



JUDUL

Analisis Malware Menggunakan Static Analysis, Dynamic Analysis, dan Reverse Engineering pada Honeypot

SKRIPSI

DINA YULIASTI 2207421002

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER POLITEKNIK NEGERI JAKARTA**

2026



JUDUL

Analisis Malware Menggunakan *Static Analysis, Dynamic Analysis*, dan *Reverse Engineering* pada *Honeypot*

SKRIPSI

DINA YULIASTI / 2207421002

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER POLITEKNIK NEGERI JAKARTA**

2026



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Dina Yuliasti

NIM : 2207421002

Jurusan/Program Studi : Teknik Informatika dan Komputer/Teknik
Multimedia dan Jaringan

Judul Skripsi : Analisis Malware Menggunakan *static analysis*,
dynamic analysis, dan *reverse engineering* pada *Honeypot*

Menyatakan dengan sebenarnya bahwa skripsi ini benar – benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 2026

Yang membuat pernyataan



Dina Yuliasti

NIM. 2207421002



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Dina Yulianti
NIM : 2207421002
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Malware menggunakan Static Analysis, Dynamic Analysis, dan Reverse Engineering pada Honeypot

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari, Tanggal, Bulan, Tahun 2026 dan dinyatakan LULUS.

Disahkan oleh:

Pembimbing I : Iik Muhamad Malik Motin, S.Kom., M.T.
Penguji I : Asep Kurniawan, S.Pd., M.Kom.
Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom.
Penguji III : Andika Riyadi Jasril, M.Pd.T

Mengetahui:

Jurusan Teknik Informatika dan Komputer
Ketua
Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

Dipindai dengan CamScanner

Dipindai dengan CamScanner



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Assalamualaikum Wr., Wb.

Puji dan syukur selalu kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Malware Menggunakan *Static Analysis*, *Dynamic Analysis*, dan *Reverse Engineering* pada *Honeypot*” dengan baik atas bantuan, motivasi, dan dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. kepada Ibu Dr. Anita Hidayati, S.Kom., M.Kom., selaku Ketua Jurusan, penulis mengucapkan terima kasih.
2. Bapak Iik Muhammad Malik Matin, S.Kom., M.T. selaku pembimbing penulis yang telah banyak membantu, mendukung, dan memberikan masukan serta saran kepada penulis selama mengerjakan skripsi ini hingga selesai.
3. Teristimewa penulis mengucapkan terima kasih yang sebesar-besarnya kepada kedua orang tua tercinta yang telah memberikan banyak dukungan, doa dan cinta tanpa syarat yang diberikan kepada penulis selama proses penyelesaian skripsi.
4. Sahabat dan teman-teman yang telah banyak membantu dan memberikan dukungan dalam pengerjaan skripsi.
5. Seluruh pihak yang telah terlibat, memberikan doa serta dukungan dalam proses penyusunan skripsi ini yang tidak dapat penulis sebutkan satu per satu.
6. Teruntuk Dina Yuliasti, anak perempuan pertama dan harapan orang tua. Terima kasih telah bertahan, tidak menyerah, dan terus berjalan melewati semua tantangan. Perjalanan ini belum selesai, tapi kamu mampu melewatinya. Ingat, kamu berhak bahagia dan bermimpi.

Akhir kata penulis mengucapkan banyak terima kasih kepada semuanya. Penulis menyadari bahwa dalam penyusunan skripsi ini masih banyak terdapat kekurangan dan keterbatasan, oleh karena itu penulis memohon maaf atas ketidaksempurnaan ini. Semoga skripsi yang ditulis ini bermanfaat dan menjadi motivasi untuk penelitian selanjutnya dan bagi pembaca.

Wassalamualaikum Wr., Wb.

Depok, Juni 2026

Penulis



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Dina Yuliasti
NIM : 2207421002
Jurusan/Program Studi : Teknik Informatika dan Komputer/Teknik
Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Analisis Malware menggunakan Static Analysis, Dynamic Analysis, dan Reverse Engineering pada HoneyPot

Dengan Hak Bebas Royalti NonEksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 2026

Yang menyatakan



Dina Yuliasti
NIM.2207421002

Analisis Malware Menggunakan Static Analysis, Dynamic Analysis, dan Reverse Engineering pada HoneyPot

ABSTRAK

Malware Windows merupakan ancaman keamanan siber yang terus berkembang dengan varian baru bermunculan setiap harinya, sementara penelitian terdahulu masih terbatas pada satu atau dua metode analisis serta bergantung pada dataset publik yang bersifat statis dan kurang mencerminkan pola serangan terkini. Penelitian ini bertujuan untuk mengembangkan honeypot sebagai sarana pengumpulan sampel malware Windows secara real-time, serta melakukan analisis mendalam terhadap sampel tersebut menggunakan tiga metode terintegrasi, yaitu Static Analysis, Dynamic Analysis, dan Reverse Engineering, guna menghasilkan kompilasi Indicators of Compromise (IoC) yang komprehensif. Studi kasus dilakukan terhadap lima sampel malware yang ditangkap oleh honeypot Dionaea pada platform T-Pot, terdiri atas dua sampel bertipe Launcher dan tiga varian WannaCry, yang sebelumnya diverifikasi menggunakan VirusTotal. Static analysis menggunakan PESTudio, Detect-It-Easy (DIE), dan FLOSS berhasil mengidentifikasi struktur PE, toolchain kompilasi yang identik pada seluruh sampel, evolusi tingkat obfuscation (entropi rendah pada Sampel 1–3 dan tinggi pada Sampel 4–5), serta domain C2 hardcoded yang menyerupai mekanisme kill-switch WannaCry tanpa risiko eksekusi. Dynamic analysis melalui Process Monitor, Process Explorer, Wireshark, dan FakeNet mengungkap perilaku runtime aktual, termasuk network scanning agresif menuju port 445 (SMB), upaya eksploitasi SMBv1/EternalBlue oleh proses mssecsvr.exe, serta pola registry enumeration dan masquerading pada berbagai proses. Reverse Engineering menggunakan Ghidra berhasil membongkar logika dropper dan mekanisme konstruksi path dinamis melalui fungsi ekspor Play Game, yang tidak terlihat pada kedua metode sebelumnya. Hasil penelitian menunjukkan bahwa ketiga metode bersifat saling melengkapi, di mana kombinasi ketiganya menghasilkan cakupan IoC yang jauh lebih komprehensif dibandingkan penggunaan satu atau dua metode saja, sehingga dapat dijadikan acuan deteksi dan respons insiden siber terhadap malware Windows canggih seperti WannaCry.

Kata kunci: Malware Analysis, Static Analysis, Dynamic Analysis, Reverse Engineering, HoneyPot, Indicators of Compromise, Windows Malware, WannaCry.



DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME	iii
LEMBAR PENGESAHAN	iv
KATA PENGANTAR.....	v
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	vi
ABSTRAK	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	ix
BAB I.....	10
PENDAHULUAN.....	10
1.1 Latar Belakang.....	10
1.2. Perumusan Masalah.....	13
1.3. Batasan Masalah.....	13
1.4. Tujuan dan Manfaat.....	13
1.4.1. Tujuan.....	13
1.4.2. Manfaat.....	14
1.5. Sistematika Penulisan.....	14
BAB V	16
PENUTUP	16
5.1 Kesimpulan.....	16
5.2 Saran	17
DAFTAR PUSTAKA.....	19
DAFTAR RIWAYAT HIDUP.....	22
LAMPIRAN	23

DAFTAR GAMBAR

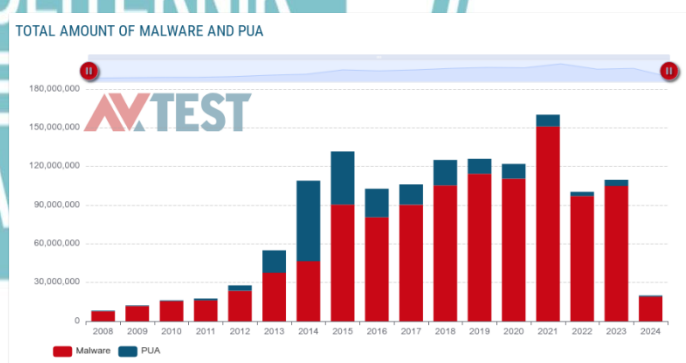
Gambar 1. 1 Statistik Total Malware dan Potentially Unwanted Applications10



BAB I PENDAHULUAN

1.1 Latar Belakang

Malware merupakan ancaman keamanan siber yang jahat dan paling kritis, yang secara sistematis menargetkan sistem operasi Windows, *platform* yang mendominasi sekitar 73,38% pasar perangkat komputasi global di lingkungan personal, *enterprise*, dan infrastruktur kritis (StatCounter, 2024). Jenis serangan ini mencakup ransomware yang mengenkripsi data berharga secara massal untuk memeras korban (Kaspersky, 2024), trojan downloader yang mengunduh *payload* tambahan secara diam-diam, serta *infostealer* canggih seperti Lumma Stealer yang mencuri kredensial perbankan dan akun korporat, mengakibatkan kerugian ekonomi mencapai ratusan miliar rupiah pada tahun 2023-2024 (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024). Menurut AV-TEST Institute, sebuah lembaga independen yang memantau ancaman siber secara global, lebih dari 450.000 malware dan program tidak diinginkan (Potentially Unwanted Application/PUA) baru terdaftar setiap hari di basis data mereka, dengan jumlah ini terus bertambah karena aktivitas penyerang yang konstan (AV-TEST Institute, 2024). *Platform* Windows tercatat sebagai salah satu target utama malware karena dominasi penggunaannya di lingkungan desktop/laptop serta luasnya serangan yang sering dieksploitasi dalam berbagai teknik malware.



Gambar 1. 1 Statistik Total Malware dan Potentially Unwanted Applications

Pada Gambar menunjukkan perkembangan jumlah total malware dan *Potentially Unwanted Applications* (PUA) secara global yang tercatat oleh AV-TEST

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Institute sejak tahun 2008 hingga 2024. Grafik disajikan dalam bentuk batang bertumpuk (stacked bar chart), di mana warna merah merepresentasikan jumlah malware dan warna biru menunjukkan jumlah PUA.

Berdasarkan data yang dipublikasikan oleh analisis antivirus independen di tahun 2025 sekitaran 87,4% dari deteksi malware terjadi pada windows, sedangkan pada mac OS mencatat sekitar 12,6% dari total kasus malware yang terdeteksi. Penelitian sebelumnya menghadapi beberapa tantangan dan keterbatasan yang signifikan. Pertama, berkaitan dengan sumber data, sebagaimana yang telah dilakukan oleh Yusirwan et al. (2020) dan Guo et al. (2023), banyak penelitian sebelumnya bergantung pada dataset publik seperti Virus Share, Malware Bazaar, atau Contagiodump yang bersifat statis dan sudah tersedia secara terbuka, sehingga menimbulkan permasalahan terhadap tingkat kebaruan sampel yang dianalisis. Di sisi lain, penelitian yang dilakukan oleh R.M. Muhammad et al. (2021) dan Holbel et al. (2024) memanfaatkan honeypot, namun fokus penelitian mereka lebih mengarah pada perancangan sistem keamanan jaringan dan proses *threat hunting*, bukan pada analisis teknis mendalam terhadap sampel malware itu sendiri. Kedua, keterbatasan metodologi analisis yang dipakai sebagaimana dilakukan oleh Eliando et al. (2022), Guo et al. (2023), dan Damaševičius et al. (2025). Penelitian terdahulu cenderung melakukan satu jenis analisis saja, baik itu *static analysis*, *dynamic analysis*, maupun *reverse engineering*, tanpa melakukan kombinasi komprehensif dari ketiga metode tersebut untuk membongkar logika internal malware secara mendalam.

Static analysis menjadi langkah penting pertama yang memungkinkan ekstraksi informasi struktural dari *Portable Executable* (PE) header tanpa eksekusi berisiko, termasuk analisis *Import Address Table* (IAT), *section permissions*, overlay data, serta *suspicious strings* yang mengindikasikan C2 domains atau *registry run keys*. Tools seperti PEiD untuk packer identification dan *Strings* untuk *hardcoded IOC extraction* memberikan *baseline analysis* yang cepat namun terbatas pada *surfacelevel artifacts*.

Dynamic analysis melengkapi keterbatasannya dengan monitoring perilaku *runtime* dalam lingkungan sandbox terisolasi, mengamati API calls mencurigakan seperti

CreateRemoteThread, *registry* *modifications* di *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*, *network beaconing* ke *external IPs*, serta *file drops* di *%AppData%* atau *%Temp%* directories. Platform tools *Process Monitoring* dan *Process Explorer* secara spesifik mencatat *behavioral indicators* yang tak terlihat pada *static examination*, seperti *process injection* dan *privilege escalation attempts*.

Reverse engineering melalui *disassembly* dan *decompilation* kode *assembly* merupakan tahap lanjutan analisis untuk mengungkap logika tersembunyi seperti *anti-analysis techniques* (*timing checks*, *red pill*), *custom crypters*, dan *hardcoded C2 infrastructure* yang luput dari dua metode sebelumnya, memerlukan tools profesional seperti Ghidra untuk *control flow reconstruction*.

Penelitian ini mengambil sampel malware terbaru yang dihasilkan langsung dari honeypot tpot, menangkap varian autentik dari penyerang nyata dalam real-time, berbeda dengan penggunaan dataset publik yang bersifat statis seperti VirusShare atau Malware Bazar yang sudah outdated dalam 24-48 jam. Sampel *Honeypot* merepresentasikan *attack patterns* terkini dengan geographical relevance ke Indonesia, memberikan ground truth data untuk validasi ketiga metode analisis secara komprehensif.

Penelitian ini menerapkan analisis sistematis terhadap sampel malware Windows terkini dari honeypot menggunakan tiga metode terintegrasi secara berurutan: *Static Analysis* dengan Detect-It-Easy (DIE), strings/Floss, PEStudio, dan Virustotal untuk *structural profiling* tanpa *execution risk*. *Dynamic Analysis* melalui *Process monitor* (Procmon), *Process explorer*, Wireshark, dan juga Fakenet. *Reverse Engineering* menggunakan Ghidra (free) untuk *full disassembly*, *function identification*, *string references*, dan *control flow graph reconstruction* guna ekstraksi IOC tingkat tinggi seperti *mutex names*, *registry persistence paths*, dan *obfuscated C2 communications*.

1.2. Perumusan Masalah

Melalui latar belakang tersebut, maka rumusan masalahnya adalah:

1. Bagaimana mengembangkan honeypot untuk mengumpulkan malware?
2. Bagaimana melakukan analisis menggunakan *static analysis*, *dynamic analysis*, dan *reverse engineering* terhadap sampel malware yang dihasilkan dari honeypot.

