Journal of Economic and Management (JEM) Terekam Jejak, Copyright © 2025
Vol. 2, Num. 2, 2025
https://journal.terekamjejak.com/index.php/jem
Author: **Fadli Riski Mainurmasen, Zainudin Hasan**

Eksaminasi Barang Bukti Digital sebagai Pembuktian Tindak Pidana Korupsi: Studi Kasus Pengadaan Alat Kesehatan RSUD Dr. Rasidin Padang Tahun Anggaran 2013

ABSTRACT

According to Constitutional Court Decision No. 25/PUU-XIV/2016, which removed the word "dapat" (can) from Article 2 paragraph (1) and Article 3 of the Anti-Corruption Law. This removal was previously considered to eliminate the element of "potential loss," but it subsequently gave rise to a new interpretation that state losses must be "actual" or "real," not merely "potential." Article 23 paragraph (5) of the 1945 Constitution contains the mandate: "To examine the accountability for state finances, a Supreme Audit Board shall be established, the provisions of which shall be regulated by law." In its implementation, state financial losses can only be calculated once deviations indicative of criminal acts (fraud) in the management of state finances have been fulfilled. In case of proving such a Fraud, the testimony of the involved parties is often deemed insufficient because the conspiring parties will never want or intend to admit to the conspiracy they have committed. This is where the role of digital forensics becomes crucial, as almost everyone today uses electronic media, electronic communication media, and electronic data to exchange information from one party to another. However, certainly, before digital forensics is conducted, the most important step for an examiner is to perform a preliminary examination. This is to determine whether the evidence to be examined through digital forensics indeed contains the substance needed for proof in the criminal case of corruption

Keyword: *BPK RI, Fraud, Digital Forensic, Examination, State Financial Loss, Corruption*

ABSTRAK

Sesuai dengan Putusan MK No. 25/PUU-XIV/2016 yang menghapus kata "dapat" dari Pasal 2 ayat (1) dan Pasal 3 UU Tipikor, yang sebelumnya dianggap menghilangkan unsur "potensial loss" tetapi kemudian menimbulkan interpretasi baru bahwa kerugian negara harus "nyata" terjadi, bukan hanya "potensial". Sesuai pasal 23 ayat (5) UUD 1945 memuat amanat: "Untuk memeriksa tanggung jawab tentang keuangan negara diadakan suatu Badan Pemeriksa Keuangan, yang peraturannya ditetapkan dengan undang-undang" , dimana dalam pelaksanaannya kerugian keuangan negara baru dapat dihitung apabila telah terpenuhinya penyimpangan yang berindikasi tindak pidana (fraud) dalam pengelolaan keuangan negara. Dalam membuktikan fraud, keterangan para pihak tentu dirasa tidak cukup hal ini dikarenakan pihak yang bersekongkol tidak akan pernah ingin ataupun berniat untuk mengakui persekongkolan yang mereka lakukan. Disinlah peran digital forensik menjadi

sangat krusial, dimana hampir pada saat ini semua orang mempergunakan media elektronik,media komunikasi elektronik dan data elektronik untuk melakukan pertukaran informasi dari satu pihak kepada pihak lain, namun tentu sebelum digital forensik dilakukan, yang paling harus dilakukan oleh pemeriksa adalam melakukan eksaminasi awal, guna mengetahui apakah barang bukti yang nantinya akan dilakukan pemeriksaan secara forensik digital memang memiliki muatan yang dibutuhkan untuk pembuktian dalam perkara tindak pidana korupsi.

Kata Kunci: *BPK RI, Fraud, Digital Forensik, Eksaminasi, Kerugian Negara, Korupsi*

PENDAHULUAN

Tindak Pidana Korupsi sebagaimana yang dimaksud dalam pasal 2 dan pasal 3 Undang undang nomor 31 tahun 1999 tentang Pemberantasan tindak pidana korupsi dikarenakan kategori tindak pidana pada pasal 2 dan pasal 3 merupakan delik materiil dengan artian perbuatan tindak pidana tersebut telah dianggap selesai.

Dalam Pembuktian pasal 2 dan pasal 3 Undang Undang tindak pidana korupsi terdapat kesamaan unsur pasal, Dimana kedua pasal tersebut mempersyaratkan dua hal yang menjadi Poros pembuktian, yakni Telah menimbulkan Kerugian Keuangan Negara dan Perbuatan melawan hukum (pasal 2) / penyalahgunaan kewenangan,kesempatan,jabatan atau posisi (pasal 3).

