



**ANALISIS KETERLIBATAN *CYBER*TERORISM MENGGUNAKAN
METODE ANALITYCAL HIERARCHY PROCESS (AHP)**

LUTHFI FEBRIANSYAH
15917112

*Tesis ini diajukan syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Magister Teknik Informatika
Program Pasca Sarjana Fakultas Teknologi Industri Universitas Islam
Indonesia
2018*

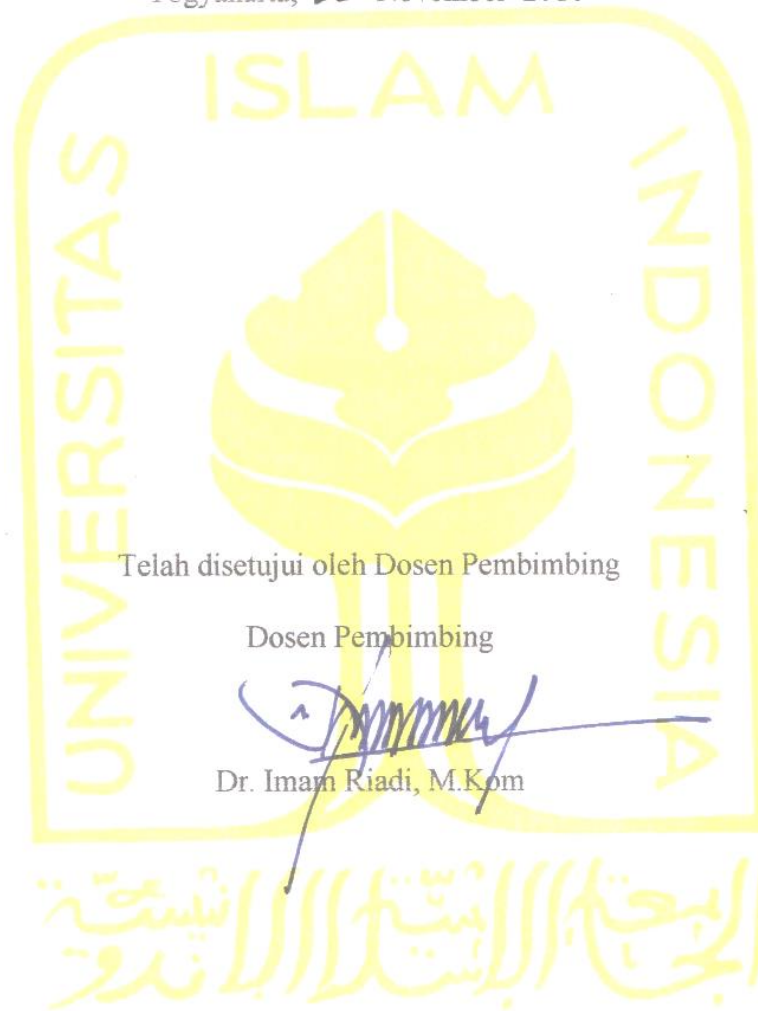
Lembar Pengesahan Pembimbing

**ANALISIS KETERLIBATAN *CYBER*TERORISM MENGGUNAKAN METODE
*ANALITYCAL HIERARCHY PROCESS (AHP)***

Nama: Luthfi Febriansyah

NIM: 15917112

Yogyakarta, 21- November 2018

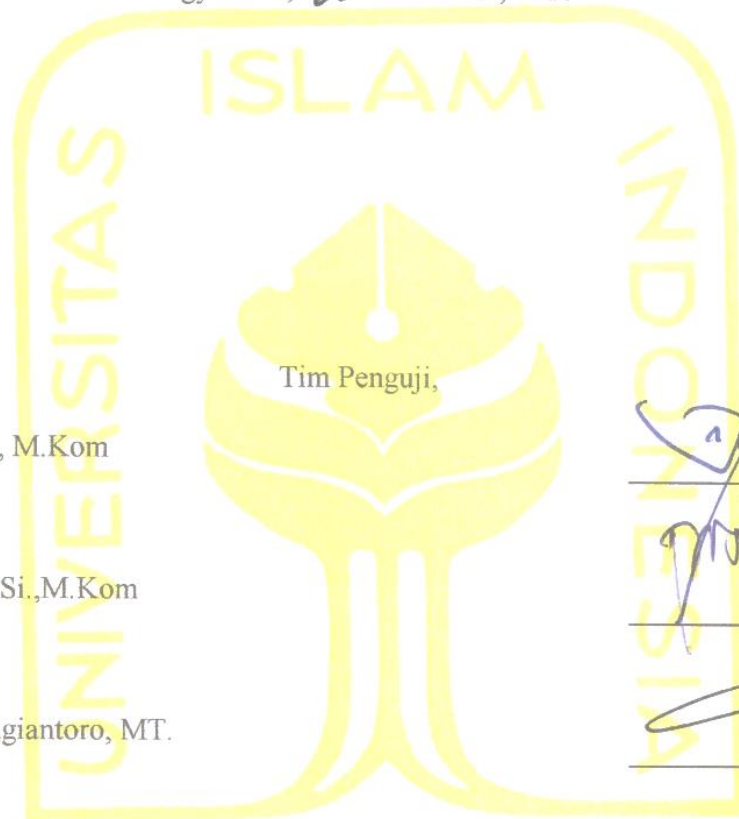


Lembar Pengesahan Penguji

ANALISIS KETERLIBATAN *CYBERTERORISM* MENGGUNAKAN METODE
ANALITYCAL HIERARCHY PROCESS (AHP)

Nama: Luthfi Febriansyah
NIM: 15917112

Yogyakarta, 23 November, 2018



Tim Penguji,

Dr. Imam Riadi., M.Kom
Ketua

Yudi Prayudi, S.Si., M.Kom
Anggota I

Dr. Bambang Sugiantoro, MT.
Anggota II

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia



Zaitunulhimmah S.T., M.Sc., Ph.D.

Abstrak

ANALISIS KETERLIBATAN *CYBERTERRORISM* MENGGUNAKAN METODE *ANALYTICAL HIERARCHY PROCESS* (AHP)

Daerah Istimewa Yogyakarta dalam kurun waktu 3 tahun terakhir ini kasus-kasus tindakan kekerasan meningkat, seperti aksi premanisme, perusakan makam yang menjadi cagar budaya dan kasus-kasus intoleransi agama. Perlu sebuah metode atau cara untuk mengidentifikasi atau mendapatkan informasi-informasi jaringan para pelaku dengan mengembangkan kasus. AHP (*Analytical Hierarchy Process*) merupakan metode analisis yang digunakan dalam penelitian ini, dengan menemukan bagaimana mendapatkan informasi-informasi keterlibatan jaringan-jaringan terorisme dari kasus yang sedang berjalan dengan melakukan *Mobile Forensik* dari barang bukti tersangka dan bagaimana cara menganalisis keterlibatan dari jaringan-jaringan tersebut dengan metode AHP. *Mobile Forensik* mampu menemukan jaringan-jaringan tersebut dan dengan metode AHP dapat ditentukan bahwa *contact alternative 3* merupakan prioritas utama untuk pengembangan kasus lebih lanjut dari jaringan-jaringan yang ditemukan.

Kata kunci: *cyberterrorism, AHP, digital evidence, mobile forensics*

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini. Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, 21-November 2018




Luthfi Febriansyah, ST

Publikasi selama masa studi

Publikasi yang menjadi bagian dari tesis

Luthfi Febriansyah, Riadi., I (n.d.). CYBERTERORISM PREDICTION ANALYSIS USING ANALITYCAL HIERARCHY PROCESS (AHP) METHOD

[JATIT] Letter of Acceptance for Submitted Research Paper ID 35516-JATIT  

 editor jatit <mailjatit@gmail.com> 3 Mei 2018 23.04   

ke saya, Imam ▾

 Inggris ▾ > Indonesia ▾ Terjemahkan pesan Nonaktifkan untuk: Inggris ×

Dear Corresponding Person LUTHFI-FEBRIANSYAH

We are pleased to inform you that your submission having title "CYBERTERORISM PREDICTION ANALYSIS USING ANALITYCAL HIERARCHY PROCESS (AHP) METHOD" and ID: 35516-JATIT having author(s): LUTHFI FEBRIANSYAH, IMAM RIADI has been **accepted for publication** in JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY (E-ISSN 1817-3195 / ISSN 1992-8645). The acceptance decision was based on the reviewers' evaluation after double blind peer review and chief editor's approval. **[Attached with this acceptance intimation]**

You shall submit OA processing fee (\$450) via credit card/paypal transaction through our online payment system (Use any valid credit card of Yourself / Friend / Family etc) . Please submit the dues via UK based payment system at <https://pay.paddle.com/checkout/507133>

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Luthfi Febriansyah	Menulis paper (60%)
Imam Riadi	Menulis dan mengedit paper (40%)

Kepersembahkan karya ini untuk kedua orang tua , istri dan anak saya juga untuk institusi Polri dan Bangsa ini. Terima Kasih atas semua doa, dukungan dan kesempatan yang sangat berharga ini.

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Alhamdulillah, segala puji bagi Allah SWT atas segala rahmat, hidayah, dan inayah-Nya, sehingga penulisan laporan tesis sebagai salah satu syarat memperoleh gelar Pascasarjana Magister Informatika Fakultas Teknologi Industri Universitas Islam Indonesia yang berjudul "**ANALISIS KETERLIBATAN CYBERTERORISM MENGGUNAKAN METODE ANALITYCAL HIERARCHY PROCESS (AHP)**" dapat penulis selesaikan dengan baik. Shalawat serta salam semoga senantiasa tercurah atas Nabi Muhammad SAW, para sahabat, serta pengikutnya hingga hari kiamat nanti.

Penyusunan laporan tesis ini tidak lepas dari bimbingan, dukungan, dan bantuan dari berbagai pihak. Oleh karena itu dalam kesempatan ini dengan segala kerendahan hati, penulis ingin menyampaikan ucapan terima kasih yang setulus-tulusnya kepada:

1. Kedua orang tua dan seluruh keluarga yang telah memberikan dukungan dan doa nya sehingga penulis dapat menyelesaikan studinya dengan baik.
2. Istri saya Arsanti Damawati, AM.Kg dan putra saya Keandre Luthfansa MR atas kesabaran, dukungan dan support nya.
3. Kapolda DIY **Brigjen Pol Drs. Ahmad Dofiri, M.Si** yang telah memberikan kesempatan untuk menjalankan study S2 di UII Yogyakarta.
4. Direktur Intelijen Keamanan Polda DIY **Kombes Pol Nanang Juni Mawanto, S.I.K** yang telah memberikan kesempatan dan support nya dalam penyelesaian study ini.
5. Rekan-rekan Subbagrenmin Ditintelkam Polda DIY.
6. Mbak Dwi angkatan X dan semua teman-teman saya angkatan XII, sebagai senior dan rekan se-angkatan yang memberikan masukan dan ide-ide dalam penelitian untuk menyelesaikan tesis ini.
7. Rektor dan seluruh jajaran Rektorat Universitas Islam Indonesia..
8. Dr. R. Teduh Dirgahayu, S.T., M.Sc. selaku Direktur Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
9. Dr. Imam Riadi, M.Kom., Dr. Bambang Sugiantoro, MT, dan Yudi Prayudi, M.Kom selaku dosen pembimbing dan penguji yang telah memberikan pengarahan, bimbingan, masukan, serta semangat selama pelaksanaan penulisan Tesis.
10. Dosen-dosen, jajaran staf program Pascasarjana Keluarga besar Magister Informatika

Semoga segala kebaikan yang telah diberikan kepada penulis, akan dibalas Allah dengan yang lebih baik. Penulis menyadari bahwa dalam penyusunan laporan tesis ini masih banyak terdapat kekurangan. Untuk itu penulis menyampaikan permohonan maaf serta sangat mengharapkan kritik dan saran yang membangun untuk penyempurnaan di masa mendatang. Akhir kata semoga laporan ini dapat bermanfaat bagi kita semua. Amin.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, November 2018

Luthfi Febriansyah, ST

DAFTAR ISI

Lembar Pengesahan Pembimbing.....	ii
Lembar Pengesahan Penguji.....	iii
Abstrak.....	iv
Pernyataan Keaslian Tulisan.....	v
Publikasi selama studi.....	vi
Publikasi yang menjadi bagian dari tesis.....	vi
Kata Pengantar.....	vii
	i
Daftar Isi	ix
Daftar Bagan/ Gambar.....	xi
Daftar Tabel	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
.	
1.2 Rumusan Masalah	6
.	
1.3 Batasan Masalah.....	6
.	
1.4 Tujuan Penelitian.....	6
.	
1.5 Manfaat Penelitian	7
.	
1.6 Review Penelitian.....	7
.	
1.7 Metodologi Penelitian	11
.	
1.8 Sistematika Penelitian	13
.	
BAB II TINJAUAN PUSTAKA	15
2.1 Forensic Digital	15
.	
2.2 Mobile Forensic	16
.	
2.3 Dampak Sosial Media	17
.	
2.4 <i>Analitycal Hierarchy Process (AHP)</i>	18
.	
2.5 Cyberterrorism	19
.	
2.6 Paham Radikal pada Sosial Media	21
.	
2.7 Intelijen Keamanan Polri	22
.	
BAB III METODOLOGI PENELITIAN	24

3.1	Preparation.....	24
.		
3.2	Case Simulation	26
.		
3.2	Digital Evidence	26
.		
3.3	Investigation Digital Evidence	27
.		
3.4	Report of Investigation	27
.		
3.5	Analisis Process AHP Method.....	27
.		
3.6	Found New TO	28
.		
3.7	Report/Produk Intelijen	28
.		
BAB IV ANALISIS DAN PEMBAHASAN		30
4.1	Case Simulation	30
.		
4.2	Digital Evidence	31
.		
4.3	Investigation Digital Evidence	32
.		
4.4	Report of Investigation	37
.		
4.5	Analisis.....	40
.		
4.6	Report/Produk Intelijen	46
.		
4.7	Pengujian Aplikasi Pemetaan Jaringan Terorisme.....	47
BAB V KESIMPULAN DAN SARAN		50
5.1	Kesimpulan	50
.		
5.2	Saran	50
.		
DAFTAR PUSTAKA		51

DAFTAR BAGAN/GAMBAR

1.1.	Metodologi Penelitian	11
2.1.	Struktur Tahapan AHP	19
2.2.	Struktur Organisasi Ditintelkam Tingkat Polda Tipe B	24
3.1.	Tahap-Tahap Penelitian	25
3.2.	Tahap Identifikasi Digital Evidence	27
3.3.	Bagan Alur Analisis Dengan AHP	28
3.4.	Alur analisa dengan aplikasi	29
4.1.	Tahap Penangkapan dan Penggeledahan Rumah RS	30
4.2.	Proses Meminjam Pakaian Barang Bukti kepada Ditintelkam Polda DIY melalui Ditreskrim yang Ditemukan Densus 88 AT di Lokasi Penggeledahan	31
4.3.	Hasil Investigasi Sie Inteltek Ditintelkam Polda DIY	31
4.4.	IMEI dari Smartphone Tersangka Samsung E7	32
4.5.	Informasi berdasarkan IMEI dari Barang Bukti Tersangka Smartphone Samsung E7 dengan Tools Online http://www.imei.info	32
4.6.	Persiapan Proses Root dengan Laptop atau PC	33
4.7.	Proses Root dengan Odin V3	33
4.8.	Tampilan Tools Andriller V2.5.2.0	34
4.9.	Proses Aquisisi Smartphone Tersangka dengan Menggunakan Tools Andriller	34
4.10.	Proses Aquisisi Smartphone Tersangka dengan Menggunakan Tools Oxygen Forensic	36
4.11.	Proses Physical Dump Oxygen Forensic Smartphone Tersangka	36
4.12.	Finishing Proccess Physical Dump Oxygen Forensic Smartphone Tersangka ..	37
4.13.	Hasil Proses Aquisisi dengan <i>Tools Oxygen Forensics</i>	37
4.14.	Capture Percakapan Tersangka dengan Whatsapp Messenger	38
4.15.	Capture Buku Tabungan dari Rekan Tersangka yang Bernama Muh. Syukron	39
4.16.	Capture Dokumen-Dokumen yang Ditemukan pada Smartphone Tersangka ...	40
4.17.	Capture Dokumen yang Mencurigakan dan Diproteksi	40
4.18.	Capture Dokumen Berupa Daftar Donatur Mengirimkan Sejumlah Dana	40
4.19.	Capture Halaman Login	41
4.20.	Capture Halaman Utama Aplikasi	41
4.21.	Produk Intelijen Sebagai Hasil dari Analisis	47
4.22.	Skenario System Pemetaan Jaringan Terorisme	47
4.23.	Proses penggunaan Aplikasi Pemetaan Jaringan Terorisme	48

