

Cyber Forensic HoL

V.1.2

Author : Yonathan Wieliem

Course Code : COMP6193 - Cyber Forensic

Description :

This is a Hands on Lab made by me, specially designed to help you to understand how to perform Cyber Forensic operation in a safe way & also in a fast way. If you have a questions, don't hesitate to contact me.

List of Materials that we're discussing in here :

- Forensic Imaging
 - File identification and analysis
 - Registry analysis
 - Data Recovery
 - Memory dump analysis
 - Creating memory dump
 - Accessing Hiberfil.sys
 - Finding relevant evidence (browser history, email, last running program, etc)
 - Antiforensics (Steganography)
-

*** This HoL Will be updated soon if there's a material that not present in here*

*** I will put some extra exercise file for you to try it (trust me, it's worthed to try)*

*** Another Case Study will be available soon*

Forensic Imaging

Apa itu Forensic Imaging ?

Forensic Imaging merupakan proses dimana kita akan melakukan duplikasi dari sebuah evidence fisik, dan kita mau mengambil semua barang bukti yang ada dalam sebuah device evidence.

Untuk file yang akan di-copy tidak sebatas file yang masih bisa dilihat secara langsung dalam OS, namun juga file-file hidden , tiap bit dari data , tiap sektor partisi, MBR, data yang dihapus, dan unallocated space dari sebuah drive evidence. Semua copy ini sifatnya akan identik dengan struktur drive dan konten originalnya.

Best practicenya forensic imaging?

Kita harus meng-klon evidence dan JANGAN bekerja pada evidencenya secara langsung karena perubahan yang kita lakukan bisa mencemari evidence bahkan bisa merusak barang bukti. Prinsipnya, semua evidence file itu sifatnya rapuh, jadi harus ditangani dengan sebaik dan sehati-hati mungkin.

Apa saja metode yang ada dalam forensic imaging?

- Copy & Paste
Cara paling umum. Namun untuk file sistem tidak bisa dengan hanya main copas. Semua metadata dan file-file hidden akan ikut terhapus jika memakai metode ini. Cara ini hanya dilakukan utk transfer file yang evidencenya memang sudah visible dengan kita aja tanpa perlu cek isi hidden datanya.
- Disk Cloning
Membuat klon dari original drive dan memasukkan semua informasi yang memungkinkan drive clone bisa booting. Jadi drive cloning ini akan berjalan semua sistemnya dan identik dengan yang originalnya. (ya mirip kasus kita mau klon sistem kita dari HDD ke SSD sih)

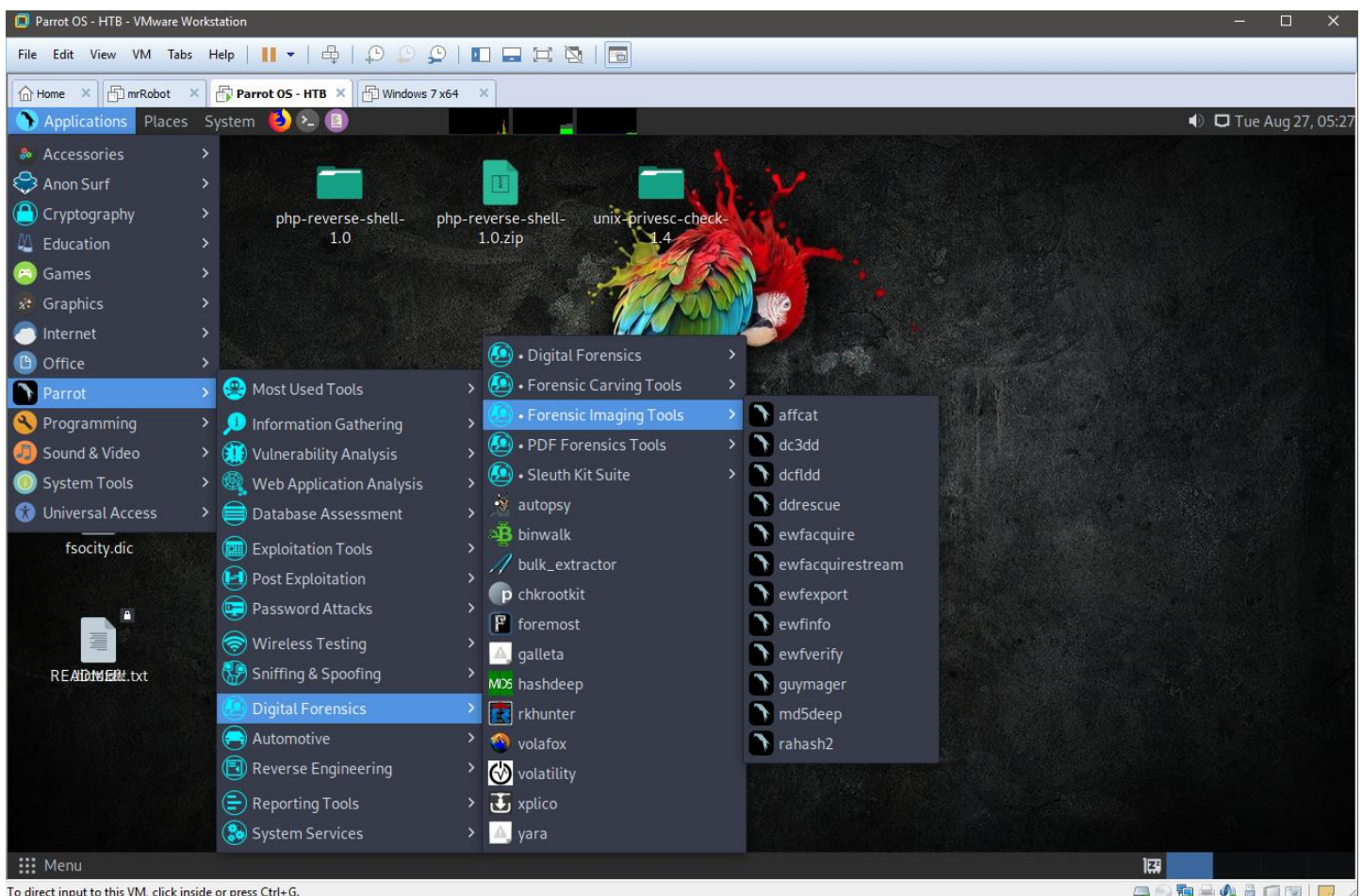
- Disk Imaging

Merupakan proses dimana kita melakukan copy pada isi hard drive sebagai backup copy / arsip. Kita bisa meng-copy bahkan sampai data-data yang ada pada source drive seperti FAT dan MBR. Image ini hanya 1 dan dia bisa disimpan di device manapun dan ga harus identik dengan hard drive awal. Disk imaging akan membantu kita saat kita mau melakukan system restore .

Checksums

Kita butuh melakukan internal verification semisal mengecek integritas file evidence via checksum hash. Kita bisa cek integritas copy dari original drive dengan yang aslinya. Beberapa tools disk imaging memakai CRC / MD5 checksums untuk mengecek integritas file.

Tools Forensic Imaging adalah sebagai berikut :



File Identification & Analysis

Apa saja yang akan dilakukan dalam identifikasi & analisa file?

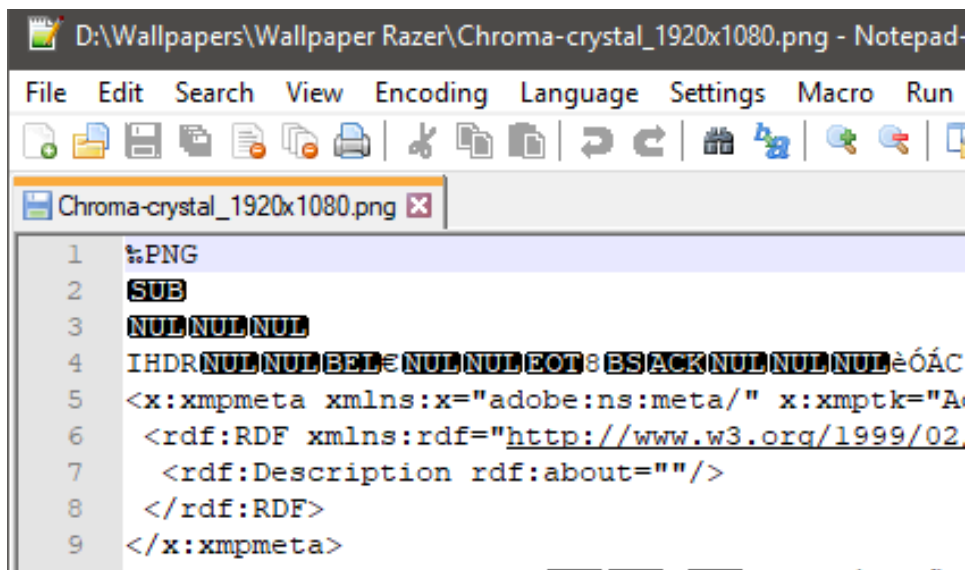
Kita melakukan proses identifikasi jenis file dengan melihat format dari urutan byte yang ada dalam sebuah file. Biasanya OS saat mau mengidentifikasi jenis file, dia melihat MIME information yang ada dalam sebuah file dan juga file headernya.

