Support Guide: Create a Virtual Hard Disk to use as a collection container

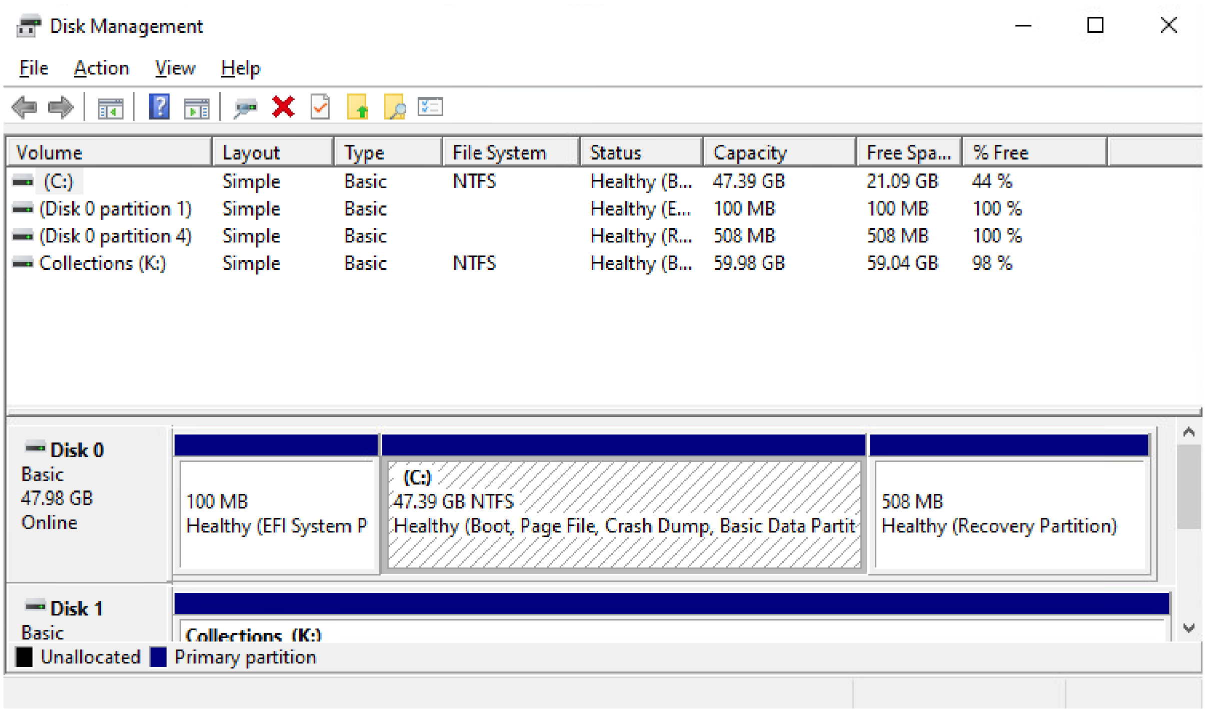
How to set up a dynamic VHD to store collected data.

Important Note

Disclaimer: The following guide is provided as-is. The exact steps necessary to create, attach, and manage a Virtual Hard Disk (VHD) may be different in different versions of Windows. Your screens and the steps required may not match up directly to the ones pictured below. When in doubt, always refer to Microsoft's documentation for your specific version of Windows.

Step 1: Open the Windows Disk Manager

Open Windows Disk Management tool (this can be accessed any number of ways depending on the version of Windows you are running):



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	47.39 GB	21.09 GB	44 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	508 MB	508 MB	100 %
Collections (K:)	Simple	Basic	NTFS	Healthy (B...	59.98 GB	59.04 GB	98 %

Disk 0
Basic
47.98 GB
Online

100 MB
Healthy (EFI System P

(C:)
47.39 GB NTFS
Healthy (Boot, Page File, Crash Dump, Basic Data Partit

508 MB
Healthy (Recovery Partition)

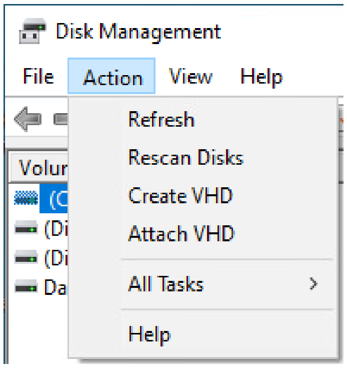
Disk 1
Basic

Collections (K:)

