

PROSES INVESTIGASI MOBILE FORENSIK PADA SMARTPHONE BERBASIS IOS

INVESTIGATION PROCESS MOBILE FORENSICS ON SMARTPHONE IOS BASED

¹ Sidik Madiyanto, ² Husni Mubarak, ³ Nur Widiyasono

^{1,2,3} Teknik Informatika Fakultas Teknik Universitas Siliwangi Tasikmalaya
Jl. Siliwangi No. 24 Kota Tasikmalaya 46115

¹sidik_madiyanto@student.unsil.ac.id, ²husni.mubarak@unsil.ac.id, ³nur.widiyasono@unsil.ac.id

Abstrak— Ponsel merupakan salah satu teknologi yang sering digunakan oleh manusia dalam kegiatan sehari-hari. Tujuan utamanya adalah orang yang menggunakan ponsel untuk berkomunikasi dengan orang lain. Bentuk komunikasi melalui udara dapat tujuan bervariasi, dari yang hanya berbicara tentang hal-hal sederhana sampai hal-hal yang serius, misalnya tentang pekerjaan dan kegiatan positif dan negatif. Ini bisa menjadi bentuk negatif dari percakapan tentang rencana untuk kejahatan seperti pembunuhan, perampokan, pemerasan, korupsi dan narkoba. Analisis forensik digital dan peneliti harus dapat mengantisipasi hal-hal ini, sehingga ketika ada bukti ponsel yang disita dari para pelaku dapat diperiksa dengan baik sesuai dengan prinsip-prinsip dasar forensik digital. Penelitian ini menggunakan DFIF (Digital Forensik Investigasi Framework) dalam penyelidikan perangkat smartphone dengan mencari bukti berupa percakapan digital melalui pesan teks. Hasil investigasi yang dilakukan dalam bentuk informasi untuk membuktikan bahwa pelaku tindak pidana, informasi tersebut kemudian disajikan dalam bentuk laporan forensik yang akan digunakan selama persidangan.

Kata kunci: Bukti, Digital, DFIF, Investigasi, IOS, Smartphone

Abstract— Mobile phone is one of high technology is now used by humans. The main objective people using mobile phones to communicate with others. Form of communication through the air can be varied objectives, which just talking about simple things until serious things, for example talking about work and activities both positive and negative. This could be a negative of a conversation about the plans for a crime such as murder, robbery, extortion, corruption and drug dealing. Analysis of digital forensics and investigators should be able to anticipate these things, so when there is evidence of mobile phone, which was confiscated from the perpetrators, can be checked properly in accordance with the basic principles of digital forensics. This study uses DFIF (Digital Forensics Investigation Framework) in the investigation of smartphone devices by looking for evidence in the form of digital conversation via text message. The results of investigations carried out in the form of information to prove that the perpetrator of a criminal act, the information is then presented in the form of a forensic report that will be used during the court.

Keywords: Digital, DFIF, Evidence, Investigation, IOS, Smartphone.

I. PENDAHULUAN

Perkembangan teknologi komunikasi sudah sangat pesat merambah ke semua lapisan, sehingga dalam beberapa aspek sudah mengubah pola kehidupan masyarakat. Perkembangan teknologi

salah satunya adalah munculnya *smartphone*, benda yang sangat pintar yang dapat digunakan berbagai macam hal oleh penggunanya. *Smartphone* dapat digunakan sebagai asisten pribadi, karena dapat menyimpan berbagai macam dokumen maupun data pribadi. *Smartphone* dilengkapi berbagai macam aplikasi untuk keperluan telepon, sms (*short message service*), *chat*, *email*, media sosial dan aplikasi-aplikasi lain [1].

Smartphone dapat digunakan sebagai alat *cybercrime* dengan berbagai fitur yang tersedia di dalamnya. Pelaku *cybercrime* memanfaatkan *smartphone* sebagai alat komunikasi untuk membantu melakukan kejahatan. Pelaku kasus pengedaran narkoba dapat menggunakan *smartphone* dalam melakukan komunikasi antara pengedar dengan bandar narkoba, hal ini termasuk ke dalam *cybercrime* karena menggunakan media elektronik *smartphone* dalam melakukan kejahatan sesuai dengan undang-undang ITE (Informasi dan Transaksi Elektronik) no. 11 tahun 2008.

