LOFIAN: Jurnal Teknologi Informasi dan Komunikasi
https://ejournal.umbp.ac.id/index.php/lofian/
Vol. 3, No. 1, Agustus 2023, Halaman 12-19

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Implementasi Metode Standar NIST Dalam Analisis Data Forensik Studi Kasus Penipuan Salah Transfer Mencatut Nama Wabup Pada SMP Ar-rohman Krangkeng

Didi Royadi[1], Marsani Asfi[2], Agus Sevtiana[3]

[1,2]*Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Catur Insan Cendekia*
Jl. Kesambi 202, Kota Cirebon, Jawa Barat, Indonesia - 45133

[3]*Program Studi Manajemen Informatika, Fakultas Teknologi Informasi, Universitas Catur Insan Cendekia*
Jl. Kesambi 202, Kota Cirebon, Jawa Barat, Indonesia - 45133

[1]*didiroyadi123@gmail.com,* [2]*marsani.asfi@cic.ac.id,* [3]*agus.sevtiana@cic.ac.id*

DOI: 10.58918/lofian.v3i1.216

Abstrak

Dalam beberapa waktu terakhir, kemajuan pesat teknologi tidak hanya membawa dampak positif, tetapi juga dampak negatif, termasuk munculnya modus penipuan baru yang memanfaatkan teknologi dan mencatut nama pejabat publik untuk mempermudah aksinya. Pelaku seringkali menggunakan media sosial seperti WhatsApp untuk melancarkan kejahatannya. Pada studi kasus ini, terjadi penipuan dengan mengatasnamakan pejabat publik yang terjadi di SMP Ar-rohman Krangkeng. Penelitian ini menggunakan metode NIST (*National Institute of Standards and Technology*), yang terdiri dari empat tahap: Pengumpulan (*collecting*), Pemeriksaan (*examination*), Analisis (*analysis*), dan Pelaporan (*Reporting*). Pada tahap Pengumpulan (*collecting*), penulis mengumpulkan barang bukti dari sisi korban dan pelaku (*phishing link*). Pada tahap Pemeriksaan (*examination*), penulis menggunakan alat *FTK Imager* dan *hashmyfile* untuk validasi. Setelah itu, dilakukan analisis (*analysis*), data dan hasil akhirnya disusun dalam bentuk laporan *Reporting*. Penggunaan metode NIST menghasilkan bukti penting dari perspektif korban, seperti percakapan *WhatsApp Web* dengan pelaku, sedangkan dari sisi pelaku, bukti yang ditemukan meliputi foto pelaku, alamat *IP* (202.67.41.246), lokasi di Surabaya, Jawa Timur (*latitude* -7.2574719, *longitude* 112.7520883), dan jenis perangkat Android yang digunakan oleh pelaku dalam menjalankan aksinya. Diharapkan bukti yang ditemukan dapat membantu pihak berwenang dalam mengambil tindakan yang tepat dan mencegah kejadian serupa terulang di masa mendatang. Efektivitas metode analisis forensik berbasis NIST yang ditunjukkan dalam penelitian ini menjadi referensi untuk penyelidikan di masa depan.

Kata Kunci: NIST, Security, Analisis, Penipuan, FTK imager.

1. Pendahuluan

Penipuan dalam bentuk transfer uang semakin marak terjadi, terutama dengan adanya perkembangan teknologi yang memungkinkan pelaku untuk dengan mudah menciptakan berbagai modus baru. Hal ini semakin memperkuat perlunya penggunaan metode analisis forensik data untuk mengungkap kasus-kasus penipuan tersebut. Salah satu metode analisis forensik data yang paling umum digunakan adalah metode Standar NIST.

Metode Standar NIST adalah Metode yang diterapkan dalam analisis forensik data bertujuan untuk memverifikasi keabsahan, keutuhan, dan keakuratan data yang sedang dianalisis. Metode ini telah digunakan secara luas oleh instansi dan lembaga pemerintah di seluruh dunia dalam rangka penyelidikan tindak kejahatan. NIST adalah sebuah metode yang memiliki empat tahapan dalam menyelesaikan dan menyelidikan kasus *Cyber Crime*, tahap pertama yaitu *Collection* (Pengumpulan Data), *Examination* (Pemeriksaan barang bukti), *Analysis*, dan yang terakhir adalah *Reporting* (Membuat laporan berdasarkan hasil analisis).

