TUGAS AKHIR

ANALISIS SERANGAN PHISING PADA WHATSAPP MENGGUNAKAN METODE DFRWS DAN END-TO-END FORENSICS: PERBANDINGAN KOMPLEKSITAS METODE

DISUSUN OLEH:

IHFANSYAH MAULANA

21106050071

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2025

SURAT PENGESAHAN TUGAS AKHIR

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2506/Un.02/DST/PP.00.9/12/2025

Tugas Akhir dengan judul : ANALISIS SERANGAN PHISING PADA WHATSAPP MENGGUNAKAN METODE DFRWS DAN END-TO-END FORENSICS: PERBANDINGAN KOMPLEKSITAS METODE

yang dipersiapkan dan disusun oleh:

Nama : IHFANSYAH MAULANA
Nomor Induk Mahasiswa : 21106050071
Telah diujikan pada : Selasa, 16 Desember 2025
Nilai ujian Tugas Akhir : A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 6944ea72d857f

Penguji I

Dr. Agung Fatwanto, S.Si., M.Kom.
SIGNED

Valid ID: 6944966020fe9

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 69443c9b1e63e

Yogyakarta, 16 Desember 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6944eeaf9149d2

SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Ihfansyah Maulana
NIM	: 21106050071
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi

Menyatakan dengan sesungguhnya, bahwa skripsi saya yang berjudul: Analisis Serangan Phising Pada Whatsapp Menggunakan Metode Dfrws Dan End-To-End Forensics: Perbandingan Kompleksitas Metode adalah hasil karya pribadi dan sepanjang pengetahuan penyusun tidak berisi materi yang dipublikasikan atau ditulis orang lain, kecuali bagian-bagian tertentu yang penulis ambil sebagai acuan pada tinjauan pustaka.

Apabila terbukti pernyataan ini tidak benar, maka sepenuhnya menjadi tanggungjawab penulis.

sember 2025

Inlansyah Maulana

SURAT PERSETUJUAN TUGAS AKHIR

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalammu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudari:

Nama	:	Ihfansyah Maulana
NIM	:	21106050071
Judul Skripsi	:	ANALISIS SERANGAN PHISING PADA WHATSAPP MENGGUNAKAN METODE DFRWS DAN END-TO-END FORENSICS: PERBANDINGAN KOMPLEKSITAS METODE

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudari dapat segera dimunaqasyahkan. Atas perhatiannya saya ucapkan terima kasih.

Wassalammu'alaikum wr. wb.

Yogyakarta, 10 Desember 2025
Pembimbing

Dr. Ir. Bambang Sugiantoro, M.T., IPU.,
ASEAN Eng.
19751024 200912 1 002

HALAMAN PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.

HALAMAN MOTO

”Allah tidak membebankan seseorang melainkan sesuai dengan kesanggupannya”
(Q.S. Al-Baqarah: 286)

“Demi masa. Sesungguhnya manusia itu benar-benar dalam kerugian, kecuali orang-orang yang beriman dan mengerjakan amal saleh dan nasehat menasehati supaya mentaati kebenaran dan nasehat menasehati supaya menetapi kesabaran.”
(QS. Al-‘Ashr: 1-3)

“Sesungguhnya bersama kesulitan ada kemudahan. Maka apabila engkau telah selesai (dari suatu urusan), tetaplah bekerja keras (untuk urusan yang lain), dan hanya kepada Tuhanmu lah engkau berharap”
(Q.S. Al-Insyirah : 6-8)

"Allah mengabulkan doa-doa ketika kita sudah siap, bukan ketika kita menginginkannya"
(KH. Ahmad Bahauddin Nursalim)

KATA PENGANTAR

Assalamu'alaikum wr wb.

Segala puji penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, dan karuniaNya, sehingga penulis dapat menyelesaikan tugas penulisan skripsi ini. Shalawat serta salam semoga selalu terlimpahkan kepada junjungan kita nabi Muhammad SWA, teladan seluruh umat yang telah membawa agama kebenaran dan keadilan yaitu agama islam, untuk dapat membedakan mana yang hak dan bathil sehingga kita masih bisa merasakan indahnya iman dan islam.