DAFTAR TABEL

1.1.	Literature Review terhadap Penelitian	7
4.1.	Fitur Oxygen Forensic	35
4.2.	Tabel Contact Frekuensi Tertinggi yang Menghubungi Tersangka	38
4.3.	Tabel Contact yang Pernah Mengirimkan Dokumen atau Foto kepada Tersangka	38
4.4.	Tabel Keberadaan Contact yang Menghubungi Tersangka dalam Database Simpatisan ISIS dan Paham Radikal	39
4.5.	Tabel Konsep Eigenvector tentang Perbandingan dari Kriteria	42
4.6.	Tabel Pembobotan Kriteria	42
4.7.	Tabel Hasil Perhitungan dari Pembobotan Kriteria	43
4.8.	Tabel Normalisasi Pembobotan	44
4.9.	Tabel Uji Konsistensi	44
4.10.	Tabel Hasil Uji Konsistensi	44
4.11.	Perhitungan Penentuan Alternatif Berdasar Frekuensi	45
4.12.	Perhitungan Penentuan Alternatif berdasar Database	45
4.13.	Perhitungan Penentuan Alternatif Berdasar Dokumen	46
4.14.	Penentuan Ranking dari Alternatif yang Ada	46
4.15.	Pengujian Aplikasi	48
4.16.	Daftar Penguji Sistem 1.....	49
4.17.	Daftar Penguji Sistem 2.....	49

BAB I PENDAHULUAN

1.1. Latar Belakang Masalah

Daerah Istimewa Yogyakarta adalah daerah yang memiliki banyak julukan antar lain Kota budaya, Kota Sejarah, Kota Pelajar dan Kota Wisata. Sebagai konsekuensinya, Daerah Istimewa Yogyakarta memiliki masyarakat majemuk dengan karakteristik yang terdiri berbagai dari berbagai suku bangsa, agama, bahasa, budaya dan adat istiadat berbeda-beda. Keanekaragaman tersebut (dalam interaksi sosial antar warga) di kehidupan sehari-hari sering menimbulkan gesekan yang berpotensi menimbulkan gangguan kamtibmas. Hal ini perlu dikelola dengan baik oleh seluruh aparat pemerintah yang ada di Daerah Istimewa Yogyakarta sehingga setiap permasalahan yang muncul dapat terdeteksi dan terantisipasi dengan baik, mengingat DIY juga sebagai *city of tolerance*. Dalam kurun waktu 3 tahun terakhir ini kasus-kasus tindakan kekerasan di Daerah Istimewa Yogyakarta meningkat, seperti aksi premanisme, perusakan makam yang menjadi cagar budaya dan kasus-kasus intoleransi agama. Khusus dalam kasus-kasus intoleransi agama di Daerah Istimewa Yogyakarta disebabkan adanya komunitas ormas-ormas agama tertentu dengan paham Radikal yang dalam operasionalisasi di lapangan selalu menerapkan faham-faham fanatik yang kemudian diwujudkan dengan aksi-aksi radikal mulai dari melakukan operasi (*sweeping*) penyakit masyarakat sampai dengan ketidak setujuannya penganut agama yang lain melaksanakan kegiatan ibadah.

Terbukanya kran demokratisasi akhir-akhir ini telah menjadi lahan subur tumbuhnya kelompok Islam radikal. Fenomena radikalisme di kalangan umat Islam seringkali disandarkan dengan paham keagamaan, sekalipun pencetus radikalisme bisa lahir dari berbagai sumbu, seperti ekonomi, politik, sosial dan sebagainya. Radikalisme yang berujung pada terorisme menjadi masalah penting bagi umat Islam Indonesia dewasa ini. Dua isu itu telah menyebabkan Islam dicap sebagai agama teroris dan umat Islam dianggap menyukai jalan kekerasan suci untuk menyebarkan agamanya. Sekalipun anggapan itu mudah dimentahkan, namun fakta bahwa pelaku teror di Indonesia adalah seorang Muslim garis keras sangat membebani kondisi psikologis umat Islam secara keseluruhan. Keterlibatan berbagai pihak dalam menangani masalah radikalisme dan terorisme sangat diharapkan. Tujuannya adalah untuk mempersempit ruang gerak radikalisme dan terorisme, serta kalau perlu menghilangkan sama sekali. Dalam konteks di atas, peran sekolah dan lembaga pendidikan sangat penting dalam menghentikan laju radikalisme Islam. (Rokhmad, 2012).

Banyaknya kekacauan yang timbul dengan mengatasnamakan pembelaan terhadap agama menjadikan seorang bersikap radikal. Sikap radikal tersebut tidak hanya sebatas pemikiran ataupun pendapat, namun meningkat kepada perilaku dan perbuatan, yang kemudian muncul tindakan-tindakan yang merugikan banyak pihak, seperti klaim kebenaran, pengkafiran terhadap orang lain, hingga aksi bom dan aksi radikal lainnya. (Rahmawati, 2014)

Potensi terjadinya kasus-kasus intoleransi yang disebabkan adanya ormas-ormas agama paham Radikal di Daerah Istimewa Yogyakarta, menjadi ancaman tersendiri bagi Pemerintah RI pada umumnya dan Daerah Istimewa Yogyakarta pada khususnya sehubungan dengan munculnya fenomena kelompok radikal *Islamic State Iraq Syria* (ISIS). Sejarah dan ideologi ISIS ini diikuti berdasarkan kepemimpinan kelompok ini yang berawal dari kepemimpinan Abu Musqab Az Zaraqawi atau nama aslinya Ahmad Fadhil Nazzal al Khalaylah. Pola kepemimpinan dan strategi dari mulai Zaraqawi sampai kepada Abu bakar Al-Bagdadi memiliki beberapa strategi dalam melakukan implementasi dan mendiseminasi ketakutan kepada audiens, terutama daerah yang akan mereka duduki dengan melakukan invasi kekuatan militer secara besar-besaran. Di Indonesia, ISIS belum berdiri, hal ini dikarenakan beberapa kelompok radikal terdahulu hanya melakukan baiat dalam mendukung semua yang dilakukan ISIS (Tambunan, 2016).

Fenomena dan pengaruh paham ISIS di seluruh belahan di dunia sangat luar biasa dan dikhawatirkan paham ISIS ini berkembang di Daerah Istimewa Yogyakarta, sehingga sangat perlu dilakukan langkah-langkah antisipatif terhadap kelompok-kelompok radikal ini dengan cara deteksi dini dengan menggunakan *mobile forensic* guna mengetahui teknologi-teknologi yang digunakan dan tahapan-tahapan penggunaan *mobile forensic* tersebut sehingga didapatkan sebuah bahan keterangan/informasi yang bermanfaat bagi tugas kepolisian khususnya fungsi intelijen dalam deteksi dini dan peringatan dini (*early warning*), mengantisipasi pergerakan-pergerakan kelompok radikal tersebut.

Pada bulan September 2009, seorang gembong teroris bernama Noordin M Top tewas dalam penggrebekan Densus 88 Polri di Jebres Surakarta.

Dalam penggerebekan tersebut di sita sebuah laptop yang kemudian diselidiki oleh pihak kepolisian dan ditemukan data-data sebagai berikut:

1. file dokumen dalam bahasa indonesia berformat *pdf* menguraikan secara rinci cara mencari bahan, merakit, meledakkan bom;

2. ada bab Tadrid Takhasus yang menguraikan segala petunjuk tingkat mahir penggunaan segala jenis senjata api, cara menyimpan, membawa ke target saat pelaksanaan amaliat;
3. manual taktik strategi berperang diperkirakan bersumber dari kitab Mudzakaratul Amni milik Tandzim Al-qaida yang isinya dinilai berkualitas;
4. pada bab mengenai intelijen, isinya seperti menyalin buku mausuah Jihad Afghan;
5. dokumen Alqaida Asia Tenggara dalam bahasa Arab yang menyebutkan prosedur kaderisasi dan langkah-langkah menyelamatkan organisasi;
6. dokumen pengakuan Tandzim Alqaida di Afghanistan terhadap kepemimpinan Noordin M Top, Muhammad Syahrir, Syaefuddin Jaelani dan Ibrohim Muharram sebagai pimpinan Al-Qaeda Asia Tenggara;
7. pernyataan Al-Qaeda yang memberikan dukungan dan pembelaan terhadap tindakan kelompok Noordin di Asia Tenggara (Syafyess, 2009).

Hasil yang diperoleh dari pengungkapan isi laptop Noordin M Top tersebut sangat dirasakan manfaatnya dalam mendalami struktur dan kekuatan dari jaringan terorist yang dipimpin oleh Noordin M Top.

Dalam tubuh organisasi Polri yang memiliki *job description* mendapatkan informasi guna kepentingan tugas kepolisian lebih lanjut adalah fungsi Intelijen. Fungsi Intelijen pada Kepolisian Republik Indonesia dikenal dengan Intelijen Keamanan Polri yang pada tingkat Mabes Polri (pusat) adalah Badan Intelijen Keamanan (Baintelkam) Polri sedangkan di tingkat Polda adalah Direktorat Intelijen Keamanan (Ditintelkam) dan pada tingkat Polres disebut Satuan Intelijen Keamanan (Satintelkam). Sesuai peraturan Kapolri no 22 tahun 2010, Ditintelkam bertugas:

- a. membina dan menyelenggarakan kegiatan intelijen dalam bidang keamanan, termasuk persandian dan produk intelijen, pembentukan dan pembinaan jaringan intelijen kepolisian baik sebagai bagian dari kegiatan satuan-satuan atas maupun sebagai bahan masukan penyusunan rencana kegiatan operasional, dan peringatan dini (*early warning*);
- b. memberikan pelayanan administrasi dan pengawasan senjata api atau bahan peledak, orang asing, dan kegiatan sosial atau politik masyarakat sesuai dengan ketentuan peraturan perundang-undangan;
- c. mengumpulkan dan mengolah data serta menyajikan informasi dan dokumentasi kegiatan Ditintelkam.

Dalam melaksanakan tugas, Ditintelkam berfungsi:

- a. pembinaan kegiatan intelijen dalam bidang keamanan, antara lain persandian dan produk intelijen di lingkungan Polda;

- b. pelaksanaan kegiatan operasional intelijen keamanan guna terselenggaranya deteksi dini (*early detection*) dan peringatan dini (*early warning*) melalui pemberdayaan personel pengemban fungsi intelijen;
- c. pengumpulan, penyimpanan, dan pemutakhiran biodata tokoh formal atau informal organisasi sosial, masyarakat, politik, dan pemerintah;
- d. mendokumentasi dan menganalisa terhadap perkembangan lingkungan strategis serta penyusunan produk intelijen untuk mendukung kegiatan Polda;
- e. penyusunan prakiraan intelijen keamanan dan menyajikan hasil analisis setiap perkembangan yang perlu mendapat perhatian pimpinan;
- f. pemberian pelayanan dalam bentuk surat izin atau keterangan yang menyangkut orang asing, senjata api dan bahan peledak, serta kegiatan sosial atau politik masyarakat, dan SKCK kepada masyarakat yang membutuhkan, serta melakukan pengawasan dan pengamanan atas pelaksanaannya (Kapolri, 2010).

Forensika digital adalah Penggunaan metode ilmiah turunan dan pembuktian melalui tahapan *collection, validation, identification, analysis, interpretation, documentation, and presentation* dari barang bukti digital untuk merekonstruksi peristiwa sebagai temuan pidana, atau membantu untuk mengantisipasi tindakan ilegal yang merusak proses penyidikan. Sebagai bagian dari metode ilmiah dibutuhkan sebuah analisis yang dapat menuntun proses pembuktian yang prosedural dan menjaga proses tersebut dari kontaminasi barang bukti. Analisis ini dibutuhkan untuk membantu menentukan orang-orang atau bersifat kelompok dalam proses perkembangan paham-paham radikalisme di Yogyakarta. Dalam hal ini dibutuhkan metode pengambilan keputusan guna mempermudah proses analisis dan pada akhirnya membantu dalam proses pengambilan keputusan.

Dalam penelitian ini metode pengambilan keputusan yang digunakan adalah *Analitycal Hierarchy Process (AHP)*. *Analitycal Hierarchy Process (AHP)* merupakan suatu model pendukung keputusan yang dikembangkan oleh Thomas L Saaty. Model pendukung keputusan ini akan menguraikan masalah multi faktor atau multi kriteria yang kompleks menjadi suatu hirarki. Menurut Saaty (1993), hirarki didefinisikan sebagai suatu representasi dari sebuah permasalahan yang kompleks dalam suatu struktur multi level dimana level pertama adalah tujuan, yang diikuti level faktor, kriteria, sub kriteria, dan seterusnya ke bawah hingga level terakhir dari alternatif. Dengan hirarki, suatu masalah yang kompleks dapat diuraikan ke dalam kelompok-kelompoknya yang kemudian diatur menjadi suatu bentuk hirarki sehingga permasalahan akan tampak lebih terstruktur dan sistematis.

Analitycal Hierarchy Process (AHP) sering digunakan sebagai metode pemecahan masalah dibanding dengan metode yang lain karena alasan-alasan sebagai berikut:

1. struktur yang berhirarki, sebagai konsekuensi dari kriteria yang dipilih, sampai pada subkriteria yang paling dalam.
2. memperhitungkan validitas sampai dengan batas toleransi inkonsistensi berbagai kriteria dan alternatif yang dipilih oleh pengambil keputusan.
3. memperhitungkan daya tahan output analisis sensitivitas pengambilan keputusan.

(Syaifullah, 2010)

Dalam penelitian ini, penulis melakukan eksperimen dengan membuat sebuah simulasi kasus dari tersangka yang terkait dengan terorisme dan diperoleh beberapa alat bukti yang disita oleh pihak kepolisian dalam hal ini adalah Densus AT 88. Salah satu barang bukti tersebut adalah barang bukti digital berupa Smartphone yang dipinjam pakaikan kepada Direktorat Intelijen Keamanan Polda DIY untuk mengembangkan kasus terorisme dengan menemukan target-target baru untuk dilakukan pemantauan untuk keperluan kontra radikal dan terorisme.

Dalam penelitian ini *Analitic Hierarki Process* (AHP) merupakan metode yang digunakan untuk melakukan analisis dari hasil *aquisisi Smartphone* tersangka untuk mencari beberapa *contact* dari *Whatsapp Messenger* dengan kriteria-kriteria sebagai berikut:

- a. Frekuensi atau intensitas tinggi kepada tersangka
- b. *Contact* atau individu atau kelompok tersebut belum masuk dalam dalam Daftar Simpatisan ISIS atau Daftar Kelompok-Kelompok Radikal (*database*)
- c. Adanya dokumen atau informasi-informasi yang mengarah pada pergerakan ISIS atau Kelompok-Kelompok Radikal yang mengarah pada Terorisme

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan masalah yaitu :

- a. Bagaimana Mobile Forensics dapat membantu mendapatkan informasi-informasi yang berguna bagi tugas Kepolisian dalam mengungkap jaringan teroris?
- b. Bagaimana metode *Analitycal Hierarchy Process* (AHP) menganalisis keterlibatan jaringan *Cyberterrorism*?