Jadi dalam forensik untuk menganalisis sebuah file, kita hanya memerlukan preset signature dari header file. (secara umumnya).

Untuk tipe forensik ini biasanya tahap pertamanya kita harus mengecek jenis file evidence yang ada. Terkadang kita membutuhkan tindakan lanjut jika file tersebut rusak. Secara umum, kasus file rusak karena header filenya rusak.

Untuk contoh bagaimana cara melakukan file identification, saya akan mencontohkan metode biasa dan cara cepatnya.

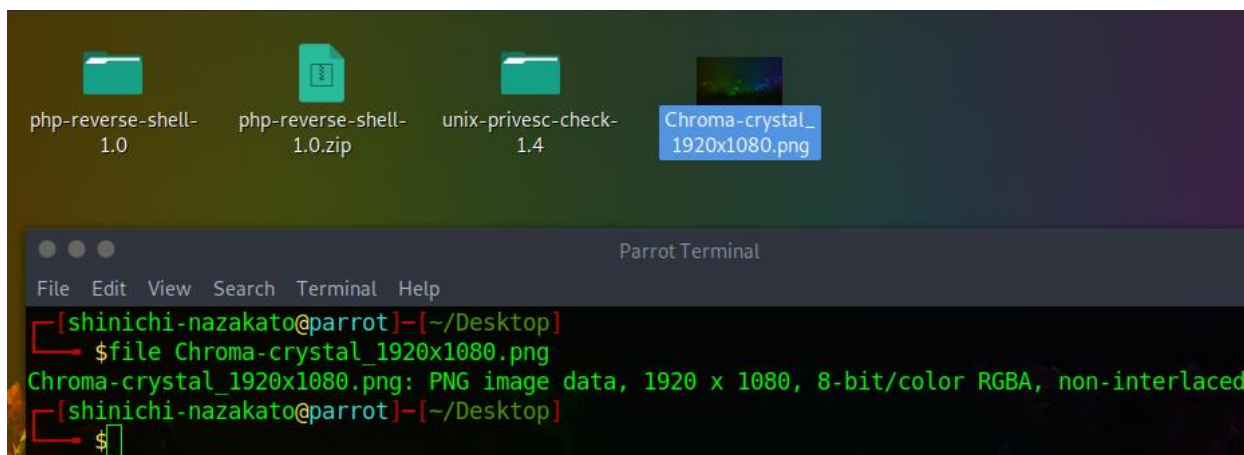
Metode Biasa - memakai notepad++



The screenshot shows a Notepad++ window titled "D:\Wallpapers\Wallpaper Razer\Chroma-crystal_1920x1080.png - Notepad++". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Macro, and Run. The toolbar contains various icons for file operations and editing. The active tab is "Chroma-crystal_1920x1080.png". The text content is as follows:

```
1  %PNG
2  SUB
3  NULNULNUL
4  IHDRNULNULBELNULNULEOTBSACKNULNULNULèóÁÇ
5  <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="A
6  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02
7  <rdf:Description rdf:about=""/>
8  </rdf:RDF>
9  </x:xmpmeta>
```

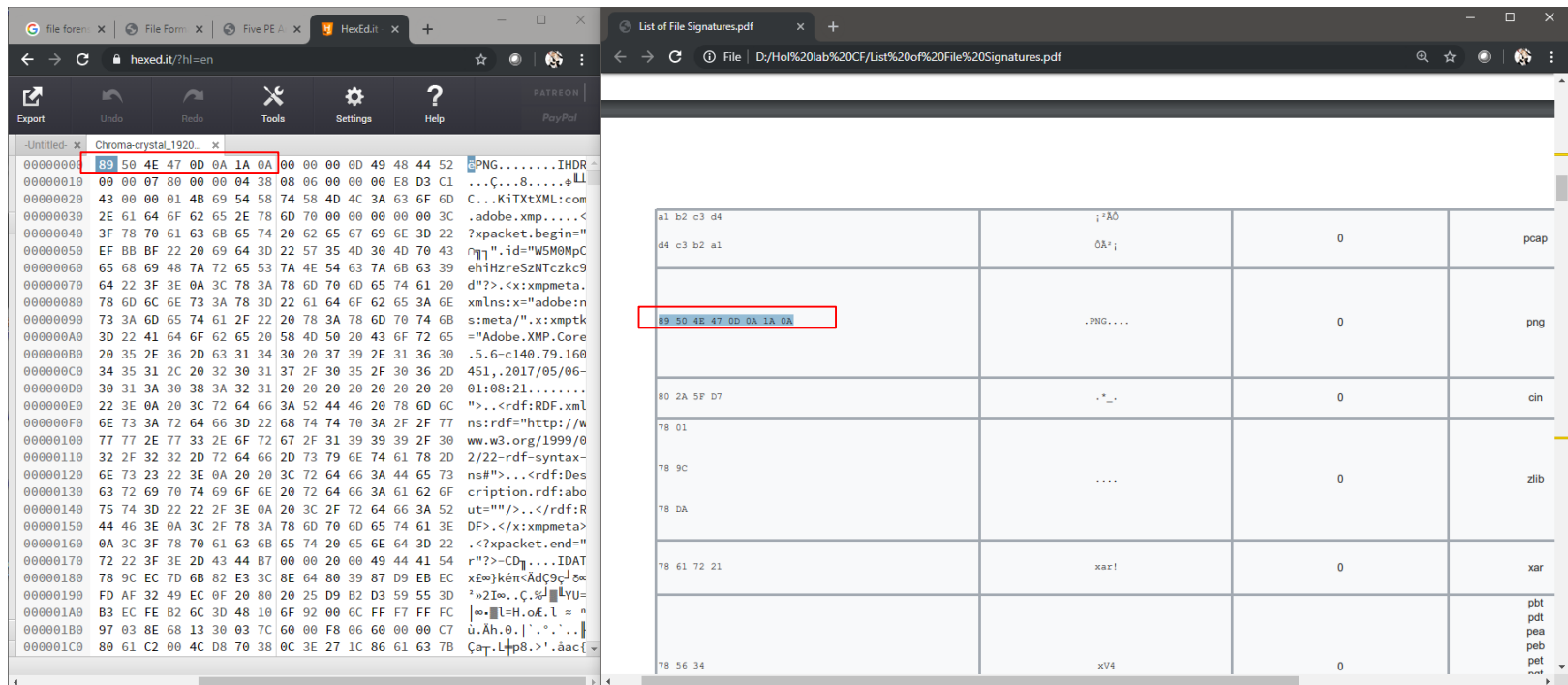
Metode cepat – 1 : memakai utility file di linux



*kalo mau sekaligus banyak file yang mau dicek, tinggal ganti aja commandnya jadi 'file *'

Metode cepat – 2 : Memakai hex editor + comparing dgn preset signature

url Hex Editor : <https://hexed.it/?hl=en>



dalam file identification dan analysis, prinsip pertama yang harus kalian pegang : file ekstensi yang kita lihat di mata ga selalu sama dengan isinya.

Btw saya sudah menyiapkan pdf berisi preset signature hex header file untuk memandu kalian jika ingin melakukan analisis hex pada file evidence.

Link :

https://drive.google.com/drive/folders/1QouHauW_3s4EEMoRo_f9uuG23ZY1-vLh?usp=sharing

Extra materials - CTF Forensik

Terkadang dalam challenge CTF forensik yang mengharuskan kita melakukan identifikasi file, seringkali terdapat flagnya di footer sebuah file.

