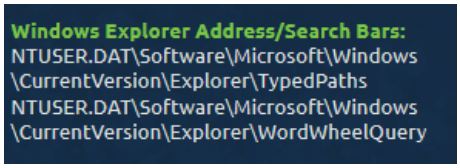
TryHackMe: unattended

The following is a writeup for the unattended room on TryHackMe. It is a digital forensics room that involved using tools like Registry Explorer and Autopsy to investigate a KapeFiles dump. The overall goal of this room was to answer a series of investigative questions to determine if the machine what infected. I really enjoyed this room, and I hope my writeup can be of use to someone out there. Please feel free to give me feedback as I am in no way shape or form a writeup expert or digital forensics/security professional.

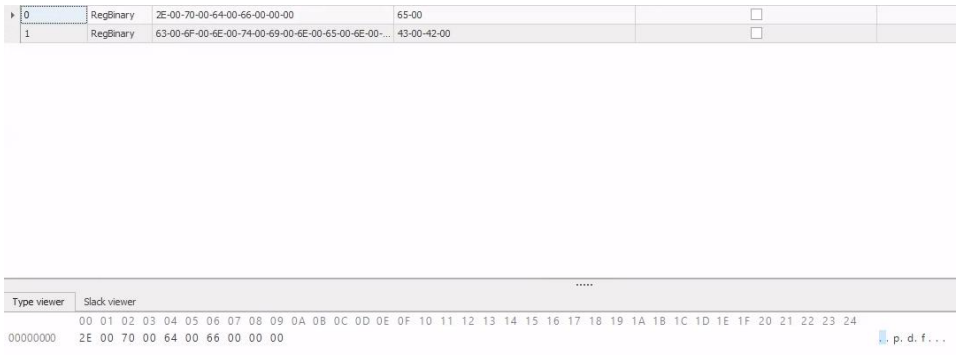
Scenario: Our client has a newly hired employee who saw a suspicious-looking janitor exiting his office as he was about to return from lunch. I want you to investigate if there was user activity while the user was away between 12:05 to 12:45 PM on the 19th of November 2022. If there are, figure out what files were accessed and exfiltrated externally.

What file type was searched for using the search bar in Windows Explorer?

If you use the provided cheat sheet, or make a google search, you will determine that we can find what the user searched for using the search bar in Windows Explorer by investigating the following registry location:



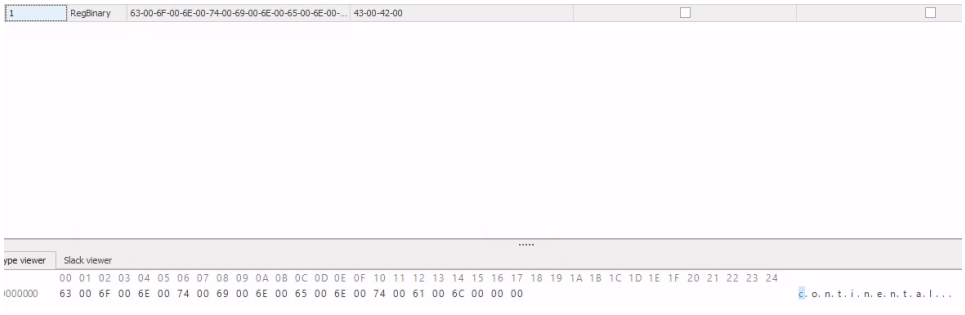
We can use RegistryExplorer to read the second registry path:



We can see in that the user searched for .pdf which is the answer.

