

Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensik Pendekatan Statis Dan Dinamis

Eka Dewi Melania 1^a, Indra Gunawan 2^{b*}

^a Jurusan Teknik Elektro

^b Jurusan Informatika

^{ab} Sekolah Tinggi Teknologi Ronggolawe

* Penulis Korenspondensi, Alamat Email: igunstr@mail.com

Diterima : 29-12-2021

Direview : 29-12-2021

Diterbitkan : 31-12-2021

Intisari

Kejahatan dunia maya setiap tahunnya mengalami peningkatan salah satunya adalah kebocoran data. Aplikasi android non Playstore tidak dijamin keamanannya karena sistem aplikasi hanya mempunyai akses ke direktori khusus, dan inilah yang memperumit proses instalasi pengguna aplikasi non Playstore. Pada penelitian ini penulis melakukan analisis keamanan dengan 5 aplikasi non Playstore dengan pendekatan statis dan dinamis, setelah melakukan eksperimen menggunakan software Wireshark dan Network Miner dengan tahapan alur proses metode dari National Institute of Justice (NIJ) yang terbagi menjadi lima tahapan yakni identification, collection, examination, analysis, dan reporting telah mendapatkan bukti bahwa aplikasi non Playstore dicurigai tidak menjamin keamanan data pengguna.

Pada aplikasi yang dipantau ini yang nantinya akan memperoleh bukti digital berisi aman atau tidaknya aplikasi android dari tingkat ancaman tindak kejahatan dengan menggunakan metode statis untuk membongkar program aplikasi dan dinamis digunakan untuk melihat keamanan datanya yang terpapar apakah terdapat virus pada aplikasi tersebut serta kebocoran data lainnya. dari analisis ini dapat diperoleh hasil eksperimen menggunakan software Wireshark dan Network Miner untuk dianalisis.

Penelitian ini bertujuan untuk menganalisis tingkat kerentanan aplikasi yang bersumber dari non Playstore dengan tingkat ancaman. Hasil yang didapatkan dari aplikasi 5 yang dipantau diketahui bahwa aplikasi Michat Lite dan Bigo Live memiliki risiko Extreme Risk dengan poin 45 %, pada aplikasi Rolling Scrooll, Flying Sketboard diketahui High Risk risiko tinggi dengan point 25%, sedangkan aplikasi Crash Car Engine memiliki tingkat keamanan Moderate Risk dengan risiko yang sedang dengan point 20%. Kesimpulan dari penelitian ini adalah aplikasi yang diinstal dari pihak ketiga memiliki tingkat ancaman yang lebih tinggi jika dibandingkan aplikasi resmi yang ada pada Playstore..

Kata Kunci : Analisis Keamanan, Forensik, Android, Pendekatan Statis Dan Dinamis

Abstract

The crime of cyberspace every year has increased, one of which is a data leak. The non-playstore Android application is not guaranteed its security because the application system only has access to special directories, and this is what complicates the installation process of non-playstore application users. In this study the author conducted a security analysis with 5 non-playstore applications with a static and dynamic approach, after experimenting using Wireshark and Network Miner software with the process of the process of the method of the method of the National Institute of Justice (NIJ) which was divided into five stages, namely identification, collection, collection, Collection Examination, Analysis, and Reporting have received evidence that the non-playstore application is suspected not guarantee user data security.

In this monitored application which will later obtain digital proof of safe or whether or not Android applications from the threat level of crime by using a static method to dismantle the application and dynamic programs used to see the data security exposed whether there is a virus in the application and other data leaks. From this analysis it can be obtained by experimental results using Software Wireshark and Network Miner to be analyzed.

This study aims to analyze the vulnerability level of applications sourced from non-playstore with a threat level. The results obtained from the 5 applications are monitored, it is known that the MICHAT Lite and BIGO LIVE application has an extreme risk with 45% points, on the Rolling Scroll application, Flying Sketchboard is known to high risk high risk with 25% point, while the Car Engine crash application has a security level Moderate risk with a risk that is 20%. The conclusion of this study is that applications installed from third parties have a higher level of threat when compared to the official application on the Playstore

Keywords : Security analysis, forensic, android, static and dynamic approach

1. Pendahuluan

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat, kebutuhan akan mobilitas membuat masyarakat di seluruh belahan dunia marak menggunakan gadget seperti tablet dan smartphone dengan berbagai macam sistem operasi. Sistem operasi untuk perangkat smartphone yang paling banyak digunakan adalah

Android yakni sebanyak 76,82% dari total market share (Rusdi et al., 2019).

Meskipun memiliki kelebihan yang bagus tidak menjamin aplikasi android non Playstore itu aman karena sistem aplikasi hanya mempunyai akses ke direktori khusus, dan inilah yang memperumit proses instalasi pengguna aplikasi non Playstore. Setelah diberikan izin untuk menginstal

aplikasi non Playstore, izinnya akan berhenti lalu prosesnya akan dimulai ketika aplikasi dibuka. Sehingga aplikasi tidak dapat berkerja di background, dan membuat aplikasinya terlihat Crash atau bermasalah.

Penelitian ini bertujuan untuk melakukan analisis keamanan hanya 5 aplikasi non Playstore dengan menggunakan metode statis untuk membongkar program aplikasi dan dinamis digunakan untuk melihat keamanan datanya yang terpapar apakah terdapat virus pada aplikasi tersebut serta kebocoran data lainnya. Pada aplikasi yang dipantau ini yang nantinya akan memperoleh bukti digital berisi aman atau tidaknya aplikasi android dari tingkat ancaman tindak kejahatan seperti aplikasi Rolling Scrooll yang bersumber dari <https://m.apkpure.com>, aplikasi Flying Skateboard yaitu <https://m.apkpure.com>, aplikasi Crash Car Engine yang bersumber dari <https://m.apkpure.com>, aplikasi Michat Lite yang bersumber dari <https://m.apkpure.com>, sumber yang diperoleh dari aplikasi Bigo Live yang bersumber <https://m.apkpure.com>. Dari aplikasi tersebut dapat mengendalikn permasalahan yang terjadi nantinya.

Ada beberapa penelitian yang sudah pernah dilakukan yang berkaitan dengan dengan pendekatan statis dan dinamis, diantara lain adalah penelitian pertama oleh (Syaputra et al., 2020) "Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis dan Statis" hasil penelitian menunjukkan bahwa Dalam menganalisis program tersebut, diperlukan tahap pengujian yang dapat digunakan sebagai acuan dalam menentukan karakteristik dan menggali informasi terkait dari perilaku yang akan ditimbulkan oleh program malware tersebut. Penelitian kedua oleh (Riadi et al., 2018) dengan judul "Analisis forensic digital pada frozen solid state drive dengan metode National institute of justice (NIJ). Penelitian ini membahas perbandingan terkait tools Forensik yang digunakan untuk proses eksaminasi dan analisa.

Dari penelitian yang dilakukan sebelumnya tentang metode statis dan dinamis pada malware untuk berikan pembelajaran tentang efek yang ditimbulkan oleh malware dan membantu praktisi dalam menemukan barang bukti digital (Syaputra et al., 2020), penelitian oleh (Riadi et al., 2018) data yang tersimpan tidak akan hilang penelitian. (Rusdi et al., 2019) dan (Riskiyadi, 2020) menyatakan bahwa analisis digital forensik amat berguna untuk memantau apakah aplikasi yang beredar di non Playstore benar benar aman dari pencurian data dan kejahatan lainnya atau tidak. Dari pernyataan diatas yang membuat penulis tertarik untuk mengembangkan penelitian dan menganalisis dengan menggunakan metode pendekatan Statis dan Dinamis. Menggunakanya ke dalam karya ilmiah tugas akhir skripsi yang berjudul "Analisis keamanan aplikasi android non Playstore dengan metode digital forensik pendekatan statis dan dinamis".

