**Cyberspace**: Jurnal Pendidikan Teknologi Informasi
Volume 4, Nomor 1, Maret 2020, 29-39

# PENERAPAN METODE *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN *CYBER CRIME*

**Mulia Fitriana[1], Khairan AR[2], Jiwa Malem Marsya[3]**

[1,2,3] Pendidikan Teknologi Informasi, Fakutas Tarbiyah dan Keguruan
Universitas Islam Negeri Ar-Raniry Banda Aceh
E-mail: muliafitriana5@gmail.com, khairan.ar@ar-raniry.ac.id,
jiwa.malem.marsya@gmail.com

**Abstract**

The development of technology is currently developing very quickly, this is directly proportional to releasing cyber crime. One crime that often occurs is the case of Pornography. This application is done using one of the very popular Instant Messenger (IM) applications, the WhatsApp application. But after the crime is committed next or sending evidence in the form of conversations, video recordings, images and others committed by the suspect using the WhatsApp application. Therefore, this study proposes to find evidence related to digital pornography. This research produced a forensic procedure in conducting an investigation of the WhatsApp application to obtain previously published evidence containing a conversation session, a list of contact numbers, a profile photo of the victim and others. This research was conducted by reading a backup file of the encrypted WhatsApp application database that stores the conversation session that has been released. This research uses the method (National Institute of Standards and Technology (NIST). This digital evidence can be obtained using one of the forensic tools namely WhtasApp Viewer. The results obtained in this study contain WhatsApp contents that have been available which can be found digitally in uncovering the crime of pornography that is happen.

**Keywords**: *Digital Forensic, Cyber Crime, WhatsApp*

**Abstrak**

Perkembangan teknologi Smartphone saat ini tumbuh dengan semakin pesat, perkembangan yang demikian ternyata diikuti pula dengan meningkatnya tindak kejahatan dunia maya. Salah satu tindak kejahatan yang sering terjadi adalah kasus Pornografi. Kejahatan ini dilakukan dengan menggunakan salah satu aplikasi Instant Messenger (IM) yaitu aplikasi WhatsApp. Namun setelah kejahatan tersebut dilakukan selanjutnya pelaku atau tersangka menghapus barang bukti berupa percakapan, rekaman video, gambar dan lain sebagainya 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 yang sebelumnya telah dibackup melalui aplikasi WhatsApp yang terenkripsi yang menyimpan sesi percakapan yang sudang dihapus. Penelitian ini menggunakan metode (*National Institute of Standards and Technology* (NIST). Bukti digital tersebut dapat diperoleh menggunakan salah satu *tools* forensik yaitu

WhatsApp Viewer. Hasil yang didapat pada penelitian ini adalah isi percakapan WhatsApp yang sudah dihapus yang dapat menjadi bukti digital dalam mengungkap tindak kejahatan Pornografi yang terjadi.

**Kata kunci**: *Digital Forensik, Cyber Crime, WhatsApp*

## 1. Pendahuluan

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 [2]. Kapolri Jenderal Polisi Tito Karnavian mengatakan jumlah kasus yang menyangkut dengan kejahatan 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. Komisaris Jenderal Syafruddin yaitu Wakil Kepala Kepolisian Republik Indonesia menegaskan bahwa negara Indonesia masuk sebagai negara ke dua di dunia dengan kejahatan dunia maya tertinggi setelah negara jepang (CNN Indonesia, 2018).

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 kejahatan *Cyber Crime (Jurnalis, JH, 2014)*. 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*.

Berdasarkan penjelasan permasalahan diatas, maka 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.

## 2. Landasan Teori

### 2.1 Digital Forensik

Menurut Deris Stiawan (2006) dalam bukunya yang berjudul *Sistem Keamanan Komputer*, mendefinisikan Komputer Forensik adalah ilmu yang membahas tentang temuan yang berupa bukti digital setelah peristiwa yang berkaitan dengan keamanan komputer terjadi. Digital Forensik bisa dikatakan 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.

### 2.2 Mobile Forensik

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

### 2.3 *Cyber Crime*

*Cyber Crime* adalah kejahatan yang dilakukan oleh seseorang atau kelompok orang dengan pemanfaatan komputer atau internet. Menurut Pajar Pahrudin (2010) dalam bukunya Etika Profesi Komputer mendefinisikan bahwa Cyber Crime merupakan salah satu dampak negatif dari perkembangan teknologi yang menyebabkan kerugian sangat luas bagi seluruh kehidupan modern saat ini [3].

