



blackhat[®]
USA 2020
AUGUST 5-6, 2020
BRIEFINGS



Fooling Windows through Superfetch

Mathilde Venault & Baptiste David

#BHUSA @BLACKHATEVENTS

Who are we?



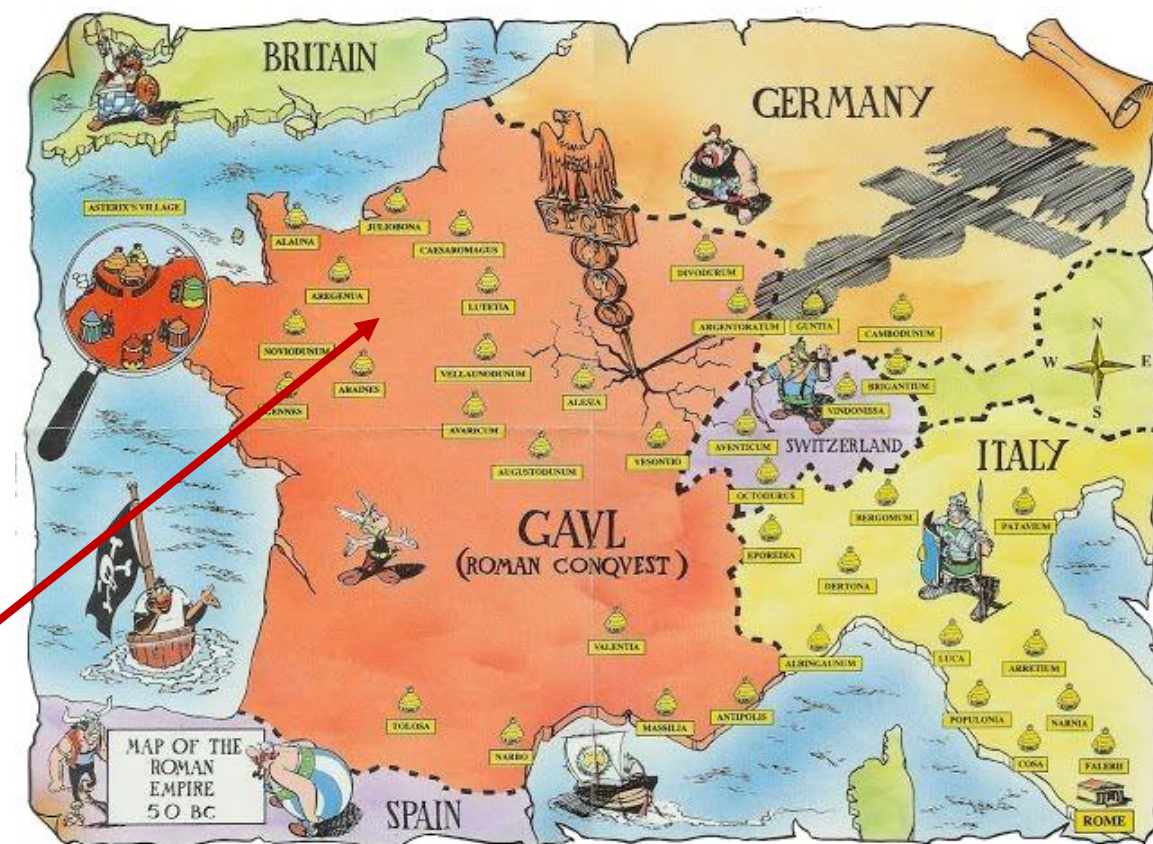
Mathilde VENAULT
venault@et.esiea.fr



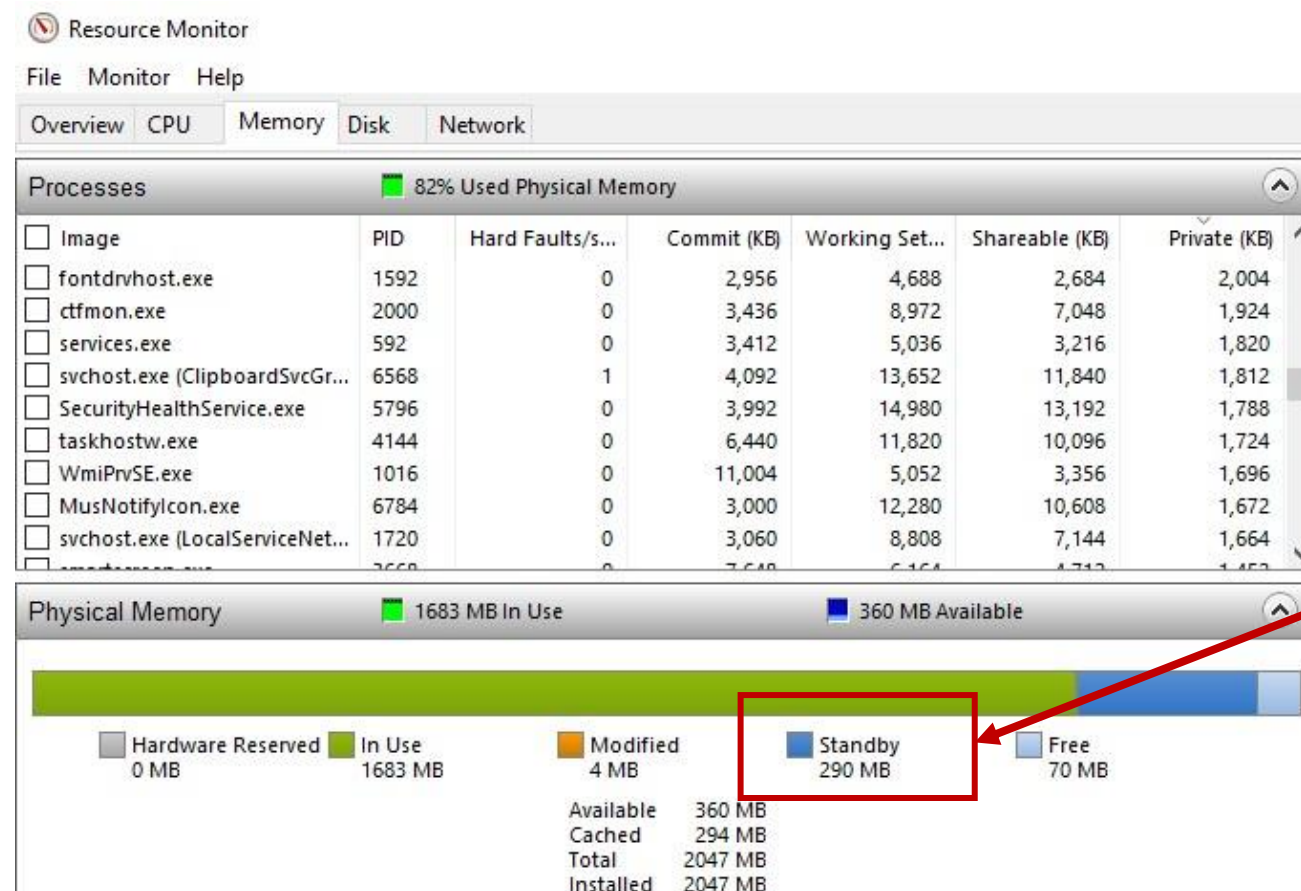
Baptiste DAVID
bdavid@et.esiea.fr



Laval, France



What is it?

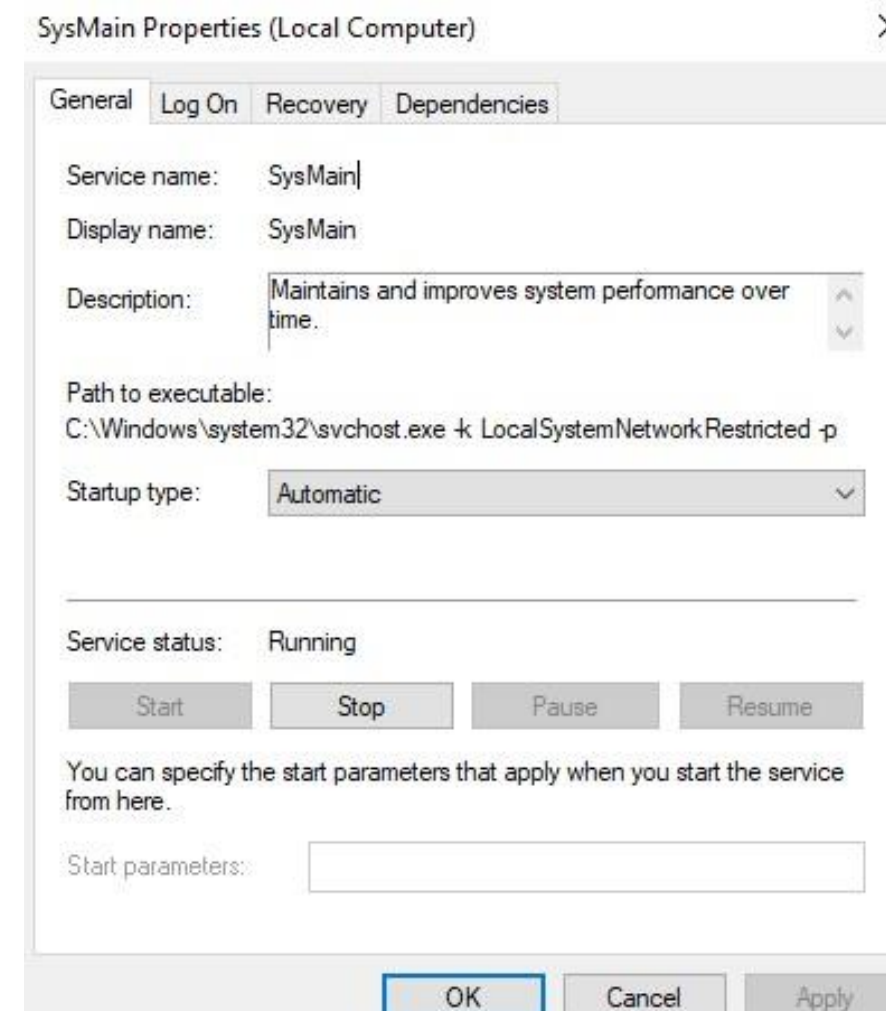


Resource Monitor view

- SysMain = preloaded memory + preloaded processes + scenarios

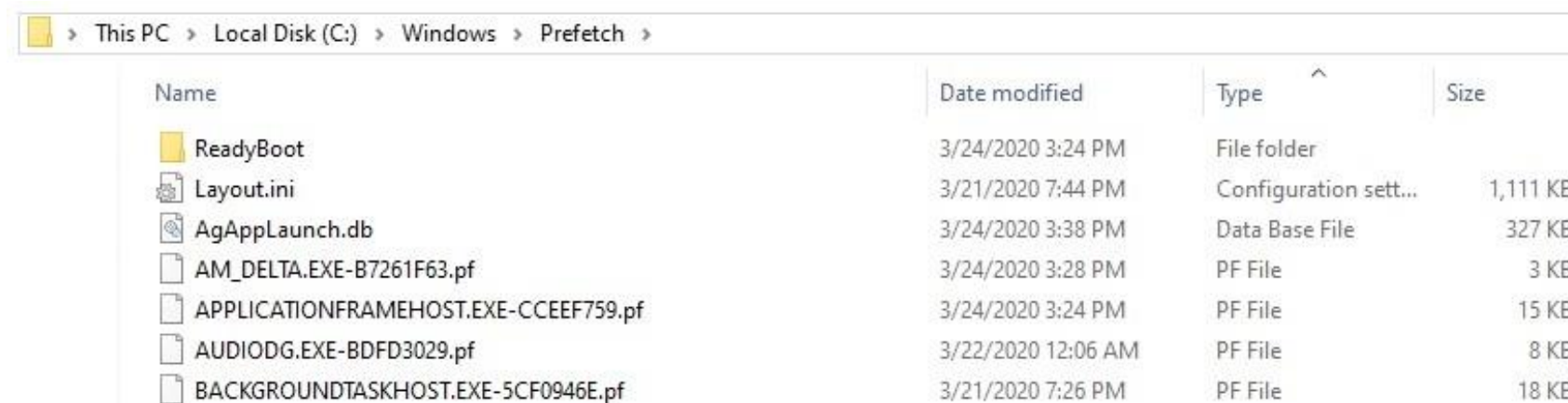
The service SysMain

- The main goal is to **increase speed of user experience** through:
 - Optimizing boot of the os.
 - Analyzing software use & prelaunching programs the user might need next time.
- Misuse of language: « Superfetch » is only a part of SysMain, which is the name of the whole service. It is often called Superfetch because on older Windows versions, the service was called Superfetch.



SysMain properties

SysMain's headquarters



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

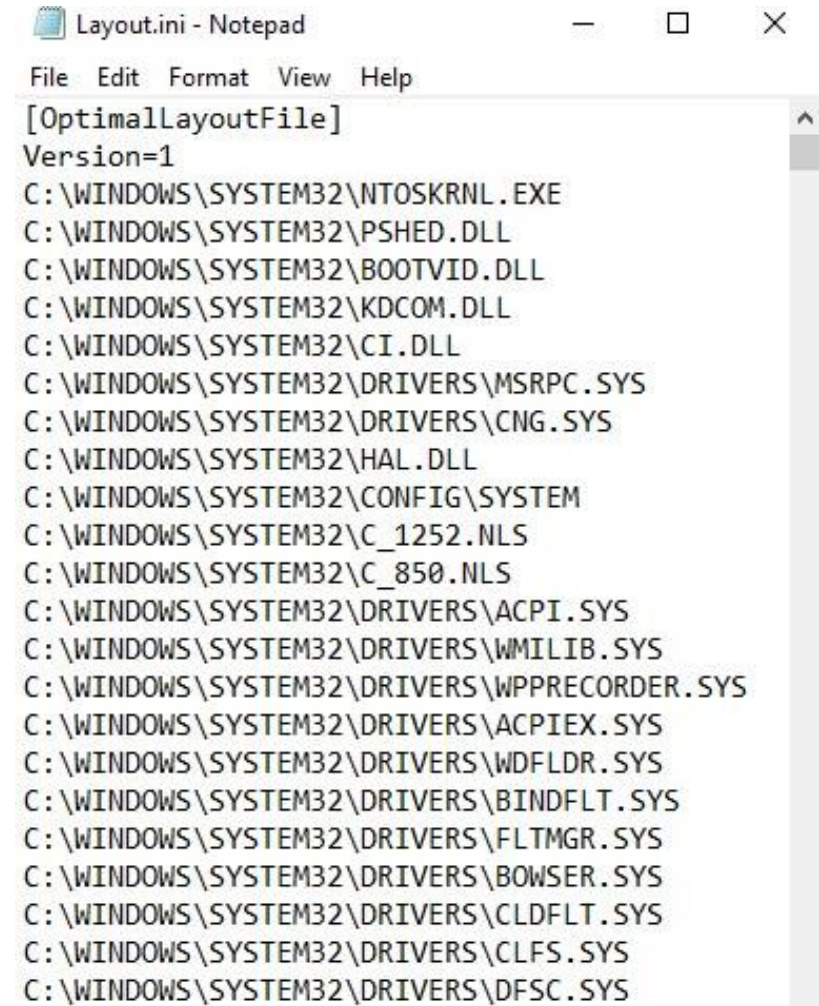
Name	Date modified	Type	Size
ReadyBoot	3/24/2020 3:24 PM	File folder	
Layout.ini	3/21/2020 7:44 PM	Configuration sett...	1,111 KB
AgAppLaunch.db	3/24/2020 3:38 PM	Data Base File	327 KB
AM_DELTA.EXE-B7261F63.pf	3/24/2020 3:28 PM	PF File	3 KB
APPLICATIONFRAMEHOST.EXE-CCEE759.pf	3/24/2020 3:24 PM	PF File	15 KB
AUDIODG.EXE-BDFD3029.pf	3/22/2020 12:06 AM	PF File	8 KB
BACKGROUNDTASKHOST.EXE-5CF0946E.pf	3/21/2020 7:26 PM	PF File	18 KB

C:\Windows\Prefetch directory

- SysMain stores its files on C:\Windows\Prefetch.
- This directory includes:
 - « ReadyBoot » directory related to the Readyboost driver functionalities.
 - Files related to the service (with .db and .pf extension): traces of Superfetch's activity.
 - A file named « Layout.ini » which is the key file to speed up the boot.

