CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 2, November 2019, hlm. 52-56

ANALISIS BARANG BUKTI DIGITAL APLIKASI PAZIIM PADA PONSEL CERDAS ANDROID DENGAN PENDEKATAN *LOGICAL ACQUISITION*

Dedy Hariyadi [1], Hendro Wijayanto[2], Indah Daila Sari[3]

[1,3]Program Studi Teknologi Informasi Universitas Jendral Achmad Yani Yogyakarta
[2]Program Studi Teknik Informatika STMIK Sinar Nusantara Surakarta
Email: [1]dedy@unjaya.ac.id, [2]hendro@sinus.ac.id, [3]indahdaila285@gmail.com

Abstrak

Penggunaan sosial media di Indonesia mengalami peningkatan yang sangat pesat di tahun 2018 dibanding tahun sebelumnya. Hal ini menjadikan banyak sosial media buatan anak bangsa bermunculan, salah satunya *Paziim*. Bersosialisasi di internet sangat mudah terjadi kebocoran data pribadi. Ada tiga aspek yang dapat dimanfaatkan pada *online social network (OSN)* dalam pengungkapan data pribadi ke publik, yaitu kekuatan hubungan (kuat atau lemah), jenis hubungan dan karakteristik kebiasaan seseorang. Diperlukan forensik ponsel untuk menganalisis barang bukti digital pada aplikasi sosial media yang terinstall di ponsel cerdas *Android*. Indonesia melalui Badan Standarisasi Nasional (BSN) juga mengeluarkan standar terkait forensik digital. Standar yang merupakan turunan dari *ISO/IEC* mengatur tentang Teknik Keamanan - Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital. Standarisasi ini dikenal sebagai SNI ISO/IEC 27037:2014. Dari hasil analisis forensik ponsel pada aplikasi Paziim, diperoleh hasil ditemukannya username, koordinat, model perangkat, dan operator yang digunakan oleh pengguna pada *SQLite Web_Data* dan berkas *OneSignal.xml*.

Kata kunci: *forensik ponsel, paziim, logical acquisition, forensik sosial media, android debug bridge*

PAZIIM DIGITAL EVIDENCE ANALYSIS APPLICATION ON ANDROID SMARTPHONES WITH A LOGICAL ACQUISITION APPROACH

Abstract

The use of social media in Indonesia has increased very rapidly in 2018 compared to the previous year. This makes a lot of social media made by the children of the nation appear, one of which is Paziim. Socializing on the internet is very easy to leak personal data. There are three aspects that can be utilized on online social networks (OSN) in the disclosure of private data to the public, namely the strength of the relationship (strong or weak), the type of relationship and the characteristics of one's habits. Mobile forensics is needed to analyze digital evidence on social media applications installed on Android smartphones. Indonesia through the National Standardization Agency (BSN) also issued standards related to digital forensics. Standards which are derived from ISO / IEC regulate Security Techniques - Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence. This standardization is known as SNI ISO / IEC 27037: 2014. From the results of cell phone forensic analysis on the Paziim application, the results found the username, coordinates, device models, and operators used by users in SQLite Web_Data and OneSignal.xml files.

Keywords: *mobile forensic, paziim, logical acquisition, social media forensic, android debug bridge*

1. PENDAHULUAN

Hasil survei penggunaan sosial media pada kuartal kedua tahun 2018 di Indonesia cukup tinggi seperti Jakarta merupakan kota pengguna Facebook urutan kedua dengan jumlah pengguna sekitar 20.000.000. Indonesia merupakan negara pengguna Instagram urutan keempat dengan jumlah pengguna sekitar 56.000.000. Merupakan pengguna Twitter urutan keduabelas dengan jumlah pengguna sekitar 6.600.000 (HOOTSUITE, 2018). Pada akhir tahun 2018 penggunaan sosial media ada yang mengalami peningkatan seperti Facebook total pengguna sekitar 130.000.000, Twitter mengalami penurunan jumlah pengguna menjadi 6.430.000, Instagram mengalami kenaikan jumlah pengguna menjadi 62.000.000, dan LinkedIn mengalami peningkatan jumlah pengguna sekitar 12.000.000 (HOOTSUITE, 2019). Besarnya pengguna sosial media di Indonesia yang menjadi latar belakang PT. Paziim AIO Platformindo mengembangkan media sosial dengan nama Pazzim (PASA, 2019). Fitur yang diusung sosial media ini tak jauh beda dengan sosial media lainnya seperti Whatsapp.

