

# Rahul Prithu

## CSCI395 – Digital Forensics

### LAB 2

#### Answer: 1A

dd: Convert and copy file

Usage Example: **\$ dd if=/dev/zero of=my\_fat\_file bs=1k count=4096**

if=FILEIN	:	Uses FILEIN instead of stdin.
of=FILEOUT	:	Write to FILEOUT instead of stdout.
bs=BYTES	:	Read and write BYTES number of bytes, at a time.
count=BLOCKS	:	Copy BLOCKS input blocks.

dd command converts and copies a file. In this example, the command creates a new file “my\_fat\_file” of 4MB size, and populates it with zeros (null characters).

Step 1:

```
bluephoenixra:lab2$dd if=/dev/zero of=my_fat_file bs=1k count=4096
4096+0 records in
4096+0 records out
4194304 bytes (4.2 MB) copied, 0.0221766 s, 189 MB/s
```

Step 2:

```
root:lab2#losetup /dev/loop0 my_fat_file
losetup: /dev/loop0: device is busy
root:lab2#losetup /dev/loop1 my_fat_file
root:lab2#
```

Step 3:

```
root:lab2#mkfs -t vfat /dev/loop1
mkfs.vfat 3.0.12 (29 Oct 2011)
Loop device does not match a floppy size, using default hd params
root:lab2#
```

Step 4:

```
root:lab2#mkfs -t vfat /dev/loop1
mkfs.vfat 3.0.12 (29 Oct 2011)
Loop device does not match a floppy size, using default hd params
root:lab2#pwd
/home/bluephoenixra/lab2
root:lab2#cd /mnt
root:mnt#mkdir my_fat_disk
root:mnt#mount /dev/loop1 my_fat_disk
```

**Q 1B:** What command can you use to check if your device has been properly mounted?

**Answer 1B:** "mount" command can be used to list all mounted devices.

```
bluephoenixra@bluephoenixra-VirtualBox:~$ mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
gvfs-fuse-daemon on /home/bluephoenixra/.gvfs type fuse.gvfs-fuse-daemon (rw,nosuid,nodev,user=bluephoenixra)
/dev/loop1 on /mnt/my_fat_disk type vfat (rw)
```

Step 5:

cp command:

```
root:lab2#cp my_fat_file my_fat_file00
root:lab2#ls
my_fat_file  my_fat_file00
```

mount:

```
root:lab2#cd /mnt/my_fat_disk
root:my_fat_disk#ls
root:my_fat_disk#echo 'This is a test line' > lab2.txt
root:my_fat_disk#ls
lab2.txt
root:my_fat_disk#cd ..
root:mnt#cd /home/bluephoenixra/lab2
root:lab2#ls -l
total 8192
-rw-rw-r-- 1 bluephoenixra bluephoenixra 4194304 Sep 29 19:57 my_fat_file
-rw-r--r-- 1 root          root          4194304 Sep 29 19:48 my_fat_file00
```

umount:

```
root:lab2#umount /mnt/my_fat_disk
root:lab2#losetup -d /dev/loop0
root:lab2#losetup -d /dev/loop1
```

diff:

```
root:lab2#diff my_fat_file my_fat_file00
Binary files my_fat_file and my_fat_file00 differ
```

my\_fat\_file00: Contains the empty file system.  
my\_fat\_file01: Contains a file with a line of text.

my\_fat\_file01: Contains a file with a line of text.

My\_fat\_file00 with my\_fat\_file01

In FAT12 system, 12 bits are used for each entry per cluster. Since 12bits is not an integral number of bytes, two FAT12 entries are stored into three bytes.

