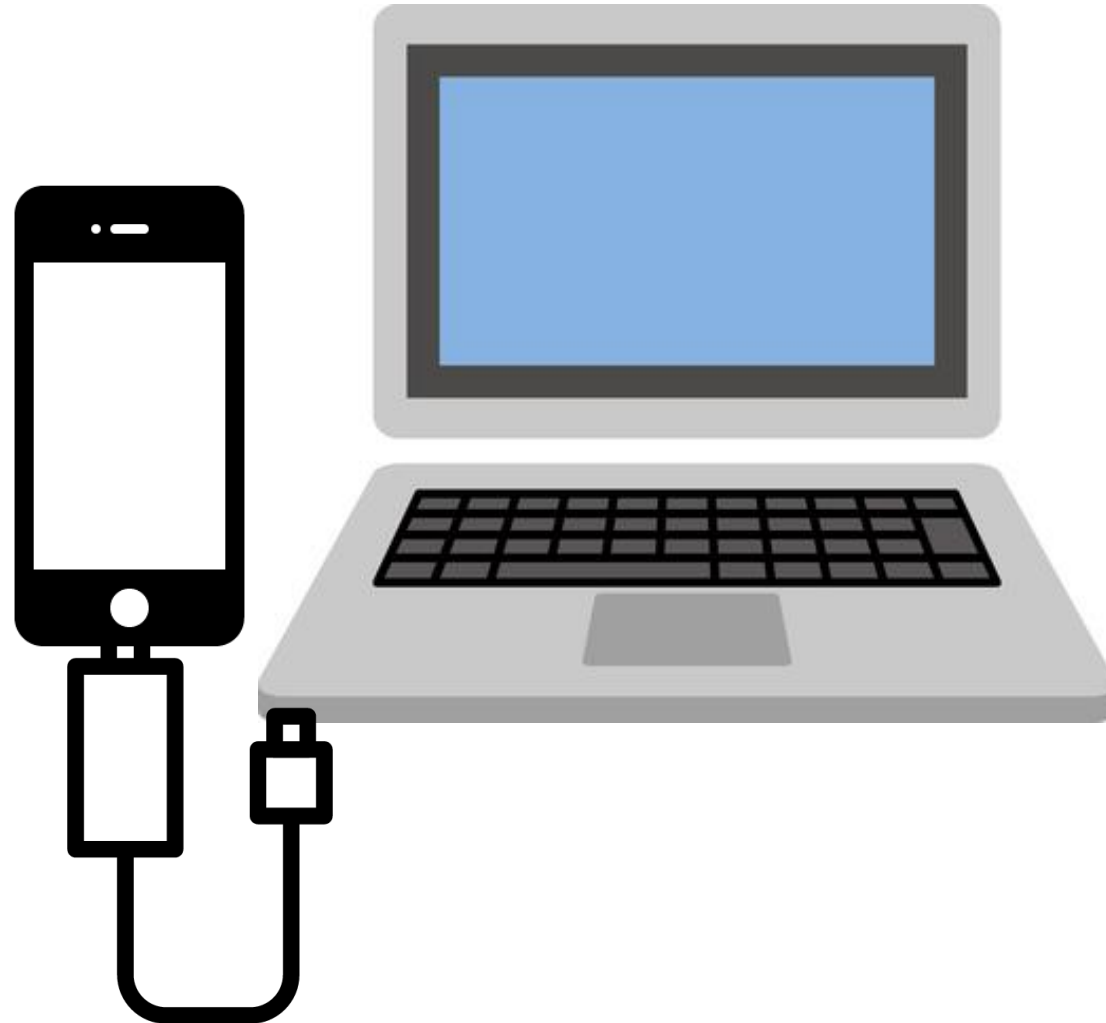


Smart Phone connection Trace?



