
Autore: Daniele Murrau
Report soluzione challenge:
Data Hide, un pen-drive multistrato (12/2008)

```
$ wget http://www.ismprofessional.net/pascucci/repo/pen-drive-iisfa-2008.zip
$ unzip pen-drive-iisfa-2008.zip
$ sha1sum pen-drive.dd > pen-drive.sha1
$ more pen-drive.sha1
ac4f5ed6c43a59074045557677e674d4fe243f45 pen-drive.dd
$ du -sb pen-drive.dd
2021654528 pen-drive.dd
```

```
$ fdisk -ul pen-drive.dd
```

You must set cylinders.
You can do this from the extra functions menu.

```
Disk pen-drive.dd: 0 MB, 0 bytes
63 heads, 62 sectors/track, 0 cylinders, total 0 sectors
Units = sectors of 1 * 512 = 512 bytes
Disk identifier: 0x1ae05d97
```

Device	Boot	Start	End	Blocks	Id	System
pen-drive.dd1		62	1972529	986234	b	W95 FAT32

```
$ testdisk /log pen-drive.dd
```

TestDisk 6.8, Data Recovery Utility, August 2007
Christophe GRENIER <grenier@cgsecurity.org>
<http://www.cgsecurity.org>

```
Disk pen-drive.dd - 2021 MB / 1928 MiB - CHS 246 255 63
Partition      Start      End  Size in sectors
D FAT32         0 0 63 122 254 63 1975933 [data-hide]
D FAT32        122 200 1 245 254 63 1979460 [nascosto1]
```

Ignoro partizione non nascosta con label [data-hide]

```
Calcolo offset da utilizzare per mount partizione con label [nascosto1]
LBA = ( ( CYL * HPC + HEAD ) * SPT ) + SECT - 1
LBA = ((122*255+200)*63)+1-1=1972530
offset=1972530*512=1009935360
```

```
$ mount -t auto -o ro,loop,nodev,noexec,noatime,offset=1009935360 pen-drive.dd pen
```

Ok monta senza errori, verifico il contenuto:

```
$ ls -al pen
total 11436
drwxr-xr-x 2 root root 4096 1970-01-01 01:00 .
drwxr-xr-x 3 root root 4096 2009-01-06 12:33 ..
-rwxr-xr-x 1 root root 3256972 2008-10-21 13:26 img_0154.jpg
-rwxr-xr-x 1 root root 2882079 2008-10-21 13:26 img_0155.jpg
-rwxr-xr-x 1 root root 3447899 2008-10-21 13:26 img_0156.jpg
-rwxr-xr-x 1 root root 2107408 2008-10-21 13:26 img_0477.jpg
```

Hex dump in corrispondenza dell'offset:

```
$ xxd -s 1009935360 pen-drive.dd | more
3c326400:eb58 906d 6b64 6f73 6673 0000 0208 2000 .X.mkdosfs.... .
3c326410:0200 0000 00f8 0000 2000 4000 0000 0000 ..... .@.....
3c326420:ce26 1e00 8607 0000 0000 0000 0200 0000 .&.....
3c326430:0100 0600 0000 0000 0000 0000 0000 0000 .....
3c326440:0000 2942 aefd 486e 6173 636f 7374 6f31 ..)B..Hnascosto1
3c326450:2020 4641 5433 3220 2020 0e1f be77 7cac FAT32 ...wl.
3c326460:22c0 740b 56b4 0ebb 0700 cd10 5eeb f032 ".t.V.....^..2
3c326470:e4cd 16cd 19eb fe54 6869 7320 6973 206e .....This is n
3c326480:6f74 2061 2062 6f6f 7461 626c 6520 6469 ot a bootable di
3c326490:736b 2e20 2050 6c65 6173 6520 696e 7365 sk. Please inse
3c3264a0:7274 2061 2062 6f6f 7461 626c 6520 666c rt a bootable fl
3c3264b0:6f70 7079 2061 6e64 0d0a 7072 6573 7320 oppy and..press
3c3264c0:616e 7920 6b65 7920 746f 2074 7279 2061 any key to try a
3c3264d0:6761 696e 202e 2e2e 200d 0a00 0000 0000 gain ... .....
3c3264e0:0000 0000 0000 0000 0000 0000 0000 0000 .....
```

Non sono convinto che sia l'unica partizione oltre quella non nascosta.

Utilizzo un piccolo script in bash che cerca di montare in automatico eventuali partizioni provando ogni offset possibile, il kernel da me utilizzato supporta i filesystem più comuni e questi vengono provati tutti in fase di mount (ext2/3,vfat/ntfs,minix,hfs,hfs+).

```
-----
#!/bin/bash
#f**k the offset
#Daniele Murrau

if [ $# -lt 3 ]; then
{
echo "Usage: $0 image-file starting-block ending-block"
exit
}
fi
```

```

FILE=$1
SBLOCK=$2
EBLOCK=$3
LOG=offset.log

echo -e "Started at: $(date) \n\n" >> $LOG
echo "Image: $FILE" >> $LOG
echo -e "Searching in the block range: $SBLOCK-$EBLOCK\n\n" >> $LOG
for ((i = $SBLOCK; i <= $EBLOCK; i++)); do
    typeset -i offset
    offset=$((i*512))
    echo "Trying offset: $offset"
    mount -t auto -o ro,loop,nodev,noexec,noatime,offset=$offset $FILE pen 2>/dev/null
    a=${?}
    if [ "$a" -eq 0 ]; then
        {
            echo "Error code:" $? "Success! Mounted at offset: " $offset

            echo "Error code:" $? "Success! Mounted at offset: " $offset >> $LOG
            losetup -a >> $LOG
            umount pen
            losetup -d /dev/loop0 2>/dev/null
            echo -e "\nGoing to search next offset..\n" >> $LOG
        }
    else
        {
            losetup -d /dev/loop0 2>/dev/null
        }
    fi
done
echo -e "\n\nFinished at: $(date) \n">> $LOG
-----

```

Prendendo come riferimento blocchi con dimensione da 512 byte faccio un brute force per cercare le partizioni da montare .

Lo script che richiede 3 argomenti, nome immagine, blocco di partenza e blocco di fine, viene lanciato in questo modo:

```
$ ./force.sh pen-drive.dd 0 4194304 <- (questo valore è calcolato su 2 GB, in questo caso in eccesso)
```

Dopo 6 ore circa lo script ha finito e vado a vedere se ha pescato qualcosa.

Il risultato viene inserito in un file chiamato offset.log ed è il seguente:

Error code: 0 Success! Mounted at offset: 31744
/dev/loop0: [0805]:1007658 (pascucci/pen-drive.dd), offset 31744

Going to search next offset..

Error code: 0 Success! Mounted at offset: 512000000
/dev/loop0: [0805]:1007658 (pascucci/pen-drive.dd), offset 512000000

Going to search next offset..

Error code: 0 Success! Mounted at offset: 1009935360
/dev/loop0: [0805]:1007658 (pascucci/pen-drive.dd), offset 1009935360

Going to search next offset..

Sporco, lento e brutto ma in questo caso efficace :)

Quindi abbiamo 3 partizioni:

@offset 31744 abbiamo la partizione nota non nascosta

@offset 512000000 abbiamo una nuova partizione che adesso andiamo ad esaminare

@offset 1009935360 abbiamo la partizione nascosta che avevamo già individuato

Andiamo a verificare cosa si monta di bello all'offset 512000000:

```
$ mount -t auto -o ro,loop,nodev,noexec,noatime,offset=512000000 pen-drive.dd pen
```

```
$ ls -al pen
```

```
total 524
```

```
drwxr-xr-x 2 root root 16384 1970-01-01 01:00 .
```

```
drwxr-xr-x 3 root root 4096 2009-01-06 18:54 ..
```

```
-rwxr-xr-x 1 root root 364643 2008-10-21 13:32 16c450.pdf
```

```
-rwxr-xr-x 1 root root 146960 2008-10-21 13:33 62256.pdf
```

Hex dump in corrispondenza dell'offset:

```
# xxd -s 512000000 pen-drive.dd | more
```

```
1e848000:eb3c 906d 6b64 6f73 6673 0000 0210 0100 .<.mkdosfs.....
1e848010:0200 0200 00f8 c400 2000 4000 0000 0000 ..... .@.....
1e848020:0035 0c00 0000 2931 affd 486e 6173 636f .5....)1..Hnasco
1e848030:7374 6f32 2020 4641 5431 3620 2020 0e1f sto2 FAT16 ..
1e848040:be5b 7cac 22c0 740b 56b4 0ebb 0700 cd10 .[!."t.V.....
1e848050:5eeb f032 e4cd 16cd 19eb fe54 6869 7320 ^..2.....This
1e848060:6973 206e 6f74 2061 2062 6f6f 7461 626c is not a bootabl
1e848070:6520 6469 736b 2e20 2050 6c65 6173 6520 e disk. Please
1e848080:696e 7365 7274 2061 2062 6f6f 7461 626c insert a bootabl
1e848090:6520 666c 6f70 7079 2061 6e64 0d0a 7072 e floppy and..pr
1e8480a0:6573 7320 616e 7920 6b65 7920 746f 2074 ess any key to t
```

1e8480b0:7279 2061 6761 696e 202e 2e2e 200d 0a00 ry again

A questo punto i file individuati sulle 2 partizioni nascoste sono stati analizzati con exif e pdftk, allego in coda (Allegato 1) i risultati già presenti nel report inviato a Mario.

Per concludere verifico che l'integrità dell'immagine sia stata preservata durante il processo:

```
# sha1sum pen-drive.dd > pen-drive.sha1.final  
# diff pen-drive.sha1 pen-drive.sha1.final
```

Fine.

ALLEGATO 1).

Escludendo la partizione non nascosta riesco a montare:

@ offset: 1e848000 (Label: nascosto2 Filesystem: fat16)

Spazio totale: 391M

Spazio occupato: 504K

Spazio libero: 390M

Contenuto:

drwxr-xr-x 2 root root 16384 1970-01-01 01:00 .

drwxr-xr-x 3 root root 4096 2008-12-17 09:41 ..

-rwxr-xr-x 1 root root 364643 2008-10-21 13:32 16c450.pdf

-rwxr-xr-x 1 root root 146960 2008-10-21 13:33 62256.pdf

Pdf files:

62256.pdf:

InfoKey: Producer

InfoValue: Acrobat Distiller 2.0 for Power Macintosh

InfoKey: ModDate

InfoValue: D:19960906015941

InfoKey: CreationDate

InfoValue: D:19960905171208

PdfID0: c97326c63b27656c5e549cf6cb54a8d

PdfID1: f94656c48df4da81b4233c0e1fed3f1

NumberOfPages: 15

16c450.pdf:

InfoKey: Creator

InfoValue: xpdf/pdftops 3.01

InfoKey: Producer

InfoValue: ESP Ghostscript 815.01

InfoKey: ModDate
InfoValue: D:20060315203518
InfoKey: CreationDate
InfoValue: D:20060315203518
PdfID0: c8692bf873b0a664bba1f1e4bfef4b48
PdfID1: c8692bf873b0a664bba1f1e4bfef4b48
NumberOfPages: 25

@ offset: 3c326400 (Label: nascosto1 Filesystem: fat32)

Spazio totale: 963M
Spazio occupato: 12M
Spazio libero: 952M

Contenuto:

```
drwxr-xr-x 2 root root 4096 1970-01-01 01:00 .  
drwxr-xr-x 3 root root 4096 2008-12-17 09:42 ..  
-rwxr-xr-x 1 root root 3256972 2008-10-21 13:26 img_0154.jpg  
-rwxr-xr-x 1 root root 2882079 2008-10-21 13:26 img_0155.jpg  
-rwxr-xr-x 1 root root 3447899 2008-10-21 13:26 img_0156.jpg  
-rwxr-xr-x 1 root root 2107408 2008-10-21 13:26 img_0477.jpg
```

Image files:

EXIF tags in 'pen/img_0154.jpg' ('Intel' byte order):

-----+-----

Tag	Value
Manufacturer	Canon
Model	Canon EOS 350D DIGITAL
Orientation	top - left
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Date and Time	2007:08:24 12:05:40
YCbCr Positioning	co-sited
Compression	JPEG compression
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Exposure Time	1/60 sec.
FNumber	f/5,6
ExposureProgram	Normal program
ISO Speed Ratings	400
Exif Version	Exif Version 2.21

-----+-----

Date and Time (origi|2007:08:24 12:05:40
Date and Time (digit|2007:08:24 12:05:40
ComponentsConfigurat|Y Cb Cr -
Shutter speed |5,91 EV (APEX: 7, 1/60 sec.)
Aperture |4,97 EV (f/5,6)
Exposure Bias |0,00 EV
Metering Mode |Pattern
Flash |Flash fired, auto mode.
Focal Length |45,0 mm
Maker Note |8340 bytes unknown data
User Comment |
FlashPixVersion |FlashPix Version 1.0
Color Space |sRGB
PixelXDimension |3456
PixelYDimension |2304
Focal Plane x-Resolul|3954,23
Focal Plane y-Resolul|3958,76
Focal Plane Resolutil|Inch
Custom Rendered |Normal process
Exposure Mode |Auto exposure
White Balance |Auto white balance
Scene Capture Type |Standard
InteroperabilityIndel|R98
InteroperabilityVers|0100

-----+-----
EXIF data contains a thumbnail (7030 bytes).
EXIF tags in 'pen/img_0155.jpg' ('Intel' byte order):
-----+-----

Tag	Value
Manufacturer	Canon
Model	Canon EOS 350D DIGITAL
Orientation	top - left
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Date and Time	2007:08:24 12:42:50
YCbCr Positioning	co-sited
Compression	JPEG compression
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Exposure Time	1/60 sec.
FNumber	f/5,0
ExposureProgram	Normal program
ISO Speed Ratings	400
Exif Version	Exif Version 2.21
Date and Time (origi 2007:08:24 12:42:50	

Date and Time (digitl|2007:08:24 12:42:50
ComponentsConfigurat|Y Cb Cr -
Shutter speed |5,91 EV (APEX: 7, 1/60 sec.)
Aperture |4,64 EV (f/5,0)
Exposure Bias |0,00 EV
Metering Mode |Pattern
Flash |Flash fired, auto mode.
Focal Length |44,0 mm
Maker Note |8340 bytes unknown data
User Comment |
FlashPixVersion |FlashPix Version 1.0
Color Space |sRGB
PixelXDimension |3456
PixelYDimension |2304
Focal Plane x-Resolul|3954,23
Focal Plane y-Resolul|3958,76
Focal Plane Resolutil|Inch
Custom Rendered |Normal process
Exposure Mode |Auto exposure
White Balance |Auto white balance
Scene Capture Type |Standard
InteroperabilityIndel|R98
InteroperabilityVersl|0100

-----+-----
EXIF data contains a thumbnail (5908 bytes).
EXIF tags in 'pen/img_0156.jpg' ('Intel' byte order):
-----+-----

Tag	Value
Manufacturer	Canon
Model	Canon EOS 350D DIGITAL
Orientation	top - left
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Date and Time	2007:08:24 12:43:05
YCbCr Positioning	co-sited
Compression	JPEG compression
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Exposure Time	1/60 sec.
FNumber	f/4,5
ExposureProgram	Normal program
ISO Speed Ratings	400
Exif Version	Exif Version 2.21
Date and Time (origil 2007:08:24 12:43:05	
Date and Time (digitl 2007:08:24 12:43:05	

ComponentsConfigurat|Y Cb Cr -
Shutter speed |5,91 EV (APEX: 7, 1/60 sec.)
Aperture |4,34 EV (f/4,5)
Exposure Bias |0,00 EV
Metering Mode |Pattern
Flash |Flash fired, auto mode.
Focal Length |35,0 mm
Maker Note |8340 bytes unknown data
User Comment |
FlashPixVersion |FlashPix Version 1.0
Color Space |sRGB
PixelXDimension |3456
PixelYDimension |2304
Focal Plane x-Resolul|3954,23
Focal Plane y-Resolul|3958,76
Focal Plane Resolutil|Inch
Custom Rendered |Normal process
Exposure Mode |Auto exposure
White Balance |Auto white balance
Scene Capture Type |Standard
InteroperabilityIndel|R98
InteroperabilityVersl|0100

-----+-----
EXIF data contains a thumbnail (7126 bytes).
EXIF tags in 'pen/img_0477.jpg' ('Intel' byte order):
-----+-----

Tag	Value
Manufacturer	Canon
Model	Canon EOS 350D DIGITAL
Orientation	top - left
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Date and Time	2007:11:27 23:39:47
YCbCr Positioning	co-sited
Compression	JPEG compression
x-Resolution	72,00
y-Resolution	72,00
Resolution Unit	Inch
Exposure Time	1/1 sec.
FNumber	f/5,6
ExposureProgram	Shutter priority
ISO Speed Ratings	400
Exif Version	Exif Version 2.21
Date and Time (origi	2007:11:27 23:39:47
Date and Time (digit	2007:11:27 23:39:47
ComponentsConfigurat	Y Cb Cr -

Shutter speed 10,74 EV (APEX: 1, 1/1 sec.)
Aperture 14,97 EV (f/5,6)
Exposure Bias 10,00 EV
Metering Mode 1Pattern
Flash 1Flash did not fire, compulsory flash mode.
Focal Length 155,0 mm
Maker Note 18340 bytes unknown data
User Comment 1
FlashPixVersion 1FlashPix Version 1.0
Color Space 1sRGB
PixelXDimension 13456
PixelYDimension 12304
Focal Plane x-Resolul3954,23
Focal Plane y-Resolul3958,76
Focal Plane ResolutilInch
Custom Rendered 1Normal process
Exposure Mode 1Auto exposure
White Balance 1Auto white balance
Scene Capture Type 1Standard
InteroperabilityIndelR98
InteroperabilityVersl0100

-----+-----
EXIF data contains a thumbnail (4238 bytes).