Jurnal Kesehatan, Sains, dan Teknologi (JAKASAKTI)
Vol. 5, No. 1 April 2026
Available online at https://jurnal.undhirabali.ac.id/index.php/jakasakti/index

Research Article e-ISSN:2963-0940

Effectiveness Analysis of DNS Filtering on Cyberslacking Control

Analisis Efektifitas DNS *Filtering* terhadap Pengendalian *Cyberslacking*

Firmansyah Pipii[1*], Syahrial[2], Rizal Lamusu[3], Irawan Ibrahim[4]

[1,2,3,4]Ilmu Komputer, Universitas Muhammadiyah Gorontalo, Indonesia

(*) Corresponding Author: coroner.firman466@gmail.com

Article info

Keywords:
DNS Filtering, MikroTik, Cyberslacking, Network Security, Confusion Matrix

Abstract

The development of information technology in educational environments has increased internet accessibility to support learning activities, but it has also contributed to cyberslacking behavior, namely the use of the internet for non-academic activities during study hours. This study aims to analyze the effectiveness of MikroTik-based DNS Filtering in controlling access to non-productive websites within educational networks. The research employed a quantitative approach with a quasi-experimental design by comparing network conditions before and after the implementation of DNS Filtering. Additional testing was conducted under Virtual Private Network (VPN) and DNS over HTTPS (DoH) scenarios to identify system limitations. Data analysis was performed using the Confusion Matrix method with evaluation parameters including accuracy, precision, recall, F1-score, and specificity. The results indicate that DNS Filtering effectively blocks access to non-productive websites under normal network conditions with a high level of accuracy without disrupting access to educational resources. The system was also able to classify productive and non-productive websites appropriately based on the implemented filtering rules. However, the effectiveness of the system decreased when users utilized VPN and DoH as bypass methods, indicating the limitations of conventional DNS-based filtering approaches. This study concludes that MikroTik-based DNS Filtering is a lightweight, easy-to-implement, and sufficiently effective solution for controlling cyberslacking in educational environments, although it still requires integration with additional network security methods to improve resistance against bypass techniques.

Kata kunci:
DNS Filtering, MikroTik, Cyberslacking, Keamanan Jaringan, Confusion Matrix

Abstrak

Perkembangan teknologi informasi di lingkungan pendidikan meningkatkan akses internet yang mendukung proses pembelajaran, namun juga memunculkan perilaku *cyberslacking* berupa penggunaan internet untuk aktivitas non-akademik selama jam belajar. Penelitian ini bertujuan menganalisis efektivitas penerapan DNS *Filtering* berbasis MikroTik dalam mengendalikan akses terhadap situs non-produktif pada jaringan pendidikan. Penelitian menggunakan pendekatan kuantitatif dengan desain quasi experiment melalui perbandingan kondisi jaringan sebelum dan sesudah implementasi DNS Filtering. Pengujian juga dilakukan pada skenario penggunaan *Virtual Private Network* (VPN) dan DNS *over* HTTPS (DoH) untuk mengidentifikasi keterbatasan sistem filtering. Analisis data dilakukan menggunakan metode *Confusion Matrix* dengan parameter evaluasi *accuracy*, *precision*, *recall*, F1-*score*, dan

Jurnal Kesehatan, Sains, dan Teknologi (JAKASAKTI)
Vol. 5, No. 1 April 2026
Available online at https://jurnal.undhirabali.ac.id/index.php/jakasakti/index
Research Article e-ISSN:2963-0940

specificity. Hasil penelitian menunjukkan bahwa DNS *Filtering* mampu memblokir akses ke situs non-produktif secara efektif pada kondisi jaringan normal dengan tingkat akurasi yang tinggi tanpa mengganggu akses ke situs pembelajaran. Sistem juga mampu mengklasifikasikan situs produktif dan non-produktif secara tepat berdasarkan aturan filtering yang diterapkan. Namun, efektivitas sistem mengalami penurunan ketika pengguna menggunakan VPN dan DoH sebagai metode *bypass*, yang menunjukkan keterbatasan pendekatan *filtering* berbasis DNS konvensional. Penelitian ini menyimpulkan bahwa DNS *Filtering* berbasis MikroTik merupakan solusi yang ringan, mudah diimplementasikan, dan cukup efektif dalam pengendalian *cyberslacking* di lingkungan pendidikan, meskipun masih memerlukan kombinasi dengan metode keamanan jaringan tambahan untuk meningkatkan ketahanan sistem terhadap teknik *bypass*.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital pada berbagai sektor, termasuk bidang pendidikan. Pemanfaatan internet dalam lingkungan pendidikan saat ini tidak hanya berfungsi sebagai media komunikasi, tetapi juga menjadi sarana utama dalam mendukung proses pembelajaran, akses informasi, pengelolaan administrasi sekolah, serta pengembangan sumber belajar berbasis digital. Integrasi teknologi internet dalam sistem pendidikan memberikan dampak positif terhadap efektivitas dan efisiensi pembelajaran karena peserta didik dapat memperoleh akses pengetahuan secara lebih luas, cepat, dan interaktif. Pemanfaatan teknologi informasi dalam pendidikan juga berperan penting dalam meningkatkan kualitas pembelajaran melalui kemudahan distribusi informasi serta akses terhadap sumber belajar daring (Salim *et al*., 2023).

Meskipun demikian, peningkatan penggunaan internet di lingkungan pendidikan tidak hanya memberikan manfaat, tetapi juga memunculkan berbagai permasalahan baru terkait perilaku penggunaan internet yang tidak sesuai dengan tujuan pembelajaran. Beberapa penelitian sebelumnya menunjukkan bahwa akses internet yang tidak terkontrol di lingkungan pendidikan dapat memicu penyalahgunaan fasilitas jaringan untuk aktivitas non-akademik, seperti penggunaan media sosial, hiburan digital, maupun aktivitas personal lainnya selama jam pembelajaran berlangsung. Salah satu perilaku yang banyak ditemukan adalah *cyberslacking*. *Cyberslacking* merupakan perilaku penggunaan fasilitas internet untuk aktivitas di luar kepentingan akademik selama jam belajar atau jam kerja, seperti mengakses media sosial, menonton video *streaming*, bermain *game online*, membuka situs hiburan, maupun aktivitas personal lainnya yang tidak berkaitan dengan proses pembelajaran. Perilaku tersebut termasuk bentuk penyalahgunaan akses internet yang dapat menurunkan produktivitas, mengganggu konsentrasi belajar, serta mengurangi efektivitas kegiatan akademik (Chrisnatalia *et al*., 2023).

