



# Laporan Investigasi Forensik 2020

[ LAPORAN INVESTIGASI FORENSIK DIGITAL PENYERANGAN SERVER ]



S1 Teknik Komputer  
Fakultas Teknologi Elektro  
Telkom University  
Jln. Telekomunikasi, Terusan Buah Batu  
Bandung, 40257, Indonesia

---

## DAFTAR ISI

I. PEMBUKAAN	3
II. PENDAHULUAN	3
III. BARANG BUKTI	3
IV. MAKSUD PEMERIKSAAN	4
V. PROSEDUR PEMERIKSAAN	5
A. PROSES PENERIMAAN BARANG BUKTI	5
B. WAKTU DAN TEMPAT	5
VI. HASIL PEMERIKSAAN	5
VII. KESIMPULAN	25
A. HASIL ANALISIS	25
B. KESIMPULAN	33
VIII. PENUTUP	33

## I. Pembukaan

Tugas Besar mata kuliah komputer forensik kali ini adalah mengidentifikasi kasus penyerangan terhadap server sebuah perusahaan, dalam laporan ini akan diungkap apa bentuk penyerangan server, siapa yang melakukan penyerangan, kapan penyerangan terjadi, dimana penyerangan terjadi, hingga bagaimana penyerangan dapat terjadi.

## II. Pendahuluan

Komputer Forensik adalah sebuah ilmu dalam menyelidiki jejak forensik yang dilakukan oleh sebuah perangkat komputer. Komputer forensik dapat dilakukan oleh siapa saja yang mengerti betul tentang perangkat Komputer.

Dalam laporan ini berisikan langkah Langkah pencarian fakta hingga metode metode apa saja yang digunakan untuk mendapatkan jawaban dari barang bukti yang ada.

## III. Barang Bukti

Barang bukti yang dikirimkan dan diberikan oleh pak Faris adalah sebuah file bernama CASE.tar.bz dengan ukuran 577MB untuk kemudian dianalisis

## IV. Maksud Pemeriksaan

Sesuai dengan permintaan untuk mengungkap kasus ini. Adapun beberapa informasi yang dibutuhkan adalah :

- Siapa yang melakukan serangan?
- Kepada siapa serangan dikirimkan?
- Kapan serangan dikirimkan?
- Kapan serangan dieksekusi?
- Berapa alamat ip server c&c ?
- Apa nama file dropper?
- Apa nama file backdoor?
- Apa proses yang digunakan backdoor?
- Berapa proses id (pid) backdoor pada setiap komputer/server yang terinstal backdoor?
- User apa yang digunakan pada serangan?
- Berapa level akses yang dimiliki penyerang?
- Script \*.bat apa saja yang diletakkan pada setiap perangkat?
- Apa saja isi masing-masing file \*.bat?
- Directory/folder apa yang digunakan penyerang untuk meletakkan tools yang digunakan?
- Apa saja nama file yang dicuri?
- Apa saja isi file yang dicuri?
- Apa md5sum dari pump1.dwg?
- Komputer/server mana saja yang terkompromikan dan perlu segera ditangani?
- User account mana saja yang terkompromikan dan perlu segera ditangani?
- Apa ada komputer/server lain yang perlu dianalisis?

## V. Prosedur Pemeriksaan

### a. Proses Penerimaan Barang Bukti

- Pada proses pengerjaan Tugas Besar Mata Kuliah Komputer Forensik, kami menggunakan Linux sebagai operating sistem dalam proses pengolahan. Adapun beberapa tahapan dalam pengerjaannya adalah sebagai berikut.
- Dalam proses penganalisan ini, terdapat 3 orang yang melakukannya dengan 3 komputer yang berbeda. Hal ini bertujuan untuk meningkatkan efisiensi dari pengerjaan tugas ini. Orang tersebut adalah sebagai berikut :
  - Novansyah Herman (1103164005)
  - Naufal Fais Hakim (1103160030)
  - Lili Djunaedi (1103164168)
  - Rifky Ardi Eka Saputra (1103164054)
  - Excel Kumara Sudiantoro (1103164078)

### b. Waktu dan Tempat

Proses eksaminasi barang bukti dilakukan pada:

Waktu : Kamis, 30 April 2020, pukul. 18.00 – 03.00 WIB

Tempat : Tempat tinggal masing-masing

## VI. Hasil Pemeriksaan

Hasil pemeriksaan merupakan hasil eksaminasi barang bukti, yaitu:

- a. Pertama-tama mendownload barang bukti berupa file CASE.tar.bz2 yang sudah diberikan oleh Bapak Faris melalui link <https://s.id/fTK3X>, lokasi penyimpanan barang bukti :
  - Pada komputer Naufal Fais, file CASE.tar.bz2 disimpan kedalam directori ~/Documents/KomFor/TuBes/Percobaan.
  - Lalu pada komputer Novan, file CASE.tar.bz2 disimpan di dalam directori ~/Downloads
  - Sedangkan pada komputer Lili Djunaedi, file CASE.tar.bz2 disimpan di dalam directori ~/Desktop/tubes/bukti/proses.
- b. Analisis yang pertama kali dilakukan adalah mengetahui ekstensi sesungguhnya dari barang bukti, metode yang dilakukan menggunakan fungsi xxd tujuannya mendapatkan magic number atau nilai file signature dari file tersebut.

```

lilidjunaedi@lilidjunaedi-VirtualBox:~$ cd Desktop
lilidjunaedi@lilidjunaedi-VirtualBox:~/Desktop$ cd tubes
lilidjunaedi@lilidjunaedi-VirtualBox:~/Desktop/tubes$ cd bukti
lilidjunaedi@lilidjunaedi-VirtualBox:~/Desktop/tubes/bukti$ cd proses
lilidjunaedi@lilidjunaedi-VirtualBox:~/Desktop/tubes/bukti/proses$ xxd CASE.tar
.bz2 | head
00000000: 425a 6836 3141 5926 5359 628d 393f 0277  BZh61AY&SYb.9?.w
00000010: faff 907e 9003 fc44 63ff f03f ffff f0ff  ...~...Dc..?....
00000020: ffff fa04 0061 54df 7dbd 5f4b 43d0 006e  ....aT.}._KC..n
00000030: d903 7418 0aa1 5b6d d8f5 e940 154a ae81  ..t...[m...@.J..
00000040: 456f 6edb cbcd 883a 5340 0000 6e0f a280  Eon...:S@..n...
00000050: 0044 93c8 0032 a011 0500 0002 a9aa 3432  .D...2.....42
00000060: 00f0 0000 0000 007d e000 0000 0e80 0000  ....}......
00000070: 0000 0000 0000 0000 0a3d e00f beb6 3402  ....==....4.
00000080: ec00 0000 0000 0000 0034 0000 0a03 c800  ....4.....
00000090: 3c72 801e 001a fa0d 5000 0001 db00 5500  <r.....P.....U.

```

- c. Magic number yang didapatkan seperti gambar diatas adalah 42 5a 68 untuk file barang bukti, kemudian di cek file signature tersebut untuk menentukan ekstensi.

42 5A 68

BZh

BZ2, TAR.BZ2, TBZ2, TB2 [bzip2](#) compressed archive

DMG Mac Disk image (BZ2 compressed)

- d. Setelah dipastikan file tersebut ternyata sudah sesuai ekstensinya yaitu file terkompresi dengan metode bzip2, file siap diekstraksi melalui terminal dengan cara :

- Buka terminal (ctrl+alt+t).
- Masuk kedalam directory dimana file CASE.tar.bz2 disimpan, misal pada komputer Naufal Fais, (cd Documents/KomFor/TuBes/Percobaan).
- Ekstrak file CASE.tar.bz2 dengan command (tar -xf ).

```

Terminal
Sel Apr 28, 15:36:11
arnayysz@arnayysz-VirtualBox: ~/Documents/KomFor/TuBes

File Edit View Search Terminal Help
arnayysz@arnayysz-VirtualBox:/home$ ls
arnayysz
arnayysz@arnayysz-VirtualBox:/home$ cd arnayysz
arnayysz@arnayysz-VirtualBox:~$ ls
Desktop  Downloads  Music      Public  Templates
Documents examples.desktop Pictures snap  Videos
arnayysz@arnayysz-VirtualBox:~$ cd Documents/ Komputer Forensik
bash: cd: too many arguments
arnayysz@arnayysz-VirtualBox:~$ cd Documents
arnayysz@arnayysz-VirtualBox:~/Documents$ cd Komputer Forensik
bash: cd: too many arguments
arnayysz@arnayysz-VirtualBox:~/Documents$ cd KonFor/TuBes
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes$ ls
CASE dummy Percobaan tubes
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes$ cd Percobaan
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan$ tar -xf CASE.tar.bz2

```

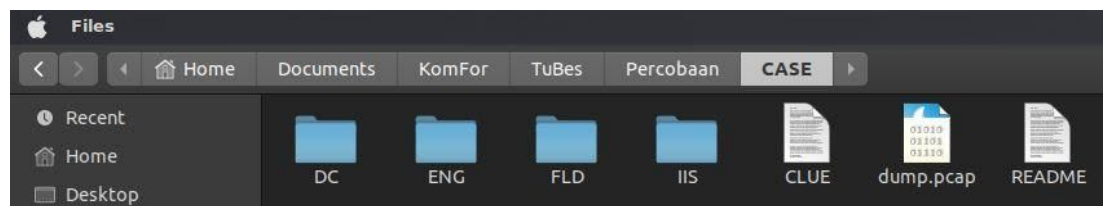
- e. Setelah melakukan pengekstrakan, masuk kedalam folder CASE dan mengecek apa saja isi didalam folder CASE dengan command (ls).

```
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan$ ls
CASE CASE.tar.bz2
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan$ cd CASE
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ ls
CLUE DC dump.pcap ENG FLD IIS README
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$
```

- f. Dalam folder Case terdapat 4 folder dan 3 file dimana dari 3 file hanya 1 file yang memiliki ekstensi yaitu dump.pcap, sisanya tidak berextensi, sehingga perlu dilakukan analisis file signature untuk mengetahui ekstensi

