Kickstart Cymru Digital Preservation Bundles

Ingest Workflow Guidance

Version 2

July 2023

LLGC NLW LLYFRGELL GENEDLAETHOL CYMRU THE NATIONAL LIBRARY OF WALES

Summary

This guidance document outlines a digital preservation ingest workflow suggested for use with the workstations supplied through the Kickstart Cymru project. It outlines how the hardware and software provided can be used to perform basic tasks in the accessioning of digital records, including:

- Ingesting digital records from external physical storage media
- Running anti-virus software
- Creating checksums
- Format identification and validation
- Saving the records to an external storage device
- Creating and storing metadata to document the steps you have taken

The steps in this guidance document complement the workflow introduced in the National Library of Wales' 'Saving the Bits' training programme.[1] Accompanying videos, PowerPoint presentations and further documentation are available on the Archives Wales **Saving the Bits staff toolkit**: https://archives.wales/staff-toolkit/saving-the-bits-programme/

It is recommended that you use the videos together with this document.

Accompanying guidance on how the steps in this workflow map to digital preservation self-assessment using the DPC's Rapid Assessment Model (DPC RAM) and the NDSA Levels of Digital Preservation will be circulated separately.[2]

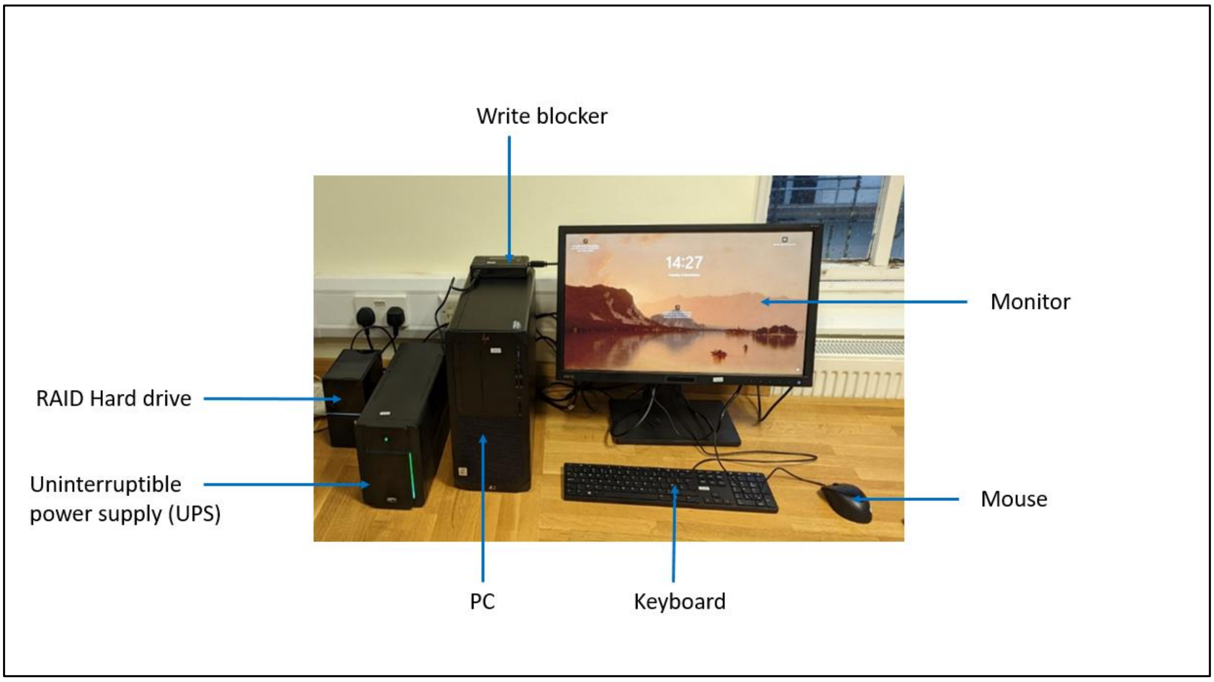
The Kickstart Cymru bundles and accompanying guidance have been supported and funded by Welsh Government.

[1] The workflow includes some adaptations to accommodate changes in the availability of software tools since the Saving the Bits Programme was run. For example, AVP's Fixity which was recommended for performing fixity checks is now only available through a paid subscription: https://www.weareavp.com/fixity-pro-release-2020/?__hstc=156770468.5e22c6233002329a133fc349f5a233d9.1672656443066.1672656443066.1672656443066.1&__hssc=156770468.1.1672656443067&__hsfp=2828332932

[2] NDSA Levels of Digital Preservation: https://ndsa.org/publications/levels-of-digital-preservation/
DPC Rapid Assessment model: https://www.dpconline.org/digipres/dpc-ram

Kickstart Cymru bundle contents

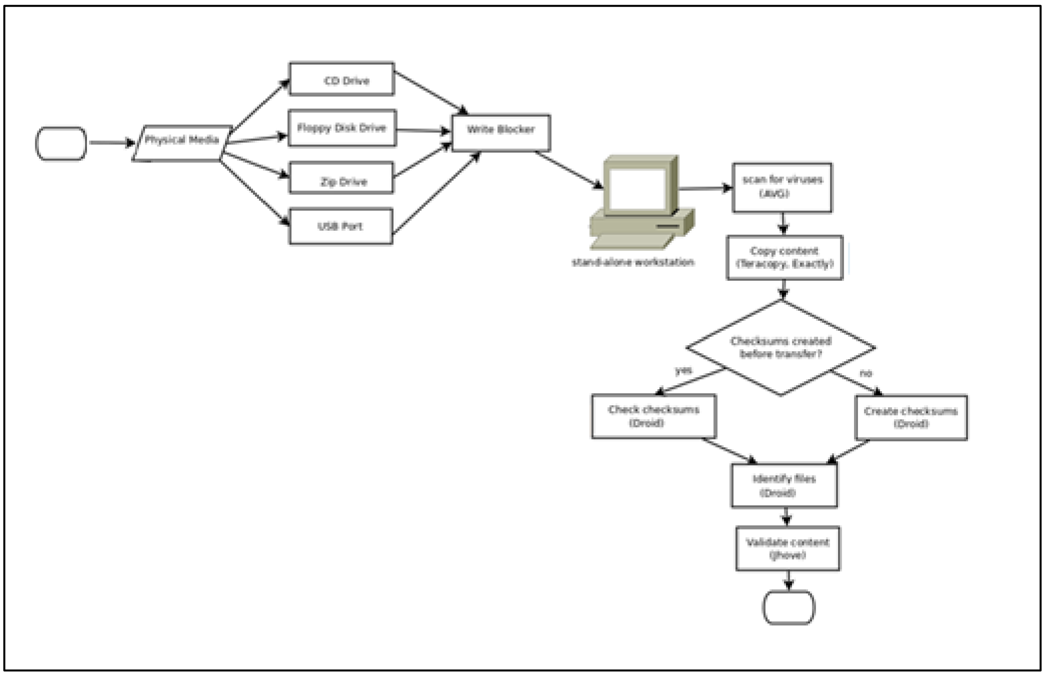
The image below shows the items of hardware supplied with the Kickstart Cymru bundles.



A diagram of how the cables for the bundle fit together is provided on page 30. This may be helpful if you need to move the workstation.

Workflow overview

The figure below shows a diagram adapted from the original Saving the Bits workflow and outlines the key steps in this process.



In addition to the steps outlined above, the guidance also covers the preliminary steps of setting up folders (or ‘directories’) for the transfer and temporary storage of both data and metadata as part of the ingest process, keeping software up to date, and transferring the records to an external hard disk drive together with their associated metadata.

The main example used in this guidance focuses on the ingest of digital records via the USB write blocker, which could include files deposited on a USB stick or USB-connected device such as an external CD/DVD drive, or floppy disc drive.

It is important that the drives are not password protected or encrypted as this will prevent access to the data.

An example of how you could use the workstation to perform online ingest of records deposited via email or another web-based transfer method is included at the end of this document, though the workstation is primarily intended for offline ingest.

As the workflow focuses on the ingest of records, subsequent preservation actions such as regular fixity and integrity checking, format migration, and providing access to the records are not covered in detail in this guidance. However, there are some suggestions for how to approach these tasks towards the end of the document.

Step 1 Switching on

The Uninterruptable Power Supply (UPS) should be the first item you turn on, and the last to be switched off, as it will supply power to all workstation items including the PC and Monitor. If the UPS is working correctly, it should make a loud sound and a green light will appear. Once the UPS is switched on, you can turn on everything else. The UPS should remain on while you are working on the workstation. Once work is completed, switch off the PC, Monitor etc., and finally the UPS. This will save energy.

Note: The UPS gets hot during use so avoid putting items on top of it.

Step 2 Create working folders on the PC

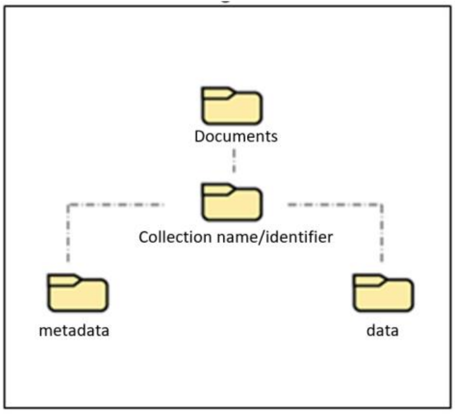
2.1 Before you begin the process of transferring digital records to your workstation, it is a good idea to create the folders (also known as 'directories') where you will be transferring the records. In accordance with the *Saving the Bits Workflow,* it is recommended that these directories consist of:

- A high-level folder which includes, e.g. the name of the digital collection or records (include a unique ID if possible) is to be transferred.
- Two subfolders containing:

i. A 'data' folder which will include folders for the digital records themselves (i.e. the content of digital records to be transferred).

ii. A 'metadata' folder which will include an exact copy of the metadata which can be saved and accessed separately.

Towards the end of the ingest process, it will be recommended that you create a copy of the metadata folder which can be stored and accessed separately (see Step 10: Managing Your Desktop Files).



In the above example the folders are saved within the 'Documents' directory on the PC, but you could choose to save this elsewhere, such as in (C:) drive or on your Desktop if you will only be storing the files temporarily prior to transfer to your external hard drive.

2.2 If you received or created any documentation which may serve as useful administrative/preservation metadata (e.g. a completed standard depositor/accession form) upon acquisition of the files, it is recommended that you save a copy of this to the 'metadata' folder.

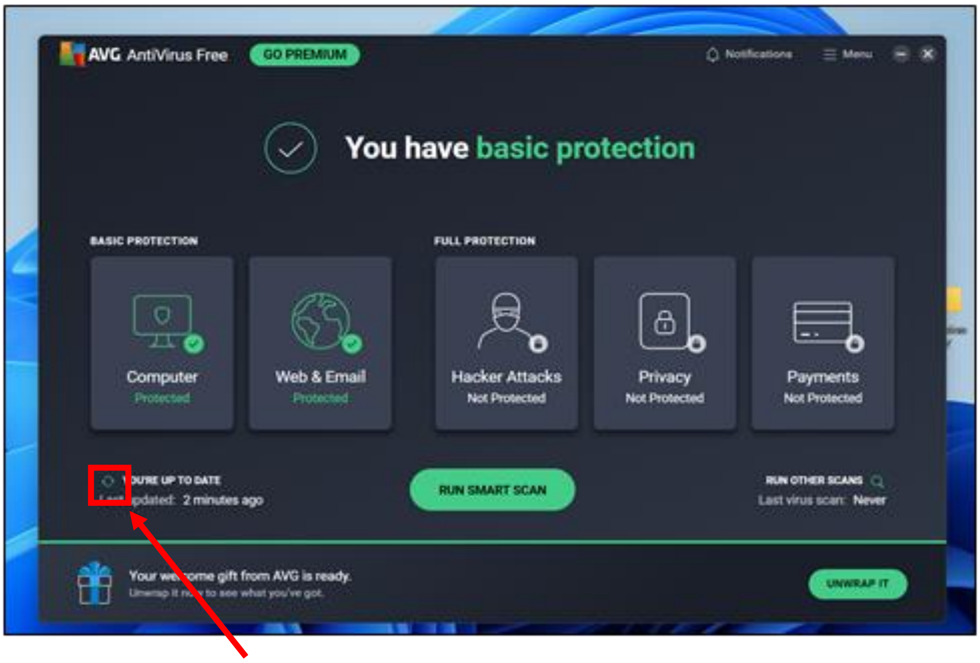
If you do not have a form for depositors to fill out upon accessioning digital records, an example of the Digital Material Transfer Form used by the National Library of Wales may serve as a useful template and is available on the *Saving the Bits* staff toolkit.[3].

Step 3 Update your virus definitions

If you do not perform regular software updates it is recommended, as an initial step before transfer, to connect your standalone workstation PC to your Wi-Fi or network and check for updates to the virus definitions in AVG antivirus.

3.1 Connect your standalone workstation PC to your Wi-Fi or Local Area Network (LAN).

3.2 Open AVG antivirus from the icon on your desktop and select the **update** icon. The update window will open, and any new virus definitions should be installed automatically.



Update icon

[3] See 'Session 3: Managing the transfer of digital content to the archive' > Digital Material Accession Form: https://archives.wales/staff-toolkit/saving-the-bits-programme/

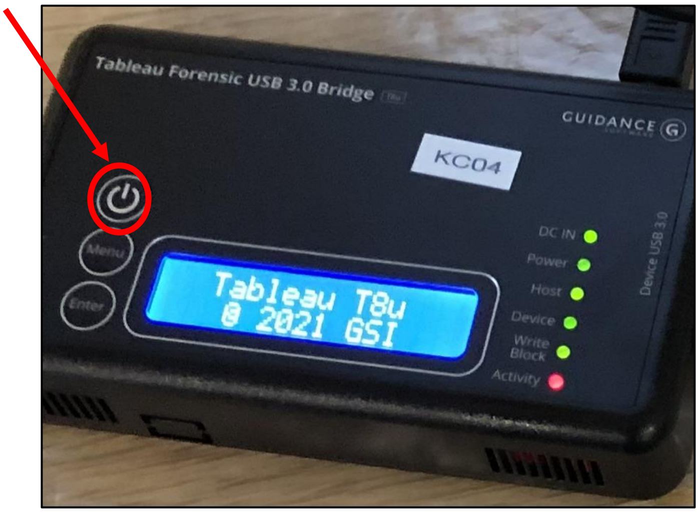
Note: In older releases of the AVG software, the update icon is in the bottom right-hand corner of the window. Once you update the software it will appear as in the above image.

