CyberSecurity dan Forensik Digital e-ISSN: 2615-8442

Vol. 2, No. 1, Mei 2019, hlm. 30-37

PENGGUNAAN PERANGKAT *MOBILE* TERHADAP SUATU TINDAK KEJAHATAN (STUDI KASUS PADA TEMUAN BUKTI DIGITAL *SHORT MESSAGE SERVICE* (SMS) DI *UNALLOCATED DATA*)

Tommy Nugraha Manoppo

[1]Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Email: [1]tommynugrahamanoppo@gmail.com,

Abstrak

Penggunaan *mobile device* sudah menjadi bagian dari kehidupan sehari-hari manusia modern saat ini. Dan salah satu *mobile device* yang hampir dimiliki oleh sebagian besar pengguna *mobile device* adalah perangkat selular atau *mobile phone* termasuk didalamnya *smartphone*. Sebagai perangkat elektronik yang dapat menyimpan data, berbagai macam data, informasi yang tersimpan dari data pada *mobile phone* dapat mencerminkan aktivitas penggunanya. Sehingga informasi yang diperoleh dari *mobile phone* dapat dijabarkan secara kronologi kejadian jika dibutuhkan. Pada penelitian ini, terdapat studi kasus mengenai penanganan dan temuan bukti digital berupa *short message services* (SMS) yang diperoleh pada *unallocated data* di sebuah *smartphone* android. Dengan melakukan pengujian secara praktikal terhadap prosedur penanganan *mobile devices*, hasil yang diperoleh memperlihatkan bahwa langkah dan tahapan dalam penanganan bukti berupa *mobile devices* dapat dijalankan secara dinamis, dalam artian ada beberapa tahapan prosedural yang dapat dijalankan secara bersamaan, tetapi tahapan aktivitas dapat dijalankan secara teratur, sehingga hasil temuan memiliki unsur *forensically sound* atau dapat dibuktikan secara ilmiah dengan tahapan yang jelas.

Kata kunci: *Mobile Device, Mobile Phone, SMS, bukti digital, prosedural penanganan, forensically sound.*

MOBILE DEVICE NEAR ON CRIME SCENE (A CASE STUDY FINDINGS SHORT MESSAGE SERVICE (SMS) AS A DIGITAL EVIDENCE IN UNALLOCATED DATA)

Abstract

Mobile devices usage has become a part of daily life modern humans today. And one of mobile devices that is almost owned by mobile devices users is mobile phone, including a smartphones. As an electronic devices that can store data, even various kinds of data types, that information stored from data on mobile phone can reflect the user's activity. So the information can be described as a chronologically if needed. In this study, there are case studies about findings and handlings of digital evidence form of Short Message Services (SMS) that obtained on unallocated data in an android smartphone. By practically testing the procedures, the results show that steps and stages used for handling mobile devices evidence could be run dynamically, in the sense that, there are several procedural steps can be run as simultaneously, but the activity stages could be run regularly too. So the artefacts has a forensically sound elements and can be proven as a scientific with the clear stages.

Keywords: *Mobile Device, Mobile Phone, SMS, digital evidence, handling procedural, forensically sound.*

1. PENDAHULUAN

Penggunaan *mobile device* sudah menjadi bagian dari kehidupan sehari-hari manusia modern saat ini. (Reiber, 2016) menjelaskan bahwa semenjak tahun 2003, jumlah *mobile device* telah mencapai 3 : 1 dari jumlah perangkat komputer desktop yang ada. Sehingga jika dianalogikan terdapat sebanyak seratus ribu dekstop di dunia, maka akan ada sebanyak tiga-ratus ribu *mobile devices*. Tetapi jauh lebih besar dari analogi tersebut, (Hootsuite, 2018) memaparkan fakta bahwa pengguna perangkat *mobile* di tahun 2018 telah mencapai 5,135 Miliar. Dan salah satu *mobile device* yang hampir dimiliki oleh sebagian besar pengguna *mobile device* adalah perangkat selular atau *mobile phone* termasuk didalamnya *smartphone*.

