Digital Forensics : Digital Evidence in Criminal Investigation #1
Rabu, 1 Februari 2017 | 03:37:50 WIB **| Endang Kurniawan**

Barang bukti menjadi salah satu kalimat yang amat penting dalam mengungkap suatu kejadian atau peristiwa. Dalam peristiwa tindak kejahatan, barang bukti merupakan bagian penting dalam menjerat pelaku kejahatan. Para penyidik dapat mengungkap tindak kejahatan dengan kronologis yang lengkap, dan mencari pelaku tindak kejahatan dan membawanya ke pengadilan.

Dalam dunia forensik komputer, barang bukti digital atau biasa di sebut digital evidence digunakan para forensic analyst mengungkap kasus-kasus kejahatan komputer. Oleh karena posisi barang bukti ini sangat strategis, investigator dan forensic analyst harus bisa memahami jenis-jenis barang bukti yang dapat digunakan untuk menjerat pelaku kejahatan.

Barang bukti digital (digital evidence) didapatkan di TKP (tempat kejadian perkara) tindak kejahatan kemudian di analisa lebih lanjut, apakah bisa dijadikan barang bukti atau tidak. Karena tidak semua hasil temuan di TKP dapat dijadikan barang bukti, sebagaimana telah dijelaskan dalam penjelasan dalam digital forensic mengenai kriteria yang harus dipenuhi untuk bisa dijadikan barang bukti (*Rules of evidence*).

Barang bukti digital (digital evidence) dibagi menjadi 2, yaitu :

1. Barang Bukti Elektronik
Barang bukti ini bersifat fisik dan dapat dikenali secara visual, karena sifatnya itu investigator ataupun penyidik sudah bisa mengenali masing-masing barang bukti elektronik ketika sedang proses pencarian (searching) di TKP. Adapun contoh dari barang bukti elektronik diantaranya adalah :

a. Komputer PC, Laptop, Notebook, Netbook, Tablet
b. Handphone, Smartphone
c. Flashdisk
d. Floppydisk
e. Hardsik
f. CD/DVD
g. Router, Switch, Hub, Modem
h. Kamera Video, CCTV
i. Kamera Digital
j. Digital Recorder
k. Music/Video Player, dan lain sebagainya

2. Barang Bukti Digital
Barang bukti ini bersifat digital atau abstrak yang di ekstrak atau di urai atau di recover dari barang bukti elektronik. Dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah informasi elektronik dan dokumen elektronik. Barang bukti ini di analisa oleh forensic analyst untuk kemudian di periksa secara teliti keterkaitan masing-masing file dalam mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik yang ditemukan di TKP.

Adapun contoh dari barang bukti digital diantaranya, adalah :

a. Logical file
File yang masih tercatat di file system yang sedang berjalan (running) disuatu partisi. File tersebut bisa berupa file library, office, text, logs, multimedia, aplikasi, dll

b. Deleted file

Dikenal dengan istilah unallocated cluster yang merujuk kepada cluster dan sector penyimpnanan file yang sudah terhapus dan tidak teralokasikan lagi untuk file tersebut dengan ditandai di file system sebagai bagian yang dapat digunakan lagi untuk menyimpan file baru. Artinya, file yang sudah terhapus masih tetap berada di cluster atau sector tempat penyimpnanannya sampai file tersebut tertimpa (overwritten) oleh file yang baru pada sekotor dan cluster tersebut. Dalam kondisi deleted file tersebut belum tertimpa oleh file yang baru, maka proses recovery secara utuh terhadap file tersebut sangat memungkinkan terjadi.

c. Lost file

File sudah tidak tercatat lagi di file system yang sedang berjalan (running system) dari suatu partisi tapi masih tersimpan di sector penyimpananya. Hal ini terjadi jika harddirve ataupun flashdisk dilakukan re-format yang menghasilkan file system yang baru, sehingga file-file yang ada sebelumnya tidak tercatat lagi di file system yang baru. Untuk proses recoverynya didasarkan pada signature dari header maupun footer yang tergantung pada jenis format file tersebut apakah FAT32, FAT, atapun NTFS.

