Vol. 07, No. 1 2025, pp. 3744 – 3756

Sultra Law Review

Vol. 07, No. 01 April 2025
ISSN: 2685-208X (Online)
Publisher: Fakultas Hukum Universitas Sulawesi Tenggara
Website: https://jurnal-unsultra.ac.id/index.php/sulrev

FUNGSI DIGITAL FORENSIK DALAM PEMBUKTIAN TINDAK PIDANA SIBER (Studi Kasus di Polda Sultra)

Riston, Basoddin, La Ode Muhram

Fakultas Hukum Universitas Sulawesi Tenggara

ARTICLE INFO

Keywords:
Cybercrime, Digital Forensics, Evidence, Information Technology. Southeast Sulawesi Regional Police.

e-mail:
riston78@gmail.com

Corresponding Author:
Riston

Received:18/09/2024
Accepted:21/12/2024
Published:30/04/2025

ABSTRACT

The development of information and communication technology has had a significant impact on various aspects of life, but has also created challenges in the form of increasing cybercrime. Digital forensics is a key element in cybercrime investigations, with the aim of identifying, collecting, analyzing, and validating digital evidence. This study aims to analyze the role of digital forensics in proving cybercrime in the Southeast Sulawesi Regional Police area, identify the obstacles faced, and formulate strategies to improve the effectiveness of investigations. This study uses a juridical-empirical method, which combines a normative approach to related laws and regulations with empirical studies through data collection in the field, including interviews with Southeast Sulawesi Regional Police personnel. The results of the study indicate that the function of digital forensics is very important in presenting legally valid evidence, although there are still obstacles such as limited human resources, technological infrastructure, and lengthy legal procedures. The case study in Kendari shows real challenges in dealing with online fraud and hacking of social media accounts, which requires in-depth analysis of digital evidence. This study recommends improving the competence of officers, procuring modern forensic devices, and educating the public as strategic steps. By optimizing digital forensics, it is hoped that law enforcement efforts against cyber crimes can be more effective and provide a sense of security for the community.

I. PENDAHULUAN

Dalam era digital, teknologi informasi dan komunikasi berkembang pesat, memberikan kemudahan dalam berbagai aspek kehidupan manusia, mulai dari aktivitas ekonomi, sosial, hingga pemerintahan. Namun, di balik kemajuan tersebut, muncul tantangan besar berupa meningkatnya kejahatan siber *(cybercrime).*

Kejahatan ini melibatkan penggunaan teknologi untuk melakukan tindakan melanggar hukum, seperti penipuan online, pencurian identitas, peretasan, dan penyebaran konten ilegal. Di Indonesia, khususnya di Sulawesi Tenggara, kejahatan siber menjadi salah satu ancaman nyata yang mengganggu stabilitas sosial dan keamanan masyarakat.

Dalam idealitas , sistem peradilan pidana di Indonesia, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016, memberikan landasan hukum untuk menangani tindak pidana siber secara efektif. Aparat penegak hukum diharapkan memiliki kompetensi dan infrastruktur memadai untuk menggunakan bukti digital secara sah dan dapat diterima di pengadilan. Namun, pada kenyataannya, implementasi digital forensik dalam penyidikan tindak pidana siber di berbagai wilayah, termasuk Sulawesi Tenggara, masih menghadapi banyak kendala. Keterbatasan sumber daya manusia yang memiliki keahlian di bidang digital forensik menjadi salah satu hambatan utama.

Selain itu, infrastruktur yang kurang memadai, seperti perangkat lunak dan keras untuk menganalisis bukti digital, membuat proses penyidikan sering kali terhambat. Hal ini berimplikasi pada lambatnya pengungkapan kasus dan memberikan ruang bagi pelaku untuk terus menjalankan aksi mereka. Fenomena kejahatan siber di Kota Kendari sebagai ibu kota Provinsi Sulawesi Tenggara mencerminkan realitas tersebut. Kasus penipuan online, peretasan akun media sosial, dan penyebaran konten ilegal sering kali menjadi perhatian publik. Misalnya, kasus penipuan melalui platform e-commerce pada tahun 2023, di mana pelaku berhasil mencuri uang sejumlah besar dengan memanfaatkan identitas palsu. Selain itu, kasus peretasan akun media sosial tokoh masyarakat di Kendari juga menjadi bukti nyata betapa kejahatan ini dapat merugikan individu maupun institusi.

Dalam konvensi internasional seperti Konvensi Budapest, yang menjadi acuan penanganan kejahatan siber secara global, penekanan diberikan pada pentingnya metode forensik yang akurat dan sesuai dengan standar hukum. Walaupun Indonesia belum meratifikasi konvensi ini, prinsip-prinsip yang ada di dalamnya tetap relevan untuk diadopsi dalam konteks nasional.

Melihat kondisi ini, optimalisasi fungsi digital forensik dalam penyidikan tindak pidana siber di wilayah Polda Sultra menjadi kebutuhan mendesak. Penelitian ini bertujuan untuk menganalisis peran digital forensik, hambatan yang dihadapi, dan langkah strategis yang dapat diambil untuk meningkatkan efektivitas penyidikan kejahatan siber di Sulawesi Tenggara. Melalui penelitian ini, diharapkan dapat ditemukan solusi konkret untuk meningkatkan fungsi digital forensik di Polda Sultra, baik melalui peningkatan kapasitas personel, pengadaan perangkat forensik yang memadai, maupun penyusunan kebijakan yang mendukung.

