

Forensics – Windows Prefetch

Presenter: Zeming Yao



Understanding Prefetch Files in Window

Presented by Zeming Yao



Acknowledgement of Country

On behalf of those present I acknowledge the Wurundjeri people of the Kulin Nation who are the traditional custodians of the land on which we now meet. I pay my respect to their Elders: past, present and emerging.

I also pay my respect to all Aboriginal and Torres Strait Islander people of Australia and hope that the path towards reconciliation continues to be shared and embraced.



Topics Covered

- An Introduction to Prefetch
- Prefetch Location
- File Naming Convention
- Prefetch Hash Computation
- Prefetch File Analysis via Timestamps
- Parsing Prefetch Files via PECmd



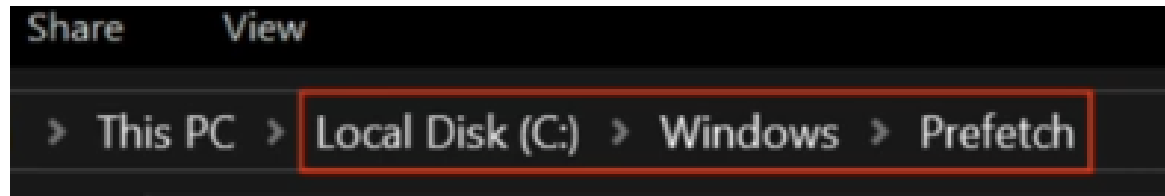
What are Prefetch Files?

- Definition:** Prefetch files are used by Windows to speed up the startup process of applications. They store information about the program's startup and commonly accessed files.
- Prefetch monitors the first **10 seconds** of an application's execution. The goal is to increase the speed of subsequent launches of that application by caching required files and resources into memory, decreasing the need for disk access.
- Range:** include GUI applications , command line, exes, .com. binary



What are Prefetch Files?

- Format:** Prefetch files have a .pf extension (e.g., APPNAME.EXE-XXXXXXXXX.pf).
- Location:** Found in the **C:\Windows\Prefetch** directory.



Purpose of Prefetch Files

- **Faster Boot and Application Load Times:** They optimize the loading of applications by pre-loading necessary data into memory.
- **Tracking Usage:** Helps track how often and when a program is used.

Increase or enhance or improve the user experience



File Naming Convention

File name = Application executable + Hash value

This PC > Local Disk (C:) > Windows > Prefetch

Name	Date modified	Date accessed	Date created
ResPriHMStaticDb.ebd	9/20/2019 9:30 PM	9/20/2019 9:30 PM	9/20/2019 9:30 PM
PfPre_6938f15d.mkd	6/3/2019 1:39 PM	6/3/2019 1:39 PM	6/3/2019 1:39 PM
AUDIODG.EXE-BDFD3029.pf	9/21/2019 11:26 AM	9/21/2019 11:26 AM	9/20/2019 10:44 PM
CMD.EXE-4A81B364.pf	9/21/2019 11:25 AM	9/21/2019 11:25 AM	9/20/2019 10:44 PM
CONHOST.EXE-1B27F204.pf	9/21/2019 11:12 AM	9/21/2019 11:12 AM	9/21/2019 11:12 AM
CONHOST.EXE-1F3E9D7E.pf	9/21/2019 11:25 AM	9/21/2019 11:25 AM	9/20/2019 10:44 PM
CONSENT.EXE-531BD9EA.pf	9/21/2019 11:25 AM	9/21/2019 11:25 AM	9/20/2019 10:46 PM
DLLHOST.EXE-2E884D3E.pf	9/21/2019 11:12 AM	9/21/2019 11:12 AM	9/21/2019 11:12 AM
DLLHOST.EXE-5A984E5F.pf	9/21/2019 11:12 AM	9/21/2019 11:12 AM	9/21/2019 11:12 AM
DLLHOST.EXE-88F23425.pf	9/21/2019 11:11 AM	9/21/2019 11:11 AM	9/21/2019 11:11 AM
DLLHOST.EXE-9037274D.pf	9/21/2019 11:11 AM	9/21/2019 11:11 AM	9/20/2019 10:46 PM
DLLHOST.EXE-B43976F9.pf	9/20/2019 10:46 PM	9/20/2019 10:46 PM	9/20/2019 10:46 PM



Prefetch Hash Generation

Prefetch Hash Generation:

- Full path for file is determined (e.g. C:\WINDOWS\notepad.exe)
- Path is converted to a Unicode string
- Path is converted to a device path (e.g. \Device\HarddiskVolumeX\WINDOWS\notepad.exe)
- Hashing function is applied
- Prefetch filename is generated (e.g. notepad.exe-XXXXXXXXX.pf)

Source: [Hexacorn.com](https://hexacorn.com) (Link in Description)



How Prefetch Files Work

Process:

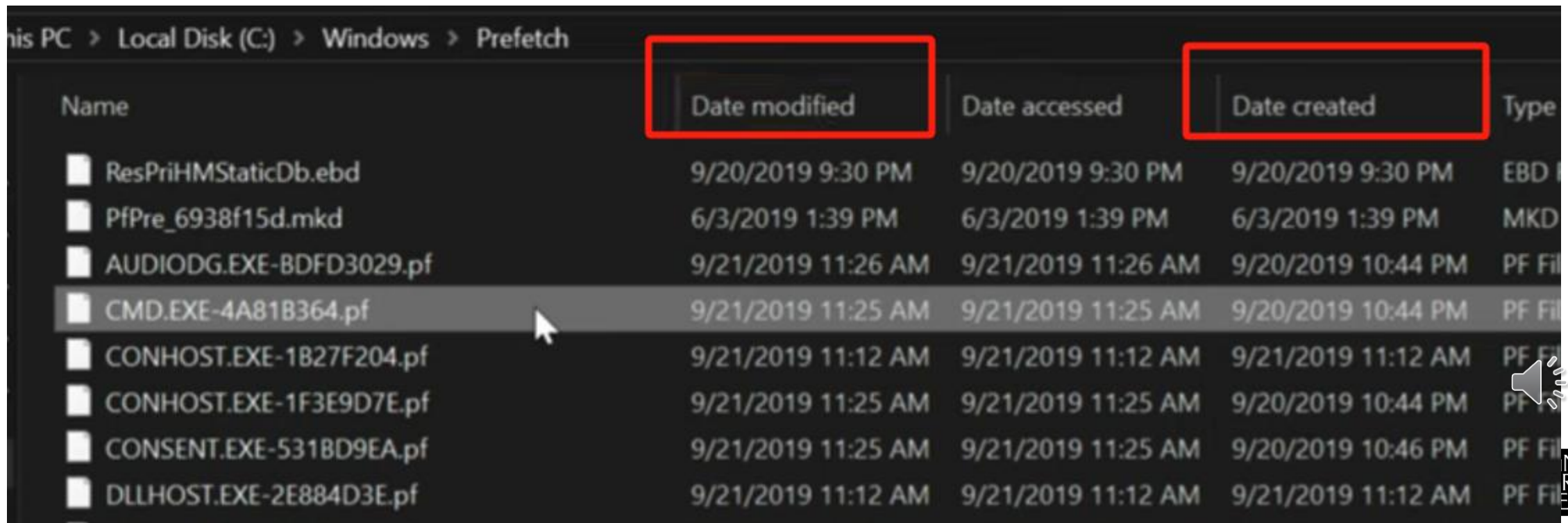
1. When a program is executed, Windows checks if a prefetch file exists.
2. If it does, Windows uses the prefetch data to load the program faster.
3. If not, Windows creates a new prefetch file for that application.



Prefetch File Analysis via Timestamps

The creation timestamp – about 10 secs = the first time the application was run.

The modification timestamp – about 10 secs = the last time the application was run.



This PC > Local Disk (C:) > Windows > Prefetch

Name	Date modified	Date accessed	Date created	Type
ResPriHMStaticDb.ebd	9/20/2019 9:30 PM	9/20/2019 9:30 PM	9/20/2019 9:30 PM	EBD
PfPre_6938f15d.mkd	6/3/2019 1:39 PM	6/3/2019 1:39 PM	6/3/2019 1:39 PM	MKD
AUDIODG.EXE-BDFD3029.pf	9/21/2019 11:26 AM	9/21/2019 11:26 AM	9/20/2019 10:44 PM	PF File
CMD.EXE-4A81B364.pf	9/21/2019 11:25 AM	9/21/2019 11:25 AM	9/20/2019 10:44 PM	PF File
CONHOST.EXE-1B27F204.pf	9/21/2019 11:12 AM	9/21/2019 11:12 AM	9/21/2019 11:12 AM	PF File
CONHOST.EXE-1F3E9D7E.pf	9/21/2019 11:25 AM	9/21/2019 11:25 AM	9/20/2019 10:44 PM	PF File
CONSENT.EXE-531BD9EA.pf	9/21/2019 11:25 AM	9/21/2019 11:25 AM	9/20/2019 10:46 PM	PF File
DLLHOST.EXE-2E884D3E.pf	9/21/2019 11:12 AM	9/21/2019 11:12 AM	9/21/2019 11:12 AM	PF File

