PEMBUKTIAN KASUS KEJAHATAN DOOS DENGAN MENGGUNAKAN METODE FILE SISTEM ANALISIS DIGITAL FORENSIK

EVIDENCE OF THE CASE OF CRIME DOOS USING FORENSIC DIGITAL FILE ANALYSIS SYSTEM METHOD

Muhammad Fathi Mubara¹, Dadang Rusmana², Siti Madinah Ladjamuddin³ Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi Institut Sains dan Teknologi Nasional Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640 Telp. (021) 7874647, Fax. (021) 7866955 ¹fathimubarak@ymail.com, ²dadangrusmana@istn.ac.id, ³citymadinah07@istn.ac.id

ABSTRAK

Keamanan merupakan hal yang sangat penting dalam dunia teknologi informasi. DDos merupakan salah satu serangan yang banyak ditemui dalam dunia *networking*. DDos bertujuan untuk mematikan pelayanan dari komputer atau jaringan yang diserang. Efek dari serangan DDos sangat menganggu pengguna internet yang ingin mengunjungi situs yang telah diserang. Adanya celah kejahatan ini harus dihadapi dengan kemampuan pengetahuan tentang karakteristik barang bukti elektronik/digital dan teknik analisi data yang mendukung supaya penyelidikan dan penanganan barang bukti digital yang relevan. Dalam penelitian ini telah dilakukan pembuktikan kasus kejahatan DDos dengan menggunakan metode analisis file sistem digital forensik. Tahapan analisis diawali dengan pengumpulan bukti digital, identifikasi data hasil temuan, analisis data dan pembuktian bukti digital. Software yang digunakan untuk menganalisi data merupakan tools forensic DEFT Linux dan sleuth kit. Objek penelitian diambil dari file windXP.dd yang merupakan file hasil imaging harddisk sebuah komputer yang diduga memiliki keterkaitan dengan kasus tindak kejahatan serangan DDos terhadap sebuah akun web blog dengan URL http://fathimubarak.blogspot.com. Dari hasil penelitian analisis data bukti kejahatan ditemukan sejumlah history file yang dianggap mencurigakan dan diduga memiliki keterkaitan dengan kasus kejahatan DDos. Dari hasil penelitian ditemukan beberapa file yang dihapus, diantaranya file DDos.bat yang digunakan oleh pelaku untuk melakukan serangan DDos.

Kata kunci : digital forensik, forensic komputer, file sistem analisis, kejahatan komputer, digital forensik windows

ABSTRACT

Security is very important in the world of information technology. DDos is one of the most common attacks in the networking world. DDos aims to turn off services from the attacked computer or network. The effects of DDos attacks are very disruptive to internet users who wish to visit the sites that have been attacked. The existence of this crime gap must be faced with knowledge skills about the characteristics of electronic / digital evidence and data analysis techniques that support the investigation and handling of relevant digital evidence. In this research, the DDos crime case has been proven by using the digital forensic file system analysis method. The analysis stage begins with collecting digital evidence, identifying data from the findings, analyzing data and proving digital evidence. The software used to analyze the data is a DEFT Linux forensic tool and a single kit. The object of the research is taken from the windXP.dd file, which is a computer hard drive imaging file that is suspected of having a connection with a DDos attack crime against a web blog account with the URL <u>http://fathimubarak.blogspot.com</u>. From the results of the research on the analysis of evidence of crime data, it was found that a number of history files were considered suspicious and were suspected of having links with DDos crime cases. From the research results, it was found that several files were deleted, including the DDos.bat file used by the perpetrator to carry out DDos attacks.

Keywords: digital forensics, computer forensics, file system analysis, computer crime, digital windows forensics

1. PENDAHULUAN

Teknologi komputer dapat diguanakan sebagai alat bagi para pelaku kejahatan komputer, seperti: pencurian, penggelapan uang dan lain sebagainya. Terkait dengan hal tersebut kini barang bukti yang berasal dari komputer semakin banyak ditemukan dalam kasus persidangan kejahatan. Bukti yang berasal dari komputer sulit dibedakan antara yang asli dan salinannya, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi. Proses pembuktian bukti tindak kejahatan tentunya memiliki kriteria, demikian juga dengan proses pembuktian pada bukti yang didapat dari komputer. Tingkat kejahatan yang melibatkan komputer sebagai alat kejahatan maupun alat terkait kejahatan semakin terus meningkat, sehingga semakin banyak perusahaan atau produk yang berusaha membantu penegak hukum dalam proses pembuktian berbasis komputer untuk menentukan siapa, apa, dimana, kapan, dan bagaimana kejahatan dilakukan.

DDos merupakan salah satu serangan yang banyak ditemui dalam dunia *networking* saat ini. Serangan ini biasanya bertujuan untuk mematikan pelayanan dari komputer atau jaringan yang diserang. Serangan ini dapat ditujukan kepada siapa saja, bahkan ke personal. Efek dari serangan DDos sangat menganggu pengguna internet yang ingin mengunjungi situs yang telah diserang menggunakan DDos. Situs yang terserang DDos sulit untuk diakses bahkan mungkin tidak bisa untuk diakses.

Salah satu kemampuan utama yang dapat dilakukan oleh sebuah komputer adalah menyimpan data kemudian (store) menggunakannya (retrieve) kembali dengan cara yang tepat dan akurat. File sistem merupakan struktur logika yang digunakan untuk mengendalikan akses terhadap data yang ada pada *disk/media* penyimpanan. File sistem adalah bagian yang sangat penting dari sebuah sistem operasi, dimana file sistem yang akan mengatur penyimpan semua data. File sistem juga menangani penyimpanan data dari aplikasi yang terinstal dan semua data yang berkaitan dengan sistem operasi itu sendiri. Secara garis besar file sistem akan memberikan sejumlah informasi terkait dengan organisasi dari file sistem, misalnya informasi tentang : panjang dari file sistem block, ukuran file sistem, area block tempat dari mengalokasikan file, dan informasi lainnya. Hasil dari analisis file sistem ini nantinya dapat dikembangkan kembali sebagai acuan dalam proses pencarian bukti digital.

Dalam penelitian ini akan dibahas tentang tahapan-tahapan yang harus dilakukan dalam menganalisis data pada *harddisk* komputer berbasis sistem operasi Windows dengan menggunakan metode file sistem analisis guna mencari bukti kejahatan yang dilakukan oleh seorang pelaku kejahatan komputer (dalam kasus ini pelaku telah menghilangkan barang bukti kejahatan berupa *software* DDos.bat yang digunakan untuk melakukan serangan DDos). Teknik kejahatan komputer yang digunakan dalam penelitian merupakan sebuah serangan DDos terhadap sebuah situs website.

Dari uraian diatas timbul permasalahan yang berkaitan dengan proses analisis digital forensik file sistem Windows, yaitu pembuktian terhadap data hasil *imaging forensic* windXP.dd memiliki keterkaitan sebagai alat kejahatan yang digunakan untuk melakukan serangan DDos.

