Forensic Recovery Techniques on Android Devices with the National Institute of Standards and Technology (NIST) Approach

Teknik Forensic Recovery pada Perangkat Android dengan Pendekatan National Institute of Standard and Technology (NIST)

Nadila Hamid[1], Jeki Kuswanto[2*], Dwi Nurani[3], Andriyan Dwi Putra[4], Fiyas Mahananing Puri[5], Surya Tri Atmaja Ramadhani[6]

[1,2]Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

[3]Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

[4,5]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

[6]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

E-mail: [1]nadila.hamid@students.amikom.ac.id, [*2]jeki@amikom.ac.id, [3]dwinurani@amikom.ac.id, [4]andriyan.putra@amikom.ac.id, [5]fiyas@amikom.ac.id, [6]surya@amikom.ac.id

Abstract – *In the current era of advances in information technology, WhatsApp usage in Indonesia reached 88.7% in the first quarter of 2022 according to data from Hootsuite We are Social. Even though this phenomenon has positive impacts, such as ease of communication, it has negative impacts, especially in terms of increasing cybercrime. One example of a common crime is online prostitution which is carried out via the WhatsApp application, where messages, images, logs or someone's contacts can easily change hands without being noticed by the authorities. Criminals who use WhatsApp as their medium often delete electronic evidence of the crimes they have committed, making it a challenge for law enforcement, especially in obtaining evidence of the crimes committed by the perpetrators. Therefore, this research aims to implement digital forensic techniques to extract various evidence related to online prostitution cases that utilize the WhatsApp platform. The research method involves the use of forensic tools such as Mobiledit Forensic and Oxygen Forensic SQLite Viewer, by applying the National Institute of Standards and Technology (NIST) method which is a popular method in digital forensics. The results of the research show that using the Mobiledit forensic and Oxygen Forensic SQLite tools in digging up digital evidence in online prostitution cases via the WhatsApp application can find evidence with an accuracy value of up to 100%, especially for evidence in the form of text messages, contact information, call logs, and messages in image form. With the performance produced based on the findings of this evidence, it shows that the ability of these tools to detect digital evidence on Android smartphones is expected to help law enforcement in facing the challenges of digital forensic investigations and make a positive contribution in eradicating crime in cyberspace.*

Keywords *— digital forensics, mobileedit forensics, nist, online prostitution, oxygen forensics*

Abstrak – Dalam era kemajuan teknologi informasi saat ini, penggunaan *WhatsApp* di Indonesia mencapai angka 88,7% pada kuartal pertama tahun 2022 menurut data *Hootsuite We are Social*. Meskipun fenomena ini membawa dampak positif, seperti adanya kemudahan dalam komunikasi, namun menimbulkan dampak negatif, terutama dari sisi meningkatnya kejahatan dunia maya. Salah satu contoh kejahatan yang umum terjadi adalah prostitusi *online* yang dilakukan melalui aplikasi *WhatsApp*, dimana sebuah pesan, gambar, *log*, maupun kontak seseorang dapat dengan mudah

 doi: https://doi.org/10.32503/jtecs.v4i1.4676

bertukar tangan tanpa diketahui oleh pihak yang berwajib. Pelaku kejahatan yang memanfaatkan *WhatsApp* sebagai medianya seringkali menghapus bukti elektronik atas kejahatan yang dilakukannya, menjadikannya tantangan bagi penegak hukum terutama dalam memperoleh bukti atas kejahatan yang dilakukan oleh pelaku. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan teknik *digital forensic* guna mengekstrak berbagai bukti terkait dengan kasus prostitusi *online* yang memanfaatkan platform *WhatsApp*. Metode penelitian melibatkan penggunaan alat forensik seperti *Mobiledit Forensic* dan *Oxygen Forensic SQLite Viewer*, dengan menerapkan metode *National Institute of Standard and Technology* (NIST) yang merupakan metode popular dalam forensika digital. Hasil penelitian menunjukkan bahwa penggunaan *tools Mobiledit forensic* dan *Oxygen Forensic SQLite* dalam menggali barang bukti digital pada kasus prostitusi online melalui aplikasi *Whatsapp* dapat menemukan barang bukti dengan nilai akurasi hingga 100% terutama untuk barang bukti dalam bentuk pesan teks, informasi kontak, *log* panggilan, dan pesan dalam bentuk gambar. Dengan kinerja yang dihasilkan berdasarkan temuan barang bukti tersebut, menunjukkan bahwa kemampuan alat-alat tersebut dalam mendeteksi bukti digital pada *smartphone Android* yang diharapkan dapat membantu penegak hukum dalam menghadapi tantangan investigasi forensik digital dan memberikan kontribusi positif dalam memberantas kejahatan di dunia maya.

Kata Kunci — forensik digital, *nist*, *mobileedit forensic*, *oxygen forensic*, prostitusi *online*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini terus meningkat, salah satu indikatornya yakni kemajuan pada *platform Instant Messaging* (IM). *Instant Messaging* merupakan salah satu *platform* media yang sangat populer digunakan untuk berinteraksi secara efisien dan nyaman [1], [2]. Menurut data *Hootsuite We Are Social* yang diambil pada bulan Februari 2022, tercatat sebanyak 88,7% pengguna di Indonesia memanfaatkan *WhatsApp Messanger* sebagai salah satu *platform* untuk berkomunikasi secara *online*, diikuti dengan *Instagram* pada dengan prosentase sebesar 84,8%, *Facebook* dengan 81,3%, dan *Twitter* dengan 58,3% [3]–[5]. Sebagai salah satu *Instant Messaging* yang populer digunakan oleh kalangan *netizen* di Indonesia, *WhatsApp* memiliki fitur yang cukup lengkap Dimana tidak hanya pesan teks yang dapat dikirimkan, melainkan dapat digunakan untuk berbagi berkas, gambar, audio dan video, kontak, dan bahkan lokasi pengguna [4]. Dengan adanya *WhatsApp* tentu semakin memudahkan seseorang dalam berkomunikasi dan berinteraksi antar pengguna tanpa adanya berbagai batasan. Sayangnya, dengan adanya kemudahan yang ditawarkan oleh *WhatsApp* sebagai *Instant Messaging*, tersimpan adanya sisi gelap berbentuk kejahatan digital. Menurut *Databooks*, dilaporkan sebanyak 8.357 kasus kejahatan digital seperti penipuan, terdapat sebanyak 3.101 kasus, pemerasan dengan 1.606 kasus, konten pornografi 333 kasus dan ada juga tentang perdagangan palsu, dan pemalsuan kredensial yang rerata nilainya diatas 94 kasus [2], [5].

