Unit 29, Assignment 2

Plan & Implement an Installation and Upgrade

George Hotten

April 25, 2023

Planning the Upgrade

To ensure a smooth upgrade, I have put together the following plan for the upgrading to Open Office within the school. To further support the learning and security of the school's computers, I will install Blender and Avast Free Antivirus.

Activities

The following activities will take place during the upgrade:

- Perform a network-wide file backup
- Ensure data integrity: hashing user files and checking system files
- Create a system restore point
- Update the operating system to its latest version
- Install Avast Free Antivirus
- Install Open Office
- Install Blender

Materials

To speed up the upgrade, all installation files for Avast, Open Office and Blender will be put onto a USB stick, removing the need of trying to find the download link for each software for every computer. Optionally, for larger networks, the installers could be put on a network share. This would cut down costs on USB sticks and would allow a quicker upgrade.

Timings

The estimated time for each computer to upgrade should be no more than 30 minutes. The operating system upgrade should take no longer than 15-20 minutes. Whilst the final three applications should take no longer than 10 minutes.

Communications

Ideally, users should be warned of the upgrade with no less than 2 weeks of notice. Users should be informed on exactly what is changing on the systems and they should be provided with the proper training to understand how to use the new programs.

School management should be consulted before picking a time to complete the upgrade to ensure there is no clashing of events. A time should be picked where there will be as little disruption as possible. In our case, the upgrade should happen outside of school hours, such as on a Friday evening or over half-term.

Gaining Permission and Access

Once permission has been granted from the school's management, access to the school buildings and machines should be setup. This could have to include having a key-holder present on the day, able to give the technicians access to the building.

Back-out Procedures

NB: This aims to cover P3 and M4.

In the event of a failed upgrade, there is a high risk of data being corrupted or lost. Because of this, it is vital a proper plan is put in place to enable the technicians to restore a system to its previous state before the upgrade.

To begin, a full backup of user data should be taken. If user data is stored on a different drive to the operating system and applications, this should be unplugged, and a backup would be optional. A system restore point should also be taken to ensure that the operating system is able to be restored in the event of corruption.

If the upgrade fails, the situation should first be assessed. You should check the state of the system: can it boot into Windows, can you perform general tasks such as creating files and folder, and can you browse the web? If you can't, the operating system is corrupted. To resolve this, try booting into Windows recovery by power cycling the system three times. From there, the restore point can be selected and Windows will attempt to restore to it. If that fails, Windows will have to be re-installed. If you cannot get into Windows recovery, boot from a Windows installer USB stick, select recovery and select restore point.

Once the operating system has been checked and restored, user data should be inspected. If there are missing or corrupted files, the backup taken must be restored. This can often be done by directly copying the files back to the system drive, or programs such as Macrium Reflect can be used.

Required Hardware and Software

To ensure the technicians are able to complete the upgrade inline with the above plan, the following hardware and software are needed.

Hardware

The following hardware would be required to perform the upgrade:

- The appropriate peripherals - mouse, keyboard and monitor, allowing the technicians can perform the upgrade.
- A link to the internet - preferably via a CAT-6 cable.
- USB sticks - required to contain the installation files for the new software to be installed.
- Storage - such as an HDD or SSD to back up user files and system files.
- Storage Server - instead of individual drives, a storage server could be used to storage backups to. The server would contain numerous drives in a RAID array.

Software

The following software would be required to perform the upgrade:

- Installation files - for Open Office, Blender and Avast Free Antivirus.
- A file backup applications - used to back up user files or system files to an external location, such as Macrium Reflect or Synology Drive.
- Modern operating system - modern applications required a modern OS, such as Windows 10, to run.

Handover: User Acceptance

To ensure the school's management are happy with the proposed upgraded, an individual machine should be upgraded first and presented to the management. This gives the management time to check the new software and verify that they are happy with it. It would also be suitable to create and provide training on the new software so that the management can relay it to the other users who will need to use it.

After having the finished upgrade reviewed, any feedback should be taken onboard and the upgrade should be repeated with the changes and presented to management. This cycle would repeat until they are 100% happy with the upgrade.

Now management have approved the changes, the rollout can begin for the upgrade. A small handful should be completed at first, and checked by management for quality control. Once they are happy, the rest can be completed. Finally, once all the machines have been upgraded, management will check to ensure they are happy with the upgrade. If they are happy, training for the new software and features should be created and given to all the users so that they can feel confident in using the new software.

Ensuring Data Integrity

What is data integrity? Data integrity refers to the accuracy and reliability of data, during all stages of its life: creation, transport and at rest. Data integrity ensures data has not been tampered with or corrupted. This can often be caused by general communication issues or a bad actor could tamper with data.

Within industries such as Healthcare, data integrity is vital to its operations. For smooth and safe operation, all data must retain its integrity. For example if dosage amounts were tampered with or got corrupted, it could be fatal to patients as the wrong amount of medicine would be given.

How can it be implemented?

There are many ways data integrity can be implemented, some examples include hashing, encryption and data validation rules.

Hashing This method of data integrity uses an algorithm such as MD5 or SHA-256. This turns data into a string of characters that can only be created from the exact data inputted. If one character changes, the whole output changes. A hash can be taken before data is transported and the receiving device can check the received data to see if its hash matches.

Encryption This method also uses an algorithm to ensure data integrity. Examples include AES and Public-key encryption. Public-key encryption generates two random keys: a public and a private key. The public key is used to encrypt data and the private key is used to decrypt. If the recipient generates two keys and provides their public key, the sender will be able to encrypt data, send it and then only the recipient can decrypt it. This ensures that data cannot be tampered with as the attacker will not be able to read or modify the encrypted data.

Data Validation Rules This method ensures that all data inputted into a system meets a set of rules. For the dosage example, there would be checks to ensure that data does not exceed certain thresholds. This means that this data could only be inputted if it is in between a range two amounts.

