PAPER NAME

13. MTI-60181103-fitri1.pdf

AUTHOR

Fitri Anggraini

WORD COUNT

4238 Words

CHARACTER COUNT

25147 Characters

PAGE COUNT

11 Pages

FILE SIZE

917.6KB

SUBMISSION DATE

Apr 4, 2023 12:45 PM GMT+7

REPORT DATE

Apr 4, 2023 12:46 PM GMT+7

24% Overall Similarity

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

- 17% Internet database
- 14% 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

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers

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

[1,2]Program Studi Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1*]fitri2008048047@webmil.uad.ac.id, [2]hermankaha@mti.uad.ac.id, [3]eyudhana@mti.uad.ac.id
Email Penulis Korespondensi: fitri2008048047@webmil.uad.ac.id
Submitted **25-08-2022**; Accepted **30-08-2022**; Published **30-08-2022**

Abstrak

TikTok Merupakan aplikasi media sosial favorit yang menempati urutan keenam di dunia pada Januari 2022 menurut We Are Media & Hootsuite. Seiring dengan semakin banyaknya penggunaan aplikasi ini, semakin meningkat pula dampak negatif yang ditimbulkannya, mulai dari penipuan, cyberbullying, hingga penyebaran berita bohong (hoax). Penelitian ini fokus pada dampak negatif dalam hal pencemaran nama baik. Tujuan dari penelitian adalah merencanakan dan menerapkan sebuah proses forensik digital menggunakan kerangka Association of Chief Police Officers (ACPO) untuk mengangkat barang bukti kasus pencemaran nama baik pada aplikasi TikTok. Proses forensik tersebut dijalankan dalam bentuk static forensics terhadap kasus yang sengaja dibuat dalam bentuk simulasi postingan TikTok menggunakan smartphone android. Penelitian ini mengkombinasikan forensics framework ACPO dengan forensics tools Magnet Axiom. Kombinasi keduanya berhasil mengangkat 77% barang bukti berupa data messages, video, dan hashtag. Dimana data-data ini sudah didefinisikan sebelumnya sebagai data awal yang diposting pada proses simulasi.

Kata Kunci: Forensik; Aplikasi TikTok; Smartphone; Android; ACPO

Abstract

TikTok is the most popular social media app that ranks sixth in the world in January 2022 according to We Are Media & Hootsuite. Along with the increasing number of uses of the application, the negative impacts it causes are also increasing, ranging from fraud, cyberbullying, to the spread of fake news (hoax). This study focuses on the negative impact of defamation. The purpose of the research is to plan and implement a digital forensics process using the Association of Chief Police Officers (ACPO) framework to raise evidence of defamation cases on the TikTok application. The forensic process is carried out in the form of static forensics on cases that are intentionally made in the form of simulating TikTok postings using an android smartphone. This research combines the ACPO forensics framework with the Magnet Axiom forensics tools. The combination of the two succeeded in raising 77% of evidence in the form of data messages, videos, and hashtags. Where these data have been previously defined as initial data posted in the simulation process.

Keywords: Forensic; TikTok Application; Smartphone; Android; ACPO

1. PENDAHULUAN

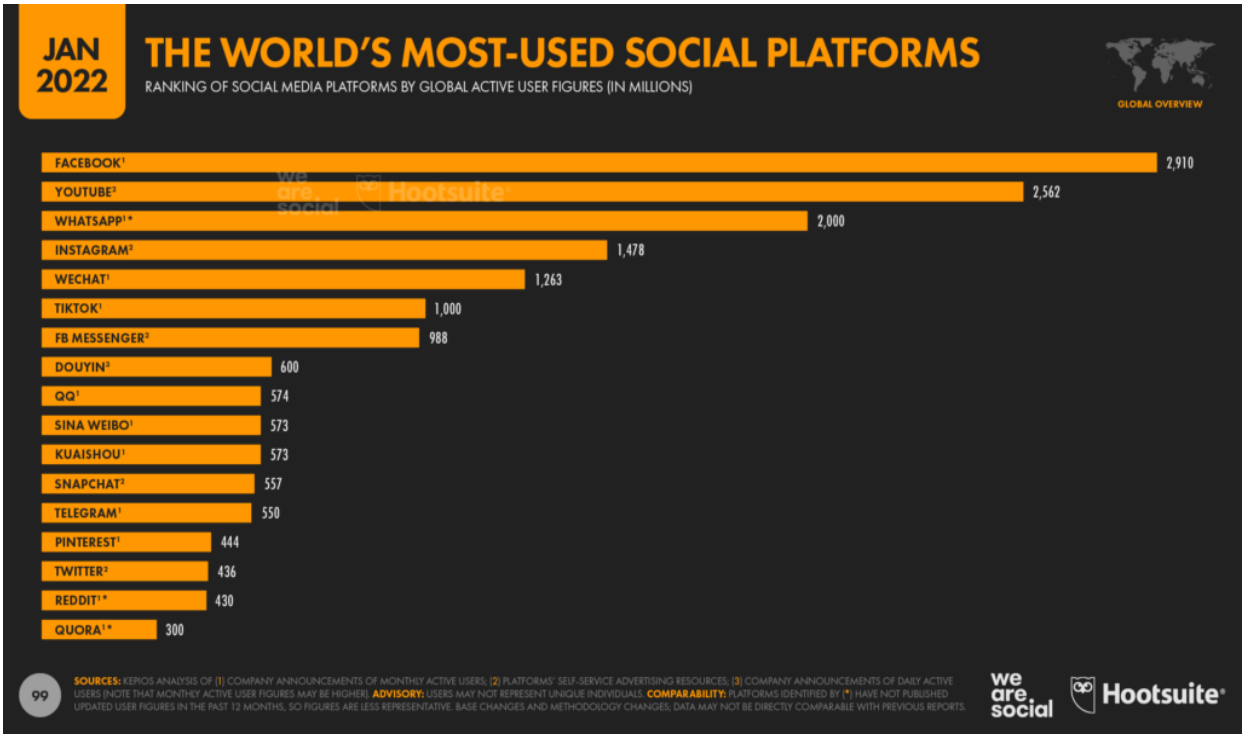
Perangkat seluler mengalami perkembangan yang sangat pesat seiring dengan perkembangan teknologi [1][2]. Salah satu teknologi dengan jumlah pengguna yang terbanyak adalah *smartphone* berbasis *Android* sebagai sistem operasinya [3][4]. Dampak negatif perkembangan *smartphone* terhadap pengguna terkait dengan pencurian dan penghapusan data untuk menghilangkan barang bukti kejahatan yang dilakukan pelaku. Barang bukti digital ini dapat berupa data pada *smartphone* seperti detail kontak, *log* panggilan, pesan, video, gambar, file dokumen, dll yang digunakan sebagai alat bukti kejahatan di pengadilan [5][2].

