Unattended - Windows Forensics Lab

Welcome to the team, kid. I have something for you to get your feet wet.

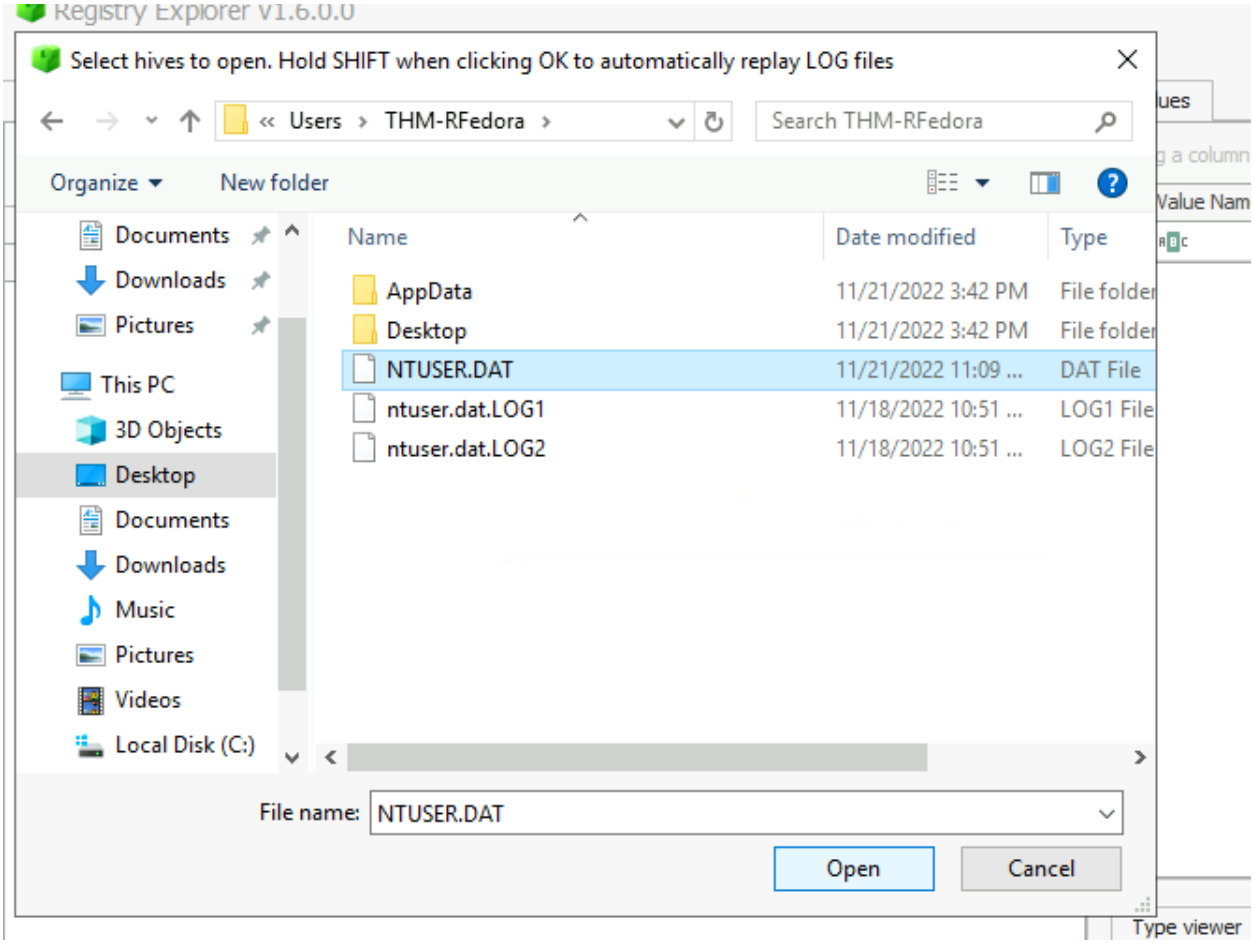
Our client has a newly hired employee who saw a suspicious-looking janitor exiting his office as he was about to return from lunch.
I want you to investigate if there was user activity while the user was away between 12:05 PM to 12:45 PM on the 19th of November 2022. If there are, figure out what files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