Fenomena *cyberslacking* menjadi perhatian serius karena perkembangan platform digital modern dan media sosial menyebabkan pengguna internet semakin mudah mengakses berbagai layanan hiburan secara *real-time* melalui perangkat yang selalu terhubung dengan internet. Platform seperti TikTok, Instagram, YouTube, dan layanan *streaming* lainnya dirancang menggunakan sistem rekomendasi algoritmik, notifikasi instan, serta fitur *autoplay* yang mampu mempertahankan perhatian pengguna dalam waktu yang lama. Kondisi tersebut meningkatkan potensi distraksi selama proses pembelajaran karena peserta didik dapat dengan mudah beralih dari aktivitas akademik menuju aktivitas hiburan digital tanpa hambatan teknis yang signifikan.

Beberapa penelitian terdahulu juga menunjukkan bahwa penggunaan media sosial dan layanan hiburan digital secara berlebihan selama jam pembelajaran dapat menyebabkan penurunan fokus belajar, berkurangnya keterlibatan peserta didik dalam proses pembelajaran, serta terganggunya konsentrasi terhadap materi yang disampaikan. Selain berdampak pada aspek akademik, aktivitas akses terhadap layanan *streaming* video, media sosial, dan hiburan digital juga berkontribusi terhadap peningkatan konsumsi bandwidth jaringan sekolah. Penggunaan bandwidth yang tidak terkontrol untuk aktivitas non-akademik berpotensi menurunkan kualitas layanan internet, terutama ketika jaringan digunakan secara bersamaan untuk kebutuhan pembelajaran daring seperti *video conference*, akses platform pembelajaran, maupun layanan berbasis *cloud*. Oleh karena itu, diperlukan mekanisme pengendalian akses internet yang mampu membatasi akses terhadap situs non-produktif agar pemanfaatan jaringan di lingkungan pendidikan tetap terfokus pada kegiatan akademik dan proses pembelajaran.

Hasil observasi awal yang dilakukan pada jaringan internet SMP Negeri 1 Tibawa menunjukkan bahwa masih terdapat pengguna jaringan yang mengakses media sosial, layanan *streaming*, dan situs hiburan selama jam pelajaran berlangsung. Aktivitas tersebut menyebabkan penggunaan *bandwidth* jaringan menjadi tidak optimal dan mengganggu stabilitas koneksi internet untuk kegiatan pembelajaran. Kondisi ini menunjukkan bahwa sistem pengendalian akses internet pada jaringan sekolah belum berjalan secara efektif sehingga diperlukan mekanisme *filtering* yang mampu membatasi akses terhadap situs non-produktif.

Pengendalian akses internet pada jaringan komputer dapat dilakukan melalui berbagai metode *filtering*. Salah satu metode yang umum digunakan adalah *filtering* berbasis *firewall* dan *proxy server*. Metode tersebut mampu melakukan pembatasan akses berdasarkan alamat IP, port, maupun domain tertentu. Namun, *filtering* berbasis *firewall* konvensional memiliki keterbatasan karena belum mampu melakukan identifikasi konten secara lebih spesifik terhadap lalu lintas aplikasi *modern* yang menggunakan koneksi terenkripsi HTTPS. Selain itu, implementasi *proxy server* memerlukan sumber daya tambahan dan konfigurasi yang relatif kompleks pada jaringan dengan jumlah pengguna yang besar.

Metode lain yang banyak diterapkan adalah *Deep Packet Inspection* (DPI) dan Layer 7 *Filtering*. *Deep Packet Inspection* bekerja dengan menganalisis isi paket data secara mendalam untuk mengidentifikasi jenis layanan dan aplikasi yang digunakan pengguna jaringan. *Layer 7 Filtering* juga mampu melakukan klasifikasi lalu lintas berdasarkan pola aplikasi tertentu. Meskipun memiliki tingkat pengendalian yang lebih baik, kedua metode tersebut membutuhkan penggunaan sumber daya perangkat yang cukup tinggi sehingga berpotensi menurunkan performa jaringan apabila diterapkan pada perangkat dengan spesifikasi terbatas. Penggunaan metode inspeksi paket juga memiliki keterbatasan terhadap lalu lintas terenkripsi serta dapat menimbulkan isu privasi pengguna (Magnusson, 2024).

Salah satu alternatif pengendalian akses internet yang lebih ringan dan mudah diimplementasikan adalah *DNS Filtering*. *DNS Filtering* merupakan metode pembatasan akses internet dengan memanfaatkan sistem *Domain Name System* (DNS) untuk mengontrol proses resolusi nama domain. Ketika pengguna mencoba mengakses domain yang telah diblokir, sistem DNS akan mengarahkan permintaan tersebut ke alamat tertentu atau menolak proses resolusi domain sehingga situs tidak dapat diakses. Pendekatan ini dinilai lebih efisien karena tidak melakukan inspeksi terhadap keseluruhan isi paket data, sehingga penggunaan sumber daya jaringan menjadi lebih rendah dibandingkan metode filtering lainnya.

Penerapan *DNS Filtering* pada perangkat MikroTik dapat dilakukan melalui fitur *Static DNS* maupun pengaturan *firewall* yang terintegrasi dengan layanan *DNS serve*. MikroTik dipilih karena memiliki kemampuan manajemen jaringan yang cukup lengkap, biaya implementasi yang relatif rendah, serta mudah diterapkan pada lingkungan pendidikan. Selain mendukung filtering domain, MikroTik juga memungkinkan administrator jaringan melakukan pengaturan *bandwidth*, monitoring trafik, serta pengendalian akses pengguna secara terpusat.

Penelitian terdahulu menunjukkan bahwa implementasi *DNS Filtering* mampu meningkatkan efektivitas pengendalian akses internet pada jaringan pendidikan dan perkantoran. Penelitian sebelumnya menunjukkan bahwa *DNS Filtering* efektif dalam memblokir akses terhadap situs hiburan dan media sosial tanpa mengganggu akses terhadap situs akademik (Sharma & Gupta, 2021). Penelitian lain juga menjelaskan bahwa metode filtering berbasis DNS memiliki keunggulan pada efisiensi penggunaan sumber daya jaringan serta kemudahan implementasi dibandingkan metode filtering berbasis inspeksi paket.

Meskipun demikian, perkembangan teknologi keamanan dan privasi internet menyebabkan *DNS Filtering* konvensional memiliki sejumlah keterbatasan. Penggunaan *Virtual Private Network* (VPN) memungkinkan pengguna menyembunyikan lalu lintas jaringan sehingga akses terhadap situs tertentu dapat melewati sistem filtering. Selain itu, teknologi *DNS over HTTPS* (DoH) menyebabkan permintaan DNS dienkripsi melalui protokol HTTPS sehingga proses monitoring dan filtering DNS menjadi lebih sulit dilakukan. Kondisi tersebut menunjukkan bahwa efektivitas *DNS Filtering* masih perlu dianalisis lebih lanjut, khususnya dalam menghadapi teknik *bypass modern* yang digunakan pengguna jaringan.

Penelitian ini bertujuan untuk menganalisis efektivitas penerapan *DNS Filtering* berbasis MikroTik dalam pengendalian *cyberslacking* pada jaringan pendidikan. Pengujian dilakukan melalui pendekatan *quasi experiment* dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi *DNS Filtering*. Evaluasi sistem dilakukan menggunakan metode *Confusion Matrix* dengan *parameter accuracy, precision*, *recall*, *F1-score*, dan *specificity* untuk mengukur tingkat keberhasilan *filtering* terhadap situs produktif dan non-produktif. Pengujian tambahan pada skenario penggunaan VPN dan *DNS over HTTPS* (DoH) dilakukan untuk mengidentifikasi keterbatasan sistem *filtering* terhadap teknik *bypass*. Hasil penelitian diharapkan dapat menjadi referensi dalam pengembangan sistem pengendalian akses internet yang efektif, ringan, dan mudah diterapkan pada lingkungan pendidikan.

METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan desain *quasi experiment* untuk menganalisis efektivitas penerapan *DNS Filtering* dalam pengendalian *cyberslacking* pada jaringan pendidikan. Pendekatan kuantitatif digunakan karena penelitian berfokus pada pengukuran tingkat keberhasilan sistem *filtering* berdasarkan data hasil pengujian jaringan sebelum dan sesudah implementasi *DNS Filtering*. Desain *quasi experiment* diterapkan melalui skenario pengujian yang dilakukan secara langsung pada jaringan sekolah tanpa melakukan randomisasi terhadap subjek penelitian.

Penelitian dilaksanakan pada jaringan internet SMP Negeri 1 Tibawa dengan memanfaatkan perangkat MikroTik sebagai pusat pengelolaan jaringan dan implementasi *DNS Filtering*. Objek penelitian meliputi aktivitas akses internet pengguna jaringan sekolah, khususnya terhadap situs produktif dan non-produktif yang berpotensi

memunculkan perilaku *cyberslacking*. Situs produktif dalam penelitian ini mencakup platform pembelajaran, mesin pencari akademik, dan layanan pendidikan *daring*, sedangkan situs non-produktif meliputi media sosial, layanan *streaming*, dan situs hiburan.

Tahapan penelitian dimulai dengan identifikasi permasalahan jaringan dan observasi awal terhadap pola penggunaan internet pengguna. Tahap berikutnya dilakukan perancangan sistem *DNS Filtering* menggunakan fitur *Static DNS* pada MikroTik untuk membatasi akses terhadap domain tertentu. Setelah konfigurasi sistem selesai dilakukan, pengujian jaringan dilaksanakan melalui dua kondisi, yaitu sebelum dan sesudah implementasi *DNS Filtering*.

Pengujian dilakukan dengan mengakses sejumlah domain yang telah diklasifikasikan sebagai situs produktif dan non-produktif. Pengujian tambahan dilakukan menggunakan *Virtual Private Network* (VPN) dan *DNS over HTTPS* (DoH) untuk mengidentifikasi kemampuan sistem dalam menghadapi teknik *bypass filtering*. Seluruh aktivitas pengujian dicatat dan dianalisis berdasarkan keberhasilan sistem dalam mengizinkan maupun memblokir akses *domain*.

Teknik pengumpulan data dilakukan melalui observasi, dokumentasi konfigurasi jaringan, dan pengujian langsung terhadap akses domain pada jaringan sekolah. Data hasil pengujian kemudian dianalisis menggunakan metode *Confusion Matrix* untuk mengukur tingkat efektivitas sistem *filtering*. Parameter evaluasi yang digunakan meliputi *accuracy*, *precision*, *recall*, *F1-score*, dan *specificity*.

Perhitungan *accuracy* digunakan untuk mengukur tingkat ketepatan sistem dalam melakukan klasifikasi *domain* produktif dan non-produktif. *Precision* digunakan untuk mengetahui tingkat ketepatan sistem dalam memblokir situs non-produktif, sedangkan recall digunakan untuk mengukur kemampuan sistem dalam mendeteksi seluruh situs non-produktif yang diuji. *F1-score* digunakan untuk mengevaluasi keseimbangan antara *precision* dan *recall*, sementara *specificity* digunakan untuk mengukur kemampuan sistem dalam mempertahankan akses terhadap situs produktif.

Nilai *accuracy* dihitung menggunakan perbandingan antara jumlah klasifikasi yang benar dengan keseluruhan data pengujian. *Precision* dihitung berdasarkan proporsi situs non-produktif yang berhasil diblokir secara tepat oleh sistem. *Recall* digunakan untuk mengetahui tingkat keberhasilan sistem dalam mendeteksi seluruh situs non-produktif yang diuji, sedangkan *F1-score* digunakan untuk menunjukkan keseimbangan performa antara *precision* dan *recall*. *Specificity* digunakan untuk mengukur kemampuan sistem dalam mengizinkan akses terhadap situs produktif tanpa mengalami kesalahan blokir.

Pengujian sistem dilakukan menggunakan beberapa perangkat klien yang terhubung pada jaringan sekolah. Setiap perangkat melakukan akses terhadap daftar domain yang telah ditentukan berdasarkan kategori produktif dan non-produktif. Pengujian dilakukan secara berulang pada kondisi normal, kondisi penggunaan VPN, dan kondisi penggunaan *DNS over HTTPS* (DoH). Hasil pengujian kemudian dicatat dalam bentuk true *positive*, *true negative*, *false positive*, dan *false negative* untuk selanjutnya dianalisis menggunakan metode *Confusion Matrix*.

