Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia p-ISSN 2086-5805
Akademi Angkatan Udara | Yogyakarta, 24-25 November 2021 e-ISSN 2808-2540
Volume 3, Tahun 2021, hlm. 213-222 DOI:10.54706/senastindo.v3.2021.128

Analisis Keamanan Informasi Kesadaran Pengguna *WhatsApp Mod* dengan Metode Analisis Statis dan Metode Kuantitatif

(Analysis of WhatsApp Mod User Awareness Information Security with Static Analysis Methods and Quantitative Methods)

Fahmy Trimuti Saputra[1], Banu Santoso[2*], Jeki Kuswanto[3], M. Abdul Ghofur[4]

[1,2,3] *Program Studi Teknik Komputer, Universitas Amikom Yogyakarta*
E-mail : fahmy.s@students.amikom.ac.id, banu@amikom.ac.id, jeki@amikom.ac.id
[4]*Prodi Teknik Aeronautika Pertahanan Akademi Angkatan Udara*
E-mail: m-abdulghofur@aau.ac.id

Abstract— ***Increasing technological developments make the use of technology in the world also increase and have a good or bad impact on the security of information that exists in cyberspace, this existing information security can be spread and accessed by irresponsible people by taking advantage of security gaps from every information media that exist in cyberspace, one of the gaps that allows for crimes to occur by utilizing unofficial applications where the application offers more attractive features so that users want to use the application. Applications that are widely used include the type of social chat network, where in this case the theme of WhatsApp mod users is raised, where the WhatsApp mod offers several features that do not exist in the official WhatsApp application on the Android platform. This can be one of the gaps where application development is not carried out officially, where data and information disseminated through the WhatsApp mod communication media cannot be guaranteed. Therefore, this research is expected to provide a percentage value related to the level of awareness of WhatsApp users which can be used as learning related to existing information security by paying attention to the results of static analysis related to security holes in the WhatsApp mod application.***

Keywords— **WhatsApp, WhatsApp Mod, Security, Information**

Abstrak**—** ***Perkembangan teknologi yang semakin meningkat membuat penggunaan teknologi di dunia juga semakin meningkat dan memberi dampak yang baik maupun buruk terhadap keamanan informasi yang ada pada dunia maya, keamanan informasi yang ada ini dapat tersebar dan diakses oleh orang yang tidak bertanggung jawab dengan memanfaatkan celah keamanan dari setiap media informasi yang ada pada dunia maya, Salah satu celah yang memungkinkan adanya tindak kejahatan dengan memanfaatkan aplikasi yang tidak resmi dimana pada aplikasi tersebut menawarkan fitur-fitur yang lebih menarik sehingga para pengguna mau untuk menggunakan aplikasi tersebut. Aplikasi yang marak digunakan adalah diantaranya jenis jejaring sosial chatting, dimana pada kasus ini diangkat tema tentang pengguna whatsapp mod, dimana pada whatsapp mod tersebut ditawarkan beberapa fitur yang tidak ada pada aplikasi whatsapp yang resmi ada pada platform android. Hal ini dapat menjadi salah satu celah yang mana pengembangan aplikasi tidak dilakukan secara resmi, dimana data dan informasi yang disebarkan melalui media komunikasi whatsapp mod tersebut tidak dapat dijamin keamanannya. Maka dari itu dengan adanya penelitian ini diharapkan dapat***

** Penulis Korespondensi (Banu Santoso)*
Email: banu@amikom.ac.id

p-ISSN 2086-5805
e-ISSN 2808-2540

memberikan nilai persentase terkait tingkat kewaspadaan pengguna whatsapp yang dapat dijadikan pembelajaran terkait keamanan informasi yang ada dengan memperhatikan hasil analisis statis terkait celah keamanan yang ada pada aplikasi whatsapp mod.