When a file is created with size less than a cluster, the beginning cluster is stored in the FAT followed by end of file indicator.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000001b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001f0:	0000	0000	0000	0000	0000	0000	0000	55aa	.....U.
00000200:	f8ff	ff00	0000	0000	0000	0000	0000	0000	.....
00000210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
<hr/>									
--::--	my_fat_file00			1% L33		(Hexl)		<hr/>	
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000001b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001f0:	0000	0000	0000	0000	0000	0000	0000	55aa	.....U.
00000200:	f8ff	ff00	f0ff	0000	0000	0000	0000	0000	.....
00000210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
<hr/>									
--::--	my_fat_file01			1% L33		(Hexl)		<hr/>	

### Difference 2:

The system maintains a second copy of FAT.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00000db0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000dc0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000dd0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000de0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000df0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e00:	f8ff	ff00	0000	0000	0000	0000	0000	0000	.....
00000e10:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e20:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e30:	0000	0000	0000	0000	0000	0000	0000	0000	.....
<hr/>									
--::-- my_fat_file00      1% L225      (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00000db0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000dc0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000dd0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000de0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000df0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e00:	f8ff	ff00	f0ff	0000	0000	0000	0000	0000	.....
00000e10:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e20:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e30:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000e40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
<hr/>									
--::-- my_fat_file01      1% L225      (Hexl)-----									

### Difference 3:

This is the directory entry. When a file is created, the first character “**A**” contains important attributes about the file. The next few bytes contain the long name subcomponent. The characters are separated with null characters between each other. This is followed by the short file name.

In FAT, each file name is stored in UPPERCASE. The dot separator is skipped. Thus the dot is implied between the extension and the file name.

The system stores date in 7/4/5 bits format. (For year: since 1980, Month: 1-12, Day 1-31)

In this exercise the modification date, 29-September-2013, is stored as: 0x43 0x3D, at 24-25<sup>th</sup> byte of the directory entry.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a10:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a20:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a30:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
--:--- my_fat_file00      1% L417      (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	002e	000f	00f4	7400	A1.a.b.2.....t.
00001a10:	7800	7400	0000	ffff	ffff	0000	ffff	ffff	x.t.....
00001a20:	4c41	4232	2020	2020	5458	5420	0064	169f	LAB2      TXT .d..
00001a30:	3d43	3d43	0000	169f	3d43	0300	1400	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
--:--- my_fat_file01      1% L417      (Hexl)-----									

#### Difference 4:

This is the data area. In the second file (*my\_fat\_file01*), the contents of the ASCII file appears in this area.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000061c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006200:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
: -=:--- my_fat_file00 1% L1569 (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000061b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006200:	5468	6973	2069	7320	6120	7465	7374	206c	This is a test l
00006210:	696e	650a	0000	0000	0000	0000	0000	0000	ine.....
00006220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
: -=:--- my_fat_file01 1% L1569 (Hexl)-----									

## 1D: Contents of the File

The content of *my\_fat\_file* viewed in hexedit (screenshot attached below) and also in emacs (Difference 4 of 1-C, from above)

000019DC	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
000019F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	41 6C 00 61 .....Al.a
00001A04	00 62 00 32	00 2E 00 0F	00 F4 74 00	78 00 74 00	00 00 FF FF .b.2.....t.x.t....
00001A18	FF FF 00 00	FF FF FF FF	4C 41 42 32	20 20 20 20	54 58 54 20 .....LAB2 TXT
00001A2C	00 64 16 9F	3D 43 3D 43	00 00 16 9F	3D 43 03 00	14 00 00 00 .d..=C=C....=C.....
00001A40	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
00001A54	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
00001A68	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
00001A7C	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
00001A90	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
--- my_fat_file --0x1838/0x400000-----					
000061E4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
000061F8	00 00 00 00	00 00 00 00	54 68 69 73	20 69 73 20	61 20 74 65 .....This is a te
0000620C	73 74 20 6C	69 6E 65 0A	00 00 00 00	00 00 00 00	00 00 00 00 st line.....
00006220	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
00006234	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00 .....
--- my_fat_file --0x5FDC/0x400000-----					

### 1-E: Modify File To Be Larger Than One Cluster:

my\_fat\_file01: Contains file with only one line.

my\_fat\_file02: Contains file larger than one cluster.

