ANALISIS DIGITAL FORENSIK APLIKASI OVO PADA ANDROID

Michelle Mawar J. Sianipar[1], Setia Juli Irzal Ismail[2], Gandeva Bayu Satrya[3]

[1,2,3] Universitas Telkom, Bandung
michellesianipar@student.telkomuniversity.ac.id[1], julismail@tass.telkomuniversity.ac.id[2], gandevabs@tass.telkomuniversity.ac.id[3]

Abstrak

Perkembangan teknologi pada era ini mengalami perkembangan yang sangat pesat dan menghasilkan dampak yang berbeda-beda. Salah satu dampak negatifnya merupakan kasus *cybercrime* yang menimbulkan banyaknya motif kejahatan terbaru. Beberapa kasus yang terkenal di antaranya, pembayaran digital (*e-money*) seperti OVO, Go-Pay, dan DANA. Penelitian ini akan membahas *cybercrime* pada OVO dengan menggunakan metode analisis digital forensik. Proses dari analisis digital forensik dengan implementasi dari *Smartphone Android* ini mendapatkan pengaruh yang dapat memulihkan, menganalisis, dan melestarikan barang bukti untuk mengungkap identitas pelaku kejahatan pada aplikasi OVO.

Kata Kunci : Digital Forensik, *NIST*, *Cybercrime*.

Abstract

The development of technology in this era is experiencing very rapid development and produces different impacts. One of the negative impacts is the case of cybercrime that gives rise to many recent criminal motives. Some of the well-known cases include digital payments (e-money) such as OVO, Go-Pay, and DANA. This study will discuss cybercrime in OVO using forensic digital analysis methods. The process of forensic digital analysis with the implementation of this Android Smartphone gained influence that can recover, analyze, and preserve evidence to uncover the identity of the perpetrators of crimes on the OVO application.

Keywords: Image Processing, Garage, Camera, Raspberry Pi

1. Pendahuluan

Pemanfaatan teknologi informasi media dan komunikasi telah mengubah sistem dan pola pembayaran dalam transaksi ekonomi ke dalam bentuk yang lebih efisien dan ekonomis. Kemajuan teknologi ini juga membawa kita ke dalam pembayaran digital yang biasa disebut *Electronic Money (e-money)* yang dimana telah banyak digunakan di beberapa negara karena dapat memberikan kemudahan dalam melakukan transaksi pembayaran. Selain itu, hal ini juga dapat mencegah inflasi. Aplikasi pembayaran digital yang skarang sedang marak di masyarakat antara lain OVO, GO-PAY, dan DANA. [1]

PT Visionet Internasional atau yang lebih dikenal sebagai OVO mencatatkan pertumbuhan transaksi dobel digit sepanjang 2019. Tahun lalu OVO mencatat pertumbuhan jumlah nilai transaksi 55%. Selain itu peningkatan jumlah pengguna aktif bulanan lebih dari 40%. Kini OVO telah hadir di 115 juta perangkat di lebih dari 363 kota. Pertumbuhan ini bisa memberi dampak baik juga dampak buruk terhadap data dari pengguna OVO. [2]

Berbicara dalam konteks cybercrime, serangan cyber di Indonesia telah terjadi sebanyak 232,4 juta kali. [3] Penjualan data pribadi di darkweb juga makin marak di kalangan penjahat cyber. Sebagai contoh, Tokopedia mengalami kebocoran data 91 juta penggunanya. [4] Hal ini menunjukkan seberapa

rentan kita terhadap serangan tersebut serta sangat berisiko bagi masyarakat pengguna aplikasi OVO.

2. Metode Penelitian

a. Digital Forensik

Digital forensik merupakan ilmu yang digunakan untuk kepentingan bukti hukum, yang dalam hal ini adalah membuktikan kejahatan komputer secara ilmiah untuk bisa didapatkan bukti digital yang valid. [5]

b. Bukti Digital

Bukti digital merupakan barang bukti yang di ekstrak ataupun di *recovery* dari barang bukti elektronik. Jenis barang bukti ini yang harus dicari oleh analis forensik yang kemudian akan diteliti keterkaitan barang bukti tersebut dengan kasus kejahatan [6]

c. Smartphone

Smartphone adalah telepon internet-*enabled* yang biasanya menyediakan fungsi *Personal Digital Assistant* (PDA) seperti fungsi kalender, buku agenda, buku alamat, kalkulator dan catatan. [7]

d. OVO

OVO merupakan salah satu startup dalam mobile payment. Di bawah naungan LippoX sebagai perusahaan digital payment milik grup perusahaan Lippo, sebuah *smart financial apps* diluncurkan bernama OVO, aplikasi ini mencoba mengakomodasi berbagai kebutuhan terkait dengan cashless dan mobile payment. [8]

e. Cybercrime

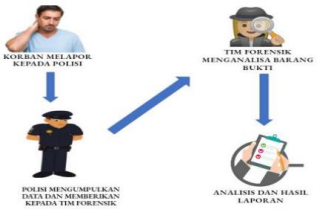
Cybercrime adalah kejahatan yang menggunakan informasi teknologi sebagai target kejahatan, dan digital forensik, pada dasarnya, menjawab pertanyaan: kapan, apa, siapa, di mana, bagaimana dan mengapa terkait dengan digital kejahatan. [9]

f. NIST SP 800-86

SP 800-86 (NIST SP800-86; NIST, 2006) membahas fase proses forensik digital: pengumpulan, pemeriksaan, analisis, dan pelaporan. Standar ini termasuk rekomendasi umum serta pedoman teknis yang lebih rinci untuk pengumpulan dan pemeriksaan bukti dari file data, sistem operasi, jaringan, aplikasi, dan sumber lainnya. [10]

3. Analisis dan Perancangan Sistem

a. Gambaran Sistem Saat Ini



Gambar diatas menjelaskan tentang cara kerja sistem yang dimana korban melapor kepada pihak kepolisian terlebih dahulu. Lalu tim kepolisian mengumpulkan data dari korban dan memberi ke tim forensik. Setelah itu, tim forensik melakukan analisa menggunakan metode statis untuk menghasilkan analisa dan laporan akhir.

b. Analisis Kebutuhan Produk

Pada pengerjaan proyek akhir ini diperlukan analisis terlebih dahulu, yaitu analisis kebutuhan perangkat lunak yang nantinya akan digunakan dalam menganalisis sampel.

c. Perancangan Sistem

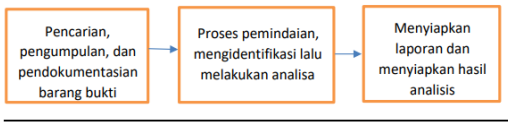


Diagram diatas menjelaskan cara kerja yang akan dilakukan selama penelitian dengan menggunakan metode NIST SP 800-86.

1. Melakukan pencarian, pengumpulan, dan dokumentasi barang bukti (Android),
2. Melakukan proses rooting atau pengkloningan perangkat mobile,
3. Melakukan proses analisa terhadap hasil acquisition,
4. Melaporkan dan menyimpulkan hasil analisis kedalam bentuk laporan

4. Hasil dan Pembahasan

4.1 Implementasi

4.1.1 Perangkat Lunak Pembangunan

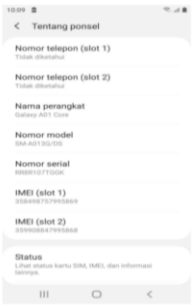
Perangkat lunak pembangunan merupakan software atau aplikasi yang digunakan untuk mendukung pembangunan kebutuhan aplikasi terhadap sistem yang dibuat, software atau aplikasi yang digunakan sebagai berikut :

1. OVO, Aplikasi yang berupa dompet digital (E-Wallet) yang digunakan sebagai pusat untuk

melakukan setiap aktivitas yang dilakukan oleh pelaku cybercrime sesuai kebutuhan sistem yang diperlukan.
2. Rooting Android, untuk memberikan akses rooting terhadap Smartphone Android.

4.1.2 Tampilan Android Menggunakan Stock ROM

Hasil tampilan Android menggunakan Stock ROM sebagai berikut :



Pada Gambar 4-1 ini merupakan Android menggunakan Stock ROM, karena untuk Samsung tidak perlu di root seperti Android yang lain. Langkah rooting Android tersebut adalah :

1. Perangkat sudah harus mode USB Debuggin.
2. Siapkan software Odin v3.13.1, ADB Fastboot Tools v1.4.2, dan CF Auto Root.
3. Buka aplikasi Odin v3.13.1 lalu perangkat masuk ke Download Mode dan disambungkan ke PC/Laptop. 15
4. Klik AP pada Odin v3.13.1, masukkan file, dan klik start.
5. Tunggu proses sampai bertulisan Pass. Maka Android sudah di rooting.
6. Periksa verifikasi root melalui Magisk.