Dalam hal melakukan pembuktian terhadap perbautan yang telah menimbulkan kerugian keuangan negara, pemeriksa diminta untuk melakukan pembuktian atas Fraud yang benar benar telah terjadi dalam perkara yang diselidiki, dimana fraud yang ditemukan oleh pemeriksa tersebut merupakan dasar agar dapat atau tidaknya perkara tersebut disebut sebagai perkara korupsi yang telah menimbulkan kerugian keuangan negara.

Selama pembuktian atas Fraud ini, pemeriksa diharapkan untuk dapat menemukan Fraud apakah yang terjadi dalam perkara yang diselidiki dan apakah dampak nyata yang ditimbulkan atas fraud tersebut. Atas hal tersebut pemeriksa kerap mempergunakan serangkaian Tindakan penyelidikan baik dengan melakukan pemeriksaan dokumen dalam bentuk cetakan atau melakukan pemeriksaan atas dokumen elektronik, hal ini sesuai dengan perkembangan

zaman yang terjadi Dimana pada saat ini, semua orang mempergunakan Android, IOS, email dan Media elektronik lainnya untuk bertukar informasi.

Dalam melakukan analisis guna menemukan Suatu Fraud, pemeriksa diminta dan diharuskan untuk dapat melakukan analisis secara forensic baik secara Forensic Konvensional ataupun Forensik secara Digital. Forensik konvensional adalah penerapan prinsip-prinsip ilmu pengetahuan alam untuk menganalisis barang bukti fisik yang ditemukan di tempat kejadian perkara (TKP) guna membantu proses penyelidikan dan peradilan pidana (Saferstein,2011). Sedangkan Forensik Digital adalah penggunaan teknik investigasi khusus untuk mengidentifikasi, menyimpan, menganalisis, dan menyajikan data komputer yang telah diproses secara elektronik sebagai barang bukti dalam proses hukum (Kruse dan Heiser,2002).

Dalam era digitalisasi yang berkembang pesat, transformasi teknologi telah mengubah persepsi analisis fraud secara signifikan, tingginya tendensi pelaksanaan komunikasi antara para pihak terkait melalui media elektronik menyebabkan dibutuhkannya analisis fraud secara forensic untuk dilakukan guna menganalisis fraud yang terjadi pada suatu kasus.

Hal ini terlihat dari meningkatnya nilai pengungkapan perkara tindak pidana korupsi pada Unit III/Tipidkor Sat Reskrim Polresta Padang atas perkara tindak pidana korupsi yang terjadi di wilayah hukum Polresta Padang. Berdasarkan Latar belakang yang telah diuraikan, maka permasalahan yang akan dibahas yaitu “Bagaimana cara melakukan Eksaminasi terhadap Barang Bukti Digital untuk pembuktian tindak pidana korupsi”.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif melaluii pendekatan studi yuridis normatif dan studi kepustakaaan dengn berbagai macam literatur berupa buku, jurnal, dan berbagai literatur penunjang hukum

yang lainnya. Oleh karena itu, untuk menggali, mengungkapkan, mengembangkan, serta menguji kebenaran suatu konsep, teori, dan gagasan, diperlukan penelitian mendalam terhadap buku, jurnal, atau literatur yang menjadi fokus kajian

Dengan tujuan agar pembaca dapat memahami Eksamniasi terhadap barang bukti digital untuk pembuktian suatu tindak pidana korupsi, hal ini ditujukan agar seluruh pihak dan elemen Masyarakat dapat secara pro-aktif melakukan deteksi terhadap dugaan tindak pidana korupsi dengan memahami proses eksaminasi terhadap Barang Bukti Elektronik baik dari sumber tertutup (Closed-Source) ataupun sumber terbuka (Open-Source).

