

**PENERAPAN METODE
DIGITAL FORENSIC NIST UNTUK INVESTIGASI
SERANGAN BRUTE FORCE PADA SISTEM LOGIN
WEBSITE BERBASIS PHP MELALUI ANALISIS LOG
SERVER**

SKRIPSI

DISUSUN OLEH

SHINTYA ANGGIE SYAFITRI

NPM. 2209010128



**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2026**

**PENERAPAN METODE
DIGITAL FORENSIC NIST UNTUK INVESTIGASI
SERANGAN BRUTE FORCE PADA SISTEM LOGIN
WEBSITE BERBASIS PHP MELALUI ANALISIS LOG
SERVER**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
(S.Kom) dalam Program Studi Sistem Informasai pada Fakultas Ilmu Komputer
dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara**

SHINTYA ANGGIE SYAFITRI

NPM. 2209010128

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2026**

LEMBAR PENGESAHAN

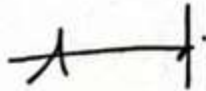
Judul Skripsi : PENERAPAN METODE DIGITAL FORENSIC NIST
UNTUK INVESTIGASI SERANGAN BRUTE FORCE
PADA SISTEM LOGIN WEBSITE BERBASIS PHP
MELALUI ANALISIS LOG SERVER

Nama Mahasiswa : SHINTYA ANGGIE SYAFITRI

NPM : 2209010128

Program Studi : SISTEM INFORMASI

Menyetujui
Komisi Pembimbing



(Andy Zulherry, S.Kom., M.Kom)
NIDN. 0129117901

Ketua Program Studi



(Mahardika Abdi Prawira Tanjung,
S.Kom., M.Kom)
NIDN. 0117088902

Dekan



(Dr. Alif Alfarizmi, S.Kom., M.Kom.)
NIDN. 0127099201

PERNYATAAN ORISINALITAS

**PENERAPAN METODE
DIGITAL FORENSIC NIST UNTUK INVESTIGASI SERANGAN BRUTE
FORCE PADA SISTEM LOGIN WEBSITE BERBASIS PHP MELALUI
ANALISIS LOG SERVER**

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri,
kecuali beberapa kutipan dan ringkasan yang masing-masing
disebutkan sumbernya.

Medan, 07 oktober 2026

Yang membuat
pernyataan



Shintya Anggie Syafitri
NPM. 2209010128

**PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS**

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Shintya Anggie Syafitri
NPM	: 2209010128
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif (*Non-Exclusive Royalty free Right*) atas penelitian skripsi saya yang berjudul:

**PENERAPAN METODE DIGITAL FORENSIC NIST UNTUK
INVESTIGASI SERANGAN BRUTE FORCE PADA SISTEM LOGIN
WEBSITE BERBASIS PHP MELALUI ANALISIS LOG SERVER**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 07 Oktober 2026

Yang membuat pernyataan



Shintya Anggie Syafitri

NPM. 2209010128

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap : Shintya Anggie Syafitri
Tempat dan Tanggal Lahir : Tanjung Morawa, 22 September 2003
Alamat Rumah : Tanjung Morawa, Limau Manis, Gg. Swadaya
Telepon/Faks/HP : 085664033288
E-mail : anggishintya444@gmail.com
Instansi Tempat Kerja : -
Alamat Kantor : -

DATA PENDIDIKAN

SD	: MIN 1 Deli Serdang	TAMAT: 2015
SMP	: MTs 1 Deli Serdang	TAMAT: 2018
SMA	: MAN 1 Deli Serdang	TAMAT: 2021

KATA PENGANTAR



Pendahuluan

Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Akrim, M.Pd., Selaku Rektor Universitas Muhammadiyah Sumatera Utara (UMSU).
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom., Selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Dr. Firahmi Rizky, S.Kom., M.Kom., Selaku Wakil Dekan I Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU serta Selaku Dosen penguji, yang telah memberikan kritik, saran, dan masukan yang membangun demi penyempurnaan skripsi ini.
4. Bapak Mhd Basri, S.Si., M.Kom., Selaku Wakil Dekan III Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
5. Bapak Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom., Selaku Ketua Program Studi sistem informasi.
6. Bapak Mulkan Azhari, S.Kom., M.Kom., Selaku Sekretaris Program Studi sistem informasi.
7. Ibu Zuli Agustina Gultom, S.Si., M.Si., Selaku Dosen Pembimbing, yang telah meluangkan waktu, memberikan bimbingan, arahan, ilmu serta motivasi kepada penulis selama proses penyusunan skripsi ini hingga dapat diselesaikan dengan baik.
8. Ibu Indah Purnama Sari, S.T., M.Kom., Selaku Dosen Penguji, yang telah memberikan kritik, saran, dan masukan yang membangun demi penyempurnaan skripsi ini.
9. Seluruh Bapak dan Ibu Dosen serta Staf Program Studi Sistem Informasi, yang telah memberikan ilmu, pengetahuan, dan pelayanan selama penulis menempuh pendidikan di Universitas Muhammadiyah Sumatera Utara.

10. Teristimewa kepada Ayah dan Mama tercinta, yang selalu menjadi sumber kekuatan bagi penulis. Terima kasih atas setiap doa, kasih sayang, pengorbanan, dukungan, dan kepercayaan yang tidak pernah berhenti diberikan kepada penulis. Tanpa doa dan dukungan dari Ayah dan Mama, penulis tidak akan mampu sampai pada tahap ini.
11. Kepada adik tersayang, Azhra Fitri Safira, terima kasih karena telah menjadi salah satu support system terbaik bagi penulis dalam setiap proses perjalanan menyelesaikan skripsi ini. Terima kasih atas segala perhatian, semangat, dan dukungan yang selalu diberikan, terutama ketika penulis merasa lelah dan hampir menyerah. Kehadiranmu mungkin terlihat sederhana, tetapi memiliki arti yang begitu besar dalam perjalanan ini. Terima kasih telah menjadi adik sekaligus teman berbagi cerita yang selalu memberikan semangat hingga penulis dapat menyelesaikan skripsi ini. Semoga kelak penulis juga dapat selalu menjadi seseorang yang mendukung dan membanggakanmu.
12. Kepada kakak dan adik tersayang, Indah Ramadhani dan Saqilla Khofifah, terima kasih atas segala doa, perhatian, dukungan, dan semangat yang selalu diberikan kepada penulis selama menjalani proses perkuliahan hingga menyelesaikan skripsi ini. Kehadiran kalian menjadi salah satu bagian penting dan berharga dalam perjalanan penulis hingga dapat menyelesaikan skripsi ini. Semoga kita selalu dapat saling mendukung, menyayangi, dan menjadi kebanggaan satu sama lain.
13. Kepada keluarga tercinta, yang senantiasa memberikan doa, perhatian, semangat, dan dukungan kepada penulis selama proses perkuliahan hingga penyelesaian skripsi ini.
14. Kepada teman seperjuangan, Adinda Nurul, S.Kom, terima kasih telah menjadi bagian dari perjalanan panjang penulis selama menjalani perkuliahan hingga menyelesaikan skripsi ini. Terima kasih telah menemani, mendengarkan segala cerita dan keluh kesah, memberikan semangat, serta selalu hadir dalam berbagai keadaan. Banyak hal yang telah kita lalui bersama, baik suka maupun duka, dan semuanya menjadi kenangan berharga yang akan selalu penulis ingat.

15. Kepada Rini Afrizal Sembiring, S.kom, terima kasih telah menjadi teman yang selalu memberikan dukungan, semangat dan kebersamaan selama perjalanan perkuliahan hingga penyelesaian skripsi ini.
16. Kepada teman-teman seperkuliahan yang tidak dapat penulis sebutkan satu per satu, terima kasih atas kebersamaan, dukungan, bantuan, cerita, dan kenangan yang telah diberikan selama menjalani perkuliahan hingga proses penyelesaian skripsi ini. Terima kasih telah menjadi bagian dari perjalanan penulis dalam menyelesaikan pendidikan ini. Semoga segala perjuangan dan kebersamaan yang telah dilalui menjadi kenangan indah dan membawa kita menuju kesuksesan masing-masing.
17. Terakhir, penulis ingin mengucapkan terima kasih kepada diri sendiri yang telah bertahan, berusaha, dan terus melangkah hingga sampai pada tahap ini. Terima kasih karena tetap memilih untuk menyelesaikan apa yang telah dimulai, meskipun dalam prosesnya terdapat banyak kesulitan, rasa lelah, keraguan, dan tantangan. Semoga pencapaian ini menjadi pengingat bahwa setiap proses yang dijalani dengan sabar dan sungguh-sungguh akan menemukan hasilnya pada waktu yang tepat.

Medan, 07 Oktober 2026

Yang membuat pernyataan

Shintya Anggie Syfitri

NPM. 2209010128

PENERAPAN METODE DIGITAL FORENSIC NIST UNTUK INVESTIGASI SERANGAN BRUTE FORCE PADA SISTEM LOGIN WEBSITE BERBASIS PHP MELALUI ANALISIS LOG SERVER

ABSTRAK

Serangan *brute force* merupakan salah satu bentuk serangan terhadap sistem autentikasi yang dilakukan dengan mencoba berbagai kombinasi kredensial secara berulang untuk memperoleh akses ke suatu akun. Aktivitas tersebut dapat meninggalkan jejak digital pada log server yang dapat digunakan sebagai barang bukti dalam proses investigasi. Penelitian ini bertujuan untuk menerapkan metode Digital Forensic National Institute of Standards and Technology (NIST) dalam menginvestigasi serangan *brute force* pada sistem login website berbasis PHP melalui analisis log server, mengidentifikasi dan menganalisis artefak digital, merekonstruksi kronologi serangan, serta menghasilkan laporan investigasi. Penelitian dilakukan pada lingkungan *localhost* menggunakan XAMPP dengan membangun sistem login berbasis PHP dan melakukan simulasi serangan *brute force* secara terkendali. Proses investigasi menggunakan empat tahapan NIST SP 800-86, yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*. Hasil penelitian menunjukkan bahwa simulasi menghasilkan tiga percobaan login gagal yang berasal dari alamat IP 172.18.150.182 pada pukul 17:35:35, 17:35:41, dan 17:35:42, dengan target URL http://localhost/nist_forensic/includes/login.php. Analisis *access.log* memberikan informasi mengenai alamat IP, waktu akses, URL, metode HTTP, dan *status code*, sedangkan *error.log* memberikan informasi aktivitas *LOGIN_ATTEMPT*, username, alamat IP, serta status login. Berdasarkan keterkaitan kedua log tersebut, kronologi aktivitas dapat direkonstruksi mulai dari akses halaman login pada pukul 17:34:39, tiga percobaan login gagal, hingga akses ke halaman dashboard pada pukul 17:37:11 dengan *status code* 200. Tahap *Reporting* menghasilkan laporan investigasi yang memuat barang bukti digital, hasil analisis, dan kronologi aktivitas sebagai dasar dokumentasi investigasi insiden keamanan pada sistem login website berbasis PHP.

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

**APPLICATION OF THE NIST DIGITAL FORENSIC METHOD FOR
INVESTIGATING BRUTE FORCE ATTACKS ON A PHP-BASED WEBSITE
LOGIN SYSTEM THROUGH SERVER LOG ANALYSIS
ABSTRACT**

Brute force attacks are a form of attack against authentication systems that repeatedly attempt various combinations of credentials to gain unauthorized access to an account. Such activities may leave digital traces in server logs that can be used as evidence in a forensic investigation. This study aims to apply the National Institute of Standards and Technology (NIST) Digital Forensic method to investigate *brute force* attacks on a PHP-based website login system through server log analysis, identify and analyze digital artifacts, reconstruct the attack chronology, and produce an investigation report. The research was conducted in a *localhost* environment using XAMPP by developing a PHP-based login system and performing a controlled *brute force* attack simulation. The investigation process followed four stages of NIST SP 800-86: *Collection*, *Examination*, *Analysis*, and *Reporting*. The results showed that the simulation generated three failed login attempts originating from IP address 172.18.150.182 at 17:35:35, 17:35:41, and 17:35:42, targeting the URL http://localhost/nist_forensic/includes/login.php. The *access.log* analysis provided information regarding the IP address, access time, URL, HTTP method, and *status code*, while the *error.log* provided information about *LOGIN_ATTEMPT* activities, username, IP address, and login status. Based on the correlation between the two logs, the activity chronology was reconstructed starting from access to the login page at 17:34:39, followed by three failed login attempts, and then access to the dashboard at 17:37:11 with a *status code* of 200. The *Reporting* stage produced an investigation report containing digital evidence, analysis results, and activity chronology as documentation for investigating security incidents on a PHP-based website login system.

Keywords: Digital Forensic, NIST SP 800-86, Brute Force, Access Log, Error Log, PHP.

DAFTAR ISI

DAFTAR ISI	x
DAFTAR TABEL	xv
DAFTAR GAMBAR	1
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	7
1.3 Batasan Masalah.....	7
1.4 Tujuan Penelitian.....	8
1.5 Manfaat Penelitian.....	9
BAB II LANDASAN TEORI	11
2.1 Digital Forensic	11
2.2.1 Pengertian Digital Forensic.....	11
2.2.2. Metode Digital Forensic NIST.....	15
2.2.3. Serangan Brute Force.....	19
2.2.4. Website Berbasis PHP	23
2.2.5 Web Server dan Log Server	26
2.2.5.5 Kaitan Web Server dan Log Server dengan Penelitian.....	29
2.2 Kerangka Berpikir	30

2.2.2 Diagram Kerangka Berpikir.....	30
2.2.2.1 Penjelasan Kerangka Berpikir.....	30
2.3 Penelitian Terdahulu.....	31
2.3.1 Penjelasan Penelitian Terdahulu.....	31
BAB III ANALISA DAN PERANCANGAN	37
3.1 Analisis Permasalahan	37
3.1.1 Diagram Alur Analisis Permasalahan	38
3.2 Metodologi Penelitian	39
3.2.2 Lokasi dan Waktu Penelitian	40
3.2.3 Sumber dan Teknik Pengumpulan Data	40
3.2.4 Tahapan Penelitian.....	41
3.3 Algoritma Sistem	47
3.3.1 Tahapan Algoritma Sistem	47
3.3.2 Use Case Diagram.....	51
3.3.3 Class Diagram	52
3.3.4 Rancangan Tampilan Antarmuka (UI).....	55
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM	59
4.1 Implementasi Sistem.....	59
4.1.1 Implementasi Lingkungan Sistem.....	59
4.1.2 Implementasi Basis Data.....	61
4.1.3 Implementasi Halaman Login	63

4.1.4 Implementasi Halaman Dashboard	64
4.2 Implementasi Sistem	66
4.2.1 Implementasi Database	66
4.2.3 Implementasi Proses Autentikasi	68
4.2.4 Implementasi Dashboard	70
4.2.5 Implementasi Logging	71
4.3 Simulasi Serangan <i>Brute Force</i>	73
4.3.1 Menentukan Parameter Percobaan.....	74
4.3.3 Melakukan Percobaan Login Berulang pada Lingkungan <i>Localhost</i>	75
4.3.4 Mencatat Hasil Percobaan.....	76
4.3.5 Menghasilkan <i>Access Log</i> dan <i>Error Log</i>	77
4.4 Pengumpulan Barang Bukti Digital	79
4.4.1 Proses Collection	80
4.5 Examination	83
4.5.1 Pemeriksaan Alamat IP	84
4.5.2 Pemeriksaan Tanggal dan Waktu.....	84
4.5.3 Pemeriksaan URL Login.....	85
4.5.4 Pemeriksaan Metode HTTP	86
4.5.5 Pemeriksaan Status Code.....	87
4.5.6 Pemeriksaan User Agent.....	87

4.5.7 Pemeriksaan Jumlah Percobaan Login	88
4.6 Analysis.....	90
4.6.1 Analisis IP Address.....	91
4.6.2 Analisis Waktu Serangan.....	92
4.6.3 Analisis Frekuensi Percobaan Login	93
4.6.4 Analisis Pola Percobaan.....	94
4.6.5 Analisis URL yang Ditargetkan.....	94
4.6.6 Analisis Respons Server	95
4.6.7 Analisis Hubungan access.log dan error.log.....	96
4.6.8 Penyusunan Kronologi Serangan.....	99
4.7 Rekonstruksi Kronologi Serangan	101
4.8 Reporting.....	103
4.8.1 Identitas Kasus	104
4.8.2 Sumber Barang Bukti Digital.....	104
4.8.3 Hasil Pemeriksaan.....	105
4.8.4 Hasil Analisis	107
4.8.5 IP Address	108
4.8.6 Waktu Kejadian	109
4.8.7 Jumlah Percobaan	110
4.8.8 Kronologi Serangan	110
4.9 Hasil Pengujian dan Pembahasan	112

BAB V PENUTUP	115
5.1 Kesimpulan	115
DAFTAR PUSTAKA	119
LAMPIRAN	122

DAFTAR TABEL

Tabel 2.1 Prinsip Digital Forensik	13
Tabel 2.2 Implementasi Tahapan NIST Pada Penelitian	18
Tabel 2.3 Jenis-Jenis Serangan Brute Force	20
Tabel 2.4 Karakteristik Website Berbasis PHP	24
Tabel 2.5 Artefak Digital pada Log Server	28
Tabel 2.6 Penelitian Terdahulu	32
Tabel 3.1 Data Sekunder	43
Tabel 3.2 Data Primer	45
Tabel 4. 1 Lingkungan Implementasi Sistem.....	61
Tabel 4. 2 Menentukan Parameter Percobaan.....	74
Tabel 4. 3 Mencatat Hasil Percobaan.....	76
Tabel 4. 4 Daftar Barang Bukti Digital.....	81
Tabel 4. 5 Hasil Pemeriksaan Aktivitas Login.....	88
Tabel 4. 6 Analisis IP Address.....	91
Tabel 4. 7 Analisis Waktu Aktivitas	92
Tabel 4. 8 Frekuensi Percobaan Login.....	93
Tabel 4. 9 Analisis URL.....	95
Tabel 4. 10 Analisis Respons Server.....	96
Tabel 4. 11 Korelasi access.log dan error.log	96
Tabel 4. 12 Kronologi Aktivitas Simulasi.....	100
Tabel 4. 13 Rekonstruksi Kronologi Simulasi Serangan	102

DAFTAR GAMBAR

Gambar 2.1 Kerangka Berpikir Penelitian	30
Gambar 3.1 Analisis Permasalahan Penelitian	38
Gambar 3.2 Tahapan Penelitian	42
Gambar 3.3 Alur Proses Algoritma	50
Gambar 3.4 Use Case Diagram	51
Gambar 3.5 Class Diagram	52
Gambar 3.6 Rancangan Dashboard	55
Gambar 4. 1 Implementasi Basis Data Sistem	62
Gambar 4. 2 Implementasi Halaman Login	63
Gambar 4. 3 Implementasi Halaman Dashboard	65
Gambar 4. 4 Implementasi Database	67
Gambar 4. 5 Proses Login Berhasil.....	69
Gambar 4. 6 Proses Login Gagal	69
Gambar 4. 7 Implementasi Dashboard.....	70
Gambar 4. 8 Implementasi acces.log	71
Gambar 4. 9 Implementasi error.log	72
Gambar 4. 10 Simulasi Serangan Brute Force	73
Gambar 4. 11 Percobaan Login Berulang pada Lingkungan Localhost	75
Gambar 4. 12 Acces Log.....	77
Gambar 4. 13 Error Log	78
Gambar 4. 14 Acces Log dan Error Log	82
Gambar 4. 15 Pemeriksaan Alamat IP	84

Gambar 4. 16 Tanggal dan Waktu (Timestamp).....	85
Gambar 4. 17 URL Login	85
Gambar 4. 18 Metode HTTP.....	86
Gambar 4. 19 Status Code.....	87
Gambar 4. 20 User Agent.....	88

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan transformasi digital telah mendorong pemanfaatan aplikasi berbasis web pada berbagai sektor, seperti pemerintahan, pendidikan, kesehatan, perbankan, dan perdagangan elektronik. Peningkatan pemanfaatan aplikasi web tersebut diikuti oleh meningkatnya kebutuhan terhadap keamanan aplikasi karena berbagai ancaman siber terus berkembang seiring dengan meningkatnya ketergantungan terhadap layanan digital (Disawal & Suman, 2024; Fachri, 2023; Pradana Aji et al., 2023; Sulisnawati & Subektiningsih, 2023).

Di balik perkembangan teknologi tersebut, ancaman terhadap keamanan siber juga terus mengalami peningkatan seiring dengan semakin luasnya pemanfaatan aplikasi berbasis web pada berbagai sektor ((Disawal & Suman, 2024). Serangan terhadap aplikasi web umumnya memanfaatkan kelemahan pada mekanisme autentikasi, seperti penggunaan kata sandi yang lemah, pengelolaan kredensial yang kurang baik, maupun tidak diterapkannya mekanisme pembatasan percobaan login sehingga meningkatkan risiko akses tidak sah ke dalam sistem. Salah satu bentuk serangan yang paling sering menargetkan mekanisme autentikasi adalah *brute force attack*, yaitu teknik penyerangan dengan mencoba berbagai kombinasi *username* dan *password* secara berulang hingga memperoleh kredensial yang valid (Aji et al., 2023). Kondisi tersebut menunjukkan bahwa keamanan sistem login menjadi salah satu aspek penting dalam menjaga

kerahasiaan, integritas, dan ketersediaan informasi pada aplikasi berbasis web (Disawal & Sulisnawati, 2024). Oleh karena itu, diperlukan proses investigasi digital forensik yang mampu mengidentifikasi penyebab, pola serangan, serta mengumpulkan dan menganalisis bukti digital secara sistematis agar kronologi serangan dapat direkonstruksi dan dijadikan dasar dalam meningkatkan keamanan sistem (Horsman & Sunde, 2022; Wulandari, 2025). Brute force attack merupakan metode penyerangan terhadap mekanisme autentikasi yang dilakukan dengan mencoba berbagai kombinasi kredensial secara berulang dan otomatis hingga ditemukan pasangan *username* dan *password* yang valid. Serangan ini umumnya memanfaatkan perangkat lunak otomatis sehingga mampu melakukan ribuan percobaan login dalam waktu singkat dan berpotensi menyebabkan akses tidak sah ke dalam sistem (Tanriverdi, 2024; Pradana Aji, Prayudi, & Luthfi, 2023). Serangan brute force umumnya memanfaatkan kelemahan pada sistem autentikasi, seperti tidak adanya pembatasan jumlah percobaan login (account lockout), penggunaan kata sandi yang lemah, serta tidak diterapkannya mekanisme multi-factor authentication (MFA), sehingga peluang keberhasilan penyerang menjadi lebih besar (Lakh et al., 2021). Selain mengancam kerahasiaan data, serangan brute force juga dapat menyebabkan penyalahgunaan akun pengguna, pencurian informasi sensitif, gangguan terhadap ketersediaan layanan, hingga menjadi pintu masuk bagi serangan siber lanjutan (Chimuco et al., 2023). Setiap percobaan login yang dilakukan selama serangan akan meninggalkan jejak digital (digital footprint) pada *access log* maupun *error log web server*, sehingga informasi tersebut dapat dimanfaatkan sebagai barang bukti digital untuk mengidentifikasi alamat IP penyerang, waktu serangan, pola percobaan login, serta karakteristik

aktivitas yang dilakukan (Aji et al., 2023). Oleh karena itu, analisis terhadap log server menjadi langkah penting dalam proses investigasi digital forensik karena mampu membantu merekonstruksi kronologi serangan serta menyediakan informasi yang dapat digunakan sebagai dasar dalam pengambilan keputusan terkait penanganan insiden keamanan siber (Pradana Aji, R., Prayudi, Y., & Luthfi, A. (2023).

Website berbasis PHP (Hypertext Preprocessor) masih menjadi salah satu platform yang banyak digunakan dalam pengembangan aplikasi web karena bersifat open source, mudah dikembangkan, serta didukung oleh berbagai framework dan komunitas pengembang yang luas (Rahman & Saiful, 2023; Sari, Nugroho, & Prasetyo, 2024). PHP banyak dimanfaatkan dalam pembangunan berbagai sistem informasi berbasis web, seperti sistem akademik, pelayanan pemerintahan, perdagangan elektronik (e-commerce), hingga aplikasi perbankan, sehingga keamanan aplikasi yang dibangun menggunakan PHP menjadi aspek yang sangat penting (Neef et al., 2024). Meskipun aplikasi web berbasis PHP terus mengalami perkembangan dari sisi performa dan ekosistem pengembangannya, aspek keamanan tetap menjadi perhatian utama karena aplikasi yang tidak menerapkan mekanisme pengamanan yang memadai, khususnya pada proses autentikasi pengguna, masih berpotensi mengalami berbagai serangan siber (Yin & Lee, 2023; Sulisnawati & Subertiningsih, 2023). Pada mekanisme autentikasi, setiap permintaan (*request*) yang diterima web server akan direkam dalam *access log*, sedangkan berbagai kesalahan yang terjadi selama proses autentikasi akan dicatat pada *error log*. Kedua jenis log tersebut menyimpan artefak digital, seperti alamat IP, *timestamp*, metode HTTP, URL,

status code, dan *user agent*, yang dapat dimanfaatkan sebagai barang bukti digital untuk mengidentifikasi pola serangan serta merekonstruksi kronologi insiden keamanan siber (Pradana Aji, Prayudi, & Lutfi, 2023; Horsman & Sunde, 2022). Oleh karena itu, website berbasis PHP dipilih sebagai objek penelitian karena mampu merepresentasikan implementasi aplikasi web yang umum digunakan sekaligus menyediakan artefak digital yang diperlukan untuk menganalisis dan merekonstruksi kronologi serangan brute force melalui analisis log server (Neef et al., 2024).

Beberapa penelitian terdahulu telah menerapkan metode digital forensik untuk menginvestigasi serangan brute force melalui analisis artefak digital yang tersimpan pada perangkat maupun log sistem (Pamungkas et al., 2023; Aji dkk, 2023). Berhasil mengidentifikasi alamat IP penyerang, waktu serangan, serta pola brute force pada router menggunakan tahapan Collection, Examination, Analysis, dan Reporting berdasarkan metode NIST, sehingga menunjukkan bahwa metode tersebut efektif dalam proses investigasi digital (Catur Pamungkas dkk., 2023). Menganalisis log serangan brute force pada web server Nginx menggunakan pendekatan investigasi digital forensik dan membuktikan bahwa analisis log server mampu merekonstruksi kronologi serangan serta mengidentifikasi aktivitas penyerang secara rinci (Rio Pradana Aji dkk., 2023). Berdasarkan telaah terhadap penelitian-penelitian tersebut, mayoritas penelitian masih berfokus pada investigasi serangan *brute force* pada router, web server, atau infrastruktur jaringan. Penelitian yang secara khusus menerapkan metode NIST untuk menginvestigasi serangan brute force pada sistem login website berbasis PHP

melalui analisis *access log* dan *error log* masih terbatas, sehingga topik tersebut masih memiliki peluang untuk dikembangkan lebih lanjut.