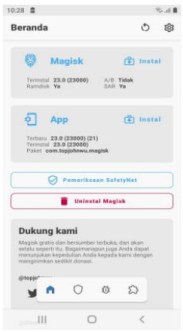
4.1.3 Perangkat Keras Pembangunan

Perangkat keras pembangun merupakan penjelasan dari perangkat keras yang digunakan untuk mendukung proses investigasi, alat yang digunakan pada sistem ini sebagai berikut:

1. Smartphone Android jenis A01 Core, sebagai barang bukti pertama yang diamankan dari pelaku cybercrime untuk memecahkan proses investigasi. Smartphone Android disini sebelumnya harus sudah di beri akses rooting.

4.1.4 Tampilan Verifikasi Android Telah Di Rooting

Hasil verifikasi Android yang telah diberi akses rooting adalah sebagai berikut :



Pada gambar 4-2 ini merupakan proses verifikasi Android telah di beri akses rooting. Proses verifikasi ini menggunakan Magisk yang tersedia di PlayStore. Setelah proses rooting selesai, langkah selanjutnya adalah melakukan tahap forensik digital terhadap keseluruhan aktivitas pelaku saat menggunakan OVO sebagai Aplikasi.

4.1.5 Analisa Berupa Tabel Aktivitas Yang Akan Dilakukan

Analisa ini dilakukan untuk menentukan apa saja aktivitas yang dilakukan oleh pelaku cybercrime di Aplikasi OVO. Berikut adalah beberapa aktivitas yang dilakukan pelaku cybercrime terhadap Aplikasi OVO tersebut.

4.2 Pengujian

Pengujian yang dilakukan hasil dari beberapa analisa yang disusun dalam setiap proses investigasi. Pada pengujian ini di buat tabel untuk menentukan path direktori yang sesuai dari aktivitas yang telah dilakukan pada Aplikasi OVO tersebut. Berikut tabel path direktori hasil pengujian dari setiap aktivitas.

4.2.1 Skenario Pengujian

Skenario yang digunakan untuk melakukan analisa terhadap barang bukti ialah, pengumpulan barang bukti dengan mencari file database dari OVO dan dilakukannya eksaminasi yakni validasi barang bukti kemudian aplikasi akan menganalisa sampel dan menampilkan data dari sampel. Setelah itu akan dilakukan pencarian menggunakan metode NIST SP 800-86 untuk menemukan perintah atau intruksi yang mencurigakan pada sampel.

4.2.2 Collection Proses

Collection atau pengamanan barang bukti elektronik dan/atau digital pada penelitian ini mengikuti standarisasi SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital. Pengamanan barang bukti elektronik dan/atau digital harus dilakukan oleh orang yang memiliki kompetensi dibidang Forensik

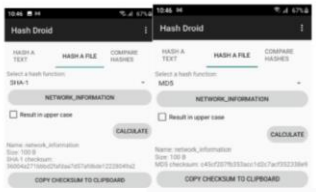
Digital (Badan Standarisasi Nasional, 2014). Barang bukti digital yang diamankan dalam bentuk berkas percakapan dalam bentuk raw data. Untuk menjaga keutuhan barang bukti digital maka barang bukti digital tersebut dilakukan kompresi dan dilakukan hashing [10]

4.2.3 Examination

Sebelum dilakukan ekstraksi dilakukan validasi barang bukti dengan mencocokan nilai hash sesuai proses collection. Barang bukti digital yang telah diamankan dilakukan ekstraksi sesuai dengan format data tanpa mengubah konten.

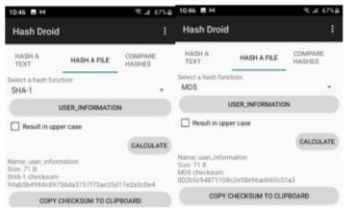
1. Hash network_information
   Berikut merupakan perbandingan hash network information melalui PC dan Smartphone menggunakan barang bukti yang di amankan.

Gambar 4- 3 Hash Network Information via PC



2. Hash User Information
   Berikut merupakan perbandingan hash user information melalui PC dan Smartphone menggunakan barang bukti yang di amankan.

