Analisis Kinerja Aplikasi Forensik *Open-Source* Pada Ponsel Cerdas Berbasis Android dalam Mendapatkan Bukti Digital

M. Machrush Aliy Sirojjam Mushlich [1*], Muhammad Andik Izzuddin [2], Mujib Ridwan [3]

[1,2,3]Sistem Informasi; Universitas Islam Negeri Sunan Ampel Surabaya;
Jl. Jend. A. Yani No. 117, Surabaya 60237; Telp (031) 8410298;
email: jampirojam@gmail.com, andik@uinsby.ac.id, mujibrw@uinsby.ac.id

Abstrak: Dewasa ini, forensik digital berkembang pesat sebagai upaya untuk mengungkap tindak kejahatan siber. *Mobile forensics* merupakan bagian dari forensik digital yang berfokus pada penanganan perangkat seluler. *NIST Special Publication 800-101 Revision 1* merupakan salah satu metode yang digunakan untuk melakukan analisis forensik pada perangkat seluler. Pada penelitian ini, *WhatsApp Key/DB Extractor*, BitPim, dan *Autopsy* dipilih untuk melakukan analisis forensik pada Samsung Young 2 Duos dalam mendapatkan artefak *WhatsApp*. Namun, BitPim mengalami eror saat dijalankan, karena BitPim tidak dapat mendeteksi ponsel yang digunakan, sehingga data yang ingin didapatkan kemudian diperiksa dan dianalisis menggunakan aplikasi BitPim tidak dapat dilakukan. Oleh karena itu, hanya *WhatsApp Key/DB Extractor* dan *Autopsy* yang digunakan. Hasil dari penelitian ini, aplikasi forensik tidak selalu dapat digunakan untuk setiap tahapan yang ada pada *NIST Special Publication 800-101 Revision 1*, dan aplikasi forensik juga tidak selalu dapat memenuhi setiap parameter yang telah ditetapkan. Sehingga secara keseluruhan terkait kinerja setiap aplikasi forensik maupun bukti digital yang ditemukan, baik jenis data, jumlah data, dan data yang dapat dibuka, *Autopsy* unggul dari *WhatsApp Key/DB Extractor* karena mampu mendapatkan indeks kuantitas sebesar 58.44%, sedangkan *WhatsApp Key/DB Extractor* hanya mendapatkan indeks sebesar 44.15%.

Kata kunci: Forensik Digital, Aplikasi *Open-Source*, *NIST*

Abstract: *Nowadays, digital forensic is growing rapidly in an effort to uncover cybercrime. Mobile forensics is a part of digital forensics that focuses on handling mobile devices. NIST Special Publication 800-101 Revision 1 is one of the methods used to perform forensic analysis on mobile devices. In this study, WhatsApp Key/DB Extractor, BitPim, and Autopsy were selected to perform forensic analysis on Samsung Young 2 Duos in collecting WhatsApp artifacts. However, BitPim encountered an error when running, because BitPim couldn't detect the phone being used, so the data that wanted to be obtain then checked and analyzed using BitPim application couldn't be done. Therefore, only WhatsApp Key/DB Extractor and Autopsy are used. The results of this study, forensic tools can't always be used for every stage of NIST Special Publication 800-101 Revision 1, and forensic tools also can't always comply every predefined parameter. So overall, it's related to the performance of each forensic application and the digital evidence found, both the type of data, the amount of data, and the data that can be opened, Autopsy is superior to WhatsApp Key/DB Extractor because it's able to get a quantity index of 58.44%, while WhatsApp Key/DB Extractor only get index of 44.15%.*

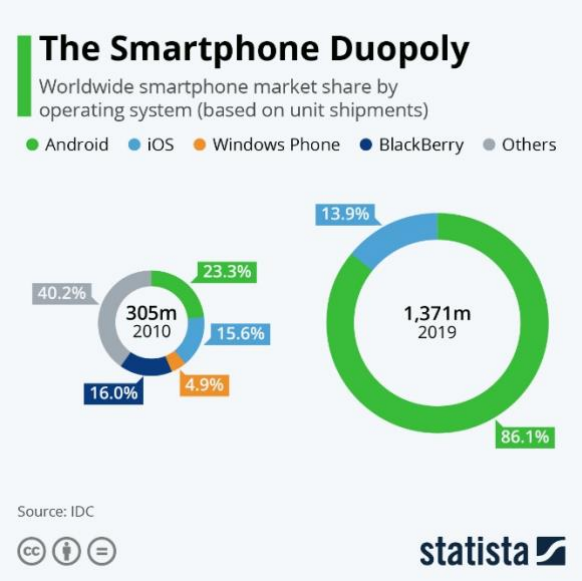
Keywords: Digital Forensic, Open-Source Applications, NIST

