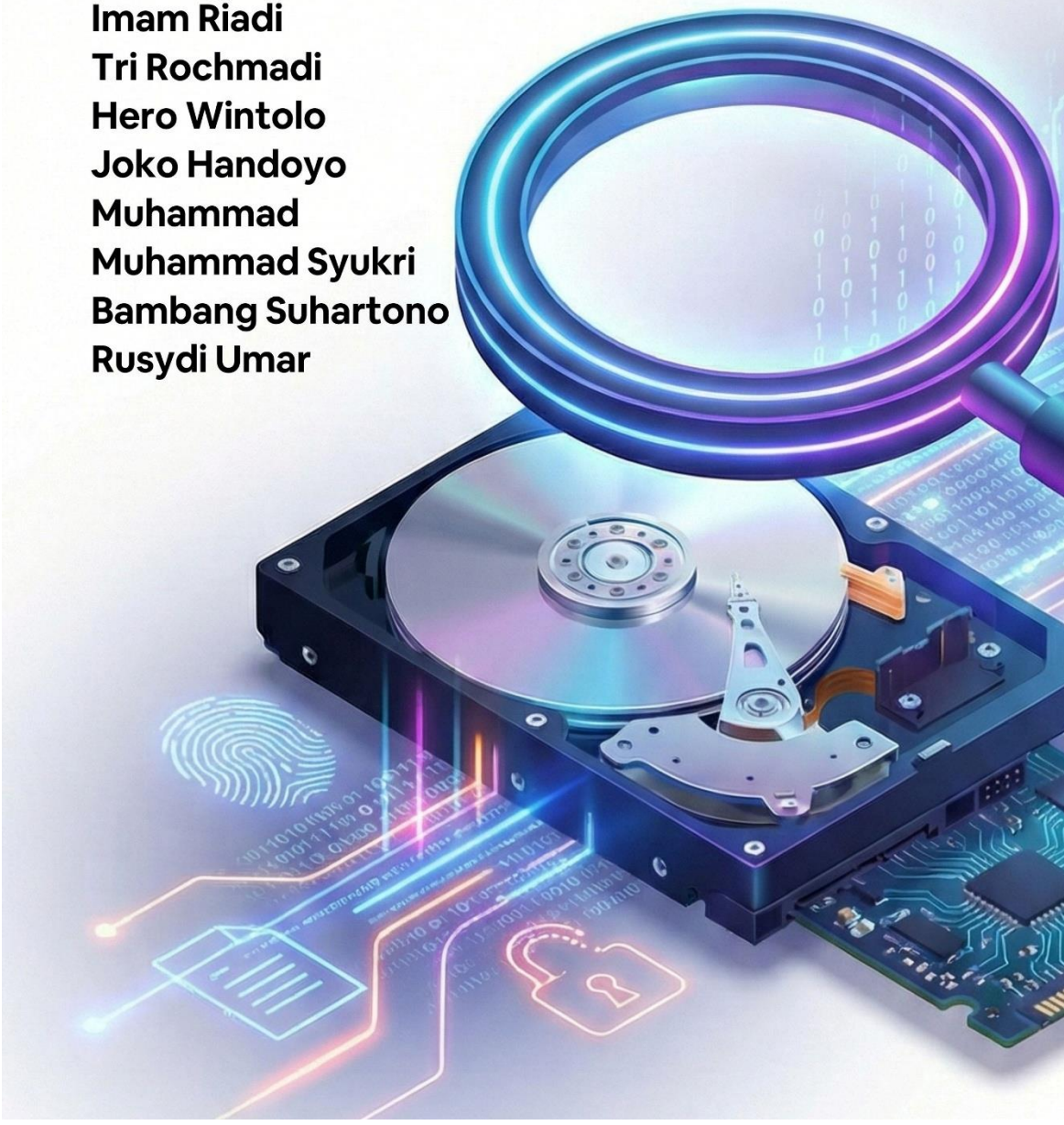
HADLA
MEDIA INFORMASI

Analisis Forensik Digital #1

Penulis :

Imam Riadi
Tri Rochmadi
Hero Wintolo
Joko Handoyo
Muhammad
Muhammad Syukri
Bambang Suhartono
Rusydi Umar



Analisis Forensik Digital #1

Penulis

Imam Riadi

Tri Rochmadi

Hero Wintolo

Joko Handoyo

Muhammad

Muhammad Syukri

Bambang Suhartono

Rusydi Umar

PENERBIT:

HADLA
MEDIA INFORMASI

UU No 28 tahun 2014 tentang Hak Cipta

Pasal 113

1) Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp 100.000.000 (seratus juta rupiah).

2) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah).

3) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (l) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah).

Analisis Forensik Digital #1

Tim Penulis:

Imam Riadi
Tri Rochmadi
Hero Wintolo
Joko Handoyo
Muhammad
Muhammad Syukri
Bambang Suhartono
Rusydi Umar

Editor :
Nurhadi

Desain Cover:
Sulaiman

Tata Letak:
Sulaiman

ISBN:
978-634-04-8479-3 (no.jil.lengkap)
978-634-04-8480-9 (jil.1)

Cetakan Pertama:
Januari, 2026

PENERBIT:
HADLA
MEDIA INFORMASI

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan buku *Analisis Forensik Digital* ini. Buku ini hadir sebagai upaya untuk memberikan pemahaman komprehensif mengenai bagaimana forensik digital dilakukan dengan tetap memenuhi dan mengikuti metode yang berlaku dan secara ilmiah dapat dipertanggungjawabkan.

Perkembangan teknologi informasi yang begitu pesat dan kejahatan komputer yang meningkat, menempatkan forensik digital sebagai upaya dalam menginvestigasi terhadap insiden dan kejahatan yang dilakukan oleh penyerangan menggunakan perangkat komputer. Kemampuan melakukan analisis forensik yang tepat, terstruktur, dan berbasis kebutuhan menjadi semakin penting karena sangat tidak dimungkinkan jika semua perangkat harus diinvestigasi. Oleh karena itu, materi yang disajikan dalam buku ini disusun secara runtut, mulai dari konsep dasar forensik digital, metode investigasi forensik digital, hingga hambatan dan tantanga, serta etika dalam forensik digital dibahas di buku ini.

Buku ini diharapkan dapat menjadi referensi bagi mahasiswa, peneliti, maupun praktisi yang ingin memahami konsep dan praktik analisis forensik digital secara lebih mendalam. Selain itu, penyajian contoh kasus dan ilustrasi di dalamnya juga dimaksudkan agar pembaca dapat mengaitkan teori dengan situasi nyata yang sering ditemui dalam dunia teknologi informasi.

Penulis menyadari bahwa buku ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan karya ini di masa mendatang. Semoga buku ini dapat memberikan kontribusi yang berarti bagi pengembangan ilmu pengetahuan dan praktik manajemen data serta analisis sistem di berbagai bidang.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dan motivasi dalam proses penyusunan buku ini. Semoga buku ini bermanfaat bagi para pembaca dan menjadi salah satu referensi yang berguna dalam memahami tantangan dan peluang di era digital saat ini.

Hormat kami,

Tim Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
Forensik Digital

A. Definisi, Tujuan, Ruang Lingkup Forensik Digital

1. Definisi Forensik Digital

Forensik digital merupakan cabang ilmu forensik yang berfokus pada identifikasi, akuisisi, pemrosesan, analisis, dan pelaporan bukti digital untuk keperluan hukum. Aktivitas ini mencakup investigasi pada berbagai perangkat elektronik seperti komputer, *smartphone*, hard drive, *smartwatch*, dan lainnya (Muflih et al., 2023), seperti pada Gambar 1.1. M. Nuh Al-Azhar menjelaskan bahwa proses forensik digital menuntut keahlian teknis dan ketelitian prosedural dalam menjaga integritas bukti sejak dari Tempat Kejadian Perkara (TKP) hingga proses persidangan (Al-Azhar, 2012). Ia menekankan pentingnya pendekatan sistematis untuk memastikan bahwa data yang dikumpulkan dapat diterima sebagai bukti sah di pengadilan.

Gambar 1.1 Jenis Perangkat Elektronik (Daniel, 2024)

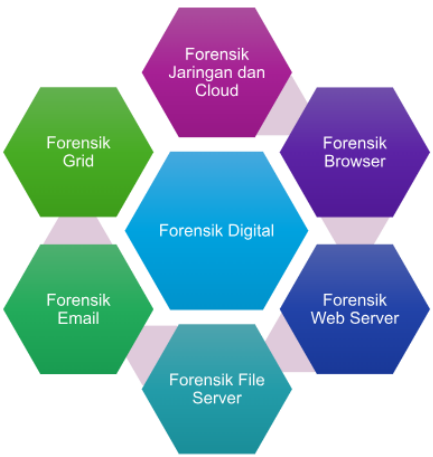
2. Tujuan Forensik Digital

Tujuan utama forensik digital adalah mengungkap kebenaran yang tersembunyi di balik aktivitas digital, khususnya dalam konteks tindak kejahatan siber, pelanggaran kebijakan organisasi, atau konflik hukum. Proses ini tidak hanya bertujuan menemukan pelaku, waktu kejadian, dan modus operandi, tetapi juga menyediakan rekonstruksi aktivitas digital yang akurat dan dapat diverifikasi (Casey, 2011). Imam Riadi dan Rusydi Umar dalam penelitian mereka menunjukkan bahwa penerapan metode National Institute of Justice (NIJ) dapat memfasilitasi tahapan investigasi digital yang valid dan sistematis, seperti dalam kasus forensik (*solid state drive)* SSD (Riadi et al., 2018). Tujuan akhir dari proses ini adalah untuk menyediakan laporan forensik yang dapat dipertanggungjawabkan secara teknis maupun hukum dari bukti digital yang ada, Gambar 1.2.

Gambar 1.2 Berbagai Jenis Bukti Digital (Morgan, 2023)

3. Ruang Lingkup Forensik Digital

Ruang lingkup forensik digital sangat luas dan terus berkembang seiring dengan kompleksitas teknologi informasi. Menurut M. Nuh Al-Azhar, cakupannya meliputi komputer, jaringan, perangkat seluler, sistem cloud, hingga multimedia (gambar, audio, dan video) (Al-Azhar, 2012), sehingga terdapat banyak jenis forensik digital sesuai perkembangan teknologi, Gambar 1.3. Setiap jenis perangkat atau media memiliki tantangan tersendiri, baik dalam hal teknik akuisisi data maupun strategi analisisnya. Misalnya, Riadi dan Umar mencatat bahwa pada media SSD, hanya sekitar 28,7% bukti digital yang dapat dipulihkan secara efektif dengan salah satu *software* pembeku drive yaitu *Shadow Defender* yang dapat membekukan suatu drive SSD (*frozen solid state drive*) (Riadi et al., 2018).



Gambar 1.3 Jenis Forensik Digital

Hal ini menunjukkan bahwa setiap jenis investigasi memerlukan pendekatan forensik yang disesuaikan, serta metodologi yang tepat guna menjaga validitas bukti yang diperoleh. Gambar 1.3 menggambarkan cakupan utama dari forensik digital yang terbagi ke dalam beberapa bidang spesifik berdasarkan sumber atau jenis media digital yang menjadi objek investigasi. Di pusat diagram terdapat "Forensik Digital" sebagai inti disiplin ilmu, yang kemudian bercabang menjadi enam bidang aplikasi utama yang akan dibahas di buku ini pada sub bahasan yang lain: forensik jaringan dan cloud, forensik browser, forensik web server, forensik file server, forensik email, dan forensik grid. Masing-masing bidang ini memiliki pendekatan teknis dan tantangan forensik yang berbeda, tergantung pada karakteristik data dan lingkungan sistem yang dianalisis.

