Analisis *Malware* Aquvaprn.exe untuk Investigasi Sistem Operasi dengan Metode *Memory Forensics*

http://dx.doi.org/10.28932/jutisi.v10i2.6562

Riwayat Artikel
Received: 25 Mei 2024 | *Final Revision*: 6 Agustus 2024 | *Accepted*: 6 Agustus 2024

Hafish Naufal Aditya [#1], Nur Widiyasono[#2], Alam Rahmatulloh[✉#3]

[#] *Program Studi Informatika, Universitas Siliwangi*
Jl. Siliwangi No. 24, Tasikmalaya, Jawa Barat, 46115 Indonesia
[1]spaz.devil15@gmail.com
[2]nur.widiyasono@unsil.ac.id
[3]alam@unsil.ac.id
✉Corresponding author: *alam@unsil.ac.id*

Abstrak — **Di era serba digital saat ini, data menjadi sebuah aset yang sangat berharga. Berbagai macam teknik digunakan untuk mencuri data pribadi yang berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab. Objek yang digunakan pada penelitian ini adalah *AQUVAPRN.exe* yang memiliki jenis *malware* RAT (*Remote Access Trojan*) yang saat *malware* ini berjalan pembuat *malware* tersebut dapat mengambil data pribadi pengguna yang sistem operasinya terinfeksi. Cara kerja dari *malware* AQUVAPRN.exe dengan berjalan pada latar belakang saat aplikasi dijalankan atau dieksekusi lalu membuat beberapa proses seperti mengubah *file registry*, membuat *file*, membaca *file*, dan melakukan koneksi internet dengan *IP Address* tertentu secara terus menerus tanpa diketahui oleh pengguna dari komputer itu sendiri. Hasil yang diperoleh terhadap *malware AQUVAPRN.exe* berupa alamat *IP Address* 109.51.76.80, memiliki domain Kota Lisbon Negara Portugal, memiliki nilai *hash* MD5 55c2c12970cda52f58bfad7b8c7d37d5. Diketahui pula, *malware AQUVAPRN.exe* menggunakan teknik *anti reverse engineering* tepatnya *obfuscation* yang menghambat atau menghalangi *malware* untuk dibedah atau di *reverse engineering* agar mengetahui *code* penyusun dari *malware*. Didapatkan pula PID *(Process ID)* dari proses *AQUVAPRN.exe* adalah 8332 dengan alat virtual (*Virtual Address*) 0x8e0f57042080.**

Kata kunci— **Data;*IP Address*; *Malware*; *Obfuscation*; RAT**

Analysis of Aquvaprn.exe Malware for Operating System Investigation using Memory Forensics Method

Abstract — ***In today's digital age, data has become a valuable asset. Various techniques are used to steal personal data that could potentially be misused by irresponsible parties. The object used in this study is AQUVAPRN.exe, which is a type of malware known as a Remote Access Trojan (RAT). When this malware runs, the creator of the malware can access personal data from the infected operating system without the user's knowledge. AQUVAPRN.exe works in the background when an application is executed, creating several processes such as modifying the registry, creating files, reading files, and making continuous internet connections to a specific IP address without the user's knowledge. The result obtained from the AQUVAPRN.exe malware is an IP address of 109.51.76.80, with the domain located in Lisbon, Portugal, and has an MD5 hash value of 55c2c12970cda52f58bfad7b8c7d37d5. It is also known that the AQUVAPRN.exe malware uses an anti-reverse engineering technique, specifically obfuscation, which obstructs or hinders the malware from being analyzed or reverse-engineered to determine the code used to create the malware. The PID (Process ID) of the AQUVAPRN.EXE process is 8332 with a virtual tool (Virtual Address) of 0x8e0f57042080.***

Keywords— ***Data; IP Address; Malware; Obfuscation; RAT***

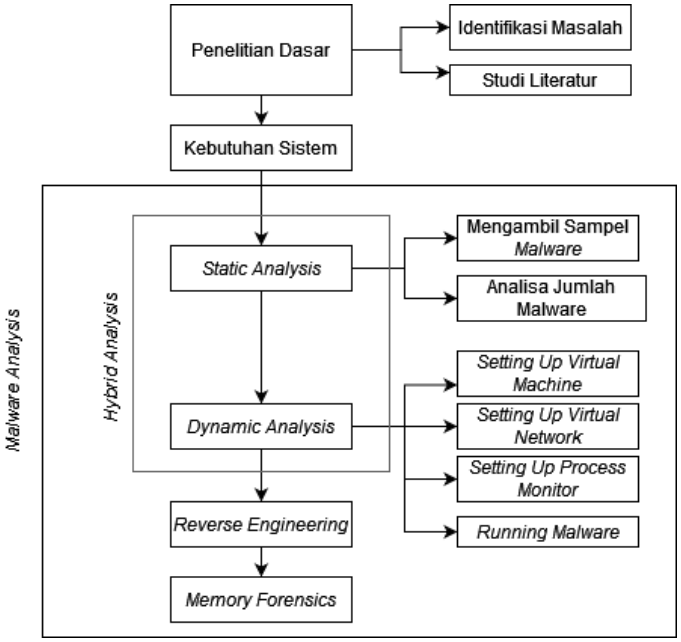
I. PENDAHULUAN

Era digital yang semakin maju, data telah menjadi aset yang sangat berharga. Sayangnya, kejahatan siber semakin marak dan membuat data pribadi dan instansi pemerintahan rentan dicuri [1]. *Malware* menjadi salah satu teknik yang sering digunakan untuk mencuri data, karena sulit dideteksi oleh pengguna. Bentuk *malware* sangat beragam, dan dapat berupa aplikasi yang umum digunakan, seperti aplikasi berekstensi (*.exe*) di sistem operasi *Windows* 10 [2]. *Malware* tidak hanya berpotensi mencuri data pribadi pengguna, tetapi juga dapat mengganggu jalannya sistem operasi dengan berjalan di latar belakang sistem. Hal ini dapat menurunkan kinerja komputer, malfungsi sistem operasi, dan bahkan mengunci komputer sehingga tidak dapat digunakan oleh pengguna [3].