HASIL DAN PEMBAHASAN

Pengenalan Tahapan Eksamniasi Bukti Digital

Dalam Proses Eksaminasi Bukti Digital terdapat 2 (dua) unsur yang tidak dapat dipisahkan dan saling berkaitan antara satu dengan lainnya yakni Akuisisi (Pengambilan) dan Analisis (Analisa). Kedua unsur tersebut diharuskan saling memiliki keterkaitan antara satu sama lain, dimana keberhasilan eksaminasi atas barang bukti elektronik sangat bergantung kepada keberhasilan pelaksanaan kedua unsur tersebut, sering sekali terjadi beberapa pihak terlalu acuh untuk memahami konsep dasar pelaksanaan dari kedua unsur tersebut dimana hal tadi menimbulkan terjadinya kegagalan dalam akuisisi dan analisis dari barang bukti elektronik yang ingin di eksaminasi sehingga barang bukti elektronik tersebut menjadi rusak dan tidak dapat dipergunakan untuk pembuktian perkara tindak pidana korupsi.

a. Akuisisi

Akuisisi adalah proses membuat salinan bit-per-bit (bit-stream image) dari media penyimpanan digital untuk memastikan bukti asli tetap utuh dan tidak berubah selama proses investigasi (Nelson, B., Phillips, A., & Steuart, C. (2020). Guide to Computer Forensics and Investigations (6th ed.). Cengage Learning.) Selanjutnya, akuisisi merupakan tahap penting dalam penyelidikan forensik digital yang bertujuan untuk mengumpulkan data digital secara menyeluruh dan autentik dari berbagai sumber tanpa mengubah bukti aslinya (Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.). Artinya, dalam hal ini, akuisisi Adalah proses perolehan barang bukti elektronik , dimana dalam tahapan akuisisi ini diwajibkan agar seluruh eksaminer untuk dapat melakukan dokumentasi terhadap proses akuisisi dan melakukan akuisisi secara utuh.

Dalam Pelaksanaan Akuisisi terhadap Perangkat Email, dapat pemeriksa dapat melakukan akuisisi dengan mempergunakan alat berbayar (mis.OXYGEN SUITE,MSAB XRY, MAGNET AXIOMM SUITE , MD -NEXT , MAIL XAMINER ,METASPIKE FORENSIC EMAIL COLLECTOR dan AID4MAIL), akan tetapi terdapat beberapa perangkat lunak berbasis Gratis atau Open-Source yang juga dapat untuk dipergunakan dalam melakukan akuisisi atas email diantaranya yang saat ini akan dikaji adalah dengan mempergunakan Freezing Internet Tool.

b. Akuisisi email dengan freezing internet tool (fit)

FIT adalah sebuah suite Python modular untuk forensic acquisition of online contents dapat mem-spawn browser ter-modifikasi untuk merender/dapatkan konten dinamis, merekam desktop saat akuisisi (video capture), dan menyimpan artefak hasil akuisisi. Proyeknya bersifat open-source, selain itu IT bisa digunakan untuk mengakuisisi konten email dari berbagai sumber, terutama:

1. Webmail (misalnya Gmail, Outlook.com, Yahoo Mail)
2. Server IMAP/POP3 (misalnya mail.office365.com, imap.gmail.com)
3. Mailbox file (PST/EML/MBOX) yang disimpan online.

FIT tidak membatasi hanya situs web, tapi dapat “membekukan” session browsing dan komunikasi data dari webmail yang menampilkan email, namun dengan melakukan Akuisisi saja dalam format (.mbox/.eml) tidak semerta merta menjadi FIT sebagai perangkat forensik yang dapat dipergunakan untuk secara otomatis dapat dipergunakan untuk pembuktian suatu tindak pidana, namun karena saat ini yang dibahas Adalah Eksaminasi Barang Bukti Digital (Digital Evidence Examination) maka cukup kita melakukam pembahasan dasar terkait dengan Penggunaan FIT dalam Akuisisi Email.

c. Ekstraksi dan analisis

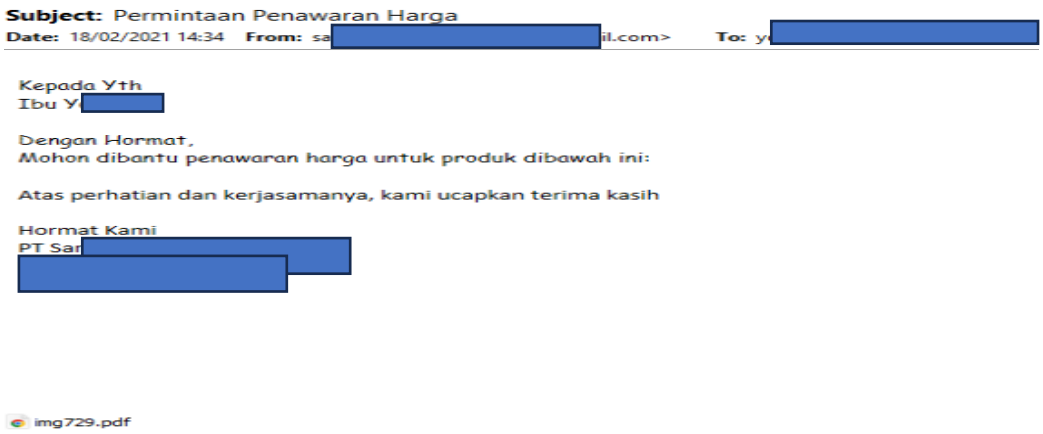
Dengan Menggunakan Freezing Internet Tool (FIT) kami mulai melakukan Extraksi atas Pesan masuk (melalui IMAP:993 dan SMTP:25,465,587) dan membuat Email terekstrak menjadi .mbox/.eml Untuk Freezing Internet Tool (FIT) dapat diunduh di : https://rb.gy/f2ltlr.

