Analisis *Digital Forensic* Aplikasi Pelacak Nomor *Handphone Android* Pihak Ketiga Menggunakan Metode Statis Dan Dinamis

Digital Forensic Analysis Of Third Party Android Cellphone Number Tracker Applications Using Static And Dynamic Methods

Indra Gunawan*[1], Oei Gregorius Grasia[2]
[1,2,3] Program Studi Informatika, Sekolah Tinggi Teknologi Ronggolawe Cepu
e-mail: *[1] igunsttr@gmail.com

Abstrak **-** *Teknologi informasi pada dasarnya dibutuhkan manusia untuk mempermudah kegiatannya tanpa perlu membuang tenaga serta biaya dan dapat memberikan hasil yang maksimal secara cepat dan akurat. Salah satunya yaitu dengan menggunakan Handphone Android. Tujuan penelitian ini adalah untuk mengetahui tingkat keamanan aplikasi GetContact Mod, Truecaller Mod, Phone Number Locator, Showcaller, dan phone Number Tracker dengan menggunakan metode Statis dan Dinamis Forensic. Analisis ini menggunakan 2 metode yaitu dinamis menggunakan Wireshark dan Network Miner sebagai aplikasi perekam aktifitas jaringan, Mobile Security Framework sebagai metode statis untuk menganalisis file sumber kelima aplikasi. Hasil penelitian menggunakan metode statis menunjukkan bahwa aplikasi Getcontact adalah aplikasi yang paling direkomendasikan dan paling aman. Sedangkan menggunakan metode dinamis tidak menunjukkan adanya kebocoran data pribadi pada aplikasi yg diteliti.*

Kata kunci – Analisis statis dan dinamis, Forensica digital, analisis keamanan, aplikasi android

Abstract *- Information technology is basically needed by humans to facilitate their activities without the need to waste energy and costs and can provide maximum results quickly and accurately. One of them is by using an Android cellphone. The purpose of this study was to determine the security level of the GetContact Mod, Truecaller Mod, Phone Number Locator, Showcaller, and Phone Number Tracker applications using Static and Dynamic Forensic methods. This analysis uses 2 methods, namely dynamic using Wireshark and Network Miner as network activity recorder applications, Mobile Security Framework as a static method to analyze the source files of the five applications. The results of research using static methods show that the Getcontact application is the most recommended and safest application. Meanwhile, using the dynamic method does not indicate any leakage of personal data in the application under study.*

Keywords - Static and dynamic analysis, digital forensics, security analysis, android application

I. PENDAHULUAN

Teknologi informasi pada dasarnya dibutuhkan manusia untuk mempermudah kegiatannya tanpa perlu membuang tenaga serta biaya dan dapat memberikan hasil yang maksimal secara cepat dan akurat. Salah satunya yaitu dengan menggunakan Handphone Android. Teknologi yang sedang banyak dicari manusia saat ini untuk mengetahui informasi yang dicari adalah aplikasi pelacak nomor seluler. Hal ini dikarenakan banyaknya kasus penipuan menggunakan nomor-nomor yang tidak dikenal yang sering menghubungi

dan membuat tidak nyaman. Banyaknya aplikasi pelacak nomor seluler ini dan bermunculan aplikasi-aplikasi baru membuat pengguna Smartphone Android terkadang salah memilih aplikasi yang aman untuk Smartphone Android mereka, salah satunya aplikasi pelacak nomor seluler dari pihak ketiga. Misalnya pada aplikasi GetContact Mod, Truecaller Mod, Phone Number Locator, Showcaller, dan phone Number Tracker. Kelima aplikasi tersebut juga tidak dapat diunduh di Play Store dikarenakan belum memiliki izin resmi. Aplikasi tersebut hanya dapat diunduh lewat situs web/apk dari pihak ketiga. Seperti yang kita ketahui bahwa mengunduh aplikasi dari pihak ketiga sangat beresiko dibandingkan mengunduh aplikasi lewat Situs Resmi.

