Windows Artifacts – Programs

This lesson will focus on artifacts that can be gathered from systems running Windows, specifically focusing on artifacts related to the use of applications and programs on the system. Seeing what files have been run on the system can provide valuable evidence such as: how many times a file has been run, when it was last run, when it was created, full file paths, and more. We will explore the following artifacts:

- **LNK Files**
- **Prefetch Files**
- **Jump List Files**

After this lesson, we have designed a practical exercise where you will be able to try out analyzing files for each of the artifacts that we cover in this lesson. Under each artifact heading we have provided a download link for the tool that you'll need to analyze them in the exercise.

LNK FILES / SHORTCUT ANALYSIS

Artifact Description

LNK files are used by the Windows OS to link one file to another, which is how we can have application shortcuts that work as a redirector – so when we click on a shortcut it will go and find the application wherever it resides in the file system and runs the corresponding application. We can collect valuable metadata from LNK files such as the location of the folder it is linked to, the date the LNK file was created, modified, last accessed, the file size, and more.

Artifact Location

LNK files can be found at: `C:\Users\$USER$\AppData\Roaming\Microsoft\Windows\Recent`

Artifact Analysis

To view these files in a human-readable format, we can use Windows File Analyzer (download this now as we'll use it in the next lesson for a practical activity!)

Transcript

In this video, we will be looking at how to analyze LNK files and file shortcuts to gather useful information from the metadata. First, let's show you where these files are stored on a Windows system.

We need to navigate to the C drive, users, our current user, AppData, roaming, Microsoft, Windows, recent. We can list the contents of this directory to see lots of LNK files for different applications.

We can take a deeper look at these files using Windows File Analyse. We go to File > Analyse shortcuts, and the tool should have already selected the Recent Items location. Click OK, state our Windows OS version, and now we can look through all of the LNK files in one panel. We have information such as the filename, linked path, the date the file was created, written and last accessed, and the size.

We can double click on an LNK file to view it separately in a new pane, making it clearer to read the information. This example here is a PowerPoint file that was last opened on the 29th of May.

We can also click Save to export this information to a new text file making it easy to save information we need to keep.

Alternatively, we can click the copy button and then paste it wherever we want ourselves.

In the practical exercise, you will have a chance to analyze some LNK files yourself and retrieve information about a user's activity!

PREFETCH FILES

Artifact Description

Prefetch files can provide us with incredibly useful information about programs including the name of the application, the path to the executable file, when the program was last run, and when the program was created/installed.

Artifact Location

Prefetch files can be found at: `C:\Windows\Prefetch`

Artifact Analysis

To view these files in a human-readable format, we can use Prefetch Explorer Command Line also known as PECmd.exe (download this now as we'll use it in the next lesson for a practical activity!)

Transcript

> *In this video we're going to show you how to access and analyze prefetch files to see when files were last run, how many times they've been run, and their file paths.*
>
> *First let's show you where these files reside on a Windows system. We want to use an admin-level CMD prompt and head over to the C drive, Windows, prefetch, then list the directory. Inside we can see lots of prefetch files with the .pf file extension.*
>
> *We can see one here for Spotify, one here for Photoshop, one for Discord, and one for chrome.*
>
> *Let's take a look at a prefetch file for Outlook. We can copy it to our desktop so it's easier to work with. We're using a tool called Prefetch explorer command line, or PECmd.exe . So we run a command prompt in the location of the tool's exe file, type the name of the exe follow be the "f" flag, this is how we declare the file we want to input, which in our cause is C:\Users\JBeam\Desktop\ then the Outlook .pf file.*
>
> *At the top of the output we can see how many times this file has been run, the created time, modified time and when it was last accessed. We also have the last run time and some other times that this application has been run. All the other lines in this output are files that are related to the application, stating their full file paths.*
>
> *In the next exercise you will have a chance to analyse some prefetch files to collect information.*

JUMP LIST

Artifact Description

Using the Windows Jump List feature we are able to find two different types of files: *automaticDestination-ms* and *customDestination-ms*. These files contain information about applications that are pinned to the taskbar, such as the file path, timestamps, and application identifiers (AppIDs).

Artifact Location

The Jump List files can be found at: `C:\Users\% USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`
`C:\Users\%USERNAME%\AppData\ Roaming\Microsoft\Windows\Recent\CustomDestinations`

Artifact Analysis

To analyze these files we can use tools such as JumpList Explorer (download this now as we'll use it in the next lesson for a practical activity!).

Transcript

In this video, we'll show you how to access and analyze jump files to identify evidence that can point directly to a user's interactions with a computer.

For the next exercise you will be provided with jump files, but first we'll show you where they're located. If we head over to our C drive, users, our current users jbeam, appdata, roaming, Microsoft, windows, recent, and customdestinations, then use dir to list all of this files in this folder, we can see lots of jump files.

We've already copied some to our desktop, so let's open up JumpList Explorer and import one.

We can see at the top we have the source file path, the file size in the top right, and then we can see that the file path is for a Bit Defender .exe, which is an anti-virus product.

Let's add in another, and this time we can see that it's PowerPoint 2016, 64-bit edition. And under the absolute path we can actually see that name of the powerpoint, when the LNK file was created, modified, and last accessed.

In the activity you'll have a chance to look through some Jump files to determine what applications were used, potential file names that were opened in these applications, and the times they were last accessed.

Quizzes

Lab) Windows Investigation 1

Previous Topic | Back to Lesson | Next Topic

Privacy & Cookies Policy