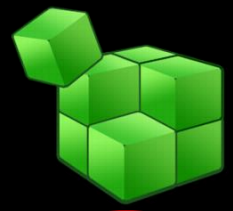
Registry Forensic

Find trace of smart phone

2020.05.12
Yum

0.Index

1.Tool

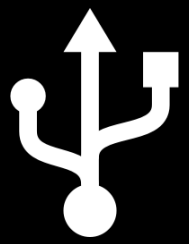


2.Registry

3.Pratice

1.Tool

Physical



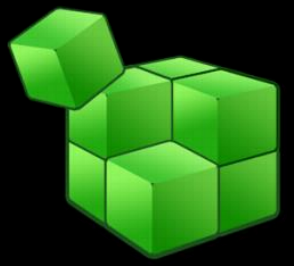
USB cable

Android

Apple

Software

FTK Imager

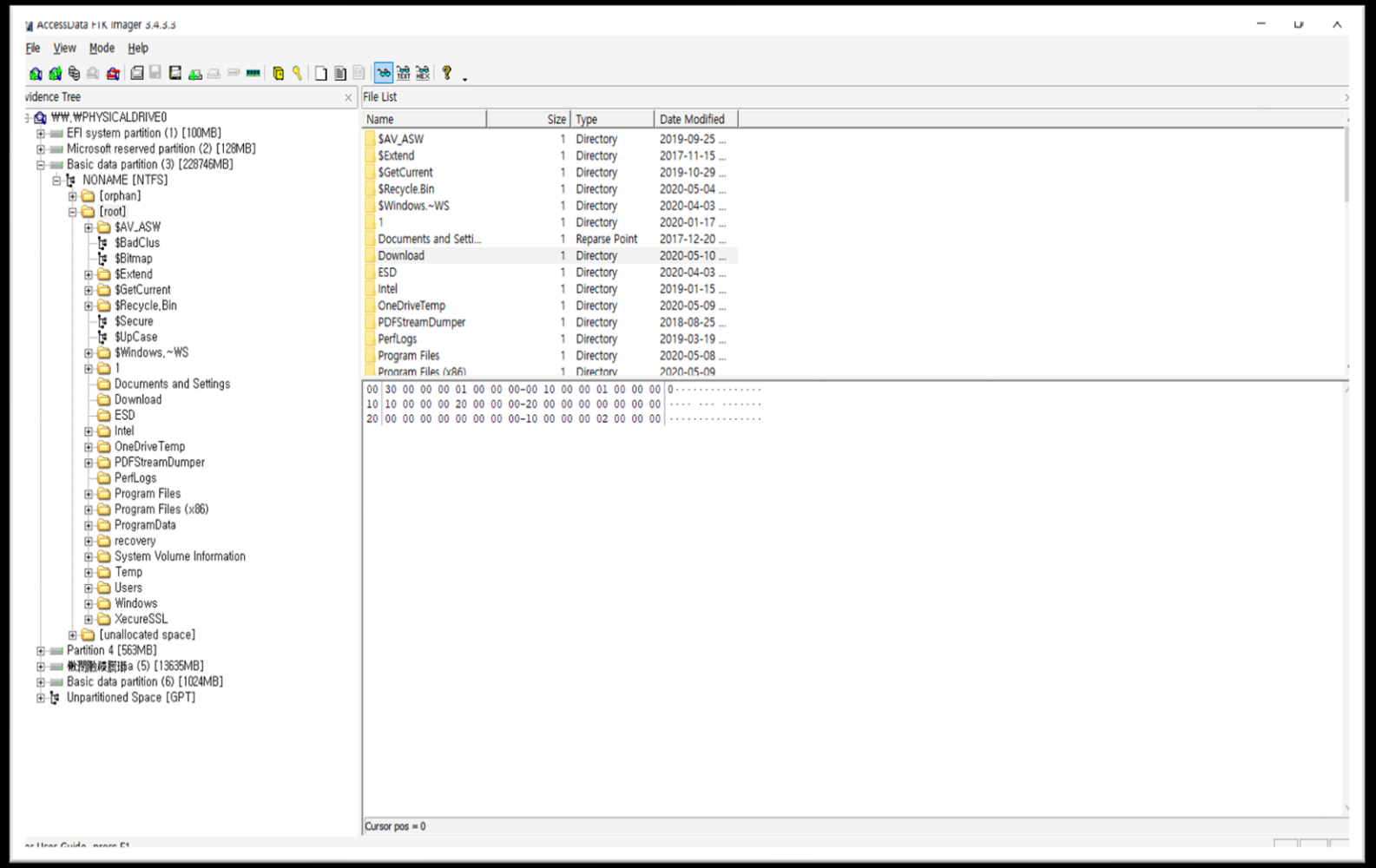


Registry Explorer

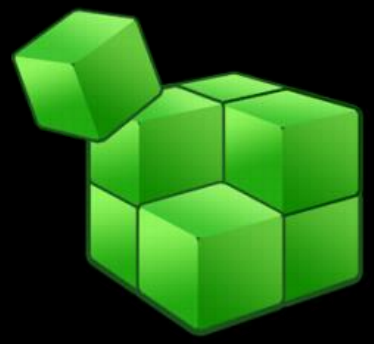
1.Tool

FTK Imager

1. Forensics Basic Tool
2. Tree Structure
3. Check Hidden Files
4. Export Files



2.Registry



Registry

OS

CLASSES_ ROOT | CURRENT_ USER | LOCAL_ MACHINE | USERS | CURRENT_ CONFIG

ROOT KEY

SAM | SECURITY | SOFTWARE | SYSTEM

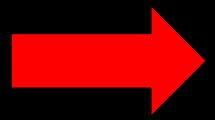
HIVE FILE

3.Practice

Connect my phone to my laptop
using the USB cable.