Tidak ada perangkat elektronik lain yang sangat melekat dengan aktivitas sehari-hari penggunanya, baik dalam pekerjaan ataupun untuk urusan pribadi selain daripada *mobile phone*. Sebagai perangkat elektronik yang dapat menyimpan data, berbagai macam data, informasi yang tersimpan dari data pada *mobile phone* dapat mencerminkan aktivitas penggunanya, lebih secara khusus dapat memaparkan pikiran ataupun tindakan penggunanya secara substansional atau secara realitas adanya. Sehingga informasi yang diperoleh dari *mobile phone* dapat dijabarkan secara kronologi kejadian jika dibutuhkan. Misalnya informasi yang diperoleh dari data riwayat aktivitas kunjungan dari *web browser* yang digunakan. Informasi seperti ini seringkali berpotensi menjadi sumber bukti dalam pengungkapan suatu kasus tindak kejahatan.

Pada penelitian ini, terdapat studi kasus mengenai penanganan dan temuan bukti digital berupa *short message services* (SMS) yang diperoleh pada *unallocated data* di sebuah *smartphone* android. Sehingga dengan adanya studi kasus tersebut pada penelitian ini, diharapkan dapat mewakili untuk menguji cakupan secara praktikal mengenai standar prosedural secara umum yang digunakan saat ini dalam penanganan *mobile devices*. Dengan pengujian secara praktikal terhadap prosedur penanganan *mobile devices*, maka akan diketahui apakah penanganan untuk pemerolehan bukti digital dengan menggunakan prosedural tersebut telah memenuhi standar metodologi secara ”*forensically sound*” atau terkualifikasi secara ilmiah, dalam arti lain, bersifat *repeatable* (dapat diulang dengan hasil yang sama) dan *defendable* (dapat dipertahankan integritasnya).

2. PERAN *MOBILE DEVICES* SEBAGAI BARANG BUKTI

Dalam proses pembuktian terhadap suatu kasus tindak kejahatan, *mobile devices* dapat memiliki dua peran, yakni sebagai alat langsung yang digunakan dalam tindak kejahatan itu sendiri ataupun dapat digunakan sebagai alat untuk pengungkapan kasus kejahatan tetapi tidak digunakan dalam proses kejahatan tersebut.

2.1. Sebagai Alat Langsung Dalam Suatu Tindak Kejahatan

(Duggal, n.d.) membagi *mobile crime* menjadi beberapa kategori sebagai berikut :

a. Mobile Hacking

Mobile Hacking didefinisikan sebagai adanya gangguan secara tidak sah pada sistem komputer dan/atau jaringan. Ataupun setiap tindakan untuk mengakses secara tidak sah keamanan suatu perangkat *mobile*. Termasuk didalamnya aktivitas *cracking* yang merupakan tindakan *hacking* yang merugikan baik secara materiil ataupun non-materiil.

b. Mobile Cyber Defamation

Mobile Cyber Defamation merupakan aktivitas pada *cyber-world* dengan menggunakan perangkat *mobile* yang memiliki tujuan untuk merendahkan, menghina dan mengirimkan kata-kata yang tergolong kasar yang mengandung unsur melecehkan dengan menggunakan *mobile devices* yang ditujukan kepada satu pihak atau kelompok.

c. Mobile Pornography

Sama dengan pengertian kasus tindak kejahatan seksual hanya saja media yang digunakan merupakan perangkat mobile. Baik melalui media sosial, *e-mail*, *video-chat*, *texting* (Pesan Singkat, termasuk SMS) dan media komunikasi lainnya.

d. Denial of Service Attack

Denial of Service (DoS) *Attack* merupakan jenis serangan terhadap suatu perangkat komputer termasuk *mobile devices* ataupun *server* di dalam jaringan internet dengan targetnya adalah *resource* pada sistem ataupun jaringan sehingga *resource* tidak dapat mengkases sistem, misalnya ”membanjiri” *traffic* jaringan dengan *bomb* data atau biasa disebut *traffic-flooding*.

e. Mobile Virus Dissemination

Mobile Virus Dissemination bertujuan untuk melakukan aktivitas penyebaran terhadap virus ataupun *malware* pada sistem ataupun perangkat

mobile melalui *fake-application*, *email*, dan media lainnya.

f. Mobile Phishing

Sama seperti aktivitas *phising* pada perangkat komputer, *phishing* terhadap *mobile devices* juga bermotif mengirimkan *fake-email* pada akun yang terkait di *mobile-devices*. Tujuan dari *Mobile Phishing* salah satunya adalah pencurian identitas (*identity theft*) atau informasi penting pada perangkat.