Pada penelitian ini menggunakan obyek penelitian sosial media lokal Paziim. Tujuan dari penelitian ini adalah untuk menganalisis barang bukti digital pada aplikasi sosial media yang terinstall di ponsel cerdas Android. Secara umum ponsel cerdas Android memiliki partisi boot, system, data, recovery, dan cache (DRAKE, 2014). Penelitian sebelumnya menyatakan bahwa aplikasi yang terinstall pada ponsel cerdas Android terletak di direktori /data/data (HARIYADI & HUDA, 2015).

Bersosialisasi melalui sosial media daring atau biasa disebut *online social network (OSN)* sangat mungkin dapat terungkap informasi data pribadi. Informasi tersebut dapat digunakan oleh penjahat untuk disalahgunakan. Ada tiga aspek informasi yang dapat dimanfaatkan pada *OSN*, yaitu kekuatan hubungan (kuat atau lemah), jenis hubungan dan karakteristik kebiasaaan seseorang (UMAIR, et al., 2017). Hal ini tidak menutup kemungkinan terjadi pada *OSN* lokal seperti Paziim.

2. TINJAUAN PUSTAKA

2.1. Forensik Digital

Beberapa ahli berpendapat bahwa Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Maka menurut peneliti dari Institut Teknologi Bandung, forensik digital dapat diartikan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (RAHARDJO, 2013). Pendapat peneliti dari California State University, barang bukti digital adalah suatu informasi dari nilai pembuktian, baik yang tersimpan maupun disebarkan dalam bentuk digital (BIDGOLI, 2006). Sedangkan menurut Kamus Besar Bahasa Indonesia istilah forensik terdapat beberapa kata kunci yang perlu menjadi perhatian, yaitu penerapan fakta-fakta, masalah-masalah hukum, ilmu bedah, dan kehakiman dan peradilan. Berdasarkan pernyataan *Bidgoli* dan Kamus Besar Bahasa Indonesia maka dapat disimpulkan bahwa forensik digital adalah pengungkapan fakta-fakta dari bukti digital menggunakan metode ilmiah untuk mendukung atau menyelesaikan permasalahan yang tidak wajar seperti kriminal dalam proses penegakan aturan yang berlaku (HARIYADI, 2014). Forensik Digital sendiri memiliki sub-disiplin yang terbagi beberapa diantaranya: forensik komputer, forensik ponsel, forensik memori, forensik jaringan, forensik malware, forensik sistem operasi, forensik citra, forensik komputasi awan, dan forensik audio (DOGAN & AKBAL, 2017).

2.2. Teknik Forensik Ponsel

Berdasarkan definisi forensik digital tersebut maka aktivitas atau pun teknik pada forensik digital mengikuti suatu standar yang dikeluarkan oleh beberapa organisasi untuk menjadi acuan diantaranya *Association of Chief Police Officers (ACPO), National Institute of Standards and Technology (NIST)*, Standar Nasional Indonesia (SNI). Standar yang dikenal Pedoman ACPO merupakan hasil kerjasama asosiasi kepolisian di Britania Raya dengan perusahaan 7Safe. Pedoman ACPO juga diadopsi oleh Pusat Laboratorium Forensik Polisi Republik Indonesia yang tertuang dalam *Standar Operating Procedure (SOP)* penangangan barang bukti elektronik dan/atau bukti digital (AL_AZHAR, 2012).

Departemen Perdagangan Amerika Serikat memiliki beberapa standarisasi terkait dengan teknologi informasi diantaranya adalah standarisasi tengan forensik digital. Badan dari Departemen Perdagangan Amerika Serikat yaitu *National Institute of Standards and Technology (NIST).* Oleh sebab itu standar tersebut dikenal sebagai standar NIST. Khusus untuk forensik ponsel NIST mengeluarkan standar *NIST Special Publication* 800-101. Pada standar ini diatur level pengamanan/akuisisi barang bukti digital, yaitu 1-Ekstrasi Manual, 2-Ekstraksi Logikal, 3-Ekstrasi Fisikal, 4-Chip-Off, dan 5-Micro Read (AYERS & BROTHERS, 2014).