Text file larger than one cluster:

[illegible]

### Difference 1:

Directory Information. File modification date and file size information are different.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	002e	000f	00f4	7400	Al.a.b.2.....t.
00001a10:	7800	7400	0000	ffff	ffff	0000	ffff	ffff	x.t.....
00001a20:	4c41	4232	2020	2020	5458	5420	0064	169f	LAB2      TXT    .d..
00001a30:	3d43	3d43	0000	169f	3d43	0300	1400	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a60:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a70:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a80:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a90:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001aa0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001ab0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001ac0:	0000	0000	0000	0000	0000	0000	0000	0000	.....

:-:--- my\_fat\_file01      1% L420      (Hexl)-----

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	002e	000f	00f4	7400	Al.a.b.2.....t.
00001a10:	7800	7400	0000	ffff	ffff	0000	ffff	ffff	x.t.....
00001a20:	4c41	4232	2020	2020	5458	5420	0000	c5a3	LAB2      TXT    ....
00001a30:	3d43	3d43	0000	c5a3	3d43	0300	ae02	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a60:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a70:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a80:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a90:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001aa0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001ab0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001ac0:	0000	0000	0000	0000	0000	0000	0000	0000	.....

:-:--- my\_fat\_file02      1% L415      (Hexl)-----



### Difference 2:

**Data Segment.** The data in second file is spread over more than one cluster.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000061f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006200:	5468	6973	2069	7320	6120	7465	7374	206c	This is a test l
00006210:	696e	650a	0000	0000	0000	0000	0000	0000	ine.....
00006220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006250:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006260:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006270:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006280:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006290:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000062a0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000062b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000062c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000062d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
: --:--- my_fat_file01      1% L1577    (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00006190:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061a0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000061f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006200:	5468	6973	2069	7320	6120	7465	7374	206c	This is a test l
00006210:	696e	650a	5468	6973	2069	7320	616e	6f74	ine.This is anot
00006220:	6865	7220	6c69	6e65	206f	6620	7465	7874	her line of text
00006230:	2077	7269	7474	656e	2074	6f20	696e	6372	written to incr
00006240:	6561	7365	2074	6865	2063	6c75	7374	6572	ease the cluster
00006250:	2073	697a	6520	6279	206f	6e65	2e0a	5468	size by one..Th
00006260:	6973	2069	7320	616e	6f74	6865	7220	6c69	is is another li
00006270:	6e65	206f	6620	7465	7874	2077	7269	7474	ne of text writt
: --:--- my_fat_file02      1% L1569    (Hexl)-----									



End of File:

[illegible]

## 1-F: Deleting A File

my\_fat\_file02: Contains a text file.

my\_fat\_file03: The text file (in *my\_fat\_file02*) is deleted. In effect, the file system is empty.

```
root@mnt#mount /dev/loop1 my_fat_disk
root@mnt#cd my_fat_disk
root@my_fat_disk#ls -l
total 2
-rwxr-xr-x 1 root root 686 Sep 29 20:30 lab2.txt
root@my_fat_disk#rm lab2.txt
root@my_fat_disk#ls -l
total 0
root@my_fat_disk#
```

### Difference 1:

When the file is deleted, the cluster is free'd. In FAT (in `my_fat_file03`), after deletion, the cluster entry appears as 0x0000

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00000180:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000190:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001a0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001f0:	0000	0000	0000	0000	0000	0000	0000	55aa	.....U.
00000200:	f8ff	ff00	0000	0000	0000	0000	0000	0000	.....
00000210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
-=:---	my_fat_file03			1% L33	(Hexl)	-----			
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00000180:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000190:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001a0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001e0:	0000	0000	0000	0000	0000	0000	0000	0000	. .....
000001f0:	0000	0000	0000	0000	0000	0000	0000	55aa	.....U.
00000200:	f8ff	ff00	f0ff	0000	0000	0000	0000	0000	.....
00000210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
-=:---	my fat file02			1% L31	(Hexl)	-----			

Second copy of FAT is maintained by the system.

### Difference 3:

When a file is deleted, the first character of the directory entry is replaced with 0xE5

[illegible]

#### Difference 4:

When a file is deleted, the system also replaces the first character of the short name with 0xE5.