1.3. Batasan Masalah

Batasan masalah ini bertujuan untuk memperjelas ruang lingkup penelitian sehingga pembahasan tidak terlalu luas. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Sampel malware terbatas pada varian Windows yang ditangkap honeypot dan dipilih sebanyak 5 sampel
2. Analisis *static* menggunakan tools DIE, PESTudio, VirusTotal, dan strings/Floss
3. Analisis *dinamik* menggunakan Procmon, Process Explorer, Wireshark, dan Fakenet
4. *Reverse Analysis* menggunakan tools Ghidra untuk *disassemble* dan *decompilation*.
5. Penelitian ini Tidak membahas pengembangan tools baru atau integrasi dengan SIEM production systems
6. Lingkungan pengujian dibatasi hanya pada windows 11
7. Penelitian ini Tidak membahas *behavioral machine learning classification*
8. Penelitian ini tidak menggunakan YARA rules untuk mendeteksi malware.

1.4. Tujuan dan Manfaat

1.4.1. Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan honeypot untuk mengumpulkan malware

2. Melakukan analisis menggunakan *static analysis*, *dynamic analysis*, dan *reverse engineering* terhadap sampel malware yang dihasilkan dari honeypot

1.4.2. Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut.

1. Menyediakan referensi analisis malware berbasis honeypot dengan *dataset real-time* untuk penelitian *cybersecurity* akademik .
2. Memperkaya literatur tentang sinergi *static-dynamic-reverse engineering* pada varian Windows malware terkini.
3. Memberikan studi kasus praktis tools analisis yang direkomendasikan komunitas peneliti malware.
4. Menghasilkan kompilasi IoC *actionable* (*registry keys*, *mutexes*, *C2 domains*)
5. Memberikan panduan analisis malware bagi praktisi *cyber security* Indonesia menghadapi ancaman Windows dominan.
6. Mendukung validasi honeypot *deployment* untuk pengumpulan sampel malware berkualitas tinggi di organisasi lokal.
7. Menjadi bahan evaluasi pada sampel malware yang dihasilkan dari honeypot sebagai sumber data analisis malware berbasis serangan nyata.

1.5. Sistematika Penulisan

Adapun sistematika penulisan dari laporan ini adalah sebagai berikut

a. BAB I PENDAHULUAN

Bab I ini menjelaskan latar belakang penelitian, perumusan masalah, batasan, tujuan, dan manfaat penelitian, serta sistematika penulisan.

b. BAB II TINJAUAN PUSTAKA

Bab II berisikan penjelasan mengenai landasan teori atau kajian ilmu yang berhubungan dengan berbagai pokok pikiran topik penyusunan skripsi ini yang relevan dari sumber yang valid.

c. BAB III METODE PENELITIAN

Bab III menjelaskan rancangan penelitian dan alur sistem analisis malware berbasis honeypot yang diusulkan, sumber data dan sampel yang digunakan, teknik pengumpulan data dari lingkungan honeypot dan lab analisis, teknik analisis data secara kualitatif dan kuantitatif terhadap hasil *static*, *dynamic*, dan *reverse engineering*, serta jadwal pelaksanaan penelitian dan rincian biaya yang diperlukan.

d. BAB IV HASIL DAN PEMBAHASAN

Bab IV menyajikan hasil penelitian dan pembahasan dari analisis malware menggunakan tiga metode terintegrasi. Bab ini terdiri dari sub-sub bab mencakup analisis kebutuhan, perancangan sistem, implementasi sistem, dan pengujian dengan *static analysis*, *dynamic analysis*, dan *reverse engineering* serta evaluasi pengujian berupa kompilasi IoC dari hasil ketiga metode analisis.

e. BAB V PENUTUP

Bab V berisikan kesimpulan atau hasil akhir dari penelitian yang telah dilakukan, serta saran untuk penelitian berikutnya.

POLITEKNIK
NEGERI
JAKARTA

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan terhadap lima sampel malware Windows yang diperoleh dari honeypot selama 2 bulan menggunakan tiga metode analisis secara berurutan (*static analysis*, *dynamic analysis*, dan *reverse engineering*), menghasilkan kesimpulan sebagai berikut:

1. Proses pengumpulan sampel dan temuan teknis ketiga metode analisis. *Honeypot* Dionaea yang dijalankan dalam platform T-Pot dan dikonfigurasi pada VPS berhasil menangkap sampel malware secara *real-time* dari penyerang nyata yang menargetkan port SMB (445), HTTP (80), dan FTP (21). Sampel yang tertangkap diverifikasi menggunakan VirusTotal, kemudian diseleksi secara *purposive* (keunikan hash, validitas format PE, keberagaman tipe) sehingga diperoleh 5 sampel *representative* yaitu 2 sampel bertipe Launcher (Sampel 1–2) dan 3 varian WannaCry (Sampel 3–5). Ketiga metode analisis yang diterapkan secara berurutan berhasil mengungkap karakteristik malware secara bertahap dan saling melengkapi. *Static analysis* (PEStudio, DIE, FLOSS) mengidentifikasi bahwa kelima sampel dikompilasi dengan *toolchain* identik dan bernama asli "launcher.dll" mengindikasikan satu *builder framework* yang sama dengan entropi rendah pada Sampel 1–3 (4,0–4,3) dan tinggi pada Sampel 4–5 (6,4+, *payload* terenkripsi pada .rsrc), serta *domain C2 hardcoded* yang menyerupai *kill-switch* WannaCry pada Sampel 2 dan 3. *Dynamic analysis* (Procmon, Process Explorer, Wireshark, FakeNet) mengungkap perilaku *runtime* yang tidak terlihat pada static analysis, di antaranya *masquerading* dan *persistence* pada Sampel 1, *registry enumeration* pada Sampel 2, perilaku *worm* paling agresif dengan upaya eksploitasi SMBv1/*EternalBlue* oleh mssecsvr.exe pada Sampel 3 dan 4, serta persiapan eksploitasi SMB melalui *LanmanServer\Parameters* pada Sampel 5. *Reverse engineering* (Ghidra) mengonfirmasi logika internal di baliknya yaitu fungsi ekspor Play Game pada Sampel 3–5 sebagai *entry point payload*, *mekanisme two-stage*

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

execution pada Sampel 4 (konstruksi path *mssecsvr.exe* via *sprintf* diikuti eksekusi), pola *dropper/packer FindResource-LoadResource-LockResource-SizeofResource* pada Sampel 1, serta *conditional dispatcher logic* pada fungsi entry Sampel 5 yang memanggil sub-rutin *FUN_1000113e* sebagai logika inti malware.

2. Komplementaritas ketiga metode analisis. *Static*, *dynamic*, dan *reverse engineering* terbukti bersifat saling melengkapi dan tidak dapat saling menggantikan dalam menghasilkan *Indicator of Compromise* (IoC) yang komprehensif. *Static analysis* unggul dalam kecepatan dan keamanan eksekusi untuk *profiling* awal (IoC berbasis *file/hash*), *dynamic analysis* mengungkap *tradecraft* nyata (IoC jaringan, *registry*, dan proses), sedangkan *reverse engineering* menghasilkan IoC tingkat lanjut (mekanisme enkripsi, anti-debugging, dan logika C2) yang tidak dapat diperoleh dari kedua metode lainnya. Kombinasi ketiganya menghasilkan cakupan IoC yang jauh lebih lengkap dibandingkan penggunaan satu atau dua metode saja, mengonfirmasi bahwa pendekatan *mono-* atau *dual-*metode tidak memadai untuk menganalisis malware canggih seperti WannaCry yang mengimplementasikan *packing*, *anti-debugging*, C2 *terenkripsi*, dan *process injection* secara bersamaan.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah dipaparkan, berikut adalah saran yang dapat dijadikan bahan pertimbangan untuk penelitian dan pengembangan selanjutnya:

1. Perluasan sampel dan periode pengumpulan, memperpanjang operasi honeypot menjadi minimal 3 bulan dan menambah sampel menjadi 20–50 untuk hasil *statistik* yang lebih representatif.
2. Integrasi *threat intelligence*, mengintegrasikan IoC (*hash*, *domain* C2, *registry key*, *mutex*) ke platform seperti MISP atau OpenCTI untuk mempercepat respons terhadap varian malware serupa.
3. Pengembangan YARA rules, menyusun dan mengevaluasi YARA rules berbasis IoC hasil penelitian terhadap sampel malware baru dari honeypot.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4. Otomatisasi *pipeline* analisis, mengembangkan scripting (Python/PowerShell) untuk menjalankan tools secara berurutan dan menyusun matriks IoC otomatis, guna meningkatkan skalabilitas dan replikabilitas.
5. Perluasan ke *platform* non-Windows, mengadaptasi metodologi tiga metode ini untuk malware Linux (server/IoT) dan Android (APK), mengingat meningkatnya ancaman pada *platform* tersebut.



DAFTAR PUSTAKA

- AV-TEST Institute. (2025). *Malware statistics*. <https://www.av-test.org/en/statistics/malware/>
- Bombardieri, C., & Capretti, S. (2015). *Honeypot-powered malware reverse engineering (HERESy)* [Preprint]. arXiv. <https://arxiv.org/abs/1510.03892>
- Damaševičius, R., Maskeliūnas, R., Blažauskas, T., & Smuikys, A. (2025). FETA: A systematic and efficient approach for feature extraction in malware analysis. *Journal of Information Security and Applications*, 90, 103965. <https://doi.org/10.1016/j.jisa.2025.103965>
- Eliando, E., Lumenta, A. S. M., & Najoran, X. B. N. (2022). LockBit 2.0 ransomware: Analysis of infection, persistence, and impact. *Cogito Smart Journal*, 8(2), 356–370. <https://cogito.unklab.ac.id/index.php/cogito/article/view/356>
- Guo, M. I., Anwer, I., Riasat, A., & Kim, S. (2023). Windows malware detection based on static analysis with multiple features. *PeerJ Computer Science*, 9, e1319. <https://doi.org/10.7717/peerj-cs.1319>
- Holbel, T., Combs, J., Graves, J., & Haynes, T. (2024). Utilizing virtualized honeypots for threat hunting, malware analysis and reporting. *Issues in Information Systems*, 25(1), 265–278. https://iacis.org/iis/2024/1_iis_2024_265-278.pdf
- Infosec Institute. (2024). *Static malware analysis tutorial*. <https://resources.infosecinstitute.com/topic/static-malware-analysis/>
- International Journal for Multidisciplinary Research. (2023). Malware analysis and reverse engineering. *IJFMR*, 5(6). <https://www.ijfmr.com/papers/2023/6/10296.pdf>
- Kaspersky. (2024). *Ransomware: The biggest cyber threat of 2024*. Kaspersky Security Blog. <https://www.kaspersky.com/resourcecenter/threats/ransomware>
- Muhammad, R. M., Stiawan, D., & Idris, M. Y. (2021). Integrated security system implementation for network environment using honeypot. *Journal of Navy and University Studies (JONUNS)*, 1(1). <https://jonuns.com/index.php/journal/article/view/619>

- StatCounter GlobalStats. (2024). *Desktop operating system market share worldwide*.
<https://gs.statcounter.com/os-market-share/desktop/worldwide/>
- Surfshark. (2025). *Malware cases by operating system*.
<https://surfshark.com/research/chart/malware-cases-windows-macOS/>
- YARA Project. (2024). *YARA official documentation*. ReadTheDocs.
<https://yara.readthedocs.io/>
- Yusirwan, S., Wahyudi, A., & Sanjaya, R. (2020). Implementation of malware analysis using static and dynamic analysis method. *Proceedings of the 2020 International Conference on Electrical Engineering and Informatics (ICEEI)*. IEEE.
<https://doi.org/10.1109/ICEEI51358.2020.9254935>
- National Institute of Standards and Technology. (2021). *Malware incident prevention and handling for desktops and laptops* (NIST Special Publication 800-83 Rev. 1). U.S. Department of Commerce.
<https://doi.org/10.6028/NIST.SP.800-83r1>
- Afianian, A., Niksefat, S., Sadeghiyan, B., & Baptiste, D. (2022). Malware dynamic analysis evasion techniques: A survey. *ACM Computing Surveys*, 54(6), 1–35. <https://doi.org/10.1145/3365001>
- Grigorios, L., Apostolidis, K. D., & Kanas, V. G. (2021). Comparative review of malware analysis methodologies. *International Journal of Network Security & Its Applications*, 13(6), 91–104. <https://doi.org/10.5121/ijnsa.2021.13608>
- Fortinet. (2024). *What are indicators of compromise (IoC)?* FortiGuard Glossary.
<https://www.fortinet.com/resources/cyberglossary/indicators-ofcompromise>
- Microsoft Security. (2024). *Indicators of compromise (IoCs) in Microsoft Defender*. Microsoft Learn. <https://learn.microsoft.com/en-us/defenderendpoint/manage-indicators>
- Mandiant/Google. (2023). *FLARE FLOSS: FireEye Labs Obfuscated String Solver* (Version 3.0) [Software]. GitHub. <https://github.com/mandiant/flare-floss>
- Microsoft Sysinternals. (2023). *Process Monitor (Procmon) for Windows* [Software]. Microsoft. <https://learn.microsoft.com/en-us/sysinternals/downloads/procmon>
- VirusTotal. (2024). *VirusTotal: Analyze suspicious files, domains, IPs and URLs* [Web service]. Google. <https://www.virustotal.com/>
- Wireshark Foundation. (2024). *Wireshark: Network protocol analyzer* (Version 4.2) [Software]. <https://www.wireshark.org/>



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Avanzato, J. (2025). From CPU spikes to defense: How Varonis prevented a ransomware disaster. Varonis Blog. Retrieved from

<https://www.varonis.com/blog/varonis-prevents-ransomware-disaster>

varo, S., Vila, G., & Pegueroles, J. (2026). Automating the detection of evasive Windows malware: An evaluated YARA rule library for anti-VM and antisandbox techniques. Journal of Cybersecurity and Privacy, 6(2), 69.