Studi kasus yang digunakan dalam penelitian ini adalah kasus penipuan transfer yang mencatut nama wakil bupati pada sebuah SMP di Arrohman. Kasus ini menjadi menarik untuk diteliti karena pelaku berhasil memanfaatkan nama pejabat publik untuk memperoleh keuntungan secara ilegal. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan metode Standar NIST dalam analisis forensik data untuk membantu mengungkap kejahatan tersebut.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

2. Landasan Teori

2.1. Forensik Digital

Menurut Al-Azhar dan N. Muhammad (2012) dikutip dari [8] merupakan aplikasi dalam ilmu pengetahuan terutama teknologi komputer yang berguna untuk pembuktian di bidang hukum (*pro justice*), dalam hal ini untuk membuktikan kejahatan dengan smartphone atau kejahatan computer secara ilmiah sehingga didapatkan bukti-bukti digital yang digunakan untuk menghukum pelaku kejahatan.

Berdasarkan jurnal [9] digital forensic adalah cabang ilmu yang melibatkan penerapan prinsip-prinsip ilmiah untuk penyelidikan artefak dalam satu atau lebih perangkat digital untuk memahami dan merekonstruksi urutan peristiwa yang pasti terjadi dalam menghasilkan artefak tersebut. Forensik digital berkaitan dengan memperoleh, memeriksa, menganalisis, dan mungkin mendokumentasikan dan menyajikan artefak dan urutan peristiwa yang direkonstruksi sebagai bukti dalam pengadilan. Forensik digital dikembangkan secara independen bidang pada akhir 1990-an dan awal 2000-an ketika kejahatan berbasis komputer mulai tumbuh dengan meningkatnya penggunaan komputer dan lebih lagi, internet. Pada awalnya itu disebut forensik komputer karena bukti yang dikumpulkan adalah terbatas pada komputer. Namun, dalam beberapa tahun terakhir dengan beberapa kemajuan teknologi pembatasan ini tidak lagi benar.

2.2. Bukti Digital

Di Menurut [14] 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. Sedangkan menurut [15] berikut ini adalah contoh barang bukti digital diantaranya adalah *logical file, deleted file, lost file, log file, video file, image file*, dll.

2.3. Teknik Phising

Menurut jurnal [16] *Phishing* adalah tindakan yang mengancam atau menjerat orang dengan menggunakan konsep memancing. Dalam kegiatan ini, seseorang akan ditipu untuk memberikan informasi yang diinginkan oleh pelaku tanpa disadarinya. Sumber ancaman *phishing* bisa berasal dari *email*, *website*, dan *malware*. Berdasarkan hasil survei, website merupakan sumber ancaman phishing yang paling sering terjadi, dan cara pencegahan yang paling umum dilakukan adalah dengan meningkatkan *self-efficacy* atau keyakinan individu untuk mengambil tindakan. Sedangkan pada jurnal [17] *phising* didefinisikan sebagai teknik yang digunakan *hacker* untuk dapat mengakses sebuah komputer secara tidak sah yang mana menimbulkan sebuah ancaman. Berdasarkan dua penelitian terdahulu, dapat disimpulkan bahwa *phishing* merupakan tindakan yang mengancam dan menjerat orang dengan menggunakan konsep memancing. Hal ini dilakukan dengan cara menipu individu untuk memberikan informasi yang diinginkan oleh pelaku tanpa disadarinya. Sumber ancaman *phishing* dapat berasal dari *email*, *website*, dan *malware*. Hasil survei menunjukkan bahwa website menjadi sumber ancaman phishing yang paling sering terjadi, dan upaya pencegahan yang umum dilakukan adalah dengan meningkatkan *self-efficacy* atau keyakinan individu untuk mengambil tindakan.

Namun, penting untuk dicatat bahwa dalam konteks penelitian ini, penggunaan teknik *phishing* tidak dilakukan dengan tujuan jahat atau merugikan pihak lain. Sebaliknya, teknik *phishing* digunakan sebagai metode investigasi dalam rangka pengungkapan kasus penipuan salah transfer. Penelitian ini bertujuan untuk mendapatkan bukti dan informasi yang relevan guna mengidentifikasi pelaku dan mengungkap kebenaran dalam kasus tersebut. Oleh karena itu, penggunaan teknik *phishing* dalam penelitian ini dapat diterima karena bertujuan baik dan dilakukan dalam kerangka hukum yang berlaku.

