

**PENERAPAN METODE NATIONAL INSTITUTE OF STANDARDS AND
TECHNOLOGY (NIST) DALAM ANALISIS FORENSIC DIGITAL
UNTUK PENANGANAN CYBER CRIME
DITINJAU DARI ASPEK HUKUM YANG BERLAKU**

SKRIPSI

Diajukan Oleh:

**MULIA FITRIANA
NIM. 150212108**

**Mahasiswa Fakultas Tarbiyah dan Keguruan
Prodi Pendidikan Teknologi Informasi**



**FAKULTAS TARBIYAH DAN KEGURUAN (FTK)
UNIVERSITAS ISLAM NEGERI AR-RANIRY
DARUSALAM- BANDA ACEH
2019 M /1441 H**

**PENERAPAN METODE NATIONAL INSTITUTE OF STANDARDS AND
TECHNOLOGY (NIST) DALAM ANALISIS FORENSIC DIGITAL
UNTUK PENANGANAN CYBER CRIME
DITINJAU DARI ASPEK HUKUM YANG BERLAKU**

SKRIPSI

Diajukan Kepada Fakultas Tarbiyah dan Keguruan (FTK)
Universitas Islam Negeri Ar-Raniry Darussalam Banda Aceh
Sebagai Beban Studi Untuk Memperoleh Gelar Sarjana
Dalam Ilmu Pendidikan Teknologi Informasi

Oleh

MULIA FITRIANA
NIM. 150212108

Mahasiswa Fakultas Tarbiyah dan Keguruan
Prodi Pendidikan Teknologi Informasi

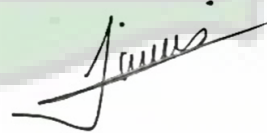
Disetujui Oleh:

Pembimbing I,



Khairan, M.Kom
NIP. 198607042014031001

Pembimbing II,



Jiwa Malem Marsya, M.Sc
NIP.-

**PENERAPAN METODE NATIONAL INSTITUTE OF STANDARDS AND
TECHNOLOGY (NIST) DALAM ANALISIS FORENSIC DIGITAL
UNTUK PENANGANAN CYBER CRIME
DITINJAU DARI ASPEK HUKUM YANG BERLAKU**

SKRIPSI

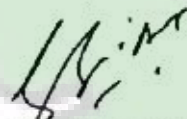
**Telah Diuji Oleh Panitia Ujian Munaqasyah Skripsi
Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry dan Dinyatakan Lulus
Serta Diterima Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
dalam Ilmu Pendidikan Teknologi Informasi**

Pada Hari/Tanggal :

Selasa, 7 Januari 2020 M
11 Jumadil Awal 1441 H

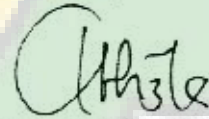
Panitia Ujian Munaqasyah Skripsi

Ketua,



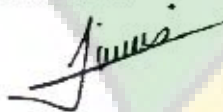
Khairan, M. Kom
NIP. 198607042014031001

Sekretaris,



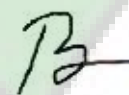
Izzah Al-Fikry, M. Pd

Penguji I,



Jiwa Malem Marsya, M.Sc
NIP.-

Penguji II,



Basrul, MS
NIDN.2027038701

Mengetahui,
Dekan Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry
Darussalam Banda Aceh



Dr. H. Nugraha Razali, M. Ag

NIP. 1989031001

SURAT PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Mulia Fitriana
NIM : 150212108
Prodi : Pendidikan Teknologi Informasi
Fakultas : Tarbiyah dan Keguruan UIN Ar-Raniry
Judul Skripsi : Penerapan Metode *National Institute of Standards and Technology* (NIST) Dalam Analisis *Forensic Digital* Untuk Penanganan *Cybercrime* Ditinjau Dari Aspek Hukum Yang Berlaku.

Dengan ini menyatakan bahwa dalam penulisan skripsi ini:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggung jawabkan.
2. Tidak melakukan plagiat terhadap naskah karya orang lain.
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya.
4. Tidak memanipulasi dan memalsukan data.
5. Mengerjakan sendiri karya ini dan mampu bertanggung jawab atas karya ini.

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggung jawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar persyaratan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh.

Demikian surat pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh, 30 Desember 2019

Yang Menyatakan,



Mulia Fitriana
NTM. 150212108

ABSTRAK

Nama : Mulia Fitriana
NIM : 150212108
Fakultas/Prodi : Tarbiyah dan Keguruan/Pendidikan Teknologi Informasi
Judul : Penerapan Metode *National Institute of Standards and Technology* (NIST) Dalam Analisis *Forensic Digital* Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku
Tanggal Sidang : 7 Januari 2020
Tebal Skripsi : 64 Halaman
Pembimbing I : Khairan, M.Kom
Pembimbing II : Jiwa Malem Marsya, M.Sc
Kata Kunci : Digital Forensik, *Cyber Crime*, WhatsApp Messenger, Prosedur forensik.

Perkembangan teknologi saat ini berkembang dengan sangat pesat, hal ini berbanding lurus dengan meningkatnya tindak kejahatan dunia maya. Salah satu tindak kejahatan yang sering terjadi adalah kasus Pornografi. Kejahatan ini dilakukan dengan memanfaatkan salah satu aplikasi Instant Messenger (IM) yang sangat populer yaitu aplikasi WhatsApp. Namun setelah kejahatan tersebut dilakukan selanjutnya pelaku atau tersangka menghapus barang bukti berupa percakapan, rekaman video, gambar dan lainnya yang dilakukan tersangka menggunakan aplikasi WhatsApp. Oleh karena itu, penelitian ini bertujuan untuk menemukan bukti digital terkait kasus Pornografi. Penelitian ini menghasilkan prosedur forensik dalam melakukan investigasi aplikasi WhatsApp untuk mendapatkan barang bukti yang telah dihapus sebelumnya yang berupa sesi percakapan, daftar nomor kontak, foto profil korban dan lainnya. Penelitian ini dilakukan dengan cara membaca file database backup aplikasi WhatsApp yang terenkripsi yang menyimpan sesi percakapan yang sudah dihapus. Penelitian ini menggunakan metode (*National Institute of Standards and Technology*) (NIST). Bukti digital tersebut dapat diperoleh menggunakan salah satu *tools* forensik yaitu WhtasApp Viewer. Hasil yang didapat pada penelitian ini berupa isi percakapan WhatsApp yang sudah dihapus yang dapat menjadi bukti digital dalam mengungkap tindak kejahatan Pornografi yang terjadi.

KATA PENGANTAR



Alhamdulillah puji dan syukur kepada kehadiran Allah SWT, yang telah memberikan kesehatan dan kekuatan, sehingga penulisan skripsi yang berjudul **“Penerapan Metode *National Institute of Standards and Technology* (NIST) Dalam Analisis *Forensic Digital* Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku”** dapat penulis selesaikan.

Penulisan skripsi ini merupakan salah satu beban studi untuk mendapatkan gelar sarjana pada jurusan Pendidikan Teknologi Informasi Fakultas Tarbiyah dan Keguruan Universitas Islam Negeri Ar-Raniry, Banda Aceh. Penulis berserah diri kepada Allah karena tidak ada yang terjadi tanpa kehendak-Nya. Segala usaha telah dilakukan untuk menyempurnakan skripsi ini. Namun, penulis menyadari dalam penulisan skripsi ini masih banyak ditemukan kekurangan dan kekhilafan. Oleh karena itu, penulis mengharapkan saran dan kritik yang dapat dijadikan masukan guna perbaikan di masa yang akan datang sehingga akhirnya skripsi ini dapat dikembangkan lebih lanjut lagi. Semoga Allah SWT meridhai penulisan ini dan senantiasa memberikan rahmat dan hidayah-Nya kepada kita semua. Amin ya rabbal alamin. Pada kesempatan ini penulis mengucapkan ribuan terima kasih kepada :

1. Terima kasih kepada Allah SWT, dan kepada Baginda Nabi Besar Muhammad SAW.

2. Terima kasih kepada orang tua dan keluarga yang selalu mendoakan dan memberi dukungan tiada henti dari awal hingga akhir.
3. Terima kasih kepada Bapak Yusran M.Pd. selaku ketua pada Program Studi Pendidikan Teknologi Informasi, yang selalu memberikan arahan dan semangat dari awal sampai akhir untuk menggarap skripsi agar selesai tepat pada waktunya.
4. Terima kasih kepada Bapak Khairan, M.Kom. selaku pembimbing pertama dan Bapak Jiwa Malem Marsya, M.Sc selaku pembimbing kedua, yang telah meluangkan waktunya dan mencurahkan pemikirannya dalam membimbing penulis untuk menyelesaikan karya ilmiah ini.
5. Terima kasih kepada CCI, Unit 03, dan teman-teman mahasiswa Jurusan Pendidikan Teknologi Informasi leting 2015 serta seluruh keluarga PTI yang telah mendoakan dan memberi dukungan selama ini.

Banda Aceh, 25 Desember 2019
Penulis,

Mulia Fitriana

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
PENGESAHAN PEMBIMBING.....	ii
PENGESAHAN SIDANG	iii
SURAT PERNYATAAN	iv
ABSTRAK	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN.....	1
A. Latar Belakang.....	1
A. Rumusan Masalah	7
B. Tujuan Penelitian.....	7
C. Manfaat Penelitian.....	7
D. Batasan Masalah.....	8
BAB II KAJIAN PUSTAKA.....	10
A. Penelitian Terdahulu.....	10
B. Definisi Analisis	14
C. Digital Forensik.....	15
D. Mobile Forensik.....	16
E. <i>Cyber Crime</i>	17
F. Data Recovery	19
G. KingRoot	19
H. Flashify.....	20
I. CWM Recovery.....	21
J. WhatsApp Viewer	21

K. DB Browser for SQLite.....	22
L. FTK Imager	22
M. <i>National Institute of Standards and Technology</i> (NIST).....	23
N. WhatsApp.....	24
O. Pornografi.....	25
P. Penegakan Hukum Pidana	27
BAB III METODOLOGI PENELITIAN	30
A. Prosedur Penelitian.....	30
B. Metode Penelitian.....	31
C. Rancangan Skenario	34
D. Alat dan Bahan Penelitian	37
BAB IV HASIL DAN PEMBAHASAN	39
A. <i>Collection</i> (Pengumpulan)	40
B. <i>Examination dan Analysis</i>	49
C. <i>Reporting</i> (Laporan).....	58
D. Analisa Hukum Berdasarkan Barang Bukti yang telah di skenariokan.....	60
BAB V KESIMPULAN DAN SARAN	64
A. Kesimpulan.....	64
B. Saran.....	65
DAFTAR PUSTAKA.....	66
LAMPIRAN-LAMPIRAN	68

DAFTAR GAMBAR

Gambar 3.1	Prosedur Penelitian.....	29
Gambar 3.2	Tahapan Metode NIST	31
Gambar 3.3	Flowchart Analisis Aplikasi WhatsApp	35
Gambar 3.4	Proses Menggunakan Metode NIST.....	36
Gambar 4.1	Proses Skenario dari Akun A kepada Akun B.....	38
Gambar 4.2	Screenshots percakapan yang telah dihapus.....	39
Gambar 4.3	Proses Rooting Smartphone	40
Gambar 4.4	Spesifikasi Smartphone yang digunakan.....	41
Gambar 4.5	File CWM Recovery.....	43
Gambar 4.6	Halaman Utama Aplikasi Flashify	43
Gambar 4.7	Proses Instalasi CWM Recovery	44
Gambar 4.8	Mode pada CWM Recovery.....	45
Gambar 4.9	Proses Backup data dengan CWM Recovery	46
Gambar 4.10	Halaman utama aplikasi FTK Imager.....	47
Gambar 4.11	Proses <i>Imaging</i> data dengan FTK Imager	48
Gambar 4.12	Proses Ekstraksi File data.ext4.tar.....	49
Gambar 4.13	Hasil Ekstraksi data.ext4.tar	49
Gambar 4.14	Struktur Folder com.whatsapp.....	50
Gambar 4.15	Struktur Folder WhatsApp	51
Gambar 4.16	Data di Folder WhatsApp.....	52
Gambar 4.17	Halaman utama Aplikasi WhatsApp Viewer	53
Gambar 4.18	Proses Deskripsi Database WhatsApp menggunakan aplikasi WhatsApp Viewer	53
Gambar 4.19	Database WhatsApp berhasil di dekripsi.....	54
Gambar 4.20	File Database yang sudah terdekripsi	54
Gambar 4.21	Proses membuka Database WhatsApp yang sudah didekripsi.....	55
Gambar 4.22	Contoh chat WhatsApp yang didapatkan	56
Gambar 4.23	Percakapan pada database terdekripsi di Export ke format html ..	57

Gambar 4.24 Foto Profil dari kontak pengguna WhatsApp..... 57
Gambar 4.25 Isi file wa.db yang merupakan kontak pada smartphone 59



DAFTAR TABEL

Tabel 3.1	Alat dan Bahan Penelitian	36
Tabel 4.1	Tempat Penyimpanan Folder WhatsApp dan folder com.whatsapp ..	50
Tabel 4.2	Laporan Barang Bukti yang berhasil didapatkan	58



DAFTAR LAMPIRAN

Lampiran 1 : Sk Pembimbing Skripsi

Lampiran 2 : Surat Izin Penelitian

Lampiran 3 : Dokumentasi Penelitian



BAB I

PENDAHULUAN

A. Latar Belakang

Di abad 21 ini perkembangan teknologi telah mengalami kemajuan yang sangat pesat. Namun perkembangan yang demikian, ternyata diikuti pula dengan berkembangnya sisi negatif dari penggunaan teknologi yang mengarah pada tindakan-tindakan kejahatan yang dilakukan menggunakan komputer, kejahatan pada dunia maya ini dikenal dengan istilah *Cyber Crime*. *Cyber Crime* merupakan suatu kejahatan yang dilakukan dengan menjadikan komputer atau jaringan komputer sebagai alat, sasaran dan tempat terjadinya kejahatan, termasuk di dalamnya adalah pornografi anak, penipuan secara online, pembulian, penipuan identitas, dan lain-lain.¹ Berdasarkan informasi dalam *Internet Security Threat Report* volume 17 dari perusahaan keamanan *Symantec*, sepanjang tahun 2011 Indonesia adalah negara yang aktivitas kejahatan *cyber* terbanyak dengan menempati peringkat 10. Indonesia menyumbang 2,4% kejahatan *cyber* di dunia.² Kapolri Jenderal Polisi Tito Karnavian mengatakan jumlah kasus yang menyangkut dengan kejahatan

¹Muhammad sobri dkk, *Pengantar Teknologi Informasi – Konsep dan Teori*, (Yogyakarta: CV.Andi Offset, 2017) hal. 217.

²Christiany Juditha (2015), *Pola Komunikasi dalam Cybercrime (Kasus Love Scams)*, Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika Vol.6, No.2, hal.30.

dunia maya atau *Cyber Crime* mengalami peningkatan. Pada tahun 2016 kejahatan *Cyber Crime* yang ditangani oleh Polri sebanyak 4.931 kasus, kemudian mengalami peningkatan menjadi 5.061 kasus pada tahun 2017. Namun tidak semua kasus *Cyber Crime* dapat terselesaikan. Pada tahun 2016 sebanyak 1.119 kasus kejahatan *Cyber Crime* yang terselesaikan, dan pada tahun 2017 hanya 1.369 kasus yang berhasil diselesaikan. Kejahatan *Cyber Crime* yang sering terjadi adalah kasus ujaran kebencian yaitu sebanyak 1.829 kasus dan meningkat drastis menjadi 3.325 kasus pada tahun 2017.³ Komisaris Jenderal Syafruddin yaitu Wakil Kepala Kepolisian Republik Indonesia menegaskan bahwa Indonesia masuk dalam jajaran dua besar negara di dunia dengan kejahatan dunia maya, Indonesia merupakan negara dengan kasus *Cyber Crime* tertinggi ke dua di dunia setelah negara Jepang.⁴

Aceh merupakan daerah yang banyak menyediakan fasilitas internet sehingga jaringannya sangat mudah untuk diakses, seperti di kantor, kampus, warung kopi, dan layanan publik. Namun dengan ketersediaan internet disetiap sudutnya berpeluang menjadi sasaran dan tujuan untuk tindakan

³Ambaranie Nadia Kemala Movanita, 2017: *Ini Hasil Kerja Polri Perangi Kejahatan Kejahatan Cyber Sepanjang 2017*, diakses pada tanggal 13 Agustus 2019, pukul 23:29 WIB, <https://nasional.kompas.com/read/2017/12/29/17233911/ini-hasil-kerja-polri%20perangi-kejahatan-siber-sepanjang-2017>.

⁴Ramadhan Rizki, 2018: *Polri:Indonesia Tertinggi Kedua Kejahatan Siber di Dunia*, diakses pada tanggal 19 Agustus 2019, pukul 11:02 WIB, <https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia>.

kejahatan *Cyber Crime*.⁵ Beberapa kasus *Cyber Crime* telah ditemukan di Aceh, seperti yang beritakan oleh surat kabar (koran) *Oke Nasional*, sepanjang 2017 Polda Aceh menangani tiga kasus kejahatan *Cyber Crime*, satu kasus dengan konten pornografi dan dua perkara kasus penghinaan dan pencemaran nama baik, berdasarkan hasil wawancara yang peneliti lakukan dengan salah satu tim *Cyber Crime* Polda Aceh, beliau mengatakan bahwa ditahun 2019 Polda Aceh berhasil menangani dan menyelesaikan sebanyak 37 kasus yang menyangkut tentang *Cyber Crime*. Selain itu kasus *Cyber Crime* juga terjadi di kabupaten aceh timur berdasarkan informasi yang diberitakan oleh surat kabar (koran) *Serambi News*, dari 560 kasus yang ditangani oleh Polres Aceh Timur selama 2018, ada delapan kasus yang paling menonjol, salah satunya adalah kasus kejahatan dunia maya atau *Cyber Crime* sebanyak 9 kasus. Berdasarkan paparan permasalahan diatas, dibutuhkan sebuah teknik yang mampu mencari dan menemukan bukti digital forensik untuk menangani kasus *Cyber Crime*, untuk mendapatkan bukti digital maka peneliti akan melakukan simulasi dengan memanfaatkan aplikasi Instant Messenger WhatsApp menggunakan metode *National Institute of Standards and Technology* (NIST) dan beberapa *tools* sebagai alat bantu untuk menemukan bukti digital forensik.

⁵Jurnal JH, 2014: 'Cybercrime' Kejahatan Baru di Aceh, diakses pada tanggal 15 Agustus 2019, pukul 19:27 WIB.

Pemanfaatan metode *National Institute of Standards and Technology* (NIST) ini juga pernah dilakukan pada beberapa penelitian, seperti penelitian yang dilakukan oleh Muhammad Irwan Syahib, Imam Riadi, dan Rusydi Umar yaitu “Analisis Forensik Digital Aplikasi Beetalk untuk Penanganan *Cyber Crime* Menggunakan Metode NIST”. Namun pada penelitian yang mereka lakukan aplikasi yang digunakan adalah Beetalk untuk mensimulasikan prostitusi online melalui handphone android.

Adapun pemanfaatan Aplikasi Instant Messenger WhatsApp juga terdapat pada penelitian lain yaitu penelitian yang dilakukan oleh Imam Riadi, Sunardi, dan Muhammad Ermansyah Rauli dengan judul “Identifikasi Bukti Digital WhatsApp pada Sistem Operasi *Proprietary* Menggunakan *Live Forensics*”. Namun pada penelitian ini metode yang digunakan adalah metode Ravneet Kaur dan Amandeep Kaur yang meliputi beberapa tahapan yaitu *Preservation, Collection, Examination* dan *Analysis* dengan mensimulasikan kasus penipuan online shop berupa percakapan menggunakan WhatsApp berbasis Dekstop dan WhatsApp berbasis Android.

Pemanfaatan metode *National Institute of Standards and Technology* (NIST) ini juga pernah dilakukan pada penelitian lain yaitu penelitian yang dilakukan oleh Imam Riadi, Anton Yudhana, Muhamad Caesar Febriansyah Putra dengan judul “Analisis Recovery Bukti Digital Instagram Messenger Menggunakan Metode *National Institute of Standards and Technology*

(NIST). Dengan memanfaatkan salah satu Instant Messenger yaitu aplikasi instagram untuk mensimulasikan kasus pornografi.

Metode yang digunakan dalam penelitian ini adalah metode *National Institute of Standards and Technology* (NIST). Metode ini digunakan untuk mengetahui langkah-langkah dan alur penelitian secara sistematis, dan menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang terjadi. Metode ini memiliki beberapa tahapan yaitu *Collection*, *Examination*, *Analysis* dan *Reporting*. Pada Penelitian ini kasus yang akan disimulasikan adalah penyebaran Pornografi, Aplikasi Instant Messenger yang digunakan untuk mensimulasikan dua kasus tersebut adalah aplikasi WhatsApp. WhatsApp merupakan salah satu aplikasi Instan Messenger yang sangat populer dan bisa digunakan pada smartphone dan komputer. WhatsApp memiliki banyak fitur seperti telepon, pengiriman pesan, group chat, pengiriman file, video call, dan pesan suara. Di Indonesia Whatsapp berada di peringkat kedua sebagai salah satu media sosial yang di minati masyarakat setelah Youtube. Menurut data Statista, hingga bulan desember 2017 jumlah pengguna aktif WhatsApp diseluruh dunia sebanyak 1,5 miliar. Jumlah tersebut mengalami peningkatan dibandingkan jumlah pengguna WhatsApp

pada bulan januari 2017 sebanyak 1,2 miliar.⁶ Maka dapat diambil suatu kesimpulan bahwa banyaknya pengguna memungkinkan WhatsApp dijadikan sebagai media untuk tindakan kejahatan *Cyber Crime*, kejahatan *Cyber Crime* setiap tahunnya mengalami peningkatan. Hal ini tidak seharusnya terjadi karena di Indonesia dasar hukum pidana untuk kejahatan *Cyber Crime* sudah tertera dalam undang-undang no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisi tentang ketentuan pidana bagi pelaku *Cyber Crime*. Meskipun sudah ditetapkan di dalam undang-undang, pelaku kejahatan *Cyber Crime* ini tetap melakukan aksinya secara terus menerus. Untuk itu penting dilakukan penelitian ini karena kasus *Cyber Crime* merupakan bagian dari tindak pidana dan dapat dijadikan barang bukti untuk di bawa ke pengadilan.

Oleh karena itu penelitian ini dilakukan dengan harapan dapat membantu pihak yang berwajib menemukan bukti forensik untuk menyelesaikan kasus *Cyber Crime* yang terjadi pada media sosial khususnya aplikasi WhatsApp. Adapun penelitian ini diberi judul “**Penerapan Metode *National Institute of Standards and Technology (NIST)* Dalam Analisis *Forensic Digital* Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku**”.

⁶Imam Riadi dkk (2018), *Indetifikasi Bukti Digital WhatsApp Pada Sistem Operasi Proprietary Menggunakan Live Forensics*, Jurnal Teknik Elektro, Vol. 10, No. 1, hal. 18.

A. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka dapat dirumuskan permasalahan dalam penelitian ini yaitu sebagai berikut:

1. Bagaimana menemukan bukti digital kasus kejahatan *Cyber Crime* yang dapat dijadikan barang bukti tindak pidana?

B. Tujuan Penelitian

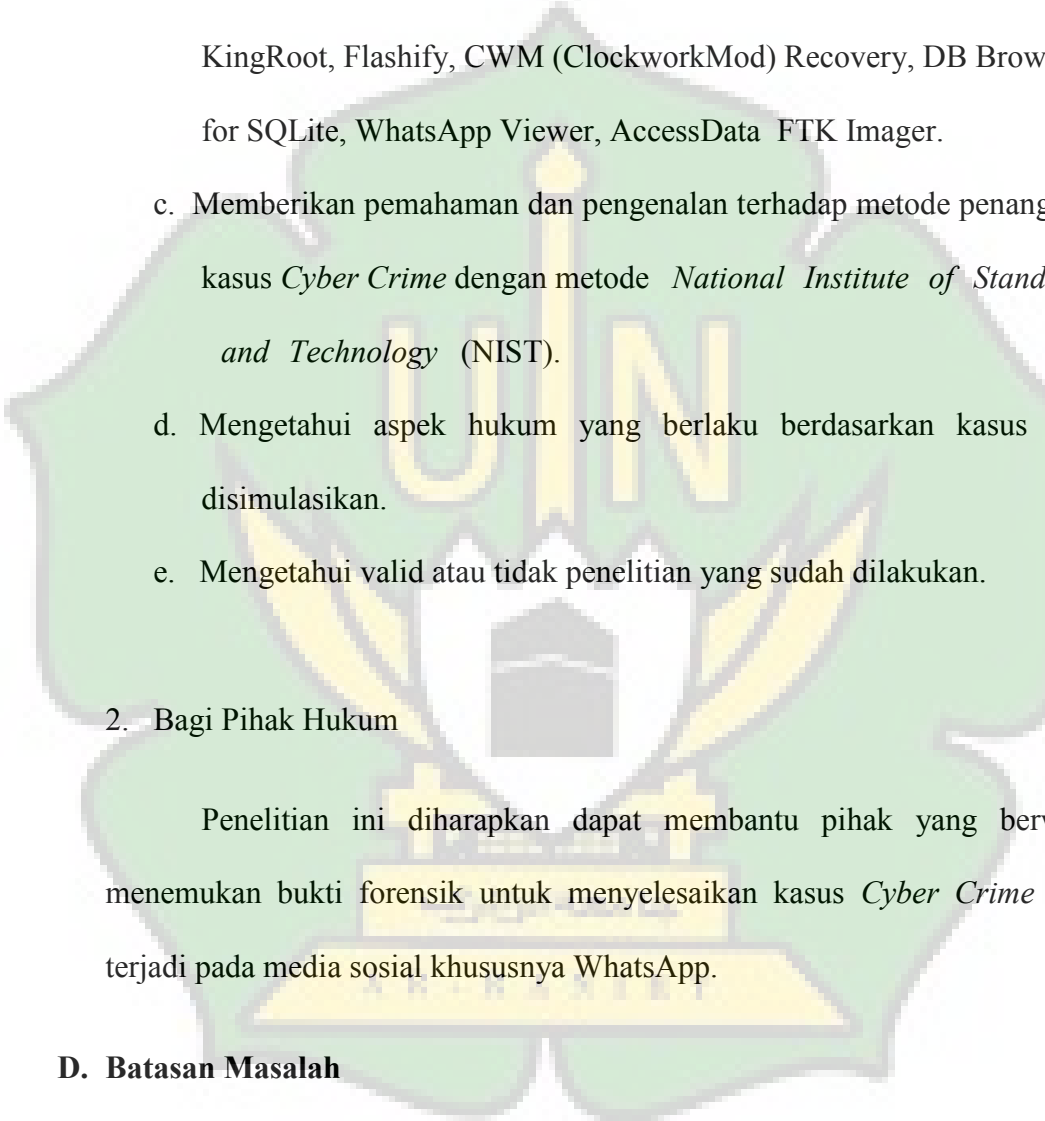
Berdasarkan rumusan masalah yang telah diuraikan diatas, maka tujuan yang hendak dicapai dari penelitian ini adalah:

1. Menerapkan metode *National Institute of Standards and Technology* (NIST) untuk menemukan barang bukti kejahatan *Cyber Crime* pada smartphone yang dapat dijadikan barang bukti tindak pidana.
2. Menentukan *tools forensic* yang dapat digunakan untuk membantu menemukan barang bukti kejahatan *Cyber Crime* pada smartphone.
3. Menentukan aspek hukum yang berlaku berdasarkan kasus yang disimulasikan.
4. Melakukan validasi hasil penelitian kepada ahli hukum.

C. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Bagi Peneliti

- 
- a. Menambah pengetahuan dan lebih memahami ilmu forensik khususnya *mobile forensic* pada smartphone bersistem android.
 - b. Memberikan pemahaman dalam penggunaan tools forensik khususnya, KingRoot, Flashify, CWM (ClockworkMod) Recovery, DB Browser for SQLite, WhatsApp Viewer, AccessData FTK Imager.
 - c. Memberikan pemahaman dan pengenalan terhadap metode penanganan kasus *Cyber Crime* dengan metode *National Institute of Standards and Technology* (NIST).
 - d. Mengetahui aspek hukum yang berlaku berdasarkan kasus yang disimulasikan.
 - e. Mengetahui valid atau tidak penelitian yang sudah dilakukan.

2. Bagi Pihak Hukum

Penelitian ini diharapkan dapat membantu pihak yang berwajib menemukan bukti forensik untuk menyelesaikan kasus *Cyber Crime* yang terjadi pada media sosial khususnya WhatsApp.

D. Batasan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan di atas, maka permasalahan dibatasi pada:

1. Analisis kejahatan digital yang dilakukan hanya pada smartphone Lenovo Model A369i.
2. Analisis kejahatan digital yang dilakukan hanya pada aplikasi sosial media WhatsApp.
3. Pengembalian barang bukti digital hanya berupa percakapan, dan menampilkan daftar kontak baik pengguna WhatsApp maupun yang tidak terdaftar pada aplikasi WhatsApp.
4. Menggunakan *tools* KingRoot, Flashify, CWM (ClockworkMod) Recovery, DB Browser for SQLite, WhatsApp Viewer, AccessData FTK Imager, .
5. Metode yang digunakan adalah *National Institute of Standards and Technology* (NIST).
6. Aspek hukum yang dijelaskan hanya pada kasus Pornografi yang telah disimulasikan.
7. Pemulihan bukti digital tidak pada semua kasus *Cyber Crime*, akan tetapi hanya pada kasus penyebaran pornografi.

BAB II

KAJIAN PUSTAKA

A. Penelitian Terdahulu

Beberapa penelitian serupa sudah pernah dilakukan yaitu penelitian yang dilakukan oleh Ikhwan Anshori, dkk (2018) yang berjudul Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. Metode yang digunakan pada penelitian ini adalah metode NIST (*National Institute of Standards and Technology*) untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital. Sedangkan alat bantu atau *tools* yang digunakan adalah Oxygen Forensik.

Imam Mahfudl Nasrulloh, dkk (2018) yang berjudul Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ). Penelitian ini menggunakan metode dari National Institute of Justice (NIJ). Metode ini digunakan untuk mengetahui langkah-langkah dan alur penelitian secara sistematis, dan menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang terjadi. Berdasarkan hasil dari penelitian yang telah dilakukan pada implementasi salah satu software pembeku drive yaitu Shadow Defender yang dapat membekukan suatu drive SSD (frozen solid state drive) dan terbukti berpengaruh terhadap praktik eksaminasi dan

analisa forensik terhadap didapatkannya bukti-bukti digital. Tidak semua file dapat direstor dengan baik karena struktur file dan data sudah rusak, serta catatan pengguna komputer (recent activity) dan sejarah internet (history internet) tercatat ketika fitur pembeku drive diaktifkan.

Ammar Fauzan, dkk (2016) yang berjudul Analisis Forensik Digital Pada Line Messenger Untuk Penanganan *Cyber Crime*. Dalam penelitiannya Amar Fauzan melakukan penelitian dengan beberapa langkah, yaitu *Preservation, Collection, Examination*, dan langkah terakhir adalah *Analysis*. Proses investigasi dilakukan pada perangkat pelaku. Proses pengumpulan data atau *Collection* diawali dengan melakukan rooting pada smartphone menggunakan bantuan dari tool Zefone RootKit yang bertujuan untuk mempermudah pengangkatan data-data yang ada di dalam perangkat Android. Kemudian perangkat Android yang telah di-root, direcovery menggunakan tool AFLogical atau Kamas Lite. Hasil yang diharapkan adalah data-data yang direcovery dapat menunjukkan file percakapan pada aplikasi Line yang berupa teks maupun gambar.

Muhammad Irwan Syahib, dkk (2018) yang berjudul Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan *Cyber Crime* Menggunakan Metode NIST. Penelitian ini mengimplementasikan metode analisa forensik dari *National Institute of Standards and Technology* (NIST). Metode ini bermanfaat untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan. Pada penelitian ini, proses backup data pada smartphone dilakukan

dengan menggunakan MOBILedit Forensik. Hasil yang diharapkan dari penelitian ini adalah proses analisis bisa berjalan dengan baik dan mendapatkan barang bukti digital dari aplikasi Beetalk pada smartphone Android yang digunakan sebagai objek penelitian.