Setelah mengunduh Aplikasi tersebut, selanjutnya dapat dilanjutnya dengan mulai melakukan extract back-up dengan menggunakan 2 Metode:

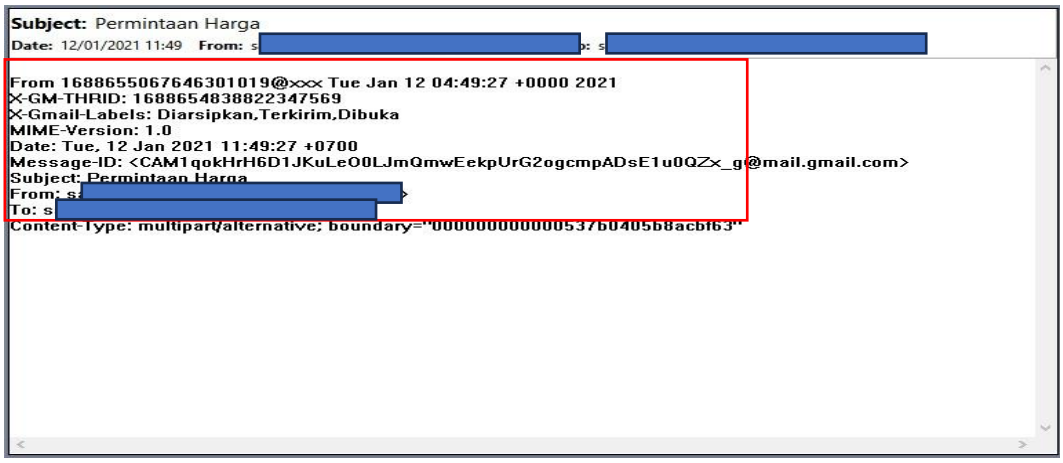
1. Input Credentials (Memasukkan password).
2. Menggunakan Sandi Aplikasi (Recommended).

Setelah Ekstrak Selesai dilaksanakan, selanjutnya pemeriksan wajib untuk melakukan analisis serderhana dari Raw Data (Data Mentah) dari email yang telah diekstrak tersebut, dengan tampilan sebagai berikut:

a. Tampilan Email (Surat Elektronik)



b. Tampilan Email Raw Data (Data Mentah Email)



Setelah berhasil melakukan ekstraksi atas email tersbeut, artinya Proses akuisisi terhadap email telah berhasil dilaksanakan, dan tahapan selanjutnya masuk kedalam tahapan analisis.

Penerapan Eksaminasi Bukti Digital Dalam Perkara

Setelah akuisisi dan ekstraksi berhasil dilaksanakan, tugas selanjutnya yang harus dilakukan adalah melakukan analisis terhadap hasil ekstraksi dari email tersebut, serta menemukan korelasi antara barang bukti elektronik yang diakuisisi dan diekstraksi dengan perkara yang sedang ditangani. Dalam hal ini, pemeriksa diharapkan memahami runtutan waktu yang terjadi dalam kegiatan pengadaan, serta larangan dan etika dalam pengadaan.

Artinya, dalam melakukan analisis atas barang bukti elektronik yang telah diakuisisi dan diekstraksi, pemeriksa diwajibkan mampu menemukan korelasi antara barang bukti yang diperiksa dengan perkara yang ditangani. Berdasarkan korelasi tersebut, pemeriksa selanjutnya diharapkan dapat menginterpretasikan hubungan tersebut sehingga mampu menemukan berbagai penyimpangan dalam perkara yang sedang ditangani.

