ANALISIS KINERJA AUTOPSY PADA SMARTPHONE BERBASIS ANDROID MENGGUNAKAN NIST MEASUREMENTS

SKRIPSI



Disusun Oleh:

ARSYIAN ALDI WARSITO H06216005

PROGRAM STUDI SISTEM INFORMASI FAKULTAS SAINS DAN TEKNOLOGI UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA 2020

LEMBAR PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini,

Nama

: Arsyian Aldi Warsito

NIM

: H06216005

Program Studi: Sistem Informasi

Angkatan

: 2016

Menyatakan bahwa saya tidak melakukan plagiasi dalam penulisan skripsi saya yang berjudul: "ANALISIS KINERJA AUTOPSY PADA SMARTPHONE BERBASIS ANDROID MENGGUNAKAN NIST MEASUREMENTS". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 05 Agustus 2020

Yang menyatakan,

(Arsyian Aldi Warsito)

NIM. H06216005

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA : ARSYIAN ALDI WARSITO

NIM : H06216005

JUDUL : ANALISIS KINERJA AUTOPSY PADA SMARTPHONE

BERBASIS ANDROID MENGGUNAKAN NIST

MEASUREMENTS

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 30 Juni 2020

Dosep Pembimbing 1

Muhammad Andik Izzudin, MT

NIP. 198403072014031001

/ / / /

Dosen Pembimbing 2

Faris Mushlihul Amin, M. Kom

NIP. 198800132014031001

PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi Arsyian Aldi Warsito ini telah dipertahankan Di depan tim penguji skripsi Di Surabaya, 30 Juni 2020

> Mengesahkan, Dewan Penguji

Muhammad Andik Izzudin, MT

NP. 198403072014031001

Penguji II

Faris Mushlihul Amia, M. Kom

NIP. 198800132014031001

Penguji III

Indri Sudanawati Rozas, M.Kom

NIP. 198207212014032001

Penguji IV

Nita Yalina. S.Kom. • M.MT

NIP. 198702082014032003

Mengetahui,

Plt. Dekan Fakultas Sains dan Teknologi

UIN Sunan Ampel Surabaya

Evi Fatimatur Rusydiyah. M.Ag

NIP 197312272005012003



KEMENTERIAN 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

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas ak saya:	ademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini,
Nama	: Arsyian Aldi Warsito
NIM	: H06216005
Fakultas/Jurusan	: Fakultas Sains dan Teknologi / Sistem Informasi
E-mail address	: arsyian.aldi@gmail.com / H06216005@uinsby.ac.id
UIN Sunan Ampel Skripsi yang berjudul: ANALISIS KINEI	gan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah: Tesis Desertasi Lain-lain () RJA AUTOPSY PADA SMARTPHONE BERBASIS ANDROID
MENGGUNAKA	N NIST MEASUREMENTS
Perpustakaan UIN mengelolanya da menampilkan/men kepentingan akade saya sebagai penul	yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, alam bentuk pangkalan data (database), mendistribusikannya, dan npublikasikannya di Internet atau media lain secara <i>fulltext</i> untuk emis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama is/pencipta dan atau penerbit yang bersangkutan.
	uk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN baya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta

Demikian pernyataan ini yang saya buat dengan sebenarnya.

dalam karya ilmiah saya ini.

Surabaya, 05 Agustus 2020

Penulis

(Arsyian Aldi Warsito) nama terang dan tanda tangan

ABSTRAK

ANALISIS KINERJA AUTOPSY PADA *SMARTPHONE* BERBASIS ANDROID MENGGUNAKAN NIST *MEASUREMENTS*

Oleh:

Arsyian Aldi Warsito

Perkembangan teknologi di dunia perangkat *mobile* semakin berkembang. Namun dari perkembangan tersebut memiliki dampak kerugian salah satunya adalah tindakan *cybercrime*. *Cybercrime* adalah tindak kejahatan yang menggunakan teknologi informasi, salah satunya adalah menggunakan perangkat mobile *android*. Pada penelitian ini menggunakan NIST *Measurements* sebagai acuan untuk kriteria alat forensik. Pada penelitian ini menggunakan aplikasi Autopsy untuk menganalisis data yang telah diakuisisi. Hasil dari 2 objek penelitian yang digunakan hasil presentase kinerja Autopsy mengembalikan dan memulihkan data Xiaomi Redmi Note 3 sebesar 31,16%, sedangkan Samsung Galaxy ACE sebesar 32,46%. Setelah melakukan digital forensik terdapat analisis kinerja dari aplikasi Autopsy menggunakan NIST *Measurements*. Hasil dari analisis menggunakan NIST *Measurement* bahwa aplikasi Autopsy pada Xiaomi Redmi Note 3 memenuhi 10 dari 28 standar pengukuran yang memiliki nilai prosentase 35,71% sedangkan pada Samsung Galaxy ACE 3 memenuhi 10 dari 28 standar pengukuran yang memiliki nilai prosentase 32,14%

Kata kunci: Android Smartphone, Autopsy, NIST Measurements

ABSTRACT

AUTOPSY PERFOMANCE ANALYSIS ON ANDROID SMARTPHONE USING NIST MEASUREMENTS

By:

Arsyian Aldi Warsito

The development of technology in the world of mobile devices is growing. These developments have detrimental impacts one of which is cybercrime action. Cybercrime is a crime that uses information technology, one of which is using an android mobile device. In this study NIST Measurements was used as a reference for forensic tool criteria. In this study using the Autopsy application to analyze the data that has been acquired. The results of the 2 research objects that are used are the percentage of Autopsy's performance to restore and recover Xiaomi Redmi Note 3 data is 31.16%, while the Samsung Galaxy ACE is 32.46%. After conducting digital forensics there is a performance analysis of the Autopsy application using NIST Measurements. The results of the analysis using NIST Measurement that the Autopsy application on the Xiaomi Redmi Note 3 meets 10 of the 28 measurement standards that have a percentage value of 35.71% while the Samsung Galaxy ACE 3 meets 10 of 28 measurement standards that have a percentage value of 32.14%

Keywords: Android Smartphone, Autopsy, NIST Measurements

DAFTAR ISI

PERNYATAAN KEASLIAN	j
PERSETUJUAN PEMBIMBING	ii
PENGESAHAN TIM PENGUJI SKRIPSI	ii
PERNYATAAN PERSTUJUAN PUBLIKASI	iv
ABSTRAK	v
ABSTRACT	v i
DAFTAR ISI	vi
DAFTAR TABEL	Х
DAFTAR GAMBAR	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masala <mark>h</mark>	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan Skripsi	3
BAB 2	
TINJAUAN PUSTAKA	5
2.1 Tinjauan Penelitian Terdahulu	5
2.2 Dasar Teori	6
2.2.1 Digital Forensik	<i>6</i>
2.2.2 Mobile Forensic	7
2.2.3 NIST Special Publication 800-101 Revision 1	8
2.2.4 Mobile Device Tool Classification System	16
2.2.5 NIST Measurements	18

	2.2.6	Smartphone	20
	2.2.7	WhatsApp Messenger	20
	2.2.8	Telegram	21
	2.2.9	Autopsy	21
	2.2.10	Magnet Acquire	21
	2.3	Integrasi Keilmuan	21
В	AB III		23
M	IETOI	OOLOGI PENELITIAN	23
	3.1	Perumusan Masalah	24
	3.2	Persiapan Penelitian	24
	3.2.1	Studi Literatur	24
	3.2.2	Menyusun Lembar Kerja	24
	3.2.3	Mempersiapkan Alat dan Bahan	24
	3.2.4	Penyusunan dan <mark>Im</mark> plementasi Skenario	26
	3.3	Analisis Digital Forensik Menggunakan NIST SP 800-101 R1	26
	3.3.1	Preservation	26
	3.3.2	Acquisition	27
	3.3.3	Examination dan Analysis	27
	3.3.4	Reporting	27
В	AB IV	•••••••••••••••••••••••••••••••••••••••	28
H	ASIL	DAN PEMBAHASAN	28
	4.1	Lembar Kerja Berdasarkan Framework NIST SP 800-101 R1	28
	4.1.1	Informasi Kasus	28
	4.1.2	Informasi Perangkat Seluler	29
	4.1.3	Laporan	30
	4.2	Skenario Sebelum Melakukan Digital Forensik	30

4.3	Implementasi Lembar Kerja Untuk Menganalisis Digital	Forensik33
4.3.1	Digital Forensik Xiaomi Redmi Note 3	33
4.3.2	Digital Forensik Samsung Galaxy ACE 3	46
4.4	Analisis Kinerja Aplikasi Autopsy Menggunakan NIST	Measurements 60
4.4.1	Xiaomi Redmi Note 3	60
4.4.2	Samsung Galaxy ACE 3	64
4.4.3	Perhitungan Angka Indeks	68
4.5	Perbandingan Bukti Digital	71
BAB V		75
KESIM	PULAN	75
5.1	Kesimpulan	75
5.2	Saran	75
DAFTA	AR PUSTAKA	76

DAFTAR TABEL

Tabel 2.1 Evidence Sources	7
Tabel 2.2 NIST Measurements	18
Tabel 3.1 Software forensik yang digunakan	25
Tabel 4.1 Informasi Kasus	_28
Tabel 4.2 Informasi Perangkat Seluler	29
Tabel 4.3 Laporan Digital Forensik	30
Tabel 4.4 Informasi Kasus Xiaomi Redmi Note 3	33
Tabel 4.5 Informasi Perangkat Seluler Xiaomi Redmi Note 3	35
Tabel 4.6 Informasi Perangkat Seluler Xiaomi Redmi Note 3	43
Tabel 4.7 Laporan Digital Forensik Xiaomi Redmi Note 3	44
Tabel 4.8 Informasi Kasus Samsung Galaxy ACE 3	46
Tabel 4.9 Informasi Perangkat Seluler Samsung Galaxy Ace 3	48
Tabel 4.10 Informasi Perangkat Seluler Samsung Galaxy ACE 3	57
Tabel 4.11 Laporan Digital Forensik Samsung Galaxy ACE 3	58
Tabel 4.12 Analisis Aplikas <mark>i A</mark> utopsy Menggunakan NIST Measurements	68
Tabel 4.13 Perbandingan Bukti Digital	72

DAFTAR GAMBAR

Gambar 2.1 NIST SP 800-101 R1 (Ayers et al., 2014)	8
Gambar 2.2 Generic On-Site Decision Tree	12
Gambar 2.3 Tool Classification System (Ayers et al., 2014)	17
Gambar 3.1 Alur Penelitian	23
Gambar 4.1 Screenshoot Percakapan Prostitusi Online WhatsApp	31
Gambar 4.2 Screenshoot Percakapan Pembunuhan Berencana Telegram	32
Gambar 4.3 Bukti Digital di Kedua Penyimpanan Smartphone	32
Gambar 4.4 Screenshoot Percakapan Menggunakan SMS	33
Gambar 4.5 Airplane Mode Pada Xiaomi Redmi Note 3	35
Gambar 4.6 Jumlah Partisi Penyimpanan Pada Xiaomi Redmi Note	37
Gambar 4.7 Hasil Akuisisi Dari Xiaomi Redmi Note 3	
Gambar 4.8 SMS yang Terhapus Pada Xiaomi Redmi Note 3	38
Gambar 4.9 Ditemukan Call Log yang Dihapus	
Gambar 4.10 Kontak Telepon Pelaku A yang Dihapus	38
Gambar 4.11 Bukti Gambar WhatsApp Messenger	39
Gambar 4.12 Bukti Kontak WhatsApp Pelaku B Dihapus	39
Gambar 4.13 Bukti Pesan Telegram yang Dihapus Pelaku A	40
Gambar 4.14 Bukti Pesan Gambar Telegram yang Dihapus Pelaku A	40
Gambar 4.15 Bukti Pesan Gambar Telegram yang Dihapus Pelaku A	40
Gambar 4.16 Bukti Pesan Video Telegram yang Dihapus Pelaku A	41
Gambar 4.17 Bukti Pesan Gambar Telegram yang Dihapus Pelaku A	41
Gambar 4.18 Bukti Pesan Dokumen Telegram yang Dihapus Pelaku A	42
Gambar 4.19 Bukti Kontak Telepon Telegram yang Dihapus Pelaku A	42
Gambar 4.20 Airplane Mode Pada Samsung Galaxy Ace 3	48
Gambar 4.21 SMS yang Dihapus Pada Samsung Galaxy Ace 3	50
Gambar 4.22 Bukti Gambar yang Dihapus Pada Samsung Galaxy Ace 3	51
Gambar 4.23 Kontak Telepon Pelaku A yang Dihapus	51
Gambar 4.24 Percakapan Whatsapp yang Dihapus	52
Gambar 4.25 Pesan Gambar WhatsApp yang Dihapus	52
Gambar 4.26 Pesan Dokumen WhatsApp yang Dihapus	53
Gambar 4.27 Kontak Telepon WhatsApp yang Dihapus	53

Gambar 4.28 Pesan Telegram yang Dihapus	. 54
Gambar 4.29 Pesan Gambar Telegram yang Dihapus	. 54
Gambar 4.30 Pesan Video Telegram yang Dihapus	. 55
Gambar 4.31 Pesan Audio Telegram yang Dihapus	. 55
Gambar 4.32 Pesan Dokumen Telegram yang Dihapus	.56
Gambar 4.33 Kontak Telepon Telegram yang Dihapus	.56
Gambar 4.34 Aplikasi Autopsy Menampilkan Data Pendukung Artifact	.61
Gambar 4.35 Aplikasi Autopsy Menggabungkan dengan Benar	.61
Gambar 4.36 Aplikasi Autopsy Tidak Memodifikasi Image File	.61
Gambar 4.37 Autopsy Menampilkan Pelanggan dan Peralatan yang Tersedia	. 62
Gambar 4.38 Autopsy Dapat Menampilkan PIM dari Image File	. 62
Gambar 4.39 Autopsy Menampilkan Log Panggilan	. 63
Gambar 4.40 Autopsy Dapat Menampilkan Audio, Gambar dan Video	. 63
Gambar 4.41 Autopsy Menamp <mark>i</mark> lk <mark>an</mark> History <mark>dan</mark> Bookmarks	. 64
Gambar 4.42 Autopsy Dapat Mengekstrasi Data Pendukung Artifact	. 64
Gambar 4.43 Autopsy Dap <mark>at M</mark> engg <mark>ab</mark> ungkan Text Dengan Benar	. 65
Gambar 4.44 Tidak Memo <mark>difi</mark> kas <mark>i Ima</mark> ge <mark>Fi</mark> le da <mark>n D</mark> apat Menampilkan Pesan .	. 65
Gambar 4.45 Autopsy Dap <mark>at Menampilkan</mark> Infor <mark>ma</mark> si Pelanggan	. 66
Gambar 4.46 Autopsy Dapat Menampilkan PIM	. 66
Gambar 4.47 Autopsy Dapat Menampilkan SMS dan Instant Message	. 67
Gambar 4.48 Autopsy Dapat Menampilkan Audio, Gambar dan Video	. 67
Gambar 4.49 Autopsy Dapat Menampilkan History dan Bookmarks	. 68

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di dunia perangkat *mobile* semakin berkembang. Salah satunya adalah *smartphone*. Penggunaan *smartphone* semakin meningkat dari tahun ke tahun, menurut Statista penggunaan *smartphone* di Indonesia pada tahun 2019 mencapai 76,64 juta pengguna. *Smartphone* memiliki beberapa *operation system* (OS), salah satunya adalah Android.

Smartphone dengan sistem operasi berbasis Android diperkenalkan pada tahun 2007 dan menjadi mobile OS paling banyak digunakan di Indonesia (Umar et al., 2017). Smartphone memiliki lebih banyak kelebihan daripada ponsel biasa yang hanya bisa untuk melakukan panggilan suara atau mengirim pesan singkat. Kelebihan smartphone antara lain untuk berinteraksi di media sosial dan melakukan video call.

Selain mempunyai kelebihan, *smartphone* juga memiliki dampak kerugian salah satunya adalah untuk melakukan *cybercrime*. *Cybercrime* adalah tindakan kejahatan yang menggunakan teknologi informasi (Riadi *et al.*, 2018). Penyalahgunaan *smartphone* termasuk kasus *cybercrime* yang paling banyak ditemukan di Indonesia antara lain prostitusi *online*, *grooming* dan penipuan menggunakan media *smartphone*.

Beberapa berita kasus penyalahgunaan *smartphone* yang telah diungkap kepolisian Republik Indonesia yaitu pertama kasus *grooming* di Surabaya yang melibatkan pelaku berinisial TS (25) menyamar sebagai guru di sekolah, menggunakan media sosial Instagram (Wahid, 2019). Kedua, kasus penipuan dengan menggunakan media sosial Whatsapp dengan menyamar sebagai teman SMP korban (Mawardi, 2019). Terakhir kasus prostitusi *online* yang menggunakan media sosial Michat dan Whatsapp (Mappiwali, 2019).