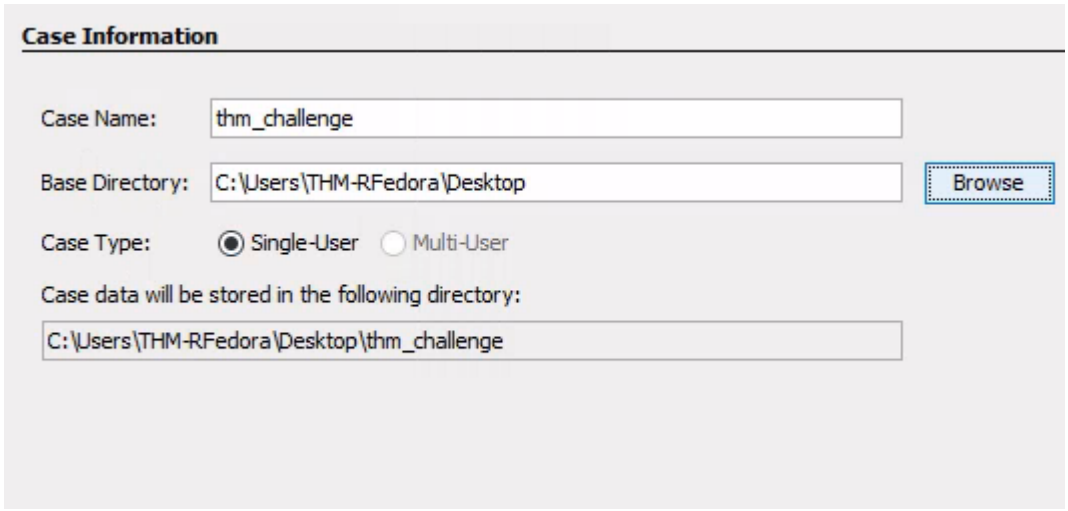
What top-secret keyword was searched for using the search bar in Windows Explorer?

If you view the other value in the WordWheelQuery key, you can see that the value is ‘continental’:

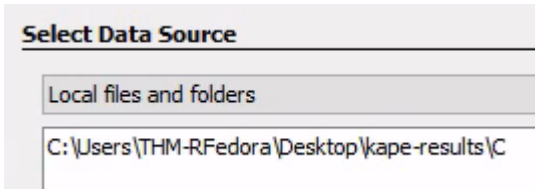


What is the name of the downloaded file to the Downloads folder?

Open Autopsy and start a new case (the name of the case and other details are not important for this challenge):



Then click the Add Data Source button and make sure to select the Logical Files data source:



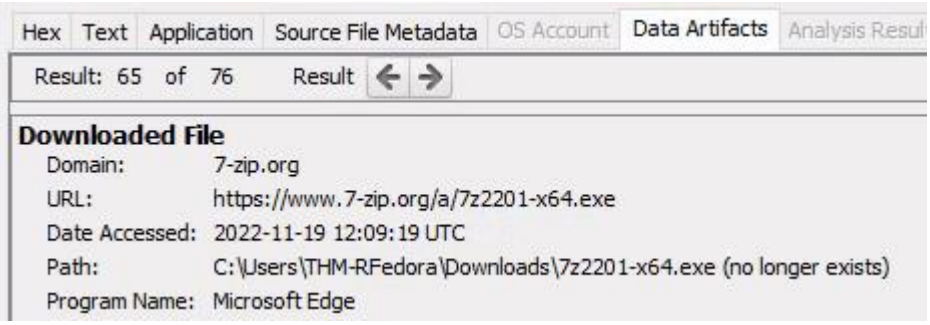
If you look at the Web Downloads section, you can quickly identify

that an executable was downloaded from 7-zip.org and saved to the downloads directory:

The name of the executable (7z2201-x64.exe) is the answer.

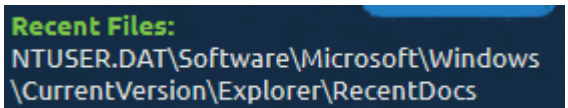
When was the file from the previous question downloaded?