Penemuan barang bukti berupa *smartphone* yang dipakai oleh pelaku dapat dijadikan barang bukti yang sah di pengadilan. Pemeriksaan terhadap *smartphone* menggunakan ilmu *mobile forensics* dengan melakukan akuisisi perangkat *mobile* tersebut untuk mencari histori atau *logs* yang terkait dengan komunikasi para pelaku pengedaran narkoba.

Penelitian ini menggunakan skenario kasus kejahatan narkoba, menurut pasal 112 KUHP tidak diperkenankan menggunakan kasus asli dalam melakukan penelitian ilmiah karena catatan kasus kejahatan bersifat sangat rahasia. Proses investigasi pada *smartphone* menggunakan ilmu *mobile forensics* dengan *tools Magnet AXIOM* akan membantu kepolisian untuk mencari bukti digital pada *smartphone* terkait kasus pengedaran narkoba, hal ini menjadi daya tarik tersendiri untuk dijadikan penelitian yang nantinya diharapkan akan membantu kepolisian dalam mencari bukti tambahan kasus pengedaran narkoba.

A. Rumusan masalah

Permasalahan yang terjadi dapat diketahui dalam hal-hal berikut ini :

1. Bagaimana proses investigasi *mobile* forensik *smartphone* berbasis ios?
2. Bagaimana potensi bukti digital yang terdapat pada *smartphone* berbasis ios?

B. Batasan masalah

Batasan masalah pada penelitian Proses Investigasi *Mobile Forensics* Pada *Smartphone* Berbasis IOS ini yaitu :

1. Penelitian ini tidak membahas prosedur hukum kasus pencedaran narkoba.
2. Investigasi hanya dilakukan pada *smartphone* berbasis *ios* *iphone 3gs* (*ios* 6.16), dan *iphone 5* (*ios* 10.1.1).
3. Penelitian ini tidak membahas *smartphone* dengan *password*, karena membutuhkan alat forensik khusus untuk membuka *password* tersebut.
4. Investigasi pada *smartphone* *iphone 3gs*, dan *iphone 5* tidak dilakukan *jailbreak*.
5. Fokus penelitian ini mencari bukti digital yang terkait dengan komunikasi pelaku untuk melakukan transaksi narkoba.
6. Tidak membahas anti forensik.

C. Tujuan penelitian

Tujuan penelitian ini adalah :

1. Mengetahui proses investigasi *mobile* forensik *smartphone* berbasis *ios*?
2. Mengetahui potensi bukti *data digital* yang terdapat pada *smartphone* berbasis *ios*?

D. Manfaat penelitian

Manfaat yang diharapkan dari penelitian ini adalah :

1. Membantu pihak kepolisian untuk mengidentifikasi temuan barang bukti berupa *smartphone* berbasis *ios* yang digunakan pelaku untuk melakukan tindak kejahatan pencedaran narkoba.
2. Penemuan barang bukti berupa *smartphone* berbasis *ios* dapat digunakan sebagai barang bukti tambahan yang sah di pengadilan.
3. Melakukan data akuisisi pada *smartphone* berbasis *ios*.
4. Melakukan analisis terhadap hasil akuisisi yang berpotensi menjadi barang bukti digital.
5. Sebagai bahan referensi atau acuan untuk penelitian berikutnya.

Merujuk masalah tersebut, maka diperlukan metode untuk menangani kasus kejahatan *cyber*, yaitu dengan menggunakan teknik *mobile* forensik untuk menganalisa dan menelusuri bukti-bukti digital yang digunakan oleh pelaku tindak kejahatan.

