Jurnal Riset Teknologi Informasi dan Komputer (JURISTIK) p-ISSN: .....
Vol. 1, No. 1, Juni 2021, hlm. 8-15 e-ISSN: .....
Akreditasi KEMENRISTEKDIKTI, No. /E/KPT/

Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)

Muhammad Abdul Aziz[1], Wicaksono Yuli Sulistyo[2], Sri Rahayu Astari[3]
[1]Program Studi Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
[2]Program Studi Sistem Informasi, Universitas Siber Muhammadiyah Yogyakarta
[3]Jurusan Informatika, Universitas Pembangunan Nasional "Veteran" Yogyakarta
[1]dotacome@gmail.com, [2]sonow292@gmail.com, [3]tarisrtari@gmail.com

Abstract

Anti-forensic technology has become a major concern for instant messaging application developers as one of the factors to determine the level of vulnerability or vulnerability of the application. This research was conducted to determine the vulnerability value of web-based instant messaging Skype, WhatsApp, and Telegram from the comparative results of the anti-forensic technology of each of these applications. The Association of Chief Police Officers (ACPO) method was chosen as a reference in carrying out the stages of this research. Plan, capture, analysis, present are the research stages of the Association of Chief Police Officers (ACPO) method. Digital data in the form of images, conversation texts, videos, user IDs, and telephone numbers are used as parameters in the research process. These parameters were acquired from each instant messaging using the FTK imager and Fiddler tools. The results obtained from this study indicate that the Skype instant messaging application has a vulnerability value of 97%, while the instant messaging applications Telegram and WhatsApp have the same vulnerability value of 66% based on all digital data obtained from the acquisition process.

Keywords: Anti-Forensic, ACPO, Vulnerability, Instant Messaging

Abstrak

Teknologi anti forensik telah menjadi perhatian utama para pengembang aplikasi instant messaging sebagai salah satu faktor untuk menentukan tingkat kerentanan atau *vulnerability* aplikasinya. Penelitian ini dilakukan agar dapat mengetahui nilai kerentanan *instant messaging* Skype, WhatsApp, dan Telegram berbasis *web* dari hasil komparatif teknologi anti forensiknya masing-masing aplikasi tersebut. Metode *Association of Chief Police Officers* (ACPO) dipilih sebagai acuan dalam melakukan tahapan-tahapan penelitian ini. *Plan, capture, analysis, present* merupakan tahapan penelitian dari metode *Association of Chief Police Officers* (ACPO). Data digital berupa gambar, teks percakapan, video, ID user, dan nomor telepon digunakan sebagai parameter dalam proses penelitian. Parameter-parameter tersebut diakuisisi dari masing-masing instant messaging menggunakan *tools* FTK imager dan Fiddler. Hasil yang diperoleh dari penelitian ini menunjukkan aplikasi *instant messaging* Skype mempunyai nilai kerentanan sebesar 97%, sedangkan aplikasi *instant messaging* Telegram dan WhatsApp mempunyai nilai kerentanan yang sama sebesar 66% berdasarkan seluruh data digital yang diperoleh dari proses akuisisi.

Kata kunci: Anti Forensik, ACPO, *Vulnerability*, *Instant Messaging*

1. Pendahuluan

Teknologi pesan singkat atau *instant messaging* baik yang berbasis smartphone maupun berbasis web telah menjadi pilihan utama sarana komunikasi di masa serba digital ini [1]. Skype, Telegram, dan WhatsApp termasuk dalam aplikasi *instant messaging* dengan layanan berbasis smartphone dan web yang paling sering digunakan pada beberapa tahun terakhir ini [2].

Website statista melakukan survei pada Oktober 2018 tentang aplikasi *instant messaging* yang paling sering digunakan pada tahun itu. Hasil survei tersebut menunjukkan *instant messaging* Skype telah digunakan oleh 300 juta orang, Telegram telah digunakan oleh 200 juta orang, dan WhatsApp telah digunakan oleh lebih dari 1,5 miliar orang [3]. Data tersebut telah menunjukkan bahwa aplikasi *instant messaging* Skype, Telegram, dan WhatsApp dapat menarik perhatian banyak orang untuk menggunakannya sebagai sarana berkomunikasi dengan media digital [4].

