HASIL CEK_60020397_Point-C45-IRD-850GB-Comparative Security Analysis of Web-Based Instant Messaging Applications

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:29AM (UTC+0700)
Submission ID: 1471679843
File name: ecurity_Analysis_of_Web-Based_Instant_Messaging_Applications.pdf (518.42K)
Word count: 4011
Character count: 23987

Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 5 (2020) 813 - 819 ISSN Media Elektronik: 2580-0760

Komparatif *Web-based Instant Messaging Vulnerability* Menggunakan Metode *Association of Chief Police Officers*

Imam Riadi[1], Rusydi Umar[2], Muhammad Abdul Aziz[3]
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[2,3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[1]imamriadi@is.uad.ac.id*, [2]rusydi@mti.uad.ac.id, [3]muhammad1807048013@webmail.uad.ac.id

Abstract

Web-based instant messaging applications vulnerability has become one of the main concerns for its users in line with the increasing number of cybercrimes that occur on social media. This research was conducted to determine the comparability of the vulnerability value of the web-based WhatsApp, Telegram, and Skype applications using the Association of Chief Police Officers (ACPO) method. Digital artifacts in the form of text messages, picture messages, video messages, telephone numbers, and user IDs have been acquired in this research process using FTK imager and OSForensic tools. The results of the study using the FTK imager and OSForensic tools show that the web-based Skype application has a vulnerability value of 92%, while WhatsApp and Web-based Telegram have the same vulnerability value with 67% each based on all digital artifacts that successfully acquired.

Keywords: Instant Messaging, Vulnerability, ACPO, FTK Imager, OSForensic.

Abstrak

Vulnerability aplikasi *instant messaging* berbasis *web* telah menjadi salah satu perhatian utama bagi para penggunanya seiring dengan semakin meningkatnya *cybercrime* yang terjadi pada media sosial. Penelitian ini dilakukan untuk mengetahui komparatif dari nilai *vulnerability* aplikasi WhatsApp, Telegram, dan Skype berbasis *web* menggunakan metode *Association of Chief Police Officers* (ACPO). Artefak digital berupa pesan teks, pesan gambar, pesan video, nomor telepon, dan *user* ID telah dapat diakuisisi pada proses penelitian ini dengan menggunakan *tool* FTK imager dan OSForensic. Hasil dari penelitian menggunakan *tool* FTK imager dan OSForensic menunjukkan aplikasi Skype berbasis *web* memiliki nilai *vulnerability* sebesar 92%, sedangkan WhatsApp dan Telegram berbasis *web* memiliki nilai *vulnerability* yang sama dengan perolehan nilai masing-masing sebesar 67% berdasarkan dari keseluruhan artefak digital yang telah berhasil diakuisisi.

Kata kunci: Instant Messaging, Vulnerability, ACPO, FTK Imager, OSForensic.

1. Pendahuluan

Teknologi komunikasi digital dengan menggunakan media komputer dan *smartphone* telah berkembang semakin pesat seiring dengan meningkatnya pengguna aplikasi *instant messaging* baik yang berbasis *web* maupun android [1]. WhatsApp, Telegram, dan Skype merupakan beberapa contoh aplikasi *instant messaging* yang memiliki pengguna aktif terbanyak selama beberapa tahun terakhir [2]. Berdasarkan survei *website* statista pada bulan Oktober tahun 2018 dapat diketahui aplikasi *instant messaging* WhatsApp memiliki 1,5 miliar pengguna aktif bulanan, Skype memiliki 300 juta pengguna aktif bulanan, dan Telegram memiliki 200 juta pengguna aktif bulanan [3]. Hal ini menunjukkan aplikasi *instant messaging* telah menjadi primadona dikalangan para pengguna media sosial [4]. Aplikasi *instant messaging* seperti WhatsApp, Telegram, dan Skype memiliki banyak pengguna karena aplikasi tersebut mudah digunakan dan memiliki fitur-fitur menarik yang dapat menciptakan rasa menyenangkan dalam berkomunikasi [5].