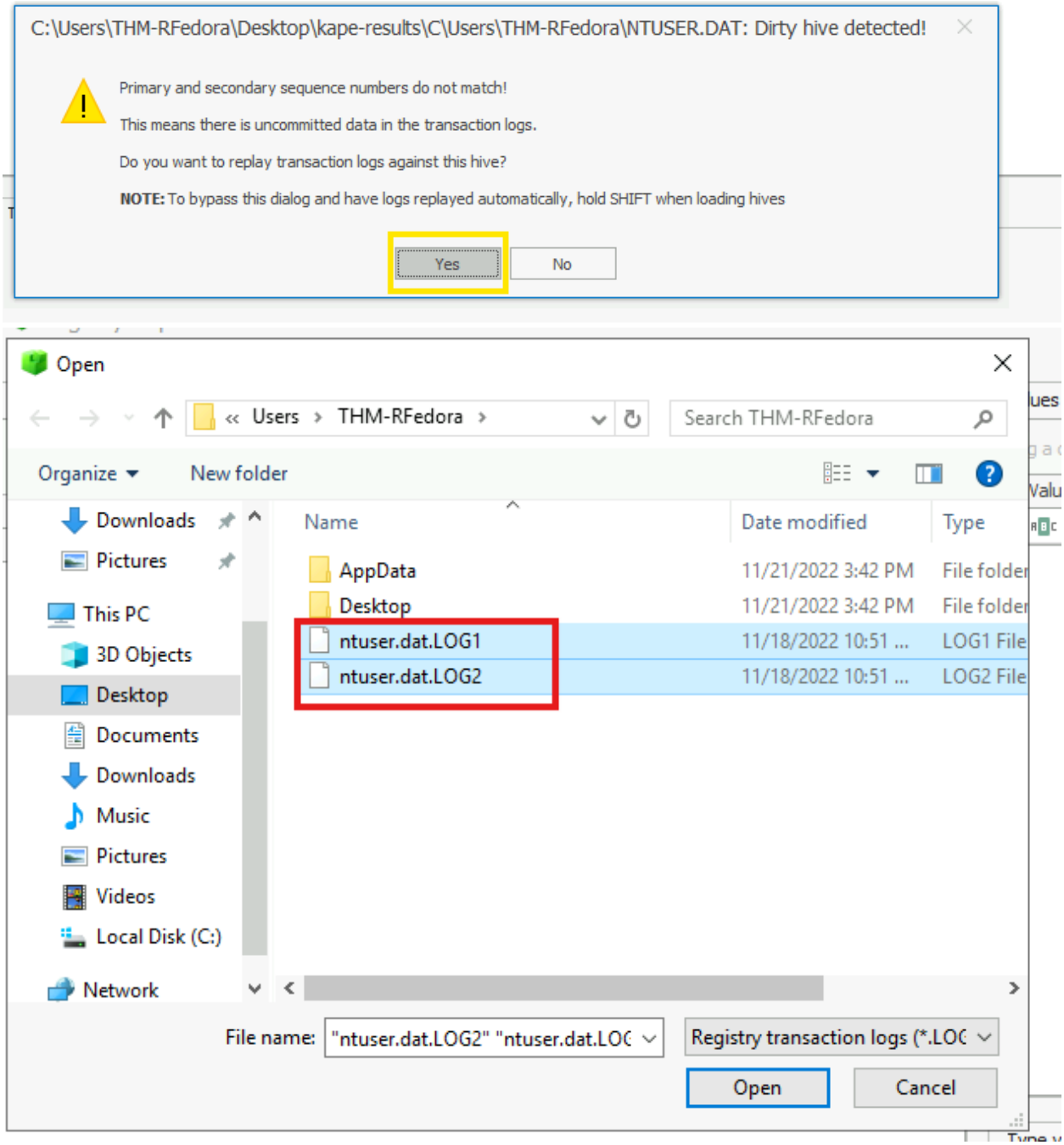
Initial investigations reveal that someone accessed the user's computer during the previously specified timeframe.

