



Investigasi Forensik Digital Serangan Brute Force pada Sistem Login Web Menggunakan Metode NIST

Shintya Anggie Syafitri^{1*}, Andy Zulherry²

^{1,2}Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia

Email: ^{1*}anggishintya444@gmail.com, ²andizulherry@umsu.ac.id

Abstrak

dengan mencoba berbagai kombinasi kredensial secara berulang untuk memperoleh akses tidak sah ke suatu akun. Aktivitas tersebut meninggalkan jejak digital pada log server yang berpotensi digunakan sebagai barang bukti dalam proses investigasi forensik. Penelitian ini bertujuan menerapkan metode Digital Forensic National Institute of Standards and Technology (NIST) SP 800-86 untuk menginvestigasi serangan brute force pada sistem login website berbasis PHP melalui analisis log server, meliputi identifikasi dan analisis artefak digital, rekonstruksi kronologi serangan, serta penyusunan laporan investigasi. Penelitian dilaksanakan pada lingkungan localhost menggunakan XAMPP dengan membangun sistem login berbasis PHP dan MySQL, kemudian melakukan simulasi percobaan login berulang secara terkendali sebanyak 500 kali kombinasi kredensial yang menghasilkan 700 permintaan tercatat pada server, terdiri atas 500 autentikasi berhasil dan 200 autentikasi gagal. Proses investigasi mengikuti empat tahapan NIST SP 800-86, yaitu Collection, Examination, Analysis, dan Reporting. Hasil analisis terhadap access.log dan error.log menunjukkan pola percobaan login gagal yang berulang dari alamat IP yang sama terhadap endpoint login yang identik dalam rentang waktu yang berdekatan, diikuti dengan autentikasi yang berhasil dan akses menuju halaman dashboard. Rekonstruksi kronologi menunjukkan keterkaitan yang konsisten antara access.log, error.log, dan hasil pencatatan percobaan login secara langsung. Tahap Reporting menghasilkan laporan investigasi yang memuat identitas kasus, sumber barang bukti digital, hasil pemeriksaan, hasil analisis, serta kronologi aktivitas sebagai dokumentasi forensik terhadap insiden keamanan pada sistem login berbasis web.

Kata Kunci: Forensik Digital, NIST SP 800-86, Brute Force, Access Log, Error Log.

PENDAHULUAN

Perkembangan teknologi informasi mendorong banyak organisasi membangun sistem berbasis website untuk mendukung layanan dan proses bisnisnya, salah satunya melalui mekanisme login sebagai gerbang utama autentikasi pengguna. Mekanisme login yang hanya mengandalkan kombinasi username dan password rentan terhadap berbagai bentuk serangan siber, salah satunya adalah serangan brute force, yaitu upaya memperoleh akses tidak sah dengan mencoba berbagai kombinasi kredensial secara berulang hingga ditemukan kombinasi yang sesuai. Disawal dan Suman (2024) menunjukkan bahwa aplikasi web masih banyak memiliki celah keamanan pada lapisan autentikasi yang dapat dieksploitasi apabila tidak disertai mekanisme pencegahan yang memadai, sementara Sulisnawati dan Subektiningsih (2023) melalui pengujian Open Web Application Security Project (OWASP) pada website institusi pendidikan turut mengonfirmasi bahwa kerentanan pada mekanisme autentikasi menjadi salah satu titik lemah yang paling sering dieksploitasi.

Serangan brute force dapat dideteksi melalui analisis pola aktivitas yang tercatat pada log server. Fachri (2023) membuktikan melalui pengujian penetration testing bahwa pola percobaan login yang berulang dalam rentang waktu singkat dapat diidentifikasi pada log web server dan digunakan sebagai dasar optimasi keamanan. Hal serupa juga ditunjukkan oleh Pamungkas dkk. (2023) yang menganalisis serangan brute force pada perangkat router menggunakan pendekatan National Institute of Standards and Technology (NIST), serta Rustianto dkk. (2025) yang merancang sistem pencegahan dan visualisasi serangan brute force menggunakan Fail2Ban, Prometheus, dan Grafana. Temuan-temuan tersebut menegaskan bahwa log server, khususnya access log dan error log, menyimpan jejak digital yang relevan untuk mengidentifikasi karakteristik aktivitas autentikasi yang mencurigakan.

