JOISIE Journal Of Information System And Informatics Engineering ISSN: 2503-5304
Vol. 3, No.1 Juni 2019, Hlm 10-15 E-ISSN: 2527-3116

ANALISIS INVESTIGASI ANDROID FORENSIK *SHORT MESSAGE SERVICE* (SMS) PADA SMARTPHONE

Mitra Unik[1)], Vicky Gema Larenda[2)]
[1,2,] Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau
email : mitraunik@umri.ac.id, larendavicky@student.umri.ac.id, harunmukhtar@umri.ac.id

Abstract

Mobile devices (Smartphones) are important domains in communication. Short Message Service (SMS) is a service that can be used to send short messages in the form of text. Most modern cellphones (smartphones) store SMS in internal memory, not on a SIM card so that in the acquisition process requires material on the SMS. The purpose of this study is to explain the process of implementing digital evidence on the material examining the SMS on a Smartphone, so that it can become legitimate digital evidence. Furthermore, this research is also to get traces of digital communication on Smartphone evidence. This study uses forensic methods that can really support the data or information obtained. On smartphones, all activities of messages are stored and processed in the database. The database for SMS is found in folderdata / com.android.providers.telephony / database found. For sms files stored in mmssms.db, which is in the database sub folder. Review the location using a forensic tool capable of finding and extracting incoming and outgoing messages, the metadata of the mmssms.db file contains the md5 hash value, capacity file, creation (created), access time (accessed), modified transmission), change time (changed). Furthermore in this study, a search to rediscover the message that was successfully carried out.

Keywords: *Digital Forensic, SMS, Smartphone, Digital Evidence.*

Abstrak

Perangkat seluler (*Smartphone*) menjadi domain penting dalam berkomunikasi. Layanan Pesan Singkat (SMS) adalah layanan yang dapat digunakan utnuk mengirim pesan singkat berupa teks. Sebagian besar ponsel modern (*smartphone*) menyimpan SMS dalam memori internal, bukan pada kartu SIM sehingga dalam proses akuisisi kasus yang melibatkan materi pada SMS. Tujuan dari penelitian ini yakni menjelaskan proses penanganan bukti digital pada materi periksa yaitu SMS pada *Smartphone*, sehingga dapat menjadi barang bukti digital yang sah. Selanjutnya Penelitian ini juga untuk mendapatkan jejak – jejak digital komunikasi sms pada barang bukti *Smartphone*. Penelitian ini menunjukkan penggunaan metode forensik yang benar dapat menjaga integrasi data atau informasi yang diperoleh. Pada *smartphone*, seluruh aktivitas dari pesan disimpan dan diproses dalam database. Database untuk sms terdapat dalam ditemukan *folderdata/com.android.providers.telephony/databases.* Untuk *file* sms tersebut tersimpan pada *mmssms.db* yang terdapat didalam sub folder *databases*. Akuisis pada lokasi tersebut dengan menggunakan tool forensik mampu menemukan dan mengektraksi pesan masuk maupun pesan keluar yang terengkripsi, Metadata dari *file* mmssms.db berisikan nilai *hash* md5, kapasitas *file*, waktu pembuatan (*created*), waktu akses (*accessed*), waktu modifikasi (*modified*), waktu perubahan (*changed*). Selanjutnya pada penelitian ini pencarian untuk menemukan kembali pesan SMS yang telah dihapus berhasil dilakukan.

Kata Kunci *: Digital Forensik, SMS, Smartphone, Bukti Digital*

1. PENDAHULUAN

Insiden dunia maya berlangsung sangat cepat dan meningkat dalam jumlah dan korban, ketika insiden dunia maya terjadi, orang-orang yang diserang atau menjadi korban merespon dengan serangkaian tindakan yang telah ditentukan (ISACA 2015). Bidang forensik digital dimulai pada pertengahan 1980-an dengan pemahaman dari beberapa lembaga penegak hukum bahwa komputer akan memainkan peran penting dalam penyelidikan *future criminal* (Gentry 2019).

Menerapkan keilmuan forensik digital untuk membantu dalam pemulihan dan penyelidikan materi pada media digital dan jaringan komunikasi adalah tindakan yang biasa dilakukan (Unik 2015). Ada banyak jenis media digital dan perangkat pengguna akhir, yang mungkin ditemui selama pencarian di tempat kejadian, yang semuanya memiliki potensi untuk menyimpan data yang mungkin bernilai bagi penyelidikan. Proses mengidentifikasi, melestarikan, menganalisis dan menyajikan bukti digital dengan cara yang tepat dapat diterima secara hukum dalam setiap proses hukum (yaitu, peradilan) (Kent et al. 2006). Digital Forensik mempunyai banyak cabang salah satunya adalah *Mobile* Forensik. *Mobile* Forensik adalah ilmu untuk memulihkan bukti digital dari perangkat *mobile* dibawah kondisi forensik menggunakan metode yang diterima (Butterfield et al. 2007).

