E T I K A & P R O F E S I O N A L I S M E T S I

“Tools Information Technology Forensic”

Disusun Oleh :

Nama Anggota Kelompok :	**Daniel**	**(1D114129)**
	Joko Himawan	**(15114687)**
	Meydi Annisa	**(16114610)**
	Nitha Tiara Putri	**(17114992)**
	Zuan Fauzan	**(1C114681)**
Kelas	**: 4KA34**	

UNIVERSITAS GUNADARMA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

JURUSAN SISTEM INFORMASI

ATA 2017/2018

KATA PENGANTAR

Puji dan syukur atas kehadirat Tuhan Yang Maha Esa atas rahmatNya sehingga kami dapat menyelesaikan makalah ini tepat pada waktunya. Makalah ini dibuat untuk memenuhi tugas mata kuliah Etika & Profesionalisme Teknologi Sistem Informasi. Dalam makalah ini kami membahas tentang tools - tools apa saja yang biasa digunakan oleh seorang ahli IT Forensik. Ucapan terima kasih pun tidak lupa kami ucapkan kepada teman - teman sekelompok yang telah membantu dalam menyelesaikan makalah ini yang tidak dapat disebutkan satu per satu.

Kami menyadari bahwa makalah ini masih jauh dari kesempurnaan, oleh karena itu masukan berupa kritikan dan saran sangat kami harapkan demi penyempurnaan makalah ini. Akhir kata, kiranya makalah ini dapat berguna dan bisa menjadi pedoman bagi mahasiswa/I untuk dapat mempelajari serta memahami tentang Tools IT Forensik. Sekian dan terima kasih.

Bekasi, April 2018

Penulis

Tools IT Forensic

Makna atau Pemahaman Tools IT Forensic :

Komputer forensik adalah cabang ilmu komputer yang sangat penting dalam kaitannya dengan kejahatan terkait komputer dan internet. Sebelumnya, komputer hanya digunakan untuk menghasilkan data - data tetapi sekarang telah diperluas ke semua perangkat yang terkait dengan data digital. Tujuan dari IT Forensik adalah untuk melakukan investigasi kejahatan dengan menggunakan bukti dari data digital untuk menemukan siapa yang bertanggung jawab atas kejahatan tersebut.

Setiap tools yang digunakan oleh seorang ahli IT Forensik adalah untuk membantu dalam melakukan proses investigasi kejahatan yang terjadi. Dalam kasus hukum, teknik digital forensik sering digunakan untuk meneliti sistem komputer milik terdakwa (dalam perkara pidana) atau tergugat (dalam perkara perdata). Memulihkan data dalam hal suatu hardware atau software yang mengalami kegagalan/kerusakan (failure).

Prinsip kerja komputer forensik pada dasarnya mirip dengan proses yang terjadi pada kepolisian ketika hendak mengusut bukti tindak kejahatan dengan menelusuri fakta-fakta yang ada. Hanya saja pada komputer forensik proses dan kejadiannya terdapat pada dunia maya. Selain untuk kepentingan pembuktian, penggunaan forensik komputer secara tepat juga dapat membersihkan seseorang yang tidak bersalah dari dakwaan atau sebaliknya membawa seseorang yang terbukti bersalah kehadapan hukum.

Macam - Macam Tools IT Forensik

1) Digital Forensics Framework

Digital Forensics Framework adalah platform populer lainnya yang didedikasikan untuk forensik digital. Alat ini open source dan berada di bawah Lisensi GPL. Ini dapat digunakan baik oleh para profesional atau non-ahli, ini dapat digunakan untuk alat lacak digital, untuk mengakses perangkat jarak jauh atau lokal, forensik OS Windows atau Linux, pemulihan tersembunyi dari file yang dihapus, pencarian cepat untuk meta data file, dan berbagai hal lainnya.

Framework for a Digital Forensic Investigation

Preparation : Preperation investigasi mencakup hal berikut :

- Standar yang digunakan dalam organisasi.
- Kebijakan dan prosedur di tempat untuk membantu dalam penyelidikan
- Pelatihan
- Nasihat hukum
- Pemberitahuan kepada otoritas yang benar
- Dokumentasi insiden sebelumnya
- Perencanaan, juga dikenal sebagai “strategi pendekatan”.