Jejak digital yang tersimpan pada log server perlu diinterpretasikan secara sistematis agar dapat digunakan sebagai barang bukti yang sah dalam proses investigasi. Horsman (2024) menekankan bahwa

interpretasi jejak digital memerlukan kerangka kerja yang terstruktur agar opini forensik yang dihasilkan dapat dipertanggungjawabkan secara metodologis. Salah satu kerangka kerja yang banyak diadopsi dalam investigasi forensik digital adalah National Institute of Standards and Technology (NIST) Special Publication 800-86, yang terdiri atas empat tahapan, yaitu Collection, Examination, Analysis, dan Reporting. Dasmen dkk. (2024) menerapkan metode tersebut dalam investigasi kasus cyberbullying dan membuktikan efektivitasnya dalam mengekstraksi barang bukti digital secara sistematis, sementara Faizal dan Luthfi (2024) melakukan studi perbandingan antara NIST SP 800-86 dan ISO/IEC 27037 serta menyimpulkan bahwa kedua kerangka kerja tersebut saling melengkapi dalam proses analisis bukti forensik digital.

Penerapan metode NIST SP 800-86 pada konteks analisis log server web juga telah dibuktikan relevansinya oleh beberapa penelitian terdahulu. Pradana Aji dkk. (2023) menganalisis log serangan brute force pada web server Nginx menggunakan sistem logging yang disempurnakan dan metode investigasi forensik, sedangkan Rasyid dan Zen (2023) menerapkan metode NIST 800-86 untuk melakukan dead forensic analysis pada aplikasi peramban Qutebrowser dan LibreWolf. Penelitian forensik digital berbasis NIST juga ditemukan pada lingkup Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS), misalnya Saifani dan Tanjung (2026) yang menerapkan framework NIST SP 800-86 untuk mengidentifikasi dan mengekstraksi artefak digital pada aplikasi GBWhatsApp di perangkat Android, mencakup tahapan collection, examination, analysis, dan reporting hingga menghasilkan sistem pendukung investigasi berbasis web. Penelitian tersebut memperkuat relevansi metode NIST SP 800-86 sebagai kerangka kerja forensik digital yang dapat diadaptasi pada berbagai objek investigasi, termasuk sistem login berbasis website.

Berdasarkan uraian tersebut, penelitian-penelitian terdahulu umumnya berfokus pada deteksi serangan brute force dari sisi pencegahan atau pada penerapan metode NIST untuk objek forensik lain seperti aplikasi perpesanan dan peramban, sedangkan investigasi forensik digital yang secara khusus merekonstruksi kronologi serangan brute force pada sistem login website berbasis PHP melalui korelasi access log dan error log masih terbatas. Penelitian ini bertujuan untuk menerapkan metode Digital Forensic NIST SP 800-86 dalam menginvestigasi serangan brute force pada sistem login website berbasis PHP melalui analisis log server, mengidentifikasi dan menganalisis artefak digital yang dihasilkan, merekonstruksi kronologi serangan secara sistematis, serta menyusun laporan investigasi yang dapat menjadi dokumentasi dan referensi dalam penanganan insiden keamanan serupa.

METODE

Penelitian ini menggunakan pendekatan eksperimental dengan menerapkan metode Digital Forensic National Institute of Standards and Technology (NIST) SP 800-86 untuk menginvestigasi serangan brute force pada sistem login website berbasis PHP. Objek penelitian adalah sistem login berbasis PHP yang dibangun dan dijalankan pada lingkungan localhost menggunakan XAMPP, dengan Apache sebagai web server, PHP sebagai bahasa pemrograman, dan MySQL sebagai sistem manajemen basis data.

Lokasi dan Waktu Penelitian

Penelitian dilaksanakan pada lingkungan pengujian localhost milik peneliti. Simulasi serangan brute force dilakukan pada 24 Agustus 2026 pukul 16:48–17:58 WIB.