Muhamad Caesar Febriansyah Putra, dkk (2017) yang berjudul Analisis Recovery Bukti Digital Instagram Messenger Menggunakan Metode *National Institute of Standards and Technology* (NIST). Proses pengumpulan data atau *Collection* diawali dengan melakukan *rooting* pada smartphone menggunakan *tool* KingRoot Rooting Application untuk mempermudah pengangkatan data-data yang ada di dalam perangkat Android. Pada tahap *Examination* perangkat android yang berhasil di root kemudian data akan dijadikan bukti digital berupa (Pesan dan Gambar) yang dihapus akan direcovery menggunakan *tool* Android Data Recovery dari aplikasi instagram. Penelitian yang dilakukan masih dalam proses dikerjakan pada proses analisis forensik yang dilakukan untuk kasus cyber pornografi pada aplikasi Instagram.

Muhamad Ermansyah Rauli (2018) yang berjudul Identifikasi Bukti Digital WhatsApp pada Sistem Operasi *Proprietary* Menggunakan *Live Forensics*. Penelitian ini dilakukan dengan menggunakan sebuah laptop Sistem Operasi Windows 8.1 64 Bit yang sudah terpasang aplikasi IM WhatsApp berbasis dekstop versi 0.2.8691. Penggunaan teknik live forensics

dilakukan untuk mendapatkan bukti digital percakapan WhatsApp yang terdapat pada RAM. *Tools* live forensics yang digunakan pada penelitian ini adalah FTK Imager. Hasil dari penelitian ini berupa bukti digital yang diperoleh berupa teks percakapan WhatsApp yang terjadi antara tersangka dan korban yang dapat dijadikan bukti digital terkait kasus tindak kejahatan penipuan online shop yang terjadi.

Agung Purnama Saputra (2017) yang berjudul Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba). Steganografi merupakan suatu metode yang digunakan untuk menyembunyikan suatu pesan didalam pesan yang lain dalam bentuk media digital. Penelitian ini mengambil contoh kasus berkas informasi dari tersangka yang telah disembunyikan menggunakan teknik steganografi dan kemudian dilakukan sebuah analisa tentang isi berkas dan jenis ekstensi berkas yang digunakan, dengan menggunakan beberapa bantuan *tools* yaitu FTK Imager, WinHex, dan Simple Steganalisis.

Hongmei Chi (2018) yang berjudul Analysis of Encrypted Instant Messaging Applications on Android. Penelitian ini bertujuan untuk menganalisis aplikasi Instant Messaging (IM) terenkripsi yang banyak digunakan yaitu WeChat, Telegram, Viber dan Whatsapp sekaligus menunjukkan bagaimana aplikasi ini menyimpan data dalam sistem file Android. *Tools* yang digunakan dalam penelitian ini adalah Android

Debugging Bridge (ADB), WhatsApp KeyDB Extractor, WhatsApp Viewer Dan SQLiteSpy.

Lijun Zhang (2016) yang berjudul Analisis Forensik Pesan WeChat. Penelitian ini bertujuan untuk mempelajari teknik forensic data pesan WeChat termasuk identifikasi lokasi penyimpanan dan metode ekstraksi informasi. Karena pesan teks disimpan dalam basis data SQLite terenkripsi, Maka penelitian ini menganalisis algoritma kriptografi, dll. Selain itu penelitian ini juga mengusahakan pemulihan data suara dan pesan yang dihapus yang akan membantu dalam forensik data untuk investigasi kriminal.

Qingzhong Liu (2018) yang berjudul Digital Forensic Analysis of Instant Messaging Applications on Android Smartphone. Penelitian ini menggunakan dua smartphone dengan merek berbeda dan sistem operasi Android terbaru sebagai objek eksperimen. Kemudian mereka merangkum temuan mengenai berbagai mode obrolan Pesan Instan dan status enkripsi artefak yang sesuai untuk masing-masing dari empat aplikasi yang diuji.

B. Definisi Analisis

Analisis adalah bagian yang penting dari tradisi berpikir sehingga hampir seluruh sistem pendidikan tinggi diarahkan untuk mengembangkan keterampilan menganalisis. Tidak diragukan lagi, analisis memang bagian “berpikir” yang sangat penting. Melalui analisis, kita membagi-bagi situasi yang rumit menjadi bagian-bagian yang lebih mudah ditangani. Melalui

analisis, kita menemukan sebab suatu masalah dan menyingkirkannya.⁷ Menurut Wiradi, analisis adalah aktivitas yang memuat sejumlah kegiatan seperti mengurai, membedakan, memilah sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditafsir maknanya.⁸

Maka berdasarkan pengertian diatas dapat ditarik kesimpulan bahwa analisis adalah suatu kegiatan berfikir dengan tujuan menyelidiki suatu masalah untuk mengetahui lebih detail mengenai masalah tersebut serta mencari jalan keluarnya.

C. Digital Forensik

Menurut Deris Stiawan (2006) dalam bukunya yang berjudul *Sistem Keamanan Komputer*, mendefinisikan Komputer Forensik adalah suatu disiplin ilmu baru dalam keamanan komputer yang membahas atas temuan bukti digital setelah suatu peristiwa keamanan komputer terjadi. Komputer forensik akan melakukan analisa penyelidikan secara sistematis dan harus menemukan bukti pada suatu sistem digital yang nantinya dapat dipergunakan

⁷ Edward De Bono, *Revolusi Berfikir*, Bandung: kaifa, 2007, hal.34.

⁸ Makinuddin, *Analisis sosial: bersaksi dalam advokasi irigasi*, (Bandung: Yayasan Akatiga, 2006), hal.40

dan diterima di depan pengadilan, otentik, akurat, komplit, menyakinkan dihadapan juri, dan diterima di depan masyarakat.⁹

Sedangkan Feri Sulianta (2008) dalam bukunya *Komputer Forensik*, mendefinisikan Forensik memiliki arti “membawa ke pengadilan”. Istilah forensik adalah suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.¹⁰

Dari kedua definisi diatas dapat disimpulkan bahwa Digital forensik merupakan penerapan ilmu pengetahuan untuk memulihkan bukti digital dari suatu perangkat baik itu komputer maupun smartphone dengan metode tertentu yang bertujuan untuk mengumpulkan data yang dapat diterima oleh pengadilan sebagai salah satu pembuktian. Semua fakta atau data yang terbaca dan berhasil di dapatkan oleh pakar komputer forensik harus terjaga kondisinya, sehingga dapat dibuktikan bahwa data tersebut memang benar adanya dan tidak mengalami perubahan, baik disengaja maupun tidak.

D. Mobile Forensik

Mobile Forensik merupakan cabang atau turunan dari digital forensik, mobile forensik bertujuan untuk melakukan pemulihan bukti digital atau data dari perangkat mobile. Sedangkan digital forensik bertujuan melakukan

⁹ Deris Stiawan, *Sistem Keamanan Komputer*, (Jakarta: PT Elex Media Komputindo, 2006), Hal.173.

¹⁰ Feri Sulianta, *Komputer Forensik*, (Jakarta: PT Elex Media Komputindo, 2008), hal.2

pemulihan bukti digital dari perangkat digital termasuk di dalamnya pemulihan pada perangkat mobile.

E. Cyber Crime

Menurut Pajar Pahrudin (2010) dalam bukunya *Etika Profesi Komputer* mendefinisikan bahwa *Cyber Crime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh kehidupan modern saat ini.¹¹

Menurut Widodo (2013) kejahatan di dunia siber atau *Cyber Crime* merupakan bentuk kejahatan baru berbasis teknologi informasi dengan memanfaatkan perangkat keras maupun perangkat lunak komputer.¹²

Dari definisi diatas dapat disimpulkan bahwa *Cyber Crime* adalah kejahatan yang dilakukan oleh seseorang atau kelompok orang dengan pemanfaatan komputer atau internet.

Cyber Crime dibagi menjadi dua kelompok yaitu *Violent*, dan *Non-Violent*. *Violent* adalah penyalahgunaan komputer yang akan berdampak secara fisik kepada orang lain.

Secara garis besar *Violent* terbagi dalam 3 kelompok utama yaitu :

¹¹ Pajar Pahrudin, *Etika Profesi Komputer*, (Jawa Barat: Goresan Pena Kuningan, 2010) hal. 172.

¹² Dr. Rulli Nasrullah, M.Si, *Teori dan Riset Media Siber*, (Jakarta: Kencana, 2016) hal.128.

1. *Cyberterrorism*, yaitu kegiatan yang mengarah pada aktivitas terorisme dengan memanfaatkan media cyberspace.
2. *Cyber bullying*, yaitu upaya untuk menimbulkan ketakutan pada diri seseorang dengan merendahkan kehormatan orang lain.
3. *Child pornography*, kejahatan ini melibatkan tiga kelompok yaitu mereka yang terlibat untuk *create, distribute*, dan akses material pornografi.

Sedangkan *Non-Violent* adalah penyalahgunaan komputer yang tidak berdampak langsung pada fisik seseorang namun lebih pada kerugian secara sistemik. Contoh *Non-Violent* yaitu:

1. *Plagiarisme*: yaitu pengakuan karya orang lain sebagai karya individu
2. *Others crime*: penawaran jasa prostitusi, judi online, penjualan obat-obat terlarang, penawaran barang-barang yang tidak lazim diperjualbelikan dalam wilayah hukum tertentu (misalnya untuk Indonesia jual beli arca dan hewan langka).

Semua jenis kejahatan cyber tersebut sudah tercantum di dalam undang-undang negara Indonesia. Dasar hukum pidana untuk kejahatan cyber di Indonesia, dimuat dalam UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisi ketentuan pidana bagi pelaku *Cyber Crime*.

F. Data Recovery

Data Recovery merupakan proses mengembalikan data dari kondisi yang rusak, gagal, atau tidak bisa diakses ke kondisi awal yang normal. Data recovery merupakan bagian penting dari analisis forensik yang harus dilakukan untuk mengetahui apa yang telah terjadi, dan mengambil kembali file data yang telah terhapus sebelumnya. Data yang dikembalikan bisa dari hard disk, flash disk, dan media simpan lainnya seperti kamera digital, dan camcorder.¹³ Kasus kehilangan data yang paling banyak terjadi umumnya adalah kegagalan logis, yaitu ketika sistem operasi gagal untuk mengenali sistem file, baik disk, partisi atau karena sistem operasinya yang rusak, kasus yang juga umum menyebabkan kehilangan data adalah kesalahan penghapusan file secara tidak sengaja dari hard disk dan dari recycle bin. Apapun penyebabnya, tujuan dari data recovery adalah mengembalikan file yang sudah hilang tersebut kemudian memindahkannya ke tempat yang aman dengan cara menyalin/mengcopy.

G. KingRoot

KingRoot merupakan salah satu software atau *tools* yang digunakan untuk melakukan rooting pada semua jenis smarphone Android. Software ini merupakan software yang berasal dari Tiongkok yang mensupport hampir semua perangkat smartphone Android. Untuk melakukan rooting sendiri

¹³ Tim EMS, *Mengatasi Data Hilang dan Serangan Virus*, (Jakarta: PT Elex Media Komputindo, 2009) hal.2.

dibutuhkan beberapa persyaratan serta backup terlebih dahulu data-data penting yang ada di smartphone. Beberapa model smartphone seperti HTC dan Sony Xperia akan membutuhkan tindakan yang lebih lanjut, karena kedua merek smartphone tersebut membutuhkan bootloader agar dapat melakukan proses rooting. Selain itu, proses rooting ini juga akan membatalkan garansi smartphone Anda.

Ada beberapa persyaratan yang harus disiapkan sebelum melakukan proses rooting, yaitu sebagai berikut:

1. Baterai tidak boleh kurang dari 75%, ini untuk mengantisipasi agar smartphone tidak mati saat proses sedang berjalan.
2. Backup semua data-data penting yang ada di smartphone, termasuk kontak, pesan, dan lain-lain.
3. Pastikan smartphone memiliki akses internet saat melakukan proses rooting.

H. Flashify

Flashify merupakan sebuah aplikasi untuk Android yang berfungsi untuk melakukan flash atau install file-file “.img” seperti recovery, dan sebagainya. Aplikasi Flashify ini sangat bermanfaat terutama untuk perangkat Android yang tidak terpasang custom recovery namun membutuhkan beberapa fungsinya karena aplikasi Flashify bisa menggantikan beberapa fungsi custom recovery untuk menginstall secara langsung file-file berekstensi

“.img” seperti memasang custom recovery, dan lain-lain secara langsung ke sistem perangkat Android.

I. CWM Recovery

Custom ROM adalah sebuah rom firmware yang telah dimodifikasi oleh developer sehingga menjadi rom kreasinya dengan tambahan fitur-fitur dan tampilan yang menarik. Untuk menginstall custom rom tersebut pada android maka diperlukan beberapa perlengkapan, salah satunya adalah CWM (Clock Work Mod). CWM merupakan custom recovery yang menggantikan recovery android (Recovery bawaan pabrik).¹⁴ Clock Work Mod (CWM) merupakan metode recovery yang sangat membantu dalam pengambilan data pada partisi sistem android.

J. WhatsApp Viewer

WhatsApp Viewer merupakan sebuah aplikasi yang dapat digunakan untuk menampilkan riwayat obrolan atau percakapan whatsapp dari database whatsapp itu sendiri yaitu msgstore.db, selain itu aplikasi WhatsApp Viewer ini juga dapat digunakan untuk membuka whatsapp dari database yang terenkripsi menjadi database yang terdekripsi dengan menggunakan key (kunci) yang terletak pada folder com.whatsapp, versi crypt yang didukung oleh aplikasi whatsapp viewer ini adalah crypt 5, crypt 7, crypt 8, crypt 12.

¹⁴ Wahana Komputer, *Tip, Trik, Hacking Ponsel dan Tablet Android*, (Jakarta: PT Elex Media Komputindo, 2013) hal.141.

K. DB Browser for SQLite

DB Browser for SQLite adalah sebuah alat yang bertujuan untuk memudahkan pengguna dalam membuat maupun memperbaiki file pada database SQLite, tanpa perlu berhadapan dengan perintah-perintah SQL. Tampilan dari aplikasi ini memudahkan pengguna untuk melihat dan menelusuri tabel dan field dengan menggunakan tree view, selain itu aplikasi ini juga mudah dipahami dan efisien dalam pengaturan data. Dengan hadirnya aplikasi ini dapat membantu pengguna untuk melihat konten dari database dengan tampilan yang terstruktur dengan baik. DB Browser for SQLite mengadopsi penggunaan yang sederhana untuk mengatur database SQL. Termasuk wizard untuk membuat dan mengubah tabel, menyaring data, memunculkan SQL query, semua itu dapat dilakukan tanpa membutuhkan perintah dari SQL.

L. FTK Imager

Access Data Forensic ToolKit Imager atau biasa di sebut “AD FTK Imager” merupakan salah satu aplikasi yang dikembangkan oleh perusahaan Access Data yang digunakan dalam dunia forensik digital untuk melakukan sistem akuisisi data. FTK Imager (*Forensic Toolkit Imager*) merupakan aplikasi digital forensics yang terkenal dengan paket lengkap, aplikasi yang

bisa dioperasikan saat penyidik menggunakan teknik live atau static bahkan keduanya, aplikasi ini dapat menangkap citra, menyimpan menganalisisnya.¹⁵ Dimana sistem akuisisi itu sendiri merupakan suatu sistem yang berfungsi untuk mengambil, mengumpulkan dan menyiapkan data, hingga memprosesnya untuk menghasilkan data yang dikehendaki.

M. *National Institute of Standards and Technology (NIST)*

NIST (*National Institute of Standards and Technology*) merupakan Badan Nasional Standar dan Teknologi, sebuah unit dari Departemen Perdagangan Amerika Serikat. Yang dulunya dikenal sebagai National Bureau of Standards – NBS (Biro Standar Nasional), sebuah nama yang diberikan dari tahun 1901 sampai 1988. NIST memiliki program aktif untuk mendorong dan membantu industri dan ilmu pengetahuan untuk mengembangkan dan menggunakan standar ini.¹⁶ Misi dari badan ini adalah untuk membuat dan mendorong pengukuran, standar dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang. Sebagai bagian dari misi ini, ilmuwan-ilmuwan dan insinyur-insinyur NIST secara terus menerus mengembangkan ilmu pengukuran, yang memungkinkan rekayasa yang diperlukan oleh teknologi maju zaman

¹⁵ Muhammad Fajar Sidiq, (2019), *Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital*, Jurnal Edukasi dan Penelitian Informatika Vol. 5 No. 1, hal.69.