Penelitian pertama dilakukan oleh (Syaputra et al., 2020) yang berjudul "Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis dan Statis" hasil penelitian ini berpotensi digunakan sebagai bukti digital

mempunyai beberapa karakteristik dari program malware pada umumnya yaitu melakukan penambahan dan perubahan terhadap sistem (*Windows Registry* dan *_le prefetch*) sebagaimana ditemukan seperti kode *string* atau *secret agent*" serta perilaku ketika program *poison ivy* diaktifkan tidak memberikan informasi maupun akti_tas secara kasat mata melainkan dalam perilakunya program *poison ivy* berupaya untuk menghubungkan diri pada program induknya yang dilakukan pada proses background (tidak kasat mata). Dari penelitian ini, telah diketahui Cara kerja program *poison ivy* dapat dianalisis menggunakan dua metode analisis *malware* yaitu metode analisis malware dinamis yang dapat memberikan solusi dalam Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis dan Statis.

Penelitian kedua dilakukan oleh (Riadi et al., 2018) yang berjudul "Analisis forensic digital pada frozen solid state drive dengan metode national institute of justice (NIJ)" hasil penelitian ini dilakukan pada implementasi salah satu software pembeku drive yaitu *Shadow Defender* yang dapat membekukan suatu drive SSD (*frozen solid state drive*) dan terbukti berpengaruh terhadap praktik eksaminasi dan analisa forensik didapatkannya bukti-bukti digital.

Penelitian ketiga dilakukan oleh (Rusdi et al., 2019) yang berjudul "Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis" hasil penelitian ini dapat mendeteksi karakteristik dari malware pada perangkat android dengan kelebihan dan kekurangan masing-masing. Analisis statis dengan teknik *reverse engineering* dapat dilakukan untuk memahami fungsi malware dengan melihat perizinan yang digunakan dan kode sumber. Analisis dinamis dapat dilakukan untuk melihat bagaimana perilaku dari malware ketika dipasang dan dijalankan serta aktifitas jaringan.

Penelitian keempat dilakukan oleh (Riskiyadi, 2020) yang berjudul "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkapkan CYBERCRIME" Hasil Penelitian ini dari proses investigasi forensik bukti digital dari bukti elektronik *flash disk*, perbedaan perlakuan pada *flash disk* memberikan hasil yang berbeda, yang ditunjukkan dengan nilai *hash* yang berbeda dari masing-masing perlakuan.

Berdasarkan latar belakang diatas, maka permasalahan yang ingin dibahas oleh penulis adalah "Bagaimana melakukan analisis keamanan aplikasi android non Playstore menggunakan metode digital forensik pendekatan statis dan dinamis".

2. Kerangka Teori

2.1 Forensik Digital

Forensik digital atau forensik adalah suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengoleksi, menganalisa dan menguji bukti-bukti digital pada saat menangani sebuah kasus yang memerlukan penanganan dan identifikasi barang digital ilmu forensik, terutama dapat menyelidiki dari penemuan konten perangkat digital, dan seringkali dikaitkan dengan kejahatan. Istilah forensik digital pada awalnya identik dengan forensik komputer tetapi kini telah diperluas untuk menyelidiki semua perangkat yang dapat menyimpan data digital (Parmaza, 2018).

2.2 Pendekatan Statis

Metode statis yaitu membongkar program aplikasi. Penjelasan ringkas mengenai hal tersebut dapat dilihat dengan menggunakan statis untuk mengetahui pada pengguna yang melakukan akan tidak kejahatan (Fianggara, 2018). Dengan cara memakai aplikasi *manifest* untuk melakukan analisis dengan aplikasi-aplikasi forensik.

2.3 Analisis Dinamis

Metode analisis aplikasi dengan cara menjalankan aplikasi. Diketahui keuntungan dari analisis ini yaitu aplikasi yang diuji diperiksa dan diaktifkan menggunakan *software* virtual untuk selanjutnya dapat dikumpulkan informasi yang rentan dimasuki peretas cara kerja analisis ini yaitu penulis akan memantau dan memonitor trafik jaringan (*network trafik*) dan sumber komunikasi lainnya seperti kebocoran data untuk mengetahui aktivitas yang mencurigakan (Karuniawan, 2016).