3.Practice

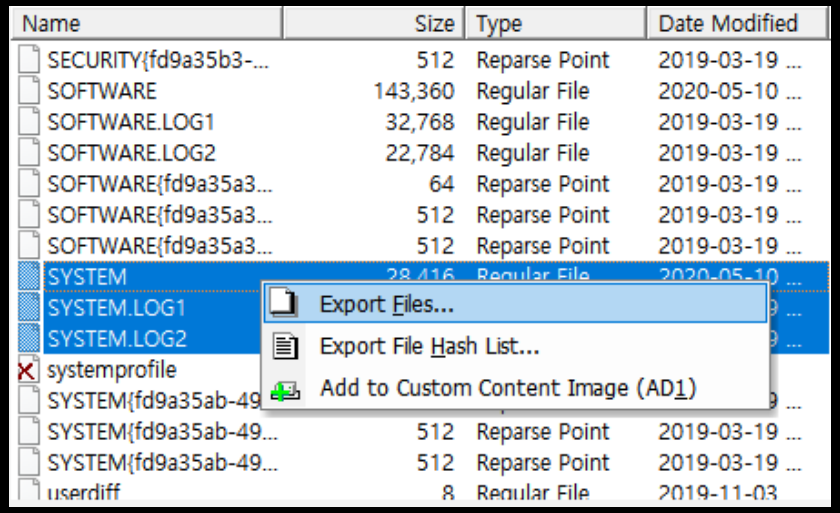
FTK Imager



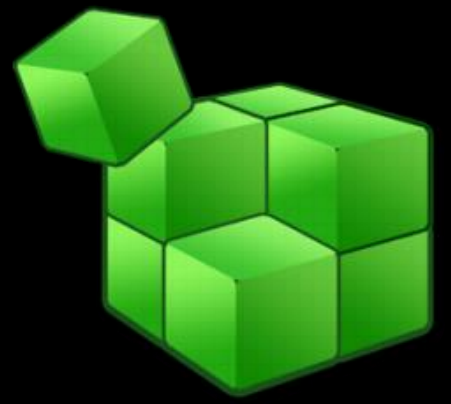
Name	Size	Type	Date Modified
SECURITY{fd9a35b3-...	512	Reparse Point	2019-03-19 ...
SOFTWARE	143,360	Regular File	2020-05-10 ...
SOFTWARE.LOG1	32,768	Regular File	2019-03-19 ...
SOFTWARE.LOG2	22,784	Regular File	2019-03-19 ...
SOFTWARE{fd9a35a3...	64	Reparse Point	2019-03-19 ...
SOFTWARE{fd9a35a3...	512	Reparse Point	2019-03-19 ...
SOFTWARE{fd9a35a3...	512	Reparse Point	2019-03-19 ...
SYSTEM	28,416	Regular File	2020-05-10 ...
SYSTEM.LOG1	5,888	Regular File	2019-03-19 ...
SYSTEM.LOG2	6,336	Regular File	2019-03-19 ...
systemprofile		$I30 INDX Entry	
SYSTEM{fd9a35ab-49...	64	Reparse Point	2019-03-19 ...
SYSTEM{fd9a35ab-49...	512	Reparse Point	2019-03-19 ...
SYSTEM{fd9a35ab-49...	512	Reparse Point	2019-03-19 ...
userdiff	8	Regular File	2019-11-03

C:\Windows\System32\config\SYSTEM

3.Practice



Export Files…



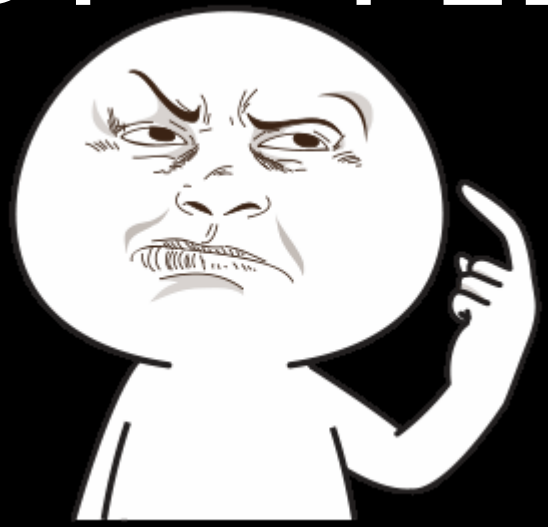
Run Registry Explorer

3.Practice

ame	# values	# subkeys	Last write timestamp
	=	=	=
PCI	0	15	2019-11-03 13:11:55
ROOT	0	18	2020-05-01 16:31:48
SCSI	0	2	2020-01-30 05:32:17
STORAGE	0	2	2019-11-03 15:10:36
SW	0	2	2020-04-22 18:48:54
SWD	0	9	2019-11-24 12:17:22
UEFI	0	1	2019-11-03 13:11:58
USB	0	19	2020-04-19 08:56:47
ROOT_HUB30	0	1	2019-11-03 13:11:56
VID_0483&PID_5750	0	1	2020-02-18 18:53:41
VID_04B8&PID_08AA	0	1	2019-11-14 03:56:26
VID_04B8&PID_08AA&MI_00	0	1	2019-11-14 03:56:27
VID_04B8&PID_08AA&MI_01	0	1	2019-11-14 03:56:27
VID_04E8&PID_393E	0	1	2020-04-19 08:56:47
VID_04E8&PID_393E&MI_00	0	1	2020-04-19 08:56:47
VID_04E8&PID_393E&MI_01	0	1	2020-04-19 08:56:47
VID_04E8&PID_393E&MI_02	0	1	2020-04-19 08:56:47
VID_04E8&PID_61F5	0	1	2020-01-30 05:32:16
VID_04E8&PID_7301	0	1	2019-11-03 13:11:57
VID_05AC&PID_12A8	0	1	2020-02-09 19:18:18
VID_05AC&PID_12A8&MI_00	0	1	2020-02-09 19:18:24
VID_05AC&PID_12A8&MI_01	0	1	2020-02-09 19:18:18
VID_0781&PID_5567	0	3	2020-01-28 05:26:37
Vid_0E0F&Pid_0001	0	4	2020-04-19 09:00:42
VID_2232&PID_1083	0	1	2019-11-03 13:11:57
VID_2232&PID_1083&MI_00	0	1	2019-11-03 13:11:57
VID_8087&PID_0A2B	0	1	2019-11-03 13:11:57
USBPRINT	0	2	2020-04-19 08:56:47
USBSTOR	0	1	2020-01-10 16:51:24
{5d624f94-8850-40c3-a3fa-a4fd208...	0	1	2019-11-03 13:14:38
Hardware Profiles	0	2	2020-05-10 23:30:24
Policies	0	0	2019-11-03 13:13:33
Services	0	834	2020-05-12 02:49:46

ControlSet001\Enum\USB

VID? PID?

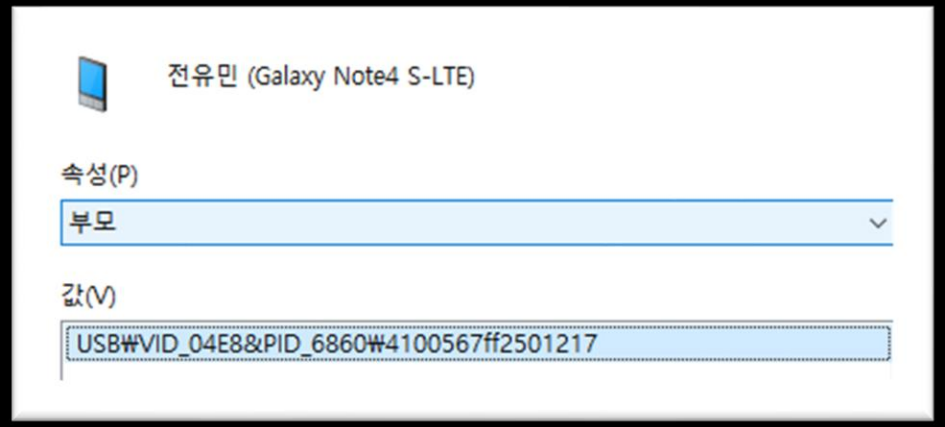


3.Practice

VID (Vender ID)