Sebagai contoh, forensik jaringan dan cloud berfokus pada pengumpulan bukti dari lalu lintas jaringan, log koneksi, serta layanan berbasis cloud yang tersebar, sehingga memerlukan metode seperti packet sniffing, API logging, dan korelasi timestamp multisumber. Forensik browser berperan penting dalam menganalisis histori penelusuran, cache, cookie, dan file sementara untuk melacak aktivitas daring pengguna. Sementara itu, forensik web server memeriksa log server HTTP, file konfigurasi, dan direktori root untuk

BAB 2
Forensik Tata Kelola TI

A. Pengantar Forensik dalam Tata Kelola TI

Tata Kelola Teknologi Informasi (TI) mengacu pada struktur, kebijakan, dan proses yang digunakan organisasi untuk memastikan bahwa TI mendukung dan memperluas tujuan bisnis Organisasi (ISACA, 2019). Forensik digital, sebagai bagian dari keamanan informasi dan respons insiden, memiliki peran penting dalam mendukung tata kelola TI dengan menyediakan bukti digital yang valid dan sah untuk audit, kepatuhan, dan investigasi (Casey, E. ,2011).

Forensik Tata Kelola TI adalah penerapan prinsip dan teknik forensik digital untuk menilai efektivitas, efisiensi, dan kepatuhan proses tata kelola TI terhadap kebijakan dan peraturan yang berlaku. Pendekatan ini mencakup pengumpulan, analisis, dan pelaporan bukti digital yang relevan dengan pengambilan keputusan dan pengawasan manajemen TI.

Forensik Tata Kelola TI tidak hanya berfokus pada pencarian pelaku insiden, tetapi lebih luas lagi mencakup penilaian kontrol internal, kepatuhan terhadap standar tata kelola, serta perbaikan berkelanjutan terhadap sistem dan kebijakan TI. Peran ini sangat penting terutama pada

organisasi yang mengandalkan sistem informasi sebagai bagian dari operasional dan strategi bisnis. (Grispos. G, 2017)

Integrasi antara proses tata kelola dan forensik digital memungkinkan organisasi untuk memperkuat struktur pengendalian internal dan meningkatkan ketahanan siber secara menyeluruh. Hal ini mendukung terciptanya sistem tata kelola yang tidak hanya responsif terhadap insiden, tetapi juga preventif dan adaptif terhadap dinamika ancaman digital. (Brown, Gommers, 2013)

B. Mengapa Forensik Penting dalam Tata Kelola TI

Forensik memainkan peran strategis dalam tata kelola TI, terutama dalam hal:

1. Mengidentifikasi pelanggaran kebijakan internal seperti penyalahgunaan sumber daya TI, akses tidak sah, atau manipulasi data (Ogunbukola, 2024).
2. Mendukung audit internal dan eksternal melalui penyediaan bukti digital yang autentik dan dapat diverifikasi (Ogunbukola, 2024; Enterprise Security Mag, 2024).
3. Menjamin integritas sistem dan data dengan mendeteksi perubahan tidak sah, penyusupan, atau aktivitas abnormal (Ogunbukola, 2024).

4. Membantu pengambilan keputusan berbasis bukti sehingga manajemen dapat melakukan tindakan korektif yang tepat (Impact My Biz, 2024).
5. Menjadi mitigasi risiko reputasi dan finansial dengan mempercepat respons terhadap insiden dan mencegah eskalasi pelanggaran (Enterprise Security Mag, 2024; Ogunbukola, 2024).

Implementasi prinsip-prinsip forensik dalam tata kelola TI membantu membangun sistem pengawasan yang responsif, mendeteksi potensi anomali, dan menjaga kredibilitas organisasi di mata pemangku kepentingan dan regulator.

C. *Framework* dan Standar yang Mendukung

Beberapa *framework* dan standar internasional yang mendukung integrasi forensik dalam tata kelola TI antara lain:

1. COBIT 2019: Menyediakan kerangka kerja tata kelola TI terstruktur. Proses seperti:
    - MEA03: Monitor, Evaluate and Assess Compliance
    - BAI08: Manage Knowledge (termasuk dokumentasi insiden dan pelajaran yang diambil)
    - DSS05: Manage Security Services (terkait penanganan insiden)

2. ISO/IEC 27001 dan ISO/IEC 27002: Standar sistem manajemen keamanan informasi, termasuk kontrol terhadap audit dan logging.
3. ISO/IEC 27037: Panduan identifikasi, pengumpulan, akuisisi, dan pelestarian bukti digital.
4. NIST SP 800-61 & SP 800-86: Panduan respons insiden dan integrasi teknik forensik ke dalam proses.

Dengan mengacu pada kerangka kerja ini, organisasi dapat memastikan setiap langkah forensik dilakukan secara sah, terdokumentasi, dan dapat dipertanggungjawabkan dalam ranah hukum dan operasional.

D. Langkah-Langkah Forensik dalam Tata Kelola TI

Berdasarkan pendapatn (Casey, 2011) ,implementasi forensik dalam tata kelola TI dilakukan melalui langkah-langkah berikut:

Gambar 2.1 Tahapan Forensik Tata Kelola TI

i. Identification (Identifikasi)

Proses awal untuk mendeteksi dan mengenali adanya insiden keamanan atau pelanggaran yang memerlukan investigasi forensik. Fokus pada penentuan sumber insiden,

sistem yang terdampak, dan jenis pelanggaran. Tahapan ini dapat dipicu oleh:

1. Hasil audit internal
2. Laporan whistleblower
3. Sistem deteksi intrusi (IDS/IPS)

Tujuan:

Menentukan bahwa suatu insiden telah terjadi dan memutuskan ruang lingkup investigasi forensik.

Beberapa aktivitas yang dilakukan:

1. Mendeteksi anomali atau pelanggaran kebijakan melalui log SIEM (Security Information and Event Management).
2. Melakukan triase awal terhadap laporan insiden dari tim keamanan TI.
3. Mengidentifikasi sistem, data, dan pengguna yang terlibat.

Adapun Luaran dari aktivitas diatas adalah sebagai berikut:

1. Dokumen insiden (Incident Log).
2. Surat penugasan investigasi.
3. Peta awal sistem terdampak dan daftar artefak potensial.
4. Identifikasi kontrol tata kelola yang mungkin dilanggar (misalnya kontrol akses pengguna).

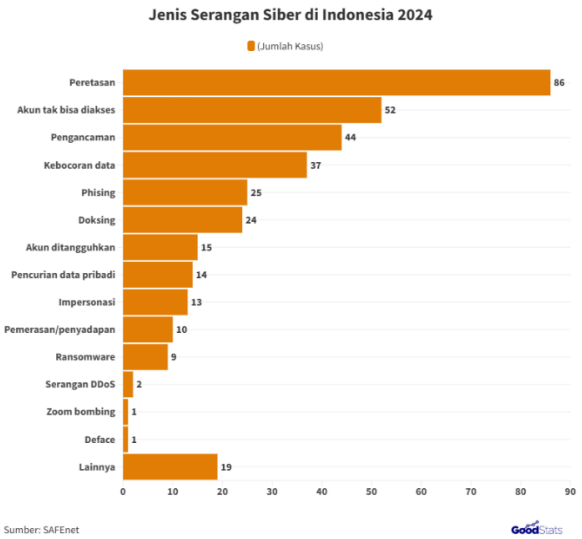
ii. Preservation (Preservasi / Pelestarian)

Tahap pelestarian bukti digital dengan cara mengamankan dan menjaga keaslian data agar tidak berubah

BAB 3
Forensik Cloud

A. Pengantar

Forensik digital merupakan cabang dari ilmu forensik yang bermanfaat dalam pembuktian tindak kejahatan yang memanfaatkan teknologi informasi. Kejahatan yang dilakukan oleh para pelaku kejahatan yang memanfaatkan teknologi informasi ini mengalami perkembangan yang cukup signifikan, baik secara kuantitas maupun kualitas. Tindakan kejahatan ini juga dikenal sebagai cyber crime juga mengalami peningkatan kejadiannya di Indonesia(Agnes Z. Yonatan, 2025) yang dapat dilihat pada Gambar 3.1.



Gambar 3.1 Jenis Serangan Siber di Indonesia

Peretasan menempati peringkat teratas sebagai jenis serangan siber yang paling sering terjadi di Indonesia. Fenomena ini menunjukkan bahwa sistem keamanan siber di berbagai sektor masih rentan terhadap akses tidak sah yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Dampaknya bisa sangat merugikan, baik dari segi finansial, reputasi, maupun kerahasiaan data. Oleh karena itu, penanganan kasus peretasan menjadi isu krusial dalam konteks keamanan digital. Dalam hal ini, kajian forensik digital memainkan peran penting untuk mengidentifikasi jejak digital, mengumpulkan bukti, serta menganalisis pola serangan guna mendukung proses investigasi dan penegakan hukum. Forensik digital tidak hanya membantu menemukan pelaku, tetapi juga memberikan pemahaman lebih dalam tentang modus operandi serangan, sehingga dapat digunakan untuk meningkatkan sistem pertahanan dan mencegah serangan serupa di masa mendatang.

Forensik cloud merupakan salah satu cabang dari ilmu forensik digital(Sudyana et al., 2023) yang berfokus pada investigasi insiden keamanan siber dalam lingkungan komputasi awan (cloud computing). Tujuan utama forensik cloud adalah mengidentifikasi, mengumpulkan, mengevaluasi, dan menjaga integritas bukti digital yang disimpan atau diproses di cloud. Metode ini sangat berguna

untuk menemukan kejahatan digital yang terjadi melalui layanan cloud, seperti peretasan, pencurian data, atau penggunaan akses yang salah. Dalam dunia cloud computing, terdapat dua jenis model layanan utama yang perlu dipahami, yaitu public cloud dan private cloud. Keduanya memiliki struktur dasar dan fungsi teknologi yang serupa, namun berbeda dalam hal aksesibilitas dan pengelolaan.

Public cloud adalah jenis layanan cloud yang dapat diakses secara luas oleh masyarakat umum melalui jaringan internet(Solanke, 2014). Layanan ini disediakan oleh penyedia cloud seperti Google Cloud, Microsoft Azure, atau Amazon Web Services, dan ditujukan untuk berbagai kalangan, baik individu maupun organisasi, tanpa batasan institusional. Sebaliknya, private cloud merupakan layanan cloud yang dirancang khusus untuk penggunaan internal suatu organisasi atau perusahaan. Akses ke dalam sistem ini dibatasi hanya untuk pengguna yang berada di dalam lingkup institusi tertentu, sehingga lebih eksklusif dan aman untuk kebutuhan yang bersifat sensitif, seperti data keuangan atau informasi rahasia perusahaan. Pemahaman terhadap perbedaan kedua jenis cloud ini sangat penting dalam forensik cloud, karena setiap jenis memerlukan pendekatan dan metode investigasi yang berbeda, terutama dalam hal akses data, otorisasi, serta prosedur hukum yang berlaku.

Baik forensik cloud publik maupun privat menganut prinsip yang sama dengan forensik digital secara keseluruhan. Hal ini karena forensik digital mencakup forensik cloud sebagai salah satu subbidangnya. Oleh karena itu, teknik, konsep, dan proses forensik digital dapat ditransfer ke forensik cloud. Artinya, proses seperti pengumpulan bukti digital, analisis data, pelestarian integritas informasi, dan pelaporan hasil investigasi dilakukan dengan pendekatan yang konsisten di antara keduanya. Meskipun lingkungan cloud memiliki karakteristik teknisnya sendiri, seperti arsitektur berbasis virtualisasi, multi-tenancy, dan skala elastis, langkah-langkah forensik tetap berada dalam kerangka standar yang telah ditetapkan oleh praktik forensik digital yang diakui secara luas. Ini termasuk penerapan prinsip-prinsip seperti rantai penyimpanan, dokumentasi sistematis, dan validitas data yang dapat diuji di pengadilan.

