CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 1, No. 2, November 2018, hlm. 67-74

PENERAPAN FRAMEWORK *HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS (HDFIP)* UNTUK MENDAPATKAN *ARTIFAK* BUKTI DIGITAL PADA *SMARTPHONE* TIZEN

Widodo[1], Bambang Sugiantoro[2]

[1]Magister Teknik Informatika Fakultas Teknologi Industri
Universitas Islam Indonesia. Jl. Kaliurang Km. 14,5 Sleman, Yogyakarta.
[2]Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Jl. Lakssda Adisucipto Yogyakarta
Email : [1]widd.simple@yahoo.co.id, [2]bambang.sugiantoro@uin-suka.ac.id

Abstrak

Menurut *Tizen Team (2016)* s*martphone* dengan sistem operasi *tizen* termasuk *smartphone* yang baru dan memiliki jenis aplikasi *Web, Hybrid, Native*/asli dengan extensi *file* berupa *file.tpk* yang berbeda dengan jenis *smartphone* lainnya. Dari beberapa *review* penelitian sebelumnya, dapat diketahui bahwa belum ada penelitian tentang proses penanganan *smartphone tizen* beserta *platform whatsapp* yang berada didalamnya. Sebagian besar hasil penelitian hanya meliputi tentang bagaimana ekplorasi bukti digital pada *smarphone android* dan membahas *tizen* dari segi keamanan. Berdasarkan *review* dari penelitian tersebut, terdapat beberapa masalah diantaranya belum adanya metode dan penerapan *framework* yang cocok untuk proses penanganan *smartphone tizen* dan *platform whatsapp* yang berada didalamnya tersebut. Untuk itu, metode *live forensics* dan model *HDFIP* dapat dijadikan acuan *framework* yang cocok untuk mengidentifikasi karakteristik *tizen* dan *platform whatsapp*. Dimana metode *live forensics* akan digunakan untuk melakukan tahapan analisa secara terperinci dan teliti terhadap peangkat barang bukti digital dan dilakukan dalam sebuah perangkat elektronik dalam keadaan *power on.* Sehingga penelitian ini menghasilkan perbedaan mendasar artifak *android* dan *tizen*, mendapatkan karakteristik bukti digital pada *Smartphone Tizen,* yaitu berbentuk *logical* dan berupa *file* dengan ektensi *.CSV* dan *file.db,* dimana hasil penelitian ini terfokus pada sistem aplikasi *WhatsApp* dan *SMS.*

Kata Kunci: *smartphone tizen, akuisisi langsung, hdfip, arteifak, SMS, whatsapp*

THE IMPLEMENTATION OF FRAMEWORK HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS (HDFIP) TO GET ARTIFACTS DIGITAL EVIDENCE ON SMARTPHONE TIZEN

Abstract

According to Tizen Team (2016) smartphones with the Tizen operating system include new smartphones and have a type of Web application, Hybrid, Original with file extensions in the form of .tpk files that are different from other types of smartphones. From some of the reviews of previous research, it can be seen that there has been no research on the process of handling tizen smartphones along with whatsapp platforms that are in it. Most of the research results only cover how digital evidence was explored on Android smartphones and discussed Tizen in terms of security. Based on the review of the research, there are several problems including the absence of methods and application frameworks that are suitable for the handling of Tizen smartphones and whatsapp platforms that are in it. For this reason, direct forensic methods and HDFIP models can be used as references for appropriate frameworks to identify the characteristics of the tizen and whatsapp platforms. Where live forensic methods will be used to carry out detailed and rigorous analysis of digital evidence and carried out in electronic devices in the strength of the state. So that this study produces a fundamental difference between Android and Tizen artifacts, obtaining digital evidence characteristics on Tizen Smartphones, which in logical form and files with extensions .CSV and file.db, where the results of this study focus on the WhatsApp and SMS application systems.

Keywords : *smartphone tizen, live forensics, HDFIP, artifacts, SMS, whatsapp*

1. PENDAHULUAN

Penggunaan *smartphone* terus meningkat diberbagai kalangan usia, terutama usia dibawah 25 tahun. Menurut *survey* di Indonesia, menunjukkan bahwa pada tahun 2018, 157% dari orang Indonesia memiliki *smartphone* dengan pengguna mencapai 103.000.000. pengguna. Perkembangan *smartphone* tidak hanya memberikan dampak positif tetapi juga membawa dampak negatif, hal ini dibuktikan dengan data kejahatan yang diperoleh ***Okezone*** dari Direktorat Tindak Pidana Kejahatan Siber (DIT TIPIDSIBER) BARESKRIM POLRI sepanjang (2017), yaitu menangani 1.763 kasus kejahatan siber *(https://news.okezone.com).* Selain itu, data tersebut diperkuat dengan kejahatan pengguna *smartphone* yang di rilis oleh Josua Sinambela (2017) seorang *PCN & ISC*, Digital *Forensic Investigator*, yang mengungkap kasus *mobile* forensik & kasus audio dan chat *WhatsApp* Asusila dengan tersangka Firza Husein. Akan tetapi proses pengungkapan kasus *cybercrime* melalui *smartphone* masih belum efektif, karena terbatasnya alat dan *tools* yang digunakan untuk proses investigasi.

Penelitian terkait tentang *mobile forensics* seperti yang dilakukan (Dedi Hariyadi, 2016) melakukan *forensik Blackbarry* untuk menemukan percakapan *Chat* BBM sebagai barang bukti digital pada *smartphone* android, namun penelitian ini hanya sebatas pada *smartphone* android. Penelitian lain yang dilakukan oleh Raymond dkk., (2014) melakukan pengujian *framework HDFIP* yang sebelumnya diterapkan untuk *computer forensics*, penelitian ini menghasilkan penerapan *HDFIP* pada proses penanganan *smartphone forensics*, tetapi penerapanya baru sebatas pada *smartphone android*. Dengan demikian, penanganan kasus *cybercrime* pada *smartphone* belum efektif, dikarenakan setiap jenis *smartphone* memiliki arsitektur dan metode penanganan investigasi yang berbeda-beda. Salah satu jenis bukti digital yang kurang mendapatkan perhatian pada *smartphone* adalah bukti digital pada *smartphone* Tizen. Menurut Danial Song, (2015) Tizen adalah sebuah *platform open source* berbasis Linux yang baru pada perangkat *smartphone* dan memiliki koleksi *library* yang diimplementasikan dalam bahasa C dan C++. Menurut informasi dari Tizen Team (2016) SKKU Embedded Software Laboratory, perbedaan *Smartphone* Tizen dengan *smartphone* lainnya adalah Tizen termasuk *smartphone* baru dan merupakan *smartphone* yang memiliki jenis aplikasi Web, *Hybrid*, Native/asli dengan extensi file berupa *file.tpk*, dan mengadopsi file ext4, yang berbeda dengan jenis *smartphone* lainya, serta penggunaan aplikasi yang masih terbatas.

Berdasarkan penjelasan dan uraian diatas maka akuisisi barang bukti digital pada *smartphone* tizen dan *platform whatsapp* yang berada didalamnya berbeda dengan cara akuisisi pada *android*. Dengan karakteristik Tizen tersebut, maka muncul beberapa masalah seperti metode yang digunakan untuk akuisisi dalam menemukan bukti digital dan model/*framework* yang akan diterapkan untuk eksplorasi *smartphone* tizen dan *platform whatsapp* tersebut. Karena hal tersebut peneliti anggap cukup beralasan untuk mengajukan penelitian tentang investigasi pada *smartphone* tizen yang bertujuan untuk mendapatkan artefak barang bukti digital, dengan cara menggunakan metode *live forensics* serta mengadopsi model *Harmonised Digital Forensic Investigation Process* (HDFIP).

2. TINJAUAN PUSTAKA

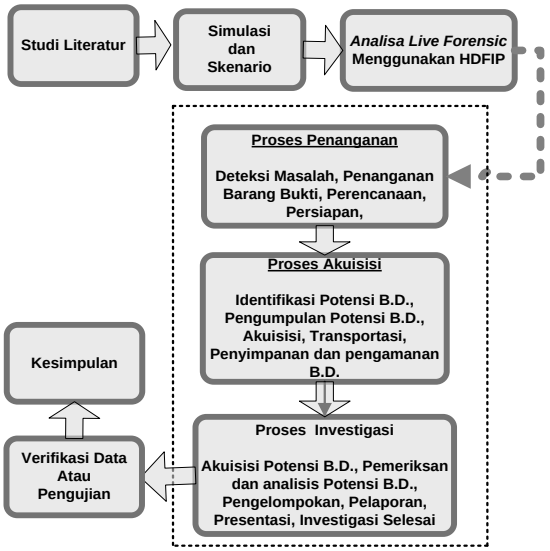
Digital Forensik Adalah cabang dari forensik yang berhubungan dengan pemulihan, investigasi dan analisis bukti yang ditemukan diperangkat digital yang dapat disajikan dalam pengadilan hukum. Saat melakukan penyelidikan harus mengikuti prosedur yang tepat dan mendokumentasikan dari setiap tahapan saat mencari bukti digital (Noorulla, 2014). Menurut Divyesh G Dharan (2014) proses pengumpulan barang bukti digital ada dua yaitu offline dan live analisa. Analisa offline dalam forensik digital adalah proses investigasi yang dilakukan untuk mencari barang bukti dari sebuah barang elektronik yang sudah mati atau OFF. Sedangkan analisa live adalah sebuah analisa yang dilakukan ketika itu juga pada perangkat elektronik atau komputer yang masih menyala ON dan dilakukan setelah kejadian.

Menurut Pasal 5 undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ayat 1 berbunyi, Informasi dan Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetakan merupakan alat bukti hukum yang sah. Terlepas dari pasal 184 KUHP yang membuat penggolongan alat bukti yang sah, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Pada Pasal 5 Ayat 2 undang-undang No. 11 Tahun 2008 Tentang ITE menjelaskan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti lain, selain alat bukti yang sebagaimana dimaksud dalam ketentuan perundang-undangan.

Mobile Phone Forensics adalah ilmu yang melakukan proses *recovery* bukti digital dari perangkat *mobile* menggunakan cara yang sesuai dengan kondisi forensik (Ilman Z., 2014), proses *recovey* ini untuk tujuan mendapatkan bukti digital secara hukum.

3. METODOLOGI PENELITIAN

Secara ringkas urutan langkah-langkah penelitian penyelesaian masalah dengan metode live forensics dan penerapan model HDFIP dapat dilihat pada Gambar 1.



