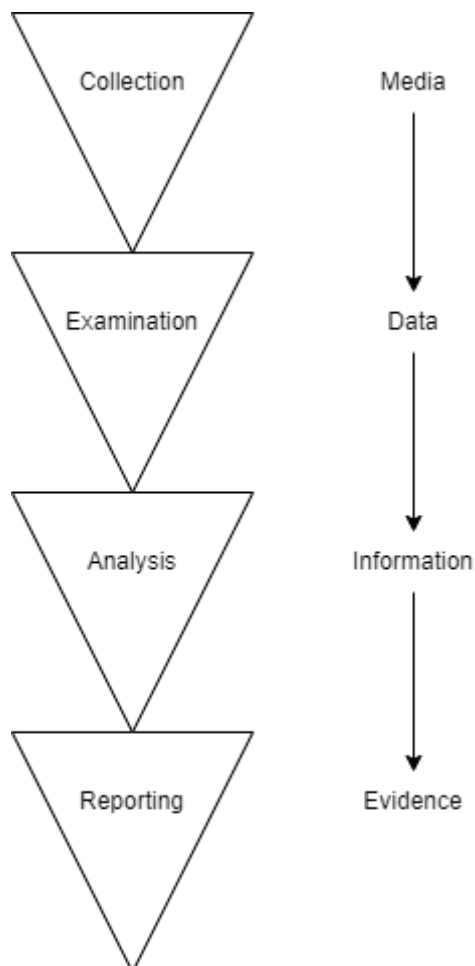


# Data Collection Process:

- Forensic Process.
- Compromised system containment.
- Memory acquisition.
- Disk acquisition.

## Forensic Process



- Collection needs:
  - Data Identification

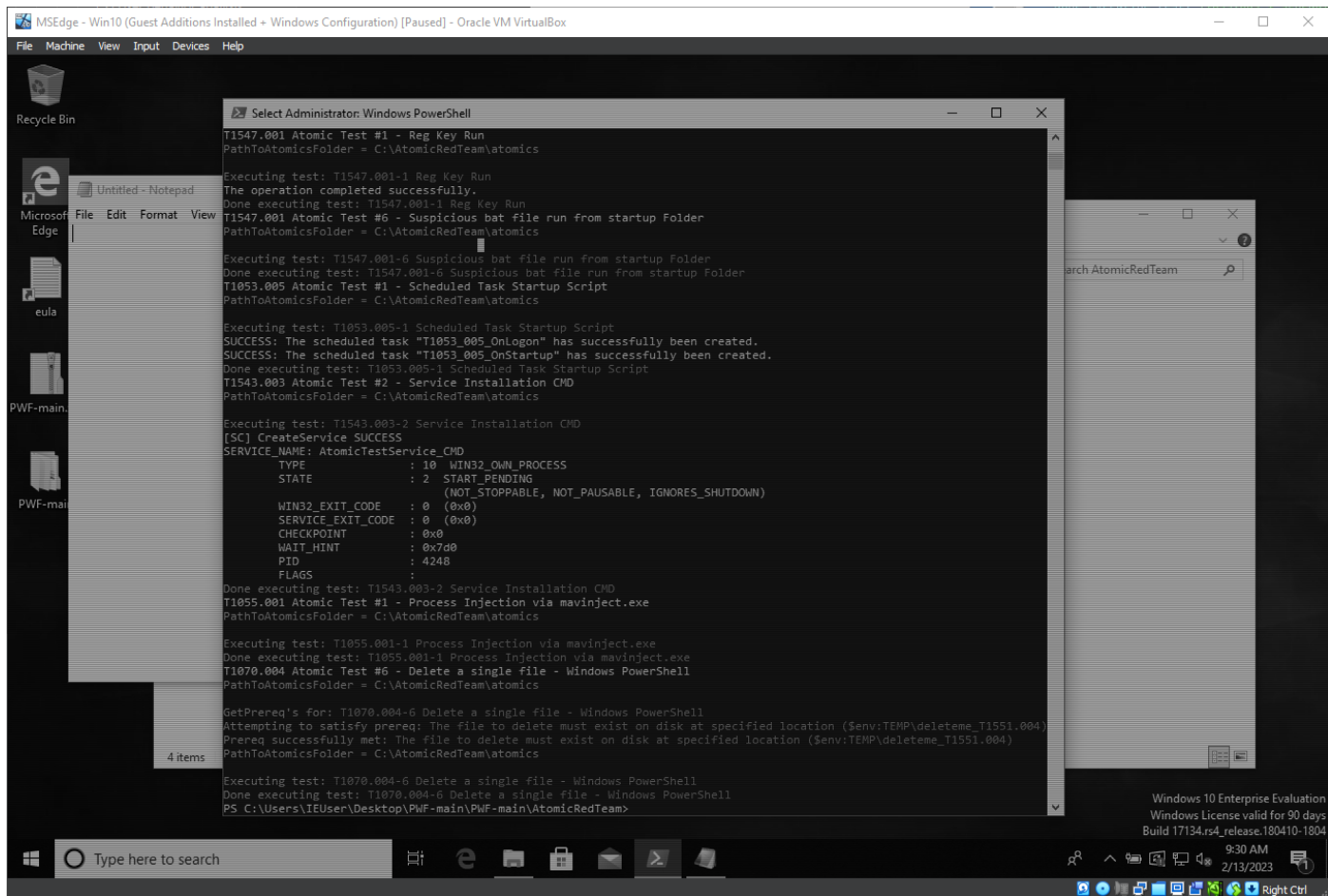
- Data Acquisition
- Verifying Integrity of the data