Gambar 3.2 Posisi Ilmu Forensik Cloud

Gambaran mengenai hubungan antara forensik cloud dan forensik digital dapat dilihat pada Gambar 3.2, yang menunjukkan bahwa forensik cloud merupakan sub-bagian dari lingkup yang lebih luas, yaitu forensik digital. Oleh karena itu, ketika seorang analis forensik bekerja dalam lingkungan cloud, ia tetap harus mematuhi pedoman dan kerangka kerja yang berlaku di dunia forensik digital secara umum(Zawoad, 2013). Sehingga dapat dikatakan meskipun terdapat perbedaan pada aspek teknis implementasinya, secara prinsip tidak ada perbedaan mendasar antara standar yang digunakan dalam forensik digital dan forensik cloud. Keduanya berjalan beriringan dalam upaya menjaga validitas dan legalitas bukti digital yang dikumpulkan dari sistem berbasis cloud. Perbedaan ilmu forensik, forensik digital dan forensik cloud terletak pada obyek yang akan diakuisisi data forensiknya, kadang juga tool yang digunakan dalam akuisisi juga terdapat perbedaan.

B. Karakteristik Cloud Computing

Layanan cloud yang dapat dinikmati oleh para konsumennya terbagi menjadi tiga bentuk layanan(Wintolo et al., 2020), yaitu:

1. Infrastructure as a Service(IaaS). Perusahaan layanan cloud computing yang menyediakan bentuk layanan

BAB 4
Forensik Browser

A. Pendahuluan

Perkembangan teknologi internet telah membawa banyak kemudahan, tetapi juga tantangan besar dalam hal keamanan dan privasi (Syukri et al., 2025). Salah satu fitur yang banyak digunakan oleh pengguna untuk menjaga privasi saat berselancar di dunia maya adalah mode privat atau incognito mode pada browser. Mode ini dirancang untuk tidak menyimpan riwayat penelusuran, data formulir, maupun cookie setelah sesi ditutup. Namun, pertanyaan kritis muncul: apakah mode privat benar-benar mampu menjaga data pribadi pengguna? (Fernández-Fuentes et al., 2022).

Forensik digital hadir untuk menjawab pertanyaan tersebut dengan pendekatan sistematis dalam mengungkap bukti digital, termasuk dari browser yang digunakan dalam mode privat(Fernández-Fuentes et al., 2023). Melalui metode investigasi seperti National Institute of Standards and Technology (NIST), dapat diketahui sejauh mana data tetap "tersisa" dalam sistem, khususnya pada memori (RAM), meskipun tidak tampak secara kasat mata(Imam Riadi et al., 2021).

Forensik digital merupakan disiplin ilmu yang menggunakan metode ilmiah untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi, serta mempresentasikan barang bukti digital yang terkait dengan suatu kasus. Tujuan dari proses ini adalah untuk merekonstruksi kejadian dan memastikan keabsahan bukti dalam proses peradilan (Agarwal & Gupta, 2011).

Menurut ISACA (2015), forensik digital juga dapat dipahami sebagai proses identifikasi, pemeliharaan, analisis, dan penyajian bukti digital dengan cara yang dapat diterima secara hukum, khususnya dalam konteks hukum seperti pengadilan.

Sejalan dengan itu, Altheide & Carvey (2011) menekankan bahwa forensik digital melibatkan penggunaan metode yang terbukti efektif dalam memperoleh, memvalidasi, mengumpulkan, serta menganalisis bukti digital. Bukti tersebut kemudian dipresentasikan untuk mendukung rekonstruksi peristiwa yang berhubungan dengan tindak kriminal atau untuk memfasilitasi tindakan operasional yang telah direncanakan.

Selain itu, Zou, Huang, Lei, Zhou, & Zheng (2015) menjelaskan bahwa meskipun forensik digital sering diasosiasikan dengan penyelidikan kesalahan atau kejahatan,

dalam beberapa tahun terakhir, ia juga berkembang menjadi alat yang penting untuk pelestarian dan kurasi digital.

Pendekatan ini berperan dalam melindungi dan menyelidiki bukti kejahatan yang telah terjadi, serta membantu dalam pengawasan yang lebih efektif terhadap bukti digital dalam berbagai konteks.

Dengan demikian, forensik digital bukan hanya berfungsi sebagai sarana untuk penyelidikan kriminal, tetapi juga sebagai pendekatan ilmiah yang memungkinkan pengelolaan dan investigasi bukti digital secara sah dan sistematis(Riadi, Imam, Muthohirin, 2022).

B. Dasar Teori Forensik Browser

Forensik browser merupakan cabang dari forensik digital(Wibowo et al., n.d.) yang secara spesifik meneliti aktivitas browser, termasuk data yang ditinggalkan selama atau setelah sesi penelusuran, baik pada mode reguler maupun mode privat. Penelitian forensik terhadap browser melibatkan proses identifikasi, ekstraksi, analisis, dan pelaporan terhadap data digital yang berhubungan dengan aktivitas pengguna(Pribadi et al., 2023).

Mode privat hanya membatasi penyimpanan data di hard disk(Imam Riadi et al., 2020), namun tidak mencegah keberadaan informasi dalam RAM(Iqbal et al., 2022). Oleh

karena itu, forensik live(Rochmadi, 2019), yakni pengambilan bukti dari sistem yang sedang berjalan, sangat penting untuk mengidentifikasi potensi kebocoran data yang tidak terlihat secara umum.

C. Metodologi Forensik Browser

Untuk melaksanakan investigasi yang akurat dan sah secara hukum, berbagai metode forensik digital telah dikembangkan. Beberapa metodologi yang paling dikenal dan banyak digunakan dalam dunia forensik digital adalah National Institute of Justice (NIJ), National Institute of Standards and Technology (NIST), ACPO (Association of Chief Police Officers), dan Digital Forensic Research Workshop (DFRWS). Setiap metodologi memiliki karakteristik yang berbeda dan dapat dipilih sesuai dengan konteks investigasi yang dilakukan.

1. NIJ (National Institute of Justice)

NIJ adalah lembaga yang berfokus pada pengembangan pedoman forensik digital khusus untuk aplikasi di dunia penegakan hukum di Amerika Serikat. Pedoman yang disusun oleh NIJ menekankan pada standar yang memastikan bahwa bukti digital yang ditemukan selama investigasi dapat diterima secara hukum. Metode ini sering digunakan dalam investigasi yang melibatkan hukum kriminal.

Kelebihan:

- Menyediakan pedoman yang sangat aplikatif dalam konteks penegakan hukum.
- Memastikan pengumpulan dan pengelolaan bukti yang sah secara hukum.

Kekurangan:

- Kurang fleksibel dalam aplikasi di luar penegakan hukum.
- Fokus utamanya pada praktik di Amerika Serikat, yang mungkin tidak selalu relevan di negara lain.

2. NIST (National Institute of Standards and Technology)

NIST adalah salah satu lembaga yang paling dihormati dalam bidang forensik digital, dan memiliki metodologi yang sangat terstruktur dan dapat diterima di seluruh dunia. Metode NIST terdiri dari empat tahap utama: collection (pengumpulan data), examination (pemeriksaan data), analysis (analisis data), dan reporting (pelaporan). Prosedur yang sangat sistematis ini memastikan bahwa bukti yang dikumpulkan selama investigasi dapat dipertanggungjawabkan, baik dari segi teknis maupun hukum.

Kelebihan:

- Diakui secara internasional: Standar yang diterima luas di berbagai negara.

- Prosedur yang terstruktur: Memastikan konsistensi dan validitas hasil investigasi.
- Fleksibel: Dapat diterapkan dalam berbagai konteks, baik dalam dunia penegakan hukum, keamanan siber, maupun riset akademik.

Kekurangan:

- Memerlukan pemahaman teknis yang mendalam: Pendekatan ini mungkin sulit diterapkan oleh pihak yang tidak memiliki latar belakang teknis.
- Kurang fokus pada konteks hukum spesifik: Pada beberapa kasus, prosedur NIST mungkin lebih berorientasi pada aspek teknis, sehingga dapat kurang memadai dalam konteks yang lebih fokus pada peraturan hukum tertentu.

3. ACPO (Association of Chief Police Officers)

Metode yang dikembangkan oleh ACPO di Inggris lebih berfokus pada pengumpulan dan pengelolaan bukti digital yang sah secara hukum dalam konteks penegakan hukum. ACPO memberikan pedoman yang dirancang untuk memastikan bahwa bukti yang diperoleh dapat diterima di pengadilan, dengan menekankan pentingnya prosedur yang sesuai dengan peraturan hukum yang berlaku.

BAB 5
Forensik Webserver

A. Pendahuluan

Dalam era digital saat ini, web server tidak hanya menjadi komponen teknis dalam ekosistem teknologi informasi, tetapi telah berevolusi menjadi fondasi utama dari hampir seluruh layanan daring mulai dari portal berita, layanan perbankan, sistem pendidikan, hingga aplikasi pemerintahan (Budianto et al., 2025). Fungsinya yang vital sebagai penyedia, pengelola, dan penjaga data menjadikannya sasaran strategis bagi berbagai bentuk ancaman siber (Rusydi et al., 2024). Serangan seperti *website defacement*, pencurian data, *malware injection*, dan serangan *denial-of-service* (DoS) telah menjadi ancaman nyata yang berpotensi mengganggu ketersediaan layanan dan merusak integritas sistem.

Dengan semakin kompleksnya lanskap kejahatan siber, kebutuhan akan kemampuan forensik digital yang handal menjadi sangat mendesak. Forensik digital pada *web server* tidak hanya berfungsi untuk menelusuri jejak pelaku setelah insiden terjadi, tetapi juga sebagai pendekatan sistematis dalam mendokumentasikan, menganalisis, dan merekonstruksi peristiwa siber secara sahih dan legal. Forensik digital berperan penting dalam mengungkap

kejahatan siber yang menyerang infrastruktur daring seperti *web server*, melalui proses identifikasi, pengumpulan, dan analisis artefak digital (Rachmie, 2020). Perkembangan pesat dalam bidang forensik digital turut mendorong efektivitas penyelidikan terhadap berbagai serangan siber, termasuk yang menyasar sistem berbasis web dan jaringan virtual modern (Iman et al., 2023).

B. Anatomi Web Server dan Arsitektur Umum

Sebelum menyelami lebih dalam ke ranah forensik digital pada infrastruktur web, pemahaman terhadap cara kerja web server dan komponen-komponen utamanya menjadi fondasi yang sangat penting (Ihsan et al., 2023). Web server berperan sebagai perantara antara klien, umumnya melalui peramban web, dan sumber daya digital seperti file HTML, basis data, maupun aplikasi sisi server (Setiawan et al., 2021). Dengan kata lain, web server bertanggung jawab untuk menerima permintaan dari pengguna dan mengembalikannya dalam bentuk halaman atau konten digital yang diminta.

Secara umum, beberapa jenis web server yang banyak digunakan di seluruh dunia memiliki keunggulannya masing-masing (Setiawan et al., 2021). Apache HTTP Server dikenal luas karena fleksibilitas, dukungan modular, serta komunitas yang besar dan aktif, sementara Nginx menonjol karena

kemampuannya melayani konten statis dengan efisien serta perannya sebagai *reverse proxy* yang andal. Di sisi lain, Microsoft Internet Information Services (IIS) dirancang untuk integrasi mendalam dengan ekosistem Windows, menjadikannya solusi ideal bagi organisasi yang bergantung pada teknologi Microsoft. Web server seperti LiteSpeed dan Caddy juga mulai populer karena fitur keamanan bawaan, konfigurasi otomatis, serta efisiensi dalam beban kerja tertentu (Ihsan et al., 2023).

Untuk memahami keseluruhan ekosistem kerja web server, perlu dipahami arsitektur umumnya yang terdiri dari berbagai komponen. Sistem operasi seperti Linux (*Ubuntu, CentOS, Debian*) dan Windows Server berfungsi sebagai landasan, di atasnya dijalankan perangkat lunak *web server* seperti *Apache, Nginx, atau IIS. Web server* ini kemudian berinteraksi dengan bahasa pemrograman sisi server seperti *PHP, Python, Ruby, Node.js,* hingga *ASP.NET*, serta dihubungkan dengan sistem basis data seperti *MySQL, PostgreSQL, MongoDB,* atau *SQL Server* untuk penyimpanan dan pengambilan data (Setiawan et al., 2021). Dalam struktur yang lebih kompleks, dapat pula ditemukan server aplikasi seperti *Tomcat* atau *JBoss*, serta komponen tambahan seperti *load balancer, reverse proxy, CDN*, dan *Web Application*

Firewall (WAF) guna menunjang performa dan keamanan layanan (Ihsan et al., 2023).

