PAPER NAME

14. MTI-60181103-fitri2.pdf

AUTHOR

Fitri Anggraini

WORD COUNT

4016 Words

CHARACTER COUNT

24849 Characters

PAGE COUNT

8 Pages

FILE SIZE

1.6MB

SUBMISSION DATE

Apr 4, 2023 12:49 PM GMT+7

REPORT DATE

Apr 4, 2023 12:50 PM GMT+7

24% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 23% Internet database
- 9% Publications database
- Crossref database
- Crossref Posted Content database
- 0% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Manually excluded sources

Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)
Vol. 10, No. 1, Februari 2023, hlm. 89-96
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019
DOI: 10.25126/jtiik.2023106416
p-ISSN: 2355-7699
e-ISSN: 2528-6579

AKUISISI BUKTI DIGITAL TIKTOK BERBASIS *ANDROID* MENGGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE*

Herman[1], Anton Yudhana[2], Fitri Anggraini*[3]

[1,2,3]Universitas Ahmad Dahlan, Yogyakarta
Email: [1]hermankaha@mti.uad.ac.id, [2]eyudhana@mti.uad.ac.id, [3*]fitri2008048047@webmil.uad.ac.id
*Penulis Korespondensi

(Naskah masuk: 12 Juli 2022, diterima untuk diterbitkan: 28 Februari 2023)

Abstrak

Seiring mudahnya menjangkau internet maka masyarakat sangat mudah menggunakan media sosial. Media sosial sangat berdampak positif bagi khalayak ramai seperti mudahnya dijangkau informasi dan mengakses perkembangan zaman, meskipun demikian tidak menutup kemungkinan media sosial dapat mendatangkan pengaruh negatif seperti tindak kejahatan *cyberbullying*, penipuan, ancaman, dan pencemaran nama baik. Aplikasi TikTok merupakan media sosial yang paling banyak diunduh menurut *We Are Social* dan *Hootsuite* pada Januari 2022 dan aplikasi TikTok rentan menyebabkan terjadinya kejahatan pencemaran nama baik, dan terjadinya ancaman. Penelitian ini bertujuan melakukan proses forensik untuk mendapatkan bukti-bukti pencemaran nama baik dan ancaman pada media sosial TikTok. Penelitian ini menggunakan *framework* dari *National Institute of Justice* (NIJ) dengan tahap *identification, collection, examination, analysis*, dan *reporting*. Tools yang digunakan dalam penelitian yaitu *MOBILedit forensic Express.* Proses forensik yang dilakukan berhasil mendapatkan data pada *smartphone* yang belum di-*root* hanya bisa mendapatkan informasi aplikasi TikTok, *images,* dan waktu kejadian dengan persantase tingkat keberhasilan 42,8%. Sedangkan pada *smartphone* yang sudah di-*root* didapatkan data berupa informasi aplikasi TikTok, nama akun, *Messanges, image*, waktu kejadian, dan video serta *hastag* tidak dapat ditemukan dengan persantase tingkat keberhasilan 85,7%.

Kata kunci: *Digital Forensic, TikTok, Android, NIJ*

ACQUISITION DIGITAL EVIDENCE TIKTOK OF ANDROID-BASED USING NATIONAL INSTITUTE OF JUSTICE METHOD

Abstract

As it is easy to reach the internet, it is very easy for people to use social media. Social media has a very positive impact on the general public such as easy access to information and access to the times, however it is possible that social media can have negative effects such as cyberbullying, fraud, threats, and defamation. The TikTok application is the most downloaded social media according to We Are Social and Hootsuite in January 2022 and the TikTok application is vulnerable to causing crimes of defamation, and threats. This study aims to conduct a forensic process to obtain evidence of defamation and threats on TikTok social media. This study uses a framework from the National Institute of Justice (NIJ) with the stages of identification, collection, examination, analysis, and reporting. The tools used in this research are MOBILedit Forensic Express. The forensic process that was carried out succeeded in obtaining data on a smartphone that had not been rooted, only being able to get information on the TikTok application, images, and the time of the incident with a success rate of 42.8%. Meanwhile, on a rooted smartphone, data in the form of TikTok application information, account names, messages, images, time of occurrence, and videos and hashtags could not be found with a success rate of 85.7%.

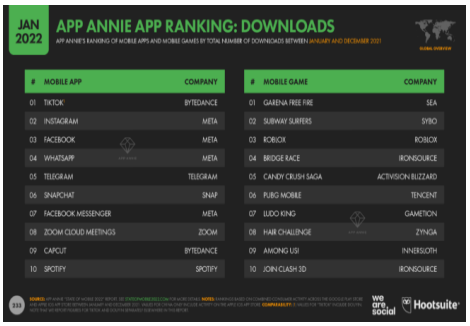
Keywords: *Digital Forensic, TikTok, Android, NIJ*

1. PENDAHULUAN

Perkembangan dunia teknologi saat ini sangat cepat, begitu juga dengan evolusi teknologi *smartphone* yang menggunakan sistem operasi *Android* dengan banyak fitur canggih (Prasongko, Yudhana, & Fadil, 2018). *Smartphone* secara perlahan mulai menggantikan peran komputer dengan meningkatkan jumlah fitur dan aplikasi yang tersedia pada perangkat *mobile* (Umar, Riadi, & Zamroni, 2018)(Riadi, Yudhana, & Putra, 2018). *Smartphone* berbasis *Android* paling populer dengan pengguna yang semakin banyak setiap tahunnya

(Riadi, Umar, & Firdonsyah, 2018)(Riadi, Yudhana & Putra, 2018). Aktivitas penggunaan *smartphone* saat ini selain digunakan untuk berkomunikasi juga digunakan untuk mencari informasi. Dengan berkembangnya teknologi informasi dan komunikasi, masyarakat kini dapat lebih mudah mendapatkan kebutuhan akan informasi (Sari, 2017)(Riadi *et al.*, 2018). Salah satu tempat mencari informasi yaitu media sosial. Media sosial yang paling banyak digemari dari kalangan anak sampai dewasa saat ini salah satunya yaitu TikTok.