II. STUDI LITERATUR

A. *Digital Forensic*

Digital Forensics adalah suatu disiplin ilmu turunan keamanan komputer yang membahas tentang temuan bukti digital setelah suatu peristiwa terjadi. Kegiatan *digital forensics* sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa dan mempergunakan bukti digital menurut hukum yang berlaku [2]. *ECCouncil*, *Digital forensics* menyatakan bahwa aplikasi ilmu komputer untuk pencarian kepastian hukum bagi perbuatan criminal dan sejenisnya. Ilmu *Digital forensics* terdapat prinsip-prinsip dasar. Prinsip dasar *Digital forensics* menurut *ACPO* antara lain [3]:

1. Lembaga hukum dan atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya dibawa ke pengadilan.
2. Seseorang yang merasa perlu mengakses data digital yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
3. Catatan teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan dan analisa berlangsung, jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut mendapatkan hasil yang sama.

Penanggung jawab dari investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

B. *Mobile Forensics*

Mobile device forensics merupakan ilmu yang melakukan proses *recovery* bukti digital dari perangkat *mobile* menggunakan cara yang sesuai dengan forensik [4]. Forensik perangkat *mobile* merupakan forensik yang datanya diambil dari ponsel, dengan sendirinya bisa dijadikan sebagai bukti. Bukti – bukti ini bisa menjadi landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum.

Terdapat sejumlah bukti yang dapat diekstraksi dari ponsel. Jenis barang bukti yang dapat diekstraksi dari ponsel antara lain nomor kontak, log panggilan, pesan sms, file audio, *email* dan internet *history*. Artefak ini bisa diekstrak dengan metode *logic* maupun fisik. Secara *logic* adalah mengekstrak data dari *file* sistem dengan langsung berinteraksi dengan perangkat menggunakan *tools* atau *software* khusus untuk *mobile device forensics*.

Pengembang *tool* forensik menggunakan metode yang berbeda untuk mendapatkan akses memori pada ponsel [5]. *International Organization of Computer Evidence* (IOCE) menyatakan bahwa bukti digital adalah informasi yang disimpan atau ditransmisikan dalam bentuk biner yang dapat diandalkan di pengadilan. [6] juga menegaskan bahwa bukti digital sebagai benda fisik yang dapat menetapkan bahwa kejahatan telah dilakukan, dapat memberikan hubungan antara kejahatan dan korbannya atau dapat menyediakan *link* antara kejahatan dan pelakunya. Empat elemen kunci forensik adalah sebagai berikut [7]:

1. Identifikasi dari bukti digital

Merupakan tahap paling awal forensik dalam teknologi informasi. Tahapan ini dilakukan identifikasi di mana bukti itu berada, di mana bukti itu disimpan dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya.

2. Penyimpanan bukti digital

Termasuk tahapan yang paling kritis dalam forensik. Tahapan ini, bukti digital dapat saja hilang karena penyimpanannya yang kurang baik.

3. Analisa bukti digital

Pengambilan, pemrosesan dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital

4. Presentasi bukti digital

Proses persidangan di mana bukti digital diuji otentifikasi dan korelasi dengan kasus yang ada. Tahapan yang harus dilakukan oleh investigator untuk melindungi bukti adalah *the chain of custody*. Istilah tersebut mengandung arti bahwa pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi. Tujuan dari *the chain of custody* adalah :

- a. Bukti itu benar-benar masih asli
- b. Bukti masih bisa dikatakan seperti saat ditemukan pada saat persidangan. (biasanya jarak antara penyidikan dan persidangan relatif lama)

C. Tools mobile forensic

Mobile Forensik merupakan bidang yang relatif baru di area forensik digital, sehingga perangkat lunak dan *tool* yang bisa digunakan untuk mengambil data dari ponsel masih relatif baru. *Tool* ekstraksi bisa berupa *hardware* atau *software* tergantung kebutuhan pada saat data diekstrak dari perangkat *mobile*. *Tool* yang ada kebanyakan merupakan *tool* komersial dan ada juga sedikit yang berupa *tool open source*, akan tetapi pengadaan *tool-tool* ini cukup sulit didapatkan terkait masalah privasi dan masalah keamanan serta biaya yang dibutuhkan. *Tool* ekstraksi dalam penelitian ini menggunakan *Magnet AXIOM*.

III. METODOLOGI PENELITIAN

Tahapan berdasarkan landasan teori dan studi pustaka, langkah-langkah dalam menentukan komponen-komponen penelitian dengan metode penelitian dalam investigasi *mobile forensik smartphone* berbasis *ios*. Tahapan-tahapan tersebut dapat dilihat pada gambar 1.



