ANALISIS *MALWARE* MENGGUNAKAN METODE *STATIC ANALYSIS* PADA JARINGAN UNIVERSITAS TANJUNGPURA

SKRIPSI

Program Studi Sarjana Informatika
Jurusan Informatika

Oleh:
YOGA NURDIANSYAH
NIM D1041191038

FAKULTAS TEKNIK
UNIVERSITAS TANJUNGPURA
PONTIANAK
2025

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

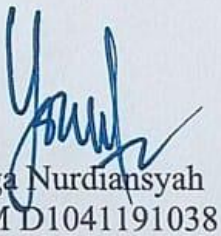
Nama : Yoga Nurdiansyah

NIM : D141191038

menyatakan bahwa dalam skripsi yang berjudul "Analisis *Malware* Menggunakan Metode *Static Analysis* Pada Jaringan Universitas Tanjungpura" tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi manapun. Sepanjang pengetahuan Saya, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Demikian pernyataan ini dibuat dengan sebenar-benarnya. Saya sanggup menerima konsekuensi akademis dan hukum di kemudian hari apabila pernyataan yang dibuat ini tidak benar.

Pontianak, 10 Juni 2025



Yoga Nurdiansyah
NIM D1041191038

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS TANJUNGPURA
FAKULTAS TEKNIK
Jalan Prof. Dr. H. Hadari Nawawi Pontianak 78124
Telepon (0561) 740186, WA: +6282152280907
Email : ft@untan.ac.id Website : http://teknik.untan.ac.id

HALAMAN PENGESAHAN

ANALISIS *MALWARE* MENGGUNAKAN METODE *STATIC ANALYSIS* PADA JARINGAN UNIVERSITAS TANJUNGURA

Program Studi Sarjana Informatika
Jurusan Informatika

Oleh:

Yoga Nurdiansyah
NIM D1041191038

Telah dipertahankan di depan Penguji Skripsi pada tanggal 10 Juni 2025
dan diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana.

Susunan Penguji Skripsi:

Ketua,

Haried Novriando, S.Kom., M.Eng.
NIP 198611132020121005

Penguji Utama,

Helfi Nasution, S.Kom., M.Cs.
NIP 197104291998021002

Sekretaris,

Alfian Abdul Jalid, S.Kom., M.Cs.
NIP 199106292022031003

Penguji Pendamping,

Rickhy Artha Octaviyana, S.Kom., M.M., M.Kom.
NIP 199510302024061002

Pontianak, 10 Juni 2025
Dekan,

Dr.-Ing. Ir. Slamet Widodo, M.T., IPM
NIP 196712231992031002

HALAMAN PERSEMBAHAN

بِسْمِ ٱللَّهِ الرَّحْمَنِ الرَّحِيْمِ

Skripsi ini saya dedikasikan sebagai bentuk tanggung jawab saya kepada bapak saya **A.rahman** dan Ibu saya **Fauziah**. Berkat do'a dan motivasi mereka, saya dapat menyelesaikan jenjang pendidikan S1. Terima kasih juga kepada saudari-saudari saya, **Rindy Nursyela** dan **Fathin Nursilqiah** yang selalu memberikan doa dan dukungan serta selalu mengingatkan saya sehingga saya dapat menyelesaikan skripsi ini, semoga kalian dapat melampaui saya dikemudian hari. Tidak lupa pula saya ucapkan terima kasih kepada **cinta pertama dan terakhir saya** yang selalu mendo'akan saya agar selalu sukses dalam menghadapi urusan saya. Serta terima kasih saya ucapkan kepada teman-teman **Angkatan 2019** dan **Anteiku Culture** yang selalu menyertai dan membantu saya selama proses perkuliahan ini, semoga kita semua menjadi orang yang sukses dan bermartabat. Tidak lupa pula sedikit pesan untuk teman-teman yang membaca tulisan ini suatu hari nanti :

"Skripsi yang baik adalah skripsi yang selesai"

☺ Yoga Nurdiansyah ☺

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Allah SWT. Tuhan Yang Maha Esa atas Rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis *Malware* Menggunakan Metode *Static Analysis* Pada Jaringan Universitas Tanjungpura" yang mana penulisan skripsi ini merupakan syarat untuk memperolah gelar Sarjana Komputer (S.Kom.) pada Program Studi Informatika Fakultas Teknik Universitas Tanjungpura Pontianak.