As the long name is not deleted, it is possible to replace the first character with the first character in long file name. This way, the deleted file may be restored.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	e56c	0061	0062	0032	002e	000f	00f4	7400	.l.a.b.2.....t.
00001a10:	7800	7400	0000	ffff	ffff	0000	ffff	ffff	x.t.....
00001a20:	e541	4232	2020	2020	5458	5420	0000	c5a3	.AB2 TXT ....
00001a30:	3d43	3d43	0000	c5a3	3d43	0300	ae02	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a60:	0000	0000	0000	0000	0000	0000	0000	0000	.....
----- my_fat_file03 1% L419 (Hexl) -----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	002e	000f	00f4	7400	A.l.a.b.2.....t.
00001a10:	7800	7400	0000	ffff	ffff	0000	ffff	ffff	x.t.....
00001a20:	4c41	4232	2020	2020	5458	5420	0000	c5a3	LAB2 TXT ....
00001a30:	3d43	3d43	0000	c5a3	3d43	0300	ae02	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a60:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a70:	0000	0000	0000	0000	0000	0000	0000	0000	.....
----- my_fat_file02 1% L419 (Hexl) -----									

**NOTE:** Data area not changed, data remains there. That is why ediff doesn't find any differences in the data area.

## 1-G: Create Directory

my\_fat\_file03: The text file (in *my\_fat\_file02*) is deleted in previous step (F). In effect, the file system is empty.

my\_fat\_file04: A subdirectory (*lab2dir*) is created in the file system.

```
root:mnt#mount /dev/loop1 my_fat_disk
root:mnt#cd my_fat_disk
root:my_fat_disk#mkdir lab2dir
root:my_fat_disk#cd lab2dir
root:lab2dir#ls -l
total 0
root:lab2dir#cd ..
root:my_fat_disk# cd ..
root:mnt#umount my_fat_disk
root:mnt#losetup -d /dev/loop1
root:mnt#cd /home/bluephoenixra/lab2
root:lab2#cp my_fat_file my_fat_file04
root:lab2#ls -l
total 24576
-rw-rw-r-- 1 bluephoenixra bluephoenixra 4194304 Sep 29 20:57 my_fat_file
-rw-r--r-- 1 root root 4194304 Sep 29 19:48 my_fat_file00
-rw-r--r-- 1 root root 4194304 Sep 29 20:02 my_fat_file01
-rw-r--r-- 1 root root 4194304 Sep 29 20:33 my_fat_file02
-rw-r--r-- 1 root root 4194304 Sep 29 20:46 my_fat_file03
-rw-r--r-- 1 root root 4194304 Sep 29 20:58 my_fat_file04
root:lab2#
```

### Difference 1:

When a subdirectory is created, the FAT stores the cluster address.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000001b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001f0:	0000	0000	0000	0000	0000	0000	0000	55aa	.....U.
00000200:	f8ff	ff00	f0ff	0000	0000	0000	0000	0000	.....
00000210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
--:-- my_fat_file04 1% L33 (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000001b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000001f0:	0000	0000	0000	0000	0000	0000	0000	55aa	.....U.
00000200:	f8ff	ff00	0000	0000	0000	0000	0000	0000	.....
00000210:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000220:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000230:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00000240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
--:-- my_fat_file03 1% L33 (Hexl)-----									



System maintained a copy of the FAT.

### Difference 3:

The old directory entry (lab1.txt), which was marked free after deletion of file, is overwritten by the new entry (lab2dir).

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	0064	000f	0014	6900	Al.a.b.2.d....i.
00001a10:	7200	0000	ffff	ffff	ffff	0000	ffff	ffff	r.....
00001a20:	4c41	4232	4449	5220	2020	2010	0000	16a7	LAB2DIR ....
00001a30:	3d43	3d43	0000	16a7	3d43	0300	0000	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
--:-- my_fat_file04 1% L417 (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	e56c	0061	0062	0032	002e	000f	00f4	7400	.l.a.b.2.....t.
00001a10:	7800	7400	0000	ffff	ffff	0000	ffff	ffff	x.t.....
00001a20:	e541	4232	2020	2020	5458	5420	0000	c5a3	.AB2 TXT ...
00001a30:	3d43	3d43	0000	c5a3	3d43	0300	ae02	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
--:-- my_fat_file03 1% L417 (Hexl)-----									

#### Difference 4:

My\_fat\_file04 created the subdirectory at the beginning of data area. Old data in this cluster is overwritten.

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00006200:	2e20	2020	2020	2020	2020	2010	0000	16a7	. . . . .
00006210:	3d43	3d43	0000	16a7	3d43	0300	0000	0000	=C=C....=C.....
00006220:	2e2e	2020	2020	2020	2020	2010	0000	16a7	.. . . .
00006230:	3d43	3d43	0000	16a7	3d43	0000	0000	0000	=C=C....=C.....
00006240:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006250:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006260:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006270:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006280:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00006290:	0000	0000	0000	0000	0000	0000	0000	0000	.....
-=:--- my_fat_file04 1% L1569 (Hexl) -----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
00006200:	5468	6973	2069	7320	6120	7465	7374	206c	This is a test l
00006210:	696e	650a	5468	6973	2069	7320	616e	6f74	ine.This is anot
00006220:	6865	7220	6c69	6e65	206f	6620	7465	7874	her line of text
00006230:	2077	7269	7474	656e	2074	6f20	696e	6372	written to incr
00006240:	6561	7365	2074	6865	2063	6c75	7374	6572	ease the cluster
00006250:	2073	697a	6520	6279	206f	6e65	2e0a	5468	size by one..Th
00006260:	6973	2069	7320	616e	6f74	6865	7220	6c69	is is another li
00006270:	6e65	206f	6620	7465	7874	2077	7269	7474	ne of text writt
00006280:	656e	2074	6f20	696e	6372	6561	7365	2074	en to increase t
00006290:	6865	2063	6c75	7374	6572	2073	697a	6520	he cluster size
-=:--- my_fat_file03 1% L1569 (Hexl) -----									

## 1-H: Creating A File Inside The Directory:

my\_fat\_file04: A subdirectory (*lab2dir*) is created in the file system.

my\_fat\_file05: A new file (*lab2h.txt*) is created inside the subdirectory.

```
root:my_fat_disk#cd lab2dir
root:lab2dir#echo 'This is a new file!' > lab2h.txt
root:lab2dir#ls -l
total 2
-rwxr-xr-x 1 root root 20 Sep 29 21:05 lab2h.txt
root:lab2dir#cd ..
root:my_fat_disk#cd ..
root:mnt#umount my_fat_disk
root:mnt#losetup -d /dev/loop1
root:mnt#cd /home/bluephoenixra/lab2
root:lab2#cp my_fat_file my_fat_file05
root:lab2#ls -l
total 28672
-rw-rw-r-- 1 bluephoenixra bluephoenixra 4194304 Sep 29 21:05 my_fat_file
-rw-r--r-- 1 root root 4194304 Sep 29 19:48 my_fat_file00
-rw-r--r-- 1 root root 4194304 Sep 29 20:02 my_fat_file01
-rw-r--r-- 1 root root 4194304 Sep 29 20:33 my_fat_file02
-rw-r--r-- 1 root root 4194304 Sep 29 20:46 my_fat_file03
-rw-r--r-- 1 root root 4194304 Sep 29 20:58 my_fat_file04
-rw-r--r-- 1 root root 4194304 Sep 29 21:06 my_fat_file05
```

#### Difference 1:

A new cluster is allocated for the text file. The cluster address is stored in the FAT file.



```

87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
000001b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa .....U.
00000200: f8ff ff00 f0ff ff0f 0000 0000 0000 0000 .....
00000210: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000220: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-=:--- my_fat_file05 1% L33 (Hexl)-----
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
000001b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa .....U.
00000200: f8ff ff00 f0ff 0000 0000 0000 0000 0000 .....
00000210: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000220: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000230: 0000 0000 0000 0000 0000 0000 0000 0000 .....
-=:--- my_fat_file04 1% L33 (Hexl)-----

```

The FAT files are copied by the system.

