

윈도우 7 파일시스템



JK Kim

@pr0neer

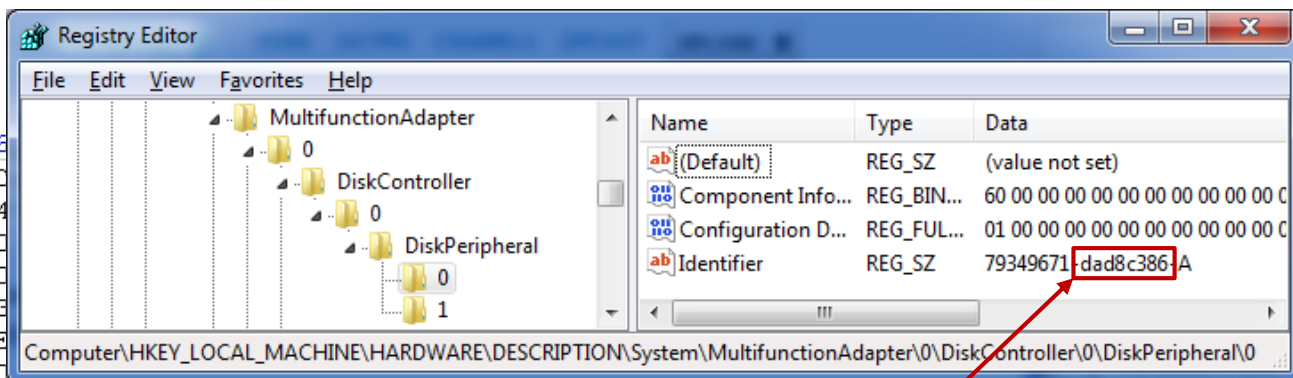
forensic-proof.com

proneer@gmail.com

1. **DISK Identification**
2. **DISKPART clean**
3. **Symbolic Links, Hard Links and Junctions**
4. **Update Last Access Date**
5. **Transactional NTFS (TxF)**
6. **Volume Boot Record sector**
7. **Additional Command**

DISK Identification

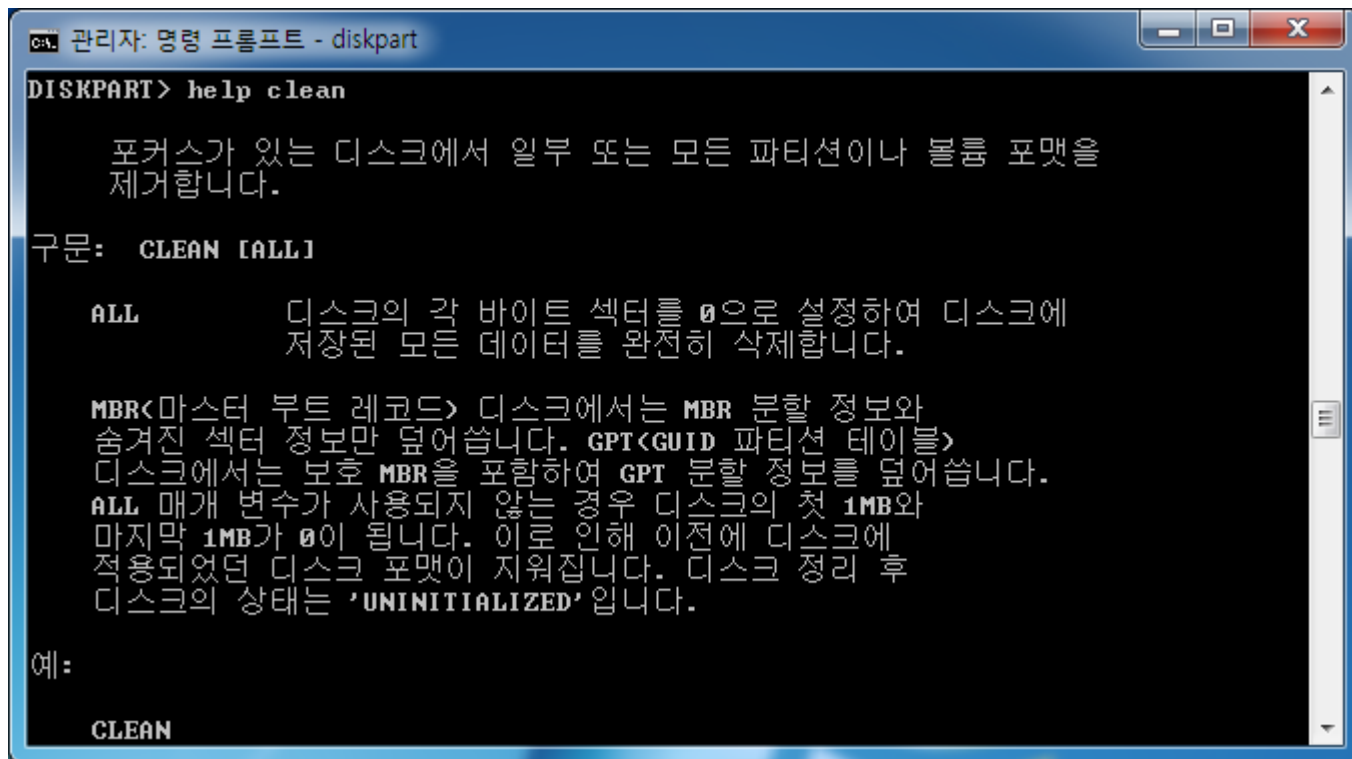
Offset	0	1	2	3	4	5	6
0000000000	33	C0	8E	D0	BC	00	7C
0000000010	06	B9	00	02	FC	F3	A4
0000000020	BD	BE	07	80	7E	00	00
0000000030	E2	F1	CD	18	88	56	00
0000000040	B4	41	BB	AA	55	CD	13
0000000050	F7	C1	01	00	74	03	FE
0000000060	26	66	68	00	00	00	00
0000000070	7C	68	01	00	68	10	00
0000000080	9F	83	C4	10	9E	EB	14
0000000090	8A	76	01	8A	4E	02	8A
00000000A0	4E	11	75	0C	80	7E	00
00000000B0	55	32	E4	8A	56	00	CD
00000000C0	AA	75	6E	FF	76	00	E8
00000000D0	E8	83	00	B0	DF	E6	60
00000000E0	00	FB	B8	00	BB	CD	1A
00000000F0	43	50	41	75	32	81	F9
0000000100	00	66	68	00	02	00	00
0000000110	53	66	55	66	68	00	00
0000000120	61	68	00	00	07	CD	1A
0000000130	18	A0	B7	07	EB	08	A0
0000000140	05	00	07	8B	F0	AC	3C
0000000150	10	EB	F2	F4	EB	FD	2B
0000000160	24	02	C3	49	6E	76	61
0000000170	74	69	6F	6E	20	74	61
0000000180	20	6C	6F	61	64	69	6E
0000000190	6E	67	20	73	79	73	74
00000001A0	67	20	6F	70	65	72	61
00000001B0	65	6D	00	00	00	63	7B
00000001C0	21	00	07	DF	13	0C	00
00000001D0	14	0C	07	FE	FF	FF	00
00000001E0	FF	FF	07	FE	FF	FF	00
00000001F0	00	00	00	00	00	00	00