3.3 If your PC needs to be restarted following the update, select ‘Restart Now’.

3.4 Once the update is complete, **disconnect your PC from your Wi-Fi/LAN** before you take any of the steps below. This is important to protect your network and ensure that it remains offline while a virus scan is performed.

Step 4 Connect external storage media via write blocker

4.1 Plug the lead from the write blocker into one of the PC’s USB ports and press the ‘on’ button.



4.2 Insert the USB stick or other USB-compatible external device (e.g. floppy disc drive/CD drive) into the write blocker.

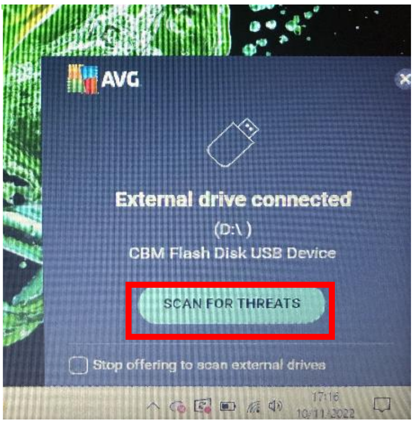
4.3 The external device should now appear as an external USB drive within the file explorer menu on your PC.

Step 5 Scan for viruses

The first step whenever materials are being transferred to your workstation is always to scan the content for viruses and malware, even if you believe a scan has been done recently. The virus scan option should appear automatically, but if it does not you will need to begin the process manually:

5.1 **Automatic scan option:**

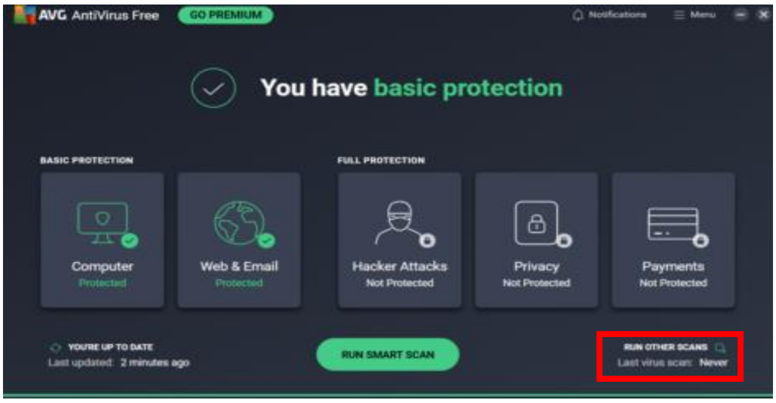
If you connect an external media device, such as a USB stick, to the PC via the write blocker, AVG antivirus should pop up automatically. Select 'Scan for Threats'. This should perform a scan on the external device only.


AVG
External drive connected
(D:\ )
CBM Flash Disk USB Device
SCAN FOR THREATS
□ Stop offering to scan external drives
17:16
10/11/2022

5.2 **Manual selection:**

If the option to scan does not pop up automatically, then:

i. Open AVG Antivirus and click on 'Run Other Scan'



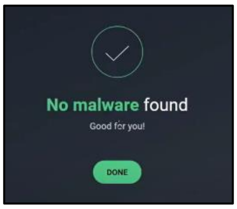
ii. Select 'file or folder scan'.

iii. Browse through the folder list which appears and select the external USB drive.

iv. Click 'OK'.

5.3 **Results**

Run the scan through until completion. If no malware has been detected, click 'done' and close AVG antivirus.


No malware found

Good for you!

If the scan reports that malware has been detected, remove the USB drive (via the file explorer menu > Drive tools > eject). Contact the depositor and inform them of the files which are infected with malware. You may wish to discuss whether another virus-free copy is available, and if it is permissible to delete the affected files. Be sure that before you attempt to transfer any of the remaining files, your repeat the virus scan step to ensure that no infected files remain.

We recommend you ask that any material transferred to you is scanned for malware and viruses at source to limit the possibility of this occurring.

Step 6 Copy content using Teracopy

Once you have virus-checked the content, the next step is to copy it from the external media source (e.g. USB stick), to the standalone workstation PC. To do this, we will use Teracopy to copy the content to the 'data' folder you created in step 1. Do not copy any program files that may be present.

6.1 Locate the USB drive in your file explorer and navigate to the folder(s) you want to transfer.

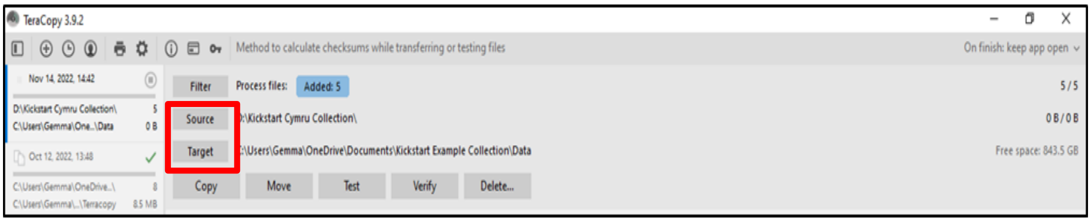
6.2 Select the folder(s) and **right-click on the mouse**. Select 'Teracopy'. To transfer multiple folders, you can use the shift or Ctrl keys to highlight them, then right click and select Teracopy.

Note: you may need to click 'show more options' in the right-click menu to see the option for Teracopy.

6.3 The Teracopy user interface will appear.

6.4. Within Teracopy, check that the 'Source' lists the correct folder location on the USB stick.

6.5 Click 'Target' and browse to the 'data' folder you have already created to transfer the files to. Press 'Select folder' to confirm. The data folder location should now appear as the Target:


TeraCopy 3.9.2

Method to calculate checksums while transferring or testing files

On finish: keep app open

Nov 14, 2022, 14:42

D:\Kickstart Cymru Collection\ 5

C:\Users\Gemma\One...\Data 0 B

Oct 12, 2022, 13:48

C:\Users\Gemma\OneDrive...\ 8

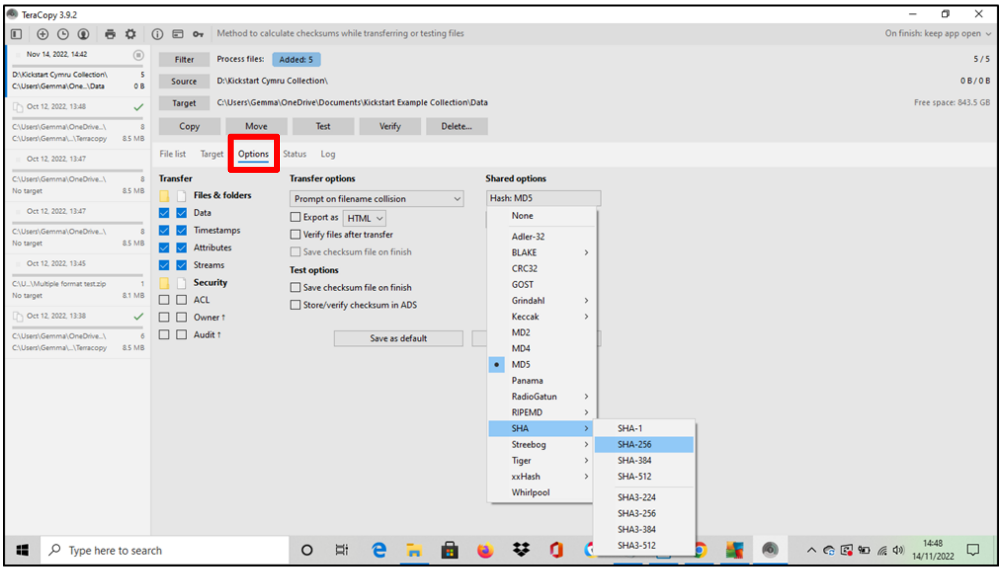
C:\Users\Gemma\...\Teracopy 8.5 MB

Process files: Added: 5 5 / 5

Source D:\Kickstart Cymru Collection\ 0 B / 0 B

Target C:\Users\Gemma\OneDrive\Documents\Kickstart Example Collection\Data Free space: 843.5 GB

6.6 Under 'Options' > 'Shared options' check that the Hash listed is 'SHA 256'. If it is not, select this option and then click 'Save as default' to ensure this is selected next time you use the program. You will not need to do this for future transfers.

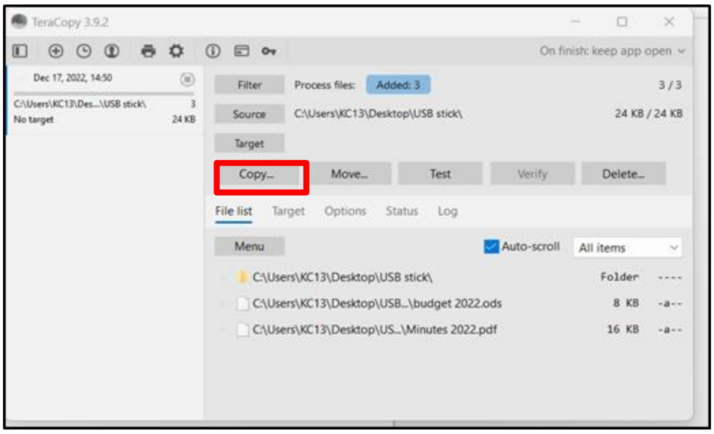


Source: D:\Kickstart Cymru Collection\

Target: C:\Users\Gemma\OneDrive\Documents\Kickstart Example Collection\Data

Free space: 843.5 GB

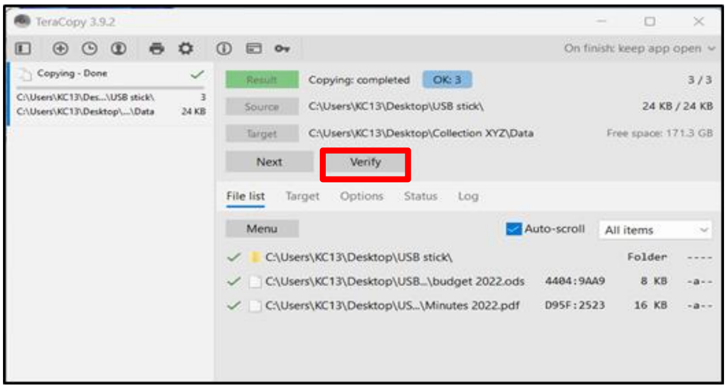
6.7 Select ‘Copy’.



Source: C:\Users\KC13\Desktop\USB stick\ 24 KB / 24 KB

```
C:\Users\KC13\Desktop\USB stick\                     Folder  ----
C:\Users\KC13\Desktop\USB...\budget 2022.ods          8 KB   -a--
C:\Users\KC13\Desktop\US...\Minutes 2022.pdf         16 KB   -a--
```

6.8 When copying is complete, select ‘Verify’.

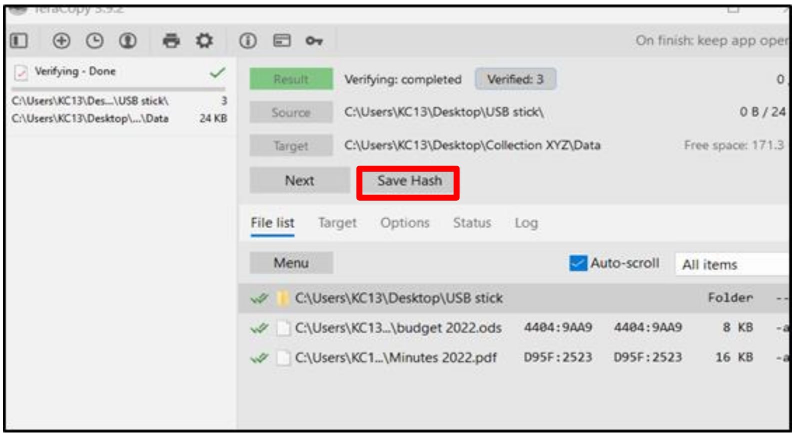


Source: C:\Users\KC13\Desktop\USB stick\ 24 KB / 24 KB

Target: C:\Users\KC13\Desktop\Collection XYZ\Data Free space: 171.3 GB

```
✓ C:\Users\KC13\Desktop\USB stick\                               Folder  ----
✓ C:\Users\KC13\Desktop\USB...\budget 2022.ods     4484:9AA9      8 KB   -a--
✓ C:\Users\KC13\Desktop\US...\Minutes 2022.pdf     D95F:2523     16 KB   -a--
```

6.9 Now select ‘Save Hash’



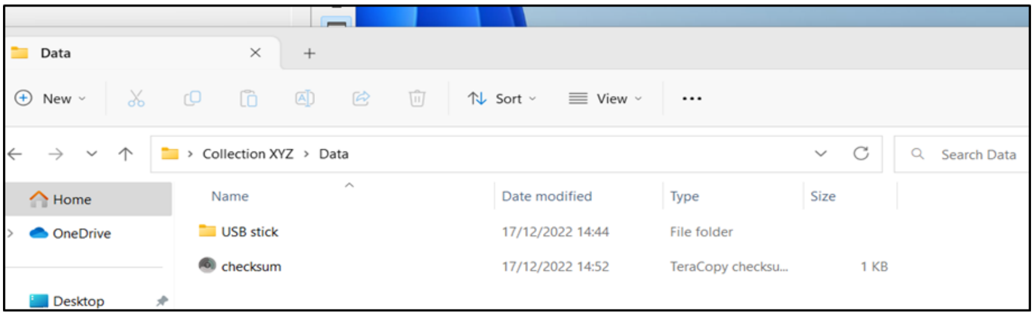
```
Verifying - Done
C:\Users\KC13\Des...\USB stick\        3
C:\Users\KC13\Desktop\...\Data     24 KB

Verifying: completed   Verified: 3                          0
C:\Users\KC13\Desktop\USB stick\                     0 B / 24
C:\Users\KC13\Desktop\Collection XYZ\Data      Free space: 171.3

C:\Users\KC13\Desktop\USB stick                                      Folder  --
C:\Users\KC13...\budget 2022.ods   4404:9AA9   4404:9AA9    8 KB  -a
C:\Users\KC1...\Minutes 2022.pdf   D95F:2523   D95F:2523   16 KB  -a
```

6.10 Within the file explorer, browse to the 'data' folder you have transferred the files to, and you should now be able to see:

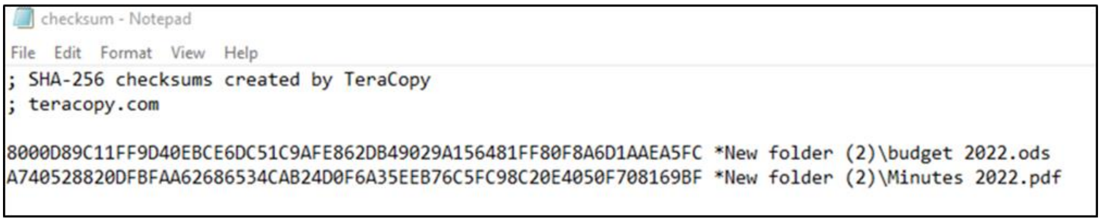
i) The transferred files/folders (titled 'USB stick' below)
ii) A new checksum file



Name	Date modified	Type	Size
USB stick	17/12/2022 14:44	File folder	
checksum	17/12/2022 14:52	TeraCopy checksu...	1 KB

6.11 Move the 'checksum' file into the 'metadata' folder. You can use the normal cut and paste function for this.

6.12 Right-click on the checksum file and select 'open with' Notepad. You should see a list of SHA-256 checksums generated by Teracopy for the number of files transferred. Take care not to change any of the data. In the event of accidental changes, you will need to repeat step 6 to create new checksums:



```
; SHA-256 checksums created by TeraCopy
; teracopy.com

8000D89C11FF9D40EBCE6DC51C9AFE862DB49029A156481FF80F8A6D1AAEA5FC *New folder (2)\budget 2022.ods
A740528820DFBFAA62686534CAB24D0F6A35EEB76C5FC98C20E4050F708169BF *New folder (2)\Minutes 2022.pdf
```

6.13 Now that you have copied the files, you can remove the USB device as follows:

i) Browse to the USB device location in file explorer and click drive tools > ‘EJECT’.

ii) Remove the USB stick from the USB Write blocker.

iii) Switch off the write blocker and unplug it from the PC.

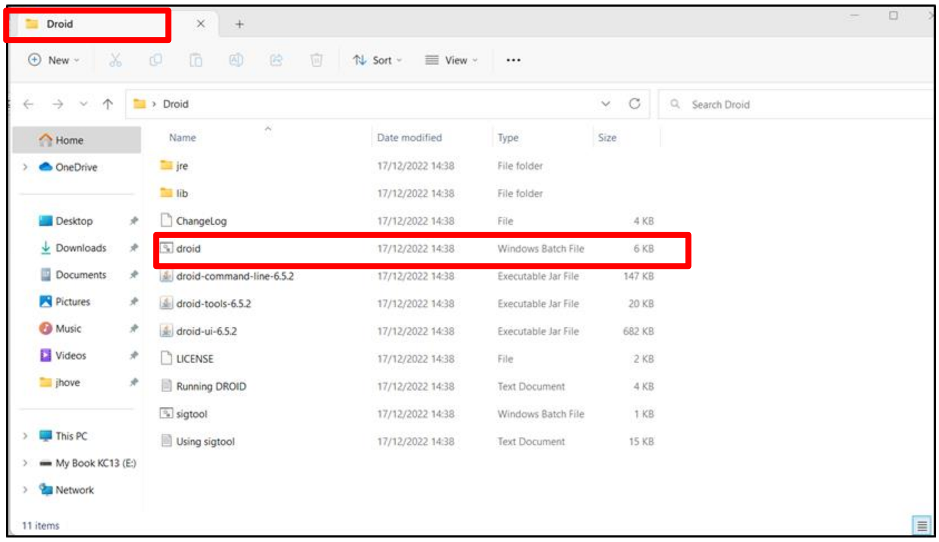
Step 7 File format identification (Droid)

7.1 Identify File Formats

Droid is a program created by The National Archives for format identification which utilises their PRONOM database. As PRONOM is regularly updated to accommodate new file formats and versions, it is recommended that you open Droid and download any updates as part of your updates schedule (see ‘Updates’ below).

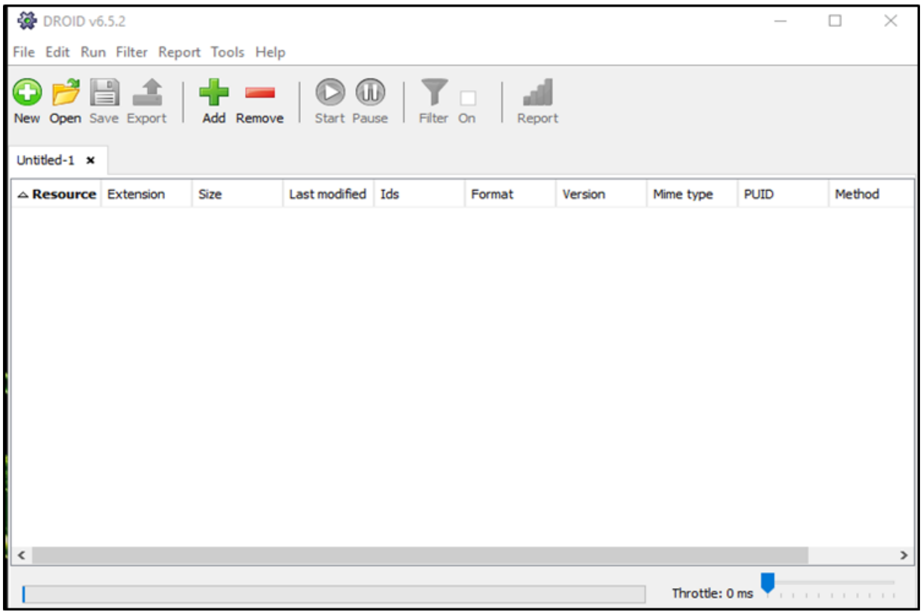
The National Archives’ own Droid user guide is available here: https://cdn.nationalarchives.gov.uk/documents/information-management/droid-user-guide.pdf

7.1.1 Open the ‘Droid’ folder on the Desktop. Open the folder titled ‘droid’ which says ‘Windows Batch File’ under ‘Type’:



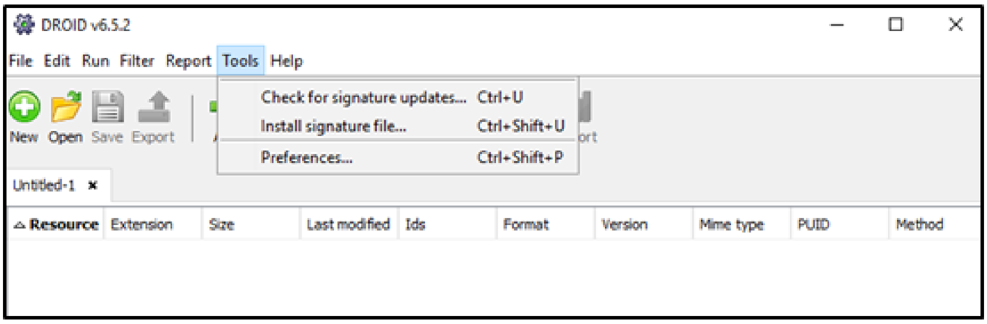
Name	Date modified	Type	Size
jre	17/12/2022 14:38	File folder	
lib	17/12/2022 14:38	File folder	
ChangeLog	17/12/2022 14:38	File	4 KB
droid	17/12/2022 14:38	Windows Batch File	6 KB
droid-command-line-6.5.2	17/12/2022 14:38	Executable Jar File	147 KB
droid-tools-6.5.2	17/12/2022 14:38	Executable Jar File	20 KB
droid-ui-6.5.2	17/12/2022 14:38	Executable Jar File	682 KB
LICENSE	17/12/2022 14:38	File	2 KB
Running DROID	17/12/2022 14:38	Text Document	4 KB
sigtool	17/12/2022 14:38	Windows Batch File	1 KB
Using sigtool	17/12/2022 14:38	Text Document	15 KB

The Droid user interface will open:


DROID v6.5.2
File Edit Run Filter Report Tools Help
New Open Save Export
Add Remove
Start Pause
Filter On
Report
Untitled-1
Resource Extension Size Last modified Ids Format Version Mime type PUID Method
Throttle: 0 ms

7.1.2 Check that the checksums generated by droid are using the SHA-256 hash format.

- Click on 'Tools' > Preferences:


DROID v6.5.2
File Edit Run Filter Report Tools Help
New Open Save Export
Check for signature updates... Ctrl+U
Install signature file... Ctrl+Shift+U
Preferences... Ctrl+Shift+P
Untitled-1
Resource Extension Size Last modified Ids Format Version Mime type PUID Method

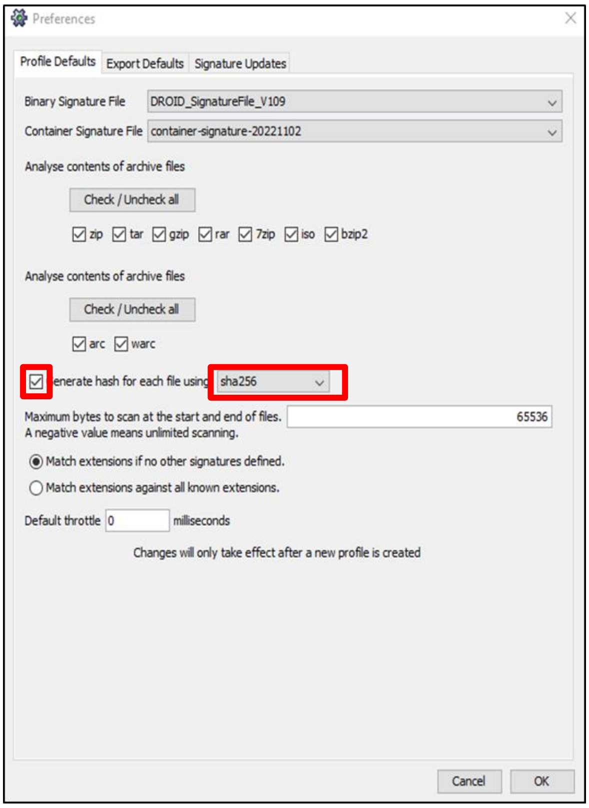
Within the 'Profile Defaults' tab:

- Ensure that:

i. The ‘Generate hash for each file using’ check box is ticked

ii. The drop-down menu next to it says ‘sha256’

- Click ‘OK’ to save any changes.



Preferences

Profile Defaults | Export Defaults | Signature Updates

Binary Signature File: DROID_SignatureFile_V109

Container Signature File: container-signature-20221102

Analyse contents of archive files

Check / Uncheck all

☑ zip ☑ tar ☑ gzip ☑ rar ☑ 7zip ☑ iso ☑ bzip2

Analyse contents of archive files

Check / Uncheck all

☑ arc ☑ warc

☑ Generate hash for each file using: sha256

Maximum bytes to scan at the start and end of files. A negative value means unlimited scanning. 65536

● Match extensions if no other signatures defined.

○ Match extensions against all known extensions.

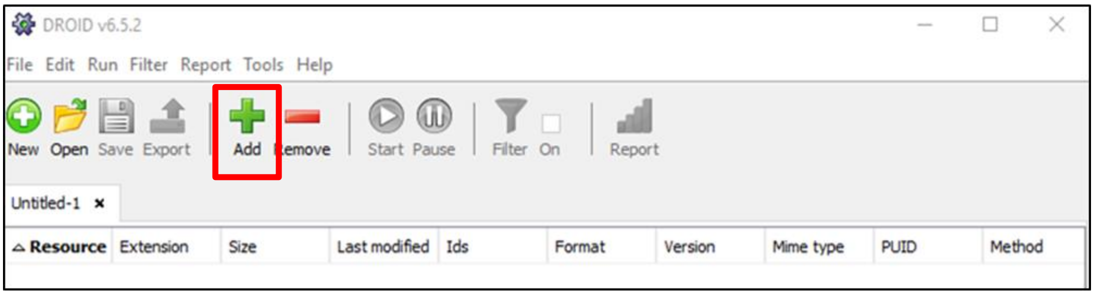
Default throttle 0 milliseconds

Changes will only take effect after a new profile is created

Cancel | OK

These pre-sets should already be selected on the version of Droid installed on your PC. If you need to reinstall Droid for any reason, when you follow the steps above, you will need to click ‘New’ to create a new profile before the changes take effect.

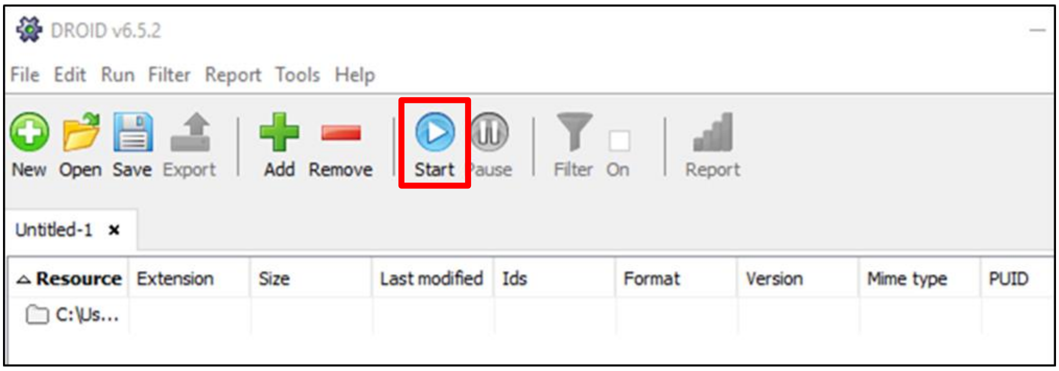
7.1.3 To run droid on your transferred collection of digital records, first click ‘Add’



7.1.4 Navigate to the directory for the top-level folder you have transferred (i.e. within the ‘data’ folder, but <u>excluding</u> metadata):

7.1.5 Click ‘OK’

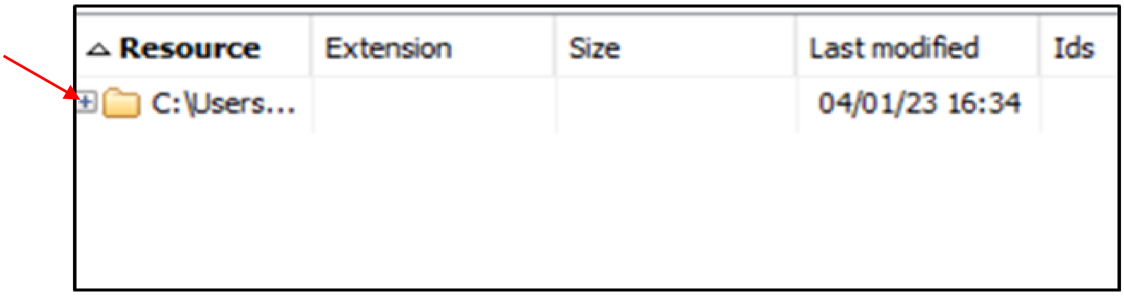
7.1.6 The directory for the folder should appear under ‘Resource’. Click ‘Start’:



Resource	Extension	Size	Last modified	Ids	Format	Version	Mime type	PUID
C:\Us…								

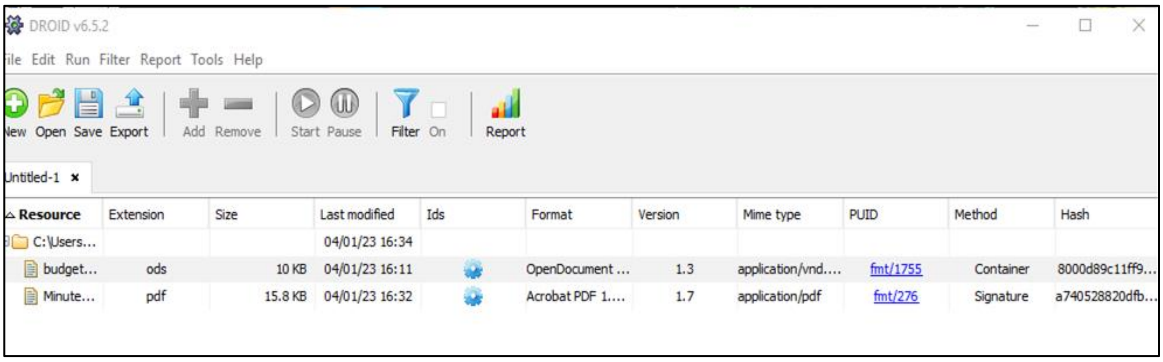
If the process runs successfully, you will see a little expandable plus (+) sign appear next to the listed folder under Resource.