¹⁶ Riyanto, Ph.D, *Validasi & Verifikasi Metode Uji*, (Yogyakarta: Deepublish, 2014) hal.48.

sekarang. Mereka pun terlibat secara langsung di dalam pembuatan standar dan pemeriksaan yang dilakukan oleh badan-badan pemerintah. Inovasi dan kemajuan teknologi di Amerika Serikat bergantung pada keahlian dan kemampuan unik dari NIST di empat bidang utama: bioteknologi, nanoteknologi, teknologi informasi, dan manufaktur modern. NIST membuat sebuah metode yang memiliki empat tahapan dalam menyelesaikan dan menyelidiki kasus *Cyber Crime*, tahap pertama yaitu *Collection* (Pengumpulan Data), *Examination* (Pemeriksaan barang bukti), *Analysis*, dan yang terakhir adalah *Reporting* (Membuat laporan berdasarkan hasil analisis).

N. WhatsApp

WhatsApp merupakan aplikasi perpesanan paling populer saat ini dan merupakan aplikasi perpesanan tak berbayar yang difasilitasi oleh internet. Aplikasi WhatsApp utamanya berjalan pada perangkat seluler, namun juga dapat digunakan pada dekstop selama perangkat seluler yang digunakan terhubung dengan aplikasi WhatsApp pada dekstop.¹⁷

Media Sosial WhatsApp yang sering disingkat WA adalah salah satu media komunikasi yang dapat di install dalam smartpone, WhatsApp sering

¹⁷ Moh Faidol Juddi,dkk. *Communication and Information Beyond Boundaries: Seminar macom III Book Chapter* (Bandung: Aksel Media Akselerasi, 2019) hal.901.

digunakan sebagai sarana komunikasi seperti chat dimana saling mengirim pesan teks, gambar, video bahkan dapat melakukan aktivitas telepon.¹⁸

Maka berdasarkan penjelasan diatas dapat ditarik kesimpulan bahwa WhatsApp merupakan aplikasi *instant messenger* yang berfungsi sebagai alat untuk komunikasi, WhatsApp memiliki fitur chat, telepon, video call, dan lain-lain. WhatsApp dapat dijalankan pada smartphome dan dekstop selama smartphome yang digunakan terhubung dengan aplikasi WhatsApp yang terdapat pada dekstop. Untuk dapat menggunakan aplikasi ini maka pengguna harus mendaftarkan nomor telepon yang ingin digunakan. WhatsApp hanya akan berjalan apabila pengguna memiliki paket data internet. Apabila pengguna tidak memiliki paket data dan internet maka WhatsApp tidak dapat berjalan sebagai mana mestinya.

O. Pornografi

Kejaksaaan Agung RI pada tahun 1970 membentuk sebuah tim yang diberi nama Tim Penelaah Masalah Porno Kejaksaan Agung, yang terdiri atas unsur-unsur agama, pendidikan, dan ilmuuan. Tim ini bertugas untuk mencari batasan tentang pornografi. Pengertian yang dihasilkan Tim ini mengenai pornografi adalah perbuatan, gambar, tulisan, lagu, suara, bunyi, benda atau

¹⁸ Edi Suryadi, M,dkk (2013), *Penggunaan sosial media whatsapp dan pengaruhnya terhadap disiplin belajar peserta Didik Pada Mata Pelajaran Pendidikan Agama Islam*, Jurnal Pendidikan Islam Vol. 07, No.1, hal.5.

segala sesuatu yang dapat merangsang birahi manusia, dan dapat mengakibatkan tindakan maksiat serta mengganggu ketentraman umum.¹⁹

Menurut undang-undang tentang pornografi No.44 tahun 2008 pasal 1, pornografi merupakan gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat.

Maka berdasarkan penjelasan diatas dapat ditarik kesimpulan bahwa pornografi merupakan perbuatan yang memuat kecabulan dan melanggar kesusilaan. Margaret Aliyatul Maimunah selaku Komisioner Bidang Pornografi dan *Cyber Crime* Komisi Perlindungan Anak Indonesia (KPAI) menyebutkan, jumlah total pengaduan kasus pornografi dan *Cyber Crime* pada tahun 2015 sebanyak 463 kasus, 2016 meningkat menjadi 587 kasus, 2017 menjadi 608 kasus, dan pada tahun 2018 naik menjadi 679 kasus. Ini membuktikan bahwa kasus pornografi dan *Cyber Crime* setiap tahunnya mengalami peningkatan.²⁰

¹⁹Sulistyowati Irianto, *Perempuan dan Hukum: Menuju Hukum yang Berperspektif Kesetaraan dan keadilan*, (Jakarta: Yayasan Obor Indonesia, 2006) hal.299.

²⁰Rusdy Nurdiansyah, 2019, *KPAI Catat Peningkatan Kasus Pornografi Anak Lewat Medsos*, diakses pada tanggal 28 Agustus 2019, pukul 23.54 WIB, <https://www.republika.co.id/berita/nasional/umum/19/07/24/pv5ezi320-kpai-catat-peningkatan-kasus-pornografi-anak-lewat-medsos>.

P. Penegakan Hukum Pidana

Di Indonesia dasar hukum pidana untuk kejahatan *Cyber Crime* sudah ada dalam Undang-undang no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisi ketentuan pidana bagi pelaku *Cyber Crime*. Untuk kasus *Cyber* pornografi sendiri tidak tercantum secara jelas di dalam undang-undang no. 11 tahun 2008, tetapi “muatan yang melanggar kesusilaan”. Penyebarluasan muatan yang melanggar kesusilaan melalui internet diatur dalam pasal 27 ayat (1) UU ITE, yaitu:

“Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.²¹ Pelanggaran terhadap pasal 27 ayat (1) UU ITE dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp 1 milyar”.

Selain undang-undang no. 11 tahun 2008, telah ada beberapa undang-undang yang mengatur mengenai pornografi, antara lain Kitab Undang-undang Hukum Pidana (KUHP) dan undang-undang Nomor 44 Tahun 2008 tentang pornografi (UU Pornografi). Penyebarluasan tentang pornografi melalui internet tidak diatur secara khusus dalam KUHP, namun ada pasal KUHP yang bisa dikenakan untuk kasus pornografi ini, yaitu pasal 282 KUHP mengenai kejahatan terhadap kesusilaan, yaitu:

²¹ L. Heru Sujamawardi (2018), *Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik*, Jurnal Hukum Bisnis dan Investasi Vol.9, No. 2, hal.87.

“Barangsiapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang telah diketahui isinya melanggar kesusilaan, atau barang siapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkannya ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau memiliki persediaan, ataupun barang siapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau menunjukkannya sebagai bisa diperoleh, diancam dengan pidana penjara paling lama satu tahun enam bulan”.²²

Yang ketiga yaitu Undang-undang Pornografi (UU Pornografi), Penyebarluasan tentang pornografi, termasuk melalui media internet diatur dalam Pasal 4 ayat 1, yaitu:

“Setiap orang dilarang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang memuat:

- a. kekerasan seksual
- b. masturbasi atau onani
- c. ketelanjangan atau tampilan yang mengesankan ketelanjangan
- d. alat kelamin
- e. pornografi anak.”²³

Pelanggaran pasal 4 ayat (1) UU Pornografi dapat diancam pidana sebagaimana yang telah diatur dalam Pasal 29 Undang-Undang Pornografi yaitu: dipidana dengan pidana penjara paling singkat 6 (enam)

²² Hardianto Djanggih (2013), *Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime di Bidang Kesusilaan*, Jurnal Media Hukum Vol.1, No.2, hal.60.

²³ Dadin Eka Saputra (2017), *Kajian Yuridis Terhadap Tindak Pidana Pornografi Melalui Media Sosial*, Al’adl Vol.IX, No.2, hal.278.

bulan dan paling lama 12 (dua belas) tahun dan/atau pidana denda paling sedikit Rp 250 juta dan paling banyak Rp 6 miliar.

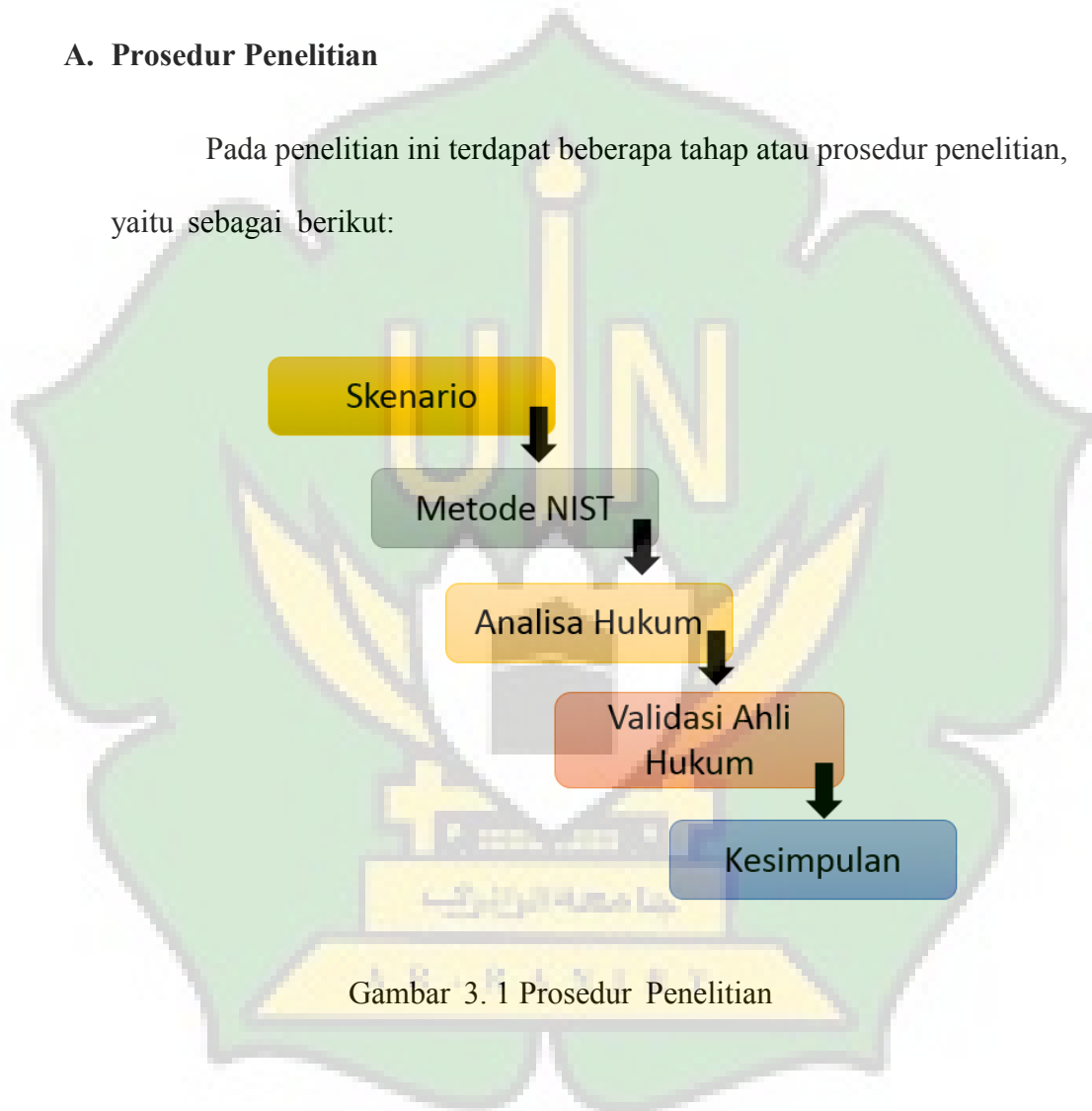


BAB III

METODOLOGI PENELITIAN

A. Prosedur Penelitian

Pada penelitian ini terdapat beberapa tahap atau prosedur penelitian, yaitu sebagai berikut:



Berikut adalah penjelasan dari gambar diatas:

1. Skenario adalah tahap awal yang dilakukan dalam penelitian ini, yang merupakan sebuah kegiatan percakapan antara pelaku dan korban yang

berisi konten pornografi menggunakan WhatsApp, dimana setelah percakapan yang berisi konten pornografi tersebut dilakukan kemudian tersangka menghapus semua data dari perangkat komunikasi untuk menghilangkan barang bukti.

2. NIST (*National Institute of Standards and Technology*) merupakan metode atau tahapan-tahapan yang digunakan dalam penelitian ini untuk mendapatkan barang bukti digital.
3. Analisa Hukum merupakan tahap untuk menentukan hukum dari kasus pornografi berdasarkan undang-undang yang berlaku, yaitu UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Kitab Undang-undang Hukum Pidana (KUHP), dan undang-undang Nomor 44 Tahun 2008 tentang pornografi.
4. Validasi ahli hukum merupakan tahap untuk memeriksa hasil penelitian, *tool*, dan metode yang digunakan kepada ahli hukum terkait kasus pornografi.
5. Kesimpulan adalah tahap memberikan solusi berdasarkan analisa hukum dan validasi ahli hukum yang telah dilaksanakan.

B. Metode Penelitian

Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST (*National Institute of Standards and Technology*).

Metode ini digunakan untuk menjelaskan bagaimana tahapan-tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis kemudian dapat dijadikan pedoman dalam menyelesaikan permasalahan yang terjadi. Berdasarkan gambar 2 dapat dijelaskan tahapan Analisis Forensik sebagai berikut:



Gambar 3. 2 Tahapan Metode NIST

Metode ini merekomendasikan sebuah tahapan dalam proses forensik, yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*.

Tahap *Collection* atau biasa disebut tahap pengumpulan merupakan kegiatan mengumpulkan data-data untuk mendukung proses penyelidikan dalam pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan kemudian menjaga barang bukti agar tidak terjadi perubahan.

Tahap *Examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik, serta memastikan bahwa

data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan digital.

Tahap *Analysis* atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

Tahap *Reporting* atau tahap pelaporan dilakukan setelah proses pemeriksaan dan analisis dilakukan kemudian diperoleh barang bukti digital. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yaitu penggambaran tindakan yang dilakukan, penjelasan mengenai *tool*, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan digital forensik.

Pada penelitian ini barang bukti digital yang digunakan tidak didapatkan dari lingkungan yang sebenarnya atau barang bukti digital tidak didapatkan dari hasil tindakan kejahatan komputer yang sebenarnya, melainkan barang bukti digital dalam penelitian ini dibuat dan peroleh dari hasil skenario. Proses implementasi dan pengujiannya dilakukan dengan

skenario, yang bertujuan untuk mendapatkan barang bukti digital seperti pada kasus kejahatan komputer yang sebenarnya terjadi.

Langkah-langkah menentukan *tools forensic* yang sesuai untuk menemukan barang bukti kejahatan *Cyber Crime* dalam penelitian ini adalah sebagai berikut:

1. *Tools* yang akan digunakan harus sesuai dengan spesifikasi smartphone.
2. *Tools* yang digunakan dapat menampilkan keterangan lengkap mengenai waktu terjadinya percakapan.
3. *Tools* yang tidak berbayar atau gratis

Langkah-langkah untuk menentukan aspek hukum yang berlaku berdasarkan kasus yang disimulasikan yaitu peneliti mempelajari secara mendalam mengenai Undang-undang ITE dan KUHP, selanjutnya mengaitkan Undang-undang tersebut dengan kasus yang sudah disimulasikan, kemudian peneliti melakukan validasi hukum kepada ahli hukum guna memastikan bahwa Undang-undang yang dikenai sesuai dengan kasus yang disimulasikan.