Penulisan skripsi ini bertujuan untuk memenuhi persyaratan untuk memperoleh gelar S.Kom, Program Studi Informatika, Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta, dengan judul **"(ANALISI SERANGAN PHISING PADA WHATSAPP MENGGUNAKAN METODE DRWS DAN END-TO-END FORENSICS:PERBANDINGAN KOMPLEKSITAS METODE)".**

Penulis memahami bahwa penyusunan skripsi ini tidak akan dapat terselesaikan dan terwujud tanpa adanya bantuan partisipasi banyak pihak. Untuk itu, penulis menyampaikan banyak terima kasih kepada:

1. Bapak Prof. Noorhaidi Hasan S.Ag., M.A., M.Phil., Ph.D. selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Ibu Prof. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Bapak Muhammad Mustakim, S.T. M.T., selaku Ketua Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
4. Bapak Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng., selaku dosen pembimbing skripsi yang telah meluangkan waktu untuk membantu dan mengarahkan selama proses penyusunan skripsi.
5. Bapak Eko Hadi Gunawan, M.Eng., selaku Dosen Pembimbing Akademik yang telah mengarahkan dan membantu selama proses perkuliahan.

6. Bapak dan Ibu Dosen Fakultas Sains dan Teknologi UIN Sunan Kalijaga yang telah memberikan banyak ilmu serta pengalamannya yang bermanfaat selama perkuliahan hingga pada akhirnya penulis dapat menyelasaikan studi di Program Studi Informatika.
7. Penulis ingin menyampaikan rasa terima kasih yang sedalam-dalamnya kepada kedua orang tua tercinta, Ayah dan Ibu, yang telah menjadi sumber semangat, doa, dan kasih sayang tanpa henti selama proses pendidikan ini. Ketulusan doa yang tak pernah putus, dukungan moral yang tak tergantikan, serta pengorbanan yang tak terhitung nilainya adalah kekuatan terbesar penulis dalam menempuh setiap langkah perjalanan akademik hingga tahap akhir ini.
8. Fadel, Rizal, Sava dan Hanif yang sudah menjadi teman belajar, pada menjelang akhir penyusunan penulisan tugas akhir ini yang selalu menemani, tidak lupa dengan Rokhman dan Kai yang sudah menajdi teman traveling, teman keluar beberapa bulan akhir ini hingga sekarang.
9. Teman-Teman seperjuangan Informatika angkatan 2021 Univeristas Islam Negeri Sunan Kalijaga.
10. Semua pihak yang tidak dapat penulis sebutkan satu persatu telah memberikan bantuan dan doa dalam proses penulisan skripsi ini.

Dengan menyadari adanya keterbatasan kemampuan dan pengetahuan yang penulis miliki, tentunya hasil skripsi ini jauh dari sempurna, oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi kesempuranaan skripsi ini dan semoga bermanfaat bagi kita semua. Amin.

Wassalamu'alaikum wr wb.

Yogyakarta, 15 Desember 2025

Penulis

Ihfansyah Maulana

NIM.21106050071

INTISARI

Perkembangan serangan phishing di platform *WhatsApp* menuntut analisis forensik digital yang efektif untuk mengungkap artefak bukti. Penelitian ini membandingkan kompleksitas penerapan metode DFRWS (*Digital Forensic Research Workshop*) dan *End-to-End Forensics* dalam menganalisis kasus phishing pada aplikasi WhatsApp, dengan metrik kompleksitas meliputi jumlah tahapan, waktu eksekusi, kebutuhan *tools*, dan tingkat skill investigator.

Pendekatan penelitian menggunakan simulasi skenario phishing berbasis Android, di mana artefak seperti *chat log*, metadata URL, dan *file* media diekstrak serta dibandingkan antar metode. Hasil menunjukkan bahwa metode DFRWS lebih komprehensif dengan 6 tahapan utama (*identification* hingga *presentation*), sedangkan *End-to-End Forensics* lebih linier namun memerlukan integrasi tools khusus untuk *tracing* lintas perangkat.

Penelitian ini berkontribusi secara praktis dengan memberikan panduan pemilihan metode forensik berdasarkan kompleksitas kasus phishing, serta secara akademis menyediakan baseline perbandingan untuk pengembangan *framework* forensik mobile di Indonesia.

Kata kunci: Phishing WhatsApp, DFRWS, End-to-End Forensics, Kompleksitas forensic, Analisis perbandingan, Artefak digital, Forensik mobile.

