Identifikasi Barang Bukti Percakapan Aplikasi Dual Apps Whatsapp Pada Ponsel Xiaomi Menggunakan Metode NIST Mobile Forensics

Dedy Hariyadi[1*], Ike Yunia Pasa[2]
[1]Komunitas Forensik Digital, Yogyakarta 55000, Indonesia
[2]Teknik Informatika, Universitas Muhammadiyah Purworejo, Purworejo 54111, Indonesia

Abstrak

Mobile Forensics merupakan cabang keilmuan dari Forensik Digital terkait penanganan barang bukti digital pada perangkat gemerak. Perkembangan teknologi perangkat gemerak seperti ponsel cerdas perlu penanganan yang cukup unik dan adaptif dengan perkembangan teknologi. Munculnya inovasi teknologi pada perangkat gemerak harus ditangani dengan teliti dan cermat. Sebagai contoh fitur baru Dual Apps yang diluncurkan oleh Xiaomi juga perlu dilakukan identifikasi jejak digitalnya. Fitur Dual Apps memungkinkan 1 ponsel dapat memiliki 2 akun pada 1 aplikasi media sosial yang sama. Menggunakan metode NIST Mobile Forensics untuk melakukan identifikasi barang bukti digital yang ditinggalkan ekosistem Dual Apps.

Kata kunci: Dual Apps, Mobile Forensics, NIST, WhatsApp, Xiaomi

Abstract

Mobile Forensics is a scientific branch of Digital Forensics related to the handling of digital evidence on mobile devices. The growth of mobile devices technologies such as smartphones need quite unique and adaptive handling with technological developments. Technological innovations in mobile devices should be handled thoroughly. As an example of Dual Apps new features launched by Xiaomi also need to be identification of digital traces. Dual Apps feature allows 1 phone to have 2 accounts on 1 social media app. Using the NIST Mobile Forensics method to identify digital evidences left behind by the Dual Apps ecosystem.

Keywords: *Dual Apps, Mobile Forensics, NIST, WhatsApp, Xiaomi*

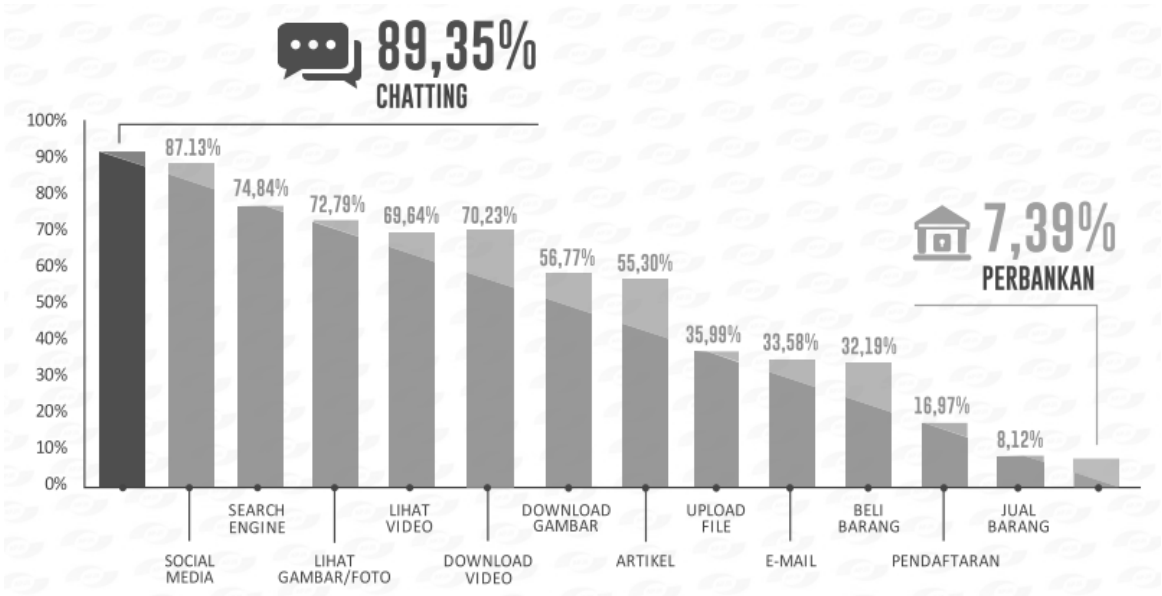
1. PENDAHULUAN

Dari 262 juta penduduk Indonesia pada tahun 2017 pengguna internet kurang lebih sekitar 143 juta jiwa atau kurang lebih 54% dari jumlah penduduk. Sedangkan prosentase kepemilikan ponsel cerdas dari jumlah penduduk sekitar 50%. Sedangkan kepemilikan komputer atau laptop lebih kecil dibandingkan ponsel certas yaitu se kitar 25%. Layanan internet yang diakses paling besar adalah *chatting* sekitar 89% yang kemudian disusul layanan medial sosial, mesin pencarian, melihat foto, melihat video, mengunduh video, mengunduh gambar, membaca artikel, mengunggah berkas, komunikasi melalui surel, membeli barang secara daring, pendaftaran layanan lain-lain, menjual barang secara daring, dan mengakses perbankan daring seperti yang ditunjukan pada Gambar 1 (Asosiasi Penyelenggara Jasa Internet Indonesia & Teknopreneur Indonesia, 2017).

derungan sebagai pelaku dan/atau korban hal ini ditunjukan melalui kajian yang menyatakan bahwa berita bohong atau hoaks menyebar melalui tulisan 62.1 %, gambar 37.5% dan video 0.4%. Sedangkan media penyebaran hoaks terbesar melalui sosial media sebesar 92.4% kemudian disusul aplikasi chatting 62.8%, situs web 34.9%, televisi 8.7%, media cetak 5%, surel 3.1%, dan radio 1.2% (Masyarakat Telematika Indonesia, 2017).

Tingginya prosentase penggunaan aplikasi chatting untuk melakukan penyebaran hoaks perlu diwaspadai karena hal ini merupakan tindak kejahatan yang telah diatur oleh perundangan yang telah berlaku. Pada UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 28 telah mengatur perihal berita bohong yang dapat menyebabkan kerugian konsumen dalam bertransaksi elektronik dan menyebarkan informasi yang dapat menimbulkan kebencian

p-ISSN 2620 – 4843
e-ISSN 2620 – 4924



Gambar 1. Survey Layanan Internet yang Diakses pada Ponsel Cerdas

Komunikasi melalui *instant messaging* atau *chatting* saat ini memang banyak penggunanya. Di Indonesia terdapat beberapa aplikasi chatting yang populer diantaranya, WhatsApp, Line, Blackberry Messenger, Facebook Messenger, dan Telegram. Saat ini aplikasi WhatsApp masih menduduki peringkat teratas penggunaan di Indonesia (Dailysocial, 2017).

Pertumbuhan ponsel cerdas yang tinggi membuka kesempatan kejahatan melalui ponsel cerdas baik sebagai pelaku atau korban (RSA, 2016). Melalui media *chatting* memiliki kecendengan landasan suku, agama, rasa, dan antargolongan (SARA). Informasi yang disebarkan atau diterima melalui aplikasi WhatsApp meninggalkan jejak berupa barang bukti digital pada ponsel. Bukti digital yang dapat ditemukan diantaranya berisi, daftar kontak, komunikasi chatting, berkas salinan komunikasi, foto dari daftar kontak, salinan foto dari daftar kontak, berkas catatan, berkas yang diunduh, berkas yang dikirimkan, dan berkas konfigurasi lainnya. Barang bukti digital tersebut memiliki korelasi satu sama lainnya oleh sebab itu penyidik atau investigator harus cermat karena perbedaan sis-

tem operasi merupakan tantangan baru (Anglano, 2014).

2. STUDI LITERATUR

2.1. NIST: Incident Response

U.S. Departement of Commerce melalui *National Institute of Standar and Technology (NIST)* memberikan usulan dalam penanganan tindak kejahatan yang melibatkan barang bukti elektronik dan/atau digital. Terdapat 4 tahap proses penanganan forensik digital diantaranya:

1. Collection

Melakukan identifikasi dan mengakuisisi barang bukti elektronik dan/atau digital yang berpontensial dan relevan terkait tindak kejahatan. Dalam tahap ini perlu diperhatikan sifat-sifat barang bukti digital yang dipengaruhi oleh waktu dan sumber daya listrik. Sebagai contoh dalam mengakuisisi ponsel harus diperhatikan ketersedian sumber listrik, dipastikan memiliki sumber listrik yang cukup saat dilakukan pengumpulan barang bukti atau pun analisis.

