



FORENSIC SHELL FU

Bash, a hex editor, and dd– what more do you need?



Alexis Brignoni (He/Him) • 1st

Special Agent - Digital Forensics Examiner - Opinions are mine only & subj...

3w • 🌐

**AI, 3RD PARTY
TOOLS, PARSERS,
ANALYTICS, AUTOMATION**

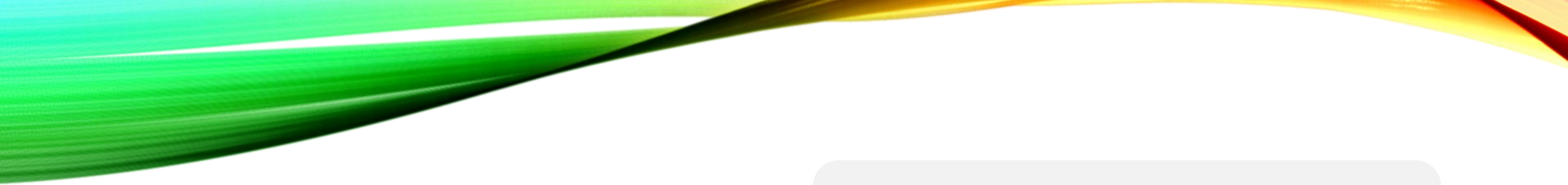
HEX EDITOR





Give me a bash command line to help me determine the "magic number" for a previously uncatalogued file

```
for file in *; do xxd $file | head -1; done
```



How can I translate hex-encoded characters back into ASCII using only the Linux command-line?

```
echo 7375646F00... | xxd -r -p | tr '\\0 ' '; echo
```

Starting with the byte offset to a string in an EXT file system image, how can I determine the containing that string using only standard Linux commands?

```
# strings -a -t d /dev/mapper/LabVM-root
```

```
...
```

```
6272992038 MA-L,001A54,Hip Shing Electronics,"Unit 1/2/3, 20/F, New Treasure Center HK"
```

```
...
```

```
# echo $((6272992038 / 4096))
```

```
1531492
```

```
# debugfs -R 'icheck 1531492' /dev/mapper/LabVM-root
```

```
Block      Inode number
```

```
1531492 1706273
```

```
# find / -xdev -inum 1706273
```

```
/usr/share/ieee-data/oui.csv
```

Sorry, did I say EXT? I meant XFS!

```
# strings -a -t d centos-root.raw
...
9010062352                                Unit 1/2/3, 20/F, New Treasure Center
...
# echo $((9010062352 / 512))
17597778
# xfs_db -r -c 'convert daddr 17597778 fsblock' centos-root.raw
0x3390aa (3379370)
# xfs_db -r -c 'blockget -ns' -c 'fsblock 3379370' -c 'blockuse -n' centos-root.raw
block 3379370 (3/233642) type data inode 25629955 usr/share/hwdata/oui.txt
```

Oh sure, Mr Smarty-AI! But xfs_db still doesn't let me dump raw block info. How are you going to deal with that?!

```
# xfs_db -r -c 'convert daddr 17597778 agno' centos-root.raw
0x3 (3)
# xfs_db -r -c 'convert daddr 17597778 agblock' centos-root.raw
0x390aa (233642)
# xfs_db -r -c 'sb 0' -c 'print agblocks' centos-root.raw
agblocks = 655360
# dd if=centos-root.raw bs=4096 skip=$((3*655360 + 233642)) count=1
```

...

Unit 1/2/3, 20/F, New Treasure Center

...

Stop! This is all too dangerous!
Where will it end?!

<https://github.com/halpomeranz/dfis/blob/master/xfs-extents.sh>

```
46 xfs_db -r -c "inode $Inode" -c 'type text' -c print $Device | tail -n +12 | cut -c 7-55 | tr -d ' ' |
47     while read line; do
48         [[ $line == "00000000000000000000000000000000" ]] && break          # no more extents
49
50         # Dump each extent as binary, then use cut to extract each field of the extent
51         bits=$(echo $line | xxd -r -p | xxd -b -c 16 | cut -c 10-154 | tr -d ' ')
52         logicaloffset=$(echo $((2#$(echo $bits | cut -c2-55))))
53         startblk=$(echo $((2#$(echo $bits | cut -c56-107))))
54         numblks=$(echo $((2#$(echo $bits | cut -c108-128))))
55
56         # Convert fsblock addresses to agno and agblock for "dd" command
57         agno=$(xfs_db -r -c "convert fsblock $startblk agno" $Device | cut -f2 -d' ' | tr -dc 0-9)
58         agblock=$(xfs_db -r -c "convert fsblock $startblk agblock" $Device | cut -f2 -d' ' | tr -dc 0-9)
59
60         [[ $Debug -gt 0 ]] && echo "logical offset: $logicaloffset / start block: $startblk (agno=$agno, agblock=$agblock) / num blocks: $numblks"
61
62         # Output working "dd" command to extract the raw blocks for each extent
63         echo "(offset $logicaloffset) -- dd if=$Device bs=$blocksize skip=$(( $agno * $agblocks + $agblock )) count=$numblks"
64     done
```

Shut up and take my money!



*Linux Command Line for Analysts & Operators
On-Demand and LIVE at Wild West Hackin Fest, Oct 8-9*



*Zero to Linux ("Pay What You Can" Virtual Event)
September 5, 11:00 – 16:00 US/Eastern (UTC-4)*

hrpommeranz@gmail.com
@hal_pommeranz@infosec.exchange
<https://RighteousIT.com/resources/>