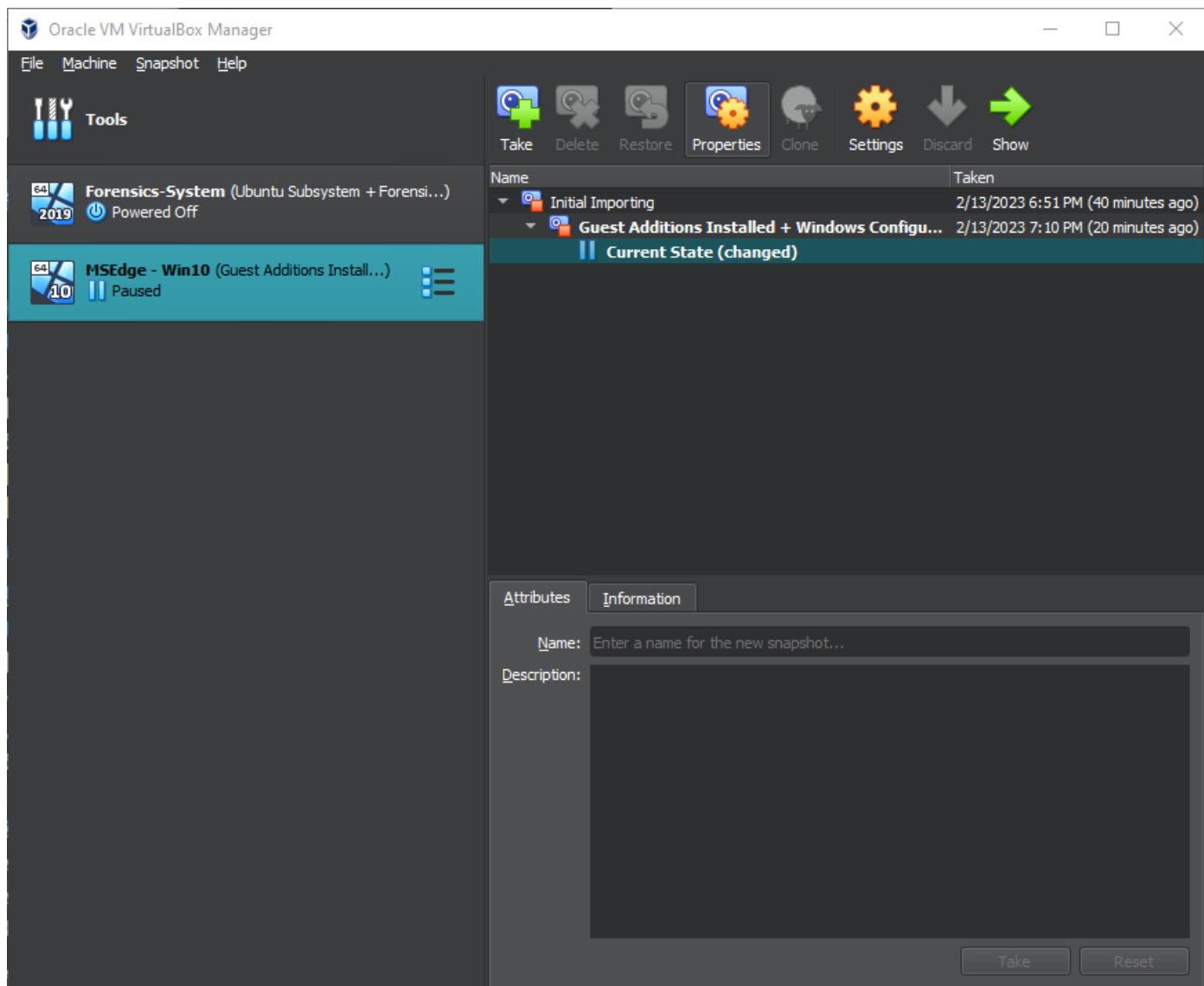
## Compromised system containment

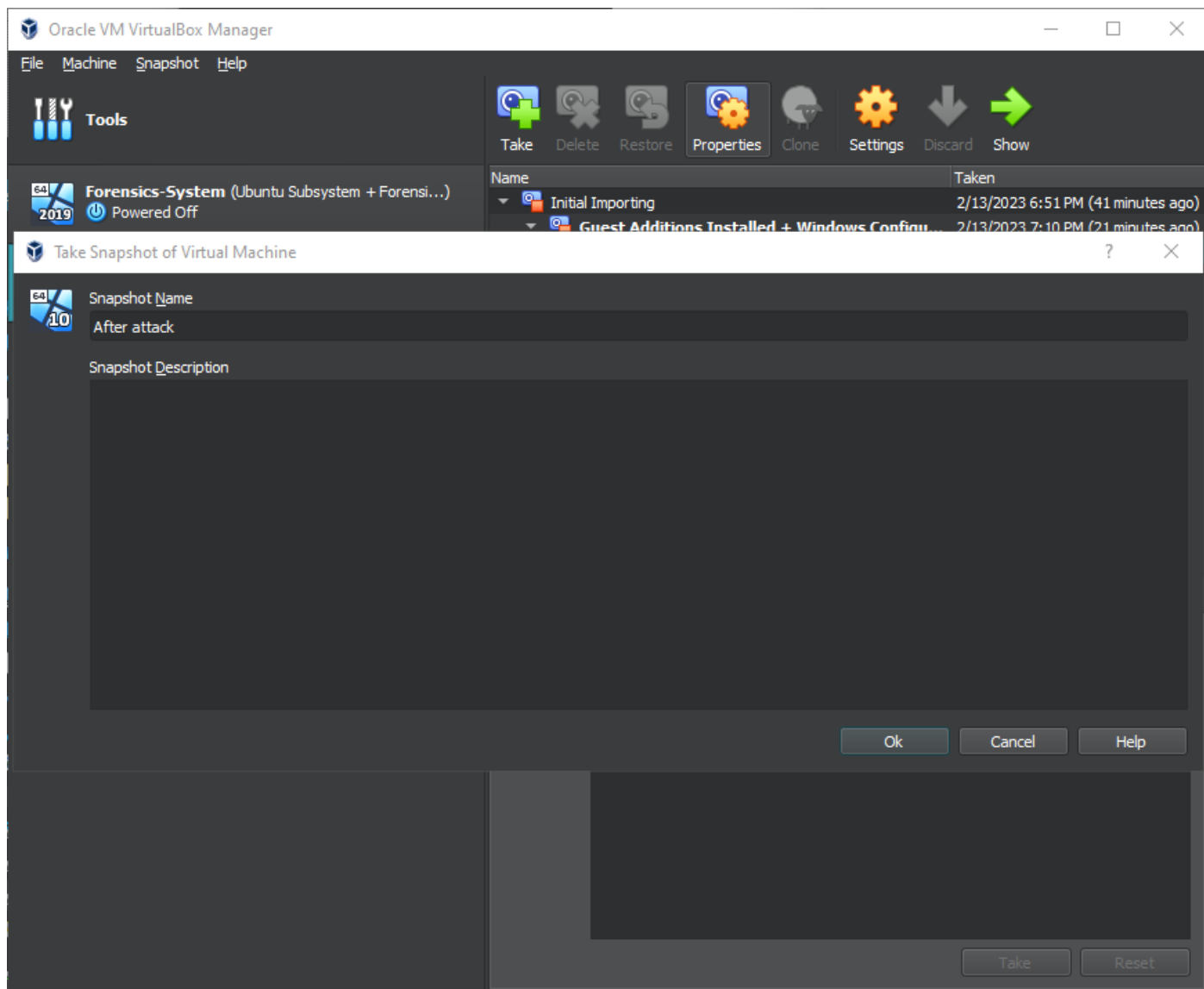
- We want to make sure we contain the system as quickly as possible, not to expose the rest enterprise environment.
- We don't want to tamper with the evidence, to remove files, create files, or another operations.
- Timeline of the cyber attack:
  - 9:26-27AM 2/13/2023.
  - 9:29-30AM 2/13/2023.
- Pause the virtual machine for memory preservation.



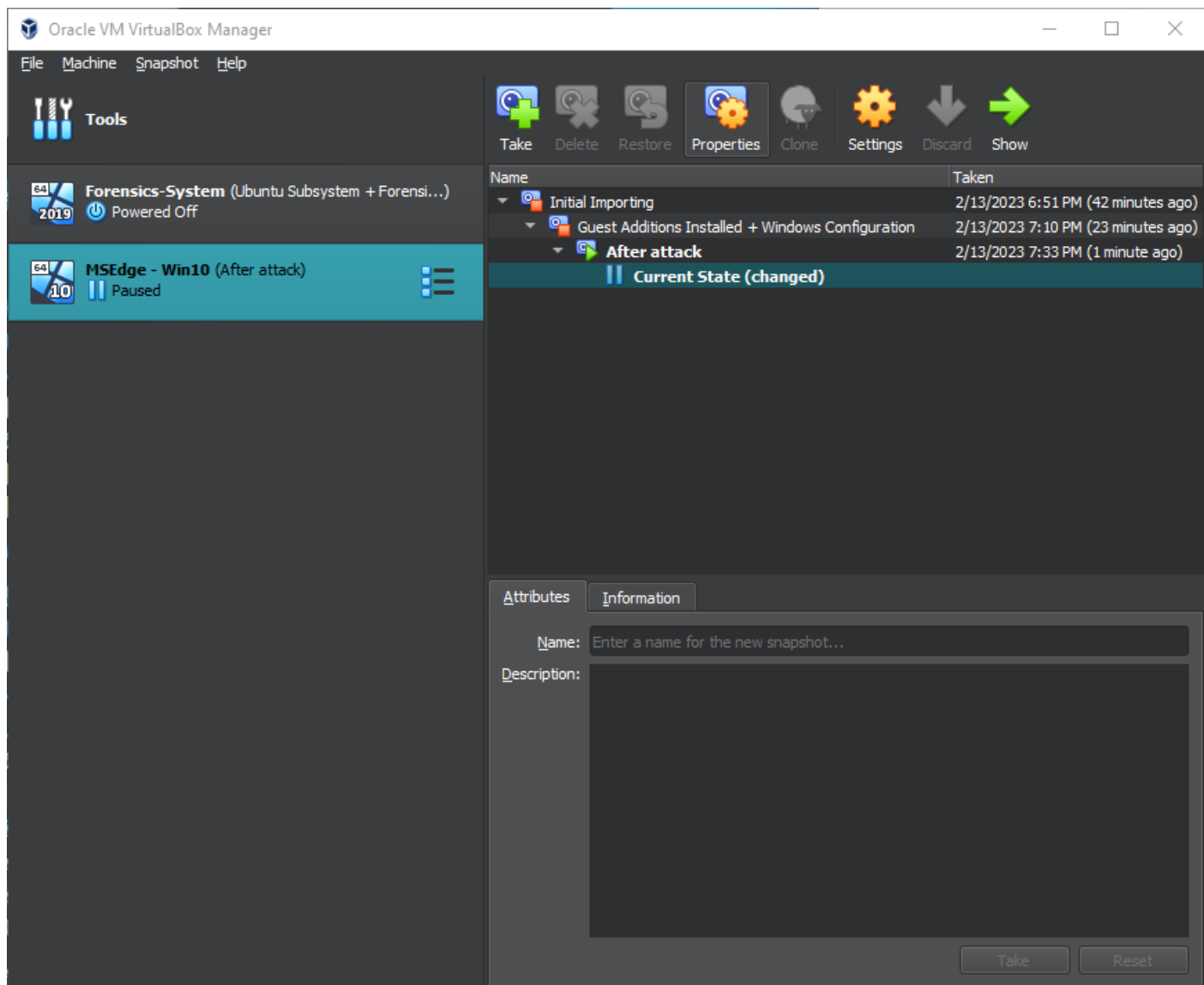


- Take snapshot of the vm.





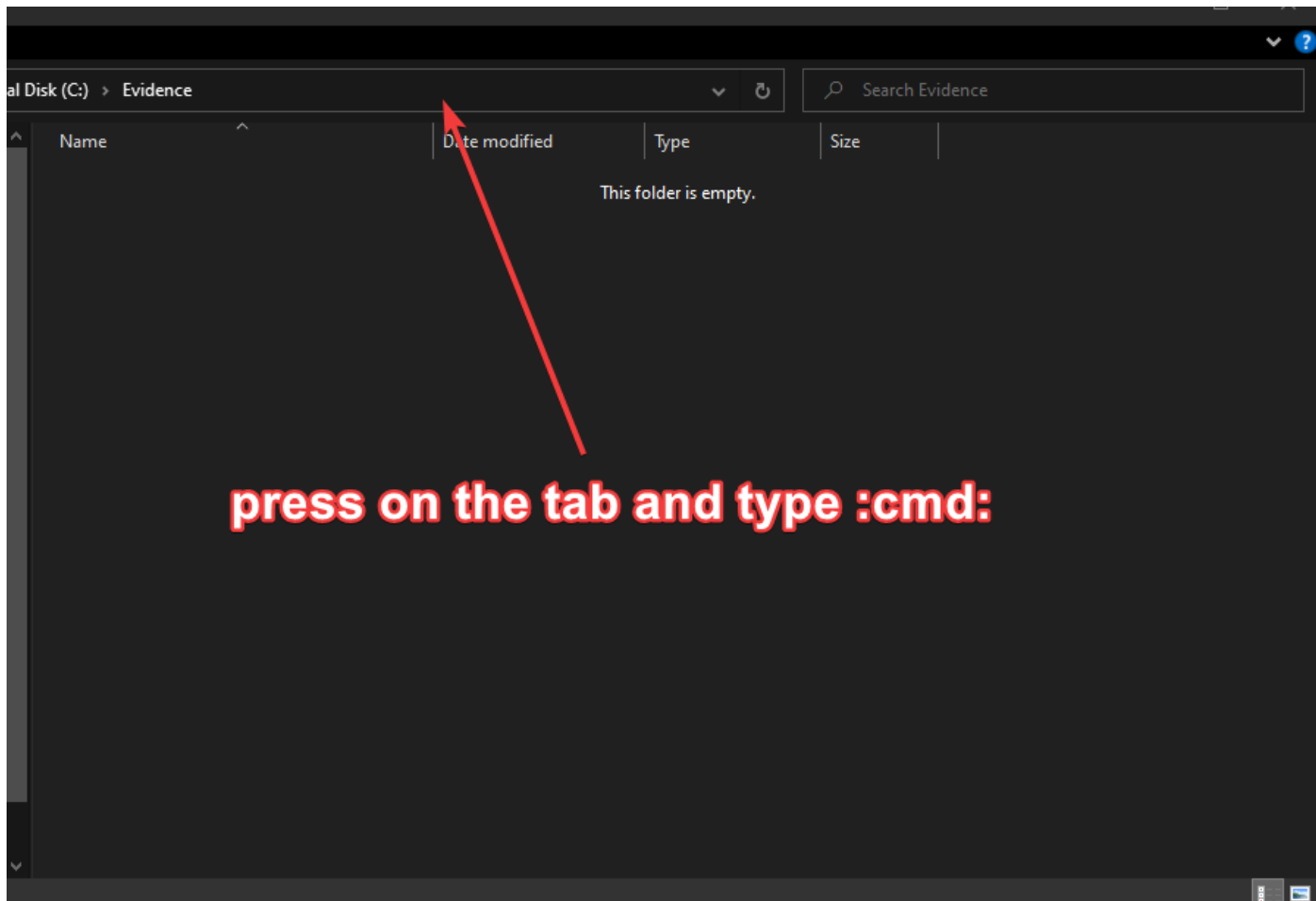
- Because of the snapshot feature , we can later continue to run the virtual machine in a safe environment , to investigate it live.