<https://doi.org/10.3390/jcp6020069>

Kanj, S., Vila, G., & Pegueroles, J. (2026). Automating the detection of evasive Windows malware: An evaluated YARA rule library for anti-VM and antisandbox techniques. Journal of Cybersecurity and Privacy, 6(2), 69. <https://doi.org/10.3390/jcp6020069>

Varonis Systems. (2025). From CPU spikes to defense: How Varonis prevented a ransomware disaster. Retrieved from <https://www.varonis.com/blog/varonisprevents-ransomware-disaster>

Cyber Security News. (2025, February 6). *Ghidra 11.3 released*. Diakses dari

<https://cybersecuritynews.com/ghidra-11-3-released/>



DAFTAR RIWAYAT HIDUP



Dina Yuliasti, akrab disapa Dina. Lahir di Bekasi, pada tanggal 23 Juli 2003. Penulis memulai Pendidikan formal di SD Negeri 062 Mompang Jae pada tahun 2009, setelah itu melanjutkan Pendidikan di SMP Negeri 1

Panyabungan Utara.

pada tahun 2015, Kemudian meneruskan Pendidikan di SMK Negeri 3 Panyabungan pada tahun 2019. Pada tahun 2022 penulis menempuh Pendidikan Diploma IV di Politeknik Negeri Jakarta dengan jurusan Teknik Informatika dan Komputer pada Program Studi Teknik Multimedia dan Jaringan.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LAMPIRAN

pestudio 9.61 - Malware Initial Assessment - www.winitor.com c:\sample7a4ee\7a4eecc3b0222545d598564d3485997 (read-only)		
file settings about		
c:\sample7a4ee\7a4eecc3b0222545d598564d3485997		
property	value	
file		
file > sha256	C4EC46A0CE486CC3861C6DC1623D88C4907E0974178904D89CC5046C647FAA80	
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
file > first 32 bytes (text)	MZ.....@.....	
file > info	size: 5267459 bytes, entropy: 6.293	
file > type	dynamic-link-library, 32-bit, GUI	
file > version	n/a	
file > description	n/a	
entry-point > first 32 bytes (hex)	55 8B EC 53 8B 5D 08 56 88 75 0C 57 8B 7D 10 85 F6 75 09 83 3D 40 31 00 10 00 EB 26 83 FE 01 74	
entry-point > location	0x000011E9 (section[.text])	
file > signature	Microsoft Linker 6.0	
stamps		
stamp > compiler	Thu May 11 12:21:37 2017 (UTC)	
stamp > debug	n/a	
stamp > resource	n/a	
stamp > import	n/a	
stamp > export	Thu May 11 12:21:37 2017 (UTC)	
names		
file > name	c:\sample7a4ee\7a4eecc3b0222545d598564d3485997	
debug > file	n/a	
export > original-file-name	launcher.dll	
version	n/a	
manifest	n/a	
.NET > module > name	n/a	
certificate > program-name	n/a	

Lampiran 1 Tampilan PESTudio pada tahap analisis sampel 1

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\sample44bc\44bc540ed22c83517f5068ba58da383 (read-only)

file settings about

c:\sample44bc\44bc540ed22c83517f5068ba58da383

indicators (wait...) footprints (wait...) virustotal (offline) dos-header (size > 64) dos-stub (size > 160) rich-header (tooling > file-header (dll > 32-bit optional-header (subs) directories (count > 5) sections (file > unknown libraries (count > 2) imports (flag > 2) exports (name > PlayG thread-local-storage (NET (n/a) resources (signature > abc strings (wait...) debug (n/a) manifest (n/a) version (n/a) certificate (n/a) overlay (entropy > zero

property

value

file

file > sha256

file > first 32 bytes (hex)

file > first 32 bytes (text)

file > info

file > type

file > version

file > description

entry-point > first 32 bytes (hex)

entry-point > location

file > signature

stamps

stamp > compiler

stamp > debug

stamp > resource

stamp > import

stamp > export

names

file > name

debug > file

export > original-file-name

version

manifest

.NET > module > name

certificate > program-name

529DAD9429B7D3A12DEC140FC790D7FE842C6B8CF4CDC3330DEEC6B94E050609

4D 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

MZ.....@.....

size: 5267459 bytes, entropy: 4.097

dynamic-link-library, 32-bit, GUI

n/a

n/a

55 8B EC 53 8B 5D 08 56 88 75 0C 57 8B 7D 10 85 F6 75 09 83 3D 40 31 00 10 00 EB 26 83 FE 01 74

0x000011E9 (section[.text])

Microsoft Linker 6.0

Thu May 11 12:21:37 2017 (UTC)

n/a

n/a

n/a

Thu May 11 12:21:37 2017 (UTC)

c:\sample44bc\44bc540ed22c83517f5068ba58da383

n/a

launcher.dll

n/a

n/a

n/a

n/a

notepad++

cpu > 32-bit

file > type > dynamic-link-library

subsystem > GUI

Activate Windows

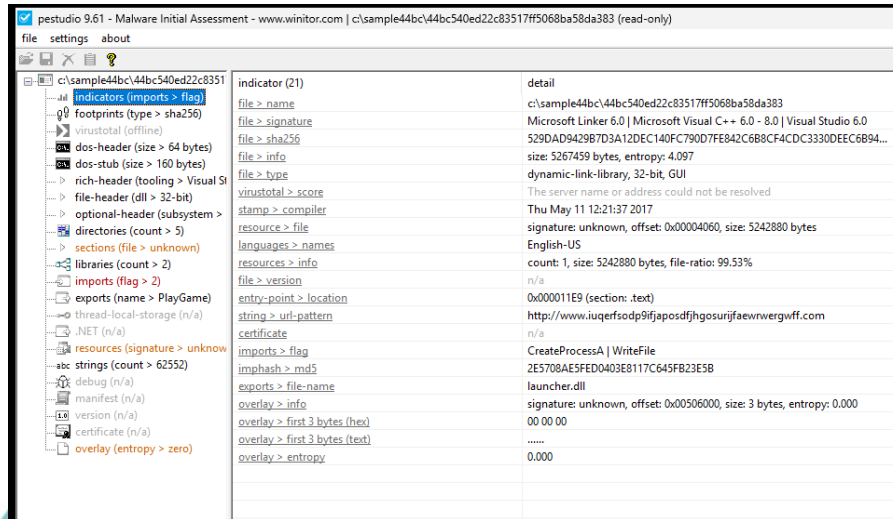
Go to Settings to activate Windows

Activate Windows
Go to Settings to activate Windows

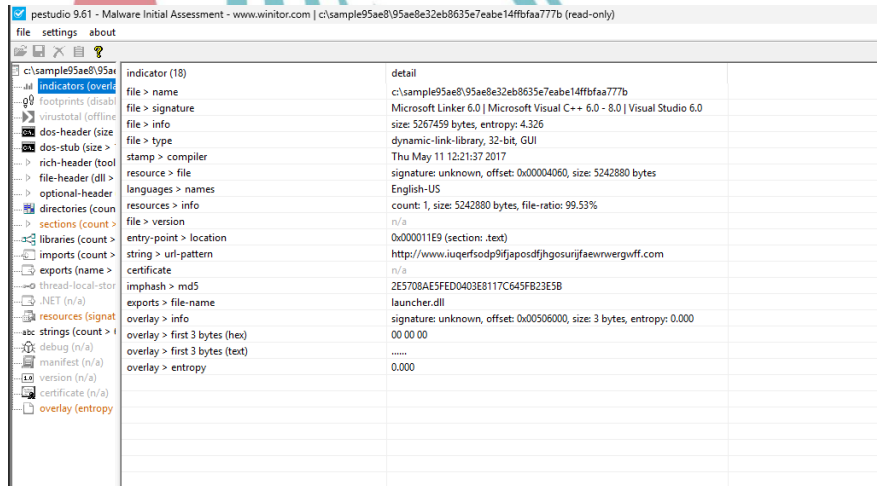
Lampiran 2 Tampilan PESTudio pada tahap analisis sampel 2

Hak Cipta :

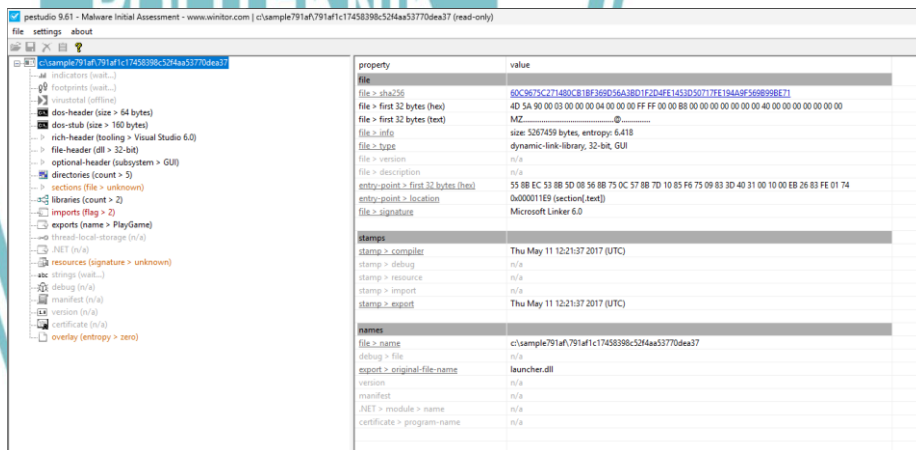
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 3 . Tampilan jendela indicators pada sampel 2



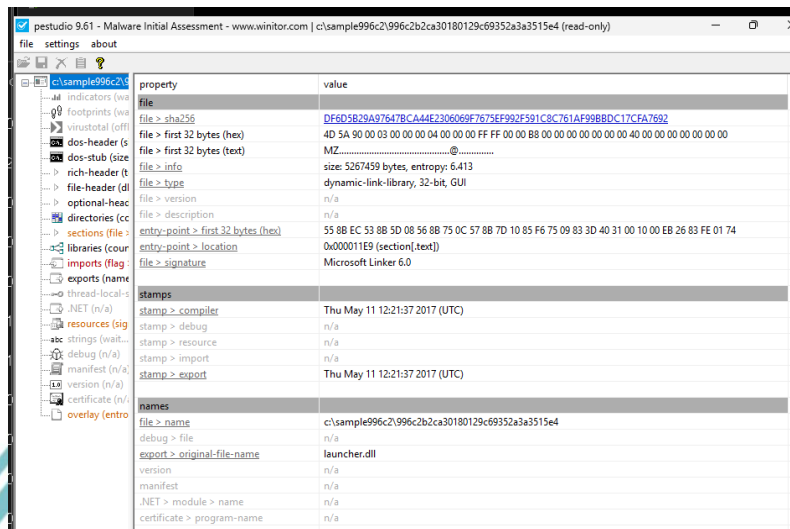
Lampiran 4 Tampilan menu indicators pada sampel 3



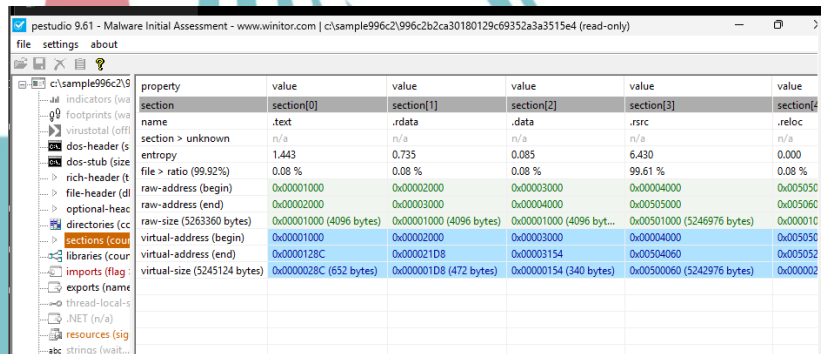
Lampiran 5 Tampilan jendela PESTUDIO pada sampel 4

Hak Cipta :

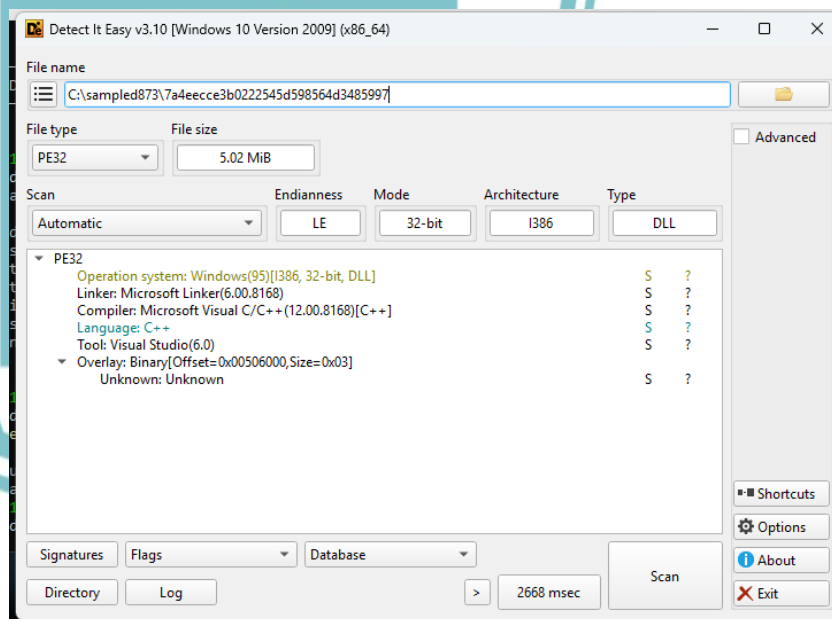
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 6 Tampilan jendela PESTudio pada sampel 5



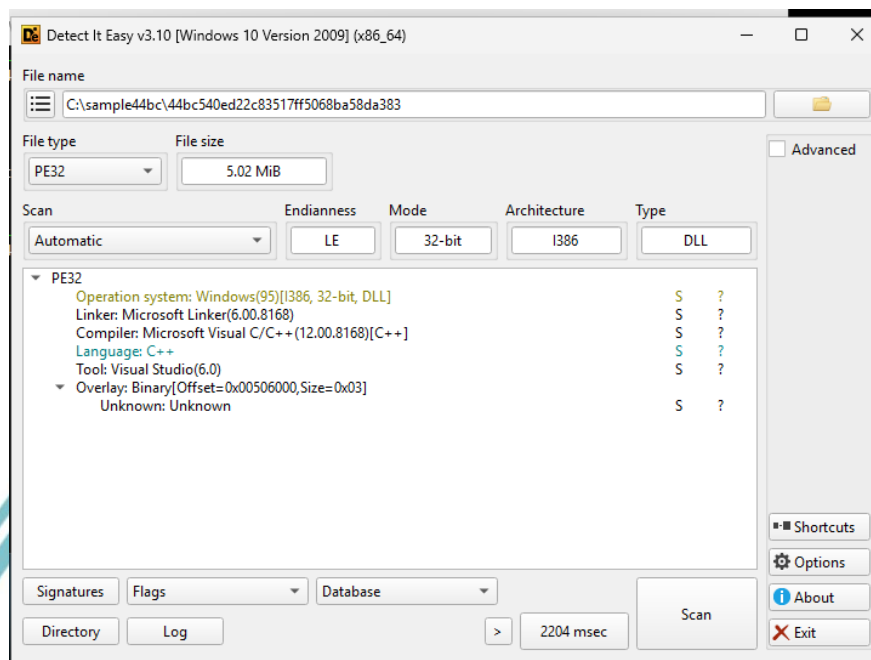
Lampiran 7 Tampilan menu section pada sampel 5