1. Pendahuluan

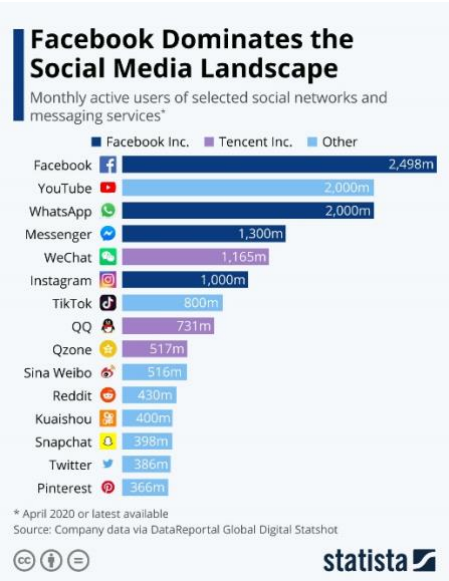
Teknologi informasi dewasa ini berkembang dengan pesat. Banyak pengguna memanfaatan teknologi informasi yang terdapat pada perangkat seluler untuk melakukan tindakan kejahatan siber (*cybercrime*) yang menyebabkan banyak kerugian jaringan *borderless* (Zuraida, 2015). Maraknya kejahatan yang menggunakan perangkat seluler, memunculkan bidang baru dari ilmu forensik, yakni *mobile forensic* yang mempelajari tentang proses pemulihan bukti digital (*digital evidence*) menggunakan aturan dan langkah yang tepat sesuai

dengan kondisi forensik pada perangkat seluler; bukti digital bersifat rentan rusak jika tidak ditangani dengan baik dan benar (Yadi & Kunang, 2014).

Pemilihan perangkat seluler serta aplikasi yang datanya akan dijadikan sebagai barang bukti berdasarkan data statistik dari Statista (2020). Perangkat seluler dengan sistem operasi Android saat ini menjadi perangkat dengan pejualan tertinggi di dunia seperti yang terdapat pada Gambar 1. Aplikasi *WhatsApp* menjadi aplikasi media sosial yang khusus digunakan untuk melakukan telepon dan berbagi pesan, baik yang berupa teks, gambar, audio, video, dokumen, dan *GPS* (*Global Positioning System*) seperti yang terdapat pada Gambar 2.



Gambar 1 Penjualan *Smartphone* Berbasis Sistem Operasi (Sumber: Statista)



Gambar 2 Pengguna Aktif Media Sosial (Sumber: Statista)

Penanganan pada perangkat seluler membutuhkan alat atau aplikasi forensik untuk memudahkan dalam mendapatkan bukti digital, baik aplikasi forensik *open-source* maupun *proprietary*; tidak semua aplikasi forensik dapat digunakan untuk semua ponsel. Namun, pada penelitian ini menggunakan aplikasi *open-source* karena mudahnya dalam mendapat akses tanpa kendala privasi serta biaya yang digunakan tidaklah banyak dalam pengadaannya. Terdapat daftar aplikasi forensik *open-source* pada penelitian yang telah dilakukan oleh Lohiya, John dan Shah (2015) yang tersaji pada Tabel 1, serta penelitian yang telah dilakukan oleh Patankar dan Bhandari (2014) seperti yang tersaji pada Tabel 2.

Tabel 1: Daftar Aplikasi Forensik *Open-Source* (Sumber: Hasil penelitian Lohiya, John dan Shah)

No.	Nama	Sistem Operasi	Ketersediaan	Keterangan
1	*Mobiledit Lite*	Windows	Tidak Tersedia	Semua Ponsel
2	*BitPim*	Windows	Tersedia	Semua Ponsel
3	*Autopsy*	Windows	Tersedia	Semua Ponsel

Tabel 2: Daftar Aplikasi Forensik *Open-Source* (Sumber: Hasil penelitian Patankar dan Bhandari)

No.	Nama	Sistem Operasi	Ketersediaan	Keterangan
1	*Oxygen Forensic Suite*	Windows	Tidak Tersedia	Semua Ponsel
2	*iPhone Analyzer*	Windows	Tersedia	Hanya iOS
3	*WhatsApp Key/DB Extractor*	Windows	Tersedia	Hanya *WhatsApp*
4	*Skype Extractor*	Windows	Tersedia	Hanya *Skype*
5	*SIM Manager*	Windows	Tersedia	Hanya SIM
6	*OSAF-TK*	Linux	Tersedia	Semua Ponsel

Dari daftar aplikasi forensik tersebut, dipilihlah *WhatsApp Key/DB Extractor*, *BitPim*, dan *Autopsy* untuk melakukan analisis forensik berdasarkan ketersedian dan basis sistem operasi aplikasi serta kesesuaian aplikasi dengan fokus penelitian.

Dalam melakukan analisis forensik terhadap perangkat seluler, dibutuhkan panduan untuk melakukan penanganan untuk meminimalisir kesalahan selama poses analisis. Ajijola, Zavarsky, dan Ruhl (2014), dalam penelitiannya telah membandingkan dua pedoman forensik tentang penanganan bukti digital, yakni *NIST SP 800-101 Rev. 1* dan *ISO/IEC 27037*. Perbandingan dua pedoman forensik tersebut tersaji pada Tabel 3.

Tabel 3: Perbandingan Pedoman Forensik (Sumber: Hasil penelitian Ajijola, Zavarsky, dan Ruhl)

No.	NIST SP 800-101 Rev. 1	ISO/IEC 27037
1	Hanya perangkat seluler.	Semua perangkat digital.
2	Penyidikan secara teknis dan nonteknis.	Hanya penyidikan secara nonteknis.
3	Penanganan forensik dijelaskan secara rinci.	Hanya menjelaskan awal penanganan forensik.
4	Analisis untuk perangkat seluler dan bukti digital.	Hanya analisis terhadap perangkat digital.

Dari perbandingan dua pedoman forensik tersebut, maka pedoman yang akan digunakan dalam penelitian ini yakni *NIST Special Publication 800-101 Revision 1*, karena pedoman ini lebih dikhususkan untuk penanganan perangkat seluler dalam mendapatkan bukti digital.