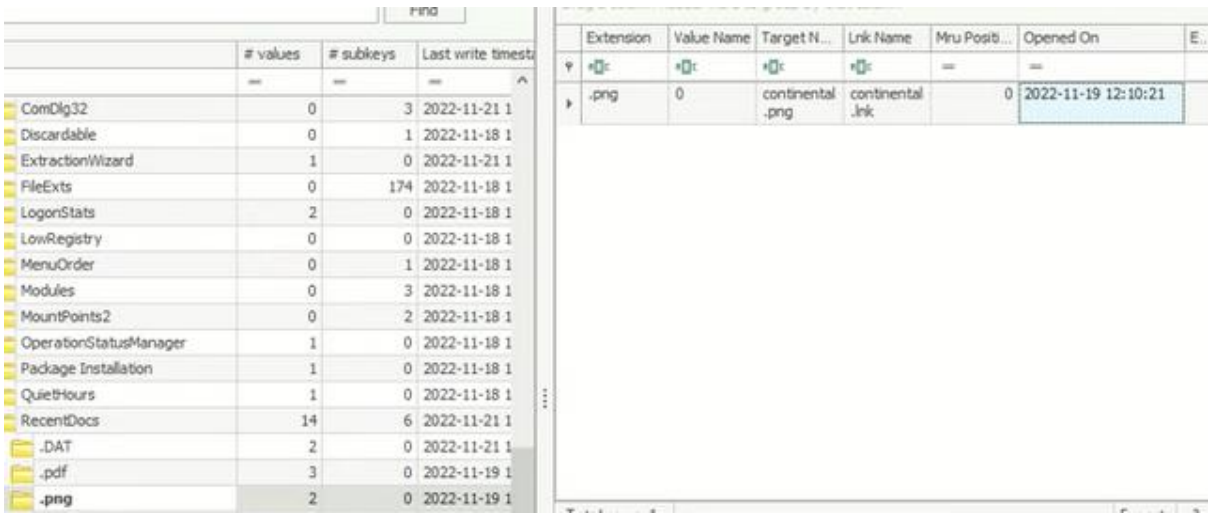
If you look at the Data Accessed column, you can see when the file was downloaded. Alternatively, you can click on the row and navigate to the Data Artifacts tab to copy the data accessed value:



Thanks to the previously downloaded file, a PNG file was opened. When was this file opened?

We can once again use the provided Windows forensic cheat sheet to find what registry path to investigate, in this case it is the following:





A text file was created in the Desktop folder. How many times was this file opened?

As said in the hint, we can use JLECmd.exe which is a Jump List parser created by Eric Zimmerman. For context, Windows introduced jump lists to help users go directly to their recently used files from the taskbar. You can view jumplists by right-clicking an application's icon in the taskbar. The data is stored in:

- C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Jumplists include information about the applications executed, first time of execution, and last time of execution.

To use JLECmd.exe, open up an elevated command prompt and enter:

```
C:\tools\JLECmd>JLECmd.exe -d C:\Users\THM-RFedora\Desktop\kape-results\C\Users\THM-RFedora
```

If you scroll through the results, you can see an entry for launchcode.txt which is on the Desktop:

```
--- DestList entries ---
Entry #: 1
  MRU: 0
  Path: C:\Users\THM-RFedora\Desktop\launchcode.txt
  Pinned: False
  Created on:    2022-11-19 11:45:46
  Last modified: 2022-11-19 12:12:35
  Hostname: tryhatme-rfedor
  Mac Address: 02:aa:8b:ff:d5:25
  Interaction count: 2

--- Lnk information ---
  Absolute path: My Computer\C:\Users\\Desktop\
```

The interaction count value of 2 is the amount of times this file was opened.

When was the text file from the previous question last modified?

The answer to this can be found in the image on the previous question, you just need to change the format:

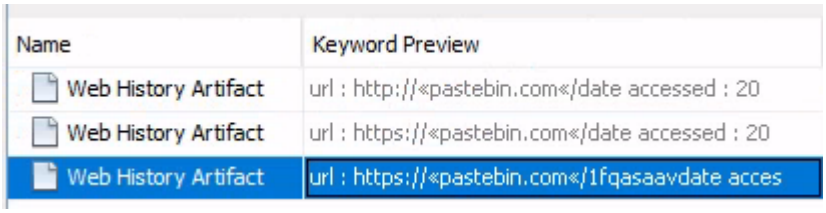
```
Last modified: 2022-11-19 12:12:35
```

Answer is 11/19/2022 12:12.

The contents of the file were exfiltrated to Pastebin.com. What is the generated URL of the exfiltrated data?

Navigate back to Autopsy and check web history:

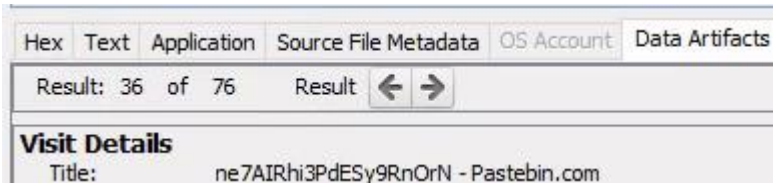
If you use the keyword search for sub-string match, you can search for 'pastebin' which gives three results:



The third result, 'https://pastebin.com/1FQASAav' is the answer.

What is the string that was copied to the Pastebin URL?

The string that was copied to the Pastebin URL can be seen in the title value:



Make sure to remove '- Pastebin.com'.