DATA ANALYSIS

Analisis sistem (system analysis) dapat didefinisikan sebagai berikut: Penguraian dari suatu system informasi yang utuh kedalam bagian-bagian komponennya dengan maksud mengidentifikasikan dan mengevaluasi permasalahan-permasalahannya, kesempatan kesempatan, hambatan - hambatan yang terjadi dan kebutuhan - kebutuhan yang diharapkan sehingga dapat di usulkan perbaikan - perbaikannya. Atau secara lebih mudahnya, analisis system adalah penelitian atas sistem yang telah ada dengan tujuan untuk merancang sistem yang baru atau diperbarui. Tahapan alisis system ini merupakan tahap yang sangat kritis dan sangat penting, karena kesalahan didalam tahap ini akan menyebabkan juga kesalahan ditahap selanjutnya. Tugas utama analisis system dalam tahap ini adalah menemukan kelemahan-kelemahan dari sistem yang berjalan sehingga dapat diusulkan perbaikannya.

Analisis dapat dilakukan dengan menggunakan pendekatan sejumlah metode. Untuk memberikan kesimpulan yang berkualitas harus didasarkan pada ketersediaan sejumlah data atau bahkan sebaliknya, Dengan menyimpul kan bahwa “tidak ada kesimpulan”. Hal tersebut sangat dimungkinankan. Tugas analisis ini mencakup berbagaik egiatan, sepertiidentifikasi user atau orang di luarpengguna yang terlibat secara tidak langsung, lokasi, perangkat, kejadiaan, dan mempertimbangkan bagaimana semua komponen tersebut saling terhubung hingga mendapat kesimpulan akhir.

Berikut yang perlu diperhatikan untuk menganalisis data :

1. Teliti analisis data yang diperoleh untuk menarik kesimpulan terkait kasus ini
2. Teknik analisis data bergantung pada cakupan kasus atau kebutuhan klien
3. Fase ini meliputi:
    a) Analisis isi file, tanggal dan waktu pembuatan file dan modifikasi, pengguna yang terkait dengan pembuatan file, akses, dan modifikasi file, dan lokasi penyimpanan fisik file.
    b) Generasi timeline.
4. Mengidentifikasi dan mengkategorikan data sesuai relevansinya

AlatAnalisis Data

1. Alat forensik membantu dalam menyortir dan menganalisis sejumlah besar data untuk menarik kesimpulan yang berarti.

2. Contohdarialatanalisis data:

- Data Akses FTK
- Guidance Software's En Case
- Brian Carrier's Sleuth Kit

Yang perlu dilakukan setelah mengumpulkan bukti digital :

a) -Bukti digital harus dinilai secara menyeluruh sehubungan dengan ruang lingkup. Kasus untuk menentukan jalannya tindakan
b) Lakukan penilaian menyeluruh dengan meninjau ulang surat perintah penggeledahan atau yang lainnya. Otorisasi, detail kasus, sifat perangkat keras dan perangkat lunak, potensial bukti yang dicari, dan keadaan seputar akuisisi bukti untuk diperiksa

Penilai kasus

a) tinjau permintaan penyidik kasus untuk layanan
b) Identifikasi otoritas hukum untuk permintaan pemeriksaan forensik
c) Dokumentasikan rantai hak asuh
d) Diskusikan apakah proses forensik lain perlu dilakukanpada bukti (misalnya, analisis DNA, sidik jari, tanda alat, jejak, dan dokumen yang dipertanyakan)

Penilaian Kasus (lanjutan)

a) Diskusikan kemungkinan untuk mengejar jalan investigasi lain untuk mendapatkan tambahanbukti digital (misalnya, mengirim pesanan pelestarian ke penyedia layanan Internet(ISP), mengidentifikasi lokasi penyimpanan jauh, mendapatkan email)
b) Pertimbangkan relevansi komponen perifer untuk penyelidikan; misalnya dipemalsuan atau kasus penipuan, pertimbangkan peralatan non-komputer seperti laminators, creditkartu kosong, kertas cek, scanner, dan printer (Dalam kasus pornografi anak,pertimbangkan kamera digital)
c) Tentukan bukti potensial yang dicari (mis., foto, spreadsheet,dokumen, database, dan catatan keuangan)
d) Tentukan informasi tambahan mengenai kasus ini (mis., alias, akun email,alamat email, ISP yang digunakan, nama, konfigurasi jaringan dan pengguna, log sistem,kata

sandi, nama pengguna) yang dapat diperoleh melalui wawancara dengan sistemadministrator, pengguna, dan karyawan

Pengolahan penilaian lokasi

a) Menilai bukti untuk menentukan di mana melakukan pemeriksaan
b) Lebih baik menyelesaikan pemeriksaan di lingkungan yang terkendali, seperti area kerja forensik khusus atau laboratorium
c) Kapan pun keadaan memerlukan pemeriksaan di tempat yang akan dilakukan, mencoba mengendalikan lingkungan

Penilaian Kasus (lanjutan)

1. Pertimbangan penilaianmeliputi:
   a) Waktu yang dibutuhkan di tempat untuk mencapainya bukti pemulihan
   b) Masalah logistik dan personil terkait dengan penyebaran jangka panjang
   c) Dampaknya terhadap bisnis karena panjangnya pencarian
   d) Kesesuaian peralatan, sumber daya, media, pelatihan, dan pengalaman untuk penukaran pemeriksaan.

Praktik terbaik

1. Analisis bukti fisik dan logis untuk nilai mereka terhadap kasus ini
2. Gunakan lemari yang aman untuk mengamankan buktinya
3. Periksa log layanan jaringan untuk setiap peristiwa yang diminati
4. Periksa sejumlah besar data host, di mana hanya sebagian data yang mungkin relevan dengan kejadian tersebut
5. Lakukan analisis offline pada salinan sedikit bukti asli
6. Cari isi semua file yang dikumpulkan untuk membantu mengidentifikasi file -yang mungkin menarik
7. Tinjau perangko waktu dan tanggal dalam metadata sistem file
8. Berkorelasi header file ke ekstensi file yang sesuai untuk mengidentifikasi ketidakcocokan
9. Tinjau kembali nama file untuk relevansi dan pola