An introduction to using write blockers and *FTK Imager* software

With 2 post event updates in red

Simon P Wilson
Archives Consultant

Simon P Wilson
Archives Consultant

Agenda

1.45	Welcome and introductions
1.50 – 2.20	Introduction to write blockers and their place in the workflow
2:25 – 2:45	Walk through using a write blocker & FTK Imager software
2:45 – 3:00	Q & A
3.00 – 3:15	*Break*
3:15 – 4:15	Group split into two A) hands-on with the write blocker B) scenarios to prompt discussion on digital archives, depositors and ethics swap after 30 mins (3:45)
4:20 – 4:30	Draw the event to a close – any comments on the activities and discussion
4:30	End

Simon P Wilson
Archives Consultant

Overview – part 1

1. An introduction to write blockers
   - what exactly are they and why are they important

2. Their place in the digital preservation workflow
   - relationship between external drives, write blockers and your forensic workstation

3. Walk-through using a write blocker with FTK Imager software

There will be pauses to review/reflect and ask questions and distinct Q&A
Slides will be shared after the event (with any updates, further links etc)

Simon P Wilson
Archives Consultant

Terminology

Born-digital archives

Material originating in digital format that we wish to keep permanently

Forensic workstation

Dedicated device used for digital preservation it might include a range of tools and utilities including DROID, virus check etc

I have found that having a distinct device can also help focus attention on the digital archives tasks without the distraction of email/twitter etc

Simon P Wilson
Archives Consultant

What is a write blocker?

A write blocker is a device that sits between your media containing born-digital content and your forensic workstation

The physical device (or software) creates a one-way system allowing data to be read by the forensic workstation but **blocks data** on the media from being modified

Simon P Wilson
Archives Consultant

Why is it important?

Two key challenges with born-digital material are:

1) to safely extract the contents from removeable drives and media and to consider the contents effective at risk until we have a copy elsewhere

2) to not change the metadata that is embedded within the file as we are likely to rely on this in the future

A write blocker can help with both of these aspects

Simon P Wilson
Archives Consultant

Why is it important? (2)

Date modified – allows us to demonstrate to users the authenticity of the asset and that it hasn't changed whilst in our care (via checksum)

Consider a poem that the embedded metadata tells us was last modified 3 years after the death of the poet…?

There are situations where a write blocker is not needed – eg material is only received from internal sources on the network, or via file upload/transfer

Simon P Wilson
Archives Consultant

Built-in write protection in some media

Some media formats have built-in write protection:

3.5” floppy disk

– slide the tab to **reveal the hole** makes the disk write protected

CD-R and DVD-R

– once the data has been burnt onto the disk it effectively becomes read-only

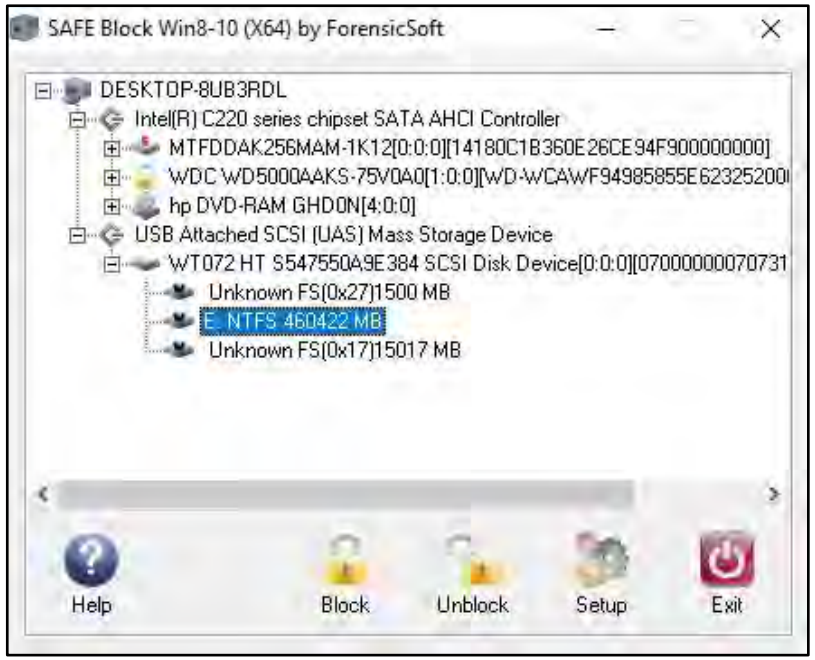
SD cards with a notched corner

– **slide the tab down** to make it write protected

Simon P Wilson
Archives Consultant

What types of write blocker are there?

SOFTWARE



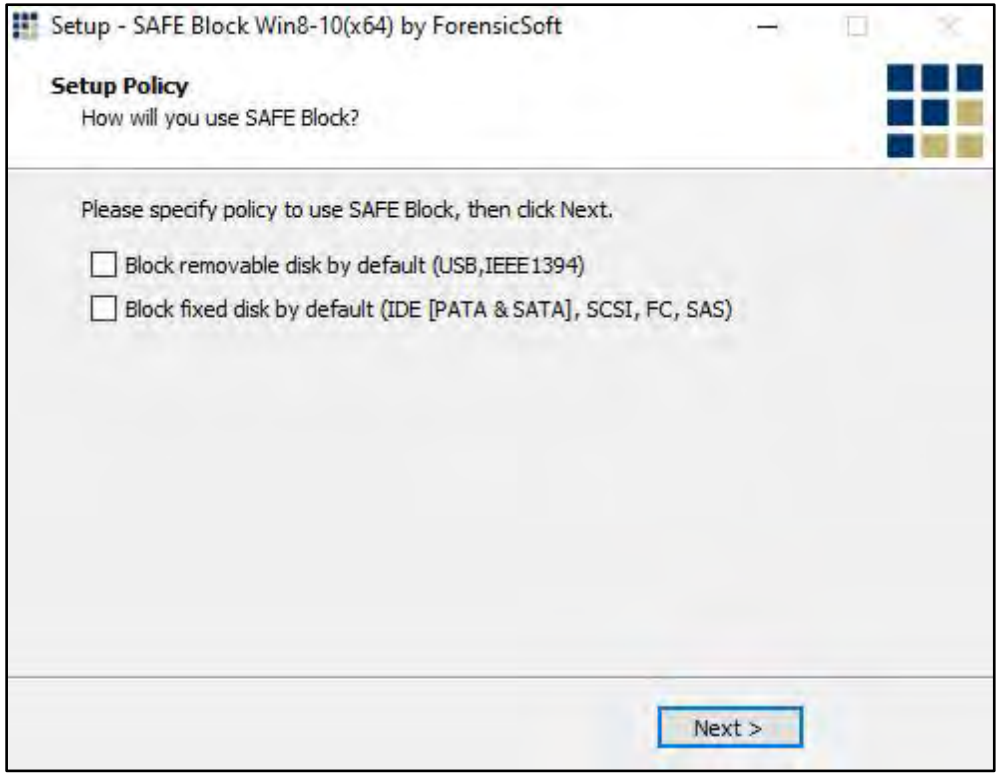
HARDWARE

Simon P Wilson
Archives Consultant

Software write blockers

ForensicSoft's *SafeBlock* software has a very simple interface. During installation you define your policy which can include blocking fixed and or removeable drives.

You also need to create a password which you need to enter **each time** you use the software



