CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 5, No. 1, Mei 2022, hlm. 6-11

ANALISIS BUKTI DIGITAL PADA *RANDOM ACCESS MEMORY* ANDROID MENGGUNAKAN METODE *LIVE FORENSIC* KASUS PENJUALAN SENJATA ILLEGAL

Arjun Zakari Yahya[1], Dirman[2], Dadang Juwoto Buru[3], Bambang Sugiantoro[4]

[1,2,3,4] Program Studi Magister Teknik Informatika Universitas Islam Indonesia

Email: [1]19917001@students.uii.ac.id, [2]19917002@students.uii.ac.id, [3]17917205@students.uii.ac.id, [4]Bambang.sugiantoro@uin-suka.ac.id

Abstrak

Metode *Live forensic* adalah analisis data yang berjalan langsung pada bagian *Random Access Memory*. Tempat penyimpana sementara disebut juga *Random Access Memory*, data yang ada tersimpan di dalam *Random Access Memory* sifatnya adalah *volatile* atau mudah menghilang. Tujuan dari penelitian ini akan mendapatkan hasil bukti berupa digital melalui cara analisis bukti digital pada *random access memory* pada *smartphone* android pelaku dan *smartphone* korban menggunakan metode *live forensic* dalam kasus penjualan senjata illegal. Pada penelitian barang bukti digital yang disita berupa *smartphone* pelaku maupun *smartphone* korban. Korban diposisi sebagai mahasiswa yang ditawari untuk membeli senjata ilegal oleh pelaku. Metode analisis data yang dilakukan menggunakan metode *NIST (National Institute Of Standart Technology)* yang memiliki langkah-langkah analisis berupa *preservation, acquisition, examination, analysis* dan *reporting*. Data yang diambil dari *random access memory* berupa log *file* telephone, sms, dan data dari whatsapp. *FTK (Forensic Tool Kit)* digunakan untuk mencari bukti-bukti digital kejahatan penjualan senjata illegal. Hasilnya berupa bukti kejahatan yang telah dihapus oleh pelaku, antara lain bukti log telephone, sms, chat whatsapp, dan *file* gambar berekstensi .jpg. Mem*tools* sangat berguna untuk mendapatkan data dari *random access memory* secara menyeluruh.

Kata kunci: Live Forensik, Digital Forensik, *Random Access Memory*

ANALYSIS OF DIGITAL EVIDENCE ON *RANDOM ACCESS MEMORY* ANDROID USING *LIVE FORENSIC* METHOD CASE OF ILLEGAL WEAPON SALES

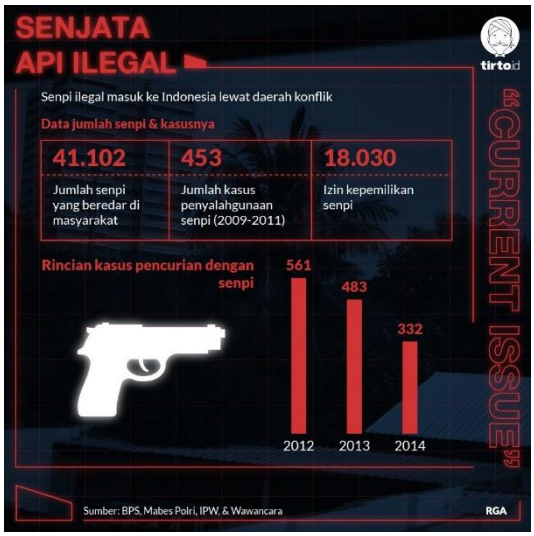
Abstract

Live forensic method is data analysis that runs directly on the Random Access Memory section. Temporary storage places are also called Random Access Memory, the data stored in Random Access Memory is volatile or easily disappears. The purpose of this research is to obtain digital evidence through digital evidence analysis on random access memory on the perpetrators 'android smartphones and victims' smartphones using the live forensic method in the case of illegal weapons sales. In the study of digital evidence seized in the form of a perpetrator's smartphone and the victim's smartphone. The victim is positioned as a student who was offered to buy illegal weapons by the perpetrator. The method of data analysis is carried out using the NIST (National Institute of Standards Technology) method which has analysis steps in the form of preservation, acquisition, examination, analysis and reporting. Data taken from random access memory in the form of log files telephone, sms, and data from whatsapp. The FTK (Forensic Tool Kit) is used to look for digital evidence of the crime of selling illegal weapons. The result is evidence of crime that has been deleted by the perpetrators, including evidence of telephone logs, sms, chat whatsapp, and image files with the extension .jpg. Mem*tools are very useful for getting data from random access memory as a whole.*

