantuan perangkat lunak *MobiLedit Forensik Express* [1]. Selain itu, penelitian yang dilakukan oleh Irhash membahas tentang "Perbandingan Alat Forensik pada *Instagram* Menggunakan Metode NIST", pada penelitiannya Irhash berhasil melakukan pemulihan data pada *smartphone* Samsung Galaxy J2 Prime dari aplikasi *Instagram* yang telah dihapus dengan bantuan perangkat lunak *Belkasoft Evidence* dan *Magnet* Axiom [4]. Sedangkan penelitian ini menyelidiki kasus pencemaran nama baik pada aplikasi *Tiktok* dengan menggunakan *tools Mobiledit Forensik* dan *FTK Imager*. Penelitian menggunakan bantuan tools *mobiledit forensic* dan *FTK Imager* untuk menginvestigasi pencemaran nama baik di tiktok dengan memulihkan video, *hashtag*, serta pesan teks kemudian dihapus dari perangkat *smartphone* Android.

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik merupakan bidang ilmu dan teknologi komputer yang mempelajari cara memeriksa dan menganalisis bukti digital atau elektronik untuk mengungkap keterkaitannya dengan aktivitas kriminal. Berdasarkan Goel et al. (2012), terdapat empat prinsip utama dalam forensik digital yaitu:

a. Instansi hukum maupun petugas yang terlibat tidak diperbolehkan mengubah data digital yang terdapat pada media penyimpanan yang akan digunakan sebagai barang bukti di pengadilan.
b. Setiap orang yang mengakses data digital pada media penyimpanan barang bukti harus memiliki keahlian yang memadai, memahami pentingnya data tersebut, dan mempertimbangkan dampak dari tindakannya terhadap integritas barang bukti.
c. Seluruh langkah pemeriksaan yang dilakukan terhadap media penyimpanan harus dicatat secara teknis dan rinci. Hal ini bertujuan agar pihak ketiga yang melakukan investigasi ulang dapat memperoleh hasil yang sama.
d. Semua individu yang terlibat dalam investigasi bertanggung jawab sepenuhnya atas setiap tahap pemeriksaan dan analisis, serta harus memastikan bahwa seluruh proses dijalankan sesuai dengan ketentuan hukum yang berlaku [7].

2.2. *Smarphone Android*

Smartphone, yang berarti "ponsel pintar" atau "ponsel cerdas" dalam bahasa Inggris, adalah perangkat telepon seluler yang memiliki kemampuan canggih mirip dengan komputer. Menurut David Wood, Wakil Presiden Eksekutif PT Symbian OS, smartphone berbeda dari ponsel biasa berdasarkan dua hal utama, yaitu metode pembuatannya dan fitur yang dimilikinya.

Untuk sementara, Williams dan Sawyer mencirikan smartphone sebagai gadget portabel yang disiapkan dengan chip, memori, layar, dan modem internal. Smartphone adalah perangkat media interaktif yang menggabungkan kapasitas komputer dan ponsel, membuat alat canggih dengan berbagai fitur seperti pesan konten, kamera, pemutar musik, rekaman, pengalihan, akses email, TV terkomputerisasi, mesin tampilan, pengawas data individu, GPS, layanan telepon web, dan kapasitas untuk digunakan sebagai kartu kredit.

Setuju dengan Ridi Ferdianan, smartphone yang sama adalah semacam gadget serbaguna yang memiliki lebih banyak sorotan total daripada ponsel

serbaguna standar. Dalam ekspansi untuk bekerja sebagai alat komunikasi, smartphone juga dapat digunakan untuk keperluan perdagangan (bisnis) oleh pemilik media atau terbuka umum melalui asosiasi online .

Sementara itu, web dari sudut pandang keilmuan dapat dibandingkan dengan perpustakaan raksasa yang menyimpan jutaan hingga miliaran data atau informasi dalam berbagai bentuk, seperti konten, ilustrasi, suara, gerakan, dan media elektronik lainnya. Dalam hal komunikasi, internet bisa menjadi implikasi perdagangan yang sangat menarik dan mahir, baik pemisahan panjang maupun singkat, seperti dalam situasi kantor, pengajaran instruktif, dan organisasi lainnya.

