JIKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang *P ISSN : 2549-0710*
Tangerang, April 2024, Vol 8 No.2, pp 187-196 *E ISSN : 2722-2713*

ANALISIS FORENSIK APLIKASI PENIPUAN BERBASIS ANDROID MENGGUNAKAN METODE NIST

Irfan Maulana[1)], Ardi Pujiyanta[2)]
[1,2]Informatika, Teknologi Industri, Universitas Ahmad Dahlan, Jalan Ring Road Selatan
Tamanan Banguntapan Bantul Yogyakarta
Co Responden Email: ardipujiyanta@tif.uad.ac.id

Article history
Received 08 Jan 2024
Revised 23 Feb 2024
Accepted 04 Apr 2024
Available online 30 Apr 2024

Keywords
android,
digital forensics,
mobile,
malware,
NIST

Abstract

The increasing use of Android-based applications is in line with technological developments. One problem is that it can be misused in criminal acts by planting malware or phishing into Android applications. Applications such as WhatsApp can be a means for criminals to send malicious application files to victims. For evidence in criminal cases, forensic analysis will be carried out to obtain digital evidence, in the form of conversation histories, images, documents and others. The method used in this research uses the National Institute of Standards and Technology (NIST) method. The NIST method has four stages as a reference for analyzing evidence, including collection, examination, analysis and reporting. The research stages carried out started from literature study, observation, scenario design, preparing research needs, and applying the NIST method. Next, look for digital evidence in the form of malicious application files for system analysis of the application. This research resulted in information stored in the WhatsApp database in the form of conversation data and malicious application files. The information obtained from the analyzed application is that the application is manipulated as if it were another file, the impact of the manipulated application can steal personal data from the victim, in the form of SMS. An important SMS can be an OTP code for the victim's bank account.

Riwayat
Diterima 08 Jan 2024
Revisi 23 Feb 2024
Disetujui 04 Apr 2024
Terbit Online 30 Apr 2024

Kata Kunci
android,
digital forensik,
mobile,
malware,
NIST

Abstrak

Meningkatnya penggunaan aplikasi berbasis Android seiring dengan perkembangan teknologi. Salah satu permasalahan yang bisa disalah gunakan dalam tindak kejahatan dengan menanamkan malware atau phising ke dalam aplikasi Android. Aplikasi seperti Whatsapp bisa menjadi sarana bagi pelaku kejahatan untuk mengirimkan file aplikasi berbahaya ke korban. Barang bukti dalam kasus pidana, akan dilakukan analisis forensik untuk mendapatkan bukti digital, baik berupa riwayat percakapan, gambar, dokumen dan lainnya. Metode yang digunakan dalam penelitian ini menggunakan metode National Institute of Standards and Technology (NIST). Metode NIST memiliki empat tahapan untuk acuan analisis barang bukti antara lain, collection, examination, analysis, dan reporting. Tahapan penelitian yang dilakukan dimulai dari studi literatur, observasi, perancangan skenario, mempersiapkan kebutuhan penelitian, dan penerapan metode NIST. Selanjutnya mencari bukti digital berupa file aplikasi berbahaya untuk dianalisis sistem dari aplikasi tersebut. Penelitian ini menghasilkan informasi yang tersimpan di dalam database Whatsapp berupa data percakapan dan file aplikasi berbahaya. Informasi yang didapat dari aplikasi yang dianalisis tersebut yaitu aplikasi tersebut dimanipulasi seolah-olah file lain, dampak dari aplikasi yang telah dimanipulasi dapat mencuri data pribadi dari korban, berupa SMS. SMS penting bisa berupa kode OTP rekening bank milik korban.

PENDAHULUAN

Berbagai jenis gadget seperti tablet PC dan smarthphone, telah banyak didukung oleh beberapa jenis sistem operasi. Sistem operasi android adalah salah satu sistem operasi yang digunakan untuk mendukung kinerja smarthphone. Android adalah sistem operasi berbasis linux yang dirancang untuk perangkat bergerak layar sentuh seperti telepon pintar dan komputer tablet (Saputra & Borman,

2020). Aplikasi berbasis android merupakan aplikasi yang dibuat menggunakan bahasa pemrogramman. Aplikasi ini dapat berupa toko online, pinjam online, jasa transportasi. Server komputer digunakan sebagai tempat aplikasi tersebut. Pengguna dapat mengakses aplikasi melalui device seperti *PC tablet* dan *smarthphone*. Aplikasi tersebut dibuat sebagai solusi untuk mengatasi berbagai masalah atau dengan kata lain untuk mempermudah berbagai macam aktifitas (Arista Yuliani & Riadi, 2019). Aplikasi lintas *platform* Whatsapp tersedia untuk sistem operasi Android, Windows, dan IOS. Whatsapp memungkinkan untuk mengirim pesan teks, mengirim pesan audio, dan pesan video (Arista Yuliani & Riadi, 2019; Zamroni & Riadi, 2019).