Gambar 1. Konsep Metodologi Penelitian

1. Tahap tahap awal untuk mengumpulkan teori-teori yang berhubungan dengan *Mobile Forensics*.
2. Tahap kedua adalah simulasi dan skenario.
3. Tahap ketiga adalah analisis *live forensics* menggunakan HDFIP yang terdiri dari 3 tahapan utama yaitu
   a. **Proses Penanganan** yang terdiri dari deteksi masalah, penanganan barang bukti, perencanan dan persiapan.
   b. **Proses Akuisisi** yang terdiri dari beberapa sub tahapan yaitu identifikasi potensi bukti digital, pengumpulan potensi bukti digital, akuisisi, transportasi, penyimpanan dan pengamanan bukti digital.
   c. **Proses Investigasi** yang terdiri dari beberapa sub tahapan yaitu akuisisi potensi bukti digital, pemeriksan dan analisis potensi bukti digital, pengelompokan, pelaporan, presentasi, investigasi selesai.
4. Tahap yang keempat adalah verifikasi data dan pengujian, yaitu merupakan tahap pengujian barang bukti sumber dengan barang bukti yang di analisa dengan mencocokan hash MD5 dan SH1.
5. Dan tahap yang terakhir adalah kesimpulan.

4. HASIL DAN PEMBAHASAN

4.1 Persiapan Sistem

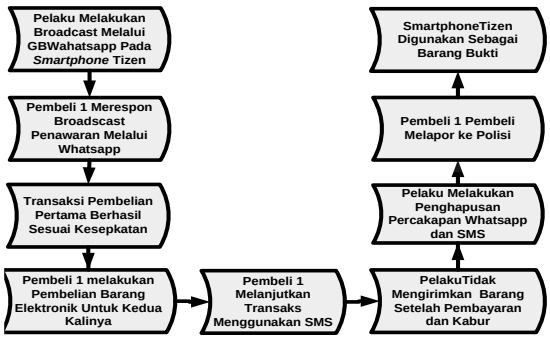
Langkah pertama yang harus dilakukan dalam penelitian ini adalah mempersiapkan perangkat *hardware* dan *software* untuk investigasi dan penerapan *framework* pada akuisisi *smartphone* disistem operasi windows.

4.2 Skenario Kasus

Pada penelitian ini dilakukan 2 macam skenario dalam transakasi penipuan jual-beli *online*, skenario tersebut terdiri dari skenario percakapan *Whatsapp* dan *SMS* pendukung yang sudah terhapus, dan sekenario yang ke-2 merupakan skenario percakapan *Whatsapp* yang belum terhapus atau tidak dilakukan penghapusan pada *smartphone* tizen yang digunakan oleh pelaku penipuan *online*. Untuk lebih jelasnya skenario akan dijelaskan sebagai berikut :

4.1.1 Skenario Penipuan *Online* 1

Pada alur proses penipuan online 1 yang dilakukan oleh pelaku dijelaskan pada Gambar 2. dimana pelaku melakukan jual-beli *online* melalui *broadcast Whatsapp* dan direspon oleh pembeli 1 bernama **Oki Pratama**. Transaksi pertama pembelian barang elektronik Oki Pratama kepada pelaku berjalan lancar sesuai kesepakatan. Akan tetapi, untuk transaksi kedua berindikasi penipuan.



Gambar 2. Alur Proses Skenario Penipuan *Online* 1

Pada sekenario ini dilakukan investigasi pada *storage* yang terdapat pada *smartphone tizen*, yang berupa kartu memori dan *storage smartphone* apabila memungkinkan untuk diambil datanya. Dari data-data yang terdapat didalam *storage* tersebut akan dicari data-data apasaja yang berpotensi untuk dijadikan barang bukti digital guna memberatkan pelaku penipuan jual-beli *online* atas tuduhan korban.

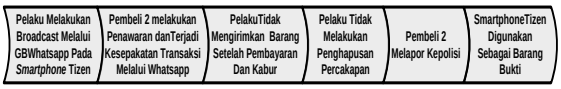
Setelah pelaku selesai melakukan penipuan *online* pada skenario 1, ditempat kejadian perkara. Pelaku berusaha menghilangkan barang bukti dengan melakukan penghapusan data-data penting yang terdapat didalam *storage smartphonenya*. Adapun beberapa tindakan pelaku akan dijelaskan sebagai berikut;

1. Pelaku / pemilik *smartphone tizen* menghapus semua percakapan whatsapp setelah uang ditransfer ke rekeningnya, ini dilakukan untuk menghilangkan barang bukti berupa percakapan whatsaap saat transaksi.
2. Pelaku menghapus *SMS* pendukung transaksi pada *smartphone tizen* tersebut. Dengan menghapus *SMS* pendukung transaksi tersebut, pelaku berharap data berupa *file/* percakapan *SMS* yang tersimpan pada *storage smartphone*

miliknya tidak dapat ditemukan apabila *Smartphone Tizen* tersebut dilakukan investigasi.

4.1.2 Skenario Penipuan Online 2

Pada alur proses skenario penipuan *online* 2 yang dilakukan oleh pelaku, dijelaskan bahwa pelaku melakukan jual-beli *online* melalui *broadcast GBWhatsapp dan* direspon oleh pembeli 2 bernama **Toni** melalui percakapan *whatsapp***,** kemudian terjadilah kesepakatan transaksi, dan korban melakukan transfer sejumlah uang kepada pelaku, akan tetapi setalah uang selesai ditransfer pelaku tidak mengirimkan barang yang sudah dibayar oleh korban. Pada alur proses penipuan online 2 ini dalam penggunaan *smartphone tizen* akan dijelaskan pada Gambar 3.

