

# Forensic Study - 4

## Windows Dump (2) -

### Example

---

---

2017.10.30

---

KUICS

---

2014210009 주어진

---

# 목차

- 
1. Memory Dump & Introduction of the Memory Dump Analysis - 복습
  2. Example 2 - 예제
  3. Example 2 - 풀이
-

# Memory Dump?

컴퓨팅에서, 코어 덤프(core dump), 메모리 덤프(memory dump), 또는 시스템 덤프(system dump)는 컴퓨터 프로그램이 특정 시점에 작업 중이던 메모리 상태를 기록한 것으로, 보통 프로그램이 비정상적으로 종료했을 때 만들어진다.

실제로는, 그 외에 중요한 프로그램 상태도 같이 기록되곤 하는데, 프로그램 카운터, 스택 포인터 등 CPU 레지스터나, 메모리 관리 정보, 그 외 프로세서 및 운영 체제 플래그 및 정보 등이 포함된다.

출처 : [https://ko.wikipedia.org/wiki/%EC%BD%94%EC%96%B4\\_%EB%8D%A4%ED%94%84](https://ko.wikipedia.org/wiki/%EC%BD%94%EC%96%B4_%EB%8D%A4%ED%94%84)

# Intro of the Memory Dump Analysis

1. Strings로 Alphanumeric 문자열을 뽑아낸다.
2. 근거가 될 수 있는 문자열을 발견하지 못했다면 메모리 덤프 툴을 이용해 분석을 시작한다.
  - 운영체제의 종류를 알아낸다. ( Memory Map이 Windows 버전마다 다르기 때문에 최우선 )
  - 이를 바탕으로 어떤 프로세스가 로드되어 있는지 또는 프로세스들간의 부모-자식 관계를 확인한다.
    - 의심가는 프로세스를 발견했다면 이를 추출하거나 PID를 근거로 Network Connection, Dll list등을 확인한다.
    - 만약 발견하지 못했다면 Driver나 Dll Injection등이 있는지를 확인한다.
  - 레지스트리 항목을 확인한다. ( 특히 Software항목이나 Run/RunOnce 또는 BHO )

---

# Example 2

다운로드 :

<https://drive.google.com/file/d/0B7Llj1y13UeaMXNxdjBzQ2o1eW8/view?usp=sharing>

# Example 2

## 목표

### 1. Flag 찾기 ( 3번째 시간보단 어려운 편 )

시간 : 40분

- 3번째 시간의 PPT를 참조하시면 큰 도움이 됩니다. ( 특히 풀이 )
- Wiki에 필요한 명령어들의 사용법이 있습니다.
- 정말 모르겠다 싶으면 뒤의 풀이를 따라해보셔도 좋습니다.
- 큰 힌트 1 : 제 컴퓨터를 망가뜨리진 말아주세요.
- 큰 힌트 2 : 멍청한 저는 비밀번호를 아이디입력란에 기입하고 말았습니다.
- 큰 힌트 3 : SSH가 뭘까요?

# Example 2 - 풀이

C:\Users\wakwe\Desktop\Study>volatility\_2.6\_win64\_standalone.exe pslist -f EX2.raw --profile=Win7SP1x64