### Difference 3:

87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	0064	000f	0014	6900	Al.a.b.2.d....i.
00001a10:	7200	0000	ffff	ffff	ffff	0000	ffff	ffff	r.....
00001a20:	4c41	4232	4449	5220	2020	2010	0064	aea8	LAB2DIR ..d..
00001a30:	3d43	3d43	0000	aea8	3d43	0300	0000	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
-=:--- my_fat_file05 1% L419 (Hexl)-----									
87654321	0011	2233	4455	6677	8899	aabb	ccdd	eeff	0123456789abcdef
000019e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
000019f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a00:	416c	0061	0062	0032	0064	000f	0014	6900	Al.a.b.2.d....i.
00001a10:	7200	0000	ffff	ffff	ffff	0000	ffff	ffff	r.....
00001a20:	4c41	4232	4449	5220	2020	2010	0000	16a7	LAB2DIR .....
00001a30:	3d43	3d43	0000	16a7	3d43	0300	0000	0000	=C=C....=C.....
00001a40:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a50:	0000	0000	0000	0000	0000	0000	0000	0000	.....
00001a60:	0000	0000	0000	0000	0000	0000	0000	0000	.....
-=:--- my_fat_file04 1% L419 (Hexl)-----									

#### Difference 4:

This is the subdirectory entry. The entry refers to the text file created inside. The subdirectory is placed in the same cluster where the text file was created earlier. Every subdirectory has two system entries "." and ".." which are followed by the directory entry for the new file.

```
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
00006200: 2e20 2020 2020 2020 2020 2010 0000 16a7 .
00006210: 3d43 3d43 0000 16a7 3d43 0300 0000 0000 =C=C....=C.....
00006220: 2e2e 2020 2020 2020 2020 2010 0000 16a7 ..
00006230: 3d43 3d43 0000 16a7 3d43 0000 0000 0000 =C=C....=C.....
00006240: 416c 0061 0062 0032 0068 000f 0075 2e00 Al.a.b.2.h...u..
00006250: 7400 7800 7400 0000 ffff 0000 ffff ffff t.x.t.....
00006260: 4c41 4232 4820 2020 5458 5420 0064 aea8 LAB2H TXT .d..
00006270: 3d43 3d43 0000 aea8 3d43 0400 1400 0000 =C=C....=C.....
00006280: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006290: 0000 0000 0000 0000 0000 0000 0000 0000 .....
: -=:--- my_fat_file05 1% L1573 (Hexl)-----
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
000061c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000061d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000061e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000061f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006200: 2e20 2020 2020 2020 2020 2010 0000 16a7 .
00006210: 3d43 3d43 0000 16a7 3d43 0300 0000 0000 =C=C....=C.....
00006220: 2e2e 2020 2020 2020 2020 2010 0000 16a7 ..
00006230: 3d43 3d43 0000 16a7 3d43 0000 0000 0000 =C=C....=C.....
00006240: 0000 0000 0000 0000 0000 0000 0000 0000 .....
: -=:--- my_fat_file04 1% L1573 (Hexl)-----
```

#### Difference 5:

This is the data area. The data is now stored in a different location than the data location in 1C.

```
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
000069b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a00: 5468 6973 2069 7320 6120 6e65 7720 6669 This is a new fi
00006a10: 6c65 210a 0000 0000 0000 0000 0000 0000 le!.....
00006a20: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a30: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a40: 0000 0000 0000 0000 0000 0000 0000 0000 .....
: -=:--- my_fat_file05 1% L1697 (Hexl)-----
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
000069c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000069f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a00: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a10: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a20: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a30: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00006a40: 0000 0000 0000 0000 0000 0000 0000 0000 .....
: -=:--- my_fat_file04 1% L1697 (Hexl)-----
```