1.3. Batasan Masalah

Dalam penelitian ini, ada beberapa batasan masalah yang dibuat adalah sebagai berikut:

- a. kasus yang dibahas adalah kasus yang sudah terjadi dan ditangani oleh pihak Kepolisian yaitu Direktorat Reserse Kriminal Umum (Ditreskrim) yang barang bukti digitalnya dipinjam pakaikan kepada Direktorat Intelijen Keamanan (Ditintelkam) guna mendapatkan informasi lebih lanjut;
- b. *investigasi Mobile Forensic*, yang diambil datanya adalah SMS, *call Log*, *email*, *facebook database* dan *Chat Whatsaap personal chat* beserta grup yang terdapat dalam *digital evidence*;
- c. data di analisis dengan menggunakan metode *Analitycal Hierarchy Process (AHP)* yang kemudian di olah dalam produk intelijen (laporan informasi) sebelum dilaporkan kepada *end user* (Kapolda DIY)

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

- a. mengembangkan tahap-tahap dalam penggunaan *mobile forensic* dari kasus-kasus sebelumnya;
- b. mendapatkan informasi yang bermanfaat tentang paham-paham Radikal dan dituangkan dalam produk intelijen.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah mendapatkan hasil analisis dengan *Analitycal Hierarchy Process (AHP)* dalam penggunaan *mobile forensic* dari kasus-kasus sebelumnya sehingga *end user* dalam hal ini adalah Kapolda DIY mendapatkan informasi untuk memonitor perkembangan paham radikal dan dapat menentukan langkah-langkah tepat untuk mengantisipasi.

1.6. Review Penelitian

Penelitian dengan tema yang hampir serupa pernah dilakukan seperti pada Tabel 1.1 :

Tabel 1.1 *Literature Review* Terhadap Penelitian

No	Peneliti dan Tahun	Metode	Hasil
1	Gabriel Weiman (2004)	<i>How Cyberterrorism Real and Threat</i>	Tantangan terbesar kita di depan adalah menghadapi ancaman cyberterrorism yang membingungkan, yang cukup menakutkan. Denning dan pakar terorisme menyimpulkan bahwa aksi pembajakan kendaraan, teror bom dan senjata biologis seperti aksi teror 9 november lalu yang sangat mengejutkan, tapi sebenarnya adalah pemberitaan yang dibesarbesarkan dan dimanipulasi tapi kita tidak bisa mengabaikan ataupun menolaknya.
2	Mikhail Kotykhov (2005)	<i>Determinant attributes of Customer Choice of Banks, Supplying Mortgage roduct</i>	Proses Hirarki Analitik digunakan untuk menjawab tujuan penelitian. Keputusan pilihan pelanggan telah terstruktur dari hierarki, menggabungkan keseluruhan tujuan (pilihan penyedia hipotek terbaik), atribut pengambilan keputusan pelanggan, serta sub-atribut, yang terkait dengan masing-masing atribut dan alternatif (bank)

Lanjutan tabel 1.1. *Literature Review* Terhadap Penelitian

No	Peneliti dan Tahun	Metode	Hasil
3	Nur Angga Adhitya Pratamaputra, dkk (2010)	Sistem Pendukung Keputusan Kenaikan jabatan dengan model AHP pada Biro Kepegawaian di Sekretariat Negara Republik Indonesia	<ol style="list-style-type: none"> 1. Perhitungan penilaian pegawai sudah menggunakan sistem pendukung keputusan yang terkomputerisasi sehingga dapat memberikan solusi pendukung keputusan BAPERJAKAT dalam menilai pegawai dan tidak menghabiskan banyak waktu dalam proses penilaiannya . 2. Dengan adanya SPK dapat memberikan solusi pendukung keputusan BAPERJAKAT untuk mengambil keputusan kenaikan jabatan pegawai, khususnya pada jabatan Kepala Biro Kepegawaian, Kepala Subbagian Mutasi Jabatan Non Struktural dan Kepala Subbagian Tata Usaha Kepegawaian. 3. Dengan adanya SPK ini BAPERJAKAT dapat langsung mencetak laporan hasil sidang BAPERJAKAT yang disertai dengan adanya grafik hasil penilaian.
4	Steve Saint-Claire (2011)	<i>Overview and Analysis on Cyber Terrorism</i>	Cyber-terorisme adalah isu kompleks yang sangat penting bagi pihak kepolisian dan harus bisa memahami karakteristik agar dapat melakukan evaluasi bagaimana pelaku-pelaku teror melakukan aksinya. Sehingga kita atau pihak kepolisian dapat melakukan pencegahan dan mengamankan dari aksi teror tersebut

No	Peneliti dan Tahun	Metode	Hasil
5	Indra Setia Dewi, dkk (2012)	Aplikasi Metode AHP dan SWOT untuk Perencanaan Strategi Lembaga Non Profit	Hasil analisis AHP-SWOT menghasilkan bahwa faktor Kekuatan memiliki bobot terendah dari kelompok faktor yang lain yaitu 0,138. Kelemahan mempunyai bobot 0,223, Peluang mempunyai bobot 0,298, dan Ancaman mempunyai bobot 0,341. Hal ini berarti Kekuatan yang dimiliki LEI belum dimanfaatkan secara maksimal sehingga harus ditingkatkan dan diperbaiki. Faktor-faktor Kelemahan dan Peluang juga penting untuk diperhatikan agar mampu menunjang program-program LEI yang sebaiknya ditujukan untuk mengatasi Ancaman, karena Ancaman merupakan kelompok faktor dengan bobot tertinggi
6	Eko Darmanto, dkk (2014)	Penerapan Metode AHP (<i>Analytic Hierarchy Process</i>) Untuk Menentukan Kualitas Gula Tumbu	<ol style="list-style-type: none"> 1. Aplikasi SPK Menentukan Kualitas Gula Tumbu ini, sudah dapat melakukan perhitungan dengan metode AHP (<i>Analytic Hierarchy Process</i>) lebih cepat dibandingkan perhitungan secara manual sehingga bisa lebih efisien dan tingkat keakuratan data sudah mendekati sempurna. 2. Seluruh pendataan yang berhubungan dalam Menentukan Kualitas Gula Tumbu meliputi data warna, data rasa, data kekerasan dan data perhitungan metode dapat diolah seluruhnya di dalam Aplikasi SPK Menentukan Kualitas Gula Tumbu ini dan dapat terorganisir dengan baik.

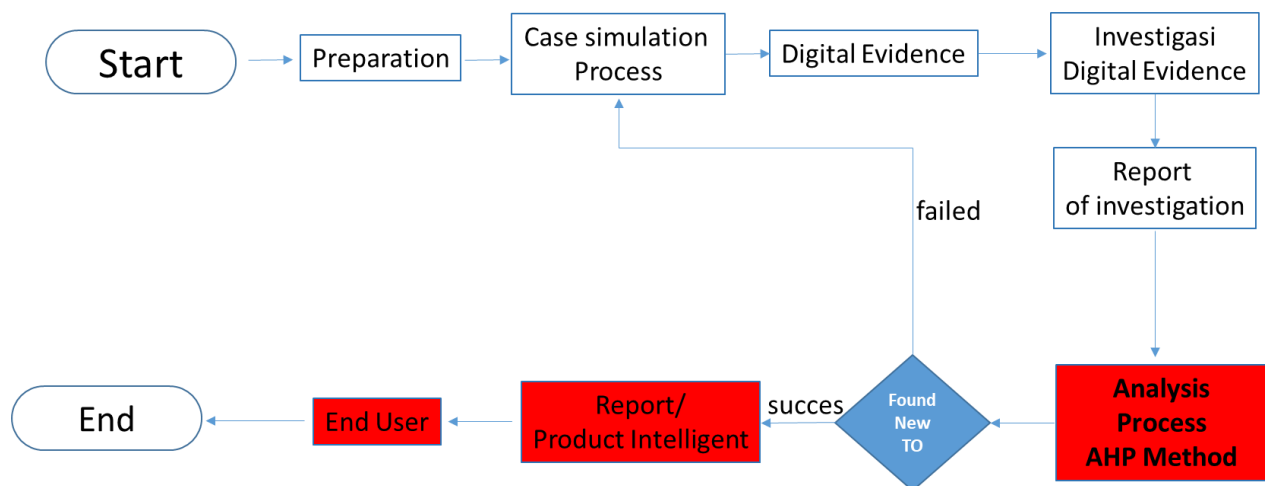
Lanjutan tabel 1.1. *Literature Review* Terhadap Penelitian

No	Peneliti dan Tahun	Metode	Hasil
7	Ming-Chang Lee (2014)	<i>Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method</i>	<ol style="list-style-type: none"> 1. Di bidang evaluasi; menentukan kriteria meliputi analisis risiko keamanan informasi, penilaian risiko keamanan informasi, dan manajemen keamanan informasi. 2. Sebagian besar penelitian tampaknya lebih menyukai metode AHP. 3. metode AHP dan Fuzzy Comprehensive Evaluation Method, lebih praktis untuk mengevaluasi keamanan informasi.
8	Rosaria de F. S. M. Russo and Roberto Camanho (2015)	<i>Criteria in AHP: a Systematic Review of Literature</i>	<p><i>Analytic Hierarchy Process</i> (AHP) banyak digunakan oleh pengambil keputusan dan peneliti. Definisi kriteria dan perhitungan bobotnya sangat penting dalam metode ini untuk menilai alternatifnya. Tujuan dari penelitian ini adalah untuk mengembangkan tinjauan literatur yang sistematis terhadap kasus nyata yang menerapkan AHP untuk dievaluasi bagaimana kriteria didefinisikan dan diukur. Dalam 33 kasus yang dipilih, mereka menggunakan literatur untuk membuat kriteria dan AHP atau Fuzzy AHP untuk menghitung beratnya, sedangkan teknik lainnya digunakan untuk mengevaluasi alternatif.</p>
9	Gianluca Riglietti (2016)	<i>Defining The Threat: What Cyber Terrorism Means Today And What It Could Mean Tomorrow</i>	<ol style="list-style-type: none"> 1. Komputer merupakan senjata utama dalam dunia cyberterrorism 2. Komputer digunakan sebagai alat untuk mendukung kelompok teroris (dengan sumber daya keuangan dan tenaga kerja) dan merencanakan serangan.
No	Peneliti dan Tahun	Metode	Hasil

10	Wiwik HT, SH (2017)	Optimalisasi Pelaksanaan Kontra Radikal dan Terorisme dalam Rangka Meningkatkan Sikap Waspada Masyarakat	Dalam upaya Kontra Radikal dan Terorisme maka perlu adanya terobosan berupa: a. Petunjuk arahan dalam pelaksanaan tugas dilapangan b. Pelatihan, pembentukan tim khusus serta pembentukan Posko Kontra Radikal dan Terorisme
----	---------------------	--	--

1.7. Metodologi Penelitian

Metodologi penelitian ini melalui tahapan seperti Gambar 1.1 :



Gambar 1.1 Metodologi Penelitian.

1.7.1. Preparation

Pada tahap ini, peneliti mempersiapkan baik itu literatur review dan pendukung penelitian ini seperti perangkat lunak (software) maupun perangkat kerasnya (hardware)

1.7.2. Case Simulation

Tahap ini berisi pembuatan skenario kasus yang merupakan gambaran kasus yang telah terjadi dan sudah ditidak lanjuti oleh pihak Kepolisian. Dimana kasus tersebut terdapat beberapa barang bukti yang salah satunya adalah *digital evidence*, yang dapat dipergunakan untuk mendapatkan informasi lebih lanjut dari kasus yang sudah ditindak lanjuti, sehingga dari informasi tersebut dapat memonitor jaringan dari kasus yang serupa.

1.7.3. Digital Evidence

Yaitu tahap mengidentifikasi barang bukti digital untuk mempersiapkan *tools* yang akan digunakan, berikut tahapan-tahapan yang dilakukan:

- a. *Identification Digital Evidence*, yaitu mengidentifikasi barang bukti digital apasaja yang dapat diinvestigasi guna mendapatkan informasi baru.
- b. *Preparing tools*, yaitu mempersiapkan *tools* yang dapat menginvestigasi dan sesuai dengan *digital evidence* tersebut.
- c. *Storage of digital evidence*, merupakan penyimpanan *digital evidence* guna menjamin keamanan dan keaslian *digital evidence* tersebut.

1.7.4. Investigasi Digital Evidence

Tahap ini berisi proses *extraction/ imaging* dari *digital evidence* yang diharapkan akan muncul atau diketahui sasaran baru yang dapat dimonitor perkembangannya.

1.7.5. Report of Investigation

Tahap ini merupakan hasil dari tahap ke 3 yang berupa dokumen sehingga investigator dapat melakukan penelitian terhadap target/sasaran dan dapat melakukan penginputan data ke dalam aplikasi Pemetaan Jaringan Teroris untuk *Analisis Process*.

1.7.6. Analisis Process AHP Method

Sebuah aplikasi yang mengolah *database* dari hasil investigasi *Digital Evidence* untuk mendapatkan informasi dari sosial media (*whatsapp messenger*) dari seorang tersangka yang dapat dianalisa sehingga *end user* dapat menentukan kebijakan dan langkah-langkah strategis.

Metode analisis menggunakan *Analitycal Hierarchy Process* (AHP), yaitu memberikan pembobotan pada *contact* yang berhubungan dengan tersangka dengan kriteria sebagai berikut:

- a. frekuensi atau intensitas tinggi kepada tersangka;
- b. *contact* atau individu atau kelompok tersebut belum masuk dalam dalam Daftar Simpatisan ISIS atau Daftar Kelompok-Kelompok Radikal (*database*);
- c. adanya dokumen atau informasi-informasi yang mengarah pada pergerakan ISIS atau Kelompok-Kelompok Radikal yang mengarah pada Terorisme

1.7.7. Report Produk Intelijen

Tahap ini merupakan pembuatan sebuah produk intelijen yang menggambarkan hasil analisis dengan menggunakan *Analitycal Hierarchy Process* (AHP) dalam menentukan target-target baru yang layak untuk dimonitor atau diwaspadai serta dimasukkan dalam *database*.

1.8. Sistematika Penelitian

Pada penulisan laporan tesis ini terdiri dari lima bab dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini akan diuraikan latar belakang permasalahan yang diangkat, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai teori-teori yang berkaitan dengan Analisis Prediksi *Cyberterrorism* Menggunakan Metode *Analitycal Hierarchy Process* (AHP).

BAB III METODOLOGI PENELITIAN

Pada bab ini diuraikan mengenai langkah-langkah yang dilakukan dalam Analisis Prediksi *Cyberterrorism* Menggunakan Metode *Analitycal Hierarchy Process* (AHP).

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini berisi tentang analisa dan evaluasi dari Analisis Prediksi *Cyberterrorism* Menggunakan Metode *Analitycal Hierarchy Process* (AHP).

BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi kesimpulan dari penelitian serta saran sehubungan dengan kemungkinan pengembangan pada penelitian selanjutnya.

BAB II TINJAUAN PUSTAKA

2.1. Forensic Digital

2.1. 1. Definisi

Penanganan kasus yang terkait dengan penggunaan teknologi informasi sering membutuhkan forensik. Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, *handphone*, tablet, PDA, *net-working devices*, *storage*, dan sejenisnya) Forensik digital dapat dibagi lebih jauh menjadi forensik yang terkait dengan komputer (*host*, *server*), jaringan (*network*), aplikasi (termasuk *database*), dan perangkat (*digital devices*). Masingmasing memiliki pendalaman tersendiri. (Raharjo, 2013)

Menurut Budhisantoso, “*digital* forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum.” (Asrizal, 2015)

2.2.2. Fungsi Komputer Forensik

Selaras dengan definisinya, secara prinsip ada tujuan utama dari aktivitas forensik komputer (Indrajit, 2011), yaitu:

- a. untuk membantu mengembalikan data (*recovery*), menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan;
- b. untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud. Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Kedua adalah

pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

2.2. Mobile Forensic

Mobile phone Forensic adalah sebuah ilmu untuk *recovery digital evidence* dimana *mobile phone* tersebut dalam kondisi *Forensically Sound* (keadaan jika mati agar tetap dalam kondisi mati, jika hidup tetap dalam kondisi hidup" saat diterima dilakukan sesuai prosedur penanganan. *Mobile Forensic* saat ini berkembang dengan pesat seiring berkembangnya *phone mobile* di masyarakat.