Ada beberapa penelitian yang sudah dilakukan yang berkaitan dengan analisis digital Forensic, antara lain yaitu penelitian pertama oleh Melania, D.E dan Gunawan, I. [5] yang berjudul "Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensic Pendekatan Statis Dan Dinamis". Penelitian kedua oleh Krisdayanti, N dan Gunawan, I. [2] yang berjudul "Analisis Keamanan Aplikasi Chat Android Pihak Ketiga Atau Non Playstore Menggunakan Digital Forensics" . Penelitian ketiga oleh (Gazhi, Erza., 2018) dengan judul "Permission-based Privacy Analysis for Android Applications". Perbedaan penelitian berikut dengan penelitian sebelumnya adalah penulis akan membuat kebaharuan dari penelitian sebelumnya yaitu GetContact Mod, Truecaller Mod, Phone Number Locator, Showcaller, dan phone Number Tracker sebagai studi kasus serta statis dan dinamis Forensic sebagai metode penelitian ini. Dan proses Forensic pada penelitian ini menggunakan aplikasi software Wireshark dan Network Miner.

Dari penelitian sebelumnya menunjukkan bahwa analisis pelacak lokasi sangat berguna untuk membantu pengguna smartphone android baru dalam mengatasi hal-hal yang berbahaya seperti kebocoran lokasi pribadi atau cybercrime. Hal inilah yang membuat penulis merasa tertarik untuk meneliti dan menganalisis dengan menggunakan metode statis dan dinamis Forensic dan meletakkan nya kedalam karya ilmiah tugas akhir skripsi yang berjudul "Analisis Digital Forensic Aplikasi Pelacak Nomor Handphone Android Pihak Ketiga Atau Non Playstore Menggunakan Metode Statis Dan Dinamis".

1.1 Level Keamanan *Smartphone*

Keamanan informasi secara umum bertujuan untuk mengamankan ketiga faktor yaitu confidentiality, availability, dan integrity [1] yang pada akhirnya diturunkan menjadi banyak cabang. Keamanan smartphone memiliki cabang-cabang yang banyak. Dalam pengamanan sistem, banyak yang harus diperhatikan seperti database, keamanan data, keamanan smartphone, keamanan aplikasi, keamanan jaringan dan keamanan informasi. Pengamanan smartphone dilakukan berdasarkan level dan sistem. Berdasarkan level, pengamanan disusun seperti piramida, yaitu keamanan level 0, level 1, level 2, level 3, dan level 4. Sedangkan berdasarkan system, pengamanan smartphone dibedakan menjadi network topology, security information management, dan IDS/IPS.

Keamanan Level 0 merupakan keamanan fisik (physical security) atau keamanan tingkat awal. Apabila keamanan fisik terjaga maka keamanan di dalam smartphone juga akan terjaga. Keamanan Level 1 terdiri dari database security, data security, dan device security. Dari pembuatan database dapat dilihat apakah digunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan data security yaitu desain database, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah device security yaitu alat yang dipakai untuk keamanan dari database tersebut. Keamanan level 2 merupakan keamanan dari segi keamanan jaringan. Keamanan

ini merupakan tindak lanjut dari keamanan level 1. Keamanan level 3 merupakan information security. Informasi -informasi seperti kata sandi yang dikirimkan kepada teman atau file-file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut. Keamanan Level 4 adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi dikutip oleh [2].

1.2 Digital Forensic

Dalam bahasa Inggris Forensic artinya "yang berhubungan dengan kehakiman atau peradilan". Karena memang pada awalnya Forensic berguna untuk mengungkap bukti bukti yang digunakan dalam kasus peradilan. Bila digabungkan dengan digital yang artinya sesuatu yang berhubungan dengan komputer atau teknologi informasi. Maka, digital forensic atau Forensic digital adalah suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengumpulkan, menganalisa dan menguji bukti bukti digital yang menjadi kasus untuk ditangani.

Digital forensic merupakan aktifitas penyelidikan yang dilakukan untuk menemukan bukti digital yang akan memperkuat atau melemahkan bukti fisik dari kasus yang ditangani. Istilah Forensic digital pada awalnya identik dengan Forensic komputer. tetapi saat ini berkembang menjadi lebih luas yaitu menganalisa semua perangkat yang dapat menyimpan data digital. Forensic digital sendiri diperlukan karena biasanya data di perangkat digital dikunci, diganti, disembunyikan atau bahkan dihapus.