Para ahli berpendapat bahwa *smartphone* adalah telepon seluler yang dilengkapi dengan perangkat menyerupai komputer dan dapat ditambahkan berbagai fitur atau aplikasi melalui koneksi internet. Dengan demikian, *smarphone* tidak hanya berfungsi sebagai alat komunikasi, tetapi juga mencakup peran sebagai media massa, media hiburan, media informasi, dan lain sebagainya, tergantung pada bagaimana pengguna memanfaatkannya [10].

2.3. *Tool FTK Imager*

FTK Imager atau *Forensic Toolkit Imager* adalah perangkat lunak forensik digital yang digunakan dalam penyelidikan kejahatan s*yber*. Alat ini melakukan akuisisi data dengan teknik live, static atau kombinasi keduanya. *FTK Imager* berfungsi mengambil, mengumpulkan dan memproses data untuk mendapatkan informasi relevan. Pemilihan metode akuisisi yang tepat mempermudah proses penyelidikan [9].

2.4. *Tool Mobiledit*

MOBILedit Forensik adalah perangkat lunak forensik digital yang dirancang untuk mengekstraksi, menganalisis, dan membuat laporan data dari perangkat seluler seperti ponsel pintar dan ponsel fitur. Alat ini memungkinkan penyidik untuk menghubungkan perangkat melalui USB, Bluetooth, Wi-Fi, atau inframerah guna mengakses berbagai data, seperti riwayat panggilan, pesan, file multimedia, data yang terhapus, informasi aplikasi, hingga lokasi GPS.

Fitur utama *MOBILedit* mencakup analisis data aplikasi tertentu (seperti percakapan dari aplikasi perpesanan), pemulihan data yang terhapus, dekripsi kata sandi pada perangkat iOS, dan pembuatan citra fisik atau logis perangkat untuk memastikan bukti tetap aman. Laporan yang dihasilkan tersedia dalam berbagai format, seperti *PDF*, *HTML*, atau *Excel*, sehingga memudahkan penggunaannya dalam investigasi resmi. *MOBILedit* banyak digunakan dalam penyelidikan hukum untuk mengakses dan menyimpan bukti secara aman, termasuk analisis mendalam pada file tersembunyi atau data cache dari perangkat yang dianalisis [7].

2.5. *Tiktok*

TikTok bisa menjadi tahap media sosial berbasis video singkat yang diuraikan untuk menampilkan substansi yang relevan dan sangat mengunci klien. Aplikasi ini memungkinkan klien untuk membuat, berbagi, dan mengamati rekaman dengan subjek yang berbeda, seperti kegembiraan, instruksi, dan data. TikTok telah berkembang pesat dan memiliki pengaruh yang patut diperhatikan dalam berbagai sudut, menghitung kesejahteraan mental, pembelajaran, dan kecenderungan sosial, terutama di kalangan anak muda dan siswa [11].

2.6. Metode NIST

Metode NIST dibagi menjadi beberapa fase. Salah satunya adalah tahap collection atau disebut pengumpulan, yaitu serangkaian tindakan mengumpulkan informasi untuk membantu proses penyidikan sekaligus mencari bukti kejahatan digital. Saat ini, data diambil dari sumber data terkait dengan tetap menjaga integritas bukti terhadap tahap modifikasi. Examination (pemrosesan data), atau pemeriksaan. Langkah ini melibatkan peninjauan data forensic yang telah dikumpulkan, baik secara otomatis maupun manual, untuk memastikan informasi yang diperoleh sesuai dengan apa yang ditemukan di tempat kejadian. Setelah memperoleh berkas atau data digital yang diperlukan dari langkah sebelumnya, dilakukan tahap Analysis (analisis temuan pemeriksaan) atau tahap penelitian. Dan Reporting, yang juga dikenal sebagai tahap pelaporan, diselesaikan setelah diperolehnya bukti digital dari prosedur pemeriksaan dan analisis temuan studi kasus, yang berfungsi sebagai bukti yang dapat diandalkan [12].