Ensuring Data Integrity during the Upgrade

To ensure data integrity during an upgrade, a hash should be taken of all user data. This should be stored safely during the upgrade and once it is complete, another hash should be taken and compared against the previous hash. If it is different, the data may have been corrupted and should be restored from a backup. To take a hash, the following powershell commands can be used:

```
1. $HashString = (Get-ChildItem H:\Yourdata -Recurse | Get-FileHash
   -Algorithm MD5).Hash | Out-String
2. Get-FileHash -InputStream ([IO.MemoryStream]::new([char[]]$HashString))
```

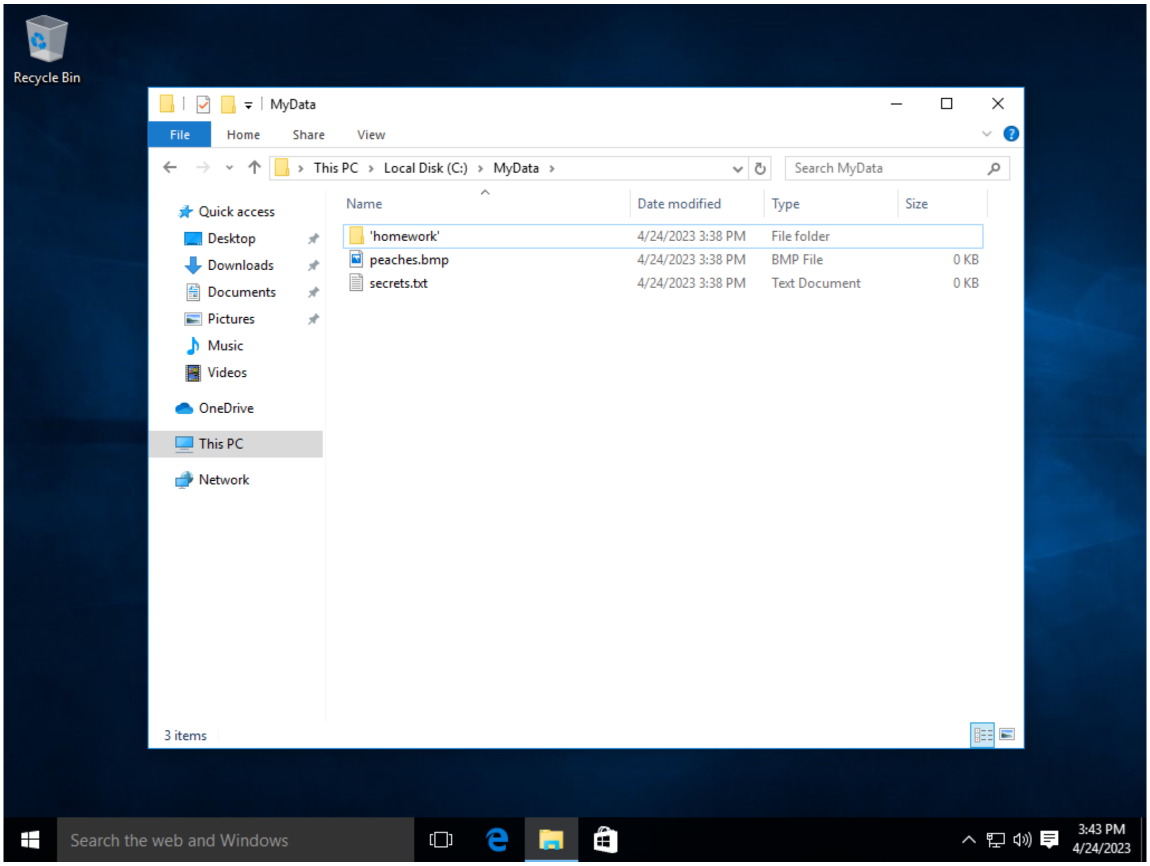
The first command gets all the files within the `H:\Yourdata` directory and creates an MD5 hash of each file. This is then added to the `HashString` variable. The second command then hashes the list of hashes from the `HashString` variable, using SHA256, and prints it to the console.

For system files, the following command should be ran before and after the upgrade to ensure all system files have their integrity: `DISM.exe /Online /Cleanup-image /Restorehealth`. This command checks and repairs any issues with the integrity of system files.

Installing the Upgrade

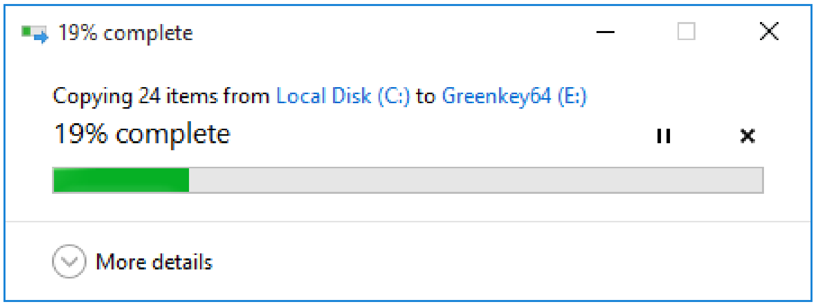
Stage 1: Backing-up user files

On the system I will be upgrading, user data is located inside `C:\MyData`. For this backup as the user doesn't have much data, I will be backing it up to a USB drive with a simple-copy and paste.



Name	Date modified	Type	Size
'homework'	4/24/2023 3:38 PM	File folder	
peaches.bmp	4/24/2023 3:38 PM	BMP File	0 KB
secrets.txt	4/24/2023 3:38 PM	Text Document	0 KB

Figure 1: User data to be backed-up.



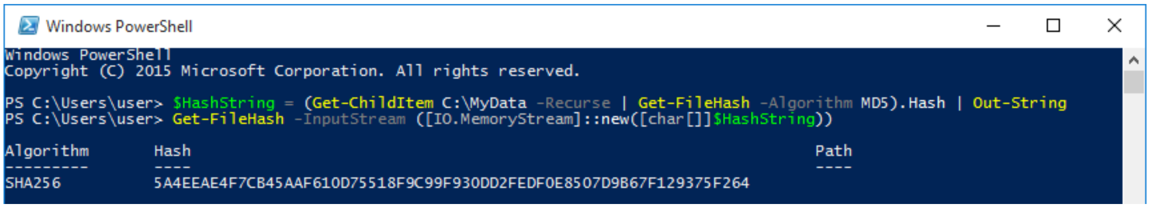
Copying 24 items from Local Disk (C:) to Greenkey64 (E:)

19% complete

Figure 2: Backing-up user data.