Sumber dan Teknik Pengumpulan Data

Data penelitian dikumpulkan dari barang bukti digital yang dihasilkan selama proses implementasi dan simulasi serangan, meliputi access.log dan error.log yang dihasilkan oleh server Apache, log aktivitas login yang mencatat hasil autentikasi, hasil simulasi brute force, hasil pencatatan percobaan login secara langsung, serta dokumentasi tangkapan layar sistem sebagai data pendukung.

Simulasi Serangan Brute Force

Simulasi dilakukan dengan menentukan parameter pengujian terlebih dahulu, meliputi lingkungan localhost, target berupa sistem login berbasis PHP, akun pengguna yang telah terdaftar pada basis data, metode percobaan login berulang menggunakan kombinasi username dan password, serta jumlah percobaan sebanyak 500 kombinasi kredensial. Percobaan login dilakukan secara berulang terhadap halaman login sehingga menghasilkan aktivitas autentikasi yang direkam oleh server, terdiri atas 700 permintaan yang tercatat pada access.log, yakni 500 permintaan dengan autentikasi berhasil dan 200 permintaan dengan autentikasi gagal, dalam rentang waktu pengujian sekitar satu jam sepuluh menit. Informasi sensitif seperti kata sandi akun target tidak ditampilkan secara terbuka dalam dokumentasi penelitian.

Tahapan Investigasi Digital Forensic NIST SP 800-86

Proses investigasi mengikuti empat tahapan NIST SP 800-86. Tahap Collection dilakukan dengan mengidentifikasi dan mengumpulkan seluruh barang bukti digital yang berkaitan dengan aktivitas simulasi, yaitu access.log, error.log, log aktivitas login, hasil simulasi, dan dokumentasi sistem, tanpa melakukan

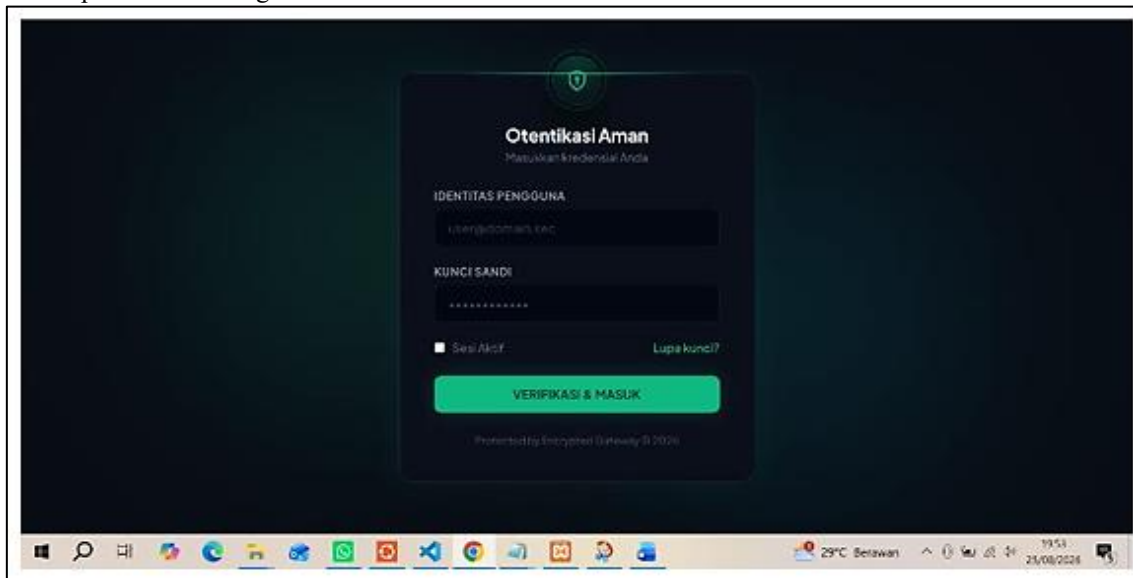
perubahan terhadap data asli. Tahap Examination dilakukan dengan memeriksa dan mengekstraksi informasi relevan dari barang bukti yang telah dikumpulkan, meliputi alamat IP, timestamp, URL yang diakses, metode HTTP, status code, user agent, serta jumlah percobaan login. Tahap Analysis dilakukan dengan menghubungkan dan mengorelasikan informasi hasil pemeriksaan dari access.log dan error.log untuk menentukan pola aktivitas, frekuensi percobaan, serta urutan kejadian yang mengindikasikan karakteristik serangan brute force. Tahap Reporting dilakukan dengan menyusun hasil Collection, Examination, dan Analysis menjadi laporan investigasi yang sistematis, mencakup identitas kasus, sumber barang bukti digital, hasil pemeriksaan, hasil analisis, alamat IP, waktu kejadian, jumlah percobaan, dan kronologi serangan.