Fitur yang ada pada aplikasi Whatsapp dapat disalahgunakan pengguna untuk tujuan tindak kejahatan, seperti kegiatan teroris, perdagangan narkoba, perencanaan pembunuhan, dan tindak kejahatan lainnya (Arista Yuliani & Riadi, 2019). Aplikasi messanger banyak digunakan oleh para pelaku kejahatan, sebagai sarana untuk berinteraksi dengan sesama rekan penjahat maupun korban. Nomor ponsel digunakan sebagai identitas dalam aplikasi Whatsapp. Identitas pengguna dimanfaatkan oleh pelaku kejahatan, untuk melancarkan aksinya (Yudhana et al., 2018).

Pelaku kejahatan biasanya mengirimkan *file* yang mengandung *malware* atau *phising* dan korban tanpa sengaja terjebak dalam skenario tersebut. Program *Malware* (*Malicious Software*) dirancang dengan tujuan merusak atau menyusup ke sistem komputer. Cara yang digunakan *Malware* adalah dengan menginfeksi banyak perangkat komputer atau android. *Malware* masuk melalui email, *download* internet, atau aplikasi yang terinfeksi. Dampak yang ditimbulkan adalah kerusakan pada sistem komputer atau android dan memungkinkan juga terjadi pencurian data/informasi. *Malware* mencakup virus, *worm*, *trojan horse*, perangkat pengintai (*spyware*), perangkat iklan (*adware*) yang tidak jujur, dan perangkat kejahatan (*crimeware*), serta *software* lain yang berbahaya (Bintang et al., 2020).

Piranti digital yang digunakan untuk tindak kejahatan dapat membantu proses peradilan akan efek yang ditimbulkannya. Barang bukti kasus kejahatan dapat berupa perangkat smartphone dan komputer yang ter-*install* Whatsapp dan didalamnya juga terdapat *file malware* atau *phising*. Dimana didalamnya terdapat percakapan Whatsapp pelaku kejahatan dan korban. Perangkat tersebut yang akan menjadi barang bukti dan dapat dilakukan analisis agar dapat ditindak lanjuti (Setyawan et al., 2020). Kasus kejahatan dalam hal penipuan dengan menemukan artefak digital yang berkaitan dengan barang bukti yang dicari (Muhammad Abdul Aziz et al., 2021).

Penyalahgunaan fitur layanan pesan instan Whatsapp dapat diinvestigasi menggunakan forensik digital. Rangkaian tahapan baku sesuai prosedur forensik digital, akan dilakukan untuk menginvestigasi kasus penipuan melalui pesan chat Whatsapp (Rifqi et al., 2023).

Penerapan ilmu digital forensik dapat membantu dalam mencari barang bukti pada kasus kejahatan yang terjadi, khususnya yang terjadi melalui Whatsapp, karena jumlah pengguna yang banyak, khususnya di Indonesia. Dalam persidangan forensik yang dijadikan acuan saksi ahli dalam sebuah kasus, adalah aplikasi Whatsapp yang berisi percakapan pesan tindak kejahatan telekomunikasi (Riadi et al., 2018). Selanjutnya akan dilakukan report investigasi forensik yang melibatkan barang bukti perangkat (Zamroni & Riadi, 2019). Hal ini menimbulkan perspektif dari penyelidikan forensik, dimana aplikasi Whatsapp menyimpan data-data pembuktian berupa percakapan dan media yang dikirimkan pelaku kejahatan, yaitu *file* aplikasi yang mengandung malware atau phising, yang dapat digunakan di pengadilan. Oleh karena itu pemilihan metodologi yang tepat akan membantu terhadap langkah-langkah yang diterapkan dalam investigasi forensik.

Salah satu penerapan alur investigasi yang digunakan dalam penentuan langkah-langkah investigasi forensik yaitu dengan menggunakan *metode National Institute of Standards and Technology* (NIST). Metode NIST memiliki empat tahapan dalam proses investigasi yaitu *collection, examination, analysis, reporting* (Muhammad Abdul Aziz et al., 2021; Riadi et al., 2021; Yudhana et al., 2018).

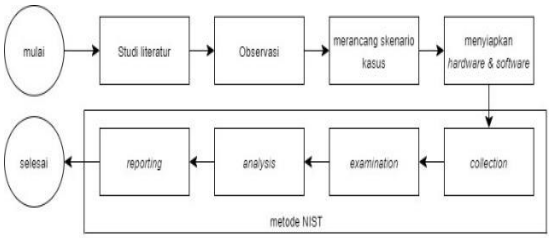
Penelitian ini akan membahas kasus penipuan melalui pesan percakapan yang terjadi di dalam aplikasi Whatsapp, yang berdasarkan skenario kasus tindak kejahatan penipuan, dengan menggunakan emulator Android sebagai perangkat korban penerima pesan penipuan dari pelaku. Penerapan digital forensik dan metode NIST dapat memberikan kontribusi kerangka kerja yang dapat diterapkan pada proses investigasi forensik dalam menganalisa *database* yang tersimpan di perangkat korban, yaitu emulator Android dan juga *file* aplikasi yang dikirimkan oleh penipu. Dengan pendekatan forensik yang digunakan dapat menemukan sesi percakapan yang terjadi antara pelaku kejahatan dan korban yang tersimpan di dalam database Whatsapp. *Tools* yang digunakan dapat memaparkan *file* aplikasi berbahaya yang dikirimkan pelaku, dengan cara melakukan *reverse engineering* terhadap *file* aplikasi tersebut .