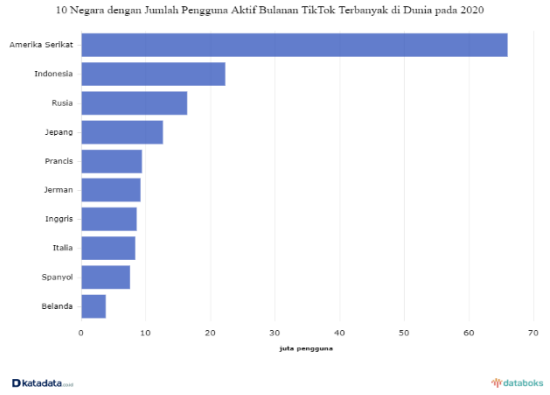
TikTok adalah salah satu media sosial yang perkembangannya paling cepat didunia dan paling banyak diunduh pada tahun 2021 seperti yang dilaporkan oleh *We Are Social* dan *Hootsuite* pada Januari 2022 ditunjukkan pada gambar 1. Pada aplikasi TikTok pengguna dapat membuat video mencapai 10 menit dengan disertai musik, filter dan berbagai fitur lainnya serta dapat mengirimkan pesan obrolan berupa pesan text. Pada aplikasi TikTok dapat mengunduh video yang diupload orang lain, atau menyimpannya ke fitur favorit serta dapat dibagikan ke beberapa media sosial lain seperti *Whatsapp, Line*, Cerita Facebook, Instagram *Story,* dan banyak lainnya.



Gambar 1. Aplikasi yang Paling Banyak di Download pada Januari 2022 menurut *We Are Social* dan *Hootsuite*

Berdasarakan lembaga statistika dan data portal (databoks, 26 Juli 2021), Indonesia merupakan negara terbanyak nomor dua pengguna aktif bulanan pada tahun 2020 yaitu 22,2 juta pengguna dan posisi pertama ditempati oleh Amerika serikat dengan jumlah 65,9 juta pengguna, sedangkan Rusia menyusul Indonesia dengan pengguna aktif bulanan 16,4 juta pengguna. Tiktok dapat digunakan sebagai sarana menggerakkan massa, iklan dan penunjukkan bakat. Jumlah pengguna Tiktok di beberapa negara disajikan pada Gambar 2.

Media sosial TikTok dapat menguntungkan bagi para pengguna dengan cara menghasilkan uang melalui *sponsored content post*, pemasukkan dari donasi atau *payout coins*, jasa jual beli akun TikTok, TikTok *marketing*, TikTok *influencer*, dan membangun agensi *influencer*. Selain berdampak positif aplikasi TikTok juga berpotensi dimanfaatkan oleh pengguna yang tidak bertanggung jawab atas kejahatan *cybercrime*.



Gambar 2. Sepuluh Negara dengan Pengguna Aktif TikTok Terbanyak di Dunia pada Tahun 2020.

Cybercrime merupakan setiap kejahatan yang dilakukan dengan menggunakan komputer atau alat komunikasi lainnya untuk menimbulkan ketakutan dan kecemasan pada orang atau merusak, merugikan, dan menghancurkan properti. *Cybercrime* memiliki dua kategori, yaitu *cybercrime* yang dibantu komputer dan yang berfokus pada komputer. Contoh *cybercrime* yang dibantu komputer adalah pornografi anak, penipuan, pencucian uang, dan penguntitan dunia maya, sedangkan contoh *cybercrime* yang berfokus pada komputer adalah peretasan, *phishing*, dan perusakan situs web (Yar & Steinmetz, 2019)(Al-Khater *et al.*, 2020).

Digital forensic adalah istilah yang digunakan secara luas, mengacu pada identifikasi, akuisisi, dan analisis bukti digital yang berasal lebih dari sekadar komputer, bisa seperti *Smartphone*, tablet, perangkat *Internet of Things*, atau data yang disimpan di *cloud* (Du, Le-Khac & Scanlon, 2017). *Digital forensic* memiliki banyak bidang, salah satunya adalah *mobile forensic* (Riadi *et al.*, 2018)(Riadi, Umar, & Firdonsyah, 2017). *Mobile forensic* adalah cabang dari digital forensik berkaitan dengan pemulihan bukti digital atau data dari perangkat *mobile* di bawah kondisi forensik suara (Yudhana, Riadi and Anshori, 2018). Bukti digital merupakan informasi elektronik yang dikumpulkan pada saat melakukan investigasi pada sebuah kasus, yang melibatkan perangkat-perangkat digital seperti *e-mail*, transaksi perbankan *online,* foto, *web histori,* maupun audio dan video (Larasati & Hidayanto, 2017). Bukti digital dapat ditemukan di *hard drive, flash drive,* telepon, *smartphone*, router, tablet, dan instrumen seperti GPS (Sadiku, Tembely, & Musa, 2017)(Riadi, Fauzan, & Sunardi, 2018).