Fitur-fitur dan segala kemudahan yang ditawarkan oleh aplikasi *instant messaging* tidak lantas membuat aplikasi tersebut luput dari ancaman kejahatan siber (*cybercrime*) [6]. Banyaknya kejahatan siber yang terjadi pada aplikasi *instant messaging* menunjukkan aplikasi tersebut memiliki kerentanan (*vulnerability*) dari segi keamanannya [7]. Pesan *chat* pengguna yang dapat diakuisisi oleh pelaku *cybercrime* merupakan salah satu contoh *vulnerability* pada artefak digital

Diterima Redaksi : 25-07-2020 | Selesai Revisi : 06-09-2020 | Diterbitkan Online : 30-10-2020

aplikasi *instant messaging* itu sendiri [8][9]. Hal ini tentunya menjadi kekhawatiran tersendiri bagi para pengguna aplikasi *instant messaging* khususnya yang berbasis *web*, karena dari aplikasi tersebut pelaku *cybercrime* dapat dengan mudah mengakuisisi artefak digital milik korban tanpa perlu menggunakan *smartphone* korban [10].

RSA *Anti Fraud Command Center* menunjukkan pada tahun 2013-2015 telah terjadi peningkatan kasus *cybercrime* sebanyak 173% yang terjadi di seluruh dunia dan mengakibat kerugian sebanyak US$ 325 miliar [11]. Kasus penipuan melalui media daring mengalami peningkatan pada tahun 2015 tercatat sebanyak 61% penipuan daring telah terjadi dalam jangka waktu satu tahun [12][13]. Pengguna aplikasi *instant messaging* khususnya yang berbasis *web* perlu memperoleh referensi dari komparatif *vulnerability* aplikasi *instant messaging* berbasis *web* agar dapat lebih berhati-hati dalam menggunakan aplikasi tersebut [14].

Penelitian tentang Perbandingan *Tool* Forensik Data *Recovery* Berbasis Android Menggunakan Metode *National Institute of Standards and Technology* (NIST) menghasilkan informasi tentang perbandingan kinerja *tool* forensik berbasis android dalam mengembalikan data yang sudah dihapus berupa kontak, *log* panggilan, dan pesan [15]. Penelitian serupa lainnya adalah *Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method* yang menghasilkan informasi mengenai perbandingan tingkat keberhasilan *tool* forensik dalam memperoleh bukti digital berupa pesan teks dan gambar pada aplikasi Instagram berbasis android [16].

Penelitian-penelitian terdahulu tersebut hanya memfokuskan pada perbandingan kinerja *tool* forensik dalam memperoleh bukti digital, namun belum membahas tentang *vulnerability* dari objek penelitiannya [17]. Berdasarkan hal tersebut perlu dilakukan penelitian untuk dapat mengetahui komparatif nilai *vunerablity* aplikasi *instant messaging* WhatsApp, Telegram, dan Skype berbasis *web* dengan menggunakan metode *Association of Chief Police Officers (ACPO)* [18]. Nilai *vulnerability* dari aplikasi *instant messaging* berbasis *web* ditentukan berdasarkan banyaknya artefak digital yang telah berhasil diakuisisi menggunakan *tool* FTK imager dan OSForensic [19].

2. Metode Penelitian

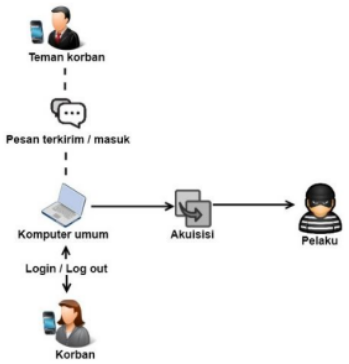
Proses akuisisi diperlukan untuk memperoleh artefak digital dari aplikasi *instant messaging* WhatsApp, Telegram, dan Skype berbasis *web* [20]. Penelitian ini melakukan proses akuisisi artefak digital menggunakan *tool* FTK imager dan OSForensic pada masing-masing aplikasi *instant messaging* tersebut [21]. Artefak digital yang berhasil diakuisisi tersebut kemudian digunakan sebagai dasar untuk menentukan nilai *vulnerability* dari masing-masing aplikasi *instant messaging* berbasis *web* [22]. Nilai *vulnerability* masing-masing aplikasi *instant messaging* berbasis *web* yang telah diketahui kemudian dibandingkan antara satu dengan yang lainnya [23].