METODE PENELITIAN

A. Tahapan Penelitian

Tahapan penelitian yang akan dikerjakan pada penelitian ini yaitu dengan menggunakan studi literatur, untuk mencari referensi kemudian ditentukan simulasi dari suatu skenario kasus tindak kejahatan. Tahapan tersebut di atas untuk mengetahui dampak dari file aplikasi terhadap perangkat korban yang dikirimkan oleh pelaku tindak kejahatan melalui pesan percakapan Whatsapp. Awal tahapan pada implementasi *mobile forensic* yaitu melakukan pemeliharaan barang bukti, dengan tujuan agar barang bukti yang ditemukan bebas dari pihak yang tidak bertanggung jawab. Proses selanjutnya adalah melakukan proses imaging, dengan tujuan untuk menduplikat data yang tersimpan pada barang bukti tanpa merubah sedikitpun data yang ada didalamnya (Mahendra & Ari Mogi, 2021).

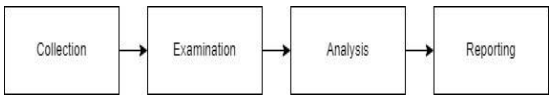
Setelah proses imaging, tahap selanjutnya yaitu menganalisis data yang sudah di imaging. Tahap ini memerlukan tools untuk menunjang proses analisis. Untuk mendekripsi database Whatsapp diperlukan *tools* Whatsapp Viewer. Dalam mendekripsikan *database* menggunakan Whatsapp Viewer yang memerlukan *file key*, untuk mengaksesnya perangkat harus dalam keadaan *roo*t dan menggunakan aplikasi Root Explorer. Untuk proses *reverse engineering* atau *decompile file* dengan cara me-*rename* format aplikasi dari .apk ke .zip, kemudian di ekstrak. Setelah di ekstrak terdapat folder dan file, yang akan di analisis yaitu *file* "AndroidManifest.xml" dan "classes.dex" untuk di analisis *permission* dari aplikasi tersebut (Al-Fawa'reh et al., 2020). Selanjutnya dilakukan proses *reporting* dari serangkaian tahapan sebelumnya. Kemudian reporting tersebut dijadikan parameter sebagai barang bukti kejahatan, berdasarkan hasil temuan dan serangkaian tahapan dan proses. Berikut adalah tahapan penelitian yang ditunjukkan pada gambar 1:



Gambar 1. Flowchart Tahapan Penelitian

B. National Institue of Standards and Technology

Metode yang digunakan dalam penelitian ini adalah metode NIST (Achmad Iqbal Yuladi & ..., 2021; Anggraini et al., 2023; Ardiningtias et al., 2021), dengan tahapan sebagai berikut, yang ditunjukkan pada gambar 2 :



Gambar 2. Tahapan Metode NIST

i. Collection

ii. Pelabelan, identifikasi, rekaman, dan pengambilan data menggunakan sumber data yang relevan supaya integritas data dapat terjaga .

iii. Examination

iv. Pengolahan data yang dikumpulkan dalam penggunaan forensik merupakan kombinasi berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sesuai dengan kebutuhan.

v. Analysis

vi. Analisis hasil pemeriksaan dengan menggunakan metode teknis yang dibenarkan secara hukum.

vii. Reporting
viii. Hasil analisis yang menggambarkan tindakan yang dilakukan

C. Skenario Kasus Kejahatan

Tujuan skenario ini adalah untuk mempermudah investigasi kasus Cyber Crime. Skenario tersebut yaitu :

i. Pelaku kejahatan membuat sebuah aplikasi berbahaya yang nantinya akan disebarkan via Whatsapp.
ii. Selanjutnya tersangka membuat akun Whatsapp untuk menyebarkan aplikasi *malware*.
iii. Kemudian tersangka mendapatkan nomor telepon korban yang digunakan pada akun Whatsapp korban. Pelaku mendapatkan nomor telepon korban dari bungkusan paket barang yang dibuang sembarangan oleh korban.
iv. Pelaku kejahatan mengirimkan percakapan dengan modus pengiriman paket barang, kemudian mengirimkan file aplikasi berbahaya namun dimanipulasikan seolah-olah *file* aplikasi tersebut adalah file "Cek Resi J&T".

HASIL DAN PEMBAHASAN

A. Analisis Kebutuhan

Kebutuhan dalam penelitian ini dibagi menjadi dua bagian, *software* dan *hardware*, terdiri dari beberapa komponen berikut (Tabel 1).