Fitur-fitur yang menarik dan jaminan keamanan data yang ditawarkan oleh aplikasi *instant messaging* menjadi faktor utama yang mempengaruhi banyaknya pengguna aplikasi ini [5]. Hal tersebut menjadikan para pengembang aplikasi *instant messaging* lebih memeperhatikan tentang keamanan data dan privasi aplikasi mereka [6]. Pengguna cenderung lebih suka menggunakan aplikasi *instant messaging* yang dapat melindungi data dan privasinya seiring dengan meningkatnya kasus kejahatan digital (*cybercrime*) yang

menggunakan media aplikasi pesan singkat tersebut [7].

Pengembang perlu menguji fitur keamanan data aplikasinya dengan melihat nilai kerentanan atau *vulnerability* dari teknologi anti forensik aplikasi mereka [8]. Nilai kerentanan atau *vulnerability* dari teknologi anti forensik aplikasi *instant messaging* dapat menjadi referensi bagi pengembang untuk meningkatkan fitur keamanan data aplikasinya dan bagi pengguna nilai tersebut dapat digunakan sebagai acuan dalam memilih aplikasi *instant messaging* yang dapat memberikan jaminan keamanan data dan privasi bagi penggunanya [9].

Penelitian sebelumnya lebih banyak membahas tentang perbandingan *tools* forensik seperti pada penelitian *Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method* yang meneliti keberhasilan *tools* forensik dalam mengakuisisi bukti digital dari aplikasi instagram pada perangkat smartphone [10]. Penelitian lainya tidak jauh berbeda seperti penelitian Perbandingan *Tool* Forensik Data *Recovery* Berbasis Android Menggunakan Metode *National Institute of Standards and Technology* (NIST), pada penelitian tersebut hanya dapat diketahui tingkat keberhasilan *tools* forensik dalam proses *recovery* data yang telah dihapus [11].

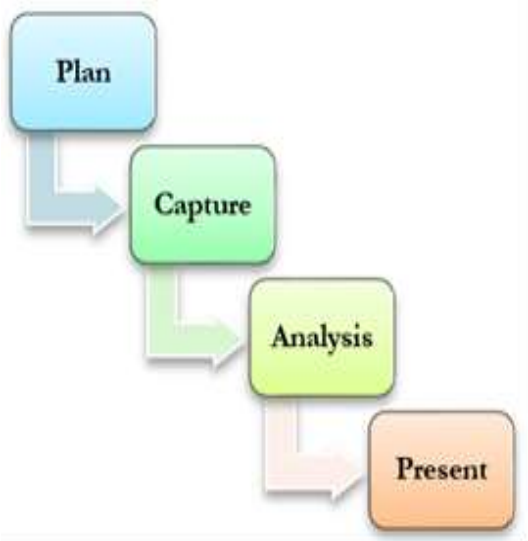
Penelitian-penelitian tersebut tidak ada yang membahas tentang kerentanan teknologi anti forensik pada aplikasi *instant mess*aging berbasis *web*, keduanya hanya memfokuskan pada tingkat keberhasilan *tools* yang digunakan [12]. Hal tersebut menunjukkan perlunya dilakukan penelitian tentang komparatif teknologi anti forensik pada aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis web menggunakan metode *Association of Chief Police Officers* (ACPO) [13].

Hasil dari penitian tersebut berupa perandingan dari nilai kerentanan teknologi anti forensik masing-masing aplikasi *instant messaging* berbasis *web*. Nilai kerentanan diperoleh dari banyaknya data digital yang berhasil diambil dari masing-masing aplikasi menggunakan *tools* FTK imager dan Fiddler [14].

2. Metode Penelitian

Data digital diperoleh dari proses akuisisi aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis *web* [15]. Penelitian yang dilakukan menggunakan *tools* FTK imager dan Fiddler dalam proses akuisisi data digital pada masing-masing aplikasi *instant messaging* berbasis *web* [16]. Hasil akuisisi data digital tersebut digunakan untuk dasar menentukan nilai kerentanan teknologi anti forensik masing-masing aplikasi *instant messaging* berbasis *web* [17]. Nilai kerentanan teknologi anti forensik tersebut kemudian dikomparasikan antara satu dan yang lainya agar dapat diketahui mana saja aplikasi *intant messaging* berbasis web dengan nilai kerentanan tinggi dan rendah [18].