2.7. Pencemaran Nama Baik

Hukum pencemaran nama baik merupakan hukum yang melindungi individu dari pernyataan palsu yang merusak reputasi. Hukum ini menjaga privasi dan reputasi seseorang dari pencemaran nama baik [13].

Di Indonesia, kasus fitnah atau tersinggung yang terjadi melalui media sosial dapat dikenakan sanksi pidana berdasarkan beberapa undang-undang dan arahan. Pertama-tama, dalam Kitab Undang-Undang Hukum Pidana (KUHP), ada beberapa pasal yang mengatur umum dan tidak umum yang tidak dapat diatasi, seperti Pasal 310 ayat (1) dan (2), Pasal 311 ayat (1), dan Pasal 315, 317 ayat (1), dan 318 bagian (1), yang mengarahkan umum yang tidak dapat diatasi. Sementara itu, tidak biasa yang tidak dapat diatasi diarahkan dalam Pasal 134, 136, 137, dan sejumlah pasal lain yang lebih khusus. Dalam perluasan, dengan hadirnya UU ITE (UU Data dan Bursa Elektronik) No. 11 Tahun 2008 yang kemudian diperiksa kembali menjadi UU No. 19 Tahun 2016, Indonesia saat ini memiliki arah yang sah yang secara khusus mengarahkan kesalahan dunia maya. Salah satu kasus yang sering terjadi adalah kritik atau tidak dapat diatasi di media sosial [3].

3. METODE PENELITIAN

Pada penelitian ini laptop menjadi alat utama dalam penelitian ini untuk menjalankan simulasi kasus, melakukan proses forensik, dan kegiatan penelitian lainnya. Dalam simulasi pencemaran nama baik, digunakan perangkat Xiomi readmi 4 sebagai smartphone. Data dari perangkat ini akan diambil selama proses forensik. *USB connector* digunakan untuk menghubungkan smartphone ke laptop dalam proses pengambilan data. Aplikasi *TikTok versi* 37.4.4 digunakan dalam simulasi penelitian ini, sedangkan *Mobileedit* dan *FTK Imager* digunakan sebagai alat forensik untuk mengekstraksi data dari *smartphone*

Tabel 1. Alat Forensik

No	Nama	Deskripsi
1	Laptop	Lenovo, Intel(R) Core(TM) i7-7600U CPU @ 2.80GHz 2.90 GHz
2	*Smarphone*	Xiomi readmi 4
3	*USB Conektor*	Penghubung Smarphone dan Laptop
4	*Mobileedit Forensic*	Pro 7.4.1.21502 (x64)
5	*FTK Imager*	Versi 4.7.1
6	*Tiktok*	Versi 37.4.4
7	*Tiktok*	Web

3.1 Skenario Kasus

Adapun alur sekenario kasus yang dilakukan dalam penelitian ini adalah sebagai berikut:

Gambar 2. Skenario Kasus

a. Pelaku

Awal mula dari perbuatan pencemaran nama baik yang dilakukan oleh pelaku adalah bermula dari rasa tidak suka dengan korban. Pelaku membuat postingan di *Tiktok* dengan konten dan *hastag cyberbullying* atau fitnah dengan mencemarkan nama baik secara sengaja. Ketika korban telah mengetahui perbuatan pelaku, lalu pelaku berusaha langsung menghapus postingan yang berada di akun Tiktok.

b. Korban

Melihat postingan cyberbullying di akun Tiktok kemudian korban menanyakan pesan langsung kepada pelaku sebab dan akibat unggahan tersebut. Kemudian pelaku melakukan ancaman kepada korban. Korban melaporkan kepada pihak yang berwajib.