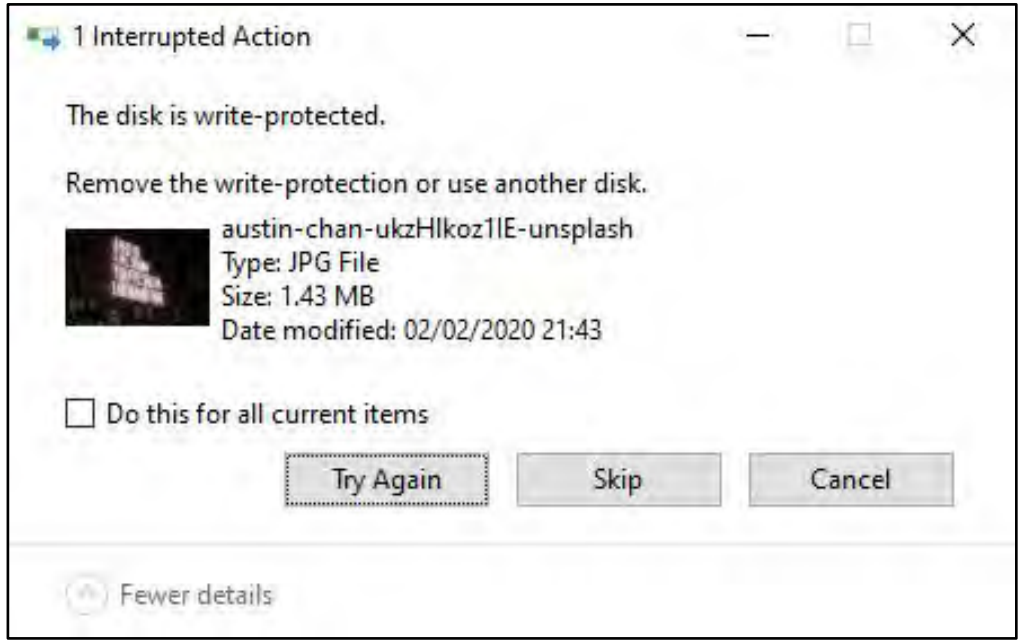
ForensicSoft™

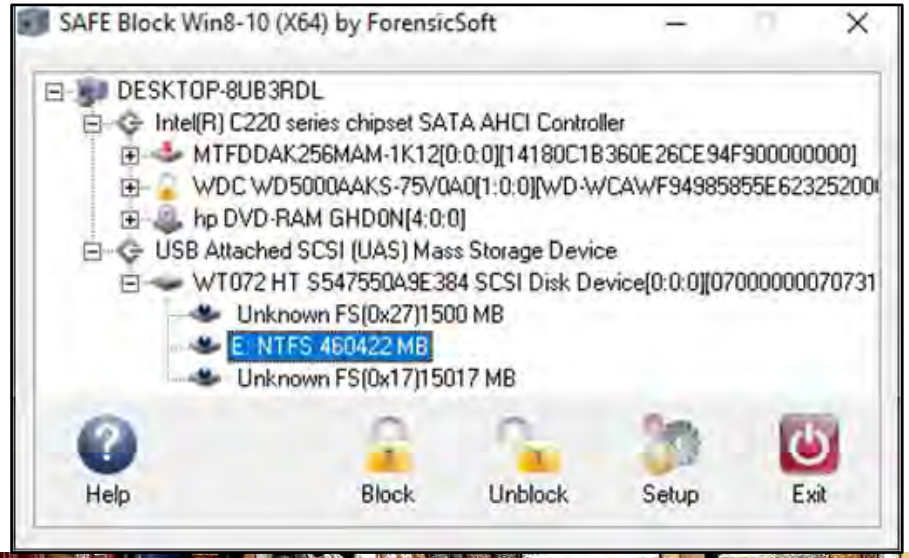
Simon P Wilson
Archives Consultant

Software write blockers (2)

You can open a file on a protected drive…

but the software blocks you from copying or saving a file to a blocked drive





You can change the settings via a simple options box, select the drive and click Block / Unblock

Simon P Wilson
Archives Consultant

Hardware write blockers

Hardware write blocker is more widely used than software option. The 2 main manufacturers are Tableau & CRU/WiebeTech.

A write blocker will support any device that has a specific type of connection - eg IDE or SATA hard drives. [IDE was introduced in 1986 but replaced by its faster more flexible cousin SATA in 2003]

The WiebeTech ComboDock v5.5 (right) works with both SATA & IDE drives and comes with all the necessary cables and connectors

Simon P Wilson
Archives Consultant

Media WriteBlocker

Write block support for SD cards, Compact Flash, USB pen drives and USB hard drives. The Media WriteBlocker (Black) supports drives upto 2TB has been replaced by USB 3.1 WriteBlocker (White) with no stated limitations.

Works the same way as the ComboDock, with a status light instead of the on-device display; light is green in write-blocked mode and amber when read/write mode.

Simon P Wilson
Archives Consultant

Media WriteBlocker (2)

A question was asked about using a media write blocker with a USB floppy disk or CD drive. When I tested this with a floppy disk and a CD drive they both **failed** to appear in Windows Explorer.

- use the built-in write protection option (tab open) for floppy disks
- with CD-Rs it is not possible to overwrite existing content, you might be able to add new content (with on-screen prompts) if there is space on the media

Simon P Wilson
Archives Consultant

Hardware vs Software – summary

	Hardware write blocker	Software write blocker
Works with….	Any device (eg IDE drive) that matches the write blocker capability	Any device that can be attached to the forensic workstation where the software is installed
Visual prompts…	Usually has a light to show when it is in use, some also have a small display screen	There is a visual element to enabling or disabling drives but not when in normal use
Use…	Widespread use by the digital preservation community	Unclear – rarely mentioned in digital preservation literature
In the future…	Purchase additional hardware to work with new connection device types	Contact software company to move license from one PC to another
Cost..	CRU/WiebeTech *ComboDock v5.6* [for IDE & SATA drives] £320 *USB 3.1 WriteBlocker* [USB, SD & CompactFlash] £320	*SafeBlock* (forensicsoft.com) £450

Simon P Wilson
Archives Consultant

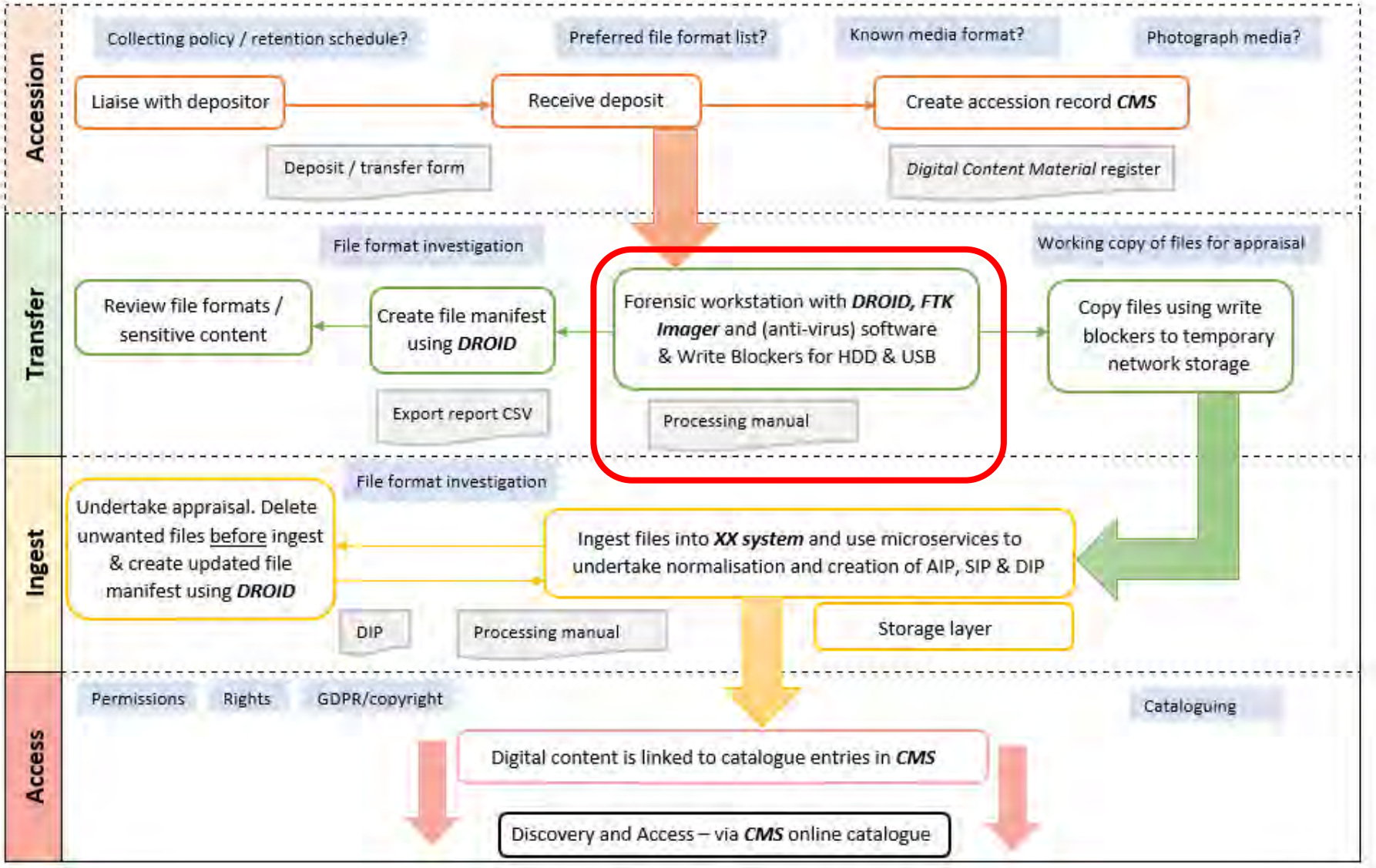
Quick recap

- Write blockers can help us to safely transfer content which must be considered “at risk” whilst it exists ONLY on removeable media
- A write-blocker may be software or hardware
- A write blocker is quite simple; lack of widespread availability seems to have magnified the uncertainty about what it does

Any questions about what we have covered so far?

Simon P Wilson
Archives Consultant

Where does it fit in the workflow?



Simon P Wilson
Archives Consultant

To use a write-blocker you will need…

1. A drive with born-digital content that you wish to add to the archives

2. A write blocker that can connect to drive and the workstation

3. Forensic workstation with appropriate ports and software

Simon P Wilson
Archives Consultant

The disappearing write blocker

With the write blocker sitting between your drive and your forensic workstation it is designed to **not be seen,** this means:

- it won't register with windows as a device in its own right

- the drive (not the write blocker) appears in Windows Explorer

Simon P Wilson
Archives Consultant

Forensic workstation

You **might** need to purchase hardware to support media formats - your audit of digital content held amongst the collections to create a digital asset register should inform this

Note media formats (eg 6 floppy disks) you can't currently read

You can then decide (based on quantity of media or importance of the collection) whether a solution is needed **<u>now or in the future</u>**

Simon P Wilson
Archives Consultant

Forensic workstation (2)

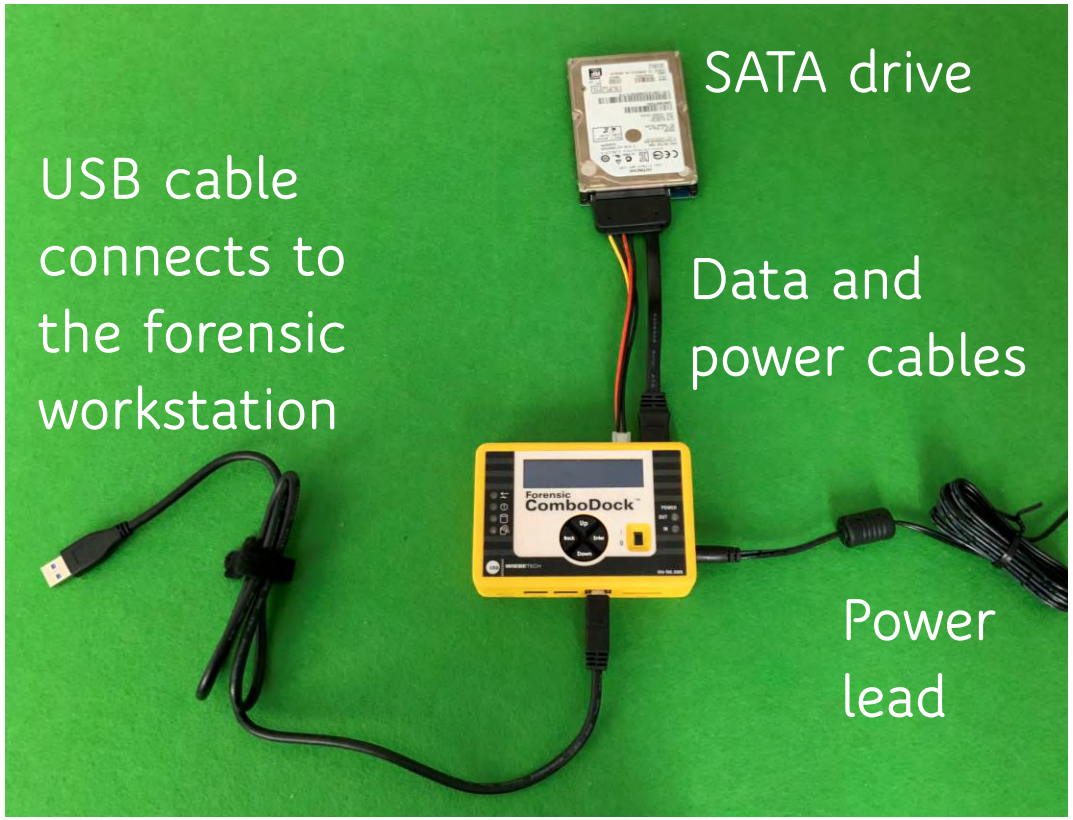
In this way the capabilities can be developed over time

Suggested core kit
– USB drive for floppy disks (currently £20-£25 on Amazon)
– USB drive for CD/DVDs (currently £15-£25 on Amazon)
– media card reader (currently £10-£15 on Amazon)

Software start with DROID and key utilities like TeraCopy, then add LibreOffice, Audacity (for audio), VLC/Handbrake (for video) etc

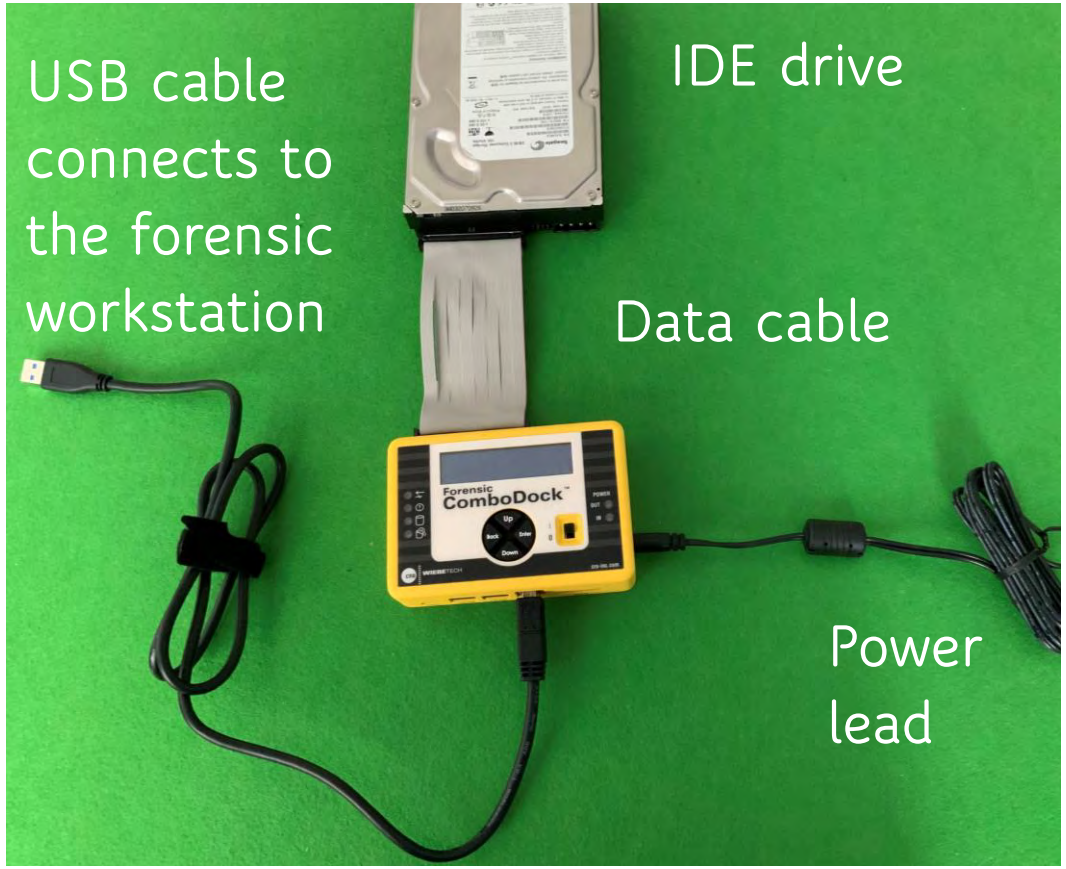
Simon P Wilson
Archives Consultant

ComboDock – with SATA hard drive



Simon P Wilson
Archives Consultant

ComboDock – with IDE hard drive



Simon P Wilson
Archives Consultant

ComboDock menu

1. Connect and turn-on power
2. Write blocker menu shows key information:

Mode: write-blocked

Drive Info: manufacturer, serial number, drive capacity (MB) etc

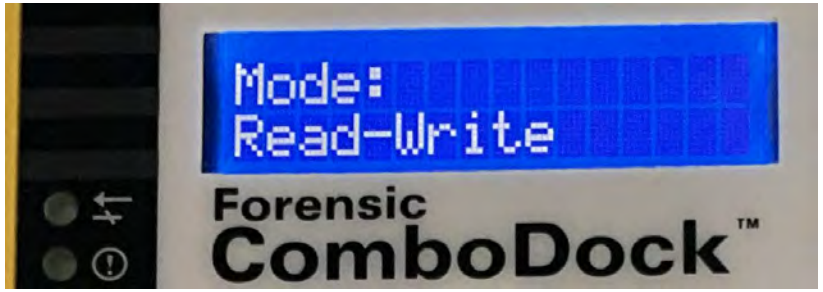
You navigate the menu using Back, Up & Down, use Enter to confirm your choice (eg Mode)