Metode *Association of Chief Police Officers* (ACPO) merupakan suatu kerangka kerja penelitian dengan 4 dasar elemen kunci yang terdiri dari identifikasi, mengamankan bukti, analisa dan pemaparan atau presentasi [19]. Skema tahapan-tahapan penelitian metode *Association of Chief Police Officers* (ACPO) dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian Metode ACPO

Berdasarkan Gambar 1 dapat diketahui metode *Association of Chief Police Officers* (ACPO) mempunyai beberapa tahapan penelitian, tahapan-tahapan penelitian tersebut dapat dijelaskan sebagai berikut:

a. Rencana (*plan*) tahap dimana rancangan tentang segala sesuatu yang akan dilakukan pada proses penelitian sudah terlebih dahulu disusun pada tahap ini.
b. Menangkap (*capture*) tahapan dimana dilakukan penyimpanan terhadap hasil penelitian agar nantinya dapat dilanjutkan dengan tahap analisis menggunakan hasil tersebut.
c. Analisis (*analysis*) pada tahap ini dilakukan analisis menggunakan parameter hasil yang telah diperoleh dari tahap sebelumnya.
d. Presentasi (*present*) tahap diamana data hasil analisis pada tahap sebelumnya dipresentasikan agar dapat diketahui oleh publik.

Penelitian yang dilakukan dalam prosesnya tentunya memerlukan alat dan bahan penelitian, hal tersebut perlu disiapkan di awal agar nantinya apabila di tengah proses penelitian tidak ada yang kurang sehingga tidak mengganggu jalannya

penelitian. Alat dan bahan yang dibutuhkan dalam penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Alat dan Bahan Penelitian

No	Alat dan Bahan	Diskripsi/Versi	Keterangan
1.	Laptop	LENOVO E084	*Hardware*
2.	Smartphone	Xiaomi A1	*Hardware*
3.	FTK Imager	Versi 4.2.0.13	*Software*
4.	Fiddler	Versi 5.0.20204	*Software*
5.	WhatsApp *Web Based*	Versi 0.4.2088	*Software*
6.	Telegram *Web Based*	Versi 0.7.0	*Software*
7.	Skype *Web Based*	Versi 8.58.0.93	*Software*
8.	Google Chrome	Versi 84.0.4147.125	*Software*

Berdasarkan Tabel 1. dapat diketahui alat dan bahan yang digunakan dalam proses penelitian ini terdiri dari enam *software* dan dua *hardware*. Skenario penelitian diperlukan untuk menentukan langkah-langkah apa saja yang akan dilakukan nantinya.

Penelitian ini menggunakan skenario dimana kronologi kejadianya terdapat dua orang pengguna yang sedang saling mengirim pesan berupa video, gambar, dan teks melalui aplikasi *instant messaging* Skype, Telegram, dan WhatsApp. Pengguna 1 menggunakan aplikasi instant messaging berbasis *web*, sedangkan pengguna 2 menggunakan aplikasi *instant messaging* pada smartphone seperti yang diperlihatkan pada Gambar 2.

Gambar 2. Skenario Penelitian

Berdasarkan Gambar 2 dapat diketahui pengguna 1 dan pengguna 2 saling mengirimkan pesan menggunakan aplikasi *instant messaging* Skype, Telegram, dan WhatsApp. Pengguna 1 dan pengguna 2 yang telah selesai mengirimkan pesan video, gambar, dan teks dari ketiga *aplikasi instant messaging* tersebut kemudian mematikan perangkatnya masing-masing. Perangkat pengguna 1 dan pengguna 2 sengaja dimatikan untuk mengecek apakah data digital dari aplikasi *instant messaging* berbasis *web* tersebut masih tersimpan di *volatile memory* laptop pengguna 1.

