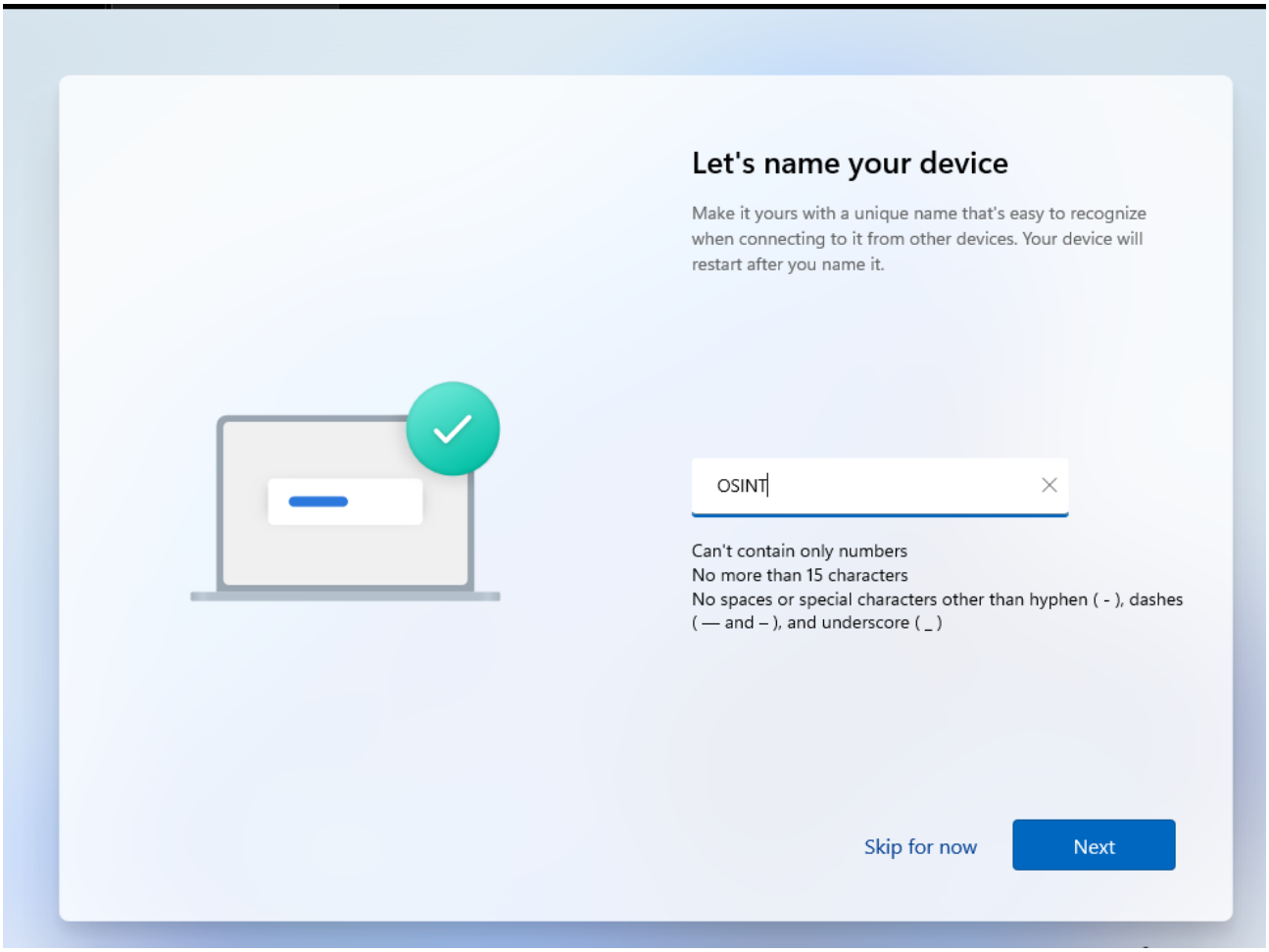
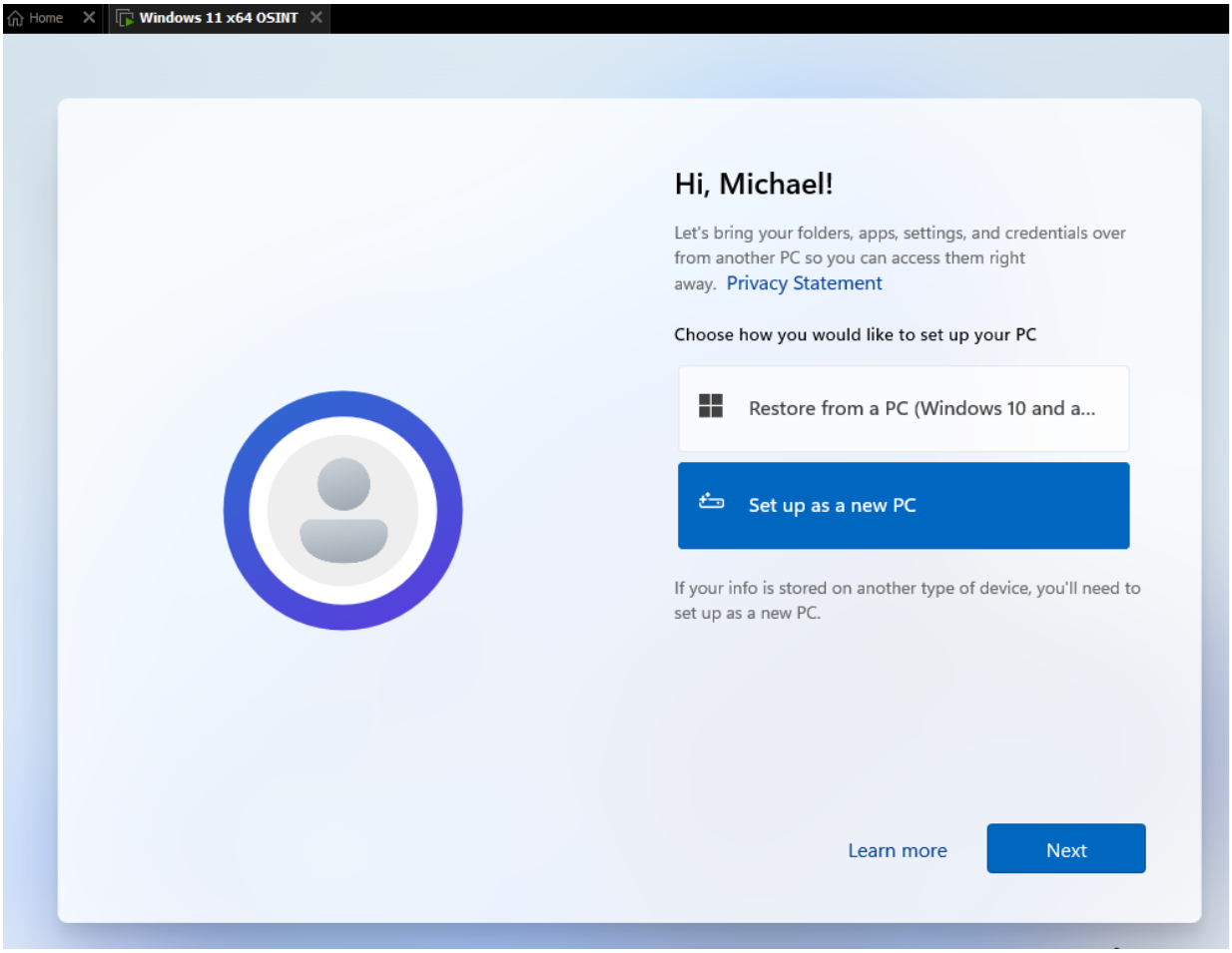
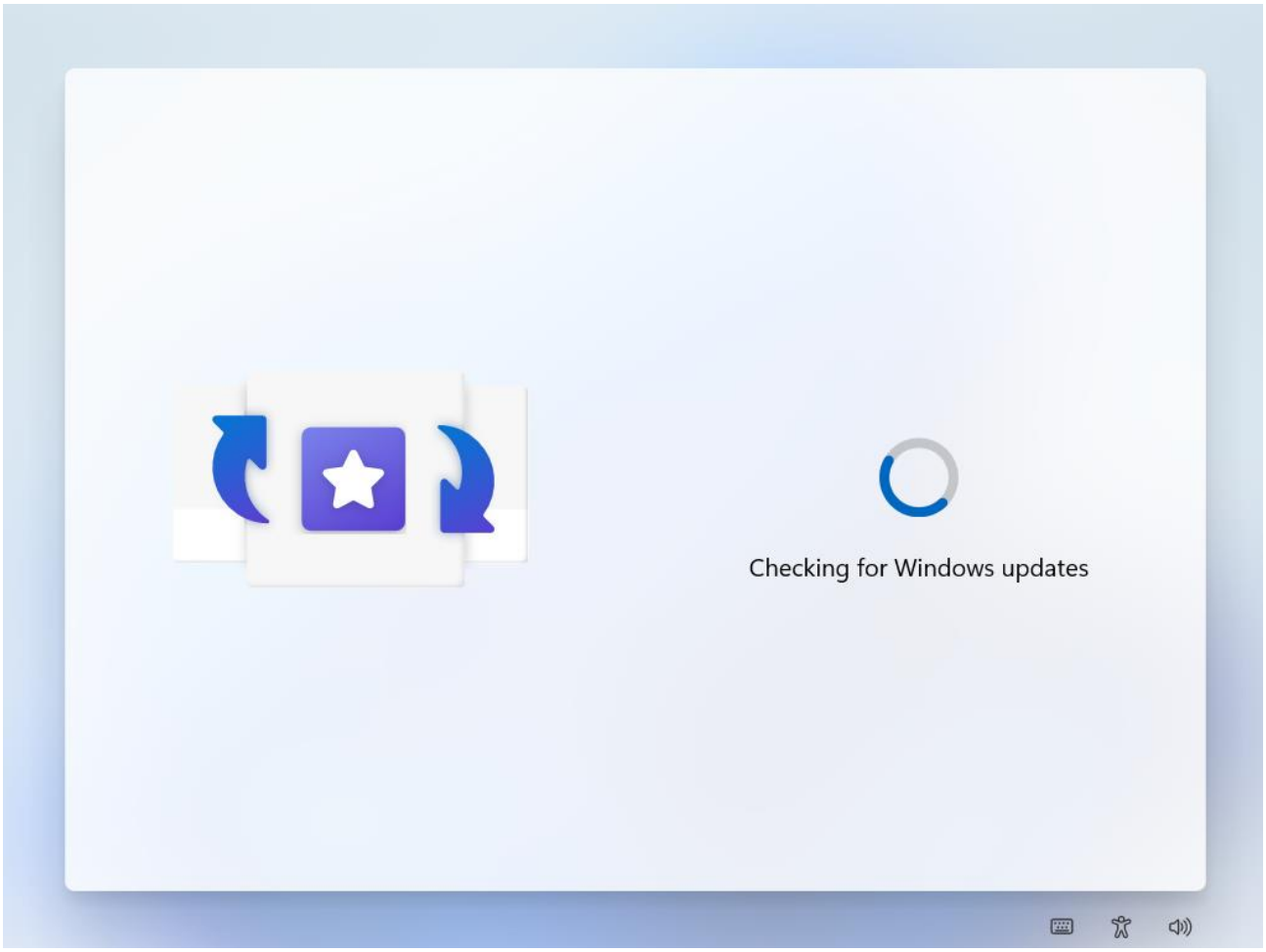
MOHAMAD ALMASRI *101167438*

