ANALISIS KINERJA APLIKASI FORENSIK *OPEN-SOURCE* PADA PONSEL CERDAS BERBASIS ANDROID DALAM MENDAPATKAN BUKTI DIGITAL

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh:

M. MACHRUSH ALIY SIROJJAM MUSHLICH

H76215019

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN AMPEL

SURABAYA

2021

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini,

Nama	:	M. MACHRUSH ALIY SIROJJAM MUSHLICH
NIM	:	H76215019
Program Studi	:	Sistem Informasi
Angkatan	:	2015

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul "ANALISIS KINERJA APLIKASI FORENSIK *OPEN-SOURCE* PADA PONSEL CERDAS BERBASIS ANDROID DALAM MENDAPATKAN BUKTI DIGITAL". Apabila suatu saat nanti, saya terbukti melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 4 Mei 2021

Yang menyatakan,

M. Machrush Aliy S. M.

NIM H76215019

PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA	:	M. MACHRUSH ALIY SIROJJAM MUSHLICH
NIM	:	H76215019
JUDUL	:	ANALISIS KINERJA APLIKASI FORENSIK *OPEN-SOURCE* PADA PONSEL CERDAS BERBASIS ANDROID DALAM MENDAPATKAN BUKTI DIGITAL

telah diperiksa dan disetujui untuk diujikan.

Surabaya, 4 Mei 2021

Dosen Pembimbing 1	Dosen Pembimbing 2
Muhammad Andik Izzuddin, M.T.	Mujib Ridwan, M.T.
NIP 19840307 201403 1 001	NIP 19860427 201403 1 004

PENGESAHAN TIM PENGUJI

Skripsi M. Machrush Aliy Sirojjam Mushlich ini telah dipertahankan
di depan tim penguji skripsi
di Surabaya, 22 Juni 2021

Mengesahkan,
Dewan Penguji

Dosen Pembimbing 1	Dosen Pembimbing 2
Muhammad Andik Izzuddin, M.T.	Mujib Ridwan, M.T.
NIP 19840307 201403 1 001	NIP 19860427 201403 1 004

Dosen Penguji 1	Dosen Penguji 2
Indri Sudanawati Rozas, M.Kom.	Ahmad Yusuf, M. Kom.
NIP 19820721 201403 2 001	NIP 19900120 201403 1 003

Mengetahui,
Dekan Fakultas Sains dan Teknologi
Universitas Islam Negeri Sunan Ampel Surabaya

Dr. Evi Fatimatur Rusydiyah, M.Ag.
NIP 19731227 200501 2 003

KEMENTRIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117, Surabaya 60237. Telp. (031) 8431972. Fax. (031) 8413300
e-mail. perpus@uinsby.ac.id

PERNYATAAN PUBLIKASI KARYA ILMIAH
UNTUK KEPENTINGAN AKADEMIS

Saya yang bertanda tangan di bawah ini, civitas academica Universitas Islam Negeri Sunan Ampel Surabaya.

Nama	: M. MACHRUSH ALIY SIROJJAM MUSHLICH
NIM	: H76215019
Fakultas/Jurusan	: SAINS DAN TEKNOLOGI/SISTEM INFORMASI
Alamat surel	: jampirojam@gmail.com

Menyetujui untuk memberikan ke Perpustakaan Universitas Islam Negeri Sunan Ampel dengan Hak Bebas Royalti Non-Ekskulif (*Non-Exclusive Royalty Free Rights*) atas karya ilmiah "skripsi" saya yang berjudul "ANALISIS KINERJA APLIKASI FORENSIK *OPEN-SOURCE* PADA PONSEL CERDAS BERBASIS ANDROID DALAM MENDAPATKAN BUKTI DIGITAL," demi perkembangan ilmu pengetahuan beserta dengan perangkat yang diperlukan (*bila ada*). Dengan Hak Bebas Royalti Non-Ekskulif, Perpustakaan Universitas Islam Negeri Sunan Ampel Surabaya berhak untuk menyimpan, mengalih media, mendistribusi, mengelola dalam bentuk basis data (*database*), menampilkan serta mempublikasikan ke internet atau media lain dalam bentuk tulisan penuh *(fulltext)* untuk kepentingan akademis tanpa perlu meminta izin kepada saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan/atau penerbit.

Saya bersedia untuk menanggung secara pribadi tanpa melibatkan pihak Perpustakaan Universitas Islam Negeri Sunan Ampel Surabaya terhadap segala bentuk tuntutan hukum yang timbul akibat atas pelanggaran hak cipta dalam karya ilmiah "skripsi" saya ini.

Demikian penyataan ini saya buat dengan sebenarnya.

Surabaya, 22 Juli 2021

Yang menyatakan,

M. Machrush Aliy S. M.

NIM H76215019

ABSTRAK

ANALISIS KINERJA APLIKASI FORENSIK *OPEN-SOURCE* PADA PONSEL CERDAS BERBASIS ANDROID DALAM MENDAPATKAN BUKTI DIGITAL

Oleh:

M. Machrush Aliy Sirojjam Mushlich

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, Forensik Perangkat Seluler, Aplikasi *Open-Source,* National Institute of Standards and Technology (NIST)

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

ABSTRACT

OPEN-SOURCE FORENSIC APPLICATIONS PERFORMANCE ANALYSIS ON SMARTPHONE ANDROID-BASED IN COLLECTING DIGITAL EVIDENCE

***By*:**

M. Machrush Aliy Sirojjam Mushlich

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, Mobile Forensic, Open-Source Applications, National Institute of Standards and Technology (NIST)

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR ISI

PERSETUJUAN PEMBIMBING i

PENGESAHAN TIM PENGUJI ii

PERNYATAAN KEASLIAN iii

PERNYATAAN PUBLIKASI KARYA ILMIAH iv

ABSTRAK v

ABSTRACT vi

DAFTAR ISI vii

DAFTAR GAMBAR x

DAFTAR TABEL xi

BAB I PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Rumusan Masalah 5

1.3. Batasan Masalah 5

1.4. Tujuan Penelitian 6

1.5. Manfaat Penelitian 6

1.6. Sistematika Penulisan 6

BAB II LANDASAN TEORI 8

2.1. Penelitian Terdahulu 8

2.2. Forensik Digital (*Digital Forensic*) 10

2.2.1. Forensik Perangkat Seluler (*Mobile Forensic*) 10

2.3. Bukti Digital (*Digital Evidence*) 11

2.4. Alat Forensik (*Forensic Tool*) 12

2.4.1. Alat Forensik Perangkat Seluler *Open-Source* 12

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2.4.2. Alat Forensik Perangkat Seluler Proprietary 12
2.5. Kejahatan Siber (*Cybercrime*) 13
2.5.1. *Violent/Potentially Violent* 13
2.5.2. *Non-Violent* 14
2.6. National Institute of Standards and Technology (NIST) 15
2.7. Ponsel Cerdas (*Smartphone*) 17
2.8. Media Sosial (*Social Media*) 17
2.9. Integrasi Keilmuan 18
BAB III METODOLOGI PENELITIAN 19
3.1. Identifikasi Masalah 19
3.2. Persiapan Sebelum Pengujian 20
3.2.1. Studi Literatur 20
3.2.2. Pembuatan Skenario 20
3.3. Analisis Forensik 21
3.3.1. *Preservation* 21
3.3.2. *Acquisition* 21
3.3.3. *Examination & Analysis* 22
3.3.4. *Reporting* 25
BAB IV HASIL DAN PEMBAHASAN 26
4.1. Persiapan Sebelum Pengujian 26
4.1.1. Persiapan Bahan 26
4.1.2. Pembuatan Skenario 28
4.2. Analisis Forensik pada Samsung Young 2 Duos 29
4.2.1. *Preservation* 30
4.2.2. *Acquisition* 31

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

4.2.3. *Examination & Analysis* 32
4.2.4. *Reporting* 55
BAB V PENUTUP 61
5.1. Simpulan 61
5.2. Saran 61
DAFTAR PUSTAKA 62
LAMPIRAN 01 DATA SKENARIO PENGUJIAN 66
LAMPIRAN 02 PENGUJIAN WHATSAPP KEY/DB EXTRACTOR 70
LAMPIRAN 03 PENGUJIAN AUTOPSY 81
LAMPIRAN 04 LEMBAR PEMBIMBING SATU 95
LAMPIRAN 05 LEMBAR PEMBIMBING DUA 96
LAMPIRAN 06 WAWANCARA NARASUMBER 97

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR GAMBAR

Gambar 1.1. Diagram Penjualan *Smartphone* 3

Gambar 1.2. Grafik Pengguna Sosial Media 4

Gambar 2.1. Tahapan NIST Special Publication 800-101 Revision 1 15

Gambar 2.2. Alur Kerja Penanganan Forensik Perangkat Seluler.....16

Gambar 3.1. Alur Penelitian 19

Gambar 3.2. Analisis Forensik NIST Special Publication 800-101 Revision 1.....21

Gambar 4.1. Samsung Young 2 Duos Diamankan dan Diisolasi 30

Gambar 4.2. Detail Informasi Memori Samsung Young 2 Duos 31

Gambar 4.3. Direktori dan Data Hasil Akuisisi.....32

Gambar 4.4. Tampilan Awal WhatsApp Key/DB Extractor 33

Gambar 4.5. Hasil Akuisisi WhatsApp Key/DB Extractor 34

Gambar 4.6. Tampilan Eror Aplikasi BitPim 34

Gambar 4.7. Tampilan Awal BitPim 35

Gambar 4.8. BitPim Gagal Mendeteksi Ponsel 36

Gambar 4.9. Koneksi antara VirtualBox dengan Ponsel 36

Gambar 4.10. Dukungan BitPim untuk Model Ponsel 37

Gambar 4.11. Tampilan Awal Autopsy 37

Gambar 4.12. Direktori Penyimpanan Informasi Kasus.....38

Gambar 4.13. Memilih Data Hasil Akusisi untuk Diekstraksi 38

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR TABEL

Tabel 1.1. Daftar Aplikasi Forensik *Open-Source* 2

Tabel 1.2. Perbandingan Pedoman Forensik 4

Tabel 2.1. Penelitian Terdahulu.....8

Tabel 2.2. Daftar Alat Forensik Perangkat Seluler *Open-Source*.....12

Tabel 2.3. Daftar Alat Forensik Perangkat Seluler 13

Tabel 3.1. Parameter National Institute of Standards and Technology (NIST) 23

Tabel 4.1. Daftar Bahan Persiapan 26

Tabel 4.2. Informasi Perangkat.....28

Tabel 4.3. Jumlah Data Awal 29

Tabel 4.4. Berkas Informasi Pengujian 30

Tabel 4.5. Hasil Kinerja WhatsApp Key/DB Extractor 40

Tabel 4.6. Hasil Kinerja Autopsy 44

Tabel 4.7. Data Ditemukan oleh WhatsApp Key/DB Extractor.....48

Tabel 4.8. Data Ditemukan oleh Autopsy 50

Tabel 4.9. Data Dapat Dibuka oleh WhatsApp Key/DB Extractor 53

Tabel 4.10. Data Dapat Dibuka oleh Autopsy.....54

Tabel 4.11. Perbandingan Kinerja Aplikasi Forensik.....56

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi dewasa ini berkembang dengan pesat. Banyak pengguna memanfaatan teknologi informasi yang terdapat pada ponsel cerdas untuk melakukan tindakan kejahatan siber (*cybercrime*) yang menyebabkan banyak kerugian jaringan *borderless.* Jaringan *borderless* merupakan suatu jaringan yang disediakan untuk memudahkan pengguna internet agar dapat mengakses data serta informasi secara luas, akan tetapi jaringan *borderless* juga dapat menimbulkan banyak permasalahan, salah satunya yakni tindak kejahatan siber yang sifatnya lintas batas wilayah negara. Beberapa negara mengkategorikan kejahatan siber sebagai kejahatan transnasional; setiap negara perlu adanya suatu kerjasama internasional dalam penangannya. Tidak sedikit negara yang mengalami kesulitan dalam melaksanakan usaha pencegahan atau penanganan tindak kejahatan siber, karena tidak seragamnya regulasi di negara tersebut (Zuraida, 2015). Maraknya tindakan kejahatan siber yang menggunakan ponsel cerdas, memunculkan bidang baru pada penanganan kejahatan yang dikenal dengan istilah *mobile forensic. Mobile forensic* merupakan bagian dari ilmu forensik 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).

Bukti digital (*digital evidence*) penting adanya dalam pengungkapan tindak kejahatan, karena termasuk ke dalam bagian dari alat bukti. Alat bukti sendiri merupakan segala sesuatu benda yang digunakan atau ada hubungan dengan tindak kejahatan; alat bukti dapat digunakan sebagai bahan pembuktian untuk memberikan keyakinan pada hakim terhadap suatu perkara tindak kejahatan (Handoko, 2016). Menurut Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyebutkan, "*informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.*" Penanganan pada bukti digital harus dilakukan dengan baik dan benar, agar tidak terjadi kerusakan karena sifatnya yang rentan rusak. Sedikit kesalahan dalam

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

penanganan bukti digital baik disengaja maupun tidak disengaja dapat membuat bukti tersebut tidak akurat, sehingga tidak sah saat diajukan ke pengadilan sebagai alat bukti. Oleh karena itu, penanganan yang baik dan benar dapat membuat bukti digital sebagai bukti yang masif dan dapat diterima. Penanganan dan penggunaan kerangka kerja/metode/model forensik digital secara efektif dalam mendapatkan bukti digital dapat membantu dalam pengungkapan kejahatan siber dengan mudah. Dalam penanganannya, membutuhkan alat atau aplikasi forensik untuk mempermudah dalam mendapatkan bukti digital. Terdapat aplikasi forensik *open-source* maupun *proprietary* yang dapat membantu dalam mendapatkan bukti digital; tidak semua aplikasi forensik dapat digunakan untuk semua ponsel (Cahyanto, 2015).

Dalam penelitian yang dilakukan oleh Patankar dan Bhandari (2014) terdapat daftar bidang forensik: Forensik Memori dan Komputer (*Memory and Computer Forensic*), Forensik Perangkat Seluler (*Mobile Forensic*), serta Forensik Jaringan (*Network Forensic*) yang terbagi dalam aplikasi forensik bersifat berbayar (*proprietary*) maupun yang gratis (*open-source*). Penggunaan aplikasi *open-source* dipilih dalam penelitian karena mudahnya dalam mendapat akses tanpa kendala privasi serta biaya yang digunakan tidaklah banyak dalam pengadaannya. Aplikasi forensik *open-source* untuk penanganan perangkat seluler tersebut, yakni Oxygen Forensic Suite, iPhone Analyzer, WhatsApp Key/DB Extractor, Skype Extractor, SIM Manager dan OSAF-TK. Dalam penelitian lain yang dilakukan oleh Lohiya, John dan Shah (2015) terdapat daftar aplikasi *open-source* untuk penanganan perangkat seluler, yakni Mobiledit Lite, BitPim dan Autopsy. Berikut merupakan daftar aplikasi forensik *open-source* pada penanganan forensik perangkat seluler beserta ketersediaannya yang tersaji pada Tabel 1.1.

Tabel 1.1. Daftar Aplikasi Forensik *Open-Source*

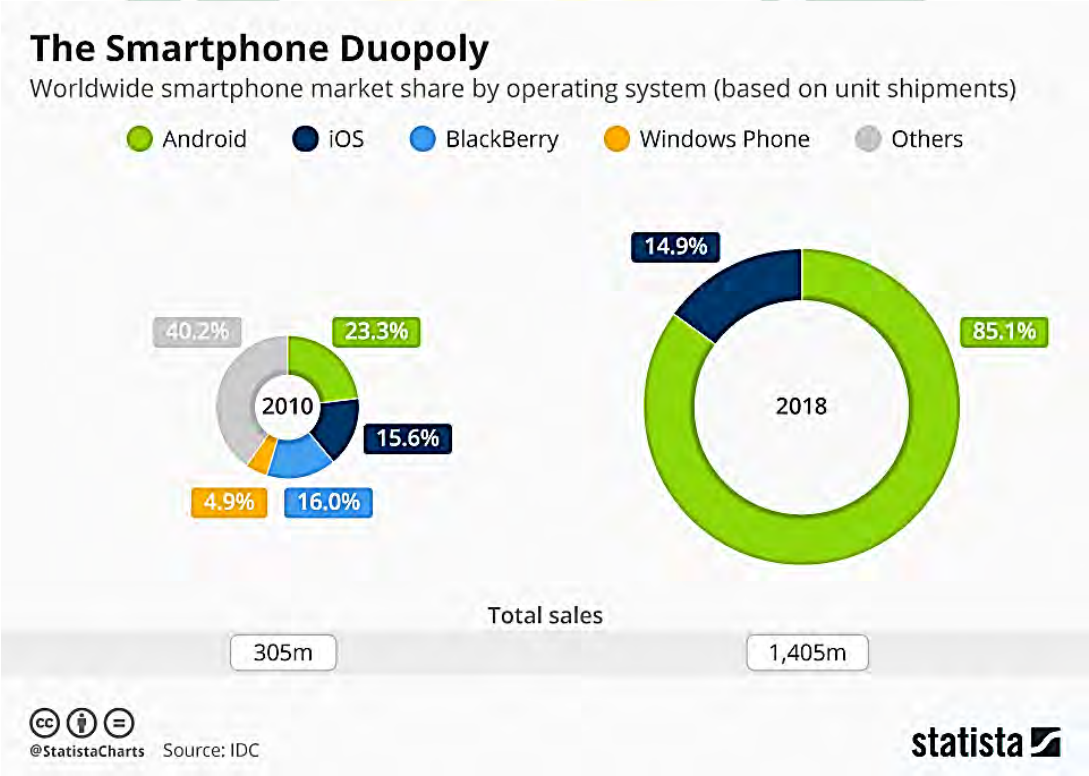
No.	Nama	Sistem Operasi	Ketersediaan	Keterangan
1.	Oxygen Forensic Suite	Windows	Tidak tersedia	Semua perangkat seluler
2.	iPhone Analyzer	Windows	Tersedia	Khusus iOS
3.	WhatsApp Key/DB Extractor	Windows	Tersedia	Khusus WhatsApp

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

No.	Nama	Sistem Operasi	Ketersediaan	Keterangan
4.	Skype Extractor	Windows	Tersedia	Khusus Skype
5.	SIM Manager	Windows	Tidak tersedia	Khusus *SIM card*
6.	OSAF-TK	Linux	Tersedia	Semua perangkat seluler
7.	Mobiledit Lite	Windows	Tidak tersedia	Semua perangkat seluler
8.	BitPim	Windows	Tersedia	Semua perangkat seluler
9.	Autopsy	Windows	Tersedia	Semua perangkat seluler

Ponsel yang berbasis Android akan dijadikan sebagai media yang akan digunakan pada penelitian ini karena sistem operasi Android bersifat *open-source,* sehingga dapat dilakukan modifikasi untuk mendapatkan fitur yang lebih luas dengan *rooting* (Kumar & Yugandhar, 2017). Serta hasil survei yang dilakukan oleh Statista (2019), terdapat diagram penjualan unit *smartphone* berdasarkan sistem operasi pada Gambar 1.1.

