Linux:

- **Navigate using shell**
    - Uname (used to find OS info), -a option (displays everything)
    - Hostname displays name of machine
    - Last (displays a list of all user logged in and out since the file was created)
    - w (displays who is logged into the machine)
    - / (indicates the root directory)
    - /home/ (when you login you are brought to a users home directory)
    - Pwd (prints the path of the directory your in)
    - ls (Returns a list of names of any files or directories held in the directory your in)
    - mkdir (makes a directory)
    - cd (change directory)
    - cd .. (change directory to one level up in your path)
    - Touch file.txt (creates an empty file in the current directory)
    - Mv file.txt newfile.txt (moves the file to a new location, and renames it)
    - cp (copies files to and from similar to mv command)
    - rm (deletes files)
    - Rm -d directory name (removes a directory)
    - rm -r directory name (deletes a directory and everything in it)
- **Understand paths**
    - Absolute vs Relative Path:
        - Absolute path: Path that describes a location of file or folder relative to the root directory.
        - Relative path: Path that describes a location of file or folder relative to the directory you currently are in.
- **How to create files and directories**
    - Touch file.txt (creates an empty file in the current directory)
    - Mv file.txt newfile.txt (moves the file to a new location, and renames it)

- cp (copies files to and from similar to mv command)
- rm (deletes files)
- Rm -d directory name (removes a directory)
- rm -r directory name (deletes a directory and everything in it)
- Cat (calls the file and displays it without having to edit anything)
- vi/nano (editors, you can edit a file using these commands)

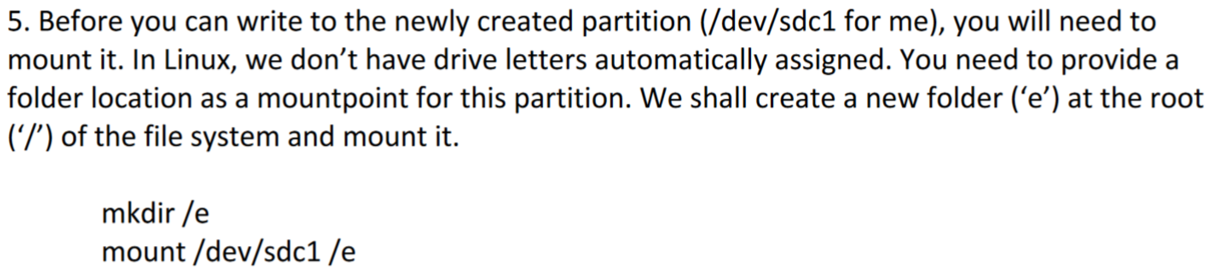
Imaging:

https://www.cyberciti.biz/faq/unix-linux-dd-create-make-disk-image-commands/

When working with disk, you want to add the disk, power on the machine. From here find the newly attached disk using lsblk | grep -v loop (lsblk would be fine to use, grep -v loop filter out anything that is a loopback (not from a real device). After this create a new partition on the disk by using fdisk. Then format it, then mount it. Then list the partition info using fdisk -l. Then you can begin to image of the partition.

- **Fdisk**
  - Fdisk (manipulates disk partition table)

- **Lsblk**
  - lsblk (shows block devices, lists info about all available or specified block devices.)
- **Mount**



5. Before you can write to the newly created partition (/dev/sdc1 for me), you will need to mount it. In Linux, we don’t have drive letters automatically assigned. You need to provide a folder location as a mountpoint for this partition. We shall create a new folder (‘e’) at the root (‘/’) of the file system and mount it.

```
mkdir /e
mount /dev/sdc1 /e
```

  -
- **dd**

2. Here you have to use 'dd' to create a clone of the evidence disk. Remember, you want the whole disk, not a partition.

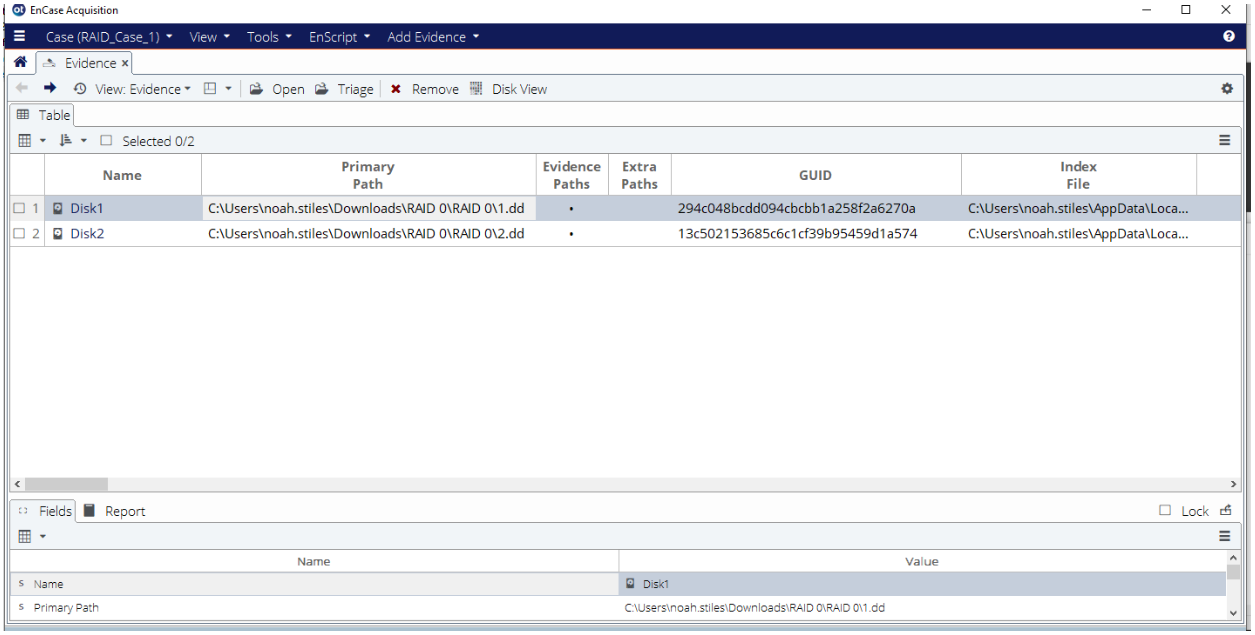
The command would be:

```
        dd if=/dev/sdd of=/dev/sdb conv=noerror,sync bs=1M
```

-

FTK / Encase:

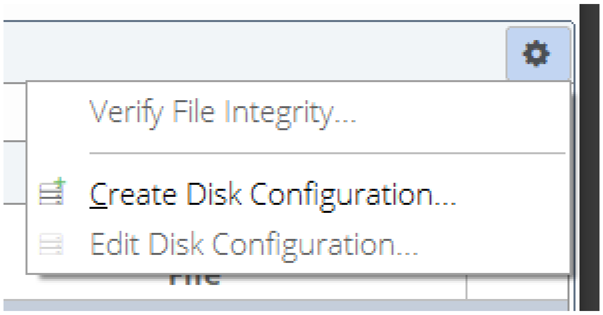
1. Using encase load these files and create a raid0 virtual view (Stripe size=64KB).



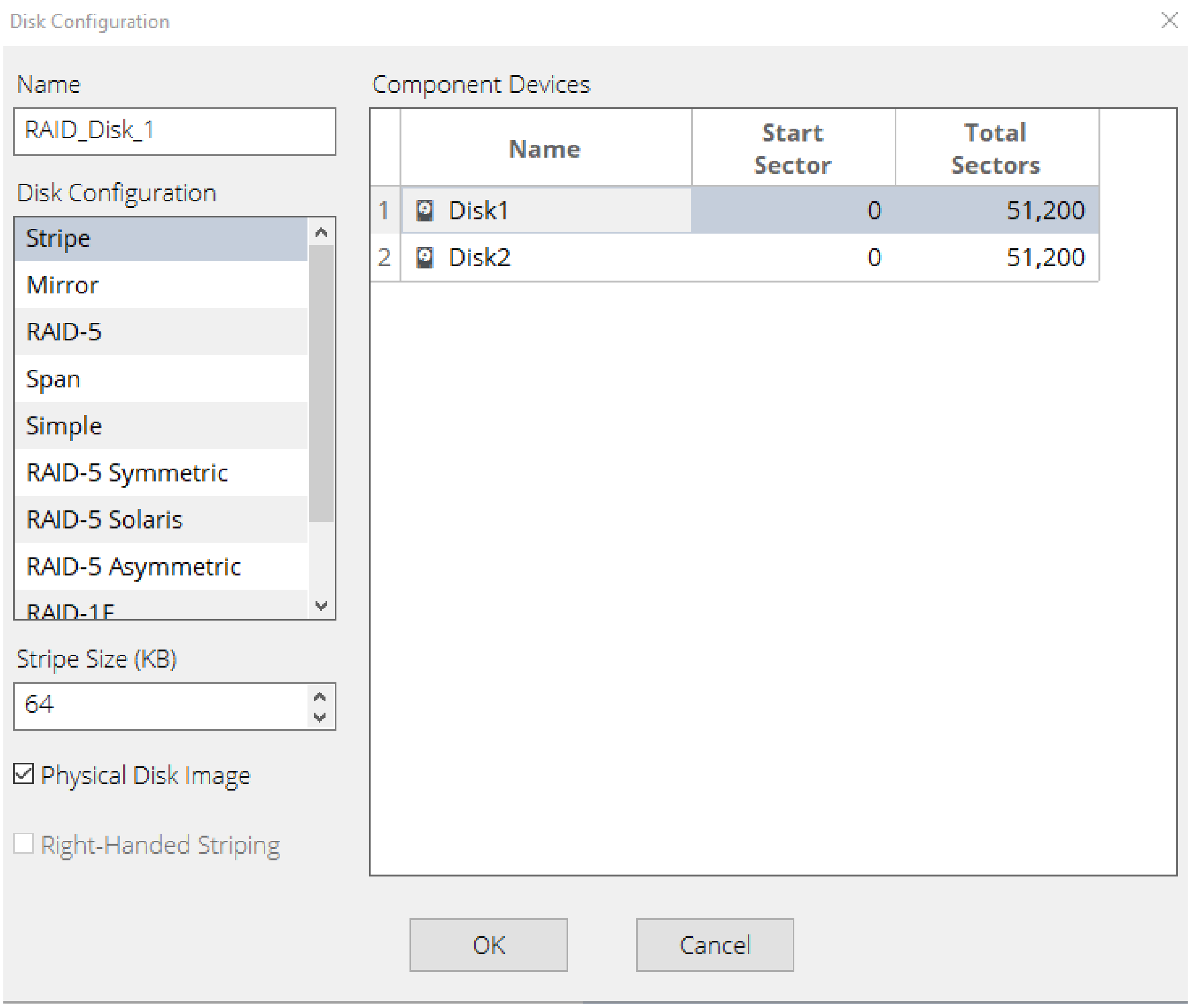
	Name	Primary Path	Evidence Paths	Extra Paths	GUID	Index File
□ 1	Disk1	C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\1.dd	•		294c048bcdd094cbcbb1a258f2a6270a	C:\Users\noah.stiles\AppData\Loca...
□ 2	Disk2	C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\2.dd	•		13c502153685c6c1cf39b95459d1a574	C:\Users\noah.stiles\AppData\Loca...

Name	Value
Name	Disk1
Primary Path	C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\1.dd

Here I went and hit add evidence, I added the two disks in the correct order.



Here I will create the raid0 virtual view, by tapping on the settings and than create disk configuration.



Disk Configuration

Name

RAID_Disk_1

Disk Configuration

- Stripe
- Mirror
- RAID-5
- Span
- Simple
- RAID-5 Symmetric
- RAID-5 Solaris
- RAID-5 Asymmetric
- RAID-1E

Stripe Size (KB)

64

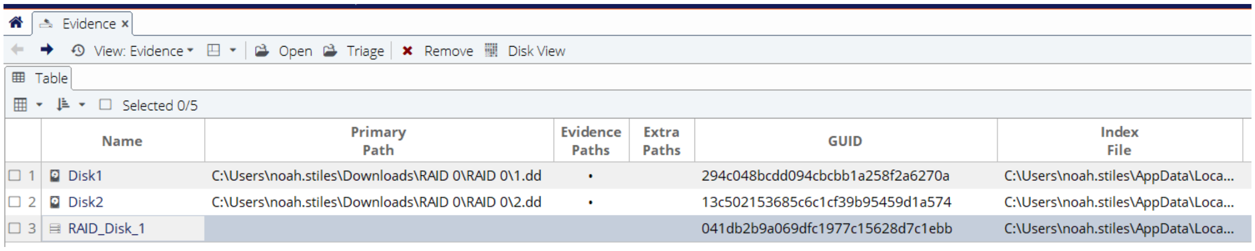
☑ Physical Disk Image

☐ Right-Handed Striping

Component Devices

	Name	Start Sector	Total Sectors
1	Disk1	0	51,200
2	Disk2	0	51,200

Here we adjust the stripe size and add the 2 disks.

