





Profile Windows XP USB Keys/Thumbdrives

XP USB KEY/Thu	XP USB KEY/Thumbdrive	
1. Write Down Vendor, Product, Version		
SYSTEM\CurrentControlSet\Enum\USBSTOR	Vendor =	
	Product =	
	Version =	
2. Write Down Serial Numbers		
SYSTEM\CurrentControlSet\Enum\USBSTOR	Serial Number =	
3. Determine Parent Prefix ID		
SYSTEM\CurrentControlSet\Enum\USBSTOR	Parent Prefix ID=	
4. Determine Vendor-ID (VID) and Product-(PID)	
SYSTEM\CurrentControlSet\Enum\USB ->	VID_XXXX =	
Perform search for S/N	PID_YYYY =	
5. Determine Drive Letter Device Mapped To		
SYSTEM\MountedDevices-> Perform search for	Drive =	
Parent Prefix ID in the Drive Letter		
6. Write Down	Volume GUIDs	
SYSTEM\MountedDevices-> Perform Search for	{GUID} =	
Parent Prefix ID in the GUIDs		
7. Find User That Used The Specific USB Device		
NTUSER.DAT\Software\Microsoft\Windows\	User =	
CurrentVersion\Explorer\MountPoints2->		
Search for Device GUID		
8. Discover First Time De		
C:\Windows\setupapi.log -> Perform search	Time/Timezone =	
for Serial Number		
9. Determine First Time Device Cor		
SYSTEM\CurrentControlSet\Control\Devic eClasses\{53f56307-b6bf-11d0-94f2-	Time/Timezone =	
00a0c91efb8b}-> Perform search for S/N		
Or SYSTEM\CurrentControlSet\Enum\USB\		
VID_XXXX&PID_YYYY -> Perform search for Serial		
Number (Last Written Time of Serial Number Key)		
10. Determine Last Time D	Nevice Connected	
NTUSER//Software/Microsoft/Windows/Cur	Time/Timezone =	
rentVersion/Explorer/MountPoints2/{GUI		
D > Perform search for Device {GUID}		
= j = 1 citoriti scarcii foi bevice (doib)		











Profile VISTA USB Key/Thumbdrives

VISTA USB KEY/Thumbdrive		
1. Write Down Vendor, Product, Version		
SYSTEM\CurrentControlSet\Enum\USBSTOR	Vendor =	
	Product =	
	Version =	
2. Write Down Serial	Numbers	
SYSTEM\CurrentControlSet\Enum\USBSTOR	Serial Number =	
3. Determine Vendor-ID (VID) and Product-(PID)		
SYSTEM\CurrentControlSet\Enum\USB ->	VID_XXXX =	
Perform search for S/N	PID_YYYY =	
4. Write Down Volume GUIDs		
SYSTEM\MountedDevices-> Perform Search for	GUID =	
Serial Number		
5. Determine Drive Letter and Volume Name Device Mapped To		
SOFTWARE\Microsoft\Windows Portable	Drive Letter =	
Devices\Devices-> Perform Search for Serial	Volume Name=	
Number and Match with Volume Name		
6. Find User That Used The Specific USB Device		
NTUSER.DAT\Software\Microsoft\Windows\C	User =	
urrentVersion\Explorer\MountPoints2->		
Search for Device GUID		
7. Discover First Time Device Connected		
<pre>C:\Windows\inf\setupapi.dev.log -> Perform</pre>	Time/Timezone =	
search for Serial Number		
8. Determine First Time Device Conn	acted After Last Reheat	
SYSTEM\CurrentControlSet\Enum\USBSTOR\	Time/Timezone =	
Vendor_Product_Version -> Perform search for	Time/Timezone =	
Serial Number (Last Written Time of Serial Number Key)		
<pre>SYSTEM\CurrentControlSet\Control\Device</pre>		
Classes\{53f56307-b6bf-11d0-94f2-		
00a0c91efb8b}-> Perform search for S/N (Last		
Written Time of Key that has Serial Number and		
Vendor/Product/Revision)		
9. Determine Last Time Dev	ice Connected	
SYSTEM\CurrentControlSet\Enum\USB\	Time/Timezone =	
VID_XXXX&PID_YYYY -> Perform search for Serial	inite, initezone	
Number (Last Written Time of Serial Number Key)		
or		
NTUSER//Software/Microsoft/Windows/Curr		
antitongian /Euroleman /Marris Daintes / (Crita)		
<pre>entVersion/Explorer/MountPoints2/{GUID}</pre>		

http://forensics.sans.org http://twitter.com/sansforensics









Profile Windows 7 USB Keys/Thumbdrives

Win7 USB Key/Thumbdrive		
1. Write Down Vendor, Product, Version		
SYSTEM\CurrentControlSet\Enum\USBSTOR	Vendor =	
	Product =	
	Version =	
2. Write Down Serial Numbers		
SYSTEM\CurrentControlSet\Enum\USBSTOR	Serial Number =	
3. Determine Vendor-ID (VID) and Product-(PID)		
SYSTEM\CurrentControlSet\Enum\USB ->	VID_XXXX =	
Perform search for S/N	PID_YYYY =	
4. Determine Drive Letter De	vice Mapped To	
SYSTEM\MountedDevices-> Perform search for	Drive =	
Serial Number in the Drive Letters		
5. Write Down Volume GUIDs		
SYSTEM\MountedDevices-> Perform Search for	GUID =	
Serial Number in the GUIDs		
6. Find User That Used The Specific USB Device		
NTUSER.DAT\Software\Microsoft\Windows\C	User =	
urrentVersion\Explorer\MountPoints2->		
Search for Device GUID		
7. Discover First Time Device Connected		
C:\Windows\inf\setupapi.dev.log -> Perform	Time/Timezone =	
search for Serial Number		
8. Determine First Time Device Conn		
SYSTEM\CurrentControlSet\Enum\USBSTOR\	Time/Timezone =	
<pre>Vendor_Product_Version -> Perform search for</pre>		
Serial Number (Last Written Time of Serial Number Key)		
<u>or</u>		
SYSTEM\CurrentControlSet\Control\Device		
Classes\{53f56307-b6bf-11d0-94f2-		
00a0c91efb8b}-> Perform search for S/N (Last		
Written Time of Key that has Serial Number and		
Vendor/Product/Revision)		
9. Determine Last Time Dev		
	Time/Timezone =	
VID_XXXX&PID_YYYY -> Perform search for Serial		
Number (Last Written Time of Serial Number Key)		
Or NTUSER//Software/Microsoft/Windows/Curr		
entVersion/Explorer/MountPoints2/{GUID}		
-> Perform search for Device {GUID}		
י רפווטוווו שבמוניו וטו שבמוני נשטושן		

http://forensics.sans.org http://twitter.com/sansforensics







http://forensics.sans.org http://twitter.com/sansforensics