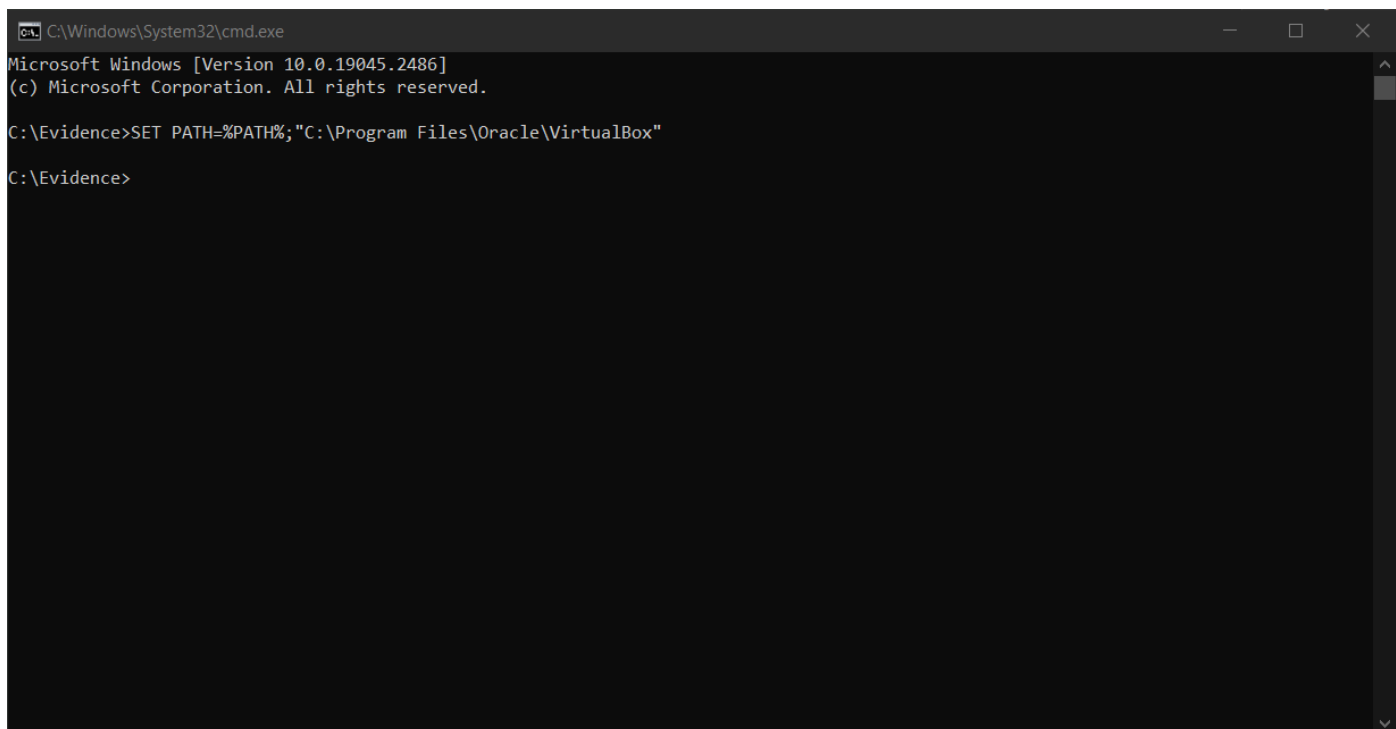
## Memory acquisition

- We will use order of volatility for evidence acquisition, which refers to the idea that you should collect evidence starting with the most volatile and moving to the least volatile.
- Create Evidence folder.



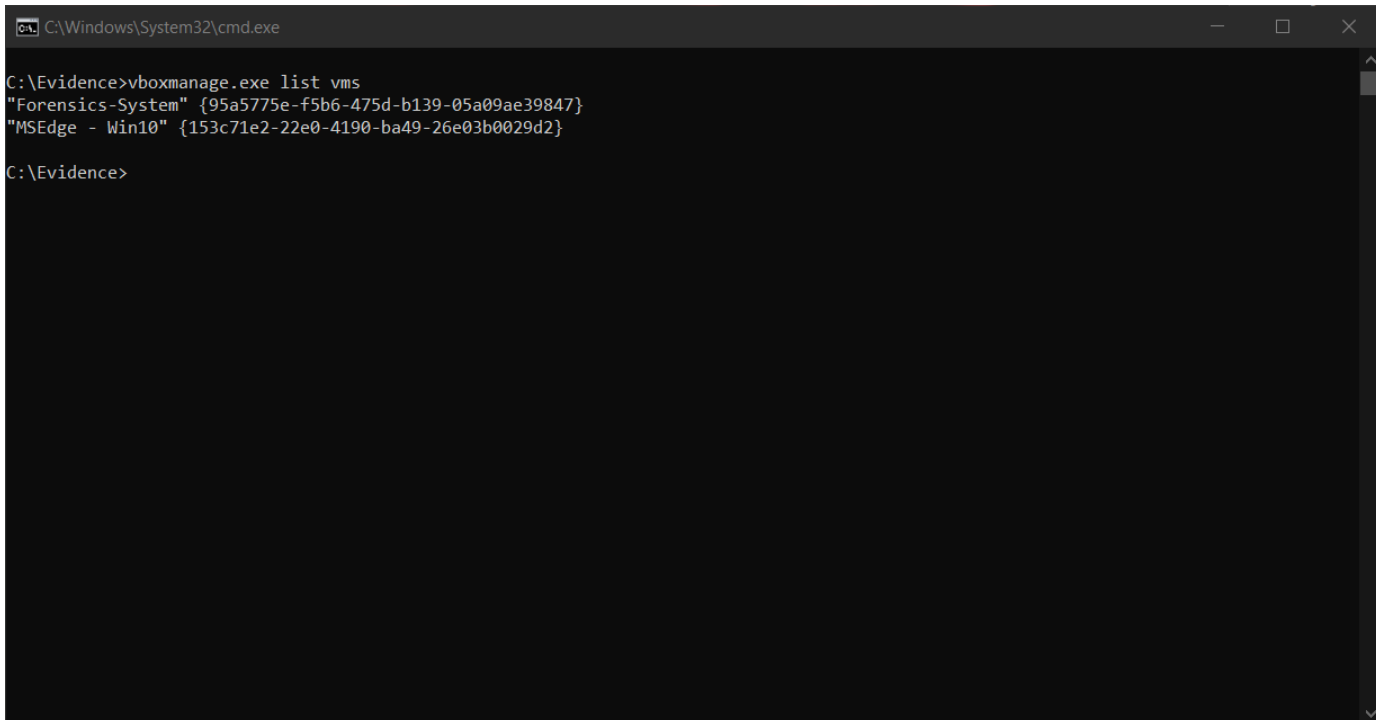


- Set Path for the vboxmanage , for the use of the executable as an environment variable.





- List VMs to find compromised machine ID.

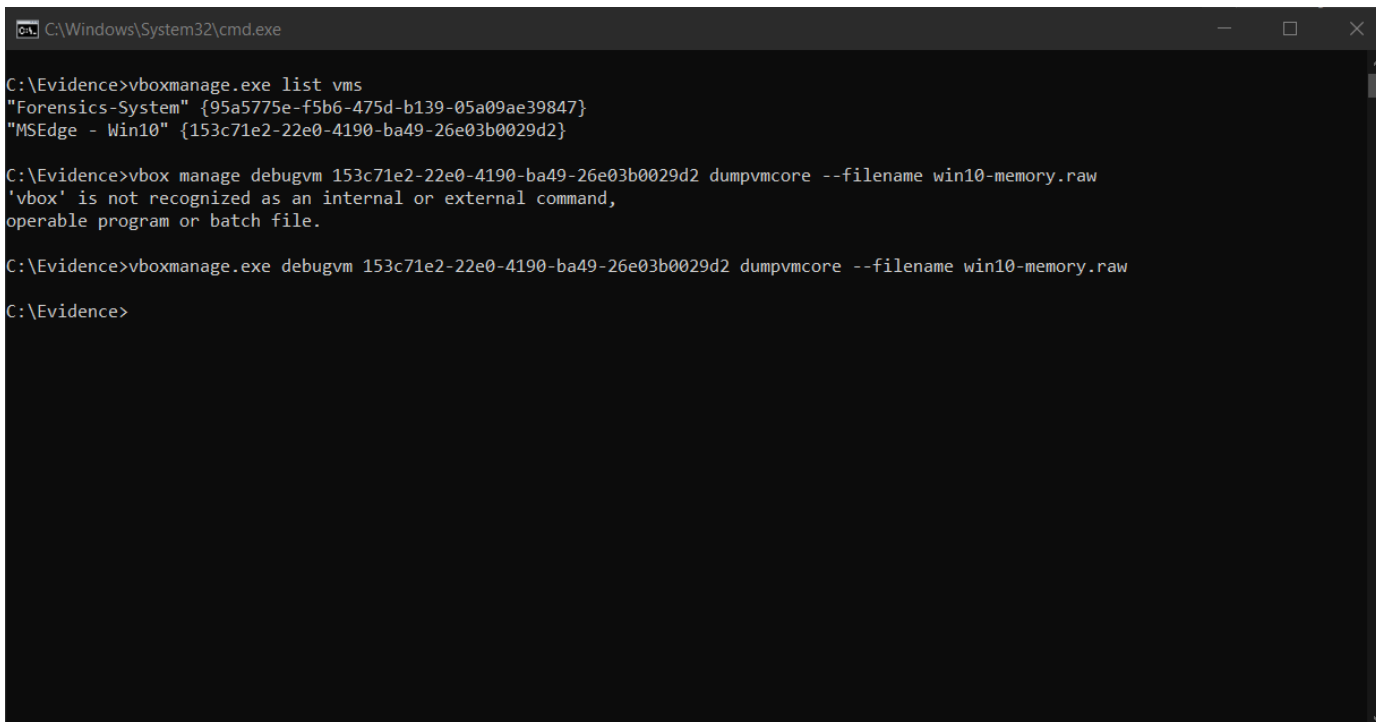


```
C:\Windows\System32\cmd.exe

C:\Evidence>vboxmanage.exe list vms
"Forensics-System" {95a5775e-f5b6-475d-b139-05a09ae39847}
"MSEdge - Win10" {153c71e2-22e0-4190-ba49-26e03b0029d2}

C:\Evidence>
```