ABSTRACT

The The rise of phishing attacks on WhatsApp platforms necessitates effective digital forensic analysis to uncover evidentiary artifacts. This study compares the complexity of implementing the DFRWS (Digital Forensic Research Workshop) method and End-to-End Forensics in analyzing WhatsApp phishing cases, using complexity metrics such as the number of stages, execution time, tool requirements, and investigator skill levels.

The research approach employs Android-based phishing scenario simulations, extracting and comparing artifacts like chat logs, URL metadata, and media files between methods. Findings reveal that DFRWS is more comprehensive with six main stages (from identification to presentation), while End-to-End Forensics is more linear but requires specialized tools for cross-device tracing.

This research contributes practically by providing guidelines for method selection based on phishing case complexity and academically by establishing a baseline comparison for mobile forensic frameworks in Indonesia.

***Keywords**: WhatsApp phishing, DFRWS, End-to-End Forensics, Forensic complexity, Comparative analysis, Digital artifacts, Mobile forensic*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam Di era kemajuan teknologi saat ini, manusia semakin bergantung pada teknologi dan internet. Berbagai aktivitas kini didukung oleh teknologi dan internet, yang memberikan kemudahan dalam menyelesaikan pekerjaan. Jacques Ellul, seorang ahli filsuf dari Universitas Bordeaux, Teknologi memiliki kekuatan yang luar biasa dalam mengubah kebiasaan dan tata kehidupan manusia. [1]

Pandangan Jacques Ellul tentang teknologi memiliki kekuatan dalam mengubah kebiasaan dan kehidupan manusia. Teknologi tidak hanya berfungsi sebagai alat, tetapi telah menjadi sistem yang memiliki logika dan hukum sendiri. Ia memperkenalkan konsep "imperatif teknis" yang menunjukkan bahwa kemajuan teknologi memaksa masyarakat untuk terus berinovasi dan meningkatkan efisiensi tanpa mempertimbangkan dampak etis atau sosial. Dengan kata lain, teknologi mengubah struktur sosial dan cara manusia berinteraksi satu sama lain. Misalnya, kemajuan dalam komunikasi digital telah mengubah cara orang berinteraksi dan membentuk identitas mereka, sering kali tanpa disadari oleh individu itu sendiri.[2]

Menurut ISO (International Organization for Standardization), cyber security pada ISO/IEC 27032:2012 adalah standar internasional yang memberikan panduan dalam pengelolaan keamanan siber, khususnya dalam melindungi informasi yang berkaitan dengan internet. Standar ini membantu organisasi dalam menghadapi risiko keamanan siber dengan lebih efektif melalui pemahaman, pencegahan, dan respons yang tepat. Selain itu, ISO/IEC 27001 menetapkan sistem manajemen keamanan informasi (ISMS) yang berfokus pada tiga prinsip utama, yaitu kerahasiaan (Confidentiality), integritas (Integrity), dan ketersediaan (Availability), atau yang dikenal sebagai CIA Triad. Dengan menerapkan standar ini, organisasi dapat meningkatkan perlindungan terhadap data dan sistem mereka, menjaga privasi informasi, mengamankan jaringan dari ancaman, serta menyusun strategi tanggap darurat terhadap insiden siber. Implementasi ISO/IEC 27001 dan

ISO/IEC 27032 juga membantu organisasi dalam membangun kepercayaan pemangku kepentingan, mematuhi regulasi yang berlaku, serta meningkatkan daya saing di era digital yang semakin kompleks. Jadi, cyber security atau keamanan siber merupakan tindakan untuk melindungi informasi di dunia maya dari aneka serangan. Cyber security makin populer berhubung makin banyaknya penggunaan komputer seperti desktop, laptop, smartphone, server, dan perangkat IoT (internet of things) serta penggunaan jaringan komputer seperti internet dalam kehidupan umat manusia sehari-hari.[3]