Dalam penulisan skripsi ini, peneliti mendapatkan bantuan dari berbagai pihak, sehingga peneliti ingin mengucapkan ribuan terima kasih kepada Dosen Pembimbing Utama, Bapak Haried Novriando, S.Kom., M.Kom. dan kepada Dosen Pembimbing Pendamping, Bapak Alfian Abdul Jalil, S.Kom., M.Cs. yang telah memberikan penulis kesempatan dan selalu mengingatkan untuk menyelesaikan skripsi ini telah memberikan bimbingan dan motivasi sehingga peneliti dapat menyelesaikan skripsi ini,

Penulis juga mengucapkan terima kasih kepada Dosen Penguji Utama, Bapak Helfi Nasution, S.Kom., M.Cs. dan Dosen Penguji Pendamping, Rickhy Artha Octaviyana, S.Kom., M.M., M.Kom. yang telah memberikan kritik dan saran dalam pengerjaan dan penulisan skripsi ini, serta penulis mengucapkan terima kasih kepada UPT TIK Universitas Tanjungpura atas bantuan-bantuan yang telah diberikan, tidak lupa pula peneliti mengucapkan banyak terima kasih kepada orang tua dan keluarga serta teman-teman yang selalu memberikan motivasi dan doa selama proses perkuliahan ini.

Dalam penelitian dan penulisan ini, penulis menyadari terdapat banyak kekurangan dan jauh dari kata sempurna sehingga penulis juga mengharapkan banyak masukan dan saran kepada setiap pihak demi menyempurnakan penelitian ini.

Pontianak, 10 Juni 2025
Penulis,

Yoga Nurdiansyah

ABSTRAK

Universitas Tanjungpura merupakan perguruan tinggi yang memiliki peran penting dalam memajukan pendidikan di Kalimantan Barat. Sebagai media pendidikan, Universitas Tanjungpura tentunya memiliki sebuah layanan informasi di internet yang dapat di akses dari berbagai kalangan untuk membantu penyebaran informasi yang ada di Universitas Tanjungpura. Dengan akses yang mudah dan skala traffic yang besar tentunya membuat jaringan Universitas Tanjungpura menjadi lebih rentan dan berpotensi terhadap *cyber crime* dan serangan *malware*. Untuk menghadapi masalah tersebut, dilakukan penelitian untuk menganalisis *malware* yang ditemukan di Jaringan Universitas Tanjungpura. Penelitian ini akan menggunakan metode static analisis yaitu metode analisis *malware* yang dilakukan dengan melakukan analisis *malware* tanpa mengeksekusi *malware* melainkan melakukan analisis terhadap kode, string dan struktur file yang dapat membantu mengungkapkan informasi tentang jenis, karakterisitik, fungsi, tujuan, dan dampak yang ditimbulkan dari *malware*. Hasil temuan penelitian berdasarkan analisis yang telah dilakukan yaitu sampel-sampel yang didapat dari UPT TIK Universitas Tanjungpura merupakan *malware* berjenis *backdoor* berdasarkan struktur kode dan fungsionalnya. *Malware backdoor* memungkinkan penyerang memiliki akses tidak sah ke dalam sistem yang dimiliki Universitas Tanjungpura. Akses yang dimiliki penyerang memungkinkan penyerang untuk dapat mengolah file, mengunduh file, menyimpan file, dan eksekusi file berbahaya di dalam server milik Universitas Tanjungpura.

Kata kunci: *malware, static analysis,* jaringan.

ABSTRACT

Tanjungpura University is a college that have an importance role in advancing education in West Kalimantan. As an educational medium, Tanjungpura University certainly has an information service on the internet *that can be accessed by various groups to help disseminate information at Tanjungpura University. With easy access and large traffic scale certainly makes the Tanjungpura University network more vulnerable and has the potential for cyber crime and malware attack. To deal with this problem, research was conducted to analyze malware that found on the Tanjungpura University network. This research will use the static analysis method, which is a malware analysis technique conducted without executing the malware. Instead, it involves analyzing the code, strings, and file structure to reveal information about the type, characteristics, functions, objectives, and potential impact of the malware. The research findings based on the analysis conducted indicate that the samples obtained from the UPT TIK of Tanjungpura University are classified as backdoor malware based on their code structure and functionality. Backdoor malware allows attackers to gain unauthorized access to the system owned by Tanjungpura University. The access gained by the attacker allows them to manipulate files, download files, store files, and execute malicious files on Tanjungpura University's server.*