Simon P Wilson
Archives Consultant

Write block & read-write modes

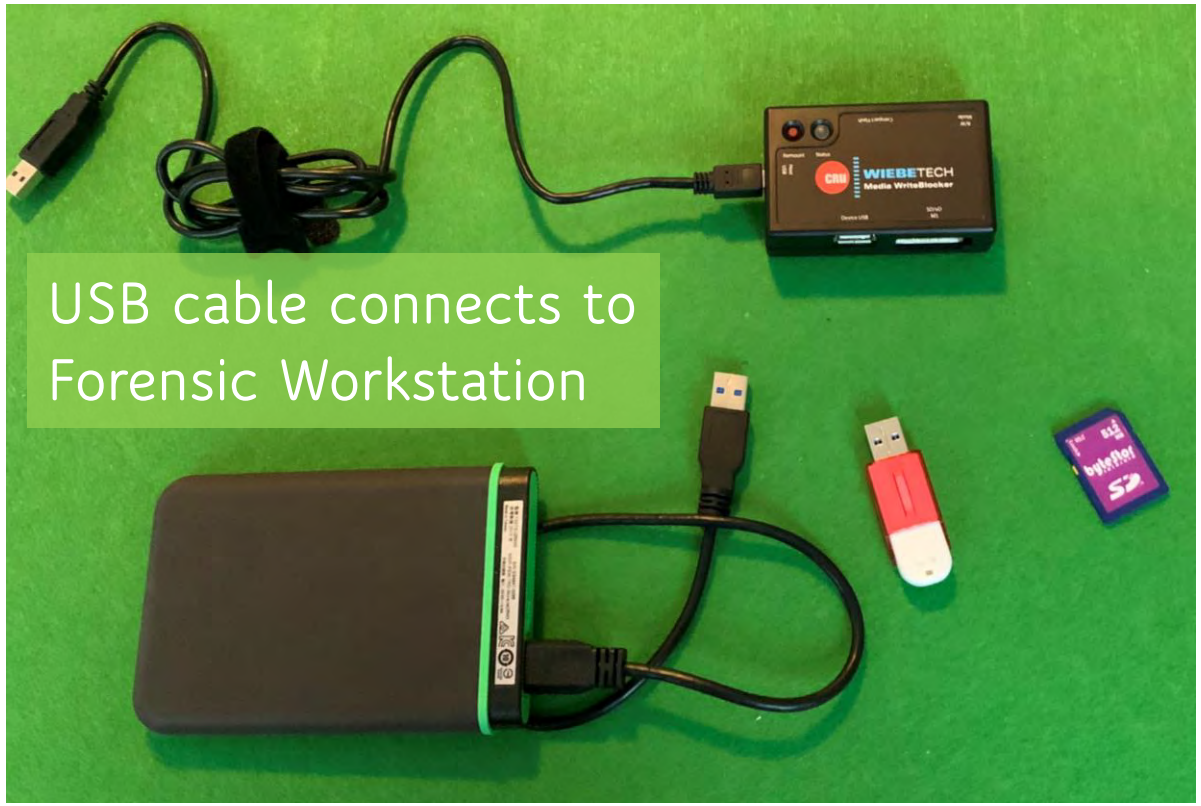
The ComboDrive supports two modes
- write-block AND read-write

write block is always the default
- <u>you can’t accidentally use read-write</u>
- top light – write block mode



Simon P Wilson
Archives Consultant

Media WriteBlocker



USB cable connects to Forensic Workstation

External hard drive

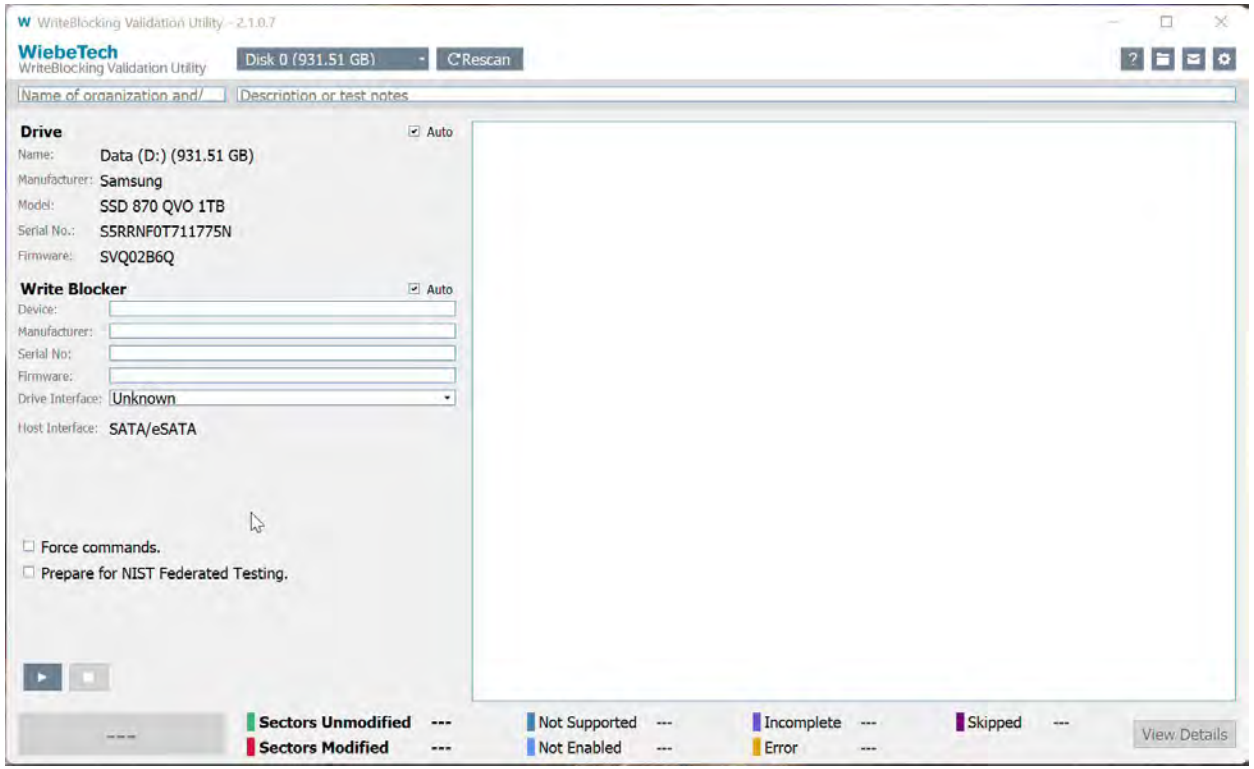
Simon P Wilson
Archives Consultant

Validation utility – test the write blocker

Free utility to test that the write blocker

1. Connect a drive to the write blocker and the write blocker to the forensic workstation
2. Run the utility – this scans the drive and produces very clear PASS / FAIL message (bottom left)