MBR Disk Signature

HKLM\HARDWARE\DESCRIPTION\System\
MultifunctionAdapter\0\DiskController\0\DiskPeripheral\0

DISKPART clean



```
C:\> 관리자: 명령 프롬프트 - diskpart

DISKPART> help clean

    포커스가 있는 디스크에서 일부 또는 모든 파티션이나 볼륨 포맷을
    제거합니다.

구문:  CLEAN [ALL]

    ALL          디스크의 각 바이트 섹터를 0으로 설정하여 디스크에
                  저장된 모든 데이터를 완전히 삭제합니다.

    MBR<마스터 부트 레코드> 디스크에서는 MBR 분할 정보와
    숨겨진 섹터 정보만 덮어씁니다. GPT<GUID 파티션 테이블>
    디스크에서는 보호 MBR을 포함하여 GPT 분할 정보를 덮어씁니다.
    ALL 매개 변수가 사용되지 않는 경우 디스크의 첫 1MB와
    마지막 1MB가 0이 됩니다. 이로 인해 이전에 디스크에
    적용되었던 디스크 포맷이 지워집니다. 디스크 정리 후
    디스크의 상태는 'UNINITIALIZED'입니다.

예:

    CLEAN
```

```
DISKPART> select disk=1
```

```
DISKPART> clean all
```

Symbolic links, Hard links and Junctions (1/12) 바로가기(LNK)와의 차이점은?

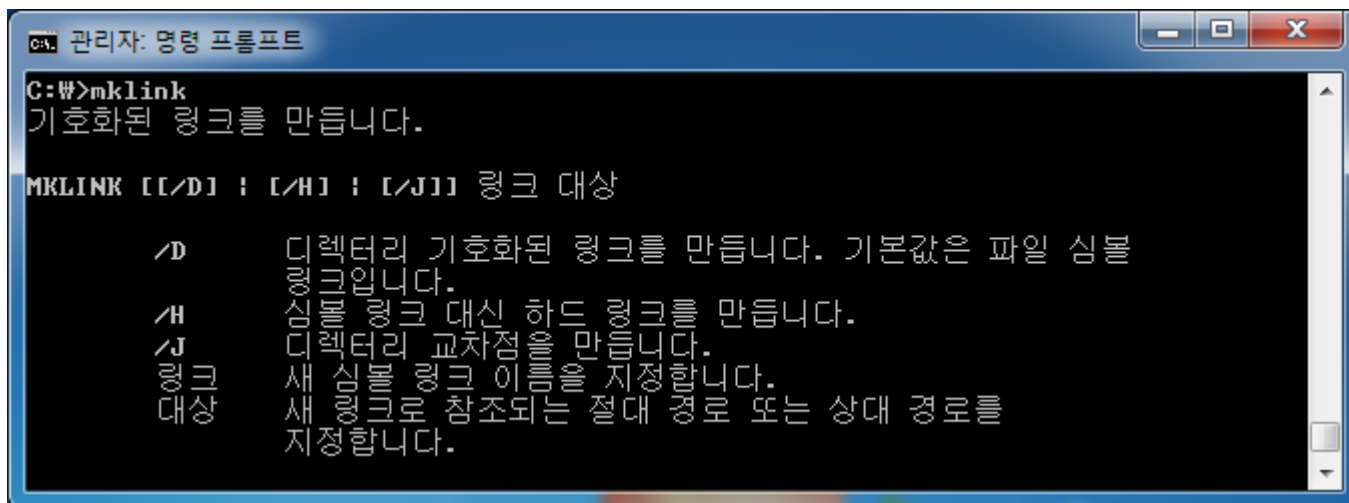
- **심볼릭 링크(Symbolic Link, Soft Link)**
 - 윈도우 Vista에 들어오면서 지원
 - 특정 파일의 경로를 이용하여 파일을 가리키는 역할 (네트워크 폴더도 가능)
 - 원본 파일이 삭제되면 링크를 사용할 수 없음

- **하드 링크(Hard Link)**
 - 윈도우 2000부터 지원
 - 원본 파일의 사본을 생성하여 두 파일의 한 파일만 변경해도 동일한 정보 유지
 - 원본 파일이 삭제되도 사본 유지

- **교차(연결)점(Junction)**
 - 윈도우 2000부터 지원되었고, NTFS만의 고유한 기능으로 NTFS 폴더만 대상
 - 하드링크와 달리 다른 볼륨의 폴더의 교차점 생성 가능 (네트워크 폴더는 불가능)

Symbolic links, Hard links and Junctions (2/12)

- 링크 기능은 Vista 이후의 UAC 가상화와 이전 버전과의 호환성을 위해 널리 사용
- 교차점은 Junction 명령을 통해 생성 가능
 - <http://technet.microsoft.com/en-us/sysinternals/bb896768.aspx>
- 윈도우 Vista 이후에서는 mklink 명령을 통해 심볼릭, 하드 링크, 폴더 교차점 생성 가능



```
관리자: 명령 프롬프트
C:\>mklink
기호화된 링크를 만듭니다.

MKLINK [[/D] : [/H] : [/J]] 링크 대상

/D      디렉터리 기호화된 링크를 만듭니다. 기본값은 파일 심볼
        링크입니다.
/H      심볼 링크 대신 하드 링크를 만듭니다.
/J      디렉터리 교차점을 만듭니다.
링크    새 심볼 링크 이름을 지정합니다.
대상    새 링크로 참조되는 절대 경로 또는 상대 경로를
        지정합니다.
```

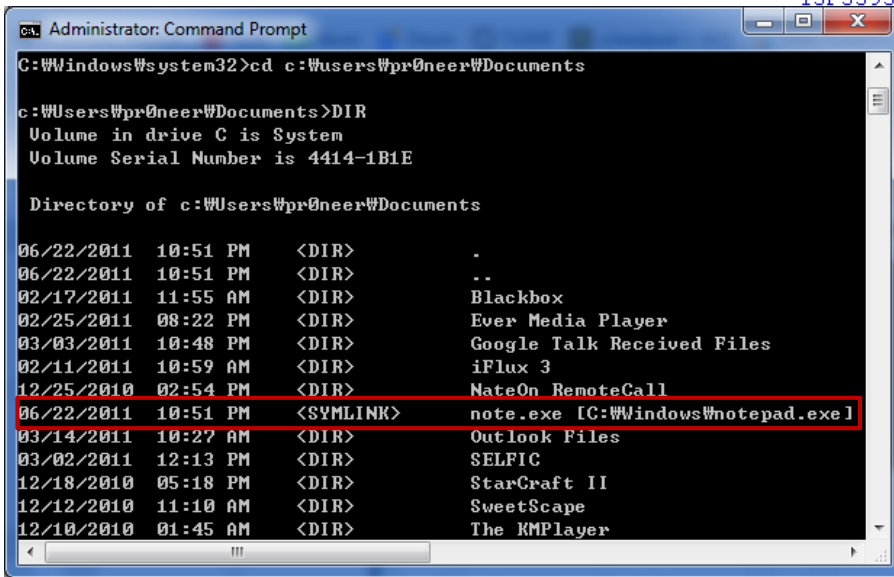
Symbolic links, Hard links and Junctions (3/12)

- 파일에 대한 심볼릭 링크 생성 <SYMLINK>

- `mklink "%USERPROFILE%\Documents\note.exe" "%SYSTEMROOT%\notepad.exe"`

- 속성 ID 0xC0의 \$REPARSE_POINT를 이용하여 심볼릭 링크 관리

- 원본이 삭제되면 링크 사용 불가



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
15F5395000	46	49	4C	45	30	00	03	00	D8	86	50	3C	04	00	00	00	FILE0 0IP<
15F5395010	B0	07	01	00	38	00	01	00	B8	01	00	00	00	04	00	00	° 8 ,
15F5395020	00	00	00	00	00	00	00	00	04	00	00	00	D4	9A	03	00	ô!
15F5395030	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	,
15F5395040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
15F5395050	7E	DB	BF	86	E3	30	CC	01	7E	DB	BF	86	E3	30	CC	01	~Û¿!ãoi~Û¿!ãoi
15F5395060	7E	DB	BF	86	E3	30	CC	01	7E	DB	BF	86	E3	30	CC	01	~Û¿!ãoi~Û¿!ãoi
15F5395070	20	04	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
15F5395080	00	00	00	00	38	05	00	00	00	00	00	00	00	00	00	00	8
15F5395090	A0	40	90	DD	00	00	00	00	30	00	00	00	70	00	00	00	@ Ý 0 p
15F53950A0	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00	R
15F53950B0	43	00	00	00	00	00	03	00	7E	DB	BF	86	E3	30	CC	01	C ~Û¿!ãoi
15F53950C0	7E	DB	BF	86	E3	30	CC	01	7E	DB	BF	86	E3	30	CC	01	~Û¿!ãoi~Û¿!ãoi
15F53950D0	7E	DB	BF	86	E3	30	CC	01	00	00	00	00	00	00	00	00	~Û¿!ãoi
15F53950E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
15F53950F0	08	03	6E	00	6F	00	74	00	65	00	2E	00	65	00	78	00	note.exe
15F5395100	65	00	00	00	00	00	00	00	80	00	00	00	18	00	00	00	e !
15F5395110	00	00	18	00	00	00	01	00	00	00	00	00	18	00	00	00	
15F5395120	C0	00	00	00	90	00	00	00	00	00	00	00	00	00	03	00	À
15F5395130	74	00	00	00	18	00	00	00	0C	00	00	A0	6C	00	00	00	t l
15F5395140	2C	00	34	00	00	00	2C	00	00	00	00	00	43	00	3A	00	, 4 , C :
15F5395150	5C	00	57	00	69	00	6E	00	64	00	6F	00	77	00	73	00	\ Windows
15F5395160	5C	00	6E	00	6F	00	74	00	65	00	70	00	61	00	64	00	\ notepad
15F5395170	2E	00	65	00	78	00	65	00	5C	00	3F	00	3F	00	5C	00	.exe\??\
15F5395180	43	00	3A	00	5C	00	57	00	69	00	6E	00	64	00	6F	00	C:\Windo
15F5395190	77	00	73	00	5C	00	6E	00	6F	00	74	00	65	00	70	00	ws\notep
15F53951A0	61	00	64	00	2E	00	65	00	78	00	65	00	00	00	00	00	ad.exe
15F53951B0	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ÿÿÿÿÿG

Symbolic links, Hard links and Junctions (4/12)

- 폴더에 대한 심볼릭 링크 생성 <SYMLINKD>
 - `mklink /d "%USERPROFILE%\Documents\symdir" "%USERPROFILE%\Favorites"`
 - 네트워크 폴더에 대해서도 링크 가능
 - 속성 ID 0xC0의 \$REPARSE_POINT를 이용하여 심볼릭 링크 관리

\Users\pr0neer\Documents\symdir							
Filename ^-	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
Reparse Point -->		0 bytes				P	236310

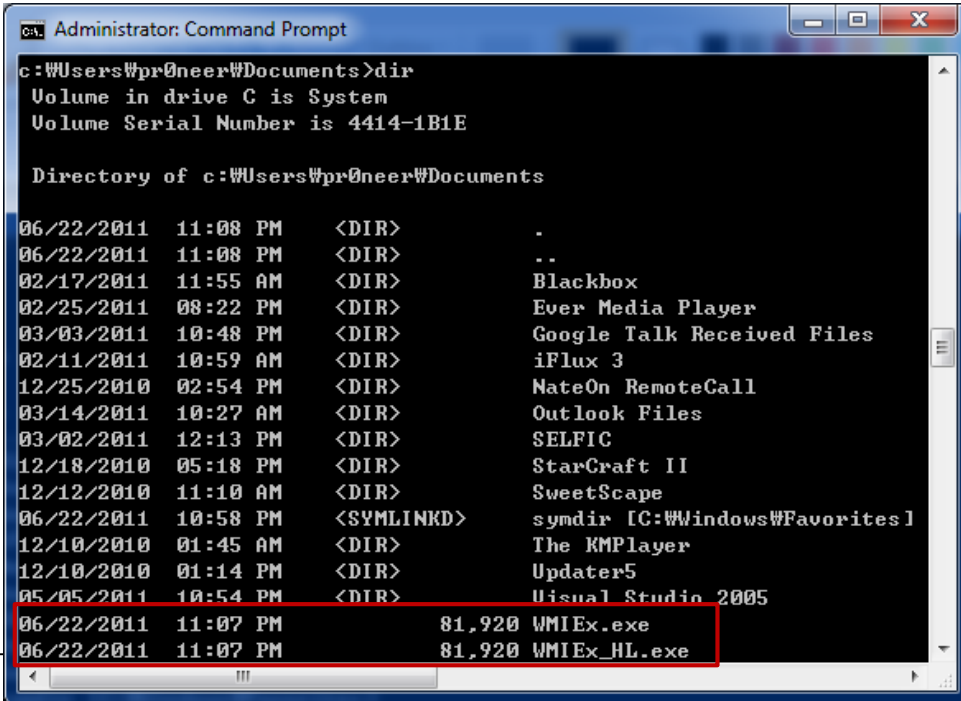
```
Administrator: Command Prompt
c:\Users\pr0neer\Documents>dir
Volume in drive C is System
Volume Serial Number is 4414-1B1E

Directory of c:\Users\pr0neer\Documents

06/22/2011  10:58 PM    <DIR>          .
06/22/2011  10:58 PM    <DIR>          ..
02/17/2011  11:55 AM    <DIR>          Blackbox
02/25/2011  08:22 PM    <DIR>          Ever Media Player
03/03/2011  10:48 PM    <DIR>          Google Talk Received Files
02/11/2011  10:59 AM    <DIR>          iFlux 3
12/25/2010  02:54 PM    <DIR>          NateOn RemoteCall
06/22/2011  10:51 PM    <SYMLINK>       note.exe [C:\Windows\notepad.exe]
03/14/2011  10:27 AM    <DIR>          Outlook Files
03/02/2011  12:13 PM    <DIR>          SELFIC
12/18/2010  05:18 PM    <DIR>          StarCraft II
12/12/2010  11:10 AM    <DIR>          SweetScape
06/22/2011  10:58 PM    <SYMLINKD>     symdir [C:\Windows\Favorites]
12/10/2010  01:45 AM    <DIR>          The KMPlayer
```


Symbolic links, Hard links and Junctions (5/12)

- 파일에 대한 하드 링크 생성
 - `mklink /h "%USERPROFILE%\Documents\WMIEx_HL.exe" "%USERPROFILE%\Documents\WMIEx.exe"`
 - 복사본을 생성하여 둘 중 어느 것을 수정해도 두 파일에 모두 반영
 - 둘 중 하나가 삭제되어도 상관 없음
 - 두 파일 모두 하나의 MFT 엔트리에 연결



```
Administrator: Command Prompt
c:\Users\wpr0neer\Documents>dir
Volume in drive C is System
Volume Serial Number is 4414-1B1E

Directory of c:\Users\wpr0neer\Documents

06/22/2011  11:08 PM    <DIR>          .
06/22/2011  11:08 PM    <DIR>          ..
02/17/2011  11:55 AM    <DIR>          Blackbox
02/25/2011  08:22 PM    <DIR>          Ever Media Player
03/03/2011  10:48 PM    <DIR>          Google Talk Received Files
02/11/2011  10:59 AM    <DIR>          iFlux 3
12/25/2010  02:54 PM    <DIR>          NateOn RemoteCall
03/14/2011  10:27 AM    <DIR>          Outlook Files
03/02/2011  12:13 PM    <DIR>          SELFIC
12/18/2010  05:18 PM    <DIR>          StarCraft II
12/12/2010  11:10 AM    <DIR>          SweetScape
06/22/2011  10:58 PM    <SYMLINKD>      syndir [C:\Windows\Favorites]
12/10/2010  01:45 AM    <DIR>          The KMPlayer
12/10/2010  01:14 PM    <DIR>          Updater5
05/05/2011  10:54 PM    <DIR>          Visual Studio 2005
06/22/2011  11:07 PM             81,920 WMIEx.exe
06/22/2011  11:07 PM             81,920 WMIEx_HL.exe
```

Symbolic links, Hard links and Junctions (6/12)

- 폴더에 대한 폴더 교차점 생성 <JUNCTION>
 - `mklink /j "%USERPROFILE%\Documents\symdir" "%USERPROFILE%\Documents\Favorites"`
 - 심볼릭 링크와 거의 유사 (폴더와 네트워크 경로는 링크할 수 없음)

\\Users\pr0neer\Documents\symdir							
Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
Reparse Point --> \\??\C:\Users\pr0neer\Favorites		0 bytes				P	235775

```
Administrator: Command Prompt
c:\Users\pr0neer\Documents>dir
Volume in drive C is System
Volume Serial Number is 4414-1B1E

Directory of c:\Users\pr0neer\Documents

06/22/2011  11:15 PM    <DIR>          .
06/22/2011  11:15 PM    <DIR>          ..
02/17/2011  11:55 AM    <DIR>          Blackbox
02/25/2011  08:22 PM    <DIR>          Ever Media Player
03/03/2011  10:48 PM    <DIR>          Google Talk Received Files
02/11/2011  10:59 AM    <DIR>          iFlux 3
12/25/2010  02:54 PM    <DIR>          NateOn RemoteCall
03/14/2011  10:27 AM    <DIR>          Outlook Files
03/02/2011  12:13 PM    <DIR>          SELFIC
12/18/2010  05:18 PM    <DIR>          StarCraft II
12/12/2010  11:10 AM    <DIR>          SweetScane
06/22/2011  11:15 PM    <JUNCTION>     symdir [C:\Users\pr0neer\Favorites]
12/10/2010  01:45 AM    <DIR>          The KMPlayer
12/10/2010  01:14 PM    <DIR>          Updater5
05/05/2011  10:54 PM    <DIR>          Visual Studio 2005
```

Symbolic links, Hard links and Junctions (7/12)