Kejahatan dunia maya semakin meningkat setiap tahunnya [6][7]. Jejaring sosial TikTok telah menjadi penghubung komunikasi antar manusia di dunia maya. Pertumbuhan media sosial dan aplikasi pesan instan telah mempermudah perkembangan banyak kejahatan duni maya yang serius [4][6].

TikTok adalah media sosial yang berpusat pada pembuatan dan berbagi video berbasis musik. Videonya sangat pendek, dengan durasi mulai dari 15 detik sampai 60 detik untuk mencapai kesuksesannya video harus dibuat lucu serta menarik [8][9]. Perkembangan terbaru pada Juni 2021 aplikasi TikTok melakukan pengembangan pada durasi video karena durasi video yang sebelumya dianggap terlalu pendek hanya 60 detik lalu di update menjadi 3 menit. Namun tidak lama kemudian TikTok meluncurkan pengembangan terbaru pada Februari 2022 dan durasi video dapat dibuat hingga 10 menit. Semakin digemarinya media sosial maka akan meningkatnya kejahatan dunia maya seperti pencemaran nama baik, *bullying*, penipuan dan banyak lainnya.

TikTok merupakan media social *favorit* yang menempati urutan ke enam menurut *We Are Social and Hootsuite* pada Januari 2022. Seperti pada Gambar 1.

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom



Gambar 1. Data media sosial favorit pada bulan Januari 2022

Pada bidang teknologi, analisa forensik terhadap barang bukti digital atau elektronik disebut dengan sebutan komputer forensik atau *digital forensic* [10][11]. *Digital Forensic* adalah teknologi komputer yang digunakan untuk memperoleh bukti hukum (*pro justice*) dengan membuktikan kejahatan menggunakan teknologi canggih atau komputer dan memerangi penjahat menggunakan bukti digital [12][13][14]. Mobile forensik adalah cabang dari *digital forensic* berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile di bawah kondisi forensik suara [15][16]. Analisa barang bukti digital meliputi pengumpulan data digital penting dan pembacaan bukti digital [17][16]. Bukti digital adalah hasil ekstraksi atau pemulihan seperti dokumen, akun email, kontak, obrolan text, file media (suara/gambar/video) atau *file log* [12].

Proses penyidikan untuk kejahatan *cyber* memerlukan *framework* forensik agar proses penyidikan lebih efisien dan efektif. Berikut beberapa *framework* yang digunakan oleh beberapa peneliti antara lain; penelitian yang dilakukan oleh Feryan dan Yudi menggunakan *framework National Institute of Standards and Technology* (NIST) yang melakukan pengujian dan analisa forensik terhadap aplikasi *signal messenger* berbasis *android*. Penelitian ini menggunakan skenario pemasangan aplikasi *signal messenger* pada *smartphone* kemudian dilakukan komunikasi antar kedua *smartphone* seperti mengirim pesan teks, gambar dan video [18].

Penelitian yang dilakukan oleh Soni, Yulia, dan Rizki yang menggunakan *framework National Institute of Justice* (NIJ) yang melakukan penelitian untuk mengungkap kasus pesan *chat* yang dihapus menggunakan *tools FTK Imager*, *Mobiledit Forensic*, dan *Oxygen Forensic SQLite Viewer*. Pada penelitian ini berhasil menemukan data *chating* dan gambar yang telah dihapus dari perangkat *smartphone* pelaku [19].

Penelitian dari Anton, Imam, dan Ikhsan menggunakan *framework* proses forensik dari *Digital Forensics Research Workshop* (DFRWS) melakukan penelitian pada keamanan aplikasi Twitter menggunakan *tools FTK Imager*, penelitian ini menggunakan teknik *live forensics* [6].

Serta penelitian yang dilakukan oleh Muhammad, Wicaksono, dan Rahayu yang menggunakan *framework Association of Chief Police Officers* (ACPO) pada aplikasi *instant messanging Skype*, telegram, dan *Whatsapp*. Penelitian tersebut menggunakan *tools FTK Imager* dan *fiddler* [20].