TOOL

-FTK Imager

-Registry Explorer

-USB 케이블

-Smart Phone (Samsung & Apple)

SYSTEM FILE



FTK Imager



SYSTEM

Evidence Tree

C:\W

NONAME [NTFS]

[orphan]

[root]

\$BadClus

\$Extend

\$Recycle.Bin

\$Secure

\$UpCase

Documents and Settings

Download

Garena

Intel

kali-linux.iso

Netmarble

Nexon

PDFStreamDumper

Program Files

Program Files (x86)

ProgramData

recovery

File List

Name	Size	Type	Date Modified
SOFTWARE.LOG1	4,096	Regular File	2018-04-11 ...
SOFTWARE.LOG1		\$I30 INDX Entry	
SOFTWARE.LOG2	28,583	Regular File	2018-04-11 ...
SOFTWARE{8ebe95c6...	64	Regular File	2018-04-12 ...
SOFTWARE{8ebe95c6...	512	Regular File	2018-04-12 ...
SOFTWARE{8ebe95c6...	512	Regular File	2018-04-12 ...
SYSTEM	24,320	Regular File	2019-01-03 ...
SYSTEM.LOG1	6,043	Regular File	2018-04-11 ...
SYSTEM.LOG2	1,536	Regular File	2018-04-11 ...
SYSTEM{ad35a797-3...	64	Regular File	2018-04-12 ...
SYSTEM{ad35a797-3...	512	Regular File	2018-04-12 ...
SYSTEM{ad35a797-3...	512	Regular File	2018-04-12 ...
SYSTEM~1		\$I30 INDX Entry	
userdiff	8	Regular File	2018-05-26 ...
userdiff LOG1	8	Regular File	2018-05-26

Properties

Name	SYSTEM
File Class	Regular File
File Size	24,903,680
Physical Size	24,903,680
Start Cluster	14,675,972
Date Accessed	2019-01-03 오후 5:00:43
Date Created	2018-04-11 오후 9:04:33
Date Modified	2019-01-03 오후 5:00:43
Encrypted	False
Compressed	False
Actual File	True
Start Sector	117,407,776

Hex Value Interpreter

00000000	72 65 67 66 7D D5 07 00-7C D5 07 00 00 00 00 00	regf}õ... õ.....
00000010	00 00 00 00 01 00 00 00-05 00 00 00 00 00 00 00Pw.....
00000020	01 00 00 00 20 00 00 00-00 50 77 01 01 00 00 00S-Y-S-T-E-M.....
00000030	53 00 59 00 53 00 54 00-45 00 4D 00 00 00 00 00
00000040	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000050	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000070	96 A7 35 AD DF 3D E8 11-A9 DB E4 1D 2D B3 B7 B1	-\$5-B=è-ëÜä--³ ±
00000080	96 A7 35 AD DF 3D E8 11-A9 DB E4 1D 2D B3 B7 B1	-\$5-B=è-ëÜä--³ ±
00000090	01 00 00 00 97 A7 35 AD-DF 3D E8 11 A9 DB E4 1D\$5-B=è-ëÜä-
000000a0	2D B3 B7 B1 72 6D 74 6D-51 0B DE E1 85 A3 D4 01	--³ ±rmtmQ-Pá-£Ö-
000000b0	4F 66 52 67 01 00 00 00-00 00 00 00 00 00 00	OfRg.....
000000c0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000d0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000e0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000f0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000100	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000110	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000120	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000130	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000140	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000150	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000160	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000170	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000180	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000190	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000001a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000001b0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000001c0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00