Gambar 1. Alur Penelitian

A. Literature Reviews

Tahapan *literature reviews* mengumpulkan data-data dari penelitian sebelumnya mengenai digital forensik untuk mendapatkan tahapan investigasi *smartphone* berbasis *ios* dengan bahan-bahan yang sudah ada dan dapat mempelajari dari membaca buku atau referensi lainnya.

Informasi *literature reviews* diambil dari paper, jurnal yang sudah masuk jurnal nasional dan internasional yang dapat dipercaya.

Penelitian-penelitian terdahulu yang berkaitan dengan digital forensik dan *mobile forensik* dapat dijadikan bahan acuan untuk penelitian ini sebagai acuan peneliti menginvestigasi *smartphone* berbasis *ios*.

B. Observation & Data Collection

Penelitian ini menggunakan *hardware* dan *software* untuk mendukung proses investigasi *mobile forensik*, dalam skenario kasus penelitian ini dijelaskan bahwa tertangkapnya bandar dan pengedar narkoba mempunyai *smartphone* berbasis *ios* yang dijadikan barang bukti, kemudian *smartphone* tersebut akan di investigasi untuk mencari potensi barang bukti digital yang terdapat pada *smartphone* tersebut menggunakan *laptop* yang telah terpasang *software Magnet AXIOM*. *Hardware* yang digunakan dalam penelitian ini berupa *laptop* dan *smartphone* berbasis *ios*.

TABEL I
SPESIFIKASI HARDWARE

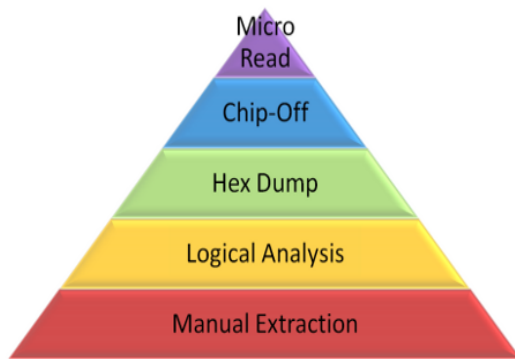
| No. | Nama Hardware | Spesifikasi |
|-----|-------------------------|--|
| 1. | Laptop DELL Vostro 3350 | Computer Name : Sansan-PC Operating System : Windows 7 Ultimate 64-bit (6.1, Build 7601) Processor : Intel® Core™ i3-2350M Memory : 5120MB RAM |
| 2. | Smartphone Iphone 3Gs | Nama : Ucok Kapasitas : 6.2 GB Versi : 6.1.6 Operator : Telkomsel Model : MC637PA/A No. Seri : 86219NDHEDG IMEI : 012992005311265 |
| 3. | Smartphone Iphone 5 | Nama : Jarot iphone's Kapasitas : 13.11 GB Versi : 10.2 Operator : Carrier Model : ND293LL/A No. Seri : DNQK512XDTTN IMEI : 01342600398659 |

Hardware di atas akan digunakan sebagai bahan investigasi *mobile forensik* untuk mencari potensi bukti digital yang terdapat pada *smartphone* tersebut menggunakan *software Magnet AXIOM*. Penelitian ini menggunakan *software Magnet AXIOM* untuk mengakuisisi perangkat *smartphone* berbasis *ios* untuk mencari potensi bukti digital yang terdapat pada *smartphone*.

C. Extraction Model

Tahapan *extraction model* merupakan tahapan penentuan model ekstraksi yang akan digunakan dalam penelitian ini. *Extraction model* melibatkan alat yang akan dipakai untuk pemeriksaan *smartphone*. Tujuan dari klasifikasi sistem alat *mobile device forensics* adalah untuk memungkinkan pemeriksa / investigator untuk mengkategorikan alat forensik berdasarkan metodologi pemeriksaan alat. Metode dan alat umumnya menjadi lebih teknis, kompleks, dan memerlukan waktu analisis lebih lama. Bukti dapat dihancurkan sepenuhnya oleh pelaku kejahatan, oleh sebab itu pemilihan model ekstraksi menentukan keberhasilan pemeriksaan *mobile device forensics*. Model ekstraksi dari perangkat ponsel dibagi menjadi lima tahapan, yaitu *Manual*, *Logical*, *Hex Dump*, *Chip-Off*, *Micro Read* yang dapat dilihat pada gambar 2. Penelitian ini menggunakan model ekstraksi *logical analysis* karena

