

TESIS



**MEMBANGUN PROFIL RISIKO
PADA PEMBUATAN PETA DIGITAL
MENGUNAKAN *FRAMEWORK* NIST**

Koes Wiyatmoko

13917150

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

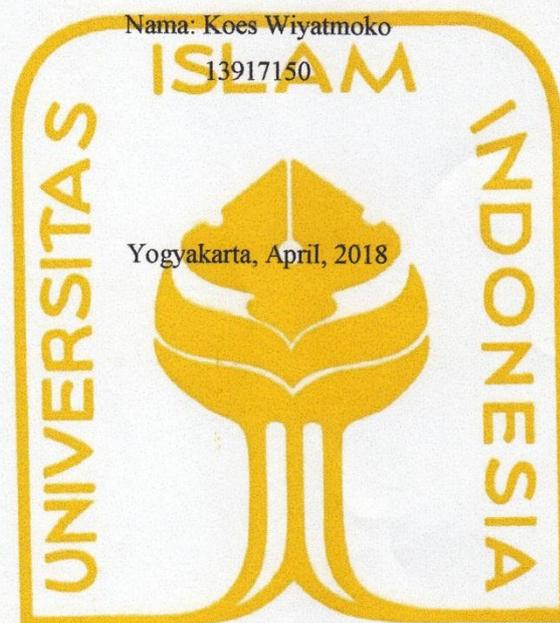
Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2018

Lembar Pengesahan Pembimbing

**MEMBANGUN PROFIL RESIKO
PADA PEMBUATAN PETA DIGITAL
MENGUNAKAN FRAMEWORK NIST**



Pembimbing I

Dr. Bambang Sugiantoro, M.T

Pembimbing II

Yudi Prayudi, S.Si, M.Kom.

Lembar Pengesahan Penguji

**MEMBANGUN PROFIL RESIKO
PADA PEMBUATAN PETA DIGITAL
MENGUNAKAN FRAMEWORK NIST**

Nama: Koes Wiyatmoko

13917150

Yogyakarta, April 2018

Tim Penguji,

Dr. Bambang Sugiantoro, M.T

Ketua

Yudi Paryudi, S.Si, M.Kom.

Anggota I

Dr. Imam Riadi, M.Kom

Anggota II



Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia



Dr. R. Teduh Dirgahayu, ST, M.Sc

Abstrak

Teknologi digital berkembang pesat, selain penyimpanan dan pendistribusian yang praktis data digital mudah di edit atau diperbarui, di gandakan dan di hapus, demikian juga dengan peta digital. Peta digital juga lebih mudah diperbarui untuk keperluan pemutakhiran data, penggandaan dengan kualitas yang tetap seperti asalnya. Namun kemudahan tersebut menimbulkan ancaman berupa manipulasi data hasil survey. Risikonya hasil dan kualitas peta digital yang tidak maksimal baik kwlaitas maupu data. Untuk menghindari ancaman risiko dan kerentanan terhadap kualitas hasil akhir peta digital maka seharusnya ada sebuah sistem yang mengatur atau memanajemen sistem pengolahan data digital.

Manajemen risiko adalah proses yang berkelanjutan untuk mengidentifikasi, menilai, dan menanggapi risiko. *Framework NIST (National Institute of Standard and Technology) Special Publication (SP) 800-30*, yang merupakan standar Panduan Manajemen Risiko untuk Sistem Teknologi Informasi. Metodologi ini terutama dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisa keamanan yang cukup. Hasil analisa evaluasi dan pengelolaan risiko dengan basis acuan *Framework NIST* yang disesuaikan dengan kebutuhan pencegahan, identifikasi, evaluasi dan pengelolaan sistem TI, menjadi profile untuk kasus penanganan pembuatan peta digital..

Dengan di terapkannya *Framework NIST* maka dapat disimpulkan juga bahwa step step yang sudah dibuat dapat dijadikan profile dalam rangka menilai kegiatan pembuatan peta digital, dimana ancaman risiko dan kerentanan mudah teridentifikasi karena sudah ada pola dari profile yang di bangun ini.

Keywords

gps, profil peta digital, akurasi *survey*, *way point fake location*, manajemen risiko, *NIST Framework*

Abstrak

Digital technology is growing very fast, in addition to the practical storage and distribution, it is really easy to be edited or updated, duplicated and deleted, as well as the digital maps. Digital maps are also easy to update for the purposes of updating data, copying with quality remains as the original. However, this convenience poses a threat such as data manipulation of survey results. This results in not optimal digital maps, both in terms of quality and data. To avoid the threat of risk and vulnerability to the quality of the digital maps, there should be a system that regulates or manages digital data processing systems.

Digital technology is growing very fast, in addition to the practical storage and distribution, it is really easy to be edited or updated, duplicated and deleted, as well as the digital maps. Digital maps are also easy to update for the purposes of updating data, copying with quality remains as the original. However, this convenience poses a threat such as data manipulation of survey results. This results in not optimal digital maps, both in terms of quality and data. To avoid the threat of risk and vulnerability to the quality of the digital maps, there should be a system that regulates or manages digital data processing systems.

Risk management is a process to identify, evaluate and respond to risks. NIST Framework (National Institute of Standard and Technology) Special Publication (SP) 800-30, is a standard Risk Management Guide for Information Technology Systems. This methodology is specifically designed to be a qualitative calculation and is based on sufficient security analysis. The results of the risk evaluation and management analysis based on NIST Framework that are adjusted to the need for prevention, identification, evaluation and IT systems management, become the profile to handle the digital map making .

The application of the NIST Framework leads to the conclusion that the steps that has been made can be used as a profile in order to evaluate digital map making activities, where the threat of risk and vulnerability is easily identified because there are already patterns from this profile.

Keywords

GPS, Digital Map Profile, survey accuracy, way point fake location, risk management, NIST Framework

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 ciptayang 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.



yakarta, April 2018


Koes Wiyatmoko

Halaman Persembahan

Tesis ini saya persembahkan persembahkan kepada semua pihak sebagai ucapan syukur dan terima kasih yang mana telah membantu dalam rangka proses penyelesaiannya, diantaranya:

1. Allah SAW yang telah memberikan rahmat dan karunianya sehingga kesehatan dan keselamatan selalu menyertai dalam kegiatan ini. Semoga hasil dari tulisan ini mendapat ridho dariNYA Amien.
2. Bapak Yudi Prayudi S.Si,M. Kom yang yang telah meluangkan waktu dan tenaga baik diwaktu jadwal bimbingan maupun diluar jadwal dan telah dengan tegas dan tanpa henti memberikan motivasi agar tetap semangat.
3. Bapak Dr. Bambang Sugiantoro, M.T yang telah meluangkan waktu dan tenaga untuk membimbing dan senantiasa memberikan motivasi, sehingga kami tetap semangat.
4. Bapak Dr. Imam Riadi, M.Kom yang tiada henti selalu memberi semangat kepada kami serta telah meluangkan waktu, tenaga dan pikiran untuk sempurnanya tesis ini.
5. Rekan rekan sesama mahasiswa yang dalam masa perjuangan maupun rekan rekan kerja yg selalu memerikan dorongan baik moril maupun materiil.
6. Semua pihak yang tidak dapat saya sebutkan disini.

Kata Pengantar

Alhamdulillah segala puji syukur penulis panjatkan kehadirat Allah Subhanahu Wa Ta'ala atas segala ridho dan karunia-Nya, sehingga tesis dengan judul “Membangun Profil Risiko Pada Pembuatan Peta Digital Menggunakan *Framwork NIST* ini dapat diselesaikan.

Tesis ini disusun untuk memenuhi syarat untuk memperoleh gelar Magister Komputer (M.Kom.) pada program studi Magister Teknik Informatika Universitas Islam Indonesia.

Dalam kesempatan ini juga penulis ucapkan terimakasih dan rasa hormat yang sebesar besarnya kepada :

1. Bapak Yudi Prayudi S.Si,M. Kom yang telah meluangkan waktu dan tenaga baik diwaktu jadwal bimbingan maupun diluar jadwal dan telah dengan tegas dan tanpa henti memberikan motivasi agar tetap semangat.
2. Bapak Dr. Bambang Sugiantoro, M.T yang telah meluangkan waktu dan tenaga untuk membimbing dan senantiasa memberikan motivasi, sehingga kami tetap semangat.
3. Bapak Dr. Imam Riadi, M.Kom yang tiada henti selalu memberi semangat kepada kami serta telah meluangkan waktu, tenaga dan pikiran untuk sempurnanya tesis ini.
4. Ketua Program Studi Pasca Sarjana Fakultas Teknik Industri bapak Dr. R. Teduh Dirgahayu ST, M.Sc beserta jajarannya.
5. Rekan rekan sesama mahasiswa yang dalam masa perjuangan maupun rekan rekan kerja yg selalu memerikan dorongan baik moril maupun materiil.
6. Semua pihak yang tidak dapat saya sebutkan disini.

Disadari bahwa hasil penulisan ini belum sempurna karena keterbatasan ilmu dan pengalaman, oleh karena itu saran dan kritik diharapkan untuk kesempurnaan tulisan ini.

Akir kata semoga tulisan inidapat bermanfaat bagi perkembangan dunia forensik

Yogyakarta, April 2018

Koes Wiyatmoko

Daftar Isi

Daftar Isi	viii
Daftar Tabel.....	x
Daftar Gambar	xi
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	6
1.3 Batasan Masalah	6
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	7
1.6 Metode Penelitian	8
1.7 Literature Review.....	8
1.8 Sistematika Penulisan	18
BAB 2 Tinjauan Pustaka	19
2.1 Tinjauan Pustaka.....	19
2.1.1 Manajemen Risiko.....	19
2.1.2 Bukti Digital	20
2.1.3 Peta Digital	20
2.1.4 Sistem Informasi Geografis.....	21
2.1.5 Model Data Geografis.....	22
2.1.6 Global Positioning System (GPS)	25
2.1.7 Waypoint	28
2.1.8 <i>National Institute of Standards and Technology (NIST)</i>	29
BAB 3 Metodologi Penelitian	33
3.1 Metode Penelitian	33
3.2 Studi Kepustakaan	33

3.3	Observasi.....	33
3.4	Tempat dan Waktu Penelitian.....	34
3.5	Bahan dan Alat Penelitian.....	34
3.6	Persiapan Tahap Penelitian.....	35
3.7	Pengumpulan Data.....	36
3.8	Akuisisi Data <i>Waypoint</i>	37
3.9	Penerapan <i>Framework NIST</i>	38
3.9.1	Penilaian Risiko (<i>Risk Assesment</i>).....	38
3.10	Simulasi Kasus.....	40
BAB 4 Implementasi Dan Analisa Data.....		42
4.1	Capture Data.....	42
4.2	Data.....	43
4.2.1	Simulasi Kasus.....	43
4.2.2	Sumber data.....	43
4.2.3	Cara Mendapatkan Data.....	43
4.2.4	Format Data.....	43
4.3	Penerapan NIST dalam Pembuatan Peta Digital.....	44
4.3.1	Proses Implementasi.....	44
4.3.2	Mengatasi Ancaman Risiko dan Kerentanan <i>Geodata</i>	53
4.4	Analisa Terhadap Hasil Uji Coba.....	60
BAB 5 Kesimpulan Dan Saran.....		62
5.1	Kesimpulan.....	62
5.2	Saran.....	62
Daftar Pustaka.....		63

Daftar Tabel

Tabel 3.1 Matrik Level Risiko.....	40
Tabel 3.2 Gambaran risiko dan tindakan yang di perlukan.....	40
Tabel 4.1 Ancaman pada yang muncul dari karakter sistem.....	45
Tabel 4.2 Dampak Risiko	49
Tabel 4.3 Besaran definisi dampak.....	49
Tabel 4.4 Rekomendasi Kontrol.....	50
Tabel 4.5 Laporan hasil identifikasi	59
Tabel 4.6 Hasil Identifikasi Perbandingan atribut Data survey <i>On Location</i> dan <i>Fake Location</i>	59

Daftar Gambar

Gambar 1.1 GPS Map 76 CSx Merek Garmin	2
Gambar 2.1 Tahapan Kerangka Kerja NIST	29
Gambar 2.2 Sembilan Langkah Utama Penilaian Risiko NIST	30
Gambar 2.3 Tahapan Mitigasi risiko	31
Gambar 3.1 Prangkat GPS Garmin GPSMAP 76 CSx.....	34
Gambar 3.2 Proses Survey Pengambilan Data Koordinat (<i>Tracks, Waypoint</i>)	36
Gambar 3.3 <i>Flowchart</i> Akuisisi Log File data survey dari GPS Map	37
Gambar 3.4 Proses Ekspor <i>Log File</i> Data Survey	37
Gambar 3.5 Alur Penangan <i>Vulnerability Identification</i> pada pembuatan Peta Digital.....	41
Gambar 4.1 Proses Pengunduhan Log File Dari GPS Maps	42
Gambar 4.2 Hasil Unduhan data GPS Map	42
Gambar 4.3 System Characterization step process.....	45
Gambar 4.4 Jenis dan Sumber Ancaman.....	46
Gambar 4.5 Identifikasi Kerentanan Proses	47
Gambar 4.6 Control Activity Pembuatan Peta Digital	48
Gambar 4.7 Penentuan Kemungkinan Risiko Pembuatan Peta Digital.....	49
Gambar 4.8 Profile Digital Map With <i>Framework</i> NIST	52
Gambar 4.9 Proses Implementasi <i>Vulnerability Identification</i>	53
Gambar 4.10 Data survey <i>waypoint</i>	53
Gambar 4.11 Data <i>Route waypoint</i> dan <i>Trackpoint</i>	54
Gambar 4.12 Identifikasi data yang berbeda pada log file <i>waypoint</i>	54
Gambar 4.13 <i>Waypoint</i> Hasil Akuisisi dari GPS Map	55
Gambar 4.14 Tracks Hasil Akuisisi data dari GPS Map	55
Gambar 4.15 Hasil Akusisi data <i>Survey</i> lokasi dari GPS.....	56
Gambar 4.16 Tampilan <i>Tracks Properties</i> dari data hasil kelokasi survey.....	56
Gambar 4.17 Tampilan hasil <i>Tracks</i> dan <i>Waypoint</i> yang tidak ke lokasi survey.....	57
Gambar 4.18 Tampilan <i>vertical Profile</i>	57
Gambar 4.19 Menampilkan Properties dari bagian <i>Tracks On Location</i>	58
Gambar 4.20 Menampilkan Properties dari bagian <i>Tracks Fake Location</i>	58

BAB 1

Pendahuluan

1.1 Latar Belakang

Perkembangan dan penerapan penggunaan data digital telah merambah di segala bidang. Model data diterapkan pada perangkat digital (komputer, handphone, tablet, PDA, networking devices, storage, dan sejenisnya)(Budi, 2016). Data digital merupakan salah satu obyek utama dalam forensik digital yang dapat dibagi menjadi forensik komputer (host, server), jaringan (network), aplikasi (termasuk database), dan perangkat (digital *devices*), dimana tiap bidang forensik memiliki pendalaman tersendiri. Pada forensik komputer, fokus penyidikan terkait dengan data yang berada atau terkait dengan perangkat itu sendiri. Layanan yang disediakan oleh perangkat biasanya tercatat dalam berbagai berkas log.

Keunggulan data digital adalah dapat digandakan yang bisa sama persis dengan aslinya, mudah di update atau di edit, di hapus, praktis. Keunggulan data digital tersebut sekaligus menjadi titik ancaman kerawanan bagi data digital itu sendiri karena jika tingkat manajemen dan pengamanan data tidak baik maka potensi manipulasi terhadap data tersebut juga semakin tinggi. Jadi dapat disimpulkan bahwa semua data yang di simpan dalam bentuk digital dapat dengan mudah di edit, dihapus dan digandakan untuk tujuan tertentu.

Perkembangan teknologi digital, juga telah membuat revolusi dalam dunia pemetaan khususnya dalam hal pencetakan peta. Pada era sebelum digital, peta dicetak berdasarkan teknik kartografi dimana koordinat sudah di dapat sebelumnya melalui survey pemetaan menggunakan alat seperti *theodolite*, *azimuth* dan lain sebagainya. Teknologi digital telah berkembang pesat dan saat ini cara pembuatan peta secara analog sudah bergeser ke teknologi digital, atau kita sebut peta digital. Telah dikemukakan pada paragraph sebelumnya tentang data digital, maka peta digital juga mempunyai keunggulan sekaligus menjadi titik kelemahan yang sama yaitu mudah di ubah, di hapus dan di gandakan.

Peta digital adalah representasi fenomena geografik yang disimpan dan dianalisis oleh komputer digital atau yang sekarang kita sebut sebagai sistem informasi geografis. Sistem Informasi Geografis adalah sistem informasi khusus yang mengelola data yang memiliki informasi spasial. SIG juga merupakan perangkat lunak yang dapat digunakan untuk pemasukan, penyimpanan, manipulasi, menampilkan dan keluaran informasi geografis berikut atributnya(Prahasta, 2009). Data SIG pada dasarnya adalah sebuah titik titik yang disebut *waypoint* dimana kumpulan titik titik yang di ambil pada saat survey dengan GPS akan membentuk polyline atau garis dan membentuk polygon area. Setiap titik atau *waypoint* akan di simpan didalam sebuah koordinat dan disimpan dalam perangkat GPS tersebut. Berikut foto GPS Map Garmin 76 CSx yang di pakai sebagai perangkat praktek penelitian dalam rangka pengambilan data ke lapangan (survey).



Gambar 1.1 GPS Map 76 CSx Merek Garmin

Dari *Mauul Book* yang disertakan dalam *Case Box*, GPS Map 76 CSx merupakan produk GPS Garmin dengan kemampuan menangkap sinyal lebih cepat dan menyediakan

Chanel Satellite sebanyak 12 stasiun sehingga presisi lebih bagus. Perangkat ini dikhususkan untuk *survey Mapping* kelokasi semua medan sehingga perangkat dilengkapi dengan fasilitas anti air dimana perangkat akan mengambang jika jatuh keair. Fasilitas lain yaitu bisa di isi dan *update* peta serta mempunyai slot memori external sehingga kemampuan untuk menyimpan peta digital dari hasil survey bias lebih banyak sehingga tidak perlu ganti ganti memori penyimpanan yang akan berpengaruh pada hasil survey untuk bahan peta digital.

Kelebihan peta digital dibandingkan dengan peta analog atau peta rupabumi terletak pada kualitas yang tetap dan bisa dikembalikan ke bentuk asalnya tanpa penurunan kualitas, sedangkan kertas mudah sobek, terlipat atau kerusakan dalam bentuk lainnya. Selain praktis dalam hal penyimpanan dan pendistribusiannya dibanding peta analog, peta digital juga lebih mudah diperbarui untuk keperluan pemutakhiran data atau perubahan sistem koordinat.

Namun disisi lain mudahnya pembaruan peta digital menimbulkan ancaman baru, karena sifat peta digital yang mudah dirubah tersebut maka ancaman terhadap perubahan atau manipulasi data hasil survey juga bias di ubah untuk tujuan tertentu misalnya, *karena* alasan menghemat biaya seorang surveyor tidak turun kelokasi survey untuk melakukan proses pengambilan data, pendataan dibuat di GPS atau di perangkat komputer. Bentuk manipulasi lain adalah dengan menempatkan data koordinat dengan cara perkiraan dengan melihat dan membandingkan lokasi pengenalan lain yang ada pada layar computer atau media lain. Banyaknya perangkat lunak yang dapat di unduh secara gratis menjadikan pelaku manipulasi data digital semakin mudah melakukan manipulasinya. Risiko terjadinya manipulasi merupakan ancaman terhadap hasil dan kualitas peta digital. Untuk menghindari ancaman risiko dan kerentanan terhadap kualitas hasil akhir peta digital maka seharusnya ada sebuah sistem yang mengatur atau memajemen sistem pengolahan data digital. Sistem ini perlu di bangun mengingat aktivitas ini melibatkan beberapa pihak seperti bagian peralatan (*logistic*), pelaku survey (*surveyor*), penerima dan pengolah data (*operator*) dan administrator sebagai pengolah akhir peta digital sekaligus *team leader*. Melihat hal tersebut maka diperlukan sebuah manajemen risiko untuk melindungi aset informasi dari risiko kejahatan manipulasi data digital atau diperlukan sebuah kerangka kerja untuk melindungi, mengelola dan mengantisipasi ancaman kejahatan digital (Stoneburner Gary, Goguen Alice, 2002).

Manajemen risiko adalah sebuah proses yang berkelanjutan untuk mengidentifikasi, menilai, dan menanggapi risiko. Untuk mengelola risiko, organisasi harus memahami kemungkinan bahwa suatu peristiwa akan terjadi dan menghasilkan dampak negatif. Dengan informasi ini, organisasi dapat menentukan tingkat risiko yang dapat diterima, sebagai toleransi risiko mereka (Purbo Onno W, 2017). Kerangka kerja ini memungkinkan organisasi perusahaan memberikan informasi dan memprioritaskan keputusan mengenai *cybersecurity* / *IT Security* atau keamanan informasi. Contoh dari proses manajemen risiko *cybersecurity* / *IT Security* termasuk *International Organization for Standardization (ISO) 31000: 2009*, *ISO / IEC 27005: 2011*, *National Institute of Standards and Technology (NIST) Special Publications (SP) 800-39* serta *NIST 800-30*, dan *Guidelines Electricity Subsector Cybersecurity Risk Management Process (RMP)*. Diantara beberapa *Framework* tersebut, *NIST SP800-30* merupakan *Framework* standart untuk mitigasi risiko yang dikembangkan oleh *National Institute of Standards and Technology (NIST)* yang mana merupakan tindak lanjut dari tanggung jawab hukum didalam undang undang *Computer Security Act* tahun 1987 dan *the Information Technology Management Reform Act* tahun 1996 (Stoneburner Gary , Goguen Alice, 2002).

Penelitian penerapan *Framework NIST SP 800 -30* yang dilakukan oleh (Ucu Nugraha, 2016) tentang penerapan manajemen risiko pada sistem informasi menyimpulkan bahwa *Framework NIST SP 800-30* membuktikan bahwa dengan melakukan analisa manajemen risiko menggunakan *Framework NIST SP 800-30* hasilnya dapat mengurangi risiko ancaman pencurian data dan informasi yang berpotensi disalah gunakan. Penelitian terkait berikutnya dilakukan oleh (Fabian Bustamante, Walter Fuertes, Paul Diaz, 2017), *famework* yang digunakan adalah kombinasi dari *PMI-PMBOK v5* dan *ITIL v3* serta *NIST 800-82* dan *800-30*. Kombinasi dari *Framework* tersebut hasilnya menunjukkan perbaikan telah berfungsi seperti yang diharapkan, terutama dalam konteks ketersediaan dan integritas informasi, yang menghasilkan nilai tambah bagi perusahaan.