Meskipun berbagai penelitian telah berhasil menerapkan metode digital forensik untuk menginvestigasi serangan brute force, masih terdapat beberapa keterbatasan yang perlu dikembangkan lebih lanjut (Pamungkas et al., 2023; Aji et al., 2023). Sebagian besar penelitian terdahulu berfokus pada analisis serangan terhadap perangkat jaringan, web server, atau sistem operasi, sehingga objek penelitian belum secara spesifik mengkaji mekanisme autentikasi pada sistem login website berbasis PHP yang banyak digunakan dalam pengembangan aplikasi web (Pamungkas et al., 2023; Aji et al., 2023). Selain itu, penelitian-penelitian tersebut umumnya hanya menitikberatkan pada proses identifikasi artefak digital tanpa menguraikan secara mendalam keterkaitan antara *access log* dan *error log* dalam merekonstruksi kronologi serangan *brute force*, sehingga informasi yang dihasilkan masih terbatas pada identifikasi aktivitas penyerang (Aji et al., 2023). Integrasi analisis *access log* dan *error log* memberikan gambaran yang lebih komprehensif mengenai pola serangan, waktu kejadian, respons server, serta artefak digital yang ditinggalkan oleh pelaku. Informasi tersebut mendukung proses rekonstruksi kronologi insiden sehingga investigasi digital forensik dapat dilakukan secara lebih sistematis (Pradana Aji, Prayudi, & Luthfi, 2023; Horsman & Sunde, 2022). Berdasarkan kondisi tersebut, masih terdapat peluang penelitian untuk menerapkan metode Digital Forensic NIST pada investigasi serangan brute force terhadap sistem login website berbasis PHP melalui analisis *access log* dan *error log* sebagai upaya menghasilkan proses investigasi yang lebih komprehensif dan mudah direplikasi.

Berdasarkan *research gap* yang telah diuraikan, penelitian ini menawarkan kebaruan (*novelty*) berupa penerapan metode Digital Forensic NIST SP 800-86 untuk menginvestigasi serangan *brute force* pada sistem login website berbasis PHP melalui analisis *access log* dan *error log* secara terintegrasi. Pendekatan tersebut dirancang untuk menghasilkan proses investigasi yang lebih sistematis, memudahkan rekonstruksi kronologi serangan, serta mengidentifikasi artefak digital secara lebih komprehensif melalui pemanfaatan dua sumber log server sebagai barang bukti digital (Pradana Aji, Prayudi, & Luthfi, 2023; Horsman & Sunde, 2022). Berbeda dengan penelitian terdahulu yang umumnya berfokus pada investigasi perangkat jaringan, web server, atau analisis satu jenis log, penelitian ini mengintegrasikan analisis beberapa artefak digital dari log server untuk merekonstruksi kronologi serangan, mengidentifikasi pola percobaan login, serta memperoleh bukti digital yang dapat dipertanggungjawabkan dalam proses investigasi (Pamungkas et al., 2023; Aji et al., 2023). Pendekatan tersebut diharapkan mampu memberikan gambaran yang lebih komprehensif mengenai kronologi dan pola serangan *brute force*, termasuk identifikasi alamat IP penyerang, waktu kejadian (*timestamp*), frekuensi percobaan login, URL yang diakses, *status code*, serta respons web server. Informasi tersebut menjadi dasar dalam proses rekonstruksi insiden dan penyusunan laporan hasil investigasi digital forensik (Pradana Aji, Prayudi, & Luthfi, 2023; Horsman & Sunde, 2022). Dengan demikian, 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 *access log* dan *error log* guna memperoleh bukti digital, merekonstruksi kronologi serangan, serta menghasilkan

rekomendasi yang dapat mendukung peningkatan keamanan sistem autentikasi aplikasi web.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

- a. Bagaimana penerapan metode Digital Forensic National Institute of Standards and Technology (NIST) dalam proses investigasi serangan brute force pada sistem login website berbasis PHP?
- b. Bagaimana proses identifikasi dan analisis artefak digital yang diperoleh dari access log dan error log server untuk mengungkap aktivitas serangan brute force pada sistem login website berbasis PHP?
- c. Bagaimana hasil rekonstruksi kronologi serangan brute force berdasarkan analisis log server menggunakan tahapan metode Digital Forensic NIST?
- d. Bagaimana hasil penerapan metode Digital Forensic NIST dalam menghasilkan laporan investigasi yang dapat digunakan sebagai dasar analisis insiden keamanan pada website berbasis PHP?

1.3 Batasan Masalah

Agar penelitian ini tidak melebar dari fokus yang telah ditentukan, sehingga penelitian dapat dilakukan secara lebih terarah dan sesuai dengan tujuan yang ingin dicapai. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut .:

- a. Penelitian dibatasi pada penerapana metode digital forensic NIST SP 800-86 dalam proses investigasi serangan Brute Force dengan tahapan Collection, Examination, Analysis, dan Reporting.

- b. Objek penelitian dibatasi pada sistem login website berbasis PHP yang dijalankan pada lingkungan *Localhost* menggunakan XAMPP, dengan serangan yang dilakukan berupa simulasi brute force terhadap halaman login.
- c. Barang bukti digital yang digunakan dalam proses identifikasi dan analisis dibatasi pada access log dan error log server, serta data pendukung berupa hasil percobaan login dan dokumentasi pengujian. Analisis difokuskan pada informasi seperti alamat IP, Timestamp, URL, metode HTTP, status code, user-agent, dan frekuensi percobaan.
- d. Hasil penelitian dibatasi pada identifikasi aktivitas serangan, rekonstruksi kronologi serangan berdasarkan analisis log server, dan penyusunan laporan hasil investigasi menggunakan metode digital forensic NIST. Penelitian tidak membahas mekanisme pencegahan serangan seperti firewall, IDS/IPS, CAPTCHA, maupun multifactor authentication.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, maka tujuan dari penelitian ini adalah sebagai berikut :

- a. Menerapkan metode Digital Forensic National Institute of Standards and Technology (NIST) dalam proses investigasi serangan brute force pada sistem login website berbasis PHP.
- b. Mengidentifikasi dan menganalisis artefak digital yang diperoleh dari access log dan error log server sebagai bukti digital untuk mengungkap aktivitas serangan brute force.

- c. Merekonstruksi kronologi serangan brute force berdasarkan hasil analisis log server melalui tahapan Collection, Examination, Analysis, dan Reporting pada metode NIST.
- d. Menghasilkan laporan investigasi digital forensik yang dapat digunakan sebagai referensi dalam analisis dan penanganan insiden keamanan pada website berbasis PHP.

1.5 Manfaat Penelitian

Manfaat penelitian ini disusun untuk menjelaskan distribusi yang diharapkan dari hasil penelitian.

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan siber (cybersecurity) dan digital forensik, khususnya terkait penerapan metode Digital Forensic National Institute of Standards and Technology (NIST) dalam proses investigasi serangan brute force pada sistem login website berbasis PHP. Selain itu, hasil penelitian ini diharapkan dapat menjadi referensi ilmiah bagi mahasiswa, akademisi, maupun peneliti yang ingin mengembangkan penelitian mengenai investigasi insiden keamanan website melalui analisis log server.

2. Manfaat Praktis

1. Bagi Administrator Website

Hasil penelitian ini diharapkan dapat membantu administrator website dalam memahami proses investigasi serangan brute force, mengidentifikasi artefak digital yang terdapat pada access log dan

error log, serta memanfaatkan hasil analisis tersebut sebagai dasar dalam meningkatkan keamanan sistem login website. Memberikan gambaran penerapan metode NIST dalam investigasi serangan siber secara sistematis.

2. Bagi Peneliti Selanjutnya

Penelitian ini diharapkan dapat menjadi acuan bagi penelitian selanjutnya yang berkaitan dengan penerapan digital forensik pada berbagai jenis serangan siber, pengembangan metode investigasi digital, maupun analisis artefak digital yang berasal dari log server atau sumber bukti digital lainnya.

3. Bagi Penulis

Penelitian ini diharapkan dapat menambah wawasan, pengetahuan, dan pengalaman penulis dalam menerapkan metode Digital Forensic NIST untuk menginvestigasi serangan brute force, serta meningkatkan kemampuan dalam melakukan analisis bukti digital dan penyusunan laporan investigasi digital forensik.

BAB II

LANDASAN TEORI

2.1 Digital Forensic

2.2.1 Pengertian Digital Forensic

Digital forensik merupakan cabang ilmu forensik yang berfokus pada proses identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital yang berasal dari perangkat elektronik maupun sistem informasi. Proses tersebut bertujuan memperoleh bukti digital yang valid, terjaga integritasnya, serta dapat dipertanggungjawabkan sehingga mampu mendukung investigasi insiden keamanan siber maupun proses penegakan hukum (Horsman & Sunde, 2022; Alenezi, 2023).

Menurut (Horsman, 2024), digital forensik merupakan proses ilmiah yang bertujuan mengidentifikasi, mengumpulkan, memeriksa, menganalisis, dan menyajikan bukti digital secara sistematis dengan menjaga integritas bukti agar dapat dipertanggungjawabkan dalam proses investigasi. Pendekatan digital forensik diterapkan untuk mengungkap berbagai bentuk insiden keamanan siber, seperti peretasan, pencurian data, penyebaran *malware*, *ransomware*, hingga serangan *brute force*.

Selain itu, menurut Eoghan Casey (2020), digital forensik merupakan proses ilmiah untuk memperoleh, memelihara, menganalisis, serta menyajikan bukti digital sehingga dapat digunakan dalam proses investigasi maupun pembuktian.

Proses tersebut tidak hanya berorientasi pada pencarian bukti, tetapi juga memastikan bahwa setiap bukti yang diperoleh memiliki nilai integritas dan keaslian yang tetap terjaga selama proses investigasi.

2.2.1.1 Tujuan Digital Forensic

Digital forensik bertujuan memperoleh, menjaga, dan menganalisis bukti digital melalui prosedur yang sistematis sehingga keaslian (*authenticity*), integritas (*integrity*), dan validitas bukti tetap terpelihara selama proses investigasi. Bukti digital yang telah diperoleh kemudian digunakan untuk mengidentifikasi penyebab insiden, merekonstruksi kronologi kejadian, mengungkapkan aktivitas pelaku, serta mendukung proses penegakan hukum maupun penanganan insiden keamanan siber (Horsman & Sunde, 2022; Horsman, 2023). Secara umum, tujuan digital forensik meliputi:

1. Mengidentifikasi sumber terjadinya insiden keamanan siber.
2. Mengumpulkan bukti digital dengan tetap menjaga keaslian dan integritas data.
3. Menganalisis bukti digital untuk mengidentifikasi pola dan karakteristik serangan.
4. Merekonstruksi kronologi kejadian berdasarkan artefak digital yang ditemukan.
5. Menyusun laporan investigasi yang dapat dipertanggungjawabkan sebagai dasar pengambilan keputusan maupun proses hukum.

2.2.1.2 Ruang Lingkup Digital Forensic

Perkembangan teknologi informasi menyebabkan ruang lingkup digital forensik menjadi semakin luas. Digital forensik tidak hanya diterapkan pada

komputer pribadi, tetapi juga mencakup berbagai perangkat dan sistem digital yang menyimpan informasi elektronik (Casey, 2020).

Beberapa ruang lingkup digital forensik meliputi:

1. Computer Forensics
2. Network Forensics
3. Mobile Device Forensics
4. Cloud Forensics
5. Database Forensics
6. Web Forensics
7. IoT Forensics

Dalam penelitian ini, ruang lingkup yang digunakan termasuk ke dalam Web Forensics, karena objek penelitian berupa sistem login website berbasis PHP serta analisis terhadap access log dan error log sebagai sumber bukti digital.

2.2.1.3 Prinsip Digital Forensic

Prinsip-prinsip digital forensik menekankan pentingnya menjaga integritas bukti digital, transparansi proses investigasi, kemampuan reproduksi hasil, serta akuntabilitas dalam setiap tahapan investigasi. Ringkasan prinsip-prinsip tersebut disajikan pada Tabel 2.1 (Horsman, 2024; Adel, Ahsan, & Davison, 2024).

Tabel 2. 1 Prinsip Digital Forensik

Prinsip	Penjelasan
Integrity	Menjaga keaslian dan integritas barang bukti digital agar tidak mengalami perubahan selama proses investigasi.
Authenticity	Memastikan bahwa barang bukti digital berasal dari sumber yang sah dan dapat

	diverifikasi.
Repeatability	Proses investigasi dapat diulang dengan prosedur yang sama sehingga menghasilkan temuan yang konsisten.
Accountability	Seluruh tahapan investigasi harus terdokumentasi dengan baik dan dapat dipertanggungjawabkan.

2.2.1.4 Barang Bukti Digital (Digital Evidence)

Dalam konteks investigasi serangan *brute force* pada website berbasis PHP, barang bukti digital yang dianalisis meliputi *access log* dan *error log* web server yang berisi informasi seperti alamat IP, *timestamp*, metode HTTP, URL yang diakses, *status code*, dan *user agent*. Informasi tersebut digunakan untuk mengidentifikasi aktivitas penyerang dan merekonstruksi kronologi serangan (Pradana Aji, Prayudi, & Luthfi, 2023).

Dalam konteks keamanan website, salah satu bentuk barang bukti digital yang paling sering digunakan adalah log server. Log server menyimpan berbagai informasi aktivitas pengguna, seperti alamat IP, waktu akses (*timestamp*), metode HTTP, URL yang diakses, *status code*, serta *user agent*. Informasi tersebut dapat dimanfaatkan untuk mengidentifikasi aktivitas penyerang dan merekonstruksi kronologi suatu insiden keamanan siber.

Secara umum, contoh barang bukti digital meliputi:

1. Access Log
2. Error Log
3. File konfigurasi server
4. Database

5. File sistem
6. Riwayat browser
7. Log autentikasi
8. Metadata file

2.2.1.5 Kaitan Digital Forensic dengan Penelitian

Penelitian ini menerapkan konsep digital forensik sebagai landasan utama dalam proses investigasi serangan *brute force* pada sistem login website berbasis PHP. Melalui pendekatan digital forensik, bukti digital yang terdapat pada *access log* dan *error log* dikumpulkan, diperiksa, dianalisis, kemudian disusun menjadi kronologi serangan berdasarkan tahapan metode NIST SP 800-86.

Penerapan digital forensik pada penelitian ini diharapkan mampu menghasilkan proses investigasi yang sistematis, menjaga integritas bukti digital, serta memberikan informasi yang akurat mengenai pola serangan, identitas penyerang, dan waktu terjadinya serangan. Dengan demikian, hasil penelitian tidak hanya memberikan kontribusi terhadap pengembangan ilmu digital forensik, tetapi juga dapat menjadi acuan dalam penanganan insiden keamanan pada aplikasi web berbasis PHP.

2.2.2. Metode Digital Forensic NIST

2.2.2.1 Pengertian Metode Digital Forensic NIST

Metode National Institute of Standards and Technology (NIST) SP 800-86 merupakan salah satu kerangka kerja digital forensik yang banyak digunakan dalam proses investigasi bukti digital karena menyediakan tahapan investigasi yang sistematis, meliputi *Collection*, *Examination*, *Analysis*, dan *Reporting*. Tahapan tersebut membantu investigator dalam memperoleh, memeriksa,

menganalisis, serta menyusun laporan berdasarkan barang bukti digital secara terstruktur (Dasmen et al., 2024).

Metode Digital Forensic NIST SP 800-86 merupakan salah satu kerangka kerja yang banyak diterapkan dalam proses investigasi digital karena menyediakan tahapan investigasi yang sistematis, mulai dari pengumpulan, pemeriksaan, analisis, hingga pelaporan barang bukti digital. Penerapan metode ini membantu investigator memperoleh dan menganalisis bukti digital secara terstruktur sehingga mendukung proses rekonstruksi insiden keamanan siber, seperti serangan *malware*, *ransomware*, pencurian data, maupun serangan *brute force* terhadap sistem informasi (Dasmen et al., 2024)

2.2.2.2 Tahapan Metode NIST

Metode Digital Forensic NIST SP 800-86 terdiri atas empat tahapan utama, yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*. Keempat tahapan tersebut membentuk proses investigasi digital yang sistematis untuk mengumpulkan, memeriksa, menganalisis, serta menyusun laporan berdasarkan barang bukti digital yang diperoleh sehingga hasil investigasi dapat dipertanggungjawabkan (fFaizal & Luthfi, 2024).

a. Collection

Tahap Collection merupakan proses identifikasi, pengumpulan, dan pengamanan barang bukti digital yang berkaitan dengan insiden. Pada tahap ini, investigator memastikan bahwa bukti digital dikumpulkan tanpa mengubah isi maupun struktur data sehingga integritas bukti tetap terjaga.

b. Examination

Tahap Examination bertujuan untuk melakukan pemeriksaan terhadap barang bukti digital yang telah dikumpulkan. Pemeriksaan dilakukan dengan mengekstraksi informasi yang relevan, menghilangkan data yang tidak berkaitan dengan kasus, serta menyiapkan data agar dapat dianalisis lebih lanjut.

c. Analysis

Tahap Analysis merupakan proses menganalisis hasil pemeriksaan untuk memperoleh informasi yang dapat menjelaskan penyebab, pola, serta kronologi insiden. Pada tahap ini, investigator menghubungkan berbagai artefak digital sehingga dapat mengidentifikasi aktivitas pelaku, waktu kejadian, serta bukti pendukung lainnya.

d. Reporting

Tahap Reporting merupakan proses penyusunan laporan hasil investigasi. Laporan berisi tahapan investigasi, metode yang digunakan, barang bukti yang ditemukan, hasil analisis, serta kesimpulan yang dapat dipertanggungjawabkan secara ilmiah maupun hukum.

2.2.2.3 Alasan Memilih Metode NIST

Metode NIST dipilih dalam penelitian ini karena memiliki tahapan investigasi yang sederhana, sistematis, dan mudah diterapkan pada berbagai jenis investigasi digital. Selain itu, metode ini merupakan salah satu framework yang paling banyak digunakan dalam penelitian digital forensik karena mampu menjaga integritas barang bukti digital serta menghasilkan proses investigasi yang terdokumentasi dengan baik.

Tahapan yang dimiliki metode NIST juga sesuai dengan kebutuhan penelitian ini karena memungkinkan proses investigasi dilakukan secara bertahap,

mulai dari pengumpulan access log dan error log, pemeriksaan artefak digital, analisis pola serangan brute force, hingga penyusunan laporan hasil investigasi. Dengan demikian, metode NIST dinilai mampu mendukung proses rekonstruksi kronologi serangan secara sistematis.

Berdasarkan empat tahapan dalam metode NIST, implementasi setiap tahapan pada penelitian ini dapat dijelaskan sebagaimana disajikan pada Tabel 2.2.

Tabel 2.2 Implementasi Tahapan NIST Pada Penelitian

Tahapan NIST	Implementasi pada Penelitian
Collection	Mengumpulkan access log dan error log dari web server setelah simulasi serangan brute force.
Examination	Memeriksa isi log server, menyeleksi data yang relevan, serta mengidentifikasi artefak digital seperti alamat IP, timestamp, URL, metode HTTP, dan status code.
Analysis	Menganalisis pola serangan brute force, menghubungkan artefak digital, serta merekonstruksi kronologi serangan berdasarkan hasil analisis log server.
Reporting	Menyusun laporan hasil investigasi yang berisi proses investigasi, temuan barang bukti digital, hasil analisis, dan kesimpulan penelitian.

2.2.2.4 Kaitan Metode NIST dengan Penelitian

Penelitian ini menerapkan metode Digital Forensic NIST sebagai pedoman utama dalam proses investigasi serangan *brute force* pada sistem login website berbasis PHP. Keempat tahapan dalam metode NIST digunakan untuk mengumpulkan, memeriksa, menganalisis, dan melaporkan bukti digital yang diperoleh dari *access log* dan *error log web server*.

Melalui penerapan metode tersebut, penelitian ini diharapkan mampu menghasilkan proses investigasi yang sistematis, menjaga integritas bukti digital, serta memberikan rekonstruksi kronologi serangan yang akurat. Selain itu, hasil investigasi diharapkan dapat menjadi dasar dalam mengidentifikasi pola serangan, sumber serangan, serta rekomendasi untuk meningkatkan keamanan sistem login website berbasis PHP.

2.2.3. Serangan Brute Force

2.2.3.1 Definisi Serangan Brute Force

Serangan *brute force* merupakan salah satu bentuk serangan siber yang dilakukan dengan mencoba berbagai kombinasi *username* dan *password* secara berulang hingga berhasil memperoleh akses ke dalam suatu sistem. Serangan ini memanfaatkan metode *trial and error* yang dijalankan secara otomatis menggunakan perangkat lunak tertentu sehingga mampu melakukan ribuan hingga jutaan percobaan autentikasi dalam waktu yang relatif singkat (Pradana Aji, Prayudi, & Luthfi, 2023; Krombholz, Hobel, Huber, & Weippl, 2021).

Serangan *brute force* umumnya menargetkan mekanisme autentikasi pada aplikasi web yang tidak menerapkan kontrol keamanan secara memadai. Tidak adanya pembatasan jumlah percobaan login (*login rate limiting*), penggunaan kata

sandi yang lemah, serta tidak diterapkannya autentikasi multi-faktor (*Multi-Factor Authentication/MFA*) dapat meningkatkan peluang keberhasilan serangan dan mengakibatkan akses tidak sah ke dalam sistem (Alsmadi & Xu, 2022; Pradana Aji, Prayudi, & Luthfi, 2023). Selain menyebabkan akses tidak sah ke dalam sistem, serangan *brute force* juga dapat menjadi tahap awal bagi pelaku untuk melakukan pencurian data, eskalasi hak akses, maupun penyebaran malware. Oleh karena itu, proses identifikasi dan investigasi terhadap serangan brute force menjadi salah satu aspek penting dalam menjaga keamanan aplikasi web.

2.2.3.2 Jenis-Jenis Serangan Brute Force

Menurut Tanriverdi (2024), serangan *brute force* memiliki beberapa variasi berdasarkan teknik yang digunakan oleh penyerang. Variasi tersebut bertujuan untuk meningkatkan peluang keberhasilan dalam memperoleh kredensial pengguna dengan memanfaatkan karakteristik sistem autentikasi yang menjadi target. Jenis-jenis serangan *brute force* yang umum dijumpai dapat dilihat pada Tabel 2.3.

Tabel 2.3 Jenis-Jenis Serangan Brute Force

Jenis Serangan	Penjelasan
Simple Brute Force	Mencoba seluruh kemungkinan kombinasi kata sandi hingga menemukan kombinasi yang benar.
Dictionary Attack	Menggunakan daftar kata sandi (dictionary) yang umum digunakan sebagai bahan percobaan login.
Hybrid Attack	Menggabungkan metode dictionary attack dengan penambahan karakter, angka, atau simbol sehingga

	menghasilkan variasi kata sandi yang lebih banyak.
Credential Stuffing	Menggunakan pasangan username dan password yang diperoleh dari kebocoran data sebelumnya untuk mencoba masuk ke sistem lain.
Reverse Brute Force	Menggunakan satu kata sandi yang sama untuk diuji pada banyak akun pengguna yang berbeda.

2.2.3.3 Dampak Serangan Brute Force

Serangan *brute force* dapat menimbulkan berbagai dampak terhadap keamanan sistem informasi apabila tidak segera ditangani. Dampak yang paling umum adalah diperolehnya akses tidak sah ke akun pengguna sehingga data maupun layanan yang tersedia di dalam sistem dapat disalahgunakan.

Selain itu, serangan *brute force* dapat menyebabkan kebocoran informasi sensitif, perubahan maupun penghapusan data, gangguan terhadap ketersediaan layanan (*availability*), serta meningkatnya beban kerja server akibat banyaknya permintaan autentikasi dalam waktu singkat. Pada beberapa kasus, keberhasilan serangan *brute force* juga menjadi titik awal bagi pelaku untuk melakukan serangan lanjutan seperti *privilege escalation*, *malware deployment*, maupun pencurian data.

2.2.3.4 Mitigasi Serangan Brute Force

Upaya mitigasi diperlukan untuk mengurangi risiko keberhasilan serangan *brute force* terhadap sistem autentikasi. Beberapa mekanisme pengamanan yang dapat diterapkan meliputi pembatasan jumlah percobaan login (*rate limiting* atau

account lockout), penerapan kebijakan kata sandi yang kuat, penggunaan *Multi-Factor Authentication* (MFA), implementasi CAPTCHA, pemantauan aktivitas autentikasi, serta analisis *access log* dan *error log* secara berkala untuk mendeteksi aktivitas yang mencurigakan dan merespons insiden keamanan secara lebih cepat (Pradana Aji, Prayudi, & Luthfi, 2023; Alsmadi & Xu, 2022).

Selain mekanisme pencegahan, proses investigasi terhadap log server juga memiliki peranan penting dalam mengidentifikasi pola serangan, alamat IP penyerang, waktu kejadian, serta jumlah percobaan login yang dilakukan. Informasi tersebut dapat dimanfaatkan sebagai barang bukti digital dalam proses digital forensik dan evaluasi keamanan sistem.

2.2.3.5 Kaitan Serangan Brute Force dengan Penelitian

Penelitian ini menjadikan serangan *brute force* sebagai skenario utama dalam proses investigasi digital forensik. Serangan dilakukan terhadap sistem login website berbasis PHP untuk menghasilkan artefak digital berupa *access log* dan *error log* yang selanjutnya dianalisis menggunakan metode NIST SP 800-86.

Melalui penerapan metode tersebut, penelitian ini bertujuan mengidentifikasi alamat IP penyerang, waktu terjadinya serangan, frekuensi percobaan login, serta pola serangan yang terekam pada log server. Hasil analisis diharapkan mampu merekonstruksi kronologi serangan secara sistematis sehingga dapat menjadi dasar dalam pengambilan keputusan untuk meningkatkan keamanan sistem autentikasi website berbasis PHP.

2.2.4. Website Berbasis PHP

2.2.4.1 Pengertian Website Berbasis PHP

Website merupakan kumpulan halaman web yang saling terhubung melalui jaringan internet dan dapat diakses menggunakan *web browser*. Website berfungsi sebagai media penyampaian informasi, penyedia layanan, serta sarana interaksi antara pengguna dengan sistem. Berdasarkan cara pengolahan datanya, website dibedakan menjadi website statis dan website dinamis. Website dinamis memanfaatkan bahasa pemrograman sisi server (*server-side scripting*) sehingga mampu menghasilkan tampilan yang disesuaikan dengan permintaan pengguna serta data yang tersimpan pada basis data (Rustianto et al., 2025)

PHP (*Hypertext Preprocessor*) merupakan bahasa pemrograman *server-side* yang banyak digunakan dalam pengembangan aplikasi web dinamis. PHP bekerja dengan memproses permintaan (*request*) dari pengguna pada sisi server, kemudian menghasilkan halaman web dalam format HTML yang selanjutnya dikirimkan ke *web browser*. Selain bersifat *open source*, PHP mendukung integrasi dengan berbagai sistem manajemen basis data, seperti MySQL, PostgreSQL, dan MariaDB, sehingga banyak dimanfaatkan dalam pengembangan aplikasi web karena kemudahan implementasi, fleksibilitas, serta kompatibilitasnya dengan berbagai platform (Pressman & Maxim, 2020; Nixon, 2021).

2.2.4.2 Karakteristik Website Berbasis PHP

Website berbasis PHP memiliki beberapa karakteristik yang menjadikannya sebagai salah satu platform yang banyak digunakan dalam pengembangan aplikasi web. Pertama, PHP merupakan bahasa pemrograman

server-side yang memproses seluruh permintaan pengguna pada sisi server sebelum menghasilkan keluaran dalam bentuk halaman HTML yang ditampilkan melalui *web browser*. Kedua, PHP mendukung integrasi dengan berbagai *Database Management System* (DBMS), seperti MySQL, PostgreSQL, dan MariaDB, sehingga memudahkan pengelolaan data dalam aplikasi web. Ketiga, PHP bersifat *cross-platform*, sehingga dapat dijalankan pada berbagai sistem operasi, seperti Windows, Linux, dan macOS. Selain itu, PHP didukung oleh komunitas pengembang yang luas serta berbagai *framework* populer, seperti Laravel, CodeIgniter, dan Symfony, yang membantu proses pengembangan aplikasi menjadi lebih cepat, efisien, dan terstruktur (Nixon, 2021; Pressman & Maxim, 2020). Salah satu karakteristik website berbasis PHP adalah penerapan mekanisme autentikasi melalui formulir login (*login form*) yang menggunakan kombinasi *username* dan *password* untuk memverifikasi identitas pengguna. Mekanisme autentikasi tersebut merupakan komponen penting dalam pengendalian akses, namun juga menjadi salah satu target utama serangan siber, terutama *brute force attack*, apabila tidak dilengkapi dengan mekanisme keamanan yang memadai, seperti pembatasan percobaan login, autentikasi multi-faktor, dan kebijakan kata sandi yang kuat (Pradana Aji, Prayudi, & Luthfi, 2023; Alsmadi & Xu, 2022).