Tabel 1. Analisis Kebutuhan

Software	Hardware
7zip	Laptop Lenovo Thinkpad T440p
Dex2Jar	-
JD-GUI	-
Visual Studio Code	-
Androguard xml	-
Whatsapp Viewer	-
Root Explorer	-
DB Browser for SQLite	-
FTK Imager	-
Whatsapp Crypt14 Crypt15 Decrypter	-

B. Alur Investigasi

Pada alur investigasi, investigator mendapat barang bukti tidak langsung dari pelaku kejahatan melainkan dari pihak kepolisian yang sebelumnya sudah mengamankan barang bukti. Alur investigasi menjelaskan proses bagaimana investigator mendapatkan barang bukti dari pihak kepolisian. Proses investigasi tidak boleh langsung dari barang bukti asli. Barang bukti harus melakukan proses *imaging* agar barang bukti asli tidak terkontaminasi oleh hal-hal yang tidak bertanggung jawab. Berikut alur proses mendapatkan barang bukti, ditunjukkan pada gambar 3 :

Gambar 3. Alur Pengambilan Barang Bukti

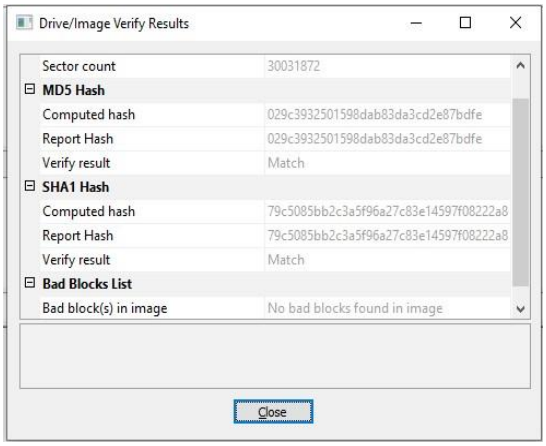
C. Collection

Tahapan *collection* dimulai pasca simulasi, dengan barang bukti sebuah laptop, dan *smarthphone* yang digambarkan pada emulator yang terpasang di laptop. Berikut barang bukti yang ditunjukkan pada tabel 2 :

Tabel 2. Barang Bukti Fisik

No.	Barang bukti	Gambar	Keterangan
1	Laptop berjumlah 1 (milik korban)		Laptop bermerk Lenovo
2	Adaptor berjumlah 1 (milik korban)		Adaptor bermerk Lenovo

Selanjutnya setelah mengumpulkan barang bukti dilakukan akuisisi file. Akuisisi file memerlukan software yaitu FTK Imager, kemudian memvalidasi kode hash antara file yang diakuisisi dengan file yang asli (Krisnadi, 2020). Karena dalam penelitian ini menggunakan laptop yang terinstall emulator android, maka untuk media penyimpan emulator yang akan diakuisisi tersimpan di dalam sebuah flashdik, sebagai perantara dalam hal mengakuisisi media penyimpanan emulator, flashdisk digunakan agar media penyimpanan emulator bisa diakuisisi menggunakan FTK Imager.
Pada gambar 4 merupakan nilai kode *hash*, kode *hash* akan dilihat apakah cocok *computed hash* dengan *report hash.*



Gambar 4. Nilai kode hash akuisisi

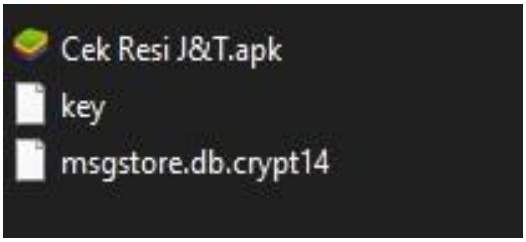
Gambar 5 merupakan *file* hasil akuisisi yang tersimpan sesuai dengan destinasi penyimpanan yang telah ditentukan pada saat proses akuisisi menggunakan FTK Imager

Gambar 5. File Hasil Akuisisi

D. Examination

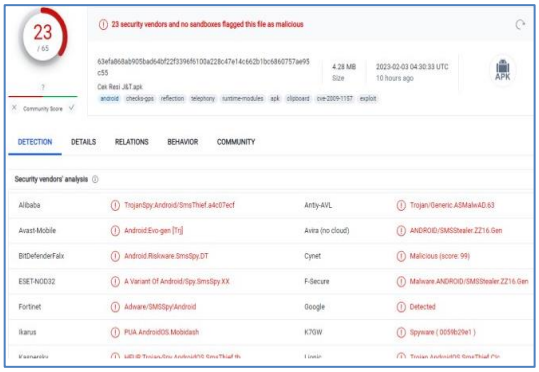
Tahapan *examination* merupakan tahapan pemeriksaan terhadap data dan pengolahan data hasil proses imaging. Kemudian dilakukan eksplorasi untuk mendapatkan atau menemukan barang bukti yang dibutuhkan yaitu *database* Whatsapp dan juga *file* aplikasi yang tersimpan di dalam penyimpanan emulator, tanpa mengubah integritas data (Albarida, 2020).

Gambar 6 merupakan hasil dari ekstraksi imaging menggunakan FTK Imager.



Gambar 6. Hasil Ekstraksi

Gambar 7 menunjukkan hasil dari pemeriksaan *file* yang sudah diekstrak menggunakan Virustotal, hasilnya menandakan bahwa aplikasi tersebut ditandakan sebagai aplikasi "*malicious*" atau mencurigakan. Hal tersebut terbukti dari total 65 *security vendors* pada Virustotal, 23 diantaranya menandakan bahwa aplikasi tersebut mencurigakan mengandung *malware*.