Mobile phone Forensic Analysis melibatkan *examiner mobile forensic* baik secara manual maupun secara otomatis, *Auto extraction* diguna jika *device compatible* dengan *software* dan *manual extraction* jika *device* tidak *compatible*. (Kevin Curran, 2010).

Penggunaan ponsel dalam kejahatan diakui dalam beberapa tahun ini, sedangkan studi forensik perangkat mobile merupakan bidang keilmuan yang relatif baru yang berawal pada tahun 2000-an. Perkembangan ponsel (terutama *smartphone*) di pasar konsumen menyebabkan peningkatan permintaan untuk mobile forensik, yang tidak semua dapat dipenuhi oleh bidang teknik komputer forensik (*Digital Forensic*).

Proses investigasi biasanya difokuskan pada data yang sederhana seperti data panggilan, dan komunikasi seperti email atau sms, dan juga data yang sudah terhapus dari media penyimpanan *mobile device*. *Mobile devices* biasanya juga bisa digunakan untuk menemukan informasi mengenai lokasi, yaitu menggunakan GPS atau alat pencari lokasi atau melalui *cell site logs*, yang melacak perangkat yang masuk di dalam *range* nya.

Informasi yang diambil dari perangkat mobile dapat berguna dalam berbagai masalah hukum, administratif dan investigasi seperti:

- a. pencurian kekayaan intelektual;
- b. penipuan online;
- c. penyalahgunaan properti;
- d. perceraian dan hukum keluarga;
- e. geo-lokasi kontroversi;
- f. bukti kejahatan (Fajar, 2014).

Dewasa ini trend *social networking* melalui media sosial telah menggiring perubahan perilaku dan gaya hidup manusia dalam bermasyarakat. Sebut saja diantaranya *facebook*, *twitter*, *path*, dan beberapa lainnya dengan *facebook* sebagai *leader*. Hal ini terbukti dari banyaknya pengguna aktif *facebook* sampai saat ini dan akan terus bertambah setiap harinya. Release resmi dari *newsroom facebook* sendiri bahwa sebanyak 1.01 milliard *user* aktif setiap

harinya dan sebanyak 894 jutanya merupakan pengguna aktif melalui ponsel, data per-september 2015. Sementara itu dikutip dari artikel *consumer.org* yang direlease pada tahun 2011 menyatakan bahwa 5 juta pengguna akun *facebook* pernah mengalami pelecehan dan 9,5 juta pengguna *facebook* menggunakan identitas palsu. Beberapa angka statistik dari *facebook* ini cukup memberikan kita gambaran seberapa banyak pengguna dan seberapa besar potensi media sosial ini untuk terlibat dalam semua jenis kegiatan manusia baik itu yang positif maupun yang negatif dan bukan tidak mungkin juga termasuk kegiatan yang bertentangan dengan hukum.

Data dan fakta tersebut kemudian menuntut dibutuhkannya suatu prosedur investigasi untuk membantu mengungkap sebuah kasus kejahatan sebagai respon ketika aktivitas salah satu akun *facebook* sudah menyentuh ranah hukum, baik itu pemalsuan/pencurian data pribadi, penipuan, penculikan, pencemaran nama baik, pembunuhan dan masih banyak potensi lain yang bisa saja menjadi modus operandi terbaru dalam sebuah kejahatan. *Facebook* merupakan ranah digital dan melibatkan teknologi komputer didalamnya tentu saja investigasi yang dilakukan adalah dengan cara teknik *digital forensics*. (fori.blogspot.co.id, 2016).

2.3. Dampak Sosial Media

Membaca berita dari internet, selain praktis, banyak sumber dan selalu *up to date*. Namun tak jarang saya juga dibingungkan dengan pemberitaan yang kontras antara media satu dengan media lain. Dimana media yang satu terkesan menjatuhkan, sedang media lainnya melakukan pembelaan. Tak sedikit pembaca yang kemudian terprovokasi berita-berita "yang seringnya belum jelas kebenaran atau sumbernya" tersebut. Buktinya bisa kita simak di postingan komentar yang lebih banyak hujatannya daripada kiritik/saran yang membangun. Komentar yang berisi hujatan, kata-kata kotor, bahkan binatang pun diabsen disana. Sering saya tak sanggup membacanya karena miris. (Hanifa, 2013)

Propaganda media untuk menghembuskan perang saat ini bisa diambil alih oleh media sosial atau jejaring sosial. Pertanyaannya, mengapa media sosial sedemikian dahsyat dalam menyebarkan pesan-pesannya? Pertama, masyarakat sedang euforia terhadap media sosial. Media itu sedang digandrungi masyarakat dunia. Tak ada warga kota yang tidak terpengaruh oleh media sosial. Bahkan semua media massa cetak dan elektronik sekarang harus memanfaatkan media sosial itu untuk menyebarkan pesan-pesannya. Dimanapun tempat, masyarakat memanfaatkan media sosial. Itu bukti betapa hebatnya pengaruh media sosial. Bahkan Indonesia menduduki ranking ke-4 pemakai *facebook* (43 juta pengguna) setelah

Amerika, India, dan Brazil. Kedua, media sosial mampu menyebarkan pesan secara revolusioner. Pesan yang disebarkan lewat media sosial sedemikian dahsyatnya memengaruhi sikap dan perilaku masyarakat. Contohnya adalah terjadinya Revolusi Mesir (2011) dengan tergulingnya Hosni Mubarak yang terjadi karena media sosial. Kaitannya dengan media sosial, Revolusi Mesir berawal dari inisiatif Wael Ghonim yang membuat akun FB ‘*We are all Khaled Said*’ pada Juli 2010. Akun tersebut kemudian menarik massa yang sangat banyak, khususnya yang menjadi oposan pemerintah. Akun itu dibuat Ghonim sebagai bentuk simpati terhadap Khaled Said yang menjadi korban penyiksaan anggota kepolisian Mesir di sebuah warnet di Alexandria. Akhirnya, kasus itu menjadi media komunikasi kelompok anti pemerintah dalam melakukan gerakan demonstrasi (Lutvia, 2011). Setelah akun ‘*We are all Khaled Said*’, pendukung-pendukung Ghonim kemudian membuat akun *facebook* lain. Salah satunya akun ‘*6th of April Youth Movement*’ yang juga digunakan untuk gerakan anti pemerintah. Selain FB, *twitter* juga digunakan. Melalui *twitter*, para demonstran saling berkomunikasi dan memberikan informasi tentang perkembangan demonstrasi Mesir. Ketiga, kepercayaan masyarakat pada media sosial melebihi kenyataan sebenarnya. Ini bisa dilihat karena sedemikian kuatnya kepercayaan manusia pada media sosial, meskipun kenyataannya belum tentu seperti itu. Analoginya bisa begini, seseorang yang kecanduan nonton tayangan hantu di TV mendadak bisa takut keluar malam karena seolah banyak hantu di sekelilingnya. Padahal kenyataan sebenarnya tidak sebagaimana ditayangkan dalam televisi. Itu sebabnya, media sosial juga telah menanamkan sebuah kepercayaan yang melampaui kenyataan sebenarnya. (Nurudin, 2012).

2.4. Analytical Hierarchy Process (AHP)

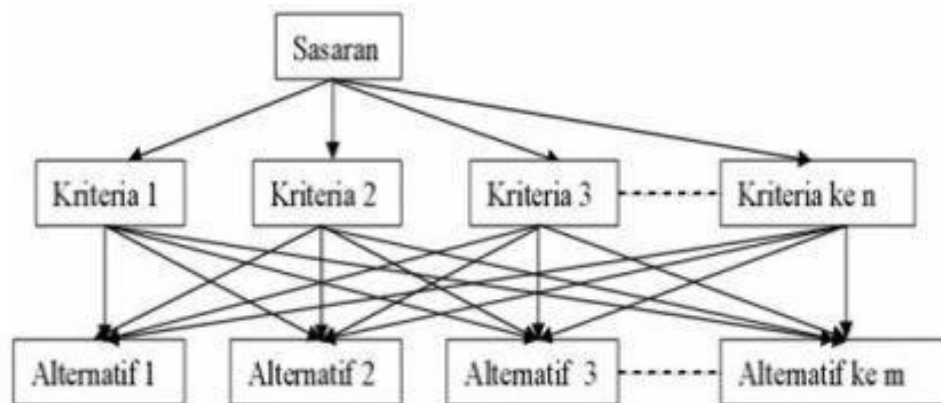
AHP merupakan suatu model pendukung keputusan yang dikembangkan oleh Thomas L Saaty. Model pendukung keputusan ini akan menguraikan masalah multi faktor atau multi kriteria yang kompleks menjadi suatu hirarki menurut Saaty (1993), hirarki didefinisikan sebagai suatu representasi dari sebuah permasalahan yang kompleks dalam suatu struktur multi level dimana level pertama adalah tujuan, yang diikuti level faktor kriteria, sub kriteria, dan seterusnya ke bawah hingga level terakhir dari alternatif. Dengan hirarki suatu masalah yang kompleks dapat diuraikan ke dalam kelompok-kelompoknya yang kemudian diatur menjadi suatu bentuk hirarki sehingga permasalahan akan tampak lebih terstruktur dan sistematis.

AHP sering digunakan sebagai metode pemecahan masalah dibanding dengan metode yang lain karena alasan-alasan sebagai berikut:

1. struktur yang berhirarki, sebagai konsekuensi dari kriteria yang dipilih, sampai pada subkriteria yang paling dalam;
2. memperhitungkan validitas sampai dengan batas toleransi inkonsistensi berbagai kriteria dan alternatif yang dipilih oleh pengambil keputusan;
3. memperhitungkan daya tahan output analisis sensitivitas pengambilan keputusan (Syaifullah, 2010).

Tahapan-tahapan yang dilakukan dalam mendukung pengambilan keputusan AHP adalah sebagai berikut:

- a. mendefinisikan masalah dan menentukan solusi yang diinginkan.
- b. membuat struktur hierarki yang diawali dengan tujuan umum, dilanjutkan dengan kriteria-kriteria dan alternatif-alternatif pilihan (Eko Darmanto, 2014), seperti Gambar 2.1.



Gambar 2.1. Struktur tahapan AHP.

2.5. Cyber Terrorism

Christopher Beggs et al dalam penelitiannya pada tahun 2009 yang berjudul “*Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption*” mengatakan bahwa saat ini kelompok teroris menggunakan *Information and Communication Technologies (ICTs)* dalam mengatur serangan-serangan mereka. Baru-baru ini mereka mengembangkan serangan dengan berbasis *Cyber*. Dalam penelitiannya Christopher Beggs mengidentifikasi bagaimana pentingnya *cyber terrorism* yang memiliki *capabilitas*, *imperative* dan integral juga melakukan penelitian dalam melakukan penilaian komponen-komponen yang dapat meningkatkan resiko dari *cyber terrorism* pada system SCADA. (Waren, 2009)

William Gibson dalam bukunya *Neuromancer* (1984) mengatakan bahwa *Cyberspace* dapat disebut juga sebagai komunikasi elektronik dunia virtual yang memungkinkan interaksi dari sebuah komunitas atau kelompok dalam menyimpan dan mendapatkan informasi. Eksploitasi *cyberspace* terus dikembangkan oleh semua pihak yang memiliki kepentingan. (Rollins et al 2015).

Dalam sebuah pernyataan dilaporkan Hamid Mir Koran Ausaf, Osama Bin Laden mengatakan, setelah serangan 11 September dimana ratusan pemuda telah berjanji kepadanya bahwa mereka siap untuk mati dan bahwa ribuan ilmuwan muslim yang bersama dengannya dan dengan menggunakan pengetahuan mereka dalam bidang kimia, biologi dan komputer untuk membantu melawan kaum kafir. Sejak pernyataan ini dicetak, telah dilaporkan bahwa:

- a) *encrypted*, rencana rinci untuk menghancurkan pesawat berada pada komputer laptop Ramzi Yousef;
- b) Osama bin Laden memanfaatkan email yang telah terenkripsi untuk mengirimkan instruksi serangan 11 September kepada Mohhamed Atta;
- c) sistem Kontrol Pengawasan dan Akuisisi Data (SCADA) telah mampu diakses oleh kelompok Al Qaeda dalam mengumpulkan para intelijen sebagai sasaran potensial.

Sistem SCADA digunakan untuk memantau dan mengontrol peralatan utilitas seperti Sistem listrik dan distribusi air;

- d) dalam komputer yang dimiliki Al Qaeda ditemukan struktur dan olah data yang terkait dengan kekuatan kelompoknya;
- e) Khalid Ibrahim anggota dari Pakistan kelompok teroris Harkat Al Ansar, diketahui menggunakan metode social engineering untuk mendapatkan informasi tentang *hacking* ke jaringan militer US;
- f) jaringan Al Qaeda yang telah ditahan, selama interogasi menyatakan niat mereka untuk menggunakan jaringan komputer untuk melancarkan tujuan mereka (Colarik, 2006).

2.6. Paham Radikal Pada Sosial Media

Menurut Kamus Besar Bahasa Indonesia (KBBI) Media sosial merupakan sarana untuk berkomunikasi dengan sesama manusia di suatu lingkungan kelompok secara bersama yang sangat baik dan pas digunakan dalam menyebarkan berbagai informasi penting terlepas dari hanya sekedar hiburan, informasi pribadi bahkan hingga informasi yang sifatnya propaganda. Media sosial ini juga tidak jarang dijadikan sasaran para oknum yang memiliki

kepentingan dalam menggalang, propaganda bahkan untuk provokasi yang lebih cenderung ke arah negatif.

Banyak lapisan masyarakat dari berbagai daerah di seluruh dunia telah mampu mengoperasikan media sosial ini, mulai dari anak-anak hingga kaum manula. Kebutuhan manusia akan informasi dan didukung oleh kemajuan teknologi yang semakin pesat mendorong setiap manusia menggunakan teknologi dalam sosial media untuk mendapatkan dan menyebarkan informasi. (Mahrus, 2014)

Dalam film dokumenter *Jihad Selfie* yang dibuat oleh Noor Huda Ismail, dijelaskan bagaimana proses anggota perekrutan ISIS. Mereka mulai dari sosial media, masuk ke anak-anak muda, memberikan mereka pemahaman tentang citra ideal islam versi mereka, kemudian setelah si anak muda tadi tertarik mereka diminta berbaiat menjadi gerombolan ISIS. Sementara ISIS dengan gencar bekerja merekrut, mencari, dan menyebarkan paham mereka di Internet, beberapa dari kita berdebat tentang apakah melawan ISIS di Internet itu efektif? Apakah #hashtag bisa mengubah keadaan? Perdebatan ini membuat banyak orang berhenti memerangi ISIS di media sosial. ISIS tidak peduli akan debat itu, mereka terus gencar mempropagandakan kebencian mereka setiap hari. Berdasarkan laporan dari Brookings Institute pada Desember (2014) ada 46.000 akun *twitter* yang berafiliasi dan mendukung ISIS tentu saja tidak semua akun itu hidup dan aktif, namun jika 10 persen saja aktif, bayangkan berapa banyak propaganda kebencian yang dilancarkan? (IRIB Indonesia/VIVAnews/RA, 2014). Kementerian Komunikasi dan Informatika (Kemkominfo) diminta untuk tidak diam dan segera menggerakkan masyarakat dalam memerangi propaganda kelompok militan Islamic State of Iraq and Syria (ISIS).