Berdasarkan karakteristik tersebut, website berbasis PHP memiliki beberapa keunggulan yang mendukung pengembangan aplikasi web. Ringkasan karakteristik website berbasis PHP disajikan pada Tabel 2.4.

Tabel 2.4 Karakteristik Website Berbasis PHP

Karakteristik	Penjelasan
---------------	------------

Server-side scripting	Pemrosesan program dilakukan di sisi server sebelum dikirim ke browser.
Open source	PHP dapat digunakan dan dikembangkan secara bebas.
Cross-platform	Dapat berjalan pada Windows, Linux, dan macOS.
Database support	Mendukung MySQL, PostgreSQL, MariaDB, SQLite, dan DBMS lainnya.
Integrasi framework	Mendukung framework seperti Laravel, CodeIgniter, dan Symfony.
Mendukung autentikasi	Umumnya digunakan untuk membangun sistem login berbasis username dan password.

2.2.4.3 Kaitan Website Berbasis PHP dengan Penelitian

Penelitian ini menggunakan website berbasis PHP sebagai objek penelitian karena PHP merupakan salah satu bahasa pemrograman yang banyak digunakan dalam pengembangan aplikasi web dan umumnya menerapkan mekanisme autentikasi menggunakan *username* dan *password*. Karakteristik tersebut menjadikan sistem login pada aplikasi PHP rentan terhadap serangan brute force apabila tidak dilengkapi dengan mekanisme pengamanan yang memadai.

Dalam penelitian ini, serangan *brute force* disimulasikan pada sistem login website berbasis PHP untuk menghasilkan artefak digital berupa *access log* dan *error log*. Selanjutnya, kedua jenis log tersebut dianalisis menggunakan metode NIST SP 800-86 guna mengidentifikasi alamat IP penyerang, waktu terjadinya serangan, frekuensi percobaan login, serta merekonstruksi kronologi serangan. Dengan demikian, website berbasis PHP berperan sebagai media implementasi dalam penerapan metode digital forensik pada penelitian ini.

2.2.5 Web Server dan Log Server

2.2.5.1 Web Server (Apache)

Web server merupakan perangkat lunak yang berfungsi menerima permintaan (*request*) dari pengguna melalui protokol HTTP atau HTTPS, memproses permintaan tersebut, kemudian mengirimkan respons (*response*) berupa halaman web atau data lainnya kepada *client*. Web server berperan sebagai penghubung antara pengguna dengan aplikasi web serta bertanggung jawab dalam mengelola komunikasi, pemrosesan permintaan, dan penyampaian informasi kepada pengguna. Dalam implementasinya, web server juga berfungsi mencatat setiap aktivitas yang terjadi selama proses komunikasi melalui berkas log, seperti *access log* dan *error log*, yang dapat dimanfaatkan sebagai sumber bukti digital dalam proses investigasi keamanan siber (Pressman & Maxim, 2020; Sommerville, 2021).

Apache HTTP Server merupakan salah satu perangkat lunak web server yang banyak digunakan dalam pengembangan aplikasi berbasis web. Apache bersifat *open source*, mendukung berbagai sistem operasi, serta kompatibel dengan bahasa pemrograman *server-side* seperti PHP. Selain melayani permintaan (*request*) dari pengguna, Apache juga menyediakan fasilitas pencatatan aktivitas (*logging*) melalui *access log* dan *error log* yang dapat dimanfaatkan untuk memantau aktivitas sistem maupun sebagai sumber bukti digital dalam proses investigasi keamanan siber (Pradana Aji, Prayudi, & Luthfi, 2023).

Dalam implementasinya, Apache secara otomatis mencatat setiap aktivitas yang terjadi pada server ke dalam file log. Informasi tersebut sangat penting dalam proses pemantauan sistem maupun investigasi insiden keamanan karena

merekam seluruh aktivitas akses pengguna dan kesalahan (*error*) yang terjadi selama server beroperasi.

2.2.5.2 Access Log

Access log merupakan berkas log yang secara otomatis mencatat seluruh permintaan (*request*) yang diterima oleh web server dari pengguna. Informasi yang tersimpan dalam *access log* meliputi alamat IP pengguna, waktu akses (*timestamp*), metode HTTP, URL yang diakses, kode status (*status code*), serta *user agent*. Data tersebut dapat dimanfaatkan untuk memantau aktivitas pengguna, mendeteksi aktivitas yang mencurigakan, serta menjadi sumber barang bukti digital dalam proses investigasi serangan siber (Pradana Aji, Prayudi, & Luthfi, 2023).

Informasi yang umumnya tersimpan pada *access log* meliputi alamat IP pengguna, waktu akses (*timestamp*), metode HTTP (GET, POST), URL yang diakses, *status code*, ukuran data yang dikirimkan, serta informasi user agent. Data tersebut dapat dimanfaatkan untuk mengidentifikasi pola akses yang normal maupun aktivitas mencurigakan seperti serangan brute force.

2.2.5.3 Error Log

Selain *access log*, web server juga menghasilkan *error log* yang berfungsi mencatat berbagai kesalahan (*error*) yang terjadi selama proses operasional aplikasi web. Informasi yang tersimpan dalam *error log* meliputi waktu terjadinya kesalahan (*timestamp*), jenis kesalahan, lokasi terjadinya kesalahan, serta pesan (*error message*) yang dihasilkan oleh server. Data tersebut dapat dimanfaatkan untuk mengidentifikasi kegagalan autentikasi, kesalahan konfigurasi, maupun aktivitas mencurigakan yang berkaitan dengan insiden keamanan siber. Oleh

karena itu, *error log* menjadi salah satu sumber barang bukti digital yang penting dalam proses investigasi digital forensik (Pradana Aji, Prayudi, & Luthfi, 2023).

Error log membantu administrator maupun investigator dalam mengidentifikasi penyebab terjadinya suatu masalah pada server. Dalam konteks digital forensik, informasi yang terdapat pada error log dapat digunakan sebagai bukti pendukung untuk memperkuat hasil analisis yang diperoleh dari access log.

2.2.5.4 Artefak Digital pada Log Server

Log server merupakan salah satu sumber barang bukti digital (*digital evidence*) yang memiliki peran penting dalam proses investigasi digital forensik. Informasi yang tersimpan pada *access log* dan *error log* dapat dimanfaatkan untuk mengidentifikasi aktivitas pengguna maupun aktivitas penyerang, seperti alamat IP, *timestamp*, URL yang diakses, metode HTTP, *status code*, serta berbagai informasi lain yang berkaitan dengan aktivitas pada sistem. Melalui analisis terhadap artefak digital tersebut, investigator dapat merekonstruksi kronologi insiden keamanan, mengidentifikasi pola serangan, serta memperoleh bukti digital yang mendukung proses investigasi serangan *brute force* (Pradana Aji, Prayudi, & Luthfi, 2023).

Untuk mempermudah identifikasi, artefak digital yang dianalisis dalam penelitian ini disajikan pada Tabel 2.5.

Tabel 2.5 Artefak Digital pada Log Server

Artefak Digital	Keterangan	Fungsi dalam Investigasi
IP Address	Alamat IP pengguna atau penyerang	Mengidentifikasi sumber serangan.
Timestamp	Tanggal dan waktu	Menentukan waktu

	aktivitas.	terjadinya serangan dan menyusun kronologi.
HTTP Method	Metode seperti GET atau POST	Mengetahui jenis permintaan yang dikirim ke server.
Request URL	Halaman atau endpoint yang diakses	Mengidentifikasi target serangan, misalnya halaman login.
HTTP Status Code	Kode respons server (200, 302, 403, 404, 500, dll.)	Mengetahui hasil dari setiap permintaan.
User Agent	Informasi browser atau aplikasi klien	Mengidentifikasi perangkat atau alat yang digunakan penyerang.

2.2.5.5 Kaitan Web Server dan Log Server dengan Penelitian

Penelitian ini menggunakan web server *Apache* sebagai lingkungan implementasi sistem login website berbasis PHP. Seluruh aktivitas yang terjadi selama simulasi serangan *brute force* direkam secara otomatis ke dalam *access log* dan *error log*. Kedua jenis log tersebut menjadi sumber utama barang bukti digital yang dikumpulkan pada tahap *Collection* dalam metode NIST SP 800-86.

Selanjutnya, informasi yang terdapat pada log server, seperti alamat IP, *timestamp*, metode HTTP, *request URL*, *status code*, dan *user agent*, diperiksa serta dianalisis untuk mengidentifikasi pola serangan dan merekonstruksi kronologi kejadian. Dengan demikian, *access log* dan *error log* berperan sebagai sumber bukti digital utama dalam proses investigasi serangan *brute force* pada sistem login website berbasis PHP.

2.2 Kerangka Berpikir

2.2.2 Diagram Kerangka Berpikir



Gambar 2.1 Kerangka Berpikir Penelitian

2.2.2.1 Penjelasan Kerangka Berpikir

Kerangka berpikir penelitian ini disusun berdasarkan fenomena meningkatnya serangan *brute force* yang menargetkan sistem login website berbasis PHP. Serangan tersebut berpotensi menyebabkan akses tidak sah ke dalam sistem apabila mekanisme autentikasi tidak dilengkapi dengan pengamanan yang memadai. Selain menimbulkan risiko kebocoran data, serangan *brute force* juga memerlukan proses investigasi untuk mengidentifikasi pelaku, pola serangan, serta kronologi kejadian.

Untuk mengatasi permasalahan tersebut, penelitian ini menerapkan pendekatan *digital forensic* dengan menggunakan metode NIST SP 800-86

sebagai pedoman investigasi. Metode tersebut terdiri atas empat tahapan, yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*, yang memungkinkan proses investigasi dilakukan secara sistematis dan tetap menjaga integritas barang bukti digital.

Barang bukti digital yang digunakan dalam penelitian ini berasal dari *access log* dan *error log* pada web server Apache. Kedua jenis log tersebut dianalisis untuk memperoleh informasi penting, seperti alamat IP penyerang, *timestamp*, metode HTTP, *request URL*, *status code*, dan *user agent*. Informasi tersebut kemudian digunakan untuk merekonstruksi kronologi serangan *brute force* serta mengidentifikasi pola aktivitas penyerang.

Hasil investigasi diharapkan dapat memberikan gambaran yang jelas mengenai proses terjadinya serangan *brute force* pada sistem login website berbasis PHP. Selain itu, hasil penelitian diharapkan dapat menjadi dasar dalam penyusunan rekomendasi untuk meningkatkan keamanan sistem autentikasi website serta menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan digital forensik dan analisis log server.

2.3 Penelitian Terdahulu

2.3.1 Penjelasan Penelitian Terdahulu

Penelitian terdahulu merupakan salah satu bagian penting dalam penyusunan karya ilmiah karena digunakan untuk mengetahui perkembangan penelitian pada bidang yang sama, mengidentifikasi metode yang telah digunakan, serta menemukan kesenjangan penelitian (*research gap*) yang masih dapat dikembangkan. Melalui kajian terhadap penelitian terdahulu, peneliti dapat membandingkan objek, metode, maupun hasil penelitian sehingga diperoleh dasar

yang kuat dalam menentukan kontribusi dan kebaruan (*novelty*) penelitian yang dilakukan.

Tabel 2.6 Penelitian Terdahulu

No	Peneliti	Judul	Metode	Hasil	Perbedaan dengan penelitian
1.		Analysis of Brute Force Attacks Using National Institute of Standards and Technology (NIST) Methods on Routers	NIST SP 800-86	Berhasil mengidentifikasi IP penyerang, waktu serangan, dan pola brute force pada router.	Penelitian dilakukan pada router, sedangkan penelitian ini berfokus pada website berbasis PHP melalui analisis access log dan error log.
2.	(Aji et al., 2023, p. 32)	Analysis of Brute Force Attack Logs Toward Nginx Web Server on Dashboard Improved Log Logging System	Investigasi Digital Forensik	Berhasil merekonstruksi aktivitas penyerang melalui analisis log server Nginx menggunakan dashboard monitoring.	Penelitian menggunakan Nginx, sedangkan penelitian ini menggunakan website PHP dengan tahapan NIST.

		Using Forensic Investigation Method			
3.	Hendrawan dkk., (2023)	Analisis Bukti Digital pada Discord Browser Menggunakan Teknik Live Forensic dengan Metode NIST SP 800-86	NIST SP 800-86	Berhasil memperoleh artefak digital dan membuktikan efektivitas tahapan NIST dalam proses investigasi digital.	Fokus pada browser Discord, sedangkan penelitian ini berfokus pada log server website PHP.
4.	(Rasyid & Zen, 2023)	Dead Forensic Analysis of Qutebrowser and LibreWolf Browsers Using the NIST 800-86 Method	NIST SP 800-86	Mengidentifikasi artefak digital dari browser menggunakan tahapan NIST.	Objek penelitian berupa browser, bukan sistem login website.
5.	Atul Raj, dkk., (2024)	Brute Forcing on Secured Shell Servers Emphasizing the Role of	Cyber Forensic	Menunjukkan bahwa digital forensik dapat digunakan untuk mengidentifikasi aktivitas brute force	Objek penelitian berupa SSH Server, bukan website berbasis PHP.

		Cyber Forensics		pada server SSH.	
6.	Hanaputra, dkk., (2024)	Identifikasi Digital Evidence dalam Transaction Fraud pada WhatsApp Desktop Berdasarkan Metode NIST SP 800-86	NIST SP 800-86	Berhasil mengidentifikasi bukti digital transaksi menggunakan tahapan NIST.	Fokus pada WhatsApp Desktop, bukan analisis log server website.
7.	Syukri, dkk., (2025)	Validation and Evaluation of Browser Forensics Using Digital Forensic Approach Based on the NIST Framework	NIST Framework	Membuktikan bahwa kerangka kerja NIST efektif untuk proses validasi investigasi digital pada browser	Fokus pada browser forensic, sedangkan penelitian ini mengkaji log server website berbasis PHP.

8.	Kaestria, dkk., (2025)	Analisis Digital Forensik Pasca Serangan Ransomware LockBit 3.0 Menggunakan Metode NIST SP 800-86	NIST SP 800-86	Berhasil merekonstruksi kronologi serangan ransomware dan memperoleh artefak digital menggunakan tahapan NIST.	Fokus pada serangan ransomware, sedangkan penelitian ini berfokus pada serangan brute force pada sistem login website berbasis PHP.
----	------------------------	---	----------------	--	---

Berdasarkan Tabel 2.6, dapat diketahui bahwa sebagian besar penelitian terdahulu telah membahas penerapan digital forensik maupun mekanisme keamanan untuk menangani serangan brute force. Namun, penelitian-penelitian tersebut umumnya berfokus pada objek seperti router, server SSH, web server Nginx, media penyimpanan digital, atau pengujian penetrasi server, sehingga belum secara spesifik mengkaji sistem login website berbasis PHP.

Selain itu, penelitian sebelumnya cenderung hanya menitikberatkan pada identifikasi artefak digital, pemulihan barang bukti, deteksi serangan, atau evaluasi keamanan sistem. Penelitian yang mengintegrasikan analisis *access log* dan *error log* sebagai sumber utama barang bukti digital untuk merekonstruksi kronologi serangan brute force menggunakan tahapan *Collection*, *Examination*, *Analysis*, dan *Reporting* pada metode NIST SP 800-86 masih relatif terbatas.

Oleh karena itu, penelitian ini bertujuan mengisi kesenjangan tersebut dengan menerapkan metode Digital Forensic NIST untuk menginvestigasi

serangan brute force pada sistem login website berbasis PHP melalui analisis *access log* dan *error log*. Pendekatan ini diharapkan mampu menghasilkan proses investigasi yang lebih sistematis, memberikan rekonstruksi kronologi serangan yang lebih lengkap, serta memperkuat identifikasi bukti digital yang dapat digunakan sebagai dasar pengambilan keputusan dalam penanganan insiden keamanan siber.

BAB III

ANALISA DAN PERANCANGAN

3.1 Analisis Permasalahan

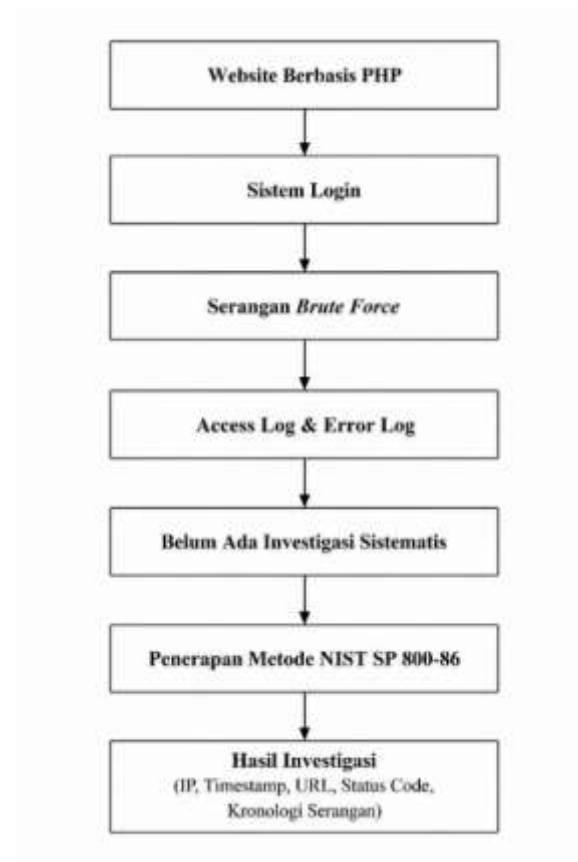
Penelitian ini berfokus pada permasalahan keamanan sistem login pada website berbasis PHP yang rentan terhadap serangan *brute force*. Serangan dilakukan dengan mencoba berbagai kombinasi *username* dan *password* secara berulang hingga memperoleh kredensial yang valid. Apabila sistem login belum menerapkan mekanisme pengamanan yang memadai, seperti pembatasan percobaan login (*rate limiting*), CAPTCHA, atau autentikasi multi-faktor, maka peluang keberhasilan serangan akan semakin besar.

Pada kondisi tersebut, web server akan menghasilkan *access log* dan *error log* yang merekam seluruh aktivitas selama proses autentikasi. Namun, data log yang tersedia umumnya hanya dimanfaatkan sebagai media pemantauan sistem dan belum dianalisis secara sistematis untuk mengungkap kronologi serangan maupun mengidentifikasi pelaku. Akibatnya, informasi penting seperti alamat IP penyerang, waktu kejadian, jumlah percobaan login, URL yang diakses, metode HTTP, serta *status code* belum dapat dimanfaatkan secara optimal sebagai barang bukti digital.

Permasalahan tersebut menyebabkan proses investigasi insiden keamanan menjadi kurang efektif karena tidak terdapat prosedur yang terstruktur dalam pengumpulan, pemeriksaan, analisis, dan pelaporan barang bukti digital. Selain itu, tanpa penerapan metode digital forensik yang baku, hasil investigasi berpotensi kurang akurat dan sulit dipertanggungjawabkan sebagai dasar pengambilan keputusan untuk meningkatkan keamanan sistem.

Berdasarkan kondisi tersebut, penelitian ini menerapkan metode *Digital Forensic NIST SP 800-86* sebagai kerangka kerja investigasi terhadap serangan *brute force* pada sistem login website berbasis PHP. Melalui tahapan *Collection*, *Examination*, *Analysis*, dan *Reporting*, penelitian ini bertujuan mengidentifikasi artefak digital yang terdapat pada *access log* dan *error log*, merekonstruksi kronologi serangan, serta menghasilkan informasi investigasi yang dapat digunakan sebagai dasar dalam memberikan rekomendasi peningkatan keamanan sistem login website

3.1.1 Diagram Alur Analisis Permasalahan



Gambar 3.1 Analisis Permasalahan Penelitian

3.2 Metodologi Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode deskriptif. Pendekatan kuantitatif dipilih karena penelitian menganalisis data yang bersifat objektif dan terukur, yaitu data yang diperoleh dari *access log* dan *error log* pada web server setelah dilakukan simulasi serangan *brute force* terhadap sistem login website berbasis PHP. Data tersebut meliputi alamat IP, *timestamp*, metode HTTP, *request URL*, *status code*, *user agent*, serta jumlah percobaan login yang selanjutnya dianalisis untuk memperoleh informasi mengenai pola dan kronologi serangan.

Metode deskriptif digunakan untuk menggambarkan secara sistematis proses investigasi digital forensik berdasarkan data yang diperoleh dari log server. Penelitian ini tidak hanya mendeskripsikan artefak digital yang ditemukan, tetapi juga menjelaskan hubungan antarartefak untuk merekonstruksi kronologi serangan *brute force* pada sistem login website berbasis PHP.

Proses penelitian diawali dengan simulasi serangan *brute force* pada sistem login website berbasis PHP untuk menghasilkan barang bukti digital berupa *access log* dan *error log*. Selanjutnya, barang bukti digital tersebut dianalisis menggunakan metode *Digital Forensic NIST SP 800-86* yang terdiri atas tahapan *Collection*, *Examination*, *Analysis*, dan *Reporting*. Melalui penerapan metode tersebut, penelitian ini bertujuan mengidentifikasi artefak digital, merekonstruksi kronologi serangan, serta menghasilkan rekomendasi yang dapat digunakan untuk meningkatkan keamanan sistem login website berbasis PHP.

3.2.2 Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan pada lingkungan pengembangan (*localhost*) menggunakan perangkat komputer pribadi yang telah dikonfigurasi sebagai web server dengan memanfaatkan Apache, PHP, dan MySQL melalui aplikasi XAMPP. Lingkungan tersebut digunakan untuk membangun sistem login website berbasis PHP, melakukan simulasi serangan *brute force*, serta memperoleh barang bukti digital berupa *access log* dan *error log* yang selanjutnya dianalisis menggunakan metode Digital Forensic NIST SP 800-86.

Waktu pelaksanaan penelitian direncanakan berlangsung pada bulan Juli 2026 sampai dengan Agustus 2026, yang meliputi tahap persiapan, perancangan sistem, simulasi serangan *brute force*, pengumpulan dan analisis log server, hingga penyusunan laporan hasil penelitian.

3.2.3 Sumber dan Teknik Pengumpulan Data

a. Sumber Data

Sumber data yang digunakan dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh secara langsung melalui simulasi serangan *brute force* pada sistem login website berbasis PHP yang dibangun dalam lingkungan pengembangan (*localhost*). Hasil simulasi tersebut menghasilkan barang bukti digital berupa *access log* dan *error log* yang menjadi objek utama dalam proses investigasi menggunakan metode Digital Forensic NIST SP 800-86.

Sementara itu, data sekunder diperoleh melalui studi literatur yang berasal dari buku, jurnal ilmiah, standar NIST SP 800-86, dokumentasi Apache HTTP Server, dokumentasi PHP, serta referensi lain yang berkaitan dengan digital forensik, serangan *brute force*, keamanan aplikasi web, dan analisis log server. Data

sekunder digunakan sebagai landasan teori dan pendukung dalam proses analisis hasil penelitian.

b. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini meliputi:

1. Studi Literatur

Studi literatur dilakukan dengan mengumpulkan dan mempelajari berbagai referensi yang berkaitan dengan digital forensik, metode NIST SP 800-86, serangan *brute force*, website berbasis PHP, serta analisis *access log* dan *error log*. Referensi tersebut diperoleh dari buku, jurnal ilmiah, standar resmi, dan dokumentasi teknis yang relevan dengan penelitian.

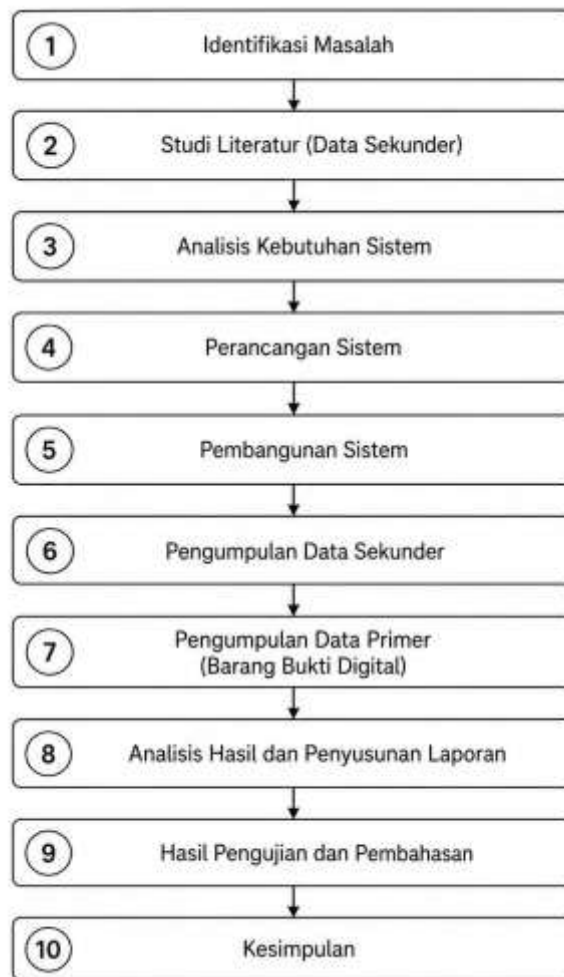
2. Simulasi Serangan Brute Force

Simulasi dilakukan terhadap sistem login website berbasis PHP yang telah dibangun pada lingkungan pengembangan (*localhost*). Simulasi ini bertujuan menghasilkan aktivitas serangan yang terekam pada *access log* dan *error log* sebagai sumber barang bukti digital dalam penelitian.

3. Dokumentasi

Dokumentasi dilakukan dengan mengumpulkan dan menyimpan seluruh data yang dihasilkan selama proses penelitian, meliputi konfigurasi sistem, hasil simulasi serangan, file *access log*, file *error log*, tangkapan layar (*screenshot*), serta hasil analisis yang digunakan sebagai pendukung penyusunan laporan penelitian.

3.2.4 Tahapan Penelitian



Gambar 3.2 Tahapan Penelitian

1. Identifikasi Permasalahan

Tahap ini dilakukan untuk mengidentifikasi permasalahan keamanan pada sistem login website berbasis PHP yang rentan terhadap serangan *brute force*. Hasil identifikasi digunakan sebagai dasar dalam menentukan tujuan, rumusan masalah, serta ruang lingkup penelitian.

Berdasarkan flowchart tahapan penelitian, setiap tahapan penelitian dapat dijelaskan sebagai berikut.

2. Studi Literatur

Pada tahap ini dilakukan pengumpulan data sekunder yang bertujuan untuk memperoleh landasan teori dan informasi pendukung yang relevan dengan penelitian. Data sekunder diperoleh dari berbagai sumber, seperti buku, jurnal ilmiah, standar digital forensik, serta dokumentasi teknis yang berkaitan dengan sistem login berbasis PHP, serangan brute force, analisis log server, dan metode digital forensik NIST SP 800-86. Data sekunder ini digunakan sebagai acuan dalam perancangan sistem, pelaksanaan investigasi digital, serta analisis hasil penelitian.