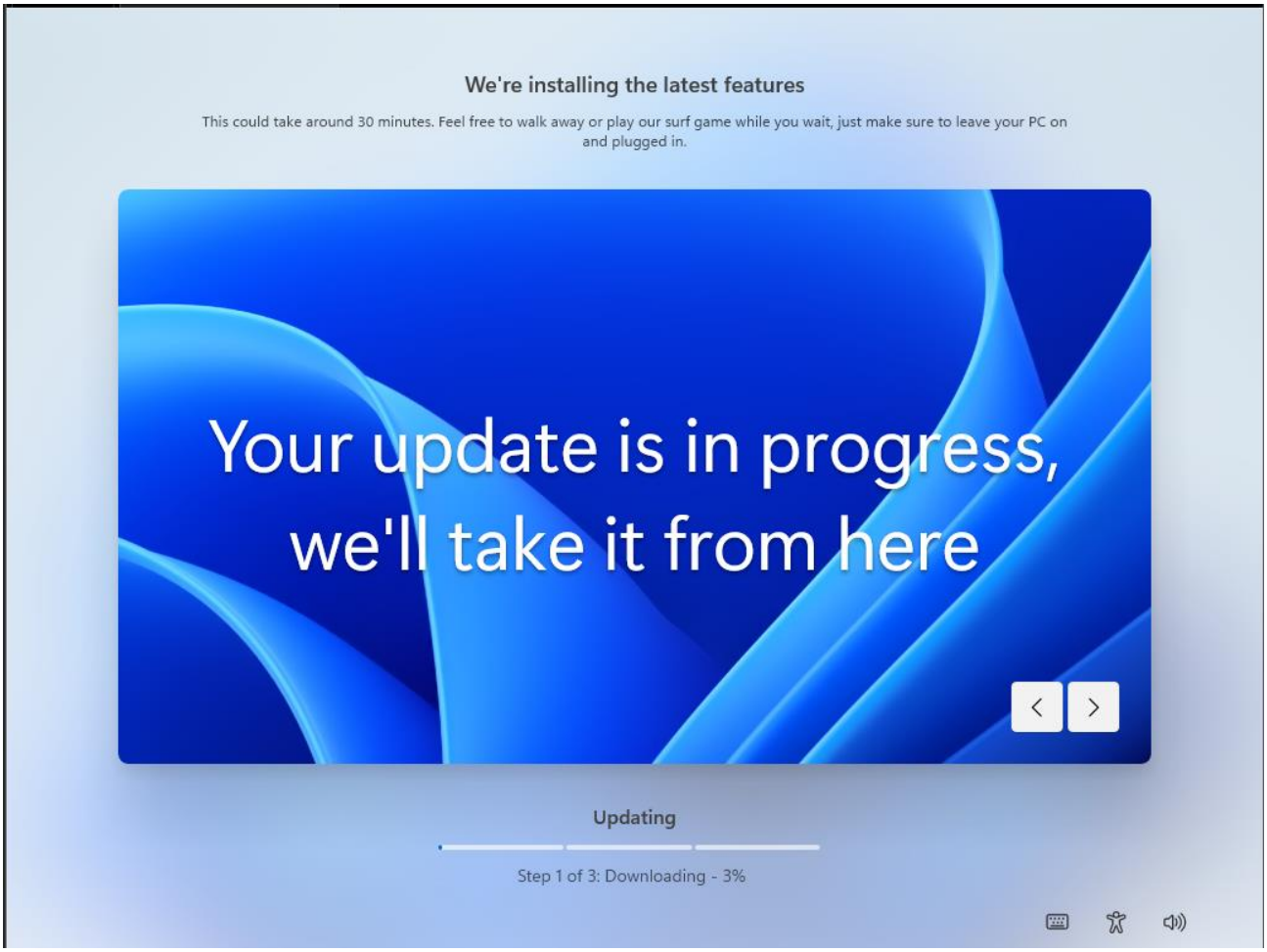
ADVANCED SOC - COMP 4078

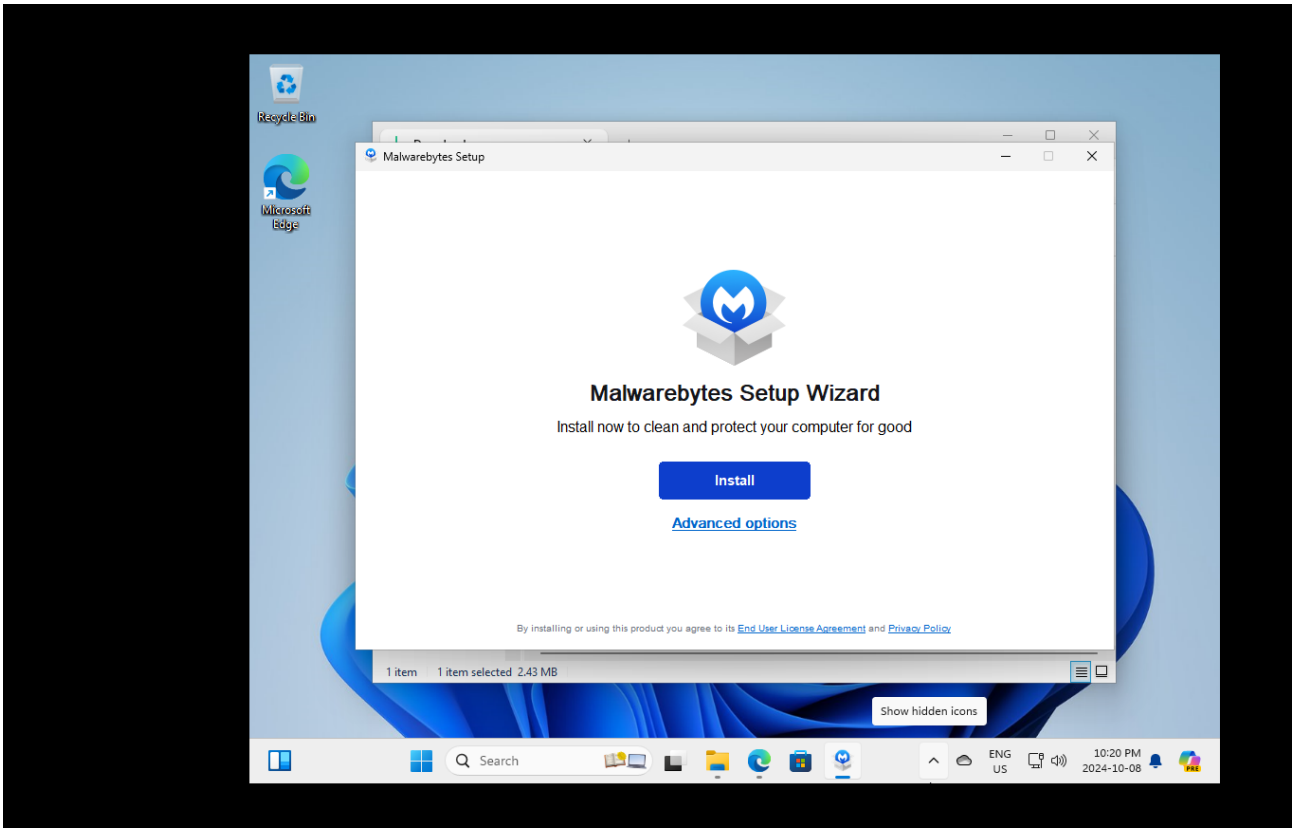
Lab03



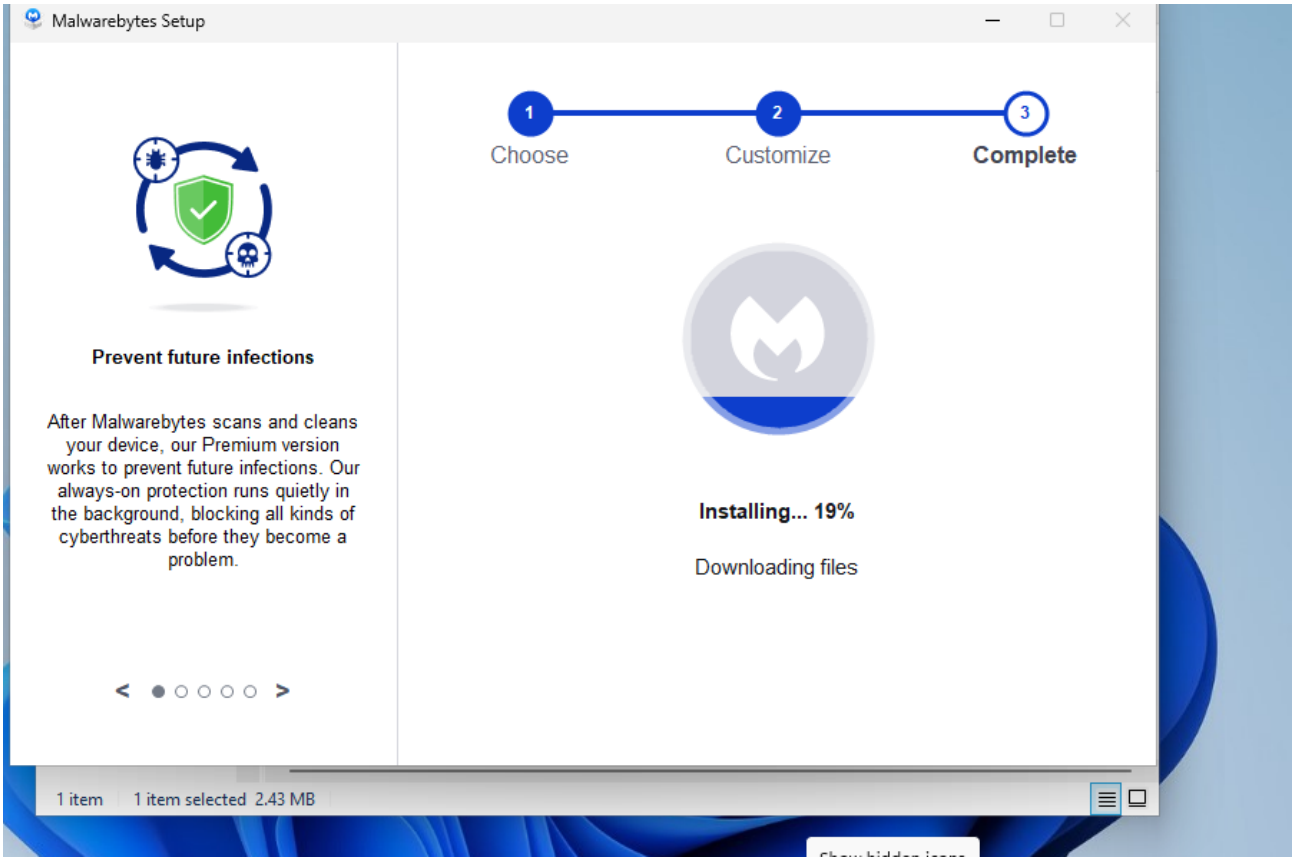

Home
Windows 11 x64 OSINT
Hi, Michael!
Let's bring your folders, apps, settings, and credentials over from another PC so you can access them right away. Privacy Statement
Choose how you would like to set up your PC
Restore from a PC (Windows 10 and a...
Set up as a new PC
If your info is stored on another type of device, you'll need to set up as a new PC.
Learn more
Next


Checking for Windows updates

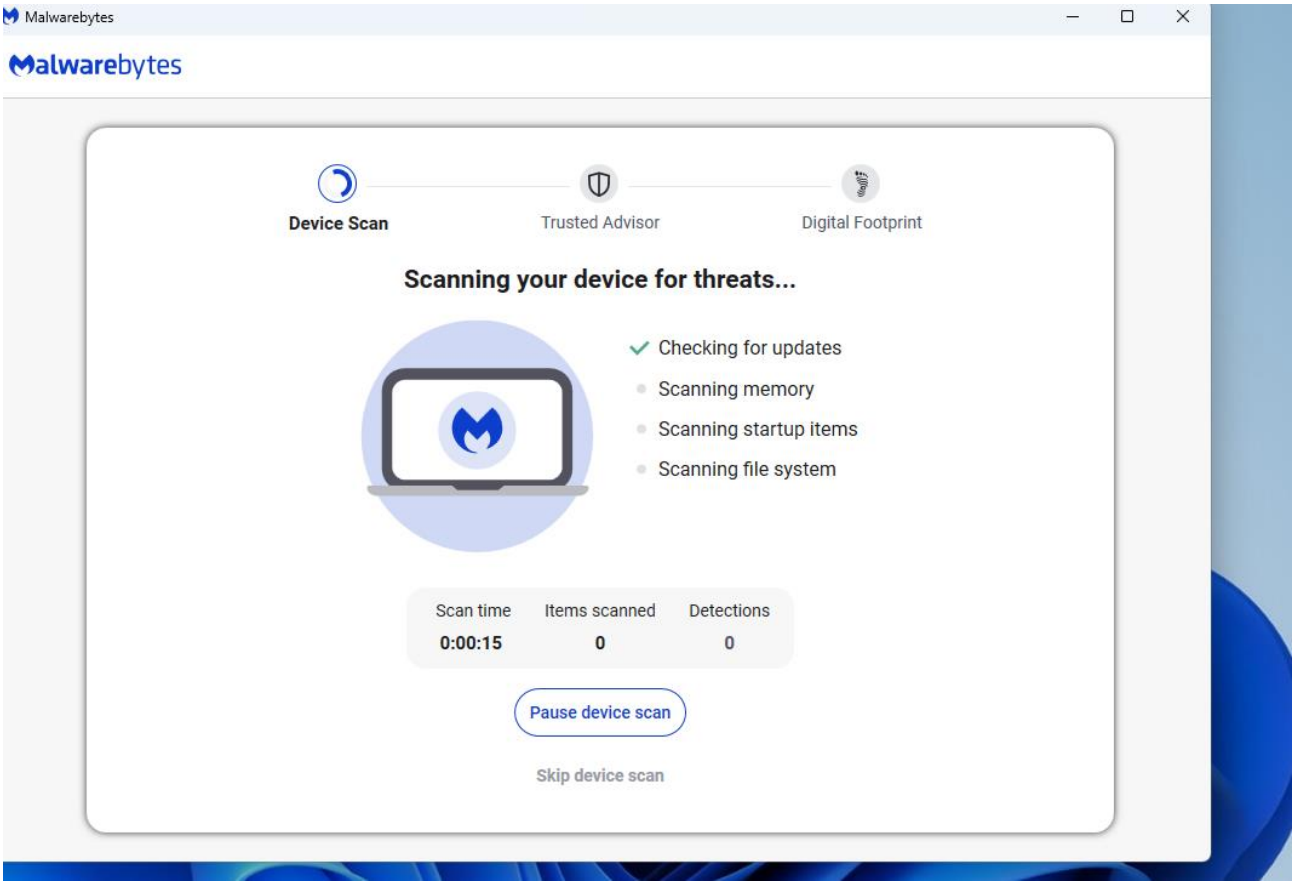

We're installing the latest features
This could take around 30 minutes. Feel free to walk away or play our surf game while you wait, just make sure to leave your PC on and plugged in.
Your update is in progress, we'll take it from here
Updating
Step 1 of 3: Downloading - 3%



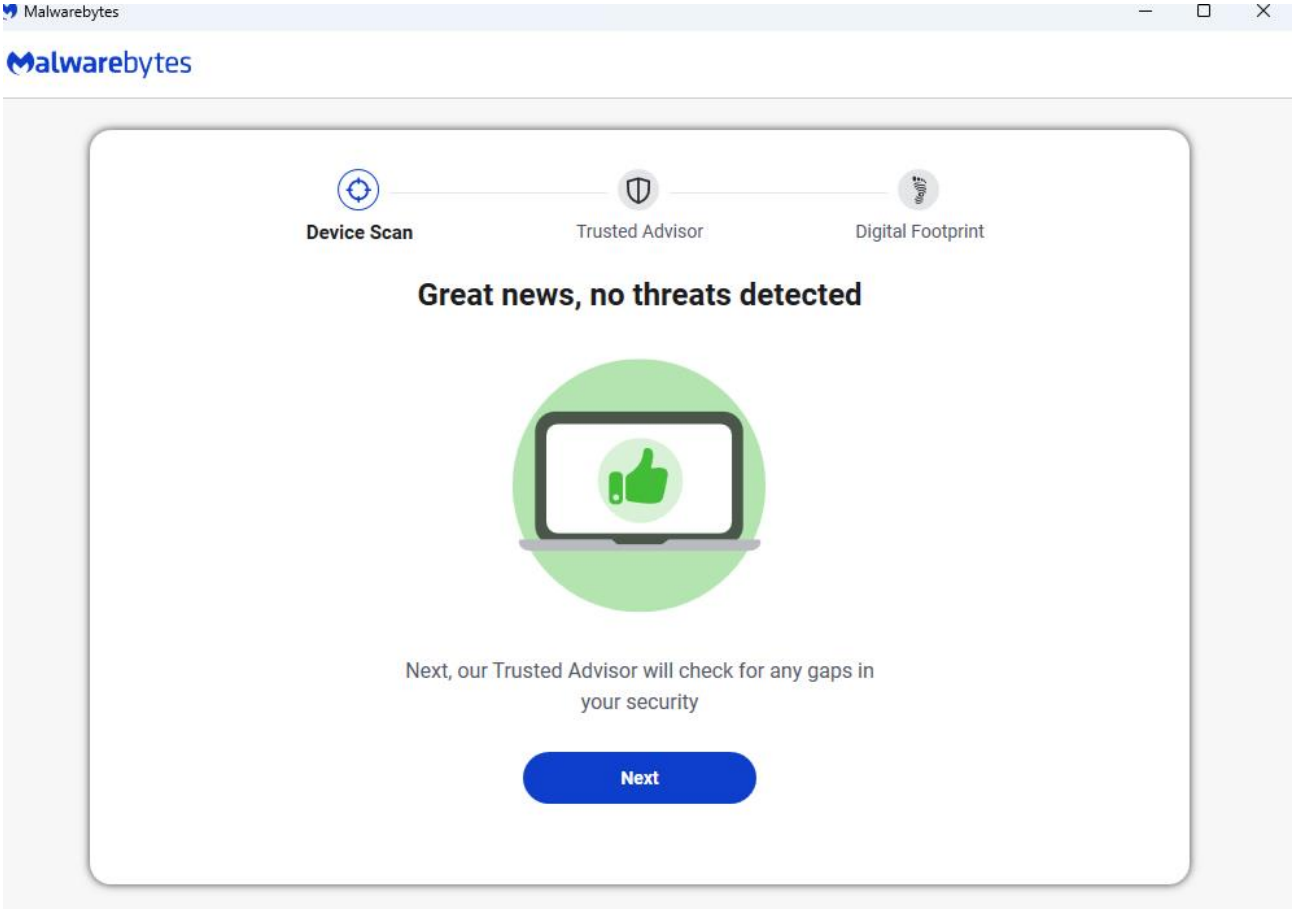
+Use Malwarebytes for Windows https:/ /www.malwarebytes.com/