Penggunaan Forensic digital dimulai ketika penggunaan komputasi personal pada akhir 1970-an dan awal 1980-an, kemudian pada tahun 1990-an era dimulainya internet, dan baru pada awal abad ke-21 negara negara di dunia secara bertahap membentuk kebijakan terhadap pelaksanaan digital Forensic ini. Adapun tahapan dalam melakukan Forensic digital ada 5 (lima), yaitu:

1. Identification

Tahap identification atau tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti

2. Collection

Tahap collection atau tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.

3. Examination

Tahap examination atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara Forensic baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik hashing.

4. Analysis

Tahap 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 dengan metode yang dibenarkan secara teknik dan hukum

untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

5. Reporting

Tahap reporting atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tool, atau aspek pendukung lainnya pada proses tindakan digital Forensic. [2]

Gambar 1. Langkah-Langkah Digital Forensic

1.2.1 Metode Forensic Statis

Forensic statis menggunakan prosedur dan pendekatan konvensional di mana bukti di olah secara bit-by-bit image untuk melakukan proses Forensic. Proses Forensicnya sendiri berjalan pada sistem yang tidak dalam keadaan menyala. Forensic statik difokuskan pada pemeriksaan hasil imaging untuk menganalisis isi dari bukti digital, seperti berkas yang dihapus, riwayat penjelajahan web, berkas fragmen, koneksi jaringan, berkas yang diakses, riwayat user login, dll guna membuat timeline berupa ringkasan tentang kegiatan yang dilakukan pada bukti digital sewaktu digunakan [3].

1.2.2 Metode Forensic Dinamis

Analisis Dinamis merupakan metode analisis aplikasi dengan menjalankan aplikasi. Keuntungan dari analisis ini yaitu aplikasi yang diuji diperiksa dan diaktifkan menggunakan mesin virtual untuk selanjutnya dapat dikumpulkan informasi dan celah yang rentan dimasuki oleh peretas. Cara kerja analisis ini yaitu penulis akan memonitor trafik jaringan (Network Traffic) dan sumber komunikasi lainnya seperti database untuk mengetahui aktivitas yang mencurigakan. Dalam metode dinamis, program diuji kembali dan dievaluasi dengan menjalankan data secara langsung dengan tujuan menemukan kesalahan dalam program yang sedang berjalan untuk menghindari pemeriksaan secara berulang kali [4].

1.2.3 Mobile Security Framework (MobSF)

Mobile Security Framework (MobSF) adalah framework pengujian otomatis bersifat open-source, yang mampu melakukan analisis statis dan dinamis dalam melakukan proses analisis akan menampilkan hasil berupa laporan mengenai aplikasi android tersebut [4].

1.3 Studi Literatur

Teknologi informasi pada dasarnya dibutuhkan manusia untuk mempermudah kegiatannya tanpa perlu membuang tenaga serta biaya dan dapat memberikan hasil yang maksimal secara cepat dan akurat. Salah satunya yaitu dengan menggunakan Handphone Android. Teknologi yang sedang banyak dicari manusia saat ini untuk mengetahui informasi yang dicari adalah aplikasi pelacak nomor seluler. Hal ini dikarenakan banyaknya kasus penipuan menggunakan nomor-nomor yang tidak dikenal yang sering menghubungi

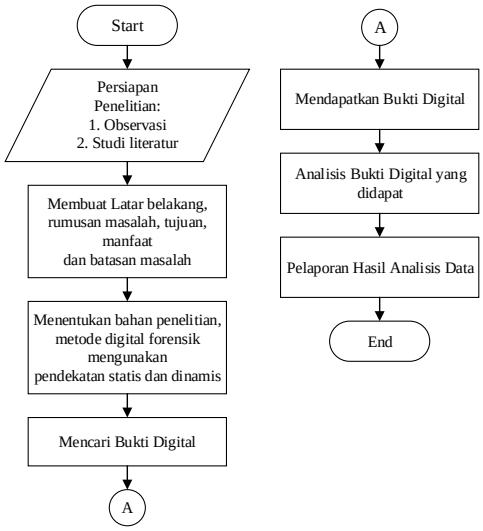
dan membuat tidak nyaman. Banyaknya aplikasi pelacak nomor seluler ini dan bermunculan aplikasi-aplikasi baru membuat pengguna Smartphone Android terkadang salah memilih aplikasi yang aman untuk Smartphone Android mereka, salah satunya aplikasi pelacak nomor seluler dari pihak ketiga. Misalnya pada aplikasi GetContact Mod, Truecaller Mod, Phone Number Locator, Showcaller, dan phone Number Tracker. Kelima aplikasi tersebut juga tidak dapat diunduh di Play Store dikarenakan belum memiliki izin resmi. Aplikasi tersebut hanya dapat diunduh lewat situs web/apk dari pihak ketiga. Seperti yang kita ketahui bahwa mengunduh aplikasi dari pihak ketiga sangat beresiko dibandingkan mengunduh aplikasi lewat Situs Resmi.