1. Peran dan Fungsi Web Server

Web server memegang peran fundamental dalam arsitektur sistem informasi modern sebagai penghubung utama antara klien umumnya browser pengguna dan konten web yang disimpan di sisi server (R. A. Ginting & Siregar, 2022). Fungsi utamanya meliputi penerimaan permintaan (*request*) dari klien melalui protokol HTTP atau HTTPS, pemrosesan permintaan tersebut, dan pengiriman respons yang sesuai dalam bentuk file statis (seperti HTML, CSS, gambar), data dari basis data, atau hasil eksekusi aplikasi web dinamis (Alviando et al., 2023). Dengan demikian, *web server* bertindak sebagai jembatan yang menjamin komunikasi dua arah antara pengguna dan layanan digital berlangsung secara efisien, aman, dan dapat diandalkan.

2. Jenis-Jenis Web Server Populer

Dalam pengelolaan web modern, sejumlah web server populer menawarkan keunggulan masing-masing yang signifikan (R. A. Ginting & Siregar, 2022). Apache HTTP Server dikenal karena fleksibilitas dan modularitas yang tinggi; sebagai server tertua dan paling banyak digunakan, Apache mendukung berbagai modul mulai dari autentikasi hingga penataan URL (Putra & Prasetyo, 2023). Nginx

menonjol dalam hal performa dan efisiensi: mengadopsi arsitektur event-driven, server ini mampu menangani ribuan koneksi simultan dengan jejak memori rendah, sekaligus populer sebagai *reverse proxy* dan server statis (Siregar & Siregar, 2022). Microsoft IIS, yang terintegrasi erat dalam ekosistem Windows, menjadi pilihan utama organisasi yang mengandalkan platform ini karena kemudahan integrasi dan manajemen. Selain itu, LiteSpeed Web Server menawarkan performa tinggi sebagai *drop-in replacement* untuk Apache: arsitektur *event-driven*, kompatibilitas dengan konfigurasi Apache, dan fasilitas caching canggih menjadikannya efisien untuk lalu lintas tinggi (Putra & Prasetyo, 2023). Sementara itu, Caddy memikat karena fitur otomatisasi HTTPS termasuk *Encrypted Client Hello* (ECH), sertifikat TLS tanpa konfigurasi, serta fokus pada kemudahan penggunaan. Dengan demikian, pilihan web server dapat disesuaikan berdasarkan kebutuhan organisasi, seperti fleksibilitas dan modularitas (*Apache*), performa dan efisiensi (*Nginx, LiteSpeed*), integrasi sistem operasi (IIS), serta otomatisasi konfigurasi keamanan (*Caddy*) (Yuliana & Nugroho, 2024).

3. Arsitektur Umum Web Server

Arsitektur umum sebuah web server terdiri dari berbagai komponen yang saling terintegrasi untuk memastikan layanan web berjalan optimal (Setiawan et al., 2021). Pada lapisan

BAB 6
Forensik File Server

A. Pendahuluan

Forensik digital merupakan disiplin ilmu yang bertujuan untuk mengidentifikasi, mengumpulkan, menganalisis, dan melaporkan bukti digital secara sah dan akurat guna mendukung proses penyelidikan dan pengambilan keputusan (Casey, 2023). Dalam infrastruktur teknologi informasi, file server memegang peranan penting sebagai penyimpan dan pengelola data yang kritis. Oleh sebab itu, forensik pada file server menjadi aspek yang sangat vital untuk mengungkap insiden keamanan serta mendukung proses pengambilan keputusan yang optimal.

Namun, pengambilan keputusan yang akurat sering kali terhambat oleh masalah missing value pada data forensik yang dikumpulkan dari file server, baik akibat kerusakan data, manipulasi, maupun keterbatasan log. Hal ini menimbulkan kebutuhan untuk mengembangkan model adaptif dalam menangani missing value guna memaksimalkan kualitas analisis dan keputusan yang dihasilkan dalam penyelidikan forensik (Zhang et al., 2024).

Forensik File Server merupakan disiplin dalam forensik digital yang khusus menangani proses identifikasi,

pengumpulan, analisis, dan pelaporan bukti elektronis yang tersimpan di file server. File server sangat vital dalam infrastruktur teknologi informasi (TI) organisasi karena berfungsi sebagai pusat penyimpanan dan pengelolaan data penting yang mendukung operasional bisnis. Di tengah meningkatnya ancaman siber, termasuk malware, serangan ransomware, dan akses tidak sah, fungsi forensik file server menjadi sangat penting untuk menjaga integritas, ketersediaan, dan kerahasiaan data (Casey, 2011).

Salah satu masalah signifikan yang dihadapi dalam forensik file server adalah fenomena *missing value* atau data yang hilang. Kehilangan data ini dapat disebabkan oleh sejumlah faktor, seperti kegagalan perangkat keras, korupsi data, penghapusan sengaja untuk menutupi jejak, atau mekanisme pemeliharaan otomatis pada sistem file server. Dalam konteks investigasi forensik, *missing value* dapat mengakibatkan kesenjangan informasi yang berpotensi menghambat proses rekonstruksi kejadian, analisis jejak digital, dan pembuktian dalam ranah hukum (Pal, 2016). Evaluasi alat forensik sangat penting dalam mengidentifikasi dan menangani kejanggalan atau kehilangan data selama investigasi kejahatan digital (Rusydi Umar et al., 2018).

Mengelola *missing value* dalam forensik file server memerlukan pendekatan dan metodologi yang sistematis dan

cermat. Salah satu pendekatan adalah penggunaan teknik rekonstruksi dan pemulihan data melalui metode forensik khusus yang mampu mengidentifikasi keberadaan data yang hilang atau tersembunyi dan mengembalikannya ke dalam bentuk yang utuh atau dapat dianalisis (Carrier, 2005). Selain itu, penggunaan algoritma analisis statistik dan teknik imputasi data juga dapat membantu dalam memperkirakan dan menangani *missing value*, sehingga mengurangi bias dan meningkatkan keandalan hasil forensik (Little & Rubin, 2019).

Tantangan lain yang melekat adalah perkembangan teknologi penyimpanan yang semakin kompleks, seperti penggunaan enkripsi, sistem file terdistribusi, dan virtualization, yang dapat memperumit proses deteksi dan penanganan data yang hilang. Oleh karena itu, forensik file server harus disertai dengan pengetahuan teknis mendalam, pemahaman tentang arsitektur penyimpanan, serta keterampilan menggunakan perangkat dan metode analisis terbaru (Altheide & Carvey, 2011).

B. Konsep Dasar Forensik File Server

File Server adalah server khusus yang bertugas menyimpan, mengatur, dan mengelola akses ke file di jaringan komputer (Singh & Kumar, 2022). Dalam konteks forensik,

file server menyimpan berbagai jenis artefak digital seperti log akses, metadata file, aktivitas file system, dan data konfigurasi yang dapat memberikan bukti penting dalam investigasi keamanan siber.

Tantangan utama dalam forensik file server meliputi kompleksitas jumlah data, kerusakan atau kehilangan data (missing data), serta kebutuhan untuk analisis yang cepat dan tepat. Missing value khususnya dapat mengurangi efektivitas dan akurasi analisis forensik, sehingga diperlukan metode penanganan yang adaptif dan canggih untuk mengatasi kendala ini (Lee & Park, 2023).

Konsep dasar dari forensik file server meliputi pemahaman tentang arsitektur file server, sistem file yang digunakan, teknik pengumpulan data, serta metodologi analisis bukti digital. Sistem file server mengelola penyimpanan dan akses data menggunakan berbagai sistem file seperti NTFS, FAT, ext4, atau sistem file terdistribusi yang lebih kompleks. Pengetahuan terhadap struktur dan karakteristik sistem file ini sangat penting agar investigator dapat mengidentifikasi dan mengekstrak bukti digital secara akurat (Carrier, 2005).

Selain itu, forensik file server juga melibatkan teknik pengumpulan data yang terstruktur dan sesuai prosedur agar bukti tetap terjaga keasliannya dan dapat diterima secara

hukum. Teknik ini mencakup pembuatan image bitwise dari media penyimpanan, pencatatan metadata file, serta pemantauan jejak digital seperti log akses dan aktivitas modifikasi file (Altheide & Carvey, 2011).

Forensik file server tidak hanya bergantung pada kemampuan teknis, tetapi juga harus mengikuti standar dan regulasi keamanan yang berlaku serta prinsip-prinsip etika untuk memastikan proses investigasi berjalan adil dan transparan. Dengan fondasi konsep dasar yang kuat, praktisi forensik dapat menjalankan tugasnya secara efektif dalam mengungkap kejadian digital dan memberikan kontribusi penting dalam penegakan hukum dan keamanan data organisasi.

C. Missing Value dalam Forensik File Server

Missing value atau nilai data yang hilang dapat berasal dari berbagai sumber, seperti kesalahan pencatatan log, kerusakan media penyimpanan, atau manipulasi oleh pelaku kejahatan (Chen et al., 2021). Dalam konteks forensik file server, missing data dapat menyebabkan keraguan terhadap keabsahan temuan serta menghambat proses pengambilan keputusan yang kritis. Penggunaan metode forensik jaringan dan tools IDS dapat membantu mengidentifikasi anomali dan kejadian serangan yang berpotensi menyebabkan kehilangan

data pada sistem file server (Riadi I, 2021) . Selain itu, teknik live forensic acquisition pada SSD memberikan wawasan penting terkait pemulihan data dan integritas bukti digital yang rentan terhadap missing value akibat fitur pengelolaan data seperti TRIM (Riadi I, 2022).

Dampak missing value ini signifikan, karena dapat menyebabkan bias dalam analisis, mengurangi keakuratan rekonstruksi kejadian, dan memperlambat proses investigasi (Patel & Shah, 2022). Oleh karena itu, penanganan missing value harus dilakukan secara sistematis dan adaptif mengikuti karakteristik data dan konteks investigasi.

D. Jenis Missing Value di File Server

Jenis missing value di file server dapat dikategorikan berdasarkan mekanisme hilangnya data, yaitu:

1. Missing Completely at Random (MCAR)

Data hilang secara acak tanpa pola tertentu dan tidak terkait dengan nilai data lain maupun variabel pengamatan. Contohnya adalah kegagalan sensor log yang terjadi secara tiba-tiba dan tidak dipengaruhi oleh kondisi lain (Lee et al., 2021).

2. Missing at Random (MAR)

Ketidakhadiran data bergantung pada variabel lain yang diamati, tetapi tidak bergantung pada nilai data yang hilang itu

sendiri. Contoh kasusnya adalah kegagalan pencatatan log yang terkait dengan jam sibuk operasi server namun tidak terkait langsung dengan isi data log (Patel & Singh, 2022).

3. Missing Not at Random (MNAR)

Data hilang dengan alasan yang berhubungan langsung dengan nilai data yang hilang. Misalnya, manipulasi data sensitif oleh pelaku kejahatan untuk menutupi jejak aktivitas yang mencurigakan (Kumar et al., 2024).