Use an old drive with some sample data

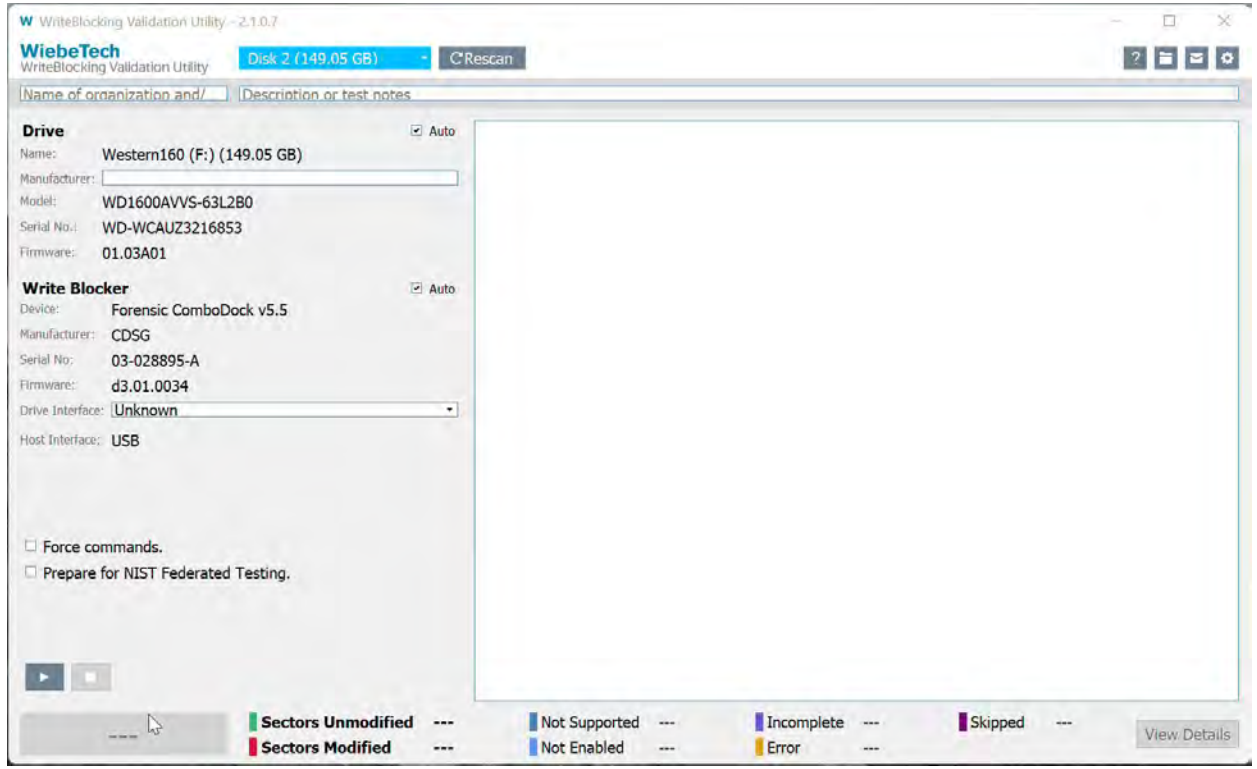


Simon P Wilson
Archives Consultant

Validation utility – write blocker fails

I was able to engineer a fail [as expected]

1. Connect a drive to the write blocker and the write blocker to the forensic workstation
2. Change Mode to read/write and confirm yes when prompted
3. Run the utility – this scans the drive and produces very clear PASS / FAIL message (bottom left)



If you are repeating this – use an **old drive** not one with archival content on.

Simon P Wilson
Archives Consultant

Quick recap

- Write blockers connect to drive(s) in an almost foolproof manner with different drives having different connectors
- With external drives you need to connect data & power cables
- Confidence comes with repetition – use an old drive with sample data; keep getting the same results **then** document the process

Any questions from what we have just looked at?

Simon P Wilson
Archives Consultant

Practical tasks using a write blocker

Let's now look at a range of digital preservation tasks we might wish to undertake on an external drive

- Extent (Number of files & total MB/GB/TB)
- Browse files and folder structure
- Open file(s)
- Review content for appraisal purposes
- Copy a selection of files/folders onto PC
- Logical image (visible files)
- Physical image (entire drive)

Simon P Wilson
Archives Consultant

Preparatory steps (each/every time)

Lets look at the first 3 steps (and avoid re-stating this every time)

1. **Get your hardware in place:** I tend to arrange everything in a chain; this is how I think of the process (drive > write blocker > forensic workstation) it ensures space for the drive and its associated data and power cables

2. **Connect all of the devices/cables:** then switch-on PC then the write blocker

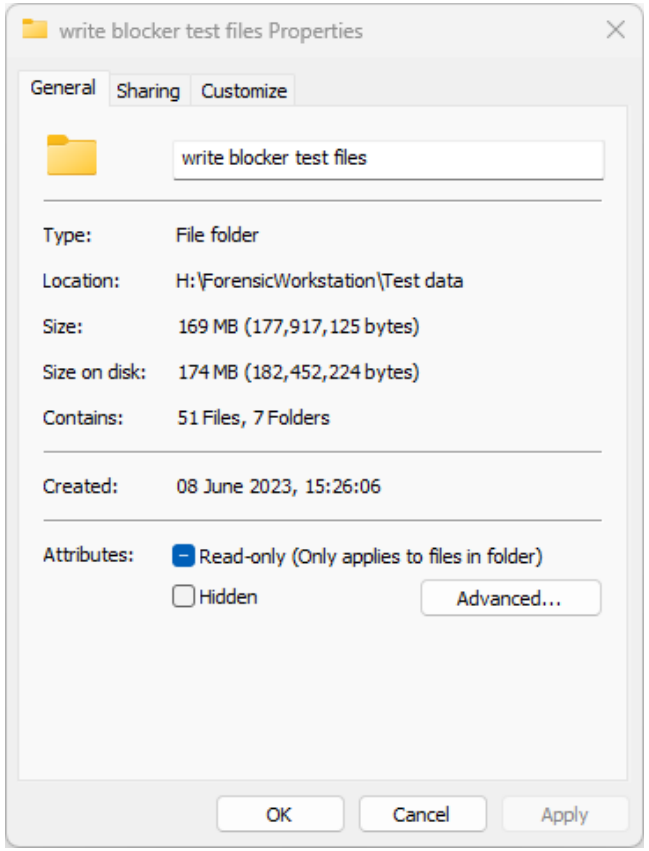
3. **Test the write blocker:** especially if it is some time since we last used it

Simon P Wilson
Archives Consultant

Practical tasks: files/extent information

An important part of securing intellectual control of digital assets that are held by the archives is through the audit / digital asset register.

With the drive connected to the forensic workstation via the write blocker we can use Windows Explorer to look at the folder properties to get the information we need.



Simon P Wilson
Archives Consultant

Practical tasks: browse files/folder structure

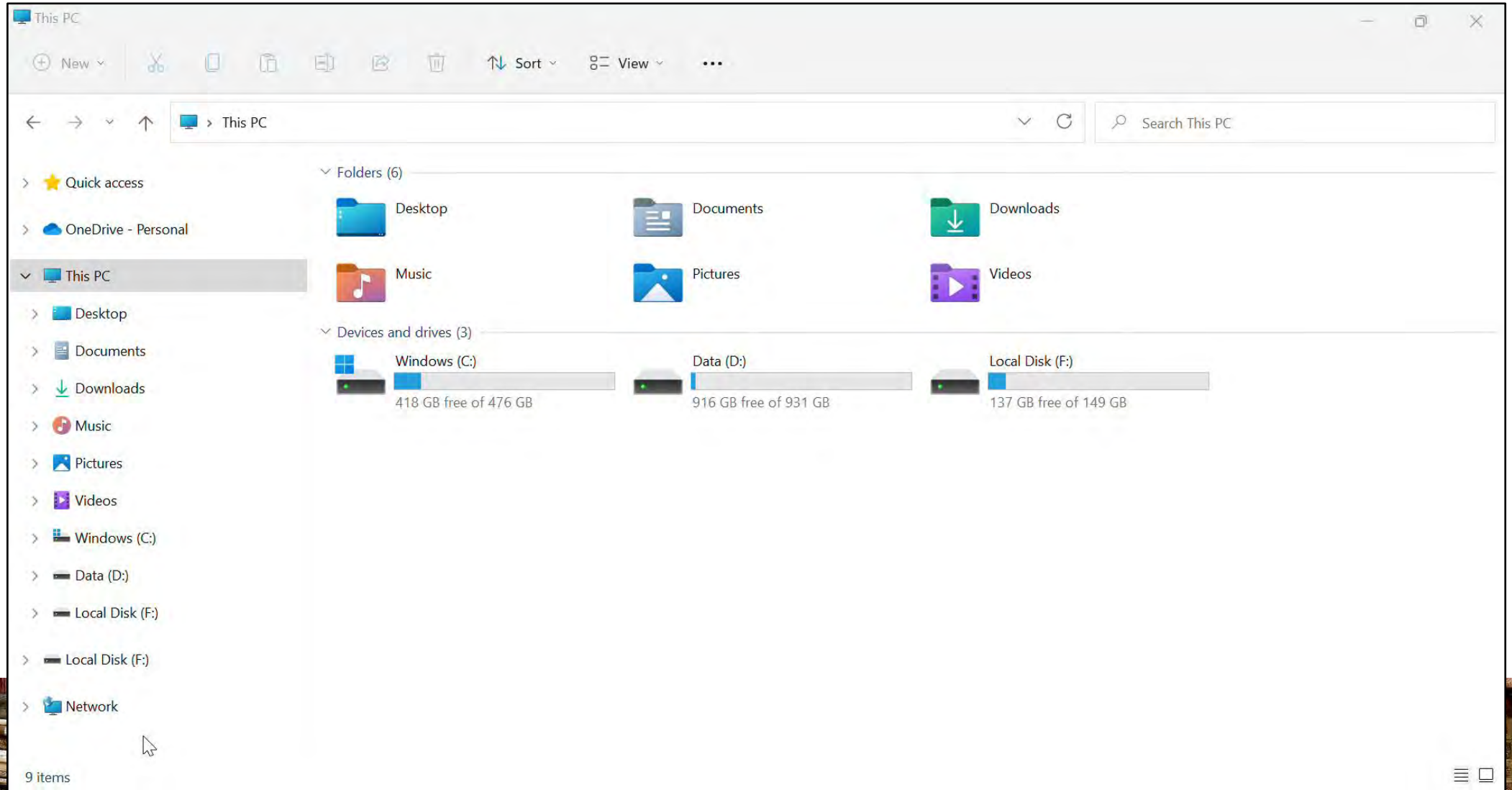
Another priority is to check the drive – does it contain what you thought?