Ada beberapa penelitian yang sudah dilakukan yang berkaitan dengan analisis digital Forensic, antara lain yaitu penelitian pertama oleh [5] yang berjudul "Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensic Pendekatan Statis Dan Dinamis". Penelitian kedua oleh [2] yang berjudul "Analisis Keamanan Aplikasi Chat Android Pihak Ketiga Atau Non Playstore Menggunakan Digital Forensics" . Penelitian ketiga oleh [6] dengan judul "Permission-based Privacy Analysis for Android Applications". Perbedaan penelitian berikut dengan penelitian sebelumnya adalah penulis akan membuat kebaharuan dari penelitian sebelumnya yaitu GetContact Mod, Truecaller Mod, Phone Number Locator, Showcaller, dan phone Number Tracker sebagai studi kasus serta statis dan dinamis Forensic sebagai metode penelitian ini. Dan proses Forensic pada penelitian ini menggunakan aplikasi software Wireshark dan Network Miner. Dari penelitian sebelumnya menunjukkan bahwa analisis pelacak lokasi sangat berguna untuk membantu pengguna smartphone android baru dalam mengatasi hal-hal yang berbahaya seperti kebocoran lokasi pribadi atau cybercrime. Hal inilah yang membuat penulis merasa tertarik untuk meneliti dan menganalisis dengan menggunakan metode statis dan dinamis Forensic.

II. METODE

2.1 Desain Penelitian

Diagram alir penelitian sangat dibutuhkan untuk melakukan perencanaan proses, analisis proses, dan dokumentasi proses sebagai pedoman untuk melakukan suatu penelitian. Berikut diagram alir penelitian yang ditampilkan pada gambar 2.

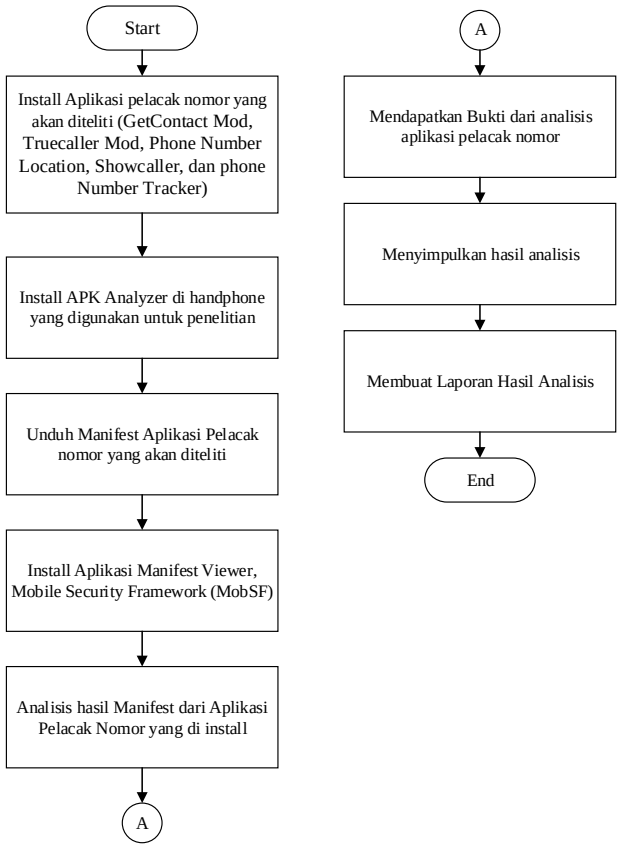


Gambar 2. Diagram Alir Penelitian.

