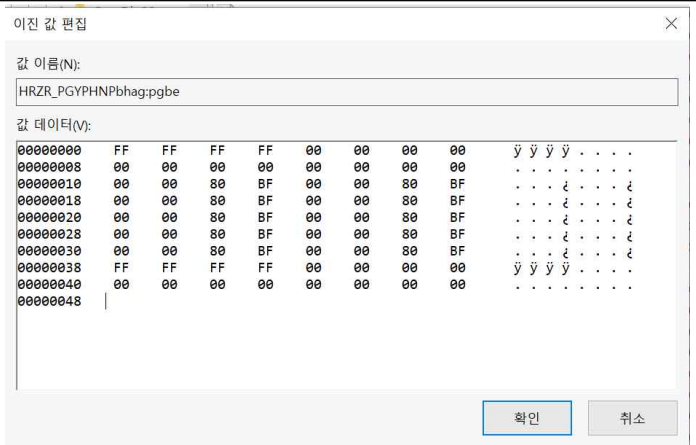
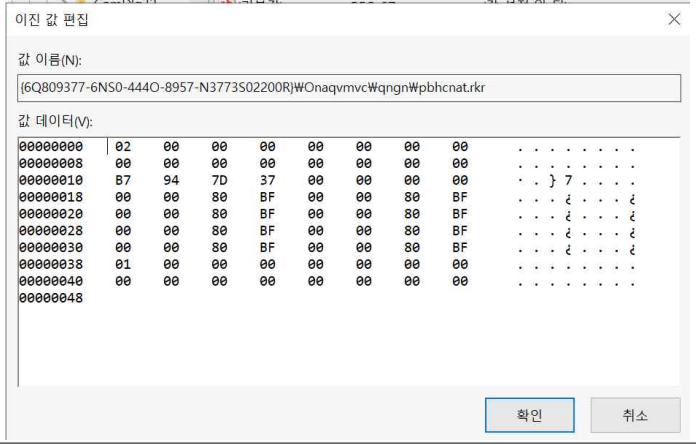
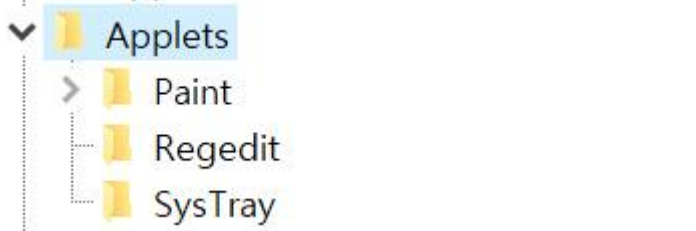
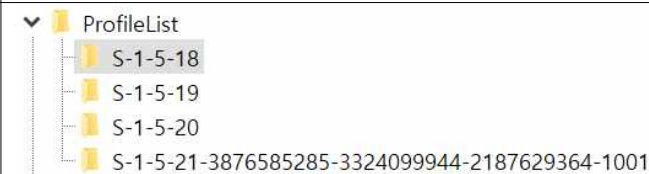


