Salah satu jenis *malware* yang berbahaya adalah *Remote Access Trojan* (RAT), yang memberikan hak akses kepada pengguna *malware* yang berpotensi mengambil data pribadi korban termasuk membobol *web* dan kata sandi [4]. *Malware* juga dapat disisipkan pada file dengan ekstensi *.exe* yang diunduh oleh pengguna *Personal Computer* (PC), atau melalui *e-mail* yang memiliki lampiran atau link yang tidak diketahui asal-usulnya [5]. Melalui analisis *malware* menggunakan *Memory Forensics*, penelitian dapat dilakukan untuk mengetahui cara kerja *malware* dalam menginfeksi pengguna melalui file yang disisipkan pada sebuah surat elektronik atau *file* yang diunduh dari internet [6]. Penelitian ini dapat memberikan pemahaman yang lebih dalam tentang cara kerja *malware* dan membantu pengguna untuk menghindari serangan *malware*. Studi kasus yang dilakukan pada penelitian ini menggunakan *AQUVAPRN.exe* sebagai objek penelitian. Melalui penelitian ini, dapat diketahui cara kerja dari *malware AQUVAPRN.exe* dalam menginfeksi sistem operasi dan berpotensi mengambil data pribadi pengguna. Penelitian ini juga dapat menjadi acuan bagi pengguna untuk mengetahui celah yang digunakan *malware* dalam menginfeksi sistem operasi sehingga dapat meminimalisir serangan *malware* [7]. Edukasi dan pemahaman tentang cara kerja *malware* sangat penting agar pengguna dapat terhindar dari serangan *malware* yang berbahaya [8].

II. METODE PENELITIAN

Proses metodologi penelitian dilakukan berkesinambungan agar dapat melihat tahapan dari sebuah penelitian [9]. Gambar 1 merupakan tahapan-tahapan penelitian yang dilakukan pada penelitian ini.



Gambar 1. Tahapan Penelitian

A. Penelitian Dasar

Penelitian dasar merupakan tahap pertama dalam melaksanakan sebuah penelitian. Ada 2 (dua) cara dalam melakukan tahap awal dalam sebuah penelitian, yaitu:

1) Identifikasi masalah: Malware yang digunakan memiliki jenis RAT (Remote Access Trojan) yang dapat mengambil, mengubah, atau menghapus data pribadi pada komputer yang terinfeksi.

2) Studi literatur: Setelah melakukan identifikasi masalah, pada tahap ini melakukan pencarian referensi terkait informasi cara kerja malware dan metode yang digunakan pada penelitian ini.

B. Kebutuhan Sistem

Memahami sebuah masalah pada sistem, perlu dilakukan proses pembagian sistem menjadi beberapa bagian dengan tujuan untuk mengidentifikasi kebutuhan sistem. Sistem yang telah berjalan akan dianalisis untuk mencari kekurangan yang perlu diperbaiki. Proses mencari kebutuhan sistem bertujuan untuk memecahkan masalah dan menentukan langkah-langkah perbaikan yang perlu dilakukan[10].

C. Malware Analysis

Tahapan ini merupakan implementasi dari tahap penelitian dasar terkait metode penelitian yang digunakan pada penelitian malware. Ada 8 (enam) alur dalam tahap ini, yaitu[11]:

1) Mengambil Sample Malware: Malware yang digunakan diambil dari website https://any.run/ [12].

2) Analisa Jumlah Hash Malware: Malware akan diidentifikasi dengan tools HashCalc untuk mendapatkan informasi terkait nilai MD5 (Message-Digest Algorithm 5) [13].

3) Setting Up Virtual Machine: Ruang lingkup yang digunakan adalah virtual karena dinilai lebih aman dalam melakukan pengujian sample malware yang diteliti [14].

4) Setting Up Virtual Network: Tahap ini menggunakan tools ApateDNS [15].

5) Starting Process Explorer: Tahap ini memiliki tujuan untuk menampilkan informasi proses yang berjalan pada latar belakang sistem operasi. Tools yang digunakan adalah Process Monitor versi 3.89 [16].

6) Running Malware: Pengujian ini dilaksanakan menggunakan ruang virtual untuk mencegah malware menginfeksi komputer fisik [17].

7) Reverse Engineering: Tahapan ini menggunakan tools IDA Pro dalam melakukan proses disassembler pada malware AQUVAPRN.exe [18].

8) Memory Forensics: Alur analisis ini menggunakan tools volatility [19].

III. HASIL DAN PEMBAHASAN

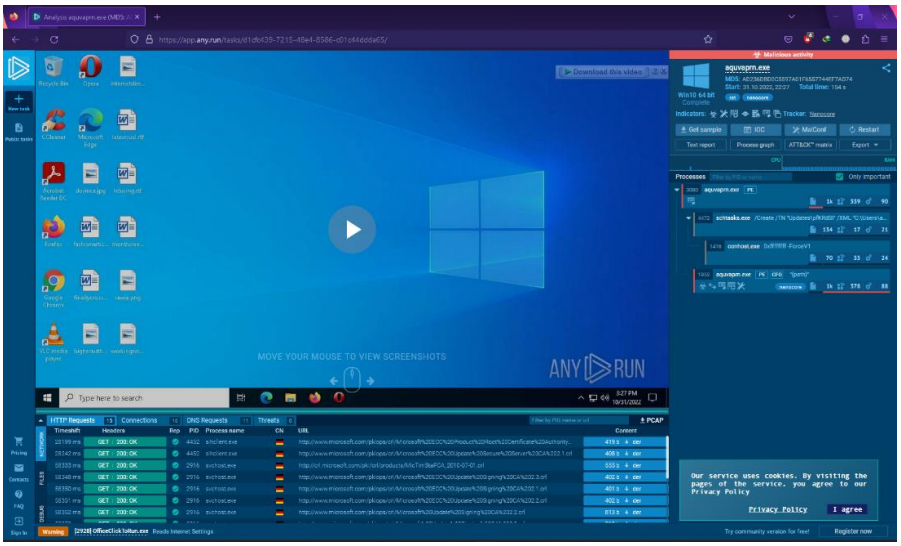
A. Penelitian Dasar

Penelitian dasar terbagi menjadi 2 tahapan, yaitu identifikasi masalah yang terjadi, dan studi literatur dari topik masalah yang dibahas dalam penelitian ini[20].