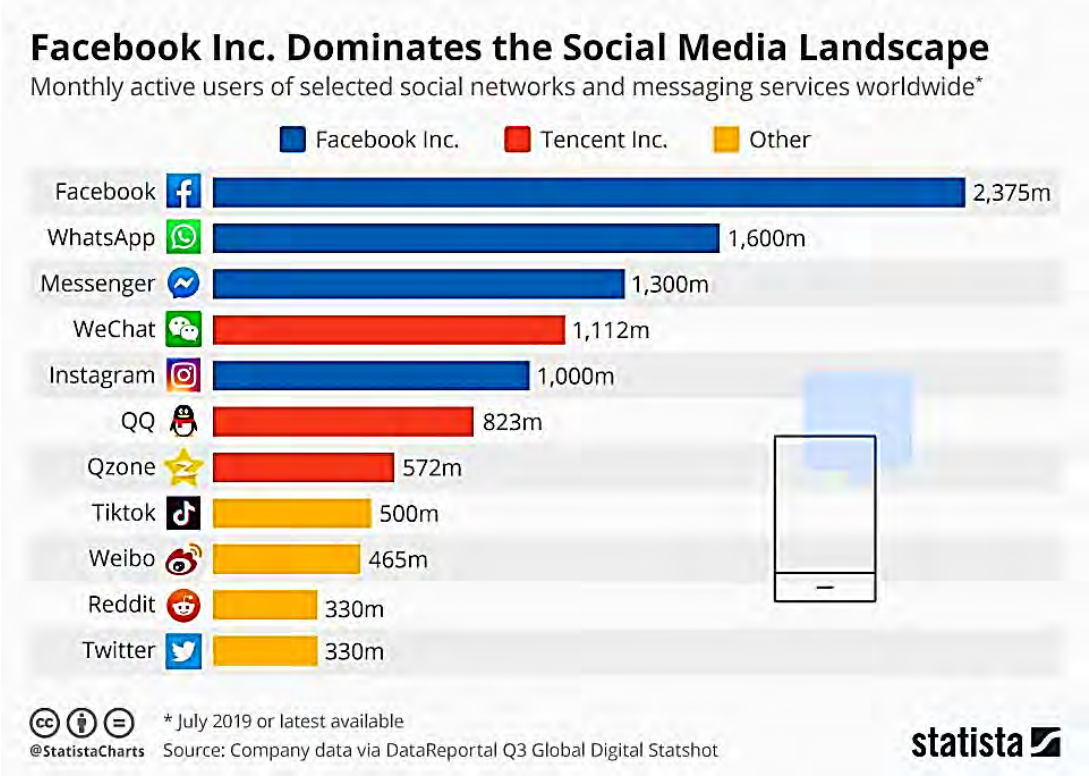


Gambar 1.1. Diagram Penjualan *Smartphone*

WhatsApp akan dijadikan sebagai bukti digital pada penelitian ini karena merupakan aplikasi media sosial yang berfokus pada layanan berbagi pesan, baik

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

yang berupa teks, gambar, audio, video, dokumen, dan GPS (*Global Positioning System*) serta dapat digunakan untuk melakukan telepon; isi dari pesan dan penggunan telepon pada aplikasi WhatsApp tersebut akan dijadikan sebagai artefak pada penelitian ini. WhatsApp juga merupakan aplikasi media sosial yang banyak digunakan di seluruh dunia berdasarkan data hasil survei dari Statista (2019) yang terdapat pada Gambar 1.2.



Gambar 1.2. Grafik Pengguna Sosial Media

Terdapat banyak kerangka kerja/metode/model forensik digital yang umum digunakan pada penanganan kejahatan siber. Dalam penelitian yang dilakukan oleh Ajijola, Zavarsky, dan Ruhl pada 2014, penelitian tersebut membandingkan dua pedoman forensik tentang penanganan bukti digital, yakni *NIST SP 800-101 Rev. 1*:*2014* dan *IOS/IEC 27037*:*2012*. Perbandingan dua pedoman forensik tersebut tersaji pada Tabel 1.2.

Tabel 1.2. Perbandingan Pedoman Forensik

No.	NIST SP 800-101 Rev. 1	ISO/IEC 27037
1.	Pedoman penggunaan khusus untuk perangkat seluler.	Pedoman penggunaan untuk semua perangkat digital secara umum.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

No.	NIST SP 800-101 Rev. 1	ISO/IEC 27037
2.	Proses penyidikan secara teknis dan nonteknis.	Proses penyidikan hanya secara nonteknis.
3	Investigasi forensik pada perangkat seluler dijelaskan secara rinci.	Penjelasan penanganan hanya pada saat awal investigasi forensik.
4.	Dapat digunakan untuk analisis terhadap perangkat seluler serta bukti digital.	Analisis hanya pada perangkat digital secara umum tanpa analisis terhadap bukti.

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 pada perangkat seluler dalam mendapatkan bukti digital.

Aplikasi forensik yang akan digunakan dalam penelitian ini yakni WhatsApp Key/DB Extractor, BitPim, dan Autopsy. Pemilihan ketiga aplikasi tersebut berdasarkan paparan dari latar belakang terhadap kesesuaian aplikasi dengan bukti yang akan digunakan, ketersediaan aplikasi serta basis sistem operasi aplikasi forensik terpasang.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, dapat dirumuskan permasalahan yang akan diselesaikan dalam penelitian ini yakni bagaimana analisis kinerja WhatsApp Key/DB Extractor, BitPim, dan Autopsy dalam mendapatkan bukti digital yang akan dijadikan sebagai barang bukti berdasarkan pengukuran dari *NIST Special Publication 800-101 Revision 1*?

1.3. Batasan Masalah

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka permasalahan dibatasi pada

1. Penelitian terbatas pada pengungkapan bukti digital yang terdapat pada aplikasi WhatsApp.
2. Pemulihan menggunakan Samsung Young 2 Duos, ponsel cerdas dengan sistem operasi Android.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

3. Ponsel cerdas sebelum dilakukan pembuatan skenario berada pada kondisi kembali ke pengaturan pabrik (*factory reset*).
4. Proses akuisisi menggunakan metode akuisisi logis (*logical acquisition*).
5. Aplikasi forensik yang digunakan bersifat *open-source* dan berbasis sistem operasi Windows.

1.4. Tujuan Penelitian

Sesuai dengan masalah yang telah dirumuskan, maka tujuan dari penelitian ini yakni untuk mendapatkan hasil analisis kinerja WhatsApp Key/DB Extractor, BitPim, dan Autopsy dalam mendapatkan bukti digital yang akan dijadikan sebagai barang bukti berdasarkan pengukuran *NIST Special Publication 800-101 Revision 1*.

1.5. Manfaat Penelitian

Dalam penelitian ini terdapat dua manfaat, yakni manfaat secara akademis dan manfaat secara aplikatif.

1. Manfaat Secara Akademis
   a. Mendapatkan banyak wawasan dan ilmu baru dari penerapan pengukuran National Institute of Standards and Technology (NIST) pada bidang forensik digital.
   b. Menambah wawasan terkait aplikasi forensik yang dapat digunakan untuk mendapatkan bukti digital pada perangkat seluler.
2. Manfaat Secara Aplikatif
   a. Dengan adanya ilmu forensik digital dapat mengetahui bahwa data yang hilang dapat dipulihkan.
   b. Dengan penggunaan alat forensik yang tepat, maka bukti digital dapat dipulihkan dengan baik.

1.6. Sistematika Penulisan

Sistematika penulisan laporan pada penelitian ini disusun menjadi beberapa bab, sebagai berikut.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

1. BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang memaparkan terkait latar belakang dalam penelitian, rumusan masalah, tujuan penelitian, batasan masalah, serta sistematika penulisan.

2. BAB II LANDASAN TEORI

Bab ini berisi landasan teori sebagai parameter rujukan penelitian. Landasan teori yang disebutkan merupakan hasil penelitian terkait, forensik digital (*digital forensic*), bukti digital (*digital evidence*), pengukuran National Institute of Standards and Technology (NIST) serta teori pendukung lainnya.

3. BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan tentang tahapan pada penelitian ini serta konsep penelitian yang digunakan untuk mengungkapkan bukti digital ini. Dengan adanya metodologi penelitian ini diharapkan dapat mempermudah dalam merumuskan masalah penelitian.

4. BAB IV HASIL DAN PEMBAHASAN

Bab ini memaparkan terkait perancangan skenario pemulihan bukti digital menggunakan pengukuran National Institute of Standards and Technology (NIST) serta melakukan pengujian menggunakan alat forensik yang sudah ditentukan.

5. BAB V PENUTUP

Pada bab ini berisikan simpulan dari hasil analisis yang telah dilakukan serta saran untuk pengembangan penelitian.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB II
LANDASAN TEORI

2.1. Penelitian Terdahulu

Penelitian terdahulu menjadi parameter dalam melakukan penelitian ini, sehingga dapat memperluas teori yang digunakan dalam mengkaji penelitian yang dilakukan. Topik dalam penelitian ini mengangkat beberapa penelitian lain sebagai referensi. Landasan teori dari penelitian terdahulu diambil dari jurnal, skripsi maupun karya ilmiah lain yang terkait dengan penelitian ini. Penelitian terdahulu tersaji pada Tabel 2.1.

Tabel 2.1. Penelitian Terdahulu

No	Judul	Metode	Alat	Media	Hasil
1.	*A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements.* (Umar, Riadi & Maulana, 2017).	National Institute of Standards and Technology (NIST)	WhatsApp Key/DB Extractor, Belkasoft Evidence, dan Oxygen Forensic.	Samsung Galaxy S4 (Android - *Rooted*).	Belkasoft Evidence memiliki indeks nilai tertinggi, yakni 88,23%, diikuti oleh Oxygen Forensic dengan 82,35%, dan WhatsApp DB/Key Extractor dengan 23,52%. Meski Belkasoft Evidence memiliki indeks nilai tertinggi dan WhatsApp Key/DB Extractor unggul dalam hal biaya, Oxygen Forensic lebih unggul dalam memperoleh artefak WhatsApp, baik melalui *logical acquisition* maupun *physical acquisition.*
2.	*Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST.* (Riadi, Sunardi, & Sahiruddin, 2020).	National Institute of Standards and Technology (NIST)	Wondershare dan Oxygen Forensic	Samsung J5 2015 (Android - *Rooted*) dan Samsung J1 Ace (Android - *Rooted*).	Pada *smartphone* pertama, Wondershare memiliki indeks 31%, Oxygen Forensic memiliki indeks 67%, sedangkan pada *smartphone* kedua, Wondershare memiliki indeks 35%, Oxygen Forensic memiliki indeks 69% data terhapus yang dapat dikembalikan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

No	Judul	Metode	Alat	Media	Hasil
3.	*A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger.* (Riadi, Fadlil & Fauzan, 2018)	National Institute of Standards and Technology (NIST)	Mobiledit Forensic dan Oxygen Forensic.	SONY Xperia Z (Android - *Rooted*).	Data yang didapatkan oleh Oxygen Forensic memiliki indeks 61.90% sedangkan Mobiledit Forensic memiliki indeks 76.19%. Oxygen Forensic lebih baik dalam mendapatkan data pada aplikasi LINE, karena mempunyai fungsi *case management.* Sedangkan pada Mobiledit Forensic tidak memiliki fungsi *case management,* namun sangat efisien dalam hal laporan serta ekstraksi data.
4.	*Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method.* (Riadi, Yudhana, & Putra, 2018).	National Institute of Standards and Technology (NIST)	Axiom Magnet dan Oxygen Forensic.	Samsung Galaxy Star (Android - *Rooted*).	Dari dua jenis data yang ingin didapatkan dari Instagram, yakni *chat* dan gambar. Data yang didapatkan oleh Axiom Magnet memiliki indeks nilai 100% sedangkan Oxygen Forensic memiliki indeks nilai 84%.
5.	*Analisa dan Evaluasi Kemampuan Tools untuk Forensik Smartphone Berbasis Android Studi Kasus PUSLABFOR BARESKRIM MABES POLRI.* (Cahyanto, 2015).	National Institute of Standards and Technology (NIST)	UFED, XRY, dan Device Seizure.	Samsung Galaxy Young (Android) dan Samsung Galaxy Gio (Android).	*Chipset* serta sistem operasi berpengaruh pada proses akuisisi serta analisis data pada *smartphone* secara *physical.* Keberhasilan akuisisi data ditentukan oleh aplikasi *bootloader* alat forensik dalam melakukan *root, dump file,* serta *decoding* data hasil ekstraksi. Hanya UFED yang mampu mendapatkan data secara *physical*, sedangkan XRY dan Device Seizure mengalami kendala dalam mendapatkan akses *super user*.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Lima penelitian yang telah dijadikan landasan pada penelitian ini, semuanya menggunakan National Institute of Standards and Technology (NIST) sebagai kerangka kerja/metode/model forensik digital serta menggunakan *smartphone* dengan sistem operasi Android sebagai media pembanding untuk menguji kinerja setiap aplikasi forensik yang digunakan. Penelitian ini berfokus untuk mengetahui kinerja setiap aplikasi forensik yang bersifat *open-source* dalam mendapatkan bukti digital pada perangkat seluler. Aplikasi forensik tersebut yakni WhatsApp Key/DB Extractor, BitPim, dan Autopsy. Media yang digunakan –*Samsung Young 2 Duos*– merupakan *smartphone* yang berjalan pada sistem operasi Android. Aplikasi WhatsApp digunakan sebagai bahan pengujian, sehingga dalam pengujian akan dilakukan pencarian data berupa catatan panggilan, daftar kontak serta media komunikasi yang digunakan pada pesan, baik yang berupa teks, gambar, audio, video, dokumen serta GPS (*Global Positioning System*) dengan menggunakan metode akuisisi logis (*logical acquisition*).

2.2. Forensik Digital (*Digital Forensic*)

Forensik merupakan ilmu tentang pencarian suatu fakta bukti akan adanya kejadian yang berhubungan dengan permasalahan hukum, sehingga fakta bukti tersebut akan dijadikan sebagai barang bukti di pengadilan; forensik digital (*digital forensic*) merupakan bagian dari ilmu forensik yang penanganannya dikhususkan untuk perangkat digital, baik itu komputer, ponsel atau perangkat digital lainnya (Riadi, Sunardi, & Rauli, 2018).

Forensik digital juga merupakan suatu tindakan investigasi untuk mendapatkan data informasi pada perangkat digital yang digunakan sebagai fakta bukti terkait tindak kejahatan serta permasalahan hukum (Raharjo, 2013).

2.2.1. Forensik Perangkat Seluler (*Mobile Forensic*)

Forensik perangkat seluler (*mobile forensic*) merupakan bidang ilmu pada forensik digital yang mempelajari tentang proses pemulihan bukti digital menggunakan aturan dan langkah yang tepat dari ponsel. Data yang diambil dari ponsel melalui proses forensik dapat dijadikan sebagai bukti yang sah apabila ditangani dengan baik dan benar (Yadi & Kunang, 2018).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Terdapat kerangka kerja/metode/model forensik digital yang dapat digunakan untuk melakukan analisis pada perangkat digital secara umum, yakni *Integrated Digital Forensic Investigation Framework (IDFIF), National Institute of Standards and Technology (NIST), Association of Chief Police Officers (ACPO), International Organization for Standardization (ISO), Smartphone Forensic Investigation Process Model (SFIPM), Symbian Smartphones Forensic Process Model (SSFP), Harmonized Digital Forensic Investigation Process (HDFIP), dan Windows Mobile Device Forensic Model (WMDFM)* (Ruuhwan, Riadi, & Prayudi, 2017). Dalam penelitian yang dilakukan oleh Ajijola, Zavarsky, dan Ruhl (2014), penelitian tersebut membandingkan 2 pedoman forensik tentang penanganan bukti digital, yakni *NIST SP 800-101 Rev. 1:2014* dan *ISO/IEC 27037:2012*. Dalam pedoman tersebut *NIST SP 800-101 Rev. 1* lebih dikhususkan untuk penanganan pada perangkat seluler, sedangkan *ISO/IEC 27037* penanganan forensik secara umum.

2.3. Bukti Digital (*Digital Evidence*)

Bukti digital (*digital evidence*) merupakan data atau informasi yang disimpan atau dikirim menggunakan komputer yang mendukung, termasuk pada perangkat seluler. Hal ini sebagai upaya untuk membantah teori tentang bagaimana suatu pelanggaran terjadi atau hal yang membahas unsur-unsur penting dari pelanggaran seperti niat atau alibi (Casey, 2011).

Bukti digital penting adanya dalam pengungkapan tindak kejahatan, karena termasuk ke dalam bagian dari alat bukti. Alat bukti merupakan segala sesuatu yang berhubungan dengan tindak kejahatan yang dapat digunakan sebagai bahan pembuktian atas adanya kebenaran dari tindak kejahatan yang telah dilakukan oleh terdakwa dalam persidangan (Handoko, 2016).

Bukti digital mempunyai sifat yang rentan rusak jika tidak mendapatkan penanganan dengan baik dan benar. Sedikit banyaknya perubahan pada bukti digital dapat dianggap sebagai bukti yang tidak sah saat diajukan dalam persidangan (Albanna & Riadi, 2017).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2.4. Alat Forensik (*Forensic Tool*)

Alat forensik (*forensic tool*) merupakan alat yang digunakan untuk membantu mendapatkan bukti yang akan digunakan sebagai barang bukti. Sedangkan alat forensik digital (*digital forensic tool*) atau aplikasi forensik digital (*digital forensic application*) yakni alat atau aplikasi yang digunakan untuk mendapatkan data serta informasi yang terdapat pada perangkat digital. Terdapat banyak alat atau aplikasi forensik digital yang dapat digunakan untuk membantu penanganan pada perangkat digital, baik itu yang bersifat *open-source* maupun *proprietary*; tidak semua alat atau aplikasi forensik dapat digunakan pada setiap perangkat digital (Cahyanto, 2015).

2.4.1. Alat Forensik Perangkat Seluler *Open-Source*

Daftar alat atau aplikasi forensik *open-source* yang dikhususkan untuk penanganan pada perangkat seluler hasil dari penelitian yang dilakukan oleh Lohiya, John, dan Shah (2015), serta penelitian yang dilakukan oleh Patankar dan Bhandari (2014) tersaji pada Tebel 2.2.

Tabel 2.2. Daftar Alat Forensik Perangkat Seluler *Open-Source*

No.	Nama
1.	Oxygen Forensic Suite
2.	iPhone Analyzer
3.	WhatsApp Key/DB Extractor
4.	Skype Extractor
5.	SIM Manager
6.	OSAF-TK
7.	Mobiledit Lite
8.	BitPim
9.	Autopsy

2.4.2. Alat Forensik Perangkat Seluler *Proprietary*

Daftar alat atau aplikasi forensik proprietary yang dikhususkan untuk penanganan pada perangkat seluler hasil dari penelitian yang dilakukan oleh Lohiya, John, dan Shah (2015), serta penelitian yang dilakukan oleh Patankar dan Bhandari (2014) tersaji pada Tabel 2.3.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Tabel 2.3. Daftar Alat Forensik Perangkat Seluler *Proprietary*

No.	Nama
1.	Mobiledit Forensic
2.	iXAM
3.	MSAB XRY
4.	CellDEK TEK
5.	Oxygen Forensic
6.	Paraben DDS / Paraben's Cell Seizure
7.	Cellebrite UFED / Cellebrite Mobile Forensic Toolkits (UFED 4PC)
8.	ACESO KIOSK
9.	Elcomsoft iOS Forensic Toolkit

2.5. Kejahatan Siber (*Cybercrime*)

Kejahatan siber (*cybercrime*) merupakan bentuk kejahatan yang timbul karena adanya penyalagunaan pada teknologi informasi yang menggunakan internet. Kejahatan siber didefinisikan juga sebagai suatu tindak kejahatan yang melanggar hukum dengan menggunakan perangkat digital sebagai alat kejahatannya; para penjahat siber melakukan tindak kejahatan untuk tujuan mencari keuntungan atau hanya sekedar iseng (Kataren, 2016).

Dibutuhkan tindakan yang tegas untuk para penjahat siber agar mereka jera. Kejahatan siber termasuk dalam kategori tindakan kejahatan tanpa batasan ruang dan waktu (*borderless crime*), sehingga upaya untuk memberantas tindak kejahatan ini memerlukan langkah yang kompleks, terintegrasi serta berkesinambungan dari banyak pihak, tidak hanya para penegak hukum, namun juga para pengguna teknologi (Arifah, 2011).

Kejahatan siber terbagi dalam 2 kategori tindak kejahatan, yakni *Violent/Potentially Violent* dan *Non-Violent* (Ghosh & Turrini, 2010).

2.5.1. Violent/Potentially Violent

Violent/Potentially Violent merupakan penyalahgunaan pada teknologi informasi yang mempunyai dampak langsung secara fisik pada orang lain. Secara garis besar penyalagunaan ini terbagi dalam 3 kelompok utama, yakni:

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

1. *Cyberterrorism*

Suatu kegiatan yang mengarah pada aktivitas pertentangan di suatu wilayah atau yang lebih dikenal dengan terorisme dengan memanfaatkan media *cyberspace*.

2. *Cyberbullying*

Suatu tindakan yang dilakukan oleh sesorang atau kelompok untuk menimbulkan ketakutan pada diri orang lain dengan memanfaatkan media *cyberspace*.

3. *Child Pornography*

Suatu kejahatan ponografi yang melibatkan anak kecil sebagai medianya. Tindak kejahatan ini melibatkan para pembuat, penyebar, serta mereka yang mengakses materi pornografi.

2.5.2. Non-Violent

Non-Violent merupakan penyalahgunaan pada teknologi informasi yang tidak berdampak langsung pada fisik seseorang namun lebih pada kerugian secara sistem atau materi. Secara garis besar penyalahgunaan ini terbagi dalam 4 kelompok utama yakni:

1. *Cybertrespass*

Suatu tindakan yang dilakukan untuk mengakses data atau informasi yang ada pada komputer orang lain atau perusahaan yang besifat privasi secara illegal.

2. *Cybertheft*

Suatu tindakan pencurian, peniruan serta penggunaan data atau informasi penting pada komputer orang lain atau perusahaan.

3. *Cyberfraud*

Suatu tindakan penyalagunaan teknologi informasi dengan memanipulasi data atau informasi penting untuk mendapatkan keuntungan sebesar-besarnya.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

4. *Destructive Crime*

Suatu tindakan penyalagunaan teknologi informasi yang dilakukan untuk membuat suatu dampak kerusakan atau kehilangan data informasi pada komputer orang lain atau perusahaan.

2.6. National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) merupakan salah satu kerangka kerja/metode/model dalam bidang *cybersecurity* yang salah satu dari fokusnya yakni pada bidang forensik digital. Terdapat berbagai macam bidang forensik digital pada kerangka kerja/metode/model dari National Institute of Standards and Technology (NIST), salah satunya yakni bidang *mobile forensics* (forensik perangkat seluler). Dalam publikasi yang dilakukan oleh Ayers, Brothers, dan Jansen (2014), yang termuat dalam dokumen *Guidelines on Mobile Device Forensics*: *NIST Special Publication 800-101 Revision 1* terdapat tahapan yang digunakan untuk melakukan analisis terhadap perangkat seluler dalam mendapatkan bukti digital atau tahapan untuk mendapatkan informasi dari perangkat seluler menjadi bukti digital. Tahapan dalam penanganan forensik pada perangkat seluler berdasarkan pengukuran *NIST Special Publication 800-101 Revision 1,* dimulai dari *Preservation* (Penjagaan), *Acquisition* (Akuisisi), *Examination & Analysis* (Pemeriksaan & Analisis) hingga *Reporting* (Pelaporan) yang terdapat pada Gambar 2.1.

Gambar 2.1. Tahapan *NIST Special Publication 800-101 Revision 1*

Berikut merupakan penjelasan terkait gambar dari tahapan penelitian berdasarkan pengukuran *NIST Special Publication 800-101 Revision 1*:

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.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

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.

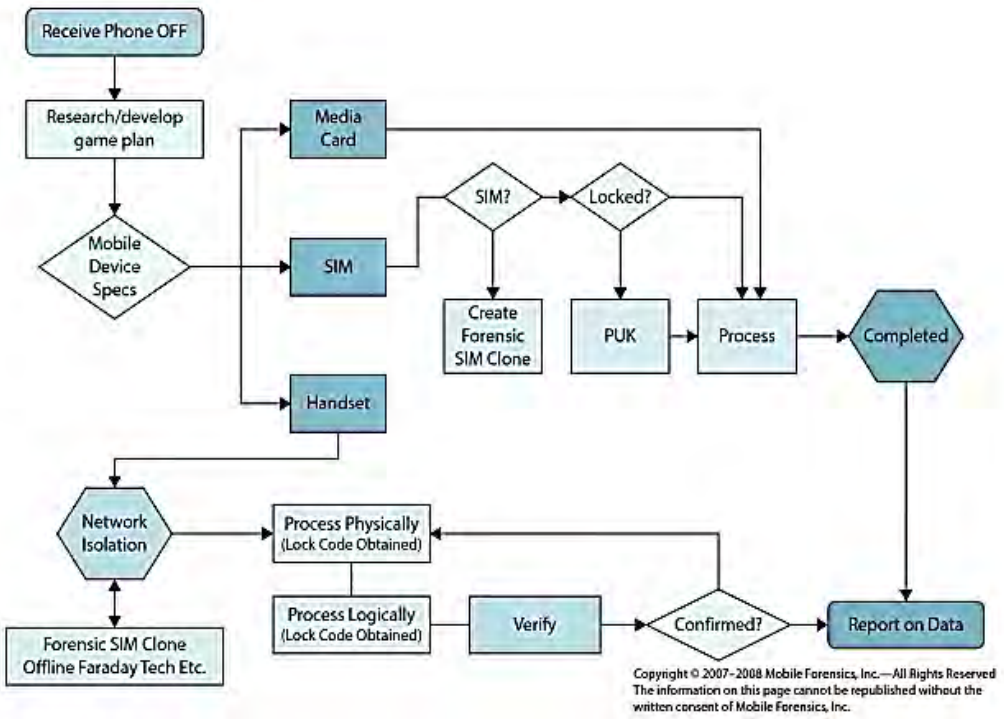
3. *Examination & Analysis*

Tahap ini merupakan tahapan pemerikasaan serta analisis terhadap data dilakukan sesuai dengan aturan yang dibenarkan, hingga akhirnya data dapat menjadi bukti yang sah.

4. *Reporting*

Tahap ini merupakan tahapan pada pelaporan terkait hasil analisis pada data diberikan.

Gambaran alur kerja menurut Lee Reiber (2019) dalam melakukan penanganan forensik terhadap perangkat seluler berdasarkan pengukuran National Institute of Standards and Technology (NIST) terdapat pada Gambar 2.2.



Gambar 2.2. Alur Kerja Penanganan Forensik Perangkat Seluler

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2.7. Ponsel Cerdas (*Smartphone*)

Ponsel cerdas (s*martphone*) merupakan telepon genggam yang mempunyai kemampuan serta fungsi menyerupai komputer. Layaknya komputer, s*martphone* juga bekerja menggunakan sistem operasi serta berbagai perangkat lunak yang mendukungnya. S*martphone* juga disebut dengan komputer kecil yang berbentuk telepon (Daeng, Mewengkang, & Kalesaran, 2017).

Smartphone mempunyai banyak manfaat; penggunaan nama besar *brand* pada *smartphone* dianggap sebagai salah satu gaya hidup. Optimalisasi penggunaan s*martphone* dengan memanfaatkan semua fitur yang ada di dalamnya sebaik mungkin; jika pengguna tidak memanfaatkan fitur yang ada secara optimal, identifikasi *smartphone* tidak ada bedanya dengan ponsel genggam lainnya (Chuzaimah Mabruroh, & Dihan, 2010).

Terdapat berbagai sistem operasi yang melekat sebagai alat untuk menampilkan antarmuka, kebanyakan dari sistem operasi tersebut bersifat *open-source*. Hal ini memungkin setiap pengguna yang mempunyai kemampuan di bidang teknologi informasi, khususnya bidang pemrograman dapat melakukan perubahan di dalamnya (Kumar & Yugandhar, 2017).

2.8. Media Sosial (*Social Media*)

Media sosial (*social media*) merupakan sarana yang digunakan oleh individu maupun kelompok untuk mengekspesikan identitasnya secara daring dengan cara berbagi isi, berita, foto, video atau hal lainnya dengan orang lain. Setiap individu memiliki tujuan serta perilaku tersendiri yang membuat mereka menggunakan media sosial, seperti: swafoto, *cyberwar*, belanja daring, personalisasi diri pengguna, dan budaya berbagi (Mulawarman & Nurfitri, 2017).

Media sosial juga mempunyai peranan strategis sebagai sarana komunikasi antara masyarakat dengan pemerintah atau perusahaan sebagai bentuk aspirasi untuk menyampaikan kritikan maupun saran terkait suatu kebijakan yang dikeluarkan, karena media sosial telah menjadi kunci untuk melakukan provokasi terhadap pemikiran, pembicaraan, serta tindakan terkait isu sosial yang terjadi. Namun, perlu adanya kesadaran untuk bijak dalam menggunakan media sosial (Rahadi, 2017).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2.9. Integrasi Keilmuan

Integrasi keilmuan pada penelitian ini menggunakan metode penelitian kualitatif dengan melakukan wawancara kepada Kepala Urusan Kesejahteraan Rakyat (Kaur Kesra) Desa Cangkir, Kecamatan Driyorejo, Kabupaten Gresik sekaligus modin di desa tersebut, yakni Ustaz M. Sutadji MZ. Dengan diajukan pertanyaan terkait konsep integrasi antara ilmu tafsir Alquran dan Hadis dengan ilmu forensik digital dalam pemulihan bukti digital, beliau memaparkan beberapa surat yang berkaitan dengan forensik serta barang bukti digital sebagai berikut:

1. Surat Yasin ayat 12:

إِنَّا نَحْنُ نُحْيِ ٱلْمَوْتَىٰ وَنَكْتُبُ مَا قَدَّمُوا۟ وَءَاثَٰرَهُمْ ۚ وَكُلَّ شَىْءٍ أَحْصَيْنَٰهُ فِىٓ إِمَامٍ مُّبِينٍ ۞

Artinya: *Sesungguhnya Kami menghidupkan orang-orang mati dan Kami menuliskan apa yang telah mereka kerjakan dan bekas-bekas yang mereka tinggalkan. Dan segala sesuatu Kami kumpulkan dalam Kitab Induk yang nyata (Lauh Mahfuzh).*

2. Surat Al Qiyamah ayat 3–4:

أَيَحْسَبُ ٱلْإِنسَٰنُ أَلَّن نَّجْمَعَ عِظَامَهُۥ ۞ بَلَىٰ قَٰدِرِينَ عَلَىٰٓ أَن نُّسَوِّىَ بَنَانَهُۥ ۞

Artinya: *Apakah manusia mengira, bahwa Kami tidak akan mengumpulkan (kembali) tulang belulangnya? Bukan demikian, sebenarnya Kami kuasa menyusun (kembali) jari jemarinya dengan sempurna*.

