

**SVEUČILIŠTE U SPLITU
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I
BRODOGRADNJE**

SEMINARSKI RAD

FORENZIKA OS-a - ORACLE VIRTUALBOX

Vlaho Petković, Leo Štroliga

Split, 8.7.2024.

SADRŽAJ

1	Uvod.....	1
2	Priprema radnog okruženja	2
2.1	<i>Instalacija VritualBox-a</i>	2
2.2	<i>Omogućavanje virtualizacije</i>	2
3	Kreiranje VMDK datoteke.....	4
4	Kreiranje virtualne mašine	6
5	Analiza hard diska.....	8
6	Zaključak.....	11
	Sažetak i ključne riječi	12

1 Uvod

Oracle VM VirtualBox, često nazivan samo VirtualBox, moćan je softverski paket za virtualizaciju x86 i AMD64/Intel64 platformi otvorenog koda, razvijen od strane Oracle Corporation. Omogućuje korisnicima pokretanje više operativnih sustava istovremeno na jednom fizičkom računalu, omogućujući nesmetane prijelaze između različitih OS okruženja bez potrebe za više uređaja. Ova značajka je posebno korisna za razvojne programere, testere i IT profesionalce koji zahtijevaju različite postavke operativnih sustava za svoj rad.

VirtualBox podržava širok raspon matičnih operativnih sustava, uključujući Windows, macOS, Linux i Solaris. Njegova svestranost proteže se i na gostujuće operativne sustave, s podrškom za brojne verzije Windowsa, Linux distribucija, macOS-a i drugih. Ova kompatibilnost između platformi čini VirtualBox neprocjenjivim alatom u različitim IT i razvojnim okruženjima, pružajući dosljedno virtualno iskustvo na različitim platformama.

Jedna od ključnih prednosti VirtualBoxa je njegov sveobuhvatni set značajki. Uključuje mogućnosti poput snimanja stanja (snapshots), koje omogućuju korisnicima spremanje i vraćanje stanja virtualnog stroja (VM) u bilo kojem trenutku, olakšavajući eksperimentiranje s različitim konfiguracijama i brzo oporavak od bilo kakvih promjena koje uzrokuju probleme. Osim toga, VirtualBox nudi kloniranje virtualnih strojeva, omogućujući korisnicima stvaranje točnih kopija VM-ova za potrebe testiranja i implementacije. Softver također podržava zajedničke mape, omogućujući nesmetan prijenos datoteka između matičnih i gostujućih sustava.

Oracle VM VirtualBox je robustno i svestrano virtualizacijsko rješenje pogodno za širok raspon primjena. Njegova podrška za više matičnih i gostujućih operativnih sustava, u kombinaciji s bogatim setom značajki i korisnički pristupačnim sučeljem, čini ga idealnim izborom za razvojne programere, testere i IT profesionalce koji trebaju pokretati i upravljati više operativnih sustava na jednoj hardverskoj platformi.

2 Priprema radnog okruženja

2.1 Instalacija VritualBox-a

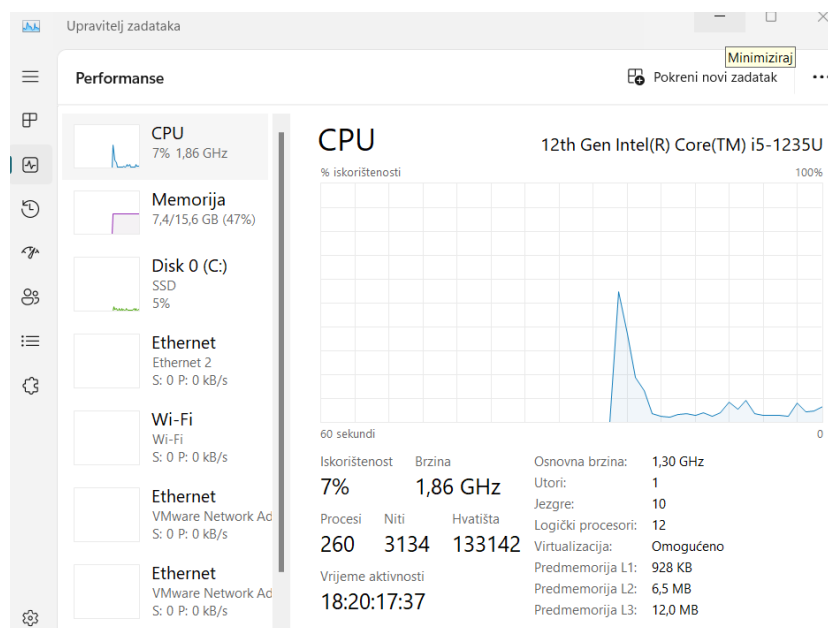
Upišemo u Web Browser *Oracle VirtualBox*. Prvi link koji nam iskoči jest <https://www.virtualbox.org/>. Kliknemo na *Downloads* te odaberemo *Instalacija za Windows Host*. Instaliramo .exe file i pokrenemo ga. Na svaki prozor kliknemo *Next* te na zadnjem prozoru kliknemo *Finish*. Time smo instalirali VirtualBox.