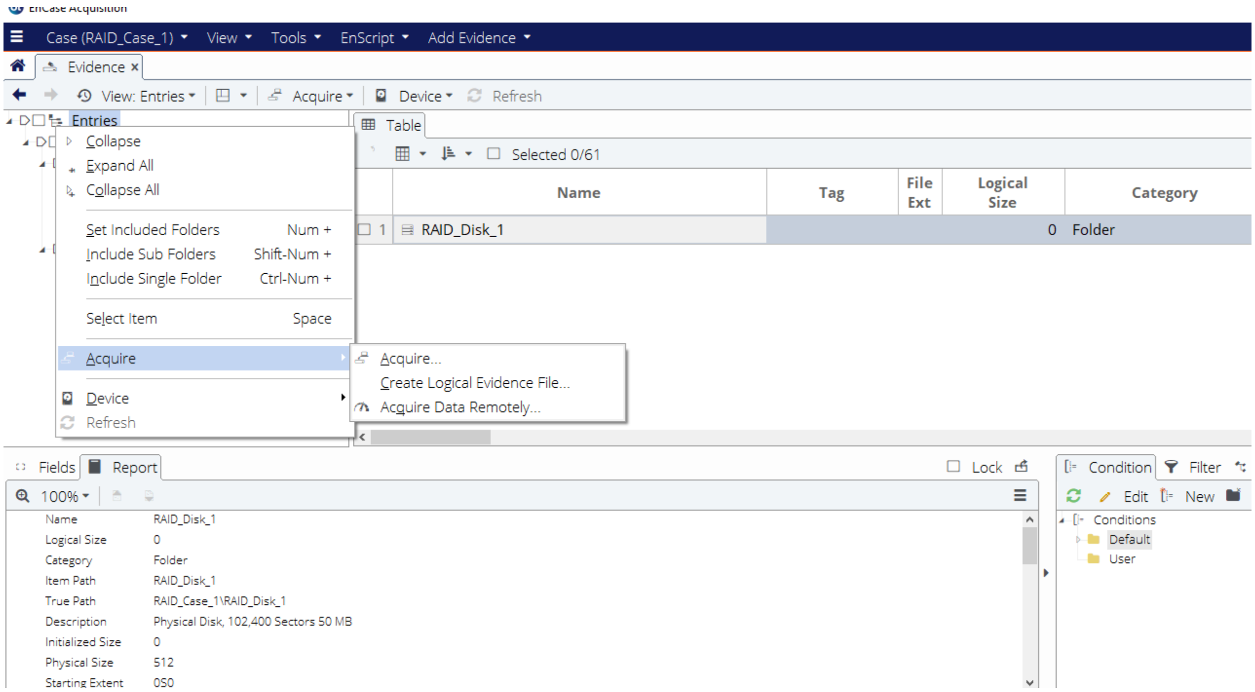


☐ Selected 0/5

	Name	Primary Path	Evidence Paths	Extra Paths	GUID	Index File
☐ 1	Disk1	C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\1.dd	•		294c048bcdd094cbcbb1a258f2a6270a	C:\Users\noah.stiles\AppData\Loca...
☐ 2	Disk2	C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\2.dd	•		13c502153685c6c1cf39b95459d1a574	C:\Users\noah.stiles\AppData\Loca...
☐ 3	RAID_Disk_1				041db2b9a069dfc1977c15628d7c1ebb	C:\Users\noah.stiles\AppData\Loca...

Here is the view after it was created.

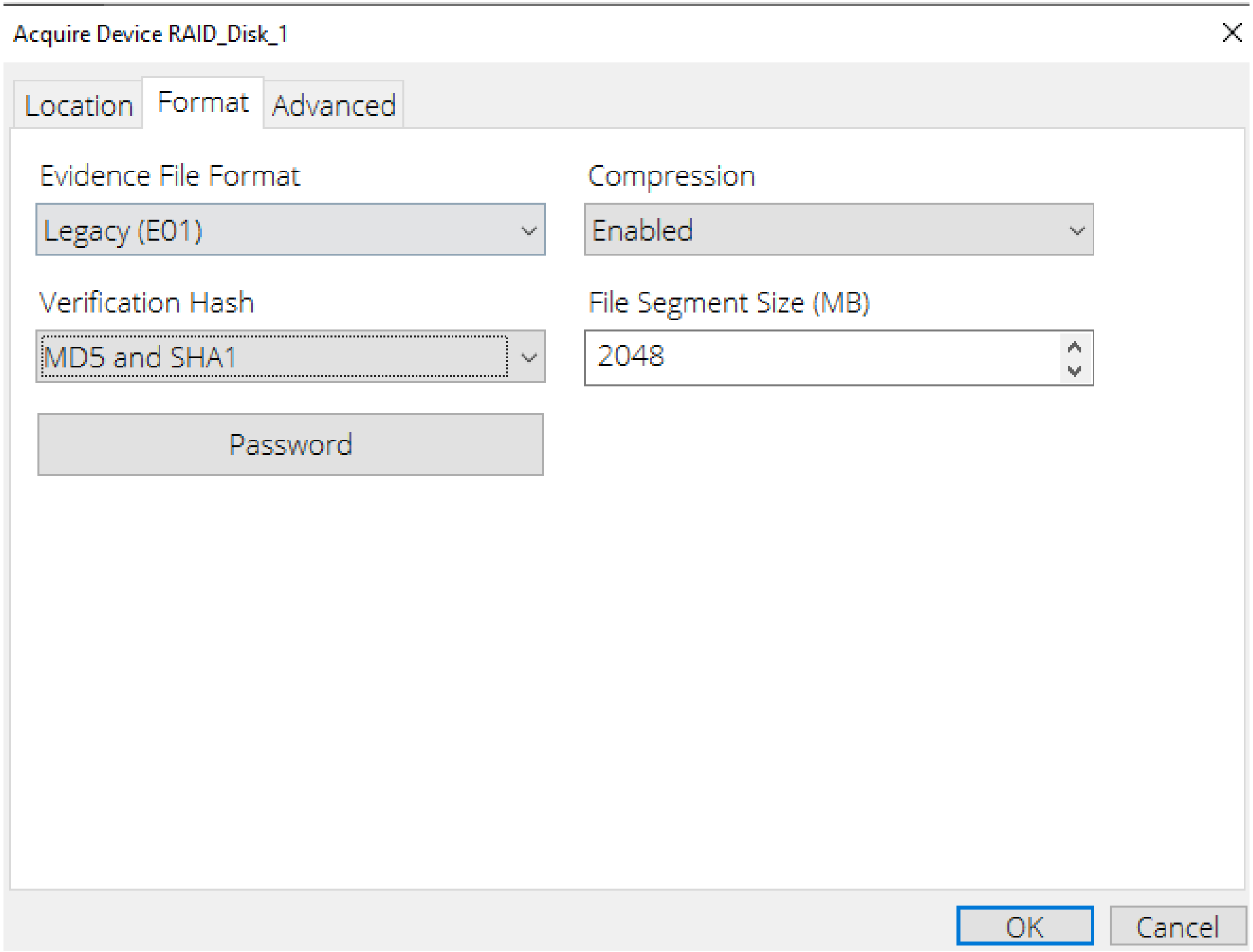
2. Create an E01 file from this virtual RAID.



	Name	Tag	File Ext	Logical Size	Category
□ 1	RAID_Disk_1			0	Folder

Name	RAID_Disk_1
Logical Size	0
Category	Folder
Item Path	RAID_Disk_1
True Path	RAID_Case_1\RAID_Disk_1
Description	Physical Disk, 102,400 Sectors 50 MB
Initialized Size	0
Physical Size	512
Starting Extent	0S0

Within the virtual view of the RAID0 you right click on entries, hit acquire and then on to the next step!



Acquire Device RAID_Disk_1

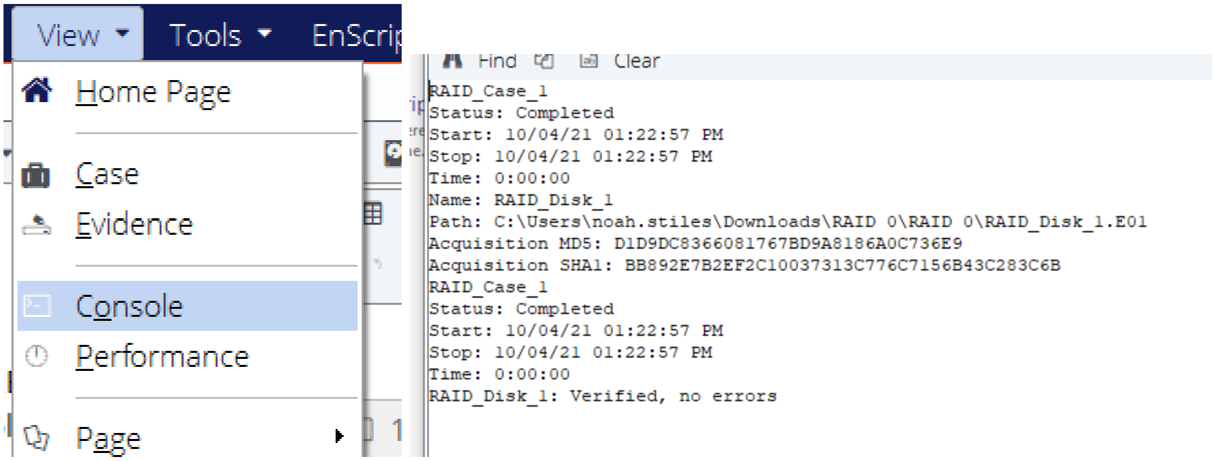
Evidence File Format: Legacy (E01)

Compression: Enabled

Verification Hash: MD5 and SHA1

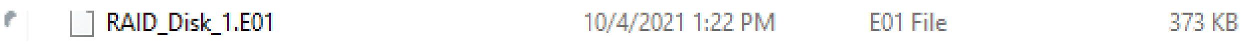
File Segment Size (MB): 2048

Here is the next step where we pick the location and then in format we switched to legacy, we compressed it, and changed the hash to be both.



```
RAID_Case_1
Status: Completed
Start: 10/04/21 01:22:57 PM
Stop: 10/04/21 01:22:57 PM
Time: 0:00:00
Name: RAID_Disk_1
Path: C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\RAID_Disk_1.E01
Acquisition MD5: D1D9DC8366081767BD9A8186A0C736E9
Acquisition SHA1: BB892E7B2EF2C10037313C776C7156B43C283C6B
RAID_Case_1
Status: Completed
Start: 10/04/21 01:22:57 PM
Stop: 10/04/21 01:22:57 PM
Time: 0:00:00
RAID_Disk_1: Verified, no errors
```

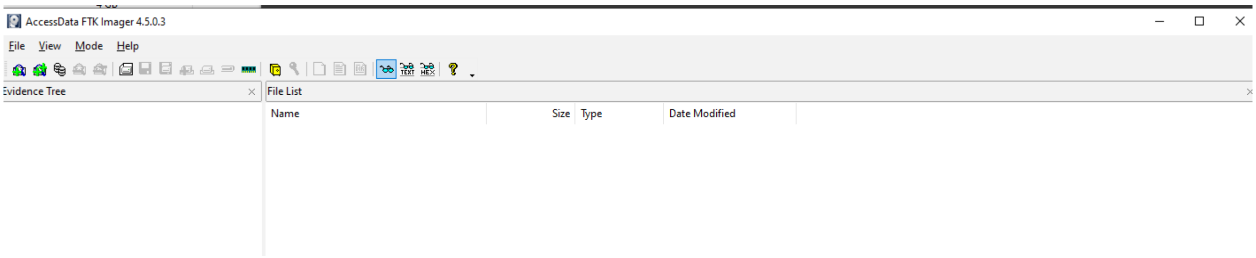
Here we hit view and look at the console to make sure the file was created correctly without errors.



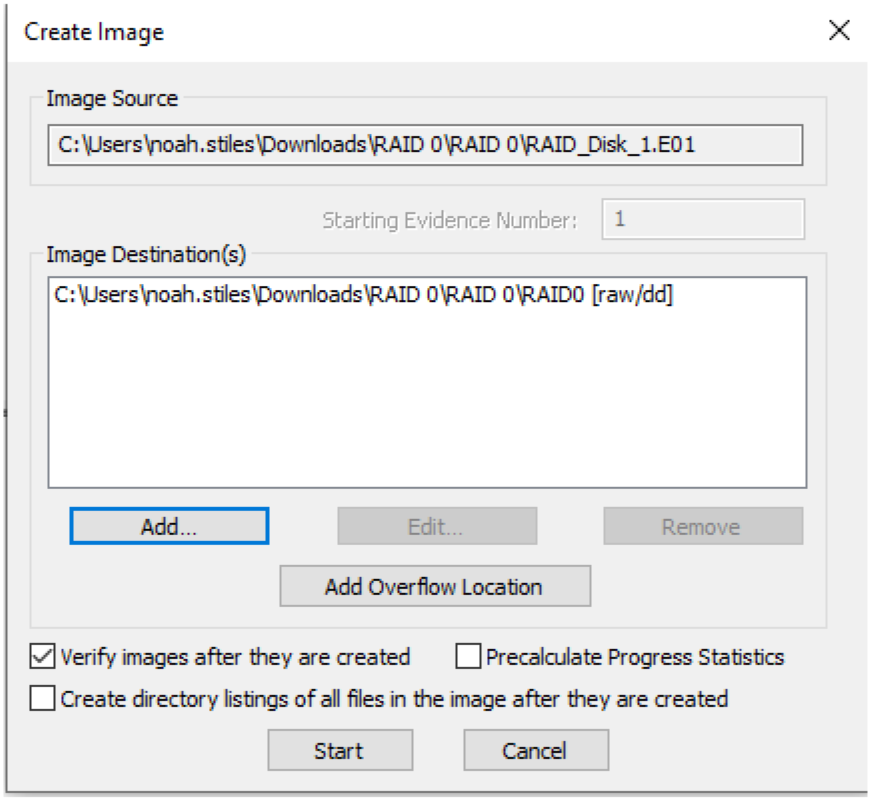
RAID_Disk_1.E01 10/4/2021 1:22 PM E01 File 373 KB

Here is the disk and it is smaller than the other files because of compression.