3. Surat Al Baqarah ayat 42:

وَلَا تَلْبِسُوا۟ ٱلْحَقَّ بِٱلْبَٰطِلِ وَتَكْتُمُوا۟ ٱلْحَقَّ وَأَنتُمْ تَعْلَمُونَ ۞

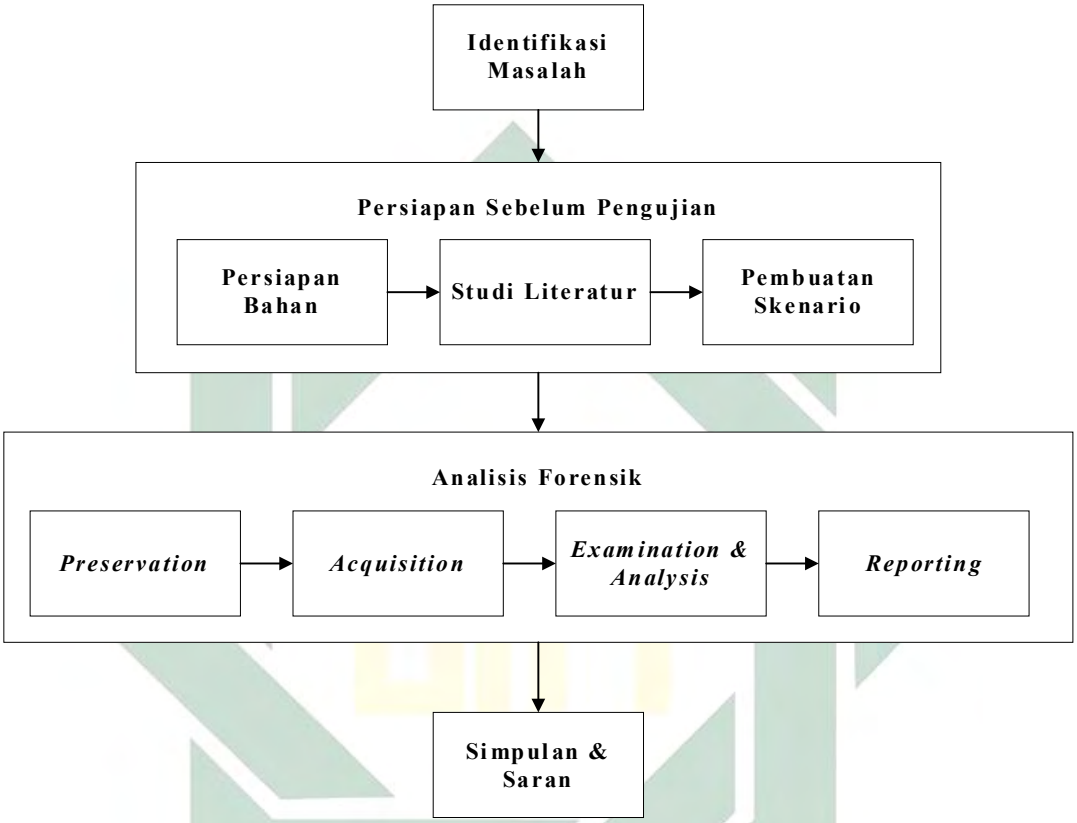
Artinya: *Janganlah kalian campur-adukkan antara kebenaran dan kebatilan, dan kalian sembunyikan yang benar padahal kamu mengetahuinya*.

Dari ketiga surat yang sudah dipaparkan, beliau menjelaskan, "*setiap benda yang dihilangkan jejaknya pasti dapat dikembalikan, meski melalui proses yang mudah atau susah, cepat atau lambat, karena setiap perkara yang batil pasti akan terkuak kebenarannya sebagai bentuk dari kasih Allah SWT kepada umat-Nya.*"

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB III
METODOLOGI PENELITIAN

Alur penelitian bertujuan agar proses yang dilakukan berjalan dengan runtut. Alur penelitian ini terdapat pada Gambar 3.1.



Gambar 3.1. Alur Penelitian

3.1. Identifikasi Masalah

Identifikasi masalah merupakan penentuan masalah yang akan dipecahkan dalam penelitian ini. Masalah yang ditentukan dijabarkan pada pada latar belakang penulisan, terkait banyaknya kejahatan yang menggunakan teknologi informasi, salah satunya dengan perantara media sosial, yang pada penelitian ini menggunakan aplikasi WhatsApp, sehingga dengan dilakukannya investigasi terhadap ponsel –*Samsung Young 2 Duos*– yang dijadikan sebagai barang bukti, diharapkan dapat mengungkapkan barang bukti dalam bentuk digital yang sudah dihilangkan jejaknya dengan menggunakan pengukuran *NIST Special Publication 800-101 Revision 1* serta aplikasi forensik, WhatsApp Key/DB Extractor, BitPim, dan Autopsy.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

3.2. Persiapan Sebelum Pengujian

Persiapan sebelum pengujian merupakan tahapan yang dilakukan untuk mempersiapkan segala sesuatu sebelum proses analisis forensik terhadap ponsel dilakukan. Terdapat dua tahapan pada proses persiapan sebelum pengujian ini, yakni studi literatur dan pembuatan skenario.

3.2.1. Studi Literatur

Studi literatur merupakan tahapan yang dilakukan dengan mencari referensi yang berasal dari buku, jurnal maupun karya ilmiah lainnya untuk mendapatkan informasi terkait digital forensik, forensik perangkat seluler, National Institute of Standards and Technology (NIST), serta hal lainnya yang terkait. Studi literatur diharapkan dapat membantu mempermudah dalam penanganan pemulihan bukti digital ini.

3.2.2. Pembuatan Skenario

Pembuatan skenario merupakan tahapan yang dilakukan untuk membuat rencana kejahatan siber. Data hasil pembuatan skenario ini yang akan dijadikan data awal, dan kemudian diungkap melalui proses analisis forensik. Berikut merupakan skenario yang akan dilakukan

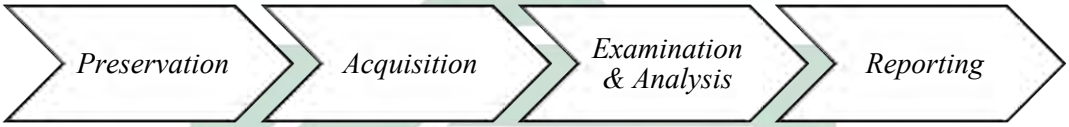
1. Menyimpan nomor telepon;
2. Membuat dokumen di aplikasi pembuat dokumen;
3. Merekam suara diaplikasi perekam suara;
4. Membuat gambar dan video di aplikasi kamera.
5. Mengirim pesan WhatsApp baik berupa teks, audio, gambar, video, dokumen dan GPS;
6. Melakukan *miss-call* dan panggilan telepon melalui aplikasi WhatsApp;
7. Menghapus semua pesan WhatsApp baik berupa teks, audio, gambar, video, dokumen, dan GPS;
8. Menghapus semua dokumen di aplikasi pembuat dokumen;
9. Menghapus semua audio di aplikasi perekam suara;

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

10. Menghapus semua gambar dan video di galeri.
11. Menghapus semua riwayat *miss-call* dan panggilan telepon melalui aplikasi WhatsApp; serta
12. Menghapus semua kontak telepon.

3.3. Analisis Forensik

Analisis forensik digital dalam pemulihan bukti digital berdasarkan pengukuran *NIST Special Publication 800-101 Revision 1* terdapat pada Gambar 3.2.



Gambar 3.2. Analisis Forensik *NIST Special Publication 800-101 Revision 1*

Berikut merupakan penjelasan analisis forensik digital dalam pemulihan bukti digital berdasarkan pengukuran *NIST Special Publication 800-101 Revision 1*:

3.3.1. *Preservation*

Pada tahapan *preservation*, ponsel yang digunakan akan diamankan, kemudian dilakukan identifikasi serta pelabelan pada setiap ponsel terkait informasi dari ponsel tersebut dengan tetap mengikuti prosedur dalam menjaga integritas data, yakni dengan mematikan koneksi telekomunikasi atau tindakan lain yang mungkin dapat mempengaruhi perubahan data yang ada pada ponsel saat diamankan dan sesudah diamankan. Serta pembuatan berkas informasi awal barang bukti serta berkas terkait investigasi forensik yang akan dilakukan.

3.3.2. *Acquisition*

Pada tahapan *acquisition*, data pada ponsel akan diambil secara forensik dengan metode akuisisi secara logis (*logical acquisition*), yakni metode pengambilan data *file system* secara keseluruhan atau langsung ke pencarian secara spesifik, sehingga akuisisi secara logis ini memungkinkan untuk membuat *image disk* yang digunakan untuk melakukan akuisisi secara fisik (*physical acquisition*). Jenis ekstensi nama berkas *image disk* yang berbeda pada setiap aplikasi forensik dan tidak semua aplikasi forensik dapat membuat ekstensi

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

image disk sehingga membutuhkan aplikasi pihak ketiga untuk melakukan akuisisi atau hanya dapat membuat *image disk* untuk aplikasinya saja. Dengan demikian pembuatan *image disk* akan dilakukan jika memungkinkan untuk membuat *image disk* yang dapat dijadikan sebagai barang bukti untuk dilakukan pengujian ulang jika dibutuhkan.

Metode akuisisi secara logis dipilih agar data pada ponsel tidak akan berubah meski digunakan berulang, baik dengan menggunakan *image disk* yang sudah dibuat atau akuisisi langsung pada perangkat. Dalam akuisisi data juga harus tetap mengikuti prosedur dalam menjaga integritas data, sehingga bukti digital yang akan dijadikan sebagai barang bukti bersifat masif dan dapat diterima.

3.3.3. *Examination & Analysis*

Pada tahapan *examination* & *analysis,* data hasil akuisisi pada ponsel akan dilakukan pemeriksaan dan analisis sesuai dengan fokus investigasi, yakni pengembalian data berupa catatan panggilan, daftar kontak serta media komunikasi yang digunakan pada pesan, baik yang berupa teks, gambar, audio maupun video pada aplikasi WhatsApp sesuai dengan aturan yang dibenarkan, hingga akhirnya data dapat menjadi bukti yang bersifat masif dan dapat diterima. Analisis dilakukan secara manual sesuai dengan kebutuhan karena proses akuisisi menggunakan metode akuisisi logis (*logical acquisition*).

Parameter yang digunakan untuk melakukan analisis terhadap kinerja aplikasi 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, Optional Features Requirements.* Untuk parameter *Artifacts* merupakan data yang ada pada perangkat digital yang akan dikembalikan untuk dijadikan bukti digital. 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

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

melibatkan aplikasi pihak ketiga dalam melakukan perubahan data saat proses akuisisi berlangsung. Untuk parameter *Artifacts* tergantung kebutuhan dalam penelitian atau data yang dapat dijadikan sebagai barang bukti. Karena penelitian ini menggunakan aplikasi WhatsApp, maka artefaknya merupakan data yang ada pada aplikasi WhatsApp. Parameter pada penelitian ini tersaji dalam Table 3.1.

Tabel 3.1. Parameter National Institute of Standards and Technology (NIST)

Parameter		**Deskripsi**
Core Assertions	MDT-CA-01	Jika aplikasi forensik perangkat seluler menyediakan opsi akuisisi objek data "Dapatkan Semua" kepada pengguna, maka alat tersebut harus menyelesaikan akuisisi logis dari semua objek data tanpa kesalahan.
	MDT-CA-02	Jika aplikasi forensik perangkat seluler menyediakan objek data individual "Pilih Semua" kepada pengguna, alat tersebut harus menyelesaikan akuisisi logis dari semua objek data yang dipilih secara individual tanpa kesalahan.
	MDT-CA-03	Jika aplikasi forensik perangkat seluler memberi pengguna kemampuan untuk "Pilih Individu" objek data untuk akuisisi, maka alat tersebut harus menyelesaikan akuisisi logis untuk setiap objek data eksklusif tanpa kesalahan.
	MDT-CA-04	Jika konektivitas antara perangkat seluler dan alat forensik terganggu untuk akuisisi logis/sistem file, maka alat tersebut akan memberi tahu pengguna bahwa konektivitas telah terganggu.
	MDT-CA-05	Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka alat tersebut harus memiliki kemampuan untuk menyajikan objek data yang diperoleh dalam format yang dapat digunakan baik melalui panel pratinjau atau laporan yang dihasilkan.
	MDT-CA-06	Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka alat tersebut harus memiliki kemampuan untuk menyajikan informasi terkait pelanggan dan peralatan (misalnya, IMSI, IMEI, MEID / ESN, MSISDN) dalam format yang dapat digunakan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Parameter		Deskripsi
Core Assertions	MDT-CA-07	Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka semua elemen data yang didukung: data PIM, daftar kontak, SMS, MMS, riwayat panggilan, file yang berdiri sendiri (audio, gambar, video), aplikasi, media sosial atau data internet (bookmark, riwayat penelusuran), data email atau GPS harus disajikan dalam format yang dapat digunakan.
	MDT-CA-08	Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, data yang diperoleh berisi karakter non-latin harus disajikan dalam format aslinya.
	MDT-CA-09	Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, nilai *hash* dilaporkan untuk objek data yang diperoleh atau file kasus keseluruhan.
Core Features Requirements	MDT-CR-01	Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk mengenali perangkat yang didukung melalui antarmuka yang disarankan (misalnya, kabel, *Bluetooth*).
	MDT-CR-02	Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk memberi tahu pengguna tentang kesalahan konektivitas antara perangkat dan aplikasi selama ekstraksi data.
	MDT-CR-03	Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk melakukan ekstraksi data logis dari objek data yang didukung tanpa modifikasi.
Artifacts	WA-AO-01: Pesan WhatsApp	Pesan teks yang dikirim melalui aplikasi *WhatsApp.*
	WA-AO-02: Riwayat Panggilan WhatsApp	Riwayat panggilan yang dilakukan melalui aplikasi WhatsApp, baik melaui *audio-call* atau *video-call.*
	WA-AO-03: Daftar Kontak WhatsApp	Daftar kontak atau nomor telepon yang tersimpan ataupun yang tidak disimpan pada aplikasi WhatsApp.
	WA-AO-04: Gambar WhatsApp	Gambar yang berada pada aplikasi WhatsApp hasil dari mengirim pesan gambar atau menerima pesan gambar.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Parameter		Deskripsi
Artifacts	WA-AO-05: Video WhatsApp	Video yang berada pada aplikasi WhatsApp hasil dari mengirim pesan video atau menerima pesan video.
	WA-AO-06: Audio WhatsApp	Audio yang berada pada aplikasi WhatsApp hasil dari mengirim pesan atau menerima pesan suara, lagu atau jenis audio lainnya.
	WA-AO-07: Dokumen WhatsApp	Pesan yang berupa data atau dokumen yang bersifat tertulis pada aplikasi WhatsApp yang tersaji dalam ekstensi *.doc, .xls, .pdf* atau yang sejajar.
	WA-AO-08: Lokasi (GPS) WhatsApp	Pesan yang berupa kiriman lokasi pada aplikasi WhatsApp.

3.3.4. *Reporting*

Pada tahap *reporting,* hasil analisis akan memberikan informasi terkait data transaksi apa saja yang berhasil dikembalikan oleh setiap aplikasi forensik. Informasi tersebut akan dijadikan sebagai laporan terperinci. Laporan hasil uji kinerja setiap aplikasi forensik yang didapat melalui penghitungan indeks. Perhitungan indeks terdapat dua macam, yakni indeks harga dan indeks kuantitas. Indeks harga digunakan untuk perhitungan pada harga atau biaya, sedangkan untuk indeks kuantitas berdasarkan jumlah (Penangsang, Studiviany & Wiwoho, 2020). Untuk mengetahui presentase dari jumlah bukti digital yang dapat diperoleh, maka pemilihan indeks kuantitas lebih tepat digunakan pada penelitian ini. Perhitungan indeks kuantitas menggunakan metode agregatif sederhana, dengan rumus berikut

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

Definisi : I_A = Indeks agregatif tidak tertimbang

$\sum Q_n$ = Jumlah data hasil akuisisi

$\sum Q_0$ = Jumlah data asli

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB IV
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.

4.1. Persiapan Sebelum Pengujian

Tahapan ini merupakan persiapan sebelum melakukan analisis forensik pada Samsung Young 2 Duos.

4.1.1. Persiapan Bahan

Sebelum dua tahapan tersebut, bahan terlebih dahulu dipersiapkan. Berikut daftar bahan perisiapan yang tersaji pada Tabel 4.1.

Tabel 4.1. Daftar Bahan Persiapan

Nama	Keterangan
Asus A455LF	Laptop yang digunakan sebagai media untuk memasang aplikasi forensik, dengan spesifikasi: - Prosesor Intel Core i3-4030U 1.9 GHz - 500Gb / 10Gb RAM - Sistem Operasi Windows 10 Pro
Samsung Young 2 Duos	Ponsel yang digunakan sebagai media barang bukti, dengan spesifikasi: - Prosesor Cortex-A7 1.0 GHz - 4Gb / 516Mb RAM - Sistem Operasi Android 4.4.2
Autopsy v4.17.01	Aplikasi forensik yang digunakan untuk melakukan analisis terhadap ponsel.
BitPim v1.0.7	Aplikasi forensik yang digunakan untuk melakukan analisis terhadap ponsel.
WhatsApp Key/DB Extractor v4.7	Aplikasi forensik yang digunakan untuk melakukan analisis terhadap ponsel.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Nama	Keterangan
WhatsApp v2.21.2.16	Aplikasi yang digunakan sebagai barang bukti.
KingoRoot v4.5.0.	Aplikasi yang digunakan untuk melakukan *root* pada ponsel.
Busybox Free v1.26.2	Aplikasi yang digunakan untuk menjalankan baris perintah Linux/UNIX yang ada pada kernel Android.
WPS Office (BETA) v11.7.1	Aplikasi yang digunakan untuk membuat dokumen.
SDK Platform Tools v30.0.5	Aplikasi yang digunakan untuk mengambil data dari ponsel.
Ncat Platform v5.59BETA1	Aplikasi yang digunakan untuk membaca dan menulis data di seluruh jaringan dari command line.
WhatsApp Viewer v1.13	Aplikasi yang digunakan untuk membaca *database* WhatsApp.
Notepad++ v6.8.2	Aplikasi yang digunakan untuk membaca *database* WhatsApp.
Oracle VM VirtualBox v6.1.18	Aplikasi yang digunakan untuk memasang Sistem Operasi lain dalam satu laptop, dengan spesifikasi: - 18Gb / 2Gb RAM - Sistem Operasi Windows 7 Ultimate SP1
Veger USB	Kabel data yang digunakan untuk menghubungkan ponsel dengan laptop.