2. Examination

Tahap ini dilakukan proses ekstraksi data berupa barang bukti digital dari barang bukti elektronik menggunakan metode otomatis dalam hal ini aplikasi forensik digital atau secara manual. Saat melakukan ekstrasi barang bukti digital harus dipastikan intregitasnya terjaga dari kontaminasi hal-hal yang dapat membatalkan statusnya sebagai barang bukti digital di pengadilan. Untuk mempersingkat proses ini sebaiknya ekstrasi barang bukti digital harus relevan dengan tindak kejahatan yang sedang ditangani.

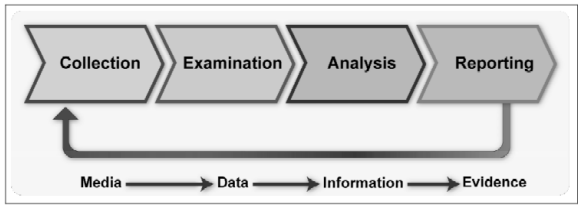
3. Analysis

Data yang telah dilakukan ekstraksi dilakukan analisis menggunakan metode dan teknik yang sesuai dengan aturan yang berlaku. Identifikasi dana analisinya melibatkan banyak hal yang saling terkait dalam tindak kejahatan. Proses analisis dapat melibatkan ahli sesuai dengan bidang keahlian terkait analasis yang lebih detil. Sebagai contoh saat terjadi tindak kejahatan pemalsuan atau rekayasa foto maka ahli yang dilibatkan memiliki keahlian dalam pengolahan citra.

4. Reporting

Semua aktivitas 3 tahap tersebut harus terdokumentasi dengan baik sehingga memudahkan membuat laporan secara detil baik menyangkut hal teknis maupun non-teknis. Bahasa yang digunakan dalam membuat laporan harus menggunakan bahasa yang mudah dipahami oleh pihak lain sehingga mudah untuk ditindaklanjuti.

Gambar 2 menunjukan proses penanganan barang bukti digital yang dapat disajikan di pengadilan atau kebutuhan sendiri pada institusi investigasi. Pada proses *Collection* dan *Examination* diperlukan sebuah alat bantu forensik untuk mengekstraksi barang bukti digital menjadi data untuk dianalisis (Kent, Chevalier, Grance, & Dang, 2006). Pada penelitian ini fokus pada *Collection* dan *Examination*.



Gambar 2. Proses Forensik Digital

2.2. NIST: Mobile Forensics

Proses *Collection* pada perangkat gemerak memiliki karakteristik berbeda dengan sebuah PC. Perkembangan ponsel cerdas saat ini juga mengalami pertumbuhan yang tinggi. Oleh sebab itu perlu penanganan khusus dalam menindaklanjuti tindak kejahatan yang menggunakan perangkat digital seperti ponsel cerdas. Pada saat melakukan *Examination* dengan melakukan ekstraksi data pun juga perlu penanganan khusus. Adapun metode ekstraksi pada ponsel cerdas diantaranya (Ayers, Brothers, & Jansen, 2014):

1. Manual Extraction

Metode yang dilakukan pada *Manual Extraction* adalah dengan melihat secara langsung data-data yang terkait dengan tindak kejahatan pada ponsel. Sehubungan metode ini rentan terkontaminasi disarankan saat melakukannya harus terekam oleh kamera. Bukti digital yang telah terhapus tentu tidak bisa didapatkan.

2. Logical Extraction

Untuk melakukan metode ini memerlukan konektivitas seperti media kabel ataupun

nirkabel antara ponsel dengan komputer dengan aplikasi forensik digital. Dalam barang bukti digital tetap memperhatikan integritas data yang diambil

3. Hex Dumping/JTAG

Hex Dumping dan/atau *Joint Test Action Group (JTAG)* metode yang dilakukan untuk mendapatkan informasi yang lebih besar dibandingkan *Logical Extraction* dan *Manual Extraction* karena barang bukti yang terhapus dapat dilakukan ekstraksi. Sehingga akan lebih memudahkan dalam proses analisis. Metode ini memerlukan ketelitian karena harus perangkat khusus untuk mengurangi resiko barang bukti digital hilang.