II. TINJAUAN PUSTAKA

A. Digital Forensik

Digital forensik adalah cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, analisis, dan penyajian bukti digital. Bukti digital ini dapat ditemukan di perangkat elektronik seperti komputer, ponsel, atau laptop. Tujuan utama digital forensik adalah untuk mengumpulkan bukti yang sah secara hukum untuk digunakan dalam: Investigasi kriminal, Penyelesaian sengketa hukum, Penyelidikan internal di organisasi, Pemulihan data yang hilang atau dihapus. Digital forensik mencakup berbagai bidang, seperti komputer, perangkat mobile, jaringan, dan media penyimpanan. Bukti-bukti yang dikumpulkan dalam digital forensik dapat berupa email, pesan teks, file dokumen, metadata, dan aktivitas online lainnya.

Tujuan penggunaan forensik digital yang paling umum adalah mendukung atau menyangkal hipotesis di pengadilan pidana atau perdata. Kemudian secara khusus, berikut ini adalah tujuan dalam penggunaan serta penerapan digital forensic yang harus diketahui:

1. Kasus pidana, yaitu melibatkan dugaan pelanggaran hukum dan lembaga penegak hukum dan pemeriksa forensik digital mereka.

2. Kasus perdata, yaitu melibatkan perlindungan hak dan properti individu atau perselisihan kontrak antara entitas komersial yang mungkin melibatkan bentuk forensik digital yang disebut penemuan elektronik *(e-discovery).*

Analisis forensik digital juga dapat menjadi bagian dari proses merespons insiden untuk membantu *recovery* (memulihkan) atau mengidentifikasi data sensitif atau informasi identitas pribadi atau *Personal Information Identity* (PII) apa pun yang hilang atau dicuri dalam kejahatan dunia maya.
Adapun tahapan dalam melakukan forensik digital ada empat, penjelasan selengkapnya dapat disimak melalui ulasan di bawah ini:
1. Tahap 1: Assessment
2. Tahap 2: *Acquisition*
3. Tahap 3: *Examination*
4. Tahap 4 : *Documenting dan Reporting*

Pemeriksaan media digital dicakup dalam undang-undang nasional maupun internasional. Khusus penyelidikan perdata, undang-undang dapat membatasi kemampuan analis untuk melakukan pemeriksaan. Pembatasan pemantauan jaringan, atau pembacaan komunikasi pribadi sering terjadi. Dalam penyelidikan pidana, undang-undang nasional membatasi seberapa banyak informasi yang dapat disita.[39] Misalnya, di Inggris, penyitaan barang bukti oleh penegak hukum diatur oleh Police and Criminal Evidence Act 1984. Selama keberadaan awalnya di bidang ini, *"International Organization on Computer Evidence"* (IOCE) adalah salah satu lembaga yang bekerja untuk menetapkan standar internasional yang kompatibel terhadap penyitaan barang bukti.

Di Inggris, hukum yang sama terkait kejahatan komputer juga dapat mempengaruhi penyelidik forensik. *Computer Misuse Act 1990* mengatur larangan akses tanpa otorisasi pada materi komputer, aturan ini menjadi perhatian khusus bagi penyidik sipil yang memiliki lebih banyak batasan dibanding penegak hukum. Hak individu atas privasi adalah salah satu bidang forensik digital yang sebagian besar belum diputuskan oleh pengadilan. *Electronic Communications Privacy Act (ECPA)* di AS memberikan batasan kemampuan kepada penegak hukum atau penyidik sipil untuk menyadap dan mengakses bukti. Undang-undang tersebut membedakan antara komunikasi tersimpan (misalnya arsip surat elektronik) dan komunikasi yang ditransmisikan (seperti VoIP).

Yang terakhir, lebih dianggap sebagai serangan privasi, dan lebih sulit untuk mendapatkan surat perintah. ECPA juga mempengaruhi kemampuan perusahaan dalam menyelidiki komputer dan komunikasi karyawan mereka, suatu aspek yang masih diperdebatkan adalah sejauh mana perusahaan dapat melakukan pemantauan tersebut. Pasal 5 Konvensi Eropa tentang Hak Asasi Manusia menegaskan pembatasan privasi yang serupa dengan ECPA dan membatasi pemrosesan dan pembagian data pribadi baik di dalam UE maupun dengan negara-negara luar. Kemampuan penegak hukum Inggris untuk melakukan penyelidikan forensik digital diatur oleh *Regulation of Investigatory Powers Act 2000*.

B. Pembuktian

1. Pengertian dan Tujuan Pembuktian

Pembuktian dalam hukum pidana merupakan proses yang krusial dalam sistem peradilan pidana. Ia merupakan serangkaian tindakan yang dilakukan untuk mencari dan menemukan kebenaran materiil, yaitu kebenaran yang sesungguhnya mengenai terjadinya suatu tindak pidana, siapa pelakunya, dan bagaimana tindak pidana tersebut dilakukan. Tujuan utama pembuktian adalah untuk:
a. Meyakinkan Hakim: Pembuktian bertujuan untuk meyakinkan hakim bahwa suatu tindak pidana telah terjadi dan terdakwa adalah pelakunya. Keyakinan hakim ini akan menjadi dasar putusan yang akan dijatuhkan.

b. Menegakkan Keadilan: Proses pembuktian yang adil dan transparan merupakan fondasi dari penegakan hukum yang adil dan berkeadilan.
c. Melindungi Hak Asasi Manusia: Pembuktian yang cermat dan sesuai prosedur akan melindungi hak asasi manusia, terutama hak terdakwa untuk dianggap tidak bersalah sebelum dibuktikan kesalahannya secara sah.