Dengan demikian, penting untuk memahami bahwa konteks penggunaan teknik *phishing* dapat berbeda tergantung pada niat dan tujuan yang ada. Dalam konteks penelitian forensik seperti ini, teknik *phishing* dapat menjadi alat yang berguna dalam mengumpulkan informasi dan bukti yang relevan. Namun, dalam situasi umum, penting untuk selalu menjaga keamanan dan privasi data serta berhati-hati terhadap ancaman phishing yang mungkin merugikan individu atau organisasi.

2.4. FTK Imager

FTK merupakan [18] *software* yang digunakan untuk membuat salinan yang identik dengan *file* asli dari data elektronik korban. Proses ini dilakukan agar data awal tidak mengalami perubahan. *Hardware* dan *software* yang digunakan pada computer forensic dapat menjaga agar data tetap utuh seperti sebelumnya (tidak adaperubahan), bahkan dapat menemukan *file* yang telah terhapus sehingga akan ditemukan bukti (*evidence*) dari kasus yang terjadi. Untuk mengumpulkan bukti dalam forensik digital,

e-ISSN: 2798-9593
p-ISSN: 2798-9836

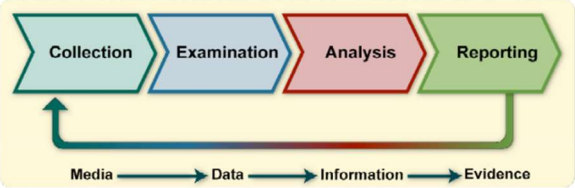
diperlukan tahapan pengumpulan barang bukti dan melakukan *imaging* data terhadap barang bukti yang telah diperoleh. Salah satu jenis barang bukti yang dapat di-*imaging* adalah *notebook*, dimana *hardisk* pada *notebook* tersebut dapat di-*imaging* dengan dua pilihan, yaitu *physical drive* atau *logical drive*. Jika memilih *physical drive*, maka FTK *imager* akan melakukan *imaging* terhadap seluruh *hardisk* berdasarkan kapasitasnya, sedangkan pada *logical drive*, *examiner* dapat memilih partisi mana yang akan diimaging sesuai dengan kebutuhan. Data yang akan dianalisis meliputi dokumen, pesan *email*, *file* yang telah dihapus, *thumbnail*, grafik, *folder* dan log jaringan. Dari data tersebut, *examiner* akan mencari bukti yang terkait dengan kasus yang sedang ditangani.

3. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode National Institute of Standards and Technology (NIST). NIST adalah sebuah metode yang memiliki empat tahapan dalam menyelesaikan dan menyelidikan kasus Cyber Crime, tahap pertama yaitu Collection (Pengumpulan Data), Examination (Pemeriksaan barang bukti), Analysis, dan yang terakhir adalah Reporting (Membuat laporan berdasarkan hasil analisis).

3.1. Tahapan Metodologi NIST

Metodologi NIST [6] dalam analisis forensik data terdiri dari beberapa tahapan, yaitu:



Gbr. 1. Tahap penelitian

1. *Collection*: Tahap pengumpulan bukti digital dari sumber yang relevan dengan kasus yang sedang diselidiki, perangkat lunak, jaringan, dan penyimpanan data.
   Fase pertama dalam proses adalah mengidentifikasi, memberi label, merekam, dan memperoleh data dari kemungkinan sumber data yang relevan, sambil mengikuti pedoman dan prosedur yang menjaga integritas data. Pengumpulan biasanya dilakukan tepat waktu karena kemungkinan kehilangan data dinamis seperti koneksi jaringan saat ini, serta kehilangan data dari perangkat bertenaga baterai dalam hal kegiatan pengumpulan data ini penulis menggunakan teknik *Live forensic* menggunakan *tools* FTK *imager* serta melakukan pengamanan terhadap perangkat PC untuk mengumpulkan data dari sisi korban dan penulis juga menggunakan teknik *Phising* berupa *link* menggunakan alat Maxphisher untuk akuisisi data (foto dll) dari penipu.
2. *Examination*: Tahap pemeriksaan dan analisis bukti digital dengan menggunakan teknik dan alat forensik yang terstandarisasi, termasuk pengambilan gambar forensik, analisis file dan metadata, serta pemulihan data yang hilang. Pemeriksaan melibatkan pemrosesan sejumlah besar data yang dikumpulkan secara forensik menggunakan kombinasi metode otomatis dan manual untuk menilai dan mengekstrak data tertentu, dengan tetap menjaga integritas data.
3. *Analysis*: Tahap analisis data digital yang ditemukan dan dianalisis, termasuk identifikasi, validasi, dan interpretasi data untuk mendukung temuan dan kesimpulan.
   Tahap proses selanjutnya adalah menganalisis hasil pemeriksaan, dengan menggunakan metode dan teknik yang dapat dibenarkan, untuk memperoleh informasi yang berguna yang menjawab pertanyaan-pertanyaan itu adalah dorongan untuk melakukan pengumpulan dan pemeriksaan.
4. *Reporting*: Tahap penyusunan laporan hasil analisis forensik data, termasuk temuan, metodologi, dan kesimpulan, serta disampaikan ke pihak yang berwenang.