Keywords: *Live forensics, Digital Forensics, Random Access Memory*

1. PENDAHULUAN

Tercatat 41.102 senjata yang telah beredar di Indonesia, dalam aspek administrasi yang memiliki izin kepemilikan senjata hanya 18.030. ada pun penyalagunaan mencapai 450 kasus senjata api sepanjang tahun 2009-2011. Kasus pencurian yang menggunakan senjata api pada tahun 2012 masih sangat bayak yaitu 561 kasus, dua tahun berikutnya 2013 menurun 483 dan 2014 adalah 332 kasus. Senjata ilegal dapat dilihat pada Gambar 1.



Gambar 1. Senjata api ilegal

2. TINJAUAN PUSTAKA

Perdagangan senjata ilegal di Indonesia sangat membahayakan dan merugikan masyarkat. Sepanjang tahun 2012-2014 kasus pencurian mencapai 1.373. merespon maraknya senjata ilegal yang disalah gunakan masyarakat yang tidak bertanggung jawab maka diperlukan metode standarisasi investigasi digital forensik yang mampu mengungkap pelaku penjualan senjata api ilegal di Indonesia.

Revolusi teknologi yang sangat cepat berkembang dan mudah, dimanfaatkan sebagian orang yang hanya mencari keuntungan semata tanpa memperhatikan kerugian dan keamanan orang lain. Digital forensik yang mengkombinasikan dua bidang disiplin ilmu hukum dan teknologi informasi mampu menjadi instrumen pengumpulan barang bukti penjualan senjata api ilegal.

Terminologi forensik sering disebut dalam kriminal khususnya digital forensik merupakan usaha manusia menyampaikan kepengadilan dengan kaidah-kaidah ilmiah yaitu persiapan, pencarian, pengumpulan, analisis dan pelaporan diranah hukum. Cakupan digital forensik selingkupi segala sesuatu yang berkaitan dengan teknologi komputer (Sulianta, 2016).

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kualitatif

3.A Variabel Yang Diteliti

Variabel yang diteliti pada *Random Access Memory* antaralain :

1. SMS : Bukti Chat
2. Telephone : Bukti panggilan masuk, keluar
3. Whatsapp : Bukti chat dan *file* image

3.B Pengumpulan Data

Pengumpulan data yang kami peroleh mengacu pada Donnie & Tindall (2015) dengan mengambil PID (process ID) dari aplikasi yang sedang berjalan pada *random access memory* menggunakan mem*tools*. Yang didapat dari *random access memory* berupa log *file* telephone, transkrip SMS, data Whatsapp.

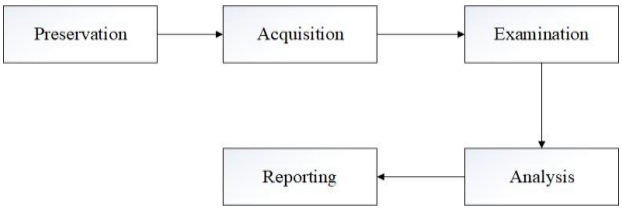
3.C Sumber Data

Sumber data berasal dari barang bukti yaitu *smartphone* pelaku dan *smartphone* android korban yang akan dilakukan akusisi pada RAM. Pada skenario yang dilakukan korban berperan sebagai mahasiswa yang ditawari senjata illegal oleh pelaku.

Pelaku melakukan komunikasi melalui *smartphone* dengan korban (mahasiswa) melalui panggilan telephone setelah itu pelaku mengirim pesan SMS ke korban dan mengirim foto senjata illegal yang dijual melalui pesan Whatsapp. Pelaku meghapus log berupa log panggilan telephone, pesan SMS dan Whatsapp.

3.D Analisis Data

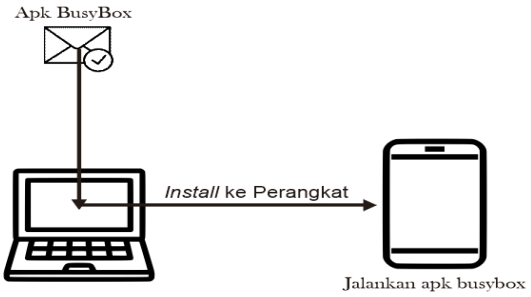
Analisis pada penelitian ini mengacu pada metode NIST (*National Institute of Standars Technology*), sebuah badan administrasi teknologi dari departemen perdagangan Amerika Serikat (Ayers, et al. 2014) Seperti Gambar 2.