Untuk mengelola ancaman risiko dan kerentanan sistem informasi atau *cybersecurity*, harus jelas tentang arah tujuan bisnis yang sedang dijalankan sehingga faktor keamanan menjadi pertimbangan dalam rangka menghadapi ancaman risiko dan kerentanan dan bagaimana mengelola sistem keamanan yang pada tujuannya untuk mengurangi risiko ancaman yang terjadi di perusahaan akibat adanya kerentanan sistem. Setiap organisasi perusahaan atau kantor yang menggunakan teknologi informasi

mempunyai karakter bisnis yang berbeda beda sehingga bentuk ancaman serta cara penangananyapun juga berbeda. *Framework* NIST menawarkan sebuah kerangka kerja manajemen tata kelola sistem informasi yang berupa langkah langkah yang harus diterapkan. Kerangka kerja yang dimaksud bukan untuk menggantikan sistem keamanan yang sudah ada namun justru akan mendukung sistem kerja untuk mengidentifikasi ancaman risiko akibat kerentanan sistem.

Framework NIST SP 800-30 akan memetakan aktifitas sebuah sistem mulai dari keberadaan *hardware*, *software*, *brainware* serta aturan atau kebijakan untuk mengontrol sistem yang berjalan sehingga akan ada gambaran kapan, bagaimana, dimana dan ancaman risiko seperti apa yang akan terjadi, kerangka kerja ini akan membantu memberikan gambaran terhadap ancaman seperti apa yang akan terjadi dengan memebrikan sebuah matrik nilai pembobotan terhadap suatu ancaman risiko.

Sebagai sebuah rangkaian aktivitas yang *output*-nya adalah peta digital maka aktivitas tersebut sudah selayaknya disebut juga sebuah sistem sistem pembuatan peta digital. Peta adalah sebuah gambaran representasi dari sebuah ide yang tertuang dalam gambar, sedangkan peta digital adalah gambaran representasi ide yang dituangkan dalam bentuk data digital (Prahasta, 2009). Dalam penerapan peta digital untuk bidang bidang tertentu istilah yang digunakan saat ini adalah Sistem Informasi Geografis. Seperti sistem informasi yang lain, maka sistem informasi geografis mempunyai ancaman risiko keamanan juga. Data digital dalam peta, atau geodata mempunyai karakter kusus dibanding data digital yang lain, baik dari cara memperoleh, mengolah dan mempresentasikannya. Sistem informasi geografis pada dasarnya terdiri dari tiga unsur pokok yaitu sistem, informasi dan geografis. Sistem informasi geografis merupakan satu kesatuan formal yang bersumber dari fisik dan logika yang berkenaan dari obyek obyek di muka bumi. SIG juga merupakan jenis perangkat lunak yang juga digunakan untuk pemasukan, penyimpanan , manipulasi menampilkan dan keluaran informasi berikut atribut atributnya (Prahasta, 2004).

Dengan adanya manajemen risiko yang menjadi standar penilaian kemanan data digital, diharapkan dapat membantu mencegah potensi manipulasi data digital seperti pada peta digital atau dapat teridentifikasi lebih dini. Tidak teridentifikasinya ancaman risiko kerentanan dalam rangkaian pembuatan peta digital berakibat pada tumpang tindihnya

posisi dan luasan peta digital atau tidak sinkronnya suatu obyek. Kondisi tersebut tersebut berpotensi menimbulkan konflik lahan, salah dalam pengambilan keputusan dan lain lain. Hal ini mengacu pada fakta kepastian hukum yang didasari pada ketepatan penentuan titik titik data koordinat dengan dirilisnya peraturan tentang standarisasi sistem koordinat yang telah dituangkan dalam Peraturan Pemerintah No. 24 tahun 1997. Perkembangan teknologi berupa penyediaan data, seperti ETS, GPS ataupun citra satelit, dan perangkat lunak pengelolaan data, akan dapat meningkatkan layanan kebutuhan informasi dalam akurasi dan presisi sesuai dengan harapan(Sendsow et al., 2012).

Dari uraian diatas dapat disimpulkan bahwa *Framework NIST SP 800-30* melalui langkah langkah yang digunakan sebagai acuan kerja sebuah sistem maka seharusnya langkah langkah kerangka kerja NIST 800-30 seharusnya dapat dijadikan sebagai sarana untuk mendeteksi adanya *fake data survey*. Untuk mendapatkan fakta fakta obyektif serta model deteksi yang tepat maka diperlukan profil sebagai acuan untuk mengetahui adanya *fake data survey* sehingga aktifitas manipulasi peta digital dapat terdeteksi lebih cepat. Profil dapat dicirikan sebagai penyelarasan standar, pedoman, dalam implementasi skenario tertentu. Profil digunakan untuk mengidentifikasi peluang untuk meningkatkan kekuatan untuk menghadapi ancaman risiko *cybersecurity* dengan membandingkan “*Current*” Profil (kondisi “apa adanya”) dengan “*Target*” Profil (kondisi “akhir”). Profil saat ini kemudian dapat digunakan untuk mendukung prioritas dan pengukuran kemajuan menuju Profil Sasaran, yang disinkronkan dengan kebutuhan bisnis lainnya termasuk efektivitas biaya dan inovasi. Profil dapat digunakan untuk melakukan penilaian diri dan berkomunikasi dalam sebuah organisasi atau antar organisasi(Purbo Onno W, 2017).

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka rumusan masalah yang dapat penulis sampaikan adalah sebagai berikut :

1. Bagaimana membangun profil ancaman risiko *Geodata* menggunakan *Framework nist* ?
2. Bagaimana detail identifikasi ancaman dan kerentanan pada *geodata* ?
3. Bagaimana mengatasi ancaman risiko dan kerentanan *geodata* ?.

1.3 Batasan Masalah

Agar penelitian ini lebih fokus dan terarah sesuai dengan latar belakang, maka batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Pembuatan profil ini hanya pada *Framework NIST SP 800-30*
2. Detail analisa data dengan tehnik digital forensik yang hanya mengacu *Vulnerability Identification* pada *Framework NIST*
3. Perangkat GPS yang digunakan untuk proses penitikan *waypoint* adalah produk dari GARMIN seri GPS Map 76 CSx
4. Lokasi penelitian dilakukan pada Konsultan CV. Rickomputer Kota Banjarbaru

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Membangun profile ancaman risiko *Geodata* menggunakan *Framework nist*.
2. Mendapatkan fakta fakta ancaman risiko akibat kerentanan sistem sehingga dapat melakukan antisipasi lebih dini.
3. Membangun profil pencetakan peta digital untuk acuan antisipasi tindakan pemalsuan data hasil survey

1.5 Manfaat Penelitian

Dari uraian yang telah dipaparkan pada latar belakang dan rumusan masalah, maka manfaat yang ingin di capai dalam penelitian ini adalah sebagai berikut :

1. Untuk Penulis
Proses penelitian ini diharapkan dapat meningkatkan kualitas akademis dan non akademis, serta wawasan baik secara teori dan praktek
2. Untuk Pengembangan Keilmuan dan Teknologi
 - a. Diharapkan profile ini dapat mengantisipasi ancaman risiko dalam pembuatan peta digital sehingga hasil pencetakan peta digital menjadi akurat dan obyektif.
 - b. Dengan adanya pola metadata log maka akan meminimalisir kesalahan penetapan lokasi yang disebabkan *fake location waypoint*.
 - c. Diharapkan profile ini menjadi sebuah sistem yang akan membantu penanganan antisipasi pemalsuan dalam pembuatan peta digital.

1.6 Metode Penelitian

1. Tahap Persiapan Penelitian

Tahap ini dibuat langkah langkah yang akan dilakukan pada proses penelitian *fake waypoint*

2. Akuisisi Data

Tahap melakukan akuisisi data dari GPS *Map* yang akan di analisa.

3. Analisa data

Tahap melakukan analisa data dari GPS yang telah di akuisisi.

4. Hasil Analisa dan Laporan

Tahap dimana menyimpulkan hasil analisa dan membuat kesimpulan dan laporan.

5. Kesimpulan

Tahap menyimpulkan hasil penelitian

1.7 Literature Review

Pada bagian ini akan di ulas tentang penelitian terkait yang telah dilakukan sebelumnya dengan topik GPS, *Framework* manajemen risiko.

Literature Review ini diawali dengan penelitian (Daryono, 2017). Penelitian ini merupakan pengembangan dari penelitian sebelumnya yang dilakukan oleh Yong-dal Shin,yaitu tentang *Framework* tahapan penanganan kasus cyber crime. Dalam penelitian Pengembangan *Framework* pelaporan Cybercrime metode yang digunakan adalah Metode Zachman *Framework* yang merupakan salah satu metode EAP, yaitu membuat *Framework* pelaporan cybercrime dengan membangun sistem informasi. Tujuan dari membangun membangun sistem informasi cybercrime report agar masarakat akan cepat dan mudah dalam melaporkan apabila menjadi korban cyber,begitu pula pihak kepolisian cepat merespon

(Fabian Bustamante, Walter Fuertes, Paul Diaz, 2017), yang membahas tentang peningkatan keamanan sistem informasi dan *system control industry*. Studi ini menjelaskan

tentang penyesuaian dan peningkatan metodologi untuk menyelaraskan proposal untuk pengelolaan keamanan informasi yang tepat untuk tujuan strategis. Penelitian ini terbagi dalam tiga tahap yang berbeda. Pertama, menginduksi artikulasi PMI-PMBOK v5 dan ITIL v3 baik untuk pengelolaan proyek dan mengurangi penyaluran dana ke dalam layanan PELUANG. Kedua, penerapan serangkaian strategi mitigasi risiko berdasarkan standar internasional sebagai NIST 800-82 dan 800-30. Ketiga, mengkombinasikan dua tahap yang disebutkan di dalam Panduan untuk instruksi dan kebijakan keamanan berbasis standar, yang sebelumnya telah didorong pada NIST 800-82, 800-53 dan 800-12. Hasilnya menunjukkan perbaikan telah berfungsi seperti yang diharapkan, terutama dalam konteks ketersediaan dan integritas informasi, yang menghasilkan nilai tambah bagi perusahaan.

Penelitian yang dilakukan oleh (Ucu Nugraha, 2016) Penelitian ini membahas tentang penerapan manajemen risiko pada sistem informasi dengan menggunakan *Framework SP 800-30*. Tujuan penelitian ini menganalisa tentang keamanan data dan informasi dalam menerapkan sistem informasi. Dengan melakukan analisa manajemen risiko maka diharapkan hasilnya dapat mengurangi risiko ancaman pencurian data dan informasi yang berpotensi disalah gunakan.

(Nurdiati Sri, Barus Baba, 2015) mengembangkan penelitiannya tentang Sistem Informasi Geografis Tindak Kejahatan Multilevel berbasis Web. Penelitian ini membahas tentang pemetaan wilayah kejahatan untuk tindakan antisipasi. Sistem ini memetakan tindak kejahatan dari aspek kapan terjadi ,dimana , motifnya apa , dalam rangka apa. Sistem juga dapat memberikan saran sebagai masukan kepada aparat penegak hukum dalam hal ini kepolisian dalam pengambilan keputusan. Pemetaan wilayah kejahatan ini juga menampilkan grafik yang dapat digunakan untuk menganalisa tingkat kerawanan wilayah dan segera mengambil keputusan berikutnya.

Penelitian (Widyantara, Agus, & Warmayana, 2015) kali ini membahas tentang Adapun fokus penelitiannya membahas tentang penerapan teknologi GPS, Seluler dan database Sistem Informasi Geografis. Topik bahasan pada paper ini adalah bagaimana mengidentifikasi trafik lalu lintas dengan menggunakan variabel data kecepatan, koordinat dan heading yang diperoleh dari perangkat GPS Tracker. Mekanisme yang digunakan adalah merealisasikan sebuah server GPS untuk mencapture data GPS secara real time. Dari server teknologi ini memberikan layanan *real time* tentang kondisi lalulintas seperti

kemacetan, kepadatan dan kelancaran lalulintas. Penelitian ini diharapkan dapat membantu menemukan solusi mengatasi kemacetan akibat kepadatan di jalan raya.

(Prayudi Yudi, 2014) pokok bahasan penelitian ini adalah tentang analisis bukti digital berupa database GPS di smartphone Android, dan teknik *acquisition, extraction, conversion* dan *presentation*. Adapun penekanannya pada prinsip kerja penggunaan tool untuk proses *acquisition* dan ekstraksi database GPS sehingga menemukan bukti digital yang dapat digunakan untuk bukti dipengadilan.

(Guntur Bagus Pamungkas, Bambang Sudarsono, 2014) dalam penelitiannya membuat analisis pembatasan daerah antara Kabupaten Sukoharjo dengan Kabupaten Karanganyar. Pokok permasalahan yang menjadi bahasan utama adalah bagaimana letak batas daerah tersebut sudah sesuai dengan SNI 19-6724-2002 atau Permendagri no.76/2012 dan bagaimana perbandingan antara pengukuran dengan ikatan orde-2 (pengukuran sebelumnya) dan pengukuran dengan orde-1 (pengukuran sekarang) ?. Penelitian ini juga menekankan bagaimana penentuan titik titik batas begitu penting dengan pengikatan ke orde-1 sebagai pengikatan kerangka pengukurannya, sementara hasil pengukuran sebelumnya dengan orde-2.

(Last David, 2014), meneliti tentang GPS Forensik dimana fokusnya pada perangkat GPS *Mobile Navigator Satellite* yang banyak digunakan saat ini. Beberapa kendaraan yang memiliki navigator tersebut diantaranya digunakan untuk tujuan criminal. GPS *Mobile Navigator Satellite* memiliki semua rekaman yang catatan dapat diinvestigasi dengan teknik teknik forensik yang baru dikembangkan yang menggunakan alat ini untuk menginvestigasi berbagai jenis kendaraan. Beberapa informasi di antaranya adalah tentang pergerakan kendaraan, kondisi real time terjadinya penyimpangan route .

(Mohamed Ghazouani, Sophia Faris, Hicham Medromi, n.d.) dalam penelitiannya membahas beberapa *Framework*. Dalam penelitiannya di sampaikan bahwa masing masing *Framework* dalam menilai ancaman risiko kerentanan mempunyai penafsiran standar pembobotan yang subyektif versi mereka sendiri. Tujuan penelitian ini ini adalah untuk mengusulkan adanya formulasi matematis untuk mengukur risiko dengan menggunakan tingkat yang lebih rendah granularitas unsur-unsurnya: ancaman, probabilitas, kriteria yang

digunakan untuk menentukan nilai aset, eksposur, frekuensi dan yang ada ukuran perlindungannya.

(Ibnu, 2013) melakukan penelitian tentang bagaimana merancang dan membangun teknologi untuk pelacakan lokasi menggunakan perangkat GPS. Pada penelitian ini alat pelacak hasil rancangannya di tempatkan di dalam HELM, dimana helm sebagai media pengganti kendaraan bermotor dengan cara menanamnya. GPS dapat dijadikan sebagai jawaban dari permasalahan bagaimana cara melacak lokasi tersebut.

(Kramer, 2013) peneliti dari Iowa State University pada tahun 2013 melakukan penelitian tentang Droid Spooter : A Forensic tool for Android Location Data Collection and Analysis. Penelitian ini menitik beratkan pada pembuatan alat yang dinamakan DROID SPOOTER, yang berfungsi untuk membantu penyidik dalam mengidentifikasi lokasi data penting yang tersimpan pada perangkat android dan alat ini memudahkan penyidik melakukan analisa forensik, serta kecepatan dalam menyelesaikan banyak kasus.

(J Kiyoshi, 2013) dan William Bradley Glisson University of South Alabama dan L. Milton Glisson Ret. N.C. A&T State University menyelidiki sejauh mana perangkat GPS digunakan dalam kasus perkara pidana dan perdata melalui pemeriksaan database hukum Lexis Nexis, Westlaw. Penelitian ini mengidentifikasi 83 kasus yang melibatkan bukti GPS dari dalam Inggris dan Eropa untuk periode waktu dari 1 Juni 1993 sampai 01 Juni 2013. Analisis empiris awal menunjukkan bahwa bukti GPS dalam kasus pengadilan meningkat dari waktu ke waktu dan mayoritas tentang kasus pidana.

(Lestari & Kristiyana, 2013) tentang rancang bangun suatu alat yang digunakan untuk melacak obyek bergerak. Alat tersebut berupa rangkaian module D-GPS508 yang dilengkapi dengan modul Development System untuk aplikasi GSM/GPRS/GPS yang telah dilengkapi dengan beberapa fitur tambahan seperti open collector output 3A, atmel microcontroller pada ISP Port, Onboard Power Regulator dan Extra I/O port. Rangkaian modul tersebut akan di kombinasikan dengan perangkat handphone. Tujuan dari penelitian ini adalah untuk melacak dan mendapatkan posisi obyek atau koordinat maka handphone akan digunakan untuk mengirim posisi koordinat obyek bergerak tersebut melalui fasilitas SMS

NO	Paper Utama	Uraian Singkat	Data	Perangkat	Framework
1	(Daryono, 2017)	<p>Penelitian ini pengembangan dari penelitian sebelumnya yang dilakukan oleh Yong-dal Shin,yaitu tentang <i>Framework</i> tahapan melakukan penanganan kasus cyber crime. Dalam penelitian Pengembangan <i>Framework</i> pelaporan Cybercrime menggunakan Metode Zachman <i>Framework</i> merupakan salah satu metode EAP. Penulis yaitu membuat <i>Framework</i> pelaporan cybercrime dengan menggunakan sistem informasi. Tujuanya adalah sistem informasi cybercrime report maka masyarakat akan cepat dan mudah dalam melaporkan apabila menjadi korban cyber,begitu pula pihak kepolisian cepat merespon</p>	-	-	<p><i>Framework</i> <i>Cybercrime</i>, Membangun <i>Framework</i> baru</p>
2	(Fabian Bustamante, Walter Fuertes, Paul Diaz, 2017)	<p>Penelitian ini membahas tentang penyelarasan keamanan informasi untuk tujuan strategis, caranya adalah dengan membahas tentang penyesuaian dan peningkatan metodologi tersebut dengan tujuan menyelaraskan proposal untuk pengelolaan keamanan informasi yang tepat dengan tujuan strategis.</p>	-	-	<p>NIST 800-30, 800-53, 800-82, PMI-PMBOK v5 dan ITIL v3, PMI-PMBOK v5</p>

NO	Paper Utama	Uraian Singkat	Data	Perangkat	Framework
3	(Ucu Nugraha, 2016)	Pembahasan penelitian ini adalah tentang penerapan manajemen risiko pada sistem informasi. Tujuannya untuk menganalisa tentang keamanan data dan informasi menggunakan <i>Framework SP 800-30</i> dalam menerapkan sistem informasi. Dengan melakukan analisa manajemen risiko ini maka diharapkan hasilnya dapat mengurangi risiko ancaman pencurian data dan informasi yang berpotensi disalah gunakan.	Database dan sistem	Komputer dan Jaringan	NIST sp 800-300
4	(Nurdiati Sri, Barus Baba, 2015)	Penelitiannya tentang Web GIS Tindak Kejahatan Multilevel , membahas tentang pemetaan wilayah kejahatan untuk tindakan antisipasi. Sistem ini memetakan tindak kejahatan dari aspek kapan terjadi ,dimana , motifnya apa , dalam rangka apa. Sistem juga dapat memberikan saran sebagai masukan kepada aparat penegak hukum dalam hal ini kepolisian dalam pengambilan keputusan. Pemetaan menampilkan grafik untuk analisa pengambilan keputusan.	Koordinat Longitude dan latitude, kelurahan, wilayah kejahatan, kantor polisi.	Komputer dan aplikasi pendukung web gis	-
5	(Widyantara et al., 2015)	Penelitian ini membahas tentang gabungan teknologi GPS, GIS, GPRS dan teknologi telekomunikasi yang di kontrol dengan sebuah server. Dari server teknologi ini memberikan layanan <i>real time</i> tentang kondisi lalulintas seperti kemacetan, kepadatan dan kelancaran lalulintas. Server posisi kendaraan sehingga pengaturan kondisi jalan raya. Penelitian ini diharapkan dapat membantu menemukan solusi mengatasi kemacetan dan kepadatan di jalan raya.	Log File GPS	GPS Tracker	-

NO	Paper Utama	Uraian Singkat	Data	Perangkat	Framework
6	(Yudi Paryudi – Sukriadi) (2014)	Forensik bukti digital GPS pada perangkat mobile Android Pokok bahasan penelitian ini adalah tentang analisis bukti digital berupa data database GPS di smartphone Android, dan teknik <i>acquisition, extraction, conversion</i> dan <i>presentation</i> . Adapun penekanannya pada prinsip kerja penggunaan tool untuk proses <i>acquisition</i> dan ekstraksi database GPS.	Log File Android	Handphone/ Smartphone Android	Maus, Stefan., Höfken, Hans., Schuba, Marko
7	(Guntur Bagus Pamungkas, Bambang Sudarsono, 2014)	Teknik Pengaturan dan validasi data survey, studi kasus pengukuran batas Kabupaten Sukoharjo dan Karang Anyar. Penelitian ini mengemukakan betapa pentingnya penentuan titik titik batas wilayah serta perlunya verifikasi ulang. Output dari penelitian ini adalah bagaimana membuat peta wilayah masing masing daerah dengan teknik pen	Log File hasil survey	GPS dan Komputer	SNI 19-6724-2002
8	(Last David, 2014)	Fokusnya penelitian pada perangkat GPS <i>Mobile Navigator Satelite</i> yang digunakan untuk tujuan criminal. GPS Mobile Navigator Satelite memiliki semua rekaman yang catatan dapat diinvestigasi dengan teknik teknik forensik yang baru dikembangkan yang menggunakan alat ini untuk menginvestigasi berbagai jenis kendaraan. Beberapa informasi di antaranya adalah tentang pergerakan kendaraan, kondisi real time terjadinya penyimpangan route	Koordinat	Perangkat Mobile dan Jamming	-

NO	Paper Utama	Uraian Singkat	Data	Perangkat	Framework
9	(Ibnu, 2013)	Merancang dan membangun teknologi untuk pelacakan lokasi menggunakan perangkat GPS. Pada penelitian ini alat pelacak hasil rancangannya di tempatkan di dalam HELM, dimana helm sebagai media pengganti kendaraan bermotor dengan cara menanamnya. GPS dapat dijadikan sebagai jawaban permasalahan cara melacak lokasi tersebut.	-	GPS	-
10	(Kramer, 2013)	Penelitian ini menitik beratkan pada pembuatan alat yang dinamakan DROID SPOOTER, yang berfungsi untuk membantu penyidik dalam mengidentifikasi lokasi data penting yang tersimpan pada perangkat android dan alat ini memudahkan penyidik melakukan analisa forensik, serta kecepatan dalam menyelesaikan banyak kasus.	Kasus Kejahatan	GPS, Droid Sooter	
11	(J Kiyoshi, 2013)	Penelitian ini tentang pemanfaatan n Global Positioning Systems (GPS) ke dalam aktivitas sehari-hari. Perangkat ini akan semakin memberikan kontribusi penting dalam kasus forensik digital. Studi ini menyelidiki sejauh mana perangkat GPS digunakan dalam mengungkap kasus perkara pidana dan perdata, melalui pemeriksaan database hukum Lexis Nexis, Westlaw, dan Inggris dan Irlandia. Penelitian tersebut mengidentifikasi 83 kasus yang melibatkan bukti GPS dari dalam Inggris dan Eropa untuk periode waktu dari 1 Juni 1993 sampai 01 Juni 2013. Analisis empiris awal menunjukkan bahwa bukti GPS diperlukan untuk mengungkap kasus	Data Tindak Kejahatan	GPS, Komputer	-

NO	Paper Utama	Uraian Singkat	Data	Perangkat	Framework
12	(Lestari & Kristiyana, 2013)	Perancangan dan Pembuatan alat Pelacak untuk Mendeteksi Obyek bergerak dengan mengkombinasikan GPS dengan SMS. Gambaran rangkaian module D-GPS508 yang dilengkapi dengan modul Development System untuk aplikasi GSM/GPRS/GPS yang telah dilengkapi dengan beberapa fitur tambahan seperti open collector output 3A, atmel microcontroller pada ISP Port, Onboard Power Regulator dan Extra I/O port. Rangkain modul tersebut akan di kombinasikan dengan perangkat handphone.	-	GPS, <i>Smarphone</i>	-
	Usulan Penelitian	Membangun profile ancaman risiko <i>Geodata</i> menggunakan <i>Framework nist</i> dan untuk mendapatkan fakta fakta ancaman risiko akibat kerentanan sistem sehingga dapat melakukan antisipasi lebih dini.	Fokus penelitian ini adalah bagaimana mengidentifikasi ancaman risiko keamanan informasi pada pembuatan peta digital dengan menggunakan <i>Framework NIST SP 800-</i>		

Judul	Uraian Singkat Masalah Penelitian	Solusi	Hasil Yang Diharapkan
Membangun Profil Risiko Pada Pembuatan Peta Digital Menggunakan <i>Framework Nist</i>	Penelitian ini membahas bagaimana menekan dan mendeteksi ancaman risiko dan kerentanan sistem yang berpengaruh terhadap hasil akurasi peta digital, dengan menganalisa proses dan data hasil suvey.	Membangun profil dan menerapkan kerangka kerja Manajemen Risiko Sistem Informasi untuk mendeteksi adanya ancaman risiko dan kerentanan sistem pedata digital.	Dengan diterapkannya <i>Framework</i> Manajemen Risiko Sistem Informasi maka diharapkan ancaman risiko dapat terdeteksi lebih cepat dan lebih awal sehingga menghasilkan integritas validitas dan akurasi peta digital lebih baik.