3.2. Implementasi kronologi kasus ke Metode NIST

1. *Data Collection*

Dalam proses forensik, langkah pertama yang harus dilakukan adalah mengidentifikasi sumber data potensial dan memperoleh data darinya. Oleh karena itu, penulis meminta kepada ibu A, yang merupakan korban penipuan salah transfer, untuk memberikan bukti tangkapan layar percakapan dengan pelaku dan memberikan akses terhadap pesan *Whatsapp Web* miliknya. Dalam tahap ini, penulis menggunakan teknik *live forensic* pada laptop korban dan juga menerapkan teknik *phishing* untuk mendapatkan informasi yang relevan, pada perangkat pelaku akan dilakukan pemberian *link phising* yang mirip dengan bukti transfer senilai 7 juta kepada pelaku. Dalam hal ini, tujuan pemberian link phising tersebut adalah untuk mendapatkan data tambahan seperti foto, *IP address*, jenis *browser* yang digunakan, serta latitude dan longitude nya. Jika pelaku menekan link phising

e-ISSN: 2798-9593
p-ISSN: 2798-9836

tersebut, maka penulis akan mendapatkan data yang dibutuhkan untuk keperluan analisis selanjutnya. Dengan mengumpulkan data dari sumber yang sah dan valid, proses forensik selanjutnya dapat dilakukan secara terstruktur dan akurat.

2. *Examination*

Setelah data terkumpul, tahap selanjutnya dalam proses forensik adalah pemeriksaan data. Tahap ini meliputi penilaian dan mengekstrak potongan informasi yang relevan dari data yang telah dikumpulkan. Data yang dikumpulkan berupa foto tangkapan layar percakapan dengan pelaku. Data ini kemudian akan dibandingkan dan dibuktikan keasliannya menggunakan alat FTK *imager*.

3. *Analysis*

Setelah informasi yang relevan telah diekstraksi, penulis akan mempelajari dan menganalisis data untuk ditarik kesimpulan darinya, upaya ini akan mencakup menghubungkan data Antara beberapa sumber yang sudah disebutkan sebelumnya.

4. *Reporting*

Tahap terakhir dalam proses forensik adalah pelaporan. Pada tahap ini, informasi yang dihasilkan dari tahap analisis akan disusun dan disajikan. Penulis akan memberikan hasil analisis kepada pihak sekolah. Pelaporan ini penting untuk memberikan gambaran yang jelas dan komprehensif mengenai temuan dan kesimpulan yang diperoleh dari proses *forensic* yang telah dilakukan.

4. Implementasi dan Pembahasan

4.1. Collection

Pada tahapan ini penulis mengamankan laptop ibu A untuk diamankan data *WhatsApp Web* untuk proses selanjutnya dan meminta tangkapan layar pesan dari pelaku kepada ibu A. Tangkapan layar yang diperoleh dari korban merupakan bukti digital yang relevan untuk menunjukkan percakapan antara korban dengan pelaku. Gambar 5.1 adalah tampilan tangkapan layar beserta penjelasan singkatnya.

Tabel 1
Data Barang Bukti dari korban

No.	Jenis Barang Bukti
1.	Perangkat Laptop Korban Merk Lenovo 110
2.	Tangkapan layar percakapan dengan pelaku