Sebagai ilustrasi rinci penerapan keempat tahapan tersebut, dilakukan rekonstruksi kronologi terhadap satu rangkaian aktivitas representatif pada log server, yaitu akses awal menuju halaman login, tiga kali percobaan login gagal yang berasal dari alamat IP dan endpoint yang sama dalam rentang waktu yang berdekatan, kemudian diikuti satu kali autentikasi yang berhasil dan akses menuju halaman dashboard. Rangkaian aktivitas tersebut digunakan untuk menunjukkan secara konkret bagaimana korelasi access.log dan error.log dapat menghasilkan kronologi serangan yang konsisten dengan skenario simulasi yang telah dirancang.

HASIL DAN PEMBAHASAN

Hasil Implementasi Sistem dan Simulasi Serangan

Sistem login berbasis PHP berhasil diimplementasikan pada lingkungan localhost menggunakan XAMPP dengan Apache sebagai web server dan MySQL sebagai basis data. Sistem terdiri atas halaman login, halaman dashboard, serta mekanisme logging yang mencatat setiap aktivitas akses pada access.log dan error.log. Mekanisme autentikasi berjalan sesuai rancangan: kredensial yang sesuai dengan data pada basis data diarahkan menuju dashboard, sedangkan kredensial yang tidak sesuai ditolak dan pengguna tetap berada pada halaman login.



Gambar 1. Tampilan Halaman Login Sistem

Simulasi serangan brute force dilakukan secara terkendali pada lingkungan localhost dengan melakukan percobaan login berulang menggunakan 500 kombinasi kredensial terhadap akun target yang telah terdaftar pada basis data. Proses simulasi menghasilkan 700 permintaan yang tercatat pada access.log dalam rentang waktu pengujian 16:47:32–17:58:22 WIB (sekitar satu jam sepuluh menit lima puluh detik), terdiri atas 500 permintaan dengan autentikasi berhasil dan 200 permintaan dengan autentikasi gagal, sebagaimana dirangkum pada Tabel 1.

Tabel 1. Ringkasan Hasil Simulasi Serangan Brute Force

Parameter	Hasil
Jumlah percobaan login	700
Login berhasil	500
Login gagal	200
Rentang waktu pengujian	16:47:32–17:58:22 (± 1 jam 10 menit 50 detik)
Target endpoint	/nist_forensic/includes/login.php

Sumber: hasil pengolahan access.log dan error.log hasil simulasi (2026)

Hasil Examination terhadap Barang Bukti Digital

Pemeriksaan terhadap access.log mengungkap informasi alamat IP, timestamp, URL, metode HTTP, dan status code dari setiap permintaan, sedangkan pemeriksaan terhadap error.log mengungkap catatan LOGIN_ATTEMPT yang memuat username, alamat IP, dan status autentikasi (failed/success). Hasil pemeriksaan terhadap alamat IP menunjukkan dua sumber aktivitas yang berbeda, sebagaimana dirangkum pada Tabel 2.