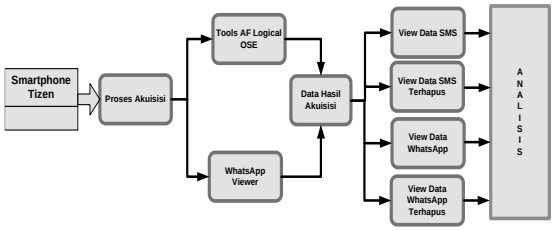


Gambar 3. Alur Proses Skenario Penipuan *Online* 2

Pada sekenario 2 ini, masih mirip dengan proses alur skenario 1 akan tetapi yang berbeda adalah korban dari penipuan tersebut. Proses alur skenario 2 dilakukan investigasi pada *storage* yang terdapat pada *smartphone tizen*, yang berupa kartu memori dan *storage smartphone* apabila memungkinkan untuk diambil datanya. Dari data-data yang terdapat didalam *storage* tersebut akan dicari data-data apasaja yang berpotensi untuk dijadikan barang bukti digital guna memberatkan pelaku penipuan *online* atas tuduhan korban. Setelah pelaku selesai melakukan penipuan *online* melalui *broadcast* dan percakapan *whatsap* pada skenario 2 di TKP. Pelaku lupa tidak berusaha menghilangkan barang bukti dengan melakukan penghapusan data-data penting yang terdapat didalam *storage smartphone* miliknya dan pada transaksi ini, korban tidak melakukan percakapan pendukung melalui SMS.

4.3 Cara Memperoleh Data

Pada tahap memperoleh data, terdapat beberapa alur proses diantaranya *smartphone* dilakukan akuisisi dengan menggunakan *tools AFLogcal OSE*, *Whatsapp Viewer, dari akuisisi* tersebut menghasilkan data *SMS* dengan *file.CSV* dan *database GBWhatsapp* yang masih di *encrypt12.* Cara memperoleh data dijelaskan pada Gambar 4:

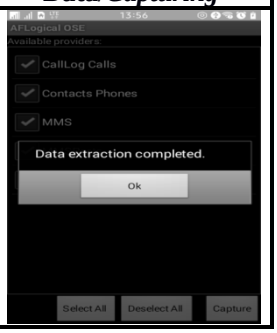


Gambar 4. Alur Proses Memperoleh Data

Proses perolehan data dilakukan dengan mengakuisisi *smartphone tizen*, dengan bantuan *tool AFLogical OSE* dan *Whatsapp Viewer* kemudian data hasil akuisisi dianalisa. Pada proses analisa, untuk file SMS.CSV dianalisa menggunakan MS. Office Excel karena aplikasi ini dapat mngakomodasi data tersebut, kemudian untuk melakukan *decrypt database Whatsapp* menggunakan aplikasi *Whatsapp Viewer* dengan memfungsikan *file key* yang diperoleh dari direktori/folder data dari *smartphone tizen* tersebut.

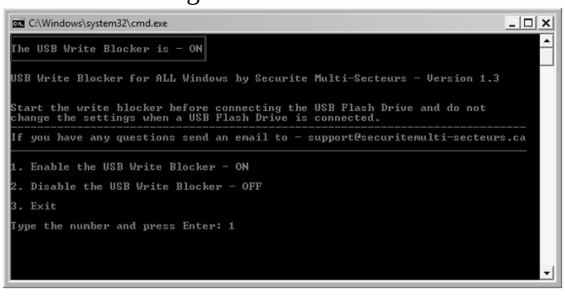
4.4 Akuisisi Menggunakan *Tools AFLogical OSE*

Tahap selanjutnya adalah akuisisi memanfaatkan layanan ACL *Menggunakan tool forensic AFLogical OSE*. Untuk proses akuisisinya dapat dilihat pada gambar 5 :

Pemilihan data yang akan diextract	***Proses Extraction* Data/*Capturing***
	

Gambar 5. Tampilan Proses *Capturing*

Selanjutnya seperti gambar 5, dilakukan proses akuisisi dengan cara *capturing*. Pada tahap proses *capturing* dilakukan untuk meng-cloning data, yang sebelumnya dilakukan pengamanan terlebih dahulu menggunakan *USB Write Blocker*. Dengan tujuan supaya tidak terjadi kontaminasi atau perubahan pada data-data bukti digital.

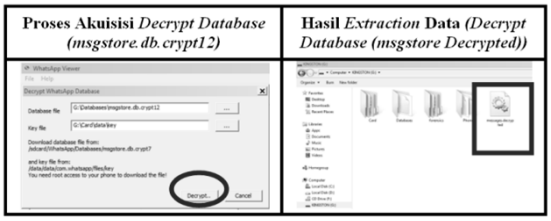


Gambar 6. Aplikasi *USB Write Blocker*

Untuk permasalahan keaslian data yang telah diakuisisi, peneliti melakukan pencatatan nilai *hash* pada data hasil *capturing.* Terdapat beberapa informasi penting yang harus dicatat, seperti waktu akuisisi, nilai hash, dan ukuran data hasil capturing. karena informasi nilai hash hasil *cloning* nantinya akan diverifikasi dengan nilai hash pada data hasil analisa.

4.5 Akuisisi Menggunakan *Tool Whatsapp Viewer*

Proses akuisisi selanjutnya untuk menemukan barang bukti digital peneliti menggunakan *Whatsapp Viewer* yang bertujuan untuk mengambil data atau melakukan *decrypt database GBWhatsapp* yang akan dianalisis dalam *smartphone* tizen. Saat dilakaukan *decrypt* perangkat *smartphone Tizen* dalam keadaan On dan paket data internet dimatikan. Proses *decrypt* data tersebut dijelaskan pada Gambar 7.:



Gambar 7. Akuisisi Menggunakan *Tool WhatsApp Viewer*

Selanjutnya seperti gambar 7, dilakukan proses akuisisi dengan cara *decrypt database whatsapp*. Pada tahap proses *decrypt database GBWhatsapp* proses ini, dilakukan untuk membaca data seluruh percakapan wahatsapp agar bisa ditemukan/bisa terbaca, karena sebelumnya *database* ini dienkripsi dengan keamanan *encrypt12*. Pada saat proses decrypt sebelumnya dilakukan pengamanan terlebih dahulu menggunakan *USB Write Blocker.* Dengan tujuan supaya tidak terjadi kontaminasi atau perubahan pada data-data bukti digital. Kemudian hasil dari *decrypt* tersebut disimpan kedalam *Flaskdisk* yang telah disediakan *investigator* dengan *file* berbernama *messages.decrypted*. *File* hasil *decrypt* tersebut dijelaskan pada Gambar 7.

4.6 Verifikasi Data dan Pengujian

1. Pengujian Data *SMS*

Setelah peneliti melakukan akuisisi dan ekstraksi terhadap *smartphone tizen* yang digunakan sebagai perangkat transaksi penipuan jual-beli *online*, kemudian dilakukan verifikasi pengujian kecocokan antara *file* hasil *Capture* dengan data asli yang terdapat pada barang bukti. Hal tersebut dilakukan sebagai pembuktian keberhasilan dari tahap akuisisi sehingga data hasil *capture* dapat dianggap sah untuk untuk proses hukum. Proses verifikasi yang akan dilakukan guna mencocokan nilai *hash* antara *file* data hasil *analisis* dengan *file* pada data asli. Peneliti menggunakan *software* atau alat bantu perangkat lunak berupa *Hash Generator* untuk mencocokan nilai *hash MD5/SH1*. Dengan tampilan seperti pada gambar 8 :

Gambar 8. Penggunaan Aplikasi *Hash Generator*

Selanjutnya peneliti akan akan menguji hasil dari verifikasi kecocokan antara nilai *hash file* data *capture* dengan *file* data asli dalam bentuk tabel agar mudah dibaca dan dipahami.

Tabel 1. Pengujian Kecocokan Barang Bukti Digital

MD5 / SH1	*File* Data Sumber	*File* Data Hasil Analisa	Ket.
MD5	*ad4f84bcbc70e4b6aa7577af0a1d8b23*	*ad4f84bcbc70e4b6aa7577af0a1d8b23*	Hasil *MD5* ***VERIFIED***
SH1	*00fa2c8ecb30e985a7cf4085e7e3ddac80cdb847*	*00fa2c8ecb30e985a7cf4085e7e3ddac80cdb847*	Hasil *SH1* ***VERIFIED***

Peneliti melakukan verifiksi data menggunakan kecocokan nilai *hash MD5* antara *file* data yang dianalisa (sumber dari *Kingston*/***Storage/Forensics/20180909.1400)*** terhadap barang bukti (bersumber dari *Phone*/***Storage/Forensics/20180909.1400)*** sebagai pembuktian bahwa benar adanya proses analisa terhadap data digital secara otentik bersumber dari barang bukti. Sebatas pembuktian validasi kecocokan nilai *hash MD5* dan *SH1.*

2. Verifikasi data GBWhatsapp

Setelah peneliti melakukan ekstraksi terhadap *GBWhatsapp* pada *smartphone* tizen yang digunakan sebagai perangkat transaksi penipuan jual-beli *online*, kemudian dilakukan verifikasi. Proses verifikasi yang akan dilakukan untuk menyajikan nilai *hash MD5* dan *SH1* guna membuktikan barang bukti tersebut berasal dari *file* data asli yang dilakukan *decrypt.*

Tabel 2. Nilai *Hash Md5* dan *SH1 Hasil Decrypt*

Nama	*GBWhatsApp*
Sumber Data	*Logical*
Waktu Akuisisi	*Sun*, 13:45:57, 09-09-2018
	Sun, 14:00:00, 09-09-2018
Nilai *Hash*	*MD5*: 10a438fc4d7c9abf76369302b656f542

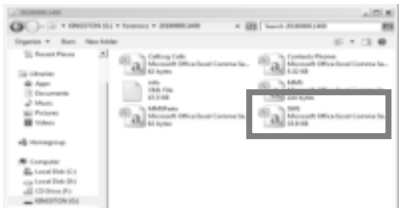
	SH1 : b55f0098124a73553cc4030e4444b19c4365c3d1
Aplikasi	*WhatsApp Viewer*

Data hasil *decrypt* selanjutnya dilakukan uji keaslian atau ontentikasi teknik hasing, pada penelitian ini menggunakan nilai *hash MD5* dan *SHA1* seperti pada Tabel 2 diatas.