Asas-asas pembuktian merupakan landasan filosofis dan yuridis yang mendasari proses pembuktian. Beberapa asas penting, antara lain:
a. Praduga Tak Bersalah (Presumption of Innocence):
b. Bebas (Vrij Bewijs):
c. Audi et Alteram Partem (Mendengar Kedua Belah Pihak):
d. Persidangan Terbuka untuk Umum:

Alat Bukti dalam KUHAP (Pasal 184), KUHAP mengatur lima alat bukti yang sah, yaitu:
1. Keterangan Saksi: Keterangan yang diberikan oleh orang yang melihat, mendengar, atau mengalami sendiri suatu peristiwa pidana. Keterangan saksi di bawah sumpah memiliki nilai pembuktian yang kuat.
2. Keterangan Ahli: Keterangan yang diberikan oleh seseorang yang memiliki keahlian khusus di bidang tertentu, yang diperlukan untuk menjelaskan suatu fakta atau persoalan dalam perkara pidana. Misalnya, ahli forensik, ahli psikologi, atau ahli hukum.
3. Surat: Dokumen atau tulisan yang berisi informasi yang berkaitan dengan perkara pidana. Contohnya, surat visum et repertum, surat keterangan bank, atau dokumen kontrak.
4. Petunjuk: Perbuatan, kejadian, atau keadaan yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi[4] suatu tindak pidana dan siapa pelakunya.[5] Petunjuk merupakan alat bukti tidak langsung yang ditarik kesimpulannya dari alat bukti lain.
5. Keterangan Terdakwa: Keterangan yang diberikan oleh terdakwa di persidangan mengenai perbuatan yang didakwakan kepadanya. Keterangan terdakwa bukan merupakan alat bukti yang berdiri sendiri, tetapi dinilai bersama-sama dengan alat bukti lainnya.

Proses pembuktian di persidangan merupakan serangkaian tahapan yang sistematis, antara lain:
1. Pengajuan Alat Bukti: Penuntut umum mengajukan alat bukti yang mendukung dakwaannya, sedangkan penasihat hukum mengajukan alat bukti yang meringankan atau membantah dakwaan.
2. Pemeriksaan Alat Bukti: Hakim memeriksa keabsahan dan relevansi alat bukti yang diajukan.
3. Pemeriksaan Saksi: Saksi-saksi dihadirkan di persidangan dan diperiksa di bawah sumpah.
4. Pemeriksaan Ahli: Ahli dapat dihadirkan untuk memberikan keterangan yang relevan dengan keahliannya.
5. Pembacaan Surat: Surat-surat yang relevan dibacakan di persidangan.
6. Penunjukan Barang Bukti: Barang bukti yang berkaitan dengan perkara dapat diperlihatkan dan diperiksa di persidangan.
7. Pemeriksaan Terdakwa: Terdakwa diberi kesempatan untuk memberikan keterangan di persidangan.
8. Tuntutan dan Pembelaan: Setelah proses pemeriksaan selesai, penuntut umum mengajukan tuntutan pidana, sedangkan penasihat hukum mengajukan pembelaan.
9. Putusan Hakim: Hakim menjatuhkan putusan berdasarkan keyakinannya yang didasari pada alat bukti yang sah yang terungkap di persidangan.

2. Bukti Digital

Bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Dengan demikian segala sesuatu yang membawa informasi

digital dapat menjadi subjek penyelidikan, dan setiap pembawa informasi yang ditargetkan untuk pemeriksaan harus diperlakukan sebagai bukti.

Seorang pakar digital forensik harus benar-benar terlatih dan berpengalaman dalam menggunakan cara untuk mengumpulkan semua data-data yang diperlukan sehingga bisa dijadikan bukti legal yang semuanya sudah diatur dalam undang-undang. Ketika digunakan dalam pengadilan, bukti digital berada di bawah pedoman hukum yang sama seperti bentuk bukti lainnya; pengadilan biasanya tidak memerlukan panduan yang lebih ketat.

Di Amerika Serikat, *Federal Rules of Evidence* digunakan un tuk mengevaluasi diterimanya bukti digital, PACE Kerajaan Inggris dan *Civil Evidence acts* memiliki pedoman serupa dan banyak negara lain memiliki hukumnya sendiri. Undang-undang federal AS membatasi penyitaan hanya pada barang bukti yang jelas. Hal ini diakui tidak selalu memungkinkan dilakukan pada media digital sebelum dilakukan pemeriksaan.

Hukum yang berurusan dengan bukti digital terkait dengan dua permasalahan: integritas dan keaslian. Integritas memastikan bahwa tindakan menyita dan memperoleh media digital tidak mengubah bukti (baik yang asli atau salinannya). Keaslian mengacu pada kemampuan untuk mengkonfirmasi integritas informasi; misalnya bahwa media yang dicitrakan (imaged) sesuai dengan bukti asli.[39] Mudahnya media digital untuk termodifikasi berarti mendokumentasikan lacak balak [en] mulai dari TKP, analisis, hingga ke pengadilan penting dilakukan untuk menjaga keaslian barang bukti.

Lembaga penegak hukum harus memiliki lacak balak yang tepat ketika menangani bukti digital dan menjamin bahwa semua bukti digunakan untuk analisis forensik yang tepat. Agensi juga harus mengambil tindakan pencegahan yang tepat saat menangani bukti digital. Ketika para penyelidik mengumpulkan bukti dari perangkat digital, bukti yang terkait dengan kejahatan lain mungkin ditemukan. Penyelidik perlu mendapatkan surat perintah kedua agar bukti dapat diterima ke pengadilan. Penanganan bukti digital perlu dilakukan secara khusus mengingat barang bukti digital tergolong "rapuh" sehingga besar kemungkinan terjadinya pencemaran barang bukti digital baik disengaja maupun tidak disengaja.

Kesalahan kecil pada penanganan barang bukti dapat membuat barang bukti digital tidak dapat diajukan dipengadilan sebagai alat bukti yang sah dan akurat. Data digital juga dapat diciptakan dengan mudah. Salah satu hal yang ditakutkan adalah adanya penambahan data oleh penyidik (misalnya ada penambahan data untuk menyudutkan pemilik perangkat digital). Untuk itu, diperlukan adanya mekanisme yang memastikan bahwa penyidik tidak dapat (atau sulit) untuk melakukan rekayasa terhadap data.