Metode *Association of Chief Police Officers* (ACPO) merupakan kerangka kerja ilmiah dengan dasar 4 elemen kunci proses investigasi forensik yang terdiri dari identifikasi, penyimpanan bukti, analisa, dan presentasi [24]. Proses penelitian metode ACPO memiliki beberapa tahapan sebagai berikut:

a. Tahap rencana (*plan*) membuat rencana tentang segala tindakan yang akan dilakukan dalam proses penelitian.
b. Tahap menangkap (*capture*) mendokumentasikan dan menyimpan hasil yang diperoleh dari proses penelitian agar dapat dilakukan analisis terhadap hasil tersebut.
c. Tahap analisis (*analysis*) melakukan analisis terhadap hasil yang diperoleh pada tahap *capture*.
d. Tahap presentasi (*presentation*) melakukan presentasi terhadap hasil dari tahap *analysis* agar dengan mudah dapat dipahami oleh publik.

2.1. Skenario Kasus

Simulasi kasus dilakukan dengan kronologi kejadian seorang korban yang telah selasai *chat* dengan temannya menggunakan komputer umum milik perpustakaan. Korban tersebut hanya melakukan *logout* pada akun *instant messaging* berbasis *web* miliknya dan lupa untuk mematikan komputer yang dia gunakan. Pelaku yang telah mengamati korban kemudian mengambil alih komputer tersebut dan selanjutnya melakukan akuisisi terhadap artefak digital *instant messaging* berbasis *web* yang ditinggalkan oleh korban seperti pada Gambar 1. Artefak digital yang telah berhasil diakuisisi oleh pelaku tersebut nantinya akan digunakan pelaku untuk melakukan penipuan terhadap korban.



Gambar 1. Simulasi Kasus *Cybercrime*

Berdasarkan informasi dari Gambar 1 simulasi penelitian dilakukan dengan menggunkan 2 buah *smartphone* dan 1 buah laptop, *smartphone* yang digunakan terdiri dari *smartphone* milik korban dan teman korban. *Smartphone* milik korban digunakan

untuk melakukan login aplikasi *instant messaging* berbasis *web* sebelum melakukan chat dengan temannya menggunakan aplikasi tersebut. Proses penelitian dilakukan dengan mengulang simulasi pada Gambar 1 menggunakan aplikasi *instant messaging* berbasis *web* yang berbeda pada setiap simulasi yang dilakukan. Hal tersebut dimaksudkan agar dapat diperoleh hasil akuisisi artefak digital dari masing-masing aplikasi *instant messaging* berbasis *web*.

Akuisisi artefak digital pada simulasi Gambar 1 dilakukan dengan menggunakan *tool* FTK imager dan OSForensic agar dapat diketahui perbedaan hasil akuisisi dari kedua *tool* tersebut. Akun aplikasi *instant messaging* berbasis *web* pada semulasi yang dilakukan telah dalam kondisi *logout* seluruhnya, hal ini dilakukan untuk mengetahui apakah aplikasi tersebut masih meninggalkan artefak digital meskipun akun telah *logout*. Simulasi ini melakukan akuisisi pada saat komputer masih menyala dengan maksud untuk menjaga agar *volatile memory* pada komputer tidak hilang sebelum dilakukan proses akuisisi.

Artefak digital yang diakuisisi pada penelitian ini berdasarkan pada data awal aplikasi *instant messaging* berbasis *web* sebelum akun aplikasi tersebut *logout* dari komputer. Data awal tersebut berupa pesan teks, pesan gambar, pesan video, nomor telepon, dan *user* ID seperti yang ditunjukkan pada Tabel 1. Nilai *vulnerability* dari aplikasi WhatsApp, Telegram, dan Skype berbasis *web* ditentukan berdasarkan banyaknya artefak digital yang berhasil diakuisisi pelaku dari masing-masing aplikasi tersebut. Hal ini dapat diasumsikan dengan semakin banyak artefak digital yang berhasil diakuisisi dari suatu aplikasi *instant messaging* berbasis *web* semakin banyak pula nilai *vulnerability* dari aplikasi tersebut

Tabel 1. Data Awal *Instant Messaging*

No	Jenis Data Awal	Jumlah Data Awal
1.	Pesan teks	12
2.	Pesan gambar	9
3.	Pesan video	3
4.	Nomor telepon	6
5.	*User* ID	6

Akuisisi artefak digital pada penelitian ini dilakukan sesuai dengan data awal pada Tabel 1 yang terdiri dari 12 pesan teks, 9 pesan gambar, 3 pesan video, 6 nomor telepon, dan terakhir 6 *user* ID pada masing-masing aplikasi *instant messaging* berbasis *web*.