Gambar 7. Hasil pemeriksaan dengan virustotal

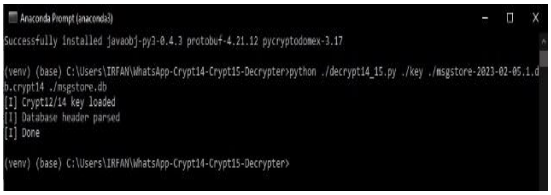
E. Analisis

Tahap ini bertujuan untuk melakukan analisis dan mengungkap hasil dari tahap sebelumnya, yaitu *Examination* untuk memperoleh data yang berkaitan dengan hasil yang sudah didapatkan dari tahap sebelumnya. Data yang diperoleh berupa hasil ekstrak database Whatsapp dan *decompile file* aplikasi yang akan memberikan informasi secara terperinci terhadap barang bukti.

Pada database Whatsapp dilakukan enkripsi *database* menggunakan enkripsi crypt14. Kemudian untuk melakukan *decrypt database file* memerlukan *file key*, dan dengan menggunakan *tools* Whatsapp Viewer atau Whatsapp Crypt14 Crypt15 Decrypter dan untuk melihat *database chat* menggunakan

DB Browser for SQLite atau Whatsapp Viewer (Afzal et al., 2021).

Gambar 8 menunjukkan proses *decrypt* menggunakan Whatsapp Crypt14 Crypt15 Decrypter.



Gambar 8. Proses decrypt

Gambar 9 merupakan isi dari *file* hasil dari proses decrypt yang dibuka menggunakan DB Browser for SQLite.

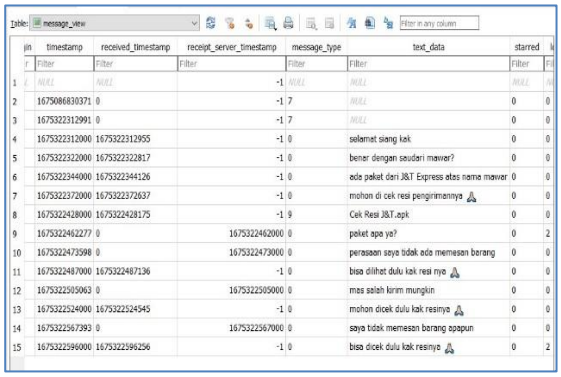
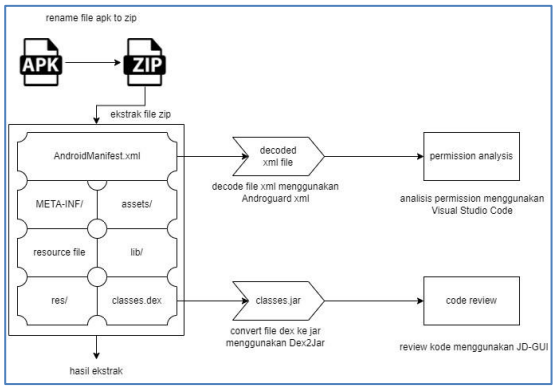


Table: message_view

_id	timestamp	received_timestamp	receipt_server_timestamp	message_type	text_data	starred
1	NULL	NULL	-1	NULL	NULL	NULL
2	1675086830371	0	-1	7	NULL	0
3	1675322312991	0	-1	7	NULL	0
4	1675322312000	1675322312955	-1	0	selamat siang kak	0
5	1675322322000	1675322322817	-1	0	bener dengan saudari mawar?	0
6	1675322344000	1675322344126	-1	0	ada paket dari J&T Express atas nama mawar	0
7	1675322372000	1675322372637	-1	0	mohon di cek resi pengirimannya	0
8	1675322428000	1675322428175	-1	9	Cek Resi J&T.apk	0
9	1675322462277	0	1675322462000	0	paket apa ya?	0
10	1675322473598	0	1675322473000	0	perasaan saya tidak ada memesan barang	0
11	1675322487000	1675322487136	-1	0	bisa dilihat dulu kak resi nya	0
12	1675322505063	0	1675322505000	0	mas salah kirim mungkin	0
13	1675322524000	1675322524545	-1	0	mohon dicek dulu kak resinya	0
14	1675322567393	0	1675322567000	0	saya tidak memesan barang apapun	0
15	1675322596000	1675322596256	-1	0	bisa dicek dulu kak resinya	0

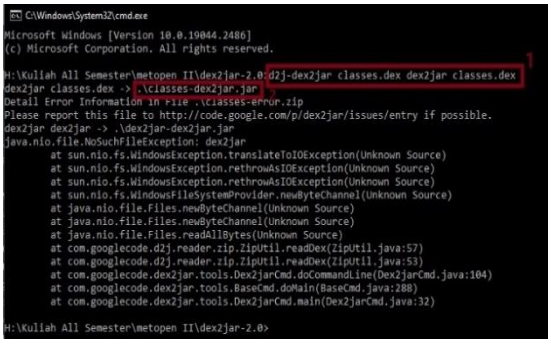
Gambar 9. Isi dari file hasil decrypt

Setelah proses *decrypt*, kemudian beralih ke proses *decompile file* aplikasi yang ditunjukkan pada gambar 10 :



Gambar 10. Alur Proses Decompile Aplikasi

Gambar 11 merupakan konversi *file* "classes.dex" menggunakan Dex2Jar agar kode dari aplikasi tersebut bisa terbaca menggunakan *text editor*.



