Ada 3 konsep informasi sistem

CIA triad

1. confidentility = kerahasiaan

2. Intergriti = keutuhan datanya.

3. Availability = akses tidak bisa diakses, sangat terjaga

Datang dari mana?

Bad guy, bad code, insider, human eror.

Ngapain mereka tindak kejahatan

* Mencuri uang
* Menjual data
* Ransomeware (exort)
* Mischief (iseng)

Dari mana saja?

* Phising
* Password cracker
* Malware

Barang digital rawan perubahan, karna barang bukti bisa diedit. Sehingga ada teknik tertentu yang dilakukan oleh digital forensik.

Digital forensik (komputer forensik, siber forensik)

Proses pengumpulan data, kemudian dianalisa dan disiapkan untuk barang bukti untuk persidangan.

DF digunakan juga untuk peningkatan sistem security mereka.

Siapa yang melakukan?

Diperusahaan, profesional, law enforcement agency.

Yang dianalisa / object DF

Email, foto, fike sistem, memory, network, document, external storage, usb flash drive, browser, mobile device, all digital things.

Key terms

* Porensice clone/ bitstream image

Mengkopy sama persis semua file2 yang ada di flashdisk/storage

* Image file

Hasil dari clone forensice clone

* Golden image

Kumpulan file dari clone

* Working kopy

File dari golden image

* Write blocker

Menjaga agar tidak terjadi perubahan terhadap data

* Data recovery

Merecovery data yang sudah dihapus

* Hash

Karakter unik dari setiap file

* File integritiy

extension

* File signature

Mengetahui extension sebenarnya dari file

* Chain of custody

Riwayat pengakses dari file2 yang ada

Tahapan digital forensik

* Identifikasi

Mengetahui kasus apa yg ditangani, mengetahui tools apa saja yang dipakai

* Preservation

Melakukan penanganan pada tkp tersebut

* Aquisition

Mengecek apliaksi apa saja yang ada dimemory

* Analysa
* Interprestation

Membuat jalan cerita apa yang terjadi

* Documentary

Bagaimana cara membuat live forensik?

Merupakan live respon terhadap prose pengumpulan data analisa fari apk yang sedang running.

Kapan dilakukan?

* Dilakukan pada saat inversitasi pada sistem yang kiritikal(yng tidak boleh down time)
* Melaukan malware analysis. Malware sedang berjalan di ram saja
* Performan investigasi

Object apa saja?

Memory, running service

Network conect

Sistem network log

Yang perlu diperhatikan pada live forensik

* Volatility
* Non instruksif

Harus hati2

* Remote acqusition
* Memory axqusition
* Network traffic analysis
* Live data analysis
* Running analysis

Step by step live

* Plainning

Mempersiapkan apa saja yg disiapkan

* Preparation

Menyiapkan workstation, network,

* documentation
* voletail data collection
* memory aquisiton
* network
* live data analysis
* documentation and reposting
* legal comdentation
* post investigation steps

tools digital forensik

* the sleuth kit
* autopsy
* FTK imager
* OSForensik
* HEX editor
* wireshark