2.2. Metode Komparatif

Penelitian ini menggunakan perhitungan nilai indeks untuk menentukan tingkat *vulnerability* dari masing-masing aplikasi *instant messaging* berbasis *web* berdasarkan dari hasil akuisisi artefak digital aplikasi tersebut. Rumus yang digunakan dalam perhitungan komparatif nilai *vulnerability* adalah persamaan indeks tidak tertimbang. Nilai *vulnerability* aplikasi *instant messaging* berbasis *web* dapat diketahui menggunakan Persamaan 1 [25].

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

Keterangan:

Pon : presentase nilai *vulnerability* aplikasi instant messaging berbasis *web*

$\sum Po$: jumlah data awal artefak digital

$\sum Pn$: jumlah data artefak digital hasil akuisisi

3. Hasil dan Pembahasan

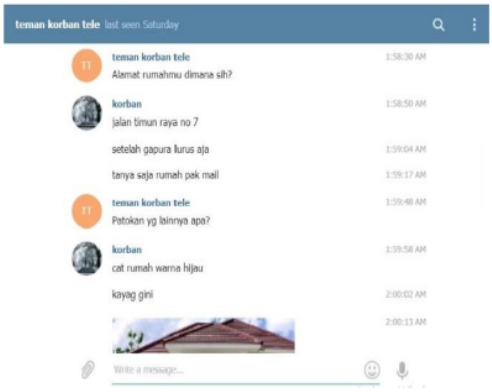
3.1. *Plan*

Tahap *plan* dilakukan dengan membuat rencana secara mendetail tentang proses penelitian termasuk dalam menentukan alat dan bahan yang digunakan dalam penelitian seperti yang ditunjukkan pada Tabel 2. Simulasi penelitian pada Gambar 1 dan data awal artefak pada Tabel termasuk ke dalam rencana yang telah dibuat pada tahap ini. Data awal artefak digital diambil dari isi *chat* korban dengan temannya seperti yang ditunjukkan pada Gambar 2.

Tabel 2. Alat dan Bahan Penelitian

No	Alat dan Bahan	Diskripsi/Versi	Keterangan
1.	Laptop	LENOVO E084	*Hardware*
2.	*Smartphone*	Xiaomi A1	*Hardware*
3.	*Smartphone*	Oppo A39	*Hardware*
4.	FTK Imager	Versi 4.2.0.13	*Software*
5.	OSForensic	Versi 7.0	*Software*
6.	WhatsApp *Web*	Versi 0.4.2088	*Software*
7.	Telegram *Web*	Versi 0.7.0	*Software*
8.	Skype *Web*	Versi 8.58.0.93	*Software*
9.	Google Chrome	Versi 84.0.4147.125	*Software*

Penyusunan rencana diperlukan untuk mempermudah proses penelitian, dengan adanya rencana segala sesuatu yang akan digunakan pada proses tersebut dapat dipersiapkan terlebih dahulu.

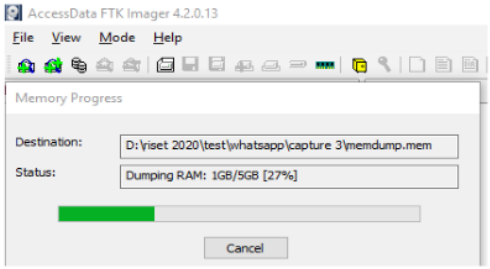


Gambar 2. Simulasi *Chat* Korban

3.2. *Capture*

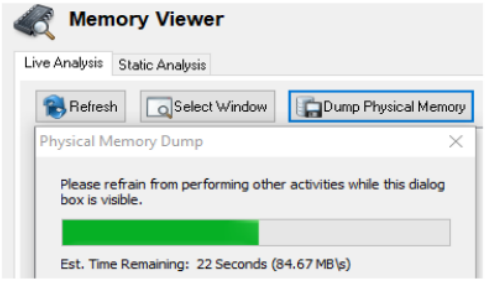
Tahap *capture* dilakukan untuk menangkap, mendokumentasikan, mengelompokan, dan menyimpan seluruh artefak digital yang diperoleh dari *physical memory* komputer. Penelitian ini melakukan proses

capture pada *physical memory* komputer yang digunakan oleh korban dengan menggunakan *tool* FTK imager seperti pada Gambar 3 dan menggunakan *tool* OSForensic seperti pada Gambar 4. Proses *capture* yang dilakukan pada penelitian ini menggunakan 2 buah *tool* dengan maksud agar pada saat dilakukan analisis dapat diketahui perbedaan hasil artefak digital yang berhasil dakuisisi kedua *tool* tersebut.