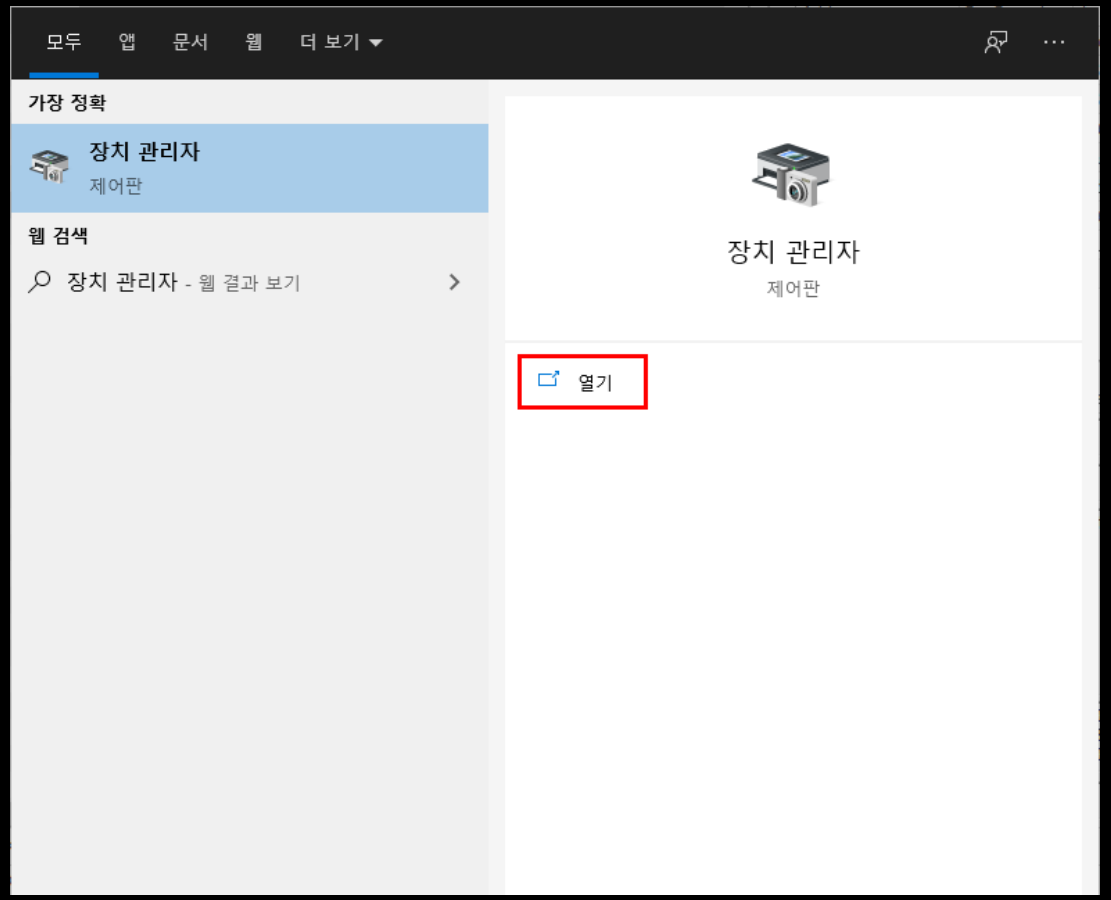
+

PID (Product ID)

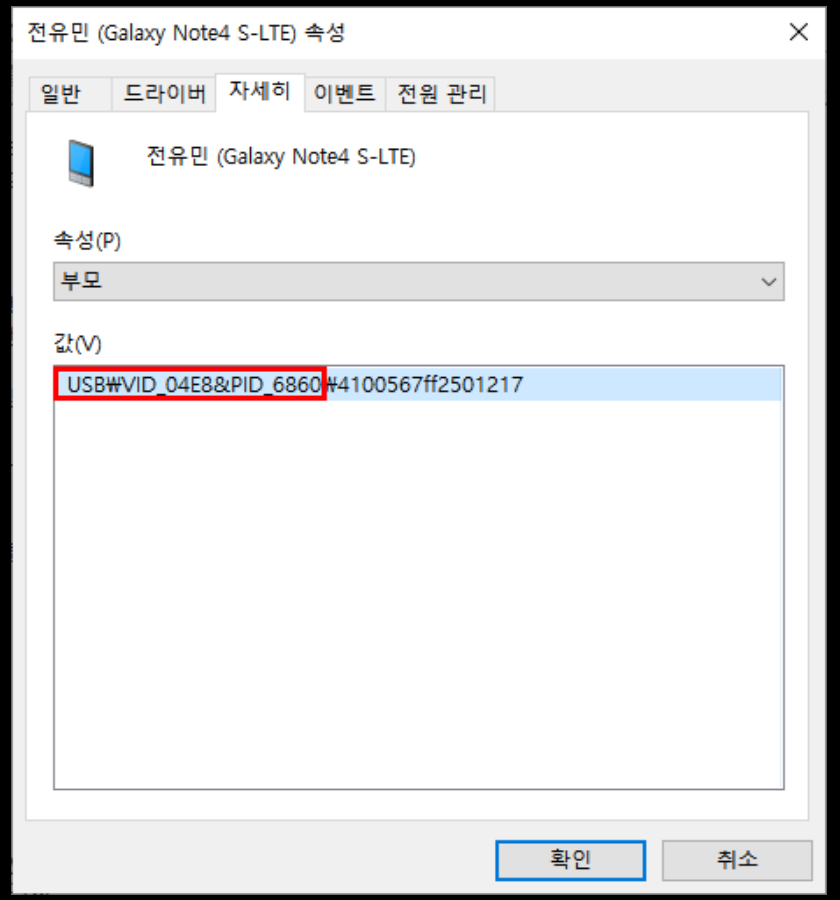


VID & PID

3.Practice



Search(Device Manager)



Portable Device(Property)

3.Practice

VID_04E8&PID_6860	0	1	2020-05-12 05:30:58
4100567ff2501217	13	2	2020-05-12 06:49:19
VID_04E8&PID_6860&Modem	0	1	2020-05-12 05:30:59
6&1ae49685&0&0001	13	2	2020-05-12 06:49:19
VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android	0	1	2020-05-12 05:30:59
6&1ae49685&0&0000	13	2	2020-05-12 06:49:21
VID_04E8&PID_7301	0	1	2019-11-03 13:11:57

Galaxy(Android)

VID_05AC&PID_12A8	0	1	2020-02-09 19:18:18
f57ba2090e9f9d947ced21fb53ac2ca70dc1a928	15	2	2020-05-12 07:49:12
VID_05AC&PID_12A8&MI_00	0	1	2020-02-09 19:18:24
6&351ac9cd&1&0000	14	2	2020-05-12 07:49:17
VID_05AC&PID_12A8&MI_01	0	1	2020-02-09 19:18:18
6&351ac9cd&1&0001	14	2	2020-05-12 07:49:12
VID_0781&PID_5567	0	3	2020-01-28 05:26:37

Iphone(Apple)

3.Practice

Android

Value Name	Value Type	Data
DeviceDesc	RegSz	@oem20.inf,%ssud.devicedesc%;SAMSUNG Mobile USB Modem
Capabilities	RegDword	128
Address	RegDword	1
ContainerID	RegSz	{a431557d-625f-50ba-aed9-1ba63460b205}
HardwareID	RegMultiSz	USB₩VID_04E8&PID_6860&REV_0400&Modem USB₩VID_04E8&PID_6860&Modem USB₩SAMSUNG_MOBILE&Modem USB₩SAMSUNG_MOBILE&MI_01 USB₩Vid...
CompatibleIDs	RegMultiSz	USB₩Class_02&SubClass_02&Prot_01 USB₩Class_02&SubClass_02 USB₩Class_02 USB₩SAMSUNG_MOBILE&Modem USB₩Vid_04E8&Pid_6860&MI_01 USB₩Vid_...
ConfigFlags	RegDword	0
ClassGUID	RegSz	{4d36e96d-e325-11ce-bfc1-08002be10318}
Driver	RegSz	{4d36e96d-e325-11ce-bfc1-08002be10318}₩0000
FriendlyName	RegSz	SAMSUNG Mobile USB Modem
LowerFilters	RegMultiSz	ssudmdm
Service	RegSz	Modem
Mfg	RegSz	@oem20.inf,%ssud%;SAMSUNG Electronics Co., Ltd.

Samsung USB Model information

Value Name	Value Type	Data
DeviceDesc	RegSz	SM-N916L
Capabilities	RegDword	128
Address	RegDword	1
ContainerID	RegSz	{a431557d-625f-50ba-aed9-1ba63460b205}
HardwareID	RegMultiSz	USB₩VID_04E8&PID_6860&REV_0400&MS_COMP_MTP&SAMSUNG_Android USB₩VID_04E8&PID_6860&MS_COMP_MTP&SAMSUNG_Android USB₩SAMSUNG_MO...
CompatibleIDs	RegMultiSz	USB₩MS_COMP_MTP USB₩Class_06&SubClass_01&Prot_01 USB₩Class_06&SubClass_01 USB₩Class_06 USB₩Vid_04E8&Pid_6860&MI_00 USB₩Vid_04E8&Pid_68...
ConfigFlags	RegDword	0
ClassGUID	RegSz	{eec5ad98-8080-425f-922a-dabf3de3f69a}
Driver	RegSz	{eec5ad98-8080-425f-922a-dabf3de3f69a}₩0003
LowerFilters	RegMultiSz	WinUsb
Mfg	RegSz	Samsung Electronics Co., Ltd.
Service	RegSz	WUDFWpdMtp
FriendlyName	RegSz	전유민 (Galaxy Note4 S-LTE)

