Digitalna forenzika

Andrej Brodnik

Operacijski sistem Unix

poglavje 18

- razvoj skozi zgodovino: *System V*, *HP-UX*, *BSD, ...*
- kasneje so se pojavili odprtokodne inačice:
  - Linux: RedHat, SUSE, Ubuntu, ...
  - BSD: FreeBSD, OpenBSD, NetBSD

Standardna datotečna hierarhija

- *Filesystem Hierarchy Standard* – FHS (http://www.pathname.com/fhs/pub/fhs-2.3.html)
- delo prevzela *Linux Foundation* (http://www.linuxfoundation.org/collaborate/workgroups/lsb/fhs)
- večinoma formalizacija BSD datotečnega sistema

Korenski imenik

- */boot : Static files of the boot loader*
- */dev : Device files*
- */etc : Host-specific system configuration*
  - */etc/opt : Configuration files for /opt*
  - */etc/X11 : Configuration for the X Window System (optional)*
  - */etc/sgml : Configuration files for SGML (optional)*
  - */etc/xml : Configuration files for XML (optional)*

- /bin : Essential user command binaries (for use by all users)
- /sbin : System binaries
- /lib : Essential shared libraries and kernel modules
- /lib<qual> : Alternate format essential shared libraries (optional)

Korenski imenik

- */home : User home directories (optional)*
- */root : Home directory for the root user (optional)*
- */media : Mount point for removeable media*
- */mnt : Mount point for a temporarily mounted filesystem*
- */opt : Add-on application software packages*
- */srv : Data for services provided by this system*
- */tmp : Temporary files*
- */usr, /var : Separate hierachies*

/usr imenik

- vsebuje datoteke,ki so namenjene samo branju
- jih uporabljajo hkrati različni sistemi
- v njem naj bi ne bilo datotek, ki so specifične za določen sistem
- izjema: /usr/local, ki je lokalni imenik določenega sistema

/var imenik

- vsebuje datoteke, ki se spreminjajo skozi čas
  - poštne in tiskalniške vrste
  - beležke (*logging*)
  - podatkovja (podatkovne baze ipd.)
  - začasne datoteke

Sistemske datoteke

- operacijski sistem je zasnovan tako, da so sistemske datoteke človeku prijazne ➔ navadne besedilne datoteke
  - konfiguracijske datoteke: hosts, syslog.conf, ...
    - običajno v imeniku etc (/etc, /usr/local/etc, /opt/etc, ...)
  - beležke: mail, cups, ...
    - običajno v imeniku log (/var/log, /usr/local/var/log, /opt/var/log)