1) Identifikasi masalah

Malware pada penelitian ini didapat pada *website* https://any.run/ yang didapatkan beberapa informasi terkait malware *AQUVAPRN.exe* yang dapat dilihat pada gambar 2.

p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 2. Tampilan *Website* Any.run

Seperti yang ditampilkan pada *website any.run* terdapat informasi terkait *malware AQUVAPRN.exe* yang disitu juga menampilkan bagaimana *malware* ini bekerja pada sebuah sistem operasi yang diinfeksinya.

2) Studi literatur

Fokus penelitian ini, meliputi jenis *malware* yang digunakan berjenis *RAT* (*Remote Access Trojan*)[21], menggunakan *Hybrid Analysis* sebagai metode penelitian, dan *tools* (*IDA Pro, Volatility, DumpIt, ApateDNS, HashCalc, Process Monitor, hingga VMWare*).

B. Kebutuhan Sistem

Analisa kebutuhan sistem terbagi menjadi 2 (dua) proses, yaitu:

1) Hardware Requirement

Spesifikasi *hardware* yang digunakan dalam pengujian *malware AQUVAPRN.exe* dapat dilihat pada tabel 1.

TABEL 1
HARDWARE REQUIREMENT

Processor	**Intel Core i5-8300H CPU @ 2.2GHz**
RAM	16 GB DDR4
Storage	SSD 128 GB, HDD 1 TB

2) Software Requirement

Spesifikasi *hardware* yang digunakan dalam pengujian *malware AQUVAPRN.exe* dapat dilihat pada tabel 2.

TABEL 2
SOFTWARE REQUIREMENT

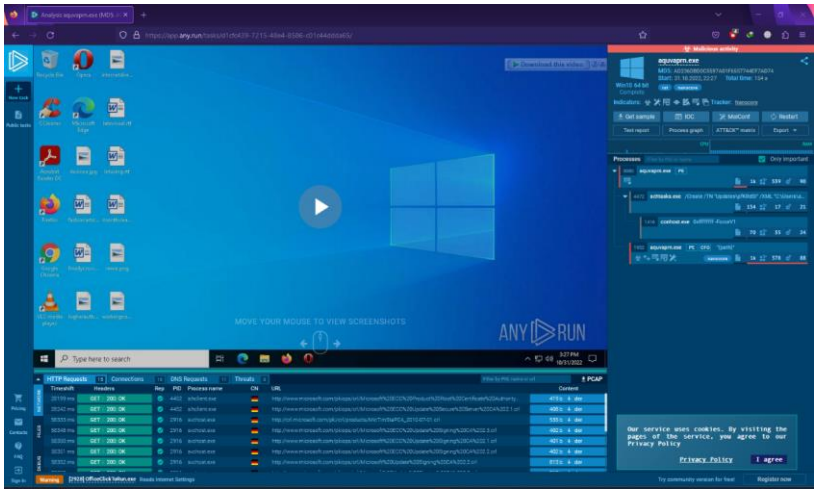
Jenis	**Spesifikasi**
Sistem Operasi	*Windows* 11 Home 22H2 22621.674
Virtual Machine	*VMWare Workstation Pro Ver*. 16.2.4 build-20089737
Sistem Operasi (*Virtual Machine*)	*Windows* 10 Home 2004 Build 19041.264
Reverse Engineering Software	*IDA Pro* v7.5 SP3
Memory Forensics Software	*Process Monitor* v3.92, *Volatility* 3.2.4, *DumpIt*
Virtual Network Software	*ApateDNS* v1.0
Hashing Software	*HashCalc* v2.02

C. Malware Analysis

Malware Analysis dilakukan dengan beberapa tahapan yang dilakukan antara lain :

1) Mengambil Sampel Malware

Langkah awal yang dilakukan adalah mengambil sampel *malware AQUVAPRN.exe* pada *website any.run*[22] yang dapat dilihat pada gambar 3.

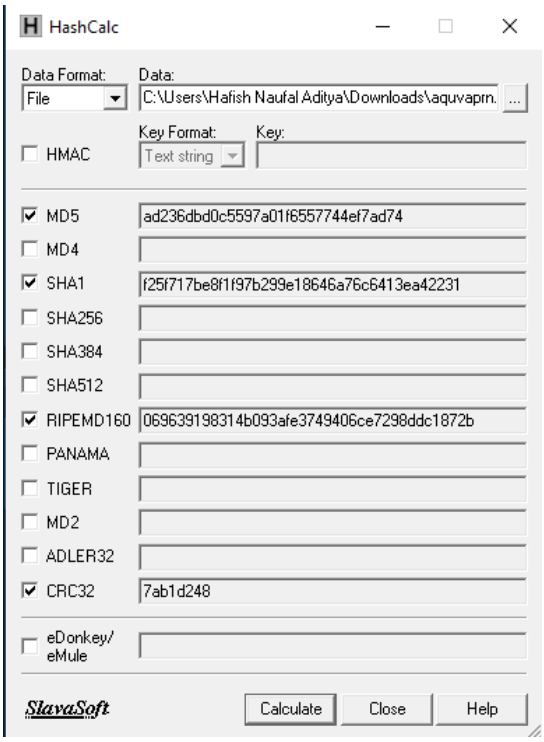


Gambar 3. *Sample Malware AQUVAPRN.exe* pada *Website* Any.run

Website tersebut dapat mengklik pada bagian *get sample* untuk mendapatkan sampel *malware* yang akan otomatis terunduh dalam bentuk berkas berekstensi *.rar* yang berisi berkas yang terinfeksi oleh *malware* tersebut.

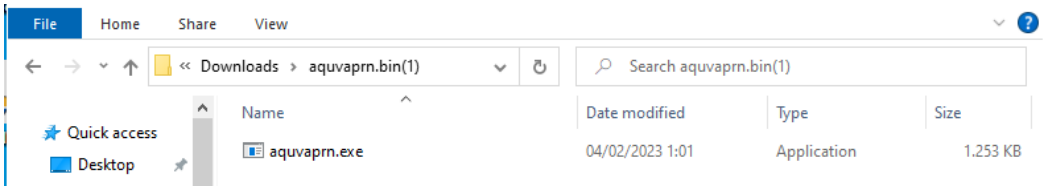
2) Analisa Jumlah Hash

Memeriksa *hash* dari berkas *malware* yang telah diunduh dari *website any.run* untuk memastikan bahwa berkas yang diunduh tidak mengalami perubahan dan masih sama seperti pada *website* [19]. Hal ini dapat dilihat pada gambar 4.



Gambar 4. MD5 *File Malware AQUVAPRN.EXE*

Gambar 4 didapatkan bahwa *file* yang terinfeksi *malware* memiliki nilai *MD5* (*Message-Digest Algorithm* 5) `55c2c12970cda52f58bfad7b8c7d37d5`. Nilai tersebut bertujuan untuk memastikan *file* tersebut merupakan *file* yang sama dan tidak ada perubahan didalamnya[23]. Ukuran dan jenis *file* yang terinfeksi dapat dilihat pada Gambar 5.



Gambar 5. Sampel File Terinfeksi *Malware AQUVAPRN.exe*

Hasil pemeriksaan diatas didapat informasi terkait *file* yang terinfeksi *malware AQUVAPRN.exe* yang dapat dilihat pada tabel 3.

TABEL 3
INFORMASI FILE TERINFEKSI *MALWARE* AQUVAPRN.EXE

Nama *File*	***AQUVAPRN.exe***
MD5	`ad236dbd0c5597a01f6557744ef7ad74`
Ukuran *File*	1.253 KB
Tipe *File*	EXE

3) Setting Up Virtual Machine

Virtual Machine digunakan sebagai lab penelitian dalam penelitian ini[24]. *Virtual Machine* ini menggunakan sistem operasi *Windows* 10 yang memiliki fungsi sama seperti layaknya komputer fisik dengan konfigurasi yang dapat dilihat pada tabel 4.

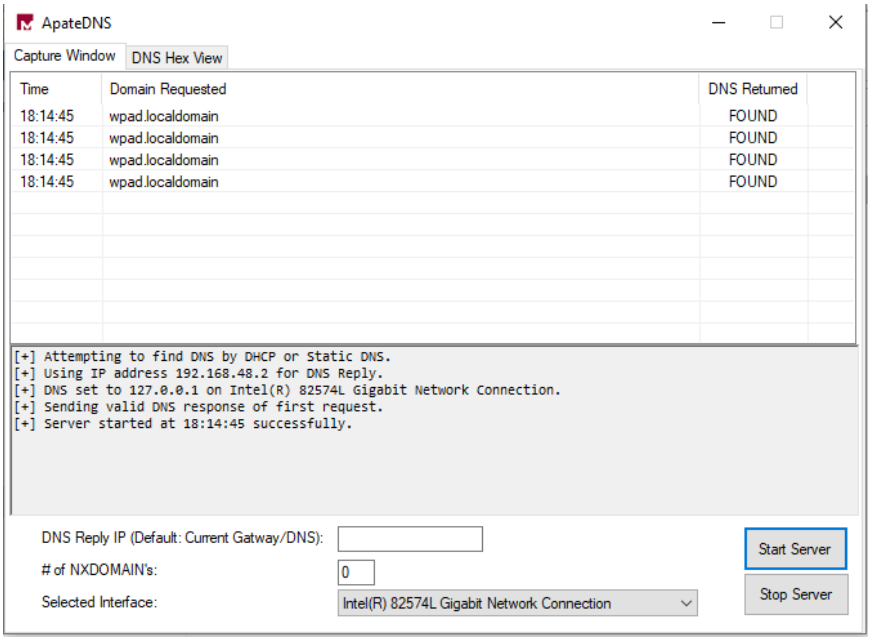
TABEL 4
VIRTUAL MACHINE CONFIGURATION

Processor	**2 *Core***
Memory	4 GB
Storage	60 GB
Network Adapter	*NAT*

Virtual Machine ini menjadi wadah dalam melakukan penelitian ini dikarenakan memiliki resiko yang relatif lebih kecil dibandingkan dengan menggunakan komputer fisik yang dapat diinfeksi sistem operasinya oleh *malware AQUVAPRN.exe*.

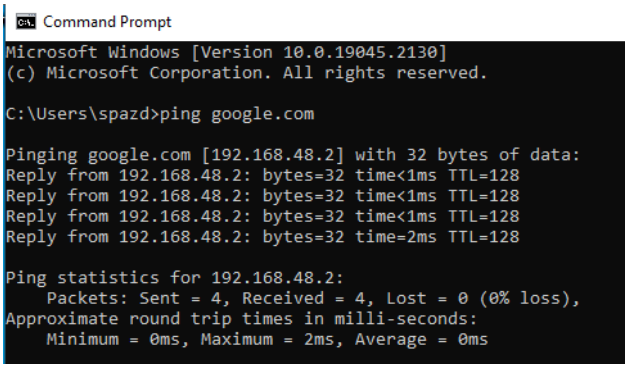
4) Setting Up Virtual Network

Tahapan ini dilakukan untuk membuat jaringan *virtual* yang dideteksi oleh *malware* ketika berjalan di latar belakang sistem operasi yang sebenarnya mengunci atau mengisolasi jaringan[25]. *Software* ini ketika diklik pada tombol *Start Server* maka *software* akan langsung berjalan dan membuat *virtual server* dan mengubah *IP Address localhost* menjadi 127.0.0.1 dapat dilihat pada gambar 6.



Gambar 6. *Software ApateDNS* Berjalan

ApateDNS berjalan untuk memeriksa *software* tersebut sudah berjalan menggunakan *CMD* (*Command Prompt*) dengan melakukan ping seperti pada gambar 7.

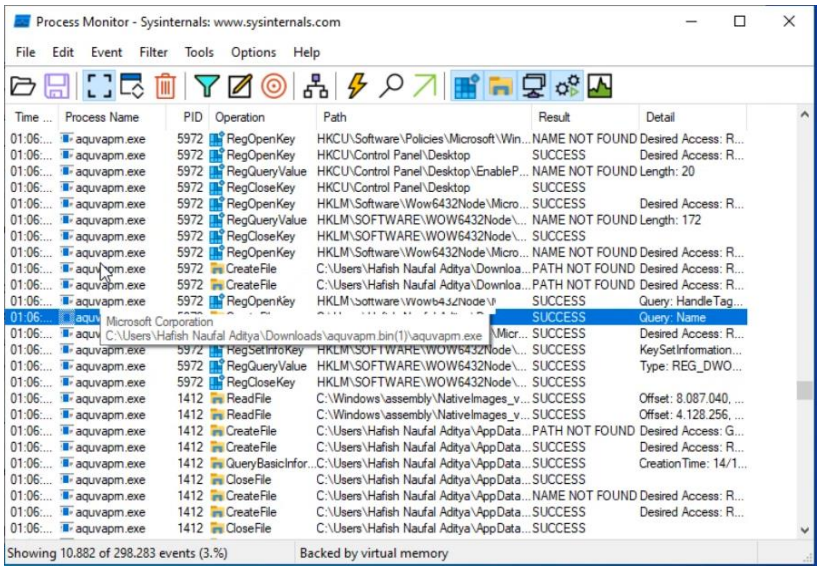


Gambar 7. *Ping* pada CMD

Hasil pengujian pada gambar 7 menunjukkan bahwa saat melakukan *ping* ke *domain google.com ApateDNS*[26] melakukan *reply* dengan *IP* 192.168.48.2 yang menunjukkan seakan perangkat *virtual machine* terkoneksi dengan internet.

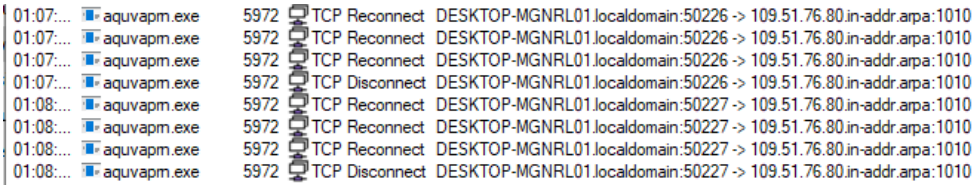
5) Starting Process Explorer

Tahapan ini menggunakan *software Process Monitor* yang memiliki fungsi untuk melihat semua kegiatan atau proses yang berjalan pada latar belakang sistem operasi[27]. *Software* ini juga terdapat fungsi *filter* yang berfungsi untuk menampilkan proses yang ingin dilihat saja. Bertujuan untuk melihat proses yang dilakukan oleh *malware AQUVAPRN.exe* yang berjalan saat *file* yang terinfeksi dibuka dapat dilihat pada gambar 8.



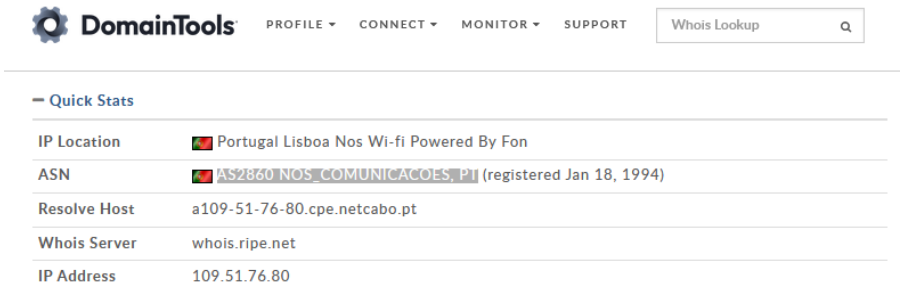
Gambar 8. Tampilan *Malware AQUVAPRN.EXE* pada *Process Monitor*

Hasil pengujian pada *tools Process Monitor* didapatkan juga hasil bahwa *malware* melakukan koneksi internet terhadap *IP Address* 109.51.76.80 yang dalam proses berjalannya *malware* dalam mendapatkan informasi pada sistem operasi yang diinfeksi disinkronkan dengan *IP* tersebut[28]. Hal ini dapat dilihat pada gambar 9.



Gambar 9. *Process Monitor Network AQUVAPRN.EXE*

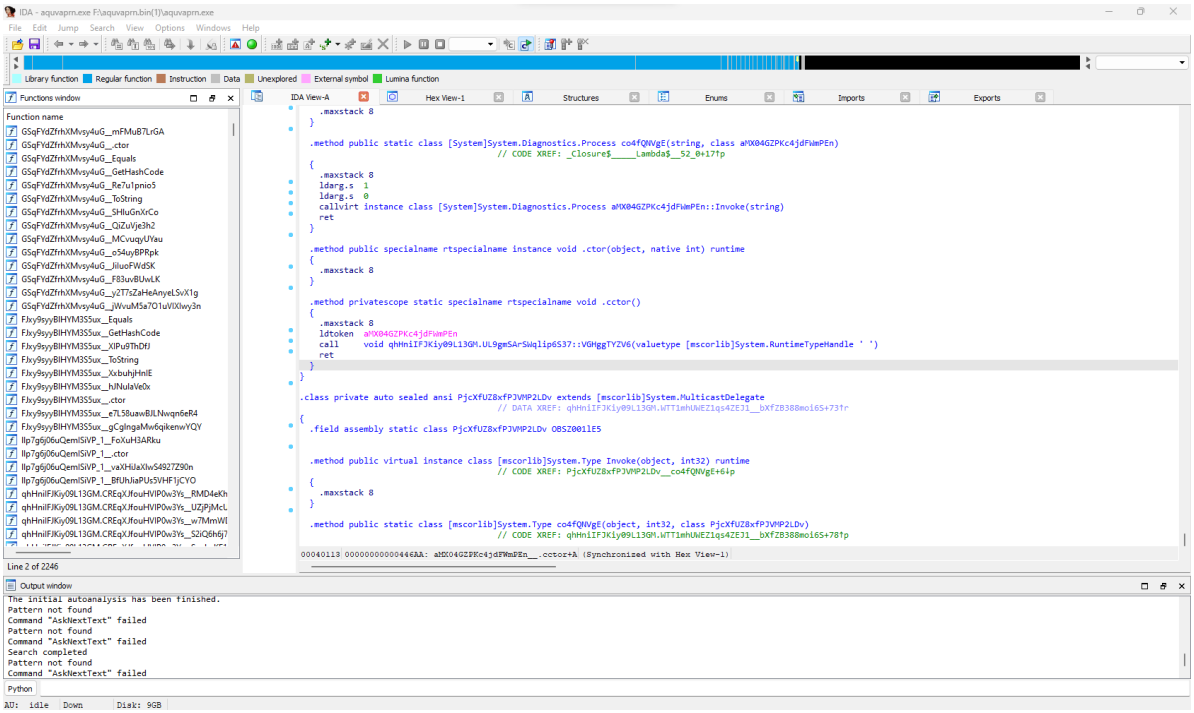
Hasil *IP address* yang didapatkan dari *Process Monitor* selanjutnya lacak menggunakan *tools Domaintools.com* yang menampilkan informasi *IP Address* 109.51.76.80 memiliki nama terdaftar `AS2860 NOS_COMUNICACOES, PT` , asal Negara Portugal dengan alamat Kota Lisboa atau Lisbon yang dapat dilihat pada gambar 10.