Untuk mengangkat barang bukti digital bisa menggunakan dua metode yaitu dengan cara *dead forensics* dan *live forensics*. *Dead forensic* atau *static forensic* adalah suatu teknik yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan seperti memori dan *hardisk*. *Live forensic* adalah suatu metode untuk medapatkan barang bukti digital yang kejadiannya sedang

berlangsung atau kejadian tersebut sedang berjalan biasanya dilakukan pada *system* transit jaringan atau bisa juga pada *Random Access Memory* (RAM).

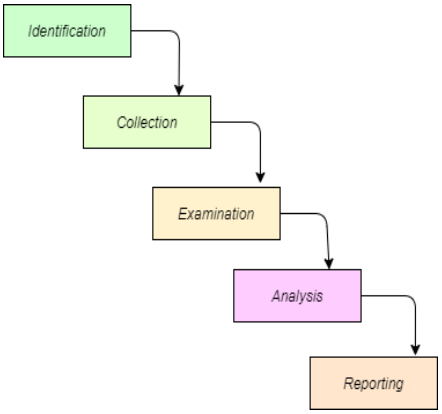
Penelitian ini melanjutkan penelitian dari Imam Riadi yang meneliti tentang akuisisi bukti digital pada Instagram *Messenger* berbasis android menggunakan metode *National Institute of Justice* (NIJ) dan tools Oxygen forensik. Penelitian tersebut menggunakan teknik simulasi. Data yang dikirimkan yaitu berupa *chatting* dan gambar/foto melalui aplikasi *Instagram Messager* yang mengandung *cyberbullying*. Penelitian tersebut berhasil mendapatkan data berupa gambar/foto dan *chatting* pada smartphone Samsung Galaxy Star GT-S5282 dalam kondisi sudah diroot, sedangkan pada *smartphone* Samsung Galaxy SM-J100H belum di-*root* tidak dapat dapat mengangkat data gambar/foto dan *chatting* tersebut (Riadi *et al.*, 2018).

Selain itu proses forensik menggunakan *framework* NIJ juga pernah dilakukan oleh Iman Riadi yang meneliti tentang forensik digital pada *Frozen Solid State Drive* (SSD). Penelitian tersebut meneliti tentang membekukan *drive SSD* menggunakan *software* pembeku *drive shadow defender* dan menggunakan teknik simulasi dengan membuat seolah-olah terjadi kejahatan komputer dengan membuat dan menyalin berbagai macam *file* dokumen *(.doc, .xls,.ppt, .pdf), file* gambar *(.jpg, .png), file* multimedia *(.mp3, .mp4)*. Proses forensik penelitian *frozen* SSD mendapatkan prosentase keberhasilan 28,7% yang diperoleh dari 85 *file* yang disimulasikan dan *file* yang berhasil direstorasi hanya 25 *file* (Riadi, Umar and Nasrulloh, 2018).

Sedangkan pada panelitian ini akan melakukan penelitian pada aplikasi TikTok menggunakan *MOBILedit forensic express* menggunakan *Framework* proses forensik dari NIJ untuk menemukan barang bukti digital berupa pencemaran nama baik dan ancaman pada aplikasi TikTok, dengan kondisi *smartphone* belum di-*root* dan sudah di-*root.* Penelitian ini dilakukan untuk memberikan rekomendasi kepada penyidik dalam meggunakan *tools* dan kondisi *smartphone* dalam mengakuisisi bukti digital pada aplikasi TikTok

2. METODE PENELITIAN

Dalam melakukan penelitian ini tentunya diperlukan sebuah metode untuk mencapai keberhasilan dari penelitian tersebut (Rahmansyah, 2021). Melakukan teknik dan analisis forensik berdasarkan prosedur yang benar akan memiliki kesuksesan mendekati 100% dalam akumulasi data forensik (Riadi, Fadlil, & Aulia, 2019). Pada penelitian ini, peneliti untuk mendapatkan barang bukti pencemaran nama baik dan ancaman pada aplikasi TikTok menggunakan *framework* proses *forensic* dari *National Institute of Justice* (NIJ) dengan tahapan *identification, collection, examination, analysis,* dan *reporting*. *Framework* forensik dapat dilihat pada Gambar 3.



Gambar 3. *Framework* Proses Forensik NIJ.

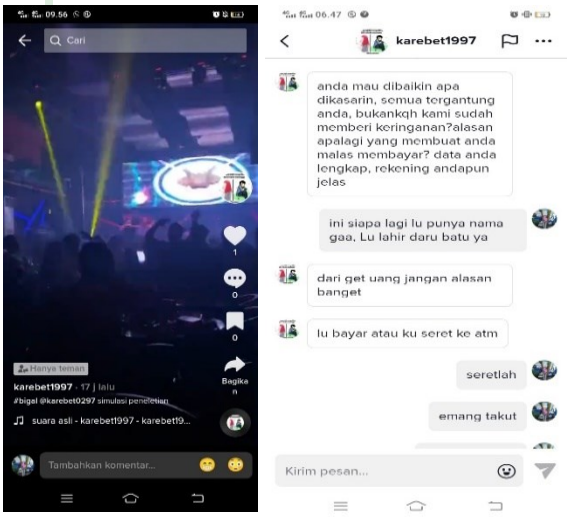
Pada Gambar 3. Merupakan Metode penelitian menggunakan *framework* forensik NIJ, memiliki lima tahapan yang dapat dijelaskan seperti berikut.