Stage 2: Ensuring Data Integrity

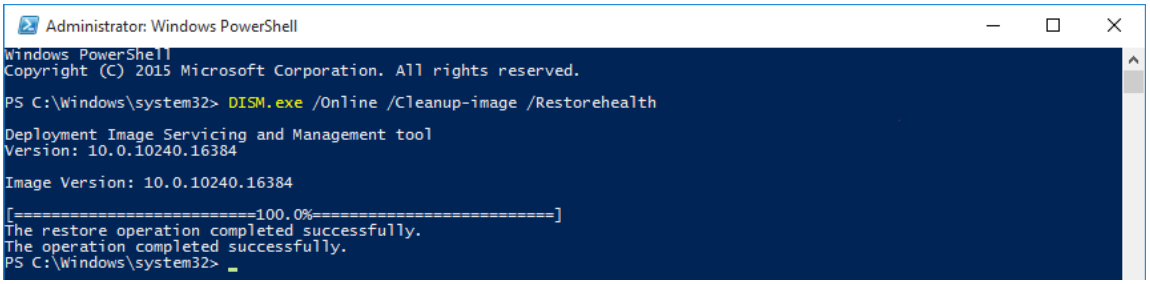
To ensure data integrity, I will create a hash of all user data.



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\user> $HashString = (Get-ChildItem C:\MyData -Recurse | Get-FileHash -Algorithm MD5).Hash | Out-String
PS C:\Users\user> Get-FileHash -InputStream ([IO.MemoryStream]::new([char[]]$HashString))

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          5A4EEAE4F7CB45AAF610D75518F9C99F930DD2FEDF0E8507D9B67F129375F264
```

Figure 3: Creating a hash of user data.

Now I have the hash, I will store it for later use after the backup. With user data hashed, I will now check the integrity of system files.

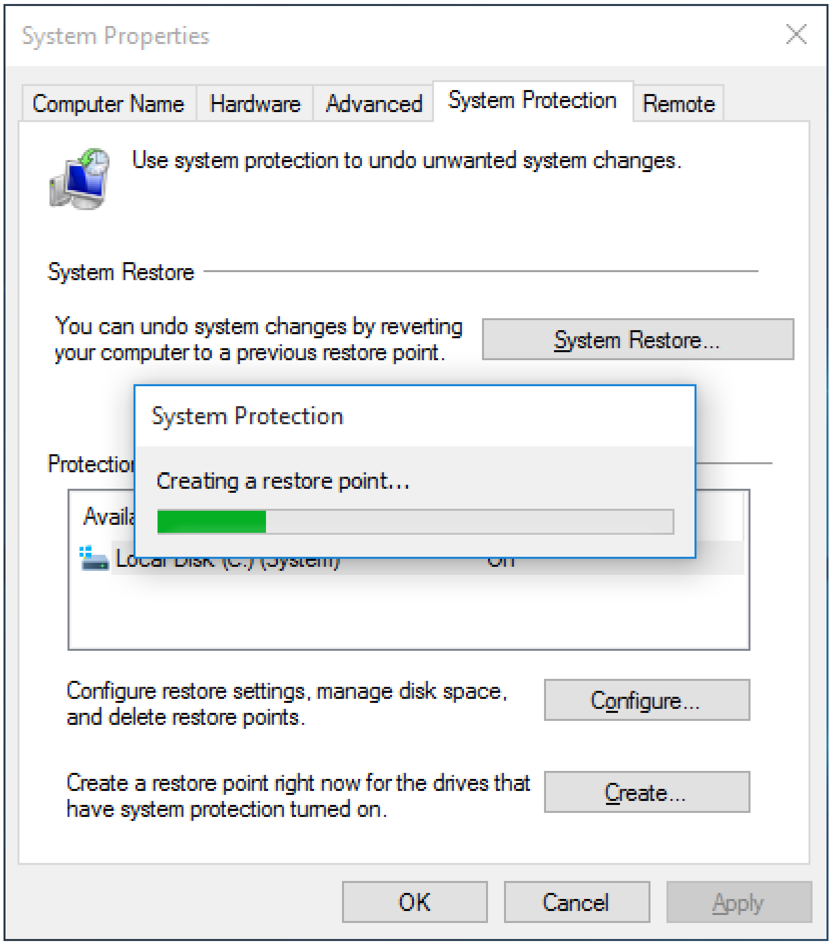


```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> DISM.exe /Online /Cleanup-image /Restorehealth