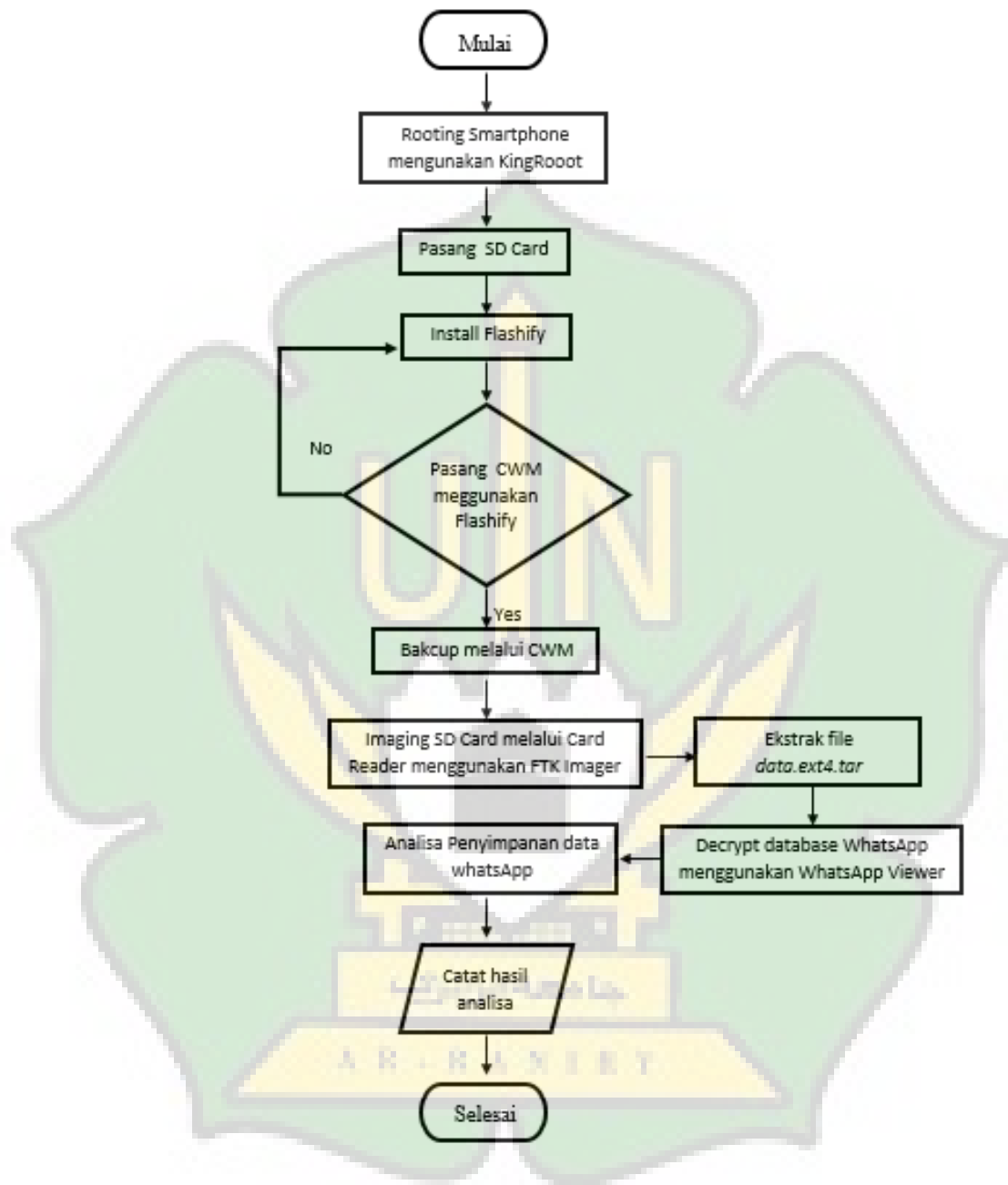
C. Rancangan Skenario

Untuk mendapatkan barang bukti digital maka sebuah skenario atau rekayasa harus dilakukan. Dalam penelitian ini peneliti membuat sebuah skenario mengenai aktivitas percakapan yang dilakukan pada WhatsApp tentang kasus pornografi. Tujuan dijalankannya skenario ini untuk

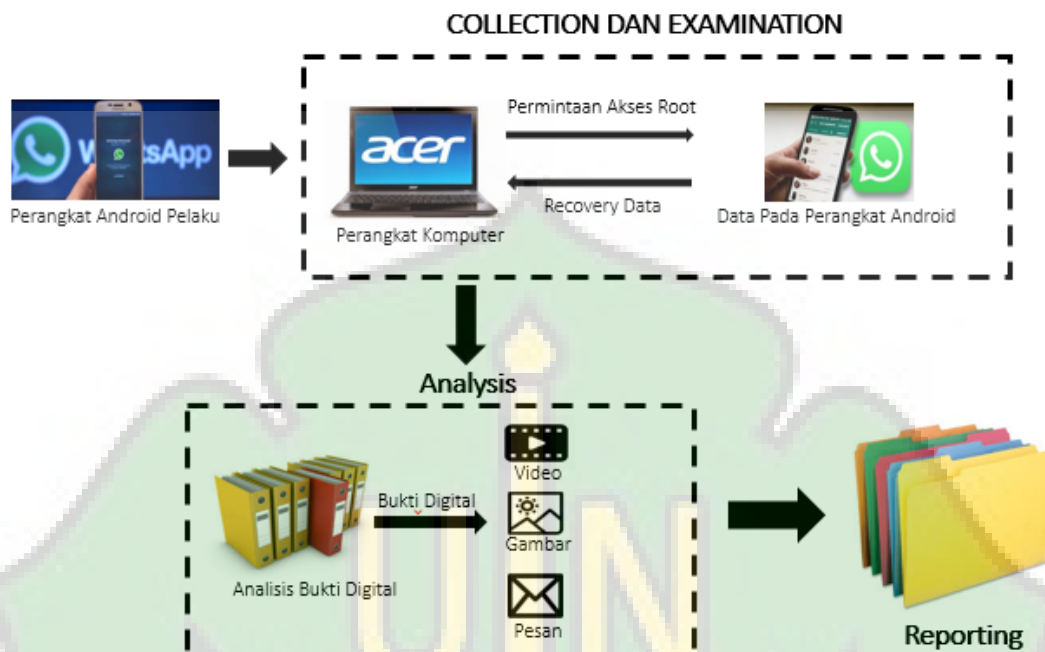
mempermudah investigasi dari kasus *cyber* pornografi. Skenario tersebut yaitu:

1. Awalnya tersangka membuat sebuah akun WhatsApp (Akun A)
2. Selanjutnya tersangka meminta nomor telepon korban yang digunakan pada akun WhatsApp guna untuk mendapatkan akun korban (Akun B).
3. Kemudian tersangka mengirimkan percakapan kepada akun korban (kondisi awal normal).
4. Akun A mengirimkan percakapan yang berisi konten pornografi terhadap akun B.
5. Setelah percakapan selesai dilakukan, tersangka menghapus semua data percakapan yang berisi konten pornografi tersebut dari perangkat.

Semua data yang berupa percakapan yang telah dihapus pada perangkat tersangka dari WhatsApp akan diungkap atau dimunculkan kembali menggunakan bantuan *tools*. Berikut alur kerja dari analisis forensik digital, yaitu:



Gambar 3. 3 Flowchart Analisis aplikasi WhatsApp



Gambar 3. 4 Proses Menggunakan Metode NIST

D. Alat dan Bahan Penelitian

Alat dan bahan yang digunakan dalam investigasi forensik digital ini dapat dilihat pada tabel 3.1 berikut:

Tabel 3. 1 Alat dan Bahan Penelitian

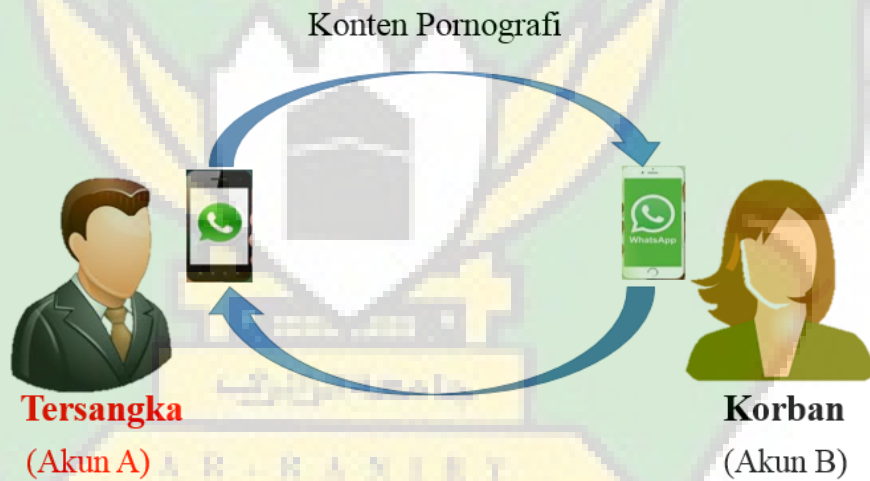
No.	Nama Alat dan Bahan	Deskripsi/Spesifikasi	Keterangan
1.	Satu buah laptop	Merk Acer Z1401, Sistem Operasi Windows 8.0, 32 bit.	Perangkat Keras
2.	Satu Buah Smartphone Android	Merk Lenovo A369i, terinstall Aplikasi WhatsApp.	Perangkat Keras

3.	KingRoot	Aplikasi yang digunakan untuk melakukan <i>rooting smartphone</i> android.	Perangkat Lunak
4.	CWM Recovery dan Flashify	Aplikasi yang digunakan untuk mengangkat data-data pada smartphone.	Perangkat Lunak
5.	WhatsApp Versi 2.19.341	Aplikasi instan messenger yang menjadi objek dari penelitian	Perangkat Lunak
6.	WhatsApp Viewer, dan DB Browser for SQLite	Aplikasi yang digunakan untuk menganalisis data-data WhatsApp.	Perangkat Lunak
7.	AccessData FTK Imager	Aplikasi yang digunakan untuk melakukan <i>imaging</i> data.	Perangkat Lunak

BAB IV

HASIL DAN PEMBAHASAN

Penelitian ini diawali dengan membuat akun WhatsApp pada handphone android yang sudah disiapkan, kemudian melakukan skenario percakapan antara Akun A dan Akun B tentang Pornografi melalui handphone android tersebut, percakapan yang telah dilakukan selanjutnya dihapus dari perangkat pelaku yang bertujuan untuk menghilangkan barang bukti. Berikut ini merupakan gambar skenario yang penulis lakukan, yaitu:



Gambar 4.1 Proses Skenario dari Akun A Kepada Akun B melakukan Pengiriman Konten Pornografi

Skenario teks percakapan yang dilakukan dapat dilihat dibawah ini:



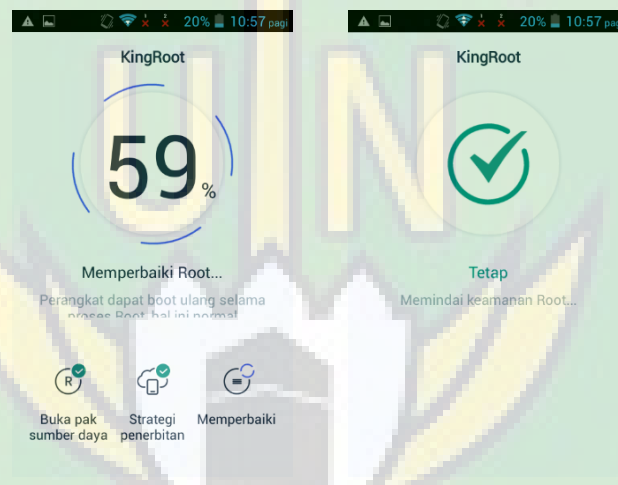
Gambar 4.2 Screenshots dari smartphone korban percakapan yang telah dihapus

Setelah proses skenario berhasil dilakukan selanjutnya adalah mencari informasi dan menganalisis handphone android tersebut untuk memperoleh barang bukti sebagaimana yang telah diskenariokan, berikut ini merupakan tahapan-tahapan yang dilakukan untuk mendapatkan dan menganalisis barang bukti yaitu sebagai berikut:

A. *Collection* (Pengumpulan)

a. *Rooting*

Proses *Collection* atau biasa disebut dengan pengumpulan data diawali dengan melakukan *Rooting* pada *smartphone* menggunakan aplikasi *KingRoot* untuk mempermudah pengangkatan data-data yang ada di dalam perangkat Android. Aplikasi *KingRoot* sendiri dapat didownload melalui *Google Chrome*. Proses *Rooting smartphone* menggunakan aplikasi *Kingroot* dapat dilihat pada gambar dibawah ini:



Gambar 4.3 Proses *Rooting Smartphone* Android Lenovo

Handphone android yang digunakan dalam kondisi sudah di root. Karena kebanyakan sistem operasi, *smartphone* android yang tidak di root beberapa fiturnya telah dinonaktifkan untuk mencegah pengguna bisa merusak sistem operasi. Kondisi *rooting* sendiri bertujuan untuk menghilangkan keterbatasan tersebut sehingga pengguna diperbolehkan untuk akses penuh ke dalam sistem. Untuk kondisi ponsel Android yang

sudah di rooting, pengguna akan memiliki kontrol lebih besar untuk pengaturan, fitur dan performa ponsel sehingga proses mengakses file sistem untuk analisis forensik akan menjadi lebih mudah.

Android yang digunakan dalam penelitian ini adalah Smartphone Lenovo Model A369i, berikut adalah Spesifikasi *smartphone* yang digunakan:



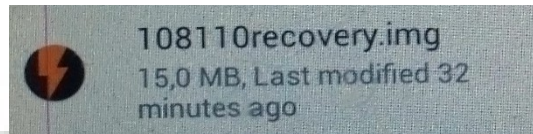
Gambar 4.4 Spesifikasi Smartphone yang digunakan dalam penelitian

b. Instalasi CWM (ClockworkMod) Recovery

Dalam penelitian ini peneliti menggunakan *tool* CWM (ClockworkMod) Recovery untuk melakukan *imaging* memori internal pada smartphone android. Jadi, langkah kedua yang harus dilakukan adalah menginstall CWM Recovery. CWM sendiri adalah mode recovery yang sudah dirubah dan disesuaikan sedemikian rupa dengan berbagai fungsi tambahan seperti *backup* dan *restore*, yang tidak ada di mode recovery standar atau mode recovery bawaan pabrik yang memang sudah tertanam pada smartphone. Dengan menggunakan CWM dapat mengambil data-data pada smartphone baik pada memori internal maupun partisi sistem Android dengan mengaktifkan *USB Debugging* dan melakukan *rooting*, karna tanpa melakukan *rooting* dan mengaktifkan *USB Debugging* pada smartphone maka CWM sulit di install. Untuk mendownload CWM Recovery silahkan ikuti langkah-langkah sebagai berikut:

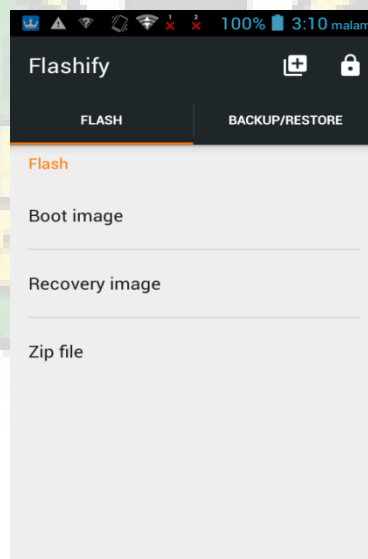
1. Sebelumnya masukkan sebuah SD Card, yang mana pada SD Card tersebut akan diletakkan file CWM, SD Card tersebut juga akan digunakan untuk menampung hasil backup.
2. Selanjutnya download file CWM Recovery sesuai dengan tipe hp masing-masing, File CWM dapat didownload melalui *Google Chrome*, kemudian letakkan file tersebut pada SD Card, jangan di letakkan di dalam folder tetapi diluar folder agar mudah

terdeteksi. Berikut adalah file CWM Recovery yang peneliti gunakan untuk smartphone Lenovo tipe A369i:



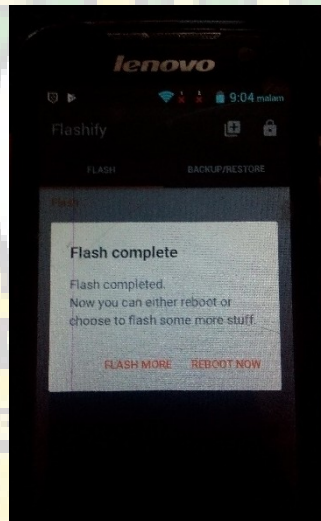
Gambar 4.5 File CWM Recovery

3. Setelah mendownload file CWM Recovery selanjutnya download aplikasi yang menyediakan Flashing. Flashing adalah proses menginstall kembali sistem operasi agar kembali seperti baru, pada penelitian ini aplikasi yang digunakan adalah Flashify. Aplikasi tersebut digunakan untuk menginstall CWM Recovery, dapat di download melalui *Google Play Store*. Berikut gambar halaman utama dari aplikasi Flashify.