Laptop yang tadi digunakan oleh pengguna 1 dinyalakan kembali untuk diambil data digital dari aplikasi *instant messaging* berbasis *web* yang telah digunakan tadi. Data digital dari laptop pengguna 1 diakuisisi menggunakan *tools* FTK imager dan Fiddler. Hasil dari proses akuisisi tersebut akan digunakan sebagai dasar dalam menentukan nilai kerentanan teknologi anti forensik dari ketiga aplikasi *instant mesagging* berbasis *web* tersebut.

3. Hasil dan Pembahasan

3.1 Rencana (*Plan*)

Tahap rencana (*plan*) terlebih dahulu dilakukan dengan menyusun suatu rencana dengan sedatail mungkin berkaitan dengan langkah-langkah apa saja yang akan dilakukan dalam proses penelitian termasuk membuat skenario penelitian dan mempersiapkan alat dan bahan penelitian. Parameter penelitian diambil dari data digital aplikasi *instant messaging* berbasis *web* berupa pesan video, teks, gambar, nomor telepon, dan ID *user* seperti yang ditampilkan pada Tabel 2.

Tabel 2. Data Digital Instant Messaging

No	Jenis Data	Jumlah Data
1.	Pesan teks	120
2.	Pesan gambar	72
3.	Pesan video	6
4.	Nomor telepon	8
5.	*User* ID	24

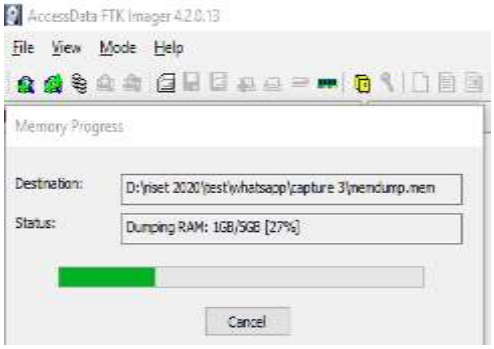
Berdasarkan Tabel 2 diketahui data digital yang telah berhasil diakuisisi dari aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis *web*. Data digital tersebut diakuisisi menggunakan *tools* FTK imager dan Fiddler dengan jumlah total data digital yang berhasil diperoleh berdasarkan Tabel 2 sebanyak 230 data.

3.2 Menangkap (*Capture*)

Tahap menangkap (*capture*) merupakan tahap dilakukannya penyimpanan atau mendokumentasikan seluruh data digital yang diperoleh dari proses akuisisi, data-data tersebut kemudian dikelompokan sesuai denang jenis data masing-masing. Data digital tersebut merupakan hasil dari *capture physical memory* menggunakan FTK imager dan *debugging web proxy browser* menggunakan Fiddler pada laptop yang digunakan untuk penelitian. Gambar 3 menunjukkan proses capture *physical memory* menggunakan FTK imager

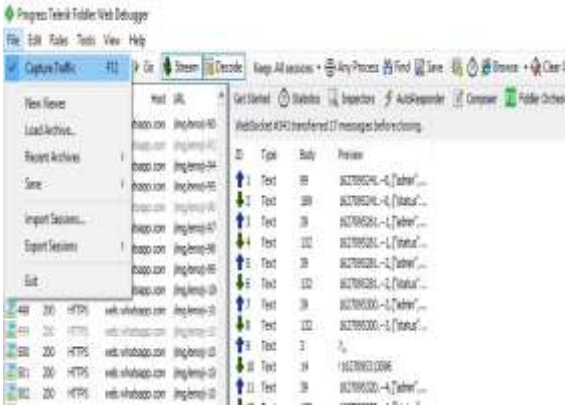
DOI: https://doi.org/xx.xxx/juristik.xxx.xxx

dan Gambar 4 menunjukkan proses *debugging web proxy browser* menggunakan Fiddler.



Gambar 3. *Capture Physical Memory* dengan FTK imager

Hasil dari proses *capture Physical Memory* menggunakan FTK imager seperti yang ditunjukkan pada Gambar 3 adalah berupa *dump file* dari masing-masing aplikasi *instant messaging* berbasis web tersebut. *Dump file* tersebut perlu melalui proses *extract* agar dapat diperoleh data-data digital yang nantinya akan digunakan sebagai parameter penelitian pada tahap analisis.