2.4 Perizinan Hak Akses

Normalnya pada aplikasi game hanya memerlukan akses perizinan seperti pada Tabel 1 dengan ketentuan normal *permission*. Sedangkan akses yang tidak normal dapat dilihat pada Tabel 1 dengan ketentuan *dangerous permission*. Maka dinyatakan *dangerous permission* jika memiliki kemungkinan mengambil data-data pribadi dari perangkat pengguna, terdeteksi malware saat proses pemasangan aplikasi. Hal ini dapat diketahui melalui metode statis dengan cara membongkar file program *manifest.xml*.

Tabel 1. Perizinan Hak Akses Game (Rusdi et al., 2019)

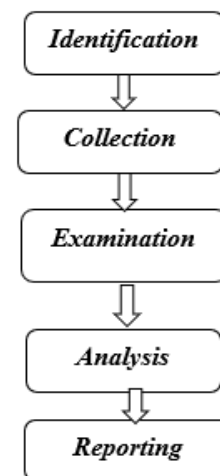
N O	Normal Permission	Dangerous Permission
1	INTERNET	READ_PHONE_STATE
2	ACCESS_NETWORK_STATE	ACCESS_COARSE_LOCATION
3	WAKE_LOCK	WRITE_EXTERNAL_STORAGE
4	RECEIVE_BOOT_COMPLETED	READ_EXTERNAL_STORAGE
5	BILLING	REQUEST_INSTALL_PACKAGES
6	VIBRATE	INSTALL_SHORTCUT
7	ACCESS_WIFI_STATE	WRITE_CALENDAR
8	RECEIVE	SET_ALARM

Normalnya pada aplikasi game hanya memerlukan akses perizinan seperti pada Tabel 1 dengan ketentuan normal *permission*. Sedangkan akses yang tidak normal dapat dilihat pada Tabel 1 dengan ketentuan *dangerous permission*. Maka

dinyatakan *dangerous permission* jika memiliki kemungkinan mengambil data-data pribadi dari perangkat pengguna, terjadi kebocoran data saat melakukan proses analisis. Hal ini dapat diketahui melalui metode statis dengan cara membongkar file program *manifest.xml*.

2.5 Tahap Forensik

Secara umum ada empat tahapan yang harus dilakukan dalam mengelola bukti pada forensik digital yaitu pengumpulan, pemeliharaan, analisa, dan presentasi. Dalam tugas akhir ini, penulis menggunakan metode penelitian dari (Riadi et al., 2018). Pada penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensik dari *National Institute of Justice (NIJ)*. Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Disebutkan tahapan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data forensik. Tahapan berikut pada Gambar 1



Gambar 1 Tahap Forensik

Tahapan metode dari *National Institute of Justice (NIJ)* ini terbagi menjadi lima tahapan yakni *identification*, *collection*, *examination*, *analysis*, dan *reporting*, secara lengkap dipaparkan sebagai berikut:

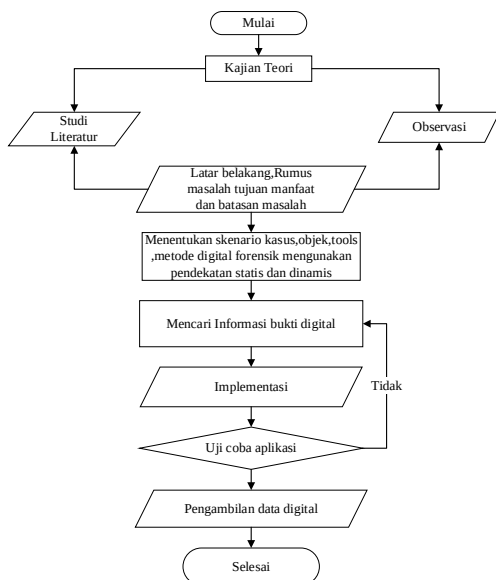
- *Identification* merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital.
- *Collection* merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital.
- *Examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual.