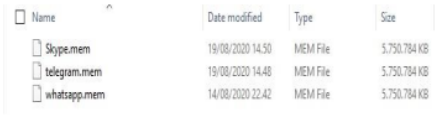
Gambar 3. Proses *Capture Tool* FTK Imager

Hasil dari proses *capture* menggunakan kedua *tool* tersebut merupakan dump *file* seperti pada Gambar 5, *file* tersebut perlu melalui proses *extract* sebelum dapat dilakukan analisis terhadap artefak digital yang terdapat di dalamnya.



Gambar 4. Proses *Capture Tool* OSForensic

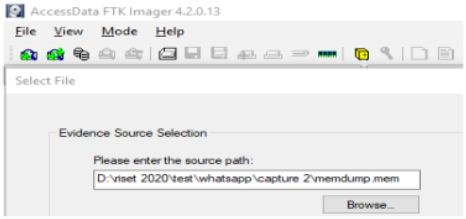
Dump *file* yang diperoleh dari proses *capture physical memory* dikelompokan dan disimpan sesuai dengan masing-masing simulasi penelitian yang dilakukan. *File* tersebut kemudian akan digunakan pada proses analisis untuk dapat mengetahui berapa banyak artefak digital aplikasi *instant messaging* berbasis *web* yang berhasil di akuisisi menggunakan *tool* FTK imager dan OSForensic.



Gambar 5. *File* Hasil Proses *Capture*

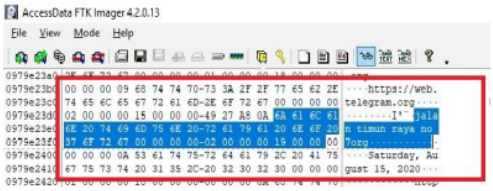
3.3. *Analysis*

Tahap ini dilakukan analisis terhadap dump *file* yang diperoleh pada tahap *capture* untuk mengetahui berapa banyak artefak digital aplikasi *instant messaging* berbasis *web* yang berhasil diakuisisi menggunakan *tool* FTK imager dan OSForensic. Analisis pertama dilakukan pada *dumb file* yang diperoleh dari proses *capture* menggunakan *tool* FTK imager. *Dumb file* tersebut terlebih dahulu melalui proses *extract* seperti pada Gambar 6 sebelum dilakukan analisis menggunakan *tool* FTK imager.



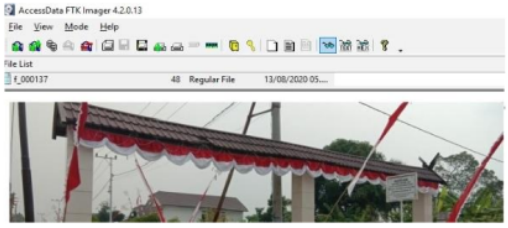
Gambar 6. Proses *Extract Tool* FTK Imager

Proses analisis *tool* FTK imager sepeti pada Gambar 7 bertujuan untuk mengetahui berapa banyak artefak digital yang berhasil diakuisisi berdasarkan data awal artefak digital pada Tabel 1. Artefak digital aplikasi *instant messaging* Telegram berupa pesan teks yang diperoleh dari proses analisis telah membuktikan bahwa *tool* FTK imager berhasil melakukan akuisisi artefak digital dari aplikasi *instant messaging* tersebut.

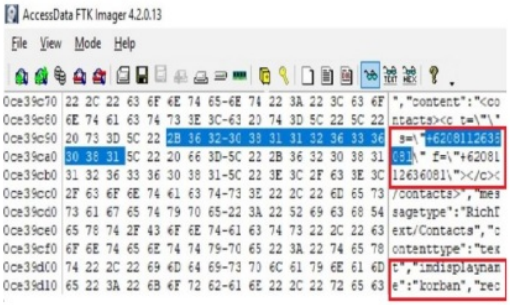


Gambar 7. Proses Analisis *Tool* FTK Imager

Hasil keseluruhan dari proses analisis menggunakan *tool* FTK imager menunjukkan bahwa selain artefak digital berupa pesan teks, *tool* tersebut juga berhasil melakukan akuisisi terhadap artefak digital berupa pesan gambar, *user* ID, dan nomor telepon. Akuisisi artefak digital berupa pesan gambar ditunjukkan pada Gambar 8, sedangkan untuk artefak digital berupa *user* ID dan nomor telepon ditunjukkan pada Gambar 9.

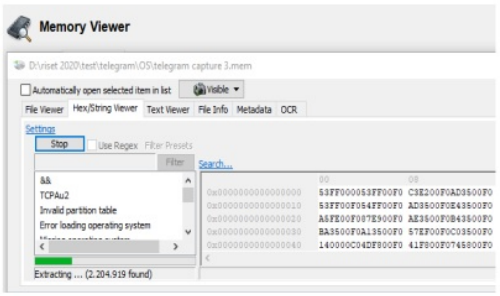


Gambar 8, Artefak Pesan Gambar *Tool* FTK Imager



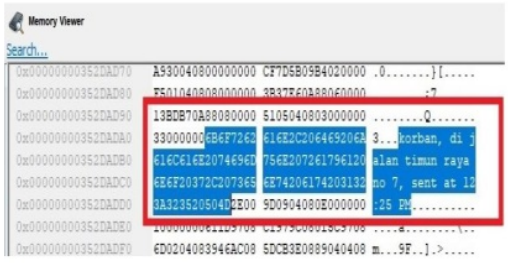
Gambar 9. Artefak *User* ID dan Nomor Telepon *Tool* FTK Imager

Analisis kedua dilakukan pada *dumb file* yang telah melaui proses *extract* seperti pada Gambar 10. Proses analisis menggunakan *tool* OSForensic seperti pada Gambar 11 dilakukan untuk mengetahui perbedaan hasil akuisisi artefak digital dari kedua *tool* yang digunakan.



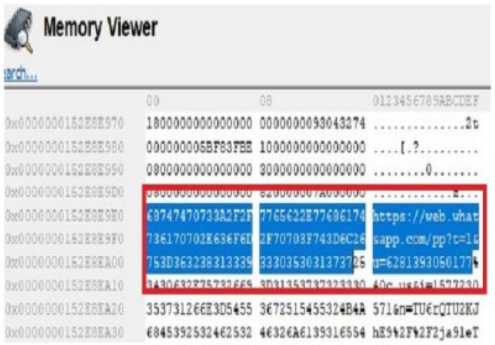
Gambar 10. Proses *Extract Tool* OSForensic

Proses *extract* pada *tool* OSForensic seperti yang ditunjukkan Gambar 10 memiliki sedikit perbedaan dari *tool* FTK imager. Filter string pada *tool* OSForensic dapat langsung dimasukan sebelum proses *extract* berlangsung, sedangkan pada *tool* FTK imager filter string harus dimasukan secara manual setelah proses *extract* selesai.



Gambar 11. Proses Analisis *Tool* OSForensic

Berdasarkan analisis menggunakan *tool* OSForensic yang ditunjukkan pada Gambar 11, dapat diketahui bahwa pada proses tersebut terdapat artefak digital berupa pesan teks dan *user* ID dari aplikasi *instant messaging* Skype berbasis *web*. Proses analisis tersebut juga berhasil mengakuisisi artefak digital berupa nomor telepon seperti pada Gambar 12.



Gambar 12. Artefak Nomor Telepon *Tool* OSForensic

Proses analisis ini menghasilkan data jumlah keseluruhan artefak digital dari masing-masing aplikasi *instant messaging* berbasis *web* yang telah berhasil diakuisisi menggunakan *tool* FTK imager dan OSForensic. Hasil akuisisi artefak digital yang diperoleh menggunakan kedua *tool* tersebut ditunjukkan pada Tabel 3 untuk *tool* FTK imager dan Tabel 4 untuk *tool* OSForensic.