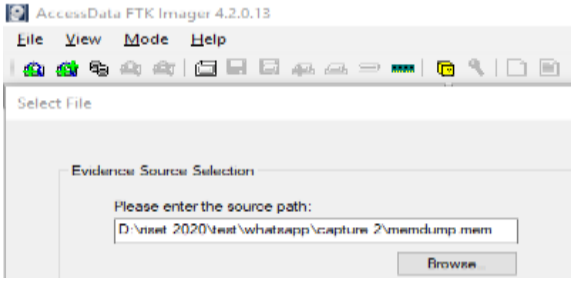


Gambar 4. *Debugging Web Proxy* dengan Fiddler

Tahap *capture debugging web proxy* dengan menggunakan Fiddler tidak menghasikan *dump files*. Data digital diperoleh melalui penulusuran traffic paket data yang ditangkap menggunakan Fiddler. Parameter penelitian merupakan data-data digital hasil dari kedua proses *capture* tersebut. Hasil analisis berupa nilai kerentanan teknologi anti forensik aplikasi *instant messaging* tergantung dari banyaknya data digital yang diperoleh, semakin banyak data digital yang diperoleh dari suatu aplikasi *instant messaging* berbasis *web* berarti semakin tinggi pula nilai kerentanan dari teknologi anti forensik aplikasi tersebut.

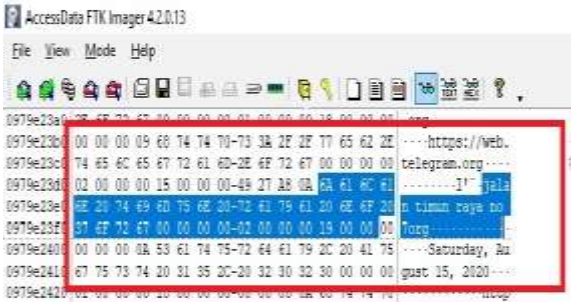
3.3 Analisis (*Analys*)

Tahap analisis (*analys*) merupakan proses analisis dari hasil *extract dump file* FTK imager seperti yang ditunjukan pada Gambar 5 dan penulusuran *traffic* paket data menggunakan Fiddler. Data digital dianalisis adalah hasil *extract* dari *dump file* menggunakan FTK imager.



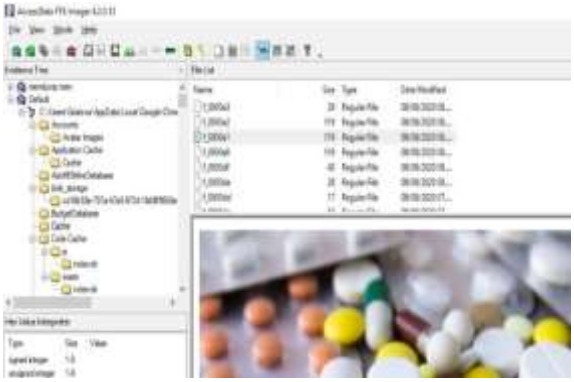
Gambar 5. *Extract Dump File* dengan FTK imager

Berdasarkan Gambar 5 dapat diketahui proses *extract dump file* dapat dilakukan dengan menggunakan FTK imager. Hasil yang diperoleh dari proses extract tersebut kemudian dianalisa agar diperoleh data-data digital dari aplikasi *instant messaging* berbasis *web*. Gambar 6 menunjukkan proses analisis menggunakan FTK imager. Data digital berupa pesan teks yang ditemukan pada proses analisis tersebut membuktikan bahwa FTK imager mampu mengakuisisi data-data digital dari aplikasi *instant messaging* Skype, Telegram dan WhatsApp berbasis *web*.