Indonesia melalui Badan Standarisasi Nasional (BSN) juga mengeluarkan standar terkait forensik digital. Standar yang merupakan turunan dari ISO/IEC mengatur tentang Teknik Keamanan - Pedoman Identifikasi, Pengumpulan, Akuisisi dan

Preservasi Bukti Digital. Standarisasi ini dikenal sebagai SNI ISO/IEC 27037:2014 (KURNIAWAN, 2014).

2.3. Alat Forensik Ponsel

Proses forensik pada ponsel cerdas Android menggunakan *Android Debug Bridge (ADB),* sehingga saat proses akuisisi ponsel harus diaktifkan sebagai syarat utama (FAHEEM & LE-KHAC, 2014). *ADB* merupakan bagian dari *Software Development Kit* yang disediakan oleh Google untuk mendukung pengembangan aplikasi yang berjalan pada ponsel cerdas Android. Saat komputer dan ponsel cerdas terhubung maka komputer dapat mengakses perintah shell pada ponsel, menginstall atau menghapus aplikasi, membaca file log, mentransfer berkas (SIMAO, et al., 2011).

2.4. Teknik Akuisisi Ponsel

Dalam teknik forensik ponsel dikenal beberapa teknik akuisisi ponsel, yaitu *manual acquisition, logical acquisition*, dan *physical acquisition.*

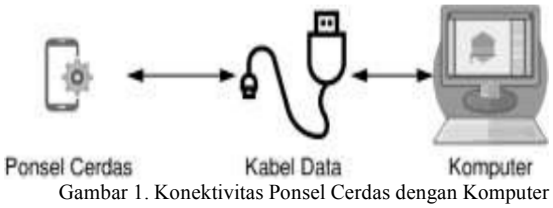
Manual acquisition adalah metodologi akuisisi yang paling mudah dimana untuk pengambilan data, investigator langsung bersentuhan dengan perangkat ponsel, membuka data lewat ponsel secara langsung untuk mengambil informasi yang dibutuhkan. Teknik ini dapat bekerja di semua jenis ponsel pintar, selama ponsel tidak dalam keadaan dikunci.

Logical acquisition adalah mengambil objek yang berada di partisi logis dari memori ponsel. Jadi, *logical acquisition* tidak mengambil data yang terletak di luar partisi logis, seperti ruang yang tidak terisi. Sebagian besar metode yang ada digunakan dalam digital forensik ponsel mengikuti pendekatan *logical acquisition*. Proses ini dilakukan dengan membuat koneksi antara ponsel komputer investigator menggunakan *Infrared, Bluetooth* atau kabel (WILLASSEN, 2005). Lalu penyelidik forensik dapat menggunakan satu set perintah AT untuk mengekstrak item bukti potensial spesifik dari ponsel. Daftar perintah AT standar untuk ponsel 3G dan sintaksnya tersedia dalam referensi ini (SAGEMCOM, 2011).

Physical acquisition adalah cara mendapatkan informasi dengan melakukan duplikat (*copy*) seluruh data dari memori chip ponsel ke memori fisik ponsel seperti SD Card dan sejenisnya. *Tools* yang sering digunakan adalah Flasher box dan Joint Test Action Group (JTAG) (ABDULLA & JONES, 2012)

3. METODOLOGI PENELITIAN

Penanganan barang bukti elektronik berupa poncel cerdas perlu tindakan yang lebih cermat saat pengambilan barang bukti digital (ACPO, 2012). Pada penelitian ini pengambilan barang bukti digital level 2 sesuai kaidah *NIST Special Publication* 800-101 yaitu ekstrasi logikal untuk menganalisis dan identifikasi barang bukti digital. Adapun konektivitasnya menggunakan kabel data yang terhubung antara komputer analis dan ponsel cerdas. Teknik ekstrasinya menggunakan ADB melalui konsol shell untuk melakukan analisis struktur direktori dari aplikasi Paziim dan transfer barang bukti digital yang pontensial ke komputer analis, seperti tampak pada Gambar 1 (HARIYADI & PASA, 2018)



Gambar 1. Konektivitas Ponsel Cerdas dengan Komputer Analis

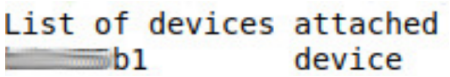
Alat dan bahan yang perlu disiapkan dalam proses analisis barang bukti digital diperlukan Komputer dengan sistem operasi Linux, Kabel Data dan Ponsel Cerdas. Adapun penjelasan alat dan bahan tersebut dapat dilihat pada Tabel 1.

