Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android dengan metode NIST

Feryan Lutfie Nafila[1], Yudi prayudi[2]
[1,2]Jurusan Informatika Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta
17917207@students.uii.ac.id, prayudi@uii.ac.id

Abstract

Message applications have now become a part of today's society. Beside from features, security and privacy are important things for users. Security and privacy are important because some users of this application are worried if the message their send will misused by the company. This concern is heightened after a new rule issued by a popular instant messaging application company where data from the messaging application will be linked to other applications for business purposes, some popular messenger users are worried about their privacy choosing to switch to other messaging applications that are considered more secure and offers privacy. One of the applications of choice is Signal Messenger becouse this application is more secure in maintaining privacy. This is a concern if applications that offer more privacy become a means to commit crimes. Consider that, the research work will focused on conducting forensic testing and analysis of the Android-based Signal Messenger application. The test will carried out on SMA530F and RedmiNote 4 smartphone devices. The scenario that will applied is by installing the Signal Messenger application on each smartphone, then communication between the two smartphones is such as sending text messages, images, and videos. From these activities, the mobile forensics stage using the NIST method such as making acquisitions and then analysis to obtain digital evidence. The test results will be expect for a reference for the authorities and related parties if there is a case using the Signal Messenger application and it is hoped that this research can add to the literature in the field of digital forensics, especially mobile forensics.

Keywords*: mobile forensic, signal messenger, android.*

Abstrak

Aplikasi pesan singkat saat ini sudah menjadi bagian yang melekat pada masyarakat. Selain fitur yang ditawarkan, keamanan dan privasi adalah hal yang penting bagi pengguna. Keamanan dan privasi menjadi penting karena beberapa pengguna aplikasi ini menjadi khawatir dengan data pesan yang mereka kirimkan akan disalahgunakan oleh perusahaan aplikasi pesan tersebut. Kekhawatiran ini semakin tinggi setelah aturan baru yang dikeluarkan oleh perusahaan aplikasi tersebut dimana data dari aplikasi pesan akan dihubungkan dengan aplikasi lain untuk keperluan bisnis perusahaan, beberapa pengguna aplikasi tersebut merasa khawatir akan privasi mereka memilih untuk beralih ke aplikasi pesan lain yang dirasa lebih aman dan menawarkan privasi. Salah satu aplikasi yang menjadi pilihan adalah Signal Messenger karena aplikasi ini dianggap lebih aman dalam menjaga privasi. Hal ini menjadi perhatian apabila aplikasi yang lebih menawarkan privasi ini menjadi sarana untuk melakukan tindak kejahatan. Dengan mempertimbangkan hal tersebut, maka karya penelitian difokuskan untuk melakukan pengujian dan analisa forensik terhadap aplikasi Signal Messenger berbasis android. Pengujian akan dilakukan pada perangkat smartphone SMA530F dan RedmiNote 4. Skenario yang akan dilakukan dengan pemasangan aplikasi Signal Messenger pada setiap smartphone, kemudian dilakukan komunikasi antara kedua smartphone tersebut seperti mengirim pesan teks, gambar, dan video. Dari aktivitas tersebut dilakukan tahap mobile forensik menggunakan metode NIST seperti melakukan akuisisi dan kemudian dilakukan analisa untuk mendapatkan bukti digital. Hasil pengujian diharapkan bisa menjadi referensi pihak berwenang maupun pihak terkait apabila terdapat suatu kasus

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

dengan menggunakan aplikasi Signal Messenger. Dan diharapkan dengan adanya penelitian ini bisa menambah kepustakaan dibidang ilmu digital forensik khususnya mobile forensik.

***Kata kunci**: mobile forensik, signal messenger, android.*

1. PENDAHULUAN

Penggunaan aplikasi pesan singkat berbasis online saat ini sudah menjadi salah satu kegiatan sehari-hari, selain menawarkan kemudahan dalam berkomunikasi berbagai fitur yang disediakan oleh beragam aplikasi pesan singkat online menjadi daya tarik aplikasi ini. Namun dibalik kemudahan tersebut terdapat aplikasi popular yang mengeluarkan aturan baru berkaitan dengan privasi pengguna. Aturan baru tersebut membahas tentang kebijakan privasi yang akan menghubungkan data pengguna ke aplikasi lain untuk keperluan bisnis, beberapa pengguna mulai mempertimbangkan penggunakan aplikasi *messenger* lain karena merasa khawatir dengan privasi mereka seperti aplikasi *messenger* Signal. Setelah keluarnya aturan baru tersebut peningkatan pengunduh Signal menjadi 2 juta per hari setelah sebelumnya hanya 20 ribu per hari.