2. Metode Penelitian

Metode penelitian yang digunakan untuk melakukan analisis forensik pada penelitian ini, yakni pedoman dari *NIST Special Publication 800-101 Revision 1*, tahapan penanganan perangkat seluler pada pedoman ini terdapat pada Gambar 3.

Gambar 3 Tahapan NIST Special Publication 800-101 Revision 1 (Sumber: NIST)

2.1. *Preservation*

Tahap ini merupakan tahapan terhadap data yang diambil dari media akan dilakukan identifikasi serta pelabelan dengan tetap mengikuti prosedur dalam menjaga integritas data.

2.2. *Acquisition*

Tahap ini merupakan tahapan terhadap data yang dikumpulkan akan diproses dengan metode forensik secara otomatis maupun manual, serta menilai dan mengeluarkan datanya sesuai kebutuhan dengan tetap mempertahankan integritas data. Karena ponsel yang akan digunakan dalam penelitian ini tidak dalam keadaan rusak, maka metode akuisisi data dari perangkat yang digunakan pada penelitian ini yakni metode akuisisi logis (*logical acquisition*). Metode akuisisi logis sendiri merupakan metode mendapatkan data dari perangkat digital yang datanya dapat digunakan berulang tanpa merusak data yang digunakan.

2.3. *Examination & Analysis*

Tahap ini merupakan tahapan pemerikasaan serta analisis terhadap kinerja aplikasi serta data hasil akuisisi dilakukan sesuai dengan aturan yang dibenarkan. Pemeriksaan dan analisis terhadap kinerja pada penelitian ini berdasarkan buku panduan dari National Institute of Standards and Technology (NIST), yakni *Mobile Device Tool Specification* (2016) *dan Mobile Device Tool Test Assertions and Test Plan* (2016). Parameter tersebut terbagi atas. *Core Assertions, Optional Assertions, Core Features Requirements,* dan *Optional Features Requirements*. Karena *Optional Assertions* serta *Optional Features Requirements* dikhususkan untuk penanganan akuisisi fisik (*physical acquisition*) sehingga parameter tersebut dihilangkan dalam penelitian ini. Sedangkan untuk *Core Assertions* hanya mengambil 9 dari 10 parameter yang ada. Parameter yang dihilangkan dari *Core Assertions* yakni MDT-CA 10, karena parameter ini melibatkan aplikasi pihak ketiga dalam melakukan perubahan data saat proses akuisisi berlangsung. Parameter yang digunakan untuk melakukan pemeriksaan dan analisis terhadap kinerja aplikasi forensik tersaji pada Tabel 4.

Tabel 4: Parameter Kinerja Aplikasi (Sumber: NIST)

Parameter	Kode
Core Assertions	MDT-CA-01
	MDT-CA-02
	MDT-CA-03
	MDT-CA-04
	MDT-CA-05
	MDT-CA-06
	MDT-CA-07
	MDT-CA-08
	MDT-CA-09
Core Features requirements	MDT-CR-01
	MDT-CR-02
	MDT-CR-03

Dalam hal mendapatkan bukti digital, parameter yang digunakan yakni parameter *Artifacts*. Parameter *Artifacts* sendiri isi penggunaannya atau data yang kemudian dapat dijadikan sebagai barang bukti tergantung dengan kebutuhan dalam penelitian. Karena penelitian ini menggunakan aplikasi *WhatsApp*, maka data yang akan didapatkan (artefak) merupakan data pada aplikasi *WhatsApp*, yakni daftar kontak, riwayat panggilan, serta pesan baik yang berupa teks, gambar, video, audio, dokumen, dan lokasi (*GPS*). Parameter yang digunakan untuk melakukan pemeriksaan dan analisis dalam mendapatkan bukti digital tersaji pada Tabel 5.

Tabel 5: Parameter Bukti Digital (Sumber: Hasil penelitian Penulis)

Parameter	Nama	Kode
Artifacts	Pesan Teks	WA-AO-01
	Riwayat Panggilan	WA-AO-02
	Daftar Kontak	WA-AO-03
	Pesan Gambar	WA-AO-04
	Pesan Video	WA-AO-05
	Pesan Audio	WA-AO-06
	Pesan Dokumen	WA-AO-07
	Pesan GPS	WA-AO-08

2.4. *Reporting*

Pada tahap ini, hasil pemeriksaan dan analisis dibuat sebagai laporan. Laporan yang akan disajikan dari hasil pemeriksaan dan analisis terdapat tiga, yakni

a. Kinerja setiap aplikasi forensik;

b. Data ditemukan, baik jenis data maupun jumlah data; serta

c. Data yang dapat dibuka.

Laporan hasil pemeriksaan dan analisis tersebut dilakukan perhitungan menggunakan indeks kuantitas untuk mengetahui presentase dari setiap aplikasi. Dengan rumus sebagai berikut.

$$I_A = \frac{\sum Q_n}{\sum Q_0} \times 100\%$$

Keterangan.

I_A : Indeks agregatif tidak tertimbang

$\sum Q_n$: Jumlah data hasil akuisisi

$\sum Q_0$: Jumlah data asli

3. Hasil dan Pembahasan

Hasil dan pembahasan pada penelitian ini menggunakan pengukuran *NIST Special Publication 800-101 Revision 1* untuk mengetahui kinerja aplikasi forensik dalam mendapatkan bukti digital. Aplikasi forensik yang digunakan untuk melakukan analisis pada Samsung Young 2 Duos, yakni *WhatsApp Key/DB Extractor*, *BitPim, dan Autopsy*. Terdapat dua tahapan pada bab ini, yakni persiapan sebelum analisis forensik dan saat melakukan analisis forensik.