Setelah semua barang telah dipersiapkan, langkah selanjutnya yakni melakukan reset pada Samsung Young 2 Duos menjadi seperti kembali ke pengaturan pabrik (*factory reset*). Hal ini bertujuan agar data awal benar-benar dapat diketahui, sehingga data dapat dibandingan dengan hasil akhir dari analisis forensik.

Setelah kembali ke pengaturan pabrik, dilakukan pendaftaran awal pada ponsel sesuai dengan arahan. Setelah selesai, kemudian dilakukan *root* menggunakan aplikasi KingoRoot. Hal ini bertujuan untuk meminimalisir data dimodifikasi. Jika dilakukan *root* setelah ponsel diamankan, kemungkinan data dapat dimodifikasi karena adanya jaringan telekomukasi yang masih menyala. Kecuali alat atau aplikasi forensik mempunyai fitur untuk mendapatkan hak akses *root* tanpa menggunakan jaringan. Kemudian melakukan instalasi Busybox Free yang bertujuan untuk menjalankan baris perintah Linux/UNIX yang ada pada

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Android, sehingga dapat melalukan akuisisi data dengan baik. Setelah ponsel dalam keadaan *root*, kemudian memasang aplikasi WhatsApp dan melakukan pendaftaran akun yang akan dijadikan sebagai akun pelaku serta memasang aplikasi WPS Office (BETA) yang akan digunakan untuk membuat dokumen. Dari semua itu, dapat diketahui data awal informasi ponsel seperti yang tersaji pada Tabel 4.2

Tabel 4.2. Informasi Perangkat

Informasi Perangkat	
Nama Pemilik	Arvio Setyobudi
Nama Perangkat	Samsung Young 2 Duos
Model Perangkat	SM-G130H
Sistem Operasi	Android 4.4.2
Nomor IMEI	- 355971062066140 - 355972062066148
Jaringan	- Indosat Ooredoo
Informasi Tambahan	- Ponsel dalam keadaan tidak terkunci - Tidak terdapat memori eksternal pada ponsel - Ponsel berada dalam kondisi sudah di-*root*

4.1.2. Pembuatan Skenario

Sebelum analisis forensik pada Samsung Young 2 Duos, dilakukan pembuatan skenario yang bertujuan untuk menentukan data awal pada penelitian ini. Data yang disebut artefak (*artifacts*) merupakan data yang akan dibandingkan jumlah data awal dengan data akhir hasil analisis forensik. Data ini berasal dari aplikasi WhatsApp, yakni daftar kontak, riwayat panggilan, serta pesan baik yang berupa pesan teks, gambar, video, audio, dokumen, dan lokasi (GPS). Berikut merupakan skenario yang digunakan pada penelitian ini

1. Menyimpan nomor telepon;
2. Membuat dokumen di aplikasi pembuat dokumen;
3. Membuat audio di aplikasi perekam suara;
4. Membuat gambar dan video di aplikasi kamera.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

5. Mengirim pesan WhatsApp baik berupa teks, audio, gambar, video, dokumen, dan GPS;
6. Melakukan miss-call dan panggilan telepon melalui aplikasi WhatsApp;
7. Menghapus semua pesan WhatsApp baik berupa teks, audio, gambar, video, dokumen, dan GPS;
8. Menghapus semua dokumen di aplikasi pembuat dokumen;
9. Menghapus semua audio di aplikasi perekam suara;
10. Menghapus semua gambar dan video di galeri.
11. Menghapus semua riwayat miss-call dan panggilan telepon melalui aplikasi WhatsApp; serta
12. Menghapus semua kontak telepon;

Berdasarkan skenario yang telah dilakukan, berikut jumlah data awal dalam penelitian yang tersaji pada Tabel 4.3. Sedangkan untuk detail data terdapat pada LAMPIRAN 01.

Tabel 4.3. Jumlah Data Awal

Artefak (*Artifacts*)		**Jumlah Data Awal**
Artefak	Pesan WhatsApp	40
	Riwayat Panggilan WhatsApp	5
	Daftar Kontak WhatsApp	10
	Gambar WhatsApp	3
	Video WhatsApp	2
	Audio WhatsApp	2
	Dokumen WhatsApp	3
	Lokasi (GPS) WhatsApp	2

4.2. Analisis Forensik pada *Samsung Young* 2 *Duos*

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).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

4.2.1. *Preservation*

Pada tahap ini, Samsung Young 2 Duos diamankan dan dilakukan isolasi, dengan mematikan koneksi telekomunikasi (*airplane* mode) 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 4.1.

Gambar 4.1. Samsung Young 2 Duos Diamankan dan Diisolasi

Setelah Samsung Young 2 Duos diamankan dan diisolasi, kemudian dilakukan pembuatan berkas pengujian kasus. Berkas ini akan digunakan untuk mengetahui setiap proses pengujian pada tahapan *examination* & *analysis.* Berkas pengujian tersaji pada Tabel 4.4.

Tabel 4.4. Berkas Informasi Pengujian

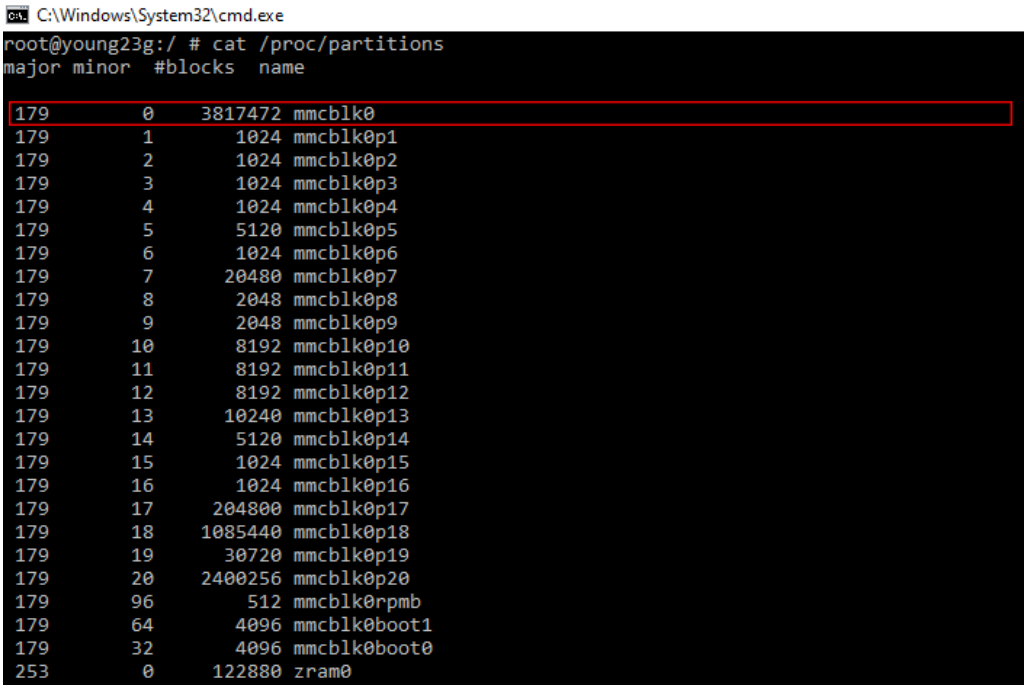
Berkas Pengujian Kasus	
Penguji	
Tanggal Pengujian	
Perangkat Pengujian	
Kode Pengujian	
Keterangan Pengujian	
Hasil Pengujian	
Status Pengujian	

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Adapun pada kolom “Penguji” akan diisi dengan nama penguji. Pada kolom “Tanggal Pengujian” akan diisi dengan tanggal dilakukannya pengujian. Pada kolom “Perangkat Pengujian” akan diisi dengan nama perangkat yang sedang diuji. Pada kolom “Kode Pengujian” akan diisi dengan kode pengujian, yakni kode pada parameter. Pada kolom “Keterangan Pengujian” akan diisi dengan keterangan dari setiap parameter yang digunakan. Pada kolom “Hasil Pengujian” akan diisi dengan hasil yang didapatkan dari pengujian yang telah dilakukan. Dan pada kolom “Status Pengujian” akan diisi dengan status antara berhasil, gagal atau telah selesai dilakukan.

4.2.2. *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 yang dapat dilihat pada Gambar 4.2.



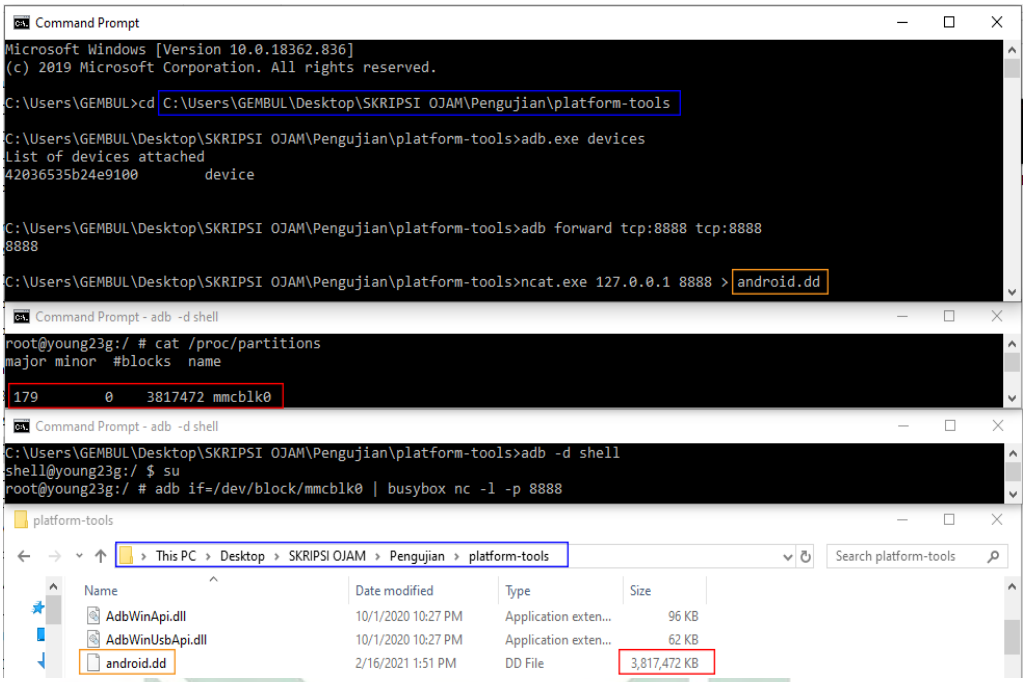
```
C:\Windows\System32\cmd.exe
root@young23g:/ # cat /proc/partitions
major minor  #blocks  name

179        0    3817472 mmcblk0
179        1       1024 mmcblk0p1
179        2       1024 mmcblk0p2
179        3       1024 mmcblk0p3
179        4       1024 mmcblk0p4
179        5       5120 mmcblk0p5
179        6       1024 mmcblk0p6
179        7      20480 mmcblk0p7
179        8       2048 mmcblk0p8
179        9       2048 mmcblk0p9
179       10       8192 mmcblk0p10
179       11       8192 mmcblk0p11
179       12       8192 mmcblk0p12
179       13      10240 mmcblk0p13
179       14       5120 mmcblk0p14
179       15       1024 mmcblk0p15
179       16       1024 mmcblk0p16
179       17     204800 mmcblk0p17
179       18    1085440 mmcblk0p18
179       19      30720 mmcblk0p19
179       20    2400256 mmcblk0p20
179       96        512 mmcblk0rpmb
179       64       4096 mmcblk0boot1
179       32       4096 mmcblk0boot0
253        0     122880 zram0
```

Gambar 4.2. Detail Informasi Memori Samsung Young 2 Duos

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Berdasarkan Gambar 4.1 diketahui bahwa memori internal pada Samsung Young 2 Duos terbagi atas beberapa partisi memori. Akan tetapi ukuran total dari semua partisi memori tersebut teletak pada *mmcblk0*, yakni sebesar 3.817.472 KB. Sehingga ukuran data hasil akuisisi memori dari Samsung Young 2 Duos harus sama, yakni sebesar 3.817.472 KB. Proses akuisisi serta direktori dan data hasil akuisisi dapat dilihat pada Gambar 4.3.



Gambar 4.3. Direktori dan Data Hasil Akuisisi

Dari Gambar 4.3. dapat disimpulkan bahwa proses akuisisi data pada Samsung Young 2 Duos berhasil, karena

1. Direktori data hasil akusisi sama, yakni terletak pada *Desktop\SKRIPSI OJAM\Pengujian\platform-tools*;
2. Nama serta ekstensi file data hasil akuisisi sama, yakni *android.dd*; dan
3. Ukuran data hasil akusisi sama dengan informasi ukuran data pada memori internal Samsung Young 2 Duos, yakni *3.817.472 KB.*

4.2.3. *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

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

1. Kinerja setiap aplikasi forensik;

Kinerja aplikasi forensik pemeriksaan dan analisisnya berdasarkan parameter yang digunakan. Parameter tersebut berasal dari buku panduan National Institute of Standards and Technology (NIST), yakni *Mobile Device Tool Specification* (2016) dan *Mobile Device Tool Test Assertions and Test Plan* (2016).

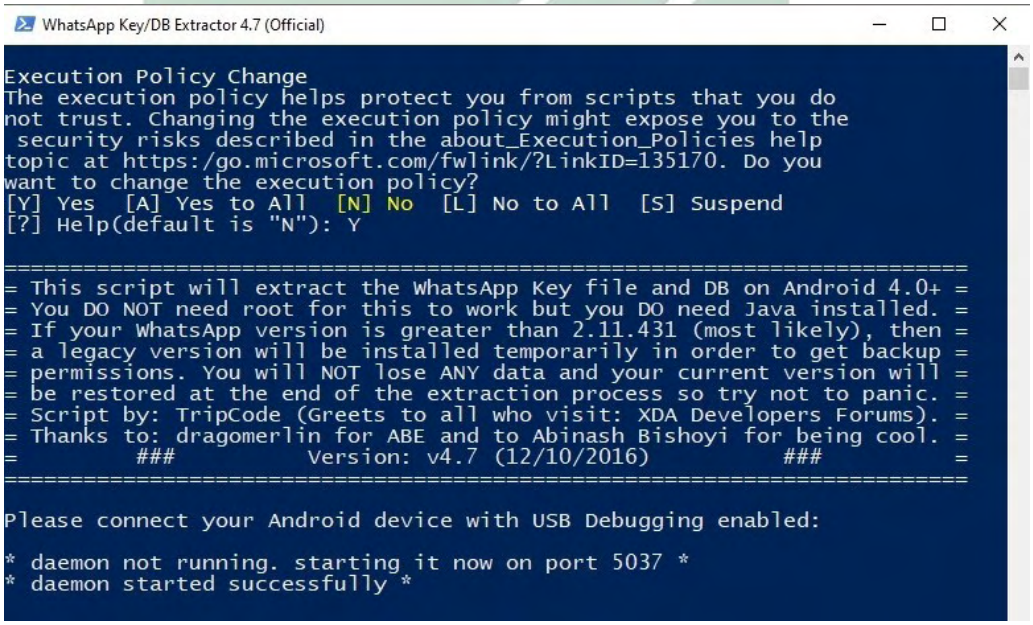
2. Data yang ditemukan, baik jenis data maupun jumlah data.

Data yang ditemukan, baik itu jenis data maupun jumlah data merupakan hasil pencarian data pada aplikasi WhatsApp yang digunakan sebelumnya dan data tersebut telah dihapus.

3. Data ditemukan yang dapat dibuka.

Data yang dapat dibuka merupakan data pada aplikasi WhatsApp yang sudah ditemukan, dan data tersebut tidak mengalami kerusakan saat dibuka, seperti kehilangan teks, gambar rusak, atau hal lainnya yang mempengaruhi sehingga isi dari data tersebut tidak dapat dilihat utuh.

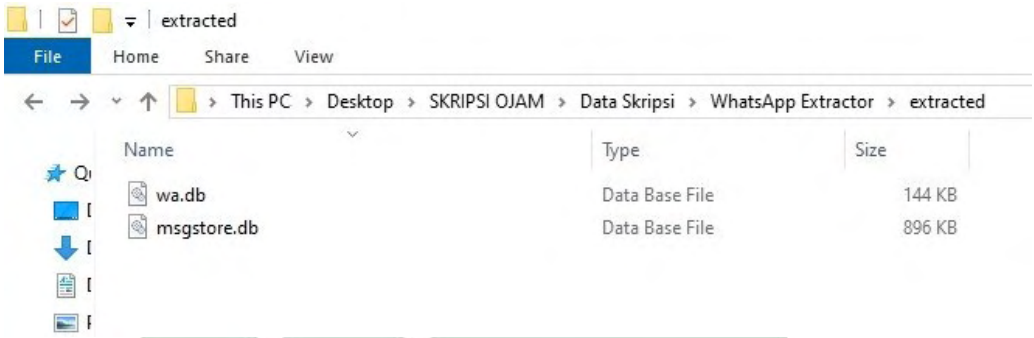
WhatsApp Key/DB Extractor aplikasi pertama yang digunakan untuk melakukan pemeriksaan dan analisis pada Samsung Young 2 Duos. Berikut tampilan awal WhatsApp Key/DB Extractor yang terdapat pada Gambar 4.4.



