ANÁLISIS FORENSE

Unidad 1. Actividad 7

9 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Práctica Evaluable análisis de memoria

1. Comprueba que la imagen de memoria pertenece al ordenador del alumno, llamado "DESKTOP-01S7HH9".

Primero descargamos el archivo que esta junto al pdf, despues lo metemos en la carpeta compartida que tenemos y lo descomprimimos con unzip.

Ahora para comprobar que la imagen de memoria pertenece al mismo usuario, hacemos el hash y lo comparamos:

```
┌──(kali㉿kali)-[~/volatility3]
└─$ shasum -a 256 DESKTOP-01S7HH9-20220408-171552.dmp
edcdbcac27263a45d6dfe27f6c8baff55952b2357a70031de20de057730cd359  DESKTOP-01S7HH9-20220408-171552.dmp
```

```
edcdbcac27263a45d6dfe27f6c8baff55952b2357a70031de20de057730cd359  DESKTOP-01S7HH9-20220408-171552.dmp
```

Como vemos son los mismos.

2. Determina el o los PID del proceso correspondiente a una aplicación para realizar chats, especialmente entre jugadores .de videojuegos. ¿Cuál es su proceso padre?

Ahora lo primero que vamos a usar es el comando imageinfo para saber que tipo de sistema operativo utilizaba:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search ...
```

```
          Suggested Profile(s) : Win10x64_17134, Win10x64_10240_17770, Win10x64_18362, Win10x64_14393, Win10x64, Win2016x64_14
393, Win10x64_16299, Win10x64_19041, Win10x64_17763, Win10x64_10586, Win10x64_15063 (Instantiated with Win10x64_15063)
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/kali/volatility/DESKTOP-01S7HH9-20220408-171552.dmp)
                      PAE type : No PAE
                           DTB : 0x1aa002L
                          KDBG : 0xf80013000b20L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff8000ecc3000L
                KPCR for CPU 1 : 0xffff9d01e1fc0000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2022-04-08 17:15:56 UTC+0000
     Image local date and time : 2022-04-08 19:15:56 +0200
```

Ahora sabemos que el que necesitamos es el **19041,** podemos usar el comando pslist para ver los procesos:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp --profile=Win10x64_19041 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffe70f4fa7b040 System                    4      0    142        0 ------      0 2022-04-08 17:01:02 UTC+0000
0xfffe70f4fbba040 Registry                 92      4      4        0 ------      0 2022-04-08 17:00:57 UTC+0000
0xfffe70f516e6040 smss.exe                344      4      2        0 ------      0 2022-04-08 17:01:02 UTC+0000
0xfffe70f554b1080 csrss.exe               452    436     10        0      0      0 2022-04-08 17:01:19 UTC+0000
0xfffe70f55676080 wininit.exe             524    436      1        0      0      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f55675080 csrss.exe               536    516     12        0      1      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f556c5080 winlogon.exe            616    516      3        0      1      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f55704100 services.exe            644    524      9        0      0      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f55706080 lsass.exe               660    524      9        0      0      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f5574b2c0 svchost.exe             772    644     17        0      0      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f5575a1c0 fontdrvhost.ex          796    616      5        0      1      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f557521c0 fontdrvhost.ex          804    524      5        0      0      0 2022-04-08 17:01:20 UTC+0000
0xfffe70f5579c340 svchost.exe             892    644     12        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f5641b2c0 svchost.exe             940    644      6        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f5643e080 dwm.exe                1016    616     16        0      1      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f564e62c0 svchost.exe             836    644      7        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f56504300 svchost.exe             472    644      1        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f565092c0 svchost.exe            1036    644      7        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f565372c0 svchost.exe            1120    644      8        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f5655d340 svchost.exe            1180    644      2        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f56578080 svchost.exe            1192    644      3        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f56576080 svchost.exe            1200    644      1        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f565c4080 svchost.exe            1296    644      7        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f565942c0 VBoxService.ex         1328    644     11        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f56629080 svchost.exe            1368    644      1        0      0      0 2022-04-08 17:01:21 UTC+0000
0xfffe70f5663e340 svchost.exe            1400    644      3        0      0      0 2022-04-08 17:01:21 UTC+0000
```