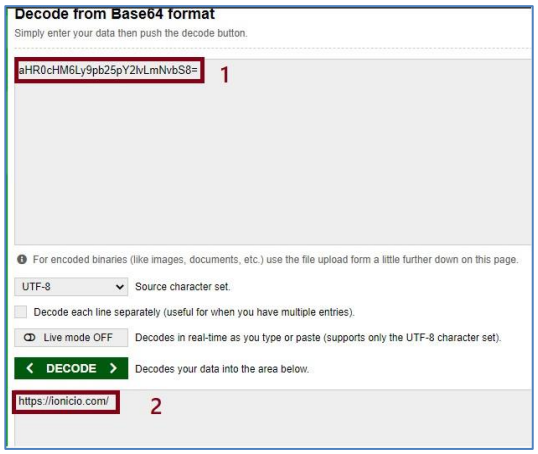
Gambar 11. Proses konversi file Classes.dex

Gambar 12 dan gambar 13 merupakan Class MainActivity dan ReceiveSMS dari aplikasi tersebut menggunakan JD-GUI.

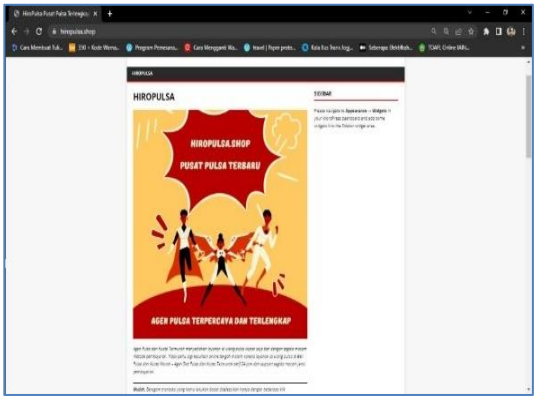
Gambar 12. Class MainActivity

Gambar. 13 Class ReceiveSMS

Pada MainActivity.Class, terdapat sebuah *string* yaitu "aHR0cHM6Ly9pb25pY2lvLmNvbS8=" yang ter-*encode* menggunakan Base64, apabila di-*decode* hasilnya ditunjukkan pada gambar 14 maka akan mendapatkan sebuah URL yang mencurigakan, dan ketika URL tersebut diakses maka akan menuju ke sebuah *website* mencurigakan yang ditunjukkan pada gambar 15.



Gambar 14. Decode String Base64



Gambar 15. Website Mencurigakan

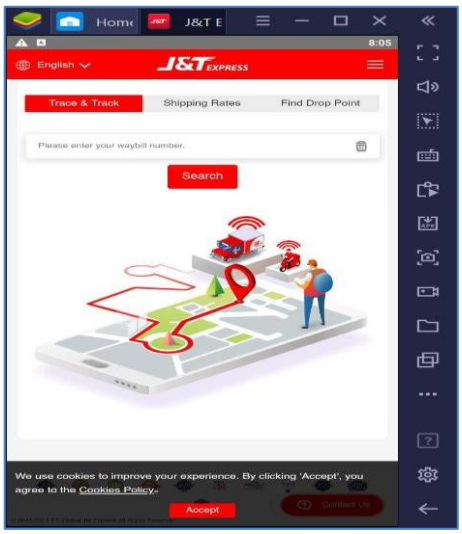
Selanjutnya masuk ke proses menganalisis file ".xml", agar file ".xml" terbaca menggunakan text editor maka dilakukan proses decode menggunakan Androguard xml. Setelah dianalisis pada file AndroidManifest.xml, terdapat permission yang diantaranya adalah sebagai berikut :

i. "android.permission.RECEIVE_SMS" untuk membaca dan memproses SMS.
ii. "android.permission.INTERNET" untuk akses internet.
iii. android.permission.ACCESS_NETWORK_STATE untuk melihat informasi koneksi jaringan.
iv. "android.permission.BROADCAST_SMS " mengizinkan aplikasi untuk menyiarkan pemberitahuan bahwa pesan SMS telah diterima.

Selanjutnya ketika aplikasi di install dan dibuka, aplikasi akan meminta perizinan ke sistem untuk "*send and view SMS messages*" pada perangkat, yang ditunjukkan pada gambar 16 dan tampilan aplikasi ditunjukkan pada gambar 17.

Gambar 16 Aplikasi meminta izin SMS

Pada gambar 16 merupakan proses permintaan izin ketika meng-*install* aplikasi tersebut, terlihat bahwa aplikasi meminta izin *"send and view SMS messages"* atau mengirim dan membaca pesan SMS pada perangkat yang akan di-*install* aplikasi tersebut.



Gambar 17. Tampilan Utama Aplikasi

Pada gambar 17 merupakan tampilan utama dari aplikasi yang sudah ter-*install* di perangkat. Aplikasi tersebut menampilkan fungsi untuk melacak lokasi pengiriman paket ketika pengguna menggunakan jasa J&T, dimana tampilan tersebut merupakan bersumber dari *web* resmi dari J&T dengan alamat situs "https://www.jet.co.id/track".