Tabel 1 Alat dan Bahan Pendukung Analisis

Alat dan Bahan	Keterangan
Komputer	CPU dengan 4 Core @ 1.90GHz, RAM sebesar 8GHz, Hard Disk 500GB
Sistem Operasi	Linux
Ponsel Cerdas	Xiaomi dengan tipe Redmi Note1.
Kabel Data	Sebagai media komunikasi/transfer data komputer dan ponsel cerdas.
ADB	Software Development Kit yang telah disediakan Google.
SQLite Browser	Berfungsi untuk membaca barang bukti digital berupa berkas SQLite.

4. PEMBAHASAN

Komputer investigator yang sudah terhubung dengan ponsel cerdas dipastikan telah terinstall *Software Development Kit Android*. Selain itu dipastikan bahwa perangkat berupa ponsel cerdas telah terdeteksi dan berfungsi dengan pada komputer investigator yang bersistem operasi Linux. Perintah untuk memastikan perangkat menggunakan perintah *adb devices*, seperti pada Gambar 2.



Gambar 2. Perintah ADB Device

Penangangan barang bukti digital pada ponsel cerdas Android dengan pendekatan *Logical Acquisition* memerlukan persyaratan yaitu :

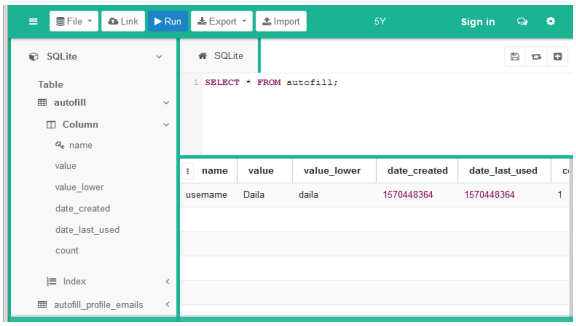
1. *USB Debugging* dalam kondisi aktif. Agar proses *logical acquisition* menggunakan perintah ADB untuk mengamankan barang bukti digital dapat berjalan.
2. Ponsel dalam kondisi *rooted*. Dimaksudkan untuk menjangkau barang bukti digital yang tertinggal di direktori */data/data/com.paziim.android*

Pada direktori tersebut terdapat beberapa sub-sub direktori pendukung aplikasi Paziim. Adapun hasil analisis barang bukti digital pada aplikasi Paziim dapat dilihat pada Tabel 2

Tabel 2 Hasil Analisis dan Temuan

Sub-sub Direktori	Temuan Barang Bukti	Keterangan
app_textures	Belum Ditemukan	Tidak ditemukan berkas.
app_xwalkcore	Ditemukan	Berkas Web_Data berformat SQLite.
cache	Belum Ditemukan	Hanya ada berkas cache.
databases	Belum Ditemukan	Berkas SQLite belum memberikan petunjuk.
files	Belum Ditemukan	Tidak ditemukan berkas.
lib	Belum Ditemukan	Berisi pustaka pendukung aplikasi.
no_backup	Tidak Ditemukan	Tidak ditemukan berkas.
shared_prefs	Ditemukan	Terdapat berkas OneSignal.xml yang menunjukan koordinat pengguna, jenis ponsel, dan operator seluler.

Barang bukti digital berupa berkas *SQLite*, yaitu *Web_Data* pada direktori *data/data/com.paziim.android/app_xwalkcore/* hanya berisi informasi username dari pengguna aplikasi Paziim. Ditunjukkan pada Gambar 3



Gambar 3. Hasil analisis SQLite Paziim

Sedangkan berkas *OneSignal.xml* pada direktori *data/data/com.paziim.android/shared_prefs* berisi tentang koordinat pengguna aplikasi Paziim yang berupa *longitude* dan *latitude*. Contoh koordinat yang terdapat pada berkas *OneSignal.xml* adalah *"long":110.3310814"* dan *"lat":-7.7933348"*. Sedangan jenis ponsel terdeteksi sebagai *"device_model":"HM NOTE 1LTE"* dan operator seluler yang digunakan adalah *"carrier":"PT Hutchison CP Telecommunications"*. Ditunjukkan pada Gambar 4

Gambar 4. Hasil Analisis berkas OneSignal.xml

Pada penelitian ini belum ditemukan barang bukti yang terkait dengan aktivitas sosial media daring yang tersimpan di dalam memori lokal ponsel pintar.