Tabel 3.1 Data Sekunder

No	Data Sekunder	Kegunaan
1	Standar NIST SP 800-86	Pedoman tahapan investigasi digital (Collection, Examination, Analysis, Reporting).
2	Buku Digital Forensik	Landasan teori digital forensik.
3	Jurnal tentang Brute Force	Referensi mengenai karakteristik serangan brute force dan penelitian terdahulu.
4	Dokumentasi Apache Web Server	Mengetahui struktur dan fungsi access.log serta error.log.
5	Dokumentasi PHP	Referensi pengembangan sistem login berbasis PHP.
6	Dokumentasi MySQL	Referensi pengelolaan database pengguna.

Berdasarkan Tabel 3.1, data sekunder yang diperoleh berasal dari berbagai sumber referensi, seperti standar NIST SP 800-86, buku, jurnal ilmiah, serta dokumentasi resmi Apache HTTP Server, PHP, dan MySQL. Data sekunder tersebut digunakan sebagai landasan teori dalam memahami konsep digital forensik, karakteristik serangan brute force, serta mekanisme analisis log server. Selain itu, data sekunder juga menjadi acuan dalam perancangan dan pembangunan sistem login berbasis PHP serta pedoman dalam menerapkan tahapan investigasi digital forensik menggunakan metode NIST SP 800-86.

3. Analisis Kebutuhan Sistem

Tahap ini dilakukan untuk mengidentifikasi kebutuhan sistem yang akan dibangun, baik kebutuhan fungsional maupun kebutuhan nonfungsional. Hasil analisis digunakan sebagai acuan dalam merancang sistem login website yang sesuai dengan kebutuhan penelitian.

4. Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem yang meliputi penyusunan algoritma sistem, *use case diagram*, *class diagram*, serta rancangan antarmuka (*user interface*). Hasil perancangan menjadi pedoman dalam proses pembangunan sistem.

5. Pembangunan Sistem

Tahap pembangunan sistem dilakukan dengan mengimplementasikan hasil perancangan ke dalam sebuah website berbasis PHP menggunakan Apache, PHP, dan MySQL. Sistem yang telah dibangun selanjutnya digunakan sebagai objek penelitian dalam proses simulasi serangan.

6. Pengumpulan Data Sekunder

Pada tahap ini peneliti mengumpulkan data pendukung yang berkaitan dengan objek penelitian, seperti dokumen organisasi, laporan kegiatan, data kebutuhan sistem, atau dokumen lain yang diperlukan sebagai bahan analisis dan implementasi sistem.

7. Pengumpulan Data Primer (Barang Bukti Digital)

Tahap ini dilakukan dengan mengumpulkan data primer berupa barang bukti digital yang akan menjadi objek penelitian. Proses pengumpulan dilakukan sesuai prosedur yang berlaku agar keaslian dan integritas data tetap terjaga.

Tabel 3.2 Data Primer

No	Data Primer	Sumber Data	Tujuan Penggunaan
1	Access Log (access.log)	Web Server Apache	Mengidentifikasi aktivitas akses, alamat IP, waktu akses, metode HTTP, dan status respons server.
2	Error Log (error.log)	Web Server Apache	Mengidentifikasi kesalahan yang terjadi selama proses pengujian.
3	Login Activity Log	Sistem Login PHP	Mengidentifikasi aktivitas login, username, alamat IP, waktu login, dan status autentikasi.

4	Hasil Simulasi Serangan <i>Brute Force</i>	Lingkungan pengujian	Menghasilkan aktivitas serangan sebagai objek investigasi digital forensik.
5	Dokumentasi Pengujian (<i>Screenshot</i>)	Proses pengujian	Mendukung dokumentasi pelaksanaan penelitian dan hasil investigasi.

Berdasarkan Tabel 3.2, data primer penelitian akan diperoleh melalui proses simulasi serangan *brute force* terhadap sistem login berbasis PHP. Simulasi tersebut akan menghasilkan barang bukti digital berupa *access log*, *error log*, *login activity log* (jika diterapkan), hasil simulasi serangan, dan dokumentasi pengujian. Seluruh data primer tersebut akan digunakan sebagai objek investigasi digital forensik menggunakan metode NIST SP 800-86.

8. Analisis Hasil dan Penyusunan Laporan

Data yang telah diperoleh dianalisis untuk mengetahui hasil implementasi sistem, kemudian disusun ke dalam bentuk laporan penelitian secara sistematis sesuai dengan metode yang digunakan.

9. Hasil Pengujian dan Pembahasan

Hasil penelitian disajikan dalam bentuk pembahasan yang menjelaskan kinerja sistem, hasil analisis data, serta pencapaian tujuan penelitian. Selanjutnya seluruh hasil penelitian disusun menjadi laporan akhir.

10. Kesimpulan

Tahap terakhir merupakan penarikan kesimpulan berdasarkan hasil penelitian yang telah dilakukan. Kesimpulan disusun untuk menjawab rumusan masalah serta memberikan rekomendasi yang diharapkan dapat menjadi masukan dalam meningkatkan keamanan sistem login website berbasis PHP terhadap serangan *brute force*.

3.3 Algoritma Sistem

Algoritma sistem merupakan rangkaian langkah yang disusun secara sistematis untuk menggambarkan mekanisme kerja sistem dalam menyelesaikan suatu proses. Pada penelitian ini, algoritma sistem digunakan untuk menjelaskan alur kerja sistem login berbasis PHP, proses simulasi serangan *brute force*, pengumpulan barang bukti digital, serta tahapan investigasi menggunakan metode Digital Forensik NIST SP 800-86 melalui analisis log server. Dengan adanya algoritma sistem, proses penelitian dapat dilakukan secara terstruktur sehingga memudahkan dalam memahami alur pengolahan data dan proses investigasi digital forensik.

3.3.1 Tahapan Algoritma Sistem

1. Memulai Sistem

Tahap awal menjalankan web server Apache, database MySQL, dan aplikasi login berbasis PHP. Pada tahap ini sistem dipastikan dapat berjalan dengan baik sehingga siap menerima permintaan (*request*) dari pengguna maupun proses pengujian.

2. Mengakses Halaman Login

Pada tahap ini, pengguna membuka halaman login melalui browser. Sistem menampilkan form login yang berisi kolom username dan password.

3. Proses Autentikasi

Tahap ini, pengguna memasukkan username dan password. Sistem memverifikasi data tersebut dengan data yang tersimpan pada database. Apabila data sesuai maka pengguna berhasil masuk ke sistem. Sebaliknya, apabila data tidak sesuai maka sistem menolak akses dan menampilkan pesan kesalahan.

4. Pencatatan Aktivitas Login

Pada tahap ini, setiap aktivitas login, baik berhasil maupun gagal, secara otomatis dicatat oleh web server ke dalam file *access.log* dan *error.log*. Apabila sistem dilengkapi dengan *login activity log*, maka aktivitas autentikasi juga akan dicatat oleh aplikasi.

5. Simulasi Serangan *Brute Force*

Pada tahap ini, melakukan simulasi serangan *brute force* terhadap halaman login menggunakan tools pengujian pada lingkungan yang telah disiapkan. Tujuan simulasi ini adalah menghasilkan aktivitas serangan yang akan terekam pada log server.

6. Pengumpulan Barang Bukti Digital

Seluruh log yang dihasilkan selama proses simulasi dikumpulkan sebagai data primer penelitian. Barang bukti digital meliputi file *access.log*, *error.log*, *login activity log* (jika digunakan), serta dokumentasi hasil pengujian.

7. Investigasi Menggunakan Metode NIST SP 800-86

Barang bukti digital dianalisis menggunakan tahapan Digital Forensik

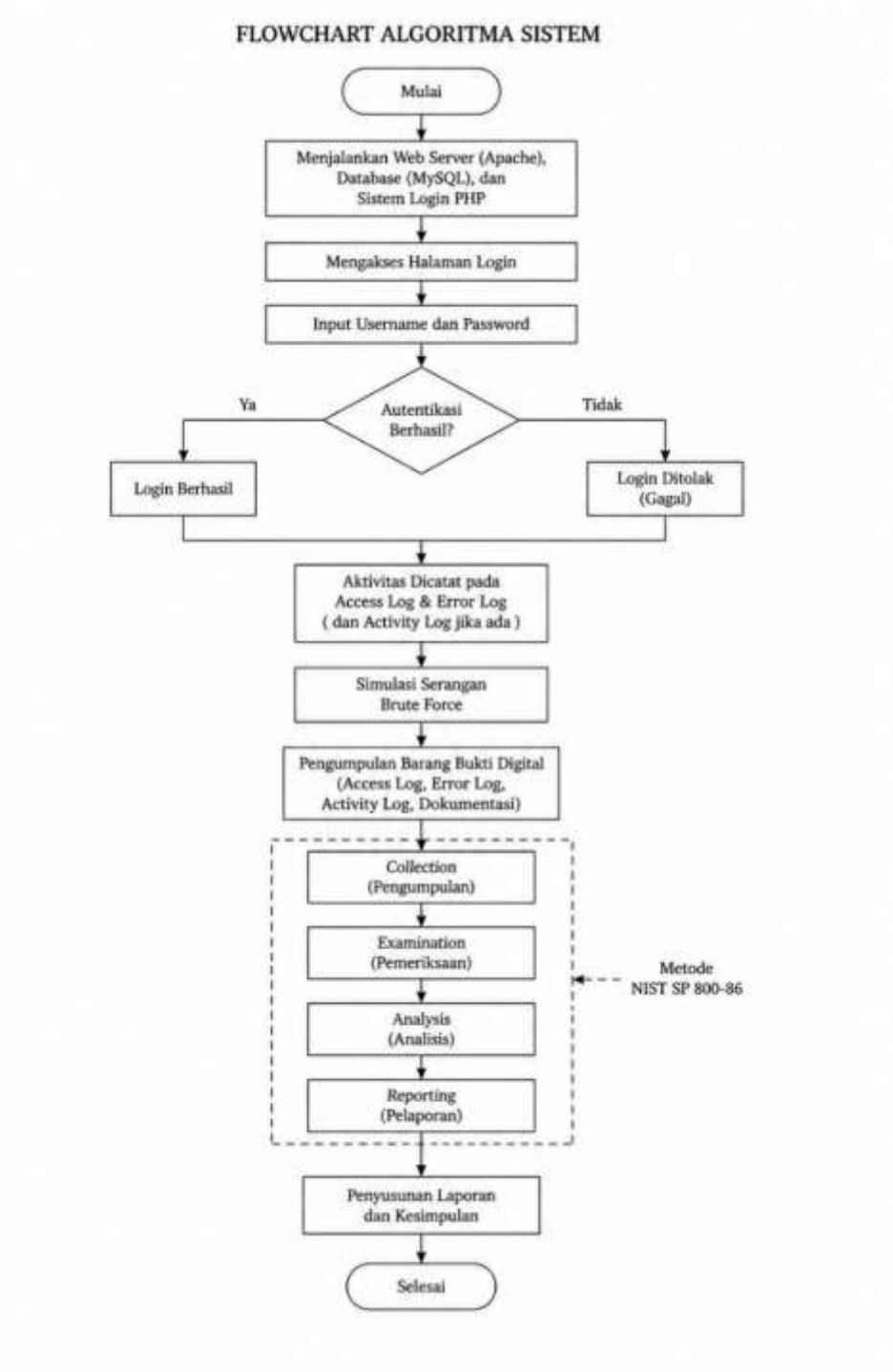
NIST SP 800-86, yaitu:

- a. Collection : Mengumpulkan barang bukti digital.
- b. Examination : Memeriksa dan menyaring data log yang relevan.
- c. Analysis : Menganalisis pola serangan berdasarkan alamat IP, waktu, jumlah percobaan login, dan status autentikasi.
- d. Reporting : Menyusun laporan hasil investigasi.

Penyusunan Laporan dan Kesimpulan

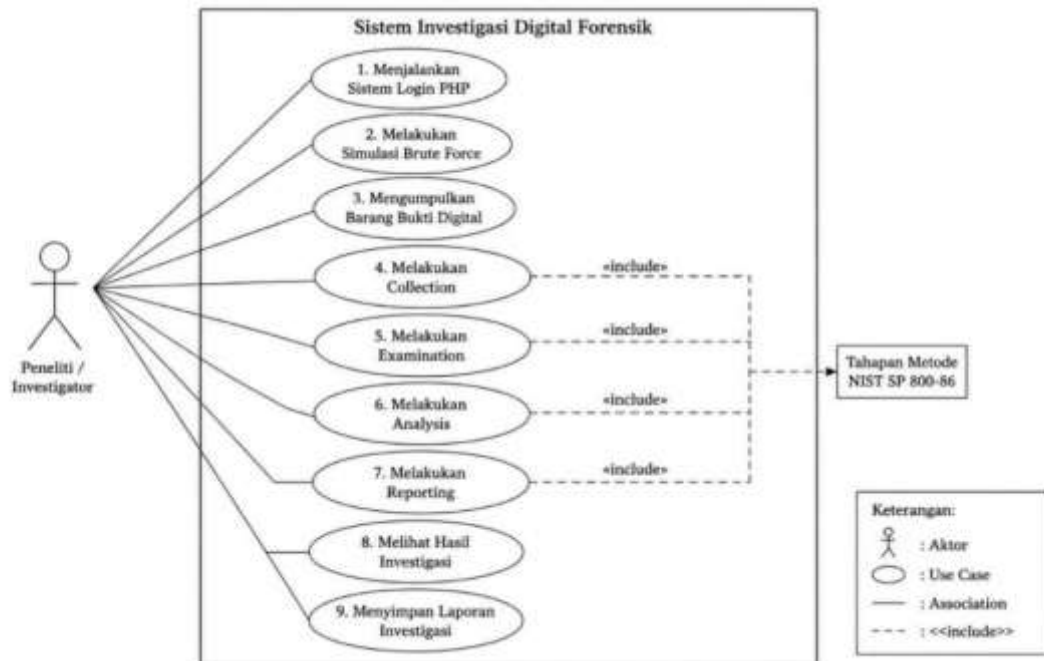
Hasil investigasi digunakan sebagai dasar penyusunan laporan penelitian serta penarikan kesimpulan mengenai penerapan metode NIST dalam mengidentifikasi serangan *brute force* melalui analisis log server.

Alur keseluruhan proses algoritma ditunjukkan pada gambar 3.3



Gambar 3.3 Alur Proses Algoritma Metode NIST SP 800-86

3.3.2 Use Case Diagram



Gambar 3.4 Use Case Diagram Sistem Investigasi Serangan Brute Force Menggunakan Metode Digital Forensik NIST pada Sistem Login PHP.

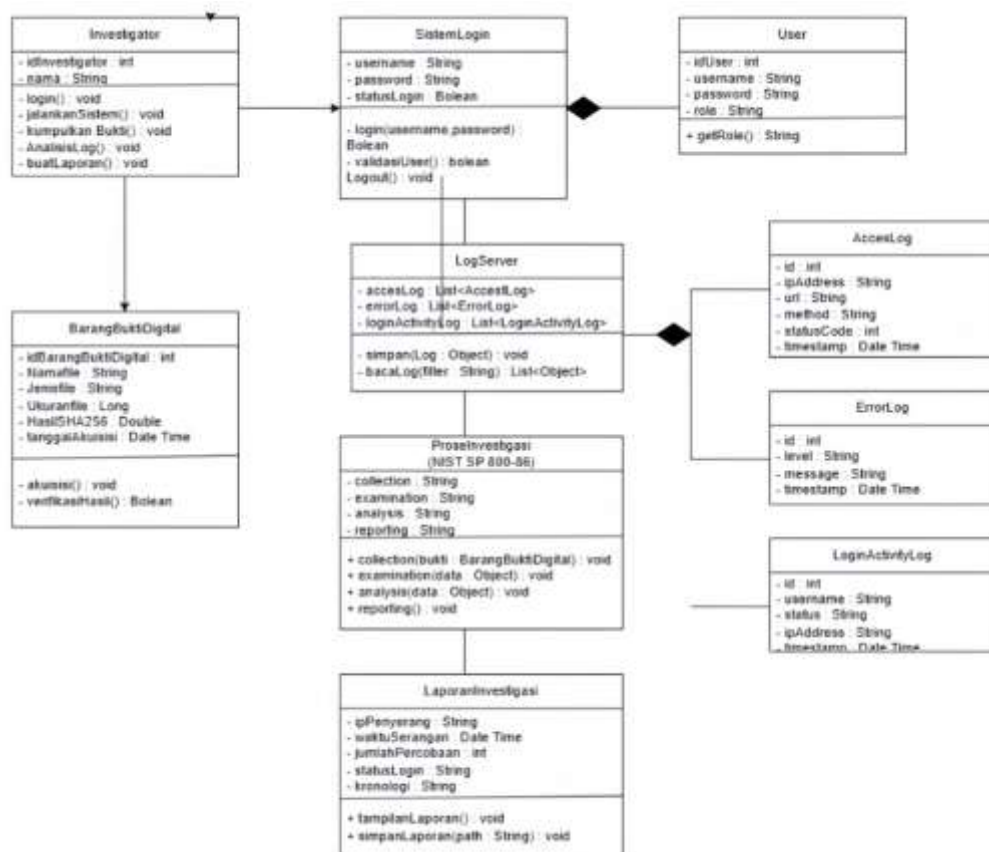
Use case diagram pada Gambar 3.4 menggambarkan satu aktor yaitu investigator, dengan Sistem Investigasi Serangan Brute Force Menggunakan Metode Digital Forensik NIST pada Sistem Login PHP.

Investigator merupakan aktor utama yang berinteraksi langsung dengan sistem selama proses penelitian. Aktor bertanggung jawab menjalankan seluruh tahapan investigasi digital forensik, mulai dari menyiapkan sistem, melakukan simulasi serangan *brute force*, mengumpulkan barang bukti digital, hingga menyusun dan menyimpan laporan hasil investigasi.

Investigator dalam system ini adalah aktor utama yang berinteraksi langsung dengan sistem investigasi serangan *brute force*. Aktor ini berperan

menjalankan seluruh proses investigasi, mulai dari menjalankan sistem login berbasis PHP, melakukan simulasi serangan *brute force*, mengumpulkan barang bukti digital, menerapkan tahapan metode Digital Forensik NIST SP 800-86 (Collection, Examination, Analysis, dan Reporting), hingga melihat serta menyimpan laporan hasil investigasi. Examination, Analysis, dan Reporting), hingga melihat serta menyimpan laporan hasil investigasi.

3.3.3 Class Diagram



Gambar 3.5 Class Diagram Sistem Investigasi Serangan Brute Force Menggunakan Metode Digital Forensik NIST pada Sistem Login PHP.

Diagram pada gambar tersebut menggambarkan alur kerja Sistem Investigasi Serangan Brute Force Menggunakan Metode Digital Forensik NIST

pada Sistem Login PHP. Sistem hanya melibatkan satu aktor saja, yaitu investigator, serta beberapa komponen utama yang saling berhubungan.

Investigator merupakan aktor utama yang berinteraksi secara langsung dengan sistem investigasi serangan *brute force*. Dalam penelitian ini, Investigator berperan sebagai pengguna yang bertanggung jawab mengelola seluruh data yang digunakan selama proses investigasi digital forensik. Pengelolaan data dilakukan sejak tahap persiapan sistem, pelaksanaan simulasi serangan, pengumpulan barang bukti digital, hingga penyusunan laporan hasil investigasi. Seluruh aktivitas tersebut dilakukan untuk memperoleh informasi yang akurat mengenai serangan *brute force* pada sistem login berbasis PHP.

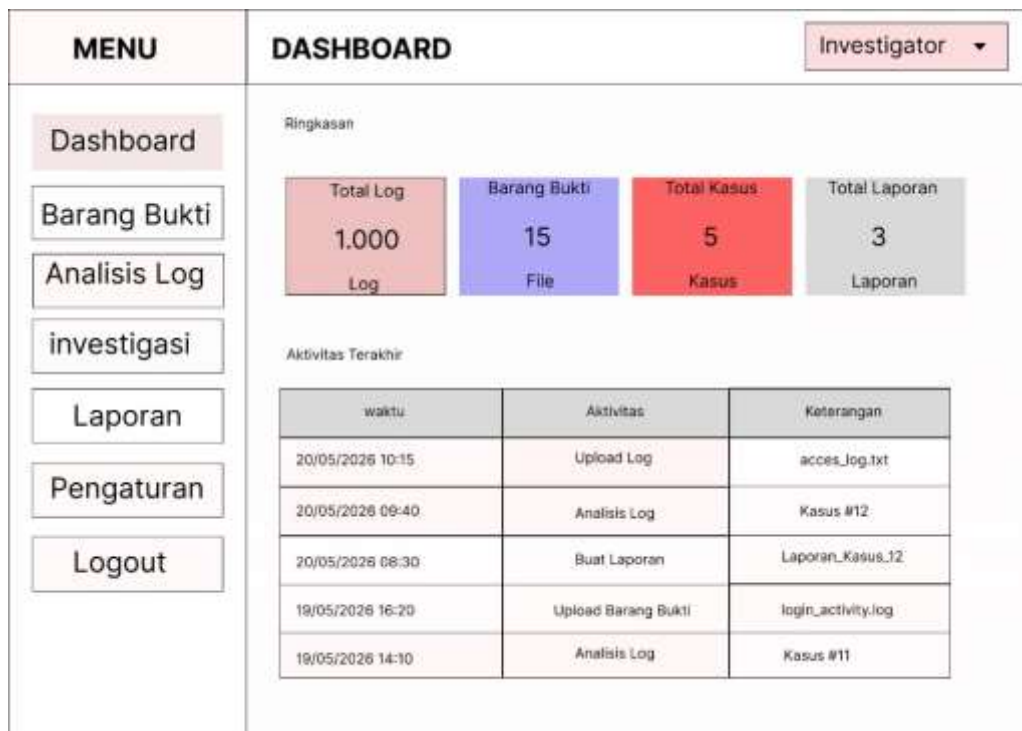
Pada tahap awal, Investigator menjalankan sistem login berbasis PHP yang telah dikembangkan sebagai objek penelitian. Sistem tersebut dikonfigurasi menggunakan web server Apache dan database MySQL sehingga mampu menerima aktivitas login dan menghasilkan file log server secara otomatis. Setelah sistem berjalan dengan baik, Investigator melakukan simulasi serangan *brute force* menggunakan tools pengujian untuk menghasilkan aktivitas serangan yang akan direkam oleh web server.

Selanjutnya, Investigator mengumpulkan seluruh barang bukti digital yang dihasilkan selama proses simulasi. Barang bukti digital tersebut meliputi file *access.log*, *error.log*, *login activity log* (jika diterapkan), hasil simulasi serangan *brute force*, serta dokumentasi berupa *screenshot* proses pengujian. Data-data tersebut merupakan data primer penelitian yang akan digunakan sebagai objek investigasi digital forensik.

Setelah barang bukti digital berhasil dikumpulkan, Investigator mengelola data tersebut dengan menerapkan tahapan metode Digital Forensik NIST SP 800-86. Tahap *Collection* dilakukan untuk mengidentifikasi dan mengumpulkan barang bukti digital yang relevan. Selanjutnya, pada tahap *Examination*, Investigator memeriksa dan menyaring data log untuk memperoleh informasi penting seperti alamat IP, waktu akses, metode HTTP, serta status autentikasi pengguna. Informasi yang telah diperoleh kemudian dianalisis pada tahap *Analysis* untuk mengidentifikasi pola serangan, jumlah percobaan login, akun yang menjadi target, dan kronologi serangan *brute force*. Hasil analisis tersebut kemudian didokumentasikan pada tahap *Reporting* dalam bentuk laporan investigasi digital forensik.

Dengan demikian, peran Investigator tidak hanya sebagai pengguna sistem, tetapi juga sebagai pihak yang bertanggung jawab mengelola data penelitian, memastikan proses investigasi berjalan sesuai tahapan metode NIST SP 800-86, serta menghasilkan laporan investigasi yang menjadi dasar dalam penarikan kesimpulan penelitian.

3.3.4 Rancangan Tampilan Antarmuka (UI)



Gambar 3.6 Rancangan Dashboard Sistem Investigasi Serangan Brute Force Menggunakan Metode Digital Forensik NIST pada Sistem Login PHP.

Dashboard yang dirancang pada Sistem Investigasi Serangan Brute Force Menggunakan Metode Digital Forensik NIST pada Sistem Login PHP ini bertujuan untuk menyediakan halaman utama yang menyajikan informasi penting mengenai kondisi sistem investigasi secara ringkas dan terstruktur. Halaman ini dirancang agar investigator dapat dengan mudah memantau jumlah log, barang bukti digital, kasus yang sedang ditangani, serta laporan hasil investigasi tanpa harus membuka setiap menu secara terpisah. Selain itu, dashboard juga bertujuan untuk mempermudah navigasi menuju fitur-fitur utama sistem dan memberikan informasi mengenai aktivitas terbaru yang dilakukan selama proses investigasi, sehingga proses analisis dapat dilakukan dengan lebih efektif dan efisien.

1. Dashboard (Halaman Utama)

Halaman ini berfungsi sebagai pusat informasi yang menyajikan ringkasan data investigasi secara cepat dan memudahkan pengguna dalam mengakses seluruh fitur sistem. Pada halaman ini ditampilkan informasi berupa jumlah log yang telah dikumpulkan, jumlah barang bukti digital, jumlah kasus yang sedang ditangani, serta jumlah laporan investigasi yang telah dibuat. Selain itu, terdapat tabel aktivitas terbaru yang menampilkan riwayat proses investigasi, seperti unggah log, analisis log, unggah barang bukti, dan pembuatan laporan. Melalui menu navigasi di sisi kiri, investigator dapat berpindah ke halaman Dashboard, Barang Bukti, Analisis Log, Investigasi, Laporan, Pengaturan, dan Logout. Dengan adanya halaman utama ini, investigator dapat memantau perkembangan proses investigasi secara menyeluruh dan mengakses setiap fitur sistem dengan lebih efisien.

2. Informasi Ringkas

Pada bagian atas dashboard terdapat beberapa panel ringkasan yang menampilkan informasi penting secara tepat, yaitu :

- a. Total Log : jumlah file log yang telah dikumpulkan.
- b. Barang Bukti : jumlah barang bukti digital yang telah diunggah.
- c. Total Kasus : jumlah kasus investigasi yang sedang atau telah ditangani.
- d. Total Laporan : jumlah laporan hasil investigasi yang telah dibuat.

Panel tersebut berfungsi sebagai informasi ringkas (summary panel) yang memberikan gambaran umum mengenai kondisi data investigasi, sehingga investigator dapat memantau perkembangan proses investigasi secara cepat tanpa harus membuka setiap menu secara terpisah.

3. Header Dashboard

Header dashboard berfungsi untuk menampilkan identitas halaman serta informasi akun investigator yang sedang menggunakan sistem. Pada bagian ini juga tersedia menu profil yang dapat digunakan untuk mengakses pengaturan akun atau keluar dari sistem.

4. Menu Navigasi (Sidebar)

a. Dashboard

Menampilkan ringkasan informasi sistem.

b. Barang Bukti

Mengelola data barang bukti digital yang digunakan dalam investigasi.

c. Analisis Log

Melakukan analisis terhadap file log server untuk mendeteksi aktivitas brute force.

d. Investigasi

Mengelola proses investigasi berdasarkan barang bukti dan hasil analisis.

e. Laporan

Menampilkan dan mencetak laporan hasil investigasi.

f. Pengaturan

Mengatur konfigurasi sistem atau akun pengguna.

g. Logout

Mengakhiri sesi penggunaan sistem dengan aman.