Gambar 4.6 Halaman Utama Aplikasi Flashify

4. Setelah melakukan download dan install aplikasi Flashify, lalu buka aplikasi tersebut. Untuk menginstall CWM Recovery maka pilih menu *Recovery image*.
5. Pilih menu *choose a file*.
6. Pilih file CWM Recovery yang sudah di download dan diletakkan di SD Card tadi.
7. Selanjutnya klik Ok. Maka proses menginstall CWM recovery berhasil dilakukan.
8. Kemudian tekan *Reboot Now* untuk memulai ulang smartphone.

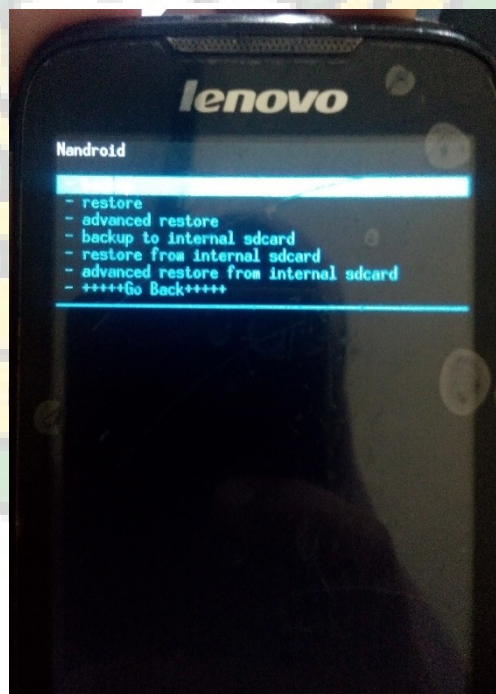


Gambar 4.7 Proses instalasi CWM Recovery dengan aplikasi Flashify berhasil

Untuk masuk ke mode CWM Recovery maka matikan terlebih dahulu smartphonanya, karna untuk masuk ke mode CWM Recovery dilakukan

pada saat smartphone dalam keadaan mati, setelah smartphonenya mati, ikuti langkah-langkah berikut ini:

1. Tekan tombol *power* + *Volume up* + *Volume Down* secara bersamaan.
2. Ketika sudah muncul tulisan Lenovo lepaskan tombol *power* dan tahan tombol *Volume up* + *Volume Down*, tunggu hingga muncul menu CWM Recovery. Untuk memilih menu pada CWM Recovery silahkan menekan tombol *power* untuk Ok, tombol *Volume Down* untuk menggeser ke bawah, dan tombol *Volume Up* untuk menggeser ke atas.



Gambar 4.8 Mode pada *CWM Recovery*

c. *Backup* Memori Internal Smartphone dengan Tool *CWM Recovery*

Setelah berhasil masuk ke mode *CWM Recovery* langkah selanjutnya adalah backup memori internal smartphone dengan cara berikut ini:

1. Pilih menu *backup and restore*.
2. Kemudian pilih menu *backup*. Tunggu beberapa menit hingga proses selesai.
3. Setelah proses *backup* selesai selanjutnya pilih menu *Reboot System Now* untuk memulai kembali smartphone.

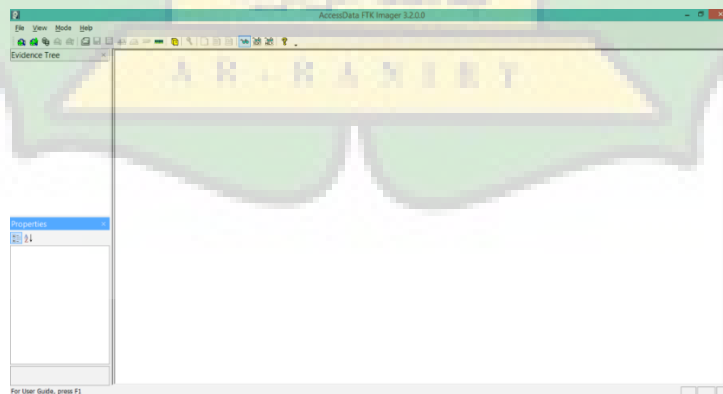


Gambar 4.9 Proses Backup data menggunakan *CWM Recovery*

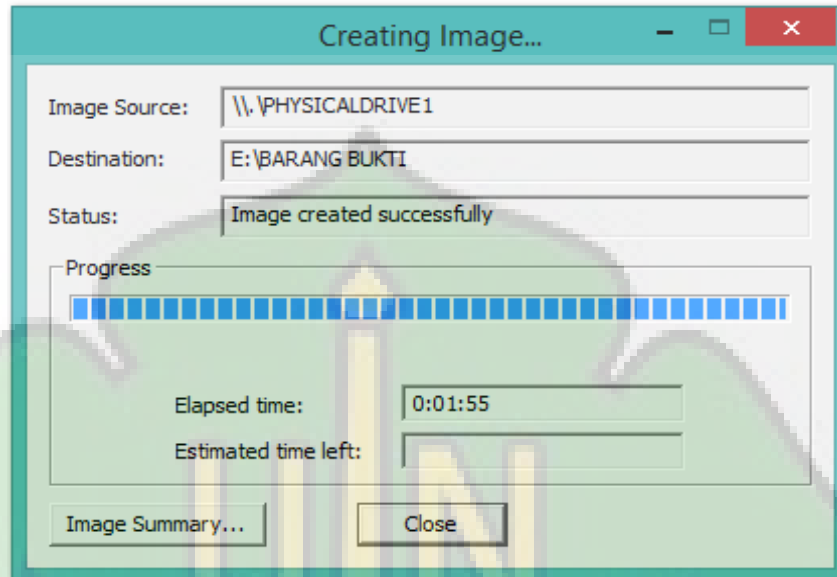
d. *Imaging SD Card*

Setelah proses backup melalui CWM berhasil dilakukan, maka selanjutnya adalah melakukan *imaging* terhadap *SD Card*, yang mana pada *SD Card* tersebut terdapat hasil backup. Untuk melakukan *imaging* tahapan-tahapannya yaitu:

1. Dibutuhkan sebuah *Card Reader* yang akan digunakan sebagai media untuk mengkoneksi ke komputer. Masukkan *SD Card* kedalam *Card Reader* tersebut kemudian hubungkan *Card Reader* ke komputer.
2. *Imaging* data hasil *backup*, *imaging* dilakukan dengan menggunakan *tools AccessData FTK Imager*, yang dapat didownload melalui *Google Chrome*. Cepat atau lambatnya proses *imaging* ini berjalan bergantung pada ukuran *file* yang akan di *imaging*. berikut adalah proses *imaging* menggunakan aplikasi FTK Imager:



Gambar 4.10 Halaman utama aplikasi FTK Imager



Gambar 4.11 Proses *Imaging* data menggunakan aplikasi FTK Imager

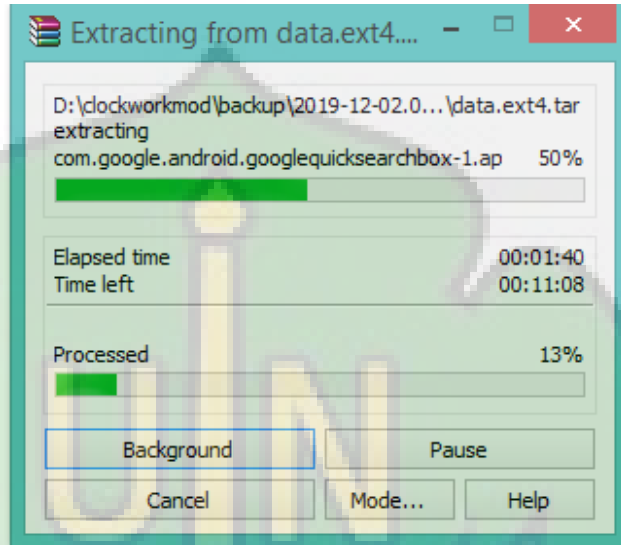
B. *Examination* dan *Analysis*

Tahap *Examintaion* dan *Analysis* ini bertujuan untuk mengungkapkan dan melakukan analisis pada hasil dari tahap *Collection* atau pengumpulan data yang telah dilakukan untuk memperoleh data yang berkaitan dengan aplikasi WhatsApp. Tahapan pertama yang dilakukan untuk menganalisis hasil *imaging* adalah:

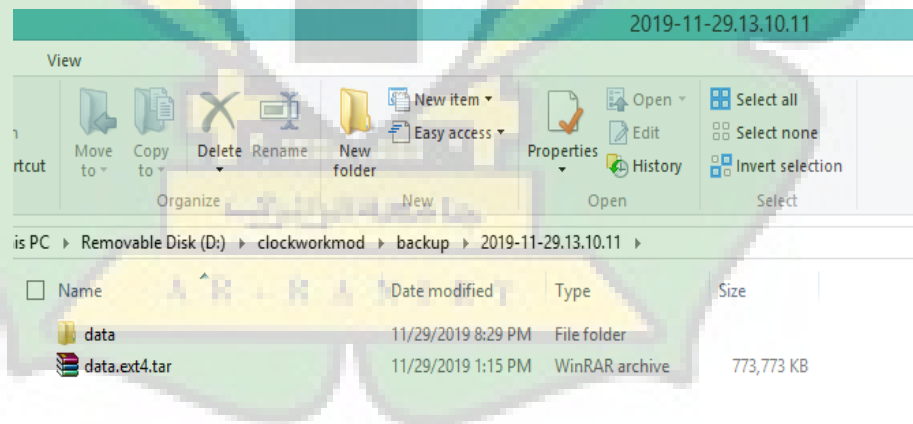
a. Ekstraksi Data WhatsApp dari Data *Image*

Data yang sudah di *imaging* tadi selanjutnya di ekstrak, data tersimpan dalam folder yang nama foldernya berlabel sesuai tanggal *backup*,

kemudian yang dicari adalah file dengan nama *data.ext4.tar* kemudian diekstrak.



Gambar 4.12 Proses Ekstraksi *File data.ext4.tar* dari data *image*



Gambar 4.13 Hasil Ekstraksi *data.ext4.tar*

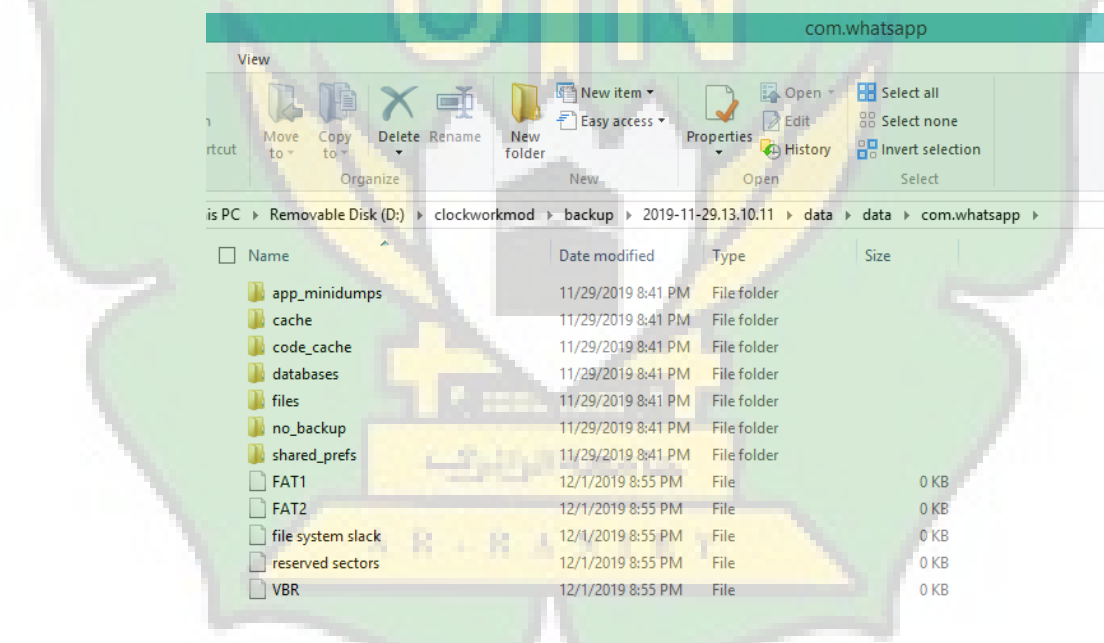
Setelah proses ekstrak selesai selanjutnya hasil ekstrak dianalisis dengan menggunakan aplikasi *WhtasApp Viewer*. Aplikasi tersebut bisa

didapat dengan mendownload melalui *Google Chrome*. Berikut adalah tempat penyimpanan folder WhatsApp dan folder com.whatsapp.

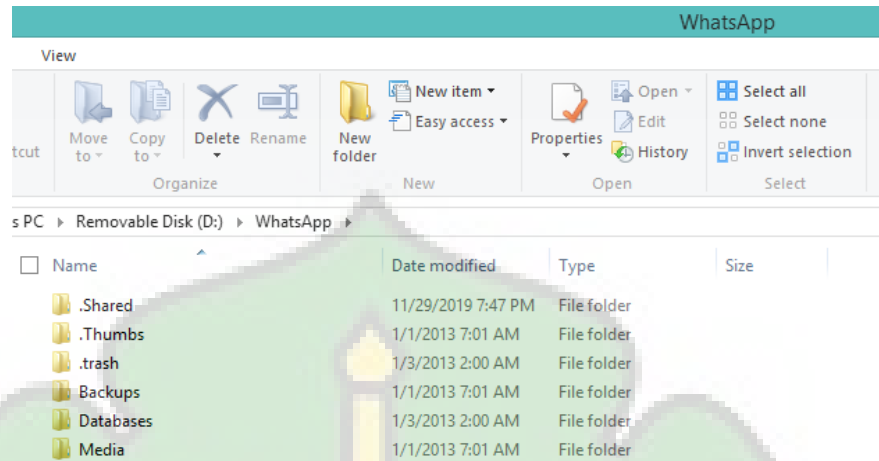
Tabel 4.1 Tempat penyimpanan Folder WhatsApp dan folder com.whatsapp

Barang Bukti	Tempat Penyimpanan	Folder Data
Smartphone Lenovo A369i	- Memori Internal	Folder com.whatsapp Folder WhatsApp

Berikut ini adalah gambar struktur folder com.whatsapp dan folder WhatsApp, yaitu:



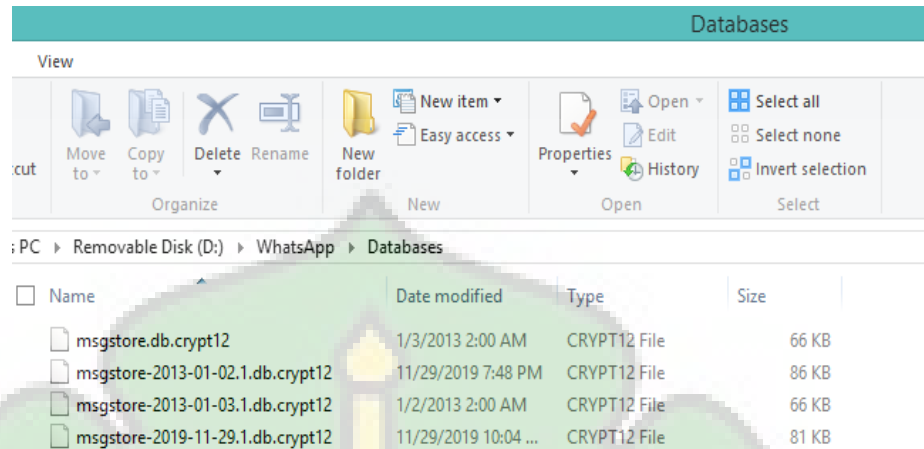
Gambar 4.14 Struktur Folder com.whatsapp



Gambar 4.15 Struktur Folder WhatsApp

b. *Decrypt Database* WhatsApp

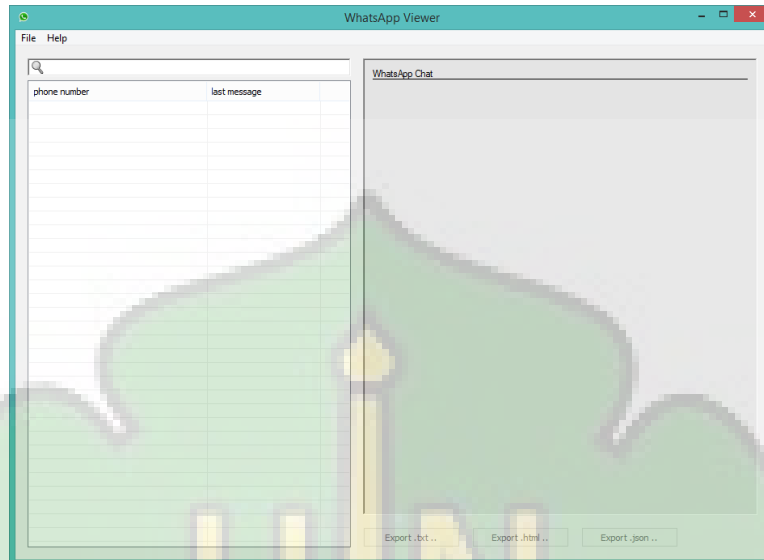
Setelah semua data-data yang berkaitan dengan aplikasi WhatsApp telah didapatkan, maka selanjutnya adalah mendeskripsikan database aplikasi WhatsApp yang terenkripsi *crypt12*. Pada gambar berikut dapat dilihat file di folder WhatsApp dienkripsi menggunakan *crypt12*.