Ahora buscamos una aplicación de chat y videojuegos, como Discord.exe :

```
. 0xfffe70f513d8300:firefox.exe          1096   5664     16      0 2022-04-08 17:04:16 UTC+0000
 0xfffe70f56dbf300:Discord.exe           3112   5236     34      0 2022-04-08 17:03:37 UTC+0000
. 0xfffe70f57f99080:Discord.exe          6324   3112     42      0 2022-04-08 17:07:00 UTC+0000
. 0xfffe70f579f8080:Discord.exe           464   3112      7      0 2022-04-08 17:04:23 UTC+0000
. 0xfffe70f58863080:Discord.exe          8620   3112      6      0 2022-04-08 17:07:40 UTC+0000
. 0xfffe70f5817f080:Discord.exe          7068   3112      9      0 2022-04-08 17:05:59 UTC+0000
. 0xfffe70f57df1080:Discord.exe          6224   3112      9      0 2022-04-08 17:05:03 UTC+0000
 0xfffe70f55222080:jusched.exe           5572   4124      1      0 2022-04-08 17:03:28 UTC+0000
```

3. Determina a través de los manejadores qué documento estaba editando el alumno durante la redada policial.

Con el comando handles podemos obtener información sobre los objetos de manejo de archivos y procesos. Buscando un poco encontré este documento:

```
0xffffe70f57caa4d0   8852          0xc08        0x12019f File            \Device\HarddiskVolume2\Users\Pacopepe\Desktop\Trabajo historia Pacopepe.odt
0xffffe70f58b81d10   8852          0xc0c          0x804 EtwRegistration
0xffffc480045339b0   8852          0xc14           0x10 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SYNCROOTMANAGER
0xffffe70f57f2a5d0   8852          0xc18            0x1 WaitCom ... Packet
0xffffe70f58d79b60   8852          0xc1c        0x1f0003 Event
0xffffe70f5815f9e0   8852          0xc24        0x1f0003 Event
```

Ahora lo que queremos hacer es descargarnos el -odt, en mi caso he probado de muchas formas como con dumpfiles pero no me ha dejado.

Al final he optado por usar volatility3:

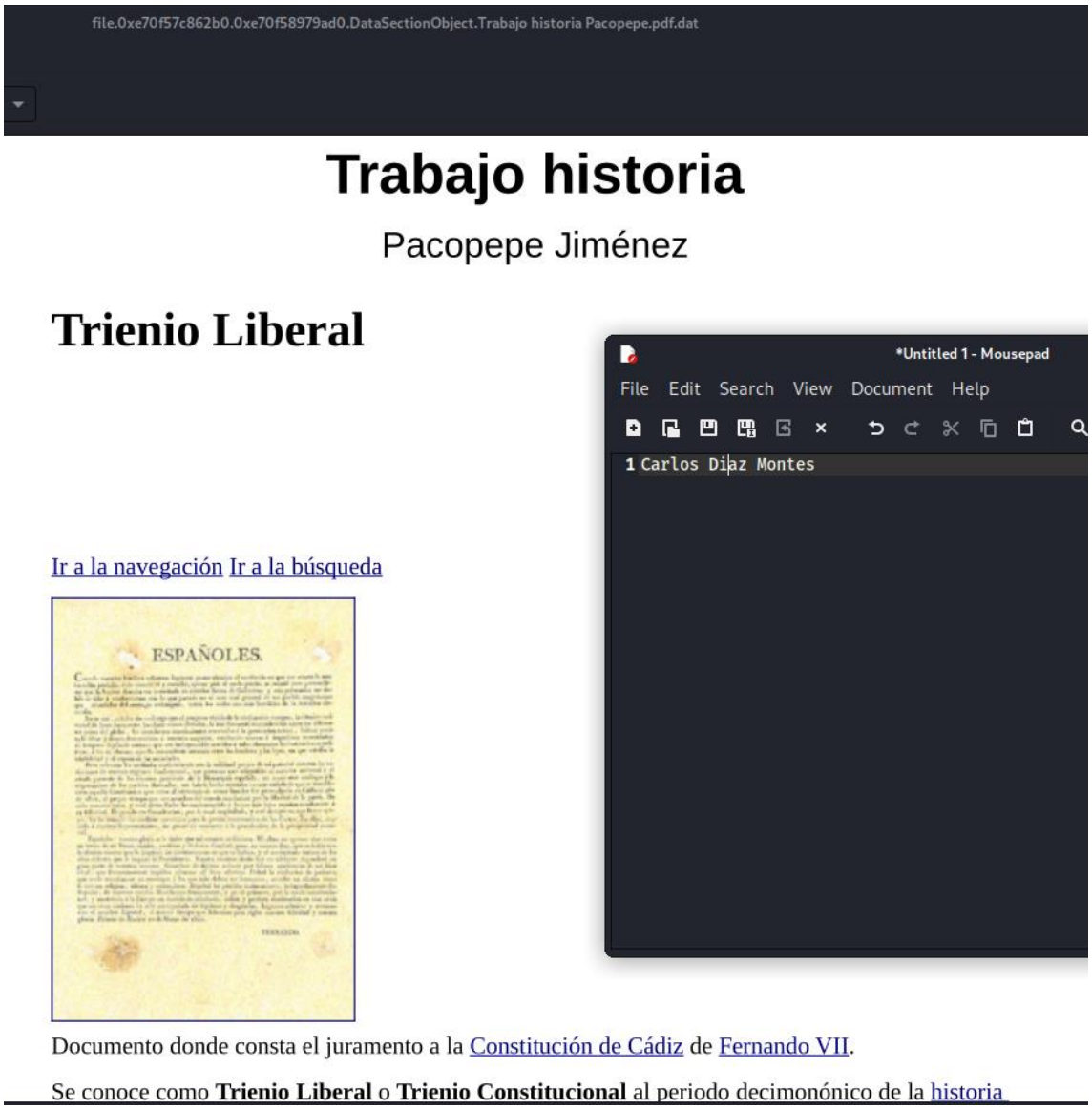
```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp windows.dumpfiles --virtaddr 0x0000e70f57c862b0
```

```
Progress:  100.00               PDB scanning finished

Cache   FileObject      FileName        Result

DataSectionObject       0xe70f57c862b0  Trabajo historia Pacopepe.pdf   file.0xe70f57c862b0.0xe70f58979ad0.DataSectionObject.T
rabajo historia Pacopepe.pdf.dat
SharedCacheMap  0xe70f57c862b0  Trabajo historia Pacopepe.pdf   file.0xe70f57c862b0.0xe70f58763d90.SharedCacheMap.Trabajo hist
oria Pacopepe.pdf.vacb
```

Ahora vamos a comprobar el archivo:



4. Encuentra pruebas de que el usuario del equipo está tras la falsa amenaza de bomba

Para esto vamos a comprobar los procesos antes vistos (los de discord).

Para esto vamos a descarnarnos todos los procesos:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f DESKTOP-01S7HH9-20220408-171552.dmp --profile=Win10×64_19041 memdump -p 3112,6324,464,8620,6224,7068 -
D /home/kali/Desktop/
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing Discord.exe [  3112] to 3112.dmp
************************************************************************
Writing Discord.exe [   464] to 464.dmp
************************************************************************
Writing Discord.exe [  6224] to 6224.dmp
************************************************************************
Writing Discord.exe [  7068] to 7068.dmp
************************************************************************
Writing Discord.exe [  6324] to 6324.dmp
************************************************************************
Writing Discord.exe [  8620] to 8620.dmp
```

Ahora comprobamos los procesos (el proceso clavees el 6324).Primero vamos a usar el comando string para comprobar que sale alguna palabra clave como “bomba”:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings 6324.dmp | grep "bomba"
```

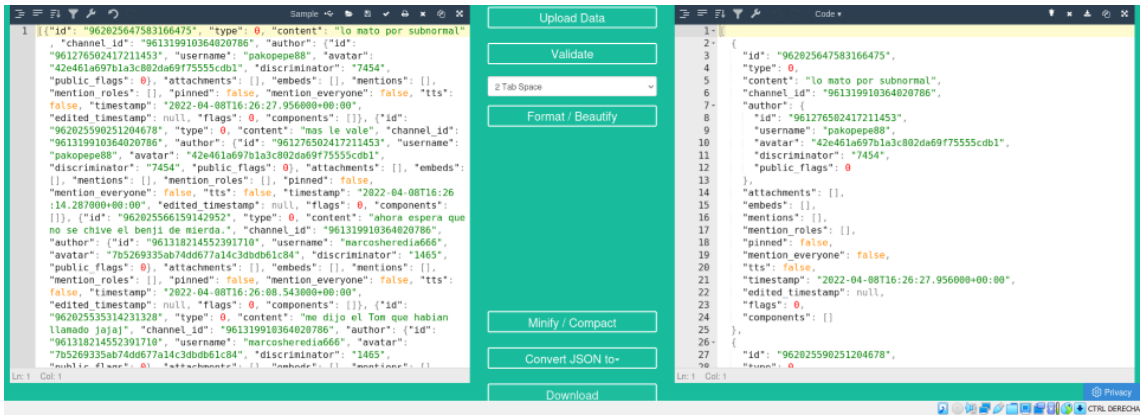
Ahora vamos a copiar todo el contenido y vamos a pegarlos en un fichero .json:

```
", "username": "pakopepe88", "avatar": "42e461a697b1a3c802da69f75555cdb1", "discriminator": "7454", "public_flags": 0}, "attac
hments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "mention_everyone": false, "tts": false, "tim
estamp": "2022-04-07T18:46:57.509000+00:00", "edited_timestamp": null, "flags": 0, "components": []}, {"id": "9616985258198590
04", "type": 0, "content": "ya me toca los huevos hacer el puto trabajo en vacaciones", "channel_id": "961319910364020786", "a
uthor": {"id": "961318214552391710", "username": "marcosheredia666", "avatar": "7b5269335ab74dd677a14c3dbdb61c84", "discrimina
tor": "1465", "public_flags": 0}, "attachments": [], "embeds": [], "mentions": [], "mention_roles": [], "pinned": false, "ment
ion_everyone": false, "tts": false, "timestamp": "2022-04-07T18:46:36.050000+00:00", "edited_timestamp": null, "flags": 0, "co
mponents": []}]
 al insti con la amenaza de bomba, so colgao?
 al insti con la amenaza de bomba, so colgao?
 al insti con la amenaza de bomba, so colgao?
 al insti con la amenaza de bomba, so colgao?
bombarding

┌──(kali㉿kali)-[~/Desktop]
└─$ touch fichero_bomba.json

┌──(kali㉿kali)-[~/Desktop]
└─$ nano fichero_bomba.json
```

Ahora vamos a poner el contenido legible desde internet:



Vamos a convertirlo para comprobar su contenido:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat jsonformatter.txt | tac | grep -E "content|username"
    "username": "marcosheredia666",
  "content": "ya me toca los huevos hacer el puto trabajo en vacaciones",
    "username": "pakopepe88",
  "content": "yo ni lo voy hacer",
    "username": "pakopepe88",
  "content": "el sábado ya me vuelvo a Graná",
    "username": "marcosheredia666",
  "content": "ya echaremos los vicios entonces",
    "username": "marcosheredia666",
  "content": "y te veré por Pedro Antonio",
    "username": "pakopepe88",
  "content": "me voy a chumar hasta las trancas",
    "username": "pakopepe88",
  "content": "le damos al fortnite?",
    "username": "marcosheredia666",
  "content": "dale",
    "username": "pakopepe88",
  "content": "Bueno, voy al gym, hablamos",
    "username": "pakopepe88",
  "content": "opa Marcos",
```

```
    "username": "marcosheredia666",
  "content": "venga, dale",
    "username": "pakopepe88",
  "content": "mira ni lo de historia le hago la verda",
    "username": "marcosheredia666",
  "content": "bah tampoco yo",
    "username": "pakopepe88",
  "content": "es ke ni copiar de la wikipedia, te lo juro.",
    "username": "marcosheredia666",
  "content": "bueno, yo eso si",
    "username": "marcosheredia666",
  "content": "Fuiste tu el que llamó al insti con la amenaza de bomba, so colgao?",
    "username": "pakopepe88",
  "content": "si buajajaja",
    "username": "pakopepe88",
  "content": "hala, ya no hai examen de lengua",
    "username": "pakopepe88",
  "content": "ke le den por kulo",
    "username": "marcosheredia666",
  "content": "🤣",
    "username": "marcosheredia666",
  "content": "me dijo el Tom que habian llamado jajaj",
    "username": "marcosheredia666",
  "content": "ahora espera que no se chive el benji de mierda.",
    "username": "pakopepe88",
  "content": "mas le vale",
```