5. Tabel Aktivitas

Tabel Aktivitas Terbaru berfungsi menampilkan riwayat aktivitas investigator yang dilakukan pada sistem. Informasi yang ditampilkan meliputi waktu aktivitas, jenis aktivitas yang dilakukan, dan keterangan aktivitas. Riwayat tersebut membantu investigator memantau setiap proses investigasi yang telah dilakukan.

6. Alur Penggunaan Dashbord

Setelah berhasil login, investigator akan diarahkan ke halaman Dashboard. Pada halaman ini investigator dapat melihat ringkasan data investigasi, memantau aktivitas terbaru, kemudian memilih menu yang diperlukan, seperti mengunggah barang bukti, melakukan analisis log, memulai investigasi, atau menyusun laporan.

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem

Implementasi sistem merupakan tahap penerapan hasil perancangan sistem login berbasis PHP ke dalam bentuk sistem yang dapat dijalankan dan digunakan dalam penelitian. Sistem yang dibangun terdiri dari beberapa komponen utama, yaitu lingkungan sistem, basis data, halaman login, dan halaman dashboard. Implementasi dilakukan untuk memastikan bahwa sistem login dapat berjalan sesuai dengan fungsi yang telah dirancang sebelum digunakan sebagai lingkungan pengujian simulasi serangan *brute force*.

Sistem login yang diimplementasikan digunakan sebagai objek penelitian untuk mengamati aktivitas autentikasi pengguna. Pada tahap pengujian, sistem akan digunakan untuk melakukan simulasi percobaan login secara berulang sehingga aktivitas yang dihasilkan dapat diamati dan selanjutnya digunakan dalam proses investigasi berdasarkan metode Digital Forensic NIST.

4.1.1 Implementasi Lingkungan Sistem

Implementasi lingkungan sistem menjelaskan perangkat keras dan perangkat lunak yang digunakan untuk membangun serta menjalankan sistem login berbasis PHP. Lingkungan sistem diperlukan agar proses pengembangan, pengujian, dan simulasi serangan dapat dilakukan pada lingkungan yang telah ditentukan.

Perangkat keras yang digunakan berupa laptop atau komputer yang berfungsi sebagai media untuk menjalankan sistem, server lokal, database, serta browser yang digunakan untuk mengakses website. Spesifikasi perangkat keras yang digunakan dalam penelitian disesuaikan dengan perangkat yang digunakan secara langsung selama proses penelitian.

Perangkat lunak yang digunakan dalam implementasi sistem meliputi XAMPP sebagai lingkungan server lokal, Apache sebagai web server, PHP sebagai bahasa pemrograman yang digunakan untuk membangun sistem, MySQL sebagai sistem manajemen basis data, serta browser sebagai media untuk mengakses sistem login.

XAMPP digunakan untuk menyediakan lingkungan server lokal sehingga sistem PHP dapat dijalankan pada komputer peneliti tanpa harus menggunakan server yang tersedia secara daring. Di dalam XAMPP terdapat Apache yang berfungsi sebagai web server untuk memproses permintaan terhadap aplikasi PHP, sedangkan MySQL digunakan untuk menyimpan dan mengelola data pengguna yang diperlukan dalam proses autentikasi.

PHP digunakan untuk mengembangkan logika sistem, khususnya dalam proses penerimaan data login, validasi *username* dan *password*, serta pengaturan akses pengguna setelah proses autentikasi berhasil. Browser digunakan untuk mengakses halaman login dan dashboard yang telah dijalankan melalui server lokal.

Sistem operasi yang digunakan pada perangkat penelitian adalah windows 10. Seluruh komponen tersebut digunakan secara terintegrasi untuk mendukung proses implementasi dan pengujian sistem login.

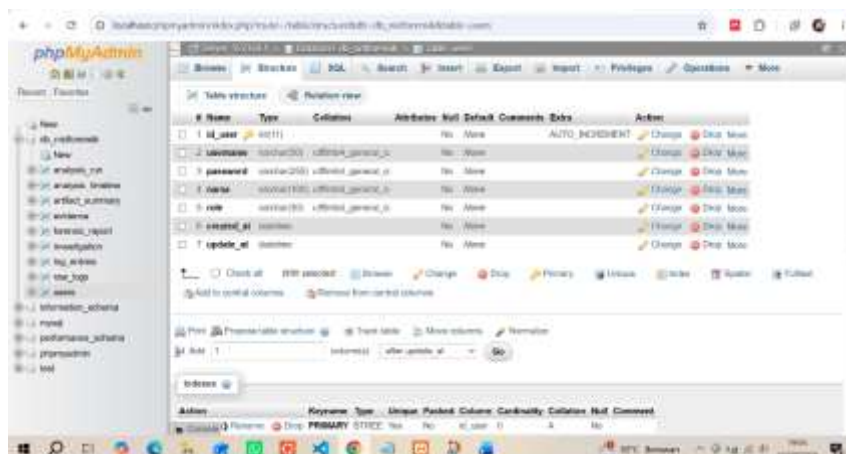
Tabel 4. 1 Lingkungan Implementasi Sistem

NO	KOMPONEN	KETERANGAN
1	Laptop	Digunakan sebagai perangkat utama penelitian
2	Sistem operasi	Windows 10
3	XAMPP	Sebagai lingkungan server lokal
4	Apache	Sebagai web server
5	PHP	Sebagai bahasa pemograman sistem
6	MySQL	Sebagai basis data
7	Browser	Digunakan untuk mengakses sistem

Berdasarkan lingkungan implementasi tersebut, sistem login dapat dijalankan secara lokal dan digunakan untuk melakukan pengujian terhadap mekanisme autentikasi sebelum dilakukan simulasi serangan *brute force*.

4.1.2 Implementasi Basis Data

Basis data digunakan untuk menyimpan data pengguna yang diperlukan dalam proses autentikasi pada sistem login. Basis data pada penelitian ini dibangun menggunakan MySQL yang dijalankan melalui XAMPP. Basis data tersebut terhubung dengan aplikasi PHP sehingga sistem dapat mengambil dan memeriksa data pengguna ketika proses login dilakukan.



Gambar 4. 1 Implementasi Basis Data Sistem

Berdasarkan Gambar 4.1, dapat dilihat basis data yang digunakan untuk mendukung proses autentikasi pada sistem. Di dalam basis data terdapat tabel pengguna yang menyimpan informasi akun yang dapat digunakan untuk melakukan login ke dalam sistem.

Tabel pengguna memiliki beberapa field yang digunakan dalam proses autentikasi, antara lain id, username, password, nama, role, created_at, dan update_at. Field id digunakan sebagai identitas unik dari setiap pengguna. Field username digunakan untuk menyimpan nama pengguna yang digunakan pada saat proses login, field password digunakan untuk menyimpan kata sandi pengguna. Field nama digunakan untuk menyimpan nama pengguna.

Selanjutnya, field role digunakan untuk menentukan peran atau hak akses pengguna dalam sistem. Dengan adanya field tersebut, sistem dapat membedakan jenis pengguna berdasarkan peran yang telah ditentukan. Sementara itu, field created_at digunakan untuk mencatat waktu ketika data pengguna dibuat dan

updated_at digunakan untuk mencatat waktu terakhir data pengguna mengalami perubahan.

Dengan struktur tersebut, basis data dapat mendukung proses autentikasi dan pengelolaan data pengguna pada sistem login. Data yang tersimpan dalam tabel pengguna selanjutnya digunakan oleh sistem ketika melakukan proses validasi *username* dan *password*. Apabila kredensial yang diberikan sesuai dengan data yang tersimpan, pengguna dapat memperoleh akses sesuai dengan *role* yang dimilikinya.

4.1.3 Implementasi Halaman Login

Halaman login merupakan halaman yang digunakan pengguna untuk melakukan proses autentikasi sebelum memperoleh akses ke dalam sistem. Halaman ini menyediakan form yang digunakan untuk memasukkan *username* dan *password*. Data yang dimasukkan kemudian diproses oleh sistem untuk menentukan apakah pengguna memiliki hak akses terhadap sistem.



Gambar 4. 2 Implementasi Halaman Login

Berdasarkan Gambar 4.2, halaman login terdiri dari beberapa komponen utama berupa input *username*, input *password*, dan tombol login. Pengguna harus memasukkan kredensial yang sesuai dengan data yang tersimpan pada basis data.

Setelah tombol login dipilih, sistem akan memproses data tersebut dan melakukan validasi terhadap data pengguna.

Apabila *username* dan *password* yang dimasukkan sesuai dengan data yang terdapat pada basis data, sistem akan memberikan akses kepada pengguna dan mengarahkan pengguna menuju halaman dashboard. Namun, apabila salah satu atau kedua data tersebut tidak sesuai, sistem akan menolak proses autentikasi dan pengguna tidak dapat mengakses dashboard.

Halaman login dalam penelitian ini memiliki peran penting karena digunakan sebagai target simulasi serangan *brute force*. Simulasi dilakukan dengan memberikan sejumlah percobaan login secara berulang menggunakan kombinasi kredensial tertentu. Percobaan tersebut dilakukan untuk menghasilkan aktivitas autentikasi yang selanjutnya dapat diamati dan dianalisis dalam proses investigasi digital.

Dengan adanya halaman login yang dapat membedakan antara autentikasi berhasil dan gagal, sistem dapat digunakan sebagai lingkungan pengujian untuk melihat karakteristik aktivitas yang muncul ketika terjadi percobaan login secara berulang. Aktivitas tersebut kemudian menjadi bagian dari data yang digunakan dalam penelitian untuk mengidentifikasi indikasi serangan *brute force*.

4.1.4 Implementasi Halaman Dashboard

Dashboard merupakan halaman yang dapat diakses oleh pengguna setelah berhasil melakukan proses autentikasi. Halaman ini berfungsi sebagai halaman utama setelah pengguna memperoleh hak akses ke dalam sistem.



Gambar 4. 3 Implementasi Halaman Dashboard

Berdasarkan Gambar 4.3, halaman dashboard dapat diakses setelah sistem berhasil memverifikasi *username* dan *password* yang dimasukkan oleh pengguna. Hal tersebut menunjukkan bahwa proses autentikasi pada sistem telah berhasil dilakukan dan pengguna memperoleh akses ke halaman yang dituju.

Dashboard pada penelitian ini tidak dikembangkan dengan fitur yang kompleks karena fokus penelitian bukan pada pengembangan aplikasi atau fitur dashboard. Dashboard hanya digunakan sebagai halaman tujuan setelah proses login berhasil sehingga dapat menunjukkan bahwa mekanisme autentikasi sistem berjalan sesuai dengan rancangan.

Keberadaan dashboard juga digunakan sebagai pembanding antara proses autentikasi yang berhasil dan proses autentikasi yang gagal. Pada autentikasi yang berhasil, pengguna dapat masuk ke dashboard, sedangkan pada autentikasi yang gagal, pengguna tidak memperoleh akses ke halaman tersebut.

Dengan demikian, implementasi halaman dashboard melengkapi mekanisme sistem login yang digunakan dalam penelitian. Sistem telah memiliki alur autentikasi mulai dari pengisian kredensial pada halaman login, proses validasi terhadap basis data, hingga pemberian akses menuju dashboard apabila

otentikasi berhasil. Sistem yang telah berjalan tersebut selanjutnya dapat digunakan sebagai lingkungan untuk melakukan simulasi serangan *brute force* dan menghasilkan aktivitas yang diperlukan dalam proses investigasi digital.

4.2 Implementasi Sistem

Implementasi sistem merupakan tahap penerapan hasil perancangan sistem login berbasis PHP ke dalam bentuk sistem yang dapat dijalankan dan digunakan pada proses pengujian. Sistem yang diimplementasikan terdiri atas database pengguna, halaman login, proses autentikasi, dashboard, serta mekanisme pencatatan aktivitas pada log server. Sistem tersebut digunakan sebagai lingkungan pengujian dalam penelitian untuk melakukan simulasi serangan *brute force* terhadap mekanisme login.

Implementasi sistem dilakukan untuk memastikan bahwa seluruh komponen yang telah dirancang dapat berjalan sesuai dengan fungsinya. Selain itu, implementasi ini bertujuan untuk menghasilkan aktivitas akses yang dapat digunakan sebagai sumber data dalam proses investigasi digital. Aktivitas yang dihasilkan selama proses login, khususnya percobaan login yang gagal secara berulang, kemudian diamati melalui log server untuk memperoleh bukti digital yang berkaitan dengan serangan *brute force*.

4.2.1 Implementasi Database

Database digunakan untuk menyimpan data yang diperlukan oleh sistem, khususnya data pengguna yang digunakan dalam proses autentikasi. Database dihubungkan dengan sistem login berbasis PHP sehingga ketika pengguna

`created_at` digunakan untuk mencatat waktu ketika data pengguna dibuat dan `updated_at` digunakan untuk mencatat waktu terakhir data pengguna mengalami perubahan.

Struktur tabel tersebut memungkinkan sistem untuk membandingkan data yang dimasukkan pengguna pada halaman login dengan data pengguna yang tersimpan di dalam database. Apabila data yang dimasukkan sesuai dengan data yang tersimpan, maka sistem akan memberikan akses kepada pengguna. Sebaliknya, apabila data tidak sesuai, sistem akan menolak proses login.

4.2.3 Implementasi Proses Autentikasi

Proses autentikasi merupakan proses pemeriksaan kredensial pengguna untuk menentukan apakah pengguna memperoleh hak akses ke dalam sistem. Proses dimulai ketika pengguna memasukkan *username* dan *password* pada halaman login.

Secara umum, proses autentikasi pada sistem dapat digambarkan sebagai berikut:

Username + Password → Validasi → Pemeriksaan Database → Hasil Autentikasi

Ketika pengguna mengirimkan data login, sistem akan melakukan validasi terhadap data yang diberikan. Selanjutnya, data tersebut dibandingkan dengan data pengguna yang tersimpan di dalam database. Apabila *username* dan *password* sesuai, proses autentikasi dinyatakan berhasil dan pengguna diarahkan menuju halaman dashboard.

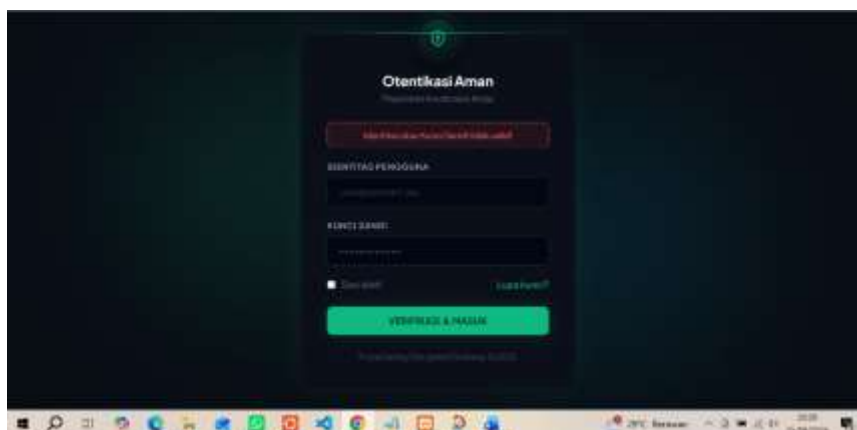
Sebaliknya, apabila data yang dimasukkan tidak sesuai, sistem akan menolak proses autentikasi dan pengguna tetap berada pada halaman login atau diarahkan kembali ke halaman login. Percobaan login yang gagal tersebut

menghasilkan aktivitas akses pada sistem yang selanjutnya dapat tercatat pada log server.



Gambar 4. 5 Proses Login Berhasil

Gambar 4.5 menunjukkan kondisi ketika pengguna memasukkan kredensial yang benar sehingga sistem berhasil melakukan autentikasi dan memberikan akses menuju dashboard.



Gambar 4. 6 Proses Login Gagal

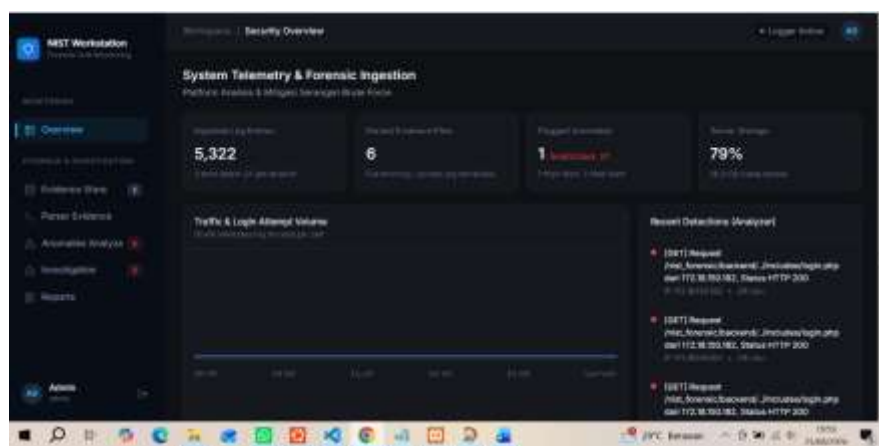
Gambar 4.6 menunjukkan kondisi ketika kredensial yang dimasukkan tidak sesuai dengan data yang terdapat pada database. Sistem menolak proses autentikasi dan pengguna tidak memperoleh akses ke halaman dashboard.

Proses login gagal tersebut menjadi bagian penting dalam penelitian karena aktivitas login yang dilakukan secara berulang dapat menghasilkan pola

aktivitas yang digunakan untuk mengidentifikasi adanya indikasi serangan *brute force*.

4.2.4 Implementasi Dashboard

Dashboard merupakan halaman yang ditampilkan setelah pengguna berhasil melakukan proses autentikasi. Halaman ini berfungsi sebagai halaman utama setelah pengguna memperoleh akses ke dalam sistem.



Gambar 4. 7 Implementasi Dashboard

Berdasarkan Gambar 4.7, dashboard dapat diakses setelah sistem berhasil melakukan verifikasi terhadap kredensial pengguna. Implementasi dashboard dalam penelitian ini tidak dibuat dengan kompleks karena fokus penelitian bukan pada pengembangan fitur dashboard, melainkan pada proses autentikasi dan investigasi terhadap aktivitas serangan *brute force* pada sistem login.

Dashboard digunakan sebagai indikator bahwa mekanisme autentikasi telah berjalan dengan baik. Ketika kredensial yang digunakan benar, pengguna dapat masuk ke dashboard, sedangkan percobaan dengan kredensial yang salah akan ditolak oleh sistem.

4.2.5 Implementasi Logging

Logging merupakan bagian yang sangat penting dalam penelitian karena digunakan untuk memperoleh data aktivitas yang terjadi pada sistem selama proses pengujian. Setiap aktivitas akses terhadap website dapat menghasilkan catatan pada log server. Data tersebut kemudian digunakan sebagai sumber bukti digital dalam proses investigasi serangan *brute force*.

Dalam penelitian ini, log yang digunakan terdiri atas `access.log` dan `error.log`. Kedua log tersebut digunakan untuk melihat aktivitas yang terjadi pada server selama sistem digunakan dan selama simulasi serangan dilakukan.

a. Implementasi `access.log`

File `access.log` digunakan untuk mencatat aktivitas permintaan atau akses yang diterima oleh server. Informasi yang terdapat dalam log dapat digunakan untuk mengetahui aktivitas akses yang terjadi selama pengujian.



```
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/js/csst/server/databases.js?v=5.1.1 HTTP/1.1" 200 4459 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36"
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_cbt1.png HTTP/1.1" 200 577 "http://localhost/phpmyadmin/themes/pmahomme/css/the
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_search.png HTTP/1.1" 200 536 "http://localhost/phpmyadmin/themes/pmahomme/css/the
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_acc.png HTTP/1.1" 200 346 "http://localhost/phpmyadmin/themes/pmahomme/css/the
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_refuse.png HTTP/1.1" 200 357 "http://localhost/phpmyadmin/themes/pmahomme/css/the
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_request=1 HTTP/1.1" 200 2286 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/server/databases/create HTTP/1.1" 200 1867 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_success.png HTTP/1.1" 200 466 "http://localhost/phpmyadmin/themes/pmahomme/css/th
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/index.php?route=/database/structure&db=distforensika&js_request=true&js_page_request=true&js_each
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_trigger.png HTTP/1.1" 200 448 "http://localhost/phpmyadmin/themes/pmahomme/css/t
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_event.png HTTP/1.1" 200 705 "http://localhost/phpmyadmin/themes/pmahomme/css/th
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_table.png HTTP/1.1" 200 571 "http://localhost/phpmyadmin/themes/pmahomme/css/t
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_routines.png HTTP/1.1" 200 346 "http://localhost/phpmyadmin/themes/pmahomme/css/t
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_proc.png HTTP/1.1" 200 479 "http://localhost/phpmyadmin/themes/pmahomme/css/t
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_err.png HTTP/1.1" 200 443 "http://localhost/phpmyadmin/themes/pmahomme/css/th
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_relations.png HTTP/1.1" 200 348 "http://localhost/phpmyadmin/themes/pmahomme/css/
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_request=1 HTTP/1.1" 200 2259 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_centralColumn.png HTTP/1.1" 200 506 "http://localhost/phpmyadmin/themes/pmahomme/c
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/js/csst/database/structure.js?v=5.2.1 HTTP/1.1" 200 4465 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/js/csst/table/change.js?v=5.2.1 HTTP/1.1" 200 20662 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_request=1 HTTP/1.1" 200 2289 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_request=1 HTTP/1.1" 200 2492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_max.png HTTP/1.1" 200 125 "http://localhost/phpmyadmin/themes/pmahomme/css/th
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/index.php?route=/database/import&db=distforensika&js_request=true&js_page_request=true&js_reload=1
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/js/csst/import.js?v=5.2.1 HTTP/1.1" 200 8630 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_request=1 HTTP/1.1" 200 2279 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/import HTTP/1.1" 200 9978 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/js/messages.php?view=5.2.1 HTTP/1.1" 200 7931 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 3474 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_request=1 HTTP/1.1" 200 2490 "-" "Mozilla/5.0 (Windows NT 10.0; Win64
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 1664 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
[11:~ - [24/Aug/2020:10:48:36 +0700] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 1664 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_err.png HTTP/1.1" 200 284 "http://localhost/phpmyadmin/themes/pmahomme/css/th
[11:~ - [24/Aug/2020:10:48:36 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_err.png HTTP/1.1" 200 284 "http://localhost/phpmyadmin/themes/pmahomme/css/th
```

Gambar 4. 8 Implementasi `access.log`

Berdasarkan Gambar 4.8, data pada `access.log` dapat memberikan informasi mengenai aktivitas akses yang dilakukan terhadap sistem. Informasi yang dapat diamati antara lain alamat IP, waktu akses (*timestamp*), metode HTTP,

Data tersebut menjadi penting dalam proses investigasi karena dapat digunakan untuk mengetahui kapan aktivitas terjadi, dari alamat IP mana aktivitas dilakukan, halaman atau sumber daya apa yang diakses, serta bagaimana server memberikan respons terhadap permintaan tersebut.

Selain access.log, penelitian ini juga menggunakan error.log sebagai sumber informasi tambahan mengenai aktivitas atau kesalahan yang tercatat pada sistem.



Berdasarkan Gambar 4.9, error.log digunakan untuk melihat catatan kesalahan atau kejadian tertentu yang dihasilkan oleh server selama sistem berjalan. Data tersebut dapat digunakan sebagai informasi pendukung dalam proses pemeriksaan terhadap aktivitas yang terjadi selama pengujian.

72

tersebut selanjutnya digunakan dalam tahapan investigasi digital berdasarkan metode NIST SP 800-86, yaitu Collection, Examination, Analysis, dan Reporting.

Dengan demikian, implementasi logging menjadi penghubung antara sistem yang telah dibangun dengan proses investigasi digital. Aktivitas yang dihasilkan dari sistem login, termasuk aktivitas login gagal yang dilakukan secara berulang pada saat simulasi *brute force*, akan menghasilkan data log yang kemudian dikumpulkan, diperiksa, dianalisis, dan dilaporkan sebagai bagian dari hasil penelitian.

4.3 Simulasi Serangan *Brute Force*

Simulasi serangan *brute force* merupakan tahap pengujian yang dilakukan untuk menghasilkan aktivitas autentikasi secara berulang pada sistem login yang telah diimplementasikan. Simulasi ini dilakukan pada lingkungan *localhost* menggunakan sistem login berbasis PHP yang telah dibuat sebelumnya. Tujuan dari simulasi adalah menghasilkan data aktivitas login yang dapat digunakan sebagai bukti digital dalam proses investigasi menggunakan metode Digital Forensic NIST.

Pada simulasi ini, percobaan login dilakukan secara berulang dengan menggunakan kombinasi *username* dan *password* yang telah ditentukan. Percobaan dilakukan pada sistem yang berada di lingkungan pengujian milik peneliti sehingga tidak melibatkan sistem atau akun milik pihak lain. Aktivitas yang dihasilkan selama simulasi kemudian diamati melalui log server, khususnya *access.log* dan *error.log*.



id_user	username	password	nama	role	created_at	update_at
1	admin	\$2y\$10\$0Auv8A8uXMaD.HsVWegDZe9ePEdRv9hXqVwMzr9ngt...	Admin	admin	2025-08-13 10:18:09	2025-08-13 10:18:09

Gambar 4. 10 Simulasi Serangan Brute Force

Gambar tersebut menunjukkan akun pengguna yang digunakan sebagai target dalam proses simulasi. Informasi sensitif seperti kata sandi tidak perlu ditampilkan secara terbuka pada gambar.

4.3.1 Menentukan Parameter Percobaan

Setelah akun target ditentukan, tahap selanjutnya adalah menentukan parameter percobaan. Parameter digunakan sebagai batasan agar proses simulasi dapat dilakukan secara terarah dan hasil pengujian dapat dicatat serta dianalisis.

Parameter percobaan meliputi alamat sistem yang digunakan, akun target, jumlah percobaan login, kombinasi kredensial yang digunakan, serta waktu pelaksanaan pengujian. Seluruh parameter ditentukan sebelum simulasi dilakukan agar setiap percobaan memiliki kondisi pengujian yang jelas.

Tabel 4. 2 Menentukan Parameter Percobaan

No	Parameter	Keterangan
1	Lingkungan	<i>Localhost</i>
2	Target	Sistem login berebasis PHP
3	Akun target	Akun pengguna yang telah dibuat pada database
4	Metode	Percobaan login berulang
5	Kredensial	Kombinasi <i>username</i> dan <i>password</i> pengujian
6	Jumlah percobaan	500
7	Waktu pengujian	24 Agustus 2026, 16:48:04
8	Data yang diamati	Aktivitas login dan log server

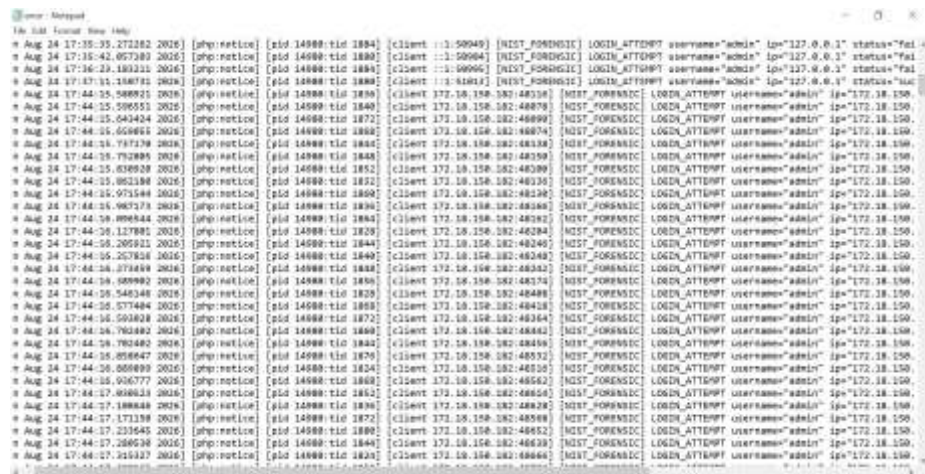
4.3.3 Melakukan Percobaan Login Berulang pada Lingkungan *Localhost*

Setelah parameter ditentukan, simulasi dilakukan dengan menjalankan sistem login pada lingkungan *localhost*. Sistem diakses melalui browser menggunakan alamat lokal yang telah ditentukan.