Metode penelitian yang diterapkan dalam studi ini adalah metode National *Institute of Standards and Technology* (NIST). NIST terdiri dari empat tahap dalam menangani dan menyelidiki kasus pencemaran nama baik. Tahap yang pertama adalah Pengumpulan Data *(Collection)*, dilanjutkan dengan pemeriksaan barang bukti *(Examination*), kemudian menganalisis data, dan terakhir penyusunan laporan berdasarkan hasil analisis tersebut (*Reporting*) [14]. Seperti pada gambar dibawah ini.

Gambar 3. Metode NIST

a. *Collection* adalah tahap awal dalam metode NIST, yang mencakup kegiatan seperti pengumpulan, pendokumentasian, isolasi, dan preservasi barang bukti.
b. *Examination* adalah tahap kedua yang melanjutkan tahap collection, di mana kegiatan yang dilakukan antara lain backup data dan imaging sistem, yang mendukung format gambar dan dapat digunakan dengan alat pemrosesan gambar.
c. *Analysis* adalah tahap yang mengikuti examination, menggunakan metode yang diakui secara hukum tanpa mengubah teknik untuk mendapatkan informasi yang relevan dan dapat memenuhi kebutuhan untuk pengumpulan dan pemeriksaan data.
d. *Reporting* adalah tahap terakhir setelah ketiga tahap sebelumnya, yang bertujuan untuk menyusun laporan mengenai hasil analisis. Laporan ini mencakup penjelasan tentang alat dan prosedur yang dipilih, deskripsi tindakan yang diambil, serta rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dalam bidang forensik.

4. HASIL DAN PEMBAHASAN

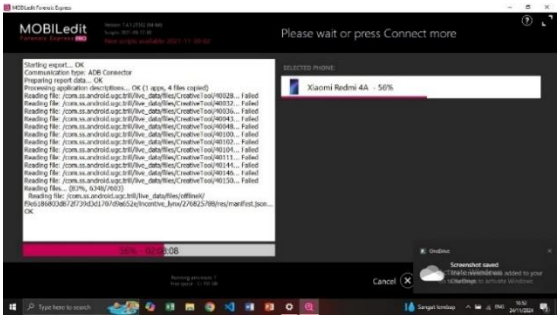
4.1 *Collection* (Tahap Pengumpulan Data)

Pada tahap *collection*, pencarian barang bukti dan pengumpulan barang bukti pada studi kasus yang telah di buat. Pada kasus ini, barang bukti yang ditemukan yaitu smarphone android Xiomi readmi 4, yang diduga menggunakan android tersebut sebagai kasus kejahatan pada aplikasi tiktok. Untuk gambar barang bukti seperti gambar dibawah ini:

Gambar 4. Barang Bukti

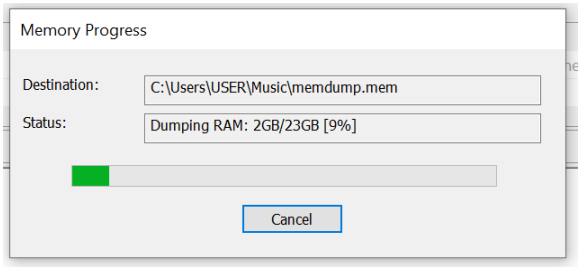
4.2 Examination (Akuisisi data)

Setelah barang bukti didapat dan diamankan, tahap selanjutnya yaitu mengakuisisi data terkait kasus yang ditangani. Pertama yang harus dilakukan pada *tools mobiledit* yaitu *smarphone* yang menjadi barang bukti dilakukan tahap *root*, tahap kedua aktifkan USB *debugging* pada *smarphone* lalu sambungkan *USB connector* dari *smarphone* ke laptop, tahap ketiga melakukan ekstraksi data pada *smarphone.* Durasi proses ekstraksi berbeda tergantung banyaknya data yang ada pada *smarphone.*