Investigation : Investigation mencakup sebagai berikut :

- Mencari dan mengidentifikasi bukti pada komputer.
- Koleksi bukti dari komputer (original diduplikasi).
- Menyimpan bukti di tempat yang aman.
- Penyimpanan bukti yang dikumpulkan di tempat kejadian.
- Pemeriksaan bukti dengan menggunakan alat yang tepat.
- Analisis (terlihat pada proses pemeriksaan untuk menentukan signifikansi dan nilai dari bukti yang ditemukan).

2) X-Ways Forensics

X-Ways Forensics adalah platform canggih untuk pemeriksa forensik digital, ini berjalan pada semua versi Windows yang tersedia. Ia mengaku tidak terlalu lapar sumber daya dan bekerja secara efisien. Jika kita berbicara tentang fitur, temukan fitur utama dalam daftar di bawah ini:

- Disk pencitraan dan kloning
- Ability untuk membaca struktur sistem file di dalam berbagai file gambar
- Mendukung sebagian besar sistem file termasuk FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS / ISO9660 / Joliet, UDF
- Deteksi otomatis partisi hard disk yang terhapus atau hilang
- Berbagai teknik pemulihan data dan ukiran file yang kuat
- Perhitungan hash massal
- Melihat dan mengedit struktur data biner menggunakan template
- Mudah mendeteksi dan mengakses NTFS ADS
- Well mempertahankan file header
- Outisasi aktivitas penebangan
- Data keaslian
- Pengelolaan kasus lengkap
- Memory dan analisis RAM
- Tampilan galeri untuk gambar
- Internal viewer untuk file registri Windows
- Laporan registri terotomasi
- Menghapus meta data dari berbagai jenis file
- Kemampuan untuk mengekstrak email dari berbagai klien email yang tersedia.

3) SANS Investigative Forensics Toolkit – SIFT

SANS Investigative Forensics Toolkit atau SIFT adalah sistem operasi forensik multi-tujuan yang dilengkapi dengan semua alat yang diperlukan yang digunakan dalam proses forensik digital, ini dibangun di Ubuntu dengan banyak alat yang berkaitan dengan digital forensik. Awal tahun ini, SIFT 3.0 dirilis. Itu datang secara gratis atau biaya dan berisi alat forensik open-source gratis, dalam

posting sebelumnya di resource.infosecinstitute.com, kami sudah membahas SIFT secara rinci. Anda dapat membaca posting tentang SIFT untuk mengetahui lebih lanjut tentang platform forensik digital ini.

4) Volatility

Volatilitas adalah kerangka forensik memori. Itu digunakan untuk respon insiden dan analisis malware. Dengan alat ini, Anda dapat mengekstrak informasi dari proses yang berjalan, soket jaringan, koneksi jaringan, DLL dan kumpulan registri. Ini juga memiliki dukungan untuk mengekstraksi informasi dari file dump crash Windows dan file hibernasi. Alat ini tersedia gratis di bawah lisensi GPL.

5) WindowsSCOPE

WindowsSCOPE adalah forensik memori lain dan alat rekayasa terbalik yang digunakan untuk menganalisis memori yang mudah menguap. Ini pada dasarnya digunakan untuk reverse engineering of malwares. Ini menyediakan kemampuan menganalisis kernel Windows, driver, DLL, memori virtual dan fisik.

6) Oxygen Forensic Suite

Oxygen Forensic Suite adalah perangkat lunak yang bagus untuk mengumpulkan bukti dari ponsel untuk mendukung kasus Anda. Alat ini membantu mengumpulkan informasi perangkat (termasuk produsen, OS, nomor IMEI, nomor seri), kontak, pesan (email, SMS, MMS), memulihkan pesan yang dihapus, log panggilan dan informasi kalender. Ini juga memungkinkan Anda mengakses dan menganalisis data dan dokumen perangkat seluler. Ini menghasilkan laporan yang mudah dipahami untuk pemahaman yang lebih baik.

7) Bulk Extractor

Bulk Extractor juga merupakan alat forensik digital yang penting dan populer. Ini scan gambar disk, file atau direktori file untuk mengekstrak informasi yang berguna. Dalam proses ini, ia mengabaikan struktur sistem file, sehingga lebih cepat daripada alat sejenis lainnya yang tersedia. Ini pada dasarnya digunakan oleh intelijen dan lembaga penegak hukum dalam menyelesaikan kejahatan cyber.

