Najprej moramo diske priklopiti, narediti checksum, narediti kopijo, preveriti checksum, nato mount.

To bomo naredili za vsak izmed diskov.

Datoteke, ki pripadajo vsakemu disku lahko najdemo v imeniku z imenom diska.

Disk AAAA

Najprej pogledamo kje je ta naprava:

```
$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0  120G  0 disk
├─sda1   8:1    0  119G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  975M  0 part [SWAP]
sdb      8:16   0   20G  0 disk
├─sdb1   8:17   0  100M  0 part
└─sdb2   8:18   0 19.9G  0 part
sr0     11:0    1 50.6M  0 rom
```

Nato naredimo zaporedje ukazov:

```
sha512sum /dev/sdb >> AAAAhash.txt
cat /dev/sdb > AAAAcopy.img
sha512sum AAAAcopy.img >> AAAAhash.txt
cat AAAAhash.txt
```

Datoteka vsebuje naslednje besedilo: `1193fed2aada9e60fc6566b8addc678f3bf3073f5599d6594b8b7bce2580a07751b588f310a1b0f15d4723037f8cb5d68c52de3ea9f4e28f0306f47bd5044da9 /dev/sdb`
`1193fed2aada9e60fc6566b8addc678f3bf3073f5599d6594b8b7bce2580a07751b588f310a1b0f15d4723037f8cb5d68c52de3ea9f4e28f0306f47bd5044da9 AAAAcopy.img`

Hash vrednosti se ujemata, zato predvidevamo, da je kopiranje uspelo.

Nato naredimo nov imenik mnt/aaaa, kjer bodo lokacija za vklopitev diska in vklopimo disk z uporabo komand:

```
mkdir /mnt/aaaa
mount AAAAcopy.img /mnt/aaaa
```

Ugotovimo, da disk ni pravilni dat. sistem, ker nam shell izpiše:

```
mount: /mnt/aaaa: wrong fs type, bad option, bad superblock on
/dev/loop0, missing codepage or helper program, or other error.
```

Pogledamo v MBR od diska. To naredimo z orodjem `randare2`. Izpis iz MBR je sledeč:

```
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00000000  33c0 8ed0 bc00 7c8e c08e d8be 007c bf00  3.....|.......|..
0x00000010  06b9 0002 fcf3 a450 681c 06cb fbb9 0400  .......Ph.......
0x00000020  bdbe 0780 7e00 007c 0b0f 850e 0183 c510  ....~..|........
0x00000030  e2f1 cd18 8856 0055 c646 1105 c646 1000  .....V.U.F...F..
0x00000040  b441 bbaa 55cd 135d 720f 81fb 55aa 7509  .A..U..]r...U.u.
0x00000050  f7c1 0100 7403 fe46 1066 6080 7e10 0074  ....t..F.f`.~..t
0x00000060  2666 6800 0000 0066 ff76 0868 0000 6800  &fh....f.v.h..h.
0x00000070  7c68 0100 6810 00b4 428a 5600 8bf4 cd13  |h..h...B.V.....
0x00000080  9f83 c410 9eeb 14b8 0102 bb00 7c8a 5600  ............|.V.
0x00000090  8a76 018a 4e02 8a6e 03cd 1366 6173 1cfe  .v..N..n...fas..
0x000000a0  4e11 750c 807e 0080 0f84 8a00 b280 eb84  N.u..~..........
0x000000b0  5532 e48a 5600 cd13 5deb 9e81 3efe 7d55  U2..V...]...>.}U
0x000000c0  aa75 6eff 7600 e88d 0075 17fa b0d1 e664  .un.v....u.....d
0x000000d0  e883 00b0 dfe6 60e8 7c00 b0ff e664 e875  ......`.|....d.u
0x000000e0  00fb b800 bbcd 1a66 23c0 753b 6681 fb54  .......f#.u;f..T
0x000000f0  4350 4175 3281 f902 0172 2c66 6807 bb00  CPAu2....r,fh...
0x00000100  0066 6800 0200 0066 6808 0000 0066 5366  .fh....fh....fSf
0x00000110  5366 5566 6800 0000 0066 6800 7c00 0066  SfUfh....fh.|..f
0x00000120  6168 0000 07cd 1a5a 32f6 ea00 7c00 00cd  ah.....Z2...|...
0x00000130  18a0 b707 eb08 a0b6 07eb 03a0 b507 32e4  ..............2.
0x00000140  0500 078b f0ac 3c00 7409 bb07 00b4 0ecd  ......<.t.......
0x00000150  10eb f2f4 ebfd 2bc9 e464 eb00 2402 e0f8  ......+..d..$...
0x00000160  2402 c349 6e76 616c 6964 2070 6172 7469  $..Invalid parti
0x00000170  7469 6f6e 2074 6162 6c65 0045 7272 6f72  tion table.Error
0x00000180  206c 6f61 6469 6e67 206f 7065 7261 7469   loading operati
0x00000190  6e67 2073 7973 7465 6d00 4d69 7373 696e  ng system.Missin
0x000001a0  6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
0x000001b0  656d 0000 0063 7b9a e072 6eca 0000 8020  em...c{..rn.... 
0x000001c0  2100 07df 130c 0008 0000 0020 0300 00df  !.......... ....
0x000001d0  140c 07fe ffff 0028 0300 00d0 7c02 0000  .......(....|...
0x000001e0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x000001f0  0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

Po temu so na disku zapisane same ničle.

Ugotovimo, da je z diskom nekaj narobe in da nima operacijskega sistema.

Nato z ukazom `file`, pogledamo, kaj sistem Linux lahko pove o tej datoteki. Dobimo naslednje:
`AAAAcopy.img: DOS/MBR boot sector MS-MBR Windows 7 english at offset 0x163 "Invalid`

`partition table" at offset 0x17b "Error loading operating system" at offset 0x19a "Missing operating system", disk signature 0xca6e72e0; partition 1 : ID=0x7, active, start-CHS (0x0,32,33), end-CHS (0xc,223,19), startsector 2048, 204800 sectors; partition 2 : ID=0x7, start-CHS (0xc,223,20), end-CHS (0x3ff,254,63), startsector 206848, 41734144 sectors`

Ugotovimo, da bil na disku prej naložen Windows 7 operacijski sistem, ki je zdaj manjkajoč.

Nato vklopimo disk skozi qemu-nbd, da lahko dostopamo lažje do posameznih particij.

Opazimo, da je Datotečni sistem NTFS, kar potrdi, da je bil na računalniku prej Windows:

```
Disk /dev/nbd0: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xca6e72e0

Device      Boot  Start      End  Sectors  Size Id Type
/dev/nbd0p1 *      2048   206847   204800  100M  7 HPFS/NTFS/exFAT
/dev/nbd0p2      206848 41940991 41734144 19.9G  7 HPFS/NTFS/exFAT
```

S pomočjo zaporedja ukazov:

```
mkdir /mnt/nbd0p2
mount /dev/nbd0p2 /mnt/nbd0p2/
ls /mnt/nbd0p2/
```

Lahko vklopimo 2. (podatkovno) particijo NTFS sistema in pogledamo kateri podatki so notri:

```
'$Recycle.Bin'           hiberfil.sys  'Program Files'           Windows
 autoexec.bat           pagefile.sys   Recovery
 config.sys           PerfLogs     'System Volume Information'
'Documents and Settings'   ProgramData      Users
```

V `Documents and Settings\user\Documents` najdemo ZIP datoteko, ki vsebuje word dokument, ki opisuje Rastrsko grafiko.

V košu lahko najdemo desktop.ini, ki ne vsebuje nobenih koristnih informacij.

Vse datoteke, ki vsebujejo "XXXX" smo dobili z ukazom:

```
find "." -type f -exec sh -c 'strings "$0"
| grep -q "XXXX" && echo "$0"' {} \;
```

Nato smo preverili, kateri izmed teh dokumentov so dokumenti ali slike z uporabo bash skripte:

```
#!/bin/bash

while read -r file; do
    file_type="$(file -b "$file")"
    if ([[ "$file_type" == *"document"* ]] || [[ "$file_type" == *"image"* ]])
    then
        echo "$file"
    fi
done < "$1"
```

Ugotovili smo, da so dokumenti in slike, ki vsebujejo "XXXX" sledeči:

```
/mnt/nbd0p2/Recovery/ffea95a2-944c-11e3-b0fa-e4e0d4e5f416/Winre.wim
/mnt/nbd0p2/Windows/PolicyDefinitions/en-US/Power.adml
/mnt/nbd0p2/Windows/System32/WindowsPowerShell/v1.0/en-
US/Microsoft.Wsman.Management.dll-Help.xml
/mnt/nbd0p2/Windows/winsxs/x86_microsoft-windows-p..ll-
preloc.resources_31bf3856ad364e35_6.1.7600.16385_en-
us_c188a87b02c13257/Microsoft.Wsman.Management.dll-Help.xml
/mnt/nbd0p2/Windows/winsxs/x86_microsoft-windows-power-
adm.resources_31bf3856ad364e35_6.1.7600.16385_en-us_68e01cb2afe0f216/Power.adml
```

Nobena izmed datotek ni bila izbrisana ali namerno skrita, saj so to sistemske datoteke.

Pogledamo, če so bile kakšne datoteke izbrisane z orodjem `testdisk` in ugotovimo, da izbrisanih datotek ni.

Na koncu bomo poizkusili še z zagonom diska na virtualnem stroju. Najprej smo disk kopirali, in ga dali v VirtualBox, kjer smo naredili nov VM že prej.

Ugotovimo, da ne moremo dostopati do Windows sitema, ker so problemi z boot particijo, kot smo jih omenili že prej.

S tem zaženemo system restore na VM in pogledamo, če je bil uspešen. V našem primeru ni bil uspešen, zato lahko z raziskavo zaključimo.

Disk BBBB

Ponovno izvedemo iste ukaze kot pri disku AAAA in ugotovimo, da se hash vrednosti ujemajo:

```
fd6401e02d9f56856a32b88f7ffe9ab79b4fb6dc38711b9530dd0623c786722c970484
1f924b21cf73e8a349b7406bb8fd605187187f1a340730f30f3879002a  /dev/sdb
fd6401e02d9f56856a32b88f7ffe9ab79b4fb6dc38711b9530dd0623c786722c970484
1f924b21cf73e8a349b7406bb8fd605187187f1a340730f30f3879002a  BBBBcopy.img
```

Ko disk vklopimo z `qemu-nbd`, vidimo, da ima disk 3 particije:

```
NAME     MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda        8:0    0  120G  0 disk
├─sda1     8:1    0  119G  0 part /
├─sda2     8:2    0    1K  0 part
└─sda5     8:5    0  975M  0 part [SWAP]
sdb        8:16   0   40G  0 disk
├─sdb1     8:17   0   39G  0 part
├─sdb2     8:18   0    1K  0 part
└─sdb5     8:21   0 1022M  0 part
sr0       11:0    1   51M  0 rom  /media/cdrom0
nbd0      43:0    0   40G  0 disk
├─nbd0p1  43:1    0   39G  0 part
├─nbd0p2  43:2    0    1K  0 part
└─nbd0p5  43:5    0 1022M  0 part
```

Zdaj pogledamo še informacije o disku z orodjem `fdisk`, ki nam da naslednji izhod:

```
Disk /dev/nbd0: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000bd355


Device      Boot    Start      End  Sectors  Size Id Type
/dev/nbd0p1 *        2048 81788927 81786880   39G 83 Linux
/dev/nbd0p2      81790974 83884031  2093058 1022M  5 Extended
/dev/nbd0p5      81790976 83884031  2093056 1022M 82 Linux swap / Solaris
```

Kot vidimo ima disk 3 particije, zato lahko pogledamo, kaj se skriva v njih. Vklopimo lahko samo particijo nbd0p1, saj sta drugi dve particiji Swap in Extended, ki se ne dajo vklopiti.

Najprej moramo vklopiti to particijo z `mount /dev/nbd0p1 /mnt/bbbbp1`

Vidimo, da ima dat. sistem klasično linux ahritekturo:

```
bin    dev   initrd.img  lost+found  opt   run     sys  var
boot   etc   lib     media         proc  sbin  tmp  vmlinuz
cdrom  home  lib64     mnt         root  srv     usr
```

Po kratkem raziskovanju opazimo, da je v `/home/user/Documents`, zip datoteka, ki vsebuje predstavitev o tiskarskih tehnikah.

Sedaj pogledamo, katere datoteke vsebujejo niz "XXXX" s komando: `grep -lr "XXXX" /mnt/bbbbp1/ >> /home/dig/bbbb/containingXXX.txt`

Opazimo, da so dokumenti in slike, ki vsebujejo niz "XXXX" sledeči:

```
/mnt/bbbbp1/usr/share/app-install/icons/kraptor.png
/mnt/bbbbp1/usr/share/app-install/icons/dell-dvd.svg
/mnt/bbbbp1/usr/share/app-install/icons/gromit.svg
/mnt/bbbbp1/usr/share/app-install/icons/gromit-mpx.svg
/mnt/bbbbp1/usr/share/app-install/icons/dreampie.png
/mnt/bbbbp1/usr/share/icons/HighContrast/256x256/emblems/emblem-default.png
/mnt/bbbbp1/usr/share/icons/HighContrast/256x256/apps/goa-panel.png
/mnt/bbbbp1/usr/share/nux/4.0/UITextures/RoundCorner_10px_shadow.tga
/mnt/bbbbp1/usr/share/cups/data/form_russian.pdf
/mnt/bbbbp1/usr/share/cups/data/form_english.pdf
/mnt/bbbbp1/usr/share/mobile-broadband-provider-info/serviceproviders.xml
/mnt/bbbbp1/usr/share/ghostscript/9.10/lib/gs_m.xpm
/mnt/bbbbp1/usr/share/ghostscript/9.10/lib/gs_l.xpm
/mnt/bbbbp1/usr/share/ghostscript/9.10/lib/gs_s.xpm
/mnt/bbbbp1/usr/share/ghostscript/9.10/lib/gs_t.xpm
/mnt/bbbbp1/usr/share/webbrowser-app/screenshot.png
/mnt/bbbbp1/usr/share/help/C/gnome-system-monitor/figures/gnome-system-
monitor_window.png
/mnt/bbbbp1/usr/share/help/C/cheese/figures/effects.png
/mnt/bbbbp1/usr/lib/libreoffice/share/gallery/txtshapes/Hexagon03-Green.svg
/mnt/bbbbp1/usr/lib/libreoffice/share/gallery/arrows/A27-CurvedArrow-DarkRed.png
/mnt/bbbbp1/usr/lib/libreoffice/share/config/psetupl.xpm
/mnt/bbbbp1/usr/lib/libreoffice/share/config/psetup.xpm
```

Vsakega od teh dokumentov pogledamo. V nobenem od dokumentov ne najdemo nič kaj preveč zanimivega.

Nato pogledamo za skrite doklumente z orodjem `testdisk`. Opazimo, da so izbrisane datoteke brez kakršne koli velike vrednosti.

Sedaj, pa probamo še vklopiti disk v VM. Ugotovimo, da ima računalnik zaščito z geslom. Poizkusimo z iskanjem tega gesla, ki ga najdemo v /etc/shadow. Za razbitje gesla bi uporabili orodje John the Ripper, ker pa imamo malo zmogljiv računalnik bi to trajalo preveč časa.

Med razbijanjem gesla lahko pogledamo zabeležke sistema, če opazimo kaj zanimivega. najprej pogledamo v `syslog`.

Opazimo, da je bil v računalnik vstacljen CD-ROM, ter da je operacijski sistem tekel na virtualki, saj je kot vhodna naprava izbrana `VMware WMMouse`. Vidimo tudi, da je uporabnik 'avahi' izgubil root privilegije, ter da je na računalniku potekala komunikacija prek bluetootha, ter etherneta. Opazimo tudi, da se je spreminjala ipconfig konfiguracija. Opazimo tudi, da je potekala komunikacija prek DHCP s strežnikom na naslovu **10.0.2.2**. Na koncu je uporabnik še pognal storitve `org.freedesktop.ColorManager` in `org.freedesktop.UDisks2`. Izhod datoteke syslog je shranjen v imeniku *bbbb*.

DISK CCCC

Ponovno izvedemo iste ukaze kot pri disku AAAA in ugotovimo, da se hash vrednosti ujemajo:

```
cb153cdcbee73f89e1d11d97dd2972b89f1e679c4b78d304505ddbe786a3e63e346a4f
763c26cf3c305e341bf892b74b6d379824f4122c1b5b01e805f842fc7a  /dev/sdc
cb153cdcbee73f89e1d11d97dd2972b89f1e679c4b78d304505ddbe786a3e63e346a4f
763c26cf3c305e341bf892b74b6d379824f4122c1b5b01e805f842fc7a  CCCCcopy.img
```

Ko disk vklopimo z `qemu-nbd` v napravo `nbd1` vidimo, da ima disk 2 particiji in podobno strukturo disku AAAA:

```
NAME     MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda        8:0    0  120G  0 disk
├─sda1     8:1    0  119G  0 part /
├─sda2     8:2    0    1K  0 part
└─sda5     8:5    0  975M  0 part [SWAP]
sdb        8:16   0   40G  0 disk
├─sdb1     8:17   0   39G  0 part
├─sdb2     8:18   0    1K  0 part
└─sdb5     8:21   0 1022M  0 part
sdc        8:32   0   20G  0 disk
├─sdc1     8:33   0  100M  0 part
└─sdc2     8:34   0 19.9G  0 part
sr0       11:0    1   51M  0 rom  /media/cdrom0
nbd0      43:0    0   40G  0 disk
├─nbd0p1  43:1    0   39G  0 part /mnt/bbbbp1
├─nbd0p2  43:2    0    1K  0 part
└─nbd0p5  43:5    0 1022M  0 part
nbd1      43:64   0   20G  0 disk
├─nbd1p1  43:65   0  100M  0 part
└─nbd1p2  43:66   0 19.9G  0 part
```

disk pogledamo še z orodjem `fdisk`, ki nam da naslednji izhod:

```
Disk /dev/nbd1: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xca6e72e0


Device      Boot  Start      End  Sectors  Size Id Type
/dev/nbd1p1 *      2048   206847   204800  100M  7 HPFS/NTFS/exFAT
/dev/nbd1p2      206848 41940991 41734144 19.9G  7 HPFS/NTFS/exFAT
```

Vidimo, da disk uporablja NTFS podatkovni sistem, zato pogledamo še MBR, kjer opazimo isti problem kot pri prvem disku:

```
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x00000000  33c0 8ed0 bc00 7c8e c08e d8be 007c bf00  3.....|......|..
0x00000010  06b9 0002 fcf3 a450 681c 06cb fbb9 0400  .......Ph.......
0x00000020  bdbe 0780 7e00 007c 0b0f 850e 0183 c510  ....~..|........
0x00000030  e2f1 cd18 8856 0055 c646 1105 c646 1000  .....V.U.F...F..
0x00000040  b441 bbaa 55cd 135d 720f 81fb 55aa 7509  .A..U..]r...U.u.
0x00000050  f7c1 0100 7403 fe46 1066 6080 7e10 0074  ....t..F.f`.~..t
0x00000060  2666 6800 0000 0066 ff76 0868 0000 6800  &fh....f.v.h..h.
0x00000070  7c68 0100 6810 00b4 428a 5600 8bf4 cd13  |h..h...B.V.....
0x00000080  9f83 c410 9eeb 14b8 0102 bb00 7c8a 5600  ............|.V.
0x00000090  8a76 018a 4e02 8a6e 03cd 1366 6173 1cfe  .v..N..n...fas..
0x000000a0  4e11 750c 807e 0080 0f84 8a00 b280 eb84  N.u..~..........
0x000000b0  5532 e48a 5600 cd13 5deb 9e81 3efe 7d55  U2..V...]...>.}U
0x000000c0  aa75 6eff 7600 e88d 0075 17fa b0d1 e664  .un.v....u.....d
0x000000d0  e883 00b0 dfe6 60e8 7c00 b0ff e664 e875  ......`.|....d.u
0x000000e0  00fb b800 bbcd 1a66 23c0 753b 6681 fb54  .......f#.u;f..T
0x000000f0  4350 4175 3281 f902 0172 2c66 6807 bb00  CPAu2....r,fh...
0x00000100  0066 6800 0200 0066 6808 0000 0066 5366  .fh....fh....fSf
0x00000110  5366 5566 6800 0000 0066 6800 7c00 0066  SfUfh....fh.|..f
0x00000120  6168 0000 07cd 1a5a 32f6 ea00 7c00 00cd  ah.....Z2...|...
0x00000130  18a0 b707 eb08 a0b6 07eb 03a0 b507 32e4  ..............2.
0x00000140  0500 078b f0ac 3c00 7409 bb07 00b4 0ecd  ......<.t.......
0x00000150  10eb f2f4 ebfd 2bc9 e464 eb00 2402 e0f8  ......+..d..$...
0x00000160  2402 c349 6e76 616c 6964 2070 6172 7469  $..Invalid parti
0x00000170  7469 6f6e 2074 6162 6c65 0045 7272 6f72  tion table.Error
0x00000180  206c 6f61 6469 6e67 206f 7065 7261 7469   loading operati
0x00000190  6e67 2073 7973 7465 6d00 4d69 7373 696e  ng system.Missin
0x000001a0  6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
0x000001b0  656d 0000 0063 7b9a e072 6eca 0000 8020  em...c{..rn.... 
0x000001c0  2100 07df 130c 0008 0000 0020 0300 00df  !.......... ....
0x000001d0  140c 07fe ffff 0028 0300 00d0 7c02 0000  .......(....|...
0x000001e0  0000 0000 0000 0000 0000 0000 0000 0000  ................
0x000001f0  0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

Nato lahko drugo particijo diska vklopimo z ukazom `mount` in pogledamo, kaj se skriva v dat. sistemu.

Opazimo, da imajo datoteke klasično Windows strukturo:

```
'$Recycle.Bin'            ProgramData
 autoexec.bat            'Program Files'
 config.sys              Recovery
'Documents and Settings'  'System Volume Information'
 hiberfil.sys             Users
 pagefile.sys             Windows
 PerfLogs
```

Naredimo pregled datotek, ki vsebujejo "XXXX" z že prej omenjenim ukazom. Raziskava pokaže, da so dokumenti in slike, ki vsebujejo niz sledeče:

```
/mnt/cccc/Recovery/ffea95a2-944c-11e3-b0fa-e4e0d4e5f416/Winre.wim
/mnt/cccc/Users/user/Documents/Harry Potter and the Methods of
Rationality, Chapter 2: Everything I Believe Is False.html
/mnt/cccc/Users/user/Pictures/xxxx.jpg
/mnt/cccc/Windows/PolicyDefinitions/en-US/Power.adml
/mnt/cccc/Windows/System32/WindowsPowerShell/v1.0/en-US/
Microsoft.Wsman.Management.dll-Help.xml
/mnt/cccc/Windows/winsxs/x86_microsoft-windows-p.
.ll-preloc.resources_31bf3856ad364e35_6.1.7600.
16385_en-us_c188a87b02c13257/Microsoft.Wsman.Management.dll-Help.xml
/mnt/cccc/Windows/winsxs/x86_microsoft-windows-power
-adm.resources_31bf3856ad364e35_6.1.7600.16385_en-us_
68e01cb2afe0f216/Power.adml
```

Najbolj zanimivi zgledata datoteki *xxxx.jpg* in *Harry Potter and the Methods of Rationality, Chapter 2: Everything I Believe Is False.html*, a si vseeno ogledamo vse datoteke.

Prva datoteka vsebuje podatke, ki jih windows potrebuje za obnovitev. Pogledali bomo tudi v winre.wim, za datoteke, ki vsebujejo niz "XXXX" in ugotovimo, da dokumentov in slik, ki vsebujejo niz ni.

Odpremo mapo Users/user/Documents/My Pictures in najdelo precej informacij.

Najdemo 3 slike, ki izgledajo zaupne, vsaj po imenu. ena izmed teh (confidential-04.jpg) vsebuje niz "XXXX". Slike: *chat_systems_2x.png*, *SabOnline10.GIF* in *sukellusta_tulvassa.jpg*, pravtako vsebujejo niz "XXXX".

V User/Documents najdemo še več datotek in imenikov ter vsako analiziramo.

Ko odpremo dokument *document.odt*, vidimo, da notri piše "To je ena od iskanih datotek", ter še ena ponovitev niza "XXXX".

Ko odpremo dokument *eko_cert.odt* najdemo še eno pojavitev niza "XXXX" in zraven prilepljeno sliko nekakšnih vrat.

Ob pregledu dokumenta *Harry Potter and the Methods of Rationality, Chapter 2: Everything I Believe Is False.html* opazimo, da se iskani niz ponovi kar dvakrat.

Ko odpremo dokument *gro_sno_tisk_01.zip*, najdemo še en dokument, ki vsebuje predstavitev o tiskarskih tehnikah.

Pogledamo še v imenik *Harry Potter and the Methods of Rationality, Chapter 2: Everything I Believe Is False_files*, kjer najdemo skripto, ki izgleda kot podporna skripta za dokument .html

Nato pregledamo še disk z orodjem `testdisk`, da vidimo, če obstaja kakšna izbrisana datoteka. Opazimo, da je izbrisanih datotek kar nekaj, zato jih pregledamo.

Datoteki v imeniku *Harry Potter and the Methods of Rationality, Chapter 2_ Everything I Believe Is False_files*, sta datoteki, ki pripadata html dkoumentu in ne vsebujeta nič zanimivega.

Dokument *narocilo.odt* tudi ne vsebuje nič zanimivega.

Slika *confidential-01.jpg* vsebuje naš iskani niz "XXXX", zraven najdemo tudi drugo sliko *confidential-03.jpg*. Obe sliki izgledata zaupne narave.

Video posnetek *Lie_detector.mp4*, tudi ne vsebuje za raziskavo nič zanimivega.

Video posnetek test.mp4, pa vsebuje naš iskani niz "XXXX".

S tem zaključimo raziskavo tega diska.

Podobno kot pri disku AAAA, ko poizkušamo pognati sistem na VM, ne deluje.

DISK DDDD

Ponovno izvedemo iste ukaze kot pri disku AAAA in ugotovimo, da se hash vrednosti ujemajo:

```
a7a03d02ecc04f8b0b4f3fc79cc3d46767fd3245f2bcdd33361f949dca2fcfe480c57
a56fc5050b88f6924ee04bf400c18bffdd0e1f3d33c0e7ea0f0b75d3a9c  /dev/sdb
a7a03d02ecc04f8b0b4f3fc79cc3d46767fd3245f2bcdd33361f949dca2fcfe480c57
a56fc5050b88f6924ee04bf400c18bffdd0e1f3d33c0e7ea0f0b75d3a9c  DDDDcopy.img
```

Ko disk vklopimo z `qemu-nbd` v napravo `nbd0` vidimo, da ima disk 3 particije in podobno strukturo disku BBBB:

```
NAME     MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda        8:0    0  120G  0 disk
├─sda1     8:1    0  119G  0 part /
├─sda2     8:2    0    1K  0 part
└─sda5     8:5    0  975M  0 part [SWAP]
sdb        8:16   0   40G  0 disk
├─sdb1     8:17   0   39G  0 part
├─sdb2     8:18   0    1K  0 part
└─sdb5     8:21   0 1022M  0 part
sr0       11:0    1   51M  0 rom  /media/cdrom0
nbd0      43:0    0   40G  0 disk
├─nbd0p1  43:1    0   39G  0 part
├─nbd0p2  43:2    0    1K  0 part
└─nbd0p5  43:5    0 1022M  0 part
```

To nam potrdi še orodje `fdisk`:

```
Disk /dev/nbd0: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000bd355


Device      Boot    Start      End  Sectors  Size Id Type
/dev/nbd0p1 *        2048 81788927 81786880   39G 83 Linux
/dev/nbd0p2      81790974 83884031  2093058 1022M  5 Extended
/dev/nbd0p5      81790976 83884031  2093056 1022M 82 Linux swap / Sol
```

S tem lahko vklopimo 1. particijo z ukazom `mount /dev/nbd0p1 /mnt/dddd`.

Opazimo, da ima dat. sistem klasično linux strukturo:

```
bin    dev   initrd.img  lost+found  opt   run     sys  var
boot   etc   lib     media         proc  sbin  tmp  vmlinuz
cdrom  home  lib64     mnt           root  srv     usr
```

Naredimo pregled datotek, ki vsebujejo "XXXX" z že prej omenjenim ukazom. Raziskava pokaže, da so dokumenti in slike, ki vsebujejo niz sledeče:

```
/mnt/dddd/usr/share/app-install/icons/kraptor.png
/mnt/dddd/usr/share/app-install/icons/dell-dvd.svg
/mnt/dddd/usr/share/app-install/icons/gromit.svg
/mnt/dddd/usr/share/app-install/icons/gromit-mpx.svg
/mnt/dddd/usr/share/app-install/icons/dreampie.png
/mnt/dddd/usr/share/icons/HighContrast/256x256/emblems/emblem-default.png
/mnt/dddd/usr/share/icons/HighContrast/256x256/apps/goa-panel.png
/mnt/dddd/usr/share/nux/4.0/UITextures/RoundCorner_10px_shadow.tga
/mnt/dddd/usr/share/cups/data/form_russian.pdf
/mnt/dddd/usr/share/cups/data/form_english.pdf
/mnt/dddd/usr/share/mobile-broadband-provider-info/serviceproviders.xml
/mnt/dddd/usr/share/ghostscript/9.10/lib/gs_m.xpm
/mnt/dddd/usr/share/ghostscript/9.10/lib/gs_l.xpm
/mnt/dddd/usr/share/ghostscript/9.10/lib/gs_s.xpm
/mnt/dddd/usr/share/ghostscript/9.10/lib/gs_t.xpm
/mnt/dddd/usr/share/webbrowser-app/screenshot.png
/mnt/dddd/usr/share/help/C/gnome-system-monitor/figures/gnome-system-
monitor_window.png
/mnt/dddd/usr/share/help/C/cheese/figures/effects.png
/mnt/dddd/usr/lib/libreoffice/share/gallery/txtshapes/Hexagon03-Green.svg
/mnt/dddd/usr/lib/libreoffice/share/gallery/arrows/A27-CurvedArrow-DarkRed.png
/mnt/dddd/usr/lib/libreoffice/share/config/psetupl.xpm
/mnt/dddd/usr/lib/libreoffice/share/config/psetup.xpm
```

Datoteke so identične, kot na disku BBBB, zato predpostavimo, da vsebujejo iste podatke in jih s tem razlogom ne pregledujemo. Nato gremo pogledati v datotečni sistem.

V imeniku /home/user najdemo kar nekaj zanimivih datotek.

Video posnetek *What If Wild Animals Ate Fast Food.flv* ne vsebuje nič raziskavi zanimivega.

Video posnetek *test.mp4* vsebuje naš iskan niz "XXXX".

Ko odpremo dokument *eko_cert.odt* najdemo še eno pojavitev niza "XXXX" in zraven prilepljeno sliko nekakšnih vrat.

Nato se pomaknemo v imenik Documents.

Ko odpremo dokument *document.odt* vidimo da v njej piše "To je ena od iskanih datotek" in naš iskan niz "XXXX".

Ob pregledu datoteke *script.js* ne najdemo nič zanimivega.

Ob pregledu datoteke *print.css* ne najdemo nič zanimivega.

Nato se premaknemo v imenik Pictures.

Najdemo 2 sliki, ki zgledata zaupni (*confidential-02.jpg* in *confidential-03.jpg*).

Najdemo tudi sliko *sukellusta_tulvassa.jpg*, ki vsebuje naš iskani niz.

Nato pregledamo še disk z orodjem `testdisk`, da vidimo, če obstaja kakšna izbrisana datoteka. Opazimo, da je izbrisanih datotek kar nekaj, zato jih pregledamo.

Ob pregeldu vidimo, da so vse te datoteke velikosti 0. Predvidevamo, da je bila velikost datotek spremenjena z namenom skrivanja podatkov.

Z uporabo orodja `extundelete` nam je uspelo pridobiti nazaj 2 datoteki in sicer */home/user/Lie_Detector.mp4*, ter */home/user/Documents/Harry Potter and the Methods of Rationality, Chapter 2: Everything I Believe Is False.html*.

Video *Lie_Detector.mp4* ne vsebuje raziskavi zanimive vsebine.

Datoteka *Harry Potter and the Methods of Rationality, Chapter 2: Everything I Believe Is False.html*, pa vsebuje 2 pojavitve niza "XXXX".

Nato preverimo še zabeležke v `syslog`, če opazimo kaj zanimivega. Opazimo, da je bil na sda5 prikljkuček dodana swap particija in da se je prižgal Bluetooth. Nato opazimo nekaj komunikacije po eth0 in začetek DHCPv4 transakcije. Opazimo, da se naprava pogovarja z naslovom *10.0.2.2*, in da mu je ta posredoval naslov *10.0.2.15*. To pomeni, da se je naprava priklopila na mrežo, kjer ji je bil dodeljen IP naslov dinamično. Na koncu sta bila zagnani še storitvi *org.freedesktop.ColorManager* in *org.freedesktop.UDisk2*.