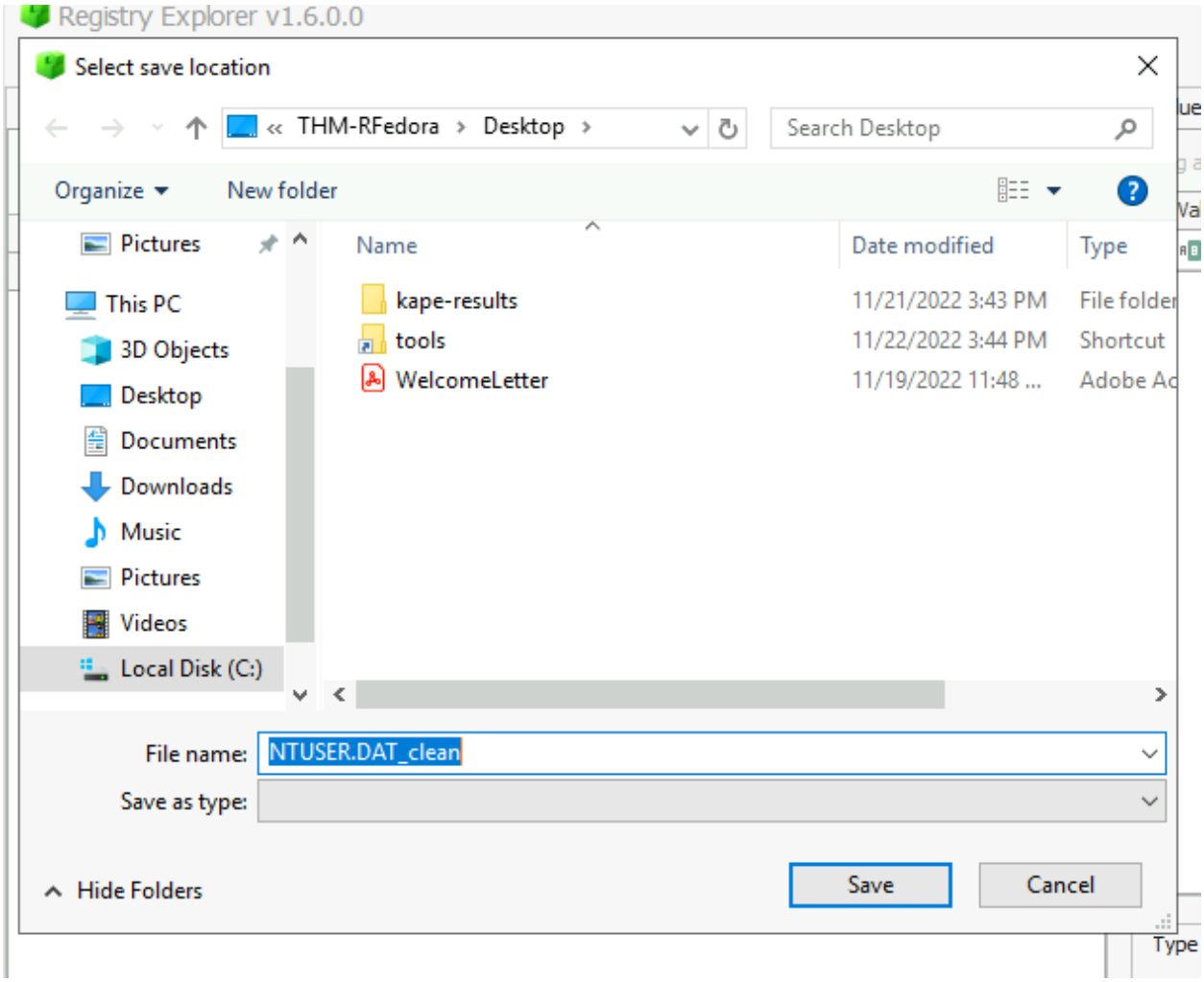
Whoever this someone is, it is evident they already know what to search for. Hmm. Curious.