Setelah terjadinya teror Paris yang menewaskan 129 orang, gerakan peretas dunia bersatu dalam wadah Anonymous, bergerak memerangi *hacker-hacker* ISIS yang selama ini gencar melakukan propaganda melalui dunia maya. "Ini sangat positif dan menjadi semacam mobilisasi dari masyarakat. Artinya ada arus baru yang langsung tumbuh dari masyarakat untuk melawan ISIS. Ini tentu bisa menjadi kekuatan yang dahsyat karena lahir dari masyarakat dan wajib digalakkan di Indonesia," "Intinya, harus ada yang membentengi sehingga pemerintah perlu berbicara serius dengan kelompok masyarakat seperti NU untuk membuat aksi pencegahan membendung propaganda ISIS melalui sosial media. Salah satu contoh, adalah tindakan NU melaporkan situs VOA-Islam yang selama ini nyata-nyata menjadi corong ISIS di Indonesia. Situs itu dinilainya dengan membuat berita dengan sumber tidak benar, fitnah, apalagi menunjuk organisasi dan juga tokoh NU Gus Dur. Ini sudah ada yang berani muncul yaitu NU. Kita harapkan pemerintah menangani serius laporan ini. Efek

yang ditimbulkan dari keberadaan situs-situs negatif ini sudah sangat buruk. Dalam kaitan itu, Adnan menilai apa yang pernah dilakukan Badan Nasional Penanggulangan Terorisme (BNPT), yang pernah mengusulkan pemblokiran situs-situs negatif tentang propaganda paham kekerasan dan ISIS, adalah salah satu tindakan yang tepat. kata Tokoh Muda Nahdlatul Ulama, Adnan Anwar, Kamis (26/11). (www.beritasatu.com, 2015)

Cyber Terrorism adalah konvergensi dunia maya dan terorisme. Hal ini mengacu pada serangan yang melanggar hukum dan ancaman serangan terhadap komputer, jaringan dan informasi yang tersimpan di dalamnya dilakukan untuk mengintimidasi atau memaksa pemerintah atau orang-orang dalam kelanjutan dari tujuan politik atau sosial. Selanjutnya, untuk memenuhi syarat sebagai cyber terorisme, serangan harus menghasilkan kekerasan terhadap orang atau properti, atau setidaknya menyebabkan cukup membahayakan untuk menghasilkan rasa takut. Serangan yang menyebabkan kematian atau luka-luka, ledakan, atau kerugian ekonomi yang parah adalah contoh seperti itu. serangan serius terhadap infrastruktur penting mungkin aksi terorisme *cyber*, tergantung pada dampaknya. Serangan yang mengganggu layanan yang tidak penting atau yang terutama gangguan mahal tidak akan dianggap terorisme *cyber*. (Nor 2016)

2.7. Intelijen Keamanan Polri

Kepolisian Republik Indonesia (Polri) adalah sebuah lembaga negara yang bertugas untuk menjaga keamanan, ketertiban, perlindungan dan pengayoman terhadap masyarakat. Ada 5 fungsi teknis kepolisian yaitu Intelijen Keamanan (Intelkam), Reserse Kriminal (Reskrim), Lalu Lintas (Polantas), Sabhara dan Pembinaan Masyarakat (Binmas).

Peranan Intelkam Polri sangat menentukan tugas-tugas kepolisian dan mendukung semua fungsi teknis yang ada di kepolisian karena tugas Intelkam Polri adalah mendahului, menyertai dan mengakhiri.

2.7.1. Pengertian Intelijen

Istilah “intelijen” berasal dari kata *Intelegensia* yang artinya adalah “kecerdasan”. Ini memberikan makna bahwa pekerjaan intelijen memerlukan kecerdasan. Dalam arti luas, intelijen merupakan suatu proses yang pengelolaannya memerlukan pemikiran, untuk menghasilkan informasi penting tentang sesuatu yang telah dan akan terjadi. Untuk melaksanakannya diperlukan suatu alat yang disebut kecerdasan, namun makna kecerdasan dalam intelijen tidak hanya sekedar pintar menguasai Ilmu Intelijen, tetapi juga bermakna

memiliki banyak akal, mampu memahami masalah, mampu membaca situasi dan mampu menyesuaikannya dengan cepat.

Sebagai ilustrasi, alat kecerdasan itu pula yang membedakan Intelijen dengan peramal dalam menghasilkan informasi penting tentang sesuatu yang akan terjadi. Sedangkan peramal menggunakan kekuatan batin, ilmu gaib, perasaan dan lain-lain yang bersifat mistik atau irasional. (Karwita, 2001)

2.7.2. Intelijen dalam Kepolisian Republik Indonesia

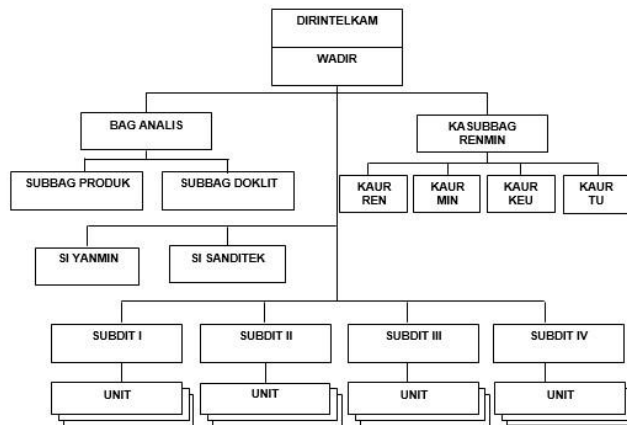
Fungsi Intelijen pada Kepolisian Republik Indonesia dikenal dengan Intelijen Keamanan Polri yang pada tingkat Mabes Polri (pusat) adalah Badan Intelijen Keamanan (Baintelkam) Polri sedangkan di tingkat Polda adalah Direktorat Intelijen Keamanan dan pada tingkat Polres disebut Satuan Intelijen Keamanan. Sesuai peraturan Kapolri no 22 tahun 2010, Direktorat Intelijen Keamanan (Ditintelkam) bertugas:

- a. membina dan menyelenggarakan kegiatan intelijen dalam bidang keamanan, termasuk persandian dan produk intelijen, pembentukan dan pembinaan jaringan intelijen kepolisian baik sebagai bagian dari kegiatan satuan-satuan atas maupun sebagai bahan masukan penyusunan rencana kegiatan operasional, dan peringatan dini (*early warning*);
- b. memberikan pelayanan administrasi dan pengawasan senjata api atau bahan peledak, orang asing, dan kegiatan sosial atau politik masyarakat sesuai dengan ketentuan peraturan perundang-undangan;
- c. mengumpulkan dan mengolah data serta menyajikan informasi dan dokumentasi kegiatan Ditintelkam.

Dalam melaksanakan tugas, Ditintelkam berfungsi:

- a. pembinaan kegiatan intelijen dalam bidang keamanan, antara lain persandian dan produk intelijen di lingkungan Polda;
- b. pelaksanaan kegiatan operasional intelijen keamanan guna terselenggaranya deteksi dini (*early detection*) dan peringatan dini (*early warning*) melalui pemberdayaan personel pengemban fungsi intelijen;
- c. pengumpulan, penyimpanan, dan pemutakhiran biodata tokoh formal atau informal organisasi sosial, masyarakat, politik, dan pemerintah;
- d. pendokumentasian dan penganalisisan terhadap perkembangan lingkungan strategis serta penyusunan produk intelijen untuk mendukung kegiatan Polda;
- e. penyusunan perkiraan intelijen keamanan dan menyajikan hasil analisis setiap perkembangan yang perlu mendapat perhatian pimpinan;

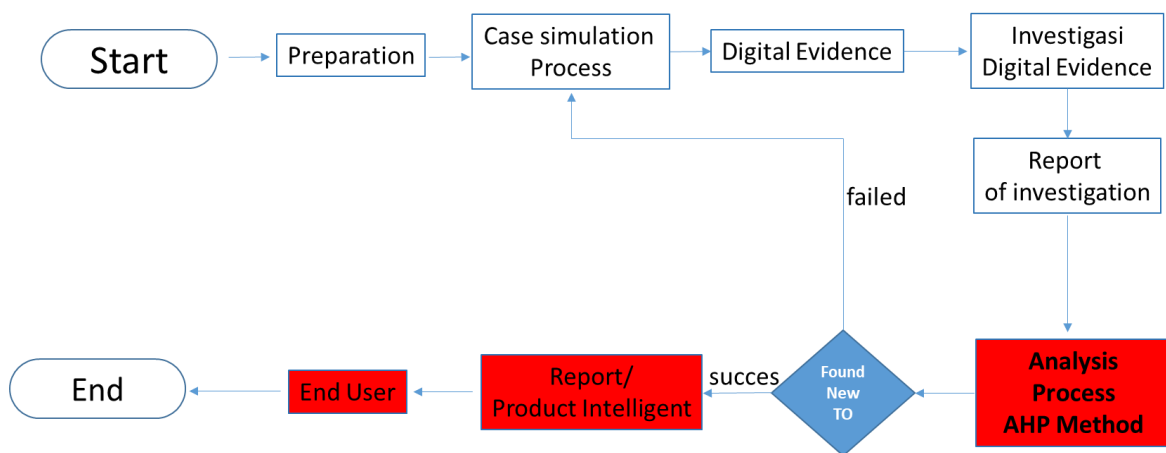
- f. memberikan pelayanan dalam bentuk surat izin atau keterangan yang menyangkut orang asing, senjata api dan bahan peledak, serta kegiatan sosial atau politik masyarakat, dan SKCK kepada masyarakat yang membutuhkan, serta melakukan pengawasan dan pengamanan atas pelaksanaannya (Kapolri, 2010) seperti tampilan pada Gambar 2.2.



Gambar 2.2. Struktur organisasi Ditintelkam tingkat Polda tipe B.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan bagaimana cara penelitian ini dilakukan sehingga dapat diketahui rincian tentang langkah-langkah dalam mendapatkan informasi dan dapat dijadikan pedoman yang jelas dalam penyelidikan guna memonitor target sehingga dapat diambil langkah-langkah yang tepat. Adapun langkah-langkah atau tahapan-tahapan penelitian ini seperti dalam tampilan pada Gambar 3.1.



Gambar 3.1. Tahap-tahap penelitian.

3.1. Preparation

3.1.1. Literatur Review

Studi literature/*Literature Review* dilakukan untuk mendapatkan informasi mengenai topik penelitian yang dapat bersumber dari dokumen, buku, artikel, atau bahan tertulis lainnya, yang berupa teori, laporan penelitian, atau penemuan sebelumnya dimana menemukan uraian tentang teori, temuan, dan bahan penelitian lainnya yang diperoleh dari bahan acuan untuk dijadikan landasan kegiatan penelitian untuk menyusun kerangka pemikiran yang jelas dari perumusan masalah yang ingin diteliti. *Literature Review* merupakan cerita ilmiah terhadap suatu permasalahan tertentu.

Literature Review berisi ulasan, rangkuman, dan pemikiran-pemikiran tentang beberapa sumber pustaka (paper, artikel, buku, slide, informasi dari Internet, dan lain-lain) tentang topik yang dibahas.

3.1.2. Preparing Tools

Sebelum melakukan penelitian maka penulis mempersiapkan beberapa tools mulai dari identifikasi Digital Evidence sampai dengan tahap analisis EWS (*Early Warning System*), antara lain adalah:

A. Software

- 1) Info IMEI online : <http://www.imei.info>
- 2) Oxygen Forensic
- 3) Andriller
- 4) Sqlite Browser
- 5) Odin3-v3.10.6
- 6) Notepad ++
- 7) Php Myadmin / Sql Database

B. Hardware

- 1) Laptop Lenovo G40
- 2) Data Cable
- 3) OTG
- 4) Eksternal HD

3.2. Case Simulation

Atau simulasi kasus, merupakan gambaran kasus yang telah terjadi dan sudah ditindak lanjuti oleh pihak Kepolisian. Dimana kasus tersebut terdapat beberapa barang bukti yang salah satunya adalah *digital evidence*, yang dapat dipergunakan untuk mendapatkan informasi lebih lanjut dari kasus yang sudah ditindak lanjuti, sehingga dari informasi tersebut dapat memonitor jaringan dari kasus yang serupa.

3.3. Digital Evidence

Ini didapatkan dari simulasi kasus yang sudah ditindak lanjuti oleh pihak kepolisian. Adapun tahapan setelah adanya *digital evidence* adalah sebagai berikut:

- a. *indentification Digital Evidence*, yaitu mengidentifikasi barang bukti digital apa saja yang dapat diinvestigasi guna mendapatkan informasi baru.
- b. *preparing tools*, yaitu mempersiapkan tools yang dapat menginvestigasi dan sesuai dengan *digital evidence* tersebut.

c. *storage of digital evidence*, merupakan penyimpanan *digital evidence* guna menjamin keamanan dan keaslian *digital evidence* tersebut. (Asrizal, 2012). Adapun tampilan tahapan setelah adanya *digital evidence* seperti Gambar 3.2.



Gambar 3.2. Tahap identifikasi *digital evidence*.

3.4. *Investigation Digital Evidence*

Tahap ini adalah melakukan proses *extraction/imaging* dari digital evidence yang diharapkan akan muncul atau diketahui sasaran baru yang dapat dimonitor perkembangannya (Yunus Yussof, 2011).

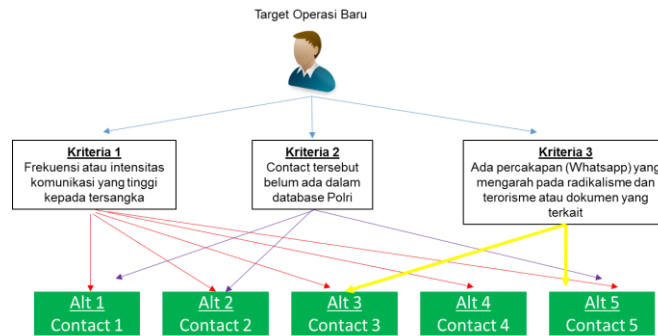
3.5. *Report of Investigation*

Tahap ini merupakan hasil dari tahap ke 3 yang berupa dokumen sehingga investigator dapat melakukan penelitian terhadap target/sasaran dan dapat melakukan penginputan ke dalam Early Warning System (Ben Martini, 2012).

3.6. *Analisis Process AHP Method*

Metode analisis yang digunakan adalah AHP (*Analytical Hierarchy Process*). Yaitu memberikan pembobotan pada contact-contact yang berhubungan dengan tersangka dengan kriteria sebagai berikut:

- Frekuensi atau intensitas komunikasi yang tinggi kepada tersangka;
- Contact atau individu atau kelompok tersebut belum masuk dalam daftar simpatisan ISIS atau daftar kelompok-kelompok radikal (database);
- Adanya dokumen atau informasi-informasi yang mengarah pada pergerakan ISIS atau kelompok-kelompok radikal yang mengarah pada terorisme seperti terlihat dalam Gambar 3.3.



Gambar 3.3. Bagan alur analisis dengan AHP.

Keterangan :

- Alt 1 : Alternatif contact 1
- Alt 2 : Alternatif contact 2
- Alt 3 : Alternatif contact 3
- Alt 4 : Alternatif contact 4
- Alt 5 : Alternatif contact 5

3.7. Found New TO

Dari hasil aquisisi Smartphone milik tersangka, maka didapatkan beberapa contact yang sering berhubungan dengan tersangka dengan kriteria sebagai berikut:

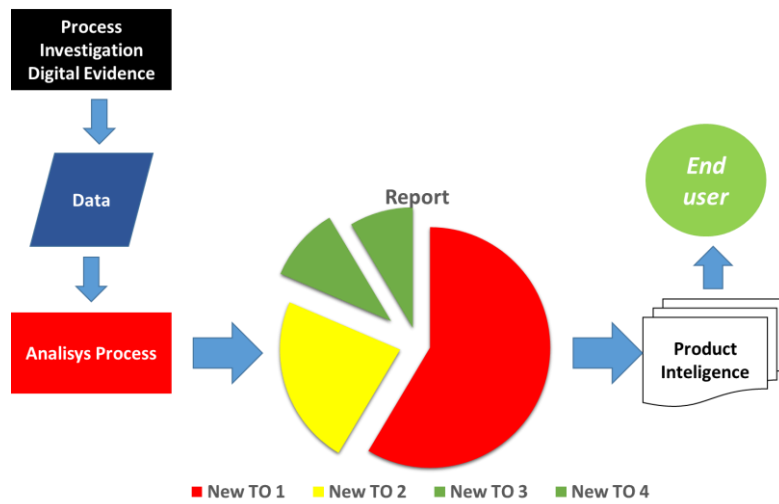
- Frekuensi atau intensitas komunikasi yang tinggi kepada tersangka;
- Contact atau individu atau kelompok tersebut belum masuk dalam database simpatisan ISIS atau Kelompok-Kelompok Radikal;
- Adanya dokumen atau informasi-informasi yang mengarah pada pergerakan ISIS atau Kelompok-Kelompok Radikal yang mengarah pada Terorisme.