3.1. Persiapan Sebelum Analisis Forensik

Persiapan sebelum analisis forensik dilakukan untuk mempersiapkan bahan untuk pengujian serta skenario pengujian yang akan dilakukan. Hal itu dilakukan agar mengetahui data atau informasi awal sebelum dilakukan pengujian. Bahan yang digunakan dalam penelitian ini tersaji pada Tabel 6.

Tabel 6: Daftar Bahan Pengujian (Sumber: Hasil penelitian Penulis)

No.	Nama
1	*Asus A455LF*
2	*Samsung Young 2 Duos "SM-G130H"*
3	*Autopsy v4.17.01*
4	*BitPim v1.0.7*
5	*WhatsApp Key/DB Extractor v4.7*
6	*WhatsApp v2.21.2.16*
7	*KingoRoot v4.5.0.*
8	*Busybox Free v1.26.2*
9	*WPS Office (BETA) v11.7.1*
10	*SDK Platform Tools v30.0.5*
11	*Ncat Platform v5.59BETA1*
12	*WhatsApp Viewer v1.13*
13	*Notepad++ v6.8.2*
14	*Oracle VM VirtualBox v6.1.18*
15	*Veger USB*

Kemudian dilakukanlah pembuatan skenario, yakni membuat kontak; melakukan *miss-call* dan panggilan telepon *WhatsApp*; serta mengirim pesan *WhatsApp*, baik yang berupa teks, gambar, video, audio, dokumen, dan *GPS* (*Global Positioning Systems*). Kemudian semua data tersebut dihapus dan dilakukanlah pencarian serta pemulihan artefak WhatApp menggunakan *WhatsApp Key/DB Extractor*, *BitPim*, dan *Autopsy* yang bertujuan untuk mengetahui kinerja aplikasi tersebut dalam mendapatkan bukti digital. Jumlah data hasil skenario tersaji pada Tabel 7.

Tabel 7: Jumlah Data Awal (Sumber: Hasil penelitian Penulis)

No.	Nama	Kode	Jumlah
1	Pesan Teks	WA-AO-01	40
2	Riwayat Panggilan	WA-AO-02	5
3	Daftar Kontak	WA-AO-03	10
4	Pesan Gambar	WA-AO-04	3
5	Pesan Video	WA-AO-05	2
7	Pesan Audio	WA-AO-06	2
8	Pesan Dokumen	WA-AO-07	3
9	Pesan GPS	WA-AO-08	2

3.2. Analisis Forensik

Analisis forensik pada Samsung Young 2 Duos menggunakan pengukuran dari *NIST Special Publication 800-101 Revision 1*. Terdapat empat (4) tahapan, yakni *Preservation* (Penjagaan), *Acquisition* (Akuisisi*), Examination & Analysis* (Pemeriksaan & Analisis) dan *Reporting* (Pelaporan).

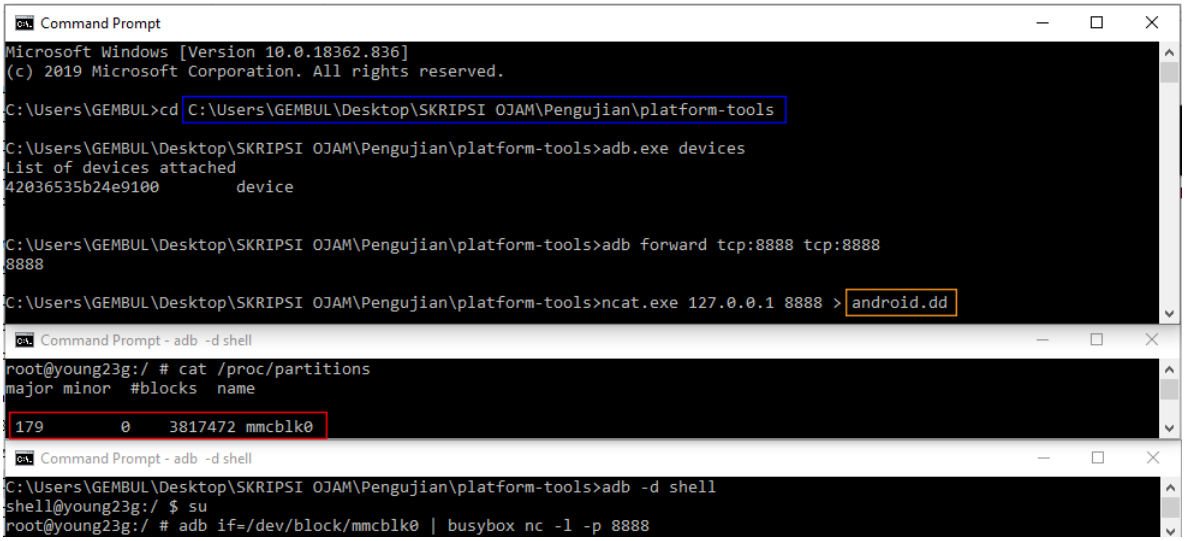
A. *Preservation*

Pada tahap ini, Samsung Young 2 Duos diamankan dan dilakukan isolasi, dengan mengaktifkan mode pesawat atau tindakan lain yang mungkin dapat mempengaruhi perubahan data pada Samsung Young 2 Duos saat diamankan dan sesudah diamankan. Kondisi ponsel saat diamankan dan dilakukan isolasi terdapat pada Gambar 4.

