

Analisis dan Recovery Bukti Digital pada Media Sosial di Perangkat Mobile Berbasis Android

Rendi Prasetyawan¹, Rini Indrayani²

Universitas Amikom Yogyakarta¹, Universitas Muhammadiyah Palopo²

rendi.prasetyawan@students.amikom.ac.id¹, riniindrayani@umpalopo.ac.id²

Abstrak – Penggunaan dan perkembangan media sosial berbasis internet yang cepat memberikan dampak yang baik bagi pengguna sebagai fasilitas untuk dapat berkomunikasi jarak jauh dan dapat diakses melalui genggaman ponsel android yang sangat praktis. Namun tentu saja sisi positif tersebut diikuti dengan isu kejahatan cyber. Penanggulangan terhadap tindak kejahatan di media sosial dapat dilakukan dengan memperbanyak literasi tentang cyber security tetapi apabila terjadi tindak kejahatan serius yang merugikan perlu dilakukan tindakan pemeriksaan untuk keperluan proses hukum dan pembelajaran. Salah satu Tindakan lanjutan yang dibutuhkan dalam tindakan pemeriksaan tersebut adalah forensik digital. Melakukan tindakan Mobile Forensik dan Digital Forensik untuk analisis bukti digital tindak kejahatan cyber akan meningkatkan persentase penemuan bukti yang konkret untuk membantu pihak berwajib dalam mengambil keputusan terhadap kasus kejahatan cyber. Penelitian ini mengangkat permasalahan yang sering ditemui pada proses forensik digital mengenai pencarian bukti-bukti digital pada kasus tertentu menggunakan framework forensik National Institute of Justice (NIJ). Penelitian ini menggunakan 2 aplikasi media social populer yaitu WhatsApp dan Line yang diujikan. Hasil yang didapatkan dari penelitian ini menunjukkan bahwa aplikasi media sosial pada perangkat android dalam keadaan UnRoot memiliki persentase yang rendah dalam penemuan bukti digital yaitu 40% untuk aplikasi WhatsApp dan 30% pada aplikasi Line sedangkan pada perangkat android yang telah dilakukan Root maka persentase keberhasilan meningkat pesat menjadi 90% pada masing-masing aplikasi berdasarkan skenario yang telah ditentukan.

Kata kunci: Forensik digital; Forensik Mobile; Bukti digital; NIJ;

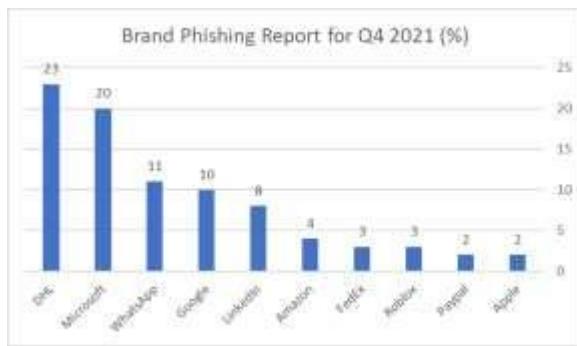
Abstract - The rapid use and development of internet-based social media has a good impact on users as a facility to communicate remotely and can be accessed via a very practical Android phone grip. But the positive side is followed by the issue of cyber crime. Countermeasures against crimes on social media can be carried out by increasing literacy about cyber security, but if a serious crime occurs that is detrimental, it is necessary to carry out inspection actions for the purposes of the legal process and learning. One of the follow-up actions needed in the inspection is digital forensics. Carrying out Mobile Forensic and Digital Forensic actions to analyze digital evidence of cyber crimes will increase the percentage of finding concrete evidence to assist the authorities in making decisions on cyber crime cases. This study raises issues that are often encountered in digital forensic processes regarding the search for digital evidence in certain cases using the National Institute of Justice (NIJ) forensic framework. This study used 2 popular social media applications, namely WhatsApp and Line, which were tested. The results obtained from this study indicate that social media applications on Android devices in the UnRoot state have a low percentage of digital evidence discovery, namely 40% for the WhatsApp application and 30% for the Line application, while for Android devices that have been rooted, the percentage of success increases rapidly to 90% for each application based on predetermined scenarios.