Ketika seseorang melakukan *cybercrime* dan ditemukan sebuah *smartphone* yang di dalamnya menunjukan bahwa seseorang tersebut melakukan *cybercrime*. *Smartphone* ini dapat dijadikan barang bukti dan dilakukan identifikasi untuk membantu penegakan hukum di pengadilan (Yudhana *et al.*, 2018). Terkait barang bukti digital telah diatur menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 BAB III Informasi, Dokumen dan Tanda Tangan Elektronik Pasal 6

yang berbunyi "Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan".

Untuk melakukan identifikasi terkait *smartphone*, penyidik melakukan digital forensik. Digital forensik adalah teknik penyelidikan terkait konten perangkat digital didasarkan untuk mengumpulkan, menganalisis dan menyajikan bukti untuk mengungkap kejahatan saat proses pengadilan (Riadi *et al.*, 2020). Pengambilan data barang bukti terdapat dua cara yaitu *dead forensic* dan *live forensic*. *Dead forensic* adalah suatu teknik pengambilan data permanen dari media penyimpanan pada umumnya, sedangkan *live forensic* adalah teknik pengambilan data saat sistem dalam kondisi berjalan (Yudhana *et al.*, 2018). Permasalahan terbesar dalam proses pengambilan data adalah para pelaku menyembunyikan atau melakukan penghapusan barang bukti digital pada *smartphone* untuk menghilangkan barang bukti (Riadi *et al.*, 2020).

Untuk melakukan analisis digital forensik terdapat beberapa *framework*, salah satunya adalah menggunakan *National Institute Standards and Technology* (NIST). NIST adalah suatu standar atau pedoman untuk melakukan forensik pada perangkat *mobile* yang menjamin supaya pekerjaan penyidik dapat terdokumentasikan, dapat diulang dan dipertahankan (Ajijola *et al.*, 2014).

Maka dari itu penelitian ini dapat digunakan sebagai solusi untuk membantu proses penyidikan dalam menemukan barang bukti yang terhapus atau disembunyikan sehingga dapat digunakan saat proses pengadilan. Berawal dari latar belakang yang telah dipaparkan, maka perlu dilakukan penelitian dengan judul "ANALISIS KINERJA AUTOPSY PADA SMARTPHONE BERBASIS ANDROID MENGGUNAKAN NIST MEASUREMENTS", sehingga hasil dari penelitian ini dapat digunakan sebagai alternatif penyidikan.

1.2 Perumusan Masalah

Berdasarkan permasalahan di atas, dirumuskan permasalahan yaitu bagaimana kinerja Autopsy pada *smartphone* berbasis Android menggunakan NIST *Measurements*?

1.3 Batasan Masalah

Untuk menjaga cakupan batasan masalah, maka terdapat ruang lingkup penelitian di antara lain:

- 1. Penelitian ini menggunakan framework NIST Special Publication 808-101 Revision 1.
- 2. Alat yang digunakan untuk analisis digital forensik adalah *Autopsy* 4.14.0.
- 3. Alat yang digunakan untuk melakukan akuisisi adalah Magnet *Acquire* 2.0.1.6843.
- 4. Aplikasi *Instant Messenger* yang digunakan adalah Telegram versi 6.2.0 WhatsApp versi 2.20.194.16
- 5. Setelah melakukan semua skenario langsung dilakukan proses digital forensik.

1.4 Tujuan Penelitian

Setelah dirumuskan permasalahan di atas, tujuan dari penelitian ini adalah mengetahui kinerja Autopsy pada *smartphone* berbasis Android menggunakan NIST Measurements.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini terdapat secara teoritis dan praktis yaitu

- 1. Secara teoritis, hasil dari penelitian ini dapat digunakan sebagai referensi untuk melakukan analisis digital forensik pada perangkat *mobile* android.
- 2. Secara praktis, penelitian ini dapat digunakan sebagai bahan pertimbangan alternatif bagi penyidik saat melakukan penyidikan terkait digital forensik

1.6 Sistematika Penulisan Skripsi

Dalam penyusunan skripsi, terdapat sistematika dalam penulisan skripsi yang berlaku antara lain:

1. BAB 1 PENDAHULUAN

Terdapat susunan latar belakang, perumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian.

2. BAB II TINJAUAN PUSTAKA

Pada bab dua tinjauan pustaka terdapat beberapa penelitian-penelitian sebelumnya yang berhubungan dengan penelitian yang dikerjakan, teori-teori dasar yang digunakan dan integrasi keilmuan dari penelitian yang dilakukan.

3. BAB III METODOLOGI PENELITIAN

Pada bab tiga metodologi penelitian terdapat penjelasan metodologi untuk menyelesaikan penelitian yang dikerjakan.

4. BAB IV HASIL DAN PEMBAHASAN

Terdapat hasil penelitian dari kinerja aplikasi Autopsy berdasarkan NIST *Measurements*.

5. BAB V PENUTUP

Pada bab lima penutup, terdapat kesimpulan dari hasil dan pembahasan penelitian. Serta terdapat saran dan masukan untuk pengembangan penelitian berikutnya.

BAB 2 TINJAUAN PUSTAKA

2.1 Tinjauan Penelitian Terdahulu

Untuk memperoleh referensi dan pemahaman terkait penelitian ini maka dilakukan studi literatur penelitian sebelumnya yang berhubungan. Berdasarkan penelitian yang dilakukan oleh (Umar et al., 2017) dengan judul "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements" menggunakan NIST Measurement sebagai alat ukur untuk mengevaluasi alat forensik yang digunakan. Hasil dari penelitian ini yaitu untuk aplikasi Belkasoft Evidence mempunyai nilai tertinggi yaitu sebesar 88,23%, diikuti dengan aplikasi Oxygen Forensic sebesar 82,35% dan yang terakhir WhatsApp DB/Key Extractor sebesar 23,52%.

Penelitian selanjutnya yang dilakukan oleh (Orr and Castro, 2018) dengan judul "Whatsapp Messenger on the Android Platform: A Forensic Examination of a Physical Device" yang bertujuan untuk menganalisis data third-party applications selama dilakukannya investigasi kriminal dengan menggunakan aplikasi WhatsApp pada perangkat android unroot sebagai objek penelitian. Hasilnya memungkinkan penyelidik untuk menentukan tanggal dan waktu dengan siapa pengguna berhubungan.

Pada penelitian ketiga yang dilakukan oleh (Kim et al., 2018) dengan judul "Mobile Forensic Reference Set (MFReS) and Mobile Forensic Investigation for Android Devices" bertujuan untuk mengembangkan Mobile Forensic Reference Set (MFRes) sebagai prosedur alternatif investigasi serta alat untuk mobile forensic. MFRes terdiri dari 2 repositori sebagai file server (Android System Data Repository dan Android App Install), 3 Reference Data Set (RDS) Android System Data RDS, Android App Install Data RDS dan JPEG Define Quantization Table (DQT) RDS sebagai database server dan layanan Representational State Transfer (REST) untuk meminta data RDS. Kesimpulan dari penelitian ini bahwa MFRes dapat digunakan sebagai sistem infrastruktur untuk mobile forensic. Alat mobile forensic yang dikembangkan pada penelitian ini dapat digunakan sebagai tahap pra proses mobile forensic.

Pada penelitian selanjutnya yang dilakukan oleh (Riadi et al., 2018) dengan judul "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)" menggunakan metode NIJ untuk mengakuisisi bukti digital dari aplikasi Instagram Messenger dengan aplikasi Oxygen Forensic. Pada penelitian ini juga dilakukan simulasi kasus yang terindikasi sebagai kejahatan cyberbullying. Hasil dari penelitian ini dapat menemukan bukti digital pada smartphone dalam kondisi root milik tersangka berupa Gambar dan percakapan tersangka. Namun pada smartphone milik korban yang kondisinya unroot tidak ditemukan bukti digital.

Pada penelitian keempat yang dilakukan oleh (Yudhana et al., 2019) dengan judul "Identification of Digital Evidence Facebook Messenger on Mobile Phone with National Institute of Standards Technology (NIST) Method", melakukan penelitian dengan menggunakan metode NIST untuk mengidentifikasi bukti digital aplikasi Facebook Messenger pada perangkat mobile. Tujuan dari penelitian ini adalah membandingkan alat forensik Magnet Axiom dengan Oxygen Forensic dengan NIST Measurements. Hasil dari penelitian ini adalah membuktikan aplikasi Oxygen Forensic lebih unggul sebesar 79% dari Magnet Axiom 75%.

Dari beberapa penelitian terdahulu yang juga menggunakan *framework* NIST untuk melakukan analisis digital forensik. Pada penelitian kali ini juga menggunakan *framework* NIST, namun menggunakan versi SP 800-101 R1 dan juga melakukan analisis digital forensik pada seluruh fitur perangkat *mobile* dan sumber bukti digital yang ada.

2.2 Dasar Teori

2.2.1 Digital Forensik

Pada tahun 2001 di acara pertama *Digital Forensic Research Workshop* (DFRWS) diperkenalkan ilmu digital forensik sebagai konsep yang beragam yang tergantung pada metode yang telah terbukti secara ilmiah untuk menyediakan langkah-langkah yang efisien untuk mendukung siklus dari bukti digital (Chernyshev *et al.*, 2017). Forensik digital merupakan cabang dari ilmu forensik yang mencakup penemuan selama investigasi data yang ditemukan pada perangkat digital sebagai barang bukti digital. Bukti digital ini digunakan untuk mendukung atau membantah hipotesis selama investigasi yang melibatkan sumber digital.

Tahapan-tahapan dari investigasi digital forensik terdiri dari *preservation*, collection, validation, identification, analysis, interpretation, documentation dan presentation.

2.2.2 Mobile Forensic

Karena hasil yang signifikan di antara perangkat elektronik, digital forensik telah berkembang menjadi beberapa cabang ilmu pengetahuan di antara lain computer forensic, network forensic, malware forensic, database forensic dan mobile forensic. Mobile forensic adalah ilmu pengetahuan untuk memulihkan bukti digital secara forensik menggunakan metode yang diterima(Chernyshev et al., 2017). Pada perangkat mobile terdapat fitur-fitur yang dapat dijadikan sumber bukti digital yang telah disajikan di bawah pada Tabel 2.1.

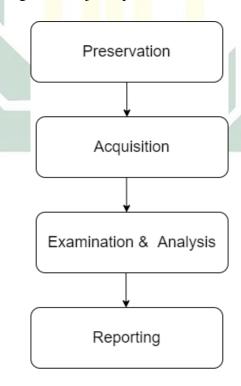
Tabel 2.1 *Evidence Sources* (Chernyshev *et al.*, 2017)

Phone Feature	/	Evidence
	Sou <mark>rc</mark> e	Description
Platform	Device	Unique and persistent device identifiers, network information, personal settings (such as locale)
Contacts and personal productivity	Device	Phonebook and contacts, calendars, email, reminders and to-do lists, electronic documents, web-browsing activities
Calls and messaging	Device	Call register and message history
Audio and image capture	Device	Photos, audio and video recordings
Positioning	Device	Accurate location data
Apps	Device	Application data, social network data, and cloud service user identities and access tokens
Local and personal networking	Device	Known or visible networks and devices (Wi-Fi networks and paired or discovered Bluetooth devices)

Phone Feature		Evidence
	Source	Description
Mobile	Carrier	Cell tower associations, less accurate
telecommunications		location information, and service usage
		data
Васкир	User	Transferred information comprising
	workstation	device and app data

2.2.3 NIST Special Publication 800-101 Revision 1

Pada NIST *Special Publication* 800-101 *Revision* 1 terdapat panduan untuk melakukan forensik terhadap perangkat *mobile*. Pedoman ini menjelaskan alur terdiri dari *preservation, acquisition, examination, analysis* dan *reporting*. Tujuan dari pedoman ini adalah untuk membantu mengembangkan kebijakan dan langkahlangkah untuk mengatasi terkait *mobile* forensik. Pada Gambar 2.1 di bawah adalah fase proses forensik yang berkelanjutan pada NIST SP 800-101 R1.



Gambar 2.1 NIST SP 800-101 R1 (Ayers et al., 2014)

- 1. Pada proses forensik, ini adalah tahap pertama dalam pemulihan bukti digital yaitu *preservation*. *Preservation* adalah tahap menjaga data pada perangkat mobile supaya tidak mengubah atau menghilangkan data saat proses forensik. Kegagalan dalam menjaga bukti dapat membahayakan proses selama penyelidikan sehingga berpotensi menghilangkan barang bukti berharga yang berhubungan dengan kasus. Terdapat beberapa prosedur dalam tahapan *preservation* antara lain:
- a. Securing and Evaluating the Scene
- Pengambilan data sidik jari atau tes DNA pengguna atau pemilik perangkat *mobile*
- Mewaspadai karakteristik dan permasalahan pada perangkat mobile
- Melakukan pencarian yang menyeluruh pada perangkat mobile seperti kartu memori eksternal, UICC dan komputer pribadi yang berhubungan dengan perangkat mobile pengguna
- Saat melakukan wawancara dengan pengguna atau pemilik perangkat *mobile*, diperlukan untuk meminta kata sandi atau pola untuk mengakses data pada perangkat mobile
- Saat mengamankan perangkat *mobile*, perlu diwaspadai untuk menghindari aktivasi kode *reset master* pada perangkat *mobile* sehingga dapat menghapus semua data. *Reset Master* dapat dilakukan dari jarak jauh sehingga diperlukan isolasi jaringan menghindari penghapusan atau modifikasi pada data perangkat *mobile*.
- Perangkat *mobile* dapat ditemukan dengan kondisi yang komplikasi sehingga perlu dilakukan penanganan oleh petugas forensik khusus.
- Perangkat *mobile* yang terendam cairan yang tidak bersifat kaustik perlu dilakukan pelepasan baterai jika baterai tersebut *removable battery*.
- Jika pada perangkat *mobile* terdapat kerusakan yang mengakibatkan mengganggu proses pengambilan data maka boleh dilakukan perbaikan komponen atau perintah pada perangkat *mobile* pada kondisi semula.
- b. Documenting the Scene
- Bukti-bukti yang ditemukan harus diidentifikasi dan dicatat secara akurat.

- Bahan non-elektronik seperti faktur pembelian, buku petunjuk maupun dus box perangkat mobile mungkin dapat bermanfaat untuk mengetahui spesifikasi perangkat mobile.
- Mengambil Gambar tempat kejadian beserta perangkat digital yang ditemukan untuk membantu penyidikan.
- Hindari menyentuh atau mencemari perangkat mobile ketika mendokumentasikan dimana bukti-bukti tersebut ditemukan.
- Jika perangkat mobile yang ditemukan dalam keadaan layar yang terdapat tampilan harus didokumentasikan secara lengkap.

c. Isolation

Terdapat beberapa perangkat mobile yang memiliki kemampuan yang digunakan penggunanya untuk melakukan penguncian atau menghapus data dari jarak jauh dengan hanya mengirimkan perintah misalnya melalui pesan teks maka perlu dilakukannya menonaktifkan konektivitas jaringan yang terdapat pada perangkat mobile. Selain itu juga menghindari modifikasi data seperti penambahan koordinat lokasi GPS baru di lokasi petugas forensik. Terdapat 3 metode dasar untuk mengisolasi perangkat seluler antara lain:

- 1. Ubah jaringan perangkat mobile ke airplane mode
- 2. Nonaktifkan perangkat mobile
- 3. Tempatkan perangkat di wadah yang terlindungi.

Namun pada saat menonaktifkan perangkat *mobile* dapat mengaktifkan authentication codes seperti UICC PIN atau kode keamanan pada perangkat mobile yang dapat mempersulit proses *acquisition* dan menunda *examination*.

d. Radio Isolation Containers

Untuk lebih menghindari aktifnya konektivitas pada perangkat *mobile* diperlukan sebuah wadah pelindung perangkat *mobile* yang dapat mengisolasi perangkat seluler untuk mencegah konektivitas jaringan. Namun sebelum dilakukan untuk pengujian perangkat seluler, perlu dilakukan pengujian pada wadah perangkat *mobile* untuk memvalidasi bahwa berfungsi dengan baik.

- e. Cellular Network Isolation Techniques
- Baterai perangkat mobile harus terisi penuh sebelum pemeriksaan dan dipertimbangkan harus memberikan sumber listrik saat pemeriksaan

- Menggunakan *Cellular Network Isolation Card* (CNIC) untuk mencegah akses jaringan kepada atau dari perangkat seluler
- Menggunakan Portable Shielded Containers selama pemeriksaan untuk mencegah terjadinya komunikasi jaringan.
- Mengamankan lokasi pemeriksaan untuk melakukan pemeriksaan dengan aman di lokasi yang tetap
- Menonaktifkan Layanan Jaringan
- Jamming / Spoofing Devices

f. Cellular Network Isolation Cards

Pendekatan yang lebih baik adalah dengan membuat pengganti UICC misalnya CNIC untuk digunakan kepada perangkat *mobile* untuk meniru karakteristik UICC asli sehingga dapat menipu perangkat untuk menerima sebagaimana aslinya. Sebagian besar alat forensik *mobile* menyediakan fitur untuk membuat sebuah CNIC.

g. Packaging, Transporting, and Storing Evidence, and Triage

Setelah perangkat *mobile* telah siap disita, petugas forensik harus menyegel wadah perangkat dengan label sesuai dengan spesifikasi agensi. Karena sifat *volatile* dari beberapa perangkat *mobile*, harus segera diperiksa di laboratorium forensik untuk pemrosesan. Fasilitas penyimpanan yang memiliki bukti harus menyediakan lingkungan yang sejuk dan kering yang sesuai untuk perangkat elektronik yang berharga. Semua bukti harus dalam wadah tertutup di tempat yang aman dengan akses terkontrol.

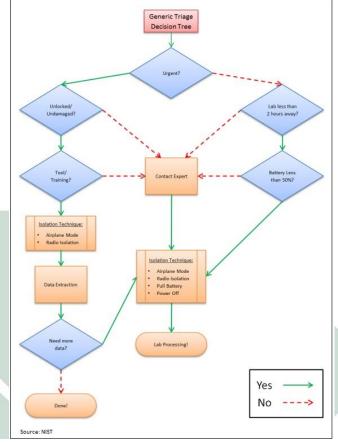
h. On-Site Processing

Jika perangkat *mobile* yang ditemukan dalam keadaan layar tidak dikunci atau baterai tidak habis, segera dilakukan pemeriksaan. Sehingga ketika perangkat terkunci sudah terhubung dengan perangkat *mobile* tersebut.

i. Generic On-Site Decision Tree

Pada Gambar 2.2 mengilustrasikan contoh decision tree di tempat yang dapat digunakan sebagai pedoman untuk organisasi dan lembaga yang lebih umum.

Bermaksud untuk penyesuaian yang memungkingkan penyelarasan dengan kebijakan dan prosedur yang ada.



Gambar 2.2 Generic On-Site Decision Tree (Ayers et al., 2014)

- 2. Tahap kedua adalah *acquisition*, *acquisition* adalah tahap proses mendapatkan informasi dari perangkat *mobile* dan media yang berkaitan. Pemeriksaan forensik pada tahap acquisition antara lain:
- a. Mobile Device Identification
- Device Characteristics Identification
- Device Interface Identification
- Device Label Identification (IMEI, ESN, ICCID of the UICC, FCC ID dan MEID)
- Carrier Identification
- Reverse Lookup
- b. Tool Selection and Expectations

Dalam melakukan acquisition pada perangkat *mobile* sebagian besar menentukan alat forensik apa yang digunakan. Alat forensik yang digunakan sebaiknya dipertimbangkan memiliki kriteria penilaian sebagai berikut:

- 1. Usability
- 2. Comprehensive
- 3. Deterministic
- 4. Verifiable
- 5. Tested
- c. Mobile Device Memory Acquisition

Pada saat pemulihan data pada perangkat mobile harap dipastikan terlebih dahulu data yang diminta misalnya hanya log telepon atau Gambar pada galeri. Jika perangkat mobile ditemukan dalam keadaan menyala, harus dilakukan acquisition sebelum dilakukan physical acquisition. Jika perangkat ditemukan dalam keadaan mati, harus dilakukan physical acquisition terlebih dahulu sebelum dilakukan acquisition terhadap internal memory perangkat mobile.

3. Selanjutnya adalah tahap *examination* dan *analysis*, tahap *examination* dan *analysis* adalah proses pemeriksaan untuk mengungkap bukti-bukti digital termasuk yang sengaja dihilangkan atau disembunyikan. Proses pemeriksaan dimulai dengan salinan bukti yang diperoleh dari perangkat mobile. Proses analisis berbeda dari pemeriksaan dalam hal melihat hasil pemeriksaan untuk signifikansi langsung dan nilai probatif untuk kasus tersebut.

Pemeriksa forensik akan membutuhkan informasi tentang kasus ini dan pihak-pihak yang terlibat untuk memberikan titik awal untuk bukti potensial yang mungkin ditemukan. Pemahaman yang diperoleh dengan mempelajari kasus ini harus memberikan gagasan tentang jenis data yang akan ditargetkan dan kata kunci atau frasa tertentu untuk digunakan saat mencari data yang diperoleh. Tergantung pada jenis kasusnya, strateginya bervariasi. Misalnya, kasus tentang pornografi anak dapat dimulai dengan menelusuri semua Gambar grafik pada sistem, sementara kasus tentang pelanggaran terkait Internet mungkin dimulai dengan menelusuri semua file riwayat Internet.

a. Potential Evidence

Pada perangkat *mobile* terdapat beberapa cakupan bukti-bukti digital di antara lain:

- 1. Subscriber and equipment identifiers
- 2. *Date/time*, *language*, *and other settings*

- 3. Phonebook/Contact information
- 4. Calendar information
- 5. Text messages
- 6. Outgoing, incoming, and missed call logs
- 7. Electronic mail
- 8. Photos
- 9. Audio and video recordings
- 10. Multi-media messages
- 11. Instant messaging
- 12. Web browsing activities
- 13. Electronic documents
- 14. Social media related data
- 15. Application related data
- 16. Location information
- 17. Geolocation data
- b. Applying Mobile Device Forensic Tools

Dua jenis investigasi forensik komputer umumnya berlangsung. Jenis pertama adalah di mana insiden telah terjadi tetapi identitas pelaku tidak diketahui contohnya adalah insiden peretasan. Kedua adalah tempat tersangka dan insiden diketahui contohnya investigasi film porno remaja. Dipersiapkan dengan latar belakang kejadian, pemeriksa forensik dan analis dapat melanjutkan menuju pencapaian tujuan berikut:

- Kumpulkan informasi tentang individu yang terlibat (Who).
- Tentukan sifat pasti dari peristiwa yang terjadi (*What*).
- Buat garis waktu kejadian (When).
- Mengungkap informasi yang menjelaskan motivasi pelanggaran (Why).
- Temukan alat atau eksploitasi apa yang digunakan (*How*).

Setelah melakukan *acquisition* dan mendapatkan salinan data dari perangkat *mobile*, langkah selanjutnya melakukan pencarian data dengan alat forensik. Sebuah panduan penegakan hukum yang dibuat oleh U.S *Department of Justice* menyarankan beberapa analisis data yang diekstraksi antara lain:

1. Ownership and Possession

- 2. Application and File
- 3. Analysis Timeframe
- 4. Analysis Data Hiding Analysis
- c. Call and Subscriber Records

Catatan yang dikelola oleh penyedia layanan menangkap informasi yang diperlukan untuk menagih pelanggan. Selain catatan panggilan detail, catatan pelanggan yang dikelola oleh penyedia layanan dapat memberikan data yang berguna dalam penyelidikan. Contohnya untuk sistem GSM, database biasanya berisi informasi tentang masing-masing pelanggan adalah sebagai berikut:

- 1. Nama dan alamat pelanggan
- 2. Nama dan alamat penagihan (jika selain pelanggan)
- 3. Nama dan alamat pengguna (jika selain pelanggan)
- 4. Detail akun penagihan Nomor telepon (MSISDN)
- 5. IMSI
- 6. Nomor seri UICC (ICCID)
- 7. PIN / PUK untuk UICC
- 8. Layanan diizinkan
- 4. Tahap terakhir adalah *reporting*, *reporting* adalah proses mempersiapkan ringkasan terperinci dari semua langkah yang diambil dan kesimpulan yang dicapai dalam penyelidikan suatu kasus. Laporan hasil pemeriksaan forensik harus mencakup semua informasi yang diperlukan untuk mengidentifikasi kasus dan sumbernya, menguraikan hasil tes dan temuan serta bertanggung jawab atas isinya. Secara umum, laporan dapat mencakup informasi sebagai berikut:
- Identitas agen pelapor
- Pengidentifikasi kasus atau nomor pengiriman
- Penyelidik kasus
- Identitas pengirim
- Tanggal penerimaan bukti
- Tanggal laporan
- Daftar deskriptif i*tem* yang diajukan untuk pemeriksaan, termasuk nomor seri, merek, dan model

- Identitas dan tanda tangan pemeriksa
- Peralatan dan perlengkapan yang digunakan dalam pemeriksaan
- Deskripsi singkat tentang langkah-langkah yang diambil selama pemeriksaan, seperti pencarian string, pencarian Gambar grafik, dan memulihkan file yang terhapus.
- Bahan pendukung seperti cetakan barang bukti tertentu, salinan bukti digital, dan dokumentasi lacak balak
- Detail temuan
- File spesifik yang terkait dengan permintaan
- File lain, termasuk file yang dihapus, yang mendukung temuan
- Pencarian string, pencarian kata kunci, dan pencarian string teks
- Bukti terkait Internet, seperti analisis lalu lintas situs Web, log obrolan, file cache, e-mail, dan aktivitas grup berita
- Analisis Gambar grafis Indikator kepemilikan, yang dapat mencakup data pendaftaran program Analisis data
- Deskripsi program yang relevan pada item yang diperiksa
- Teknik yang digunakan untuk menyembunyikan atau menyembunyikan data, seperti enkripsi, steganografi, atribut tersembunyi, partisi tersembunyi dan anomali nama file
- Laporkan kesimpulan

2.2.4 Mobile Device Tool Classification System

Dalam melakukan melakukan tahap *acquisition* pada perangkat *mobile*, diperlukan alat forensik yang tepat. Penggunaan sistem klasifikasi pada bagian ini menyediakan sebuah *framework* untuk mempermudah dalam menggunakan metode untuk proses ekstraksi dengan alat yang berbeda. Sistem klasifikasi alat dapat dilihat di bawah ini pada Tabel Gambar 2.3



Gambar 2.3 Tool Classification System (Ayers et al., 2014)

1. Manual Extraction

Pada metode *manual extraction* melibatkan pengamatan langsung pada data-data yang disimpan pada perangkat *mobile*. Data yang ditampilkan pada layer LCD, memerlukan sentuhan tombol, *keyboard* dan *touch screen* secara manual untuk melihat data perangkat *mobile*. Data-data yang ditemukan pada perangkat *mobile* dapat didokumentasikan dengan menggunakan kamera eksternal. Pada metode *manual extraction* tidak dapat memulihkan data yang dihapus tanpa menggunakan bantuan alat. Beberapa alat yang dikembangkan mempunyai kemampuan dalam mendokumentasikan serta mengkategorikan informasi dengan cepat.

Namun, jika data yang terdapat pada perangkat *mobile* terlalu besar dapat membutuhkan waktu yang lama serta dapat memungkinkan mengubah atau menghapus data saat pemeriksaan. Tantangan melakukan *acquisition* menggunakan metode *manual extraction* adalah kondisi perangkat *mobile* yang tidak memadai seperti LCD atau *keyboard* rusak. Begitupun juga, jika bahasa perangkat *mobile* yang diperiksa menggunakan bahasa yang berbeda (Ayers *et al.*, 2014).

2. Logical Analysis

Pada metode *logical analysis* dibutuhkan konektivitas antar perangkat *mobile* dengan komputer melalui USB, RS 232, WiFi maupun *Bluetooth*. Beberapa alat forensik pada aplikasi ini menyarankan menggunakan USB untuk hasil yang lebih maksimal.

3. Hex Dump

Pada umumnya untuk melakukan *Hex Dump* terlebih dahulu mengunggah *boot* loader atau aplikasi yang lain untuk melindungi bagian *memory* pada perangkat *mobile*.

4. Chip-Off

Pada tahap diperlukan kemampuan khusus untuk melakukannya. Pada tahap ekstraksi ini membutuhkan penghapus *flash memory*. Banyak sekali data mentah pada proses ekstraksi ini yang menyebabkan resiko kerusakan pada *memory*.

5. Micro Read

Tahap *micro read* adalah tahap paling akhir setelah tahap sebelumnya telah dilakukan. Tahap ini melibatkan pengamatan pada NAND atau NOR *chip* menggunakan *electron microscope* karena keberhasilan pada tahap ini membutuhkan tim ahli, alat forensik, waktu dan pengetahuan yang sesuai. Tingkat akuisis ini dilakukan jika setara dengan kasus yang diselidiki.

2.2.5 NIST Measurements

NIST *Measurements* bertujuan untuk menetapkan persyaratan, pernyataan pengujian dan *test case* untuk tahap ekstraksi dan pelaporan bukti dari perangkat *mobile*. Pada NIST *Measurements* dibagi menjadi *core features* dan *optional features*, dapat dilihat di Tabel 2.2 di bawah ini.

Tabel 2.2 NIST *Measurements* (Ayers et al., 2014)

Core Features		
Variable	Description	
MDT-CR-01	A mobile device forensic tool extracts and presents all supported	
	data artifacts from a mobile device image file.	
MDT-CR-02	The tool renders text correctly	
MDT-CR-03	A mobile device forensic tool does not modify a mobile device	
	image file being examined.	
MDT-CR-04	A mobile device forensic tool notifies the tool user if a mobile	
	device image file has been modified.	
MDT-CA-01	The tool presents all subscriber and equipment information	
	available from an image file.	
MDT-CA-02	The tool presents all PIM (address book, calendar & notes) data	
	available from an image file.	

Variable	Description		
MDT-CA-03	The tool presents all call data (call type (incoming, outgoing,		
	missed), date312 time stamps, duration) available from an		
	image file.		
MDT-CA-04	The tool presents all message (SMS, MMS & instant messages)		
	data available from an image file.		
MDT-CA-05	The tool presents all stand-alone (audio, documents, graphic &		
	video,) files available from an image file.		
MDT-CA-06	The tool presents all browsing (history & bookmarks) data		
	available from an image file.		
MDT-CA-07	The tool presents all email data available from an image file.		
MDT-CA-08	The tool presents all social media application data available		
	from an image file.		
MDT-CA-09	The tool presents all geo-location application data available		
	from an im <mark>age</mark> file.		
MDT-CA-10	Presented text is rendered with the correct character glyphs.		
MDT-CA-11	The tool d <mark>oes not mod</mark> ify an ima <mark>ge</mark> file.		
MDT-CA-12	If an image file is modified, the tool notifies the user that a		
	change has been made to the image file.		
	Optional Features		
Variable	Description		
MDT-RO-01	A mobile device forensic tool creates an image file from a		
	physical memory acquisition (e.g., boot loader).		
MDT-RO-02	A mobile device forensic tool creates an image file from a		
	logical acquisition of all supported memory artifacts.		
MDT-RO-03	A mobile device forensic tool creates an image file from a		
	logical acquisition of selected memory artifacts.		
MDT-RO-04	A mobile device forensic tool creates an image file from an		
	acquisition of the mobile device file system.		
MDT-RO-05	A mobile device forensic tool notifies the user if there is a failure		
	to access a connected mobile device.		

Variable	Description
MDT-RO-06	A mobile device forensic tool notifies the user if an acquisition
	is interrupted before completion.
MDT-AO-01	An image file is created of physical memory.
MDT-AO-02	An image file is created containing supported memory artifacts.
MDT-AO-03	An image file is created containing selected artifacts.
MDT-AO-04	An image file is created of the device file system.
MDT-AO-05	The user is notified if the tool fails to establish a connection or
	acquire data from a connected mobile device.
MDT-AO-06	The user is notified if an acquisition is disrupted.

Pada perhitungan dari kinerja alat forensik menggunakan perhitungan indeks tertimbang untuk mengukurnya (Yudhana *et al.*, 2019)

$$P ext{on} = rac{\sum P ext{n}}{\sum P ext{o}} imes 100\%$$

$$\sum P ext{n} = The \ Result \ of \ Data \ Acquisition \ Tools$$

$$\sum P ext{o} = The \ Total \ Number \ Of \ Parameters$$

$$P ext{on} = Percentage \ results \ are \ expected$$

2.2.6 Smartphone

Perkembangan teknologi dan informasi menjadikan perangkat *mobile* mempunyai kemampuan dengan penggunaan dan berfungsi seperti komputer yang disebut sebagai *smartphone*. Tidak hanya untuk melakukan panggilan suara tetapi juga dapat mengambil Gambar serta dapat melakukan *install* banyak aplikasi yang tidak dapat dilakukan perangkat *mobile* biasa seperti *chatting*, *sharing video*, foto dan dokumen (Alfawareh and Jusoh, 2017). Pada *smartphone* terdapat beberapa sistem operasi seperti iOS, Android dan Windows yang banyak digunakan di Indonesia.

2.2.7 WhatsApp Messenger

WhatsApp *Messenger* adalah aplikasi percakapan gratis yang tersedia dalam versi Android dan Mac. Dalam Google *Play Store*, aplikasi ini telah diunduh lebih dari 5 Milyar. WhatsApp *Messenger* memiliki berbagai fitur seperti mengirim pesan, foto, video, dokumen dan menelpon serta melakukan *video call*.

2.2.8 Telegram

Telegram adalah termasuk ke dalam aplikasi percakapan gratis pada umumnya. Namun Telegram berfokus kepada kecepatan dan keamanan. Keunggulan Telegram adalah dapat memiliki anggota grup yang tidak terbatas dan memiliki fitur *secret chat* yang dapat diatur supaya terhapus dengan sendirinya.

2.2.9 Autopsy

Autopsy adalah aplikasi *open source* yang dapat digunakan sebagai alat digital forensik yang mendukung tipe sistem file NTFS, FAT, Ext2/3/4, HFS/HFS+ dan UFS (Sidiq dan Faiz, 2019). Aplikasi ini menyediakan alur kerja yang intuitif untuk pengguna di penegakan hukum, militer, agen intelijen, keamanan *cyber* dan pemeriksa perusahaan. Aplikasi ini hanya membutuhkan *disk image* dari perangkat yang akan dianalisis.

2.2.10 Magnet Acquire

Magnet *Acquire* adalah perangkat lunak untuk akuisisi *image* forensik dari iOS, perangkat Android, *hard drive* dan *removable media*. Terdapat 2 pilihan saat membuat *image* yaitu *full* dan quick, namun jika melakukan akuisisi penuh pada perangkat Android, harus dilakukan *ro*oting terhadap perangkat.

2.3 Integrasi Keilmuan

Digital forensik merupakan bagian dari bagian investigasi. Data yang didapat dari perangkat digital dapat digunakan untuk membantu menjadi bukti di persidangan, sehingga dapat membantu menangkap orang yang bersalah maupun membela orang yang tidak bersalah. Berdasarkan hasil wawancara yang dilakukan dengan ta'mir masjid Baitul Muttaqien desa Jogomerto Dr. Warsito, M.Si mengatakan banyak sekali firman Allah SWT tentang kebenaran di antaranya surah As-saba' ayat 46. Dalam Al-Qur'an surah As-saba' ayat 46 dijelaskan sebagai berikut:

۞قُلۡ إِنَّمَاۤ أَعِظُكُم بِوَٰحِدَةۗ أَن تَقُومُواْ لِلَّهِ مَثْنَىٰ وَقُرٰدَىٰ ثُمَّ تَتَفَكَّرُواْۚ مَا بِصَاحِبِكُم مِّن جِنَّةۗ إِنَّ هُوَ إِلَّا نَذِيرٌ لَّكُم بَيْنَ يَدَي عَذَابٍ شَد۞قُلۡ إِنَّمَاۤ أَعِظُكُم بِوَٰحِدَةۗ أَن تَقُومُواْ لِلَّهِ مَثْنَىٰ وَقُرٰدَىٰ ثُمَّ هُوَ إِلَّا نَذِيرٌ لَكُم بَيْنَ يَدَي عَذَابِ شَدِيدٍ يِدٍ تَتَفَكَّرُواْۚ مَا بِصَاحِبِكُم مِّن جِنَّةً إِنْ هُوَ إِلَّا نَذِيرٌ لَكُم بَيْنَ يَدَي عَذَابِ شَدِيدٍ يدٍ

Artinya:

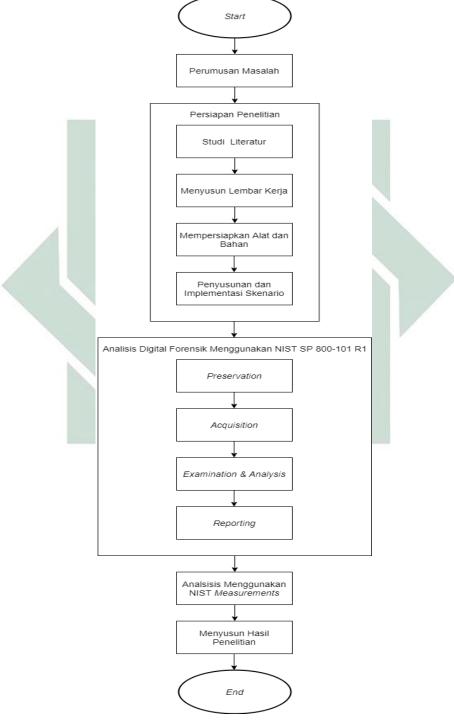
"Katakanlah: "Sesungguhnya aku hendak memperingatkan kepadamu suatu hal saja, yaitu supaya kamu menghadap Allah (dengan ikhlas) berdua-dua atau sendiri-sendiri; kemudian kamu fikirkan (tentang Muhammad)" tidak ada penyakit gila sedikitpun pada kawanmu itu. Dia tidak lain hanyalah pemberi peringatan bagi kamu sebelum (menghadapi) azab yang keras (QS.Al-Saba [34]: 1)".

Tafsir diatas apabila diintegrasikan dengan penelitian ini adalah pentingnya mencari kebenaran dalam hidup. Salah satu cara mencari kebenaran adalah dengan membuktikannya dengan ilmu pengetahuan,



BAB III METODOLOGI PENELITIAN

Alur penelitian ini dideskripsikan ke dalam bentuk *flowchart*. Dengan adanya alur penelitian dapat membantu pelaksanaan penelitian lebih terstruktur dan sistematis yang dapat dilihat pada Gambar 3.1 di bawah ini.



Gambar 3.1 Alur Penelitian

3.1 Perumusan Masalah

Pada tahap ini terdapat proses perumusan masalah yang menjadi latar belakang untuk melakukan penelitian analisis kinerja aplikasi Autopsy menggunakan NIST *Measurements*. Sesuai dengan permasalahan yang tertera di latar belakang. Permasalahan yang diangkat pada penelitian ini adalah menganalisis kinerja aplikasi forensik Autopsy pada *smartphone* berbasis android menggunakan NIST *Measurements*.

3.2 Persiapan Penelitian

Sebelum melakukan penelitian, dilakukan persiapan seperti studi literatur, menyusun lembar kerja serta mempersiapkan alat dan bahan untuk persiapan penelitian. Persiapan alat dan bahan antara lain adalah beberapa perangkat mobile android dan beberapa aplikasi untuk melakukan forensik terhadap perangkat mobile tersebut.

3.2.1 Studi Literatur

Pada tahap ini adalah melakukan studi literatur yang bertujuan untuk membantu dalam penyusunan penelitian ini. Hal ini dilakukan dengan mempelajari buku-buku dan literatur yang relevan dengan penelitian yang dilaksanakan, yaitu:

- 1. Mempelajari tentang penelitian analisis digital forensik menggunakan NIST framework terdahulu.
- 2. Mempelajari *mobile forensic* sebagai dasar pedoman dalam melakukan forensik terhadap perangkat *mobile*
- 3. Mempelajari macam *forensic tools* yang dapat digunakan saat penelitian.
- 4. Mempelajari fitur-fitur terutama pada aplikasi mengandung bukti digital pada kasus tertentu.

3.2.2 Menyusun Lembar Kerja

Pada tahap ini melakukan penyusunan lembar kerja untuk memudahkan dalam melakukan penelitian. Lembar kerja yang telah disusun dapat dijadikan referensi untuk penelitian yang relevan dalam ke depannya.

3.2.3 Mempersiapkan Alat dan Bahan

Pada tahap ini, sebelum melakukan tahap analisis diperlukan menyiapkan alat dan bahan untuk melaksanakan penelitian. Alat dan bahan tersebut adalah beberapa *software* yang terdapat di Tabel 3.1 dan beberapa perangkat *mobile* berbasis Android yang dapat dilihat di bawah ini:



Gambar 3.3 Samsung Galaxy ACE 3 Smartphone

Tabel 3.1 *Software* forensik yang digunakan

Software		
Nama	Kegunaan	
Autopsy 4.14.0	Alat yang digunakan untuk analisis digital forensik	
FTK Imager 4.2.1.	Alat yang digunakan untuk membuat image	
Magnet Acquire 2.0.1.6843.	Alat yang digunakan untuk melakukan akuisisi	

Kabel Universal Serial Bus	Alat yang digunakan untuk menghubungkan
(USB)	antara perangkat <i>mobile</i> dengan komputer

3.2.4 Penyusunan dan Implementasi Skenario

Penyusunan dan implementasi skenario dilakukan untuk merekontruksi aksi relevan yang mungkin dapat dilakukan oleh pelaku tindakan kriminal. Penyusunan skenario disusun berdasarkan analisis fungsionalitas dari perangkat *mobile* android dan referensi terkait. Skenario mencakup dari fitur dari perangkat mobile beserta fitur-fitur aplikasi Whatsapp *Messenger* dan Telegram yang memiliki potensi untuk digunakan sebagai media tindakan kriminal dan dapat digunakan untuk menutupi jejak tindakan kriminal, antara lain:

- 1. Mengirim dan menerima SMS
- 2. Menghapus riwayat pesan
- 3. Melakukan dan menerima panggilan suara
- 4. Menghapus riwayat panggilan
- 5. Menghapus berkas media seperti Gambar, video, audio dan dokumen
- 6. Mengirim dan menerima pesan melalui aplikasi messenger
- 7. Mengirim dan menerima geo-location melalui aplikasi messenger
- 8. Mengirim dan menerima berkas media seperti gambar, video, suara dan dokumen melalui aplikasi *messenger*
- 9. Restract message pada aplikasi messenger
- 10. Menghapus riwayat pesan pada aplikasi messenger
- 11. Melakukan dan menerima voice call dan video call
- 12. Menghapus riwayat panggilan pada aplikasi messanger
- 13. Menghapus kontak telepon

3.3 Analisis Digital Forensik Menggunakan NIST SP 800-101 R1

Pada penelitian ini untuk melakukan analisis digital forensik menggunakan NIST SP 800-101 R1. Tahapan dari *framework* NIST SP 800-101 R1 antara lain:

3.3.1 Preservation

Pada proses forensik *preservation*, telah dipersiapkan beberapa *smartphone* yang tidak terdapat kata kunci keamanan untuk mengakses perangkat tersebut kecuali pada perangkat Xiaomi Redmi Note 3 yang terdapat sebuah keamanan pola untuk mengakses perangkat tersebut. Pada saat proses forensik semua *smartphone*

akan dilakukan *isolation* dengan mengaktifkan *airplane mode* sehingga tidak ada jaringan yang aktif untuk menghindari modifikasi data.

3.3.2 Acquisition

Tahap selanjutnya adalah proses *acquisition*, proses dimana mereplikasi bukti-bukti digital dari *smartphone android*. Pada penelitian ini melakukan *physical acquisition* menggunakan aplikasi Magnet Acquire. Pada aplikasi Magnet Acquire menyediakan 2 tipe untuk memperoleh *disk image* dari *smartphone* yaitu *a quick image* dan *a full image*. Namun pada penelitian ini menggunakan *full image* dari *smartphone* untuk memperoleh seluruh data.

3.3.3 Examination dan Analysis

Setelah melakukan tahap *acquisition* untuk mendapatkan *full image* dari *smartphone* dilakukan analisis dan pemeriksaan menggunakan *forensic tools* Autopsy. Aplikasi Autopsy digunakan untuk membantu menemukan bukti-bukti digital yang dengan sengaja dihapus atau disembunyikan.

3.3.4 Reporting

Setelah melewati semua tahap forensik, dipersiapkan pelaporan ringkasan yang terperinci dari semua langkah yang dilakukan dan membuat kesimpulan yang dicapai dalam penyidikan.

BAB IV HASIL DAN PEMBAHASAN

Penelitian ini dilakukan untuk menyusun serta mengimplementasikan lembar kerja berdasarkan *framework* NIST SP 800-101 R1. Penelitian ini juga membahas hasil analisis kinerja Autopsy pada *Smartphone* berbasis Android menggunakan NIST *Measurements*.

4.1 Lembar Kerja Berdasarkan Framework NIST SP 800-101 R1

Lembar kerja ini disusun berdasarkan *framework* NIST SP 800-101 R1 yang berfungsi untuk melakukan digital forensik. Terdapat 3 lembar kerja yang telah disusun antara lain:

4.1.1 Informasi Kasus

Informasi kasus dibutuhkan untuk analisis digital forensik sebagai titik awal mempelajari kasus tersebut. Adapun ditunjukan pada Tabel 4.1.

Tabel 4.1 Informasi Kasus

Inf	Cormasi Kasus
Nama Petugas Penyelidik Kasus	
Nomor Petugas Penyelidik Kasus	
Nomor Kasus	
Tanggal Penerimaan Bukti	
Deskriptif Kasus	
Data yang Diajukan	
Nama Petugas Pemeriksa	
Nomor Petugas Pemeriksa	

Pada Tabel 4.1. di atas, terdapat nama penyelidik kasus untuk mengetahui petugas yang bertanggung jawab pada kasus yang diselidiki. Serta terdapat nomor kasus untuk mengidentifikasi kasus tersebut ketika disimpan. Tanggal penerimaan bukti berfungsi untuk mengetahui kapan perangkat yang akan dianalisis telah diterima. Sedangkan deskriptif kasus sebagai informasi tentang kasus yang terlibat untuk memberikan titik awal penyelidikan bukti digital. Data yang diajukan berguna untuk mengetahui data apa saya apa yang diminta oleh penyelidik kasus. Nama pemeriksa berfungsi sebagai informasi petugas pemeriksa.

4.1.2 Informasi Perangkat Seluler

Informasi perangkat seluler dibutuhkan sebelum melakukan akuisisi untuk mengetahui karakteristik perangkat *mobile* tersebut. Adapun ditunjukan pada Tabel 4.2.

Tabel 4.2 Informasi Perangkat Seluler

Setelah

Bedasarkan Tabel 4.2, terdapat nama pemilik perangkat untuk mengetahui siapa pemilik perangkat tersebut serta nama dan nomer model perangkat yang diselidiki. Terdapat beberapa informasi tentang perangkat *mobile* yang diselidiki yaitu sistem operasi, IMEI, kata sandi atau pola. Terdapat juga informasi kondisi perangkat mobile apakah dalam keaadan *rooted* atau tidak dan infomasi mengenai apakah terdapat *memory* eksternal dan kartu SIM di dalam perangkat *mobile* tersebut. Terdapat juga sumber bukti digital yang dapat disesuaikan dengan data yang diajukan.

4.1.3 Laporan

Laporan hasil dibutuhkan untuk mengetahui hasil analisis digital forensik dari perangkat *mobile* tersebut, yang ditunjukan pada Tabel 4.3.

Tabel 4.3 Laporan Digital Forensik

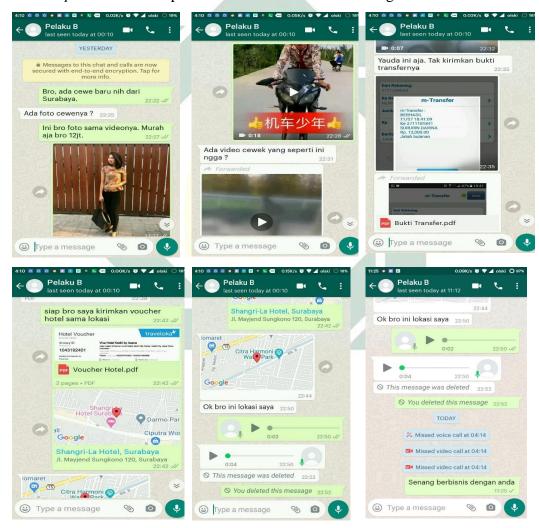
Laporan Digital Forensik	
Nomor Laporan	
Tanggal Laporan	
Nomor Kasus	
Nama Petugas Pemeriksa	
Nomor Petugas Pemeriksa	
Tanggal Penerimaan Bukti	
Nama Petugas Penyelidik Kasus	
Nomor Petugas Penyelidik Kasus	
Nama Pemilik Perangkat	
Nama Perangkat	
Nomor Model	
IMEI	
Deskriptif Kasus	
Data yang Diajukan	
Peralatan yang Digunakan	
Detail temuan	
Tanggal Penerimaan Bukti Nama Petugas Penyelidik Kasus Nomor Petugas Penyelidik Kasus Nama Pemilik Perangkat Nama Perangkat Nomor Model IMEI Deskriptif Kasus Data yang Diajukan Peralatan yang Digunakan	

Berdasarkan Tabel 4.1.4, dapat diketahui bahwa pada laporan digital forensik terdapat data nomor laporan, tanggal laporan, nomor kasus sebagai data untuk menemukan laporan digital forensik Ketika disimpan.Pada laporan digital forensik terdapat juga deskriptif kasus serta data yang diajukan untuk mempermudah petugas pemeriksa untuk melakukan digital forensik. Pada laporan digital forensik juga terdapat informasi peralatan yang digunakan dan detail temuan setelah dilakukannya digital forensik.

4.2 Skenario Sebelum Melakukan Digital Forensik

Sebelum melakukan digital forensik terdapat skenario yang dilakukan, smartphone Xiaomi Redmi Note 3 sebagai Pelaku A sedangkan *smartphone* Samsung Galaxy ACE 3 sebagai Pelaku B antara lain:

- 1. Melakukan percakapan prostitusi online menggunakan media SMS dan aplikasi WhatsApp *Messenger* yang dapat dilihat pada Gambar 4.1.
- 2. Melakukan percakapan pembunuhan berencana menggunakan media Telegram. Yang dapat dilihat pada Gambar 4.2.
- 3. Terdapat 12 bukti digital di setiap media penyimpanan *smartphone* yaitu 3 bukti digital gambar, 3 bukti digital video, 3 bukti digital audio dan 3 bukti digital dokumen yang dapat dilihat pada Gambar 4.3.
- 4. Percakapan yang telah dilakukan dan bukti digital yang terdapat pada *smartphone* telah dihapus semua sebelum melakukan digital forensik.