An initial review is similar to what we'd do with a physical collection – a quick look whilst we re-pack items into archive boxes.

With the drive connected to the forensic workstation via the write blocker we can use Windows Explorer to browse the folder structure to see how the folders are arranged, whether file-naming practices are good/meaningful (or not) etc

Simon P Wilson
Archives Consultant

Practical tasks: browse files/folder structure



Simon P Wilson
Archives Consultant

Practical tasks: open files/appraisal review

So as we have just seen you can open some files (depending on the formats and the software on the forensic workstation). I recommend that for a considered review you copy the content from the drive onto the forensic workstation (this is why we are using the write blocker).

I'd create a second copy and use this to review the content (you don't need the write blocker to be attached). You can be quicker, more inquisitive knowing that once the process is complete you can simply delete the material.

Simon P Wilson
Archives Consultant

Practical tasks: copy a selection of files

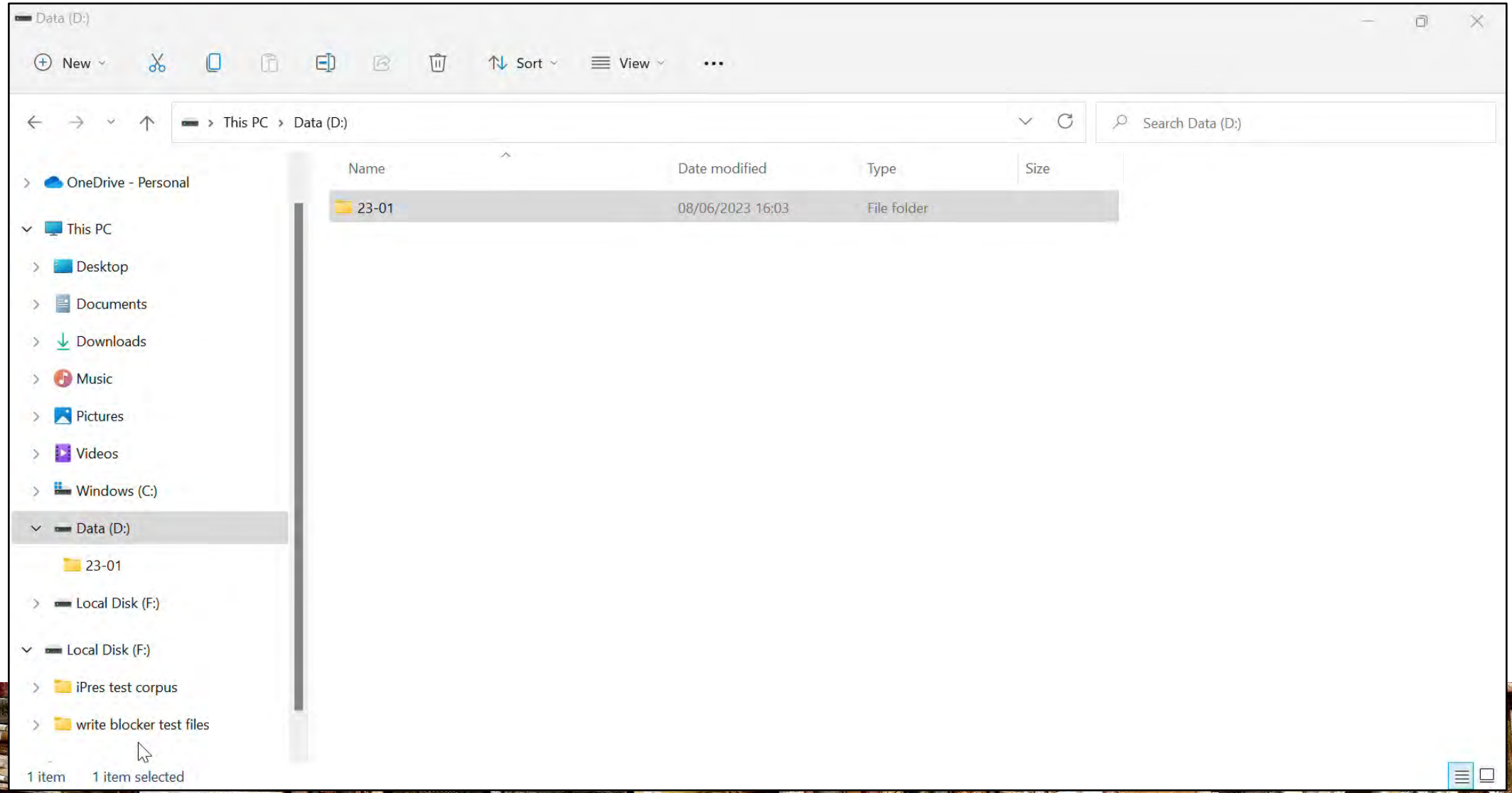
It is highly likely that you will want to copy a selection of files from the drive - whether it is for preservation purposes or a sample of files to review/appraise.

With the drive connected to the forensic workstation via the write blocker we can use Windows Explorer to copy files from the drive to the forensic workstation.

I would recommend using TeraCopy instead of Windows Explorer. This free utility can copy content – but crucially it can verify the files it has copied are identical (through checksum comparison of the original and the copied files).

Simon P Wilson
Archives Consultant

Practical tasks: copy a selection of files



Simon P Wilson
Archives Consultant

Practical tasks: logical/physical image

There are some tasks that do require more specialist software

- a **logical image** will capture the visible files ONLY
- a **physical image** is a byte for byte exact duplicate, so this captures the visible files AND any deleted files which haven't yet been over-written

A logical image is usually sufficient – might be reasons to capture a physical image

FTK Imager (Exterro purchased AccessData in 2020) & Autopsy (Basis Technology).
I use FTK Imager but take a look and see what suits your particular needs

Simon P Wilson
Archives Consultant

FTK Imager

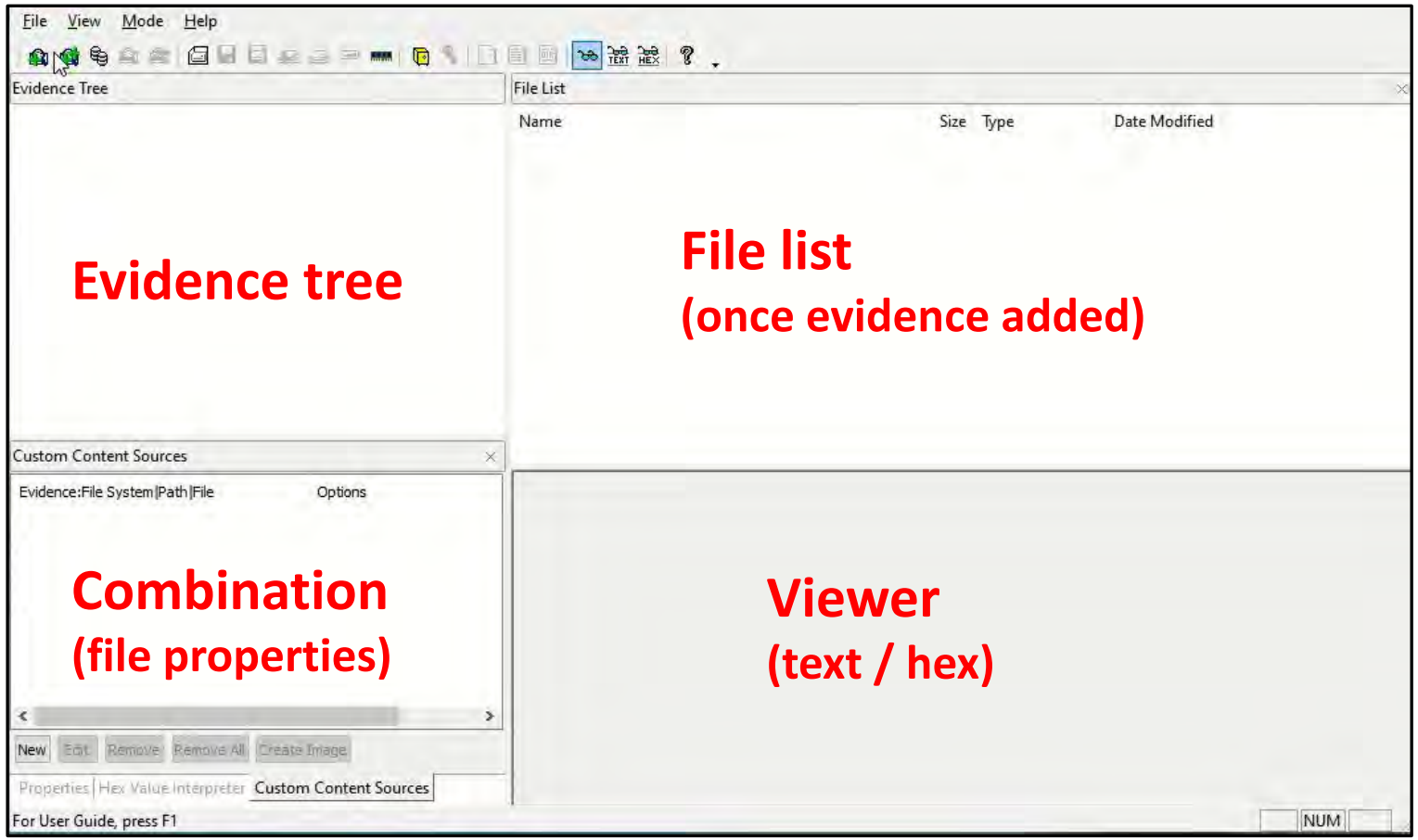
FTK Imager is a free component of a professional digital forensic tool (Forensic ToolKit costs about £3k per license)