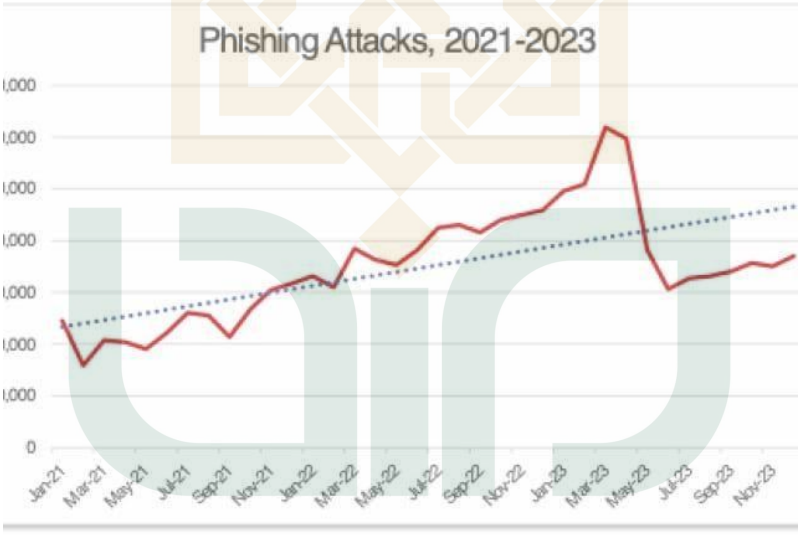
Gambar 1 kerugian kejahatan siber

kerugian kejahatan siber

Berdasarkan data Statista, kerugian akibat kejahatan siber di dunia diperkirakan mencapai US$8,15 triliun atau sekitar Rp127.466 triliun (kurs Rp15.640/US$) pada 2023. Angka tersebut meningkat 15,1% dibanding tahun sebelumnya sebesar US$7,08 triliun. Statista juga memproyeksikan kerugian dari kejahatan siber akan meningkat hampir dua kali lipat menjadi US$13,82 triliun pada lima tahun yang akan datang atau pada 2028. Di era digital yang terus berkembang, ancaman keamanan siber semakin rumit dan mengkhawatirkan. Salah

satu ancaman yang paling sering terjadi dan merugikan adalah serangan phishing. Pelaku phishing, yang dikenal sebagai phisher, menggunakan teknik penipuan online untuk mendapatkan informasi sensitif seperti kata sandi, data keuangan, atau informasi pribadi. Kata "phishing" sendiri berasal dari bahasa Inggris "fishing," yang berarti memancing, karena metode ini berusaha menipu korban dengan menyamar sebagai pihak yang tepercaya.[4]

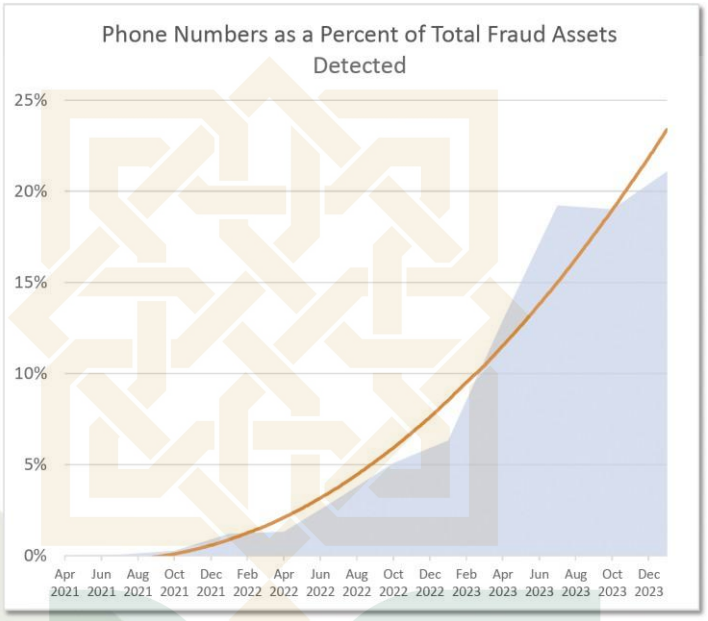
Serangan phishing dapat mengakibatkan kerugian finansial, pencurian identitas, serta kebocoran data yang berdampak negatif bagi korbannya. Berdasarkan hasil survei yang dilakukan oleh APWG (Anti-Phishing Working Group) dari April 2022 hingga Maret 2023, data mengenai serangan phishing dapat dilihat pada gambar berikut.