- *Analysis* atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif barang bukti digital.
- *Reporting* atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis.

3. Metodologi

3.1 Desain Penelitian

Diagram alir penelitian diperlukan untuk melakukan perencanaan proses, analisis proses, dan dokumentasi proses sebagai pedoman untuk melakukan penelitian, berikut diagram alir penelitian yang ditampilkan pada gambar 3.1



Gambar 3. 1 Diagram Alur Penelitian

3.2 Metode Pengumpulan Data

Dalam penelitian ini menggunakan metode pengumpulan data meliputi :

a. Studi Literatur

Studi literatur ini dilakukan oleh penulis untuk mengumpulkan sumber- sumber tertulis, dengan cara membaca, mempelajari dan mencatat hal-hal penting yang berhubungan dengan masalah yang sedang harus diselesaikan.

b. Observasi

Observasi yang dilakukan oleh penulis adalah dengan mengamati secara langsung terhadap objek penelitian. Observasi dilakukan untuk memperoleh informasi secara langsung terhadap permasalahan yang sedang diteliti untuk menentukan analisis system yang benar-benar sesuai.

3.3 Sumber Data

Data yang digunakan dalam penulisan kali ini merupakan data sekunder dimana data tersebut diambil dari jurnal- jurnal yang berkaitan dan internet. Untuk pengamatan aplikasi android yang akan diuji sendiri selama 2 jam menggunakan *software Wireshark* yang

digunakan kemudian akan dianalisis apakah aplikasi ini benar-bener aman dari kebocoran data menggunakan *Network Miner* dan sebagainya.

3.4 Peralatan Operasional

1. Hardware Yang Digunakan

Agar sistem dapat berjalan dengan baik, diperlukan beberapa perangkat keras yang mendukung sistem ini. Perangkat keras yang digunakan dalam perancangan sistem adalah sebagai berikut :

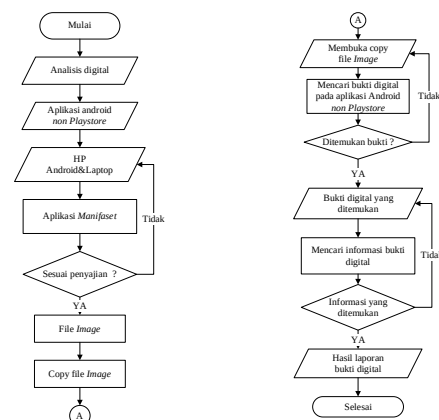
- Laptop/ PC
- Smartphone Android
- Wifi
- Memory RAM 2 GB
- Keyboard dan Mouse Standart

Software Yang Digunakan

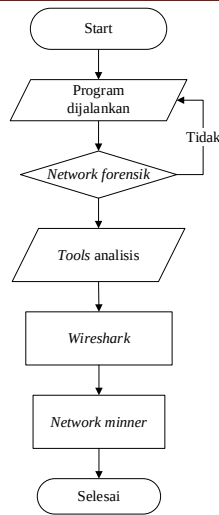
Adapun *software* yang digunakan sesuai dengan spesifikasi kebutuhan, diantaranya:

- Sistem operasi windows 10
- Browser (mozilla firefox, google chrome)
- Wireshark
- Network Miner
- Visio

Tahapan *indetification, collection, examination, analysis* dan *reporting* digambarkan dalam *flowchat* yang menggunakan metode statis dan dinamis gambar 3.2 seperti berikut :



Gambar 3. 2 Flowchart Analisis Statis



Gambar 3. 3 Flowchart Dinamis

4. Hasil dan Pembahasan

Tingkat Ancaman Aplikasi

Perizinan yang didapat dari hasil *decode* dikelompokkan berdasarkan tingkat ancaman keamanan tersebut untuk mengetahui potensi kerusakan yang akan ditimbulkan oleh malware 5 aplikasi yang dipantau :