Tabel 2
Data Barang Bukti dari pelaku

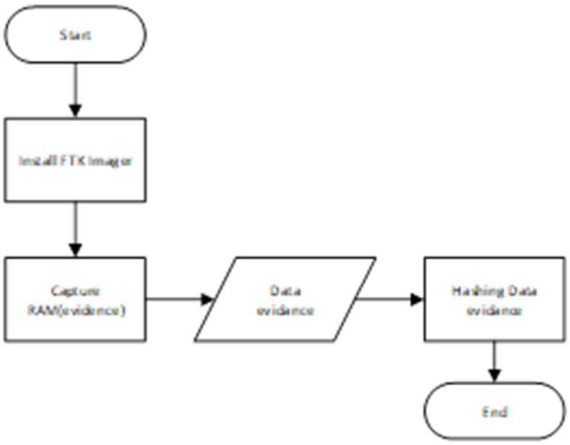
No.	Jenis Barang Bukti
1.	Foto pelaku
2.	IP Address: 202.67.41.246
3.	Lokasi: Surabaya, Indonesia, Asia
4.	Latitude: -7.2574719
5.	Longitude: 112.7520883
6.	Jenis Perangkat: Android

Dalam tahap *Collection*, penulis berhasil mengumpulkan barang bukti sementara yang terdiri dari perangkat laptop korban beserta tangkapan layar percakapan antara korban dan pelaku. Perangkat laptop korban memiliki merk Lenovo dan sebagai bukti, penulis mendapatkan tangkapan layar dari percakapan tersebut.

Selain itu, penulis juga berhasil mengumpulkan beberapa barang bukti dari sisi pelaku. Barang bukti tersebut meliputi foto pelaku, alamat IP pelaku yang digunakan saat melakukan tindakan, informasi lokasi dengan mencatat *latitude* dan *longitude*, serta jenis perangkat yang digunakan oleh pelaku dalam menjalankan aksinya.

4.2. Examination

Tahap ini meliputi penilaian dan mengekstrak potongan informasi yang relevan dari data yang telah dikumpulkan. Data yang dikumpulkan berupa foto tangkapan layar percakapan dengan pelaku. Data ini kemudian akan dibandingkan dan dibuktikan keasliannya menggunakan alat FTK *imager*. Beserta pengecekan lokasi pelaku berdasarkan *IP address* dan juga *latitude* dan *longitude* untuk memastikan keakuratan lokasi pelaku yang dihasilkan dari *link phising*.



Gbr. 2. Flow diagram mendapatkan hasil data evidence

Tabel 3
Nilai *Hash Evidence*

Nama File	MD5	SHA1	Ukuran file
memdump.mem	ba10986f331dba2bf96f6b6c68e354de	841efc57ae27924b66f7d8567d1c4fcc8a109ee7	8.573.157.376

Berdasarkan Tabel 3 nilai *hash* dari *random access memory* yang diperiksa ada tiga kategori yaitu MD5, SHA1 dan Ukuran file.

Tabel 4
Validasi FTK *Imager*

No	Pesan Tangkapan Layar	Nilai Hex Pada *Evidence*	Keterangan
1.	Perkenalkan saya Lucky Hakim	00656E616C6B616E2073617961204C75636B792048616B696D	Ada
2.	nomor rekening beserta foto bukunya	6E6F6D6F722072656B656E696E67206265736572746120666F746F2062756B756E7961	Ada
3.	Saya konfirmasikan ke sekertaris dinsos bapakMaulana ikhsan bu	73617961206B6F6E6669726D6173696B616E206B652073656B657274617269732064696E736F73206261706B4D61756C616E6120696B6873616E206275	Ada

Pada Tabel 4 Validasi FTK *Imager* menunjukkan hasil validasi dari penggunaan FTK *Imager* pada proses forensik untuk memverifikasi keaslian dan relevansi tangkapan layar yang dilakukan antara korban dan pelaku dalam kasus penipuan ini. Pada tabel ini, terdapat 3 buah tangkapan layar yang telah divalidasi menggunakan FTK Imager. Setiap baris dalam tabel menunjukkan nomor urutan tangkapan layar, nomor tangkapan layar yang mengidentifikasi gambar tersebut, pesan yang tertangkap pada layar, nilai hex pada *evidence* yang dihasilkan dari proses validasi, dan keterangan mengenai relevansi tangkapan layar tersebut.