Samsung Smart Phone Model information

3.Practice

Apple

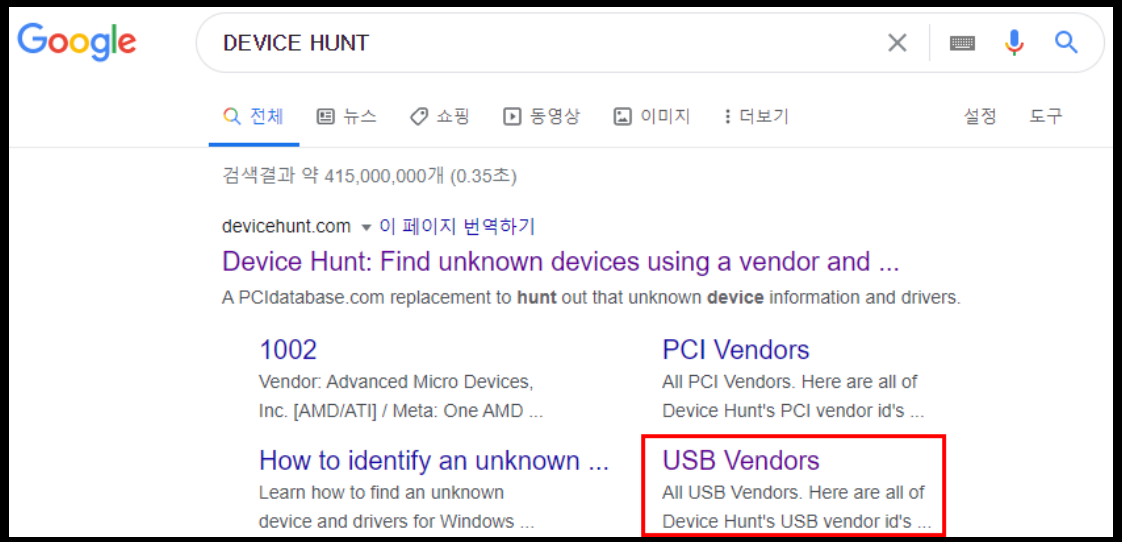
Value Name	Value Type	Data
DeviceDesc	RegSz	@oem61.inf,%iphone.appleusbmux.devicedesc%;Apple Mobile Device USB Device
LocationInformation	RegSz	0000.0014.0000.005.000.000.000.000.000
Capabilities	RegDword	132
Address	RegDword	6
ContainerID	RegSz	{83439688-d8ce-51d5-b3f1-be637738b3bd}
HardwareID	RegMultiSz	USB₩VID_05AC&PID_12A8&REV_0802&MI_01 USB₩VID_05AC&PID_12A8&MI_01
CompatibleIDs	RegMultiSz	USB₩Class_ff&SubClass_fe&Prot_02 USB₩Class_ff&SubClass_fe USB₩Class_ff
ClassGUID	RegSz	{88bae032-5a81-49f0-bc3d-a4ff138216d6}
Service	RegSz	WINUSB
UpperFilters	RegMultiSz	WUDFRd AppleKmdfFilter
Driver	RegSz	{88bae032-5a81-49f0-bc3d-a4ff138216d6}₩0001
Mfg	RegSz	@oem61.inf,%aapl%;Apple, Inc.
FriendlyName	RegSz	@oem61.inf,%iPhone.AppleUsbMux.DeviceDesc%;Apple Mobile Device USB Device
ConfigFlags	RegDword	0