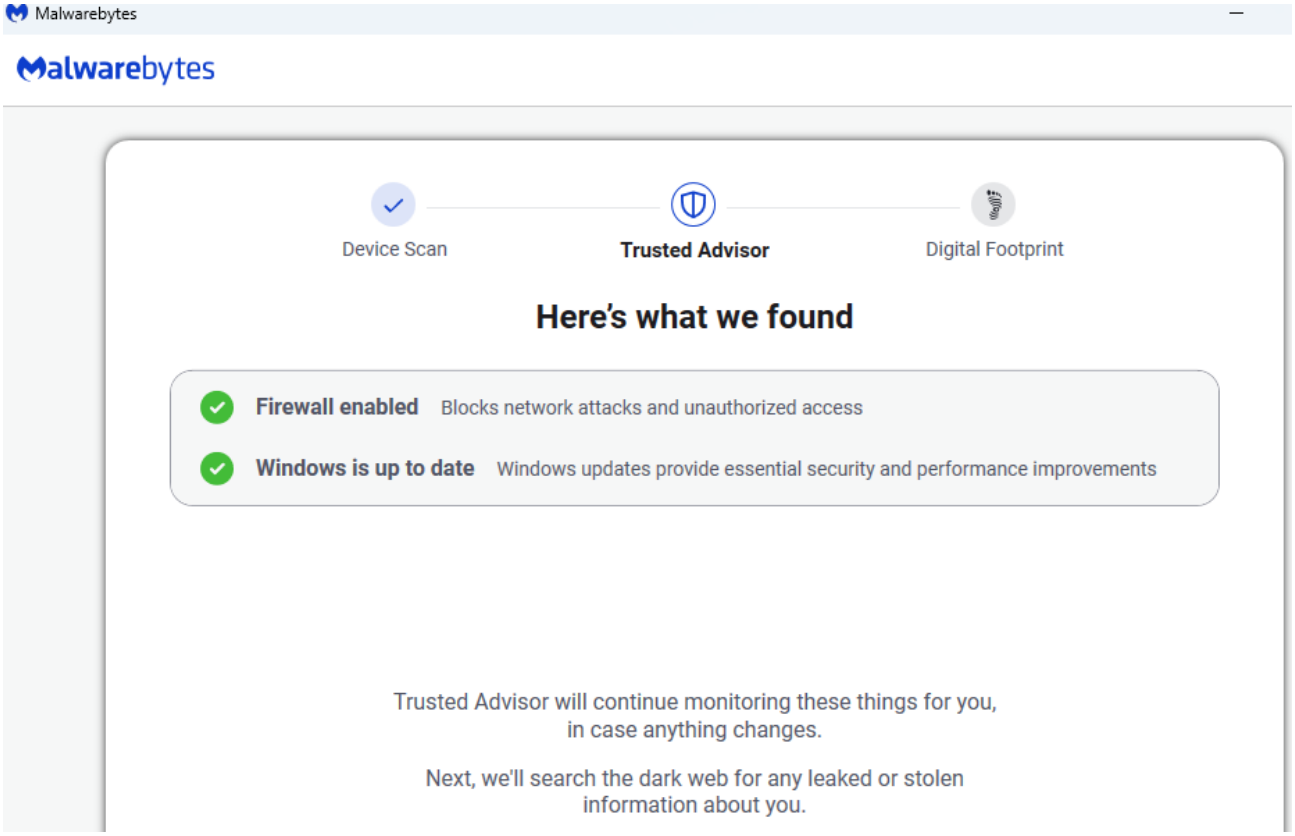
In the second step, the virtual machine is being configured as a new PC, following the setup process. The screenshot below shows the option to set up the machine as a new PC.



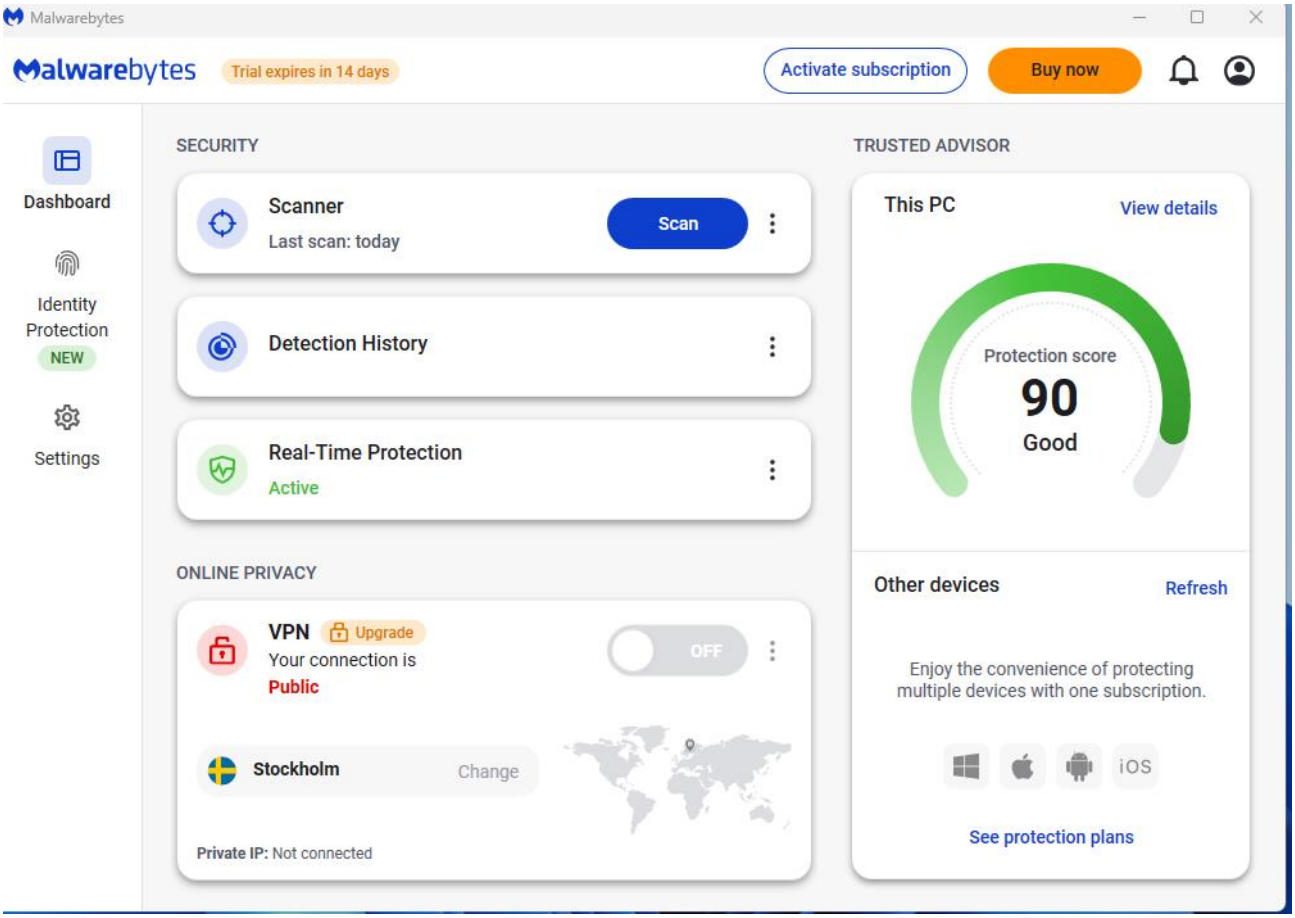
The second screenshot shows the VM setup as a new PC, which isolates the environment for safe and controlled OSINT operations. This clean setup is essential for conducting malware analysis without compromising the host machine.



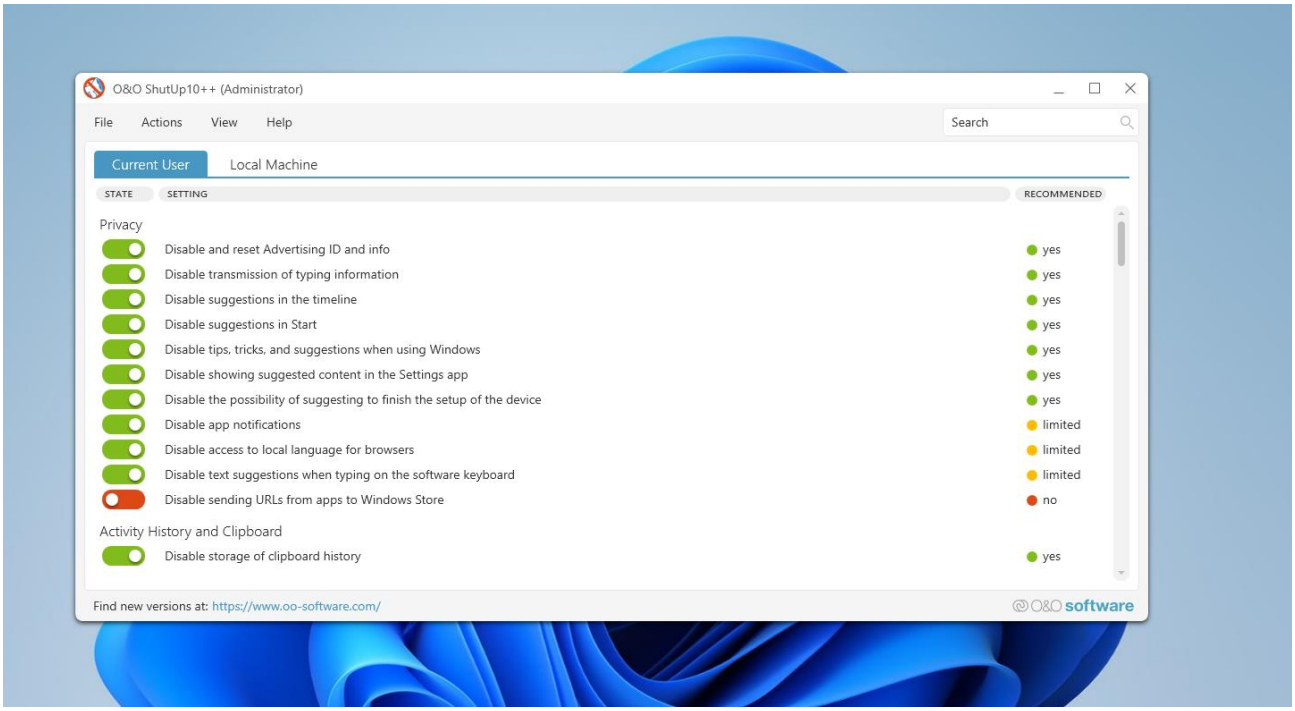
This step illustrates the process of checking for Windows updates on the virtual machine, ensuring that the latest security patches are applied



Here, Malwarebytes is shown actively scanning the system for any potential threats, ensuring that the system is secure before any further analysis is performed.

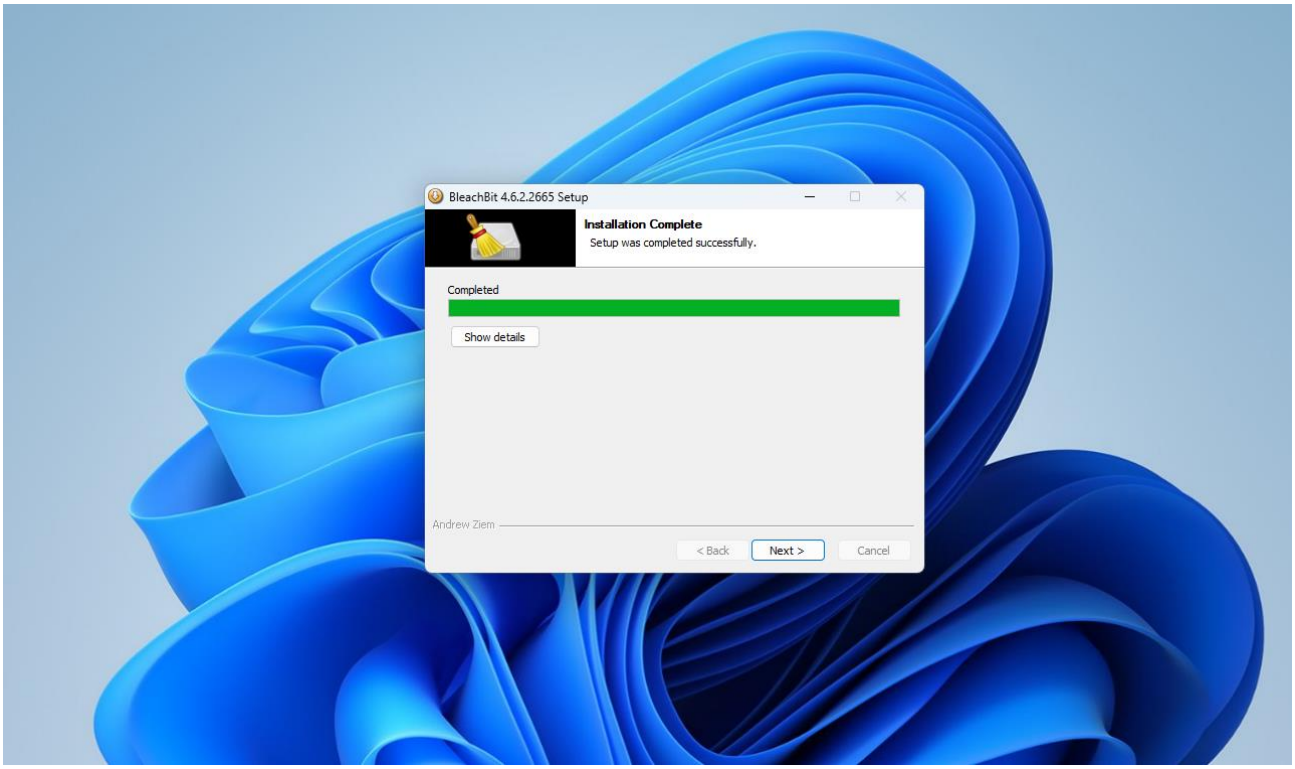

Malwarebytes
Malwarebytes
Trial expires in 14 days
Activate subscription
Buy now
Dashboard
Identity Protection
NEW
Settings
SECURITY
Scanner
Last scan: today
Scan
Detection History
Real-Time Protection
Active
ONLINE PRIVACY
VPN
Upgrade
Your connection is
Public
OFF
Stockholm
Change
Private IP: Not connected
TRUSTED ADVISOR
This PC
View details
Protection score
90
Good
Other devices
Refresh
Enjoy the convenience of protecting multiple devices with one subscription.
iOS
See protection plans

O&O Shut Up 10



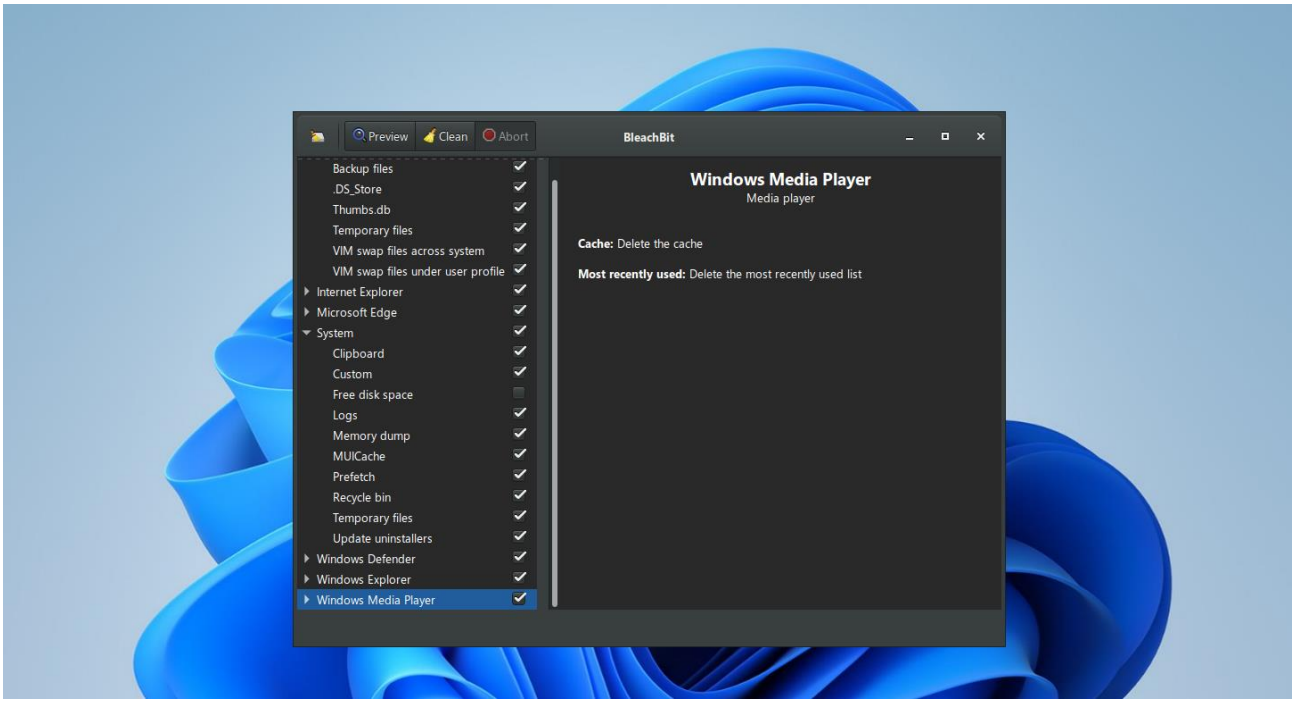
The next step involves configuring the necessary privacy settings using O&O Shut Up 10 and setting up other OSINT tools like BleachBit to ensure the environment is clean and secure.