3. Use FTK imager to convert E01 to dd image.



We open FTK, File → Create disk file → Image file → Click location of image



Create Image

Image Source

C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\RAID_Disk_1.E01

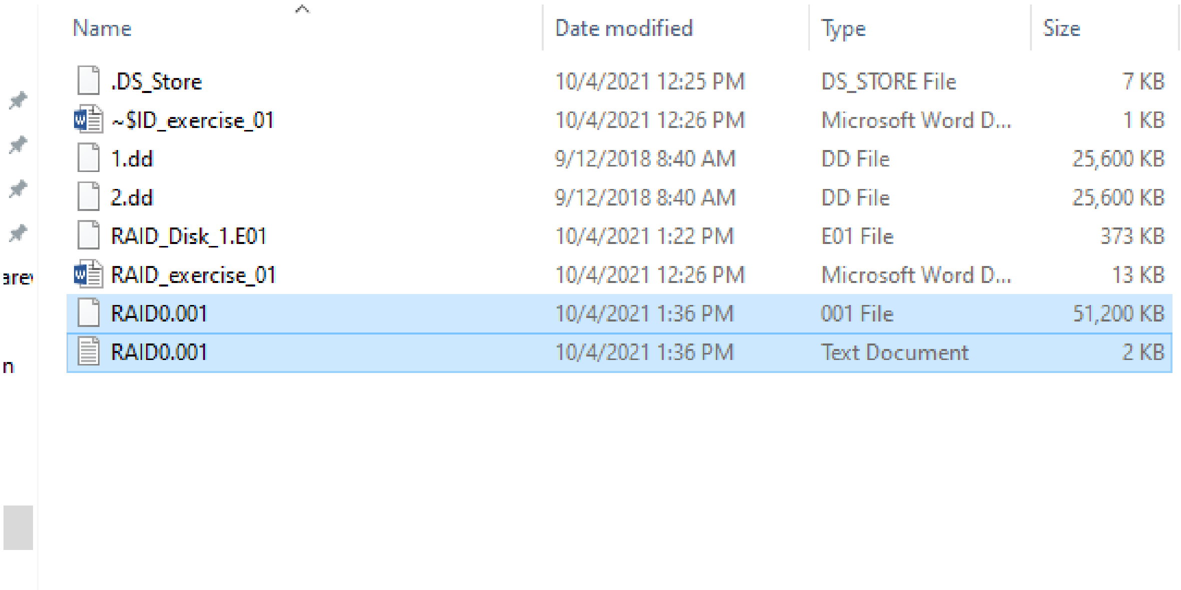
Starting Evidence Number: 1

Image Destination(s)

C:\Users\noah.stiles\Downloads\RAID 0\RAID 0\RAID0 [raw/dd]

☑ Verify images after they are created ☐ Precalculate Progress Statistics

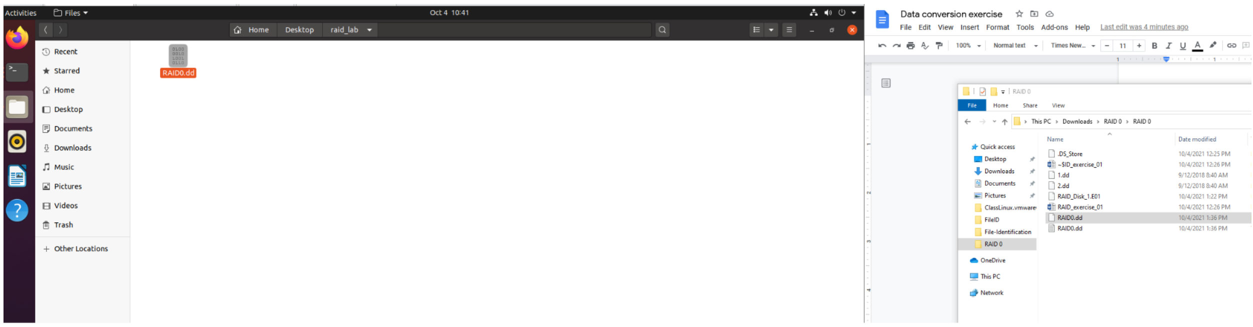
☐ Create directory listings of all files in the image after they are created



Name	Date modified	Type	Size
.DS_Store	10/4/2021 12:25 PM	DS_STORE File	7 KB
~$ID_exercise_01	10/4/2021 12:26 PM	Microsoft Word D...	1 KB
1.dd	9/12/2018 8:40 AM	DD File	25,600 KB
2.dd	9/12/2018 8:40 AM	DD File	25,600 KB
RAID_Disk_1.E01	10/4/2021 1:22 PM	E01 File	373 KB
RAID_exercise_01	10/4/2021 12:26 PM	Microsoft Word D...	13 KB
RAID0.001	10/4/2021 1:36 PM	001 File	51,200 KB
RAID0.001	10/4/2021 1:36 PM	Text Document	2 KB

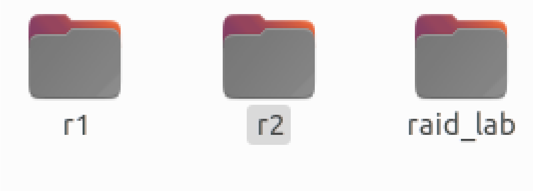
Here we created the imaged file.

4. Bring dd image to Linux and mount it!

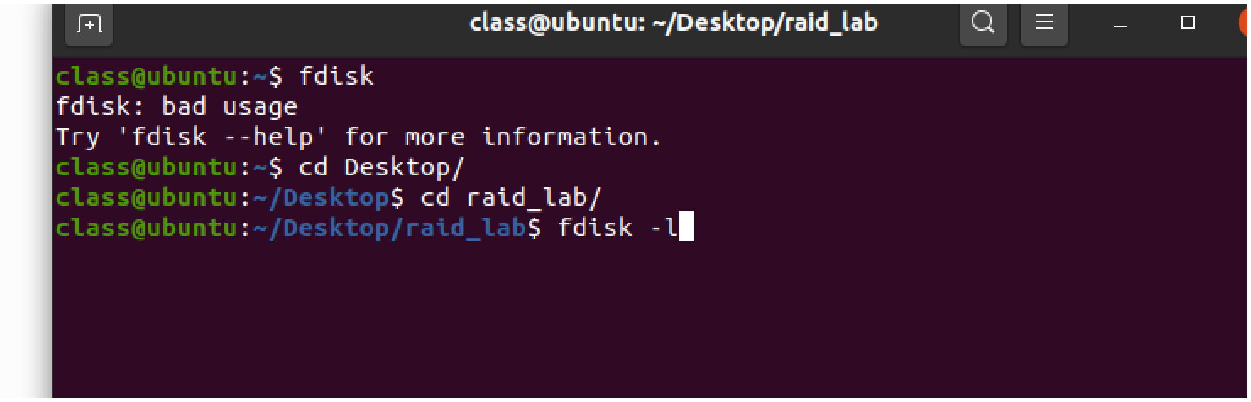


Name	Date modified
.DS_Store	10/4/2021 12:25 PM
~$ID_exercise_01	10/4/2021 12:26 PM
1.dd	9/12/2018 8:40 AM
2.dd	9/12/2018 8:40 AM
RAID_Disk_1.E01	10/4/2021 1:22 PM
RAID_exercise_01	10/4/2021 12:26 PM
RAID0.dd	10/4/2021 1:36 PM
RAID0.dd	10/4/2021 1:36 PM

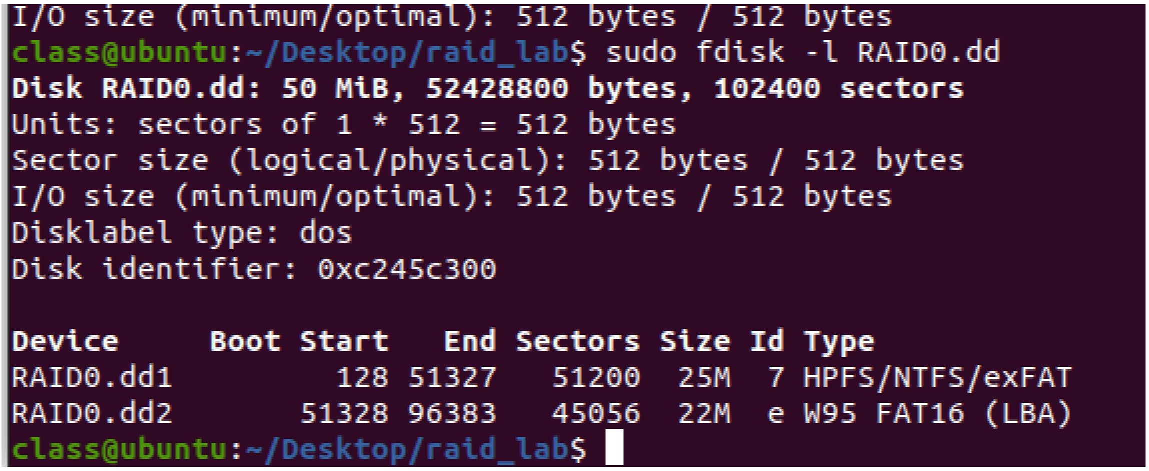
Drag and drop the file from windows explorer.



Create mount points r1 & r2



```
class@ubuntu:~$ fdisk
fdisk: bad usage
Try 'fdisk --help' for more information.
class@ubuntu:~$ cd Desktop/
class@ubuntu:~/Desktop$ cd raid_lab/
class@ubuntu:~/Desktop/raid_lab$ fdisk -l
```



```
I/O size (minimum/optimal): 512 bytes / 512 bytes
class@ubuntu:~/Desktop/raid_lab$ sudo fdisk -l RAID0.dd
Disk RAID0.dd: 50 MiB, 52428800 bytes, 102400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc245c300

Device     Boot Start   End Sectors Size Id Type
RAID0.dd1         128 51327   51200  25M  7 HPFS/NTFS/exFAT
RAID0.dd2       51328 96383   45056  22M  e W95 FAT16 (LBA)
class@ubuntu:~/Desktop/raid_lab$
```

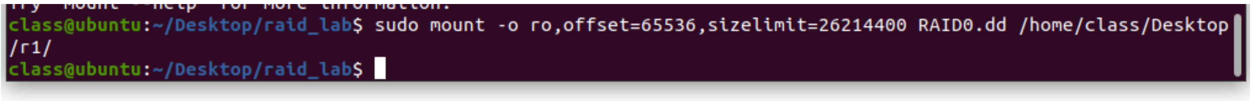
To find start of the first partition multiply boot start 128 by I/O size: 512 bytes

To find the end of the first partition multiply the 512 bytes by the number of sectors

Make sure to do -o ro for fread only

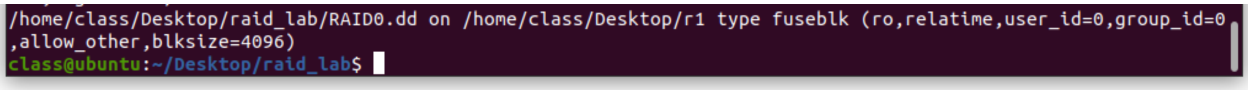
Make sure to put filename and put the destination of the file

It tells us we have two partitions and numerous other things.



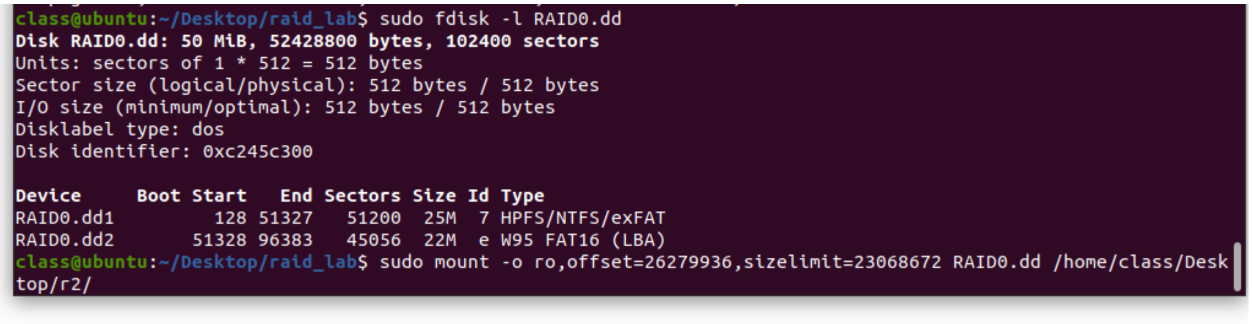
```
Try 'mount --help' for more information.
class@ubuntu:~/Desktop/raid_lab$ sudo mount -o ro,offset=65536,sizelimit=26214400 RAID0.dd /home/class/Desktop
/r1/
class@ubuntu:~/Desktop/raid_lab$
```

Command mount:



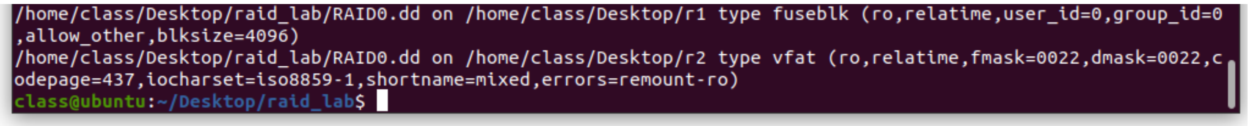
```
/home/class/Desktop/raid_lab/RAID0.dd on /home/class/Desktop/r1 type fuseblk (ro,relatime,user_id=0,group_id=0
,allow_other,blksize=4096)
class@ubuntu:~/Desktop/raid_lab$
```

Now do the second one:



```
class@ubuntu:~/Desktop/raid_lab$ sudo fdisk -l RAID0.dd
Disk RAID0.dd: 50 MiB, 52428800 bytes, 102400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xc245c300

Device     Boot Start   End Sectors Size Id Type
RAID0.dd1         128 51327   51200  25M  7 HPFS/NTFS/exFAT
RAID0.dd2       51328 96383   45056  22M  e W95 FAT16 (LBA)
class@ubuntu:~/Desktop/raid_lab$ sudo mount -o ro,offset=26279936,sizelimit=23068672 RAID0.dd /home/class/Desk
top/r2/
```



```
/home/class/Desktop/raid_lab/RAID0.dd on /home/class/Desktop/r1 type fuseblk (ro,relatime,user_id=0,group_id=0
,allow_other,blksize=4096)
/home/class/Desktop/raid_lab/RAID0.dd on /home/class/Desktop/r2 type vfat (ro,relatime,fmask=0022,dmask=0022,c
odepage=437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro)
class@ubuntu:~/Desktop/raid_lab$ 
```

Netcat:

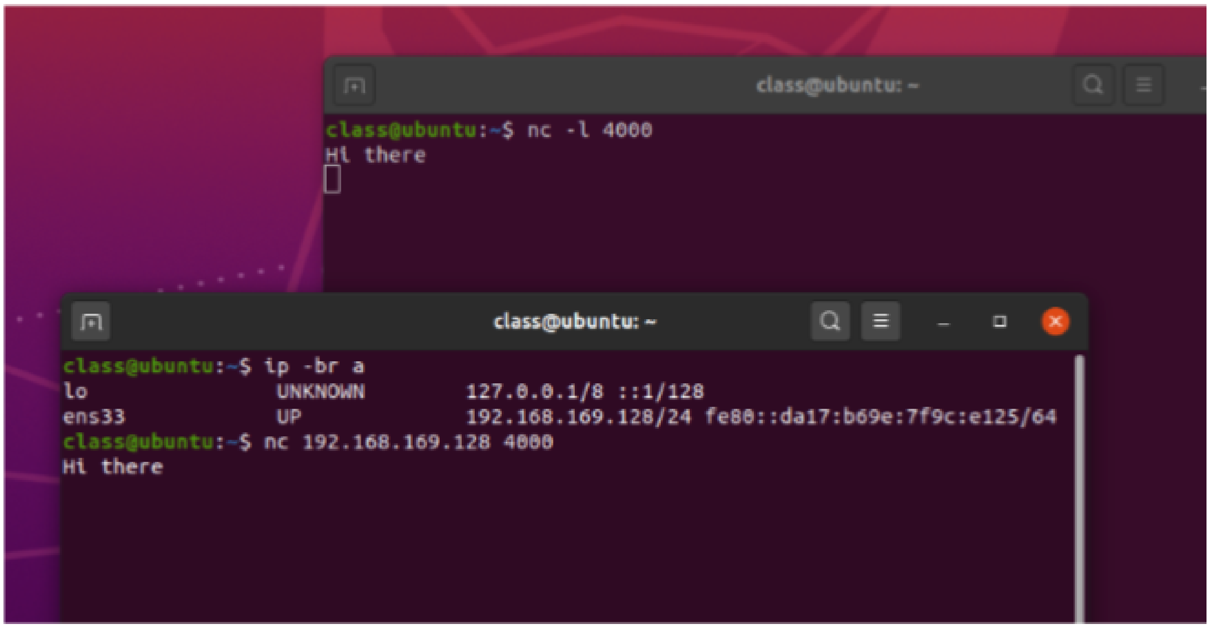
Command line tool for communicating through TCP or UDP

In linux nc www.google.com 80

GET / HTTP/1.0

Host: www.google.com

- **Send text messages**
    - On the same system:

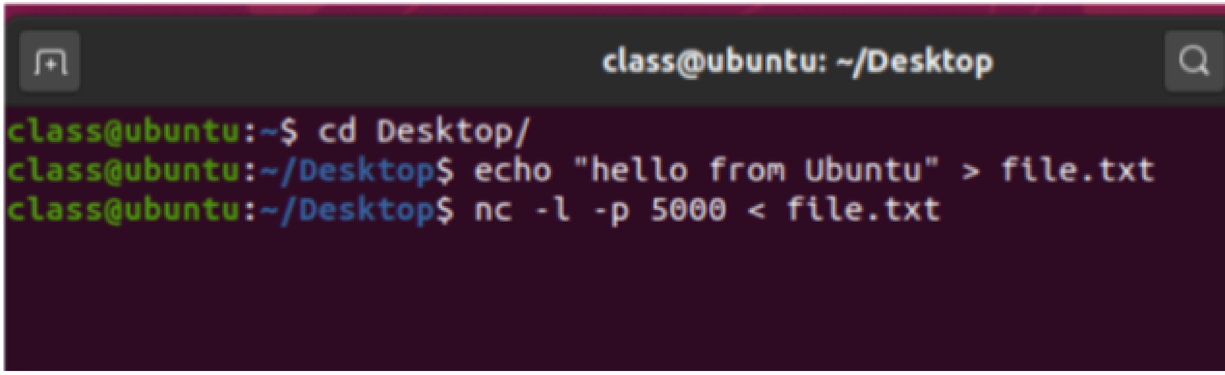


```
class@ubuntu:~$ nc -l 4000
Hi there
```

```
class@ubuntu:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             192.168.169.128/24 fe80::da17:b69e:7f9c:e125/64
class@ubuntu:~$ nc 192.168.169.128 4000
Hi there
```

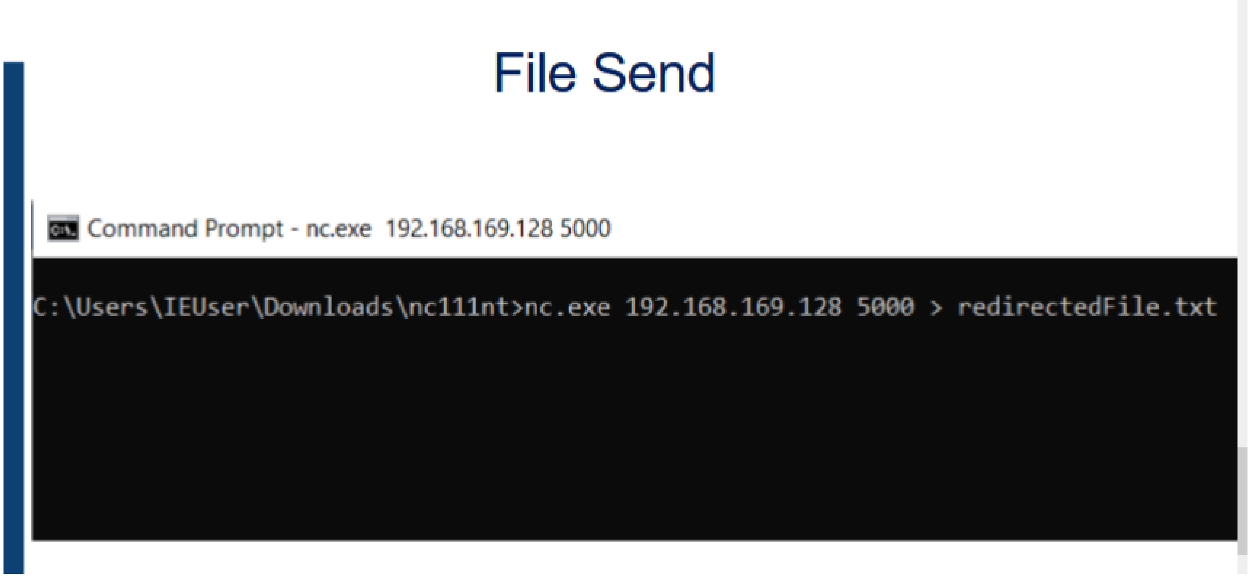
- 4000 is the port # and the IP is the IP of my machine

- **Send files**



```
class@ubuntu:~$ cd Desktop/
class@ubuntu:~/Desktop$ echo "hello from Ubuntu" > file.txt
class@ubuntu:~/Desktop$ nc -l -p 5000 < file.txt
```

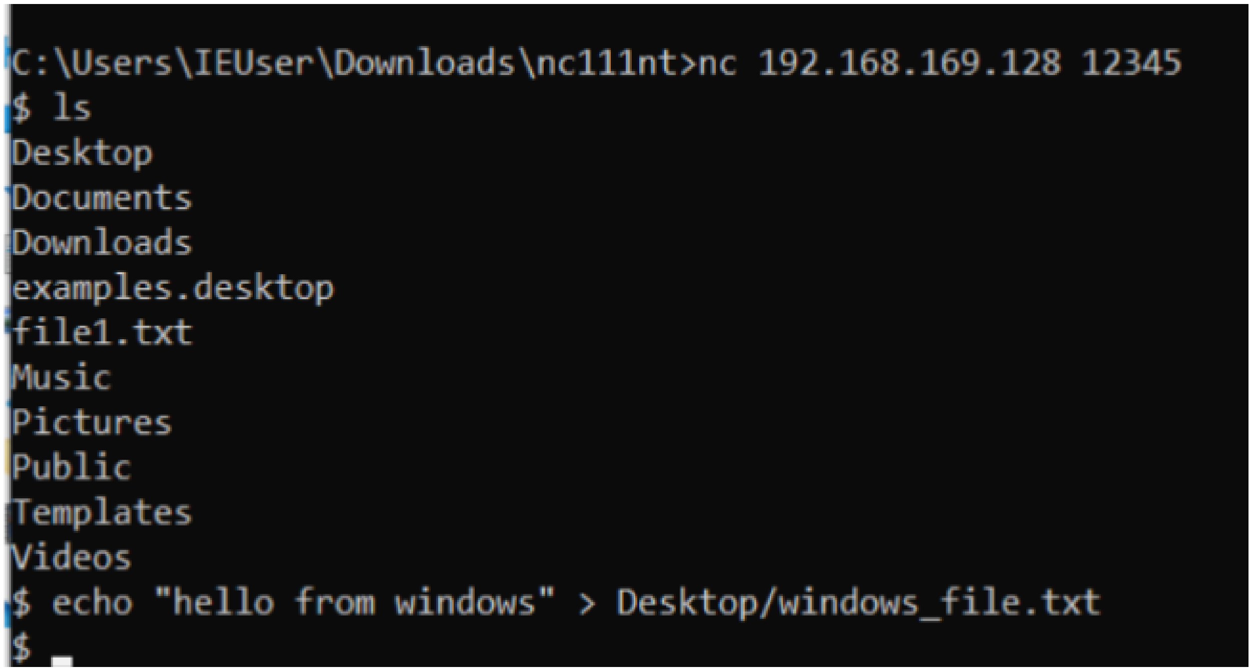
-
- On the Windows machine you then run:



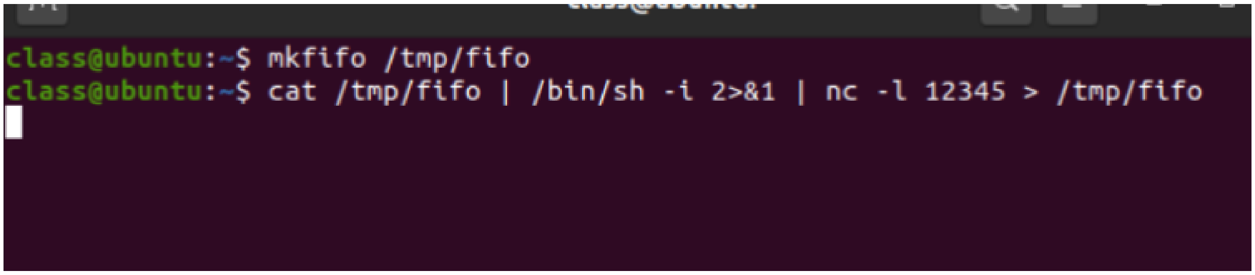
File Send

```
C:\Users\IEUser\Downloads\nc111nt>nc.exe 192.168.169.128 5000 > redirectedFile.txt
```

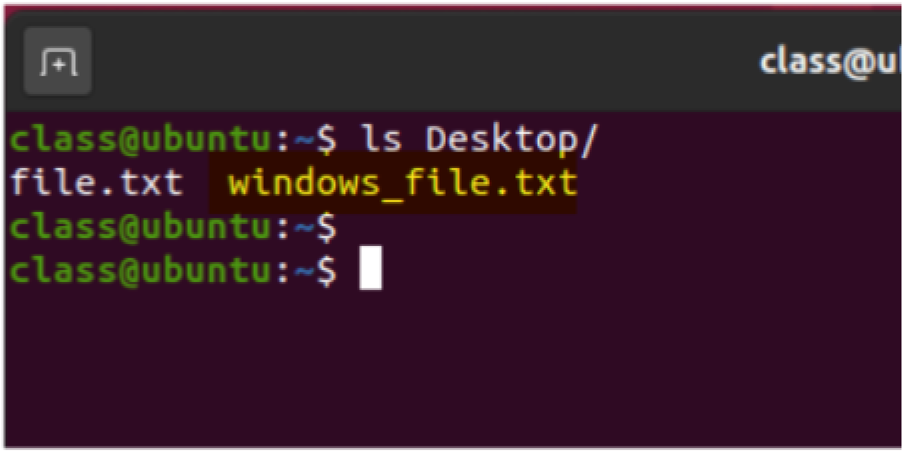
- **Open a remote cmd/shell**



```
C:\Users\IEUser\Downloads\nc111nt>nc 192.168.169.128 12345
$ ls
Desktop
Documents
Downloads
examples.desktop
file1.txt
Music
Pictures
Public
Templates
Videos
$ echo "hello from windows" > Desktop/windows_file.txt
$
```



```
class@ubuntu:~$ mkfifo /tmp/fifo
class@ubuntu:~$ cat /tmp/fifo | /bin/sh -i 2>&1 | nc -l 12345 > /tmp/fifo
```

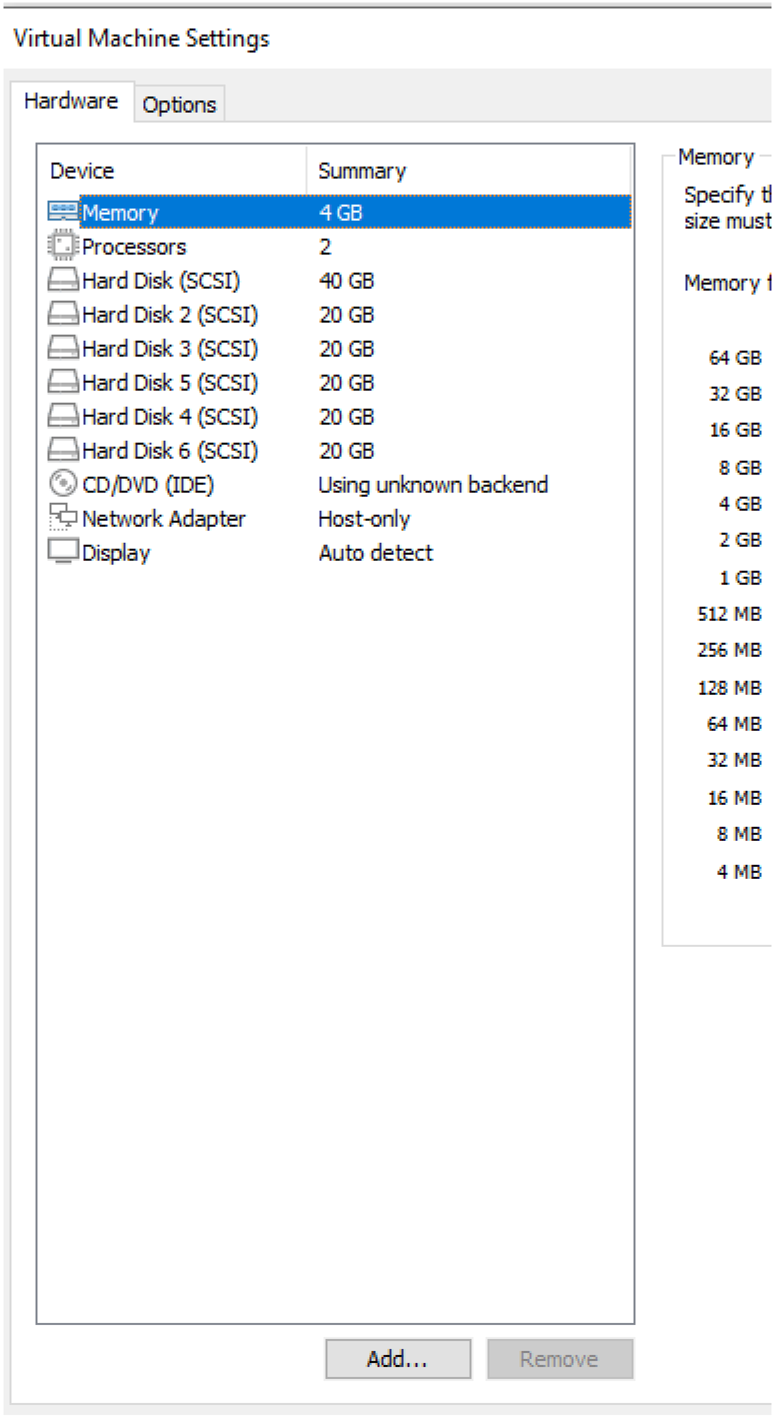


```
class@ubuntu:~$ ls Desktop/
file.txt  windows_file.txt
class@ubuntu:~$
class@ubuntu:~$ 
```

RAID:

- **Use encase to reconstruct RAID Disks**
- **Create RAID disks on Windows**

Add hard disks:



Virtual Machine Settings

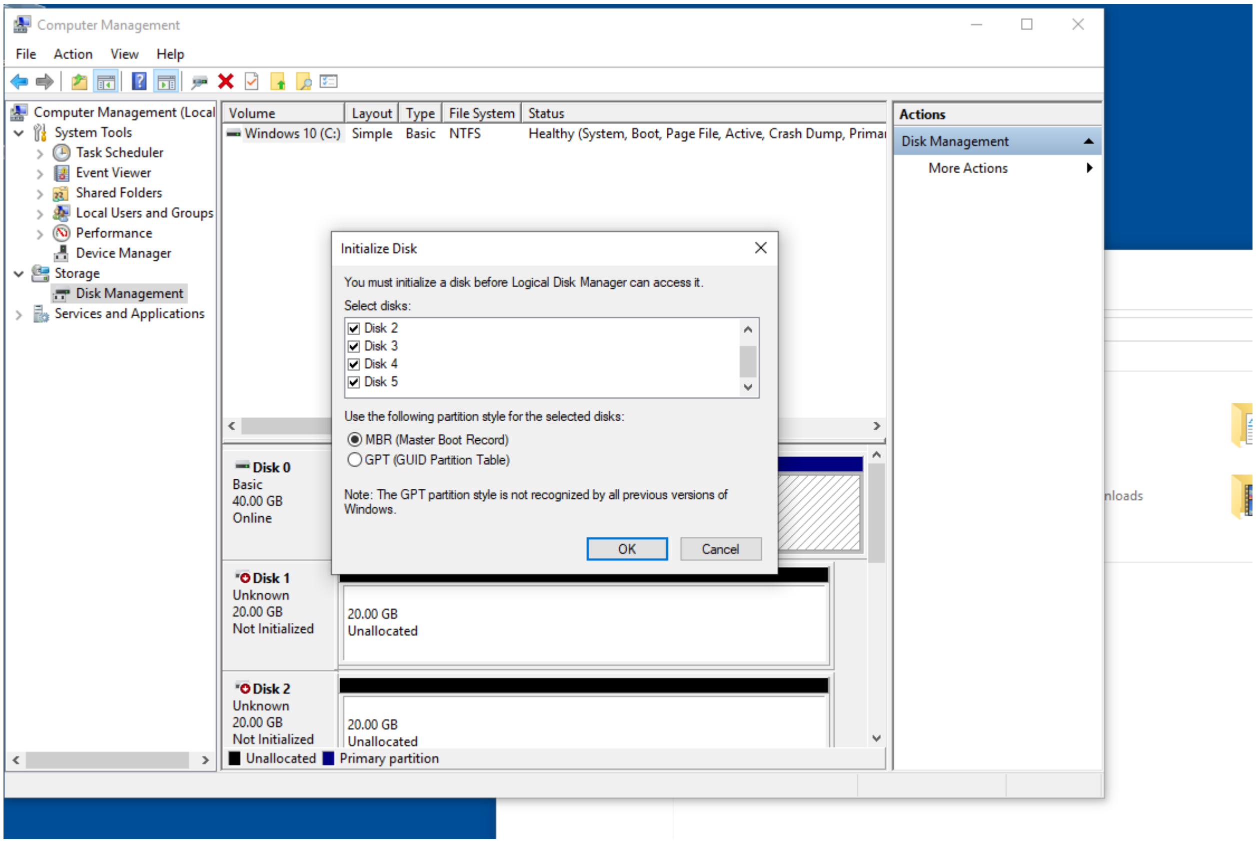
Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	40 GB
Hard Disk 2 (SCSI)	20 GB
Hard Disk 3 (SCSI)	20 GB
Hard Disk 5 (SCSI)	20 GB
Hard Disk 4 (SCSI)	20 GB
Hard Disk 6 (SCSI)	20 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	Host-only
Display	Auto detect

Memory

Specify tl
size must

Memory f

(Make sure to select single storage)



Volume	Layout	Type	File System	Status
Windows 10 (C:)	Simple	Basic	NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Primai

Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 2
☑ Disk 3
☑ Disk 4
☑ Disk 5

Use the following partition style for the selected disks:

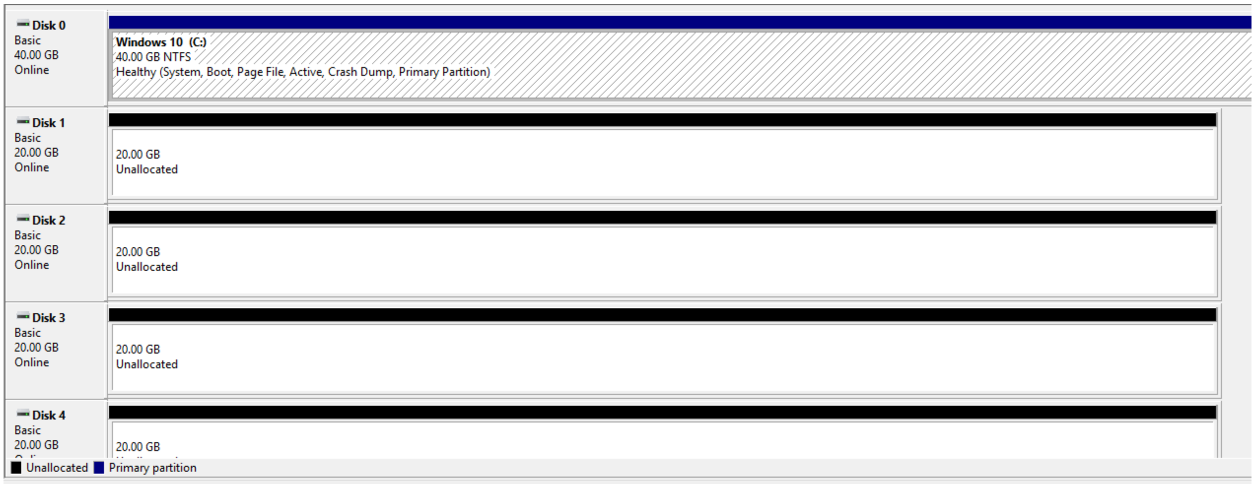
● MBR (Master Boot Record)
○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

Disk 0
Basic
40.00 GB
Online

Disk 1
Unknown
20.00 GB
Not Initialized
20.00 GB
Unallocated

Disk 2
Unknown
20.00 GB
Not Initialized
20.00 GB
Unallocated



Disk 0
Basic
40.00 GB
Online
Windows 10 (C:)
40.00 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)

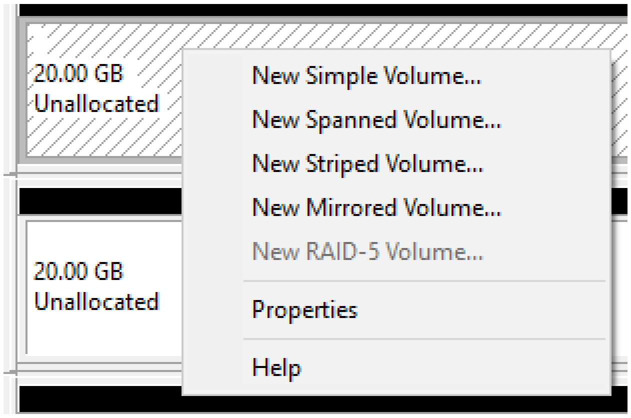
Disk 1
Basic
20.00 GB
Online
20.00 GB
Unallocated