Ada beberapa mekanisme yang dapat dilakukan, seperti penggunaan *message digest* terhadap berkas yang akan dievaluasi dan penggunaan tools yang sudah disertifikasi. Para pengacara berpendapat karena bukti digital secara teoritis mudah berubah (dimodifikasi dan digandakan), hal itu dapat merusak keandalan bukti. Para hakim AS mulai menolak teori ini, dalam kasus AS v. Bonallo, pengadilan memutuskan "fakta bahwa data yang ada dalam komputer dapat berubah jelas tidak cukup untuk membentuk ketidakpercayaan."

Dalam pedoman Inggris seperti yang dikeluarkan oleh *Association of Chief Police Officers* diikuti untuk membantu mendokumentasikan keaslian dan integritas barang bukti.
Seorang ahli harus menerapkan metode dan teknik yang terbukti andal secara ilmiah untuk mencari bukti digital. Penyidik digital khususnya dalam investigasi pidana, harus memastikan bahwa kesimpulan-kesimpulannya didasarkan pada bukti faktual dan pengetahuan kepakaran mereka sendiri.

Di AS, misalnya, *Federal Rules of Evidence* menyatakan bahwa seorang saksi yang memenuhi syarat sebagai ahli dapat bersaksi "dalam bentuk pendapat atau lainnya" jika:
1) kesaksian didasarkan pada fakta atau data yang cukup,
2) kesaksian adalah produk dari kaidah-kaidah dan metode-metode yang dapat diandalkan, dan
3) ahli telah menerapkan prinsip dan metode secara andal terhadap fakta-fakta kasus.

C. Tindak Pidana Siber

Tindak pidana siber atau cybercrime adalah fenomena kejahatan yang muncul sebagai dampak dari perkembangan teknologi informasi dan komunikasi. Kejahatan ini melibatkan penggunaan perangkat elektronik, seperti komputer dan internet, sebagai alat utama untuk melakukan tindakan melanggar hukum.

Menurut **Thomas J. Holt**, tindak pidana siber adalah kejahatan yang melibatkan komputer sebagai alat utama, baik sebagai target kejahatan, alat bantu, maupun media untuk menyebarluaskan hasil kejahatan. Ahli lain, seperti **Don Gotterbarn**, menambahkan bahwa tindak pidana siber tidak hanya mencakup kerugian finansial, tetapi juga mencakup pelanggaran privasi, reputasi, dan hak-hak digital individu.

III. METODE PENELITIAN

Penyusunan skripsi ini penulis memilih lokasi penelitian di Polda Sulawesi Tenggara. Jenis data yang digunakan adalah primer dan sekunder yang berasal dari field research dan Library research. Teknik pengumpulan data yang digunakan adalah wawancara dan dokumentasi dan menganalisis secara kualitatif.

V. HASIL DAN PEMBAHASAN

A. Fungsi Digital Forensik dalam Pembuktian Tindak Pidana Siber

Perkembangan teknologi membawa dampak positif dalam berbagai aspek kehidupan manusia, namun juga menjadi ladang subur bagi tindak pidana siber. Di Indonesia, laporan kejahatan siber meningkat secara signifikan seiring dengan tingginya penetrasi internet. Kejahatan seperti penipuan online, peretasan, pencurian identitas, dan penyebaran konten ilegal menjadi tantangan yang terus berkembang.

Digital forensik merupakan elemen kunci dalam investigasi tindak pidana siber. Dengan pesatnya perkembangan teknologi informasi dan komunikasi, kejahatan yang menggunakan perangkat digital sebagai alat maupun target semakin meningkat. Digital forensik hadir untuk menjawab kebutuhan pembuktian dalam ranah hukum, khususnya yang terkait dengan bukti elektronik. Melalui digital forensik, aparat penegak hukum dapat mengidentifikasi pelaku, menganalisis pola kejahatan, dan menyajikan bukti yang sah di hadapan pengadilan.

Dalam konteks tindak pidana siber, digital forensik memberikan solusi terhadap tantangan pengumpulan bukti yang sering kali bersifat tidak kasat mata, rentan dihapus, atau dimodifikasi. Proses ini tidak hanya penting untuk membuktikan kesalahan pelaku, tetapi juga untuk menjaga keadilan dengan memastikan integritas bukti yang digunakan dalam proses peradilan.
Landasan hukum terkait digital forensik di Indonesia telah diatur dalam beberapa peraturan, antara lain:
1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Memberikan definisi dan cakupan kejahatan siber serta mengatur penggunaan bukti elektronik sebagai alat bukti yang sah di pengadilan.

2. Undang-Undang Nomor 19 Tahun 2016 (Revisi UU ITE) Memperkuat ketentuan terkait sanksi dan perluasan definisi tindak pidana siber.
3. Peraturan Kapolri Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana, Mengatur mekanisme penggunaan bukti elektronik dalam proses penyidikan, termasuk metode digital forensik.
4. Konvensi Budapest

Dalam hal ini aparat kepolisian memiliki peran penting untuk menanggulangi kejahatan siber dengan yang semakin marak khususnya di wilayah Sulawesi Tenggara. Sebagai Gambaran berikut adalah struktur organisasi Kepolisian Daerah (Polda) Sulawesi Tenggara (Sultra) beserta nama-nama pejabat utamanya:

1. Kepala Kepolisian Daerah (Kapolda): Memimpin seluruh kegiatan operasional dan administratif Polda Sultra.
2. Wakil Kepala Kepolisian Daerah (Wakapolda): Membantu Kapolda dalam pelaksanaan tugas dan menggantikan Kapolda jika berhalangan.
3. Inspektur Pengawasan Daerah (Irwasda): Bertanggung jawab atas pengawasan dan pemeriksaan internal di lingkungan Polda Sultra.
4. Kepala Biro Operasi (Karo Ops): Mengkoordinasikan dan mengendalikan operasi kepolisian di wilayah hukum Polda Sultra.
5. Kepala Biro Sumber Daya Manusia (Karo SDM): Mengelola sumber daya manusia, termasuk rekrutmen, pelatihan, dan pengembangan personel.
6. Direktur Reserse Kriminal Umum (Dirreskrimum): Memimpin penyelidikan dan penyidikan tindak pidana umum.
7. Direktur Reserse Kriminal Khusus (Dirreskrimsus): Menangani kasus-kasus kriminal khusus, termasuk tindak pidana siber.
8. Direktur Reserse Narkoba (Dirresnarkoba): Bertanggung jawab atas penanggulangan kejahatan narkotika dan obat-obatan terlarang.
9. Direktur Lalu Lintas (Dirlantas): Mengelola lalu lintas dan angkutan jalan, termasuk penegakan hukum di bidang lalu lintas.
10. Direktur Intelijen Keamanan (Dirintelkam): Mengumpulkan dan menganalisis informasi intelijen untuk menjaga keamanan dan ketertiban.
11. Kepala Bidang Hubungan Masyarakat (Kabid Humas): Mengelola komunikasi dan informasi antara Polda Sultra dengan masyarakat dan media.

Dalam mengatasi kehatan siber, ahli digital forensik memiliki peran yang sangat penting dalam memastikan bukti digital dapat diidentifikasi, dikumpulkan, dan dianalisis dengan benar. Berikut adalah beberapa peran utama ahli digital forensik:

1. Mengidentifikasi Sumber Bukti Digital Ahli digital forensik bertugas mengidentifikasi perangkat yang menjadi sumber bukti, seperti komputer, ponsel, atau server. Mereka juga menentukan data apa yang relevan untuk diambil sebagai bagian dari penyelidikan.
2. Mengamankan dan Memastikan Keaslian Bukti Ahli digital forensik menggunakan metode yang sesuai standar untuk mengamankan bukti digital agar tidak terjadi perubahan atau kerusakan. Teknik seperti hashing digunakan untuk memastikan bahwa data yang dianalisis tetap asli dan dapat diverifikasi di pengadilan.
3. Melakukan Pemulihan Data Dalam banyak kasus, pelaku kejahatan mencoba menghapus jejak mereka dengan menghapus data. Ahli digital forensik memiliki kemampuan untuk memulihkan data yang dihapus, termasuk email, file, atau log aktivitas sistem.
4. Menganalisis Bukti Digital Analisis bukti melibatkan pemeriksaan mendalam terhadap data digital untuk mengidentifikasi pola, aktivitas mencurigakan, atau hubungan antar data yang relevan dengan tindak pidana. Misalnya, pelacakan alamat IP, log akses, atau metadata file.
5. Memberikan Kesaksian Ahli di Pengadilan Ahli digital forensik sering kali diminta untuk memberikan kesaksian di pengadilan terkait temuan mereka. Mereka menjelaskan proses pengumpulan dan analisis bukti, serta memastikan bukti tersebut memenuhi standar hukum.

6. Meningkatkan Kapasitas Penegak Hukum Ahli digital forensik juga berperan dalam memberikan pelatihan kepada aparat penegak hukum untuk meningkatkan kemampuan mereka dalam menangani barang bukti digital. Kerja sama ini penting untuk memastikan bahwa penyelidikan dapat berjalan dengan lancar.

Prosedur digital forensik di Polda Sulawesi Tenggara umumnya melibatkan tahapan berikut:
1. Penilaian Awal *(Assessment)*
2. Akuisisi *(Acquisition)*
3. Pemeriksaan dan Analisis (*Examination and Analysis)*
4. Dokumentasi dan Pelaporan *(Documentation and Reporting)*

Hasil analisis disusun dalam bentuk laporan yang terstruktur dan siap digunakan dalam proses hukum. Prosedur ini telah diterapkan di Polda Sultra untuk berbagai kasus tindak pidana siber, meskipun masih menghadapi hambatan seperti keterbatasan tenaga ahli dan infrastruktur teknologi yang kurang memadai. Salah satu kasus menonjol di Sulawesi Tenggara adalah peretasan akun media sosial milik tokoh masyarakat di Kendari. Dalam kasus ini, pelaku berhasil mengakses akun korban dan menyebarkan konten yang merugikan reputasi korban. Tim digital forensik Polda Sultra berhasil mengidentifikasi pelaku melalui analisis alamat IP, jejak digital pada perangkat, dan aktivitas login yang mencurigakan.

Kasus lainnya adalah penipuan berbasis e-commerce pada tahun 2023, di mana pelaku menggunakan data identitas palsu untuk menipu pembeli. Digital forensik berperan dalam melacak transaksi digital dan pola komunikasi pelaku, yang akhirnya menjadi bukti kuat dalam pengadilan.
Polda Sultra meminta seluruh warga untuk waspada modus penipuan online melalui media sosial, seperti facebook, twitter dan instagram. Kapolda Sultra Irjen Pol Dwi Irianto mengungkapkan, belakangan ini, Polda Sultra telah menerima banyak laporan terkait dengan tindak pidana penipuan dengan modus penjualan sepeda motor dan mobil melalui media sosial.

Dalam wawancara dengan Irjen Pol Dwi Irianto Kapolda Sultra, beliau menyatakan komitmennya untuk meningkatkan kualitas sumber daya manusia di lingkungan Polda Sultra melalui berbagai program pelatihan dan pengembangan kompetensi. Serta menekankan pentingnya pengawasan internal yang ketat untuk memastikan transparansi dan akuntabilitas dalam setiap tindakan kepolisian.