4.3. Analysis

Berdasarkan hasil tahap Examination yang telah dilakukan sebelumnya, berikut adalah analisis dan kesimpulan:

1. Validasi menggunakan FTK Imager:
   Hasil capture RAM (*evidence*) yang diperoleh dari laptop Lenovo 110 berupa file "memdump.mem" telah berhasil diperoleh menggunakan FTK Imager. Melalui proses validasi menggunakan nilai hash (MD5, SHA1, dan ukuran file), dapat disimpulkan bahwa file "memdump.mem" tidak mengalami perubahan atau modifikasi.
2. Validasi tangkapan layar:
   Tangkapan layar yang diperoleh dari percakapan antara korban dan pelaku telah divalidasi menggunakan FTK Imager. Dalam Tabel 5.4, Tabel 5.5, dan Tabel 5.6, setiap tangkapan layar telah diberikan nomor urutan, nomor identifikasi gambar, pesan yang tertangkap pada layar, nilai hex pada *evidence*, dan keterangan mengenai relevansi tangkapan layar. Berdasarkan hasil validasi, dapat disimpulkan bahwa pesan-pesan dalam tangkapan layar tersebut terkait dengan kasus penipuan yang sedang diselidiki.
3. Pengecekan lokasi pelaku:
   Dengan menggunakan *latitude* dan *longitude* yang diperoleh dari *link phising*, lokasi pelaku telah dapat ditentukan melalui penggunaan maps.ie. Selain itu, melalui pengecekan *IP address* pada ipsaya.com, informasi tentang lokasi, jenis *provider*, dan informasi lainnya terkait IP tersebut juga diperoleh. Analisis ini membantu dalam mengidentifikasi lokasi dan informasi terkait pelaku penipuan.
4. Pengecekan foto pelaku:
   Dengan menggunakan foto yang digunakan dari hasil sebelumnya diketahui bahwa pelaku bukanlah saudara LH karena wajahnya jauh berbeda.

4.4. Reporting

Setelah melalui tahap *Collection*, *Examination*, dan *Analysis*, penelitian ini berhasil mengumpulkan sejumlah barang bukti yang berkaitan dengan kasus penipuan transfer yang mencatut nama wakil bupati di SMP Ar-rohman. Barang bukti ini menjadi landasan penting dalam mengungkap kejahatan yang dilakukan oleh pelaku secara ilegal. Dalam laporan ini, akan disajikan hasil dan temuan dari barang bukti yang berhasil dikumpulkan.

Tabel 5
(a) Data Barang Bukti dari korban

No	Jenis Barang Bukti	Didapatkan	Nomor Register
1.	Perangkat Laptop Korban Merk Lenovo 110	Ya	S/N: PF0G8UYK
2.	Tangkapan layar percakapan dengan pelaku gambar 5.1	Ya	1a4f78f4a443f44213410a6935b70784ec8b1d62

e-ISSN: 2798-9593
p-ISSN: 2798-9836

3	Tangkapan layar percakapan dengan pelaku gambar 5.2	Ya	dba66304ab1d336811dd509a7c452f419b30f881
4	Tangkapan layar percakapan dengan pelaku gambar 5.3	Ya	c1603ce36d268693215cd7ff06d6e41b30df120a
5	Tangkapan layar percakapan dengan pelaku gambar 5.4	Ya	0ad028062010a650094f8d907c212d1c47dda8eb
6	Tangkapan layar percakapan dengan pelaku gambar 5.5	Ya	1b7bdf66fa4c69e826ce5685b29449ac5a412f69
7	Tangkapan layar percakapan dengan pelaku gambar 5.6	Ya	7395782e57f2dd9eaddb100481f0e98710577e3d
8	Tangkapan layar percakapan dengan pelaku gambar 5.7	Ya	76b69cc89513e1f89c667bb5380fb6641268cb4e

Tabel 5
(a) Data Barang Bukti dari korban

No.	Jenis Barang Bukti	Didapatkan	Nomor Register
1.	Tangkapan layar percakapan dengan pelaku gambar 5.8	Ya	ffb0d9778d82e28dc1abb1cce1b5f89131c9c279
2.	Tangkapan layar percakapan dengan pelaku gambar 5.9	Ya	1cf73857260cae95f9151a5902bbc99342fffc2a
3	Tangkapan layar percakapan dengan pelaku gambar 5.10	Ya	d82bb947efada3ba170aa857256316107a07a92d
4	Tangkapan layar percakapan dengan pelaku gambar 5.11	Ya	e385a0ff59d923a7d1752e502409132b905298fc
5	Tangkapan layar percakapan dengan pelaku gambar 5.12	Ya	156148593365c478ad246dae7ad4e7fe6be49804
6	Tangkapan layar percakapan dengan pelaku gambar 5.13	Ya	2c9e46a0052992ebc22969f64aa7aba539fbb5b7
7	Tangkapan layar percakapan dengan pelaku gambar 5.17	Ya	9212113e8346349d21f199c95adf07bd827ab38f
8	File Hasil imaging percakapan dengan pelaku	Ya	841efc57ae27924b66f7d8567d1c4fcc8a109ee7