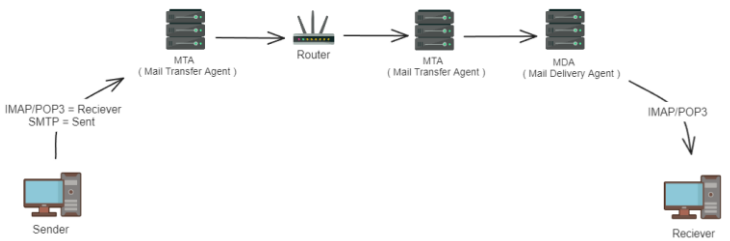
Gambar 6.1 Jenis-Jenis Missing Value

Pemahaman yang mendalam tentang sumber dan jenis missing value ini sangat penting guna memilih metode penanganan data yang sesuai dan efektif dalam forensik file server (Cheng & Tan, 2023). Model adaptif yang relevan harus mempertimbangkan karakteristik jenis missing value

BAB 7
Forensik Email

A. Pendahuluan

Forensik email adalah bidang dalam digital forensics yang fokus pada identifikasi, pelestarian, pengumpulan, analisis, dan interpretasi bukti dari sistem email. Sebagai salah satu artefak digital utama dalam penyelidikan kejahatan siber, forensik email menganalisis tidak hanya isi pesan, tetapi juga struktur teknis seperti header, metadata, jalur pengiriman, dan artefak di server atau perangkat pengguna (Casey, E., 2011).



Gambar 7.1 Email Architecture

Dalam arsitektur umum, email dibangun di atas protokol standar seperti SMTP, POP3, dan IMAP yang secara eksplisit mengatur format pesan, struktur header, dan alur distribusi melalui server. Standarisasi ini membuat forensik email dapat dilakukan secara sistematis dan terukur (Garfinkel, S., 2019).

Email sering menjadi medium utama dalam serangan seperti phishing, BEC, malware, dan rekayasa sosial. Laporan Verizon DBIR menunjukkan bahwa lebih dari 90% serangan berhasil dimulai dari email yang dimanipulasi atau mengandung tautan berbahaya. Sistem email memiliki sifat redundansi yang kuat, mencatat salinan pesan, log server, catatan routing, dan file cache, menjadikannya sumber bukti digital yang stabil.

Bukti email yang dikumpulkan dengan benar dapat diterima di pengadilan sebagai electronic evidence, dengan pedoman teknis seperti SWGDE Best Practices dan NIST 800-86 untuk menjaga integritas dan chain of custody. Layanan cloud seperti Google Workspace dan Microsoft 365 juga menghasilkan audit log yang memperkaya sumber bukti, membuat kompetensi forensik email semakin penting dalam ekosistem komputasi terdistribusi. Forensik email berperan vital dalam mengungkap sumber serangan dan pola operasi pelaku (Nelson, B., Phillips, A., & Steuart, C., 2020).

Tujuan utama forensik email adalah memverifikasi apakah pesan berasal dari sumber yang sah. Teknik seperti analisis header (Received chain), SPF, DKIM, dan DMARC dapat menunjukkan apakah email dipalsukan (spoofing) atau dimodifikasi.

Tujuan utama forensik email adalah memverifikasi keaslian pesan, dengan teknik seperti analisis header, SPF, DKIM, dan DMARC untuk mendeteksi pemalsuan atau modifikasi. Forensik email juga membantu mengidentifikasi manipulasi pengguna, seperti ajakan login palsu, lampiran berbahaya, atau instruksi pembayaran dari akun yang disusupi. Analisis gaya bahasa, struktur pesan, dan URL turut berperan penting.

Lampiran sering mengandung malware atau dokumen yang dimodifikasi. Analisis hash, metadata file, dan dynamic malware analysis dapat mengungkap tujuannya. Korelasi antara email dan aktivitas lain, seperti login sistem atau akses cloud, memberikan gambaran lengkap alur insiden. Temuan email ini dapat dijadikan bukti kuat dalam proses hukum atau investigasi internal organisasi.

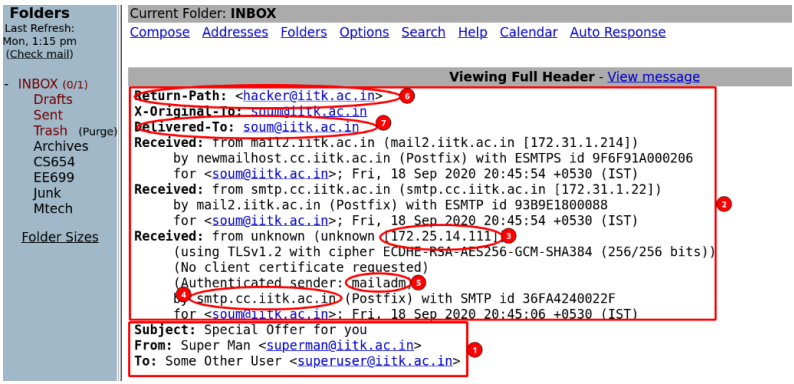
Email spoofing menjadi tantangan karena pelaku dapat memalsukan bidang From dan Return-Path, namun analisis header mendalam dapat mengidentifikasi server asli. Email disimpan dalam berbagai format (PST, OST, MBOX, EML) di perangkat lokal, server, atau cloud, dengan mekanisme akuisisi yang berbeda, menyulitkan pengumpulan bukti. Lampiran sering mengandung malware atau objek berbahaya yang memerlukan sandbox atau memory forensics. Di cloud, artefak forensik tersebar di pusat data dan hanya dapat diakses

melalui audit log. Beberapa artefak yang hilang atau terhapus menyulitkan rekonstruksi bukti (Mandia, K., Prosise, C., & Pepe, M., 2020).

Forensik email adalah kunci dalam investigasi siber, mengungkap serangan dan sumber bukti digital melalui analisis header, metadata, isi, lampiran, dan log server. Tantangan teknis seperti spoofing dan keragaman platform memerlukan kompetensi tinggi. Dengan kerangka yang tepat dan kepatuhan pada standar hukum, forensik email menyediakan bukti yang kuat dan dapat diterima dalam proses hukum dan keamanan organisasi.

B. Jejak Email dan Header Email

Email header adalah bagian metadata dalam sebuah pesan email yang berisi informasi teknis terkait proses pengiriman, identitas pengirim dan penerima, jalur distribusi, serta parameter autentikasi. Email header tidak terlihat oleh pengguna biasa, tetapi menyimpan artefak penting yang dapat digunakan untuk menelusuri asal sebuah email, memvalidasi keasliannya, dan mengidentifikasi adanya modifikasi atau spoofing (Casey, 2011).



Gambar 7.2 Email Headers

Struktur email header mencakup elemen-elemen penting yang memastikan pengiriman dan penerimaan email yang benar dan aman. Elemen seperti "From" dan "To" menunjukkan pengirim dan penerima, meskipun mudah dipalsukan. "Received" mencatat jejak server yang dilalui email, penting untuk melacak jalur pengiriman dan mendeteksi manipulasi. Alamat IP pengirim, "172.25.14.111," serta server SMTP "smtp.cc.iitk.ac.in" menunjukkan sumber pengiriman email. Informasi "mailadm" pada server SMTP dan "Return-Path" memberikan bukti tentang pengirim asli dan jalur pengembalian pesan. Meskipun elemen seperti "From" dan "To" rentan dipalsukan, "Received" dan "Return-Path" lebih dapat diandalkan dalam analisis forensik untuk memverifikasi keaslian email dan mengidentifikasi indikasi manipulasi .

Analisis header email bertujuan untuk memverifikasi keaslian pesan, melacak rute pengiriman, dan mendeteksi kejanggalan yang mengindikasikan pemalsuan. Tiga aspek utama yang dianalisis adalah autentikasi, rute pengiriman, dan deteksi anomali.

Autentikasi dilakukan menggunakan tiga teknologi utama: SPF, DKIM, dan DMARC. SPF memverifikasi apakah IP pengirim terdaftar dalam catatan domain, sementara DKIM memastikan integritas pesan melalui tanda tangan kriptografi. DMARC menggabungkan hasil SPF dan DKIM untuk menentukan keabsahan email dan memberikan instruksi bila verifikasi gagal.

Analisis rute pengiriman dilakukan dengan membaca jejak server pada bagian "Received" dari bawah ke atas, memberikan gambaran jalur yang dilalui email hingga mencapai penerima. Selain itu, korelasi antara Message-ID dan timestamp dapat mendeteksi pemalsuan, karena setiap server menghasilkan ID unik yang harus sinkron.

Deteksi anomali struktur email juga penting, seperti ketidaksesuaian timestamp atau domain server yang tidak sesuai, yang dapat menunjukkan adanya manipulasi atau upaya untuk menyembunyikan asal-usul email. Kejanggalan seperti ini menjadi indikasi adanya pemalsuan atau

BAB 8
Forensik Grid

A. Pendahuluan

Perkembangan teknologi komputasi terdistribusi mendorong lahirnya berbagai paradigma baru dalam pengelolaan sumber daya komputasi berskala besar, salah satunya adalah Grid Computing. Model ini memungkinkan kolaborasi lintas organisasi dalam pemanfaatan sumber daya komputasi secara bersama-sama melalui jaringan. Di sisi lain, kompleksitas dan keterbukaan lingkungan grid meningkatkan risiko keamanan dan potensi terjadinya insiden digital. Oleh karena itu, pendekatan forensik digital menjadi sangat penting untuk memastikan bahwa setiap aktivitas dalam sistem grid dapat ditelusuri, dianalisis, dan dipertanggungjawabkan secara teknis maupun hukum.

1. Pengantar singkat mengenai Grid Computing

Grid Computing merupakan paradigma komputasi terdistribusi yang memungkinkan integrasi dan pemanfaatan berbagai sumber daya komputasi yang tersebar secara geografis dan dikelola oleh banyak organisasi. Tujuan utama Grid Computing adalah menyediakan daya komputasi, penyimpanan, dan layanan secara kolektif untuk menyelesaikan permasalahan berskala besar yang tidak dapat

ditangani oleh sistem tunggal. Grid sering dianalogikan dengan jaringan listrik, di mana pengguna dapat mengakses sumber daya tanpa harus mengetahui lokasi fisik atau pemiliknya.

Karakteristik utama Grid Computing meliputi heterogenitas sumber daya, kolaborasi lintas institusi, serta pemanfaatan middleware sebagai penghubung antar sistem. Grid banyak digunakan dalam bidang penelitian ilmiah, seperti fisika partikel, bioinformatika, dan simulasi numerik, karena kemampuannya menangani komputasi intensif dan volume data yang besar. Meskipun kini banyak sistem beralih ke komputasi berbasis cloud, Grid Computing tetap relevan dalam konteks komputasi kolaboratif dan riset berskala besar.

2. Pentingnya forensik digital dalam lingkungan grid

Lingkungan Grid Computing memiliki tingkat kompleksitas dan keterbukaan yang tinggi karena melibatkan banyak entitas, sistem, dan kebijakan yang berbeda. Kondisi ini menjadikan grid rentan terhadap berbagai ancaman keamanan, seperti akses tidak sah, penyalahgunaan sumber daya, manipulasi data, dan serangan siber terdistribusi. Selain itu, data dan jejak aktivitas dalam grid sering kali tersebar di berbagai node, yang menyulitkan proses pelacakan ketika terjadi insiden.

Forensik digital berperan penting dalam mengidentifikasi, mengumpulkan, dan menganalisis bukti digital yang berasal dari lingkungan grid. Dengan pendekatan forensik yang tepat, aktivitas mencurigakan dapat ditelusuri secara sistematis dan bukti yang diperoleh dapat dipertanggungjawabkan secara hukum. Tanpa mekanisme forensik yang baik, investigasi insiden pada Grid Computing berisiko tidak akurat atau kehilangan bukti penting, sehingga menghambat penegakan keamanan dan keadilan digital.

3. Tujuan dan ruang lingkup

Bagian ini bertujuan untuk memberikan pemahaman konseptual dan teknis mengenai penerapan forensik digital dalam lingkungan Grid Computing. Fokus utama pembahasan adalah bagaimana karakteristik dan arsitektur grid memengaruhi proses investigasi forensik serta tantangan yang muncul akibat sifat sistem yang terdistribusi dan multi-organisasi. Bagian ini juga bertujuan menjembatani konsep Grid Computing dengan prinsip-prinsip dasar forensik digital.