Deployment Image Servicing and Management tool
Version: 10.0.10240.16384

Image Version: 10.0.10240.16384

[==========================100.0%==========================]
The restore operation completed successfully.
The operation completed successfully.
PS C:\Windows\system32> _
```

Figure 4: Checking the integrity of system files.

Stage 3: Creating a System Restore Point

In the event of the operating system getting corrupted, I will create a system restore point to restore to if disaster strikes.



Use system protection to undo unwanted system changes.

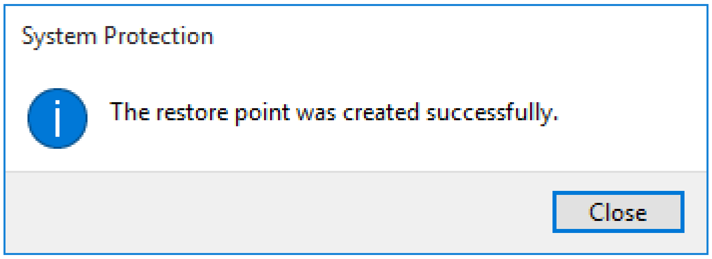
You can undo system changes by reverting your computer to a previous restore point.

Creating a restore point...

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

Figure 5: Creating a system restore point.

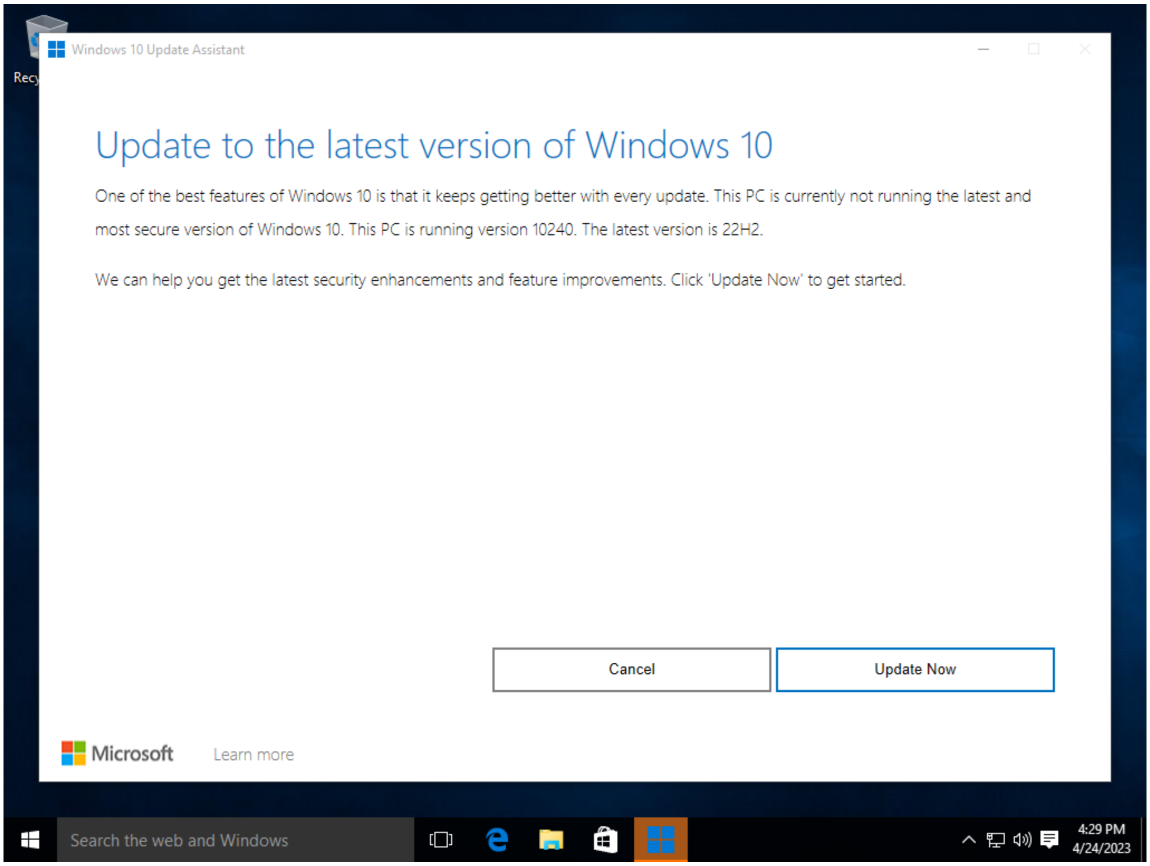


The restore point was created successfully.

Figure 6: Restore point successfully created.

Stage 4: Updating the Operating System

For the best performance and security, software creates request that users run the latest version of Windows. This helps keep the application running smoothly and helps reduces any vulnerabilities that could be exploited. I will start a Windows update using the Windows 10 Update Assistant to update my machine onto the latest version