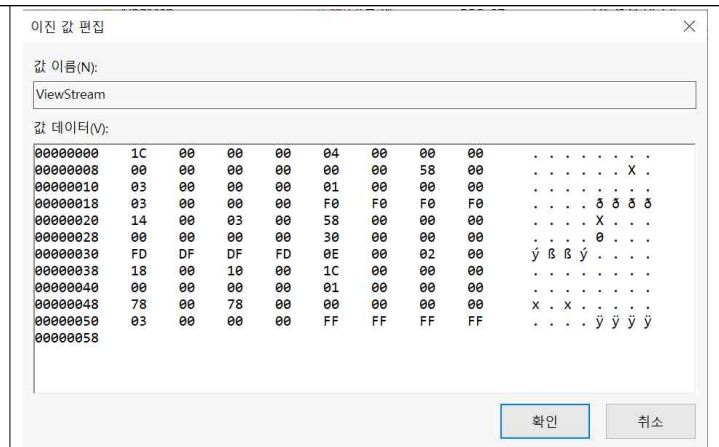


Registry Analysis

구 분			DATA VALUE
시스템 정보	ProductName	운영체제 이름	Windows 10 Pro
	RegisteredOwner	사용자 이름	jsb
	RegisteredOrganization	조직 이름	
	ProductId	운영체제 식별자	00331-10000-00001-AA935
	BuildLab	운영체제 세부 버전	19041.vb_release.191206-1406
	InstallDate	운영체제 설치 날짜	67187131 (총 2024-10-23, 오후 12:44:49)
	SystemRoot	운영체제 설치 루트 폴더	C:\WINDOWS
컴퓨터 이름	ComputerName	시스템 등록정보	DESKTOP-BB0D1AQ
시스템 마지막 종료 시각	ShutdownTime	마지막 종료 시각 저장	83 d9 c6 fa c2 4b db 01
표준시간대	TimeZoneKeyName	UTC/GMT 표준 시간대	Korea Standard Time
날짜변경 흔적	Count	ROT-13	

			
응용프로그램 사용 로그	Count	ROT-13	
워드패드에서 열어본 파일 목록	File #	종료 시점에 값 저장	
MS워드에서 열어본 파일 목록	Place MRU, File MRU	최근 사용 파일	

																																									
사용자 계정 정보	ProfileList	시스템 사용자 프로필 목록																																							
	LastUsedUsername	마지막 로그인 사용자	jsb																																						
	Shell Folders	사용자별 기본 경로	<table><tr><td></td><td>REG_SZ</td><td>(값 설정 안 됨)</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData\Microsoft\Windows\Start Me...</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData</td></tr><tr><td></td><td>REG_SZ</td><td>C:\Users\Public\Desktop</td></tr><tr><td></td><td>REG_SZ</td><td>C:\Users\Public\Documents</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData\Microsoft\Windows\Start Me...</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData\Microsoft\Windows\Start Menu</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData\Microsoft\Windows\Start Me...</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData\Microsoft\Windows\Templates</td></tr><tr><td></td><td>REG_SZ</td><td>C:\Users\Public\Music</td></tr><tr><td></td><td>REG_SZ</td><td>C:\Users\Public\Pictures</td></tr><tr><td></td><td>REG_SZ</td><td>C:\Users\Public\Videos</td></tr><tr><td></td><td>REG_SZ</td><td>C:\ProgramData\OEM\Links</td></tr></table>		REG_SZ	(값 설정 안 됨)		REG_SZ	C:\ProgramData\Microsoft\Windows\Start Me...		REG_SZ	C:\ProgramData		REG_SZ	C:\Users\Public\Desktop		REG_SZ	C:\Users\Public\Documents		REG_SZ	C:\ProgramData\Microsoft\Windows\Start Me...		REG_SZ	C:\ProgramData\Microsoft\Windows\Start Menu		REG_SZ	C:\ProgramData\Microsoft\Windows\Start Me...		REG_SZ	C:\ProgramData\Microsoft\Windows\Templates		REG_SZ	C:\Users\Public\Music		REG_SZ	C:\Users\Public\Pictures		REG_SZ	C:\Users\Public\Videos		REG_SZ
	REG_SZ	(값 설정 안 됨)																																							
	REG_SZ	C:\ProgramData\Microsoft\Windows\Start Me...																																							
	REG_SZ	C:\ProgramData																																							
	REG_SZ	C:\Users\Public\Desktop																																							
	REG_SZ	C:\Users\Public\Documents																																							
	REG_SZ	C:\ProgramData\Microsoft\Windows\Start Me...																																							
	REG_SZ	C:\ProgramData\Microsoft\Windows\Start Menu																																							
	REG_SZ	C:\ProgramData\Microsoft\Windows\Start Me...																																							
	REG_SZ	C:\ProgramData\Microsoft\Windows\Templates																																							
	REG_SZ	C:\Users\Public\Music																																							
	REG_SZ	C:\Users\Public\Pictures																																							
	REG_SZ	C:\Users\Public\Videos																																							
	REG_SZ	C:\ProgramData\OEM\Links																																							
최근 접근 흔적	MRUListEx	열어본 순서	<table><tr><td></td><td>REG_SZ</td><td>(값 설정 안 됨)</td></tr><tr><td></td><td>REG_BINARY</td><td>1c 00 00 00 04 00 00 00 00 00 00 00 00 58 0...</td></tr></table>		REG_SZ	(값 설정 안 됨)		REG_BINARY	1c 00 00 00 04 00 00 00 00 00 00 00 00 58 0...																																
	REG_SZ	(값 설정 안 됨)																																							
	REG_BINARY	1c 00 00 00 04 00 00 00 00 00 00 00 00 58 0...																																							



ows\CurrentVersion\Explorer\RunMRU		
이름	종류	데이터
 (기본값)	REG_SZ	(값 설정 안 됨)