g. Mobile Cyber Stalking

Mobile Cyber Stalking seperti pada pengertiannya yakni ”menguntit” terhadap akun target, tetapi jauh lebih luas akan pengertiannya, *Mobile Cyber Stalking* merupakan kegiatan ”menguntit” yang dilakukan secara berulang-ulang terhadap target atau korban dengan tujuan melakukan pelecehan dan ancaman yang dapat merugikan korban tersebut.

h. Cloning or Re-Chapping of Mobile

Tujuan dari *Cloning* terhadap suatu perangkat *mobile* yang paling utama selalu terkait dengan pencurian identitas atau *identy theft*, dimana pelaku akan berpura-pura atau menduplikasi identitas korbannya untuk melakukan suatu tindak kejahatan yang terkait dengan data atau informasi korbannya tersebut. *Cloning* atau *Re-Chapping* pada perangkat *mobile* yang sering dilakukan yakni pada *SIM Card* korbannya ataupun langsung pada perangkat korbannya.

i. Identity Theft

Identity Theft atau pencurian identitas merupakan tindak kejahatan pada perangkat *mobile* yang paling sering ditemukan, baik secara motif kejahatan ataupun tujuan dari tindak kejahatan itu sendiri. Karena informasi yang terkandung pada identitas korban di perangkat *mobile*nya sangatlah bervariatif, seperti data akun *mobile banking*, informasi pribadi pada media sosial, *e-mail* dan lain sebagainya.

j. Mobile Software Piracy

Mobile Software Piracy bertujuan untuk melakukan pembajakan terhadap *software* ataupun aplikasi dengan cara memalsukan dan menyalin secara *illegal*, *source code* dari *software* atau aplikasi aslinya.

k. Mobile Credit Card Fraud

Fraud atau kejahatan dengan target ataupun tujuannya adalah mendapatkan keuntungan secara finansial. Banyak cara yang sering dilakukan untuk tujuan *fraud* pada *perangkat mobile*, salah satunya adalah pencurian identitas pada akun *credit card* yang tersimpan ataupun cache history di aplikasi *mobile bank* terkait.

2.2. Sebagai Alat Untuk Pengungkapan Kasus Tindak Kejahatan

(Reiber, 2016) menerangkan contoh yang sangat relevan, dimana *mobile device* dapat berperan dalam pengungkapan kasus tindak kejahatan. Pada tahun 2009 di *Bay Area Rapid Transit* (BART) salah satu negara bagian di Amerika Serikat terjadi keributan antar kelompok pemuda di daerah itu. Selang beberapa lama polisi berada dilokasi kejadian dan mengamankan beberapa pemuda yang terlibat keributan tersebut, kemudian salah satu polisi menembakkan peluru ke tubuh salah satu pemuda yang terlibat keributan tersebut hingga akhirnya meninggal dunia. Di lokasi kejadian merupakan wilayah yang tidak ter-*cover* oleh CCTV, sehingga menyulitkan pembuktian dalam proses persidangan. Setelah melakukan penyelidikan, pihak berwajib mendapatkan sekiranya enam rekamanan pada saat proses penembakan tersebut dari berbagai sudut dan sisi yang berbeda. Rekamanan dari *mobile device* para pengunjung di BART tersebut akhirnya mempermudah proses pembuktian dan menjadi bukti yang tidak dapat terbantahkan di pengadilan.

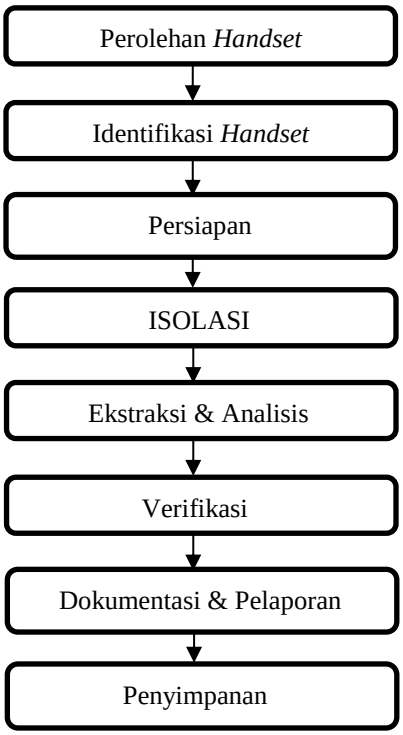
Berdasarkan contoh kasus nyata tersebut, menyadarkan kita mengapa ada-kalanya bukti digital dapat menjadi saksi yang sifatnya ”*real-time*” merekam proses kejadian yang krusial dan tidak terbantahkan. Ketika saksi merupakan manusia, terkadang banyak persepsi pada keterangannya, sehingga memang membutuhkan analisa dan pembelajaran yang lebih rumit dibandingkan jika bukti yang diperoleh merupakan rekaman dari berbagai sudut dan sisi di lokasi kejadian. Maka tugas dari *examiner* forensik untuk menemukan dan menjaga bukti digital agar integritasnya dapat dipertahankan di pengadilan.