Keyword : Digital Forensic; Mobile Forensic; Digital Evidence; NIJ;

1. Latar Belakang

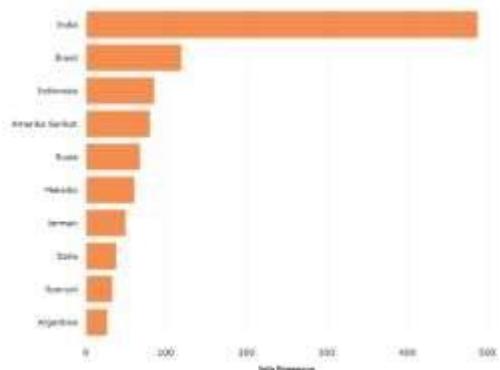
Penggunaan dan perkembangan media sosial berbasis internet yang cepat memberikan dampak yang baik bagi pengguna sebagai fasilitas untuk dapat berkomunikasi jarak jauh dan dapat diakses melalui genggaman ponsel android yang sangat praktis[1]. Namun tentu saja sisi positif tersebut diikuti dengan isu keamanan data seperti pencurian data. Menurut Check Point Research (CPR) yang

telah menerbitkan Brand Phishing Report for Q4 2021 terdapat beberapa aplikasi dari brand teratas dengan tingkat upaya pencurian data pribadi melebihi 10%, yaitu DHL, Microsoft dan pada posisi ketiga teratas terdapat brand WhatsApp yang menyediakan layanan media sosial dengan upaya pencurian data hingga 11%. Pada Gambar 1 dapat dilihat 10 brand dengan upaya pencurian data tertinggi [2].

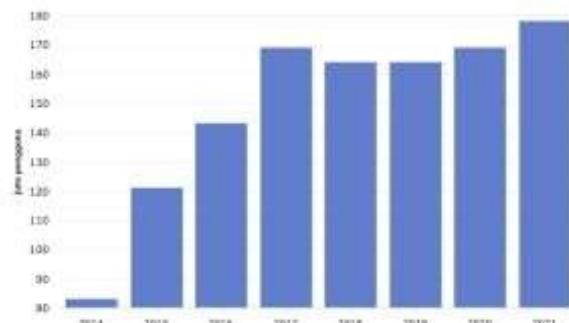


Gambar 1. Brand Phising Report for Q4 2021[2]

Hal ini sejalan dengan popularitas WhatsApp sebagai salah satu aplikasi yang paling diminati. Penggunaan media sosial jenis WhatsApp menempati posisi ketiga didunia terbanyak dengan pengguna lebih dari seratus juta pengguna aktif pada tahun 2021 [3]. Tidak hanya aplikasi WhatsApp saja yang popular di Indonesia, aplikasi yang juga populer di Indonesia adalah Line Messenger dengan pengguna aktif pada tahun 2021 mencapai 178 juta[4]. Grafik pengguna WhatsApp dapat dilihat pada gambar 2, sedangkan grafik pengguna Line dapat dilihat pada gambar 3.



Gambar 2. Negara pengguna WhatsApp terbanyak[3]



Gambar 3. Pengguna Line di Indonesia[4]

Oleh karena itu, selain aplikasi WhatsApp yang memiliki catatan 11% upaya pencurian data, aplikasi Line juga perlu diwaspadai karena kepopulerannya dengan jumlah pengguna yang mencapai 178 juta[4].

Penanggulangan terhadap tindak kejahatan di media sosial dapat dilakukan dengan memperbanyak literasi tentang cyber security tetapi apabila terjadi tindak kejahatan serius yang merugikan perlu dilakukan tindakan pemeriksaan untuk keperluan proses hukum dan pembelajaran. Salah satu tindakan lanjutan yang dibutuhkan dalam tindakan pemeriksaan tersebut adalah forensik digital. Forensik digital khususnya *mobile forensic* dapat membantu menemukan bukti digital dari device korban dan device pelaku kejahatan cyber[5]. Melakukan tindakan Mobile Forensik dan Digital Forensik untuk analisis bukti digital tindak kejahatan cyber akan meningkatkan persentase penemuan bukti yang konkret untuk membantu pihak berwajib dalam mengambil keputusan terhadap kasus kejahatan cyber.