Slika 2-1 VirtualBox ikona

2.2 Omogućavanje virtualizacije

Ukoliko nismo sigurni je li nam virtualizacija omogućena, klikom na *Ctrl + Shift + Esc* provjeravamo u Performansama sustava je li nam virtualizacija omogućena.



Slika 2-2 Performanse sustava

Ukoliko virtualizacija nije omogućena radimo sljedeće. Ugasimo računalo. Ponovno ga pokrenemo, te uđemo u BIOS postavke računala. Kliknemo na ili *Advanced* ili *CPU Configuration* ili *Chipset* ili *Security*. Zatim kliknemo na *Virtualization* i omogućimo je. Omogućimo *Intel VT-x* ili *AMD-V*.

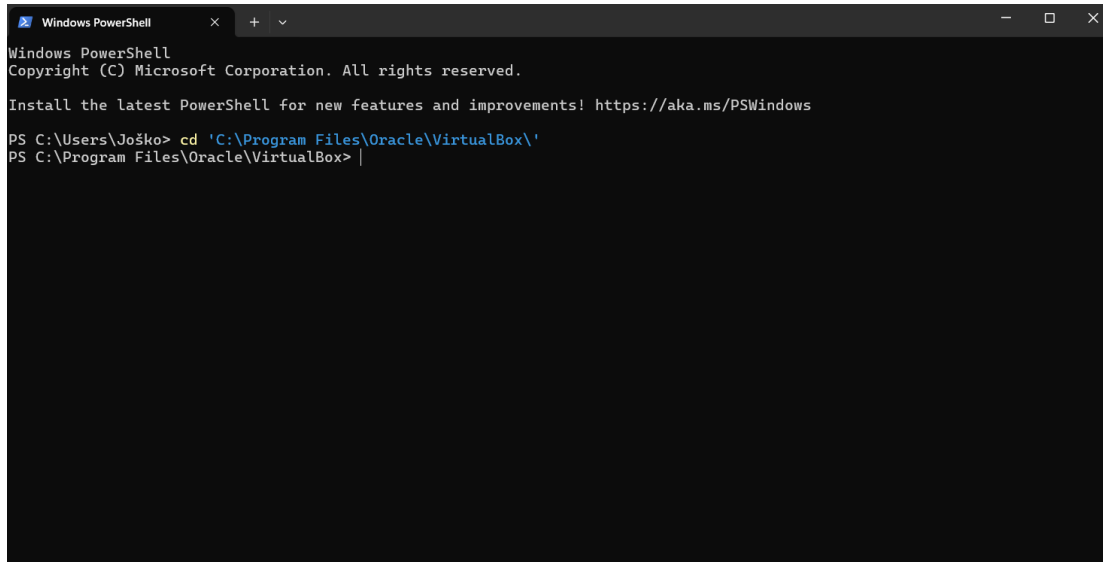
Spremni smo za daljnji rad.

3 Kreiranje VMDK datoteke

Otvorimo terminal kao administrator.

