



## Windows Forensics and Incident Response



Anders Carlsson  
BTH



## dd.exe for Windows

- dd.exe for Windows
- • Isn't dd a UNIX tool?
- • Yes... originally
- • It was ported for use as a part of
- many packages that converted the
- most useful Unix Tools for use in
- Windows Based OS'es.



Anders Carlsson  
BTH



- Dd was originally written as a UNIX tool and distributed for free as a part of the GNU Open Source
- package. Most Unix systems have dd that functions on it.
- The good thing for Windows users is that it was also ported to a command line utility for use in
- Windows Based operating systems as well.
- The thing you need to know is the syntax behind the tool to enable it to work!
- 1 - 3



Anders Carlsson  
BTH



## dd.exe as a Backup Tool

- Our *GOAL*: Preserve the state of the evidence
- dd command is most effective
  - MD5 Sums
  - Integrity checker
  - Powerful options
  - Able to obtain Physical Memory as well
  - dd as a backup method in the following slides. But the most obvious features of dd



Anders Carlsson  
BTH



## But the most obvious features of dd are

1. It is free to use and download.
2. It can perform MD5 sums as a part of its normal functioning.
3. It has an ability to compare the MD5 sum from the data and the MD5 sum from the image and will tell you if they do not match.
4. It puts the power, creativity, and usability back into the hands of the investigator. In other words, it can do MANY different things for you.
5. The tool is also able to obtain physical memory as well.)



Anders Carlsson  
BTH



## dd.exe Command

- It is not a backup command.
- It is a low-level command.
- copies bits of information from one place to another
- dd does not have any knowledge of the "data structure" of the data it is copying.
- Think of it as just copying ones and zeroes and writing ones and zeros to another location.
- The dd command is not a backup command. Dd is a low level command designed for copying bits from one place to another.



Anders Carlsson  
BTH



## dd.exe Command

Can copy:

- Single file
- Part of a file
- Partition
- Logical and physical disks
- Physical memory
- Swap files or pagefiles
- Even copy data from stdin and stdout



Anders Carlsson  
BTH



- dd can also copy **physical memory** from **ram**, **image swap files** or **pagefiles**, and even copy data from standard in or move it to standard out.
- This is useful when you would like to "**pipe**" commands together, meaning that the output from one command is "piped" to another command that would manipulate the data in one form.



Anders Carlsson  
BTH



## Basic dd.exe Operation

dd if=device  
of=device  
bs=blocksize  
if= argument specifies the input file  
of= argument specifies the output file  
bs= argument specifies the block size



Anders Carlsson  
BTH



## basic arguments

if= argument specifies the input file  
(examples pagefile.sys, boot.ini, etc)  
of= argument specifies the output file  
(data1.img, pagefile.img, boot\_ini.img)  
bs= argument specifies the block size,  
or the amount of data that is to be  
transferred in one I/O



Anders Carlsson  
BTH



- Note: Changing block size does not affect how the data is physically written to a disk device.
- This option mainly matters when used with the option "count."
- The count and block size will be used together to figure out how far into a disk each record is.
- Say for example you dd a file with a **count** of **4** and a **block** size of **512**, you will effectively copy only 2048 bytes of that file or image.



Anders Carlsson  
BTH



## dd.exe Physical Drives

- Physical drive opened using syntax `\\PhysicalDriveX`  
"X" = drive number (0, 1, 2)  
\\ Represents the local machine.  
(Note the absence of a trailing backslash.)
- In the Unix world, most machines are referred to as `/dev/hda` (first ide drive). However, in the Windows world things are different! While I know that didn't shock you, you need to know the nomenclature for naming similar items in a Windows world.  
The first physical drive is referred to as `\\.\PhysicalDrive0` and subsequent drives would be identified as 1,2,3 etc.  
As you may have learned when looking for computers on your network neighborhood,



Anders Carlsson  
BTH



## dd.exe Logical Drives

- Physical volume or partition
- Opened using either the mount point
- `\\.\C:`
- `\\.\D:`
- Or unique volume name

```
\\?\Volume{cc5deda7-d558-11d5-9226-806d6172696f}
```



Anders Carlsson  
BTH



## The physical volume or partition on a hard drive

- `C:` is the common value for the systems main partition.
- In the Unix world, this would be equivalent to the `/dev/hda1`.