Gambar 4.4. Tampilan Awal WhatsApp Key/DB Extractor

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

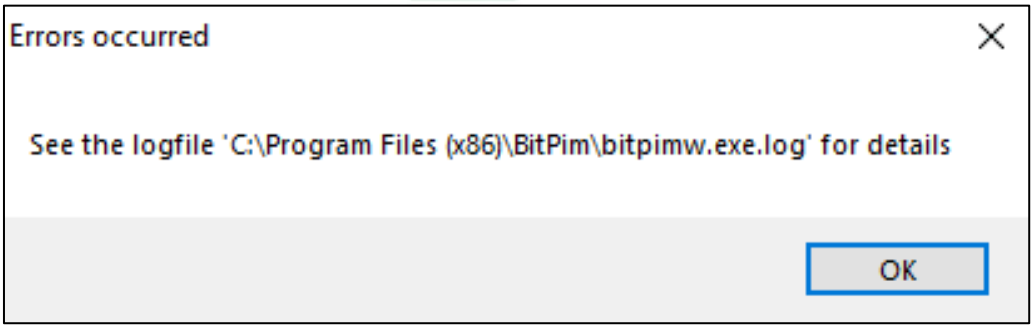
WhatsApp Key/DB Extractor merupakan aplikasi yang melakukan akuisisi langsung terhadap perangkat, data hasil akuisisi merupakan *database file* yang terletak pada direktori *C:\Users\GEMBUL\Desktop\SKRIPSI OJAM\Data Skripsi\WhatsApp Extractor\extracted* seperti yang terdapat pada Gambar 4.5.



Gambar 4.5. Hasil Akuisisi WhatsApp Key/DB Extractor

Karena 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++.

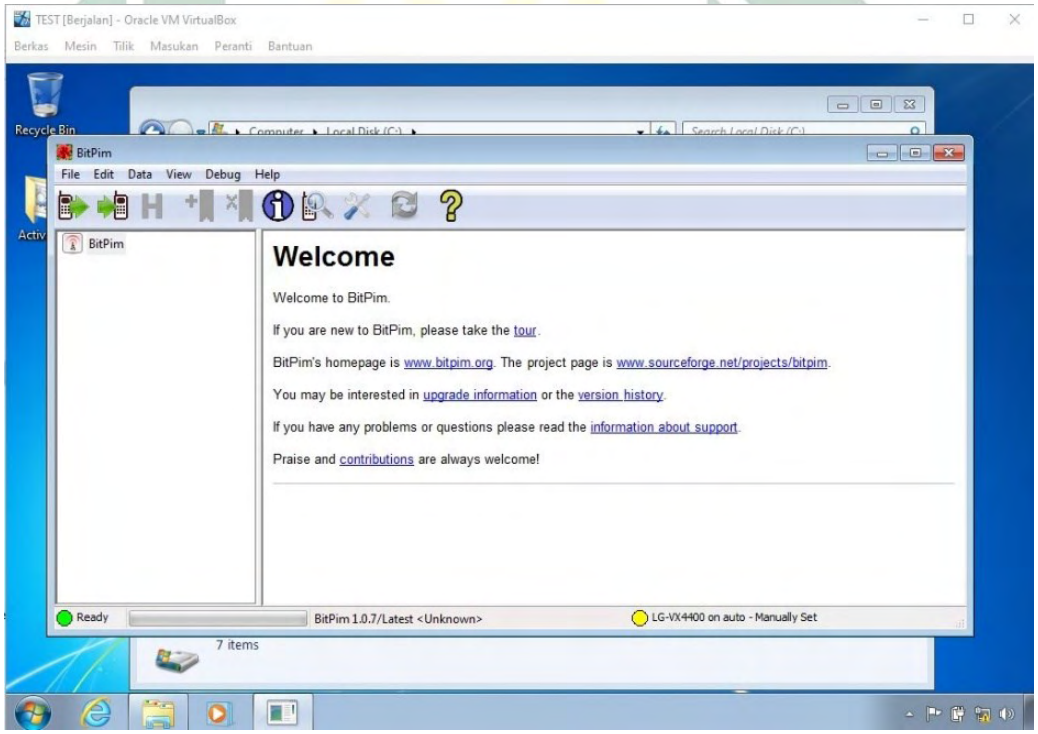
Setelah selesai melakukan pemeriksaan dan analisis data dari WhatsApp Key/DB Extractor menggunakan WhatsApp Viewer dan Notepad++, kemudian dilanjutkan melakukan pemeriksaan dan analisis data menggunakan aplikasi BitPim. Akan tetapi, saat aplikasi BitPim dijalankan, muncul notifikasi eror, seperti yang terlihat pada Gambar 4.6.



Gambar 4.6. Tampilan Eror Aplikasi BitPim

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Saat melihat isi dari *logfile* yang terdapat pada direktori *C:\Program Files (x86)\BitPim\bitpimw.exe.log*, ternyata terdapat kesalahan pada saat memuat *specified module* yang menyebabkan BitPim gagal saat dijalankan. Demikian juga saat dilakukan pencarian informasi terkait pemecahan masalah ini di internet serta web dari BitPim, diketahui bahwa dukungan pengembang hanya sampai versi 1.0.7 yang dirilis pada Januari 2010, dan BitPim hanya dapat berjalan di Windows 7 ke bawah (Windows Vista, Windows XP dan Windows 98), sedangkan pengujian ini menggunakan Windows 10. Kemudian, untuk menyesuaikan dengan persyaratan sistem yang dibutuhkan oleh aplikasi BitPim agar dapat berjalan, maka dipasanglah Windows 7 Ultimate SP1 menggunakan Oracle VM VirtualBox. Setelah pemasangan Windows 7 Ultimate SP1 selesai, kemudian dipasanglah aplikasi BitPim. Dan aplikasi BitPim dapat berjalan di Windows 7 Ultimate SP1, berikut tampilan awal dari aplikasi BitPim seperti yang terdapat pada Gambar 4.7.



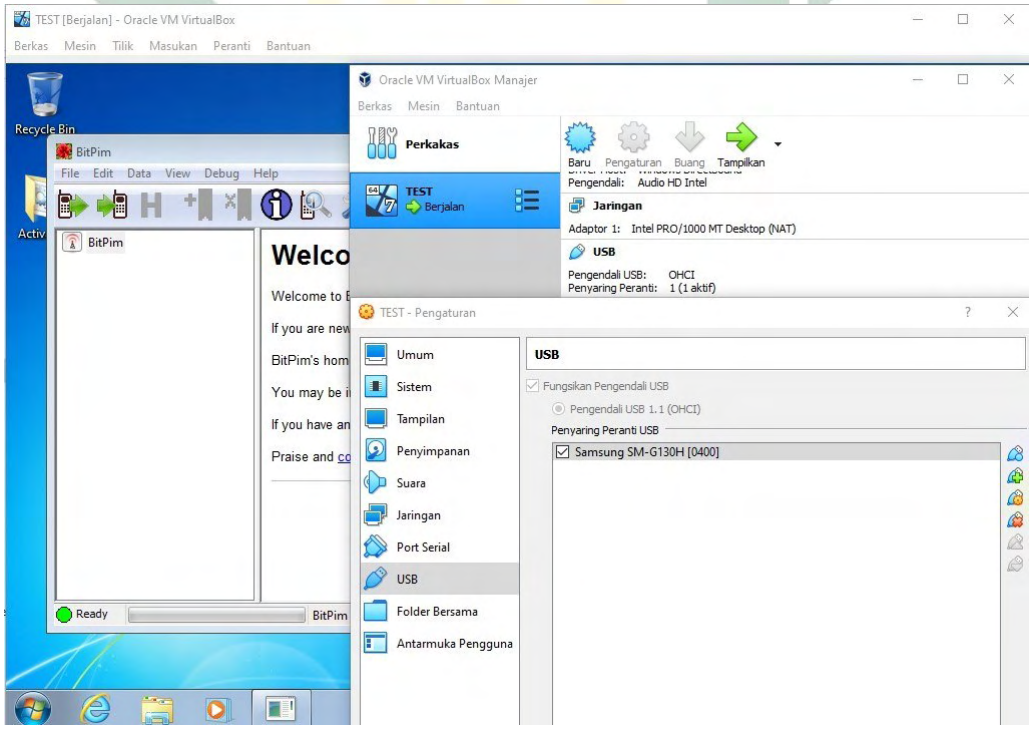
Gambar 4.7. Tampilan Awal BitPim

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Akan tetapi aplikasi BitPim gagal untuk mendeteksi Samsung Young 2 Duos, seperti yang terdapat pada Gambar 4.8.

Gambar 4.8. BitPim Gagal Mendeteksi Ponsel

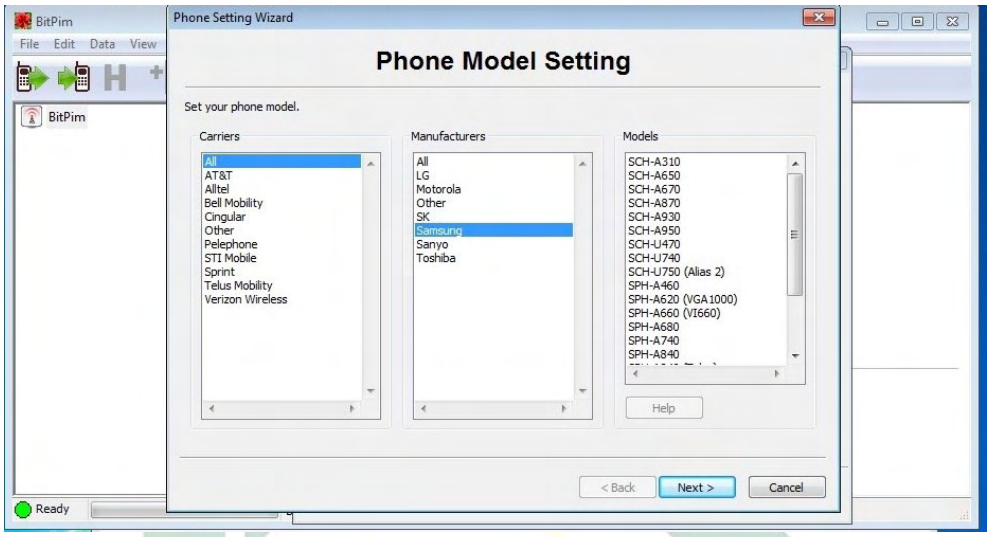
Meski Samsung Young 2 Duos sudah terhubung dengan Windows 7 Ultimate SP1 yang ada pada Oracle VM VirtualBox, seperti yang terdapat pada Gambar 4.9.



Gambar 4.9. Koneksi antara VirtualBox dengan Ponsel

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

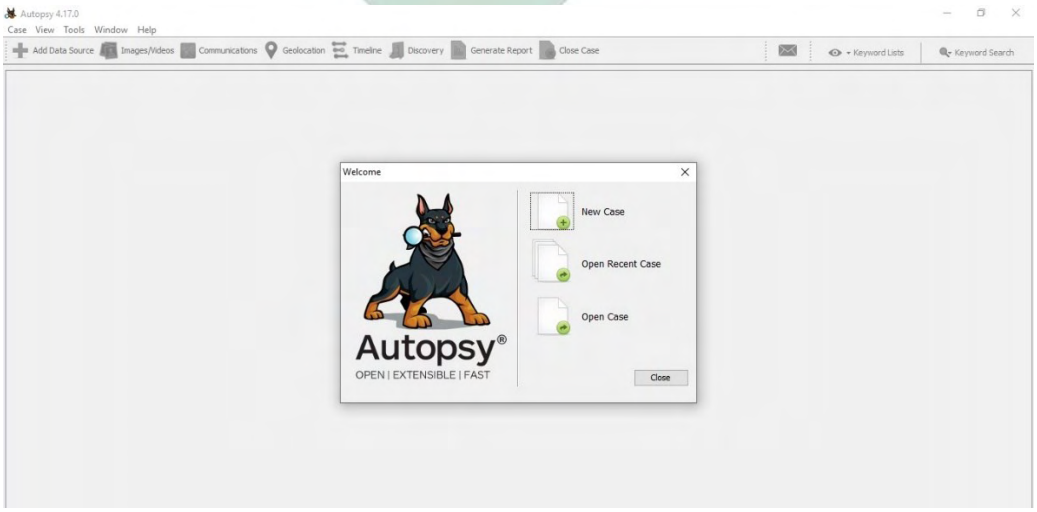
Demikian juga saat dilihat dukungan untuk model Samsung yang digunakan, yakni “SM-G130H”. Model tersebut tidak tersedia pada aplikasi BitPim, seperti yang terdapat pada Gambar 4.10.



Gambar 4.10. Dukungan BitPim untuk Model Ponsel

Karena tidak dapat mendeteksi ponsel, sehingga BitPim tidak dapat digunakan untuk melakukan pemeriksaan dan analisis terhadap Samsung Young 2 Duos, baik terhadap kinerja aplikasi maupun dalam mendapatkan bukti digital *–jenis data, jumlah data, serta data yang dapat dibuka–*.

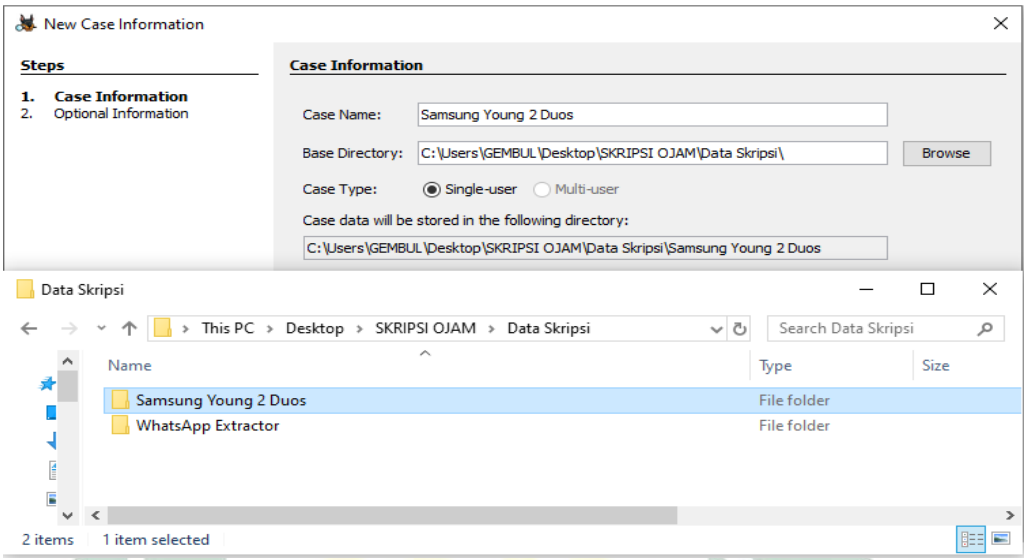
Kemudian dilakukan pemeriksaan dan analisis menggunakan aplikasi Autopsy. Berikut tampilan awal dari Autopsy sebelum melakukan pemeriksaan dan analisis pada Samsung Young 2 Duos yang terdapat pada Gambar 4.11.



Gambar 4.11. Tampilan Awal Autopsy

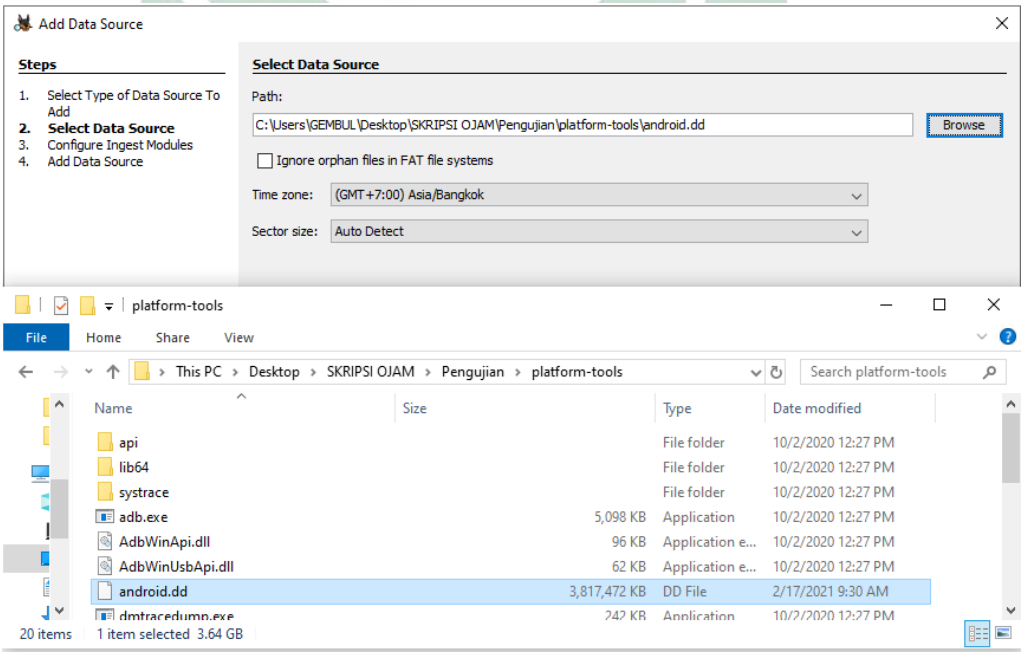
digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Setelah itu, memilih "*New Case*" untuk melakukan penanganan pada kasus baru, yang kemudian informasi kasus baru tersebut akan disimpan dan diletakan pada direktori *C:\Users\GEMBUL\Desktop\SKRIPSI OJAM\Data Skripsi,* seperti yang terdapat pada Gambar 4.12.