Kata Kunci— **WhatsApp, WhatsApp Mod, Keamanan, Informasi**

I. PENDAHULUAN

Pada saat ini, pengiriman pesan instan menunjukkan perkembangan yang sangat pesat, seiring berjalannya waktu pengiriman pesan instan menjadi sesuatu yang sangat dibutuhkan oleh pengguna internet di dunia, salah satu pengiriman pesan instan yang popular ialah Whatsapp yang lagi ramai digunakan pada zaman ini, Whatsapp berasal dari kata Bahasa inggris yaitu "What's Up?" yang memiliki arti dalam Bahasa Indonesia yaitu "Apa Kabar? atau Ada yang baru?" [1] karena fiturnya yang sangat mudah dipakai seperti chat grup, video call, pengiriman dari foto hingga file dan juga telepon yang tidak menggunakan pulsa sehingga menjadikannya sebagai perpesanan instan yang sangat popular di semua kalangan umur [2], Whatsapp memiliki dampak positif yaitu komunikasi tidak lagi terhalang oleh jarak, dibalik dampak positif Whatsapp juga memiliki dampak negatif ketika digunakan dengan cara yang salah, seperti tindakan kejahatan atau transaksi barang ilegal [3].

Whatsapp Mod ialah Whatsapp seperti pada umumnya tetapi yang menjadi pembeda daripada whatsapp pada umumnya ialah fiturnya, ada beberapa oknum yang memodifikasi ataupun menambahkan fitur yang tidak ada pada whatsapp resmi, Mod sendiri memiliki arti yaitu modifikasi [4] adanya modifikasi tersebut ada yang memanfaatkan aplikasi tersebut menyisipkan kode untuk mengambil data informasi pengguna dan juga membuat perangkat menjadi berat, oknum tersebut dapat mengeksploitasi perangkat untuk mendapatkan akses dan informasi pengguna untuk kepentingan pribadi dan merugikan pengguna yang memiliki informasi pribadi tersebut [5].

Dengan itu dapat dirumuskan permasalahan yang diteliti untuk mendapatkan nilai persentase dari tingkat kewaspadaan pengguna whatsapp Mod terhadap keamanan informasi yang ada pada smartphone mereka, dimana dengan melakukan instalasi aplikasi yang tidak resmi dapat menyebabkan kemungkinan terjadinya kebocoran data yang dapat merugikan pengguna whatsapp itu sendiri.

Tujuan dari penulisan ini adalah untuk mendapatkan nilai persentase dari penelitian tingkat kewaspadaan pengguna WhatsApp mod guna peningkatan pengetahuan terhadap ancaman kebocoran data melalui aplikasi-aplikasi modifikasi atau ilegal.

II. LANDASAN TEORI

Studi literatur dilakukan di tahap awal dalam penelitian ini yang mana mengumpulkan beberapa informasi ataupun data yang diambil dari buku maupun jurnal yang relevan untuk penelitian ini.

A. Metode Kuantitatif

Metode penelitian yang digunakan di dalam penelitian ini menggunakan penelitian dengan metode kuantitatif. Metode kuantitatif adalah salah satu jenis metode penelitian yang sistematis, terencana dan terstruktur jelas dari awal hingga akhir penelitian.

Metode kuantitatif adalah "metode yang berprinsip pada *filsafat positivisme*, yang digunakan untuk meneliti sebuah populasi atau sampel tertentu, pengumpulan data untuk meneliti juga menggunakan instrumen penelitian, analisis data bersifat *statistic/kuantitatif*, dengan tujuan untuk menguji hipotesis yang telah ditetapkan sebelumnya" [6].

Pendekatan kuantitatif ini digunakan peneliti untuk mengukur tingkat kewaspadaan masyarakat akan bahayanya penggunaan aplikasi modifikasi dan aplikasi ilegal *whatsapp mod* pada *smartphone* pribadi yang saat ini digunakan.

B. Metode Pengumpulan Data

Pengumpulan data merupakan suatu langkah utama dalam suatu penelitian, yang memiliki tujuan utama dari penelitian ialah mendapatkan data, dan jika peneliti tidak mampu mengetahui teknik pengumpulan data, maka peneliti tidak akan mendapatkan data optimal yang memenuhi standar data [7].