Indonesia berada di urutan ke-24 dari 27 negara terbanyak yang menggunakan *Mobile – smartphone* (Yanuar 2019). Tipe – tipe yang termasuk kedalam *Mobile* Forensik adalah sebagai berikut (Martin 2008), yaitu : *Cellular Phone, Smart Phone*, dan *Mp3 Player*

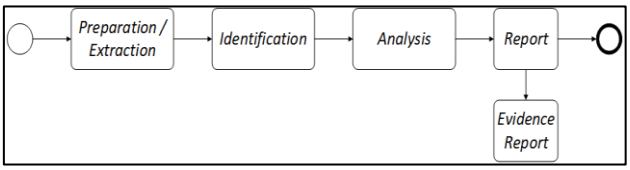
Barang bukti pada *forensik* digital bersifat fisik dan dapat dikenali secara *visual*, sehingga investigator dan analisis *forensik* harus sudah memahami serta mengenali masing – masing barang bukti elektronik ini ketika sedang melakukan proses pencarian (*Searching*) barang bukti di TKP (Al-Azhar 2012).

Short Message Service (SMS) Merupakan sebuah teknologi yang menyediakan pelayanan pengiriman dan penerimaan pesan antar ponsel. SMS pertama kali diperkenalkan di Eropa sekitar tahun 1992, yang pertama kali terintegrasi dengan GSM (*Global System for Mobile Communications*) yang kemudian berkembang dalam CDMA dan TDMA (Sunardi, Hari Murti 2014).

Tujuan dari penelitian ini adalah menjelaskan proses penanganan bukti digital berupa *Smartphone* sehingga dapat menjadi barang bukti digital yang sah. Penelitian ini juga untuk mendapatkan jejak – jejak digital komunikasi sms pada barang bukti *Smartphone*.

2. METODE PENELITIAN

Metode proses investigasi ditetapkan sebagai pross linear dari *Prepartion* hingga Laporan.



Gambar 1. Metode Investigasi Digital Forensik
Sumber: (DFRWS 2001)

a. Preparation/Extraction
   Pada proses persiapan barang bukti dan ektraksi ini melibatkan proses dan cara yang digunakan sesuai dengan perangkat yang akan diperiksa.
b. Identification
   Pada tahap ini merupakan tahapan untuk mengidentifikasi keseluruhan barang bukti, terkait dengan relevansi barang bukti tersebut terhadap studi kasus.
c. Analysis
   Proses ini melakukan pencarian yang mendalam untuk barang bukti fisik, mengembangkan teori berdasarkan hasil analisis dan pengujian terhadap barang bukti.
d. Report
   Proses ini merupakan tahap akhir dari proses digital forensik, dalam proses ini memaparkan hasil analisis dari barang bukti kedalam *form* khusus.

3. HASIL DAN PEMBAHASAN

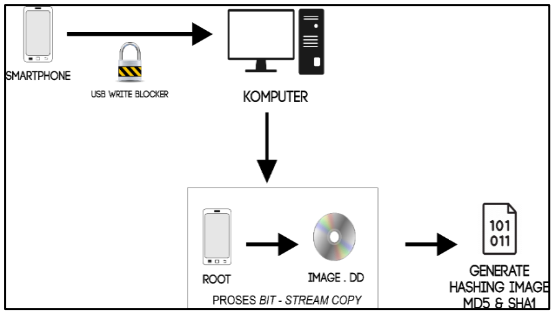
3.1 Preparation / Extraction

a. Identifikasi barang bukti

Untuk identifikasi barang bukti *smartphone*, pada penelitian ini menggunakan *Smartphone* Android yang diperoleh dalam kondisi fisik baik. Untuk akuisisi objek penelitian ini diakuisisi dalam keadaan menyala / hidup (*on*).

b. Proses akuisisi bukti digital

Proses akuisi diikat dalam sebuah prosedur dan aturan yang berlaku, sesuai dengan prinsip-prinsip investigasi (ACPO 2012) :



Gambar 2. Proses Akuisisi Bukti Digital *Smartphone*

Pada gambar 6 merupakan proses akuisisi bukti digital *smartphone*. Proses yang ada meliputi :