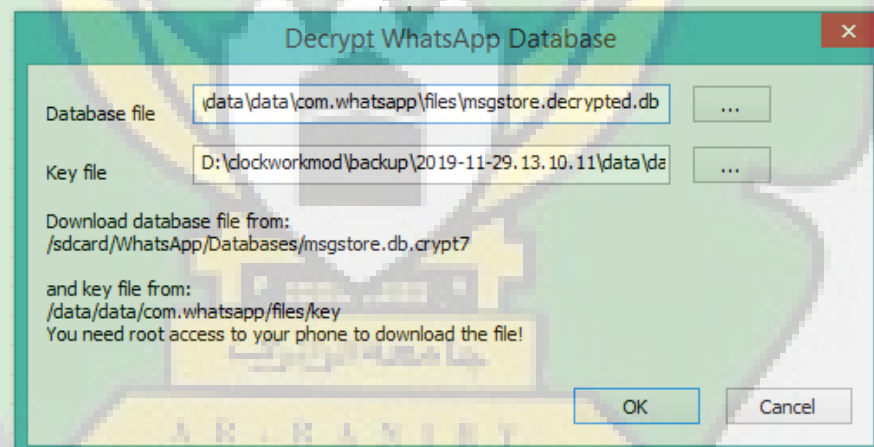
Gambar 4.16 Data di Folder WhatsApp yang terenkripsi menggunakan crypt12.

Untuk mendeskripsi *database* yang terenkripsi tersebut dapat menggunakan aplikasi *WhatsApp Viewer*. Ikuti langkah-langkah sebagai berikut:

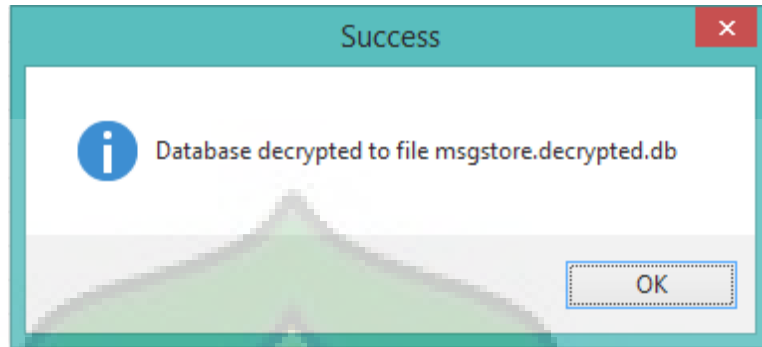
1. Pilih menu *Decrypt .crypt12* pada aplikasi *WhatsApp Viewer* tersebut.
2. Pilih *database* dengan nama *msgstore.db.crypt12* yang ingin didekripsi.
3. Untuk mendekripsikan dibutuhkan sebuah *file key* yang mana file tersebut terletak pada folder *com.whatsapp/files/*. Dapat dilihat seperti gambar dibawah ini:



Gambar 4.17 Halaman utama aplikasi *WhatsApp Viewer*

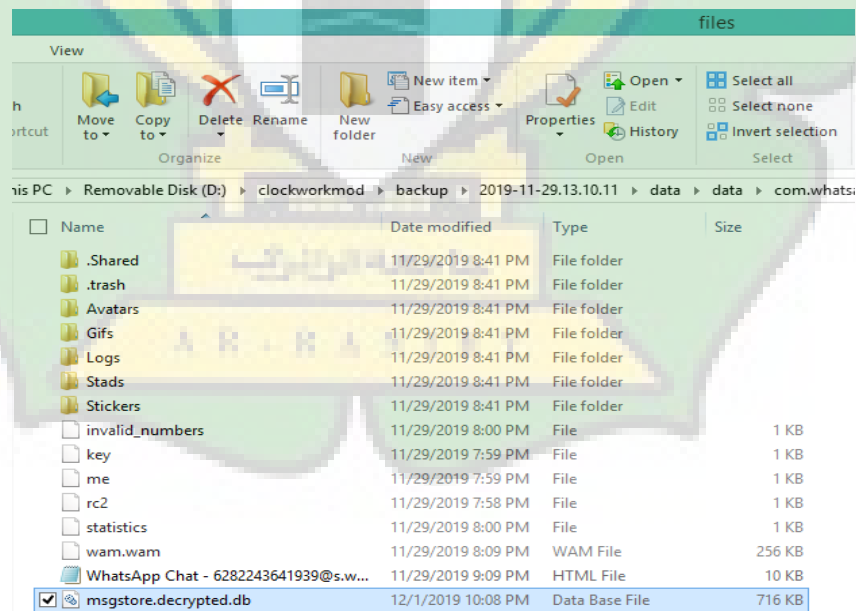


Gambar 4.18 Proses Deskripsi *Database* WhatsApp menggunakan aplikasi *WhatsApp Viewer*



Gambar 4.19 Database WhatsApp berhasil di dekripsi

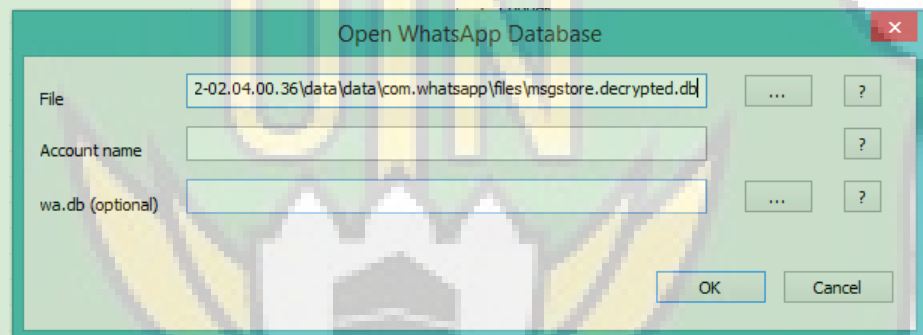
Setelah proses dekripsi selesai dilakukan, maka akan muncul sebuah file *database* baru yang bernama *msgstore.decrypted.db* pada folder yang sama dengan file *database* yang sudah *didekripsi*.



Gambar 4.20 File Database yang sudah terdekripsi

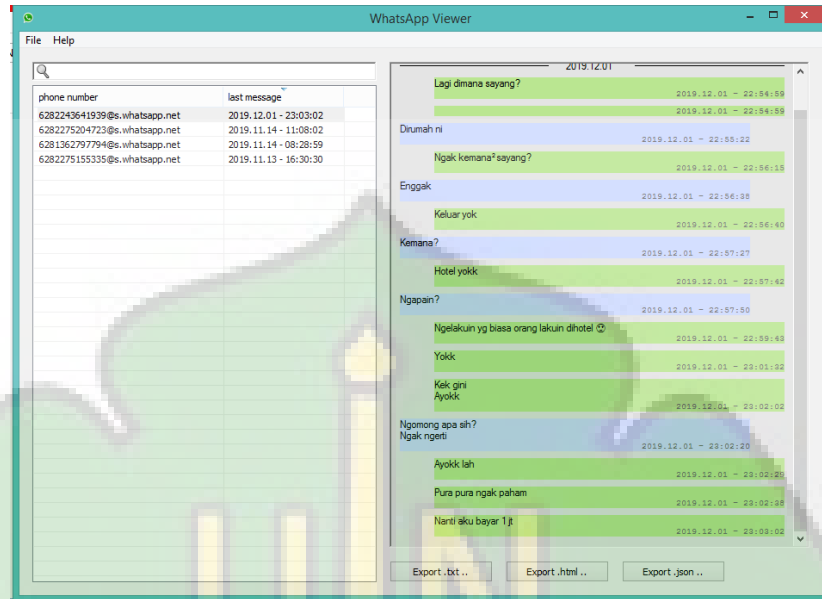
Setelah mendekripsi *file database backup* yang terenkripsi tersebut selanjutnya adalah membuka *database* yang telah di dekripsi tadi untuk mengetahui sesi percakapan yang telah di hapus dengan menggunakan aplikasi *WhatsApp Viewer*. Caranya adalah sebagai berikut:

1. pilih *fitur file* pada aplikasi *WhatsApp Viewer*.
2. Pilih menu *Open* lalu masukkan *file database* yang sudah didekripsi dengan menekan tombol titik tiga disebelah kanan.



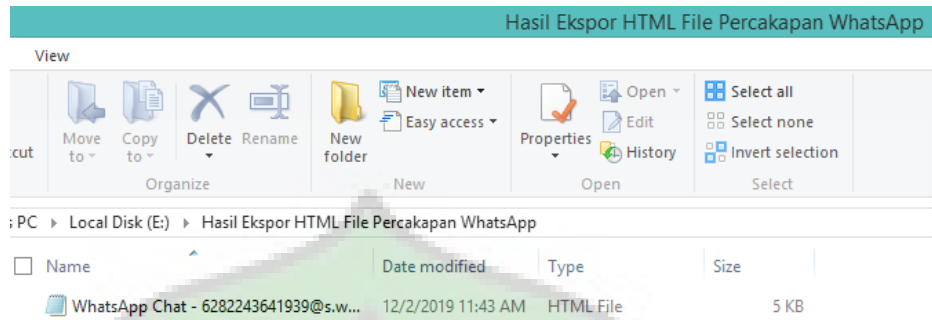
Gambar 4.21 Proses membuka *Database* WhatsApp yang sudah didekripsi menggunakan aplikasi *WhatsApp Viewer*.

Setelah Proses membuka *file Database* berhasil dilakukan maka sesi percakapan yang sudah di skenarioikan berhasil didapat, Selain sesi percakapan, nomor kontak WhatsApp, tanggal/bulan/tahun dilakukannya percakapan beserta keterangan waktu yaitu dijam berapa percakapan tersebut dilakukan juga berhasil di dapat. seperti gambar dibawah ini:

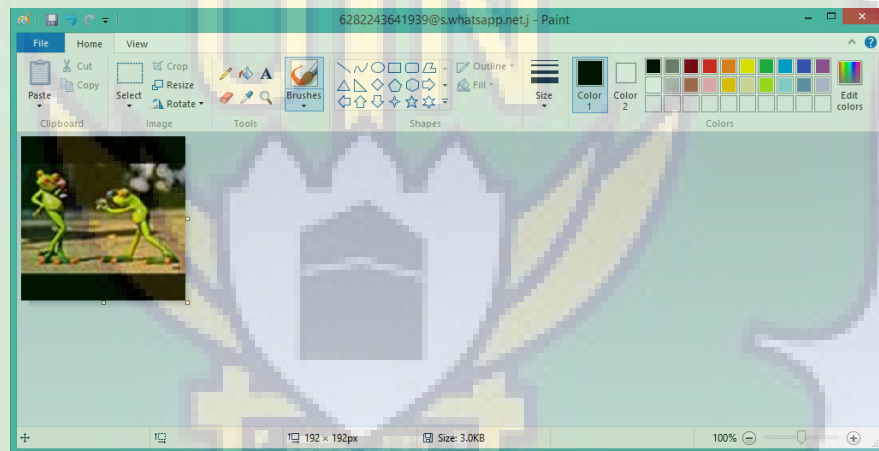


Gambar 4.22 Contoh Chat WhatsApp yang berhasil didapatkan

Pada aplikasi *WhatsApp Viewer* ini juga terdapat menu untuk mengconvert/mengubah isi percakapan pada *database* yang sudah terdekripsi ke *format.html*, untuk mengubah ke *html*, maka pilih *chat* yang ingin diubah, kemudian klik *Export.html*, lalu pilih lokasi tempat untuk menyimpan hasil yang diubah tersebut, kemudian klik *save*, maka hasil *convert* ke *html* berhasil disimpan.



Gambar 4.23 File isi percakapan pada database terdekripsi di Export ke format html.



Gambar 4.24 Foto Profil dari kontak pengguna WhatsApp

C. Reporting (Laporan)

Setelah tahap Pengumpulan, *Examination dan Analysis* berhasil dilakukan, maka barang bukti yang berkaitan dengan aplikasi WhatsApp telah didapatkan. Pada tahapan ini akan membahas dan menyajikan barang bukti

yang berhasil didapat yang berkaitan dengan aplikasi WhatsApp untuk mengungkapkan sebuah kasus kejahatan yang telah diskenariokan.

Tabel 4.2 Laporan Barang Bukti yang berhasil didapatkan

Informasi	Barang Bukti	Keterangan
Smartphone	Lenovo Model A369i	Ada
Nomor Handphone Pengguna	6282370786xxx	Ada
Nama Akun Korban	Raisa Korban	Ada
Penyimpanan Eksternal	SD Card	Ada
Kontak	10	Ada
Percakapan	4	Ada
Profil Picture	4	Ada
Tahun Percakapan	2019	Ada
Bulan Percakapan	Desember	Ada
Tanggal Percakapan	01	Ada
Waktu terjadi percakapan	Pukul : 23.03.02	Ada
<i>Tools</i>	Kingroot, Flashify, CWM Recovery, AccessData FTK Imager, WhatsApp Viewer, DB Browser for SQLite.	Ada

Untuk melihat kontak diponsel tersimpan pada file *wa.db* yang dapat dibuka dengan aplikasi *DB Browser for SQLite*, Aplikasi *DB Browser for SQLite* bisa didapat dengan mendownload melalui *Google Chrome*. Semua kontak yang tersimpan pada smartphone ditemukan, tidak hanya kontak yang terdaftar sebagai

pengguna aplikasi WhatsApp saja yang didapatkan, tetapi juga kontak pada smartphone yang tidak terdaftar sebagai pengguna aplikasi WhatsApp. Dapat dilihat pada gambar dibawah ini:

id	jid	whatsapp_use	status	status_timestamp	number	raw_contact_id	display_name	photo
1	62822751553...	1	you only see ...	1556071438000	082275155335	154	Putri Purwati	2
2	62853723420...	1	NULL	0	085372342088	164	Pi Wulan	2
3	621110@.wha...	0	NULL	0	+62111	353	TEKOMSSEL	2
4	62813166869...	0	NULL	0	+6281316686...	356	Pak Guh	2
5	62852949015...	1	NULL	0	085294901543	168	Kak Lita	2
6	62822767436...	1	NULL	0	082276743686	160	Pi Refi	2
7	6282757581...	1	Urgent calls o...	1572942726000	085275758123	156	Pi Maysarah ...	2
8	6282752047...	1	kekuatan doa	1540882560000	082275204723	162	Pi Rimmy	2
9	62813627977...	1	<input type="checkbox"/>	1568164583000	081362797794	158	Pi Darmita	2
10	62822436419...	1	Hey there! I a...	1573702973000	082243641939	166	Raisa Karbon	2

Gambar 4.25 Isi file wa.db yang merupakan Kontak pada smartphone Lenovo

D. Analisa Hukum Berdasarkan Barang Bukti yang telah di skenarioikan

Pada saat melakukan proses penelitian, penulis juga melakukan proses wawancara dan validasi hukum, yaitu:

1. Dengan salah satu anggota bagian *Cyber Crime* Polda Aceh, yang bertujuan untuk memastikan bahwa langkah-langkah penelitian yang penulis lakukan ini memiliki kesesuaian dengan yang dilakukan oleh bagian *Cyber Crime* Polda Aceh. Namun, ada beberapa data yang tidak boleh di publikasikan atau berbentuk rahasia yang tidak boleh diketahui oleh orang lain untuk menghindari agar tidak terjadi hal-hal yang tidak

diinginkan. Contohnya adalah *tools* yang digunakan dalam melakukan penyelidikan di Polda Aceh. Hasil yang diperoleh berdasarkan wawancara tersebut adalah langkah-langkah penelitian ini memiliki kesesuaian dengan yang dilakukan oleh bagian *Cyber Crime* Polda Aceh.