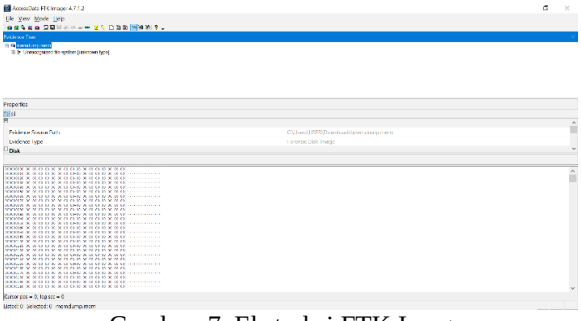
Gambar 5. Proses Ekstraksi Data oleh Mobiledit

Pada tools *FTK Imager*, membutuhkan proses pengumpulan data dari memori RAM *(Random Access Memory)* atau menangkap memory. Setelah proses pengumpulan data, dilanjutkan proses *ekstraksi* oleh *FTK Imager*.



Gambar 6. Proses Pengumpulan Data FTK Imager

Pada gambar diatas merupakan proses pengumpulan data oleh FTK Imager dengan nama memdump.mem. Setelah data dikumpulkan kemudian data tersebut di ekstraksi.

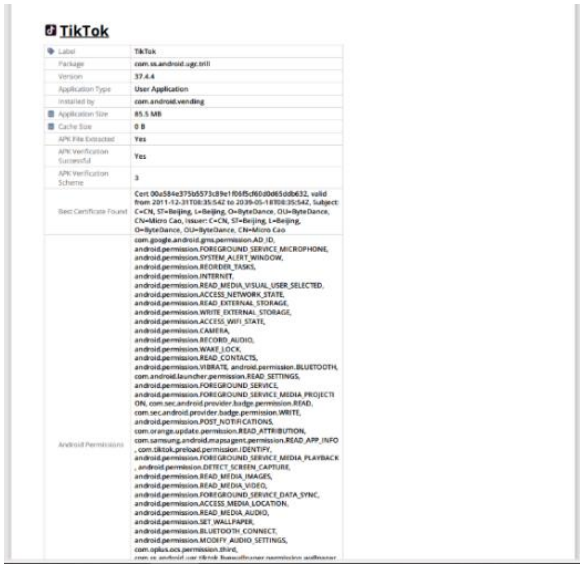


Gambar 7. Ekstraksi FTK Imager

Gambar 7 merupakan proses ekstaksi pada tools FTK imager sebelum tahap analisis. Data tersebut kemudian dianalisis untuk menemukan bukti-bukti berupa teks.

4.3 *Analysis* (Analisis Data yang di temukan)

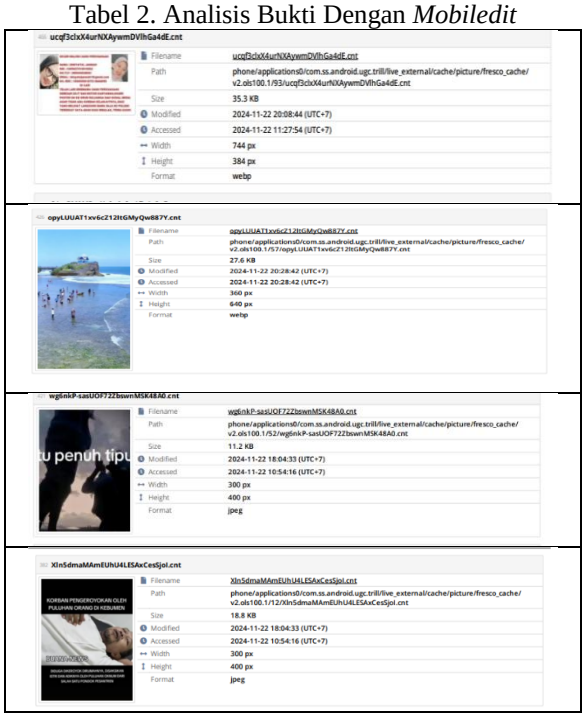
Setelah melakukan akuisisi data, kemudian dilanjutkan pada tahap analysis data yaitu hasil dari tahap examination secara rinci dari Langkah Langkah yang sudah dilakukan untuk mendapatkan barang bukti. Hasil analisis dapat dilihat pada gambar berikut:



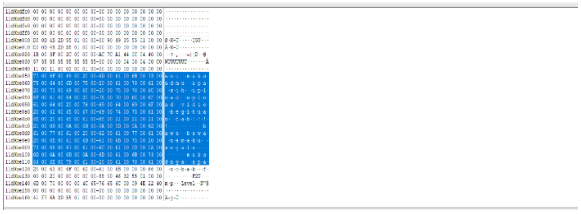
Gambar 8. Hasil Analisis Mobiledit

Pada gambar diatas terdapat informasi-informasi pelaku menggunakan akun media social tiktok. Dan ditemukannya thumbail vidio dan gambar unggahan pelaku diakun social media tiktok.

Tabel 2. Analisis Bukti Dengan *Mobiledit*



Pada tools *FTK Imager* hanya mendapatkan analisis bukti berupa teks saja baik itu bukti percakapan, komentar, maupun caption unggahan tetapi tidak menemukan bukti gambar ataupun video thumbail akun pada hasil ekstraksi. Bukti analisis seperti gambar dibawah ini:



Gambar 9. Hasil Analisis FTK Imager

Pada gambar 9, merupakan hasil dari data digital obrolan berupa teks antara pelaku dan korban pada aplikasi tiktok terlihat oleh tools FTK Imager.

4.4 *Reporting* (Pelaporan Hasil Analisa)

Setelah tahap demi tahap dilakukan, selanjutnya yaitu tahap reporting. Tahapan ini merupakan tahap terakhir dari metode NIST dilakukan pelaporan terhadap proses yang dilakukan untuk menampilkan kembali hasil pada tahap sebelumnya dan menjelaskan informasi apa saja yang ditemukan setelah melalui proses ekstraksi data dari kedua tools yang digunakan. Tahapan ini akan melaporkan hasil analisis barang bukti digital hasil ekstraksi melalui perbandingan bukti dari sekenario kasus awal yang ada hingga hasil yang didapatkan dengan tools *Mobiledit Forensik* dan *FTK Imager* dari studi kasus yang dibentuk. Dibawah ini akan disajikan tabel terkait barang bukti yang didapatkan.

Tabel 3. Tabel Analisis

Hasil Analisis Forensik dari Tools *Mobiledit* dan *FTK Imager* Aplikasi Tiktok				
No	Sumber Bukti	Data Awal	*Mobiledit Forensik*	*FTK Imager*
1	Chat	15	0	14
	Teks	14	0	14
	Gambar	1	1	1
2	Caption	3	0	3
3	Unggahan Vidio	3	3	0
4	Info Akun	1	1	0
5	Kontak	6	6	0
Jumlah Data		43	11	32

Dari tabel diatas terdapat jumlah data awal sebanyak 43 data, jumlah hasil yang didapat dari tools *mobiledit* sebanyak 11 data, dan jumlah data hasil dari tools *FTK imager* sebanyak 32 data. Untuk mendapatkan tingkat ak urasi dalam mendapatkan bukti digital digunakan analisa perbandingan dengan mencari presentase masing masing tools dalam mendapatkan bukti digital dengan rumus perhitungan sebagai berikut:

$$Pon = \frac{\Sigma Pn}{\Sigma Po}\ x\ 100\%$$

Keterangan :
Pon : Presentase Hasil Tools
ΣPn : Jumlah Hasil Data Ditemukan
ΣPo : Jumlah Data Awal

Hasil perhitugan analisis menggunakan *Mobiledit*

$$Pon = \frac{11}{43} x\ 100\% = 25\%$$

Untuk hasil perhitungan analisis tools *FTK Imager*

$$\text{Pon} = \frac{32}{43} x\ 100\% = 74{,}4\%$$

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dari pembahasan dan penelitian yang telah dilakukan pada penelitian ini yaitu "Analisis Forensik Smarphone Android pada Aplikasi Tiktok Menggunakan Metode NIST" berhasil mendapatkan bukti digital. Bukti digital yang didapatkan dari Tools *Mobiledit* berupa kontak, video, info akun, dan gambar. sedangkan *FTK Imager* hanya mendapatkan bukti berupa teks yaitu caption dan *massage*. Hasil presense dengan tools *mobiledit* sebesar 25,5 % berhasil menemukan 11 data dari 43 data awal. Dan hasil presense dengan *tools FTK Imager* sebesar 74,4% berhasil menemukan sejumlah 32 data dari 43 data awal. Dari penelitin ini, disarankan untuk mencoba menggunakan tools lain yang lebih beragam, seperti Belkasoft, XRY, atau Oxygen Forensic Suite, untuk memperluas cakupan analisis dan membandingkan hasil bukti digital yang diperoleh dari berbagai perangkat lunak.

DAFTAR PUSTAKA

[1] I. Riadi, Nasirudin, dan Sunardi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, hal. 89–94, 2020.

[2] F. Anggraini, H. Herman, dan A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 4, hal. 1117, 2022, doi: 10.30865/jurikom.v9i4.4738.

[3] T. Mulyadi, Hanna Fitri Raziah, dan Caesar Almunir Putra Semedi, "Penegakan Hukum Terhadap Tindak Pidana Penghinaan Dalam Sosial Media Platform Tiktok," *J. Rechten Ris. Huk. dan Hak Asasi Mns.*, vol. 4, no. 1, hal. 21–26, 2022, doi: 10.52005/rechten.v4i1.74.

[4] Irhash Ainur Rafiq, Imam Riadi, dan Herman, "Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 2, hal. 134–142, 2022, doi: 10.14421/jiska.2022.7.2.134-142.

[5] Y. Safitri, I. Riadi, dan S. Sunardi, "Mobile Forensic for Body Shaming Investigation Using

Association of Chief Police Officers Framework," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 3, hal. 651–664, 2023, doi: 10.30812/matrik.v22i3.2987.

[6] Elsya indah Fitria, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video," *J. Komput. Teknol. Inf. dan Sist. Inf.*, vol. 2, no. 2, hal. 390–399, 2023, doi: 10.62712/juktisi.v2i2.108.

[7] G. Fanani, I. Riadi, dan A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, hal. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[8] J. S. Komputer, I. Gilbert, R. Mailangkay, E. Zakharia, A. Hadi, dan T. Informatika, "Komparasi Analisis Bukti Digital Tiktok Lite Menggunakan Metode National Institute of," vol. 6, no. September, hal. 661–670, 2022.

[9] M. Ali Diko Putra, A. Wirawan Muhammad, B. Parga Zen, R. Yunita Kisworini, dan T. Rohayati, "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86," *J. Sist. Inf. Galuh*, vol. 2, no. 1, hal. 44–54, 2024, doi: 10.25157/jsig.v2i1.3695.

[10] M. Abidin, "Bentuk Pemanfaatan Smartphone Dalam Aktivitas Belajar Pendidikan Agama Islam Oleh Siswa Kelas XI di SMAN 7 Kota Kediri," *IAIN Kediri* , no. April, hal. 13–30, 2020.

[11] A. Regasa dan D. Lemmi Ettisa, "The Impact of TikTok on Students: A Literature Review," *Qeios*, hal. 4–11, 2023, doi: 10.32388/epfgo6.2.

[12] D. Mualfah dan R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT J. Res. Dev.*, vol. 5, no. 2, hal. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[13] E. Asmadi, "Rumusan Delik Dan Pemidanaan Bagi Tindak Pidana Pencemaran Nama Baik Di Media Sosial," *Lega Lata J. Ilmu Huk.*, vol. 6, no. 1, hal. 16–33, 2020.

[14] M. Fitriana, K. A. AR, dan J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, hal. 29, 2020, doi: 10.22373/cj.v4i1.7241.