Dalam perkara Tindak Pidana Korupsi Pengadaan Alat Kesehatan (Alkes) RSUD Dr. Rasidin Padang Tahun 2013 pada Unit III Tipidkor Polresta Padang yang dijadikan sebagai studi kasus, AIPDA ANDIKO HENDROVIKO selaku Panit

I Unit Tipidkor Sat Reskrim Polresta Padang bersama-sama dengan BRIPKA RIVANDI PERMANA PUTRA selaku Ba Unit III Sat Reskrim Polresta Padang menyampaikan bahwa dalam perkara tersebut pemeriksaan dimulai dengan melakukan identifikasi bukti elektronik atau jejak elektronik (digital footage) dari pelaksanaan unggah dokumen penawaran para calon penyedia melalui portal lpse.padang.go.id. Pada saat itu, pemeriksa menemukan adanya kesamaan IP Address (Alamat Internet Protocol) pada ketiga perusahaan yang memberikan penawaran dalam kegiatan pengadaan tersebut.

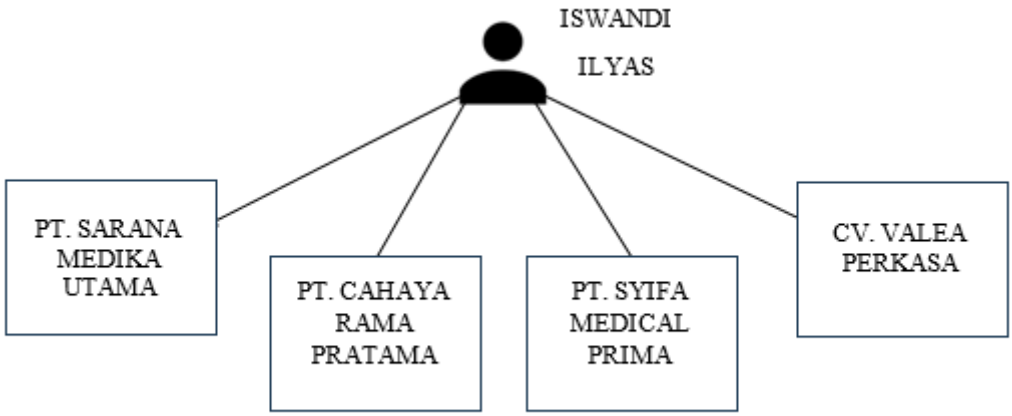
Berdasarkan analisis terhadap IP address tersebut, ditemukan fakta bahwa:

No	Perusahaan	Taggal Dan Waktu Penggunaan	IP Address
1.	Pt. Sarana Medika Utama	Tanggal 17 Juni 2013 Pk. 18 : 19 S.D. 19 : 10 WIB	36.68.57.85
2.	Pt. Cahaya Rama Pratama	Tanggal 17 Juni 2013 Pk. 21 : 06 S.D. 21 : 08 WIB	
3.	Pt. Syifa Medical Prima	Tanggal 17 Juni 2013 Pk. 23 : 19 WIB	
4.	Cv. Valea Perkasa		