- 무한 반복 폴더 생성

```
#> md "C:\testdir"
```

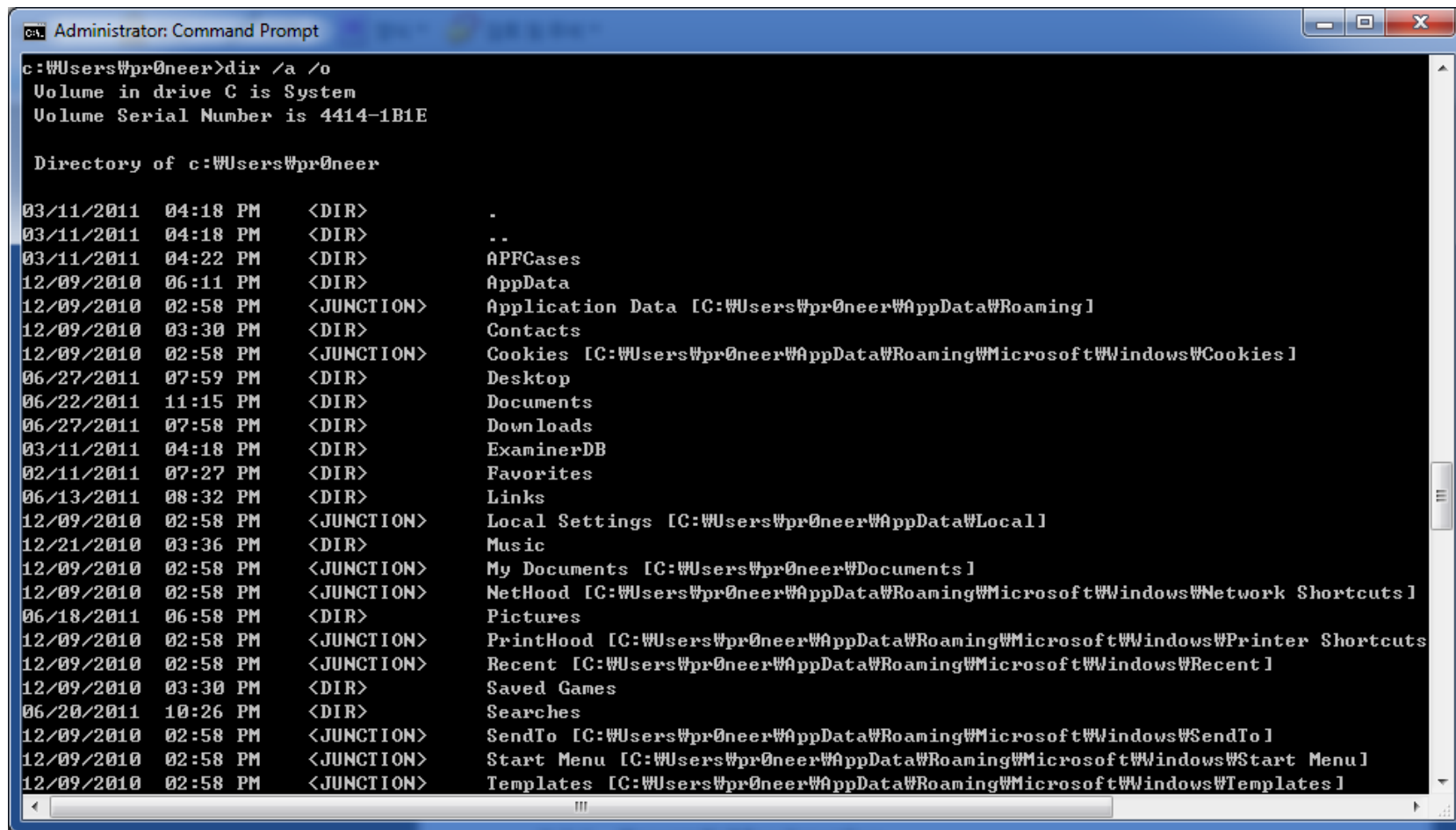
```
#> mklink /d "C:\testdir\testdir" "C:\testdir"
```

```
#> md "C:\testdir"
```

```
#> mklink /j "C:\testdir\testdir" "C:\testdir"
```

Symbolic links, Hard links and Junctions (8/12)

- 폴더 구조 변화에 따른 심볼릭 링크와 교차점 사용



```
Administrator: Command Prompt
c:\Users\wpr0neer>dir /a /o
Volume in drive C is System
Volume Serial Number is 4414-1B1E

Directory of c:\Users\wpr0neer

03/11/2011  04:18 PM    <DIR>          .
03/11/2011  04:18 PM    <DIR>          ..
03/11/2011  04:22 PM    <DIR>          APPCases
12/09/2010  06:11 PM    <DIR>          AppData
12/09/2010  02:58 PM    <JUNCTION>     Application Data [C:\Users\wpr0neer\AppData\Roaming]
12/09/2010  03:30 PM    <DIR>          Contacts
12/09/2010  02:58 PM    <JUNCTION>     Cookies [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\Cookies]
06/27/2011  07:59 PM    <DIR>          Desktop
06/22/2011  11:15 PM    <DIR>          Documents
06/27/2011  07:58 PM    <DIR>          Downloads
03/11/2011  04:18 PM    <DIR>          ExaminerDB
02/11/2011  07:27 PM    <DIR>          Favorites
06/13/2011  08:32 PM    <DIR>          Links
12/09/2010  02:58 PM    <JUNCTION>     Local Settings [C:\Users\wpr0neer\AppData\Local]
12/21/2010  03:36 PM    <DIR>          Music
12/09/2010  02:58 PM    <JUNCTION>     My Documents [C:\Users\wpr0neer\Documents]
12/09/2010  02:58 PM    <JUNCTION>     NetHood [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
06/18/2011  06:58 PM    <DIR>          Pictures
12/09/2010  02:58 PM    <JUNCTION>     PrintHood [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
12/09/2010  02:58 PM    <JUNCTION>     Recent [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\Recent]
12/09/2010  03:30 PM    <DIR>          Saved Games
06/20/2011  10:26 PM    <DIR>          Searches
12/09/2010  02:58 PM    <JUNCTION>     SendTo [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\SendTo]
12/09/2010  02:58 PM    <JUNCTION>     Start Menu [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\Start Menu]
12/09/2010  02:58 PM    <JUNCTION>     Templates [C:\Users\wpr0neer\AppData\Roaming\Microsoft\Windows\Templates]
```

Symbolic links, Hard links and Junctions (9/12)

- 폴더 구조 변화에 따른 심볼릭 링크와 교차점 사용 (사용자 폴더)