Fungsi digital forensik dalam pembuktian tindak pidana siber tidak dapat disangkal sebagai elemen vital dalam proses penegakan hukum. Dengan landasan hukum yang kuat dan prosedur yang terstandar, digital forensik memberikan jaminan keabsahan bukti yang digunakan di pengadilan. Namun, untuk mengoptimalkan fungsi ini di Polda Sulawesi Tenggara, diperlukan langkah strategis seperti:
1. Peningkatan Kompetensi SDM: Melalui pelatihan intensif bagi aparat penegak hukum.
2. Pengadaan Infrastruktur Modern: Meliputi perangkat lunak dan perangkat keras forensik terkini.
3. Kolaborasi dengan Institusi Akademik dan Internasional: Untuk mengadopsi metode forensik terbaik dan berbagi pengetahuan.

B. Kendala yang Dihadapi Digital Forensik pada Penyidikan Tindak Pidana Siber

Digital forensik merupakan salah satu elemen paling vital dalam penyidikan kejahatan siber, terutama di era digital yang terus berkembang. Peran digital forensik meliputi identifikasi, pengumpulan, analisis, dan pelaporan bukti elektronik yang digunakan dalam proses hukum. Dalam penyidikan tindak pidana siber, digital forensik memungkinkan aparat penegak hukum untuk melacak jejak digital pelaku, memulihkan data yang hilang atau dihapus, dan menyajikan bukti yang sah di pengadilan. Namun, implementasi digital forensik di Indonesia, khususnya di daerah seperti Sulawesi Tenggara, tidak terlepas dari berbagai kendala yang memengaruhi efektivitasnya. Kendala-

kendala tersebut tidak hanya berasal dari keterbatasan teknis, tetapi juga dari aspek sumber daya manusia, infrastruktur, hingga regulasi yang belum optimal.

Untuk memahami lebih jauh, pembahasan ini akan menguraikan secara umum kendala digital forensik di Indonesia dan mengaitkannya dengan kasus konkret yang terjadi di Kota Kendari, Sulawesi Tenggara. Kendala Umum dalam Implementasi Digital Forensik adalah :

1. Keterbatasan Sumber Daya Manusia (SDM) yang Terampil Salah satu kendala utama dalam implementasi digital forensik adalah kurangnya personel dengan kompetensi khusus di bidang ini. Digital forensik memerlukan keahlian teknis yang tinggi, termasuk kemampuan dalam pemulihan data, analisis jaringan, dan pengenalan pola kejahatan. Namun, tidak semua aparat penegak hukum di Indonesia memiliki pelatihan atau sertifikasi di bidang ini, sehingga proses penyelidikan sering kali menjadi lambat.
2. Kurangnya Infrastruktur Teknologi Peralatan dan perangkat lunak forensik yang canggih sangat diperlukan untuk mendukung analisis bukti digital. Sayangnya, banyak institusi penegak hukum di Indonesia yang masih menghadapi keterbatasan dalam hal pengadaan alat tersebut. Misalnya, perangkat lunak analisis forensik seperti EnCase atau Forensic Toolkit (FTK) sering kali tidak tersedia secara merata di berbagai daerah.
3. Hambatan Hukum dan Regulasi Regulasi yang ada, seperti UU ITE, telah memberikan dasar hukum untuk penggunaan bukti digital. Namun, implementasinya masih menghadapi hambatan. Salah satunya adalah prosedur hukum yang panjang untuk mendapatkan akses ke data yang diperlukan, terutama jika melibatkan platform internasional seperti Facebook atau WhatsApp.
4. Kerentanan Bukti Digital Barang bukti digital memiliki sifat yang rentan terhadap manipulasi, kerusakan, atau penghapusan. Tanpa prosedur yang tepat, integritas bukti dapat terganggu, sehingga tidak dapat diterima di pengadilan.
5. Minimnya Kesadaran Masyarakat tentang Keamanan Siber Rendahnya kesadaran masyarakat tentang ancaman kejahatan siber juga menjadi kendala. Banyak korban yang tidak sadar bahwa mereka telah menjadi target penipuan hingga terlambat, sehingga menyulitkan aparat untuk mengumpulkan bukti yang relevan.

Fenomena kejahatan siber di Kota Kendari, Sulawesi Tenggara, memberikan gambaran nyata tentang tantangan yang dihadapi dalam implementasi digital forensik. Salah satu kasus yang menarik perhatian publik adalah kasus penipuan online yang memanfaatkan media sosial. Artikel RRI yang berjudul *"Warga Kendari Diimbau Waspada Penipuan Online di Media Sosial"* (RRI, 2023) mengungkapkan bahwa pelaku kejahatan siber menggunakan akun media sosial palsu untuk menawarkan barang dengan harga sangat murah. Setelah korban melakukan pembayaran, pelaku menghilang tanpa memberikan barang yang dijanjikan.

Dalam kasus ini, Polda Sultra melalui unit digital forensik berupaya melacak jejak digital pelaku. Namun, pelaku menggunakan metode seperti Virtual Private Network (VPN) untuk menyembunyikan alamat IP dan identitas aslinya, sehingga menyulitkan proses pelacakan. Selain itu, akun media sosial yang digunakan sering kali dibuat dengan identitas palsu, yang mempersulit proses verifikasi data oleh pihak berwenang.