Optimizing the boot

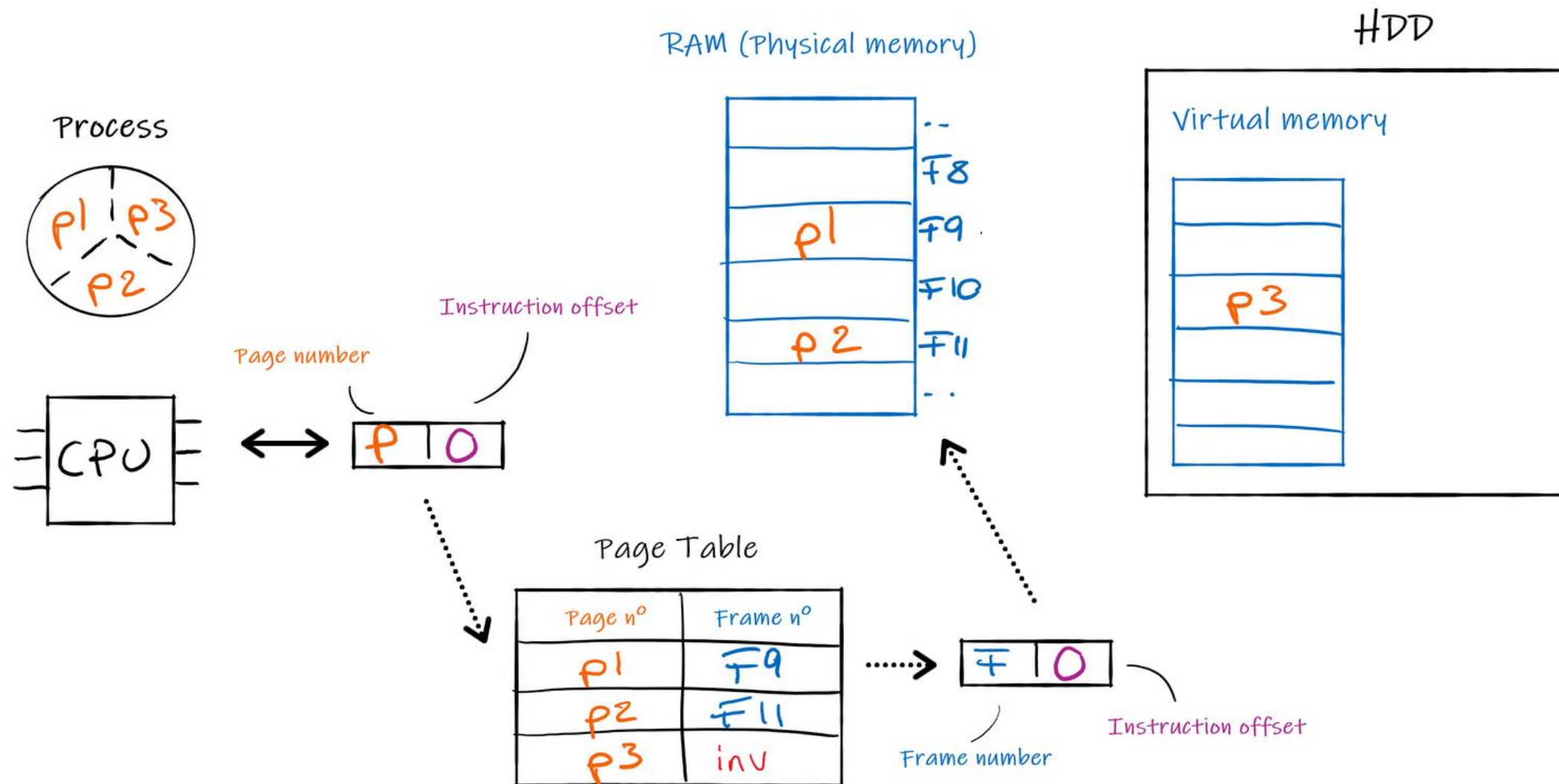
- The goal: find the **quickest way** for the OS to boot.
- The list represents the **best order to load the given files** in memory.
- Begins with the kernel!



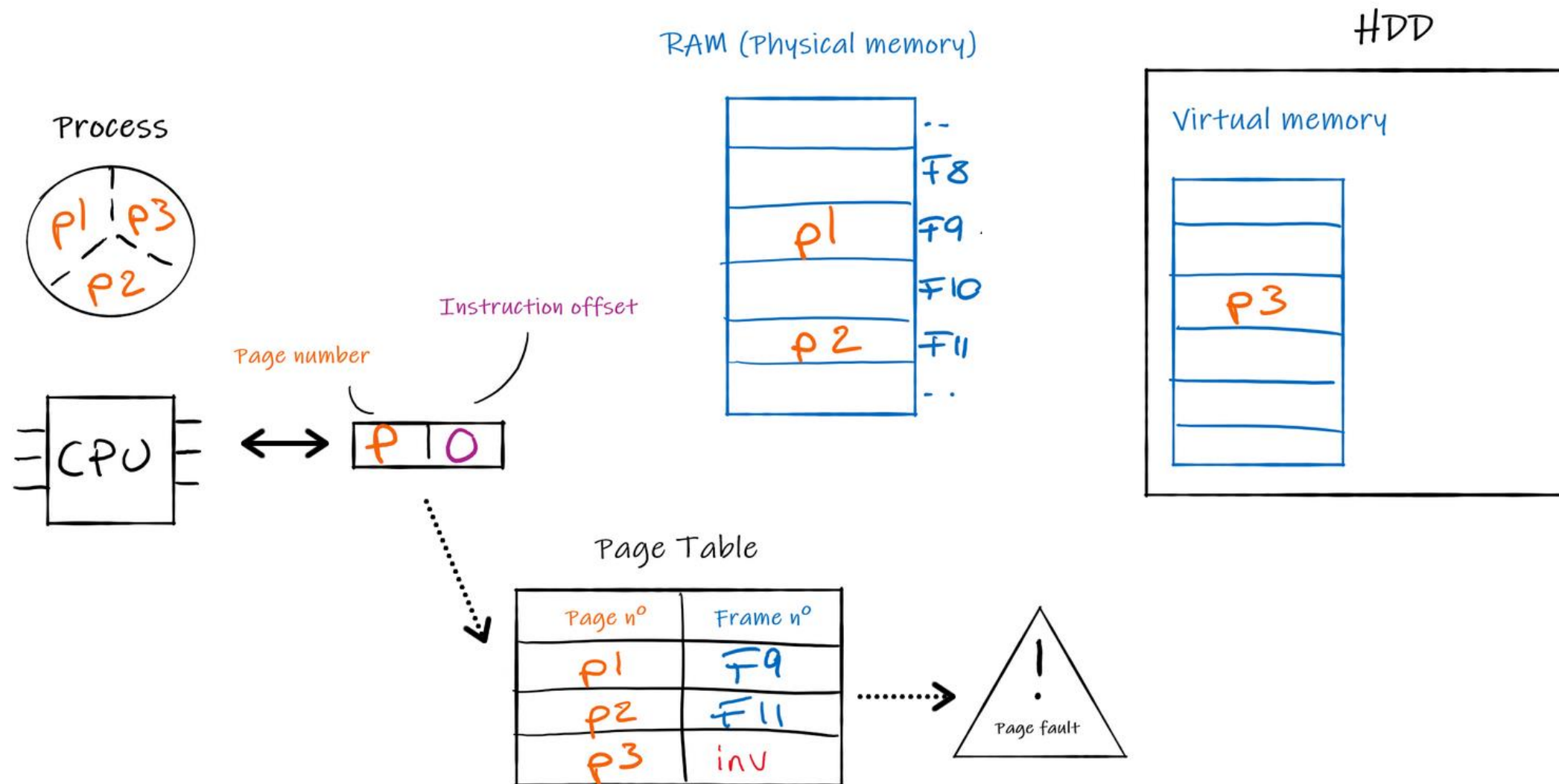
```
Layout.ini - Notepad
File Edit Format View Help
[OptimalLayoutFile]
Version=1
C:\WINDOWS\SYSTEM32\NTOSKRNL.EXE
C:\WINDOWS\SYSTEM32\PSHED.DLL
C:\WINDOWS\SYSTEM32\BOOTVID.DLL
C:\WINDOWS\SYSTEM32\KDCOM.DLL
C:\WINDOWS\SYSTEM32\CI.DLL
C:\WINDOWS\SYSTEM32\DRIVERS\MSRPC.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CNG.SYS
C:\WINDOWS\SYSTEM32\HAL.DLL
C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM
C:\WINDOWS\SYSTEM32\C_1252.NLS
C:\WINDOWS\SYSTEM32\C_850.NLS
C:\WINDOWS\SYSTEM32\DRIVERS\ACPI.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\WMILIB.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\WPPREORDER.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\ACPIEX.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\WDFLDR.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\BINDFLT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\FLTMGR.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\BOWSER.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CLDFLT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CLFS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DFSC.SYS
```