2K/XP 폴더	Vista/7 폴더	Junction/ Symlink
C:\Documents and Settings\ 	C:\Users\ 	Junction
C:\Documents and Settings\ <username>\my documents\<br=""></username>\my>	C:\Users\ <username>\documents< td=""><td>Junction</td></username>\documents<>	Junction
C:\Documents and Settings\ <username>\my documents\my="" music<="" td=""><td>C:\Users\<username>\music< td=""><td>Junction</td></username>\music<></td></username>\my>	C:\Users\ <username>\music< td=""><td>Junction</td></username>\music<>	Junction
C:\Documents and Settings\ <username>\my documents\my="" picture<="" td=""><td>C:\Users\<username>\pictures< td=""><td>Junction</td></username>\pictures<></td></username>\my>	C:\Users\ <username>\pictures< td=""><td>Junction</td></username>\pictures<>	Junction
C:\Documents and Settings\ <username>\my documents\my="" td="" videos<=""><td>C:\Users\<username>\videos< td=""><td>Junction</td></username>\videos<></td></username>\my>	C:\Users\ <username>\videos< td=""><td>Junction</td></username>\videos<>	Junction

Symbolic links, Hard links and Junctions (10/12)

- 폴더 구조 변화에 따른 심볼릭 링크와 교차점 사용 (응용데이터 폴더)

2K/XP 폴더	Vista/7 폴더	Junction/ Symlink
C:\Documents and Settings\<username>\Local Settings	C:\Users\<username>\AppData\Local	Junction
C:\Documents and Settings\<username>\Local Settings\Application Data	C:\Users\<username>\AppData\Local	Junction
C:\Documents and Settings\<username>\Local Settings\Temporary Internet Files	C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files	Junction
C:\Documents and Settings\<username>\Local Settings\History	C:\Users\<username>\AppData\Local\Microsoft\Windows\History	Junction
C:\Documents and Settings\<username>\Application Data\	C:\Users\<username>\AppData\Roaming	Junction

Symbolic links, Hard links and Junctions (11/12)

- 폴더 구조 변화에 따른 심볼릭 링크와 교차점 사용 (사용자 OS 설정 폴더)

2K/XP 폴더	Vista/7 폴더	Junction/ Symlink
C:\Documents and Settings\<username>\Cookies\	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies	Junction
C:\Documents and Settings\<username>\Recent\	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent	Junction
C:\Documents and Settings\<username>\Nethood\	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Network Shortcuts	Junction
C:\Documents and Settings\<username>\Printhood\	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Printer Shortcuts	Junction
C:\Documents and Settings\<username>\Send To\	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\SendTo	Junction
C:\Documents and Settings\<username>\Start Menu	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu	Junction
C:\Documents and Settings\<username>\Templates\	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Templates	Junction

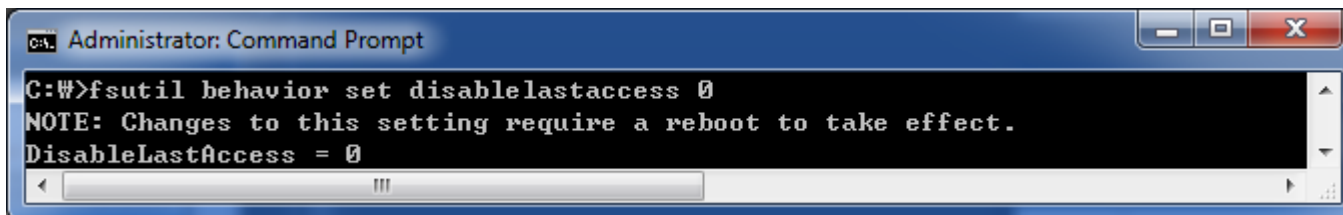
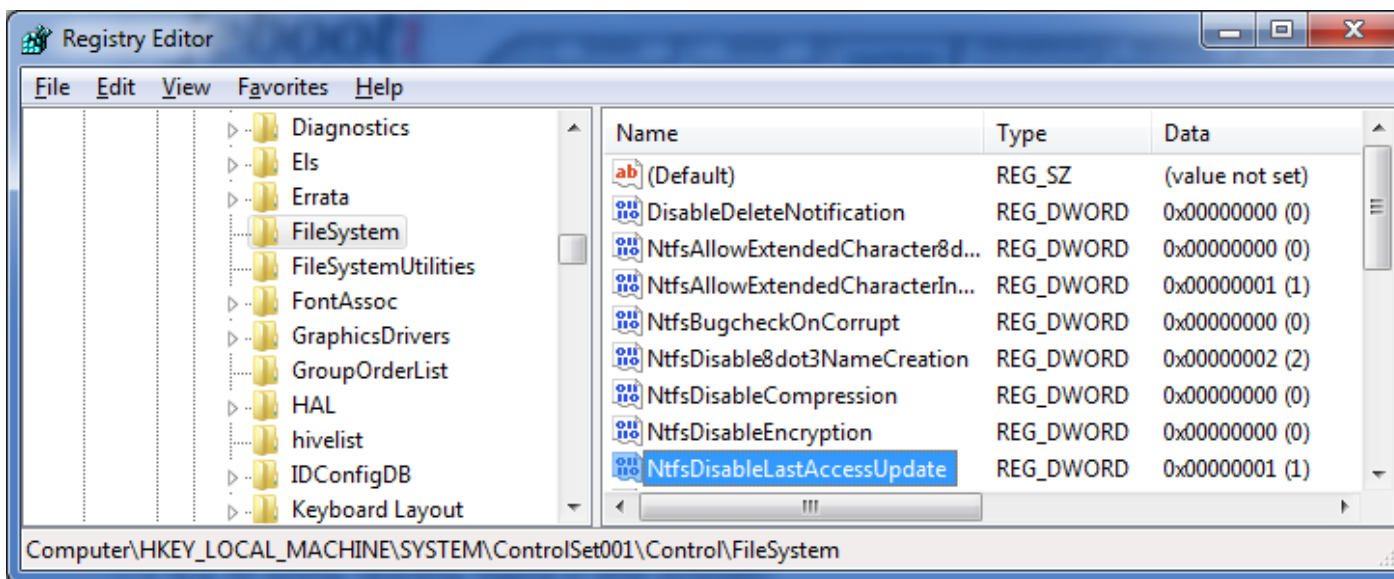
Symbolic links, Hard links and Junctions (12/12)

- 폴더 구조 변화에 따른 심볼릭 링크와 교차점 사용 (사용자 기본 폴더)