FTK Imager can be used for the following tasks:

1) selected file(s)/folder(s)
2) logical drive (ie the visible files)
3) a physical image (complete byte for byte copy of a drive)
4) open an image file previously created
   including *.AD1 (logical image) and *.E01 (physical image)

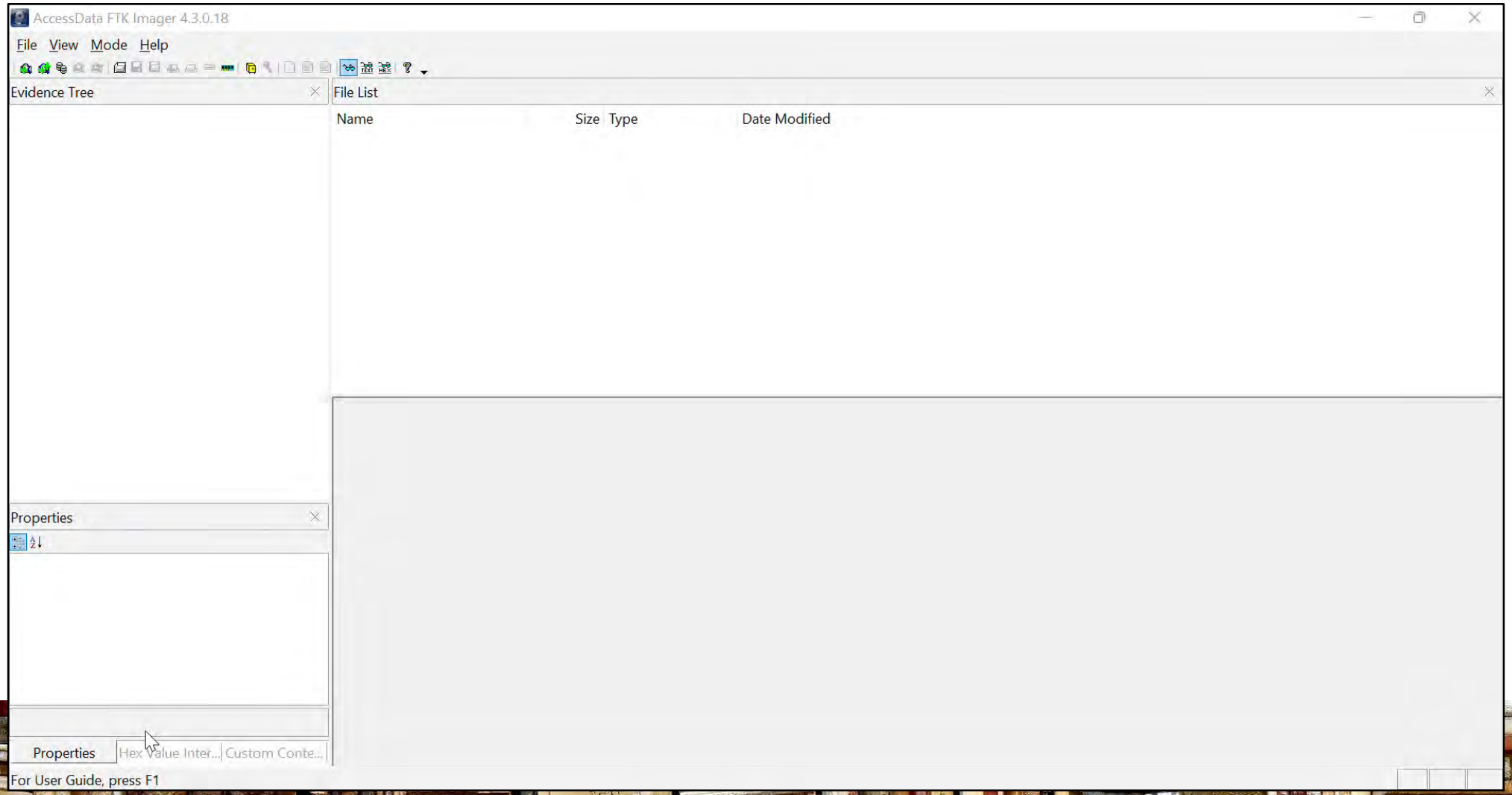
Simon P Wilson
Archives Consultant

FTK Imager interface – 4 panes



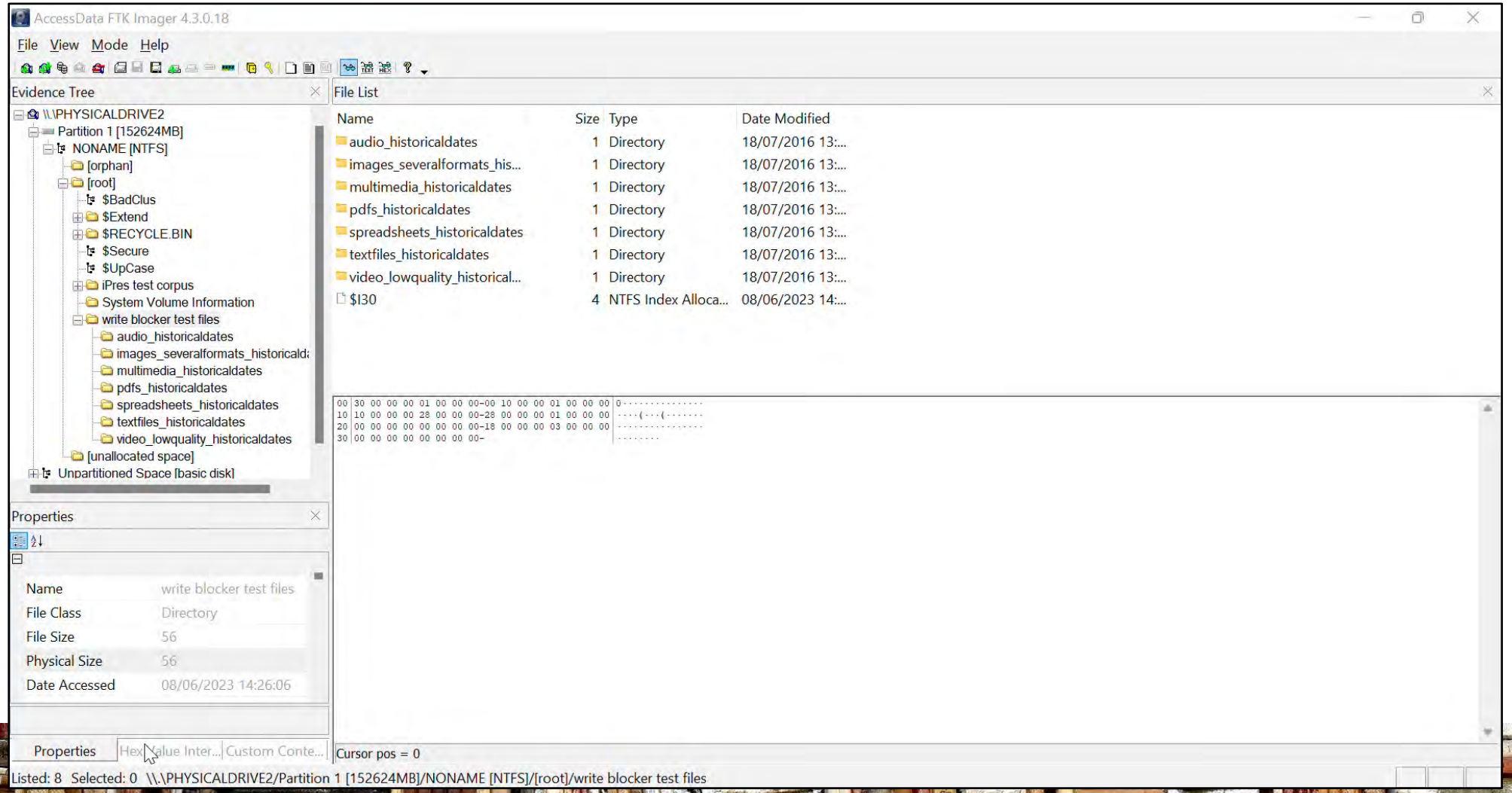
Simon P Wilson
Archives Consultant

Practical tasks: add evidence in FTK Imager



Simon P Wilson
Archives Consultant

Practical tasks: physical image



Simon P Wilson
Archives Consultant

Practical tasks: return to an image file

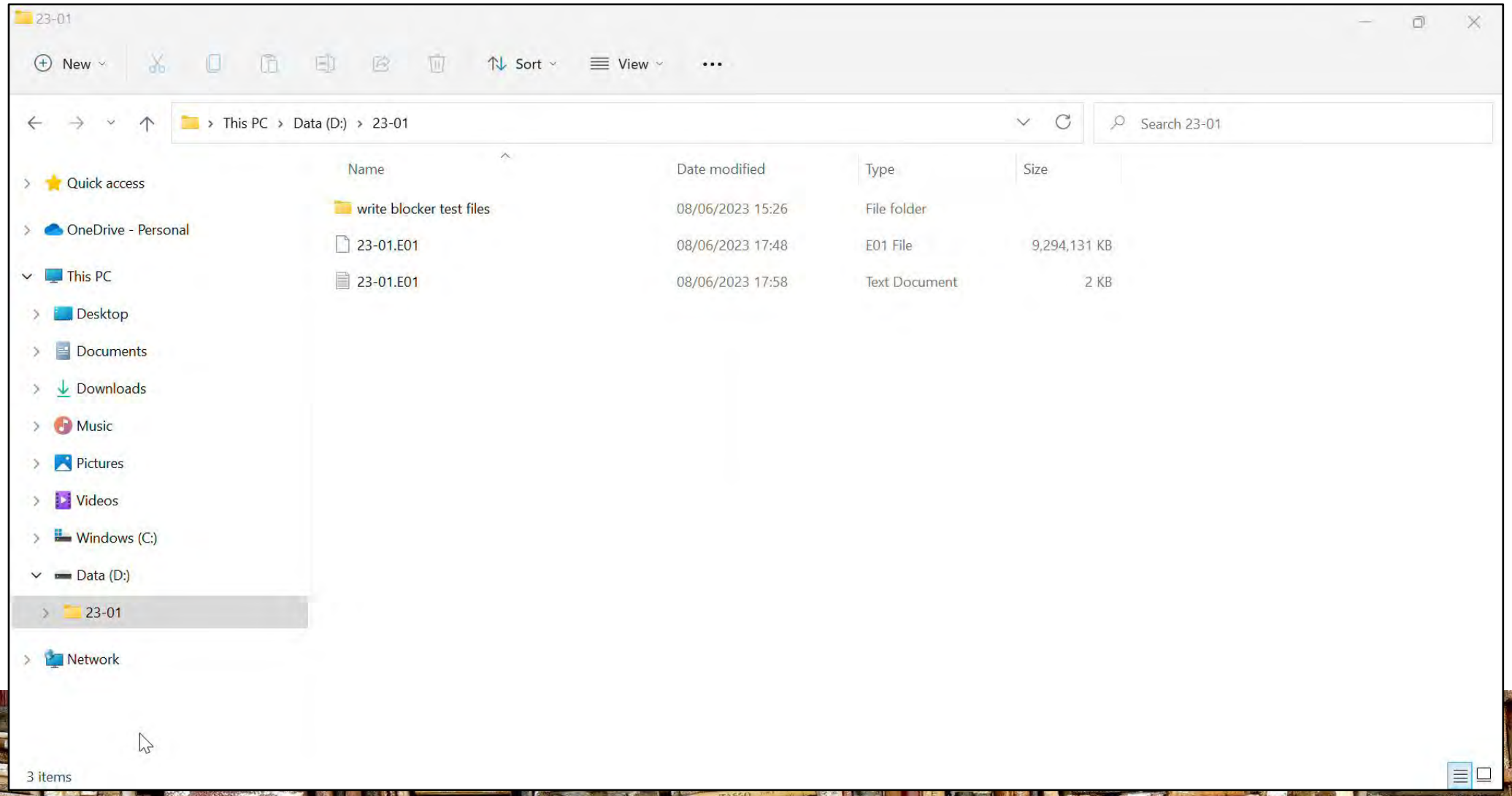
Once you have a logical image or physical image file you can look at the contents of the drive **without the physical drive or the write-blocker needing to be attached**.

Wrapping the files into a logical or physical image file does make them easier to move between devices / drives etc

Archivematica and *Preservica* can both handle the import of disk image files as part of the ingest workflow

Simon P Wilson
Archives Consultant

Practical tasks: open existing image



Simon P Wilson
Archives Consultant

Which tool for which task (summary)

	Windows Explorer	TeraCopy	FTK Imager
Extent (Number of files & total GB/TB)	✓	n/a	(Number of files: select folder, details in properties pane)
Browse files and folder structure	✓	n/a	✓
Open file(s)	✓	n/a	Can view some files
Review content for appraisal purposes	✓	n/a	Not easily
Copy a selection of files/folders onto PC	✓	✓ (+ verify checksums)	Select folder, right click and select Export files
Physical image (entire drive)	✘	✘	✓ (+ file list)
Logical image (visible files)	✘	✘	✓ (+ file list)

Simon P Wilson
Archives Consultant

Digital archives & ethics

It can be difficult to discuss digital archives with depositors – the conversation can be so intrusive when we ask about:

- the software they use (to identify potential non-standard file formats)
- the identities (on social media platforms) they may have
- whether any of the content is sensitive (GDPR) / password protected

Simon P Wilson
Archives Consultant

Digital archives & ethics (2)

When faced with a hard drive we have two distinct options:

– to take a logical image (visible files) or a physical image (byte for byte)

However how do we broach the subject of digital forensics and the fact that we might be able to restore delete files without causing alarm?