Gambar 4.1 Screenshoot Percakapan Prostitusi Online WhatsApp



Gambar 4.3 Bukti Digital di Kedua Penyimpanan Smartphone

Bukti 3 Samsung

Bukti 3 Samsung

Bukti 2 Samsung

Bukti 3 Samsung





Gambar 4.4 Screenshoot Percakapan Menggunakan SMS

Namun pada Gambar 4.4 pengiriman gambar dan video melalui SMS tidak berhasil sehingga dihilangkan dari skenario.

4.3 Implementasi Lembar Kerja Untuk Menganalisis Digital Forensik

Pada tahap ini dilakukan implementasi dari lembar kerja yang telah disusun berdasarkan *framework* NIST SP 800-101 R1 untuk melakukan analisis digital forensik pada objek penelitian yang telah dipersiapkan. Terdapat beberapa objek penelitian yang dianalisis antara lain:

4.3.1 Digital Forensik Xiaomi Redmi Note 3

Pada tahap ini dilakukan analisis digital forensik terhadap objek penelitian yang pertama yaitu Xiaomi Redmi Note 3 Adapun implementasi lembar kerja pada untuk analisis digital forensik terhadap Xiaomi Redmi Note 3 dapat dilihat pada Tabel 4.4.

Tabel 4.4 Informasi Kasus Xiaomi Redmi Note 3

Informasi Kasus		
Nama Penyelidik Kasus	Arsyian Aldi Warsito	
Nomor Penyelidik Kasus	H06216005	
Nomor Kasus	Smartphone-001	
Tanggal Penerimaan Bukti	Kamis, 19 Maret 2020	
Deskriptif Kasus	Pemulihan data-data pada perangkat mobile yang	
	telah dihapus atau dihilangkan.	
Data yang Diajukan	SMS, gambar, video, audio, dokumen, call log,	
	kontak telepon, WhatsApp Messenger Artifact	

	(pesan, retract message, gambar, video, audio,	
	dokumen, geo-location, call log dan kontak	
	telepon), Telegram Artifact (pesan, retract	
	message, secret chat, gambar, video, audio,	
	dokumen, geo-location, call log dan kontak	
	telepon).	
Nama Pemeriksa	Arsyian Aldi Warsito	
Nomor Pemeriksa	H06216005	

Pada Tabel 4.4, terdapat nama penyelidik kasus Arsyian Aldi Warsito yang bertanggung jawab pada kasus yang diselidiki. Serta terdapat nomor kasus Smartphone-001 untuk mengidentifikasi kasus tersebut ketika disimpan. Tanggal penerimaan bukti berfungsi untuk mengetahui kapan perangkat yang akan dianalisis telah diterima. Sedangkan deskriptif kasus adalah untuk pemulihan data-data pada perangkat mobile yang telah dihapus atau dihilangkan. Data yang diajukan adalah Gambar, video, audio, archives, dokumen, call log, phone contact, message, web history, email, SMS, gambar, video, audio, dokumen, call log, kontak telepon, WhatsApp Messenger Artifact (pesan, retract message, gambar, video, audio, dokumen, geo-location, call log dan kontak telepon), Telegram Artifact (pesan, retract message, secret chat, gambar, video, audio, dokumen, geo-location, call log dan kontak telepon). Nama pemeriksa pada kasus ini adalah Arsyian Aldi Warsito.

1) Preservation

Analisis digital forensik pada tahap *preservation*, perlu dilakukan *isolation* terhadap perangkat Xiaomi Redmi Note 3 dengan mengaktifkan *airplane mode* sehingga tidak ada jaringan yang aktif untuk menghindari modifikasi data. Pengaktifkan *airplane mode* dapat dilihat pada Gambar 4.5.



Gambar 4.5 Airplane Mode Pada Xiaomi Redmi Note 3

2) Acquisition

Tahap selanjutnya adalah *acquisition* terhadap perangkat Xiaomi Redmi Note 3 menggunakan aplikasi *Magnet Acquire*, sebelum dilakukan akuisisi terdapat informasi perangkat seluler yang dapat dilihat pada Tabel 4.5

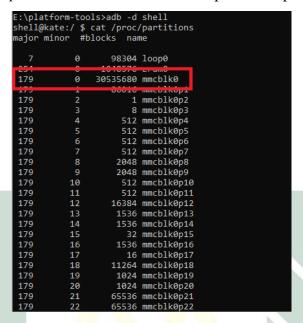
Tabel 4.5 Informasi Perangkat Seluler Xiaomi Redmi Note 3

Informasi Perangkat Seluler		
Nama Pemilik Perangkat	Anindita Lola	
Nama Perangkat	Xiaomi Redmi Note 3	
Nomor Model	Redmi Note 3	
Sistem Operasi	Android 6.0 (Marshmallow)	
IMEI	861735039212336	
Kata Sandi atau Pola	Ada	
Rooted	Rooted	
Memory Eksternal	Tidak Ada	
Kartu SIM	Ada	
Sumber Bukti Digital	Data Awal	Data Setelah
SMS	6	

Gambar	3	
Video	3	
Audio	3	
Dokumen	3	
Call Log	4	
Phone Contact	1	
WhatsApp Messenger	1	
Pesan	8	
Retract Message	2	
Gambar	2	
Video	2	
Audio	2	
Dokumen	2	
Geo-location	2	
Call Log	10	
Phone Contact	1	
Telegram		
Pesan	4	
Retract Message	2	
Secret Chat	2	
Gambar	2	
Video	2	
Audio	2	
Dokumen	2	
Geo-location	2	
Call Log	4	
Phone Contact	1	
Dandagankan Tahal 4	5. danat diketahui hahwa nera	nalsat vana disalidilsi dalam

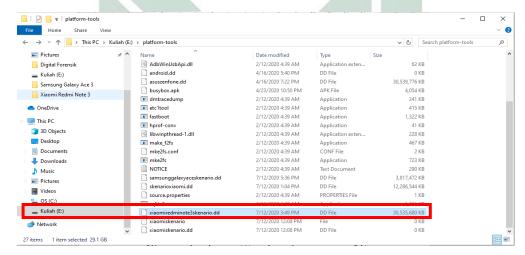
Berdasarkan Tabel 4.5, dapat diketahui bahwa perangkat yang diselidiki dalam kondisi *rooted* serta tidak ada kartu *memory* eksternal dan terdapat kartu SIM di dalamnya. Pada Tabel 4.5 dapat juga diketahui jumlah sumber digital pada perangkat *mobile* sebelum dilakukan *acquisition*.

Sebelum melakukan *acquisition* perlu dilakukan pengecekan untuk mengetahui partisi pada penyimpanan internal *smartphone*. Adapun partisi penyimpanan internal pada *smartphone* Xiaomi Redmi Note 3 dapat dilihat pada Gambar 4.6.



Gambar 4.6 Jumlah Partisi Penyimpanan Pada Xiaomi Redmi Note

Dapat dilihat pada Gambar 4.6, *mmcblk0* menunjukan bahwa partisi internal pada *smartphone* Asus Zenfone 2 sebesar 30535680 *kilo byte* (kb). Sehingga hasil dari akuisisi pada *smartphone* harus sesuai dengan besarnya *mmcblk0* yang tercantum.



Gambar 4.7 Hasil Akuisisi Dari Xiaomi Redmi Note 3

Pada Gambar 4.7, dapat dilihat bahwa hasil akuisisi sebesar 30535680 *kilo byte* (kb) yang sama besar dengan partisi internal *smartphone* yang tercantum. Sehingga

bisa dinyatakan bahwa telah mengakuisisi partisi internal *smartphone* Xiaomi Redmi Note 3.

3) Examination dan Analysis

Pada tahap ini dilakukan *examination* dan *analysis* terhadap hasil akuisisi dari *smartphone* Xiaomi Redmi Note 3. Hasil dari tahap *examination* dan *analysis* antara lain:

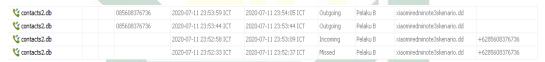
a. Ditemukan SMS yang Dihapus

Pada saat melakukan *examination* dan *analysis* ditemukan SMS yang Terhapus. SMS yang terhapus dapat dilihat pada Gambar 4.8.

Gambar 4.8 SMS yang Terhapus Pada Xiaomi Redmi Note 3

b. Ditemukan Call Log yang Dihapus

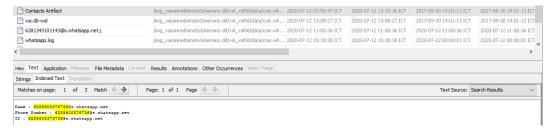
Pada saat melakukan *manual extraction* tidak ditemukan *call log*. Namun setelah *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan beberapa *call log* yang dapat dilihat pada Gambar 4.9.



Gambar 4.9 Ditemukan Call Log yang Dihapus

c. Ditemukan Kontak Telepon Pelaku A yang Dihapus

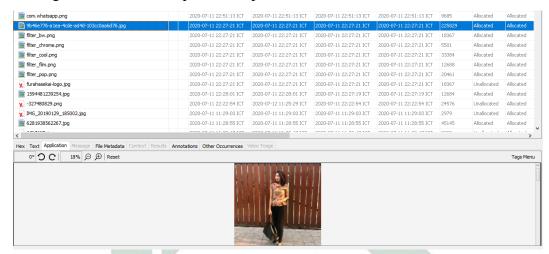
Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan kontak telepon Pelaku A. Kontak telepon Pelaku A dapat dilihat pada Gambar 4.10.



Gambar 4.10 Kontak Telepon Pelaku A yang Dihapus

d. Ditemukan Bukti Gambar WhatsApp Messenger

Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti gambar Pelaku A yang mengirimkan foto wanita yang ditawarkan. Bukti gambar Pelaku A dapat dilihat pada Gambar 4.11.



Gambar 4.11 Bukti Gambar WhatsApp Messenger

e. Ditemukan Bukti Kontak WhatsApp Pelaku B Dihapus

Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti Pelaku A menghapus kontak WhatsApp Pelaku B. Bukti Pelaku A menghapus kontak WhatsApp Pelaku B dapat dilihat pada Gambar 4.12.



Gambar 4.12 Bukti Kontak WhatsApp Pelaku B Dihapus

f. Ditemukan Bukti Pesan Telegram yang Dihapus Pelaku A

Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti pesan Telegram yang dihapus Pelaku A. Bukti pesan Telegram yang dihapus Pelaku A dapat dilihat pada Gambar 4.13.



Gambar 4.13 Bukti Pesan Telegram yang Dihapus Pelaku A

g. Ditemukan Pesan Gambar Telegram yang Dihapus Pelaku A

Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti pesan gambar Telegram yang dihapus Pelaku A. Bukti pesan Telegram yang dihapus Pelaku A dapat dilihat pada Gambar 4.14 dan Gambar 4.15.



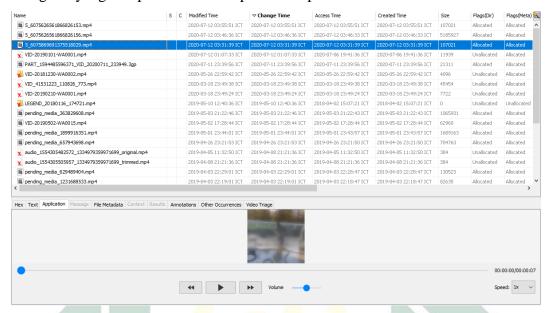
Gambar 4.14 Bukti Pesan Gambar Telegram yang Dihapus Pelaku A



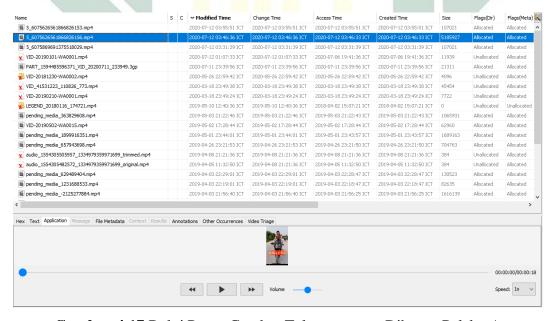
Gambar 4.15 Bukti Pesan Gambar Telegram yang Dihapus Pelaku A

h. Ditemukan Pesan Video Telegram yang Dihapus Pelaku A

Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti video Telegram yang dihapus Pelaku A. Bukti pesan video Telegram yang dihapus Pelaku A dapat dilihat pada Gambar 4.16 dan Gambar 4.17.



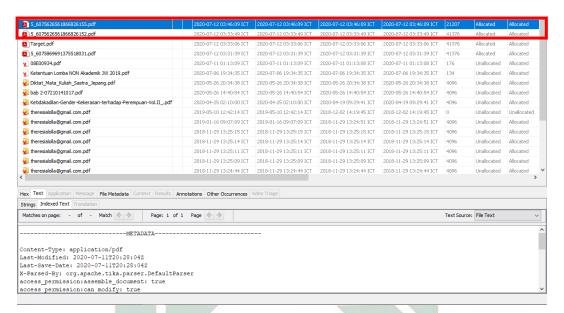
Gambar 4.16 Bukti Pesan Video Telegram yang Dihapus Pelaku A



Gambar 4.17 Bukti Pesan Gambar Telegram yang Dihapus Pelaku A

i. Ditemukan Pesan Dokumen Telegram yang Dihapus Pelaku A

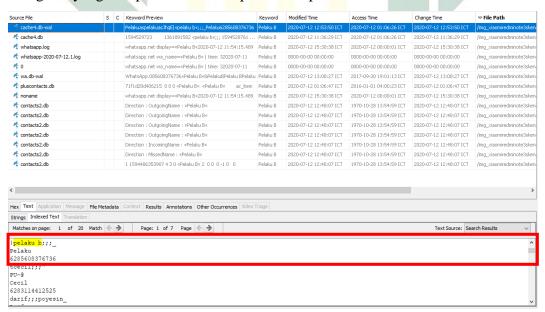
Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti dokumen Telegram yang dihapus Pelaku A. Bukti pesan dokumen Telegram yang dihapus Pelaku A dapat dilihat pada Gambar 4.18.



Gambar 4.18 Bukti Pesan Dokumen Telegram yang Dihapus Pelaku A

j. Ditemukan Kontak Telepon Telegram yang Dihapus Pelaku A

Setelah melakukan *examination* dan *analysis* menggunakan aplikasi Autopsy ditemukan bukti dokumen Telegram yang dihapus Pelaku A. Bukti pesan dokumen Telegram yang dihapus Pelaku A dapat dilihat pada Gambar 4.19.



Gambar 4.19 Bukti Kontak Telepon Telegram yang Dihapus Pelaku A

k. Jumlah Data Setelah Dilakukan Examination dan Analysis

Proses *examination* dan *analysis* untuk mengetahui data-data apa saja yang dapat ditemukan dan dipulihkan menggunakan aplikasi *autopsy*. Adapun hasil *examination* dan *analysis* disajikan pada Tabel 4.6.

Tabel 4.6 Informasi Perangkat Seluler Xiaomi Redmi Note 3

I	Informasi Perangkat Seluler		
Nama Pemilik Perangkat	Anindita Lola		
Nama Perangkat	Xiaomi Redmi Note 3		
Nomor Model	Redmi Note 3		
Sistem Operasi	Android 6.0 (Marshmallow)	
IMEI	861735039212336		
Kata Sandi atau Pola	Tidak Ada		
Rooted	Rooted		
Memory Eksternal	Tidak Ada		
Kartu SIM	Tidak Ada		
Sumber Bukti Digital	Data Awal	Data Setelah	
SMS	6	6	
Gambar	3	0	
Video	3	0	
Audio	3	0	
Dokumen	3	0	
Call Log	4	4	
Phone Contact	1	1	
WhatsApp Messenger	WhatsApp Messenger		
Pesan	8	0	
Retract Message	2	0	
Gambar	2	1	
Video	2	0	
Audio	2	0	
Dokumen	2	0	
Geo-location	2	0	
Call Log	10	0	

Phone Contact	1	1	
Telegram	Telegram		
Pesan	4	4	
Retract Message	2	0	
Secret Chat	2	0	
Gambar	2	2	
Video	2	2	
Audio	2	0	
Dokumen	2	2	
Geo-location	2	0	
Call Log	4	0	
Phone Contact	1	1	

Berdasarkan Tabel 4.6, ditemukan dan dipulihkan pada *file* dengan *extension* SMS (6), *call log* (4), phone contact (1), gambar WhatsApp (1), phone contact WhatsApp (1), pesan Telegram (4), gambar Telegram (2), video Telegram (2), dokumen Telegram (2), phone contact Telegram (1). Namun pada data yang lain tidak dapat ditemukan atau dipulihkan.