Keywords : malware, static analysis, network

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan zaman yang semakin maju, manusia tidak dapat dipisahkan dengan penggunaan internet dalam berbagai hal. Internet menjadi sarana umum yang digunakan manusia pada masa ini untuk memudahkan manusia dalam mencari melakukan berbagai hal seperti penyebaran dan pencarian informasi, media komunikasi, media hiburan, media pendidikan. Internet dapat digunakan berbagai kalangan karena sifatnya yang dapat diakses oleh siapa saja tanpa batas wilayah (global). Menurut (Susana & Suarna, 2022) Internet adalah singkatan dari *Interconnected Networking* yang apabila diartikan dalam Bahasa Indonesia berarti rangkaian komputer yang terhubung di dalam beberapa rangkaian jaringan. Menurut KBBI, Internet merupakan jaringan komunikasi elektronik yang menghubungkan jaringan komputer dan fasilitas komputer yang terorganisasi di seluruh dunia melalui telepon atau satelit.

Dengan mudahnya penggunaan internet dimasa ini membuat beberapa golongan orang ataupun individu tergerak dalam melakukan *cyber crime* untuk keuntungan sendiri dan berdampak buruk bagi orang lain. Salah satu *cyber crime* yang umum terjadi di-internet yaitu penyebaran *malware. Malware* merupakan *software* yang diciptakan pembuatnya untuk melakukan sebuah tindakan kejahatan *cyber* seperti pencurian data dan merusak sistem. Menurut (Sianipar & Pangaribuan, 2023) *Malware* merupakan perangkat lunak atau *Software* yang diciptakan untuk meretas atau merusak sistem komputer. *Malware* dapat ditemukan di berbagai tempat dan dapat menyusupi perangkat dengan beberapa cara, terutama dengan adanya aktivitas internet dan pertukaran data yang luas. *Malware* dapat memberikan dampak negatif tergantung dari jenisnya. Beberapa contoh dari jenis-jenis *malware* yaitu *Virus, Trojan, Ransomware, Adware, Worms*, *backdoor* dan lain-lain. Menurut Menurut data yang dipaparkan Slamet Aji Pamungkas yang merupakan Deputi Bidang Keamanan Siber dan Sandi Perekonomian BSSN pada (artikel tertanggal 16/05/2024 diakses tanggal 28/10/2024), terdapat total 74.696.163 anomali trafik pada periode 1 Januari hingga 6 Mei 2024. Sebanyak 44.637.929 atau 59,76 persen anomali tersebut teridentifikasi sebagai aktivitas

malware. Kemudian, sebanyak 13.084.948 atau 17,52 persen anomali tersebut terdeteksi sebagai aktivitas trojan (CNN Indonesia, 2024).

Sebagai salah satu perguruan tinggi di Kalimantan Barat, Universitas Tanjungpura merupakan perguruan tinggi yang memiliki peran penting dalam memajukan pendidikan di Kalimantan Barat. Sebagai lembaga pendidikan, Universitas Tanjungpura tentunya memiliki sebuah layanan informasi di internet yang dapat di akses dari berbagai kalangan untuk membantu penyebaran informasi yang ada di Universitas Tanjungpura. Dengan akses yang mudah dan skala *traffic* yang besar tentunya membuat jaringan Universitas Tanjungpura menjadi lebih rentan dan berpotensi terhadap *cyber crime* dan serangan *malware*. Ancaman ini berpotensi mengganggu keamanan data dan operasional Universitas Tanjungpura. Oleh karena itu, universitas perlu meningkatkan keamanan jaringan untuk melindungi informasi dan sistemnya.

Berdasarkan pemaparan dari admin UPT TIK Universitas Tanjungpura, perlindungan jaringan di Universitas Tanjungpura menggunakan *firewall* untuk meningkatkan keamanan sistemnya. Pada lapisan pertama, UPT TIK Universitas Tanjungpura menggunakan fortigate. Sementara itu untuk lapisan selanjutnya menggunakan hosting immunify360 dan ModSecurity. Selain itu pada *firewall* tipe VPS menggunakan UFW untuk distro Ubuntu. Selanjutnya, jika terdapat *malware* yang berhasil lolos dari firewall dan running, untuk kasus hostingan (cPanel) yang memberikan tanda-tanda anomali seperti CPU meningkat pesat, memory (RAM) meningkat pesat, storage tiba-tiba penuh, ataupun bandwidth tiba-tiba melonjak, maka hostingan (cPanel) akan memberikan notifikasi kepada admin hosting.