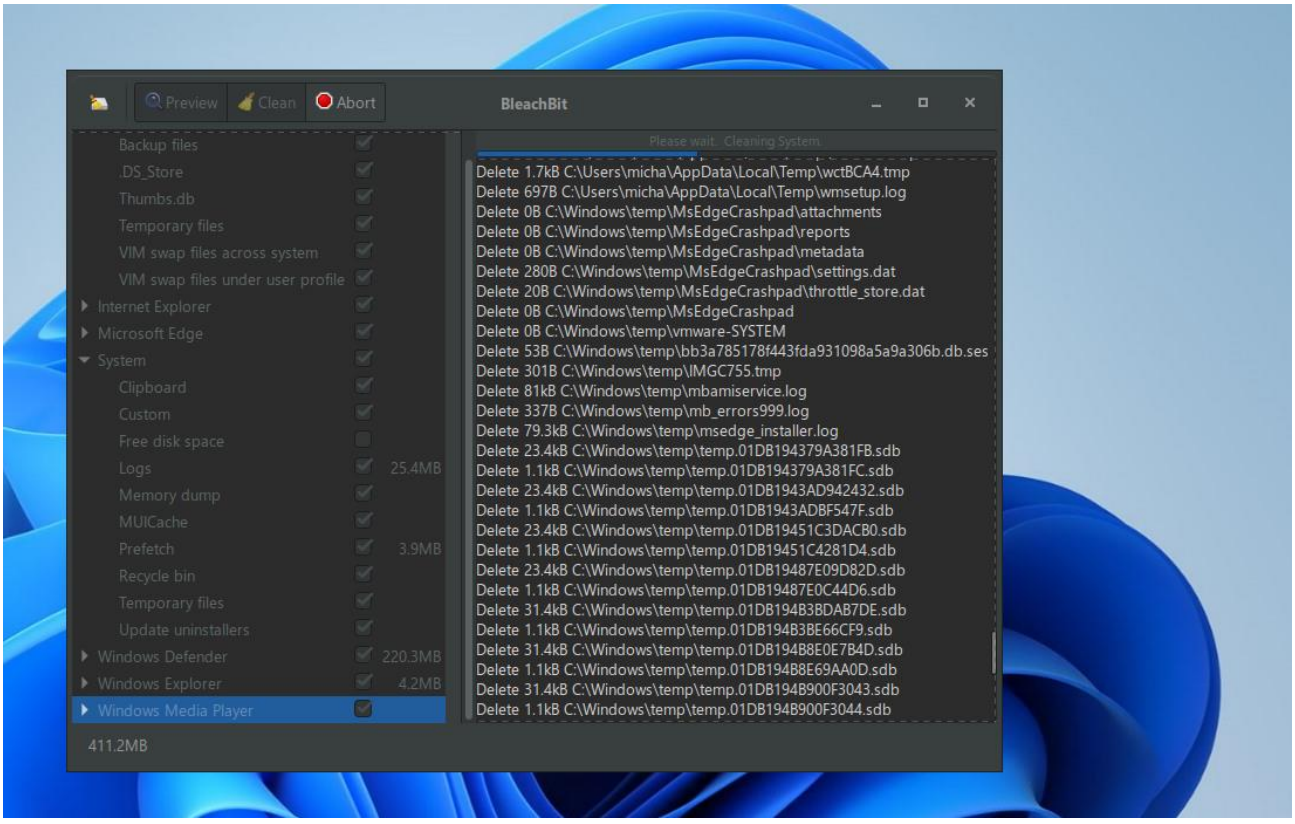
O&O Shut Up 10 is shown in this screenshot, which disables Windows telemetry and other privacy-intrusive features. This setup ensures a minimal data footprint during the analysis

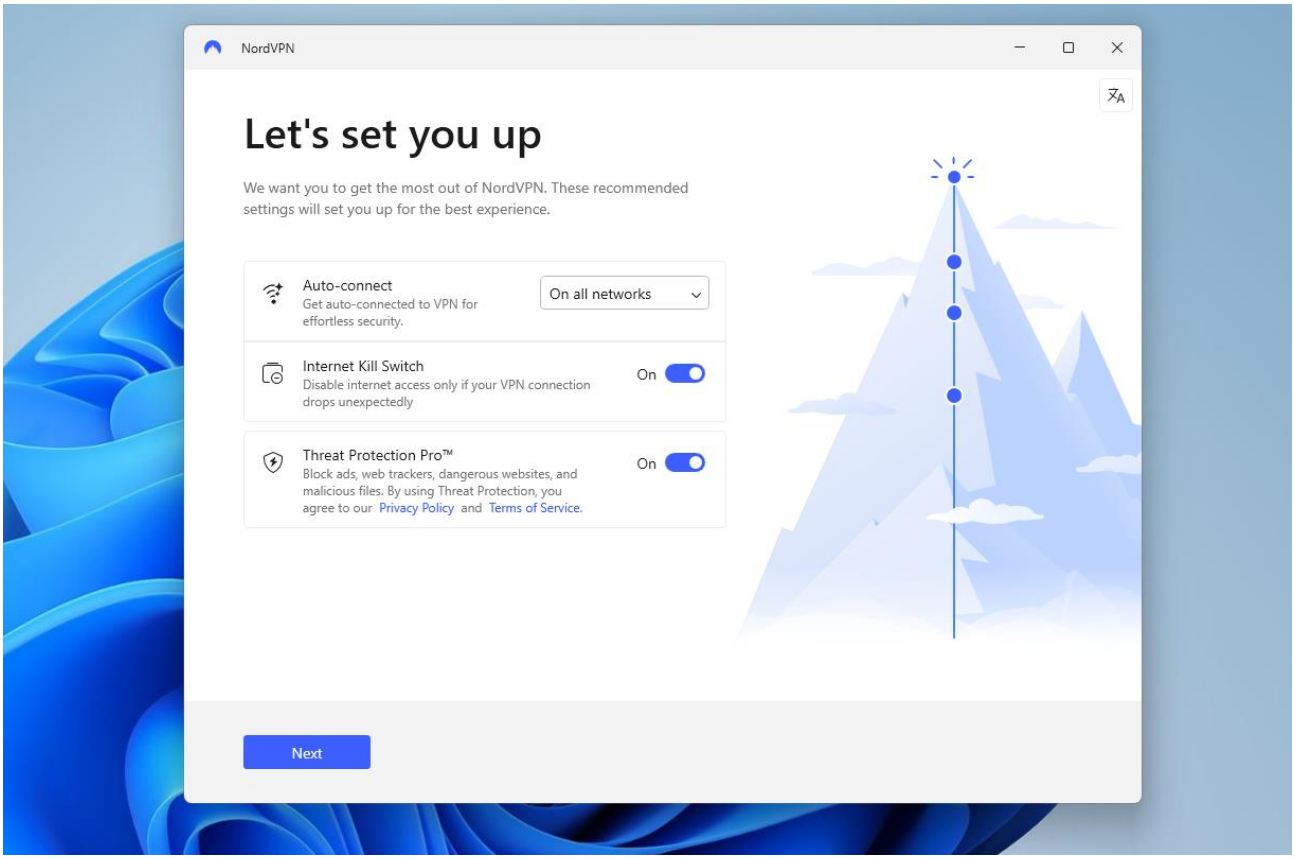


System Cleaner

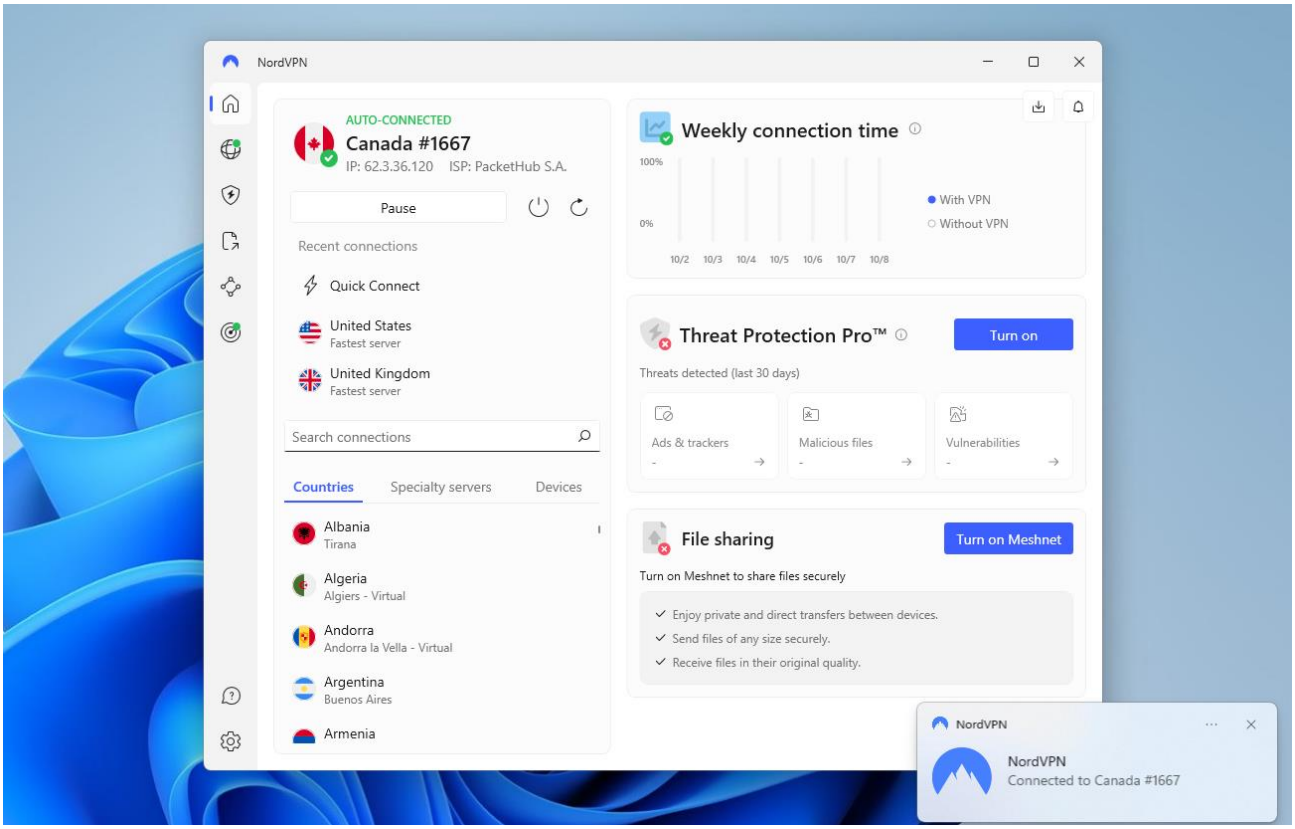
(bleachbit.org).


Preview
Clean
Abort
BleachBit
Backup files
.DS_Store
Thumbs.db
Temporary files
VIM swap files across system
VIM swap files under user profile
Internet Explorer
Microsoft Edge
System
Clipboard
Custom
Free disk space
Logs
Memory dump
MUICache
Prefetch
Recycle bin
Temporary files
Update uninstallers
Windows Defender
Windows Explorer
Windows Media Player
Windows Media Player
Media player
Cache: Delete the cache
Most recently used: Delete the most recently used list