8) Xplico

Xplico adalah alat analisis forensik jaringan open source. Ini pada dasarnya digunakan untuk mengekstrak data yang berguna dari aplikasi yang menggunakan Internet dan protokol jaringan. Mendukung sebagian besar protokol populer termasuk HTTP, IMAP, POP, SMTP, SIP, TCP, UDP, TCP dan lainnya. Data output dari alat disimpan dalam database SQLite dari database MySQL. Ini juga mendukung IPv4 dan IPv6 keduanya.

9) Computer Online Forensic Evidence Extractor (COFEE)

Komputer Online Forensic Evidence Extractor atau COFEE adalah tool kit yang dikembangkan untuk ahli forensik komputer. Alat ini dikembangkan oleh Microsoft untuk mengumpulkan bukti dari sistem Windows. Ini dapat diinstal pada USB pen drive atau hard disk eksternal. Cukup colokkan perangkat USB di komputer target dan memulai analisis langsung. Muncul dengan 150 alat yang berbeda dengan antarmuka berbasis GUI untuk memerintahkan alat. Ini cepat dan dapat melakukan seluruh analisis hanya dalam waktu 20 menit. Untuk lembaga penegak hukum, Microsoft menyediakan dukungan teknis gratis untuk alat tersebut.

10) P2 eXplorer

P2 eXplorer adalah alat pemasangan gambar forensik yang bertujuan membantu menyelidiki petugas dengan pemeriksaan kasus. Dengan gambar ini, Anda dapat memasang gambar forensik sebagai disk lokal dan fisik baca-saja dan kemudian menjelajahi konten gambar dengan file explorer. Anda dapat dengan

mudah melihat data yang dihapus dan ruang gambar yang tidak terisi. Dapat memasang beberapa gambar sekaligus. Mendukung sebagian besar format gambar termasuk EnCasem, safeBack, PFR, FTK DD, WinImage, gambar Mentah dari Linux DD, dan gambar VMWare. Mendukung jenis gambar logis dan fisik. Alat ini datang seharga $ 199, tetapi Anda dapat mengambil versi fitur terbatas dari alat tersebut secara gratis.

Kesimpulan

Beberapa alat forensik digital di atas digunakan oleh berbagai lembaga penegak hukum dalam melakukan investigasi kejahatan. Dalam makalah ini, saya menambahkan semua jenis alat seperti premium, gratis, open source, komputer forensik, forensik seluler dan lain-lain. Jika kita akan mulai belajar forensik digital, kita dapat mengunduh atau membeli alat-alat ini dan mulai mengerjakannya, ini akan membantu kita untuk lebih memahami seluruh proses investigasi, dengan meningkatnya penggunaan data digital dan smartphone, forensik digital menjadi lebih penting, kejahatan cyber juga meningkat dari hari ke hari. Jadi perusahaan juga mencoba meluncurkan versi alat yang lebih kuat.

IT Forensik digunakan untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti yang sah di pengadilan, untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Daftar Pustaka

a) Shankdhar, P. ”22 Popular Computer Forensics Tools”. 26 Mei 2017. http://resources.infosecinstitute.com/computer-forensics-tools/
b) Sandsfir. “SANS Digital Forensics and Incident Response”. 29 Januari 2018. https://digital-forensics.sans.org/blog/2018/01/29/sans-threat-hunting-and-incident-response-summit-2018-call-for-speakers-deadline-35
c) Susanto, B. “Komputer Forensik:Pengertian dan Tujuan Lengkap”. 27 November 2014.http://www.spengetahuan.com/2014/11/komputer-forensik-pengertian-dan-tujuan.html
d) Irfansyah, D. “Dasar Komputer Forensik”. 8 Desember 2016. https://diaryintrovert.weebly.com/dasar-komputer-forensik/dasar-komputer-forensik-apa-itu-komputer-forensik
e) Detik. “Mengintip Cara Kerja Digital Forensik”. 24 Januari 2012. https://inet.detik.com/cyberlife/d-1823098/mengintip-cara-kerja-digital-forensik-