1.8 Sistematika Penulisan

Tahap ini memberikan gambaran secara umum terkait sistematika penulisan, dengan tujuan gambaran singkat tentang penulisan.

BAB I : PENDAHULUAN

Bab ini merupakan tahapan awal yang menguraikan tentang Latar Belakang Masalah yang mendasari perlunya diadakan penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan.

BAB II : KAJIAN PUSTAKA

Bab ini berisi tentang teori teori yang mendukung proses pemecahan masalah penelitian. Teori yang terkait antara lain tentang Sistem Informasi Geograifis , perangkat GPS, digital forensik dan metode klasifikasi.

BAB III: METODOLOGI

Bab ini berisi gambaran umum tentang proses penanganan data *waypoint*, mulai dari akuisi data, identifikasi *waypoint* sehingga menemukan pola data *waypoint*.

BAB IV : PEMBAHASAN

Bab ini menguraikan tentang pengolahan dan analisa data hasil *survey* dikaitkan dengan teori dan kerangka analisis yang telah disampaikan di BAB II, sehingga analisisnya akan memecahkan permasalahan dalam kerangka teoritik yang telah dikemukakan terdahulu.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisi dua hal pokok yaitu simpulan dan saran.

1. Simpulan, isinya bersifat konseptual dan terkait secara substantive dengan temuan penelitian yang mengacu pada tujuan yang telah ditetapkan sebelumnya.
2. Saran, yang berisi tentang harapan anjuran yang berkaitan dengan pemanfaat hasil penelitian dan kelanjutan penelitian

BAB 2

Tinjauan Pustaka

2.1 Tinjauan Pustaka

2.1.1 Manajemen Risiko

Manajemen Risiko adalah proses yang berkelanjutan untuk mengidentifikasi, menilai, dan menanggapi risiko. Untuk mengelola risiko, organisasi harus memahami kemungkinan bahwa suatu peristiwa akan terjadi dan dampak yang dihasilkan. Dengan informasi ini, organisasi dapat menentukan tingkat risiko yang dapat diterima untuk pengiriman layanan dan dapat mengekspresikan ini sebagai toleransi risiko mereka (Purbo Onno W, 2017).

Kemampuan memahami toleransi risiko, organisasi perusahaan dapat menempatkan skala prioritas kegiatan cybersecurity, dan membuat keputusan tentang pengeluaran cybersecurity. Implementasi program manajemen risiko menawarkan kepada organisasi perusahaan untuk mampu mengukur dan penyesuaian komunikasi untuk program cybersecurity yang dapat diterapkan pada asset data dan informasinya. Organisasi perusahaan dapat menentukan panangan risiko dengan cara yang berbeda, termasuk mengurangi risiko, mentransfer risiko, menghindari risiko, atau menerima risiko, tergantung pada dampak potensial terhadap pelayanan kritis.

Framework ini menggunakan proses manajemen risiko yang memungkinkan organisasi untuk menginformasikan dan memprioritaskan keputusan mengenai cybersecurity. *Framework* ini mendukung penilaian risiko berulang dan validasi pendorong bisnis untuk membantu organisasi pilih tahapan target untuk kegiatan cybersecurity yang mencerminkan hasil yang diinginkan. Dengan demikian, *Framework* memberikan organisasi kemampuan untuk secara dinamis memilih dan peningkatan langsung dalam manajemen risiko keamanan cyber untuk lingkungan IT dan ICS.

Framework menyediakan implementasi yang fleksibel dan berdasarkan risiko yang dapat digunakan dengan array yang luas dari proses manajemen risiko cybersecurity. Contoh dari proses manajemen risiko cybersecurity termasuk Organisasi Internasional untuk Standardisasi (ISO) 31000: 2009, ISO / IEC 27005: 2011, Institut Nasional Standar

dan Teknologi (NIST) Publikasi Khusus (SP) 800-39, dan Pedoman *Electricity Subsector Cybersecurity Risk Management Process* (RMP).

2.1.2 Bukti Digital

Undang – undang No.11 Tahun 2008 Pasal 5 Tentang Informasi dan Trasaksi Eletronik Ayat 1 berbunyi sebagai berikut, Informasi dan Eletronik dan/atau Dokumen eletronik dan/atau hasil cetakan merupakan alat bukti hukum yang sah. Dijelaskan di Ayat 2 Pasal 5 UUD No 11 Tahun 2008 Tentang ITE bahwa informasi eletronik dan/atau dokumen eletronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Pada Pasal 44 Huruf b UUD No.11 Tahun 2008 Tentang ITE bahwa informasi eletronik dan dokumen eletronik merupakan alat bukti lain, selain alat bukti yang sebagaimana dimaksud dalam ketentuan perundang – undangan. Log file yang berisi data koordinat dan atributnya pada GPS adalah bukti digital. Data koordinat tersebut adalah titik waypoint yang mewakili obyek tertentu atau jika sekumpulan *waypoint* mewakili area tertentu

2.1.3 Peta Digital

Peta digital adalah representasi fenomena geografik yang disimpan dan dianalisis oleh komputer digital (Nuryadin, 2005:19). Setiap titik akan di simpan didalam sebuah koordinat, kumpulan dari titik titik tersebut akan membentuk sebuah objek yang ada pada peta digital disimpan sebagai sekumpulan koordinat. Peta digital memiliki kelebihan jika dibandingkan dengan peta analog atau peta rupabumi yang dicetak di kertas atau media lain. Kelebihannya diantaranya adalah :

1. Peta digital mempunyai kualitas yang tetap dan bisa dikembalikan ke bentuk asalnya tanpa penurunan kualitas, sedangkan kertas mudah sobek, terlipat atau kerusakan bentuk lainnya.
2. Peta digital praktis dalam hal penyimpanan dan pendistribusiannya, sedangkan peta analog perlu ruang lebih besar
3. Peta digital lebih mudah diperbaharui. Penyuntingan untuk keperluan pemutakhiran data atau perubahan sistem koordinat misalnya, dapat lebih mudah dilakukan menggunakan perangkat lunak tertentu.

2.1.4 Sistem Informasi Geografis

Berdasarkan jenis data yang menjadi inputnya maupun unsur unsur pokok yang membentuknya, pengertian atau definisi SIG sebagai sebuah sistem sampai saat ini belum ada kesepakatan tentang definisi yang baku. Sebagaimana besar definisi dari berbagai pustaka masih bersifat umum belum lengkap, tidak presisi dan bersifat elastik. Beberapa negara menggunakan istilah berbeda dalam merujuk terminologi SIG. Berikut terminologi yang merujuk pada istilah SIG(Prahasta, 2009) :

Tabel 2. 1 : Definisi Sistem Informasi Geografis (SIG)

No	Definisi	Nama
1	Sistem komputer yang digunakan untuk memasukan (<i>captureing</i>), menyimpan, memeriksa, mengintegrasikan, memanipulasi, menganalisis dan menampilkan data data yang berhubungan dengan posisi posisinya di permukaan bumi	Rice
2	Kombinasi perangkat keras dan lunak sistem komputer yang memungkinkan penggunaanya untuk mengelola, menganalisa dan memetakan informasi spasial berikut data atributnya (data deskriptif) dengan akurasi kartografi.	Basic
3	Sistem yang berbasis komputer (CBIS) yang digunakan untuk menyimpan dan memanipulasi informasi-informasi geografis. SIG dirancang untuk mengumpulkan, menyimpan dan menganalisis objek-objek dan fenomena di mana lokasi geografis merupakan karakteristik yang penting atau kritis untuk dianalisis. Dengan demikian, SIG merupakan sistem komputer yang memiliki empat kemampuan berikut dalam menangani data yang bereferensi geografis: (a) masukan, (b) manajemen data (penyimpanan dan pemanggilan data), (c) analisis dan manipulasi data, dan (d) keluaran.	Aronoff

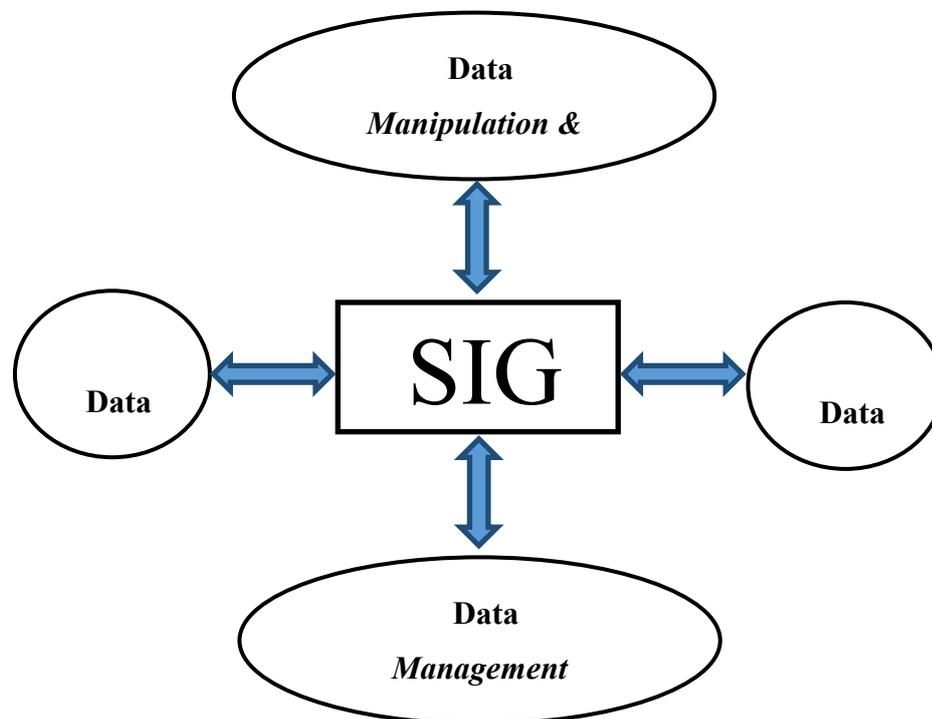
SIG dapat kita kelompokkan menjadi beberapa subsistem seperti berikut ini :

1. **Data Input** : adalah sebuah proses untuk mengumpulkan, mempersiapkan, dan menyimpan data spasial dan atributnya dari berbagai sumber kemudian mengkonversikan atau mentransformasikan format format data aslinya kedalam format (*native*) yang dapat digunakan oleh perangkat SIG (. Proses *digitizer/digitasi*)
2. **Data Output** : adalah proses untuk menampilkan atau menghasilkan keluaran (termasuk mengeksponnya ke format lain) baik sebagian atau seluruh basis data

(spasial), dimana keluarannya berbentuk *softcopy* dan *hardcopy* diantaranya ttabel, grafik, report, peta.

- 3. Data Management:** tahap ini berhubungan dengan proses pengolahan, penyimpanan dan analisis data serta disimpan ke dalam sebuah sistem basis data dalam format tertentu sehingga mudah di *retrieve* (di load ke dalam memori) untuk dapat di *update*, dan di *edit*.
- 4. Data Manipulation dan Analysis:** tahap ini menentukan informasi-informasi yang dapat di hasilkan oleh SIG. selain itu, subsistem ini juga melakukan manipulasi (evaluasi dan penggunaan fungsi-fungsi dan operator matematis dan logika) dan pemodelan data untuk menghasilkan informasi yang di harapkan.

Berikut ilustrasi sub sistem SIG.



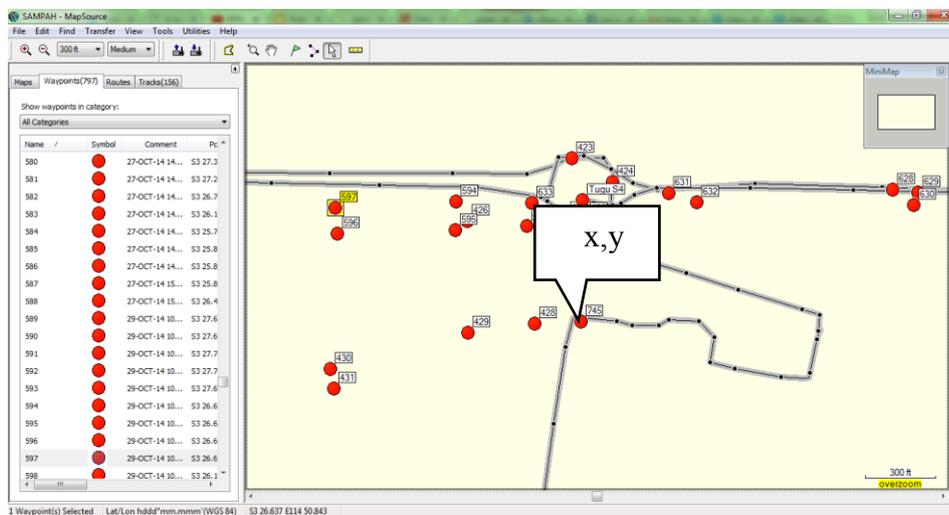
Gambar 2. 1 : Ilustrasi Sub-Sistem SIG

2.1.5 Model Data Geografis

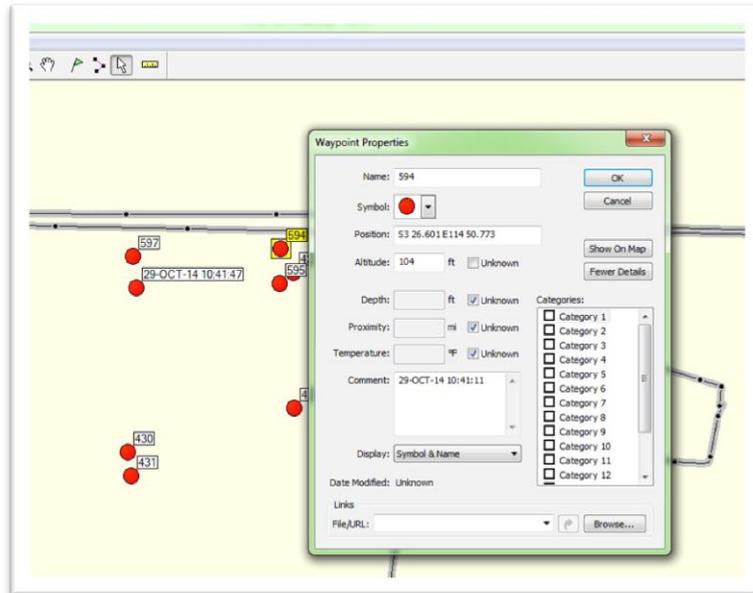
Data geografis adalah data yang merepresentasikan obyek nyata di bumi kedalam peta dalam bentuk simbol simbol yang mengandung informasi setiap obyeknya. Ada dua jenis data geografis yaitu data tabular yang berisi informasi tentang obyek bumi, dan data spasial

yang mewakili obyek bumi. Berikut penjelasan model data geografis (Riyanto, Prilnali EP, 2009):

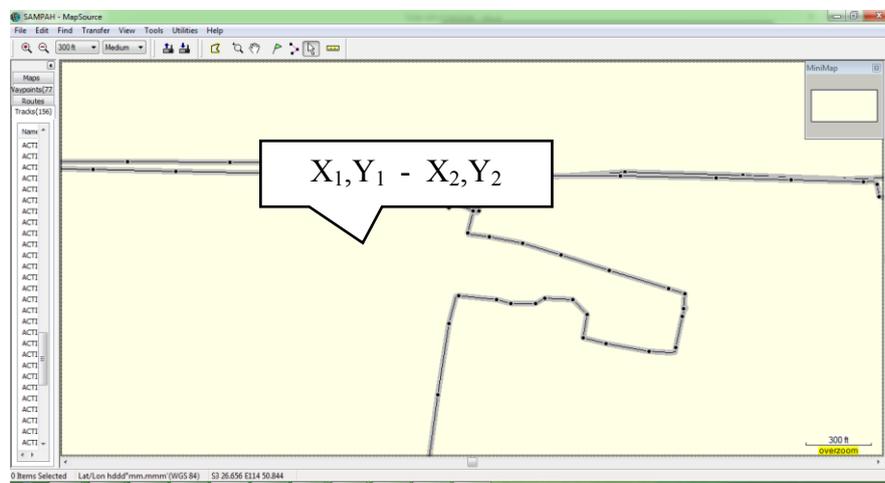
1. Data spasial : model ini di kelompokkan menjadi **Model Data Vektor** dan **Model Data Raster**. Model data vektor diwakili oleh simbol simbol atau dalam SIG dikenal dengan *feature*, fitur fitur tersebut adalah (1) *feature point* (titik) yang mempunyai sepasang koordinat X,Y tidak berdimensi (tidak punya luasan), (2) *feature line* (garis) yang mempunyai pasangan pasangan koordinat, titik awal titik akhir (X_1, Y_1, X_2, Y_2) berdimensi 1, (3) *feature polygon* (area) yang mempunyai koodinat berpasangan pasangan dimana titik awal sama dengan titik akhir ($X_1, Y_1 = X_2, Y_2$) mempunyai dimensi 2 dengan ukuran dimensi panjang dan luas , (4) *feature surface* (permukaan) merupakan suatu area dengan besaran (X,Y,Z) dan disebut berdimensi 3 dengan ukuran panjang, luas dan ketinggian.



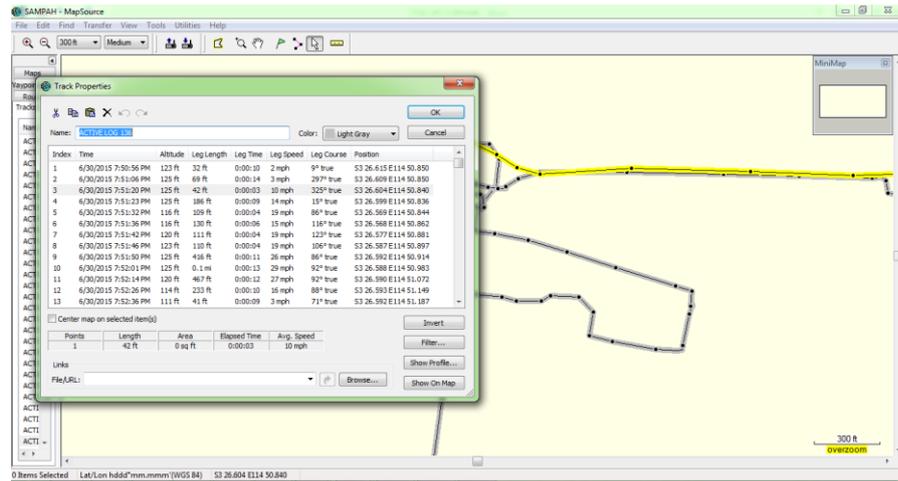
Gambar 2. 2 : Model Data Feature Point



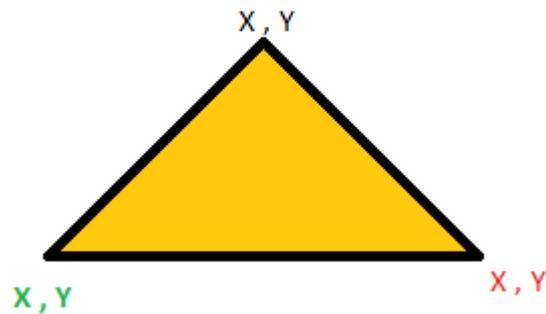
Gambar 2. 3 Model Data Log Waypoint



Gambar 2. 4 Model data Feature Line (Garis)



Gambar 2. 5 : Meta data Log Feature Line



Gambar 2. 6 : Model Data feature polygon

Sedangkan Data Raster adalah merupakan model data yang disimpan dalam petak petak bujur sangkar (*grid*) yang membentuk sebuah bidang. Petak petak ini disebut dengan Pixel. Posisi piksel dinyatakan dalam kolom ke m dan kolom ke n. Beberapa data ini disebut juga data citra.

2. Data Tabular adalah data yang menyimpan nilai atribut dari kenampakan kenampakan permukaan bumi tersebut, misal lahan mempunyai atribut luas ketinggian panjang, lebar. Model data tabular tersimpan ke dalam bentuk *row* dan *field*.

2.1.6 Global Positioning System (GPS)

GPS (Global Positioning System) adalah sebuah sistem satelit navigasi dan penentuan posisi. Sistem ini di kelola oleh Amerika Serikat dimana didesain untuk memberikan posisi dan kecepatan tiga-dimensi serta informasi mengenai waktu secara kontinyu tanpa

tergantung cuaca dan waktu dan berlaku di seluruh dunia. Sebagian besar orang menggunakan GPS untuk mendapatkan informasi tentang posisi, kecepatan, percepatan ataupun waktu yang teliti. GPS dapat memberikan informasi posisi dengan ketelitian bervariasi dari beberapa millimeter (orde nol) sampai dengan puluhan meter (Rini Fathoni Lestari, 2014).