- Memory acquisition, with dumpvmcore, it makes a bit by bit copy of the RAM.



```
C:\Windows\System32\cmd.exe

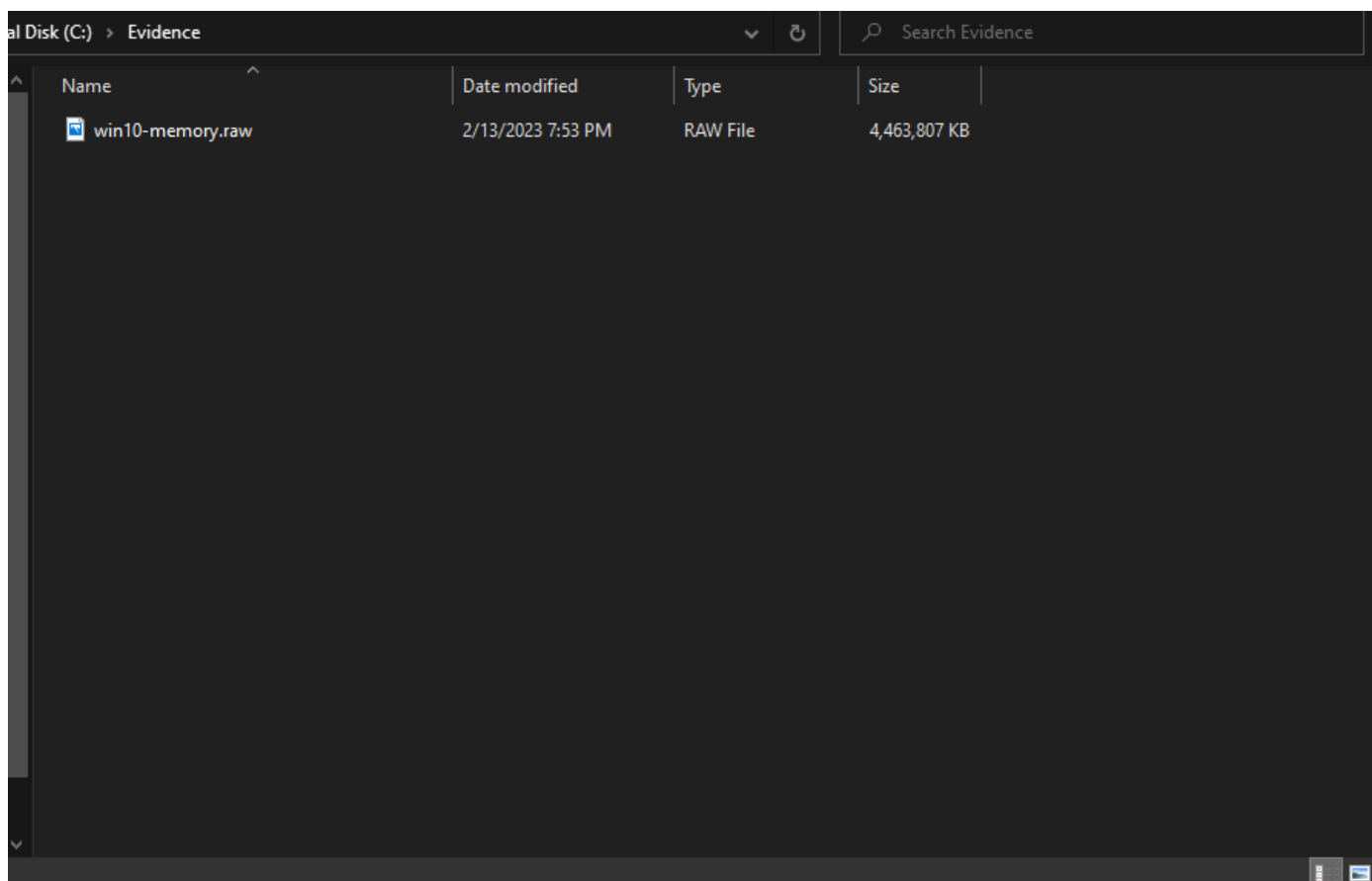
C:\Evidence>vboxmanage.exe list vms
"Forensics-System" {95a5775e-f5b6-475d-b139-05a09ae39847}
"MSEdge - Win10" {153c71e2-22e0-4190-ba49-26e03b0029d2}

C:\Evidence>vbox manage debugvm 153c71e2-22e0-4190-ba49-26e03b0029d2 dumpvmcore --filename win10-memory.raw
'vbox' is not recognized as an internal or external command,
operable program or batch file.

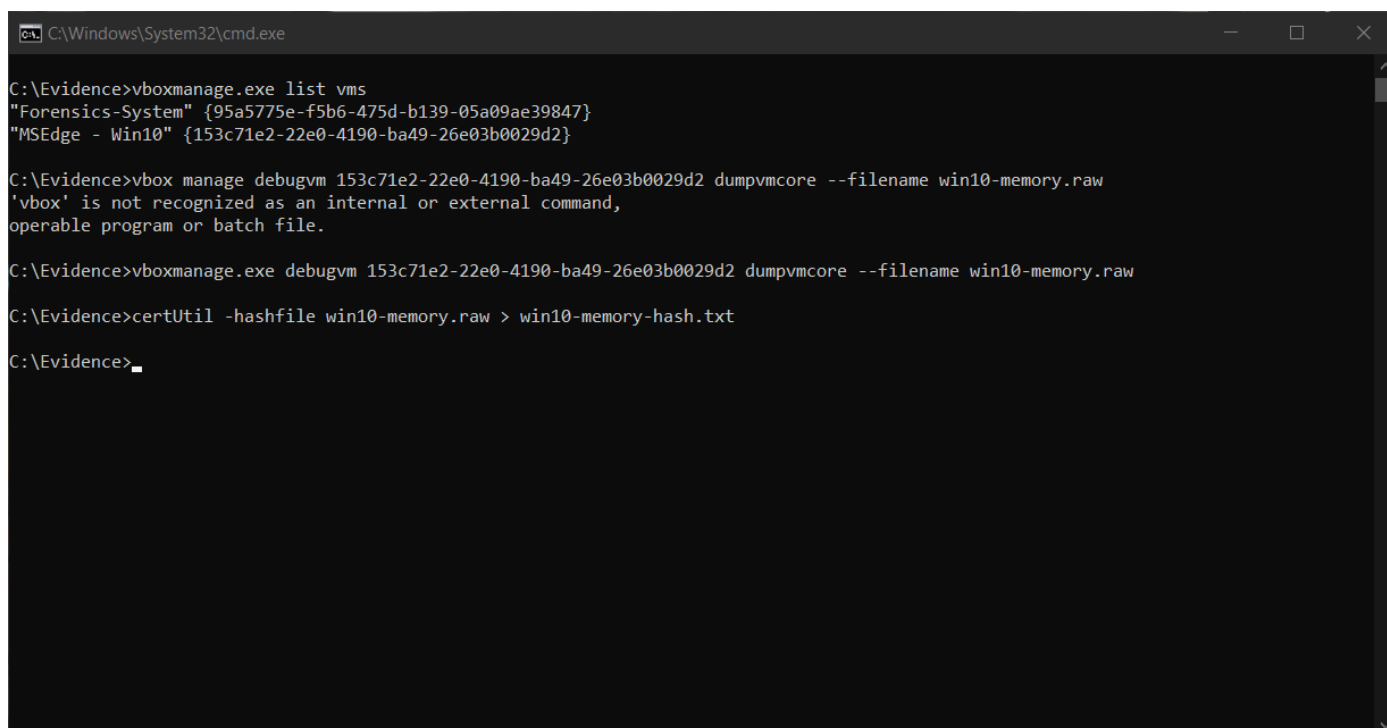
C:\Evidence>vboxmanage.exe debugvm 153c71e2-22e0-4190-ba49-26e03b0029d2 dumpvmcore --filename win10-memory.raw

C:\Evidence>
```

- Memory acquisition, with dumpvmcore.