Dari berbagai kasus tersebut, salah satu kejahatan digital yang juga sering terjadi akibat penyalahgunaan dari penggunaan *WhatsApp* sebagai *Instant Messaging* adalah kasus Prostitusi *Online* [6]. Masalah prostitusi tetap menjadi isu signifikan yang belum dapat diselesaikan hingga saat ini. Praktik prostitusi merupakan permasalahan sosial yang telah terus berlanjut dari generasi ke generasi, mengambil berbagai bentuk modus operandi, seperti perdagangan wanita, penjualan alkohol, dan penjualan rokok tanpa bea cukai. Semua tindakan tersebut dilakukan dengan tujuan tertentu. Melansir dari laman berita yang mencatat adanya penangkapan dua orang mucikari di Yogyakarta terkait dengan kasus prostitusi *online*. Modus operandi yang digunakan melibatkan calon pelanggan yang berkomunikasi dengan mucikari melalui aplikasi *WhatsApp*. Pelanggan membayar uang muka (DP) untuk mendapatkan akses ke link media sosial sang angel atau pekerja seks komersial (PSK) yang ditawarkan. Setelah kesepakatan tercapai, 30% dari pembayaran diberikan kepada mucikari, sementara sisanya diberikan kepada PSK. Kedua pelaku ini kemudian dijerat dengan Pasal 45 ayat (1) dan/atau Pasal 27 ayat (1) Undang-Undang 21/2007 tentang perdagangan orang, serta Pasal 30 dan Pasal 4 ayat (2) Undang-Undang 44/2008 tentang pornografi. Berita lainnya, dua oknum DJ yang berperan sebagai PSK dan mucikari ditangkap di sebuah hotel, dimana Mucikari ini menggunakan aplikasi *WhatsApp* untuk menawarkan jasa PSK kepada pelanggan. Setelah kesepakatan tercapai, PSK dikirim ke hotel yang telah ditentukan. Barang bukti yang diamankan meliputi handphone dan sejumlah uang. Para pelaku dijerat dengan Undang-Undang No. 21/2007 Pasal 2 dan Pasal 12 tentang tindak pidana perdagangan orang, serta Pasal 296 Kitab Undang-Undang Hukum Pidana (KUHP) karena merekrut,

mengirim, dan menawarkan orang dengan maksud mencari keuntungan, dengan ancaman pidana minimal 3 tahun dan maksimal 12 tahun [7]. Meskipun setiap tindakan kejahatan meninggalkan barang bukti atau jejak digital, beberapa data telah dihapus oleh para pelaku, sehingga barang bukti tersebut kurang dapat memperkuat keputusan di pengadilan. Oleh karena itu, proses investigasi kejahatan dunia maya membutuhkan pemahaman dan keahlian di bidang forensik digital untuk membantu pihak berwenang dalam mengungkap bukti kejahatan yang telah dihapus oleh pelaku kejahatan.

Forensik digital adalah metode yang dapat digunakan untuk menyelidiki dan mengevaluasi bukti digital dengan tujuan untuk mendukung pihak berwenang dalam mengungkapkan bukti kejahatan yang telah dihapus oleh pelaku kejahatan [5]. Penelitian [1] menjadi salah satu contoh implementasi forensik digital yang mengungkap bukti dari pelaku kejahatan dalam kasus perdagangan narkoba. dengan menggunakan *tools Oxygen Forensic* pada *platform Facebook Messenger*, didapatkan barang bukti berupa pesan percakapan, waktu pesan percakapan berlangsung, audio dan gambar pada saat transaksi berlangsung. penelitian serupa yang juga mengungkap barang bukti digital pada sebuah kasus penyebaran pornografi [8], dimana *framework National Institute of Justice* (NIJ) yang digunakan sebagai langkah investigasi menggunakan *tools Magnet Axiom* dan *Belkasoft Evidence Center* berhasil mengangkat barang bukti berupa gambar, video, audio, pesan percakapan, akun dan email pelaku. berbagai *tools* forensik yang digunakan dalam proses investigasi digital dalam rangka menarik barang bukti juga dibandingkan pada penelitian [7]. *tools* forensik populer seperti *MobileEdit Forensic* dan *Oxygen Forensic* dibandingkan kinerjanya terutama dalam mendapatkan bukti digital berupa profil pelaku, kontak, gambar, pesan percakapan, audio, video, database, dan log khususnya pada aplikasi *instant messenger WhatsApp* yang terpasang pada perangkat android. hasilnya, penggunaan *mobileEdit Forensik* lebih direkomendasikan karena mampu mengekstrak barang bukti dalam bentuk gambar, video, *logs* dan *database* pesan percakapan, sedangkan penggunaan *Oxygen Forensic* hanya mampu mengekstrak kontak dan pesan percakapan dalam bentuk teks.

penelitian ini akan mengimplementasikan teknik *forensik recovery* terutama pada kasus prostitusi *online* yang dilakukan melalui aplikasi *WhatsApp* yang terpasang pada perangkat Android menggunakan kerangka kerja *National Institute of Standards and Technology* (NIST). penelitian ini akan berfokus pada teknik untuk mengekstraksi barang bukti dari kasus prostitusi *online* yang diharapkan dapat mendukung penyidik dalam menggali dan mengidentifikasi barang bukti yang sah dan dapat digunakan dalam persidangan.