A. Reporting

Dari hasil analisis yang telah dilakukan akan didapatkan reporting, berikut adalah hasil analisis yang telah dilakukan.

Tabel 3 merupakan transaksi percakapan antara pelaku dan korban yang tersimpan di dalam *database* Whatsapp.

Tabel 3. Percakapan whatsapp pelaku dan korban

Timestamp	Received_ti	Receipt serv	Mess	Text_data
		-1		
1,6751E+12	0	-1	7	
1,6753E+12	0	-1	7	
1,6753E+12	1,6753E+12	-1	0	selamat siang
1,6753E+12	1,6753E+12	-1	0	benar dengan
1,6753E+12	1,6753E+12	-1	0	ada paket dari
1,6753E+12	1,6753E+12	-1	0	mohon di cek
1,6753E+12	1,6753E+12	-1	9	Cek Resi
1,6753E+12	0	1,6753E+12	0	paket apa ya?
1,6753E+12	0	1,6753E+12	0	perasaan saya
1,6753E+12	1,6753E+12	-1	0	bisa dilihat dulu
1,6753E+12	0	1,6753E+12	0	mas salah kirim
1,6753E+12	1,6753E+12	-1	0	mohon dicek
1,6753E+12	0	1,6753E+12	0	saya tidak
1,6753E+12	1,6753E+12	-1	0	bisa dicek dulu

Kemudian pada tabel 4 menunjukkan informasi aplikasi berbahaya yang dikirimkan pelaku ke korban.

Tabel 4. Informasi aplikasi

Nama File	Cek Resi J&T.apk
Nama	J&T Express
Package Name	com.ngscript.smstest
Main	com.ngscript.smstest.MainActivity
Ukuran	4.3 MB
MD5	e45f50c4464176306db106be730af3a0
SHA-1	16de7f1ac09f3667627d5330ca14b0ddc45b68c2

Hasil uji coba yang telah dilakukan adalah sebagai berikut:

i. Setelah pertama kali diinstal, aplikasi meminta perizinan untuk mengirim dan melihat pesan SMS di perangkat.
ii. Tampilan aplikasi ketika dibuka menampilkan *webview* dari *website* jet.co.id sebagai tampilan awal.
iii. Ketika aplikasi ditutup dan dibuka kembali, aplikasi hanya menampilkan layar putih dan setelah ditunggu beberapa saat aplikasi tetap menampilkan layar putih.
iv. Emulator mulai terasa berat ketika aplikasi dijalankan (setelah aplikasi ditutup dan dibuka kembali dan menampilkan layar putih).
v. Peneliti mencoba menguji pencurian SMS di perangkat emulator, namun server pelaku sudah tidak aktif dan keterbatasan peneliti karena emulator yang digunakan tidak memiliki fitur SMS di dalamnya.
vi. Kemudian hasil dari penelusuran *file* dalam mencari *string "flag"* (*capture the flag*) yang tersembunyi, peneliti hanya menemukan 2 (dua) *string* yang mencurigakan, diantaranya adalah sebagai berikut:
vii. aHR0cHM6Ly9pb25pY2lvLmNvbS8=
viii. Merupakan sebuah string yang di-*encode* ke dalam format Base64, setelah di-*decode string* tersebut menjadi sebuah URL yaitu "https://ionicio.com/". URL tersebut domainnya sudah tidak aktif lagi. *String* tersebut ditemukan pada Main Activity.class dan ReceiveSms.class.
ix. 5797152557JNT
x. Setelah dilakukan penelusuran lebih lanjut terhadap pembahasan yang berkaitan dengan kasus penipuan ini, diketahui kalau string ini merupakan sebuah id Telegram milik pelaku kejahatan, namun sepertinya akun Telegram tersebut sudah dihapus. *String* tersebut juga ditemukan pada Main Activity.class dan ReceiveSms.class.

Dari hasil pembuktian yang ditemukan dari aplikasi berbahaya tersebut melalui analisis. Aplikasi tersebut adalah aplikasi dengan tujuan untuk mencuri data pribadi milik korban yaitu berupa SMS.

Contoh SMS yaitu kode OTP dari suatu bank yang biasanya diterima melalui SMS, dari kode OTP tersebut pelaku bisa mengakses

rekening bank korban dan melakukan pencurian uang milik korban.

KESIMPULAN

Kesimpulan yang didapat berdasar uraian di atas, sebagai berikut:

Dalam melakukan ekstrak terhadap *database* percakapan Whatsapp diharuskan memiliki *file key* yang mana untuk mendapatkannya *device* harus dalam keadaan *root*. Untuk crypt14 yaitu *cyrpt* dari Whatsapp versi terbaru tidak bisa dilakukan *decrypt* menggunakan *tools* Whatsapp Viewer. Alternatif untuk melakukan *decrypt database* Whatsapp dengan menggunakan *tools* berbasis python yaitu Whatsapp Crypt14 Crypt15 Decrypter. Hasil *decrypt* dari crypt14 juga tidak bisa dibuka menggunakan Whatsapp Viewer, untuk membukanya menggunakan DB Browser for SQLite. Proses analisis *file* aplikasi dengan cara *reverse engineering* atau juga disebut *decompile*. Proses tersebut berhasil mengetahui permission dan "*malicious*" *code* dari aplikasi tersebut. Hal yang didapati dari aplikasi tersebut yaitu aplikasi berbahaya tersebut bertujuan untuk mencuri data pribadi korban yang berupa SMS, data pribadi banyak ditemui dalam bentuk SMS yaitu kode OTP dari suatu bank. Pelaku kejahatan bisa mengakses rekening bank korban apabila telah berhasil mendapatkan kode OTP milik korban.

