Disk Imaging: FTK Imager

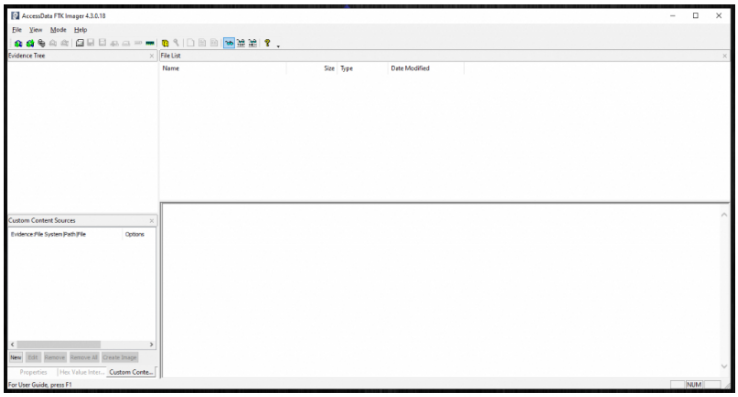
In this lesson, we're going to show you how to use FTK Imager to collect forensically-sound copies of hard drives, which can later be analyzed to retrieve evidence. If you have a spare USB laying around, we recommend students download the tool and try to take a forensic copy of the data on their USB while it is inserted into their laptop or desktop PC. Obviously this isn't how security teams and law enforcement take copies, but it will give you a chance to understand how the tools function for yourself.

FTK Imager is an extremely powerful tool, and is used in real-world investigations by investigators and security teams. Let's cover some of the features quickly:

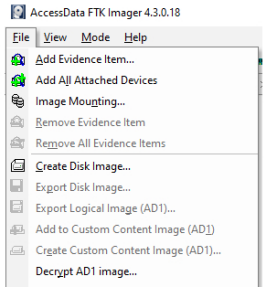
- **Dumping RAM** and storing it in a `.mem` file, so we can output it to other tools such as Volatility for analysis purposes.
- **Taking forensically-sound disk images** that can be analyzed in tools such as Autopsy.
- **Export files** directly from disk images.
- **Generate MD5 and SHA1 hashes** for evidence files.
- **Provide a read-only view** of the contents of a disk image, exactly how the user would have seen it.
- **And lots more!**

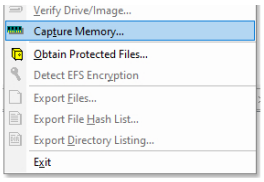
DUMPING MEMORY

Once we've installed FTK Imager and loaded it up, we're presented with this display:

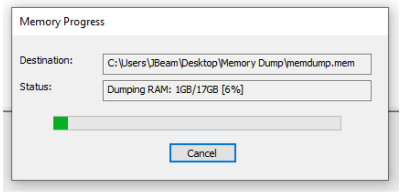


The first thing we want to show you how to do, is taking a snapshot of RAM from the system we're running FTK Imager on. To do this, we go to **File > Capture Memory**.





We are then prompted to enter a location for the file to be saved to, so we've created a new directory on our Desktop named "Memory Dump". We can change the filename if we want, but in this example, we'll leave it as "memdump.mem". As covered earlier in this domain, pagefile may contain additional evidence, but we will not include it in this walkthrough. And at the bottom, we have the option to create an AD1 file – the signature filetype for The Forensic Toolkit (TFK), another tool developed by AccessData. We will leave both of those options un-checked, and click "Capture Memory". FTK Imager will now get to work dumping everything from the RAM, and storing it in a .mem file.

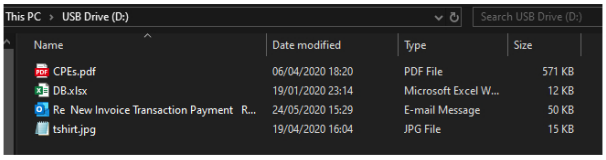


Once it's completed, we'll now have a memory file in our designated destination. We can use tools such as Volatility to analyze this dump, but we'll cover that in a future lesson.