Tabel 2. Hasil Pemeriksaan Alamat IP

Alamat IP	Jumlah Aktivitas	Keterangan
127.0.0.1	12	Alamat loopback; akses awal dari lingkungan komputer lokal
172.18.150.182	700	Sumber percobaan login berulang (500 berhasil, 200 gagal)

Sumber: hasil pengolahan access.log (2026)

Temuan ini sejalan dengan Pradana Aji dkk. (2023) yang menunjukkan bahwa access log pada web server dapat diekstraksi menjadi informasi terstruktur berupa alamat IP, timestamp, dan status code guna mengidentifikasi sumber dan pola aktivitas yang mencurigakan. Pemeriksaan terhadap user agent juga menunjukkan bahwa seluruh permintaan percobaan login berasal dari jenis browser yang konsisten, yang menguatkan indikasi bahwa aktivitas tersebut berasal dari satu sumber simulasi yang sama.

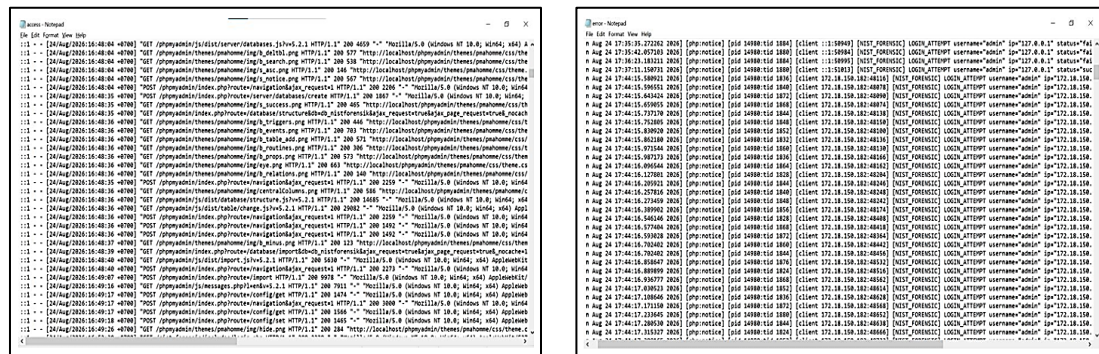
Hasil Analysis dan Rekonstruksi Kronologi

Tahap Analysis menghubungkan informasi dari access.log dan error.log berdasarkan kesesuaian waktu, alamat IP, dan URL untuk menentukan pola aktivitas serta menyusun kronologi kejadian. Sebagai ilustrasi representatif, Tabel 3 menyajikan rekonstruksi kronologi terhadap satu rangkaian aktivitas yang menunjukkan pola percobaan login gagal secara berulang diikuti autentikasi yang berhasil.

Tabel 3. Rekonstruksi Kronologi Aktivitas Simulasi Serangan

No	Waktu	Alamat IP	Aktivitas	Status Code	Keterangan
1	17:34:39	127.0.0.1	Akses halaman login	200	Aktivitas awal
2	17:35:35	172.18.150.182	Percobaan login	302	Login gagal
3	17:35:41	172.18.150.182	Percobaan login	302	Login gagal
4	17:35:42	172.18.150.182	Percobaan login	302	Login gagal
5	17:37:11	172.18.150.182	Akses dashboard	200	Setelah login berhasil

Sumber: korelasi access.log dan error.log hasil simulasi (2026)



Gambar 2. Cuplikan Access Log dan Error Log Hasil Simulasi

Pola aktivitas berupa akses halaman login, diikuti tiga percobaan login gagal yang berasal dari alamat IP dan endpoint yang sama dalam rentang waktu yang relatif berdekatan (± 7 detik), kemudian diikuti autentikasi yang berhasil dan akses menuju dashboard, menunjukkan karakteristik yang konsisten dengan pola serangan brute force sebagaimana dijelaskan oleh Fachri (2023) dan Pamungkas dkk. (2023). Hasil ini juga memperkuat temuan Rasyid dan Zen (2023) yang menegaskan bahwa metode NIST SP 800-86 mampu menyusun kronologi aktivitas secara akurat berdasarkan korelasi berbagai sumber artefak digital. Sejalan dengan Dasmen dkk. (2024) yang menerapkan NIST SP 800-86 pada kasus cyberbullying, penelitian ini membuktikan bahwa kerangka kerja yang sama dapat diaplikasikan pada objek investigasi yang berbeda, yaitu insiden keamanan pada sistem login berbasis web, dengan tetap menghasilkan proses investigasi yang terstruktur mulai dari Collection hingga Reporting.