Gambar 2 Laporan aktivitas Phising

Laporan Tren Aktivitas Phishing Q4 2023 mengungkapkan bahwa pada tahun 2023 terjadi hampir lima juta serangan phishing, menjadikannya tahun terburuk dalam sejarah untuk serangan phishing. Meskipun sempat mengalami penurunan pada kuartal kedua, jumlah serangan kembali meningkat di akhir tahun, dengan 1.077.501 serangan phishing tercatat hanya dalam kuartal keempat 2023. Pada Q4 2023, anggota pendiri APWG, OpSec Security, menemukan bahwa serangan phishing terhadap platform media sosial meningkat pesat, mencakup 42,8% dari total serangan, naik drastis dari 18,9% pada Q3 2023. Sementara itu,

serangan phishing terhadap lembaga keuangan justru menurun dari 24,9% pada Q3 menjadi 14% pada Q4. APWG juga melakukan penelitian pada jumlah kasus phising pada handphone. Data pada kurva Activity Trends Report berikut merupakan laporan yang didapat oleh APWG.



Gambar 3 Laporan serangan Phising

Pada laporan diatas diketahui bahwa serangan phishing yang menggunakan panggilan telepon (*vishing*) dan pesan teks (*smishing*) terus meningkat dalam dua tahun terakhir. Perkembangan ini menunjukkan bahwa ancaman kejahatan siber semakin bergeser ke penyalahgunaan layanan dan infrastruktur telekomunikasi. Pada Q1 2024, lebih dari 20% aset yang terkait dengan penipuan yang teridentifikasi oleh OpSec Security merupakan nomor telepon yang digunakan untuk kegiatan kriminal. Selama Q1 2024, APWG mencatat 963.994 serangan phishing. Setelah mengalami lonjakan pada awal 2023, jumlah serangan phishing per bulan stabil dari Juni 2023 hingga Maret 2024. Sektor yang paling sering menjadi target adalah platform media sosial, yang mencakup 37,4% dari total serangan phishing. Perusahaan perangkat lunak berbasis layanan (SaaS) dan webmail menjadi target kedua dengan 21% dari total serangan. Sementara itu, serangan terhadap sektor perbankan terus menurun, mencapai hanya 9,8% di Q1 2024. Umumnya informasi yang dicari phisher adalah berupa username, password,

baik itu akun media sosial atau akun nomor kartu kredit dengan cara diarahkan ke sebuah situs website palsu.[5]

Dalam upaya mendeteksi web phishing, meningkatnya ketergantungan manusia pada teknologi dan internet menegaskan pentingnya pengembangan metode deteksi phishing yang efektif dan terpercaya. Seiring dengan semakin seringnya penggunaan teknologi untuk komunikasi, transaksi, dan akses informasi, risiko menjadi korban serangan phishing juga semakin besar. Oleh karena itu, diperlukan sistem deteksi web phishing yang mampu melindungi pengguna dari pencurian informasi pribadi. Sistem ini harus dapat mengidentifikasi dan mengklasifikasikan situs web, apakah tergolong sebagai phishing atau aman untuk diakses.[6]

Untuk mengklasifikasikan url website yang merupakan link phishing atau tidak dapat menggunakan beberapa metode Forensik digital. Ada banyak metode klasifikasi pada Forensik digital yang dapat digunakan diantaranya adalah Digital Forensic Research Workshop (DFRWS) dan End-to-End Forensic (E2EF). Dari penelitian yang telah dilakukan oleh (Biaq Widari Datu Samara, Ahmad Subki, M.Zulpahmi, Lalu Delsi Samsumar) dengan judul *Analisis Forensik Aplikasi Telegram Menggunakan Metode Digital Forensics Research Workshop* Peneliti menganalisis artefak forensik pada aplikasi Telegram untuk mengungkap bukti kejahatan siber, fokus pada pesan terenkripsi, file terkirim, dan aktivitas penipuan di platform pesan instan tersebut. Bukti yang berhasil diperoleh antara lain: Berhasil mengekstrak bukti end-to-end termasuk pesan terenkripsi (dengan kunci dekripsi dari perangkat), file media penipuan, dan timeline aktivitas pelaku-korban.

Dengan membandingkan kinerja berbagai metode klasifikasi dalam deteksi phishing web, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem keamanan siber yang lebih kuat dan efektif. Pemahaman yang lebih mendalam mengenai fitur-fitur utama yang membedakan situs phishing dari situs asli, serta kelebihan dan kekurangan masing-masing metode, akan membantu praktisi keamanan siber dalam mengambil langkah-

langkah yang lebih tepat untuk melindungi pengguna internet dari ancaman phishing.