- Make a hash (SHA1) of the memory file because that ensures the file is still the original , and has not been tampered with.



```
C:\Windows\System32\cmd.exe

C:\Evidence>vboxmanage.exe list vms
"Forensics-System" {95a5775e-f5b6-475d-b139-05a09ae39847}
"MSEdge - Win10" {153c71e2-22e0-4190-ba49-26e03b0029d2}

C:\Evidence>vbox manage debugvm 153c71e2-22e0-4190-ba49-26e03b0029d2 dumpvmcore --filename win10-memory.raw
'vbox' is not recognized as an internal or external command,
operable program or batch file.

C:\Evidence>vboxmanage.exe debugvm 153c71e2-22e0-4190-ba49-26e03b0029d2 dumpvmcore --filename win10-memory.raw

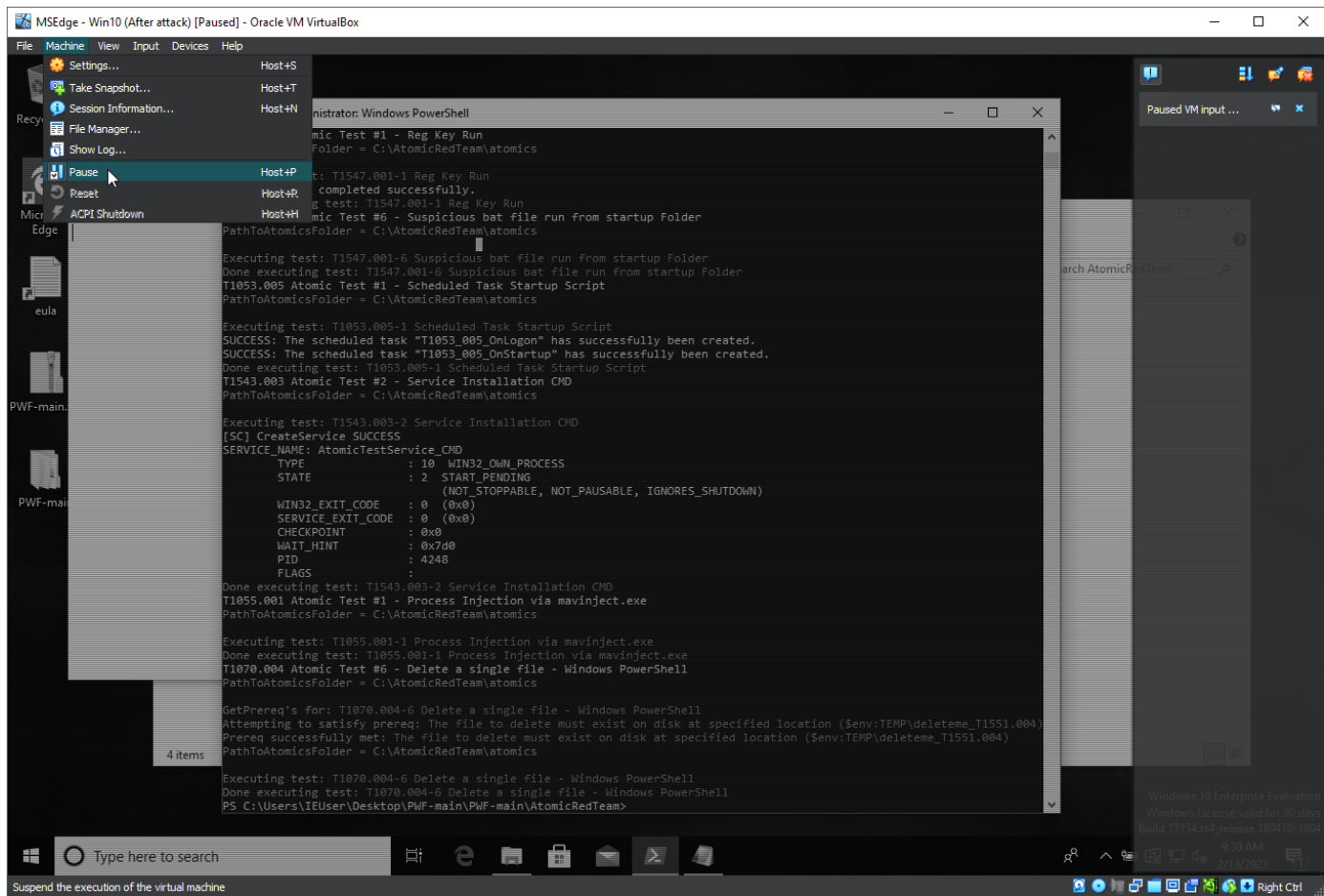
C:\Evidence>certUtil -hashfile win10-memory.raw > win10-memory-hash.txt

C:\Evidence>type win10-memory-hash.txt
SHA1 hash of win10-memory.raw:
683f47a6461ab7a88c7d7655160c315b9691dd44
CertUtil: -hashfile command completed successfully.

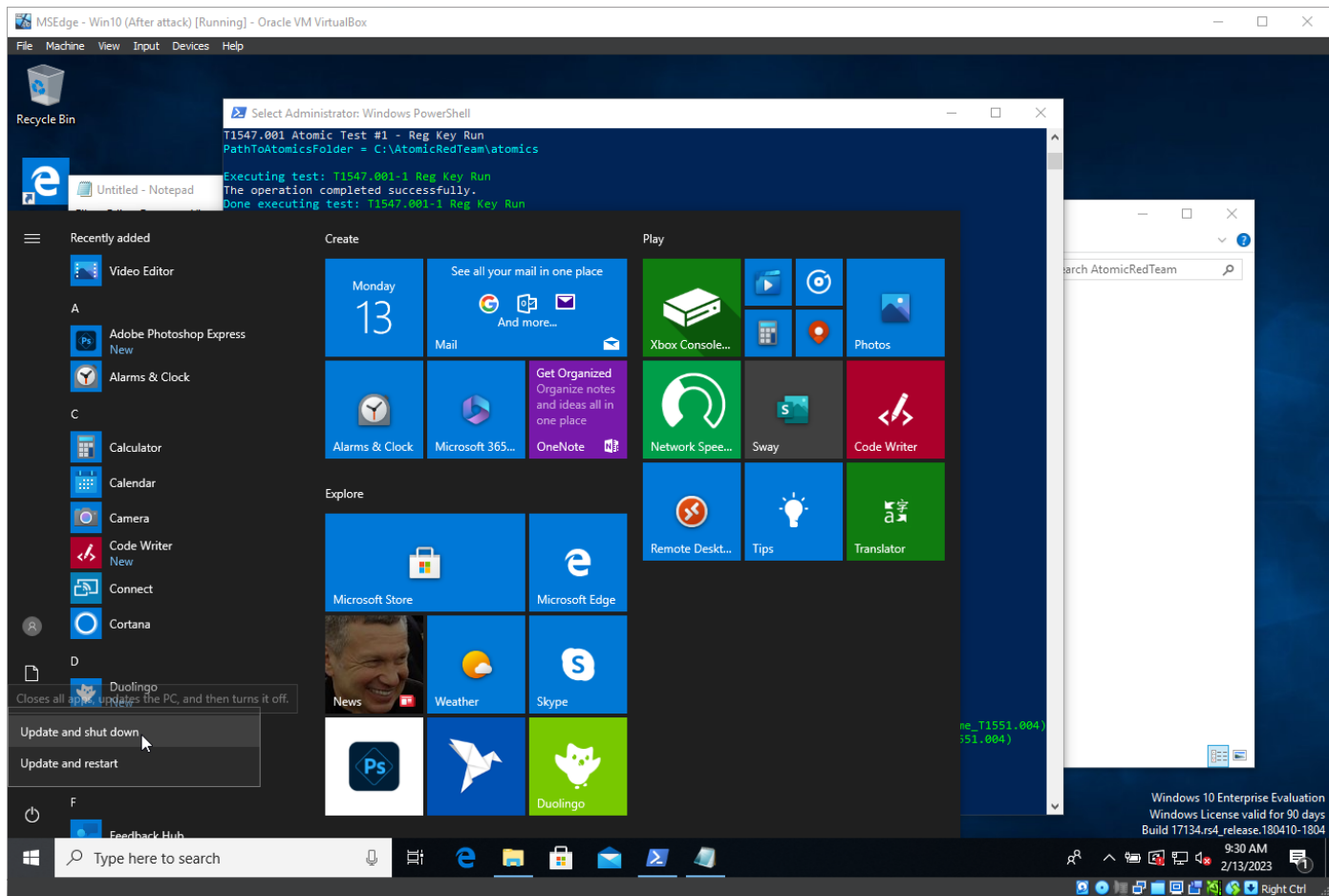
C:\Evidence>
```