d. Slack file

Sector penyimpanan yang diantara End of File (EoF) dan End of Cluster (EoC). Bagian ini sangat memungkinan terdapat informasi yang mungkin dapat dijadikan barang bukti digital dari bagian-bagian file yang sudah dihapus sebelumnya.

e. Log file

File yang merekam segala aktifitas yang dilakukan dari keadaaan tertentu, pada log dari sistem operasi, internet, aplikasi yang digunakan, internet traffic, dan lain sebagainya.

f. Encrypted file

File yang isinya sudah dilakukan enkripsi dengan menggunakan algoritma cryptography yang kompleks, sehingga tidak bisa dibaca atau dilihat secara normal. Satu-satunya cara untuk membaca atau melihatnya kembali adalah dengan melakukan dekripsi terhadap file tersebut dengan menggunakan algoritma yang sama. Ini biasa digunakan dalam dunia digital information security untuk mengamankan informasi yang penting. Ini juga merupakan salah satu bentuk dari Anti-Forensic, yaitu suatu metode untuk mempersulit forensic analyst atau investigator mendapatkan informasi mengenai jejak-jejak kejahatan.

g. Steganography

File yang berisikan informasi rahasia yang disisipkan ke file lain, biasanya berbentuk file gambar, video atau audio, sehingga file-file yang bersifat carrier (pembawa pesan rahasia) tersebut terlihat normal dan wajar bagi orang lain, namun bagi orang yang tahu metodologinya, file-file tersebut memiliki makna yang dalam dari informasi rahasianya tersebut. Ini juga dianggap sebagai salah satu bentuk dari Anti-Forensic.

h. Office file

File yang merupakan produk dari aplikasi Office, seperti Microsoft Office, Open Office dan sebagainya. Ini biasanya berbentuk file dokumen, spreadsheet, database, teks, dan presentasi.

i. Audio file

File yang berisikan suara, musik dan lain-lain, yang biasanya berformat wav, mp3 dan lain-lain. File audio yang berisikan rekaman suara percakapan orang ini biasanya menjadi penting dalam investigasi ketika suara di dalam file audio tersebut perlu diperiksa dan dianalisa secara audio forensik untuk memastikan suara tersebut apakah sama dengan suara pelaku kejahatan.

j. Video file

File yang memuat rekaman video, baik dari kamera digital, handphone, handycam maupun CCTV. File video ini sangat memungkinkan memuat wajah pelaku kejahatan sehingga file ini perlu dianalisa secara detil untuk memastikan bahwa yang ada di file tersebut adalah pelaku kejahatan.

k. Image file

Untuk jenis file ini pernah di ulas oleh penulis bagaimana cara menyimpan data dalam gambar atau foto. File gambar digital yang sangat memungkinkan memuat informasi-informasi penting yang berkaitan dengan kamera dan waktu pembuatannya (time stamps). Data-data ini dikenal dengan istilah *metadata exif* (exchangeable image file). Meskipun begitu metadata exif ini bisa dimanipulasi, sehingga forensic analyst atau investigator harus hati-hati ketika memeriksa dan menganalisa metadata dari file tersebut.

l. Email

Merupakan singkatan dari electronic mail, yaitu surat berbasis sistem elektronik yang menggunakan sistem jaringan online untuk mengirimkannya atau menerimanya. Email menjadi penting di dalam investigasi khususnya phishing (yaitu kejahatan yang menggunakan email palsu dilengkapi dengan identitas palsu untuk menipu si penerima). Email berisikan header yang memuat informasi penting jalur distribusi pengiriman email mulai dari sender (pengirim) sampai di recipient (penerima), oleh karena itu data di header inilah yang sering dianalisa secara teliti untuk memastikan lokasi si pengirim yang didasarkan pada alamat IP. Meskipun begitu, data-data di header juga sangat dimungkinkan untuk dimanipulasi. Untuk itu pemeriksaan header dari email harus dilakukan secara hati-hati dan komprehensif

m. User ID dan password

Informasi ini penting untuk bisa masuk kedalam suatu sistem atau aplikasi tertentu. Dan biasanya informasinya menggunakan algoritma tertentu untuk menyulitkan pengguna lain yang tidak berhak mengkases informasi yang ada dalam sistem atau aplikasi tersebut.

