

윈도우 7 폴더 구조



JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com


1. 사용자 프로파일 폴더
2. 휴지통 폴더
3. 최근 접근 문서와 시작 메뉴 폴더
4. 바탕화면, 내 문서, 내 음악, 내 그림, 내 동영상 폴더
5. 보내기 폴더
6. 임시 폴더
7. 즐겨찾기, 쿠키, 히스토리, 임시 인터넷 파일 폴더
8. Local/LocalLow/Roaming 폴더
9. 추가된 폴더 (Downloads, Contacts, Links, Saved Games, Searches)


윈도우 7 폴더 구조

사용자 프로파일 폴더

윈도우 NT	윈도우 XP	윈도우 Vista/7
C:\WINNT\Profiles	C:\Documents and Settings\<username>	C:\Users\<username>
-	C:\Documents and Settings\Default User	C:\Users\Default
-	C:\Documents and Settings\All Users	C:\Program Data

- 윈도우 9x 시절에는 사용자 프로파일 폴더가 존재하지 않음
- 윈도우 Vista/7으로 넘어오면서 "Users" 라는 폴더로 이름 변경
- 이전 버전과의 호환성을 위해 \$REPARSE_POINT 속성을 사용하여 폴더 교차점(Junction) 생성

\Documents and Settings							
Filename ^	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
 Reparse Point --> /??/C:/Users		0 bytes				P	13752

\Users\All Users							
Filename ^	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
 Reparse Point -->		0 bytes				P	16375

윈도우 7 폴더 구조

사용자 프로파일 폴더

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00C0D6E000	46	49	4C	45	30	00	03	00	33	86	0E	08	00	00	00	00	FILE0 3I
00C0D6E010	01	00	02	00	38	00	03	00	40	02	00	00	00	04	00	00	8 @
00C0D6E020	00	00	00	00	00	00	00	00	05	00	00	00	B8	35	00	00	,5
00C0D6E030	06	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	,
00C0D6E040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
00C0D6E050	F2	90	72	30	41	04	CA	01	F2	90	72	30	41	04	CA	01	ò r0A Ê ò r0A Ê
00C0D6E060	F8	88	B6	94	F3	97	CB	01	F2	90	72	30	41	04	CA	01	ø!¶!ó!Ë ò r0A Ê
00C0D6E070	06	24	00	00	00	00	00	00	00	00	00	00	00	00	00	00	\$
00C0D6E080	00	00	00	00	C1	01	00	00	00	00	00	00	00	00	00	00	Á
00C0D6E090	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	O p
00C0D6E0A0	00	00	00	00	00	00	03	00	52	00	00	00	18	00	01	00	R
00C0D6E0B0	05	00	00	00	00	00	05	00	DF	67	C5	95	F2	97	CB	01	BgÁ!ò!Ë
00C0D6E0C0	DF	67	C5	95	F2	97	CB	01	DF	67	C5	95	F2	97	CB	01	BgÁ!ò!Ë BgÁ!ò!Ë
00C0D6E0D0	DF	67	C5	95	F2	97	CB	01	00	00	00	00	00	00	00	00	BgÁ!ò!Ë
00C0D6E0E0	00	00	00	00	00	00	00	00	00	00	00	10	00	00	00	00	
00C0D6E0F0	08	02	44	00	4F	00	43	00	55	00	4D	00	45	00	7E	00	D O C U M E ~
00C0D6E100	31	00	73	00	20	00	61	00	30	00	00	00	88	00	00	00	1 s a 0 I
00C0D6E110	00	00	00	00	00	00	02	00	6E	00	00	00	18	00	01	00	n
00C0D6E120	05	00	00	00	00	00	05	00	DF	67	C5	95	F2	97	CB	01	BgÁ!ò!Ë
00C0D6E130	DF	67	C5	95	F2	97	CB	01	DF	67	C5	95	F2	97	CB	01	BgÁ!ò!Ë BgÁ!ò!Ë
00C0D6E140	DF	67	C5	95	F2	97	CB	01	00	00	00	00	00	00	00	00	BgÁ!ò!Ë
00C0D6E150	00	00	00	00	00	00	00	00	00	00	00	10	00	00	00	00	
00C0D6E160	16	01	44	00	6F	00	63	00	75	00	6D	00	65	00	6E	00	D o c u m e n
00C0D6E170	74	00	73	00	20	00	61	00	6E	00	64	00	20	00	53	00	t s a n d S
00C0D6E180	65	00	74	00	74	00	69	00	6E	00	67	00	73	00	00	00	e t t i n g s
00C0D6E190	90	00	00	00	50	00	00	00	00	04	18	00	00	00	01	00	P
00C0D6E1A0	30	00	00	00	20	00	00	00	24	00	49	00	33	00	30	00	0 \$ I 3 0
00C0D6E1B0	30	00	00	00	01	00	00	00	00	10	00	00	01	00	00	00	0
00C0D6E1C0	10	00	00	00	20	00	00	00	20	00	00	00	00	00	00	00	
00C0D6E1D0	00	00	00	00	00	00	00	00	10	00	00	00	02	00	00	00	
00C0D6E1E0	C0	00	00	00	58	00	00	00	00	00	00	00	00	00	04	00	À X
00C0D6E1F0	3C	00	00	00	18	00	00	00	03	00	00	A0	34	00	06	00	< 4
00C0D6E200	00	00	18	00	1A	00	10	00	5C	00	3F	00	3F	00	5C	00	\ ? ? \
00C0D6E210	43	00	3A	00	5C	00	55	00	73	00	65	00	72	00	73	00	C : \ U s e r s
00C0D6E220	00	00	43	00	3A	00	5C	00	55	00	73	00	65	00	72	00	C : \ U s e r
00C0D6E230	73	00	00	00	00	00	00	00	FF	FF	FF	FF	82	79	47	11	s yyyylG

