외장장치

1 인식 절차

1) 버스 드라이버는 PnP 관리자에게 장치의 고유 식별번호(device descriptor)로 연결 알림
   - 식별번호 – 제조사, 일련번호, 드라이버 등을 포함

2) .PnP 관리자는 받은 정보를 기반으로 Device Class ID를 설정하고 드라이버 검색

3) 드라이버가 없을 경우, PnP 관리자는 장치의 펌웨어로부터 드라이버를 전달받아 설치
   - 장치 드라이버 설치 과정은 Setup API 로그에 기록

4) 드라이버 설치와 함께 레지스트리에 장치 관련 키/값 생성
   - HKLM₩SYSTEM₩ControlSet00#₩Enum₩USBSTOR₩{DID, device class identifier}
   - HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{GUID}

5) 장치가 인식되어 연결/해제될 때마다 이벤트 로그 기록

1.1 최초연결은 setup api에 남고 그 이후의 흔적은 레지스트리에 남는다.

2 Setup API

- %SystemRoot%₩inf₩Setupapi.dev.log

2.1 로그

- 장치 드라이버, 서비스 팩 등이 설치될 때 남기는 텍스트 로그
- 저장장치 최초 연결 시 장치 드라이버 설치 흔적이 남음 -> 최초 연결 시각
- 윈도우 2K/XP : %SystemRoot%₩Setupapi.log
- 윈도우 Vista+ : %SystemRoot%₩inf₩Setupapi.dev.log

3 레지스트리 하이브

- %SystemRoot%₩system32₩config₩SYSTEM

- %SystemRoot%₩system32₩config₩SOFTWARE
- %UserProfile%₩NTUSER.DAT
- OS버전마다 경로가 다르다

3.1 최초연결시각

- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩EMDMgmt₩{Device Entry}
- HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩Devices₩{Device Entry}
- 꽂은다음 시간정보가 안바뀌는키도있다. 그 것으로 최초 연결시각보면 되지만 보통은 setupAPI만 본다

3.2 부팅이후 연결 시각

- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{6AC27878-A6FA-4155-BA85-F98F491D4F33}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{A5DCBF10-6530-11D2-901F-00C04FB951ED}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩WpdBusEnumRoot₩UMB₩{Device Entry}

4 이벤트로그(윈도우 7)

- SystemRoot%₩system32₩winevt₩Logs₩Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx

4.1 중간에 꽂은 기록

- 유에스비로 작업하면 판단하기 어려우나..외장하드로 하면 하기 쉽다.
- setup : 최초 , 레지스트리 : 부팅 이후 최초 연결시각(거의 마지막시각)
- 중간에 꽂은 기록 : 이벤트로그 driverFrameworks에 유에스비에 관한 로그가 담겨있다.

5 USB 흔적 추적하기 (USB Device Tracking)

· USB 설치 과정에 따르면 드라이버 설치 로그 파일과 레지스트리를 확인하면 USB 장치의 흔적를 알 수 있을 것이다. 로그 파일과 레지스트리에서 확인할 수 있는 흔적은 다음과 같다.

- Device Class Identifier
- Unique Instance Identifier (include Serial Number)
- Vendor Name & Identifier
- Product Name & Identifier
- Volume Label
- Driver Letter
- Volume Serial Number
- Username
- Volume GUID
- First Connection Time
- First Connection Time After Booting
- Last Connection

5.1 장치 클래스 ID (Device Class Identifier)

장치 클래스 ID는 펌웨어로부터 얻은 장치의 형식, 제조사명, 상품명, 버전을 가지고 만드는 ID로 보통 다음과 같은 형태를 띄고 있다.

- Disk&Ven_{Vendor Name}&Prod_{Product Name}&Rev_{Version}

· 다음은 장치 클래스 ID의 예이다.

- Disk&Ven_Corsair&Prod_UFD&Rev_0.00
- Vendor Name : Corsair
- Product Name : UFD
- Version : 0.00

· 장치 클래스 ID는 다음 경로에서 확인할 수 있다.

- SetupAPI Logfile
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{10497B1B-BA51-44E5-8318-A65C837B6661}₩{Sub Keys}

- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{6AC27878-A6FA-4155-BA85-F98F491D4F33}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩USBSTOR₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩WpdBusEnumRoot₩UMB₩{Sub Keys}
- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩EMDMgmt₩{Sub Keys}
- HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩{Sub Keys}

5.2 고유 인스턴스 ID (Unique Instance Identifier)

· 고유 인스턴스 ID는 같은 제조사에서 만든 동일 제품이더라도 모두 다른 값을 가지는 장치 시리얼 번호가 포함된 고유의 값이다. 하지만, 모든 USB 장치가 시리얼번호를 포함하고 있는 것은 아니다. 따라서, 시리얼 번호가 있는지 여부에 따라 인스턴스 ID의 형태는 다음과 같이 달라진다.

- **Serial Number (O)** – {Serial Number}&#
- **Serial Number (X)** - #&{Random Number by PnP Manager}&#

· 다음은 시리얼번호가 존재할 때, 인스턴스 ID의 예이다.

- **545A235F&0**
- **Serial Number** : 545A235F

· 시리얼번호는 장치의 고유한 값이기 때문에 시스템에 연결했던 장치를 구별할 수 있다. USB 연결 정보를 확인하고 USB를 제출하라고 요청했는데 용의자가 동일한 제조사의 제품을 제출했다면 시리얼번호를 보고 시스템에 연결한 것과 동일한 것인지 구별해낼 수 있다.

· 고유 인스턴스 ID는 다음 경로에서 확인할 수 있다.

- SetupAPI Logfile
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{10497B1B-BA51-44E5-8318-A65C837B6661}₩{Sub Keys}

- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{6AC27878-A6FA-4155-BA85-F98F491D4F33}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{A5DCBF10-6530-11D2-901F-00C04FB951ED}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩USBS₩{Vendor ID & Product ID}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩USBSTOR₩{Device Class ID}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩WpdBusEnumRoot₩UMB₩{Sub Keys}
- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩EMDMgmt₩{Sub Keys}
- HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩{Sub Keys}

5.3 제조사 ID와 제품 ID (Vendor Identifier & Product Identifier)

· 레지스트리를 확인해보면 USB의 제조사 ID와 제품 ID를 알 수 있다. 제조사명과 제품명은 앞서 살펴본 장치 클래스 ID (Device Class Identifier)에 포함되어 있었다. 제조사 ID와 제품 ID는 다음과 같은 형태로 구성된다.

- VID_{Vendor ID}&PID_{Product ID}

· 다음은 제조사 ID와 제품 ID의 예이다.

- **VID_090C&PID_1000**
- **Vendor Identifier** : 0x090c (idVendor)
- **Product Identifier** : 0x1000 (idProduct)

· 제조사 ID와 제품 ID는 다음 경로에서 확인할 수 있다.

- HKLM₩SYSTEM₩ControlSet00#₩Enum₩USB₩{Sub Keys}

5.4 볼륨 레이블과 드라이브 문자(Volume Label & Drive Letter)

· 각 장치는 기본적으로 운영체제에서 할당한 문자로 마운트된다. 볼륨 레이블을 별도로 지정하지 않을 경우는 드라이브 문자만 나타나지만, 볼륨 레이블을 지정해놓을 경우 볼륨 레이블과 함께 드라이브 문자가 나타난다. 볼륨 레이블과 드라이브 문자도 레지스트리에서 확인할 수 있다.

· 볼륨 레이블을 다음 경로에서 확인할 수 있다.

- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩EMDMgmt₩{Sub Keys}
- HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩Devices₩{device entry}₩FriendlyName
- HKLM₩System₩{CurrentControlSet}₩Enum₩WpdBusEnumRoot₩UMB₩{device entry}₩FriendlyName
- HKLM₩SOFTWARE₩Microsoft₩Windows Search₩VolumeInfoCache₩{drive letter}

· 드라이브 문자는 다음 경로에서 확인할 수 있다.

- HKLM₩System₩MountedDevices₩{Sub Values}
- HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩Devices₩{device entry}₩FriendlyName
- HKLM₩System₩{CurrentControlSet}₩Enum₩WpdBusEnumRoot₩UMB₩{device entry}₩FriendlyName

· 볼륨 레이블 경로와 드라이브 문자 확인 경로 중에 중복되는 경로가 있다. 해당 경로에는 볼륨 레이블이 존재할 경우 볼륨 레이블이, 존재하지 않을 경우 드라이브 문자가 남는다.

5.5 볼륨 시리얼 번호 (Volume Serial Number)

· 레지스트리에는 USB의 볼륨 시리얼 번호도 저장된다. USB를 FAT12/16/32, NTFS, exFAT으로 포맷하면 VBR(Volume Boot Record)의 부트 섹터에 볼륨 시리얼번호가 기록된다. USB를 연결하면 해당 볼륨 시리얼번호도 가져와 레지스트리에 기록한다.

· 볼륨 시리얼 번호는 다음 경로에서 확인할 수 있다.

- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩EMDMgmt₩{Sub Keys}

· 다음은 EMDMgmt 하위 키의 예이다.

- **_??_USBSTOR#Disk&Ven_SMI&Prod_USB_DISK&Rev_3000#2011072800001332&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}PR0NEER_346682584**
- **Device Class Identifier** - Disk&Ven_SMI&Prod_USB_DISK&Rev_3000
- **Serial Number** : 2011072800001332
- **Volume Label** : PR0NEER

- **Volume Serial Number** : 346682584 (0x14A9F4D8)

5.6 사용자명과 볼륨 GUID (Username & Volume GUID)

· 다중 사용자가 사용하는 윈도우 시스템일 경우, 마운트된 USB가 어떤 사용자에 의해 마운트되었는지 알 필요가 있다. 마운트된 장치는 모두 고유한 볼륨 GUID를 가진다. 마운트된 장치의 볼륨 GUID는 다음 경로에서 확인할 수 있다.

- HKLM₩SYSTEM₩MountedDevices₩{Sub Values}

· 하위 값은 "₩??₩Volume" 접두사와 함께 GUID 정보를 가진다. 해당 볼륨 GUID 값의 데이터를 확인하면 어떤 장치가 마운트되었었는지 확인할 수 있다. 다음은 마운트된 USB의 값과 데이터의 예이다.

- **Value** : ₩??₩Volume{20f16aa5-b42f-11e1-91e0-1c6f65d71f1a}
- **Data** : _.?.?._.U.S.B.S.T.O.R.#.D.i.s.k.&.V.e.n._.S.M.I.&.P.r.o.d._.U.S.B._.D.I.S.K.&.R.e.v._.3.0.0.0.#.2.0.1.1.0.7.2.8.0.0.0.0.1.3.3.2.&.0.#.{.5.3.f.5.6.3.0.7.-.b.6.b.f.-.1.1.d.0.-.9.4.f.2.-.0.0.a.0.c.9.1.e.f.b.8.b.}.

· 위에서 볼륨 GUID는 "{20f16aa5-b42f-11e1-91e0-1c6f65d71f1a}"이다. 해당 볼륨 GUID 정보가 다음 경로에 있는지 확인해보자.

- HKU₩{USER}₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩MountPoints2₩{Volume GUID}

· 볼륨 GUID 값이 존재한다면 해당 경로의 {user} 값이 해당 장치를 마운트한 사용자이다.

5.7 최초 연결 시각 (First Connection Date/Time)

윈도우 시스템에 USB 장치를 처음 연결한 시점을 알아보자. USB를 처음 연결한 시점은 드라이버 설치 로그파일을 확인하면 정확하게 알 수 있다.

