COPY, IMAGING AND CLONING

- Disk cloning and disk imaging are two processes that accomplish the same goal: They copy all of a hard drive's contents. It's possible to clone a disk by using a disk image, but the two are distinctly different in the process they use to copy hard drives. Disk cloning creates a functional one-to-one copy of a hard drive, while disk imaging creates an archive of a hard drive that can be used to make a one-to-one copy.

COPY, IMAGING AND CLONING

Copy and Paste

- Disk images and disk clones are different than just copying and pasting the entire contents of one hard drive to another. When you copy and paste files from one drive to another you're copying only the actual files and not the additional data the hard drive uses to locate and access those files. Things like the master boot record and the file allocation table are not copied to the new hard drive when you copy and paste. A copy and paste backup drive won't boot.

COPY, IMAGING AND CLONING

Disk Cloning

- Disk cloning is the process of copying the entire contents of one hard drive to another including all the information that enables you to boot to the operating system from the drive. A cloning program enables you to make a one-to-one copy of one of your computer's hard drives on another hard drive. This second copy of the hard drive is fully operational and can be swapped with the computer's existing hard drive. If you boot to the cloned drive, its data will be identical to the source drive at the time it was created. A cloned drive can be used to replace its source drive in a computer in the event that something bad happens to the original drive.

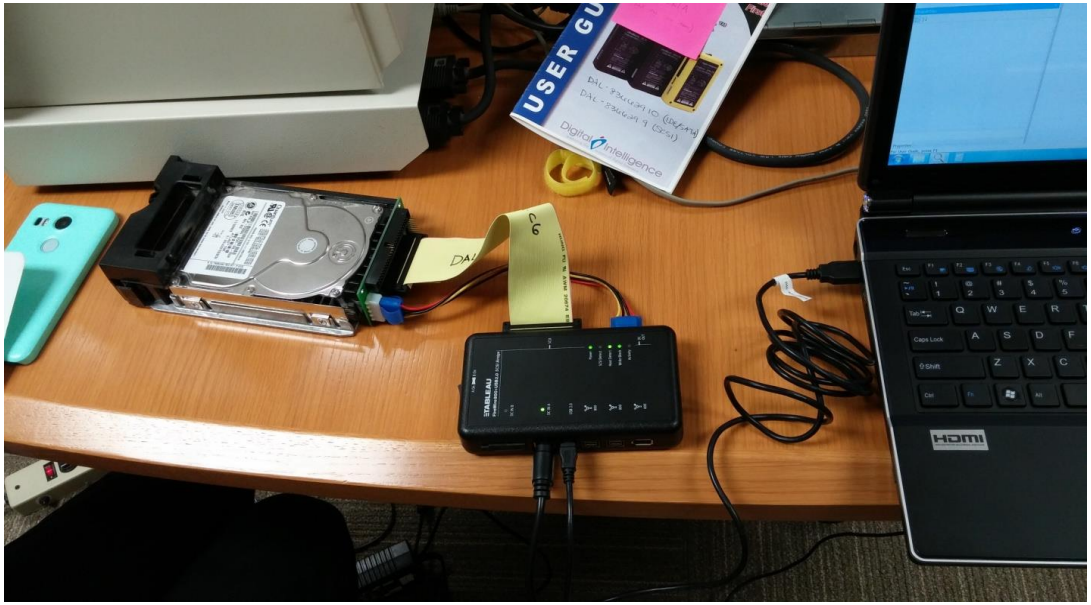
COPY, IMAGING AND CLONING

Disk Imaging

- Disk imaging is the process of making an archival or backup copy of the entire contents of a hard drive. A disk image is a storage file that contains all the data stored on the source hard drive and the necessary information to boot to the operating system. However, the disk image needs to be applied to the hard drive to work. You can't restore a hard drive by placing the disk image files on it; it needs to be opened and installed on the drive with an imaging program. Unlike cloned drives, a single hard drive can store several disk images on it. Disk images can also be stored on optical media and flash drives.

Write blocker

- A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody.
- There are both hardware and software write blockers. Some software write blockers are designed for a specific operating system. One designed for Windows will not work on Linux. Most hardware write blockers are software independent.



IMAGING PROCESS USING FTK IMAGER

- Navigate to File | Create Disk Image. From the pop-up window, select one of the following source evidence types:
  - Physical disk: This is the whole hard drive, starting from the MBR to the last sector of the hard drive
  - Logical disk: This is one partition from the hard drive. Image file: This is if you need to convert an image from one format to another, that is, from the E01 format to a raw format

IMAGING PROCESS USING FTK IMAGER

RAW

- This is simply a bit-to-bit copy of the hard drive without leaving or adding any single bit. This image format is usually accompanied by a separate file, containing meta information about the image file.

E01

- This is the EnCase evidence file. It contains information that is related to the acquisition process, such as the investigator name, the timestamp, and the typed notes during the acquisition. It calculates the checksum for every 32 KB of data, and at the end of the image file, it adds the MD5 hash for the whole bit stream

IMAGING PROCESS USING FTK IMAGER

AFF

- This is the Advanced Forensics Format, and it is used to store disk images and forensics images' metadata. This is not a proprietary but open format, which can be used with any tool for analysis and won't exclusively work with a single tool.

FORENSIC ARTIFACTS OF WINDOWS OPERATING SYSTEM

- Registry
- Prefetch
- Browsing Artifacts
- Shellbags
- Volume Shadow Copy
- USB devices
- LNK files
- Jump lists
- Timestamp Analysis
- $MFT (Master File Table)
- Amcache
- Shimcache

WINDOWS REGISTRY

- The registry or Windows registry is a database of information, settings, options, and other values for software and hardware installed on all versions of Microsoft Windows operating systems.

Registry root keys (hive name)

- When first opening the Windows Registry Editor, it displays root keys that contain all registry values. Below is a brief description about each of the most common root keys and the values contained in each of them.

WINDOWS REGISTRY

Root Key	Description
HKCR (HKEY_CLASSES_ROOT)	Describes file type, file extension, and OLE information. (Object Linking and Embedding)
HKCU (HKEY_CURRENT_USER)	Contains user who is currently logged into Windows and their settings.
HKLM (HKEY_LOCAL_MACHINE)	Contains computer-specific information about the hardware installed, software settings, and other information. The information is used for all users who log on to that computer. This key, and its subkeys, is one of the most frequently areas of the registry viewed and edited by users.
HKU (HKEY_USERS)	Contains information about all the users who log on to the computer, including both generic and user-specific information.
HKEY_CURRENT_CONFIG (HKCC)	The details about the current configuration of hardware attached to the computer.

WINDOWS REGISTRY

- Registry is a giant database contains information regarding operating system functions. It also stores programs and settings for program.

- Registry itself found in "c:\windows\system32\config"

- DEFAULT, SAM, SECURITY, SOFTWARE and SYSTEM. These are the most common and important registry hives. All of the hives are found in same location. "c:\windows\system32\config" .Even auto backup of these hives is been stores by windows in Regback folder. In regedit, you will find these hives in HKLM (Hives Key Local Machine)

- In every profile there is a file named as "NTUSER.DAT" Which means HKCU (Hives Key Current User) in registry. It is located in C:\users\username\NTUSER.DAT (Note: You have to uncheck system protected files from hidden menu)

WINDOWS REGISTRY

- **HKCU(ntuser.dat)\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer**

\RecentDocs – Shows most recent open documents
\RunMRU – Shows MRU (Most Recent Used) run command
\TypedPaths – shows what was typed in path of directory
\UserAssist – Shows what program was executed and how many time it was executed by which user

- **"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"**

Above Hive shows startup programs when computer is booting up. It can also be found in task manager.

- **"HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR"**

PREFETCH

- Each time that you run an application in your system, a Prefetch file which contains information about the files loaded by the application is created by Windows operating system. The information in the Prefetch file is used for optimizing the loading time of the application in the next time that you run it.

- Tool used for analysis is Winprefetchview by NirSoft

SHELLBAGS

- Shellbags analysis is done by many automated tool like shellbags explorer. It stores data related to path opened on computer. In forensics it is important to identify some directories which is not available anywhere in computer. It shows at some point of time it was existing in a computer. It could be even in external drive also.

