<CSI>Digitalna forenzika</CSI>

<case>predavanja</case>

<evidence>Forenzika UNIX/Linux OS-a</evidence>

Ph.D. Jasmin Azemović
University „Džemal Bijedić“ Mostar
Faculty of Information Technology
YouTube: http://www.youtube.com/mvpdba

Summary

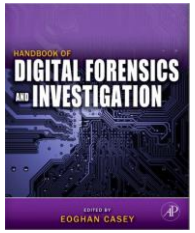
- Uvod
- Osnove
- Korisničke aktivnosti

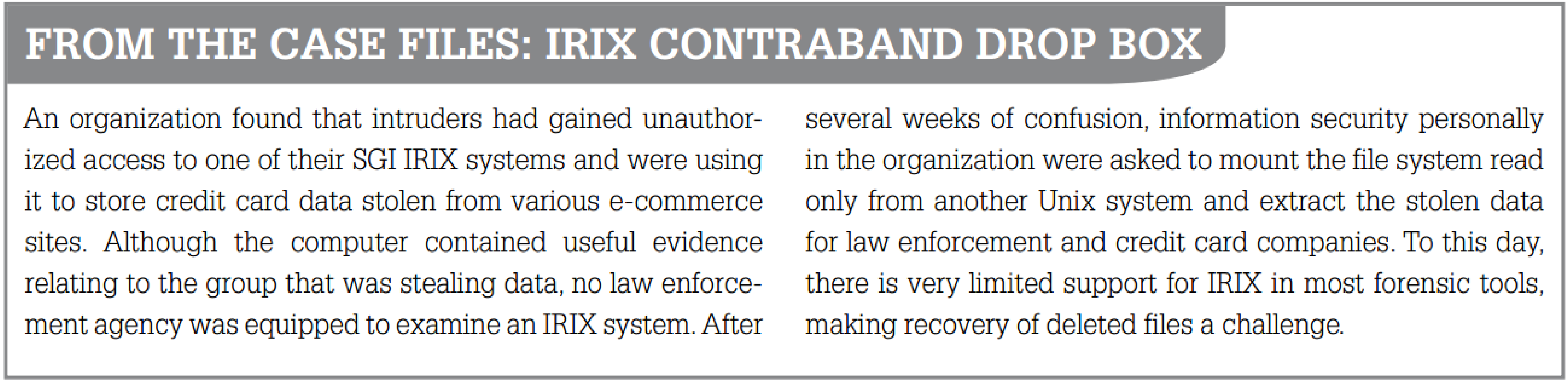
Uvod

- UNIX je razvijene kasnih 60‘tih unutar Bell Labs
- Prihvaćen od stane akademske zajednice 70‘tih koja nastavlja njegov razvoj koji je kasnije nazvan BSD-lite, preteća BSD-a
- AT&T nastavlja razvoj komercijalne verzije UNIX System V
- Linus Torwalds pravi besplatni Unix klon za Intel 386 pod nazivom GNU/Linux
- Danas postoji mnogo različih verzija
  - UNIX
  - UNIX Like
  - Linux
  - BSD
- ..operativnih sistema
- Sigurno da predstavlja izazov za forenziku

LIVE FREE OR DIE
http://www.UNIX-systems.org
UNIX®
UNIX is a Registered Trademark of The Open Group