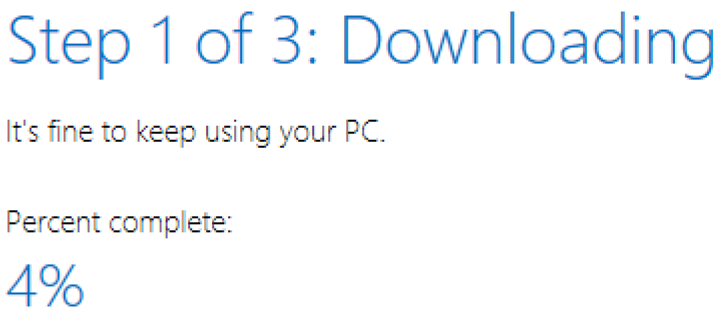


Update to the latest version of Windows 10

One of the best features of Windows 10 is that it keeps getting better with every update. This PC is currently not running the latest and most secure version of Windows 10. This PC is running version 10240. The latest version is 22H2.

We can help you get the latest security enhancements and feature improvements. Click 'Update Now' to get started.

Figure 7: The Windows 10 Update Assistant.



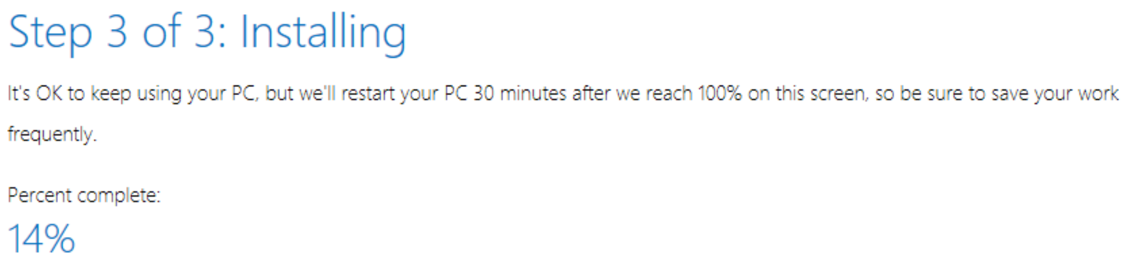
Step 1 of 3: Downloading

It's fine to keep using your PC.

Percent complete:

4%

Figure 8: Downloading the update.



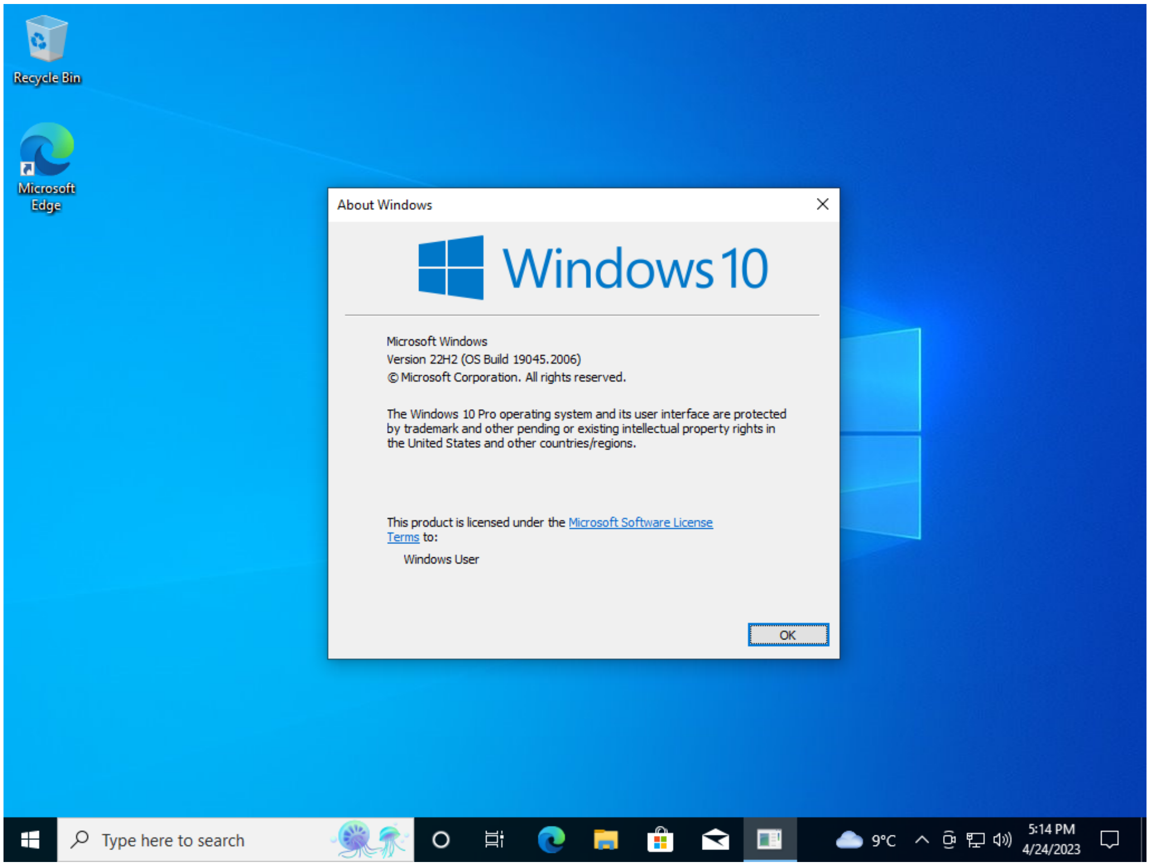
Step 3 of 3: Installing

It's OK to keep using your PC, but we'll restart your PC 30 minutes after we reach 100% on this screen, so be sure to save your work frequently.

Percent complete:

14%

Figure 9: Installing the update.



About Windows

Windows 10

Microsoft Windows
Version 22H2 (OS Build 19045.2006)
© Microsoft Corporation. All rights reserved.

The Windows 10 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