Dengan metode AHP akan melakukan pembobotan dan perangkingan dari alternatif/alternatif contact.

3.8. Report Produk Intelijen

Tahap ini merupakan pembuatan sebuah laporan yang menggambarkan hasil analisis sampai dengan tingkat penentuan target-target baru, dalam hal ini laporan yang dimaksud didunia intelijen adalah Laporan Informasi atau Laporan Khusus yang ditujukan kepada Direktur

Intelijen Keamanan Polda dan diteruskan kepada Kapolda DIY sebagai *end user*, seperti terlihat pada Gambar 3.4. (Kabaintelkam, 2014).



Gambar 3.4. Alur analisa dengan aplikasi

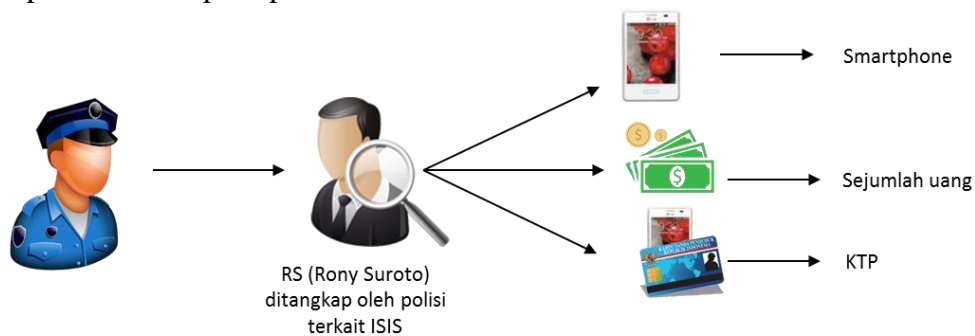
BAB IV ANALISIS DAN PEMBAHASAN

4.1. Case Simulation

Pada Selasa siang 16 Agustus 2017 di Dusun Jeruk, Desa Kepek, Kecamatan Wonosari Gunungkidul Yogyakarta telah diamankan terduga anggota teroris sdr Rony Suroto (RS) umur 33 tahun, agama Islam. Dari hasil penggeledahan dirumah RS, diamankan beberapa barang bukti yaitu berupa:

- 1 buah HP Smartphone Samsung Galaxy E7
- Uang sejumlah Rp. 240.000,-
- KTP terduga teroris berinisial RS dan domisili Tegal Jawa Tengah

Ilustrasi pra insiden seperti pada Gambar 4.1.



Gambar 4.1. Tahap penangkapan dan penggeledahan rumah RS

Proses penangkapan tersebut dilakukan oleh Densus 88 Anti Teror Polri dibantu oleh Sat Reskrim Polres Gunungkidul dan beberapa anggota Satbrimobda DIY. Selain RS juga diamankan istri RS beserta 3 anaknya dan 1 anak dari kakak RS. Barang bukti yang diamankan saat penggeledahan disimpan di Ditreskrimum Polda DIY untuk penyelidikan lebih lanjut. Ditintelkam Polda DIY meminjam pakai barang bukti tersebut untuk mendapatkan target-target yang lain, dengan melayangkan nota dinas kepada Direktur Reskrimum Polda DIY dengan nomor: B/ND- 1256/VIII/2017/Ditintelkam tanggal 18 Agustus 2017 yang selanjutnya akan dilakukan investigasi oleh Sie Inteltek Ditintelkam Polda DIY, seperti pada Gambar 4.2.

Insident



Gambar 4.2. Proses meminjam pakaian barang bukti kepada Ditintelkam Polda DIY melalui Ditreskrim yang ditemukan Densus 88 AT di lokasi penggeledahan.

Setelah dilakukan investigasi yang dilakukan oleh Sie Inteltek Ditintelkam Polda DIY, ditemukanlah hasil seperti yang terlihat pada Gambar 4.3.

Past Insiden



Gambar 4.3. Hasil investigasi Sie Inteltek Ditintelkam Polda DIY.

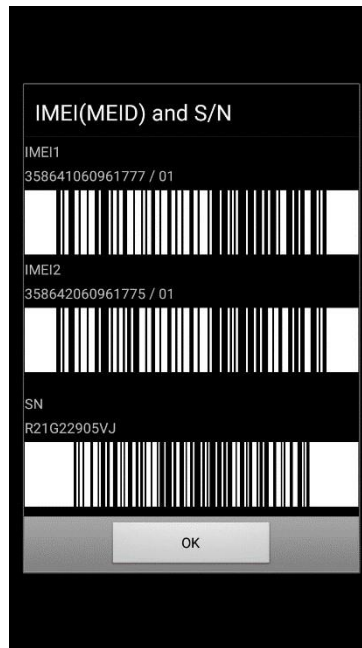
4.2. Digital Evidence

4.2.1. Identification Digital Evidence

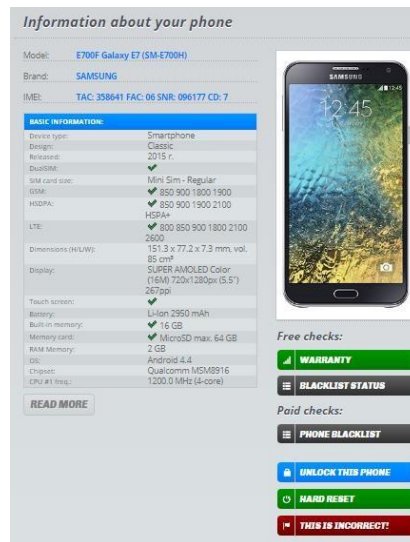
Sie Inteltek Polda DIY telah melakukan investigasi terhadap barang bukti yang telah ditemukan pada saat penggeledahan di rumah terduga teroris RS. Dari identifikasi barang bukti tersebut maka didapatkan informasi seperti terlihat pada Gambar 4.4. dan 4.5.

- Merk : Samsung Galaxy E7
- IMEI 1 : 358641060961777 / 01
- IMEI 2 : 358642060961775 / 01

- SSID :



Gambar. 4.4 IMEI dari smartphone tersangka Samsung E7.



Gambar. 4.5. Informasi berdasarkan IMEI dari barang bukti tersangka Smartphone Samsung E7 dengan tools online <http://www.imei.info>.

4.3. Investigation Digital Evidence

4.3.1. Proses Root

Melakukan *root* adalah sebuah proses untuk mengizinkan pengguna ponsel pintar, tablet, dan piranti lain yang berjalan pada sistem operasi Android untuk mendapatkan kontrol yang lebih tinggi (dikenal dengan "akses *root*") pada berbagai subsistem Android. Karena Android menggunakan kernel Linux, proses ini memberikan akses ke dalam hak administratif seperti pada Linux atau sistem operasi yang mirip dengan Linux, seperti FreeBSD atau OS X.

Root ini punya akses tanpa batas yang bisa mengubah, menghapus, menambah, bahkan merusak semua yang ada didalam sistem handphone kita. Nge-root artinya ngehack sistem handphone supaya pengguna hp punya akses ke account root tersebut. (Santoso, 2014)

Pada penelitian ini, proses *root* yang dilakukan pada smartphone Samsung E7 milik tersangka menggunakan software **Odin3-v3.10.6** yang compatible dengan smartphone tersangka seperti yang diGambarkan pada Gambar 4.6 dan 4.7



Gambar. 4.6. Persiapan proses root dengan Laptop atau PC.



Gambar. 4.7. Proses root dengan Odin V3.

4.3.2. Acquisisi

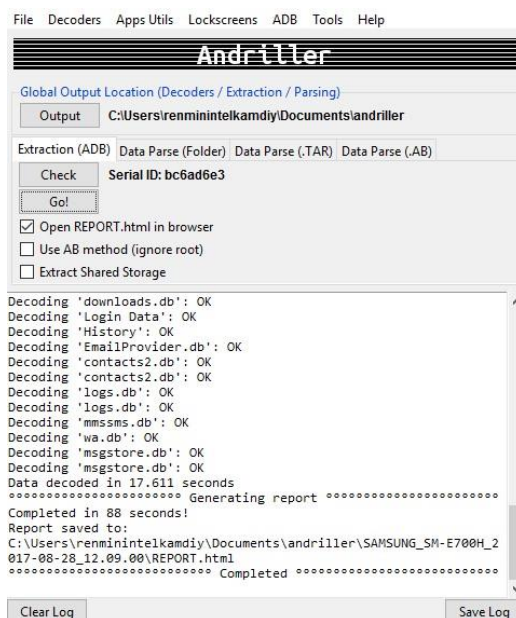
a) Andriller

Andriller adalah tools forensics untuk smartphone yang memiliki fitur sound forensics, database, pattern lock, Pin dan password. Berikut tampilan dari tools andriller dan proses aquisisi menggunakan andriller seperti Gambar 4.8.



Gambar. 4.8. Tampilan Tools Andriller V2.5.2.0.

Gambar diatas adalah tampilan utama dari tools Andriller saat dibuka pertama kali. Dan investigator perlu menghubungkan smartphone dengan PC/Laptop dengan kabel data. Hasil dari proses aquisisi dengan tools Andriller dapat dilihat pada Gambar 4.9.



Gambar.4.9. Proses aquisisi smartphone tersangka dengan menggunakan *tools Andriller*.

b) Oxygen Forensic

Oxygen Forensic merupakan software forensik untuk melakukan ekstraksi dan analisis data perangkat selular, smartphone, dan tablet. Oxygen Forensic menggunakan protokol proprietary yang memungkinkan mengekstrak data yang jauh lebih banyak, namun tetap dengan langkah-langkah standard forensic dan tidak merubah konten dari perangkat yang dianalisa. Software ini telah digunakan oleh instansi penegak hukum dan pemerintahan, swasta dan spesialis digital forensic lainnya. Berikut fitur yang dapat di ekstrak dengan oxygen forensic antara lain seperti terlihat pada Tabel 4.1.

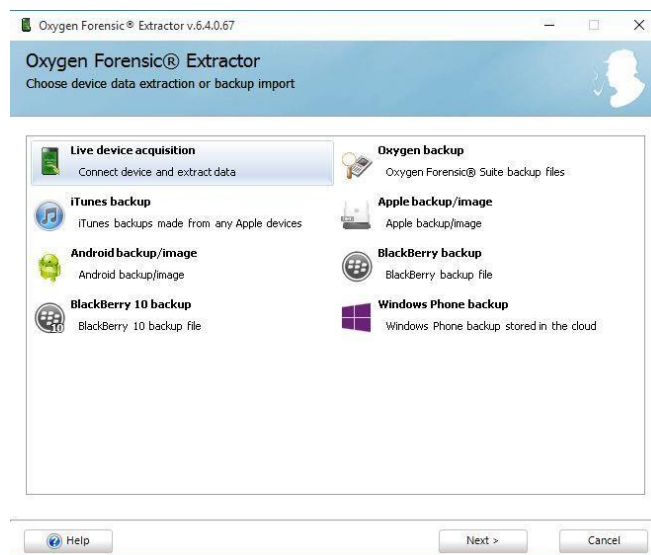
1. Informasi umum dari perangkat
2. Contact dengan informasi beserta foto
3. Call Register
4. Data Organizer seperti (meeting, appointmen, catatan dll)
5. SMS/MMS
6. Photo, video, audio file dan voice recorder
7. Peta ketika menggunakan camera
8. *Wifi connection* dengan passwordnya
9. *Device log*
10. File data yang tersimpan dalam perangkat
11. Dan fitur lainnya yang dimiliki oleh oxygen forensic adalah:

Tabel . 4.1. Fitur Oxygen Forensic

Capabilities	Oxygen Forensic® Extractor
Live device acquisition	Yes
Android devices rooting	Yes
Device backups import	Yes
Android and iOS images import	Yes
Saving data to OFB backup	Yes

Device data reports	Yes(PDF, RTF, XLS, HTML, XML, CSV, TSV, etc.)
Price (Final offer depends on the number of hardware pieces where Oxygen Forensic® Extractor will be activated)	Request Quote (20 activations)
	Request Quote (1 activation)

Tampilan tools Oxygen Forensics dapat dilihat pada Gambar 4.10

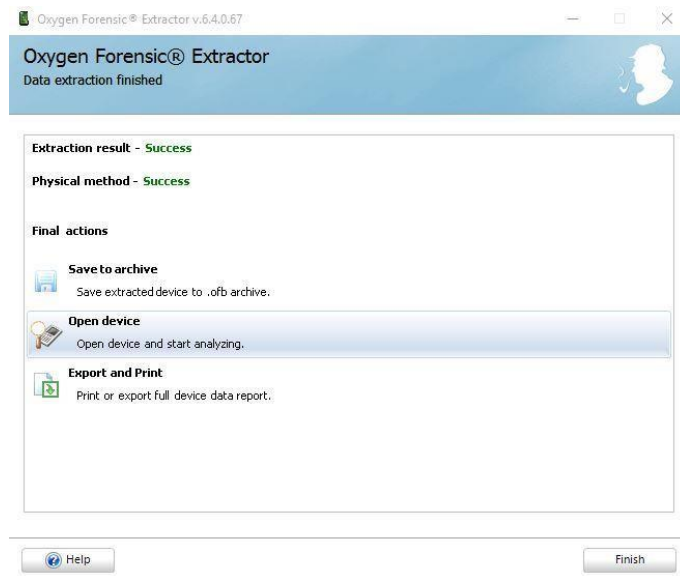


Gambar.4.10. Proses aquisisi smartphone tersangka dengan menggunakan *tools Oxygen Forensic*.

Tools Oxygen Forensics yang digunakan adalah versi 6.4.0.67. *Tools Oxygen* tersebut dapat melakukan *extractor android, blackberry, apple* dan *windows phone*. Dalam penelitian ini, *smartphone* yang digunakan tersangka berbasis android. Pada Gambar 4.11 dan 4.12 merupakan proses extrac dari smartphone tersangka oleh *Oxygen Forensics*.

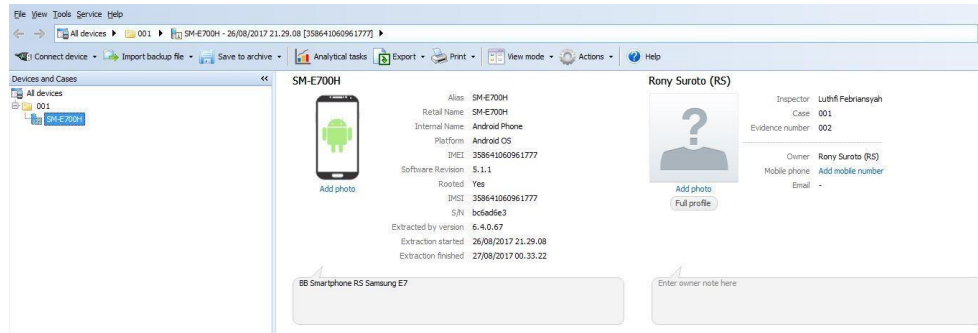


Gambar.4.11. Proses *physical dump* Oxygen Forensic smartphone tersangka.



Gambar.4.12. *Finishing Process physical dump* Oxygen Forensic smartphone tersangka.

Setelah proses aqisisi dengan tools Oxygen Forensics, maka hasil proses aqisisi tersebut dapat dilihat pada Gambar 4.13.



Gambar.4.13. Hasil proses aquisisi dengan *tools oxygen Forensics*.

4.4. Report of Investigation

Dari hasil aquisisi dengan *tools andriller* dan *Oxygen Forensic* maka ditemukan informasiinformasi dari *Whatsapp Messenger* adalah sebagai berikut:

4.4.1. Frekuensi Tertinggi

Frekuensi tertinggi dari kontak yang ada, seperti dalam Tabel 4.2.