Implementasi DNS *Filtering* pada penelitian ini menggunakan fitur *Static* DNS dan *firewall rule* pada MikroTik untuk mengarahkan domain tertentu menuju alamat IP lokal atau memblokir proses resolusi *domain*. Konfigurasi sistem dilakukan melalui aplikasi Winbox sebagai media administrasi perangkat MikroTik. Selanjutnya dilakukan monitoring terhadap aktivitas akses pengguna untuk memastikan bahwa sistem *filtering* berjalan sesuai aturan yang telah ditentukan.

Analisis hasil penelitian dilakukan dengan membandingkan performa sistem sebelum dan sesudah implementasi DNS *Filtering*. Tingkat efektivitas sistem diukur berdasarkan keberhasilan *filtering* dalam membatasi akses situs non-produktif tanpa

mengganggu akses terhadap situs pembelajaran. Selain itu, analisis juga difokuskan pada identifikasi kelemahan sistem terhadap teknik *bypass* menggunakan VPN dan *DNS over HTTPS* (DoH). Hasil evaluasi tersebut digunakan untuk menentukan tingkat efektivitas DNS *Filtering* berbasis MikroTik sebagai solusi pengendalian *cyberslacking* pada jaringan pendidikan.

HASIL DAN PEMBAHASAN

Hasil

Implementasi DNS *Filtering* pada penelitian ini dilakukan menggunakan perangkat MikroTik sebagai pusat pengelolaan jaringan internet di SMP Negeri 1 Tibawa. Sistem *filtering* dirancang untuk membatasi akses terhadap situs non-produktif yang berpotensi menimbulkan perilaku *cyberslacking* selama jam pembelajaran berlangsung. Konfigurasi *filtering* dilakukan melalui fitur *Static* DNS dan *firewall* rule dengan mekanisme pemblokiran berdasarkan *domain* tertentu yang telah diklasifikasikan sebelumnya.

Tahap awal penelitian dilakukan dengan observasi kondisi jaringan sebelum implementasi DNS *Filtering*. Berdasarkan hasil observasi, pengguna jaringan sekolah masih dapat mengakses berbagai situs non-produktif seperti media sosial, layanan *streaming video*, *game online*, dan situs hiburan lainnya tanpa adanya pembatasan akses. Aktivitas tersebut menyebabkan penggunaan *bandwidth* menjadi tidak terkontrol sehingga memengaruhi stabilitas jaringan internet sekolah. Pada beberapa kondisi, akses terhadap platform pembelajaran daring mengalami penurunan performa akibat tingginya konsumsi *bandwidth* untuk aktivitas non-akademik.

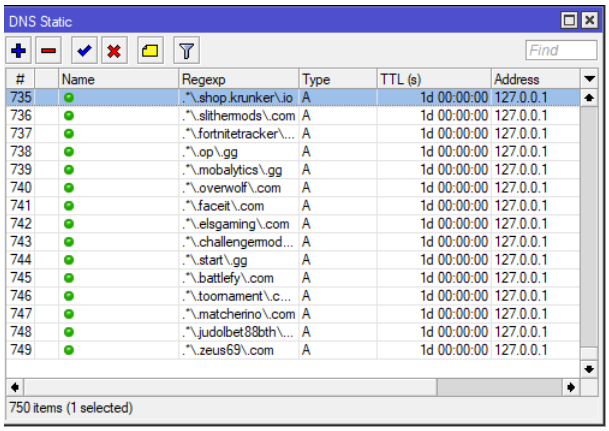
Hasil observasi juga menunjukkan bahwa belum terdapat sistem *filtering* yang mampu melakukan pengendalian akses internet secara spesifik terhadap *domain* tertentu. Kondisi tersebut menyebabkan administrator jaringan mengalami kesulitan dalam membatasi akses pengguna terhadap situs non-produktif selama jam pembelajaran berlangsung.

Setelah dilakukan identifikasi permasalahan jaringan, tahap selanjutnya adalah implementasi DNS *Filtering* menggunakan perangkat MikroTik. Konfigurasi dilakukan melalui pengaturan *Static* DNS dengan metode *redirect* dan *blocking domain*. *Domain* yang dikategorikan sebagai situs non-produktif diarahkan menuju alamat IP lokal sehingga pengguna tidak dapat mengakses situs tujuan.

Selain konfigurasi *Static* DNS, penelitian ini juga menerapkan *firewall rule* untuk memperkuat proses *filtering* dan *monitoring* trafik jaringan. Pengujian konfigurasi dilakukan secara bertahap untuk memastikan bahwa sistem *filtering* berjalan sesuai dengan aturan yang telah dirancang.

Gambar 1 pada penelitian ini diperoleh dari hasil dokumentasi langsung peneliti saat melakukan konfigurasi DNS *Filtering* pada perangkat MikroTik menggunakan aplikasi Winbox. Gambar yang digunakan berupa tangkapan layar (screenshot) konfigurasi *Static* DNS dan *firewall rule* yang diterapkan pada jaringan SMP Negeri 1 Tibawa.

Jurnal Kesehatan, Sains, dan Teknologi (JAKASAKTI)
Vol. 5, No. 1 April 2026
Available online at https://jurnal.undhirabali.ac.id/index.php/jakasakti/index
Research Article e-ISSN:2963-0940



Gambar 1. Daftar Static DNS yang Berisi Domain Non-Produktif
(Sumber: Dokumen Tim Peneliti, 2026)

Pengujian sistem dilakukan menggunakan beberapa perangkat klien yang terhubung pada jaringan sekolah. Setiap perangkat melakukan akses terhadap *domain* yang telah diklasifikasikan menjadi situs produktif dan non-produktif. Pengujian dilakukan pada kondisi sebelum dan sesudah implementasi DNS *Filtering*. Tabel 1 menunjukkan hasil pengujian akses *domain* sebelum dan sesudah implementasi DNS *Filtering*.

Tabel 1. Hasil Pengujian Akses Domain

Kategori Domain	Sebelum Filtering	Sesudah Filtering
Situs Produktif	Dapat diakses	Dapat diakses
Media Sosial	Dapat diakses	Diblokir
Situs Streaming	Dapat diakses	Diblokir
Situs Hiburan	Dapat diakses	Diblokir
Platform Pembelajaran	Dapat diakses	Dapat diakses

Berdasarkan hasil pengujian pada Tabel 1, implementasi DNS *Filtering* berhasil membatasi akses terhadap situs non-produktif tanpa mengganggu akses terhadap platform pembelajaran dan layanan akademik. Situs seperti *YouTube* non-edukatif, *Facebook*, *Instagram*, *TikTok*, dan beberapa layanan *streaming* tidak dapat diakses setelah sistem *filtering* diterapkan. Sebaliknya, akses terhadap *Google Classroom*, situs pencarian akademik, dan platform pembelajaran *daring* tetap berjalan normal.