C:\Windows\Prefetch\Layout.ini

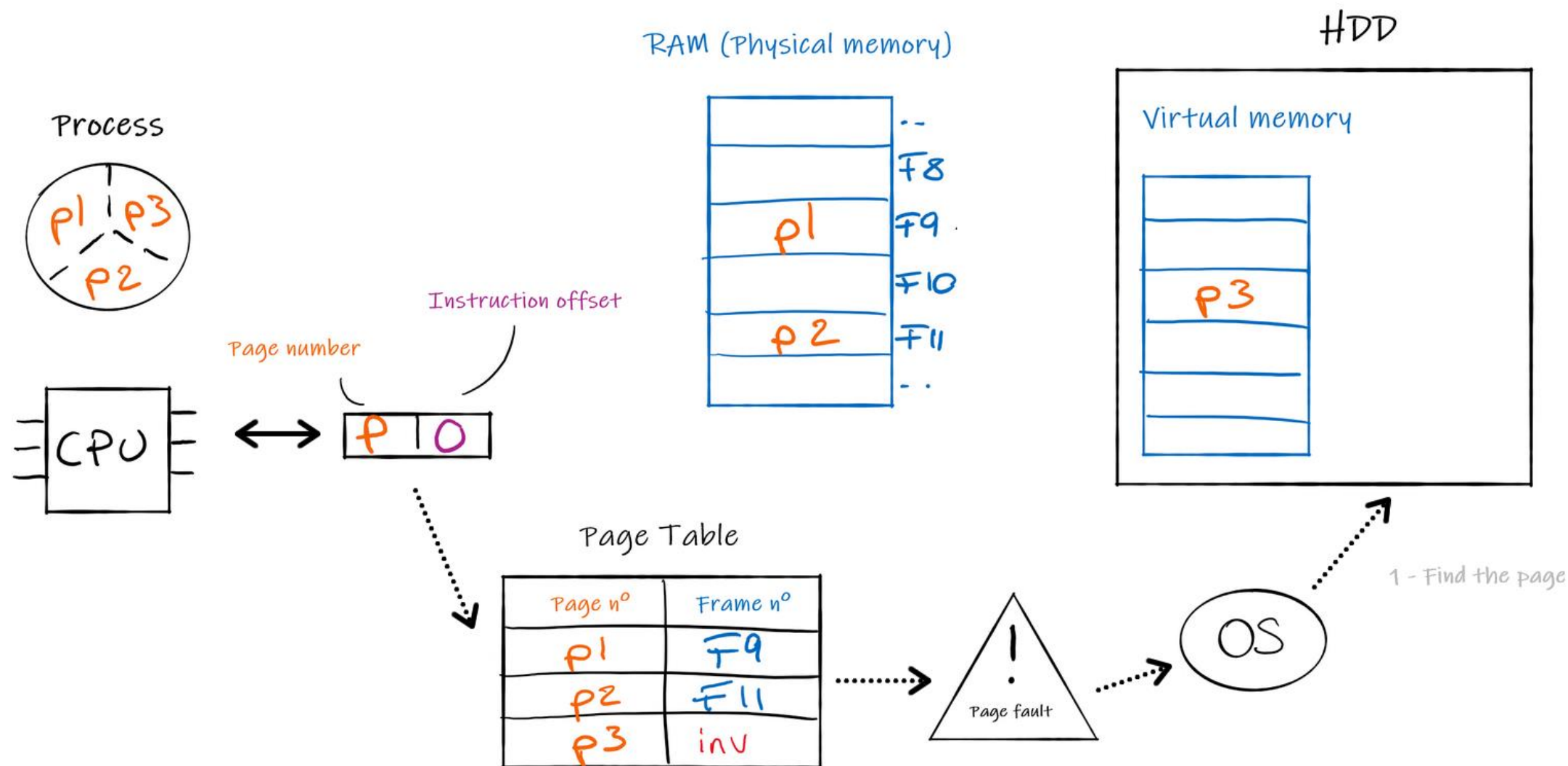
Mechanism: memory paging



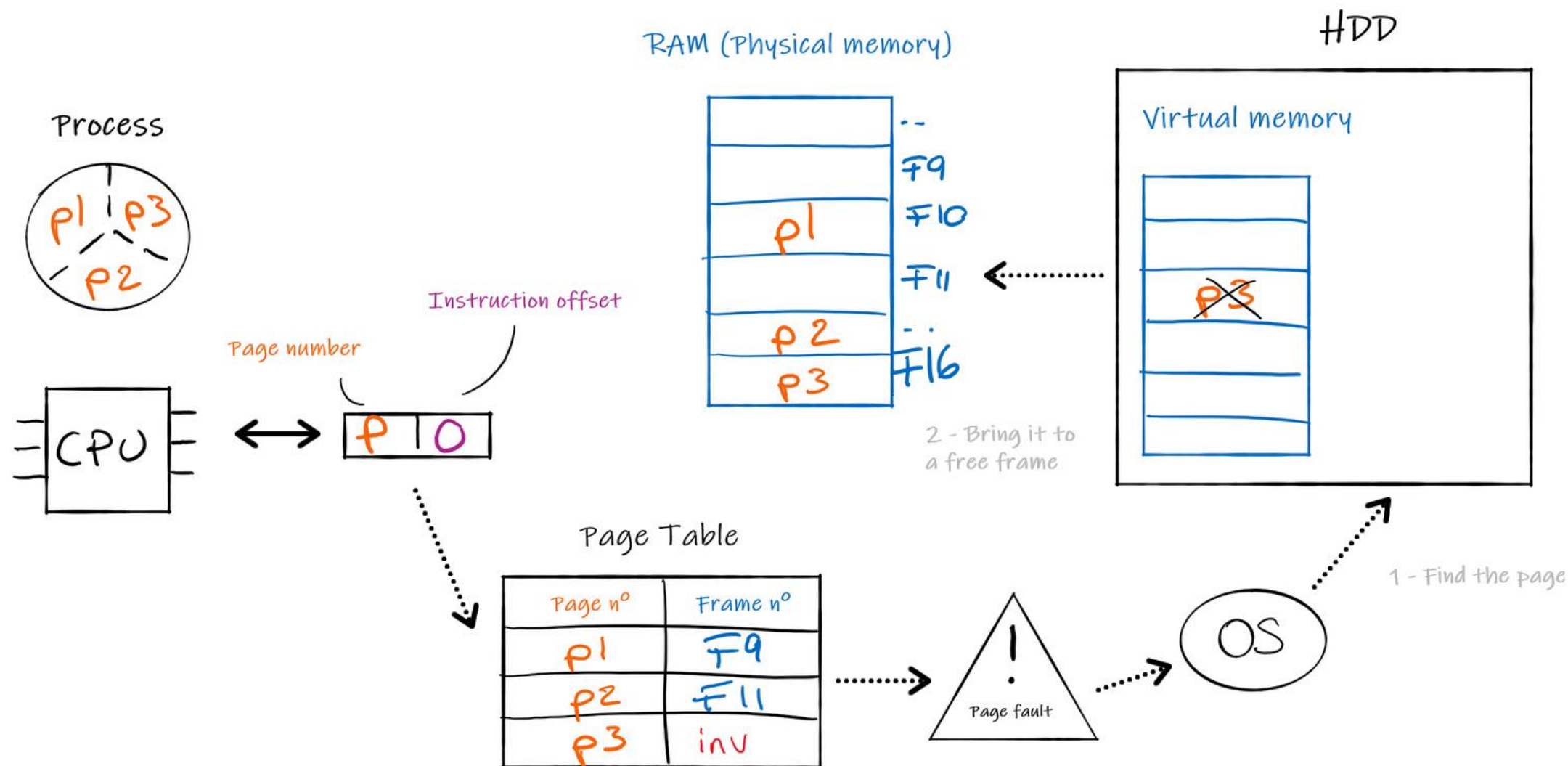
Mechanism: page faults



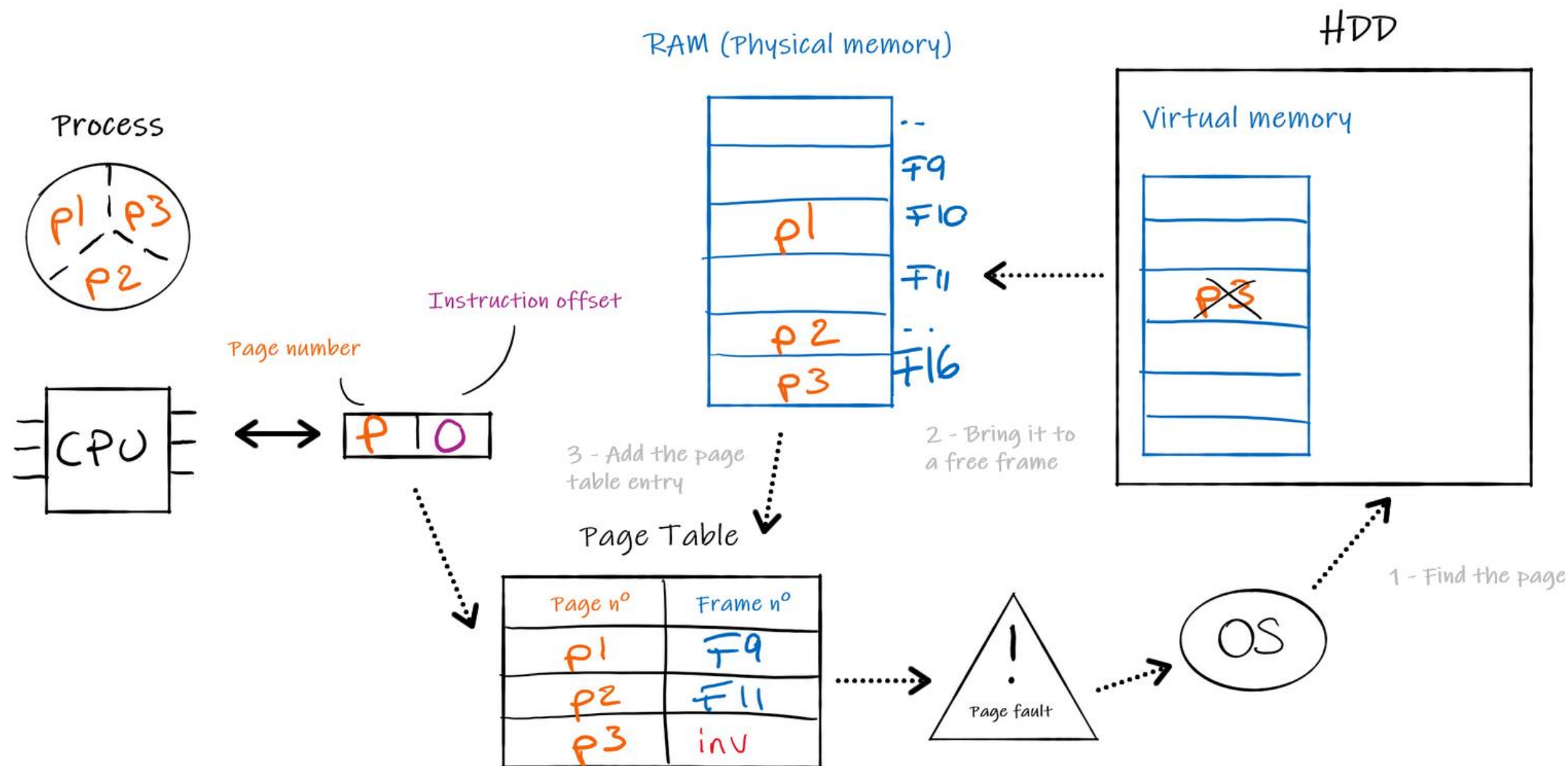
Mechanism: page faults



Mechanism: page faults



Mechanism: page faults



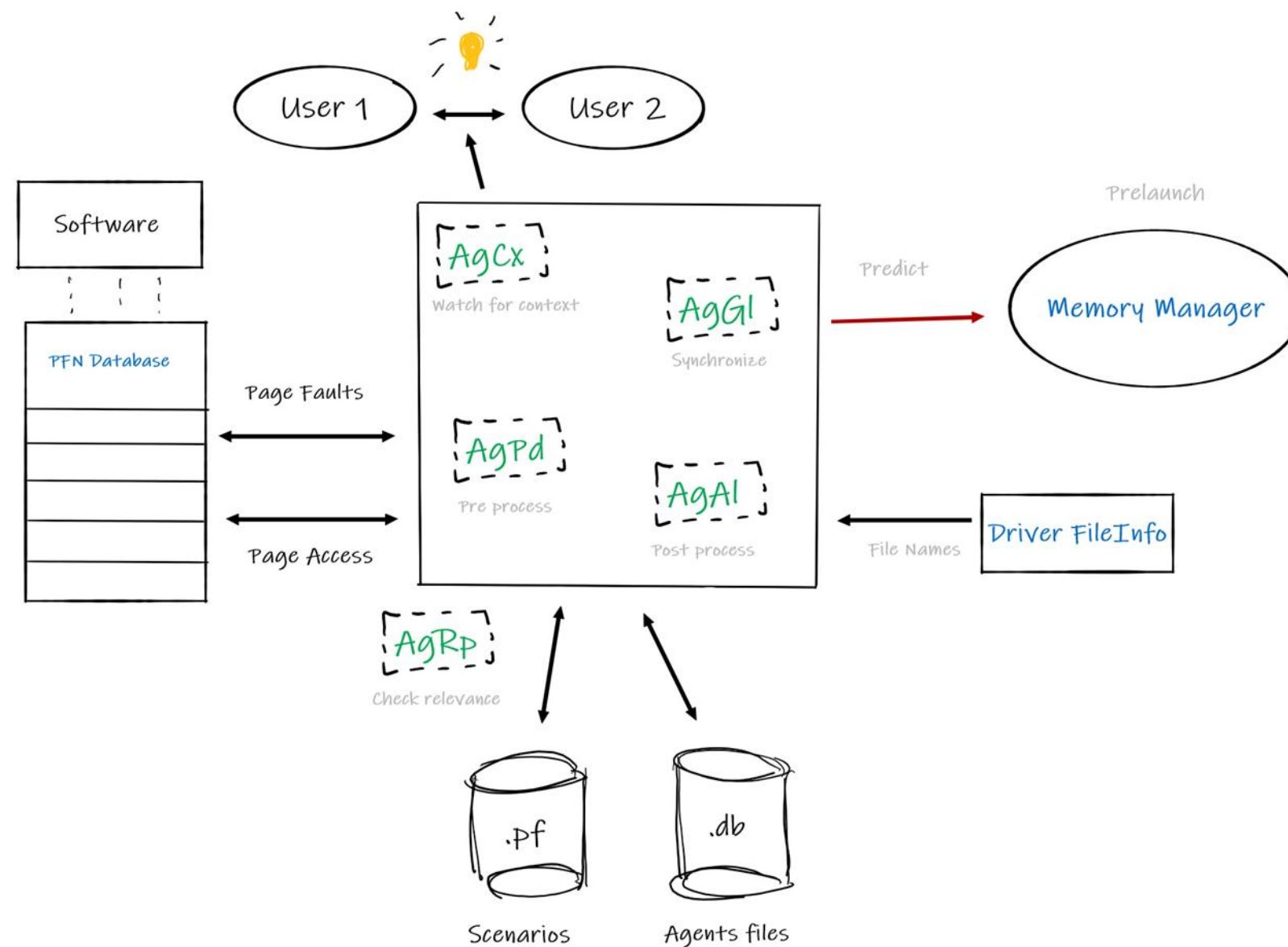
Mechanism: reducing memory operations

- Superfetch aims at **reducing the occurrence of page faults**, which require time & operations from memory.

- To this end Superfetch:
 - Remembers **page accesses**.
 - Logs **pages faults**.
 - Maps to physical memory pages referenced whenever the relative program is launched.

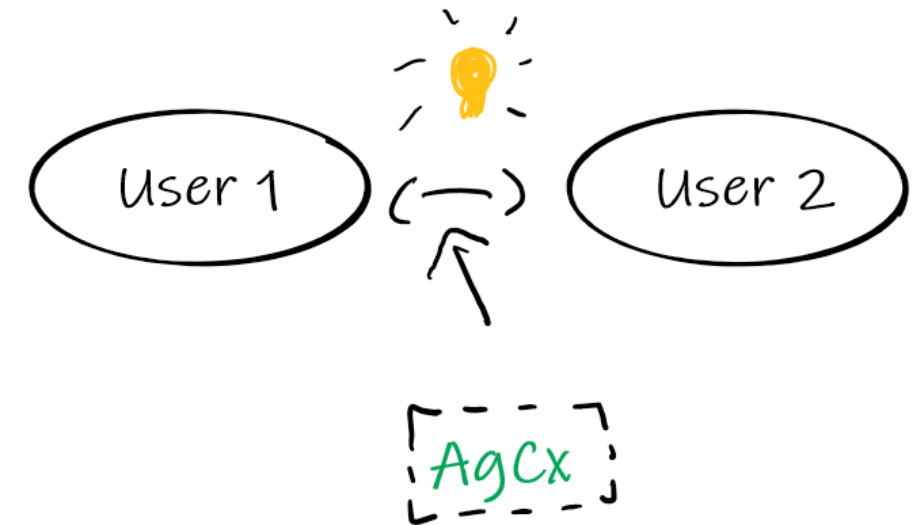
How does it work?

Global architecture



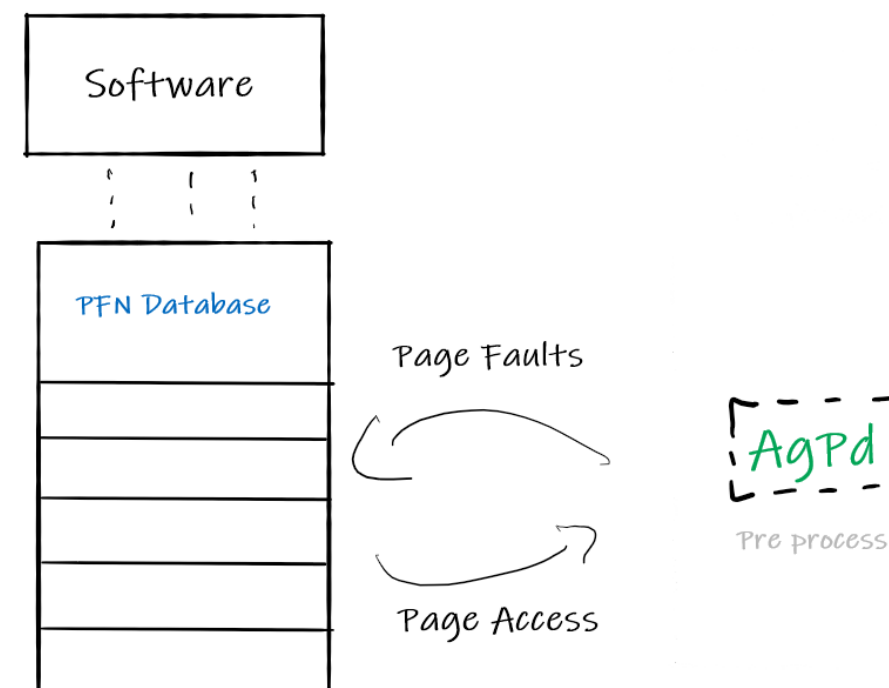
Agent Context (AgCx)

- Deals session information based on SID & Token User.
- Watches **for context change**:
 - hibernation (long pause).
 - standby (short pause).
 - fast user switching (change of user session).
- Takes a snapshot of the situation when this is about to change. Includes two types of disconnection:
 - Classic Disconnect (quitting & logging).
 - « Lazy Disconnect » (without quitting).

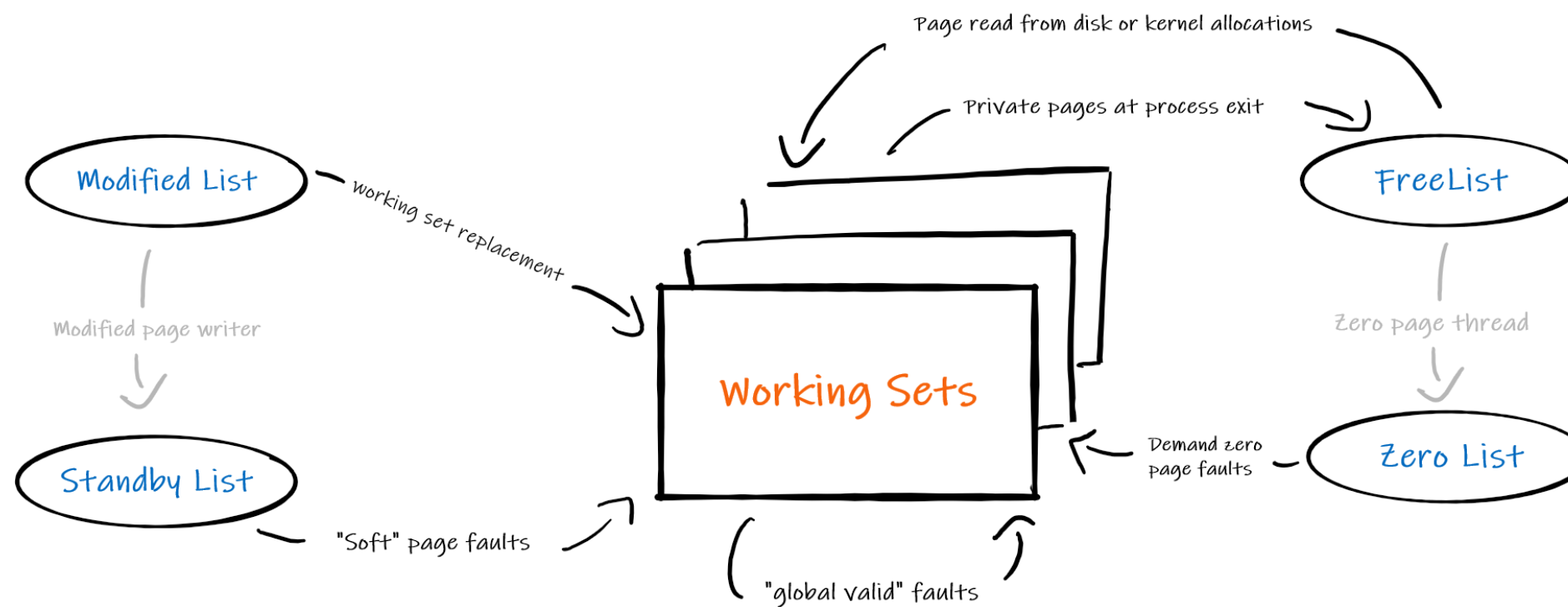


Agent PfnDb (AgPd)

- Based on interactions with the **Page Frame Number** database (PFN).
- Logs page faults encountered by each program.
- Classifies responses (among others):
 - Is it a « private page »? (**committed/non shared page**)
 - Is the page from a background app?



