Division of Information Technology & Sciences
Department of Computer & Digital Forensics
FOR 120– Introduction to Digital Forensic Analysis

Creating Virtual Hard Disks

Overview:

The lab consists of four tasks. The objective of the lab is to create virtual hard disks to simulate real hard disks. Using VHDs is much easier than real hard disks for our labs, so we will be using the virtual hard disks as an evidence drive or storage device.

Notes:

1. You are required to provide screenshots of any step performed during the Lab. Screenshots should clearly show any step used and its results. This could be done using a tool such as the “Snip and Sketch” tool, to highlight your work.
2. A thorough explanation and analysis are required to demonstrate your understanding of all steps that you performed.
3. Submission rules: please submit all answers to Canvas.

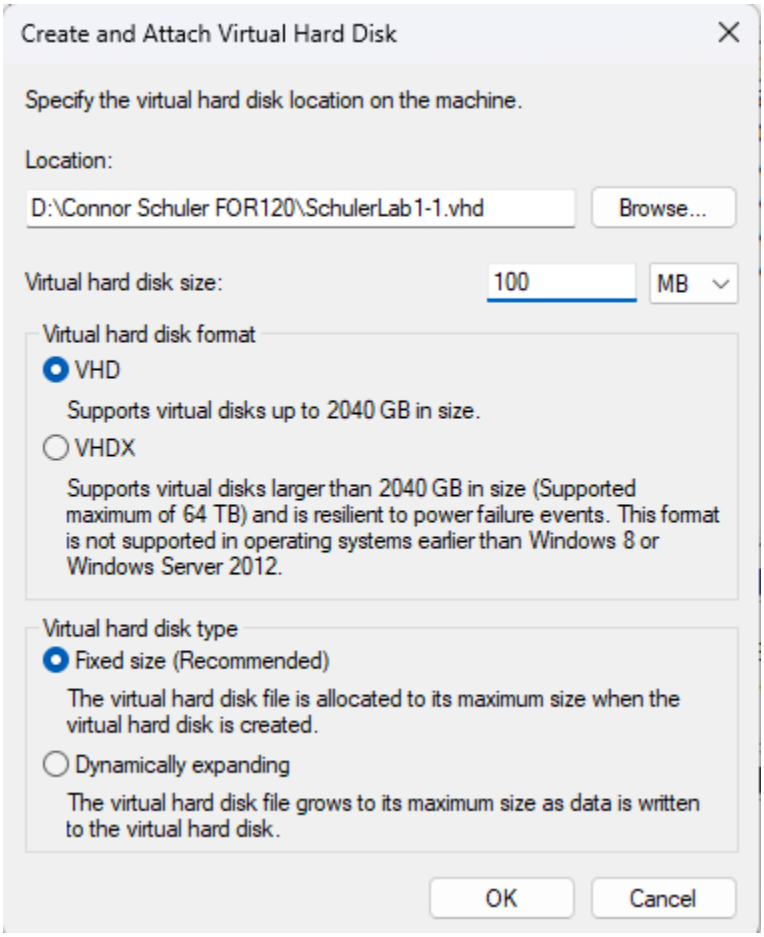
Required Tools:
Disk Management utility in Windows

**The VHD that you create in this lab will be used in next labs as well, so remember their path, so you do not repeat these steps again.

Task #1 – Creating an NTFS Virtual Hard Disk (VHD) - Evidence #1

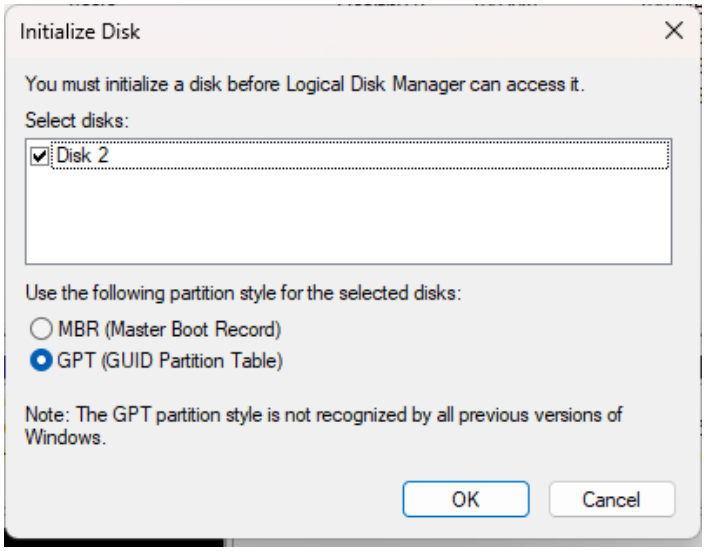
Create a virtual hard disk as follows (Disk Management > Action > Create VHD):

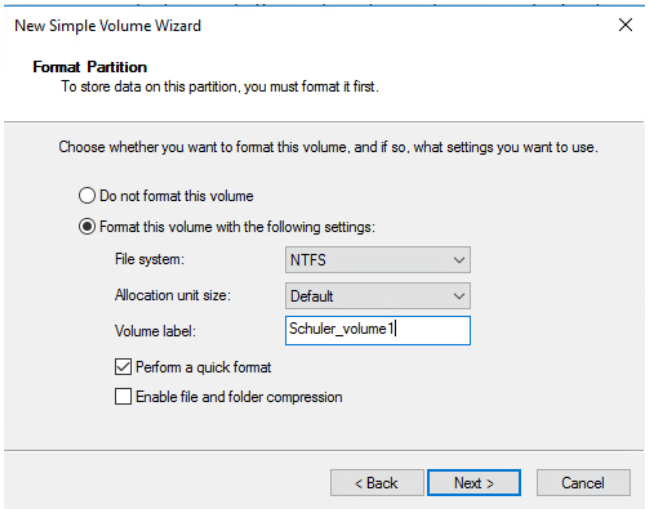
Image shows the create virtual disk menu for a fixed size VHD file. Its specifies the path of the VHD as on the D: drive is a folder called "Connor Schuler FOR-120"



1. The VHD size is 100 MB
2. Call the volume as follows: YourLastName_evidence1
3. Format the VHD into an NTFS file system
4. Add some files to your VHD: images, documents, and PDFs

The first image shows Disk 2 (disk 3 technically but numbering starts at 0), being initialized with GPT partitioning. Image 2 shows the disk being quick formatted with a single NTFS volume called "Schuler_volume1."

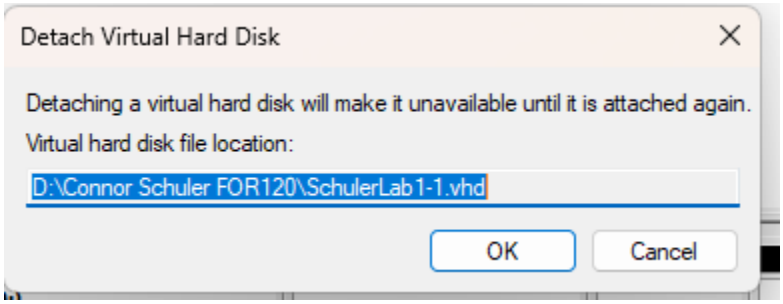




Task #2 – Detaching a VHD

1. Detach the VHD that you have created in task #1

Images shows a VHD being detached, Its specifies the path of the VHD as on the D: drive is a folder called "Connor Schuler FOR-120."

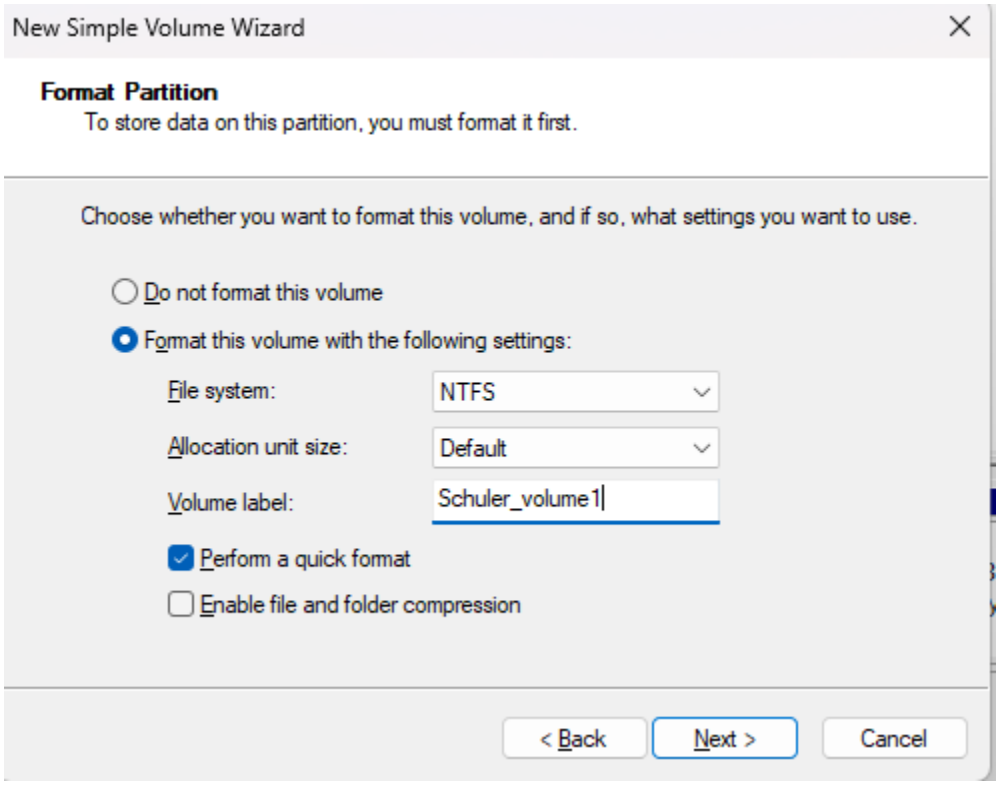


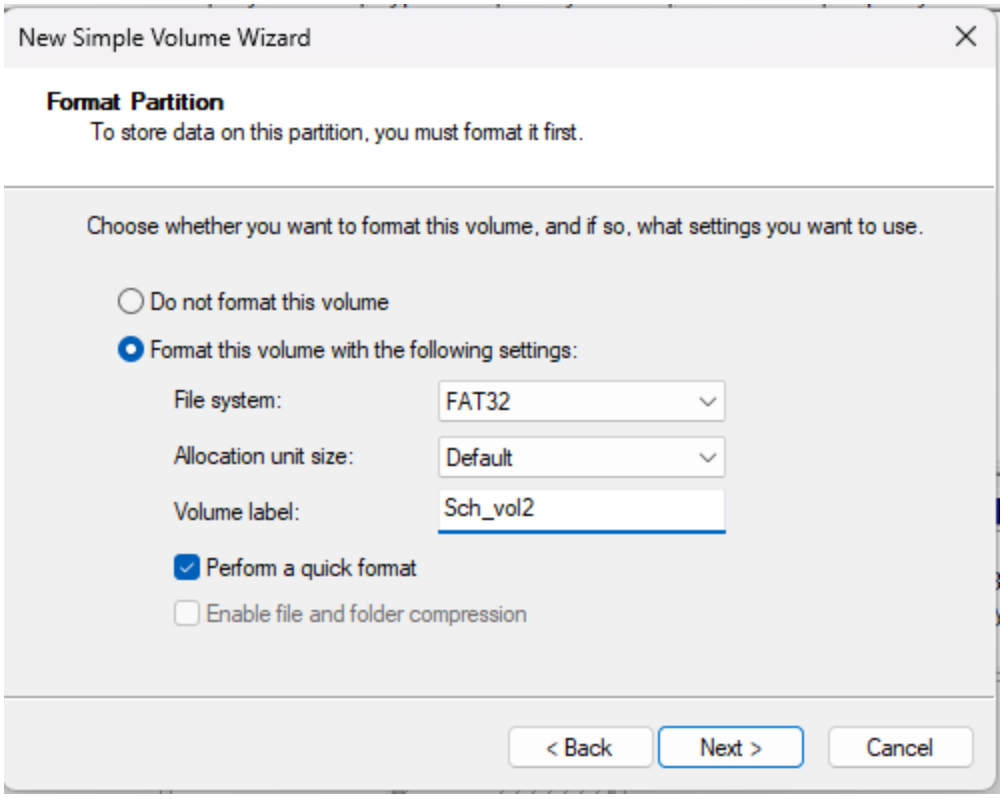
Task #3 – Creating a Virtual Hard Disk (VHD) with two volumes - Evidence #2

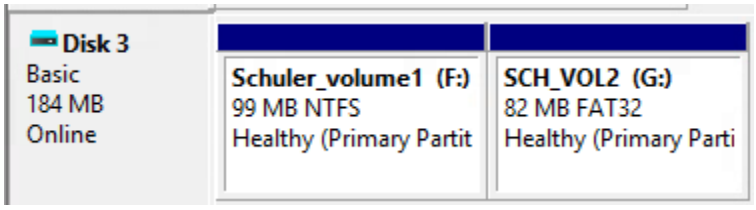
Create a virtual hard disk as follows:

1. The VHD size is 200 MB and call it YourLastName_evidence2
2. Initialize the disk and add a new NTFS volume (100 MB). Call the volume as follows: YourLastName_volume1
3. Add a second volume with a FAT32 file system. Call the volume as follows: YourLastName_volume2
4. Add different files to your two volumes images, documents, and PDFs

First two images show two volumes being quick formatted, one to NTFS and one to FAT32. The third image shows the two volumes and their capacities.



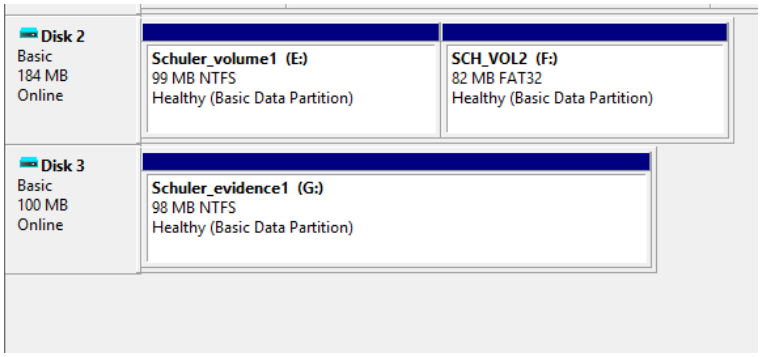




TASK #4 – ATTACH A VHD

1. Attach the VHD that you have created in task #1

Image shows both VHDs attached to the same computer.



2. How many disks are in your system?
    a. **4 disks, 2 physical, 2 virtual**
3. Detach the two VHDs that you have created

Images show both VHDs being detached. Note: final steps were completed on an alternate computer, so file paths are different.

TASK #5 – REFLECT WHAT YOU HAVE LEARNED IN THIS LAB

While I have worked with VHD(x) files in the past, this lab showed how to create one directly. I've only ever used them within virtual machines/hypervisor systems which handle it for me.