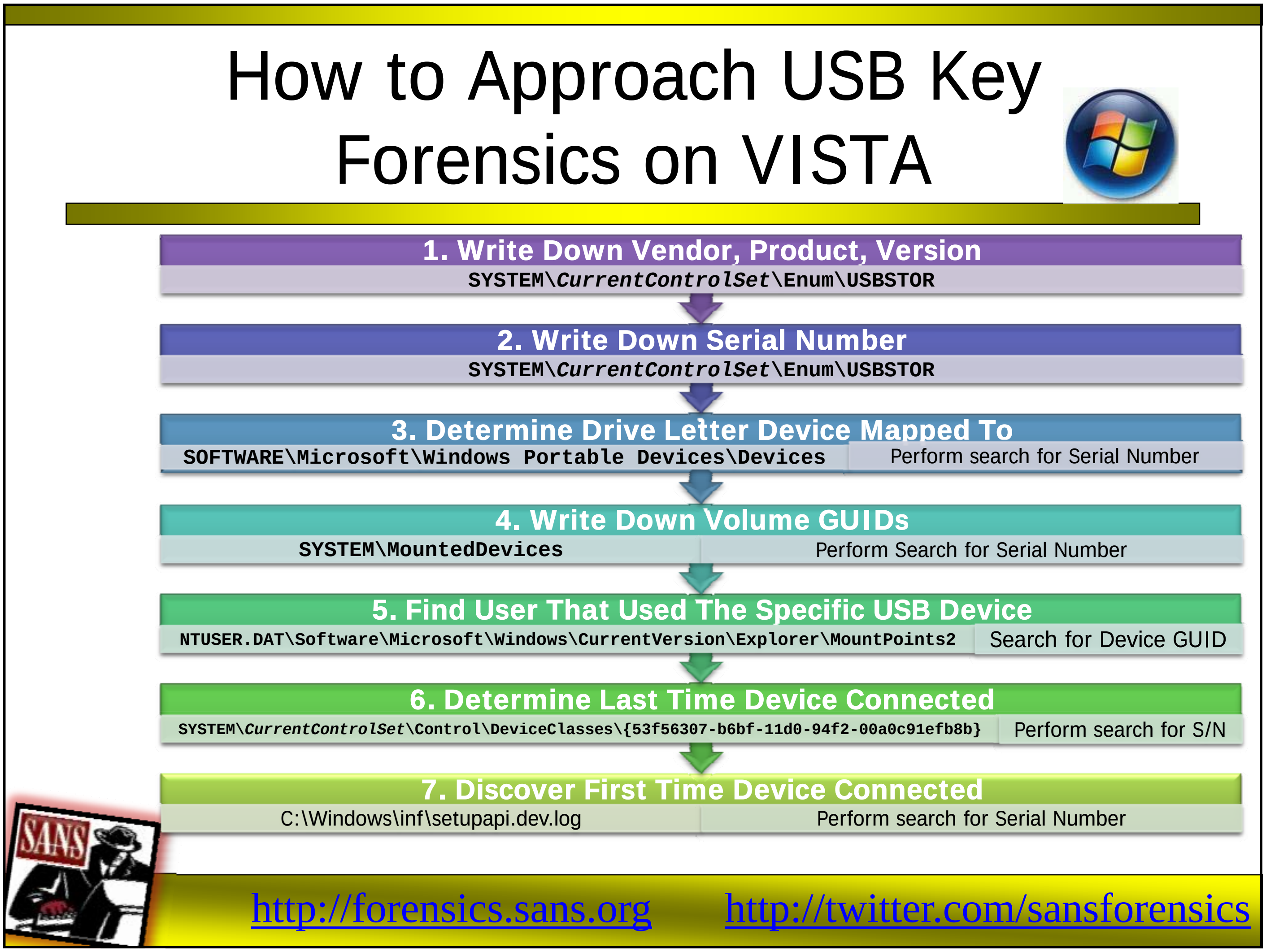

How to Approach USB Key Forensics on VISTA

1. Write Down Vendor, Product, Version

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

2. Write Down Serial Number

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

3. Determine Drive Letter Device Mapped To

`SOFTWARE\Microsoft\Windows Portable Devices\Devices` — Perform search for Serial Number

4. Write Down Volume GUIDs

`SYSTEM\MountedDevices` — Perform Search for Serial Number

5. Find User That Used The Specific USB Device

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2` — Search for Device GUID

6. Determine Last Time Device Connected

`SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}` — Perform search for S/N

7. Discover First Time Device Connected

C:\Windows\inf\setupapi.dev.log — Perform search for Serial Number

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

Profile VISTA/Win7 USB Devices

USBDEVICE 1	
1. Write Down Vendor, Product, Version	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
2. Write Down Serial Numbers	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
3. Determine Drive Letter Device Mapped To	
SOFTWARE\Microsoft\Windows Portable Devices\Devices-> Perform Search for Serial Number	
4. Write Down Volume GUIDs	
SYSTEM\MountedDevices-> Perform Search for Serial Number	
5. Find User That Used The Specific USB Device	
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2-> Search for Device GUID	
6. Determine Last Time Device Connected	
SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}-> Perform search for S/N	
7. Discover First Time Device Connected	
C:\Windows\setupapi.log -> Perform search for Serial Number	

USBDEVICE 2

1. Write Down Vendor, Product, Version	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
2. Write Down Serial Numbers	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
3. Determine Drive Letter Device Mapped To	
SOFTWARE\Microsoft\Windows Portable Devices\Devices-> Perform Search for Serial Number	
4. Write Down Volume GUIDs	
SYSTEM\MountedDevices-> Perform Search for Serial Number	
5. Find User That Used The Specific USB Device	
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2-> Search for Device GUID	
6. Determine Last Time Device Connected	
SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}-> Perform search for S/N	
7. Discover First Time Device Connected	
C:\Windows\setupapi.log -> Perform search for Serial Number	

USBDEVICE 3

1. Write Down Vendor, Product, Version	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
2. Write Down Serial Numbers	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
3. Determine Drive Letter Device Mapped To	
SOFTWARE\Microsoft\Windows Portable Devices\Devices-> Perform Search for Serial Number	
4. Write Down Volume GUIDs	
SYSTEM\MountedDevices-> Perform Search for Serial Number	
5. Find User That Used The Specific USB Device	
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2-> Search for Device GUID	
6. Determine Last Time Device Connected	
SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}-> Perform search for S/N	
7. Discover First Time Device Connected	
C:\Windows\setupapi.log -> Perform search for Serial Number	

USBDEVICE 4	
1. Write Down Vendor, Product, Version	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
2. Write Down Serial Numbers	
SYSTEM\CurrentControlSet\Enum\USBSTOR	
3. Determine Drive Letter Device Mapped To	
SOFTWARE\Microsoft\Windows Portable Devices\Devices-> Perform Search for Serial Number	
4. Write Down Volume GUIDs	
SYSTEM\MountedDevices-> Perform Search for Serial Number	
5. Find User That Used The Specific USB Device	
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2-> Search for Device GUID	
6. Determine Last Time Device Connected	
SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}-> Perform search for S/N	
7. Discover First Time Device Connected	
C:\Windows\setupapi.log -> Perform search for Serial Number	