## Disk acquisition

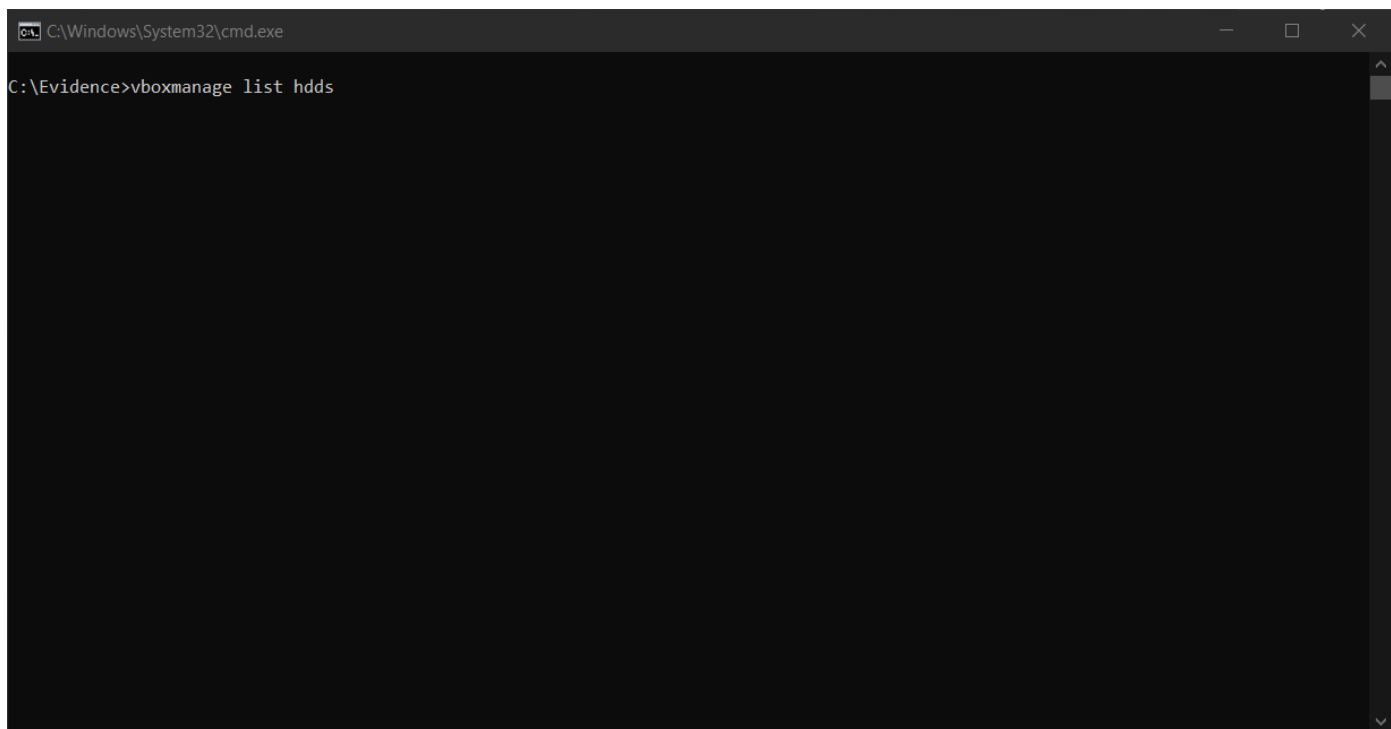
- Unpause VM.



- Shut down the VM.



- List hdds.



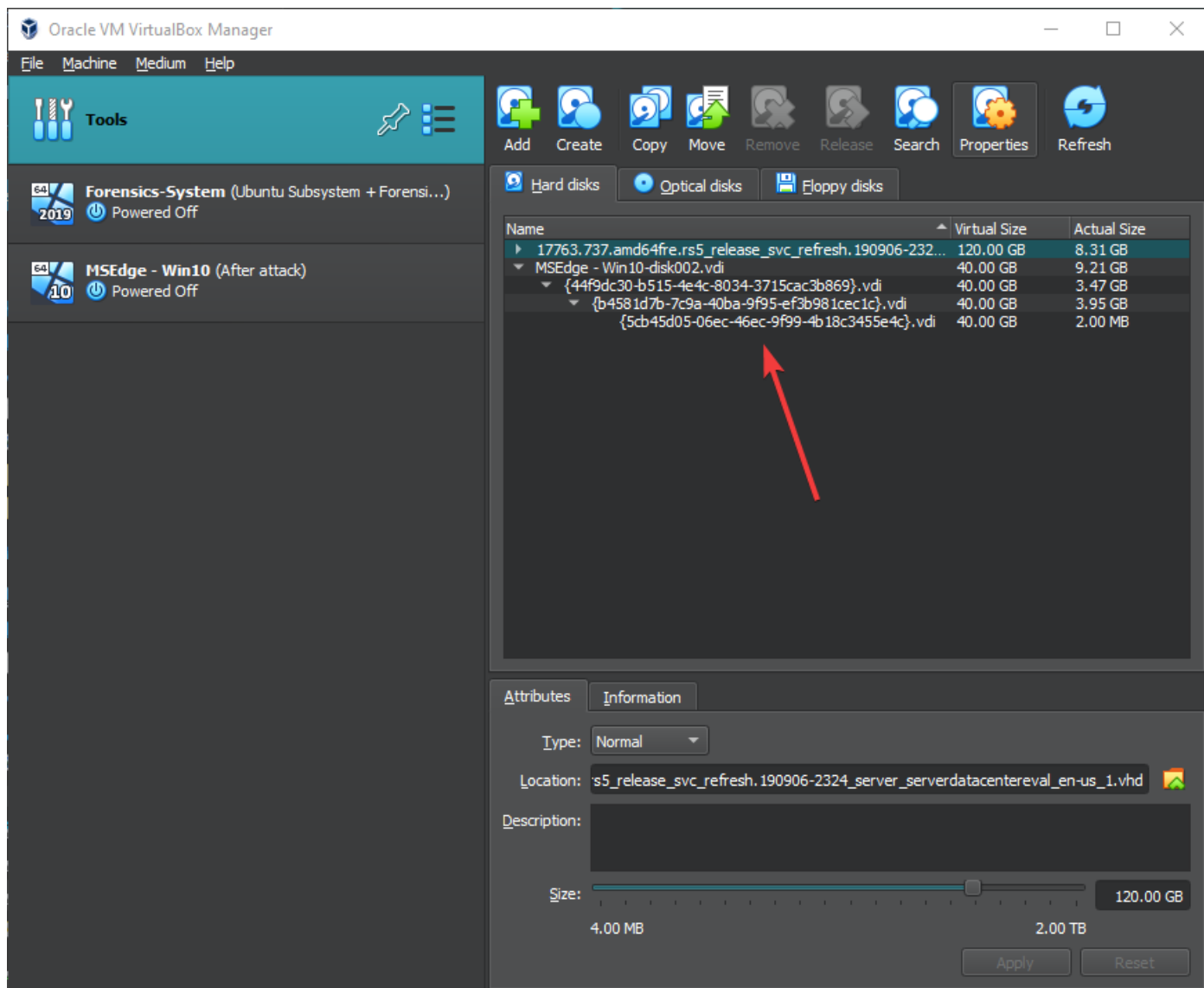
- Verify that the UUIDs are the same.

```
C:\Windows\System32\cmd.exe
Parent UUID: 7babf2c4-054c-4f42-b523-5ec068b6d04b
State: created
Type: normal (differencing)
Location: C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{44f9dc30-b515-4e4c-8034-3715cac3b869}.vdi
Storage format: vdi
Capacity: 40960 MBytes
Encryption: disabled

UUID: b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
Parent UUID: 44f9dc30-b515-4e4c-8034-3715cac3b869
State: created
Type: normal (differencing)
Location: C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{b4581d7b-7c9a-40ba-9f95-ef3b981cec1c}.vdi
Storage format: vdi
Capacity: 40960 MBytes
Encryption: disabled

UUID: 5cb45d05-06ec-46ec-9f99-4b18c3455e4c
Parent UUID: b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
State: created
Type: normal (differencing)
Location: C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{5cb45d05-06ec-46ec-9f99-4b18c3455e4c}.vdi
Storage format: vdi
Capacity: 40960 MBytes
Encryption: disabled

C:\Evidence>
```