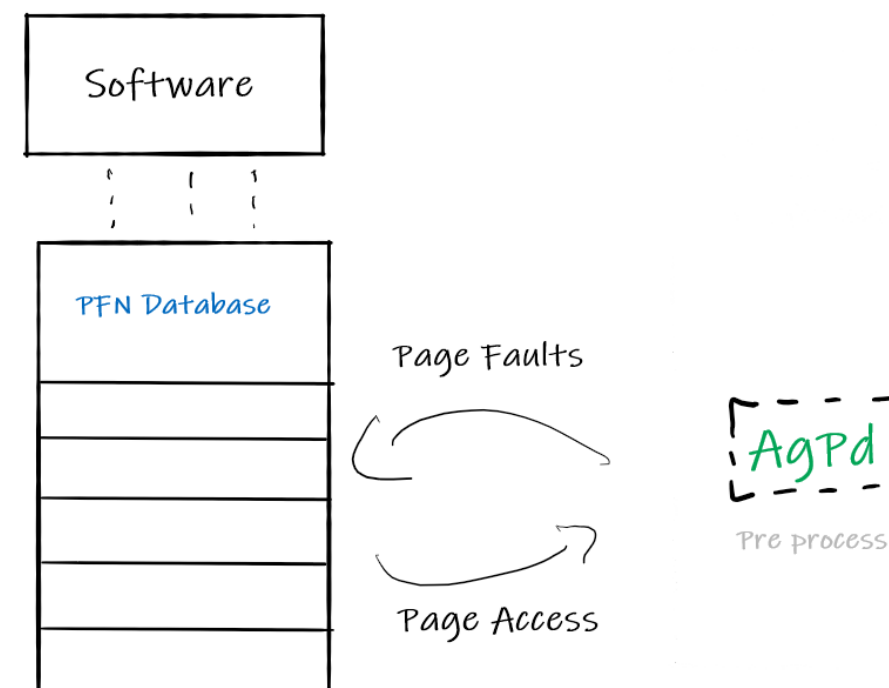
The PFN database



- Page Frame Number (PFN) is an array representing each **physical page state** of memory on the system (Active / Standby / Freed ...).

Agent PfnDb (AgPd)

- Based on interactions with the **Page Frame Number** database (PFN).
- Logs page faults encountered by each program.
- Classifies responses:
 - Is it a « private page »? (committed page)
 - Is the page from a background app?



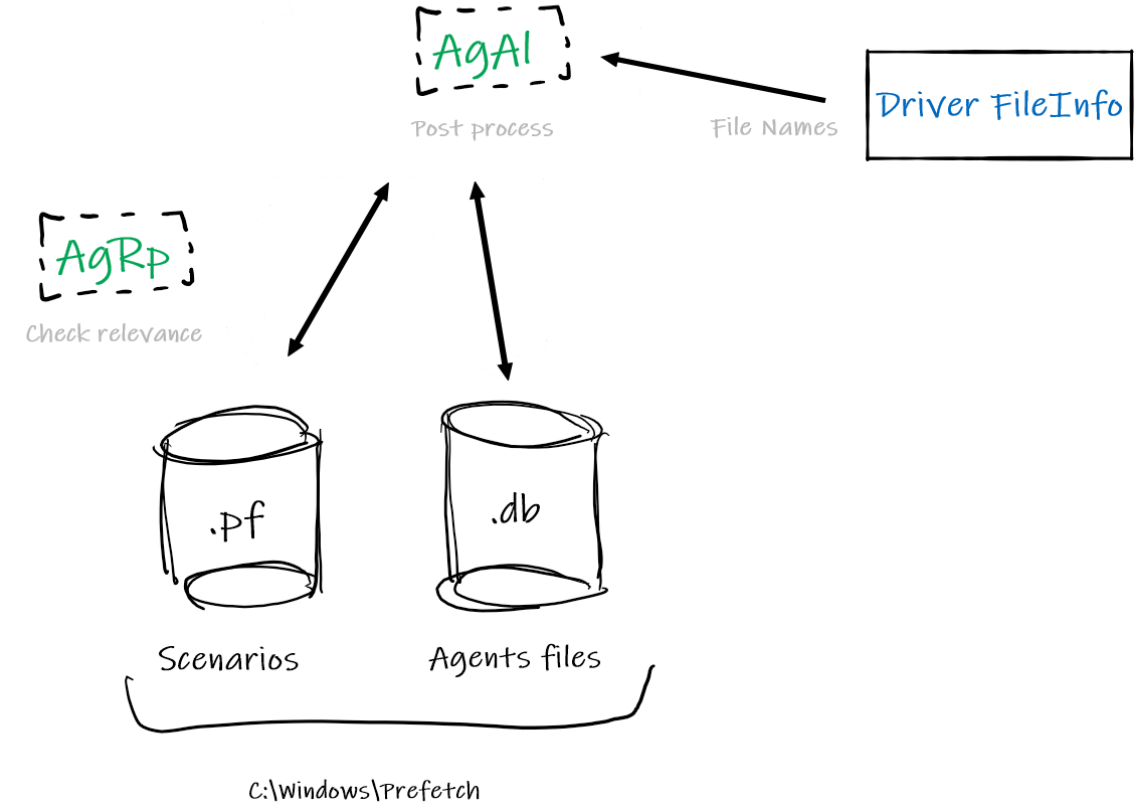
Agent AppLaunch (AgAI) & Robust performance (AgRp)

▪ AgAI

- **Post processes data** received from FileInfo to take future decisions.
- Creates Markov chains to represent probabilities of pattern use.

▪ AgRp

- Assures **relevance of the databases**:
- Checks how many times/since when the data has been used.
- Calculates a « **pertinence threshold** » depending on other scenario use.



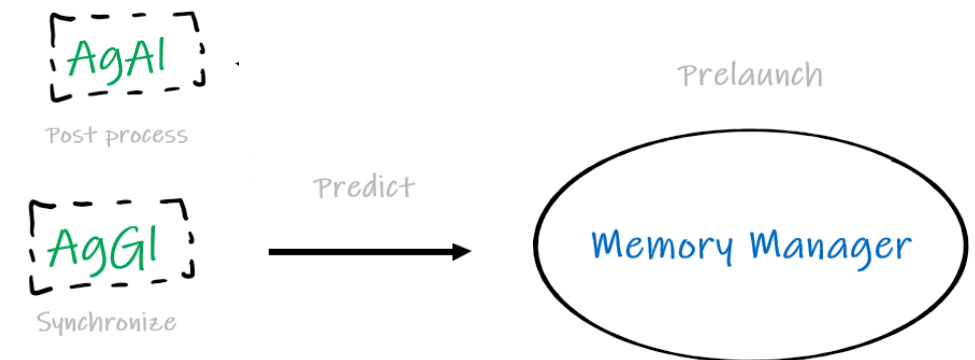
Agent Global (AgGI) & Agent AppLaunch (AgAI)

- AgGI

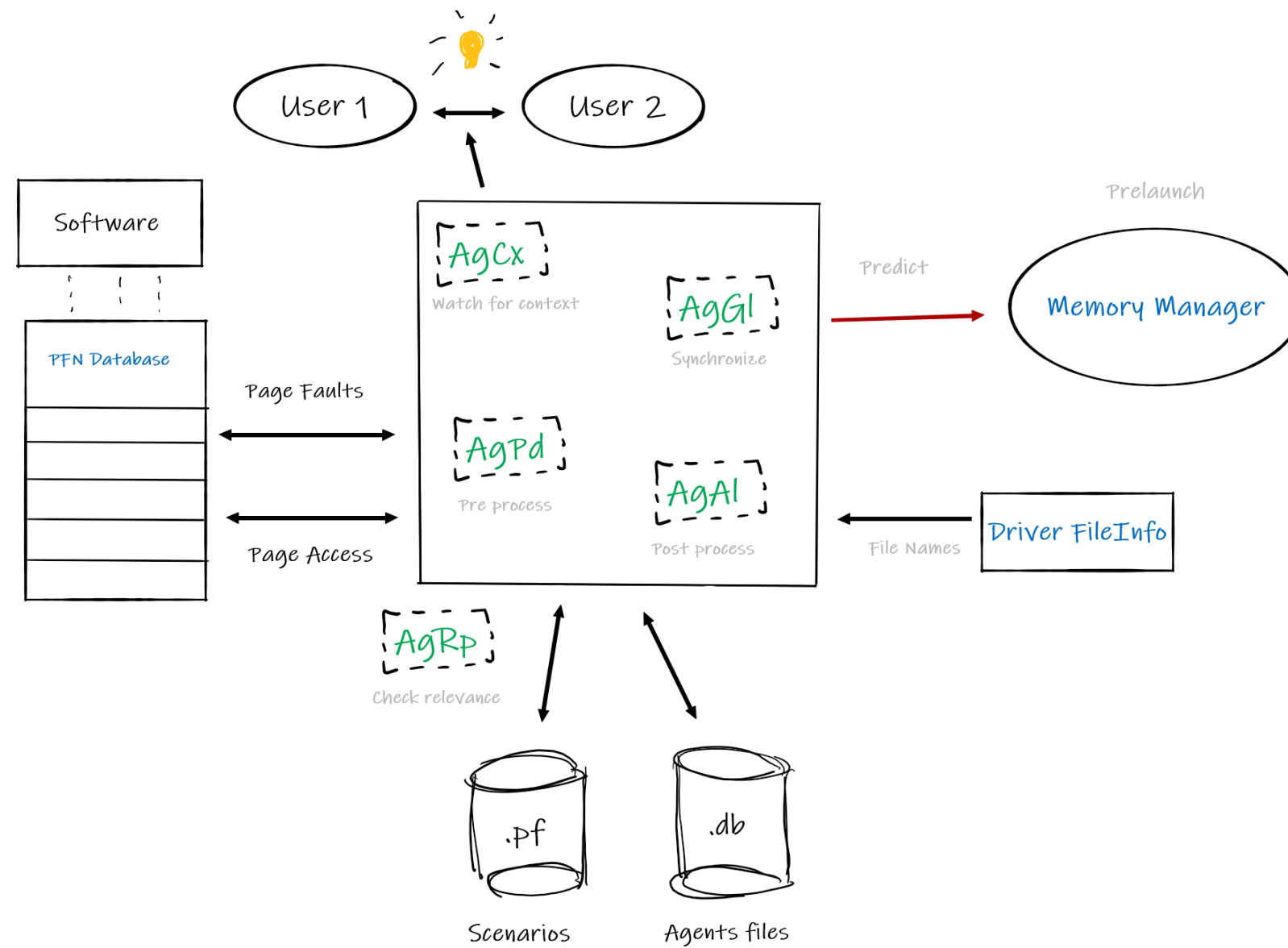
- Organizes « **histories** » (individual history, fault history, global history).
- Defines phases per days (morning/ weekdays, weekends..).

- AgAI

- Make **predictions** depending on the Markov chains established before.



Global architecture



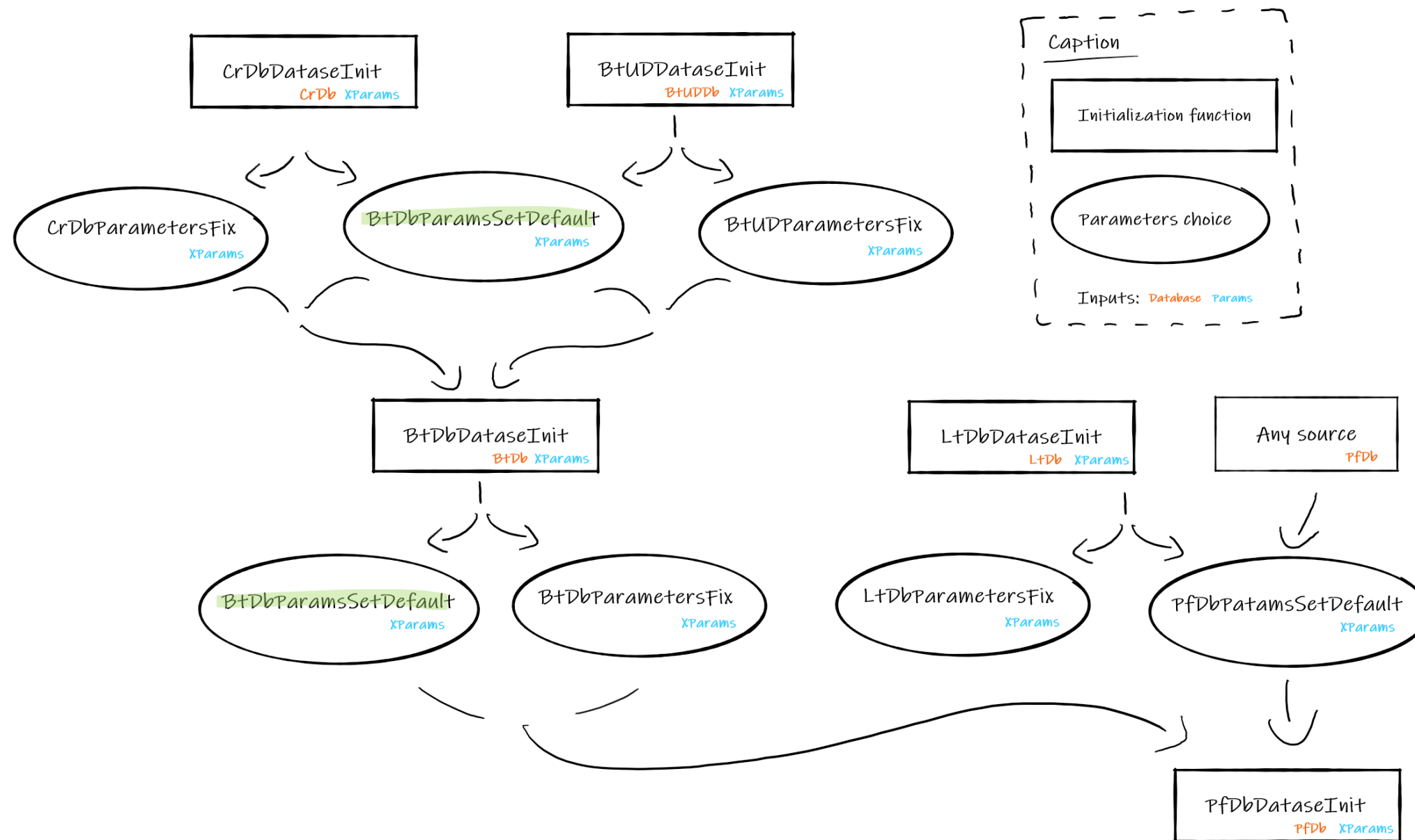
Types of Superfetch tasks

- Prefetch routines
 - « **Non stop** » job.
 - Processing traces (building & updating scenarios), predicting and pre launching, daily checks..
- Periodic saves
 - Each 3 days on average, but depends on the value to save.
 - Saving databases, updating registry keys...
- Idle tasks
 - Under **special circumstances** (cpu, disk & memory utilization + power supply).
 - Updating optimal layout ; launching « defrag.exe - s -b »

Surprising facts

- Influence of power supply:
 - During an « **idle state** », if there is no power supply detected Superfetch will not process what it first planned to do.
 - Depending on power supply, the decision of prefetching some applications will not be the same.
- More than **22 registry keys** are frequently consulted, deleted and created, as a way of communication with the rest of the kernel or as internal markers. For instance, the date of the last optimal layout calculation is stored and checked by Superfetch in the registry.
- Superfetch has **5 different types** of databases.. But at their initialization, we found out each is **based on the others!**

API Internal database



What about the prefetch files?