Ruang lingkup bagian mencakup pengenalan Grid Computing, risiko dan ancaman keamanan yang relevan, serta dasar metodologi forensik digital dalam konteks grid. Pembahasan juga diarahkan untuk mendukung pemahaman bagian-bagian selanjutnya yang akan mengulas aspek teknis, studi kasus, dan isu hukum terkait forensik Grid Computing.

Dengan demikian, bagian ini berfungsi sebagai landasan konseptual bagi pembaca dalam memahami peran forensik digital pada sistem komputasi terdistribusi.

B. Konsep Dasar Grid Computing

Grid Computing adalah paradigma komputasi terdistribusi yang menyatukan sumber daya dari banyak node, sering dari organisasi berbeda, untuk melakukan pemrosesan bersama pada tugas besar. Sistem ini memungkinkan kolaborasi komputasi, penyimpanan, dan layanan secara kolektif tanpa pengguna perlu mengetahui lokasi fisik dari sumber daya. Melalui koordinasi dan middleware, grid menyediakan daya komputasi besar dengan efisiensi penggunaan sumber daya. Pemahaman konsep ini penting sebagai landasan sebelum membahas aspek keamanan dan forensiknya.

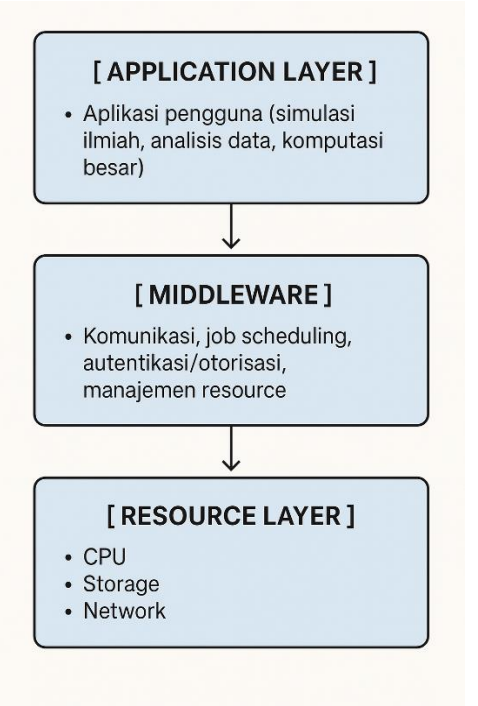
1. Definisi dan karakteristik Grid Computing

Grid Computing didefinisikan sebagai infrastruktur komputasi terdistribusi yang memungkinkan berbagi sumber daya (komputasi, penyimpanan, jaringan) milik banyak institusi untuk menyelesaikan masalah skala besar secara bersama-sama. Karakteristik utama mencakup heterogenitas sistem dan perangkat keras, desentralisasi, distribusi geografis node, serta fleksibilitas dan skalabilitas dalam penggunaan.

Grid mendukung pemanfaatan resource idle dari berbagai organisasi, memungkinkan kolaborasi riset atau komputasi intensif yang tidak mungkin dilakukan oleh satu mesin saja. Menurut literatur, sharing sumber daya dalam grid melibatkan koordinasi kompleks akibat perbedaan platform dan lokasi (Asadzadeh, P., et al, 2004).

2. Arsitektur Grid: Resource Layer, Middleware, Application Layer

Arsitektur Grid seperti terlihat di Gambar 1, lazim dibagi dalam beberapa lapisan. Di lapisan dasar (resource/fabric), terdapat hardware dan sistem fisik seperti CPU, penyimpanan, dan jaringan — sumber daya yang disediakan node grid. Di atasnya, lapisan middleware bertugas sebagai "otak" grid: mengatur komunikasi, penjadwalan tugas (job scheduling), autentikasi/otorisasi, dan manajemen resource antar node yang heterogen. Middleware menyediakan antarmuka seragam sehingga aplikasi dapat berjalan tanpa peduli perbedaan sistem. Lapisan tertinggi, application layer, adalah tempat aplikasi pengguna dijalankan seperti simulasi ilmiah, analisis data, atau tugas komputasi besar yang memanfaatkan resource terkoordinasi di bawahnya. Arsitektur berlapis ini memungkinkan interoperabilitas dan efisiensi di lingkungan grid heterogeny (Prajapati, H. B., & Dabhi, V. K, 2013).



Gambar 8.1 Arsitektur Grid

3. Perbandingan dengan Cloud dan Cluster Computing

Meski Grid, Cloud, dan Cluster sama-sama menyasar komputasi terdistribusi atau terpusat, ketiganya memiliki perbedaan signifikan (Al Etawi, N. A., 2018). Cluster Computing melibatkan sekelompok komputer homogen di lokasi terpusat, bekerja bersama sebagai satu sistem paralel cocok untuk tugas terkoordinasi dengan latensi rendah. Sebaliknya, Grid bersifat heterogen dan terdistribusi geografis, menggabungkan resource dari banyak institusi. Cloud Computing menawarkan sumber daya secara on-

demand melalui penyedia layanan, dengan model layanan seperti IaaS/PaaS/SaaS dan manajemen terpusat, berbeda dari model kolaboratif dan middleware-oriented grid. Cloud fokus pada fleksibilitas, penyederhanaan akses, dan layanan komersial; grid bergantung pada kolaborasi institusional dan berbagi resource

C. Ancaman dan Risiko Keamanan di Grid Computing

Lingkungan Grid sering terasa seperti komunitas ilmiah besar yang saling bergantung: berjejaring, saling meminjam sumber daya, dan bergerak cepat. Dalam suasana kolaboratif itu tumbuh pula celah-celah keamanan jejak yang mudah terpecah, otoritas yang berlapis, serta titik rentan pada komunikasi antar node. Bagian ini membahas ancaman yang sering muncul, titik lemah komunikasi dan autentikasi, serta satu studi kasus singkat untuk memberi gambaran nyata bagaimana insiden dapat terjadi dan ditangani.

Akses tidak sah di grid bisa berasal dari kredensial yang dicuri, delegasi sertifikat tanpa kontrol, atau node yang telah dikompromikan. Modifikasi data (integrity attacks) berbahaya karena data eksperimen atau hasil komputasi yang diubah dapat merusak penelitian. Serangan DoS yang menargetkan layanan middleware atau schedulers dapat menurunkan ketersediaan resource yang dibutuhkan banyak pengguna.

Daftar Pustaka

Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. In Cybersecurity (Vol. 7, Issue 1). Springer Science and Business Media B.V. https://doi.org/10.1186/s42400-023-00200-w

Adinata, I., & Servanda, Y. (2023). Kajian Literatur: Metode Analisis dan Tools Live Forensics Pada Random Access Memory (RAM). Jurnal Sistem Informasi Dan Teknologi, 4(2). https://doi.org/10.47233/jsit.v4i2.1760

Administrator. (2024, July 24). Kampus dalam Bahaya Siber. ACAD CSIRT. https://acad-csirt.org/news/kampus-dalam-bahaya-siber

Agnes Z. Yonatan. (2025, March 23). 330 Kasus Serangan Siber Ancam Indonesia 2024. Https://Goodstats.Id/Article/330-Kasus-Serangan-Siber-Ancam-Indonesia-2024-7dLZZ.

Agustiono, W., Wulan Suci, D., & Prastiti, N. (2024). Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence. Jurnal Teknologi Dan Informasi (JATI), 14. https://doi.org/10.34010/jati.v14i2

Ahmad, R., Abbas, H., & Asghar, M. R. (2023). Zero-day attack detection: A systematic literature review. Artificial Intelligence Review. https://doi.org/10.1007/s10462-023-10437-z

Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, 3(1), 11–18. https://doi.org/10.26555/jiteki.v3i1.5665

Al Etawi, N. A. (2018). A Comparison between Cluster, Grid, and Cloud Computing. International Journal of Computer Applications, 179(32), 37–42

Al-Azhar, M. N. (2012). Digital forensic: Panduan praktis investigasi komputer. Jakarta: Salemba Infotek.

Alharthi, D., & Garcia, I. R. K. (2025). Cloud investigation automation framework (ciaf): An ai-driven approach to cloud forensics. arXiv preprint arXiv:2510.00452.

Almulla, S., Iraqi, Y., & Jones, A. (2016). Digital forensic of a cloud based snapshot. 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 724–729. https://doi.org/10.1109/INTECH.2016.7845140

Alotaibi, F. M., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2022). A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. Computational Intelligence and Neuroscience, 2022. https://doi.org/10.1155/2022/8002963

Alshabibi, A. A., Bu Dookhi, B. A., & Rahman, S. M. M. (2024). Forensic investigation, challenges, and issues of cloud data: A systematic literature review. Computers, 13(8), 213. https://doi.org/10.3390/computers13080213

Altheide, C., & Carvey, H. (2011). Digital forensics with open source tools (2nd ed.). Elsevier.

Alviando, L., Bhawiyuga, A., & Kartikasari, D. P. (2023). Penerapan WebSocket pada sistem live chat berbasis web (studi kasus website Kwikku.com). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK), 7(2). https://doi.org/10.21776/ub.j-ptiik.2023.007.02.12333

Asadzadeh, P., Buyya, R., Ling Kei, C., Nayar, D., & Venugopal, S. (2004). Global Grids and Software Toolkits: A Study of Four Grid Middleware Technologies Barske, D., Stander, A., & Jordaan, J. (2010). A Digital Forensic Readiness Framework for South African SME's. Proceedings of the 2010 Information Security for South

Africa Conference, ISSA 2010. https://doi.org/10.1109/ISSA.2010.5588281

Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavué, C. (2019, June). Blockchain solutions for forensic evidence preservation in IoT environments. In 2019 IEEE conference on network softwarization (NetSoft) (pp. 110-114). IEEE.

Brown, C., & Gommers, J. (2013). From cyber security to cyber resiliency: A review of the standards. Computer Law & Security Review, 29(3), 273–281. https://doi.org/10.1016/j.clsr.2013.03.002

Budianto, I., Nurchim, & Permatasari, H. (2025). Klasifikasi Ancaman Keamanan Siber Menggunakan Algoritma Naive Bayes. International Journal of Artificial Intelligence. https://doi.org/10.20961/ijai.v9i2.104668

Caesarany, T. A. (2022). Pengaruh Integritas, Kompetensi, Kerahasiaan, & Objektivitas Auditor Internal Pemerintah dalam Mendeteksi Kecurangan (Studi Empiris pada Inspektorat Kota Serang Banten).

Cahyanto, T. A., & Prayudi, Y. (2021). Investigasi Forensika Pada Log Web Server untuk Menemukan Bukti Digital. OSF Preprints. https://doi.org/10.31227/osf.io/7xgqz

Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.).

Chen, Y., Liu, X., & Zhang, H. (2021). Handling missing data in digital forensic logs: Challenges and solutions. Journal of Digital Investigation, 34(2), 54-67.

Cheng, H., & Tan, W. (2023). Understanding missing data mechanisms in digital forensic environments. Journal of Cyber Forensics, 15(2), 89-104.

Choi, M., Lee, H., & Jung, S. (2022). Anomaly detection techniques for missing data identification in forensic log analysis. IEEE Access, 10, 12345-12357.

Daniel, L. (2024, July 9). Tech Gadgets Vocabulary in

English. 7ESL. https://7esl.com/technological-gadgets-vocabulary/

Dhumal, M. M., & Rokade, P. M. (2021). An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots. International Journal of Current Engineering and Technology, 8. http://inpressco.com/category/ijcet

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from cloud environments. Digital Investigation, 9(S1), S90–S98.