Volatility Foundation Volatility Framework 2.6

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xffffffff80024cb870	System	4	0	95	529	-----	0	2017-10-30 10:10:16 UTC+0000	
0xffffffff8003c889e0	smss.exe	276	4	2	30	-----	0	2017-10-30 10:10:16 UTC+0000	
0xffffffff800454c060	csrss.exe	360	348	9	615	0	0	2017-10-30 10:10:19 UTC+0000	
0xffffffff8003f898f0	wininit.exe	400	348	4	85	0	0	2017-10-30 10:10:19 UTC+0000	
0xffffffff8003eb9b10	csrss.exe	412	392	10	222	1	0	2017-10-30 10:10:19 UTC+0000	
0xffffffff8005f8cb10	services.exe	452	400	10	249	0	0	2017-10-30 10:10:19 UTC+0000	
0xffffffff80047dbb10	lsass.exe	472	400	9	602	0	0	2017-10-30 10:10:19 UTC+0000	
0xffffffff80047da840	lsass.exe	480	400	11	149	0	0	2017-10-30 10:10:19 UTC+0000	
0xffffffff800486a940	winlogon.exe	508	392	5	127	1	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff80048c4060	svchost.exe	632	452	14	379	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff80049a6700	vmacthlp.exe	696	452	4	57	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff80049c9730	svchost.exe	744	452	9	289	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff8004a00b10	svchost.exe	792	452	22	458	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff8004a3e060	svchost.exe	876	452	24	479	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff800488fb10	svchost.exe	920	452	34	801	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff8004a8d9c0	svchost.exe	960	452	39	828	0	0	2017-10-30 10:10:20 UTC+0000	
0xffffffff8004aaeb10	audiogd.exe	1016	792	6	136	0	0	2017-10-30 10:10:21 UTC+0000	
0xffffffff8004b329c0	svchost.exe	476	452	22	411	0	0	2017-10-30 10:10:21 UTC+0000	
0xffffffff8004bc5870	spoolsv.exe	1120	452	16	355	0	0	2017-10-30 10:10:21 UTC+0000	
0xffffffff8004bebb10	svchost.exe	1156	452	21	325	0	0	2017-10-30 10:10:21 UTC+0000	
0xffffffff8004bcd060	svchost.exe	1272	452	12	149	0	0	2017-10-30 10:10:22 UTC+0000	
0xffffffff8004be5060	svchost.exe	1356	452	23	269	0	0	2017-10-30 10:10:22 UTC+0000	
0xffffffff8004c7d7e0	taskhost.exe	1420	452	11	243	1	0	2017-10-30 10:10:22 UTC+0000	
0xffffffff8002ff7b10	sppsvc.exe	1488	452	5	155	0	0	2017-10-30 10:10:22 UTC+0000	
0xffffffff80025741f0	dwm.exe	1584	876	5	80	1	0	2017-10-30 10:10:22 UTC+0000	
0xffffffff80025d5b10	VGAuthService.exe	1612	452	3	90	0	0	2017-10-30 10:10:22 UTC+0000	
0xffffffff80025c9b10	explorer.exe	1660	1552	33	687	1	0	2017-10-30 10:10:23 UTC+0000	
0xffffffff8004d620f0	vmtoolsd.exe	1704	452	10	301	0	0	2017-10-30 10:10:23 UTC+0000	
0xffffffff8004daa900	ManagementAgent	1780	452	11	103	0	0	2017-10-30 10:10:23 UTC+0000	
0xffffffff8004e2b060	vmtoolsd.exe	1896	1660	7	192	1	0	2017-10-30 10:10:24 UTC+0000	
0xffffffff8004a22230	svchost.exe	1844	452	6	98	0	0	2017-10-30 10:10:26 UTC+0000	
0xffffffff8004f1ab10	dlhhost.exe	2092	452	21	211	0	0	2017-10-30 10:10:26 UTC+0000	
0xffffffff8004f5ab10	WmiPrvSE.exe	2164	632	9	185	0	0	2017-10-30 10:10:26 UTC+0000	
0xffffffff8004bd5360	dlhhost.exe	2268	452	17	222	0	0	2017-10-30 10:10:26 UTC+0000	
0xffffffff80050575d0	msdtc.exe	2420	452	16	161	0	0	2017-10-30 10:10:27 UTC+0000	
0xffffffff8003b96830	VSSVC.exe	2612	452	7	126	0	0	2017-10-30 10:10:29 UTC+0000	
0xffffffff8005128b10	SearchIndexer.exe	2672	452	13	612	0	0	2017-10-30 10:10:30 UTC+0000	
0xffffffff80051a45d0	wmpnetwk.exe	2800	452	12	221	0	0	2017-10-30 10:10:30 UTC+0000	
0xffffffff8009425b10	WmiPrvSE.exe	2884	632	13	300	0	0	2017-10-30 10:10:46 UTC+0000	
0xffffffff80052f3930	WmiAnSvc.exe	2972	452	8	122	0	0	2017-10-30 10:10:47 UTC+0000	
0xffffffff8003d8f850	putty.exe	2332	1660	8	174	1	1	2017-10-30 10:10:52 UTC+0000	
0xffffffff8005265370	putty.exe	3056	1660	7	174	1	1	2017-10-30 10:10:54 UTC+0000	
0xffffffff8003760060	Dumpit.exe	1324	1660	2	46	1	1	2017-10-30 10:11:19 UTC+0000	
0xffffffff8003f65b10	conhost.exe	2664	412	3	91	1	0	2017-10-30 10:11:19 UTC+0000	