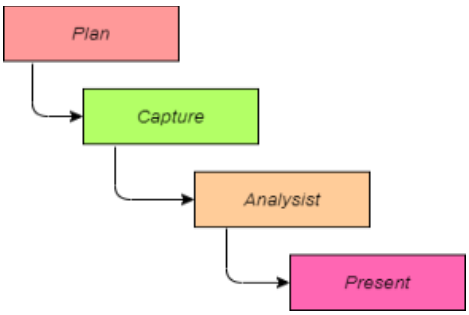
Penelitian ini merupakan lanjutan dari beberapa penelitian sebelumnya seperti penelitian Nasirudin yang berjudul "Analisis Forensik *Smartphone Android* Menggunakan Metode NIST dan *Tool* MOBILedit Forensic Express". Penelitian ini melakukan pengembalian data pada *smartphone* Samsung Galaxy A8 menggunakan MOBILedit Forensic Express [21]. Selain itu penelitian dari Irhash yang meneliti tentang "Perbandingan *Forensic Tools* pada Instagram Menggunakan Metode NIST" penelitian ini melakukan pengembalian data dari aplikasi Instagram yang sudah dihapus pada *smartphone* Samsung Galaxy J2 Prime [3]. Sedangkan penelitian ini berfokus pada aplikasi TikTok dangan *tools* Magnet Axiom. Pada penelitian ini melakukan investigasi dengan mengembalikan bukti digital berupa pencemaran nama baik yang sudah dihapus berupa video, *hastag* dari video yang diposting, dan pesan teks yang sebelumnya sudah di-*upload* pada aplikasi TikTok lalu dihapus kembali dari perangkat *smartphone Android*.

2. METODOLOGI PENELITIAN

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

2.1 Tahapan Penelitian

Metode dan tahapan proses forensik digital telah banyak dikembangkan oleh penyidik dan praktisi forensik [22][23]. Penerapan metode yang tepat dalam mengumpulkan data forensik akan memberikan dampak keberhasilan hingga 100% [24][25]. Penelitian ini mengunakan metode yang mengaplikasikan *framework* proses forensik *Association of Chief Police Officers* (ACPO) dengan tahapan *Plan, Capture, Analysist* dan *Present* pada aplikasi TikTok dimana kasusnya adalah pencemaran nama baik. *framework* proses forensik ACPO dapat dilihat pada gambar 2.



Gambar 2. *Framework* proses forensik ACPO

Pada Gambar 2 dapat diketahui *framework* proses forensik *Association of Chief Police Officers* (ACPO) memiliki beberapa tahapan. Tapahan kerangka kerja tersebut dapat diuraikan sebagai berikut.

a. *Plan* merupakan tahap merancang tentang segala sesuatu yang akan dilakukan pada proses penlitian dan terlebih dahulu disusun pada tahap ini.
b. *Capture* merupakan tahapan dimana hasil penelitian tersebut disimpan agar nantinya dapat dilanjutkan dengan tahapan analisis menggunakan hasil tersebut.
c. *Analysis* merupakan tahap menganalisis menggunakan parameter data-data yang didapatkan dari tahap *capture.*
d. *Present* merupakan tahap mempresentasikan hasil yang didapatkan dari tahap sebelumnya agar dapat diketui oleh publik.

Dalam metode penelitian ini menggunakan teknik *static forensic* yaitu mengambil data setelah kejadian berlalu atau setelah *smartphone*nya mati. Penelitian ini menggunakan *tools* Magnet AXIOM yang merupakan platform investigasi produksi yang digunakan oleh *Magnet Forensics*, salah satu penyedia perangkat lunak forensik digital terkemuka di dunia. Perangkat lunak ini mampu memeriksa informasi dari komputer, laptop, IoT, cloud, *smartphone*, tablet, dan hasil imaging dari software lain. Magnet Axiom dapat menyederhanakan penyelidikan dengan menampilkan bukti yang relevan sebagai artefak yang mudah terlihat dan mendukung setiap langkah pengumpulan data, pemulihan data, analisis, dan proses pelaporan [23].

2.2 Simulasi Kasus

Sebelum melakukan proses forensik, penelitian ini terlebih dahulu merekayasa dan membuat kasus pencemaran nama baik dalam bentuk simulasi. Simulasi tersebut terbagi dua. Pertama tersangka memposting video beserta *hastag* pada halaman beranda TikTok yang menyinggung orang lain secara sengaja, setelah video tersebut diposting dan sudah dilihat orang lain maka tersangka langsung menghapus postingan tersebut dari *smartphone*nya. Dan simulasi yang kedua yaitu dimana dua orang saling berkirim pesan dimana pesan tersebut berupa pencemaran nama baik sekaligus ancaman yang membahas tentang pembayaran dan penyebaran foto setelah itu pesan tersebut dihapus dari *smartphone* tersangka. Proses forensik diupayakan untuk mendapatkan kembali data-data yang sudah dihapus oleh tersangka pada *smartphone*nya.

2.3 Alat dan Bahan Penelitian

Untuk dapat terlaksananya penelitian ini digunakan beberapa alat dan bahan sebagaimana ditunjukkan pada Tabel 1. Laptop adalah alat utama penelitian yang diperlukan untuk simulasi kasus, proses forensik, dan aktifitas penelitian lainnya. *Smartphone* Samsung Galaxy Tab digunakan dalam simulasi pencemaran nama baik. Data dari smartphone inilah yang nanti akan diangkat selama proses forensik. Untuk menghubungkan smartphone ke Laptop pada proses data capturing digunakan sebuah USB connector. Aplikasi TikTok yang digunakan pada simulasi dalam penelitian ini adalah versi 23.3.2. Sedangkan Magnet Axiom yang digunakan sebagai forensic tools untuk mengangkat data dari smartpone adalah versi 4.6.0.21968.