Properties

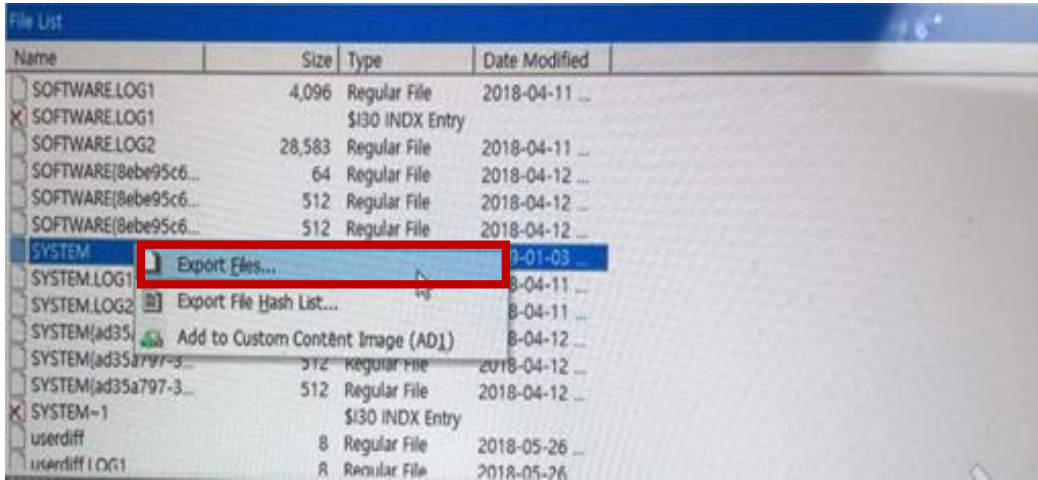
Hex Value Interpreter

Cursor pos = 0; dus = 14675972; log sec = 117407776

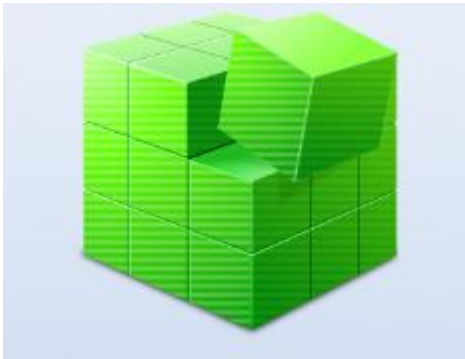
For User Guide, press F1

경로 : C: - Windows - System32 - config - SYSTEM