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

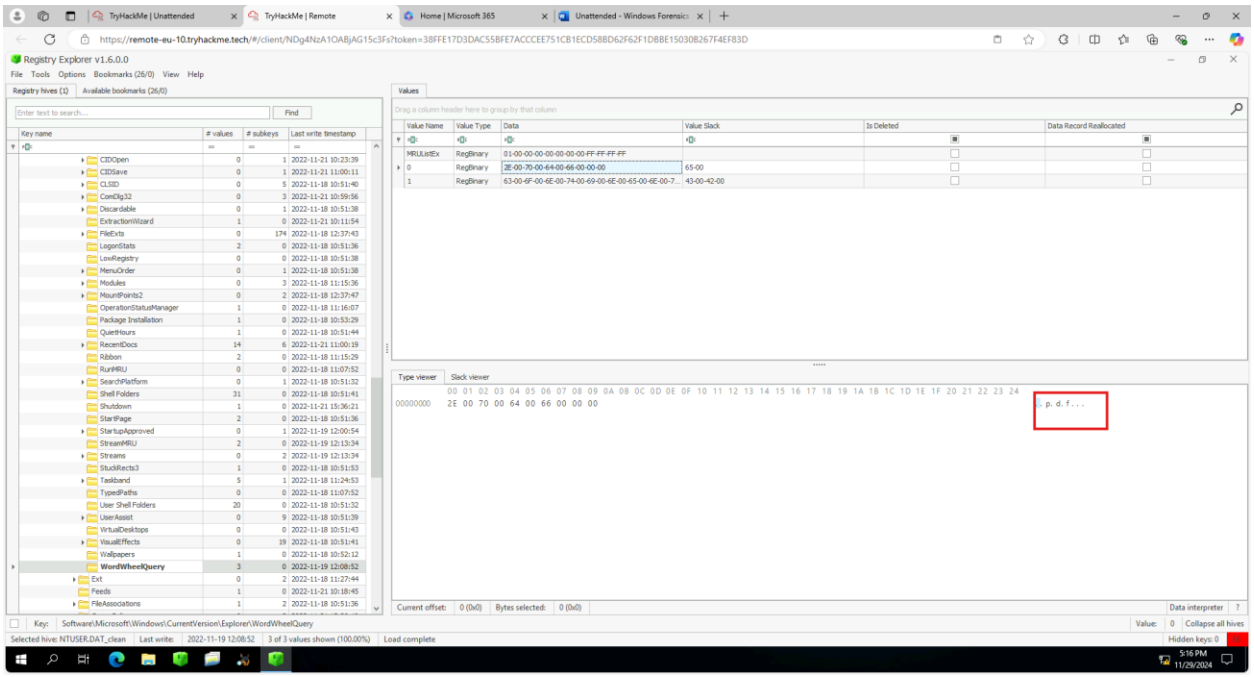
Answer: .pdf




C:\Users\THM-RFedora\Desktop\kape-results\C\Users\THM-RFedora\NTUSER.DAT: Dirty hive detected!
Primary and secondary sequence numbers do not match!
This means there is uncommitted data in the transaction logs.
Do you want to replay transaction logs against this hive?
NOTE: To bypass this dialog and have logs replayed automatically, hold SHIFT when loading hives
Yes
No
Open
« Users › THM-RFedora ›
Search THM-RFedora
Organize
New folder
Downloads
Pictures
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
AppData
11/21/2022 3:42 PM
File folder
Desktop
11/21/2022 3:42 PM
File folder
ntuser.dat.LOG1
11/18/2022 10:51 ...
LOG1 File
ntuser.dat.LOG2
11/18/2022 10:51 ...
LOG2 File
File name:
"ntuser.dat.LOG2" "ntuser.dat.LOC
Registry transaction logs (*.LOC
Open
Cancel

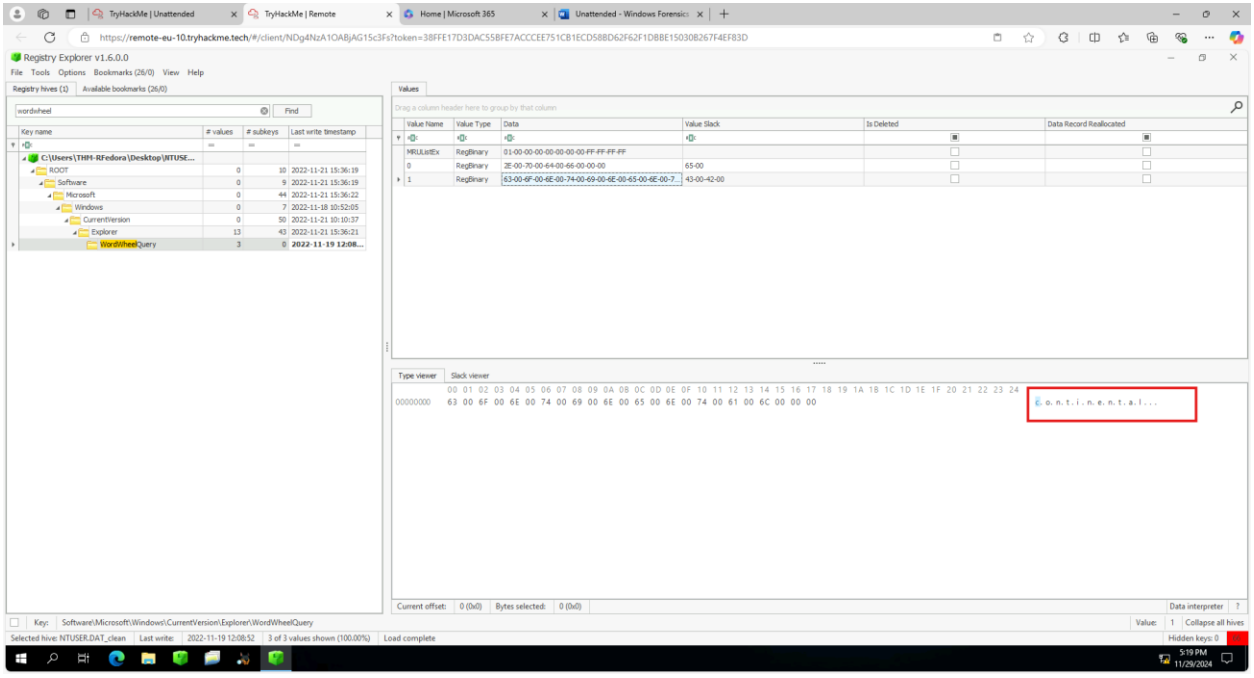


we need to follow this path to locate the information in question:
NTUSER.DAT\Software\Microsoft\Windows \CurrentVersion\Explorer\WordWheelQuery