Gambar 2. Metode NIST

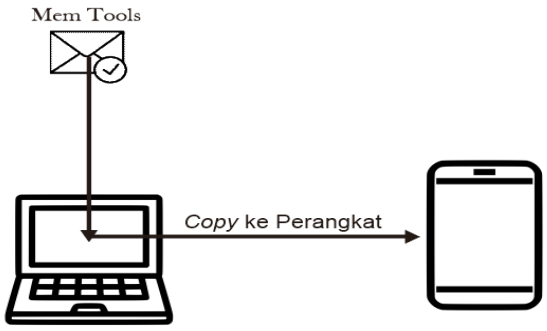
Langkah-langkah dalam melakukan analisis data menggunakan NIST adalah :

a. *Preservation* Adalah langkah mengidentifikasi perangkat *smartphone* pelaku dan korban, serta melihat kode IMEI kedua smarphone dengan cara menekan tombol melalui keypad *#06#.
b. *Acquisition* (akusisi) adalah langkah mencari dan mendapatkan data *file* yang berada didalam *random access memory* menggunakan mem*tools*. Berikut alur akusisi *file random access memory* :



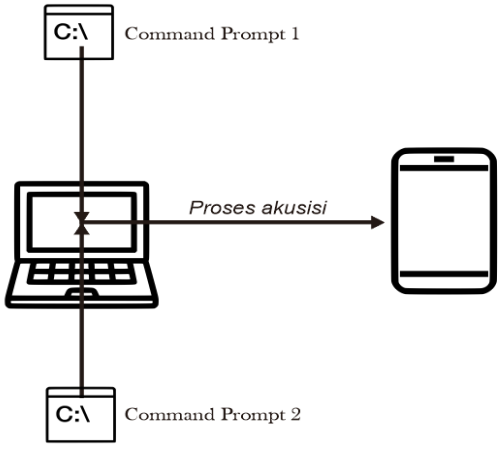
Gambar 3. Langkah pertama acquisition

Langkah pertama adalah memasang aplikasi busybox.apk dari komputer ke perangkat *smartphone* android dengan melakukan perintah ”adb -d install busybox.apk” pada perangkat *smartphone*, kemudian membuat koneksi antara komputer dan *smartphone* melalui perintah ”adb forward TCP TCP”.



Gambar 4. Langkah kedua acquisition

Langkah kedua menyalin mem*tools* ke perangkat *smartphone* android dengan menjalankan perintah ”adb push mem sdcard”, selanjutnya adalah melakukan konfigurasi systeLangkah kedua pada sistem android melalui perintah ”adb shell”, dan masuk mode root dengan perintah ”su”. Kemudian buat folder pada directory dev, lalu pindahkan mem*tools* ke directory dev. Ganti *permission file* mem*tools* dengan perintah chmod (change mood), setelah itu ketik perintah ”dumpsys meminfo | grep activities” untuk melihat aplikasi yang sedang aktif pada *random access memory*.

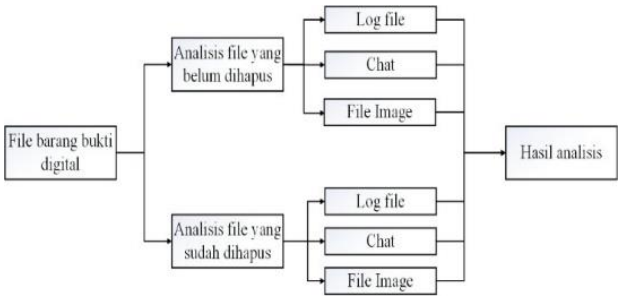


Gambar 5. Langkah ketiga acquisition

Langkah ketiga adalah mencari PID (Process ID) Contact, SMS, dan Whatsapp dengan perintah ps tetapi data yang dihasilakn terlalu banyak jadi disederhanakan menjadi ”ps | grep (nama PID)”, fungsi grep untuk pencarian karakter yang cocok. Bila PID sudah ditemukan lakukanlah proses akusisi dengan perintah ”./mem PID | busybox nc -l -p TCP”, tcp harus sama degan adb forward, sambil berjalan proses akusisi buka terminal command prompt kedua dan ketikkan perintah ”ncat 127.0.0.1 tcp > namaberkas*”* bertujuan untuk mengirim data dari *smartphone* ke komputer melalui port tcp.

c. Examination (Pemeriksaan) adalah untuk mengecek nilai hash dari setiap *file* imaging pada *random access memory* yang diperoleh menggunakan *tools* FTK, yang bertujuan untuk mengetahui nilai hash nya, agar saat diperiksa kembali memiliki nilai yang sama untuk menghindari *file* yang berubah.

d. *Analysis* Adalah langkah pencarian bukti kejahatan menggunakan *tools* FTK *(Forensic Tool Kit)*. Berikut diagram alur analisis data tersaji pada Gambar 3.