a. *Identification* yaitu proses mempersiapkan alat dan bahan yang akan digunakan dalam proses proses penyidikan.
b. *Collection* adalah proses mencari/ mengumpulkan bukti fisik barang bukti yang mengandung barang bukti elektronik.
c. *Examination* merupakan tahapan dimana proses pengambilan barang bukti elektronik dan pendokumentasian isi dan sistem, dilakukan reduksi data untuk mengidentifikasi barang bukti. Pada tahap ini penelitian yang digunakan menggunakan dua metode dalam pengambilan data barang bukti pada *smartphone*. Metode yang pertama yaitu *examination* data denga cara *smartphone* dalam kondisi tidak di-*root*, dan metode yang kedua *smartphone* yang menjadi barang bukti fisik dalam kondisi sudah di-*root*. *Rooting* adalah proses membuka akses total pada *smartphone Android* (Yudhana, Riadi, & Anshori, 2018).
d. Setelah itu dilakukan tahap *analysis* dimana proses pembuktian untuk tahap pemeriksaan guna menentukan nilai signifikansi dan probabilitas.
e. *Reporting* adalah tahapan yang dalam proses ini membuat catatan pemeriksaan semua kasus.

Penelitian ini menggunakan metode *static forensic* yaitu melakukan forensik setalah kejadian berlalu atau setelah percakapan telah selesai dan *smartphone* sudah mati.

Penelitian ini menggunakan teknik simulasi. Simulasi penelitian ini menggunakan dua skenario. Skenario yang pertama yaitu mengupload postingan video beserta *hastag* yang mencemarkan nama baik orang lain. Video tersebut di unggah oleh akun karebet 1997 yang menandai akun @karebet0297 serta memberikan *hastag* "bigal". Setelah video tersebut tersebar dan sudah dilihat oleh orang lain

maka pelaku langsung menghapus video tersebut dari *smartphone*nya. Lalu skenario yang kedua dimana pelaku mengirimkan pesan sebuah ancaman kepada korban yang mengaku dari get uang dan meminta mentransfer uang, jika tidak di transfer maka pelaku akan menyebarkan data pribadi dan foto korban. Data simulasi tersebut dapat dilihat pada Gambar 4.



4.a 4.b

Gambar 4. Simulasi Pengiriman Video (a) dan Pesan (b)

Pada Gambar 4.a merupakan skenario penelitian yang mencemarkan nama baik berupa video yang menandai akun @karebet0297 dan memberikan #bigal, serta Gambar 4.b merupakan skenario penelitian berupa ancaman dimana pelaku mengaku dari get uang dan mengancam ingin menyebarkan data pribadi. Proses forensik yang dilakukan dalam penelitian ini bertujuan untuk mendapatkan kembali data-data yang disimulasikan, yaitu data video berserta *hastag* yang di-*upload* pada skenario pertama dan data pesan ancaman yang dikirim pada skenario kedua. Dimana dalam simulasi ini data-data tersebut telah dihapus oleh pelaku dari *smartphone* yang kemudian dijadikan sebagai barang bukti. Proses forensik dilanjutkan dengan analisis terhadap data video, *hastag,* pesan-pesan, dan data lain yang berhasil didapatkan kembali selama proses forensik. Analisis berupaya menggali informasi tambahan, berupa detail *metadata video*, detail waktu kejadian, detail akun TikTok yang digunakan, dan kecocokan *hardware/software* yang dijadikan barang bukti dengan yang sebenarnya digunakan pada waktu simulasi.

Pada penelitian ini mengguanakan *tools* MOBILedit Forensic Express untuk membantu penyidik menemukan barang barang bukti digital berupa pencemaran nama baik dan ancaman. MOBILedit Forensic Express merupakan perangkat lunak yang digunakan untuk melakukan ekstraksi, analisis data, dan membuat laporan hasil ekstraksi data pada *smartphone* (Anshori *et al.*, 2021).

3. HASIL DAN PEMBAHASAN

3.1. *Identification* (Persiapan)

Tahap persiapan ini merupakan tahap mempersiapkan alat-alat dan bahan-bahan yang akan digunakan oleh penyidik untuk melakukan proses investigasi forensik. Alat dan bahan yang digunakan pada penelitian ini dapat dilihat pada Tabel 1.

Tabel 2. Alat dan Bahan

Nama	Spesifikasi
Laptop	Thinkpad, Intel(R) Core (TM) i5, Windows 10, 64 Bit
Smartphone	Samsung Galaxy Tab A8 SM-P355
USB *Connector*	Penghubung *Smartphone* dan Laptop
Aplikasi Tiktok	Objek Penelitian Versi 23.3.2
MOBILedit Forensic Express	*Tool forensic* Versi 7.2.0.17975

2. *Collection* (Koleksi)

Pada tahap ini adalah melakukan pengumpulan bukti fisik, pengumpulan data, dan dokumentasi bukti fisik dalam bentuk *smartphone.* Pada tahap skenario, penelitian ini menggunakan *Smartphone* Samsung Galaxy Tab A8 SM-P355 versi android 7.1.1. Barang bukti dapat dilihat pada Gambar 5.