2. METODE PENELITIAN

2.1. Digital Forensik

Secara umum, digital forensik merupakan cabang dari ilmu komputer yang digunakan untuk mendukung kepentingan hukum. digital forensik bertujuan untuk mengekstrak barang bukti, dan membuktikan keabsahan dari barang bukti secara digital dari suatu tindak kejahatan yang memanfaatkan teknologi komputer [1], [4], [5], [8]–[10]. Proses dalam digital forensik melibatkan tahapan dalam pengumpulan data, tahapan analisis, dan tahapan pelaporan bukti digital yang bertujuan untuk memperoleh bukti yang valid dan sah terkait dengan tindak pidana dan kasus hukum. bukti digital yang diperoleh melalui digital forensik harapannya dapat digunakan sebagai bukti yang kuat di persidangan untuk menjerat pelaku dari kejahatan [8], [11].

2.2. Mobiledit Forensic

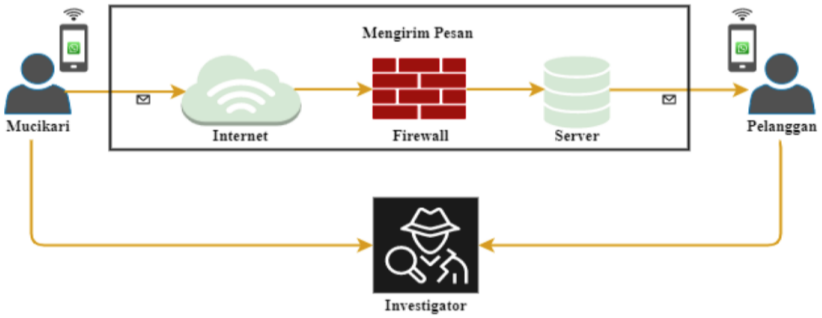
Mobiledit Forensic merupakan sebuah aplikasi atau peralatan forensik yang secara khusus digunakan dalam rangka untuk proses *forensic recovery* pada perangkat *mobile* seperti *smartphone*. *Mobiledit* merupakan perangkat lunak yang berfungsi untuk mengakses data pada *smartphone* selama proses penyelidikan. Alat ini mampu membaca berbagai jenis data yang tersimpan di dalam *smartphone* seperti pesan, *log* aktivitas, dokumen, video, gambar, dan berkas lainnya. Instalasi *Mobiledit* relatif tidak rumit dan cukup mudah dilakukan. Untuk dapat menggunakan alat ini, diperlukan koneksi *debug* dari mode USB yang diaktifkan pada *smartphone*. Koneksi antara *smartphone* dan *Mobiledit* bisa dilakukan melalui kabel langsung atau melalui koneksi nirkabel. Alat ini terhubung dengan *smartphone*

 doi: https://doi.org/10.32503/jtecs.v4i1.4676

untuk mengekstrak data, namun data yang dapat diekstrak terbatas pada teks pesan, daftar kontak, gambar, video, *log* panggilan, berkas, dan dokumen [9], [12], [13].

2.3. Skenario Kasus

Skenario kasus yang digunakan dalam penelitian ini bersifat simulasi yang mengangkat kasus kejahatan yang berkaitan dengan prostitusi *online* yang melibatkan transaksi antara penyedia jasa prostitusi (mucikari) *online* dengan calon pelanggan melalui aplikasi *WhatsApp*. Skenario yang digunakan dalam penelitian ini ditunjukkan sebagaimana Gambar 1.



Gambar 1 Skenario Kasus

Gambar 1 menunjukkan ilustrasi dari kasus kejahatan yang nantinya akan dicari buktinya melalui teknik forensik *recovery*. Ilustrasi tersebut melibatkan dua objek utama yaitu mucikari dan pelanggan yang saling berkomunikasi, serta melakukan transaksi dalam konteks prostitusi *online* melalui *WhatsApp*. Agar terhindar dari jeratan hukum, umumnya mucikari akan menghapus berbagai *log*, pesan, dan aktivitas yang memiliki jejak digital. Oleh karena itu, teknik forensic *recovery* ini akan difokuskan untuk mengakuisisi bukti-bukti yang dihapus oleh mucikari terkait dengan kejahatan prostitusi *online* yang dilakukan.

2.4. National Institute of Standards and Technology (NIST)

NIST merupakan kerangka kerja yang menjadi standar internasional khususnya dalam hal investigasi forensik. NIST memberikan panduan dalam melakukan investigasi secara benar dan dapat dipertanggungjawabkan sesuai dengan hukum yang berlaku. Guna menjaga integritas dari barang bukti, NIST memiliki alur sistematis yang ditunjukkan sebagaimana pada Gambar 2, yang dapat dijadikan acuan dalam proses forensik yang digital guna menghasilkan barang bukti yang dapat dipertanggungjawabkan [14].

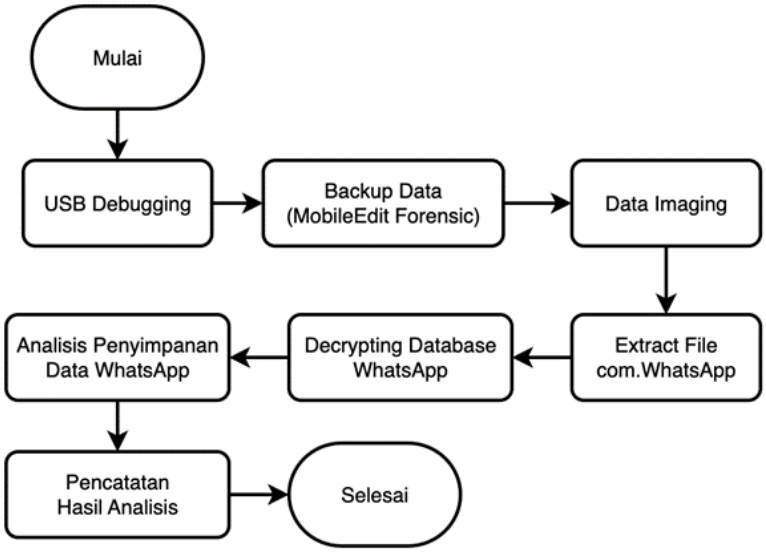
Gambar 2 Alur Kerangka Kerja NIST [14]

Berdasarkan alur sistematika yang ditunjukkan pada Gambar 2., kerangka kerja NIST akan memulai tahapannya dari proses *Collection*, dilanjutkan dengan tahapan *Examination*, lalu dilakukan tahapan *Analysis*, dan terakhir adalah tahapan *Reporting*.