2. Kajian Pustaka

Beberapa penelitian mengenai analisis forensik digital pada aplikasi WhatsApp messenger antara lain mengenai penelitian dengan menggunakan metode NIST SP 800-86 dan menerapkan beberapa skenario pada objek perangkat android dan IOS untuk mendapatkan database dari kedua sistem operasi tersebut. Penelitian tersebut menggunakan aplikasi/tools pendukung pada proses akuisisi data menggunakan tools XRY version 8.0.0 dan Encase Mobile Forensic version 8.09.00.192. Hasil database berhasil didapatkan walaupun perangkat tidak dalam keadaan root[6]. Sebuah penelitian lain terkait analisis forensik digital membahas mengenai penggunaan *framework* NIJ (National Institute of Justice) untuk melakukan recovery data digital pada perangkat berbasis android, hasil dari penelitiannya berhasil melakukan recovery data pada perangkat smartphone android, namun data yang telah dihapus tidak dapat berhasil melewati proses *recovery*[7].

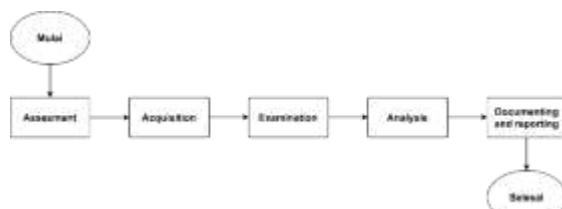
Selain pada aplikasi WhatsApp, terdapat penelitian pada aplikasi media sosial instant messaging lain yaitu Line Messenger dengan tujuan untuk menemukan bukti digital dari tindak pidana cyberbullying dan kasus cybercrime menggunakan *framework* NIST (National Institute of Standards and Technology). Penelitian ini menerapkan skenario dimana terjadi percakapan 2 orang yang memuat tindakan *cyberbullying*. Penelitian ini menggunakan beberapa tools tambahan yang digunakan pada proses akuisisi dan proses *rooting* pada ponsel. Tools *rooting* menggunakan ZenFone RootKit dan pada proses akuisisi menggunakan tools tambahan AFLLogical OSE. Penelitian ini

menggunakan *device* yang telah mengalami proses *root* dimana hasilnya menunjukkan bahwa bukti-bukti percakapan dapat ditemukan[8]. Penelitian pada aplikasi Line juga sebelumnya dilakukan terkait penyalahgunaan aplikasi pesan singkat sebagai tempat broadcast berita HOAX dan membuat group terselubung. Permasalahan skenario utama yang diangkat adalah seringnya terjadi *personal chat* atau *chatting* yang berpotensi merusak nama baik seseorang dengan barang bukti ponsel android korban yang memuat bukti-bukti. Penelitian ini dilakukan dengan objek perangkat smartphone berbasis android dan menggunakan metode NIST (National Institute of Standards and Technology). Tools tambahan yang digunakan pada penelitian ini adalah SQLITE DB Browser berfungsi untuk membaca database hasil akuisisi dan mendapatkan hasil barang bukti digital berupa database yang berisi pesan, riwayat panggilan, gambar dan media lainnya[9].

3. Perancangan Sistem / Metode Penelitian

a. Framework

Framework yang digunakan dalam penelitian ini adalah analisis forensik National Institute of Justice (NIJ). *Framework* ini membantu menjelaskan tahapan investigasi yang dilakukan sehingga dapat menyelesaikan proses investigasi secara sistematis dan menggunakannya sebagai panduan untuk menyelesaikan skenario yang ada. Melakukan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data forensik[10]. *Framework* National Institute of Justice (NIJ) mempunyai tahapan Assesment, Acquisition, Examination, Analysis, dan Documenting and Reporting[6]. Tentunya setiap tahapan memiliki proses masing-masing. Tahapan-tahapan dapat dilihat pada gambar 4.



Gambar 4. Framework NIJ

b. Objek Penelitian

Penelitian ini berfokus pada *recovery* dan analisis bukti digital menggunakan ponsel

android *Unroot* dengan jenis Samsung Galaxy J2 PRIME yang mempunyai system operasi Android Marshmello dengan versi 6.0.1 dan perangkat *Root* dengan *device* yang sama. Proses penelitian dilakukan pada device UnRoot dan dilanjutkan pada perangkat Root. Visual fisik objek penelitian yang digunakan ditunjukkan pada gambar 5, sedangkan spesifikasi lengkap mengenai ponsel yang digunakan sebagai objek penelitian dapat dilihat pada tabel 1.