→ \$FILE_NAME

→ \$REPARSE_POINT

휴지통 폴더

윈도우 NT/2K/XP	윈도우 Vista/7
<volume>:\Recycler\<user sid>	<volume>:\\$Recycle.Bin\<user sid>

- 윈도우 Vista/7으로 넘어오면서 휴지통 폴더가 변경
 - Recycler → Recycle.Bin

윈도우 7 폴더 구조

최근 접근 문서와 시작 메뉴 폴더

윈도우 2K/XP	윈도우 Vista/7
C:\Documents and Settings\<username>\Recent	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent
C:\Documents and Settings\Start Menu	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu

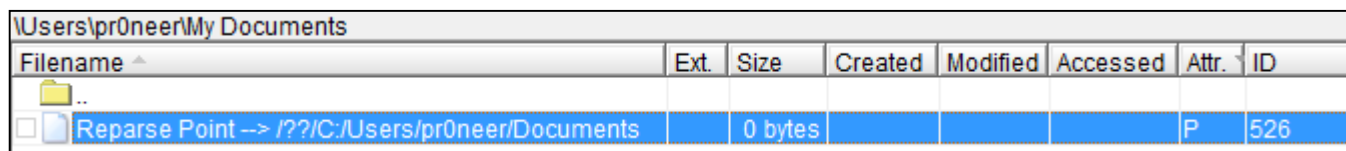
- 최근 접근 문서에 대한 링크 파일 정보 저장
- 최근 접근 순서는 레지스트리를 통해 관리
 - **HKUW{USER}WSOFTWAREWMicrosoftWCurrentVersionWExplorerWRecentDocs**
- 시작 메뉴 또한 각 프로그램을 링크 파일로 관리

바탕화면, 내 문서, 내 음악, 내 그림 폴더

항목	윈도우 2K/XP	윈도우 Vista/7
바탕화면	C:\Documents and Settings\<username>\Desktop	C:\Users\<username>\Desktop
내 문서	C:\Documents and Settings\<username>\My Documents	C:\Users\<username>\Documents
내 음악	C:\Documents and Settings\<username>\My Music	C:\Users\<username>\Music
내 그림	C:\Documents and Settings\<username>\My Pictures	C:\Users\<username>\Pictures
내 동영상	C:\Documents and Settings\<username>\My Videos	C:\Users\<username>\Videos

- 바탕화면, 내 문서 등의 폴더에는 사용자가 자주 사용하는 파일이 존재할 가능성이 높음
- 이전 버전과의 호환성을 위해 \$REPARSE_POINT 속성을 사용하여 폴더 교차점(Junction) 생성

- **My Documents → Documents**



The screenshot shows a Windows Explorer window with the address bar set to 'Users\pr0neer\My Documents'. The file list contains a single entry: a folder icon followed by 'Reparse Point --> /??/C:/Users/pr0neer/Documents'. The columns are labeled: Filename, Ext., Size, Created, Modified, Accessed, Attr., and ID. The 'Size' column shows '0 bytes' and the 'Attr.' column shows 'P'.