File compression

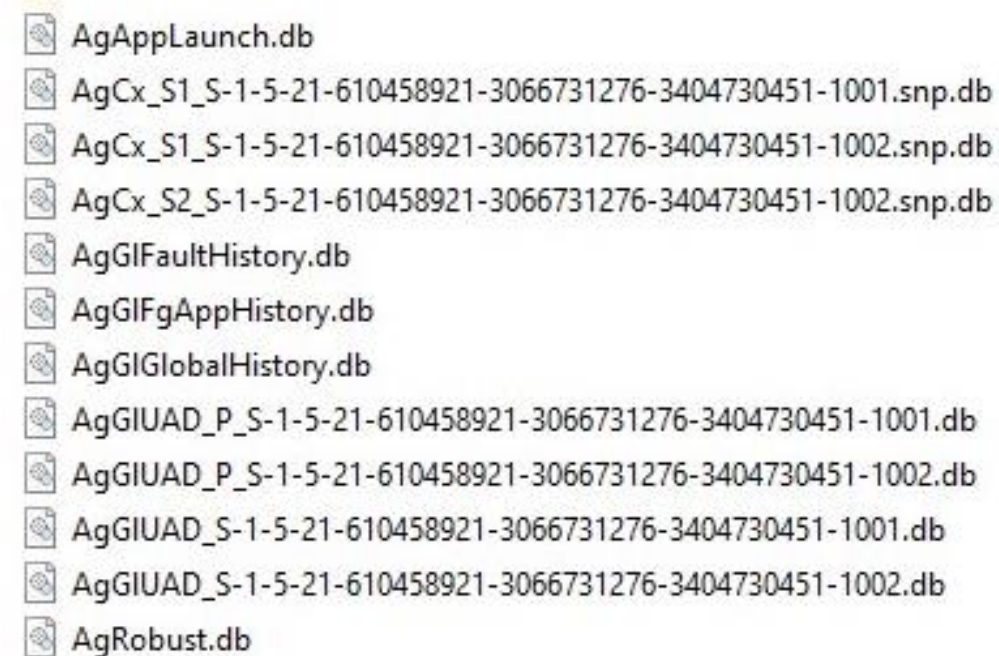
- All the prefetch files, except AgAppLaunch.db, AgRobust.db, dynrespri.db & cadrespri.db are compressed.
- The files are compressed within the function `RtlCompressBuffer()` from NtosKrnl.lib.
- The compression format is the `XPRESS_HUFFMAN` format.

```
NT_RTL_COMPRESS_API NTSTATUS RtlCompressBuffer(  
    USHORT CompressionFormatAndEngine,  
    PCHAR UncompressedBuffer,  
    ULONG UncompressedBufferSize,  
    PCHAR CompressedBuffer,  
    ULONG CompressedBufferSize,  
    ULONG UncompressedChunkSize,  
    PULONG FinalCompressedSize,  
    PVOID WorkSpace  
);
```

RtlCompressBuffer() prototype, msdn.com

Database files: generalities

- Traces of **agent's activity**: way to build internal database.
- One agent has 1 or more « .db ».
- They are **not always present** on the prefetch directory.
- Until now, their format was undocumented.



AgAppLaunch.db
AgCx_S1_S-1-5-21-610458921-3066731276-3404730451-1001.snp.db
AgCx_S1_S-1-5-21-610458921-3066731276-3404730451-1002.snp.db
AgCx_S2_S-1-5-21-610458921-3066731276-3404730451-1002.snp.db
AgGIFaultHistory.db
AgGIFgAppHistory.db
AgGIGlobalHistory.db
AgGIUAD_P_S-1-5-21-610458921-3066731276-3404730451-1001.db
AgGIUAD_P_S-1-5-21-610458921-3066731276-3404730451-1002.db
AgGIUAD_S-1-5-21-610458921-3066731276-3404730451-1001.db
AgGIUAD_S-1-5-21-610458921-3066731276-3404730451-1002.db
AgRobust.db

C:\Windows\Prefetch directory

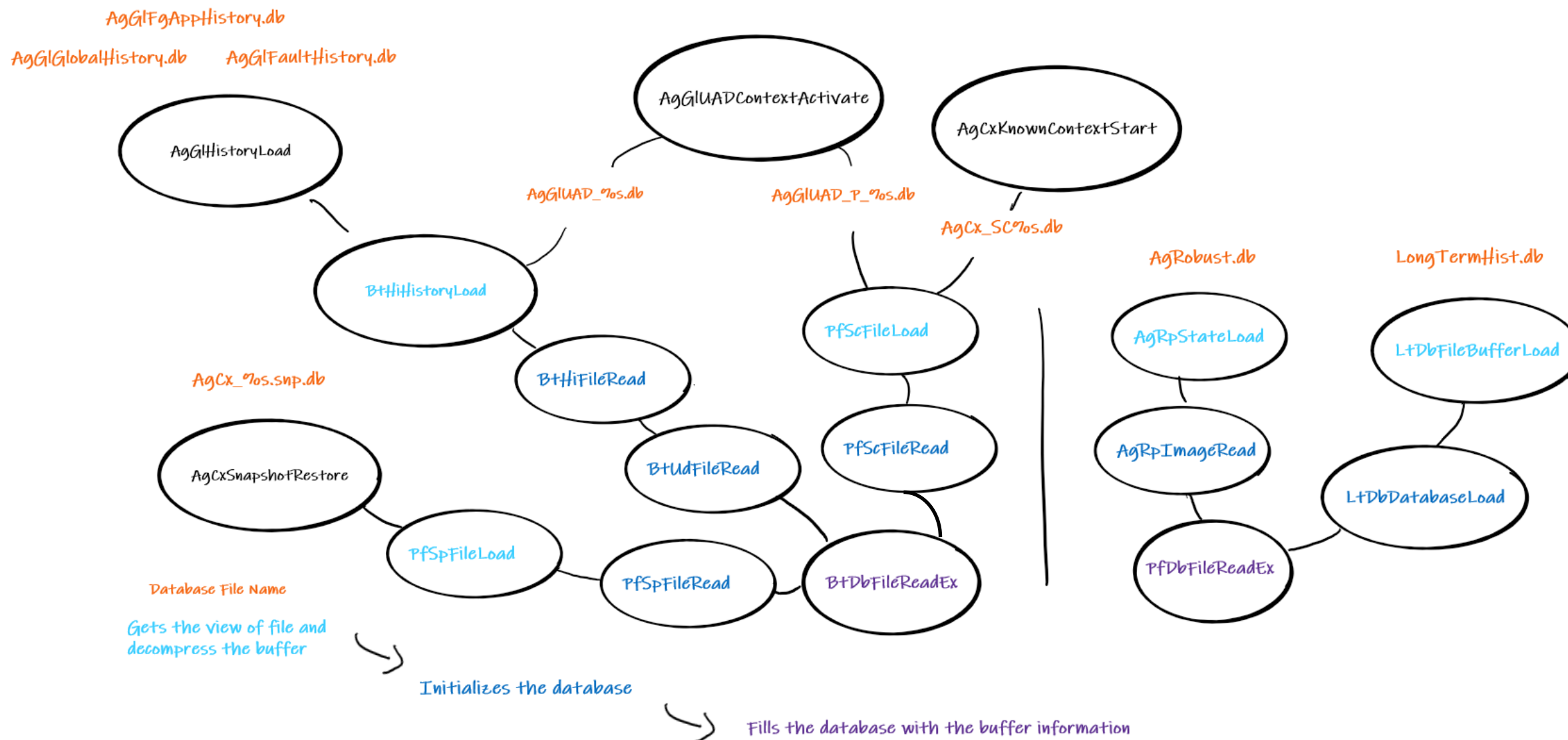
Database files: generalities

- AgAppLauch.db
- AgCx_%SIDofUser.db
- AgGlobalFaultHistory.db
- AgForegroundAppHistory.db
- AgGlobalHistory.db
- AgGIUserActiveDays_%sid (assumption)
- Dynamicreservedpriority.db

- AgAppLaunch.db
- AgCx_S1_S-1-5-21-610458921-3066731276-3404730451-1001.snp.db
- AgCx_S1_S-1-5-21-610458921-3066731276-3404730451-1002.snp.db
- AgCx_S2_S-1-5-21-610458921-3066731276-3404730451-1002.snp.db
- AgGIFaultHistory.db
- AgGIFgAppHistory.db
- AgGIGlobalHistory.db
- AgGIUAD_P_S-1-5-21-610458921-3066731276-3404730451-1001.db
- AgGIUAD_P_S-1-5-21-610458921-3066731276-3404730451-1002.db
- AgGIUAD_S-1-5-21-610458921-3066731276-3404730451-1001.db
- AgGIUAD_S-1-5-21-610458921-3066731276-3404730451-1002.db
- AgRobust.db

C:\Windows\Prefetch directory

Database reading process



Database files: compressed format

Decompressed Size

Magic Number Checksum

AgCx_S1_S-1-5-21-610458921-3066731276-3404730451-1001.snp.db

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	4D	41	4D	84	B8	CF	4B	00	39	10	1F	E8	96	A6	9A	AA	MAM,, İK.9..è-!š²
00000010	A9	A8	AA	BA	AA	A7	9A	A9	AA	A6	AA	BA	AA	A7	AA	AA	@`²²²šš@²!²²²š²²
00000020	A9	A7	AA	A9	99	A6	AA	AA	A9	A7	AA	AA	A9	96	99	BA	@š²@²²!²²@š²²@²²²²²
00000030	A9	A6	9A	AA	A9	96	AA	9A	AA	B6	AA	AA	99	A6	AA	AA	@!š²@²-²š²q²²²²!²²
00000040	A9	A7	AA	AA	AA	A7	AA	AA	A9	B7	BB	AA	B9	A7	BA	AA	@š²²²š²²@²²²²²²²²²²²²
00000050	AA	A7	AA	BA	AA	A7	AB	BB	BB	B7	BB	BA	AA	B6	AA	AA	²š²²²š²²²²²²²²²²²²²²²²²²
00000060	BB	B6	BB	BB	BB	B6	BB	BB	BB	B6	BB	BB	BB	B6	BB	BB	²²²²²²²²²²²²²²²²²²²²²²²²

AgCx.db : original file (compressed)

Database files: decompressed format

Offset (h)	Decompressed Size																Database Parameters Type		Texte Décodé
	Magic Number				Header Size				Database Parameters Type										
00000000	03	00	00	00	B8	CF	4B	00	58	00	00	00	0C	00	00	00	İK.X.....	
00000010	60	00	00	00	38	00	00	00	50	00	00	00	0C	00	00	00		...8...P.....	
00000020	08	00	00	00	08	00	00	00	08	00	00	00	00	00	00	00	 Database Parameters	
00000030	00	00	00	00	02	00	00	00	16	0E	00	00	8B	5E	05	00	<^.. Number of entries	
00000040	51	00	00	00	DC	05	08	00	00	00	00	00	00	00	00	00		Q...Û.....	
00000050	02	00	00	00	A7	00	00	00	50	42	DF	00	00	00	00	00		...\$...PBB.....	
00000060	D0	CD	08	01	00	00	00	00	10	0E	00	00	00	00	02	00		ĐÍ.....	
00000070	70	40	D7	00	00	00	00	00	3E	8B	1A	1C	90	65	D5	01		p@*.....><...eÖ.	
00000080	3E	81	1C	2C	00	00	00	00	68	00	00	80	00	00	00	00		>...h..€..... Length of volume path	
00000090	17	00	01	00	00	00	00	00	F0	2F	F5	82	00	00	00	00	ð/ð,....	
000000A0	00	84	D1	82	00	00	00	00	E1	CF	02	00	00	00	00	00		..Ñ,....áĪ.....	
000000B0	E0	D0	08	01	00	00	00	00	5C	00	44	00	45	00	56	00		àÐ.....\D.E.V.	
000000C0	49	00	43	00	45	00	5C	00	48	00	41	00	52	00	44	00		I.C.E.\H.A.R.D.	
000000D0	44	00	49	00	53	00	4B	00	56	00	4F	00	4C	00	55	00		D.I.S.K.V.O.L.U.	
000000E0	4D	00	45	00	32	00	00	00	30	4A	F5	82	00	00	00	00		M.E.2...0Jð,....	
000000F0	1B	00	32	1A	3E	C1	C7	AF	70	00	00	00	00	00	00	00		..2.>ÁÇ̄p.....	
00000100	50	4D	DF	00	00	00	00	00	C9	0A	00	00	00	00	00	00		PMB.....É.....	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	80	00	€.	
00000120	5C	00	57	00	49	00	4E	00	44	00	4F	00	57	00	53	00		\.W.I.N.D.O.W.S.	
00000130	5C	00	53	00	59	00	53	00	57	00	4F	00	57	00	36	00		\.S.Y.S.W.O.W.6.	
00000140	34	00	5C	00	4D	00	53	00	48	00	54	00	4D	00	4C	00		4.\.M.S.H.T.M.L.	
00000150	2E	00	44	00	4C	00	4C	00	00	00	00	00	00	00	00	00		..D.L.L.....	
00000160	00	10	00	00	04	00	00	00	00	00	30	00	00	10	00	00	0.....	

AgCx.db (decompressed)

Database Parameters Type

- Parameters are defined for a specific **FileType**.
- 16 different types of **FileType**.
- 2 main uses:
 - offset calculation on the file.
 - database size parameters.

```

.data:00000001800F0668 00 00 00 00 00 00 00 00 align 10h
.data:00000001800F0670 48 PFDATABASEPARAMSFORFILETYPE db 48h ;
.data:00000001800F0670
.data:00000001800F0670
.data:00000001800F0671 00 db 0
.data:00000001800F0672 00 db 0
.data:00000001800F0673 00 db 0
.data:00000001800F0674 40 db 40h ; @
.data:00000001800F0675 00 db 0
.data:00000001800F0676 00 db 0
.data:00000001800F0677 00 db 0
.data:00000001800F0678 58 db 58h ; X
.data:00000001800F0679 00 db 0
.data:00000001800F067A 00 db 0
.data:00000001800F067B 00 db 0
.data:00000001800F067C 10 db 10h
.data:00000001800F067D 00 db 0
.data:00000001800F067E 00 db 0
.data:00000001800F067F 00 db 0
.data:00000001800F0680 10 db 10h
.data:00000001800F0681 00 db 0
.data:00000001800F0682 00 db 0
.data:00000001800F0683 00 db 0
.data:00000001800F0684 10 db 10h
.data:00000001800F0685 00 db 0
.data:00000001800F0686 00 db 0
.data:00000001800F0687 00 db 0
.data:00000001800F0688 10 db 10h
.data:00000001800F0689 00 db 0
.data:00000001800F068A 00 db 0
.data:00000001800F068B 00 db 0
.data:00000001800F068C 00 db 0
.data:00000001800F068D 00 db 0
.data:00000001800F068E 00 db 0
.data:00000001800F068F 00 db 0
.data:00000001800F0690 00 db 0

```

DatabaseParams in SysMain.sys

Database Parameters

- Parameters are defined for a specific **FileType**.
- 16 different types of **FileType**.
- 2 main uses:
 - offset calculation on the file.
 - database size parameters.