Primjer





FROM THE CASE FILES: IRIX CONTRABAND DROP BOX

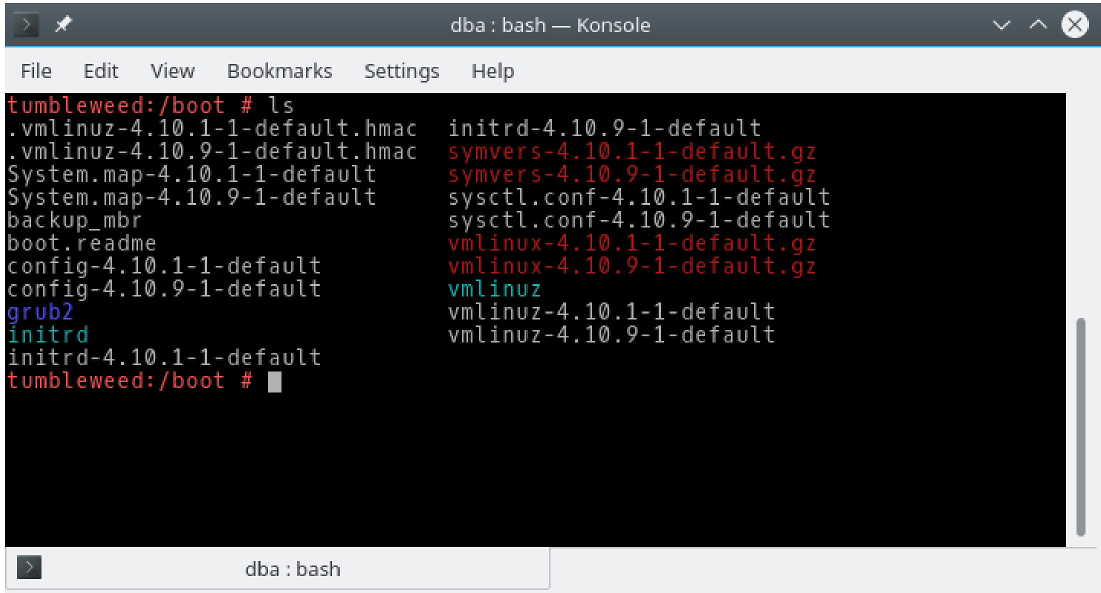
An organization found that intruders had gained unauthorized access to one of their SGI IRIX systems and were using it to store credit card data stolen from various e-commerce sites. Although the computer contained useful evidence relating to the group that was stealing data, no law enforcement agency was equipped to examine an IRIX system. After several weeks of confusion, information security personally in the organization were asked to mount the file system read only from another Unix system and extract the stolen data for law enforcement and credit card companies. To this day, there is very limited support for IRIX in most forensic tools, making recovery of deleted files a challenge.

Lekcija 1. Osnove

- Boot proces
- Fajl sistem
- Lokacija fajlova
- Struktura direktorija

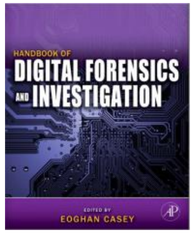
Boot proces

- Za istražitelja je vrlo važno da razumije UNIX/Linux startup proces
- Proces
  - BIOS provjera
  - Učitavanje bootloader koda iz MBR
  - Pronalaženje i učitavanje kernela **/boot** direktorij pod PID 1 (init)
  - Inicijalizacija ramdisk modula



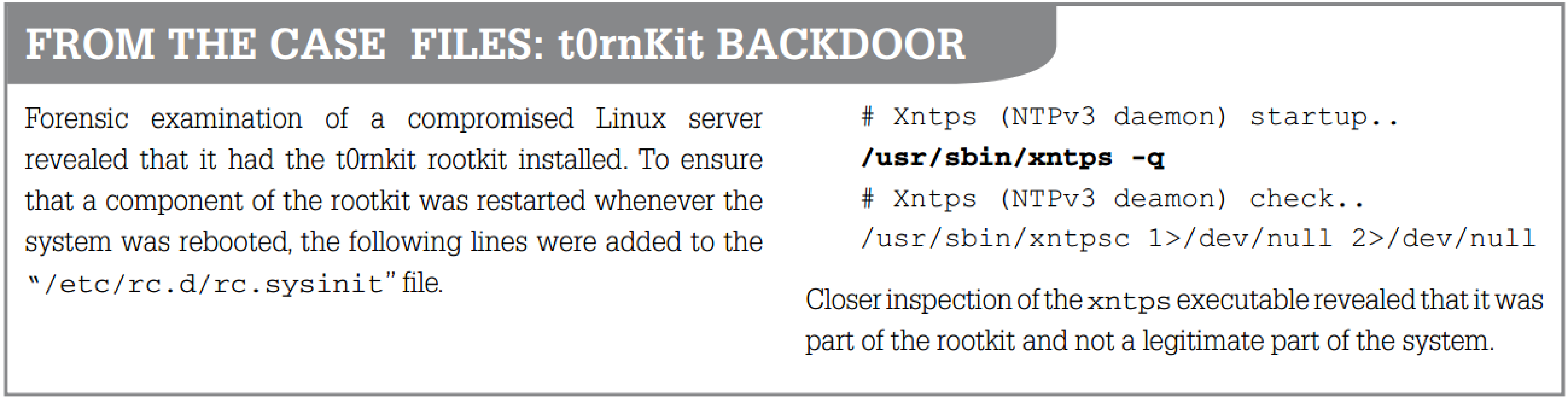
```
tumbleweed:/boot # ls
.vmlinuz-4.10.1-1-default.hmac  initrd-4.10.9-1-default
.vmlinuz-4.10.9-1-default.hmac  symvers-4.10.1-1-default.gz
System.map-4.10.1-1-default     symvers-4.10.9-1-default.gz
System.map-4.10.9-1-default     sysctl.conf-4.10.1-1-default
backup_mbr                      sysctl.conf-4.10.9-1-default
boot.readme                     vmlinux-4.10.1-1-default.gz
config-4.10.1-1-default         vmlinux-4.10.9-1-default.gz
config-4.10.9-1-default         vmlinuz
grub2                           vmlinuz-4.10.1-1-default
initrd                          vmlinuz-4.10.9-1-default
initrd-4.10.1-1-default
tumbleweed:/boot #
```

Primjer



HANDBOOK OF DIGITAL FORENSICS AND INVESTIGATION

EDITED BY EOGHAN CASEY



FROM THE CASE FILES: t0rnKit BACKDOOR

Forensic examination of a compromised Linux server revealed that it had the t0rnkit rootkit installed. To ensure that a component of the rootkit was restarted whenever the system was rebooted, the following lines were added to the "`/etc/rc.d/rc.sysinit`" file.

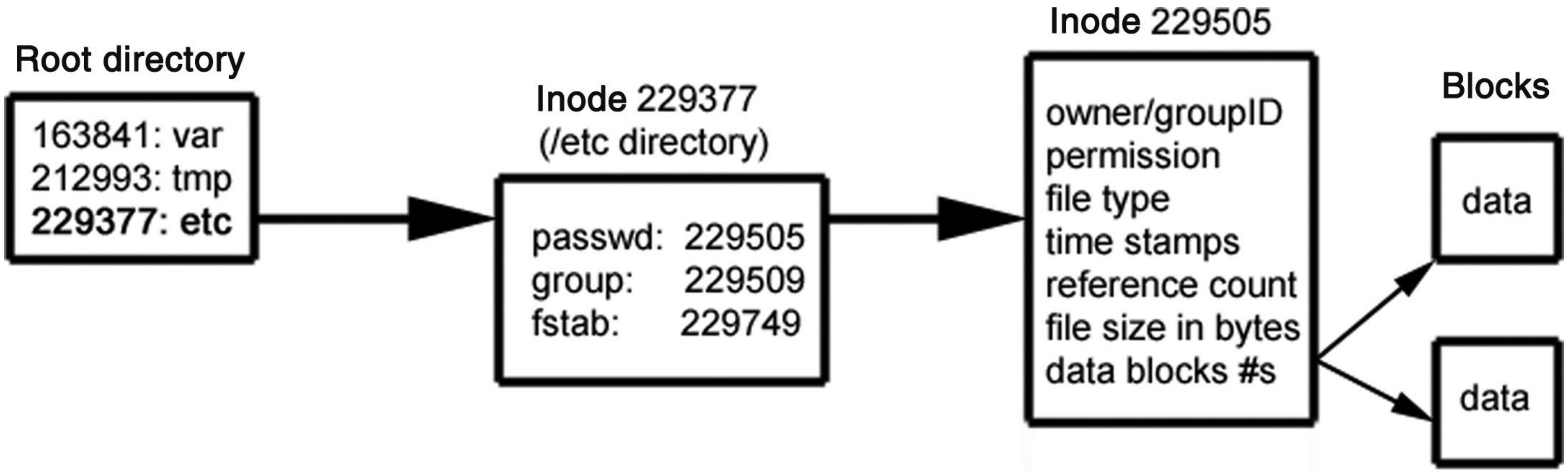
```
# Xntps (NTPv3 daemon) startup..
/usr/sbin/xntps -q
# Xntps (NTPv3 deamon) check..
/usr/sbin/xntpsc 1>/dev/null 2>/dev/null
```