Gambar 6.Alur Analisis Bukti

Penjelasan dari Gambar . bukti digital berupa *file random access memory* sebagai *input*, dilakukan proses pencarian data yang belum dihapus berasal dari *smartphone* korban dan pencarian data yang sudah dihapus dari *smartphone* pelaku, berupa *log file* (panggilan masuk dan panggilan keluar), *chatting* antara pelaku dan korban melalui SMS dan WhatsApp, *file image* yang dikirim atau diterima berupa foto. Hasil *output* dari bukti digital antara lain bukti kejahatan berupa log panggilan telephone, *chatting* SMS dan *chatting* Whatsapp dalam bentuk teks dan gambar .

e. *Reporting* Adalah langkah menguji perbandingan hasil analisis bukti digital antara pelaku dan korban untuk mendapatkan bahwa melaku melakukan penjualan senjata illegal.

3.E Alat Penelitian

Alat yang digunakan dalam penelitian untuk melakukan simulasi dan skenario sebagai berikut :

a. Perangkat Keras
   1. Laptop Asus Intel Core i5
   2. Asus Zenfone
   3. Xiaomi redmi 6

b. Perangkat Lunak
   1. Windows 10 64 Bit.
   2. Busybox

3. ADB (Android Debuge Bridge)
4. Mem*tools*
5. FTK (Forensic Tool Kit)
6. NETCAT (ncat)s

4. HASIL DAN PEMBAHASAN

4.A Preservation

Tahap pertama untuk mengidentifikasi barang bukti kedua *smartphone* yang sudah di root, dengan cara mengakses systemnya dengan perintah cat system/build.prop dan mengakses kode IMEI (International Mobile Enquipment Identity) dengan perintah *#06#

Table 1. Identifikasi *Smartphone* Korban

Nama *Smartphone*	Asus Zenfone Max
Model *Smartphone*	ASUS_Z010D
Versi Android	Lollipop 5.0.2
Versi SDK	21
Nomor IMEI	3533810751xxxxx 3533810751xxxxx

Dari hasil identifikasi *smartphone* korban, yang digunakan adalah asus model ASUS_Z010D, versi android lollipop 5.0.2, versi SDK 21 dengan kode IMEI 3533810751xxxxx dan 3533810751xxxxx.

Tabel 2. Identifikasi *Smartphone* Pelaku

Nama *Smartphone*	Samsung
Model *Smartphone*	SM-J210F
Versi Android	Lollipop 5.1.1
Versi SDK	22
Nomor IMEI	3570040788xxxxx 3570040788xxxxx

Dari hasil Tabel 2 identifikasi yang diperoleh dari *smartphone* pelaku, menggunakan *smartphone* android bertipe Samsung dengan model SM-J210F, versi android lollipop 5.1.1, versi SDK 22, dengan IMEI 3570040788xxxxx dan 3570050788xxxxx.

4.B Acquisition

Pengambilan data yang terdapat pada *random access memory* menggunakan *tools* ADB (Android Debug Bridge) untuk masuk kedalam system android, sedangkan mem*tools* dipergunakan mengambil data pada *random access memory*.

Tabel 3. Hasil akuisisi

Barang Bukti	Model	Tool	*File* RAM
Asus	ASUS_Z010D	Mem	Logasus.raw
Asus	ASUS_Z010D	Mem	Smsasus.raw
Asus	ASUS_Z010D	Mem	Waasus.raw
Samsung	SM-J210F	Mem	Logsamsung.raw
Samsung	SM-J210F	Mem	Smssamsung.raw
Samsung	SM-J210F	Mem	Wasamsung.raw

Berdasarkan Tabel 3, hasil dari akuisisi mendapatkan *file-file* dari masing-masing *smartphone* sebagai barang bukti digital, pada *smartphone* korban mendapatkan logasus.raw, smsasus.raw, waasus.raw sedangkan *smartphone* pelaku yaitu logsamsung.raw, smssamsung.raw, wasamsung.raw.