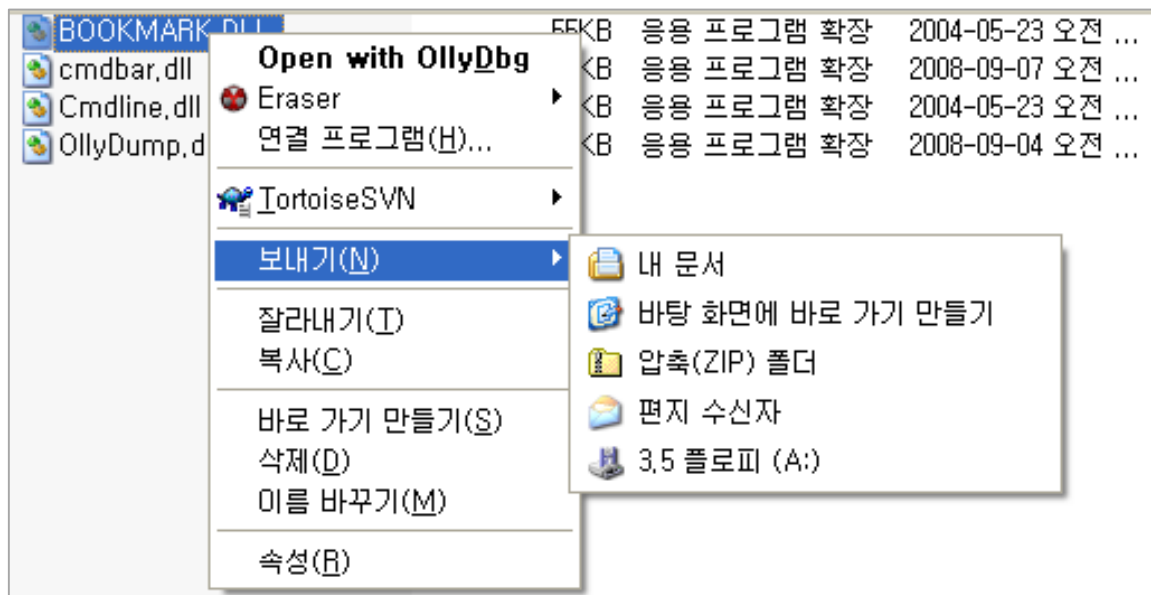
Users\pr0neer\My Documents							
Filename ^	Ext.	Size	Created	Modified	Accessed	Attr.	ID
..							
Reparse Point --> /??/C:/Users/pr0neer/Documents		0 bytes				P	526

윈도우 7 폴더 구조

보내기 폴더

윈도우 2K/XP	윈도우 Vista/7
C:\Documents and Settings\ <username>\Send To</username>	C:\Users\ <username>\AppData\Roaming\Microsoft\Windows\Send To</username>

- 사용자 편의성을 위해 반복적인 작업을 등록하여 사용
- 파일에 대한 특정 행위를 즉시 수행



윈도우 7 폴더 구조

임시 폴더

윈도우 2K/XP	윈도우 Vista/7
C:\Documents and Settings\<username>\Local Settings\Temp	C:\Users\<username>\AppData\Local\Temp

