**Tahapan-tahapan pada Digital Forensik**

Seorang ahli Digital Forensik dapat menggambarkan tahapan dan metode-metode yang digunakan untuk mendapatkan informasi tentang file terhapus, terenkripsi ataupun yang rusak. Lalu apa saja sebenarnya tahapan-tahapan dalam implementasi Digital Forensik? Secara umum ada 4 (empat) tahapan yang harus dilakukan dalam implementasi Digital Forensik, yaitu:

1. **Pengumpulan *(Acquisition)***

2. **Pemeliharaan *(Preservation)***

3. **Analisa *(Analysis)***

4. **Presentasi *(Presentation)***

**1.       Acquisition (Pengumpulan).**

Mengumpulkan dan mendapatkan bukti-bukti yang mendukung penyelidikan. Tahapan ini merupakan tahapan yang sangat menentukan karena bukti-bukti yang didapatkan akan sangat mendukung penyelidikan untuk mengajukan seseorang ke pengadilan dan diproses sesuai hukum hingga akhirnya dijebloskan ke tahanan. Media digital yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, pen drive, hard disk, atau CD-ROM), PDA, handphone, smart card, sms, e-mail, cookies, log file, dokumen atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Penelusuran bisa dilakukan untuk sekedar mencari *"ada informasi apa disini?"* sampai serinci pada *"apa urutan peristiwa yang menyebabkan terjadinya situasi terkini?"*.

Software ataupun tools yang bisa digunakan dalam mendukung tahapan ini antara lain:

·         Forensic Acquisition Utilities *(<http://users.erols.com/gmgarner/forensics/>)*

·         FTimes *(<http://ftimes.sourceforge.net/FTimes/index.shtml>)*

·         liveview *(<http://liveview.sourceforge.net/>)*

·         netcat *(<http://www.atstake.com/research/tools/network_utilities/pdd>)*

·         ProDiscover DFT *([www.techpathways.com](http://www.techpathways.com/))*

·         psloggedon *(<http://www.sysinternals.com/ntw2k/freeware/psloggedon.shtml>)*

·         TULP2G *(<http://sourceforge.net/projects/tulp2g/>)*

·         UnxUtils *([http://unxutils.sourceforge.net](http://unxutils.sourceforge.net/))*

·         Webjob *(<http://webjob.sourceforge.net/WebJob/index.shtml>)*.

**2.       Preservation (Pemeliharaan).**

Memelihara dan menyiapkan bukti-bukti yang ada. Termasuk pada tahapan ini melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk diteliti. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan komputer dengan tidak hati-hati bisa saja merusak/merubah barang bukti tersebut. Seperti yang diungkapkan Peter Plummer[[1]](#footnote-0)[5] : *“When you boot up a computer, several hundred files get changed, the data of access, and so on. Can you say that computer is still exactly as it was when the bad guy had it last?”.* Sebuah pernyataan yang patut dipikirkan bahwa bagaimana kita bisa menjamin kondisi komputer tetap seperti keadaan terakhirnya ketika ditinggalkan oleh pelaku kriminal manakala komputer tersebut kita matikan atau hidupkan kembali. Karena ketika komputer kita hidupkan terjadi beberapa perubahan pada *temporary file*, waktu akses, dan seterusnya.Sekali file-file ini telah berubah ketika komputer dihidupkan tidak ada lagi cara untuk mengembalikan *(recover)* file-file tersebut kepada keadaan semula. Komputer dalam kondisi hidup juga tidak bisa sembarangan dimatikan. Sebab ketika komputer dimatikan bisa saja ada program penghapus/perusak yang dapat menghapus dan menghilangkan bukti-bukti yang ada. Ada langkah-langkah tertentu yang harus dikuasai oleh seorang ahli digital forensik dalam mematikan/menghidupkan komputer tanpa ikut merusak/menghilangkan barang bukti yang ada didalamnya.

Karena bukti digital bersifat sementara *(volatile),* mudah rusak, berubah dan hilang, maka seorang ahli Digital Forensik harus mendapatkan pelatihan *(training)* yang cukup untuk melakukan tahapan ini. Aturan utama pada tahap ini adalah penyelidikan tidak boleh dilakukan langsung pada bukti asli karena dikhawatirkan akan dapat merubah isi dan struktur yang ada didalamnya. Hal ini dapat dilakukan dengan melakukan copy data secara *Bitstream Image* pada tempat yang sudah pasti aman. *Bitstream image* adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk file yang tersembunyi (*hidden files*), file temporer *(temporary file)*, file yang terdefrag (*defragmented file*), dan file yang belum ter­*overwrite*. Dengan kata lain, setiap biner digit demi digit di-copy secara utuh dalam media baru. Teknik ini umumnya diistilahkan dengan *cloning* atau *imaging*. Data hasil *cloning* inilah yang selanjutnya menjadi objek penelitian dan penyelidikan.

