**Data theft**

A confidential file from an organization is leaked online.

1. Check what type of confidential information was leaked.
2. Look at the event logs to check when the file was created, and when the file was last accessed. This will be the initial time frame for the analysis.
3. Which users have access to the confidential file
   1. In the Windows registry under HKEY\_USERS
   2. If AD is there, we should get the information from the administrator.
   3. Remote connection - Event logs
4. Check for the User's activities during the initial time frame to find out if there are any suspicious events as mentioned in the next point.
5. Possible ways the file transfer is done:
   1. Personal USB or hard drive.
   2. Through remote connection
   3. Connecting to cloud drives
   4. Sending emails
   5. Printers
   6. Suspicious file executions/unauthorized software installation(Application logs)
   7. FTP

Check for the above events one by one and analyze if the file has been accessed during the time of that event.

1. To check USB activity we go to
   1. Event Viewer > Windows Logs > System, use the event source USBSTOR for the filter to see relevant logs
   2. Event viewer >> system log >> usb events >> usb connection and disconnection will be shown there.
2. Remote connection
   1. Check the Windows event log for remote connections
   2. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication: check for rdp authentication
   3. Check application-specific logs like Teamviewer logs, if there was any screen sharing done on the machine
   4. In case of AD: check if any group policies for remote connections have been changed
3. Cloud-based file-sharing application access like OneDrive/Google Drive
   1. Check for Browser history related to drives
   2. Business one drive logs will be available while personal one drive logs won't be available.
   3. File sharing can also occur with online tools/sites such as sendanywhere.com and wetransfer. (Check browser history and Windows event logs for such info)
4. Data transfer through email
   1. if the organization email has been accessed look at the email server for logs
   2. For personal email, search the browser history
5. Check if anything has been printed to create a hard copy
   1. In the Windows event viewer, check Applications and Services Logs >> Microsoft >> Windows >> Printservice >> Operational to see the printer events.
6. Check when the executable was executed, and what type of activities that executable ran. Verify that the executable was responsible for the suspicious activities
7. Microsoft windows system logs : The system monitor log provides detailed information about the process creation,network creation,file creation.

Jumplist , lnk , shellback usb connection

Application specific logs 2 types

If cloud was synced

File access