Percobaan login dilakukan secara berulang menggunakan kombinasi kredensial yang telah disiapkan. Pada setiap percobaan, sistem menerima data *username* dan *password*, kemudian melakukan proses validasi terhadap data yang tersimpan pada basis data.

Apabila kombinasi kredensial tidak sesuai, sistem memberikan respons berupa kegagalan autentikasi. Percobaan dilakukan secara berulang untuk menghasilkan pola aktivitas login yang menyerupai karakteristik serangan *brute force*, yaitu adanya sejumlah percobaan autentikasi dalam periode tertentu.

Selama proses tersebut, sistem tetap berjalan sebagaimana kondisi normal. Setiap permintaan yang diterima oleh server diamati untuk mengetahui aktivitas yang tercatat pada log.



```
16:00:00.000 [Info]
# Aug 24 17:35:35.27282 2026 [php:notice] [pid 14000:tid 1894] [client ::1:50949] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="127.0.0.1" status="fail"
# Aug 24 17:35:42.05780 2026 [php:notice] [pid 14000:tid 1890] [client ::1:50964] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="127.0.0.1" status="fail"
# Aug 24 17:36:23.18321 2026 [php:notice] [pid 14000:tid 1898] [client ::1:50966] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="127.0.0.1" status="fail"
# Aug 24 17:37:51.10875 2026 [php:notice] [pid 14000:tid 1890] [client ::1:51017] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="127.0.0.1" status="suc"
# Aug 24 17:44:15.50821 2026 [php:notice] [pid 14000:tid 1890] [client 172.18.150.182:48338] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.50955 2026 [php:notice] [pid 14000:tid 1840] [client 172.18.150.182:48378] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.64344 2026 [php:notice] [pid 14000:tid 1872] [client 172.18.150.182:48399] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.64665 2026 [php:notice] [pid 14000:tid 1868] [client 172.18.150.182:48374] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.78739 2026 [php:notice] [pid 14000:tid 1844] [client 172.18.150.182:48338] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.79289 2026 [php:notice] [pid 14000:tid 1848] [client 172.18.150.182:48359] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.83828 2026 [php:notice] [pid 14000:tid 1852] [client 172.18.150.182:48309] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.85238 2026 [php:notice] [pid 14000:tid 1832] [client 172.18.150.182:48338] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.97154 2026 [php:notice] [pid 14000:tid 1860] [client 172.18.150.182:48338] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:15.98737 2026 [php:notice] [pid 14000:tid 1890] [client 172.18.150.182:48348] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.00844 2026 [php:notice] [pid 14000:tid 1844] [client 172.18.150.182:48382] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.12785 2026 [php:notice] [pid 14000:tid 1828] [client 172.18.150.182:48284] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.20921 2026 [php:notice] [pid 14000:tid 1844] [client 172.18.150.182:48248] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.25784 2026 [php:notice] [pid 14000:tid 1840] [client 172.18.150.182:48248] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.27488 2026 [php:notice] [pid 14000:tid 1848] [client 172.18.150.182:48382] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.58982 2026 [php:notice] [pid 14000:tid 1848] [client 172.18.150.182:48374] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.54634 2026 [php:notice] [pid 14000:tid 1828] [client 172.18.150.182:48488] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.57748 2026 [php:notice] [pid 14000:tid 1868] [client 172.18.150.182:48428] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.59388 2026 [php:notice] [pid 14000:tid 1872] [client 172.18.150.182:48364] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.76282 2026 [php:notice] [pid 14000:tid 1840] [client 172.18.150.182:48482] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.78248 2026 [php:notice] [pid 14000:tid 1848] [client 172.18.150.182:48458] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.85847 2026 [php:notice] [pid 14000:tid 1878] [client 172.18.150.182:48532] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.88889 2026 [php:notice] [pid 14000:tid 1824] [client 172.18.150.182:48518] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:16.90677 2026 [php:notice] [pid 14000:tid 1848] [client 172.18.150.182:48542] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:17.00613 2026 [php:notice] [pid 14000:tid 1852] [client 172.18.150.182:48654] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:17.18848 2026 [php:notice] [pid 14000:tid 1890] [client 172.18.150.182:48628] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:17.17138 2026 [php:notice] [pid 14000:tid 1872] [client 172.18.150.182:48588] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:17.23545 2026 [php:notice] [pid 14000:tid 1890] [client 172.18.150.182:48632] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:17.28638 2026 [php:notice] [pid 14000:tid 1840] [client 172.18.150.182:48638] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
# Aug 24 17:44:17.31827 2026 [php:notice] [pid 14000:tid 1824] [client 172.18.150.182:48668] [NIST_FORNSICC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" status="fail"
```

Gambar 4. 11 Percobaan Login Berulang pada Lingkungan *Localhost*

Gambar tersebut menunjukkan proses pengujian terhadap halaman login pada lingkungan *localhost*. Percobaan dilakukan terhadap sistem yang telah dibangun dan bukan terhadap sistem pihak lain.

4.3.4 Mencatat Hasil Percobaan

Setiap percobaan yang dilakukan selama simulasi dicatat untuk mengetahui hasil autentikasi yang diberikan oleh sistem. Pencatatan dilakukan berdasarkan beberapa informasi yang relevan, seperti nomor percobaan, waktu percobaan, *username* yang digunakan, hasil autentikasi, serta keterangan tambahan apabila diperlukan.

Tabel 4. 3 Mencatat Hasil Percobaan

No	Waktu	Username	Hasil	Keterangan
1	16:47:24	Admin	Gagal	Username/password tidak sesuai
2	16:47:25	Admin	Gagal	Username/password tidak sesuai
3	16:47:26	Admin	Gagal	Username/password tidak sesuai
4	16:52:50	Admin	Gagal	Username/password tidak sesuai
5	17:34:38	Admin	Berhasil	Kredensial sesuai dan pengguna berhasil masuk ke dashboard

Tabel tersebut digunakan untuk mendokumentasikan aktivitas yang dilakukan selama proses simulasi *brute force*. Pencatatan hasil percobaan dilakukan berdasarkan data yang diperoleh secara langsung selama proses pengujian. Setiap percobaan dicatat berdasarkan waktu, *username*, hasil autentikasi, dan keterangan yang menunjukkan kondisi dari percobaan tersebut.

Pencatatan hasil percobaan juga digunakan untuk menghubungkan aktivitas yang dilakukan pada halaman login dengan data yang tercatat pada log server. Hasil percobaan kemudian dibandingkan dengan informasi yang terdapat pada log, seperti *timestamp*, alamat IP, URL yang diakses, dan *status code*. Perbandingan tersebut dilakukan untuk memastikan bahwa aktivitas yang dilakukan selama simulasi memiliki kesesuaian dengan catatan yang dihasilkan oleh server dan dapat digunakan sebagai data dalam proses investigasi digital.

4.3.5 Menghasilkan Access Log dan Error Log

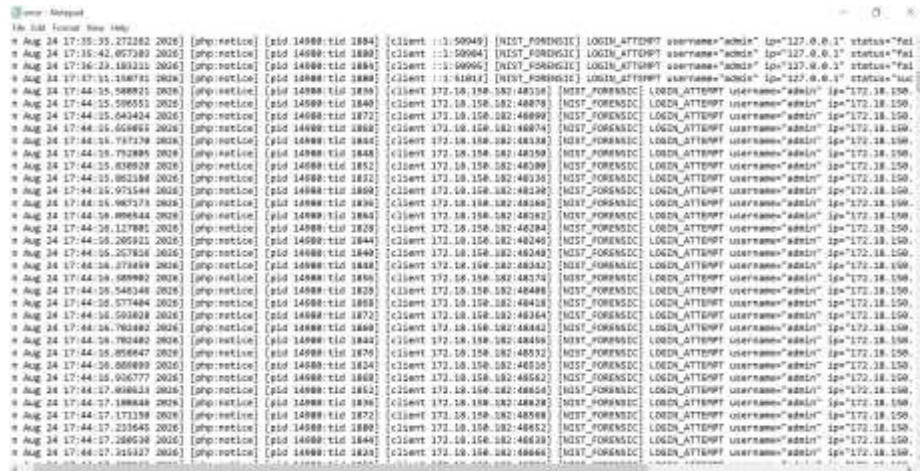
Selama simulasi berlangsung, aktivitas yang dilakukan terhadap sistem menghasilkan catatan pada log server. Log tersebut menjadi salah satu sumber bukti digital yang digunakan dalam penelitian.

File *access.log* digunakan untuk melihat aktivitas akses yang diterima oleh server. Informasi yang tersedia pada log dapat mencakup alamat IP, waktu akses, metode HTTP, URL yang diakses, dan status code sesuai dengan konfigurasi server.

```
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/js/csst/server/databases.js?v=5.2.1 HTTP/1.1" 200 4459 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_detail.png HTTP/1.1" 200 577 "http://localhost/phpmyadmin/themes/pmahomme/css/the
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_search.png HTTP/1.1" 200 536 "http://localhost/phpmyadmin/themes/pmahomme/css/the
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_asc.png HTTP/1.1" 200 248 "http://localhost/phpmyadmin/themes/pmahomme/css/theme
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_md5.png HTTP/1.1" 200 507 "http://localhost/phpmyadmin/themes/pmahomme/css/the
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_requests=1 HTTP/1.1" 200 2200 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/server/databases/create HTTP/1.1" 200 1867 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_success.png HTTP/1.1" 200 666 "http://localhost/phpmyadmin/themes/pmahomme/css/th
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/index.php?route=/database/structure&js_requests=1 HTTP/1.1" 200 2492 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_iframe.png HTTP/1.1" 200 448 "http://localhost/phpmyadmin/themes/pmahomme/css/t
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_events.png HTTP/1.1" 200 703 "http://localhost/phpmyadmin/themes/pmahomme/css/the
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_table_editor.png HTTP/1.1" 200 571 "http://localhost/phpmyadmin/themes/pmahomme/css/t
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_routine.png HTTP/1.1" 200 364 "http://localhost/phpmyadmin/themes/pmahomme/css/t
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_group.png HTTP/1.1" 200 479 "http://localhost/phpmyadmin/themes/pmahomme/css/the
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_eye.png HTTP/1.1" 200 643 "http://localhost/phpmyadmin/themes/pmahomme/css/theme.c
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_relations.png HTTP/1.1" 200 348 "http://localhost/phpmyadmin/themes/pmahomme/css/
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_requests=1 HTTP/1.1" 200 2200 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_table_columns.png HTTP/1.1" 200 500 "http://localhost/phpmyadmin/themes/pmahomme/c
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/js/csst/databases/structure.js?v=5.2.1 HTTP/1.1" 200 14685 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/js/csst/table/change.js?v=5.2.1 HTTP/1.1" 200 20062 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_requests=1 HTTP/1.1" 200 2200 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_requests=1 HTTP/1.1" 200 2492 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_requests=1 HTTP/1.1" 200 2492 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/themes/pmahomme/img/0_min.png HTTP/1.1" 200 125 "http://localhost/phpmyadmin/themes/pmahomme/css/them
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/index.php?route=/database/import&js_requests=1 HTTP/1.1" 200 2200 "-" Mozilla/5.0 (Windows NT 10.0; Win64
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/js/csst/import.js?v=5.2.1 HTTP/1.1" 200 1636 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/navigation&js_requests=1 HTTP/1.1" 200 2200 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/support HTTP/1.1" 200 8978 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
24/Aug/2020:16:48:04 +0700] "GET /phpmyadmin/js/messages.php?view=5.2.1 HTTP/1.1" 200 7931 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
24/Aug/2020:16:48:04 +0700] "POST /phpmyadmin/index.php?route=/config/get HTTP/1.1" 200 3474 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
```

Gambar 4. 12 Access Log

Sementara itu, error.log digunakan sebagai sumber informasi tambahan mengenai kesalahan atau kejadian tertentu yang tercatat pada server selama sistem berjalan.



Gambar 4. 13 Error Log

Data dari kedua log tersebut kemudian dikumpulkan sebagai bahan untuk proses investigasi digital. Informasi yang terdapat di dalam log tidak langsung dianggap sebagai serangan *brute force*, tetapi terlebih dahulu diperiksa dan dianalisis berdasarkan aktivitas pengujian yang telah dilakukan.

Hasil simulasi selanjutnya digunakan sebagai input pada tahapan investigasi menggunakan metode NIST SP 800-86, yang meliputi Collection, Examination, Analysis, dan Reporting. Pada tahap berikutnya, data log diperiksa untuk mengidentifikasi informasi yang berkaitan dengan aktivitas serangan, seperti alamat IP, waktu kejadian, URL yang diakses, status code, jumlah percobaan, serta kronologi aktivitas.

Dengan demikian, simulasi serangan *brute force* berfungsi sebagai tahap untuk menghasilkan data aktivitas yang diperlukan dalam penelitian. Data tersebut kemudian menjadi dasar dalam proses investigasi dan analisis digital untuk

mengetahui karakteristik serta bukti aktivitas *brute force* pada sistem login berbasis PHP.

4.4 Pengumpulan Barang Bukti Digital

Pengumpulan barang bukti digital merupakan tahap awal dalam proses investigasi digital setelah simulasi serangan *brute force* dilakukan. Tahap ini bertujuan untuk mengumpulkan dan mengamankan data digital yang berkaitan dengan aktivitas pengujian sehingga dapat digunakan pada tahap pemeriksaan dan analisis selanjutnya.

Dalam penelitian ini, proses pengumpulan barang bukti digital mengacu pada tahapan Collection dalam metode NIST SP 800-86. Tahap Collection dilakukan dengan mengidentifikasi sumber data yang berkaitan dengan aktivitas login dan mengumpulkan data tersebut dari lingkungan sistem yang digunakan untuk pengujian.

Barang bukti digital yang dikumpulkan berasal dari sistem login berbasis PHP yang dijalankan pada lingkungan *localhost*. Data yang dikumpulkan merupakan data yang dihasilkan selama proses implementasi dan simulasi serangan *brute force*. Pengumpulan dilakukan terhadap data yang memiliki hubungan dengan aktivitas autentikasi dan akses terhadap sistem.

Barang bukti digital yang digunakan dalam penelitian ini meliputi:

1. *access.log*, yaitu file log server yang digunakan untuk mengetahui aktivitas akses yang diterima oleh server. Informasi yang terdapat pada file ini dapat digunakan untuk melihat alamat IP, *timestamp*, URL, metode HTTP, *status code*, serta informasi akses lainnya sesuai dengan konfigurasi server.

2. *error.log*, yaitu file log server yang digunakan sebagai sumber informasi tambahan mengenai kesalahan atau kejadian tertentu yang tercatat pada server selama sistem berjalan.
3. Log aktivitas login, yaitu catatan aktivitas yang berkaitan dengan proses autentikasi pengguna, termasuk percobaan login berhasil maupun gagal yang dilakukan selama pengujian.
4. Hasil simulasi *brute force*, yaitu data yang diperoleh dari serangkaian percobaan login berulang terhadap sistem login yang telah dibuat pada lingkungan *localhost*. Data ini digunakan untuk mengetahui aktivitas yang dihasilkan selama simulasi.
5. Screenshot sistem, yaitu dokumentasi visual terhadap kondisi sistem selama penelitian, seperti halaman login, halaman dashboard, database, dan tampilan log server. Screenshot digunakan sebagai dokumentasi pendukung untuk menunjukkan kondisi sistem dan proses pengujian.
6. Hasil percobaan login, yaitu data yang mencatat hasil setiap percobaan autentikasi selama simulasi. Data tersebut dapat berupa percobaan login berhasil maupun gagal, waktu percobaan, *username* yang digunakan, serta keterangan hasil autentikasi.

4.4.1 Proses Collection

Tahap Collection dilakukan dengan mengidentifikasi dan mengumpulkan seluruh data digital yang berkaitan dengan aktivitas simulasi *brute force*. Data dikumpulkan setelah proses pengujian selesai dilakukan sehingga aktivitas yang dihasilkan selama simulasi dapat digunakan sebagai sumber bukti digital.

Proses pengumpulan diawali dengan mengidentifikasi file log yang dihasilkan oleh server Apache. File acces log dan error log diperiksa untuk memastikan bahwa data log tersedia dan dapat digunakan dalam proses investigasi. Selain kedua file tersebut, hasil pencatatan aktivitas login dan hasil simulasi juga dikumpulkan sebagai data pendukung.

Selanjutnya, data yang telah dikumpulkan disimpan dan didokumentasikan untuk menjaga ketersediaannya selama proses pemeriksaan dan analisis. Setiap barang bukti diberikan identitas atau keterangan yang sesuai dengan sumber dan jenis datanya sehingga memudahkan peneliti dalam melakukan pemeriksaan pada tahap berikutnya.

Tabel 4. 4 Daftar Barang Bukti Digital

No	Barang Bukti	Sumber	Keterangan
1	Acces log	Server Apache	Catatan aktivitas akses ke server
2	Error log	Server Apache	Catatan kesalahan atau kejadian pada server
3	Log aktivitas login	Sistem login PHP	Catatan aktivitas autentikasi
4	Hasil simulasi <i>brute</i>	Sistem login <i>localhost</i>	Data percobaan login

	<i>force</i>		berulang
5	Screenshot sistem	Sistem login dan server	Dokumentasi kondisi sistem
6	Hasil percobaan	Hasil pengujian	Catatan login berhasil dan gagal

```

# Aug 24 17:35:35.27282 2026 [php:notice] [pid 14900:tid 1894] [client ::1:50949] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.0.0.1 status=fai
# Aug 24 17:35:42.05780 2026 [php:notice] [pid 14900:tid 1894] [client ::1:50964] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.0.0.1 status=fai
# Aug 24 17:36:29.19321 2026 [php:notice] [pid 14900:tid 1894] [client ::1:50995] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.0.0.1 status=fai
# Aug 24 17:37:31.13875 2026 [php:notice] [pid 14900:tid 1894] [client ::1:51813] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.0.0.1 status=fai
# Aug 24 17:44:15.58895 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48358] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.59651 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48878] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.64344 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48899] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.65065 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48874] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.79739 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48338] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.79299 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48359] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.83929 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48389] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.85138 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48338] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.97544 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48338] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:15.98773 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48388] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.09844 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48382] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.13785 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48384] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.20592 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48348] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.25763 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48348] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.27489 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48342] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.30992 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48374] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.34034 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48488] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.37484 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48438] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.50382 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48364] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.76382 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48882] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.78382 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48858] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.80647 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48532] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.80889 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48518] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:16.90677 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48562] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:17.03623 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48654] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:17.18848 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48828] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:17.17338 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48568] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:17.23645 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48552] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:17.24634 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48638] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.
# Aug 24 17:44:17.25137 2026 [php:notice] [pid 14900:tid 1894] [client 172.18.158.182:48664] [HOST:FORENSIC] LOGIN_ATTEMPT username=admin ip=172.18.158.

```

Gambar 4. 14 Acces Log dan Error Log

Pada tahap Collection, data yang dikumpulkan belum dilakukan perubahan atau interpretasi terhadap isi bukti. Data tersebut dipersiapkan untuk memasuki tahap berikutnya, yaitu Examination. Pada tahap Examination, barang bukti yang telah dikumpulkan akan diperiksa dan diekstraksi untuk memperoleh informasi yang relevan dengan tujuan penelitian.

Pengumpulan barang bukti digital dilakukan secara terarah berdasarkan aktivitas yang terjadi selama simulasi. Dengan demikian, data yang dikumpulkan memiliki keterkaitan langsung dengan objek penelitian, yaitu investigasi serangan *brute force* pada sistem login website berbasis PHP melalui analisis log server.

Hasil dari tahap *Collection* berupa kumpulan barang bukti digital yang terdiri atas file log, data aktivitas login, hasil simulasi, dan dokumentasi sistem. Barang bukti tersebut selanjutnya digunakan sebagai sumber data pada tahap *Examination* untuk mengidentifikasi informasi yang relevan, seperti *timestamp*, alamat IP, URL, metode HTTP, *status code*, dan pola aktivitas login.

4.5 Examination

Tahap *Examination* merupakan tahap pemeriksaan terhadap barang bukti digital yang telah dikumpulkan pada tahap *Collection*. Pada tahap ini dilakukan pemeriksaan terhadap data yang terdapat pada *access.log*, *error.log*, serta data hasil simulasi dan pencatatan aktivitas login. Pemeriksaan dilakukan untuk memperoleh informasi yang relevan dengan aktivitas autentikasi dan akses terhadap sistem selama proses pengujian.

Tahap *Examination* bertujuan untuk mengidentifikasi dan mengekstraksi informasi penting dari barang bukti digital tanpa melakukan perubahan terhadap data asli. Informasi yang diperoleh dari tahap ini kemudian digunakan sebagai dasar untuk melakukan analisis pada tahap berikutnya.

Dalam penelitian ini, pemeriksaan difokuskan pada informasi yang berkaitan dengan aktivitas login dan indikasi percobaan akses secara berulang. Beberapa informasi yang diperiksa meliputi alamat IP, tanggal dan waktu kejadian, URL login, metode HTTP, *status code*, *user agent*, serta jumlah percobaan login.

4.5.1 Pemeriksaan Alamat IP

Pemeriksaan alamat IP dilakukan untuk mengetahui alamat sumber yang melakukan permintaan terhadap sistem selama proses pengujian. Informasi alamat IP diperoleh dari baris-baris yang terdapat pada access.log.

```
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/vendor/codemirror/lib/codemirror.css?v=5.2.1 HTTP/1.1" 200 8720 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/themes/pmahomme/css/themes.css?v=5.2.1 HTTP/1.1" 200 257267 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/vendor/jquery/jquery.min.js?v=5.2.1 HTTP/1.1" 200 88947 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/vendor/jquery/jquery-migrate.min.js?v=5.2.1 HTTP/1.1" 200 13467 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/vendor/sprintf.js?v=5.2.1 HTTP/1.1" 200 7469 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/dist/ejex.js?v=5.2.1 HTTP/1.1" 200 23948 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/dist/keyhandler.js?v=5.2.1 HTTP/1.1" 200 2859 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:54 +0700] "GET /phpmyadmin/js/vendor/jquery/jquery-ui.min.js?v=5.2.1 HTTP/1.1" 200 215084 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:55 +0700] "GET /phpmyadmin/js/vendor/codemirror/addon/lint/lint.css?v=5.2.1 HTTP/1.1" 200 3635 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:55 +0700] "GET /phpmyadmin/js/vendor/codemirror/addon/lint/show-hint.css?v=5.2.1 HTTP/1.1" 200 648 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
227.0.0.1 - - [24/Aug/2026:16:47:55 +0700] "GET /phpmyadmin/js/dist/name-conflict-fixes.js?v=5.2.1 HTTP/1.1" 200 43 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
```

Gambar 4. 15 Pemeriksaan Alamat IP

Alamat IP digunakan untuk mengidentifikasi sumber koneksi yang melakukan aktivitas terhadap halaman login. Karena pengujian dilakukan pada lingkungan *localhost*, alamat IP yang tercatat dapat berupa alamat lokal seperti 172.0.0.1, tergantung pada konfigurasi lingkungan pengujian.

Hasil pemeriksaan alamat IP kemudian dicatat sebagai salah satu informasi yang digunakan untuk menghubungkan aktivitas login yang dilakukan selama simulasi dengan catatan yang dihasilkan oleh server.

4.5.2 Pemeriksaan Tanggal dan Waktu

Pemeriksaan tanggal dan waktu atau *timestamp* dilakukan untuk mengetahui kapan aktivitas akses terhadap sistem terjadi. Informasi waktu diperoleh dari catatan yang terdapat pada access.log.

Timestamp menjadi informasi penting karena dapat digunakan untuk menyusun urutan kejadian selama simulasi. Dengan melihat waktu pada setiap aktivitas, peneliti dapat mengetahui kapan percobaan login pertama dilakukan, kapan percobaan berikutnya terjadi, serta rentang waktu antara satu aktivitas dengan aktivitas lainnya.

-
[24/Aug/2026:16:47:32
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:33
[24/Aug/2026:16:47:34
[24/Aug/2026:16:47:49
[24/Aug/2026:16:47:49
[24/Aug/2026:16:47:54

Gambar 4. 16 Tanggal dan Waktu
(Timestamp)

Informasi waktu yang diperoleh kemudian dibandingkan dengan waktu pelaksanaan simulasi dan hasil pencatatan percobaan login untuk memastikan kesesuaian antara aktivitas pengujian dan data log.

4.5.3 Pemeriksaan URL Login

Pemeriksaan URL dilakukan untuk mengetahui halaman atau sumber daya yang diakses selama proses pengujian. Pada penelitian ini, perhatian diberikan pada URL yang berkaitan dengan proses login.

URL yang tercatat pada access.log dapat menunjukkan permintaan yang dikirimkan menuju halaman login atau proses yang digunakan untuk melakukan autentikasi. Informasi tersebut membantu peneliti menentukan apakah aktivitas yang tercatat pada log berkaitan dengan sistem login yang menjadi objek

`"http://localhost/nist_forensic/includes/login.php"`

Gambar 4. 17 URL Login

penelitian.

Hasil pemeriksaan URL kemudian dicatat untuk digunakan pada tahap analisis dan penyusunan kronologi aktivitas.

4.5.4 Pemeriksaan Metode HTTP

Metode HTTP digunakan untuk mengetahui jenis permintaan yang dikirimkan oleh browser atau aplikasi kepada server. Metode yang umum ditemukan pada aktivitas website antara lain GET dan POST.

Pada proses login, metode POST dapat digunakan untuk mengirimkan data *username* dan *password* ke server, tergantung pada implementasi sistem. Sementara itu, metode GET dapat digunakan untuk mengakses halaman atau sumber daya tertentu.

```
::1 - - [24/Aug/2026:16:47:56 +0700] "POST
::1 - - [24/Aug/2026:16:47:56 +0700] "POST
::1 - - [24/Aug/2026:16:47:58 +0700] "POST
::1 - - [24/Aug/2026:16:47:58 +0700] "GET /
::1 - - [24/Aug/2026:16:48:04 +0700] "GET /
::1 - - [24/Aug/2026:16:48:04 +0700] "GET /
::1 - - [24/Aug/2026:16:48:04 +0700] "GET /
::1 - - [24/Aug/2026:16:48:04 +0700] "GET /
::1 - - [24/Aug/2026:16:48:04 +0700] "GET /
::1 - - [24/Aug/2026:16:48:04 +0700] "POST
::1 - - [24/Aug/2026:16:48:35 +0700] "POST
```

Gambar 4. 18 Metode HTTP

Pemeriksaan metode HTTP dilakukan untuk mengetahui jenis permintaan yang berkaitan dengan aktivitas login selama pengujian. Informasi ini selanjutnya dapat digunakan untuk membedakan permintaan akses halaman dengan permintaan yang berkaitan dengan proses autentikasi.

4.5.5 Pemeriksaan Status Code

Status code merupakan kode respons HTTP yang diberikan server setelah menerima permintaan dari pengguna atau aplikasi. Pemeriksaan *status code* dilakukan untuk mengetahui respons server terhadap setiap permintaan yang tercatat dalam `access.log`.