Gambar 5. Spesifikasi *Smartphone* yang Menjadi Barang Bukti

Pada Gambar 5 merupakan *smartpnone android* yang digunakan dalam penelitian ini. *Smartphone* tersebut telah terinstal aplikasi TikTok yang merupakan alat pencemaran nama baik berupa postingan video beserta *hastag* dan *Messages* sebagai alat komunikasi yang digunakan untuk melakukan ancaman. Data yang terdapat pada *smartphone Android* akan diambil dengan cara dikloning untuk mehindari perubahan data atau penghapusan data yang akan menjadi barang bukti digital, untuk melakukan kloning akan menggunakan *tools* MOBILedit Forensic Express.

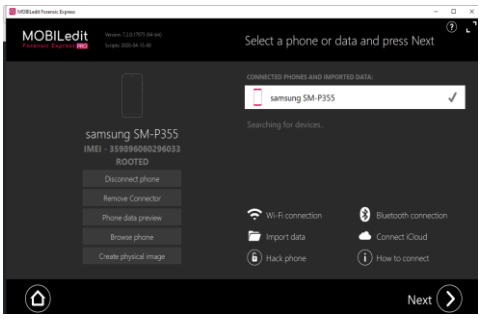
3.3. *Examination* (Pemeriksaan)

Pada tahap *examination* ini malakukan pengujian pada *software* aplikasi TikTok dengan menggunakan *tools forensic*. Tahap *examination* ini mengekstraksi data dan *imaging* data yang dilakukan pada sistem yang menggunakan alat *tools forensic* (Bintang, Umar & Yudhana, 2020).

Pada penelitian ini untuk mendapatkan barang bukti digital, *smartphone* yang menjadi barang bukti akan diambil datanya menggunakan *tools*

MOBILedit forensik express dengan kondisi *smartphone* di *root* dan tidak di-*root,* hal tersebut dilakukan untuk membandingkan tingkat keberhasilan dari kedua proses dan memilih proses mana yang terbaik untuk digunakan dalam mengangkat data aplikasi TikTok.

Langkah pertama dalam proses akuisisi data yaitu barang bukti elektronik berupa *smartphone* Samsung Galaxy Tab A SM-P355. Akusisi pertama dilakukan ketika smartphone belum di-root danyang kedua setelah di-*root.* Proses akuisisi dimulai dengan menghubungkan *smartphone* dan Laptop yang telah terinstal aplikasi MOBILedit Forensic Express menggunakan USB *connector* untuk menyambungkan perangkat, lalu aktifkan mode *USB Debugging* pada *smartphone* yang menjadi barang bukti. Proses akuisisi data menggunakan aplikasi MOBILedit Forensic Express dapat dilihat pada Gambar 6.



Gambar 6. Smartphone Samsung Galaxy Tab A SM-P355 Terkoneksi dengan MOBILedit Forensic Express

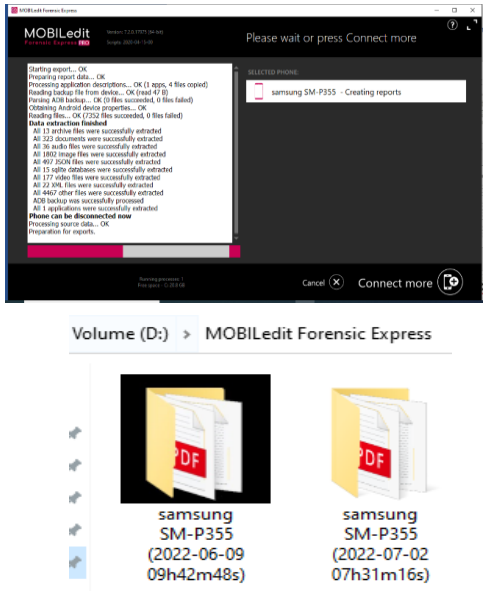
Setelah terhubung dan telah terkoneksi dengan aplikasi MOBILedit forensic express tahapan selanjutnya melakukan proses ekstraksi atau akuisisi data dengan MOBILedit forensic express. Proses ekstraksi dapat dilihat pada gambar 7.

Pada Gambar 7 merupakan proses ekstraksi dan data-data yang didapatkan disimpan dalam bentuk folder.

3.4. *Analysis* (Analisis)

Tahapan ini melakukan analisis terhadap hasil yang sudah didapatkan dari proses *examination* pada barang bukti elektronik *smartphone* Samsung Galaxy Tab A SM-P355 yang belum di-*root* maupun yang sudah di-*root*.

Dari proses analisis hasil pengambilan data-data dari TikTok menggunakan MOBILedit Forensic Express pada *smartphone* Samsung Galaxy Tab A SM-P355 yang belum di-*root* hanya bisa mendapatkan data berupa informasi aplikasi TikTok dan *image* seperti yang di tunjukkan pada Gambar 8 dan 11. Sedangkan pada *smartphone* Samsung Galaxy Tab A SM-P355 yang sudah di-*root* mendapatkan data berupa informasi aplikasi, nama akun, *messages, image*, Video serta waktu kejadian.