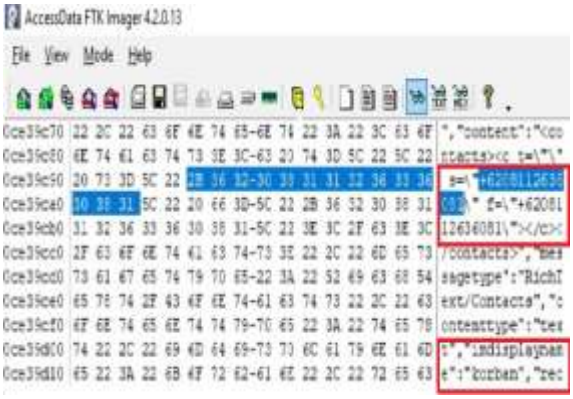


Gambar 6. Proses Analisis Menggunakan FTK imager

Berdasarkan Gambar 6 FTK imager berhasil mengakuisisi pesan teks dari aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis *web*. Tahap analisis tersebut tidak hanya dapat mengakuisisi pesan teks saja melainkan ditemukan juga data digital berupa pesan gambar seperti yang ditunjukkan pada Gambar 7 serta ID user dan nomor telepon pengguna aplikasi *instant messaging* berbasis *web* yang diperlihatkan pada Gambar 8.



Gambar 7. Data Digital Pesan Gambar pada FTK Imager



Gambar 8. ID *user* dan Nomor Telepon pada FTK Imager

Tahap analisis selanjutnya dilakukan pada *capture traffic* paket data menggunakan Fiddler *debugging web proxy*, pada proses analisis ini berhasil menemukan data digital berupa ID user dan nomor telepon seperti yang diperlihatkan pada Gambar 9. Hal ini membuktikan bahwa Fiddler juga telah berhasil untuk mengakuisisi data-data digital dari aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis *web*.

Instant Messaging	Jumlah Data Digital				
	Pesan Teks	Pesan Gambar	Pesan Video	No. Tlp.	ID *User*
Skype	120	72	0	8	24
Telegram	120	0	0	8	24
WhatsApp	120	0	0	8	24

Instant Messaging	Jumlah Data Digital				
	Pesan Teks	Pesan Gambar	Pesan Video	No. Tlp.	ID *User*
Skype	0	0	0	8	24
Telegram	0	0	0	8	24
WhatsApp	0	0	0	8	24

Gambar 9. ID *User* dan Nomor Telepon pada Fiddler

Tahap analisis ini telah berhasil mengumpulkan keseluruhan data-data digital yang diperoleh dari aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis web menggunakan tools FTK imager dan Fiddler. Data-data digital hasil akuisisi menggunakan FTK imager keseluruhanya dapat dilihat pada Tabel 3 dan keseluruhan data-data digital hasil akuisisi menggunakan Fiddler dapat dilihat Tabel 4.

Tabel 1. Jumlah Data Digital Hasil Akuisisi FTK Imager

Berdasarkan Tabel 3 data-data digital aplikasi *instant messaging* berbasis *web* yang berhasil diakuisisi menggunakan FTK imager dari aplikasi Skype berbasis web berupa 120 pesan teks, 72 pesan gambar, 8 nomor telepon, dan 24 ID user. Data-data digital hasil akuisisi menggunakan FTK imager pada aplikasi Telegram dan WhatsApp memiliki jumlah yang sama berupa 120 pesan teks, 8 nomor telepon, dan 24 ID user.

Tabel 4. Jumlah Data Digital Hasil Akuisisi Fiddler

Hasil Akuisisi data-data digital menggunakan Fiddler pada Tabel 4 menunjukkan bahwa aplikasi *instant messaging* Skype, Telegram, dan WhatsApp

DOI: https://doi.org/xx.xxx/juristik.xxx.xxx

berbasis *web* memiliki jumlah perolehan data yang sama berupa 8 nomor telepon dan 24 ID user. Data-data digital yang telah berhasil diakuisisi dari aplikasi instant messaging Skype, Telegram, dan WhatsApp nantinya akan menjadi faktor utama yang menentukan nilai kerentanan dari teknologi anti forensik masing-masing aplikasi *instant messaging tersebut*.

3.4 Presentasi (*Present*)

Penelitian ini dalam menentukan nilai kerentanan dari masing-masing teknologi anti forensik aplikasi *instant messaging* berbasis *web* menggunakan perhitungan nilai indeks berdasarkan dari jumlah data-data digital yang telah berhasil diakuisisi. Rumus untuk menghitung nilai kerentanan teknologi anti forensik aplikasi *instant messaging* berbasis *web* adalah menggunakan persamaan indeks tidak tertimbang seperti yang dapat dilihat pada Persamaan 1 [20].