Setelah melakukan riset penelitian selama satu bulan dan untuk menghindari meluasnya masalah, maka batasan masalah yang berkaitan dalam penelitian hanya membatasi pada pembuktian adanya *software* aplikasi yang digunakan, serta keterkaitan *software* aplikasi terkait lainnya yang digunakan pelaku dalam melakukan serangan DDos pada website dengan menganalisa dari histori file aplikasi komputer dengan metode file sistem analisis digital forensik.

2. METODOLOGI PENELITIAN

Alat dan Bahan Penelitian : Perangkat Keras (*hardware*)

Perangkat keras yang digunakan dalam penelitian adalah Laptop ASUS seri A43S dengan spesifikasi *hardware*, sebagai berikut :

- *Mikroprocessor*: Intel Atom 1,6 Ghz
- *Memory* : 1 GB DDR2
- Harddisk : 160 GB
- *Monitor* : 16" LCD
- *Printer* : Inkjet

Perangkat Lunak (software)

Adapun perangkat lunak yang digunakan dalam penelitian ini adalah :

- 1. VMware :
- 2. DEFT Linux 7.2
- 3. Sleuth KIT

Objek Penelitian

Objek yang digunakan dalam penelitian adalah sebuah file *image* dari *harddisk* yang diduga digunakan sebagai alat kejahatan berupa file windXP.dd, dari file ini nantinya akan digunakan untuk membuktikan kebenaran komputer terduga tersebut digunakan sebagai alat kejahatan untuk melakukan serangan DDos atau *Distributed denial-of-service*. DDos merupakan jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain

untuk memperoleh akses layanan dari komputer yang diserang Tersebut^[10].

Tempat Penelitian

Tempat penelitian dilaksanakan pada lab. digital forensik Indonesia Security Incident Responses Team on Internet Infrastructure / Coordintator Center (ID-SIRTII/CC). pada Laboratorium *Digital Forensic*, yang berkantor di Menara Ravindo lantai 17, Jalan Kebon Sirih No. 75, Jakarta 10340.

Prosedur Penelitian Analisis File Sistem Windows

Prosedur analisis file sistem windows dilakukan dengan beberapa tahapan utama, diantaranya:

Pengumpulan Bukti-Bukti Digital 1 Merupakan proses mengumpulkan bukti digital yang tersimpan pada harddisk barang bukti elektronik (komputer) yang diduga sebagai alat bukti kejahatan. teknik pengumpulan barnag bukti dilakukan dengan cara melakukan forensic imaging, yaitu menggandakan isi harddisk secara physical (sektor per sektor atau bit-steram copy) sehingga hasil imaging akan sama persis seperti dengan barang bukti secara physical. Untuk mengetahui derajat kesamaan barang bukti dengan hasil imaging dapat dilihat dari nilai hashing yang diterapkan pada keduanya. Proses imaging forensic memiliki peranan yang sangat penting, sebab jika terjadi kesalahan dalam proses imaging maka akan sangat berpengaruh pada proses pencarian file, dan juga proses analisis file sistem.

2. Identifikasi Data Hasil Temuan

Setelah data yang perlukan dalam proses penyelidikan terkumpul maka selanjutnya adalah proses identifikasi hasil temuan. Proses yang dilakukan adalah mengidentifikasi file sistem dimana pada tahapan ini identifikasi dilakukan untuk memperoleh informasi yang berkaitan dengan file sistem yang digunakan. mulai dari struktur partisi harddisk, file sistem yang digunakan dan informasi penting terkait dengan file sistem. Proses analisis dilakukan dengan cara Analisis Media Management Disk (partition disk) yaitu dengan mengambil Master Boot Record file (MBR file). Dari file MBR seorang analis akan mengetahui struktur harddisk dan dapat mempermudah dalam pemetaan sector pada saat pencarian file bukti kejahatan.

3. Analisa Data

Analisa data dilakukan dengan dua cara, yaitu dengan melakukan analisis terhadap *timeline history file* dan analisis *history file*.

Pada tahapan pertama atau tahapan *analisis timeline* dilakukan dengan cara membuat

catatan waktu histori penggunaan komputer (*history timeline*). Pada proses analisa *timeline* pemeriksaan terfokus pada historis kegiatan yang pernah dilakukan dan history tentang aktifitas file (seperti eksekusi file, deleted file, dan transfer file) yang terjadi di dalam komputer, termasuk dalam rentang satu bulan terakhir.

Setelah proses analisis *timeline* selanjutnya adalah proses analisis *history file*, analisis dilakukan dengan metode file sistem analisis. Dimana dilakukan analisis terhadap pemetaan *sector* pada file sistem. Dari hasil pemetaan *sector* ini nantinya dapat ditemukan lokasi *sector* file yang diduga sebagai alat bukti kejahatan DDos di eksekusi dan disimpan. Data hasil analisis *history file* berupa kumpulan data *string* yang merujuk pada seluruh aktifitas yang dilakukan oleh seluruh file yang ada di dalam komputer beserta lokasi *sector* pada *harddisk*.

4. **Pembuktian**

Setelah dilakukan analisis secara mendalam, telah di temukan banyak petunjuk yang merujuk pada penggunaan software aplikasi untuk melakukan serangan DDos pada file windXP.dd. hasil imaging Pembuktian dilakukan dengan mengambil file DDos.bat yang telah dihapus. Hasil pembuktian selanjutnya dilaporkan secara detail dan lengkap dengan bukti-bukti temuan yang ditemukan pada saat proses analisis dilakukan. Seluruh data yang dilaporkan ini nantinya dapat diserahkan kepengadilan sebagai salah satu bukti yang kuat dan dapat dipertanggung jawabkan keabsahannya.



Gambar Alur Flowchart File Sistem Analisis Windows

3. HASIL DAN PEMBAHASAN

ISSN 2337-6805

Pembahasan Penelitian

Proses analisis digital forensik bertolak pada penemuan barang bukti. Pemilihan dan penggunaan tools forensik juga disesuaikan dengan kemampuan penguasaan investigator forensik. Muhammad Nuh Al-Azhar dalam bukunya menjelaskanada filosofi lama yang senantiasa sesuai dengan perkembangan zaman, yaitu "THE MAN BEHIND THE GUN" artinya kemampuan yang manusia (investigator) lebih diutamakan ketimbang peralatan atau persenjataan. Peralatan yang canggih dan lengkap, tidak akan berguna jika penggunanya tidak dapat mengunakannya.

penelitian dilakukan Proses dengan menggunakan prinsip triage forensic. Sebab dengan metode ini mampu membantu seorang investigator memperoleh barang atau file-file terkait dengan barang bukti digital.^[3] Tujuan dari triage forensic ini sendiri adalah (1) menyelamatkan bukti digital yang bersifat volatile (2) memberikan bukti digital secara cepat kepada investigator dan analisis forensik. Penelitian dengan menggunakan metode analis file sistem Windows di bagi kedalam beberapa tahapan utama, dimana setiap tahapan memiliki ketersinambungan antara tahapan satu dengan yang lain.