4.7 Analisa Data *SMS* Hasil Akuisisi Menggunakan Tools AFLogical OSE

1. Hasil Capturing

Dari Hasil hasil akuisisi atau *capturing* terdapat beberapa *file* yang dapat ditemukan dari *smartphone tizen* milik pelaku diantaranya *file CallLog Calls.CSV*, *file Contacts Phones.CSV*, *MMS.CSV*, dan *MMSParts.CSV*, *Info.xml*. Temuan file-file potensi bukti digital tersebut dijelaskan pada Gambar 9 :



Gambar 9. Data Hasil Akuisisi/*Capturing*

Pada data hasil akuisisi *smartphone tizen* menggunakan *AFLogical OSE* seperti pada Gambar 9. Selanjutanya data tersebut akan dianalisa menggunakan *Ms. Office Excell*, karena aplikasi tersebut dapat mengakomodir data *file .CSV* tersebut. Proses *capture* yang dilakukan dengan cara *logica*l, informasinya dijelaskan pada tabel 3 :

Tabel 3. Pencatatan Informasi Hasil *Capturing*

Nama	*TizenDevices*
Sumber Data	*Logical*
Waktu Akuisisi	*Sun, 13:45:57, 09-09-2018*
	Sun, 14:00:00, 09-09-2018
Nilai *Hash File SMS* dari *Smartphone*	*MD5: ad4f84bcbc70e4b6aa7577af0a1d8b23*
	SH1 : 00fa2c8ecb30e985a7cf4085e7e3ddac80cdb847
Aplikasi	*AFLogical OSE*

Pada data hasil *capturing* setelah dilakukan uji keaslian atau ontentikasi teknik hasing, pada penelitian ini menggunakan nilai *hash MD5* dan *SHA1* seperti pada tabel 3. Diatas. Kemudian selanjutnya dilakukan analisa.

1. Analisa Data SMS Hasil *Capturing*

Pada Analisa hasil *Capturing* ini ditemukan percakapan pendukung penipuan jual-beli *online* melalui *SMS*. Barang bukti pendukung berupa percakapan *SMS* ini merupakan B.B. pada skenario 1 dengan korban bernama Oki Pratama. Isi Percakapan data *SMS* tersebut dijelaskan pada Gambar 10:

Gambar 10. Analisa Hasil *Capturing Smartphone Tizen*

Analisa hasil percakapan *SMS* pada Gambar 10. ditemukan keselurahan *SMS* dari *smarthone tizen* baik *SMS* yang sudah terhapus maupun belum dilakukan penghapusan. Untuk percakapan pendukung transaksi penipuan jual-beli online ini seperti pada skenario 1 sebelumnya, yaitu dengan korban bernama **Oki Pratama**, dalam skenario tersebut telah dilakukan penghapusan percakapan *SMS* pendukung transaksi oleh pelaku bernama Koko Saputro, dengan tujuan untuk menghilangkan barang bukti. Akan tetapi peneliti dapat menemukan / merecovery kembali data *SMS* dari *smartphone tizen* yang sudah terhapus tersebut dengan menggunakan *tools AFLogical OSE* dan hasil temuan data *SMS* tersebut dalam bentuk *file SMS.CSV*, kemudian peneliti melakukan analisa dengan *MS. Office Excell.* Hasil analisa tersebut terdapat *SMS* masuk dari nomer ***085725795077*** yang merupakan nomer *Hanphone* dari Oki Pratama (korban) kepada pelaku beranama **Koko saputro** yang terdapat dalam data *capturing* hasil analisa *smartphone* pelaku. Data-data file tersebut peneliti rangkum dalam dalam Tabel 4:

Tabel 4. Data Hasil Penelitian

No	Hasil Temuan	Sumber/Berkas *Folder*	Ket.
1	*SMS* (Percakapan *SMS* Pendukung)	***Storage/Forensics/20180909.1400***	*File SMS. CSV*
2	*SMS* yang sudah terhapus (percakapan *SMS* pendukung yang sudah terhapus)	***Storage/Forensics/20180909.1400***	*File SMS. CSV*

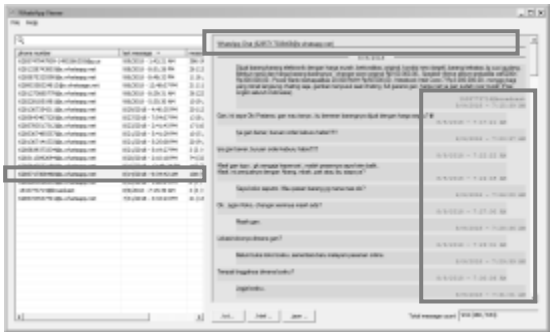
Penjelasan mengenai Tabel 4, pada kolom hasil temuan merupakan poin yang menjadi hasil analisa pencarian data pada perangkat *smartphone tizen* yang diprioritaskan menajadi alur penting dalam alur kinerja proses. yang bermula dari percakapan pendukung kelancaran traksaksi penipuan jual-beli *online* berupa percakapan *SMS*. Pada kolom sumber adalah penjelasan dimana hasil analisa tersebut dapat ditemukan, baik bersumber dari direktori folder, *Storage/Forensics/20180909.1400.* Singkatnya peneliti dapat menjelaskan secara teknis

hasil temuan tersebut berada**.** Pada kolom keterangan merupakan penjelasan teknis, atau penjelasan analisa terhadap hasil temuan. Hasil percakapan *SMS***,** dapat dijelaskan bahwa hasil temuan tersebut berbentuk *file* dengan *exstensi .CSV***.**