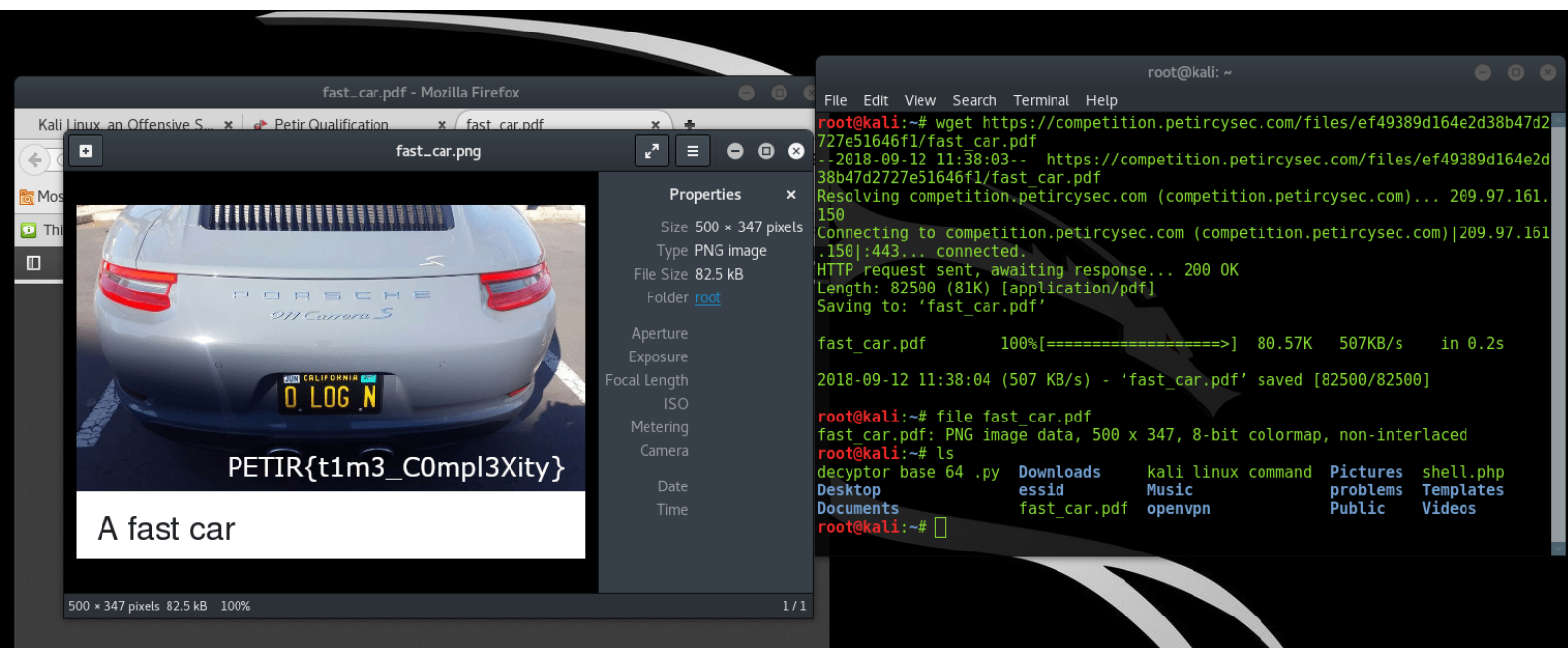
Saya kasih contoh deh memakai soal Qual petir 2018.

```
root@kali:~/Documents# strings isitbroken.png
xxxx
IHDR
      pHYS
8(iTXtXML:com.adobe.xmp
<?xpacket begin="
" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="i don't think it's broken">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    <rdf:Description rdf:find something xmlns:xmp="http://ns.adobe.com/xap/1.0/"
0/"
      xmlns:dc="http://purl.org/dc/elements/1.1/"
      xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/"
      xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/"
12714 227.396 2024
12715 227.399 2164
12716 227.399 456
12717 227.457 219
12718 227.458 593
12719 227.464 526
Urgent pointer:
Operations: (12 byte
  No-Operation (
  No-Operation (
  Timestamp TS
  [SEQ/ACK analysi
  Secure Sockets Laye
0000 c0 70 09 0 f2
0010 00 e4 98 10 40
0020 00 00 00 00 00
```

```
~;W"
JPc:
]F;Ikf
w EI
'c:?
e;=6
PETIR{iT_1s_Br0k3n_F0r_som3_R3as0n}
root@kali:~/Documents#
```

jadi awalnya file yang mau saya periksa itu ga bisa dibuka , lalu saya memutuskan untuk melihat isi dari file tersebut dengan memakai command “strings”.

Contoh lagi, kali ini yang bermasalah adalah extension filenya yang tidak sesuai dengan header file yang bersangkutan



ini cara solvenya tinggal ganti extension aja sih dari pdf ke .png

Registry Analysis

Requirements :

Registry Workshop, Regripper, hivexsh, .etc

File yang dianalisa : .reg

WARNING ! jangan melakukan analisis registry di main system kalau mau sekedar coba-coba ! gunakan VM windows dan atau VM Parrot OS / Kali

--- --- Welcome to the hell :D --- ---

Registry Analysis berfokus pada analisa pada Registry windows yang rusak / ada masalah di dalamnya.

Untuk materinya, saya akan mengambil dari sini:

<https://what-when-how.com/windows-forensic-analysis/registry-analysis-windows-forensic-analysis-part-1/>

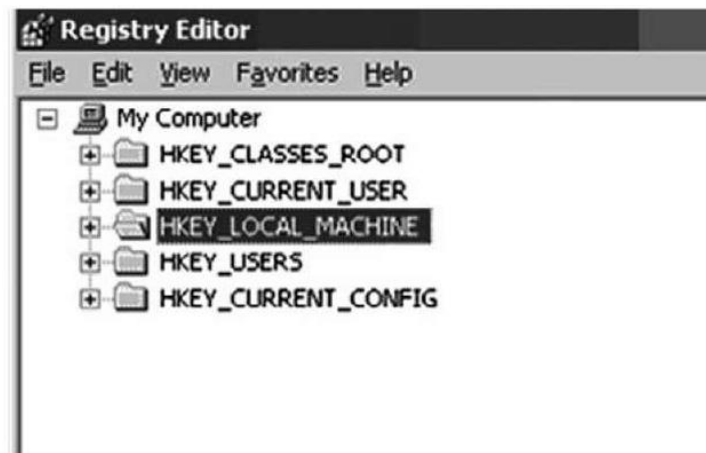
<https://what-when-how.com/windows-forensic-analysis/registry-analysis-windows-forensic-analysis-part-2/>

Apa itu Registry?

Intinya, Registry itu adalah database pusat yang secara hierarki memanajemen konfigurasi untuk aplikasi, hardware device, dan Registry menggantikan sistem text-based config yang digunakan pada windows 3.1 dan yang jadul-jadul sebelum windows NT.

Kalau pada jaman dulu, semua konfigurasi itu di windows masih terpisah-pisah. Dan user bisa berkontak langsung dengan settingnya (kurang bagus karena jika ada misconfig bisa kena semuanya.). maka dari itu diciptakan registry sebagai core dari windows. Untuk bisa berinteraksi dengan registry, user harus memakai aplikasi perantara agar user tidak berinteraksi secara langsung dengan key yang spesifik dan value yang ada dalam registry (reg.exe, RegEdit.exe).

Jadi kalau kita buka regedit, inilah yang akan kita dapatkan.



Tiap Hive disini memainkan peran penting dalam fungsionalitas sistem.

- **HKEY_USERS**
berisi semua profil pengguna yang dimuat secara aktif untuk sistem.
- **HKEY_CURRENT_USER**
Isinya adalah semua active, loaded user profile yang dimana usernya sedang logged-in di sistem.
- **HKEY_LOCAL_MACHINE**
Isinya merupakan beragam config information untuk sistem, sudah termasuk settingan hardware kita dan software setting.
- **HKEY_CURRENT_CONFIG**
Berisi profile hardware yang sistem pakai saat startup.
- **HKEY_CLASSES_ROOT**
Berisi informasi konfigurasi yang berkaitan dengan aplikasi mana yang digunakan untuk membuka berbagai file pada sistem. Hive ini disubklasifikasikan ke HKEY_CURRENT_USER \ Software \ Classes (pengaturan khusus pengguna) dan HKEY_LOCAL_MACHINE \ Software \ Classes (pengaturan seluruh sistem).

Registry Path dan file path yang berkaitan :

- HKEY_LOCAL_MACHINE\System ::: %WINDIR%\system32\config\System
- HKEY_LOCAL_MACHINE\SAM ::: %WINDIR%\system32\config\Sam
- HKEY_LOCAL_MACHINE\Security ::: %WINDIR%\system32\config\Security
- HKEY_LOCAL_MACHINE\Software ::: %WINDIR%\system32\config\Software
- HKEY_LOCAL_MACHINE\Hardware ::: Volatile hive
- HKEY_LOCAL_MACHINE\System\Clone ::: Volatile hive
- HKEY_USERS\Default ::: %WINDIR%\system32\config\default
- HKEY_USERS\User SID ::: User profile (NTUSER.DAT); "Documents and Settings\User (changed to "Users\User" on Vista)

Tip :

Windows vista dan windows 7 punya tambahan file Registry hive, dimana ada komponen hive file (bisa ditemukan di system32\Config dir) dan usrclass.dat yang semuanya ini terletak pada C:\Users\username\AppData\Local\Microsoft\Windows.

Beberapa registry hive bersifat volatile dan tidak terdapat dalam file di hard drive. Hive-hive yang volatile ini dibuat saat sistem baru berjalan dan tidak tersedia jika sistemnya sudah mati. Penting utk tahu saat mau melakukan forensic registry, jika ada data dalam hive yang volatile , kita bisa melakukan export semua volatile hive ke .reg file via regedit.exe atau memakai mekanisme lain untuk mengumpulkan data spesifik dari volatile hive sebelum sistemnya dimatikan.

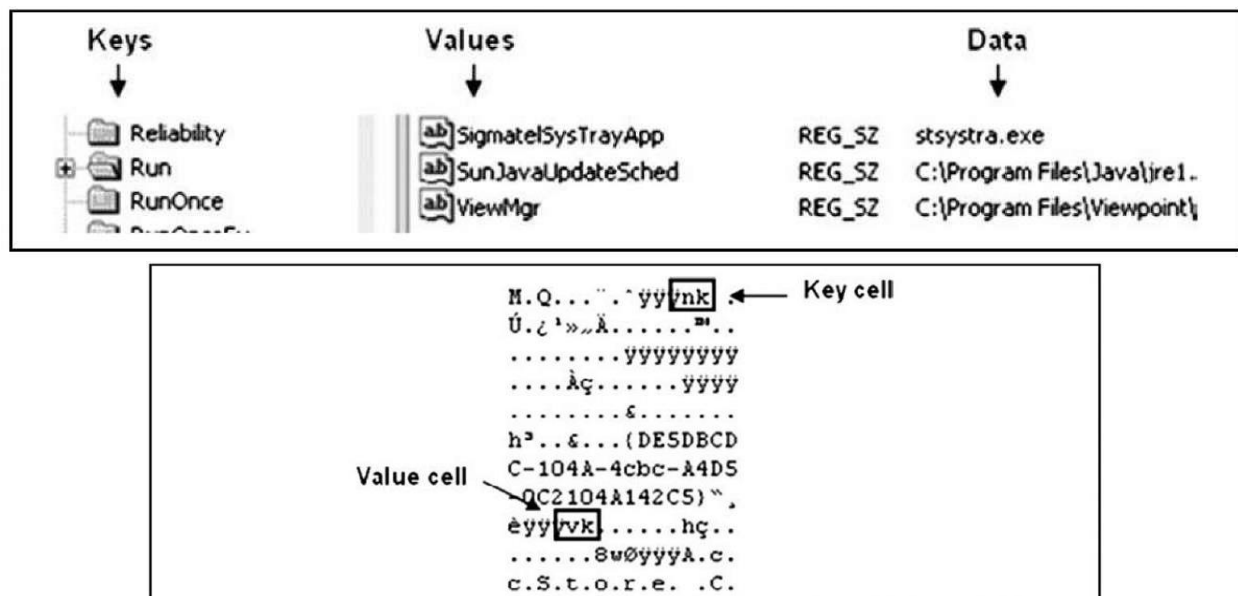
Registry Data Types

- **REG_BINARY** : Raw binary data
- **REG_DWORD** : Data represented as a 32-bit (4-byte) integer
- **REG_SZ** : A fixed-length text string
- **REG_EXPAND_SZ** : A variable-length data string
- **REG_MULTI_SZ** : Multiple strings, separated by a space, comma, or other delimiter
- **REG_NONE** : No data type
- **REG_QWORD** : Data represented by a 64-bit (8-byte) integer
- **REG_LINK** : A Unicode string naming a symbolic link
- **REG_RESOURCE_LIST**
A series of nested arrays designed to store a resource list
- **REG_RESOURCE_REQUIREMENTS_LIST**
A series of nested arrays designed to store a device driver's list of possible hardware resources
- **REG_FULL_RESOURCE_DESCRIPTOR**
A series of nested arrays designed to store a resource list used by a physical hardware device

Bisa kita lihat, berbagai tipe data ditemukan di Registry. Tampaknya tidak ada aturan atau konsistensi antara nilai-nilai yang ditemukan dalam kunci yang berbeda; nilai-nilai yang melayani tujuan yang sama mungkin memiliki tipe data yang berbeda, memungkinkan data mereka diformat dan disimpan secara berbeda. Ini dapat menjadi masalah ketika kita melakukan pencarian teks untuk data dalam Registry. Di mana satu aplikasi mungkin menyimpan daftar dokumen yang baru-baru ini diakses sebagai string teks ASCII, yang lain mungkin menyimpan daftar yang mirip dengan string Unicode dalam tipe binary data, dalam hal ini pencarian teks ASCII akan kehilangan data itu.

Tapi dalam regedit sekarang ada 'find tool' untuk mencari string ASCII saja dan bukan DWORD / Binary Data.

Struktur Registry Hive



- Key Cell
Berisi semua registry key information dan sudah termasuk offset untuk cell lain sebagaimana LastWrite time untuk key nya (signature : kn)
- Value Cell
isi cell ini adalah value dan data-datanya (signature : kv)
- Subkey List cell
Merupakan cell yang terdiri dari beberapa index / offset yang menjadi pointer ke key cells ; semua subkey untuk ke parent key cell

- Value list cell
cell yang terdiri dari beberapa index / offset yang menjadi pointer ke value cells ; semua value dari sebuah key cell
- Security Descriptor cell
Cell yang berisi security descriptor information untuk sebuah key cell.
(signature : ks)

Contoh Case Study :

Cyber Jawa 2018 – Windows Registry

Anda dimintai tolong oleh rekan Anda untuk memeriksa Windows-nya yang terkena **malware**. Anda pun melakukan dump terhadap Registry-nya. Diketahui bahwa malware tersebut berhasil menanamkan persistence dan tereksekusi setiap Windows tersebut startup. Apakah ada sesuatu pada Registry tersebut?

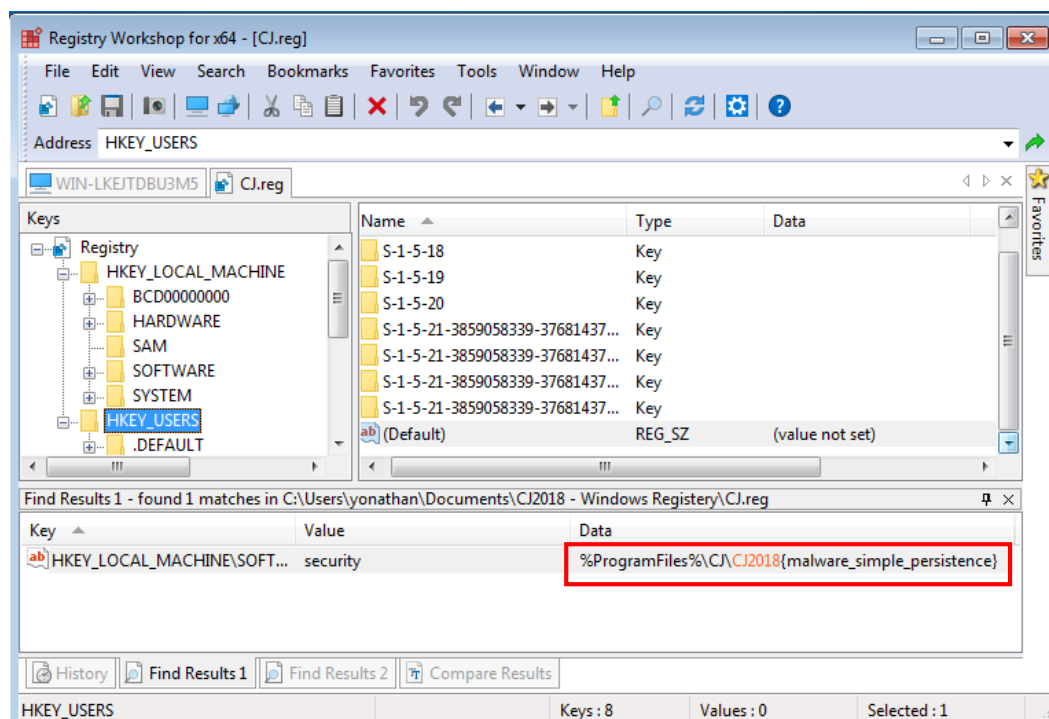
Attachment-file:

<https://drive.google.com/drive/folders/1IwHMww37EOB2eS1tLw-lydeBBQXitMqA?usp=sharing>

***Catatan : Flag dalam format CJ2018{flag}*

Solve :

Dengan memakai Registry Workshop , saya tinggal melakukan search flag dengan memakai fitur 'find'.



Data Recovery

Intinya adalah kita melakukan proses recovery atas data yang rusak agar bisa diakses seperti sediakala. Bisa juga diartikan kita mengekstrak data spesifik dari media yang mengalami kerusakan.

Disini masih dibagi lagi apa saja yang biasanya di-recover:

- File-file yang dihapus secara sengaja
- File-file yang terhapus secara tak sengaja
- File-file hidden dalam partisi - memerlukan carving
- File-file yang di-hidden akibat infeksi malware

Untuk tools-toolsnya secara lengkap bisa cek ke sini:

https://www.forensicswiki.org/wiki/Tools:Data_Recovery

untuk tools-tools yang biasanya digunakan secara umumnya :

- Recuva - digunakan untuk melakukan recover pada file yang terhapus dan file yang di-hidden oleh malware.
- Foremost - merecover file berdasarkan header, footer dan internal data structures filenya.
- Stellar Data Recovery
- MiniTool Partition recovery - bantu recover partisi yang rusak, terhapus di windows.

Memory Dump Analysis

Apa itu memory dump?

Memory dump merupakan proses dimana kita mengambil semua informasi dalam RAM dan write semua kontennya ke drive kita. Biasanya dump memori digunakan banyak dev untuk mendapatkan informasi diagnostik atas sebuah crash yang terjadi, untuk membantu troubleshooting dimana masalahnya dan juga event-event yg jadi biang kerok masalah.

Beberapa error tidak bisa direcover karena mereka butuh re-booting utk mendapatkan fungsionalitasnya lagi, namun informasi yang tersimpan di RAM saat terjadinya crash sistem memberikan code yang menjadi penanda errornya. Memory dump menyimpan semua data yang bisa aja hilang karena overwrite memory dan juga karena sifatnya RAM yang volatile.

Di OS windows, biasanya memory dump akan nampak di BsoD, dan biasanya kita ditampilkan apa masalahnya. Perlu diingat bahwa di dalam dump memori bisa terdapat pula beberapa data penting semisal password dan username kita (dan semua itu dalam plaintext), juga decryption key yang ga bisa dijangkau dengan cara biasa.

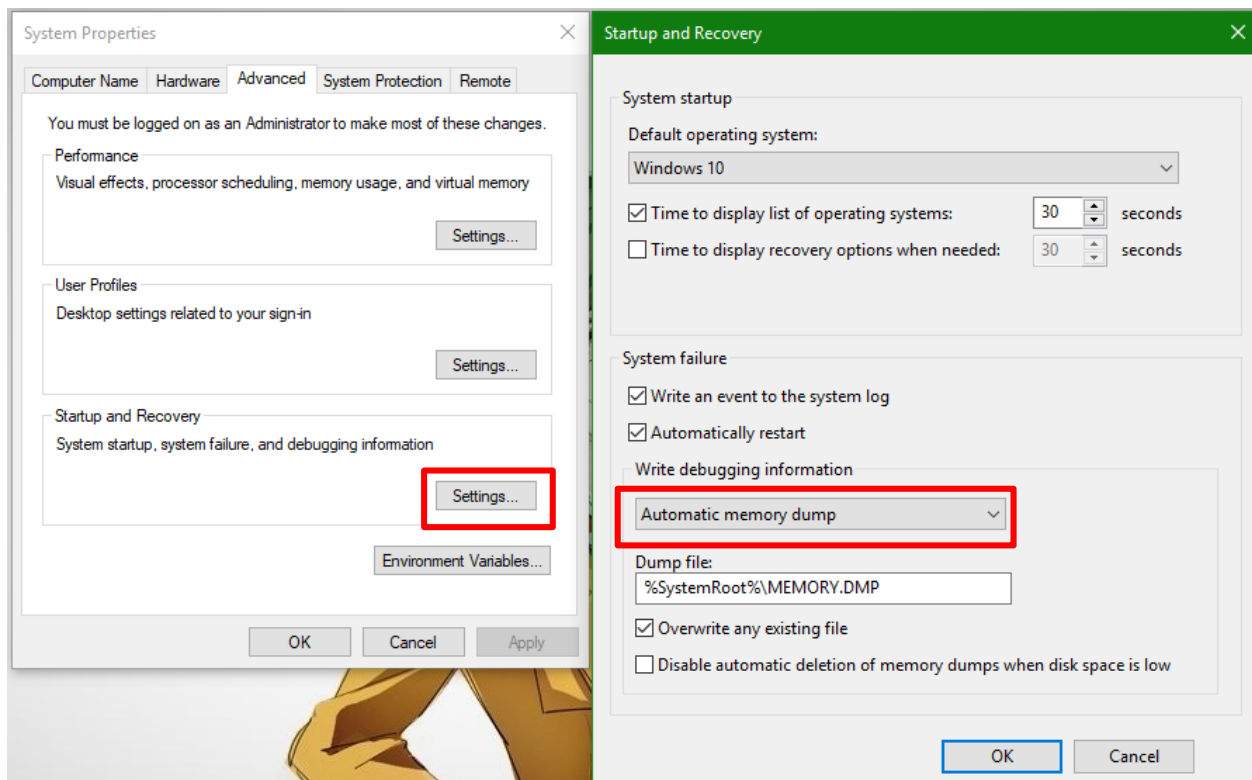
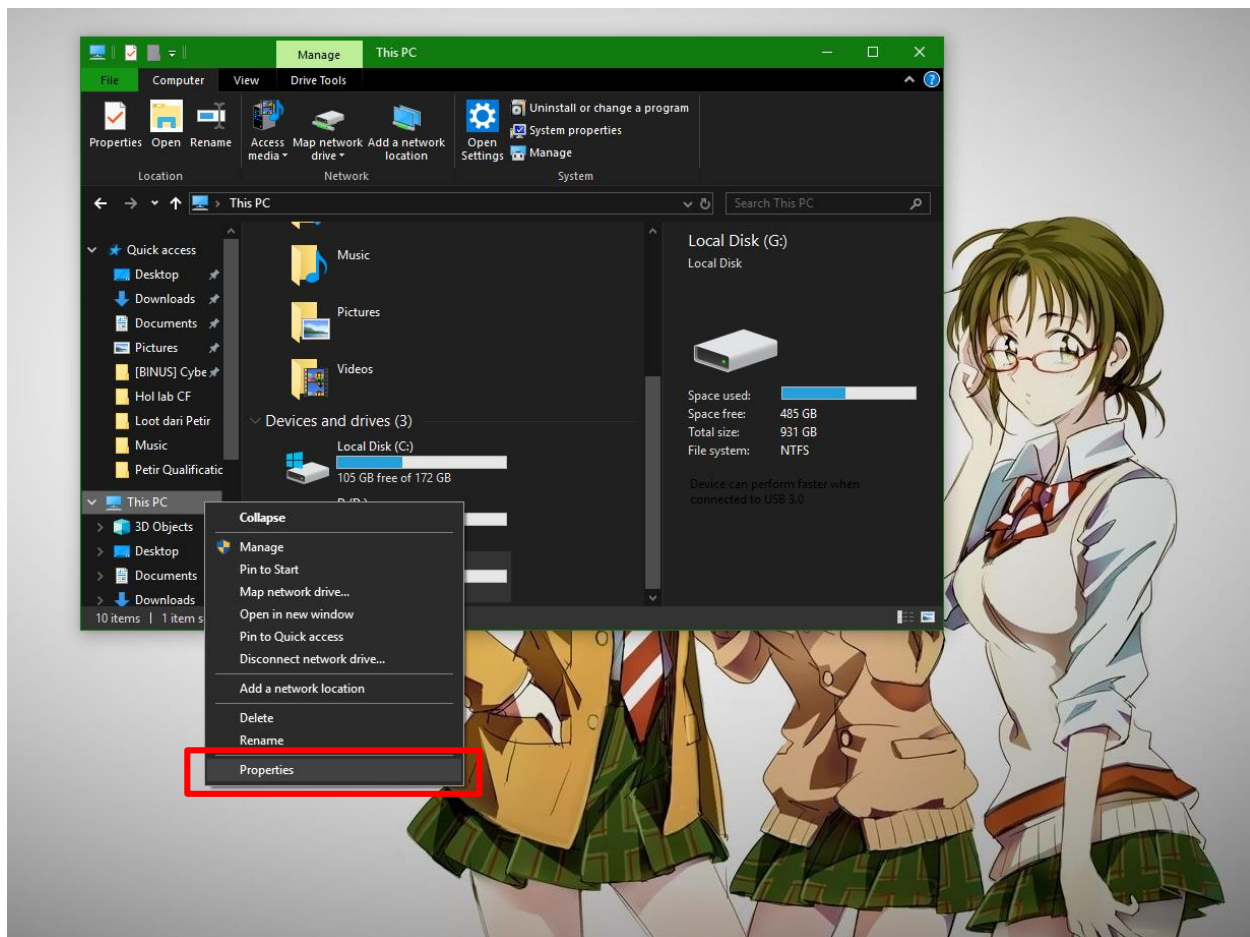
Tools : volatility, mimkatz (windows)

File yang dianalisa : .dmp

Cara membuat file dump secara komplit

- Buka File Explorer
- Klik kanan pada 'This PC'
- Pilih properties
- Masuk ke tab 'Advanced'
- Masuk ke settings dari 'Startup & Recovery'
- Pada bagian write debugging indormation, ganti aja automatic ke complete.

Saya kasih lihat mana-mana saja yang harus dibuka. Lihat yang saya tandain merah.



Mengakses Hiberfil.sys

Hiberfil.sys sendiri merupakan file yang secara default digunakan windows untuk menyimpan keadaan mesin sebagai bagian dari proses hibernasi. OS juga menyimpan pegangan file yang terbuka untuk file ini, sehingga tidak ada pengguna, termasuk Administrator, yang dapat membaca file saat sistem sedang berjalan. Hiberfil.sys juga Merupakan file yang terkompres yang berisi copy dari daat sistem mau hibernasi.

Hiberfil.sys harus di-dekompres dengan memakai volatility dan mengkonversinya menjadi bentuk raw memory dump. Kita bisa memanfaatkan plugin imagecopy untuk mengcopy hiberfil.sys jadi file raw dump.

Sebenarnya ada beberapa plugin dalam volatility yang bisa memberikan informasi yang relevan sesuai plugin yang digunakan. Biasanya karena sistem hibernasi itu memutus koneksi jaringan, maka plugin untuk meng-capture isi koneksi networknya tidak bisa bekerja. Secara umum proses yang paling penting dilakukan saat mengecek file ini adalah mengecek proses yang berjalan dengan plugin 'pslist'.

Malware biasanya juga suka membersihkan jejak sebelum komputer masuk mode hibernasi, yang membuat proses forensik makin susah. Kita masih ada kesempatan untuk mendapatkan informasi dengan memanfaatkan plugin 'malfind' untuk mencari tahu mana malware yang menginjeksi dirinya ke beberapa proses yang berbeda.

Ada tambahan lagi, terdapat pula pagefile.sys yang biasanya digunakan untuk menyimpan frame dari memori yang tidak fit ke memori fisik. Windows support sampai 16 paging file, namun secara praktikal yang dipakai Cuma 1 aja. Page file tidak bisa diproses dengan volatility.

Link Materi (hiberfil.sys) :

- <https://www.groovypost.com/howto/microsoft/what-is-hiberfil-sys-and-why-is-it-using-so-much-hard-drive-space/>
- <https://technical.nttsecurity.com/post/102dwiw/hibernation-and-page-file-analysis>
- <https://www.forensicswiki.org/wiki/Hiberfil.sys>
- <https://www.hackingarticles.in/forensics-analysis-of-pagefile-and-hibersys-file-in-physical-memory/>

Finding relevant evidence (browser history, email, last running program, etc)

Kita pakai contoh kasus aja ya biar lebih jelas. Kebetulan saya sudah membackup beberapa soal Cyber Jawa 2018 untuk bagian forensiknya saat akan membuat HoL ini. Saya akan membahasnya semua disini. Jika kalian mau coba-coba solve soalnya, silakan saja, tapi untuk safety measures, saya menyarankan untuk mengerjakannya di VM, jangan di main system.

Cyber Jawa 2018 - LSASS

LSASS atau Local Security Authority Subsystem Service adalah layanan pada Windows terkait dengan otentikasi seperti pergantian password dan access token. Berikut adalah memory dump terhadap lsass.exe pada Windows 7. Dapatkah Anda menemukan **password** dari salah satu user pada sistem tersebut? (Flag dalam format CJ2018{flag})

Attachment :

https://drive.google.com/drive/folders/1EFU_f9h9nV2tHRAubUhBIAC0pwe6OPsb?usp=sharing

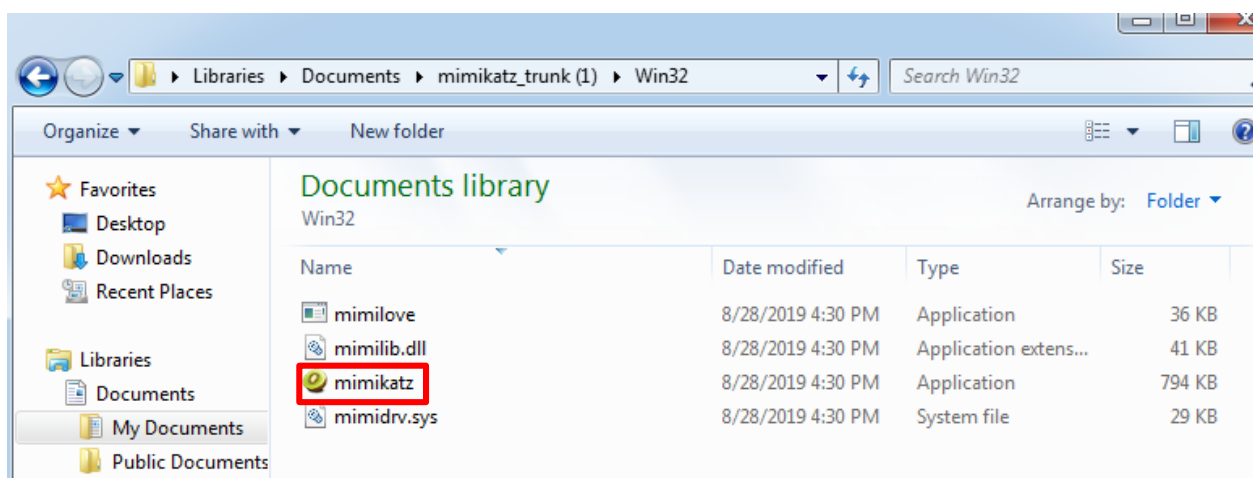
Solve :

Saya memakai **mimikatz** untuk menyelesaikan soal ini.

Silakan download mimikatz versi yang sudah di-compile disini ;

https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20190710/mimikatz_trunk.zip

Setelah ter-download, saya tinggal buka saja mimikatz.exe-nya



Dump file LSASS.dmpnya ke Mimikatz

sekurlsa::minidump lsass.dmp

lalu kita buka file dump tersebut memakai tspkg

sekurlsa::tspkg



```
mimikatz 2.2.0 x86 (oe.eo)
mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::tspkg
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 631221 (00000000:0009a1b5)
Session : Interactive from 2
User Name : CJ
Domain : IE11WIN7
Logon Server : IE11WIN7
Logon Time : 8/15/2018 2:21:26 PM
SID : S-1-5-21-3463664321-2923530833-3546627382-1001
tspkg :

Authentication Id : 0 ; 631199 (00000000:0009a19f)
Session : Interactive from 2
User Name : CJ
Domain : IE11WIN7
Logon Server : IE11WIN7
Logon Time : 8/15/2018 2:21:26 PM
SID : S-1-5-21-3463664321-2923530833-3546627382-1001
tspkg :

Authentication Id : 0 ; 137302 (00000000:00021856)
Session : Interactive from 1
User Name : IEUser
Domain : IE11WIN7
Logon Server : IE11WIN7
Logon Time : 8/15/2018 2:16:11 PM
SID : S-1-5-21-3463664321-2923530833-3546627382-1000
tspkg :

Authentication Id : 0 ; 137239 (00000000:00021817)
Session : Interactive from 1
User Name : IEUser
Domain : IE11WIN7
Logon Server : IE11WIN7
Logon Time : 8/15/2018 2:16:11 PM
SID : S-1-5-21-3463664321-2923530833-3546627382-1000
tspkg :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session : Service from 0
User Name : LOCAL SERVICE
Domain : NT AUTHORITY
Logon Server : <null>
Logon Time : 8/15/2018 2:16:04 PM
SID : S-1-5-19
tspkg :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session : Service from 0
User Name : IE11WIN7$
Domain : WORKGROUP
Logon Server : <null>
Logon Time : 8/15/2018 2:16:04 PM
SID : S-1-5-20
tspkg :

Authentication Id : 0 ; 25452 (00000000:0000636c)
Session : UndefinedLogonType from 0
User Name : <null>
Domain : <null>
Logon Server : <null>
Logon Time : 8/16/2018 5:16:00 AM
SID :
tspkg :
```

Tujuan kita adalah untuk mendapatkan password dari usernya saja.

Sekurlsa::logonPasswords

```
mimikatz 2.2.0 x86 (oe.eo)
Authentication Id : 0 ; 999 (00000000:000003e7)
Session          : UndefinedLogonType from 0
User Name        : IE11WIN7$
Domain           : WORKGROUP
Logon Server      : (null)
Logon Time       : 8/16/2018 5:16:00 AM
SID              : S-1-5-18
      tspkg :

mimikatz # sekurlsa::logonPasswords
Authentication Id : 0 ; 631221 (00000000:0009a1b5)
Session          : Interactive from 2
User Name        : CJ
Domain           : IE11WIN7
Logon Server      : IE11WIN7
Logon Time       : 8/15/2018 2:21:26 PM
SID              : S-1-5-21-3463664321-2923530833-3546627382-1001
      msv :
      [00000003] Primary
      * Username : CJ
      * Domain   : IE11WIN7
      * NTLM     : 24191937d471eea79e394dc523a872b0
      * SHA1     : fd50f14b4a8b5b100840ea73d10af766ad8d1586
      [00010000] CredentialKeys
      * NTLM     : 24191937d471eea79e394dc523a872b0
      * SHA1     : fd50f14b4a8b5b100840ea73d10af766ad8d1586
      tspkg :
      wdigest :
      * Username : CJ
      * Domain   : IE11WIN7
      * Password : CJ2018<red_teaming>
      kerberos :
      * Username : CJ
      * Domain   : IE11WIN7
      * Password : (null)
      ssp :
      credman :
```

Cyber Jawa 2018 - In Memory Forensic

Kepolisian Republik Indonesia dan BSSN di bawah koordinasi Forensik Specialist Mr. Hamdan Abdul Aziz melacak dan menangkap tersangka utama pimpinan geng penjahat siber yang beroperasi di Bali. Dalam modus operandinya pelaku dengan inisial M.S melancarkan aksinya dengan mengkordinasikan geng cyber criminalnya yang beroperasi dari Eropa Timur melalui Facebook. Didapatkan barang bukti berupa puluhan kartu kredit serta debit, 7 buah smartphone, dan 3 buah laptop. Dari sekian artifact forensik yang harus dilakukan analisis secara mendalam, terdapat sebuah file penting yang didapatkan ketika komputer masih dalam keadaan hidup. Bantu Kang Hamdan untuk menemukan credential facebook tersangka M.S

Attachment :

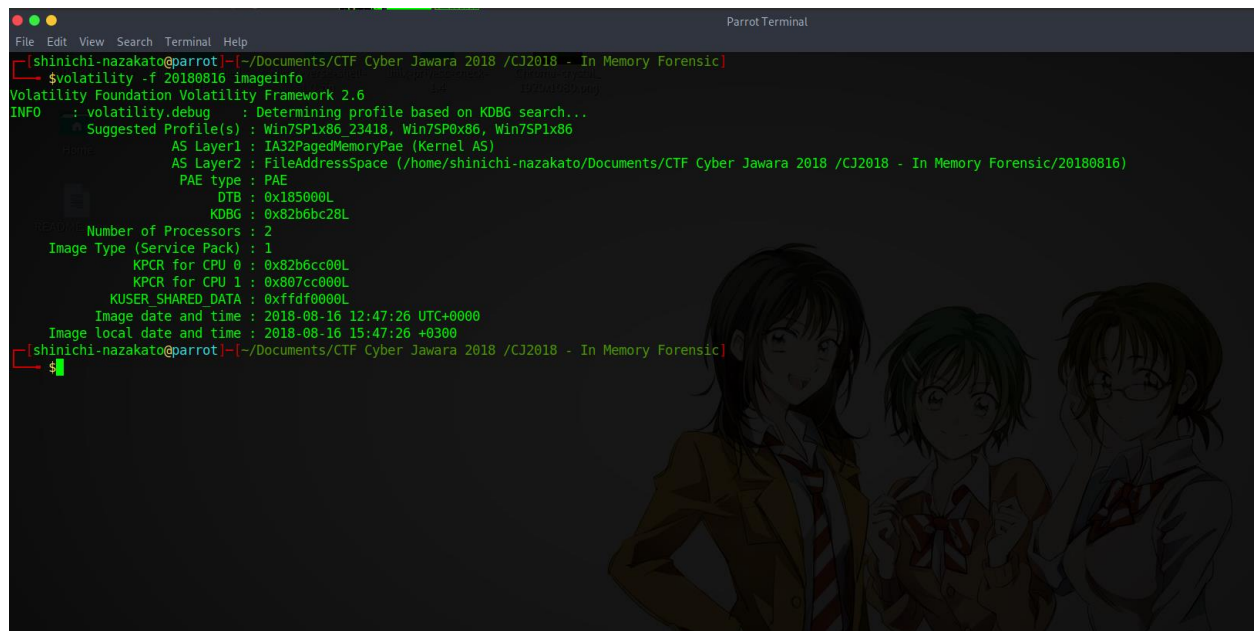
<https://drive.google.com/drive/folders/1SBjly2roUdgoK48Dwseq8AGNENVVn-kp?usp=sharing>

Format Flag: CJ2018{passwordfacebook}

Solve:

Decompress file nya dengan command : **lzma -d 20180816.lzma**

Kami memakai Volatility untuk menyelesaikan analisa terhadap file memory dump yang ada.



```
shinichi-nazakato@parrot: ~/Documents/CTF Cyber Jawa 2018 /CJ2018 - In Memory Forensic
$volatility -f 20180816 imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/shinichi-nazakato/Documents/CTF Cyber Jawa 2018 /CJ2018 - In Memory Forensic/20180816)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82b6bc28L
      Number of Processors : 2
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x82b6cc00L
      KPCR for CPU 1 : 0x807cc000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2018-08-16 12:47:26 UTC+0000
      Image local date and time : 2018-08-16 15:47:26 +0300
shinichi-nazakato@parrot: ~/Documents/CTF Cyber Jawa 2018 /CJ2018 - In Memory Forensic
$
```

Kita melakukan pengecekan profile dengan memakai imageinfo. Dapat informasi kalo pelaku memakai sistem windows 7. Profile yang akan kita gunakan selanjutnya adalah **Win7SP1x86_23418** untuk melakukan memory dump dan analisa proses yang berjalan.

Untuk mengecek proses, tinggal gunakan **pslist** untuk list proses. Kenapa kita list proses? Karena kita disuruh mencari password FB yang kemungkinan besar ada di browser.

```

[shinichi-nazakato@parrot]~/Documents/CTF Cyber Jawa 2018 /CJ2018 - In Memory Forensic
$volatility -f 20180816 --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name      PID  PPID  Thds  Hnds  Sess  Wow64  Start      Exit
-----
0x8433a8a8 System    4      0     89   509   -----  0  2018-08-16 11:32:22 UTC+0000
0x84d76d40 smss.exe  264    4      2     30   -----  0  2018-08-16 11:32:22 UTC+0000
0x84d88030 csrss.exe 340   320    9    365    0  2018-08-16 11:32:23 UTC+0000
0x84cd2d40 csrss.exe 388   380    9    512    1  2018-08-16 11:32:24 UTC+0000
0x843a2200 wininit.exe 396   320    3     77    0  2018-08-16 11:32:24 UTC+0000
0x853c6d40 winlogon.exe 436   380    3    110    1  2018-08-16 11:32:24 UTC+0000
0x853e1030 services.exe 484   396    8    191    0  2018-08-16 11:32:24 UTC+0000
0x853e9b80 lsass.exe 492   396    7    611    0  2018-08-16 11:32:24 UTC+0000
0x853e6170 lsm.exe 500   396   11    203    0  2018-08-16 11:32:24 UTC+0000
0x8541fa58 svchost.exe 604   484    9    359    0  2018-08-16 11:32:25 UTC+0000
0x85431380 VBoxService.exe 668   484   12    117    0  2018-08-16 11:32:25 UTC+0000
0x8543d030 vmacthlp.exe 688   484    3     55    0  2018-08-16 11:32:26 UTC+0000
0x8544a890 svchost.exe 764   484    8    266    0  2018-08-16 11:32:26 UTC+0000
0x85466030 svchost.exe 848   484   18    431    0  2018-08-16 11:32:26 UTC+0000
0x85484b78 svchost.exe 900   484   16    416    0  2018-08-16 11:32:26 UTC+0000
0x8548b030 svchost.exe 944   484   29   1015    0  2018-08-16 11:32:26 UTC+0000
0x854cf840 svchost.exe 1068   484   10    276    0  2018-08-16 11:32:27 UTC+0000
0x854cf840 svchost.exe 1184   484   23    758    0  2018-08-16 11:32:27 UTC+0000
0x854ff228 spoolsv.exe 1300   484   12    317    0  2018-08-16 11:32:28 UTC+0000
0x85512c88 svchost.exe 1328   484   19    310    0  2018-08-16 11:32:28 UTC+0000
0x85578030 VGAuthService.exe 1456   484    3     89    0  2018-08-16 11:32:28 UTC+0000
0x856c8318 taskhost.exe 620   484    7    159    1  2018-08-16 11:32:47 UTC+0000
0x856e2b08 dwm.exe 1140   900    3     73    1  2018-08-16 11:32:47 UTC+0000
0x856ef5b0 explorer.exe 1452  1016   29    950    1  2018-08-16 11:32:47 UTC+0000
0x85728208 VBoxTray.exe 1912  1452   13    154    1  2018-08-16 11:32:49 UTC+0000
0x854c2430 SearchIndexer.exe 320   484   13    806    0  2018-08-16 11:32:56 UTC+0000
0x855c9030 svchost.exe 3188   484    5     84    0  2018-08-16 11:34:35 UTC+0000
0x855c0030 svchost.exe 3248   484   12    341    0  2018-08-16 11:34:35 UTC+0000
0x8581e768 iexplore.exe 3392  1452   12    585    1  2018-08-16 11:34:39 UTC+0000
0x85401b58 iexplore.exe 3432  3392   28    692    1  2018-08-16 11:34:39 UTC+0000
0x84508030 firefox.exe 2876  1452   64   1224    1  2018-08-16 11:35:53 UTC+0000
0x844ef030 firefox.exe 3844  2876    0 -----  1  2018-08-16 11:36:00 UTC+0000 2018-08-16 11:36:20 UTC+0000
0x84502848 firefox.exe 1612  2876   26    351    1  2018-08-16 11:36:01 UTC+0000
0x844f9030 firefox.exe 2512  2876    0 -----  1  2018-08-16 11:36:03 UTC+0000 2018-08-16 11:45:15 UTC+0000
0x84548298 firefox.exe 860   2876   25    323    1  2018-08-16 11:36:07 UTC+0000
0x84c50298 firefox.exe 2968  2876    0 -----  1  2018-08-16 11:36:52 UTC+0000 2018-08-16 11:45:03 UTC+0000
0x84ccc750 firefox.exe 3912  2876    0 -----  1  2018-08-16 11:38:18 UTC+0000 2018-08-16 11:45:06 UTC+0000
0x855a1030 notepad.exe 2752  1452    4    257    1  2018-08-16 11:43:47 UTC+0000
0x844aa4c8 iexplore.exe 2024  3392   27    716    1  2018-08-16 11:44:15 UTC+0000
0x85839ab8 firefox.exe 2276  2876   24    336    1  2018-08-16 11:45:19 UTC+0000
0x844bab50 firefox.exe 1124  2876   27    344    1  2018-08-16 11:45:24 UTC+0000
0x854f9030 firefox.exe 3772  2876   28    387    1  2018-08-16 11:50:15 UTC+0000
0x854a9708 cmd.exe 2920  1452    1     19    1  2018-08-16 11:50:32 UTC+0000
0x857fe340 conhost.exe 2344  388    2     51    1  2018-08-16 11:50:32 UTC+0000
0x857a6768 RamCapture.exe 1160  1452    6     69    1  2018-08-16 12:46:19 UTC+0000
0x857f2bd0 conhost.exe 3088  388    2     51    1  2018-08-16 12:46:19 UTC+0000

```

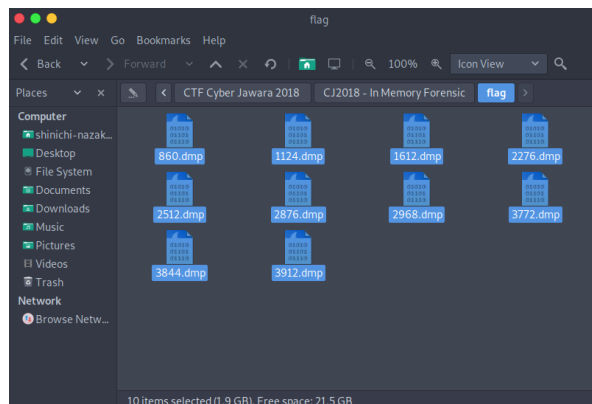
Ternyata ada beberapa proses firefox yang berjalan. Kita harus dump memorinya memakai memdump untuk menganalisa raw string yang ada di dalamnya.

```

0x84508030 firefox.exe 2876 1452 64 1224 1 0 2018-08-16 11:35:53 UTC+0000
0x844ef030 firefox.exe 3844 2876 0 ----- 1 0 2018-08-16 11:36:00 UTC+0000 2018-08-16 11:36:20 UTC+0000
0x84502848 firefox.exe 1612 2876 26 351 1 0 2018-08-16 11:36:01 UTC+0000
0x844f9030 firefox.exe 2512 2876 0 ----- 1 0 2018-08-16 11:36:03 UTC+0000 2018-08-16 11:45:15 UTC+0000
0x84548298 firefox.exe 860 2876 25 323 1 0 2018-08-16 11:36:07 UTC+0000
0x84c50298 firefox.exe 2968 2876 0 ----- 1 0 2018-08-16 11:36:52 UTC+0000 2018-08-16 11:45:03 UTC+0000
0x84ccc750 firefox.exe 3912 2876 0 ----- 1 0 2018-08-16 11:38:18 UTC+0000 2018-08-16 11:45:06 UTC+0000
0x855a1030 notepad.exe 2752 1452 4 257 1 0 2018-08-16 11:43:47 UTC+0000
0x844aa4c8 iexplore.exe 2024 3392 27 716 1 0 2018-08-16 11:44:15 UTC+0000
0x85839ab8 firefox.exe 2276 2876 24 336 1 0 2018-08-16 11:45:19 UTC+0000
0x844bab50 firefox.exe 1124 2876 27 344 1 0 2018-08-16 11:45:24 UTC+0000
0x854f9030 firefox.exe 3772 2876 28 387 1 0 2018-08-16 11:50:15 UTC+0000
0x854a9708 cmd.exe 2920 1452 1 19 1 0 2018-08-16 11:50:32 UTC+0000
0x857fe340 conhost.exe 2344 388 2 51 1 0 2018-08-16 11:50:32 UTC+0000
0x857a6768 RamCapture.exe 1160 1452 6 69 1 0 2018-08-16 12:46:19 UTC+0000
0x857f2bd0 conhost.exe 3088 388 2 51 1 0 2018-08-16 12:46:19 UTC+0000
[shinichi-nazakato@parrot]~/Documents/CTF Cyber Jawa 2018 /CJ2018 - In Memory Forensic
$volatility -f 20180816 --profile=Win7SP1x86_23418 memdump -p 2876,3844,1612,2512,860,2968,3912,2276,1124,3772 -D .

```

Tandai semua PID yang mau kita dump di memdump.



Ini hasil dump yang harus kita cek lebih lanjut

```
Parrot Terminal
File Edit View Search Terminal Help

10","formdata":"login_form\tlsd\tAVpnD-Wz\tthidden\tnotseen\nlogin_form\terror
_box\t\tthidden\tnotseen\nlogin_form\tdisplay\t\tthidden\tnotseen\nlogin_form\t
enable_profile_selector\t\tthidden\tnotseen\nlogin_form\tisprivate\t\tthidden\t
notseen\nlogin_form\tlegacy_return\t0\tthidden\tnotseen\nlogin_form\tprofile_s
elector_ids\t\tthidden\tnotseen\nlogin_form\treturn_session\t\tthidden\tnotseen
\nlogin_form\tskip_api_login\t\tthidden\tnotseen\nlogin_form\tsigned_next\t\tth
idden\tnotseen\nlogin_form\ttrynum\t2\tthidden\tnotseen\nlogin_form\ttimezone\t
-180\tthidden\tnotseen\nlogin_form\tlgndim\teyJ3IjozMjQ3LCJoIjo2NzQsImF3IjozM
DQ3LCJhaCI6Nm0LCJjIjoyNH0%3D\tthidden\tnotseen\nlogin_form\tlgnrnd\t054607_PV
pc\tthidden\tnotseen\nlogin_form\tlgnjs\t1534423571\tthidden\tnotseen\nlogin_fo
rm\temail\trateo.soldo%40gmail.com\ttext\tseen\nlogin_form\tpass\tYEa6H7pARnJ
nqFSb\tpassword\tseen\nlogin_form\tprefill_contact_point\trateo.soldo%40gmail
.com\tthidden\tnotseen\nlogin_form\tprefill_source\tbrowser_onload\tthidden\tno
tseen\nlogin_form\tprefill_type\tpassword\tthidden\tnotseen\nlogin_form\tfirst
_prefill_source\tbrowser_onload\tthidden\tnotseen\nlogin_form\tfirst_prefill_t
ype\tcontact_point\tthidden\tnotseen\nlogin_form\tthad_cp_prefilled\ttrue\tthidd
en\tnotseen\nlogin_form\tthad_password_prefilled\ttrue\tthidden\tnotseen\n0\tac
tion\thttps%3A%2F%2Fwww.facebook.com%2Flogin.php%3Flogin_attempt%3D1%26lww%3D
120%26lwc%3D1348092\taction\n0\tmethod\tpost\tmethod\n","current_pw_field_nam
e":"","docnum":0,"timestamp":1534423582616,"username":"rateo.soldo@gmail.com"
,"password":"YEa6H7pARnJnqFSb","tld":"facebook.com"}
└─[shinichi-nazakato@parrot]─[~/Documents/CTF Cyber Jawa 2018 /CJ2018 - In
Memory Forensic/flag]
└─ $strings *.dmp | grep "facebook" | grep "email" | grep "password"
```

Tinggal memakai regex dasar dan grep, langsung dapat flagnya.

Username cocok dengan inisial pelaku yang diberitahu sebelumnya.

****contoh kasus lain akan menyusul nanti.**

Antiforensics – Steganography

Steganography

Untuk teknik Steganografi sudah pernah dibahas di mata kuliah Security for Multimedia. Saya sudah memasukkan beberapa contoh prakteknya juga.

Attachments:

<https://drive.google.com/drive/folders/1iThkQwwgVISINcTXMNZhCaVA-ozgc57Y?usp=sharing>

Untuk latihan soal, soalnya akan menyusul nanti. (saya belum buat soalnya hehe)