Hasil tersebut menunjukkan bahwa sistem *filtering* mampu melakukan klasifikasi *domain* sesuai dengan aturan yang diterapkan administrator jaringan. Proses *filtering* juga berjalan secara konsisten pada beberapa perangkat klien yang digunakan selama pengujian.

Pengujian efektivitas sistem dilakukan menggunakan metode *Confusion Matrix* untuk mengukur tingkat keberhasilan *filtering* terhadap *domain* produktif dan non-produktif. Evaluasi dilakukan berdasarkan klasifikasi *true positive*, *true negative*, *false positive*, dan *false negative*.

Tabel 2. Hasil Evaluasi Pengujian Confusion Matrix

Parameter	Hasil
True Positive (TP)	729
True Negative (TN)	749

False Positive (FP)	1
False Negative (FN)	21
Accuracy	98.53%
Precision	99.86%
Recall	97.20%
F1-Score	98.52%
Specificity	99.87%

Hasil evaluasi pada Tabel 2 menunjukkan bahwa sistem DNS *Filtering* memiliki tingkat akurasi sebesar 98.53% dalam mengidentifikasi dan memblokir situs non-produktif. Nilai tersebut menunjukkan bahwa sistem mampu melakukan klasifikasi *domain* dengan tingkat kesalahan yang sangat rendah.

Nilai *precision* sebesar 99.86% menunjukkan bahwa hampir seluruh domain yang diblokir oleh sistem benar-benar termasuk kategori non-produktif. Hal tersebut menunjukkan bahwa sistem *filtering* mampu melakukan pemblokiran secara tepat tanpa banyak menghasilkan kesalahan klasifikasi atau *false positive*.

Nilai *recall* sebesar 97.20% menunjukkan bahwa sebagian besar situs non-produktif berhasil dideteksi dan diblokir oleh sistem DNS *Filtering*. Selain itu, nilai *F1-score* sebesar 98.52% menunjukkan keseimbangan performa sistem antara *precision* dan *recall* sehingga sistem memiliki tingkat konsistensi *filtering* yang tinggi.

Nilai *specificity* sebesar 99.87% menunjukkan bahwa sistem tetap mampu mempertahankan akses terhadap situs produktif tanpa mengalami kesalahan blokir terhadap layanan akademik. Hasil tersebut menunjukkan bahwa implementasi DNS *Filtering* tidak mengganggu akses terhadap platform pembelajaran yang digunakan dalam kegiatan belajar mengajar.

Selama pengujian berlangsung, penelitian ini juga melakukan evaluasi terhadap performa jaringan setelah implementasi DNS *Filtering*. Hasil pengamatan menunjukkan bahwa penggunaan *bandwidth* menjadi lebih stabil dibandingkan kondisi sebelum *filtering* diterapkan. Penurunan akses terhadap situs hiburan dan layanan streaming menyebabkan trafik jaringan menjadi lebih terkontrol sehingga kualitas akses internet untuk kegiatan pembelajaran meningkat.

Selain pengujian pada kondisi normal, penelitian ini juga melakukan pengujian terhadap teknik *bypass* menggunakan *Virtual Private Network* (VPN) dan *DNS over HTTPS* (DoH). Pengujian dilakukan untuk mengetahui tingkat ketahanan sistem *filtering* terhadap lalu lintas jaringan terenkripsi.

Tabel 3. Hasil Pengujian Teknik *Bypass*

Parameter	**VPN**	**DNS over HTTPS (DoH)**
Accuracy	50%	50%
Precision	0%	0%
Recall	0%	0%
F1-Score	0%	0%
Specificity	100%	100%

Hasil pengujian *bypass* pada Tabel 3 menunjukkan bahwa efektivitas DNS *Filtering* mengalami penurunan signifikan ketika pengguna menggunakan VPN dan DNS *over* HTTPS (DoH). Nilai *accuracy* hanya mencapai 50% dengan nilai *precision*, *recall*, dan *F1-score* sebesar 0%. Hasil tersebut menunjukkan bahwa sistem *filtering* tidak mampu

mendeteksi dan memblokir sebagian besar akses terhadap situs non-produktif ketika lalu lintas jaringan dienkripsi menggunakan VPN maupun DoH. Meskipun demikian, nilai *specificity* tetap mencapai 100% karena sistem masih mampu mempertahankan akses terhadap situs produktif tanpa mengalami kesalahan blokir.

Hasil pengujian pada Tabel 3 menunjukkan bahwa penggunaan VPN memungkinkan sebagian akses terhadap situs non-produktif dapat melewati sistem *filtering*. Hal tersebut terjadi karena VPN melakukan *tunneling* lalu lintas jaringan sehingga sistem DNS *Filtering* kesulitan mengidentifikasi *domain* tujuan pengguna.

Pada pengujian menggunakan DNS *over* HTTPS (DoH), efektivitas *filtering* juga mengalami penurunan. Permintaan DNS yang dienkripsi melalui protokol HTTPS menyebabkan sistem *filtering* berbasis DNS konvensional tidak dapat melakukan *monitoring* dan pemblokiran *domain* secara optimal. Meskipun demikian, pada kondisi jaringan normal tanpa penggunaan teknik *bypass*, DNS *Filtering* tetap menunjukkan performa yang stabil dan efektif dalam membatasi akses terhadap situs non-produktif.

Implementasi DNS *Filtering* berbasis MikroTik juga menunjukkan keunggulan dari sisi efisiensi penggunaan sumber daya jaringan. Selama pengujian berlangsung, sistem *filtering* dapat berjalan tanpa memberikan beban berlebih pada perangkat jaringan. Pengelolaan konfigurasi *filtering* relatif mudah dilakukan melalui aplikasi Winbox sehingga administrator jaringan dapat melakukan pembaruan daftar domain secara cepat dan terpusat.

Selain itu, pendekatan *filtering* berbasis DNS tidak memerlukan inspeksi mendalam terhadap paket data sehingga penggunaan CPU dan memori perangkat jaringan tetap stabil selama proses *filtering* berlangsung. Kondisi tersebut menjadikan DNS *Filtering* cocok diterapkan pada lingkungan pendidikan yang memiliki keterbatasan sumber daya perangkat jaringan.