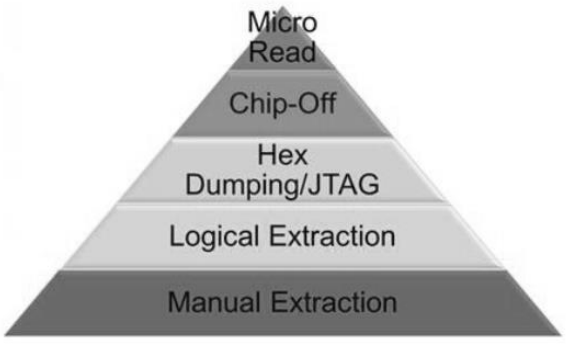
4. Chip-Off

Tingkat kompleksitas metode ini serupa dengan *Hex Dumping* atau *JTAG* karena proses yang dilakukan dengan cara melakukan ekstraksi barang bukti dari chip pada ponsel. Sebelumnya chip pada ponsel diambil dulu dengan pendekatan elektronika.

5. Micro Read

Proses melakukan ekstraksi dengan metode *Micro Read* dilakukan dengan atensi khusus seperti ancaman negara, dokumen rahasia, atau tindak kejahatan yang melibatkan antar negara sehingga memerlukan kerjasama antar penegak hukum dengan pembuat ponsel. Teknik pada *Micro Read* dengan cara melakukan observasi pada *chip NAND* atau *OR* menggunakan mikroskop elektron.

Piramida metode ekstraksi barang bukti digital dari ponsel merujuk pada pada Gambar 3.



Gambar 3. Piramida Ekstrasi pada Ponsel

2.3. Dual Apps pada MIUI

Xiaomi membenamkan sistem operasi pada produk ponsel cerdasnya menggunakan MIUI (*Mi User Interface*) yang merupakan turunan dari sistem operasi Android. Tahun 2016 Xiaomi merilis versi baru MIUI dengan berberapa fitur diantaranya Dual Apps. Melalui fitur Dual Apps pengguna dapat menggunakan 1 aplikasi dengan 2 akun yang berjalan sekaligus. Sehingga pengguna yang memiliki 2 akun tidak perlu memiliki ponsel 2 buah atau memasang aplikasi tambahan yang sifatnya tidak resmi. Aplikasi yang terdukung dalam fitur Dual Apps diantaranya aplikasi *chatting*. Pengguna cukup mengaktifkan fitur Dual Apps pada bagian Settings (Xiaomi, 2016).

3. METODE PENELITIAN

3.1. Alat dan Bahan

Pada penelitian ini memerlukan beberapa alat dan bahan terkait dengan proses forensik pada ponsel cerdas. Hal ini serupa pada proses forensik digital tindak kejahatan yang melibatkan ponsel cerdas sebagai barang buktinya. Adapun alat dan bahan yang diperlukan seperti tercantum pada Tabel 1.

Tabel 1. Alat dan Bahan Penelitian

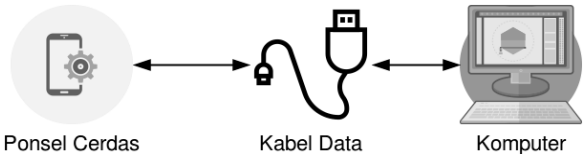
No	Alat dan Bahan	Keterangan
1.	Komputer	CPU dengan 4 Core @ 1.90GHz, RAM sebesar 8GHz, Hard Disk 500GB
2.	Sistem Operasi	Linux
3.	Ponsel Cerdas	Xiaomi dengan tipe Mi5 bersistem operasi MIUI v9
4.	Kabel Data	Konektivitas komputer dengan ponsel menggunakan kabel data yang dapat mentransfer data
5.	Andriller dan Laron	Aplikasi forensik digital untuk melakukan logical extraction
6	WhatsApp	Aplikasi chatting yang dikembangkan oleh WhatsApp Inc yang merupakan anak perusahaan Facebook.

3.2. Alur Penelitian

Metode ekstrasksi yang diterapkan menggunakan *Logical Extraction* dengan 2 teknik, yaitu:

1. Tanpa memasang *agent*, artinya teknik ekstraksinya menggunakan Android Debug Bridge

(ADB) baik perintah *console* maupun aplikasi dalam hal ini menggunakan Andriller. Media komunikasinya menggunakan kabel data seperti tampak pada Gambar 4.