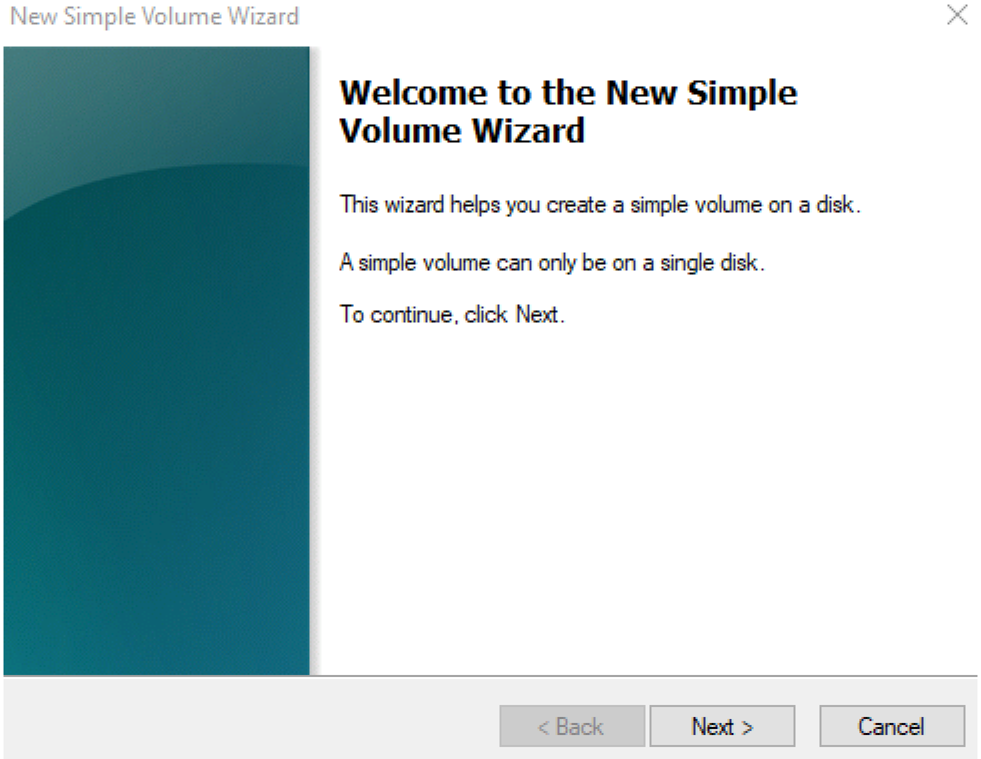
Disk 2
Basic
20.00 GB
Online
20.00 GB
Unallocated

Disk 3
Basic
20.00 GB
Online
20.00 GB
Unallocated

Disk 4
Basic
20.00 GB
20.00 GB

Right click on the disk, (simple voule, spanned, striped, mirror)



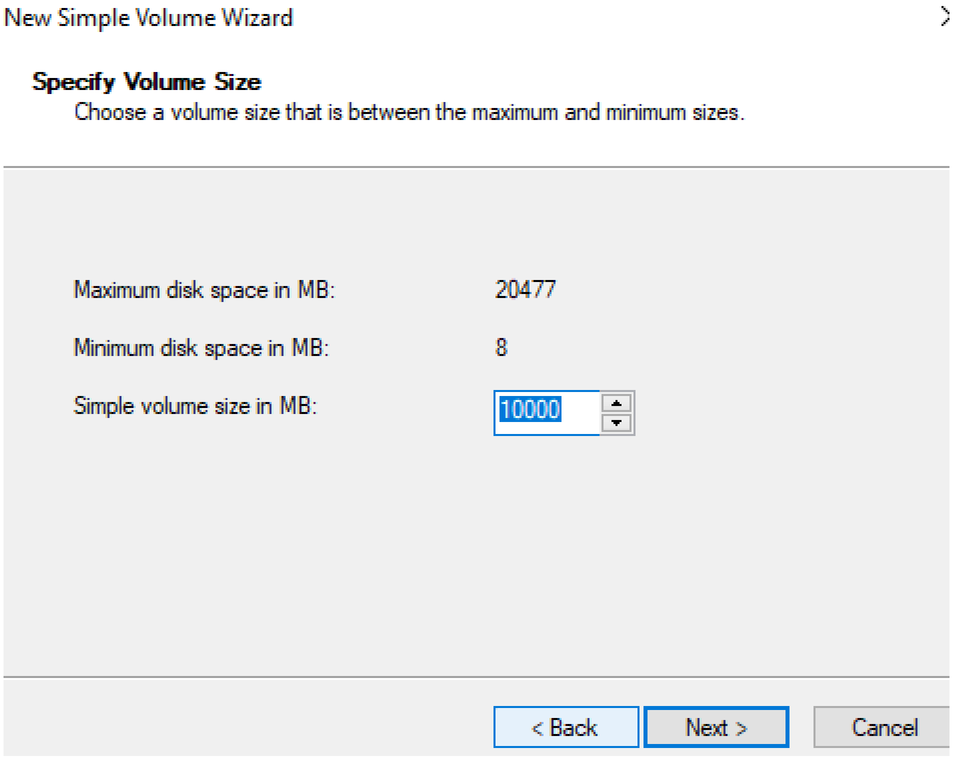


Welcome to the New Simple Volume Wizard

This wizard helps you create a simple volume on a disk.

A simple volume can only be on a single disk.

To continue, click Next.



New Simple Volume Wizard

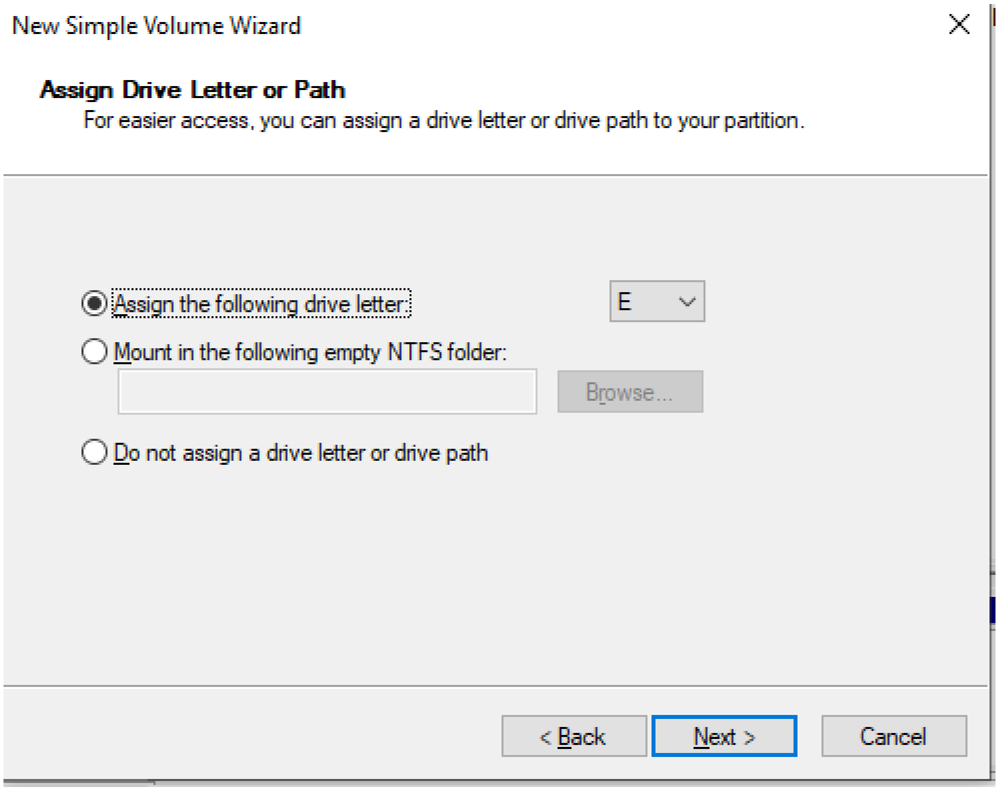
Specify Volume Size

Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 20477

Minimum disk space in MB: 8

Simple volume size in MB: 10000



New Simple Volume Wizard

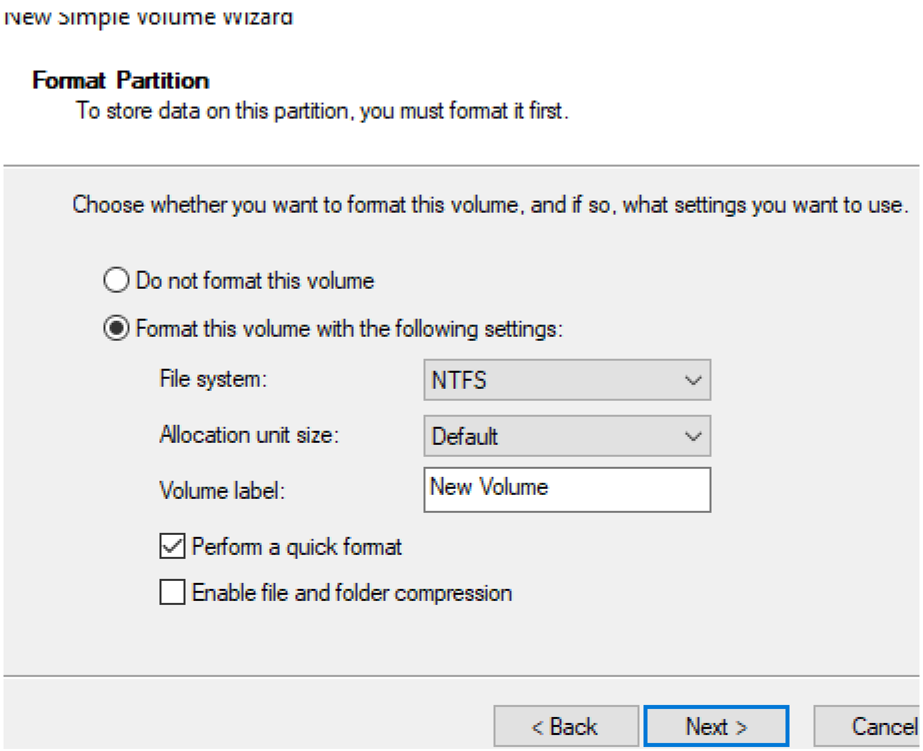
Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: E