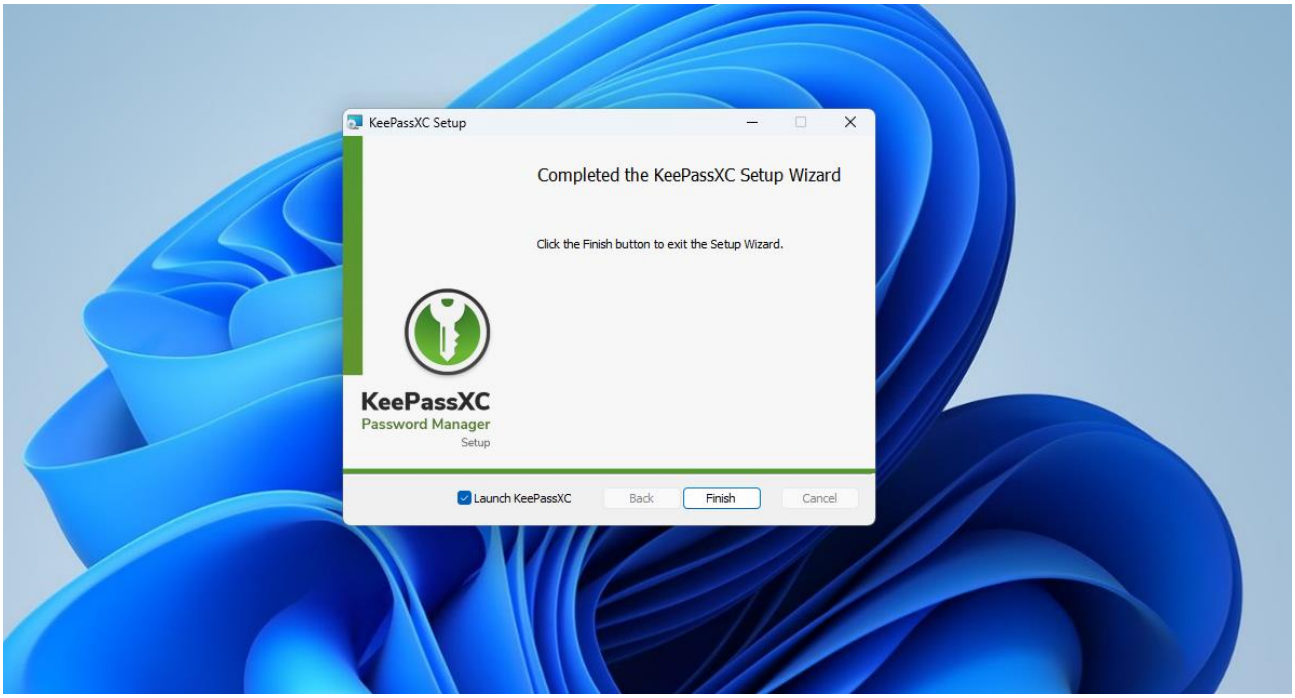

Preview
Clean
Abort
BleachBit
Please wait. Cleaning System.
Backup files
.DS_Store
Thumbs.db
Temporary files
VIM swap files across system
VIM swap files under user profile
Internet Explorer
Microsoft Edge
System
Clipboard
Custom
Free disk space
Logs 25.4MB
Memory dump
MUICache
Prefetch 3.9MB
Recycle bin
Temporary files
Update uninstallers
Windows Defender 220.3MB
Windows Explorer 4.2MB
Windows Media Player
411.2MB
Delete 1.7kB C:\Users\micha\AppData\Local\Temp\wctBCA4.tmp
Delete 697B C:\Users\micha\AppData\Local\Temp\wmsetup.log
Delete 0B C:\Windows\temp\MsEdgeCrashpad\attachments
Delete 0B C:\Windows\temp\MsEdgeCrashpad\reports
Delete 0B C:\Windows\temp\MsEdgeCrashpad\metadata
Delete 280B C:\Windows\temp\MsEdgeCrashpad\settings.dat
Delete 20B C:\Windows\temp\MsEdgeCrashpad\throttle_store.dat
Delete 0B C:\Windows\temp\MsEdgeCrashpad
Delete 0B C:\Windows\temp\vmware-SYSTEM
Delete 53B C:\Windows\temp\bb3a785178f443fda931098a5a9a306b.db.ses
Delete 301B C:\Windows\temp\IMGC755.tmp
Delete 81kB C:\Windows\temp\mbamiservice.log
Delete 337B C:\Windows\temp\mb_errors999.log
Delete 79.3kB C:\Windows\temp\msedge_installer.log
Delete 23.4kB C:\Windows\temp\temp.01DB194379A381FB.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB194379A381FC.sdb
Delete 23.4kB C:\Windows\temp\temp.01DB1943AD942432.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB1943ADBF547F.sdb
Delete 23.4kB C:\Windows\temp\temp.01DB19451C3DACB0.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB19451C4281D4.sdb
Delete 23.4kB C:\Windows\temp\temp.01DB19487E09D82D.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB19487E0C44D6.sdb
Delete 31.4kB C:\Windows\temp\temp.01DB194B3BDAB7DE.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB194B3BE66CF9.sdb
Delete 31.4kB C:\Windows\temp\temp.01DB194B8E0E7B4D.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB194B8E69AA0D.sdb
Delete 31.4kB C:\Windows\temp\temp.01DB194B900F3043.sdb
Delete 1.1kB C:\Windows\temp\temp.01DB194B900F3044.sdb

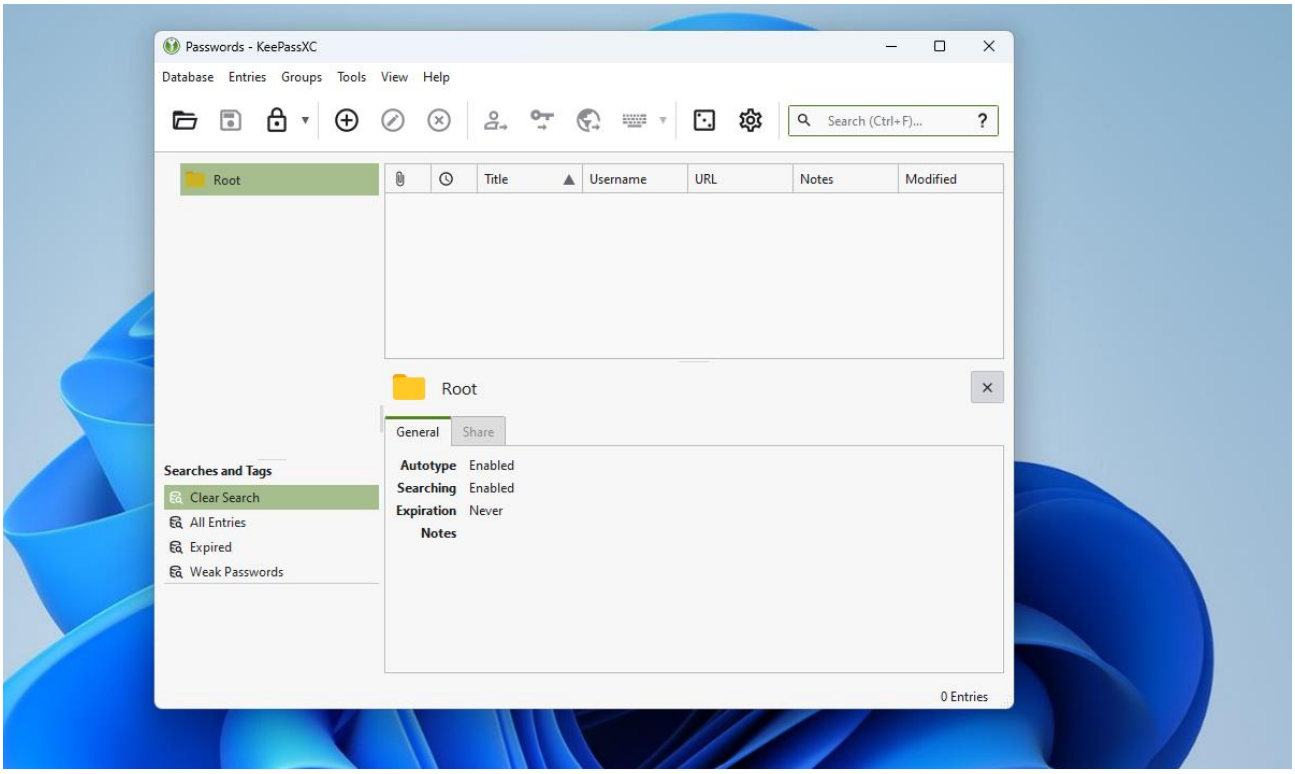


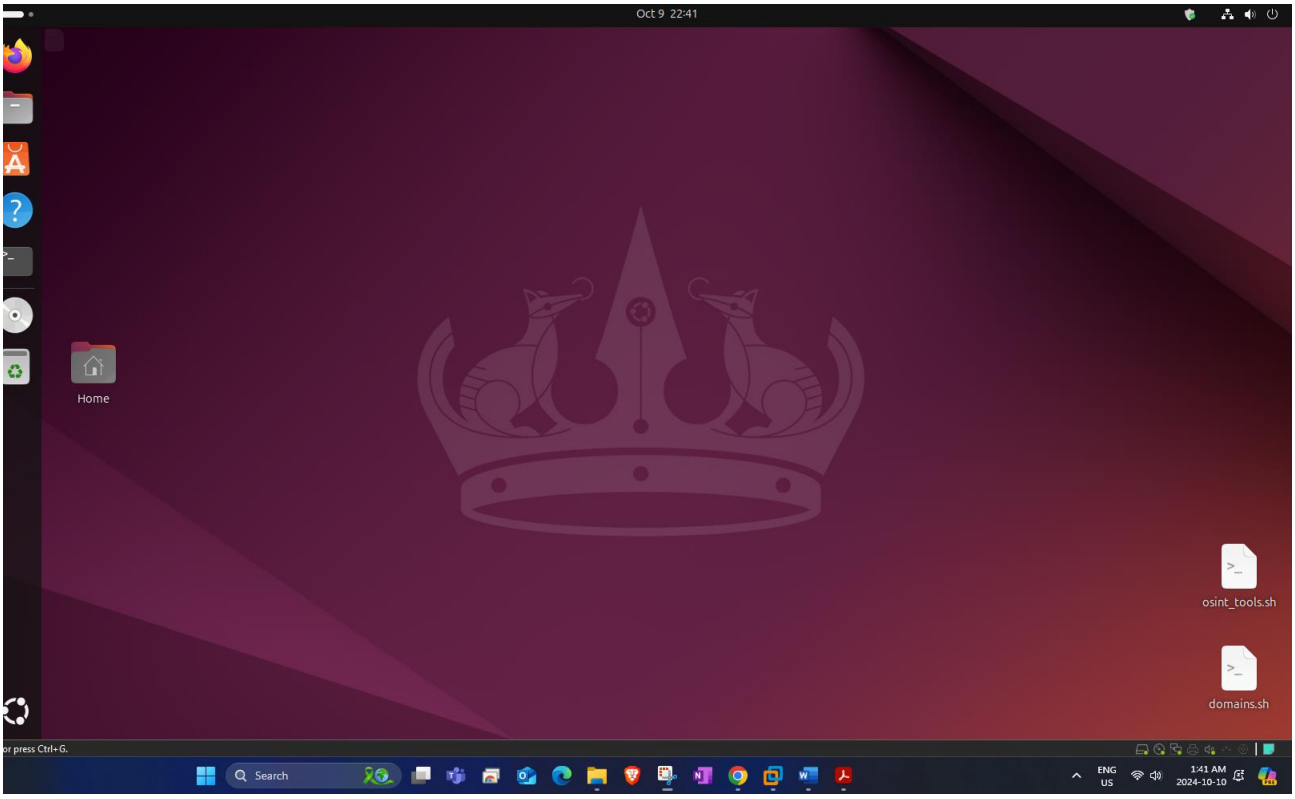
Here, the images show the setup of NordVPN, which provides secure and encrypted network access. Following the VPN configuration



KeePassXC is used for managing passwords securely.


KeePassXC Setup
Completed the KeePassXC Setup Wizard
Click the Finish button to exit the Setup Wizard.
KeePassXC
Password Manager
Setup
Launch KeePassXC
Back
Finish
Cancel


Passwords - KeePassXC
Database Entries Groups Tools View Help
Search (Ctrl+F)...
Root
Title
Username
URL
Notes
Modified
Root
General
Share
Autotype Enabled
Searching Enabled
Expiration Never
Notes
Searches and Tags
Clear Search
All Entries
Expired
Weak Passwords
0 Entries



Firefox is configured with secure browsing settings to prevent tracking and ensure privacy during browsing sessions. The following placeholders show the various configurations made to enhance privacy and security.

Browsing

- [ ] Use autoscrolling
- [x] Use smooth scrolling
- [ ] Always show scrollbars
- [ ] Always use the cursor keys to navigate within pages
- [ ] Always underline links
- [ ] Search for text when you start typing
- [x] Enable picture-in-picture video controls Learn more
- [x] Control media via keyboard, headset, or virtual interface Learn more
- [ ] Recommend extensions as you browse Learn more
- [ ] Recommend features as you browse Learn more

Network Settings

Home

Restore Defaults

New Windows and Tabs

Choose what you see when you open your homepage, new windows, and new tabs.