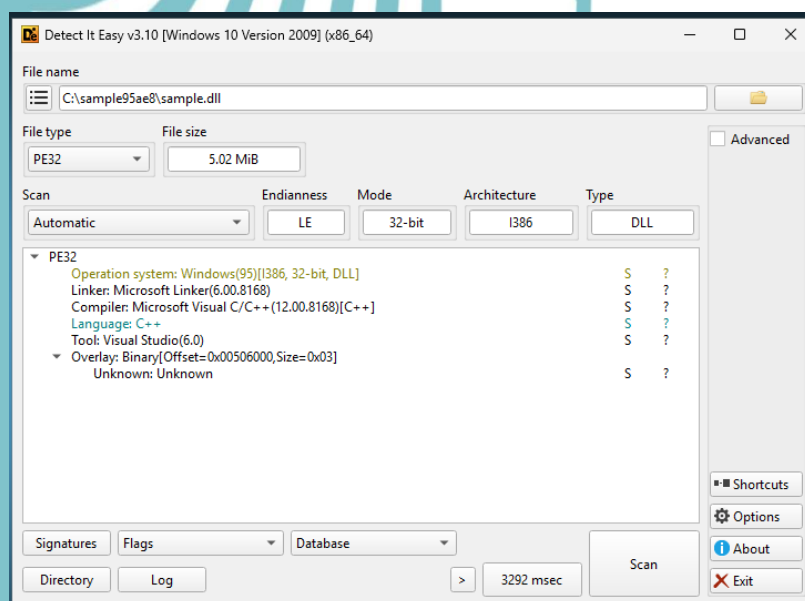
Lampiran 8 Tampilan DIE pada analisis sampel 1

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



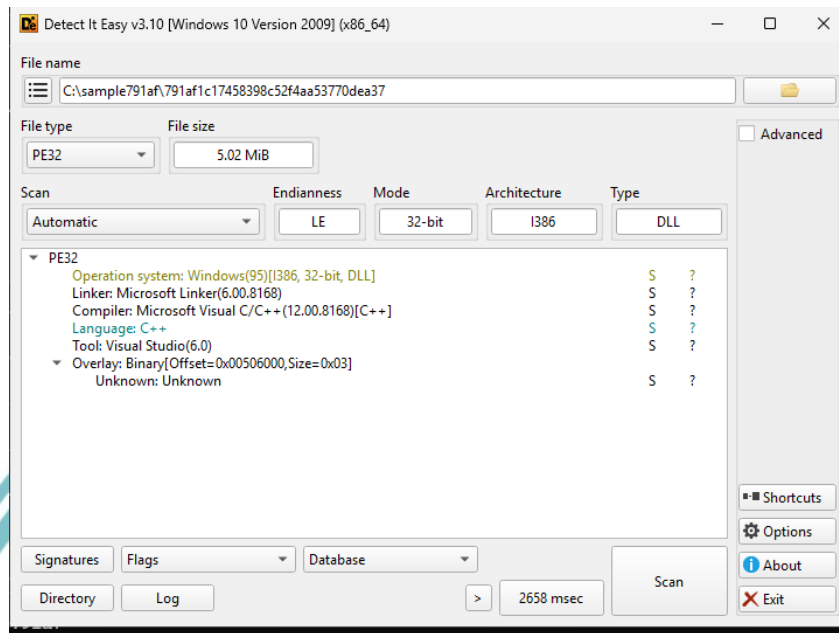
Lampiran 9 Tampilan DIE pada analisis sampel 2



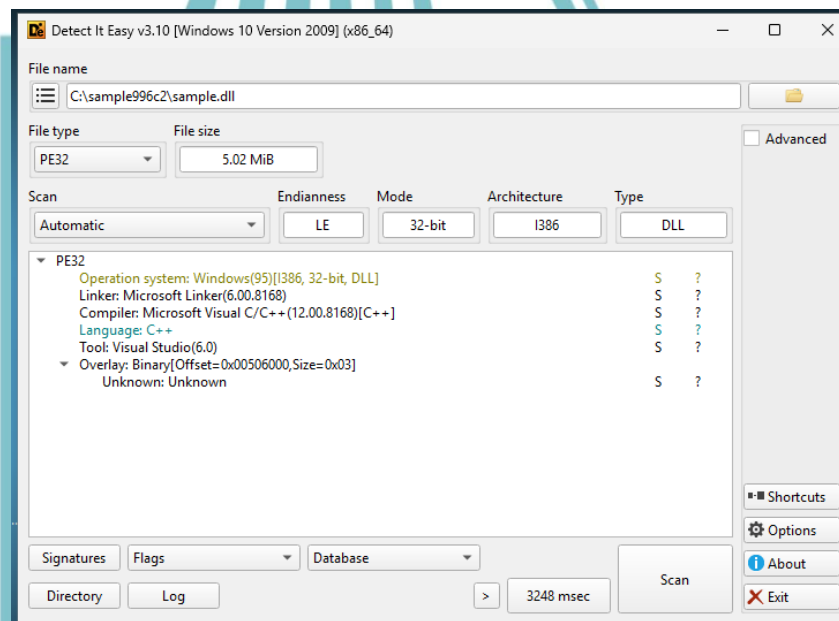
Lampiran 10 Tampilan DIE pada analisis sampel 3

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 11 Tampilan DIE pada analisis sampel 4



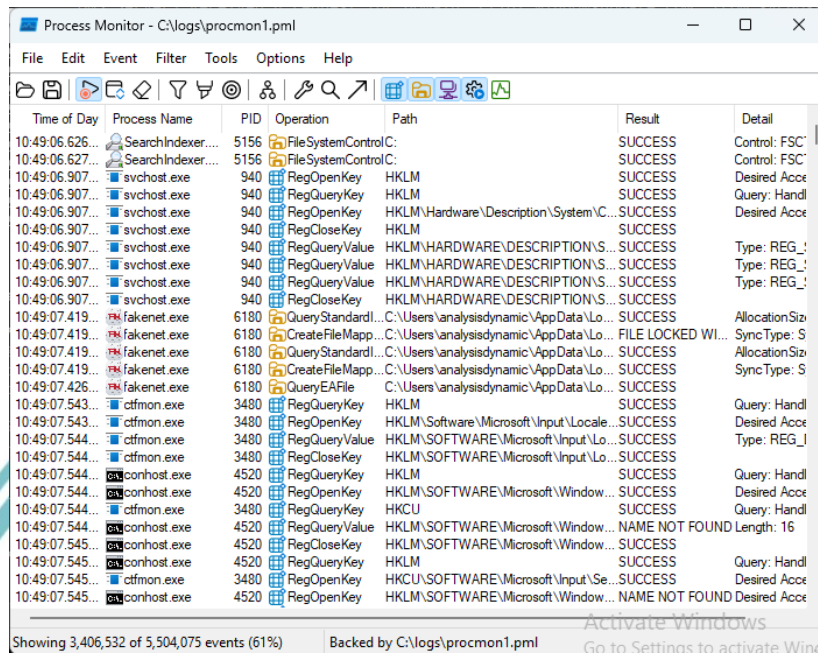
Lampiran 12 Tampilan DIE pada analisis sampel 4

```
PS C:\sample7a4ee > floss .\7a4eecc3b0222545d598564d3485997 > hasil_floss.txt
INFO: floss: extracting static strings
finding decoding function features: 100%[ ] 7/7 [00:00<00:00, 103.62 functions/s, skipped 2 library functions (28%)]
INFO: floss.stackstrings: extracting stackstrings from 4 functions
extracting stackstrings: 100%[ ] 4/4 [00:00<00:00, 22.18 functions/s]
INFO: floss.tightstrings: extracting tightstrings from 0 functions...
extracting tightstrings: 0 functions [00:00, ? functions/s]
INFO: floss.string_decoder: decoding strings
emulating function 0x100010ab (call 1/1): 100%[ ] 4/4 [00:00<00:00, 12.86 functions/s]
INFO: floss: finished execution after 111.95 seconds
INFO: floss: rendering results
```

Lampiran 13 Proses ekstraksi dan deskripsi string pada sampel 1

Hak Cipta :

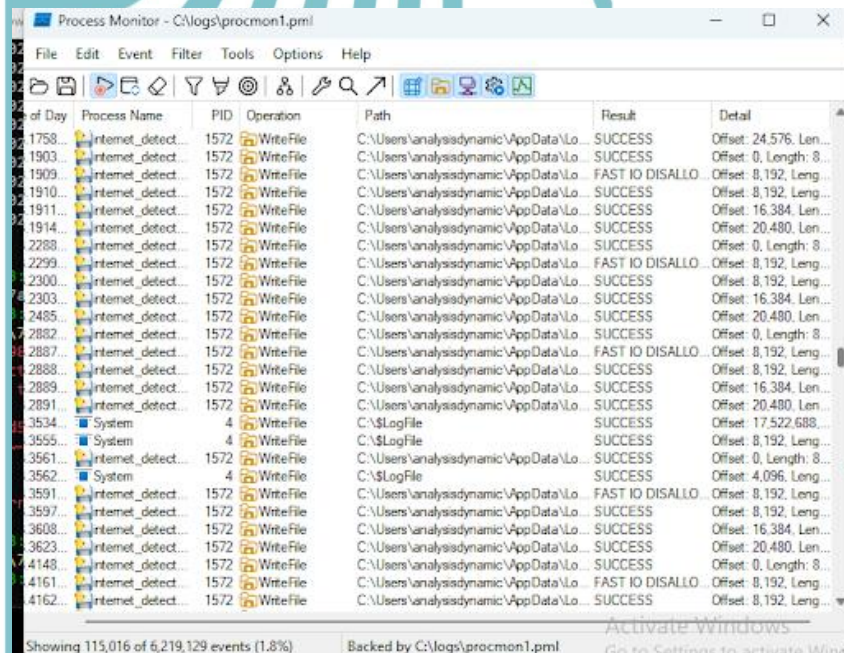
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:49:06.626...	SearchIndexer...	5156	FileSystemControl C:		SUCCESS	Control: FSC
10:49:06.627...	SearchIndexer...	5156	FileSystemControl C:		SUCCESS	Control: FSC
10:49:06.907...	svchost.exe	940	RegOpenKey	HKLM	SUCCESS	Desired Acco
10:49:06.907...	svchost.exe	940	RegOpenKey	HKLM	SUCCESS	Query: Handl
10:49:06.907...	svchost.exe	940	RegOpenKey	HKLM\Hardware\Description\System\...	SUCCESS	Desired Acco
10:49:06.907...	svchost.exe	940	RegCloseKey	HKLM	SUCCESS	
10:49:06.907...	svchost.exe	940	RegQueryValue	HKLM\HARDWARE\DESCRIPTION\...	SUCCESS	Type: REG_
10:49:06.907...	svchost.exe	940	RegQueryValue	HKLM\HARDWARE\DESCRIPTION\...	SUCCESS	Type: REG_
10:49:06.907...	svchost.exe	940	RegQueryValue	HKLM\HARDWARE\DESCRIPTION\...	SUCCESS	Type: REG_
10:49:06.907...	svchost.exe	940	RegCloseKey	HKLM\HARDWARE\DESCRIPTION\...	SUCCESS	
10:49:07.419...	fakenet.exe	6180	QueryStandardI...	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	AllocationSiz
10:49:07.419...	fakenet.exe	6180	CreateFileMapp...	C:\Users\analysisdynamic\AppData\Lo...	FILE LOCKED WI...	SyncType: S
10:49:07.419...	fakenet.exe	6180	QueryStandardI...	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	AllocationSiz
10:49:07.419...	fakenet.exe	6180	CreateFileMapp...	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	SyncType: S
10:49:07.426...	fakenet.exe	6180	QueryEaFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	
10:49:07.543...	ctfmon.exe	3480	RegOpenKey	HKLM	SUCCESS	Query: Handl
10:49:07.543...	ctfmon.exe	3480	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Acco
10:49:07.544...	ctfmon.exe	3480	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_I
10:49:07.544...	ctfmon.exe	3480	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
10:49:07.544...	conhost.exe	4520	RegOpenKey	HKLM	SUCCESS	Query: Handl
10:49:07.544...	conhost.exe	4520	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Acco
10:49:07.544...	ctfmon.exe	3480	RegOpenKey	HKCU	SUCCESS	Query: Handl
10:49:07.544...	conhost.exe	4520	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Length: 16	
10:49:07.545...	conhost.exe	4520	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
10:49:07.545...	conhost.exe	4520	RegOpenKey	HKLM	SUCCESS	Query: Handl
10:49:07.545...	ctfmon.exe	3480	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Acco
10:49:07.545...	conhost.exe	4520	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Desired Acco	

Showing 3,406,532 of 5,504,075 events (61%) Backed by C:\logs\procmon1.pml

Lampiran 14 Pemantauan aktivitas terhadap sampel 1



Time of Day	Process Name	PID	Operation	Path	Result	Detail
1758...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 24,576, Len...
1903...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 0, Length: 8...
1909...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	FAST IO DISALLO	Offset: 8,192, Leng...
1910...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 8,192, Leng...
1911...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 16,384, Len...
1914...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 20,480, Len...
2288...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 0, Length: 8...
2299...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	FAST IO DISALLO	Offset: 8,192, Leng...
2300...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 8,192, Leng...
2303...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 16,384, Len...
2485...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 20,480, Len...
2882...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 0, Length: 8...
2887...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	FAST IO DISALLO	Offset: 8,192, Leng...
2888...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 8,192, Leng...
2889...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 16,384, Len...
2891...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 20,480, Len...
3534...	System	4	WriteFile	C:\\$LogFile	SUCCESS	Offset: 17,522,688...
3555...	System	4	WriteFile	C:\\$LogFile	SUCCESS	Offset: 8,192, Leng...
3561...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 0, Length: 8...
3562...	System	4	WriteFile	C:\\$LogFile	SUCCESS	Offset: 4,096, Leng...
3591...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	FAST IO DISALLO	Offset: 8,192, Leng...
3597...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 8,192, Leng...
3608...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 16,384, Len...
3623...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 20,480, Len...
4148...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 0, Length: 8...
4161...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	FAST IO DISALLO	Offset: 8,192, Leng...
4162...	Internet_detect...	1572	WriteFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Offset: 8,192, Leng...