Meningkatnya penggunaan aplikasi *messenger* yang menawarkan keamanan dan privasi menjadi bukti kekhawatiran para pengguna aplikasi *messenger* peduli terhadap privasi mereka dalam menggunakan aplikasi *messenger* tersebut. Disisi lain semakin tinggi tingkat privasi sebuah aplikasi maka semakin sedikit pula hal yang bisa dibuka atau diungkap karena faktor keamanan yang dimiliki oleh aplikasi tersebut, hal ini menjadi perhatian bila mana aplikasi yang menawarkan privasi ini dimanfaatkan oleh seseorang sebagai media komunikasi untuk melakukan tindak kejahatan sehingga akan menyulitkan bagi seorang penyidik untuk menggali bukti yang terdapat pada aplikasi *messenger* tersebut.

Permasalahan yang akan dibahas di dalam penelitian ini adalah bagaimana sebuah proses digital forensik khususnya mobile forensik dalam rangka mencari jejak digital yang terdapat pada aplikasi Signal Messeger dengan menggunakan metode *National Institute of Standard and Technology* (NIST) sehingga jejak digital tersebut bisa dijadikan sebagai barang bukti dalam sebuah kasus. Digital forensik harus dilakukan sesuai dengan standar operasional untuk menjamin tidak ada terjadi perubahan terhadap media digital yang akan di forensik selama proses investigasi, Selain itu menurut penelitian [1] forensik digital adalah sebuah cabang ilmu forensik dengan penggunaan ilmu dan metode ilmiah dalam mencari dan menemukan barang bukti digital untuk merekonstruksi peristiwa kejahatan yang terjadi dengan tahapan-tahapan yang terstruktur sehingga dapat diterima dalam pengadilan untuk penegakkan hukum.

Didalam Forensik digital sendiri mempunyai beberapa sub disiplin ilmu dan turunannya. [2] menjabarkan bahwa subdisiplin ilmu dalam dunia forensik digital. Namun dalam subdisiplin ilmu Komputer Forensik, juga terdapat banyak turunan subdivisi ilmu dalam forensik digital lainnya. Yang

mana setiap subdisiplin membutuhkan teknik dan metode yang berbeda dalam pencarian barang bukti digitalnya.

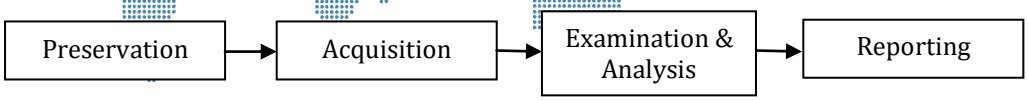
Tujuan utama dari mobile forensik adalah mencari dan menggali berbagai informasi yang terkandung dalam mobile devices yang berpotensi sebagai alat bukti digital untuk kemudian dianalisa dan diolah agar dapat dihadirkan ke tengah persidangan sebagai alat bukti yang sah tanpa mengurangi kaedah dari aturan dan metode digital forensik sehingga hasilnya dapat dipertanggung jawabkan. Dari sudut pandang forensik digital dalam hal ini melakukan investigasi pada perangkat mobile dapat memberikan banyak barang bukti tentang pengguna dan kemampuan lain terkait pemulihan informasi tambahan sebagai barang bukti [3]. Bukti digital didefinisikan sebagai data yang disimpan atau dikirimkan menggunakan komputer yang digunakan untuk mendukung atau menyangkal teori tentang bagaimana suatu pelanggaran terjadi atau elemen-elemen penting dari pelanggaran tersebut [4]. Data yang dimaksud kombinasi dasar dari angka-angka yang merepresentasikan dari berbagai jenis informasi seperti teks, gambar, audio, dan video. Pada jurnal [5] membagi bukti digital ke dalam dua kategori menurut sumber pembuatannya yaitu *user-created* dan *computer-created*. Dari kedua kategori tersebut dijabarkan hal hal yang bisa dijadikan sebagai barang bukti.

a. *User-created*
   1) Teks Teks (dokumen, e-mail, pesan)
   2) *Database*
   3) Halaman web
   4) Video dan Foto
   5) Gambar dan Foto
b. *Computer-created*
   1) *Logs*
   2) *Metadata*
   3) *Browser cache, history, cookies*
   4) *File printer spool*
   5) *File backup dan registry*