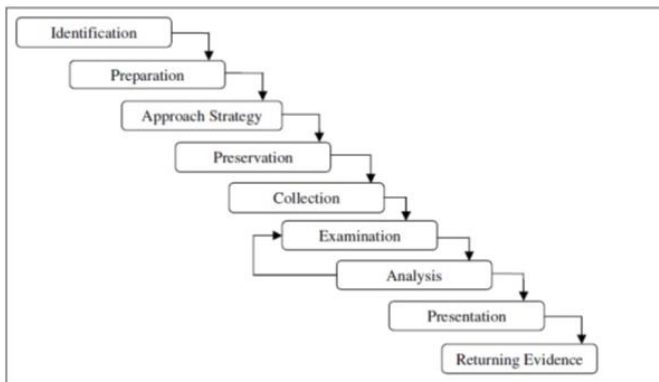
barang bukti yang disita dari pelaku merupakan *smartphone* yang masih utuh dan dapat berjalan normal dan tanpa adanya *passcode*, sehingga model ekstraksinya menggunakan *logical analysis*.



Gambar 2. Model Ekstraksi *Mobile Forensics*

D. Investigation

Tahapan berdasarkan hasil *literature reviews*, langkah-langkah dalam menentukan komponen penelitian dengan metode DFIF (*Digital Forensics Investigation Framework*) dalam investigasi *mobile forensik smartphone* berbasis *ios*. Tahapan DFIF yaitu *Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation* dan *Returning Evidence* yang dapat dilihat pada gambar 3. Penelitian ini menggunakan metode DFIF (*Digital Forensics Investigation Framework*) sebagai metode investigasi *smartphone* berbasis *ios*.



Gambar 3. Metode DFIF

E. Documentations

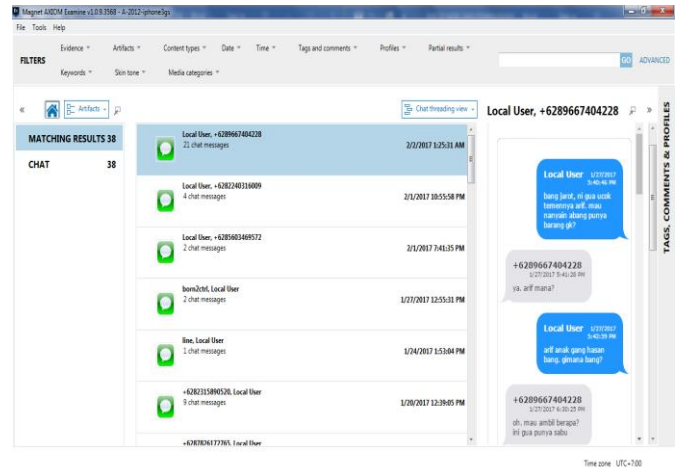
Tahapan dokumentasi merupakan tahapan penjelasan secara keseluruhan terhadap tindak kejahatan pengedaran narkoba yang telah dilakukan akuisisi data kemudian dilakukan pemeriksaan data digital untuk menemukan korelasi antara bukti digital yang relevan.