Tabel 4.2. *Contact* Frekuensi Tertinggi Yang Menghubungi Tersangka

NO	KONTAK/NO. HP	FREKUENSI	KET
1	+6285601430XXX	21	ALT 1
2	+6285101410XXX	6	ALT 2
3	+6281229545XXX	9	ALT 3
4	+6282136767XXX	64	ALT 4
5	+62895344275XX	10	ALT 5

Berdasar Tabel 4.2 kontak yang melakukan percakapan terhadap tersangka dengan frekuensi tinggi yaitu alternatif 1 sampai dengan alternatif 5, yang merupakan hasil *extract* dari *smartphone* tersangka seperti Gambar 4.14.

key_id	status	needs_push	data
ACEE01B64E39D771F6B3036D00FB20	6	0	NULL
3746C147C24820E597FD3568F4CDFA	5	0	Assalamu'alaikum...ente jadi mau berangkat ngaji kagak...
14265C11462BA5838199CE81A08AAAC	5	0	Danang Hadi Wibowo Dtt Djogja: 'ngat...
AFT7DDAF1AC6C947124485C01FA6A7E	5	0	Ji...lo jgn lupa ya informasi ini jgn sampe bocor...
2057B2B3A6E9A52E6D702FE2C0288	5	0	Inget..., Polisi, aparat2 pemerintah, bs gagaln hajatan kita...
B47B3242A295090CFBF30582386C25	0	0	Insy Allah ane Dateng
3C888AD1868323A874104CA5878D36	0	0	Iya...insya Allah gw jaga baik2...
B1A8969650CC492EA49B5B217D7E25	0	0	Assalamu'alaikum bang...INI Ada yg mau nyumbang nih...
A1E85A26F653520C7816102E28C082	0	0	Fulus nya dikirim kemana..
EOC13D1108F084EFBE3F82B6C89FDE	5	0	NULL
332C05CAD109A9154FD850B7ABC76E	5	0	Ntar si donat kirim ke rekening itu aja...
260DB2109C4F95E01FF4934A478051	0	0	Ok bang
CC4DB2D749093AB58813039F0C196C	5	0	Ji lo monitor trus ya...ttg HTI yg dibubarin...dasar pemerintah skrg ni kurang ajar...jgn sampe ke
1AEFAC7C81990F27DFF3122B4472AA	5	0	Salam
41EE31D80F5AD286F7862CA29B59A6	5	0	👉 Ketika kita saolt...Allah tarik 3 perkara:
0A473A89FEABE2E3D9B320BA5C0888D	5	0	Danang Hadi Wibowo Dtt Djogja:RESOLUSI JOGJA
8049CC41977F940794E66508203C0	0	0	Ping
3EB0F9C8A4D985948BF8	13	0	NULL
3EB042879F0AEA70DCA	0	0	itu ane kirim daftar donatur utk kelompok kita...pass (akubisa)
FFBDDF98B291D04F3645F48BC2E8	5	0	Ok ji...ntar kalo ane nemu donatur...kirim ke rek itu ya...
3EB06B52A991DF6C623B	0	0	ok...salam👉

Gambar.4.14. capture percakapan tersangka dengan Whatsapp Messenger.

4.4.2. Dokumen atau Gambar yang mencurigakan

Dari hasil aquisisi, maka ditemukan dokumen-dokumen berupa Gambar maupun dokumen yang dapat dilihat pada Tabel 4.3.

Tabel 4.3. Contact Yang Pernah Mengirimkan Dokumen Atau Foto Kepada Tersangka

NO	CONTACT/NO. HP	DOKUMEN/ GAMBAR	KET
1	+6285601430XXX	0	
2	+6285101410XXX	0	
3	+6281229545XXX	2	Format XLS dan Jpeg
4	+6282136767XXX	0	
5	+62895344275XXX	0	

4.4.3. Keberadaan dalam database

Beberapa contact yang ditetapkan sebagai alternatif atau sasaran, tidak terdapat dalam database yang dimiliki kepolisian, seperti terlihat pada Tabel 4.4.

Tabel 4.4. Keberadaan Contact Yang Menghubungi Tersangka Dalam Database Simpatisan ISIS Dan Paham Radikal

NO	CONTACT/NO. HP	ADA ATAU TIDAK DALAM DATABASE	KET
1	+6285601430XXX	0	TIDAK ADA
2	+6285101410XXX	0	TIDAK ADA
3	+6281229545XXX	0	TIDAK ADA
4	+6282136767XXX	0	TIDAK ADA
5	+62895344275XXX	0	TIDAK ADA

4.4.4. Dokumen yang ditemukan

Berikut adalah dokumen atau Gambar yang didapatkan dari hasil aquisisi, seperti dalam Gambar 4.15 dan Gambar 4.16.

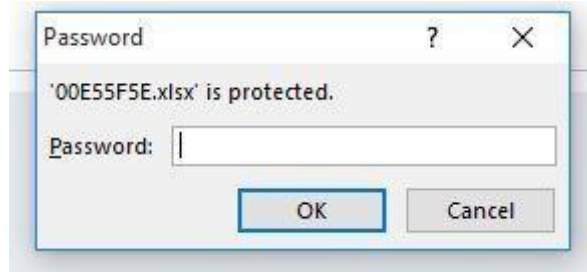


Gambar.4.15. *capture* buku tabungan dari rekan tersangka yang bernama Muh. Syukron.

00BA2061	26/08/2017 22.59	Microsoft Excel W...	51 KB
00BDB757	26/08/2017 23.42	Microsoft Excel W...	90 KB
00BE79DE	26/08/2017 23.42	Microsoft Excel W...	148 KB
00BF9B99	26/08/2017 23.42	Microsoft Excel W...	64 KB
00BFF392	26/08/2017 22.59	Microsoft Excel W...	90 KB
00C78969	26/08/2017 23.42	Microsoft Excel W...	36 KB
00D5CB37	26/08/2017 22.59	Microsoft Excel W...	11 KB
00D132A6	26/08/2017 23.41	Microsoft Excel W...	15 KB
00D7028F	26/08/2017 23.42	Microsoft Excel W...	19 KB
00DC5364	26/08/2017 23.42	Microsoft Excel W...	46 KB
00DE1E94	27/08/2017 00.05	Microsoft Excel W...	12 KB
00E1FCDD	27/08/2017 00.03	Microsoft Excel W...	11 KB
00E5D6FA	26/08/2017 23.42	Microsoft Excel W...	46 KB
00E55F5E	27/08/2017 00.04	Microsoft Excel W...	17 KB
00E58E32	27/08/2017 00.03	Microsoft Excel W...	9 KB
00E79F23	26/08/2017 23.42	Microsoft Excel W...	20 KB
00EC423D	26/08/2017 22.59	Microsoft Excel W...	64 KB
00EE1DBF	26/08/2017 23.42	Microsoft Excel W...	116 KB
00F66954	27/08/2017 00.19	Microsoft Excel W...	17 KB
00FFC088	26/08/2017 22.59	Microsoft Excel W...	90 KB
001AE630	27/08/2017 00.03	Microsoft Excel W...	11 KB

Gambar.4.16. *capture* dokumen-dokumen yang ditemukan pada smartphone tersangka.

Salah satu dokumen yang ditemukan dikunci dengan password dan hasil dari dokumen yang terkunci password seperti pada Gambar 4.17 dan 4.18.



Gambar.4.17. *capture* dokumen yang mencurigakan dan diproteksi.

DAFTAR DONATUR DANA UMAT							
NO	NAMA DONATUR	Alamat	TGL PENGIRIMAN	BANK PENGIRIM	BANK PENERIMA	JUMLAH TRANSFER (Rp)	KETERANGAN
1	H. Badrudin Iqbal	-	12 Januari 2010	Bank BCA	Bank Mandiri	2.000.000	1 BANK MANDIRI Cabang Brigjen Katamsa Yogyakarta 137-000-0622423
2	MT. Ukhuwah Islamiyah	Bogor Jawa Barat	15 Mei 2010	Bank Mandiri atas nama Budi	Bank Mandiri	5.000.000	2 BANK BCA Cabang Ahmad Dahlan Yogyakarta 024-7654789
3	MT. Muttaqien	Jaten Jawa Tengah	12 Mei 2012	Bank Mandiri a.n Arif Syaifulloh	BANK MANDIRI	3.500.000	

Gambar.4.18. *capture* dokumen berupa daftar donatur mengirimkan sejumlah dana.

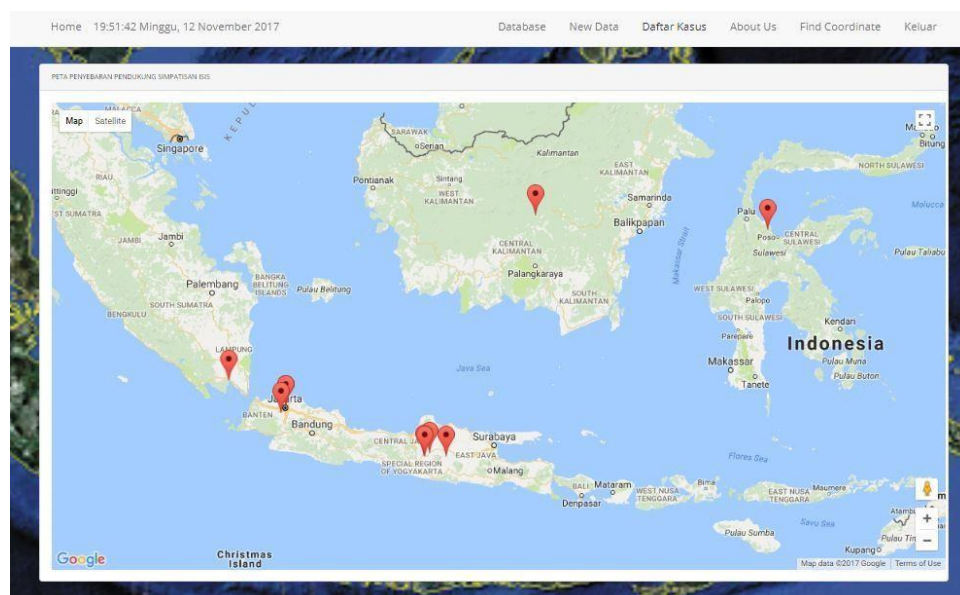
4.5. Analisis

Tujuan aplikasi ini adalah untuk memetakan individu atau kelompok yang memiliki paham radikal yang mengarah pada terorisme. Aplikasi ini berisi database individu maupun kelompok yang telah dideteksi oleh Polri sebagai simpatisan ISIS atau memiliki hubungan dengan seseorang yang telah menjadi Target Operasi kepolisian, berikut tampilan halaman

login dari aplikasi Pemetaan Jaringan Teroris dan sebaran lokasi dari para terduga alternatif contact di seluruh Indonesia, seperti dalam Gambar 4.19. dan Gambar 4.20.



Gambar.4.19. *capture* halaman login Aplikasi Pemetaan Jaringan Teroris



Gambar.4.20. *capture* halaman utama Aplikasi Pemetaan Jaringan Teroris

4.5.1. Proses Analisis

Dari data diatas, penulis menentukan kriteria-kriteria sebagai berikut:

- a. kriteria dokumen yaitu contact yang mengirimkan dokumen baik dalam bentuk doc, xls, pdf maupun jpeg;

- b. kriteria database yaitu contact tersebut belum ada dalam database simpatisan ISIS atau paham radikal baik kelompok maupun individu di Mabes Polri;
- c. kriteria frekuensi yaitu contact tersebut memiliki frekuensi tinggi berkomunikasi dengan tersangka RS.

Untuk meranking prioritas setiap kriteria dan alternatif berdasarkan matriks perbandingan berpasangan dapat dilakukan menggunakan konsep **Eigenvector** (Saaty, 1980).

Tabel 4.5. Konsep Eigenvector Tentang Perbandingan Dari Kriteria

<u>Intensity of Importance</u>	<u>Definition</u>
1	Equal Importance
3	Moderate Importance
5	Strong Importance
7	Very Strong Importance
9	Extreme Importance
2, 4, 6, 8	For compromises between the above
Reciprocals of above	In comparing elements i and j - if i is 3 compared to j - then j is 1/3 compared to i
Rationals	Force consistency Measured values available

Dari konsep **Eigenvector** tersebut, maka penulis memberikan perbandingan dari kriteria-kriteria yang sudah ditentukan berdasarkan wawancara dengan beberapa pejabat kepolisian seperti Kapusdik Intelkam, Kasubdit IV Ditintelkam Polda DIY dan Kasat Intelkam Polres gunungkidul, dan menghasilkan bahwa Dokumen paling penting, kemudian keberadaan dalam database kemudian Frekuensi percakapan, seperti Tabel 4.6 berikut :

Tabel 4.6. Pembobotan Kriteria

NO	KRITERIA	BOBOT	KEPENTINGAN
1	Dokumen	9	Mutlak Sangat Penting
2	Database	5	Sangat Penting
3	Frekuensi	3	Penting

Pembobotan Kriteria

$$(A)(W^T) = (n) (W^T)$$

(1)

Keterangan :

(A) : Matrik Perbandingan

(W) : Bobot Kriteria

(n) : Jumlah Kriteria

Dari hasil perhitungan pembobotan kriteria, maka dapat dilihat matrik pembobotan seperti Tabel 4.7.

Tabel 4.7. hasil perhitungan dari pembobotan kriteria

TABEL PEMBOBOTAN KRITERIA			
	FREKUENSI CHAT	DOKUMEN	DATABASE
FREKUENSI	3/3	3/9	3/5
DOKUMEN	9/3	9/9	9/5
DATABASE	5/3	5/9	5/5

	FREKUENSI CHAT	DOKUMEN	DATABASE
FREKUENSI	1	0,3333	0,6000
DOKUMEN	3	1	1,8000
DATABASE	1,6667	0,5556	1
	5,666666667	1,888888889	3,4

W	0,176470588	0,529411765	0,29411765
---	-------------	-------------	------------

Normalisasi

$$\sum_i a_{ij} = 1$$

(2)

Setelah dilakukan pembobotan kriteria, maka dilakukan normalisasi dari kriteria, hasilnya dapat dilihat pada Tabel 4.8.

Tabel 4.8. Tabel normalisasi pembobotan

Normalisasi						
	FREK CHAT	DOK	DATA BASE	Rata-rata	Rank Prioritas	
FREKUENSI	0,18	0,18	0,18	0,176470588	3	Frekuensi
DOKUMEN	0,53	0,53	0,53	0,529411765	1	Dokumen
DATABASE	0,29	0,29	0,29	0,294117647	2	Database

Uji Konsistensi

$$t = \frac{1}{n} \sum_{i=1}^n \left(\frac{\text{elemen ke - i pada } (A)(w^T)}{\text{elemen ke - i pada } w^T} \right) \quad (3)$$

Setelah mendapatkan prioritas dari kriteria yang sudah ditetapkan, maka perlu dilakukan uji konsistensi, dapat dilihat pada Tabel 4.9.

Tabel 4.9. Tabel uji konsistensi

Tabel Uji Konsistensi			
FREKUENSI	1	0,3333	0,6000
DOKUMEN	3	1	1,8000
DATABASE	1,6667	0,55556	1

$$CI = \frac{t - n}{n - 1} \quad (4)$$

Dari hasil perhitungan uji konsistensi, maka didapatkan hasil 0,0000 seperti Tabel 4.10.

Tabel 4.10. Tabel hasil uji konsistensi

Dan yang terakhir, alternatif-alternatif tersebut diperhitungkan pada kriteria dokumen, seperti Tabel 4.13.

Tabel 4.13. Perhitungan penentuan alternative berdasar dokumen

DOKUMEN							
	ALT 1	ALT 2	ALT 3	ALT 4	ALT 5	DOKUMEN	
ALT 1	0	0	0	0	0	ALT 1	0
ALT 2	0	0	0	0	0	ALT 2	0
ALT 3	0	0	1	0	0	ALT 3	2
ALT 4	0	0	0	0	0	ALT 4	0
ALT 5	0	0	0	0	0	ALT 5	0
	0	0	1	0	0		
W	0	0	1	0	0		

Dari hasil perhitungan alternatif dan kriteria diatas, maka dilakukan proses perangkingan seperti Tabel 4.14.