Pozicioniramo se u naše mjesto instalacije VirtualBox-a: *cd '/path/to/Oracle/Virtualbox'*

U našem slučaju je to bilo: *cd 'C:\Program Files\Oracle\VirtualBox\'*



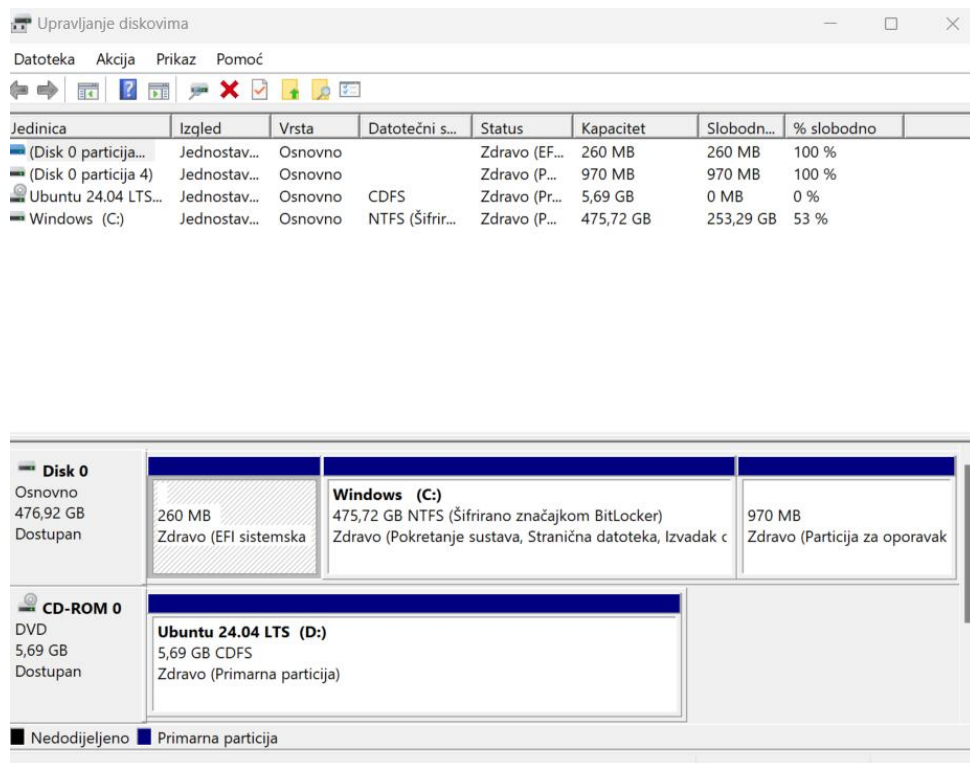
Slika 3-1 Windows PowerShell

Upišemo naredbu za kreiranje VMDK datoteke gdje ćemo kreirati datoteku našeg diska koju ćemo ukomponirati u virtualnu mašinu. Na taj način ćemo u mašinu učitavati naš fizički disk, a ne virtualni.

Naredba je sljedeća: *& "C:\Program Files\Oracle\VirtualBox\VBxManage.exe" internalcommands createrawvmdk -filename "C:\Users\Joško\MyRawDiskVM.vmdk" -rawdisk [\\.\PhysicalDrive0](#)*

Pokrenemo VBxManage naredbu te odaberemo mjesto gdje će se naša datoteka spremiti. Kod nas se sprema u *"C:\Users\Joško\MyRawDiskVM.vmdk"*. Također ukomponiramo i ime našeg diska: *PhysicalDrive0* kao *MyRawDiskVM.vmdk*

Pomoću *Windows Key + X* -> *Upravljanje Diskom* pogledamo ime diska (Disk 0).



Slika 3-2 Disc Management

Zatim kliknemo tipku *Enter* i sačekamo da nam se datoteka stvori.