Tabel 1. Alat dan Bahan Penelitian

Nama	Spesifikasi	Keterangan
Laptop	Thinkpad, Intel I Core I i5	Perangkat Keras
Smartphone	Samsung Galaxy Tab A SM-P355 Versi 7.1.1	Perangkat Keras
USB *Connector*	Penghubung Smartphone dan Laptop	Perangkat Keras
Aplikasi TikTok	Versi 23.3.2	Perangkat Lunak
Magnet Axiom	Versi 4.6.0.21968	Perangkat Lunak

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

3. HASIL DAN PEMBAHASAN

3.1 *Plans*

Tahap perencanaan dilakukan dengan membuat rencana sedetail mungkin, terkait dengan langkah-langkah yang akan dilakukan selama proses penelitian, seperti membuat skenario penelitian dan menyiapkan alat dan bahan penelitian. Proses investigasi berfokus pada pencarian barang bukti digital dengan beberapa variabel yang ditentukan yakni *Messages*, video, dan *Hastag* seperti pada Tabel 2.

Tabel 2. Data Asal

No	Data				Jumlah
	Data Digital		Meta Data		
1	Messages		Sender Receiver Message Date/ Time	Karebet1997 Karebet0297 20/06/2022	21
2.	Video & Hastag		File Extension Created Date Modified Date File Size (Bytes) Duration (Sec) Resolution	.mp4 2022-06-07 15:59:19 2022-06-07 15:59:27 8.63 MB 0.29 544*960	Video = 15 Hastag = 12
			File Extension Created Date Modified Date File Size (Bytes) Duration (Sec) Resolution	.mp4 2022-06-07 16:01:04 2022-06-07 16:01:15 2.10 MB 0.27 352*640	
			File Extension Created Date Modified Date File Size (Bytes) Duration (Sec) Resolution	.mp4 2022-06-07 15:56:58 2022-06-07 15:57:07 1.70 MB 0.03 720*1280	

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

File Extension	.mp4
Created Date	2022-06-07 15:39:37
Modified Date	2022-06-07 15:40:18
File Size (Bytes)	27.88 MB
Duration (Sec)	0.15
Resolution	720*1280

File Extension	.mp4
Created Date	2022-06-07 16:03:08
Modified Date	2022-06-07 16:03:15
File Size (Bytes)	3.70 MB
Duration (Sec)	0.15
Resolution	352*640

File Extension	.mp4
Created Date	2022-06-07 15:36:05
Modified Date	2022-06-07 15:35:46
File Size (Bytes)	4.38 MB
Duration (Sec)	0.14
Resolution	640*480

File Extension	.mp4
Created Date	2022-06-07 16:07:59
Modified Date	2022-06-07 16:08:26
File Size (Bytes)	28.51 MB
Duration (Sec)	0.11
Resolution	1080*1920

File Extension	.mp4
Created Date	2022-04-19 11:36:39
Modified Date	2022-04-19 11:37:31
File Size (Bytes)	3 MB
Duration (Sec)	0.15
Resolution	720*1544

File Extension	.mp4
Created Date	2022-06-07 16:25:20
Modified Date	2022-06-07 16:25:58
File Size (Bytes)	3.4 MB
Duration (Sec)	0.15
Resolution	640*480

File Extension	.mp4
Created Date	2022-06-07 16:22:27
Modified Date	2022-06-07 16:30:00
File Size (Bytes)	3.7 MB
Duration (Sec)	0.15
Resolution	1536*3264

File Extension	.mp4
Created Date	2022-06-07 16:15:33
Modified Date	2022-06-07 16:15:56
File Size (Bytes)	3.7 MB
Duration (Sec)	0.15
Resolution	720*960

File Extension	.mp4
Created Date	2022-06-07 16:18:21
Modified Date	2022-06-07 16:18:53
File Size (Bytes)	7.9 MB
Duration (Sec)	0.15
Resolution	720*960

File Extension	.mp4
Created Date	2022-06-07 16:10:50
Modified Date	2022-06-07 16:11:24
File Size (Bytes)	6 MB
Duration (Sec)	0.15
Resolution	720*1544

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

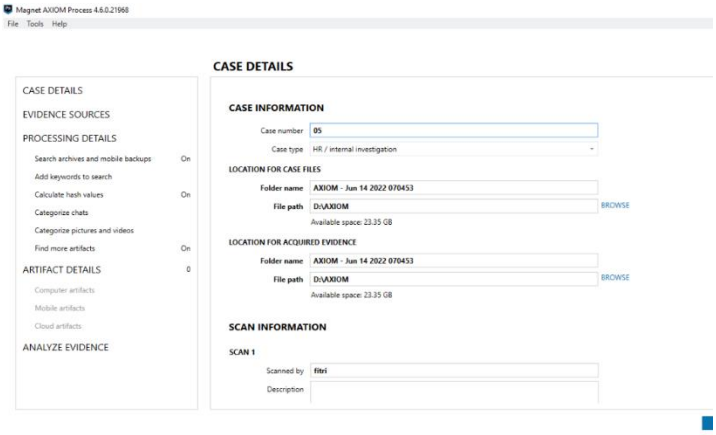
File Extension	.mp4
Created Date	2022-06-07 16:27:16
Modified Date	2022-06-07 16:27:51
File Size (Bytes)	2.6 MB
Duration (Sec)	0.15
Resolution	720*1544

File Extension	.mp4
Created Date	2022-06-07 16:05:41
Modified Date	2022-06-07 16:06:47
File Size (Bytes)	6.6 MB
Duration (Sec)	0.15
Resolution	720*1280

File Extension	.mp4
Created Date	2022-04-19 11:41:39
Modified Date	2022-04-19 11:41:52
File Size (Bytes)	8.63 MB
Duration (Sec)	0.29
Resolution	544*960