## 1. Imageinfo 이후 프로세스 리스트 확인

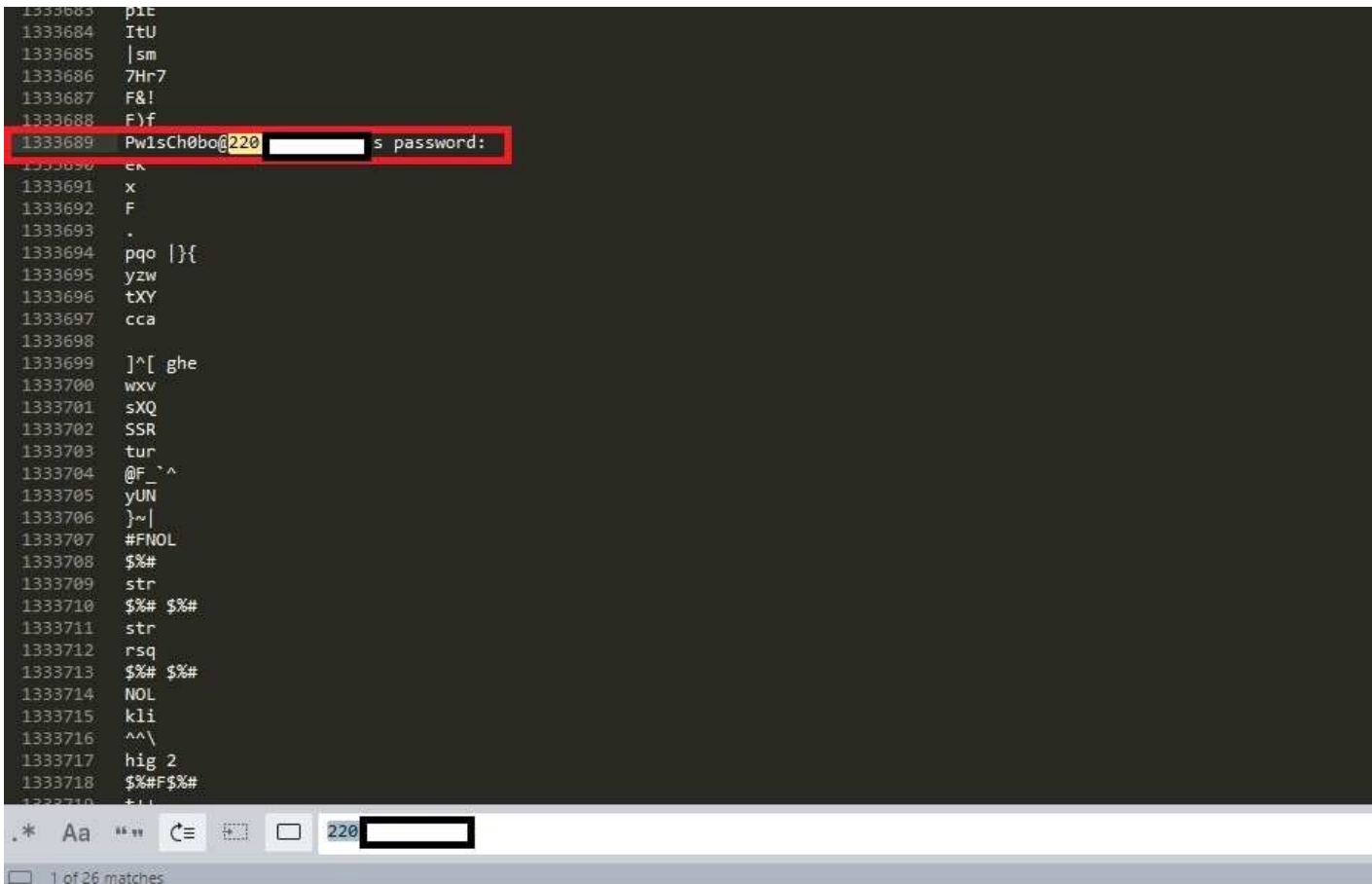
# Example 2 - 풀이

```
C:\Users\wakke\Desktop\Study>volatility_2.6_win64_standalone.exe nscan -f EX2.raw --profile=Win7SP1x64
Volatility Foundation Volatility Framework 2.6
Offset(P) Proto Local Address Foreign Address State Pid Owner Created
0xbc5b1620 UDPv4 0.0.0.0:61865 *** 920 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd2df130 UDPv4 0.0.0.0:5355 *** 476 svchost.exe 2017-10-30 10:10:29 UTC+0000
0xbd2f0c30 UDPv4 0.0.0.0:3702 *** 920 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd336340 UDPv6 fe80::1d0a:dde0:f685:7fdd:61867 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd3713d0 UDPv6 :::1:61868 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd380540 UDPv4 192.168.244.128:61869 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd3bfb20 UDPv6 :::1:1900 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd3cf400 UDPv4 0.0.0.0:61866 *** 920 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd3cf400 UDPv6 :::61866 *** 920 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd3d5a20 UDPv4 0.0.0.0:3702 *** 1356 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd3d5a20 UDPv6 :::3702 *** 1356 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd3e010 UDPv4 192.168.244.128:1900 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd3f74b0 UDPv6 fe80::1d0a:dde0:f685:7fdd:1900 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd493ec0 UDPv4 0.0.0.0:0 *** 476 svchost.exe 2017-10-30 10:10:26 UTC+0000
0xbd493ec0 UDPv6 :::0 *** 476 svchost.exe 2017-10-30 10:10:26 UTC+0000
0xbd4d1d60 UDPv4 192.168.244.128:138 *** 4 System 2017-10-30 10:10:26 UTC+0000