Gambar 4. Konektivitas Ponsel Cerdas dan Komputer

2. Memasang *agent*, artinya ponsel terpasang terlebih dahulu sebuah aplikasi dalam hal ini Laron yang selanjut prosesnya ekstraksi ke komputer menggunakan ADB. Aplikasi Laron merupakan aplikasi forensik secara logikal yang mengakuisisi data dari aplikasi yang terpasang pada ponsel cerdas bersistem Android dengan lisensi MIT. Adapun proses akuisis secara logikal menggunakan Laron seperti pada Gambar 5 (Hariyadi & Huda, 2015).

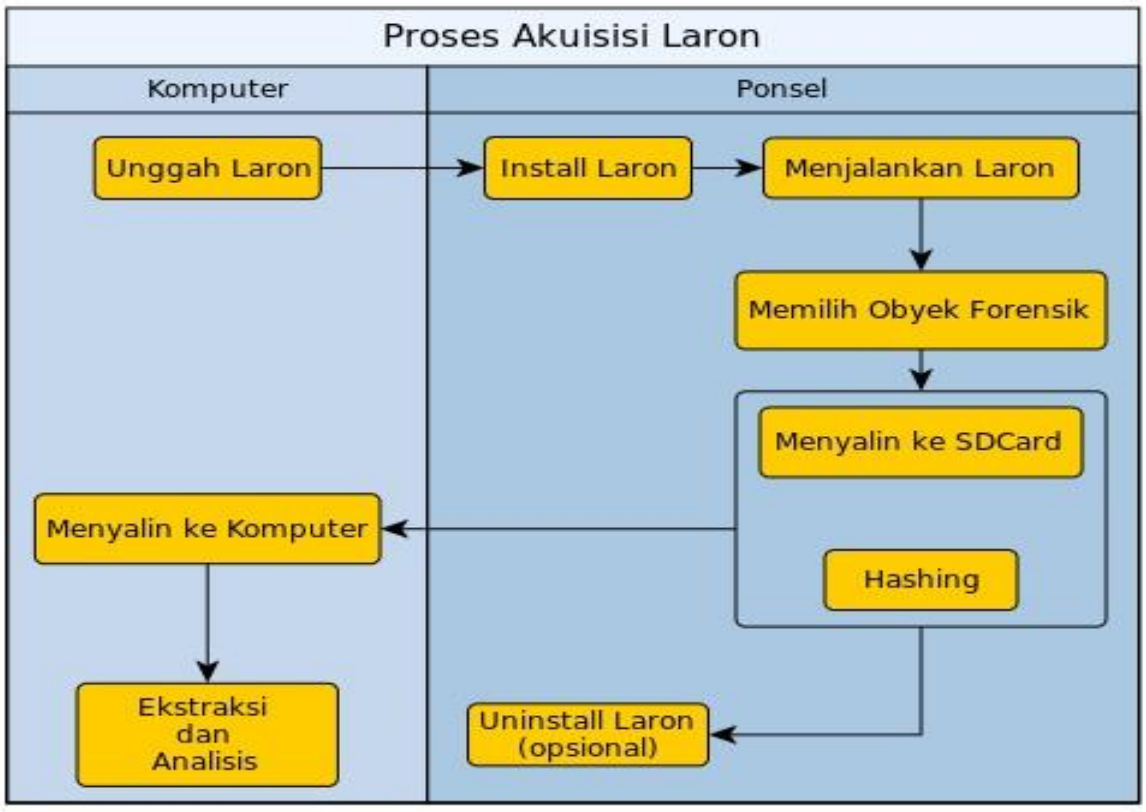
4. HASIL DAN PEMBAHASAN

Dalam proses ekstrasi barang bukti digital pada ponsel cerdas bersistem operasi Android minimal harus memenuhi syarat diantaranya ponsel dalam kondisi menyala, ponsel dalam kondisi tidak terkunci dan telah diaktifkan mode USB Debugging. Baik Andriller dan Laron tetap menggunakan ADB dalam proses ekstraksinya oleh sebab itu ketiga syarat tersebut harus terpenuhi.

Pada proses ekstraksi menggunakan Andriller pada obyek berupa ponsel Xiaomi Mi5 tidak didapat barang bukti digital berupa basis data atau berkas lainnya. Andriller yang digunakan untuk mengekstraksi barang bukti digital yang terdapat pada ponsel Xiaomi Mi5 adalah versi terbaru saat peneltian ini dilakukan (versi 2.6.40). Hal ini ditunjukan seperti pada Gambar 6 yang merupakan hasil laporan penggunaan Andriller dalam proses ekstraksi.