2K/XP 폴더	Vista/7 폴더	Junction/ Symlink
C:\Documents and Settings\All Users	C:\ProgramData	Symlink
C:\Documents and Settings\Default User	C:\Users\Dfault	Junction

Update Last Access Date

- **HKLM\SYSTEM\ControlSet00X\Control\FileSystem\NtfsDisableLastAccessUpdate**
 - Vista, Windows 2008 / 2008 R2, Windows 7 에서 모두 성능 향상을 목적으로 기본 설정(1)됨



Transactional NTFS (TxF)

- **\$Extend\$RmMetadata\$**

- Vista 부터 사용됨
- NTFS 파일시스템에서 파일 처리는 트랜잭션(Transaction) 단위로 수행
- 파일시스템 메타데이터(MFT 엔트리)와 관련된 트랜잭션 정보 저장
- \$Extend\$RmMetadata\$TxfLog\$Tops:\$T 파일은 XML 형식으로 정보 저장

\$Extend\$RmMetadata							
Filename ^-	Ext.	Size	Created	Modified	Accessed	Attr.	ID
...							
<input type="checkbox"/> \$Txf		16.0 KB	12/09/2...	06/22/2...	06/22/20...	SH	30
<input type="checkbox"/> \$TxfLog		4.1 KB	12/09/2...	12/09/2...	12/09/20...	SH	29
<input type="checkbox"/> \$Repair		0 bytes	12/09/2...	12/09/2...	12/09/20...	SHA	28
<input type="checkbox"/> \$Repair:\$Config		8 bytes	12/09/2...	12/09/2...	12/09/20...	(ADS)	28
<input type="checkbox"/> \$Txf:\$TXF_DATA		56 bytes	12/09/2...	06/22/2...	06/22/20...	(\$EFS)	30

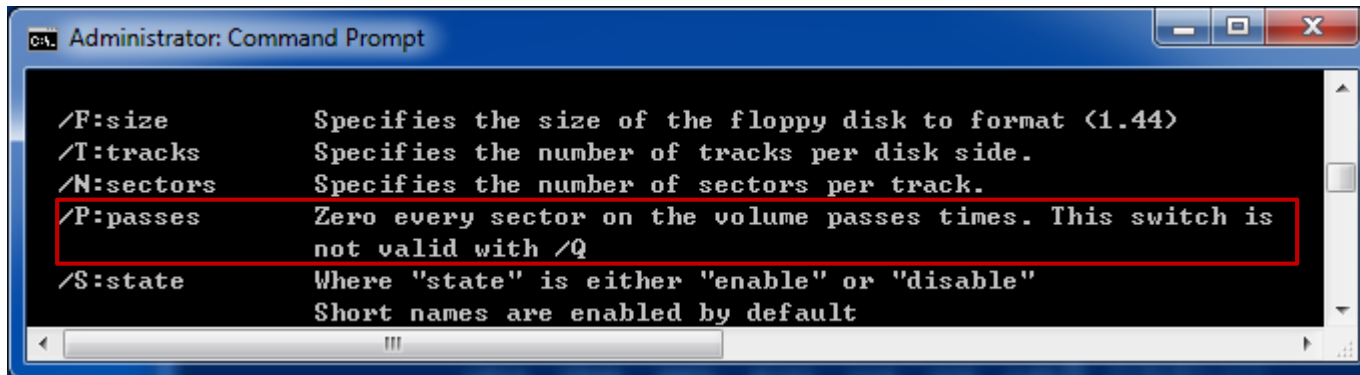
Volume Boot Record sector

- 63 → 2048

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Access ▼
0000100000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	NTFS
0000100010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00	ø ? ý
0000100020	00	00	00	00	80	00	80	00	FF	1F	03	00	00	00	00	00	! ! ý
0000100030	55	21	00	00	00	00	00	00	02	00	00	00	00	00	00	00	U!
0000100040	F6	00	00	00	01	00	00	00	8F	B8	5B	60	E3	5B	60	66	ö , [`ã [`f
0000100050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	ú3À!Đ% úhÀ
0000100060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	hf Ë! f > N
0000100070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu 'A»@UÍ r ú
0000100080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uau +Á u éÝ !i
0000100090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	h 'H! !ô Í
00001000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	!!Ä !X rá; uÛf
00001000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	Á. Z3Û! +È
00001000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fÿ !Äÿ è
00001000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	K +Èwi, »Í f#Àu-
00001000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f ûTCPAu\$ û r
00001000F0	68	07	BB	16	68	70	0E	16	68	09	00	66	53	66	53	66	h » hp h fSfSf

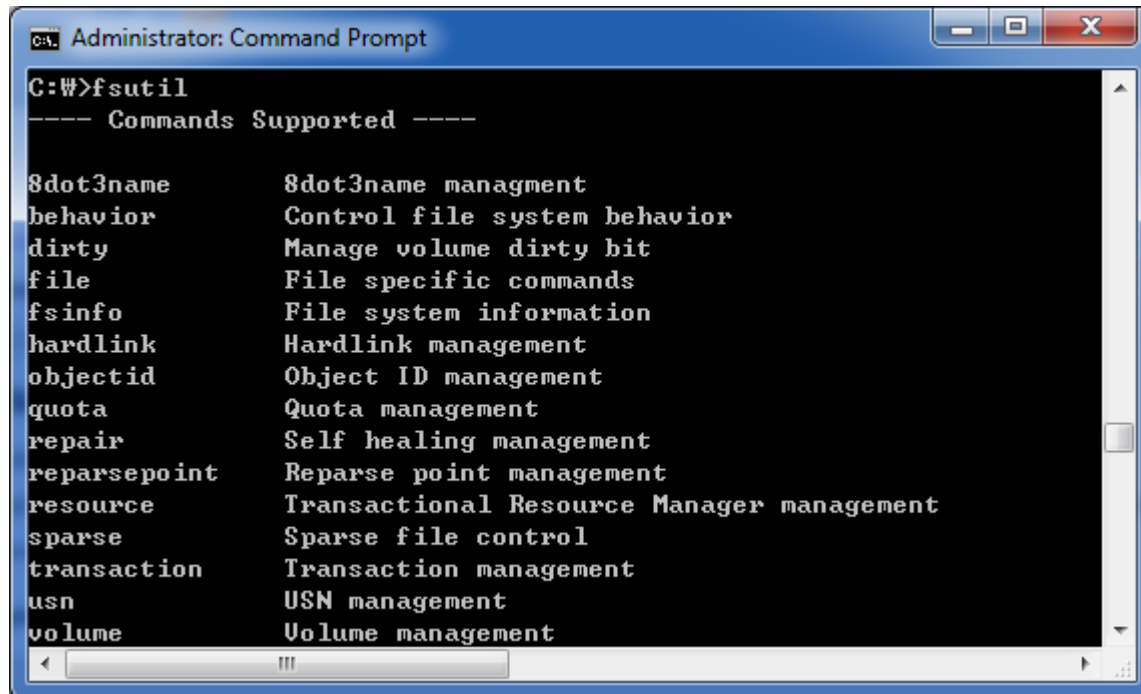
Additional Command

- **Format** ([http://technet.microsoft.com/en-us/library/cc730730\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc730730(WS.10).aspx))