3. PROSEDURAL PENANGANAN *HANDSET* PADA *MOBILE FORENSICS*

Perlunya mengikuti setiap tahapan atau *workflow* dalam prosedural penanganan barang bukti, khususnya pada bukti elektronik berupa mobile device atau yang lebih dikenal oleh para examiner *mobile forensics* yakni *handset*, dapat menjadi

”pegangan” bagi seorang *examiner* agar dapat menyelaraskan alur informasi dari aktivitas apa saja yang telah dilakukan kepada *handset*. Sehingga setiap tahapan yang dilakukan dapat terdokumentasi dengan baik dan hasilnya dapat diulang (*repeatable*) dan dapat dipertahankan (*defendable*).

Berikut merupakan tahapan dalam proses penanganan *handset* yang berlaku hingga saat ini dan digunakan secara umum (Puspo Heriyanto, 2016) :



Gambar 3.1. Tahapan Prosedural Penanganan *Handset*

3.1. *Chain of Custody*

Chain of Custody atau CoC bisa dikatakan menjadi hal penting yang tidak dapat dipisahkan dalam proses penanganan bukti digital. CoC merupakan dokumentasi runtutan peristiwa yang menyatakan bagaimana bukti diperoleh, dianalisis hingga disimpan untuk akhirnya dapat disajikan sebagai bukti yang sah di pengadilan. (Cosic & Baca, 2010) memaparkan ada beberapa pertanyaan yang harus terjawab didalam dokumentasi CoC sebagai berikut :

1. Apa bukti yang diperoleh ?
2. Dimana bukti ditemukan, diamankan, dipindah-tangankan, dan/atau diperiksa ?
3. Siapa saja yang melakukan kontak dan/atau menangani dan/atau menemukan bukti tersebut ?
4. Apa alasan kenapa temuan tersebut dijadikan bukti sehingga perlu diamankan ?
5. Kapan bukti tersebut ditemukan, diperoleh, diakses, dianalisis dan/atau ditransfer (mengenai waktu) ?
6. Bagaimana kemudian bukti tersebut digunakan ?

Sementara (Campbell, Goodyear, Messer, Stuart, & Fairbanks, 2018) lebih menyederhanakan apa saja yang harus ada dalam dokumentasi CoC. Menurutnya dokumentasi CoC hanya harus dapat menjawab dua pertanyaan berikut :

1. Jika bukti diubah, dirusak, atau gagal dalam proses penanganannya, siapa saja pihak yang bertanggung-jawab ?
2. Apakah bukti diperoleh secara legal dan sah ? Bagaimana membuktikannya ?

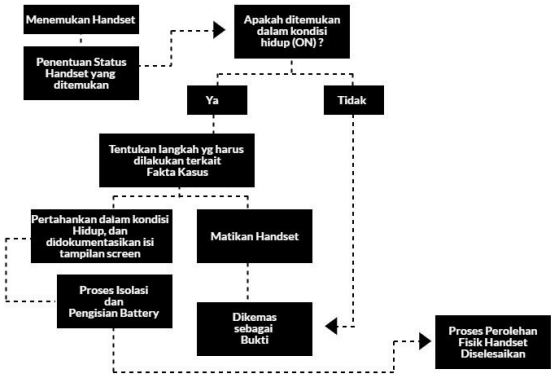
4. STUDI KASUS & IMPLEMENTASI TAHAPAN PROSEDURAL PENANGANAN BUKTI BERUPA *MOBILE DEVICES*