1. Kuesioner (Angket)

Angket atau kuesioner ialah salah satu teknik pengumpulan data yang dapat dilakukan dengan cara memberikan pertanyaan-pertanyaan kepada responden agar menjawab. Angket ini ialah teknik yang sangat efisien dan efektif apabila peneliti mengetahui variabel yang ingin diukur dan tau apa yang diinginkan responden [7].

2. Responden

Pada penelitian ini menggunakan responden dengan jumlah 50 orang, yang mana responden ini terdiri dari berbagai macam latar belakang pekerjaan, maupun pendidikan. Dasar pengambilan responden ini menggunakan metode *simple random sampling* sehingga responden yang didapatkan benar-benar murni dari golongan masyarakat awam. Selain itu responden yang didapatkan juga sudah memenuhi syarat untuk mengisikan kuesioner karena responden yang ada merupakan pengguna *whatsapp mod* yang memang dijadikan target utama dari pengambilan data yang ada. Di sini penulis menggunakan *simple random sampli*ng untuk metode pengambilan data.

3. Simple Random Sampling

Metode pemilihan responden yang dilakukan adalah dengan menggunakan metode simple random sampling dimana pengambilan anggota sampel dari populasi yang ada dilakukan secara acak tanpa memperhatikan strata sosial ataupun latar belakang responden yang ada (Sugiyono, 2018).

4. SPSS

SPSS adalah sebuah program pengolahan *statistic* yang paling banyak digunakan dalam penelitian yang menggunakan metode analisis data kuantitatif ataupun kualitatif yang dikuantitatifkan [8], SPSS singkatan dari *Statistical Package for the Social Science* yang di kembangkan oleh Perusahaan IBM, Keunggulan dari SPSS yaitu, Mudah digunakan karena ada visualisasi antarmuka, pengondisian data yang efisien, cepat dan handal, terintegrasi sumber terbuka dan keamanan data [9]. SPSS digunakan dalam berbagai riset pasar, pengendalian dan perbaikan mutu (*Quality Improvement*), dan juga riset sains. Karena kepopulerannya ini SPSS digunakan sebagai alat untuk pengolahan data (SPSS, 2017). SPSS dapat mengerti berbagai data dengan cara menginputkan data secara langsung kedalam Aplikasi SPSS Data Editor [10].

C. Analisis Statis

Merupakan salah satu dari dua metode analisis yang ada yaitu metode analisis statis dan metode analisis dinamis, metode analisis statis ini merupakan analisis yang file malware tersebut tidak aktif saat analisis, metode ini menelusuri dan meneliti terhadap kode sumber yang dituliskan pada program dengan dilakukannya pembedahan terhadap file tersebut,, sehingga didapatkan hasil analisis yang lengkap dan memberikan gambaran bagaimana kode tersebut berjalan [11], tool yang biasa digunakan untuk menganalisis statis adalah virus total dan *Mob*SF.

Keuntungan analisis statis ialah cepat dan dapat mencakup semua kemungkinan jalur eksekusi malware dan juga analisis statis lebih aman karena kode yang ada tidak dijalankan secara langsung [12]. Kekurangan analisis statis adalah sumber kode sulit masih banyak aplikasi yang tidak menyediakannya.

1. VirusTotal

p-ISSN 2086-5805
e-ISSN 2808-2540

Merupakan alat atau tool gratis yang dapat diakses online melalui desktop maupun mobile untuk menganalisis file dan *Uniform Resource Locator* (URL) yang mencurigakan, virus total bersifat terbuka dan menyediakan akses kepada siapapun untuk menggunakan sumber daya yang sudah disediakan, virus total juga menyediakan metadata yang kaya [13]. Virus Total menggunakan beberapa mesin antivirus untuk memberi fasilitas deteksi virus, worm dan trojan dan juga virustotal bisa digunakan untuk menganalisis situs web dan mendeteksi konten berbahaya yang ada pada situs web [14].