Homepage and new windows: Blank Page

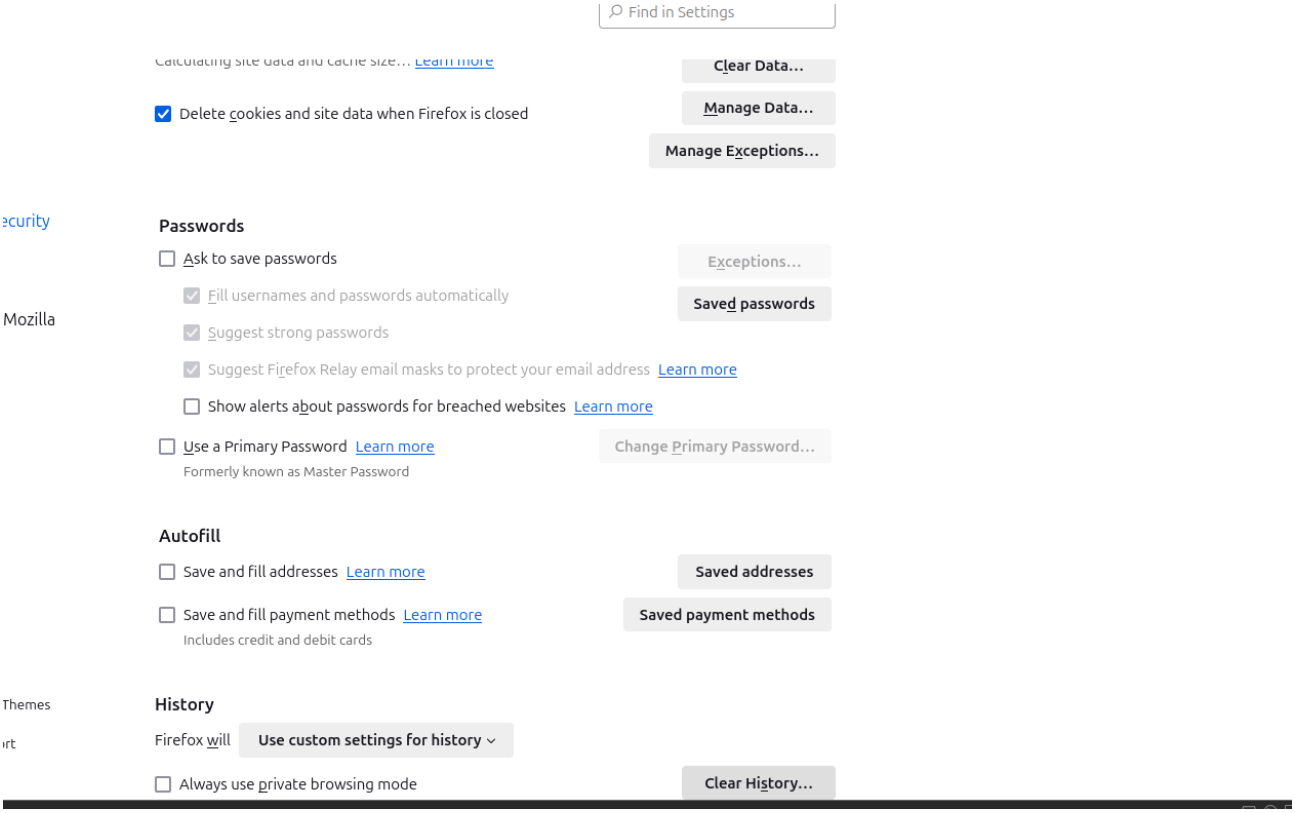
New tabs: Blank Page

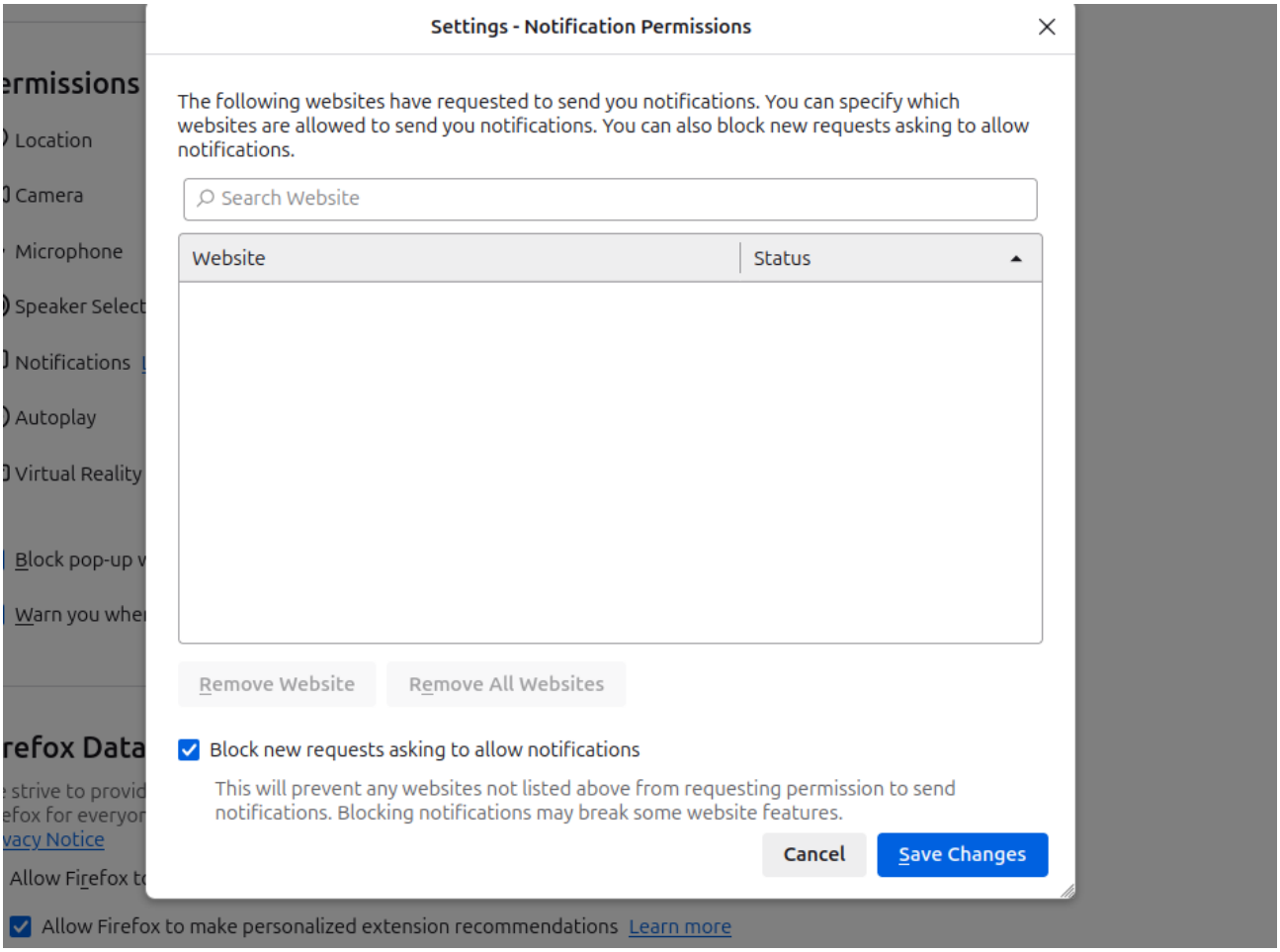
Firefox Home Content

Choose what content you want on your Firefox Home screen.

- [ ] Web Search
- [ ] Shortcuts
  - Sites you save or visit: 1 row
  - [ ] Sponsored shortcuts
- [ ] Recommended stories How it works
  - Exceptional content curated by the Firefox family
  - [ ] Sponsored stories
- [ ] Recent activity
  - A selection of recent sites and content: 1 row
  - [ ] Visited pages
  - [ ] Bookmarks

MOHAMAD ALMASRI 101167438





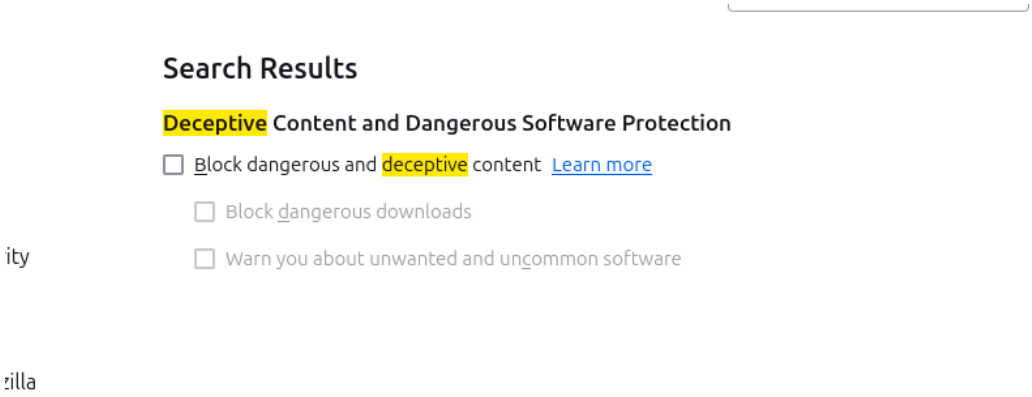
Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.
Privacy Notice

You're no longer allowing Mozilla to capture technical and interaction data. All past data will be deleted within 30 days. Learn more

- [ ] Allow Firefox to send technical and interaction data to Mozilla Learn more
  - [ ] Allow Firefox to make personalized extension recommendations Learn more
- [ ] Allow Firefox to install and run studies View Firefox studies
- [ ] Allow Firefox to send backlogged crash reports on your behalf Learn more

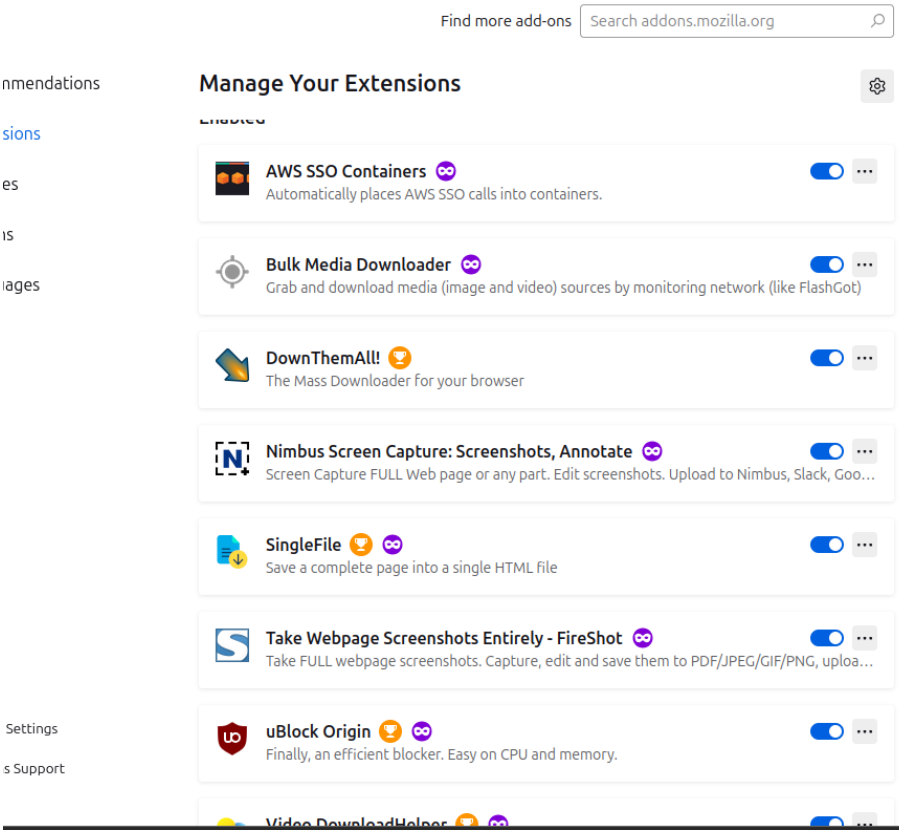
Website Advertising Preferences

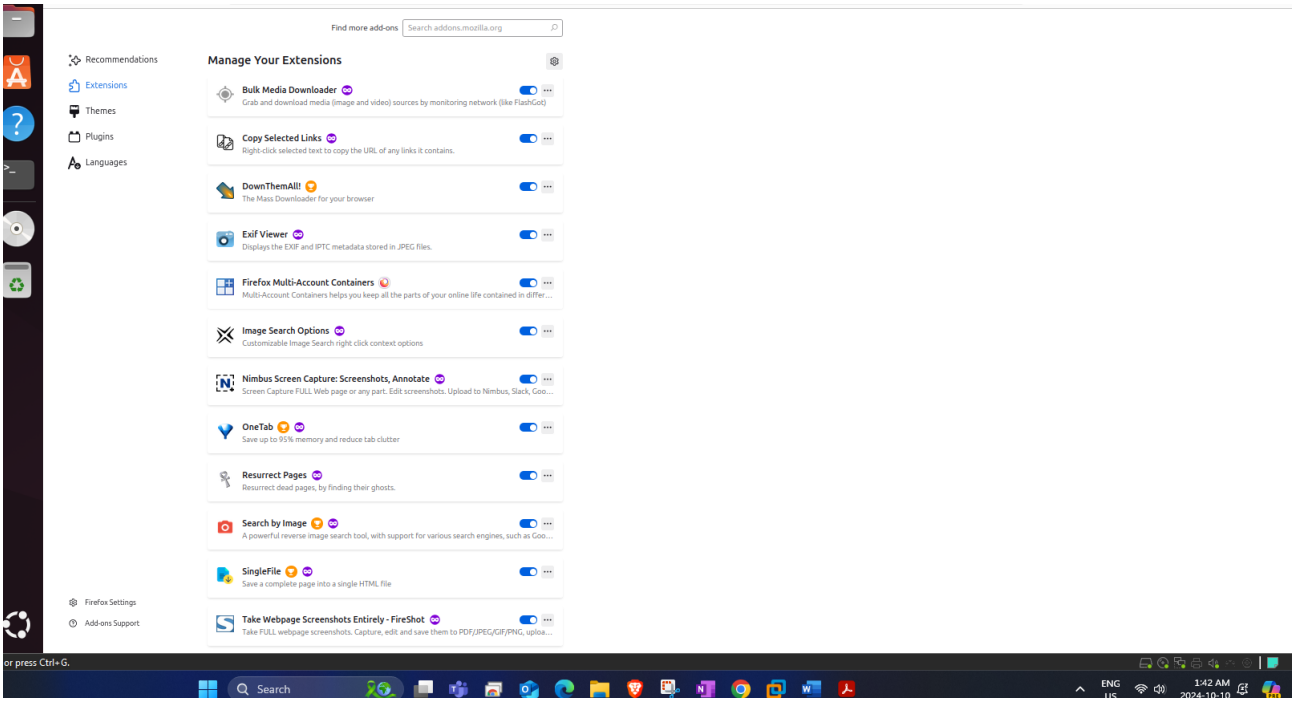


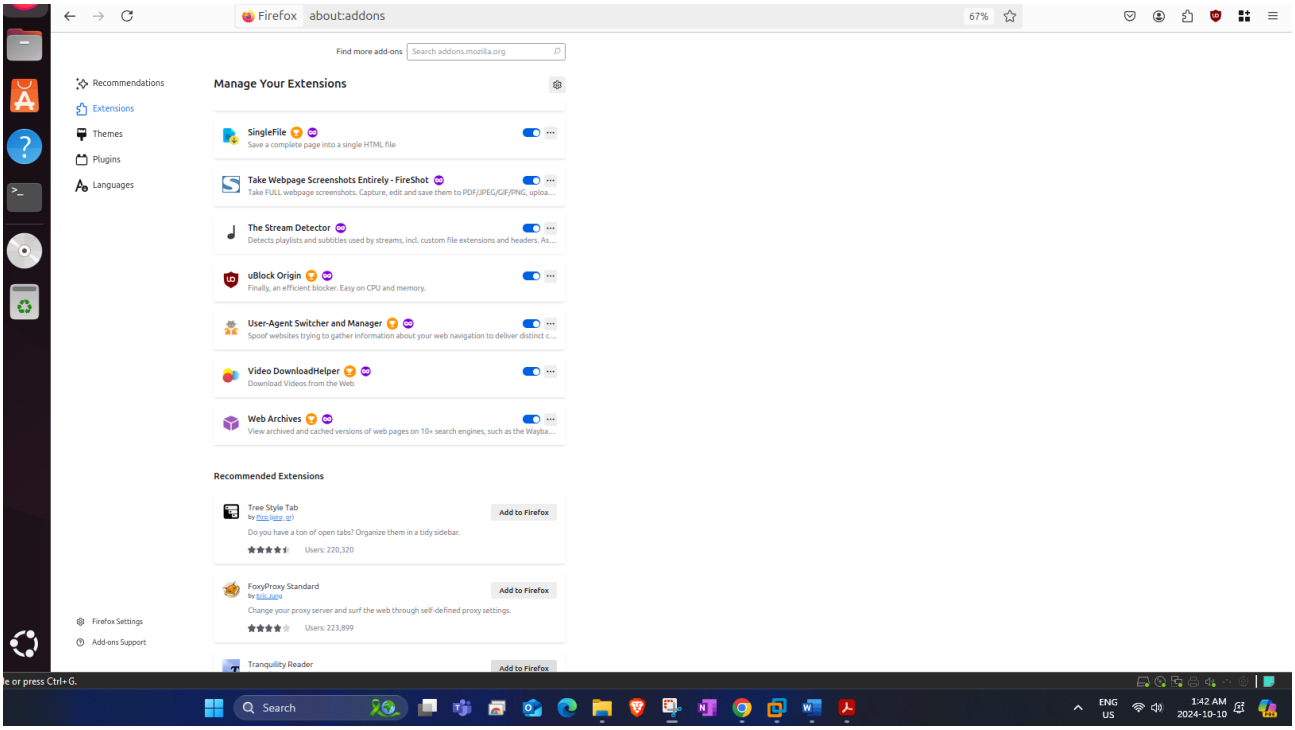
Recommended Add-ons:

- **Firefox Containers**: Isolates websites in separate tabs.
- **uBlock Origin**: Blocks unwanted scripts.
- **DownThemAll**: Downloads bulk media.
- **Bulk Media Downloader**: Downloads bulk media.
- **VideoDownloadHelper**: Downloads media with one click.
- **FireShot**: Takes screenshots of web pages.
- **Nimbus**: Captures large web pages.
- **SingleFile**: Saves web pages as HTML files.

I've installed all these add-ons, as shown in your screenshot.


Find more add-ons
Search addons.mozilla.org
nmendations
sions
es
ıs
ıages
Manage Your Extensions
AWS SSO Containers
Automatically places AWS SSO calls into containers.
Bulk Media Downloader
Grab and download media (image and video) sources by monitoring network (like FlashGot)
DownThemAll!
The Mass Downloader for your browser
Nimbus Screen Capture: Screenshots, Annotate
Screen Capture FULL Web page or any part. Edit screenshots. Upload to Nimbus, Slack, Goo...
SingleFile
Save a complete page into a single HTML file
Take Webpage Screenshots Entirely - FireShot
Take FULL webpage screenshots. Capture, edit and save them to PDF/JPEG/GIF/PNG, uploa...
Settings
s Support
uBlock Origin
Finally, an efficient blocker. Easy on CPU and memory.