4) Reporting

Tahap terakhir dari analisi digital forensik berdasarkan framework NIST SP-800 101 R1 adalah *reporting*. Adapun Tabel *reporting* dapat dilihat pada Tabel 4.7. Laporan Digital Forensik Xiaomi Redmi Note 3

Tabel 4.7 Laporan Digital Forensik Xiaomi Redmi Note 3

Laporan Digital Forensik		
Nomor Laporan	Smartphone - 19-05-2020 - Xiaomi Redmi	
	Note 3	
Tanggal Laporan	Selasa, 19 Mei 2020	
Nomor Kasus	Smartphone-002	
Nama Petugas Pemeriksa	Arsyian Aldi Warsito	
Nomor Petugas Pemeriksa	H06216005	
Tanggal Penerimaan Bukti	Kamis, 19 Maret 2020	
Nama Petugas Penyelidik Kasus	Arsyian Aldi Warsito	

Nomor Petugas Penyelidik Kasus	H06216005	
Nama Pemilik Perangkat	Arsyian Aldi Warsito	
Nama Perangkat	Xiaomi Redmi Note 3	
Nomor Model	Redmi Note 3	
IMEI	861735039212336	
Deskriptif Kasus	Pemulihan data-data pada perangkat mobile	
	yang telah dihapus atau dihilangkan.	
Data yang Diajukan	SMS, gambar, video, audio, dokumen, call	
	log, kontak telepon, WhatsApp Messenger	
	Artifact (pesan, retract message, gambar,	
	video, audio, dokumen, geo-location, call	
	log dan kontak telepon), Telegram Artifact	
	(pesan, retract message, secret chat,	
	gambar, video, audio, dokumen, geo-	
	location, call log dan kontak telepon).	
Peralatan yang Digunakan	1. Magnet Acquire	
	2. Autopsy	
	3. USB Cable	
Detail temuan	1. Ditemukan SMS yang Dihapus	
	2. Ditemukan Call Log yang Dihapus	
	3. Ditemukan Kontak Telepon Pelaku A	
	yang Dihapus	
	4. Ditemukan Bukti Gambar WhatsApp	
	Messenger	
	5. Ditemukan Bukti Kontak WhatsApp	
	Pelaku B Dihapus	
	6. Ditemukan Bukti Pesan Telegram yang	
	Dihapus Pelaku A	
	7. Ditemukan Pesan Gambar Telegram	
	yang Dihapus Pelaku A	
	8. Ditemukan Pesan Video Telegram yang	
	Dihapus Pelaku A	

9. Ditemukan Pesan Dokumen Telegram
yang Dihapus Pelaku A
10. Ditemukan Kontak Telepon Telegram
yang Dihapus Pelaku A

Berdasarkan Tabel 4.11, dapat diketahui bahwa pada laporan digital forensik terkait *smartphone* Xiaomi Redmi Note 3 yang dianalisis bahwa penerimaan bukti diterima tanggal 19 Maret 2020. Deskriptif kasus adalah menemukan dan memulihkan data yang diajukan. Data yang diajukan adalah SMS, gambar, video, audio, dokumen, *call log*, kontak telepon, WhatsApp *Messenger Artifact* (pesan, *retract message*, gambar, video, audio, dokumen, *geo-location*, *call log* dan kontak telepon), Telegram *Artifact* (pesan, retract *message*, *secret chat*, gambar, video, audio, dokumen, *geo-location*, *call log* dan kontak telepon). Peralatan yang digunakan selama proses digital forensik adalah aplikasi *magnet acquire* dan *autopsy* serta USB *Cable*. *Detai*1 temuan yang ditemukan adalah terdapat data kontak *whatsapp* serta sms yang terindikasi dihapus atau disembunyikan.

4.3.2 Digital Forensik Samsung Galaxy ACE 3

Pada tahap ini dilakukan analisis digital forensik terhadap objek penelitian yang pertama yaitu Samsung Galaxy ACE 3. Adapun implementasi lembar kerja pada untuk analisis digital forensik terhadap Samsung Galaxy ACE 3dapat dilihat pada Tabel 4.8.

Tabel 4.8 Informasi Kasus Samsung Galaxy ACE 3

Informasi Kasus		
Nama Penyelidik Kasus	Arsyian Aldi Warsito	
Nomor Penyelidik Kasus	H06216005	
Nomor Kasus	Smartphone-002	
Tanggal Penerimaan Bukti	Jumat, 10 April 2020	
Deskriptif Kasus	Pemulihan data-data pada perangkat mobile yang	
	telah dihapus atau dihilangkan.	
Data yang Diajukan	SMS, gambar, video, audio, dokumen, call log,	
	kontak telepon, WhatsApp Messenger Artifact	
	(pesan, retract message, gambar, video, audio,	

	dokumen, geo-location, call log dan kontak
	telepon), Telegram Artifact (pesan, retract
	message, secret chat, gambar, video, audio,
	dokumen, geo-location, call log dan kontak
	telepon).
Nama Pemeriksa	Arsyian Aldi Warsito
Nomor Pemeriksa	H06216005

Pada Tabel 4.8, terdapat nama penyelidik kasus Arsyian Aldi Warsito yang bertanggung jawab pada kasus yang diselidiki. Serta terdapat nomor kasus Smartphone-002 untuk mengidentifikasi kasus tersebut ketika disimpan. Tanggal penerimaan bukti berfungsi untuk mengetahui kapan perangkat yang akan dianalisis telah diterima. Sedangkan deskriptif kasus adalah untuk pemulihan data-data pada perangkat mobile yang telah dihapus atau dihilangkan. Data yang diajukan adalah SMS, gambar, video, audio, dokumen, *call log*, kontak telepon, WhatsApp *Messenger Artifact* (pesan, *retract message*, gambar, video, audio, dokumen, *geolocation*, *call log* dan kontak telepon), Telegram *Artifact* (pesan, retract *message*, *secret chat*, gambar, video, audio, dokumen, *geo-location*, *call log* dan kontak telepon). Nama pemeriksa pada kasus ini adalah Arsyian Aldi Warsito.

1) Preservation

Analisis digital forensik pada tahap *preservation*, perlu dilakukan *isolation* terhadap perangkat Samsung Galaxy Ace 3 dengan mengaktifkan *airplane mode* sehingga tidak ada jaringan yang aktif untuk menghindari modifikasi data. Pengaktifkan *airplane mode* dapat dilihat pada Gambar 4.20.



Gambar 4.20 Airplane Mode Pada Samsung Galaxy Ace 3

2) Acquisition

Tahap selanjutnya adalah *acquisition* terhadap perangkat Samsung Galaxy Ace 3 menggunakan aplikasi *Magnet Acquire*, sebelum dilakukan akuisisi terdapat informasi perangkat seluler yang dapat dilihat pada Tabel 4.9.

Tabel 4.9 Informasi Perangkat Seluler Samsung Galaxy Ace 3

Informasi Perangkat Seluler	
Nama Pemilik Perangkat	Wanda
Nama Perangkat	Samsung Galaxy Ace 3
Nomor Model	GT-S7270
Sistem Operasi	Android 4.2.2 (Jelly Bean)
IMEI	351651060564205
Kata Sandi atau Pola	Tidak Ada
Rooted	Rooted
Memory Eksternal	Tidak Ada
Kartu SIM	Ada

Data Awal	Data Setelah
6	
3	
3	
3	
3	
4	
1	
8	
2	
2	
2	
2	
2	
2	
10	
1	
4	
2	
2	
2	
2	
2	
2	
2	
4	
1	
	6 3 3 3 3 4 1 1 8 8 2 2 2 2 2 2 10 10 1

Berdasarkan Tabel 4.9, dapat diketahui bahwa perangkat yang diselidiki dalam kondisi *rooted* serta terdapat kartu SIM namun terdapat kartu *memory* eksternal di

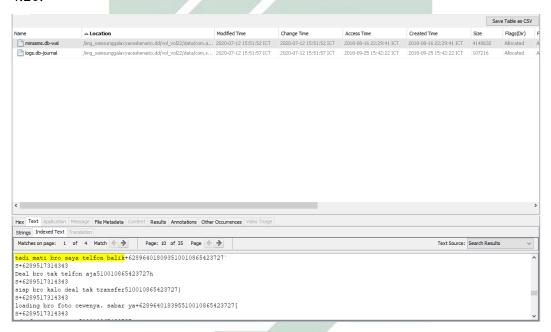
dalamnya. Pada Tabel 4.9 dapat juga diketahui jumlah sumber digital pada perangkat *mobile* sebelum dilakukan *acquisition*

3) Examination dan Analysis

Pada tahap ini dilakukan *examination* dan *analysis* terhadap hasil akuisisi dari *smartphone* Samsung Galaxy Ace 3. Hasil dari tahap *examination* dan *analysis* antara lain:

a. Ditemukan SMS yang dihapus

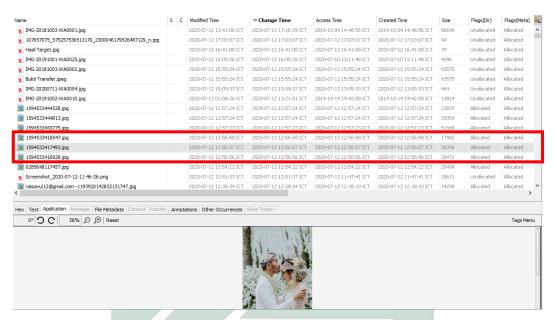
Pada saat melakukan *examination* dan *analysis* ditemukan SMS yang dihapus. Pada *file mmssms.db-wal* ditemukan beberapa SMS yang dapat dilihat pada Gambar 4.21.



Gambar 4.21 SMS yang Dihapus Pada Samsung Galaxy Ace 3

b. Ditemukan Bukti Gambar yang Dihapus

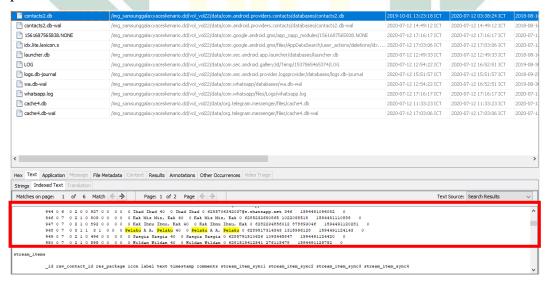
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan beberapa gambar yang dihapus dari *gallery*. Gambar yang dihapus dapat dilihat pada Gambar 4.22.



Gambar 4.22 Bukti Gambar yang Dihapus Pada Samsung Galaxy Ace 3

c. Ditemukan Kontak Telepon Pelaku A yang Dihapus

Pada saaat melakukan proses pemeriksaan dan analisis ditemukan kontak telepon Pelaku A yang dihapus. Kontak telepon Pelaku A yang dihapus dapat dilihat pada Gambar 4.23.



Gambar 4.23 Kontak Telepon Pelaku A yang Dihapus

d. Ditemukan Percakapan WhatsApp yang Dihapus

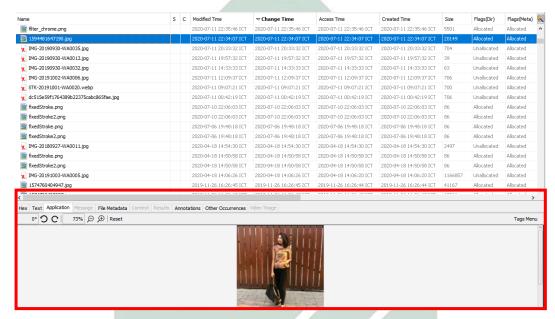
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan percakapan Whatsapp yang dihapus. Percakapan Whatsapp yang dihapus dapat dilihat pada Gambar 4.24.



Gambar 4.24 Percakapan Whatsapp yang Dihapus

e. Ditemukan Pesan Gambar WhatsApp yang Dihapus

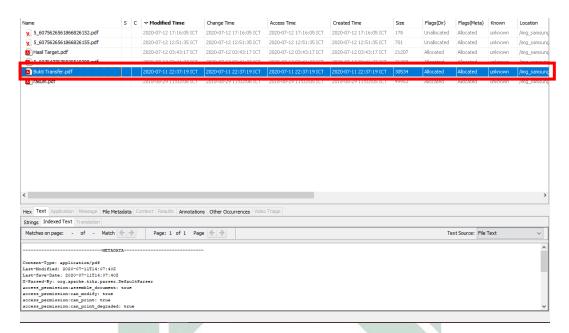
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan pesan gambar Whatsapp yang dihapus. Pesan gambar WhatsApp yang dihapus dapat dilihat pada Gambar 4.25.



Gambar 4.25 Pesan Gambar WhatsApp yang Dihapus

f. Ditemukan Pesan Dokumen WhatsApp yang Dihapus

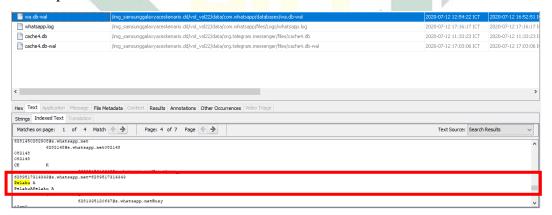
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan pesan dokumen Whatsapp yang dihapus. Pesan dokumen WhatsApp yang dihapus dapat dilihat pada Gambar 4.26.



Gambar 4.26 Pesan Dokumen WhatsApp yang Dihapus

g. Ditemukan Kontak Telepon WhatsApp yang Dihapus

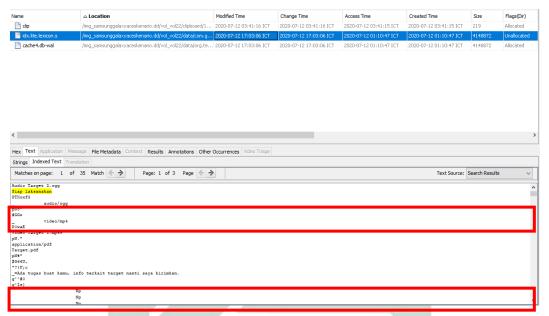
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan kontak telepon Whatsapp yang dihapus. Kontak telepon WhatsApp yang dihapus dapat dilihat pada Gambar 4.27.



Gambar 4.27 Kontak Telepon WhatsApp yang Dihapus

h. Ditemukan Pesan Telegram yang Dihapus

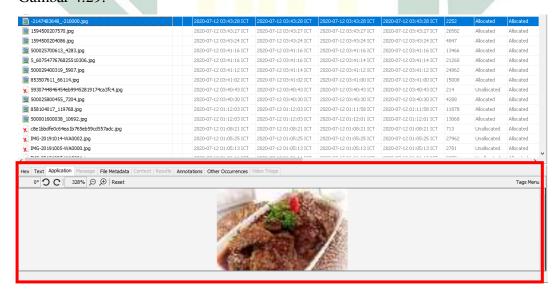
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan pesan Telegram yang dihapus. Pesan Telegram yang dihapus dapat dilihat pada Gambar 4.28.



Gambar 4.28 Pesan Telegram yang Dihapus

i. Ditemukan Pesan Gambar Telegram yang Dihapus

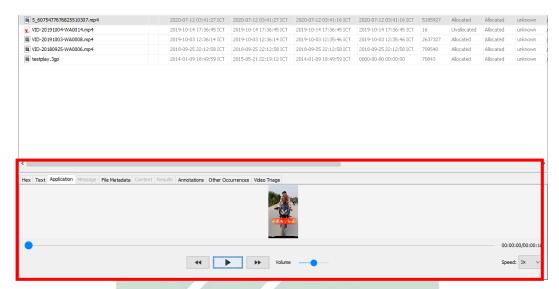
Pada saaat melakukan proses pemeriksaan dan analisis ditemukan pesan gambar Telegram yang dihapus. Pesan gambar Telegram yang dihapus dapat dilihat pada Gambar 4.29.



Gambar 4.29 Pesan Gambar Telegram yang Dihapus

j. Ditemukan Pesan Video Telegram yang Dihapus

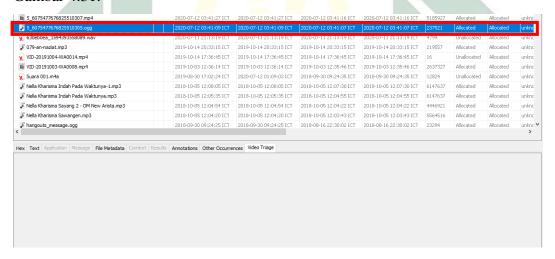
Pada saat melakukan proses pemeriksaan dan analisis ditemukan pesan video Telegram yang dihapus. Pesan video Telegram yang dihapus dapat dilihat pada Gambar 4.30.



Gambar 4.30 Pesan Video Telegram yang Dihapus

k. Ditemukan Pesan Audio Telegram yang Dihapus

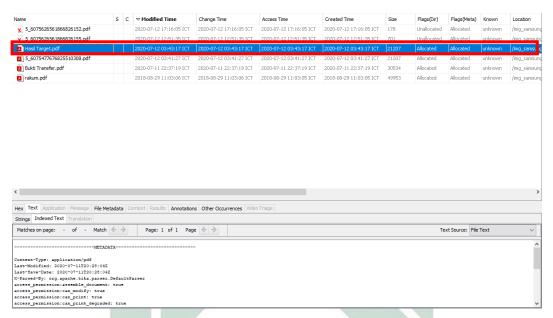
Pada saat melakukan proses pemeriksaan dan analisis ditemukan pesan audio Telegram yang dihapus. Pesan audio Telegram yang dihapus dapat dilihat pada Gambar 4.31.



Gambar 4.31 Pesan Audio Telegram yang Dihapus

l. Ditemukan Pesan Dokumen Telegram yang Dihapus

Pada saat melakukan proses pemeriksaan dan analisis ditemukan pesan dokumen Telegram yang dihapus. Pesan dokumen Telegram yang dihapus dapat dilihat pada Gambar 4.32.



