How to Approach USB Key Forensics on XP

1. Write Down Vendor, Product, Version

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

2. Write Down Serial Number

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

3. Determine Parent Prefix ID

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

4. Determine Drive Letter Device Mapped To

`SYSTEM\MountedDevices` — Perform search for Parent Prefix ID

5. Write Down Volume GUIDs

`SYSTEM\MountedDevices` — Perform Search for Parent Prefix ID

6. Find User That Used The Specific USB Device

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

7. Determine Last Time Device Connected

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

8. Discover First Time Device Connected

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

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

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

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

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