Apple USB Model information

Value Name	Value Type	Data
DeviceDesc	RegSz	Apple iPhone
LocationInformation	RegSz	0000.0014.0000.005.000.000.000.000.000
Capabilities	RegDword	128
Address	RegDword	5
ContainerID	RegSz	{83439688-d8ce-51d5-b3f1-be637738b3bd}
HardwareID	RegMultiSz	USB₩VID_05AC&PID_12A8&REV_0802&MI_00 USB₩VID_05AC&PID_12A8&MI_00
CompatibleIDs	RegMultiSz	USB₩Class_06&SubClass_01&Prot_01 USB₩Class_06&SubClass_01 USB₩Class_06
ConfigFlags	RegDword	0
ClassGUID	RegSz	{eec5ad98-8080-425f-922a-dabf3de3f69a}
Driver	RegSz	{eec5ad98-8080-425f-922a-dabf3de3f69a}₩0002
LowerFilters	RegMultiSz	WinUsb
Mfg	RegSz	Apple Inc.
Service	RegSz	WUDFWpdMtp
FriendlyName	RegSz	Apple iPhone

Apple Smart Phone Model information

3.Practice



Device Hunt(USB Vendors)

USB Search (Vendor & Device)

3.Practice

USB	04E8	Samsung Electronics Co., Ltd	6865	Galaxy (PTP mode)
USB	04E8	Samsung Electronics Co., Ltd	6866	Galaxy (debugging mode)
USB	04E8	Samsung Electronics Co., Ltd	6860	Galaxy series, misc. (MTP mode)
USB	04E8	Samsung Electronics Co., Ltd	6863	Galaxy series, misc. (tethering mode)
USB	04E8	Samsung Electronics Co., Ltd	6864	GT-I9070 (network tethering, USB debugging enabled)

Samsung Vendor & Product

Device Details

Galaxy series, misc. (MTP mode)

Type	*Information*
ID	6860

Vendor Details

Samsung Electronics Co., Ltd

Type	*Information*
ID	04E8

Check Result

3.Practice

USB	05AC	Apple, Inc.	12AA	iPod Touch 5.Gen [A1421]
USB	05AC	Apple, Inc.	12A6	iPad 3 (3G, 16 GB)
USB	05AC	Apple, Inc.	12A8	iPhone5/5C/5S/6
USB	05AC	Apple, Inc.	12A4	iPad 3 (wifi)
USB	05AC	Apple, Inc.	12A5	iPad 3 (CDMA)

Apple Vendor & Product

Device Details

iPhone5/5C/5S/6

Type	*Information*
ID	12A8

Vendor Details

Apple, Inc.

Type	*Information*
ID	05AC

Check Result

ETC?

Value Name	Value Type	Data	V...
DeviceDesc	RegSz	EPSON M205 Series	
Capabilities	RegDword	192	
ConfigFlags	RegDword	0	
ContainerID	RegSz	{9c3fee8a-5dec-5d82-ab7a-ae9945dbecf3}	F...
HardwareID	RegMultiSz	USBPRINT₩EPSONM205_SeriesE16B EPSONM205_SeriesE16B	F...
CompatibleIDs	RegMultiSz	USBPRINT₩1284_CID_EpsonRGB 1284_CID_EpsonRGB CID_MS_GENERICPRINT	
ClassGUID	RegSz	{4d36e979-e325-11ce-bfc1-08002be10318}	F...
Driver	RegSz	{4d36e979-e325-11ce-bfc1-08002be10318}₩0001	7...
Mfg	RegSz	@oem76.inf,%epson%;EPSON	F...

Print USB information

Value Name	Value Type	Data
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	RegDword	16
Address	RegDword	1
ContainerID	RegSz	{f5fdcbf7-97d1-5161-b4fb-93ede5d65f7a}
HardwareID	RegMultiSz	USBSTOR₩DiskSanDisk_Cruzer_Blade____1.00 USBSTOR₩DiskSanDisk_Cruzer_Blade____ USBSTOR₩DiskSanDisk_ USBSTOR₩SanDisk_Cruzer_Blade____1 SanDis...
CompatibleIDs	RegMultiSz	USBSTOR₩Disk USBSTOR₩RAW GenDisk
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	RegSz	disk
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}₩0001
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Standard disk drives)
FriendlyName	RegSz	SanDisk Cruzer Blade USB Device
ConfigFlags	RegDword	0

General USB information

Thank You for listening!