1. Proses Pengumpulan Bukti-Bukti Digital

Barang bukti elektronik seperti komputer yang telah ditemukan di tempat kejadian perkara diambil *harddisk*-nya yang berfungsi sebagai media penyimpanan untuk selanjutnya dilakukan proses *forensic imageing* (akuisisi). Sebelum dilakukan proses akuisisi, komputer yang digunakan untuk kegiatan akuisisi (komputer forensik) harus sudah dilengkapi dengan *write blocker*. Tujuan dari pemasangan *write blocker* adalah untuk menjaga keutuham isi dari barang bukti.



Gambar Proses Forensic Imaging dengan Menggunakan FTK Imager

Forensic imaging merupakan proses menggandakan isi harddisk secara physical (sektor per sektor atau bit-steram copy) sehingga hasil imaging akan sama persis seperti dengan barang bukti secara physical. Untuk mengetahui derajat kesamaan barang bukti dengan hasil imageing dapat dilihat dari nilai hashing yang diterapkan pada keduanya. Jika nilai hash antara hasil imaging dan barang bukti adalah sama, maka dapat dipastikan bahwa keduanya adalah identik dan hasil *imaging* bersifat forensik, artinya dapat di pertanggungjawabkan secara ilmiah dan hukum, untuk selanjutnya hasil *imaging* ini dapat digunakan untuk pemeriksaan dan analisis lebih lanjut. Sebaliknya, jika nilai *hash* antara keduanya berbeda, maka proses *forensic imaging* harus diulang sampai mendapatkan nilai yang sama.

Seperti yang terlihat pada gambar data nilai hash hasil imaging dengan nilai hash pada harddisk memiliki kesamaan nilai, yaitu 38ab6b3df14154e6e7ea4927f1301e14. Maka tidak diragukan lagi bahwa file hasil imaging identik dengan isi file harddisk. Proses hashing ini juga dikenal dengan istilah digital fingerprint (sidik jari digital) yang biasa digunakan untuk membuktikan secara pasti apakah kedua file yang dipertanyakan adalah sama atau berbeda.

E	1 D	rive/Image Verify Results								
	Ξ									
		Name	windXP.001							
Sector count 20971520										
	Ξ	MD5 Hash								
		Computed hash	38ab6b3df14154e6e7ea4927f1301e14							
		Report Hash	38ab6b3df14154e6e7ea4927f1301e14							
		Verify result	Match							
1	root:/investigation/images									
E	File Edit Tabs Help									
fa	th:	-virtual-machine/investigat	ion/images % md5sum windXP.dd							
38	abe	b3df14154e6e7ea4927f1301e14 w	indXP.dd							
fa	th	-virtual-machine/investigat	ion/images %							
_										

Gambar Proses Identifikasi Nilai Hashing Harddisk Barang Bukti dengan nilai Hashing file Image Hasil Imaging Forensic

Proses identifikasi nilai *hashing* dilakukan dengan membandingkan antar *nilai hashing harddisk* barang bukti dengan *file image* hasil proses *forensic imagin* dan didapatkan nilai *hashing* yang sama, maka dapat dipastikan data yang ada di dalamnya pun identic (sama). Apabila nilai *hashing* yang diperoleh tidak sama. Maka proses *forensic* imageing harus diulang hingga didapatkan nilai *hashing* yang sama. Selanjutnya apabila proses *forensic imaging* selesai, barang bukti komputer dimatikan secara paksa (tanpa melalui perintah *shutdown*), dan file hasil *imaging* digunakan untuk tahapan pemeriksaan selanjutnya.

2. Proses Identifikasi Data Hasil Temuan

Proses yang dilakukan selanjutnya adalah mengidentifikasi file sistem dimana pada tahapan ini identifikasi dilakukan untuk memperoleh informasi yang berkaitan dengan file sistem yang digunakan. Proses identifikasi file sistem di fokuskan pada pencarian file MBR (*Master Boot Record*). File MBR merupakan sebutan untuk *sector* dari file sistem yang berisi daftar seluruh partisi yang terdapat dalam *harddisk*. Tujuan dari pengidentifikasian file MBR adalah untuk mencari partisi yang aktif (yang dapat melakukan proses *booting*) dalam tabel partisi pada *harddisk* barang bukti.

	root:/investigation/images	٣	^	×
Eile	Edit Tabs Help			
total -rw-r- fathi- 1+0 re 1+0 re 512 by fathi-	<pre>116</pre>	t=1		

Gambar Proses Pencarian File MBR dengan Menggunakan *Tools* dd

Pencarian file MBR diambil dari sector pertama file image hasil imaging forensic (dalam penelitian ini File windXP.dd). Ukuran file MBR sebesar 512 bytes dan berada pada sector pertama. File MBR di beri label windows_mbr.img seperti yang terlihat pada gambar screenshot gambar dengan menguunakan tools forensik dd. Proses identifikasi selanjutnya dilakukan dengan membaca nilai hexadesimal dari file MBR. Dimana seluruh data digital ditampilkan dalam bentuk runtutan nilai heksa. Heksadesimal atau sistem bilangan basis 16 merupakan sebuah sistem bilangan yang menggunakan 16 simbol. Sistem bilangan ini digunakan untuk menampilkan nilai alamat memori dalam pemrograman komputer. Untuk menampilkan data ke dalam bentuk heksadesimal digunakan tool hexeditor (dalam DEFT Linux 7.2 menggunakan Ghex?)

•						٧	vind	low	s_ml	or.ir	ng -	GH	ex					3		
<u>File Edit Vie</u>	w	Win	dows	: H	elp															
000000FF60	6A	00	6A	00	FF	76	0A	FF	76	89	6A	00	68	00	70	6A `	j.jvv.	j.h.[j		
0000011001	6A	10	B4	42	88	F4	CD	13	61	61	73	0E	4F	74	0B	32 .	.jBaas.Ot			
00000121E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	бE	76	61	60	69 .	VaInv			
0000013264	20	70	61	72	74	69	74	69	6F	6E	20	74	61	62	60	65 d	partition	table		
0000014300	45	72	72	6F	72	20	60	6F	61	64	69	6E	67	20	6F	70 .	Error load	ling op		
000015465	72	61	74	69	6E	67	20	73	79	73	74	65	6D	00	4D	69 e	rating sys	tem.Mi		
0000016573	73	69	бE	67	20	6F	70	65	72	61	74	69	бE	67	20	73 s	sing opera	ting s		
0000017679	73	74	65	60	00	00	00	00	00	00	00	00	00	88	00	00 y	stem			
000018700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 .				
3000019800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 .		*****		
000001A900	00	00	00	00	00	00	00	00	00	00	00	2C	44	63	07	B3 .		.,Dc		
000001BA07	00001BA07 B3 00 00 80 01		01	00	07	FE	F8	FF	38	00	60	00	E0 .		.8					
300001CBA6	3F	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00 .	?			
90001DC 00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 .				
000001ED00	00	00	00	00	00	00	60	00	00	00	00	00	00	60	00	00 .		*****		
000001FE55	AA															0				
igned 8 bit:	7	_	_	_	_	Si	gned	32 b	it:	-459257				_	н	exadecimal	07			
Insigned 8 bit:	7					U	isign	ed 3.	z bit:	42	9450	8039			0	ctal:	007			
igned 16 bit:	-505				32	bit	loat		-nan					В	inary:	00000111				
Insigned 16 bit:	650	31				64	bit I	loat		1.2	0953	5e-3	12		5	tream Lengt	h: 8			
₩ s	how	little	end	ian d	lecor	fina						113	ihow	unsi	aner	and float a	s hexadecimal			