n. SMS

Pelayanan pengiriman dan penerimaan pesan pendek yang diberikan oleh operator seluler terhadap pelanggannya. SMS-SMS yang bisa berupa SMS inbox (masuk), sent (keluar), dan draft (rancangan) dapat menjadi petunjuk dalam investigasi untuk mengetahui keterkaitan antara pelaku yang satu dengan yang lain.

o. MMS

Merupakan jasa layanan yang diberikan oleh operator seluler berupa pengiriman dan penerimaan pesan multimedia yang bisa berbentuk suara, gambar atau video.

p. Call Logs

Catatan panggilan yang terekam pada suatu nomor panggilan seluler. Panggilan ini bisa berupa incoming (panggilan masuk), outgoing (panggilan keluar), dan missed (panggilan tak terjawab).Berdasarkan penjelasan di atas, dapat diketahui bahwa ada perbedaan antara barang bukti elektronik dengan barang bukti digital. Yang pertama bersifat bentuk fisik, sementara yang kedua memiliki isi yang bersifat digital. Ini harus dapat dipahami dengan jelas oleh forensic analyst dan investigator ketika mereka melakukan pencarian barang bukti elektronik di TKP (Tempat Kejadian Perkara), untuk kemudian membawanya ke laboratorium dan menganalisanya dengan tepat dan prosedural, sehingga menghasilkan barang bukti digital seperti yang diharapkan.

Berikut penulis gambarkan yang termasuk dalam barang bukti digital dibawah ini :

Berdasarkan uraian diatas, maka penulis menyimpulkan sumber bukti digital dibagi menjadi 3 (tiga) kategori besar, yaitu :

1. Open Computer Systems
Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagaiperangkat sistem yang memiliki media penyimpanan, komputer.

Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya laptop, desktop, server, dan perangkat-perangkat sejenis lain.

Perangkat yang memiliki sistem media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi.

Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut di akses, dan informasi lainnya semua merupakan informasi penting

2. Communication Systems
Sistem telepon tradisional, komunikasi wireless, Internet, jaringan komunikasi data.

Sebagai contoh, jaringan Internet membawa pesan-pesan dari seluruh dunia melalui email. Kapan waktu pengiriman e-mail ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari e-mail pengirim mengirim, apa isi dari e-mail tersebut merupakan bukti digital yang amat sangat penting dalam investigasi.

3. Embedded Computer Systems
Perangkat telepon bergerak (ponsel), personal digital assistant (PDA), smartcard, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini.

Hal ini dikarenakan bukti-bukti digital juga dapat tersimpan di sini. Sebagai contoh, sistem navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor dan modul-modul diagnosa yang dipasang dapat menyimpan informasi digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna.

KARAKTERISTIK BARANG BUKTI DIGITAL (DIGITAL EVIDENCE)
Dalam dokumen SWGDE (Scientific Working Group on Digital Evidence) tahun 1999, menyebutkan bahwa Digital evidence atau sering disebut dengan e-evidence merupakan informasi yang didapat dalam bentuk atau format digital. Berbeda dengan barang bukti konvensial lainnya, barang bukti digital memiliki karakteristik yang unik, diantaranya :

1. Sangat rentan dimodifikasi dan dihilangkan.
2. Bersifat time sensitive, yang artinya bukti digital sangat rentan terhadap perubahan waktu.
3. Bukti digital mempunyai kemungkinan bersifat lintas negara dan yurisdiksi.

Barang bukti digital yang diperoleh oleh investigator tidak langsung dapat diterima dalam proses peradilan, agar dapat diterima maka harus memenuhi beberapa kriteria berikut :

1. Data di terima (Admissible)

Dimana data harus mampu diterima dan digunakan demi hukum, mulai dari kepentingan penyelidikan sampai dengan kepentingan pengadilan.