Kasus lainnya adalah peretasan akun media sosial milik tokoh masyarakat di Kendari. Pelaku berhasil mengakses akun korban dan menyebarkan informasi yang merugikan reputasi korban. Dalam penyelidikan, Polda Sultra menghadapi tantangan dalam memulihkan data dan melacak aktivitas login yang mencurigakan. Proses ini memakan waktu lebih lama karena keterbatasan perangkat lunak forensik yang tersedia di wilayah tersebut. Langkah Strategis untuk Mengatasi Kendala tersebut

1. Peningkatan Kompetensi SDM
   a. Menyelenggarakan pelatihan dan sertifikasi intensif bagi personel di bidang digital forensik, khususnya yang bertugas di daerah seperti Sulawesi Tenggara.

   b. Mengembangkan program kerja sama dengan institusi akademik dan profesional di bidang teknologi informasi untuk memperluas pengetahuan dan keterampilan aparat penegak hukum.
2. Pengadaan Infrastruktur Teknologi
   a. Mengalokasikan anggaran khusus untuk pengadaan perangkat keras dan perangkat lunak forensik yang canggih.
   b. Meningkatkan kapasitas server dan infrastruktur jaringan untuk mendukung analisis data secara real-time.
3. Optimalisasi Regulasi
   a. Mempercepat proses legislasi yang mendukung efisiensi penyelidikan digital.
   b. Mendorong kerja sama dengan platform media sosial internasional untuk mempercepat akses terhadap data pengguna yang terlibat dalam tindak pidana siber.
4. Edukasi Masyarakat
   a. Mengadakan kampanye publik untuk meningkatkan kesadaran masyarakat tentang modus operandi kejahatan siber dan cara melindungi diri.
   b. Mendorong pelaporan dini oleh korban agar bukti dapat segera dikumpulkan sebelum pelaku menghapus jejak digitalnya.
5. Penguatan Prosedur Penanganan Bukti Digital
   a. Mengembangkan Standard Operating Procedure (SOP) yang ketat untuk menangani barang bukti digital.
   b. Memanfaatkan teknologi enkripsi dan hash untuk menjaga keaslian bukti digital selama proses penyelidikan.

Peningkatan kompetensi personel Polda Sulawesi Tenggara (Sultra) dalam bidang forensik digital merupakan langkah strategis untuk mengatasi berbagai kendala yang telah diidentifikasi sebelumnya. Salah satu upaya konkret yang dilakukan adalah melalui program edukasi yang diselenggarakan oleh tim dari Universitas Islam Indonesia (UII).

Program ini bertujuan untuk membekali personel Polda Sultra dengan pengetahuan dan keterampilan terkini dalam forensik digital, sehingga mereka lebih siap menghadapi tantangan dalam penyidikan tindak pidana siber. Tim Universitas Islam Indonesia (UII) menyambangi personel Kepolisian Daerah (Polda) Sulawesi Tenggara (Sultra) di Ruangan Vicon SDM Polda Sultra.Selasa, 20 Juni 2023.

Dalam kegiatan workshop mini ini, Magister Informatika (MI) Fakultas Teknologi Industri (FTI) UII menghadirkan pemateri berkompeten di bidang forensik digital dan keamanan komputer yakni Dr. Yudi Prayudi, S.Si, M.Kom. Manajer Keilmuan Program Studi Informatika FTI UII Yogyakarta, Dr. Ahmad Luthfi mengatakan, kunjungan ini dalam rangka menjalin silaturahmi dan memberikan edukasi kepada institusi Polri khususnya Polda Sultra.

Melalui pelatihan ini, personel diharapkan mampu mengoperasikan perangkat lunak dan perangkat keras forensik dengan lebih efektif, memahami prosedur penanganan barang bukti digital sesuai standar internasional, serta meningkatkan kemampuan analisis terhadap berbagai modus operandi kejahatan siber. Langkah ini sejalan dengan rekomendasi untuk meningkatkan kompetensi sumber daya manusia dalam menghadapi kompleksitas kejahatan digital di era modern.“Materi yang disampaikan tadi terkait dengan penanganan proses bukti elektronik secara umum tadi juga ada mini Workshop begitu, bagaimana cara melakukan manajemen bukti elektronik. Harapannya dari pihak Siber Polda Sultra memeliki pemahaman yang lebih baik terkait dengan isu-isu terkini pada bidang kejahatan siber,”

Sementara itu, Porseleksi Bagdalpers SDM Polda Sultra, Iptu Muhammad Rosman mengucapkan terima kasih atas kunjungan dan ilmu yang telah diberikan kepada personel Polda Sultra. “Mengucapkan terima kasih kepada USN Kolaka yang telah memprakarsai kegiatan ini, kami cukup

terbantu atas pemateri yang dihadirkan dari Universitas Islam Indonesia terkait dengan peningkatan kemampuan teman-teman yang ada di Siber, kemudian di Inteltek juga dari Resmob," ucap Iptu Rosman.

Ia mengungkapkan, dengan adanya kolaborasi antara kepolisian dan perguruan tinggi ini tentunya sangat membantu dalam meningkatkan kapasitas personel Polda Sultra khususnya. "Semua ini sangat besar manfaatnya terkait dengan peningkatan kemampuan personel Polda Sultra," ungkap Iptu Rosman. Implementasi program edukasi seperti yang dilakukan oleh tim UII ini diharapkan dapat menjadi model bagi institusi penegak hukum lainnya dalam upaya memperkuat kapasitas forensik digital di Indonesia. Dengan demikian, penegakan hukum terhadap tindak pidana siber dapat dilakukan secara lebih efektif dan efisien, serta memberikan rasa aman bagi masyarakat dalam beraktivitas di dunia digital.