Gambar 4 Samsung Young 2 Duos Diamankan dan Diisolasi (Sumber: Hasil penelitian Penulis)

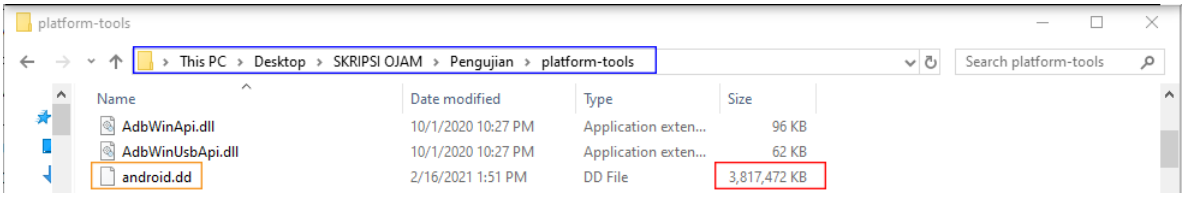
B. *Acquisition*

Pada tahap ini, data pada Samsung Young 2 Duos diambil secara forensik dengan pembuatan image disk menggunakan SDK Platform Tools dengan fitur Android Debug Bridge (ADB) disertai dengan Ncat Platform yang semua proses akuisinya menggunakan fitur baris perintah dari Windows Command Prompt. Hal yang harus diketahui pertama kali yakni ukuran data pada Samsung Young 2 Duos. Pada saat Samsung Young 2 Duos diamankan, tidak ditemukan memori eksternal, sehingga fokus pengujian langsung pada ukuran data memori internal Samsung Young 2 Duos, seperti yang terdapat pada Gambar 5.



Gambar 5 Proses Akuisisi (Sumber: Hasil penelitian Penulis)

Dari Gambar 5, dapat diketahui bahwa lokasi data hasil akuisisi terletak pada direktori *Desktop\SKRIPSI OJAM\Pengujian\platform-tools*; hasil akuisisi diberi nama *android.dd*; serta ukuran data hasil akusisi sebesar 3.817.472 KB. Oleh karena itu, data hasil akuisisi harus sama dengan informasi data yang ada pada saat proses akuisisi berlangsung. Setelah proses akuisisi selesai, kemudian direktori data akuisisi disimpan dibuka. Saat dilihat terdapat data hasil akusisi dengan nama dan ukuran data yang sama, yakni *android.dd* dengan ukuran data 3.817.472 KB, seperti yang terdapat pada Gambar 6.



Gambar 6 Direktori Data Hasil Akuisisi (Sumber: Hasil penelitian Penulis)

C. *Examination & Analysis*

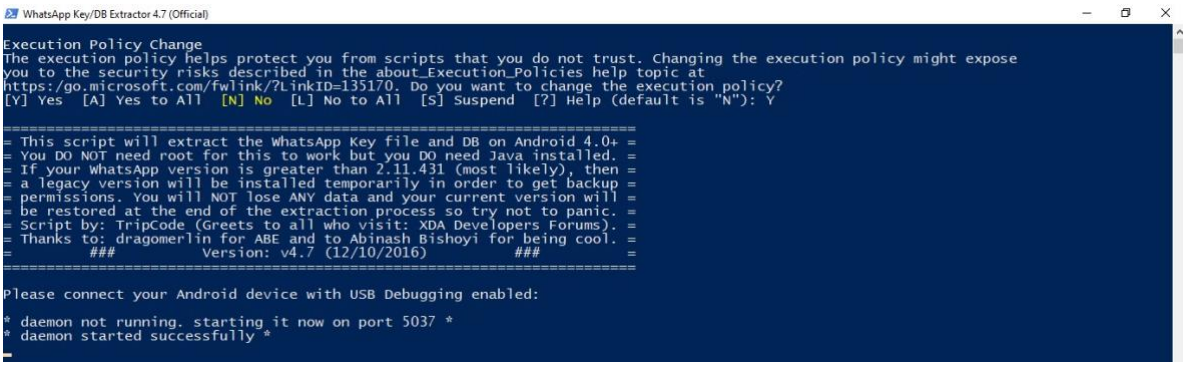
Pada tahap ini, data hasil akuisisi akan dilakukan pemeriksaan dan analisis menggunakan tiga aplikasi forensik, yakni *WhatsApp Key/DB Extractor*, *BitPim*, dan *Autopsy*. Pemeriksaan dan analisis dilakukan untuk mengetahui

a. Kinerja setiap aplikasi forensik;

b. Data yang ditemukan, baik jenis data maupun jumlah data; dan

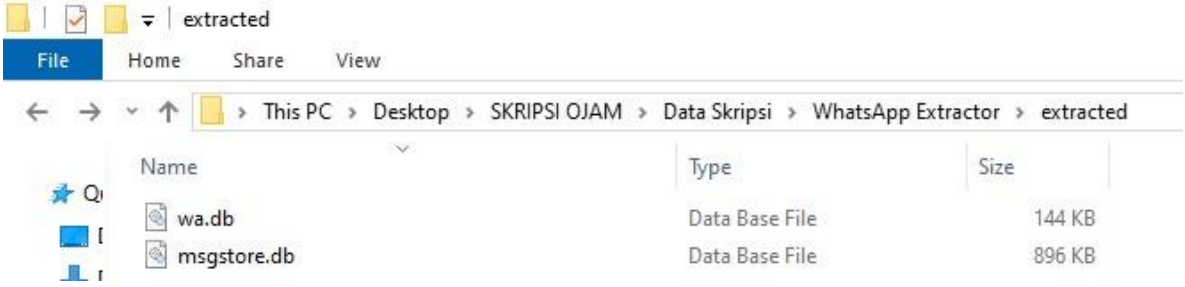
c. Data yang dapat dibuka.