Penelitian [6] meneliti tentang aplikasi *messenger* whatsapp. Keamanan yang digunakan whatsapp adalah teknologi enkripsi terbaru yaitu enkripsi *end-to-end*, hal ini menjadi tantangan peneliti dalam memecahkan enkripsi tersebut. Peneliti berkesperimen menggunakan metode NIST untuk mengekstrak artefak whatsapp. Metode NIST ini juga dipakai pada penelitian [7][8][9][10]. Metode NIST atau National Institute of Standard and Technology merupakan badan yang bertanggung jawab didalam mengembangkan standar, panduan, dan persyaratan minimum untuk menyediakan keamanan informasi yang cukup bagi semua asset dan pihak-pihak yang memiliki kompetensi di bidang digital forensik, metode ini dipergunakan oleh para agen pemerintah pusat di Amerika, namun tidak menutup kemungkinan dapat dipergunakan oleh organisasi seperti akademisi, badan penyidik swasta dan lainnya.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Metode ini mempunyai empat tahapan proses yaitu *Preservation*, *Acquisition*, *Examination & Analysis*, dan *Reporting*.



Gambar 1. Tahap Metode NIST

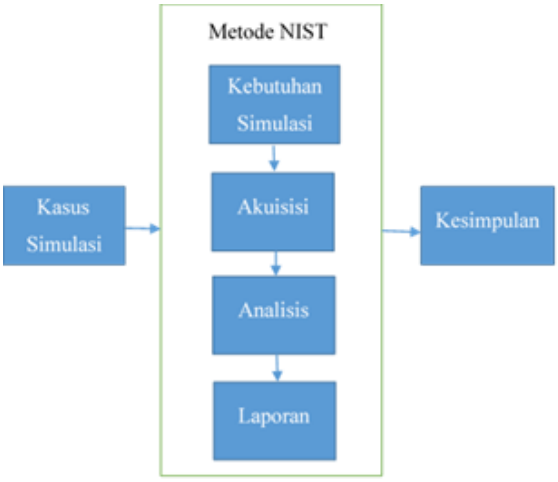
a. *Preservation*
   Dalam tahap ini dilakukan persiapan apa saja yang menjadi kebutuhan untuk melakukan proses analisa forensik. Seperti mempersiapkan barang bukti yang akan dianalisa, Alat yang akan dipakai atau diperlukan, serta alat-alat untuk melakukan dokumentasi.
b. *Acquisition*
   Dalam tahap ini dilakukan proses persalinan atau imaging terhadap ponsel pintar yang menjadi barang bukti menggunakan alat yang telah dipersiapkan. Tujuan dari proses persalinan ini adalah untuk melindungi keutuhan atau integrasi dari barang bukti pada saat melakukan pemeriksaan lebih lanjut terhadap barang bukti tersebut. Salinan tersebut kemudian disertai nilai hash untuk memastikan bahwa salinan ini sama dengan yang asli sesuai apa yang terdapat dalam barang bukti.
c. *Examination & Analysis*
   Dalam tahap ini selanjutnya proses pemeriksaan dan analisis dilakukan. Pemeriksaan diperlukan untuk mengidentifikasi keterkaitan suatu barang bukti dengan kasus yang sedang ditangani. Kemudian hasil dari pemeriksaan tersebut dikumpulkan untuk selanjutnya ditarik sebuah kesimpulan.
d. *Reporting*
   Setelah semua tahapan dan prosedur dijalankan dengan benar, kemudian dibuat laporan hasil.

Disini peneliti [8] membandingkan dan mengevaluasi alat forensik dalam penanganan aplikasi whatsapp. Beberapa aplikasi yang digunakan antara lain yaitu WhatsApp Key/DB Extractor, Belkasoft Evidence (ver trial), DB browser SQLite. Kemudian peneliti [13] juga membandingkan beberapa alat forensik sperti Oxygen Forensic, MOBILedit Forensic dan Beberapa aplikasi ini juga digunakan oleh peneliti [6] yang menggunakan DB browser SQLite untuk menbuka database hasil akuisisi pada aplikasi instant *messenger* IMO.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

2. METODOLOGI PENELITIAN

Penelitian ini bertujuan untuk mencari jejak digital yang bisa digunakan sebagai sebagai barang bukti pada sebuah kasus kejahatan. Disini peneliti membuat sebuah alur seperti pada gambar 2 tentang bagaimana proses penelitian ini nanti akan berjalan. Lemudian untuk melengkapi alur tersebut disini peneliti akan membuat sebuah simulasi kasus sebagai objek pada penelitian ini.