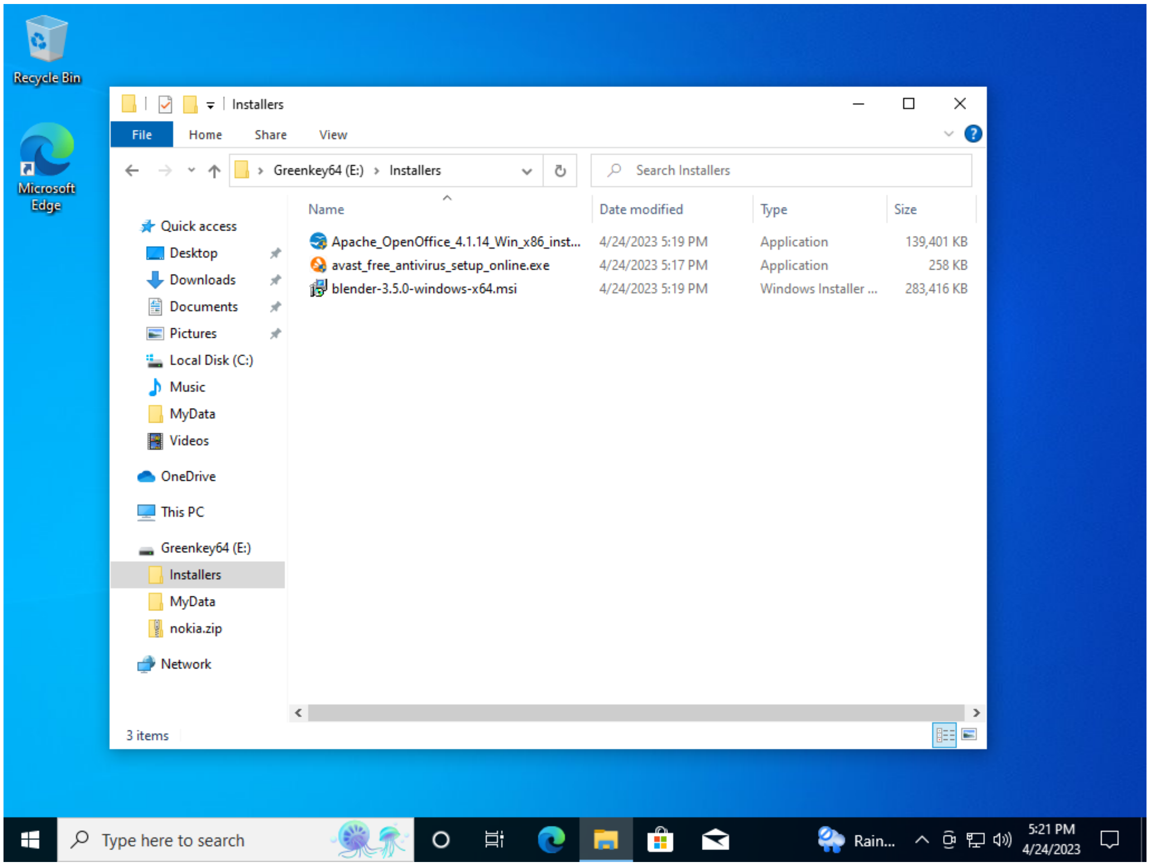
Windows User

Figure 10: winver.exe showing our OS version.

The update is now complete and we are running the latest version of Windows 10: 22H2.

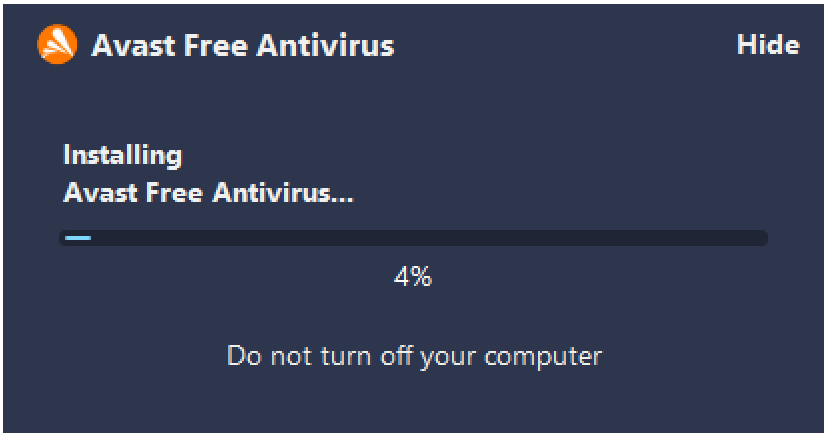
Stage 5: Installing the Software

With the operating system at its latest version, I will now install Avast Free Antivirus, Blender and Open Office. I have the installers downloaded to a USB stick as set out in the installation plan.



Name	Date modified	Type	Size
Apache_OpenOffice_4.1.14_Win_x86_inst...	4/24/2023 5:19 PM	Application	139,401 KB
avast_free_antivirus_setup_online.exe	4/24/2023 5:17 PM	Application	258 KB
blender-3.5.0-windows-x64.msi	4/24/2023 5:19 PM	Windows Installer ...	283,416 KB

Figure 11: File Explorer showing the software installation files.

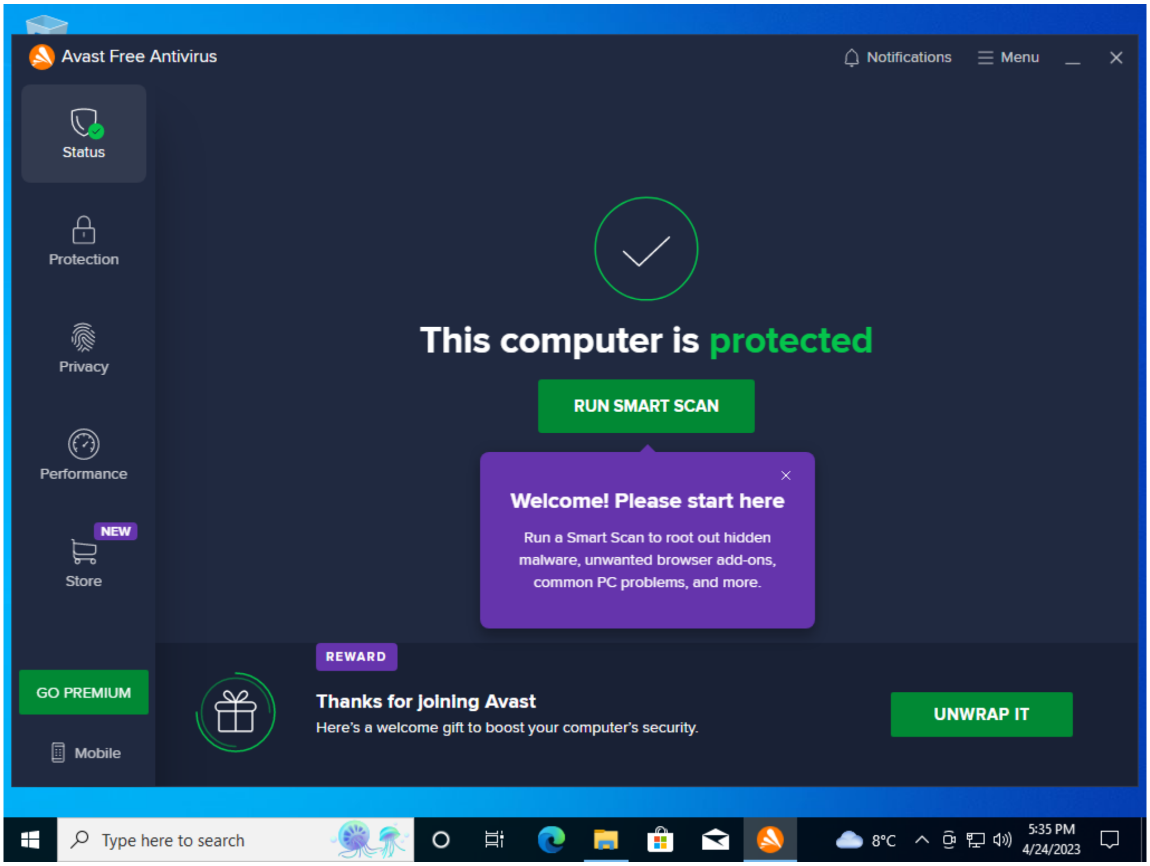


Installing
Avast Free Antivirus...

4%

Do not turn off your computer

Figure 12: The Avast Free Antivirus installer.



This computer is protected

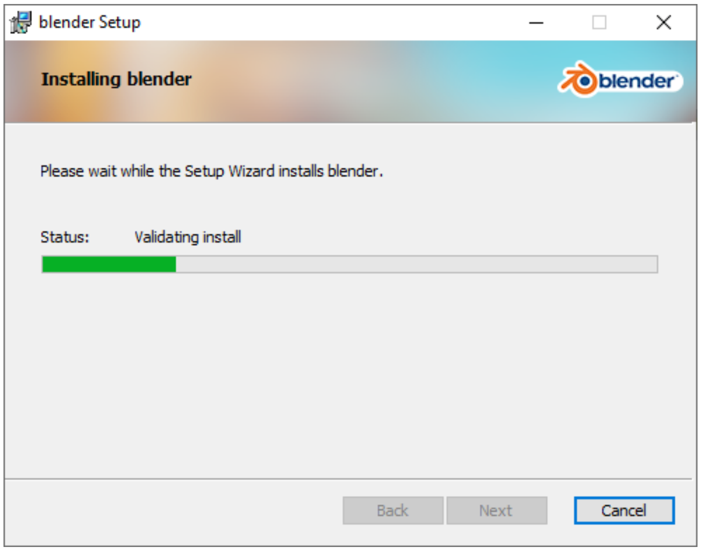
Welcome! Please start here

Run a Smart Scan to root out hidden malware, unwanted browser add-ons, common PC problems, and more.

Thanks for joining Avast