Gambar Tampilan Nilai Hexadesimal dari File MBR

Dengan mengacu pada ketentuan analisis file MBR yang di kemukakan dalam teori aplikas terkait File MBR, maka pada proses penelitian didapatkan nilai hexadesimal pada file windows_mbr.img sebagai berikut :

000001F	132	AA	_					-					_		_		
0000015																	
000001E	000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000010	3A6	3F	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B	٥7	B3	00	00	80	01	01	00	07	FE	F8	FF	38	00	00	00	E0
000001A	900	00	00	00	00	00	00	00	00	00	00	00	2C	44	63	07	B3
0000019	300	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000018	700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Gambar Nilai Hexadesimal File MBR windows_xp.img pada offset 0x1BE / byte 446 dengan panjang offset 16 byte Posisi awal partisi berada pada *offset* ke 0x1BE / byte 446 dengan ketentuan, nilai/value dari konten pada *offset* tersebut bernilai 80 yang menandakan partisi aktif. Maka nilai hexsadesimal yang diambil sepanjang 16 *offset* seperti yang terlihat pada gambar adalah sebagai berikut :

Tabel data hexa desimal partisi aktif diambil sepanjang 16 byte.

80 01 01 00 07 FE F8 FF 38 00 00 00 E0 A6 3F 01 Selanjutnya untuk menentukan type file sistem yang digunakan dalam partisi tersebut mengacu pada offset ke-4 (untuk perhitungan offset dimulai dari 0) sehingga nilai dari offset ke-4 adalah 07. Maka dapat dipastikan jenis file sistem yang digunakan merupakan jenis New Technology File System (NTFS). Jumlah sector yang terdapat pada partisinya di ketahu dari membaca nilai pada offset ke 12-16 yaitu dengan nilai [E0 A6 3F 01] untuk mengetahui jumlah sector, maka jumlah sectornya didapat dari nilai pada offset ke 12-16. Untuk perhitungannya di lakukan dari angka urutan offset terakhir, yaitu [01 3F A6 E0] di konversi menjadi bilangan desimal menjadi 20948494. Total sector yang dimiliki partisi sebanyak 20.948.494 unit dengan ukuran 512 byte per sector

Dari file MBR didapatkan informasi mengenai type jenis file sistem yang digunakan pada partisi *harddisk* komputer barang bukti dan jumlah *sector* yang digunakan dalam struktur tata letak partisi.

Selanjutnya setelah diketahui jenis partisi yang digunakan yaitu berupa *New Technology File System* (NTFS) maka tahapan selanjutnya adalah menampilkan tata letak partisi dalam sistem volume, yang meliputi tabel partisi dan disk label. *Tool* sleuth kit yang digunakan adalah mmls untuk mengetahui detail partisi yang terinstal pada *harddisk*.

DOS Partition Table Offset Sector: 0 Units are in 512-byte sectors Slot Start End Length Description 00: Meta 0000000000 0000000000 001 Primary Table (#0) 01: 0000000000 000000055 002: 0000000050 002: 0000000050 002: 000000055 002: 000000054 0000000054 0020948754	.uu	ls -t dos windXP	ı/images % mm	/investigatio	al-machine	i-virtua	fath
Offset Sector: 0 Units are in 512-byte sectors Slot Start End Length Description 00: Meta 000000000 00000000000 Primary Table (#0) 01: 0000000000 0000000055 0000000055 Unallocated 02: 00:00 00000005 0020948750 MTFS (0x07)					on Table	Partitio	DOS
Units are in 512-byte sectors Slot Start End Length Description 6000000000 0000000001 Primary Table (#0) 61: 0000000000 000000055 0000000055 Unallocated 02: 00:00 000000055 0020940750 HTF5 (0x07)					or: 0	et Secto	0ffs
Slot Start End Length Description 00: Meta 00000000000 00000000001 Primary Table (#0) 01: 0000000000 00000000055 0000000056 Unallocated 02: 0000000005 0020948759 0020948744 NTFS (0x07)				ctors	512-byte sec	s are in	Unit
00: Meta 0000000000 000000000 00000000 Primary Table (#0) 01: 00000000000 000000055 000000056 Unallocated 02: 00:00 000000055 0020948759 0020948764 NTFS (0x07)		Description	Length	End	Start	Slot	
01: 0000000000 000000055 000000056 Unallocated 02: 00:00 000000056 0020948759 0020948704 NTFS (0x07)	(#0)	Primary Table	0000000001	0000000000	0000000000	Meta	00:
02: 00:00 000000056 0020948759 0020948704 NTFS (0x07)		Unallocated	0000000056	0000000055	0000000000		01:
		NTFS (0x07)	0020948704	0020948759	0000000056	00:00	02:
03: 0020948760 0020971519 0000022760 Unallocated		Unallocated	0000022760	0020971519	0020948760		03:
fathi-virtual-machine/investigation/images %			n/images %	/investigation	al-machine	i-virtua	fath

Gambar Tampilan tabel partisi dari sistem Volume (tabel partisi)

Dari tampilan tabel partisi pada gambar 4.dengan *tools* mmls dapat diketahui lokasi *sector* dimana partisi dengan format NTFS terinstall, yaitu pada *sector* 0000000056 sampai *sector* 0020948704 *description* NTFS (0x07). Untuk mengetahui sistem operasi yang digunakan maka selanjutnya proses analisis terfokus pada partisi NTFS. Dengan menggunakan *tool* dc3dd investigator menyaring/memfilter file imaging hanya sebatas pada partisi NTFS saja, sehingga penelitian hanya terfokus pada satu partisi.