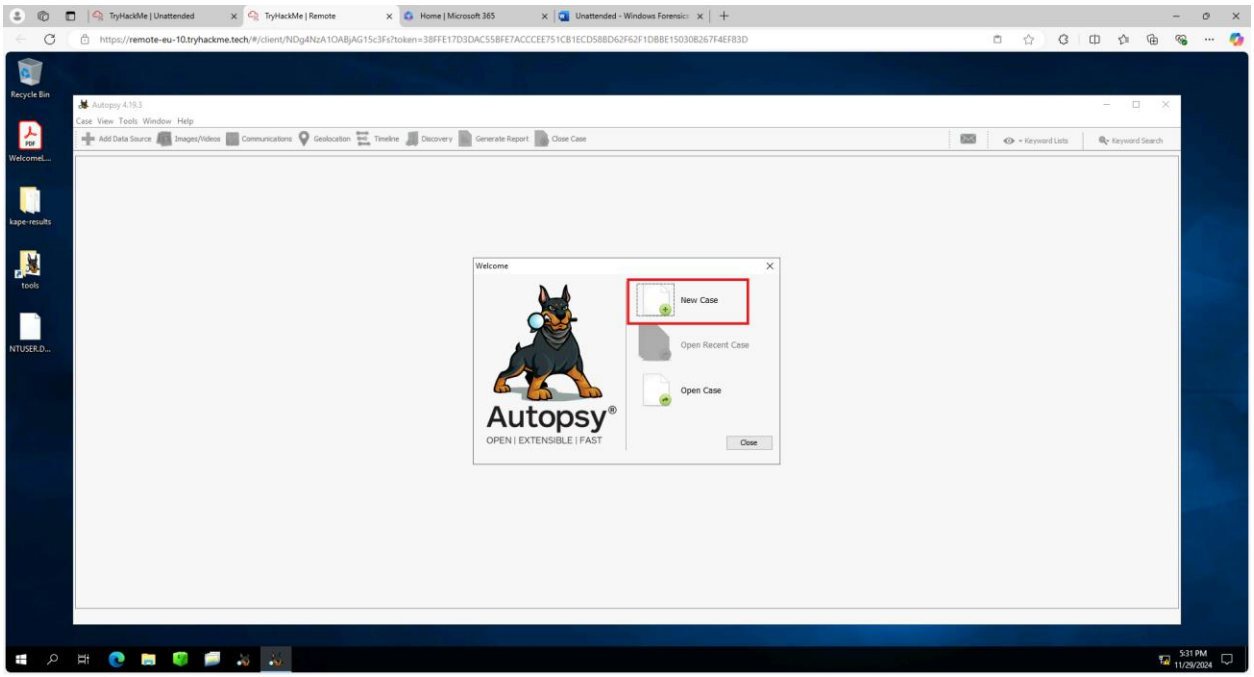
What top-secret keyword was searched for using the search bar in Windows Explorer?