Important of Prefetch Files in Digital Forensics

- **Evidence Collection:** Prefetch files can provide timestamps of program execution.
- **Identifying Malicious Activity:** They help forensic analysts identify unusual or unauthorized program usage.
- **User Behavior Analysis:** Understanding which applications were used and when.



Practical Exercise

- **Objective:** Locate and analyze a prefetch file for a commonly used application (e.g., DEMO).
- **Steps:**
 1. Open the Prefetch directory.
 2. Identify the prefetch file for DEMO.
 3. Open it in a hex editor.
 4. Document the application's start time and frequency of use.



New Text Document.txt

C:\Windows\Prefetch

←

→

↑

↻

🖨

>

This PC

>

Local Disk (C:)

>

Windows

>

Prefetch

>

Search Prefetch

+

New

✂

📁

📄

📄

🗑

↕ Sort

☰ View

...

🎵 Music

📺 Videos

📁 download

📁 PLAYERUNKNOWN'S BATT

📁 PLAYERUNKNOWN'S BATT

📁 week2

📁 COS30015

> 📁 Creative Cloud Files

> 📁 iCloud Drive

> 📁 iCloud 照片

▼ 📁 This PC

> 📁 Local Disk (C:)

> 📁 Local Disk (D:)

> 📁 1T固态硬盘 (E:)

> 📁 Network

Name	Date modified	Date created	Type
📄 DLLHOST.EXE-B8720A9F.pf	29/08/2024 10:51 AM	29/08/2024 10:48 AM	PF File
📄 RUNTIMEBROKER.EXE-35443DE5.pf	29/08/2024 10:50 AM	29/08/2024 1:50 AM	PF File
📄 CHROME.EXE-AED7BA3D.pf	29/08/2024 10:49 AM	29/08/2024 1:54 AM	PF File
📄 DATAEXCHANGEHOST.EXE-8B66795C.pf	29/08/2024 10:52 AM	29/08/2024 10:49 AM	PF File
📄 SMARTSCREEN.EXE-EACC1250.pf	29/08/2024 10:49 AM	29/08/2024 1:55 AM	PF File
📄 NOTEPAD.EXE-0D6A91FB.pf	29/08/2024 10:52 AM	29/08/2024 10:49 AM	PF File
📄 SEARCHFILTERHOST.EXE-44162447.pf	29/08/2024 10:49 AM	29/08/2024 2:01 AM	PF File
📄 DLLHOST.EXE-7C46829E.pf	29/08/2024 10:48 AM	29/08/2024 10:48 AM	PF File
📄 DLLHOST.EXE-99048A82.pf	29/08/2024 10:48 AM	29/08/2024 10:48 AM	PF File
📄 DLLHOST.EXE-B39B04B3.pf	29/08/2024 10:48 AM	29/08/2024 10:48 AM	PF File
📄 DLLHOST.EXE-C6DAFF35.pf	29/08/2024 10:48 AM	29/08/2024 10:48 AM	PF File
📄 DLLHOST.EXE-C530983A.pf	29/08/2024 10:48 AM	29/08/2024 10:48 AM	PF File
📄 DLLHOST.EXE-DD3573CE.pf	29/08/2024 10:48 AM	29/08/2024 2:01 AM	PF File
📄 WMIPRVSE.EXE-E888DD29.pf	29/08/2024 10:52 AM	29/08/2024 1:55 AM	PF File
📄 SYSTEMINFO.EXE-16093B84.pf	29/08/2024 10:48 AM	29/08/2024 2:15 AM	PF File
📄 DOUYIN.EXE-80DCA105.pf	29/08/2024 10:48 AM	29/08/2024 10:48 AM	PF File

📁

Prefetch (369 items)

Select a single file to get more information and share your cloud content.

369 items



Search



Conclusion

- **Key Takeaways:**

- Prefetch files are crucial for performance optimization in Windows.
- They provide valuable data for forensic investigations.
- Understanding prefetch files can help in both system optimization and digital forensic analysis



Thank you