Beberapa *status code* yang dapat ditemukan antara lain 200 yang menunjukkan permintaan berhasil diproses, sedangkan kode lain dapat menunjukkan pengalihan, kesalahan klien, atau kesalahan server. Nilai yang sebenarnya digunakan dalam penelitian harus disesuaikan dengan *status code* yang terdapat pada log hasil pengujian.

200

200

200

Gambar 4. 19
Status Code

Pemeriksaan *status code* membantu peneliti mengetahui respons server terhadap aktivitas yang dilakukan selama simulasi. Data tersebut kemudian dapat dibandingkan dengan hasil percobaan login untuk melihat kesesuaian antara aktivitas pengujian dan respons server.

4.5.6 Pemeriksaan User Agent

User agent merupakan informasi yang dapat menunjukkan perangkat lunak atau browser yang digunakan ketika melakukan permintaan terhadap server. Informasi ini dapat digunakan sebagai data pendukung dalam pemeriksaan aktivitas akses.

Pemeriksaan *user agent* dilakukan apabila informasi tersebut tersedia pada log yang digunakan dalam penelitian. Data tersebut dapat menunjukkan jenis

```
*Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/151.0.0.0 Safari/537.36
*Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/151.0.0.0 Safari/537.36
*Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/151.0.0.0 Safari/537.36
```

Gambar 4. 20 User Agent

browser atau perangkat lunak yang digunakan untuk mengakses sistem selama proses pengujian.

Informasi *user agent* tidak digunakan sebagai satu-satunya dasar untuk menentukan adanya serangan *brute force*, tetapi digunakan sebagai informasi pendukung dalam mengidentifikasi karakteristik aktivitas yang tercatat.

4.5.7 Pemeriksaan Jumlah Percobaan Login

Pemeriksaan jumlah percobaan dilakukan dengan menghitung aktivitas login yang tercatat selama simulasi. Perhitungan dilakukan berdasarkan catatan aktivitas yang berkaitan dengan halaman atau proses autentikasi.

Jumlah percobaan login digunakan untuk mengetahui seberapa banyak permintaan autentikasi yang dilakukan selama periode pengujian. Data tersebut kemudian dibandingkan dengan hasil pencatatan percobaan login yang dilakukan secara langsung pada sistem.

Tabel 4. 5 Hasil Pemeriksaan Aktivitas Login

No	Timesta mp	Ip Addres	Url	Method	Status Code	User Agent	Ha sil
1	24/Aug /2026 : 16:47:3 2	172.18.1 50.182	"http://local host/nist forensic/incl udes/login.p hp"	POST	200	" Mozilla/5.0 (Windows NT 10.0; Win64;	Ga gal

						x64) AppleWeb Kit/537.36 (KHTML, like Gecko) Chrome/151 .0.0.0 Safari/537.3 6"	
2	24/Aug /2026 : 16:47:3 3	172.18.1 50.182	"http://local host/nist forensic/incl udes/login.p hp"	GET	200	" Mozilla/5. 0 (Windows NT 10.0; Win64; x64) AppleWeb Kit/537.36 (KHTML, like Gecko) Chrome/151 .0.0.0 Safari/537.3 6"	Ga gal
3	24/Aug /2026 : 16:47:3 4	172.18.1 50.182	"http://local host/nist_fo rensic/inclu des/login.ph p"	POST	200	"Mozilla/5. 0 (Windows NT 10.0; Win64; x64) AppleWeb Kit/537.36 (KHTML, like Gecko) Chrome/151	Ber has il

						.0.0.0 Safari/537.3 6”	
--	--	--	--	--	--	------------------------------	--

Berdasarkan hasil pemeriksaan tersebut, data dari log server telah diekstraksi ke dalam bentuk informasi yang lebih terstruktur. Informasi berupa alamat IP, *timestamp*, URL, metode HTTP, *status code*, *user agent*, dan jumlah percobaan kemudian digunakan sebagai dasar untuk melakukan analisis terhadap pola aktivitas yang terjadi selama simulasi.

Pada tahap *Examination*, data yang diperoleh belum digunakan untuk menetapkan kesimpulan akhir mengenai serangan *brute force*. Pemeriksaan hanya berfokus pada identifikasi dan ekstraksi informasi dari barang bukti digital. Penentuan pola, hubungan antaraktivitas, serta indikasi serangan dilakukan pada tahap Analysis.

4.6 Analysis

Tahap *Analysis* merupakan tahap untuk menganalisis hasil pemeriksaan barang bukti digital yang telah dilakukan pada tahap *Examination*. Pada tahap ini, informasi yang telah diperoleh dari *access.log*, *error.log*, hasil simulasi *brute force*, dan hasil pencatatan percobaan login dianalisis untuk mengetahui pola aktivitas yang terjadi pada sistem login.

Analisis dilakukan dengan menghubungkan data hasil simulasi dengan informasi yang tercatat pada log server. Tujuan dari tahap ini adalah untuk mengetahui sumber aktivitas, waktu terjadinya percobaan, frekuensi percobaan login, pola aktivitas, URL yang menjadi target, respons server, serta urutan kejadian selama proses simulasi.

Hasil analisis tersebut digunakan untuk mengetahui apakah aktivitas yang tercatat pada sistem memiliki karakteristik yang sesuai dengan pola serangan *brute force*. Penentuan tersebut dilakukan berdasarkan kesesuaian antara aktivitas yang sengaja dilakukan pada saat simulasi dengan bukti digital yang ditemukan pada log server.

4.6.1 Analisis IP Address

Analisis IP address dilakukan untuk mengetahui alamat sumber yang melakukan aktivitas akses terhadap sistem login. Informasi tersebut diperoleh dari *access.log* dan dibandingkan dengan alamat IP yang digunakan pada lingkungan pengujian.

Karena penelitian dilakukan pada lingkungan *localhost*, alamat IP yang tercatat dapat berupa alamat IP lokal, seperti 127.0.0.1, sesuai dengan konfigurasi sistem. IP address yang sama pada sejumlah aktivitas dapat menunjukkan bahwa berbagai percobaan login berasal dari sumber koneksi yang sama.

Tabel 4. 6 Analisis IP Address

No	IP Address	Jumlah Aktivitas	Keterangan
1	127.0.0.1	12	Melakukan percobaan login
2	172.18.150.182	700	Melakukan percobaan login sebanyak 700 kali, (500 berhasil dan 200 gagal)

Berdasarkan hasil tersebut, IP address digunakan sebagai salah satu indikator untuk menghubungkan sejumlah aktivitas login yang tercatat selama proses simulasi.

4.6.2 Analisis Waktu Serangan

Analisis waktu dilakukan dengan menggunakan informasi *timestamp* yang terdapat pada log. Waktu setiap aktivitas dibandingkan dengan waktu pelaksanaan simulasi untuk mengetahui kapan percobaan login terjadi.

Dengan mengurutkan *timestamp*, peneliti dapat mengetahui aktivitas pertama, aktivitas berikutnya, hingga aktivitas terakhir. Informasi tersebut digunakan untuk membentuk kronologi kejadian selama proses simulasi.

Tabel 4. 7 Analisis Waktu Aktivitas

No	Timestamp	Aktivitas	Keterangan
1	24/Aug/2026:16:47:32	Percobaan Login	Aktivitas Awal
2	24/Aug/2026:16:47:33	Percobaan Login	Aktivitas Berikutnya
3	24/Aug/2026:16:47:33	Percobaan Login	Aktivitas Berikutnya
4	24/Aug/2026:16:47:49	Percobaan Berhasil	Aktivitas Akhir

Rentang waktu antara percobaan juga dapat diamati untuk mengetahui apakah terdapat sejumlah percobaan yang terjadi dalam interval waktu yang relatif

singkat. Pola tersebut menjadi salah satu informasi pendukung dalam analisis aktivitas *brute force*.

4.6.3 Analisis Frekuensi Percobaan Login

Frekuensi percobaan login dianalisis dengan menghitung jumlah aktivitas autentikasi yang tercatat selama periode simulasi. Data tersebut diperoleh dengan mengidentifikasi permintaan yang berkaitan dengan proses login pada access.log.

Hasil perhitungan kemudian dibandingkan dengan jumlah percobaan yang dilakukan secara langsung selama simulasi. Perbandingan tersebut bertujuan untuk mengetahui kesesuaian antara aktivitas pengujian dengan aktivitas yang tercatat pada server.

Tabel 4. 8 Frekuensi Percobaan Login

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

Jumlah percobaan login yang dilakukan secara berulang dalam periode tertentu dapat menjadi salah satu karakteristik yang diamati dalam identifikasi aktivitas *brute force*. Namun, frekuensi percobaan tidak digunakan sebagai satu-satunya dasar untuk menentukan adanya serangan, melainkan dianalisis bersama indikator lainnya.

4.6.4 Analisis Pola Percobaan

Analisis pola dilakukan dengan mengamati karakteristik percobaan login yang tercatat selama simulasi. Pola yang diperhatikan meliputi pengulangan permintaan terhadap halaman atau proses login, penggunaan akun target yang sama, serta adanya percobaan autentikasi yang dilakukan secara berurutan.

Apabila sejumlah percobaan login dilakukan secara berulang terhadap akun target dalam rentang waktu tertentu, aktivitas tersebut dapat menunjukkan pola yang sesuai dengan karakteristik *brute force*. Hasil pengamatan kemudian dibandingkan dengan skenario simulasi yang telah ditentukan sebelumnya.

Analisis pola dilakukan berdasarkan data aktual yang diperoleh dari log sehingga kesimpulan tidak hanya didasarkan pada asumsi, tetapi juga berdasarkan bukti digital yang tersedia.

4.6.5 Analisis URL yang Ditargetkan

URL yang ditargetkan dianalisis untuk mengetahui halaman atau endpoint yang menjadi tujuan permintaan selama proses simulasi. Informasi tersebut diperoleh dari bagian URL pada access.log.

URL yang berkaitan dengan halaman atau proses login digunakan untuk mengidentifikasi aktivitas yang berhubungan langsung dengan autentikasi. Dengan demikian, peneliti dapat membedakan aktivitas login dari aktivitas akses lainnya yang mungkin terjadi pada sistem.

Tabel 4. 9 Analisis URL

No	URL	Method	Jumlah Akses	Keterangan
1	"http://localhost/nist forensic/includes/login.php"	POST/GET	500	Percobaan autentikasi
2	"http://localhost/dashboard/"	GET	500	Akses dashboard setelah autentikasi berhasil

Data tersebut digunakan untuk memastikan bahwa aktivitas yang dianalisis memang berkaitan dengan endpoint login yang menjadi objek simulasi.

4.6.6 Analisis Respons Server

Respons server dianalisis berdasarkan *status code* yang tercatat pada *access.log*. *Status code* digunakan untuk mengetahui bagaimana server memberikan respons terhadap permintaan yang diterima selama simulasi.

Setiap respons dibandingkan dengan hasil percobaan login yang dicatat secara langsung. Dengan cara tersebut, peneliti dapat mengetahui hubungan antara permintaan yang dikirimkan, respons server, dan hasil autentikasi yang terjadi pada sistem.

Tabel 4. 10 Analisis Respons Server

No	Aktivitas	Status Code	Hasil
1	Aktivitas Percobaan Login	200	Gagal
2	Aktivitas Percobaan Login kembali	302	Gagal

Perlu diperhatikan bahwa *status code* HTTP tidak selalu menunjukkan apakah *username* dan *password* benar atau salah. Oleh karena itu, interpretasi hasil autentikasi harus disesuaikan dengan mekanisme sistem login dan data hasil pengujian.

4.6.7 Analisis Hubungan access.log dan error.log

Analisis selanjutnya dilakukan dengan menghubungkan informasi yang terdapat pada access.log dengan error.log. Kedua sumber log tersebut digunakan secara bersama-sama untuk memperoleh gambaran aktivitas yang lebih lengkap. access.log digunakan untuk mengetahui aktivitas permintaan yang diterima server, sedangkan error.log digunakan sebagai sumber informasi tambahan mengenai kesalahan atau kejadian tertentu yang tercatat pada server.

Penggabungan informasi dilakukan dengan membandingkan waktu kejadian, alamat IP, serta konteks aktivitas yang tercatat pada kedua log. Dengan menggunakan *timestamp* sebagai salah satu acuan, peneliti dapat mencocokkan aktivitas yang muncul pada access.log dengan kejadian yang tercatat pada error.log.

Tabel 4. 11 Korelasi access.log dan error.log

N	Timestam	Ip	Informasi	Informasi	Hasi
---	----------	----	-----------	-----------	------

o	p	Adresse	Acces.log	Error.log	l Kor elasi
1	[24/Aug/ 2026:16: 52:32	"127.0 .0.1"	"GET/ http://localhost/nist_forensic/includes/login.php/ HTTP/1.1" 200 4986	[Mon Aug 24 16:52:50.773352 2026] [php:notice] [pid 4592:tid 1864] [client ::1:49893] [NIST_FORENSIC] LOGIN_ATTEMPT username="admin" ip="127.0.0.1" status="success", referer: http://localhost/nist_forensic/includes/login.php	Aktivitas akses login pada access.log berkorelasi dengan catatan autentikasi pada error.log
2	24/Aug/2 026:16:5 2:32	"127.0 .0.1"	"GET/ http://localhost/nist_forensic/includes/login.php/ HTTP/1.1" 200 4986	Mon Aug 24 17:35:35.272262 2026] [php:notice] [pid 14980:tid 1884] [client ::1:50949]	Aktivitas permintaan login

				[NIST_FORENSIC] LOGIN_ATTEMPT username="admin" ip="127.0.0.1" status="failed", referer: http://localhost/nist_forensic/includes/login.php	n terh ubu ng den gan perc obaa n aute ntik asi yan g gaga l.
3	24/Aug/2026:17:48:12	172.18.150.182	"GET/http://localhost/nist_forensic/includes/login.php/ HTTP/1.0" 200 2412	[Mon Aug 24 17:48:12.037355 2026] [php:notice] [pid 14980:tid 1880] [client 172.18.150.182:54336] [NIST_FORENSIC] LOGIN_ATTEMPT username="admin" ip="172.18.150.182" " status="failed"	Akti vitas per mint aan logi n terh ubu ng den gan perc obaa n aute

					ntik asi yan g gaga l.
--	--	--	--	--	---------------------------------------

Korelasi tersebut digunakan untuk melihat apakah terdapat informasi yang saling mendukung antara kedua sumber log. Apabila suatu aktivitas tercatat pada access.log dan memiliki kejadian pendukung pada error.log dalam waktu yang berdekatan, kedua informasi tersebut dapat digunakan secara bersama-sama dalam penyusunan kronologi.

Namun, apabila error.log tidak mencatat kejadian yang berkaitan dengan percobaan login, kondisi tersebut tetap dicatat sebagai hasil pemeriksaan. Tidak semua aktivitas login gagal harus menghasilkan catatan pada error.log, karena pencatatan bergantung pada konfigurasi server dan cara aplikasi menangani kegagalan autentikasi.

4.6.8 Penyusunan Kronologi Serangan

Berdasarkan hasil analisis IP address, waktu, frekuensi percobaan, pola aktivitas, URL, respons server, serta korelasi antara access.log dan error.log, selanjutnya dilakukan penyusunan kronologi aktivitas.

Kronologi digunakan untuk menggambarkan urutan kejadian mulai dari aktivitas awal hingga aktivitas terakhir selama simulasi. Penyusunan kronologi dilakukan berdasarkan *timestamp* yang terdapat pada barang bukti digital dan dibandingkan dengan catatan hasil pengujian.

Tabel 4. 12 Kronologi Aktivitas Simulasi

N o	Waktu	IP	Aktivita s	URL	Stat us	ket
1	17:34: 39	172.0.0.1	Akses login	/nist_forensic/includes/login.php	200	Aktivitas awal
2	17:35: 35	172.18.150. 182	Percobaan login	/nist_forensic/includes/login.php	302	Redirect
3	17:35: 41	172.18.150. 182	Percobaan login	/nist_forensic/includes/login.php	302	Redirect
4	17:35: 42	172.18.150. 182	Percobaan login	/nist_forensic/includes/login.php	302	Redirect
5	17:37: 11	172.18.150. 182	Akses dashboard	/nist_forensic/includes/login.php	200	Setelah login berhasil

Berdasarkan keseluruhan hasil analisis, aktivitas yang ditemukan dibandingkan dengan karakteristik serangan *brute force*. Indikator yang digunakan meliputi adanya percobaan autentikasi secara berulang, penggunaan akun target yang sama, frekuensi percobaan dalam rentang waktu tertentu, serta pola permintaan yang tercatat pada server.

Hasil analisis menunjukkan bahwa terdapat tiga percobaan login gagal dari IP 172.18.150.182 dalam rentang waktu 17:35:35–17:35:42 yang ditujukan pada

endpoint login yang sama. Aktivitas tersebut kemudian diikuti dengan akses ke dashboard pada pukul 17:37:11 dengan *status code* 200. Pola percobaan autentikasi berulang tersebut menunjukkan karakteristik aktivitas *brute force* pada lingkungan pengujian. Apabila data menunjukkan adanya sejumlah percobaan login yang dilakukan secara berulang terhadap akun target dalam waktu tertentu dan pola tersebut sesuai dengan skenario simulasi, maka aktivitas tersebut dapat diidentifikasi memiliki karakteristik serangan *brute force*.

Dengan demikian, tahap *Analysis* menghasilkan informasi mengenai sumber aktivitas, waktu kejadian, frekuensi dan pola percobaan, URL yang ditargetkan, respons server, serta kronologi kejadian. Hasil tersebut selanjutnya digunakan sebagai dasar dalam tahap *Reporting*, yaitu menyusun dan menyajikan hasil investigasi digital secara sistematis.

4.7 Rekonstruksi Kronologi Serangan

Berdasarkan hasil pemeriksaan dan analisis terhadap *access.log*, *error.log*, serta hasil simulasi yang telah dilakukan, diperoleh rangkaian aktivitas yang menggambarkan proses terjadinya simulasi serangan *brute force* pada sistem login.

Aktivitas diawali pada pukul 17:34:39 dengan akses menuju halaman login http://localhost/nist_forensic/includes/login.php dari alamat IP 127.0.0.1. Permintaan tersebut menghasilkan *status code* 200, yang menunjukkan bahwa halaman login berhasil diakses dan menjadi awal dari proses pengujian.

Selanjutnya, pada pukul 17:35:35, terjadi percobaan login dari alamat IP 172.18.150.182 menuju endpoint login yang sama. Percobaan tersebut menghasilkan *status code* 302 dan berdasarkan catatan aktivitas autentikasi

dinyatakan sebagai login gagal. Percobaan kembali dilakukan pada pukul 17:35:41 dan 17:35:42 dari alamat IP yang sama dengan tujuan URL yang sama. Kedua percobaan tersebut juga menghasilkan respons 302 dan tercatat sebagai login gagal.

Tiga percobaan login tersebut terjadi dalam rentang waktu yang relatif berdekatan, yaitu sekitar 7 detik, sehingga menunjukkan adanya aktivitas autentikasi secara berulang terhadap endpoint login. Setelah rangkaian percobaan tersebut, pada pukul 17:37:11 tercatat akses menuju `http://localhost/nist_forensic/dashboard.php` dari alamat IP 172.18.150.182 dengan *status code* 200. Aktivitas tersebut menunjukkan bahwa dashboard berhasil diakses setelah proses autentikasi berhasil.

Berdasarkan urutan kejadian tersebut, ditemukan pola percobaan login gagal secara berulang yang kemudian diikuti dengan akses dashboard yang berhasil. Pola tersebut sesuai dengan skenario simulasi *brute force* yang dilakukan pada penelitian. Hasil kronologi ini selanjutnya digunakan sebagai dasar dalam penyusunan laporan investigasi digital.

Tabel 4. 13 Rekonstruksi Kronologi Simulasi Serangan

N o	Waktu	IP	Aktivita s	URL	Stat us	Ket
1	17:34: 39	127.0.0.1	Akses halama n login	/nist_forensic/includes/login.php	200	Halam an login diakse s

2	17:35:35	172.18.150.182	Percobaan login	/nist_forensic/includes/login.php	302	Login gagal
3	17:35:41	172.18.150.182	Percobaan login	/nist_forensic/includes/login.php	302	Login gagal
4	17:35:42	172.18.150.182	Percobaan login	/nist_forensic/includes/login.php	302	Login gagal
5	17:37:11	172.18.150.182	Akses dashboard	/nist_forensic/dashboard.php	200	Setelah login berhasil

4.8 Reporting

Tahap *Reporting* merupakan tahap akhir dalam proses investigasi digital berdasarkan metode NIST SP 800-86. Pada tahap ini, seluruh hasil yang diperoleh dari proses *Collection*, *Examination*, dan *Analysis* disusun menjadi laporan investigasi secara sistematis. Laporan bertujuan untuk menyajikan hasil pemeriksaan dan analisis terhadap aktivitas simulasi serangan *brute force* pada sistem login berbasis PHP.

Laporan investigasi disusun berdasarkan barang bukti digital yang telah dikumpulkan, hasil pemeriksaan terhadap log, hasil analisis aktivitas, serta rekonstruksi kronologi kejadian. Hasil tersebut kemudian digunakan untuk menjelaskan karakteristik aktivitas yang terjadi selama proses simulasi.

4.8.1 Identitas Kasus

Identitas kasus digunakan untuk memberikan informasi mengenai penelitian dan kegiatan investigasi yang dilakukan.

Informasi	Keterangan
Judul Investigasi	Investigasi Simulasi Serangan <i>Brute Force</i> pada Sistem Login Website Berbasis PHP
Objek Investigasi	Sistem Login Website Berbasis PHP
Metode Investigasi	NIST SP 800-86
Lingkungan Pengujian	Localhost
Jenis Pengujian	Simulasi Serangan <i>Brute Force</i>
Waktu Pengujian	17:34:39

4.8.2 Sumber Barang Bukti Digital

Barang bukti digital yang digunakan dalam proses investigasi diperoleh dari sistem login berbasis PHP dan server Apache yang digunakan selama pelaksanaan pengujian. Barang bukti tersebut dikumpulkan setelah proses simulasi serangan *brute force* dilakukan untuk memastikan bahwa seluruh aktivitas yang terjadi selama pengujian dapat dianalisis berdasarkan data yang tercatat pada sistem.

Sumber barang bukti digital yang digunakan dalam penelitian ini meliputi access.log, error.log, log aktivitas login, hasil simulasi *brute force*, hasil percobaan login, serta screenshot sistem sebagai dokumentasi pendukung. File access.log digunakan untuk memperoleh informasi mengenai aktivitas permintaan

yang diterima oleh server, seperti alamat IP, waktu akses, URL, metode HTTP, dan *status code*. Sementara itu, *error.log* digunakan untuk memperoleh informasi mengenai kejadian atau pesan yang dicatat oleh server maupun aplikasi selama proses pengujian, termasuk catatan aktivitas autentikasi yang dihasilkan oleh sistem.

Selain log server, log aktivitas login digunakan untuk mengetahui hasil dari proses autentikasi, seperti percobaan login yang berhasil maupun gagal. Hasil simulasi *brute force* digunakan untuk mengetahui aktivitas pengujian yang sengaja dilakukan terhadap sistem login, sedangkan hasil percobaan login digunakan sebagai pembandingan antara aktivitas yang dilakukan secara langsung dengan aktivitas yang tercatat pada log server. Adapun screenshot sistem digunakan sebagai dokumentasi pendukung yang menunjukkan kondisi halaman login, dashboard, konfigurasi sistem, serta proses pengumpulan barang bukti.

Seluruh barang bukti tersebut digunakan sebagai sumber informasi dalam proses pemeriksaan dan analisis. Data dari masing-masing sumber kemudian dibandingkan dan dikorelasikan berdasarkan informasi seperti waktu kejadian, alamat IP, URL, serta aktivitas autentikasi. Proses tersebut dilakukan untuk memperoleh gambaran yang lebih lengkap mengenai aktivitas selama simulasi dan membantu peneliti dalam menyusun kronologi serta menentukan karakteristik aktivitas *brute force* yang terjadi pada sistem.

4.8.3 Hasil Pemeriksaan

Berdasarkan tahap *Examination* yang telah dilakukan terhadap barang bukti digital, diperoleh sejumlah informasi yang berkaitan dengan aktivitas pada sistem login selama pelaksanaan simulasi. Pemeriksaan dilakukan terhadap

access.log, error.log, log aktivitas login, serta hasil percobaan login yang telah dikumpulkan pada tahap *Collection*. Setiap informasi yang ditemukan diperiksa untuk mengetahui keterkaitannya dengan aktivitas autentikasi pada sistem.

Pada access.log ditemukan informasi mengenai alamat IP, waktu aktivitas (*timestamp*), URL yang diakses, metode HTTP, dan *status code* yang diberikan oleh server. Informasi tersebut digunakan untuk mengetahui aktivitas permintaan yang terjadi selama proses pengujian. Berdasarkan hasil pemeriksaan, ditemukan aktivitas akses terhadap halaman login pada URL /nist_forensic/includes/login.php serta aktivitas akses terhadap halaman dashboard pada URL /nist_forensic/dashboard.php.

Selain itu, pemeriksaan terhadap error.log digunakan untuk mengetahui catatan aktivitas autentikasi yang dihasilkan oleh aplikasi. Pada log tersebut ditemukan informasi dengan format LOGIN_ATTEMPT yang mencatat username, alamat IP, serta status autentikasi, baik *failed* maupun *success*. Informasi tersebut menjadi data pendukung untuk menentukan hasil dari setiap percobaan login.

Hasil pemeriksaan juga dibandingkan dengan catatan percobaan login yang dilakukan selama simulasi. Perbandingan tersebut bertujuan untuk memastikan bahwa aktivitas yang dilakukan selama pengujian memiliki kesesuaian dengan aktivitas yang tercatat pada log server. Dengan demikian, hasil pemeriksaan dapat digunakan sebagai dasar untuk melakukan analisis terhadap pola aktivitas dan penyusunan kronologi simulasi serangan.

4.8.4 Hasil Analisis

Berdasarkan hasil analisis terhadap barang bukti digital yang telah diperiksa, ditemukan adanya aktivitas autentikasi secara berulang pada sistem login. Analisis dilakukan dengan menghubungkan informasi yang terdapat pada `access.log`, `error.log`, dan hasil percobaan login untuk mengetahui hubungan antara aktivitas yang dilakukan selama simulasi dengan aktivitas yang tercatat pada server.

Berdasarkan data yang diperoleh, aktivitas awal terjadi pada pukul 17:34:39 ketika halaman login `/nist_forensic/includes/login.php` diakses dengan alamat IP 127.0.0.1 dan menghasilkan *status code* 200. Aktivitas tersebut menunjukkan bahwa halaman login berhasil diakses dan menjadi awal dari proses pengujian.

Selanjutnya, ditemukan tiga percobaan login pada pukul 17:35:35, 17:35:41, dan 17:35:42 yang berasal dari alamat IP 172.18.150.182. Ketiga aktivitas tersebut ditujukan pada URL login yang sama dan menghasilkan *status code* 302. Berdasarkan hasil pemeriksaan terhadap log aktivitas autentikasi, percobaan tersebut diketahui sebagai percobaan login yang gagal.

Ketiga percobaan login tersebut terjadi dalam rentang waktu yang relatif berdekatan. Hal tersebut menunjukkan adanya aktivitas autentikasi secara berulang terhadap endpoint login yang sama. Setelah rangkaian percobaan tersebut, ditemukan aktivitas akses terhadap halaman dashboard pada pukul 17:37:11 dari alamat IP 172.18.150.182 dengan *status code* 200. Aktivitas tersebut menunjukkan bahwa dashboard berhasil diakses setelah proses autentikasi berhasil.