■ Unallocated ■ Primary partition

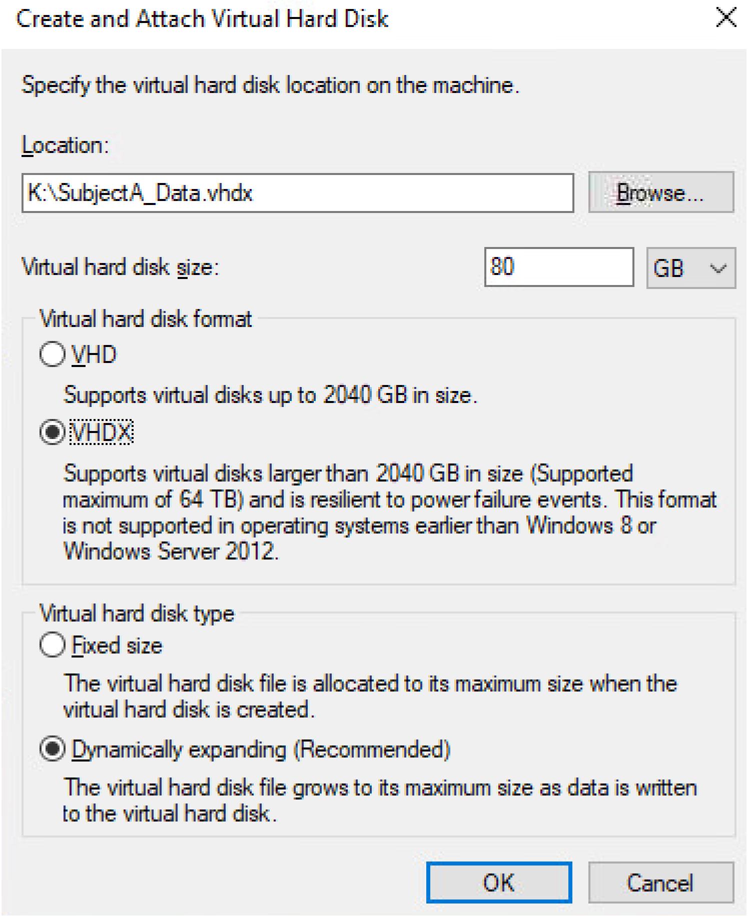
Windows Disk Management

In the Disk Management tool, choose Create VHD from the Action drop-down menu.



Step 2: Create a dynamic VHD

Now you can create a dynamic VHD on your destination drive.



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location: K:\SubjectA_Data.vhdx

Virtual hard disk size: 80 GB

Virtual hard disk format

○ VHD

Supports virtual disks up to 2040 GB in size.

● VHDX

Supports virtual disks larger than 2040 GB in size (Supported maximum of 64 TB) and is resilient to power failure events. This format is not supported in operating systems earlier than Windows 8 or Windows Server 2012.

Virtual hard disk type

○ Fixed size

The virtual hard disk file is allocated to its maximum size when the virtual hard disk is created.

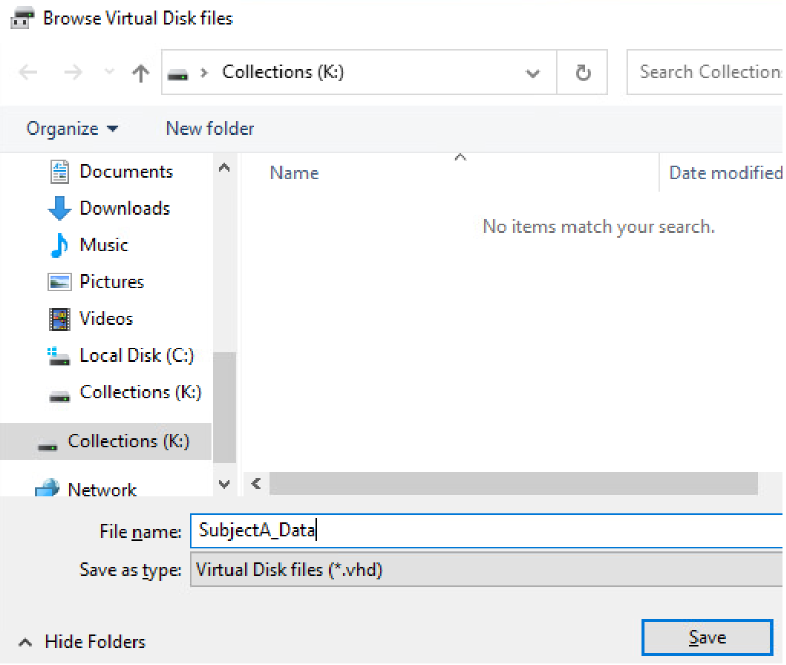
● Dynamically expanding (Recommended)

The virtual hard disk file grows to its maximum size as data is written to the virtual hard disk.

Options for creating a VHD

There are 4 options to specify in this window, each is covered below.

First you need to specify the location for your dynamic VHD container. Click the browse button to locate your drive. In this example we have a destination drive attached to our examiner machine assigned to the K volume.



Browse Virtual Disk files

File name: SubjectA_Data

Save as type: Virtual Disk files (*.vhd)

Destination Drive location for dynamic VHD

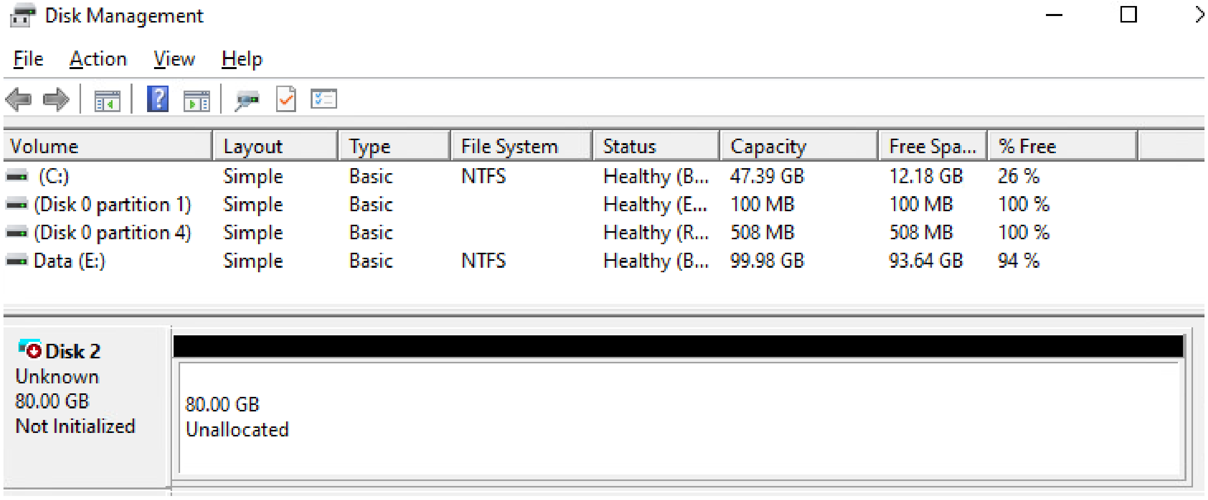
Create a name for the VHD container in the File name field and click Save.

Next, you'll need to choose the Max size for the dynamic VHD in the Virtual Hard Disk Size field. We recommend not exceeding 90% of the available destination drive space.

VHD vs VHDx is a matter of personal preference as most collections will not exceed 2TB (2040 GB) in size. Select the Dynamically Expanding option to allow the collection to expand to only what is needed. Click OK to finalize and create the dynamic VHD.

Step 3: Initialize and format the VHD

Once the VHD is created, it will appear in the list of disks in the disk management tool.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	47.39 GB	12.18 GB	26 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	508 MB	508 MB	100 %
Data (E:)	Simple	Basic	NTFS	Healthy (B...	99.98 GB	93.64 GB	94 %

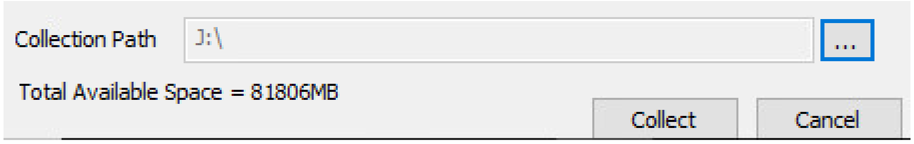
Disk 2
Unknown
80.00 GB
Not Initialized

80.00 GB
Unallocated

To finish the process, you'll need to simply initialize, format the disk, and assign a volume letter as you would for any newly attached disk in the Windows OS.