MyRawDiskVM

4.7.2024. 22:08

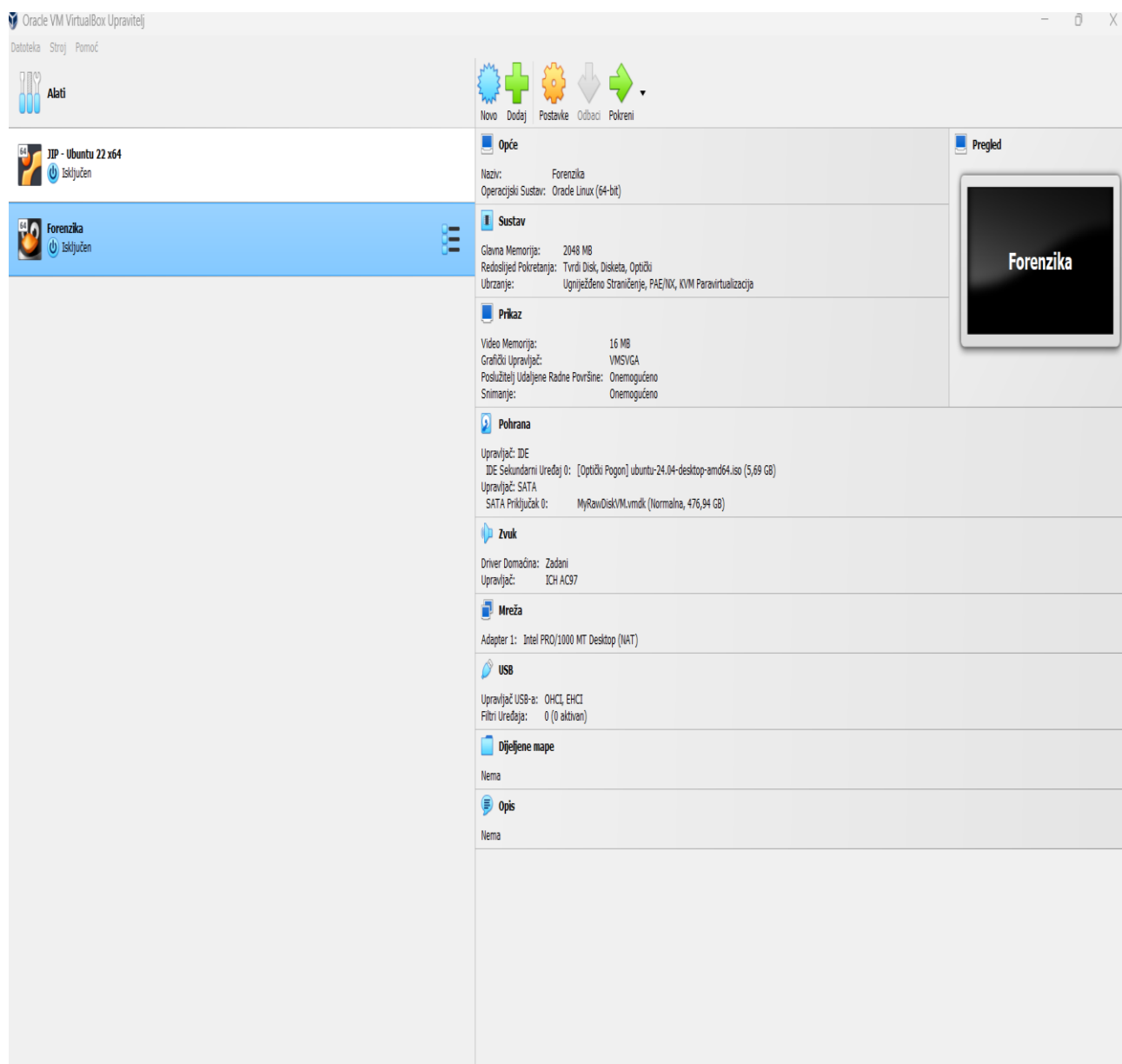
Virtual Machine Di...