2.4.1. Collection

Collection merupakan tahapan pertama dari kerangka kerja NIST. Tahapan *Collection* umumnya merujuk pada proses untuk mengidentifikasi dan mengenali sumber data yang relevan yang mungkin ditemukan, proses pelabelan data yang bertujuan untuk memudahkan pengelompokan informasi berdasarkan alat bukti, serta proses untuk pencatatan dan pengumpulan data yang relevan yang akan memperkuat alat bukti yang akan diolah yang tentunya harus mengikuti berbagai prosedur dan standar operasi yang bertujuan untuk menjaga integritas dari bukti yang akan diperoleh.

Proses pengambilan data pada tahapan *collection* akan dilakukan menggunakan *tools forensik Mobiledit Express* untuk memperoleh data yang akan dianalisis. Pada tahap ini, dilakukan duplikasi (*imaging*) untuk mengambil semua data yang ada, termasuk data yang mungkin telah mengalami kerusakan. Tindakan ini memungkinkan peneliti untuk menyelidiki data yang potensial sebagai bukti kejahatan. adapun alur yang dilakukan dalam proses akuisisi datanya ditunjukkan sebagaimana Gambar 3.



Gambar 3 Alur Proses Akuisisi Data

Gambar 3, menunjukkan alur proses pengambilan data dari pesan *WhatsApp* berdasarkan skenario penelitian. Pesan *WhatsApp* yang diakuisisi dari perangkat android ini dimulai dari proses *USB Debugging* yang bertujuan untuk menghubungkan antara perangkat *Android* dengan perangkat (laptop) yang digunakan dalam proses investigasi. Adapun gambaran dan ilustrasi dari proses *USB Debugging* ditunjukkan menggunakan Gambar 4.

Gambar 4 Ilustrasi Proses *USB Debugging*

 doi: https://doi.org/10.32503/jtecs.v4i1.4676

Setelah perangkat *Android* terhubung dengan laptop melalui proses *USB Debugging*, langkah berikutnya adalah melakukan proses *Backup Data* menggunakan *tools MobileEdit Forensics* yang ter-*install* pada laptop sang investigator. Pada tahap ini, seluruh data yang ada pada perangkat *Android* pelaku akan diakuisisi untuk kemudian dilakukan proses imaging data.

Imaging Data merupakan proses untuk membuat salinan dari data asli yang tersimpan pada perangkat *Android* tanpa menimbulkan kerusakan pada barang bukti aslinya. selain bertujuan untuk mengakuisisi seluruh data pada perangkat pelaku, proses imaging juga berperan untuk menggali dan menemukan secara mendalam data yang ada pada smartphone serta memastikan tidak ada data yang tertinggal yang mungkin dapat menunjukkan adanya bukti kejahatan.

Setelah proses *imaging data* selesai dilakukan, langkah berikutnya adalah mengekstrak artefak yang ada pada berkas *`com.whatsapp`* yang didalamnya berisi *database* dan aktivitas yang dilakukan menggunakan *Whatsapp* khusus pada perangkat *Android*. Artefak *`com.whatsapp`* yang diperoleh kemudian dilakukan proses *decrypt* agar dapat dilakukan proses analisis terutama pada media penyimpanannya guna menemukan fakta, bukti, maupun informasi terkait kejahatan prostitusi *online* yang dilakukan.

Terakhir, adalah melakukan pencatatan dari berbagai hal yang telah diperoleh untuk diproses lebih lanjut pada tahapan dalam kerangka kerja NIST pada tahapan berikutnya.

2.4.2. Examination

Examination merupakan tahapan yang dilakukan setelah tahapan *collection* dilakukan. pada tahapan *examination*, data yang telah terkumpul melalui tahapan *collection* berikutnya akan diproses secara forensik dengan memanfaatkan berbagai metode yang melibatkan berbagai skenario kasus, baik proses forensik digital yang dilakukan secara otomatis maupun proses digital forensik yang dilakukan dengan cara yang manual. Selain itu, pada tahapan *examination* ini juga dilakukan proses evaluasi terhadap data yang telah melalui metode forensik untuk meminimalisir adanya kemungkinan pelepasan data serta tetap memastikan bahwa integritas dari data tetap terjaga.

Pada penelitian ini, data yang telah diperoleh kemudian dilakukan pemeriksaan terutama dari untuk validasi dari keabsahan datanya. Proses validasi dilakukan berdasarkan data yang masih terenkripsi, untuk selanjutnya dibandingkan dengan data yang telah dilakukan proses dekripsi (*decrypt*). proses *examination* dilakukan menggunakan *Oxygen Forensic SQLite Viewer*.

2.4.3. Analysis

Tahapan *Analysis* dilakukan untuk mengevaluasi hasil dari setiap proses yang dilakukan pada tahapan examination dengan menerapkan metode yang dapat dipertanggungjawabkan secara teknis dan hukum. Hal ini bertujuan untuk memperoleh informasi yang bermanfaat yang menjawab pertanyaan-pertanyaan yang menjadi alasan dilakukannya pengumpulan dan pemeriksaan data.

Proses *examination* yang dilakukan pada tahapan sebelumnya menggunakan *tools Oxygen Forensic SQLite Viewer* memunculkan adanya informasi terkait dengan percakapan, riwayat panggilan, serta informasi kontak dari data yang telah diakuisisi. oleh karena itu, pada tahapan *analysis* ini, dilakukan pencarian serta analisis yang memastikan bahwa informasi yang diperoleh merupakan bukti-bukti yang mengarah pada tindak kejahatan yang dilakukan oleh pelaku prostitusi *online*.