Gambar 10. Hasil Lacak *DomainTools.com IP Address 109.51.76.80*

6) Reverse Engineering

Gambar 11 merupakan proses *tools IDA Pro* untuk mengetahui *command* pada *malware AQUVAPRN.exe* yang berjalan di sistem operasi yang terinfeksi[29].

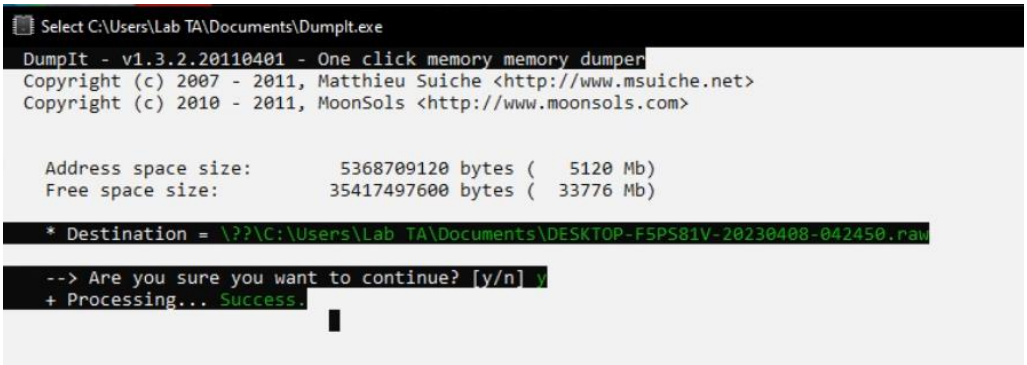


Gambar 11. Tampilan *Malware AQUVAPRN.exe* pada *IDA Pro*

Berdasarkan hasil yang dilihat dari *tools IDA Pro*, diperoleh hasil bahwa *malware AQUVAPRN.exe* menggunakan fitur *anti reverse engineering*[25] yaitu teknik yang bertujuan untuk menghambat atau mempersulit upaya *reverse engineering* baik untuk penyalinan atau penggunaan program tersebut oleh pihak yang tidak berwenang. Teknik yang digunakan pada *anti reverse engineering* ini dengan *obfuscation*, yaitu teknik mengacak atau menyembunyikan kode sumber program yang hendak di *reverse engineering* dapat dilihat dengan tidak ditemukannya *command* pada hasil dalam *tools* ini[30].

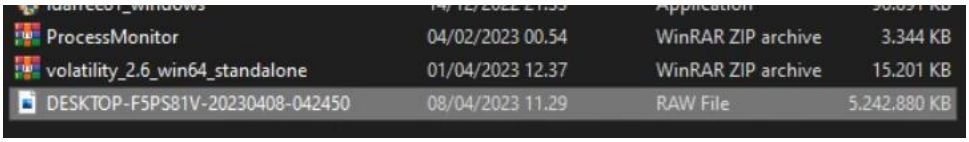
7) Memory Forensics

Tahapan ini menggunakan tools *DumpIt* dan juga *Volatility*. Langkah awal yang dilakukan adalah mengambil *memory dump*[31] pada sistem operasi yang diinfeksi menggunakan *tools DumpIt* untuk mencatat seluruh proses yang berjalan pada memori sistem operasi. Hasil dari proses ini akan menghasilkan *file* dengan ekstensi *.raw*. Tampilan aplikasi dapat dilihat pada gambar 12.



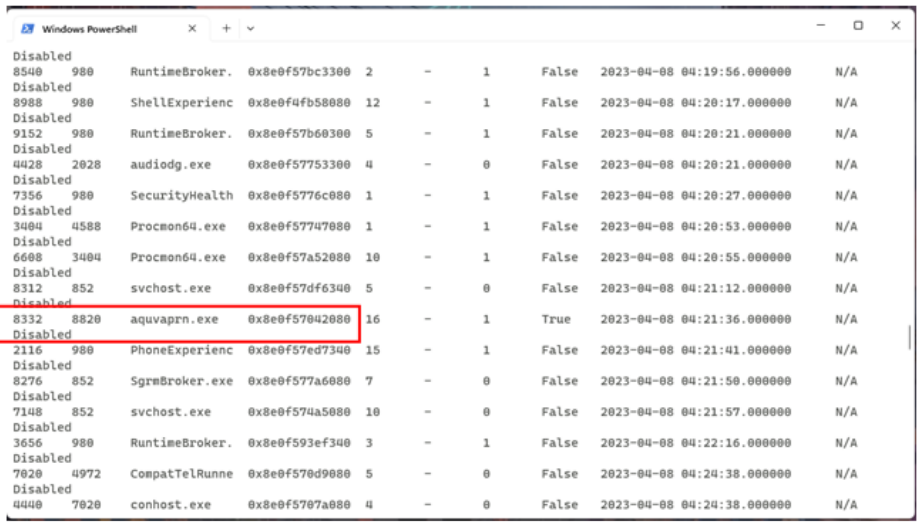
Gambar 12. Tampilan *Tools Dumpit*

Hasil dari proses *memory forensic* menghasilkan *file* dengan `DESKTOP-F5PS81V-20230408-042450.raw` yang memiliki ukuran sebesar 5.24 GB yang dilihat pada Gambar 13.