Berdasarkan tahapan-tahapan alur metode NIST yang dilakukan pada penelitian ini. Berhasil mendapatkan informasi dari hasil artefak yang ditemukan berupa sesi percakapan pelaku dan korban. Aplikasi berbahaya yang dikirimkan korban ke pelaku, dan yang terpenting sistem dari aplikasi berbahaya tersebut.

REFERENSI

Achmad Iqbal Yuladi, R. I., & ... (2021). Analisis dan Perbandingan Tools Forensik Menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber. *Jurnal Teknologi Terpadu …*, *8*(2), 86–93. https://www.academia.edu/download/92883068/233.pdf

Afzal, A., Hussain, M., Saleem, S., Shahzad, M. K., Ho, A. T. S., & Jung, K. H. (2021). Encrypted network traffic analysis of secure instant messaging application: A case study of signal messenger app. *Applied Sciences (Switzerland)*, *11*(17). https://doi.org/10.3390/app11177789

Al-Fawa'reh, M., Saif, A., Jafar, M. T., & Elhassan, A. (2020). Malware Detection by Eating a Whole APK. *2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020*, *February*. https://doi.org/10.23919/ICITST51030.2020.9351333

Albarida, N. G. W. S. H. A. A. (2020). Perbandingan analisis forensik digital aplikasi whatsapp messenger menggunakan metode NIST [Politeknik Harapan Bersama Tegal]. In *Politeknik Harapan Bersama Tegal* (Vol. 167, Issue 1). https://perpustakaan.poltektegal.ac.id/index.php?p=show_detail&id=4209930&keywords=

Anggraini, F., Herman, H., & Yudhana, A. (2023). Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(1), 89–96. https://doi.org/10.25126/jtiik.20231016416

Ardiningtias, S. R. A., Sunardi, S., & Herman, H. (2021). Investigasi Digital Pada Facebook Messenger Menggunakan National Institute of Justice. *Jurnal Informatika Polinema*, *7*(4), 19–26. https://doi.org/10.33795/jip.v7i4.709

Arista Yuliani, V., & Riadi, I. (2019). Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), 223–231. https://doi.org/10.17781/p002615

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), 125. https://doi.org/10.30595/techno.v21i2.8494

Krisnadi, D. S. I. (2020). Citra Forensik Dari Barang Bukti Elektronik Dengan Metode Physical Menggunakan Acquisition Tools Tableau Imager Dan Ftk Imager. *Academia*, 16. https://d1wqtxts1xzle7.cloudfront.net/64999902/Tableu_Imager_dan_FTK_Imager.pdf?1606003446=&response-content-disposition=inline%3B+filename%3DCitra_Forensik_dari_barang_bukti_elektro.pdf&Expires=1609391012&Signature=ggq3RFljWBmjsEj5dsc0ammrrNiznpH1oGNpK57

Mahendra, K. D. O., & Ari Mogi, I. K. (2021). Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases. *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, *9*(3), 381. https://doi.org/10.24843/jlk.2021.v09.i03.p09

Muhammad Abdul Aziz, Wicaksono Yuli Sulistyo, & Sri Rahayu Astari3. (2021). Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO). *JURISTIK (Jurnal Riset Teknologi Informasi Dan Komputer)*, *1*(01), 8–15. https://doi.org/10.53863/juristik.v1i01.341

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), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Riadi, I., Yudhana, A., & Barra, M. Al. (2021). Forensik Mobile pada Layanan Media Sosial LinkedIn. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *6*(1), 9–20. https://doi.org/10.14421/jiska.2021.61-02

Rifqi, M., Ismail, S. J. I., Rizal, M. F., Studi, P., Teknologi, D., & Telkom, U. (2023). Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute of Standard and Technology (Nist Sp 800-86). *E-Proceeding of Applied Science*, *9*(6), 3017–3022.

Saputra, A. D., & Borman, R. I. (2020). Sistem Informasi Pelayanan Jasa Foto Berbasis Android (Studi Kasus: Ace Photography Way Kanan). *Jurnal Teknologi Dan Sistem Informasi*, *1*(2), 87–94. https://doi.org/10.33365/jtsi.v1i2.420

Setyawan, M. R., Yudhana, A., & Fadlil, A. (2020). Data Acquisition On Messenger Skype Using The National Institute Of Justice Method. *Systemic: Information System and Informatics Journal*, *5*(2), 13–18. https://doi.org/10.29080/systemic.v5i2.724

Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *It Journal Research and Development*, *3*(1), 13–21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658

Zamroni, G. M., & Riadi, I. (2019). Instant Messaging Forensic Analysis on Android Operating System. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *4*(2), 137–148. https://doi.org/10.22219/kinetik.v4i2.735