Ada tiga macam type alat GPS

1. Tipe alat GPS Navigasi (Handheld, Handy GPS)



Gambar 2. 7 GPS Type Handy

2. Tipe alat geodetik single frekuensi (tipe pemetaan), digunakan survey dan pemetaan yang membutuhkan ketelitian posisi centimeter hingga beberapa desimeter.



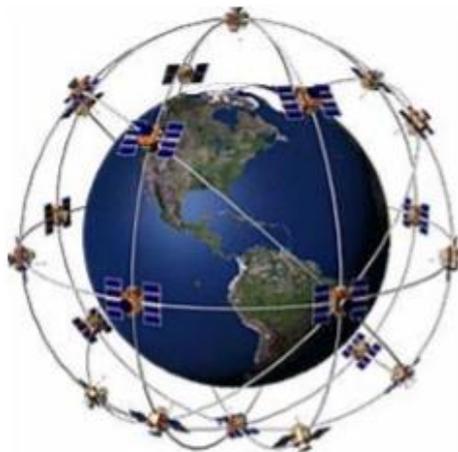
Gambar 2. 8 GPS Type Geodetic Single Frekuensi (Rini Fathoni Lestari, 2014)

3. Tipe terakhir adalah tipe *Geodetik dual frekuensi* yang dapat memberikan ketelitian posisi hingga mencapai milimeter. Tipe ini biasa digunakan untuk aplikasi precise positioning seperti pembangunan jaring titik kontrol, survey deformasi, dan geodinamika.



Gambar 2. 9 GPS Type *Geodetik dual frekuensi* (Rini Fathoni Lestari, 2014)

Sebagai perangkat untuk menentukan posisi GPS (*Global Positioning System*) ada 4 faktor yang mendasar : latitude, longitude, altitude and time.. Variabel turunannya adalah (1) Kecepatan, (2) Percepatan (Akselerasi), (3) Arah laju, dan (4) Ukuran Interval (Jarak, Selang Waktu). Sedangkan arsitektur GPS terdiri dari 3 segmen yaitu *space segmen*, *user segmen* dan *control segment*.



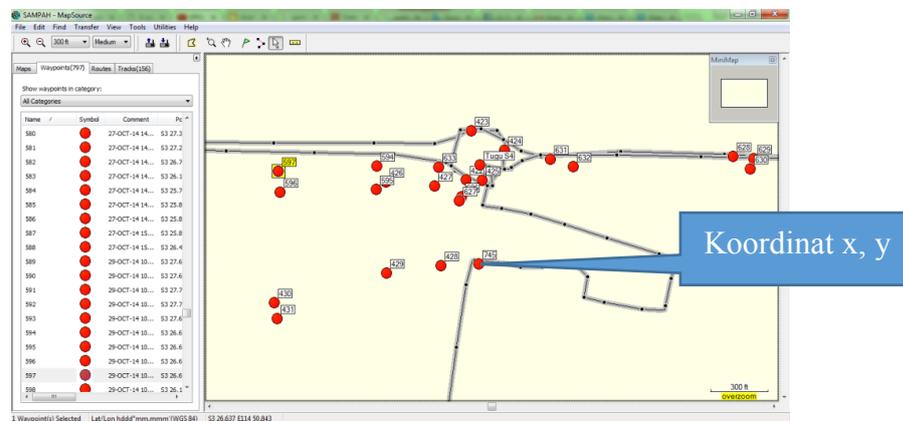
Gambar 2. 10. Space Segmen Pada GPS (Rini Fathoni Lestari, 2014)

Space segment adalah stasiun bumi yang mengontrol GPS dimana GPS bekerja menggunakan bantuan sinyal 27 satelit yang mengorbit mengelilingi bumi. Posisi dari satelit ini tidak akan berubah (latitude, longitude dan altitude-nya tidak akan berubah), karena itu satelit bisa menghitung posisi relative sesuatu benda di Bumi. 3 satelit dapat digunakan untuk menghitung posisi dalam ruang 3D. Tingkat Akurasi dari GPS terdiri dari akurasi jarak dan akurasi waktu. (Rini Fathoni Lestari, 2014).

Update segment adalah sinkronisasi jam atomic antara satellite satu dengan yang lainnya sedangkan *User segment* adalah GPS receiver atau GPS yang digunakan untuk survey oleh user dan dapat di koneksikan keperangkat lain untuk diambil data hasil survey diantaranya *data waypoint*.

2.1.7 Waypoint

Waypoint adalah koordinat yang mewakili sebuah titik di dalam peta yang dihasilkan oleh perangkat *GPS Mapping*. Titik tersebut merupakan koordinat yang biasanya menyertakan longitude, latitude, dan kadang altitude untuk keperluan tertentu. Waypoint juga digunakan sebagai penanda lokasi tertentu yang memiliki tujuan tertentu. Format waypoints lintang dan bujur. GPS waypoint biasanya diberikan dalam derajat dan fraksi derajat, atau derajat, menit dan fraksi menit (GPS Waypoint Koordinat). Waypoint mengandung informasi lintang dan bujur, hanya dengan akurasi lebih dari format derajat / menit standar / detik. "Landmark" GPS Waypoints



Gambar 2. 11 Waypoint yang di tampilkan di Map Source

2.1.8 National Institute of Standards and Technology (NIST)

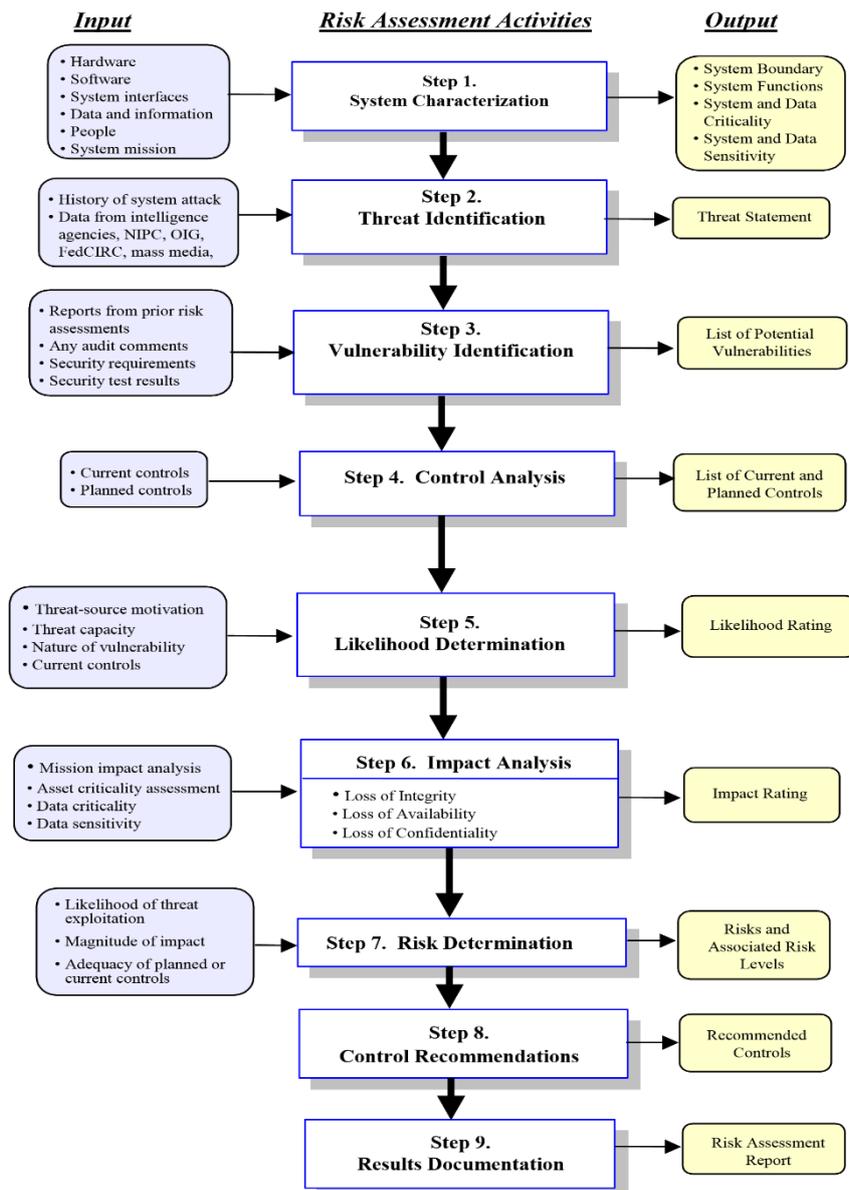
NIST (*National Institute of Standard and Technology*) adalah merupakan panduan standar Pemerintah Federal US dalam melakukan penilaian Manajemen Risiko untuk Sistem Teknologi Informasi. Metodologi ini dirancang untuk menilai perhitungan kualitatif yang didasarkan pada analisa keamanan yang sesuai publik inginkan, sehingga secara teknis pada bagian sistem ini petugas teknis benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko pada sistem TI. Proses ini meliputi segala sesuatu dari ancaman-sumber identifikasi untuk evaluasi berkelanjutan dan penilaian, yang sangat komprehensif. NIST mengeluarkan rekomendasi melalui publikasi khusus *Framework NIST SP 800-30 tentang Risk Management Guide For Information Technology System* (Ucu Nugraha, 2016). Terdapat 3 tahapan yaitu : penilaian risiko (***risk assessment***), peringanan risiko (***risk mitigation***), dan evaluasi risiko (***risk evaluation***).



Gambar 2.1 Tahapan Kerangka Kerja NIST (Ucu Nugraha, 2016)

1. Penilaian Risiko (*Risk Assesment*) mempunyai cakupan sembilan langkah utama, yaitu:
 - Langkah 1 - Karakterisasi Sistem
 - Langkah 2 - Identifikasi Ancaman
 - Langkah 3 - Identifikasi Kerentanan
 - Langkah 4 - Analisis Kontrol
 - Langkah 5 - Penentuan Kemungkinan
 - Langkah 6 - Impact Analysis
 - Langkah 7 - Penentuan Risiko
 - Langkah 8 - Rekomendasi Kontrol

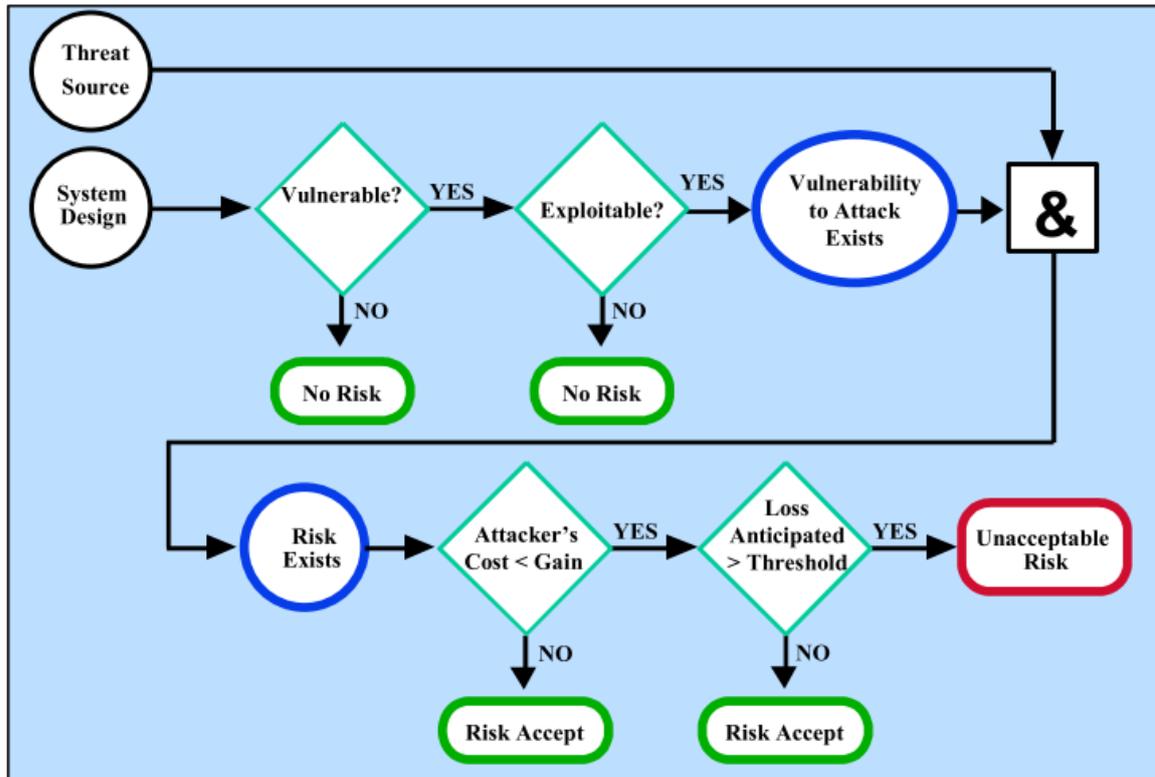
Langkah 9 - Dokumentasi Hasil.



Gambar 2.2 Sembilan Langkah Utama Penilaian Risiko NIST

2. Mitigasi Risiko (*Risk Mitigation*)

Setelah potensi risiko dan kontrol diketahui sesuai rekomendasi maka tindakan berikutnya adalah melakukan peringanan risiko dan membuat kontrol kapan dan dalam keadaan apa harus bertindak untuk mengurangi risiko dan melindungi sistem informasi. Diagram mitigasi risiko pada Gambar 2.3 membahas pertanyaan-pertanyaan ini. Point yang tepat untuk pelaksanaan tindakan pengendalian ditunjukkan pada gambar ini dengan kata YA.



Gambar 2.3 Tahapan Mitigasi risiko

Keterangan Gambar 2.3

Strategi ini selanjutnya diartikulasikan dengan aturan praktis berikut, yang memberikan panduan tindakan untuk mengurangi risiko dari ancaman manusia yang disengaja.

Bila kerentanan (atau kelemahan, kelemahan) di temukan maka diterapkan teknik pengamanan untuk mengantisipasi kemungkinan berkembangnya kerentanan yang sedang terjadi.

Bila kerentanan dapat dilakukan - terapkan perlindungan berlapis, desain arsitektur, dan kontrol administratif untuk meminimalkan risiko atau mencegah kejadian ini.

Bila risiko dibawah ambang batas maka tingkatkan sistem kontrol sehingga serangan dapat di tekan. Caranya adalah dengan menggunakan kontrol sistem seperti membatasi apa yang dapat diakses dan dilakukan oleh pengguna secara signifikan dapat mengurangi keuntungan penyerang.

Bila risiko melebihi ambang kerugian terlalu besar → menerapkan prinsip desain, desain arsitektur, dan teknis dan perlindungan non-teknis untuk membatasi tingkat serangan, sehingga mengurangi potensi kerugian.

3. Evaluasi Risiko (*Risk Evaluation*)

Evaluasi risiko ini adalah tahapan akhir di dalam proses manajemen risiko analisis *Fake Waypoint* dengan menggunakan *Framework NIST Special Publication 800-30*. Pada tahap ini melaksanakan kegiatan evaluasi dilakukan sesuai dengan kebutuhan. Pada tahap ini juga di buat solusi pemecahan berdasarkan kasus yang ditangani. Tahap berikutnya adalah menyiapkan antisipasi terhadap ancaman dan risiko yang sudah berkembang. Tahap akhir adalah melakukan backup data dan menyusun manajemen keamanan sistemnya.

BAB 3

Metodologi Penelitian

3.1 Metode Penelitian

Adapun penelitian ini menggunakan metode kualitatif yaitu dengan pendekatan studi kasus yang terjadi di Konsultan CV. Rickomputer Banjarbaru Kalimantan Selatan. Konsultan ini bergerak di bidang Teknologi Informasi, Survey, Pemetaan dan pembuatan Aplikasi diantaranya Geographic Information System. Adapun data yang di analisa terdiri dari data primer dan sekunder dimana data dilakukan dengan langsung ke lapangan dan data yang sudah ada dari pelaku survey (surveyor) pihak ke dua.

3.2 Studi Kepustakaan

Studi ini dilakukan untuk mendapatkan informasi tentang tema penelitian yang terkait. Sumber pustaka dari Jurnal, buku, artikel, atau bahan tertulis lainnya, yang berupa teori, laporan hasil penelitian atau penemuan terdahulu, Informasi yang digali berupa data GPS , *Framework* NIST (Ucu Nugraha, 2016). Berikut skema kerangka kerja metode penelitian menggunakan *Framework* NIST(Stoneburner Gary , Goguen Alice, 2002).

3.3 Observasi

Metode ini dilakukan dengan langsung mengamati lapangan dengan melakukan pencatatan pencatatan, mengamati individu maupun kelompok untuk dianalisa. Ada dua tehnik observasi yaitu :

1. Observasi yang direncanakan,

Unit-unit tingkah laku yang akan diamati dirumuskan atau ditentukan lebih dulu, dan catatan-catatan yang dibuat hanyalah mengenai aspek-aspek atau kegiatan yang telah ditentukan.

2. Observasi yang tidak direncanakan

Observasi yang dilakukan tanpa menentukan dulu individu atau kelompok serta aspek atau kegiatan dan tingkah laku yang akan diamati. Cara ini akan di harapkan akan mendapatka data yang bervariasi dan lebih luas.

3.4 Tempat dan Waktu Penelitian

Dalam penelitian ini digunakan metode kualitatif yaitu dengan pendekatan studi kasus dimana lokasinya pada Konsultan CV. Rickomputer Banjarbaru Kalimantan Selatan. Konsultan ini bergerak di bidang Teknologi Informasi, Survey, Pemetaan dan pembuatan Aplikasi diantaranya Geographic Information System. Data yang dianalisa adalah survey di rentang waktu tahun 2014 hingga 2016, dimana selama itu konsultan mengerjakan proyek pemerintah bidang kegiatan pekerjaan pemetaan.

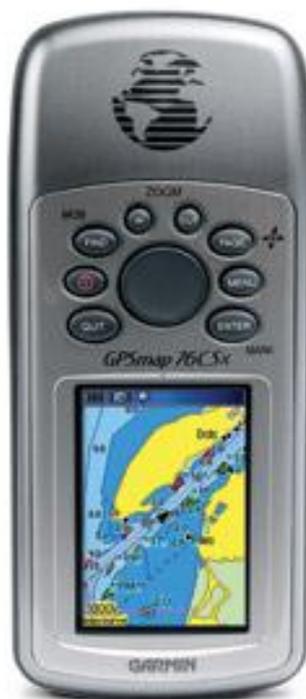
3.5 Bahan dan Alat Penelitian

Sebagai sarana pendukung penelitian perangkat yang digunakan dikelompokkan menjadi 2 :

Perangkat Keras

1. GPS Map Garmin 76 CSx
2. Laptop ASPIRE ONE , Ram 4GB, HD 500 GB
3. Kabel Data

Dalam penelitian ini perangkat GPS yang digunakan adalah GPS Garmin GPSMAP 76CSx dengan keterangan lebih lengkap sebagai berikut:



Gambar 3.1 Foto Prangkat GPS Garmin GPSMAP 76 CSx

Berikut spesifikasi yang di ambil dari Manual Book :

Merk/Tipe	: Garmin GPSMAP 76 CSx
Dimensi	: 2.7" x 6.2" x 1.2" (6.9 x 15.7 x 3.0 cm)
Ukuran layar	: 1.6" x 2.2" (4.1 x 5.6 cm)
Resolusi layar	: 160 x 240 pixels
Tipe layar	: 256 color transfective TFT
Berat	: 7.7 oz (218 g) dengan baterai
Baterai	: 2 AA baterai (tidak termasuk)
Umur baterai	: 18 jam
Tahan air	: Ya (IPX7)
Floats	: Ya
High-sensitivity receiver	: Ya
Konektor	: Serial dan USB
Memori eksternal	: 128 microSD™ card (termasuk)

Perangkat Lunak

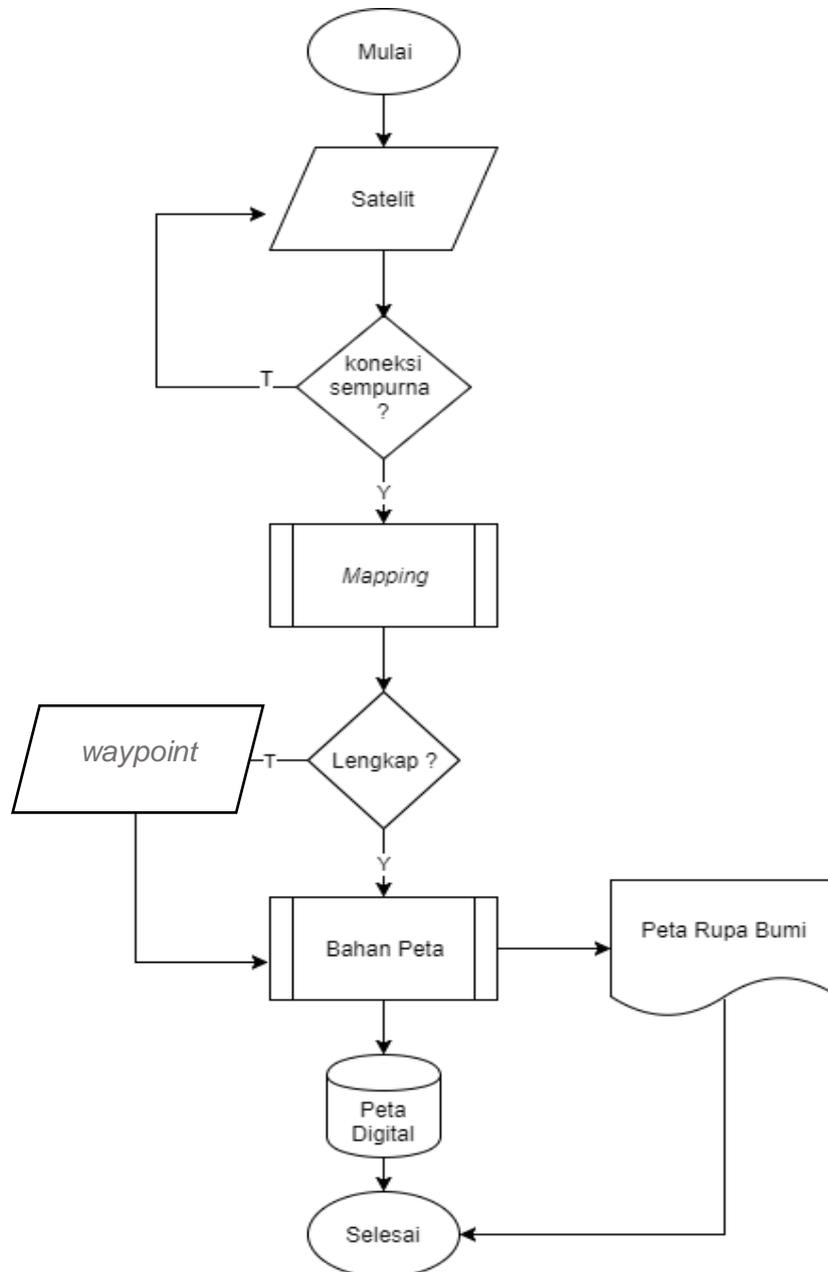
1. Windows 7 64 bit
2. Map Source berfungsi sebagai map download dan map editor
3. Transformasi Koordinat, berfungsi untuk konversi koordinat

3.6 Persiapan Tahap Penelitian

Pada tahapan ini dilakukan proses akuisisi data yang yang di ambil dari lokasi survey dengan melakukan *mapping* menggunakan perangkat GPS. Setelah selesai kemudian akuisisi data *waypoint*. Tahap berikutnya adalah mengambil data *waypoint* yang diduga *telah di maipulasi (fake waypoint)*. Pada tahap ini proses analisis sudah siap dilakukan

3.7 Pengumpulan Data

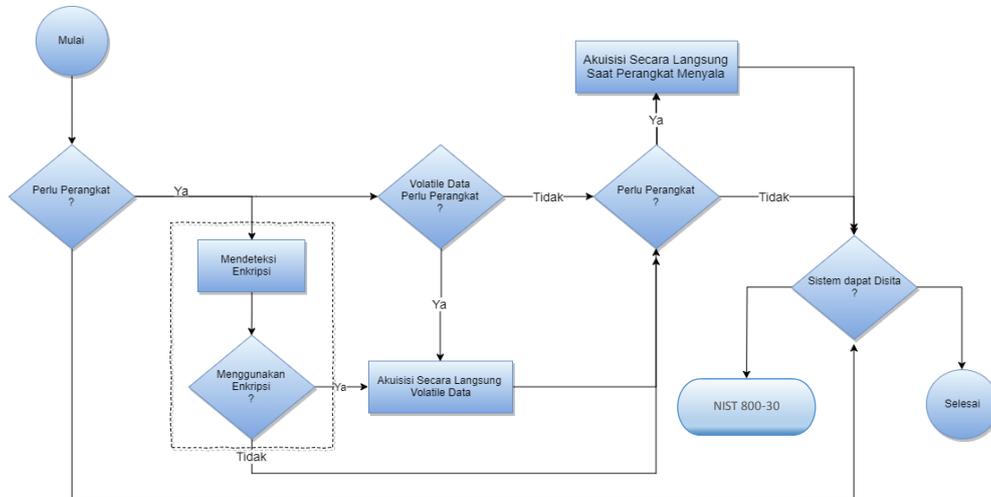
Proses pengumpulan data dilakukan dengan survey kelapangan untuk mendapatkan titik *waypoint* yang asli menggunakan GPS.