1. Menggunakan USB Write Blocker untuk melindungi keaslian objek penelitian
2. Menghubungkan *smartphone* ke komputer menggunakan kabel USB
3. Mengaktifkan *usb debugging mode* untuk melakukan proses *root* pada *smartphone*
4. Melakukan *root* pada *smartphone* dengan menggunakan *tool* KingoRoot dan BusyBox
5. Setelah proses *root* selesai, melakukan imaging pada *smartphone* dengan menggunakan teknik imaging *bit-stream copy* dan menghasilkan *file image* dengan *file* ekstensi (.dd).
6. Melakukan *generate hash*ing MD5 dan SHA1 menggunakan *tool* AccessData FTK *Image*r pada *file image* sebagai nilai *hash* dari *smartphone.*

3.2 Identifikasi

Pada pesan sms, seluruh aktivitas dari pesan disimpan dan diproses dalam database. Database untuk sms terdapat dalam *folderdata/com.android.providers.telephony/databases.* Database sms ini terletak pada folder *"com.android.providers.telephony"*/*"databases".* merupakan struktur dari com.android.providers.telephony.

3.3 Analisis

Dalam penelitian ini komponen dasar investigasi penulis lakukan guna memastikan bahwa data tersebut sama validnya dengan yang asli. (Agarwal and Gupta 2011).

a. Mencari Database dari Pesan SMS

Database dari pesan sms terdapat pada folder *com.android. providers. telephony*. Pada folder *com.android. providers. telephony* terdapat 2 subfolder yaitu *shared_pref* dan *databases*. Untuk *file* sms tersebut tersimpan pada *mmssms.db* yang terdapat didalam sub folder *databases.*

Saat *file* mmssms.db dibuka pada *tool* Autopsy, dapat dilihat metadata dari *mmssms.db* berikut ini:

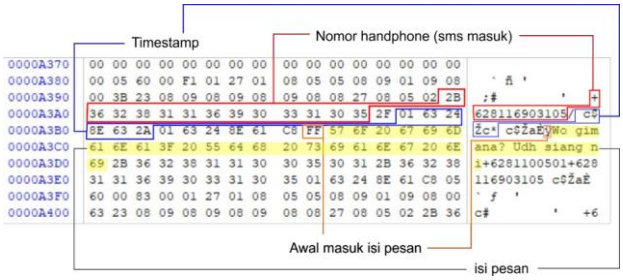
Tabel 1. Metadata *File* mmssms.db

Name	/img_bbandroidoppor815.dd/vol_vol13/data/com.android.providers.telephony/databases/mmssms.db
Type	*File* System
MIME Type	application/x-sqlite3
Size	172032
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2018-05-03 13:56:26 ICT
Accessed	2013-01-01 19:02:23 ICT
Created	2013-01-01 19:02:23 ICT
Changed	2018-05-03 13:56:26 ICT
MD5	a5779f5757af1d7bb3ad52f0a04367f3
Hash lookup Result	UNKNOWN
Intenal ID	6945

Terlihat bahwa Pesan di modifikasi terakhir pada tanggal 3 Mei 2018 pada pukul 13:56:26 ICT. Pada bagian tabulasi hex ditemukan pesan yang dihapus.

b. Mencari pesan sms yang ada pada *file* mmssms.db

Pesan sms ditemukan dan untuk pesan yang pertama dari urutan atas ke bawah merupakan sms yang terakhir kali dilakukan baik itu sms diterima maupun sms dikirim. Pada data mmssms.db pesan tersebut terdapat pada baris 0000A390.



Gambar 3. Informasi pesan SMS Masuk

Pada gambar diatas dapat dilihat Pada nomor *handphone* pertama merupakan pesan sms masuk, karena ditandai dengan nilai +62(nomor kode wilayah Indonesia).

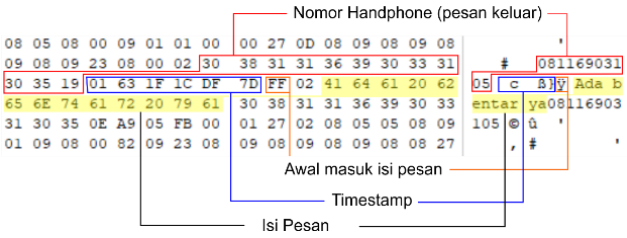
Sedangkan kode unik setelahnya merupakan *timestamp* (waktu) dari pesan sms masuk tersebut. Untuk awal masuknya pada isi pesan, kode hex ditandai dengan nilai F yang menandakan bahwa isi pesan dimulai.