2.2 Metode Pendekatan Statis

Berdasarkan Gambar 3 Analisis Statis adalah metode analisis aplikasi tanpa menjalankan aplikasi tersebut. Cara kerja metode analisis pendekataan statis yaitu penulis akan me-review kodingan dari aplikasi pelacak nomor untuk menemukan fungsi yang mencurigakan. Fungsi mencurigakan yang dimaksud adalah kode sensitif berupa username default, pin atau password. Keluaran dari proses ini yaitu signature yang dapat digunakan,salah satu fungsinya yaitu untuk mengetahui jenis enkripsi yang digunakan untuk mengamankan aplikasi. Penelitian dimulai dengan menginstall aplikasi chat yang akan di uji (GetContact Mod, Truecaller Mod, Phone Number Location, Showcaller, dan phone Number Tracker).

Setelah itu dilanjutkan dengan meng-install aplikasi APK Analyzer di handphone yang akan digunakan untuk penelitian, aplikasi ini berguna untuk melakukan ekstraksi file dari aplikasi pelacak nomor yang akan diuji. Lalu dilanjutkan dengan mengunduh *AndroidManifest.xml* dari aplikasi pelacak nomor. Setelah mengunduh *manifest* dari aplikasi pelacak nomor, dilanjutkan menginstall aplikasi Manifest Viewer untuk melihat hasil unduhan *manifest* dari aplikasi pelacak nomor di Handphone yang akan digunakan untuk menguji. Analisis hasil *manifest* aplikasi pelacak nomor yang sudah diunduh untuk menemukan bukti *manifest* yang tergolong aman (*Normal Permission*) atau tidak aman (*Dangerous Permission*). Selanjutnya menginstall *Mobile Security Framework* (MobSF) untuk pengujian penetreasi terhadap aplikasi seluler (Android) otomatis yang mampu melakukan analisis secara statis, dinamis dan malware. Setelah itu menyimpulkan hasil-hasil analisis untuk kemudian simpulan tersebut akan dijadikan laporan.



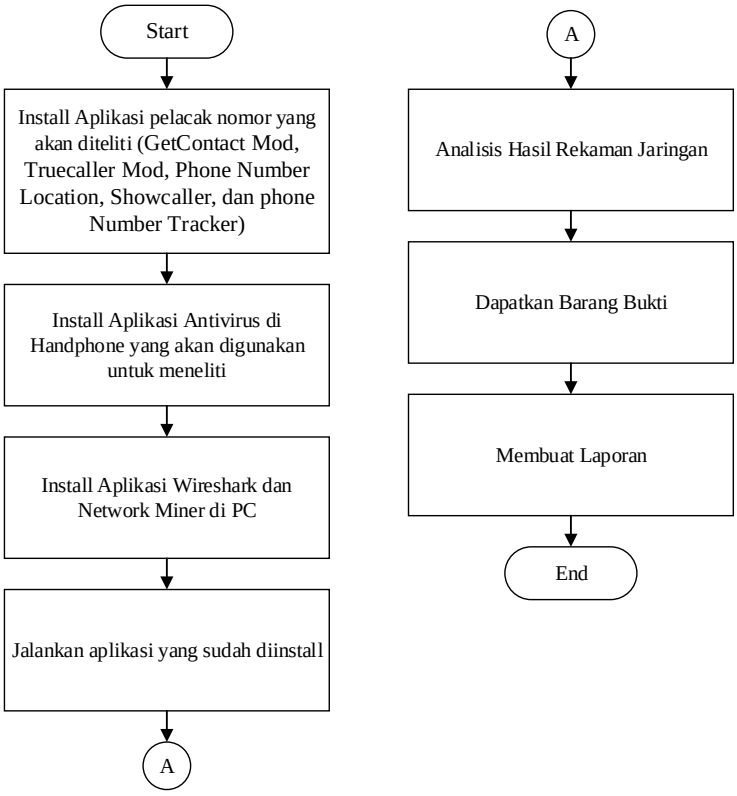
Gambar 3. Diagram Alir Digital Forensic Pendekatan Statis

2.3 Metode Pendekatan Dinamis

Metode Dinamis yang dilakukan pada penelitian dilakukan dengan melakukan pengamatan pada arus lalu lintas jaringan pada perangkat. Metode ini dilakukan menggunakan aplikasi Wireshark dan Network Miner. Kedua aplikasi tersebut merupakan aplikasi standar yang digunakan untuk network forensic maupun analisis jaringan [7], [8] [9] [10].