1 KB

Slika 3-3 VMDK datoteka

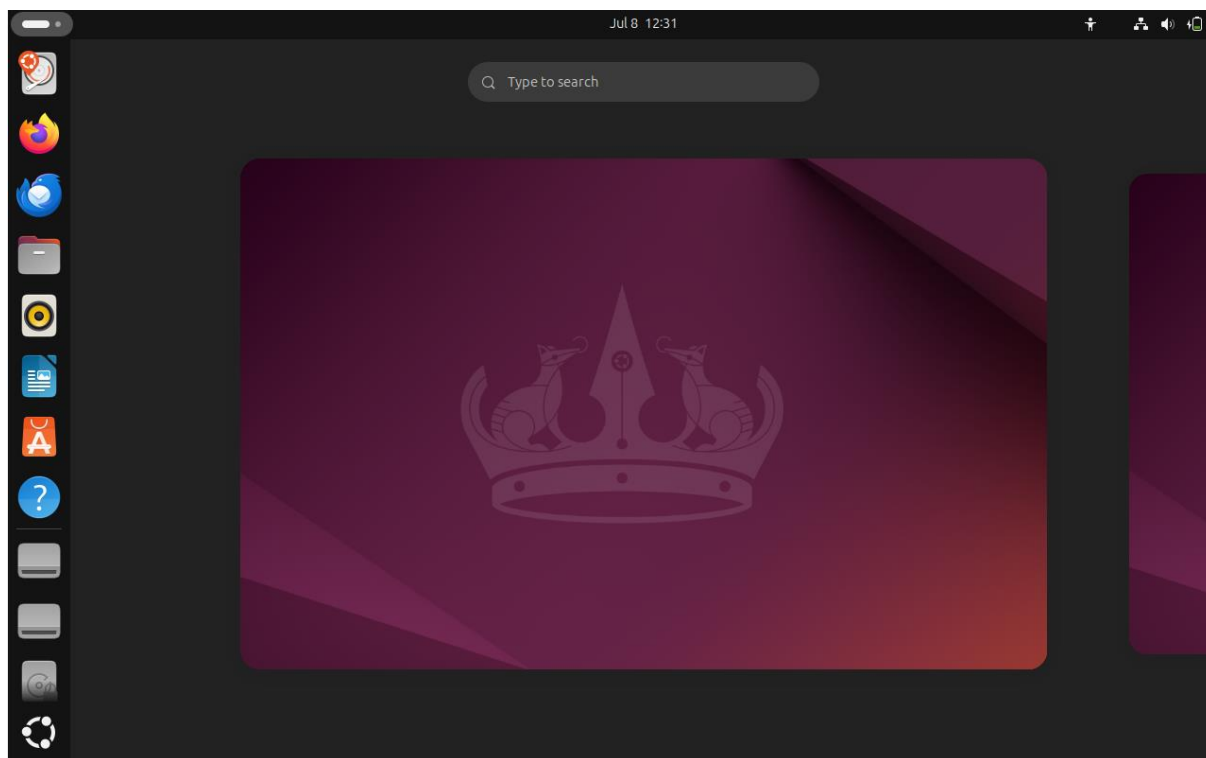
4 Kreiranje virtualne mašine

Otvorimo kao administrator aplikaciju Oracle VM VirtualBox. Kliknemo na *Novo*. Time smo omogućili kreiranje nove virtualne mašine. Odaberemo ime, npr: *Forenzika*. Odaberemo OS koji ćemo koristiti, npr: *Linux*. Na SATA priključak 0 umjesto virtualnog diska mi odaberemo naš disk, odnosno našu vmdk datoteku: *MyRawDiskVM.vmdk*. Kao optički pogon, odnosno OS ćemo instalirati Linux ISO file Ubuntu sa interneta (https://www.linuxlookup.com/linux_iso) i odabrati ga kao zadani optički pogon. Kliknemo završi. U postavkama *Sustav* ćemo staviti da nam se tvrdi disk učitava prvi. Nužno je da bude među prva tri.



Slika 4-1 Forenzika virtualna mašina

Pokrenemo virtualnu mašinu klikom na pokreni.



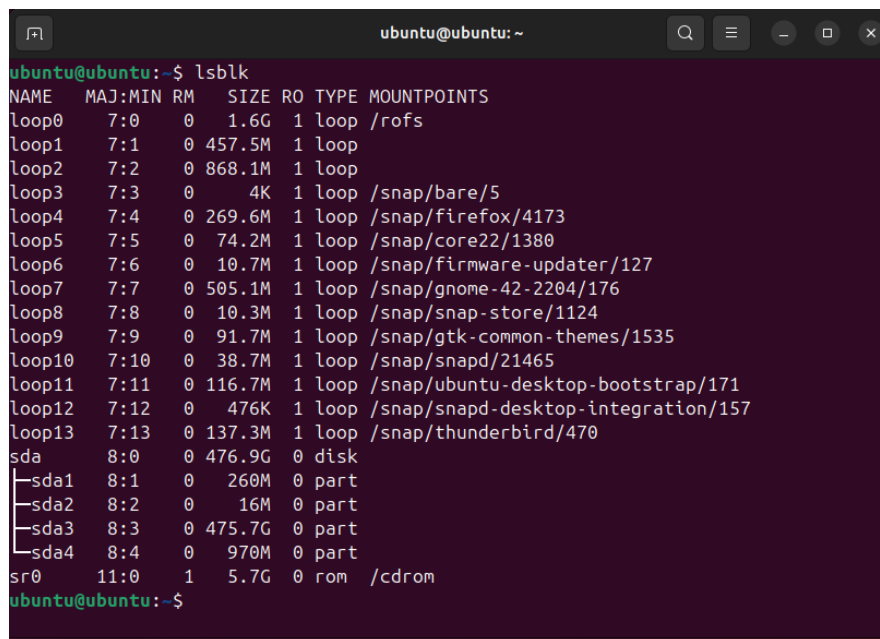
Slika 4-2 Sučelje Forenzika VM-a

5 Analiza hard diska

Nakon uspješnog učitavanja VM-a, odradit ćemo jednostavnu analizu datoteka s jedne particije diska.