Untuk konversi kode hex ke decimal dilakukan menggunakan konversi secara online pada website *https://www.binaryhexconverter.com/hextodecimalconverter*, sehingga dihasilkan nilai decimal, sedangkan untuk konversi nilai decimal tersebut ke Epoch Time menggunakan konversi secara online pada website *https://www.epochconverter.com/.EpochTime tersebut nilai waktu yang bisa dibaca oleh manusia yang dapat dilihat pada tabel 2 berikut ini :*

Tabel 2. Konversi *Timestamp*

Hexadecimal	Decimal	Unix Epoch Time	Waktu Indonesia Barat
0163248E632A	1525326701354	Thursday, May 3, 2018 5:51:41.354 AM (GMT +0)	Rabu / Thursday, 3 Mei 2018 12:51:41.354 PM

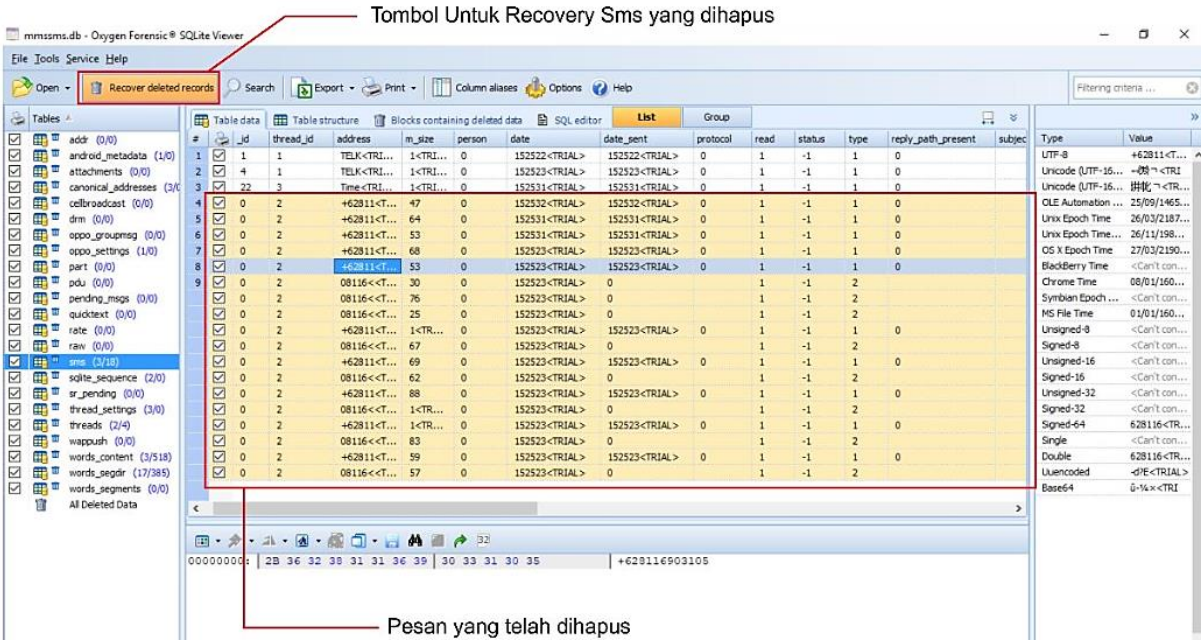
Pada tabel tersebut terlihat bahwa waktu dari kode hexadecimal diatas adalah Rabu, 3 Mei 2018 12:51:41.354 PM. Untuk pesan sms yang keluar, pada kode ASCII nomor *handphone* tujuan yang digunakan tidak langsung menggunakan kode wilayah (kode wilayah Indonesia adalah +62), namun langsung nomor *handphone* tersebut yakni 08116903105



Gambar 4. Informasi pesan SMS Keluar

c. Membaca pesan serta menampilkan artefak – artefak yang berkaitan dengan sms

Pembacaan pesan dan pengambilan artefak atau jejak dapat dilakukan dengan *tool oxygen Forensic SQLite Viewer* seperti yang penulis lakukan. Untuk itu maka *file* mmssms.db dibuka pada *tool Oxygen Forensic SQLite Viewer.*



Gambar 5. *Recovery* Pesan SMS yang Sudah Dihapus

Gambar diatas dapat dilihat bahwa isi dari record sms yang dihapus dimunculkan kembali. Pada beberapa kolom di tabel ada sebagian yang disembunyikan (*hidden*) nilainya dikarenakan *tool* Oxygen Forensic SQLite Viewer ini masih menggunakan lisensi *trial* (Percobaan). Namun jika di klik pada kolom tertentu, pada tampilan layar bawah akan menampilkan seluruh isi dari bagian tersebut.