Windows Portable Devices\Devices		
이름	종류	데이터
 (기본값)	REG_SZ	(값 설정 안 됨)
<div><div>Windows Portable Devices</div><div><div>Devices</div><div><div>SWD\WPDBusENUM#_71_USBSTOR\DISK&VEN_15B&PROD_SANDISK_3.2GENT&REV_1.00#0101830C0427A50AD4CFCD2C456964E57E3F500423D66FB09DED571F</div><div>SWD\WPDBusENUM#_71_USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07#00D055A180#F3F56307-B6BF-11D0-94F2-00ADC91EF88B</div><div>SWD\WPDBusENUM#_71_USBSTOR\DISK&VEN_GENERIC&PROD_MASSSTORAGECLASS&REV_0009#000000000000980#F3F56307-B6BF-11D0-94F2-00ADC91EF88B</div><div>SWD\WPDBusENUM#_71_USBSTOR\DISK&VEN_GENERIC&PROD_MASSSTORAGECLASS&REV_0009#000000000000980#F3F56307-B6BF-11D0-94F2-00ADC91EF88B</div><div>SWD\WPDBusENUM#7325CBC2-9651-11EF-833D-D4E9BAB80C2B#0000000000010000</div><div>SWD\WPDBusENUM#7325CBC2-9651-11EF-833D-D4E9BAB80C2B#00000000E530F3000</div></div></div></div>		










































































































DeviceClasses		

- DeviceClasses
- > {00001000-0000-1000-8000-00805f9b34fb}
 - > {0000110b-0000-1000-8000-00805f9b34fb}
 - > {0000110c-0000-1000-8000-00805f9b34fb}
 - > {0000110e-0000-1000-8000-00805f9b34fb}
 - > {0000111e-0000-1000-8000-00805f9b34fb}
 - > {00f11ce2-94d9-44a7-b858-9d894044ff43}
 - > {00f40965-e89d-4487-9890-87c3abb211f4}
 - > {05ecd13d-81da-4a2a-8a4c-524f23dd4dc9}
 - > {064092b3-625e-43bf-9eb5-dc845897dd59}
 - > {0850302a-b344-4fda-9be9-90576b8d46f0}
 - > {09485f5a-759e-42c2-bd4b-a349b75c8643}
 - > {09a5554b-da25-4461-8d80-5bc6c96dd932}
 - > {0a4252a0-7e70-11d0-a5d6-28db04c10000}
 - > {0ecef634-6ef0-472a-8085-5ad023ecbccd}
 - > {10497b1b-ba51-44e5-8318-a65c837b6661}
 - > {10910c20-0c64-4172-9409-add3064c0cad}
 - > {1ca05180-a699-450a-9a0c-de4fbe3ddd89}
 - > {1dc7cf2a-9167-5887-b1b2-16e04384f64c}
 - > {21157c1f-2651-4cc1-90ca-1f28b02263f6}
 - > {2a323d9d-edf1-430b-ab95-5860894493d4}
 - > {2accfe60-c130-11d2-b082-00a0c91efb8b}
 - > {2c6bb644-e1ae-47f8-9a2b-1d1fa750f2fa}
 - > {2e34d650-5819-42ca-84ae-d30803bae505}
 - > {2eef81be-33fa-4800-9670-1cd474972c3f}
 - > {2f2b7b01-597a-434c-8dd6-d27cd46ef73c}
 - > {30d7f776-1f32-4a14-a7e5-34e6a63807e9}
 - > {378de44c-56ef-11d1-bc8c-00a0c91405dd}
 - > {3abf6f2d-71c4-462a-8a92-1e6861e6af27}
 - > {3c0d501a-140b-11d1-b40f-00a0c9223196}
 - > {3c4852d6-d47b-4f46-b05e-b5edc1aa440e}
 - > {435b6226-1dcc-43b3-887e-217dbaa27ba3}
 - > {4747b320-62ce-11cf-a5d6-28db04c10000}
 - > {48fc632f-29b4-4465-a806-d91b667ab674}