Showing 115,016 of 6,219,129 events (1.8%) Backed by C:\logs\procmon1.pml

Lampiran 15 Perilaku anomali proses pada sampel 1



Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
7:36:2...	ctfmon.exe	6912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
7:36:2...	ctfmon.exe	6912	RegQueryValue	HKLM	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Q...
7:36:2...	ctfmon.exe	6912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	NAME NOT FOUND	Length: 16
7:36:2...	ctfmon.exe	6912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
7:36:2...	ctfmon.exe	6912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Q...
7:36:2...	ctfmon.exe	6912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_DWO...
7:36:2...	ctfmon.exe	6912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
7:36:2...	ctfmon.exe	6912	CreateFile	C:\Windows\System32\en-US\mssp7e...	NAME NOT FOUND	Desired Access: R...
7:36:2...	ctfmon.exe	6912	CreateFile	C:\Windows\Globalization\ELS\SpellDi...	SUCCESS	Desired Access: R...
7:36:2...	ctfmon.exe	6912	QueryBasicInfor...	C:\Windows\Globalization\ELS\SpellDi...	SUCCESS	CreationTime: 4/26...
7:36:2...	ctfmon.exe	6912	CloseFile	C:\Windows\Globalization\ELS\SpellDi...	SUCCESS	
7:36:2...	ctfmon.exe	6912	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
7:36:2...	ctfmon.exe	6912	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R...
7:36:2...	ctfmon.exe	6912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
7:36:2...	ctfmon.exe	6912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
7:36:2...	ctfmon.exe	6912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
7:36:2...	ctfmon.exe	6912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
7:36:2...	ctfmon.exe	6912	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
7:36:2...	ctfmon.exe	6912	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
7:36:2...	ctfmon.exe	6912	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: R...
7:36:2...	ctfmon.exe	6912	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...

Showing 76,954 of 285,429 events (26%) Backed by virtual memory

Lampiran 16 Tampilan log aktivitas Procmon pada sampel 2

Process Monitor - Sysinternals: www.sysinternals.com

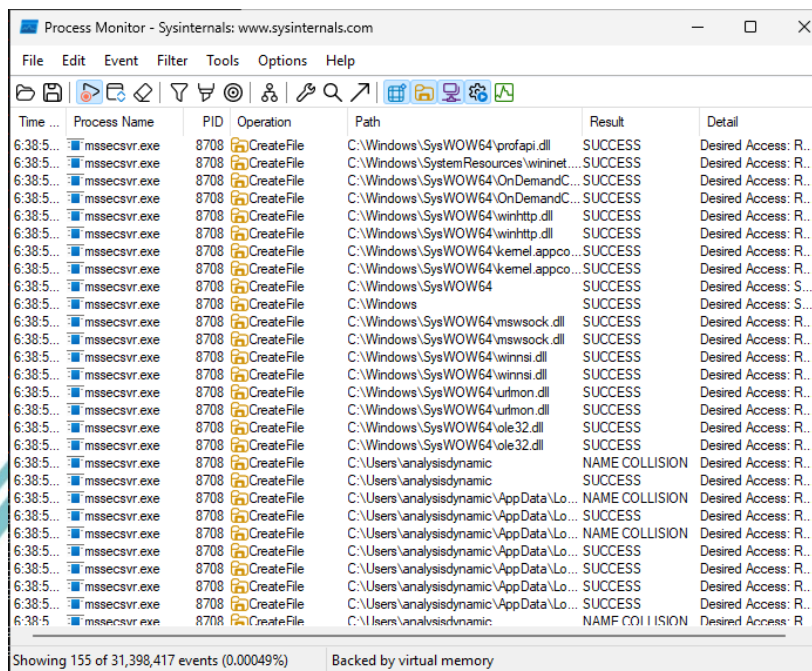
Time ...	Process Name	PID	Operation	Path	Result	Detail
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49136 -> 9.207.194.93...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49158 -> 86.13.187.168...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49160 -> 179.24.95.42...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49161 -> 8.6.78.201.mic...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49162 -> 188.182.113.1...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49165 -> 183.154.28.4...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49169 -> 67.28.131.223...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49138 -> 13.183.214.26...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49144 -> 84.138.53.111...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49148 -> 66.216.217.21...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49163 -> 204.237.200.8...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49164 -> 168.225.170.5...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49166 -> 126.148.54.95...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Reconnect	analisisdynamic:49167 -> 152.87.98.220...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49130 -> 107.224.36.10...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49132 -> 187.9.70.209...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49134 -> 32.22.82.52.m...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49135 -> 28.32.69.172...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49136 -> 9.207.194.93...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49148 -> 66.216.217.21...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49144 -> 84.138.53.111...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49138 -> 13.183.214.26...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49158 -> 86.13.187.168...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49160 -> 179.24.95.42...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49162 -> 188.182.113.1...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49161 -> 8.6.78.201.mic...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49164 -> 168.225.170.5...	SUCCESS	Length: 0, seqnum:...
6:38:5...	mssecsvr.exe	7152	TCP Disconnect	analisisdynamic:49163 -> 204.237.200.8...	SUCCESS	Length: 0, seqnum:...

Showing 37,520 of 7,118,068 events (0.52%) Backed by virtual memory

Lampiran 17 Anomali aktivitas jaringan pada sampel 3

Hak Cipta :

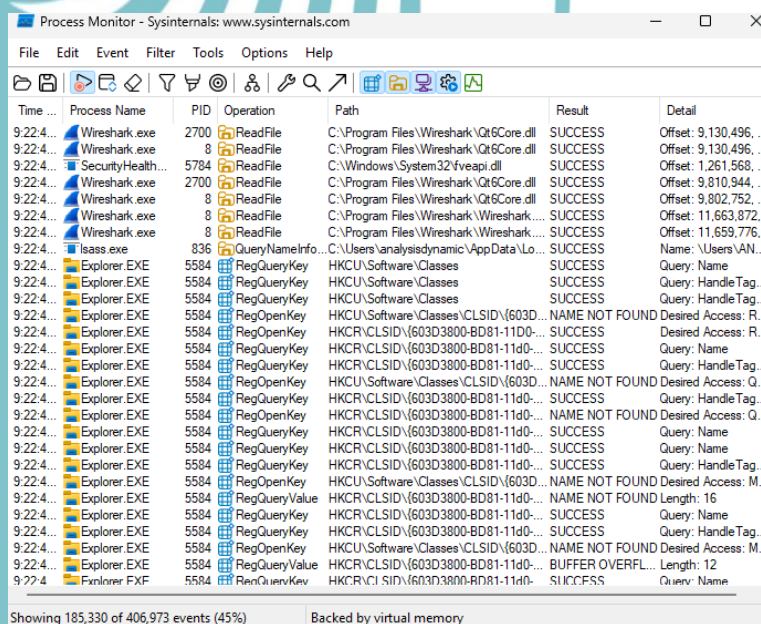
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Time ...	Process Name	PID	Operation	Path	Result	Detail
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SystemResources\wininet...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\OnDemandC...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\kernel.appco...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\kernel.appco...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64	SUCCESS	Desired Access: S...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows	SUCCESS	Desired Access: S...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\winnsi.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\winnsi.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic	NAME COLLISION	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	NAME COLLISION	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	NAME COLLISION	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Desired Access: R...
6:38:5...	mssecsvr.exe	8708	CreateFile	C:\Users\analysisdynamic\AppData\Lo...	NAME COLLISION	Desired Access: R...

Showing 155 of 31,398,417 events (0.00049%) Backed by virtual memory

Lampiran 18 Aktivitas file system pada sampel 3



Time ...	Process Name	PID	Operation	Path	Result	Detail
9:22:4...	Wireshark.exe	2700	ReadFile	C:\Program Files\Wireshark\Qt6Core.dll	SUCCESS	Offset: 9,130,496, ...
9:22:4...	Wireshark.exe	8	ReadFile	C:\Program Files\Wireshark\Qt6Core.dll	SUCCESS	Offset: 9,130,496, ...
9:22:4...	SecurityHealth...	5784	ReadFile	C:\Windows\System32\fsapi.dll	SUCCESS	Offset: 1,261,568, ...
9:22:4...	Wireshark.exe	2700	ReadFile	C:\Program Files\Wireshark\Qt6Core.dll	SUCCESS	Offset: 9,810,944, ...
9:22:4...	Wireshark.exe	8	ReadFile	C:\Program Files\Wireshark\Qt6Core.dll	SUCCESS	Offset: 9,802,752, ...
9:22:4...	Wireshark.exe	8	ReadFile	C:\Program Files\Wireshark\Wireshark...	SUCCESS	Offset: 11,663,872, ...
9:22:4...	Wireshark.exe	8	ReadFile	C:\Program Files\Wireshark\Wireshark...	SUCCESS	Offset: 11,659,776, ...
9:22:4...	lsass.exe	836	QueryNameInfo...	C:\Users\analysisdynamic\AppData\Lo...	SUCCESS	Name: \Users\AN...
9:22:4...	Explorer.EXE	5584	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
9:22:4...	Explorer.EXE	5584	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
9:22:4...	Explorer.EXE	5584	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Handle Tag...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCU\Software\Classes\CLSID\{603D...	NAME NOT FOUND	Desired Access: R...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Desired Access: R...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Name
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Handle Tag...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCU\Software\Classes\CLSID\{603D...	NAME NOT FOUND	Desired Access: Q...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Handle Tag...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Name
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Name
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Handle Tag...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCU\Software\Classes\CLSID\{603D...	NAME NOT FOUND	Desired Access: M...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	NAME NOT FOUND	Length: 16
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Name
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Handle Tag...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCU\Software\Classes\CLSID\{603D...	NAME NOT FOUND	Desired Access: M...
9:22:4...	Explorer.EXE	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	NAME NOT FOUND	Length: 12
9:22:4...	Fontlogr.FXF	5584	RegOpenKey	HKCR\CLSID\{603D3800-BD81-11d0-...	SUCCESS	Query: Name

Showing 185,330 of 406,973 events (45%) Backed by virtual memory

Lampiran 19 Proses monitor pada sampel 4



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

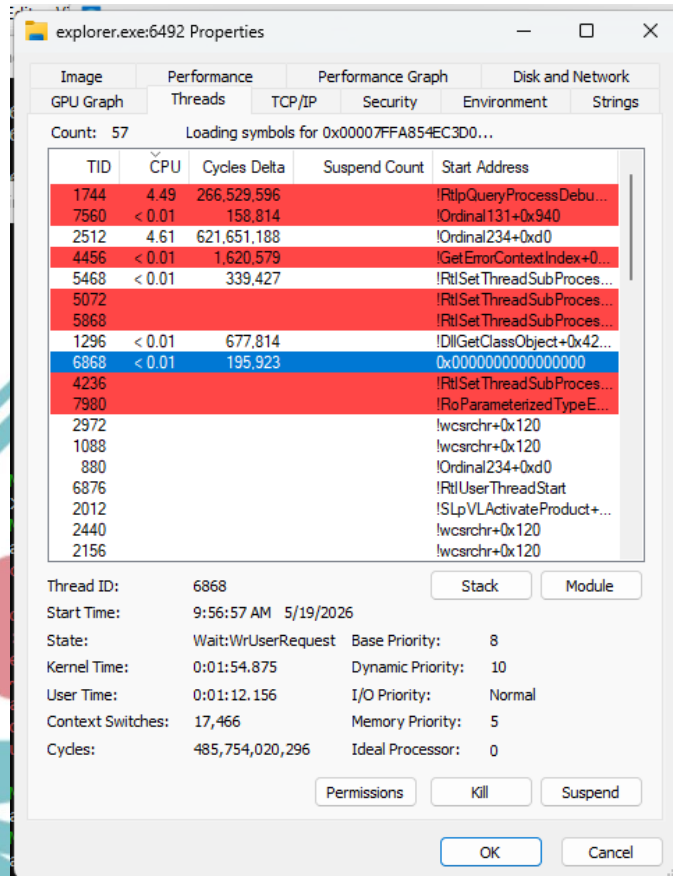
Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ... Process Name PID Operation Path Result Detail						
8:13:0...	rundll32.exe	8804	Process Start		SUCCESS	Parent PID: 6248, ...
8:13:0...	rundll32.exe	8804	Thread Create		SUCCESS	Thread ID: 8904
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\rundll32.exe	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	CreateFile	C:\Windows\Prefetch\RUNDLL32.EXE...	NAME NOT FOUND	Desired Access: G...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
8:13:0...	rundll32.exe	8804	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
8:13:0...	rundll32.exe	8804	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	BUFFER TOO SM...	Length: 0
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_BINA...
8:13:0...	rundll32.exe	8804	CreateFile	C:\sample996c2	SUCCESS	Desired Access: E...
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\kernelBase.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegQueryKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Query: Full, SubKe...
8:13:0...	rundll32.exe	8804	RegCloseKey	HKLM\System\CurrentControlSet\Win...	SUCCESS	
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
8:13:0...	rundll32.exe	8804	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
8:13:0...	rundll32.exe	8804	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
8:13:0...	rundll32.exe	8804	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
8:13:0...	rundll32.exe	8804	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	Thread Create		SUCCESS	Thread ID: 8524
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\combase.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\vpct4.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\SHCore.dll	SUCCESS	Image Base: 0x7fb...
8:13:0...	rundll32.exe	8804	Load Image	C:\Windows\System32\imagehlp.dll	SUCCESS	Image Base: 0x7fb...
Showing 99 of 2,343,394 events (0.0042%) Backed by virtual memory						

Lampiran 20 Tampilan log Procmon pada sampel 5



Hak Cipta :