Gambar 4.32 Pesan Dokumen Telegram yang Dihapus

m. Ditemukan Kontak Telepon Telegram yang Dihapus

Pada saat melakukan proses pemeriksaan dan analisis ditemukan kontak telepon Telegram yang dihapus. Kontak telepon Telegram yang dihapus dapat dilihat pada Gambar 4.29.



Gambar 4.33 Kontak Telepon Telegram yang Dihapus

n. Jumlah Data Setelah Dilakukan Examination dan Analysis

Proses *examination* dan *analysis* untuk mengetahui data-data apa saja yang dapat ditemukan dan dipulihkan menggunakan aplikasi Autopsy Adapun hasil *examination* dan *analysis* disajikan pada Tabel 4.10.

I	nformasi Perangkat Selule	er
Nama Pemilik Perangkat	Wanda Nur Rahma	
Nama Perangkat	Samsung Galaxy Ace 3	
Nomor Model	GT-S7270	
Sistem Operasi	Android 4.2.2 (Jelly Bean)	
IMEI	351651060564205	
Kata Sandi atau Pola	Tidak Ada	
Rooted	Rooted	
Memory Eksternal	Ada	
Kartu SIM	Ada	
Sumber Bukti Digital	Data Awal	Data Setelah
SMS	6	6
Gambar	3	3
Video	3	0
Audio	3	0
Dokumen	3	0
Call Log	4	0
Phone Contact	1	1
Whatsapp Messenger		
Pesan	8	3
Retract Message	2	0
Gambar	2	1
Video	2	0
Audio	2	0
Dokumen	2	1
Geo-location	2	0
Call Log	10	0
Phone Contact	1 1	
Telegram	1	
Pesan	4	4
Retract Message	2	0

Secret Chat	2	0
Gambar	2	1
Video	2	1
Audio	2	1
Dokumen	2	1
Geo-location	2	0
Call Log	4	0
Phone Contact	1	1

Berdasarkan Tabel 4.10, ditemukan dan dipulihkan pada *file* dengan *extension* SMS (6), gambar (3), phone contact (1), pesan Whatsapp (3), gambar WhatsApp (1), dokumen Whatsapp (1), phone contact WhatsApp (1), pesan Telegram (4), gambar Telegram (1), video Telegram (1), audio Telegram (1), dokumen Telegram (1), phone contact Telegram (1). Namun pada data yang lain tidak dapat ditemukan atau dipulihkan.

4) Reporting

Tahap terakhir dari analisis digital forensik berdasarkan framework NIST SP-800 101 R1 adalah *reporting*. Adapun Tabel *reporting* dapat dilihat pada Tabel 4.11.

Tabel 4.11 Laporan Digital Forensik Samsung Galaxy ACE 3

Laporan Digital Forensik	
Nomor Laporan	Smartphone - 19-05-2020 - Samsung
	Galaxy Ace 3
Tanggal Laporan	Rabu, 20 Mei 2020
Nomor Kasus	Smartphone-002
Nama Petugas Pemeriksa	Arsyian Aldi Warsito
Nomor Petugas Pemeriksa	H06216005
Tanggal Penerimaan Bukti	Jumat, 10 April 2020
Nama Petugas Penyelidik Kasus	Arsyian Aldi Warsito
Nomor Petugas Penyelidik Kasus	H06216005
Nama Pemilik Perangkat	Arsyian Aldi Warsito
Nama Perangkat	Samsung Galaxy Ace 3
Nomor Model	GT-S7270

IMEI	351651060564205
Deskriptif Kasus	Pemulihan data-data pada perangkat mobile
	yang telah dihapus atau dihilangkan.
Data yang Diajukan	SMS, gambar, video, audio, dokumen, call
	log, kontak telepon, WhatsApp Messenger
	Artifact (pesan, retract message, gambar,
	video, audio, dokumen, geo-location, call
	log dan kontak telepon), Telegram Artifact
	(pesan, retract message, secret chat,
	gambar, video, audio, dokumen, geo-
	location, call log dan kontak telepon).
Peralatan yang Digunakan	1. Magnet Acquire
	2. Autopsy
	3. USB Cable
Detail temuan	1. Ditemukan SMS yang dihapus
	2. Ditemuk <mark>an</mark> Bukti Gambar yang Dihapus
	3. Ditemuk <mark>an</mark> Kontak Telepon Pelaku A
	y <mark>an</mark> g Dih <mark>ap</mark> us
	4. Ditemukan Percakapan WhatsApp yang
	Dihapus
	5. Ditemukan Pesan Gambar WhatsApp
	yang Dihapus
	6. Ditemukan Pesan Dokumen WhatsApp
	yang Dihapus
	7. Ditemukan Kontak Telepon WhatsApp
	yang Dihapus
	8. Ditemukan Pesan Telegram yang
	Dihapus
	9. Ditemukan Pesan Gambar Telegram
	yang Dihapus
	10. Ditemukan Pesan Video Telegram
	yang Dihapus

- 11. Ditemukan Pesan Audio Telegram yang Dihapus12. Ditemukan Pesan Dokumen Telegram yang Dihapus
 - Ditemukan Kontak Telepon
 Telegram yang Dihapus

Berdasarkan Tabel 4.11, dapat diketahui bahwa pada laporan digital forensik terkait *smartphone* Samsung Galaxy Ace 3 yang dianalisis bahwa penerimaan bukti diterima tanggal 10 April 2020. Deskriptif kasus adalah menemukan dan memulihkan data yang diajukan. Data yang diajukan adalah SMS, gambar, video, audio, dokumen, *call log*, kontak telepon, WhatsApp *Messenger Artifact* (pesan, *retract message*, gambar, video, audio, dokumen, *geo-location*, *call log* dan kontak telepon), Telegram *Artifact* (pesan, retract *message*, *secret chat*, gambar, video, audio, dokumen, *geo-location*, *call log* dan kontak telepon). Peralatan yang digunakan selama proses digital forensik adalah aplikasi *magnet acquire* dan Autopsy serta USB *Cable*.

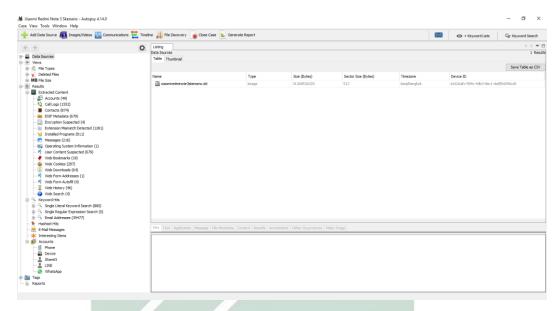
4.4 Analisis Kinerja Aplikasi Autopsy Menggunakan NIST Measurements

Setelah dilakukan digital forensik menggunakan aplikasi Autopsy, dilakukan analisis dari kinerja aplikasi Autopsy berdasarkan NIST *Measurements* yang dibagi menjadi 2 bagian yaitu *core features* dan *optional features* pada objek penelitian yang telah dipersiapkan antara lain:

4.4.1 Xiaomi Redmi Note 3

Kinerja aplikasi Autopsy pada *smartphone* Xiaomi Redmi Note 3 bahwa dapat memenuhi kriteria *variable* sebagai berikut:

a. Memenuhi kriteria *variable* MDT-CR-01 bahwa aplikasi Autopsy dapat mengekstrasi dan menampilkan data pendukung *artifact* dari *image file* yang dapat dilihat pada Gambar 4.34.

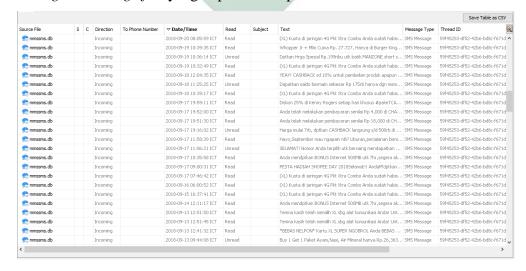


Gambar 4.34 Aplikasi Autopsy Menampilkan Data Pendukung Artifact

b. Memenuhi kriteria variable MDT-CR-02 bahwa aplikasi Autopsy dapat menggabungkan *text* dengan benar yang dapat dilihat pada Gambar 4.35.

Gambar 4.35 Aplikasi Autopsy Menggabungkan dengan Benar

c. Memenuhi kriteria variable MDT-CR-03 serta MDT-CA-11 bahwa aplikasi Autopsy tidak memodifikasi *image file* yang sedang diperiksa dan MDT-CA-04 bahwa aplikasi Autopsy juga dapat menampilan SMS, MMS dan *instant message* dari *image file* yang dapat dilihat pada Gambar 4.36.

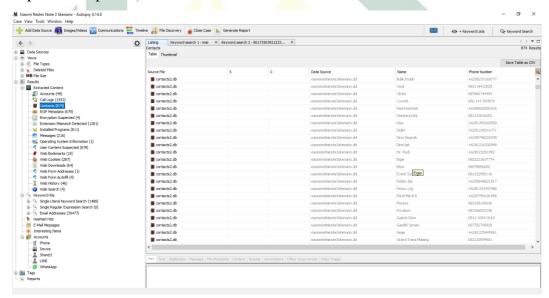


Gambar 4.36 Aplikasi Autopsy Tidak Memodifikasi Image File

d. Memenuhi kriteria variable MDT-CA-01 bahwa aplikasi Autopsy dapat menampilkan informasi pelanggan dan peralatan yang tersedia dari *image file* yang dapat dilihat pada Gambar 4.37.

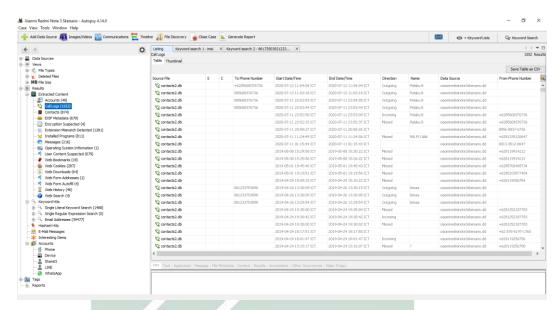
Gambar 4.37 Autopsy Menampilkan Pelanggan dan Peralatan yang Tersedia

e. Memenuhi kriteria variable MDT-CA-02 bahwa aplikasi Autopsy dapat menampilkan PIM (*Personal Information Management*) dari *image file* yang dapat dilihat pada Gambar 4.38.



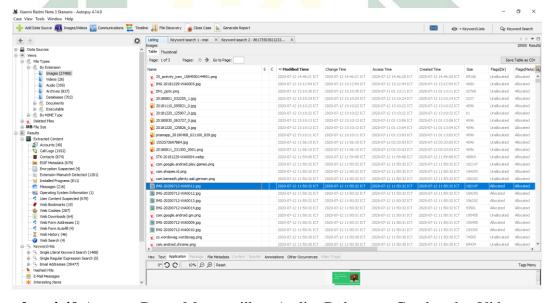
Gambar 4.38 Autopsy Dapat Menampilkan PIM dari Image File

f. Memenuhi kriteria variable MDT-CA-03 bahwa aplikasi Autopsy dapat menampilkan *log* panggilan (*Outgoing, Incoming* dan *Missed Call*) dari *image file* yang dapat dilihat pada Gambar 3.39.



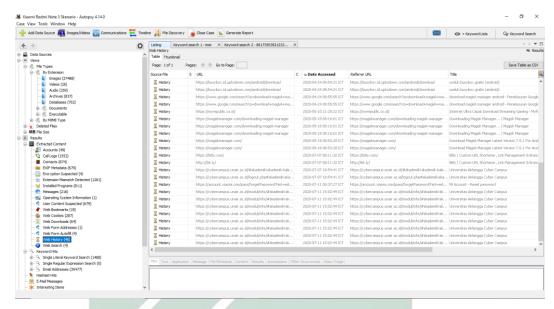
Gambar 4.39 Autopsy Menampilkan Log Panggilan

g. Memenuhi kriteria variable MDT-CA-05 bahwa aplikasi Autopsy dapat menampilan audio, dokumen, gambar dan video dari *image file* yang dapat dilihat pada Gambar 4.40.



Gambar 4.40 Autopsy Dapat Menampilkan Audio, Dokumen, Gambar dan Video

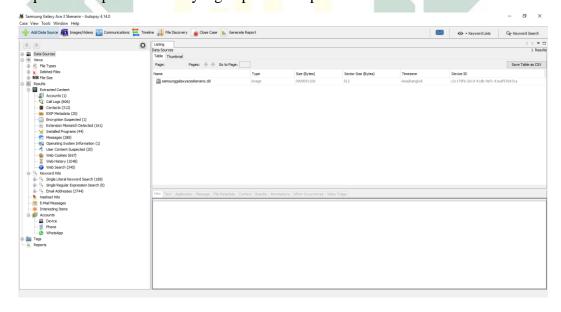
h. Memenuhi kriteria variable MDT-CA-06 bahwa aplikasi Autopsy dapat menampilan *history* dan *bookmarks* dari *image file* yang dapat dilihat pada Gambar 4.41.



Gambar 4.41 Autopsy Menampilkan History dan Bookmarks

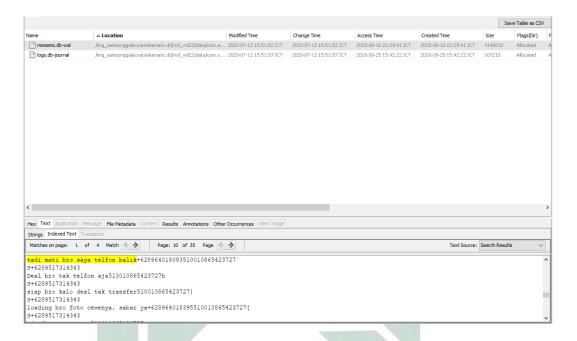
4.4.2 Samsung Galaxy ACE 3

a. Memenuhi kriteria variable MDT-CR-01 bahwa aplikasi Autopsy dapat mengekstrasi dan menampilkan data pendukung artifact dari image file yang dapat dilihat pada Gambar yang dapat dilihat pada Gambar 4.42.



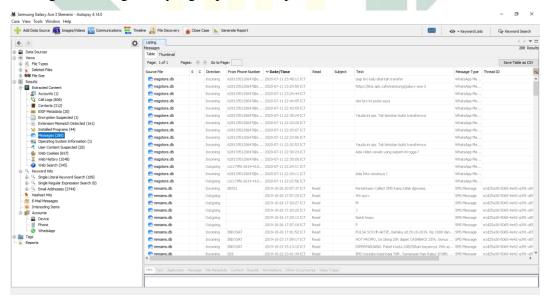
Gambar 4.42 Autopsy Dapat Mengekstrasi Data Pendukung Artifact

b. Memenuhi kriteria variable MDT-CR-02 bahwa aplikasi Autopsy dapat menggabungkan text dengan benar yang dapat dilihat pada Gambar



Gambar 4.43 Autopsy Dapat Menggabungkan Text Dengan Benar

c. Memenuhi kriteria variable MDT-CR-03 serta MDT-CA-11 bahwa aplikasi Autopsy tidak memodifikasi image file yang sedang diperiksa dan MDT-CA-04 bahwa aplikasi Autopsy juga dapat menampilan SMS, MMS dan instant message dari image file yang dapat dilihat pada Gambar 4.44.



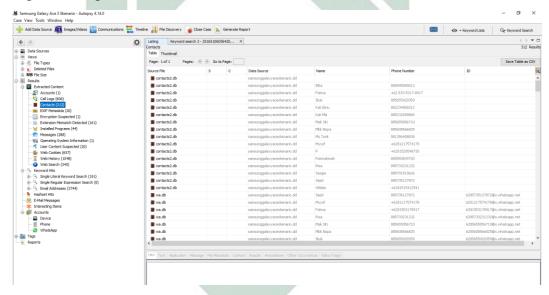
Gambar 4.44 Tidak Memodifikasi Image File dan Dapat Menampilkan Pesan

d. Memenuhi kriteria variable MDT-CA-01 bahwa aplikasi Autopsy dapat menampilkan informasi pelanggan dan peratalan yang tersedia dari image file yang dapat dilihat pada Gambar 4.45.

```
cins names"vifijing temp value" values"5/ />
choolean names"is_force_stop_service" values"false" />
choolean names"is_force_stop_service" values"false" />
choolean names"is_insel_stor_state" values"false" />
cuting names"prinarylp054.165.203.950/spring>
choolean names"is_state_state_values"values"p1/ /-
cins names"counts_values"p1/ /-
cins names"counts_values"p1/ /-
cuting names"prov_server_inddres=7v=nalspaid=164982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=164982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=164982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=164982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=164982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names"pipov_server_inddres=7v=nalspaid=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names=serveringdres=7v=nalspaid=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names=serveringdres=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names=serveringdres=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names=serveringdres=104982029.ap=southeast-1.elb.amasonaws.comc/string>
cins names=104982029.ap=southeast-1.elb.amasonaws.comc
```

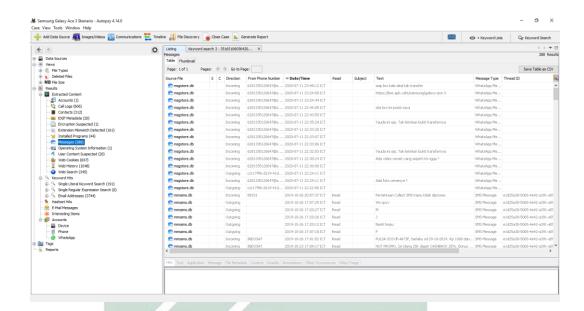
Gambar 4.45 Autopsy Dapat Menampilkan Informasi Pelanggan dan Peralatan

e. Memenuhi kriteria *variable* MDT-CA-02 bahwa aplikasi Autopsy dapat menampilkan PIM (Personal Information Management) dari image file yang dapat dilihat pada Gambar 4.46.