- We will clone the disk with the following command, in a VHD (virtual hard disk) format.

```

C:\Windows\System32\cmd.exe
Parent UUID:    7babf2c4-054c-4f42-b523-5ec068b6d04b
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{44f9dc30-b515-4e4c-8034-3715cac3b869}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
Parent UUID:   44f9dc30-b515-4e4c-8034-3715cac3b869
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{b4581d7b-7c9a-40ba-9f95-ef3b981cec1c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          5cb45d05-06ec-46ec-9f99-4b18c3455e4c
Parent UUID:   b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{5cb45d05-06ec-46ec-9f99-4b18c3455e4c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

C:\Evidence>vboxmanage clonemedium disk 5cb45d05-06ec-46ec-9f99-4b18c3455e4c --format VHD win10-disk.vhd

```

```

C:\Windows\System32\cmd.exe
Parent UUID:    7babf2c4-054c-4f42-b523-5ec068b6d04b
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{44f9dc30-b515-4e4c-8034-3715cac3b869}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
Parent UUID:   44f9dc30-b515-4e4c-8034-3715cac3b869
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{b4581d7b-7c9a-40ba-9f95-ef3b981cec1c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          5cb45d05-06ec-46ec-9f99-4b18c3455e4c
Parent UUID:   b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{5cb45d05-06ec-46ec-9f99-4b18c3455e4c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled




C:\Evidence>vboxmanage clonemedium disk 5cb45d05-06ec-46ec-9f99-4b18c3455e4c --format VHD win10-disk.vhd
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'VHD'. UUID: 8987c97a-4e9d-4415-918c-a7d2eca1dfb1

C:\Evidence>

```



- You can see the size of the virtual hard disk.

Name	Date modified	Type	Size
 win10-disk.vhd	2/13/2023 7:59 PM	Virtual Hard Disk	14,009,774 ...
 win10-memory.raw	2/13/2023 7:53 PM	RAW File	4,463,807 KB
 win10-memory-hash.txt	2/13/2023 7:54 PM	TXT File	1 KB

- Make a hash (SHA1) of the disk file because that ensures the file is still the original , and has not been tampered with.

```
C:\Windows\System32\cmd.exe
Parent UUID:    7babf2c4-054c-4f42-b523-5ec068b6d04b
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{44f9dc30-b515-4e4c-8034-3715cac3b869}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
Parent UUID:   44f9dc30-b515-4e4c-8034-3715cac3b869
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{b4581d7b-7c9a-40ba-9f95-ef3b981cec1c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          5cb45d05-06ec-46ec-9f99-4b18c3455e4c
Parent UUID:   b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{5cb45d05-06ec-46ec-9f99-4b18c3455e4c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

C:\Evidence>vboxmanage clonemedium disk 5cb45d05-06ec-46ec-9f99-4b18c3455e4c --format VHD win10-disk.vhd
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'VHD'. UUID: 8987c97a-4e9d-4415-918c-a7d2eca1dfb1

C:\Evidence>certUtil -hashfile win10-disk.vhd > win10-disk-hash.txt
```

```
C:\Windows\System32\cmd.exe
Parent UUID:    7babf2c4-054c-4f42-b523-5ec068b6d04b
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{44f9dc30-b515-4e4c-8034-3715cac3b869}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
Parent UUID:   44f9dc30-b515-4e4c-8034-3715cac3b869
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{b4581d7b-7c9a-40ba-9f95-ef3b981cec1c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          5cb45d05-06ec-46ec-9f99-4b18c3455e4c
Parent UUID:   b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{5cb45d05-06ec-46ec-9f99-4b18c3455e4c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

C:\Evidence>vboxmanage clonemedium disk 5cb45d05-06ec-46ec-9f99-4b18c3455e4c --format VHD win10-disk.vhd
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'VHD'. UUID: 8987c97a-4e9d-4415-918c-a7d2eca1dfb1

C:\Evidence>certUtil -hashfile win10-disk.vhd > win10-disk-hash.txt

C:\Evidence>
```

```
C:\Windows\System32\cmd.exe
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

UUID:          5cb45d05-06ec-46ec-9f99-4b18c3455e4c
Parent UUID:   b4581d7b-7c9a-40ba-9f95-ef3b981cec1c
State:         created
Type:          normal (differencing)
Location:      C:\Machine Folders for Virtualbox\MSEdge - Win10\Snapshots\{5cb45d05-06ec-46ec-9f99-4b18c3455e4c}.vdi
Storage format: vdi
Capacity:      40960 MBytes
Encryption:    disabled

C:\Evidence>vboxmanage clonemedium disk 5cb45d05-06ec-46ec-9f99-4b18c3455e4c --format VHD win10-disk.vhd
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'VHD'. UUID: 8987c97a-4e9d-4415-918c-a7d2eca1dfb1

C:\Evidence>certUtil -hashfile win10-disk.vhd > win10-disk-hash.txt

C:\Evidence>type *.txt

win10-disk-hash.txt





SHA1 hash of win10-disk.vhd:
eddb1051b2d4054bae5fd2fe7d8c280cfa664396
CertUtil: -hashfile command completed successfully.

win10-memory-hash.txt

SHA1 hash of win10-memory.raw:
683f47a6461ab7a88c7d7655160c315b9691dd44
CertUtil: -hashfile command completed successfully.

C:\Evidence>
```

- Evidence folder:

Name	Date modified	Type	Size
 win10-disk.vhd	2/13/2023 7:59 PM	Virtual Hard Disk	14,009,774 ...
 win10-disk-hash.txt	2/13/2023 8:00 PM	TXT File	1 KB
 win10-memory.raw	2/13/2023 7:53 PM	RAW File	4,463,807 KB
 win10-memory-hash.txt	2/13/2023 7:54 PM	TXT File	1 KB