2.4.4. Reporting

Tahapan *reporting* bertujuan untuk melaporkan hasil dari proses analisis yang dilakukan yang mencakup mengenai penjelasan tentang tindakan yang perlu untuk dilakukan, menjelaskan terkait dengan proses untuk pemilihan alat dan prosedur tindakannya, menentukan langkah-langkah tambahan yang perlu diambil (seperti melakukan pemeriksaan forensik terhadap sumber data ekstra, mengamankan kerentanan yang teridentifikasi, serta meningkatkan kontrol keamanan yang sudah ada), dan memberikan rekomendasi untuk meningkatkan kebijakan, prosedur, alat, dan aspek lain dari proses forensik. oleh karena itu, pada tahapan ini detail dari semua bukti yang dihasilkan dari kasus kejahatan prostitusi online seperti pesan percakapan, gambar, daftar kontak, dan catatan panggilan yang tercatat pada *smartphone Android* serta membuat kesimpulan berdasarkan temuan yang diungkap oleh penyelidik.

2.4.5. Evaluasi

Evaluasi hasil akan dilakukan dengan menggunakan perangkat forensik yang digunakan untuk menguji dan memperoleh bukti digital forensik. Proses akuisisi data menggunakan alat *Mobiledit* dan *Oxygen Forensic SQLite*. Data yang terkumpul akan disajikan dalam bentuk tabel yang menampilkan hasil pengujian forensik dari kedua alat yang digunakan untuk menganalisis sebuah *Smartphone Android*. Selanjutnya, dilakukan perhitungan indeks akurasi untuk menilai kemampuan dari masing-masing alat tersebut.

$$akurasi = \frac{\sum Fbb}{\sum bb} \quad \text{.....(1)}$$

Persamaan (1) menjelaskan bahwa *ΣFbb* merupakan total dari seluruh barang bukti yang berhasil di *recovery* dibagi dengan *Σbb* yang merupakan total seluruh barang bukti dikalikan dengan seratus (100) untuk memperoleh hasil dalam bentuk prosentase. Semakin besar nilai persentase yang dihasilkan, menunjukkan kinerja *tools* yang digunakan semakin baik dalam menemukan barang bukti dari tindak kejahatan yang dilakukan.

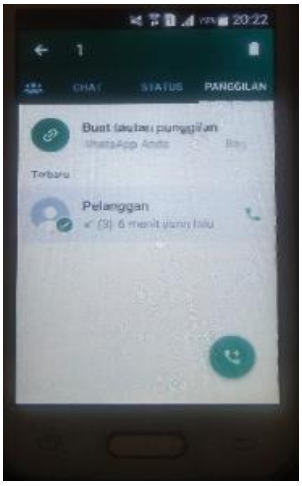
3. HASIL DAN PEMBAHASAN

Berdasarkan skenario kasus yang digunakan dalam penelitian, dimana teknik forensik *recovery* digunakan pada kasus prostitusi *online* untuk memperoleh bukti kejahatan yang telah dihapus oleh pelaku kejahatan (mucikari). Skenario kasus dalam penelitian yang melibatkan pesan percakapan antara pelanggan dengan mucikari yang didalamnya berisi informasi dan transaksi prostitusi *online*. informasi terkait dengan pekerja seks komersial yang ditawarkan kepada pelanggan dalam bentuk gambar, serta kontak yang akan menghubungkan antara pelanggan dengan PSK yang akan dipesan. berbagai pesan tersebut umumnya telah dihapus oleh pelaku (mucikari) setelah transaksi dilakukan guna menghilangkan barang bukti yang membuat pelaku terhindar dari jeratan hukum.

Gambar 5 Ilustrasi *History* Percakapan Pesan

Gambar 5 menunjukkan contoh pesan percakapan yang terjadi antara pelanggan dengan mucikari yang melakukan transaksi terkait dengan kasus prostitusi *online*.

 doi: https://doi.org/10.32503/jtecs.v4i1.4676



(a)

(b)

Gambar 6 a). *log* panggilan; b). kontak pelanggan

Gambar 6 a, merupakan skenario yang menunjukkan adanya *log* panggilan yang dilakukan antara pelanggan dengan mucikari terkait dengan transaksi dan komunikasi dalam kasus prostitusi *online*. sedangkan Gambar 6 b, menunjukkan skenario dimana kontak pelanggan disimpan oleh mucikari.

Gambar 5, Gambar 6 a, dan Gambar 6 b menjadi bukti yang dalam skenario dari penelitian ini kondisinya dihapus oleh pelaku kejahatan (mucikari) untuk menghilangkan jejak digital dan bukti dari kejahatan terkait dengan prostitusi *online*. Karena itu, digital forensik menjadi penting dalam melakukan pemulihan data pada sebuah ponsel pintar dengan memanfaatkan alat *Mobiledit Forensic Express* dan *Oxygen Forensic SQLite Viewer*, dengan mengikuti langkah-langkah metode NIST.

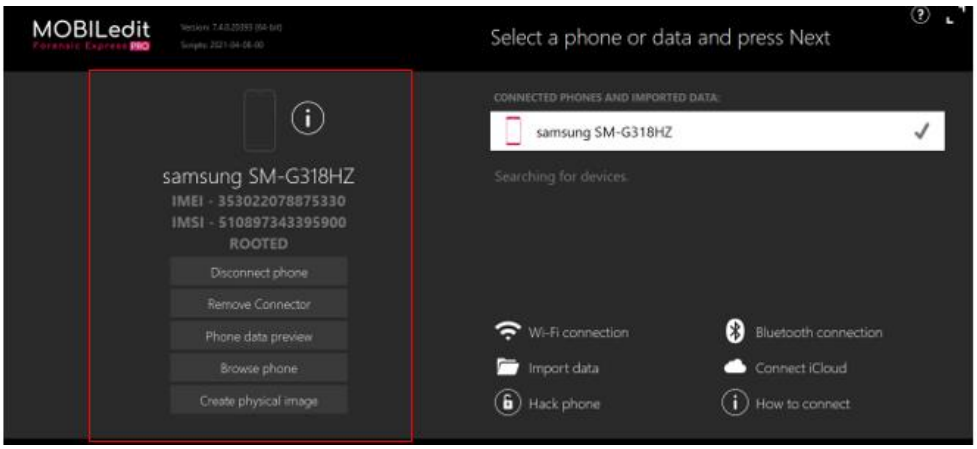
3.1. Collection

Pada tahapan *collection*, data utama yang diakuisisi menggunakan *MobileEdit Forensic Express* adalah *database WhatsApp*. *Physical imaging data* perlu dilakukan dalam tahap ini karena proses akuisisi data memiliki resiko yang tinggi terutama karena bukti digital bisa saja hilang ataupun rusak dalam proses akuisisinya. Sebelum proses akuisisi data dilakukan secara lebih lanjut, perlu adanya mekanisme dokumentasi agar integritas dari data tetap terjaga.