Berdasarkan gambar 4 Analisis Dinamis merupakan metode analisis aplikasi dengan menjalankan aplikasi. Keuntungan dari analisis ini yaitu aplikasi yang diuji diperiksa dan diaktifkan menggunakan mesin virtual untuk selanjutnya dapat dikumpulkan informasi dari analisis yang dilakukan. Metodologi penelitian dimulai dengan menginstall aplikasi chat yang akan di uji (GetContact Mod, Truecaller Mod, Phone Number Location, Showcaller, dan phone Number Tracker). Setelah itu dilanjutkan dengan menginstall Aplikasi Antivirus di Handphone Android yang akan digunakan untuk menguji.

Setelahnya install aplikasi Wireshark dan NetworkMiner di PC untuk memulai aktifitas digital forensic. Lalu jalankan aplikasi-aplikasi yang sudah di install untuk memulai perekaman jaringan di aplikasi pelacak nomor. Setelah selesai merekam jaringan, analisis hasil rekaman aplikasi pelacak nomor yang sudah dilakukan untuk mendapatkan barang bukti dari hasil rekaman. Selanjutnya buka hasil rekaman aplikasi pelacak nomor menggunakan Network Miner, dan carilah dokumen (files), gambar (images), pesan (Messages) yang bisa terdeteksi di aplikasi Network Miner. Simpulkan bukti-bukti yang di dapat untuk selanjutnya akan dijadikan bahan pembuatan laporan.



Gambar 4. Diagram Alir Digital Forensic Pendekatan Dinamis

III. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Pada tahap ini merupakan hasil penelitian untuk Analisis Digital Forensic Aplikasi Pelacak Nomor Handphone Android Pihak Ketiga Menggunakan Metode Statis dan Dinamis. Pada setiap aplikasi pelacak nomor handphone mempunyai hasil yang berbeda yang akan dikelompokkan menjadi dua bagian, yaitu Aplikasi yang normal (Normal Permissions) dan tidak aman (Dangerous Permissions). Dalam analisis digital Forensic ini menggunakan perangkat lunak Apk Analyzer dan NetworkMiner. Tahapan awal dalam analisis digital Forensic ini adalah dengan membuat tabel temuan menggunakan analisis statis dan dinamis. Kemudian membuat tabel level keamanan dari aplikasi aplikasi yang dianalisis. Berikut gambaran dari prose pengujian digital Forensic aplikasi pelacak nomor handphone.

Gambar 5. Proses Pengujian Digital Forensic.

3.2 Hasil Analisis

Setelah dilakukan tahap analisis Forensic dengan metode statis dan dinamis, maka dapat disimpulkan bahwa hanya aplikasi getcontact yang tidak ditemukan hak akses berbahaya, sedangkan keempat aplikasi lainnya terdapat hak akses berbahaya. Hasil analisis tersebut dapat dilihat pada Tabel 1.

Tabel 1. Hasil Temuan Pada Aplikasi Pelacak Nomor Handphone

No	Nama Aplikasi	Temuan Statis	Temuan Dinamis
1	Getcontact	Tidak ditemukan hak akses berbahaya	-
2	Truecaller	27 hak akses berstatus berbahaya	-
3	Phone Number Locator	8 hak akses berstatus berbahaya	-
4	ShowCaller	16 hak akses berstatus berbahaya	-
5	Phone Number Tracker	18 hak akses berstatus berbahaya	-

3.3 Tingkat Keamanan Aplikasi

Analisis risiko tingkat keamanan aplikasi pelacak nomor handphone ini pada akhirnya akan memberikan hasil identifikasi risiko, beserta rekomendasi kontrol keamanan yang terkait dengan upaya menurunkan risiko tersebut. Tahapan tersebut dinamakan rekomendasi kontrol. Tingkat keamanan ini dapat dibagi dengan beberapa tingkat (level) yaitu : Keamanan Level 0 merupakan keamanan fisik (physical security) atau keamanan tingkat awal. Apabila keamanan fisik terjaga maka keamanan di dalam smartphone juga akan terjaga. Keamanan Level 1 terdiri dari *database security*, *data security*, *dan device security*. Dari pembuatan *database* dapat dilihat apakah digunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan *data security* yaitu desain *database*, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah *device security* yaitu alat yang dipakai untuk keamanan dari *database* tersebut.