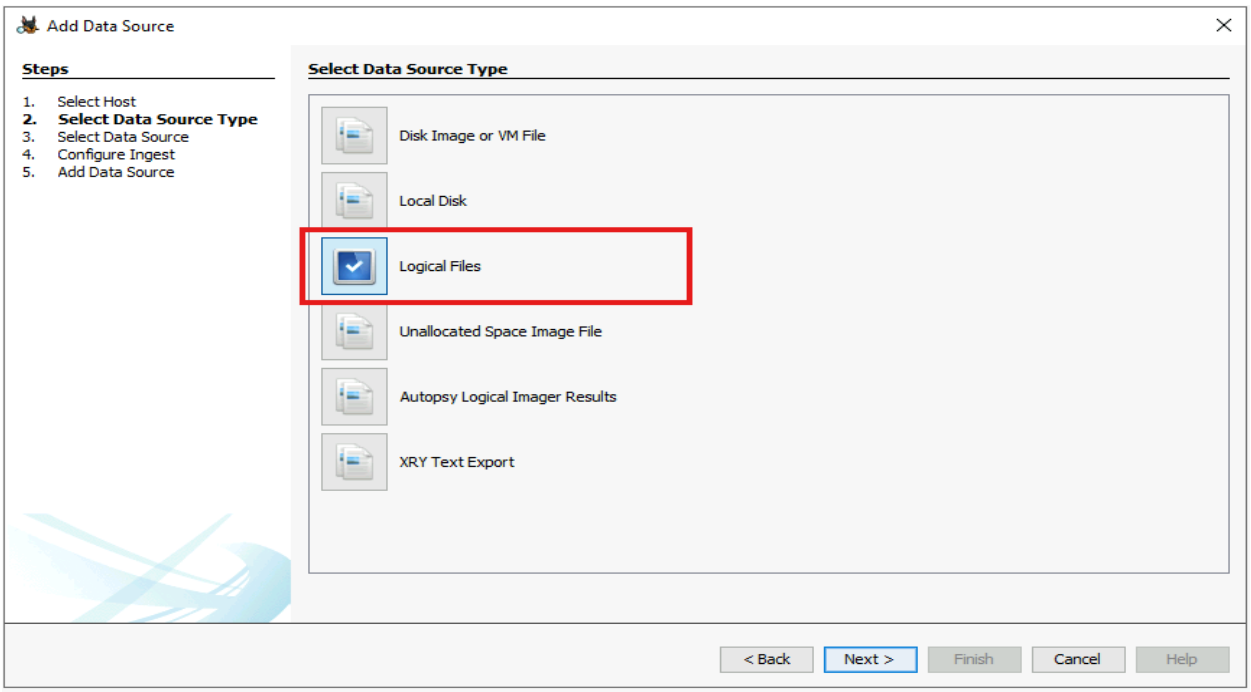
Answer: continental

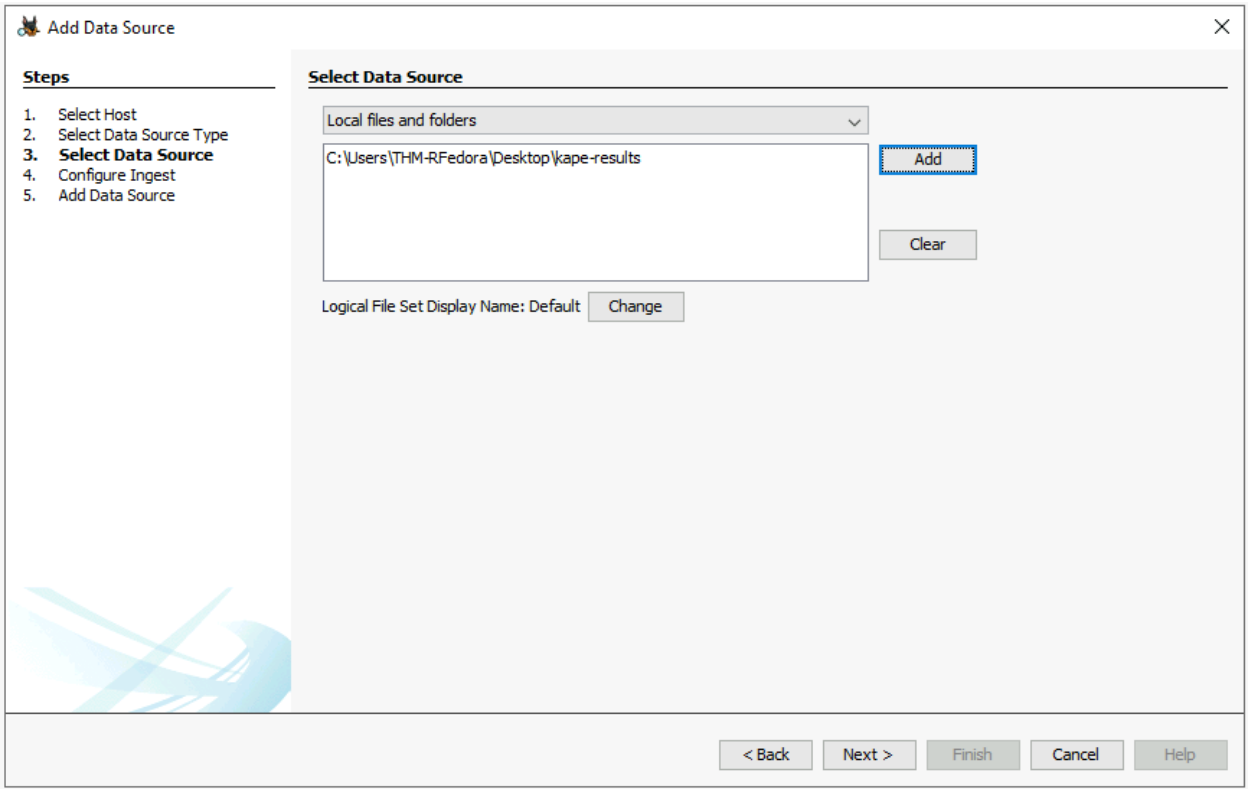


Not surprisingly, they quickly found what they are looking for in a matter of minutes.

Ha! They seem to have hit a snag! They needed something first before they could continue.


TryHackMe | Unattended
TryHackMe | Remote
Home | Microsoft 365
Unattended - Windows Forensics
https://remote-eu-10.tryhackme.tech/#/client/NDg4NzA1OABjAG15c3Fs?token=38FFE17D3DAC55BFE7ACCCEE751CB1ECD588BD62F62F1DBBE15030B267F4EF83D
Recycle Bin
WelcomeL...
kape-results
tools
NTUSER.D...
Autopsy 4.19.3
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Welcome
New Case
Open Recent Case
Open Case
Autopsy®
OPEN | EXTENSIBLE | FAST
Close
5:31 PM
11/29/2024