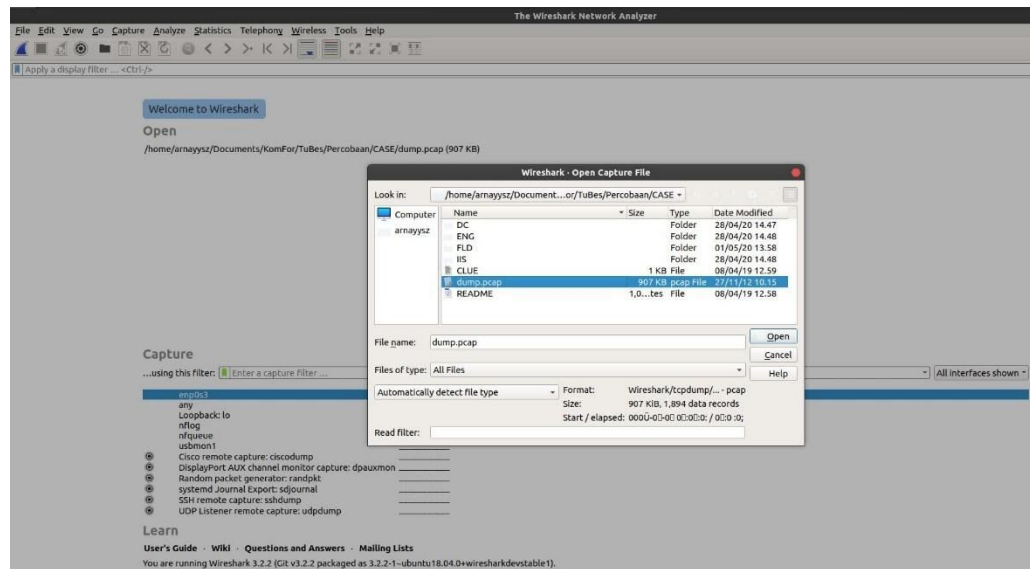
```
lilidjunaedi@lilidjunaedi-VirtualBox:~/Desktop/tubes/bukti/proses/CASE$ xxd CLUE | head
00000000: 5065 7274 616e 7961 616e 2064 6920 6261  Pertanyaan di ba
00000010: 7761 6820 6d65 7275 7061 6b61 6e20 7065  wah merupakan pe
00000020: 7475 6e6a 756b 2079 616e 6720 6269 7361  tunjuk yang bisa
00000030: 2064 6967 756e 616b 616e 2075 6e74 756b  digunakan untuk
00000040: 206d 656d 6261 6e74 7520 7072 6f73 6573  membantu proses
00000050: 2069 6e76 6573 7469 6761 7369 2e0a 0a31  investigasi...1
00000060: 2e20 5369 6170 6120 7961 6e67 206d 656c  . Siapa yang mel
00000070: 616b 756b 616e 2073 6572 616e 6761 6e3f  akukan serangan?
00000080: 0a32 2e20 4b65 7061 6461 2073 6961 7061  .2. Kepada siapa
00000090: 2073 6572 616e 6761 6e20 6469 6b69 7269  serangan dikiri
lilidjunaedi@lilidjunaedi-VirtualBox:~/Desktop/tubes/bukti/proses/CASE$ xxd README | head
00000000: 5465 7264 6170 6174 2065 6d70 6174 2028  Terdapat empat (
00000010: 3429 206b 6f6d 7075 7465 7220 6461 6c61  4) komputer dala
00000020: 6d20 7365 6275 6168 2070 6572 7573 6168  m sebuah perusah
00000030: 6161 6e2e 2044 696b 6574 6168 7569 2074  aan. Diketahui t
00000040: 6572 6461 7061 7420 696e 7369 6465 6e20  erdapat insiden
00000050: 7365 7261 6e67 616e 2070 6164 6120 7065  serangan pada pe
00000060: 7275 7361 6861 616e 2e20 4461 7269 2070  rusahaan. Dari p
00000070: 6572 696e 6761 7461 6e20 6469 2049 4453  eringatan di IDS
00000080: 206a 6172 696e 6761 6e20 7065 7275 7361  jaringan perusa
00000090: 6861 616e 2c20 6469 6461 7061 7469 206b  haan, didapati k
```

- g. Hasil analisis dapat terlihat ternyata 2 file tidak berekstensi tersebut berupa text file, dimana isi pesan langsung muncul ketika dilihat. Untuk file clue berisikan pertanyaan untuk membantu proses investigasi, sedangkan file readme berisikan masalah yang terjadi atau studi kasus dalam laporan ini.

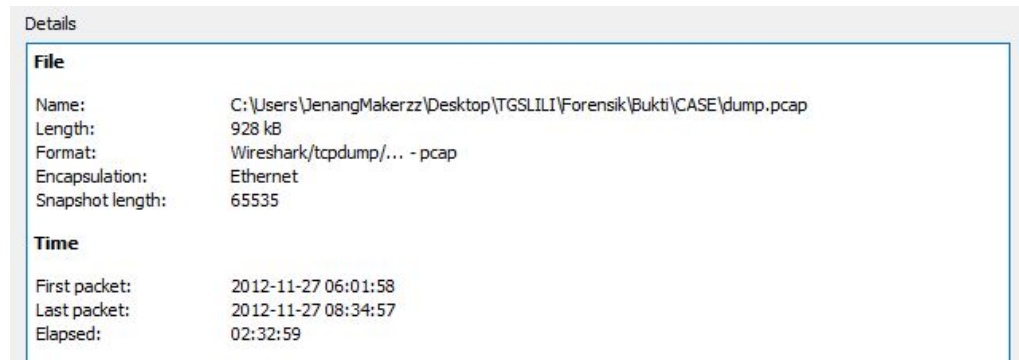


- h. Langkah selanjutnya adalah analisis file dump.pcap, file berekstensi pcap biasanya berisikan data trafik jaringan namun untuk melihat isi dari file pcap dibutuhkan aplikasi tambahan yaitu wireshark

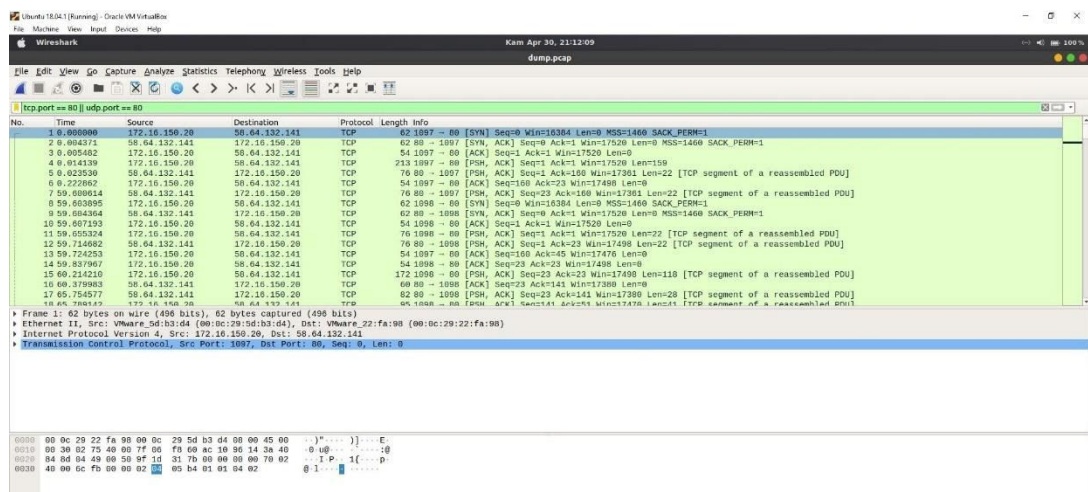




- i. Informasi awal yang bisa diketahui adalah lama kejadian itu adalah 2 jam 32 menit 59 detik pada 27 november 2012.



- j. Setelah terbuka, dapat dilihat koneksi yang terjadi antara 2 ip yaitu ip 172.16.150.20 dan ip 58.64.132.141 melalui port 80. Oleh karena itu, pencarian berfokus kenapa komunikasi melalui port 80 dengan menggunakan fungsi `tcp.port==80 | | udp.port == 80`





- k. Proses selanjutnya adalah menganalisis setiap folder yang terdapat pada folder CASE, yaitu DC, ENG, FLD, dan IIS. Setelah dilihat masing masing.

## ANALISIS FOLDER DC

- 1 menganalisis folder DC harus masuk kedalam directori tempat dimana folder DC disimpan.  
"cd Documents/KomFor/TuBes/Percobaan/CASE/DC"
- 2 Setelah sudah masuk kedalam folder DC, mulai melakukan identifikasi operating sistem yang digunakan oleh komputer DC dengan menggunakan volatility.  
"volatility imageinfo -f memdump.bin"
  - volatility adalah programnya
  - imageinfo adalah command volatility untuk pengecekan OS
  - -f adalah command untuk membuka file
  - memdump.bin adalah file yang terdapat di setiap folder komputer DC,ENG,FLD, dan IIS

```
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ cd DC
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/DC$ volatility imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win2003SP0x86, Win2003SP1x86, Win2003SP2x86 (Instantiated with Win2003SP0x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/arnayysz/Documents/KomFor/TuBes/Percobaan/CASE/DC/memdump.bin)
      PAE type : No PAE
      DTB : 0x39000L
      KDBG : 0x805583d0L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2012-11-27 02:01:57 UTC+0000
      Image local date and time : 2012-11-26 20:01:57 -0600
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/DC$
```

- 3 pengidentifikasian koneksi dan proses yang berjalan pada komputer DC sesuai dengan informasi suggested profile dan Image type (service Pack) yang didapatkan pada proses sebelumnya.  
"volatility --profile=Win2003SP0x86 connscan -f memdump.bin"

```

arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/DC$ volatility --profile=Win2003SP0x86 pslist -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                Exit
-----
0x822b07a8 System                4    0     52   842   -----  0    0 2012-11-03 20:18:29 UTC+0000
0x820c6020 smss.exe             372   4      3    17   -----  0    0 2012-11-03 20:18:30 UTC+0000
0x82031020 csrss.exe            420  372    11   505   0    0 2012-11-03 20:18:30 UTC+0000
0x820496c8 winlogon.exe         444  372    19   613   0    0 2012-11-03 20:18:30 UTC+0000
0x8203fad0 services.exe  488  444    21   422   0    0 2012-11-03 20:18:31 UTC+0000
0x82022920 lsass.exe            500  444    58   959   0    0 2012-11-03 20:18:31 UTC+0000
0x822bc770 svchost.exe          740  488    12   230   0    0 2012-11-03 20:18:33 UTC+0000
0x81fdf2e0 svchost.exe          884  488     9   133   0    0 2012-11-03 20:18:44 UTC+0000
0x81fdaf18 svchost.exe          904  488     5    78   0    0 2012-11-03 20:18:44 UTC+0000
0x81fd6968 svchost.exe          932  488    47  1092   0    0 2012-11-03 20:18:44 UTC+0000
0x81caf2d8 spoolsv.exe       1216  488     9   135   0    0 2012-11-03 20:19:12 UTC+0000
0x81cbad88 msdtc.exe         1240  488    15   160   0    0 2012-11-03 20:19:12 UTC+0000
0x81ca3d68 dfssvc.exe       1312  488    10   106   0    0 2012-11-03 20:19:12 UTC+0000
0x81c99020 svchost.exe       1404  488     2    60   0    0 2012-11-03 20:19:12 UTC+0000
0x81c82d88 ismserv.exe     1436  488    11   276   0    0 2012-11-03 20:19:12 UTC+0000
0x81c80320 ntfrs.exe      1452  488    19   282   0    0 2012-11-03 20:19:12 UTC+0000
0x81c71020 svchost.exe     1512  488     2    34   0    0 2012-11-03 20:19:13 UTC+0000
0x81c462e8 svchost.exe     1736  488    16   127   0    0 2012-11-03 20:19:27 UTC+0000
0x81c4bd88 explorer.exe         188  1996    11   337   0    0 2012-11-03 21:32:38 UTC+0000
0x81c4ad88 dns.exe        340  488    12   163   0    0 2012-11-03 21:41:26 UTC+0000
0x81b1f9020 wlns.exe          756  488    19   214   0    0 2012-11-04 17:02:01 UTC+0000
0x81be0108 wuaucnt.exe    1092  932     5    74   0    0 2012-11-04 18:57:32 UTC+0000
0x81b61b18 dllhost.exe   3292  488    18   254   0    0 2012-11-24 17:47:12 UTC+0000
0x81b4b9d0 appmgr.exe     2992  488     4   102   0    0 2012-11-24 17:47:40 UTC+0000
0x81b0bb08 srvcsvr.exe    1496  488     3    87   0    0 2012-11-24 17:47:40 UTC+0000
0x81b8f348 inetinfo.exe     308  488    25   515   0    0 2012-11-24 17:47:51 UTC+0000
0x81b17188 wmiprvse.exe     2116  740     7   208   0    0 2012-11-24 17:48:48 UTC+0000
0x81b6a4d8 POP3Svc.exe    2260  488     7   142   0    0 2012-11-24 17:55:08 UTC+0000
0x81ae2020 cmd.exe        2076  188     1    22   0    0 2012-11-27 01:37:57 UTC+0000
0x81c25b68 mdd.exe         3468  2076     1    25   0    0 2012-11-27 02:01:56 UTC+0000
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/DC$

```

- Setelah dilakukan pengecekan, ternyata tidak ditemukan koneksi dengan port 80 pada remote address pada komputer DC. Hal ini bisa kami simpulkan bahwa komputer IIS bebas dari serangan.

## ANALISIS FOLDER ENG

- menganalisis folder IIS harus masuk kedalam direktori tempat dimana folder IIS disimpan.  
"cd Documents/KomFor/TuBes/Percobaan/CASE/ENG"
- Setelah sudah masuk kedalam folder ENG, bisa mulai melakukan identifikasi operating sistem yang digunakan oleh komputer ENG dengan menggunakan volatility.  
"volatility imageinfo -f memdump.bin"

```

arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ cd ENG
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/ENG$ volatility imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/arnayysz/Documents/KomFor/TuBes/Percobaan/CASE/ENG/memdump.bin)
      PAE type : No PAE
      DTB : 0x39000L
      KDBG : 0x8054cde0L
      Number of Processors : 1
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2012-11-27 01:57:28 UTC+0000
      Image local date and time : 2012-11-26 19:57:28 -0600
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/ENG$

```

- Pada gambar diatas, bisa mendapatkan informasi bahwa komputer ENG menggunakan operating system WinXPSP3x86
- pengidentifikasian koneksi dan proses yang berjalan pada komputer ENG sesuai dengan informasi suggested profile dan Image type (service Pack) yang didapatkan pada proses sebelumnya.  
"volatility --profile=WinXPSP3x86 connscan -f memdump.bin"

```

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 connscan -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address          Remote Address          Pid
-----
0x01f60850  0.0.0.0:0                1.0.0.0:0              36569092
0x01ffa850  172.16.150.20:1291      58.64.132.141:80      1024
0x0201f850  172.16.150.20:1292      172.16.150.10:445     4
0x02084e68  172.16.150.20:1281      172.16.150.10:389     628
0x020f8988  172.16.150.20:2862      172.16.150.10:135     696
0x02201008  172.16.150.20:1280      172.16.150.10:389     628
0x18615850  172.16.150.20:1292      172.16.150.10:445     4
0x189e8850  172.16.150.20:1291      58.64.132.141:80      1024
0x18a97008  172.16.150.20:1280      172.16.150.10:389     628
0x18b8e850  0.0.0.0:0                1.0.0.0:0              36569092
0x18dce888  172.16.150.20:2862      172.16.150.10:135     696

```

5. Check apakah ada berinteraksi alamat tujuan dengan port 80. Pada folder eng didapatkan sebuah alamat remote address 58.64.132.141:80 dengan pid 1024 yang berarti terjadi interaksi pada port tsb, setelah itu kita harus proses lebih lanjut pid tersebut.
6. lakukan pengecekan pid dengan command "volatility --profile=Win2003SP0x86 pstree -f memdump.bin"

```

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 pstree -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Name                               Pid  PPid  Thds  Hnds
Time
-----
0x823c8830: System                   4    0    51   271
1970-01-01 00:00:00 UTC+0000
. 0x821841c8: smss.exe               356   4    3    19
2012-11-26 22:03:28 UTC+0000
.. 0x82189da0: winlogon.exe          628  356   18   653
2012-11-26 22:03:29 UTC+0000
... 0x82194650: services.exe           680  628   15   243
2012-11-26 22:03:30 UTC+0000
.... 0x820b3da0: svchost.exe          1024  680   76  1645
2012-11-26 22:03:32 UTC+0000
..... 0x82045da0: wuauc.lt.exe          1628 1024    3   142
2012-11-26 22:04:43 UTC+0000
..... 0x82049690: wc.exe              364 1024    1    27
2012-11-27 01:30:00 UTC+0000
.... 0x8203c020: alg.exe             1888  680    6   105

```

7. check apakah ada proses dengan pid 1024 dan ppid 1024, dan didapatkan

```

2012-11-26 22:03:30 UTC+0000
.... 0x820b3da0: svchost.exe          1024  680   76  1645
2012-11-26 22:03:32 UTC+0000
..... 0x82045da0: wuauc.lt.exe          1628 1024    3   142
2012-11-26 22:04:43 UTC+0000
..... 0x82049690: wc.exe              364 1024    1    27

```

8. yang berarti :

svchost.exe  
pid = 1024  
ppid = 680



thds = 76  
hnds = 1645  
anak proses svchost.exe : wuactl.exe

pid = 1628  
ppid = 1024  
thds = 3  
hnds = 142  
anak proses svchost.exe : wc.exe

pid = 364  
ppid = 1024  
thds = 1  
hnds = 27

svchost.exe memiliki 2 anak proses

9. Check riwayat aktivitas internet yang dilakukan computer dengan command " volatility --profile=WinXPSP3x86 iehistory -f memdump.bin"
10. Didapatkan bukti berupa pendownloadan file dengan nama Symantec-1.43-1.exe

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 iehistory -f memdump.bin
Volatility Foundation Volatility Framework 2.6
*****
Process: 284 explorer.exe
Cache type "DEST" at 0xdc69
Last modified: 2012-11-26 17:01:53 UTC+0000
Last accessed: 2012-11-26 23:01:54 UTC+0000
URL: callhttp://58.64.132.8/download/Symantec-1.43-1.exe
```

11. pencarian data pada registry dengan command " volatility --profile=WinXPSP3x86 printkey -K "network\z" -f memdump.bin "
12. Didapatkan sebuah interaksi yang dilakukan pada tanggal 27 - 11 - 2012 00:48:20 utc +0000 dengan IP penyerang 172.16.223.47  
Disk yang diserang z

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 printkey -K "network\z" -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: z (S)
Last updated: 2012-11-27 00:48:20 UTC+0000

Subkeys:

Values:
REG_SZ RemotePath : (S) \\172.16.223.47\z
REG_SZ UserName : (S) PETRO-MARKET\ENG-USTXHOU-148$
REG_SZ ProviderName : (S) Microsoft Windows Network
REG_DWORD ProviderType : (S) 131072
REG_DWORD ConnectionType : (S) 1
REG_DWORD DeferFlags : (S) 4
```

13. Carilah username dari penyerang tersebut dengan command "volatility --profile=WinXPSP3x86 -f memdump.bin envvars | grep USERNAME"

14. Didapatkan sebuah username bernama callb

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXPSP3x86 -f memdump.bin envvars | grep USERNAME
Volatility Foundation Volatility Framework 2.6
 940 svchost.exe 0x00010000 USERNAME NETWORK
SERVICE
1068 svchost.exe 0x00010000 USERNAME NETWORK
SERVICE
1116 svchost.exe 0x00010000 USERNAME LOCAL S
SERVICE
1888 alg.exe 0x00010000 USERNAME LOCAL S
SERVICE
284 explorer.exe 0x00010000 USERNAME callb
548 msmsgs.exe 0x00010000 USERNAME callb
556 ctfmon.exe 0x00010000 USERNAME callb
1628 wuauclt.exe 0x00010000 USERNAME callb
1984 msimn.exe 0x00010000 USERNAME callb
1796 cmd.exe 0x00010000 USERNAME callb
244 mdd.exe 0x00010000 USERNAME callb
Show Applications novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$
```

15. Lalu cari sebuah file backdoor dengan command "volatility --profile=WinXPSP3x86 svcscan -f memdump.bin"

16. Didapatkan sebuah service name 6to4

```
Offset: 0x389d60
Order: 228
Start: SERVICE_AUTO_START
Process ID: 1024
Service Name: 6to4
Display Name: Microsoft Device Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs
```

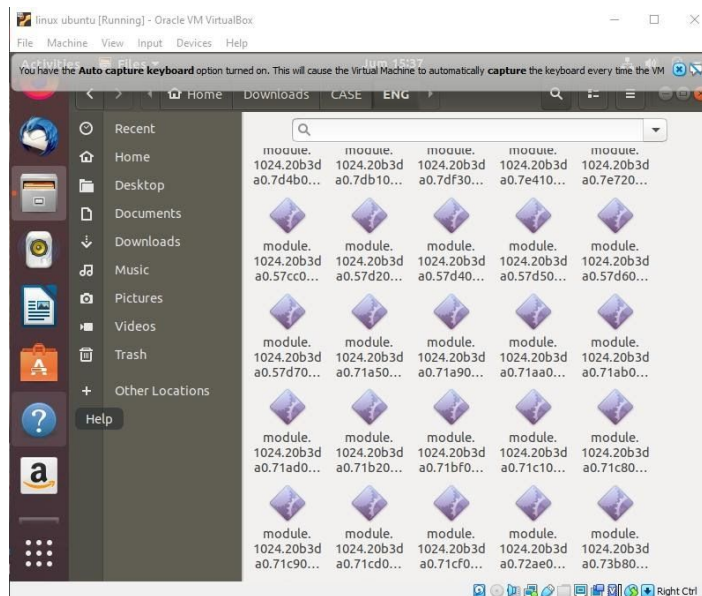
17. Lalu cari alamat untuk menemukan file backdoornya dengan command "volatility --profile=WinXPSP3x86 dlllist -f memdump.bin | grep 6to4ex.dll"

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXPSP3x86 dlllist -f memdump.bin | grep 6to4ex.dll
Volatility Foundation Volatility Framework 2.6
0x10000000 0x1c000 0x1 c:\windows\syste
em32\6to4ex.dll
```

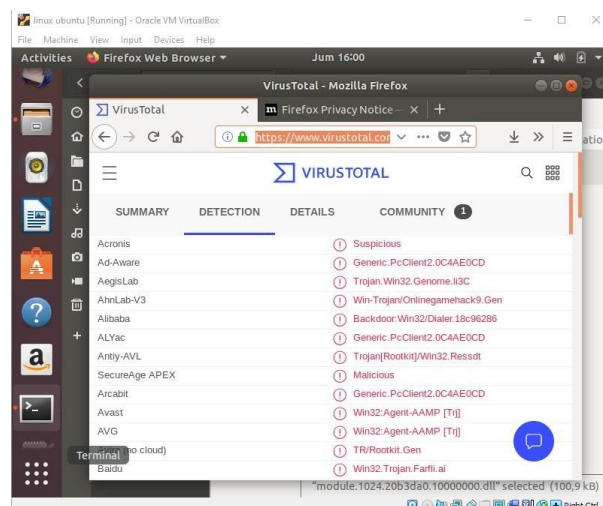
18. Selanjutnya ambil file backdoor tersebut dengan command "volatility --profile=WinXPSP3x86 dlldump --pid=1024 -f memdump.bin --dump-dir=\$(pwd)"

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 dlldump --pid=1024 -f mendump.bin --dump-dir=$(pwd)
Volatility Foundation Volatility Framework 2.6
Process(V) Name Module Base Module Name Result
-----
0x820b3da0 svchost.exe 0x001000000 svchost.exe OK: module.102
4.20b3da0.1000000.dll
0x820b3da0 svchost.exe 0x07c900000 ntdll.dll OK: module.102
4.20b3da0.7c900000.dll
0x820b3da0 svchost.exe 0x077b90000 certcli.dll OK: module.102
4.20b3da0.77b90000.dll
0x820b3da0 svchost.exe 0x076d30000 WMI.dll OK: module.102
4.20b3da0.76d30000.dll
0x820b3da0 svchost.exe 0x077f60000 SHLWAPI.dll OK: module.102
4.20b3da0.77f60000.dll
0x820b3da0 svchost.exe 0x073b80000 AVICAP32.dll OK: module.102
4.20b3da0.73b80000.dll
0x820b3da0 svchost.exe 0x050000000 wuauclnt.dll OK: module.102
4.20b3da0.50000000.dll
```

19. Perbaiki modul svchost sebagai induk dari proses
20. Check folder penyimpanan ENG, dan cari sebuah file dengan nama 0010000000

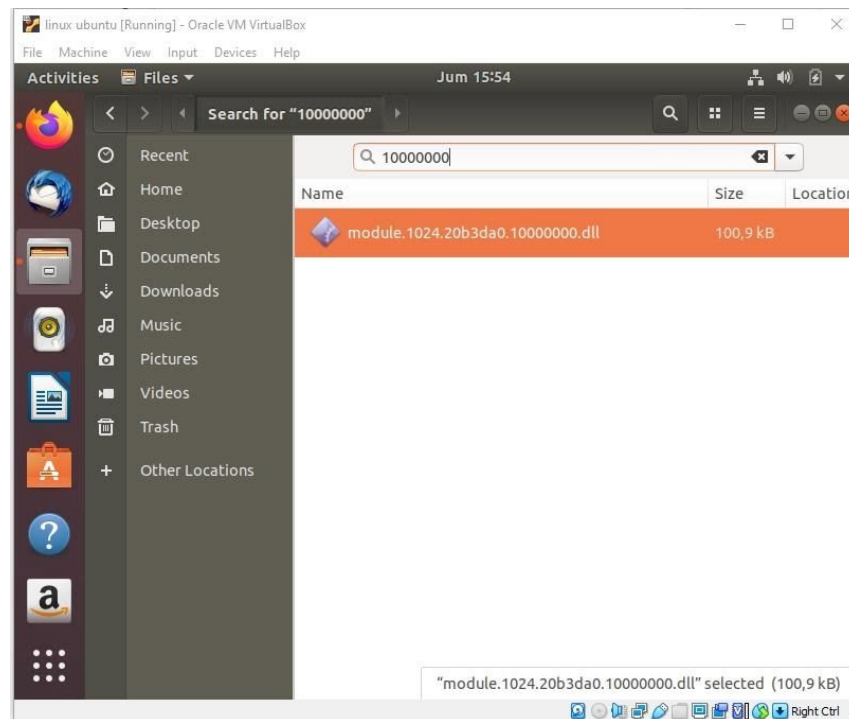


21. Setelah ditemukan filenya gunakan sebuah tool diweb dengan alamat " www.virustotal.com", upload file yang ditemukan tersebut





22. Didapatkan sebuah file backdoor yang ditandai dengan warna merah



23. Lalu kembali ke terminal, dan brute force untuk menemukan nama petro dengan command sesuai tahun terjadinya serangan " cat memdump.bin | strings | grep "2012" "

```
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
11/26/2012 07:01 PM <DIR> .
11/26/2012 07:01 PM <DIR> ..
11/26/2012 05:06 PM 303,104 gs.exe
11/26/2012 07:00 PM 5,282 https.dll
11/26/2012 05:11 PM 11,844 netuse.dll
11/26/2012 05:06 PM 403,968 ra.exe
11/26/2012 05:06 PM 20,480 sl.exe
11/26/2012 06:56 PM 1,230 svchost.dll
11/26/2012 06:44 PM 5,711 system.dll
11/26/2012 05:06 PM 208,384 wc.exe
```

24. Selanjutnya cari file ".bat" dengan command volatility --profile=WinXPSP3x86 -f memdump.bin filescan | grep -i .bat

```

linux.ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

novansyah@novansyah-VirtualBox: ~/Downloads/CASE/ENG
^[[Anovansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=W
SP3x86 -f memdump.bin filescan | grep -i .bat
Volatility Foundation Volatility Framework 2.6
0x00000000020b1a08      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
0x000000000217bd18      1      0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\compbatt.sys
0x00000000021c30d8      3      1 R--rwd \Device\HarddiskVolume1\WINDOWS\PCHealt
h\HelpCtr\BATCH
0x00000000021eab40      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
0x0000000002255a10      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\webui\s
ystem5.bat
0x0000000002260940      1      0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\battc.sys
0x00000000018891d18      1      0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\compbatt.sys
0x000000000189d6940      1      0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\battc.sys
0x00000000018c590d8      3      1 R--rwd \Device\HarddiskVolume1\WINDOWS\PCHealt
h\HelpCtr\BATCH
0x00000000018da7a08      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
0x00000000018e2ba10      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\webui\s
ystem5.bat
0x00000000018f00b40      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll

```

25. Buat folder " dump\_files" di folder ENG
26. Dan lakukan command " volatility --profile=WinXPSP3x86 -f memdump.bin dumpfiles -D dump\_files/ -Q 0x0000000002255a10" untuk mengambil file .bat

```

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 -f memdump.bin dumpfiles -D dump_files/ -Q 0x0000000002255a10
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x02255a10 None \Device\HarddiskVolume1\WINDOWS\webui\s
tem5.bat

```

27. Untuk mencari info lebih lanjut lakukan comman " cat file.None.0x8231ba30.dat "

```

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG/dump_files$ cat file.None.0
x8231ba30.dat
@echo off
copy c:\windows\webui\wc.exe c:\windows\system32
at 19:30 wc.exe -e -o h.outnovansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG/
dump_files$

```

## ANALISIS FOLDER FLD

- a. Lanjut ke folder FLD, lakukan identifikasi OS yang digunakan FLD dengan command " volatility imageinfo -f memdump.bin ", dan dapatkan sebuah bukti os Windows XP dengan **servicepack 3**.

```

arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/IIS$ cd ..
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ ls
CLUE DC dump.pcap ENG FLD IIS README
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ cd FLD
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$ ls
FLD.timeline memdump.bin
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$ volatility imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/arnayysz/Documents/KomFor/TuBes/Percobaan/CASE/FLD/memdump.bin)
      PAE type : No PAE
      DTB : 0x39000L
      KDBG : 0x8054cde0L
      Number of Processors : 1
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2012-11-27 01:46:00 UTC+0000
      Image local date and time : 2012-11-27 04:46:00 +0300
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$

```

- b. Lakukan pengecekan koneksi dan proses yg berjalan dengan command “volatility --profile=WinXPSP3x86 connscan -f memdump.bin”

```

arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 connscan -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Offset(P) Local Address Remote Address Pid
-----
0x01fb0d48 172.16.223.187:2109 172.16.150.10:389 640
0x02023638 172.16.223.187:1265 58.64.132.141:80 1032
0x02035ae8 172.16.223.187:1259 172.16.150.10:445 4
0x02080930 172.16.223.187:1261 172.16.150.10:135 1032
0x020859d0 172.16.223.187:1210 172.16.223.47:445 4
0x020f0d38 172.16.223.187:2179 172.16.150.10:1025 696
0x0230d448 172.16.223.187:1241 172.16.150.10:389 632
0x0770fd48 172.16.223.187:2109 172.16.150.10:389 640
0x0836a638 172.16.223.187:1265 58.64.132.141:80 1032
0x084c7930 172.16.223.187:1261 172.16.150.10:135 1032
0x084ec9d0 172.16.223.187:1210 172.16.223.47:445 4
0x08594448 172.16.223.187:1241 172.16.150.10:389 632
0x09b5cae8 172.16.223.187:1259 172.16.150.10:445 4
0x0ac37d38 172.16.223.187:2179 172.16.150.10:1025 696
0x10066d48 172.16.223.187:2109 172.16.150.10:389 640
0x164d3638 172.16.223.187:1265 58.64.132.141:80 1032
0x16610930 172.16.223.187:1261 172.16.150.10:135 1032
0x16c559d0 172.16.223.187:1210 172.16.223.47:445 4
0x1869d448 172.16.223.187:1241 172.16.150.10:389 632
0x197a5ae8 172.16.223.187:1259 172.16.150.10:445 4
0x1a32ad38 172.16.223.187:2179 172.16.150.10:1025 696
0x1f209d48 172.16.223.187:2109 172.16.150.10:389 640

```

- c. Check apa kah ada berinteraksi alamat tujuan dengan port 80. Pada folder FLD didapatkan sebuah alamat **remote address** **58.64.132.141:80** dengan **pid 1032** yang berarti terjadi interaksi dengan port 80, setelah itu kita harus proses lebih lanjut pid tersebut.
- d. lakukan pengecekan pid dengan command “volatility --profile=WinXPSP3x86 pstree -f memdump.bin”



```

arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 pstree -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Name                               Pid  PPid  Thds  Hnds  Time
-----
0x823c8830:System                   4      0    51   287  1970-01-01 00:00:00 UTC+0000
. 0x82274b90:smss.exe               544      4      3     19  2012-11-26 22:01:51 UTC+0000
.. 0x82238da0:csrss.exe             608    544    13    387  2012-11-26 22:01:52 UTC+0000
... 0x82214da0:winlogon.exe          632    544    17    652  2012-11-26 22:01:52 UTC+0000
... 0x822ba638:services.exe          684    632    16    256  2012-11-26 22:01:53 UTC+0000
.... 0x8228fda0:svchost.exe          1032   684    77   1558  2012-11-26 22:01:55 UTC+0000
..... 0x820297b8:cmd.exe              1048   1032      0  -----  2012-11-27 00:27:41 UTC+0000
..... 0x821f7da0:ps.exe                1052   1048      2     60  2012-11-27 01:11:17 UTC+0000
..... 0x820001e0:wc.exe                1992   1032      1     27  2012-11-27 01:30:00 UTC+0000
..... 0x82034b40:cmd.exe               456   1032      0  -----  2012-11-27 00:18:21 UTC+0000
..... 0x8230dc88:ps.exe               1448    456      1     44  2012-11-27 00:27:11 UTC+0000
..... 0x821e8918:wuauclt.exe          1616   1032      3    142  2012-11-26 22:03:07 UTC+0000
..... 0x82228da0:cmd.exe              356   1032      0  -----  2012-11-27 01:16:33 UTC+0000
..... 0x81ffb2a0:ps.exe                228    356      2     65  2012-11-27 01:22:07 UTC+0000
.... 0x8217cb10:svchost.exe            944    684      9    261  2012-11-26 22:01:55 UTC+0000
.... 0x821753d8:svchost.exe           1076    684      6     84  2012-11-26 22:01:55 UTC+0000
.... 0x82043da0:alg.exe               1888    684      6    104  2012-11-26 22:01:59 UTC+0000
.... 0x821b4a78:spoolsv.exe            1360    684      9    104  2012-11-26 22:01:58 UTC+0000
.... 0x82244460:svchost.exe            860    684     14    188  2012-11-26 22:01:54 UTC+0000
.... 0x821bac10:svchost.exe           1128    684     14    249  2012-11-26 22:01:56 UTC+0000
... 0x822ab2d8:lsass.exe               696    632     20    411  2012-11-26 22:01:53 UTC+0000
0x82223950:explorer.exe            296    260      9    366  2012-11-26 22:02:26 UTC+0000
. 0x82226a20:msmsgs.exe              660    296      3    204  2012-11-26 22:02:32 UTC+0000
. 0x821d43c0:ctfmon.exe              700    296      1     75  2012-11-26 22:02:32 UTC+0000
. 0x821d6598:msimn.exe               1984    296      7    361  2012-11-26 22:07:13 UTC+0000
. 0x82004918:cmd.exe                 1860    296      1     33  2012-11-27 01:42:52 UTC+0000
.. 0x8221d5a8:mdd.exe                 988   1860      1     24  2012-11-27 01:46:00 UTC+0000
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$

```

e. Dari gambar diatas kita bisa cek yang memiliki Pid dan PPid 1032 yang berarti :

Untuk FLD

pada WinXPSP3x86

Remote address 58.64.132.141:80

svchost.exe

Pid = 1032

PPid = 684

Thds = 77

Hnds = 1558

Anak Proses svchost.exe : cmd.exe

Pid = 1048

PPid = 1032

Thds = 0

Hnds = -

Anak Proses cmd.exe : ps.exe

Pid = 1052

PPid = 1048

Thds = 2

Hnds = 60

wc.exe

Pid = 1992

PPid = 1032

Thds = 1

Hnds = 27

cmd.exe  
Pid = 456  
PPid = 1032  
Thds = 0  
Hnds = -  
Anak Proses cmd.exe : ps.exe  
Pid = 1448  
PPid = 456  
Thds = 1  
Hnds = 44

wuauclt.exe  
Pid = 1616  
PPid = 1032  
Thds = 3  
Hnds = 142

cmd.exe  
Pid = 356  
PPid = 1032  
Thds = 0  
Hnds = -  
Anak Proses cmd.exe : ps.exe  
Pid = 228  
PPid = 356  
Thds = 2  
Hnds = 65

- f. Check riwayat aktivitas internet yang dilakukan computer dengan command " volatility --profile=WinXPSP3x86 iehistory -f memdump.bin"
- g. Didapatkan bukti berupa pendownloadan file dengan nama **Symantec-1.43-1.exe**

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 iehistory -f memdump.bin
Volatility Foundation Volatility Framework 2.6
*****
Process: 296 explorer.exe
Cache type "DEST" at 0xdc661
Last modified: 2012-11-27 03:17:56 UTC+0000
Last accessed: 2012-11-27 00:17:58 UTC+0000
URL: amirs@http://58.64.132.8/download/Symantec-1.43-1.exe
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$
```

- h. pencarian data pada registry dengan command " volatility --profile=WinXPSP3x86 printkey -K "network\z" -f memdump.bin "
- i. Didapatkan sebuah interaksi yang dilakukan pada tanggal **27 - 11 - 2012 00:48:20 utc +0000** dengan **IP penyerang 172.16.223.47** dan **Disk yang diserang z**

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 printkey -K "network\z" -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: z (S)
Last updated: 2012-11-27 00:46:10 UTC+0000

Subkeys:

Values:
REG_SZ RemotePath : (S) \\172.16.223.47\z
REG_SZ UserName : (S) PETRO-MARKET\FLD-SARIYADH-43$
REG_SZ ProviderName : (S) Microsoft Windows Network
REG_DWORD ProviderType : (S) 131072
REG_DWORD ConnectionType : (S) 1
REG_DWORD DeferFlags : (S) 4
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$
```

- j. Selanjutnya adalah cari username dari penyerang tersebut dengan command "volatility --profile=WinXPSP3x86 -f memdump.bin envvars | grep USERNAME"

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 -f memdump.bin envvars | grep USERNAME
Volatility Foundation Volatility Framework 2.6
 944 svchost.exe 0x00010000 USERNAME NETWORK SERVICE
1076 svchost.exe 0x00010000 USERNAME NETWORK SERVICE
1128 svchost.exe 0x00010000 USERNAME LOCAL SERVICE
1888 alg.exe 0x00010000 USERNAME LOCAL SERVICE
 296 explorer.exe 0x00010000 USERNAME amirs
 660 msmsgs.exe 0x00010000 USERNAME amirs
 700 ctfmon.exe 0x00010000 USERNAME amirs
1616 wuauclt.exe 0x00010000 USERNAME amirs
1984 msimn.exe 0x00010000 USERNAME amirs
1860 cmd.exe 0x00010000 USERNAME amirs
 988 mdd.exe 0x00010000 USERNAME amirs
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$
```

- k. Didapatkan sebuah username bernama **amirs**
- l. Lalu cari sebuah file backdoor dengan command "volatility --profile=WinXPSP3x86 svcscan -f memdump.bin"
- m. Didapatkan sebuah service name **6to4**

```
Offset: 0x389d60
Order: 228
Start: SERVICE_AUTO_START
Process ID: 1032
Service Name: 6to4
Display Name: Microsoft Device Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs
```

- n. Lalu cari alamat untuk menemukan file backdoornya dengan command "volatility --profile=WinXPSP3x86 dlllist -f memdump.bin | grep 6to4ex.dll"

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 dlllist -f memdump.bin | grep 6to4ex.dll
Volatility Foundation Volatility Framework 2.6
0x10000000 0x1c000 0x1 c:\windows\system32\6to4ex.dll
```

- o. Selanjutnya ambil file backdoor tersebut dengan command "volatility --profile=WinXPSP3x86 dlldump --pid=1032 -f memdump.bin --dump-dir=\$(pwd)"





- t. Lalu kembali keterminal, dan brute force untuk menemukan nama petro dengan command sesuai tahun terjadinya serangan “ cat memdump.bin | strings | grep "petro" “

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ cat memdump.bin | strings | grep "petro"
,cn=policies,cn=system,dc=petro-market,dc=org
VCN=[31B2F340-016D-11D2-945F-00C04FB984F9],cn=Polices,cn=System,dc=petro-market,dc=org
ceived: from ubuntu-router ([172.16.158.8]) by dc-ustxhou.petro-market.org with Microsoft SMTPSVC(6.0.3790.0);
Received: from d0793h (d0793h.petro-markets.info [58.04.132.141])
From: "Security Department" <lsd@petro-markets.info>
To: <amirs@petro-market.org>, <callb@petro-market.org>,
<swrightd@petro-market.org>
Return-Path: lsd@petro-markets.info
petro-market
petro-market
petro-market
dc-ustxhou.petro-market.org
dc-ustxhou.petro-market.org
petro-market.org
t-First-Site-Name,cn=Sites,cn=Configuration,dc=petro-market,dc=org
,cn=policies,cn=system,dc=petro-market,dc=org
VCN=[31B2F340-016D-11D2-945F-00C04FB984F9],cn=Polices,cn=System,dc=petro-market,dc=org
fld-sariyadh-43.petro-market.org
petro-market
petro-market
petro-market
Z:\petro-market.org\sysvol\petro-market.org\Polices\{31B2F340-016D-11D2-945F-00C04FB984F9}
petro-market
dc-ustxhou.petro-market.org
DC=DomainDNSZones,DC=petro-market,DC=org
petro-market.org
petro-market.org
petro-na
petro-na
dc-ustxhou.petro-market.org
VCN=[31B2F340-016D-11D2-945F-00C04FB984F9],cn=Polices,cn=System,dc=petro-market,dc=org
Z:\petro-market.org\sysvol\petro-market.org\Polices\{31B2F340-016D-11D2-945F-00C04FB984F9}
CN=[31B2F340-016D-11D2-945F-00C04FB984F9],cn=Polices,cn=System,dc=petro-market,dc=org
petro-market.org
petro-market.org
fld-sariyadh-43.petro-market.org
petro-market.org
petro-market.org
petro-market.org
fld-sariyadh-43.petro-market.org
petro-market.org
petro-market.org
petro-market.org
ceived: from ubuntu-router ([172.16.158.8]) by dc-ustxhou.petro-market.org with Microsoft SMTPSVC(6.0.3790.0);
Received: from d0793h (d0793h.petro-markets.info [58.04.132.141])
From: "Security Department" <lsd@petro-markets.info>
```

- u. Selanjutnya cari file “.bat “ dengan command volatility --profile=WinXPSP3x86 -f memdump.bin filescan | grep -i .bat

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 -f memdump.bin filescan | grep -i .bat
Volatility Foundation Volatility Framework 2.6
0x0000000002000468 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\webui\system3.bat
0x0000000002076340 1 0 R-r- \Device\HarddiskVolume1\WINDOWS\system32\batmeter.dll
0x00000000020764b0 1 0 R-r-d \Device\HarddiskVolume1\WINDOWS\system32\batmeter.dll
0x00000000021b3228 1 0 R---- \Device\HarddiskVolume1\WINDOWS\system32\drivers\batc.sys
0x00000000021b9a78 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\system6.bat
0x00000000021d3e28 1 0 R-rwd \Device\HarddiskVolume1\WINDOWS\Installer\tsclientmsitrans\tscdsbl.bat
0x00000000021dd8f8 1 0 R---- \Device\HarddiskVolume1\WINDOWS\system32\drivers\compbatt.sys
0x000000000220c658 3 1 R-rwd \Device\HarddiskVolume1\WINDOWS\PCHealth\HelpCtr\BATCH
0x000000000222e528 1 0 R-rw- \Device\HarddiskVolume1\WINDOWS\webui\system5.bat
0x0000000007fa7468 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\webui\system3.bat
0x0000000008113658 3 1 R-rwd \Device\HarddiskVolume1\WINDOWS\PCHealth\HelpCtr\BATCH
0x00000000088bc298 1 0 R-rw- \Device\HarddiskVolume1\WINDOWS\webui\system5.bat
0x00000000093248f8 1 0 R---- \Device\HarddiskVolume1\WINDOWS\system32\drivers\compbatt.sys
0x0000000009cdd340 1 0 R-r- \Device\HarddiskVolume1\WINDOWS\system32\batmeter.dll
0x0000000009cdd4b0 1 0 R-r-d \Device\HarddiskVolume1\WINDOWS\system32\batmeter.dll
0x000000000a0a0a78 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\system6.bat
0x000000000a4bae28 1 0 R-rwd \Device\HarddiskVolume1\WINDOWS\Installer\tsclientmsitrans\tscdsbl.bat
0x000000000a4da228 1 0 R---- \Device\HarddiskVolume1\WINDOWS\system32\drivers\batc.sys
0x0000000016908468 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\webui\system3.bat
0x0000000016a4e468 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\webui\system3.bat
0x0000000016f75298 1 0 R-rw- \Device\HarddiskVolume1\WINDOWS\webui\system5.bat
0x00000000171a0298 1 0 R-rw- \Device\HarddiskVolume1\WINDOWS\webui\system5.bat
0x00000000174dc658 3 1 R-rwd \Device\HarddiskVolume1\WINDOWS\PCHealth\HelpCtr\BATCH
0x00000000184a6340 1 0 R-r- \Device\HarddiskVolume1\WINDOWS\system32\batmeter.dll
0x00000000184a64b0 1 0 R-r-d \Device\HarddiskVolume1\WINDOWS\system32\batmeter.dll
0x00000000184cd8f8 1 0 R---- \Device\HarddiskVolume1\WINDOWS\system32\drivers\compbatt.sys
0x0000000019211a78 1 0 -W-w- \Device\HarddiskVolume1\WINDOWS\system6.bat
0x000000001a14be28 1 0 R-rwd \Device\HarddiskVolume1\WINDOWS\Installer\tsclientmsitrans\tscdsbl.bat
0x000000001a1ab228 1 0 R---- \Device\HarddiskVolume1\WINDOWS\system32\drivers\batc.sys
0x000000001ab9c298 1 0 R-rw- \Device\HarddiskVolume1\WINDOWS\webui\system5.bat
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$
```

- v. Buat folder “ dump\_files” di folder FLD

- w. Langkah selanjutnya adalah lakukan command “ volatility --profile=WinXPSP3x86 -f memdump.bin dumpfiles -D dump\_files/ -Q 0x...” untuk mengambil file system\*.bat yang terdapat dalam folder webui.

- x. Namun dari percobaan yang saya lakukan, terdapat beberapa alamat yang menghasilkan sebuah file bernama file.None.0x\*.bat. dan ada juga yang tidak menghasilkan apa-apa.

```
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLD$ volatility --profile=WinXPSP3x86 -f memdump.bin dumpfiles -D dump_files/ -Q 0x000000002000468
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x02000468 None \Device\HarddiskVolume1\WINDOWS\weui\system3.bat
```

- y. Untuk alamat yang menghasilkan file bernama file.None.0x\*.bat, penulis lakukan pendalaman lebih lanjut untuk mendapatkan informasi lebih dalam dengan command “cat file.None.0x\*.dat”. Namun dikarenakan file tersebut berukuran 0bytes dan tidak menghasilkan apa-apa, maka penganalisisan saya hentikan dengan kesimpulan file untuk fld tidak ada.



## ANALISIS FOLDER IIS

1. menganalisis folder IIS harus masuk kedalam directori tempat dimana folder IIS disimpan.  
“cd Documents/KomFor/TuBes/Percobaan/CASE/IIS”
2. Setelah sudah masuk kedalam folder IIS, bisa mulai melakukan identifikasi operating sistem yang digunakan oleh komputer IIS dengan menggunakan volatility.  
“volatility imageinfo -f memdump.bin”

```
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/DC$ cd ..
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ ls
CLUE DC dump.pcap ENG FLD IIS README
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE$ cd IIS
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/IIS$ ls
IIS.timeline memdump.bin
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/IIS$ ^C
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/IIS$ ^C
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/IIS$ volatility imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win2003SP0x86, Win2003SP1x86, Win2003SP2x86 (Instantiated with Win2003SP0x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/arnayysz/Documents/KomFor/TuBes/Percobaan/CASE/IIS/memdump.bin)
      PAE type : No PAE
      DTB : 0x39000L
      KDBG : 0x805503d0L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2012-11-27 01:52:37 UTC+0000
      Image local date and time : 2012-11-27 04:52:37 +0300
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/IIS$
```

3. Pada gambar diatas, bisa mendapatkan informasi bahwa komputer IIS menggunakan operating system Win2003SP0x86
4. pengidentifikasian koneksi dan proses yang berjalan pada komputer IIS sesuai dengan informasi suggested profile dan Image type (service Pack) yang didapatkan pada proses sebelumnya.  
“volatility --profile=Win2003SP0x86 connscan -f memdump.bin”



```

arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/IuBes/Percobaan/CASE/IIS$ volatllity --profile=Win2003SP0x86 connscan -f mendum.bln
Volatllity Foundation Volatllity Framework 2.6
Offset(P) Local Address Remote Address Pid
-----
0x01f19328 172.16.223.47:1113 172.16.150.10:445 988
0x01f52008 172.16.223.47:1112 172.16.150.10:1025 540
0x01fbc428 172.16.223.47:139 172.16.150.10:1750 4
0x01febb10 172.16.223.47:1137 172.16.150.10:135 540
0x01ff8e70 172.16.223.47:445 172.16.150.20:1235 4
0x0200b3c8 172.16.223.47:1150 172.16.150.10:135 540
0x02010cd8 172.16.223.47:42 172.16.150.10:1824 1388
0x020129c8 172.16.223.47:445 172.16.223.187:1210 4
0x02369ab8 172.16.223.47:1031 172.16.150.10:42 1388
0x02383008 172.16.223.47:1160 172.16.150.10:1025 540
0x02419a10 172.16.223.47:1164 172.16.150.10:445 4
0x025dbcd0 172.16.223.47:1165 172.16.150.10:139 4
0x02663920 172.16.223.47:1159 172.16.150.10:135 540
0x0d9f2920 172.16.223.47:1159 172.16.150.10:135 540
0x0da0acd0 172.16.223.47:1165 172.16.150.10:139 4
0x0da619c8 172.16.223.47:445 172.16.223.187:1210 4
0x0daaffcd8 172.16.223.47:42 172.16.150.10:1824 1388
0x0db1fe70 172.16.223.47:445 172.16.150.20:1235 4
0x0db38ab8 172.16.223.47:1031 172.16.150.10:42 1388
0x0dbe8a10 172.16.223.47:1164 172.16.150.10:445 4
0x0dcd2008 172.16.223.47:1160 172.16.150.10:1025 540
0x0dd59008 172.16.223.47:1112 172.16.150.10:1025 540
0x0dde0328 172.16.223.47:1113 172.16.150.10:445 988
0x0defa3c8 172.16.223.47:1150 172.16.150.10:135 540
0x0dfa3428 172.16.223.47:139 172.16.150.10:1750 4

```

- Setelah dilakukan pengecekan, ternyata tidak ditemukan koneksi dengan port 80 pada remote address pada komputer IIS. Hal ini bisa kami simpulkan bahwa komputer IIS bebas dari serangan.

```

0x0e072b10 172.16.223.47:1137 172.16.150.10:135 540
0x16f7eab8 172.16.223.47:1031 172.16.150.10:42 1388
0x16ffb920 172.16.223.47:1159 172.16.150.10:135 540
0x17163cd0 172.16.223.47:1165 172.16.150.10:139 4
0x17219a10 172.16.223.47:1164 172.16.150.10:445 4
0x172f7cd8 172.16.223.47:42 172.16.150.10:1824 1388
0x17317e70 172.16.223.47:445 172.16.150.20:1235 4
0x174959c8 172.16.223.47:445 172.16.223.187:1210 4
0x176ba008 172.16.223.47:1160 172.16.150.10:1025 540
0x177db3c8 172.16.223.47:1150 172.16.150.10:135 540
0x1781c428 172.16.223.47:139 172.16.150.10:1750 4
0x17936328 172.16.223.47:1113 172.16.150.10:445 988
0x179b3008 172.16.223.47:1112 172.16.150.10:1025 540
0x17c50b10 172.16.223.47:1137 172.16.150.10:135 540
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/IuBes/Percobaan/CASE/IIS$

```

## VII. Kesimpulan

### a. Hasil Analisis

Hasil analisis dari laporan ini dibuat menjadi sebuah kronologi kejadian berdasarkan barang bukti yang selesai dianalisis menjadi kumpulan fakta, berikut kronologi kejadian penyerangan :

Kejadian bermula pada Senin 26 November 2012 sekitar pukul 2 siang sebuah email masuk dari email penyerang yaitu [isd@petro-market.org](mailto:isd@petro-market.org) yang ditujukan kepada 3 korban yaitu [amirs@petro-market.org](mailto:amirs@petro-market.org), [callb@petro-market.org](mailto:callb@petro-market.org) dan [wrightd@petro-market.org](mailto:wrightd@petro-market.org). dari barang bukti file dump.pcap diketahui bahwa ip penyerang berkomunikasi menggunakan ip 58.64.132.141 dengan tujuan ip 172.16.150.20 yang merupakan ip dari server ENG melalui port 80 dengan protokol http. Penyerang melakukan remote kepada server ENG melalui ip 172.16.223.47 agar penyerang dapat mendownload melalui internet explorer secara remote sebuah file yang berisikan backdoor bernama symantec-1.43-1.exe melalui link [callb@http://58.64.132.8/download/Symantec-1.43-1.exe](http://58.64.132.8/download/Symantec-1.43-1.exe).

Dihari yang sama sekitar pukul 11 malam penyerang yaitu Petro-Market\ENG-USTXHOU-1485 melakukan remote ke server ENG kemudian program yang berhasil di download langsung diinstal dan berjalan di server ENG, tidak lama program yang sama diinstal dan berjalan pada server FLD dengan cara yang sama yaitu melalui remote sekitar jam 1 malam. program tersebut menjalankan service berupa 6to4ex.dll yang menjalankan proses svchost.exe dengan PID 1024 pada server ENG sedangkan pada server FLD PID nya 1032, kemudian di cek melalui virustotal ternyata 61 dari 64 antivirus menganggap bahwa 6to4ex.dll merupakan virus trojan, sehingga file 6to4ex.dll merupakan backdoor milik penyerang.

Analisis lanjutan mengungkap tool atau aplikasi yang digunakan penyerang adalah gs.exe (gsecdump), ps.exe (psexec), ra.exe (rar.exe), sl.exe (scanline), wc.exe (windows credential editor). karena menggunakan credential editor sudah dipastikan penyerang merubah user privilege menjadi local system administrator informasi ini didapatkan setelah melakukan pencarian file tipe.bat dan di temukanlah file system5.bat, seluruh tool tersebut disimpan di C:\windows\webui untuk mengambil sebuah file yaitu pump1.dwg - pump100.dwg.

Berikut bukti bukti yang diperoleh

#### 1. Siapa yang melakukan serangan?

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WINXP
SP3x86 printkey -K "network\z" -f memdump.bin
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: z (S)
Last updated: 2012-11-27 00:48:20 UTC+0000

Subkeys:

Values:
REG_SZ RemotePath : (S) \\172.16.223.47\z
REG_SZ UserName : (S) PETRO-MARKET\ENG-USTXHO-148$
REG_SZ ProviderName : (S) Microsoft Windows Network
REG_DWORD ProviderType : (S) 131072
REG_DWORD ConnectionType : (S) 1
REG_DWORD DeferFlags : (S) 4
```

Didapatkan sebuah interaksi yang dilakukan pada tanggal 27 - 11 - 2012 00:48:20 utc +0000 dengan IP penyerang 172.16.223.47 Disk yang diserang z

## 2. Kepada siapa serangan dikirimkan?

- amirs@petro-markets.org
- callb@petro-markets.org
- [wrightd@petro-markets.org](mailto:wrightd@petro-markets.org)

```
arnayysz@arnayysz-VirtualBox:~/Documents/KonFor/TuBes/Percobaan/CASE/FLD$ cat mendum.bln | strings | grep "petro"
,cn=policies,cn=system,DC=petro-market,DC=org
VCN={31B2F340-0160-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=petro-market,DC=org0
celved: from ubuntu-router ([172.16.150.8]) by dc-ustxhou.petro-market.org with Microsoft SMTPSVC(6.0.3790.0);
Received: from d0793h (d0793h.petro-markets.info [58.64.132.141])
From: "Security Department" <lsd@petro-markets.info>
To: <amirs@petro-market.org>, <callb@petro-market.org>,
<wrightd@petro-market.org>
Return-Path: lsd@petro-markets.info
petro-market
petro-market
petro-market
dc-ustxhou.petro-market.org
dc-ustxhou.petro-market.org
petro-market.org
t-First-Site-Name,CN=Sites,CN=Configuration,DC=petro-market,DC=org
,cn=policies,cn=system,DC=petro-market,DC=org
VCN={31B2F340-0160-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=petro-market,DC=org0
fld-sariyadh-43.petro-market.org
petro-market
petro-market
Z1\petro-market.org\sysvol\petro-market.org\Policies\{31B2F340-0160-11D2-945F-00C04FB984F9}0
petro-market
dc-ustxhou.petro-market.org
DC=DomainDNSZones,DC=petro-market,DC=org
petro-market.org
petro-market.org
petro-na
petro-na
dc-ustxhou.petro-market.org
VCN={31B2F340-0160-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=petro-market,DC=org0
Z1\petro-market.org\sysvol\petro-market.org\Policies\{31B2F340-0160-11D2-945F-00C04FB984F9}0
CN={31B2F340-0160-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=petro-market,DC=org
petro-market.org
petro-market.org
fld-sariyadh-43.petro-market.org
fld-sariyadh-43.petro-market.org
petro-market.org
petro-market.org
petro-market.org
fld-sariyadh-43.petro-market.org
petro-market.org
petro-market.org
petro-market.org
petro-market.org
celved: from ubuntu-router ([172.16.150.8]) by dc-ustxhou.petro-market.org with Microsoft SMTPSVC(6.0.3790.0);
Received: from d0793h (d0793h.petro-markets.info [58.64.132.141])
From: "Security Department" <lsd@petro-markets.info>
```

## 3. Kapan serangan dikirimkan?

Mon, 26 nov 2012, 14:00:08

```
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
11/26/2012 07:01 PM <DIR> .
11/26/2012 07:01 PM <DIR> ..
11/26/2012 05:06 PM 303,104 gs.exe
11/26/2012 07:00 PM 5,282 https.dll
11/26/2012 05:11 PM 11,844 netuse.dll
11/26/2012 05:06 PM 403,968 ra.exe
11/26/2012 05:06 PM 20,480 sl.exe
11/26/2012 06:56 PM 1,230 svchost.dll
11/26/2012 06:44 PM 5,711 system.dll
11/26/2012 05:06 PM 208,384 wc.exe
```

## 4. Kapan serangan dieksekusi?

tuesday, nov 27 2012, 00:17:58

Details	
<b>File</b>	
Name:	C:\Users\JenangMakerzz\Desktop\TGSLILI\Forensik\Bukti\CASE\dump.pcap
Length:	928 kB
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535
<b>Time</b>	
First packet:	2012-11-27 06:01:58
Last packet:	2012-11-27 08:34:57
Elapsed:	02:32:59



## 5. Berapa alamat ip server c&c ?

Pada folder eng didapatkan sebuah alamat remote address 58.64.132.141:80 dengan pid 1024 yang berarti terjadi interaksi pada port tsb, setelah itu kita harus proses lebih lanjut pid tersebut.

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 connscan -f memdump.bin
Volatility Foundation Volatility Framework 2.6
```

Offset(P)	Local Address	Remote Address	Pid
0x01f60850	0.0.0.0:0	1.0.0.0:0	36569092
0x01ffa850	172.16.150.20:1291	58.64.132.141:80	1024
0x0201f850	172.16.150.20:1292	172.16.150.10:445	4
0x02084e68	172.16.150.20:1281	172.16.150.10:389	628
0x020f8988	172.16.150.20:2862	172.16.150.10:135	696
0x02201008	172.16.150.20:1280	172.16.150.10:389	628
0x18615850	172.16.150.20:1292	172.16.150.10:445	4
0x189e8850	172.16.150.20:1291	58.64.132.141:80	1024
0x18a97008	172.16.150.20:1280	172.16.150.10:389	628
0x18b8e850	0.0.0.0:0	1.0.0.0:0	36569092
0x18de988	172.16.150.20:2862	172.16.150.10:135	696

## 6. Apa nama file dropper?

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 pstree -f memdump.bin
Volatility Foundation Volatility Framework 2.6
```

Name	Pid	PPid	Thds	Hnds
0x823c0830:System	4	0	51	271
1970-01-01 00:00:00 UTC+0000				
0x821841c8:smss.exe	356	4	3	19
2012-11-26 22:03:28 UTC+0000				
0x82189da0:winlogon.exe	628	356	18	653
2012-11-26 22:03:29 UTC+0000				
0x82194650:services.exe	680	628	15	243
2012-11-26 22:03:30 UTC+0000				
0x820b3da0:svchost.exe	1024	680	76	1645
2012-11-26 22:03:32 UTC+0000				
0x82045da0:wuauc.lt.exe	1628	1024	3	142
2012-11-26 22:04:43 UTC+0000				
0x82049690:wc.exe	364	1024	1	27
2012-11-27 01:30:00 UTC+0000				
0x8203c020:alg.exe	1888	680	6	105

Didapatkan bukti berupa pendownloadan file dengan nama Symantec-1.43-1.exe

## 7. Apa nama file backdoor?

6to4ex.dll

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 dlllist -f memdump.bin | grep 6to4ex.dll
Volatility Foundation Volatility Framework 2.6
```

Address	Offset	Size	Path
0x10000000	0x1c000	0x1	c:\windows\sys
em32\6to4ex.dll			

## 8. Apa proses yang digunakan backdoor?

Perhatikan modul svchost sebagai induk dari proses

```

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 dlldump --pid=1024 -f memdump.bin --dump-dir=$(pwd)
Volatility Foundation Volatility Framework 2.6
Process(V) Name Module Base Module Name Result
-----
0x820b3da0 svchost.exe 0x00100000 svchost.exe OK: module.102
4.20b3da0.1000000.dll
0x820b3da0 svchost.exe 0x07c90000 ntdll.dll OK: module.102
4.20b3da0.7c900000.dll
0x820b3da0 svchost.exe 0x077b90000 certcli.dll OK: module.102
4.20b3da0.77b90000.dll
0x820b3da0 svchost.exe 0x076d30000 WMI.dll OK: module.102
4.20b3da0.76d30000.dll
0x820b3da0 svchost.exe 0x077f60000 SHLWAPI.dll OK: module.102
4.20b3da0.77f60000.dll
0x820b3da0 svchost.exe 0x073b80000 AVICAP32.dll OK: module.102
4.20b3da0.73b80000.dll
0x820b3da0 svchost.exe 0x050000000 wuauclt.dll OK: module.102
4.20b3da0.50000000.dll

```

9. Berapa proses id (pid) backdoor pada setiap komputer/server yang terinstal backdoor?

```

Offset: 0x389d60
Order: 228
Start: SERVICE_AUTO_START
Process ID: 1024
Service Name: 6to4
Display Name: Microsoft Device Manager
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

```

dapat dilihat bahwa pada offset 0x389d60 menggunakan PID 1024 yang terindikasi terserang karena melakukan koneksi melalui port 80 dan proses menjalankannya SERVICE\_AUTO\_START dengan nama service 6to4

10. User apa yang digunakan pada serangan?

```

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 -f memdump.bin envvars | grep USERNAME
Volatility Foundation Volatility Framework 2.6
940 svchost.exe 0x00010000 USERNAME NETWORK
SERVICE
1068 svchost.exe 0x00010000 USERNAME NETWORK
SERVICE
1116 svchost.exe 0x00010000 USERNAME LOCAL S
SERVICE
1888 alg.exe 0x00010000 USERNAME LOCAL S
SERVICE
284 explorer.exe 0x00010000 USERNAME callb
548 msmsgs.exe 0x00010000 USERNAME callb
556 ctfmon.exe 0x00010000 USERNAME callb
1628 wuauclt.exe 0x00010000 USERNAME callb
1984 msimn.exe 0x00010000 USERNAME callb
1796 cmd.exe 0x00010000 USERNAME callb
244 mdd.exe 0x00010000 USERNAME callb
Show Applications
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$

```

Didapatkan sebuah username bernama callb, amirs, sysbackup

11. Berapa level akses yang dimiliki penyerang?

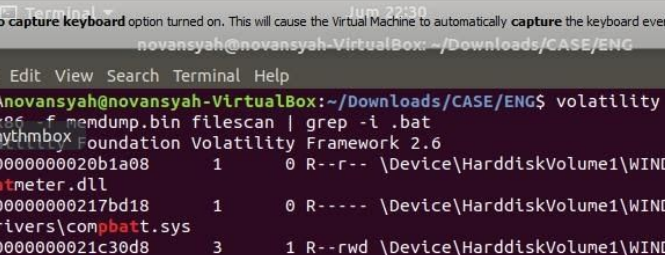
Level akses yang dimiliki penyerang ialah Local system administrator

12.Script \*.bat apa saja yang diletakkan pada setiap perangkat?

System3.bat

System5.bat

System6.bat



```
linux ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM
novansyah@novansyah-VirtualBox: ~/Downloads/CASE/ENG$
File Edit View Search Terminal Help
^[[Anovansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=W
SP3x86 -f memdump.bin filescan | grep -i .bat
Volatility Foundation Volatility Framework 2.6
0x00000000020b1a08 1 0 R-r-r- \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
0x000000000217bd18 1 0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\compbatt.sys
0x00000000021c30d8 3 1 R-r-rw- \Device\HarddiskVolume1\WINDOWS\PCHealt
h\HelpCtr\BATCH
0x00000000021eab40 1 0 R-r-r-d \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
0x0000000002255a10 1 0 R-r-rw- \Device\HarddiskVolume1\WINDOWS\webui\s
ystem5.bat
0x0000000002260940 1 0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\batctl.sys
0x0000000001889d18 1 0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\compbatt.sys
0x000000000189d6940 1 0 R----- \Device\HarddiskVolume1\WINDOWS\system3
2\drivers\batctl.sys
0x00000000018c590d8 3 1 R-r-rw- \Device\HarddiskVolume1\WINDOWS\PCHealt
h\HelpCtr\BATCH
0x00000000018da7a08 1 0 R-r-r- \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
0x00000000018e2ba10 1 0 R-r-rw- \Device\HarddiskVolume1\WINDOWS\webui\s
ystem5.bat
0x00000000018f00b40 1 0 R-r-r-d \Device\HarddiskVolume1\WINDOWS\system3
2\batmeter.dll
```

13. Apa saja isi masing-masing file \*.bat?

```
novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG$ volatility --profile=WinXP
SP3x86 -f memdump.bin dumpfiles -D dump_files/ -Q 0x0000000002255a10
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x02255a10 None \Device\HarddiskVolume1\WINDOWS\webui\sys
tem5.bat

novansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG/dump_files$ cat file.None.0
x8231ba30.dat
@echo off
copy c:\windows\webui\wc.exe c:\windows\system32
at 19:30 wc.exe -e -o h.outnovansyah@novansyah-VirtualBox:~/Downloads/CASE/ENG/
dump_files$
```

Ada file dengan extension .bat yaitu system5.bat.



c:\windows\webui

```
arnayysz@arnayysz-VirtualBox:~/Documents/KomFor/TuBes/Percobaan/CASE/FLDS$
```

Pump1.dwg-pump100.dwg

File contained all 0's

a48266248c04b2ba733238a480690a1c

perlu segera ditangani?

ENG-USTXHOU-148  
FLD-SARIYADH-43  
IIS-SARIYADH-03

## SYSBACKUP-USED BY ATTACKER

novasys@novasys-vah-VirtualBox:~/Downloads/CASE/ENGS

SAADMIN\PETRO-MARKET.ORG-HASH SEEN DUMPED BY  
GSECDUMP  
ADMINISTRATOR\CURRENT-HASH SEEN DUMPED BY  
GSECDUMP

20. Apa ada komputer/server lain yang perlu dianalisis?  
Ya, [wrightd@petro-market.or](mailto:wrightd@petro-market.or)

Berikut Timeline Penyerangan:

1. Mon, 26 nov 2012 14:00:08 -0600 atau 20:00:08 UTC = penyerang isd@petro-market.org mengirimkan email
2. Mon nov 26 2012 23:01:53 = server ENG mendownload melalui iexplorer dengan url callb@http://58.64.132.8/download/Symantec-1.43-1.exe
3. Mon Nov 26 2012 23:01:54 = symantec-1.43-1.exe berjalan di server ENG
4. Tue Nov 27 2012 00:17:58 = symantec-1.43-1.exe berjalan di server FLD
5. Mon Nov 26 2012 23:06:34 = server ENG menjalankan ps.exe
6. Tue Nov 27 2012 00:20:06 = server FLD menjalankan ps.exe
7. Tue Nov 27 2012 00:20:33 sampai Tue Nov 27 2012 00:20:46 = server FLD menjalankan c:/WINDOWS/webui/gs.exe . ps.exe , ra.exe, sl.exe, wc.exe
8. Mon Nov 26 2012 23:06:47 = server ENG menjalankan exe seperti server FLD
9. Tue Aug 17 2004 17:00:00 = server FLD menjalankan 6to4ex.dll dimana file tersebut terindeksi virus @virustotal
10. Wed Aug 18 2004 02:00:00 = server ENG menjalankan 6to4ex.dll dimana file tersebut terindeksi virus @virustotal
11. Tue Nov 27 2012 01:05:55 = winrar berjalan dengan c:/Documents and Settings/sysbackup/Application Data/WinRAR

## b. Kesimpulan

Berdasarkan hasil pemeriksaan dan analisis terhadap file "CASE.tar.bz" menggunakan tool *volatile*, *command* dan *tools* pendukung dalam sistem operasi Linux, maka didapatkan beberapa hasil temuan. Temuan-temuan tersebut sudah dapat menjawab keseluruhan pertanyaan yang ada pada file clue.

## VIII. Penutup

Dengan selesainya laporan analisis ini besar harapan kami sebagai penulis memperoleh hasil yang sesuai dengan fakta fakta yang ada.