Enterprise Security Magazine. (2024, Mei 21). Imperative of Digital Forensics in the Modern Era. Enterprise Security Mag Weekly Brief. https://www.enterprisesecuritymag.com/news/imperative-of-digital-forensics-in-the-modern-era-nid-3974-cid-59.html

Faiz, M., Umar, R., & Yudhana, A. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. ILKOM Jurnal Ilmiah, 8(3), 242–247. https://doi.org/10.33096/ilkom.v8i3.79.242-247

Fanani, G. P. I., & Riadi, I. (2020). Analysis of digital evidence on Denial of Service (DoS) attack log based. Buletin Ilmiah Sarjana Teknik Elektro, 2(2), 135–142. https://doi.org/10.12928/biste.v2i2.1065

Farhandika, R., Sabariah, M. K., & Adrian, M. (2024). Penerapan arsitektur REST API pada aplikasi backend manajemen informasi Fakultas Industri Kreatif. Logic: Jurnal Ilmu Komputer Dan Teknologi Informasi, 2(1). https://doi.org/10.25124/logic.v2i1.7530

Faruqi, I. A., Gumilang, S. F. S., & Hasibuan, M. A. (2018). Perancangan back-end aplikasi Rumantara dengan gaya arsitektur REST menggunakan metode iterative incremental. Jurnal Engineering, 5(1). https://doi.org/10.31294/engineering.v5i1.6089

Fawzan, I., & Luthfi, A. (2023). Identifikasi Jenis File pada Artefak Digital Menggunakan Algoritma K-Nearest

Neighbor. JIPI, 10(2). https://doi.org/10.29100/jipi.v10i2.6263

Fernández-Fuentes, X., F. Pena, T., & Cabaleiro, J. C. (2022). Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study. Computers and Security, 115. https://doi.org/10.1016/j.cose.2022.102626

Fernández-Fuentes, X., F. Pena, T., & Cabaleiro, J. C. (2023). Digital forensic analysis of the private mode of browsers on Android. Computers and Security, 134. https://doi.org/10.1016/j.cose.2023.103425

Fernandez, R., Kim, S., & Choi, J. (2023). KNN-based imputation for missing forensic data in FileServer environments. International Journal of Cybersecurity Analytics, 12(1), 112-128.

Friedl, S., & Pernul, G. (2024). IoT Forensics Readiness - influencing factors. In Forensic Science International: Digital Investigation (Vol. 49). Elsevier Ltd. https://doi.org/10.1016/j.fsidi.2024.301768

Garba, A. A., & Musa Bade, A. (2019). A Recommended Digital Forensic Readiness Framework For Nigerian Banks. International Journal of Development Research, 9(8), 28920–28928.

Garcia, M., & Martinez, F. (2022). The effects of missing data on forensic evidence interpretation. Journal of Forensic Sciences, 67(3), 789-798.

Garfinkel, S. (2019). Digital Forensics Research. Springer.

Ginting, A. A., Virgono, A., & Irawan, B. (2015). Perancangan dan implementasi server untuk sistem komputasi awan di intranet kampus. Indonesian Journal of Computer Science, 3(2). https://doi.org/10.31294/ijcs.v3i2.175261

Ginting, R. A., & Siregar, R. A. (2022). Implementasi web server menggunakan Apache dan Nginx untuk layanan web dinamis. Jurnal Teknologi Dan Sistem Komputer, 13(1). https://doi.org/10.31294/w.v13i1.12345

Gomez, A., Lara, C., Kebschull, U., & ALICE Collaboration. (2015, December). Intrusion prevention and detection in grid computing-the ALICE Case. In Journal of Physics: Conference Series (Vol. 664, No. 6, p. 062017). IOP Publishing.

Gomez, L., Torres, P., & Valdez, R. (2023). Adaptive models for missing value imputation in cybersecurity data. IEEE Transactions on Information Forensics and Security, 18(3), 1345-1358.

Grispos, G., Garcia-Galan, J., Pasquale, L., & Nuseibeh, B. (2017, May 9). Are you ready? Towards the engineering of forensic-ready systems [Preprint]. arXiv. https://doi.org/10.48550/arXiv.1705.03250

Hafriadi, F. D., & Ardiansyah, R. (2024). Network's access log classification for detecting SQL injection attacks with the LSTM algorithm. Jurnal Teknik Informatika, 5(4), 2157–2166. https://doi.org/10.52436/1.jutif.2024.5.4.2157

Haidar, M. I. (2024). Pemanfaatan regular expression untuk deteksi pola serangan pada log jaringan. Zenodo. https://doi.org/10.5281/zenodo.10987655

Haikal, A., Putra, S. D., & Nelmiawati. (2023). Analisis terhadap enkripsi data SSL di MySQL: Menguji keamanan in-transit. Rekayasa Teknologi, 2(2), 112–118. https://doi.org/10.25181/rt.v2i2.3446

Handoyo, J., Yudhana, A., & Sunardi. (2025). Analisis Spasial Tingkat Kerawanan Banjir di Kecamatan Cepu Kabupaten Blora dengan Pendekatan Metode Skoring Berbasis Sistem Informasi Geografis. Jurnal Sainteks, 22(1). https://doi.org/10.30595/sainteks.v22i1.25180

Hassan, A., & El-Sayed, M. (2024). Challenges of incomplete digital evidence in cybercrime investigation. Computers & Security, 137, Article 103704.

Huang, J., Wang, L., & Zhao, M. (2024). Application of adaptive missing data imputation in corporate FileServer

forensic analysis. Computers & Security, 117, Article 102870.
Hunt, R., & Zeadally, S. (2012). Network Forensics: An Analysis of Techniques, Tools, and Trends. Computer, 45(12), 36–43. https://doi.org/10.1109/MC.2012.252
Ihsan, I., Lesmideyarti, D., Hidayati, Q., & Nugroho, T. R. (2023). Perancangan infrastruktur dan implementasi web server untuk website sekolah sebagai media informasi dan komunikasi. Jurnal Teknologi Terapan, 8(1). https://doi.org/10.35313/jtt.v8i1.1598
Imam Riadi, Abdul Fadlil, & Muhammad Immawan Aulia. (2020). Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST). Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(5), 820–828. https://doi.org/10.29207/resti.v4i5.2224
Imam Riadi, Rusydi Umar, & Syahib, M. I. (2021). Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST). Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 5(1), 45–54. https://doi.org/10.29207/resti.v5i1.2626
Iman, N., Susanto, A., & Inggi, R. (2023). Analisa perkembangan forensik digital dalam penyelidikan cybercrime di Indonesia. Incomtech: Jurnal Telekomunikasi Dan Komputer, 9(3). https://doi.org/10.22441/incomtech.v9i3.7210
Impact My Biz. (2024). Digital Forensics and Incident Response in Cybersecurity. https://www.impactmybiz.com/blog/digital-forensics-incident-response-cybersecurity
Iqbal, F., Khalid, Z., Marrington, A., Shah, B., & Hung, P. C. K. (2022). Forensic investigation of Google Meet for memory and browser artifacts. Forensic Science International: Digital Investigation, 43, 301448. https://doi.org/10.1016/j.fsidi.2022.301448

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association.

Iskandar, M. I. (2024). Credential stuffing: Ancaman siber dan cara efektif menghindarinya. Zenodo. https://doi.org/10.5281/zenodo.10987656

ISO/IEC. (2012). ISO/IEC 27037:2012 – Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence. International Organization for Standardization.

ISO/IEC. (2013). ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information Security Management Systems – Requirements. International Organization for Standardization.

ISO/IEC. (2013). ISO/IEC 27002:2013 – Code of Practice for Information Security Controls. International Organization for Standardization.

Kebande, V. R., & Venter, H. S. (2019). CFRaaS: Architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent. African Journal of Science, Technology, Innovation and Development, 11(6), 749–769. https://doi.org/10.1080/20421338.2019.1585675

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology.

Kessler, G. C. (2007). An overview of digital forensic technology and methodology. Journal of Information System Security, 3(2), 43-64.

Kim, J., & Park, Y. (2024). Adaptive learning approaches for missing data detection in digital forensic investigations. Journal of Information Security and Applications, 69, Article 103359.

Kumar, R. (2024). Basic Apache Web Server Log Analysis Using Command Line Tools. Zenodo. https://doi.org/10.5281/zenodo.10012345

Kumar, S., Rao, N., & Das, A. (2024). Analysis of manipulated log data in digital forensics: Techniques and challenges. Forensic Science International: Digital Investigation, 45, Article 301412.

Kusuma, G. H. A. (2020). Implementasi Volatility dalam Menganalisis Malware pada Memory Dump. Jurnal Ilmiah Teknik Komputer, 7(2). https://doi.org/10.31294/jiac.v7i2.5491

Lee, J., Park, H., & Kim, D. (2021). Patterns and causes of missing data in server log files. International Journal of Information Security, 28(1), 56-70.

Lee, S., & Park, J. (2023). Challenges in forensic analysis of FileServers: Data integrity and missing data issues. Forensic Science International: Digital Investigation, 40, Article 301294.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. arXiv preprint arXiv:1604.03850.

Little, R.J.A., & Rubin, D.B. (2019). Statistical analysis with missing data (3rd ed.). Wiley.

Liu, Y., & Zhao, Q. (2023). Systematic study on logging failures and data loss in server environments. Computers & Security, 120, Article 102964.

Lone, A. H., & Mir, R. N. (2018). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J, 1, 21-27.

Mandia, K., Prosise, C., & Pepe, M. (2003). Incident Response and Computer Forensics (2nd ed.). McGraw-Hill.

Mandia, K., Prosise, C., & Pepe, M. (2020). Incident Response & Computer Forensics. McGraw-Hill.

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital investigation, 9(2), 71-80.
Martini, B., & Choo, K. K. R. (2014). Cloud forensic technical challenges and solutions: A snapshot. IEEE Cloud Computing, 1(4), 20-25.
Mishra, N., Yadav, R., & Maheshwari, S. (2014). Security issues in grid computing. International Journal on Computational Sciences & Applications (IJCSA) Vol, 4.
Mislan, R. P., Casey, E., & Kirschenbaum, M. G. (2010). Digital evidence in digital investigations. In IFIP Advances in Information and Communication Technology (Vol. 337, pp. 3-13). Springer.
MM0X. (2024). How to detect LFI and RFI attacks. Zenodo. https://doi.org/10.5281/zenodo.10987654
Mohanta Abhijit and Saldanha, A. (2020). Memory Forensics with Volatility. In Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware (pp. 433–476). Apress. https://doi.org/10.1007/978-1-4842-6193-4_14
Morgan, L. (2023, September 17). How To Rename A File Extension On Mobile, Windows or Mac. Lemmy Morgan. https://www.lemmymorgan.com/rename-a-file-extension/
Moussa, A. N., Ithnin, N., & Zainal, A. (2018). CFaaS: bilaterally agreed evidence collection. Journal of Cloud Computing, 7(1), 1. https://doi.org/10.1186/s13677-017-0102-3
Muflih, G. Z., Sunardi, S., Riadi, I., Yudhana, A., & Azmi, H. I. (2023). Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS). JIKO (Jurnal Informatika Dan Komputer), 6(1).
Mustafa, C. (2024). Integritas chain of custody pada pemeriksaan bukti digital. Zenodo. https://doi.org/10.5281/zenodo.10987702
National Institute of Standards and Technology (NIST).

(2006). Guide to Integrating Forensic Techniques into Incident Response (SP 800-86). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-86/final

National Institute of Standards and Technology (NIST). (2012). Computer Security Incident Handling Guide (SP 800-61 Revision 2). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Nawwar, A. (2024). Analisis forensik digital pada bukti digital kejahatan siber menggunakan Digital Forensic Research Workshop model. Jurnal Sistem Keamanan, 15(2). https://doi.org/10.31294/jsk.v15i2.123456

Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to Computer Forensics and Investigations (5th ed. dan edisi berikutnya). Cengage Learning.

Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to Computer Forensics and Investigations. Cengage Learning.

Nguyen, T., & Tran, D. (2023). Systematic approaches for missing data identification in enterprise forensic investigations. Digital Investigation, 39, Article 301320.