IV. HASIL DAN ANALISIS

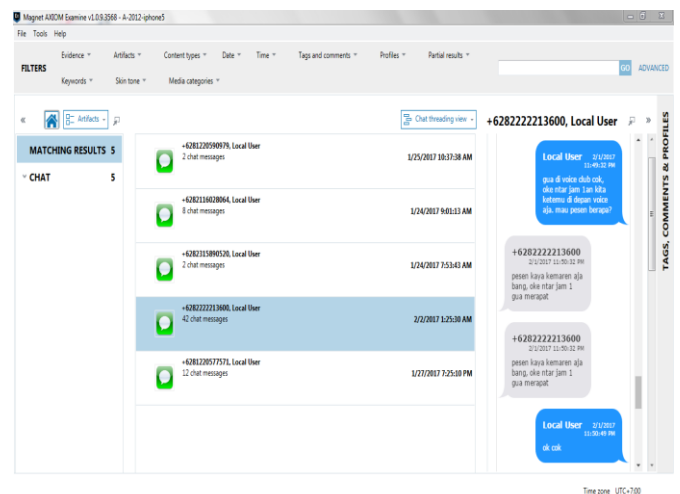
Hasil yang didapatkan setelah dilakukannya tahapan-tahapan penelitian, kemudian dikemukakan dalam pembahasan berikut ini. Barang bukti digital yang ditemukan pada *smartphone iphone 3Gs* dan *iphone 5* berupa percakapan pesan singkat yang diduga berisi

tentang transaksi narkoba antara pengedar narkoba, pemakai narkoba dan bandar narkoba.

Barang bukti yang telah diperiksa mendapatkan hasil berupa percakapan pesan singkat / *sms* antara pelaku pengedar narkoba dan bandar narkoba, pada tanggal 27 Januari 2017 pukul 05:40 *PM* pengedar narkoba mengirim pesan pertama kepada bandar narkoba dengan mengaku sebagai rekannya berinisial a yang berisi pertanyaan mengenai ketersediaan barang yang diduga narkoba kepada bandar narkoba, kemudian bandar narkoba menyebutkan mempunyai narkoba jenis sabu-sabu kepada pengedar narkoba. Pengedar narkoba memesan sabu-sabu sejumlah 3 kantong dengan masing-masing kantong diisi 1 kantong 250 gram dan 2 kantong 125 gram, kedua pelaku kemudian melakukan transaksi jual-beli narkoba di *voice club* pada pukul 11 malam.



Gambar 4. Barang Bukti Digital Pada *Smartphone Iphone 3Gs*

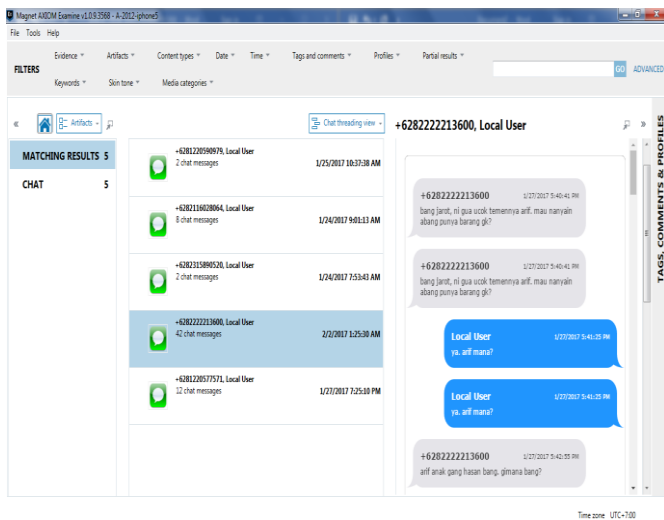


Gambar 5. Barang Bukti Pada *Iphone 5*

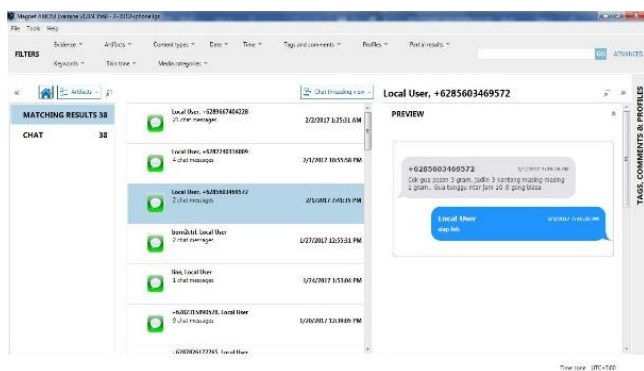
Barang bukti digital yang ditemukan pada *iphone 5* terdapat percakapan pada pesan singkat antara pengedar narkoba dengan bandar narkoba. Hasil analisis bukti digital menunjukkan bahwa percakapan tersebut merupakan percakapan kali kedua antara pengedar narkoba dengan bandar narkoba. Pengedar narkoba pada tanggal 1 Februari 2017 pukul 11:43 *PM* mengirim pesan kepada