root:.	/investigation/images	۰.	•	х
<pre>Edit Tabs Help fathi-virtual-machine/investigation/images % dc3 hlog-windXP_boot.md5</pre>	dd if=windXP.dd ssz=512 iskip=56 cnt=20948704 hash=md5 of=windXP_bo	oot.	dd	1
dc3dd 7.0.0 started at 2013-08-20 04:28:33 +0700 compiled options: command line: dc3dd ifwindXP.dd ssz=512 iskip=55 cr sector size: 512 bytes (set) 1072573044 bytes (10 0) copied (100%), 251.559 s, 4	nt=20948704 hash=md5 of=windXP_boot.dd hlog=windXP_boot.md5 41 K/s			
<pre>input results for file `windXP.dd': 20948704 sectors in e01fd044a650750ac6ece0cc2a493f90 (md5)</pre>				n
output results for file `windXP_boot.dd': 20948704 sectors out				
dc3dd completed at 2013-08-20 04:32:44 +0700				I
fathi-virtual-machine/investigation/images %				IJ

Gambar Proses *Filtering* File Terfokus pada Partisi NTFS

Setelah pemecahan file tahapan selanjunya adalah mencari analisis umum dari file sistem. Dengan *tools* fsstat dari sleuth kit akan menampilkan rincian yang terkait dengan sistem file yang digunakan oleh *disk image* tersebut. *Output* dari *tools* ini adalah detai dari sistem file, mencakup informasi rentang meta data dan konten (*block atau sector*), rincian dari *superblock*, seperti waktu mount dan fitur lainnya.

root:/investigation/images * * *
<u>File Edit Tabs H</u> elp
<pre>fathi-virtual-machine/investigation/images % fsstat windXP_boot.dd FILE SYSTEM INFORMATION</pre>
File System Type: NTFS Volume Serial Number: CAE4A8DEE4A8CDCF OEM Name: NTFS Version: Windows XP
METADATA INFORMATION
First Cluster of MFT: 786432 First Cluster of MFT Mirror: 1309293 Size of MFT Entries: 1324 bytes Size of Index Records: 4096 bytes Range: 0 - 16944 Root Directory: 5
CONTENT INFORMATION
Sector Size: 512 Cluster Size: 4096 Total Cluster Range: 0 - 2618586 Total Sector Range: 0 - 20948702

Gambar Hasi Analisis Detail File Sistem dengan Fsstat

Hasil dari fsstat pada gambar diatas didapat informasi terkait tentang file *sistem type* dimana file sistem yang digunakan merupakan benar-benar tipe file sistem NTFS, *volume serial number file system* merupakan serial number dari sistem operasi yang digunakan yaitu CAE4A8DEE4A8CDCF, *version* dari sistem operasi yang digunakan yaitu Windows XP, konten dari meta data file sistem dan konten information dari struktur file sistemnya.

3. Proses Analisis data

Tahapan proses selanjutnya adalah proses analisis. Proses analisis dilakukan dengan pembuatan *Time Line History File* bukti digital. Pada proses pencarian ini hal pertama yang dilakukan seorang investigator adalah membuat *timeline* atau runtutan aktifitas yang telah dilakukan oleh komputer yang digunakan oleh pelaku kejahatan komputer. Pembuatan *timeline* ini mengacu pada file *image* partisi NTFS yang yang sebelumnya telah di analisis struktur maupun konten metadata nya. Dari *timeline* ini akan sangat membantu investigator untuk mneganalisa runtutan waktu kejadian kejahatan yang dilakukan oleh pelaku kejahatan komputer.

	root: Unvertigation (magoes)	
Terro para como	root:/investigation/images	
<u>File Edit</u> Tabs	Help	
root:/inves ×	root:/mnt ×	
fathi-virtual-ma /mt/vvidence/> Start processing /PreProcessing] /PreProcessing /PreProcessing /PreProcessing /PreProcessing /PreProcessing /PreProcessing /PreProcessing /PreProcessing /PreProcessing /DreProce	chine/investigation/images % log2timeline -p -r -f winxp -2 Asia/2 timeline.cvs file/dir //mrt/vridecvg/j file/dir //mrt/vridecvg/i winxpack for registry is: (SEAT) SE Asia Standard Time the timezone sectording to registry is: (SEAT) SE Asia Standard Time the timezone sectording to registry is: (SEAT) SE Asia Standard Time the timezone sectings are NOT overvittem so the settings might have the default system browser is: IEXRLOME.EXE (*C.\Program Files\Inte ces [*] -nohme) Dmable to determine the default browser for user fbwuser Dmable to determine the default browser for user default user Dmable to determine the default browser for user default user Dmable to determine the default browser for user localservice Dmable to the determine the default browser for user localservice Dmable to the determine the default browser for user browser for user localservice Dmable to the determine the default browser for u	to be a rrnet Ex FIREFOX

Gambar Proses pembuatan *timeline* dengan *tools* log2timeline

Dalam pembuatan *timeline* seperti terlihat pada gambar dalam menganalisis histori dari kegitan yang telah dilakukan pelaku kejahatan, menggunakan *tools* log2timeline. Dengan *tools* ini dapat membuat histori kegiatan komputer dengan susunan yang teratur karena log2timeline menyajikannya dalam bentu file table (excel format). Melalui log2timeline ini investigator dapat dengan mudah menemukan file-file yang dicurigai digunakan untuk tindak kejahatan. Diantaranya :

• Penemuan histori internet browser yang tidak wajar kepada salah satu laman website seperti terlihat pada gambar di bawah. Dimana terdapat pengaksesan laman secara terus menerus dalam rentang waktu yang sangat berdekatan terhadap alamat URL <u>http://fathimubarak.blogspot.com/</u>. Diduga terjadi *request* pengiriman paket data secara terus menerus sehingga mengakibatkan *traffic* pada halaman website.



Gambar Screenshot Aktifitas History Internet Browser yang Mencurigakan

• Pemasangan/installasi program aplikasi proxi. Yang diketahui software proxy merupakan sebuah teknik *hacking* yang digunakan untuk menyamarkan IP address saat berselancar di internet., yaitu sebuah software HSS.