- **SetupAPI Logfile** – Section Start
- **Windows 2000/XP** : %SystemRoot%₩Setupapi.log
- **Windows Vista/7/8(RP)** : %SystemRoot%₩inf₩Setupapi.dev.log

· 로그 파일 없이 레지스트리만으로도 알 수 있다. 레지스트리의 포맷을 살펴보면 각 키에 "마지막 수정 시간(Last Written Time)"이 저장된다. USB를 최초 연결할 때만 생성되고, 이후에는 수정되지 않는 키의 "마지막 수정 시간"을 확인하면 USB의 최초 연결 시각을 알

수 있다.

· 다음은 USB의 최초 연결 시각을 알 수 있는 키 목록이다. 다만, "HKLM₩SYSTEM₩ControlSet00#₩Enum₩USB 또는 USBSTOR"는 Vista/7 이후 보안정책에 의해 PnP 관리자가 수시로 접근하여 시간이 변경될 수 있기 때문에 신뢰적이지 못하다.

- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{10497B1B-BA51-44E5-8318-A65C837B6661}₩{Sub Keys}
- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩EMDMgmt₩{Device Entry}
- HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩Devices₩{Device Entry}
- ~~HKLM₩SYSTEM₩ControlSet00#₩Enum₩USBSTOR₩{Device Class ID}₩{Unique Instance ID}₩{Sub Keys}~~
- ~~HKLM₩SYSTEM₩ControlSet00#₩Enum₩USB₩{Vendor ID & Product ID}₩{Serial Number}₩{Sub Keys except for "Device Parameters"}~~

5.8 부팅 후 최초 연결 시각 (First Connection Time After Booting)

· USB와 관련된 키 값 중에 어떤 키는 부팅 후 최초 연결했을때만 "마지막 수정 시간"을 갱신하고, 이후에는 재부팅할때까지 갱신하지 않는 키가 있다. 이런 키의 "마지막 수정 시간"의 의미는 "부팅 후 최초 연결 시각"이 된다.

· 다음은 부팅 후 최초 연결 시각을 알 수 있는 키 목록이다. 앞서 언급한 같은 이유로 "USB와 USBSTOR" 하위키는 제외해야 한다.

- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{6AC27878-A6FA-4155-BA85-F98F491D4F33}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Control₩DeviceClasses₩{A5DCBF10-6530-11D2-901F-00C04FB951ED}₩{Sub Keys}
- HKLM₩SYSTEM₩ControlSet00#₩Enum₩WpdBusEnumRoot₩UMB₩{Device Entry}
- ~~HKLM₩SYSTEM₩ControlSet00#₩Enum₩USBSTOR₩{Device Class ID}₩{Unique Instance ID}~~

5.9 마지막 연결 시각 (Last Connection Time)

- USB와 관련된 키 값 중에 USB를 연결할 때마다 갱신되는 키가 있다. 이런 키의 "마지막 수정 시간"의 의미는 "마지막 연결 시각"이 된다.

- 다음은 마지막 연결 시각을 알 수 있는 키 목록이다. 앞서 언급한 같은 이유로 "USB와 USBSTOR" 하위키는 제외해야 한다.

  - HKLM₩SYSTEM₩ControlSet00#₩Enum₩WpdBusEnumRoot₩UMB₩{device entry}₩Device Parameters
  - HKLM₩SYSTEM₩ControlSet00#₩Enum₩WpdBusEnumRoot₩UMB₩{device entry}₩Properties₩{80d81ea6-7473-4b0c-8216-efc11a2c4c8b}
  - HKU₩{USER}₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩MountPoints2₩{Volume GUID}
  - ~~HKLM₩SYSTEM₩ControlSet00#₩Enum₩USB₩{Vendor ID & Product ID}₩{Serial Number}~~

-