Gambar 2. Alur Penelitian

Dalam mendukung simulasi tersebut, maka dibuatkan sebuah skenario kasus yang bertujuan sebagai objek model untuk melakukan pengujian sebagai berikut:

1) Penelitian menggunakan 2 buah *smartphone* android dengan model berbeda
2) Kedua *smartphone* tersebut telah terpasang aplikasi pesan Signal *Messenger*
3) Antar *smartphone* saling berkirim pesan teks, gambar, file, video, dan melakukan panggilan suara maupun panggilan video
4) Beberapa pesan akan dihapus sebagai bagian dari scenario

Kemudian setelah semua kebutuhan penelitian telah disiapkan langkah selanjutnya adalah proses akuisisi. Dalam melakukan akuisisi sebuah perangkat *mobile* membutuhkan bantuan komputer untuk memperoleh data akuisisi. Sebuah perangkat *mobile* akan disambungkan kedalam komputer menggunakan kabel data kemudian pada komputer menggunakan aplikasi *software* forensik untuk melakukan akuisisi dan analisis seperti yang terlihat pada gambar 3 berikut.

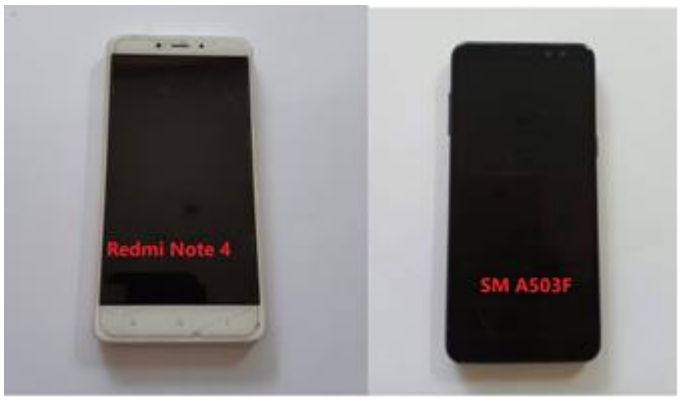
Gambar 3. Alur Akuisisi

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Setelah data hasil akuisisi diperoleh tahap selanjutnya yaitu adalah tahap analisis. Analisis adalah usaha dalam mengamati sesuatu secara mendetail dengan cara menguraikan komponen pembentuknya atau menyusun sebuah komponen untuk kemudian dikaji lebih mendalam. Menurut [11] pengertian analisis adalah suatu kegiatan memperhatikan, mengamati, dan memecahkan suatu masalah mencari seperti jalan keluar yang dilakukan oleh seseorang. Dalam penelitian dimana menggunakan kasus sebagai objek, analisis diperlukan untuk mencari dan mengamati jejak digital yang bisa dijadikan alat bukti elektronik sebagai pengembangan dalam menyelesaikan kasus tersebut.

3. HASIL DAN PEMBAHASAN

Dalam Penelitian ini simulasi menggunakan dua buah perangkat *smartphone* sebagai media penelitian. Disini perangkat yang akan digunakan adalah dua *smartphone* android yaitu Samsung *SM A530F* dan *Redmi Note 4*.



Gambar 4. Perangkat Seluler

Kedua *smartphone* seperti pada gambar 4 telah terpasang aplikasi Signal *Messenger* dan telah saling mengirim pesan berdasarkan kasus yang disimulasikan seperti mengirim pesan teks, gambar video, dokumen, panggilan suara dan video. Kemudian tahap selanjutnya adalah melakukan proses akuisisi atau proses imaging terhadap kedua perangkat *smartphone* tersebut menggunakan PC. Disini peneliti menggunakan *software* Magnet AXIOM 4.10 dalam malakukan akuisisi baik *physical* maupun *logical*.

```
Relative Segment 1 Path: redmi note 4 - physical.raw
Full Segment 1 Path: C:\Users\RYAN\Documents\Tesis\Magnet File\Kasus01 - Nov 19 2021 234014\redmi note 4 - physical.raw
Segment 1 MD5 Hash: 85090C222E7EBCE790CF5C20CEB6E23E
Segment 1 SHA1 Hash: 32D880CACF4C2127A187C26E557AD9010B5F7B1D

Relative Segment 2 Path: samsung A530F physical.raw
Full Segment 2 Path: C:\Users\RYAN\Documents\Tesis\Magnet File\Kasus01 - Nov 19 2021 234014\samsung A530F physical.raw
Segment 2 MD5 Hash: B9CF2060F16475E871D946C3D3428242
Segment 2 SHA1 Hash: 600C9036FF0B15037EB276EAAB7F221C9E5944BC
```