FileType	Params	.db file associated seen
5	< 40h; 58h; 10h; 10h; 10h ; 10h; 0h; 0h>	
6	< 48h; 58h; 60h; 18h; 20h ; 10h; 10h; 0h>	
7	< 48h; 48h ;60h ;18h ;10h ;10h ;10h; 0h>	
8	< 60h; 38h; 50h; 8; 8; 14h ; 8 ; 0h>	
9	< 0 >	
A	< 60h; 38h; 50h; 8; 8; C ; 8h ; 0h>	
B	< 60h; 38h; 50h; 10h; 10h; 10h ; 10h ; 0h>	AgGIUAD_P%s.db
C	< 60h; 38h; 50h; C; 08h; 08h; 08h; 0h ;0h>	AgCx_%s.db ; AgCx_Sc%u%s.db
D	< 0 >	
E	<48h; 70h; 90h; 10h; 10h; 10h; 10h; 0h >	AgRobust.db
F	<68h; 40h; 50h; 8h; 8h; 14h; 8h; 0h>	
10	<60h; 40h; 88h; 10h; 18h; 8h; 8h; 0h>	
11	< 0 >	
12	< 50h; 50h; 58h; 18h; 10h; 10h; 10h; 0h>	
13	<60h; 38h; 50h; 8h; 8h; 8h; 8h>	Dynrespri.9db; cadrespri.7db
	<60h; 40h; 58h; 10h; 8h; 8h; 8h	
15	<60h; 50h; 58h; 10h; 18h; 8h; 8h;0h; >	AgGIFaultHistory.db AgGIFgAppHistory.db AgGIGlobalHistory.db AgGIUAD_S_%s.db
16	<60h; 40h; 50h; 8h; 8h; 8h; 8h;0h>	Dynrespri.9db; cadrespri.7db

DatabaseParams in SysMain.sys

Database files: decompressed format

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	03	00	00	00	B8	CF	4B	00	58	00	00	00	0C	00	00	00IK.X.....
00000010	60	00	00	00	38	00	00	00	50	00	00	00	0C	00	00	00	...8...P.....
00000020	08	00	00	00	08	00	00	00	08	00	00	00	00	00	00	00
00000030	00	00	00	00	02	00	00	00	16	0E	00	00	8B	5E	05	00<^..
00000040	51	00	00	00	DC	05	08	00	00	00	00	00	00	00	00	00	Q...Ü.....
00000050	02	00	00	00	A7	00	00	00	50	42	DF	00	00	00	00	00	...\$...PBB.....
00000060	D0	CD	08	01	00	00	00	00	10	0E	00	00	00	00	02	00	ĐÍ.....
00000070	70	40	D7	00	00	00	00	00	3E	8B	1A	1C	90	65	D5	01	p&x...>...eö.
00000080	3E	81	1C	2C	00	00	00	00	68	00	00	80	00	00	00	00	>...h...€....
00000090	17	00	01	00	00	00	00	00	F0	2F	F5	82	00	00	00	00	...8/8,...
000000A0	00	84	D1	82	00	00	00	00	E1	CF	02	00	00	00	00	00	..Ñ,...áí.....
000000B0	E0	D0	08	01	00	00	00	00	5C	00	44	00	45	00	56	00	àĐ.....\D.E.V.
000000C0	49	00	43	00	45	00	5C	00	48	00	41	00	52	00	44	00	I.C.E.\H.A.R.D.
000000D0	44	00	49	00	53	00	4B	00	56	00	4F	00	4C	00	55	00	D.I.S.K.V.O.L.U.
000000E0	4D	00	45	00	32	00	00	00	30	4A	F5	82	00	00	00	00	M.E.2...0J8,...
000000F0	1B	00	32	1A	3E	C1	C7	AF	70	00	00	00	00	00	00	00	..2.>ÄÇp.....
00000100	50	4D	DF	00	00	00	00	00	C9	0A	00	00	00	00	00	00	PMB.....É.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	80	00€.
00000120	5C	00	57	00	49	00	4E	00	44	00	4F	00	57	00	53	00	\.W.I.N.D.O.W.S.
00000130	5C	00	53	00	59	00	53	00	57	00	4F	00	57	00	36	00	\.S.Y.S.W.O.W.6.
00000140	34	00	5C	00	4D	00	53	00	48	00	54	00	4D	00	4C	00	4.\.M.S.H.T.M.L.
00000150	2E	00	44	00	4C	00	4C	00	00	00	00	00	00	00	00	00	..D.L.L.....
00000160	00	10	00	00	04	00	00	00	00	00	30	00	00	10	00	000.....

End of header

Length of volume path

Offset of volume path :
End of header + Param 1

End of volume path :
Beginning + 2*(length + 1)

Offset of string 2 :
End of vol. path + Param 2

End of string 2 :
Beginning + 2*(x << 2 + 1)

AgCx.db (decompressed)

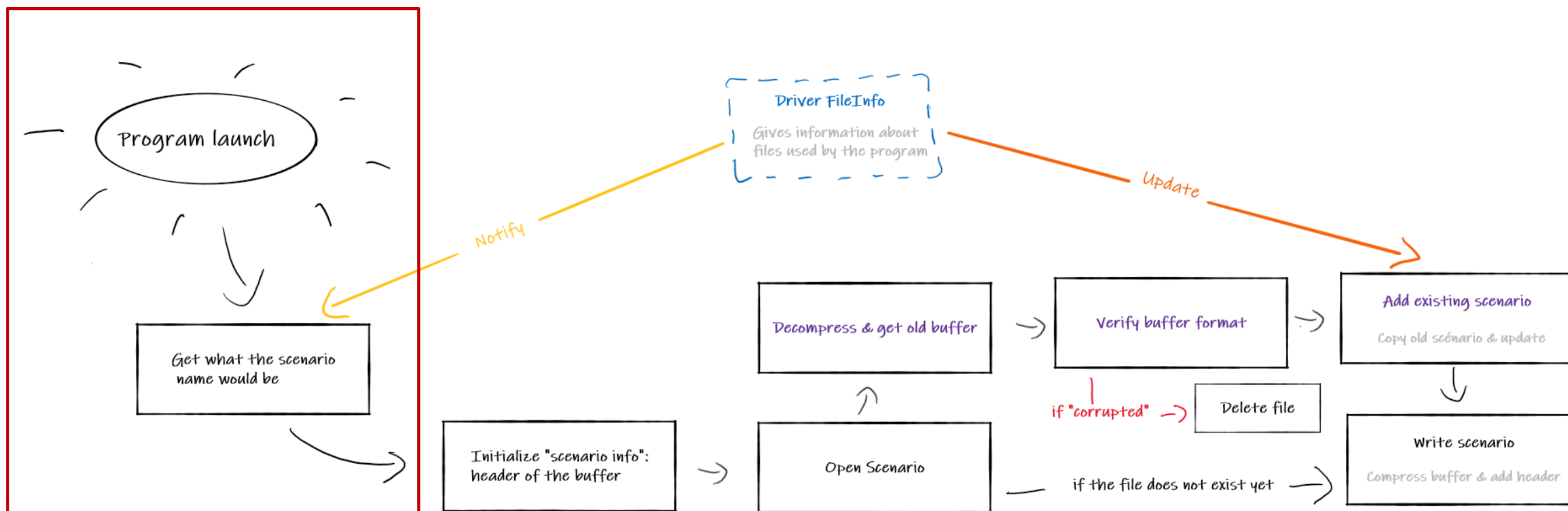
Scenario files: generalities

SPOTIFY.EXE-5FAE3A5B.pf	6/21/2020 10:37 PM	PF File	17 KB
SPOTIFY.EXE-5FAE3A53.pf	6/21/2020 10:37 PM	PF File	44 KB
SPPSVC.EXE-B0F8131B.pf	6/21/2020 9:03 PM	PF File	10 KB
STARTMENUEXPERIENCEHOST.EXE-4612B8FC.pf	6/21/2020 9:02 PM	PF File	33 KB
SVCHOST.EXE-4BA0E729.pf	6/21/2020 10:27 PM	PF File	17 KB

C:\Windows\Prefetch directory

- Each scenario file name is : « NameoftheApp - 8DIGITS.pf ».
- File ending with .pf : **trace of an application**. One application could have one or more scenario files, depending on the context of its execution.
- Information defined on the registry : *SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Prefetcher*
 - **MaxPrefetchFiles** : by default 256.
 - **MaxPrefetchFileSize** : by default 10485760 bytes.

Scenario files: construction

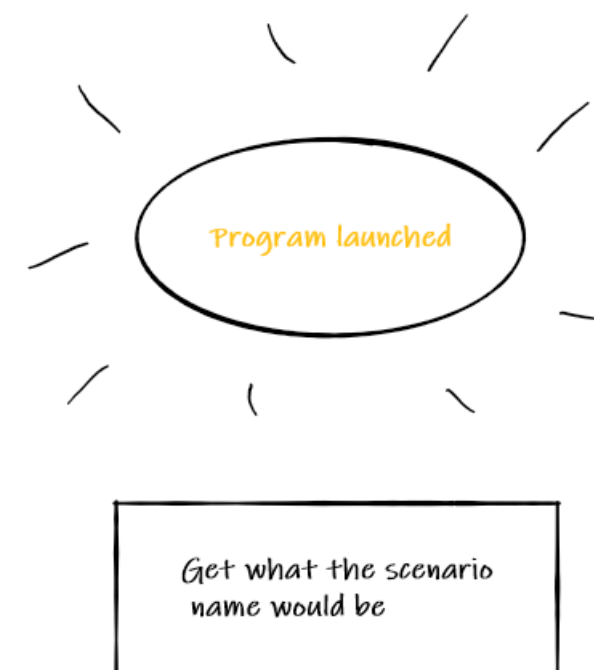


Scenario files: names

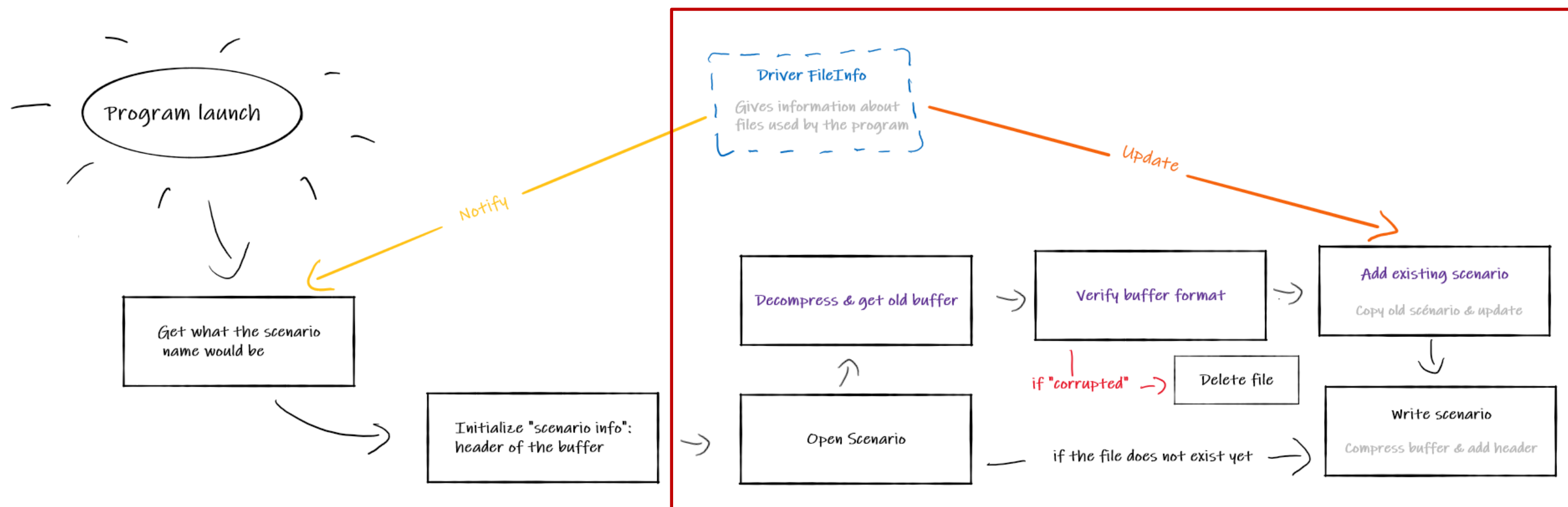
- The name results from the **full application path hashed** with the following algorithm :

```
StringHashed = 314159;
for (i = 0; i < Length(StringToHash); i++)
{
    Char = StringToHash[i];
    UpChar = RtlUppcaseUnicodeChar(c);
    StringHashed = (StringHashed * 37 + UpChar) * 37;
}
```

- Note that this algorithm **depends on your Windows version**. The following elements might change :
 - Initialization value of StringHashed.
 - Adding a modulo operation.
 - Adding a multiplier coefficient.



Scenario files: construction



The driver FileInfo

- The way to access information from ring 0 via a minifilter driver.
- Its main job is to provide name and information (read/write operations) about files.
- Follows each operation of every file for all processes, thanks to minifilter driver stream context.
- Splits a buffer formatted in a format « NL », which is going to be translated to the final path.

```

2e 00 2e 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
5c 00 44 00 45 00 56 00-49 00 43 00 45 00 5c 00 \.D.E.V.I.C.E.\.
48 00 41 00 52 00 44 00-44 00 49 00 53 00 4b 00 H.A.R.D.D.I.S.K.
56 00 4f 00 4c 00 55 00-4d 00 45 00 32 00 00 00 V.O.L.U.M.E.2...
40 03 00 00 97 10 17 23-02 00 00 00 00 00 00 00 @.....#.....
c0 95 de 7e 08 c6 ff ff-30 e0 15 72 86 dc ff ff ...~....0..r....
01 00 00 00 00 00 00 00-01 00 1a 00 5c 00 53 00 .....\.S.
59 00 53 00 54 00 45 00-4d 00 20 00 56 00 4f 00 Y.S.T.E.M. .V.O.
4c 00 55 00 4d 00 45 00-20 00 49 00 4e 00 46 00 L.U.M.E. .I.N.F.
4f 00 52 00 4d 00 41 00-54 00 49 00 4f 00 4e 00 O.R.M.A.T.I.O.N.
00 00 00 00 00 00 00 00-40 03 00 00 97 10 17 23 .....@.....#
03 00 00 00 00 00 00 00-00 47 10 80 08 c6 ff ff .....G.....
30 e0 15 72 86 dc ff ff-01 00 00 00 00 00 00 00 0..r.....
01 00 1c 00 5c 00 24 00-45 00 58 00 54 00 45 00 ....\.$.E.X.T.E.
4e 00 44 00 5c 00 24 00-52 00 4d 00 4d 00 45 00 N.D.\.$.R.M.M.E.
54 00 41 00 44 00 41 00-54 00 41 00 5c 00 24 00 T.A.D.A.T.A.\.$.
54 00 58 00 46 00 4c 00-4f 00 47 00 00 00 00 00 T.X.F.L.O.G.....
c0 01 00 00 97 10 17 23-04 00 00 00 00 00 00 00 .....#.....
10 40 16 72 86 dc ff ff-30 e0 15 72 86 dc ff ff .@.r....0..r....
01 00 00 00 00 00 00 00-01 00 05 00 5c 00 24 00 .....\.$.
4d 00 46 00 54 00 00 00-00 02 00 00 97 10 17 23 M.F.T.....#
05 00 00 00 00 00 00 00-20 6b 16 72 86 dc ff ff ..... k.r....
30 e0 15 72 86 dc ff ff-01 00 00 00 00 00 00 00 0..r.....
01 00 09 00 5c 00 24 00-4c 00 4f 00 47 00 46 00 ....\.$.L.O.G.F.
49 00 4c 00 45 00 00 00-80 03 00 00 97 10 17 23 I.L.E.....#
06 00 00 00 00 00 00 00-b0 4c 06 80 08 c6 ff ff .....L.....
30 e0 15 72 86 dc ff ff-01 00 00 00 00 00 00 00 0..r.....
01 00 1f 00 5c 00 24 00-53 00 45 00 43 00 55 00 ....\.$.S.E.C.U.
52 00 45 00 3a 00 24 00-53 00 49 00 49 00 3a 00 R.E.:$.S.I.I.:.
24 00 49 00 4e 00 44 00-45 00 58 00 5f 00 41 00 $.I.N.D.E.X._.A.
4c 00 4c 00 4f 00 43 00-41 00 54 00 49 00 4f 00 L.L.O.C.A.T.I.O.
4e 00 00 00 00 00 00 00-40 02 00 00 97 10 17 23 N.....@.....#