3.2 *Capture*

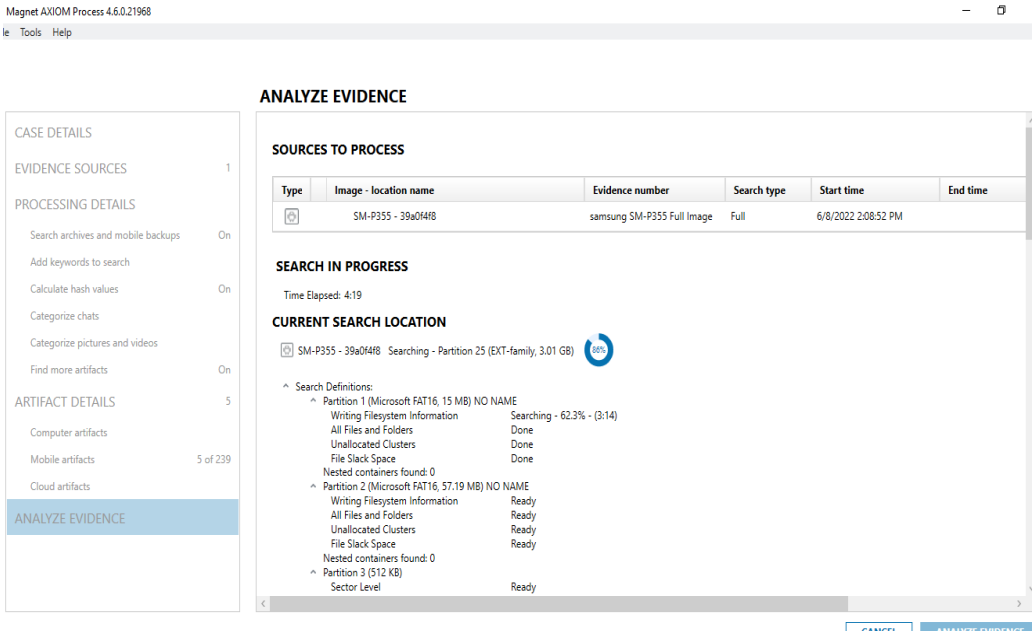
Sesuai dengan metode *static forensic* yang sudah dipilih dalam penelitian ini terdapat beberapa langkah yang digunakan pada tahap *capture* ini. Pada tahap pertama *smartphone* diamankan sebagai barang bukti, tahap kedua *smartphone* yang menjadi barang bukti dilakukan proses *root*, tahap ketiga aktifkan USB *debugging* pada *smartphone*, tahap keempat jalankan *tools* Magnet Axiom, lalu sambungkan kabel USB *connector* dari *smartphone* ke laptop, kemudian menginput *details case* berupa *case information, location for case files, location for acquired evidence*, dan *scan information*. Proses *capture* dapat dilihat seperti Gambar 3.



Gambar 3. Tampilan *input case details*

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Durasi proses ekstraksi dapat bervariasi tergantung pada jumlah data yang terkandung dalam bukti. Gambar 4 menunjukkan proses ekstraksi yang sedang berlangsung.



Gambar 4. Proses ekstraksi

Hasil dari proses *physical imaging capture* menggunakan *tools* magnet axiom selanjutnya akan diekstraksi sehingga dapat diperoleh bukti digital yang nantinya akan digunakan sebagai parameter penelitian pada tahap analisis.

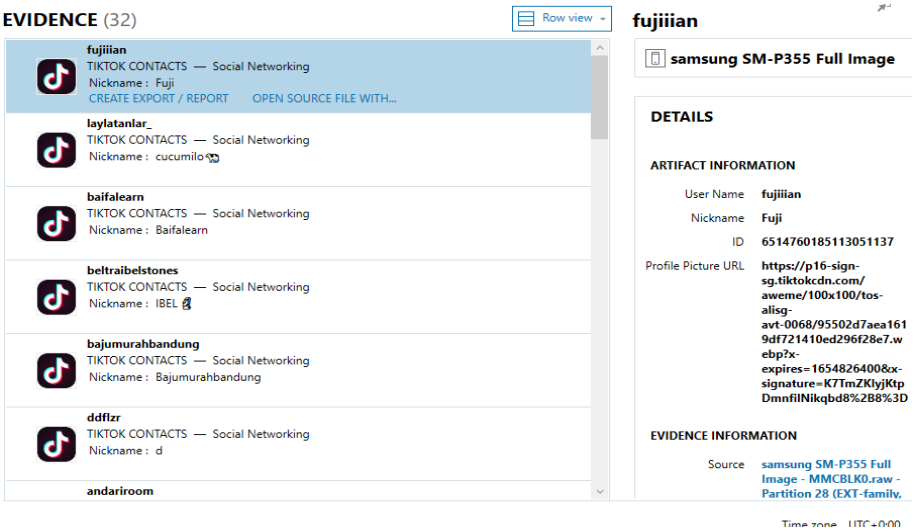
3.5 *Analysis*

Tahap ini adalah proses menganalisis data-data yang telah berhasil di ambil dari proses *exstraksi*. Hasil ekstraksi yang didapatkan dari proses *capture* yang telah dilakukan pada *Smartphone* Samsung Galaxy Tab A SM-P355 pada aplikasi TikTok menggunakan *tools* Magnet Axiom mendapatkan 32 Kontak/akun, 21 *message*, 15 Video, dan 1 *hastag*. Gambar 5 Menunjukkan pemilik akun TikTok bernama karebet1997, Gambar 6 menunjukkan data *contact* yang berhasil ditemukan, Gambar 7 menunjukkan *message*, Gambar 8 menunjukkan file video, serta *hastag* di tunjukkan pada Gambar 9.