Gambar 3.2 Proses Survey Pengambilan Data Koordinat (*Tracks, Waypoint*)

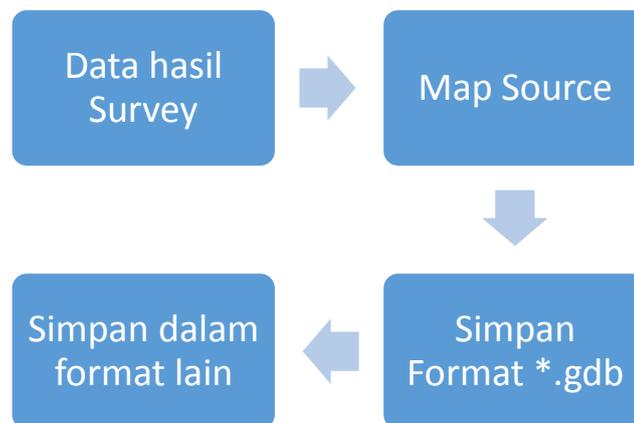
3.8 Akuisisi Data Waypoint

Tahap pengambilan data primer dan sekunder dari masing sumber. Untuk pengambilan data ini digunakan ISO 27023:24. Data Primer didapat dengan cara turun langsung kelapangan menggunakan GPS *Map*, sedangkan data sekunder adalah data sudah jadi.



Gambar 3.3 *Flowchart* Akuisisi Log File data survey dari GPS Map

Proses berikutnya adalah mengakuisisi ekspor hasil survey menggunakan Map Source, kemudian file disimpan dalam format *.gdb.



Gambar 3.4 Proses Ekspor *Log File* Data Survey

3.9 Penerapan *Framework NIST*

Dalam penelitian ini acuan untuk penilaian risiko keamanan teknologi informasi menggunakan *Framework NIST (National Institute of Standard and Technology)* Special Publication (SP) 800-30, yang merupakan standar Panduan Manajemen Risiko untuk Sistem Teknologi Informasi yang merupakan standar Pemerintah Federal US. Metodologi ini terutama dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisa keamanan yang cukup sesuai dengan keinginan pemilik sistem dan ahli teknis untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem TI. Proses ini sangat komprehensif, meliputi segala sesuatu dari ancaman-sumber identifikasi untuk evaluasi berkelanjutan dan penilaian.

Pada Bab 2 telah disebutkan, terdapat 3 tahapan dalam penerapan *Framework* ini yaitu : penilaian risiko (*risk assessment*), peringanan risiko (*risk mitigation*), dan evaluasi risiko (*risk evaluation*).

3.9.1 Penilaian Risiko (*Risk Assesment*)

Langkah awal dalam metodologi manajemen risiko yang dikeluarkan oleh NIST adalah melakukan penilaian terhadap risiko untuk mendefinisikan ancaman potensial dan risiko yang berkaitan dengan penggunaan teknologi informasi. Tujuan yang ingin di capai dari tahap ini adalah untuk dapat membantu mengidentifikasi bagaimana melakukan kontrol untuk meminimalisir atau menghilangkan risiko selama proses mitigasi. Ada 9 (Sembilan) langkah yang harus dipenuhi yaitu (Stoneburner Gary, Goguen Alice, 2002) :

Langkah 1 - Karakterisasi Sistem (*System Characterization*),

Langkah pertama dalam proses ini adalah mengidentifikasi sumber data dan potensi ancaman risiko untuk mendukung tapan berikutnya

Langkah 2 - Identifikasi Ancaman (*Threat Identification*),

Mengenali berbagai sumber gangguan yang akan terjadi pada sistem. Masukan dari proses ini berupa gangguan yang pernah terjadi, data dari berbagai pihak. Sedangkan keluaran dari proses ini berupa adalah *Threat statement* (ancaman ancaman), yaitu berupa risiko risiko yang kemungkinan terjadi serta sumber risiko yang dapat menimbulkan kerentanan

Langkah 3 - Identifikasi Kerentanan (*Vulnerability Identification*),

Langkah ini mengidentifikasi adanya berbagai kelemahan atau kekurangan dari sistem yang dapat mengancam sistem. Masukan pada langkah ini berupa laporan dari penilaian risiko terdahulu, atau serangan yang pernah terjadi, serta hasil pengecekan/pengetesan sistem. Keluaran dari proses ini adalah *list vulnerability* atau kerentanan yang mungkin terjadi risiko gangguan.

Langkah 4 - Analisis Kontrol (*Control Analysis*)

Tujuan utama langkah ini adalah untuk menganalisa kontrol yang akan dan telah diterapkan serta untuk meminimalisir terjadinya ancaman. Masukan dari langkah ini berupa kontrol yang telah diterapkan dalam masing-masing risiko/kerentanan, sementara outputnya adalah list dari kontrol terhadap risiko yang sedang dan akan diterapkan terhadap risiko yang mungkin terjadi.

Langkah 5 - Penentuan Kemungkinan (*Likelihood Determination*)

Digunakan untuk mendapatkan nilai kecenderungan yang kemungkinan terjadi terhadap kelemahan sistem. Masukan dari langkah ini berupa sumber risiko dan yang mendorong penyebab sumber risiko, kerentanan dan efektifitas kontrol yang diterapkan.

Langkah 6 – Analisa Dampak (*Impact Analysis*)

Langkah ini untuk menilai dampak serangan atas bagian lemah yang diakibatkan dari lemahnya sebuah sistem. Masukan dari sistem ini adalah tujuan sistem serta tingkat sensitifitas data atau dengan kata lain bagaimana risiko akan berpengaruh pada misi sistem dan data yang diolah. Kemungkinan yang menjadi pertimbangan adalah masalah integritas data, ketersediaan terhadap layanan dan kehilangan kepercayaan. Output dari sistem ini adalah definisi dampak dari risiko (*magnitude of impact definition*).

Langkah 7 - Penentuan Risiko (*Risk Determination*)

Tujuan penentuan risiko ini adalah untuk menilai tingkat risiko terhadap sistem, dengan mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan. Hasil penentuan risiko dapat dilihat ditabel di bawah ini (Stoneburner Gary , Goguen Alice, 2002)

Tabel 3.1 Matrik Level Risiko

<i>Threat Likelihood</i>	<i>Impact</i>		
	<i>Low (10)</i>	<i>Medium (50)</i>	<i>High (100)</i>
<i>High (1.0)</i>	<i>Low</i> $10 \times 1.0 = 10$	<i>Medium</i> $50 \times 1.0 = 50$	<i>High</i> $100 \times 1.0 = 100$
<i>Medium (0.5)</i>	<i>Low</i> $10 \times 0.5 = 5$	<i>Medium</i> $50 \times 0.5 = 25$	<i>Medium</i> $100 \times 0.5 = 50$
<i>Low (0.1)</i>	<i>Low</i> $10 \times 0.1 = 1$	<i>Low</i> $50 \times 0.1 = 5$	<i>Medium</i> $100 \times 0.1 = 10$

Tabel 3.2 Gambaran risiko dan tindakan yang di perlukan

<i>Risk Level</i>	<i>Risk Description and Necessary Actions</i>
<i>High</i>	<i>If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.</i>
<i>Medium</i>	<i>Medium If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.</i>
<i>Low</i>	<i>Low If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.</i>

Langkah 8 - Rekomendasi Kontrol (*Control Recommendations*)

Tujuannya untuk mengurangi level risiko pada sistem TI sehingga mencapai level yang bisa diterima. Inputnya adalah dari output dari tahapan sebelumnya yaitu risiko dan tingkat risiko, dari sini akan dihasilkan daftar rekomendasi kontrol.

Langkah 9 - Dokumentasi Hasil (*Results Documentation*)

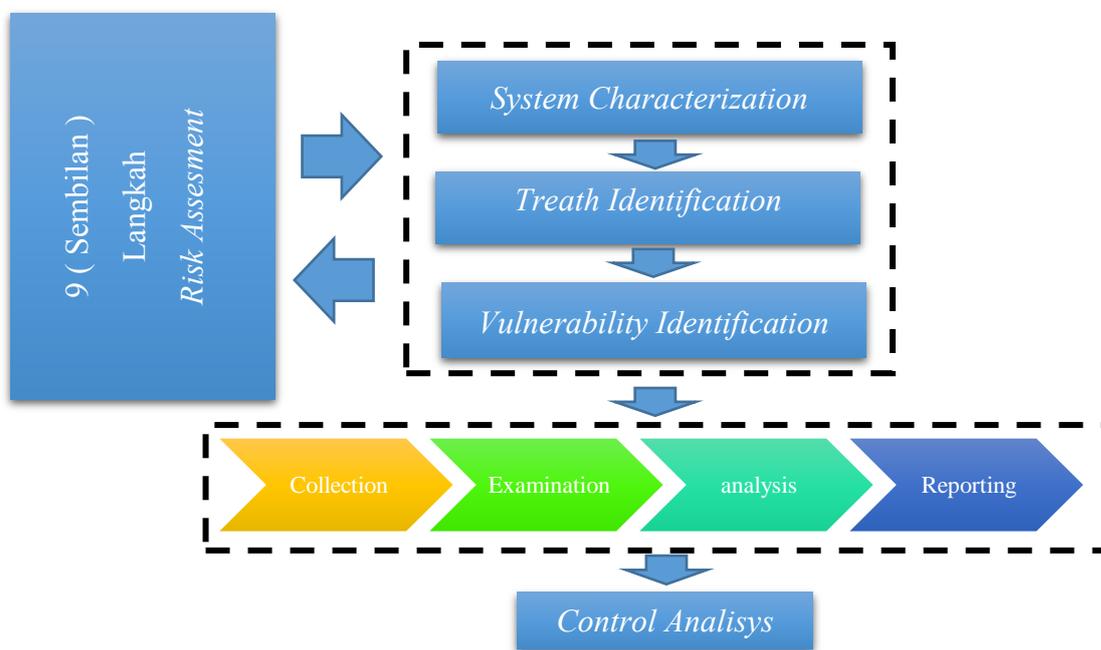
Merupakan laporan atau dokumentasi hasil dari seluruh kegiatan yang telah dilakukan, dimulai tahap karakteristik hingga rekomendasi kontrol.

3.10 Simulasi Kasus

Terdapat 9 (Sembilan) tahapan didalam *Framework* NIST, posisi tahap ke 2, ke 3 dan ke 4 menjadi titik rawan berlangsungnya ancaman risiko yang muncul dari sebuah sistem

informasi. Tahap ke 2 adalah tentang identifikasi ancaman (*Threat Identification*), pada tahap ini diketahui ancaman apa saja yang akan mengganggu sistem. Pada tahap ini juga akan mengenali berbagai sumber gangguan yang akan terjadi pada sistem. *Input* dari proses ini berupa daftar gangguan yang pernah terjadi dan yang akan terjadi, data dari berbagai pihak. *Output* dari tahap ini berupa daftar risiko risiko yang kemungkinan terjadi serta sumber risiko yang dapat menimbulkan kerentanan.

Sedangkan tahap ke 3 tentang *Vulnerability Identification* yang merupakan step 3 dari 9 step *Framework* NIST SP 800-30 menjadi sangat penting untuk mengidentifikasi adanya risiko ancaman dari kerentanan sistem yang dapat mengancam sistem itu sendiri. *Input* langkah ini berupa laporan dari penilaian risiko terdahulu, atau serangan yang pernah terjadi, serta hasil pengecekan/pengetesan sistem. *Output* dari proses ini adalah *list vulnerability* atau kerentanan yang mungkin dan telah terjadi. Berikut gambaran penanganan alur kasus yang nantinya untuk bahan masukan pada Langkah 4.



Gambar 3.5 Alur Penangan *Vulnerability Identification* pada pembuatan Peta Digital

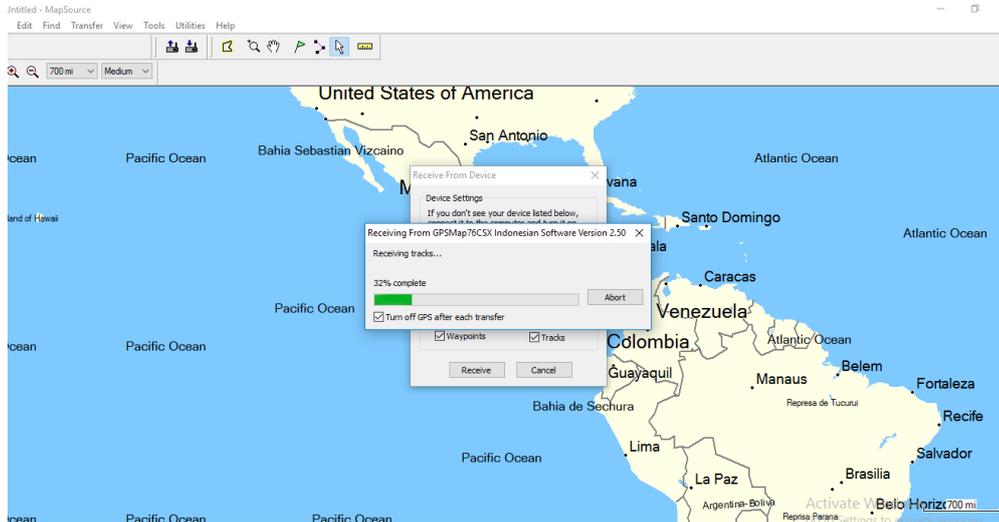
Sedangkan tahap ke 4 merupakan tahap kontrol adanya ancaman risiko dan menjadi rekomendasi terhadap penentuan kemungkinan munculnya risiko.

BAB 4

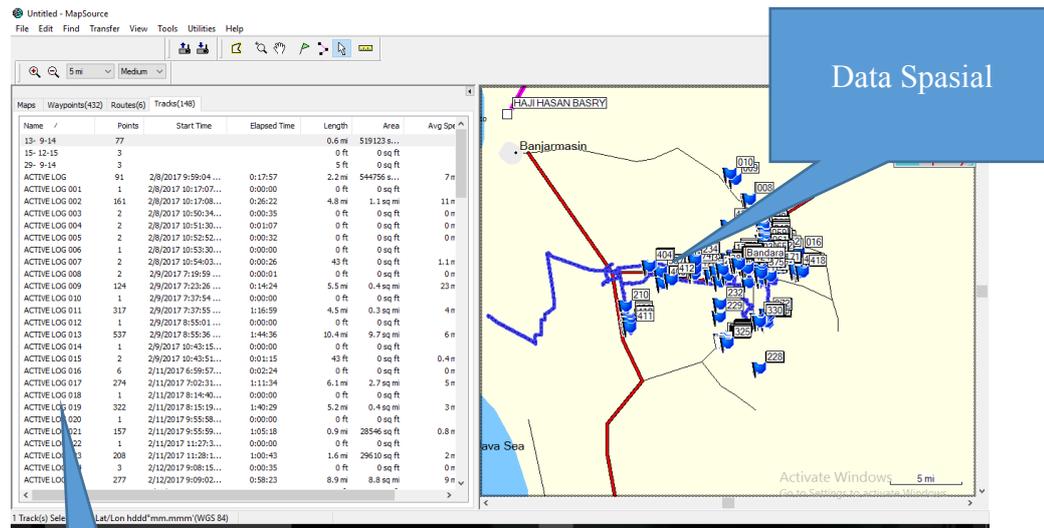
Implementasi Dan Analisa Data

4.1 Capture Data

Dalam penelitian ini ditampilkan capture dari proses pengambilan data yang akan di gunakan untuk sampel penelitian.



Gambar 4.1 Proses Pengunduhan Log File Dari GPS Maps



Gambar 4.2 Hasil Unduhan data GPS Map

Pada gambar 4.1 dan 4.2 menunjukkan proses akuisi data hasil survey dari GPS Maps menggunakan Map Source. Hasil dari akuisi data terlihat di gambar 4.2 yang menunjukkan data Atribut dan Spasial.

Data Atribut

4.2 Data

4.2.1 Simulasi Kasus

Dalam simulasi ini digunakan 2 perangkat Garmin GPS *Map* dengan seri yang sama yaitu GPS *Map 67 CSx*. GPS *Map* yang pertama digunakan untuk membuat data *Waypoint on Location* sedangkan GPS *Map* yang kedua untuk membuat data *Fake Waypoint*. Langkah berikutnya adalah mengakuisisi data dari masing masing GPS *Map* kemudian melakukan penilaian terhadap masing masing data .

4.2.2 Sumber data

Data dalam penelitian ini adalah merupakan hasil turun ke lapangan dan tersimpan didalam perangkat GPS *Map*. Dari perangkat tersebut kemudian data di akuisisi dan di simpan ke komputer dan berikutnya diolah kembali untuk dijadikan peta digital. Selain data yang diambil langsung dari GPS hasil survey data juga diambil dari file yang sudah tersimpan sebelumnya.

4.2.3 Cara Mendapatkan Data

Proses pengambilan data diawali dengan menyiapkan perangkat berupa GPS, USB kabel data dan komputer sebagai tempat penyimpanan hasil survey. Langkah berikutnya adalah mengakuisisi data langsung dari GPS *Map* Garmin 67 CSx setelah GPS dikoneksikan di komputer menggunakan USB data kabel. Tool untuk mengakuisisi data digunakan *Software Map Source* yang merupakan *driver* sekaligus *tool software* yang di ikut sertakan ketika membeli perangkat GPS. File hasil akuisisi di simpan dalam format default GDB.

4.2.4 Format Data

Format data dari file data ini adalah GDB. Isi file data GDB ada dua jenis yaitu data spasial dan atribut atau tabular, dimana kedua jenis data tersebut saling berhubungan. Data spasial mewakili obyek sedangkan data atribut memberikan keterangan tentang obyek tersebut. Jadi secara teknis visualisasi kedua jenis data tersebut tidak dapat dipisahkan. Dalam visualisasi data tabular dan spasial terdapat 4 tab attribut yaitu *Maps*, *Waypoints*, *Routers*, *Tracks*. Namun hanya atribut *Tracks* dan *Waypoint* yang di gunakan karena hanya data *Track* dan *Waypoint* yang di perlukan untuk pembuatan peta digital.

Format file data dari hasil akuisisi ada 4 (empat) yaitu *Garmin GPS Database* (*.gdb), MPS files (*.mps), Text (*.txt), DXF (*.dxf) dan GPS eXchange Format (*.gpx).