Gambar 4.12. Direktori Penyimpanan Informasi Kasus

Kemudian *image disk* hasil akuisisi dari SDK Platform Tools dan Ncat Platform, yakni *android.dd* dipilih sebagai data yang akan diperiksa dan dianalisis, seperti yang terdapat pada Gambar 4.13.



Gambar 4.13. Memilih Data Hasil Akusisi untuk Diekstraksi

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Setelah data hasil akuisisi selesai diekstraksi, dilakukan pemeriksaan dan analisis terhadap data tersebut menggunakan Autopsy. Dengan begitu, aplikasi forensik yang digunakan untuk melakukan pemeriksaan dan analisis pada penelitian ini hanya WhatsApp Key/DB Extractor dan Autopsy, sedangkan BitPim tidak dapat digunakan. Terkait BitPim yang tidak digunakan untuk melakukan pemeriksaan dan analisis pada penelitian ini, karena dukungan dari pengembang BitPim hanya terbatas sampai versi 1.0.7 yang dirilis pada Januari 2010, dan aplikasi tersebut hanya dapat berjalan di sistem operasi Windows 7 ke bawah (Windows Vista, Windows XP dan Windows 98). BitPim juga telah memiliki daftar untuk setiap model ponsel yang dapat digunakan untuk melakukan pemeriksaan dan analisis, sedangkan model ponsel yang digunakan dalam pengujian ini tidak tersedia. Hal tersebut membuat ponsel yang digunakan dalam pengujian tidak dapat terdeteksi oleh BitPim, sehingga data yang ingin didapatkan kemudian diperiksa dan dianalisis menggunakan aplikasi BitPim tidak dapat dilakukan.

Proses pengujian menggunakan aplikasi WhatsApp Key/DB Extractor secara keseluruhan serta contoh bukti hasil pengujian terdapat pada LAMPIRAN 02, sedangkan untuk proses pengujian menggunakan aplikasi Autopsy secara keseluruhan serta contoh bukti hasil pengujian terdapat pada LAMPIRAN 03. Dan berikut merupakan hasil pemeriksaan dan analisis terkait kinerja aplikasi setiap aplikasi forensik serta bukti digital yang ditemukan baik jenis data, jumlah data, dan data yang dapat dibuka.

1. Kinerja Setiap Aplikasi Forensik

Pemeriksaan dan analisis kinerja aplikasi forensik ini berfokus pada parameter *core assertions* dan *optional requirement assertions* yang digunakan. Hasil dari pemeriksaan dan analisis kinerja aplikasi WhatsApp Key/DB Extractor berdasarkan parameter NIST tersaji pada Tabel 4.5, sedangkan hasil pemeriksaan dan analisis kinerja aplikasi Autopsy berdasarkan parameter NIST tersaji pada Tabel 4.6.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Tabel 4.5. Hasil Kinerja WhatsApp Key/DB Extractor

Berkas Pengujian Kasus	
Penguji	M. Machrush Aliy Sirojjam Mushlich
Tanggal Pengujian	21 Februari 2021
Perangkat Pengujian	Samsung Young 2 Duos
Kode Pengujian	***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-CR-01 MDT-CR-02 MDT-CR-03
Keterangan Pengujian	***Core Assertions*** MDT-CA-01 Jika aplikasi forensik perangkat seluler menyediakan opsi akuisisi objek data "Dapatkan Semua" kepada pengguna, maka alat tersebut harus menyelesaikan akuisisi logis dari semua objek data tanpa kesalahan. MDT-CA-02 Jika aplikasi forensik perangkat seluler menyediakan objek data individual "Pilih Semua" kepada pengguna, alat tersebut harus menyelesaikan akuisisi logis dari semua objek data yang dipilih secara individual tanpa kesalahan. MDT-CA-03 Jika aplikasi forensik perangkat seluler memberi pengguna kemampuan untuk "Pilih Individu" objek data untuk akuisisi, maka alat tersebut harus menyelesaikan akuisisi logis untuk setiap objek data eksklusif tanpa kesalahan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Core Assertions*** MDT-CA-04 Jika konektivitas antara perangkat seluler dan alat forensik terganggu untuk akuisisi logis/sistem file, maka alat tersebut akan memberi tahu pengguna bahwa konektivitas telah terganggu. MDT-CA-05 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka alat tersebut harus memiliki kemampuan untuk menyajikan objek data yang diperoleh dalam format yang dapat digunakan baik melalui panel pratinjau atau laporan yang dihasilkan. MDT-CA-06 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka alat tersebut harus memiliki kemampuan untuk menyajikan informasi terkait pelanggan atau peralatan (misalnya, IMSI, IMEI, MEID / ESN, MSISDN) dalam format yang dapat digunakan. MDT-CA-07 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka semua elemen data yang didukung: data PIM, daftar kontak, SMS, MMS, riwayat panggilan, file yang berdiri sendiri (audio, gambar, video), aplikasi, media sosial atau data internet (bookmark, riwayat penelusuran), data email atau GPS harus disajikan dalam format yang dapat digunakan. MDT-CA-08 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, data yang diperoleh berisi karakter non-latin harus disajikan dalam format aslinya. MDT-CA-09 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, nilai hash dilaporkan untuk objek data yang diperoleh atau file kasus keseluruhan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Optional Requirement Assertions*** MDT-CR-01 Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk mengenali perangkat yang didukung melalui antarmuka yang disarankan (misalnya, kabel, Bluetooth). MDT-CR-02 Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk memberi tahu pengguna tentang kesalahan konektivitas antara perangkat dan aplikasi selama ekstraksi data. MDT-CR-03 Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk melakukan ekstraksi data logis dari objek data yang didukung tanpa modifikasi.
Hasil Pengujian	***Core Assertions*** MDT-CA-01 Aplikasi forensik tidak menyediakan opsi akuisisi objek data "dapatkan semua". MDT-CA-02 Aplikasi forensik tidak menyediakan opsi akuisisi objek data individual "dapatkan semua". MDT-CA-03 Aplikasi forensik tidak menyediakan opsi akuisisi objek data individual "Pilih Individu". MDT-CA-04 Aplikasi forensik memberitahu pengguna tentang kesalahan konektivitas perangkat. MDT-CA-05 Aplikasi forensik tidak dapat menyajikan objek data dalam bentuk laporan atau pertinjauan. MDT-CA-06 Aplikasi forensik tidak dapat menyajikan informasi pelanggan. MDT-CA-07 Aplikasi forensik dapat menyajikan hasil akuisisi dengan format yang dapat digunakan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Hasil Pengujian	***Core Assertions*** MDT-CA-08 Aplikasi forensik tidak dapat menyajikan karakter non-latin. MDT-CA-09 Aplikasi forensik tidak dapat menampilkan nilai *hash* setelah akuisisi objek data. ***Optional Requirement Assertions*** MDT-CR-01 Aplikasi forensik dapat mengenali perangkat yang didukung. MDT-CR-02 Aplikasi forensik memberitahu pengguna tentang kesalahan konektivitas perangkat. MDT-CR-03 Aplikasi forensik dapat melakukan ekstraksi objek data
Status Pengujian	***Core Assertions*** MDT-CA-01 – GAGAL MDT-CA-02 – GAGAL MDT-CA-03 – GAGAL MDT-CA-04 – BERHASIL MDT-CA-05 – GAGAL MDT-CA-06 – GAGAL MDT-CA-07 – BERHASIL MDT-CA-08 – GAGAL MDT-CA-09 – GAGAL ***Optional Requirement Assertions*** MDT-CR-01 – BERHASIL MDT-CR-02 – BERHASIL MDT-CR-03 – BERHASIL

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Tabel 4.6. Hasil Kinerja Autopsy

Berkas Pengujian Kasus	
Penguji	M. Machrush Aliy Sirojjam Mushlich
Tanggal Pengujian	21 Februari 2021
Perangkat Pengujian	Samsung Young 2 Duos
Kode Pengujian	***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-CR-01 MDT-CR-02 MDT-CR-03
Keterangan Pengujian	***Core Assertions*** MDT-CA-01 Jika aplikasi forensik perangkat seluler menyediakan opsi akuisisi objek data "Dapatkan Semua" kepada pengguna, maka alat tersebut harus menyelesaikan akuisisi logis dari semua objek data tanpa kesalahan. MDT-CA-02 Jika aplikasi forensik perangkat seluler menyediakan objek data individual "Pilih Semua" kepada pengguna, alat tersebut harus menyelesaikan akuisisi logis dari semua objek data yang dipilih secara individual tanpa kesalahan. MDT-CA-03 Jika aplikasi forensik perangkat seluler memberi pengguna kemampuan untuk "Pilih Individu" objek data untuk akuisisi, maka alat tersebut harus menyelesaikan akuisisi logis untuk setiap objek data eksklusif tanpa kesalahan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Core Assertions*** MDT-CA-04 Jika konektivitas antara perangkat seluler dan alat forensik terganggu untuk akuisisi logis/sistem file, maka alat tersebut akan memberi tahu pengguna bahwa konektivitas telah terganggu. MDT-CA-05 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka alat tersebut harus memiliki kemampuan untuk menyajikan objek data yang diperoleh dalam format yang dapat digunakan baik melalui panel pratinjau atau laporan yang dihasilkan. MDT-CA-07 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, maka semua elemen data yang didukung: data PIM, daftar kontak, SMS, MMS, riwayat panggilan, file yang berdiri sendiri (audio, gambar, video), aplikasi, media sosial atau data internet (bookmark, riwayat penelusuran), data email atau GPS harus disajikan dalam format yang dapat digunakan. MDT-CA-08 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, data yang diperoleh berisi karakter non-latin harus disajikan dalam format aslinya. MDT-CA-09 Jika aplikasi forensik perangkat seluler menyelesaikan akuisisi logis dari perangkat target tanpa kesalahan, nilai hash dilaporkan untuk objek data yang diperoleh atau file kasus keseluruhan. ***Optional Requirement Assertions*** MDT-CR-01 Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk mengenali perangkat yang didukung melalui antarmuka yang disarankan (misalnya, kabel, Bluetooth).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Optional Requirement Assertions*** MDT-CR-02 Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk memberi tahu pengguna tentang kesalahan konektivitas antara perangkat dan aplikasi selama ekstraksi data. MDT-CR-03 Aplikasi forensik perangkat seluler harus memiliki kemampuan untuk melakukan ekstraksi data logis dari objek data yang didukung tanpa modifikasi.
Hasil Pengujian	***Core Assertions*** MDT-CA-01 Aplikasi forensik tidak menyediakan opsi akuisisi objek data "dapatkan semua". MDT-CA-02 Aplikasi forensik tidak menyediakan opsi akuisisi objek data individual "dapatkan semua". MDT-CA-03 Aplikasi forensik tidak menyediakan opsi akuisisi objek data individual "Pilih Individu". MDT-CA-04 Aplikasi forensik tidak melakukan akuisisi sehingga tidak menampilkan kesalahan konektivitas. MDT-CA-05 Aplikasi forensik dapat menyajikan objek data dalam bentuk laporan atau pertinjauan. MDT-CA-06 Aplikasi forensik dapat menyajikan informasi pelanggan. MDT-CA-07 Aplikasi forensik dapat menyajikan hasil akuisisi dengan format yang dapat digunakan. MDT-CA-08 Aplikasi forensik dapat menyajikan karakter non-latin.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Hasil Pengujian	***Core Assertions*** MDT-CA-09 Aplikasi forensik dapat menampilkan nilai *hash* setelah akuisisi objek data. ***Optional Requirement Assertions*** MDT-CR-01 Aplikasi forensik tidak dapat mengenali perangkat yang didukung. MDT-CR-02 Aplikasi forensik tidak melakukan akuisisi sehingga tidak menampilkan kesalahan konektivitas. MDT-CR-03 Aplikasi forensik dapat melakukan ekstraksi objek data.
Status Pengujian	***Core Assertions*** MDT-CA-01 – GAGAL MDT-CA-02 – GAGAL MDT-CA-03 – GAGAL MDT-CA-04 – GAGAL MDT-CA-05 – BERHASIL MDT-CA-06 – BERHASIL MDT-CA-07 – BERHASIL MDT-CA-08 – BERHASIL MDT-CA-09 – BERHASIL ***Optional Requirement Assertions*** MDT-CR-01 – GAGAL MDT-CR-02 – GAGAL MDT-CR-03 – BERHASIL

2. Data yang Ditemukan, Baik Jenis Data maupun Jumlah Data

Pemeriksaan dan analisis terhadap data yang ditemukan ini berfokus pada data aplikasi WhatsApp, karena data ini yang menjadi fokus penelitian. Penelitian ini untuk menemukan jenis data maupun jumlah data. Hasil dari pemeriksaan dan analisis menggunakan WhatsApp Key/DB Extractor tersaji

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

pada Tabel 4.7, sedangkan hasil dari pemeriksaan dan analisis menggunakan Autopsy tersaji pada Tabel 4.8.

Tabel 4.7. Data Ditemukan oleh WhatsApp Key/DB Extractor

Berkas Pengujian Kasus	
Penguji	M. Machrush Aliy Sirojjam Mushlich
Tanggal Pengujian	21 Februari 2021
Perangkat Pengujian	Samsung Young 2 Duos
Kode Pengujian	***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
Keterangan Pengujian	***Artifacts*** WA-AO-01 Pesan teks yang dikirim melalui aplikasi WhatsApp. WA-AO-02 Riwayat panggilan yang dilakukan melalui aplikasi WhatsApp, baik melaui audio-call atau video-call. WA-AO-03 Daftar kontak atau nomor telepon yang tersimpan ataupun yang tidak disimpan pada aplikasi WhatsApp. WA-AO-04 Gambar yang berada pada aplikasi WhatsApp hasil dari mengirim pesan gambar atau menerima pesan gambar. WA-AO-05 Video yang berada pada aplikasi WhatsApp hasil dari mengirim pesan video atau menerima pesan video.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Artifacts*** WA-AO-06 Audio yang berada pada aplikasi WhatsApp hasil dari mengirim pesan atau menerima pesan suara, lagu atau jenis audio lainnya. WA-AO-07 Pesan yang berupa data atau dokumen yang bersifat tertulis pada aplikasi WhatsApp yang tersaji dalam ekstensi .doc, .xls, .pdf atau yang sejajar. WA-AO-08 Pesan yang berupa kiriman lokasi pada aplikasi WhatsApp.
Hasil Pengujian	***Artifacts*** WA-AO-01 Pesan WhatsApp yang berupa teks ditemukan. Dari empat-puluh (40) data pesan teks, semua data ditemukan. WA-AO-02 Riwayat panggilan WhatsApp tidak ditemukan. WA-AO-03 Data yang berupa daftar kontak ditemukan. Dari sepuluh (10) daftar kontak WhatsApp, semua data kontak ditemukan. WA-AO-04 Pesan WhatsApp yang berupa gambar tidak ditemukan. WA-AO-05 Pesan WhatsApp yang berupa video tidak ditemukan. WA-AO-06 Pesan WhatsApp yang berupa audio tidak ditemukan. WA-AO-07 Pesan WhatsApp yang berupa dokumen tidak ditemukan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
	Artifacts WA-AO-08 Pesan WhatsApp yang berupa GPS tidak ditemukan.
Status Pengujian	***Artifacts*** WA-AO-01 – BERHASIL WA-AO-02 – GAGAL WA-AO-03 – BERHASIL WA-AO-04 – GAGAL WA-AO-05 – GAGAL WA-AO-06 – GAGAL WA-AO-07 – GAGAL WA-AO-08 – GAGAL