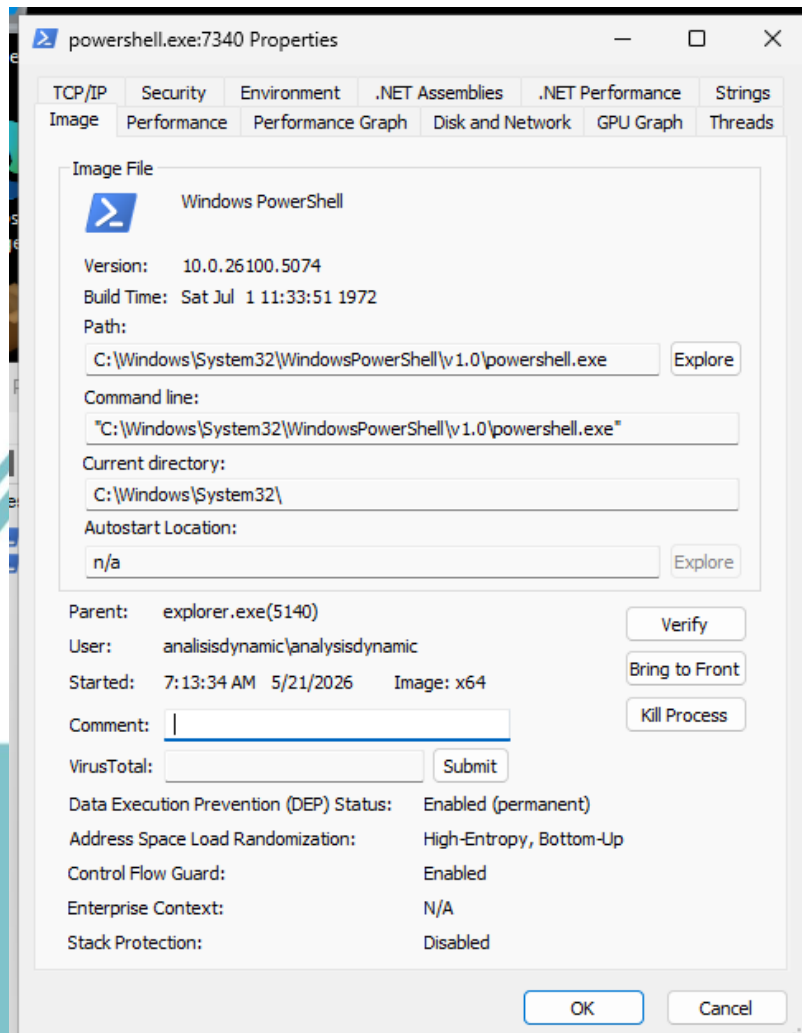
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 21 Jendela properti Process Explorer pada sampel 1

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 22 Jendela properti Process Explorer pada sampel 2

POLITEKNIK
NEGERI
JAKARTA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

P...	Local Address	Remote Address	State
TCP	analisisdynamic:54820	191.145.95.44:micro...	SYN_SENT
TCP	analisisdynamic:54823	197.134.16.178:micr...	SYN_SENT
TCP	analisisdynamic:54824	220.119.158.225:mi...	SYN_SENT
TCP	analisisdynamic:54825	74.253.214.17:micro...	SYN_SENT
TCP	analisisdynamic:54826	76.128.228.137:micr...	SYN_SENT
TCP	analisisdynamic:54827	141.122.243.154:mi...	SYN_SENT
TCP	analisisdynamic:54831	212.189.74.68:micro...	SYN_SENT
TCP	analisisdynamic:54848	136.71.30.16:micros...	SYN_SENT
TCP	analisisdynamic:54849	65.9.86.198:microsof...	SYN_SENT
TCP	analisisdynamic:54851	217.146.240.148:mi...	SYN_SENT
TCP	analisisdynamic:54852	8.63.68.35:microsoft...	SYN_SENT
TCP	analisisdynamic:54853	180.213.158.163:mi...	SYN_SENT
TCP	analisisdynamic:54858	220.169.143.120:mi...	SYN_SENT
TCP	analisisdynamic:54859	194.47.147.56:micro...	SYN_SENT
TCP	analisisdynamic:54860	193.206.105.121:mi...	SYN_SENT
TCP	analisisdynamic:54861	9.162.18.122:micros...	SYN_SENT
TCP	analisisdynamic:54864	93.3.37.187:microsof...	SYN_SENT
TCP	analisisdynamic:54879	199.37.72.54:micros...	SYN_SENT
TCP	analisisdynamic:54880	1.213.98.8:microsoft...	SYN_SENT
TCP	analisisdynamic:54881	158.251.184.11:micr...	SYN_SENT
TCP	analisisdynamic:54882	85.108.157.111:micr...	SYN_SENT
TCP	analisisdynamic:54884	101.186.153.202:mi...	SYN_SENT
TCP	analisisdynamic:54885	135.60.10.123:micro...	SYN_SENT
TCP	analisisdynamic:54886	64.100.176.3:micros...	SYN_SENT
TCP	analisisdynamic:54887	79.149.215.201:micr...	SYN_SENT
TCP	analisisdynamic:54888	221.113.110.9:micro...	SYN_SENT
TCP	analisisdynamic:54889	62.1.15.178:microsof...	SYN_SENT
TCP	analisisdynamic:54890	105.205.219.24:micr...	SYN_SENT

Lampiran 23 Perilaku jaringan pada sampel 3

POLITEKNIK
NEGERI
JAKARTA

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 24 Jendela process tree pada sampel 4

Lampiran 25 Tampilan operasi registri pada sampel 5

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No.	Time	Source	Destination	Protocol	Length	Info
274	526.758061600	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
275	526.760993400	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
644	1246.4783595	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
645	1246.4787916	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
1018	1968.3094274	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
1019	1968.3127461	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
1366	2686.8614833	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
1367	2686.8661171	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
1732	3409.3576693	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
1733	3409.3599782	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
2075	4131.6654904	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
2076	4131.6678146	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
2449	4853.7809702	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation
2450	4853.7851843	192.168.81.255	192.168.81.255	BROWSER	243	Host Announcement ANALISISDYNAMIC, Workstation, Server, NT Workstation

> Frame 274: Packet, 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
> Ethernet II, Src: VMware_b8:27:95:00:0c:29, Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.81.128, Dst: 192.168.81.255
> User Datagram Protocol, Src Port: 138, Dst Port: 138
> NetBIOS Datagram Service
> SMB (Server Message Block Protocol), Trans Request (0x25)
> SMB Mailslot Protocol
> Microsoft Windows Browser Protocol

Activate Windows
Go to Settings to activate Windows.

Lampiran 28 Tampilan analisis Wireshark pada sampel 2 (bagian 2)

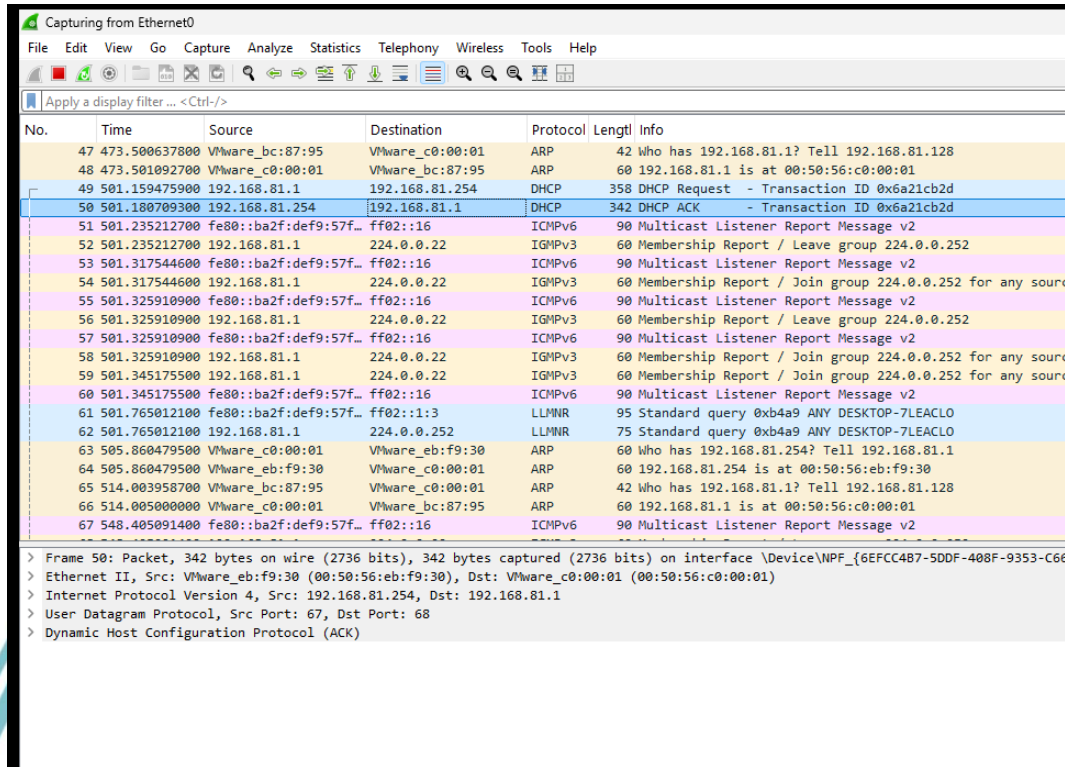
No.	Time	Source	Destination	Protocol	Length	Info
26	248.154360300	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
27	248.154360300	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
28	248.154360300	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any source
29	248.345941300	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any source
30	248.345941300	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
31	248.590916100	fe80::ba2f:def9:57f...	ff02::1:3	LLMNR	95	Standard query 0x8018 ANY DESKTOP-7LEACLO
32	248.590916100	192.168.81.1	224.0.0.252	LLMNR	75	Standard query 0x8018 ANY DESKTOP-7LEACLO
33	252.004177100	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
34	252.015004900	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
35	292.500078700	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
36	292.500736200	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
37	313.781824500	VMware_b8:27:95:00:0c:01	Broadcast	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
38	313.783055200	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
39	354.995297300	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
40	355.005168700	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
41	394.990248000	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
42	394.990867000	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
43	421.490113700	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
44	421.490516800	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
45	433.770397600	VMware_b8:27:95:00:0c:01	Broadcast	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
46	433.773077400	VMware_b8:27:95:00:0c:01	VMware_b8:27:95:00:0c:01	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01

> Frame 27: Packet, 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface Device\NPF_{6EFC487-5DDF-408F-9353-C667CB0...}
> Ethernet II, Src: VMware_b8:27:95:00:0c:01 (00:50:56:c0:00:01), Dst: IPv6mcast_16 (33:33:00:00:00:16)
> Internet Protocol Version 6, Src: fe80::ba2f:def9:57f0:4ca2, Dst: ff02::16
> Internet Control Message Protocol v6

Lampiran 29 Tampilan analisis Wireshark pada sampel 3 (bagian 1)

Hak Cipta :

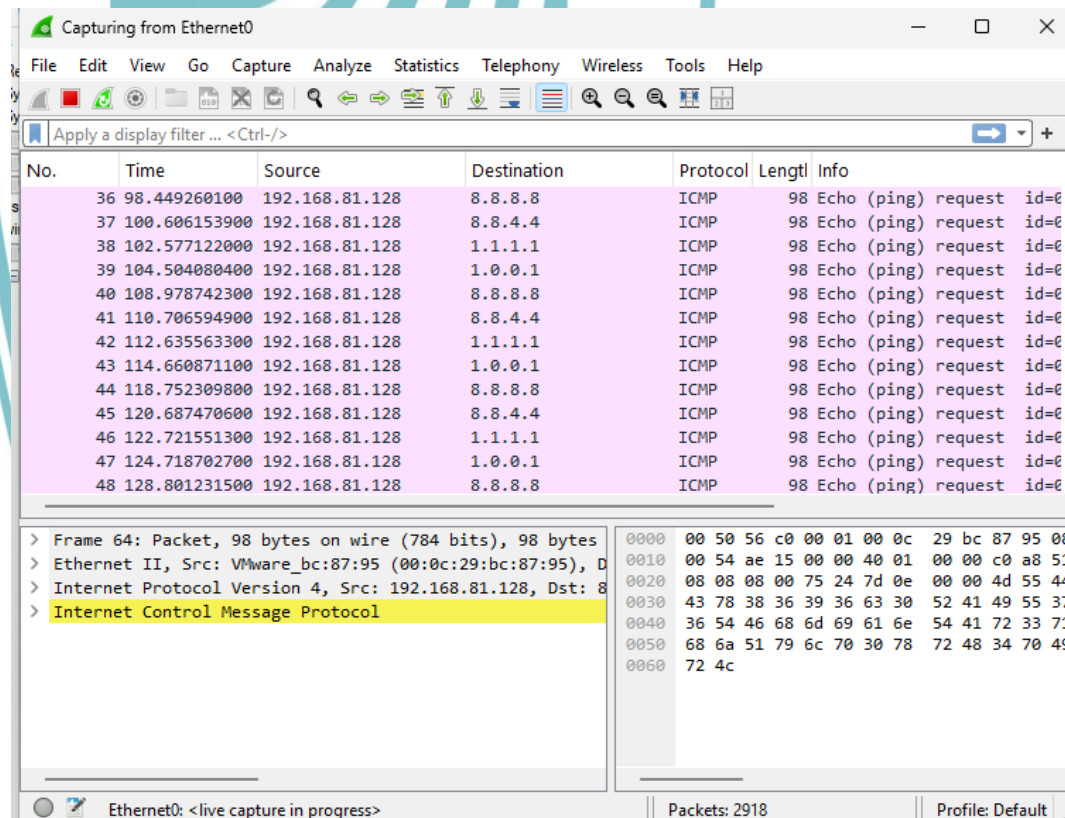
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



No.	Time	Source	Destination	Protocol	Length	Info
47	473.500637800	VMware_bc:87:95	VMware_c0:00:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
48	473.501092700	VMware_c0:00:01	VMware_bc:87:95	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
49	501.159475900	192.168.81.1	192.168.81.254	DHCP	358	DHCP Request - Transaction ID 0x6a21cb2d
50	501.180709300	192.168.81.254	192.168.81.1	DHCP	342	DHCP ACK - Transaction ID 0x6a21cb2d
51	501.235212700	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
52	501.235212700	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
53	501.317544600	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
54	501.317544600	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any source
55	501.325910900	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
56	501.325910900	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
57	501.325910900	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
58	501.325910900	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any source
59	501.345175500	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any source
60	501.345175500	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
61	501.765012100	fe80::ba2f:def9:57f...	ff02::1:3	LLMNR	95	Standard query 0xb4a9 ANY DESKTOP-7LEACLO
62	501.765012100	192.168.81.1	224.0.0.252	LLMNR	75	Standard query 0xb4a9 ANY DESKTOP-7LEACLO
63	505.860479500	VMware_c0:00:01	VMware_eb:f9:30	ARP	60	Who has 192.168.81.254? Tell 192.168.81.1
64	505.860479500	VMware_eb:f9:30	VMware_c0:00:01	ARP	60	192.168.81.254 is at 00:50:56:eb:f9:30
65	514.003958700	VMware_bc:87:95	VMware_c0:00:01	ARP	42	Who has 192.168.81.1? Tell 192.168.81.128
66	514.005000000	VMware_c0:00:01	VMware_bc:87:95	ARP	60	192.168.81.1 is at 00:50:56:c0:00:01
67	548.405091400	fe80::ba2f:def9:57f...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