- Tool used for analysis is Shellbag Explorer

VOLUME SHADOW COPY

- Windows has included the Volume Shadow Copy Service in it's releases since Windows XP.
- Windows Shadow Copy is a service that either manually or automatically creates backup copies of disk volumes. These backups are automatically created when Windows performs either a scheduled backup or a system restore point. This happens before Windows Updates are installed, or when Windows determines that it is time to create a new system restore point
- Windows Shadow Volumes are important to digital forensics because they can provide additional data that otherwise would not be available. They can allow a forensic investigator to recover deleted files, and to learn what was taking place on a system before he/she began the investigation.

- Tool used for analysis is shadowcopyview

USB DEVICES

Common Artifact Locations

HKLM\SYSTEM\CurrentControlSet\Enum\USB < VID / PID
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR < Class ID / Serial #

HKLM\SYSTEM\MountedDevices
- Find Serial # to obtain the Drive Letter of the USB device
- Find Serial # to obtain the Volume GUID of the USB device

HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices
- Find Serial # and then look for FriendlyName to obtain the Volume Name of the USB device

***NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2**
*HKCU on a live system

XP: **%SYSTEMROOT%\setupapi.log**
Vista and later: **%SYSTEMROOT%\inf\setupapi.dev.log**

%SYSTEMROOT%\AppCompat\Programs\Amcache.hve

LNK FILES

- The Windows Shortcut file has the extension .lnk. It basically is a metadata file, specific for the Microsoft Windows platform and is interpreted by the Windows Shell.
- Details can be found from LNK files are as follow:
  - Original Path of target file
  - Timestamp for the target file and link file. (MAC)
  - Size of target file
  - Attribute associated with target file (read-only, hidden, system etc…)
  - System name, volume name, volume serial number and sometimes the MAC address of the system on which the link file is present
  - Whether the file resource is local or located on a remote system.
- LNK files can be found at this path:

"C:\Users\Akash\AppData\Roaming\Microsoft\Windows\Recent (It will show recent items)"

- A tool named LNK Explorer (LECmd.exe) is command line utility written by Eric Zimmerman used for carving LNK files. To use that tool use this command: "LECmd.exe –d (Directory) c:\users\Akash\AppData\Roaming\Microsoft\Windows\Recent -q --csv .\"

JUMP LISTS

- Jump Lists are a new Windows 7 Taskbar feature that gives the user quick access to recently accessed application files and actions. Whenever you right click on icon of program shows in taskbar you will find jump lists.

- It will show you recent files opened and commons tasks associated with that file.

- Jumplists will be found at this path: "C:\Users\Akash\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations" (AutomaticDestinations folder will not be visible in windows explorer. It can be found under cmd)

- With the jumplist analysis, you can get information like what was recently opened in respective application. For ex. In VLC media player, which files have been open, you can find out using jumplist.

- Jump list Explorer is the tool used to parse this jumplist files. This tool is available in both GUI and CLI version. To use this tool follow this command: "JLECmd.exe -f C:\Users\Akash\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\faef7def55a1d4b.automaticDestinations-ms (path of the file) --csv .\"

- Another tool JumpListView from nirsoft can be used to see the jumplist data

Timestamp Analysis

- NTFS is the only file system stores record about birth or creation time of any file. In Linux there is no birth or creation time. There C stands for change in metadata not in the content.
- Timestamp of any file is stored in $MFT file of NTFS file system.
- In $MFT timestamp is stored in following manner:
  - M – Modified
  - A – Access
  - C- Creation (B)
  - E – Entry Date
- In $MFT, timestamp of the file is stored in two different attributes. Whatever we are seeing in properties of file in windows explorer or in CMD is $STANDARD_INFORMATION ($SI) another copy of timestamp is stored under $FILE_NAME ($FN). $FN can only be modifiable by windows kernel.
- Timestomp.exe is a common anti-forensic tool for timestamp changes. We can give any timestamp to any file. In all such anti-forensic tools, the common thing is they can change the entry in $SI attribute.
- We can look for prefetch file to see that timestomp has been used or not. If you find any such activity, you can use any tool (ex. NirSoft - winprefetchviewer) to parse that prefetch file to know more details about number any last accessed date of timestomp.

$MFT

- The master file table (MFT) is a database in which information about every file and directory on an NT File System (NTFS) volume is stored.

- Detailed information about a file or directory such as the type, size, date/time of creation, date/time of most recent modification and author identity is either stored in MFT entries or in space external to the MFT but described by the MFT entries.

- Tool used for analysis is MFT2CSV, MFTExplorer