Selain itu, penelitian ini juga memberikan wawasan lebih lanjut mengenai interaksi antara manusia dan teknologi dalam konteks keamanan siber. Kemajuan teknologi memang membawa banyak manfaat, tetapi juga menghadirkan tantangan baru yang perlu diatasi. Dengan memahami hubungan ini secara lebih menyeluruh, penulis dapat mengembangkan solusi yang lebih efisien dan berkelanjutan dalam menghadapi ancaman keamanan siber di era digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, permasalahan yang dijadikan objek pada penelitian ini adalah sebagai berikut :

1. Bagaimana perbandingan tingkat Kompleksitas Teknis antara Metode DFRWS dan Metode End-to-End Forensics dalam akuisisi bukti digital pada *platform* WhatsApp?
2. Bagaimana hasil dari kedua metode tersebut (dfrws dan end-to-end) dalam menangani kasus jenis smishing (simulasi kasus) yang diterapkan untuk mengetahui manakah metode yang paling unggul?

1.3 Batasan Masalah

Adapun Batasan masalah pada projek penyediaan layanan private cloud ini objek dibatasi dengan ruang lingkup sebagai berikut :

1. Penelitian hanya mencakup serangan phishing yang dilakukan melalui pesan di platform WhatsApp, tanpa melibatkan media sosial lain seperti Telegram, Facebook atau Instagram.
2. Objek Perangkat (*Device*): Penelitian ini hanya menggunakan perangkat smartphone berbasis Android dalam kondisi standar pabrik (**Non-Rooted**). Penelitian tidak mencakup perangkat iOS atau Android yang telah dimodifikasi hak aksesnya (*Rooted*).

3. Jenis Serangan: Simulasi serangan dibatasi pada teknik Social Engineering dengan metode Phishing. Modus yang digunakan adalah penyebaran tautan palsu (*Fake Link*) terkait bantuan sosial melalui aplikasi pesan instan WhatsApp. Penelitian ini tidak membahas penyisipan *malware*, *keylogger*, atau *virus*.
4. Metode Analisis: Analisis forensik difokuskan pada perbandingan Kompleksitas dan Efektivitas antara dua metode, yaitu:
    a. DFRWS (Digital Forensic Research Workshop) untuk analisis artefak penyimpanan internal.
    b. End-to-End Forensics untuk analisis visual dan lalu lintas jaringan.
5. Lingkungan Jaringan: Simulasi situs *phishing* dibangun menggunakan bahasa pemrograman Python dan dijalankan pada lingkungan jaringan lokal/terkontrol (*Localhost*) atau *Port Forwarding*. Analisis lalu lintas jaringan difokuskan pada protokol HTTP untuk pembuktian konsep (*Proof of Concept*) pencurian data.
6. Perangkat Lunak (*Tools*): *Tools* forensik yang digunakan dibatasi pada perangkat lunak *Open Source* atau *Freeware*, antara lain: FTK Imager (Akuisisi Data), DB Browser for SQLite (Analisis Database), Wireshark (Analisis Jaringan), dan layanan URL Expander berbasis web.
7. Serangan phishing yang disimulasikan terbatas pada skema Penipuan Penyamaran Instansi Pemerintah (Government Impersonation Scam) menggunakan media pesan teks, tautan (link), dan file media (pamflet/gambar). Jenis serangan lain (seperti Malware, Smishing, atau Spear Phishing tingkat lanjut) tidak dianalisis.

Eksperimen akan dilakukan dengan menggunakan 2 buah akun simulasi untuk menghindari risiko etika dan hukum dalam penyelidikan forensik.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian Analisis Serangan Phishing di WhatsApp Menggunakan Metode DFRWS dan End-to-End Forensics: Perbandingan tingkat Kompleksitas Teknis antara Metode DFRWS dan Metode End-to-End Forensics dalam akuisisi bukti digital pada *platform* WhatsApp sebagai berikut:

1. Menilai keefektifan dari kedua metode antara Metode DFRWS dan End-to-End Forensics serta hasil apa saja yang diperoleh dari masing-masing metode untuk mengidentifikasi dampak dari Phising.
2. Menganalisis implikasi dan tantangan teknis spesifik yang ditimbulkan oleh karakteristik enkripsi dan struktur penyimpanan data WhatsApp terhadap penerapan dan hasil dari kedua metodologi forensik (DFRWS dan End-to-End).