```

Buffer sent by FileInfo to SysMain

Scenario files: compressed format

	Magic Number	Decompressed Size		
00000000	4D 41 4D 04	3A 86 03 00	85 A8 A7 A9 A9 A8 AA A9	MAM.:†....."§@@`²@
00000010	A9 A8 A9 AA A9 A8 A9 A9 A9 98 A9 AA B8 B8 AA AA			©`©²©`©©©`©²,₂,²²
00000020	A8 A8 BA A9 B9 A8 BA A9 A9 A8 AA AA A9 A8 BA BA			""°©¹""°©©""²²©""°°
00000030	B9 A8 AA A9 A9 A8 AA AA B9 A8 B9 AA A8 A8 A9 BA			¹""²©©""²²¹""¹²""©°
00000040	A9 B8 BA AA B9 A8 BA AA B9 A8 BB AA B9 B8 BA A9			©, °²¹""°²¹""»²¹,°©
00000050	A9 B8 BA AB A9 C8 BB AA B9 A8 BA AA B9 A8 AA AA			©, °«©É»²¹""°²¹""²²

Scenario file : VLC.EXE-73B04BFB.pf (compressed)

Scenario files: decompressed format

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	1E	00	00	00	53	43	43	41	11	00	00	00	3A	86	03	00SCCA....:†..
00000010	56	00	4C	00	43	00	2E	00	45	00	58	00	45	00	00	00	V.L.C...E.X.E...
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	FB	4B	B0	73ûK°s
00000050	00	00	00	00	28	01	00	00	FC	01	00	00	A8	3E	00	00(....i....">..
00000060	BA	33	00	00	78	DC	01	00	92	6D	01	00	88	4A	03	00	°3...xÛ...'m...'J..
00000070	01	00	00	00	B2	3B	00	00	3C	00	00	00	02	00	00	00°;...<.....
00000080	2E	D0	CE	A5	CE	3A	D6	01	D9	67	43	12	CD	3A	D6	01	.ĐÍ¥Í:Ö.ÛgC.Í:Ö.
00000090	22	EF	1D	36	CB	3A	D6	01	C6	D5	DE	C7	CA	3A	D6	01	"i.6È:Ö.ÈÖPÇÈ:Ö.
000000A0	3C	8D	3F	4C	03	48	D6	01	E2	D8	FA	B7	02	48	D6	01	<.¿L.HÖ.âøú.HÖ.
000000B0	A3	C8	FC	B7	02	48	D6	01	7C	D7	87	2A	D6	47	D6	01	£Èü.HÖ. *+*ÖGÖ.
000000C0	00	00	00	00	00	00	00	01	00	00	00	01	00	00	00	03
000000D0	00	00	00	0A	4A	03	00	78	00	00	00	00	00	00	00	00J..x.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Scenario file : VLC.EXE-73B04BFB.pf (decompressed)

Scenario files: content

- Contains the full paths of file needed to **avoid page faults**.
- In other words three kinds of file :
 - **Every time consulted files**, such as dll, dependencies.
 - **Recent files** such as personal files.
 - **Cache files**, because they are non-stop consulted.

```
0003BDA0 4C 00 2E 00 44 00 4C 00 4C 00 00 00 5C 00 56 00 L...D.L.L...\V.  
0003BDB0 4F 00 4C 00 55 00 4D 00 45 00 7B 00 30 00 31 00 O.L.U.M.E.{.0.1.  
0003BDC0 64 00 34 00 33 00 62 00 65 00 36 00 62 00 62 00 d.4.3.b.e.6.b.b.  
0003BDD0 37 00 35 00 66 00 64 00 36 00 35 00 2D 00 30 00 7.5.f.d.6.5.-.0.  
0003BDE0 61 00 62 00 62 00 61 00 33 00 36 00 31 00 7D 00 a.b.b.a.3.6.1.).  
0003BDF0 5C 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 \.W.I.N.D.O.W.S.  
0003BE00 5C 00 53 00 59 00 53 00 54 00 45 00 4D 00 33 00 \.S.Y.S.T.E.M.3.  
0003BE10 32 00 5C 00 45 00 58 00 50 00 4C 00 4F 00 52 00 2.\.E.X.P.L.O.R.  
0003BE20 45 00 52 00 46 00 52 00 41 00 4D 00 45 00 2E 00 E.R.F.R.A.M.E...  
0003BE30 44 00 4C 00 4C 00 00 00 5C 00 56 00 4F 00 4C 00 D.L.L...\V.O.L.  
0003BE40 55 00 4D 00 45 00 7B 00 30 00 31 00 64 00 34 00 U.M.E.{.0.1.d.4.  
0003BE50 33 00 62 00 65 00 30 00 38 00 61 00 31 00 34 00 3.b.e.0.8.a.1.4.  
0003BE60 33 00 61 00 61 00 61 00 2D 00 65 00 38 00 38 00 3.a.a.a.-.e.8.8.  
0003BE70 61 00 62 00 35 00 38 00 66 00 7D 00 5C 00 4D 00 a.b.5.8.f.}\.M.  
0003BE80 59 00 20 00 4D 00 4F 00 56 00 49 00 45 00 53 00 Y. .M.O.V.I.E.S.  
0003BE90 5C 00 4D 00 41 00 52 00 56 00 45 00 4C 00 20 00 \.M.A.R.V.E.L. .  
0003BEA0 2D 00 20 00 47 00 55 00 41 00 52 00 44 00 49 00 -. .G.U.A.R.D.I.  
0003BEB0 41 00 4E 00 20 00 4F 00 46 00 20 00 54 00 48 00 A.N. .O.F. .T.H.  
0003BEC0 45 00 20 00 47 00 41 00 4C 00 41 00 58 00 59 00 E. .G.A.L.A.X.Y.  
0003BED0 2E 00 4D 00 4B 00 56 00 00 00 5C 00 56 00 4F 00 .M.K.V...\V.O.  
0003BEE0 4C 00 55 00 4D 00 45 00 7B 00 30 00 31 00 64 00 L.U.M.E.{.0.1.d.  
0003BEF0 34 00 33 00 62 00 65 00 30 00 38 00 61 00 31 00 34 00 4.3.b.e.0.8.a.1.4.
```

Scenario file : VLC.EXE-5A3EF7FA.pf (decompressed)

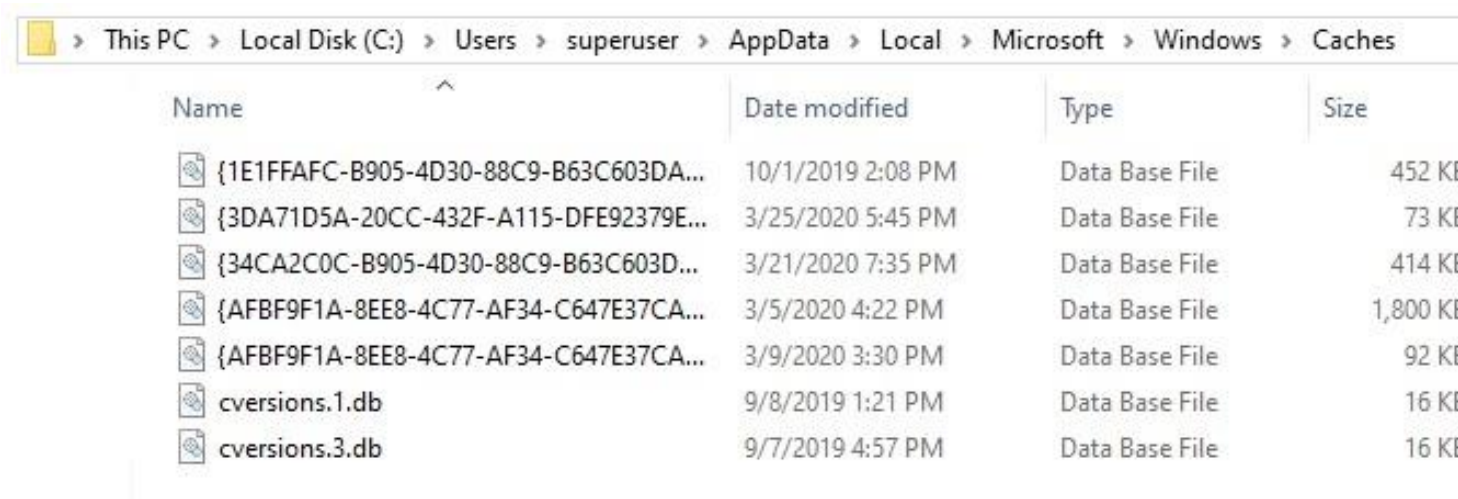
Scenario files: content

- Contains the full paths of file needed to **avoid page faults**.
- In other words three kinds of file :
 - **Every time consulted files**, such as dll, dependencies.
 - **Recent files** such as personal files.
 - **Cache files**, because they are non-stop consulted.

```
0006C780 5C 00 56 00 4F 00 4C 00 55 00 4D 00 45 00 7B 00 \.V.O.L.U.M.E.{.
0006C790 30 00 31 00 64 00 35 00 33 00 38 00 32 00 61 00 0.1.d.5.3.8.2.a.
0006C7A0 37 00 62 00 33 00 35 00 35 00 32 00 65 00 65 00 7.b.3.5.5.2.e.e.
0006C7B0 2D 00 61 00 36 00 37 00 62 00 34 00 61 00 66 00 -.a.6.7.b.4.a.f.
0006C7C0 63 00 7D 00 5C 00 50 00 52 00 4F 00 47 00 52 00 c.}.\.P.R.O.G.R.
0006C7D0 41 00 4D 00 44 00 41 00 54 00 41 00 5C 00 4D 00 A.M.D.A.T.A.\.M.
0006C7E0 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 I.C.R.O.S.O.F.T.
0006C7F0 5C 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 \.W.I.N.D.O.W.S.
0006C800 5C 00 43 00 41 00 43 00 48 00 45 00 53 00 5C 00 \.C.A.C.H.E.S.\.
0006C810 7B 00 36 00 41 00 46 00 30 00 36 00 39 00 38 00 {.6.A.F.0.6.9.8.
0006C820 45 00 2D 00 44 00 35 00 35 00 38 00 2D 00 34 00 E.-.d.5.5.8.-.4.
0006C830 46 00 36 00 45 00 2D 00 39 00 42 00 33 00 43 00 F.6.E.-.9.B.3.C.
0006C840 2D 00 33 00 37 00 31 00 36 00 36 00 38 00 39 00 -.3.7.1.6.6.8.9.
0006C850 41 00 46 00 34 00 39 00 33 00 7D 00 2E 00 32 00 A.F.4.9.3.}...2.
0006C860 2E 00 56 00 45 00 52 00 30 00 58 00 30 00 30 00 ..V.E.R.O.X.0.0.
0006C870 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 0.0.0.0.0.0.0.0.
0006C880 30 00 30 00 30 00 30 00 30 00 31 00 2E 00 44 00 0.0.0.0.0.1...D.
0006C890 42 00 00 00 5C 00 56 00 4F 00 4C 00 55 00 4D 00 B...\.V.O.L.U.M.
```

Scenario file : VLC.EXE-5A3EF7FA.pf (decompressed)

The cache files



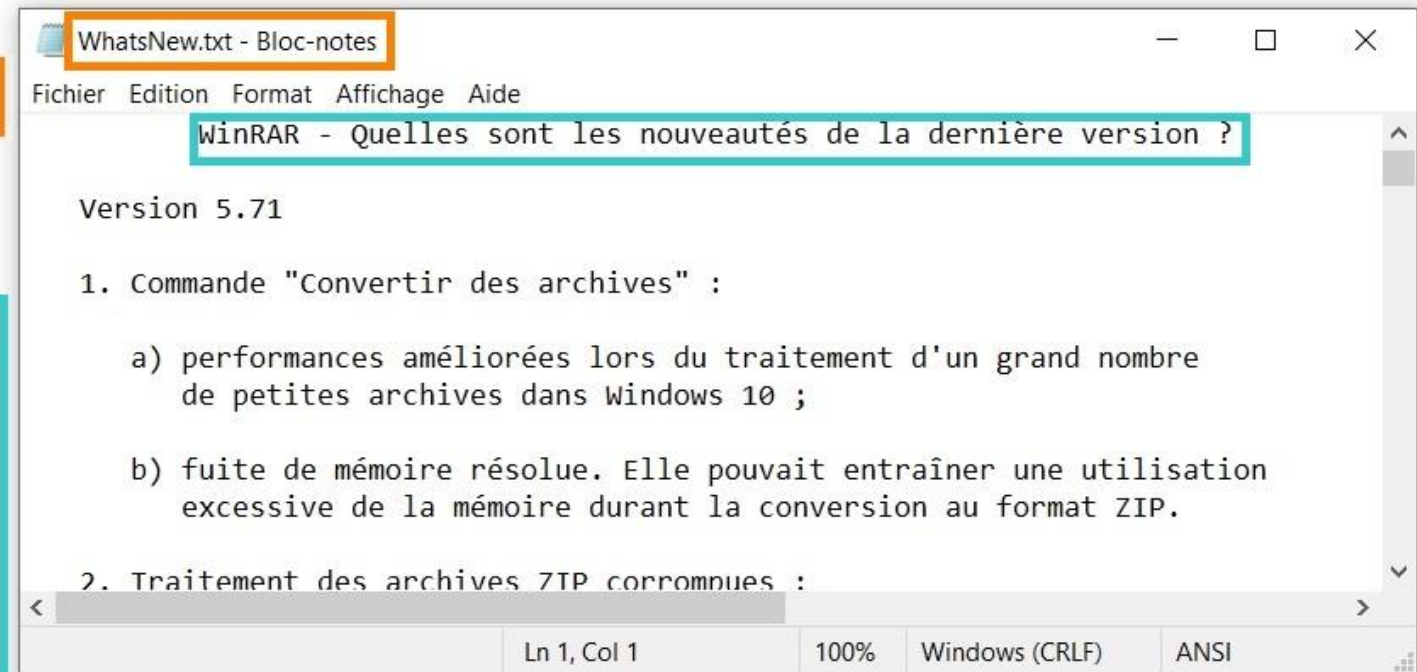
Name	Date modified	Type	Size
{1E1FFAFC-B905-4D30-88C9-B63C603DA...}	10/1/2019 2:08 PM	Data Base File	452 KB
{3DA71D5A-20CC-432F-A115-DFE92379E...}	3/25/2020 5:45 PM	Data Base File	73 KB
{34CA2C0C-B905-4D30-88C9-B63C603D...}	3/21/2020 7:35 PM	Data Base File	414 KB
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA...}	3/5/2020 4:22 PM	Data Base File	1,800 KB
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA...}	3/9/2020 3:30 PM	Data Base File	92 KB
cversions.1.db	9/8/2019 1:21 PM	Data Base File	16 KB
cversions.3.db	9/7/2019 4:57 PM	Data Base File	16 KB

Windows Cache directory

- Superfetch references **cache files**.
- Cache is a memory management which temporarily stores data to **reduce access time** to these data later, in the cache files.