Ninos, F., Karalas, K., Dechouniotis, D., & Polemis, M. (2025). On Microservice-Based Architecture for Digital Forensics Applications: A Competition Policy Perspective. In Future Internet (Vol. 17, Issue 4). https://doi.org/10.3390/fi17040137

Ogunbukola, M. (2024). The Critical Role of Digital Forensics in the Modern Information Era. Matgrace Consulting. https://www.researchgate.net/publication/381143019_The_Critical_Role_of_Digital_Forensics_in_the_Modern_Information_Era mdpi.com+8researchgate.net+8arxiv.org+8impactmybiz.com

Pal, M. (2016). Handling missing data in digital forensics investigations. International Journal of Computer Science and Engineering, 8(5), 211-216.

Paraschos Maniatis. (2023). Comparison of Public, Private, Hybrid, and Community Cloud Computing in Terms of Purchasing and Supply Management: A Quantitative Approach. International Journal Of Multidisciplinary Research And Analysis, 6(6). https://doi.org/10.47191/ijmra/v6-i6-04

Park, S., Kim, Y., Park, G., Na, O., & Chang, H. (2018). Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment. Sustainability, 10(4). https://doi.org/10.3390/su10041203

Patel, A., & Shah, K. (2022). Impact of missing forensic data on cybersecurity incident response. Journal of Forensic Sciences, 67(5), 981-992.

Patel, R., & Singh, T. (2022). Impact of workload on missing data occurrence in enterprise server logs. IEEE Transactions on Network and Service Management, 19(4), 2318-2329.

Prajapati, H. B., & Dabhi, V. K. (2013). Classification and Characterization of Core Grid Protocols for Global Grid Computing.

Pranoto, W., Riadi, I., & Prayudi, Y. (2021). Live Forensics Method for Acquisition on the Solid State Drive (SSD) NVMe TRIM Function. Kinetik, 5(2), 129–138. https://doi.org/10.22219/kinetik.v5i2.1032

Pribadi, B., Rosdiana, S., & Arifin, S. (2023). Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases. Procedia Computer Science, 216(2022), 161–167. https://doi.org/10.1016/j.procs.2022.12.123

Putra, R. A., & Prasetyo, A. (2023). Evaluasi Web Server LiteSpeed sebagai Alternatif Apache untuk Website

dengan Traffic Tinggi. Indonesian Journal of Computer Science, 9(1). https://doi.org/10.31294/ijcs.v9i1.14567

Putri, F. E., & An Nibras, F. Z. (2020). Analysis of website vulnerability to defacement attacks. Jurnal Sistem Dan Teknologi Informasi, 2(1), 30–38. https://doi.org/10.33197/justinfo.v2i1.1806

Qbeitah, M. A., & Aldwairi, M. (2018). Dynamic malware analysis of phishing emails.

Rachman, H., Sugiantoro, B., & Prayudi, Y. (2021). Forensic storage framework development using composite logic method. ILKOM Jurnal Ilmiah, 13(1), 58–66.

Rachmie, S. (2020). Peranan ilmu forensik digital terhadap penyidikan kasus peretasan website. Jurnal Litigasi, 21(1). https://doi.org/10.23969/litigasi.v21i1.2388

Ramadhan, R. A., Setiawan, P. R., & 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.

Ramos Brandao, P. (2019). Forensics and Digital Criminal Investigation Challenges in Cloud Computing and Virtualization. American Journal of Networks and Communications, 8(1), 23. https://doi.org/10.11648/j.ajnc.20190801.13

Riadi, I. (2021). Network forensic on distributed denial of service attacks using National Institute of Standards and Technology method. International Journal of Computer Applications, 183(40), 1-9.

Riadi, I. (2022). Live forensics method for acquisition on the Solid State Drive (SSD). Kinetik: Game Technology, Information System, Computer Network, Electronics, and Control, 7(2), 196-205.

Riadi, I., & Prayudi, Y. (2021). Perbandingan Tools Forensik Digital Open Source dan Komersial dalam Investigasi Keamanan Siber. Kinetik, 5(2), 121–128. https://doi.org/10.22219/kinetik.v5i2.1032

Riadi, I., Siregar, N. H., & others. (2022). Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework. Ingenierie Des Systemes d'Information, 27(6), 903.

Riadi, I., Sunardi, S., & Fitri, F. T. (2022). Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method. INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi, 6(1), 108–117. https://doi.org/10.29407/intensif.v6i1.16830

Riadi, I., Umar, R., & Bernadisman, D. (2021). Analisis Forensik Database Menggunakan Metode Forensik Statis. Jurnal Teknologi Dan Sistem Komputer, 9(1), 9–17. https://doi.org/10.21456/vol9iss1pp9-17

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute of Justice (NIJ). Elinvo (Electronics, Informatics, and Vocational Education), 3(1), 70–82.

Riadi, Imam, Muthohirin, F. B. (2022). Forensik Digital (Forensik Email). 1–23.

Rochmadi, T. (2019). Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar. Indonesian Journal of Business Intelligence (IJUBI), 1(1), 32. https://doi.org/10.21927/ijubi.v1i1.878

Rochmadi, T., Fadlil, A., & Riadi, I. (2024). Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital. CyberSecurity Dan Forensik Digital, 7(2), 81–89. https://doi.org/10.14421/csecurity.2024.7.2.4861

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(1), 37-49.

Rozi, N. R. F. (2022). Analisis Network Incident Packet Capture (PCAP) Menggunakan Wireshark. Jurnal ICT, 5(2). https://doi.org/10.52661/j_ict.v5i2.239

Ruan, K. (2013). Cybercrime and Cloud Forensics: Applications for Investigation Processes. IGI Global.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011, January). Cloud forensics. In IFIP International Conference on Digital Forensics (pp. 35-46). Berlin, Heidelberg: Springer Berlin Heidelberg.

Rusydi Umar et al. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation. Universitas Ahmad Dahlan. Diakses dari

Rusydi, R., Yuhandri, & Arlis, S. (2024). Penerapan Acunetix Vulnerability Scanner dari Serangan Siber pada Keamanan Website Kampus. KOMTEKINFO: Jurnal Komputer, Teknik, Dan Informatika. https://doi.org/10.35134/komtekinfo.v11i3.569

Saleh, M. A., Hajar Othman, S., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021). Common Investigation Process Model for Internet of Things Forensics. 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 84–89. https://doi.org/10.1109/ICSCEE50312.2021.9498045

Santra Palash and Roy, A. and M. S. and M. K. and P. S. (2018). Log-Based Cloud Forensic Techniques: A Comparative Study. In K. K. and T. S. and T. M. C. Perez Gregorio Martinez and Mishra (Ed.), Networking Communication and Data Knowledge Engineering (pp. 49–59). Springer Singapore.

Sethi, A., Ahlawat, R., & Jain, M. (2023). Web server security solution for detecting cross-site scripting attacks in real-time using deep learning BT - 2023 IEEE Conference on Artificial Intelligence Applications. https://doi.org/10.1109/ICAIA57370.2023.10169255

Setiawan, R., Kartikasari, D. P., & Rahayudi, B. (2021). Implementasi arsitektur web server cluster menggunakan

single board computer untuk menunjang kebutuhan high availability system. Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK), 8(4), 1234–1241. https://doi.org/10.25126/jtiik.202184512

Singh, R., & Kumar, A. (2022). FileServer role and forensic implications in modern IT infrastructure. International Journal of Information Security, 21(4), 567-579.

Singh, R., Kumar, A., & Gupta, P. (2023). Hybrid methods for identifying missing values in cybersecurity forensic data. Journal of Cybersecurity Research, 8(1), 45-58.

Singh, T. (2023). Computational complexity in adaptive forensic models: A survey. Journal of Artificial Intelligence Research, 75(1), 189-210.

Siregar, A. R., & Siregar, R. A. (2022). Analisis Perbandingan Kinerja Web Server Apache dan Nginx dalam Menangani Permintaan HTTP. Jurnal Teknologi Dan Sistem Komputer, 13(2). https://doi.org/10.31294/w.v13i2.12346

Solanke, V. S., & Kulkarni, G. A. (2014). Private Vs Public Cloud Maske Vishnu Government Polytechnic Mumbai. International Journal of Computer Science & Communication Networks, 3(2). https://www.researchgate.net/publication/258253155

Stallings, W. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.

Sudyana, D., Hadi, I., & Yudha, F. (2023). Analisis Investigasi Forensik Digital pada Layanan Private Cloud Computing Menggunakan SNI 27037:2014. Buletin Profesi Insinyur, 6(1), 14–19. https://doi.org/10.20527/bpi.v6i1.176

Sushil, G. S., Deshmuk, R. K., & Junnarkar, A. A. (2022). Security Challenges and Cyber Forensics For IoT Driven BYOD Systems. 2022 IEEE 7th International Conference for Convergence in Technology (I2CT), 1–7. https://doi.org/10.1109/I2CT54291.2022.9824368

Sutiono, M. T. I. (2023). Analisa Jaringan Menggunakan Wireshark dan Tcpdump untuk Deteksi Serangan. OSF Preprints. https://doi.org/10.31227/osf.io/9kz7p

Syukri, M., Riadi, I., & Sutikno, T. (2025). Jurnal Processor Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan Metode National Institute of Standards and Technology. xx(xx), 1–11.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2014). Digital Forensics: Principles, Techniques, and Tools. CRC Press.

Team., V. (2024). Digital forensics image for Windows analysis. Zenodo. https://doi.org/10.5281/zenodo.10987701

Umar, R., Riadi, I., & Surya Kusuma, R. (2021). Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control. https://doi.org/10.22219/kinetik.v6i2.1225

Virgiawan, Z. R., & Harwikarya. (2023). Perancangan arsitektur backend microservice pada startup Campaign.com. Al-Qalasadi: Jurnal Ilmiah Matematika Dan Komputer, 16(1). https://doi.org/10.35931/aq.v16i1.862

Wang, L., Chen, F., & Xu, Y. (2022). Impact of data incompleteness on machine learning-based forensic analysis. Digital Investigation, 39, Article 301273.

Wang, L., Chen, F., & Xu, Y. (2022). Sources of incompleteness in digital forensic data: A comprehensive review. Digital Investigation, 39, Article 301273.

Wibowo, I. A., Kom, M., & Si, M. (n.d.). Forensik digital.

Widianingrum, A. R. (2022). Analisis implementasi kebijakan hukum terhadap penanganan kejahatan siber di era digital. Jurnal Ilmiah Siber, 2(2), 45–56. https://doi.org/10.62263/jis.v2i2.40

Widiyasono, N. (2024a). Artificial intelligence untuk forensika digital: Peluang dan tantangan. Zenodo. https://doi.org/10.5281/zenodo.10987703

Widiyasono, N. (2024b). Pengantar ilmu forensika digital. Jurnal Forensik Digital Indonesia, 1(1). https://doi.org/10.31294/forensikdigital.v1i1.98765

Wintolo, H., Retnowati, N. D., & Ibrahim, A. A. I. (2020). Layanan Cloud Computing untuk Mendukung Kinerja Administrasi Database Tanpa Menggunakan Perintah SQL. Jurnal ELTIKOM, 4(2), 87–95. https://doi.org/10.31961/eltikom.v4i2.174

Yuliana, R., & Nugroho, T. R. (2024). Implementasi Web Server Caddy dengan Otomatisasi HTTPS untuk Aplikasi Web Modern. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK), 8(1). https://doi.org/10.21776/ub.j-ptiik.2024.008.01.14555

Zawoad, S., & Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. http://arxiv.org/abs/1302.6312

Zawoad, S., Dutta, A. K., & Hasan, R. (2013). SecLaaS: Secure Logging-as-a-Service for Cloud Forensics. Cryptography and Security. http://arxiv.org/abs/1302.6267

Zhang, Q., Li, Y., & Chen, F. (2024). Missing data handling techniques in digital forensic investigations: A review and future directions. Digital Investigation, 42, Article 301347.

Zhang, Y., Li, X., & Zhao, J. (2023). Consequences of missing data in digital forensic analytics. IEEE Transactions on Information Forensics and Security, 18(1), 112-123.

Zhu, X., & Wang, J. (2024). Enhancing cybersecurity decision-making with adaptive missing data models. Journal of Cybersecurity Research, 9(2), 99-112.