1.5 Manfaat Penelitian

Penelitian Analisis Serangan Phishing di WhatsApp Menggunakan Metode DFRWS dan End-to-End Forensics: Perbandingan tingkat Kompleksitas Teknis antara Metode DFRWS dan Metode End-to-End Forensics dalam akuisisi bukti digital pada *platform* WhatsApp, manfaatnya antara lain:

1. Menerapkan metode DFRWS dan End-to-End Forensics dalam investigasi forensik serangan phishing. Khususnya karena DRWS sangat popular sebagai metode yang sering digunakan dalam mengidentifikasi kasus diaplikasi pesan instan.
2. Memberikan panduan dalam memilih metode investigasi yang tepat. Jika kasus membutuhkan kecepatan bukti, *End-to-End* lebih direkomendasikan. Jika kasus membutuhkan integritas data mendalam pasca-kejadian, DFRWS tetap diperlukan meski dengan kompleksitas tinggi.
3. Menyediakan studi komparatif empiris yang mendalam mengenai efektivitas dan batasan dua metodologi forensik digital (DFRWS vs. End-to-End Forensics) pada lingkungan messaging modern. Penelitian ini

mengisi kekosongan literatur terkait perbandingan kedua metode ini secara langsung dalam satu kasus yang terstruktur.

4. Meningkatkan kesadaran keamanan informasi (*Security Awareness*) dengan menunjukkan betapa mudahnya data pribadi dicuri jika pengguna mengakses tautan berbahaya, serta pentingnya mengenali ciri-ciri *link phishing*.

Memberikan rekomendasi kepada para seorang dibidang terkait metode forensik digital yang lebih efektif dalam menangani kasus phishing di aplikasi pesan instan pada whatsapp.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil simulasi serangan *phishing* dan analisis forensik yang telah dilakukan menggunakan metode *Digital Forensic Research Workshop* (DFRWS) dan *End-to-End Forensics*, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Keberhasilan Simulasi Serangan Skenario serangan menggunakan teknik *Social Engineering* melalui WhatsApp dan situs web palsu (*Fake Web*) yang berjalan pada server lokal terbukti efektif dalam mengelabui korban. Penggunaan teknik *URL Shortening* dan *Typosquatting* berhasil menyamarkan identitas server penyerang, sehingga korban bersedia memasukkan data pribadi (NIK dan data pribadi).
2. Kompleksitas Metode DFRWS (Tinggi) Penerapan metode DFRWS pada perangkat Android non-root memiliki tingkat kompleksitas yang tinggi. Kendala utama ditemukan pada tahap *Collection* dan *Analysis*. Peneliti harus melakukan navigasi manual ke dalam sistem file yang tersembunyi karena keterbatasan alat forensik standar (FTK Imager) dalam membaca protokol MTP. Selain itu, enkripsi *End-to-End* pada database WhatsApp (msgstore.db.crypt) menjadi hambatan terbesar, di mana isi percakapan tidak dapat dibaca tanpa kunci dekripsi (*Key*) yang hanya dapat diakses melalui hak akses *Root*. Hal ini membuat metode DFRWS kurang efektif untuk investigasi cepat pada perangkat standar.

3. Kompleksitas Metode End-to-End Forensics (Rendah) Metode *End-to-End Forensics* terbukti memiliki kompleksitas yang lebih rendah dan efisiensi yang lebih tinggi. Metode ini tidak terkendala oleh enkripsi database internal karena berfokus pada bukti visual (*Visual Evidence*) dan lalu lintas jaringan. Penggunaan *Network Sniffer* (Wireshark) berhasil menangkap data kredensial korban yang dikirimkan melalui protokol HTTP dalam format teks jelas (*Plaintext*). Metode ini sangat direkomendasikan untuk penanganan insiden (*Incident Response*) yang membutuhkan pembuktian pencurian data (*Data Exfiltration*) secara *real-time*.
4. Metode End-to-End Forensics lebih unggul karena mampu memberikan jawaban langsung mengenai apa data yang dicuri dan ke mana data tersebut dikirim (IP 156.59.238.3) tanpa harus melakukan prosedur *rooting* yang berisiko merusak barang bukti.