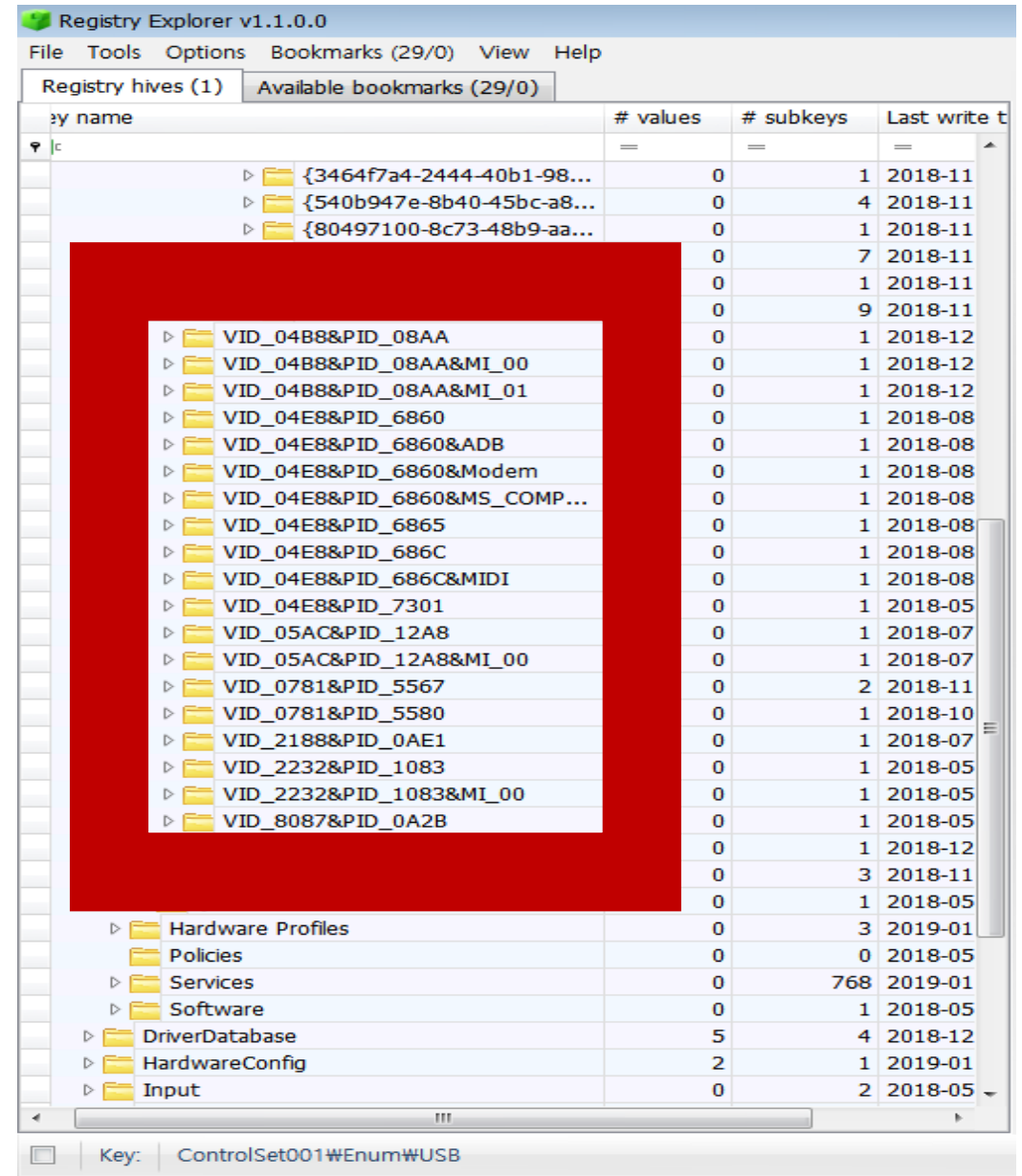
Export Files



Export Files...



Registry Explorer



경로 : ControlSet001 - Enum - USB

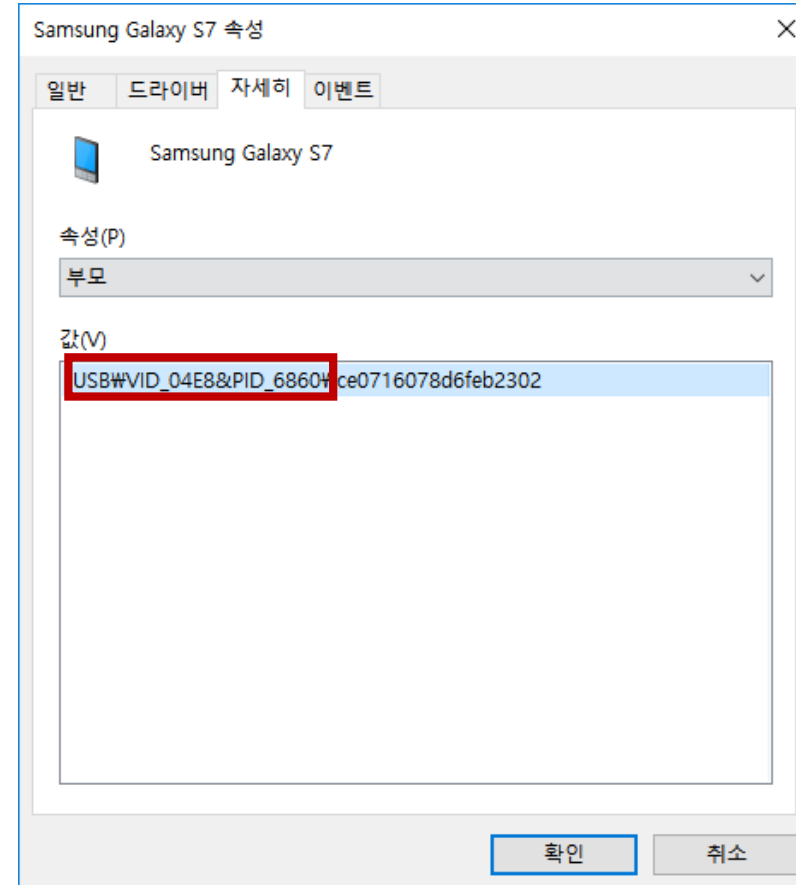
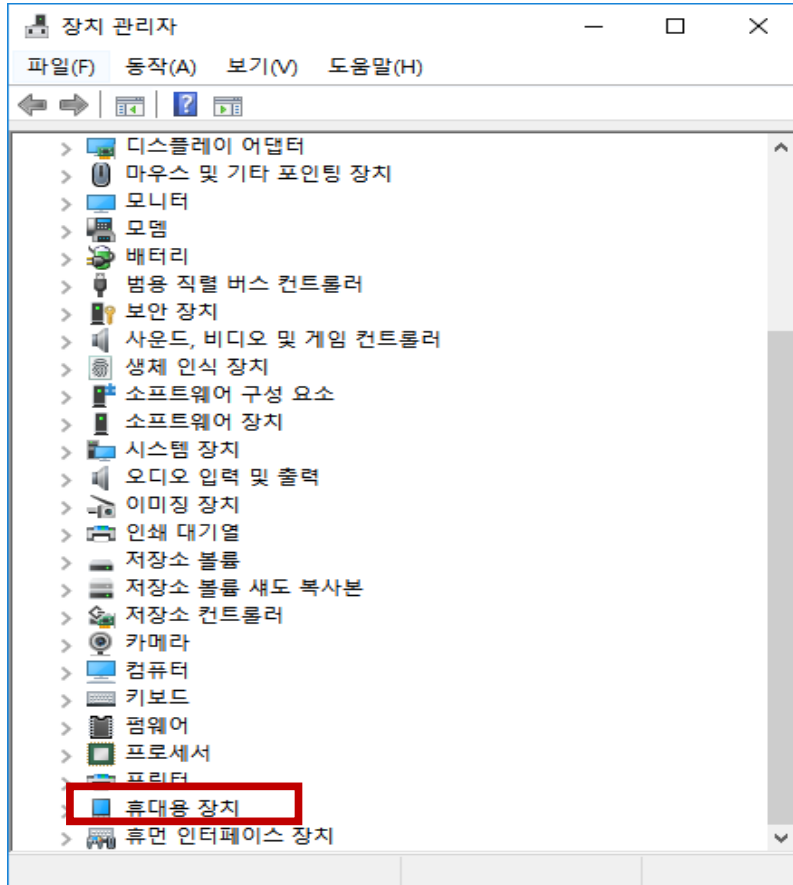
USB Device VID & PID