Rancangan dasar dari aplikasi Laron selain ponsel harus dalam kondisi menyala, ponsel tidak dalam kondisi terkunci dan USB Debugging dalam kondisi aktif, ponsel sebaiknya dalam kondisi sudah ter-*root*. Hal ini bertujuan untuk memudahkan proses ekstraksi barang bukti digital dan menjaga integritas barang bukti melalui pengujian nilai hash.

p-ISSN 2620 – 4843
e-ISSN 2620 – 4924



Gambar 5. Proses Akuisisi atau Ekstraksi Menggunakan Laron

[Andriller Report] XIAOMI Mi5 | IMEI:Unknown

Type	Data
ADB serial:	bd2a55b1
Shell permissions:	root(su)
Manufacturer:	XIAOMI
Model:	Mi5
IMEI:	Unknown
Android version:	7.0
Build name:	
Wifi MAC:	b0:e2:35:28:0f:61
Local time:	2018-03-21 21:23:29 WIB
Android time:	2018-03-21 21:23:29 WIB
Accounts:	com.xiaomi: 1585***958 com.google: milisdad***ail.com org.telegram.messenger: 17***84 org.mariotaku.twidere.account: milisdad@***tter.com com.whatsapp: Wha***pp com.facebook.auth.login: Fac***ok scribd.main_type: mil***ad com.dropbox.android.account: milisdad***ail.com phone-halo.appspot.com: Anonymous ***wd Tracker phone-halo.appspot.com: milisdad***ail.com com.linkedin.android: Lin***ln com.google.android.apps.tachyon: *** com.whatsapp: Wha***pp

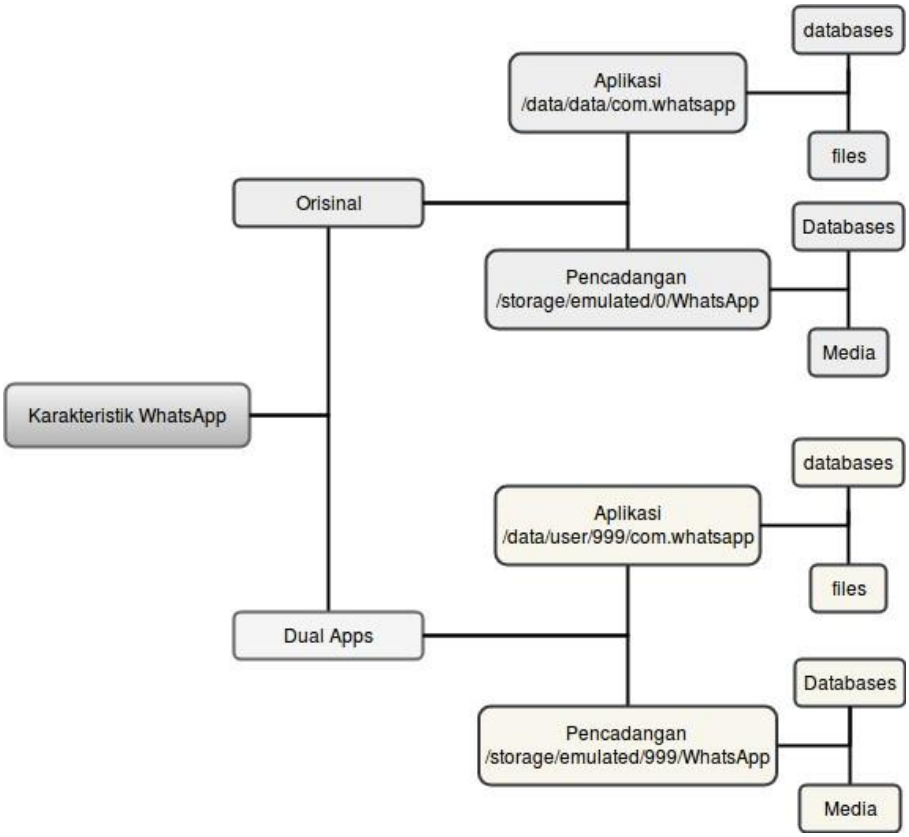
Gambar 6. Bentuk Laporan Singkat Andriller

Dalam proses ekstraksi menggunakan Laron saat pemilihan obyek atau barang bukti percakapan hanya ditemukan berkas msgstore.db dan wa.db yang terletak pada direktori /data/data/com.whatsapp/databases/. Jadi untuk mendapatkan akses ke dalam direktori /data/data/com.whatsapp/databases/ harus memiliki akses root.