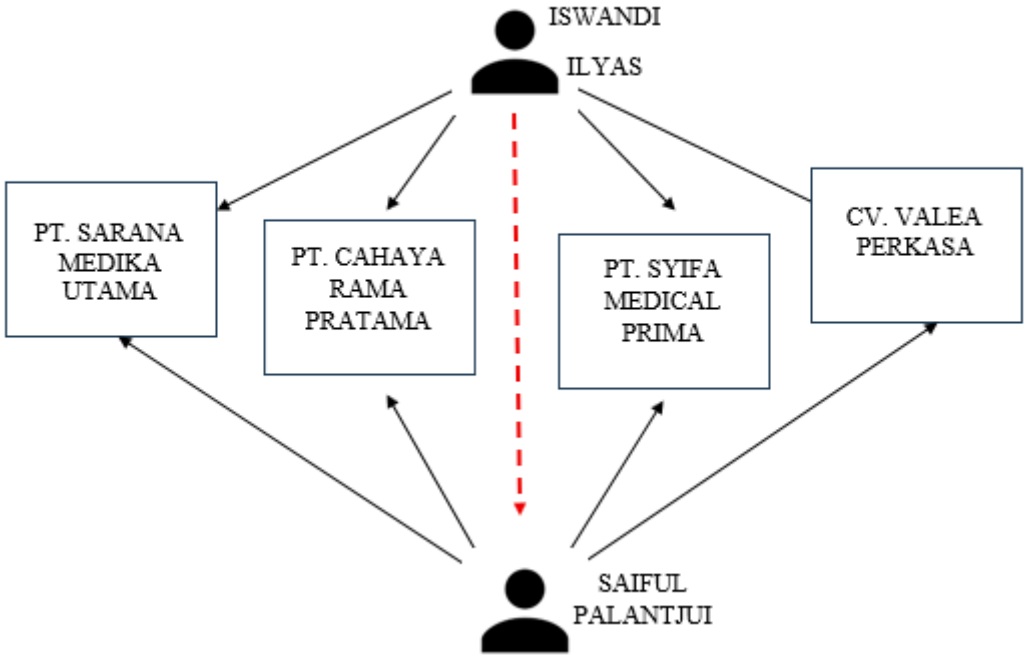
Artinya, dalam hal ini, ketika pemeriksa berhasil mengidentifikasi berdasarkan IP address yang tercatat pada Portal LPSE bahwa pengunggahan dokumen untuk keempat perusahaan tersebut dilakukan oleh satu orang yang sama, atau setidak-tidaknya melalui perangkat keras yang sama pada jaringan yang sama, maka berdasarkan temuan tersebut pemeriksa melakukan serangkaian upaya paksa dalam proses pemeriksaan, termasuk tindakan penyitaan.

Penyitaan pertama dilakukan terhadap akun email dari salah satu calon penyedia yang berada dalam satu kendali tersebut. Setelah proses akuisisi dan ekstraksi dilakukan, ditemukan bahwa terdapat satu pesan email yang berisi

dokumen penawaran teknis, termasuk penawaran harga dari para calon penyedia. Dokumen itu dikirim oleh ISWANDI ILYAS dan diterima pada akun email tersebut melalui satu IP address saja. Hal ini membuktikan bahwa penawaran dari seluruh calon penyedia dalam tender tersebut berasal dari satu orang, yaitu ISWANDI ILYAS. Jika disajikan dalam bentuk skema, maka akan terlihat sebagai berikut:



Dan selanjutnya, untuk skema dari penerima email tersebut:



Dalam hal ini, berdasarkan beberapa rilis pengiriman email yang sebelumnya telah diakuisisi dan diekstraksi atas serangkaian tindakan yang dilakukan oleh pemeriksa, ditemukan fakta bahwa para calon penyedia telah melakukan persekongkolan atau persaingan usaha tidak sehat dengan maksud dan tujuan memberikan keuntungan kepada pihak tertentu dalam tahapan pemilihan penyedia.

Hal ini tentu bertentangan dengan etika dan prinsip pengadaan yang menjunjung tinggi prinsip jujur, bersaing, dan adil. Atas temuan tersebut, pemeriksa kemudian melakukan pengumpulan keterangan lainnya dan, sesuai dengan fakta dalam persidangan, ditemukan hal-hal sebagai berikut.

Pada tanggal 1 Juni 2013, SAIFUL PALANTJUI (penuntutan terpisah) bersama rekannya, HUSEIN dan ZAKI, berangkat menuju Kota Padang untuk memasukkan dokumen penawaran. Sekitar pukul 16.57 WIB, rekan SAIFUL PALANTJUI berhasil mengunggah dokumen penawaran PT Sarana Medika Utama tanpa diketahui oleh direkturnya, yaitu ZULKARNAIN.

Karena adanya gangguan jaringan, pengunggahan dokumen penawaran untuk PT Cahaya Rama Pratama, PT Syifa Medical Prima, dan CV Valea Perkasa dilakukan oleh SAIFUL PALANTJUI (penuntutan terpisah) bersama rekannya pada tanggal 3 Juni 2013. Setelah berhasil melakukan unggah dokumen, SAIFUL PALANTJUI (penuntutan terpisah) memberitahukannya kepada ISWANDI ILYAS (DPO) dan kembali ke Jakarta untuk menemui IRHAMSYAH ILYAS LARAGA.