It is not easy to highlight the ability to restore deleted files so it may be easier to say that the policy will be to create a logical image – that is the visible files

Simon P Wilson
Archives Consultant

Final recap / Q&A

- We have covered a lot – what a write blocker is; taking a look at both the software and hardware varieties; we have seen where it fits in the digital preservation workflow and a range of tasks we can do

- We have also taken a brief look at one ethical question that arises from extracting content from a physical drive

Any specific (or tangential) questions?

Simon P Wilson
Archives Consultant

break

Simon P Wilson
Archives Consultant

Overview – part 2

Group split into two

A) (Simon) hands-on with the write blocker – take a closer look

B) (Elizabeth) scenarios to prompt discussion on digital archives, depositors and ethics

swap after 30 mins

We will come together briefly for any final questions etc

Simon P Wilson
Archives Consultant

A few take aways (hopefully)

A write-blocker can play a critical role in your digital preservation workflow and can be used with free software like TeraCopy and FTK Imager. You can download test files to play with and hard drives are cheap on ebay (160GB drive currently £3.99).

Some interesting ethical issues but working with digital archives has many similarities with working with analogue material. What would I do if it was a paper file??

Playing with hardware, tools and files really really helps build your confidence
- then capture the decisions and the process for your workflow and documentation

Simon P Wilson
Archives Consultant

Useful links

CRU/WiebeTech - see https://wiebetech.com/products/#DriveDocks_and_WriteBlockers
Validation utility - see https://wiebetech.com/software/writeblocking-validation-utility/
UK stockist of **Tableau** write blockers – see https://avatu.co.uk/collections/tableau

Autopsy – see https://www.autopsy.com/
FTK Imager 4.7 – see https://www.exterro.com/ftk-imager
TeraCopy – see https://www.codesector.com/teracopy
Test files - https://github.com/digipres/awesome-digital-preservation#find-test-files

DPC – Handbook https://www.dpconline.org/handbook and the Technology Watch series https://www.dpconline.org/digipres/discover-good-practice/tech-watch-reports always a good place to start

Contact me

Simon Wilson
Archives Consultant

Tel: 07946 415594
Email: simon@simonpwilson.com

linkedin.com/in/simonpwilson-archivist

twitter.com/simon_archivist