Perlu dipahami bahwa studi kasus merupakan simulasi dimana setiap tahapan kejadian diilustrasikan oleh penulis. Pada Senin, 26 November 2018, pukul 12:30 WIB pihak berwajib menerima laporan dari seorang perempuan bernama Sri berusia 27 tahun (Pelapor), terhadap teman kantornya bernama Ari, seorang pria berusia 30 tahun (Terlapor) atas dugaan ancaman pembunuhan melalui *short message service* (SMS) yang dikirimkan oleh terlapor. Tetapi yang emmbuat sulitnya pembuktian karena barang bukti yang menurut pelapor telah dihapus dengan paksa oleh terlapor. Menurut pelapor, pada hari yang sama dia menerima SMS dari terlapor, terlapor kemudian mendatangi kediaman pelapor sekitar pukul 20:00 WIB dan melakukan perampasan terhadap perangkat handphone milik pelapor, dimana SMS ancaman terlapor tersebut disimpan. Perampasan dilakukan untuk menghapus SMS ancaman tersebut dan mengambil *SIM Card* dari perangkat handphone. Sehingga handphone milik pelapor dibawa oleh tersangka. Pengembangan penyelidikan dilakukan oleh kepolisian, dan pada saat penggeledahan di kediaman terlapor diperoleh 2 (dua) *SIM Card* dan 1 (satu) *Handphone*. Perangkat *handphone* pelapor tidak diketemukan pada saat itu. Karena perlunya analisa mendalam terhadap bukti yang diperoleh, sehingga penyidik membutuhkan bantuan *examiner* forensik untuk mencari bukti yang

ada pada 2 (dua) *SIM Card* yang diperoleh dari terlapor A.

4.1. Tahapan Penanganan

Setelah membaca laporan kepolisian, *first responder* (anggota kepolisian) yang bertugas untuk menggeledah kediaman terlapor Ari. Sesuai dengan petunjuk terkait kasus yang menyatakan *Handphone* dan *SIM Card* pelapor Sri diambil oleh terlapor, maka pada tanggal 27 November 2018 *first responder* mengamankan barang bukti elektronik yang dicari pada lokasi. Pertama, *first responder* harus mengetahui apa yang perlu dilakukan pada saat pemerolehan bukti berupa *handset* atau *mobile devices*, maka prosedur yang berlaku secara umum menurut (Puspo Heriyanto, 2016) adalah sebagai berikut :



Gambar 4.1. Prosedur Pemerolehan *Handset* di Lokasi

4.1.1. Perolehan Bukti , Isolasi & Dokumentasi

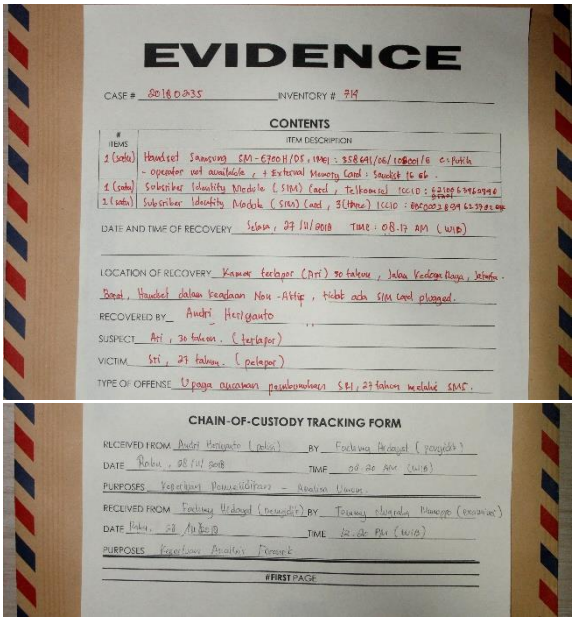
Pada studi kasus, dikamar Ari *first responder* memperoleh 1 (satu) smartphone Samsung berwarna putih dengan tipe yang tercantum dibelakangnya bertuliskan SM-E700H/DS; IMEI : 358641/06/0108001/5. Kondisi *handset* dalam keadaan *Off*, operator tidak tersedia dan terdapat *external memory card* Sandisk berukuran 16 Gb.

Gambar 4.2. Isolasi handset dengan Signal Blocker / Faraday Bag

Sesuai dengan prosedur pemerolehan *handset* di lokasi kejadian, maka *handset* langsung dikemas sebagai bukti (karena *handset* ditemukan dalam keadaan *off*) dan dilakukan tahap isolasi awal, yakni memasukkan *handset* pada *signal blocker* atau *faraday bag* sesuai dengan Gambar 4.2.