VID (Vender ID) : 제조사 ID

PID (Product ID) : 그 제조사의 제품 고유번호

VID & PID : 다른 USB와 겹치지 않는 유일한 식별번호

VID & PID Check



검색 (Search) ➡ 장치 관리자 ➡ 휴대용 장치 ➡ 속성

Check

DeviceDesc	RegSz	SM-G930L
------------	-------	----------

VID_04E8&PID_6860

VID_04E8&PID_6860&MS_COMP...

6&1ae49685&0&0000

6&1907a79e&0&0000

Key name	# values	# subkeys	Last write
ROOT_HUB30	0	1	2018-
VID_8087&PID_0A2B	0	1	2018-
VID_04E8&PID_7301	0	1	2018-
VID_2232&PID_1083	0	1	2018-
2232&PID_1083&MI_00	0	1	2018-
05AC&PID_12A8	0	1	2018-
57ba2090e9f9d947ced21fb5...	14	2	2019-
2188&PID_0AE1	0	1	2018-
0000&PID_0002	0	2	2018-
04E8&PID_6865	0	1	2018-
0781&PID_5580	0	1	2018-
0781&PID_5567	0	2	2018-
048D&PID_1181	0	1	2018-
0488&PID_08AA	0	1	2018-
0488&PID_08AA&MI_00	0	1	2018-
0488&PID_08AA&MI_01	0	1	2018-
VID_090C&PID_1000	0	1	2019-
VID_04E8&PID_6860&MS_COMP...	0	1	2019-
VID_04E8&PID_6860&Modem	0	1	2019-
VID_04E8&PID_6860&ADB	0	1	2019-
VID_04E8&PID_686C	0	1	2019-
VID_04E8&PID_686C&MIDI	0	1	2019-
VID_04E8&PID_6860	0	2	2019-
VID_04E8&PID_6860&MS_COMP...	0	2	2019-
6&1ae49685&0&0000	13	2	2019-
6&1907a79e&0&0000	13	2	2019-
VID_04E8&PID_6860&Modem	0	2	2019-
VID_04E8&PID_6860&ADB	0	1	2019-
Maps	8	3	2018-
WaaS	0	2	2018-
WPA	0	39	2018-
HardwareConfig	2	1	2019-
RNG	2	0	2019-
Setup	15	13	2019-
MountedDevices	25	0	2019-

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack
DeviceDesc	RegSz	SM-G930L	6E-00-66-00-2C-00-25-00-67-00-65-00-6E-00-65-00-72-00-69-00-63-00-6D-00-74-00-70-00-2E-00-64-00-65-00-76-00-69-00-63-00-6...
Capabilities	RegDword	128	
Address	RegDword	3	
ContainerID	RegSz	{3f3c3bbe-5029-59...	00-00-01-00-00-00
HardwareID	RegMultiSz	USB\VID_04E8&PI...	20-00
CompatibleIDs	RegMultiSz	USB\MS_COMP_M...	32-61-37-34-64-65
ConfigFlags	RegDword	0	
ClassGUID	RegSz	{eec5ad98-8080-42...	00-00-00-00-00-00
Driver	RegSz	{eec5ad98-8080-42...	73-70-6F-72
LowerFilters	RegMultiSz	WinUsb	20-80-4F-00
Mfg	RegSz	Samsung Electronics...	54-00-50-00-20-00-A5-C7-58-CE-29-00-00-00-A3-00
Service	RegSz	WUDFWpdMtp	4E-4E-45-43-54-20
FriendlyName	RegSz	Samsung Galaxy S7	