Konfiguracijske datoteke

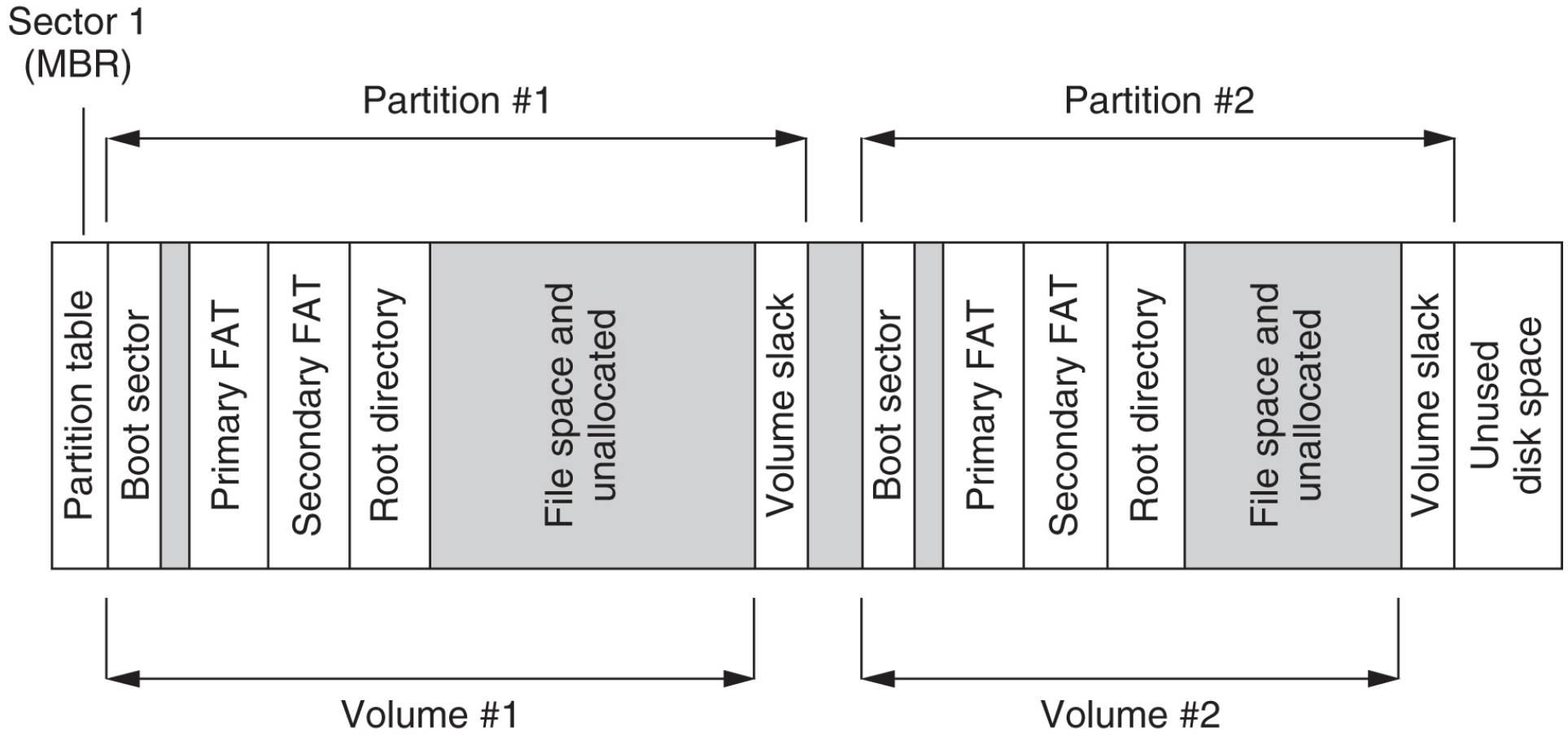
```
# $FreeBSD: release/9.0.0/etc/snmpd.config 216595 2010-12-20 17:28:15Z syrinx $
#
# Example configuration file for bsnmpd(1).
#

#
# Set some common variables
#
location := "Room 200"
contact := "sysmeister@example.com"
system := 1     # FreeBSD
traphost := localhost
trapport := 162

#
# Set the SNMP engine ID.
#
# The snmpEngineID object required from the SNMPv3 Framework. If not explicitly set via
# this configuration file, an ID is assigned based on the value of the
# kern.hostid variable
# engine := 0x80:0x10:0x08:0x10:0x80:0x25
# snmpEngineID = $(engine)
```

Beležke

Mar 8 00:00:00 svarun newsyslog[85254]: logfile turned over
Mar 8 00:00:12 svarun postfix/smtpd[85247]: connect from S0106c0c1c0ddffcf.vf.shawcable.net[70.69.32.154]
Mar 8 00:00:12 svarun postfix/smtpd[85247]: NOQUEUE: reject: RCPT from S0106c0c1c0ddffcf.vf.shawcable.net[70.69.32.154]: 554 5.7.1 Service unavailable; Client host [70.69.32.154] blocked using bl.spamcop.net; Blocked - see http://www.spamcop.net/bl.shtml?70.69.32.154; from=<unscrupulousnessiw2@deltamar.net> to=<xxxx@brodnik.org> proto=ESMTP helo=<deltamar.net>
Mar 8 00:00:12 svarun postfix/smtpd[85247]: lost connection after DATA from S0106c0c1c0ddffcf.vf.shawcable.net[70.69.32.154]