Keamanan level 2 merupakan keamanan dari segi keamanan jaringan. Keamanan ini merupakan tindak lanjut dari keamanan level 1. Keamanan level 3 merupakan *information security*. Informasi -informasi seperti kata sandi yang dikirimkan kepada teman atau file-file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut. Keamanan Level 4 adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi. (Mia A,2013).

Tabel 2. Tingkat Keamanan Aplikasi

No	Nama Aplikasi	Risiko	Level Keamanan	Rekomendasi
1	Getcontact	Statis - Tidak ditemukan temuan apapun Dinamis - Tidak ditemukan temuan apapun	Level 4	Aman, sangat Direkomendasikan
2	Truecaller	Statis Daftar hak akses berbahaya yang ditemukan adalah sebagai berikut: 1. Izin akses aplikasi access coarse location 2. Izin akses aplikasi. 3. Izin akses aplikasi answer phone calls 4. Izin akses aplikasi authenticate accounts 5. Izin akses aplikasi call phone 6. Izin akses aplikasi camera 7. Izin hak akses get accounts 8. Izin hak akses manage 9. Izin hak akses process outgoing calls 10. Izin hak akses aplikasi read call log. 11. Izin hak akses aplikasi read contacts. 12. Izin hak akses read external storage 13. Izin hak akses aplikasi read phone numbers 14. Izin hak akses aplikasi read phone state 15. Izin hak akses aplikasi read profile 16. Izin hak akses aplikasi read 17. Izin hak akses aplikasi receive mms 18. Izin hak akses aplikasi receive sms 19. Izin hak akses aplikasi record 20. Izin hak akses aplikasi send sms 21. Izin hak akses aplikasi system alert window 22. Izin hak akses aplikasi write 23. Dinamis - Tidak ditemukan temuan apapun	Level 1	Kurang Aman, Tidak Direkomendasikan
3	Phone Number Locator	Statis Daftar hak akses berbahaya yang ditemukan adalah sebagai berikut: 1. Izin akses aplikasi access coarse	Level 1	Kurang aman, Tidak Direkomendasikan

		location 2. Izin akses aplikasi access fine location 3. Izin akses aplikasi call 4. Izin hak akses aplikasi read call log 5. Izin hak akses aplikasi read contacts 6. Izin hak akses aplikasi read phone state 7. Izin hak akses aplikasi receive sms 8. Izin hak akses aplikasi send sms 9. Izin hak akses aplikasi system alert window 10. Dinamis - Tidak ditemukan temuan apapun		
4.	Showcaller	Statis Daftar hak akses berbahaya yang ditemukan adalah sebagai berikut: 1. Izin hak akses aplikasi answer phone calls 2. Izin hak kases aplikasi call phone 3. Izin akses aplikasi camera 4. Izin hak akses get accounts 5. Izin hak akses aplikasi process outgoing calls 6. Izin hak akses aplikasi read call 7. Izin hak akses aplikasi read contacts 8. Izin hak akses aplikasi read external storage 9. Izin hak akses aplikasi read phone numbers 10. Izin hak akses aplikasi read phone state 11. Izin hak akses aplikasi record audio 12. Izin hak akses aplikasi system alert window 13. Izin hak akses aplikasi write call log 14. Izin hak akses aplikasi write contacts 15. Izin hak akses aplikasi write external storage 16. Izin hak akses aplikasi write settings Dinamis Tidak ditemukan temuan apapun	Level 1	Tidak Direkomendasikan
5.	Phone Number Tracker	Statis Daftar hak akses berbahaya yang ditemukan adalah sebagai berikut: 1. Izin hak akses aplikasi access coarse location 2. Izin hak akses aplikasi access fine location 3. Izin hak akses aplikasi get 4. Izin hak akses aplikasi write contact 5. Izin hak akses aplikasi read contacts 6. Izin hak akses aplikasi read external	Level 1	Tidak Direkomendasikan

storage
7. Izin hak akses aplikasi read call log
8. Izin hak akses aplikasi use credentials
9. Izin hak akses aplikasi system alert window
10. Izin hak akses aplikasi write call log
11. Izin hak akses aplikasi write external storage
12. Izin hak akses aplikasi process outgoing calls
13. Izin hak akses aplikasi read sms
14. Izin hak akses aplikasi receive sms
15. Izin hak akses aplikasi get tasks
16. Izin hak akses aplikasi send sms
17. Izin hak akses aplikasi read phone state
18. Izin hak akses aplikasi call phone

Dinamis

Tidak ditemukan temuan apapun.