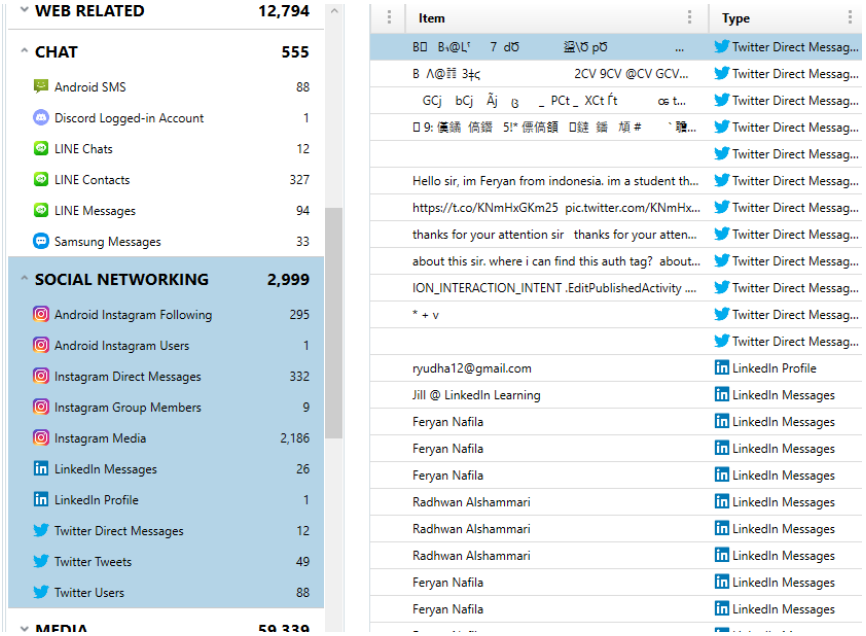
Gambar 5. Laporan Hasil Akuisisi

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Setelah proses akuisisi selesai seperti pada gambar 5 terlihat bahwa file hasil akuisisi adalah file *.raw* dari gambar tersebut juga ditampilkan nilai hash dari masing masing file akuisisi. Kemudian penelitian berlanjut pada analisis hasil akuisisi. Disini peneliti menggunakan beberapa *software* sebagai media analisis.

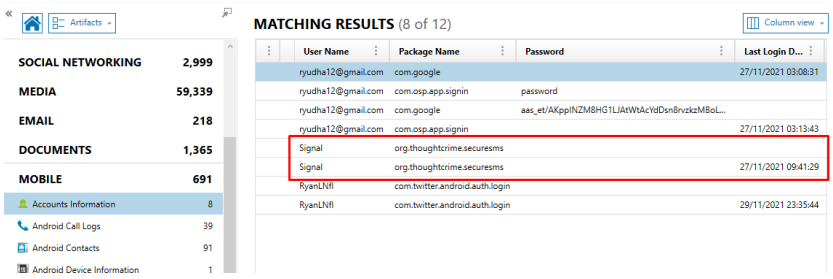
a) Magnet AXIOM 4.10

Magnet AXIOM mempunyai kemampuan untuk mengelompokkan data berdasarkan beberapa kategori. Analisis dimulai dengan membuka file *.raw* hasil akuisisi. Setelah proses membuka file selesai kemudian peneliti berfokus pada kategori *chat* dan *social networking* untuk kemudian dianalisis tentang keterkaitan data yang ditampikan dengan aplikasi yang sedang diteliti yaitu Signal *Messenger*.



Gambar 6. Tampilan Chat dan Social Networking Magnet AXIOM

Seperti yang terlihat pada gambar 6 pada tab *chat* dan *Social Networking* tidak ditemukan aplikasi Signal. Hanya beberapa social media lain seperti Intagram, Line, Twitter, maupun LinkedIn yang dapat ditampilkan. Kemudian penelitian berlanjut pada data kategori Mobile.



Gambar 7. Tampilan Tab Mobile

Pada tab mobile seperti pada gambar 7 terdapat informasi mengenai akun dengan rincian *username*, *package name*, dan *last login*. Berdasarkan informasi tersebut bahwa terdapat akun Signal *Messenger*, kemudian nama paket folder tempat tersimpan data dari signal *messenger* yaitu pada folder *org,throughtcrime.securesms* diinformasikan juga untuk terakhir aplikasi Signal *Messenger* ini digunakan. Setelah mengetahui folder tempat data itu disimpan yaitu pada folder *org,throughtcrime.securesms* penelitian kemudian berlanjut untuk melakukan analisis pada folder yang tersimpan pada *path:\data\data\org.thoughtcrime.securesms*. Data yang ditampilkan pada *software* Magnet AXIOM berisi 14 buah folder kemudian pada folder databases tersimpan file *signal.db* namun file database tersebut tidak bisa dibuka karena Magnet AXIOM tidak mampu membuka enkripsi yang dimiliki file databse tersebut.

b) MobileEdit Express 7.1

Pada *software* Mobiledit Forensic peneliti menggunakan seri Express versi 7.1. analisis dimulai dengan membuka file akuisisi. Pada pilihan analisis, dikhususkan untuk menganalisis aplikasi *messenger* Signal. Kemudian hasil bukaan akuisisi tersebut menghasilkan file *pdf_files, log_full, log_short, Report, report_configure.cfg*. Pada file Report terdapat informasi nomor akun yang digunakan yaitu +6582134449617 selain itu juga terdapat sebuah *file image* yang teridentifikasi namun tidak menampilkan gambar dari file tersebut.

c) Autopsy 4.18.0

Analisis dimulai dengan membuka file akuisisi. Setelah terbuka, Autopsy menampilkan informasi bahwa terdapat aplikasi Signal *Messenger* yang terpasang pada *smartphone*. Namun pada *tab account* tidak ditemukan data dari Signal *Messenger*. Selain itu Autopsy juga menampilkan informasi bahwa terdapat file *signal-logs.db*, *signal.db*, *signal-jobmanager.db* yang diindikasi terenkripsi. Hasil dari beberapa informasi yang ditampilkan masing masing *software* peneliti rangkum dalam tabel 1 berikut.

Tabel 1. Perbandingan Analisis Data Akuisisi

Perangkat	Software	Data informasi hasil analisis			
		Aplikasi	Akun	Database	Informasi lain
SM A530F	Magnet AXIOM	✓	✓	terenkripsi	Terdapat keterangan *last login*
	MobileEdit Express	✓	✓	terenkripsi	Nomor akun pengguna ditampilkan
	Autopsy	✓	n/a	terenkripsi	Beberapa file Signal *Messenger* terdeteksi enkripsi

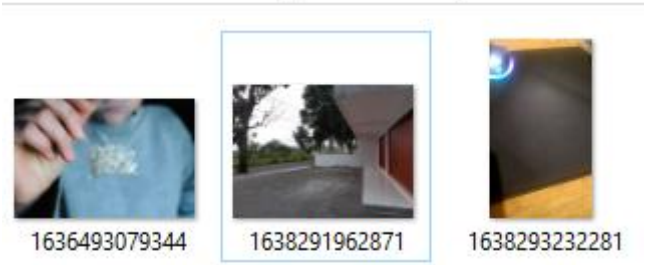
Redmi Note 4	Magnet AXIOM	✓	✓	terenkripsi	Terdapat keterangan *last login*
	MobileEdit Express	✓	✓	terenkripsi	Nomor akun pengguna ditampilkan
	Autopsy	✓	n/a	terenkripsi	Beberapa file Signal *Messenger* terdeteksi enkripsi

Selain database untuk menyimpan data pesan, aplikasi Signal *Messenger* juga mempunyai fitur berupa *backup*. Bila fitur ini diaktifkan, maka aplikasi ini akan membuat sebuah *backup* dari database disertai kunci yang bisa digunakan untuk membuka file *backup* tersebut. *Backup* file ini bisa menjadi alternative bagi peneliti untuk melihat data yang terdapat pada Signal *messenger* selain data dari database. Penelitian akan mengunakan 2 aplikasi yang berjalan pada berbasis *command propt* yaitu *signal-back* dan *signalbackup-tools.*

d) Signal-back

Melalui *command propt*. Disini peneliti mencoba mengangkat file yang terdapat pada file *backup* tersebut dengan perintah *signal-back_windows_368,axe format –f XML –o backup.xml signal-2021-11-20-21-08-32.backup.* setelah proses selesai didapat file dengan format *.xml* namun ketika dibuka, file ini tidak menampilkan data apapun.