Gambar 4.3. Pemerolehan dan Isolasi *SIM Card*

Selain itu ditemukan juga 1 (satu) *Subscriber Identity Module* (SIM) *Card*, dengan informasi logo berasal dari *provider* Telkomsel dengan *Integrated Circuit Card Identifier* (ICCID) : 6210063462948. Dan 1 (satu) *Subscriber Identity Module* (SIM) *Card*, dengan informasi logo berasal dari *Provider* 3 (tri) dengan ICCID : 8950002894623782_64k.



Gambar 4.4. Dokumentasi *Chain of Custody*

Setelah dilakukan pengemasan, maka perlu dilakukan pencatatan atau dokumentasi terhadap pemerolehan barang bukti. Maka seperti pada Gambar 4.4 informasi seperti jumlah barang bukti, deskripsi masing-masing bukti, *number of cases*, *number of inventory*, tanggal dan waktu pemerolehan

bukti, lokasi pemerolehan bukti, identitas *first responder*, *suspect*, *victim*, dan modus kejahatannya atau kasusnya harus dicatat. Dan pada Dokumen *Chain of Custody* atau alur perpindahan barang bukti juga harus dicatatkan. Informasi yang dicatat berupa barang bukti diberikan kepada siapa dan dari siapa, tanggal dan waktu perpindahan, dan tujuan dari perpindahan.

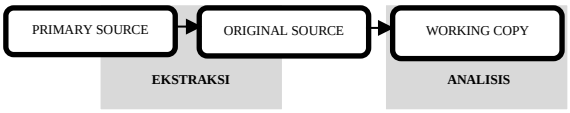
4.1.2. Identifikasi *Handset* dan Persiapan

Setelah seluruh barang bukti diperoleh dan dipindah-tangankan untuk dilakukan proses analisis oleh *examiner* forensik. Maka langkah awal yang dilakukan adalah mengidentifikasi tipe *handset* melalui informasi yang berada pada fisik *handset*. Sehingga dari studi kasus diperoleh informasi pabrikan yang dapat diperoleh dari *manual book* sesuai jenis *handset* SM-E700H. Identifikasi *Handset* perlu dilakukan untuk mempersiapkan *tools* yang akan digunakan dan tentunya *support* terhadap jenis *handset* tersebut.

Tools yang digunakan adalah Mobiledit!Forensic Vers. 10.0.0.24883 berdasarkan *upgrade* terakhir Vers. 10.0.0.24883, DB Browser for SQLite Vers. 3.10.1 (sesuai dengan laporan pelapor yang menyatakan bahwa SMS telah dihapus oleh terlapor), *Flash Drive* Berukuran 2 Gb untuk menyimpan hasil ekstraksi, SIM Card Reader Epraizer UCD 250 dan SIM reader SIMEdit Vers. 1.41.

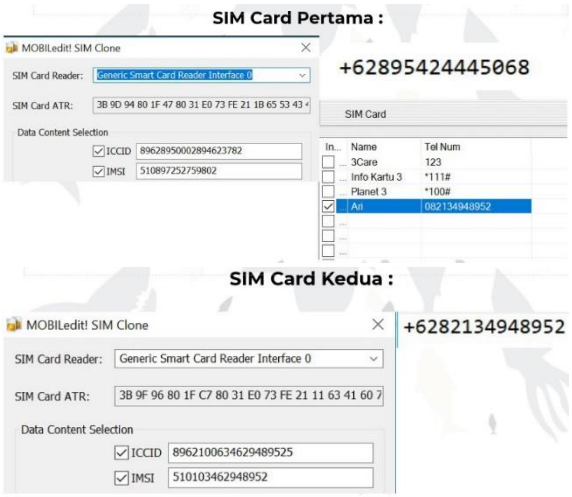
4.1.3. Ekstraksi & Analisis

Sesuai dengan informasi pada laporan kepolisian dan keterangan pelapor, bukti yang perlu dicari adalah SMS ancaman yang dituduhkan ke terlapor, oleh karena itu, sesuai dengan *system file* android (berdasarkan bukti *handset* dan informasi pabrikannya) *examiner* harus mengetahui penyimpanan (alokasi data) untuk SMS, yakni berada pada Application Data / Data Store / Internal Data / com.android.providers.telephony/databases/mmssms .db dan juga *database backupnya* berada pada / mmssms.db-wal. Karena informasi dan artefak yang dicari sudah mengerucut, maka ekstraksi hanya dilakukan untuk mendapatkan kedua *file database* yang telah disebutkan dan kemudian dilakukan tahap analisis. Keluaran dari proses ekstraksi adalah *original source* yang kemudian perlu dihitung *checksum* atau *hash value*nya untuk menjaga integritas bukti digital yang diperoleh. *Original Source* yang diperoleh dari *Primary Source* (*file* yang berada di *handset*) kemudian diduplikasi menjadi *working copy* yang-mana *file* tersebut yang digunakan untuk proses analisis.