Desni klik -> Terminal

Utipkamo naredbu **lsblk** za izlistavanje datoteka. Tu ćemo naći naš diska imenovan kao *sdx*, odnosno u našem slučaju je *sda* s pripadajućim particijama.



```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ lsblk  
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS  
loop0       7:0      0   1.6G  1 loop /rofs  
loop1       7:1      0  457.5M  1 loop  
loop2       7:2      0  868.1M  1 loop  
loop3       7:3      0     4K  1 loop /snap/bare/5  
loop4       7:4      0  269.6M  1 loop /snap/firefox/4173  
loop5       7:5      0   74.2M  1 loop /snap/core22/1380  
loop6       7:6      0   10.7M  1 loop /snap/firmware-updater/127  
loop7       7:7      0  505.1M  1 loop /snap/gnome-42-2204/176  
loop8       7:8      0   10.3M  1 loop /snap/snap-store/1124  
loop9       7:9      0   91.7M  1 loop /snap/gtk-common-themes/1535  
loop10      7:10     0   38.7M  1 loop /snap/snapd/21465  
loop11      7:11     0  116.7M  1 loop /snap/ubuntu-desktop-bootstrap/171  
loop12      7:12     0   476K  1 loop /snap/snapd-desktop-integration/157  
loop13      7:13     0  137.3M  1 loop /snap/thunderbird/470  
sda         8:0      0  476.9G  0 disk  
├─sda1      8:1      0   260M  0 part  
├─sda2      8:2      0    16M  0 part  
├─sda3      8:3      0  475.7G  0 part  
└─sda4      8:4      0   970M  0 part  
sr0        11:0     1    5.7G  0 rom  /cdrom  
ubuntu@ubuntu:~$
```

Slika 5-1 lsblk naredba

Želimo mount-at našu particiju diska *sda1* na neki direktorij. Prvo stvaramo direktorij pomoću naredbe:

sudo mkdir /mnt/forensic

Zatim mount-amo našu particiju *sda1* na taj direktorij pomoću naredbe:

sudo mount -o ro /dev/sda1 /mnt/forensic

Omogućit ćemo samo čitanje datoteka pomoću *ro* (*read only*).

Pozicioniramo se unutar */mnt/forensic*.

Izlistamo sve datoteke unutar tog direktorija pomoću naredbe: **ls -la /mnt/forensic**

```
ubuntu@ubuntu: /mnt/forensic
loop9    7:9      0  91.7M  1 loop  /snap/gtk-common-themes/1535
loop10   7:10     0  38.7M  1 loop  /snap/snapd/21465
loop11   7:11     0 116.7M  1 loop  /snap/ubuntu-desktop-bootstrap/171
loop12   7:12     0   476K  1 loop  /snap/snapd-desktop-integration/157
loop13   7:13     0 137.3M  1 loop  /snap/thunderbird/470
sda      8:0      0 476.9G  0 disk
├─sda1    8:1      0   260M  0 part
├─sda2    8:2      0    16M  0 part
├─sda3    8:3      0 475.7G  0 part
└─sda4    8:4      0   970M  0 part
sr0      11:0     1   5.7G  0 rom   /cdrom
ubuntu@ubuntu:~$ sudo mkdir mnt/forensic
mkdir: cannot create directory 'mnt/forensic': No such file or directory
ubuntu@ubuntu:~$ sudo mkdir /mnt/forensic
ubuntu@ubuntu:~$ sudo mount -o ro /dev/sda1 /mnt/forensic/
ubuntu@ubuntu:~$ cd /mnt/forensic/
ubuntu@ubuntu:/mnt/forensic$ ls -la /mnt/forensic
total 12
drwxr-xr-x 4 root root 4096 Jan  1  1970 .
drwxr-xr-x 1 root root   60 Jul  8 12:39 ..
drwxr-xr-x 5 root root 4096 Jun 19 09:56 EFI
-rwxr-xr-x 1 root root    0 Feb 25  2023 SYSTEM
drwxr-xr-x 2 root root 4096 Sep 20  2023 'System Volume Information'
ubuntu@ubuntu:/mnt/forensic$
```

Slika 5-2 Naredbe terminala

Recimo da želimo vidjeti sadržaj neke datoteke u direktoriju *EFI*.