> Frame 50: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{6EFC487-5DDF-408F-9353-C66} ...
 > Ethernet II, Src: VMware_eb:f9:30 (00:50:56:eb:f9:30), Dst: VMware_c0:00:01 (00:50:56:c0:00:01)
 > Internet Protocol Version 4, Src: 192.168.81.254, Dst: 192.168.81.1
 > User Datagram Protocol, Src Port: 67, Dst Port: 68
 > Dynamic Host Configuration Protocol (ACK)

Lampiran 30 Tampilan analisis Wireshark pada sampel 3 (bagian 2)



No.	Time	Source	Destination	Protocol	Length	Info
36	98.449260100	192.168.81.128	8.8.8.8	ICMP	98	Echo (ping) request id=0
37	100.606153900	192.168.81.128	8.8.4.4	ICMP	98	Echo (ping) request id=0
38	102.577122000	192.168.81.128	1.1.1.1	ICMP	98	Echo (ping) request id=0
39	104.504080400	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request id=0
40	108.978742300	192.168.81.128	8.8.8.8	ICMP	98	Echo (ping) request id=0
41	110.706594900	192.168.81.128	8.8.4.4	ICMP	98	Echo (ping) request id=0
42	112.635563300	192.168.81.128	1.1.1.1	ICMP	98	Echo (ping) request id=0
43	114.660871100	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request id=0
44	118.752309800	192.168.81.128	8.8.8.8	ICMP	98	Echo (ping) request id=0
45	120.687470600	192.168.81.128	8.8.4.4	ICMP	98	Echo (ping) request id=0
46	122.721551300	192.168.81.128	1.1.1.1	ICMP	98	Echo (ping) request id=0
47	124.718702700	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request id=0
48	128.801231500	192.168.81.128	8.8.8.8	ICMP	98	Echo (ping) request id=0

> Frame 64: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ...
 > Ethernet II, Src: VMware_bc:87:95 (00:0c:29:bc:87:95), Dst: VMware_c0:00:01 (00:50:56:c0:00:01)
 > Internet Protocol Version 4, Src: 192.168.81.128, Dst: 8.8.8.8
 > Internet Control Message Protocol

Ethernet0: <live capture in progress> | Packets: 2918 | Profile: Default

Lampiran 31 Tampilan analisis Wireshark pada sampel 4 (bagian 1)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun
- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

No.	Time	Source	Destination	Protocol	Length	Info
281	687.362835000	192.168.81.1	192.168.81.254	DHCP	352	DHCP Request - Transaction ID 0ba6ff04c1
282	687.363035000	192.168.81.254	192.168.81.1	DHCP	342	DHCP ACK - Transaction ID 0ba6ff04c1
283	687.411852400	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
284	687.411852400	192.168.81.1	224.0.0.252	IGMPv3	60	Membership Report / Leave group 224.0.0.252
285	687.428634000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
286	687.587570000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.22 for any sources
287	687.510375000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
288	687.516660000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.22
289	687.517801000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
290	687.518264000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
291	687.533331000	fd8b::ba2f:df9:57f::	ff02::1:1:3	LWMR	95	Standard query 0ba7711 ANY DESKTOP-ZLEACLO
292	687.533331000	192.168.81.1	224.0.0.252	LWMR	75	Standard query 0ba7711 ANY DESKTOP-ZLEACLO
293	687.796234000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
294	687.796234000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
295	687.953555000	fd8b::ba2f:df9:57f::	ff02::1:1:3	LWMR	95	Standard query 0ba7711 ANY DESKTOP-ZLEACLO
296	687.953555000	192.168.81.1	224.0.0.252	LWMR	75	Standard query 0ba7711 ANY DESKTOP-ZLEACLO
297	689.522848000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
298	689.522848000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
299	689.537953000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
300	689.597730000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
301	689.610130700	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
302	689.610130700	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
303	689.612122000	fd8b::ba2f:df9:57f::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
304	689.612122000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
305	689.617463000	fd8b::ba2f:df9:57f::	ff02::1:1:3	LWMR	95	Standard query 0ba7711 ANY DESKTOP-ZLEACLO
306	689.617463000	192.168.81.1	224.0.0.252	LWMR	75	Standard query 0ba7711 ANY DESKTOP-ZLEACLO
307	689.613601000	192.168.81.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
Frame 553: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface UDevice\NPF_{6E7CC687-5D0F-408F-9353-C6E7C8D02F17}, Id 0						
Ethernet II, Src: VMware_b8:27:95 (08:0c:29:bc:87:95), Dst: VMware_c8:00:01 (00:50:56:c8:00:01)						
Destination: VMware_b8:27:95 (08:0c:29:bc:87:95)						
Source: VMware_c8:00:01 (00:50:56:c8:00:01)						
Type: IP4 (0x0800)						
[Stream index: 0]						
Internet Protocol Version 4, Src: 192.168.81.128, Dst: 1.1.1.1						
Internet Control Message Protocol						
0000 00 50 56 c8 00 01 00 0c 29 bc 87 95 08 00 45 00 PVE						
0010 00 54 4e 04 00 00 00 01 00 00 c8 a8 51 00 01 03 T...@...Q						
0020 03 01 00 00 02 a1 7d 0e 00 00 00 31 78 63 42 53KIGRS						
0030 31 77 55 50 6d 31 65 52 05 44 67 39 48 6d 73 38 sdpMstet dgmw6d						
0040 56 50 54 4e 4e 43 59 7d 51 4f 4a 55 32 63 37 v8MPCNv qG2G2C7						
0050 63 35 71 72 4e 46 54 38 03 62 60 36 49 33 56 6f c8RfPtet abk23V0						
0060 4f 34 04						

Lampiran 32 Tampilan analisis Wireshark pada sampel 4 (bagian 2)

No.	Time	Source	Destination	Protocol	Length	Info
267	483.548842700	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
271	493.124473700	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
277	503.340071700	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
281	513.612615100	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
285	523.999893300	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
289	534.184200000	192.168.81.128	1.0.0.1	ICMP, -	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found) (SendTTL=65, Round=54)
293	544.123218000	192.168.81.128	1.0.0.1	ICMP, -	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found) (SendTTL=95, Round=104)
297	554.240435000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
301	565.131950000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
305	575.516284200	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
309	585.905601000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
313	596.701561000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
317	609.322848000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
321	635.810361000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
325	642.434868000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
329	674.234639000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
333	684.914717000	192.168.81.128	1.0.0.1	ICMP, -	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found) (SendTTL=48, Round=73)
336	695.031345000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
339	706.419232000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
342	717.002925000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
346	735.150965700	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
376	745.202012000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
378	755.330200000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
379	765.335243000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
382	775.640730000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
386	785.527668000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
398	795.680613000	192.168.81.128	1.0.0.1	ICMP	98	Echo (ping) request Id=0x70be, seq=0/0, ttl=64 (no response found)
Frame 267: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface UDevice\NPF_{6E7CC687-5D0F-408F-9353-C6E7C8D02F17}, Id 0						
Ethernet II, Src: VMware_b8:27:95 (08:0c:29:bc:87:95), Dst: VMware_c8:00:01 (00:50:56:c8:00:01)						
Internet Protocol Version 4, Src: 192.168.81.128, Dst: 1.0.0.1						
Internet Control Message Protocol						
0000 00 50 56 c8 00 01 00 0c 29 bc 87 95 08 00 45 00 PVE						
0010 00 54 4e 34 00 00 00 01 00 00 c8 a8 51 00 01 00 T...@...Q						
0020 00 01 00 00 21 dc 7d 0e 00 00 49 55 7d 34 50 6aI...UN4P3						
0030 6d 78 68 64 45 66 45 67 57 72 64 72 79 53 35 52 whdPstet indryy5d						
0040 50 6e 42 71 53 55 6c 68 77 58 31 41 75 0b 34 57 PndG5U1t wZLdW7U						
0050 66 4d 70 50 40 72 34 49 38 58 31 35 4a 6a 6a 4f fPpKr4t 0X15J3JO						
0060 4c 34						

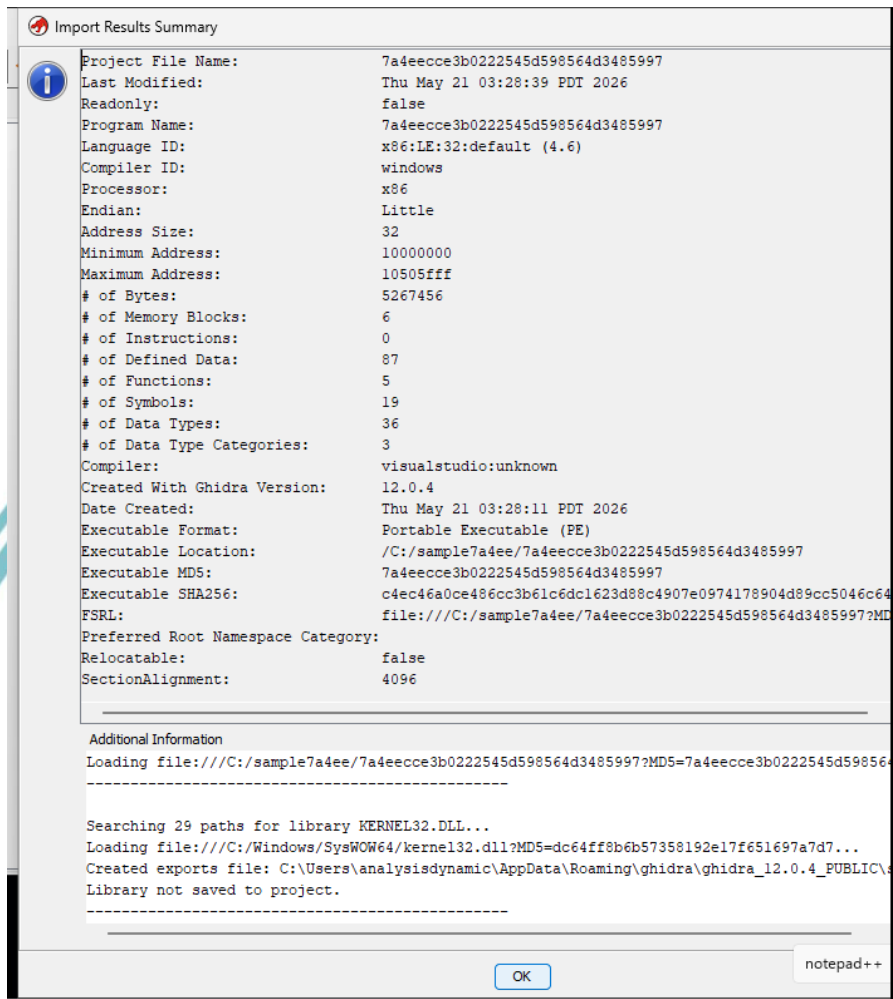
Activate Windows
Go to Settings to activate Windows.

Lampiran 33 Tampilan analisis Wireshark pada sampel 5



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

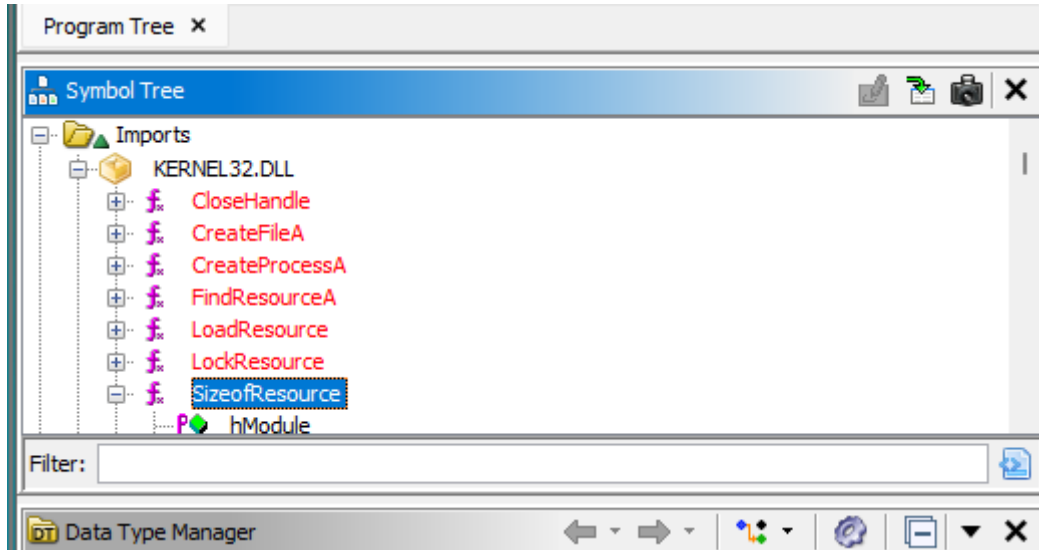


Lampiran 34 Tampilan daftar fungsi pada sampel 1

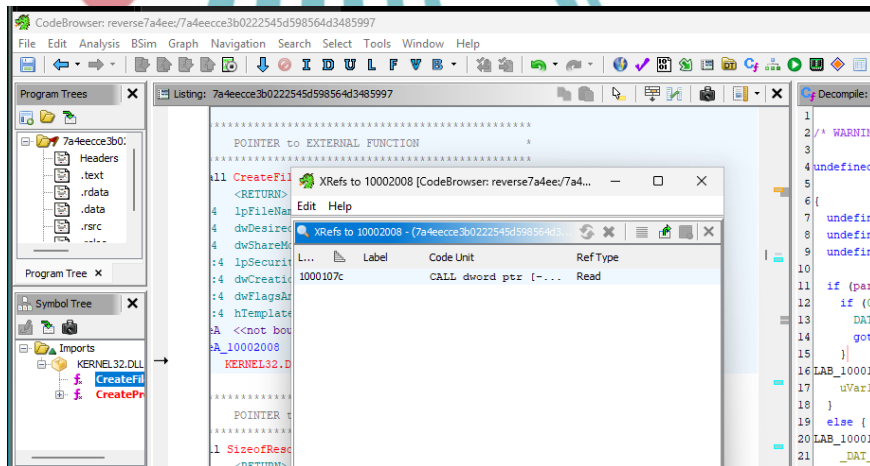
POLITEKNIK
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 35 Tampilan Symbol Tree pada sampel 1