4.7 Analisa Data *GBWhatsapp* Hasil Akuisisi Menggunakan *Tools Whatsapp Viewer*

1. **Analisa Hasil akuisisi sekenario 1 (Setelah data dihapus)**

Dari hasil akuisisi skenario 1 dengan korban penipuan jual-beli *online* bernama **Oki Pratama,** dan tersangka penipuan bernama **Koko Saputro**. Peneliti dapat menemukan seluruh percakapan Whatsapp dari *smartphone tizen* pelaku (Koko Saputro). Percakapan transaksi Koko Saputro dengan Oki Pratama yang sebelumnya sudah dilakukan pengahpusan oleh pelaku guna menghilangkan barang bukti, dapat ditemukan didalam *database GBWhatsapp* yang masih dienkripsi *dismartphone tizen* milik pelaku, kemudian dilakukan *decrypt* menggunakan *tools whatsapp viewer* untuk dapat membaca percakapan tersebut. Penjelasan keseluruhan percakapan tersebut dapat dilihat pada Gambar 11 :

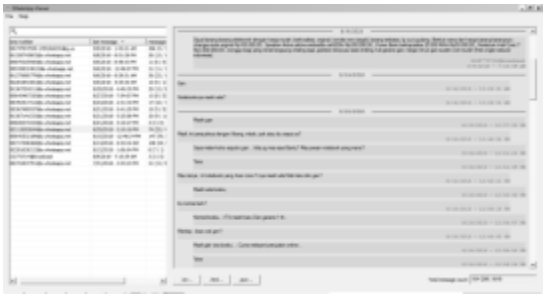


Gambar 11. Tampilan Percakapan Transaksi Setelah Penghapusan

Pada Sekenario 1 dengan korban bernama **Oki Pratama**, seprti bukti yang didapatkan pada Gambar 11. bahwa pada sekenario 1 Oki Pratama melakukan transaksi dua kali. Proses transaksi yang pertama Oki melakukan penawaran sebuah barang elektronik, kemudian setelah terjadi kesepakatan, Oki melakukan transfer uang melalui *Bank BRI* dan keesokan harinya barang sudah sampai dengan kondisi yang istimewa. Selanjutnya beberapa hari kemudian Oki melakukan transaksi lagi dengan melakukan pembelian *Netbook Acer Core i7* secara *online*, namun setelah dilakukan transfer sejumlah uang, barang tidak kunjung dikirim oleh penjual, berlanjut WA korban diblokir dan pelaku kabur. Barang bukti digital yang diperoleh dalam sekenario 1 dari percakappan *whatsapp* tersebut berupa, nomer, *whatsapp*, gambar laptop yang dijual, slip transfer Bank, baik transaksi pertama maupun yang kedua kalinya.

2. **Analisa Hasil Akuisisi Sekenario 2 (tidak dilakukan penghapusan data)**

Dari hasil akuisisi skenario 2 dengan korban penipuan jual-beli *online* bernama **Toni**, dan tersangka penipuan bernama Koko Saputro. Peneliti dapat menemukan seluruh percakapan Whatsapp dari *smartphone tizen* pelaku (Koko Saputro). Percakapan transaksi Koko Saputro dengan Toni pada skenario 2 ini tidak dilakukan penghapusan oleh pelaku. Bukti digital transaksi percakapan Whatsapp ditemukan didalam *database GBWhatsapp* yang masih dienckrpsi *dismartphone tizen* milik pelaku kemudian dilakukan *decrypt* menggunakan *Whatsapp Viewer* untuk dapat membaca percakapan tersebut. Penjelasan Keseluruhan percakapan tersebut dapat dilihat pada Gambar 12:



Gambar 12. Bukti Digital Percakapan *Whatsapp*

Pada Sekenario 2 dengan korban bernama Toni, seprti bukti yang didapatkan pada Gambar 12 bahwa pada sekenario 2 Toni melakukan transaksi pertamakali dengan melakukan penawaran sebuah barang elektronik berupa *Netbook Acer Core i7* menindaklanjuti tawaran *broadcast* pelaku, kemudian setelah terjadi kesepakatan, Toni melakukan transfer uang melalui *Bank BRI* secara *online*, namun setelah dilakukan transfer sejumlah uang, barang tidak kunjung dikirim oleh penjual, berlanjut WA korban diblokir dan pelaku kabur. Barang bukti digital yang diperoleh dalam sekenario 2 dari percakappan *whatsapp* tersebut berupa, nomer, *whatsap*p, gambar laptop yang dijual, slip transfer *Bank.*

4.8 Hasil Temuan BB Sekenario 1 dan 2

Hasil temuan barang bukti digital *GBWhatsapp* pada tabel diatas dijelaskan bahwa temuan pertama adalah Isi percakapan aplikasi *Whatsapp* (Informasi pendukung (testimoni jual beli online) yang bersumber dari direktori ***Phone/Storage/GBWhatsapp/Databases/ msgstore.db.*** dan ditemukan dalam kondisi *file* terenkripsi *(crypt12),* dan temuan kedua berupa Isi percakapan aplikasi *Whatsapp* yang terhapus (Kesepakatan jual-beli korban dan tersangka) dengan sumber temuan yang sama *: **Phone/Storage/GBWhatsapp/Databases/ msgstore.db.*** dan dalam kondisi terenkripsi. Penemuan barang bukti percakapan Whatsaap pada skenario 1 dengan korban bernama Oki Pratama dan Skenario 2 dengan korban bernama Toni dijelaskan lebih rinci pada Tabel 5.