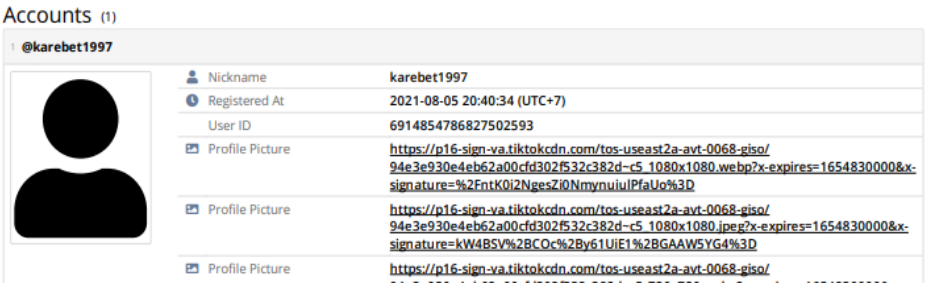


Gambar 7. Tampilan Ekstraksi menggunakan Tools MOBILedit Forensik Express

Hasil analisis yang didapatkan dapat dilihat pada Gambar 8 berupa informasi aplikasi TikTok, Gambar 9 nama akun pengguna TikTok, Gambar 10 hasil analisis *Messages*, Gambar 11 hasil analisis *image*, dan video di tunjukkan pada Gambar 12.

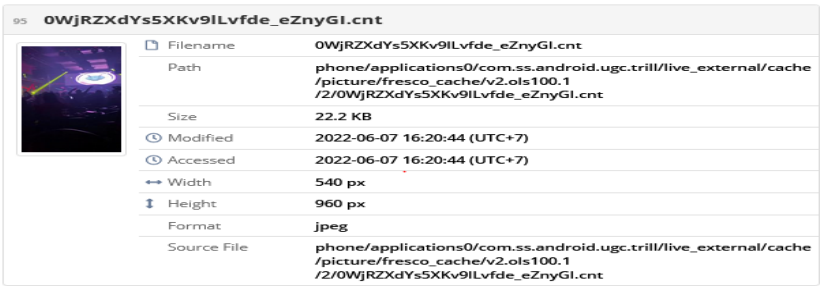
Gambar 8. Informasi Aplikasi TikTok

Pada Gambar 8 merupakan informasi aplikasi TikTok yang didapatkan dari *smartphone* yang menjadi barang bukti fisik seperti yang dibahas pada tahap simulasi. Data tersebut bisa diangkat baik dalam kondisi *smartphone* belum di-*root* maupun sudah di-*root*.



Gambar 9. Informasi Nama Akun Pengguna Tiktok

Gambar 10. Bukti Digital *Messages*



Gambar 11. Bukti Digital Gambar

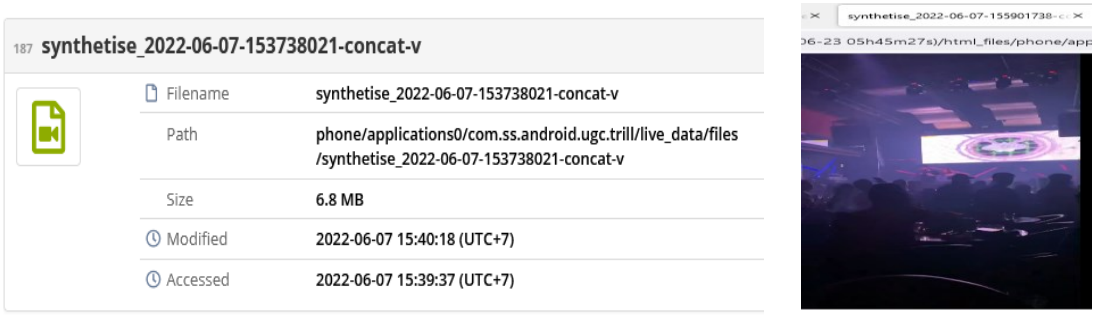
Pada Gambar 9 menampilkan informasi nama akun pengguna TikTok yaitu karebet1997 yang telah terinstall pada *Smartphone* Samsung Galaxy Tab A SM-P355. Data akun tersebut hanya bisa diangkat jika *smartphone* dalam keadaan di-*root*.

Hasil data *messages* beserta waktu kejadian yang berhasil didapatkan dari aplikasi TikTok yang terpasang pada *smartphone* Samsung Galaxy Tab A SM-P355, yang dapat diangkat jika kondisi *smartphone* sudah di-*root*.

Hasil tersebut menunjukkan telah terjadinya sebuah percakapan yang mengandung ancaman pada fitur TikTok obrolan, dapat terlihat jelas pada pada Gambar 10. Pada Gambar 11 menunjukkan hasil analisis berupa *image tumbnail* video pencemaran nama baik seperti yang disimulasikan. Data tersebut berhasil diangkat meskipun *smartphone* dalam kondisi tidak di-*root*.

Pada Gambar 12 menunjukkan hasil analisis video sama persis dengan skenario yang telah dibuat, namun *hastag* dari video yang diupload tidak dapat diangkat datanya, video tersebut hanya bisa diangkat jika *smartphone* dalam kondisi sudah di-*root*.

Dari hasil data-data keseluruhan yang telah didapatkan dari *smartphone* Samsung Galaxy Tab A SM-P355 didapatkan data-data berupa informasi aplikasi, akun pengguna, *messages, image*, video dan waktu kejadian serta *hastag* dari video yan diposting tidak dapat diangkat. Maka dari hasil data tersebut akan dikumpulkan untuk dijadikan barang bukti digital untuk kasus yang berindikasikan tindak kejahatan berupa ancaman dan pencemaran nama baik dengan menggunakan sosial media TikTok sebagai tempat melakukan tindak kejahatan.