Pembahasan

Implementasi DNS *Filtering* berbasis MikroTik pada penelitian ini menunjukkan bahwa mekanisme *filtering* berbasis DNS mampu menjadi solusi pengendalian *cyberslacking* yang efektif pada lingkungan pendidikan. Sistem *filtering* berhasil membatasi akses terhadap berbagai situs non-produktif seperti media sosial, layanan streaming, game online, dan situs hiburan tanpa mengganggu akses terhadap platform pembelajaran dan layanan akademik. Temuan tersebut menunjukkan bahwa pengendalian akses internet berbasis DNS mampu menciptakan penggunaan jaringan yang lebih terarah dan mendukung proses pembelajaran secara optimal.

Cyberslacking pada lingkungan pendidikan menjadi salah satu permasalahan yang berpengaruh terhadap efektivitas pembelajaran dan performa jaringan internet sekolah. Aktivitas penggunaan internet untuk kepentingan non-akademik selama jam pembelajaran menyebabkan peningkatan konsumsi *bandwidth* dan menurunkan kualitas akses terhadap layanan pembelajaran daring. Kondisi tersebut sesuai dengan pendapat Lim (2002) yang menjelaskan bahwa *cyberslacking* merupakan bentuk penggunaan internet yang tidak berkaitan dengan aktivitas utama organisasi maupun institusi sehingga dapat menurunkan produktivitas.

Pada penelitian ini, implementasi DNS *Filtering* dilakukan melalui konfigurasi *Static* DNS dan *firewall rule* pada perangkat MikroTik. Mekanisme *filtering* bekerja

dengan cara mengontrol proses resolusi domain sebelum pengguna memperoleh akses menuju *server* tujuan. Ketika pengguna mencoba mengakses domain yang telah dikategorikan sebagai situs non-produktif, sistem akan menghentikan proses resolusi DNS sehingga koneksi menuju domain tersebut tidak dapat dilakukan. Mekanisme tersebut menjadikan DNS *Filtering* lebih ringan dibandingkan metode *filtering* berbasis inspeksi paket karena tidak memerlukan analisis terhadap keseluruhan lalu lintas data jaringan.

Hasil penelitian menunjukkan bahwa implementasi DNS *Filtering* memiliki tingkat efektivitas yang sangat tinggi pada kondisi jaringan normal. Berdasarkan hasil evaluasi menggunakan metode Confusion Matrix, sistem memperoleh nilai accuracy sebesar 98.53%, precision sebesar 99.86%, recall sebesar 97.20%, F1-score sebesar 98.52%, dan specificity sebesar 99.87%. Nilai tersebut menunjukkan bahwa sistem *filtering* memiliki kemampuan klasifikasi domain yang sangat baik dalam membedakan situs produktif dan non-produktif.

Nilai accuracy sebesar 98.53% menunjukkan bahwa sebagian besar domain berhasil diklasifikasikan secara benar sesuai kategori yang telah ditentukan administrator jaringan. Tingginya nilai accuracy menunjukkan bahwa sistem *filtering* mampu bekerja secara konsisten dalam mendeteksi dan memblokir domain non-produktif tanpa menghasilkan banyak kesalahan klasifikasi.

Nilai precision sebesar 99.86% menunjukkan bahwa hampir seluruh domain yang diblokir benar-benar termasuk kategori non-produktif. Tingginya precision menunjukkan bahwa sistem memiliki tingkat false positive yang sangat rendah sehingga akses terhadap situs akademik tetap dapat dipertahankan. Kondisi tersebut penting pada lingkungan pendidikan karena kesalahan pemblokiran terhadap platform pembelajaran dapat menghambat proses belajar mengajar.

Nilai recall sebesar 97.20% menunjukkan bahwa sebagian besar situs non-produktif berhasil dideteksi dan diblokir oleh sistem DNS *Filtering*. Selain itu, nilai F1-score sebesar 98.52% menunjukkan bahwa sistem memiliki keseimbangan performa yang sangat baik antara precision dan recall sehingga *filtering* dapat berjalan secara konsisten.

Nilai specificity sebesar 99.87% menunjukkan bahwa sistem tetap mampu mempertahankan akses terhadap situs produktif yang mendukung aktivitas pembelajaran. Hasil tersebut memperlihatkan bahwa implementasi DNS *Filtering* tidak mengganggu akses terhadap platform pembelajaran daring maupun layanan akademik lainnya.

Hasil penelitian ini sejalan dengan penelitian Sharma dan Gupta (2021) yang menyatakan bahwa DNS *Filtering* mampu meningkatkan efektivitas pengendalian akses internet dengan penggunaan sumber daya jaringan yang lebih efisien dibandingkan metode *filtering* berbasis inspeksi paket. Penelitian ini juga mendukung penelitian Magnusson (2024) yang menjelaskan bahwa *filtering* berbasis DNS lebih mudah diterapkan pada jaringan dengan jumlah pengguna yang besar.

Selain efektivitas *filtering*, penelitian ini juga menunjukkan bahwa implementasi DNS *Filtering* memberikan dampak terhadap stabilitas penggunaan *bandwidth* jaringan sekolah. Sebelum *filtering* diterapkan, akses terhadap layanan streaming, media sosial, dan situs hiburan menyebabkan penggunaan *bandwidth* menjadi tidak terkontrol sehingga kualitas akses internet untuk pembelajaran mengalami penurunan. Setelah *filtering* diterapkan, trafik menuju situs non-produktif mengalami penurunan sehingga penggunaan *bandwidth* menjadi lebih stabil dan efisien.

Pengurangan trafik menuju situs hiburan menyebabkan kapasitas jaringan dapat lebih difokuskan untuk mendukung layanan pembelajaran daring dan akses terhadap

sumber belajar digital. Temuan ini mendukung penelitian Salim *et al*. (2023) yang menjelaskan bahwa pengelolaan akses internet yang baik pada lingkungan pendidikan dapat meningkatkan efektivitas pembelajaran dan kualitas penggunaan jaringan.

Implementasi DNS *Filtering* berbasis MikroTik juga menunjukkan keunggulan dari sisi efisiensi penggunaan sumber daya perangkat jaringan. Selama proses pengujian berlangsung, sistem *filtering* dapat berjalan tanpa memberikan beban berlebih terhadap CPU dan memori perangkat MikroTik. Selain itu, administrator jaringan dapat melakukan pembaruan daftar domain secara terpusat melalui aplikasi Winbox sehingga konfigurasi *filtering* menjadi lebih mudah dan fleksibel diterapkan pada institusi pendidikan.

Meskipun menunjukkan tingkat efektivitas yang tinggi pada kondisi jaringan normal, penelitian ini menemukan bahwa DNS *Filtering* memiliki keterbatasan terhadap teknik *bypass modern* seperti Virtual Private Network (VPN) dan DNS over HTTPS (DoH). Hasil pengujian menunjukkan bahwa penggunaan VPN dan DoH menyebabkan nilai accuracy sistem turun menjadi 50%, sedangkan nilai precision, recall, dan F1-score mencapai 0%. Kondisi tersebut menunjukkan bahwa sistem *filtering* tidak mampu mendeteksi dan memblokir sebagian besar akses terhadap situs non-produktif ketika lalu lintas jaringan dienkripsi.

Pada pengujian menggunakan VPN, pengguna masih dapat mengakses situs non-produktif meskipun sistem DNS *Filtering* telah diterapkan. Kondisi tersebut terjadi karena VPN melakukan tunneling lalu lintas jaringan sehingga sistem *filtering* tidak dapat mengidentifikasi domain tujuan pengguna secara langsung. Sementara itu, penggunaan DNS over HTTPS (DoH) menyebabkan permintaan DNS dikirim melalui protokol HTTPS dalam bentuk terenkripsi sehingga proses monitoring DNS tidak dapat dilakukan secara optimal.

Temuan tersebut menunjukkan bahwa implementasi DNS *Filtering* berbasis DNS konvensional masih memiliki keterbatasan dalam menghadapi lalu lintas jaringan terenkripsi. Oleh karena itu, implementasi DNS *Filtering* sebaiknya dikombinasikan dengan metode keamanan jaringan lain seperti *firewall* application control maupun *Deep Packet Inspection* (DPI) untuk meningkatkan efektivitas pengendalian akses internet.

Secara keseluruhan, penelitian ini menunjukkan bahwa DNS *Filtering* berbasis MikroTik dapat menjadi solusi yang ringan, mudah diimplementasikan, dan efisien dalam pengendalian *cyberslacking* pada lingkungan pendidikan. Penelitian ini juga memberikan kontribusi akademik dalam pengembangan kajian keamanan jaringan, khususnya terkait efektivitas DNS *Filtering* dan tantangannya terhadap teknik *bypass modern* seperti VPN dan DNS over HTTPS (DoH).

SIMPULAN

Berdasarkan hasil penelitian, implementasi DNS *Filtering* berbasis MikroTik terbukti efektif dalam mengendalikan perilaku *cyberslacking* pada lingkungan pendidikan. Sistem *filtering* mampu membatasi akses terhadap situs non-produktif seperti media sosial, layanan streaming, dan situs hiburan tanpa mengganggu akses terhadap platform pembelajaran dan layanan akademik. Hasil evaluasi menggunakan metode Confusion Matrix menunjukkan tingkat efektivitas yang tinggi dengan nilai accuracy sebesar 98.53%, precision sebesar 99.86%, recall sebesar 97.20%, F1-score sebesar 98.52%, dan specificity sebesar 99.87%.

Implementasi DNS *Filtering* juga memberikan dampak positif terhadap stabilitas penggunaan *bandwidth* jaringan sekolah. Penurunan akses terhadap situs non-produktif menyebabkan penggunaan *bandwidth* menjadi lebih terkontrol sehingga kualitas akses internet untuk kegiatan pembelajaran meningkat. Selain itu, pendekatan *filtering* berbasis DNS memiliki keunggulan dari sisi efisiensi penggunaan sumber daya perangkat jaringan serta kemudahan konfigurasi dan pengelolaan sistem. Meskipun demikian, penelitian ini menunjukkan bahwa DNS *Filtering* berbasis DNS konvensional masih memiliki keterbatasan dalam menghadapi teknik *bypass modern* seperti *Virtual Private Network* (VPN) dan DNS *over* HTTPS (DoH). Penggunaan VPN dan DoH menyebabkan efektivitas *filtering* mengalami penurunan karena lalu lintas jaringan terenkripsi tidak dapat dimonitor secara optimal oleh sistem *filtering* berbasis DNS.

Secara keseluruhan, DNS *Filtering* berbasis MikroTik dapat menjadi solusi yang ringan, mudah diimplementasikan, dan efisien dalam pengendalian *cyberslacking* pada lingkungan pendidikan. Namun, untuk meningkatkan efektivitas sistem terhadap teknik *bypass modern*, implementasi DNS *Filtering* perlu dikombinasikan dengan metode keamanan jaringan lain seperti *firewall* application control maupun *Deep Packet Inspection* (DPI).

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan selama proses penelitian ini. Ucapan terima kasih disampaikan kepada pihak institusi pendidikan yang telah memberikan izin dan fasilitas selama pelaksanaan penelitian, serta kepada dosen pembimbing yang telah memberikan arahan, masukan, dan dukungan dalam penyusunan penelitian hingga penulisan artikel ilmiah ini. Penulis juga menyampaikan apresiasi kepada seluruh responden dan pihak yang terlibat dalam proses pengujian sistem DNS *Filtering* sehingga penelitian dapat berjalan dengan baik dan lancar.

DAFTAR PUSTAKA

Akbulut, Y. (2016). In search of a measure to investigate cyberloafing in educational settings. *Computers in Human Behavior, 55*, 616–625.

Cheung, C. M. K., Davis, F. D., & Lee, Z. W. Y. (2023). Cyberslacking in the workplace: Antecedents and effects on job performance. *MIS Quarterly, 47*(1), 281–316. https://doi.org/10.25300/MISQ/2022/14985

Chrisnatalia, M., Leoniharza, D., & Liwun, S. B. B. (2023). Self-control dan cyberslacking pada mahasiswa. *Scholaria: Jurnal Pendidikan dan Kebudayaan, 13*(2), 128–137. https://doi.org/10.24246/j.js.2023.v13.i2.p128-137

Dawood, M., *et al*. (2024). The impact of domain name server (DNS) over hypertext transfer protocol secure (HTTPS) on cyber security: Limitations, challenges, and detection techniques. https://doi.org/10.32604/cmc.2024.050049

de Vocht, F., Katikireddi, S. V., McQuire, C., Tilling, K., Hickman, M., & Craig, P. (2021). Conceptualising natural and quasi experiments in public health. *BMC Medical Research Methodology, 21*(1), 1–8. https://doi.org/10.1186/s12874-021-01224-x

Fauzi, H. (2020). Implementasi firewall layer 7 untuk pembatasan akses internet pada laboratorium komputer sekolah. *Jurnal Teknologi dan Sistem Komputer, 8*(3), 123–130.