Menurut (Safela, 2024) pada *website* pontianakpost.jawapos.com (artikel tertanggal 09/07/2024 diakses tanggal 28/10/2024) Universitas Tanjungpura (Untan) Pontianak diduga menjadi korban kejahatan siber berupa pembobolan, dan pencurian data. Bahkan diduga ada sekitar 52 ribu data individu yang telah dibobol, dan dijual secara online. Kasus ini membuat Untan membutuhkan tindakan keamanan yang lebih baik. Peningkatan keamanan sangat diperlukan untuk mencegah serangan siber di masa depan. Dengan demikian, Untan dapat melindungi data dan sistemnya dari ancaman serupa.

Berdasarkan latar belakang yang telah diuraian di atas maka penulis

mengambil topik penelitian dengan judul "Analisis *Malware* Menggunakan Metode *Static Analysis* Pada Jaringan Universitas Tanjungpura". Penelitian ini dilakukan dengan tujuan untuk mengetahui jenis *malware,* karakteristik dan potensi dampak yang dapat ditimbulkan dari *malware* tersebut. Analisis *malware* dapat membantu dalam identifikasi *malware* dan membantu mengetahui potensi dampak yang ditimbulkannya pada *malware.* Metode *static analisis* merupakan metode analisis *malware* yang dilakukan dengan melakukan analisis *malware* tanpa mengeksekusi *malware* melainkan melakukan analisis terhadap kode, *string* dan struktur file yang dapat membantu mengungkapkan informasi tentang jenis, karakterisitik, fungsi, tujuan, dan dampak yang ditimbulkan dari *malware*. Pemilihan metode *static analysis* dilakukan karena metode *static analysis* merupakan metode yang efektif pada *malware* yang dapat dijalankan maupun yang tidak dapat dijalankan di perangkat komputer dan metode ini dijalankan dengan identifikasi kode sehingga dapat mendeteksi teknik-teknik penyembunyian kode seperti packed, *obfuscation* atau enkripsi kode. Dengan penelitian ini, diharapkan Universitas Tanjungpura dapat meningkatkan keamanan jaringannya dan mencegah *cyber crime* di masa depan.

1.2 Perumusan Masalah

Dari uraian latar belakang tersebut, didapatkan beberapa permasalahan :

1. Bagaimana menentukan langkah-langkah dalam melakukan analisis *malware* menggunakan metode *static analysis* pada Universitas Tanjungpura.
2. Bagaimana cara mendapatkan informasi menggunakan metode *static analysis*.

1.3 Tujuan Penelitian

Tujuan dari penelitian yang dilakukan terkait analisis *malware* yang ada di jaringan Universitas Tanjungpura, yaitu:

1. Dapat menentukan langkah-langkah dalam melakukan analisis *malware* menggunakan metode *static analysis* pada Universitas Tanjungpura.
2. Mendapatkan informasi *malware* dari hasil analisis menggunakan metode *static analysis.*

1.4 Pembatasan Masalah

Dalam penelitian yang dilakukan, ada beberapa batasan masalah sebagai aspek penunjang penelitian sebagai berikut :

1. Analisis *malware* hanya menggunakan metode *static analysis*.
2. Sampel yang dianalisis adalah sampel yang didapatkan di Universitas Tanjungpura.

1.5 Sistematika Penulisan

Dalam laporan tugas akhir yang dibuat, pembahasan disajikan oleh penulis dalam 5 bab dengan sistematika penulisan sebagai berikut:

BAB I: PENDAHULUAN

Pada bab ini berisikan tentang latar belakang, perumusan masalah, tujuan penelitian, pembatasan masalah, tujuan penelitian, metodelogi penelitian, dan sistematika penulisan tugas akhir yang dibuat.

BAB II: TINJAUAN PUSTAKA

Pada bab ini berisikan segala landasan teori yang berhubungan dengan penelitian yang akan dilakukan dan berisi acuan dasar penunjang yang berguna dalam pengerjaan tugas akhir ini.

BAB III: METODOLOGI PENELITIAN

Pada bab ini berisikan pembahasan mengenai alat yang digunakan dalam penelitian dan metode yang digunakan dalam kegiatan penelitian.

BAB IV: HASIL DAN ANALISIS

Pada bab ini berisikan pembahasan mengenai langkah-langkah dan proses yang dilakukan dan hasil yang ditemukan dalam penelitian yang dilakukan.

BAB V: KESIMPULAN DAN SARAN

Pada bab ini berisikan pembahasan mengenai uraian hasil yang ditemukan, penarikan kesimpulan, beserta saran yang dapat digunakan untuk membantu hasil penelitian agar menjadi lebih baik dan untuk penelitian selanjutnya yang akan dilakukan.