	8	С	E	K
1	time	timezone	source	desc
37815	18:42:34	Asia/Jakarta	FILE	/Documents and Settings/LocalService/Desktop
37816	18:42:34	Asia/Jakarta	FILE	/Documents and Settings/All Users/Desktop/Hotspot Shield.Ink
37817	13:25:51	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37818	0:29:41	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37819	18:42:34	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37820	18:42:34	Asia/Jakarta	FILE	/System Volume Information/_restore[63A64DC2-55FB-411D-93FB-18E7A6D0070A]/RP4/A0
37821	0:29:41	Asia/Jakarta	FILE	/System Volume Information/_restore{63A64DC2-55FB-411D-93FB-18E7A6D0070A}/RP4/A0
37822	13:25:49	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37823	13:25:49	Asia/Jakarta	FILE	/System Volume Information/_restore{63A64DC2-55FB-411D-93FB-18E7A6D0070A]/RP4/A0
37824	18:42:35	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37825	0:29:41	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37826	0:29:41	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37827	13:25:53	Asia/Jakarta	FILE	/System Volume Information/_restore{63A64DC2-55FB-411D-93FB-18E7A6D0070A}/RP4/A0
37828	18:42:35	Asia/Jakarta	FILE	/System Volume Information/_restore(63A64DC2-55FB-411D-93FB-18E7A6D0070A)/RP4/A0
37829	18:43:07	Asia/Jakarta	FILE	/WINDOWS/Temp/hsspk.exe
37830	23:55:56	Asia/Jakarta	FILE	/WINDOWS/Temp/hsspk.exe
37831	18:43:02	Asia/Jakarta	FILE	/WINDOWS/Temp/hsspk.exe
37832	18:42:36	Asia/Jakarta	FILE	/WINDOWS/Prefetch/HSSPK.EXE-07D85C69.pf
37833	18:43:08	Asia/Jakarta	FILE	/WINDOWS/Prefetch/HSSPK.EXE-07D85C69.pf
37834	3:02:21	Asia/Jakarta	FILE	/System Volume information/_restore{63A64DC2-55FB-411D-93FB-18E7A6D0070A}/RP4/A0
37835	18-47-18	Asia/Inkasta	EHE	/System Volume Information/ restora/634640C2.55E8.4110.93E8.18E74600070A)/804/40

Gambar Penemuan Instalasi Program HSS Privat Browser

penemuan file yang telah Dari dihapus (deleted file) ditemukan applikasi DDos.bat seperti ditampilkan pada screenshoot pada gambar yang software tersebut diduga digunakan pelaku untuk melakukan serangan DDos ke halaman website http://fathimubarak.blogspot.com/. Pelaku diduga sengaja menghapus file DDos.bat, untuk menghilangkan bukti kejahatan komputer.

date	time	timezone	sourcetype	short
4/14/2008	2:20:17	Asia/Jakarta	D0F metadata	TimeStamp
4/14/2008	7:12:04	Asia/Jakarta	EXF metadata	TimeStamp
4/14/2008	1:37:08	Asia/Jakarta	DOF metadata	TimeStamp
4/14/2008	1:37:08	Asia/Jakarta	EXIF metadata	TimeStamp
4/14/2008	1:25:58	Asia/Jakarta	EXIF metadata	TimeStamp
4/14/2008	1:37:11	Asia/Jakarta	D05 metadata	TimeStamp
4/14/2008	1:58:53	Asia/Jakarta	DOF metadata	TimeStamp
8/18/2001	12:35:37	Asia/Jakarta	DOF metadata	TimeStamp
8/18/2001	3:52:57	Asia/Jakarta	EXIF metadata	TimeStamp
4/14/2008	1:37:00	Asia/Jakarta	EXF metadata	TimeStamp
8/18/2013	14:31:38	Asia/Jakarta	\$Recycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/Attack DDos.docx
8/18/2013	14:31:25	Asia/Jakarta	SRecycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos Attack tools/DDos.bat
8/18/2013	14:24:03	Asia/Jakarta	SRecycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos attacker
8/18/2013	14:24:40	Asia/lakarta	Sillecycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/Winter.log
8/18/2013	14:23:56	Asia/Jakarta	SRecycle.bin	DELETED C://Documents and Settings/Administrator/My Documents/DDos attacker/DDos.bat
8/18/2013	14:24:40	Asia/Jakarta	SRecycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/Blue hills.jpg
B/1B/2013	14:31:28	Ania/lakarta	SRecute bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos Attack tools
8/18/2013	14:26:00	Acia/takarta	Open XMI, Metadata	
8/18/2013	14:28:00	Asia/lakarta	Open XML Metadata	
a sin e su and			dente:	

Gambar Penemuan File Aplikasi DDos yang Telah di Hapus yang diduga Sebagai Alat

Bukti Kejahatan

Dari timeline tersebut di dapatkan beberapa petunjuk khusus jenis tindakan kejahatan komputer yang digunakan.. Jenis kejahatan komputer diketahui merupakan Serangan DDoS. DDos (bahasa Inggris: denial-ofservice attacks') adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang Tersebut. Setelah diketahui jenis serangannya maka selanjutnya adalah pencarian data terkait dengan kejahatan tersebut. Pencarian data terkait tersebut menggunakan teknik pencarian search string. Dimana teknik pencarian dilakukan berdasarkan nilai string file yang merujuk pada barang bukti.

Teknik pencarian dengan *search string* diawali dengan penentuan kata kunci terkait dengan kasus kejahatan yang telah di temukan tadi (dalam hal ini adalah DDos dan HSS). Pemilihan kata kunci tersebut didasari pada file yang diduga memiliki keterkaitan dan digunakan oleh pelaku dalam melakukan aksi kejahatan.

1999 J	root:/investigation/string
Eile Edit Tabs	Help
root:/inves ×	root:/inves × root:/inves ×
fathi-virtual-mac DDos HSS fathi-virtual-mac 3 NTFS 272 fXfX 309 A disk 418 NTLDR	hile/investigation/string % nore keyword.ht hime/investigation/string % srch strings -a + t d/images/wind0 ^a _bost.dd > string.bost.txt hime/investigation/string % nore string.bost.txt read error scourced is missing is compressed

Search

Hasil dari pencarian string search berupa file text yang memuat file-file yang memiliki keterkait dengan kata kunci kejahatan yang telah kita tentukan tadi yaitu HSS dan DDos. Pencarian dengan metode string search juga memberikan informasi alamat cluster dari file terkait. Seluruh aktifitas file yang terkait dengan kata kunci akan ditampilkan secara detail. Setelah menganalisis posisi cluster yang dicurigai, maka selanjtunya pengecekan status terfokus pada cluster yang diduga memiliki keterkaita dengan barang bukti, menggunakan tool forensik sleuth kit, blkcat pada cluster yang dianggap memiliki keterkaitan barang bukti (cluster 505). Setelah menentukan cluster target selanjutnya mencari file yang memiliki keterkaitan dengan keyword yang telah di tentukan tadi. Teknik pencarian kali ini menggunakan grap pada cluster 505.