Tabel 3. Hasil Akuisisi Data Artefak Digital *Tool* FTK Imager

Instant Messaging	Jumlah Data yang Berhasil Diakuisisi				
	Pesan Teks	Pesan Gambar	Pesan Video	Nomor Telp.	User ID
WhatsApp	12	0	0	6	6
Telegram	12	0	0	6	6
Skype	12	9	0	6	6

Berdasarkan Tabel 3 *tool* FTK imager berhasil melakukan akuisisi artefak digital berupa 12 pesan teks, 9 pesan gambar, 6 nomor telepon, dan 6 *user* ID pada aplikasi *instant messaging* Skype berbasis *web*. Akuisisi *tool* FTK imager pada artefak digital aplikasi WhatsApp dan Telegram berbasis *web* memiliki hasil yang sama dengan perolehan artefak digital berupa 12 pesan teks, 6 nomor telepon, dan 6 *user* ID.

Tabel 4. Hasil Akuisisi Data Artefak Digital *Tool* OSForensic

Instant Messaging	Jumlah Data yang Berhasil Diakuisisi				
	Pesan Teks	Pesan Gambar	Pesan Video	Nomor Telp.	*User* ID
WhatsApp	12	0	0	6	6
Telegram	12	0	0	6	6
Skype	12	0	0	6	6

Tabel 4 menunjukkan hasil akuisisi *tool* OSForensic pada artefak digital dari aplikasi WhatsApp, Telegram, dan Skype berbasis *web* memiliki hasil yang sana dengan perolehan berupa 12 pesan teks, 6 nomor telepon, dan 6 *user* ID. Artefak digital yang berhasil diakuisisi dari masing-masing aplikasi *instant messaging* berbasis *web* akan digunakan untuk menentukan nilai *vulnerability* dari masi-masing aplikasi tersebut. Nilai *vulnerability* tesebut ditentukan berdasarkan pada jumlah artefak digital yang berhasil diakuisi berbanding dengan data awal artefak tersebut.

3.3. *Presentation*

Hasil akuisisi artefak digital dari aplikasi WhatsApp, Telegram, dan Skype menjadi dasar untuk menentukan nilai *vulnerability* dari masing-masing aplikasi tersebut. FTK imager dan OSForensic merupakan *tool* yang digunakan itu melakukan proses akuisisi artefak digital dari ketiga aplikasi *instant messaging* tersebut. Tabel 5 menunjukkan keseluruhan data artefak digital aplikasi WhatsApp yang telah berhasil diakuisisi menggunakan *tool* FTK imager dan OSForensic.

Tabel 5. Hasil Akuisisi Data Artefak Digital WhatsApp Berbasis *Web*

No	Jenis Data	Jumlah Data Awal	Jumlah Data yang Berhasil Diakuisisi
1.	Pesan teks	12	12
2.	Pesan gambar	9	0
3.	Pesan video	3	0
4.	Nomor telepon	6	6
5.	*User* ID	6	6

Berdasarkan hasil yang ditunjukkan pada table 5 aplikasi WhatsApp berbasis *web* memiliki nilai *vulnerability* sebesar 67%. Hasil tersebut diperoleh dengan menggunakan pertihungan perbandingan nilai indeks tidak tertimbang sebagai berikut:

$$\text{Nilai } vulnerability = \frac{24}{36} \times 100\%$$

Hasil keseluruhan akuisisi artefak digital aplikasi Skype berbasis *web* dengan menggunakan *tool* FTK imager dan OSForensic ditunjukkan pada Tabel 6.

Tabel 6. Hasil Akuisisi Data Artefak Digital Skype Berbasis *Web*

No	Jenis Data	Jumlah Data Awal	Jumlah Data yang Berhasil Diakuisisi
1.	Pesan teks	12	12
2.	Pesan gambar	9	9
3.	Pesan video	3	0
4.	Nomor telepon	6	6
5.	*User* ID	6	6

Nilai *vulnerability* aplikasi Skype berbasis *web* berdasarkan hasil yang ditunjukkan pada Tabel 6 adalah sebesar 92%. Hasil tersebut didapatkan melalui perhitungan perbandingan nilai indeks tidak tertimbang sebagai berikut:

$$\text{Nilai } vulnerability = \frac{33}{36} \times 100\%$$

Artefak digital aplikasi Telegram berbasis *web* yang telah berhasil diakuisisi menggunakan *tool* FTK imager dan OSForensic ditunjukkan pada Tabel 7.