S naredbom **cd EFI** ulazimo u EFI direktorij. Izlistamo sadržaj s naredbom **ls**. Vidimo da EFI sadrži *Boot*, *HP*, *Microsoft* direktorije. Ulazimo s **cd Boot** u *Boot* direktorij. S **ls** izlistamo sadržaj *Boot-a*. Imamo file *bootx64.efi* kojem ćemo pogledati sadržaj.

S naredbom **cat /mnt/forensic/EFI/Boot/bootx64.efi** izlistamo sadržaj i dobijemo:

```
ubuntu@ubuntu: /mnt/forensic/EFI/Boot
000000|1|F00Y00q,0vE00]0`z0.p10
0 UUS10U
Washington10URedmond10U
M10He00J00C*0He00ation1&0$UMicrosoft Time-Stamp PCA 201030]W00000
H0I 00wy0000W@0Q0040
f0ai~0000
/10000000000 a0-0e00x00{G0Y70@00iQ0000Z01cf0000000-0|1
0 UUS10U
Washington10URedmond10U
Microsoft Corporation1&0$UMicrosoft Time-Stamp PCA 201030]W00000" 0j<v00qjvo0+000
0
[*0H00[s
0U-P0@F00000007w0000#P P00040\T}000i\;H0400u0K0?0000000~,000Y5V0
000000b 00$
00
Hw00"0Qj0?.7000P0Z~t0300
D00\Z00z0W000<' .0gV00000
000rU00nQ0900000=0n000 000"0Z0_70nweh0b0
Rc0u8:9^L00i00V0CM000qt80q0P0
0Y0zi0q0xz0Z000m0E000I[*000?1tT+0oS0).0u0B0000J0(G0R(0ad0000"t00q00I000Y0f/900f
000 0N"00;00t0005izNH00I00|600
00J0s9,MT0000Âj0000IH00
$3000}=00s0p0+00J000?00t00G000j00M00"*000W00A0000DC0*000^0dM0ufGu+0w000J0p00000Q
j00ubuntu@ubuntu: /mnt/forensic/EFI/Boot$
```

Slika 5-3 Sadržaj bootx64.efi datoteke

Izlistali smo sadržaj bootx64.efi datoteke. Dobili smo znakove, odnosno podatke koji se tiču samog pokretanja laptopa.

Kada smo gotovi s pregledavanjem, pozicioniramo se skroz na početak. Za sigurno odvajanje particije diska *sda1* od direktorija */mnt/forensic/* koristimo naredbu: **sudo umount /mnt/forensic.**

Ovo je bio jedan jednostavan primjer inspektiranja datoteka hard diska pomoću VirtualBox-a.

6 Zaključak

U konačnici, Oracle VM VirtualBox se nameće kao neizostavan alat za sve koji trebaju robustno i svestrano rješenje za virtualizaciju. Njegova kombinacija snažnih značajki, fleksibilnosti, pristupačnosti i podrške zajednice čini ga idealnim izborom za širok spektar primjena. Bilo da se koristi za razvoj softvera, testiranje novih aplikacija ili upravljanje IT infrastrukturom, VirtualBox pruža pouzdano i učinkovito rješenje za sve potrebe virtualizacije.

Na jednostavan način smo vidjeli kako se hard disk može analizirati putem virtualne mašine, odnosno VirtualBox-a. Mi smo prikazali samo djelić analize diska i to onaj najjednostavniji, dok se mogu s VM-om vršiti i ostale napredne analize. Virtualne mašine često koriste forenzičari kako bi pokrenuli hard diskove, usb-ove, te razne druge aplikacije u kontroliranom okruženju.

Sažetak i ključne riječi

Sažetak

U ovom radu prikizano je učitavanje hard diska putem virtualne mašine pomoću VirtualBox Oracle aplikacije. Na jednostavan način se kreirala mašina, kao i VMDK datoteka, te se zajedno s Ubuntu Linux ISO datotekom učitala u virtualnu mašinu imena Forenzika. Dalje smo vršili analizu particije diska pomoću različitih naredbi koje smo upisali u terminal.

Ključne riječi

Virtualizacija, VirtualBox, hard disk, Linux, analiza, datoteke