WhatsApp Key/DB Extractor aplikasi pertama yang digunakan untuk melakukan pemeriksaan dan analisis pada Samsung Young 2 Duos. Berikut tampilan awal *WhatsApp Key/DB Extractor* seperti yang terdapat pada Gambar 7.



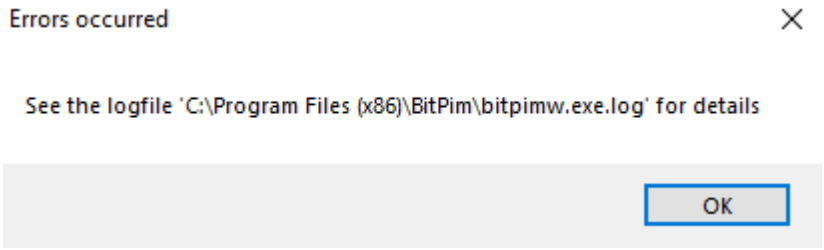
Gambar 7 Tampilan Awal *WhatsApp Key/DB Extractor* (Sumber: Hasil penelitian Penulis)

WhatsApp Key/DB Extractor hanya dapat melakukan akuisisi data dan tidak dapat melakukan pemeriksaan dan analisis terhadap data hasil akusisi, sehingga untuk dapat melihat isi data harus menggunakan aplikasi yang dapat melakukan pemeriksaan dan analisis terhadap data hasil akuisisi tersebut, aplikasi yang digunakan yakni *WhatsApp Viewer dan Notepad++*. Hasil akuisisi *WhatsApp Key/DB Extractor* merupakan file dengan ekstensi *.db* (*database*) yang terletak pada direktori *C:\Users\GEMBUL\Desktop\SKRIPSI OJAM\Data Skripsi\WhatsApp Extractor\extracted* seperti yang terdapat pada Gambar 8.



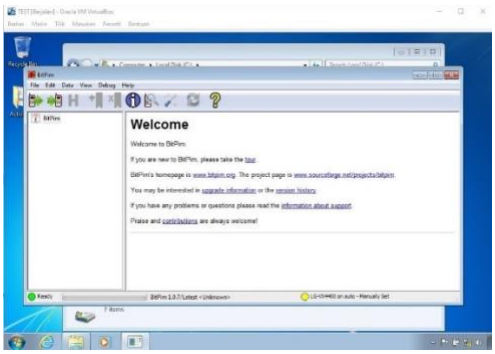
Gambar 8 Data Hasil Akusisi *WhatsApp Key/DB Extractor* (Sumber: Hasil penelitian Penulis)

Setelah selesai melakukan pemeriksaan dan analisis menggunakan *WhatsApp Key/DB Extractor*, dilanjutkan menggunakan aplikasi *BitPim*. Namun, saat aplikasi *BitPim* dijalankan, muncul notifikasi eror seperti yang ada pada Gambar 9.



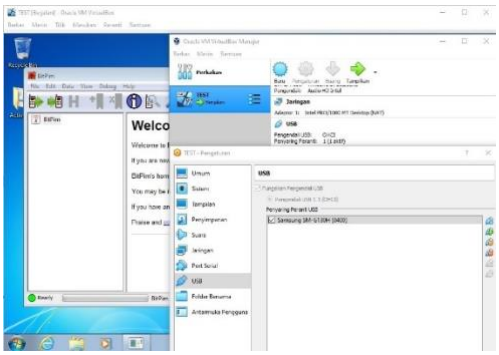
Gambar 9 Notofikasi Eror BitPim (Sumber: Hasil penelitian Penulis)

Saat melihat isi dari *logfile* yang terdapat pada direktori *C:\Program Files (x86)\BitPim\bitpimw.exe.log*, ternyata terdapat kesalahan saat memuat *specified module* yang menyebabkan BitPim gagal dijalankan. Demikian juga saat dilakukan pencarian informasi terkait pemecahan masalah ini, diketahui bahwa dukungan pengembang hanya sampai versi 1.0.7 yang dirilis pada Januari 2010, dan BitPim hanya dapat berjalan di Windows 7. Untuk menyesuaikan dengan persyaratan sistem yang dibutuhkan, maka dipasanglah Windows 7 Ultimate SP1 menggunakan Oracle VM VirtualBox. Setelah pemasangan Windows 7 Ultimate SP1 selesai, kemudian aplikasi BitPim dipasang. Dan BitPim dapat berjalan di Windows 7 Ultimate SP1 (Gambar 10). Kemudian saat aplikasi BitPim dijalankan, ternyata BitPim tidak dapat mendeteksi Samsung Young 2 Duos (Gambar 11). Meski Samsung Young 2 Duos sudah terhubung dengan Windows 7 Ultimate SP1 yang ada pada Oracle VM VirtualBox (Gambar 12). Demikian juga saat dilihat dukungan untuk model Samsung yang digunakan, yakni "SM-G130H". Model tersebut tidak tersedia pada aplikasi BitPim (Gambar 13).



