

Nombre :	Univ. Gonzalo Espinoza Chiri	Numero de practica
Materia :	Informática Forense sis-939	4
Docente:	Ing. David Sossa L.	
Auxiliar :	Univ.	

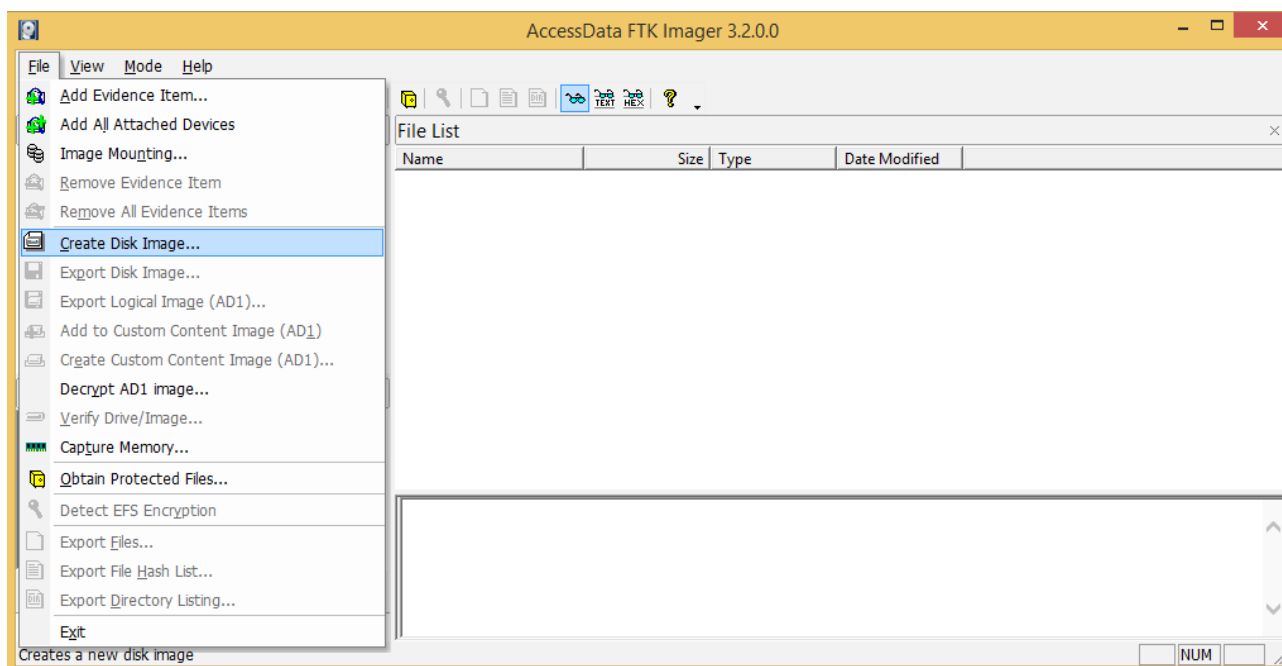
ANALISIS DE EVIDENCIAS DIGITALES

1. Explique los pasos para la captura de imagen de disco tanto en frio como en caliente.

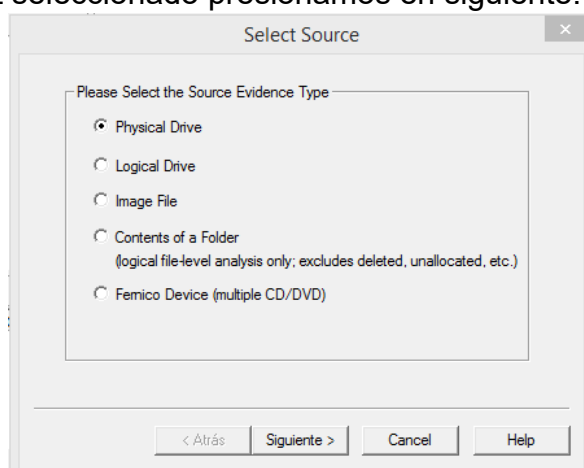
➤ Captura de un imagen de disco en caliente.

Para realizar la captura de imagen de disco en caliente se utilizara la herramienta de análisis forense “**FTK Imager**”. Para ello se empleara los siguientes pasos:

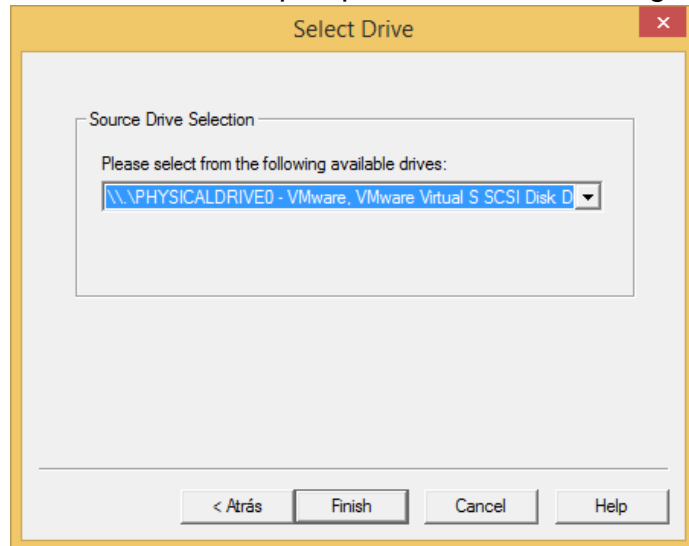
Paso 1: después de descargar la herramienta, lo instalamos y procedemos a abrirlo dicha aplicación, nos mostrara la siguiente ventana, en la que deberemos hacer clic en la opción que dice “**file**”, y luego seleccionamos “**Create Disk Image**” como se muestra en la imagen.



Se nos abrirá una pequeña ventana en la que deberemos seleccionar la opción que dice “Physical Drive”, una vez seleccionado presionamos en siguiente.

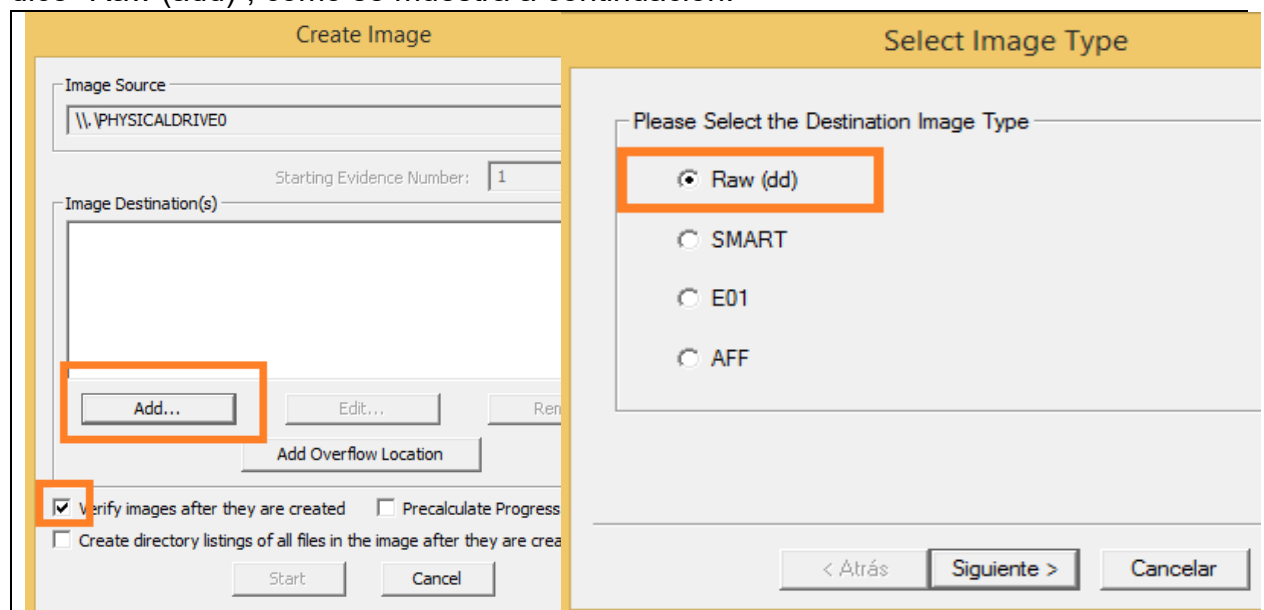


Ahora seleccionamos la unidad de la que queremos crear la imagen.

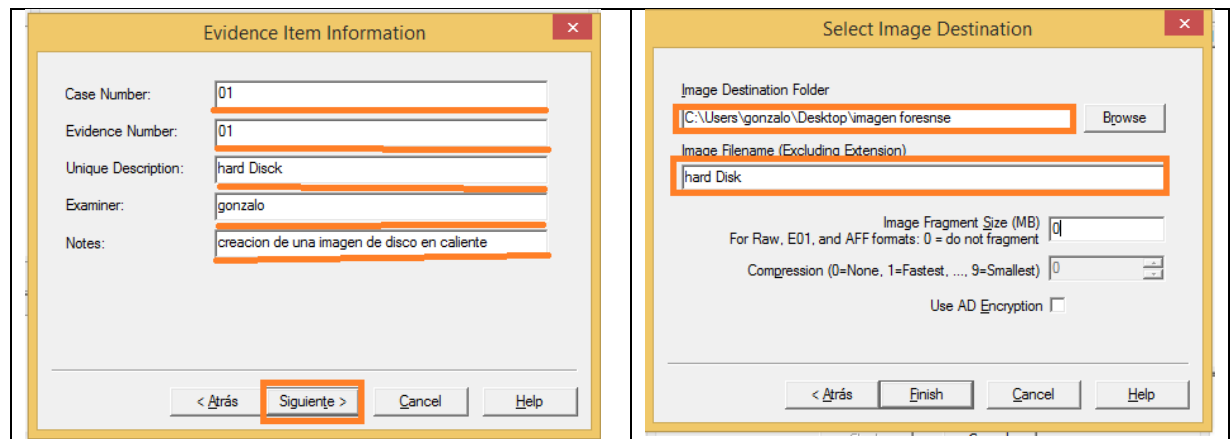


Nos aparecerá la siguiente ventana en la que deberemos etiquetar las opciones que requeriremos de la imagen, en este caso lo dejamos por defecto.

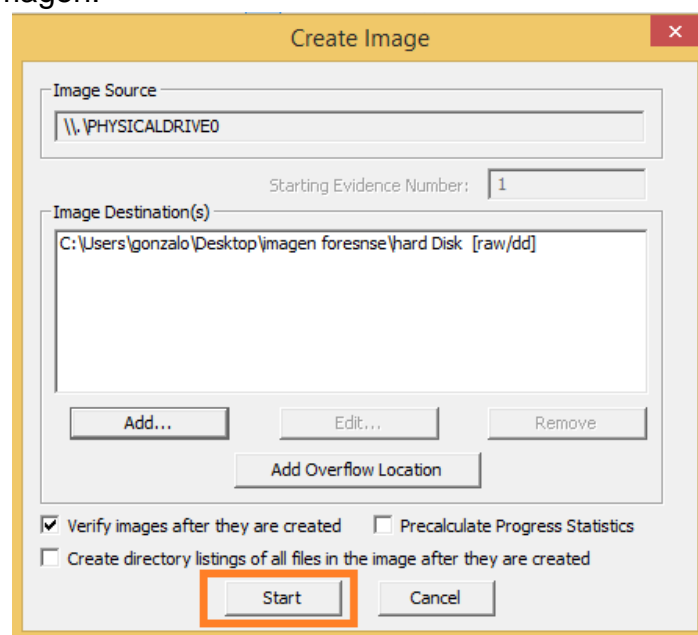
Posterior a ello nos aparecerá una nueva ventana en la que seleccionamos la opción que dice "Raw (add)", como se muestra a continuación:



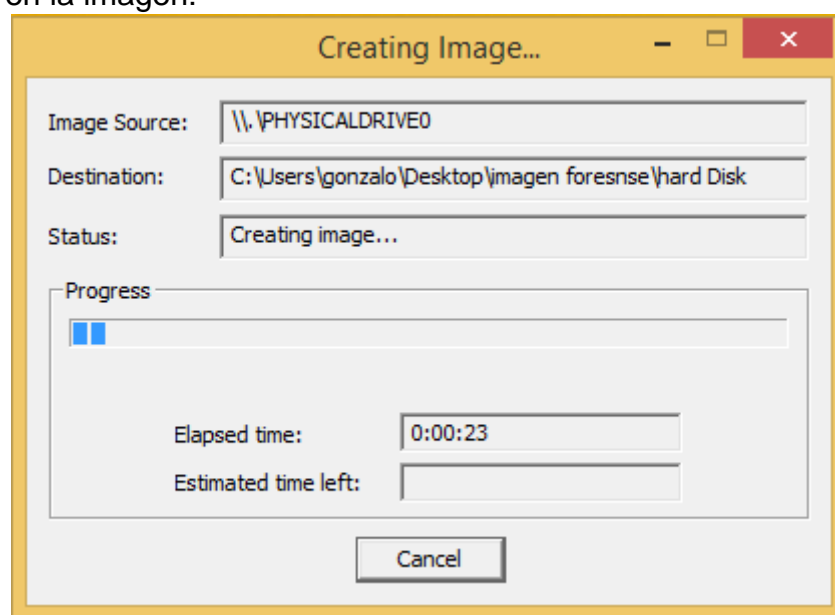
Completamos los datos de formulario, y seleccionamos la carpeta de destino y le damos un nombre al archivo de la imagen.