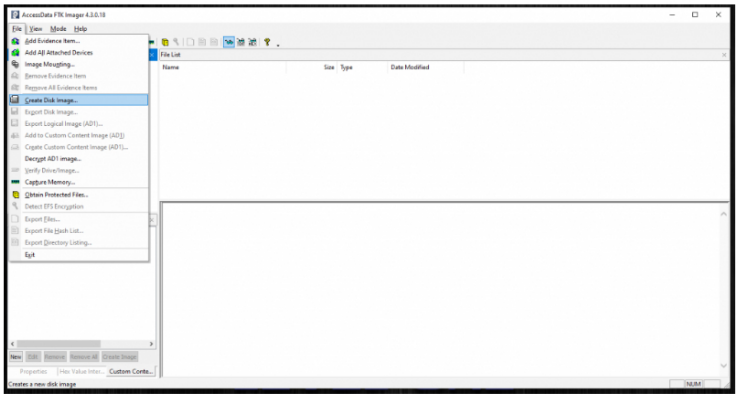
HARD DRIVE IMAGING

In the real world, a hard-drive gathered from a crime scene will be connected to a forensic workstation (a PC with high-end hardware to allow for faster analysis and data transfer) with a clean hard-drive attached. A write-blocker will be used between the workstation and the suspect hard-drive, preventing the workstation from accidentally changing anything on the hard-drive, which could lead to evidence being dismissed for tampering. The forensic analyst will then start a bit-by-bit copy of the suspect's hard-drive to the blank one. This can take an extremely long amount of time, as it is an exact copy of every piece of data so that nothing is missed.

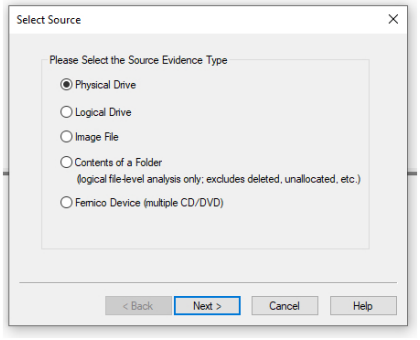
We can create a system image file (`.img`) using FTK Imager, which we can then analyze to search for digital evidence. For this example, we're going to be taking a disk image of a 15 GB USB drive we have. For demonstration purposes, we've put some random files on the USB.



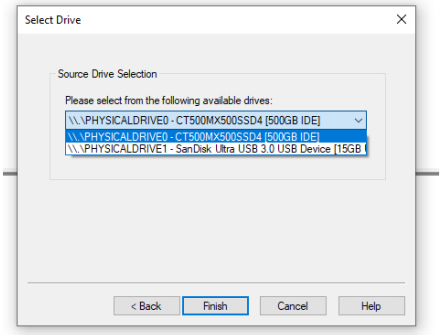
Within FTK Imager, we want to click on **File**, then go to **Create Disk Image**.



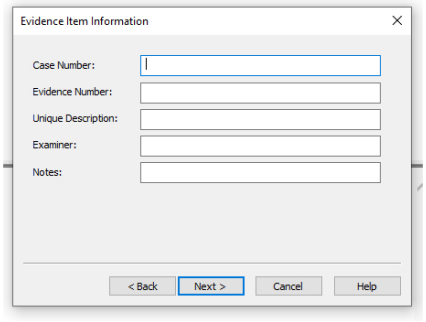
Next FTK Imager will ask us what the source of the evidence will be. As we are taking a copy of the data from a USB drive, we need to select **Physical Drive**.



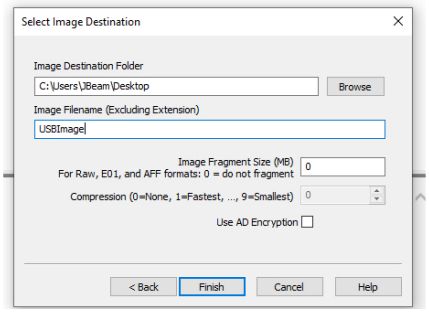
As we have selected Physical Drive, FTK Imager will now ask us to select which of the drives that are currently attached to the system running the tool. In the drop-down, you can see the 500GB SSD, and the 15GB USB. We need to select the USB drive.