Elle Edit Dab telp Delle Dat Dab telp Sector Data Sector (Sector Data Sector Data Se			root:/inves	stigation/string	7 A X
noor_Inuer, * noor_Inuer, * noor_Inuer, * India (Intia) = notion (Integrate Arrows Integrate Arrows Int	Eile Edit Ia	bs Help			
Tahl-uirtual-auchute/Levestigatian/string % prop -1 -f keyverd.txt string.boot.txt > hints.txt Tahl-uirtual-auchute/Levestigatian/string % prop -1 -f keyverd.txt string.boot.txt > hints.txt Table3205 2005277 Miss 2005277 Miss 2005277 Miss 40080273 STSNSS 40080273 STSNSS 40080273 STSNSS 40080273 STSNSS 40080273 STSNSS 4008028 Miss 6009038 Miss 6009038 Miss 6009038 Miss 8009038 Miss 8009038 Miss 8009038 Miss 8009038 Miss 8009038 Miss 8100048 Miss 810048 Miss 810048 Miss 810048 Miss 81048 M	root:/inves	× root:/inves ×	root:/inves ×		
81941248 hsswd flags 89872248 HssTrayService	fathi-virtual fathi-virtual 5827771 xH 2666323 20432768 VH 2658775 HS 3224004 hs 3224004 hs 3224004 hs 52197055 HS 52197055 HS 52197055 HS 52290451 2h 64546488 th 61450289 Wh 655930H HS 72604494 7z 79605968 rp 7901708 HS 72604494 7z 79605968 rp 7901708 HS 81523848 Ha 81523876 HH 81523876 HH 815241047 bh	-machine/investig machine/investig hss hss tis do do do do do do do do do do do do do	ntlav/string % grep stion/string % more / afrpt.gif?afcid=1702	-i -f kepend.txt string.boot.txt > hints.txt hints.txt	t=\s
	81941248 hs 89872248 Hs	swd_flags sTrayService			

Gambar Screenshoot Hasil Pencarian dengan grep

Hasil dari pencarian dengan grep seperti yang terlihat pada gambar inilah seluruh aktifitas file komputer yang digunakan pelaku kejahatan. Penemuan aktifitas penggunaan file DDos pada komputer yang digunakan sebagai alat kejahatan. Aktifitas diketahui dilakukan pada directory C:\Document and Setting\Administrator\My Document\Ddos attacker\DDos.bat.



Gambar Screenshot Penemuan Sting File DDos

Selain itu diketahui juga bahwa sebelumnya pelaku menginstal *software* aplikasi HSS atau Hotspot Shield. HSS merupakan *Software*/Aplikasi untuk merubah settingan IP *address* Internet (proxy). Untuk mengelabuhi posisi pelaku kejahatan dalam melakukan serangan seperti yang terlihat pada gambar di bawah.



Gambar Screenshoot Penggunaan HSS Sebagai Pengaturan Proxy Komputer

Setelah diketahui melalui *software online* pendeteksi alamat IP (where is my IP) bahwa alamat IP yang digunakan adalah 46.137.152.2 dan merupakan alamat IP dari Negara Irlandia.





Gambar Screenshoot Hasil Pendeteksian Alamat IP menggunakan software online whatismyipaddress.com

Selanjutnya pelaku menjalankan program DDos.bat untuk melakukan penyerangan ke halaman website target. Dengan mengirimkan paket kiriman data yang tidak penting sangat banyak secara terus menerus (*flooding file*) dapat mengakibatkan *traffic* pada lalu lintas data pada website yang dapat berakibat website menjadi lamban untuk diakses atau bahkan dapat berakibat website *down* (tidak bias diakses sama sekali).

0	root:/investigation/string	ж	
Eile Edit	Tabs Help		
root:/inves.	× root:/inves × root:/inves ×		
ignebifyidith Forms Light Verticalieifyidith Lefbands Arrowebifyidith Ugwards Arrowebifyidith Highbands Arrowebi def Downards Arrowebifyidith Black Sugarebifyidith Mite CircleInterlinear Annotation AnchorInterlinear Annotatio n SeparatorInterlinear Annotation TeminatorObject Replacement CharacterReplacement Character S9679539 Itile 0005 Attack			
596705386 echo = Hacking DDOS by anonymous =			
596705544 echo + Name : DDOS Wapsite Cyber +			
S96706/85/33 echo DDOS WITH BATCHTILE			
596786841		- 11	
59676611 acto DD05			
600437151	OHSSP	- 11	
604579142	Jclahss'	- 11	
607001990	HSSW	- 11	
607502842	AHSS	- 11	
608125512	=dbSSt>=dhSSt.	- 11	
610206498	!@HSS	- 11	
610500274	;WCHSS	- 11	
611321513	hSSS	- 11	
615235122	hssejiW	- 11	
615849488	SHSS	- 11	
617634531	x2hSsDo	- 11	
621294756	Whssq6	- 11	
621681088	If you cannot access the website while connected and disconnected from Hotspot Shield,	<a td="" 🕦<="">	
href="mailt	co:support@hsselite.com">email us. Please send a screenshot of that webpage and error messages (:	if	
		_	

Gambar Detail History Eksekusi File DDos.bat



Gambar Screenshoot Paket Data yang Dikirim Aplikasi DDos.bat

Proses Pembuktian

Pembuktian kejahatan DDos, dilakukan berdasarkan data temuan dari proses analisis data temuan. Pada data *timeline history* ditemukan beberapa file yang dihapus, diantaranya file DDos.bat yang digunakan oleh pelaku untuk melakukan serangan DDos. Diketahui pada tanggal 08/18/2013, pukul

14:31:25 terdapat aktifitas penghapusan file dari direktori C:/Document and Setting/Administrator/My Document/DDos Attack tools/DDos.bat (seperti yang terdapat pada gambar .

8/18/2013 14:31:28 Asia/lakarta \$Recycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos Attack tools
8/18/2013 14:24:40 Asia/Jakarta \$Recycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/Blue hills.jpg
8/18/2013 14:23:56 Asia/Jakarta SRecycle bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos attacker/DDos.
8/18/2013 14:24:40 Asia/Jakarta 58ecycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/Winter.jpg
8/18/2013 14:24:03 Asia/Jakarta SRecycle.bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos attacker
8/18/2013 14:31:25 Asia/lakarta 5Recycle bin	DELETED C:/Documents and Settings/Administrator/My Documents/DDos Attack tools/DC
8/18/2013 14:31:38 Asia/Jakarta 5Recycle bin	DELETED Cr/Documents and Settings/Administrator/My Documents/Attack DDos.docx

Gambar Screenshoot Detail File yang Dihapus pada direktori C:/Document and Setting/Administrator/My Document/DDos Attack tools/DDos.bat

Pembuktian dilakukan dengan melakukan *mount read only* pada file *image* windXP_boot.dd untuk menemukan file yang telah dihapus. Dari direktori RECYCLER/S-1-5-21-1220945662-1482476501-1644491937-500 ditemukan file Dc1.bat.



Gambar Screenshoot File yang Dihapus pada Direktori RECYCLER/S-1-5-21-1220945662-1482476501-1644491937-500

Setelah file Dc1.bat dieksekusi terbukti bahwa file tersebut merupakan *software* DDos yang digunakan pelaku kejahatan komputer untuk melakukan serangan DDos ke halaman website dengan alamat





Gambar Screenshoot File Dc1.bat yang merupakan software yang digunakan untuk melakukan serangan DDos.

