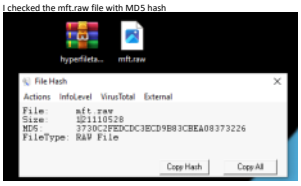
Hyperfiletable Challenge

Sherlock Scenario
There has been a new joiner in Forela, they have downloaded their onboarding documentation, however someone has managed to phish the user with a malicious attachment. We have only managed to pull the MFT record for the new user, are you able to triage this information?

Task 1:
What is the MD5 hash of the MFT?

I checked the mft.raw file with MD5 hash



Answer: 3730c2fedcdc3ecd9b83cbea08373226

Task 2:
What is the name of the only user on the system?

I used MFTECmd to parse the mft.raw and then opened it with Timeline Explorer
Then I searched for Users

.\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance
.\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools
.\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell
.\Users\Default\Documents
.\Users\Public
.\Users\Public\AccountPictures
.\Users\Public\Desktop
.\Users\Public\Documents
.\Users\Public\Downloads
.\Users\Public\Libraries
.\Users\Public\Music
.\Users\Public\Pictures
.\Users\Public\Videos
.\Users\Randy Savage
.\Users\Randy Savage\3D Objects
.\Users\Randy Savage\AppData
.\Users\Randy Savage\AppData\Local
.\Users\Randy Savage\AppData\Local\Comms
.\Users\Randy Savage\AppData\Local\Comms\Unistore
.\Users\Randy Savage\AppData\Local\Comms\Unistore\data
.\Users\Randy Savage\AppData\Local\Comms\UnistoreDB
.\Users\Randy Savage\AppData\Local\ConnectedDevicesPlatform
.\Users\Randy Savage\AppData\Local\ConnectedDevicesPlatform\L.Randy Savage
.\Users\Randy Savage\AppData\Local\D3DSCache

Answer: Randy Savage

Task 3:
What is the name of the malicious HTA that was downloaded by that user?

I searched for HTA

Parent Path	File Name	Extension
=		= .hta
.\Users\Randy Savage\Downloads	Onboarding.hta	.hta

Answer: Onboarding.hta

Task 4:
What is the ZoneId of the download for the malicious HTA file?

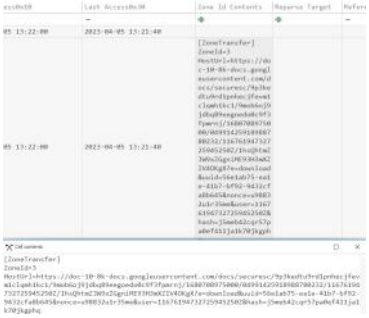
I searched for onboarding.hta and found the Zone.Identifier

Zone Id Contents
[ZoneTransfer] ZoneId=3 HostUrl=https://do

Answer: 3

Task 5:
What is the download URL for the malicious HTA?

Same from task 4



Answer:
https://doc-10-8k-docs.googleusercontent.com/docs/securesc/9p3kedtu9rd1pnhecjfevm1clqmh1kc1/9mob6oj9jdbq89eegoed0c9f3fpmrnj/1680708975000/04991425918988780232/11676194732725945250Z/1hsQhtmZJW9xZGgniME93H3mXZlV4OKgX?e=download&uuid=56e1ab75-ea1e-41b7-bf92-9432cfa8b645&nonce=u98832u1r35me&user=11676194732725945250Z&hash=j5meb42cqr57pa0ef411ja1k70jkgphq

Task 6:
What is the allocated size for the HTA file? (bytes)

I used the command "MFTECmd.exe -f C:\Users\Bubble\Desktop\mft.raw --de 103820" and then asked the ChatGPT what is the size

```
**** DATA ****
 Attribute #: 0x4, Size: 0x48, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

 Non-Resident Data
 Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x0, Allocated Size: 0x1000, Actual Size: 0x478, Initialized Size: 0x478

 DataRuns Entries (Cluster offset -> # of clusters)
 0x1481F6                        ->      0x1

**** DATA ****
 Attribute #: 0x9, Size: 0x1C0, Content size: 0x185, Name size: 0xF, ContentOffset 0x38. Resident: True
 Name: Zone.Identifier
```

The allocated size for the HTA file is **4096 bytes** (0x1000 in hexadecimal). This is indicated in the output under the `**** DATA ****` section, where it mentions the "Allocated Size."

Answer: 4096

Task 7:
What is the real size of the HTA file? (bytes)

Same like task 6, I asked the ChatGPT

The real size of the HTA file is **1144 bytes** (0x478 in hexadecimal). This is indicated in the output under the `**** DATA ****` section, where it mentions the "Actual Size."

Answer: 1144

Task 8:
When was the powerpoint presentation downloaded by the user?

I searched for pptx extension and found the file name Proposal.pptx. Then I searched for the file name and found the Zone.Identifier

Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Cre
.\Users\Randy Savage\Documents\Work	Proposal.pptx	.pptx	☐	☑	☐	16552989	202
.\Users\Randy Savage\Documents\Work	Proposal.pptx:Zone.Identifier	.Identifier	☐	☐	☑	253	202

Created0x10
2023-04-05 13:11:49
2023-04-05 13:11:49

Answer: 05/04/2023 13:11:49

Task 9:
The user has made notes of their work credentials, what is their password?

I searched for "\Users\Randy Savage\" and inside the Extension tab I choosed ".txt"

eader here to group by that column — \Users\Randy Savage\

Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Create
110620	3	107430	3	☐	.\Users\Randy Savage\Documents\Work	notes.txt	.txt	☐	☐	☐	118	2023-0

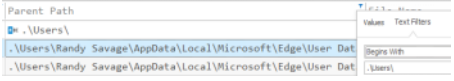
Then I used the command "MFTECmd.exe -f C:\Users\Bubble\Desktop\mft.raw --de 110620"

```
    ASCII:   New onboarding process:
Download onboarding tool from Google Drive
Username: RSavage
Password: ReallyC00lDucks2023!
    UNICODE: ??????????????????????????????????????????????????>????????M
```

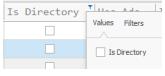
Answer: ReallyC00lDucks2023!

Task 10:
How many files remain under the C:\Users\ directory? (Recursively)

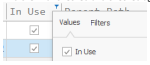
First I filtered for .\Users\ in the Parent Path tab inside the Text Filters

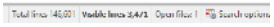


Then I unchecked the Is Directory tab



And then I unchecked and checked again the In Use tab





Answer 3471