Kejahatan siber yang terjadi di Kota Kendari, seperti penipuan online dan peretasan media sosial, menunjukkan kompleksitas tantangan yang dihadapi dalam implementasi digital forensik. Kendala utama meliputi keterbatasan SDM, infrastruktur teknologi, regulasi, serta minimnya kesadaran masyarakat tentang keamanan siber. Untuk mengatasi kendala tersebut, diperlukan langkah-langkah strategis seperti peningkatan kompetensi SDM, pengadaan infrastruktur modern, optimalisasi regulasi, edukasi masyarakat, dan penguatan prosedur penanganan bukti digital. Dengan pendekatan ini, diharapkan digital forensik dapat menjadi instrumen yang lebih efektif dalam menangani tindak pidana siber, tidak hanya di Sulawesi Tenggara tetapi juga di seluruh Indonesia. Keberhasilan ini akan memberikan dampak positif terhadap peningkatan keamanan masyarakat dan penegakan hukum di era digital.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

1. Digital forensik memiliki peran penting dalam pembuktian tindak pidana siber karena mampu mengidentifikasi, mengumpulkan, dan menganalisis bukti digital yang relevan. Proses ini memastikan bahwa bukti dapat digunakan secara sah di pengadilan, mendukung pengungkapan fakta, dan memperkuat dakwaan terhadap pelaku. Dengan prosedur yang sistematis seperti akuisisi bukti, analisis data, dan pelaporan hasil, digital forensik membantu penegak hukum menangani kejahatan siber secara efektif.
2. Kendala utama yang dihadapi dalam implementasi digital forensik meliputi keterbatasan sumber daya manusia, kurangnya infrastruktur teknologi, hambatan regulasi, serta minimnya kesadaran masyarakat. Studi kasus di Kota Kendari menunjukkan bahwa kejahatan siber seperti penipuan online dan peretasan akun media sosial masih menjadi tantangan besar. Untuk mengatasi kendala ini, diperlukan langkah strategis berupa peningkatan kompetensi aparat, penguatan kerja sama dengan ahli forensik, dan edukasi masyarakat.

B. Saran

1. Untuk ptimalisasi peran aparat penegak hukum dalam menaggulangi kejahatan siber memerlukan peningkatan kapasitas personel, pengadaan infrastruktur teknologi, dan kolaborasi lintas sektor.
2. Secara keseluruhan, sinergi antara kepolisian, ahli digital forensik, dan institusi terkait lainnya menjadi kunci utama dalam meningkatkan efektivitas penegakan hukum terhadap tindak pidana siber di era digital. Dengan pendekatan yang terintegrasi, upaya ini tidak hanya memberikan rasa aman bagi masyarakat, tetapi juga memperkuat sistem peradilan pidana di Indonesia.

DAFTAR PUSTAKA

Peraturan Perundang-undangan :

Peraturan Kapuslabfor Bareskrim Polri Nomor 1 Tahun 2014 tentang Standar Operasional Prosedur (SOP) Pemeriksaan dan Analisa Digital Forensik.

Peraturan Kepala Kepolisian Republik Indonesia Nomor 10 Tahun 2009 tentang Tata Cara dan Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik Tempat Kejadian Perkara dan Laboratoris Kriminalistik Barang Bukti Kepada Laboratorium Forensik Kepolisian Republik Indonesia

Undang-undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-undang No. 11 Tahun 2008 tentang Indofmasi dan Transaksi Elektronik. Lembaran Negara Nomor 5952

Undang-undang No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Lembaran Negara Nomor 4168

Undang-undang No. 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana. Lembaran Negara Nomor 3209

Buku :

Al-Azhar, Muhammad Nuh. *Digital Forensic Panduan Praktis Investigasi Komputer*. (Jakarta: Salemba Infotek: 2012)

Ali, Mahrus. *Dasar Dasar Hukum Pidana*, Ctk. Pertama, (Jakarta: Sinar Grafika, 2011)

Budhijanto, Danrivanto. *Revolusi Cyberlaw Indonesia Pembaruan dan Revisi UU ITE 2016*. (Bandung: Refika Aditama, 2017)

Chazawi, Adami. *Tindak Pidana Pornografi*. (Jakarta: Sinar Grafika, 2016), Djulaeka dan Devi Rahayu. *Buku Ajar Metode Penelitian Hukum.* (Surabaya: Scopindo Media Pustaka, 2019).

Ghony, M. Djunaidi, dan Fauzan Al-Mansur. *Metodologi Penelitian Kualitatif*. (Yogyakarta: Ar-Ruzz Media, 2014).

Harahap, M. Yahya. *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, dan Peninjauan Kembali*. (Jakarta: Sinar Grafika. 2015)

Manuhutu, Melda Agnes, dkk. *Pengantar Forensik Teknologi Informasi*. (Medan: Yayasan Kita Menulis, 2021)

Maskun, dan Wiwik Meilarati. *Aspek Hukum Penipuan Berbasis Internet*. (Bandung: Keni Media, 2017).

Maskun. kejahatan *Siber (Cyber Crime) Suatu Pengantar*. (Jakarta: Kencana Putra Utana, 2013).

Moeljanto. *Azaz-azaz Hukum Pidana*. (Jakarta: Rineka Cipta, 2009)

Muis, Abdul. Harry Anwar, Imas Rosidawati. *Hukum Kepolisian dan Kriminalistik.* (Bandung: Penerbit Pustaka Reka Cipta, 2021)

Mutiara, Ahmad Benny. *Panduan Komputer Forensik dalam Penanganan Bukti Digital Pada Personal Digital* Asistant. (Bogor: Penerbit Universitas Gunadarma, 2007)

Nasution, Bahder Johan. *Metode Penelitian Ilmu Hukum.* (Bandung: Penerbit CV Mandar Maju, 2008).

Purwoleksono, Didik Endro. *Hukum Acara Pidana*. (Airlangga University Press, 2015)

Raharjo, Agus. *CyberCrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi.* (Bandung: Citra Aditya Bakti, 2002)

Sudyana, Didik. *Mengenali Forensik Digital*. (Yogyakarta: Diandra Creative, 2016)

Sulianta, Feri. *Komputer Forensik Melacak Kejahatan Digital*. (Yogyakarta: CV Andi Offser, 2016)

Tahir, Ach. *Cyber Crime (Akar Masalah, Solusi, dan Penanggulangannya).* (Yogyakarta: SUKA Press, 2011)

Internet :

https://elindonews.id/2023/06/tim-uii-edukasi-personel-polda-sultra-soal-forensik-digital/
https://rri.co.id/kriminalitas/545013/warga-kendari-diimbau-waspada-penipuan-online-di-media-sosial