Berdasarkan hasil analisis tersebut, pola aktivitas yang ditemukan menunjukkan adanya beberapa percobaan login gagal secara berulang yang kemudian diikuti dengan keberhasilan autentikasi. Pola tersebut memiliki karakteristik yang sesuai dengan skenario simulasi serangan *brute force* yang dilakukan dalam penelitian. Hasil analisis selanjutnya digunakan untuk menyusun kronologi aktivitas pada tahap *Rekonstruksi Kronologi Serangan*.

4.8.5 IP Address

Berdasarkan hasil pemeriksaan dan analisis terhadap barang bukti digital, ditemukan beberapa alamat IP yang tercatat selama proses pengujian. Alamat IP digunakan sebagai salah satu informasi penting dalam investigasi karena dapat membantu mengidentifikasi sumber aktivitas yang tercatat pada server.

Pada aktivitas awal akses halaman login ditemukan alamat IP 127.0.0.1. Alamat tersebut merupakan alamat *loopback* yang menunjukkan akses dari lingkungan komputer lokal. Selanjutnya, pada rangkaian percobaan login dan akses dashboard ditemukan alamat IP 172.18.150.182.

Alamat IP tersebut dicatat berdasarkan informasi yang terdapat pada log dan tidak dilakukan perubahan terhadap data aslinya. Perbedaan alamat IP yang ditemukan pada beberapa aktivitas tetap dipertahankan dalam hasil investigasi karena merupakan bagian dari barang bukti digital yang diperoleh selama pengujian.

Dalam penelitian ini, alamat IP digunakan bersama dengan informasi *timestamp*, URL, dan aktivitas autentikasi untuk menghubungkan beberapa kejadian yang terjadi selama simulasi. Dengan demikian, IP address tidak

dianalisis secara terpisah, tetapi digunakan sebagai salah satu indikator dalam proses korelasi dan penyusunan kronologi.

4.8.6 Waktu Kejadian

Informasi waktu kejadian diperoleh dari *timestamp* yang terdapat pada log server. Waktu tersebut digunakan untuk menentukan urutan aktivitas yang terjadi selama proses simulasi. Dengan mengurutkan aktivitas berdasarkan waktu, peneliti dapat mengetahui proses yang terjadi mulai dari akses awal halaman login, percobaan autentikasi, hingga akses dashboard.

Berdasarkan hasil pemeriksaan, aktivitas pertama ditemukan pada pukul 17:34:39, yaitu ketika halaman login diakses. Selanjutnya, percobaan login pertama tercatat pada pukul 17:35:35, kemudian percobaan kedua pada pukul 17:35:41, dan percobaan ketiga pada pukul 17:35:42. Setelah rangkaian percobaan tersebut, aktivitas akses dashboard tercatat pada pukul 17:37:11.

Informasi waktu tersebut menunjukkan bahwa terdapat tiga percobaan login yang terjadi dalam interval waktu yang relatif berdekatan. Data *timestamp* kemudian dikorelasikan dengan informasi yang terdapat pada *error.log* untuk memastikan waktu terjadinya aktivitas autentikasi serta hasil dari masing-masing percobaan.

Dengan demikian, *timestamp* menjadi salah satu informasi penting dalam proses investigasi karena dapat digunakan untuk menyusun urutan kejadian dan membentuk kronologi aktivitas selama simulasi.

4.8.7 Jumlah Percobaan

Berdasarkan hasil pemeriksaan terhadap access.log dan log aktivitas login, ditemukan sebanyak tiga percobaan login gagal yang dilakukan terhadap endpoint login selama rangkaian aktivitas yang dianalisis. Percobaan tersebut terjadi pada pukul 17:35:35, 17:35:41, dan 17:35:42.

Ketiga percobaan tersebut berasal dari alamat IP 172.18.150.182 dan ditujukan pada endpoint `/nist_forensic/includes/login.php`. Berdasarkan hasil pemeriksaan terhadap aktivitas autentikasi, ketiga percobaan tersebut menghasilkan status *failed*. Aktivitas percobaan login kemudian diikuti dengan akses menuju halaman dashboard pada pukul 17:37:11.

Jumlah percobaan tersebut digunakan sebagai salah satu indikator dalam analisis karakteristik *brute force*. Namun, jumlah percobaan tidak digunakan sebagai satu-satunya dasar dalam menentukan adanya aktivitas *brute force*. Analisis juga mempertimbangkan pola pengulangan, interval waktu, alamat IP, URL yang ditargetkan, hasil autentikasi, serta kesesuaian antara hasil simulasi dengan data yang tercatat pada log.

4.8.8 Kronologi Serangan

Berdasarkan hasil pemeriksaan dan analisis terhadap seluruh barang bukti digital, dilakukan rekonstruksi kronologi untuk menggambarkan urutan aktivitas selama simulasi serangan. Rekonstruksi dilakukan dengan mengurutkan setiap aktivitas berdasarkan *timestamp* dan menghubungkan informasi dari access.log, error.log, serta hasil percobaan login.

Aktivitas diawali pada pukul 17:34:39 dengan akses menuju halaman login `/nist_forensic/includes/login.php` dari alamat IP 127.0.0.1. Permintaan

tersebut menghasilkan *status code* 200, yang menunjukkan bahwa halaman login berhasil diakses.

Selanjutnya, pada pukul 17:35:35 terjadi percobaan login dari alamat IP 172.18.150.182 menuju endpoint login yang sama. Percobaan tersebut menghasilkan *status code* 302 dan berdasarkan log aktivitas autentikasi dinyatakan sebagai percobaan login gagal. Percobaan berikutnya terjadi pada pukul 17:35:41 dan 17:35:42, dengan alamat IP dan URL yang sama. Kedua percobaan tersebut juga tercatat sebagai login gagal.

Setelah rangkaian percobaan login, pada pukul 17:37:11 ditemukan aktivitas akses menuju `/nist_forensic/dashboard.php` dari alamat IP 172.18.150.182 dengan *status code* 200. Aktivitas tersebut menunjukkan bahwa akses menuju dashboard berhasil dilakukan setelah proses autentikasi.

Berdasarkan rangkaian kejadian tersebut, dapat disusun pola aktivitas berupa akses halaman login → percobaan login gagal → percobaan login gagal → percobaan login gagal → autentikasi berhasil → akses dashboard. Pola tersebut sesuai dengan skenario simulasi yang telah dilakukan untuk menguji kemampuan log server dalam merekam aktivitas autentikasi secara berulang.

Setelah rangkaian percobaan login, pada pukul 17:37:11 ditemukan aktivitas akses menuju `/nist_forensic/dashboard.php` dari alamat IP 172.18.150.182 dengan *status code* 200. Aktivitas tersebut menunjukkan bahwa akses menuju dashboard berhasil dilakukan setelah proses autentikasi.

Berdasarkan rangkaian kejadian tersebut, dapat disusun pola aktivitas berupa akses halaman login → percobaan login gagal → percobaan login gagal → percobaan login gagal → autentikasi berhasil → akses dashboard. Pola tersebut

sesuai dengan skenario simulasi yang telah dilakukan untuk menguji kemampuan log server dalam merekam aktivitas autentikasi secara berulang.

4.9 Hasil Pengujian dan Pembahasan

Berdasarkan hasil pengujian yang telah dilakukan pada sistem login berbasis PHP, diperoleh data aktivitas autentikasi yang tercatat pada log server selama pelaksanaan simulasi serangan *brute force*. Pengujian dilakukan pada lingkungan *localhost* dengan melakukan beberapa percobaan login secara berulang terhadap akun target. Setiap aktivitas yang terjadi selama pengujian kemudian dicatat oleh sistem dan digunakan sebagai barang bukti digital untuk dilakukan proses investigasi menggunakan metode NIST SP 800-86.

Hasil pengujian menunjukkan bahwa aktivitas login dapat direkam melalui log server, khususnya `access.log` dan `error.log`. Pada `access.log` ditemukan informasi mengenai alamat IP, waktu akses, URL yang dituju, metode HTTP, serta *status code* dari setiap permintaan yang diterima oleh server. Sementara itu, `error.log` mencatat aktivitas autentikasi melalui event `LOGIN_ATTEMPT`, termasuk username, alamat IP, serta status autentikasi yang menunjukkan apakah percobaan login berhasil atau gagal.

Berdasarkan data yang diperoleh, aktivitas awal terjadi pada pukul 17:34:39 ketika halaman login `/nist_forensic/includes/login.php` diakses dari alamat IP 127.0.0.1 dengan *status code* 200. Setelah itu, terdapat tiga percobaan login yang dilakukan pada pukul 17:35:35, 17:35:41, dan 17:35:42 dari alamat IP 172.18.150.182 menuju endpoint login yang sama. Berdasarkan hasil pemeriksaan log aktivitas autentikasi, ketiga percobaan tersebut tercatat sebagai login gagal.

Tiga percobaan login tersebut terjadi dalam waktu yang relatif berdekatan. Kondisi tersebut menunjukkan adanya aktivitas autentikasi secara berulang terhadap endpoint login yang sama. Setelah rangkaian percobaan tersebut, pada pukul 17:37:11 tercatat akses menuju `/nist_forensic/dashboard.php` dari alamat IP 172.18.150.182 dengan *status code* 200. Aktivitas tersebut menunjukkan bahwa setelah proses autentikasi berhasil, pengguna dapat mengakses halaman dashboard.

Hasil tersebut kemudian dianalisis menggunakan tahapan NIST SP 800-86. Pada tahap *Collection*, barang bukti digital berupa `access.log`, `error.log`, log aktivitas login, hasil simulasi, hasil percobaan login, dan dokumentasi sistem dikumpulkan. Pada tahap *Examination*, informasi penting seperti IP address, *timestamp*, URL, metode HTTP, *status code*, username, dan status autentikasi diidentifikasi dari barang bukti. Selanjutnya, pada tahap *Analysis*, informasi tersebut dibandingkan dan dikorelasikan untuk mengetahui pola aktivitas serta hubungan antara permintaan akses dengan proses autentikasi. Tahap terakhir, yaitu *Reporting*, digunakan untuk menyusun hasil investigasi dan kronologi kejadian berdasarkan bukti yang telah dianalisis.

Hasil pengujian menunjukkan bahwa `access.log` dan `error.log` memiliki fungsi yang saling melengkapi. `access.log` memberikan informasi mengenai aktivitas permintaan yang diterima oleh server, sedangkan `error.log` memberikan informasi tambahan mengenai aktivitas autentikasi yang dilakukan oleh aplikasi. Dengan menghubungkan kedua sumber log berdasarkan waktu, alamat IP, URL, dan aktivitas login, peneliti dapat memperoleh gambaran yang lebih lengkap mengenai aktivitas yang terjadi selama simulasi.

Berdasarkan hasil tersebut, penerapan metode Digital Forensic NIST dapat membantu proses identifikasi dan analisis aktivitas simulasi *brute force* pada sistem login berbasis PHP. Informasi yang diperoleh dari log server memungkinkan peneliti mengetahui sumber aktivitas melalui IP address, waktu kejadian melalui timestamp, endpoint yang menjadi sasaran melalui URL, jumlah percobaan melalui frekuensi aktivitas, serta urutan kejadian melalui rekonstruksi kronologi.

Hasil penelitian juga menunjukkan bahwa keberadaan log server memiliki peranan penting dalam proses investigasi. Aktivitas yang dilakukan selama simulasi tidak hanya dapat diamati secara langsung pada halaman login, tetapi juga meninggalkan jejak digital pada server. Jejak tersebut dapat digunakan untuk melakukan pemeriksaan kembali terhadap aktivitas yang telah terjadi sehingga proses investigasi dapat dilakukan secara lebih terstruktur berdasarkan bukti digital.

Dengan demikian, hasil pengujian telah mendukung tujuan penelitian, yaitu menerapkan metode Digital Forensic NIST untuk melakukan investigasi terhadap simulasi serangan *brute force* pada sistem login website berbasis PHP melalui analisis log server. Penerapan tahapan Collection, Examination, Analysis, dan Reporting menghasilkan informasi yang dapat digunakan untuk mengidentifikasi aktivitas percobaan login, menganalisis pola percobaan, menghubungkan bukti dari beberapa sumber log, serta menyusun kronologi kejadian secara sistematis.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai Penerapan Metode Digital Forensic NIST untuk Investigasi Serangan *Brute Force* pada Sistem Login Website Berbasis PHP Melalui Analisis Log Server, maka dapat disimpulkan sebagai berikut:

1. Penerapan metode Digital Forensic National Institute of Standards and Technology (NIST) dalam investigasi simulasi serangan *brute force* pada sistem login website berbasis PHP dilakukan melalui empat tahapan, yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*. Tahap *Collection* digunakan untuk mengumpulkan barang bukti digital yang dihasilkan selama simulasi, tahap *Examination* digunakan untuk memeriksa dan mengekstraksi informasi dari barang bukti, tahap *Analysis* digunakan untuk menganalisis dan menghubungkan informasi yang diperoleh, sedangkan tahap *Reporting* digunakan untuk menyusun hasil investigasi secara sistematis. Penerapan keempat tahapan tersebut memungkinkan proses investigasi dilakukan secara terstruktur berdasarkan barang bukti digital yang tersedia.
2. Identifikasi dan analisis artefak digital dari *access.log* dan *error.log* dapat digunakan untuk mengungkap aktivitas simulasi *brute force* pada sistem login website berbasis PHP. *access.log* memberikan informasi berupa

alamat IP, *timestamp*, URL, metode HTTP, dan *status code*, sedangkan *error.log* memberikan informasi mengenai aktivitas autentikasi, seperti *username*, alamat IP, serta status *failed* dan *success*. Berdasarkan hasil pengujian, ditemukan tiga percobaan login gagal pada pukul 17:35:35, 17:35:41, dan 17:35:42 dari alamat IP 172.18.150.182 menuju endpoint */nist_forensic/includes/login.php*. Hasil tersebut menunjukkan bahwa log server dapat digunakan sebagai sumber bukti digital untuk mengidentifikasi aktivitas autentikasi secara berulang selama simulasi.

3. Rekonstruksi kronologi simulasi serangan *brute force* dapat dilakukan berdasarkan korelasi informasi dari log server dan hasil pengujian melalui tahapan NIST. Kronologi dimulai dari akses halaman login pada pukul 17:34:39, kemudian terdapat tiga percobaan login gagal pada pukul 17:35:35, 17:35:41, dan 17:35:42 dari IP 172.18.150.182. Setelah rangkaian percobaan tersebut, pada pukul 17:37:11 ditemukan akses menuju */nist_forensic/dashboard.php* dengan *status code* 200 setelah proses autentikasi berhasil. Urutan tersebut menunjukkan pola percobaan autentikasi secara berulang yang sesuai dengan skenario simulasi *brute force* yang dilakukan pada lingkungan pengujian.
4. Penerapan metode Digital Forensic NIST menghasilkan laporan investigasi yang memuat informasi penting mengenai aktivitas simulasi serangan. Laporan investigasi mencakup identitas kasus, sumber barang bukti digital, hasil pemeriksaan, hasil analisis, alamat IP, waktu kejadian, jumlah percobaan, serta kronologi aktivitas. Hasil tersebut dapat digunakan sebagai dokumentasi dan referensi dalam melakukan analisis

terhadap insiden keamanan pada sistem login website berbasis PHP, khususnya dalam mengidentifikasi dan memahami aktivitas percobaan autentikasi secara berulang.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran yang dapat diberikan untuk pengembangan penelitian selanjutnya adalah sebagai berikut:

1. Penelitian selanjutnya dapat melakukan simulasi dengan jumlah percobaan yang lebih banyak dan variasi pola *brute force* yang lebih beragam, sehingga karakteristik serangan dapat dianalisis secara lebih mendalam berdasarkan frekuensi dan interval percobaan.
2. Sistem login dapat dikembangkan dengan menerapkan mekanisme pencegahan serangan *brute force*, seperti *rate limiting*, *account lockout*, CAPTCHA, serta mekanisme deteksi percobaan login yang mencurigakan.
3. Pencatatan log dapat dikembangkan agar lebih lengkap dan terstruktur, sehingga informasi seperti username, IP address, *timestamp*, status autentikasi, jumlah percobaan, dan *user agent* dapat digunakan secara lebih optimal dalam proses investigasi.
4. Penelitian selanjutnya dapat menggunakan sumber artefak digital yang lebih beragam, seperti log firewall, log database, atau Web Application Firewall (WAF), sehingga hasil investigasi dapat memberikan gambaran insiden keamanan yang lebih menyeluruh.
5. Penelitian selanjutnya dapat membandingkan metode NIST SP 800-86 dengan metode digital forensik lainnya untuk mengetahui kelebihan dan

keterbatasan masing-masing metode dalam investigasi serangan terhadap sistem berbasis web.

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(01), 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/JTIK.2023105872>
- fFaizal, 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>
- 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>
- 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>

- 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>
- Lyle, J. R., Guttman, B., Butler, J., Sauerwein, K., Reed, C., & Lloyd, C. (2022). Digital investigation techniques: A NIST scientific foundation review (NISTIR 8354). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8354>
- Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. (2022). Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037:2012 and NIST SP800-86 framework. *IT Journal Research and Development*, 6(2), 162–168. <https://doi.org/10.25299/itjrd.2022.8968>
- Julian, D., & Sutabri, T. (2023). Analisa kinerja aplikasi digital forensik Autopsy untuk pengembalian data menggunakan metode NIST SP 800-86. *Jurnal Informatika Terpadu*, 9(2), 136–142. <https://doi.org/10.54914/jit.v9i2.984>
- Putra, M. A. D., Wirawan Muhammad, A., Parga Zen, B., Yunita Kisworini, R., & Rohayati, T. (2024). Analisis forensik pada Instagram dan TikTok dalam mendapatkan bukti digital dengan menggunakan metode NIST 800-86. *Jurnal Sistem Informasi Galuh*, 2(1), 44–54. <https://doi.org/10.25157/jsig.v2i1.3695>
- Kaestria, R., Djatta, A. L., Erfan, M., & Himmah, E. F. (2025). Penerapan metodologi forensik digital NIST SP 800-86 pasca serangan ransomware LockBit 3.0. *Jurnal Sains Komputer dan Teknologi Informasi*, 8(1), 55–58. <https://doi.org/10.33084/jsakti.v8i1.11137>
- Olegård, J., Axelsson, S., & Li, Y. (2025). When is logging sufficient? Tracking event causality for improved forensic analysis and correlation. *Forensic Science International: Digital Investigation*, 52, 301877. <https://doi.org/10.1016/j.fsidi.2025.301877>
- Azahari, A., & Balzarotti, D. (2024). On the inadequacy of open-source application logs for digital forensics. *Forensic Science International: Digital Investigation*, 49, 301750. <https://doi.org/10.1016/j.fsidi.2024.301750>
- Hargreaves, C., Nelson, A., & Casey, E. (2024). An abstract model for digital forensic tools: A foundation for systematic error mitigation analysis. *Forensic Science International: Digital Investigation*, 48, 301679. <https://doi.org/10.1016/j.fsidi.2023.301679>
- Breitinger, F., Hilgert, J.-N., Hargreaves, C., Sheppard, J., Overdorf, R., & Scanlon, M. (2024). DFRWS EU 10-year review and future directions in digital forensic research. *Forensic Science International: Digital Investigation*, 48, 301685. <https://doi.org/10.1016/j.fsidi.2023.301685>

- Todd, M. C., & Peterson, G. L. (2024). Temporal metadata analysis: A learning classifier system approach. *Forensic Science International: Digital Investigation*, 51, 301842. <https://doi.org/10.1016/j.fsidi.2024.301842>
- Mombelli, S., Lyle, J. R., & Breitingner, F. (2024). FAIRness in digital forensics datasets' metadata—and how to improve it. *Forensic Science International: Digital Investigation*, 48, 301681. <https://doi.org/10.1016/j.fsidi.2023.301681>
- Calzavara, S., Jonker, H. L., Krumnow, B., & Rabitti, A. (2021). Measuring web session security at scale. *Computers & Security*, 111, 102472. <https://doi.org/10.1016/j.cose.2021.102472>
- Lina, I. M., & Fernandes, G. R. (2023). Anticipate password security with Burp Suite using the brute force attack method. *Jurnal E-Komtek*, 7(1), 118–127. <https://doi.org/10.37339/e-komtek.v7i1.1162>
- Abdullah, R., & Fachri, F. (2025). Mitigasi keamanan webserver sistem informasi akademik terhadap serangan brute force menggunakan penetration testing. *REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer*, 9(3), 885–896. <https://doi.org/10.33395/remik.v9i3.15104>
- Balqis, P., & Rahman, R. (2025). Analisis keamanan layanan SSH terhadap brute force attack. *Jurnal Riset Sistem Informasi dan Teknik Informatika*, 3(4). <https://doi.org/10.61132/mercurius.v3i4.949>
- Fuzi, M. F. M., Mazlan, M. F., Jamaluddin, M. N. F., & Halim, I. H. A. H. (2024). Performance analysis of network intrusion detection using T-Pot honeypots. *Journal of Computing Research and Innovation*, 9(2), 348–360. <https://doi.org/10.24191/jcrinn.v9i2.477>
- Dalezios, N., Shiaeles, S., Kolokotronis, N., & Ghita, B. (2020). Digital forensics cloud log unification: Implementing CADF in Apache CloudStack. *Journal of Information Security and Applications*, 54, Article 102555. <https://doi.org/10.1016/j.jisa.2020.102555>
- Binnar, P., Bhirud, S., & Kazi, F. (2024). Security analysis of cyber physical system using digital forensic incident response. *Cyber Security and Applications*, 2, Article 100034. <https://doi.org/10.1016/j.csa.2023.100034>
- Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, 362, Article 112133. <https://doi.org/10.1016/j.forsciint.2024.112133>
- Ma, M. (2024). Research and application of firewall log and intrusion detection log data visualization system. *IET Software*, 2024, Article 7060298. <https://doi.org/10.1049/2024/7060298>

LAMPIRAN

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

Alamat: Universitas Muhammadiyah Sumatera Utara Jalan Sisinga 2222 Telp. (061) 822248 - 822287 Fax. (061) 822475 - 821981
 Email: info@umsu.ac.id registrar@umsu.ac.id library@umsu.ac.id finance@umsu.ac.id hrd@umsu.ac.id ids@umsu.ac.id

FORMULIR PERBAIKAN URAIAN SKRIPSI

Pada hari ini, Selasa 1 September 2020 telah dilaksanakan Ujian Skripsi bagi mahasiswa Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara. Ada:

Nama Mahasiswa : Shanyu Anggi Sialiti
 NPM : 2209010128
 Program Studi : Sistem Informasi
 Judul Proposal : Penerapan Metode Digital Forensics FOST Untuk Investigasi Serangan Ransomware Pada Sistem Logon Windows Berbasis PHP Melalui Aplikasi Log Server
 Materi Perek yang Diperbaiki :

	Peny	Peny
Andi Zulherry, S.Kom, M.Kom	Ok	
Dr. Endang Riky, M.Kom	Ok	
Indah Permata Sari, S.T., M.Kom	- Sebelum Pengerjaan harus berkoordinasi dengan Dosen Pembimbing	

Berita acara ini dibuat sebagai bukti bahwa skripsi diperbaiki sesuai petunjuk arahan dan bimbingan dari Penguji Pembimbing.

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

Alamat: Universitas Muhammadiyah Sumatera Utara Jalan Sisinga 2222 Telp. (061) 822248 - 822287 Fax. (061) 822475 - 821981
 Email: info@umsu.ac.id registrar@umsu.ac.id library@umsu.ac.id finance@umsu.ac.id hrd@umsu.ac.id ids@umsu.ac.id

Berita Acara Peninjauan Skripsi

Nama Mahasiswa : Shanyu Anggi Sialiti
 NPM : 2209010128
 Nama Dosen Pembimbing : Andi Zulherry, S.Kom, M.Kom
 Program Studi : Sistem Informasi
 Judul Penelitian : Penerapan Metode Digital Forensics FOST Untuk Investigasi Serangan Ransomware Pada Sistem Logon Windows Berbasis PHP

Tanggal Peninjauan	Isi dan Isi	Tanda Tangan
20/09/2020	Skripsi telah selesai dan siap untuk diproses.	
22/09/2020	Skripsi telah selesai dan siap untuk diproses.	
23/09/2020	Skripsi telah selesai dan siap untuk diproses.	
24/09/2020	Skripsi telah selesai dan siap untuk diproses.	
25/09/2020	Skripsi telah selesai dan siap untuk diproses.	
26/09/2020	Skripsi telah selesai dan siap untuk diproses.	
27/09/2020	Skripsi telah selesai dan siap untuk diproses.	
28/09/2020	Skripsi telah selesai dan siap untuk diproses.	


UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
12010 Teknologi & Berkeadilan: Regerasi Bekerja dan Hidup Berteknologi / Program Studi Sa. Sistem Informasi / 2023
 Jalan Khatulistiwa No. 1 Medan 20136 Telp. 061 862491 - 462491 Telp. 061 862474 - 462491

Medan, 21 Juli 2025

Disetujui oleh:
 Ketua Program Studi

 (Mubandika Abdi Prayito Taktang, S.Kom., M.Kom.)

Disetujui oleh:
 Dosen Pembimbing

 (Asri Zulkarni, S.Kom., M.Kom.)



SKRIPSI IYA 12345.RX (6).pdf

100% (1/1/2025)

16%

UNKNOWN SOURCE

14%

INTERNET SOURCES

7%

PLAGIATORS

7%

STUDENT PAPER

100% (1/1/2025)

1	repository.umsu.ac.id	2%
2	elib.pnc.ac.id	1%
3	Submitted to Universitas Putera Batam	1%
4	journal.unpas.ac.id	1%
5	Submitted to STKIP Sumatera Barat	<1%
6	Submitted to Universitas Muhammadiyah Purwokerto	<1%
7	lab.tik.pnj.ac.id	<1%
8	dspace.uin.ac.id	<1%
9	Submitted to Universitas Muhammadiyah Sumatera Utara	<1%
10	Muh. Rafi, R. Muhammad Dzaky As'ad, Abdul Ibrahim, Hasyrif Sy. "Sequential Pattern Mining untuk Analisis Navigasi SIKAAD Berbasis Log", RIIGGS: Journal of Artificial Intelligence and Digital Business, 2025	<1%
11	journal.universitaspahlawan.ac.id	<1%
12	repository.iqin.ac.id	<1%
13	Submitted to Savien HS	<1%
14	repository.harapan.ac.id	<1%



Desi Sendang, 14 Oktober 2026

No : 045/IJOMSS/LoA/X/2026
Lamp : -
Hal : Surat Penerimaan Naskah Jurnal

Kepada Yth.
Para Penulis
di Tempat

Letter of Accepted (LOA)

Terima kasih telah mengirimkan naskah anda ke *Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS)* dengan data sebagai berikut:

Penulis	Judul
SHINTYA ANGGIE SYAFITHI	INVESTIGASI FORENSIK DIGITAL SERANGAN BRUTE FORCE PADA SISTEM LOGIN WEB
ANDY ZULHERRY	MENGGUNAKAN METODE NIST

Berdasarkan hasil review akhir yang telah dilakukan, dengan ini kami menyatakan bahwa naskah tersebut **DITERIMA** untuk dipublikasikan pada *Indonesian Journal of Multidisciplinary Scientific Studies (IJOMSS)*, edisi Vol. 4 No. 4 (Oktober - November 2026).

Demikian surat penerimaan ini kami sampaikan. Atas perhatian dan kerja sama yang baik, kami ucapkan terima kasih.

Hormat Kami,



Dr. Muhammad Azhari, M.Pd
Editor in Chief