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

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

Muhammad Fathi Mubara[1], Dadang Rusmana[2], Siti Madinah Ladjamuddin[3]
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
[1]fathimubarak@ymail.com, [2]dadangrusmana@istn.ac.id, [3]citymadinah07@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 http://fathimubarak.blogspot.com. 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 (*store*) kemudian 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 dari file sistem, *area block* tempat 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 Ţersebut[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:

1. Pengumpulan Bukti-Bukti Digital

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

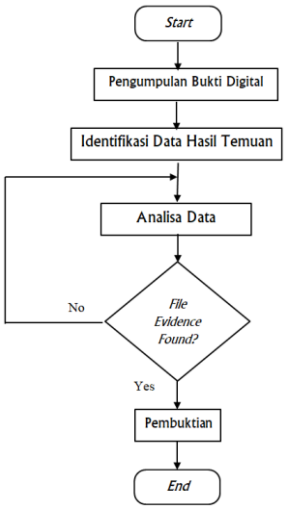
Analisa data dilakukan dengan dua cara, yaitu dengan melakukan analisis terhadap *timeline history file* dan analisis *history file*.

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 hasil *imaging* windXP.dd. 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

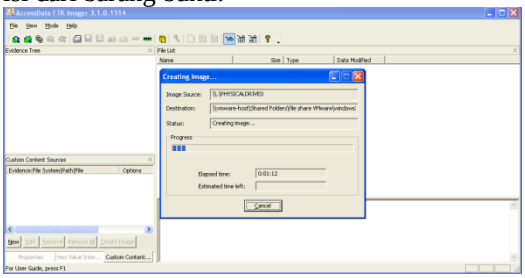
Pembahasan Penelitian

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*" yang artinya kemampuan manusia (investigator) lebih diutamakan ketimbang peralatan atau persenjataan. Peralatan yang canggih dan lengkap, tidak akan berguna jika penggunanya tidak dapat mengunakannya.

Proses penelitian dilakukan 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

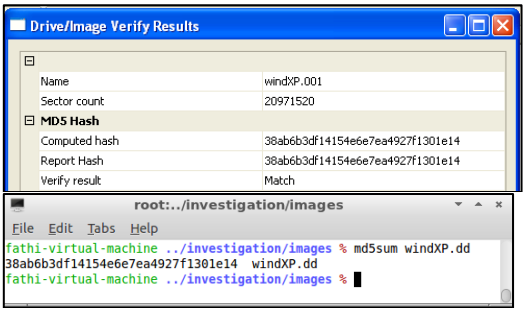
Barang bukti elektronik seperti komputer yang telah ditemukan di tempat kejadian perkara diambil *harddisk*-nya yang berfungsi sebagai media penyimpanan untuk selanjutnya dilakukan proses *forensic imageing* (akuisisi). Sebelum dilakukan proses akuisisi, komputer yang digunakan untuk kegiatan akuisisi (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.



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.

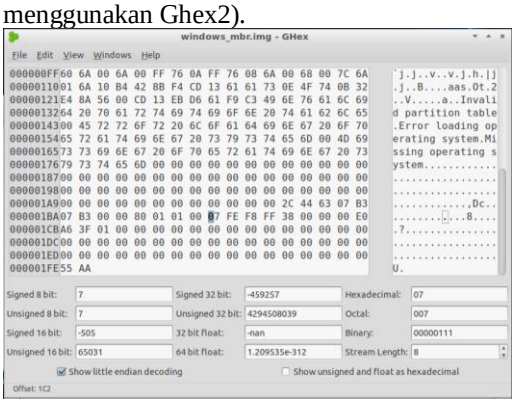
2. Proses Identifikasi Data Hasil Temuan

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.

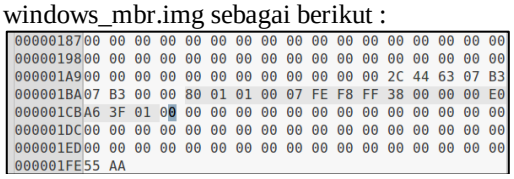
Gambar Proses Pencarian File MBR dengan Menggunakan *Tools* dd

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 Ghex2).



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 :



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 *0*x1BE / 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.*

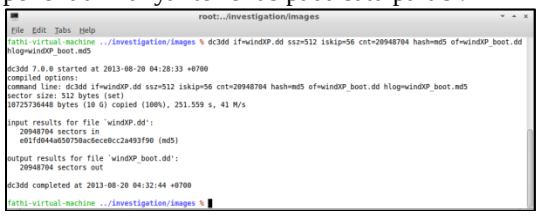
Dari file MBR didapatkan informasi mengenai type jenis file sistem yang digunakan pada partisi *harddisk* komputer barang bukti dan jumlah *sector* yang digunakan dalam struktur tata letak partisi.

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.*.

Gambar Tampilan tabel partisi dari sistem Volume (tabel partisi)

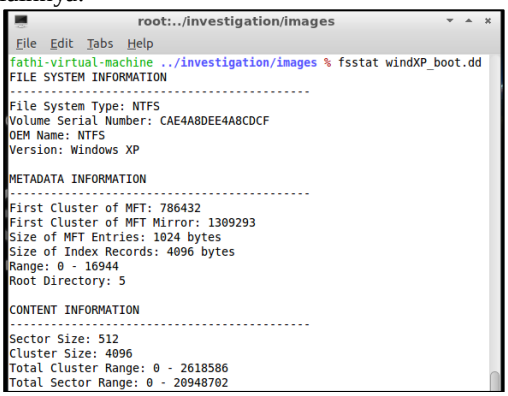
Dari tampilan tabel partisi pada gambar 4.dengan *tools* mmls dapat diketahui lokasi *sector* dimana partisi dengan format NTFS terinstall, yaitu pada *sector* 0000000056 sampai *sector* 0020948704 *description* NTFS (0x07). Untuk mengetahui sistem operasi yang digunakan maka selanjutnya proses analisis

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.



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.



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.

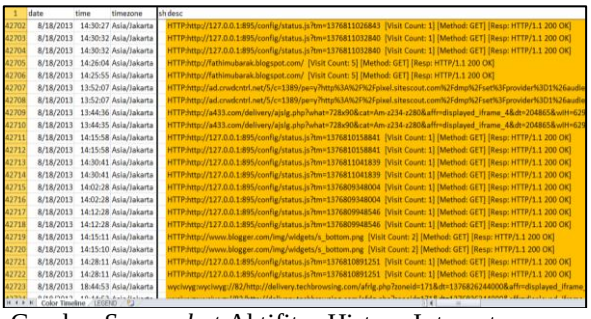
3. Proses Analisis data

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.

Gambar Proses pembuatan *timeline* dengan *tools* log2timeline

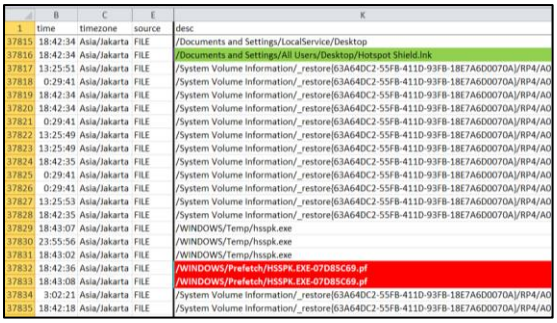
Dalam pembuatan *timeline* seperti terlihat pada gambar dalam menganalisis histori dari kegitan yang telah dilakukan pelaku kejahatan, menggunakan *tools* log2timeline. Dengan *tools* ini dapat membuat histori kegiatan komputer dengan susunan yang teratur karena log2timeline menyajikannya dalam bentu 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 http://fathimubarak.blogspot.com/. Diduga terjadi *request* pengiriman paket data secara terus menerus sehingga mengakibatkan *traffic* pada halaman website.



Gambar *Screenshot* Aktifitas History Internet Browser yang Mencurigakan

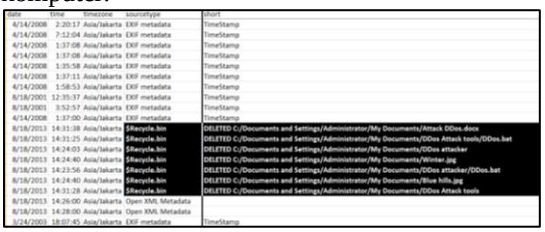
- Pemasangan/installasi program aplikasi proxi. Yang diketahui s*oftware* proxy merupakan sebuah teknik *hacking* yang digunakan untuk menyamarkan IP *address* saat berselancar di internet., yaitu sebuah *software* HSS.



	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.lnk
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	18:42:18	Asia/Jakarta	FILE	/System Volume Information/_restore{63A64DC2-55FB-411D-93FB-18E7A6D0070A}/RP4/A0

Gambar Penemuan Instalasi Program HSS Privat Browser

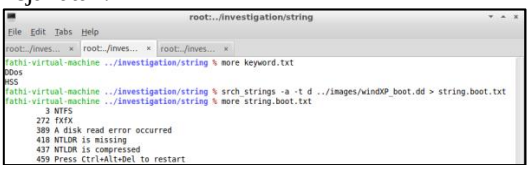
- Dari penemuan file yang telah dihapus (*deleted file*) ditemukan applikasi DDos.bat seperti ditampilkan pada *screenshoot* pada gambar yang *software* tersebut diduga digunakan pelaku untuk melakukan serangan DDos ke halaman website http://fathimubarak.blogspot.com/. Pelaku diduga sengaja menghapus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



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-of-service 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 Ţersebut. 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.

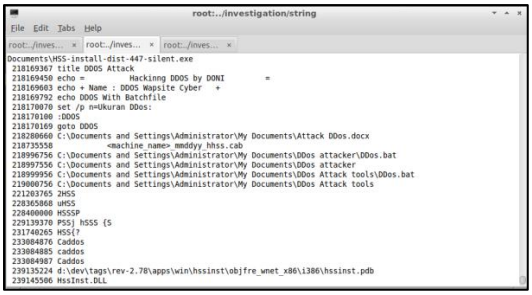


Gambar *Screenshoot* Pencarian dengan *String Search*

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.

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.

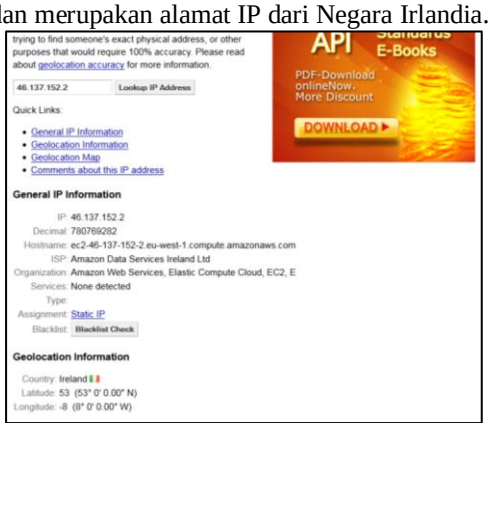


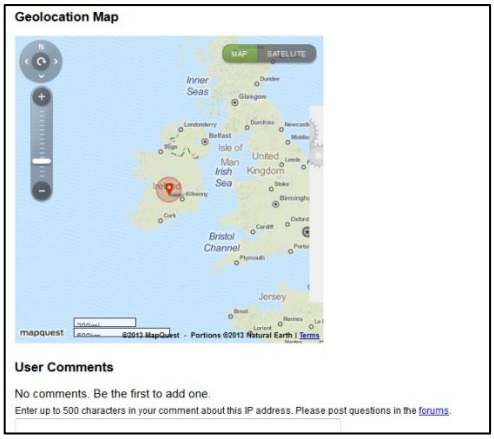
Gambar S*creenshot* Penemuan Sting File DDos

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

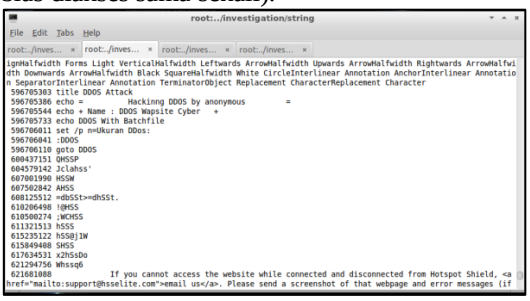
Setelah diketahui melalui *software online* pendeteksi alamat IP (where is my IP) bahwa alamat IP yang digunakan adalah 46.137.152.2 dan merupakan alamat IP dari Negara Irlandia.



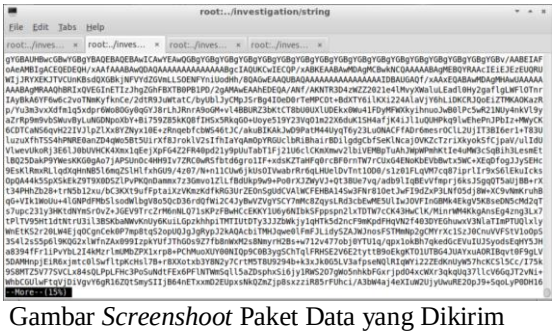


Gambar *Screenshoot* Hasil Pendeteksian Alamat IP menggunakan *software online* whatismyipaddress.com

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).



Gambar Detail *History* Eksekusi File DDos.bat



Gambar *Screenshoot* Paket Data yang Dikirim Aplikasi DDos.bat

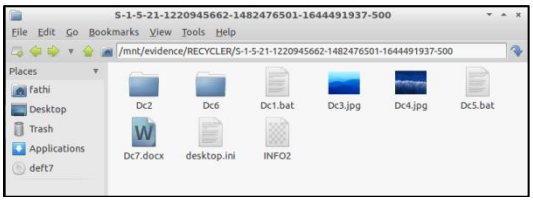
Proses Pembuktian

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 .

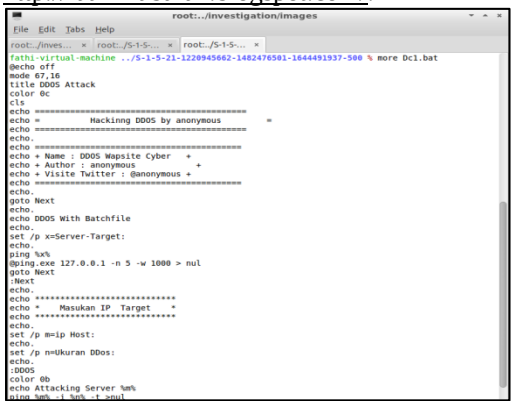
Gambar *Screenshoot* Detail File yang Dihapus pada direktori C:/Document and Setting/Administrator/My Document/DDos Attack tools/DDos.bat

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 http://fathimubarak.blogspot.com/.



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 Ţersebut. 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 s*oftware* 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.
3. Dari penemuan file yang telah dihapus (*deleted file*) ditemukan applikasi DDos yang di duga untuk melakukan serangan ke laman *webblog* URL 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 (*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 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 informasi-informasi penting terkait tindak kejahatan yang dilakukan sehingga dapat mendukung pembuktiannya.

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

1. Dari hasil penelitian dengan menggunakan moteode analisis file sistem Windows terhadap file windXP.dd yang merupakan hasil *imaging harddisk* komputer yang dicurigai, diperoleh hasil berupa aktifitas-aktifitas 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/2013/01/20/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 http://www.deftlinux.net/about/ 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.