What about the content of the file?

```
00008D60 78 00 74 00 00 00 00 43 00 3A 00 5C 00 50 00 x.t.....C.:.\.P.  
00008D70 72 00 6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 r.o.g.r.a.m. .F.  
00008D80 69 00 6C 00 65 00 73 00 5C 00 57 00 69 00 6E 00 i.l.e.s.\.W.i.n.  
00008D90 52 00 41 00 52 00 5C 00 57 00 68 00 61 00 74 00 R.A.R.\.W.h.a.t.  
00008DA0 73 00 4E 00 65 00 77 00 2E 00 74 00 78 00 74 00 s.N.e.w...t.x.t.  
00008DB0 00 00 00 00 00 00 00 7B 00 36 00 44 00 38 00 .....{.6.D.8.  
00008DC0 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 0.9.3.7.7.-.6.A.  
00008DD0 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00 F.0.-.4.4.4.B.-.  
00008DE0 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 8.9.5.7.-.A.3.7.  
00008DF0 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 7.3.F.0.2.2.0.0.  
00008E00 45 00 7D 00 5C 00 57 00 69 00 6E 00 52 00 41 00 E.)\.\.W.i.n.R.A.  
00008E10 52 00 5C 00 57 00 68 00 61 00 74 00 73 00 4E 00 R.\.W.h.a.t.s.N.  
00008E20 65 00 77 00 2E 00 74 00 78 00 74 00 00 00 00 00 e.w...t.x.t.....  
00008E30 57 00 69 00 6E 00 52 00 41 00 52 00 00 00 00 00 W.i.n.R.A.R.....  
00008E40 51 00 75 00 65 00 6C 00 6C 00 65 00 73 00 20 00 Q.u.e.l.l.e.s. .  
00008E50 73 00 6F 00 6E 00 74 00 20 00 6C 00 65 00 73 00 s.o.n.t. .l.e.s.  
00008E60 20 00 6E 00 6F 00 75 00 76 00 65 00 61 00 75 00 .n.o.u.v.e.a.u.  
00008E70 74 00 E9 00 73 00 20 00 64 00 65 00 20 00 6C 00 t.é.s. .d.e. .l.  
00008E80 61 00 20 00 64 00 65 00 72 00 6E 00 69 00 E8 00 a..d.e.r.n.i.è.  
00008E90 72 00 65 00 20 00 76 00 65 00 72 00 73 00 69 00 r.e. .v.e.r.s.i.  
00008EA0 6F 00 6E 00 00 00 00 00 07 AC AC 00 08 8F 00 00 o.n.....
```



Extract of a cache file

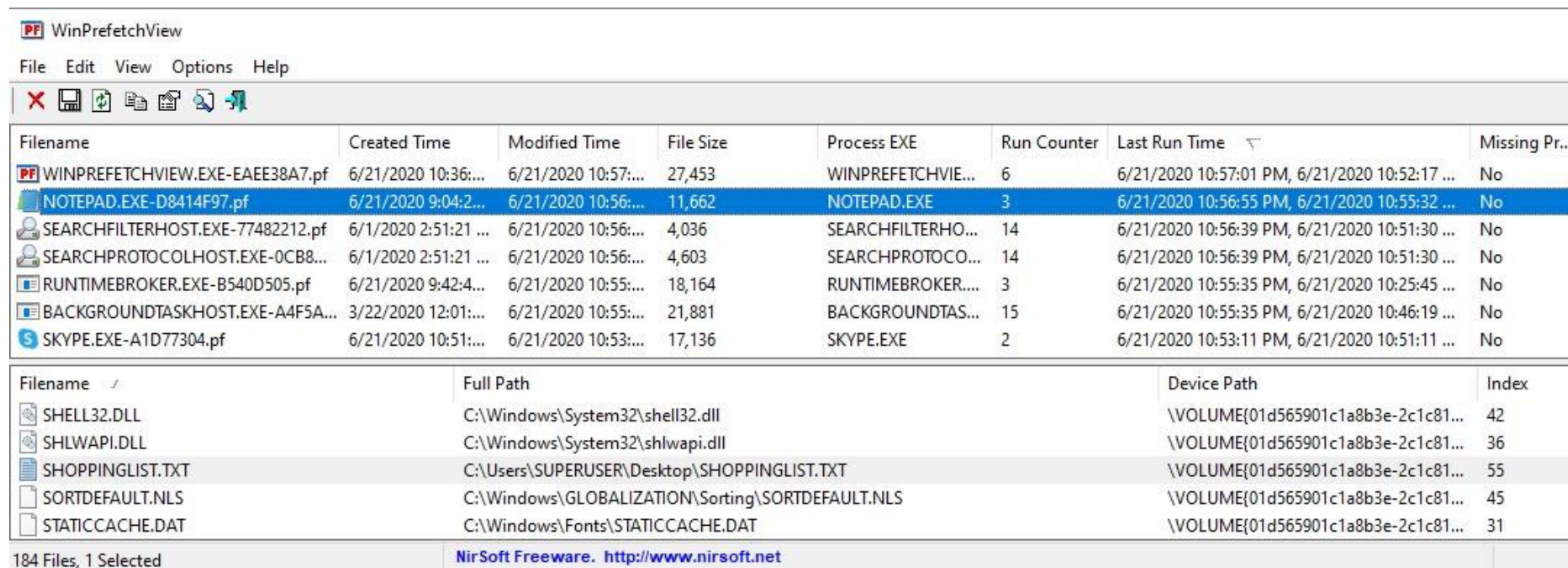
- Superfetch references **cache files** ...
- ... and cache files can contain data in **cleartext** files.

What can be done?

- Track user activities.
- Find personal file location.
- View personal content.
- Prove software installs.
- But you can also protect yourself from this...

Time to fool your OS!

Exploit the scenarios



Filename	Created Time	Modified Time	File Size	Process EXE	Run Counter	Last Run Time	Missing Pr...
WINPREFETCHVIEW.EXE-EAEE38A7.pf	6/21/2020 10:36:...	6/21/2020 10:57:...	27,453	WINPREFETCHVIE...	6	6/21/2020 10:57:01 PM, 6/21/2020 10:52:17 ...	No
NOTEPAD.EXE-D8414F97.pf	6/21/2020 9:04:2...	6/21/2020 10:56:...	11,662	NOTEPAD.EXE	3	6/21/2020 10:56:55 PM, 6/21/2020 10:55:32 ...	No
SEARCHFILTERHOST.EXE-77482212.pf	6/1/2020 2:51:21 ...	6/21/2020 10:56:...	4,036	SEARCHFILTERHO...	14	6/21/2020 10:56:39 PM, 6/21/2020 10:51:30 ...	No
SEARCHPROTOCOLHOST.EXE-0CB8...	6/1/2020 2:51:21 ...	6/21/2020 10:56:...	4,603	SEARCHPROTOCO...	14	6/21/2020 10:56:39 PM, 6/21/2020 10:51:30 ...	No
RUNTIMEBROKER.EXE-B540D505.pf	6/21/2020 9:42:4...	6/21/2020 10:55:...	18,164	RUNTIMEBROKER...	3	6/21/2020 10:55:35 PM, 6/21/2020 10:25:45 ...	No
BACKGROUNDTASKHOST.EXE-A4F5A...	3/22/2020 12:01:...	6/21/2020 10:55:...	21,881	BACKGROUND TAS...	15	6/21/2020 10:55:35 PM, 6/21/2020 10:46:19 ...	No
SKYPE.EXE-A1D77304.pf	6/21/2020 10:51:...	6/21/2020 10:53:...	17,136	SKYPE.EXE	2	6/21/2020 10:53:11 PM, 6/21/2020 10:51:11 ...	No

Filename	Full Path	Device Path	Index
SHELL32.DLL	C:\Windows\System32\shell32.dll	\VOLUME{01d565901c1a8b3e-2c1c81...	42
SHLWAPI.DLL	C:\Windows\System32\shlwapi.dll	\VOLUME{01d565901c1a8b3e-2c1c81...	36
SHOPPINGLIST.TXT	C:\Users\SUPERUSER\Desktop\SHOPPINGLIST.TXT	\VOLUME{01d565901c1a8b3e-2c1c81...	55
SORTDEFAULT.NLS	C:\Windows\GLOBALIZATION\Sorting\SORTDEFAULT.NLS	\VOLUME{01d565901c1a8b3e-2c1c81...	45
STATICCACHE.DAT	C:\Windows\Fonts\STATICCACHE.DAT	\VOLUME{01d565901c1a8b3e-2c1c81...	31

184 Files, 1 Selected | NirSoft Freeware. <http://www.nirsoft.net>

WinPrefetchView

- In 2010, Nirsoft built a tool to view the **content of the scenario files**.
- Still...
 - The tool is close source.
 - Information provided is only about .pf files.
 - Data cannot be edited...

Our tool

- Open source!
- Possibility for .db and .pf to:
 - Compress;
 - Decompress;
 - View information;
 - **Edit information...**
- Possibility to hash with Windows 10 Superfetch algorithm.

```
----- MENU -----
1 - View Information.
2 - Decompress a pf/db file.
3 - Compress pf/db file.
4 - Modify a file.
5 - Hash a string.
--- Press any key to quit.
What would you like to do ? 1

1 ; Let's do that!

Precise a file or enter n: n

----- INFORMATION -----

[+] File viewed: DefaultFiles\ida_result.pf.
Format: 1E - Windows 10
Compressed File Size: 181776 bytes
Program concerned: IDAQ64.EXE
Program hash: 589600DD

Count of executions: 101
Last time executed: 28-11-2019 at 9:05

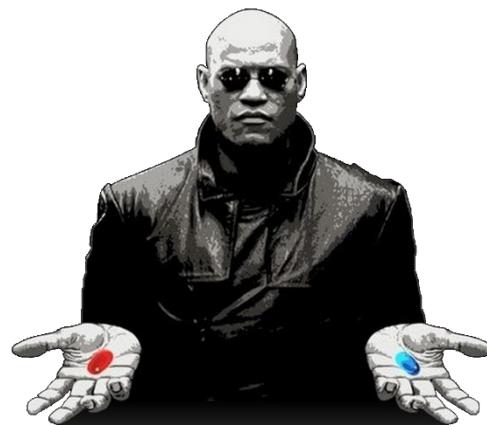
Executed also on: 17-11-2019 at 08:38
Executed also on: 17-11-2019 at 15:53
Executed also on: 20-11-2019 at 09:10
Executed also on: 20-11-2019 at 19:36
Executed also on: 21-11-2019 at 09:05
Executed also on: 26-11-2019 at 09:44
Executed also on: 27-11-2019 at 07:52

Count of paths : 200
Entries:
\VOLUME{01d5382a7b3552ee-a67b4afc}\WINDOWS\SYSWOW64\HHCTRL.OCX
\VOLUME{01d5382a7b3552ee-a67b4afc}\PROGRAM FILES (X86)\IDA 6.8\PLUGINS\STRINGS.P64
\VOLUME{01d5382a7b3552ee-a67b4afc}\PROGRAM FILES (X86)\IDA 6.8\PLUGINS\UNPACK.P64
\VOLUME{01d5382a7b3552ee-a67b4afc}\PROGRAM FILES (X86)\IDA 6.8\PLUGINS\MAKEIDT.P64
\VOLUME{01d5382a7b3552ee-a67b4afc}\PROGRAM FILES (X86)\IDA 6.8\PLUGINS\CALLEE.P64
\VOLUME{01d5382a7b3552ee-a67b4afc}\PROGRAM FILES (X86)\IDA 6.8\PLUGINS\UISWITCH.P64
\VOLUME{01d5382a7b3552ee-a67b4afc}\PROGRAM FILES (X86)\IDA 6.8\PLUGINS\NEXTFIX.P64
```

The roadmap to fool SysMain

- Choose a program's scenario.
- Decompress it.
- Edit the data.
- Save & Compress it.
- Replace the original scenario with the falsified one and let the magic happen!

What if you want to avoid that?



What Windows Internals says...



Note You can enable or disable prefetching of the boot or application startups by editing the DWORD registry value `EnablePrefetcher` in the `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters` key. Set it to 0 to disable prefetching altogether, 1 to enable prefetching of only applications, 2 for prefetching of boot only, and 3 for both boot and applications.

Windows Internals 7, Part 1. Chapter 5, p 414.

- Still, nowadays, whatever the value of `EnablePrefetcher` the scenario files keep on being updated.

Another example: «PFSvSuperfetchCheckAndEnable»

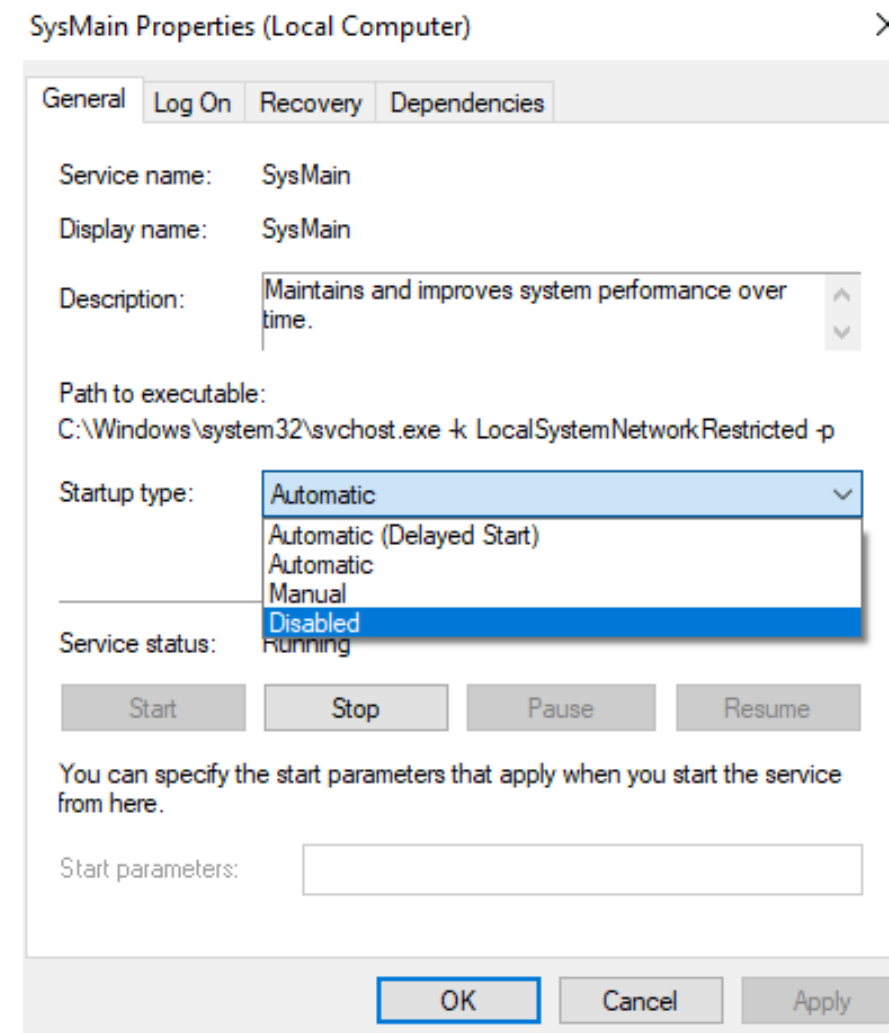
```
.STATUS PFSvSuperfetchCheckAndEnable()
{
    LSTATUS ErrCode_; // eax@1
    __int64 PFSucG; // rax@2
    HKEY hKey; // rcx@3
    int Data; // [sp+40h] [bp+8h]@3

    ErrCode_ = PFSuQueryPrefetchParameters(*(_QWORD *)&PFSucGlobals + 480i64);
    if ( !ErrCode_ )
    {
        PFSucG = *(_QWORD *)&PFSucGlobals;
        if ( *(_DWORD *)*(_QWORD *)&PFSucGlobals + 480i64 == 0x80000000 )
        {
            *(_DWORD *)*(_QWORD *)&PFSucGlobals + 480i64 = 3;
            hKey = *(HKEY *)*(_QWORD *)&PFSucGlobals + 1432; // HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
            Data = 3; // deals boot & softwares
            ErrCode_ = RegSetValueExW(hKey, L"EnableSuperfetch", 0, REG_DWORD, (const BYTE *)&Data, REG_DWORD);
            if ( ErrCode_ )
                return ErrCode_;
            PFSucG = *(_QWORD *)&PFSucGlobals;
        }
        ErrCode_ = (*(_BYTE *)*(_QWORD *)&PFSucGlobals + 480) & 3 == 0 ? (unsigned __int8)ERROR_IOPL_NOT_ENABLED : 0;
    }
    return ErrCode_;
}
```

PFSvSuperfetchCheckAndEnable() function from SysMain.dll

The solution

- One way to disable SysMain is to manually set the startup type of the SysMain service in the Task Manager to "disabled".



SysMain properties

Finally

- Extended documentation on SysMain mechanisms & databases.
- Multifunction tool, available on github at: [MathildeVenault](#).
- Future research:
 - More interaction with drivers;
 - See further on Windows Cache;
 - Improving the tool.

Any questions?