Sebagaimana ditegaskan oleh Horsman (2024), interpretasi jejak digital tidak dapat didasarkan pada satu indikator tunggal, melainkan harus mempertimbangkan beberapa pilar pendukung agar opini forensik yang dihasilkan dapat dipertanggungjawabkan. Oleh karena itu, penentuan karakteristik brute

force pada penelitian ini tidak hanya didasarkan pada jumlah percobaan, tetapi juga mempertimbangkan pola pengulangan, interval waktu, kesesuaian alamat IP dan URL yang ditargetkan, serta korelasi antara access.log dan error.log. Pendekatan yang sama juga diterapkan oleh Saifani dan Tanjung (2026) dalam penelitian forensik digital pada aplikasi GBWhatsApp yang diterbitkan pada Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS), yang menunjukkan bahwa kerangka kerja NIST SP 800-86 secara konsisten efektif digunakan untuk mengekstraksi dan menganalisis artefak digital pada berbagai jenis objek investigasi, mulai dari aplikasi perpesanan pada perangkat Android hingga, sebagaimana dibuktikan pada penelitian ini, log server pada sistem login berbasis website.

Hasil Reporting dan Implikasi

Tahap Reporting menghasilkan laporan investigasi yang menyajikan identitas kasus, sumber barang bukti digital (access.log, error.log, log aktivitas login, hasil simulasi, dan dokumentasi sistem), hasil pemeriksaan, hasil analisis, alamat IP, waktu kejadian, jumlah percobaan, serta kronologi serangan secara sistematis. Laporan tersebut dapat digunakan sebagai dokumentasi dan referensi dalam menganalisis insiden keamanan serupa pada sistem login berbasis web di lingkungan organisasi yang lebih luas. Temuan ini memperkuat hasil Faizal dan Luthfi (2024) yang menyimpulkan bahwa NIST SP 800-86 unggul dalam memberikan struktur investigasi yang sistematis, sehingga relevan diterapkan pada kasus-kasus yang memerlukan dokumentasi forensik yang dapat dipertanggungjawabkan.

Penelitian ini memiliki keterbatasan karena simulasi dilakukan pada lingkungan localhost yang terkendali dengan sumber log terbatas pada access.log dan error.log, sehingga belum merepresentasikan kompleksitas serangan pada lingkungan produksi yang sesungguhnya maupun sumber artefak digital lain seperti log firewall, log basis data, atau Web Application Firewall (WAF). Sejalan dengan rekomendasi Rustianto dkk. (2025) yang menerapkan Fail2Ban, Prometheus, dan Grafana untuk pencegahan dan visualisasi serangan brute force secara real-time, pengembangan lebih lanjut terhadap sistem login yang diteliti disarankan turut mengintegrasikan mekanisme pencegahan serupa agar hasil investigasi forensik dapat ditindaklanjuti dengan langkah mitigasi yang konkret.

KESIMPULAN

Penelitian ini berhasil menerapkan metode Digital Forensic National Institute of Standards and Technology (NIST) SP 800-86 untuk menginvestigasi simulasi serangan brute force pada sistem login website berbasis PHP melalui empat tahapan, yaitu Collection, Examination, Analysis, dan Reporting. Simulasi yang dilakukan pada lingkungan localhost menghasilkan 700 permintaan autentikasi yang tercatat pada access.log, terdiri atas 500 autentikasi berhasil dan 200 autentikasi gagal. Identifikasi dan analisis terhadap access.log dan error.log berhasil mengungkap pola percobaan login gagal yang berulang dari alamat IP yang sama terhadap endpoint login yang identik dalam rentang waktu yang berdekatan, yang kemudian diikuti autentikasi yang berhasil dan akses menuju halaman dashboard. Rekonstruksi kronologi serangan menunjukkan keterkaitan yang konsisten antara access.log, error.log, dan hasil pencatatan percobaan login secara langsung, sehingga dapat disusun urutan kejadian yang sesuai dengan skenario simulasi brute force yang dirancang. Tahap Reporting menghasilkan laporan investigasi yang memuat identitas kasus, sumber barang bukti digital, hasil pemeriksaan, hasil analisis, alamat IP, waktu kejadian, jumlah percobaan, serta kronologi aktivitas, yang dapat digunakan sebagai dokumentasi dan referensi dalam menganalisis insiden keamanan pada sistem login berbasis web. Penelitian selanjutnya disarankan memperluas sumber artefak digital yang dianalisis, seperti log firewall, log basis data, atau Web Application Firewall (WAF), serta mengintegrasikan mekanisme pencegahan seperti rate limiting, account lockout, dan CAPTCHA agar hasil investigasi forensik dapat ditindaklanjuti dengan langkah mitigasi yang lebih komprehensif.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, atas dukungan fasilitas dan bimbingan akademik selama penelitian ini dilaksanakan.