Type viewer

Slack viewer

Binary viewer

Value name

DeviceDesc

Value type

RegSz

Value

SM-G930L

Raw value

53-00-4D-00-2D-00-47-00-39-00-33-00-30-00-4C-00-00-00

Slack

6E-00-66-00-2C-00-25-00-67-00-65-00-6E-00-65-00-72-00-69-00-63-00-6D-00-74-00-70-00-2E-00-64-00-65-00-76-00-69-00-63-00-65-00-64-00-65-00-73-00-63-00-25-00-...

Key: ControlSet001\Enum\USB\VID_04E8&PID_6860&MS_COMP_MTP\SAMSUNG_Android\61907a79e00000

Value: DeviceDesc

Collapse all hives

Selected hive: SYSTEM.cpy6

Last write: 2019-01-09 11:17:28

13 of 13 values shown (100.00%)

Load complete

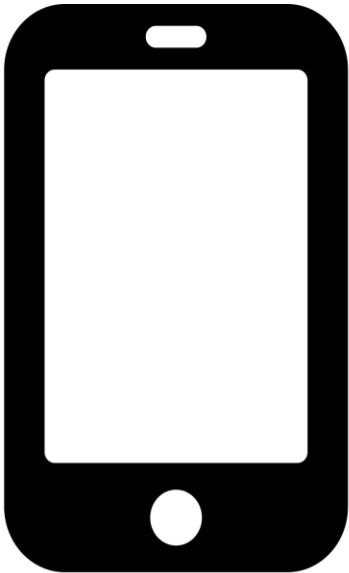
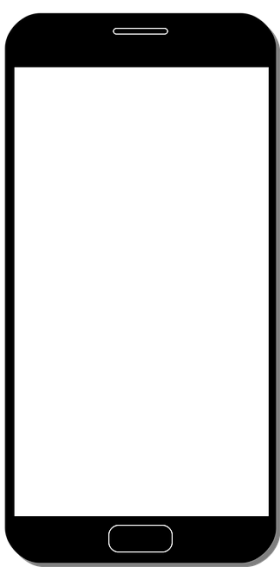
Hidden keys: 0

11

Last write:	2019-01-09 11:17:28	FriendlyName	RegSz	Samsung Galaxy S7
-------------	---------------------	--------------	-------	-------------------

Apple & Samsung

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
DeviceDesc	RegSz	Apple iPhone	67-00-65-00-6E-00-65-00-72-00-69-00-63-00-6D-00-74-00-70-00-2E-00-64-00-65-00-76-00-69-00-63-00-65-00-64-00-65-00-73-...
LocationInformation	RegSz	Port_#0005.Hub_...	D3-4B
Capabilities	RegDword	148	
Address	RegDword	5	
ContainerID	RegSz	{83439688-d8ce-5...	37-34-61-65-36-62
HardwareID	RegMultiSz	USB\VID_05AC&P...	
CompatibleIDs	RegMultiSz	USB\Class_06&Su...	32-00-34-00
ConfigFlags	RegDword	32	
ClassGUID	RegSz	{eec5ad98-8080-4...	00-00-01-00-00-00
Service	RegSz	WUDFWpdMtp	41-00-38-00-00-00
Mfg	RegSz	Apple Inc.	2C-00-25-00-67-00-65-00-6E-00-65-00-72-00-69-00-63-00-6D-00-66-00-67-00-25-00-38-00-28-00-5C-D4-00-C9-20-00-4D-00-54-...
Driver	RegSz	{eec5ad98-8080-4...	28-7B-A5-00
LowerFilters	RegMultiSz	WinUsb	76-6B-08-00
FriendlyName	RegSz	Apple iPhone	00-00



Search Results

Type	Vendor ID	Vendor Name	Device ID	Device Name	More
USB	05AC	Apple, Inc.	12A8	iPhone5/5C/5S/6	Vendor Device

Search Results

Type	Vendor ID	Vendor Name	Device ID	Device Name	More
USB	04E8	Samsung Electronics Co., Ltd	6860	Galaxy series, misc. (MTP mode)	Vendor Device