**3.       Analisa (Analysis)**

Melakukan analisa secara mendalam terhadap bukti-bukti yang ada. Bukti yang telah didapatkan perlu di-*explore* kembali kedalam sejumlah skenario yang berhubungan dengan tindak pengusutan, antara lain: siapa yang telah melakukan, apa yang telah dilakukan (contoh : apa saja software yang digunakan), hasil proses apa yang dihasilkan, dan waktu melakukan).

Penelusuran bisa dilakukan pada data sebagai berikut: alamat URL yang telah dikunjungi, pesan e-mail atau kumpulan alamat e-mail yang terdaftar, program word processing atau format ekstensi yang dipakai, dokumen spreedsheat yang dipakai, format gambar yang dipakai apabila ditemukan, file-file yang dihapus maupun diformat, password, registry windows, *hidden files, log event viewers*, dan *log application*. Termasuk juga pengecekan metadata. Kebanyakan file mempunyai metadata yang berisi informasi yang ditambahkan mengenai file tersebut seperti *computer name, total edit time,* jumlah *editing session*, dimana dicetak, berapa kali terjadi penyimpanan *(saving)*, tanggal dan waktu modifikasi.

Selanjutnya melakukan recovery dengan mengembalikan file dan folder yang terhapus, unformat drive, membuat ulang partisi, mengembalikan password, merekonstruksi ulang halaman web yang pernah dikunjungi, mengembalikan email-email yang terhapus dan seterusnya. Untuk analisis media, tools yang bisa digunakan antara lain:

·         TestDisk *(http://www.cgsecurity.org/testdisk.html)*

·         Explore2fs *(http://uranus.it.swin.edu.au/~jn/linux/explore2fs.htm)*

·         ProDiscover DFT *(http://[www.techpathways.com](http://www.techpathways.com/))*

Sedangkan untuk analisis aplikasi, tools yang bisa digunakan:

·         Event Log Parser *(http://www.whitehats.ca/main/members/Malik/malik\_eventlogs/malik\_eventlogs.html)*

·         Galleta *(http://www.foundstone.com/resources/proddesc/galleta.htm)*

·         libpff *(http://libpff.sourceforge.net)*

·         md5deep *(http://md5deep.sourceforge.net/)*

·         MD5summer *(http://www.md5summer.org/)*

·         Outport *(http://outport.sourceforge.net/)*

·         Pasco *(http://www.foundstone.com/resources/proddesc/pasco.htm)*

·         RegRipper *(http://windowsir.blogspot.com/2008/04/updated-regripper.html)*

·         Rifiuti *(http://www.foundstone.com/resources/proddesc/rifiuti.htm)*

**4.       Presentasi (Presentation).**

Menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan secara ilmiah di pengadilan. Beberapa hal penting yang perlu dicantumkan pada saat presentasi/panyajian laporan ini, antara lain:

·         Tanggal dan waktu terjadinya pelanggaran

·         Tanggal dan waktu pada saat investigasi

·         Permasalahan yang terjadi

·         Masa berlaku analisa laporan

·         Penemuan bukti yang berharga (pada laporan akhir penemuan ini sangat ditekankan sebagai bukti penting proses penyidikan)

·         Tehnik khusus yang digunakan, contoh: *password cracker*

·         Bantuan pihak lain (pihak ketiga)

Laporan yang disajikan harus di cross check langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung.

**Kesimpulan**

Digital Forensik merupakan teknik ilmiah yang meneliti perangkat digital dalam membantu pengungkapan berbagai macam kasus kejahatan. Tahapan-tahapan yang dilakukan pada Digital Forensik meliputi: Pengumpulan *(Acquisition)*, Pemeliharaan *(Preservation)*, Analisa *(Analysis)*, dan Presentasi *(Presentation)*.

Untuk menjadi seorang ahli dibidang Digital Forensik, harus didukung dengan pengetahuan tentang teknologi informasi secara menyeluruh baik hardware maupun software, meliputi: sistem operasi, bahasa pemrograman, media penyimpanan komputer, networking, routing, protokol komunikasi dan sekuriti, kriptologi, teknik pemrograman terbalik, teknik investigasi, perangkat komputer forensik, bentuk/format file, dan segala aplikasi software tools forensik. Anda pun perlu didukung berbagai sertifikat yang tidak sedikit, antara lain Certified Information System Security Professional (CISSP) yang diberikan lembaga yang bernama Information Systems Security Certification Consortium (ISC) 2, lalu Certified Forensics Analyst (CFA), Experienced Computer Forensic Examiner(ECFE), Certified Computer Examiner (CCE), Computer Hacking Forensic Investigator (CHFI) dan Advanced Information Security (AIS).

1. [↑](#footnote-ref-0)