IV. KESIMPULAN

Kesimpulan yang didapatkan dari penelitian ini adalah Untuk mengetahui tingkat keamanan aplikasi pelacak nomor handphone Getcontact, Truecaller, Phone Number Locator, Showcaller, dan Phone Number Tracker dengan menggunakan metode statis dinamis. Framework yang digunakan memiliki 6 (enam) tahapan yaitu : Membuat latar belakang,rumusan masalah, tujuan, manfaat dan batasan masalah. Dari penelitian yang dilakukan didapatkan hasil dari tabel risk level menunjukkan bahwa aplikasi Getcontact memasuki level 4, yang artinya database security, data security dan device security sudah memiliki keamanan yang sesuai aplikasi pelacak nomor handphone pada umumnya. Sedangkan pada aplikasi pelacak nomor handphone Truecaller, Phone Number Locator, Showcaller dan Phone Number Tracker memasuki level 1, yang artinya database, data dan device security pada aplikasi tersebut belum memiliki keamanan yang sesuai aplikasi pelacak nomor handphone pada umumnya.

DAFTAR PUSTAKA

[1] I. Gunawan, *Keamanan Data: Teori dan Implementasi*, 1st ed. Sukabumi: Jejak, 2021.

[2] I. Gunawan and N. Krisdayanti, "Analisis Keamanan Aplikasi Chat Android Pihak Ketiga Atau Non Playstore Menggunakan Digital Forensics," *SIMETRIS*, vol. 16, no. 2, Art. no. 2, Dec. 2022, doi: 10.51901/simetris.v16i2.257.

[3] I. Gunawan and A. Ferriyan, "Analisis Malware Botnet Proteus Pendekatan Static dan Dinamic," *SIMETRIS*, vol. 15, no. 1, pp. 12–17, Jul. 2021, doi: 10.51901/simetris.v15i01.172.

[4] A. Kukuh, Yudatama and I. Gunawan, "Analisis Keamanan Aplikasi Dompet Digital Pendekatan Statis dan Dinamis," *Jurnal Simetris*, vol. 17, no. 1, pp. 18–22, Jun. 2023.

[5] I. Gunawan and D. E. Melania, "Security Analysis of Non Playstore Android Applications with Digital Forensic Methods Static and Dynamic Approaches | SIMETRIS", Accessed: Jun. 16, 2023. [Online]. Available: https://www.sttrcepu.ac.id/jurnal/index.php/simetris/article/view/225

[6] E. Gashi, "Permission-based Privacy Analysis for Android Applications," 2018. Accessed: Jun. 16, 2023. [Online]. Available: https://knowledgecenter.ubt-uni.net/etd/1/

[7] I. Gunawan, "Analisis Keamanan Wifi Menggunakan Wireshark," *JES (Jurnal Elektro Smart)*, vol. 1, no. 1, Art. no. 1, Aug. 2021.

[8] I. Gunawan, "Analisis Keamanan Data Pada Website Dengan Wireshark," *JES (Jurnal Elektro Smart)*, vol. 1, no. 1, Art. no. 1, Aug. 2021.

[9] C. D. Berliana, T. A. Saputra, and I. Gunawan, "Analisis Serangan dan Keamanan pada Denial of Service (DOS): Sebuah Review Sistematik," *JIIFKOM (Jurnal Ilmiah Informatika dan Komputer)*, vol. 1, no. 2, Art. no. 2, Jul. 2022.

[10] I. Gunawan, "Optimasi Model Artificial Neural Network untuk Klasifikasi Paket Jaringan," *SIMETRIS*, vol. 14, no. 2, Art. no. 2, Dec. 2020, doi: 10.51901/simetris.v14i2.135.