Here's a welcome gift to boost your computer's security.

Figure 13: Avast Free Antivirus has installed successfully.



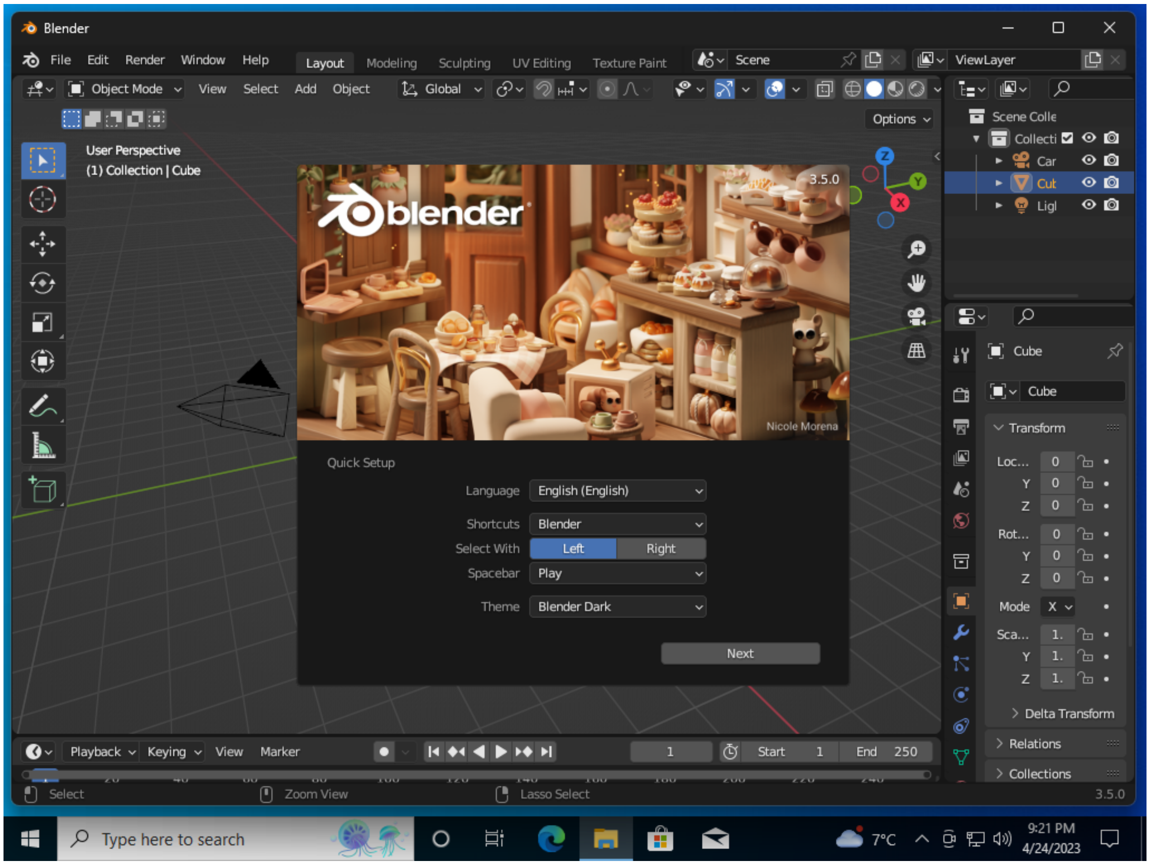
blender Setup

Installing blender

Please wait while the Setup Wizard installs blender.

Status: Validating install

Figure 14: The Blender installer.



Quick Setup

Language: English (English)

Shortcuts: Blender

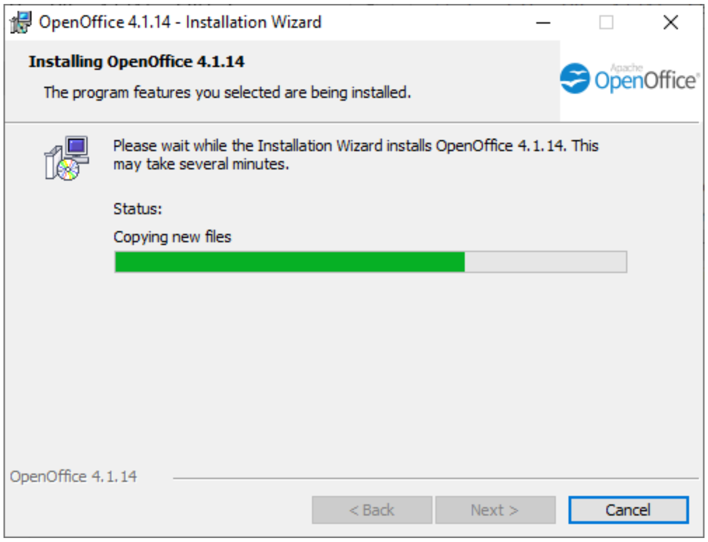
Select With: Left | Right

Spacebar: Play

Theme: Blender Dark

Next

Figure 15: Blender has installed successfully.


OpenOffice 4.1.14 - Installation Wizard

Installing OpenOffice 4.1.14

The program features you selected are being installed.

Please wait while the Installation Wizard installs OpenOffice 4.1.14. This may take several minutes.

Status:

Copying new files

OpenOffice 4.1.14

Figure 16: The Open Office installer.

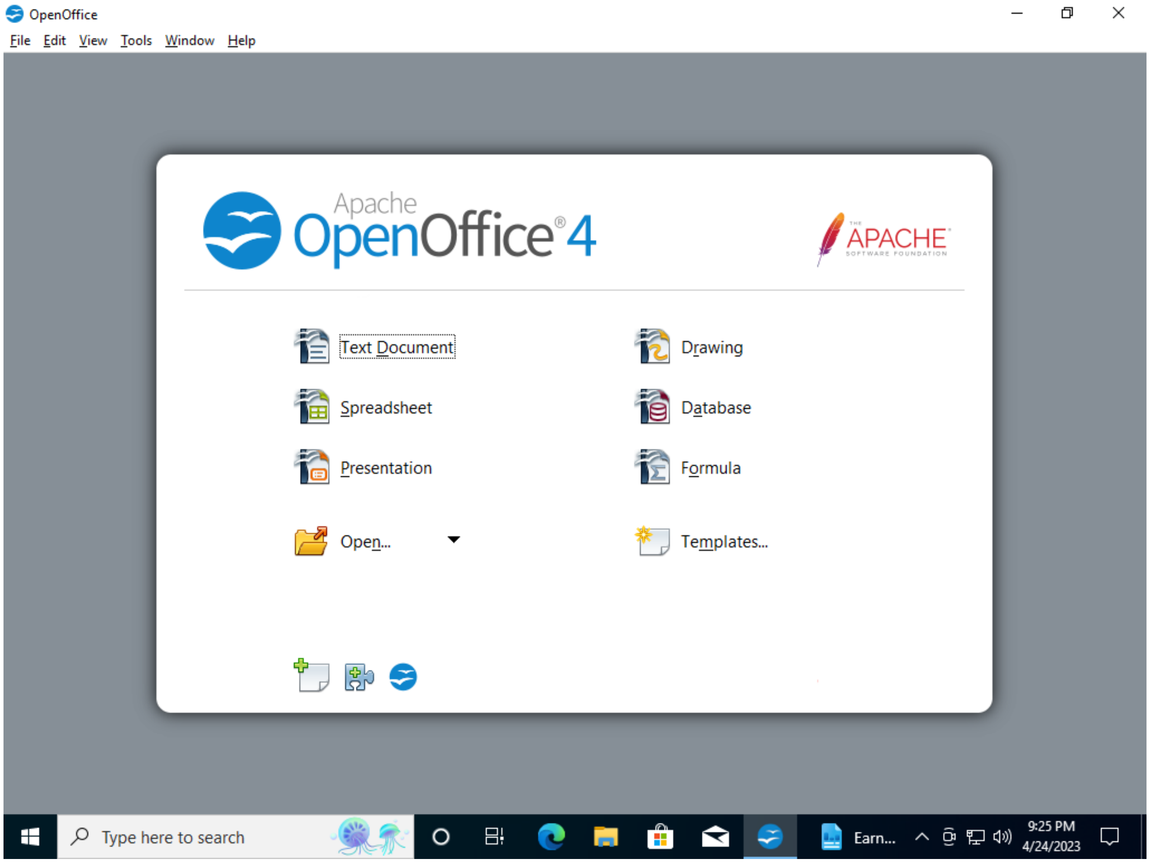


Figure 17: Open Office has installed successfully.

The installation of the required software has been completed.

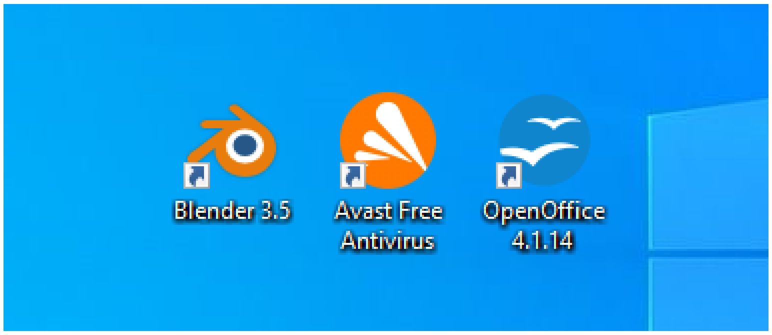
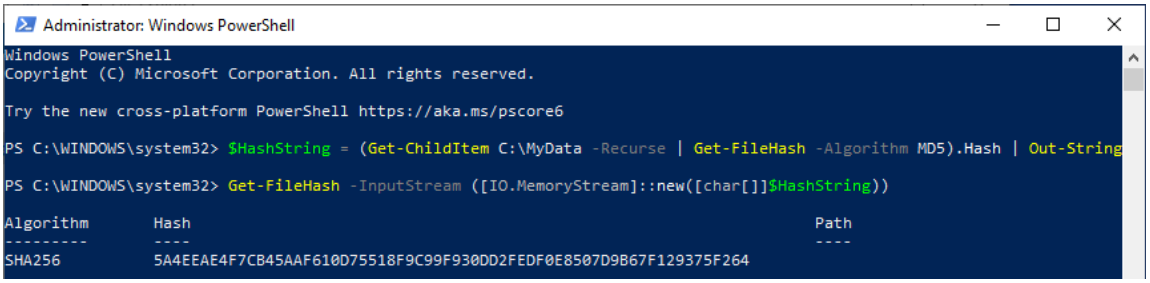


Figure 18: Shortcuts for Blender, Avast and Open Office.

Stage 6: Verifying Data Integrity

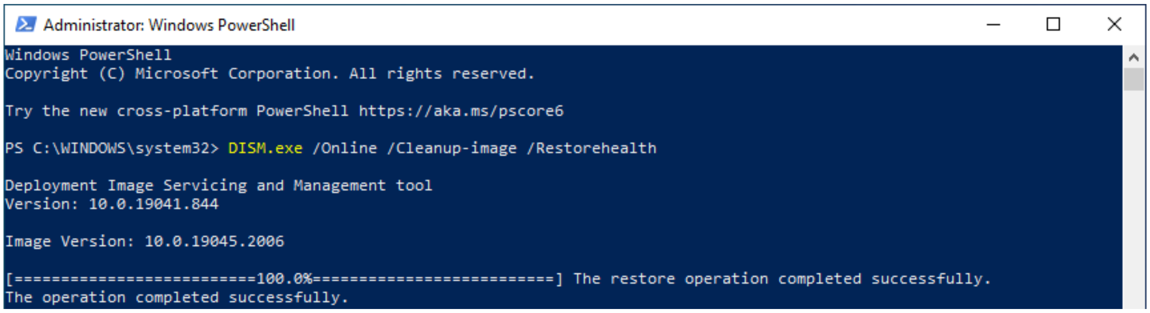
Finally, we must verify the integrity of user data and system files. Using the same commands as above, I will verify the integrity of `C:\MyData`.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> $HashString = (Get-ChildItem C:\MyData -Recurse | Get-FileHash -Algorithm MD5).Hash | Out-String

PS C:\WINDOWS\system32> Get-FileHash -InputStream ([IO.MemoryStream]::new([char[]]$HashString))

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          5A4EEAE4F7CB45AAF610D75518F9C99F930DD2FEDF0E8507D9B67F129375F264
```

Figure 19: Creating a hash of user data after the upgrade.

Our hash matches the hash generated before the upgrading, meaning our data has not been accidentally modified or corrupted.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> DISM.exe /Online /Cleanup-image /Restorehealth

Deployment Image Servicing and Management tool
Version: 10.0.19041.844

Image Version: 10.0.19045.2006

[==========================100.0%==========================] The restore operation completed successfully.
The operation completed successfully.
```

Figure 20: Checking the integrity of system files after the upgrade.

This verifies that our system files are intact, completing our upgrade.