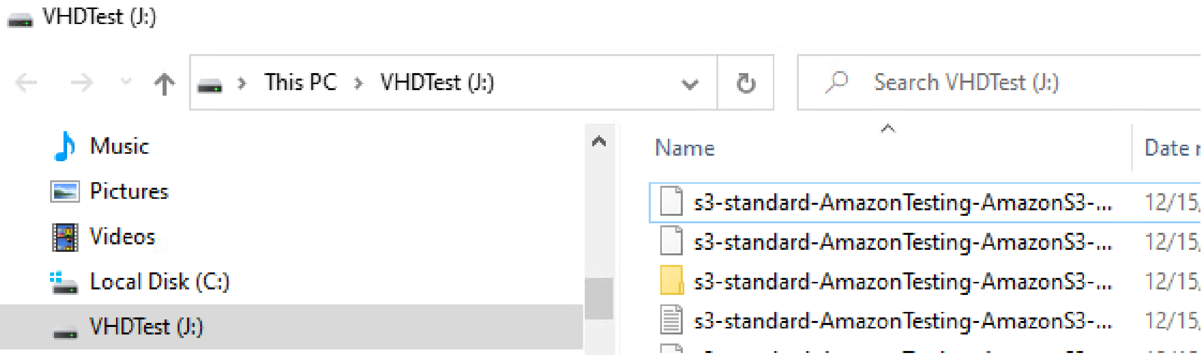
Step 4: Perform your collection

Now you can perform your collection and use the drive letter you assigned to the newly created dynamic VHD


Collection Path: J:\

Total Available Space = 81806MB

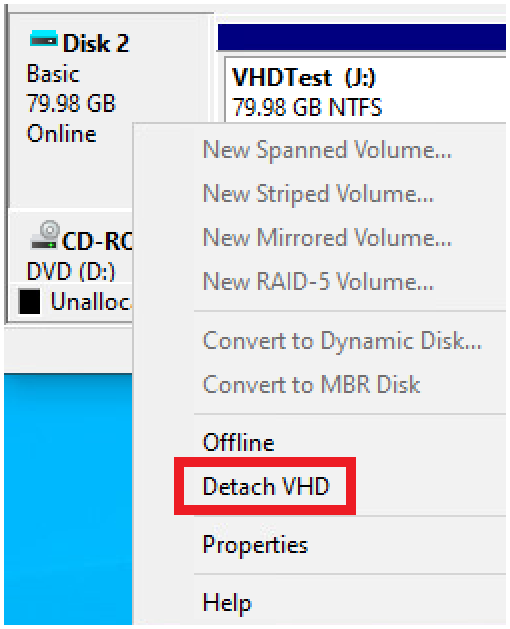
Once completed you'll can review the data in the VHD:



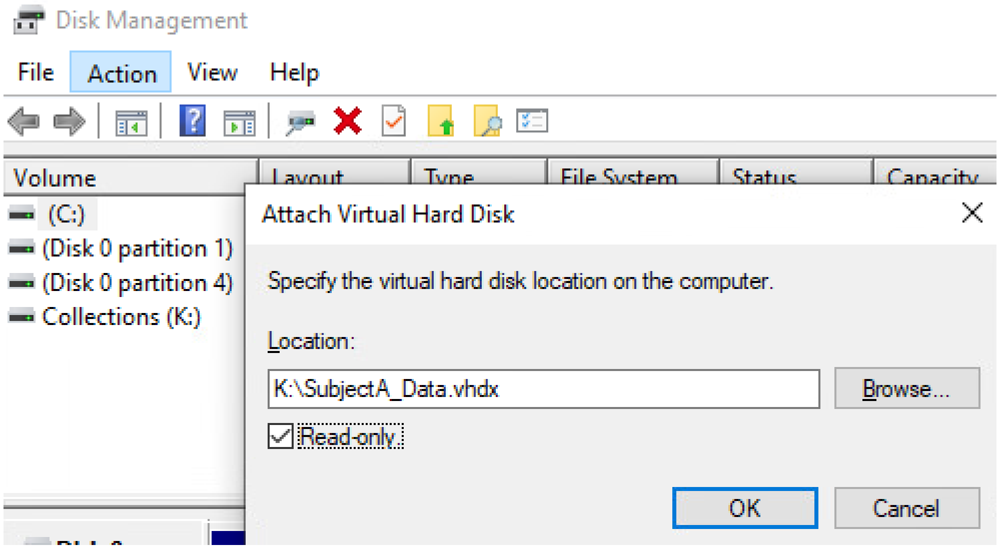
s3-standard-AmazonTesting-AmazonS3-... 12/15,
s3-standard-AmazonTesting-AmazonS3-... 12/15,
s3-standard-AmazonTesting-AmazonS3-... 12/15,
s3-standard-AmazonTesting-AmazonS3-... 12/15,

Step 5: Finalizing and working with the VHD

Once you have completed collecting all the necessary data to the VHD you can detach it in the Disk Management tool by right clicking and selecting Detach VHD. Windows will shrink the disk down shedding the unused space.



You now have a solid forensic container for your collection which can be duplicated, shared, and mounted as a read-only disk.



Specify the virtual hard disk location on the computer.

Location: K:\SubjectA_Data.vhdx

☑ Read-only