2. Kemudian Penulis juga melakukan proses validasi hukum yang bertujuan untuk memastikan bahwa pasal yang dikenakan sesuai dengan kasus yang disimulasikan, hasil yang diperoleh adalah undang-undang yang telah disebutkan diatas sudah sesuai dengan kasus yang disimulasikan. Validasi hukum ini dilakukan oleh Bapak Edi Yuhermansyah, S.H.I.,LL.M, yang merupakan salah seorang staf pengajar pada program studi Hukum Pidana Islam di Fakultas Syariah dan Hukum, UIN Ar-Raniry Banda Aceh.

Setelah menyelesaikan semua prosedur penelitian dan tahapan-tahapan yang terdapat dalam metode NIST, yaitu *Collection* (Pengumpulan), *Examination dan Analysis*, kemudian yang terakhir adalah membuat laporan atau *Reporting*, berdasarkan barang bukti yang telah didapat. Selanjutnya adalah melakukan analisa hukum terhadap kasus yang telah disimulasikan dan barang bukti yang didapatkan. Dalam penelitian ini ada dua kasus yang akan dilakukan analisis hukum, yaitu:

A. Kasus Pengiriman Konten Pornografi

Kasus ini terjadi dalam bentuk percakapan melalui aplikasi WhatsApp yang dilakukan oleh dua orang pengguna WhatsApp, mereka merupakan

seorang tersangka dan seorang korban. Berdasarkan Undang-undang yang berlaku di Indonesia, kasus pengiriman konten pornografi akan dikenai Undang-undang pasal 27 ayat (1) UU ITE, yang berbunyi sebagai berikut:

“Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.²⁴ Pelanggaran terhadap pasal 27 ayat (1) UU ITE dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp 1 milyar”.

B. Kasus Penghilangan Barang Bukti

Kasus yang kedua adalah setelah proses percakapan tentang konten pornografi dilakukan oleh tersangka terhadap korban, selanjutnya percakapan tersebut dihapus oleh tersangka, penghapusan tersebut bertujuan untuk menghilangkan barang bukti. Berdasarkan Undang-undang, kasus penghilangan barang bukti tersebut dikenai Undang-undang pasal 282 KUHP mengenai kejahatan terhadap kesusilaan, yaitu:

“barang siapa setelah dilakukan suatu kejahatan dan dengan maksud untuk menutupinya, atau untuk menghalang-halangi atau mempersukar penyidikan atau penuntutannya, menghancurkan, menghilangkan, menyembunyikan benda-benda terhadap mana atau dengan mana kejahatan dilakukan atau bekas-bekas kejahatan lainnya, atau menariknya dari pemeriksaan yang dilakukan oleh pejabat kehakiman atau kepolisian maupun oleh orang lain, yang menurut

²⁴ L. Heru Sujamawardi (2018), *Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik*, Jurnal Hukum Bisnis dan Investasi Vol.9, No. 2, hal.87.

ketentuan undang-undang terus menerus. Diancam dengan pidana penjara paling lama sembilan bulan”.



BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan permasalahan yang telah dijabarkan sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

1. Dengan menerapkan metode *National Institute of Standards and Technology* (NIST) maka akan mempermudah peneliti dalam menemukan barang bukti kejahatan digital pada smartphone yang dapat dijadikan barang bukti tindak pidana dengan mengikuti tahap demi tahap yang terdapat dalam metode *National Institute of Standards and Technology* (NIST).
2. *Tools* forensik yang digunakan untuk menemukan barang bukti digital pada perangkat pelaku adalah KingRoot (*tools* untuk melakukan *Rooting* pada smartphone), CWM (ClockworkMod) Recovery (File CWM yang akan di install), Flashify (untuk menginstall CWM), AccessData FTK Imager (melakukan *imaging* data), WhatsApp Viewer (mendekripsikan database WhatsApp yang terenkripsi dan membuka database WhatsApp yang sudah terdekripsi), DB Browser for SQLite (membuka folder wa.db untuk melihat daftar kontak ponsel).
3. Berdasarkan kasus yang disimulasikan maka aspek hukum yang akan dikenai ada dua, yang pertama adalah aspek hukum untuk kasus pornografi dikenai

Undang-undang pasal 27 ayat (1) UU ITE. Kasus yang kedua yaitu penghilangan barang bukti akan dikenai **pasal 282 KUHP**.

4. Berdasarkan kasus yang disimulasikan dan terjadi penghilangan barang bukti maka menurut ahli hukum undang-undang yang telah disebutkan diatas sudah sesuai dengan kasus tersebut.

B. Saran

Saran yang dapat diberikan untuk langkah pengembangan atau penelitian selanjutnya, sebagai berikut:

1. Dalam penelitian ini peneliti menggunakan metode *National Institute of Standards and Technology* (NIST) sebagai panduan, diharapkan untuk penelitian selanjutnya dapat menggunakan metode yang berbeda.
2. Untuk penelitian selanjutnya, dapat dilakukan pada Smartphone dengan merek yang lain sebagai objek penelitiannya.
3. Diharapkan untuk penelitian selanjutnya dapat menggunakan alat forensik yang berbeda dengan kasus *Cyber Crime* yang disimulasikan juga berbeda.
4. Diharapkan untuk program studi Pendidikan Teknologi Informasi (PTI) agar dapat memberikan materi-materi tentang *Cyber Crime* dan digital forensik pada matakuliah yang terdapat pada program studi Pendidikan Teknologi Informasi.

DAFTAR PUSTAKA

- Sobri, Muhammad, Emigawaty, Nita Rosa Damayanti. 2017. *“Pengantar Teknologi Informasi – Konsep dan Teori”*. Yogyakarta: CV. Andi Offset.
- Juditha, Christiany. 2015. *“Pola Komunikasi dalam Cybercrime (Kasus Love Scams)”*. Makassar: BBPPKI.
- Ambaranie Nadia Kemala Movanita. 2017. *“Ini Hasil Kerja Polri Perangi Kejahatan Kejahatan Cyber Sepanjang 2017”*. Kompas.com. (<https://nasional.kompas.com/read/2017/12/29/17233911/ini-hasil-kerja-polri%20perangi-kejahatan-siber-sepanjang-2017>), 2017.
- Rizki Ramadhan. *“Polri:Indonesia Tertinggi Kedua Kejahatan Siber di Dunia”*. CNN Indonesia. (<https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia>), 2018.
- JH, Jurnal. *“Cybercrime’ Kejahatan Baru di Aceh”*. Serambi news. (<https://aceh.tribunnews.com/2014/08/28/cybercrime-kejahatan-baru-di-aceh>), 2014.
- Riadi, Imam, sunardi, Muhamad Ermansyah Rauli. 2018. *“Indetifikasi Bukti Digital WhatsApp Pada Sistem Operasi Proprietary Menggunakan Live Forensics”*. Yogyakarta: Universitas Ahmad Dahlan.
- Bono, De Edward. 2007. *“Revolusi Berfikir”*. Bandung: Kaifa.
- Makinuddin. 2006. *“Analisis sosial: bersaksi dalam advokasi irigasi”*. Bandung: Yayasan Akatiga.
- Stiawan, Deris. 2006. *“Sistem Keamanan Komputer”*. Jakarta: PT Elex Media Komputindo.
- Sulianta, Feri. 2008. *“Komputer Forensik”*. Jakarta: PT Elex Media Komputindo.
- Pahrudin, Pajar. 2010. *“Etika Profesi Komputer”*. Jawa Barat: Goresan Pena Kuningan.
- Nasrullah, Rulli. 2016. *“Teori dan Riset Media Siber”*. Jakarta: Kencana.
- EMS Tim. 2009. *“Mengatasi Data Hilang dan Serangan Virus”*. Jakarta: PT Elex Media Komputindo.
- Riyanto. 2014. *“Validasi & Verifikasi Metode Uji”*. Yogyakarta: Deepublish.

Juddi, Moh Faidol, Nadya Sabrina Rahmat, Dadang Rahmat Hidayat, Aceng Abdullah, Dudi Sugianto, Siti Karlinah, Centurion Chandratama Priyatna. 2019. *“Communication and Information Beyond Boundaries: Seminar macom III Book Chapter”*. Bandung: Aksel Media Akselerasi.

Suryadi, Edi, Muhammad Hidayat Ginanjar, Muhamad Priyatna. 2013. *“Penggunaan sosial media whatsapp dan pengaruhnya terhadap disiplin belajar peserta Didik Pada Mata Pelajaran Pendidikan Agama Islam”*. Bogor: Stai Al-Hidayah.

Irianto Sulistyowati. 2006. *“Perempuan dan Hukum: Menuju Hukum yang Berperspektif Kesetaraan dan keadilan”*. Jakarta: Yayasan Obor Indonesia.

Nurdiansyah Rusdy. *“KPAI Catat Peningkatan Kasus Pornografi Anak Lewat Medsos”*. Republika.
<https://www.republika.co.id/berita/nasional/umum/19/07/24/pv5ezi320-kpai-catat-peningkatan-kasus-pornografi-anak-lewat-medsos>. 2019.



LAMPIRAN-LAMPIRAN LAMPIRAN 1

SURAT KEPUTUSAN DEKAN FTK UIN AR-RANIRY BANDA ACEH
NOMOR: B-1453/BA/03/FTK/PP.07.01/10/2019
TENTANG:

PENGANGKATAN PEMBIMBING SKRIPSI MAHASISWA FAKULTAS TARBİYAH DAN KEGURUAN
UIN AR-RANIRY BANDA ACEH
DEKAN FTK UIN AR-RANIRY BANDA ACEH

Menimbang : a. bahwa untuk kelancaran bimbingan skripsi dan ujian munaqasyah mahasiswa pada Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh maka dipandang perlu menunjuk pembimbing skripsi tersebut yang dituangkan dalam Surat Keputusan Dekan;
b. bahwa saudara yang tersebut namanya dalam surat keputusan ini dipandang cakap dan memenuhi syarat untuk diangkat sebagai pembimbing skripsi.

Mengingat : 1. Undang-Undang Nomor 20 Tahun 2003, tentang Sistem Pendidikan Nasional;
2. Undang-Undang Nomor 14 Tahun 2005, tentang Guru dan Dosen;
3. Undang-Undang Nomor 12 Tahun 2012, tentang Sistem Pendidikan Tinggi;
4. Peraturan Pemerintah No. 74 Tahun 2012 tentang Perubahan atas Peraturan Pemerintah RI Nomor 23 Tahun 2005 tentang Pengelolaan Keuangan Badan Layanan Umum;
5. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi;
6. Peraturan Presiden Nomor 64 Tahun 2013, tentang Perubahan Institut Agama Islam Negeri Ar-Raniry Banda Aceh menjadi Universitas Islam Negeri Ar-Raniry Banda Aceh;
7. Peraturan Menteri Agama RI Nomor 12 Tahun 2014, tentang Organisasi & Tata Kerja UIN Ar-Raniry Banda Aceh;
8. Peraturan Menteri Agama RI Nomor 21 Tahun 2015, tentang Statuta UIN Ar-Raniry Banda Aceh;
9. Keputusan Menteri Agama Nomor 492 Tahun 2003, tentang Pendelegasian Wewenang Pengangkatan, Pemindahan, dan Pemberhentian PNS di Lingkungan Depag RI;
10. Keputusan Menteri Keuangan Nomor 293/KMK.05/2011 tentang Penetapan Institut Agama Islam Negeri Ar-Raniry Banda Aceh pada Kementerian Agama sebagai Instansi Pemerintah yang Menerapkan Pengelolaan Badan Layanan Umum;
11. Keputusan Rektor UIN Ar-Raniry Nomor 01 Tahun 2015, tentang Pendelegasian Wewenang Kepada Dekan dan Direktur Pascasarjana di Lingkungan UIN Ar-Raniry Banda Aceh;

Memperhatikan : Keputusan Sidang/Seminar Proposal Skripsi Prodi Pendidikan Teknologi Informasi tanggal 18 September 2019

M E M U T U S K A N

Menetapkan :
PERTAMA : Menunjuk Saudara:
1. Khairan, M.Kom sebagai pembimbing pertama
2. Jiwa Malem Marsya, M.Sc sebagai pembimbing kedua

Untuk membimbing skripsi :
Nama : Mulla Fitriana
NIM : 150212108
Program Studi : Pendidikan Teknologi Informasi
Judul Skripsi : Penerapan Metode National Institute of Standards and Technology (NIST) Dalam Analisis Forensik Digital untuk Penanganan Cyber Crime ditinjau Dari Aspek Hukum yang berlaku

KEDUA : Pembiayaan honorarium pembimbing pertama dan kedua tersebut di atas dibebankan pada DIPA UIN Ar-Raniry Banda Aceh Tahun 2019;

KETIGA : Surat Keputusan ini berlaku sampai akhir semester Ganjil Tahun Akademik 2020/2021

KEEMPAT : Surat Keputusan ini berlaku sejak tanggal ditetapkan dengan ketentuan bahwa segala sesuatu akan diubah dan diperbaiki kembali sebagaimana mestinya, apabila kemudian hari ternyata terdapat kekeliruan dalam surat keputusan ini.

Ditetapkan di : Banda Aceh
Pada tanggal : 03 Oktober 2019
An. Rektor
Dekan

Muslimin Razali

Tembusan
1. Dekan UIN Ar-Raniry Banda Aceh;
2. Ketua Prodi Pendidikan Teknologi Informasi;
3. Pembimbing yang bersangkutan atau dimahasiswa dilaksanakan;
4. Yang bersangkutan.

LAMPIRAN 2



REMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
FAKULTAS TARBİYAH DAN KEGURUAN
Jl. Syekh Abdur Rauf Kope'ma Darussalam Banda Aceh
Telp: (0651) 7551423 - Fax: (0651) 7553020 Situs : ftk.uin.ar-raniry.ac.id

Nomor : B-14852/Un.08/FTK.1/TL.00/10/2019

Banda Aceh, 14 October 2019

Lamp : -

Hal : Mohon Izin Untuk Mengumpul Data
Penyusun Skripsi

Kepada Yth.

Di -
Tempat

Dekan Fakultas Tarbiyah dan Keguruan (FTK) UIN Ar-Raniry Darussalam Banda Aceh dengan ini memohon kiranya saudara memberi izin dan bantuan kepada:

N a m a : MULIA FITRIANA
N I M : 150212108
Prodi / Jurusan : Pendidikan Teknologi Informasi
Semester : IX
Fakultas : Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh
A l a m a t : Babah Jurong Kec. Kuta Baro Kab. Aceh Besar

Untuk mengumpulkan data pada:

POLDA ACEH

Dalam rangka menyusun Skripsi sebagai salah satu syarat untuk menyelesaikan studi pada Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry yang berjudul:

Penerapan Metode National Institute of Standards and Technology (NIST) dalam Analisis Forensic Digital untuk Penanganan Cyber Crime ditinjau Dari Aspek Hukum yang berlaku

Demikianlah harapan kami atas bantuan dan keizinan serta kerja sama yang baik kami ucapkan terima kasih.

An. Dekan,
Wakil Dekan Bidang Akademik
dan Kelembagaan,


Mustafar

Kode 3415

LAMPIRAN 3

Gambar 1. Foto Wawancara di Polda Aceh



Gambar 2. Foto Validasi Hukum oleh Dosen Hukum Pidana Islam UIN Ar-Raniry