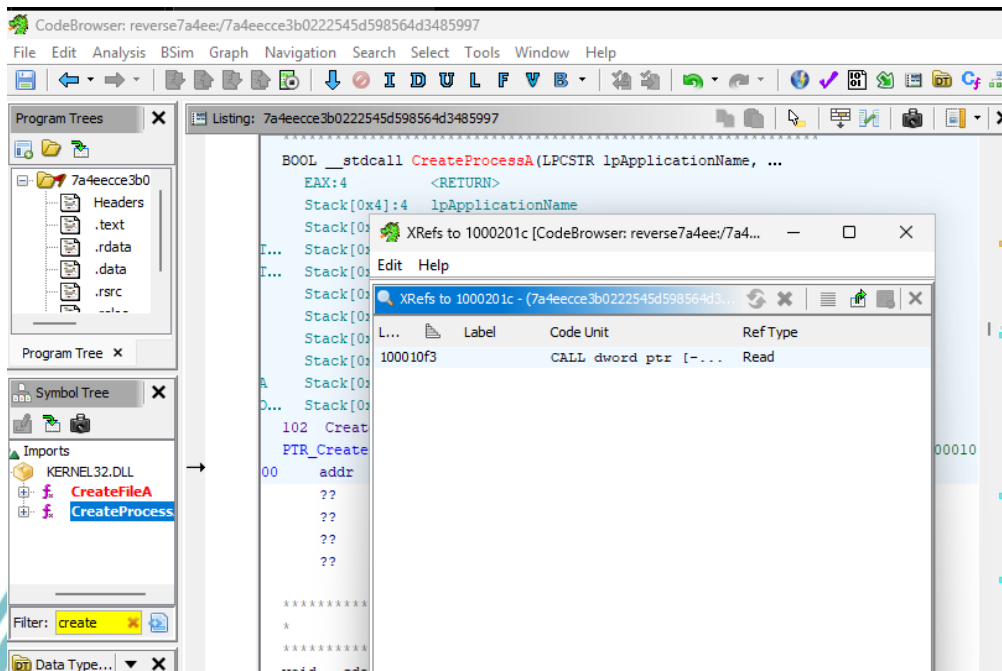


Lampiran 36 Tampilan Cross-Reference (XRefs) pada sampel 1

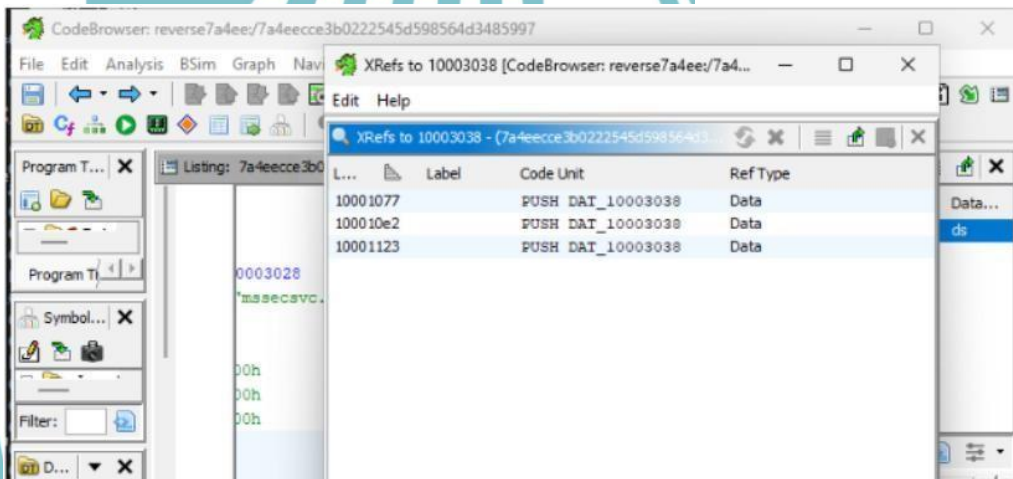


Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 37 Tampilan fungsi CreateProcessA pada sampel 1

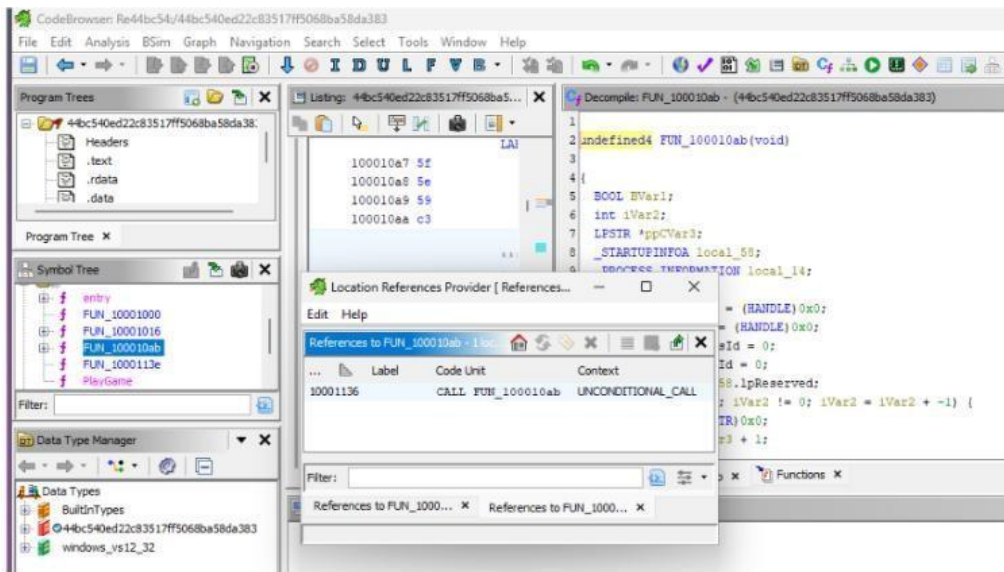


Lampiran 38 Tampilan DAT_10003038 pada sampel 1

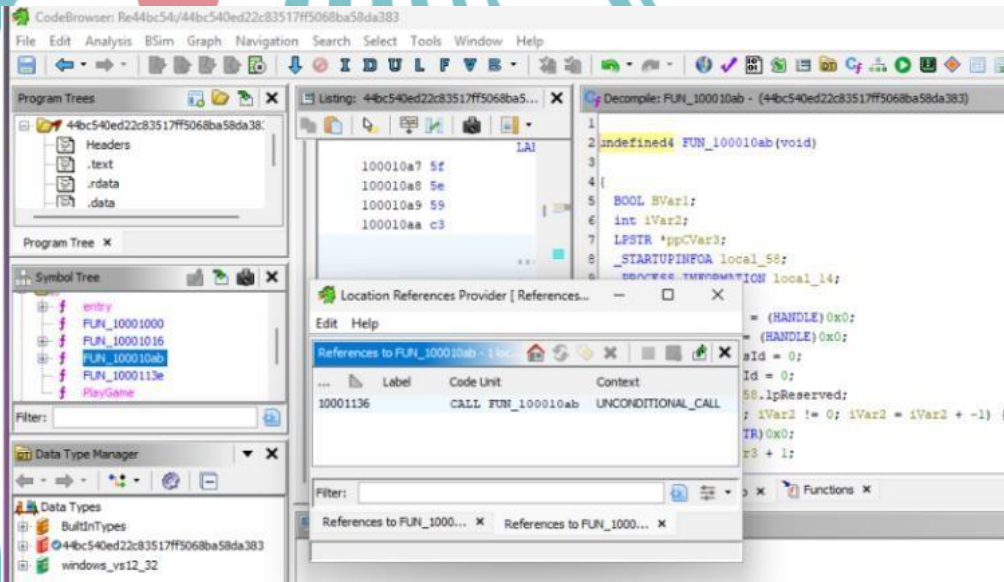
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



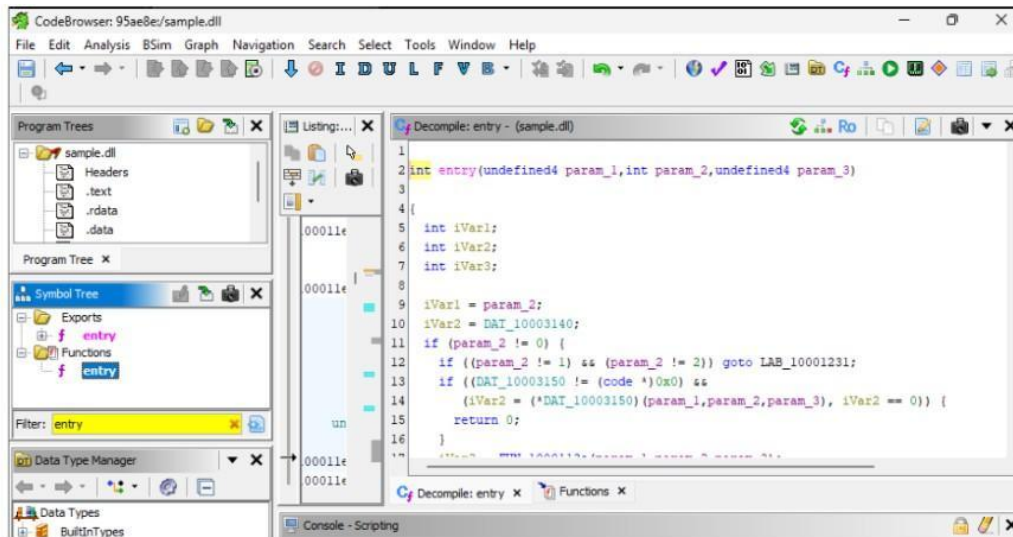
Lampiran 39 Tampilan perintah eksekusi cmd.exe pada sampel 2



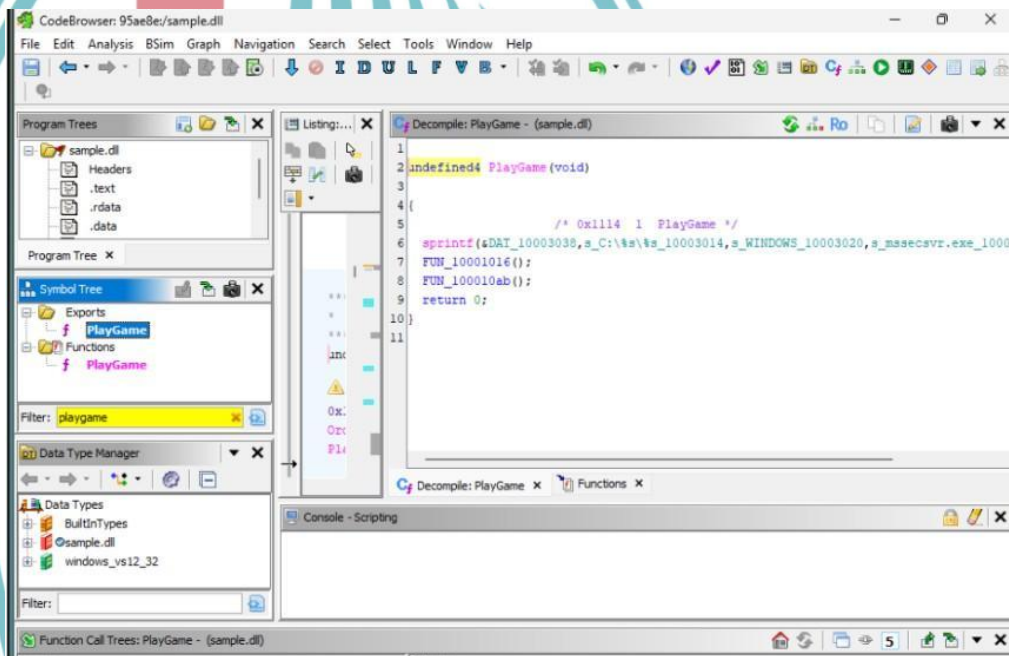
Lampiran 40 mpilan strings parameter layanan pada sampel 2

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



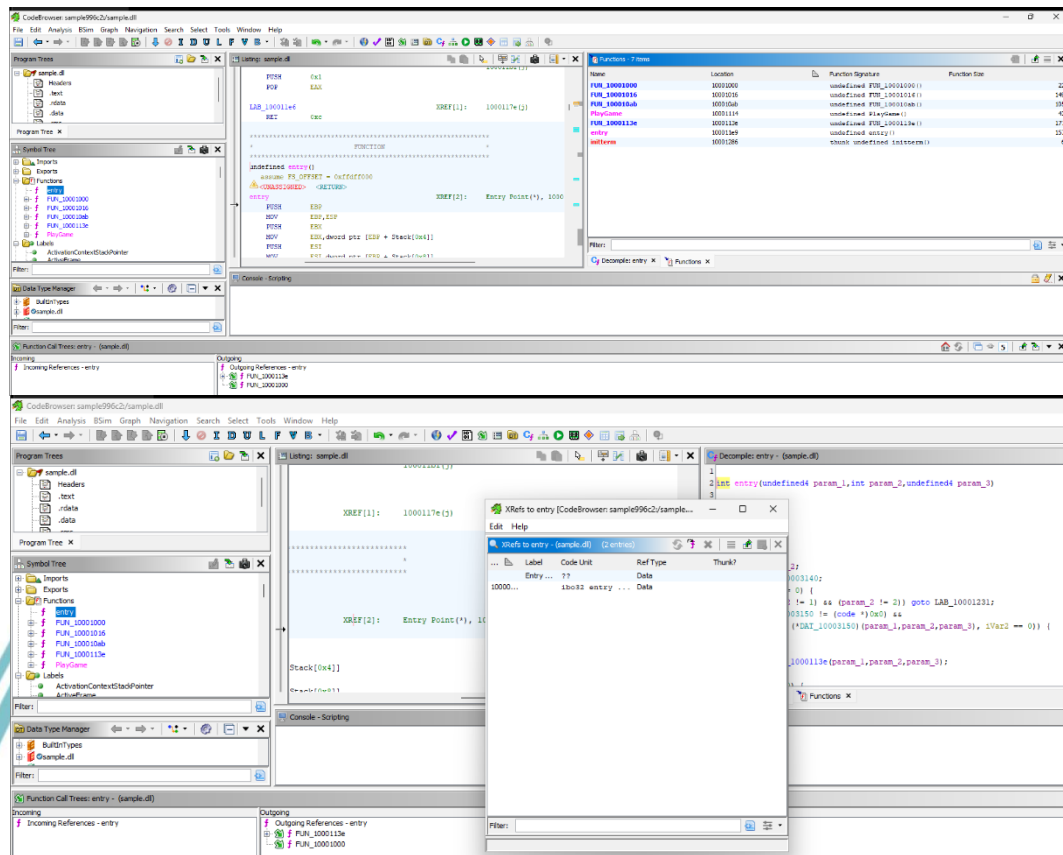
Lampiran 41 Tampilan decompile pada sampel 3



Lampiran 42 Tampilan decompile pada sampel 4

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 43 Tampilan Ghidra pada sampel 5

**POLITEKNIK
NEGERI
JAKARTA**