Aplikasi WhatsApp secara periodik melakukan pencadangan percakapan yang disimpan dalam direktori /storage/emulated/0/WhatsApp/Databases/. Berkas percakapan yang disimpan dienkripsi dengan ekstensi .crypt12. Begitu pula aplikasi WhatsApp yang berjalan di ekosistem Dual Apps juga menyimpan berkas dengan ekstensi .crypt12.

Sehubungan hasil ekstraksi menggunakan Andriller dan Laron tidak dapat menemukan bukti digital percakapan WhatsApp secara keseluruhan baik versi orisinal dan Dual Apps maka dilakukan ekstraksi menggunakan metode manual melalui ADB dengan memperhatikan kaidah dari NIST Mobile Forensics. Letak barang bukti percakapan WhatsApp versi orisinal dan Dual Apps terletak pada direktori yang berbeda namun serupa. Adapun inti dari barang bukti percakapan WhatsApp sebagai berikut:

1. Berkas wa.db merupakan daftar kontak dengan lokasi penyimpanan di direktori databases dari aplikasi.



Gambar 7. Karakteristik Direktori WhatsApp Orisinal dan Dual Apps

2. Berkas msgstore.db berisi percakapan dengan lokasi penyimpanan di direktori databases dari aplikasi.

3. Berkas msgstore-YYYYMMDD-db.crypt12 merupakan salinan berkas percakapan yang dienkripsi dengan lokasi penyimpanan di direktori Databases dari pencadangan.

4. Berkas key merupakan kunci dari berkas yang terenkripsi crypt12 dengan lokasi penyimpanan di direktori files dari aplikasi.

Pemetaan tata letak barang bukti percakapan seperti terlihat pada Gambar 7. WhatsApp orisinal memiliki direktori aplikasi pada /data/data/com.whatsapp dan direktori pencadangan pada /storage/emulated/0/WhatsApp sedangkan aplikasi Whatapp yang berjalan pada ekosistem Dual Apps memiliki direktori aplikasi pada /data/user/999/com.whatsapp dan direktori pencadangan pada /storage/emulated/999/WhatsApp.

5. SIMPULAN

Baik Andriller dan Laron tidak dapat menemukan barang bukti percakapan WhatsApp yang berjalan pada ekosistem Dual Apps. Sehingga untuk menemukan dan memetakannya menggunakan metode manual melalui ADB. Adapun pemetaan barang bukti percakapan WhatsApp sebagai berikut:

1. Orisinal terletak pada direktori /data/data/com.whatsapp dan /storage/emulated/0/WhatsApp.

2. Ekosistem Dual App terletak pada direktori /data/user/999/com.whatsapp dan /storage/emulated/999/WhatsApp.

Sehubungan aplikasi Laron merupakan aplikasi berlisensi bebas maka diharapkan dalam pengembangan selanjutnya dapat melakukan akuisisi secara *logical* pada aplikasi-aplikasi yang berjalan pada ekosistem Dual Apps.

DAFTAR PUSTAKA

Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation Journal*, *11*(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Asosiasi Penyelenggara Jasa Internet Indonesia, & Teknopreneur Indonesia. (2017). *Penetrasi & Perilaku Pengguna Internet Indonesia - Survey 2017*. Jakarta.

Ayers, R., Brothers, S., & Jansen, W. (2014). *NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics*. *NIST Special Publication* (Vol. 1). Gaithersburg, MD. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-101r1

Dailysocial. (2017). *Mobile Instant Messaging Survey 2017*.

Hariyadi, D., & Huda, A. A. (2015). Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android. *Indonesia Security Conference 2015*. Cirebon. https://doi.org/10.13140/RG.2.1.3819.9520

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. Gaithersburg: National Institute of Standards and Technology.

Masyarakat Telematika Indonesia. (2017). *Survey 2017: Wabah Hoax Nasional*.

RSA. (2016). 2016: Current State of Cybercrime, 7. Retrieved from https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf