

RE: dd for windows and imaging a 40Gb drive

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-12/msg00246.html>

- *From:* Murda Mcloud <murdamcloud@xxxxxxxxxxx>
 - *Date:* Tue, 12 Dec 2006 14:51:17 +1000
-

Thanks to all for tips and suggestions—that worked fine. We now have a binary image which has been handed to legal along with the original. I've also noted everything that I've done and will give a copy of that to legal too.

Final questions—how do you get dd to save a log of the details that it coughs up at the end of a copy process? How does the block size get determined? And should it always be a multiple of the sector size?

-----Original Message-----

From: [listbounce@xxxxxxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxxxxxx) [<mailto:xxxxxxxxxxxxxxxxxxxx>] On Behalf Of Paul daSilva
Sent: Friday, December 08, 2006 10:30 AM
To: Murad Talukdar; [security-basics@xxxxxxxxxxxxxxxxxxxx](mailto:xxxxxxxxxxxxxxxxxxxx)
Subject: Re: dd for windows and imaging a 40Gb drive

Murad,

Imaging a disk to another disk: just be sure the target is empty -- dd copies all data block for block, including partition layout and format type. The end result will be a 100% drive image, meaning you could take that target drive and boot it on another machine, assuming all the hardware was exactly the same.

Imaging a disk to a file, the output will be a raw format file which could then be analyzed with forensics applications that accept an image file as input.

Imaging a partition to another partition, just be sure the target partition is equal or larger in size. Again, dd will write over the target partition, laying down a block by block copy of the source partition including partition type.

Imaging (copying) a file to another file, the output will be an exact copy of that file, and dd would expect to find a target path that can be written to (meaning an existing partition and directory). I don't believe it would care about the target partition format. For example dd.exe for Windows dumping to a Linux server using netcat, taking input from NTFS and copying that file on to an EXT3 partition.

RE: dd for windows and imaging a 40Gb drive

Please note that I have never used dd.exe for Windows, so my statements above relate to dd for Unix. Be careful, as dd.exe for Windows has slightly different syntax and path definitions.

Also, be careful! Improper use of dd can destroy/delete your data!

Murad Talukdar wrote:

Great stuff Paul—thanks for the link to the garner page. I had found the

dd

for windows and was trying to work out whether I could somehow load that into a livecd for similar purposes(even just for backing up).

One thing which I'm trying to work out is with regards to a pst file

which,

let's say for argument's sake, lives here

C:\documents and settings\username\local settings\application data\microsoft\outlook\outlook.pst

With the whole windows directory notation being expressed as unix-style notation issue(thanks for the clarification) would that mean that if just

a

file or folder needed to be copied, would it correspond to something

similar

to :

/dev/hda1/documents and settings/username/local settings/application data/microsoft/outlook/outlook.pst

I'm going to try it on a test machine and see if this is the case or not.

One other question too—does the empty target disk need to be formatted as

an

ntfs disk before the copy? Or would something that had been an ext2 disk

be

fine?

-----Original Message-----

RE: dd for windows and imaging a 40Gb drive

RE: dd for windows and imaging a 40Gb drive

From: Paul daSilva [mailto:pdasilva@xxxxxxx]
Sent: Friday, December 08, 2006 1:23 AM
To: Murad Talukdar; security-basics@xxxxxxxxxxxxxxxxxxxxxx
Subject: Re: dd for windows and imaging a 40Gb drive

Murad,

The option is up to you and your needs. Booting the Windows machine from a Linux LiveCD will give you the ability to snapshot the entire partition or hard drive as a point in time reference, with no 'interference' – meaning no changes to the filesystem as you capture its image.

You could try to copy the files you need while booted into Windows, copying the desired .pst file over the network. I'm not sure if this will work when the file is in use (opened under Outlook or whatever by that user), but you can give it a try. Also, there is a dd for Windows which may have slightly different capabilities than the original dd, like dumping data from a live file system? I'm not sure, but you can check it out -- they do use slightly different conventions with respect to drives and partitions. Here are some links:

<http://www.chrysocome.net/dd>
<http://users.erols.com/gmgarner/forensics/>

Lastly, yes, if you boot from a Linux Live CD, your disks and partitions will assume that naming convention:

/dev/hda primary hard drive
/dev/hdb secondary drive on the primary IDE
/dev/hdc first drive on secondary IDE
/dev/hdd secondary drive on secondary IDE

/dev/hda1 first partition on primary drive
and so on....

Cheers,
Paul

Murad Talukdar wrote:

Thanks Paul,
Now the source machine in question is a winxp box so I take it that

running

RE: dd for windows and imaging a 40Gb drive

dd and piping to nc would mean booting to a live cd(on source machine) in order to prevent any 'interference' with the data?

Now I'm assuming that when running a live cd (knoppix std or FIRE eg)

will

mean that the main partition should show up as /dev/had or similar even though it is a windows box. Is that right?

What I really need is a copy of this user's pst files for legal to check

for

'incriminating' (ie non-criminal) emails but I did suggest to them that taking an image of the drive first, for possible later use may be

advisable.

Now I'm not a forensic expert and I did say that normally this should be done by such but they have said that it really is just a preliminary investigation. <shrug>

-----Original Message-----

From: Paul daSilva [<mailto:pdasilva@xxxxxxxx>]

Sent: Thursday, December 07, 2006 8:47 AM

To: Murad Talukdar

Cc: security-basics@xxxxxxxxxxxxxxxxxxxxx

Subject: Re: dd for windows and imaging a 40Gb drive

Murad,

I can't answer how long the process will take, as far too many factors are involved.

However, to use dd over the network, you could consider piping its output to netcat.

On the Target system, where image will be dumped to, run:

```
nc -l -p 9000 | dd of=/path/image-file.dd (or of=/dev/hda)
```

On the Source system to be imaged, run:

```
dd if=/dev/hda | nc 192.168.1.120 9000
```

Be sure to edit the Target system output file of=, as it can be a file or you can dd to another disk or partition (clone).

Be sure to edit the Source system input file if= (right drive device and partition number), and use the right IP address and port number for the Target system). Googling "dd and netcat" will give you lots more information on this topic.

RE: dd for windows and imaging a 40Gb drive

Cheers,
Paul

Murad Talukdar wrote:

Hi all,
I need to estimate how long it would take to image a 40gb
drive with a
single partition on it using dd. (I guess this is more
dependant on

write

speeds and throughput than anything else)
Also, what would be the syntax of the output file be if I were
to image
across the network? Or can dd be used by using a crossover
cable and

mapping

drives first?
But, if I were to map a drive to the machine in question, does
that
'interfere' with the drive in any way?
I'm planning to use dd for windows—which I can get to work
fine for
files/folders on my local machine but am struggling over the
network

because

I'm not sure of the syntax.
No man dd on windows.

RE: dd for windows and imaging a 40Gb drive

RE: dd for windows and imaging a 40Gb drive

This list is sponsored by: ByteCrusher

Detect Malicious Web Content and Exploits in Real-Time.
Anti-Virus engines can't detect unknown or new threats.
LinkScanner can. Web surfing just became a whole lot safer.

http://www.explabs.com/staging/promotions/xern_lspro.asp?loc=sfmaildetect

This list is sponsored by: ByteCrusher

Detect Malicious Web Content and Exploits in Real-Time.
Anti-Virus engines can't detect unknown or new threats.
LinkScanner can. Web surfing just became a whole lot safer.

http://www.explabs.com/staging/promotions/xern_lspro.asp?loc=sfmaildetect

This list is sponsored by: ByteCrusher

Detect Malicious Web Content and Exploits in Real-Time.
Anti-Virus engines can't detect unknown or new threats.
LinkScanner can. Web surfing just became a whole lot safer.

http://www.explabs.com/staging/promotions/xern_lspro.asp?loc=sfmaildetect