Kemudian peneliti mencoba untuk mengangkat file media dengan menggunakan perintah *signal-back_windows_386.exe extract -o output signal-2021-11-20-21-08-32.backup.* Setelah proses selesai, terdapat media gambar dan video yang berhasil diangkat seperti pada gambar 8 berikut.

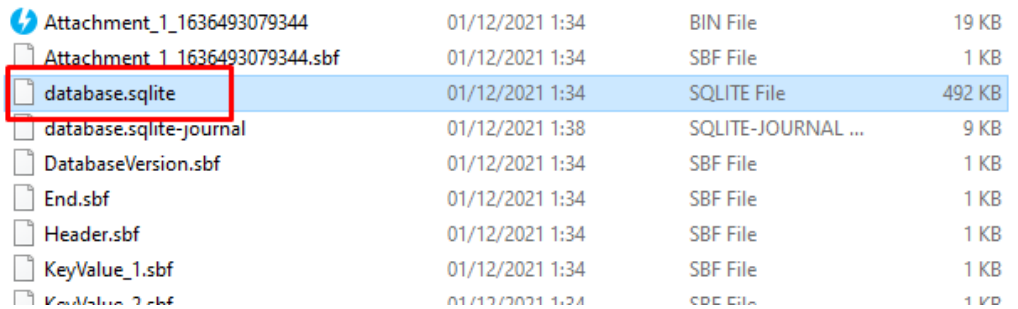


Gambar 8. Hasil Ekstrak Media

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 1, Maret 2022, pp. 532-543
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

e) Signalbackup-tools

Seperti pada dengan Signal-Back diatas, peneliti mencoba menarik data yang terdapat pada *file backup signal*. Disini peneliti menggunakan perintah *signalbackup-tools_win.exe --output signalbackup/ signal-2021-11-20-21-08-32.backup 464475992745685524810042631814 pada command prompt.* Setelah proses selesai terdapat beberapa file yang bisa terangkat. Salah satunya adalah file database signal bernama database.sqlite seperti gambar 9 berikut. Kemudian penelitian berlanjut dengan membuka file *database.sqlite* tersebut menggunakan *software DB Browser for SQLite* dan diperlihatkan bahwa terdapat 45 tabel pada database tersebut. Beberapa tabel seperti tabel *sms, mms, part, dan thread* berisikan data chat, gambar, video, dan file dokumen. Namun informasi mengenai data panggilan suara maupun video tidak terlihat pada database ini. Hasil dari analisis data *backup* ini penulis rangkum dalam tabel 3 berikut.



Gambar 9. File Database

Tabel 1. Perbandingan Analisis Data Backup

Perangkat	Software	Artifak Pada Database					
		Pesan Teks	Pesan Gambar	Pesan Video	Panggilan Suara	Panggilan Video	File Dokumen
Samsung SM A530F	Signal-Back	n/a	✓		n/a	n/a	✓
	Signalbackup-tools	✓	Informasi gambar		n/a	n/a	Informasi dokumen
Redmi Note 4	Signal-Back	n/a	✓		n/a	n/a	✓
	Signalbackup-tools	✓	Informasi gambar		n/a	n/a	Informasi dokumen

Berdasarkan latar belakang masalah mengenai proses mencari jejak digital aplikasi Signal *Messenger* berbasis Android dapat dirumuskan bahwa

untuk proses akuisisi tidak mengalami kendala. *Software* Magnet AXIOM mampu melakukan akuisisi dengan baik. Kemudian dalam proses analisis artifak hasil akuisisi, *software* yang digunakan tidak mampu membaca database dari aplikasi Signal Messenger karena database *signal.db* dilindungi oleh enkripsi. Namun beberapa informasi seperti nomor akun yang digunakan, kemudian beberapa informasi kapan aplikasi terakhir digunakan masih bisa ditampilkan.

Pada analisis data *backup*, dua *software* yang digunakan yaitu Signal-Back dan Signalbackup-tools mampu mengekstrak data dari file *backup*. Pada Signal-Back terdapat kendala ketika proses ektraksi *database file .xml* yang dihasilkan tidak menampilkan data apapun namun untuk data lain seperti gambar, video, dan file dokumen bisa ekstrak dengan baik. Pada *software* Signalbackup-tools database berhasil dienktrak kemudian database tersebut dianalisis menggunakan DB Browser for SQLite dimana beberapa artifak seperti pesan teks, gambar, video, dan file dokumen tercatat pada tabel. Disini penulis menemui kendala dan tidak bisa menemukan data untuk panggilan suara maupun panggilan video.