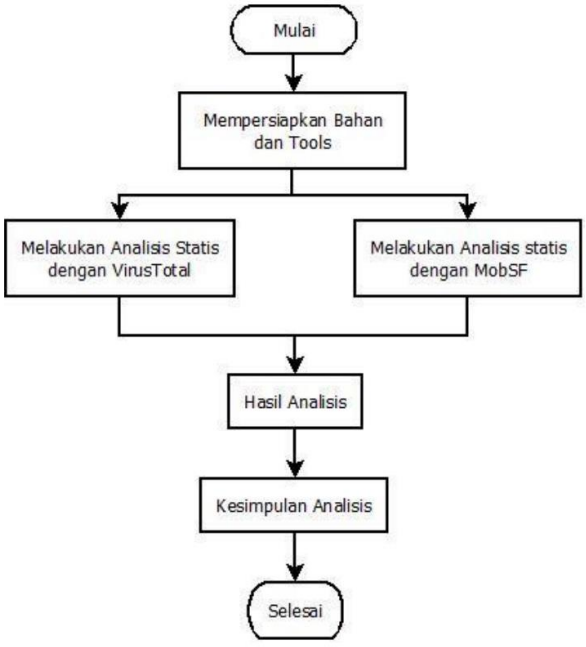
2. MobSF

MobSF ialah *Mobile Security Framework* yang merupakan framework yang digunakan untuk melakukan pengujian terhadap aplikasi seluler seperti, Android, iOS, maupun Windows, MobSF dapat melakukan analisis statis, dinamis dan menganalisis malware. MobSF digunakan analisis keamanan yang sangat efektif dan efisien.[5], MobSF juga mendukung binary dari aplikasi mobile seperti APK, XAPK, IPA dan APPX Bersama dengan format .zip. MobSF juga menyediakan REST API untuk integrasi yang mulus menggunakan pipeline CI/CD atau DevSecOps [15].

III. MODEL YANG DIUSULKAN

Metode Penelitian yang digunakan didalam penelitian ini menggunakan penelitian dengan metode kuantitatif. Metode kuantitatif ialah salah satu jenis metode penelitian yang sistematis, terencana dan terstruktur jelas dari awal hingga akhir penelitian. Metode Kuantitatif adalah "metode yang berprinsip pada *filsafat positivsme*, yang digunakan untuk meneliti sebuah populasi atau sampe tertentu, pengumpulan data untuk meneliti juga menggunakan instrument penelitian, Analisa data bersifat *statistic/kuantitatif*, dengan tujuan untuk menguji hipotesis yang telah ditetapkan sebelumnya" [6].

A. Alur Proses Analisis Statis

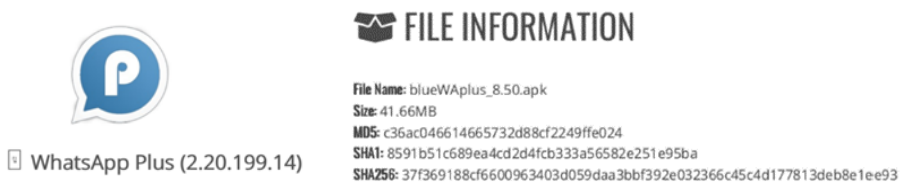


Gambar 1. Diagram alir PC dengan GPS

Pada Langkah awal pada alur analisis statis, ialah mempersiapkan tools analisis statis dan aplikasi Whatsapp Mod yaitu blueWhatsApp, GBWhatsApp, dan WhatsApp Aero. Pada Langkah selanjutnya ialah melakukan analisis statis pada VirusTotal dan MobSF untuk mendapatkan hasil dari analisis tersebut, setelah mendapatkan hasil analisis statis yang sudah dilakukan, digunakannya 2 tools yang berbeda dalam melakukan Analisa bertujuan untuk mendapatkan hasil yang lebih bervariasi, hasil yang ada akan berupa report yang dijadikan ringkasan sehingga dapat mudah dibaca dan dipahami.

