Kuliah Umum

Digital Forensics

Nama : Muhamad Ilham Fauzan

NIM : 121103004

Prodi : Teknik Informatika

**Pengertian Digital Forensics**

Digital Forensics adalah pencarian barang bukti digital, untuk dikumpulkan, dianalisa dan dijadikan barang bukti untuk persidangan. Selain itu juga digunakan untuk memperbaiki keamanan. Siapapu Sekaran dapat melakukannya, tapi saat dibawa ke pengadilan harus mempunyai sertifikasi digital forensics.

Latar belakang adanya digital forensic adalah karena informasi dapat disimpan dan diakses di mana saja, informasi saat ini mudah sekali didapatkan. Maka dari itu muncul ancaman terhadap informasi tersebut. Jika kebocoran inforamsi berhasil didapatkan dan disebarluaskan maka pihak yang informasinya bocor akan mengalami kerugian baik secara langsung maupun tidak langsung. Digital forensics sanat penting agar sehingga dapat dilakukannya analisa atau investigasi terhadap kriminal yang terjadi, membawanya ke ranah hukum sebagai barang bukti yang keabsahannya dapat dipertanggung jawabkan, melindungi data menjadi lebih baik lagi, dan memulihkan data yang sempat hilang.

**CIA Triad**

CIA triad adalah konsep keamanan informasi yang terdiri dari tiga aspek utama: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan). Konsep ini bertujuan untuk melindungi informasi secara komprehensif.

* Confidentiality (Kerahasiaan): Kerahasiaan mengacu pada perlindungan informasi agar hanya dapat diakses oleh pihak yang berwenang. Tujuannya adalah untuk mencegah akses oleh pihak yang tidak berhak atau tidak sah. Dalam menjaga kerahasiaan, metode seperti enkripsi data, pengaturan izin akses, dan kebijakan keamanan yang ketat dapat diterapkan.
* Integrity (Integritas): Integritas berarti memastikan bahwa informasi tetap utuh, tidak diubah, dan tidak rusak. Integritas melibatkan melindungi informasi dari perubahan yang tidak sah, manipulasi, atau kerusakan yang dapat mengancam keandalannya. Penggunaan tanda tangan digital, mekanisme checksum, dan kontrol versi adalah contoh metode yang digunakan untuk menjaga integritas data.
* Availability (Ketersediaan): Ketersediaan berfokus pada memastikan bahwa informasi selalu tersedia dan dapat diakses oleh pihak yang berwenang saat dibutuhkan. Hal ini mencakup melindungi informasi dari gangguan, serangan, kegagalan perangkat keras, atau bencana alam yang dapat mengganggu akses terhadap data. Upaya pemulihan bencana, redundansi sistem, dan pemeliharaan rutin adalah contoh cara menjaga ketersediaan informasi.

**Tru Threat**

Tru Threat atau ancaman dapat muncul dari beberapa sumber, termasuk "bad guy" (pelaku jahat), "bad code" (kode yang buruk), "insider" (pihak internal), dan "human error" (kesalahan manusia).

1. Bad Guy (Pelaku Jahat): Ancaman dari "bad guy" mengacu pada serangan yang dilakukan oleh individu atau kelompok yang memiliki niat jahat. Ini termasuk hacker, penjahat siber, atau kelompok yang bertujuan untuk mencuri informasi sensitif, merusak sistem, atau merugikan entitas lain secara digital. Serangan ini bisa berupa serangan siber seperti peretasan, serangan phishing, serangan DDoS, dan lain sebagainya.
2. Bad Code (Kode yang Buruk): Ancaman dari "bad code" terkait dengan kelemahan atau celah dalam perangkat lunak yang dapat dimanfaatkan oleh penyerang. Kode yang buruk dapat mencakup kerentanan dalam aplikasi atau sistem operasi yang memungkinkan penyerang untuk memanipulasi atau mengambil alih kontrol sistem. Ini dapat melibatkan serangan melalui malware, virus, worm, atau exploit yang mengeksploitasi kelemahan dalam perangkat lunak.
3. Insider (Pihak Internal): Ancaman dari "insider" adalah ancaman yang berasal dari orang dalam organisasi atau entitas yang memiliki akses dan pengetahuan yang sah terhadap sistem dan data. Pihak internal ini dapat mencakup karyawan, kontraktor, atau mitra bisnis yang memiliki niat jahat atau melakukan tindakan yang tidak sah, seperti pencurian data, pencurian kekayaan intelektual, atau penyalahgunaan hak akses.
4. Human Error (Kesalahan Manusia): Ancaman dari "human error" adalah kesalahan yang dilakukan oleh manusia yang dapat menyebabkan kerentanan atau kebocoran informasi. Kesalahan manusia bisa terjadi dalam berbagai bentuk, seperti pengguna yang tidak sengaja mengirim data rahasia ke pihak yang tidak berwenang, mengabaikan praktik keamanan yang baik, atau secara tidak sengaja merusak atau menghapus data penting.

Alasan seseorang melakukan tindakan jahat atau merugikan dalam konteks keamanan informasi dapat bervariasi tergantung pada situasi dan motif individu. Beberapa alasan umum mengapa seseorang mungkin melakukan hal tersebut adalah :

1. Keuntungan Finansial: Motif finansial adalah salah satu yang paling umum. Seseorang mungkin mencoba mencuri informasi pribadi, data keuangan, atau kekayaan intelektual untuk mendapatkan keuntungan finansial secara ilegal.
2. Ambisi dan Keuntungan Kompetitif: Beberapa individu atau organisasi mungkin melakukan serangan atau kegiatan jahat untuk mendapatkan keuntungan kompetitif dalam bisnis atau industri tertentu.
3. Tujuan Ideologis atau Politis: Ada kasus di mana individu atau kelompok menggunakan serangan siber atau aktivitas jahat dalam upaya untuk mempromosikan agenda ideologis atau politis.
4. Tekanan atau Kebutuhan: Ada situasi di mana seseorang mungkin terlibat dalam tindakan yang merugikan karena tekanan ekonomi, tekanan sosial, atau kebutuhan mendesak.

Objek-objek yang bisa dijadikan bahan atau sumber digital forensics, antara lain:

* Email
* Photos
* Files System
* Memory
* Network
* Documents
* External Storage
* USB
* Browser
* Mobile Deivces

Terminologi/key terms yang sering digunakan dalam digital forensics:

* Forensic clone
* Image file
* Golden Image
* Working copy
* Write blocker
* Data blocker
* Data recovery
* Hash
* File integrity
* File signature
* Chain of custody

Langkah-langkah untuk melakukan digital forensics:

Identification → Preservation → Acquisition → Analysis → Interpretation → Documentation & Report

**Live Forensics**

Live forensics, juga dikenal sebagai forensik langsung atau forensik pada sistem yang sedang berjalan, adalah pendekatan dalam forensik digital di mana penyelidik mengumpulkan bukti dan menganalisis data dari sistem yang sedang aktif atau "hidup". Berbeda dengan forensik tradisional yang dilakukan pada bukti yang tidak aktif, live forensics memungkinkan penyelidik untuk memeriksa dan memperoleh informasi dari sistem yang masih beroperasi.

Key Consideration

* Volatility
* Non-intrusivemess
* Remote acquisition
* Memory acquisition
* Network traffic analysis
* Live data analysis (logs, file system)
* Running processes