5.2 Saran

Berdasarkan kendala dan temuan selama penelitian berlangsung, peneliti mengajukan beberapa saran untuk pengembangan penelitian selanjutnya dan mitigasi keamanan:

1. Bagi Peneliti Selanjutnya:

Disarankan untuk melakukan penelitian serupa menggunakan perangkat *Rooted* (yang telah di-root). Hal ini bertujuan untuk membandingkan apakah metode DFRWS menjadi lebih efektif jika peneliti memiliki akses penuh untuk mengambil kunci dekripsi (*Decryption Key*) database WhatsApp.

Dapat mengembangkan skenario serangan menggunakan protokol HTTPS (SSL/TLS) untuk menguji seberapa sulit metode *End-to-End Forensics* (Wireshark) dalam membedah paket data yang terenkripsi jaringan.

2. Bagi Masyarakat (Pengguna):

Masyarakat dihimbau untuk tidak mudah percaya pada tautan pendek (*shortlink*) yang dikirimkan melalui pesan instan, meskipun mengatasnamakan instansi resmi. Pentingnya melakukan verifikasi URL menggunakan alat pelacak tautan (*Link Expander*) sebelum mengklik tautan yang mencurigakan.

3. Bagi Pengembang Aplikasi:

Disarankan bagi pengembang aplikasi pesan instan untuk meningkatkan keamanan dengan membatasi pratinjau tautan (*link preview*) dari domain yang tidak dikenal untuk meminimalisir dampak *Social Engineering*.

DAFTAR PUSTAKA

[1] I. D. Purwanti and B. Istiyanto, "PERAN MEDIA SOSIAL, INFLUENCER, DAN KEBUDAYAAN MELALUI PERILAKU KONSUMTIF TERHADAP KEPUTUSAN PEMBELIAN MENGGUNAKAN VARIABEL INTERVENING PADA PRODUK BTS MEAL," *Sci. J. Reflect. Econ. Account. Manag. Bus.*, vol. 5, no. 2, pp. 210–222, Apr. 2022, doi: 10.37481/sjr.v5i2.456.

[2] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)'," *J. Telekomun. Dan Komput.*, vol. 9, no. 3, p. 186, 2020.

[3] L. W. Evelina and F. Handayani, "Penggunaan Digital Influencer dalam Promosi Produk (Studi Kasus Akun Instagram @bylizzieparra)," *War. ISKI*, vol. 1, no. 01, p. 71, Jan. 2018, doi: 10.25008/wartaiski.v1i01.10.

[4] F. G. P. Zamsari and T. Wahyono, "Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST," *J. Ecotipe Electron. Control Telecommun. Inf. Power Eng.*, vol. 11, no. 1, Art. no. 1, Apr. 2024, doi: 10.33019/jurnalecotipe.v11i1.4489.

[5] M. Fadli, D. Widijowati, and D. Andayani, "Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi," *Co-Value J. Ekon. Kop. Dan Kewirausahaan*, vol. 14, no. 12, May 2024, doi: 10.59188/covalue.v14i11.4335.

[6] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime'," *Cyber Secur. Dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020.

[7] A. Trianurahmah, A. Fauzi, E. N. Tyas, M. Afif, M. Rizky, and P. Wibisono, "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising Dengan Modus Berbasis Linkenter 1 x".

[8] A. Yudhana, Imam Riadi, and Budi Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," *J. RESTI Rekayasa Sist.*

Dan Teknol. Inf., vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.

[9] R. E. Endeley, "End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger," *J. Inf. Secur.*, vol. 09, no. 01, pp. 95–99, 2018, doi: 10.4236/jis.2018.91008.

[10] M. M. Undari Sulung, "Volume 5, Nomor 3, September 2024," *Sept. 2024*, vol. 5, 2024.

[11] I. Riadi, A. Fadlil, and M. I. Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)'," *J. RESTI Rekayasa Sist. Dan Teknol. Inf.*, vol. 1, no. 10, pp. 820–828, 2021.

[12] D. Irawan, "MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING," *JIKI J. Llmu Komput. Lnformatika*, vol. 1, no. 1, pp. 43–46, July 2020, doi: 10.24127/jiki.v1i1.671.