IV. IMPLEMENTASI MODEL DAN PEMBAHASAN

A. Hasil Analisis Statis Menggunakan VirusTotal



Gambar 1. Informasi WhatsApp Plus

Pada WhatsApp Plus, saat dilakukan analisis statis dengan VirusTotal, VirusTotal mendeteksi 4 dari 46 mesin vendor antivirus adanya ancaman yang berada pada aplikasi tersebut dan juga pada aplikasi ini VirusTotal mendeteksi adanya relasi terindikasi Malware,pada tabel I daftar deteksi yang terdeteksi diawal hasil analisis.

TABEL I
HASIL ANALISIS WHATSAPP PLUS

Vendor	Deteksi	Keterangan
Avira	ANDROID/Dialer.FHJZ.Gen	virus yang mencoba membuat koneksi telepon dengan tarif tinggi secara signifikan.
Qihoo-360	Trojan.Android.Gen	aplikasi yang disisipkan ke dalam aplikasi
Tencent	A.Gray.VenomBanshee	keluarga dari virus A.Gray sebagai Adware
Trustlook	Android.PUA.DebugKey	aplikasi tersembunyi, yang tanpa sadar terunduh

Gambar 2. Informasi WhatsApp Aero

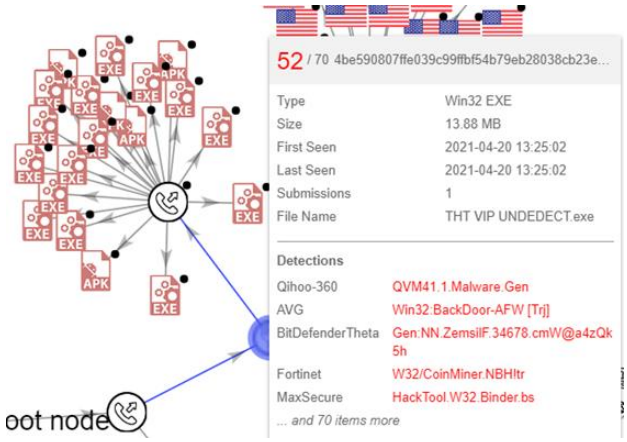
Pada WhatsApp Aero yang sudah dilakukan analisis statis dengan menggunakan bantuan tools virus total, Vendor mendeteksi 5 dari 46 mesin memberi tanda bahwa aplikasi ini mengandung malware, virus diaplikasi ini ada yang sama dengan virus pada aplikasi WhatsApp yang lain, dan dibawah ini daftar deteksi setelah di lakukan analisis dengan VirusTotal.

p-ISSN 2086-5805
e-ISSN 2808-2540

TABEL II
HASIL ANALISIS WHATSAPP AERO

Vendor	Deteksi	Keterangan
Avira	ANDROID/Dialer.FHJZ.Gen	virus yang mencoba membuat koneksi telepon dengan tarif tinggi secara signifikan.
Qihoo-360	Trojan.Android.Gen	aplikasi yang disisipkan ke dalam aplikasi
McAfee-GW-Edition	Artemis	Sebuah Trojan dan McAfee menyebutnya Artemis karena Sudah dikarantina dan diblok
K7GW	Trojan (0001140e1)	Trojan, nama lain dari Win32/ Occamy.CD3 Ransomware
CAT-QuickHeal	Android.Dialer.Adbd1	membuat koneksi telepon di latar belakang

Pada WhatsApp Aero ini setelah dilakukan scanning lebih dalam, didapatkan bahwa adanya banyak virus jahat yang berjalan di latar belakang aplikasi terlihat pada gambar 3. Terlihat bahwa di dalam aplikasi ada format .exe yang memiliki banyak kandungan virus.



Gambar 3. VirusTotal Graph WhatsApp Aero

Gambar 4. Informasi GBWhatsApp

Pada GBWhatsApp, pada hasil analisis menggunakan VirusTotal, didapatkan 2 ancaman yang ada pada aplikasi tersebut, yang dimana virus yang terdeteksi dapat mengambil informasi pribadi pengguna dan juga dapat menginfeksi perangkat sehingga dapat mengambil alih perangkat tersebut. Berikut virus yang ada pada aplikasi GBWhatsApp.