Gambar 5. Objek Penelitian

Tabel 1. Spesifikasi Objek Penelitian

Spesifikasi	Keterangan
Jenis Ponsel	Samsung Galaxy J2 Prime
Nomor Model	SM-G532G/DS
Versi Android	6.0.1
RAM	1.5 GB
Storage	8 GB
Nomor Versi	MMB29T.G532GDXU1ASA5

c. Alur Komunikasi

Penelitian ini melakukan uji skenario dimana terjadi komunikasi antara korban dan pelaku dengan menggunakan kedua media sosial masing-masing. Komunikasi memuat percakapan sesuai dengan skenario yang telah ditentukan. Proses *recovery* data dan analisis dilakukan pada ponsel korban untuk menemukan bukti digital. Alur komunikasi yang digunakan korban dan pelaku pada aplikasi Whatsapp ditunjukkan pada gambar 6, sedangkan alur komunikasi pada aplikasi Line ditunjukkan pada gambar 7.



Gambar 6. Alur Komunikasi pada WhatsApp



Gambar 7. Alur Komunikasi pada Line

c. Skenario Penelitian

Penelitian ini menggunakan 10 skenario yang terinspirasi dari hal-hal yang sering terjadi pada pengguna media sosial khususnya pada aplikasi WhatsApp dan Line. Penggunaan skenario ini ditujukan untuk memudahkan dalam memahami alur penelitian Recovery Bukti Digital pada aplikasi media sosial WhatsApp dan Line. Setiap skenario diujikan pada kedua aplikasi WhatsApp dan Line untuk mendapatkan bukti digital untuk dianalisis. 10 skenario yang digunakan ditunjukkan pada tabel 2.

Tabel 2. Tabel Skenario Penelitian

Skenario	Skenario	Bentuk Data
Skenario 1	Memulihkan database pada aplikasi tersebut	File Database
Skenario 2	Nama akun atau nomor yang digunakan	Teks
Skenario 3	Daftar kontak	Teks
Skenario 4	Group chat	Teks
Skenario 5	Mengirim pesan personal chat antara pelaku dan korban	Teks
Skenario 6	Mengirim pesan gambar	Gambar
Skenario 7	Mengirim pesan berupa video	Video
Skenario 8	Mengirim pesan suara (Voice note)	Audio
Skenario 9	Mengirim pesan berupa dokumen	Document
Skenario 10	Call History	Teks

Hasil penelitian dijabarkan menggunakan 2 kategori keadaan objek penelitian yaitu *Root* dan *Unroot*. Kedua kondisi tersebut diimplementasikan pada kedua aplikasi yaitu WhatsApp dan Line berdasarkan skenario yang telah ditentukan untuk mendapatkan bukti digital. Hasil perbandingan pengujian pada device *Root* dan *Unroot* dapat dilihat pada tabel 3.

Tabel 3. Tabel Hasil Analisis Root dan Unroot

Skenario	WhatsApp		Line	
	UnRooted	Rooted	UnRooted	Rooted
Skenario 1	-	✓	-	✓
Skenario 2	-	✓	-	✓
Skenario 3	-	✓	-	✓
Skenario 4	-	✓	-	✓
Skenario 5	-	✓	-	✓
Skenario 6	✓	✓	✓	✓
Skenario 7	✓	✓	✓	✓
Skenario 8	✓	✓	✓	✓
Skenario 9	✓	✓	-	-
Skenario 10	-	-	-	✓

Hasil pengujian berdasarkan tabel 3 menunjukkan bahwa pada kondisi *Unroot* lebih banyak ditemukan bukti digital pada aplikasi WhatsApp. Sedangkan pada kondisi *Root*, persentase jumlah bukti digital yang dihasilkan adalah sama. Persentase perbandingan ini dapat dirumuskan dengan persamaan berikut.

$$R = \frac{S}{V} \times 100\%$$

Keterangan :

- R = Persentase Perolehan Barang Bukti
- S = Skenario yang berhasil
- V = Jumlah variable skenario

Hasil perhitungan persentase tersebut ditunjukkan pada tabel 4 dan tabel 5.

