Memory Forensics

و هي من اهم الاشياء و اكثر الاشياء (RAM)بنحلل اليوم الذاكرة العشوائية حساسة في عالم التحقيق الجنائي

مقدمة بسيطة

ليش الرام من اكثر الاشياء المهمة و الحساسة ؟

1-البيانات اللي فيها تكون غير مشفرة زي كلمات المرور و غيرها

2-البرامج اللي شغالين عليها و ايش قاعد تسوي فيها كلها تكون بشكل غير مشفر

3-بيعرف كل شي شغال في العملية(process) زي المواقع اللي زرتها

اطفاء الجهاز تنحذف فيه غلط منتشر كثير عند الناس اللي هو اذا طفيت الجهاز الرام تنحذف علطول و هذا غلط الرام تقعد البيانات فيها بعد اطفاء الجهاز بمدة بسيطة ما تتجاوز 10 دقائق فيها اختلاف المدة بس بشكل عام لازم تعرف ان الرام تقعد حتى بعد اطفاء البيانات بمدة بسيطة و اذا قدر المحقق الجنائي يلحق على المدة هذي ممكن يسوي عملية تجميد(freeze) عملية التجميد ممكن تزيد فترة بقاء البيانات في الرام لدقايق اكثر او لساعات

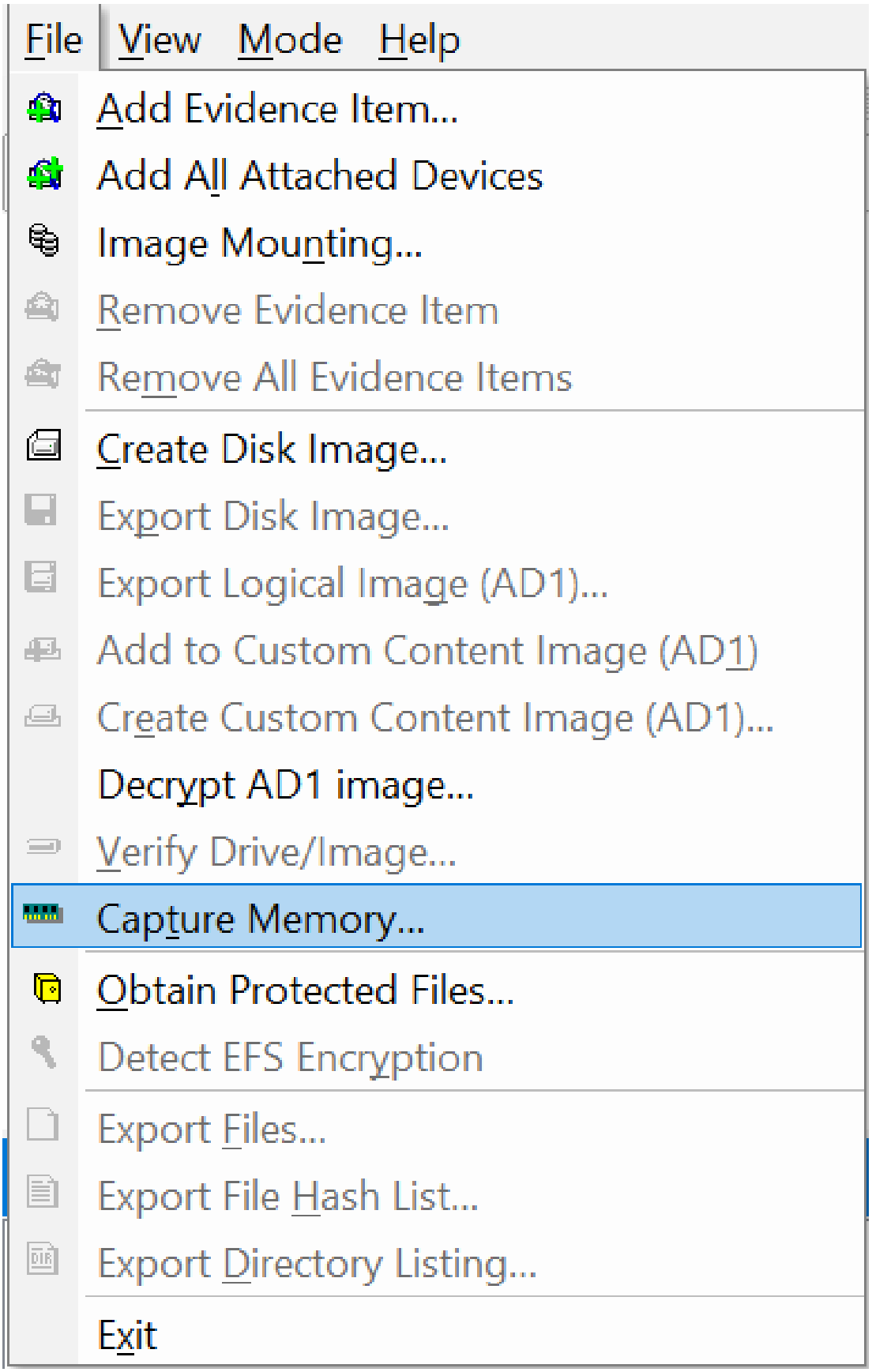
Method	Time Delay	Temperature Cooled degrees C
Liquid Nitrogen	10mins, 1 hr, 2hrs	-196
Freezing Spray	10 mins	-40
ICE	10 mins	10

يحطون الرام في درجة حرارة منخفضة جدا للمساعدة على بقاء البيانات في فترة اطول

التطبيق العملي

حفظ الرام

في البداية عشان نحفظ الرام و نبدأ نفحصها نحتاج برنامج FTK imager بعد ما تحملة و تفتح البرنامج


File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit

بعدها تختار اسم و المسار اللي تبي تحذف الملف فيه

بداية المعالجة عليها

في المثال بشرح على ذاكرة من النت مو اللي سحبتها من جهازي من افضل الادوات ل فحص الرام volatility و هذي الذاكرة اللي راح افحصها رابط التحميل

image info

و هو امر عشان نعرف نوع النظام اللي كانت شغالة علية لأن يختلف الويندوز بين نسخة و يختلف عن اللينكس

```
C:\Users\kira2\Desktop\IT\tools\volatility>volatility.exe -f memdump.bin imageinfo
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 (C:\Users\kira2\Desktop\IT\tools\volatility\memdump.bin)
                      PAE type : No PAE
                           DTB : 0x39000L
```

طلع لي WinXSPx86 لازم اعرفة عشان اكمل افحص بناء على النسخة هذي

pstree

```
C:\Users\kira2\Desktop\IT\tools\volatility>volatility.exe -f memdump.bin --profile=WinXPSP2x86 pstree
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
```

لاحظ اني حطيت profile بعدين الاصدار اللي كان طالع لي بعدين حطيت الخيار اللي ابيه و اللي هو pstree و يعطيني العمليات اللي اشتغلت من اول عملية الى اخر عملية و العمليات التابعة لعملية ثانية و تقدر تميز من PID و PPID

Show 10 entries Search:

Offset(P)	Name	PID	PPID	PDB	Time Created	Time Exited
33534624	ps.exe	228	356	507629568	2012-11-27 01:22:07 UTC+0000	
33554912	wc.exe	1992	1032	444317696	2012-11-27 01:30:00 UTC+0000	
33573144	cmd.exe	1860	296	16379904	2012-11-27 01:42:52 UTC+0000	
33724344	cmd.exe	1048	1032	386736128	2012-11-27 00:27:41 UTC+0000	2012-11-27 01:22:20 UTC+0000
33770304	cmd.exe	456	1032	157282304	2012-11-27 00:18:21 UTC+0000	2012-11-27 00:27:30 UTC+0000
33832352	alg.exe	1888	684	150056960	2012-11-26 22:01:59 UTC+0000	
35083224	svchost.exe	1076	684	123576320	2012-11-26 22:01:55 UTC+0000	
35113744	svchost.exe	944	684	122290176	2012-11-26 22:01:55 UTC+0000	
35342968	spoolsv.exe	1360	684	145006592	2012-11-26 22:01:58 UTC+0000	
35367952	svchost.exe	1128	684	140267520	2012-11-26 22:01:56 UTC+0000	

و ممكن تخليه الاداة تستخرجها ك html عشان تكون اسهل لك

DLLlist

```
mdd.exe pid:    988
Command line : mdd.exe -o c:\memdump-amirs.bin
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x19000     0xffff C:\mdd.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff C:\WINDOWS\system32\Secur32.dll
0x7c9c0000   0x817000     0xffff C:\WINDOWS\system32\SHELL32.dll
0x77f10000    0x49000     0xffff C:\WINDOWS\system32\GDI32.dll
0x7e410000    0x91000     0xffff C:\WINDOWS\system32\USER32.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x77f60000    0x76000     0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x76390000    0x1d000        0x2 C:\WINDOWS\system32\IMM32.DLL
0x773d0000   0x103000        0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144cc
0x5d090000    0x9a000        0x1 C:\WINDOWS\system32\comctl32.dll
0x68000000    0x36000        0x1 C:\WINDOWS\system32\rsaenh.dll
```

وظيفتة يعطيك كل عملية و كل ملف dll تستعمله العملية و هذي تفيدك اذا تبي تاخذ فكرة عن البرنامج بعض امثلة ملفات dll اللي ممكن تستخدم في اشياء ضارة

```
1- Socket creation using the dll file Ws2_32.dll.

2- Network communication using the dll file WININET.DLL.

3- Registry queries using the dll file ADVAPI32.DLL.

4- Encryption using the dll file SECURE32.DLL.

5- Browser interaction using the dll file URLMON.DLL.
```

connscan

```
C:\Users\kira2\Desktop\IT\tools\volatility>volatility.exe -f memdump.bin --profile=WinXPSP2x86 connscan
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
0x16066d48 172.16.223.187:2109       172.16.150.10:389        640
```

وظيفتها توريك الاتصالات اللي قاعدة تصير على جهازك كل pid و ايبي و البورت اللي شابك علية

psxview

```
C:\Users\kira2\Desktop\IT\tools\volatility>volatility.exe -f memdump.bin --profile=WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x02214da0 winlogon.exe            632 True   True   True     True   True  True    True
0x02244460 svchost.exe             860 True   True   True     True   True  True    True
0x021d6598 msimn.exe              1984 True   True   True     True   True  True    True
0x021d43c0 ctfmon.exe              700 True   True   True     True   True  True    True
0x021bac10 svchost.exe            1128 True   True   True     True   True  True    True
0x0221d5a8 mdd.exe                 988 True   True   True     True   True  True    True
0x021b4a78 spoolsv.exe            1360 True   True   True     True   True  True    True
0x02043da0 alg.exe                1888 True   True   True     True   True  True    True
0x0217cb10 svchost.exe             944 True   True   True     True   True  True    True
0x022ba638 services.exe            684 True   True   True     True   True  True    True
0x0228fda0 svchost.exe            1032 True   True   True     True   True  True    True
0x021753d8 svchost.exe            1076 True   True   True     True   True  True    True
0x020001e0 wc.exe                 1992 True   True   True     True   True  True    True
0x021f7da0 ps.exe                 1052 True   True   True     True   True  True    True
0x02226a20 msmsgs.exe              660 True   True   True     True   True  True    True
```

و وظيفتها تطلع لك العمليات المخفية و اذا فية عملية مخفية بتلاقي وحدة من اول خانتين false طبعا اذا شفتها تحاول تخفي نفسها بتشك فيها بس مو شرط يعتبر ضار بس ما اخفى نفسة الا لسبب

pcosdump

```
C:\Users\kira2\Desktop\IT\tools\volatility>volatility.exe -f memdump.bin --profile=WinXPSP2x86 procdump -p 988 --dump-dir=.
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x8221d5a8 0x00400000 mdd.exe              OK: executable.988.exe
```

تستخرج لك اي عملية مشغلة ف في حالة انك لقيت شي مشبوه تقدر تستخرجة و تسوي علية هندسة عكسية او تاخذ الهاش حقه و تحطه في مواقع زي virustotal ملاحظة: مو كل شي يقوله virustotal يعني صح

memdump

```
C:\Users\kira2\Desktop\IT\tools\volatility>volatility.exe -f memdump.bin --profile=WinXPSP2x86 memdump  -p 988 --dump-dir=.
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing mdd.exe [   988] to 988.dmp
```

تستخرج لك الذاكرة اللي كانت في العملية زي المتغيرات في العملية و هذي تفيد مع procdump
ممكن بعد ما تسخرجها تفحصها و تدور اشياء فيها زي لو فيه برنامج يطلب ايبي و بورت معين
عشان يتصل فيهم بتلاقي البورت اللي دخله و الايبي

هنا فيه بعض الاماكن اللي ممكن تفيدكم اذا تبي تمارس اكثر
https://github.com/stuxnet999/MemLabs