Gambar 12. Bukti Digital Video

3.5. *Reporting* (Pelaporan)

Tahap *reporting* merupakan tahap membuatkan laporan data apa saja yang berhasil diangkat pada proses *examination* dan ditemukan pada tahap analisis. Penelitian tersebut dilakukan pada *smartphone* Samsung Galaxy Tab A SM-P355 yang belum di-*root* dan setelah di-*root,* yang menyangkut pencemaran nama baik dan ancaman berdasarakan data yang disimulasikan menggunakan *framework* NIJ, *tools* MOBILedit Forensic Express pada aplikasi TikTok. *Reporting* tersebut dapat dilihat pada Tabel 2.

Tabel 2. Laporan Hasil Simulasi Pengiriman Video dan Pesan

Bukti digital	Smartphone belum di-*root*	Smartphone sudah di-*root*
Informasi Aplikasi TikTok	√	√
Nama Akun	X	√
Messages	X	√
Image	√	√
Video	X	√
Hastag	X	X
Waktu Kejadian	√	√
Jumlah	3	6

Perbandingan hasil yang didapatkan untuk mengembalikan data dari *smartphone* Samsung Galaxy Tab A SM-P355 dalam kondisi belum di-*root* dan setelah di-*root* untuk mengetahui tingkat persentase keberhasilan yang paling baik. Menggunakan rumus seperti pada Pers. (1)

$$\frac{X}{y} * 100 \ (persen) = n \qquad (1)$$

Keterangan:
X= jumlah data yang berhasil didapatkan
Y= jumlah keseluruhan barang bukti
N= persentase yang didapatkan

Perhitungan pada *smartphone* Samsung Galaxy Tab A SM-P355 belum di *root* $= \frac{3}{7} * 100 = 42{,}8\%$

Perhitungan pada *smartphone* Samsung Galaxy Tab A SM-P355 sudah di *root* $= \frac{6}{7} * 100 = 85{,}7\%$

Dari perhitungan tersebut dapat dilihat bahwa barang bukti yang didapatkan pada *smartphone* yang belum di *root* mendapatkan persentase tingkat keberhasilan 42,8%, sedangkan pada *smartphone* Samsung Galaxy Tab A SM-P355 yang sudah di *root* sebesar 85,7%.

4. KESIMPULAN

Penelitian yang telah dilakukan dengan proses forensik menggunakan *framework National Institute of Justice* (NIJ) dan *tools* forensik MOBILedit Forensic Express dapat digunakan dalam proses ekstraksi bukti digital pada aplikasi TikTok yang terpasang pada perangkat *smartphone* Samsung Galaxy Tab A SM-P355.

Penelitian yang menggunakan *smartphone* Samsung Galaxy Tab A SM-P355 dalam kondisi belum di-*root* berhasil mendapatkan data berupa informasi aplikasi, *image* dan waktu kejadian, penelitian dengan *metode* ini mendapatkan tingkat kesuksesan dalam mengangkat barang bukti digital hanya 42,7%. Sedangkan dalam kondisi sudah di-*root berhasil* mendapatkan data berupa informasi aplikasi, akun, *conversations*, *messages, image*, video dan waktu kejadian yang menyangkut dengan simulasi kasus pencemaran nama baik dan ancaman. Proses forensik tersebut mendapatkan tingkat keberhasilan 85,7%.

Dapat disimpulkan dalam penelitian ini bahwa untuk mendapatkan barang bukti digital aplikasi TikTok, metode yang lebih baik untuk melakukan proses forensik yaitu menggunakan *smartphone* yang sudah di-*root*, karena setelah di-*root* maka semua akses *smartphone android* terbuka total.

Penelitian ini membuka beberapa peluang untuk penelitian lanjutan *(future research)* terutama berkaitan dengan pengujian data-data yang lebih variatif, baik dalam hal jenis data, ukuran file, durasi video, dan sebagainya. Proses forensik dengan kerangka yang sama dengan penelitian ini juga bisa dikembangkan lagi dengan menggunakan *forensic tools* yang berbeda-beda untuk mendapatkan bukti digital yang lebih baik lagi.

DAFTAR PUSTAKA

AL-KHATER, W.A. *ET AL.* 2020. Comprehensive review of cybercrime detection techniques, *IEEE Access*, 8, pp. 137293–137311. doi:10.1109/ACCESS.2020.3011259.

ANSHORI, I. *ET AL.* 2021. Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada

Smartphone Android Menggunakan Metode NIJ. *IT Journal Research and Development (ITJRD)*, 5(2), pp. 118–134.

BINTANG, R.A., UMAR, R. & YUDHANA, A. 2020. Analisis Media Sosial Facebook Lite dengan tools Forensik menggunakan Metode NIST. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, 21(2), p. 125. doi:10.30595/techno.v21i2.8494.

DU, X., LE-KHAC, N.A. & SCANLON, M. 2017. Evaluation of digital forensic process models with respect to digital forensics as a service. *European Conference on Information Warfare and Security, ECCWS*, (May), pp. 573–581.

LARASATI, T.D. & HIDAYANTO, B.C. 2017. Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10. *Sesindo*, 6(November), pp. 456–256.