- 프로그램 설치/제거/사용 시 임시 파일 저장 등의 용도로 사용
- IE를 통해 파일 다운로드 시 임시적인 저장 공간

\\Users\pr0neer\AppData\Local\Temp							
Filename ^-^	Ext.	Size	Created	Modified	Accessed	Attr.	ID
...							
{7148F0A8-6813-11D6-A77B-00B0D0142180}		48 byt...	03/16/2...	03/16/2...	03/16/20...		57849
{972DB38C-ABA1-44A9-884C-079FFA02E23A}		4.1 KB	03/31/2...	03/31/2...	03/31/20...		192012
~nsu.tmp	tmp	272 by...	06/04/2...	06/06/2...	06/06/20...		247821
16FB.dir	dir	288 by...	05/21/2...	05/21/2...	05/21/20...		212885
5560.dir	dir	288 by...	05/06/2...	05/06/2...	05/06/20...		235721
A2F3.dir	dir	288 by...	06/10/2...	06/10/2...	06/10/20...		215518
Acrobat Distiller 8		48 byt...	06/04/2...	06/04/2...	06/04/20...		65867
Adobe		144 by...	03/16/2...	05/23/2...	05/23/20...		23819
ASP		136 by...	05/30/2...	05/30/2...	05/30/20...		243680
Cookies		152 by...	12/23/2...	12/23/2...	12/23/20...	SH	67645
D39B4B65_3692_4292_833F_2C81D15845EB		8.1 KB	03/31/2...	03/31/2...	03/31/20...		224464
E58E.dir	dir	288 by...	06/17/2...	06/17/2...	06/17/20...		237827
GomAudio		48 byt...	04/23/2...	06/15/2...	06/15/20...		163294
Google Talk		48 byt...	04/03/2...	04/03/2...	04/03/20...		213767
History		152 by...	12/23/2...	12/23/2...	12/23/20...	SH	67648
Hnc		144 by...	03/31/2...	03/31/2...	03/31/20...		224554

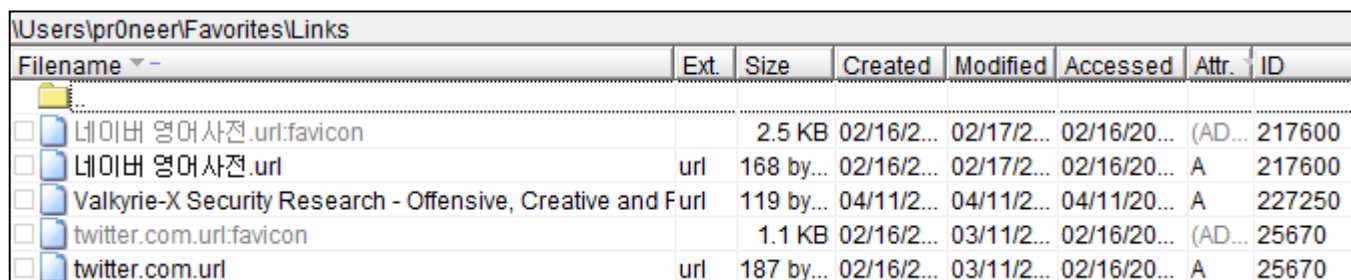
윈도우 7 폴더 구조

즐거찾기, 쿠키, 히스토리, 임시 인터넷 파일 폴더

항목	윈도우 2K/XP	윈도우 Vista/7
즐거찾기	C:\Documents and Settings\<username>\Favorites	C:\Users\<username>\Favorites
쿠키	C:\Documents and Settings\<username>\Cookies	C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies\[Low]
히스토리	C:\Documents and Settings\<username>\Local Settings\History	C:\Users\<username>\AppData\Local\Microsoft\Windows\History\[Low]
임시 파일	C:\Documents and Settings\<username>\Local Settings\Temporary Internet Files	C:\Users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\[Low]

- **즐거 찾기**

- IE의 즐겨찾기 정보를 URL Shortcut 파일로 저장, 파비콘(Favicon) 정보도 ADS(Alternated Data Stream)을 통해 저장



\\Users\pr0neer\Favorites\Links							
Filename	Ext	Size	Created	Modified	Accessed	Attr	ID
네이버 영어사전.url:favicon		2.5 KB	02/16/2...	02/17/2...	02/16/20...	(AD...	217600
네이버 영어사전.url	url	168 by...	02/16/2...	02/17/2...	02/16/20...	A	217600
Valkyrie-X Security Research - Offensive, Creative and Furl		119 by...	04/11/2...	04/11/2...	04/11/20...	A	227250
twitter.com.url:favicon		1.1 KB	02/16/2...	03/11/2...	02/16/20...	(AD...	25670
twitter.com.url	url	187 by...	02/16/2...	03/11/2...	02/16/20...	A	25670