Anders Carlsson  
BTH



## dd.exe Translations

- Logical `\\.\C:` `/dev/hda1`
- Physical `\\.\PhysicalDrive0` `/dev/hda`



Anders Carlsson  
BTH



## Physical Drive Example

- The following syntax copies -NTFS from (if=) physical drive 0 to (of=) the file `image0.dat`
- ```
dd if=\\.\PhysicalDrive0 of=C:\image0.dat
```
- (Note this is all in one command line.)

The follow syntax copes the NTFS bootsector from the physical drive 0 to the file `bootsect.nt`.

```
dd if=\\.\PhysicalDrive0 of=C:\image0.dat
```



Anders Carlsson  
BTH



The following syntax will perform a bit wise copy of the volume mounted at E: to a file.

```
dd if=\\.\E: of=C:\images\E_drive.img
```



Anders Carlsson  
BTH



## Mapping a physical

- Mapping a physical address with different attributes (e.g. cached vs. non-cached vs. write-combined) can lead to processor corruption and unpredictable results.
- Windows NT and W2k do not check for this whereas XP does.



Anders Carlsson  
BTH



## Physical Memory (2)

- The following syntax will image Windows physical memory
- ( In one line )

```
dd if=\\.\PhysicalMemory  
of=c:\images\my_physical_memory.img  
conv=noerror
```



Anders Carlsson  
BTH



- The following syntax will image your physical memory and create a file where the memory contents are placed for later examination.
- One approach would be to simply record the offsets of the regions that cannot be read and place zeros as a "placeholder" at those offsets in the image file.

dd does this already for physical disks if "conv=noerror" is specified as an argument on the command line.



Anders Carlsson  
BTH



```
dd if=\\.\PhysicalMemory  
of=myfile.img conv=noerror".
```

```
dd if=\\.\PhysicalMemory  
of=c:\images\my_physical_memory.img  
conv=noerror
```



Anders Carlsson  
BTH



```
dd if=\\.\PhysicalMemory  
of=myfile.img conv=noerror".
```

- This will grab the system memory until you reach the end of file error. As a result, you will see a
- benign error reported when the starting offset of the read goes beyond the range of addressable
- physical memory, "The parameter is incorrect." This is equivalent to an end of file condition and is
- expected.



Anders Carlsson  
BTH



## MD5 Integrity Checks

- dd.exe needs an integrity checker
- not a normal function of dd.exe
- added to increase forensic feasibility of tool



Anders Carlsson  
BTH



## md5 checksum

- md5sum
- verifymd5
- md5out



Anders Carlsson  
BTH



MD5 is seen as a way to fingerprint files to ensure that the file you obtained is the same exact same one that was downloaded.

It produces a 128 bit key hash which will produce a irreversible fingerprint of that specific file.

The fingerprint could only be generated by running it on the specific file or data and cannot be duplicated unless you have an exact copy of the file or data.

It has naturally become a forensic staple in imaging, evidence collection, and file verification.



Anders Carlsson  
BTH



## MD5 Volume Imaging

The following syntax will --

- perform a bit wise copy of the volume mounted at E: to a file,
- calculate a md5 checksum - verify the resultant image against the

- Checksum
- The following syntax will perform a bit wise copy of the volume mounted at E: to a file, calculate a md5 checksum, and verify the resultant image against the checksum.

- Again, this could take several hours so make sure you start this and have the time to accomplish it. It is recommended that you have a room you can secure so you do not have to be physically present while the imaging is ongoing.

- Otherwise, leaving an unsecured room is breaking the chain of custody on the evidence you are attempting to seize.



Anders Carlsson  
BTH



## md5 syntax

One line

```
dd if=\\.\E: of=C:\images\E_drive.img
--md5sum
--verifymd5
--md5out=C:\images\E_drive.img.md5
```



Anders Carlsson  
BTH



## Out put to networked computer

- of=\\server\share\output.img



Anders Carlsson  
BTH