Tabel 1. Informasi Perangkat Barang Bukti

Informasi Perangkat *Android*	
Model	*Samsung Galaxy V*
Nomor Model	SM-G318 GHz
Versi *Android*	*Android Kitkat* V.4.4.4
Nomor IMEI	35302207887XXX
Sandi Perangkat	*No*
Memori Eksternal	*Yes*
Kartu SIM	*Yes*

Setelah memperoleh informasi terkait dengan perangkat barang bukti yang digunakan oleh pelaku, sebagaimana yang ditunjukkan melalui Tabel 1, langkah berikutnya adalah menghubungkan perangkat tersebut dengan perangkat investigator yang telah ter-*install* aplikasi *MobileEdit Forensic* untuk dilakukan akuisisi data.



Gambar 7 *MobileEdit Forensic*

Gambar 7, merupakan tampilan dari *tools MobileEdit Forensic* yang juga menampilkan informasi mengenai perangkat yang terhubung.

Gambar 8 Proses Akuisisi Data

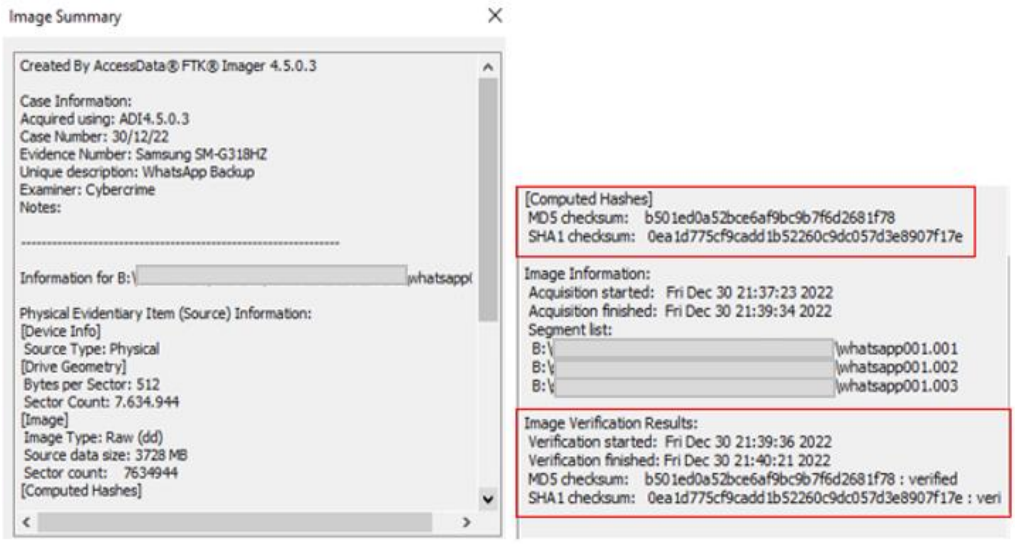
Gambar 8, merupakan tampilan proses dimana akuisi data sedang berlangsung yang akan menghasilkan *physical imaging data* yang diambil dari perangkat yang terhubung. hasil dari proses akusisi data menggunakan *tools MobileEdit Forensic* ini adalah *file* dengan ekstensi *.img*.

Name	Date modified	Type	Size
samsung SM-G318HZ.img_info	23/11/2022 17:51	WinRAR ZIP archive	3 KB
samsung SM-G318HZ_mmcblk0	23/11/2022 17:47	IMG File	3.817.472 KB
samsung SM-G318HZ_mmcblk1	23/11/2022 17:51	IMG File	994.816 KB

Gambar 9 hasil akuisisi data

Gambar 9, merupakan hasil *imaging data* yang dilakukan pada tahapan *collection*. Dimana dalam kasus ini *file imaging data* disimpan dengan nama samsung SM-G318HZ.img. Untuk memastikan dan menjaga integritas dari bukti yang diakuisisi, perlu adanya verifikasi nilai *Hash* dari data asli yang ada pada perangkat barang bukti, dengan nilai hash dari imaging data. Proses pencocokan nilai *Hash* dilakukan memanfaatkan *tools FTK Imager*, sebagaimana yang ditunjukkan pada Gambar 10.

 doi: https://doi.org/10.32503/jtecs.v4i1.4676

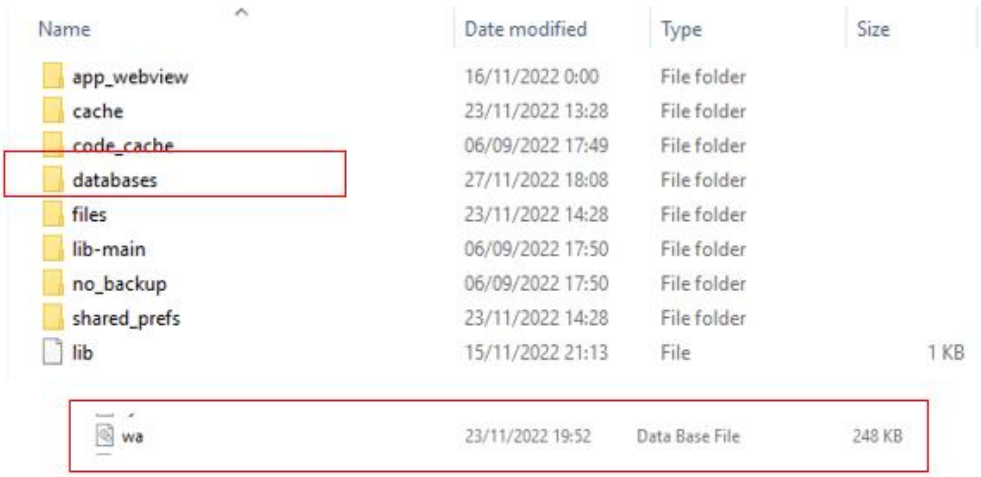


Gambar 10 Pencocokan Nilai *Hash*

Gambar 10., menunjukkan bahwa data hasil imaging memiliki nilai *hash* (*md5 checksum*) yang sama dengan data asli pada barang bukti yakni b501ed0a52bce6af9bc9b7f6d2681f78 : *verified.* sampai dengan tahap ini, integritas *imaging data* masih terjaga dan siap untuk dilanjutkan pada tahapan berikutnya.