Gambar 5. Informasi pemiliki akun TikTok

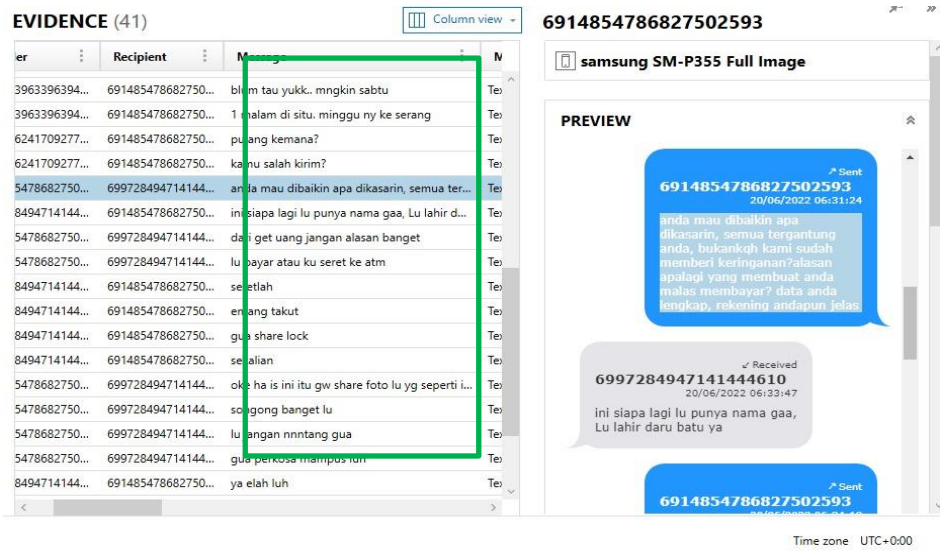
Pada Gambar 5. Merupakan informasi pemilik akun TikTok beserta *Profile Picture URL* yang telah terinstall pada *Smartphone Android* Samsung Galaxy Tab A SM-P355. Pemilik akun bernama karebet1997.

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom



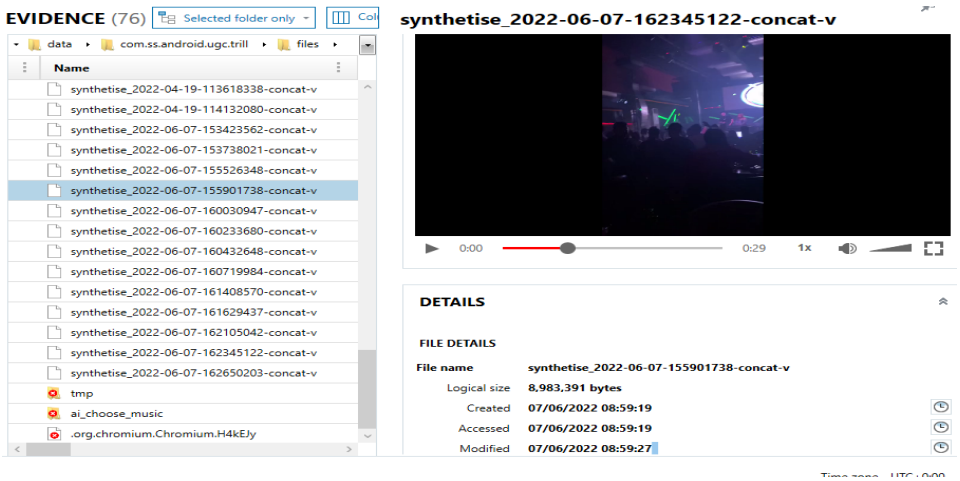
Gambar 6. Hasil analisis *contact* pada aplikasi TikTok

Gambar 6 menunjukkan hasil ekstraksi *contact* pada aplikasi TikTok yang berhasil diperoleh dengan menggunakan *tools* Magnet Axiom.



Gambar 7. Hasil analisis *messages* pada aplikasi TikTok

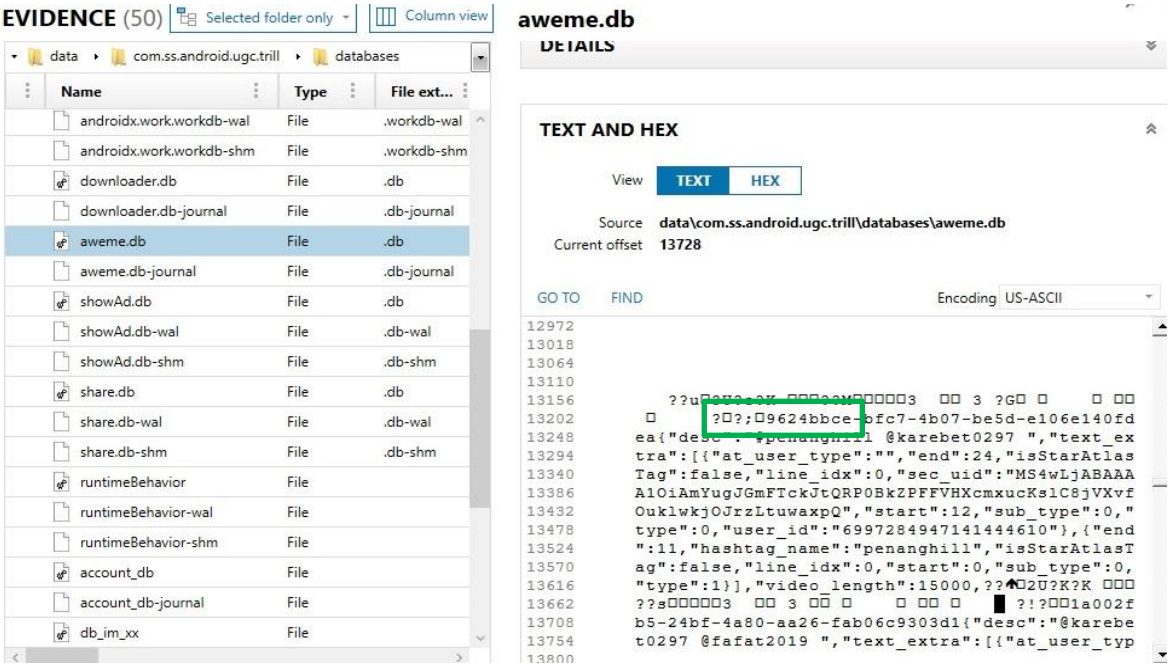
Gambar 7 menampilkan hasil data *messages* beserta *timesetup* yang berhasil didapatkan dari aplikasi TikTok yang terpasang pada *smartphone* Samsung Galaxy SM-P355 menggunakan *tools* Magnet Axiom yang dianalisis menggunakan *tools Magnet Axiom Evidance*.



