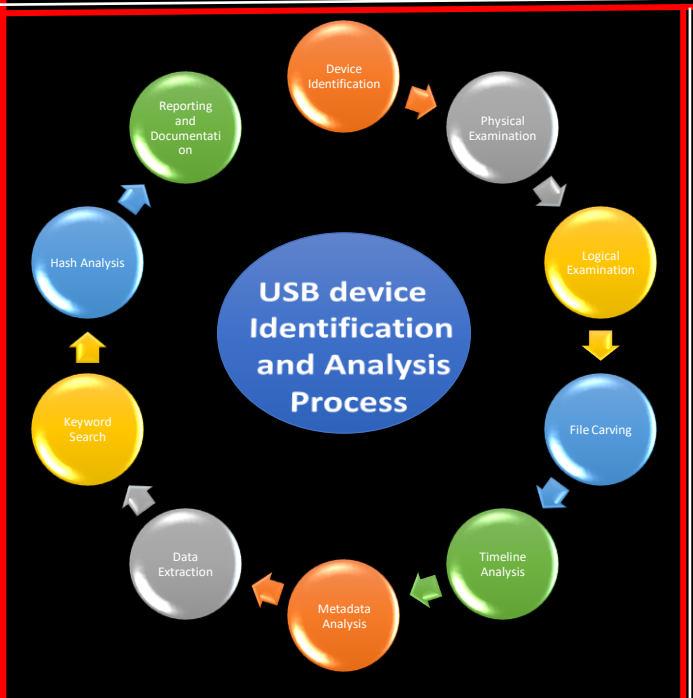
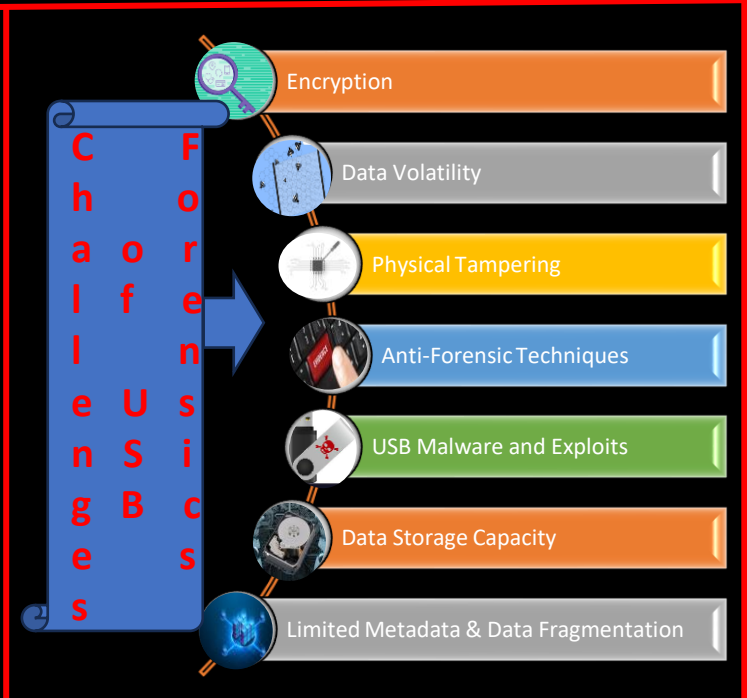
USB Analysis Cheat sheet

External Device/USB Usage Data Extraction Through Registry Hives:

1. To find out Key Identification details like Vendor, Product, Version and Device S/N:
   SYSTEM*CurrentControlSet*\Enum\USBSTOR
2. To find out VID (Vendor ID) and PID (Product ID):
   SYSTEM*CurrentControlSet*\Enum\USB
3. To find out Drive Letter and Volume GUID:
   SYSTEM\MountedDevices
4. To find out the Volume Name:
   SOFTWARE\Microsoft\Windows Portable Devices\Devices
5. To identify the user that plugged in the device:
   NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2
6. To find out Volume S/N:
   SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt
7. To Determine temporal usage of specific USB devices connected to a Windows Machine:
   (i) To find out the First Connected USB devices:
   SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USB_Serial#\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0064
   (ii) To find out the Last Connected USB devices:
   SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USB_Serial#\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0066
   (iii) To find out the Last Disconnected USB devices:
   SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USB_Serial#\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067

To get the information on last plugged in USB devices through PowerShell:
Get-ItemProperty -Path HKLM:\SYStem\CurrentControlSet\Enum\USBSTOR** | Select FriendlyName





USB Devices Data Extraction and Analysis Through Linux:

1. To create a Forensic Image through .dd extension:
   sudo dd if=/dev/sdc1 of=usb.dd bs=512 count=1
2. To create hash of the Image:
   md5sum usb.dd
3. To find out the information about file system, as well as the drive's geometry:
   file usb.dd
4. To find out NTFS boot sector layout and the boot sector information:
   minfo -i usb.dd
5. To obtain general known info, such as allocation structures, layout, and boot blocks, about the device image:
   fstat usb.dd
6. To find out all the files (especially recently deleted files) in each path and information about deleted files:
   fls -rp -f fat32 usb.dd
7. To do the Timeline Analysis:
   (i) First we need to convert data in MAC timeline output format:
   fls -m / -rp -f fat32 ok.dd > usb.fls
   cat usb.fls
   (ii) Run the mactime tool to obtain timeline analysis:
   cat usb.fls > usb.mac
   (iii) To convert this mactime output to human-readable form:
   mactime -b usb.mac > usb.mactime
   cat usb.mactime

USB Malware Attack Flow: