Mission Name

Indicators of Compromise

History Context

EUPHEA - Principal & Chancellor's office at Shanghai. The investigation leads to The Principal and the Chancellor. Ethan must place the bug.

Technical High-Level Overview

Player must locate how he/she managed to download the bug using a LOLBIN (certutil) of the operating system itself. To do so, he/she must identify the download URL.

Short Description

In previous missions, you had to check Ethan´s bug but this, you´re going to investigate how Ethan downloaded the bug into the system. Your goal will be to identify de URL used to download the bug. Finally you must calculate hash MD5, including http and so on.

Mission Description

Previously was the first time that you go to connect to a live Windows machine to investigate how Ethan placed the bug into the system. This time, you will face an offline evidence to check your capabilities in terms of finding indicators of compromise. Your goal will be to identify the URL used to download the bug. Finally you must calculate hash MD5, including http and so on.

Location

EUPHEA FACULTY | THE PRINCIPAL'S QUARTERS

Tools

- https://github.com/AbdulRhmanAlfaifi/CryptnetURLCacheParser
- https://github.com/markmckinnon/Autopsy-Plugins

Questions

Which is the size of the file downloaded in bytes?

- 123392

Which name was used, once the file was downloaded?

- winoffice.exe

Hints

1. Use Autopsy to mount the evidence provided.
2. Analyse all execution artifacts, specially Prefetch.
3. Use the timeline option On Autopsy to locate the file downloaded.

Write Up

Player should use Autopsy 4.9.0 version to mount the image provided:

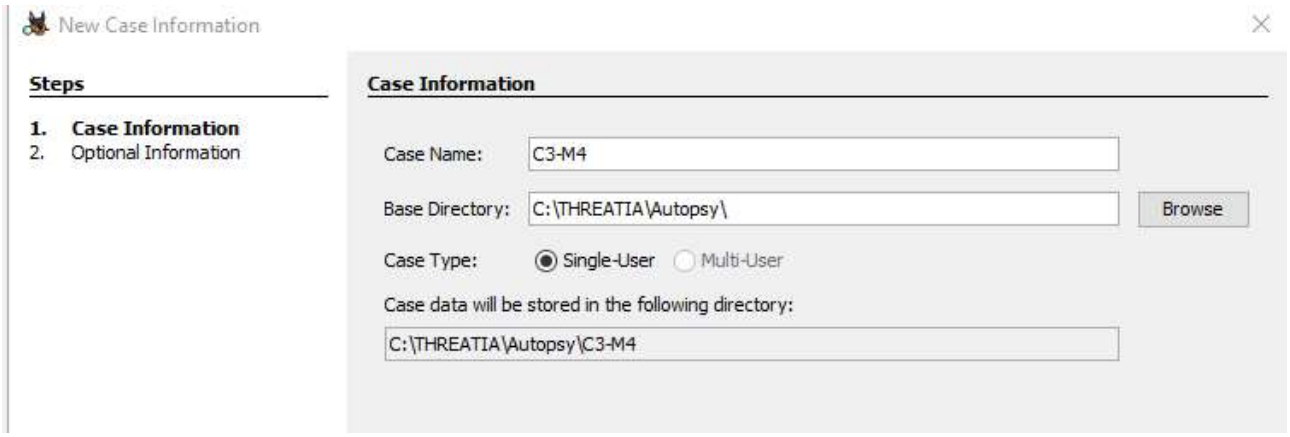


Figure 1

Fill all the necessary information to create the case:

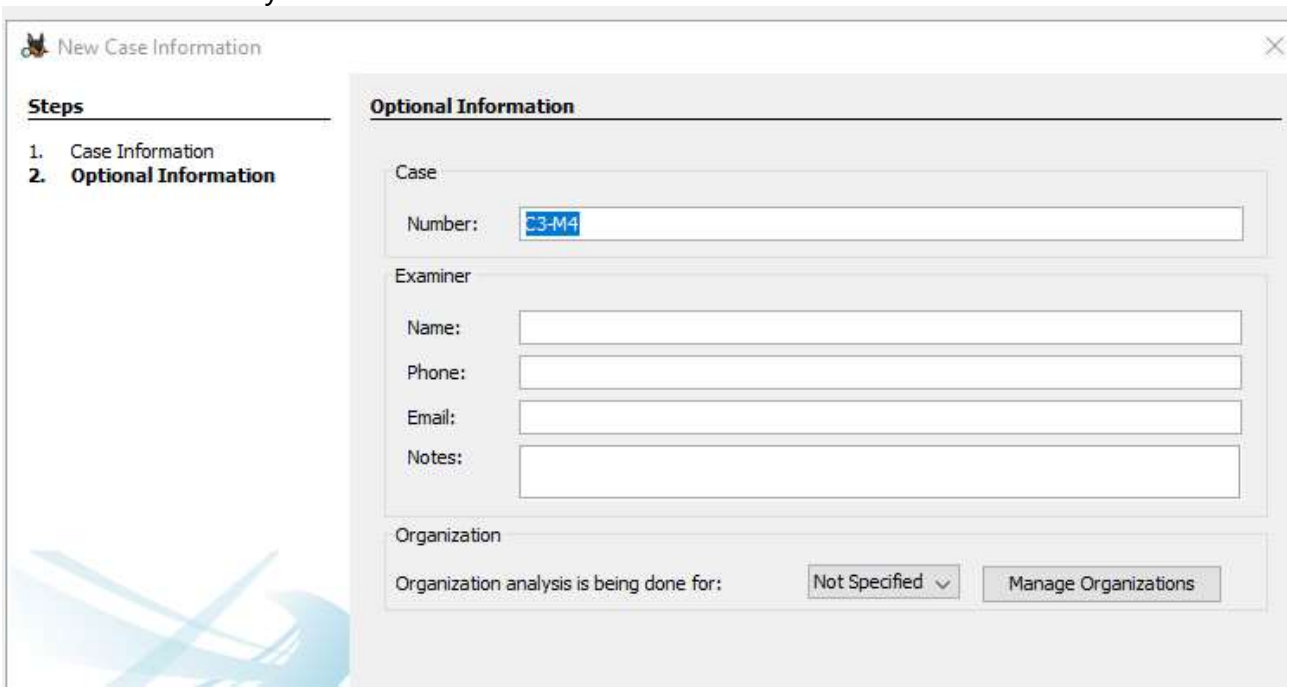


Figure 2

Select the source of the information to analyse:

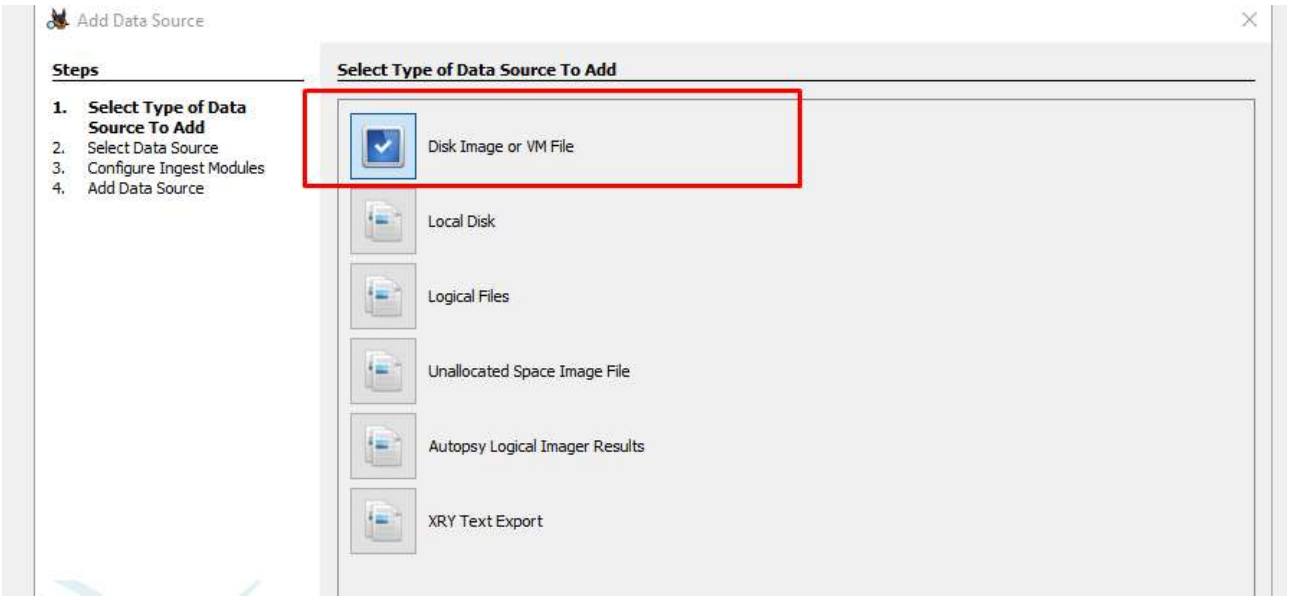


Figure 3

Once Autopsy requires you, to select ingest modules, player must select Windows Internals (Prefetch and ShimCache) and "All files and Directories):

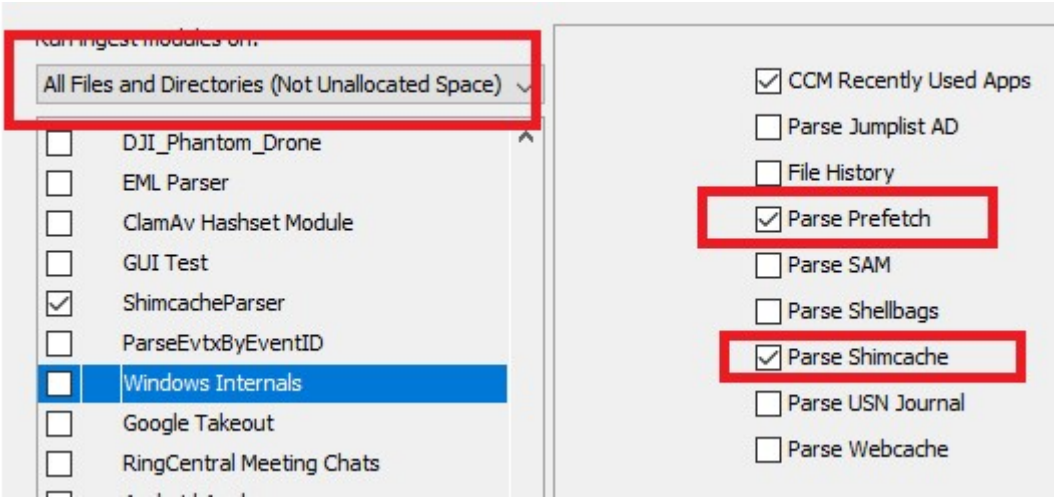


Figure 4

When Autopsy finishes, there will be two option on extracted content:

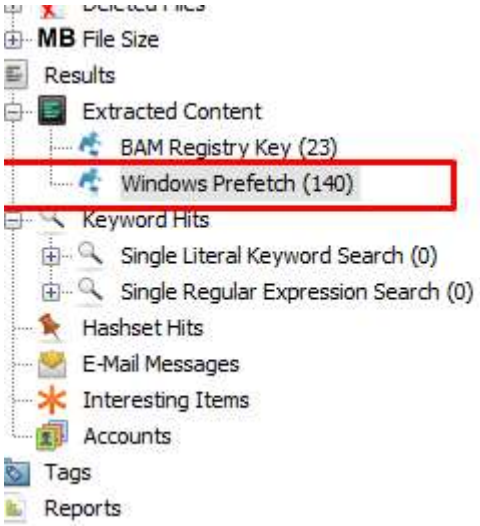


Figure 5

Select Prefetch folder and sort columns by first execution:

As you can see below, there is the typical processes tree when you executes something on command prompt:

1. CMD.exe
2. CONHOST.exe
3. CERTUTIL.exe

Source File	S	C	O	PF Execution DTTM 1
TASKHOSTW.EXE-2E5D4B75.pf				2021-06-20 22:44:33 CEST
RUNTIMEBROKER.EXE-318BAC70.pf				2021-06-20 22:44:34 CEST
SVCHOST.EXE-9F82877C.pf				2021-06-20 22:44:35 CEST
VSSVC.EXE-6C8F0C66.pf				2021-06-20 22:44:41 CEST
SVCHOST.EXE-BFF367D9.pf				2021-06-20 22:44:51 CEST
SVCHOST.EXE-FF256082.pf				2021-06-20 22:44:51 CEST
BACKGROUNDTRANSFERHOST.EXE-30A6F22E.pf				2021-06-20 22:45:06 CEST
RUNDLL32.EXE-BF72C764.pf				2021-06-20 22:45:11 CEST
RUNDLL32.EXE-FDCBB5A1.pf				2021-06-20 22:45:12 CEST
MPCMDRUN.EXE-2C9109F9.pf				2021-06-20 22:45:30 CEST
BACKGROUNDTASKHOST.EXE-4EED4AF4.pf				2021-06-20 22:45:32 CEST
WMIADAP.EXE-BB21CD77.pf				2021-06-20 22:45:33 CEST
WMIPRVSE.EXE-E8B8DD29.pf				2021-06-20 22:45:33 CEST
CMD.EXE-0BD30981.pf				2021-06-20 22:45:36 CEST
CONHOST.EXE-0C6456FB.pf				2021-06-20 22:45:36 CEST
CERTUTIL.EXE-28F1E0C1.pf				2021-06-20 22:45:48 CEST
DLLHOST.EXE-92F548BD.pf				2021-06-20 22:46:14 CEST
RUNTIMEBROKER.EXE-640D902C.pf				2021-06-20 22:46:14 CEST
SECHEALTHUI.EXE-B8DB14A2.pf				2021-06-20 22:46:14 CEST
SECURITYHEALTHHOST.EXE-06344EE9.pf				2021-06-20 22:46:14 CEST
CONSENT.EXE-40419367.pf				2021-06-20 22:46:16 CEST
BACKGROUNDTASKHOST.EXE-4A9935D7.pf				2021-06-20 22:46:17 CEST
NISSRV.EXE-09946424.pf				2021-06-20 22:46:17 CEST

Figure 6

This is the key for players. Next step would be to select the exact moment when certutil.exe was executed, right click on it and “View Source in Timeline”

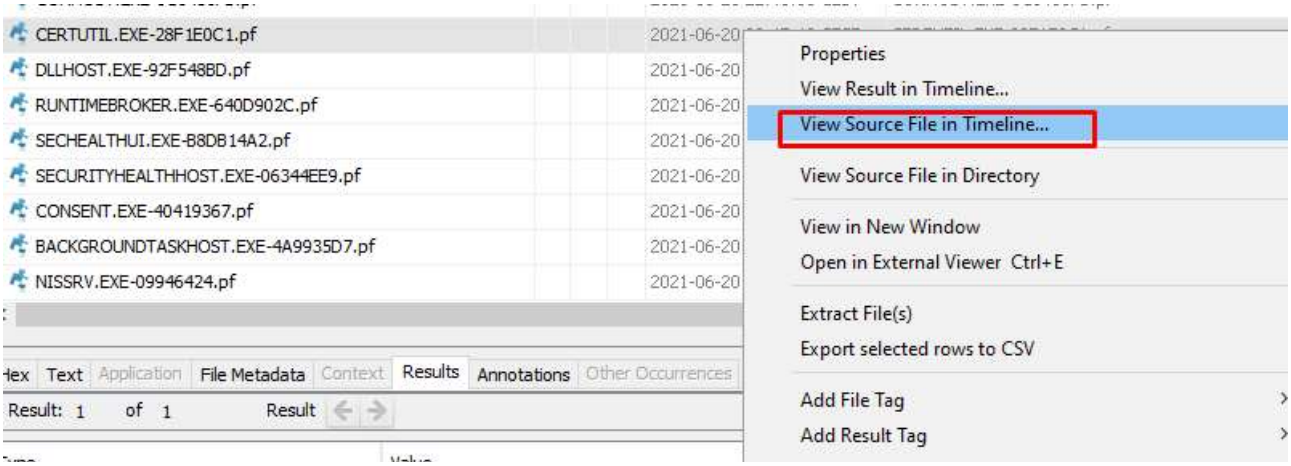


Figure 7

Select file created:

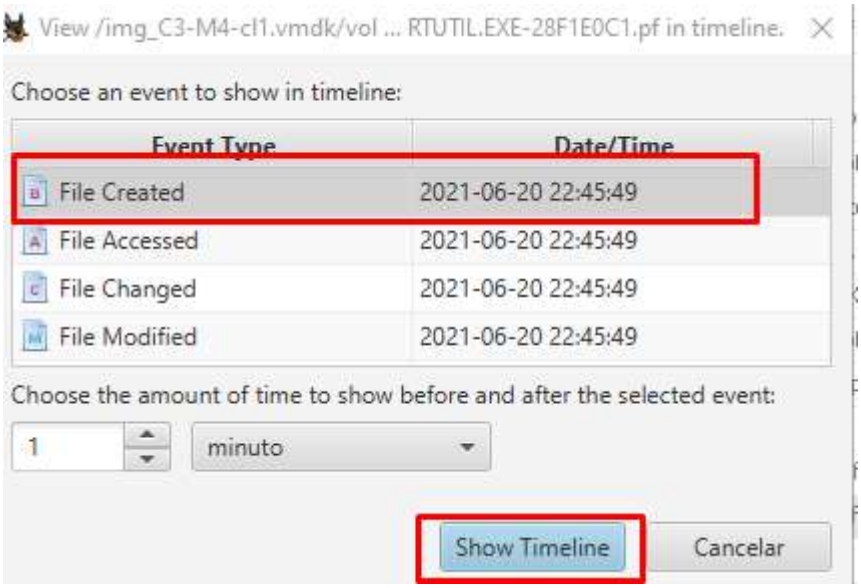


Figure 8

Finally, you will be able to identify:

- **DEL%20full.exe:** the previous name, it means, when certutil download the file before renaming. We will check in the following steps.
- **Winoffice.exe**: the name of the same file but renamed. To reach this conclusion, Winoffice has the same creation time as prefetch, and obviously the same hash.

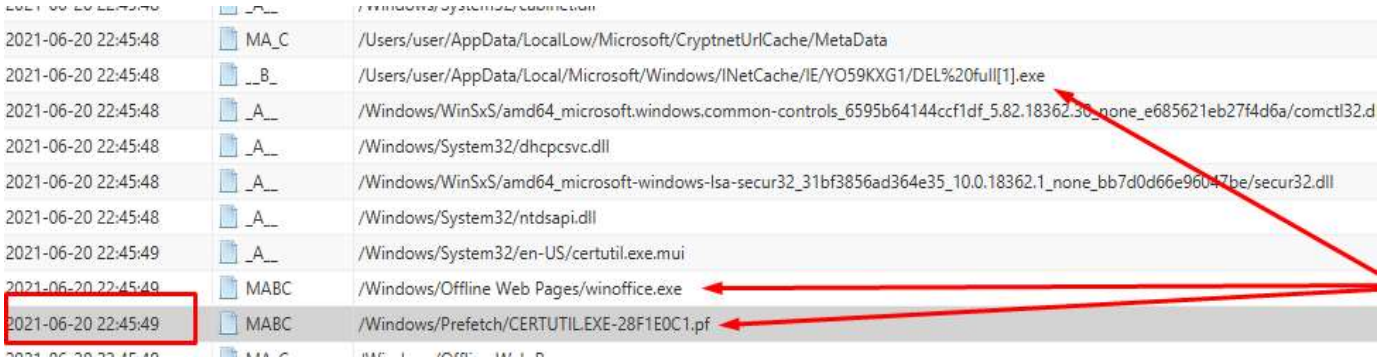


Figure 9

The new key to follow by players would be this folder:

- Users/user/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData

This folder is used by Certutil.exe to store information about downloads. If player performs a little search, he/she will be able to locate the necessary tool to parse it:

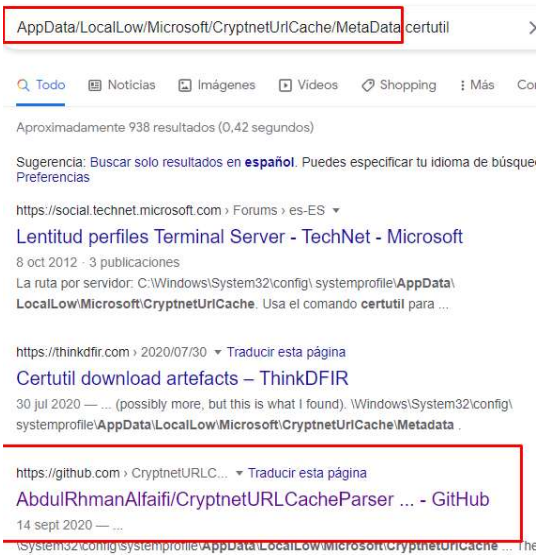
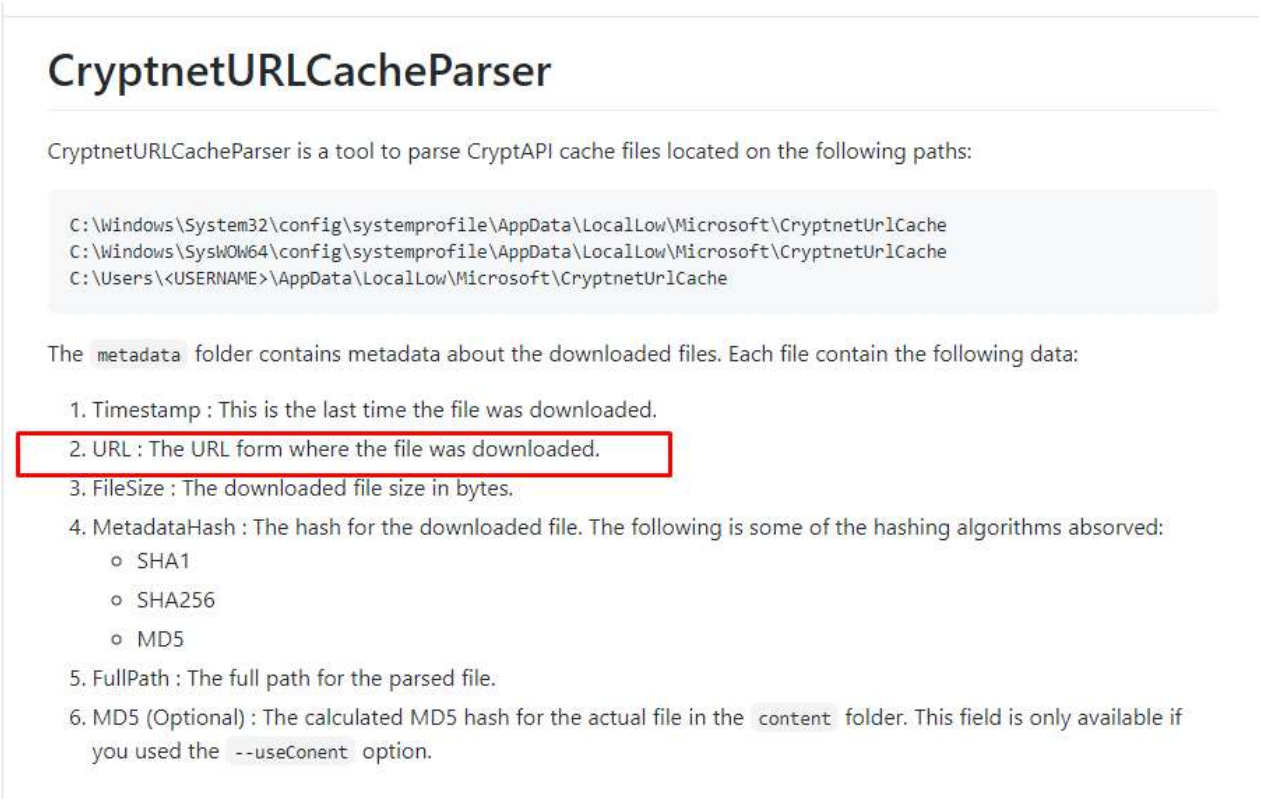


Figure 10

Player should download the tool and install it from:

- https://github.com/AbdulRhmanAlfaifi/CryptnetURLCacheParser



CryptnetURLCacheParser

CryptnetURLCacheParser is a tool to parse CryptAPI cache files located on the following paths:

```
C:\Windows\System32\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache
C:\Windows\SysWOW64\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache
C:\Users\<USERNAME>\AppData\LocalLow\Microsoft\CryptnetUrlCache
```

The `metadata` folder contains metadata about the downloaded files. Each file contain the following data:

1. Timestamp : This is the last time the file was downloaded.
2. URL : The URL form where the file was downloaded.
3. FileSize : The downloaded file size in bytes.
4. MetadataHash : The hash for the downloaded file. The following is some of the hashing algorithms absorved:
   - SHA1
   - SHA256
   - MD5
5. FullPath : The full path for the parsed file.
6. MD5 (Optional) : The calculated MD5 hash for the actual file in the `content` folder. This field is only available if you used the `--useConent` option.

- **Figure 11**

First of all, we should extract from Autopsy, the following folder:

- C:\Users\<USERNAME>\AppData\LocalLow\Microsoft\CryptnetUrlCache

To achieve this, right click on the necessary folder and select “Export”

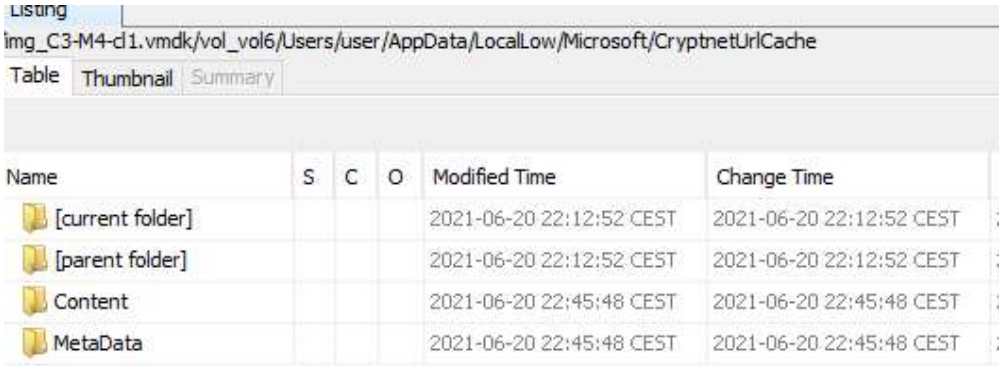


Figure 12

Eventually, player must launch **CryptnetUrlCacheParser.py** over Metadata extracted folder:

- python3 CryptnetUrlCacheParser.py -d ./CryptnetUrlCache/MetaData/ -o file_output.csv --outputFormat csv

And then open file_output.csv to identify the file downloaded:

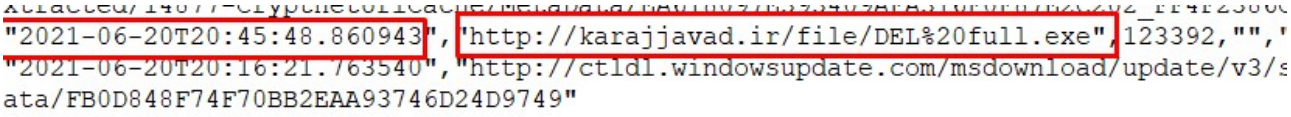


Figure 13

The key is the timestamp, is the same as Prefetch timestamp. The URL for DEL%20full.exe is

- http://karajjavad.ir/file/DEL%20full.exe

Player must provide MD5 hash of the URL:

- 11DCCEE68815BC20DBBF06AC0C415439

Flag Information

flag{11DCCEE68815BC20DBBF06AC0C415439}