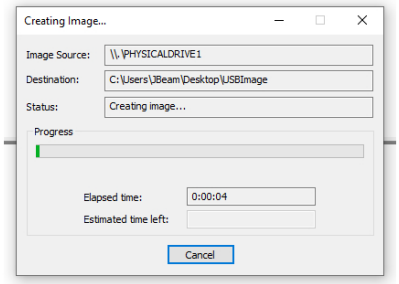
Next, we will be prompted for Evidence Item Information. This is great to follow the Chain of Custody and ACPO Principles, however, as we are doing this as an example and not a law enforcement or incident response investigation, we can leave this information blank, and click **Next**.



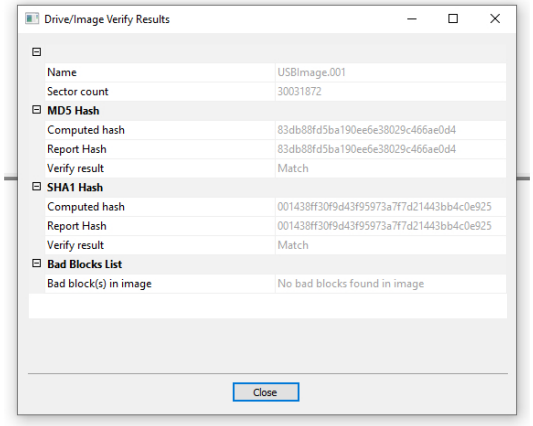
Now we have to assign an output destination, and the file name we want our disk image to have when exported from FTK Imager. We want the `.img` file to be named USBImage.img, and be placed on our Desktop. We also want to set the Image Fragment Size to 0MB – this means that the disk image won't be split into smaller segments, as we want it all in one file.



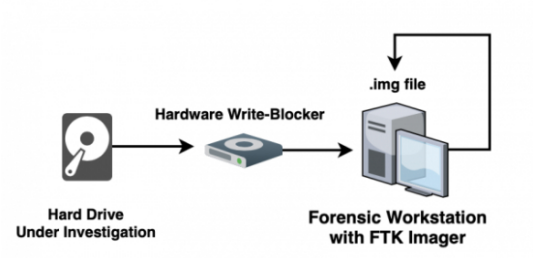
After we click Finish FTK Imager will get to work, copying over every single bit of data from the USB to our hard-drive.



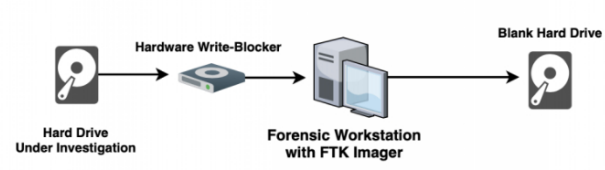
For this example, it completed quickly, as the total space of the USB is 15GB. It is also a brand new USB, meaning that there isn't existing data on it that has been deleted but hasn't yet been overwritten (remember our Hard Drive Basics lesson, where we mentioned that deleted data is still on the disk!). If you were taking a copy of a 1TB hard drive that has been used for a year, it's going to take a very long time. Once FTK Imager has finished taking the copy, the below window will popup, comparing file hashes to ensure that the copy is forensically sound.



So how does this work in the real world? The below diagrams demonstrate how a forensic analyst or law enforcement officer would take a forensic copy of a hard drive that is under investigation. The first diagram shows how a hard drive is copied to make a .img file that remains on the forensic workstation.



The second diagram below, shows how FTK imager can be used to write the contents of the hard drive under investigation to a blank hard drive.



Want to practice with FTK Imager? You can try imaging an old USB drive, or when selecting the Source Evidence Type you can make copies of folders using the "Contents of a Folder".

Previous Topic

Mark Complete

Next Topic

Back to Lesson