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path



New Simple Volume Wizard

Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

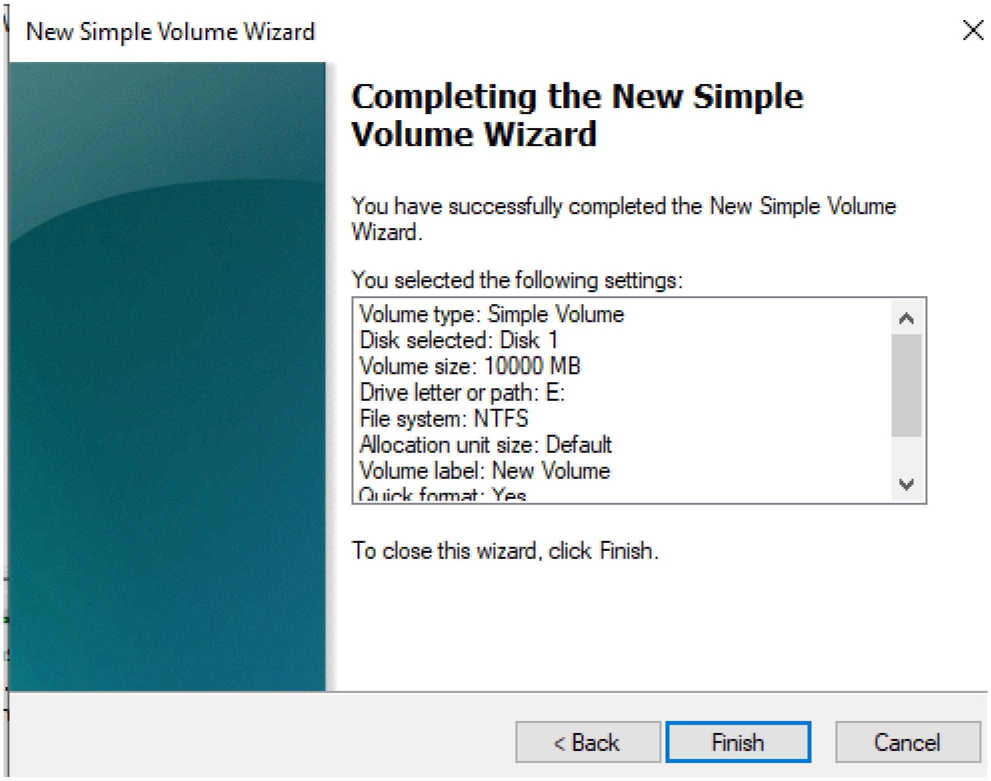
File system: NTFS

Allocation unit size: Default

Volume label: New Volume

☑ Perform a quick format

□ Enable file and folder compression



New Simple Volume Wizard

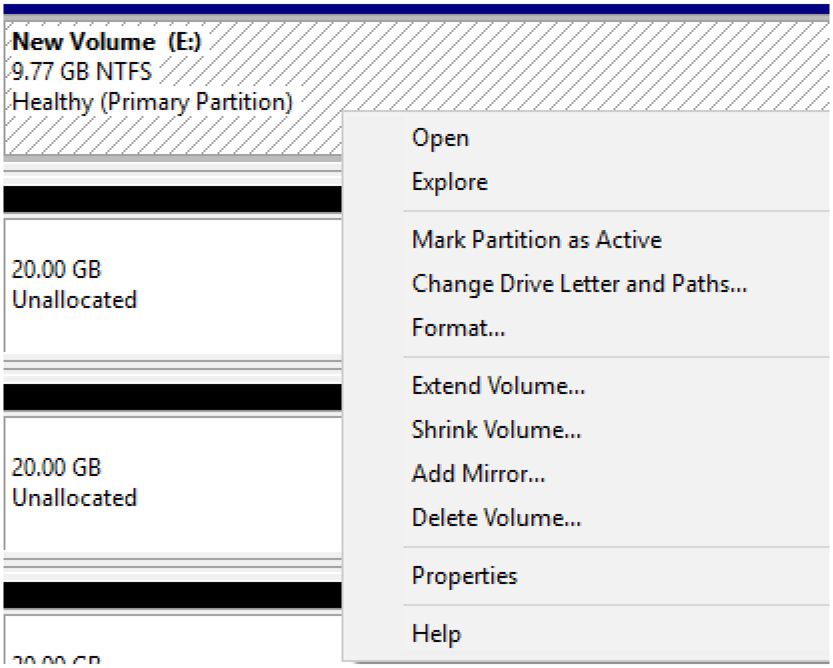
Completing the New Simple Volume Wizard

You have successfully completed the New Simple Volume Wizard.

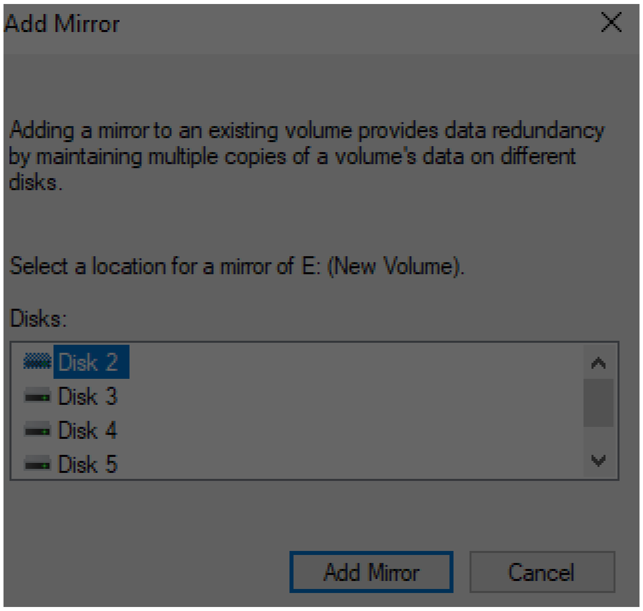
You selected the following settings:

Volume type: Simple Volume
Disk selected: Disk 1
Volume size: 10000 MB
Drive letter or path: E:
File system: NTFS
Allocation unit size: Default
Volume label: New Volume
Quick format: Yes

To close this wizard, click Finish.

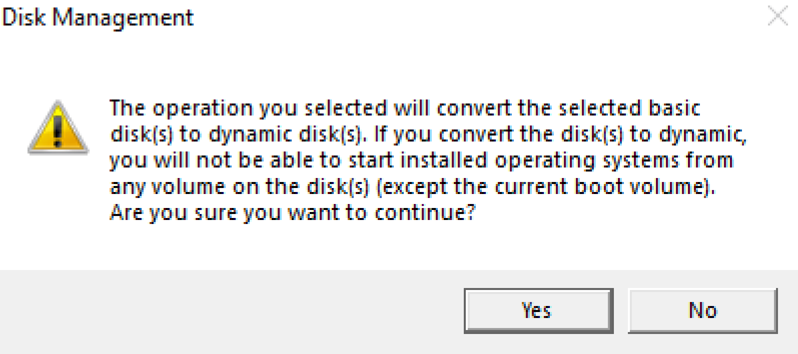


(add mirror)

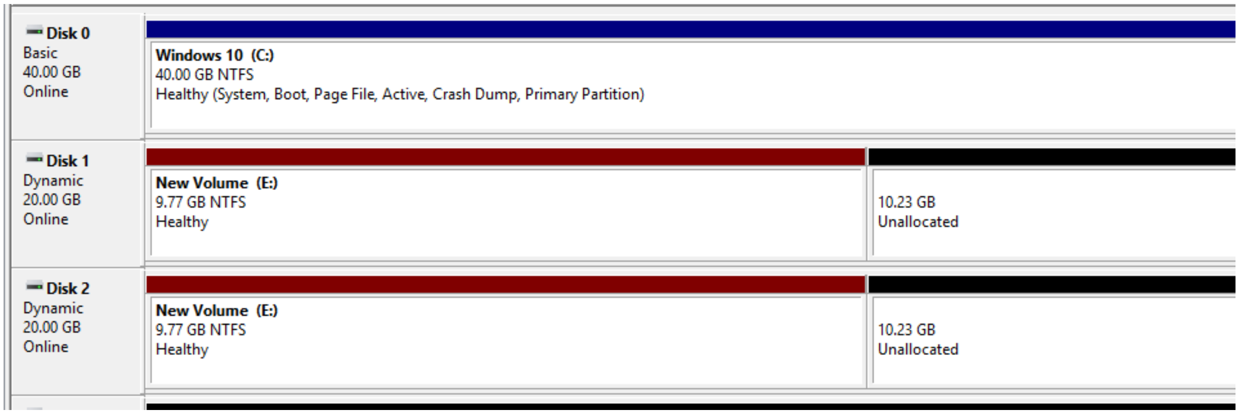


Adding a mirror to an existing volume provides data redundancy by maintaining multiple copies of a volume's data on different disks.

Select a location for a mirror of E: (New Volume).



The operation you selected will convert the selected basic disk(s) to dynamic disk(s). If you convert the disk(s) to dynamic, you will not be able to start installed operating systems from any volume on the disk(s) (except the current boot volume). Are you sure you want to continue?



Disk 0
Basic
40.00 GB
Online

Windows 10 (C:)
40.00 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)

Disk 1
Dynamic
20.00 GB
Online

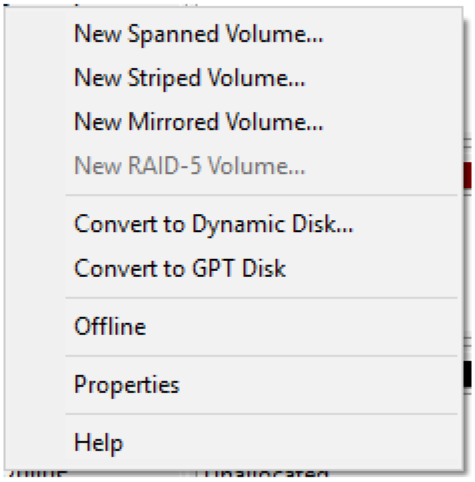
New Volume (E:)
9.77 GB NTFS
Healthy

10.23 GB
Unallocated

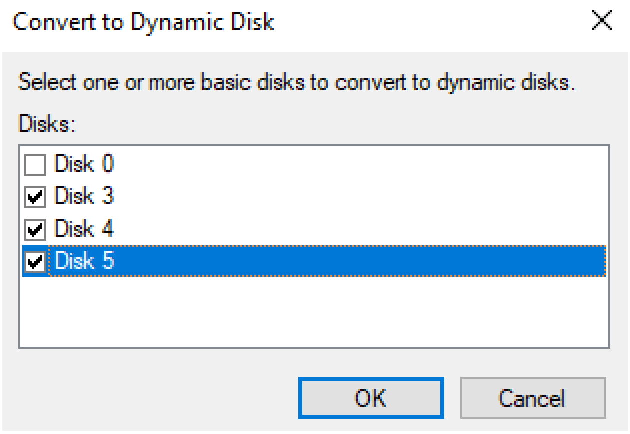
Disk 2
Dynamic
20.00 GB
Online

New Volume (E:)
9.77 GB NTFS
Healthy

10.23 GB
Unallocated



(Right click on disk 3, Select Dynamic)

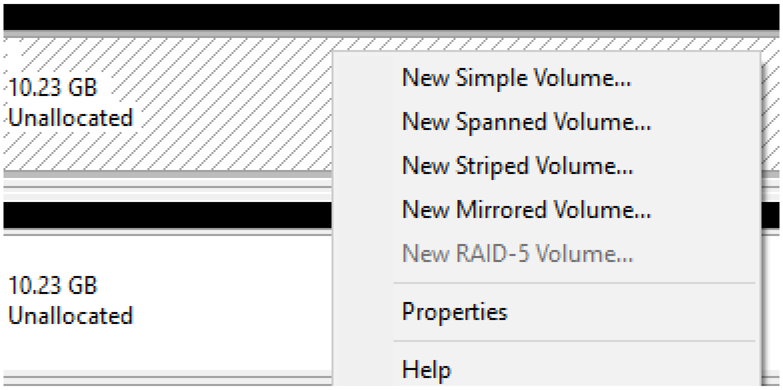


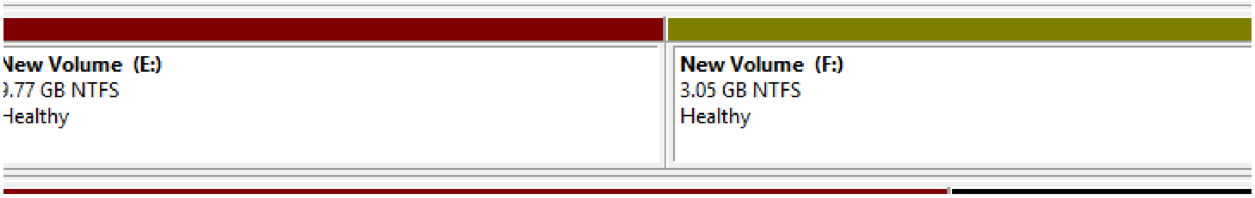
Convert to Dynamic Disk

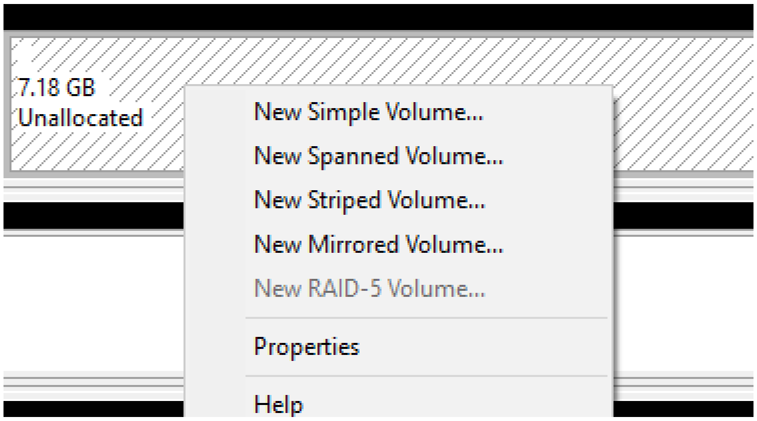
Select one or more basic disks to convert to dynamic disks.

Disks:

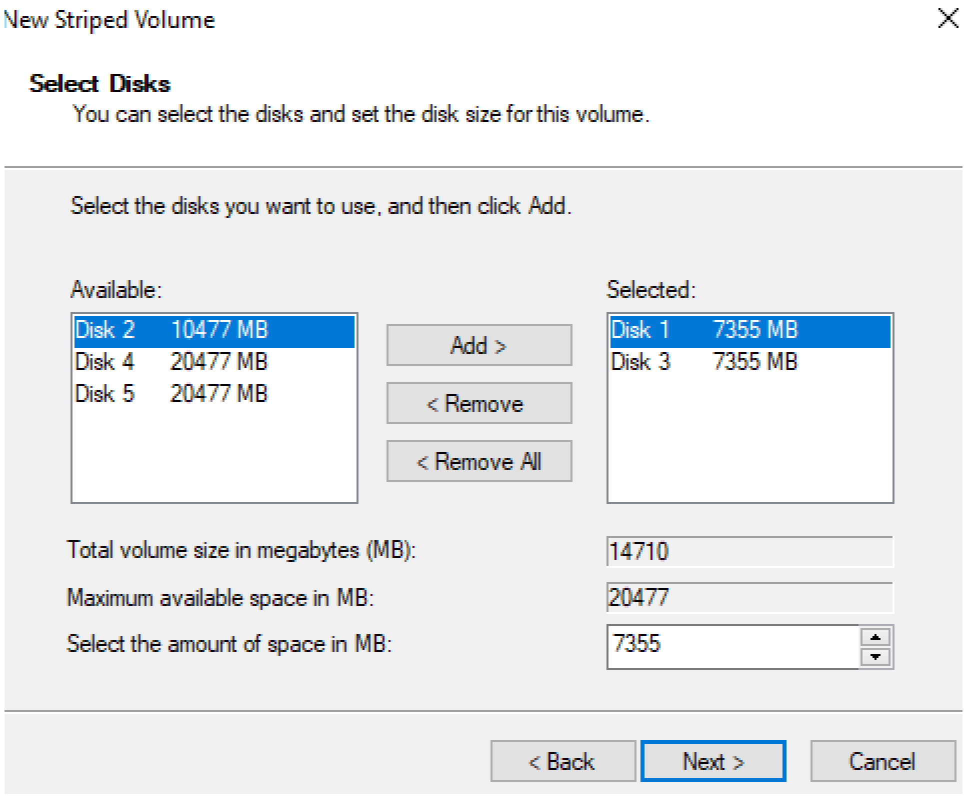
- □ Disk 0
- ☑ Disk 3
- ☑ Disk 4
- ☑ Disk 5







(Stripped volume)



New Striped Volume

Select Disks

You can select the disks and set the disk size for this volume.