TABEL III
HASIL ANALISIS GBWHATSAPP

Vendor	Deteksi	Keterangan
Tencent	A.Gray.VenomBanshee	keluarga dari virus A.Gray sebagai Adware
Microsoft	Trojan: Win32/Wacatac.D!Ml	Trojan yang dapat mengontrol dan mendominasi perangkat yang terinfeksi

B. Hasil Analisis Statis Menggunakan MobSF

Analisis Lanjutan dengan menggunakan tools yang sudah diinstall pada sistem Kali Linux yaitu MobSF, tools MobSF dapat digunakan untuk menguji aplikasi-aplikasi mobile secara otomatis, dengan cara mengupload file yang sudah disiapkan untuk dianalisis dan menunggu, akan ada report yang muncul.

C. Hasil Analisis

1. Persentase Variabel A

Data yang didapatkan pada variabel A yang membahas pemahaman penggunaan aplikasi WhatsApp Mod, terlebih dahulu mencari nilai kriterium dari setiap variabel menggunakan rumus:

∑SK = Skor tertinggi tiap pertanyaan x jumlah item pertanyaan x jumlah responden yang ada.

∑SK = 5 x 2 x 50
∑SK = 500

Jadi nilai SK pada variabel A ialah 500, setelah didapatkan nilai tersebut dilakukan perhitungan untuk rekapitulasi skor jawaban pada variabel A

TABEL IV
SKOR JAWABAN VARIABEL A

	Pertanyaan		
	1	**2**	**Total**
Total	192	197	389
Persentase	49,4%	50,6%	100%

Berdasarkan angka pada hasil yang didapatkan pada pertanyaan di variabel A yang membahas pemahaman penggunaan WhatsApp Mod dilakukan perhitungan untuk mendapatkan nilai persentase dengan rumus:

$$\text{Persentase Variabel A} = \text{Total skor yang didapat SK} \times 100 = 389500 \times 100$$

$$= 77{,}8\%$$

Dari hasil perhitungan yang sudah dilakukan persentase pemahaman penggunaan WhatsApp Mod didapatkan sebesar 77,8%.

2. Persentase Variabel B

Data yang sudah didapatkan pada variabel B yang membahas pemahaman ancaman penggunaan aplikasi ilegal akan dilakukan perhitungan kriterium dengan rumus:

p-ISSN 2086-5805
e-ISSN 2808-2540

∑SK = Skor tertinggi tiap pertanyaan x jumlah item pertanyaan x jumlah responden yang ada.

∑SK = 5 x 3 x 50

∑SK = 750

Jadi nilai SK variabel B sebesar 750, setelah didapatkan nilai tersebut dilakukan perhitungan untuk rekapitulasi skor jawaban pada variabel B.

TABEL V
SKOR JAWABAN VARIABEL B

	Pertanyaan			
	1	**2**	**3**	**Total**
Total	200	151	197	548
Persentase	36,5%	27,5%	36%	100%

Berdasarkan angka pada hasil yang didapatkan pada pertanyaan di variabel B yang membahas Pemahaman ancaman penggunaan aplikasi ilegal dilakukan perhitungan untuk mendapatkan nilai persentase dengan rumus:

Persentase Variabel B= Total skor yang didapat SK x 100= 548750 x100

= 73,1%

Dari hasil hitung yang sudah dilakukan persentase tingkat pemahaman responden tentang pemahaman ancaman yang dihadapi Ketika menggunakan aplikasi ilegal sebesar 73,1%.

3. Persentase Variabel C

Pada variabel C ini membahas fitur apa saja sih yang banyak digunakan oleh pengguna WhatsApp Mod dan dapat dilakukan perhitungan untuk menentukan nilai dari ∑SK dan rumus yang digunakan sama seperti sebelumnya juga ialah:

∑SK = Skor tertinggi tiap pertanyaan x jumlah item pertanyaan x jumlah responden yang ada.