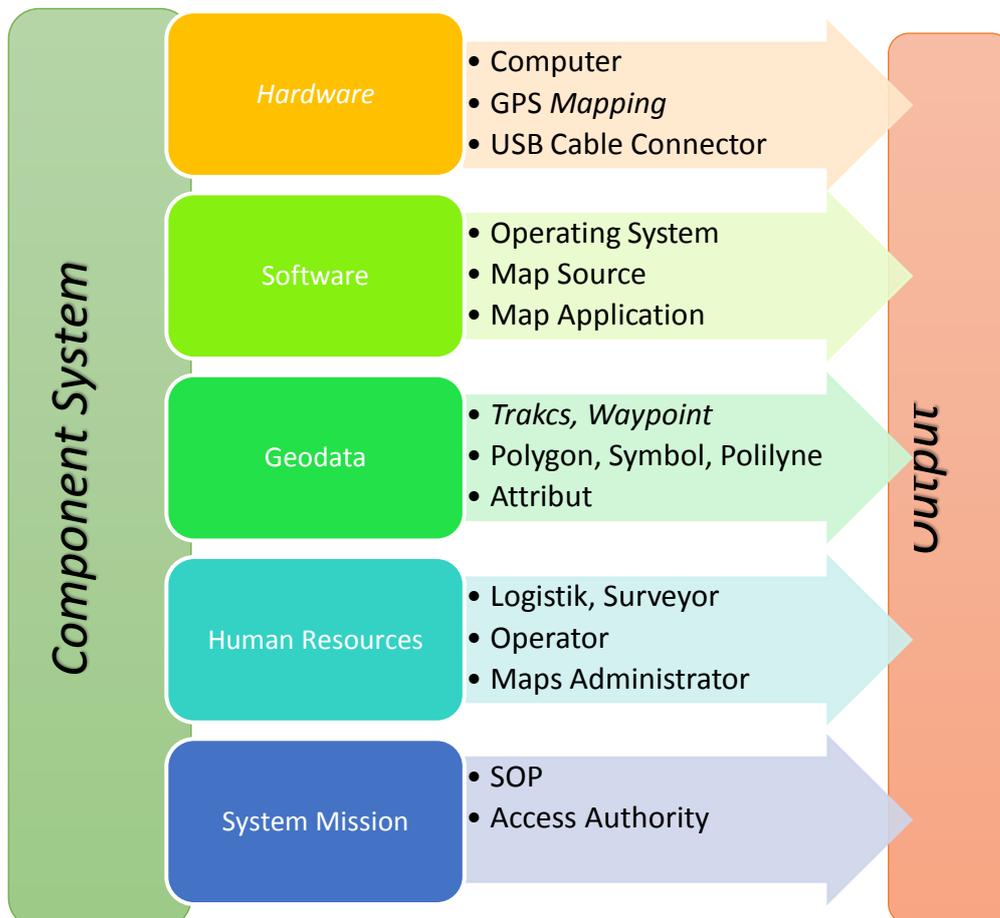
4.3 Penerapan NIST dalam Pembuatan Peta Digital

Seperti telah di sampaikan pada bab sebelumnya ada 3 tahapan dalam penilaian risiko *Framework* NIST SP 800-30 dan implementasinya pengujianya sebagai berikut :

4.3.1 Proses Implementasi

1. Karakter Sistim (*System Characterization*)

Pada tahap ini terlihat kebutuhan sistem untuk pencetakan peta digital. Inisiasi dikategorikan dalam kelompok *hardware, software, interface, Geodata, Human Resource, System Mission*. Gambar 4.3 memperlihatkan sistem tersebut yang masing masing kategori mempunyai item lagi. Dari gambar tersebut terlihat batasan sistem, fungsionalitas sistem data dan tingkat sensitifitas , pengguna. *Output* dari step ini akan menjadi masukan pada step berikutnya



Gambar 4.3 System Characterization step process

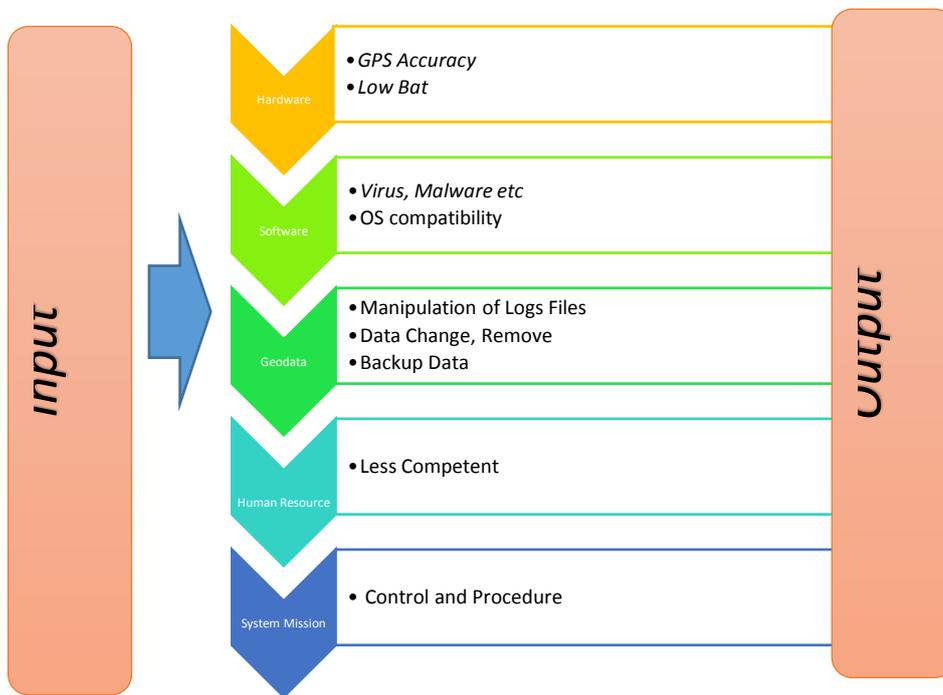
2. Identifikasi Ancaman (*Threat Identification*)

Hasil observasi lapangan, teridentifikasi ancaman yang mengganggu pada sistem pembuatan peta digital adalah penggunaan system OS yang terbatas pada Windows series , akurasi *data survey* yang *lost tolerance*, sumber daya yang melemah pada saat survey kelapangan juga menjadi ancama terhadap penerimaan data dari satelit yang bisa menyebabkan *lost tolerance*. Tidak adanya alarm pada saat baterai lemah (*Low Bat*) pada *GPS Map 76 CSx* yang memberi tanda ke surveyor, serta file peta digital yang mudah diubah. Berikut table yang menunjukkan aspek karakter sistem dan ancaman yang dimunculkan.

Tabel 4.1 Ancaman pada yang muncul dari karakter sistem.

Karakter Sistem		Ancaman	Keterangan
<i>Hardware</i>	Komputer	Akurasi GPS Maps, Baterai lemah	Lemahnya baterai selama inididak diikuti dengan alarm pemberitahuan
	GPS Maps		
	Kabel USB Konektor		
<i>Software</i>	Operating System	Windows Series	Aplikasi akuisisi data saat ini hanya bisa berjalan di OS Windows
	Map Source		
	Maps Application		
Geodata	<i>Spacial</i>	File Digital yag mudah dirubah, dicuri, digandakan , bakup	-
	<i>Tabular</i>		
	<i>Waypoints Tracks</i>		
	<i>Longitude, Latitude</i>		
<i>Human Resources</i>	Kurang Kompetent	Kualitas peta digital	-

<i>System mission</i>	Aturan dan prosedur	Proses dan tanggung jawab kerja yang tumpang tindih	-
-----------------------	---------------------	---	---



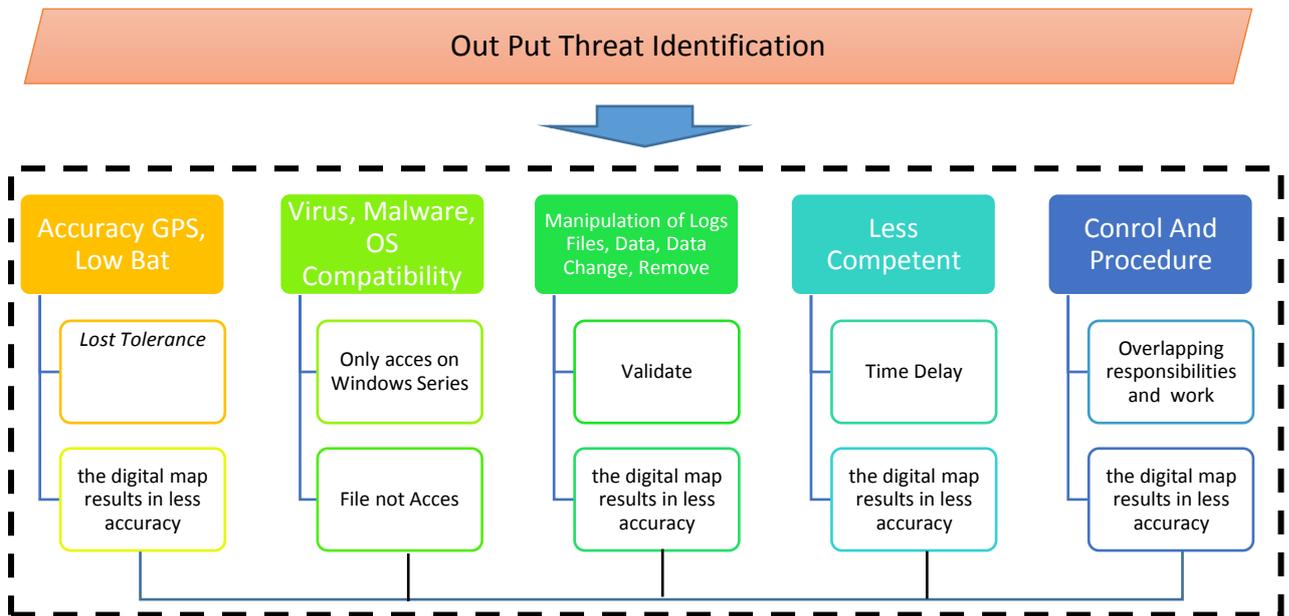
Gambar 4.4 Jenis dan Sumber Ancaman

Pada table 4.1 dan gambar 4.4 menjelaskan tentang munculnya ancaman dari masing masing aspek yaitu , hardware dengan ancaman akurasi GPS, baterai lemah , software dengan ancaman virus , malware , OS hanya windows, dari sisi data adalah mudahnya dirubah menyebabkan data mudah di manipulasi, dihapus , bakup data, dari factor sumber daya manusia adalah kurang kompeten dan yang terakhir adalah dari sisi *system mission* belum ada aturan control prosedur.

3. Identifikasi Kerentanan (*Vulnerability Identification*)

Kerentanan yang teridentifikasi pada step ini merupakan *output dari step 2* yaitu , akurasi GPS yang *lost tolerance* , data yang tidak bisa dibuka karena terinfeksi virus, penggunaan

operating sistem yang terbatas hanya windows saja, file digital yang mudah di manipulasi, tidak adanya backup data, kemudian rendahnya kompetensi, tidak adanya prosedur baku yang memuat batasan batasan pekerjaan dan otorisasi antar bagian serta belum ada standart sistem pengamanan file data dan peralatan. Hal tersebut berdampak pada, data survey tidak akurat, data survey mudah di manipulasi, terhapus, digandakan dan file mudah di akses oleh siapa saja untuk tujuan tertentu.

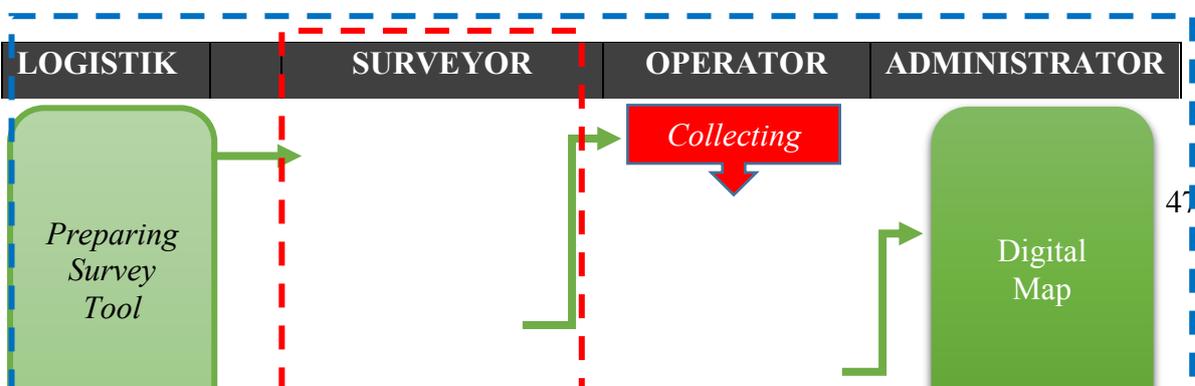


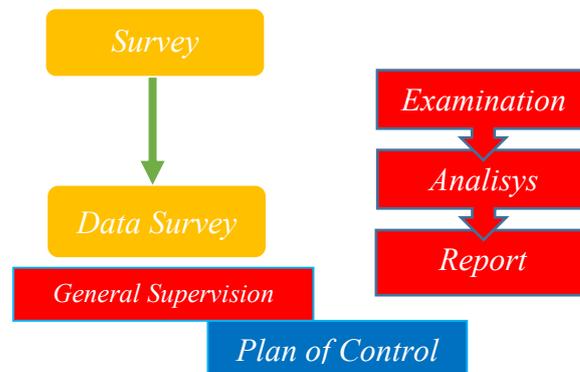
Gambar 4.5 Identifikasi Kerentanan Proses

Pada gambar 4.5 menjelaskan tentang aktiviti dari proses identifikasi penyebab munculnya ancaman risiko terhadap sitem pembuatan peta digital, dimana risiko akir adalah pencetakan peta digital yang tidak akurat.

4. Analisa Kontrol (*ControlAnalisis*)

Secara kusus analisa kontrol mulai persiapan pekerjaan, proses, penyerahan peralatan dan hasil survey hingga hasil data sampai pada pengolah informasi belum ada prosedur dan alur yang secara sistematis terlihat jelas batas batas tanggung jawab antar bagian. Sehingga siapa yang berwenang melakukannya tidak ada secara jelas terurai dalam job pekerjaan ini.



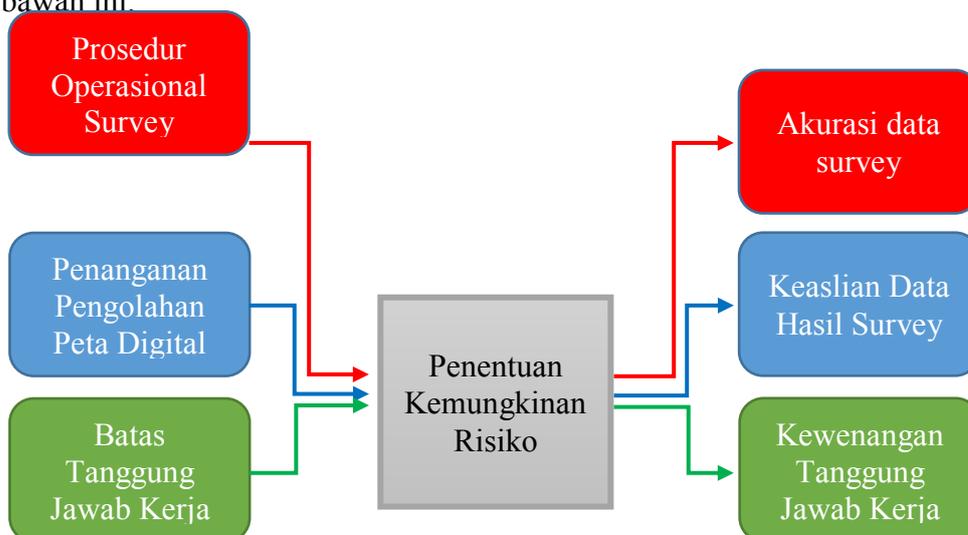


Gambar 4.6 Control Activity Pembuatan Peta Digital

Gambar 4.6 memperlihatkan proses aktivitas penanganan ancaman risiko di masing masing bagian, dimulai dari mempersiapkan penggunaan alat, melakukan survey kemudian menyerahkan hasil survey ke bagian operator yang kemudian data hasil survey dianalisa dengan menggunakan NIST SP 800-86 *Performing the Forensic Process* sebagai bahan untuk penilaian (Kent, Chevalier, Grance, & Dang, 2006). Tahap proses tersebut adalah *collecting, examination, analisys, report* dimana hasil report berupa data peta digital yang siap untuk dicetak.

5. Penentuan Kemungkinan Risiko (*Likelihood Determination*)

Belum diterapkannya kerangka kerja NIST SP 800 - 30 maka Analisa kontrol yang secara khusus untuk kegiatan penilaian risiko belum ada, selama ini pendeteksian dan pencegahan ancaman risiko yang dilakukan hanya berdasarkan pada kebiasaan ditambah dengan pengalaman serta pengetahuan saja. Dari hasil observasi analisa kontrol yang memungkinkan dapat digunakan untuk penilaian risiko meliputi : 1. Prosedur operasional survey, 2. Penanganan pengolahan peta digital. 3. Batasan Tanggung jawab kerja. 4. Manajemen penangan sistem keamanan peta digital. Berdasarkan analisa kontrol tersebut, maka potensi ancaman yang bisa dieksploitasi menjadi sumber risiko adalah: 1. Akurasi data *survey*, 2. Keaslian data hasil survey, 3. Kewenangan tanggung jawab kerja, 4. Otorisasi hak akses. Penentuan tersebut dapat tergambat dalam Gambar 4.7 seperti dibawah ini.





Gambar 4.7 Penentuan Kemungkinan Risiko Pembuatan Peta Digital

6. Analisa Dampak (*Impact Analysis*)

Berdasarkan kemungkinan ancaman risiko yang ada, maka dampaknya dapat dilihat di tabel berikut 4.2 dibawah ini.

Tabel 4.2 Dampak Risiko

Jenis Risiko	Dampak	Nilai Dampak
<i>Low Bat</i>	Kesalahan posisi koordinat	<i>High</i>
<i>Lost Tolerance</i>	Posisi koordinat berubah	<i>High</i>
Otorisasi Hak Akses	Rentan terhadap penggandaan file dan perubahan isinya oleh yang tidak berhak	<i>High</i>
Backup Data	Melakukan survey ulang jika file nya rusak atau hilang	<i>Medium</i>
Prosedur pengolahan data	Belum ada pembagian tanggung jawab pekerjaan hasil pekerjaan	<i>High</i>
Sumbe Daya Manusia	Tidak ada batasan tanggung jawab antar bagian	<i>Low</i>

7. Penentuan Risiko (*Risk Determination*)

Penentuan risiko ini untuk menilai tingkat risiko terhadap sistem, penilaian ini mengacu pada kemungkinan risiko dan dampak risiko yang telah ditentukan. Penentuan risiko dapat dilihat pada tabel berikut :

Tabel 4.3 Besaran definisi dampak

Tipe Risiko	Skor Kemungkinan Ancaman	Skor Dampak	Skor Risiko	Predikat Level Rangking
-------------	--------------------------	-------------	-------------	-------------------------

<i>Low Bat</i>	1.0 (High)	100 (High)	100	High
<i>Lost Tolerance</i>	1.0 (High)	100 (High)	100	High
Otorisasi Hak Akses	1.0 (High)	100 (High)	100	High
Backup Data	0.5 (Sedang)	50 (Sedang)	25	Sedang
Prosedur pengolahan data	0.5 (Sedang)	50 (Sedang)	25	Sedang
Sumbe Daya Manusia	0.1 (Rendah)	10 (Sedang)	10	Rendah

8. Rekomendasi Kontrol (*Control Recommendation*)

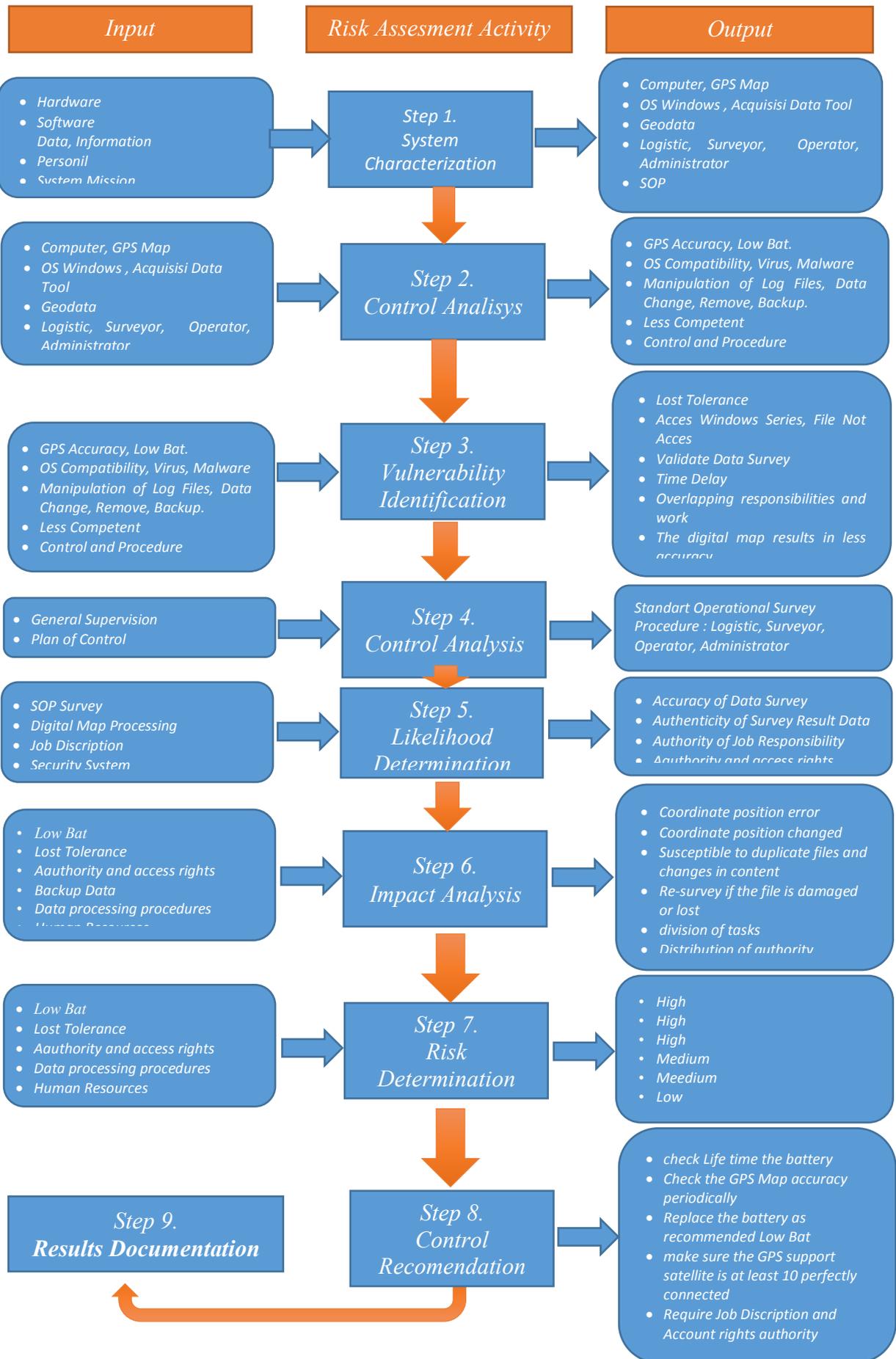
Rekomendasi kontrol dapat dilihat pada tabel berikut ini:

Tabel 4.4 Rekomendasi Kontrol

Jenis Risiko	Tingkat Risiko	Rekomendasi
<i>Low Bat</i>	High	Hitung masa hidup baterai jenis alkaline dari berbagai merek sehingga prediksi penggantian baterai dapat dilakukan
<i>Lost Tolerance</i>	High	<ol style="list-style-type: none"> 1. Cek akurasi toleran <i>GPS Map</i> secara berkala 2. Ganti baterai sesuai rekomendasi <i>Low Bat</i> 3. Sebelum survey pastikan satelit pendukung GPS minimal 10 yang terkoneksi secara sempurna
Otorisasi Hak akses	High	<ol style="list-style-type: none"> 1. Perlu adanya Job Discription 2. Akun yang mengatur hak otoritas

9. Dokumentasi Hasil (*Result Documentation*)

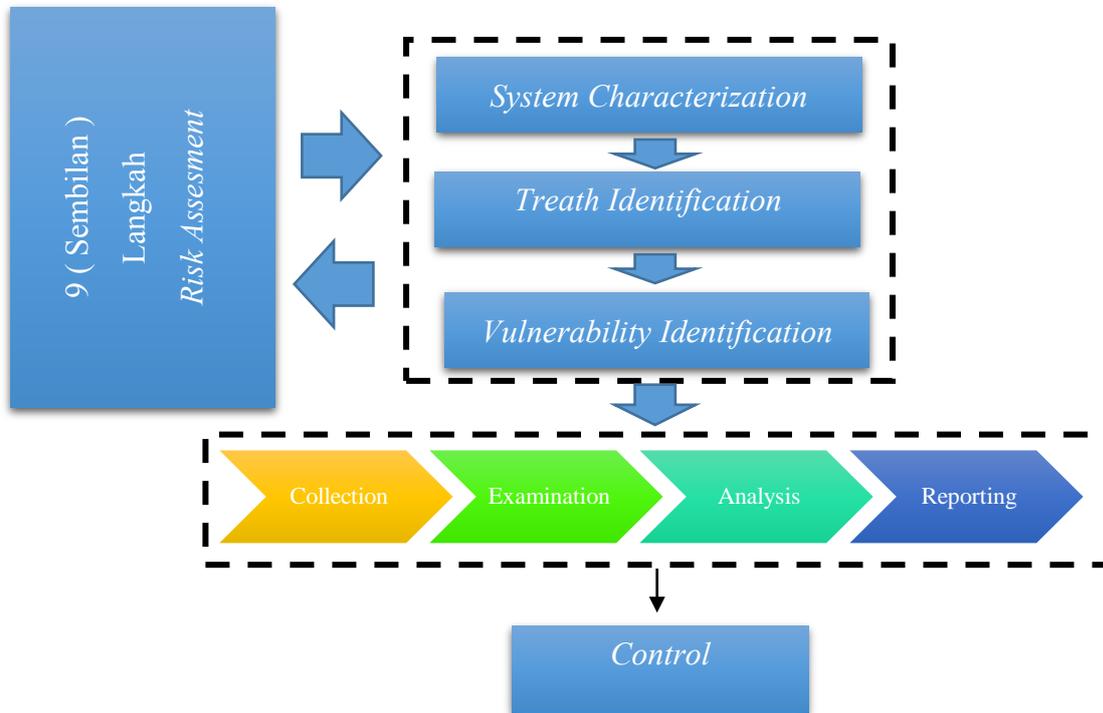
Tahap ini merupakan akhir dari Risk Assesment yang mendokumentasikan hasil dari penilaian risiko yang berupa profil risiko yang dapat mengancam keberlangsungan sistem proses pembuatan peta digital. Gambar 4.8 berikut adalah dokumentasi penanganan ancaman risiko serta rekomendasi penentuan kerentanan dan cara penanganan pembuatan peta digital. Dokumen hasil analisis mulai dari tahap 1 sampai tahap 8 menjadi profil penanganan Pembuatan peta digital seperti yang terlihat pada gambar 4.8 pada halaman berikut.