### 2.4 WhatsApp

WhatsApp merupakan aplikasi perpesanan paling popular 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 [4].

### 2.5 Data Recovery

Data Recovery merupakan suatu proses untuk mengembalikan data dari kondisi yang hilang, rusak, atau tidak bisa diakses ke kondisi awal yang normal.

### 2.6 Penegakan Hukum Pidana

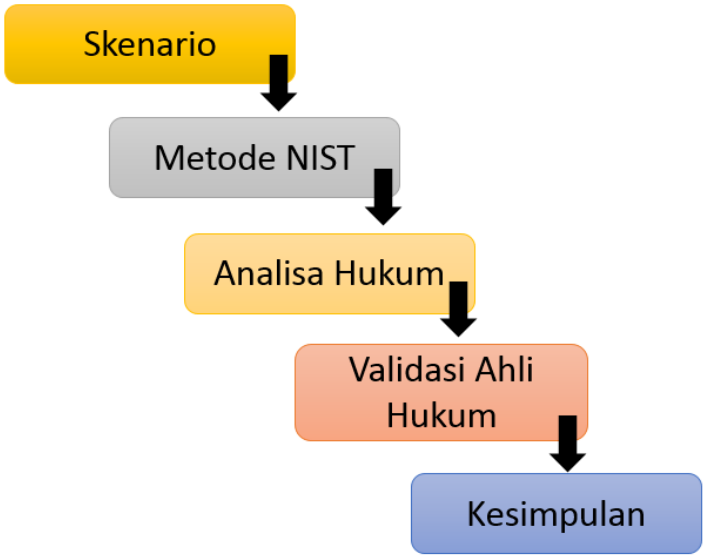
Di Indonesia dasar hukum pidana untuk kejahatan *Cyber Crime* sudah ada dalam Undang-undang no. 11 tahun 2008 yang isinya memuat ketentuan pidana bagi pelaku *Cyber Crime*. Untuk kasus *Cyber* pornografi sendiri tidak tercantum secara jelas didalam undang-undang no. 11 tahun 2008, tetapi “muatan yang melanggar kesusilaan”. Selain undang-undang no. 11 tahun 2008, telah ada beberapa undang-undang yang mengatur mengenai pornografi, antara lain KUHP yaitu Kitab Undang-undang Hukum Pidana dan undang-undang Nomor 44 Tahun 2008 tentang pornografi (UU Pornografi).

## 3. Metodologi Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode *National Institute of Standards and Technology* (NIST). NIST adalah sebuah metode yang memiliki empat tahapan dalam menyelesaikan dan menyelidikan kasus *Cyber Crime*, tahap pertama yaitu *Collection* (Pengumpulan Data), *Examination* (Pemeriksaan barang bukti), *Analysis*, dan yang terakhir adalah *Reporting* (Membuat laporan berdasarkan hasil analisis).

### 3.1 Langkah-langkah Penelitian

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




Gambar 1. Prosedur Penelitian

### 3.2 Rancangan Skenario

Skenario yang dijalankan untuk mempermudah investigasi dari kasus *cyber* pornografi 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.

### 3.3 Alat dan Bahan Penelitian

Alat dan bahan yang digunakan dalam investigasi forensik digital ini dapat dilihat pada tabel 1 berikut:

Tabel. 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 *rooting smartphone* 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 *imaging* data. | Perangkat Lunak |