∑SK = 5 x 4 x 50

∑SK = 1000

Jadi nilai SK variabel C sebesar 1000, maka rekapitulasi dari variabel C pada tabel VI menyajikan hasil persentase atau perhitungan nilai setiap poin pertanyaan yang berada pada variabel C.

TABEL VI
SKOR JAWABAN VARIABEL C

	Pertanyaan				
	1	**2**	**3**	**4**	**Total**
Total	190	167	153	171	681
Persentase	27,9%	24,5%	22,5%	25,1%	100%

Berdasarkan angka pada hasil yang didapatkan pada pertanyaan di Variabel C yang membahas fitur yang ada pada aplikasi WhatsApp Mod, dapat dihitung dengan menggunakan rumus:

Persentase Variabel C= Total skor yang didapat SK x 100 = 6811000 x 100

=68,1%

Dari hasil perhitungan yang sudah dilakukan diatas, dan mendapatkan hasil bahwa penggunaan fitur-fitur yang ada pada WhatsApp mod sebesar 68,1%.

4. Persentase Variabel D

Pada variabel ini membahas tentang kesadaran pengguna dalam mengamankan smartphone yang digunakannya, dan juga akan dilakukan perhitungan terhadap ∑SK atau nilai kriterium variabel D, dengan rumus sama seperti poin sebelumnya ialah:

∑SK = Skor tertinggi tiap pertanyaan x jumlah item pertanyaan x jumlah responden yang ada.

∑SK = 5 x 3 x 50

∑SK = 750

Jadi SK pada variabel D sebesar 750, maka rekapitulasi dari variabel D pada tabel VII menyajikan hasil persentase atau perhitungan nilai setiap poin pertanyaan yang berada pada variabel D.

TABEL VII
SKOR JAWABAN VARIABEL D

	Pertanyaan			
	1	**2**	**3**	**Total**
Total	150	157	170	477
Persentase	31,4%	32,9%	35,7%	100%

Berdasarkan angka pada hasil yang didapatkan pada pertanyaan di Variabel D tentang kesadaran dalam mengamankan smartphone yang digunakan oleh pengguna, dapat dihitung nilai persentasenya dengan menggunakan rumus:

Persentase Variabel D= Total skor yang didapat SK x 100= 477750 x 100

=63,6%

Dari hasil perhitungan yang sudah dilakukan diatas tentang Kesadaran tentang Penggunaan Smartphone, mendapatkan hasil bahwa sebesar 63,6%.

V. KESIMPULAN

Pada variabel A dengan topik pembahasan tingkat pemahaman pengguna *WhatsApp Mod* tentang dasar penggunaan *WhatsApp Mod* mendapatkan persentase sebesar 77,8% yang menandakan bahwa pengguna *WhatsApp Mod* termasuk dalam kategori paham tentang risiko penggunaan *WhatsApp Mod* dalam kegiatan sehari-hari, Pada variabel B dengan topik pembahasan penggunaan aplikasi ilegal mendapatkan persentase sebesar 73,1% yang menandakan pengguna Aplikasi Ilegal termasuk *WhatsApp Mod* sadar akan bahayanya penggunaan aplikasi ilegal walaupun sudah mendapatkan edukasi, Pada variabel C dengan topik penggunaan fitur-fitur *WhatsApp Mod* mendapatkan 68,1% yang menandakan bahwa pengguna cukup dalam menggunakan fitur-fitur yang disediakan pada masing-masing *WhatsApp Mod*, dan Pada variabel D dengan topik Kesadaran pengguna terhadap Smartphone mendapatkan persentase sebesar 63,6% yang menandakan bahwa pengguna cukup sadar dalam mengamankan dan memperhatikan smartphone pribadinya.