Gambar 4.8 Profile Digital Map With Framework NIST

4.3.2 Mengatasi Ancaman Risiko dan Kerentanan Geodata

Pada tahap ini dilakukan analisa terhadap data yang sudah di akuisisi yang hasil capturenya terlihat pada point 4.4.1 tentang implementasi dan perbandingan hasil akuisisi data dari GPS Map . Hasil dari analisa tersebut tertuang dalam Table 4.4 yang telah berhasil mengidentifikasi perbedaan survey data *On location* dan *Fake Location*.



Gambar 4.9 Proses Implementasi *Vulnerability Identification* .

Secara detail Gambar 4.7 menunjukkan bagaimana ancaman muncul dan bagaimana menangani ancaman risiko. Berikut ini uraian Gambar 4.7 :

- **Collection** , kumpulan data hasil survey GPS dapat dilihat pada gambar 4.10

Header	Name	Description	Type	Position	Altitude	Depth	Proximity	Temperature	Display Mode	Color	Symbol	Facility
Waypoint	001	03-JUN-17 11:34:02	User Waypoint	53 26.540 E114 50.373	145 ft				Symbol & Name	Black	Flag	Red
Waypoint	002	03-JUN-17 11:34:04	User Waypoint	53 26.540 E114 50.373	145 ft				Symbol & Name	Black	Flag	Red
Waypoint	003	03-JUN-17 11:36:53	User Waypoint	53 26.516 E114 50.309	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	004	03-JUN-17 11:37:07	User Waypoint	53 26.516 E114 50.310	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	005	03-JUN-17 11:37:16	User Waypoint	53 26.516 E114 50.310	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	006	03-JUN-17 11:38:11	User Waypoint	53 26.516 E114 50.310	139 ft				Symbol & Name	Black	Flag	Red
Waypoint	007	03-JUN-17 11:38:32	User Waypoint	53 26.516 E114 50.310	141 ft				Symbol & Name	Black	Flag	Red
Waypoint	008	03-JUN-17 11:38:37	User Waypoint	53 26.516 E114 50.310	141 ft				Symbol & Name	Black	Flag	Red
Waypoint	009	03-JUN-17 11:38:43	User Waypoint	53 26.516 E114 50.310	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	010	03-JUN-17 11:39:53	User Waypoint	53 26.516 E114 50.310	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	011	03-JUN-17 11:40:03	User Waypoint	53 26.516 E114 50.310	143 ft				Symbol & Name	Black	Flag	Red
Waypoint	012	03-JUN-17 11:40:11	User Waypoint	53 26.516 E114 50.310	144 ft				Symbol & Name	Black	Flag	Red
Waypoint	013	03-JUN-17 11:40:15	User Waypoint	53 26.516 E114 50.310	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	014	03-JUN-17 11:40:21	User Waypoint	53 26.516 E114 50.310	142 ft				Symbol & Name	Black	Flag	Red
Waypoint	015	03-JUN-17 11:40:41	User Waypoint	53 26.516 E114 50.310	144 ft				Symbol & Name	Black	Flag	Red
Waypoint	016	03-JUN-17 11:40:47	User Waypoint	53 26.516 E114 50.310	143 ft				Symbol & Name	Black	Flag	Red
Waypoint	017	03-JUN-17 11:40:54	User Waypoint	53 26.516 E114 50.310	143 ft				Symbol & Name	Black	Flag	Red
Waypoint	018	03-JUN-17 11:41:40	User Waypoint	53 26.516 E114 50.310	144 ft				Symbol & Name	Black	Flag	Red
Waypoint	019	03-JUN-17 11:42:02	User Waypoint	53 26.516 E114 50.310	146 ft				Symbol & Name	Black	Flag	Red
Waypoint	020	03-JUN-17 11:42:08	User Waypoint	53 26.516 E114 50.310	146 ft				Symbol & Name	Black	Flag	Red
Waypoint	021	03-JUN-17 11:42:35	User Waypoint	53 26.516 E114 50.310	145 ft				Symbol & Name	Black	Flag	Red
Waypoint	022	03-JUN-17 11:42:46	User Waypoint	53 26.516 E114 50.310	145 ft				Symbol & Name	Black	Flag	Red

Gambar 4.10 Data survey waypoint

hasil.txt - Notepad

File Edit Format View Help

Header	Name	Length	Course	Waypoints	Link
Route	062 to 071	0.5 mi	90°	true	10 waypoints

Header	Waypoint Name	Distance	Leg Length	Course
Route Waypoint	062	0 ft		
Route Waypoint	063	351 ft	351 ft	63° true
Route Waypoint	064	0.2 mi	0.1 mi	79° true
Route Waypoint	065	0.2 mi	198 ft	47° true
Route Waypoint	066	0.3 mi	0.1 mi	61° true
Route Waypoint	067	0.4 mi	468 ft	98° true
Route Waypoint	068	0.5 mi	286 ft	167° true
Route Waypoint	069	0.5 mi	101 ft	162° true
Route Waypoint	070	0.5 mi	105 ft	171° true
Route Waypoint	071	0.5 mi	241 ft	174° true

Header	Name	Start Time	Elapsed Time	Length	Average Speed	Link
Track	ACTIVE LOG	1/21/2018 7:04:03 PM	3:46:49	10.9 mi	3 mph	

Header	Position	Time	Altitude	Depth	Temperature	Leg Length	Leg Time	Leg Speed	Leg Course
Trackpoint	S7 33.597 E110 45.070	1/21/2018 7:04:03 PM	437 ft						
Trackpoint	S7 33.599 E110 45.075	1/21/2018 7:04:04 PM	439 ft	30 ft	0:00:01 21 mph	106°	true		
Trackpoint	S7 33.600 E110 45.079	1/21/2018 7:04:05 PM	436 ft	27 ft	0:00:01 18 mph	109°	true		
Trackpoint	S7 33.602 E110 45.084	1/21/2018 7:04:06 PM	434 ft	29 ft	0:00:01 20 mph	105°	true		
Trackpoint	S7 33.603 E110 45.089	1/21/2018 7:04:07 PM	436 ft	32 ft	0:00:01 22 mph	104°	true		
Trackpoint	S7 33.604 E110 45.093	1/21/2018 7:04:08 PM	436 ft	28 ft	0:00:01 19 mph	109°	true		
Trackpoint	S7 33.606 E110 45.097	1/21/2018 7:04:09 PM	434 ft	28 ft	0:00:01 19 mph	111°	true		
Trackpoint	S7 33.608 E110 45.102	1/21/2018 7:04:10 PM	434 ft	27 ft	0:00:01 19 mph	111°	true		
Trackpoint	S7 33.609 E110 45.106	1/21/2018 7:04:11 PM	434 ft	27 ft	0:00:01 19 mph	113°	true		
Trackpoint	S7 33.611 E110 45.110	1/21/2018 7:04:12 PM	434 ft	27 ft	0:00:01 19 mph	109°	true		
Trackpoint	S7 33.612 E110 45.114	1/21/2018 7:04:13 PM	434 ft	27 ft	0:00:01 18 mph	108°	true		
Trackpoint	S7 33.614 E110 45.118	1/21/2018 7:04:14 PM	434 ft	26 ft	0:00:01 18 mph	110°	true		

Activate Win
Go to Settings to

Gambar 4.11 Data Route waypoint dan Trackpoint

- **Examination**, hasil pemeriksaan data maka ditemukan pola seperti di bawah ini.

hasil.txt - Notepad

044	27-AUG-17 12:32:07	User Waypoint	S3 30.519 E114 59.004	164 ft	Symbol & Name	Black	Flag, Red
045	27-AUG-17 13:36:55	User Waypoint	S3 25.200 E114 50.836	76 ft	Symbol & Name	Black	Flag, Red
046	28-AUG-17 18:23:25	User Waypoint	S3 25.259 E114 50.839	31 ft	Symbol & Name	Black	Flag, Red
047	28-AUG-17 18:37:36	User Waypoint	S3 21.289 E114 37.092	35 ft	Symbol & Name	Black	Flag, Red
048	28-AUG-17 19:08:21	User Waypoint	S3 19.374 E114 41.949	49 ft	Symbol & Name	Black	Flag, Red
049	29-AUG-17 19:38:04	User Waypoint	S3 23.311 E114 50.449	57 ft	Symbol & Name	Black	Flag, Red
050	29-AUG-17 19:58:55	User Waypoint	S3 19.941 E114 47.779	57 ft	Symbol & Name	Black	Flag, Red
051	30-AUG-17 16:57:45	User Waypoint	S3 22.663 E114 53.747	53 ft	Symbol & Name	Black	Flag, Red
052	30-AUG-17 17:15:55	User Waypoint	S3 19.473 E114 58.160	64 ft	Symbol & Name	Black	Flag, Red
053	30-AUG-17 17:31:13	User Waypoint	S3 16.777 E115 01.591	136 ft	Symbol & Name	Black	Flag, Red
054	30-AUG-17 17:58:50	User Waypoint	S3 17.629 E115 06.405	105 ft	Symbol & Name	Black	Flag, Red
055	30-AUG-17 17:58:54	User Waypoint	S3 17.629 E115 06.405	105 ft	Symbol & Name	Black	Flag, Red
056	30-AUG-17 18:57:12	User Waypoint	S3 12.155 E115 13.793	178 ft	Symbol & Name	Black	Flag, Red
057	30-AUG-17 18:57:53	User Waypoint	S3 12.199 E115 13.850	169 ft	Symbol & Name	Black	Flag, Red
058	30-AUG-17 20:42:03	User Waypoint	S3 14.574 E115 05.131	369 ft	Symbol & Name	Black	Flag, Red
059	16-SEP-17 5:01:42	User Waypoint	S3 24.270 E114 48.682	187 ft	Symbol & Name	Black	Flag, Red
060	21-JAN-18 15:11:04	User Waypoint	S7 48.871 E110 19.542	1338 ft	Symbol & Name	Black	Flag, Red
061	21-JAN-18 15:11:50	User Waypoint	S7 48.871 E110 19.542	1338 ft	Symbol & Name	Black	Flag, Red
062	061	User Waypoint	S7 32.884 E110 49.849		Symbol & Name	Unknown	Waypoint
063	062	User Waypoint	S7 32.838 E110 49.895		Symbol & Name	Unknown	Waypoint
064	063	User Waypoint	S7 32.821 E110 49.981		Symbol & Name	Unknown	Waypoint
065	064	User Waypoint	S7 32.798 E110 50.005		Symbol & Name	Unknown	Waypoint
066	065	User Waypoint	S7 32.746 E110 50.107		Symbol & Name	Unknown	Waypoint
067	066	User Waypoint	S7 32.756 E110 50.179		Symbol & Name	Unknown	Waypoint
068	067	User Waypoint	S7 32.789 E110 50.187		Symbol & Name	Unknown	Waypoint
069	068	User Waypoint	S7 32.805 E110 50.192		Symbol & Name	Unknown	Waypoint
070	069	User Waypoint	S7 32.822 E110 50.195		Symbol & Name	Unknown	Waypoint
071	070	User Waypoint	S7 32.861 E110 50.199		Symbol & Name	Unknown	Waypoint
072	071	User Waypoint	S7 48.871 E110 19.542	1172 ft	Symbol & Name	Black	Man Overboard

Header Name Length Course Waypoints Link

Route 062 to 071 0.5 mi 90° true 10 waypoints

Header Waypoint Name Distance Leg Length Course

Log file hasil on location

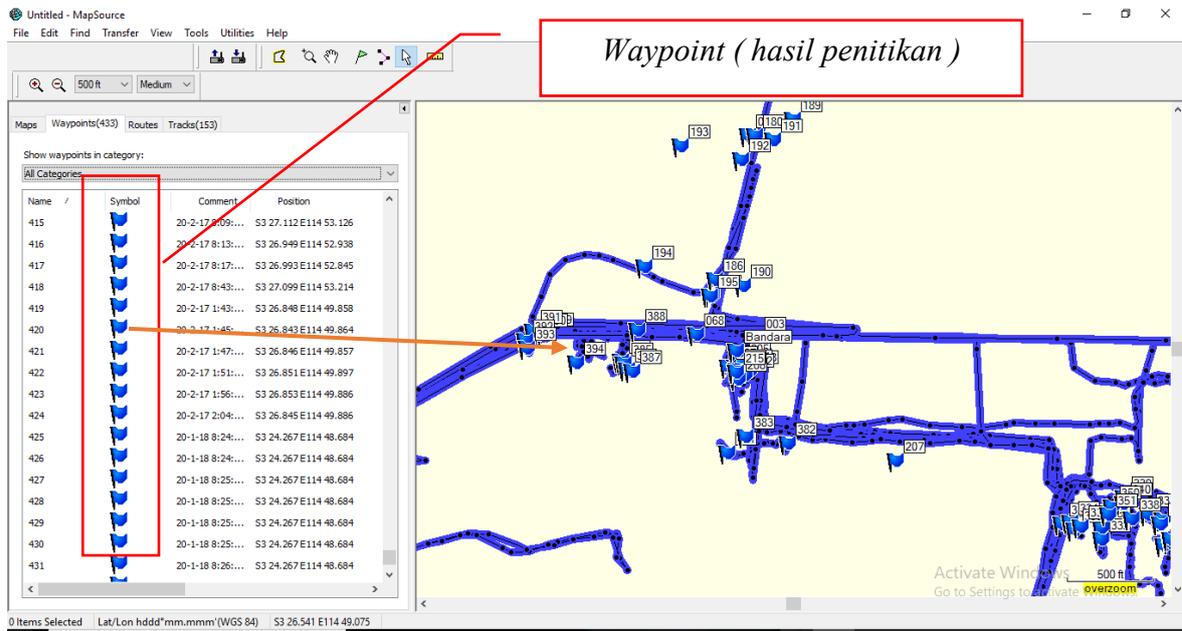
Log file hasil Fake location

Activate Windows
Go to Settings to activate Windows.

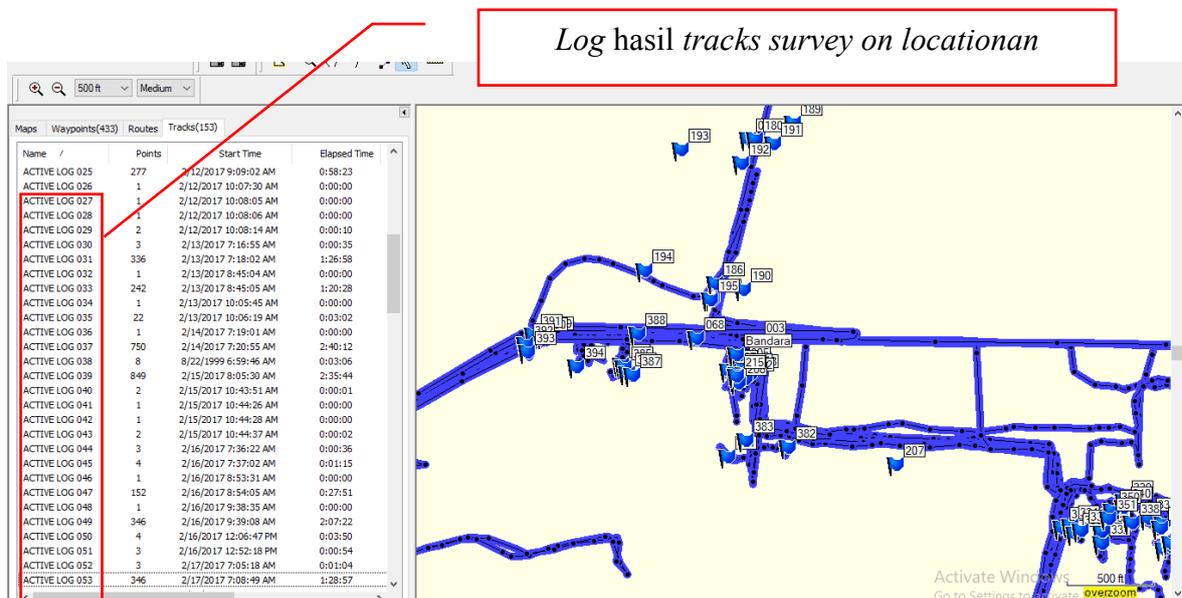
Gambar 4.12 Identifikasi data yang berbeda pada log file waypoint

Dari capture gambar 4.12 data terlihat perbedaan pada isi attribute. Perbedaan yang dimaksud adalah pada jenis data.

Sedangkan yang berikut adalah hasil data yang telah diakuisisi dari GPS Map Garmin 76 CSx dengan menggunakan menggunakan *Tool MapSource*.

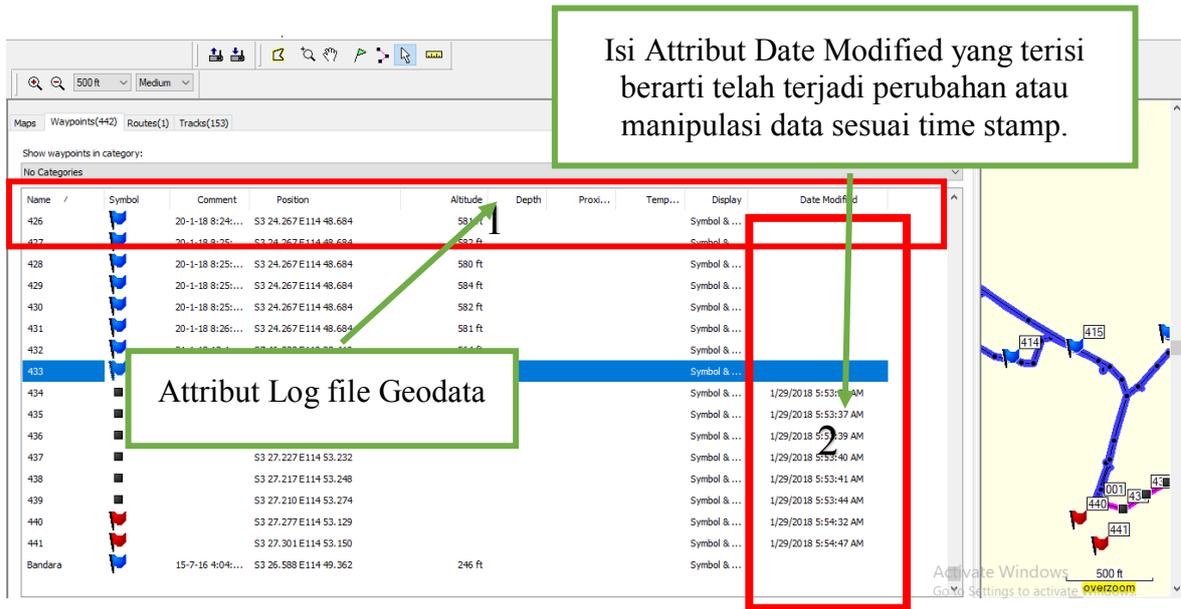


Gambar 4.13 Waypoint Hasil Akuisisi dari GPS Map



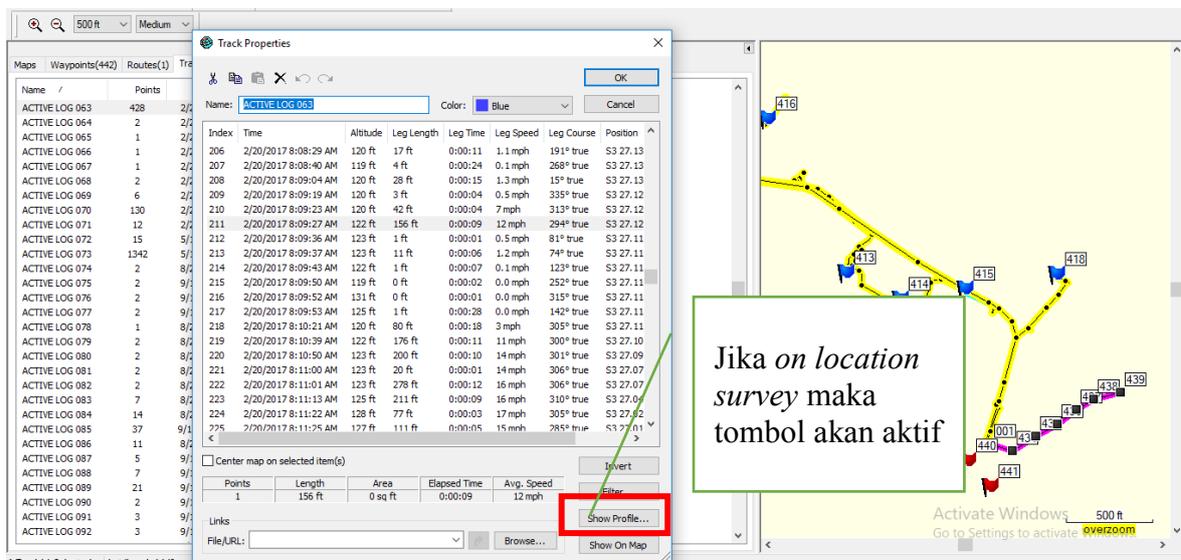
Gambar 4.14 Tracks Hasil Akuisisi data dari GPS Map

Gambar 4.13 menunjukkan hasil *Waypoint* sedangkan Gambar 4.14 menunjukkan hasil *Tracks* yang dilakukan oleh surveyor ke lokasi survey. Ada dua jenis data yang terlihat pada gambar tersebut, yaitu data tabular dan spasial.