PRASONGKO, R.Y., YUDHANA, A. & FADIL, A. 2018. Analisa forensik aplikasi kakaotalk menggunakan metode national institute standard technology. *Seminar Nasional Informatika 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 November 2018 ISSN: 1979-2328*, 2018(November), pp. 129–133.

RAHMANSYAH, R. 2021. Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook Dan Instagram Dengan Metode NIST. *Cyber Security dan Forensik Digital*, 4(1), pp. 49–57. doi:10.14421/csecurity.2021.4.1.2421.

RIADI, I. *ET AL.* 2018. Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Teknik Informatika dan Sistem Informasi*, 4, pp. 219–227.

RIADI, I., FADLIL, A. & AULIA, M.I. 2019. Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ). *Jurnal Teknik Informatika dan Sistem Informasi (JuTISI)*, 8(3), pp. 107–118.

RIADI, I., FAUZAN, A. & SUNARDI, S. 2018. Examination of Digital Evidence on Android-based LINE Messenger. *International Journal of Cyber-Security and Digital Forensics*, 7(3), pp. 336–343. doi:10.17781/p002472.

RIADI, I., UMAR, R. & FIRDONSYAH, A. 2017. Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security*, 15(5), pp. 155–160. Available at: https://www.researchgate.net/publication/317620078.

RIADI, I., UMAR, R. & FIRDONSYAH, A. 2018. Forensic tools performance analysis on android-based blackberry messenger using NIST measurements. *International Journal of Electrical and Computer Engineering*, 8(5), pp. 3991–4003. doi:10.11591/ijece.v8i5.pp3991-4003.

RIADI, I., UMAR, R. & NASRULLOH, I.M. 2018. Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ). *Elinvo (Electronics, Informatics, and Vocational Education)*, 3(1), pp. 70–82. doi:10.21831/elinvo.v3i1.19308.

RIADI, I., YUDHANA, A. & PUTRA, M.C.F. 2018. Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal of Informatics*, 5(2), pp. 235–247. doi:10.15294/sji.v5i2.16545.

SADIKU, M.N.O., TEMBELY, M. & MUSA, S.M. 2017. Digital Forensics. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), pp. 274–276.

SARI, M.P. 2017. Fenomena Penggunaan Media Sosial Instagram Sebagai Komunikasi Pembelajaran Agama Islam Oleh Mahasiswa Fisip Universitas Riau. *Fenomena Penggunan Media Sosial Instagram Sebagai Komunikasi Pembelajaran Agama Islam Oleh Mahasiswa Fisip Universitas Riau*, 53(9), pp. 1–13.

UMAR, R., RIADI, I. & ZAMRONI, G.M. 2018. Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*, 8(3), pp. 949–955. doi:10.18517/ijaseit.8.3.3591.

YAR, M. & STEINMETZ, KEVIN F. 2019. Cybercrime and Society. in. Newbury Park, CA, USA: Sage.

YUDHANA, A., RIADI, I. & ANSHORI, I. 2018. Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 3(1), pp. 13–21. doi:10.25299/itjrd.2018.vol3(1).1658.

24% Overall Similarity

Top sources found in the following databases:

- 23% Internet database
- Crossref database
- 0% Submitted Works database
- 9% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	journal.maranatha.edu Internet	5%
2	journal.uir.ac.id Internet	3%
3	journal.uny.ac.id Internet	2%
4	download.garuda.ristekdikti.go.id Internet	1%
5	jurnal.upnyk.ac.id Internet	1%
6	publishing-widyagama.ac.id Internet	1%
7	pdfs.semanticscholar.org Internet	1%
8	amikhass.ac.id Internet	1%

9	repository.its.ac.id Internet	<1%
10	dspace.uii.ac.id Internet	<1%
11	123dok.com Internet	<1%
12	jurnalnasional.ump.ac.id Internet	<1%
13	ejournal.uin-suka.ac.id Internet	<1%
14	ojs.stmik-banjarbaru.ac.id Internet	<1%
15	repository.ittelkom-pwt.ac.id Internet	<1%
16	Soni Soni, Regiolina Hayami, Muhammad Hamadi. "Akuisisi Bukti Digit... Crossref	<1%
17	eprints.uad.ac.id Internet	<1%
18	reportshop.co.kr Internet	<1%
19	id.scribd.com Internet	<1%
20	digilib.unila.ac.id Internet	<1%

21	immasangadji.wordpress.com Internet	<1%
22	jom.unpak.ac.id Internet	<1%
23	journal.ittelkom-pwt.ac.id Internet	<1%
24	Pritts, Nathan; McCollough, Christopher; Bessette, Lee Skallerup; Leo, ... Publication	<1%
25	comunitateadepractica.ase.ro Internet	<1%
26	ejournal.unkhair.ac.id Internet	<1%
27	klik.ulm.ac.id Internet	<1%
28	tabloidmitra.com Internet	<1%
29	"Proceedings of Sixth International Congress on Information and Com... Crossref	<1%
30	Takdir Ruslan, Imam Riadi, Sunardi Sunardi. "FORENSIK MULTIMEDIA ... Crossref	<1%
31	publikasi.mercubuana.ac.id Internet	<1%

Excluded from Similarity Report

- Bibliographic material
- Cited material
- Quoted material
- Manually excluded sources

EXCLUDED SOURCES

jtiik.ub.ac.id Internet	97%
researchgate.net Internet	12%
ejurnal.stmik-budidarma.ac.id Internet	7%