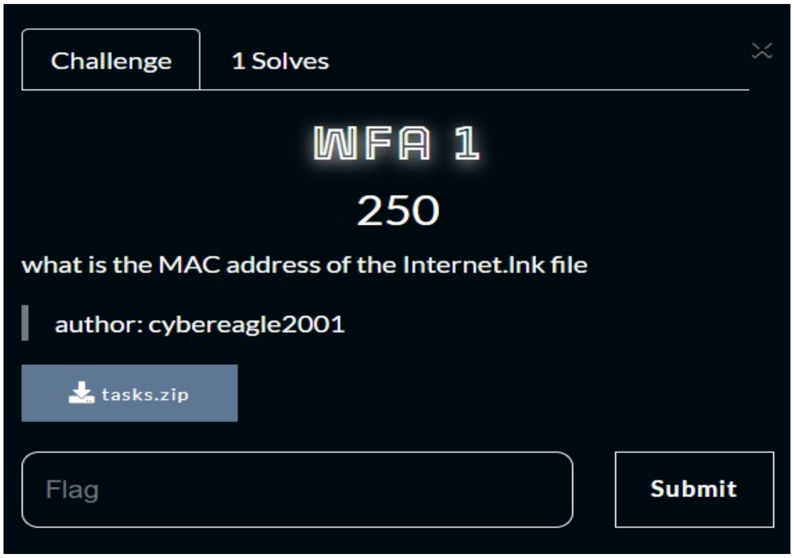
WFA Writeup
cybereagle2001
HackMaze V0.2

I – WFA 1:



WFA 1

250

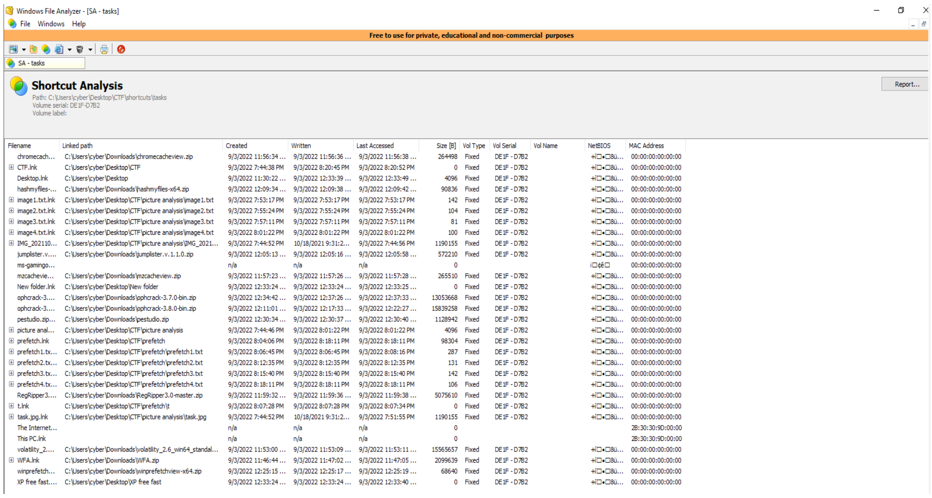
what is the MAC address of the Internet.lnk file

author: cybereagle2001

WFA means Windows File Analyser it's so important while investigating cyber crime to collect information about the hackers or the victims system in order to understand the actions and the life cycle of the different type of files the OS use and one of these files which are so interesting are the ICON's on the desktop.

The icons on the system can give us a lot of information about the computer and the behaviour of the user. One of these data is the MAC address let's try to use the WFA.exe an analyse the icons in the task.zip file:

After loading the shortcuts in the WFA tool we will get the following :



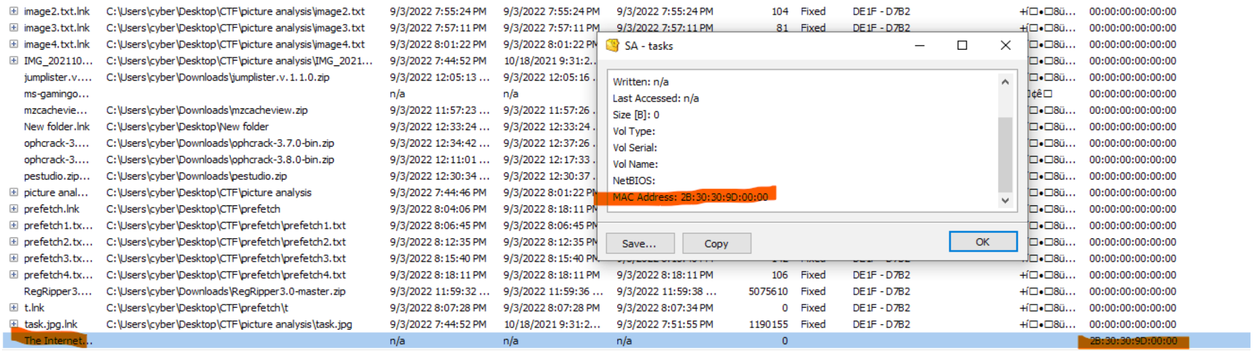
Windows File Analyzer - [SA - tasks]
File
Windows
Help
Free to use for private, educational and non-commercial purposes
SA - tasks
Report...

Shortcut Analysis

Path: C:\Users\cyber\Desktop\CTF\shortcuts\tasks
Volume serial: DE1F-D7B2
Volume label:

Filename	Linked path	Created	Written	Last Accessed	Size [B]	Vol Type	Vol Serial	Vol Name	NetBIOS	MAC Address
chromecach...	C:\Users\cyber\Downloads\chromecacheview.zip	9/3/2022 11:56:34 ...	9/3/2022 11:56:36 ...	9/3/2022 11:56:38 ...	264498	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
CTF.lnk	C:\Users\cyber\Desktop\CTF	9/3/2022 7:44:38 PM	9/3/2022 8:20:45 PM	9/3/2022 8:20:52 PM	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
Desktop.lnk	C:\Users\cyber\Desktop	9/3/2022 11:30:22 ...	9/3/2022 12:33:39 ...	9/3/2022 12:33:49 ...	4096	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
hashmyfiles-...	C:\Users\cyber\Downloads\hashmyfiles-x64.zip	9/3/2022 12:09:34 ...	9/3/2022 12:09:38 ...	9/3/2022 12:09:42 ...	90836	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
image1.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image1.txt	9/3/2022 7:53:17 PM	9/3/2022 7:53:17 PM	9/3/2022 7:53:17 PM	142	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
image2.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image2.txt	9/3/2022 7:55:24 PM	9/3/2022 7:55:24 PM	9/3/2022 7:55:24 PM	104	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
image3.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image3.txt	9/3/2022 7:57:11 PM	9/3/2022 7:57:11 PM	9/3/2022 7:57:11 PM	81	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
image4.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image4.txt	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM	100	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
IMG_202110...	C:\Users\cyber\Desktop\CTF\picture analysis\IMG_2021...	9/3/2022 7:44:52 PM	10/18/2021 9:31:2...	9/3/2022 7:44:56 PM	1190155	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
jumplister.v....	C:\Users\cyber\Downloads\jumplister.v.1.1.0.zip	9/3/2022 12:05:13 ...	9/3/2022 12:05:16 ...	9/3/2022 12:05:58 ...	572210	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
ms-gamingo...		n/a	n/a	n/a	0				i□¢ê□	00:00:00:00:00:00
mzcachevie...	C:\Users\cyber\Downloads\mzcacheview.zip	9/3/2022 11:57:23 ...	9/3/2022 11:57:26 ...	9/3/2022 11:57:28 ...	265510	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
New folder.lnk	C:\Users\cyber\Desktop\New folder	9/3/2022 12:33:24 ...	9/3/2022 12:33:24 ...	9/3/2022 12:33:25 ...	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
ophcrack-3....	C:\Users\cyber\Downloads\ophcrack-3.7.0-bin.zip	9/3/2022 12:34:42 ...	9/3/2022 12:37:26 ...	9/3/2022 12:37:33 ...	13053668	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
ophcrack-3....	C:\Users\cyber\Downloads\ophcrack-3.8.0-bin.zip	9/3/2022 12:11:01 ...	9/3/2022 12:17:33 ...	9/3/2022 12:22:27 ...	15839258	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
pestudio.zip...	C:\Users\cyber\Downloads\pestudio.zip	9/3/2022 12:30:34 ...	9/3/2022 12:30:37 ...	9/3/2022 12:30:40 ...	1128942	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
picture anal...	C:\Users\cyber\Desktop\CTF\picture analysis	9/3/2022 7:44:46 PM	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM	4096	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
prefetch.lnk	C:\Users\cyber\Desktop\CTF\prefetch	9/3/2022 8:04:06 PM	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	98304	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
prefetch1.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch1.txt	9/3/2022 8:06:45 PM	9/3/2022 8:06:45 PM	9/3/2022 8:08:16 PM	287	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
prefetch2.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch2.txt	9/3/2022 8:12:35 PM	9/3/2022 8:12:35 PM	9/3/2022 8:12:35 PM	131	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
prefetch3.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch3.txt	9/3/2022 8:15:40 PM	9/3/2022 8:15:40 PM	9/3/2022 8:15:40 PM	142	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
prefetch4.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch4.txt	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	106	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
RegRipper3....	C:\Users\cyber\Downloads\RegRipper3.0-master.zip	9/3/2022 11:59:32 ...	9/3/2022 11:59:36 ...	9/3/2022 11:59:38 ...	5075610	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
t.lnk	C:\Users\cyber\Desktop\CTF\prefetch\t	9/3/2022 8:07:28 PM	9/3/2022 8:07:28 PM	9/3/2022 8:07:34 PM	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
task.jpg.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\task.jpg	9/3/2022 7:44:52 PM	10/18/2021 9:31:2...	9/3/2022 7:51:55 PM	1190155	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
The Internet...		n/a	n/a	n/a	0					2B:30:30:9D:00:00
This PC.lnk		n/a	n/a	n/a	0					2B:30:30:9D:00:00
volatility_2....	C:\Users\cyber\Downloads\volatility_2.6_win64_standal...	9/3/2022 11:53:00 ...	9/3/2022 11:53:09 ...	9/3/2022 11:53:11 ...	15565657	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
WFA.lnk	C:\Users\cyber\Downloads\WFA.zip	9/3/2022 11:46:44 ...	9/3/2022 11:47:02 ...	9/3/2022 11:47:05 ...	2099639	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
winprefetch...	C:\Users\cyber\Downloads\winprefetchview-x64.zip	9/3/2022 12:25:15 ...	9/3/2022 12:25:17 ...	9/3/2022 12:25:19 ...	68640	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
XP free fast....	C:\Users\cyber\Desktop\XP free fast	9/3/2022 12:33:24 ...	9/3/2022 12:33:24 ...	9/3/2022 12:33:40 ...	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00

let's focus on the internet.ink Icon and see what MAC address it has :



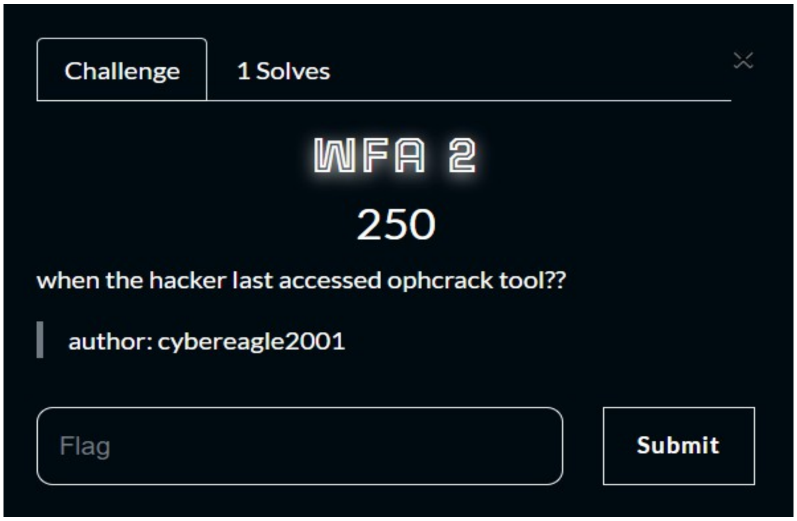
⊞ image2.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image2.txt	9/3/2022 7:55:24 PM	9/3/2022 7:55:24 PM	9/3/2022 7:55:24 PM	104	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ image3.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image3.txt	9/3/2022 7:57:11 PM	9/3/2022 7:57:11 PM	9/3/2022 7:57:11 PM	81	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ image4.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image4.txt	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM						□•□8ü...	00:00:00:00:00:00
⊞ IMG_202110...	C:\Users\cyber\Desktop\CTF\picture analysis\IMG_2021...	9/3/2022 7:44:52 PM	10/18/2021 9:31:2...						□•□8ü...	00:00:00:00:00:00
jumplister.v....	C:\Users\cyber\Downloads\jumplister.v.1.1.0.zip	9/3/2022 12:05:13 ...	9/3/2022 12:05:16 .						□•□8ü...	00:00:00:00:00:00
ms-gamingo...		n/a	n/a						¢ê□	00:00:00:00:00:00
mzcachevie...	C:\Users\cyber\Downloads\mzcacheview.zip	9/3/2022 11:57:23 ...	9/3/2022 11:57:26 .						□•□8ü...	00:00:00:00:00:00
New folder.lnk	C:\Users\cyber\Desktop\New folder	9/3/2022 12:33:24 ...	9/3/2022 12:33:24 .						□•□8ü...	00:00:00:00:00:00
ophcrack-3....	C:\Users\cyber\Downloads\ophcrack-3.7.0-bin.zip	9/3/2022 12:34:42 ...	9/3/2022 12:37:26 .						□•□8ü...	00:00:00:00:00:00
ophcrack-3....	C:\Users\cyber\Downloads\ophcrack-3.8.0-bin.zip	9/3/2022 12:11:01 ...	9/3/2022 12:17:33 .						□•□8ü...	00:00:00:00:00:00
pestudio.zip...	C:\Users\cyber\Downloads\pestudio.zip	9/3/2022 12:30:34 ...	9/3/2022 12:30:37 .						□•□8ü...	00:00:00:00:00:00
⊞ picture anal...	C:\Users\cyber\Desktop\CTF\picture analysis	9/3/2022 7:44:46 PM	9/3/2022 8:01:22 PM						□•□8ü...	00:00:00:00:00:00
⊞ prefetch.lnk	C:\Users\cyber\Desktop\CTF\prefetch	9/3/2022 8:04:06 PM	9/3/2022 8:18:11 PM						□•□8ü...	00:00:00:00:00:00
⊞ prefetch1.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch1.txt	9/3/2022 8:06:45 PM	9/3/2022 8:06:45 PM						□•□8ü...	00:00:00:00:00:00
⊞ prefetch2.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch2.txt	9/3/2022 8:12:35 PM	9/3/2022 8:12:35 PM						□•□8ü...	00:00:00:00:00:00
⊞ prefetch3.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch3.txt	9/3/2022 8:15:40 PM	9/3/2022 8:15:40 PM						□•□8ü...	00:00:00:00:00:00
⊞ prefetch4.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch4.txt	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	106	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
RegRipper3....	C:\Users\cyber\Downloads\RegRipper3.0-master.zip	9/3/2022 11:59:32 ...	9/3/2022 11:59:36 ...	9/3/2022 11:59:38 ...	5075610	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ t.lnk	C:\Users\cyber\Desktop\CTF\prefetch\t	9/3/2022 8:07:28 PM	9/3/2022 8:07:28 PM	9/3/2022 8:07:34 PM	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ task.jpg.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\task.jpg	9/3/2022 7:44:52 PM	10/18/2021 9:31:2...	9/3/2022 7:51:55 PM	1190155	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
The Internet...		n/a	n/a	n/a	0					2B:30:30:9D:00:00

SA - tasks

Written: n/a
Last Accessed: n/a
Size [B]: 0
Vol Type:
Vol Serial:
Vol Name:
NetBIOS:
MAC Address: 2B:30:30:9D:00:00

We can see that our MAC address is `2B:30:30:9D:00:00` the flag to submit `ESFST{2B:30:30:9D:00:00}`

II – WFA 2 :



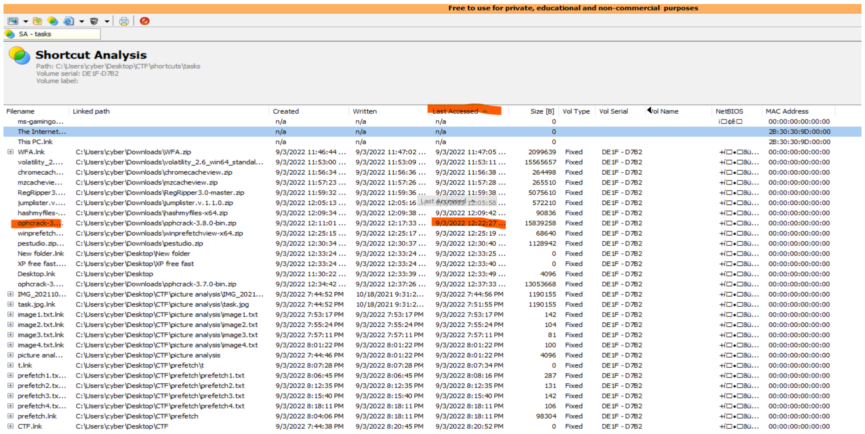
WFA 2

250

when the hacker last accessed ophcrack tool??

author: cybereagle2001

using the WFA.exe we can retreive the timing last time the user accessed the software through the timming he accessed the icon. This is how we can know for example the last time he cracked a password and that one can be a good proof if he can be a hacker we are trying to validate.
To do so we can verify the time stamp by sorting the icons using the last time they been accessed :



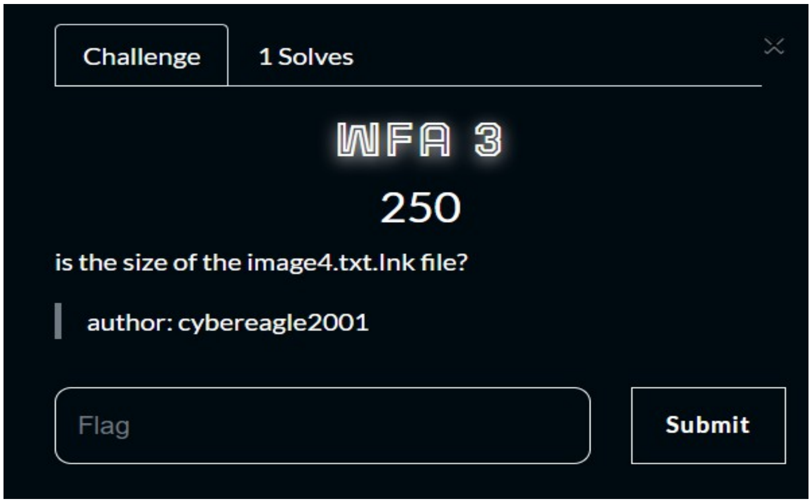
Free to use for private, educational and non-commercial purposes
SA - tasks

Shortcut Analysis
Path: C:\Users\cyber\Desktop\CTF\shortcuts\tasks
Volume serial: DE1F-D7B2
Volume label:

Filename	Linked path	Created	Written	Last Accessed	Size [B]	Vol Type	Vol Serial	Vol Name	NetBIOS	MAC Address
ms-gamingo...		n/a	n/a	n/a	0				i□¢ê□	00:00:00:00:00:00
The Internet...		n/a	n/a	n/a	0					2B:30:30:9D:00:00
This PC.lnk		n/a	n/a	n/a	0					2B:30:30:9D:00:00
⊞ WFA.lnk	C:\Users\cyber\Downloads\WFA.zip	9/3/2022 11:46:44 ...	9/3/2022 11:47:02 ...	9/3/2022 11:47:05 ...	2099639	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
volatility_2....	C:\Users\cyber\Downloads\volatility_2.6_win64_standal...	9/3/2022 11:53:00 ...	9/3/2022 11:53:09 ...	9/3/2022 11:53:11 ...	15565657	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
chromecach...	C:\Users\cyber\Downloads\chromecacheview.zip	9/3/2022 11:56:34 ...	9/3/2022 11:56:36 ...	9/3/2022 11:56:38 ...	264498	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
mzcachevie...	C:\Users\cyber\Downloads\mzcacheview.zip	9/3/2022 11:57:23 ...	9/3/2022 11:57:26 ...	9/3/2022 11:57:28 ...	265510	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
RegRipper3....	C:\Users\cyber\Downloads\RegRipper3.0-master.zip	9/3/2022 11:59:32 ...	9/3/2022 11:59:36 ...	9/3/2022 11:59:38 ...	5075610	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
jumplister.v....	C:\Users\cyber\Downloads\jumplister.v.1.1.0.zip	9/3/2022 12:05:13 ...	9/3/2022 12:05:16 ...	9/3/2022 12:05:58 ...	572210	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
hashmyfiles-...	C:\Users\cyber\Downloads\hashmyfiles-x64.zip	9/3/2022 12:09:34 ...	9/3/2022 12:09:38 ...	9/3/2022 12:09:42 ...	90836	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
ophcrack-3....	C:\Users\cyber\Downloads\ophcrack-3.8.0-bin.zip	9/3/2022 12:11:01 ...	9/3/2022 12:17:33 ...	9/3/2022 12:22:27 ...	15839258	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
winprefetch...	C:\Users\cyber\Downloads\winprefetchview-x64.zip	9/3/2022 12:25:15 ...	9/3/2022 12:25:17 ...	9/3/2022 12:25:19 ...	68640	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
pestudio.zip...	C:\Users\cyber\Downloads\pestudio.zip	9/3/2022 12:30:34 ...	9/3/2022 12:30:37 ...	9/3/2022 12:30:40 ...	1128942	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
New folder.lnk	C:\Users\cyber\Desktop\New folder	9/3/2022 12:33:24 ...	9/3/2022 12:33:24 ...	9/3/2022 12:33:25 ...	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
XP free fast....	C:\Users\cyber\Desktop\XP free fast	9/3/2022 12:33:24 ...	9/3/2022 12:33:24 ...	9/3/2022 12:33:40 ...	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
Desktop.lnk	C:\Users\cyber\Desktop	9/3/2022 11:30:22 ...	9/3/2022 12:33:39 ...	9/3/2022 12:33:49 ...	4096	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
ophcrack-3....	C:\Users\cyber\Downloads\ophcrack-3.7.0-bin.zip	9/3/2022 12:34:42 ...	9/3/2022 12:37:26 ...	9/3/2022 12:37:33 ...	13053668	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ IMG_202110...	C:\Users\cyber\Desktop\CTF\picture analysis\IMG_2021...	9/3/2022 7:44:52 PM	10/18/2021 9:31:2...	9/3/2022 7:44:56 PM	1190155	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ task.jpg.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\task.jpg	9/3/2022 7:44:52 PM	10/18/2021 9:31:2...	9/3/2022 7:51:55 PM	1190155	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ image1.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image1.txt	9/3/2022 7:53:17 PM	9/3/2022 7:53:17 PM	9/3/2022 7:53:17 PM	142	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ image2.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image2.txt	9/3/2022 7:55:24 PM	9/3/2022 7:55:24 PM	9/3/2022 7:55:24 PM	104	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ image3.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image3.txt	9/3/2022 7:57:11 PM	9/3/2022 7:57:11 PM	9/3/2022 7:57:11 PM	81	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ image4.txt.lnk	C:\Users\cyber\Desktop\CTF\picture analysis\image4.txt	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM	100	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ picture anal...	C:\Users\cyber\Desktop\CTF\picture analysis	9/3/2022 7:44:46 PM	9/3/2022 8:01:22 PM	9/3/2022 8:01:22 PM	4096	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ t.lnk	C:\Users\cyber\Desktop\CTF\prefetch\t	9/3/2022 8:07:28 PM	9/3/2022 8:07:28 PM	9/3/2022 8:07:34 PM	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ prefetch1.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch1.txt	9/3/2022 8:06:45 PM	9/3/2022 8:06:45 PM	9/3/2022 8:08:16 PM	287	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ prefetch2.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch2.txt	9/3/2022 8:12:35 PM	9/3/2022 8:12:35 PM	9/3/2022 8:12:35 PM	131	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ prefetch3.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch3.txt	9/3/2022 8:15:40 PM	9/3/2022 8:15:40 PM	9/3/2022 8:15:40 PM	142	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ prefetch4.tx...	C:\Users\cyber\Desktop\CTF\prefetch\prefetch4.txt	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	106	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ prefetch.lnk	C:\Users\cyber\Desktop\CTF\prefetch	9/3/2022 8:04:06 PM	9/3/2022 8:18:11 PM	9/3/2022 8:18:11 PM	98304	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00
⊞ CTF.lnk	C:\Users\cyber\Desktop\CTF	9/3/2022 7:44:38 PM	9/3/2022 8:20:45 PM	9/3/2022 8:20:52 PM	0	Fixed	DE1F - D7B2		+í□•□8ü...	00:00:00:00:00:00

the flag is : `ESFST{9/3/2022 2:22:27 PM}`

III – WFA 3:



is the size of the image4.txt.lnk file?

> author: cybereagle2001

We can also identify some informations about the icons like their size using the same tool.

Flag : ESFST{`100`}