Selama proses analisis, juga ditemukan informasi penting mengenai lokasi pelaku berdasarkan data latitude dan longitude. Melalui penggunaan maps.ie dan pengecekan *IP address*, dapat diidentifikasi area atau daerah di mana pelaku mungkin berada. Informasi ini dapat menjadi petunjuk berharga dalam penyelidikan lebih lanjut dan memudahkan penangkapan pelaku. Selain itu, upaya menjaga integritas dan keaslian barang bukti sangat penting dalam penelitian ini. Oleh karena itu dilakukan validasi menggunakan alat bantu FTK *Imager* dan pengujian nilai *hash* untuk memastikan bahwa data tidak mengalami perubahan atau manipulasi yang tidak sah. Dengan memiliki sejumlah barang bukti yang valid, penelitian ini memberikan diharapkan kontribusi dalam mengungkap kasus penipuan transfer yang melibatkan pencatutan nama wakil bupati di SMP Ar-rohman. Barang bukti yang berhasil dikumpulkan ini dapat menjadi dasar yang kuat untuk proses penegakan hukum dan memberikan keadilan kepada korban.

5. Kesimpulan

Berdasarkan analisis forensik data yang dilakukan dalam penelitian ini terkait kasus penipuan salah transfer yang mencatut nama wakil bupati di SMP Ar-rohman, diperoleh sejumlah kesimpulan berikut.

1. Penerapan Metode Analisis Forensik Data Berbasis Standar NIST telah berhasil digunakan dalam kasus penipuan salah transfer yang mencatut nama Wakil Bupati pada SMP Arrohman.
2. Jenis data digital dalam mengungkap kasus penipuan salah transfer telah diidentifikasi melalui penerapan Metode Analisis Forensik Data Berbasis Standar NIST yaitu Foto pelaku, *IP Address*: 202.67.41.246, Lokasi: Surabaya, Indonesia, Asia, *Latitude* -7.2574719, *Longitude*: 112.7520883, Jenis Perangkat Android.
3. Melalui penelitian ini, teknik analisis forensik data (*live forensic* dan *phising*) berbasis Standar NIST telah dipelajari dan berhasil diterapkan dalam kasus penipuan salah transfer yang mencatut nama Wakil Bupati pada SMP Ar-rohman.
4. Efektivitas Metode Analisis Forensik Data Berbasis Standar NIST telah terbukti dalam pengungkapan dan pengumpulan barang bukti kasus penipuan transfer, dan rekomendasi diberikan untuk pembuktian lebih lanjut pada kasus ini. Metode ini memiliki potensi untuk menjadi alat yang efektif dalam penyelidikan kasus-kasus serupa di masa mendatang.

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Hasil penelitian ini menunjukkan bahwa penipuan transfer dengan mencatut nama pejabat publik merupakan ancaman serius yang dapat merugikan korban secara finansial dan merusak reputasi pejabat yang dicatut namanya. Dalam kasus ini, tangkapan layar percakapan antara korban dan pelaku menjadi bukti yang kuat mengenai komunikasi terkait penipuan transfer dan penggunaan nama wakil bupati secara ilegal.

6. Saran

Berdasarkan hasil penelitian ini, terdapat beberapa saran dan rekomendasi yang dapat diajukan:

1. Penelitian lebih lanjut: Kasus penipuan transfer dengan modus pencatutan nama pejabat publik masih memerlukan penelitian yang lebih mendalam. Penelitian lebih lanjut dapat memfokuskan pada analisis faktor-faktor yang mempengaruhi keberhasilan penipuan semacam ini, strategi pelaku, dan upaya pencegahan yang lebih efektif.
2. Penggunaan Metode lain: peneliti menyadari masih ada beberapa kekurangan terkait metode NIST ini, dengan kekurangan ini diharapkan penelitian selanjutnya bisa menggunakan metode seperti NIJ (*National isntitue of justice*) atau yang terbaru dan lebih baik lagi yang mungkin belum ada/belum ditemukan saat ini.
3. Penggunaan alat/*tools*: dari berbagai alat yang digunakan peneliti bisa mendapatkan hasil yang cukup maksimal dan menyadari keterbatasan peneliti dalam penggunaan alat lain yang lebih modern diharapkan penelitian selanjutnya bisa memilih alat yang lebih canggih dan terbaru dibandingkan alat yang sudah dipakai penulis saat ini.

Dengan penerapan saran dan rekomendasi ini, diharapkan dapat meningkatkan penelitian lanjutan yang lebih baik lagi.

Ucapan Terima Kasih

Segala puji dan syukur penyusun panjatkan kehadirat Tuhan Yang Maha Esa karena atas segala karunia-Nya penyusun dapat menyelesaikan Skripsi Sistem Informasi yang berjudul "Implementasi Metode Standar NIST Dalam Analisis Data Forensik Studi Kasus Penipuan Salah Transfer Mencatut Nama Wabup Pada SMP Ar-rohman Krangkeng" ini dengan baik dan tepat pada waktunya.

Penyusun mengucapkan terima kasih sebanyak-banyaknya kepada Semua pihak terutama pembimbing 1 bapak marsani asfi dan pembimbing 2 bapak agus sevtiana beserta teman spesial saya di prodi sistem informasi angkatan 2019.

Referensi

[1] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," Cybersp. J. Pendidik. Teknol. Inf., vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[2] A. Z. Yahya, Dirman, D. J. Buru, and B. Sugiantoro, "Analisis Bukti Digital Pada Random Access Memory Android Menggunakan Metode Live Forensic Kasus Penjualan Senjata Illegal," Cyber Secur. dan Forensik Digit., vol. 5, no. 1, pp. 6–11, 2022, doi: 10.14421/csecurity.2022.5.1.1724.

[3] I. Riadi, A. Fadlil, and M. I. Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 1, no. 10, pp. 820–828, 2021.

[4] H. Trisnasenjaya, "Forensic Analysis of Android-based WhatsApp Messenger Against Fraud Crime Using The National Institute of Standard and Technology Framework," Int. J. Cyber-Security Digit. Forensics, vol. 8, no. 1, pp. 89–97, 2019, doi: 10.17781/p002567.

[5] F. Paligu and C. Varol, "Browser Forensic Investigations of Instagram Utilizing IndexedDB Persistent Storage," Futur. Internet, vol. 14, no. 6, 2022, doi: 10.3390/fi14060188.

[6] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," Natl. Inst. Stand. Technol., 2019.

[7] J. Kizza and F. Migga Kizza, Digital Evidence and Computer Crime. 2019. doi: 10.4018/978-1-59904-379-1.ch015.

[8] R. Umar and Sahiruddin, "Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android," Pros. SENDU_U_2019, pp. 978–979, 2019.

[9] S. Raghavan, "Digital forensic research: current state of the art," CSI Trans. ICT, vol. 1, no. 1, pp. 91–114, 2019, doi: 10.1007/s40012-012-0008-7.

[10] S. RACHMIE, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," Litigasi, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[11] B. Rahardjo, "Digital Forensics at a Glance," Sociotechnology, vol. 29, pp. 384–387, 2019.

[12] S. Al Musayyab, "Forensik Digital Deteksi Pemalsuan Copy-Move Citra Dengan Menggunakan Metode Block Matching," 2018, [Online]. Available: https://repository.its.ac.id/75892/

[13] P. Studi, M. Teknik, I. Universitas, I. Indonesia, and K. Sleman, "ANALISIS NETWORK FORENSICS MENGGUNAKAN HONEYPOT Winda Andrini Wulandari," Anal. Netw. Forensics, pp. 18–25.

[14] J. Kävrestad, Fundamentals of Digital Forensics. 2020. doi: 10.1007/978-3-030-38954-3.

[15] DPR RI, "UU 11 tahun 2008 tentang Informasi dan Transaksi Elektronik," Undang-undang, vol. 76, no. 3, pp. 61–64, 2008.

[16] M. H. Wibowo and N. Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media dalam Dunia Cyber Crime," JoEICT (Journal Educ. ICT), vol. 1, no. 1, pp. 1–5, 2019, [Online]. Available:

e-ISSN: 2798-9593
p-ISSN: 2798-9836

https://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69
[17] V. F. Putra Y, "Modus Operandi Tindak Pidana Phising Menurut UU ITE," Jurist-Diction, vol. 4, no. 6, p. 2525, 2021, doi: 10.20473/jd.v4i6.31857.
[18] L. Angioni, "Computer Forensic," Sicur. E Sci. Soc., no. 3, pp. 99–109, 2018, doi: 10.3280/siss2017-003009.