Finalmente presionamos la opción que dice **"Start"** para que la herramienta inicie con la creación de la imagen.

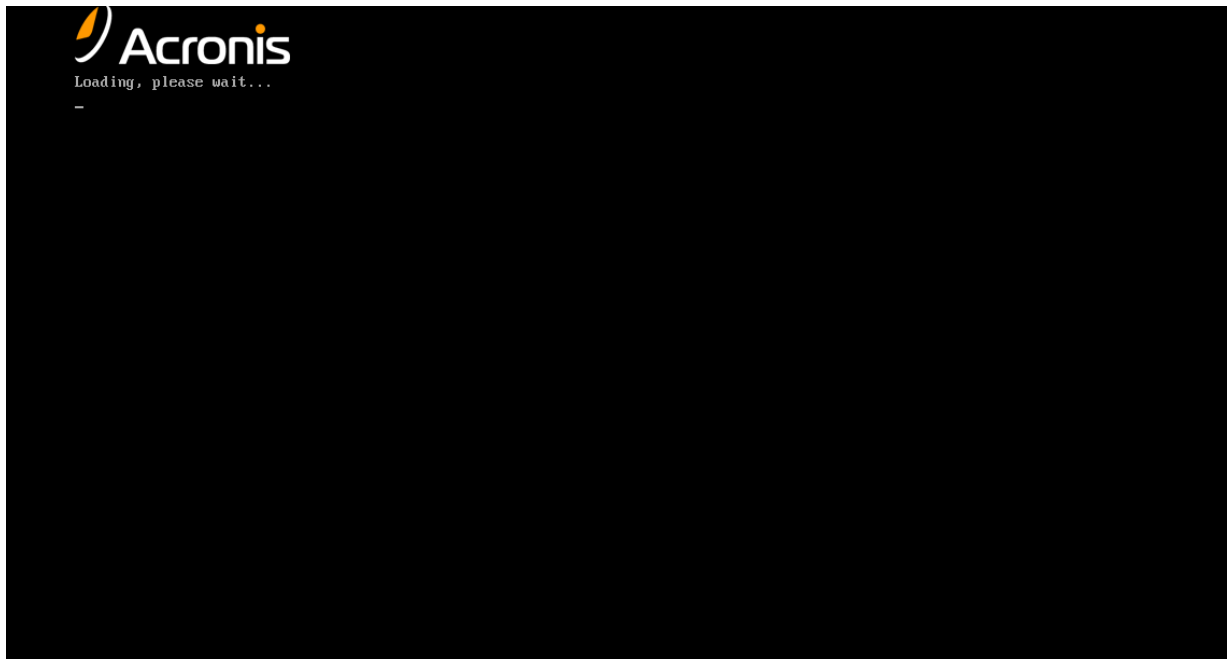


Ahora solo queda esperar con la creación de la imagen de disco, dicho proceso se muestra com en la imagen:

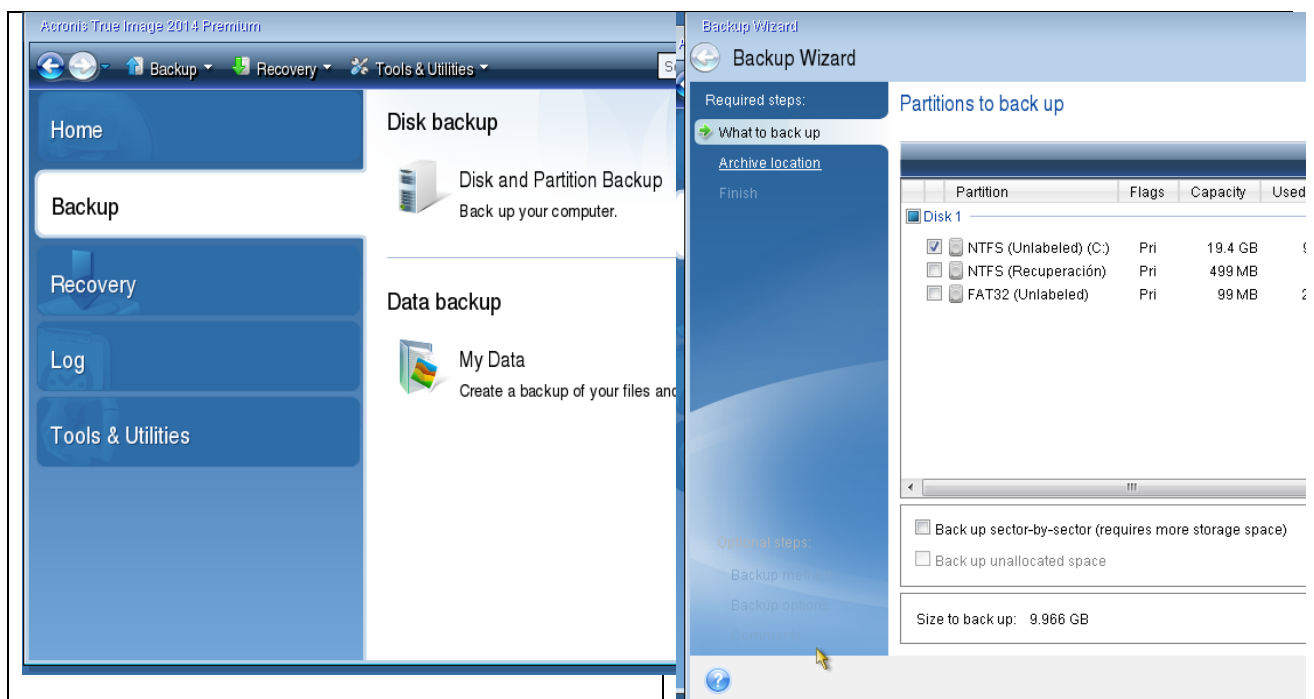


➤ **Captura de imagen de disco en frio.**

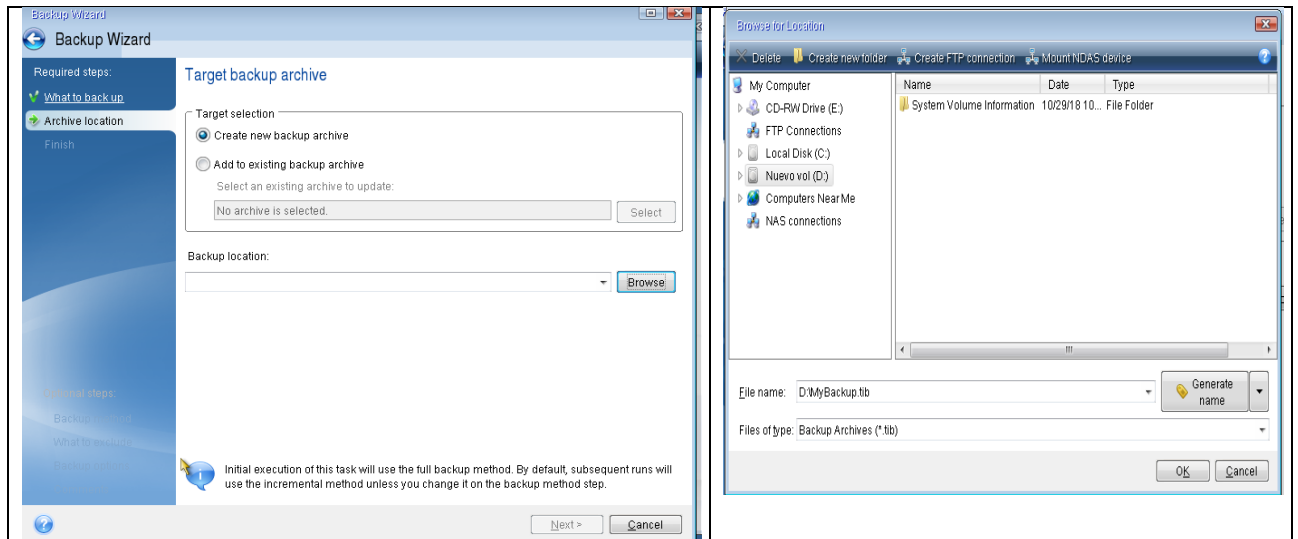
Una vez que descargado la iso de “Acronis True image” arrancamos desde cd/DvD o desde una memoria USB, en el equipo en que se desee sacar una imagen de disco en muerto, una vez arrancado desde la unidad donde se colocó la iso, al arrancar nos mostrara una imagen igual a la siguiente.



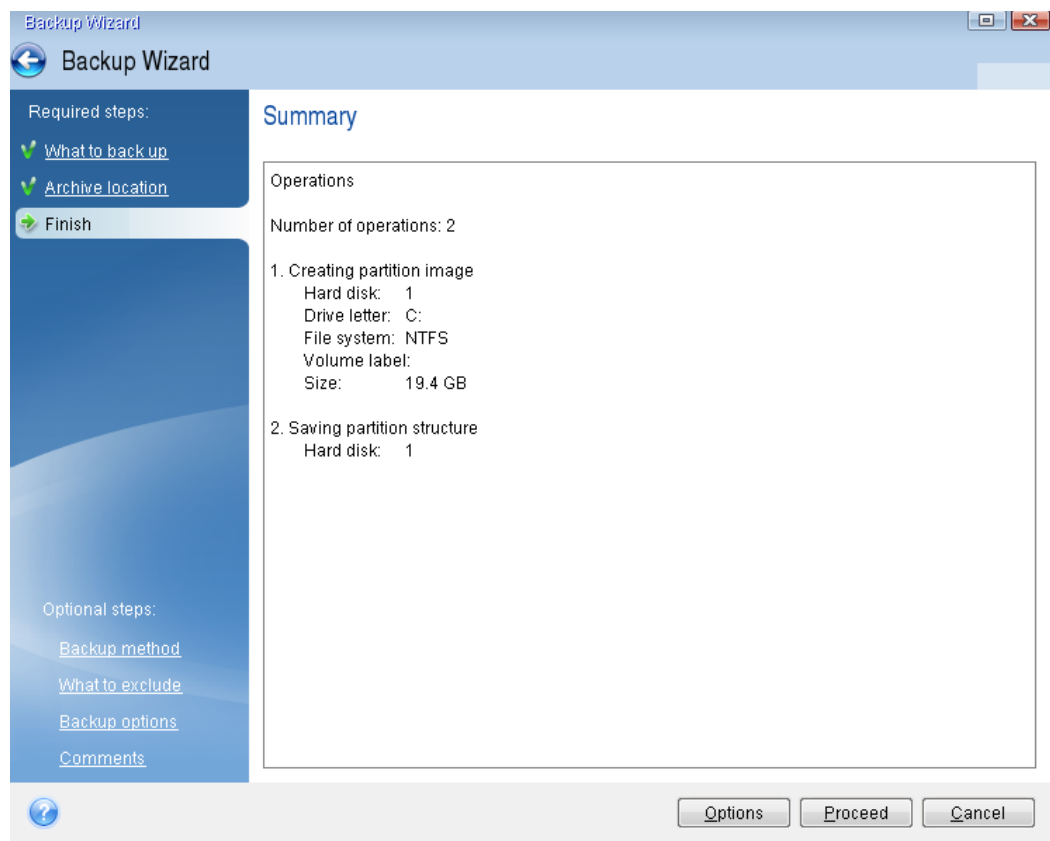
Una vez que termine de cargar la aplicación nos mostrara una interfaz en la que seleccionaremos la opción que dice “Backup” luego se nos desplegara una nueva ventana en la que se selecciona el disco que deseamos clonar, como se muestra en la imagen.



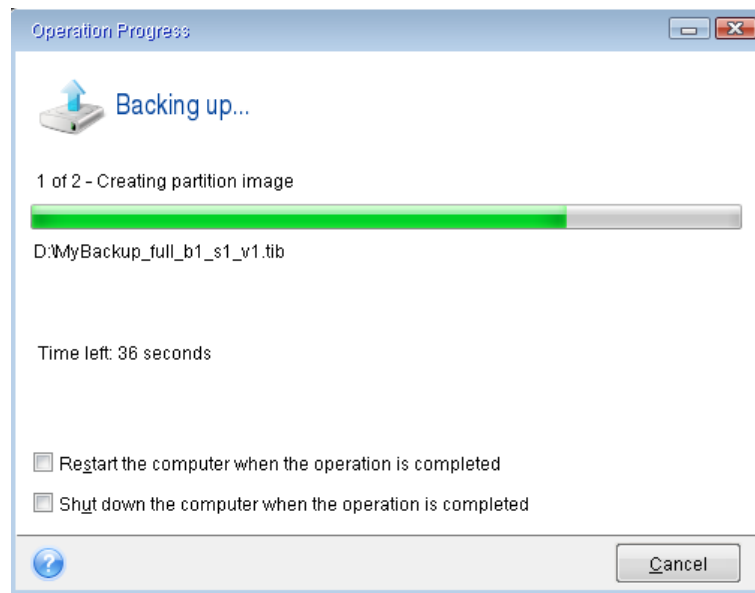
Ahora seleccionamos la primera opción, y seleccionamos la ubicación en donde queremos guardar la imagen de disco, después presionamos en “OK”



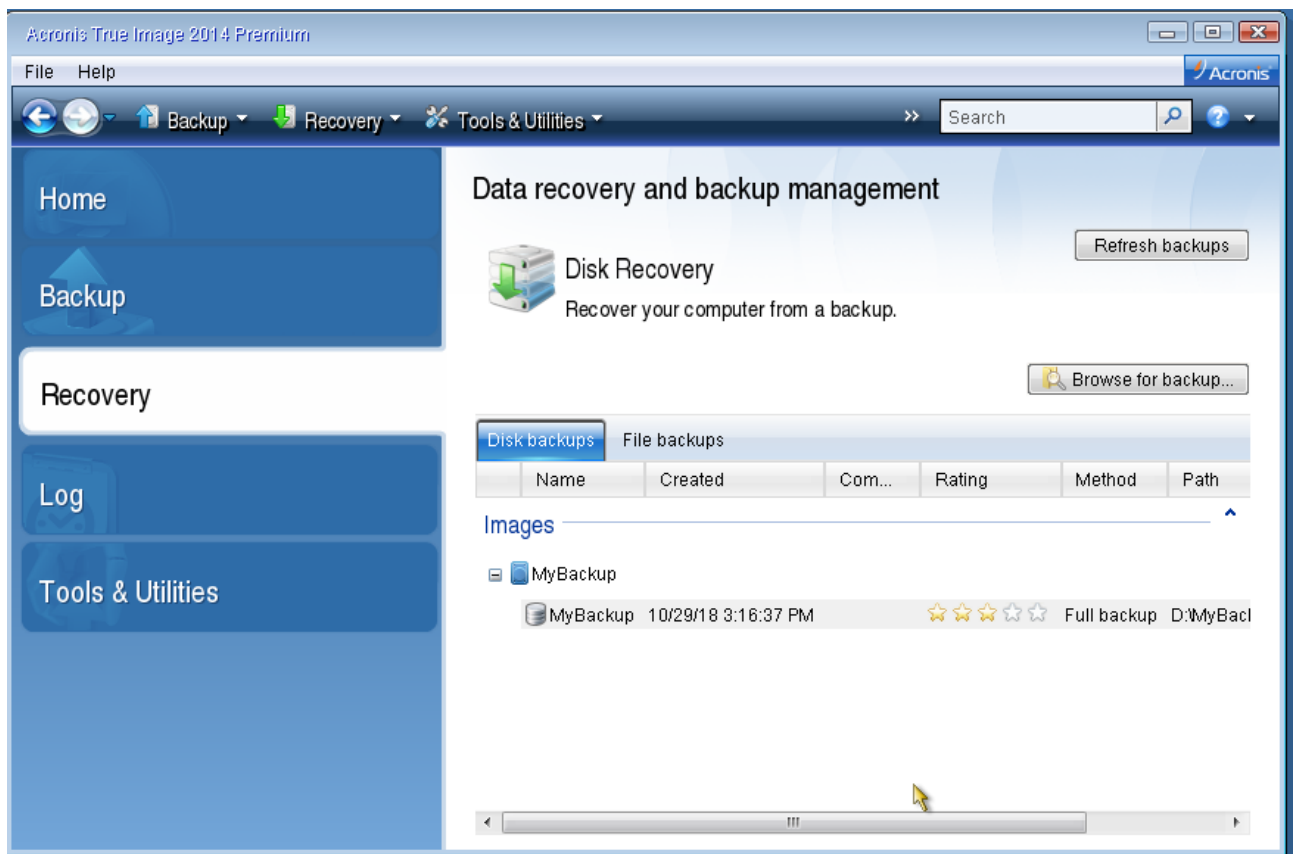
Nos aparecerá una ventana en la que nos da un informe de todo lo que hicimos interiormente. Finalmente presionamos en la opción que dice “**procced**”, como se muestra.



Por ultimo nos muestra una ventana con el estado de proceso de la creación de la imagen.



Después terminado el proceso, nos muestra el resultado de del disco que clonamos.



2. **Realice el análisis de la información volátil mediante el programa volatility y encuentre lo siguiente: (puede ser el volcado de memoria de su propia computadora u otras de ejemplo se dio en la clase)**

2.1. Listas de procesos.

Para realizar el análisis de información volátil se utilizara la imagen brindada por el docente “xp-laptop-2005-06-25.img”, comando utilizado para listar los procesos:

```
>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img pslist
```

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img pslist
Volatility Foundation Volatility Framework 2.5
Offset (V)  Name                PID  PPID  Thds    Hnds    Sess    Wow64  Start                Exit
-----
0x823c87c0  System                4      0     61    1140  -----  0
0x81fd0f020 smss.exe             448      4      3     21  -----  0  2005-06-25 16:47:28 UTC+0000
0x81f5a3b8 csrss.exe            504    448    12    596    0      0  2005-06-25 16:47:30 UTC+0000
0x81f8eb10 winlogon.exe          528    448    21    508    0      0  2005-06-25 16:47:31 UTC+0000
0x820e0da0 services.exe      580    528    18    401    0      0  2005-06-25 16:47:31 UTC+0000
0x82199668 lsass.exe            592    528    21    374    0      0  2005-06-25 16:47:31 UTC+0000
0x81fa5aa0 svchost.exe         740    580    17    198    0      0  2005-06-25 16:47:32 UTC+0000
0x81fa8650 svchost.exe         800    580    10    302    0      0  2005-06-25 16:47:33 UTC+0000
0x81faba78 svchost.exe         840    580    83    1589   0      0  2005-06-25 16:47:33 UTC+0000
0x81fa8240 Smc.exe              876    580    22    423    0      0  2005-06-25 16:47:33 UTC+0000
0x81f8dda0 svchost.exe         984    580      6     90    0      0  2005-06-25 16:47:35 UTC+0000
0x81f6e7e8 svchost.exe        1024    580    15    207    0      0  2005-06-25 16:47:35 UTC+0000
0x81f9a670 spoolsv.exe          1224    580    12    136    0      0  2005-06-25 16:47:39 UTC+0000
0x81f5f020 ssonsvr.exe          1632   1580     1     24    0      0  2005-06-25 16:47:46 UTC+0000
0x8202bda0 explorer.exe        1812   1764    22    553    0      0  2005-06-25 16:47:47 UTC+0000
0x82113c48 Directcd.exe      1936   1812     4     40    0      0  2005-06-25 16:47:48 UTC+0000
0x81f67500 TaskSwitch.exe       1952   1812     1     21    0      0  2005-06-25 16:47:48 UTC+0000
0x81f6ca90 Fast.exe          1960   1812     1     22    0      0  2005-06-25 16:47:48 UTC+0000
0x820dd588 VPTay.exe            1980   1812     2     89    0      0  2005-06-25 16:47:49 UTC+0000
0x82025608 atiptaxx.exe         2040   1812     1     51    0      0  2005-06-25 16:47:49 UTC+0000
```

2.2. Lista de sesiones en el S.O.

El objetivo es sacar una lista de todos los usuarios existentes en el S.O., para ello se utilizara el siguiente comando:

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img hashdump

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img hashdump
Volatility Foundation Volatility Framework 2.5
Administrator:500:08f3a52bdd35f179c81667e9d738c5d9:ed88ccbc08d1c18bcded317112555f4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:ddd4c9c883a8ecb2078f88d729ba2e67:e78d693bc40f92a534197dc1d3a6d34f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8bfd47482583168a0ae5ab020e1186a9:::
phoenix:1003:07b8418e83fad948aad3b435b51404ee:53905140b80b6d8cbe1ab5953f7c1c51:::
ASPNET:1004:2b5f618079400df84f9346ce3e830467:ae7f3a8bb65a0f01d9470fad55a411c:::
Sarah:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

2.3. Sospechas de virus y de procesos raros.

Para poder ver los procesos sospechosos (ocultos) o virus se utiliza el comando:

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img psscan

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img psxview

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img psxview
Volatility Foundation Volatility Framework 2.5
Offset (P)  Name                PID  pslist  psscan  thrddproc  pspcid  csrss  session  deskthrd  ExitTime
-----
0x01f67500 TaskSwitch.exe       1952  True   True   True   True   True   True   True   True
0x01faf280 jusched.exe         188  True   True   True   True   True   True   True   True
0x021ca3d0 wdfmgr.exe          1548  True   True   True   True   True   True   True   True
0x02081da0 svchost.exe        1484  True   True   True   True   True   True   True   True
0x020dd588 VPTay.exe            1980  True   True   True   True   True   True   True   True
0x17fdb020 alg.exe          2868  True   True   True   True   True   True   True   True
0x01f8eb10 winlogon.exe          528  True   True   True   True   True   True   True   True
0x02079c18 cmd.exe              2624  True   True   True   True   True   True   True   True
0x01f68518 Cryptserv.exe      688  True   True   True   True   True   True   True   True
0x01fa5aa0 svchost.exe         740  True   True   True   True   True   True   True   True
0x020e0da0 services.exe      580  True   True   True   True   True   True   True   True
0x014b13b0 iexplore.exe         2392  True   True   True   True   True   True   True   True
0x01343790 mqtgsvc.exe          2536  True   True   True   True   True   True   True   True
0x01f48da0 tcpsvcs.exe         1400  True   True   True   True   True   True   True   True
0x01f6db28 msdtc.exe           1076  True   True   True   True   True   True   True   False
0x01ed76b0 PluckTray.exe       2740  True   True   True   True   True   True   True   True
0x02025608 atiptaxx.exe        2040  True   True   True   True   True   True   True   True
0x0202bda0 explorer.exe        1812  True   True   True   True   True   True   True   True
0x01f8dda0 svchost.exe         984  True   True   True   True   True   True   True   False
0x01f6ca90 Fast.exe          1960  True   True   True   True   True   True   True   True
0x01fa8240 Smc.exe              876  True   True   True   True   True   True   True   True
0x01f5f020 ssonsvr.exe          1632  True   True   True   True   True   True   True   True
0x186fec10 firefox.exe         2160  True   True   True   True   True   True   True   True
0x02218020 PluckSvr.exe      944  True   True   True   True   True   True   True   True
0x02113c48 Directcd.exe      1936  True   True   True   True   True   True   True   True
0x01fa8650 svchost.exe         800  True   True   True   True   True   True   True   False
0x02021a78 Rtvscan.exe      1304  True   True   True   True   True   True   True   True
0x021d4da0 mqsvc.exe           1948  True   True   True   True   True   True   True   True
```

2.4. Lista de Contenido de la papelera de reciclaje.

El objetivo es el de listar el contenido de la papelera de reciclaje de la imagen del volcado de memoria, para ello se utilizara el comando:

>volatility-2.5.standalone.exe -f xp-laptop-2005-07-04-1430.img clipboard

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-07-04-1430.img clipboard
Volatility Foundation Volatility Framework 2.5
-----
Session WindowStation Format Handle Object Data
-----
0 WinSta0 0xc009L 0x4d0289 0xe1cb9430
0 WinSta0 0xc074L 0x0 -----
0 WinSta0 CF_HDROP 0x0 -----
0 WinSta0 0xc0cfl 0x0 -----
0 WinSta0 0xc0c6L 0x0 -----
0 WinSta0 0xc006L 0x0 -----
0 WinSta0 0xc007L 0x0 -----
0 WinSta0 0xc013L 0x230287 0xe2bf1008
-----
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>
```

2.5. Configuración de red.

El objetivo es conocer las conexiones establecidas por el usuario. Para dicho objetivo se utiliza los siguientes comandos:

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **sockscan**

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **connscan**

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **netscan**

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **sockets**

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **connection**

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img connections
Volatility Foundation Volatility Framework 2.5
-----
Offset(V) Local Address Remote Address Pid
-----
0x820869b0 127.0.0.1:1055 127.0.0.1:1056 2160
0xffa2baf0 127.0.0.1:1056 127.0.0.1:1055 2160
0x8220c008 192.168.2.7:1077 64.62.243.144:80 2392
0x81f11e70 192.168.2.7:1082 205.161.7.134:80 2392
0x8220d6b8 192.168.2.7:1066 199.239.137.200:80 2392
-----
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img sockscan
Volatility Foundation Volatility Framework 2.5
-----
Offset(P) PID Port Proto Protocol Address Create Time
-----
0x01341308 4 0 47 GRE 0.0.0.0 2005-06-25 16:48:13 UTC+0000
0x0136e068 2392 1064 17 UDP 127.0.0.1 2005-06-25 16:51:23 UTC+0000
0x01386170 1948 2105 6 TCP 0.0.0.0 2005-06-25 16:48:05 UTC+0000
0x013910e0 1948 2103 6 TCP 0.0.0.0 2005-06-25 16:48:05 UTC+0000
0x01ebd460 1424 161 17 UDP 0.0.0.0 2005-06-25 16:48:00 UTC+0000
0x01ed4700 2392 1077 6 TCP 0.0.0.0 2005-06-25 16:51:26 UTC+0000
0x01eed5b0 2392 1066 6 TCP 0.0.0.0 2005-06-25 16:51:24 UTC+0000
0x01f1e420 3342409 0 0 HPOPT 1.0.0.0 2250-05-07 17:31:44 UTC+0000
0x01f5be98 1400 13 17 UDP 0.0.0.0 2005-06-25 16:48:00 UTC+0000
0x01f65b68 1400 17 17 UDP 0.0.0.0 2005-06-25 16:48:00 UTC+0000
0x01f747b8 1304 2967 17 UDP 0.0.0.0 2005-06-25 16:47:59 UTC+0000
-----
```

2.6. Sistema operativo qué se estaba ejecutándose.

El objetivo de es ver la información del tipo de sistema operativo que contenia la compoutadora al momento de casar la imagen de la memoria volátil, este información nos muestra el siguiente comando:

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **imageinfo**

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img imageinfo
Volatility Foundation Volatility Framework 2.5
INFO : volatility debug : Determining profile based on KDBG search
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer 1 : IA32PagedMemory (kernel AS)
AS Layer 2 : FileAddressSpace (C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone\xp-laptop-2005-06-25.img)
PAE type : No PAE
DTB : 0x39000L
KDBG : 0x8054c060L
Number of Processors : 1
Image Type (Service Pack) : 2
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2005-06-25 16:58:47 UTC+0000
Image local date and time : 2005-06-25 12:58:47 -0400
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>
```

2.7. Historial de navegación de internet.

El objetivo es mostrar el historial de navegación de la imagen de volcado de memoria volátil, para ello se utilizo el siguiente comando:

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img **iehistory**


```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img iehistor
Volatility Foundation Volatility Framework 2.5
*****
Process: 1812 explorer.exe
Cache type "URL" at 0x1935000
Record length: 0x100
Location: Visited: Sarah@about:blank
Last modified: 2005-06-25 16:51:13 UTC+0000
Last accessed: 2005-06-25 16:51:13 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x84
*****
Process: 1812 explorer.exe
Cache type "URL" at 0x1935100
Record length: 0x100
Location: Visited: Sarah@about:Home
Last modified: 2005-06-05 21:07:15 UTC+0000
Last accessed: 2005-06-05 21:07:15 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x84
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>
```

2.8. Otros.

Mostrar una lista de comandos de consola que se ejecutaron a momento de realizar la imagen (después del volcado de memoria), el comando que nos permite mostrar dicha lista de comandos utilizados es el siguiente:

>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img consoles

```
C:\Users\GonzaloE\Desktop\volatility_2.5.win.standalone>volatility-2.5.standalone.exe -f xp-laptop-2005-06-25.img consoles
Volatility Foundation Volatility Framework 2.5
*****
ConsoleProcess: csrss.exe Pid: 504
Console: 0x4e23b0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\WINDOWS\system32\cmd.exe - dd if=\\.\PhysicalMemory of=c:\xp-laptop-2005-06-25.img conv=noerror
AttachedProcess: dd.exe Pid: 4012 Handle: 0x2a4
AttachedProcess: cmd.exe Pid: 2624 Handle: 0x4c8
----
CommandHistory: 0x11253b0 Application: dd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2a4
Cmd #0 at 0x4e2df0: c
----
CommandHistory: 0x4e4d88 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 7 LastAdded: 6 LastDisplayed: 6
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x4c8
Cmd #0 at 0x4e2d28: d:
Cmd #1 at 0x4e1f78: cd dd
Cmd #2 at 0x4e2cc8: dir
Cmd #3 at 0x4e2e00: cd UnicodeRelease
Cmd #4 at 0x4e2cb8: dir
Cmd #5 at 0x4e1f90: dd
Cmd #6 at 0x4e1ff8: dd if=\\.\PhysicalMemory of=c:\xp-laptop-2005-06-25.img conv=noerror
----
Screen 0x4e2ab0 X:80 Y:300
Dump:
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Sarah>d:
```

3. Realice el análisis de la información no volátil mediante el programa autopsy u otro similar (Entrar a la página web <http://dfft.sourceforge.net/> y resolver 2 casos cualesquiera).

1. Prueba de búsqueda JPG # 1.

- Imagen de prueba de la herramienta de forense digital #8:
- Resultados de la búsqueda:

n°	nombre del archivo	MD5 (resultado)	MD5 (de la pagina)
1	file1.jpg	75b8d00568815a36c3809b46fc84ba6d	75b8d00568815a36c3809b46fc84ba6d

Captura de pantalla de los resultados;

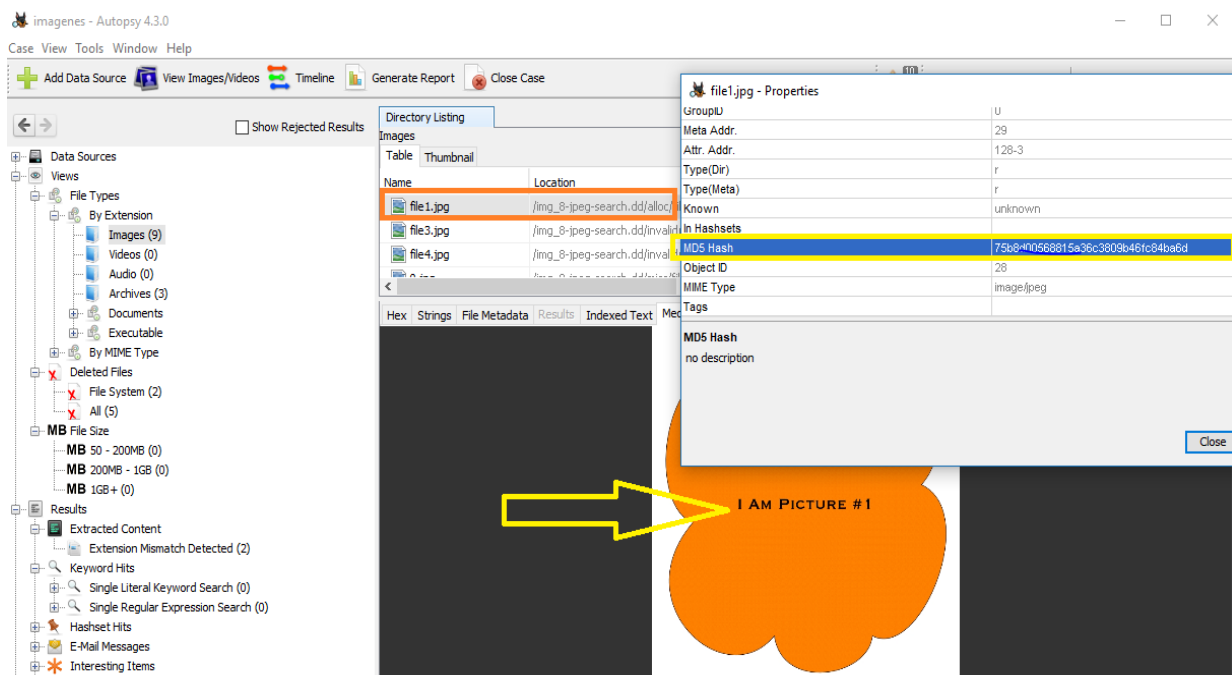
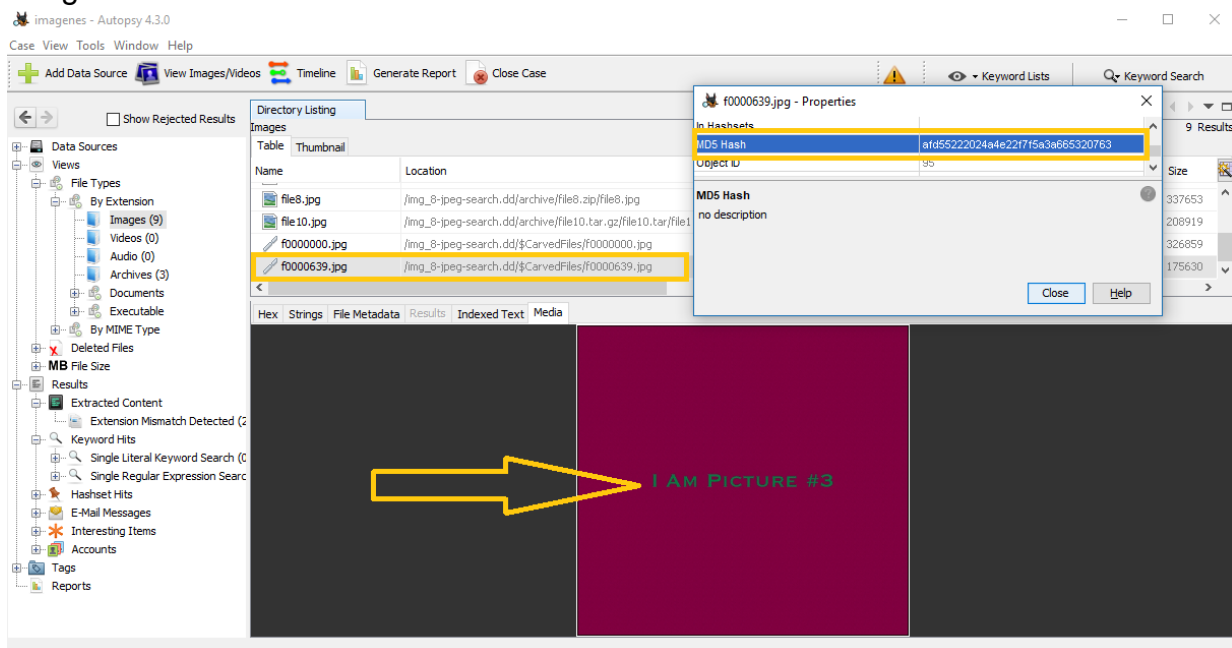
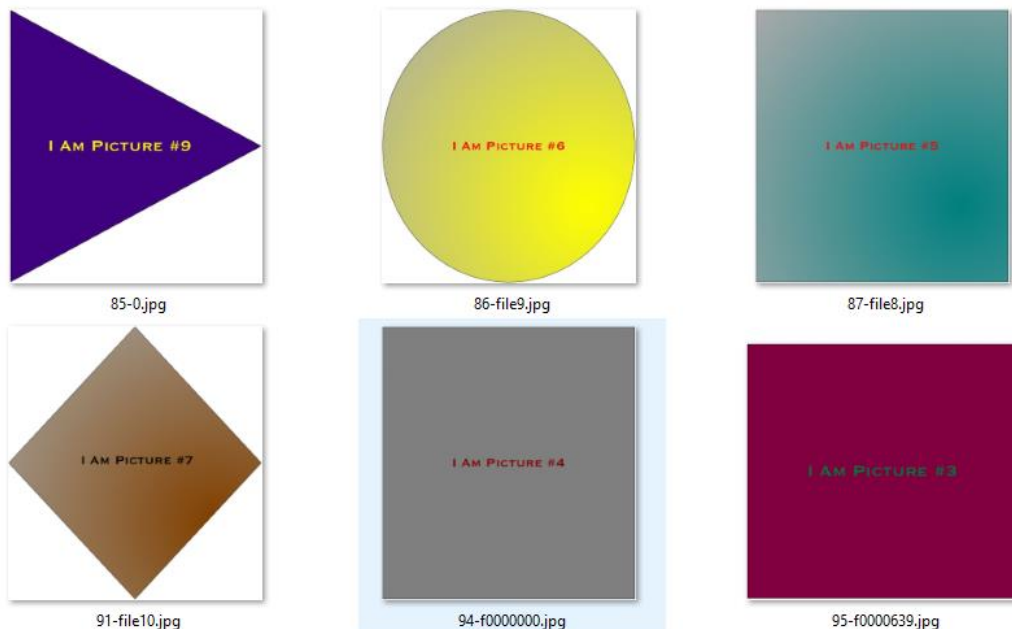


Imagen numero 3:



Como se podrá ver el resto de las imágenes que se extrajeron, me muestran a continuación:



2. Prueba de etiqueta de volumen de FAT N° 1

- Imagen de prueba de herramienta forense digital #9

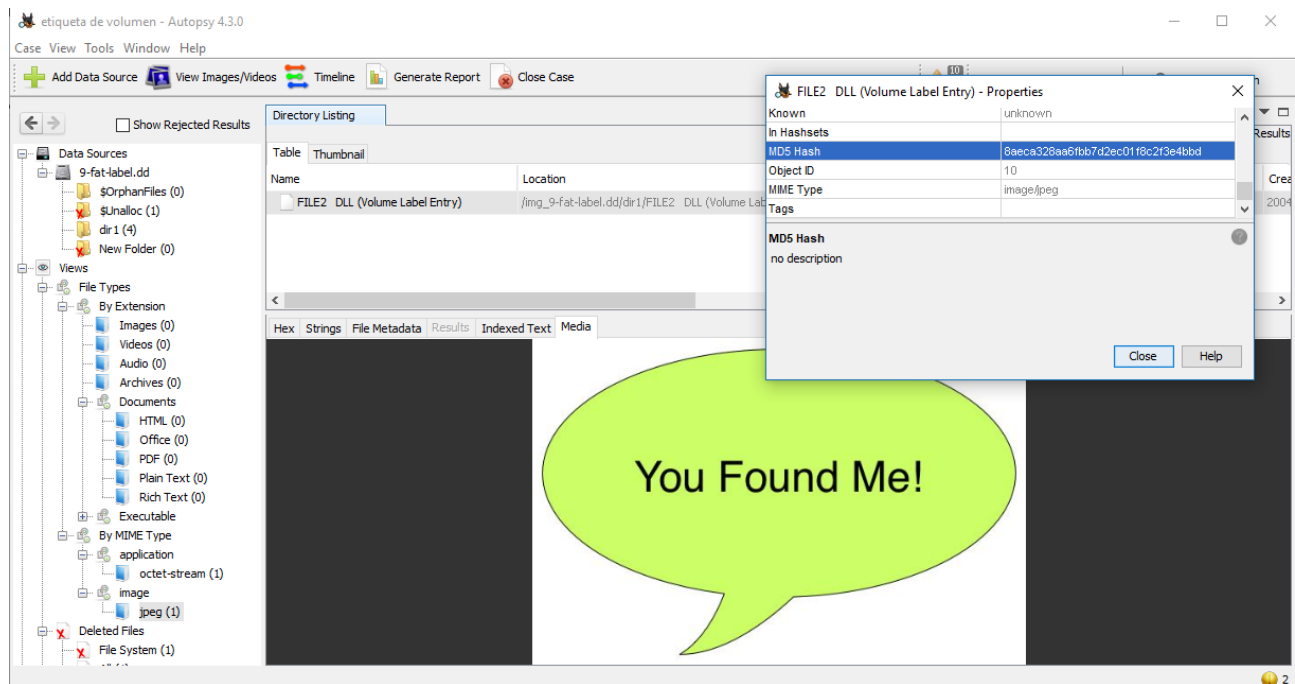
La entrada de directorio en el directorio raíz con el conjunto de atributos de etiqueta de volumen se denomina "LABEL2". Su valor MD5 es **8071eeaa52cd372a9bbb093e348e605c**

The screenshot shows the Autopsy 4.3.0 interface. On the left, the 'Data Sources' pane shows '9-fat-label.dd' with a tree view of its contents. The 'Directory Listing' pane shows a table of entries. The 'LABEL2' entry is selected, and its properties are shown in the 'Properties' pane on the right.

Name	Location	Modified Time
LABEL2 (Volume Label Entry)	/img_9-fat-label.dd/LABEL2 (Volume Label Entry)	2004-08-22 11:27:38 BOT

Property	Value
name	LABEL2 (Volume Label Entry)
Location	/img_9-fat-label.dd/LABEL2 (Volume La...
Modified Time	2004-08-22 11:27:38 BOT
Change Time	0000-00-00 00:00:00
Access Time	0000-00-00 00:00:00
Created Time	0000-00-00 00:00:00
Size	96541
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Mode	rwxrwxrwx
UserID	0
GroupID	0
Meta Addr.	3
Attr. Addr.	1-0
Type(Dir)	r
Type(Meta)	r
Known	unknown
In Hashsets	
MD5 Hash	8071eeaa52cd372a9bbb093e348e605c
Object ID	4
MIME Type	application/octet-stream
Tags	

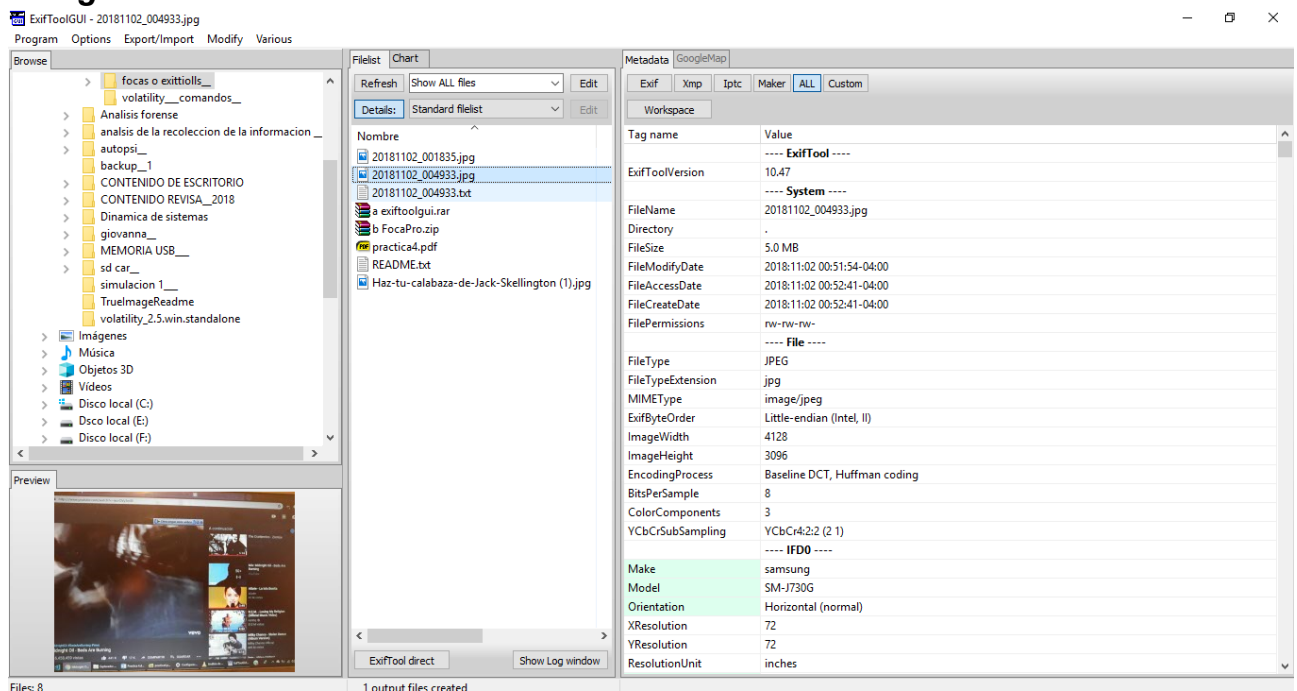
La entrada de directorio en el directorio dir1 con el conjunto de atributos de etiqueta de volumen se denomina "FILE2.DLL". Su valor MD5 es **8aeca328aa6fbb7d2ec01f8c2f3e4bbd**



4. Elija al azar 3 archivos (una foto con gps activado, un texto y una imagen) y explique qué metadatos de cada uno serian importante en algún caso de análisis forense (con exiftools o focaspro).

Análisis de metadatos realizado a los siguientes archivos

1. Fotografía tomada con GPS:



Metadatos:

```

---- ExifTool ----
ExifTool Version Number      : 10.47
---- File ----

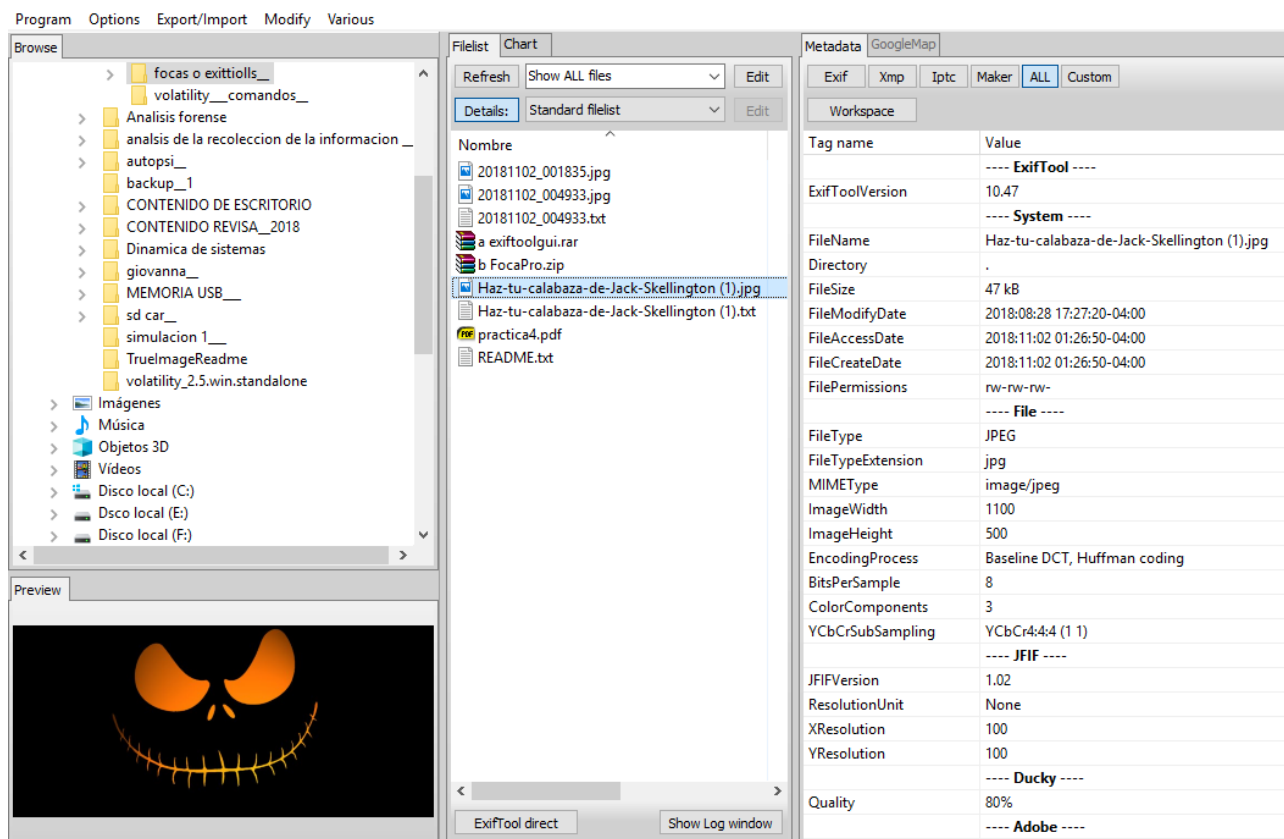
```

File Name : 20181102_004933.jpg
File Size : 5.0 MB
File Modification Date/Time : 2018:11:02 00:51:54-04:00
File Permissions : rw-rw-rw-
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
Exif Byte Order : Little-endian (Intel, II)
Image Width : 4128
Image Height : 3096
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:2 (2 1)
---- EXIF ----
Make : samsung
Camera Model Name : SM-J730G
Orientation : Horizontal (normal)
X Resolution : 72
Y Resolution : 72
Resolution Unit : inches
Software : J730GUBU4ARF1
Modify Date : 2018:11:02 00:49:33
Y Cb Cr Positioning : Centered
Exposure Time : 1/20
F Number : 1.7
Exposure Program : Program AE
ISO : 800
Exif Version : 0220
Date/Time Original : 2018:11:02 00:49:33
Create Date : 2018:11:02 00:49:33
Components Configuration : Y, Cb, Cr, -
Shutter Speed Value : 1/20
Aperture Value : 1.7
Brightness Value : -3.61
Exposure Compensation : 0
Max Aperture Value : 1.7
Metering Mode : Spot
Flash : No Flash
Focal Length : 3.7 mm
User Comment :
Sub Sec Time : 0362
Sub Sec Time Original : 0362
Sub Sec Time Digitized : 0362
Flashpix Version : 0100
Color Space : sRGB
Exif Image Width : 4128
Exif Image Height : 3096
Interoperability Index : R98 - DCF basic file (sRGB)
Interoperability Version : 0100
Exposure Mode : Auto
White Balance : Auto
Focal Length In 35mm Format : 27 mm
Scene Capture Type : Standard

Image Unique ID	: X13LSKA00AM X13LSKG01MA.
GPS Version ID	: 2.2.0.0
GPS Latitude Ref	: South
GPS Latitude	: 19.568611°
GPS Longitude Ref	: West
GPS Longitude	: 65.758333°
GPS Altitude Ref	: Below Sea Level
GPS Altitude	: 0 m
GPS Time Stamp	: 04:49:23
GPS Date Stamp	: 2018:11:02
Image Width	: 512
Image Height	: 384
Compression	: JPEG (old-style)
Orientation	: Horizontal (normal)
X Resolution	: 72
Y Resolution	: 72
Resolution Unit	: inches
Thumbnail Offset	: 1230
Thumbnail Length	: 23043
Thumbnail Image	: (Binary data 23043 bytes, use -b option to extract)
---- MakerNotes ----	
Time Stamp	: 2018:11:02 00:49:33-04:00
---- Composite ----	
Aperture	: 1.7
GPS Altitude	: 0 m Above Sea Level
GPS Date/Time	: 2018:11:02 04:49:23Z
GPS Latitude	: 19.568611° S
GPS Longitude	: 65.758333° W
GPS Position	: 19.568611° S, 65.758333° W
Image Size	: 4128x3096
Megapixels	: 12.8
Scale Factor To 35 mm Equivalent:	7.3
Shutter Speed	: 1/20
Create Date	: 2018:11:02 00:49:33.0362
Date/Time Original	: 2018:11:02 00:49:33.0362
Modify Date	: 2018:11:02 00:49:33.0362
Circle Of Confusion	: 0.004 mm
Field Of View	: 67.4 deg
Focal Length	: 3.7 mm (35 mm equivalent: 27.0 mm)
Hyperfocal Distance	: 1.96 m
Light Value	: 2.9

Como se puede observar la información que nos brindan los metadatos del foto tomada con el gps encendido es completa, el nombre el archivo, la extensión, el tamaño, con que tipo de equipo fue tomando, el nombre del fabricante del equipo, tipo de focal, capacidad de la cámara, la longitud, latitud, la hora y otros metadatos que pueden servir para realizar el análisis de este archivo.

2. Una imagen:



Metadatos de la imagen

```

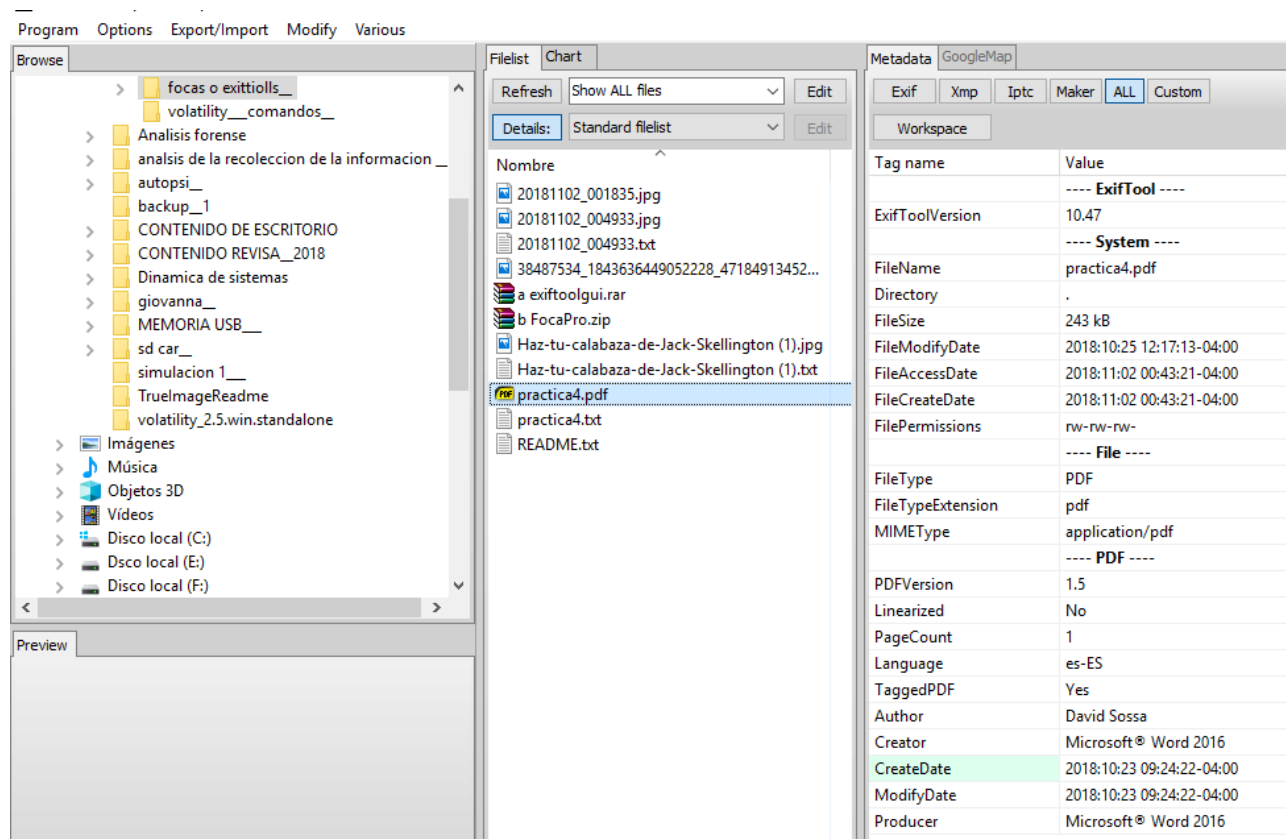
---- ExifTool ----
ExifTool Version Number      : 10.47
---- File ----
File Name                    : Haz-tu-calabaza-de-Jack-Skellington (1).jpg
Directory                   : .
File Size                   : 47 kB
File Modification Date/Time  : 2018:08:28 17:27:20-04:00
File Access Date/Time       : 2018:11:02 01:26:50-04:00
File Creation Date/Time     : 2018:11:02 01:26:50-04:00
File Permissions            : rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Image Width                 : 1100
Image Height                : 500
Encoding Process            : Baseline DCT, Huffman coding
Bits Per Sample             : 8
Color Components            : 3
Y Cb Cr Sub Sampling       : YCbCr4:4:4 (1 1)
---- JFIF ----
JFIF Version                : 1.02
Resolution Unit             : None
X Resolution                : 100
Y Resolution                : 100
---- Ducky ----
Quality                     : 80%
---- APP14 ----
DCT Encode Version         : 100

```


APP14 Flags 0	: [14], Encoded with Blend=1 downsampling
APP14 Flags 1	: (none)
Color Transform	: YCbCr
---- Composite ----	
Image Size	: 1100x500
Megapixels	: 0.550

La información que nos ofrece de una imagen es mínima como se podrá observar en las letras de color rojo

3. Texto:



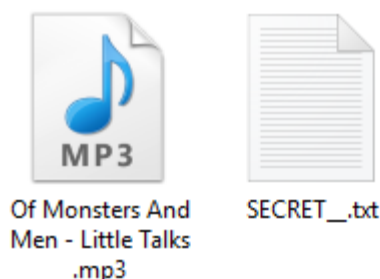
---- ExifTool ----	
ExifTool Version Number	: 10.47
---- File ----	
File Name	: practica4.pdf
Directory	: .
File Size	: 243 kB
File Modification Date/Time	: 2018:10:25 12:17:13-04:00
File Access Date/Time	: 2018:11:02 00:43:21-04:00
File Creation Date/Time	: 2018:11:02 00:43:21-04:00
File Permissions	: rw-rw-rw-
File Type	: PDF
File Type Extension	: pdf
MIME Type	: application/pdf
---- PDF ----	
PDF Version	: 1.5
Linearized	: No
Page Count	: 1

Language	: es-ES
Tagged PDF	: Yes
Author	: David Sossa
Creator	: Microsoft® Word 2016
Create Date	: 2018:10:23 09:24:22-04:00
Modify Date	: 2018:10:23 09:24:22-04:00
Producer	: Microsoft® Word 2016

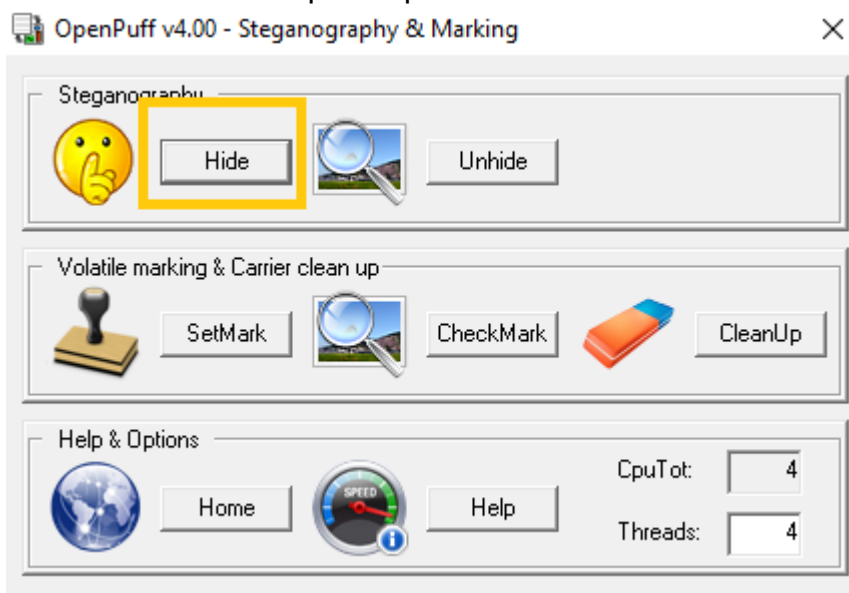
En la información de los metadatos del archivo pdf podemos observar con que tipo de programa fue creado, además que muestra la hora, el autor, el tamaño, y el tipo de archivo. Y otros aspectos que el forense considere importantes, en estos casos las letras de color rojo muestran los datos más relevantes.

5. *Realice un ejemplo de esteganografía (con open puff u otro similar).*

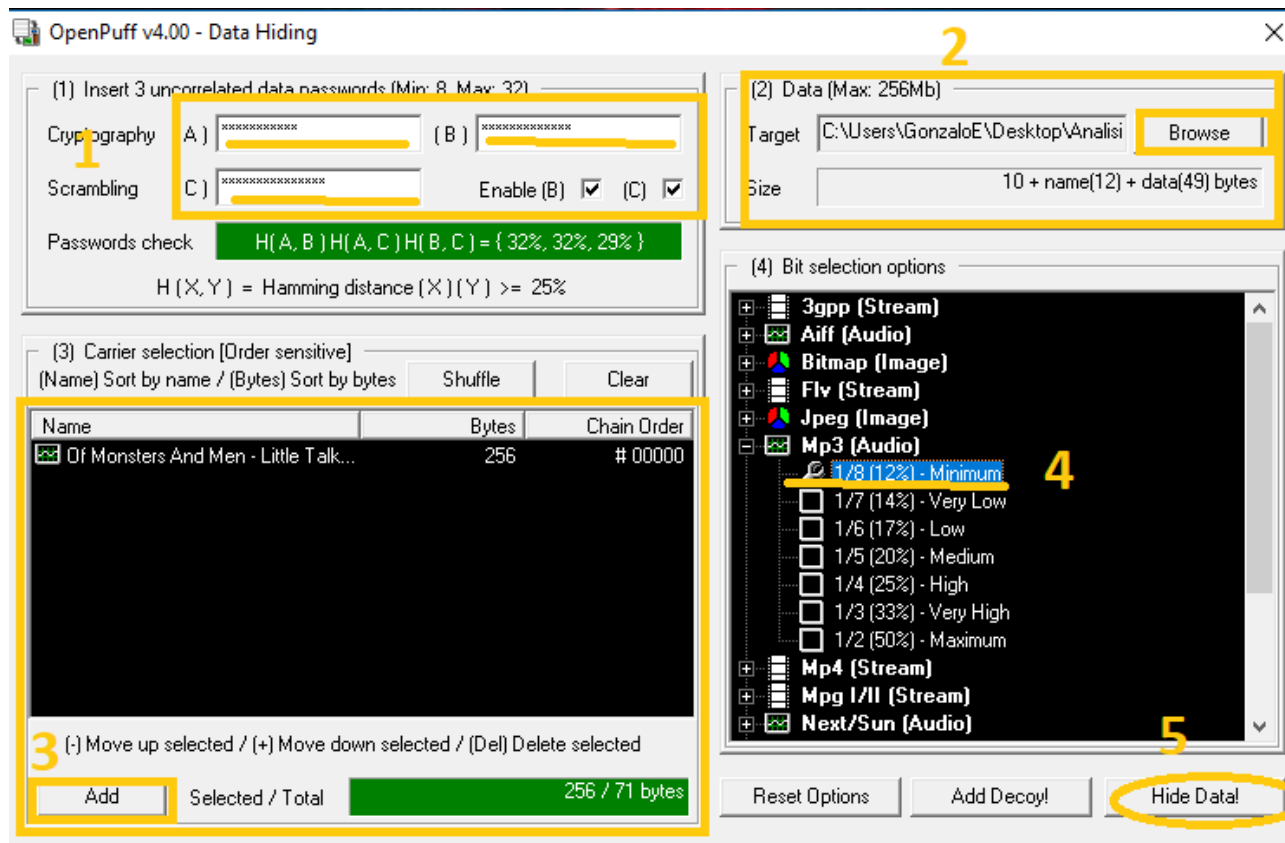
La estenografía es el arte de ocultar información dentro de otro objeto, en este caso se utilizara el programa de “open puff” para ocultar un archivo de texto en un archivo mp3:



Una vez que hacemos correr el programa, este nos muestra una peque interfaz de usuario para que deberemos seleccionar la opción que dice “**Hide**” como se muestra.



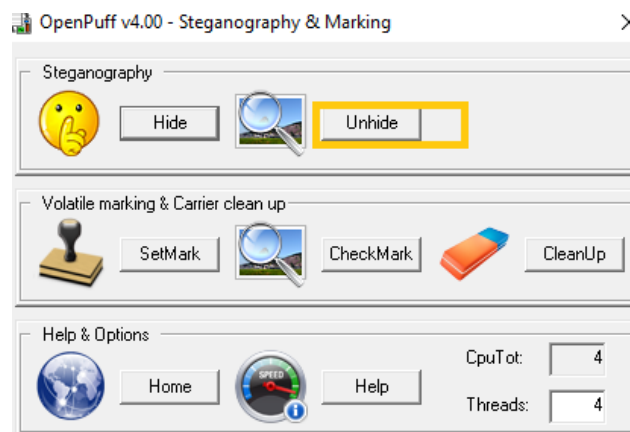
A continuación nos aparecerá la siguiente ventana, en la que debemos colocar 3 contraseñas distintas que no tengan relación (paos 1), posteriormente se seleccionara el archivo que se desea ocultar (paso 2), después se selecciona el archivo donde se oculara (paso 3), en el paso 4 seleccionamos el tipo de archivo, finalmente presionamos donde indica “Hide Data” que es el paso 5. Como se muestra en la imagen:



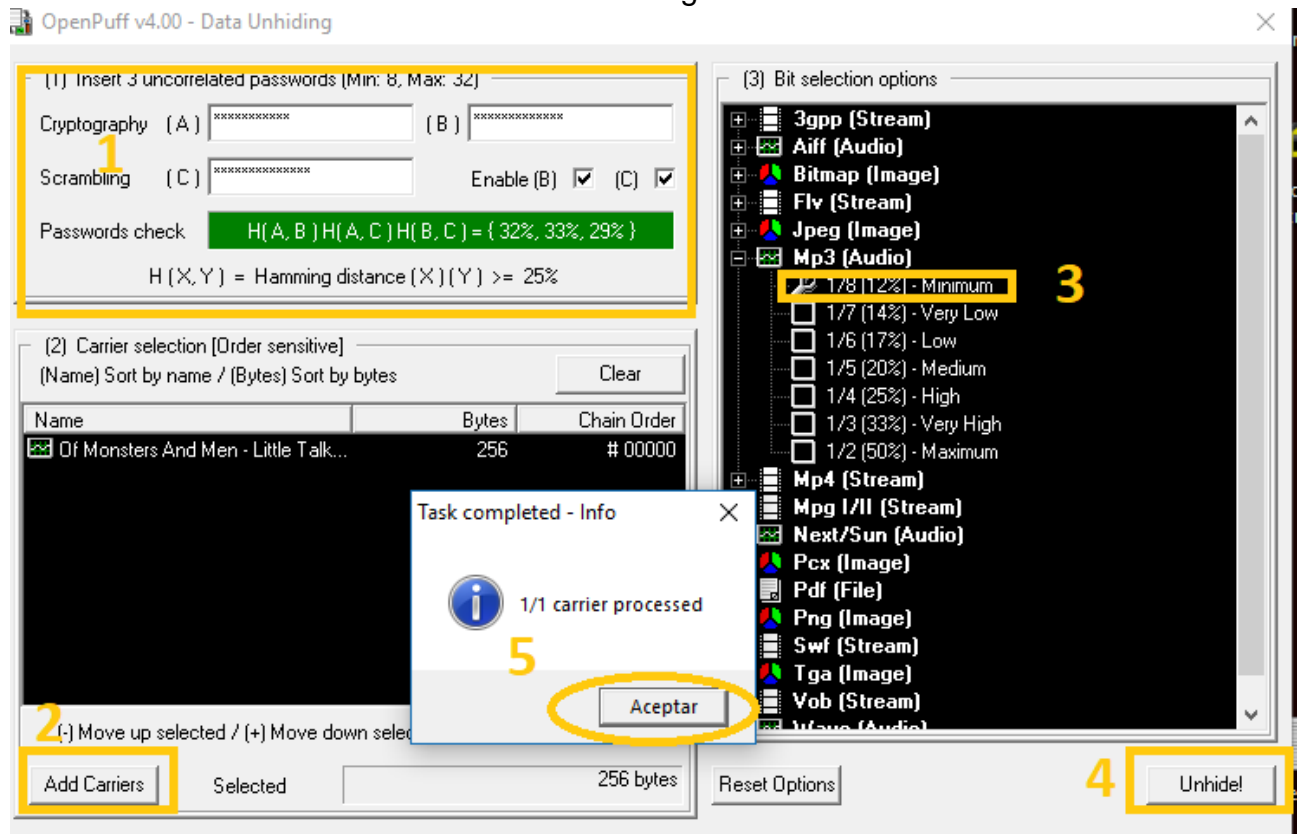
Aceptamos una vez concluido, finalmente nos feustra un solo archivo el que contendrá la el archivo oculto.



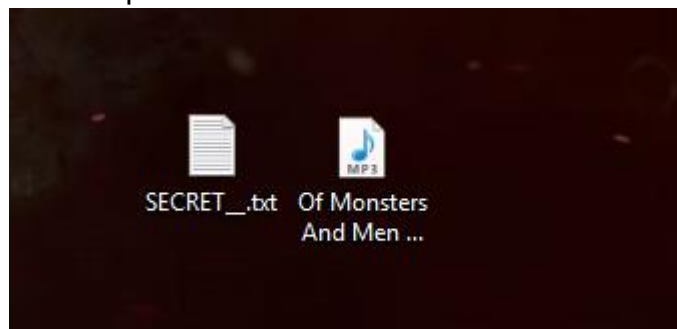
Para realizar el proceso inverso abrimos open puff y seleccionamos donde pone “unhide”, como se muestra:



A continuación colocamos las tres claves que al principio nos pidió (paso 1), en el paso 2 seleccionamos el archivo que contiene al objeto oculto, el paso 3 seleccionamos el tipo de archivo, finalmente seleccionamos "Unhide" (paso 4), finalmente nos aceptamos y se nos creará un archivo en el destino donde le asignamos:

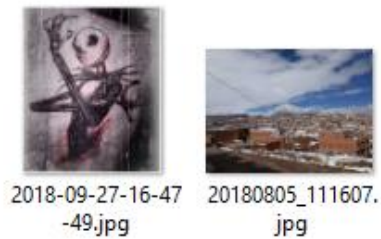


Después del proceso se nos aparecerá el archivo oculto:



6. **Elija dos fotografías al azar (una que sea toma directa de una cámara y otra que haya sido modificada) e ingresando a la página web <http://fotoforensics.com> y realice un análisis de confiabilidad de imagen y describa que diferencias existe en el análisis entre una imagen alterada y una que no haya sido alterada.**

para el análisis de confiabilidad se utilizaran 2 fotografías, una tomada con la cámara de un cel Samsung j7 y la otra es una imagen editada:



Presionamos en botón que indica seleccionar el archivo, escogemos la imagen y presionamos donde dice “upload file”:



A continuación se realizara el análisis, como se podrá ver la imagen presenta tonalidades del mismo color lo que nos indica que la foto es real y que no a sido alterada:





Las tonalidades siguen el mismo patrón y el color es el mismo en toda la imagen, lo que dice que la foto es original (no alterada).

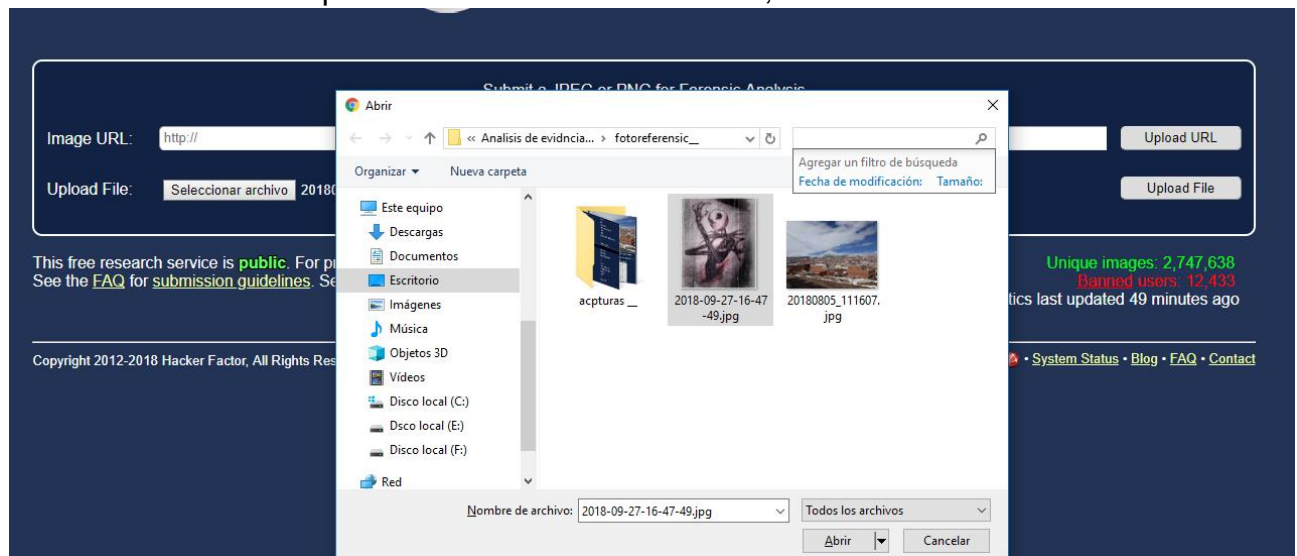
Otra forma de verificar es viendo los metadatos del archivo:

File	
File Type	JPEG
File Type Extension	.jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	4128
Image Height	3096
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:2 (2 1)
EXIF	
Make	samsung
Camera Model Name	SM-J730G
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	J730GUBU4ARF1
Modify Date	2018:08:05 11:16:07
Y Cb Cr Positioning	Centered
Exposure Time	1/6667
F Number	1.7
Exposure Program	Program AE
ISO	40
Exif Version	0220
Date/Time Original	2018:08:05 11:16:07

Estos datos nos confirman que efectivamente fue tomada con un celular Samsung

Análisis de la foto editada:

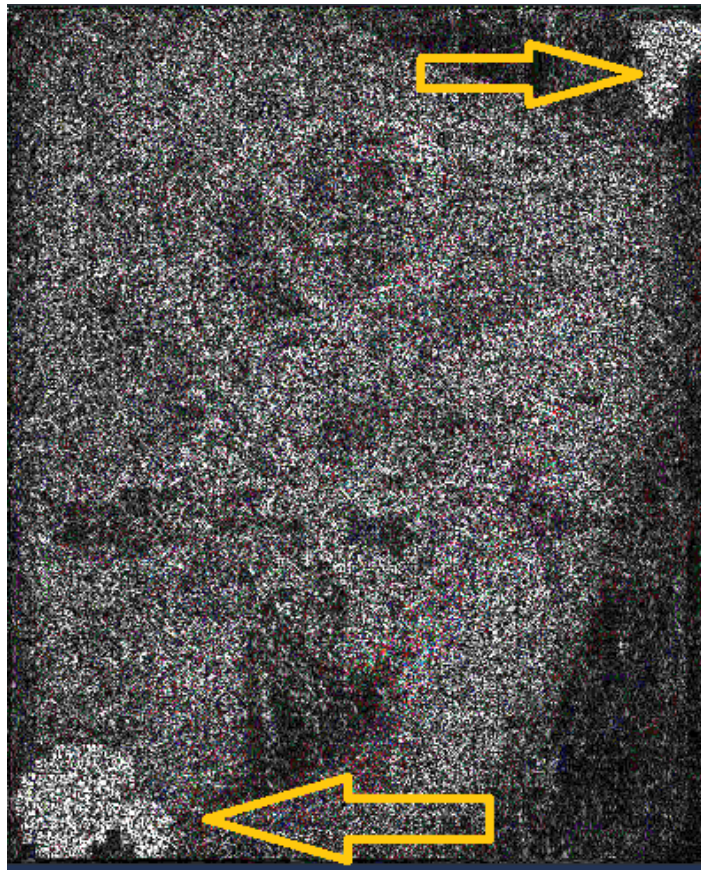
Realizamos el mismo proceso de selección de la foto;



La pigmentación de colores no es la misma lo que nos lleva a concluir que la fotografía fue editada como se muestra a continuación.

Imagen editada









Si realizamos los metadatos del archivo podemos ver que efectivamente fue editada, con un programa de Microsoft.

MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	400
Image Height	483
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
EXIF	
Modify Date	2018:09:27 16:47:49
Compression	JPEG (old-style)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Thumbnail Offset	152
Thumbnail Length	17212
Thumbnail Image	(Binary data 17212 bytes)
ICC_Profile	
Profile CMM Type	Linotronic
Profile Version	2.1.0
Profile Class	Display Device Profile
Color Space Data	RGB
Profile Connection Space	XYZ
Profile Date Time	1998:02:09 06:49:00
Profile File Signature	acsp
Primary Platform	Microsoft Corporation
CMV Flags	Not Embedded, Independent
Device Manufacturer	Hewlett-Packard
Device Model	sRGB

7. **Realice el análisis de dos archivos: a) un crack de cualquier programa y b) un archivo normal y mediante la página <https://www.virustotal.com> haga un análisis de virus.**

Para realizar el siguiente análisis se utilizaran los siguientes archivos:

 captura de pantalla	05/11/2018 02:25 ...	Carpeta de archivos
 KMSpico v.10.2.0.zip	15/07/2018 09:53 a...	Archivo WinRAR Z..
 Patch.exe	17/10/2016 04:44 ...	Aplicación
 rufus-2.15.exe	24/06/2017 10:54 a...	Aplicación

Análisis de un programa sin virus:

Rufus-2.15.exe, es un programa que no tiene virus y para demostrar esto se utilizara el siguiente sitio: <https://www.virustotal.com/#/home/upload>



Analice los archivos sospechosos y las URL para detectar tipos de malware, y compártalos automáticamente con la comunidad de seguridad.


Búsqueda deURL dearchivos



Elija el archivo

Al enviar su archivo a VirusTotal, le está pidiendo a VirusTotal que comparta su envío con la comunidad de seguridad y acepte nuestros [Términos de servicio](#) y [Política de privacidad](#). [Más información](#).

Una vez en la página presionamos donde dice “elija el archivo”. Una vez que termine de cargar el archivo nos mostrará un análisis de los antivirus que los reconocen como virus o como un archivo aprobado (sin virus)-.



Archivo publicado en la colección de software de Akeo Consulting.

SHA-256: 13d5d1aa0663f78db23701cc336956a3e5bc7f7b90981f0b46d4d219c126b498

Nombre del archivo: Rufo

Tamaño del archivo: 932.12 KB

Ultimo analisis: 2018-11-03 18:51:10 UTC

Puntuación de la comunidad: +82

0/66

Detección	detalles	relaciones	Comportamiento	comunitario
Ad-Aware	✓ Limpiar		AegisLab	✓ Limpiar
AhnLab-V3	✓ Limpiar		Alibaba	✓ Limpiar
ALYAC	✓ Limpiar		Antiy-AVL	✓ Limpiar
Arcabit	✓ Limpiar		Avast Mobile Security	✓ Limpiar
Avira	✓ Limpiar		Babable	✓ Limpiar
Baidu	✓ Limpiar		BitDefender	✓ Limpiar
Bkav	✓ Limpiar		CAT-QuickHeal	✓ Limpiar
ClamAV	✓ Limpiar		CMC	✓ Limpiar

Como se podrá ver el archivo es reconocido por diferentes tipos de antivirus, las cuales nos indican que el programa está limpio



Archivo publicado en la colección de software de Akeo Consulting.

SHA-256: 13d5d1aa0663f78db23701cc336956a3e5bc7f7b90981f0b46d4d219c126b498


Nombre del archivo: Rufo

Tamaño del archivo: 932.12 KB

Ultimo analisis: 2018-11-03 18:51:10 UTC

Puntuación de la comunidad: +82

0/66


Detección	detalles	relaciones	Comportamiento	comunitario
Votos ⓘ <div> <div>  Seguro <div>5</div> </div> <div>  Inseguro <div>0</div> </div> </div>				

Conclusión el programa es seguro.

Análisis de un programa con virus:

Para realizar el análisis del programa realizamos el mismo procedimiento:

Unas veces que termine de analizar el programa nos mostrara los resultados, como se podrá ver el archivo no es reconocido por varios antivirus:



42 engines detected this file

SHA-256 64c731adbe1b96cb5765203b1e215093dcf268d020b299445884a4ae62ed2d3a

File name KMSpico_setup.exe

File size 3.08 MB

Last analysis 2018-11-05 15:19:34 UTC

Community score -29

42 / 66

Detection	Details	Relations	Behavior	Community
Ad-Aware	Application.Hacktool.KMSAuto.N	AhnLab-V3	HackTool/Win32.Crack.C509549	
ALYac	Misc.HackTool.AutoKMS	Antiy-AVL	RiskWare[NetTool]/Win64.RPCHook	
Arcabit	Application.Hacktool.KMSAuto.N	Avast	Win32:PUP-gen [PUP]	
AVG	Win32:PUP-gen [PUP]	BitDefender	Application.Hacktool.KMSAuto.N	
Bkav	W32.HfsAdware.216A	CAT-QuickHeal	Trojan.CGeneric	
ClamAV	Win.Malware.Agent-6369644-0	Cybereason	malicious.71a50c	
Cyren	W32/S-eb8730b5!Eldorado	DrWeb	Trojan.Moneyinst.709	
Emsisoft	Application.HackTool (A)	Endgame	malicious (high confidence)	

Por ultimo podemos ver la valoración global de que la aplicación está infectado y que nos segura su utilización, la página nos muestra de la siguiente manera:



42 motores detectaron este archivo

SHA-256 64c731adbe1b96cb5765203b1e215093dcf268d020b299445884a4ae62ed2d3a

Nombre del archivo KMSpico_setup.exe

Tamaño del archivo 3.08 MB

Ultimo analisis 2018-11-05 15:19:34 UTC

Puntuación de la comunidad -29

42/66

Detección	detalles	relaciones	Comportamiento	comunitario
<div>Votos</div> <div> <div>  Caja fuerte <div>66</div> </div> <div>  Inseguro <div>29</div> </div> </div> <div>  Debes haber iniciado sesión para votar. </div>				

De acuerdo a la página podemos concluir que el programa es un programa inseguro.

- Mediante el programa prtg realice en análisis de red (cualquier red) y vea si hay alguna anomalía.