Tabel 5. Hasil Temuan BB Sekenario 1 dan 2 (Sumber *GBWhatsapp*)

HASIL TEMUAN BARANG BUKTI DIGITAL						
No Skenario	Nama Korban	Pelaku	Percakapan Whatsapp	Percakapan Whatsapp Terhapus	Sumber Temuan	Keterangan
Skenario 1	Oki Pratama	Koko Saputro	Ya	Ya	*Phone/Storage/GBWhatsapp/Databases/msgstore.db*	Terenkripsi (Crypt12)
Skenario 2	Toni	Koko Saputro	Ya	Tidak dilakukan penghapusan	*Chating Whatsapp dipercakapan smartphone tizen dan msmgstore.db*	Terenkripsi (Crypt12)

Dari hasil analisa seperti tabel 5. bahwa pada skenario 1 ditemukan bukti yang memberatkan pelaku bernama Koko Saputro yaitu percakapan transaksi penipuan *online* kepada korban bernama Oki Pratama, temuan yang diperoleh adalah percakapan *whatsapp* yang sudah terhapus yang bersumber dari ***Phone/Storage/GBWhatsapp/Databases/ msgstore.db.*** Kemudian untuk Sekenario 2 dengan korban bernama Toni, Barang bukti yang belum sempat dilakukan penghapusan ditemukan didirectori yang sama yaitu pada *file massages.db* pada *storage smartphone tizen* milik pelaku.

5. KESIMPULAN

Setelah peneliti melakukan rangkaian penelitian dan analisa terhadap sebuah apilikasi sosial media *WhatsApp* dan fitur *SMS* pada perangkat *smartphone tizen*, dapat diambil kesimpulan bahwa :

1. Percakapan yang ditemukan pada *smartphone* pelaku terbatas pada percakapan yang belum terhapus. Untuk mendapatkan percakapan yang sudah terhapus digunakan aplikasi pendukung berupa *tools whatsapp viewer* untuk membantu melakukan *decript database whatsApp* yang terenkripsi agar percakapan yang terhapus bisa terbaca.
2. Berdasarkan analisa terhadap data hasil men-decript atau pembedahan *database WhatsApp* yang telah dihapus, terdapat data percakapan yang menunjukan bahwa korban melakukan penipuan jual-beli *online*, dengan cara memberikan harga yang murah kepada korbanya. Transaksi penjualan selalu sukses untuk para pelanggan yang baru membeli pertama kalinya. Akan tetapi, untuk pembelian berikutnya atau pembelian kedua, pelaku meminta transfer uang terlebih dahulu kepada pembeli dengan pembayaran penuh, namun setelah uang dikirim kepada penjual, ternyata pelaku tidak mengirimkan pesanan yang sudah dibayar, tetapi pelaku kabur untuk menghilangkan jejak.
3. Berdasarkan analisa terhadap data *capturing smartphone tizen* pada *smartphone* milik pelaku terdapat data percakapan pendukung kelancaran transaksi penipuan jual-beli *online* yang menunjukan bahwa korban melakukan *SMS* kepada pelaku saat pelaku kehabisan paket data internet. Jadi pada percakapan SMS yang ditemukan haya sebatas pendukung transaksi untuk transaksi sepenuhnya dilakukan melalui percakapan *Whatsapp.*

DAFTAR PUSTAKA

DEDI HARIYADI. (2016). Purwapura Forensik BBM di telepon selular Android Mengunakan IGN-SDK. Retrieved from https://www.slideshare.net

H. JAYGARL, C. LUO, Y. KIM, E. CHOI, K. BRADWICK, AND OTHERS. (2014). Professional Tizen Application Development.

Kim, M., Lee, S., & Won, Y. (2014). IO Workload Characterization of Tizen Based Consumer Electronics. *Proceedings of IEEE International Symposium on Consumer Electronics*, 3–6

KUNCORO, A. P., & LUTHFI, A. (2017). Mobile Forensics Development of Mobile Banking Application using Static Forensic. *International Journal of Computer Applications (0975 – 8887), Volume 160*(1), 5–10.

LIZARTI, N., SUGIANTORO, B., & PRAYUDI, Y. (2017). Penerapan Composite Logic alam Mengkolaborasikan Framework Terkait Multimedia Forensik. *Magister Teknik Informatika Universitas Islam Indonesia, Teknik Informatika UIN Sunan Kalijaga Yogyakarta*, (August). http://doi.org/10.14421/jiska.2017.21-04

LONE, A. H., BADROO, F. A., & CHUDHARY, K. R. (2015). Implementation of Forensic Analysis Procedures for WhatsApp and Viber Android Applications. *International Journal of Computer Application*, *128*(12), 26–33.

MATULAC, J. S. (2016). Case Study of Tizen Operating System, (January), 06. http://doi.org/10.13140/RG.2.1.1805.1606

MUMBA, EMILIO RAYMOND & VENTER, H. S. (2014). Mobile Forensics using the Harmonised Digital Forensic Investigation Process. *IEEE*.

Song, D., Zhao, J., Burke, M., Wallach, D., & Sarkar, V. (2015). Finding Tizen security bugs through whole-system static analysis, *1*, 15.

SUDYANA, D., SUGIANTORO, B., & LUTHFI, A. (2016). Instrumen Evaluasi Framework Investigasi Forensika Digital menggunakan SNI 27037:2014. *Magister Teknik Informatika UII, Teknik Informatika UIN Sunan Kalijaga Yogyakarta*, Vol. *1 No.2*(November), 75–83.