## EXERCISE 2: NTFS File System and FAT Comparison

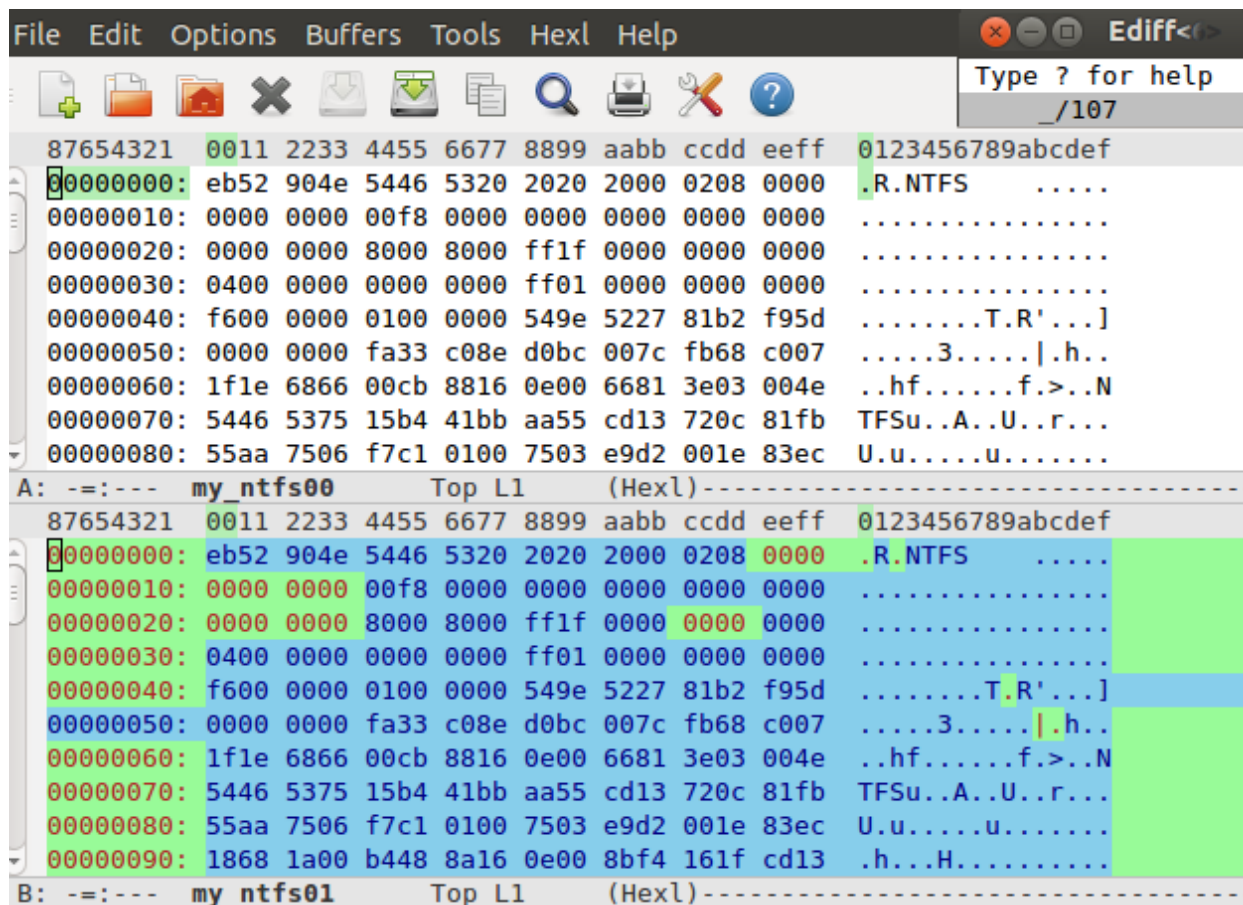
### Difference 1:

my\_ntfs00: Empty NTFS File System.

my\_ntfs01: NTFS File System, with one file containing one line of text.

There are 107 differences reported in Emacs Ediff.

Although a single line text file is added, NTFS system adds additional attributes to the file. NTFS allows access protection and ability to recover from corruptions, among many other features. These features add additional differences.



The screenshot shows the Emacs Ediff window comparing two NTFS file systems. The top panel (A) shows my\_ntfs00, which is empty. The bottom panel (B) shows my\_ntfs01, which contains a file with text. The differences are highlighted in green and blue. The window title is 'Ediff<>' and the status bar shows 'Type ? for help' and '107'.

Address	my_ntfs00 (Hex)	my_ntfs01 (Hex)	my_ntfs01 (ASCII)
87654321	0011 2233 4455 6677 8899 aabb ccdd eeff	0123456789abcdef	
00000000	eb52 904e 5446 5320 2020 2000 0208 0000	.R.NTFS	.....
00000010	0000 0000 00f8 0000 0000 0000 0000 0000	.....	
00000020	0000 0000 8000 8000 ff1f 0000 0000 0000	.....	
00000030	0400 0000 0000 0000 ff01 0000 0000 0000	.....	
00000040	f600 0000 0100 0000 549e 5227 81b2 f95d	.....T.R'...]	
00000050	0000 0000 fa33 c08e d0bc 007c fb68 c007	.....3..... .h..	
00000060	1f1e 6866 00cb 8816 0e00 6681 3e03 004e	..hf.....f.>..N	
00000070	5446 5375 15b4 41bb aa55 cd13 720c 81fb	TFSu..A..U..r...	
00000080	55aa 7506 f7c1 0100 7503 e9d2 001e 83ec	U.u.....u.....	
00000090	1868 1a00 b448 8a16 0e00 8bf4 161f cd13	.h...H.....	

## Difference 2:

my\_ntfs01: NTFS File System, with one file containing one line of text.

my\_fat\_file01: FAT File System, contains one line text file.

Total of 183 differences using Emacs Ediff.

Although both systems contained only one text file each of single line of data, an NTFS system is much more complex than a FAT system. The differences are attributable to various features like security, data streaming, and etc.

```
File Edit Options Buffers Tools Hexl Help
Type ? for help
1/183

87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
00000000: eb52 904e 5446 5320 2020 2000 0208 0000 .R.NTFS .....
00000010: 0000 0000 00f8 0000 0000 0000 0000 0000 .....
00000020: 0000 0000 8000 8000 ff1f 0000 0000 0000 .....
00000030: 0400 0000 0000 0000 ff01 0000 0000 0000 .....
00000040: f600 0000 0100 0000 549e 5227 81b2 f95d .....T.R'...
00000050: 0000 0000 fa33 c08e d0bc 007c fb68 c007 .....3.....|.h..
00000060: 1f1e 6866 00cb 8816 0e00 6681 3e03 004e ..hf.....f.>..N
00000070: 5446 5375 15b4 41bb aa55 cd13 720c 81fb TFSu..A..U..r...
00000080: 55aa 7506 f7c1 0100 7503 e9d2 001e 83ec U.u.....u.....

A: ==:--- my_ntfs01 Top L1 (Hexl)-----
87654321 0011 2233 4455 6677 8899 aabb ccdd eeff 0123456789abcdef
00000000: eb3c 906d 6b64 6f73 6673 0000 0204 0100 .<.mkdosfs.....
00000010: 0200 0200 20f8 0600 2000 4000 0000 0000 .... ..@.....
00000020: 0000 0000 0000 29a7 5bf2 9920 2020 2020 .....).[...
00000030: 2020 2020 2020 4641 5431 3220 2020 0e1f ..... FAT12 ..
00000040: be5b 7cac 22c0 740b 56b4 0ebb 0700 cd10 .[|. ".t.V.....
00000050: 5eeb f032 e4cd 16cd 19eb fe54 6869 7320 ^..2.....This
00000060: 6973 206e 6f74 2061 2062 6f6f 7461 626c is not a bootabl
00000070: 6520 6469 736b 2e20 2050 6c65 6173 6520 e disk. Please
00000080: 696e 7365 7274 2061 2062 6f6f 7461 626c insert a bootabl
00000090: 6520 666c 6f70 7079 2061 6e64 0d0a 7072 e floppy and..pr

B: ==:--- my_fat_file01 Top L1 (Hexl)-----
```