Tabel 4. 1 Ancaman Pada Setiap Aplikasi (Sumber : Anggi Elanda, 2018)

N O	Nama Aplikasi	Risiko	Risk Level	Keterangan
1.	Rolling Scrooll	Malware	High Risk	Kemungkinan terjadinya Sangat tinggi, karena banyak iklan dan virus trojan saat terhubung ke internet.
2.	Crash car engine	ROOTING	Moderate Risk	Terjadi risiko sedang, dikarenakan pada saat rooting terjadi boodluck atau kegagalan dalam sistem operasi.
3.	Michat Lite	Data mencurigakan	Extreme Risk	Dampaknya sangat tinggi, karena terjadinya kebocoran data file yang mencurigakan.
4.	Flying Sketboard	Malware	High Risk	Terdapat risiko tinggi yang terjadi, dikarenakan terdeteksi malware yang membahayakan perangkat

				dan banyak iklan situs yang masuk.
5.	Bigo Live	Gambar Image	Extreme Risk	Memiliki risiko tinggi, dikarenakan dapat mengakibatkan terjadinya ketidakamanan sebuah privasi pada gambar.

Kemungkinan yang menentukan dari daftar penilaian risiko dibawah ini dilakukan analisis untuk memprioritaskan mengenai seberapa besar level resiko paling tinggi dan seberapa tingkat risiko paling sedang sampai rendah yang telah disebutkan diatas akan terjadi hasilnya adalah sebagai berikut :

Tabel 4. 2 Keterangan Risk Level

Risk Level	Point
Low Risk	10
High Risk	25
Moderate Risk	20
Extreme Risk	45

5. Simpulan

Berdasarkan hasil analisa dan perancangan, serta eksperimen sistem dan pembahasan bab-bab sebelumnya, maka penelitian pada Tugas akhir ini dapat diambil kesimpulan sebagai berikut :

1. Analisis keamanan aplikasi android *non Playstore* yang dilakukan menggunakan metode dari *National Institute of Justice (NIJ)* dengan lima tahapan yakni *identification, collection, examination, analysis, dan reporting* telah mendapatkan hasil bukti sesuai dengan yang diharapkan penulis.
2. Hasil yang didapatkan dari aplikasi 5 yang dipantau diketahui bahwa aplikasi *Michat Lite* dan *Bigo Live* memiliki Risiko *Extreme Risk* dengan poin 45 % karena adanya kebocoran data berupa Pdf, Word, Mp3, Zip sedangkan *Bigo Live* terdapat *Gambar Image* yang bersifat privasi, dan pada aplikasi *Rolling Scrooll, Flying Sketboard* diketahui *High Risk* risiko tinggi dengan point 25% dikarenakan terdeteksi *malware* yang disebabkan oleh berbagai banyak virus dan iklan pada saat dianalisis. pada aplikasi tersebut sudah diketahui bahwa terdapat ancaman yang diindikasikan dengan hak akses pada aplikasi tersebut, setelah melalui proses analisis, aplikasi ini diketahui memiliki kerentanan yaitu berpotensi untuk mencuri data pengguna pada aplikasi dijalankan, sedangkan aplikasi *Crash Car Engine* memiliki tingkat keamanan *Moderate Risk* dengan risiko yang sedang dengan point 20%, tingkat kebahayaan yang lebih akurat belum mampu didapatkan karena terbatasnya teknik analisis yang digunakan (tidak melalui proses *rooting*).

3. Aplikasi yang dipasang dari pihak ketiga memiliki tingkat ancaman yang lebih tinggi jika dibandingkan Aplikasi resmi yang ada pada *Playstore*.

Yunanri, Riadi, I., & Yudhana, A. (2018). Analisis Deteksi Vulnerability Pada Web Server Open Journal System Menggunakan OWASP Scanner. In *Jurnal Rekayasa Teknologi Informasi (JURTI)* (Vol. 2, Issue 1, p. 1). <https://doi.org/10.30872/jurti.v2i1.1319>

5.2 Saran

Pada penelitian ini belum ditemukan *database* dikarenakan belum melakukan proses *rooting*. Diharapkan pada penelitian selanjutnya dapat melakukan proses analisis dengan melakukan proses *rooting* terlebih dahulu. Dikarenakan analisis membutuhkan waktu yang lebih lama, selain itu *https* harus di *intercept* menjadi *http* sehingga peluang untuk menemukan bukti lebih besar. Semua virus dan app komunikasi dengan server memakai protokol *https* yang tidak seluruhnya dapat terbaca pada *Network Miner* karena memiliki keamanan berupa *enkripsi*.

Daftar Pustaka

- ALBone, A. (2009). *Pembuatan rencana keamanan informasi berdasarkan analisis dan mitigasi risiko teknologi informasi*. 68.
- Fianggara, A. Ji. (2018). No Title. *Mahasiswa Universitas Brawijaya*. <http://blog.ub.ac.id/jihadalif/2018/11/12/ekonomi-kelembagaan-dan-pertumbuhan-ekonomi/>
- Gunawan, Indra (2021). Keamanan Data: Teori dan Implementasi.
- Gunawan, Indra (2020). Analisis Malware Botnet Proteus Pendekatan Statis dan Dinamis. *Simetris(Jurnal Teknologi dan Sain Terapan)*. vol 14(2), 12-17.
- Jati, S. A. (2020). Aplikasi non Play Store. *Detikinet*. <https://inet.detik.com/mobile-apps/d-5043132/aplikasi-non-play-store-bakal-dipersulit-di-android-11>
- Karuniawan, M. I. (2016). *Penerapan Analisis Dinamis Untuk Pengujian Aplikasi Sia Umj Mobile*.
- Kristianto, E. D. (2013). *NETMINE R, TOOL MONITORING JARINGAN*.
- Manfaat Aplikasi Android. (2006). *Proteknologi*. <https://proteknologi.com/informasi-manfaat-aplikasi-android>
- Obengplus. (2019). *Obengplus Permission Android*. WWW.Obengplus.COM.
- Parmaza, B. (2018). Forensik Digital. *KomTIK.Jambi*. <http://itjambi.com/apa-itu-digital-forensics-forensik-digital/>
- Paryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008, 2008(semnasIF)*, 379–386.
- Purwanto, E. (2017). Keamanan Informasi. *BBPTIK*. <https://bpptik.kominfo.go.id/2014/03/24/404/keamananinformasi/amp/#referer=%0Ahttps://www.google.com&csi=0%0A>
- Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ). 3(May), 70–82. <https://doi.org/10.21831/elinvo.v3i1.19308>
- Riskiyadi, M. (2020). INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP FORENSIC INVESTIGATION OF DIGITAL EVIDENCE TO REVEALING. 3(2), 12–21.
- Rubin, andy. (2004). Aplikasi Android. *Wikipedia*. https://id.wikipedia.org/wiki/Andy_Rubin
- Rusdi, A. S., Widiyasono, N., & Sulastri, H. (2019). *Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis*. 24.
- Sidiq, M. F., & Faiz, M. N. (2019). Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, 5(1), 67. <https://doi.org/10.26418/jp.v5i1.31430>
- Susanti, I., Sumiyati, S., & Tritjahjono, R. I. (2020). Tinjauan Pemetaan Risiko Pada Perguruan Tinggi Negeri Satuan Kerja Berdasarkan Pp No 60 Tahun 2008 Tentang Sistem Pengendalian Intern Pemerintah (Studi Kasus Di Politeknik Negeri Bandung). *Sebatik*, 24(2), 327–334. <https://doi.org/10.46984/sebatik.v24i2.1138>
- Susianto, D., & Rachmawati, A. (2018). Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner (Studi Kasus: AMIK Dian Cipta Cendikia). *Jurnal Cendikia*, XVI, 120–125.
- Syaputra, R., Informatika, T., & Mdp, S. G. I. (2020). *Studi Literatur Analisis Malware Menggunakan Metode Analisis Dinamis dan Statis*. 01(01), 14–24.