	VID_####&PID_####	마지막 연결	
--	-------------------	--------	--

- ▼ USB
 - > ROOT_HUB30
 - ▼ VID_0461&PID_4D16
 - ▼ 5&37daea04&0&1
 - > Device Parameters
 - └─ Properties
 - > VID_046D&PID_C52F
 - > VID_046D&PID_C52F&MI_00
 - > VID_046D&PID_C52F&MI_01
 - > VID_0781&PID_55A3
 - > VID_093A&PID_2510
 - > VID_0BDA&PID_5641
 - > VID_0BDA&PID_5641&MI_00
 - > VID_0BDA&PID_8153
 - > VID_1A2C&PID_0E24
 - > VID_1A2C&PID_0E24&MI_00
 - > VID_1A2C&PID_0E24&MI_01
 - > VID_2109&PID_0817
 - > VID_2109&PID_0822
 - > VID_2109&PID_2817
 - > VID_2109&PID_2820
 - > VID_21C4&PID_B060
 - > VID_27C6&PID_6A94
 - > VID_8087&PID_0033

네트워크 정보	NetworkList	네트워크 정보	<div> <div> 이름 (기본값) Category DateCreated DateLastConnec... Description Managed NameType ProfileName </div> <div> 종류 REG_SZ REG_DWORD REG_BINARY REG_BINARY REG_SZ REG_DWORD REG_DWORD REG_SZ </div> <div> 데이터 (값 설정 안 됨) 0x00000000 (0) e8 07 0a 00 04 00 0a 00 0b 00 0c 00 36 00 9d 02 e8 07 0c 00 04 00 0c 0b 00 0f 00 0d 00 44 00 JBU-WLAN 0x00000000 (0) 0x00000047 (71) JBU-WLAN </div> </div>
이벤트 로그	Eventlog	로그 파일 경로 등	<div> <div> 이름 (기본값) Description DisplayName ErrorControl FailureActions FailureActionsOn... Group ImagePath ObjectName PlugPlayServiceT... RequiredPrivileg... ServiceSidType Start SvcMemHardLi... SvcMemMidLimi... SvcMemSoftLim... Type </div> <div> 종류 REG_SZ REG_SZ REG_SZ REG_DWORD REG_BINARY REG_DWORD REG_SZ REG_EXPAND_SZ REG_SZ REG_DWORD REG_MULTI_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD </div> <div> 데이터 (값 설정 안 됨) @%SystemRoot%\system32\Wwevtvc.dll,-201 @%SystemRoot%\system32\Wwevtvc.dll,-200 0x00000001 (1) 80 51 01 00 00 00 00 00 00 00 00 03 00 00 0... 0x00000001 (1) Event Log %SystemRoot%\System32\Wsvchost.exe -k LocalS... NT AUTHORITY\LocalService 0x00000003 (3) SeChangeNotifyPrivilege SeImpersonatePrivilege ... 0x00000001 (1) 0x00000002 (2) 0x00000014 (20) 0x0000000f (15) 0x0000000b (11) 0x00000020 (32) </div> </div>
공유폴더	Shares	공유폴더 목록	<div> <div> > jhi_service > kbdcclass > kbdcid > kbdcidfltr > kdnic > Keyiso > KSecDD > KSecPkg > ksthunk > KtmRm > LanmanServer > AllocatedParameters > Certs > DefaultSecurity > Linkage > Parameters > ShareProviders > Shares > Security </div> <div> 이름 (기본값) 종류 REG_SZ 데이터 (값 설정 안 됨) </div> </div>
인터넷 사용 흔적	Main	설정 정보	