0xbd50c910 UDPv6 fe80::1d0a:dde0:f685:7fdd:546 *** 792 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd546b50 UDPv4 0.0.0.0:5355 *** 476 svchost.exe 2017-10-30 10:10:29 UTC+0000
0xbd546b50 UDPv6 :::5355 *** 476 svchost.exe 2017-10-30 10:10:29 UTC+0000
0xbd5a7ec0 UDPv4 127.0.0.1:1900 *** 1356 svchost.exe 2017-10-30 10:10:31 UTC+0000
0xbd5aa200 UDPv4 0.0.0.0:3702 *** 1356 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd5b72c0 TCPv4 0.0.0.0:49156 0.0.0.0:0 LISTENING 472 lsass.exe
0xbd5b72c0 TCPv6 :::49156 :::0 LISTENING 472 lsass.exe
0xbd5b7540 TCPv4 0.0.0.0:49156 0.0.0.0:0 LISTENING 472 lsass.exe
0xbd4896c0 TCPv4 0.0.0.0:49155 0.0.0.0:0 LISTENING 452 services.exe
0xbd4896c0 TCPv6 :::49155 :::0 LISTENING 452 services.exe
0xbd48b470 TCPv4 0.0.0.0:49155 0.0.0.0:0 LISTENING 452 services.exe
0xbd4e4920 TCPv4 192.168.244.128:139 0.0.0.0:0 LISTENING 4 System
0xbd26ba00 TCPv6 -:0 18bb:7d04:80fa:ffff:e0f6:7304:80fa:ffff:0 CLOSED 44
0xbd9939a0 TCPv4 192.168.244.128:49160 220. [REDACTED] ESTABLISHED -1
0xbd5e4390 TCPv4 127.0.0.1:5357 127.0.0.1:49161 CLOSED -1
0xbd5d1730 TCPv4 127.0.0.1:49161 127.0.0.1:5357 CLOSED -1
0xbd647d70 UDPv4 0.0.0.0:3702 *** 1356 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd676440 UDPv4 0.0.0.0:54527 *** 1356 svchost.exe 2017-10-30 10:10:23 UTC+0000
0xbd676440 UDPv6 :::54527 *** 1356 svchost.exe 2017-10-30 10:10:23 UTC+0000
0xbd676d00 UDPv4 0.0.0.0:54526 *** 1356 svchost.exe 2017-10-30 10:10:23 UTC+0000
0xbd749010 UDPv4 0.0.0.0:3702 *** 1356 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd749010 UDPv6 :::3702 *** 1356 svchost.exe 2017-10-30 10:11:25 UTC+0000
0xbd7e11b0 UDPv4 0.0.0.0:3702 *** 920 svchost.exe 2017-10-30 10:11:25 UTC+0000
```

2. Network Connection 확인 - Putty를 프로세스 리스트에서 확인 한 것이 근거.



## Example 2 - 풀이



```
1333683 p1E
1333684 ItU
1333685 |sm
1333686 7Hr7
1333687 F&!
1333688 F)f
1333689 Pw1sCh0bo@220 s password:
1333690 eK
1333691 x
1333692 F
1333693 .
1333694 pqo |}{
1333695 yzw
1333696 tXY
1333697 cca
1333698
1333699 ]^[ ghe
1333700 wxv
1333701 sXQ
1333702 SSR
1333703 tur
1333704 @F_ ^ ^
1333705 yUN
1333706 }~|
1333707 #FNOL
1333708 $%#
1333709 str
1333710 $%# $%#
1333711 str
1333712 rsq
1333713 $%# $%#
1333714 NOL
1333715 kli
1333716 ^^ \
1333717 hig 2
1333718 $%#F$%#
1333719 tL
```

1 of 26 matches

3. String 확인 - 덤프파일에서 string 추출 후, IP나 Putty와 관련된 문자열로 확인

## Example 2 - 풀이

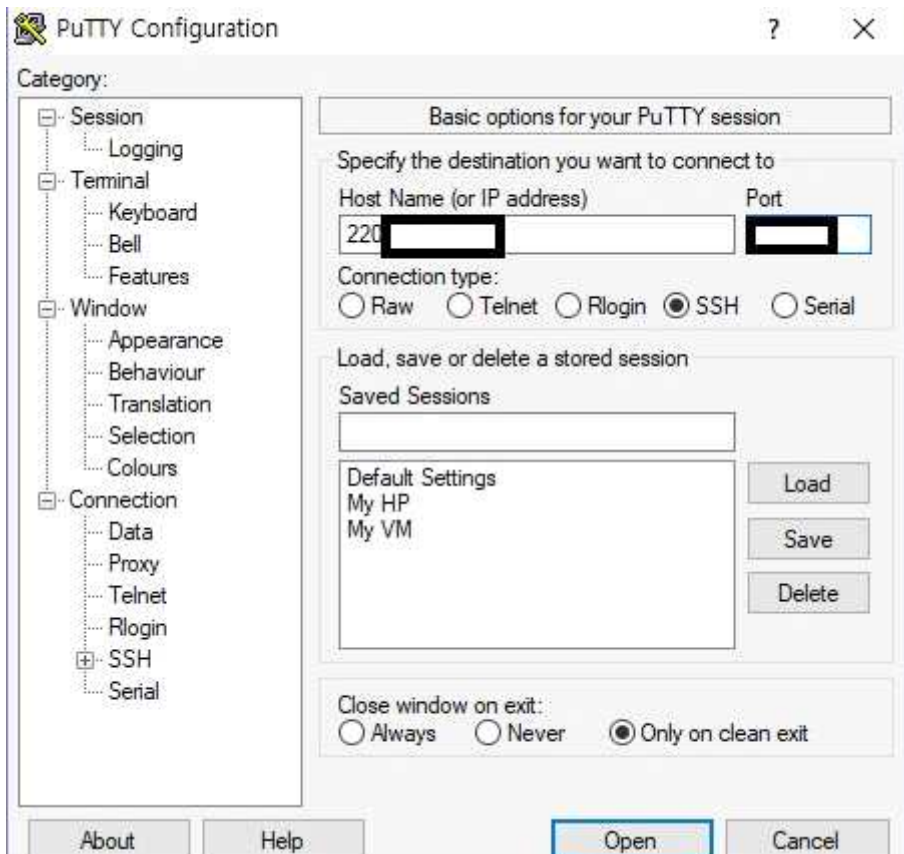


```
1419208 xFM
1419209 chobo@220 [redacted] s_password:
1419210 QS
1419211
1419212 [?12l
1419213 [?25h
1419214 [1;1H*
1419215 'i?I
1419216 rc,
1419217 ;|5
1419218 D8b
1419219 UXU
1419220 5&=
1419221 ~G*
1419222 ETT
1419223 Q
1419224 hr(
1419225 gc\t4
1419226 FU
1419227 NGS
1419228 ;fYE
```