Click on the plus sign. You may now see additional (+) icons where you can expand out any sub-folders transferred.



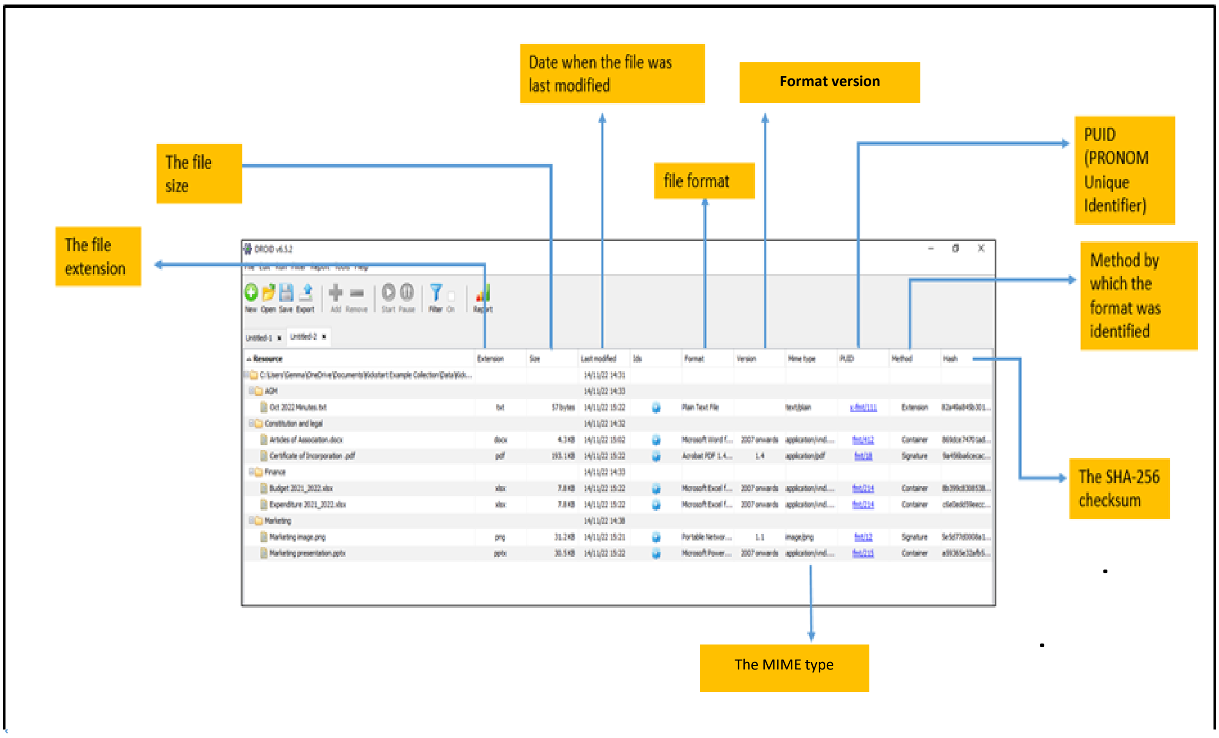
Resource	Extension	Size	Last modified	Ids
C:\Users…			04/01/23 16:34	

If you expand all the icons, you should see a list of all the individual files transferred.



Resource	Extension	Size	Last modified	Ids	Format	Version	Mime type	PUID	Method	Hash
C:\Users…			04/01/23 16:34							
budget…	ods	10 KB	04/01/23 16:11		OpenDocument …	1.3	application/vnd.…	fmt/1755	Container	8000d89c11ff9…
Minute…	pdf	15.8 KB	04/01/23 16:32		Acrobat PDF 1.…	1.7	application/pdf	fmt/276	Signature	a740528820dfb…

You will be able to view details including the following:



Resource	Extension	Size	Last modified	Ids	Format	Version	Mime type	PUID	Method	Hash
C:\Users\Gemma\OneDrive\Documents\Kickstart Example Collection\Data\Kick...			14/11/22 14:31							
AGM			14/11/22 14:33							
Oct 2022 Minutes.txt	txt	57 bytes	14/11/22 15:22		Plain Text File		text/plain	x-fmt/111	Extension	82a49a849b301...
Constitution and legal			14/11/22 14:32							
Articles of Association.docx	docx	4.3 KB	14/11/22 15:02		Microsoft Word f...	2007 onwards	application/vnd....	fmt/412	Container	868dce7470 [illegible]...
Certificate of Incorporation .pdf	pdf	193.1 KB	14/11/22 15:22		Acrobat PDF 1.4...	1.4	application/pdf	fmt/18	Signature	9a456ba6cecac...
Finance			14/11/22 14:33							
Budget 2021_2022.xlsx	xlsx	7.8 KB	14/11/22 15:22		Microsoft Excel f...	2007 onwards	application/vnd....	fmt/214	Container	8b399c8308538...
Expenditure 2021_2022.xlsx	xlsx	7.8 KB	14/11/22 15:22		Microsoft Excel f...	2007 onwards	application/vnd....	fmt/214	Container	c6e0edd59eecc...
Marketing			14/11/22 14:38							
Marketing image.png	png	31.2 KB	14/11/22 15:21		Portable Networ...	1.1	image/png	fmt/12	Signature	5e5d77d0008a1...
Marketing presentation.pptx	pptx	30.5 KB	14/11/22 15:22		Microsoft Power...	2007 onwards	application/vnd....	fmt/215	Container	a59365e32afb5...

- File extension
- File size
- Date of last modification
- File format
- Format version
- MIME type (aka 'media type' – this is a two-part identifier for file formats and contents to be transmitted via the internet (e.g. email)
- PUID (PRONOM Unique Identifier)
- The method by which the format was identified (e.g. signature, container)
- Hash (e.g. SHA256 checksum)

Some of these fields will be particularly helpful in performing appraisal checks on the files you have transferred. However, it is recommended that you firstly save the file as a .csv (step 7.1.7) and then view the fields within a spreadsheet application to take these appraisal steps (see step 7.2 below).

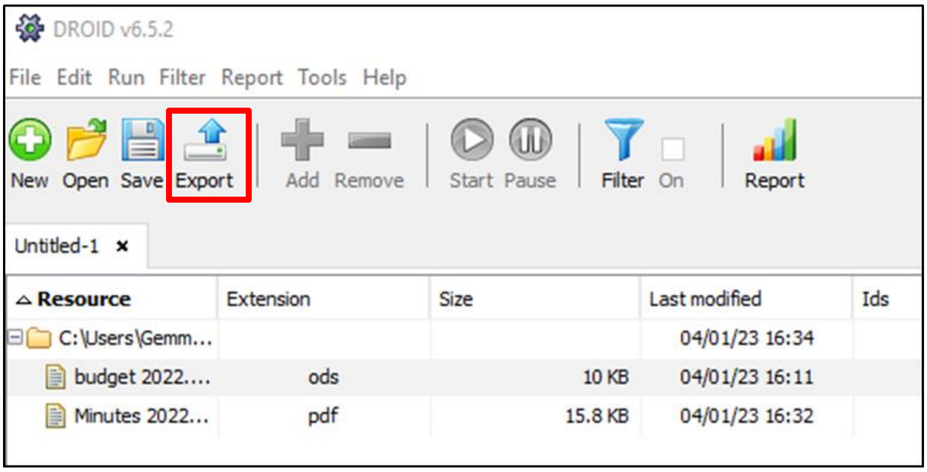
7.1.7 Save the Droid report

You can save the profile generated by Droid to evidence the checks you have run and retain useful accompanying metadata which will support integrity checks in the future. You can choose to export it as .csv format to your metadata folder, or as Droid profile.

It is recommended that as a minimum you should save the profile as .csv as this format will be easier to view and access in the future.

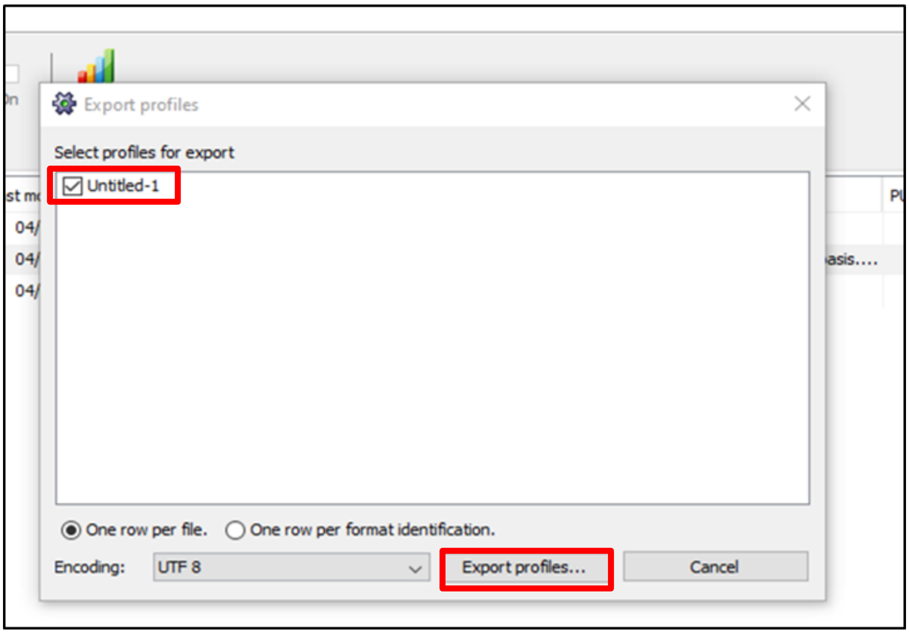
- **To save a copy as a csv. file:**

i) Click on ‘Export’



Resource	Extension	Size	Last modified	Ids
C:\Users\Gemm…			04/01/23 16:34	
budget 2022.…	ods	10 KB	04/01/23 16:11	
Minutes 2022…	pdf	15.8 KB	04/01/23 16:32	

ii) Tick the checkbox for the profile and then click ‘Export profiles’



Select profiles for export

☑ Untitled-1

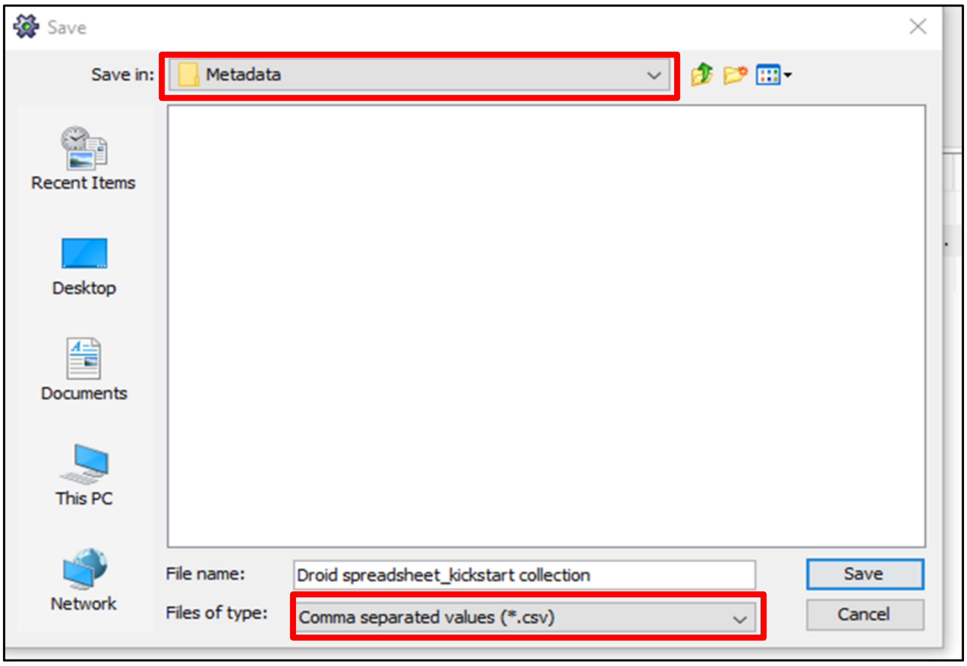
● One row per file. ○ One row per format identification.

Encoding: UTF 8

iii)	Type in a file name e.g. ('Droid_spreadsheet_ Kickstart_Collection_999999999') and select the metadata folder location

iv)	Click the 'Files of type' drop-down box and select 'Comma separated values'

v)	Click save.



Save in: Metadata

File name: Droid spreadsheet_kickstart collection

Files of type: Comma separated values (*.csv)

The .csv file should now be available in your metadata folder. You can now exit Droid.

To save the profile generated by Droid as a Droid report (optional):

i)	Click on 'save as' and select the metadata folder you saved the Teracopy checksum to previously. Give the file a name that indicates it is a Droid profile for the named collections/records. We suggest using a collection unique identifier (e.g. 'Droid profile_Kickstart_Collection_9999999')

ii)	This will save the profile as a 'DROID file'

7.2 Droid .csv file: Appraisal actions

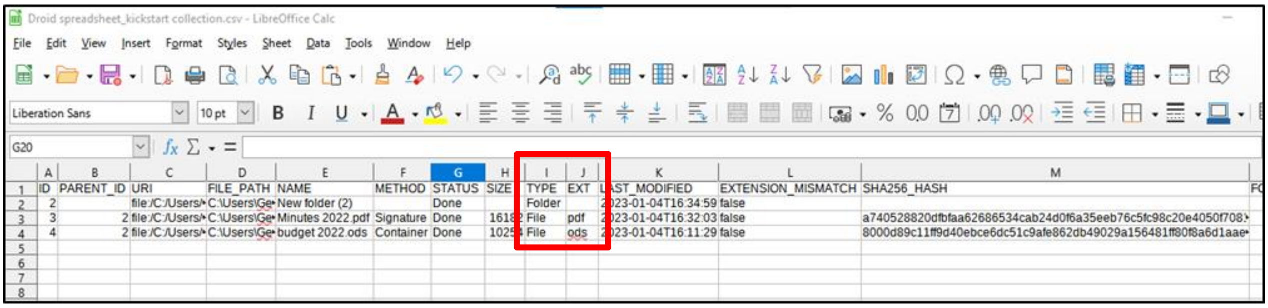
There are several actions associated with the appraisal of the transferred digital record which we can now take within the .csv file exported from Droid.

Open the Droid .csv file in LibreOffice Calc. You can see that the information in the .csv file is slightly different from the droid profile view, including the URI, file path, name, and extension mismatch fields.

Below are the fields and actions most relevant for our appraisal and verification workflow. Remember that editing or deletions will mean that the Droid report and Teracopy checksum log will need to be updated. You will also need to document your actions.

7.2.1 Check that each **file** in (Column I) has an associated **extension** in Column J and that this matches what you would anticipate.

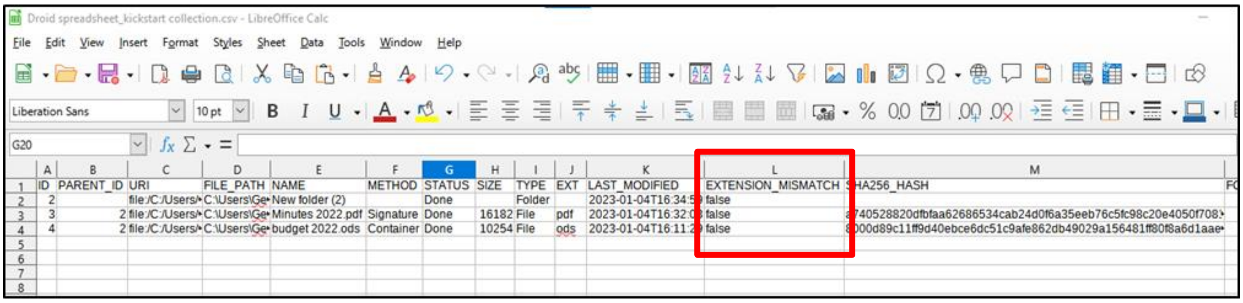
Note: Folders will not have an extension, only the files.


Droid spreadsheet_kickstart collection.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
G20

	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	ID	PARENT_ID	URI	FILE_PATH	NAME	METHOD	STATUS	SIZE	TYPE	EXT	LAST_MODIFIED	EXTENSION_MISMATCH	SHA256_HASH	FC
2	2		file:/C:/Users/	C:\Users\Ge	New folder (2)		Done		Folder		2023-01-04T16:34:59	false		
3	3	2	file:/C:/Users/	C:\Users\Ge	Minutes 2022.pdf	Signature	Done	16182	File	pdf	2023-01-04T16:32:03	false	a740528820dfbfaa62686534cab24d0f6a35eeb76c5fc98c20e4050f708	
4	4	2	file:/C:/Users/	C:\Users\Ge	budget 2022.ods	Container	Done	10254	File	ods	2023-01-04T16:11:29	false	8000d89c11ff9d40ebce6dc51c9afe862db49029a156481ff80f8a6d1aae	
5														
6														
7														
8														

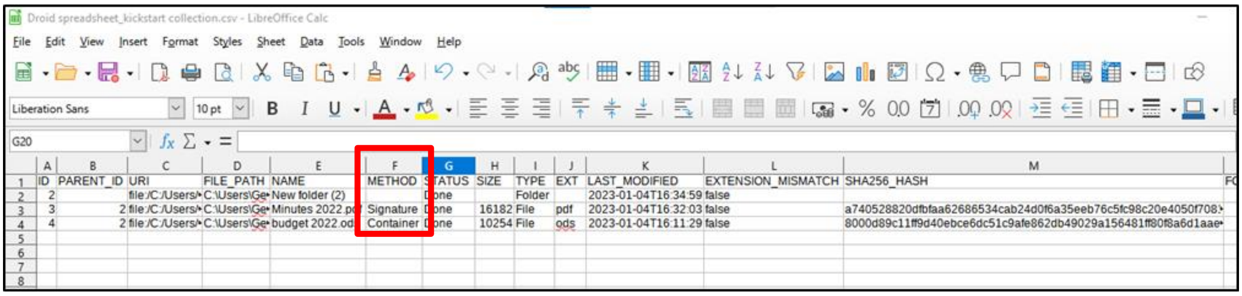
7.2.2 Check extension mismatch (column L)

Verify that the 'extension mismatch' column says 'false'. This indicates that there is no discrepancy between the file extension in a file name and the format of the file which Droid has identified. If 'true' is recorded, then a file extension mismatch has been identified, this may indicate that there could a problem opening the file in the future.


Droid spreadsheet_kickstart collection.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
G20

	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	ID	PARENT_ID	URI	FILE_PATH	NAME	METHOD	STATUS	SIZE	TYPE	EXT	LAST_MODIFIED	EXTENSION_MISMATCH	SHA256_HASH	FC
2	2		file:/C:/Users/	C:\Users\Ge	New folder (2)		Done		Folder		2023-01-04T16:34:59	false		
3	3	2	file:/C:/Users/	C:\Users\Ge	Minutes 2022.pdf	Signature	Done	16182	File	pdf	2023-01-04T16:32:03	false	a740528820dfbfaa62686534cab24d0f6a35eeb76c5fc98c20e4050f708	
4	4	2	file:/C:/Users/	C:\Users\Ge	budget 2022.ods	Container	Done	10254	File	ods	2023-01-04T16:11:29	false	8000d89c11ff9d40ebce6dc51c9afe862db49029a156481ff80f8a6d1aae	
5														
6														
7														
8														

7.2.3. Check the method of identification (column F)


Droid spreadsheet_kickstart collection.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
G20

ID	PARENT_ID	URI	FILE_PATH	NAME	METHOD	STATUS	SIZE	TYPE	EXT	LAST_MODIFIED	EXTENSION_MISMATCH	SHA256_HASH	FC
2		file:/C:/Users/	C:\Users\Ge	New folder (2)		Done		Folder		2023-01-04T16:34:59	false		
3	2	file:/C:/Users/	C:\Users\Ge	Minutes 2022.pd	Signature	Done	16182	File	pdf	2023-01-04T16:32:03	false	a740528820dfbfaa62686534cab24d0f6a35eeb76c5fc98c20e4050f708	
4	2	file:/C:/Users/	C:\Users\Ge	budget 2022.od	Container	Done	10254	File	ods	2023-01-04T16:11:29	false	8000d89c11ff9d40ebce6dc51c9afe862db49029a156481ff80f8a6d1aae	

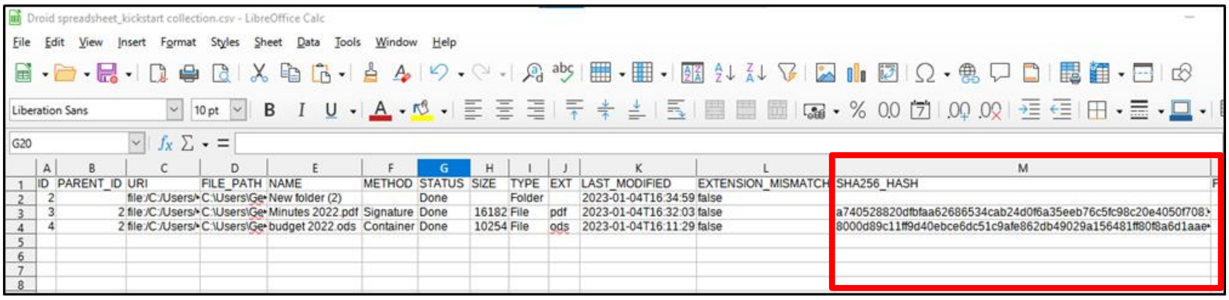
Droid can identify file formats via the extension, signature, or container.

If the method of identification is ‘extension’, this indicates a potential issue because it means that Droid was only able to identify the format based on the file extension alone. This may not be reliable because different file formats can share the same extension, so it is possible that the file may have been mis-identified. Alternatively, the file extension may have been misnamed, or altered, and may not reflect the actual format and characteristics of the file.

Both ‘signature’ and ‘container’ are more reliable methods of identification:

- Signature identifies the format through the byte sequence which is unique to the file format and version
- Container reflects identification of embedded files within a main file and verifies files at more than one level. This is more likely to be the method of identification for files produced within a suite of software (e.g., an Open Document file).[4]

7.2.4 Finally, navigate to the SHA 256 Hash column (column M)


Droid spreadsheet_kickstart collection.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
G20

ID	PARENT_ID	URI	FILE_PATH	NAME	METHOD	STATUS	SIZE	TYPE	EXT	LAST_MODIFIED	EXTENSION_MISMATCH	SHA256_HASH	F
2		file:/C:/Users/	C:\Users\Ge	New folder (2)		Done		Folder		2023-01-04T16:34:59	false		
3	2	file:/C:/Users/	C:\Users\Ge	Minutes 2022.pdf	Signature	Done	16182	File	pdf	2023-01-04T16:32:03	false	a740528820dfbfaa62686534cab24d0f6a35eeb76c5fc98c20e4050f708	
4	2	file:/C:/Users/	C:\Users\Ge	budget 2022.ods	Container	Done	10254	File	ods	2023-01-04T16:11:29	false	8000d89c11ff9d40ebce6dc51c9afe862db49029a156481ff80f8a6d1aae	

Within this column you can check the SHA 256 hash matches that which you generated in Teracopy, or which was created by the depositor prior to deposit (if any).

To compare against the checksums generated in Teracopy, you can:

- Open the Teracopy checksum from the ‘metadata’ folder via Notepad (see Step 2.12 above)

[4] For more information, see ‘Identification Method’ in *The National Archives*: *DROID User Guide*: https://cdn.nationalarchives.gov.uk/documents/information-management/droid-user-guide.pdf

- Copy (Ctrl + C) a checksum
- Press ‘Find’ (Ctrl + F) within the Droid .csv file
- Paste (Ctrl + V) the checksum from Teracopy into the search box and check that there is a corresponding checksum in Column M.

Notes:

You would not anticipate there to be any difference between the checksums generated by Teracopy and Droid at this stage as we have not made any changes to the file during the ingest process. So, if the two checksums for a file do not match then this indicates that they are not being generated according to the same hash string (e.g. SHA256) and you should double-check the settings in each tool (see step 6.6 and step 7.1.2 above). Spot checking a few files may be sufficient to ensure that the checksums are being similarly generated.

Similarly, if you received checksums with the files which were generated by the depositor previously and these do not match the checksums in Droid, verify that they were originally generated using the same hash string.

7.2.5 Check for duplicates

To check for duplicate checksums (which may indicate you have received more than one copy of the same file):

i) select and copy a hash string in column ‘M’

ii) press ‘Ctrl + F’ and enter the string in the ‘Find’ box

iii) any duplicated values should be highlighted within column M.

You could also do this in MS Excel using conditional formatting - see for example https://www.excelmojo.com/find-duplicates-in-excel/.

When duplicate files are identified you need to consider if this is intentional (add value), or accidental and if they can be deleted. Refer to your appraisal policy. Remember that if you delete any content, you will need to create new checksums as those created will be invalid.

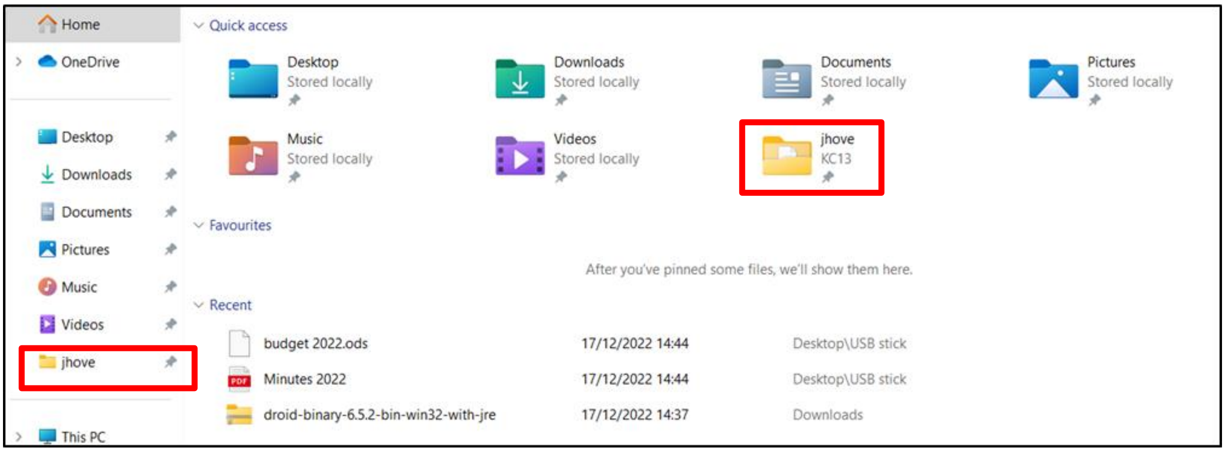
As outlined in the ‘Fixity Checking with Droid’ section below, you can also use the checksums in column M in the future to perform monitoring and verification checks to ensure that the content of the files has not been altered or corrupted during storage.

Step 8 File format validation (JHOVE)

JHOVE can be used for file format verification and validation. This complements some of the features of Droid and will enable you to perform the appraisal tasks of file format verification and validation, and investigate further any format issues that have been raised so far in the process (e.g. a failure to identify a format in Droid).

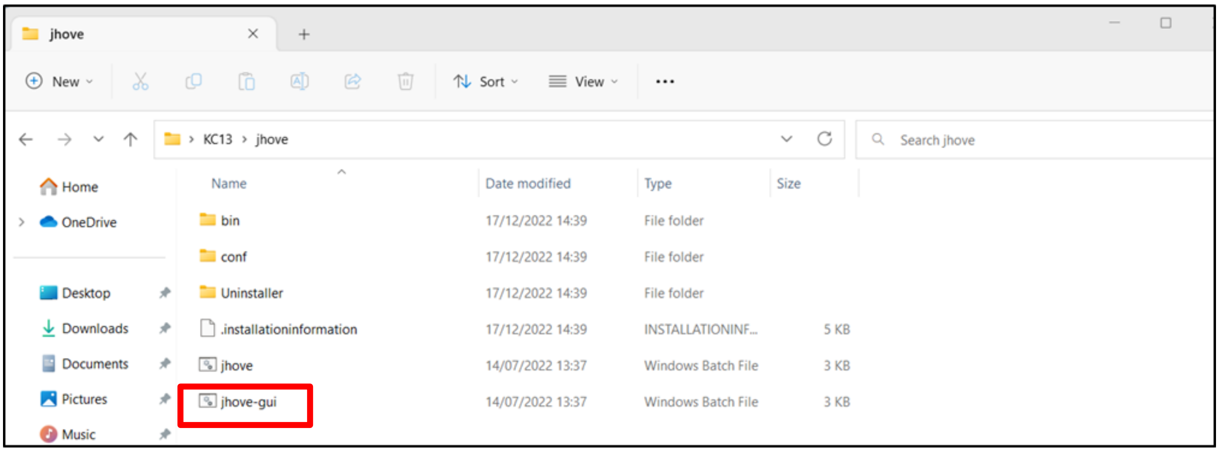
Jhove is saved within C drive > users folder on your PC. It should also be pinned to the 'Quick Access' menu within file explorer:

8.1 Open the 'jhove' folder within your quick access menu in file explorer:



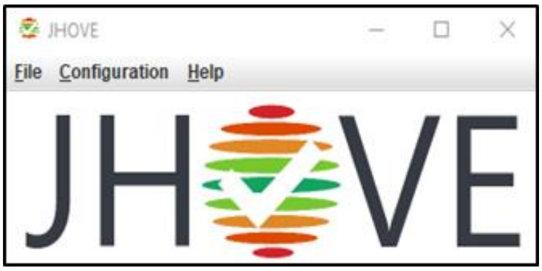
budget 2022.ods	17/12/2022 14:44	Desktop\USB stick
Minutes 2022	17/12/2022 14:44	Desktop\USB stick
droid-binary-6.5.2-bin-win32-with-jre	17/12/2022 14:37	Downloads

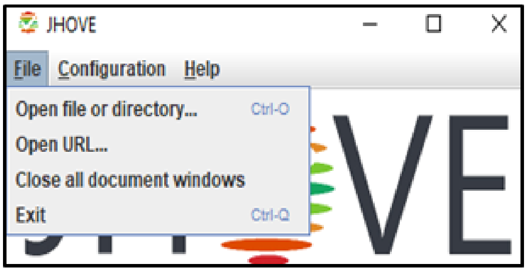
8.2 Open the Windows Batch File named 'jhove-gui':



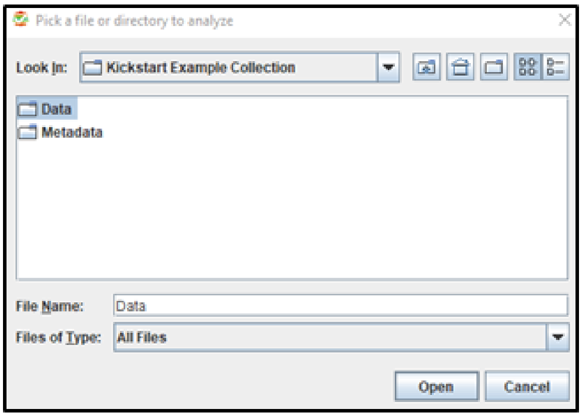
Name	Date modified	Type	Size
bin	17/12/2022 14:39	File folder	
conf	17/12/2022 14:39	File folder	
Uninstaller	17/12/2022 14:39	File folder	
.installationinformation	17/12/2022 14:39	INSTALLATIONINF...	5 KB
jhove	14/07/2022 13:37	Windows Batch File	3 KB
jhove-gui	14/07/2022 13:37	Windows Batch File	3 KB

8.3 Click on ‘File’ and then ‘Open file or directory’





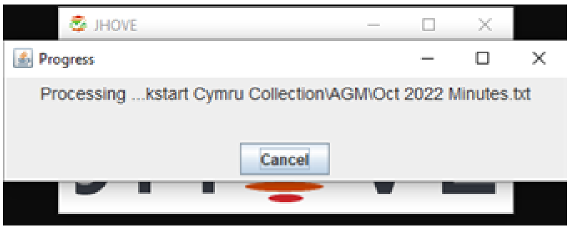
8.4 Browse to the directory for the digital records you have transferred into the ‘data’ folder and click ‘open’. Once you have selected the file, Jhove will automatically run and a ‘Progress’ window will appear:



Look In: Kickstart Example Collection

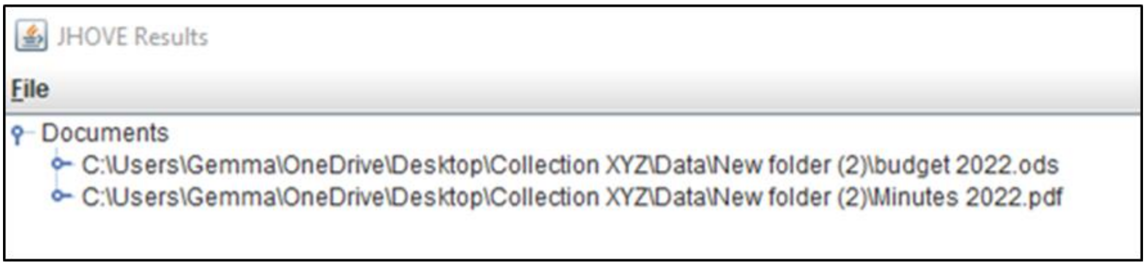
File Name: Data

Files of Type: All Files



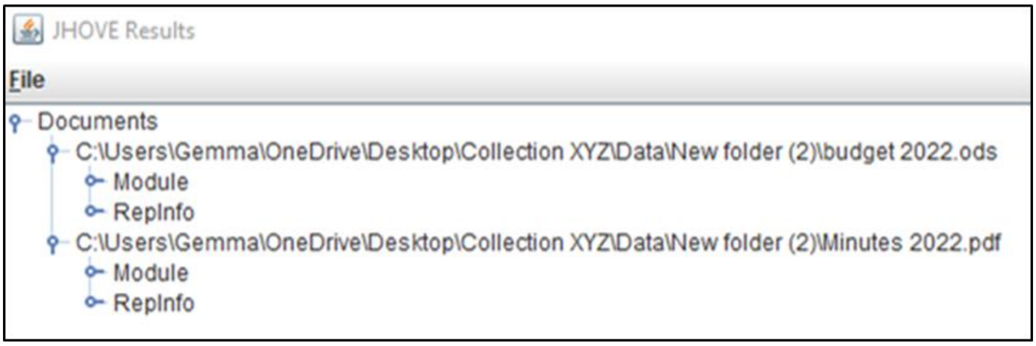
Processing ...kstart Cymru Collection\AGM\Oct 2022 Minutes.txt

8.5 Once complete a ‘JHOVE Results’ window will open



```
Documents
   C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\budget 2022.ods
   C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\Minutes 2022.pdf
```

8.6. If you double-click on a file name, it will expand out into two sub-categories:

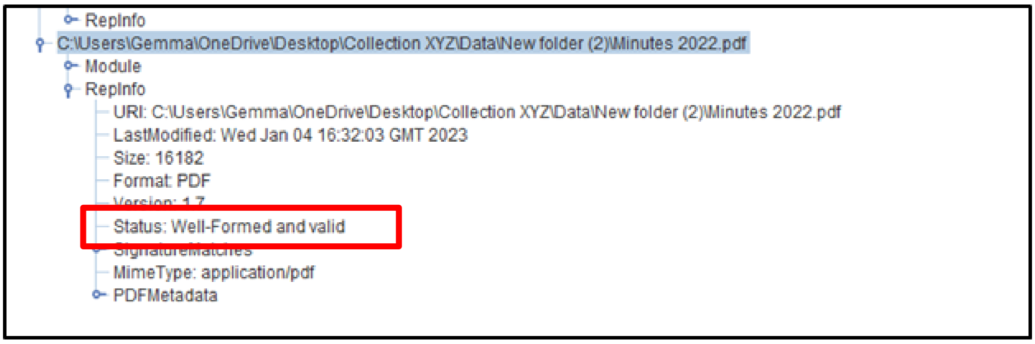


```
Documents
  C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\budget 2022.ods
    Module
    RepInfo
  C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\Minutes 2022.pdf
    Module
    RepInfo
```

The information listed under **Repinfo** includes details such as:

- the Uniform Resources Identifier (URI)
- the file size
- format and format version
- confirmation of whether the file signature matches the format of the file
- file status

8.7 Check the ‘status’ is ‘well-formed and valid’:



```
    RepInfo
  C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\Minutes 2022.pdf
    Module
    RepInfo
      URI: C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\Minutes 2022.pdf
      LastModified: Wed Jan 04 16:32:03 GMT 2023
      Size: 16182
      Format: PDF
      Version: 1.7
      Status: Well-Formed and valid
      SignatureMatches
      MimeType: application/pdf
      PDFMetadata
```

8.8 Save the file to your metadata folder:

You can save the report as either a text file and/or an audit report.

- **Saving as a text file:**

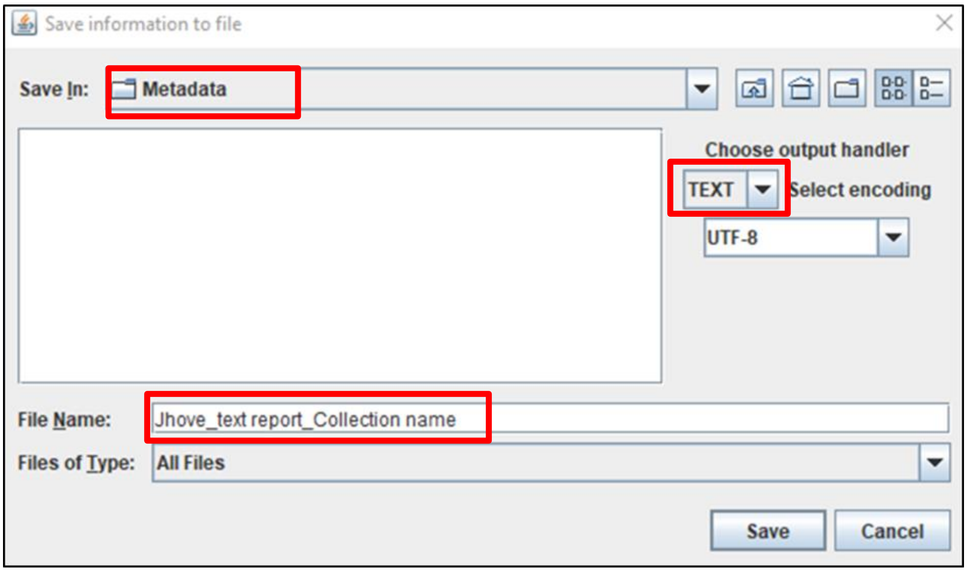
i) Select File and ‘Save’:

ii) Select the ‘Metadata’ folder as the location within ‘Save In’

iii) Ensure that ‘TEXT’ is select in the drop-down menu under ‘Choose output handler’

iv) Choose a suitable File Name which could include the collection name, or accession number, and an indication that it is a Jhove text report

v) Click ‘Save’:



Save In: Metadata

Choose output handler: TEXT

Select encoding: UTF-8

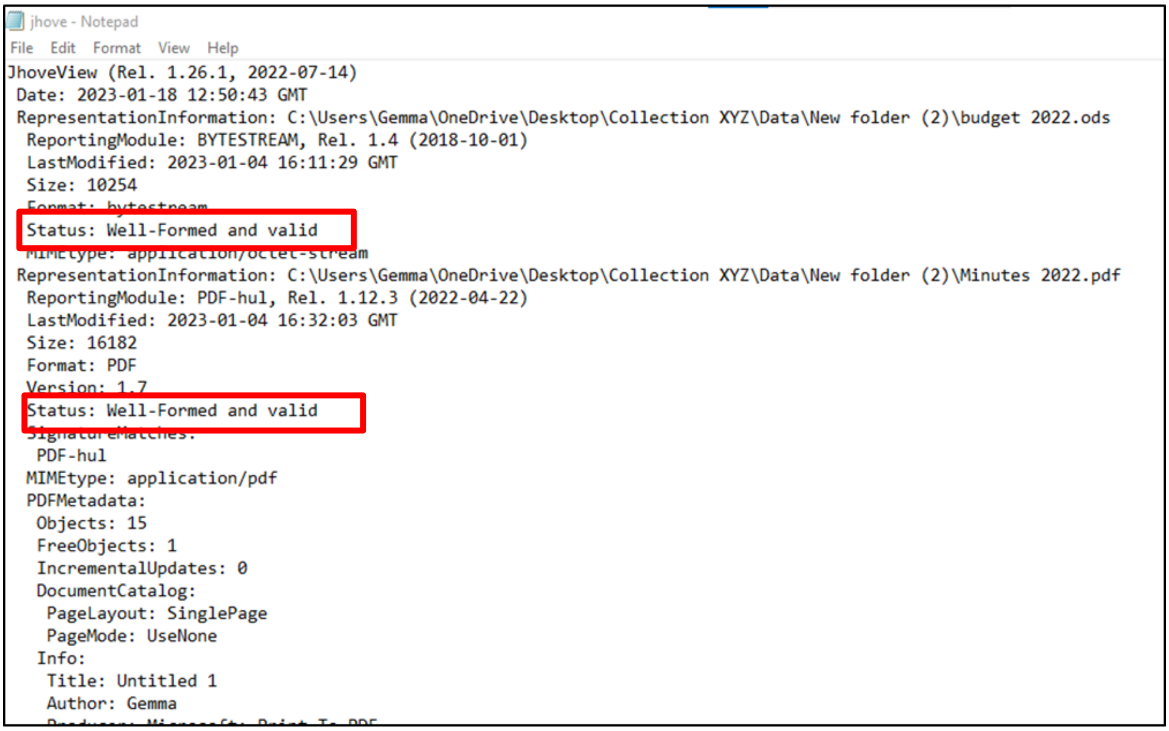
File Name: Jhove_text report_Collection name

Files of Type: All Files

vi) Navigate to your metadata folder within the File Explorer menu

vii) Open the Jhove text report you have generated (you can open using Notepad)

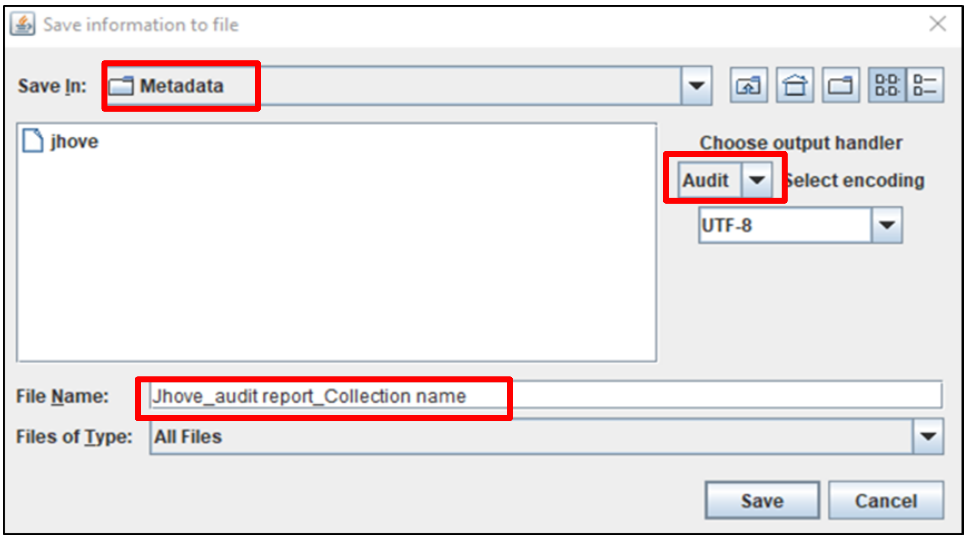
viii) You should see the following information, including a record that each file status is Well-Formed and valid:



```
JhoveView (Rel. 1.26.1, 2022-07-14)
 Date: 2023-01-18 12:50:43 GMT
 RepresentationInformation: C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\budget 2022.ods
  ReportingModule: BYTESTREAM, Rel. 1.4 (2018-10-01)
  LastModified: 2023-01-04 16:11:29 GMT
  Size: 10254
  Format: bytestream
  Status: Well-Formed and valid
  MIMEtype: application/octet-stream
 RepresentationInformation: C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\Minutes 2022.pdf
  ReportingModule: PDF-hul, Rel. 1.12.3 (2022-04-22)
  LastModified: 2023-01-04 16:32:03 GMT
  Size: 16182
  Format: PDF
  Version: 1.7
  Status: Well-Formed and valid
  SignatureMatches:
   PDF-hul
  MIMEtype: application/pdf
  PDFMetadata:
   Objects: 15
   FreeObjects: 1
   IncrementalUpdates: 0
   DocumentCatalog:
    PageLayout: SinglePage
    PageMode: UseNone
   Info:
    Title: Untitled 1
    Author: Gemma
    Producer: Microsoft: Print To PDF
```

- **Saving from Jhove as an audit file:**

i) Select File and ‘Save’:
ii) Select the ‘Metadata’ folder as the location within ‘Save In’
iii) Ensure that ‘Audit’ is select in the drop-down menu under ‘Choose output handler’
iv) Choose a suitable File Name which could include the collection name, or accession number, and an indication that it is a Jhove audit report
v) Click ‘Save’:


Save information to file

Save In: Metadata

jhove

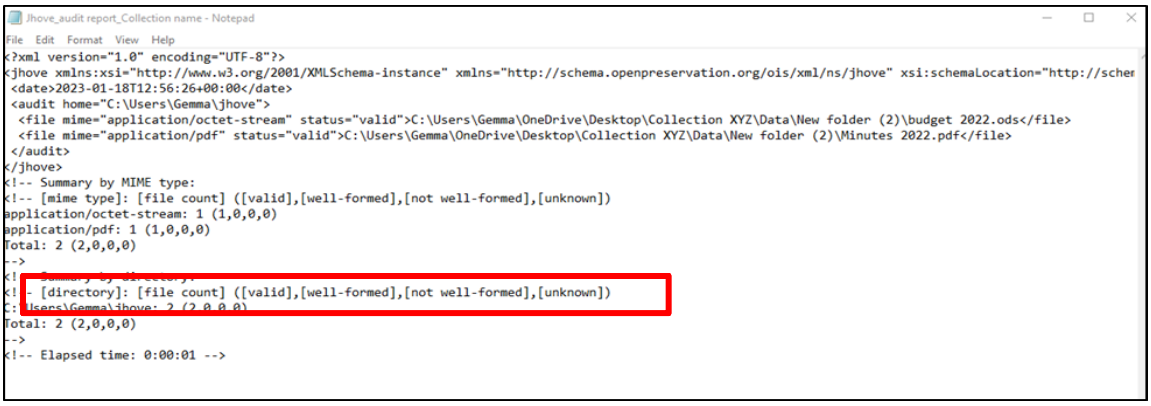
Choose output handler: Audit

Select encoding: UTF-8

File Name: Jhove_audit report_Collection name

Files of Type: All Files

vi) Navigate to your metadata folder within the file explorer menu
vii) Open the Jhove audit report you have generated (you can open using Notepad)
viii) you should see the following information, which provides a summary of the number of files matching a particular field (e.g. file count, valid, well-formed):


Jhove_audit report_Collection name - Notepad

```
<?xml version="1.0" encoding="UTF-8"?>
<jhove xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schema.openpreservation.org/ois/xml/ns/jhove" xsi:schemaLocation="http://scher
 <date>2023-01-18T12:56:26+00:00</date>
 <audit home="C:\Users\Gemma\jhove">
  <file mime="application/octet-stream" status="valid">C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\budget 2022.ods</file>
  <file mime="application/pdf" status="valid">C:\Users\Gemma\OneDrive\Desktop\Collection XYZ\Data\New folder (2)\Minutes 2022.pdf</file>
 </audit>
</jhove>
<!-- Summary by MIME type:
<!-- [mime type]: [file count] ([valid],[well-formed],[not well-formed],[unknown])
application/octet-stream: 1 (1,0,0,0)
application/pdf: 1 (1,0,0,0)
Total: 2 (2,0,0,0)
-->
<!-- Summary by directory:
<!-- [directory]: [file count] ([valid],[well-formed],[not well-formed],[unknown])
C:\Users\Gemma\jhove: 2 (2,0,0,0)
Total: 2 (2,0,0,0)
-->
<!-- Elapsed time: 0:00:01 -->
```

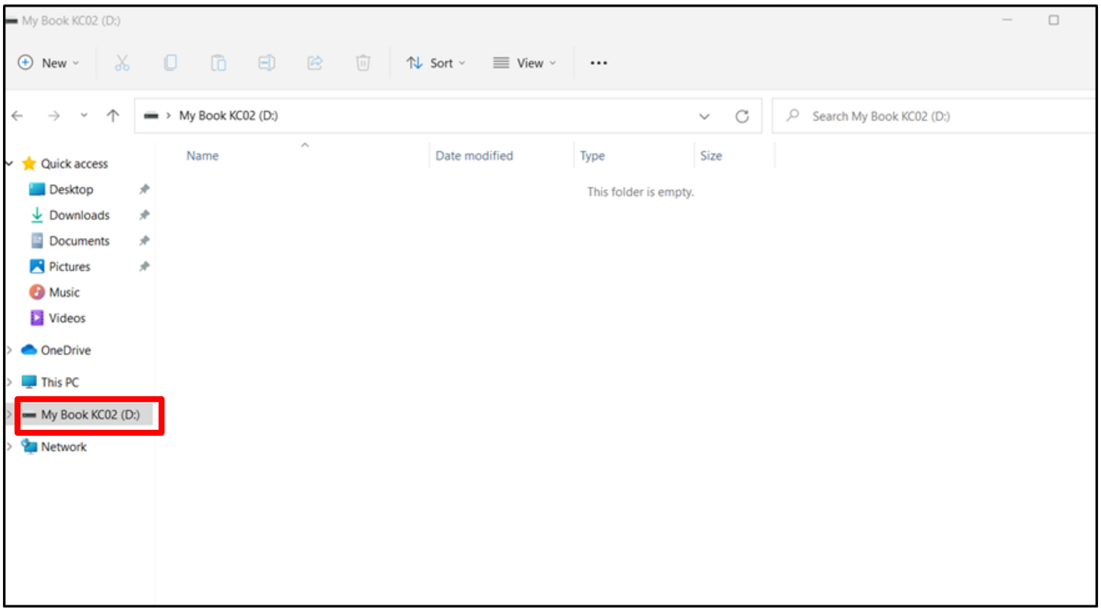
You can now exit Notepad. As you have generated the necessary metadata reports to evidence the validation steps you have taken, you can move on to transferring your files to the external hard disk.

Step 9 Transfer files to external hard drive

Now that you have successfully created a copy of the data and saved the relevant metadata reports together with it, you can move them to your external RAID Hard drive.

9.1 Open your file explorer menu

9.2 Select your RAID external hard drive. This will be named e.g. 'MyBook Duo KC##'



This folder is empty.

9.3 Using Teracopy, copy the files from the folder you have created directly into the external hard drive. To do this, select the level above the data/metadata folders, the [Collection Name] folder created in Step 2.1. above.

9.4 The files will automatically transfer and appear in the file explorer window when copied.

9.5 Do not open these files directly as this could change the checksums. We advise you to create a working copy if you wish to access them.

Note: Consider changing the permissions of your top-level directory to protect the content. It is *extremely easy* to delete files from the MyBook Duo via the file explorer menu, as there is no warning to check that you want to delete the files. If you accidentally delete a file, it should still be available in the PC recycle bin, but it is advisable to take care when navigating folders on the MyBook Duo drive to avoid this.

Step 10 Managing your desktop files

As you have now transferred (copied) the files to your external hard drive, you can delete them from the working folder you created on your workstation desktop.

Before you delete the files, however, you should save a copy of the metadata folder to a suitable designated location on the workstation PC (or on your network if this is accessible from your workstation). This will ensure that you have a separately accessible copy of your metadata.

You may wish to retain a copy of the files on your workstation PC for the time being, but beware that storing large numbers of files may slow down its performance.

Switching off

Once you have ingested the files and transferred them to your external hard drive, and ensured that a separate copy of the metadata is separately saved, it is safe to shut down your PC workstation. To do so, you can follow the same steps as you usually would to shut down any PC (via the Start menu). If you are turning off your UPS when the workstation is not in use, ensure that this is switched off *after* you have turned off the PC. Your MyBook Duo should also power down after turning off the PC and UPS; it does not need to be separately shut down.

We would also recommend that you switch off the USB write blocker via the on-off button when not in use. You do not need to disconnect the write blocker from the USB port in your computer.

Online ingest

The 10-step workflow outlined in this guidance is geared towards the offline ingest of materials deposited on external media devices. However, there may be occasions where the only option is for you to receive files online and download them to the ingest workstation. Where this is the case, the following steps outline an alternative online ingest workflow. This is not the intended purpose of the workstation, and you should be aware that any files downloaded to the workstation in this way pose a potential cybersecurity and malware risk, so you should ensure that the sender is a verified and trusted depositor.

Anti-virus scan

i. Connect to your Wi-Fi/LAN

ii. Check that your virus definitions are up to date (see step 3.2 above)

iii. Navigate to the location where the files have been sent, e.g. your email browser/We Transfer/Dropbox

iv. Download the files to an appropriately named folder on your desktop (e.g. Ingest_collection name_ID)

v. Once you have confirmed the download is complete, go back to the We Transfer/Dropbox location and delete the data. This is particularly important where there might be sensitive/confidential files. Turn off your Wi-Fi/LAN and complete the rest of the ingest steps below offline

vi. AVG antivirus should automatically scan downloads for malware and will produce a notification if any issues are detected. However, to be confident, you can perform a manual scan of the file within the download folder before moving it anywhere else:

vii. Open AVG antivirus

viii. Select 'File or folder scan'

ix. Navigate to the file within your downloads folder

x. Right click on the relevant file/folder

xi. In the drop-down menu, select 'Scan selected items for viruses'

Now use Teracopy to copy the files from the downloads folder to your data folder

i. Within the downloads directory, right click the relevant file or folder and select Teracopy

ii. Follow the steps outlined in step 6 above to copy the files to the data folder you have already created.

You can now follow the same workflow from the step 7 above onwards.

Fixity checking with Droid

One of the key activities in digital preservation is ensuring that there are no changes to digital records during their archival storage. This is described as 'fixity' checking, which aims to establish that a digital file has remained the same over time and has not been altered or corrupted, a process that is also described as 'integrity checking'.

The NDSA's definition of file fixity is 'the characteristic that indicates a digital object's bitstream remains unchanged over time'.[5]

To check that the contents of your digital content have not changed during storage, we recommend performing scheduled fixity checks on the files which you have transferred to your external hard drive

[5] 'Working Definitions for the Levels of Digital Preservation Version 2.0'. NDSA 2019: https://osf.io/rynmf

(and anywhere else it is stored). To do this, you can compare the checksums generated during the ingest process, which you have stored in the metadata folder, against those which you regenerate by running Droid over the same content again.

To generate a new report, you would follow the same process outlined in step 7.1 above**,** adding the relevant 'data' folder for the content on the hard drive as the target folder in Droid. Once the report is generated, you can then save it as an additional Droid report, in .csv format, within the metadata folder. You could also create a sub-folder within the metadata folder for this purpose, titled for example 'Droid fixity reports', and save each new file with the relevant date as an extension. (e.g. 'Droid Report_Fixity Check_[*collection name*]_YYYYMMDD'). [By using this date format, the files will automatically sort in date order].

Once you have generated and saved the report, you can compare the checksums against those generated on ingest (see 'Approaches to fixity checking' below):

How often should you perform fixity checks?

There is no specific mandate for how often fixity checks should be performed within the NDSA levels of digital preservation, which recommends verification at 'fixed intervals'. The Digital Preservation Coalition recommends checking the content on hard drives every **six months**.[6] However, more frequent checks would allow problems to be detected and fixed sooner.