			<table><tr><th>이름</th><th>종류</th><th>데이터</th></tr><tr><td> (기본값)</td><td>REG_SZ</td><td>(값 설정 안 됨)</td></tr><tr><td> Anchor Underline</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Cache_Update_F...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> CompatibilityFlags</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td> Disable Script D...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> DisableFirstRunC...</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td> DisableScriptDe...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Display Inline Im...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Do404Search</td><td>REG_BINARY</td><td>01 00 00 00</td></tr><tr><td> DownloadWindo...</td><td>REG_BINARY</td><td>2c 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff f...</td></tr><tr><td> Enable Browser ...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> FullScreen</td><td>REG_SZ</td><td>no</td></tr><tr><td> ImageStoreRand...</td><td>REG_SZ</td><td>y09ujhx</td></tr><tr><td> Local Page</td><td>REG_SZ</td><td>%11%#blank.htm</td></tr><tr><td> OperationalData</td><td>REG_QWORD</td><td>0x0000000d (13)</td></tr><tr><td> Play_Animations</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Play_Backgroun...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Save_Session_Hi...</td><td>REG_SZ</td><td>no</td></tr><tr><td> Search Page</td><td>REG_SZ</td><td>http://go.microsoft.com/fwlink/?LinkId=54896</td></tr><tr><td> SearchBandMigr...</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr><tr><td> Show_FullURL</td><td>REG_SZ</td><td>no</td></tr><tr><td> Show_StatusBar</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Show_ToolBar</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Show_URLinStat...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Show_URLToolBar</td><td>REG_SZ</td><td>yes</td></tr><tr><td> Start Page</td><td>REG_SZ</td><td>http://go.microsoft.com/fwlink/p/?LinkId=255141</td></tr><tr><td> TabShutdownDe...</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td> Use_DlgBox_Col...</td><td>REG_SZ</td><td>yes</td></tr><tr><td> UseClearType</td><td>REG_SZ</td><td>no</td></tr><tr><td> Window_Placem...</td><td>REG_BINARY</td><td>2c 00 00 00 00 00 00 01 00 00 00 ff ff ff ff f...</td></tr><tr><td> XMLHTTP</td><td>REG_DWORD</td><td>0x00000001 (1)</td></tr></table>	이름	종류	데이터	 (기본값)	REG_SZ	(값 설정 안 됨)	 Anchor Underline	REG_SZ	yes	 Cache_Update_F...	REG_SZ	yes	 CompatibilityFlags	REG_DWORD	0x00000000 (0)	 Disable Script D...	REG_SZ	yes	 DisableFirstRunC...	REG_DWORD	0x00000001 (1)	 DisableScriptDe...	REG_SZ	yes	 Display Inline Im...	REG_SZ	yes	 Do404Search	REG_BINARY	01 00 00 00	 DownloadWindo...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff f...	 Enable Browser ...	REG_SZ	yes	 FullScreen	REG_SZ	no	 ImageStoreRand...	REG_SZ	y09ujhx	 Local Page	REG_SZ	%11%#blank.htm	 OperationalData	REG_QWORD	0x0000000d (13)	 Play_Animations	REG_SZ	yes	 Play_Backgroun...	REG_SZ	yes	 Save_Session_Hi...	REG_SZ	no	 Search Page	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=54896	 SearchBandMigr...	REG_DWORD	0x00000001 (1)	 Show_FullURL	REG_SZ	no	 Show_StatusBar	REG_SZ	yes	 Show_ToolBar	REG_SZ	yes	 Show_URLinStat...	REG_SZ	yes	 Show_URLToolBar	REG_SZ	yes	 Start Page	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141	 TabShutdownDe...	REG_DWORD	0x00000000 (0)	 Use_DlgBox_Col...	REG_SZ	yes	 UseClearType	REG_SZ	no	 Window_Placem...	REG_BINARY	2c 00 00 00 00 00 00 01 00 00 00 ff ff ff ff f...	 XMLHTTP	REG_DWORD	0x00000001 (1)
이름	종류	데이터																																																																																																	
 (기본값)	REG_SZ	(값 설정 안 됨)																																																																																																	
 Anchor Underline	REG_SZ	yes																																																																																																	
 Cache_Update_F...	REG_SZ	yes																																																																																																	
 CompatibilityFlags	REG_DWORD	0x00000000 (0)																																																																																																	
 Disable Script D...	REG_SZ	yes																																																																																																	
 DisableFirstRunC...	REG_DWORD	0x00000001 (1)																																																																																																	
 DisableScriptDe...	REG_SZ	yes																																																																																																	
 Display Inline Im...	REG_SZ	yes																																																																																																	
 Do404Search	REG_BINARY	01 00 00 00																																																																																																	
 DownloadWindo...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff f...																																																																																																	
 Enable Browser ...	REG_SZ	yes																																																																																																	
 FullScreen	REG_SZ	no																																																																																																	
 ImageStoreRand...	REG_SZ	y09ujhx																																																																																																	