DAFTAR PUSTAKA

- Dasmen, R. N., Pratama, M. R., Yasir, H., & Budiman, A. (2024). Analisis forensik digital pada kasus cyberbullying dengan metode National Institute of Standard and Technology SP 800-86. *Jurnal Ilmiah Informatika*, 12(1), 68–73. <https://doi.org/10.33884/jif.v12i01.8344>
- Disawal, S., & Suman, U. (2024). Enhancing security to prevent vulnerabilities in web applications. *International Journal of Engineering Trends and Technology*, 72(7), 278–283. <https://doi.org/10.14445/22315381/IJETT-V72I7P130>

- Fachri, F. (2023). Optimasi keamanan web server terhadap serangan brute-force menggunakan penetration testing. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 10(1), 51–58. <https://doi.org/10.25126/jtiik.2023105872>
- Faizal, A., & Luthfi, A. (2024). Comparison study of NIST SP 800-86 and ISO/IEC 27037 standards as a framework for digital forensic evidence analysis. *Journal of Information Systems and Informatics*, 6(2), 701–718. <https://doi.org/10.51519/journalisi.v6i2.717>
- Horsman, G. (2024). Interpreting digital traces: 8 foundational pillars to support the formation of opinion in digital forensics. *Science & Justice*, 64(1), 38–42. <https://doi.org/10.1016/j.scijus.2023.11.007>
- Pamungkas, C., Hendradi, P., Sasongko, D., & Ghifari, A. (2023). Analysis of brute force attacks using National Institute of Standards and Technology (NIST) methods on routers. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, 5(2), 115–125. <https://doi.org/10.20895/inista.v5i2.1039>
- Pradana Aji, R., Prayudi, Y., & Luthfi, A. (2023). Analysis of brute force attack logs toward Nginx web server on dashboard improved log logging system using forensic investigation method. *Jurnal Teknik Informatika (Jutif)*, 4(1), 39–48. <https://doi.org/10.52436/1.jutif.2023.4.1.644>
- Rasyid, F. Al, & Zen, B. P. (2023). Dead forensic analysis of Qutebrowser and LibreWolf browsers using the NIST 800-86 method. *Jurnal Teknik Informatika (Jutif)*, 4(5), 1009–1019. <https://doi.org/10.52436/1.jutif.2023.4.5.688>
- Rustianto, A., Fadillah, A., & Kasih, J. (2025). Pencegahan dan visualisasi serangan brute force menggunakan Fail2Ban, Prometheus, dan Grafana: Studi kasus di Sekolah Tinggi Teknologi Terpadu Nurul Fikri. *Jurnal Publikasi Teknik Informatika*, 4(2), 195–209. <https://doi.org/10.55606/jupti.v4i2.5144>
- Saifani, R., & Tanjung, M. A. P. (2026). Analisis forensik digital dan ekstraksi artefak aplikasi GBWhatsApp pada perangkat Android menggunakan framework NIST SP 800-86. *Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS)*, 4(6), 583–593. <https://doi.org/10.33151/ijomss.v4i6.1152>
- Sulisnawati, N., & Subektiningsih, S. (2023). Implementation of Open Web Application Security Project for penetration testing on educational institution websites. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 9(2), 250–267. <https://doi.org/10.26555/jiteki.v9i2.25987>