- **쿠키**

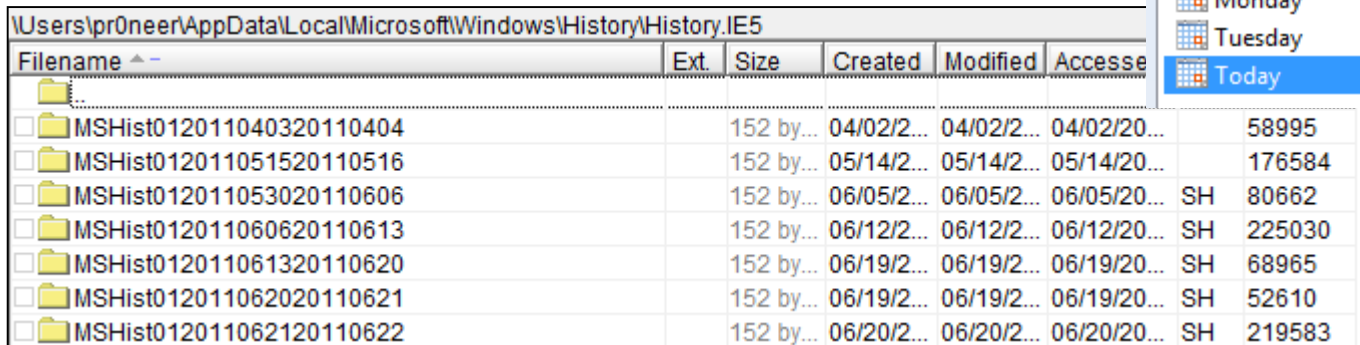
- 사이트 방문시 생성되는 쿠키 정보 저장

윈도우 7 폴더 구조

즐거찾기, 쿠키, 히스토리, 임시 인터넷 파일 폴더

- **히스토리**

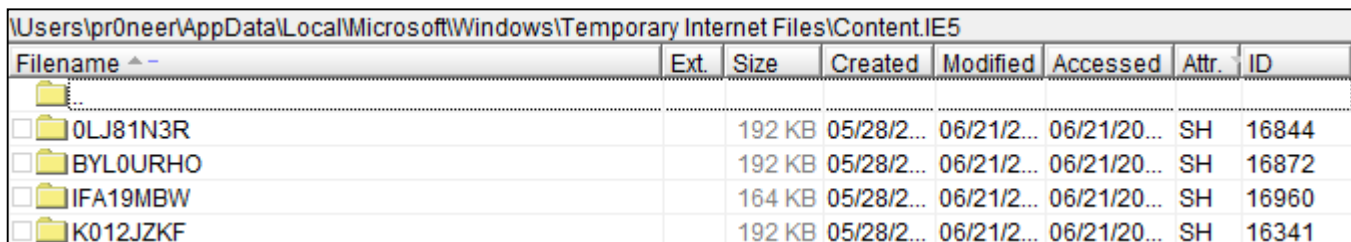
- History.IE5 폴더에 "MSHist"라는 접두어로 오늘, 2일전, 3일전, 지난 주 등의 정보 저장



Filename	Ext	Size	Created	Modified	Accessed	
MSHist012011040320110404		152 by...	04/02/2...	04/02/2...	04/02/20...	58995
MSHist012011051520110516		152 by...	05/14/2...	05/14/2...	05/14/20...	176584
MSHist012011053020110606		152 by...	06/05/2...	06/05/2...	06/05/20...	SH 80662
MSHist012011060620110613		152 by...	06/12/2...	06/12/2...	06/12/20...	SH 225030
MSHist012011061320110620		152 by...	06/19/2...	06/19/2...	06/19/20...	SH 68965
MSHist012011062020110621		152 by...	06/19/2...	06/19/2...	06/19/20...	SH 52610
MSHist012011062120110622		152 by...	06/20/2...	06/20/2...	06/20/20...	SH 219583