Tabel 7. Hasil Akuisisi Data Artefak Digital Telegram Berbasis *Web*

No	Jenis Data	Jumlah Data Awal	Jumlah Data yang Berhasil Diakuisisi
1.	Pesan teks	12	12
2.	Pesan gambar	9	0
3.	Pesan video	3	0
4.	Nomor telepon	6	6
5.	*User* ID	6	6

Aplikasi Telegram berbasis *web* memiliki nilai *vulnerability* sebesar 67% berdasarkan hasil yang ditunjukkan pada Tabel 7. Nilai tersebut diperoleh melalui perhitungan perbandingan nilai indeks tidak tertimbang sebagai berikut:

$$\text{Nilai } vulnerability = \frac{24}{36} \times 100\%$$

4. Kesimpulan

Berdasarkan hasil dari penelitian tentang komparatif nilai *vulnerability* aplikasi WhatsApp, Telegram dan Skype berbasis *web* memberikan kesimpulan bahwa pada aplikasi Skype berbasis *web* memiliki nilai *vulnerability* tertinggi dengan perolehan nilai sebesar 92%, sedangkan aplikasi WhatsApp dan Telegram memiliki nilai *vulnerability* yang sama dengan perolehan nilai masing-masing sebesar 67%. Hasil dari penelitian ini dapat dijadikan referensi pengguna aplikasi *instant messaging* agar lebih berhati-hati dalam memilih dan menggunakan aplikasi tersebut.

Daftar Rujukan

[1] 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.

[2] 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.

[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] D. Vadlamudi, D. K. Thirupathi Rao, P. Vidyullatha, and B. AjasekharReddy, "Analysis on digital forensics challenges and anti-forensics techniques in cloud computing," *Int. J. Eng. Technol.*, vol. 7, no. 2.7, p. 1072, 2018, doi: 10.14419/ijet.v7i2.7.12230.

[7] 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.

[8] 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.

[9] 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.

[10] T. D. Larasati, "Live Forensics Perbandingan Aplikasi Instant Messenger Live Forensics Analysis for Comparing Instant Messenger Applications (Line , Facebook , and Telegram) on Windows 10 Operating System . Live Forensics," 2017.

[11] T. D. Transformation, "CURRENT STATE OF CYBERCRIME e Digital Transformation of Cybercrime," 2019.

[12] I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and

entification of LINE Messenger on Android Device," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 16, no. June, pp. 201–205, 2018.
[13] M. A. Aziz, I. Riadi, and R. Umar, "Analisis Forensik LINE Messenger Berbasis Web Menggunakan Framework National Institute of Justice," vol. 2018, no. November, pp. 51–57, 2018.
[14] M. Faiz and W. A. Prabowo, "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," vol. 1, no. December, 2018, doi: 10.20895/INISTA.V1I1.
[15] 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, : 10.25126/jtiik.202071921.
[16] Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool mparison 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.
[17] E. Pimenidis, "Computer Anti-forensics Methods and Their Impact on Computer Forensic Investigation Computer Anti-forensics Methods and Their Impact on," no. August 2009, pp. 145–155, 2016, doi: 10.1007/978-3-642-04062-7.
[18] 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.
[19] 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.
[20] 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.
[21] 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, pp. 93–98, 2017, doi: 10.25124/jrsi.v4i01.149.
[22] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic vestigation Framework Version 2," no. September, 2018.
[23] 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.
[24] 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, 18.
[25] 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.

HASIL CEK_60020397_Point-C45-IRD-850GB-Comparative Security Analysis of Web-Based Instant Messaging Applications

ORIGINALITY REPORT

9%	8%	3%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to President University Student Paper	2%
2	jurnal.iaii.or.id Internet Source	2%
3	index.pkp.sfu.ca Internet Source	2%
4	thesai.org Internet Source	1%
5	kinetik.umm.ac.id Internet Source	1%
6	insightsociety.org Internet Source	1%
7	Sucipto Sucipto, Jamilah Karaman. "Integration of Legalization Information System Web-Based using Shipping API and Telegram API", JUITA: Jurnal Informatika, 2020 Publication	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		