3.2. Examination dan Analysis

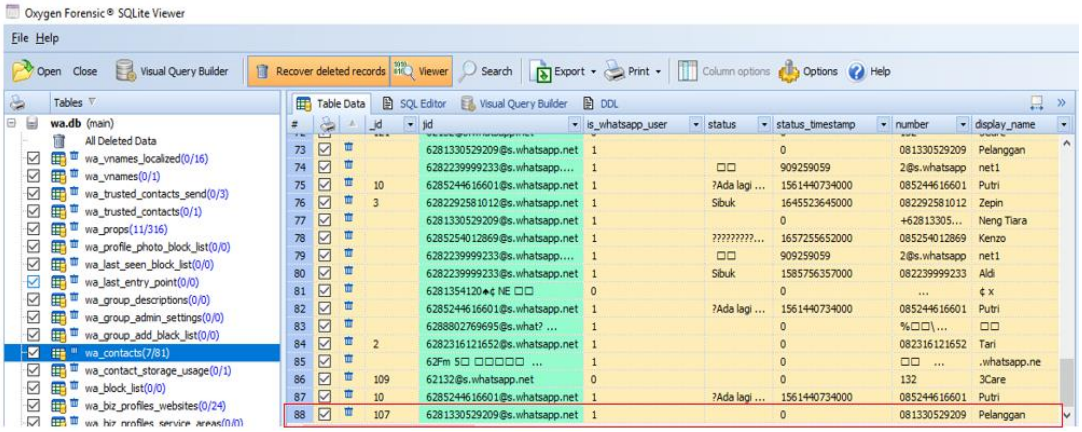
Setelah data diakuisisi pada tahapan data *collection*, langkah berikutnya adalah melakukan *data examination* dan *Analysis* untuk mendapatkan data yang berkaitan dengan kasus prostitusi *online* melalui aplikasi *WhatsApp*. Proses data *examination* dilakukan menggunakan t*ool Oxygen Forensic SQLite Viewer*. *Imaging data* yang masih berupa artefak kemudian di ekstrak terlebih dahulu untuk diambil *file database Whatsapp* dengan lokasi direktori yang ada pada ***com.whatsapp*** yang menjadi fokus penelitian dimana barang bukti akan diidentifikasi sebagaimana ditunjukkan pada Gambar 11.



Gambar 11 File *Database* Pada Direktori ***Com.Whatsapp***

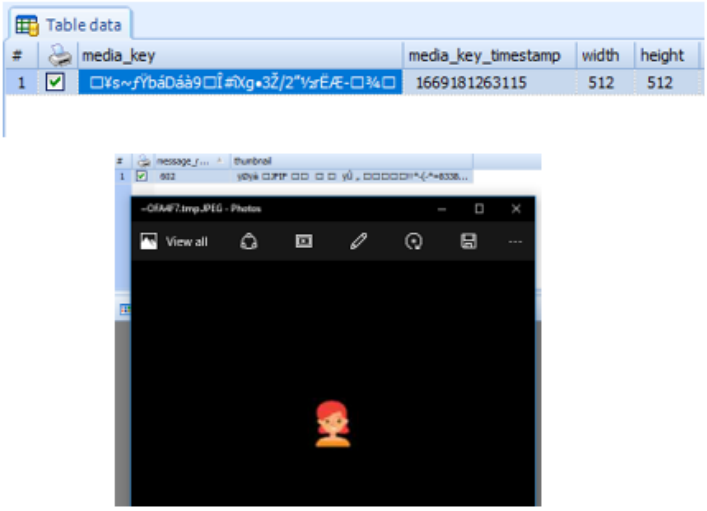
File ***wa.db*** yang ditunjukkan pada Gambar 11., merupakan *database* utama dari aplikasi *WhatsApp* yang menyimpan berbagai informasi terkait dengan aktivitas pengguna dalam menggunakan aplikasi *WhatsApp*. *File* ***wa.db*** tersebut kemudian di *import* pada *tool Oxygen Forensic SQLite Viewer*

untuk dianalisis sehingga diketahui informasi yang mengarah pada bukti-bukti kejahatan yang dilakukan.



Gambar 12 *Log* Panggilan Ditemukan

Gambar 13 Riwayat Pesan Percakapan Ditemukan



Gambar 14. ilustrasi bukti dalam bentuk *image* (ditemukan)

 doi: https://doi.org/10.32503/jtecs.v4i1.4676

Gambar 12., Gambar 13., dan Gambar 14., merupakan hasil dari penggunaan *tool Oxygen Forensic SQLite Viewer* yang berhasil digunakan untuk menemukan barang bukti dari kejahatan digital dalam kasus prostitusi *online* yang melibatkan penggunaan *WhatsApp Messenger* pada perangkat *Android*. pada Gambar 12. diketahui adanya bukti yang mengarah pada riwayat panggilan suara kepada mucikari dari pelanggan yang memuat informasi nomor kontak dari pelanggan. pada Gambar 13., ditemukan adanya riwayat pesan teks yang dilakukan antara mucikari dengan pelanggan untuk proses bertransaksi, dan Gambar 14., menunjukkan adanya pesan dalam bentuk gambar yang ditemukan dalam proses transaksi yang dilakukan.

3.3. Reporting dan Evaluasi

Pada tahapan *reporting* dan evaluasi, berbagai langkah investigasi dan penggalian barang bukti akan dicatat dan dirangkum, dievaluasi kinerjanya, untuk kemudian disajikan guna mengungkap dan menjerat pelaku kejahatan. dari proses *collection*, *examination*, dan *analysis* diperoleh rekapitulasi hasil laporan barang bukti yang ditunjukkan berdasarkan Tabel 2.