Tabel 4.8. Data Ditemukan oleh Autopsy

Berkas Pengujian Kasus	
Penguji	M. Machrush Aliy Sirojjam Mushlich
Tanggal Pengujian	21 Februari 2021
Perangkat Pengujian	Samsung Young 2 Duos
Kode Pengujian	***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
Keterangan Pengujian	***Artifacts*** WA-AO-01 Pesan teks yang dikirim melalui aplikasi WhatsApp.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Artifacts*** WA-AO-02 Riwayat panggilan yang dilakukan melalui aplikasi WhatsApp, baik melaui audio-call atau video-call. WA-AO-03 Daftar kontak atau nomor telepon yang tersimpan ataupun yang tidak disimpan pada aplikasi WhatsApp. WA-AO-04 Gambar yang berada pada aplikasi WhatsApp hasil dari mengirim pesan gambar atau menerima pesan gambar. WA-AO-05 Video yang berada pada aplikasi WhatsApp hasil dari mengirim pesan video atau menerima pesan video. WA-AO-06 Audio yang berada pada aplikasi WhatsApp hasil dari mengirim pesan atau menerima pesan suara, lagu atau jenis audio lainnya. WA-AO-07 Pesan yang berupa data atau dokumen yang bersifat tertulis pada aplikasi WhatsApp yang tersaji dalam ekstensi .doc, .xls, .pdf atau yang sejajar. WA-AO-08 Pesan yang berupa kiriman lokasi pada aplikasi WhatsApp.
Hasil Pengujian	***Artifacts*** WA-AO-01 Pesan WhatsApp yang berupa teks ditemukan. Dari empat-puluh (40) data pesan teks, semuanya ditemukan. WA-AO-02 Data yang berupa riwayat panggilan ditemukan. Dari lima (5) riwayat panggilan dilakukan, semua data riwayat panggilan ditemukan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Hasil Pengujian	***Artifacts*** WA-AO-03 Data yang berupa daftar kontak ditemukan. Dari sepuluh (10) daftar kontak WhatsApp, semua data kontak ditemukan. WA-AO-04 Pesan WhatsApp yang berupa gambar ditemukan. Dari tiga (3) data pesan gambar hanya dua (2) data ditemukan. WA-AO-05 Pesan WhatsApp yang berupa video ditemukan. Dari dua (2) data pesan video, semua data ditemukan. WA-AO-06 Pesan WhatsApp yang berupa audio ditemukan. Dari dua (2) data pesan, semua data ditemukan. WA-AO-07 Pesan WhatsApp yang berupa dokumen ditemukan. Dari tiga (3) data pesan WhatsApp yang berupa dokumen, semua data ditemukan. WA-AO-08 Pesan WhatsApp yang berupa GPS tidak ditemukan
Status Pengujian	***Artifacts*** WA-AO-01 – BERHASIL WA-AO-02 – BERHASIL WA-AO-03 – BERHASIL WA-AO-04 – BERHASIL WA-AO-05 – BERHASIL WA-AO-06 – BERHASIL WA-AO-07 – BERHASIL WA-AO-08 – GAGAL

3. Data ditemukan yang Dapat Dibuka.

Pemeriksaan dan analisis terhadap data yang dapat dibuka ini berfokus pada data aplikasi WhatsApp yang sudah ditemukan, sehingga data yang hasil pengujiannya “GAGAL” pada tahap pemeriksaan “Data Ditemukan”

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

akan dihilangkan dalam prosesnya saja, sedangkan pelaporannya tetap secara keseluruhan. Data yang diperiksa dan dianalisis pada tahap ini berfokus pada data yang tidak mengalami kerusakan saat dibuka, sehingga isi dari data tersebut dapat dilihat utuh. Hasil dari pemeriksaan dan analisis menggunakan WhatsApp Key/DB Extractor terhadap data ditemukan yang dapat dibuka tersaji pada Tabel 4.9, sedangkan hasil dari pemeriksaan dan analisis menggunakan Autopsy terhadap data ditemukan yang dapat dibuka tersaji pada Tabel 4.10.

Tabel 4.9. Data Dapat Dibuka oleh WhatsApp Key/DB Extractor

Berkas Pengujian Kasus	
Penguji	M. Machrush Aliy Sirojjam Mushlich
Tanggal Pengujian	21 Februari 2021
Perangkat Pengujian	Samsung Young 2 Duos
Kode Pengujian	***Artifacts*** WA-AO-01 WA-AO-03
Keterangan Pengujian	***Artifacts*** WA-AO-01 Pesan teks yang dikirim melalui aplikasi WhatsApp. WA-AO-03 Daftar kontak atau nomor telepon yang tersimpan ataupun yang tidak disimpan pada aplikasi WhatsApp.
Hasil Pengujian	***Artifacts*** WA-AO-01 Dari empat-puluh (40) data pesan WhatsApp berupa teks ditemukan, tetapi hanya satu (1) data yang dapat dilihat. WA-AO-03 Dari sepuluh (10) data daftar kontak WhatsApp ditemukan, semua data dapat dibuka.
Status Pengujian	Pengujian telah selesai dilakukan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Tabel 4.10. Data Dapat Dibuka oleh Autopsy

Berkas Pengujian Kasus	
Penguji	M. Machrush Aliy Sirojjam Mushlich
Tanggal Pengujian	21 Februari 2021
Perangkat Pengujian	Samsung Young 2 Duos
Kode Pengujian	***Artifacts*** WA-AO-01 WA-AO-02 WA-AO-03 WA-AO-04 WA-AO-05 WA-AO-06 WA-AO-07
Keterangan Pengujian	***Artifacts*** WA-AO-01 Pesan teks yang dikirim melalui aplikasi WhatsApp. WA-AO-02 Riwayat panggilan yang dilakukan melalui aplikasi WhatsApp, baik melaui audio-call atau video-call. WA-AO-03 Daftar kontak atau nomor telepon yang tersimpan ataupun yang tidak disimpan pada aplikasi WhatsApp. WA-AO-04 Gambar yang berada pada aplikasi WhatsApp hasil dari mengirim pesan gambar atau menerima pesan gambar. WA-AO-05 Video yang berada pada aplikasi WhatsApp hasil dari mengirim pesan video atau menerima pesan video. WA-AO-06 Audio yang berada pada aplikasi WhatsApp hasil dari mengirim pesan atau menerima pesan suara, lagu atau jenis audio lainnya.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

Berkas Pengujian Kasus	
Keterangan Pengujian	***Artifacts*** WA-AO-07 Pesan yang berupa data atau dokumen yang bersifat tertulis pada aplikasi WhatsApp yang tersaji dalam ekstensi .doc, .xls, .pdf atau yang sejajar.
Hasil Pengujian	***Artifacts*** WA-AO-01 Dari empat-puluh (40) data pesan WhatsApp berupa teks ditemukan, hanya satu (1) data dapat dibuka. WA-AO-02 Dari lima (5) data riwayat panggilan WhatsApp ditemukan, semua data dapat dibuka. WA-AO-03 Dari sepuluh (10) data daftar kontak WhatsApp ditemukan, semua data dapat dibuka. WA-AO-04 Dari dua (2) data pesan WhatsApp berupa gambar ditemukan, semua data tidak dapat dibuka. WA-AO-05 Dari dua (2) data pesan WhatsApp berupa video ditemukan, semua data tidak dapat dibuka. WA-AO-06 Dari dua (2) data pesan WhatsApp berupa audio ditemukan, semua data tidak dapat dibuka. WA-AO-07 Dari tiga (3) data pesan WhatsApp berupa dokumen ditemukan, semua data dapat dibuka.
Status Pengujian	Pengujian telah selesai dilakukan.

4.2.4. *Reporting*

Pada tahap ini, hasil dari pemeriksaan dan analisis dilakukan pelaporan berdasarkan pengujian yang telah dilakukan secara keseluruhan seperti yang terdapat pada LAMPIRAN 02 untuk WhatsApp Key/DB Extractor dan LAMPIRAN 03 untuk Autopsy terkait.

1. Kinerja setiap aplikasi forensik;

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

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

3. Data ditemukan yang dapat dibuka.

Berikut laporan hasil pemeriksaan dan analisis dari pengujian aplikasi forensik yang tersaji pada Tabel 4.11.

Tabel 4.11. Perbandingan Kinerja Aplikasi Forensik

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**

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

(lanjutan)

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
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**

Dari tabel 4.11. dapat diketahui hasil pemeriksaan dan analisis dari setiap aplikasi forensik sebagai berikut.

1. Kinerja Setiap Aplikasi Forensik

Hasil pemeriksaan dan analisis kinerja aplikasi forensik terhadap WhatsApp Key/DB Extractor (*Proses pengujian dapat dilihat pada LAMPIRAN 02, sublampiran KINERJA APLIKASI*) dan Autopsy (*Proses pengujian dapat dilihat pada LAMPIRAN 03, sublampiran KINERJA*

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

APLIKASI). Diketahui bahwa dari dua-belas (12) parameter –*sembilan (9) dari core assertions dan tiga (3) dari optional requirement assertions*– yang digunakan untuk mengukur kinerja aplikasi forensik, WhatsApp Key/DB Extractor hanya memenuhi lima (5) parameter yang tetapkan; Autopsy memenuhi enam (6) parameter yang ditetapkan.

Dalam hal kinerja aplikasi forensik, Autopsy lebih unggul dari WhatApp Key/DB Extractor. Hal ini karena Autopsy mampu melakukan pemeriksaan dan analisis secara keseluruhan data hasil akuisisi dari ponsel yang digunakan, tetapi Autopsy selalu gagal pada parameter yang berkaitan dengan akuisisi, karena Autopsy tidak mempunyai fitur untuk melakukan akuisisi terhadap data ponsel; WhatsApp Key/DB Extractor hanya dapat melakukan akuisisi saja, sehingga beberapa parameter yang berkaitan dengan akuisisi mendapatkan status berhasil.

2. Data yang Ditemukan, Baik Jenis Data Maupun Jumlah Data

Hasil pemeriksaan dan analisis pada aplikasi WhatsApp Key/DB Extractor dan Autopsy dalam menemukan bukti digital, baik jenis data maupun jumlah data. Untuk proses pengujian WhatsApp Key/DB Extractor yang dapat dilihat pada LAMPIRAN 02, sublampiran DATA DITEMUKAN (JENIS, JUMLAH, DAN DATA DAPAT DIBUKA); Proses pengujian Autopsy yang dapat dilihat pada LAMPIRAN 03, sublampiran DATA DITEMUKAN (JENIS, JUMLAH, DAN DATA DAPAT DIBUKA). Dalam menemukan jenis data, WhatsApp Key/DB Extractor menemukan dua (2) dari delapan (8) jenis data yang digunakan; Autopsy menemukan tujuh (7) dari delapan (8) jenis data yang digunakan. Dalam hal menemukan jumlah data, WhatsApp Key/DB Extractor menemukan lima-puluh (50) dari enam-puluh-tujuh (67) data yang digunakan; Autopsy menemukan enam-puluh-empat (64) dari enam-puluh-tujuh (67) data yang digunakan.

Dalam hal mendapatkan bukti digital terkait data yang ditemukan, baik jenis data maupun jumlah data, Autopsy lebih unggul dari WhatApp Key/DB Extractor. Hal ini karena Autopsy mampu melakukan pemeriksaan dan analisis secara keseluruhan data hasil akuisisi dari ponsel yang digunakan,

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

sehingga Autopsy mampu mendapatkan seluruh data dari aplikasi WhatsApp; WhatsApp Key/DB Extractor hanya dapat melakukan akuisisi saja, pun besaran ukuran data hasil akuisisinya sangat kecil jika dibanding dengan data yang digunakan oleh Autopsy untuk melakukan pemeriksaan dan analisis. Sedangkan pemeriksaan dan analisis data hasil akuisisi dari WhatsApp Key/DB Extractor menggunakan aplikasi WhatsApp Viewer dan Notepad++. Saat dilakukan pemeriksaan dan analisis, data hasil akusisi dari WhatsApp Key/DB Extractor juga hanya sebatas pengembalian data berupa *database* yang berbasis teks yang berisikan daftar kontak, isi pesan serta *time-stamp*. Hal itulah yang menyebabkan WhatsApp Key/DB Extractor hanya mampu mendapatkan data yang berupa pesan teks WhastApp dan daftar kontaknya saja.

3. Data Ditemukan yang Dapat Dibuka

Hasil pemeriksaan dan analisis pada aplikasi WhatsApp Key/DB Extractor dan Autopsy dalam menemukan bukti digital yang dapat dibuka. WhatsApp Key/DB Extractor mampu menemukan lima-puluh (50) dari enam-puluh-tujuh (67) data yang digunakan. Akan tetapi WhatsApp Key/DB Extractor hanya mampu membuka sebelas (11) data dari lima-puluh (50) data yang ditemukan tersebut; Autopsy mampu menemukan enam-puluh-empat (64) dari enam-puluh-tujuh (67) data yang digunakan. Akan tetapi hanya mampu membuka sembilan-belas (19) data dari enam-puluh-empat (64) data yang ditemukan. Untuk contoh bukti dari data yang dapat dibuka pada WhatsApp Key/DB Extractor dapat dilihat pada LAMPIRAN 02, sublampiran DATA DITEMUKAN (JENIS, JUMLAH, DAN DATA DAPAT DIBUKA); Contoh bukti dari data yang dapat dibuka pada Autopsy dapat dilihat pada LAMPIRAN 03, sublampiran DATA DITEMUKAN (JENIS, JUMLAH, DAN DATA DAPAT DIBUKA).

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.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

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.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB V
PENUTUP

5.1. Simpulan

Simpulan 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.

5.2. Saran

Saran untuk perkembangan penelitian dengan fokus forensik perangkat seluler (*mobile forensic*) selanjutnya, yakni:

1. Gunakan berbagai jenis merek serta sistem operasi pada perangkat seluler lainnya, tidak hanya terpaku pada perangkat seluler yang berbasis sistem operasi Android.
2. Penggunaan alat atau aplikasi forensik yang tepat serta dukungan pengembang yang terus diperbarui juga mempengaruhi dalam hal mendapatkan data serta pemeriksaan dan analisis terhadap data, sehingga pemilihan aplikasi yang tepat memungkinkan untuk mendapatkan data sesuai dengan keinginan.
3. Gunakan media dari aplikasi selain WhatsApp untuk dijadikan sebagai barang bukti, karena setiap tahun pasti ada aplikasi baru yang digunakan untuk melakukan komunikasi atau sebagai media melakukan tindak kejahatan siber.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR PUSTAKA

Sumber Buku/Dokumen

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).

Casey, E. (2011). *Digital Evidence and Computer Crime.* Third Edition. Academic Press.

Ghosh, S., dan Turrini, E. (2010). *Cybercrimes: A Multidisciplinary Analysis.* Springer-Verlag Berlin Heidelberg.

Reiber, L. (2019). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. Second Edition. McGraw-Hill Education

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

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

Sumber Internet

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

___. (2019). The Smartphone Duopoly. http://statista.com/chart/3268/smartphone-os-market-share. 10 Oktober 2019.

Sumber Jurnal

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)*.

Albanna, F., dan Riadi, I. (2017). Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security*, 15(1): 173–178.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi,* 18(2): 185–95.

Chuzaimah., Mabruroh., dan Dihan, F. N. (2010). Smartphone: Antara Kebutuhan dan E-Lifestyle. *Seminar Nasional Informatika 2010,* 312–321.

Daeng, I. T. M., Mewengkang, N. N., dan Kalesaran, E. R. (2017). Penggunaan Smartphone dalam Menunjang Aktivitas Perkuliahan oleh Mahasiswa Fispol Unsrat Manado. *Acta Diurna*, 6(1): 1–15.

Handoko, C. (2016). Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan. *Jurisprudence*, 6(1): 1–15.

Kataren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, 5(2): 35–42.

Kumar, J. K., dan Yugandhar, D. (2017). A Study on Current Mobile Operating Systems. *International Journal of Scientific & Engineering Research,* 8(5): 72 –78.

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

Mulawarman., dan Nurfitri, A. D. (2017). Perilaku Pengguna Media Sosial beserta Implikasinya Ditinjau dari Perspektif Psikologi Sosial Terapan. *Buletin Psikologi,* 25(1): 36–44.

Penangsang, P., Studiviany, P., dan Wiwoho, B. (2020). Kajian Pengaruh COVID-19 Terhadap Stabilitas Ekonomi. *JEB17 (Jurnal Ekonomi & Bisnis),* 5(1): 1–15.

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

Rahadi, D. R. (2017). Perilaku Pengguna dan Informasi Hoax di Media Sosial. J*urnal Manajemen dan Kewirausahaan,* 5(1): 58–70.

Raharjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sosioteknologi,* 29: 384–387.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Riadi, I., Fadlil, A., dan Fauzan, A. (2018). A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger. *International Journal of Advanced Computer Science and Applications,* 9(10): 201–206.

____., Sunardi., dan Rauli, M. E. (2018). Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics. *Jurnal Teknik Elektro,* 10(1): 18–22.

____., Sunardi., dan Sahiruddin. (2020). Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 7(1): 197–204.

____., Yudhana, A., dan Putra, M. C. F. (2018). Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal of Informatics*, 5(2): 235–247.

Ruuhwan., Riadi, I., dan Prayudi Y. (2017). Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology. *International Journal of Electrical and Computer Engineering (IJECE)*, 7(5) 2806–2817.

Umar, R., Riadi, I., dan Maulana, G. (2017). A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. *International Journal of Advanced Computer Science and Applications,* 8(12): 69–75.

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

Yudhana, A., Riadi, I., dan Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode NIST. *IT Journal Research and Development,* 3(1): 13–21.

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

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Sumber Karya Akhir

Cahyanto, A. D. (2015). Analisa dan Evaluasi Kemampuan Tools untuk Forensik Smartphone Berbasis Android Studi Kasus: PUSLABFOR BARESKRIM MABES POLRI. *Karya Akhir.* Program Studi Megister Teknologi Informasi, Universitas Indonesia. Jakarta.

Sumber Undang-Undang

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008. *Informasi dan Transaksi Elektronik*. 21 April 2008. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Jakarta.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id