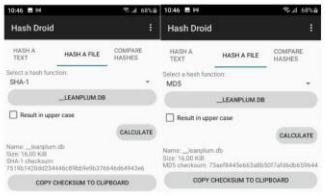
Gambar 4- 5 Hash User Information via PC



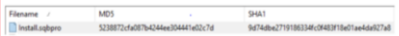
Gambar 4- 6 Hash User Information via Android

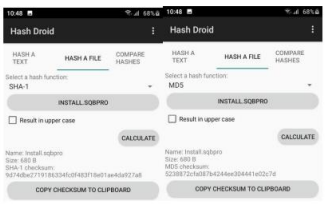
3. Hash Sign Up
   Berikut merupakan perbandingan hash login melalui PC dan Smartphone menggunakan barang bukti yang di amankan.

Gambar 4- 7 Hash Sign Up via PC



4. Hash Instalasi OVO
   Berikut merupakan perbandingan hash instalasi ovo melalui PC dan Smartphone menggunakan barang bukti yang di amankan.





5. Hash Transaksi OVO
   Berikut merupakan perbandingan hash transaksi ovo melalui PC dan Smartphone menggunakan barang bukti yang di amankan.

Gambar 4- 11 Hash Transaksi OVO via PC

4.2.4 Analysis

Proses analisis barang bukti digital berupa database dari OVO yang dianalisa menggunakan SQL DB dan Notepad. Dikarenakan beberapa file database dari OVO terbaca di Notepad tetapi tidak di SQL DB.

5. Kesimpulan

Dari hasil pengerjaan Proyek Akhir ini, dapat disimpulkan bahwa:

1. Digital forensik dapat digunakan untuk memulihkan barang bukti yang telah hilang dengan mencari artefak database pada OVO serta menganalisis barang bukti atau database yang didapat.
2. Metode NIST dapat digunakan sebagai acuan untuk menganalisa barang bukti atau

database dengan bantuan tools Notepad dan SQL DB Browser.

3. Hash merupakan sebuah fungsi algoritma matematika yang digunakan untuk menghasilkan nilai-nilai dan memberi identitas file, dan nilai algoritma yang dihasilkan akan berbeda-beda dan unik. Contohnya merupakan MD5 dan SHA-1. Algoritma hash MD5 menghasilkan nilai hash 128 bit, dan SHA-1 menghasilkan nilai hash 160 bit. Keakurasian hash dapat diperoleh dengan melihat kode yang dihasilkan melalui bukti digital. Jika hasilnya berbeda, maka integritas dan keaslian barang bukti dipertanyakan.

Referensi

[1] Emily Borom, "Study Offers Early Look at How Internet is Changing Daily Life," 2000.
[2] Internet World Stats. (2006) Internet World Stats: sage and Population Statistics. [Online]. HYPERLINK "http://www.internetworldstats.com/top20.htm" http://www.internetworldstats.com/top20.ht[
[3]Jane Lubis, Internet User Behaviour.: McMillan Publishing, 2001.
[4]John Doe, Internet Usage Within Nations. Boston: Boston Publishing, 2000.
[5] Speerman Roberts, Information System: Now and Tomorrow. Chicago: Adventure Press, 2009.
[6]Dahlan Supardi, Sistem Kerja Perpustakaan Daerah, 15th ed. Jakarta: Gramedia, 2006.
[7]John Rokoko, Pseudo-2D Hidden Markov Model. New York: McGraw Hill, 2005.
[8] Mellers, "Choice and the relative pleasure of consequences," Psychological Bulletin, p. 5, 2000. MediaWiki.2018.
[9] "Forensic: Framework, Standar, dan Metodologi pada Digital Forensic", https://lms.onnocenter.or.id/wiki/index.php/Forensic:_Framework,_Standar,_dan_Metodologi_pada_Digital_Forensic, diakses pada 21 Agustus 2021 pukul 9.01.
[10] M. W. Indriyanto, D. Hariyadi, and M. Habibi, “Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan Nist Sp 800-86 Dan Support Vector Machine Digital Forensics Investigation and Analysis on Whatsapp Group Chats Using Nist Sp 800-86 and Support Vector Machine,” Cyber Secur. dan Forensik Digit., vol. 3, no. 2, pp. 34–38, 2020.