5. KESIMPULAN

Penanganan barang bukti digital dengan pendekatan logical acquisition pada aplikasi Paziim yang ditemukan adalah username, koordinat, model perangkat, dan operator yang digunakan oleh pengguna. Aktivitas sosial media daring seperti komentar, status, foto, dan jejaring belum dapat ditemukan.

Harapannya pada penelitian selanjutnya dapat ditemukan barang bukti digital dengan metode yang lebih komprehensif baik dari sisi aplikasi Paziim yang terinstall di ponsel maupun dari sisi Web Paziim

DAFTAR PUSTAKA

ABDULLA, K. & JONES, A., 2012. Forensics data acquisition methods for mobile phones. *The7th ICITST.*

ACPO, 2012. *ACPO Good Practice Guide for Digital Evidence,* United Kingdom: Association of Chief Police Officer.

AL_AZHAR, M. N., 2012. *Digital Forensic : Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek.

AYERS, R. & BROTHERS, S., 2014. *NIST Special Publication 800-101,* USA: National Institute of Standards and Technology.

BIDGOLI, H., 2006. *Handbook of Information Security. Information Warfare, Social, Legal, and International Issues and Security Foundations.* 2 penyunt. California: Wiley.

DOGAN, S. & AKBAL, E., 2017. Analysis of Mobile Phones in Digital Forensics. *40th Int. Conv. Inf. Commun. Tecjnol. Electron. Microelectron. MIPRO,* pp. 1241-1244.

DRAKE, J. J., 2014. *Android Hackers's Handbook.* 1 penyunt. United States: Wiley.

FAHEEM, M. & LE-KHAC, T. K. N.-A., 2014. Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool. *Jurnal Information Security,* 05(03), pp. 83-90.

HARIYADI, D., 2014. *https://milisdad.blogspot.com.* [Online] Available at: https://milisdad.blogspot.com/2014/05/bermain-dengan-forensik-digital.html [Diakses 26 Mey 2014].

HARIYADI, D. & HUDA, A. A., 2015. Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android. *Indonesia Security Conference ,* pp. 1-10.

HARIYADI, D. & PASA, I. Y., 2018. Identifikasi Barang Bukti Percakapan Aplikasi Dual Apps Whatsapp pada Ponsel Xiaomi Menggunakan Metode NIST Mobile Forensics. *INTEK Universitas Muhammadiyah Purworejo,* Volume 1, pp. 1-7.

HOOTSUITE, W. A. S. A., 2018. *2018 Q2 Global Digital Statshot,* New York: We Are Social and Hootsuite.

HOOTSUITE, W. A. S. A., 2019. *Indonesia Digital 2019,* New York: We Are Social and Hootsuite.

KURNIAWAN, S., 2014. *Perancangan Prosedur Operasional Standar Penanganan Alat Bukti Digital : Studi Kasus Kementrian Komunikasi dan Informatika,* Jakarta: Universitas Indonesia.

PASA, I. Y., 2019. Analisis Pengembangan Fitur Obrolan Baru Berbasis Scan QR Code pada Aplikasi Paziim. *The 9th University Research Colloqium 2019.*

RAHARDJO, B., 2013. Sekilas Mengenai Forensik Digital. *Sosioteknologi,* 12(29), pp. 384-387.

SAGEMCOM, 2011. *AT Command Set for SAGEMCOM HiLo 3G Module,* France: SAGEMCOM.

SIMAO, A. M. D. L., MELO, L. P. D., SICOLI, F. C. & JUNIOR, R. T. D. S., 2011. Acquisition of digital evidence in android smartphones. *Australia Digital Forensic Conference.*

UMAIR, A., NANDA, P. & HE, X., 2017. Online Social Network Information Forensics: A Survey on Use of Various Tools and Determining How Cautious Facebook Users are?. *Trust, Security and Privacy in Computing and Communications (TrustCom),* pp. 1139-1144.

WILLASSEN, S. Y., 2005. Forensic Analysis of Mobile Phone Internal Memory. *Advances in Digital Forensics SPringer,* pp. 191-204.