4.C Examination

Disini kita mengecek nilai hash sebagai bukti digital dengan menggunakan *tools* FTK (Forensic Tool Kit) yang bertujuan untuk verifikasi *file* bukti digital jika diperiksa kembali *file* tersebut masih asli dan tidak ada perubahan maupun modifikasi.

Tabel 4.Nilai hash file dari *smartphone* korban

Nama *file*	MD5	SHA1
Logasus.raw	8F16AAE09A67AA3F56F28904009747F5	2EE395FC345769A5BF1FAB23972A6D724B47B44F
Smsasus.raw	26E3DBD91CF924B41E141E9CE3DC8208	206D799371375254603BC600044F05C2CBD59667
Waasus.raw	DD0ABD93A926456D61D4D702AFD92D42	6E9F662A618A9F4F2731F63C1C99C64AA4D74CF4

Berdasarkan Tabel 4, nilai hash dari *random access memory* yang diperiksa ada dua kategori yaitu MD5 dan SHA1, untuk *file* logasus.raw memiliki nilai hash 8F16AAE09A67AA3F56F28904009747F5 MD5, 2EE395FC345769A5BF1FAB23972A6D724B47B44F SHA1, *file* Smsasus.raw memiliki nilai hash 26E3DBD91CF924B41E141E9CE3DC8208 MD5, 206D799371375254603BC600044F05C2CBD59667 SHA1, *file* waasus.raw memiliki nilai hash DD0ABD93A926456D61D4D702AFD92D42 MD5, 6E9F662A618A9F4F2731F63C1C99C64AA4D74CF4 SHA1.

Tabel 5. Nilai hash file dari *smartphone* pelaku

Nama *file*	MD5	SHA1
Logsamsung.raw	2AF4DBFAEA80C9F2B38AD11E02442279	B500F84FD32CEEDD6B8C65153ECAA478811F1B3E
Smssamsung.raw	59D230AAD78CF01C21F52DC79EBD5275	903A3281AAB6D9613629F755A840FC08AC0156FD
Wasamsung.raw	FAEAF6B2815026E9B86587393F99BC56	5033D7E58E98B9995D4DA85F61FF61FB02350C5A

Berdasarkan Tabel 5, nilai hash dari *random access memory* yang diperiksa ada dua kategori yaitu MD5 dan SHA1, untuk *file* logsamsung.raw memiliki nilai hash 2AF4DBFAEA80C9F2B38AD11E02442279 MD5,B500F84FD32CEEDD6B8C65153ECAA478811 F1B3E SHA1, *file* Smssamsung.raw memiliki nilai hash 59D230AAD78CF01C21F52DC79EBD5275 MD5,903A3281AAB6D9613629F755A840FC08AC01 56FD SHA1, *file* wasamsung.raw memiliki nilai hash FAEAF6B2815026E9B86587393F99BC56 MD5,5033D7E58E98B9995D4DA85F61FF61FB02350 C5A SHA1.

4.D Analysis

Mencari bukti-bukti kejahatan yang belum dihapus dari *smartphone* korban dan mencari bukti kejahatan yang telah dihapus dari *smartphone* pelaku berdasarkan *file* bukti digital yang didapatkan dari *random access memory* melalui *tools* FTK (Forensic Tool Kit).

Tabel 6. Hasil analisis temuan bukti kejahatan

Bukti Digital	**Hasil analisis *Smartphone* korban**	**Hasil analisis *Smartphone* pelaku**
Log *file* Chat SMS	+628122987**** Siang mas ini saya agung dari jawabarat, ingin menawarkan senjata api rakitan untuk pegangan menjaga diri, jika minat balas pesan ini mas. Kami menawarkan harga yang sangat terjangkau	+628132742**** Siang mas ini saya agung dari jawabarat, ingin menawarkan senjata api rakitan untuk pegangan menjaga diri, jika minat balas pesan ini mas. Kami menawarkan harga yang sangat terjangkau
Chat Whatsapp	Ini senjata illegal atau legal ya mas? Bisa lihat foto senjatanya Ini illegal mas tapi dijamin keamanannya dan ini kami beri dengan harga yang terjangkau. Seperti ini mas senjata rakitan yang kami jual. Wah, ini illegal berarti tidak ada ijin mas dari pihak yang berwajib, dan kegiatan anda ini bisa saya laporkan kepada pihak berwajib karena melanggar undang-undang dengan menjual senjata illegal yang tidak memiliki ijin. Saya akan laporkan mas Kalau anda berani lapor polisi saya akan cari dan tembak anda.	Ini senjata illegal atau legal ya mas? Bisa lihat foto senjatanya Ini illegal mas tapi dijamin keamanannya dan ini kami beri dengan harga yang terjangkau. Seperti ini mas senjata rakitan yang kami jual. Wah, ini illegal berarti tidak ada ijin mas dari pihak yang berwajib, dan kegiatan anda ini bisa saya laporkan kepada pihak berwajib karena melanggar undang-undang dengan menjual senjata illegal yang tidak memiliki ijin. Saya akan laporkan mas Kalau anda berani lapor polisi saya akan cari dan tembak anda.
File Image	IMG-20191206-WA0000.jpg	IMG-20191206-WA0004.jpg