Gambar 10 BitPim Berjalan di Windows 7 (Sumber: Hasil penelitian Penulis)

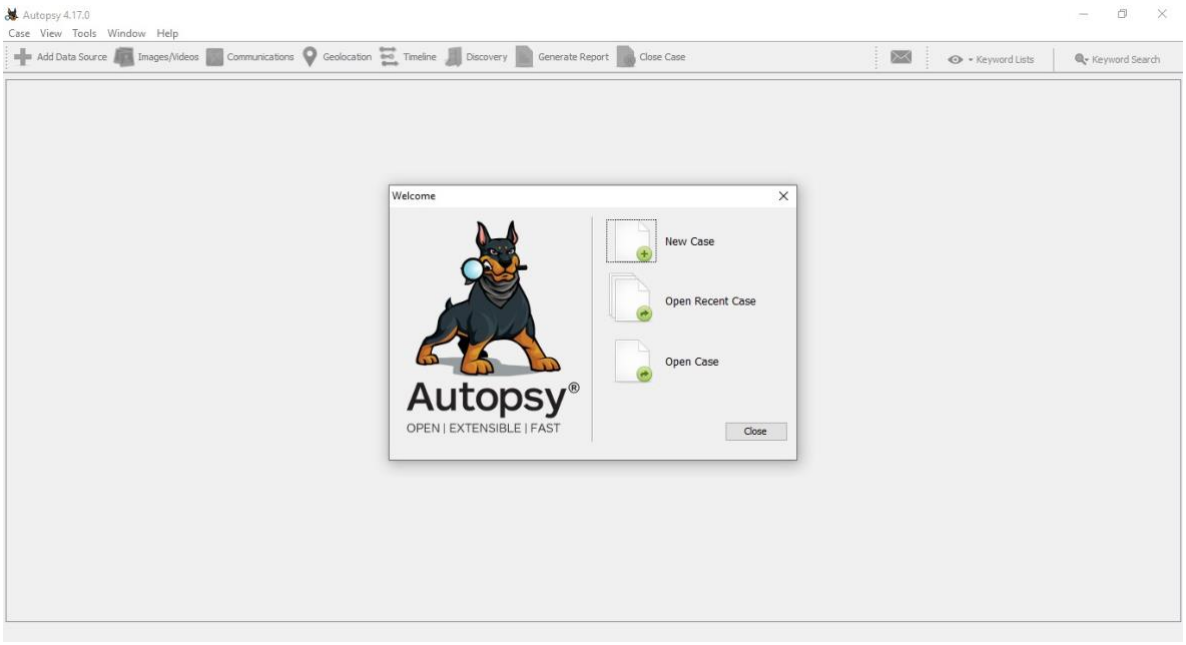
Gambar 11 BitPim Gagal Mendeteksi Ponsel (Sumber: Hasil penelitian Penulis)



Gambar 12 Ponsel Terkoneksi Windows 7
(Sumber: Hasil penelitian Penulis)

Gambar 13 Dukungan BitPim terhadap Model Ponsel
(Sumber: Hasil penelitian Penulis)

Karena tidak dapat mendeteksi ponsel, sehingga BitPim tidak dapat mendapatkan data dari ponsel. Dengan begitu BitPim tidak dapat digunakan untuk melakukan pemeriksaan dan analisis terhadap Samsung Young 2 Duos, baik terhadap kinerja aplikasi forensik; data yang ditemukan, baik jenis data maupun jumlah data; dan data yang dapat dibuka. Kemudian dilanjutkan melakukan pemeriksaan dan analisis menggunakan aplikasi Autopsy. Berikut tampilan awal dari Autopsy sebelum melakukan pemeriksaan dan analisis pada Samsung Young 2 Duos yang terdapat pada Gambar 14.



Gambar 14 Tampilan Awal Autopsy (Sumber: Hasil penelitian Penulis)

Autopsy melakukan pemeriksaan dan analisis menggunakan data hasil dari akuisisi dari SDK Platform Tools dan Ncat Platform yang terletak pada direktori *C:\Users\GEMBUL\Desktop\Desktop\SKRIPSI OJAM\Pengujian\platform-tools*, yakni *android.dd*. Dengan begitu aplikasi yang digunakan untuk melakukan pemeriksaan dan analisis pada Samsung Young 2 Duos hanya *WhatsApp Key/DB Extractor* dan *Autopsy*. Hasil dari pemeriksaan dan analisis untuk mengetahui kinerja setiap aplikasi forensik; data yang ditemukan, baik jenis data maupun jumlah data; dan data yang dapat dibuka tersaji pada Tabel 8.

Tabel 8: Hasil Pemeriksaan dan Analisis

KINERJA SETIAP APLIKASI FORENSIK			
Parameter		***WhatsApp Key/DB Extractor***	***Autopsy***
Core Assertions	MDT-CA-01	×	×
	MDT-CA-02	×	×
	MDT-CA-03	×	×
	MDT-CA-04	√	×
	MDT-CA-05	×	√
	MDT-CA-06	×	√
	MDT-CA-07	√	√
	MDT-CA-08	×	√
	MDT-CA-09	×	√
Optional Requirement Assertions	MDT-AO-01	√	×
	MDT-AO-02	√	×
	MDT-AO-03	√	√
Total	**12**	**5**	**6**
DATA YANG DITEMUKAN "JENIS DATA"			
Parameter		***WhatsApp Key/DB Extractor***	***Autopsy***
Artifacts	WA-AO-01	√	√
	WA-AO-02	×	√
	WA-AO-03	√	√
	WA-AO-04	×	√
	WA-AO-05	×	√
	WA-AO-06	×	√
	WA-AO-07	×	√
	WA-AO-08	×	×
Total	**8**	**2**	**7**
DATA YANG DITEMUKAN "JUMLAH DATA"			
Artefak	**Jumlah Data Awal**	**WhatsApp Key/DB Extractor**	**Autopsy**
WA-AO-01	40	40	40
WA-AO-02	5	0	5
WA-AO-03	10	10	10
WA-AO-04	3	0	2
WA-AO-05	2	0	2
WA-AO-06	2	0	2