Hasil Penelitian

Berdasarkan data yang ditemukan selama penelitian berlangsung melalui hasil observasi dan dokumentasi, maka akan dideskripsikan hasil temuan yang didapat selama penelitian. Objek penelitian diambil dari sebuah komputer yang diduga memiliki keterkaitan dengan kasus tindak kejahatan DDos terhadap sebuah akun web blog dengann URL

http://fathimubarak.blogspot.com. DDos adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang Tersebut. Komputer yang diduga memiliki keterkaitan dengan tindak kejahatan tersebut di analisis dengan metode file sistem analisis dan dilakukan pembuktian apakah komputer benar memiliki keterkaitan dengan tindak kajahatan komputer. Penelitian dilakukan berdasarkan data hasil *imaging harddisk* pada komputer yang diduga memiliki keterkaitan dengan kasus kejahatan, berupa file windXP.img. Dari hasil penelitian yang dilakukan ditemukan beberapa history file yang dianggap mencurigakan dan diduga memiliki keterkaitan dengan kasus kejahatanDDos, diantaranya :

1. History dari aktifitas internet browser. Dimana pada history timeline terdapat akses ke halaman *webblog* dengan alamat URL http://fathimubarak.blogspot.com/ terjadi akses data secara terus menerus seperti yang terdapat pada gambar *screenshot* pada gambar.

2. Dari hasil penelitian ditemukan sebuah software atau program aplikasi Hot Spot Shiled (HSS) privat browser. Yang diketahui software ini merupakan sebuah tool untuk melakukan teknik untuk melakukan proxy, sehingga identitas komputer anda berupa IP menjadi tersembunyi dikarenakan yang dikenali server yang direquest adalah IP dari server proxy. Proxy ini pada umumnya digunakan untuk kegiatan menyembunyikan identitas atau untuk menghindari pemblokiran akses ke suatu server. Diketahui bahwa alamat ip yang digunakan merupakan alamat IP 46.137.152.2 dan merupakan alamat IP dari Negara Irlandia seperti terlihat pada gambar.

Dari penemuan file yang telah 3. dihapus (deleted file) ditemukan applikasi DDos yang di duga untuk melakukan serangan laman webblog URL ke http://fathimubarak.blogspot.com berupa file DDos.bat seperti terlihat pada screenshoot gambar aktifitas yang dilakukan file DDos.bat adalah dengan mengirimkan file-file sampah (seperti terlihat pada gambar, dengan tujuan untuk memberikan traffic menghabiskan sumber yang dimiliki (resource) oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan sehingga secara tidak langsung benar mencegah pengguna lain untuk memperoleh akses layanan dari laman webblog tersebut

Dari ketiga hasil temuan bukti digital dan hasil pembuktian yang merujuk pada penggunaan tools Ddos.bat terbukti bahwa komputer tersebut benar digunakan untuk melakukan kejahatan DDos.

4. SIMPULAN

Tindak kejahatan komputer yang terjadi pada komputer merupakan salah satu potensi aktivitas ilegal dengan memanfaatkan kemampuan komputer dalam memberikan informasi. Dari sisi penegak hukum, adanya celah kejahatan ini harus dihadapi dengan kemampuan pengetahuan tentang karakteristik barang elektronik/digital dan teknik analisi data yang mendukung supaya penyelidikan dan penanganan barang bukti digital yang relevan. Dalam penelitian ini telah menunjukkan bagaimana skema kejahatan komputer DDos yang telah dilakukan serta bagaimana teknik mendapatkan informasiinformasi penting terkait tindak kejahatan yang sehingga dilakukan dapat mendukung pembuktiannya.

Berdasarkan pada uraian pada bab-bab di atas, maka dapat diambil suatu kesimpulan :

Dari hasil penelitian dengan 1. menggunakan moteode analisis file sistem Windows terhadap file windXP.dd yang merupakan hasil imaging harddisk komputer yang dicurigai, diperoleh hasil berupa aktifitasaktifitas mencurigakan seperti histori dari aktifitas internet browser. Dimana pada history timeline terdapat akses ke laman website (url http://fathimubarak.blogspot.com) dengan waktu akses yang tidak wajar dan terjadi pengiriman pake data yang tidak jelas terus menerus. Pemasangan/installasi program Hot Spot Shield (HSS) yang digunakan sebagai software penyamaran IP addres pelaku dalam melakukan kejahatan yang setelah dideteksi merupakan alamat IP luar negeri (Irlandia). Dari hasil temuan-temuan aktifitas tersebut, serta merujuk pada penemuan file yang telah dihapus (deleted file) ditemukan applikasi DDos yang di duga untuk melakukan serangan ke laman website, berupa sofware aplikasi DDos.bat. Ini membuktikan bahwa komputer tersebut terbukti sebagai alat bukti kejahatan yang digunakan untuk melakukan serangan DDos.

Saran

Dari hasil penelitian yang dilakukan pada Indonesia Scurity Incident Response Team in Internet Infrastructure / Coordinator Center (ID-SIRTII/CC), maka penulis memberikan beberapa saran untuk para investigator dalam melakukan pross analisis digital forensik file sistem Windows guna mencari kebenaran dari sebuah kasus kejahatan komputer, diantaranya:

1. Memahami dan mematuhi seluruh prosedur digital forensik dalam proses investigasi dan analisis barang bukti elektronik dan barang bukti digital. Sebab dalam proses investigasi digital forensik prosedur investigasi sangatlah penting. Sebab ini akan berpengaruh pada keabsahan data hasil temuan dilapangan, dan dapat memperkuat keabsahan barang bukti digital.

Gunakan *software/hardware* forensik yang terupdate (terkini) dan sesuai dengan peruntukannya. Karena dengan menggunakan perlengkapan *software* dan *hardware* dapat mempercepat proses investigasi, sehingga dapat menghemat waktu penyelidikan dengan hasil yang lebih maximal dan lebih akurat tentunya.

5. DAFTAR PUSTAKA

- [1] Yudi Prayudi, Dedy Setyo Afrianto "Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik", 2012.
- [2] Ardian Aji Dharma. M, "DOS, DDOS & cara penaggulangannya", 2006.
- [3] Nuh Al-Azhar. Muhammad, "Digital Forensic Panduan Praktis Investigasi Komputer", Penerbit Salemba Infotek : 2012.
- [4] EC-Council|Press, "Computer Forensic Investigating Harddisk, File & Operating System", 2010.
- [5] Yudi Prayudi, "Jenis File Sistem", dalam http://forensikadigital.wordpress.com/20 13/01/20/jenis-file-system/ yang di akses pada tanggal 5/8/2013 6:18:55 PM.
- [6] Carrier. Brian, "File System Forensic Analysis", 2005.
- [7] Deft Linux, dalam <u>http://www.deftlinux.net/about/</u> yang di akses pada tanggal 7/8/2013 6:18:55 PM.
- [8] Fratepietro, Stefano, Sandro Rossetti, dan Paolo Dal Checco. "*Deft 7 Manual Book*", 2012.
- [9] Widyanto. Daniel, "Evaluasi Autopsy dan Sleuthkit", 2004.
- [10] Wahana Komputer, "*Network Hacking dengan Linux Backtrack*", Penerbit Andi : 2012.