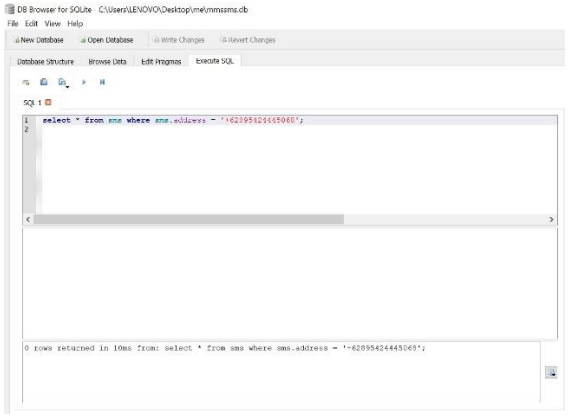
Gambar 4.5. *Digital Evidence Type* ("*Standard Operating Procedure of Digital Evidence Collection*," 2013)

Sebelum melangkah ke tahap analisis terhadap hasil ekstraksi, *examiner* perlu melihat data yang tersimpan pada kedua *SIM Card* yang sebelumnya telah diamankan bersamaan dengan *handset*.



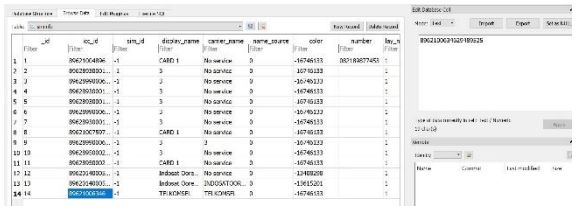
Gambar 4.6. Data pada kedua *SIM Card*

Pada *SIM Card* pertama diperoleh nomor telepon dari kartu tersebut berdasarkan ICCID-nya dan setelah dikonfrontir dengan pelapor, pelapor mengakui bahwa benar nomor tersebut adalah nomor teleponnya. Dari hasil reading menggunakan *SIM Card Reader* dan *Tool* terkait, diketahui terdapat nomor telepon yang tersimpan dengan nama Ari dan berdasarkan keterangan pelapor juga membenarkan nomor yang tersimpan itu adalah nomor Ari yang merupakan terlapor. Kemudian pada *SIM Card* kedua tidak terdapat nomor telepon yang tersimpan di *memory*-nya. Berdasarkan ICCID dari *SIM Card* tersebut ternyata identik dengan nomor telepon Ari, sehingga *examiner* dapat mengindikasikan bahwa *SIM Card* kedua benar merupakan miliki Ari (terlapor).



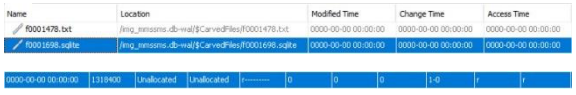
Gambar 4.7. Hasil *Filter Record* SMS pada mmssms.db

Pada mmssms.db tidak ditemukan *record* SMS yang tersimpan pada mmssms.db baik itu dari *source* ataupun *destination* berdasarkan *address* nomor Sri (pelapor).



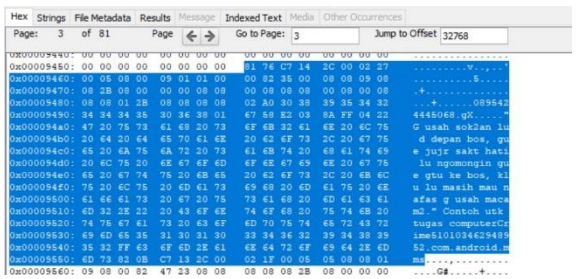
Gambar 4.8. *Filter* pada *Table SIM Info*

Namun pada *table SIM-Info* yang menyimpan *data historical SIM Card* yang pernah terpasang pada *handset* milik Ari tersebut, diketahui bahwa *record* terakhir identik dengan ICCID *SIM Card* Ari. Sehingga terindentifikasi bahwa *SIM Card* Ari-lah yang terakhir digunakan pada *handset* tersebut.