Dari hasil analisis terdapat log *file* panggilan keluar dari *smartphone* pelaku dengan nomor +628132742**** dan log panggilan masuk dari *smartphone* korban dengan nomor +628122987****, dan chat sms maupun chat whatsapp terlihat sama serta *file* image yang diterima pada *smartphone* korban yaitu IMG-20191206-WA0004.jpg dan *file* image yang terkirim dari *smartphone* pelaku yaitu IMG-20191206-WA0000.jpg.

4.E Reporting

Melakukan uji banding dengan mencocokkan hasil analisis dari kedua *smartphone*, untuk mendapatkan kesimpulan bahwa pelaku melakukan kejahatan tersebut.

Tabel 7. Uji perbandingan bukti digital

Hasil analisis	**Log file**	**Chatting SMS**	**Chatting Whatsapp**	**File Image**	**Keterangan**
Smartphone Korban	✓	✓	✓	✓	Sama
Smartphone Pelaku	✓	✓	✓	✓	Sama

Berdasarkan Tabel 7 ini uji perbandingan hasil analisis dari kedua *smartphone* android ditemukan bukti-bukti yang sama, dan kesimpulannya telah berhasil melakukan analisis bukti digital RAM pada *smartphone* pada kasus penjualan senjata illegal menggunakan metode *live forensic*. Dan pelaku terbukti melakukan perdagangan senjata illegal, menawarkan dan menjual ke warga sipil yang tidak memiliki hak untuk memiliki senjata, dan pelaku beerusaha menghapus rekam jejak digital dengan cara menghapus log panggilan telephone, chat SMS, dan Whatsapp.

5. KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa dengan menggunakan mem*tools* untuk mengcapture data pada *Random Access Memory* secara menyeluruh dengan menggunakan FTK (Forensic Tool Kit) peneliti dapat mencari bukti-bukti kejahatan yang telah dihapus maupun belum dari *smartphone* pelaku. Hasil yang didapat berupa log panggilan masuk pada *smartphone* korban yaitu nomor telephon pelaku +628132742****, sedangkan pada *smartphone* pelaku terdapat log *file* panggilan keluar yaitu nomor telephone korban +628122987****. Lalu pada SMS terdapat percakapan pelaku dengan korban, yaitu pelaku menawarkan kepada korban senjata illegal. Pada pesan Whatsapp dari *smartphone* pelaku, terdapat *file* gambar yang terkirim yaitu IMG-20191206-WA0004.jpg dan *file* gambar yang diterima pada *smartphone* korban yaitu IMG-20191206-WA0000.jpg

DAFTAR PUSTAKA

Al-Azhar, M. N (2013). Digital Forensic Panduan Praktis Investigasi Komputer.Jakarta: Salemba Infotek.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics. 800-101.USA: CreateSpace Independent Publishing Platfrom.

Donnie, R. T., & Tindall, D. (2015). Learning Android Forensic. Birmingham:Packt Publishing Ltd.

Ermadi, S. W., & Teguh, S. Analisis Bukti Digital Pada *Random Access Memory* Android Menggunakan Metode *Live forensic* Kasus Penculikan Anak.

Suhariyanto. (2017). Statistik Kriminal 2018. (S. S. P. dan Keamanan, Ed.),04330.1802.Jakarta: Badan Pusat Statistik.

Yudhana, A., Riadi, L., & Ashori, I. (2018). Analisis Bukti Digital Facebook Messanger Menggunakan Metode Nist. IT Journal Research and Development, 3(1), 13-21.

Yudhistira, D. S., Riadi, I., & Prayudi, Y. (2018). *Live forensic* Analysis Method For *Random Access Memory* On Laptop Devices. International Journal of Computer Science and Information Security, 16(4), 188-192.