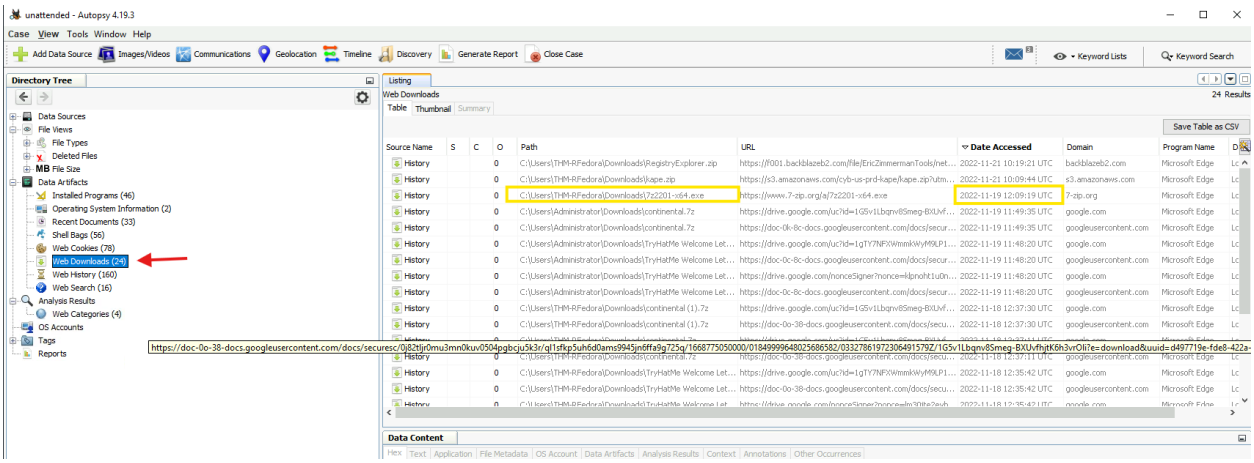




What is the name of the downloaded file to the Downloads folder?

Answer: 7z2201-x64.exe

Looking for downloaded files within the time frame.

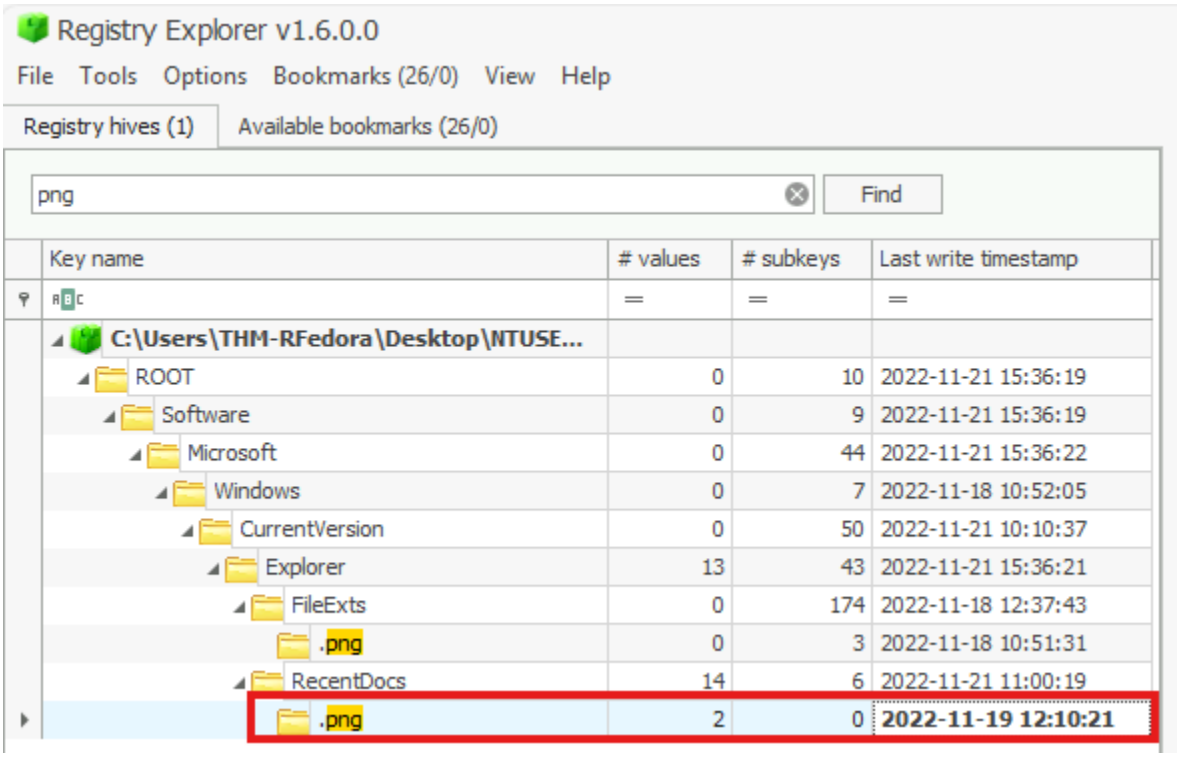


When was the file from the previous question downloaded?