Tabel 2. Rekapitulasi Barang Bukti

Barang Bukti	Ditemukan
Pesan Teks	Ya
Informasi Kontak	Ya
Log Panggilan	Ya
Pesan Gambar	Ya

Tabel 2., menunjukkan bahwa teknik *forensic recovery* yang dilakukan berdasarkan kerangka kerja NIST dengan menggunakan *tool MobileEdit Forensic* dan *Oxygen Forensic SQLite Viewer* diketahui dapat menemukan bukti kejahatan berupa pesan teks, informasi kontak, *log* panggilan, maupun pesan gambar. Sehingga, apabila diukur kinerjanya berdasarkan skenario yang dilakukan maka kinerja dari proses tersebut menunjukkan nilai akurasi sebesar 100 % (Persamaan 2) apabila diukur berdasarkan Persamaan 1.

$$akurasi = \frac{\sum Fbb}{\sum bb} \times 100 \quad \text{.....(2)}$$

Persamaan tersebut menjadi acuan dalam mengukur kinerja dari proses forensik *recovery* yang dilakukan berdasarkan skenario penelitian. formula tersebut kemudian diberikan nilai sehingga merujuk pada persamaan 2.

$$akurasi = \frac{4}{4} \times 100 \quad \text{.....(3)}$$

dimana pada persamaan 3 nilai ΣFbb akan bernilai 4 yang menunjukkan bahwa semua kriteria barang bukti dapat ditemukan yakni bukti dalam bentuk pesan teks, bukti dalam bentuk informasi kontak, bukti *log* panggilan, dan bukti yang berupa pesan gambar. sedangkan Σbb juga bernilai 4 yang juga menunjukkan semua kriteria dari barang bukti yang menjadi parameter pengukuran kinerja. Hasil perhitungan menunjukkan bahwa kinerja yang dihasilkan mencapai nilai 100% sebagaimana lanjutan perhitungan pada persamaan 3.

$$akurasi = 1 \times 100\% = 100\% \quad \text{.....(3)}$$

4. KESIMPULAN

Teknik *forensic recovery* menggunakan pendekatan kerangka kerja dari *National Institute of Standards and Technology* (NIST) berhasil dilakukan untuk memperoleh barang bukti yang mengungkap kejahatan pada kasus prostitusi *online*. Berdasarkan skenario kasus prostitusi *online* yang melibatkan komunikasi dan transaksi yang dilakukan antara mucikari dan pelanggan melalui *platform*

instant messenger WhatsApp. Dengan menerapkan alur dan sistematika dari kerangka kerja NIST, dan didukung dengan penggunaan *tool MobileEdit Forensic* dan *Oxygen Forensic SQLite Viewer*, barang bukti yang telah dihapus oleh pelaku seperti pesan teks, gambar, informasi kontak, maupun *log* panggilan dapat ditemukan dengan nilai akurasi hingga 100% sebagaimana skenario yang dilakukan dalam penelitian. Meskipun nilai akurasi yang dihasilkan dalam penelitian ini menunjukkan kinerja yang sangat baik, namun perlu untuk dievaluasi kembali menggunakan skenario yang lebih kompleks, terutama jika bukti yang tehapus merupakan bukti dalam bentuk pesan suara (*voice note*), pesan dalam bentuk video, maupun pesan dalam bentuk dokumen. penggunaan perangkat mobile yang berbeda namun dengan kasus serupa juga perlu untuk diteliti lebih lanjut, serta pendekatan kerangka kerja forensik yang berbeda memungkinkan adanya perbedaan kinerja yang berpotensi untuk dikembangkan oleh peneliti berikutnya.

DAFTAR PUSTAKA

[1] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018.

[2] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018.

[3] S. P. F. W. Pratama, I. G. N. A. C. Putra, M. A. Hamid, C. Christian, and I. K. K. Merdana, "Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi *Online*," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 10, no. 3, p. 271, 2022.

[4] T. Ruslan, I. Riadi, and S. Sunardi, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," *J. Fasilkom*, vol. 13, no. 02, pp. 286–292, 2023.

[5] I. Riadi, H. Herman, and N. H. Siregar, "Forensik Mobile Pada Kasus Cyber Fraud Layanan Signal Messenger Menggunakan Metode NIST," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 6, no. 3, p. 137, 2021.

[6] Y. A. Fajrin and A. F. Triwijaya, "Perempuan dalam Prostitusi: Konstruksi Pelindungan Hukum Terhadap Perempuan Indonesia dari Perspektif Yuridis dan Viktimologi (Women in prostitution: Construction of Legal Protection Towards Indonesian Women from a Juridical and Victimitarian Perspective)," *Negara Huk. Membangun Huk. untuk Keadilan dan Kesejaht.*, vol. 10, no. 1, pp. 67–88, 2019.

[7] I. A. Plianda and R. Indrayani, "Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp," *J. Media Inform. Budidarma*, vol. 6, no. 1, p. 500, 2022.

[8] S. R. A. Ardiningtias, S. Sunardi, and H. Herman, "Investigasi Digital Pada Facebook Messenger Menggunakan National Institute of Justice," *J. Inform. Polinema*, vol. 7, no. 4, pp. 19–26, 2021.

[9] K. D. O. Mahendra and I. K. Ari Mogi, "Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 9, no. 3, p. 381, 2021.

[10] R. F. Aushaf, S. J. I. Ismail, and ..., "Implementasi Forensik Digital Di Telegram Pada Sistem Operasi," *eProceedings …*, vol. 7, no. 6, pp. 2767–2778, 2021.

[11] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Artic. Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 155–160, 2017.

[12] H. Fayyad-Kazan, S. Kassem-Moussa, H. J. Hejase, and A. J. Hejase, "Forensic Analysis of WhatsApp SQLite Databases on the Unrooted Android Phones," *HighTech Innov. J.*, vol. 3, no. 2, pp. 175–195, 2022.

[13] N. Anggraini, S. U. Masruroh, and H. Tiaraningtias, "Analisa Forensik Whatsapp Messanger Pada Smartphone Android," *J. Ilm. FIFO*, vol. 12, no. 1, p. 83, 2020.

[14] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.