Closer inspection of the `xntps` executable revealed that it was part of the rootkit and not a legitimate part of the system.

Fajl sistem

- Linux uglavnom radi sa ext3 fajl sistemom koji je kompatibilan sa ext2
- Ispravno razumijevanje njegove strukture je važno iz ugla pronalaženja podataka i metapodataka o korisničkim aktivnostima
- Koristimo uglavnom iste forenzičke alate analizu
- Prikupljanje podataka se može razlikovati
  - Posebno ako se radi o LVM
- Komanda **fdisk –l** pomaže oko provjere LMV
- Komada dd kopira sadržaj particje i/ili diska

Lokacija fajlova



Root directory

163841: var
212993: tmp
229377: etc

Inode 229377
(/etc directory)

passwd: 229505
group: 229509
fstab: 229749

Inode 229505

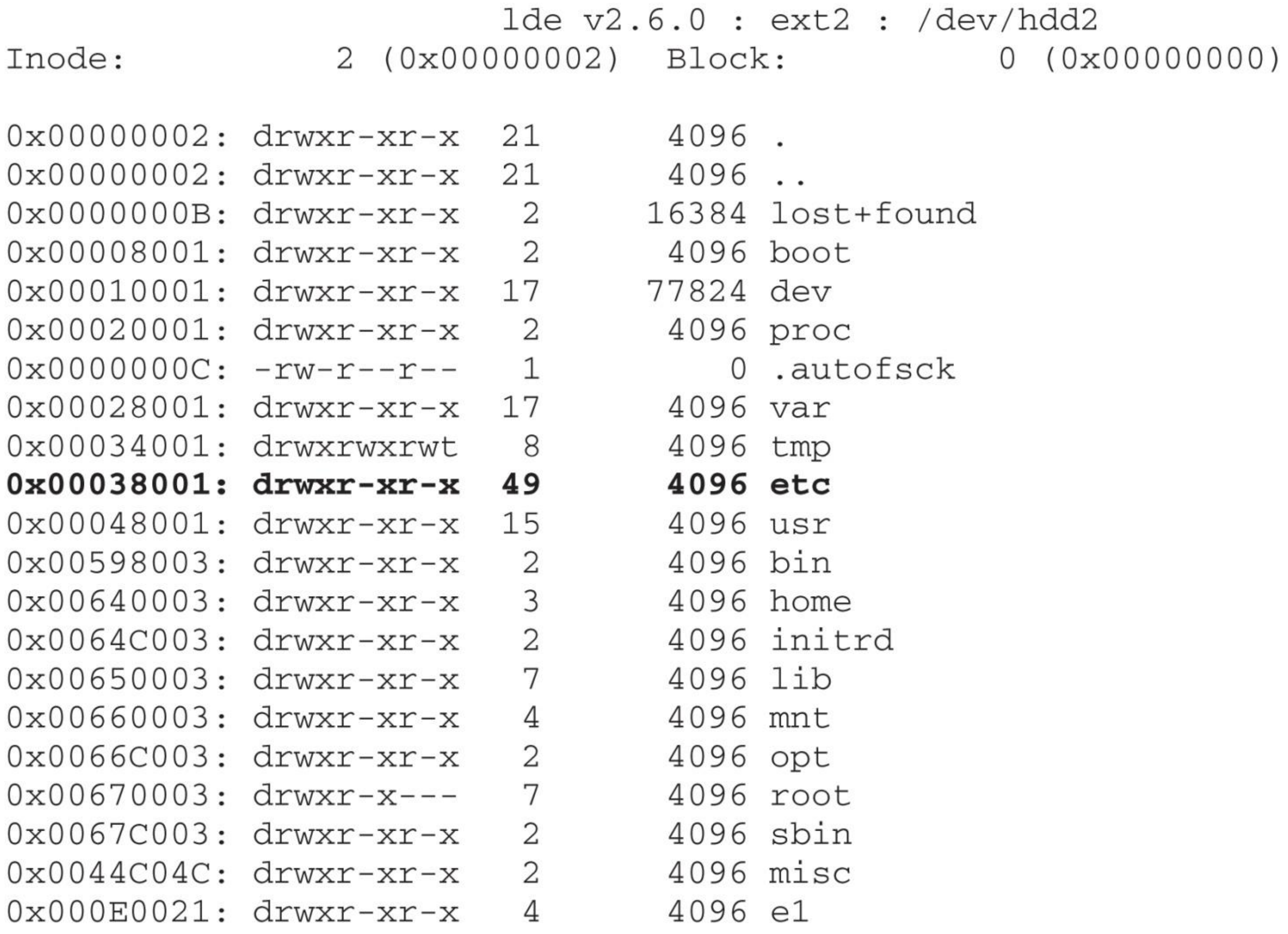
owner/groupID
permission
file type
time stamps
reference count
file size in bytes
data blocks #s