Select the disks you want to use, and then click Add.

Available:

Disk 2	10477 MB
Disk 4	20477 MB
Disk 5	20477 MB

Selected:

Disk 1	7355 MB
Disk 3	7355 MB

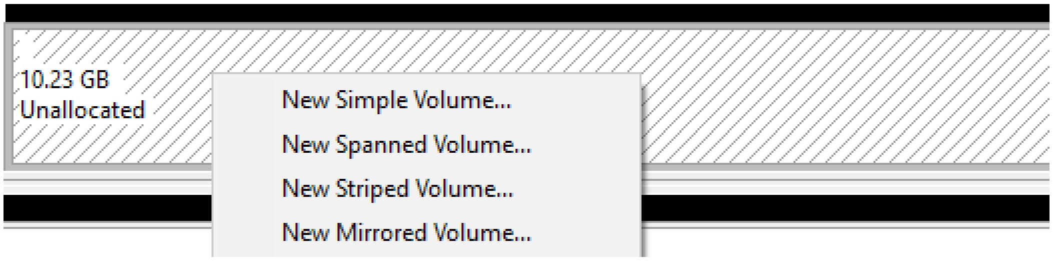
Total volume size in megabytes (MB): 14710

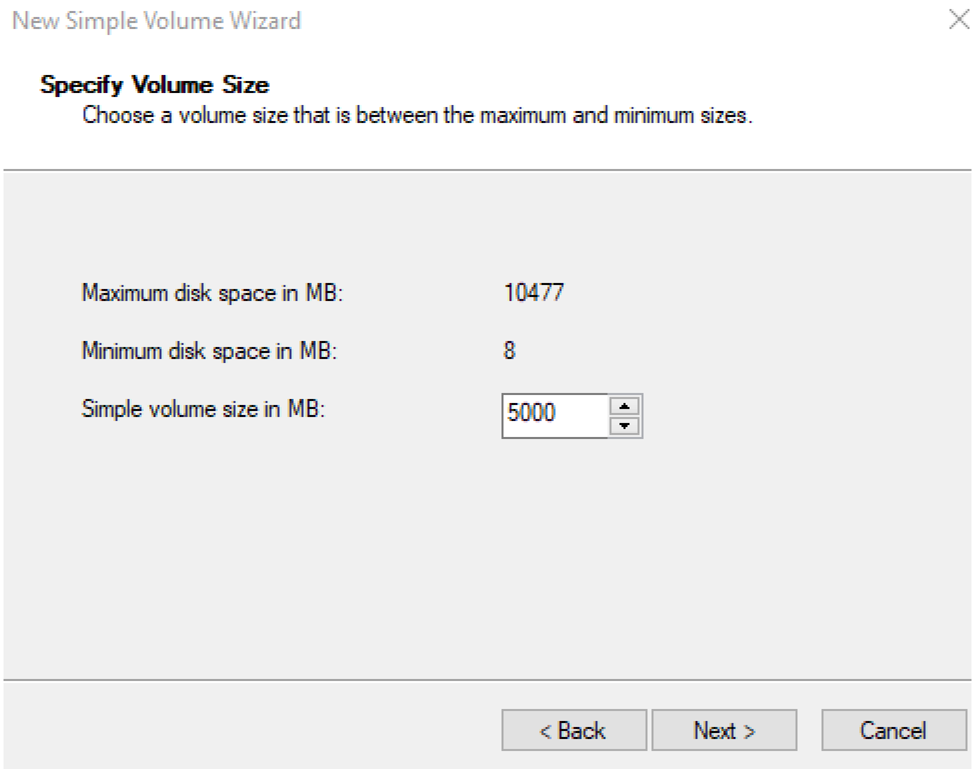
Maximum available space in MB: 20477

Select the amount of space in MB: 7355

(all defaults where no pictures are inserted)

New simple volume (disk 2)





New Simple Volume Wizard

Specify Volume Size

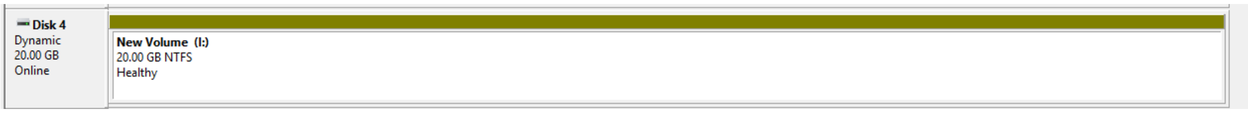
Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 10477

Minimum disk space in MB: 8

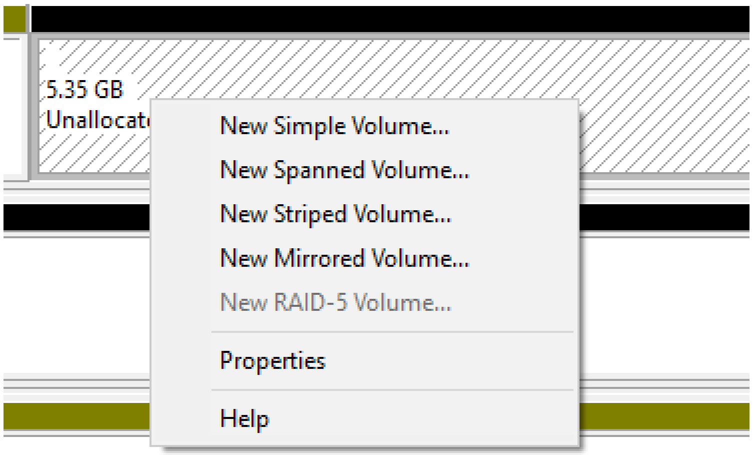
Simple volume size in MB: 5000

On disk 4 make a simple disk that is the whole disk:

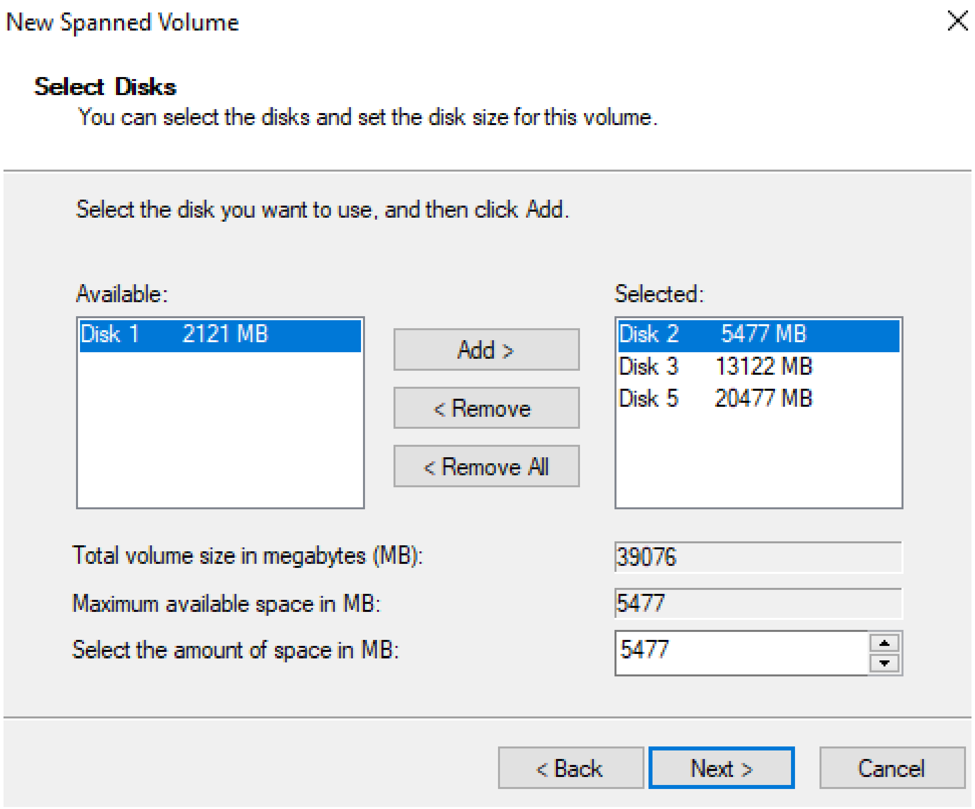


Disk 4
Dynamic
20.00 GB
Online

New Volume (I:)
20.00 GB NTFS
Healthy



New spanned volume disk 2



New Spanned Volume

Select Disks

You can select the disks and set the disk size for this volume.

Select the disk you want to use, and then click Add.

Available:

Disk	Size
Disk 1	2121 MB

Selected:

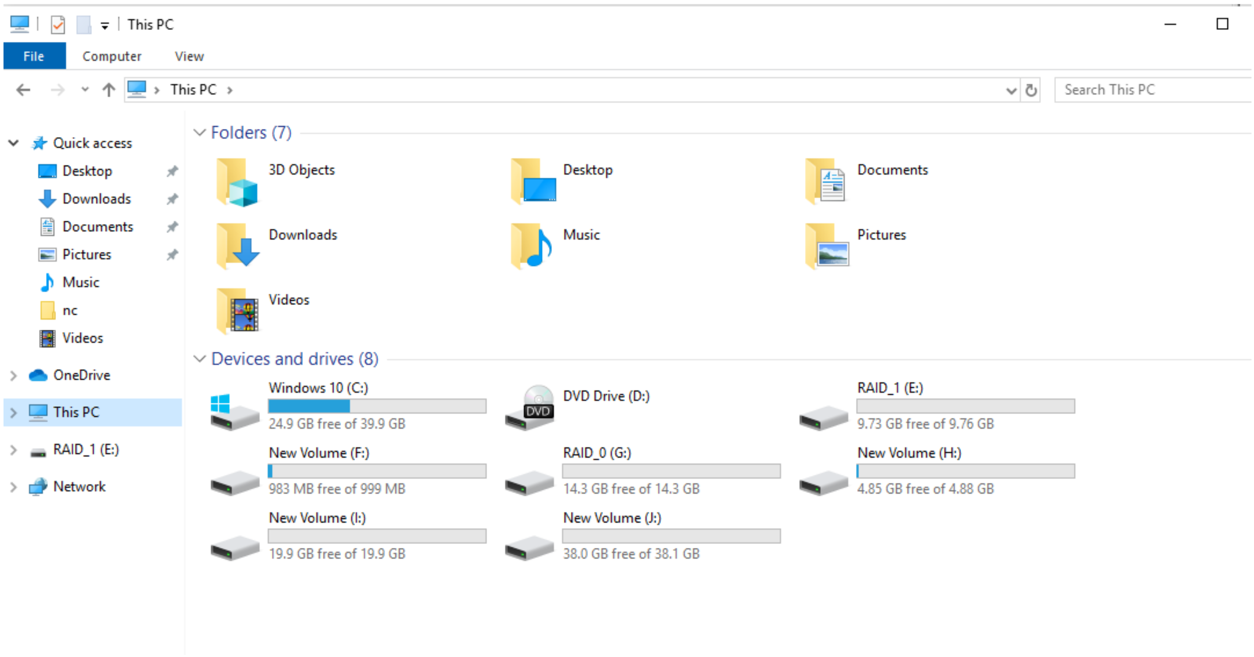
Disk	Size
Disk 2	5477 MB
Disk 3	13122 MB
Disk 5	20477 MB

Total volume size in megabytes (MB): 39076

Maximum available space in MB: 5477

Select the amount of space in MB: 5477

(I had a little left over on 1 because I allocated too much for simple drive and then when shrinking it I wasn't able to add it to raid)



Windows 10 (C:) — 24.9 GB free of 39.9 GB

DVD Drive (D:)

RAID_1 (E:) — 9.73 GB free of 9.76 GB

New Volume (F:) — 983 MB free of 999 MB

RAID_0 (G:) — 14.3 GB free of 14.3 GB

New Volume (H:) — 4.85 GB free of 4.88 GB

New Volume (I:) — 19.9 GB free of 19.9 GB

New Volume (J:) — 38.0 GB free of 38.1 GB