Gambar 13. Hasil *Memory Dump*

Hasil dari *memory dump* pada gambar 13 diproses dengan tools volatility menggunakan perintah "`python vol.py -f C:\Users\spazd\Documents\DESKTOP-F5PS81V-20230408-042450.raw Windows.pslist | more`" untuk menampilkan proses yang sudah diambil pada proses *memory dump*[32]. Hal ini memiliki tujuan untuk melihat proses yang dibuat oleh *malware* (*AQUVAPRN.exe*) sehingga dari hasil ini didapatkan[33] bahwa terdapat proses *AQUVAPRN.exe* dengan *PID* 8332, *virtual address* "`0x8e0f57042080`" dan berjalan pada waktu 8 April 2023 pukul 04.21 WIB seperti gambar 14.



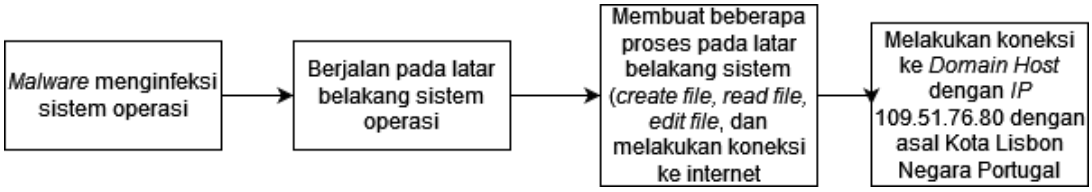
Gambar 14. Proses *Pslist Volatility*

Semua koneksi yang dilakukan pada *memory dump* ini dapat ditampilkan menggunakan perintah "`python vol.py -f C:\Users\spazd\Documents\DESKTOP-F5PS81V-20230408-042450.raw Windows.netscan | more`" yang akan menampilkan semua proses yang melakukan koneksi ke internet. Proses ini juga menampilkan proses yang dibuat oleh *malware* (*AQUVAPRN.exe*) dengan hasil melakukan interaksi dengan *IP* 192.168.170.130 dan mencoba melakukan sinkronisasi dengan alamat *IP* 13.107.21.200 yang dalam ini berbeda dengan hasil yang ditampilkan pada gambar 10. Gambar 15 merupakan hasil dari percobaan *netscan* pada *tools* ini.

```
0x8e0f51f4a4e0  TCPv4   192.168.170.130 49903   13.107.21.200   443     CLOSED  -       -       N/A
0x8e0f539d4c90  UDPv4   0.0.0.0 0       *       0               8332    aquvaprn.exe    2023-04-08 04:27:35.000000
0x8e0f539d4c90  UDPv6   ::      0       *       0               8332    aquvaprn.exe    2023-04-08 04:27:35.000000
```

Gambar 15. Proses Netscan Volatility

Berdasarkan hasil penelitian yang telah dilakukan alur kerja *malware* ketika menginfeksi sebuah sistem operasi yaitu berjalan pada latar belakang sistem operasi dengan membuat proses *create file*, *edit file*, dan *read file* terhadap data yang ada pada sistem operasi yang terinfeksi yang kemudian melakukan koneksi ke *Domain Host malware* tersebut yang berada di Kota Lisbon Negara Portugal yang memungkinkan pembuat *malware AQUVAPRN.exe* berpotensi melihat atau bahkan mencuri data dari sistem operasi yang terinfeksi. Hal ini dapat dilihat alur kerja *malware AQUVAPRN.exe* pada gambar 16[34].



Gambar 16. Alur Kerja *Malware AQUVAPRN.exe*

IV. SIMPULAN

Malware AQUVAPRN.exe merupakan jenis *RAT* yang beroperasi dengan cara mengubah, membuat, dan mengirimkan data pada komputer yang terinfeksi[35]. *Malware* ini dapat berjalan pada latar belakang saat aplikasi dijalankan dan melakukan beberapa proses seperti mengubah *file registry*, membuat *file*, membaca *file*, dan melakukan koneksi internet dengan *IP Address* tertentu. Hal ini dapat membebani sistem operasi dan *hardware* komputer, serta berpotensi membocorkan data pribadi pengguna. *Malware AQUVAPRN.exe* menggunakan teknik *anti reverse engineering obfuscation*[30] dan memiliki PID (*Process Identifier*) proses 8332 dengan alamat *virtual* `0x8e0f57042080`. Alamat *IP Address* yang dicurigai sebagai pembuat atau server *malware* berada di Kota Lisbon, Portugal, dengan nilai *hash* MD5 `55c2c12970cda52f58bfad7b8c7d37d5`.