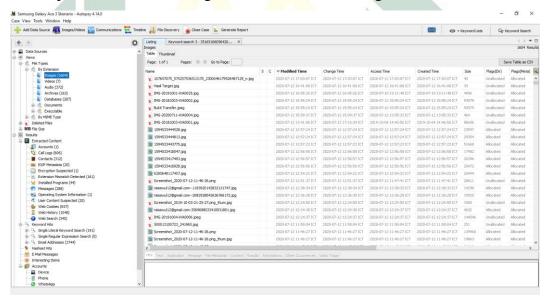
Gambar 4.46 Autopsy Dapat Menampilkan PIM

f. Memenuhi kriteria *variable* MDT-CA-04 bahwa aplikasi Autopsy dapat menampilan SMS, MMS dan *instant message* dari *image file* yang dapat dilihat pada Gambar 4.47.



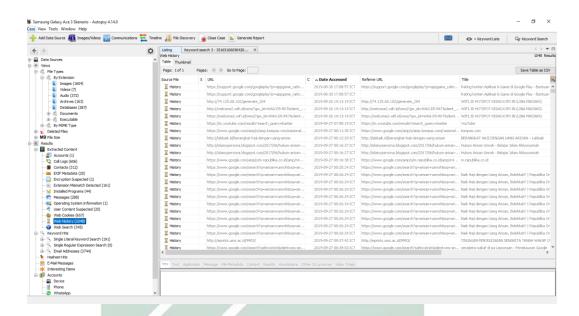
Gambar 4.47 Autopsy Dapat Menampilkan SMS dan Instant Message

g. Memenuhi kriteria variable MDT-CA-05 bahwa aplikasi Autopsy dapat menampilan audio, dokumen, gambar dan video dari image file.



Gambar 4.48 Autopsy Dapat Menampilkan Audio, Dokumen, Gambar dan Video

h. Memenuhi kriteria variable MDT-CA-06 bahwa aplikasi Autopsy dapat menampilan history dan bookmarks dari image file yang dapat dilihat pada gambar 4.49.



Gambar 4.49 Autopsy Dapat Menampilkan History dan Bookmarks

4.4.3 Perhitungan Angka Indeks

Setelah memaparkan hasil kinerja aplikasi Autopsy pada 2 objek penelitian yang telah dipersiapkan, dilakukan perhitungan menggunakan indeks tertimbang berdasarkan Tabel 4.12 yang menunjukan hasil kinerja aplikasi Autopsy menggunakan NIST *Measurements*.

Tabel 4.12 Analisis Aplikasi Autopsy Menggunakan NIST Measurements

Measurement Parameter		Digital Forensik Menggunakan		
			Aplikasi Autopsy	
		Xiaomi Redmi	Samsung Galaxy	
		Note 3	Ace 3	
Core Features	MDT-CR-01	✓	✓	
	MDT-CR-02	✓	✓	
	MDT-CR-03	✓	✓	
	MDT-CR-04	*	*	
	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	×	*
	MDT-CA-10	×	*
	MDT-CA-11	✓	✓
	MDT-CA-12	×	*
Optional Features	MDT-RO-01	×	×
	MDT-RO-02	×	*
	MDT-RO-03	*	*
	MDT-RO-04	×	*
	MDT-RO-05	×	*
	MDT-RO-06	×	*
	MDT-AO-01	×	*
	MDT-AO-02	×	*
	MDT-AO-03	×	×
	MDT-AO-04	×	×
	MDT-AO-05	×	*
	MDT-AO-06	×	*
Dandasankan nada		I laimania amlilaasi As	

Berdasarkan pada Tabel 4.12, hasil kinerja aplikasi Autopsy pada 2 objek penelitian yang telah dipersiapkan yaitu:

a. Terdapat perbedaan hasil dari kedua *smartphone* pada *variable* MDT-CA-03 bahwa aplikasi Autopsy dapat memulihkan *log* panggilan (*outgoing*, *incoming* dan *missed call*) Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy tidak dapat memulihkan *log* panggilan sehingga dapat disimpulkan bahwa aplikasi Autopsy pada Xiaomi Redmi Note 3 dapat memenuhi kriteria *variable* lebih banyak daripada Samsung Galaxy ACE 3. Pada *optional features* aplikasi Autopsy tidak dapat memenuhi semua kriteria *variable* karena aplikasi Autopsy tidak dapat melakukan *acquisition*.

b. Hasil kinerja aplikasi Autopsy pada Xiaomi Redmi Note 3 memenuhi 10 standar pengukuran dari 28 standar pengukuran yang telah ditentukan yaitu dapat mengektrasi data *artifact* dari *image file* (MDT-CR-01), dapat menggabungkan *text* dengan benar (MDT-CR-02), tidak memodifikasi data saat dilakukan pemeriksaan (MDT-CR-03), menampilkan informasi alat dan pelanggan (MDT-CA-01), menampilkan semua *personal information management* (PIM) (MDT-CA-02), menampilkan semua *log* panggilan termasuk *incoming, outgoing* dan *missed* (MDT-CA-03), menampilkan data audio, dokumen, dapat menampilan SMS, MMS dan *instant message* dari *image file* (MDT-CA-04), Gambar dan video (MDT-CA-05), menampilkan *web history* dan *bookmarks* (MDT-CA-06) dan alat ini tidak memodifikasi *image file* (MDT-CA-11). Hasil dari rumus indeks tertimbang untuk kinerja aplikasi *autopsy* berdasarkan NIST *Measurements* adalah 35,7%.

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\%$$

$$\sum Pn = The \ Result \ of \ Data \ Acquisition \ Tools$$

$$\sum Po = The \ Total \ Number \ Of \ Parameters$$

$$Pon = Percentage \ results \ are \ expected$$

$$Hasil \ Prosentase \ Kinerja \ Autopsy = \frac{10}{28} \times 100\% = 35,71\%$$

c. Hasil kinerja aplikasi Autopsy pada Samsung Galaxy Ace 3 memenuhi 9 standar pengukuran dari 28 standar pengukuran yang telah ditentukan yaitu dapat mengektrasi data *artifact* dari *image file* (MDT-CR-01), dapat menggabungkan *text* dengan benar (MDT-CR-02), tidak memodifikasi data saat dilakukan pemeriksaan (MDT-CR-03), menampilkan informasi alat dan pelanggan (MDT-CA-01), menampilkan semua *personal information management* (PIM) (MDT-CA-02), menampilkan data audio, dokumen, dapat menampilan SMS, MMS dan *instant message* dari *image file* (MDT-CA-04), Gambar dan video (MDT-CA-05), menampilkan *web history* dan *bookmarks* (MDT-CA-06) dan alat ini tidak memodifikasi *image file* (MDT-CA-11) yang menjadi perbedaan adalah bahwa pada Samsung Galaxy Ace aplikasi Autopsy tidak dapat menampilkan panggilan (*outgoing*, *incoming* dan *missed call*).

Hasil dari rumus indeks tertimbang untuk kinerja aplikasi Autopsy berdasarkan NIST *Measurements* adalah 32,14%.

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\%$$

$$\sum Pn = \textit{The Result of Data Acquisition Tools}$$

$$\sum Po = \textit{The Total Number Of Parameters}$$

$$Pon = \textit{Percentage results are expected}$$

$$\textit{Hasil Prosentase Kinerja Autopsy} = \frac{9}{28} \times 100\% = 32,14\%$$

4.5 Perbandingan Bukti Digital

Pada tahap ini adalah melakukan perbandingan bukti digital yang telah dipulihkan atau dikembalikan oleh aplikasi Autopsy. Pada Tabel 4.13 dapat dilihat perbedaan bukti digital yang dihasilkan oleh aplikasi Autopsy sebagai berkut:

- a. Pada sumber bukti digital gambar aplikasi Autopsy tidak dapat memulihkan atau mengembalikan gambar Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy dapat mengembalikan atau memulihkan semua gambar yang telah dihapus.
- b. Pada sumber bukti digital *log* panggilan aplikasi Autopsy dapat memulihkan atau mengembalikan semua *log* panggilan Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy tidak dapat mengembalikan atau memulihkan semua *log* panggilan yang telah dihapus.
- c. Pada sumber bukti digital pesan Whatsapp aplikasi Autopsy tidak dapat memulihkan atau mengembalikan semua pesan Whatsapp Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 3 dari 8 pesan Whatsapp yang telah dihapus.
- d. Pada sumber bukti digital dokumen Whatsapp aplikasi Autopsy tidak dapat memulihkan atau mengembalikan semua dokumen Whatsapp Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 1 dari 2 dokumen Whatsapp yang telah dihapus.

- e. Pada sumber bukti digital gambar Telegram aplikasi Autopsy dapat memulihkan atau mengembalikan semua gambar Telegram Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 1 dari 2 gambar Telegram yang telah dihapus.
- f. Pada sumber bukti digital video Telegram aplikasi Autopsy dapat memulihkan atau mengembalikan semua video Telegram Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 1 dari 2 video Telegram yang telah dihapus.
- g. Pada sumber bukti digital audio Telegram aplikasi Autopsy tidak dapat memulihkan atau mengembalikan semua audio Telegram Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 1 dari 2 audio Telegram yang telah dihapus.
- h. Pada sumber bukti digital dokumen Telegram aplikasi Autopsy dapat memulihkan atau mengembalikan semua dokumen Telegram Xiaomi Redmi Note 3 yang telah dihapus, sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 1 dari 2 dokumen Telegram yang telah dihapus.

Tabel 4.13 Perbandingan Bukti Digital

Sumber Bukti	umber Bukti Digital Forensik Menggunakan Aplikasi Autopsy					
Digital	Xiaomi Redmi Note 3		Samsung Galaxy Ace 3			
	Data Awal	Data Setelah	Data Awal	Data Setelah		
Sumber Bukti Digital						
SMS	6	6	6	6		
Gambar	3	0	3	3		
Video	3	0	3	0		
Audio	3	0	3	0		
Dokumen	3	0	3	0		
Call Log	4	4	4	0		
Phone Contact	1	1	1	1		

Whatsapp Messenger					
Pesan	8	0	8	3	
Retract Message	2	0	2	0	
Gambar	2	1	2	1	
Video	2	0	2	0	
Audio	2	0	2	0	
Dokumen	2	0	2	1	
Geo-location	2	0	2	0	
Call Log	10	0	10	0	
Phone Contact	1	1	1	1	
Telegram					
Pesan	4	4	4	4	
Retract Message	2	0	2	0	
Secret Chat	2	0	2	0	
Gambar	2	2	2	1	
Video	2	2	2	1	
Audio	2	0	2	1	
Dokumen	2	2	2	1	
Geo-location	2	0	2	0	
Call Log	4	0	4	0	
Phone Contact	1	1	1	1	
Total	77	24	77	25	

Keterangan:

Data Awal: Data yang telah dipersiapkan sebelum dihapus.

Data Setelah: Data yang telah dihapus dan ditemukan atau dipulihkan menggunakan aplikasi Autopsy.

Berdasarkan Tabel 4.13 dapat disimpulkan hasil perbandingan bukti digital pada 2 objek yang telah dipersiapkan yaitu:

a. Pada Xiaomi Redmi Note 3 aplikasi Autopsy dapat mengembalikan 24 data dari 77 data yang telah dipersiapkan sehingga memperoleh hasil prosentase sebesar 32,16%.

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\%$$

 $\sum Pn = Bukti \ Digital \ yang \ Dapat \ Dipulihkan$

$$\sum Po = Jumlah Bukti Digital$$

Pon = Persentase Kinerja Autopsy

Perhitungan kinerja Autopsy terhadap smartphone Xiaomi Redmi Note 3

$$Pon = \frac{24}{77} \times 100\% = 31,16\%$$

b. Sedangkan pada Samsung Galaxy ACE 3 aplikasi Autopsy dapat mengembalikan 25 data daru 77 data yang telah dipersipakan sehingga memperoleh 32,46%.

Perhitungan kinerja Autopsy terhadap smartphone Samsung Galaxy ACE 3

$$Pon = \frac{25}{77} \times 100\% = 32,46\%$$

BAB V KESIMPULAN

5.1 Kesimpulan

Dari hasil dan pembahasan penelitian yang telah dilakukan dari penelitian ini, dapat disimpulkan bahwa hasil kinerja aplikasi Autopsy pada Xiaomi Redmi Note 3 dan Samsung Galaxy ACE 3 berbeda yaitu:

- a. Hasil kinerja aplikasi Autopsy pada Xiaomi Redmi Note 3 menggunakan NIST *Measurement* hanya memenuhi 10 standar dari 28 standar pengukuran yang telah dipersiapkan dan mendapatkan nilai prosentase sebesar 35,71%. Pada perbandingan bukti digital aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 24 data dari 77 data yang telah dipersiapkan dan mendapatkan nilai prosentase sebesar 31,16%.
- b. Sedangkan hasil kinerja aplikasi Autopsy pada Samsung Galaxy ACE 3 menggunakan NIST *Measurement* hanya memenuhi 9 standar dari 28 standar pengukuran yang telah dipersiapkan dan mendapatkan nilai prosentase 32,14%. Pada perbandingan bukti digital aplikasi Autopsy hanya dapat mengembalikan atau memulihkan 25 data dari 77 data yang telah dipersiapkan dan mendapatkan nilai prosentase sebesar 32,46%.

5.2 Saran

Saran pada penelitian selanjutnya yaitu:

- 1. Disarankan untuk menggunakan menggunakan jenis *smartphone* yang berbeda dari penelitian ini serta versi android yang lebih terbaru atau selain *smartphone* android.
- 2. Disarankan juga untuk menggunakan aplikasi digital forensik yang lain antara berbayar atau tidak berbayar namun tidak *trial version*.

DAFTAR PUSTAKA

- Ajijola, A., Zavarsky, P., Ruhl, R., 2014. A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012, in: World Congress on Internet Security (WorldCIS-2014). Presented at the 2014 World Congress on Internet Security (WorldCIS), IEEE, London, United Kingdom, pp. 66–73. https://doi.org/10.1109/WorldCIS.2014.7028169
- Alfawareh, H.M., Jusoh, S., 2017. The Use and Effects of Smartphones in Higher Education. Int. J. Interact. Mob. Technol. IJIM 11, 103. https://doi.org/10.3991/ijim.v11i6.7453
- Ayers, R., Brothers, S., Jansen, W., 2014. Guidelines on mobile device forensics (No. NIST SP 800-101r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1
- Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A., 2017. Mobile Forensics: Advances, Challenges, and Research Opportunities. IEEE Secur. Priv. 15, 42–51. https://doi.org/10.1109/MSP.2017.4251107
- Kim, D., Lee, Y., Lee, S., 2018. Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices. J. Supercomput. 74, 6618–6632. https://doi.org/10.1007/s11227-017-2205-5
- Mappiwali, H., 2019. Polisi Amankan SPG dan Siswi di Makassar Terkait Prostitusi Online. detikNews.
- Mawardi, I., 2019. Penipu Via Telepon Ditangkap Polisi, Modusnya Ngaku Teman Korban. detikNews.
- Orr, D.A., Castro, A., 2018. Whatsapp Messenger on the Android Platform: A Forensic Examination of a Physical Device. Forensic Sci. Methods Tech. 1, 04–19. https://doi.org/10.33513/FSMT/1801-05
- Riadi, I., Sunardi, Sahiruddin, 2020. Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST. J. Teknol. Inf. Dan Ilmu Komput. 7, 197–204. https://doi.org/DOI: 10.25126/jtiik.202071921
- Riadi, I., Yudhana, A., Putra, M.C.F., 2018. Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ) 4, 9.
- Sidiq, M.F., Faiz, M.N., 2019. Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital. J. Edukasi Dan Penelit. Inform. JEPIN 5, 67. https://doi.org/10.26418/jp.v5i1.31430
- Umar, R., Riadi, I., Maulana, G., 2017. A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements. Int. J. Adv. Comput. Sci. Appl. 8. https://doi.org/10.14569/IJACSA.2017.081210
- Wahid, A.B., 2019. Waspada Grooming! Napi di Surabaya Cabuli 50 Lebih Anak Via Medsos. detikNews.
- Yudhana, A., Riadi, I., Anshori, I., 2019. Identification Of Digital Evidence Facebook Messenger on Mobile Phone With National Institute of Standards Technology (NIST) Method. Kursor 9. https://doi.org/10.28961/kursor.v9i3.152
- Yudhana, A., Riadi, I., Anshori, I., 2018. Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. IT J. Res. Dev. 3, 13–21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658