Pada hasil Analisis menggunakan VirusTotal mendeteksi bahwa tiga *WhatsApp Mod* yang digunakan sebagai bahan pendukung penelitian ini terdapat setidaknya dua ancaman yang dapat

p-ISSN 2086-5805
e-ISSN 2808-2540

merugikan pengguna dan perangkat yang digunakan, Pada hasil Analisis menggunakan MobSF pada Tabel Perijinan ketiga aplikasi banyak mendapatkan status Berbahaya atau Dangerous pada perijinan yang ada pada aplikasi sedangkan pada tabel analisis kode didapatkan hasil isu yang menjadi kerentanan aplikasi *WhatsApp Mod* tersebut tidak sesuai dengan Standar yang ada.

UCAPAN TERIMA KASIH

Ucapan terima kasih atas terbitnya naskah ini pada Seminar Nasional Sains Teknologi dan Inovasi Indonesia 2021 sebagai bagian kolaborasi/kerjasama penelitian antara Universitas Amikom Yogyakarta dengan Akademi Angkatan Udara.

REFERENSI

[1] C. Barhoumi, "The Effectiveness of WhatsApp Mobile Learning Activities Guided by Activty Theory on Students' Knowldege Management," *Contemp. Educ. Technol.*, vol. 6, no. 3, pp. 221–238, 2020, doi: 10.30935/cedtech/6151.
[2] G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," vol. 2, no. 1, pp. 102–105, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.
[3] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.
[4] "WhatsApp MOD | Journal of the International Child Neurology Association." https://jicna.org/index.php/journal/whatsapp-mod (accessed Jan. 06, 2021).
[5] C. Hanifurohman and D. D. Hutagalung, "Analisis Statis Menggunakan Mobile Security Framework Untuk Pengujian Keamanan Aplikasi Mobile E-Commerce Berbasis Android," *Sebatik*, vol. 24, no. 1, pp. 22–28, 2020, doi: 10.46984/sebatik.v24i1.920.
[6] Sugiyono, "Metode Penelitian Manajemen. ALFABETA. Bandung," *ALFABETA*, 2014.
[7] Sugiyono, "Prof. Dr. Sugiyono. 2018. Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.," *Prof. Dr. Sugiyono. 2018. Metod. Penelit. Kuantitatif, Kualitatif, dan R&D. Bandung Alf.*, 2018.
[8] D. N. J. Arum and Anie, *S t a t i s t i k d e s k r i p t i f & r e g r e s i l i n i e r b e r g a n d a d e n g a n s p s s.* 2012.
[9] IBM, "Statistik SPSS - Gambaran Umum | IBM." https://www.ibm.com/products/spss-statistics (accessed Jan. 08, 2021).
[10] S. Zein, L. Yasyifa, R. Ghozi, E. Harahap, F. Badruzzaman, and D. Darmawan, "Pengolahan dan Analisis Data Kuantitatif Menggunakan Aplikasi SPSS," *J. Teknol. Pendidik. dan Pembelajaran*, vol. 4, no. 1, pp. 1–7, 2019.
[11] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *Justindo, J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037.
[12] R. Adenansi and L. A. Novarina, "Malware dynamic," *J. Educ. Inf. Commun. Technol.*, vol. 1, no. 1, pp. 37–43, 2017.
[13] L. Song, H. Huang, W. Zhou, W. Wu, and Y. Zhang, "Learning from big malwares," *Proc. 7th ACM SIGOPS Asia-Pacific Work. Syst. APSys 2016*, 2016, doi: 10.1145/2967360.2967367.
[14] R. Masri and M. Aldwairi, "Automated malicious advertisement detection using VirusTotal, URLVoid, and TrendMicro," *2017 8th Int. Conf. Inf. Commun. Syst. ICICS 2017*, pp. 336–341, 2017, doi: 10.1109/IACS.2017.7921994.
[15] Abraham A., "GitHub - MobSF / Mobile-Security-Framework-MobSF: Mobile Security Framework (MobSF) adalah aplikasi seluler otomatis all-in-one (Android / iOS / Windows) pengujian pena, analisis malware, dan kerangka kerja penilaian keamanan yang mampu melakukan statis dan analisis dinamis." https://github.com/MobSF/Mobile-Security-Framework-MobSF (accessed Jan. 22, 2021).