3. String 확인 - 덤프파일에서 string 추출 후, IP나 Putty와 관련된 문자열로 확인

# Example 2 - 풀이

4. 로그인 - Putty를 이용해 SSH 접속을 시도해보자 ( IP / Port, ID / PW를 전부 알아냈으니. )



# Example 2 - 풀이

5. 로그인 - C:\Users\W~\에서 dir를 입력하면 Flag 힌트가 나오고, C:\로 경로를 바꾸었더니 Flag가 있다.

```
C:\>dir
C 드라이브의 볼륨 : Windows
볼륨 일련 번호: 383E-9E4A

C:\ 디렉터리

2017-08-22 오후 04:47 <DIR> $WINDOWS.BT
2017-08-24 오전 12:20 <DIR> .Trash-1000
2017-01-22 오후 04:11 49,388 bdlog.txt
2016-09-22 오후 02:10 <DIR> db
2017-10-10 오후 02:25 <DIR> ESD
2008-01-05 오전 11:46 5,970 eula.1042.txt
2016-04-27 오후 10:07 3,814 eula.2052.txt
2017-10-30 오후 02:58 18 FlagIsGimmeAChicken
2008-01-05 오전 11:46 1,110 globdata.ini
2008-01-05 오전 11:46 562,688 install.exe
2008-01-05 오전 11:46 843 install.ini
2008-01-05 오전 11:50 79,888 install.res.1042.dll
2016-04-27 오후 10:07 74,768 install.res.2052.dll
2017-10-14 오후 01:48 <DIR> Intel
2016-08-15 오전 12:15 <DIR> Logs
2017-10-27 오전 03:35 <DIR> Nexon
2017-03-19 오전 06:03 <DIR> PerfLogs
2017-10-30 오후 04:51 <DIR> Program Files
2017-10-27 오전 03:33 <DIR> Program Files (x86)
2016-12-20 오후 07:17 <DIR> Project
2017-09-21 오후 06:13 <DIR> Python27
2017-09-13 오후 02:04 <DIR> Sandbox
2017-07-20 오후 06:21 <DIR> Strawberry
2017-03-15 오후 07:41 <DIR> SymCache
2017-09-23 오후 10:46 <DIR> Temp
2017-06-14 오후 07:05 <DIR> Users
2017-10-30 오후 01:47 <DIR> Windows

9개 파일 778,487 바이트
18개 디렉터리 132,195,594,240 바이트 남음

C:\>
```

# 감사합니다

---

과제 : 사실 이번 예제가 과제였으나, 참여율 저조로 4번째 시간에 다루게 되었습니다. ( 그러므로 없음 )

참조 :

<https://github.com/volatilityfoundation/volatility>

<https://github.com/volatilityfoundation/volatility/wiki>