Gambar 8. Hasil analisis video pada aplikasi TikTok

JURIKOM (Jurnal Riset Komputer), Vol. 9 No. 4, Agustus 2022
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v9i4.4738
Hal 1117−1127
http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Gambar 8 menunjukkan hasil pengambilan data video beserta ukuran dan *timesetup* yang didapatkan dari akun media sosial TikTok menggunakan Magnet Axiom pada *smartphone* samsung galaxy SM-P355. Data tersebut dianalisis menggunakan *Magnet Axiom Evidence*, yang filenya nanti akan membantu penyidik dalam mengungkapkan kejahatan digital pada postingan berupa video pada aplikasi TikTok.



Gambar 9. Hasil analisis *Hastag*

Pada Gambar 9 merupakan *hastag* dari video yang telah dihapus. Hastag tersebut terletak di com.ss.android.ugc.trill\databeses\aweme.db.

3.4 *Present*

Hasil analisis dalam melakukan proses forensik pada aplikasi tiktok menggunkan *tools* Magnet Axiom terhadap data asal yang disimulasikan sebagaimana ditunjukkan pada Tabel 2 ternyata dari 21 *Messanges* yang dikirimkan dapat diangkat semua, begitupun dengan video juga dapat diangkat semua, dan 12 data *hastag* dari video yang diposting seperti yang disimulasikan hanya satu data yang berhasil diangkat dari proses forensik ini. Data tersebut dapat dilihat pada Tabel 4.

Tabel 4. Hasil Barang Bukti Digital

Bukti Digital	Data Awal	Data yang Ditemukan
Messages	21	21
Video	15	15
Hastag	12	1
Jumlah	48	37

Analisis ini menghitung tingkat keberhasilan proses forensik dengan membandingkan jumlah data yang ditemukan dengan jumlah data awal yang disimulasikan. Menggunakan rumus seperti pada Pers. (1)

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

Perhitungan kinerja menggunakan *tools* Magnet Axiom = $\frac{37}{48} * 100 = 77\%$
Dimana pada perhitungan tersebut tersebut didapatkan tingkat keberhasilan 77%.

4. KESIMPULAN

Hasil yang diperoleh dari proses penelitian tentang analisis forensik aplikasi TikTok yang berjalan pada *Smartphone Android* yang sudah di-*root* mendapatkan beberapa kesimpulan yaitu bukti digital yang didapatkan berupa akun, *contact*, *messages*, video, dan *hastag* yang terkait dengan kasus pencemaran nama baik. Proses forensik menggunakan kerangka kerja ACPO dan *tools* Magnet Axiom yang dapat digunakan untuk proses ektsraksi bukti digital pada applikasi TikTok yang terpasang pada *smartphone* samsung Galaxy tab A SM-P355. Merujuk perhitungan perbandingan data yang yang berhasil diangkat dengan data awal sebagaimana ditunjukkan pada Tabel 4 tingkat keberhasilan proses forensik

menggunakan kerangka kerja proses forensik ACPO, *tools* Magnet Axiom, pada aplikasi TikTok, untuk simulasi kasus pencemaran nama baik adalah 77%.