2. Keaslian (Authenticity)
Bukti tersebut harus berhubungan dengan kejadin atau kasus yang terjadi, bukan rekayasa.

3. Lengkap (Complete)
Bukti digital dikatakan bagus dan lengkap jika didalamnya terdapat banyak petunjuk yang dapat membantu proses investigasi.

4. Berfungsi (Reliable)
Artinya bukti dapat mengatakan hal yang terjadi dibelakangnya. Jika bukti tersebut dapat dipercaya, maka investigasi akan lebih mudah. Dalam arti lain kemungkinan dari suatu sistem atau komponen untuk dapat memenuhi fungsi yang dibutuhkan, pada kondisi tertentu dan pada periode waktu tertentu. (Institute of Electrical and Electronics Engineers, IEEE 90).

5. Dapat dipahami (Believable)
Barang bukti harus benar-benar dipahami, dipercaya, dan dimengerti, serta mempresentasikan hasil penyelidikan harus sesuai dengan audionya, sehingga mudah dipahami untuk digunakan dalam proses eksekusi.

METODOLOGI FORENSIK
Metodologi yang digunakan dalam menginvestigasi peristiwa kejahatan dalam Teknologi Informasi dibagi menjadi 2 (dua), yaitu :

1. Search dan Seizure
Investigator harus terjun langsung ke dalam kasus yang terjadi, dalam ini kasus teknologi informasi. Dengan tindakan ini diharapkan investigator mampu mengidentifikasi, menganalisa, dan memproses bukti yang berupa fisik. Investigator memiliki kewenangan untuk melakukan penyitaan terhadap barang bukti yang dapat membantu proses penyidikan sesuai dengan undang-undang yang berlaku.

2. Pencarian Informasi
Tahapan dalam pencarian informasi dapat dijelaskan dalam uraian berikut dibawah ini, yaitu :

a. Menemukan lokasi tempat kejadian perkara
b. Investigator menggali informasi dari aktifitas yang tercatat dalam log ataupun barang bukti elektronik lainnya.
c. Penyitaan media penyimpanan data (data storages) yang dianggap dapat membantu proses penyidikan.

Dalam menggali informasi yang berkaitan dengan kasus kejahatan TI, peran investigator harus bisa menguasai trik-trik kasus Teknologi Informasi.

ANCAMAN TERHADAP BARANG BUKTI
Menurut Jim Mc Millan, *“Importance of a standard methodology in computer forensics“:*

1. Virus
2. Prosedur Clean-Up
3. Ancaman Eksternal – Lingkungan

Menurut Judd Robin “ An explanation of computer forensics “ mensyaratkan :

1. Barang bukti tidak akan rusak oleh prosedur

2. penyelidikan
3. Tidak terinfeksi virus komputer
4. Barang bukti dilindungi dari keruksakan mekanis dan elektromekanis
5. Penerapan pemelihraan
6. Membatasi dampak pada operasi bisnis
7. Informasi client dihargai secara etis dan tidak diumumkan

PRINSIP KETIDAKPASTIAN HEISENBERG
Dan Farmer " Computer forensic analysis class handouts" :

"Melakukan pengujian sekumpulan atau suatu bagian dari sistem akan menimbulkan gangguan pada komponen lainnya, sehingga akan mustahil untuk melakukan capture keseluruhan sistem pada satu saat saja"

Jim Mc Millan, *"Banyak barang bukti dalam bentuk terenkripsi atau hidden"*.

Dari hasil uraian diatas penulis dapat menyimpulkan bahwa barang bukti digital atau digital evidence adalah ***informasi yang dihasilkan dari perangkat digital baik secara visual maupun abstrak.***

Sumber :

- **Marshall, A. M.(2009).** *Digital forensics: Digital evidence in criminal investigations*
- Digital Forensics: digital evidence in criminal investigations - the website of the book by Angus M. Marshall
- IT Law WIKI - Digital Evidence

All is about imagination - Endang Kurniawan
Sumber : https://endangkurniawan.com/article-digital-forensics-digital-evidence-in-criminal-investigation-1.html