 Local Page	REG_SZ	%11%#blank.htm																																																																																																	
 OperationalData	REG_QWORD	0x0000000d (13)																																																																																																	
 Play_Animations	REG_SZ	yes																																																																																																	
 Play_Backgroun...	REG_SZ	yes																																																																																																	
 Save_Session_Hi...	REG_SZ	no																																																																																																	
 Search Page	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=54896																																																																																																	
 SearchBandMigr...	REG_DWORD	0x00000001 (1)																																																																																																	
 Show_FullURL	REG_SZ	no																																																																																																	
 Show_StatusBar	REG_SZ	yes																																																																																																	
 Show_ToolBar	REG_SZ	yes																																																																																																	
 Show_URLinStat...	REG_SZ	yes																																																																																																	
 Show_URLToolBar	REG_SZ	yes																																																																																																	
 Start Page	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141																																																																																																	
 TabShutdownDe...	REG_DWORD	0x00000000 (0)																																																																																																	
 Use_DlgBox_Col...	REG_SZ	yes																																																																																																	
 UseClearType	REG_SZ	no																																																																																																	
 Window_Placem...	REG_BINARY	2c 00 00 00 00 00 00 01 00 00 00 ff ff ff ff f...																																																																																																	
 XMLHTTP	REG_DWORD	0x00000001 (1)																																																																																																	
TypedURLs	URL 목록	<table><tr><th>이름</th><th>종류</th><th>데이터</th></tr><tr><td> (기본값)</td><td>REG_SZ</td><td>(값 설정 안 됨)</td></tr><tr><td> url1</td><td>REG_SZ</td><td>http://go.microsoft.com/fwlink/p/?LinkId=255141</td></tr></table>	이름	종류	데이터	 (기본값)	REG_SZ	(값 설정 안 됨)	 url1	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141																																																																																								
이름	종류	데이터																																																																																																	
 (기본값)	REG_SZ	(값 설정 안 됨)																																																																																																	
 url1	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141																																																																																																	
Internet Exploer	다운로드 경로	<div>soft\Winternet Explorer</div> <table><tr><th>이름</th><th>종류</th><th>데이터</th></tr><tr><td> (기본값)</td><td>REG_SZ</td><td>(값 설정 안 됨)</td></tr></table>	이름	종류	데이터	 (기본값)	REG_SZ	(값 설정 안 됨)																																																																																											
이름	종류	데이터																																																																																																	
 (기본값)	REG_SZ	(값 설정 안 됨)																																																																																																	
Favorites	즐거찾기	<div>CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\AppDatalets\WRegedit</div> <div><div><div>CurrentVersion</div><div>AccountsService</div><div>ActivityDataModel</div><div>AdvertisingInfo</div><div>App Paths</div><div>AppBroadcast</div><div>AppHost</div><div>Applets</div><div>Paint</div><div>Regedit</div><div>SysTray</div></div><table><tr><th>이름</th><th>종류</th><th>데이터</th></tr><tr><td> (기본값)</td><td>REG_SZ</td><td>(값 설정 안 됨)</td></tr><tr><td> FindFlags</td><td>REG_DWORD</td><td>0x00000000 (0)</td></tr><tr><td> LastKey</td><td>REG_SZ</td><td>컴퓨터\HKEY_CURRENT_USER</td></tr><tr><td> View</td><td>REG_BINARY</td><td>2c 00 00 00 00 00 00 01 00 00 00 83 ff ff ...</td></tr></table></div>	이름	종류	데이터	 (기본값)	REG_SZ	(값 설정 안 됨)	 FindFlags	REG_DWORD	0x00000000 (0)	 LastKey	REG_SZ	컴퓨터\HKEY_CURRENT_USER	 View	REG_BINARY	2c 00 00 00 00 00 00 01 00 00 00 83 ff ff ...																																																																																		
이름	종류	데이터																																																																																																	
 (기본값)	REG_SZ	(값 설정 안 됨)																																																																																																	
 FindFlags	REG_DWORD	0x00000000 (0)																																																																																																	
 LastKey	REG_SZ	컴퓨터\HKEY_CURRENT_USER																																																																																																	
 View	REG_BINARY	2c 00 00 00 00 00 00 01 00 00 00 83 ff ff ...																																																																																																	