Tabel 4. 14. Penentuan rangking dari alternative yang ada

NO	ALTERNATIF	NILAI	RANGKING
1	ALT 1	0,03368984	3
2	ALT 2	0,009625668	5
3	ALT 3	0,543850267	1
4	ALT 4	0,102673797	2
5	ALT 5	0,016042781	4

Proses Perangkingan alternatif

$$\begin{pmatrix} 0,190909091 & 0 & 0 \\ 0,054545455 & 0 & 0 \\ 0,081818182 & 0 & 1 \\ 0,581818182 & 0 & 0 \\ 0,090909091 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0,176470588 \\ 0,294117647 \\ 0,529411765 \end{pmatrix} = \begin{pmatrix} 0,03368984 \\ 0,009625668 \\ 0,543850267 \\ 0,102673797 \\ 0,016042781 \end{pmatrix}$$

Dari hasil perangkingan diatas, maka didapatkan informasi bahwa ALT 3 mendapatkan prioritas 1 untuk dilakukan penyelidikan atau dimonitor lebih lanjut.

4.6. Report Inteligence Product

Tahap ini merupakan pembuatan sebuah produk intelijen yang mengGambarkan hasil analisis sampai dengan tingkat penentuan target-target baru. Dalam hal ini laporan yang dimaksud adalah Informasi Khusus yang ditujukan kepada Kapolda DIY sebagai *end user* untuk ditindak lanjuti kepada fungsi kepolisian lainnya atau lintas sektoral, seperti diGambarkan pada Gambar 4.21.

RAHA SIA

KEPOLISIAN NEGARA REPUBLIK INDONESIA
DAERAH ISTIMEWA YOGYAKARTA
DIREKTORAT INTELIJEN KEAMANAN
Nomor: R/Intelsub- /IX/2017

COPY ke:.....
Dari :.....Copies

INFORMASI KHUSUS
TANGGAL: September 2017

Dituang, Keselamatan

I. PERIHAL

Hasil Akuisisi Smartphone tersangka teroris RS (Rony Suroto)

II. FAKTA-FAKTA

1. Pada Selasa siang 16 Agustus 2017 di Dusun Jeruk, Desa Kepek, Kecamatan Wonosari Gunungkidul Yogyakarta telah diamankan terduga anggota teroris sdr Rony Suroto (RS) umur 33 tahun, agana Islam. Dari hasil pengeledahan di rumah RS, diamankan beberapa barang bukti yaitu berupa:

- 1 buah HP Smartphone Samsung Galaxy E7
- Uang sejumlah Rp. 240.000,-
- KTP terduga teroris berinisial RS dan domisili Tegal Jawa Tengah

Proses penangkapan tersebut dilakukan oleh Densus 88 Anti Teror Polri dibantu oleh Sat Reskrim Polres Gunungkidul dan beberapa anggota Satbrimobda DIY. Selain RS juga diamankan istri RS beserta 3 anaknya dan 1 anak dari kakak RS. Barang bukti yang diamankan saat pengeledahan disimpan di Reskrimum Polda DIY untuk penyelidikan lebih lanjut. Ditintekam Polda DIY menerima pakai barang bukti tersebut untuk mendapatkan target-target yang lain, dengan melayangkan nota dinas kepada Direktur Reskrimum Polda DIY dengan nomor: B/ ND- 1256/VIII/2017/Ditintekam tanggal 18 Agustus 2017 yang selanjutnya akan dilakukan investigasi oleh Sie Inteltek Ditintekam Polda DIY.

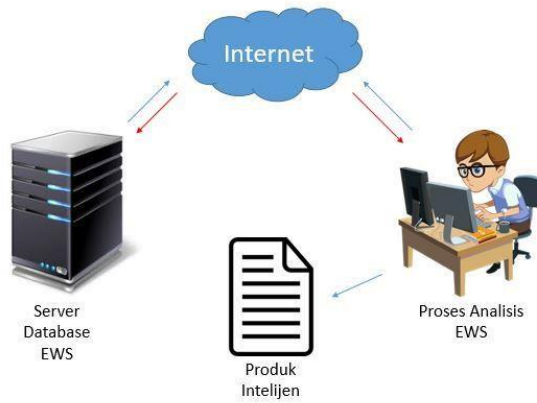
2. Pada tanggal 18 Agustus 2017 Ditintekam melayangkan nota dinas kepada Direktur Reskrimum untuk mengirim pakai bukti smartphone milik tersangka untuk dilakukan pengembangan kasus dengan mempelajari data-data yang terdapat dalam Smartphone tersangka RS.

Gambar.4.21. Produk Intelijen sebagai Hasil dari Analisis

4.7. Pengujian Aplikasi Pemetaan Jaringan Teroris

4.7.1. Skenario

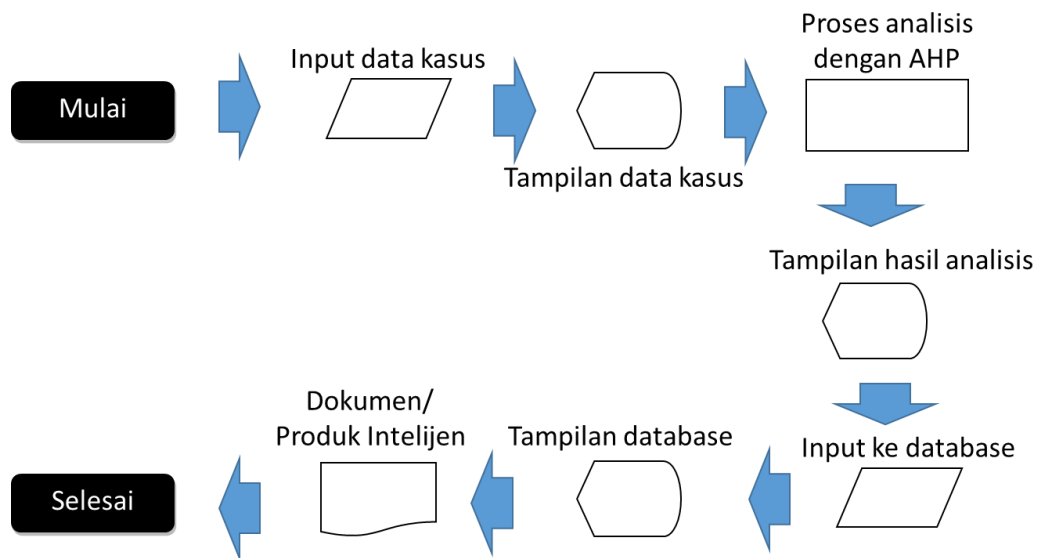
Aplikasi Pemetaan Jaringan Teroris merupakan aplikasi untuk membantu kepolisian dalam menjalankan tugasnya dalam menganalisis peranan seseorang/kelompok dalam jaringan terorisme atau paham radikal. aplikasi ini merupakan aplikasi berbasis web yang dapat diakses oleh anggota intelijen yang diijinkan untuk mengakses aplikasi tersebut, seperti Gambar 4.22.



Gambar.4.22. Skenario Sistem Pemetaan Jaringan Terorisme

4.7.2. Langkah-langkah

Aplikasi Pemetaan Jaringan Teroris ini dimulai dengan halaman login seperti Gambar 4.19 diatas, maka akan tampil halaman utama seperti Gambar 4.20 diatas. Untuk melakukan analisis maka dilakukan proses seperti Gambar 4.23.



Gambar 4.23 Proses Penggunaan Aplikasi

4.7.3. Hasil Pengujian Sistem

Setelah melalui tahap-tahap mulai dari case simulation sampai dengan menghasilkan produk intelijen, maka hasil pengujian sistem dapat digambarkan melalui Tabel 4.15.

Tabel 4.15 Pengujian Aplikasi Pemetaan Jaringan Teroris

NO	TAHAPAN	CHECK	KET
1	<i>Case Simulation</i>		☐☐ = success
2	<i>Digital Evidence</i>		
3	<i>Investigasi Digital Evidence</i>		
4	<i>Report Of Investigation</i>		
5	<i>Proses Analisis</i>		
6	<i>Found New TO</i>		
7	<i>Report/ Product Intelligence</i>		

Hasil pengujian sistem ini dilaksanakan di Ditintelkam Polda DIY khususnya di Subdit IV karena membidangi Keamanan Negara. Pengujian sistem dimulai dengan melakukan login dengan memasukkan username dan password. Pada halaman utama pengujian sistem melakukan input data kasus dari case simulation dan sampling kasus. Dari data kasus kemudian melakukan input data alternatif dan melakukan proses analisis. Proses analisis menghasilkan new target yang kemudian dimasukkan ke dalam database dan di cetak dalam bentuk produk intelijen (informasi khusus). Pengujian sistem tersebut dilaksanakan dengan beberapa pengujian seperti Tabel 4.16.

Tabel 4.16 Daftar Penguji Sistem 1 Ditintelkam Polda DIY

NO	NAMA	PANGKAT	JABATAN
1	Sigit Hariyadi, S.I.K.,M.H	AKBP	Kasubdit IV
2	Wiwik Hari T., SH	KOMPOL	Kanit B
3	Agung Dwi P	AKP	Panit B
4	Muhammad Arianto	BRIGADIR	Ba Ditintelkam
5	Vera Paulina	PENGATUR	Ba Ditintelkam

Pengujian ke 2 (dua) juga dilaksanakan di Subbagrenmin Direktorat Intelijen Keamanan Polda DIY. Pengujian sistem sama dengan yang dilakukan di Subdit IV yaitu dimulai dengan melakukan login dengan memasukkan username dan password. Pada halaman utama pengujian sistem melakukan input data kasus dari contoh kasus yang terjadi di wilayah hukum Polda DIY yaitu penangkapan terduga teroris di Jalan Kaliurang yang kemudian menangkap terduga berikutnya di Seturan Yogyakarta beberapa pengujian seperti Tabel 4.17.

Tabel 4.17 Daftar Penguji Sistem 2 Ditintelkam Polda DIY

NO	NAMA	PANGKAT	JABATAN
1	Iswahyuni	KOMPOL	Kasubbagrenmin
2	Erlita Meilianawati, s.ip	AKP	Kaurmin
3	Bangun Handoko	Brigadir	Bamin
4	Sudarji Fitriandaru	Brigadir	Bamin

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian Analisis Keterlibatan *Cyberterrorism* Menggunakan Metode *Analitycal Hierarchy Process* (AHP), maka dapat ditarik kesimpulan:

- a. *Mobile Forensics* dapat membantu memberikan informasi-informasi yaitu dengan menemukan beberapa alternatif-alternatif atau beberapa contact yang intens berkomunikasi dengan tersangka, dan berhasil menemukan sejumlah dokumen yang mencurigakan dan bermanfaat dalam tugas kepolisian, dengan aquisisi dari HP tersangka menggunakan tools Oxygen Forensic dan Andriller dan ditemukan beberapa alternatif-alternatif (contact) yang memenuhi kriteria yang sudah ditentukan.
- b. Metode AHP melakukan analisis dari dengan melakukan pembobotan kriteria dan melakukan uji konsistensi. Setelah dinilai cukup konsisten maka dilakukan penilaian alternatif dan kemudian dilakukan perangkingan yang menghasilkan bahwa alternatif ke 3 merupakan prioritas utama.

5.2 Saran

5.2.1. Pihak Akademisi

- a. saat ini kasus-kasus terorism sedang gencar-gencar nya ditangani oleh pihak kepolisian. Dalam penanganannya baik pra kejadian maupun pasca kejadian banyak menggunakan bantuan IT, maka dari itu peneliti menyarankan forensik digital dapat mengambil peran dalam penanganan terorism maupun cyberterrorism baik dalam pasca kejadian maupun dalam upaya pencegahan terorisme;
- b. Melakukan kerjasama yang baik antara akademisi dan pihak kepolisian dalam menyelaraskan dan mengembangkan bersama forensic digital agar sesuai antara teori dan pelaksanaan tugas dilapangan.

5.2.2. Peneliti selanjutnya:

Perlunya standar Investigasi Mobil Forensics yang dipadukan dengan System Pendukung Keputusan dalam melakukan monitoring atau pengembangan kasus-kasus terorism, sehingga penulis berikutnya dapat mengolah data dan mendapatkan informasi yang lebih baik dan lebih akurat lagi.

DAFTAR PUSTAKA

- Ankit Agarwal, M. G. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS)*.
- Asrizal, Z. R. (2015). <http://rubrikkomputer.blogspot.co.id/p/v-behaviorurldefaultvmlo.html>. Retrieved Januari 27, 2017, from <http://rubrikkomputer.blogspot.co.id/p/vbehaviorurldefaultvmlo.html>
- Colarik, A. (2006). *Cyberterrorism*. Idea Group Publishing.
- Fajar, S. (2014). <https://forensikadigitalstudy.wordpress.com/digital-forensic/mobile-forensic/>. Retrieved 2017, from <https://forensikadigitalstudy.wordpress.com/digitalforensic/mobile-forensic/>
- for-i.blogspot.co.id. (2016). <http://for-i.blogspot.co.id/2016/05/facebook-forensics.html>. Retrieved Januari 2017, from <http://for-i.blogspot.co.id/2016/05/facebook-forensics.html>
- Hanifa, T. (2013). <http://trihanifa.blogspot.co.id/2013/08/hebatnya-provokasi-media.html>. Retrieved 2017, from <http://trihanifa.blogspot.co.id/2013/08/hebatnya-provokasimedia.html>
- Indrajit, P. R. (2011). Forensik Komputer. *Forensik Komputer*, 3.
- IRIB Indonesia/VIVAnews/RA. (2014, Agustus 24). <http://indonesian.tribe.ir/editorial/cakrawala/item/83575-cara-isis-merekrut-anggota-danmenyebarkan-propaganda>. Retrieved from <http://indonesian.tribe.ir/editorial/cakrawala/item/83575-cara-isis-merekrut-anggota-danmenyebarkan-propaganda>: <http://indonesian.tribe.ir/editorial/cakrawala/item/83575-cara-isis-merekrut-anggota-danmenyebarkan-propaganda>
- Kapolri. (2010). *Peraturan Kapolri tentang Struktur Organisasi tingkat Polda*. Kepolisian Republik Indonesia.
- Kevin Curran, A. R. (2010). Mobile Phone Forensic Analysis. *Mobile Phone Forensic Analysis*.
- mahrus. (2014). <http://mahrusotomotif.blogdetik.com/2014/11/29/dampak-positif-negatif-darisosial-media/>. Retrieved from <http://mahrusotomotif.blogdetik.com>: <http://mahrusotomotif.blogdetik.com/2014/11/29/dampak-positif-negatif-darisosial-media/>
- NURUDIN. (2012). <http://nurudin-umm.blogspot.co.id/2012/11/media-sosial-sebagai-alatpropaganda.html>. Retrieved 2017, from <http://nurudinumm.blogspot.co.id/2012/11/media-sosial-sebagai-alat-propaganda.html>
- Raharjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sositologi*, 385.

- Rollins, C. A. (Catherine A. Theohary and John W. Rollins. 2015). *Cyberwarfare and Cyberterrorism: In Brief*.
- Waren, C. B. (2009). Safeguarding Australia from Cyber-terrorism:A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption. *Australian Information Warfare and Security Conference*.
- www.beritasatu.com. (2015). *Perangi Propaganda ISIS, Pemerintah Diminta Waspadai Gerakan "Anonymous" Lokal*. Retrieved from <http://www.beritasatu.com/digitallife/325035-perangi-propaganda-isis-pemerintah-diminta-waspadai-gerakan-anonymouslokal.html>:
<http://www.beritasatu.com/digital-life/325035-perangi-propaganda-isispemerintah-diminta-waspadai-gerakan-anonymous-lokal.html>
- Yunus Yussof, R. I. (2011). Common Phases of Computer Forensics Investigation Model. *IJCSIT*.