REFERENCES

[1] I. R. Guntur Maulana Zamroni, Rusydi Umar, "Analisis Forensik Instant Messaging (WhatsApp) Berbasis Android," *Annu. Res. Semin.*, vol. 2, no. 1, p. 116, 2016.
[2] I. Riadi, Sunardi, and Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *JURTI*, vol. 3, no. 1, pp. 87–95, 2019.
[3] I. A. Rafiq, I. Riadi, F. T. Industri, U. A. Dahlan, S. Informasi, and U. A. Dahlan, "Perbandingan Forensic Tools pada Instagram Menggunakan Metode," vol. 7, no. 2, pp. 134–142, 2022.
[4] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.
[5] Sahirudin, I. Riadi, and Sunardi, "Data Recovery Dengan Keamanan Fingerprint," *Pros. SENDI_U 2018*, pp. 978–979, 2018, [Online]. Available: https://semantikom.unira.ac.id/2017/SEMANTIKOM_2017_paper_26.pdf
[6] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *J. TECHNO*, vol. 20, no. 2, pp. 125–130, 2019.
[7] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.
[8] Z. Qiyang and H. Jung, "Learning and Sharing Creative Skills with Short Videos: A Case Study of User Behavior in TikTok and Bilibili," *Int. Assoc. Soc. Des. Res. Conf.*, no. 10, pp. 25–50, 2019, [Online]. Available: https://www.researchgate.net/publication/335335984
[9] P. Domingues, R. Nogueira, J. C. Francisco, and M. Frade, "Post-mortem digital forensic artifacts of TikTok Android App," *ACM Int. Conf. Proceeding Ser.*, no. August, 2020, doi: 10.1145/3407023.3409203.
[10] R. Imam, U. Rusydi, and N. I. Mahfudl, "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Standards and Technology (Nist)," *J. Insa. Comtech*, vol. 2, no. 2, pp. 33–40, 2017.
[11] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id
[12] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. MEDIA Inform. BUDIDARMA*, vol. 6, no. 2, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.
[13] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Digital Forensics," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 4, pp. 274–276, 2017.
[14] R. S. C. Ieong, "FORZA - Digital forensics investigation framework that incorporate legal issues," *Digit. Investig.*, vol. 3, no. SUPPL., 2006, doi: 10.1016/j.diin.2006.06.004.
[15] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 219–227, 2018, doi: 10.28932/jutisi.v4i2.769.
[16] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *IT J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
[17] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile Pada Smartwatch Berbasis Android," *J. Rekayasa Teknol. Inf.*, vol. 1, no. 1, p. 41, 2017, doi: 10.30872/jurti.v1i1.638.
[18] F. L. Nafilaafila and Y. Prayudi, "Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android dengan metode NIST," *J. Sains Komput. Inform.*, vol. 6, no. 1, pp. 532–543, 2022.
[19] Soni, Y. Fatma, and R. Anwar, "Akuisisi bukti digital aplikasi pesan instan 'bip'menggunakan metode national institute of Justice (NIJ)," *J. Comput. Sci. Inf. Technol. (CoSciTech)*, vol. 3, no. 1, pp. 34–42, 2022.
[20] Muhammad Abdul Aziz, Wicaksono Yuli Sulistyo, and Sri Rahayu Astari3, "Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)," *JURISTIK (Jurnal Ris. Teknol. Inf. dan Komputer)*, vol. 1, no. 1, pp. 8–15, 2021, doi: 10.53863/juristik.v1i01.341.
[21] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.
[22] M. Nur Faiz, W. Adi Prabowo, and M. Fajar Sidiq, "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, pp. 63–70, 2018, doi: 10.20895/INISTA.V1I1.
[23] ahwan ahmadi, T. Akbar, and H. Mandala Putra, "Perbandingan Hasil Tool Forensik Pada File Image Smartphone Android Menggunakan Metode Nist," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.
[24] A. Tanner and D. Dampier, "Concept mapping for digital forensic investigations," *IFIP Adv. Inf. Commun. Technol.*, vol. 306, pp. 291–300, 2009, doi: 10.1007/978-3-642-04155-6_22.
[25] I. Riadi, R. Umar, M. I. Syahib, and S. S. Informasi, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standar and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, 2021.

24% Overall Similarity

Top sources found in the following databases:

- 17% Internet database
- Crossref database
- 0% Submitted Works database
- 14% 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	ejurnal.seminar-id.com Internet	3%
2	journal.uir.ac.id Internet	3%
3	Enno Loria, Ahmad Fauzi, Milli Alfhi Syari. "Penerapan Metode Vikor un... Crossref	3%
4	ejournal.unkhair.ac.id Internet	3%
5	Adeel Javed, Anum Sundrani, Nadia Malik, Sidney Madison Prescott. "... Crossref	2%
6	Ismayana Teguh Pratama, Rahmatika Putri, Rian Fernanda, Sunardi. "T... Crossref	2%
7	e-journals.unmul.ac.id Internet	1%
8	download.garuda.ristekdikti.go.id Internet	1%

9	core.ac.uk Internet	<1%
10	journal.uny.ac.id Internet	<1%
11	dspace.uii.ac.id Internet	<1%
12	pdfs.semanticscholar.org Internet	<1%
13	ejournal.lppmsttpagaralam.ac.id Internet	<1%
14	dspace.marmara.edu.tr Internet	<1%
15	repository.ittelkom-pwt.ac.id Internet	<1%
16	adoc.pub Internet	<1%
17	eprints.uad.ac.id Internet	<1%
18	journal2.uad.ac.id Internet	<1%
19	repository.trisakti.ac.id Internet	<1%
20	blog.umy.ac.id Internet	<1%

21	ejurnal.umri.ac.id Internet	<1%
22	elib.pstu.ru Internet	<1%
23	jurnal.upnyk.ac.id Internet	<1%
24	doku.pub Internet	<1%
25	"Innovations in Computer Science and Engineering", Springer Science a... Crossref	<1%
26	Soni Soni, Yulia Fatma, Rizki Anwar. "Akuisisi Bukti Digital Aplikasi Pes... Crossref	<1%

Excluded from Similarity Report

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

EXCLUDED SOURCES

ejurnal.stmik-budidarma.ac.id Internet	84%
researchgate.net Internet	80%
ejurnal.stmik-budidarma.ac.id Internet	19%
stmik-budidarma.ac.id Internet	19%
stmik-budidarma.ac.id Internet	9%
jtiik.ub.ac.id Internet	8%
jurnal.iaii.or.id Internet	8%
jurnal.iaii.or.id Internet	5%
Imam Riadi, Herman Herman, Irhash Ainur Rafiq. "Mobile Forensic Investigati... Crossref	4%
pkns.portalapssi.id Internet	4%

pkns.portalapssi.id Internet	4%
jurnal.uii.ac.id Internet	4%
vmus.adu.org.za Internet	3%
strategian.com Internet	3%
journal.ubb.ac.id Internet	3%
ijeap.org Internet	3%
kursorjournal.org Internet	3%
e-journal.ivet.ac.id Internet	3%
clausiuspress.com Internet	3%
Agung Sugiarto, Robby Rizky, Susilowati Susilowati, Ayu Mira Yunita, Zaenal ... Crossref	3%