Additional Command

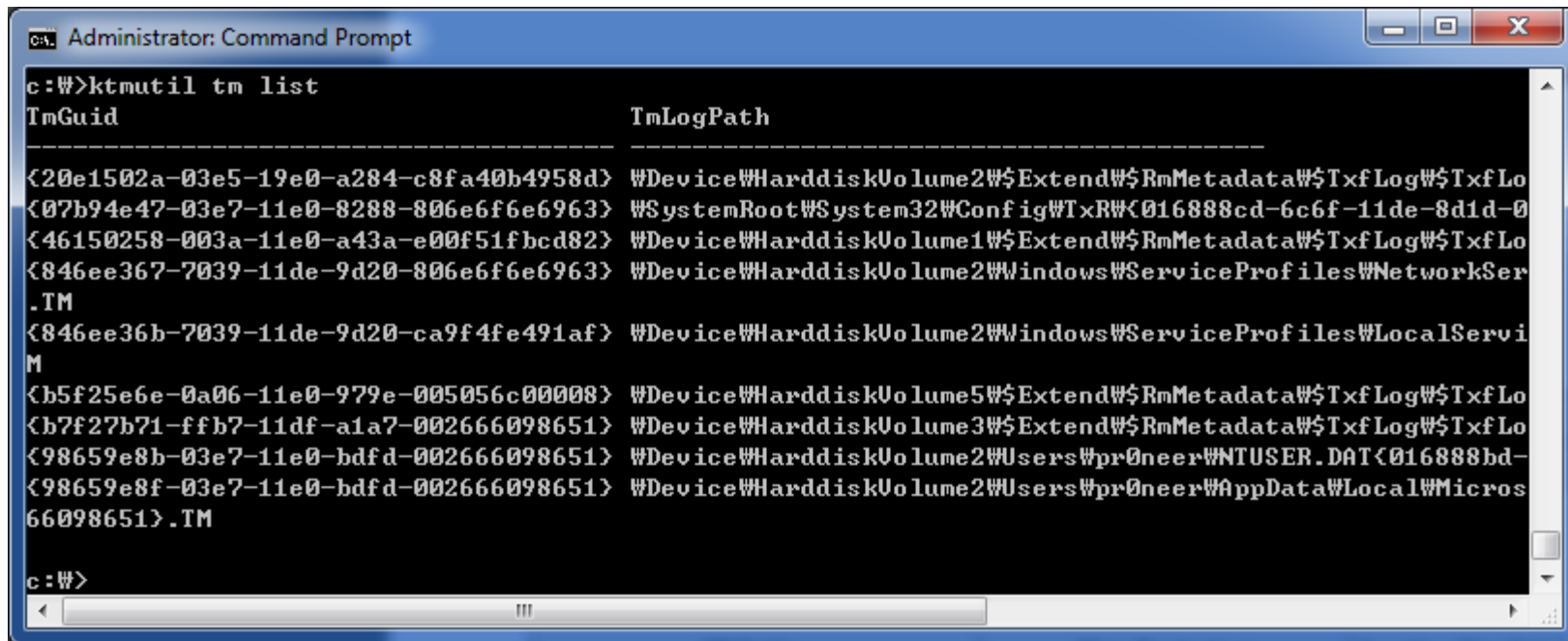
- FSUtil ([http://technet.microsoft.com/en-us/library/cc753059\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753059(WS.10).aspx))



```
Administrator: Command Prompt
C:\W>fsutil
---- Commands Supported ----
8dot3name      8dot3name managment
behavior       Control file system behavior
dirty          Manage volume dirty bit
file           File specific commands
fsinfo         File system information
hardlink       Hardlink management
objectid       Object ID management
quota          Quota management
repair         Self healing management
reparsepoint   Reparse point management
resource       Transactional Resource Manager management
sparse         Sparse file control
transaction    Transaction management
usn            USN management
volume         Volume management
```

Additional Command

- KTMUtil ([http://technet.microsoft.com/en-us/library/cc753661\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753661(WS.10).aspx))



```
Administrator: Command Prompt
c:\>ktmutil tm list
TmGuid                                TmLogPath
-----
<20e1502a-03e5-19e0-a284-c8fa40b4958d> WDevice\HarddiskVolume2\Extend\RmMetadata\TxfLog\TxfLo
<07b94e47-03e7-11e0-8288-806e6f6e6963> WSystemRoot\System32\Config\TxRW\<016888cd-6c6f-11de-8d1d-0
<46150258-003a-11e0-a43a-e00f51fbcd82> WDevice\HarddiskVolume1\Extend\RmMetadata\TxfLog\TxfLo
<846ee367-7039-11de-9d20-806e6f6e6963> WDevice\HarddiskVolume2\Windows\ServiceProfiles\NetworkSer
.TM
<846ee36b-7039-11de-9d20-ca9f4fe491af> WDevice\HarddiskVolume2\Windows\ServiceProfiles\LocalServi
M
<b5f25e6e-0a06-11e0-979e-005056c00008> WDevice\HarddiskVolume5\Extend\RmMetadata\TxfLog\TxfLo
<b7f27b71-ffb7-11df-a1a7-002666098651> WDevice\HarddiskVolume3\Extend\RmMetadata\TxfLog\TxfLo
<98659e8b-03e7-11e0-bdfd-002666098651> WDevice\HarddiskVolume2\Users\wpr0neer\NTUSER.DAT\<016888bd-
<98659e8f-03e7-11e0-bdfd-002666098651> WDevice\HarddiskVolume2\Users\wpr0neer\AppData\Local\Micros
66098651>.TM
c:\>
```