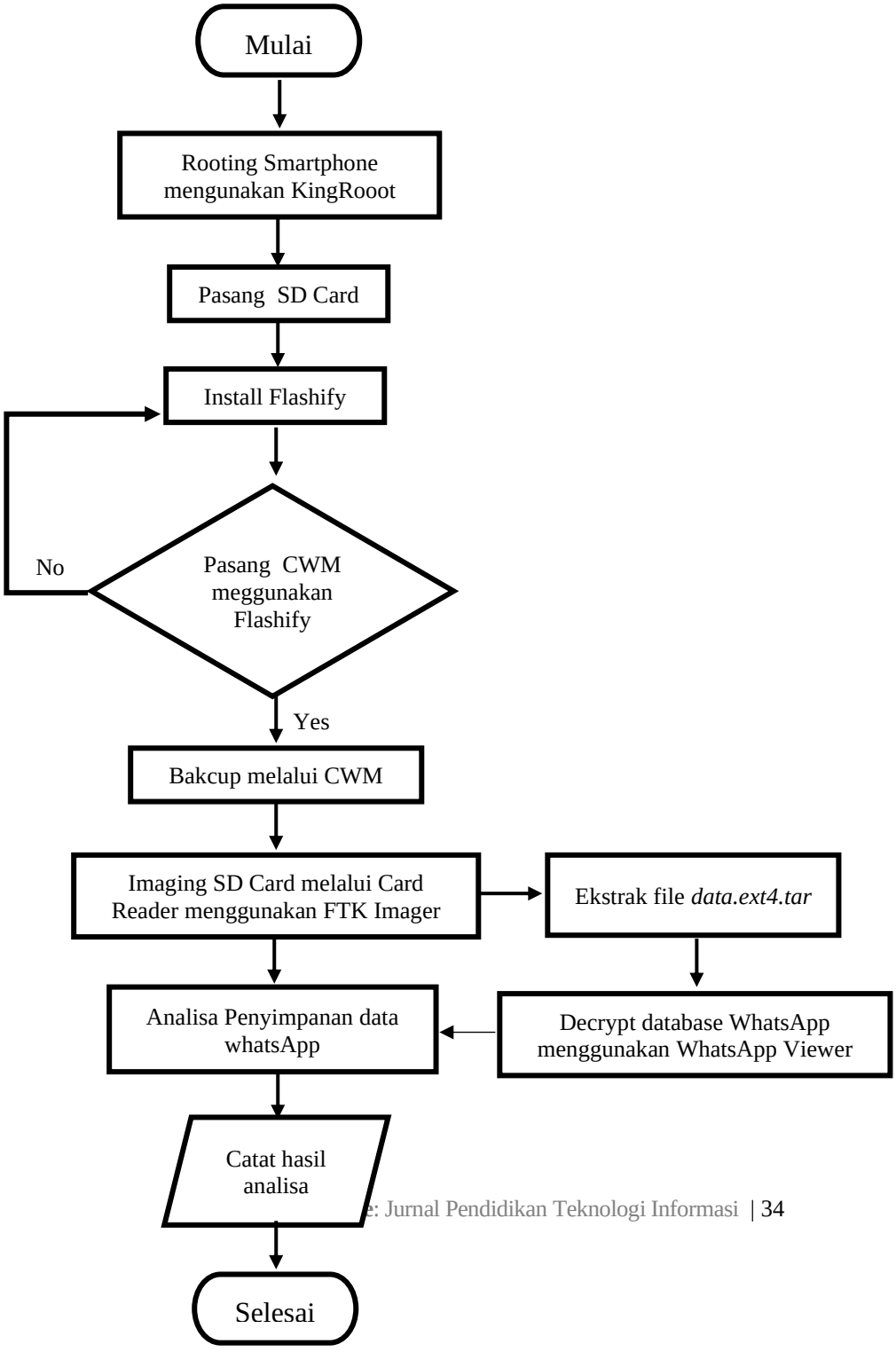
## 4. Hasil dan Pembahasan

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. Selanjutnya percakapan yang dilakukan dihapus dari perangkat pelaku yang bertujuan untuk menghilangkan barang bukti.

Gambar 2. Skenario Percakapan Tersangka dan Korban

## 4.1 Alur Kerja Analisis Forensik Digital

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:

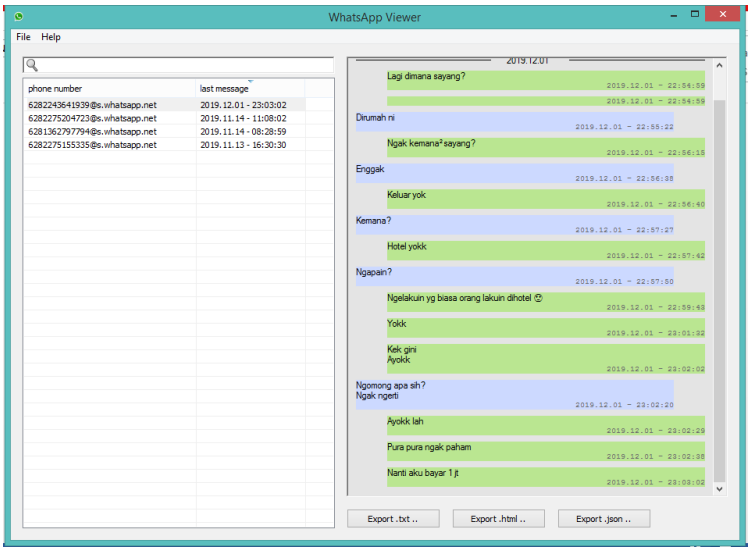


Gambar 3. Flowchart Analisis aplikasi WhatsApp

## 4.2 Hasil yang Ditemukan

### 4.2.1 Tampilan Chat WhatsApp Yang Telah Dihapus

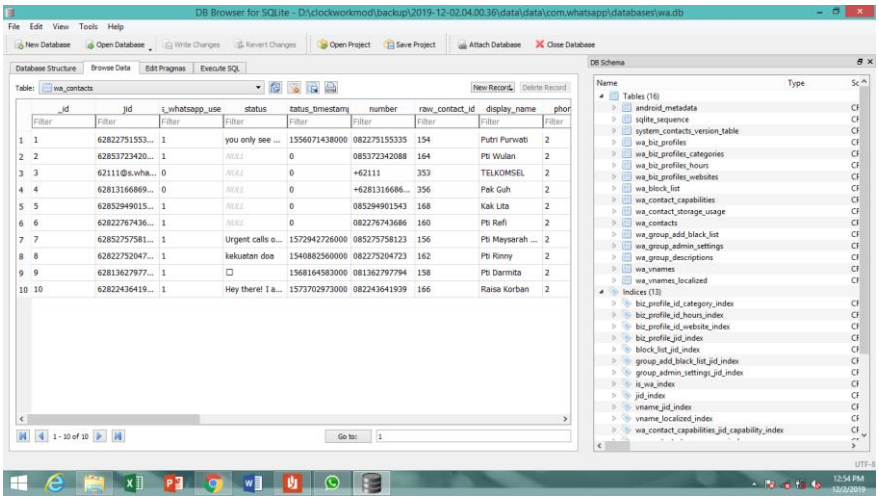
Setelah Proses berhasil dilakukan maka sesi pecakapan yang sudah di skenariokan berhasil didapat, Selain sesi percakapan, nomor kontak WhatsApp, tanggal/bulan/tahun dilakukannya percakapan beserta keterangan waktu yaitu dijam berapa percakapan tersebut dilakukan juga berhasil di dapat. seperti gambar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




Gambar 4. Contoh Chat WhatsApp yang berhasil didapatkan

### 4.2.2 Kontak pada Smartphone Pelaku

Semua kontak yang tersimpan pada smartphone berhasil ditemukan, tidak hanya kontak yang telah terdaftar sebagai pengguna aplikasi WhatsApp saja yang didapatkan, tetapi juga kontak pada smartphone yang tidak terdaftar sebagai pengguna aplikasi WhatsApp. Kontak yang ditemukan dapat dilihat pada gambar dibawah ini:



Gambar 5. Isi file wa.db yang merupakan Kontak pada smartphone Lenovo

### 4.2.3 *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 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 |
| *Tools* | Kingroot, Flashify, CWM Recovery, AccessData FTK Imager, WhatsApp Viewer, DB Browser for SQLite. | Ada |

### 4.2.4 Analisa Hukum Berdasarkan Barang Bukti yang telah di skenariokan

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 dosen 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, 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:

### 4.2.5 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.

### 4.2.6 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, Berdasarkan Undang-undang yang berlaku di Indonesia, kasus penghilangan barang bukti tersebut dikenai Undang-undang pasal 282 KUHP mengenai kejahatan terhadap kesusilaan.

## 5. Penutup

### 5.1 Simpulan

Berdasarkan permasalahan yang telah dijabarkan sebelumnya, maka dapat di tarik 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.

## 5.2 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

M. Sobri (2017). *Pengantar Teknologi Informasi-Konsep dan Teori*. CV. Andi offset.

C. Juditha (2015). *Pola Komunikasi dalam Cybercrime (Kasus Love Scams).* Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika.

Ramadhan 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.

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

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

M. faidol Juddi (2019). *Communication and Information Beyond Boundaries: Seminar macom III Book Chapter*. Bandung: Aksel Media Akselerasi.