Haqqini, M. J. A., & Aulia, F. (2025). Peran self-control dan student engagement terhadap cyberslacking pada mahasiswa Universitas Negeri Padang. *Causalita: Journal of Psychology, 2*(3), 326–330. https://doi.org/10.62260/causalita.v2i3.390

Haswad, F. T. H., Akbar, Y., & Asrori, M. U. H. (2025). Pengembangan sistem firewall adaptif berbasis DNS. *Jurnal Teknologi Informasi dan Komunikasi, 9*, 1166–1174.

Islam, S., Hasan, M. M., Sakib, M., & Mazumder, I. (2023). Phishing attack detecting system using DNS and IP filtering. *International Journal of Computer Science, 12*(1), 16–20.

Jerabek, K., Hynek, K., & Rysavy, O. (2024). Comparative analysis of DNS over HTTPS detectors. *Computer Networks, 247*, 110452. https://doi.org/10.1016/j.comnet.2024.110452

Johnson, R. K. S., & Patel, M. (2023). Enhancing network security through DNS filtering: A case study on DrayTek Vigor routers. *Journal of Network Security Management, 7*(2), 75–84.

Kamila Wilujeng, C., & Voutama, A. (2024). Implementasi firewall filter rules sebagai filtering content pada jaringan komputer menggunakan Mikrotik. *JATI (Jurnal Mahasiswa Teknik Informatika), 8*(3), 2680–2685. https://doi.org/10.36040/jati.v8i3.9530

Khormali, A., Park, J., Alasmary, H., Anwar, A., Saad, M., & Mohaisen, D. (2021). Domain name system security and privacy: A contemporary survey. *Computer Networks, 185*. https://doi.org/10.1016/j.comnet.2020.107699

Kim, J., Camtepe, S., Baek, J., Susilo, W., Pieprzyk, J., & Nepal, S. (2021). P2DPI: Practical and privacy-preserving deep packet inspection. *Proceedings of the ACM Asia Conference on Computer and Communications Security*, 135–146. https://doi.org/10.1145/3433210.3437525

Lee, S. K. J. (2020). Evaluation of DNS filtering using diversion on Asus Merlin firmware. *Journal of Network and Computer Applications, 160*.

Magnusson, J. (2024). *Survey and analysis of DNS filtering components*. Retrieved from arXiv

Maesya, A., Sugara, V. I., & Hidayat, A. H. S. (2025). Application of RPZ-based DNS filtering in educational network security. *International Journal of Safety and Security Engineering*.

Markoulidakis, I., & Markoulidakis, G. (2024). Probabilistic confusion matrix: A novel method for machine learning algorithm generalized performance analysis. *Technologies, 12*(7). https://doi.org/10.3390/technologies12070113

Mujiastuti, R., & Prasetyo, I. (2021). Membangun sistem keamanan jaringan berbasis VPN yang terintegrasi dengan DNS filtering Pihole.

Mulyana, D. I., Ardiyansyah, F., Hidayat, N., & Zulfikar, A. (2024). Optimasi keamanan jaringan wifi dari situs judi online dan pornografi dengan DNS filtering dan Orangepi. *MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4*(2), 647–655. https://doi.org/10.57152/malcom.v4i2.1274

Nasir, N., Adetya, S., Yuliana, Y. V., *et al*. (2023). Dampak cyberslacking pada tingkat pembelajaran mahasiswa. *Jurnal Educ, 5*(2), 4624–4632.

Opitz, J. (2024). A closer look at classification evaluation metrics and a critical reflection of common evaluation practice. *Transactions of the Association for Computational Linguistics, 12*, 820–836. https://doi.org/10.1162/tacl_a_00675

Rachmawati, S. A., & Pratikto, H. (2024). Stres akademik dan cyberslacking pada mahasiswa. *Jurnal Psikologi Indonesia, 2*(2), 446–461. Retrieved from Jurnal Psikologi Indonesia

Rahmatia, N., Razak, A., Ahmad, A. T., *et al*. (2024). Smartphone addiction dan perilaku cyberslacking pada mahasiswa. *Jurnal Psikologi Talenta Mahasiswa, 4*(2), 10–19.

Ramdhani, A. I., Subandri, Ramdani, & Anwar, S. (2024). Rancang bangun infrastruktur jaringan dengan metodologi NAT dynamic dan routing open shortest path first. *JUPITER: Jurnal Computer and Information Technology, 5*(2), 70–79. https://doi.org/10.53990/jupiter.v5i2.353

Rusmansyah, R., Mizuardy, H., & Yusuf, B. (2018). DNS filtering: A clean and positive internet environment in UIN Ar-Raniry Banda Aceh. *Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2*(1), 8. https://doi.org/10.22373/cs.v2i1.2502

Salim, A., Afdal, A., Deprizon, Fitri, A., & Wismanto. (2023). Peran manejemen teknologi informasi dan komunikasi dalam dunia pendidikan di era disrupsi. *Journal of Education Research, 4*(3), 1290–1297. Retrieved from Journal of Education Research

Sharma, S. S. A., & Gupta, R. (2021). Effectiveness of Pi-hole DNS filtering in institutional networks. *International Journal of Network Management, 31*(3), 21–23.

Sui, Z., Shu, H., Kang, F., Huang, Y., & Huo, G. (2023). A comprehensive review of tunnel detection on multilayer protocols: From traditional to machine learning approaches. *Applied Sciences, 13*(3). https://doi.org/10.3390/app13031974

Syahputri, C. N., Anggraini, C., Anugerah, H. F., Zufria, I., & Nahwi, M. I. (2023). Penerapan kinerja filter rule dengan metode raw dan layer 7 protocol di router Mikrotik. *Jurnal Kridatama Sains dan Teknologi, 5*(2), 433–447. https://doi.org/10.53863/kst.v5i02.969

Tian, X. (2025). A survey on VPN technologies: Concepts, implementations, and anti-detection strategies. *Journal of Network Security, 13*(1), 85–96.

Wulandari, D., & Assalamiyah, S. (2022). Dampak positif dan negatif penggunaan internet bagi peserta didik. *Jurnal Aksioma Ad-Diniyyah, 10*, 1–8. https://doi.org/10.55171/jad.v10i2.747