4. SIMPULAN

Setelah dilakukan serangkaian penelitian dan analisa terhadap perangkat android Samsung SM A530F dan Redmi Note 4 terkait penelitian aplikasi Signal *Messenger* versi 5.27.13 dapat disimpulkan bahwa dalam penelitian ini penerapan metode NIST berjalan dengan baik. Akusisi dengan menggunakan *software* Magnet AXIOM 4.10 dan hasil Akuisisi terbaca dengan baik oleh *software* Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 namun *software* tersebut tidak dapat membaca database dari aplikasi Signal Messenger yang ter decrypt sehingga informasi mengenai pesan, media, video, file tidak dapat diperoleh. Analisis data *backup* dengan menggunakan *software* Signal-back mampu menampilkan media yang tersimpan dalam data *backup* seperti gambar, video, file sedangkan untuk *software* Signalbackup-tools file database dapat didecrypt dan diektrak dan kemudian data pada pada database dapat ditampilkan dan menyimpan informasi seperti pesan teks, pesan gambar, pesan video serta informasi file dokumen namun tidak ditemukan data mengenai panggilan suara maupun panggilan video. Dari beberapa *software* yang telah diuji beberapa digital artifak yang berhasil didapat dan kemudian bisa dijadikan sebagai barang bukti adalah data pesan teks, media gambar, media video, dan file dokumen. Pada penelitian ini beberapa *software* yang digunakan seperti Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 belum mampu untuk membaca database aplikasi Signal Messenger yang terenkripsi. Kemudian *software* Signal-back dan Signalbackup-tools yang digunakan untuk melakukan decrypte pada data *backup* tidak mampu menampilkan panggilan suara dan panggilan video. Oleh karena itu diharapkan untuk penelitian berikutnya mampu melakukan analisis lebih lanjut dengan file akuisisi serta data *backup* yang dapat menampilkan informasi lebih lengkap.

DAFTAR PUSTAKA

[1] S. H. S. Halim, "Panduan Praktis Dijital Forensik," 2012.

[2] L. Daniel and L. Daniel, "Digital Forensics for Legal Professionals," *Digital Forensics for Legal Professionals*. 2012, doi: 10.1016/C2010-0-67122-7.

[3] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Cell Phone Forensics Guidelines on Mobile Device Forensics," *Arch. NIST Tech. Ser. Publ. Arch. Publ.*, vol. 1, 2007, [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-101r1http://csrc.nist.gov/groups/SNS/mobile_security/index.htmlN/A.

[4] E. Casey, *Digital Evidence and Computer Crime*. Elsevier Science, 2011.

[5] R. J. Hsieh, "Digital evidence and computer forensics," *Introd. to Forensic Sci. Crim.*, pp. 201–221, 2019, doi: 10.4324/9781315119175-9.

[6] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[7] Muhammad Kukuh Tri Haryanto, "Analisa Forensics Terhadap Database Sqlite pada Aplikasi IMO Berbasis Android," p. 17, 2018.

[8] J. Choi, J. Park, and H. Kim, "Forensic analysis of the backup database file in KakaoTalk messenger," *2017 IEEE Int. Conf. Big Data Smart Comput. BigComp 2017*, pp. 156–161, 2017, doi: 10.1109/BIGCOMP.2017.7881732.

[9] M. N. Fadillah, R. Umar, and A. Yudhana, "Rancangan Metode Nist Untuk Forensik Aplikasi Mobile Payment Berbasis Android," *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 2018, no. November, pp. 115–119, 2018, [Online]. Available: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2626.

[10] M. Praset yo Aji, I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," *Messenger Using NIST Mob. Foren… J. Comput er Sci. IJCSIS J. Comput er Sci.*, vol. 16, no. 5, pp. 201–205, 2018, [Online]. Available: https://sites.google.com/site/ijcsis/.

[11] N. M. Latuconsina and P. W. Yunanto, "Pembuatan Bank Soal Dan Analisis Butir Soal Mata Kuliah Kriptografi Untuk Mahasiswa Program Studi Pendidikan Teknik Informatika Dan Komputer Universitas Negeri Jakarta," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 1, no. 2, pp. 142–145, 2017, doi: 10.21009/pinter.1.2.7.