No	Jenis Data	Jumlah Data Awal	Jumlah Data Hasil Akuisisi
1.	Pesan teks	120	120
2.	Pesan gambar	72	72
3.	Pesan video	6	0
4.	Nomor telepon	8	8
5.	*User* ID	24	24

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\% \quad (1)$$

Keterangan:

Pon : presentase nilai kerentanan teknologi anti forensik aplikasi *instant messaging* berbasis *web*

$\sum Po$: jumlah keseluruhan data digital aplikasi *instant messaging* berbasis *web*

$\sum Pn$: jumlah data digital yang telah berhasil diakuisisi

No	Jenis Data	Jumlah Data Awal	Jumlah Data Hasil Akuisisi
1.	Pesan teks	120	120
2.	Pesan gambar	72	0
3.	Pesan video	6	0
4.	Nomor telepon	8	8
5.	*User* ID	24	24

Hasil akuisisi data digital aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis web menggunakan *tools* FTK imager dan Fiddler menjadi dasar untuk menentukan nilai kerentanan teknologi anti forensik masing-masing aplikasi tersebut. Data-data digital hasil akuisisi aplikasi *instant messaging* Skype berbasis *web* keseluruhannya dapat dilihat pada Tabel 5.

Tabel 5. Hasil Akuisisi Data Digital Skype

Tabel 5 menunjukkan keseluruhan data-data digital aplikasi *instant messaging* Skype berbasis *web*, berdasarkan data-data digital tersebut dapat diketahui nilai kerentanan teknologi anti forensiknya sebesar 97%. Hasil ini didapatkan dengan menggunakan pertihungan perbandingan nilai indeks tidak tertimbang sebagai berikut:

$$\text{Nilai Kerentanan} = \frac{224}{230} \times 100\%$$

Data-data digital hasil akuisisi aplikasi *instant messaging* Telegram berbasis *web* menggunakan *tools* FTK imager dan Fiddler keseluruhannya dapat dilihat pada Tabel 6. Hasil akuisisi tersebut akan digunakan untuk menentukan nilai kerentanan teknologi anti forensik *aplikasi instant messaging* Telegram berbasis web.

Tabel 6. Hasil Akuisisi Data Digital Telegram

Berdasarkan Tabel 6 dapat diketahui bahwa keseluruhan data-data digital aplikasi *instant messaging* Telegram berbasis *web*, berdasarkan data-data digital tersebut dapat diketahui nilai kerentanan teknologi anti forensik aplikasi tersebut sebesar 66%. Hasil tersebut didapatkan dengan menggunakan pertihungan perbandingan nilai indeks tidak tertimbang sebagai berikut:

$$\text{Nilai Kerentanan} = \frac{152}{230} \times 100\%$$

Hasil akuisisi data-data digital aplikasi *instant messaging* WhatsApp berbasis *web* menggunakan *tools* FTK imager dan Fiddler keseluruhannya dapat dilihat pada Tabel 7. Hasil akuisisi tersebut akan digunakan untuk menentukan nilai kerentanan teknologi anti forensik aplikasi *instant messaging* WhatsApp berbasis *web*.

Tabel 7. Hasil Akuisisi Data Digital WhatsApp

Tabel 7 menunjukan dapat bahwa keseluruhan data-data digital aplikasi *instant messaging* WhatsApp berbasis *web* sama dengan dengan perolehan data-data digital dari aplikasi *instant messaging* Telegram berbasis *web*. Hal tersebut membuat aplikasi *instant messaging* WhatsApp berbasis *web* memiliki nilai kerentanan teknologi anti forensik yang sama dengan aplikasi *instant messaging* Telegram berbasis *web* yaitu sebesar 66%. Hasil tersebut didapatkan dengan menggunakan pertihungan perbandingan nilai indeks tidak tertimbang sebagai berikut:

$$\text{Nilai Kerentanan} = \frac{152}{230} \times 100\%$$

4. Kesimpulan

Berdasarkan hasil dari penelitian komparatif teknologi anti forensik aplikasi *instant messaging* Skype, Telegram, dan WhatsApp berbasis *web* dapat disimpulkan bahwa pada aplikasi Skype berbasis *web* memiliki nilai kerentanan yang lebih tinggi jika dibandingkan dengan perolehan nilai kerentanan aplikasi Telegram dan WhatsApp. Aplikasi Skype berbasis *web* memiliki nilai kerentanan sebesar 97%, sedangkan aplikasi Telegram dan WhatsApp memiliki nilai kerentanan yang sama dengan masing-masing nilai yang diperoleh sebesar 66%. Hasil dari penelitian ini dapat menjadi referensi bagi pengembang dan pengguna aplikasi *instant messaging* berbasis *web* agar lebih memperhatikan tentang keamanan data aplikasinya.

Daftar Pustaka

[1] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "WhatsApp, viber and telegram: Which is the best for instant messaging?," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 3, pp. 909–914, 2016, doi: 10.11591/ijece.v6i3.10271.

[2] M. N. Yusoff, A. Dehghantanha, and R. Mahmod, "Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS," *Contemp. Digit. Forensic Investig. Cloud Mob. Appl.*, pp. 41–62, 2017, doi: 10.1016/B978-0-12-805303-4.00004-6.

[3] B. N. Prastowo, N. A. S. Putro, and O. A. Dhewa, "PLO User Interface based on Telegram Bot," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 13, no. 1, p. 21, 2019, doi: 10.22146/ijccs.29089.

[4] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," *Digit. Investig.*, vol. 23, no. October, pp. 31–49, 2017, doi: 10.1016/j.diin.2017.09.002.

[5] M. S. Asyaky, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android," vol. 3, no. October, 2019.

[6] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[7] S. Chhabra and K. Lata, "Enhancing Data Security using Obfuscated 128-bit AES Algorithm - An Active Hardware Obfuscation Approach at RTL Level," *2018 Int. Conf. Adv. Comput. Commun.*

No	Jenis Data	Jumlah Data Awal	Jumlah Data Hasil Akuisisi
1.	Pesan teks	120	120
2.	Pesan gambar	72	0
3.	Pesan video	6	0
4.	Nomor telepon	8	8
5.	*User* ID	24	24

Informatics, ICACCI 2018, no. December, pp. 401–406, 2018, doi: 10.1109/ICACCI.2018.8554562.

[8] B. Rahardjo and I. P. A. E. Pratama, "Pengujian Dan Analisa Anti Komputer Forensik Menggunakan Shred Tool," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 7, no. 2, p. 104, 2016, doi: 10.24843/lkjiti.2016.v07.i02.p04.

[9] J. Choi, J. Yu, S. Hyun, and H. Kim, "Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger," *Digit. Investig.*, vol. 28, pp. S50–S59, 2019, doi: 10.1016/j.diin.2019.01.011.

[10] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[11] I. Riadi, S. Sunardi, and Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *J. Teknol. Inf. dan Ilmu Komput.*, vol. x, no. 30, pp. 1–8, 2020, doi: 10.25126/jtiik.202071921.

[12] M. Faiz and W. A. Prabowo, "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," vol. 1, no. December, 2018, doi: 10.20895/INISTA.V1I1.

[13] I. Riadi, U. Rusydi, and M. A. Aziz, "Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO)," vol. 1, no. 1, pp. 1–11, 2019.

[14] H. Setiaji and I. V. Paputungan, "Design of Telegram Bots for Campus Information Sharing," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 325, no. 1, 2018, doi: 10.1088/1757-899X/325/1/012005.

[15] I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 16, no. June, pp. 201–205, 2018.

[16] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS," *J. Rekayasa Sist. Ind.*, vol. 4, no. 01, 2017, doi: 10.25124/jrsi.v4i01.149.

[17] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," no. September, 2018.

[18] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[19] D. Hariyadi, F. E. Nastiti, and F. N. Aini, "Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO / IEC 27037 : 2014," *Int. Conf. Informatics Dev.*, no. November, 2018.

[20] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/IJACSA.2017.081210.