Answer: 2022-11-19 12:09:19 UTC

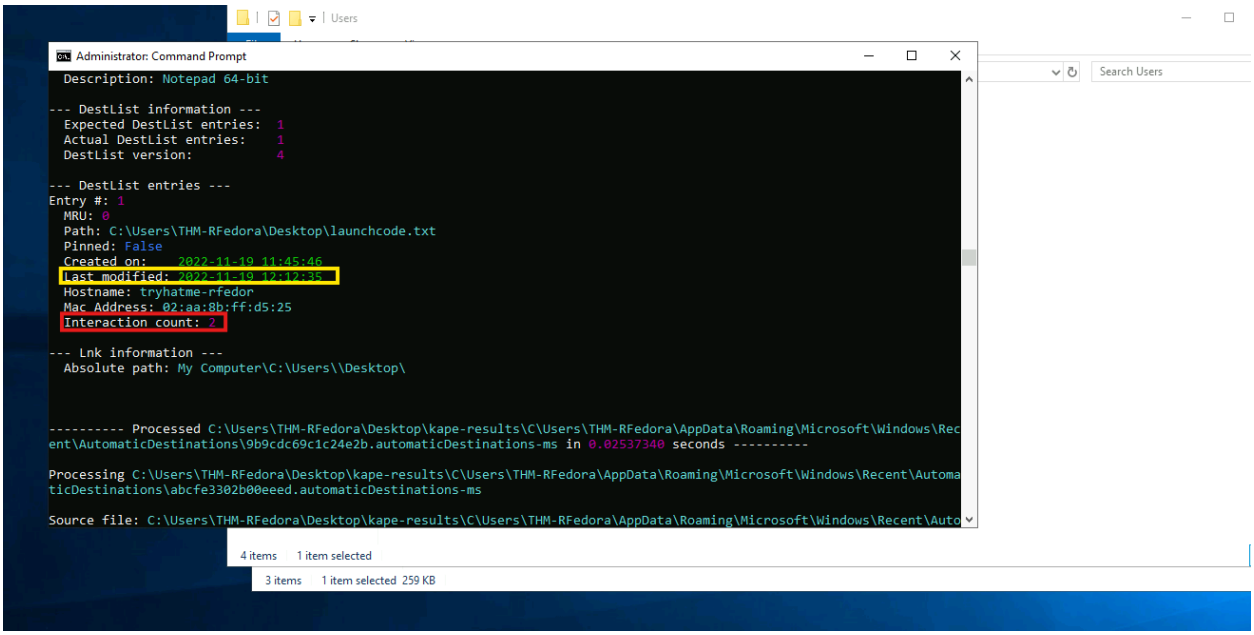
Thanks to the previously downloaded file, a PNG file was opened. When was this file opened?

Answer: 2022-11-19 12:10:21



Uh oh. They've hit the jackpot and are now preparing to exfiltrate data outside the network.

There is no way to do it via USB. So what's their other option?



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

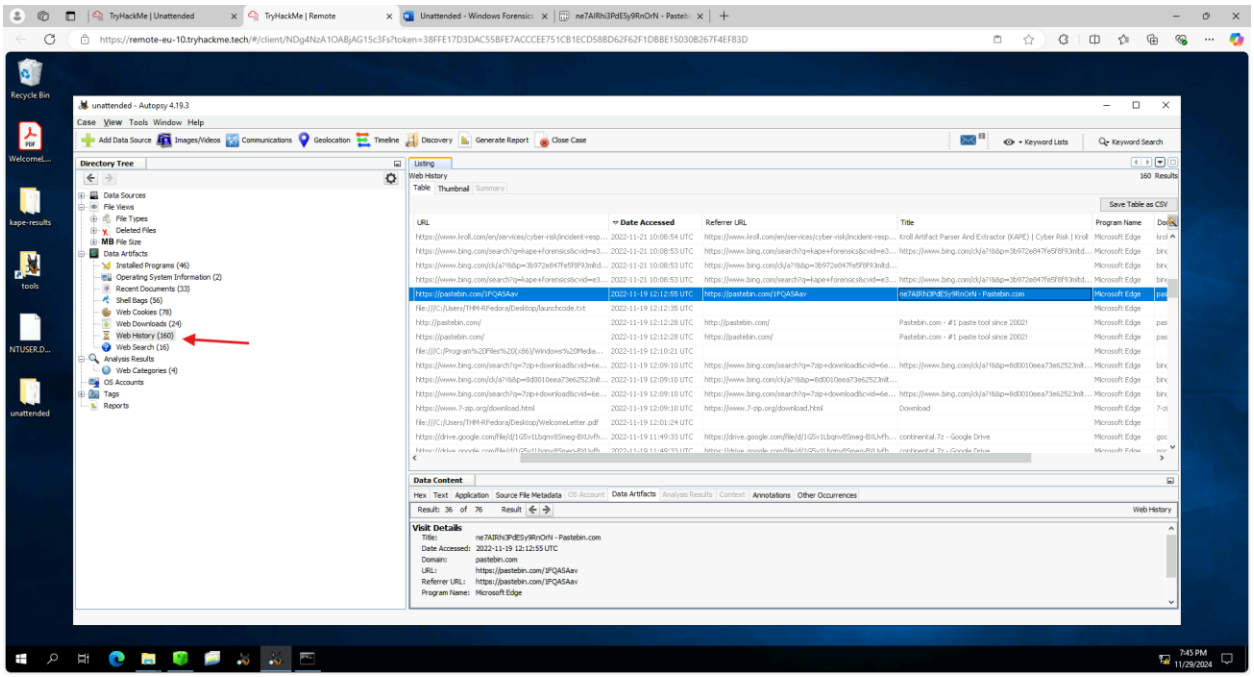
Answer: 2

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

Answer: 11/19/2022 12:12

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

Answer: https://pastebin.com/1FQASAav



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

Answer: ne7AlRhi3PdESy9RnOrN