3.4 Skup hasil akuisisi

Masing – masing pesan sms tersebut terdapat perbedaan. Untuk pesan yang dikirim (pelaku), nomor *handphone*nya tanpa diawali dengan nomor kode wilayah Indonesia (+62). Sedangkan pesan yang masuk (korban) menggunakan kode wilayah Indonesia (+62). Hasil akuisis serta keterangan informasi yang didapat penulis sajikan dalam tabel yang memperlihatkan hasil *string* dan *code Hex* dari hasil akuisisi.

Tabel 3. Hasil Akuisisi

1	0x0000aec0: 09 08 09 23 08 00 02 30 38 31 31 36 39 30 33 31 ...#...081169031 0x0000aed0: 30 35 39 01 63 1E FA 26 0E FF 02 53 65 6C 61 6D 059.c..&...Selam 0x0000aee0: 61 74 20 73 69 61 6E 67 2C 20 61 70 61 20 62 65 at siang, apa be 0x0000aef0: 6E 61 72 20 69 6E 69 20 64 65 6E 67 61 6E 20 73 nar ini dengan s 0x0000af00: 61 75 64 61 72 61 20 76 69 63 6B 79 3F 30 38 31 audara vicky?081 0x0000af10: 31 36 39 30 33 31 30 35 81 65 01 1C 00 09 1F 02 16903105.e..... **Pelaku** : Selamat siang, apa benar ini dengan saudara vicky? ***Timestamp*** : 01 63 1E FA 26 0E (Hex), *Wednesday – May* 2, 2018 10:51:40.302 am (GMT+7)
2	0x0000ad90: 2B 36 32 38 31 31 36 39 30 33 31 30 35 3B 01 63 +628116903105;.c 0x0000ada0: 1E FC 93 A0 01 63 1E FC 91 F8 FF 49 79 61 20 62 .....c.....Iya b 0x0000adb0: 65 6E 61 72 20 73 61 79 61 20 73 65 6E 64 69 72 enar saya sendir 0x0000adc0: 69 2C 20 69 6E 69 20 73 69 61 70 61 20 79 61 3F i, ini siapa ya? 0x0000add0: 2B 36 32 38 31 31 30 30 35 30 31 2B 36 32 38 31 +6281100501+6281 0x0000ade0: 31 36 39 30 33 31 30 35 01 63 1E FC 91 F8 81 38 16903105.c.....8 **Korban** : Iya benar saya sendiri, ini siapa ya? ***Timestamp*** : 01 63 1E FC 93 A0 (Hex), *Wednesday – May* 2, 2018 10:54:19.424 am (GMT+7)
3	0x0000acf0: 01 01 00 00 81 2D 0D 08 09 08 09 08 09 08 09 23 .....-.........# 0x0000ad00: 08 00 02 30 38 31 31 36 39 30 33 31 30 35 53 01 ...081169031058. 0x0000ad10: 63 1E FE 29 23 FF 02 49 6E 69 20 61 6B 75 20 62 c..)#..Ini aku b 0x0000ad20: 6F 77 6F 2C 20 6D 61 73 69 68 20 69 6E 67 61 74 owo, masih ingat 0x0000ad30: 20 67 6B 3F 20 4B 69 74 61 20 73 61 74 75 20 73 gk? Kita satu s 0x0000ad40: 6D 61 20 64 75 6C 75 20 64 61 6E 20 70 65 72 6E ma dulu dan pern 0x0000ad50: 61 68 20 73 65 6B 65 6C 61 73 20 6A 75 67 61 20 ah sekelas juga 0x0000ad60: 6B 65 6C 61 73 20 32 30 38 31 31 36 39 30 33 31 kelas 2081169031 0x0000ad70: 30 35 0E A9 00 7C 01 27 01 08 05 05 08 09 01 09 05...|.'........ **Pelaku** : Ini aku bowo, masih ingat gk? Kita satu sma dulu dan pernah sekelas juga kelas 2 ***Timestamp*** : 01 63 1E FE 29 23 (Hex), *Wednesday – May* 2, 2018 10:56:03.235 am (GMT+7)
	Selanjutnya…

Dari tabel tersebut dapat terlihat pesan sms yang dihapus didapatkan pesan nomor *handphone*, *timestamp*, serta isi dari pesan yang dihapus. Untuk kode hex yang ditandai merupakan *timestamp* dari pesan tersebut. Pembeda antara si pelaku dengan korban adalah awal dari nomor *handphone* tersebut. Jika nomor *handphone* tersebut diawali dengan nomor kode wilayah Indonesia yaitu +62 maka pesan tersebut merupakan pesan masuk (korban), sedangkan jika nomor tersebut tidak diawali dengan +62 maka pesan tersebut merupakan pesan yang dikirim (pelaku) dari *smartphone* tersebut. Untuk kode hex yang ditandai merupakan *timestamp* dari pesan tersebut. Kode hex tersebut dikonversi ke bilangan desimal lalu dikonversi kembali ke kode UNIX Epoch *time* untuk dapat dibaca namun masih dalam waktu GMT + 0, maka dikonversi kembali ke dalam waktu Indonesia yaitu GMT+ 7. Kode hex tersebut dikonversi ke bilangan desimal lalu dikonversi kembali ke kode UNIX Epoch *time* untuk dapat dibaca namun masih dalam waktu GMT + 0, maka dikonversi kembali ke dalam waktu Indonesia yaitu GMT+ 7.

4. SIMPULAN

Atas hasil penelitian ini maka diperoleh kesimpulan sebagai berikut :

1. Informasi (SMS) berhasil didapatkan dari investigasi forensik pada rankaian pencarian dan pengujian Barang bukti di penelitian ini.
2. Barang bukti berhasil didapatkan dari investigasi forensik pada kasus penipuan sms berupa nilai *hashing* md5 dan sha1 dari barang bukti sms yang ditemukan yaitu pada *file* mmssms.db. metadata dari *file* mmssms.db berisikan nilai *hash* md5, kapasitas *file*, waktu pembuatan (*created*), waktu akses (*accessed*), waktu modifikasi (*modified*), waktu perubahan (*changed*).
3. Hasil pencarian untuk menemukan kembali pesan SMS yang telah dihapus berhasil dilakukan.

5. UCAPAN TERIMAKASIH

Alhamdulillah kehadirat Allah SWT serta penulis ucapkan kepada seluruh orang-orang yang telah membantu dalam penyusunan penelitian ini.

6. DAFTAR PUSTAKA

ACPO. 2012. *ACPO Good Practice Guide for Digital Evidence*.

Agarwal, A, and M Gupta. 2011. "Systematic Digital Forensic Investigation Model." ... *Journal of Computer* ... 5(1): 118–31.

Al-Azhar, Muhammad Nuh. 2012. *Digital Forensic, Panduan Praktis Investigasi Komputer*. ed. Palupi Wuriarti. Jakarta: Salemba Infotek.

Butterfield, Jason, Miles Tracy, Wayne Jansen, and Scarfone Karen. 2007. "Guidelines on Electronic Mail Security Recommendations of the National Institute of Standards and Technology." : 139.

DFRWS. 2001. "A Road Map for Digital Forensic Research." In *The Digital Forensic Research Conference*, Utica: dfrws.org.

Gentry, Eric Elwood. 2019. "SEAKER : A Mobile Digital Forensic Triage Device By." University Channel Islands. https://prof.msoltys.com/wp-content/uploads/2019/04/SEAKER_Thesis.pdf.

ISACA. 2015. "Overview of Digital Forensics." *isaca.org*.

Kent, Karen, Chevalier Suzanne, Tim Grance, and Hung Dang. 2006. *Guide to Integrating Forensic Techniques into Incident Response*. Gaithersburg, Maryland.

Martin, Andrew. 2008. *SANS Instituted InfoSec Reading Room, Mobile Device Forensics*.

Sunardi, Hari Murti, Hersatoto Listiyono. 2014. "Aplikasi SMS Gateway." *Jurnal Teknologi Informasi DINAMIK* XIV(1): 30–34.

Unik, Mitra. 2015. "Analisis Investigasi Dan Perancangan Kerangka Kerja Forensika Digital Pada Mesin Fotokopi Multi Function Peripheral (Mfp)." UNIVERSITAS ISLAM INDONESIA.

Yanuar, Yudono. 2019. "Survei Kepemilikan Smartphone, Indonesia Peringkat Ke-24." *Tempo.co*. https://tekno.tempo.co/read/1181645/survei-kepemilikan-smartphone-indonesia-peringkat-ke-24/full&view=ok (July 3, 2019).