4. Implementasi Sistem dan Hasil

Tabel 4. Persentase Hasil Pengujian Unroot

WhatsApp	Line
$R^1 = \frac{S}{V} \times 100\%$	$R^2 = \frac{S}{V} \times 100\%$
$R^1 = \frac{4}{10} \times 100\%$	$R^2 = \frac{3}{10} \times 100\%$
$R^1 = 40\%$	$R^2 = 30\%$

Tabel 5. Persentase Hasil Pengujian Root

WhatsApp	Line
$R^1 = \frac{S}{V} \times 100\%$	$R^2 = \frac{S}{V} \times 100\%$
$R^1 = \frac{9}{10} \times 100\%$	$R^2 = \frac{9}{10} \times 100\%$
$R^1 = 90\%$	$R^2 = 90\%$

5. Kesimpulan

Berdasarkan analisis dari pengujian skenario yang dilakukan untuk mendapatkan bukti digital pada aplikasi WhatsApp dan Line dengan device dalam keadaan Root maupun UnRoot, maka diperoleh kesimpulan bahwa bukti digital yang didapatkan dari penerapan seluruh skenario pada device UnRoot sebesar 40% atau hanya menemukan 4 bukti digital dari 10 skenario di aplikasi WhatsApp dan 30% atau hanya menemukan 3 dari 10 skenario yang diterapkan di aplikasi Line. Sementara pada device yang tidak dalam keadaan Root cenderung sulit untuk mengakses atau menemukan bukti-bukti digital dari 10 skenario yang telah diterapkan. Bukti digital lebih banyak ditemukan pada perangkat Root dengan Total 90% pada aplikasi WhatsApp atau ditemukan 9 bukti digital dari 10 skenario yang telah diterapkan dan pada aplikasi Line penemuan bukti digital dengan total 90% yaitu mendapatkan 9 bukti digital dari 10 skenario yang diterapkan. Hasil yang didapatkan dari penelitian ini menunjukkan bahwa aplikasi media sosial pada perangkat android dalam keadaan UnRoot memiliki persentase yang rendah dalam penemuan bukti digital sedangkan pada perangkat android yang telah dilakukan Root persentase keberhasilan meningkat pesat pada masing-masing aplikasi berdasarkan skenario yang telah ditentukan.

6. Pustaka

- [1] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, Jun. 2017, doi: 10.26555/jiteki.v3i1.6643.
- [2] CheckPoint, "Brand Phishing Report – Q4 2020," *Check Point Blog*, 2021. <https://www.checkpoint.com/press/2022/dhl-replaces-microsoft-as-most-imitated-brand-in-phishing-attempts-in-q4-2021/>
- [3] Vika Azkiya Dihni, "Indonesia Pengguna WhatsApp Terbesar Ketiga di Dunia," *Databoks.Katadata.Co.Id*, p. Teknologi dan Telekomunikasi, 2021, [Online]. Available: <https://databoks.katadata.co.id/datapublish/2021/11/23/indonesia-pengguna-whatsapp-terbesar-ketiga-di-dunia>
- [4] Cindy Mutia Annur, "Rekor Lagi, Pengguna Aktif Line Tembus 178 Juta pada 2021," 2022. [Online]. Available: <https://databoks.katadata.co.id/datapublish/2022/06/15/rekor-lagi-pengguna-aktif-line-tembus-178-juta-pada-2021>
- [5] G. Maulana Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," 2016. [Online]. Available: <http://ars.ilkom.unsri.ac.id>
- [6] A. Wirara, B. Hardiawan, and M. Salman, "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.
- [7] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, p. 87, 2019, doi: 10.30872/jurti.v3i1.2292.
- [8] A. Fauzan, I. Riadi, and A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017.
- [9] P. D. Saksono, "Analisis Mobile Forensik Investigasi Studi kasus pada LINE Chat MESSENGER," Repository UKSW no. 672012152, p. 2, 2017.
- [10] R. Anggara, A. Fadil, and I. Riadi, "Forensik Mobile Pada Smartwatch Berbasis Android", *Jurnal Rekayasa Teknologi Informasi*, doi: 10.30872/JURTI.V1I1.638
- [11] Y. Marumo, "Forensic Examination of Soil Evidence," *Japanese J. Forensic Sci. Technol.*, vol. 7, no. 2, pp. 95–111, 2003, doi: 10.3408/jafst.7.95.