DAFTAR PUSTAKA

[1] C. C. Ciptohartono and M. K. Dermawan, "Pencegahan Viktimisasi Pencurian Data Pribadi," *Deviance: Jurnal Kriminologi*, vol. 3, no. 2, pp. 157–169, 2019.
[2] D. R. Septiani, N. Widiyasono, and H. Mubarok, "Investigasi Serangan Malware Njrat Pada PC," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 123–128, 2016.
[3] A. Triantoro, N. Widiyasono, and R. Gunawan, "Hack. exe Malware Analysis and Investigation Using Memory Forensics," *Ojs.Unud.Ac.Id*, vol. 6, no. 2, pp. 94–99, 2021.
[4] N. Zalavadiya and D. P. Sharma, "A Methodology of Malware Analysis, Tools and Technique for windows platform – RAT Analysis," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 5, no. 3, pp. 5042–5054, 2017.
[5] D. Uppal, V. Mehra, and V. Verma, "Basic survey on Malware Analysis, Tools and Techniques," *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 103–112, 2014.
[6] C. Rathnayaka and A. Jamdagni, "An efficient approach for advanced malware analysis using memory forensic technique," *Proc. - 16th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 11th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Conf. Embed. Softw. Syst.*, pp. 1145–1150, 2017.
[7] H. A. Nugroho and Y. Prayudi, "Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan," *Knsi*, pp. 27–28, 2014.
[8] I. Gunawan and A. Ferriyan, "Analisis Malware Botnet Proteus Pendekatan Static dan Dinamic," *JR J. RESPONSIVE Tek. Inform.*, vol. 1, no. 1, pp. 12–17, 2017.
[9] M. R. Fadli, "Memahami desain metode penelitian kualitatif," *Humanika*, vol. 21, no. 1, pp. 33–54, 2021.
[10] S. Almarri and P. Sant, "Optimised Malware Detection in Digital Forensics," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 1, pp. 1–15, 2014.
[11] D. Prayitno, "Systematic Literature Review: Implementasi Metode Statis Dan Dinamis Pada Analisa Malware," *Simetris*, vol. 16, no. 2, pp. 53–57, 2022.
[12] F. Bahtiar, N. Widiyasono, and A. P. Aldya, "Memory Volatile Forensik Untuk Deteksi Malware Menggunakan Algoritma Machine Learning," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, pp. 242–253, 2018.
[13] S. Megira, A. R. Pangesti, and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," *J. Phys. Conf. Ser.*, vol. 1140, no. 1, 2018.
[14] S. Yusirwan, Y. Prayudi, and I. Riadi, "Implementation of Malware Analysis using Static and Dynamic Analysis Method," *Int. J. Comput. Appl.*, vol. 117, no. 6, pp. 11–15, 2015.
[15] F. D. S. M. Moises and J. D. Santoso, "Analisis Malware Android Menggunakan Metode Reverse Engineering," *JIKMA*, vol. 1, no. 2, pp. 41–53, 2023.
[16] Y. D. Puji Rahayu and Nanang Trianto, "Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1," *Info Kripto*, vol. 15, no. 3, pp. 105–111, 2021.
[17] V. A. Manoppo, A. S. M. Lumenta, and S. D. S. Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.
[18] B. A. Saputro, L. I. Alfitra, and R. B. Oktaviaji, "Analisis Malware Android Menggunakan Metode Reverse Engineering," *J. Repos.*, vol. 2, no. 10, pp. 1331–1337, 2020.
[19] S. Sinambela, A. R. Pangestu, and R. Feriyanto, "Analisis Aplikasi Malware pada Android dengan Metode Statik," *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 3, no. 2, pp. 88–94, 2020.
[20] S. Hadi, "Pemeriksaan Keabsahan Data Penelitian Kualitatif Pada Skripsi [Examination of the Validity of Qualitative Research Data on Thesis]," *Ilmu Pendidik.*, vol. 22, no. 1, pp. 21–22, 2016.
[21] M. Alvian, H. Nasution, and A. T. Laksono, "Investigasi Serangan Backdoor Remote Access Trojan (RAT) Terhadap Smartphone," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 4, pp. 505–510, 2020.
[22] J. D. Nugraha, A. Budiono, and A. Almaarif, "Analisis Malware Berdasarkan API Call Memory Dengan Metode Deteksi Signature-Based," *J. Rekayasa Sist. Ind.*, vol. 6, no. 02, p. 77, 2019.

[23] A. R. Damanik, H. B. Seta, and T. Theresiawati, "Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis," *J. Ilm. Matrik*, vol. 25, no. 1, pp. 89–97, 20237.
[24] Y. Ilhamdi and Y. N. Kunang, "Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik," *Bina Darma Conf. Comput. Sci.*, vol. 3, pp. 256–264, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124
[25] A. Amiruddin, P. N. H. Suryani, S. D. Santoso, and M. Y. B. Setiadji, "Utilizing Reverse Engineering Technique for A Malware Analysis Model," *Sci. J. Informatics*, vol. 8, no. 2, pp. 222–229, 2021.
[26] M. Nicho, R. Yadav, and D. Singh, "Analyzing WhisperGate and BlackCat Malware: Methodology and Threat Perspective," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 504–519, 2023.
[27] D. A. Daniswara, A. Budiono, A. Almaarif, and S. Kom, "Analisis Deteksi Malicious Activity Menggunakan Metode Analisis Malware Dinamis Berbasis Anomaly Detection Analysis of Malicious Activity Using Anomaly-Based Dynamic Malware Analysis Method," *2019, e-Proceeding Eng. Vol.6*, vol. 6, no. 2, pp. 7796–7803, 2019.
[28] A. S. Rusdi, N. Widiyasono, and H. Sulastri, "Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis," *J. Ilm. Inform.*, vol. 7, no. 2, pp. 99–107, 2019.
[29] A. Rahmatulloh, *Keamanan Source Code PHP Menggunakan Teknik Obfuscation*. Banyumas: Pena Persada, 2020. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Dxn94LQAAAAJ&cstart=20&pagesize=80&citation_for_view=Dxn94LQAAAAJ:bEWYMUwI8FkC
[30] M. R. Ridho, "Pendekatan Reverse Engineering Untuk Pengujian Keamanan Guna Meningkatkan Kualitas Perangkat Lunak," *J. Inform.*, vol. 16, no. 1, 2016.
[31] M. N. Rifkiansyah, R. S. Wibowo, … R. P.-, and undefined 2021, "Penerapan Memory Forensic Menggunakan Metode Live Forensic untuk Investigasi Random Access Memory," *Conference.Upnvj.Ac.Id*, vol. 7, no. 1, pp. 531–542, 2022, [Online]. Available: https://conference.upnvj.ac.id/index.php/senamika/article/view/1422
[32] Y. B. Setiadji, D. F. Priambodo, M. Hasbi, and F. I. Sabila, "Identifikasi Malware Berdasarkan Artefak Registry Windows 10 Menggunakan Regshot dan Cuckoo," *J. Edukasi dan Penelit. Inform.*, vol. 8, no. 3, p. 482, 2022.
[33] P. Gadgil and S. Nagpure, "Analysis of Advanced Volatile Threats Using Memory Forensics," *SSRN Electron. J.*, 2019.
[34] A. Siddiq, H. Yudiastuti, and F. Panjaitan, "Analisis Perilaku Malware Dengan Metode Surface Analysis Dan Runtime Analysis," *J. Softw. Eng. Ampera*, vol. 1, no. 3, pp. 160–174, 2020.
[35] R. Mahmud and Y. Prayudi, "Analisis Cyber Threat Injeksi Malware pada Suatu Dokumen Menggunakan Metode Mandiant ' s Cyber Attack Lifecycle Model," *J. Sains Komput. Inform.*, vol. 6, no. 1, pp. 209–225, 2022.