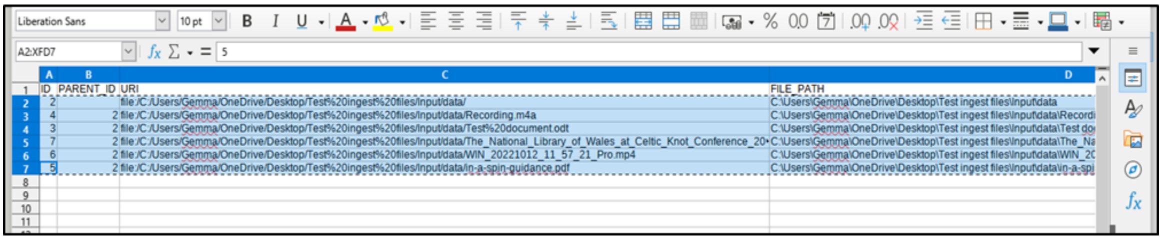
Approaches to fixity checking using Droid:

- One way to do this would be to select each checksum from the original Droid .csv report generated on ingest, copy it (ctrl + c), and enter it into the find function (ctrl + f) in the newly generated report. If the checksum has not changed, the same hash should be highlighted in the new report.
- An easier approach, particularly if you have a lot of files, is to use the 'condition' function in Libre Office Calc following the workflow outlined on the next page.

Comparing checksums via the 'condition' function in LibreOffice calc

i. Open the newly generated Droid .csv report and select all the content except the column heading fields (i.e. from Row 2 downwards)

[6] 'Fixity and checksums'. Digital Preservation Coalition *Digital Preservation Handbook*: https://www.dpconline.org/handbook/technical-solutions-and-tools/fixity-and-checksums#:~:text=As%20a%20general%20guideline%2C%20checking,system%20and%20more%20processing%20resources.



	ID	PARENT_ID	URI	FILE_PATH
2	2		file:/C:/Users/Gemma/OneDrive/Desktop/Test%20ingest%20files/Input/data/	C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data
3	4	2	file:/C:/Users/Gemma/OneDrive/Desktop/Test%20ingest%20files/Input/data/Recording.m4a	C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data\Recordi
4	3	2	file:/C:/Users/Gemma/OneDrive/Desktop/Test%20ingest%20files/Input/data/Test%20document.odt	C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data\Test do
5	7	2	file:/C:/Users/Gemma/OneDrive/Desktop/Test%20ingest%20files/Input/data/The_National_Library_of_Wales_at_Celtic_Knot_Conference_20	C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data\The_Na
6	6	2	file:/C:/Users/Gemma/OneDrive/Desktop/Test%20ingest%20files/Input/data/WIN_20221012_11_57_21_Pro.mp4	C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data\WIN_20
7	5	2	file:/C:/Users/Gemma/OneDrive/Desktop/Test%20ingest%20files/Input/data/in-a-spin-guidance.pdf	C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data\in-a-spi

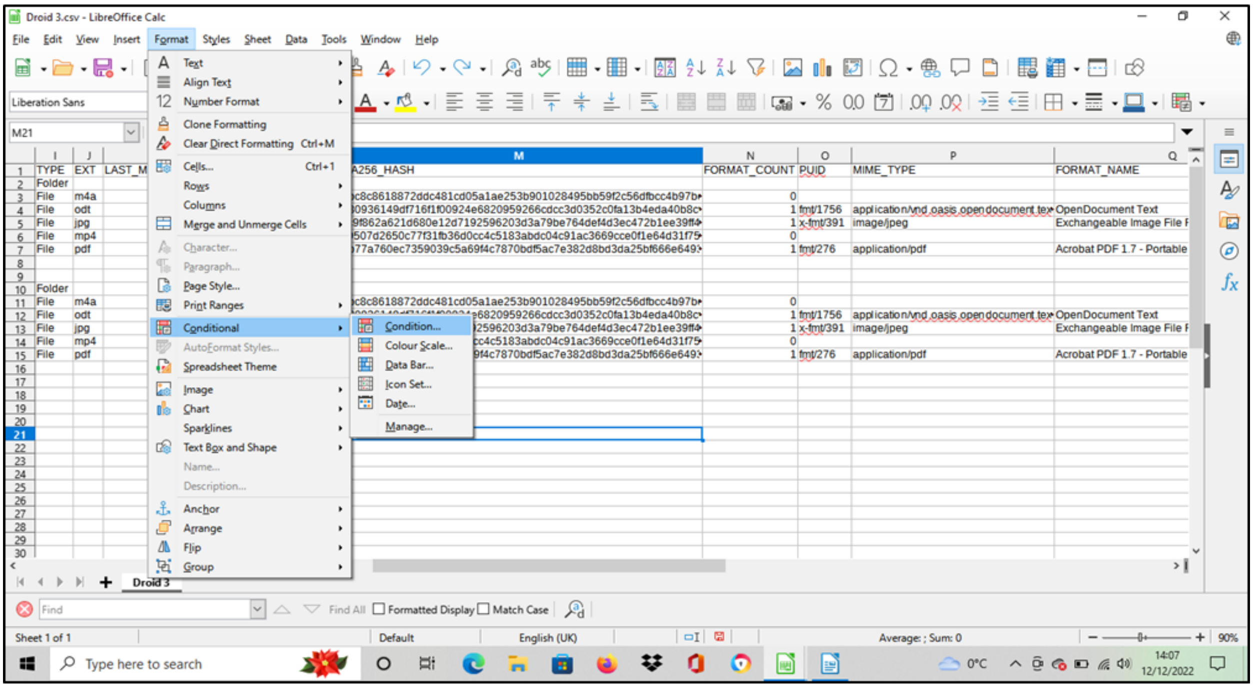
ii. Copy the selected rows (ctrl + c)

iii. Open the original Droid .csv report you saved when ingesting the files. Before anything else, save a copy of this report with a new name (e.g. Droid report_fixity working copy) to ensure that you do not lose the content of the report you generated on ingest. You can now use this working copy for any fixity checks you run in the future without fear of accidentally overwriting the original)

iv. Paste the copied rows (ctrl + v) directly under the existing entries, ensuring that the columns are aligned

v. Select column ('SHA256_HASH')

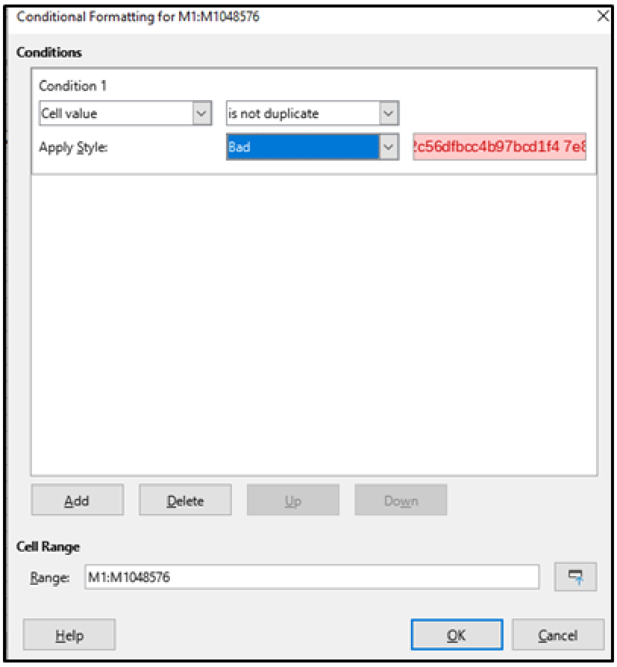
vi. Go to Format > Conditional > Condition:



	TYPE	EXT	LAST_M	A256_HASH	FORMAT_COUNT	PUID	MIME_TYPE	FORMAT_NAME
2	Folder							
3	File	m4a		c8c8618872ddc481cd05a1ae253b901028495bb59f2c56dfbcc4b97b	0			
4	File	odt		30936149df716f1f00924e6820959266cdcc3d0352c0fa13b4eda40b8c	1	fmt/1756	application/vnd.oasis.opendocument.tex	OpenDocument Text
5	File	jpg		9f862a621d680e12d7192596203d3a79be764def4d3ec472b1ee39ff4	1	x-fmt/391	image/jpeg	Exchangeable Image File F
6	File	mp4		507d2650c77f31fb36d0cc4c5183abdc04c91ac3669cce0f1e64d31f75	0			
7	File	pdf		77a760ec7359039c5a69f4c7870bdf5ac7e382d8bd3da25bf666e649	1	fmt/276	application/pdf	Acrobat PDF 1.7 - Portable
8								
9								
10	Folder							
11	File	m4a		c8c8618872ddc481cd05a1ae253b901028495bb59f2c56dfbcc4b97b	0			
12	File	odt		e6820959266cdcc3d0352c0fa13b4eda40b8c	1	fmt/1756	application/vnd.oasis.opendocument.tex	OpenDocument Text
13	File	jpg		2596203d3a79be764def4d3ec472b1ee39ff4	1	x-fmt/391	image/jpeg	Exchangeable Image File F
14	File	mp4		cc4c5183abdc04c91ac3669cce0f1e64d31f75	0			
15	File	pdf		9f4c7870bdf5ac7e382d8bd3da25bf666e649	1	fmt/276	application/pdf	Acrobat PDF 1.7 - Portable

vii. Within the condition menu:

- 'Select Cell value': 'is not duplicate'
- Select: Apply style: 'Bad':



Conditional Formatting for M1:M1048576

Conditions

Condition 1

Cell value | is not duplicate

Apply Style: Bad | ?c56dfbcc4b97bcd1f4 7e8

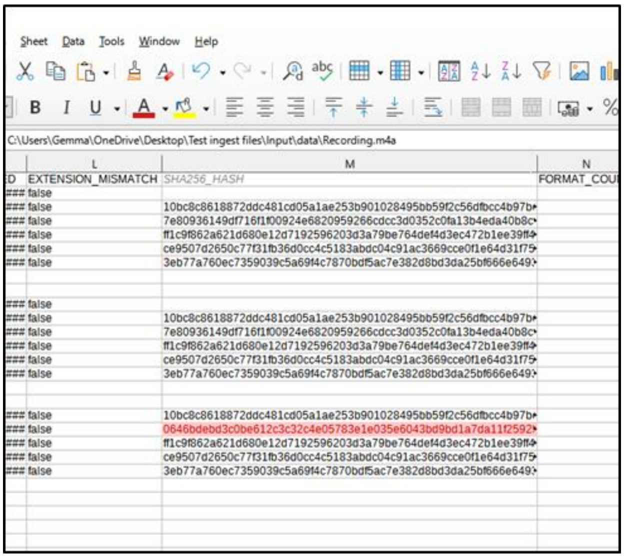
Cell Range

Range: M1:M1048576

viii. Click ‘OK’:

If none of the checksums have changed, then nothing should be highlighted within the spreadsheet.

If anything has changed within the file, and a different checksum has been generated, a cell in column M will be highlighted in red to indicate that it is different:



C:\Users\Gemma\OneDrive\Desktop\Test ingest files\Input\data\Recording.m4a

	L	M	N
ED	EXTENSION_MISMATCH	SHA256_HASH	FORMAT_COU
###	false		
###	false	10bc8c8618872ddc481cd05a1ae253b901028495bb59f2c56dfbcc4b97b	
###	false	7e80936149df716f1f00924e6820959266cdcc3d0352c0fa13b4eda40b8c	
###	false	ff1c9f862a621d680e12d7192596203d3a79be764def4d3ec472b1ee39ff4	
###	false	ce9507d2650c77f31fb36d0cc4c5183abdc04c91ac3669cce0f1e64d31f75	
###	false	3eb77a760ec7359039c5a69f4c7870bdf5ac7e382d8bd3da25bf666e649	
###	false		
###	false	10bc8c8618872ddc481cd05a1ae253b901028495bb59f2c56dfbcc4b97b	
###	false	7e80936149df716f1f00924e6820959266cdcc3d0352c0fa13b4eda40b8c	
###	false	ff1c9f862a621d680e12d7192596203d3a79be764def4d3ec472b1ee39ff4	
###	false	ce9507d2650c77f31fb36d0cc4c5183abdc04c91ac3669cce0f1e64d31f75	
###	false	3eb77a760ec7359039c5a69f4c7870bdf5ac7e382d8bd3da25bf666e649	
###	false	10bc8c8618872ddc481cd05a1ae253b901028495bb59f2c56dfbcc4b97b	
###	false	0646bdebd3c0be612c3c32c4e05783e1e035e6043bd9bd1a7da11f2592	
###	false	ff1c9f862a621d680e12d7192596203d3a79be764def4d3ec472b1ee39ff4	
###	false	ce9507d2650c77f31fb36d0cc4c5183abdc04c91ac3669cce0f1e64d31f75	
###	false	3eb77a760ec7359039c5a69f4c7870bdf5ac7e382d8bd3da25bf666e649	

A different checksum would indicate that a change to the file has occurred, and further investigation would be required to determine whether the file has been accessed and why it differs from the version of the file when ingested.

Updates

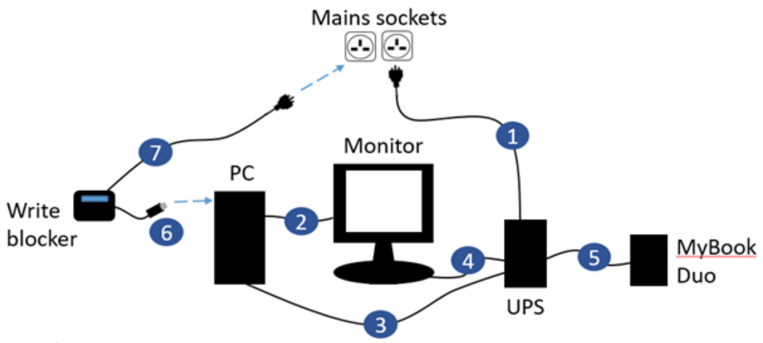
Although the workstation is designed to be used offline, particularly during the ingest process, we recommend that you connect to your Wi-Fi or LAN on a regular basis (e.g. bi-weekly or at least monthly) and perform the following updates:

- Update your AVG anti-virus definitions
- Perform any Windows updates which are available
- Update the container/signature files within Droid. If updates are available, the download will automatically be prompted when you open Droid.

Hardware setup

The below diagram shows how the hardware in the toolkit can be connected.

Cable setup



1. UPS to mains power socket
2. PC to Monitor (DisplayPort cable)
3. PC to UPS (C14 to C13 power cable)
4. Monitor to UPS (C14 to C13 power cable)
5. MyBook Duo to UPS (C14 to 13A Socket)*
6. Write blocker to PC (USB cable) – only to be connected <u>during</u> use
7. Write blocker to UPS mains socket – only to be connected <u>during</u> use

*Note: Most bundles were originally supplied with a mains cable for the MyBook Duo, but a separate cable to connect it directly to the UPS may have been supplied.