(lanjutan)

DATA YANG DITEMUKAN "JUMLAH DATA"			
Artefak	**Jumlah Data Awal**	***WhatsApp Key/DB Extractor***	***Autopsy***
WA-AO-07	3	0	3
WA-AO-08	2	0	0
Total	**67**	**50**	**64**
DATA DITEMUKAN YANG DAPAT DIBUKA			
Artefak	**Jumlah Data Awal**	***WhatsApp Key/DB Extractor***	***Autopsy***
WA-AO-01	40	1	1
WA-AO-02	5	0	5
WA-AO-03	10	10	10
WA-AO-04	3	0	0
WA-AO-05	2	0	0
WA-AO-06	2	0	0
WA-AO-07	3	0	3
WA-AO-08	2	0	0
Total	**67**	**11**	**19**
TOTAL	**154**	**68**	**90**

D. *Reporting*

Setelah keseluruhan hasil pemeriksaan dan analisis *–kinerja setiap aplikasi forensik; data yang ditemukan baik jenis data maupun jumlah data; serta data yang dapat dibuka–* diketahui, dilakukan perhitungan menggunakan indeks agregatif tidak tertimbang. Berikut merupakan hasil dari perhitungannya.

a. WhatsApp Key/DB Extractor

$$I_A = \frac{\sum Q_n}{\sum Q_0} \times 100\% = \frac{68}{154} \times 100\% = 44.15\%$$

b. Autopsy

$$I_A = \frac{\sum Q_n}{\sum Q_0} \times 100\% = \frac{90}{154} \times 100\% = 58.44\%$$

Dari hasil perhitungan diketahui, bahwa *WhatsApp Key/DB Extractor* mendapatkan indeks 44.15%; Autopsy mendapatkan indeks kuantitas sebesar 58.44%. Hal itu menandakan Autopsy lebih unggul secara keseluruhan dari *WhatsApp Key/DB Extractor*.

4. Kesimpulan

Kesimpulan dari hasil penelitian yang telah dilakukan terkait analisis kinerja aplikasi forensik *open-source –WhatsApp Key/DB Extractor, BitPim, dan Autopsy–* pada Samsung Young 2 Duos dalam mendapatkan bukti digital aplikasi WhatsApp berdasarkan pengukuran dari *NIST Special Publication 800-101 Revision 1*, bahwa aplikasi forensik yang digunakan tidak selalu ada pada setiap tahapan *NIST Special Publication 800-101 Revision 1*, dan aplikasi forensik juga tidak selalu dapat memenuhi setiap parameter yang telah ditetapkan.

Hasil analisis aplikasi forensik secara keseluruhan, Autopsy mendapatkan indeks kuantitas sebesar 58.44%. Hal itu menandakan Autopsy lebih unggul dari *WhatsApp Key/DB Extractor* yang mendapatkan indeks 44.15%. Sedangkan untuk *BitPim* tidak digunakan dalam penelitian ini karena *BitPim* tidak dapat mendeteksi ponsel yang digunakan, sehingga data yang ingin didapatkan, kemudian diperiksa dan dianalisis menggunakan aplikasi BitPim tidak dapat dilakukan.

Daftar Referensi

Ajijola, A., Zavarsky, P., dan Ruhl R. (2014). A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev. 1:2014 and ISO/IEC 27037:2012. *World Congress on Internet Security (WorldCIS-2014)*.

Ayers, R., Brothers, S., dan Jansen, W. (2014). *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101 Revision 1. National Institute of Standards and Technology (NIST).

Lohiya, R., John, P., dan Shah, P. (2015). Survey on Mobile Forensics. *International Journal of Computer Applications (0975-8887)*. 118(16): 6-11.

Patankar, M., dan Bhandari, D. (2014). Forensic Tools used in Digital Crime Investigation. *Indian Journal of Applied Research*. 4(5): 278-283.

Ritcher, F. (2019). Facebook Inc. Dominates the Social Media Landscape. *http://statista.com/chart/5194/active-users-of-social-networks-and-messaging-services*. (diakses pada 10 Juni 2021).

Ritcher, F. (2019). The Smartphone Duopoly. *http://statista.com/chart/3268/smartphone-os-market-share*. (diakses pada 10 Juni 2021).

U.S. Department of Commerce. (2016). *Mobile Device Tool Specification*. Version 2.0. National Institute of Standards and Technology (NIST).

U.S. Department of Commerce. (2016). *Mobile Device Tool Test Assertions and Test Plan*. Version 2.0. National Institute of Standards and Technology (NIST).

Yadi, I. Z., dan Kunang, Y. N. (2014). Analisis Forensik pada Platform Android. *Konferensi Nasional Ilmu Komputer 2014*. 141-148.

Zuraida, M. (2015). Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia. *Jurnal Analisis Hubungan Internasional*. 4(1): 1627–1642.