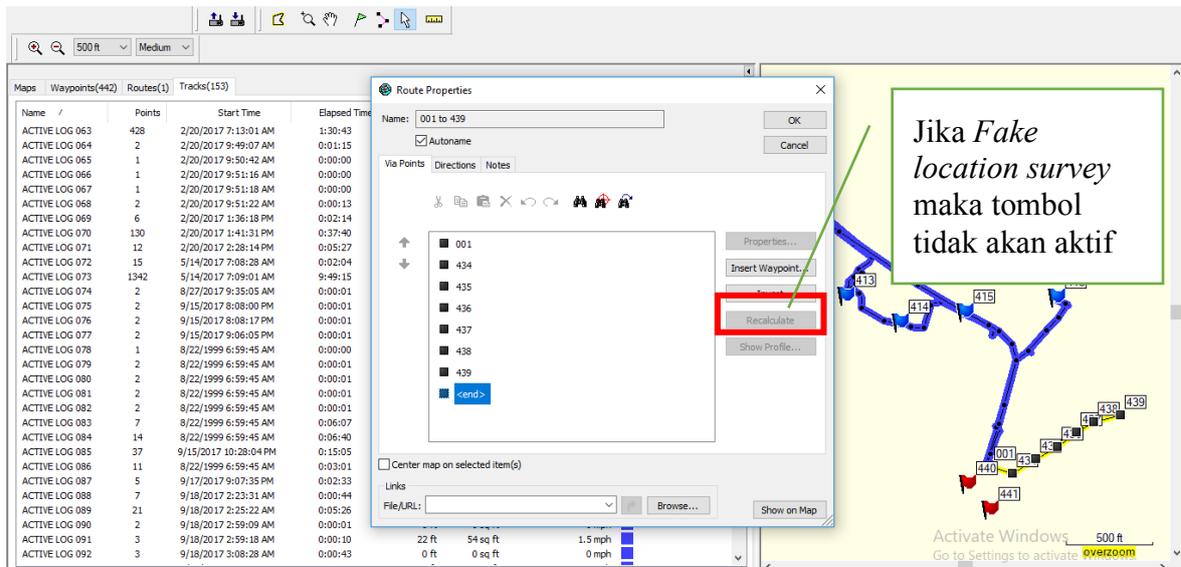
Gambar 4.15 Hasil Akusisi data *Survey* lokasi dari GPS.

Gambar 4.15 menunjukkan tampilan *properties Tracks* dan *waypoint*. **Kotak merah 1** adalah atribut dari *trakcs* dan *waypoint*, sedangkan pada “Kotak Merah 2” pada attribute “*Date Modified*” terdapat rekod yang terisi *time stamp* yang menunjukkan bahwa pada rekod tersebut telah terjadi perubahan isi. Jadi disimpulkan rekod hasil *survey* tersebut tidak valid.



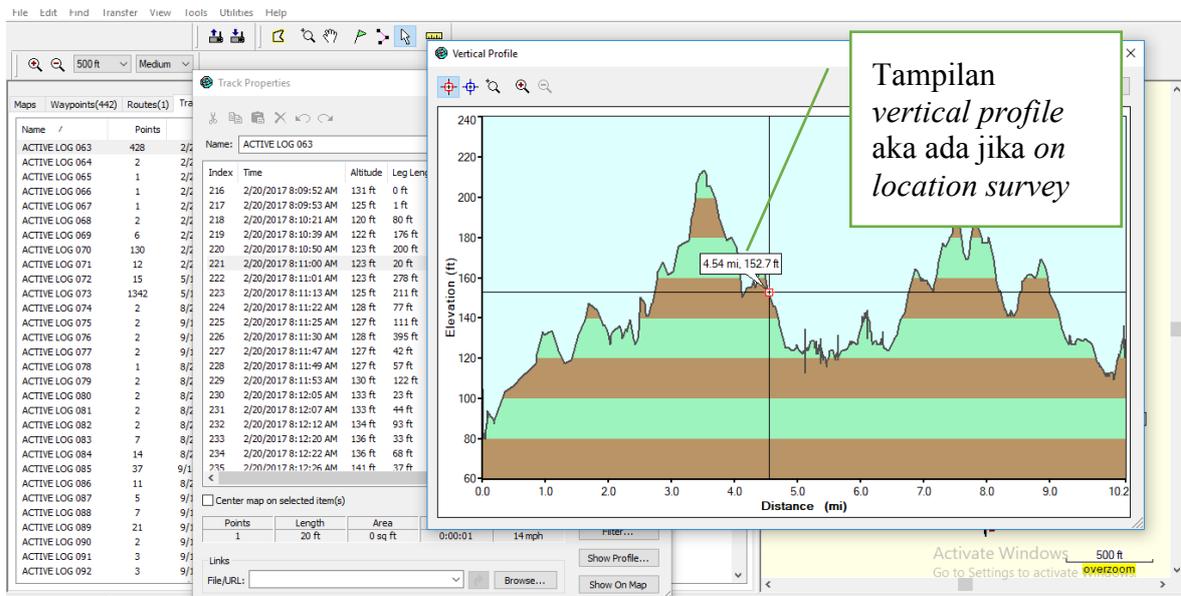
Gambar 4.16 Tampilan *Tracks Properties* dari data hasil kelokasi *survey*.

Pada gambar 4.16 teridentifikasi pada *Tracks Properties* akan aktif jika survey benar dilakukan sesuai Lokasi (*On Location*).



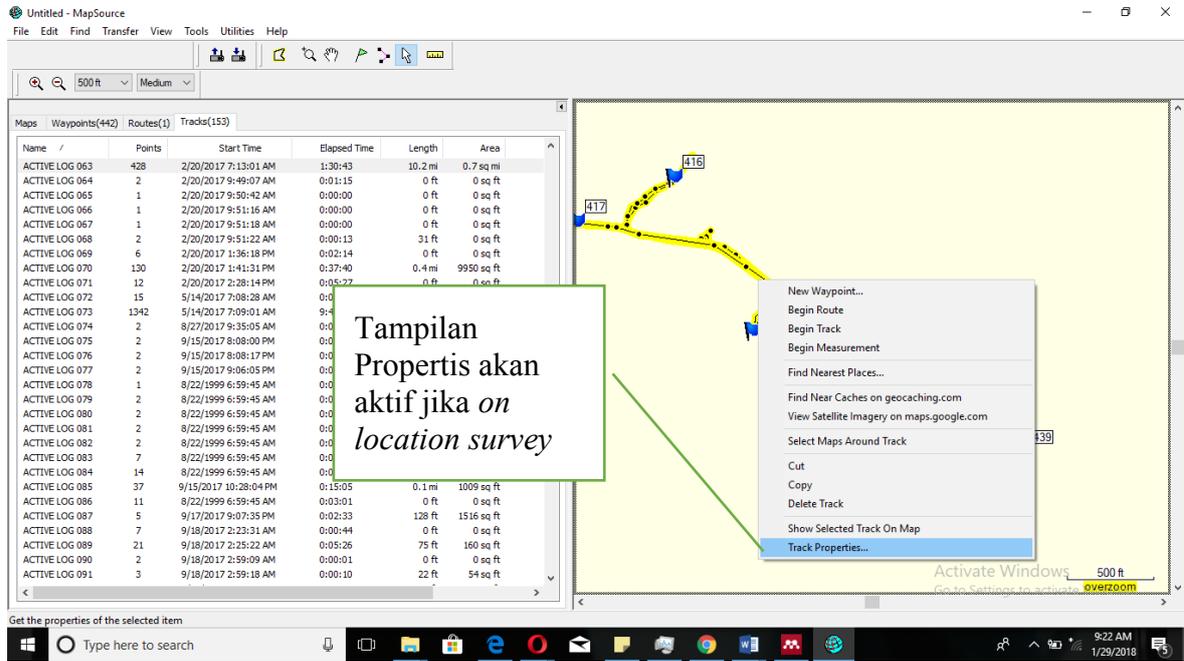
Gambar 4.17 Tampilan hasil *Tracks* dan *Waypoint* yang tidak ke lokasi survey.

Gambar 4.16 dan 4.17 jelas menunjukkan perbedaan tampilan properties *Tracks* dan *waypoint* yang *On Location* dan *Fake Location*. Dimana tombol *Show Profile* aktif jika survey dilakukan ke lapangan dan sebaliknya tidak aktif.



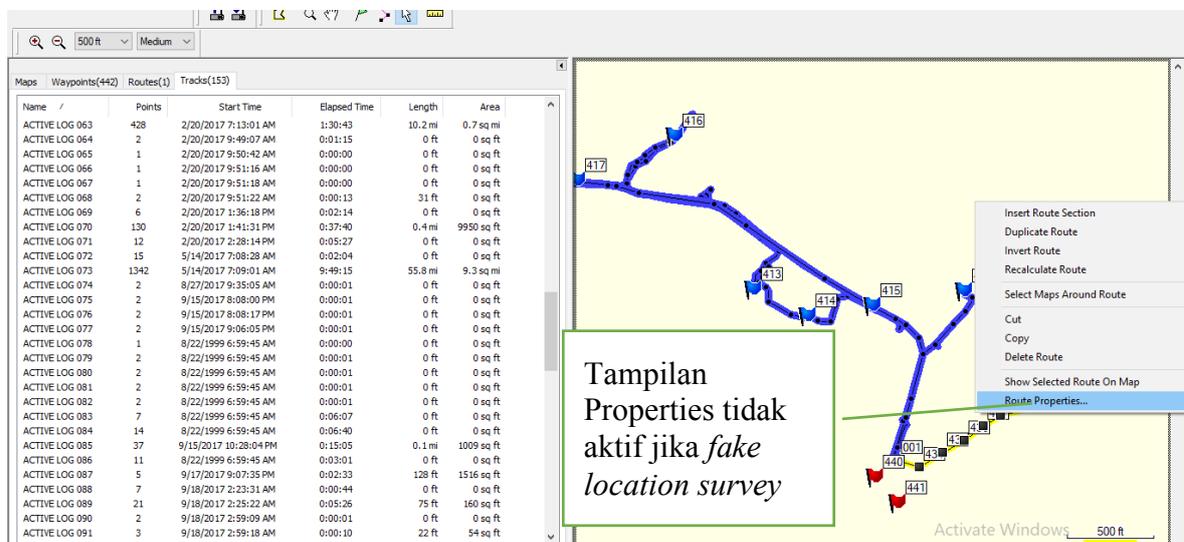
Gambar 4.18 Tampilan *vertical Profile*

Gambar 4.18 menunjukkan bahwa data yang dihasilkan dari survey ke lokasi jika di proyeksikan secara vertical akan nampakm elevasi disertai *hair cross* yang jika digerakan akan mengikuti alur tepi dari *vertical profile*



Gambar 4.19 Menampilkan Properties dari bagian *Tracks On Location*

Pada Gambar 4.19 menunjukan bahwa sebuah obyek jika kita pilih, kemudian dilihat propertiesnya dengan melakukan *Right Klik* mouse maka menu *Tracks On Location* akan *enable*.



Gambar 4.20 Menampilkan Properties dari bagian *Tracks Fake Location*

Pada Gambar 4.20 menunjukkan bahwa sebuah obyek jika kita pilih, kemudian dilihat propertiesnya dengan melakukan *Right Klik* mouse maka menu *Tracks On Location* akan *Disable*.

Dari data data yang ditampilkan dalam bentuk *capture* diatas maka dapat di simpulkan perbandingan antara data *On location Survey* dengan *Fake Location Survey* seperti terlihat pada tabel dibawah ini.

- **Analisis**, dari beberapa data dan gambar yang telah di *examination* terdapat beberapa temuan yang menunjukkan perbedaan data dan proses. Perbedaan tersebut menunjukkan bahwa jika survey dilakukan secara *on location* maka akan menghasilkan data dan proses seperti sudah diuraikan pada tahap *examination*. Demikian juga jika survey dilakukan secara *Fake Location*, maka hasilnya akan berbeda dengan jika dilakukan secara *on location*.
- **Reporting**, dari pemeriksaan dan analisa terhadap hasil survey maka dapat di sampaikan laporan sebagai berikut ,

Tabel 4.5 Laporan hasil identifikasi

No	Attribut	On Location	Fake
1	Date Modified	Tidak Ada	Ada
2	Show Profile	Aktif	Tidak Aktif
3	Vertical Profile	Ada	Tidak Ada
4	Properties	<i>Tracks Properties</i>	<i>Route Properties</i>
5	Pada perbedaan pada type data	Sesuai dengan type data yang ada	Text semua

Tabel 4.6 Hasil Identifikasi Perbandingan attribut Data survey *On Location* dan *Fake Location*

No	Attribut	On Location	Fake
1	Date Modified	Tidak Ada	Ada
2	Show Profile	Aktif	Tidak Aktif
3	Vertical Profile	Ada	Tidak Ada
4	Properties	Tracks Properties	Route Properties

4.4 Analisa Terhadap Hasil Uji Coba

Masalah penelitian yang penulis usulkan dan yang dibahas adalah tentang bagaimana menekan dan mendeteksi ancaman risiko dan kerentanan sistem yang berpengaruh terhadap hasil akurasi peta digital, dengan menganalisa proses dan data hasil survey. Dari beberapa uraian yang telah dibahas dan uji coba dan pengujian yang telah dilakukan menggunakan standart matrik pada tahapan *Framework NIST*. Tahapan ini terbagi menjadi 4 (empat) bagian dimana tahap identifikasi terhadap ancaman risiko berada pada tahap 1-4. Sedangkan tahap 5-7 adalah penentuan dari kerentanan akibat adanya ancaman risiko tersebut. Pada tahap tahap ini juga ditentukan bobot dampak risiko yang mengancam hasil dari pencetakan kualitas peta digital. Tahap 8 adalah rekomendasi dari hasil dari pelaksanaan tahap 1-7 dan tahap 9 adalah tahap pendokumentasian hasil.

Penerapan *Framework NIST SP 800-30* dalam penanganan proses sistem pembuatan peta digital terbukti mampu mengidentifikasi ancaman risiko dan mengidentifikasi kerentanan yang terjadi. Kesimpulan itu di kemukakan setelah dilakukan uji coba penerapan *Risk Assesment* dari *Framework NIST SP 800-30* yang dilakukan tahap demi tahap dan menghasilkan fakta fakta adanya ancaman risiko dimana uraiannya telah dibahas di tahap 1 – 4, hasil dari pembahasan tersebut telah menjawab rumusan masalah yang ada yaitu “Bagaimana detail identifikasi ancaman dan kerentanan pada geodata“. Selain itu juga uraian bahasan pada tahap 5 – 7 telah menjawab rumusan masalah tentang “Bagaimana detail identifikasi ancaman dan kerentanan pada geodata”.

Apa yang telah dilakukan dalam tahapan tahapan tersebut merupakan sebuah implementasi kerja untuk mendeteksi dan mengidentifikasi ancaman risiko dan kerentanan yang akan menjadi celah kelemahan sistim informasi dan bagaimana cara mengatasinya. Mengacu pada peneilitan sebelum yang terlihat pada *literature review* bahwa *Framework* telah terbukti membantu dalam mengatasi masalah masalah sitem informasi sesuai dengan kontek *Framework* dan masalahnya. Seperti beberapa penelitian yang dilakukan dan terangkum dalam *literature review* yang dapat disimpulkan bahwa dengan adanya *Framework* dapat mengurangi ancaman risiko dan kerentanan, memudahkan dalam mendeteksi kelemahan sistem, mendapatkan solusi atas kelemahan dan kerentanan tersebut.

BAB 5

Kesimpulan Dan Saran

5.1 Kesimpulan

Dengan menggunakan *Framework NIST Special Publication 800 - 30* dalam menilai step step pembuatan peta digital sesuai 9 step, maka dapat disimpulkan sebagai berikut :

1. *Framework NIST* terbukti mampu menguraikan profil ancaman risiko yang berpotensi dan sudah mengganggu pelaksanaan sistem pembuatan dan pencetakan peta digital.
2. Selain deskripsi tersebut, *Framework NIST SP 800-30* juga memberi mitigasi risiko sebagai solusi tindakan peringanan risiko dan pengawasannya dengan mengevaluasi pelaksanaan manajemen risiko secara menyeluruh.
3. Dengan di terapkannya *Framework NIST* maka dapat disimpulkan juga bahwa step step yang sudah dibuat dapat dijadikan profile dalam rangka menilai kegiatan pembuatan peta digital, dimana ancaman risiko dan kerentanan mudah teridentifikasi karena sudah ada pola dari profile yang di bangun ini.

5.2 Saran

Dari hasil kesimpulan yang telah dikemukakan maka disarankan perlu adanya bagian kusus yang mendokumentasikan ada ancaman ancaman yang telah terjadi, serta memberikan catatan catatan yang mungkin akan berpotensi menjadi ancaman. Pemahaman tentang pengetahuan terhadap teknis pekerjaan dan prosedur kerja sebaiknya di miliki oleh karyawan, sehingga dapat membedakan mana yang akan menjadi ancaman, mana yang bukan.

Karena teknologi informasi informasi selalu berkembang, maka diharapkan adanya pengujian pengujian yang dilakukan secara berkala, mengingat ancaman reko dan kerentanan dalam teknologi informasi juga pasti berkembang ke bentuk ancaman yang baru.

Daftar Pustaka

- Budi, R. (2016). Sekilas Mengenai Forensik Digital. *Jurnal Sositologi, Edisi 29*, 2–3. Retrieved from http://budi.insanmusic.com/files/digital_forensik_fsrj_journal.pdf
- Daryono, B. S. (2017). Pengembangan Pelaporan *Framework* Cyber Crime. *JISKA, Vol 1 No.*, 133–147. Retrieved from https://www.researchgate.net/publication/316510836_PENGEMBANGAN_FRAMEWORK_PELAPORAN_CYBER_CRIMEFRAMEWORK_PELAPORAN_CYBER_CRIME
- Fabian Bustamante, Walter Fuertes, Paul Diaz, T. T. (2017). Methodology for Management of Information Security in Industrial Control Systems: A Proof of Concept aligned with EnterpriseObjectives. *Advances in Science, Technology and Engineering Systems Journal, Vol. 2, No*, 88–99. Retrieved from https://www.researchgate.net/publication/317138094_Methodology_for_Management_of_Information_Security_in_Industrial_Control_Systems_A_Proof_of_Concept_aligned_with_Enterprise_Objectives
- Guntur Bagus Pamungkas, Bambang Sudarsono, S. K. (2014). Verifikasi Batas Wilayah Antara Kabupaten Sukoharjo Dan Kabupaten Karang Anyar. *Jurnal Geodesi Undip, Volume 3*,(Permasalahan Batas Daerah), 14–24.
- Ibnu, Z. (2013). Rancang Bangun Pelacak Lokasi Dengan Teknologi GPS. *Teknomatika, Vol. 3 No.*(Pelacakan Lokasi Kejahatan dengan GPS).
- J Kiyoshi. (2013). Investigating the Impact of Global Positioning System Evidence.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. Retrieved from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>
- Kramer, J. (2013). *No DroidSpotter: A forensic tool for Android location data collection and analysis*. IOWA State Univercyti.
- Last David. (2014). GPS Forensics, Crime and Jamming, (GPSJamming).
- Lestari, U., & Kristiyana, S. (2013). Rancang Bangun Mobile Tracking Application Module Untuk Pencarian Posisi Benda Bergerak Berbasis Short Message Service (Sms). *Seminar Nasional Teknologi Informasi Dan Komputasi (SENASTIK 2013)*, 30–31.
- Mohamed Ghazouani, Sophia Faris, Hicham Medromi, A. S. (n.d.). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk.

- International Journal of Computer Applications, Volume 103*(Security risk assessment, risk management system, *Framework*, audit, information system), 975 – 8887. Retrieved from <https://pdfs.semanticscholar.org/1c40/467699b011318a49d21191c272228b94dc1d.pdf>
- Nurdiati Sri, Barus Baba, P. D. (2015). Pengembangan Sistem Informasi Geografis Tindak Kejahatan Multilevel berbasis Web. Retrieved from <http://download.portalgaruda.org/article.php?article=85662&val=235>
- Prahasta, E. (2004). *Sistem Informasi Geografis, Konsep – Konsep Dasar*. (E. Prhasta, Ed.) (Ke 2). Bandung: Informatika Bandung.
- Prahasta, E. (2009). *Sistem Informasi Geografis Konsep-Konsep Dasar* (Cetakan Pe). Bandung: Informatika.
- Prayudi Yudi, S. S. (2014). Analisis Bukti Digital Global Positioning System (GPS) Pada Smartphone Android. *Konferensi Nasional Sistem Dan Informatika (KNS&I) 2014*, (bukti digital GPS).
- Purbo Onno W. (2017). *Framework Cybersecurity*. Retrieved January 13, 2018, from http://lms.onnocenter.or.id/wiki/index.php/Framework_Cybersecurity
- Rini Fathoni Lestari. (2014). *Global Navigation Satellite System DPJ P203*. Yogyakarta.
- Riyanto, Prilnali EP, H. I. (2009). *Pengembangan Aplikasi Sistem informasi Geografis* (Pertama). Yogyakarta: Gava Media.
- Sendow, T. K., Longdong, J., Jurusan, D., Fakultas, S., Universitas, T., & Ratulangi, S. (2012). Studi pemetaan peta kota, 2(1).
- Stoneburner Gary , Goguen Alice, and F. A. (2002). Risk Management Guide for Information Technology Systems. *Cumputer Security*, (Reports on Computer System Technology). Retrieved from <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf>
- Ucu Nugraha. (2016). Manajemen Risiko Sistem Informasi Pada Perguruan Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-300. *Seminar Nasional Telekomunikasi Dan Informatika (SELISIK 2016)*, 2503–2844.
- Widyantara, I. M. O., Agus, I. G., & Warmayana, K. (2015). Penerapan Teknologi GPS Tracker Untuk Identifikasi Kondisi Traffik Jalan Raya, 14(1), 31–35.