Gambar 4.9. Data Pada mmssms.db-wal

Pada mmssms.db-wal terdapat *file* f00001698.sqlite yang merupakan *unallocated data*, diketahui bahwa *unallocated data* menyimpan data yang tidak dialokasikan pada *memory* atau dengan kata lain data telah dihapus tetapi masih tersimpan dalam *backup* mmssms.db-wal.



Diperoleh *unallocated data* yang berada pada *offset* 0x9450 hingga 0x9550 yang terdapat nomor telepon identik dengan nomor telepon Sri (pelapor), sehingga mengindikasikan bahwa pernah ada SMS yang ditujukkan ke nomor pelapor tersebut (*destination* number). Selain itu, informasi paling krusial juga ditemukan, yakni isi pesan dari terlapor Ari yang ditujukan ke pelapor Sri. Sehingga tujuan dari dilakukannya proses analisis forensik untuk menemukan bukti kuat akan isi pesan ancaman pembunuhan yang berusaha dihilangkan oleh terlapor berhasil diperoleh.

4.1.4. Verifikasi, Dokumentasi & Pelaporan

Setelah bukti signifikan diperoleh, maka langkah selanjutnya adalah melakukan proses *carving-out* atau pengambilan bukti. Karena *file* yang ditemukan itu bertipe *text* maka *file* dapat langsung disimpan dengan ekstensi *text* tanpa identifikasi *file signature* dan *tail* dari nilai *hexadecimal*. Setelah itu hasil temuan kemudian diverifikasi dengan melakukan *check-sum* atau menghitung *hash value*-nya. Lalu Disertakan dalam berita acara kasus terkait, dan juga dicatatkan pada *form* hasil temuan bukti.

5. KESIMPULAN

Setelah melakukan implementasi dengan studi kasus, hasil yang diperoleh memperlihatkan bahwa langkah dan tahapan dalam penanganan bukti berupa *mobile devices* dapat dijalankan secara dinamis, dalam artian ada beberapa tahapan prosedural yang dapat dijalankan secara bersamaan, seperti tahapan dokumentasi dan pelaporan yang hampir disetiap aktivitas mulai dari pemerolehan *handset* hingga pada tahap pelaporan hasil temuan bukti digital diperlukan. Dengan mengikuti prosedural penanganan terhadap bukti digital secara umum ini, setiap tahapan aktivitas dapat dijalankan secara teratur, sehingga hasil temuan memiliki unsur *forensically sound* atau dapat dibuktikan secara ilmiah dengan tahapan yang jelas. Mengingat bahwa teknologi komunikasi dan jenis alat komunikasi semakin berkembang dan beragam, maka prosedural yang berlaku secara umum untuk penanganan *mobile devices* harus dapat meng*cover* hal tersebut, dengan harapan bahwa prosedural dapat bekerja secara dinamis dan *fleksibel* tanpa harus mengubah,menambahkan atau memperumit tahapan jika suatu saat dibutuhkan pengembangan.

DAFTAR PUSTAKA

CAMPBELL, N., GOODYEAR, T., MESSER, W., STUART, E., & FAIRBANKS, J., 2018. Digital Witness : Remote Method for Volunteering Digital Evidence on Mobile Devices. *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*,

1–5.

COSIC, J., & BACA, M., 2010. (Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. *MIPRO,Proceedings of the 33rd International Convention International Conference*, *224163003*(Im), 1226–1230. https://doi.org/10.3109/14756369609020161

DUGGAL, P. (N.D.). Kinds of Mobile Crimes. Retrieved from https://pavanduggalonmobilelaw.wordpress.com/kinds-of-mobile-crimes/

HOOTSUITE., 2018. Digital in 2018. *We Are Social*. https://doi.org/https://wearesocial.com/blog/2018/01/global-digital-report-2018

PUSPO HERIYANTO, A., 2016. *Mobile Phone Forensics : Theory*. (E. Risanto, Ed.). Indonesia: Andi Offset.

REIBER, L., 2016. *Mobile Forensic Investigation : A Guide to Evidence Collection, Analysis, and Presentation*. *McGraw-Hill Education*.

Standard Operating Procedure of Digital Evidence Collection., 2013. Digital Forensics Department, CyberSecurity Malaysia. https://doi.org/10.1039/C6TA04600B