bandar narkoba untuk memesan narkoba jenis sabu-sabu berjumlah sama dengan yang pertama kali di pesan oleh pengedar narkoba, kemudian kedua pelaku berencana melakukan transaksi ditempat yang sama pada pukul 1 malam. Barang bukti digital yang terdapat pada *smartphone iphone 5* dicocokkan dengan barang bukti digital yang terdapat pada *smartphone iphone 3Gs*, pada *iphone 3Gs* percakapan dimulai pada tanggal 27 Januari 2017 pukul 05:40 PM dan *iphone 5* percakapan dimulai pada tanggal 27 Januari pukul 05:40 PM.

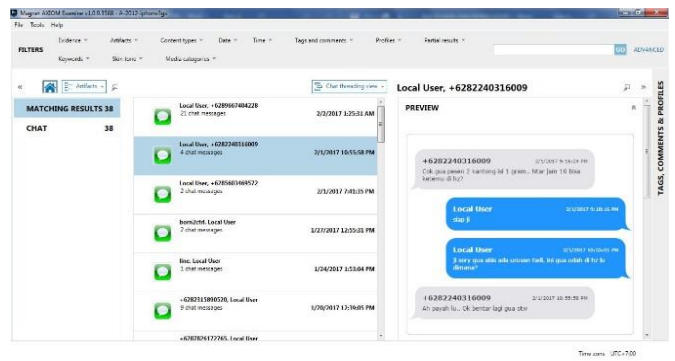
Hasil investigasi menyatakan bahwa benar *smartphone iphone 3Gs* merupakan barang bukti yang digunakan oleh pengedar narkoba dan *smartphone iphone 5* merupakan barang bukti yang digunakan oleh bandar narkoba. Barang bukti pendukung lainnya terdapat pada percakapan *iphone 3Gs* yang berisi pemesanan narkoba jenis sabu-sabu sejumlah 2 paket yang masing-masing berisi 1 gram sabu-sabu, hal ini menunjukkan bahwa barang yang dipesan oleh seseorang yang berinisial f jauh lebih sedikit dibandingkan sabu-sabu yang dipesan oleh u kepada j. Pelaku pengedar narkoba melakukan transaksi pada hari yang sama dengan seseorang berinisial p sejumlah 2 kantong yang berisi masing-masing 1 gram pada pukul 10.55 PM yang sebelumnya telah melakukan transaksi dengan seseorang yang berinisial f



Gambar 6. Kesesuaian Percakapan Pengedar Narkoba dan Bandar Narkoba



Gambar 7. Barang Bukti Pendukung Pada *Iphone 3Gs*



Gambar 8. Barang Bukti Transaksi Pada *Iphone 3Gs*

Proses presentasi terhadap barang bukti digital pada kedua *smartphone* pelaku dengan menampilkan *timeline* yang dibuat berdasarkan *timestamp* yang terdapat pada artefak bukti digital pesan singkat dan telepon.

TABEL II
TIMELINE BUKTI DIGITAL

| No. | Timestamp | Bukti Digital | Peristiwa |
|-----|-----------------------------|---|--|
| 1. | 27-01-2017 (05:40:46 PM) | Sms pengedar narkoba dan bandar narkoba pada <i>smartphone</i> pengedar narkoba | Pengedar narkoba berinisial u melakukan pemesanan narkoba jenis sabu-sabu kepada bandar narkoba berinisial j |
| 2. | 01-02-2017 (07:39:26 PM) | Sms pengedar narkoba dan pemakai narkoba pada <i>smartphone</i> pengedar narkoba | Pemakai narkoba berinisial f mengirim pesan kepada pengedar narkoba dengan membeli narkoba jenis sabu-sabu. |
| 3. | 01-02-2017 (09:16:24 PM) | Sms pengedar narkoba dan pemakai narkoba pada <i>smartphone</i> pengedar narkoba | Pemakai narkoba berinisial p mengirim pesan kepada pengedar narkoba dengan membeli narkoba jenis sabu-sabu sejumlah 2 kantong. |
| 4. | 27-01-2017 (05:40:46 PM) | Sms pengedar narkoba dan bandar narkoba pada <i>smartphone</i> pengedar narkoba | Pengedar narkoba berinisial u melakukan pemesanan narkoba jenis sabu-sabu kepada bandar narkoba berinisial j |
| 5. | 27-01-2017 (06:18:05 PM) | Sms bandar narkoba dan rekan berinisial a pada <i>smartphone</i> bandar narkoba | Bandar narkoba melakukan konfirmasi kepada rekannya yang berinisial a untuk memastikan identitas pengedar narkoba |
| 6. | 03-02-2017 (06:17:28 PM) | Telepon bandar narkoba dan pengedar narkoba pada <i>smartphone</i> bandar narkoba | Bandar narkoba melakukan panggilan kepada pengedar narkoba pada pukul 06:17 PM dengan durasi 22 detik |

Barang bukti berupa percakapan pesan singkat dan telepon yang telah dicocokkan menurut timestamp antara bandar narkoba berinisial j dan pengedar narkoba berinisial u menunjukkan bahwa kedua pelaku telah memanfaatkan *smartphone* sebagai media komunikasi untuk melakukan transaksi narkoba.

V. KESIMPULAN

Hasil penelitian yang diambil dari kesimpulan investigasi *smartphone* berbasis *ios* pada *iphone 3Gs* dan *iphone 5* menunjukkan bahwa pelaku melakukan tindak kejahatan menggunakan *smartphone* sebagai media komunikasi untuk melakukan transaksi narkoba. Proses investigasi menggunakan metode DFIF dengan tahapan *identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation* dan *returning evidence*. Pemeriksaan *smartphone* menggunakan *software Magnet AXIOM* untuk menemukan potensi bukti digital yang terdapat pada *smartphone* berbasis *ios* berupa *history sms, imessage, call logs, camera pictures, ringtones, address book, geolocation, wifi hotspot, voicemail, email, dan web history*. Fokus pencarian dilakukan pada artefak *sms* dan telepon yang dimanfaatkan oleh pelaku kejahatan sebagai media komunikasi untuk melakukan transaksi narkoba. Terdapat saran-saran yang dapat diberikan setelah proses penelitian tugas akhir ini adalah sebagai berikut :

1. Menggunakan *tools* UFED Cellebrite Physical Analysis untuk melakukan ekstraksi karena telah teruji oleh *CFTT (Computer Forensics Testing Tools)*.
2. Menggunakan *hardware forensics* untuk melakukan ekstraksi karena memungkinkan untuk di pakai di TKP (Tempat Kejadian Perkara).

DAFTAR PUSTAKA

- [1] Kohar Abdul. 2015. Analisis Kesadaran Pengguna *Smartphone* Terhadap Aktivitas *Cybercrime*. Tesis, tidak diterbitkan. Yogyakarta: Fakultas Teknologi Industri Universitas Islam Indonesia.
- [2] Asrizal. 2012. Digital Forensik. E-Dokumen Kemenag.
- [3] Yudha Fietyata. 2013. *Usb Analysis Tool* Untuk Investigasi Forensika Digital. Jurnal, telah diterbitkan. Yogyakarta: Fakultas Teknologi Industri Universitas Islam Indonesia.
- [4] W. Jansen. 2007. *Guidelines on Cell Phone Forensics*.Jurnal, diterbitkan. NIST (*National Institute of Standards and Technology*).
- [5] McCharthy Paul. 2005. *Forensic Analysis of Mobile Phones*. Tesis, diterbitkan. Australia: School of Computer and Information Science University of South Australia.
- [6] E.C., Turnbull. 2000. *Digital Evidence and Computer Crime*. Academia Press
- [7] Budiman Rahmadi. 2003. Tugas Keamanan Sistem Lanjut, Komputer Forensik Apa Dan Bagaimana. Makalah, tidak diterbitkan.Bandung: Teknik Elektro Option Teknologi Informasi Institut Teknologi Bandung
- [8] Pasal 112 KUHP (Kitab Undang-Undang Hukum Pidana).UU ITE No. 11 Tahun 2008.