- **임시 인터넷 파일**

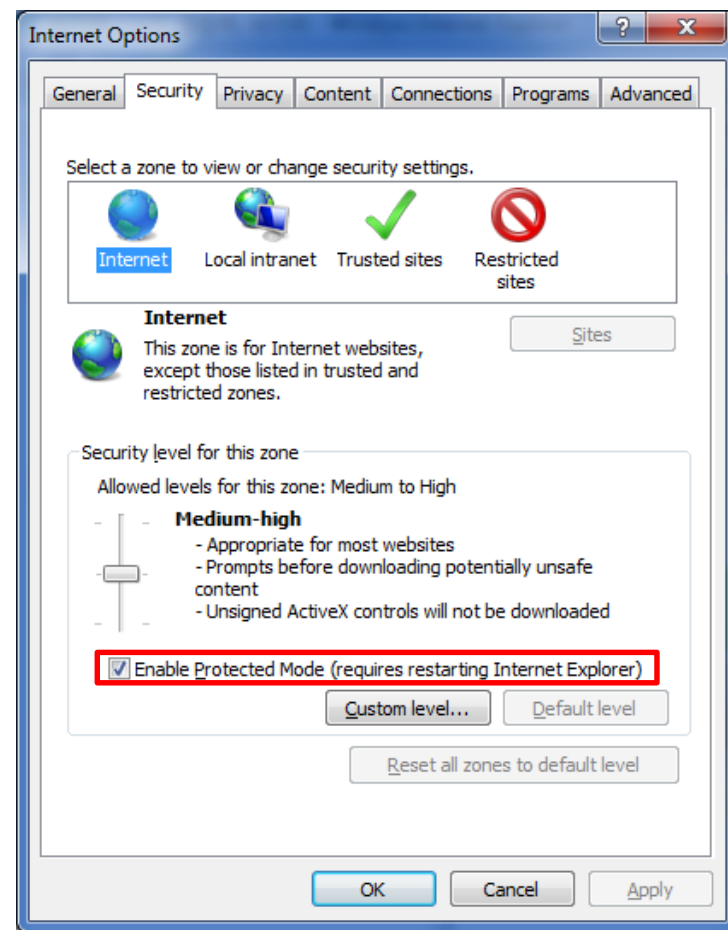
- Content.IE5 하위의 임의의 문자 폴더에 저장
- 사이트 방문 시 멀티미디어 콘텐츠를 캐시하여 재방문시 빠르게 로드



Filename	Ext	Size	Created	Modified	Accessed	Attr	ID
0LJ81N3R		192 KB	05/28/2...	06/21/2...	06/21/20...	SH	16844
BYL0URHO		192 KB	05/28/2...	06/21/2...	06/21/20...	SH	16872
IFA19MBW		164 KB	05/28/2...	06/21/2...	06/21/20...	SH	16960
K012JZKF		192 KB	05/28/2...	06/21/2...	06/21/20...	SH	16341

즐거찾기, 쿠키, 히스토리, 임시 인터넷 파일 폴더

- **Low 폴더**
 - IE7부터 추가된 보호 모드가 사용시 저장되는 폴더
 - Vista/7에서는 기본적으로 보호 모드 활성화
 - **Low Integrity Process**
 - 악의적인 공격자로부터 시스템을 보호하기 위해 IE 프로세스에게 매우 제한적인 권한만 부여
 - 사용자 프로파일 폴더, 시스템 파일, 레지스트르 쓰기 권한 제한
 - Low Integrity Mandatory Label에 정의된 폴더, 레지스트리에만 쓰기 가능



Local/LocalLow/Roaming 폴더

윈도우 2K/XP	윈도우 Vista/7
C:\Documents and Settings\<username>\Application Data	C:\Users\<username>\AppData
C:\Documents and Settings\<username>\Local Settings	C:\Users\<username>\AppData\Local

- **Local**
 - 로컬에서만 사용되는 데이터나 데이터 크기가 커서 로밍하기 적합하지 않은 데이터
- **LocalLow**
 - 로컬에서 사용되는 데이터 중 권한이 제한되는 "Low Integrity Applications"에 의해 사용되는 데이터
- **Roaming**
 - 사용자가 다른 컴퓨터에 로그인할 때에도 사용자 관련 프로파일을 이용할 수 있도록 로밍하는 데이터
 - 시스템과 독립적으로 항상 자신의 프로필과 로밍 데이터를 사용하여 로그인 가능

추가된 폴더

- **다운로드(Downloads)**
 - IE 기본 다운로드 위치
- **연락처(Contacts)**
 - XML 형식의 사용자 연락처 정보
- **링크(Links)**
 - 윈도우 익스플로러 즐겨찾기
- **저장된 게임(Saved Games)**
 - 사용자 저장 게임 정보
- **검색(Searches)**
 - 등록된 검색 쿼리 정보