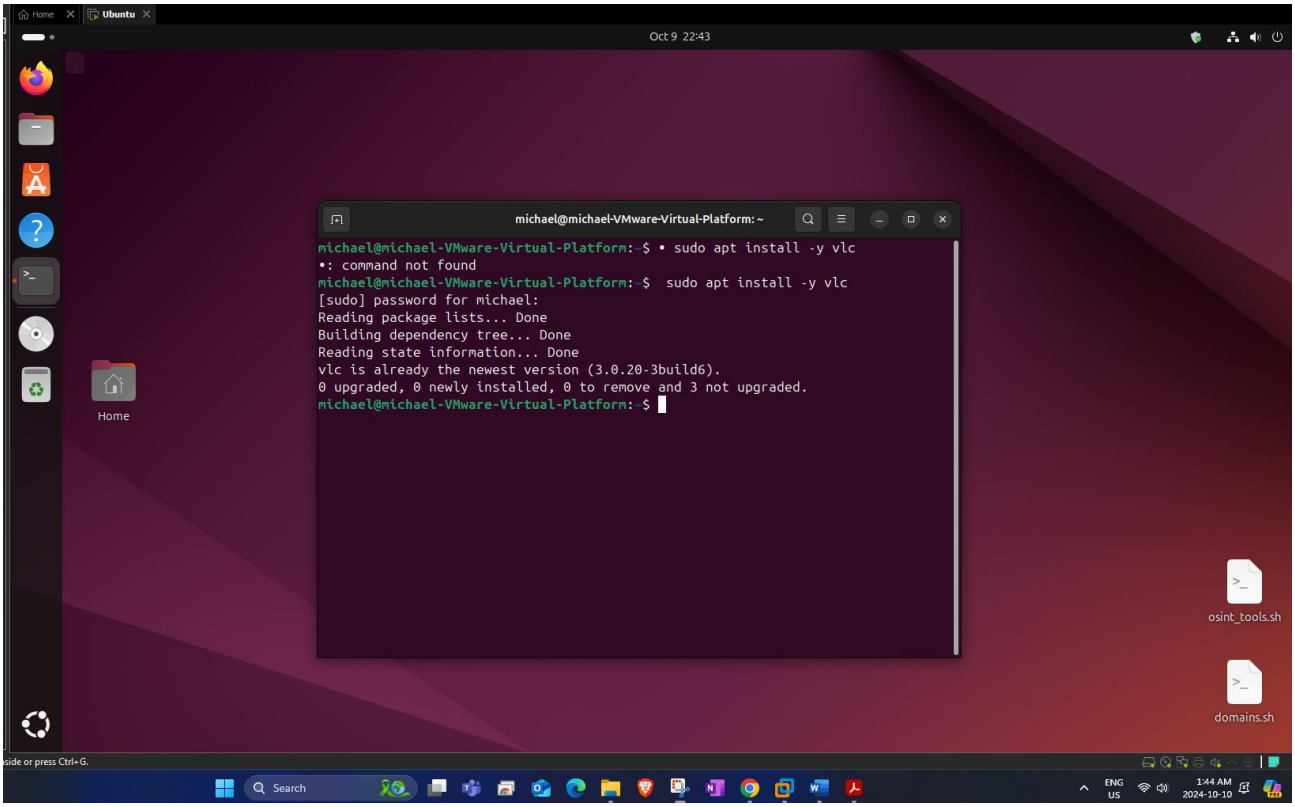

Find more add-ons
Search addons.mozilla.org
Recommendations
Extensions
Themes
Plugins
Languages
Manage Your Extensions
Bulk Media Downloader
Grab and download media (image and video) sources by monitoring network (like FlashGot)
Copy Selected Links
Right-click selected text to copy the URL of any links it contains.
DownThemAll!
The Mass Downloader for your browser
Exif Viewer
Displays the EXIF and IPTC metadata stored in JPEG files.
Firefox Multi-Account Containers
Multi-Account Containers helps you keep all the parts of your online life contained in differ...
Image Search Options
Customizable Image Search right click context options
Nimbus Screen Capture: Screenshots, Annotate
Screen Capture FULL Web page or any part. Edit screenshots. Upload to Nimbus, Slack, Goo...
OneTab
Save up to 95% memory and reduce tab clutter
Resurrect Pages
Resurrect dead pages, by finding their ghosts.
Search by Image
A powerful reverse image search tool, with support for various search engines, such as Goo...
SingleFile
Save a complete page into a single HTML file
Take Webpage Screenshots Entirely - FireShot
Take FULL webpage screenshots. Capture, edit and save them to PDF/JPEG/GIF/PNG, uploa...
Firefox Settings
Add-ons Support
or press Ctrl+G.
Search
ENG
US
1:42 AM
2024-10-10

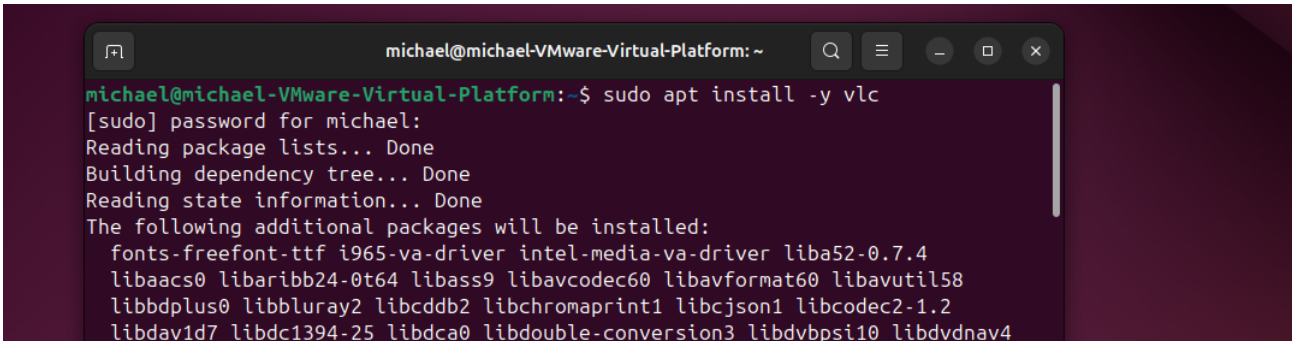


Applications for OSINT on Linux OS

VLC Media Player:

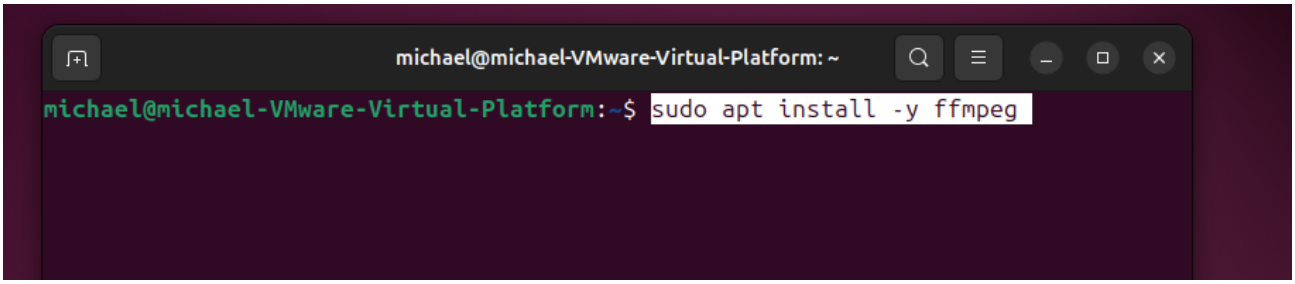
Purpose: VLC is a powerful, cross-platform multimedia player that supports a wide variety of audio and video formats, including streams, DVDs, and Blu-Rays. It's a key tool for OSINT because it can open and play almost any type of media file you may encounter during investigations.

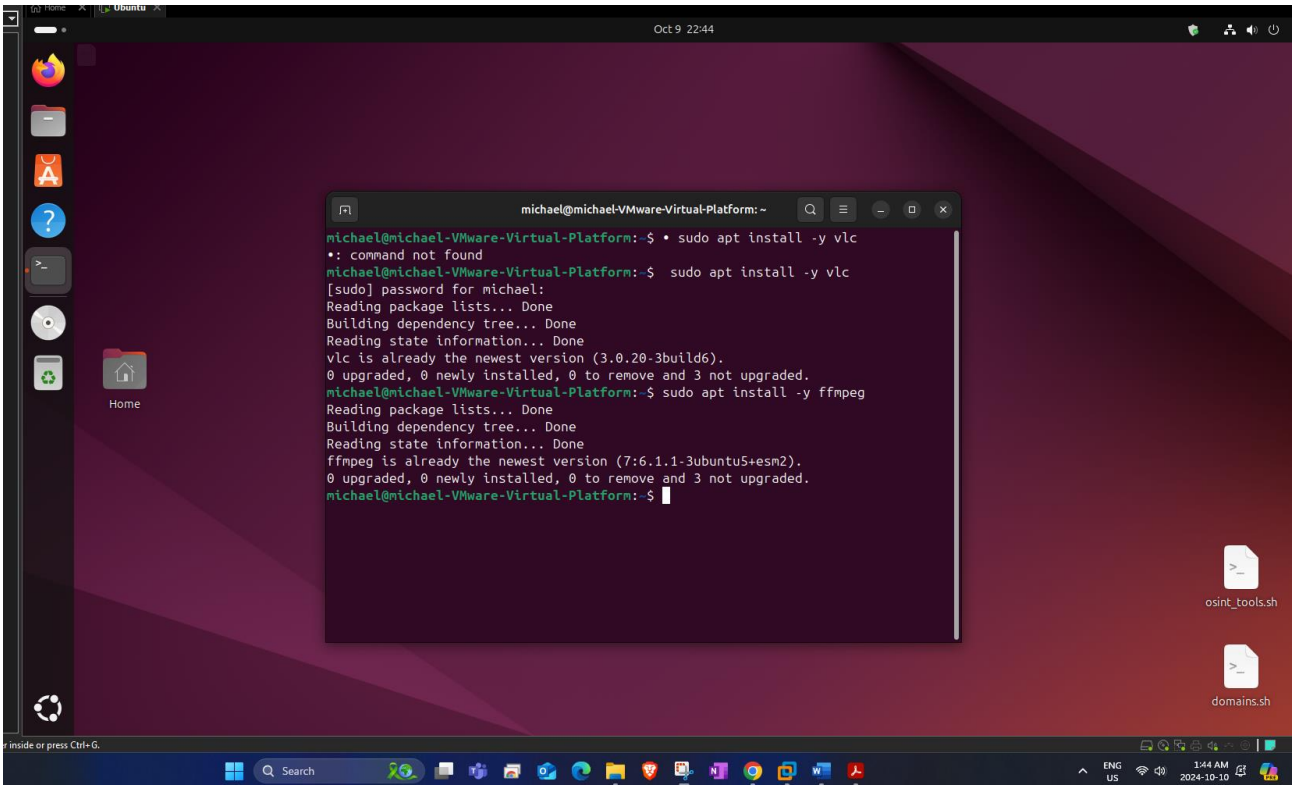




FFmpeg:

Purpose: FFmpeg is a command-line tool used to convert multimedia files between formats. It's particularly useful in OSINT when you need to manipulate, extract, or transcode video and audio files for further analysis. FFmpeg provides powerful features like converting, recording, and streaming video and audio.

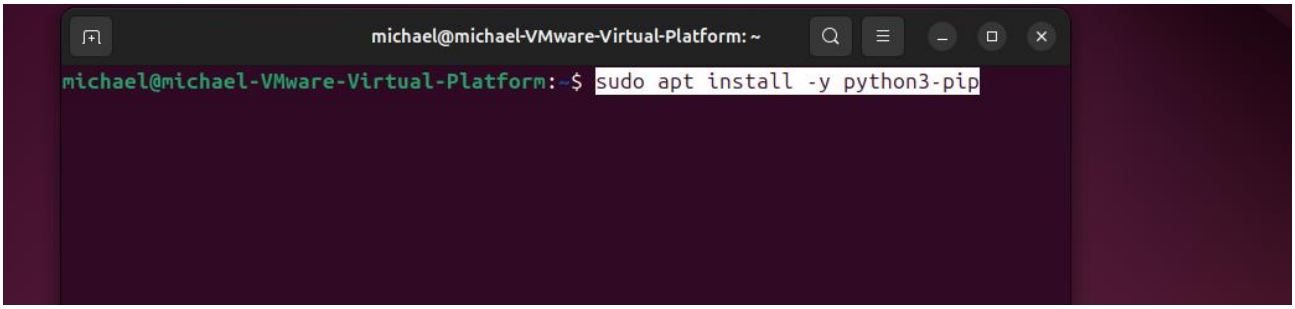


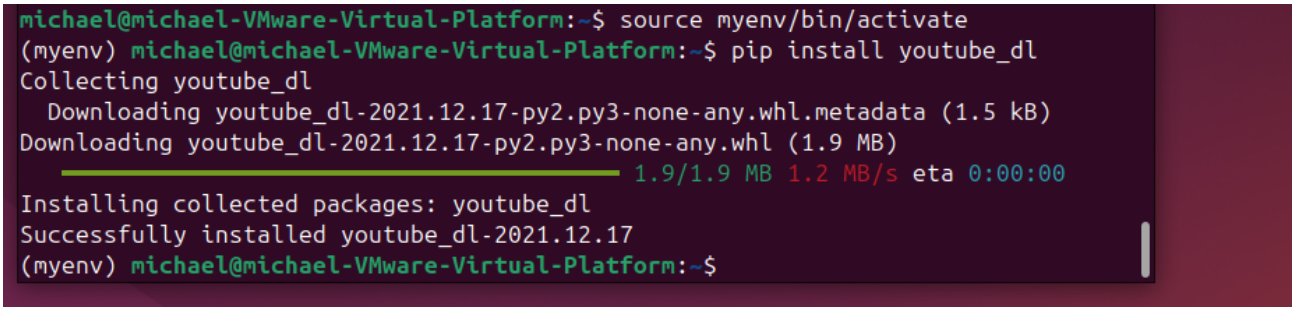


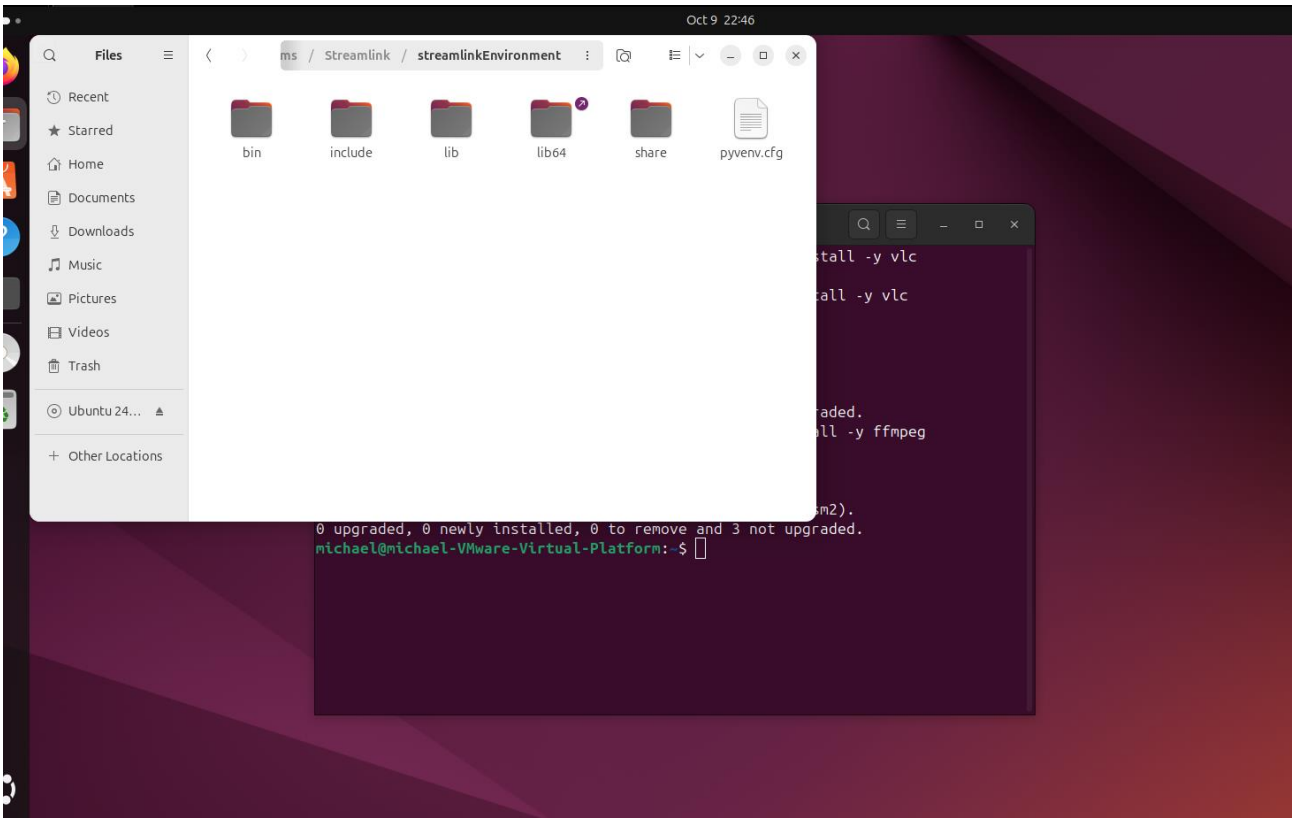
Video Download Tool:

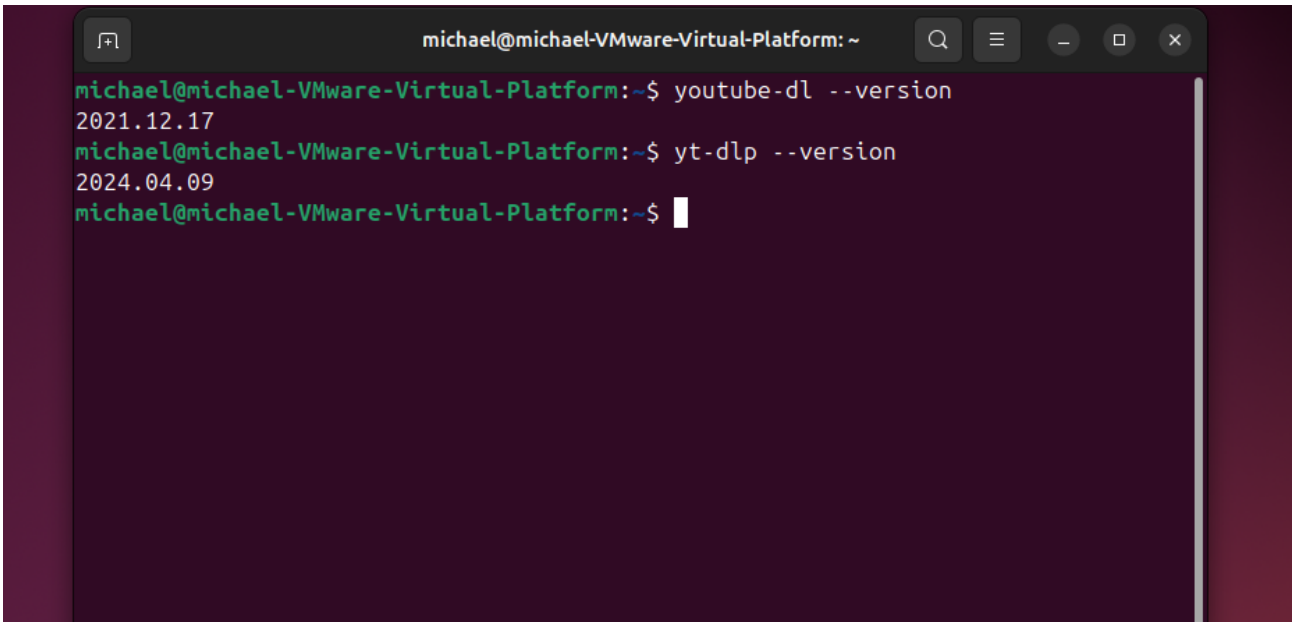
YouTube-DL

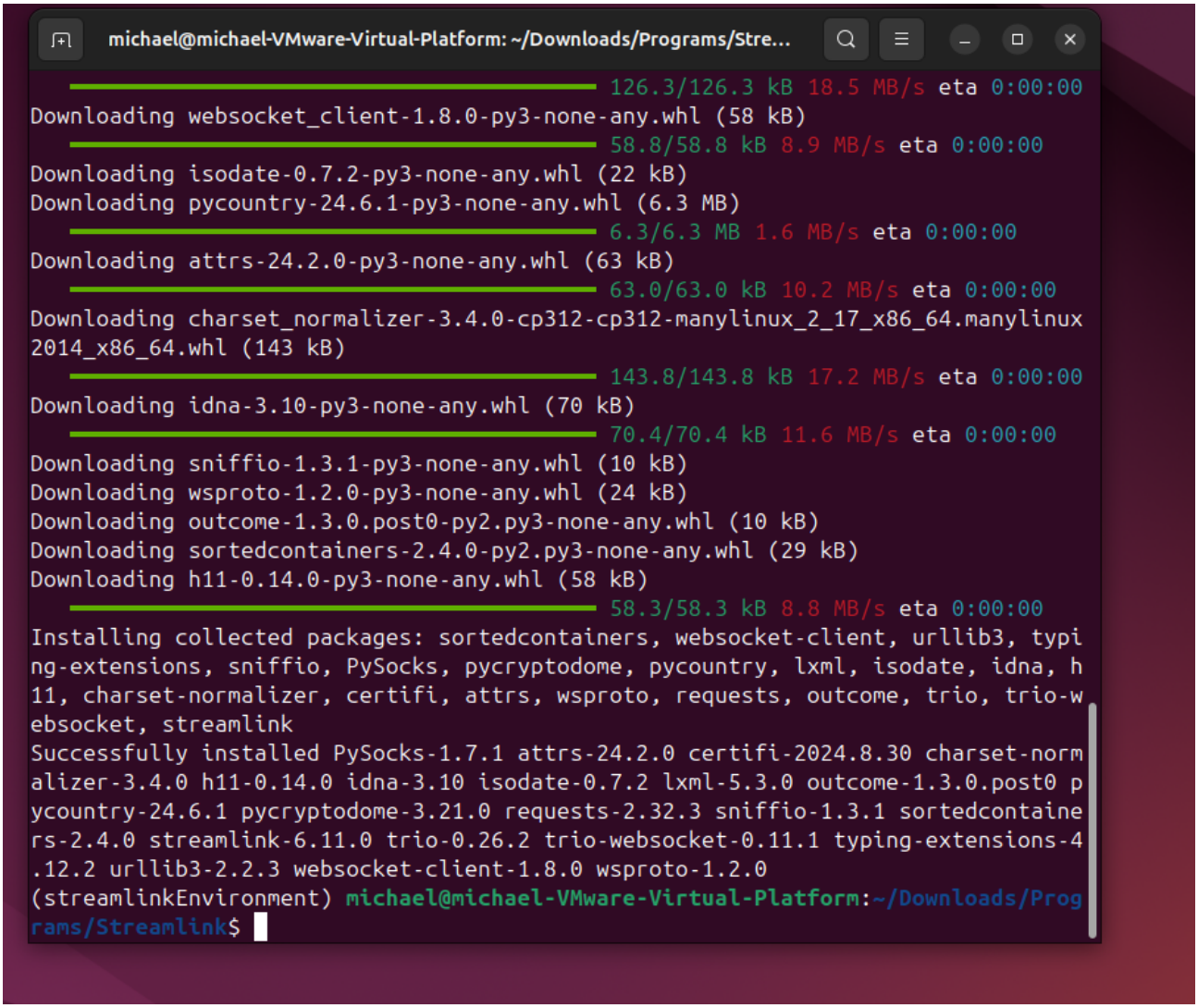
- **Purpose**: YouTube-DL is a command-line program that helps you download videos from YouTube and many other websites. It's an essential OSINT tool for downloading videos in bulk from online sources for offline analysis or archival. It is often used when you need quick and efficient video downloading.

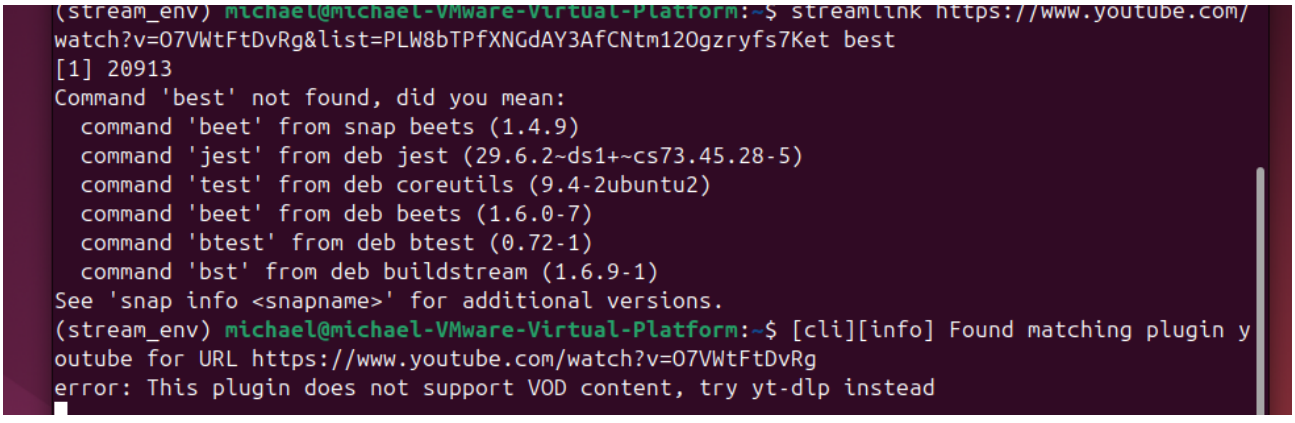

michael@michael-VMware-Virtual-Platform: ~
michael@michael-VMware-Virtual-Platform:~$ sudo apt install -y python3-pip


michael@michael-VMware-Virtual-Platform:~$ source myenv/bin/activate
(myenv) michael@michael-VMware-Virtual-Platform:~$ pip install youtube_dl
Collecting youtube_dl
Downloading youtube_dl-2021.12.17-py2.py3-none-any.whl.metadata (1.5 kB)
Downloading youtube_dl-2021.12.17-py2.py3-none-any.whl (1.9 MB)
1.9/1.9 MB 1.2 MB/s eta 0:00:00
Installing collected packages: youtube_dl
Successfully installed youtube_dl-2021.12.17
(myenv) michael@michael-VMware-Virtual-Platform:~$


Oct 9 22:46
Files
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Ubuntu 24...
Other Locations
Streamlink / streamlinkEnvironment
bin
include
lib
lib64
share
pyvenv.cfg
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
michael@michael-VMware-Virtual-Platform:~$


michael@michael-VMware-Virtual-Platform: ~
michael@michael-VMware-Virtual-Platform:~$ youtube-dl --version
2021.12.17
michael@michael-VMware-Virtual-Platform:~$ yt-dlp --version
2024.04.09
michael@michael-VMware-Virtual-Platform:~$


michael@michael-VMware-Virtual-Platform: ~/Downloads/Programs/Stre...
126.3/126.3 kB 18.5 MB/s eta 0:00:00
Downloading websocket_client-1.8.0-py3-none-any.whl (58 kB)
58.8/58.8 kB 8.9 MB/s eta 0:00:00
Downloading isodate-0.7.2-py3-none-any.whl (22 kB)
Downloading pycountry-24.6.1-py3-none-any.whl (6.3 MB)
6.3/6.3 MB 1.6 MB/s eta 0:00:00
Downloading attrs-24.2.0-py3-none-any.whl (63 kB)
63.0/63.0 kB 10.2 MB/s eta 0:00:00
Downloading charset_normalizer-3.4.0-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (143 kB)
143.8/143.8 kB 17.2 MB/s eta 0:00:00
Downloading idna-3.10-py3-none-any.whl (70 kB)
70.4/70.4 kB 11.6 MB/s eta 0:00:00
Downloading sniffio-1.3.1-py3-none-any.whl (10 kB)
Downloading wsproto-1.2.0-py3-none-any.whl (24 kB)
Downloading outcome-1.3.0.post0-py2.py3-none-any.whl (10 kB)
Downloading sortedcontainers-2.4.0-py2.py3-none-any.whl (29 kB)
Downloading h11-0.14.0-py3-none-any.whl (58 kB)
58.3/58.3 kB 8.8 MB/s eta 0:00:00
Installing collected packages: sortedcontainers, websocket-client, urllib3, typing-extensions, sniffio, PySocks, pycryptodome, pycountry, lxml, isodate, idna, h11, charset-normalizer, certifi, attrs, wsproto, requests, outcome, trio, trio-websocket, streamlink
Successfully installed PySocks-1.7.1 attrs-24.2.0 certifi-2024.8.30 charset-normalizer-3.4.0 h11-0.14.0 idna-3.10 isodate-0.7.2 lxml-5.3.0 outcome-1.3.0.post0 pycountry-24.6.1 pycryptodome-3.21.0 requests-2.32.3 sniffio-1.3.1 sortedcontainers-2.4.0 streamlink-6.11.0 trio-0.26.2 trio-websocket-0.11.1 typing-extensions-4.12.2 urllib3-2.2.3 websocket-client-1.8.0 wsproto-1.2.0
(streamlinkEnvironment) michael@michael-VMware-Virtual-Platform:~/Downloads/Programs/Streamlink$


(stream_env) michael@michael-VMware-Virtual-Platform:~$ streamlink https://www.youtube.com/watch?v=O7VWtFtDvRg&list=PLW8bTPfXNGdAY3AfCNtm12OgzryfS7Ket best
[1] 20913
Command 'best' not found, did you mean:
command 'beet' from snap beets (1.4.9)
command 'jest' from deb jest (29.6.2~ds1+~cs73.45.28-5)
command 'test' from deb coreutils (9.4-2ubuntu2)
command 'beet' from deb beets (1.6.0-7)
command 'btest' from deb btest (0.72-1)
command 'bst' from deb buildstream (1.6.9-1)
See 'snap info <snapname>' for additional versions.
(stream_env) michael@michael-VMware-Virtual-Platform:~$ [cli][info] Found matching plugin youtube for URL https://www.youtube.com/watch?v=O7VWtFtDvRg
error: This plugin does not support VOD content, try yt-dlp instead