Blocks

data

data

Struktura direktorija



```
                              lde v2.6.0 : ext2 : /dev/hdd2
Inode:           2 (0x00000002)  Block:          0 (0x00000000)

0x00000002: drwxr-xr-x  21      4096 .
0x00000002: drwxr-xr-x  21      4096 ..
0x0000000B: drwxr-xr-x   2     16384 lost+found
0x00008001: drwxr-xr-x   2      4096 boot
0x00010001: drwxr-xr-x  17     77824 dev
0x00020001: drwxr-xr-x   2      4096 proc
0x0000000C: -rw-r--r--   1         0 .autofsck
0x00028001: drwxr-xr-x  17      4096 var
0x00034001: drwxrwxrwt   8      4096 tmp
0x00038001: drwxr-xr-x  49      4096 etc
0x00048001: drwxr-xr-x  15      4096 usr
0x00598003: drwxr-xr-x   2      4096 bin
0x00640003: drwxr-xr-x   3      4096 home
0x0064C003: drwxr-xr-x   2      4096 initrd
0x00650003: drwxr-xr-x   7      4096 lib
0x00660003: drwxr-xr-x   4      4096 mnt
0x0066C003: drwxr-xr-x   2      4096 opt
0x00670003: drwxr-x---   7      4096 root
0x0067C003: drwxr-xr-x   2      4096 sbin
0x0044C04C: drwxr-xr-x   2      4096 misc
0x000E0021: drwxr-xr-x   4      4096 e1
```

Lekcija 2: Korisničke aktivnosti

- Korisnički nalozi
- Postavke sistema
- Tragovi korisničkih aktivnosti

Korisnički nalozi

- Nalaze se **/usr** direktoriju
- **etc/passwd** sadrži podatke o lozinkama
- Folder može biti enkriptovan
- **/etc/sudoers** podaci o korisnicima sa super privilegijama

Postavke sistema

- Linux nema registri
- Kompletna konfiguracija se nalazi u tekstualnim fajlovima
  - Važi za nivo sistema
  - Pojedine programe ili servise
- Decentralizovan pristup može da oteža proces pronalaženja ključnih dokaza

Tragovi korisničkih aktivnosti

- Sistemski log fajlovi
- Aplikacijski log fajlovi
- Korisnički log fajlovi
- bash_history

Pitanja