Bahwa dalam proses pelelangan, ISWANDI ILYAS (DPO) memerintahkan SAIFUL PALANTJUI (penuntutan terpisah) agar PT Syifa Medical Prima ditetapkan sebagai pemenang pada Pengadaan Alat Kedokteran, Kesehatan, dan KB TA 2013. Oleh karena itu, proses pelelangan tersebut telah diatur oleh SAIFUL PALANTJUI (penuntutan terpisah) dengan membuat dokumen CV Valea Perkasa tidak memenuhi syarat pada saat evaluasi teknis, sedangkan harga penawaran PT Cahaya Rama Pratama dibuat lebih tinggi daripada PT Syifa Medical Prima (Putusan Nomor 15/TIPIKOR/2020/PT PDG).

Pada tahun 2020, perkara tersebut dinyatakan inkracht, dan para terdakwa—baik dalam proses pemeriksaan maupun persidangan—menjalani hukuman sesuai putusan. Artinya, dalam hal ini, eksaminasi barang bukti digital yang dilakukan tidak hanya membantu pemeriksa dalam mencari dokumen yang dibutuhkan dalam rangka penyidikan tindak pidana korupsi, tetapi juga memungkinkan pemetaan komunikasi serta hubungan sosial antara pengirim dan penerima email tersebut. Hal ini menjadi poin yang krusial mengingat saat ini diperlukan pembuktian secara eksplisit mengenai persekongkolan, baik vertikal maupun horizontal, untuk membuktikan tindak pidana korupsi yang terjadi.

KESIMPULAN

Sesuai Pasal 183 KUHAP, hakim tidak boleh menjatuhkan pidana kepada seorang terdakwa kecuali apabila, dengan sekurang-kurangnya dua alat bukti yang sah, ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Selanjutnya, Pasal 184 ayat (1) KUHAP menyatakan bahwa alat bukti yang sah meliputi keterangan saksi, keterangan ahli, surat, petunjuk, serta keterangan terdakwa. Identifikasi terhadap barang bukti elektronik pada dasarnya termasuk dalam kategori petunjuk. Namun, apabila barang bukti elektronik tersebut diperiksa melalui proses forensik digital sehingga menghasilkan Laporan Hasil Pemeriksaan Digital Forensik, maka pemeriksa memperoleh dua alat bukti tambahan, yakni alat bukti surat berupa laporan forensik dan alat bukti keterangan ahli dari pemeriksa digital forensik. Dengan demikian, barang bukti elektronik tidak hanya mempermudah proses pencarian alat bukti untuk membuat terang suatu tindak pidana atau fraud yang terjadi, tetapi juga memperkuat nilai pembuktiannya.

Sementara itu, eksaminasi barang bukti digital—dalam hal ini email sebagai media komunikasi—berperan sebagai tindakan awal dalam mengidentifikasi penyimpangan yang terjadi.

DAFTAR PUSTAKA

Badan Pemeriksa Keuangan Republik Indonesia. 2020. Standar Pemeriksaan Keuangan Negara (SPKN). Jakarta: BPK RI.

Casey, Eoghan. 2011. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Edisi Ketiga). Academic Press.

Kruse, Warren G. dan Jay G. Heiser. 2002. Computer Forensics: Incident Response Essentials. Addison-Wesley Professional.

Mahkamah Konstitusi Republik Indonesia. 2016. Putusan Mahkamah Konstitusi Nomor 25/PUU-XIV/2016. Jakarta: MK RI.

Nelson, Bill., Amelia Phillips, dan Christopher Steuart. 2020. Guide to Computer Forensics and Investigations (Edisi Keenam). Cengage Learning.

Republik Indonesia. 1945. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Republik Indonesia. 1999. Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 140.

Republik Indonesia. 2001. Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.

Saferstein, Richard. 2011. Criminalistics: An Introduction to Forensic Science (Edisi Kesepuluh). Prentice Hall.

Subroto, Agus dan Andi Santoso. 2018. Forensik Digital: Konsep dan Implementasi. Jakarta: Mitra Wacana Media.

Sutarman. 2012. Cyber Crime: Modus Operandi dan Penanggulangannya. Yogyakarta: Graha Ilmu.

Wahyudi, Andi. 2020. Analisis Forensik Digital dalam Pembuktian Tindak Pidana Korupsi. Jurnal Hukum dan Pembangunan, Vol. 50 No. 3, Hal. 453–471.

Freezing Internet Tool (FIT). 2023. Digital Forensic Acquisition Framework (Open Source Project). Diakses melalui: https://rb.gy/f2ltlr

Putusan Pengadilan Tinggi Padang. 2020. Putusan Nomor 15/TIPIKOR/2020/PT PDG.