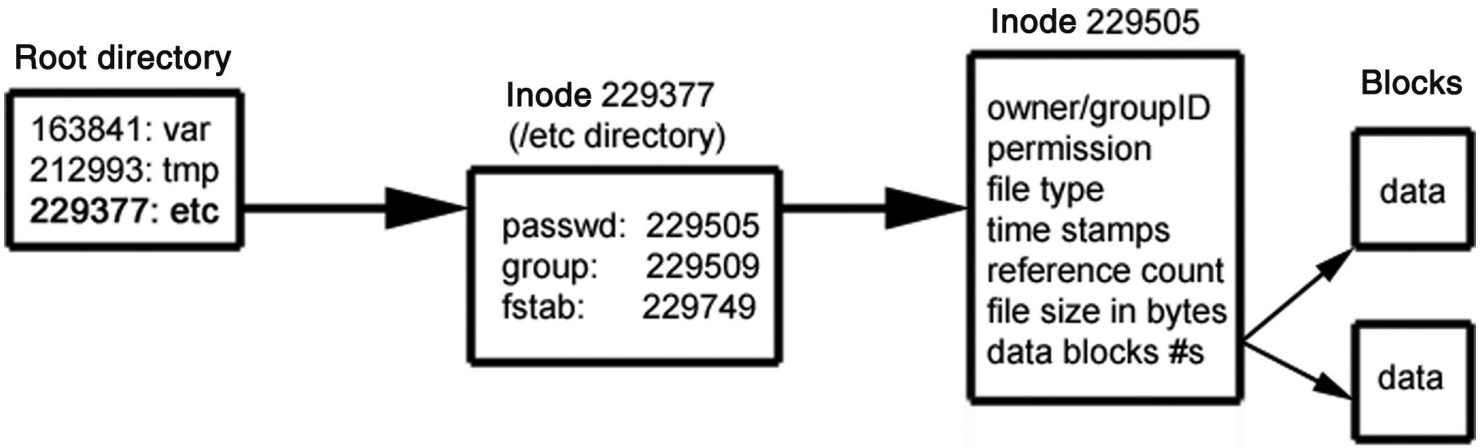
Shramba podatkov in skrivanje

- poenostavljena organiziranost diska z datotečnim sistemom FAT



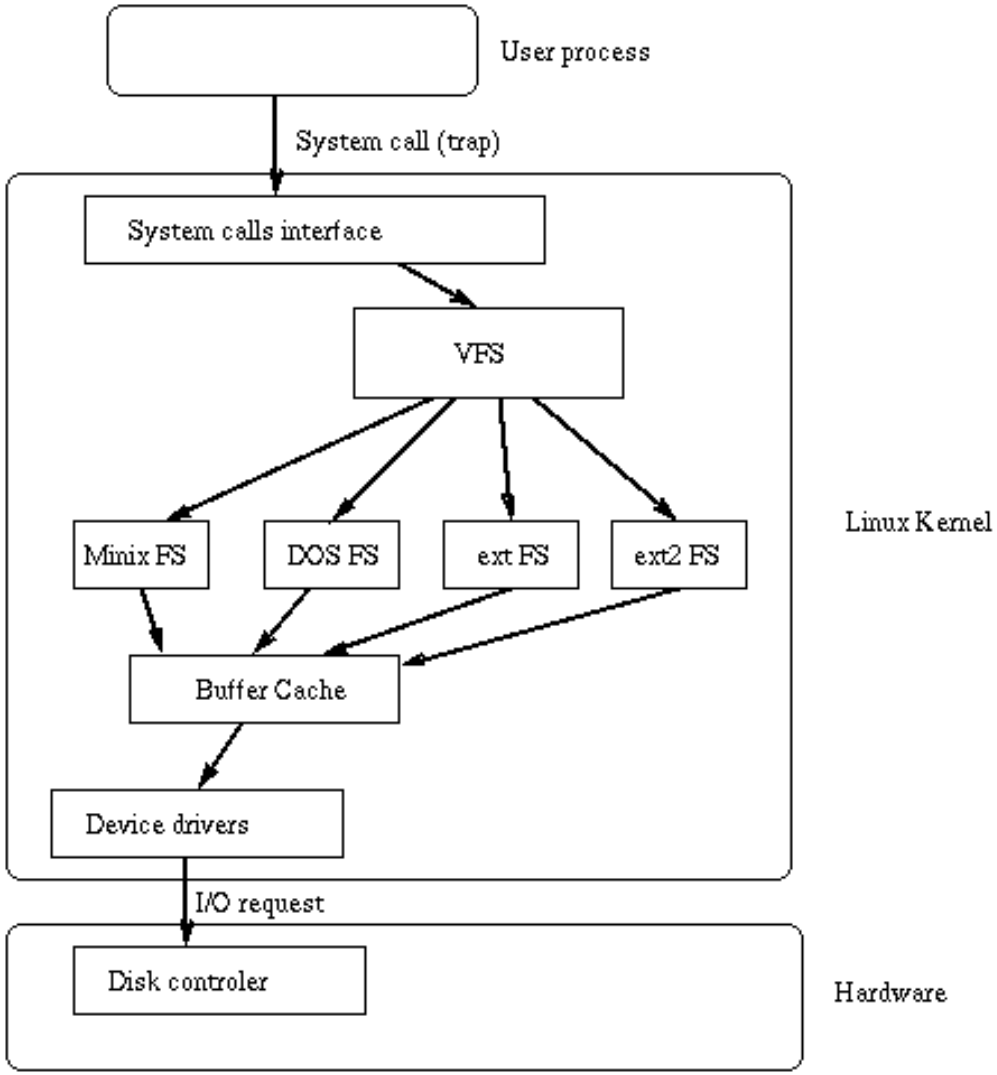
Datotečni sistemi

- imamo imenike in indeksna vozlišča (*inode*)
- inode ima podobno funkcijo kot FAT in MFT hkrati
- imenik je samo posebna oblika datoteke
  - imamo še posebne datoteke: povezave (*links*), cevovode (*pipe*), vtič (*socket*), ...



Datotečni sistemi

- najstarejši: Unix File System – UFS
- mlajša in uporabljena v sistemih Linux: ext2 in ext3
  - obstajata tudi ext in ext4
- obstaja še vrsta drugih datotečnih sistemov



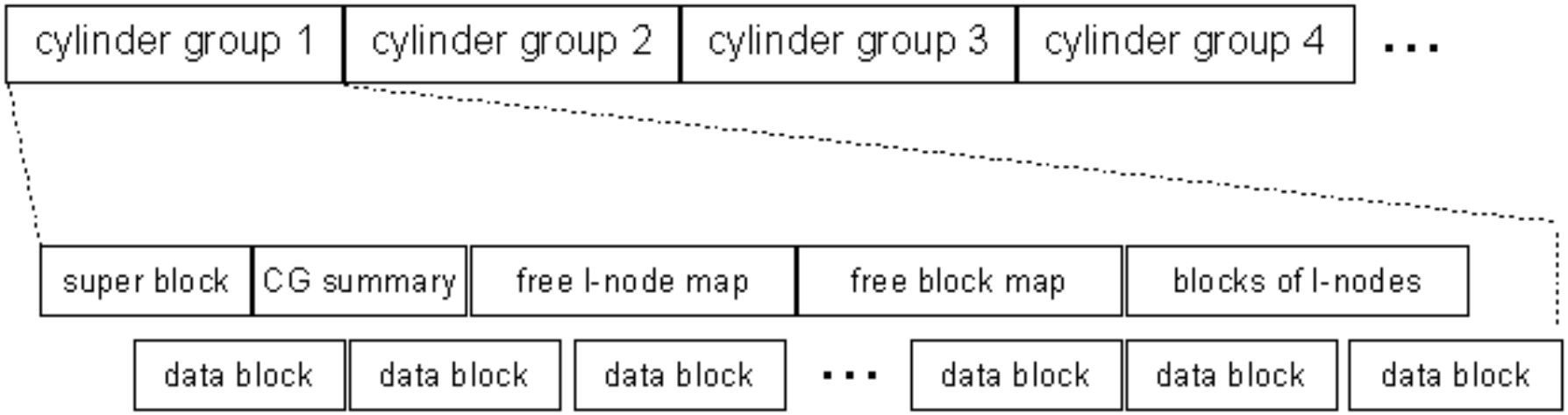
Čas v operacijskem sistemu Unix

- čas se meri v sekundah
- hrani se kot število, ki ima začetek 1. prosinca 1970 – *epoch*
  - če je čas shranjen kot 32-bitno število, bo prišlo do preliva v torek, 19. prosinca 2038 ob 03:14:07 UTC – Y2K38 problem
- UTC – *Coordinate Universal Time*: usklajena definicija časa, ki upošteva prestopna leta, prestopne sekunde, ...
  - zadnja prestopna sekunda se je zgodila 31. grudna 2016
  - usklajen čas med večimi atomskimi urami
  - eden od naslednikov GMT

Datotečni sistemi UFS

- definiran, ko je bil uveden VFS v BSD4.2
- uporabljen v *BSD sistemih
- kasneje uporabljen v Solaris OS

vir: *Solaris Internals, The UFS File System*, Updated by Frank Batschulat, Shawn Debnath, Sarah Jelinek, Dworkin Muller, and Karen Rochford

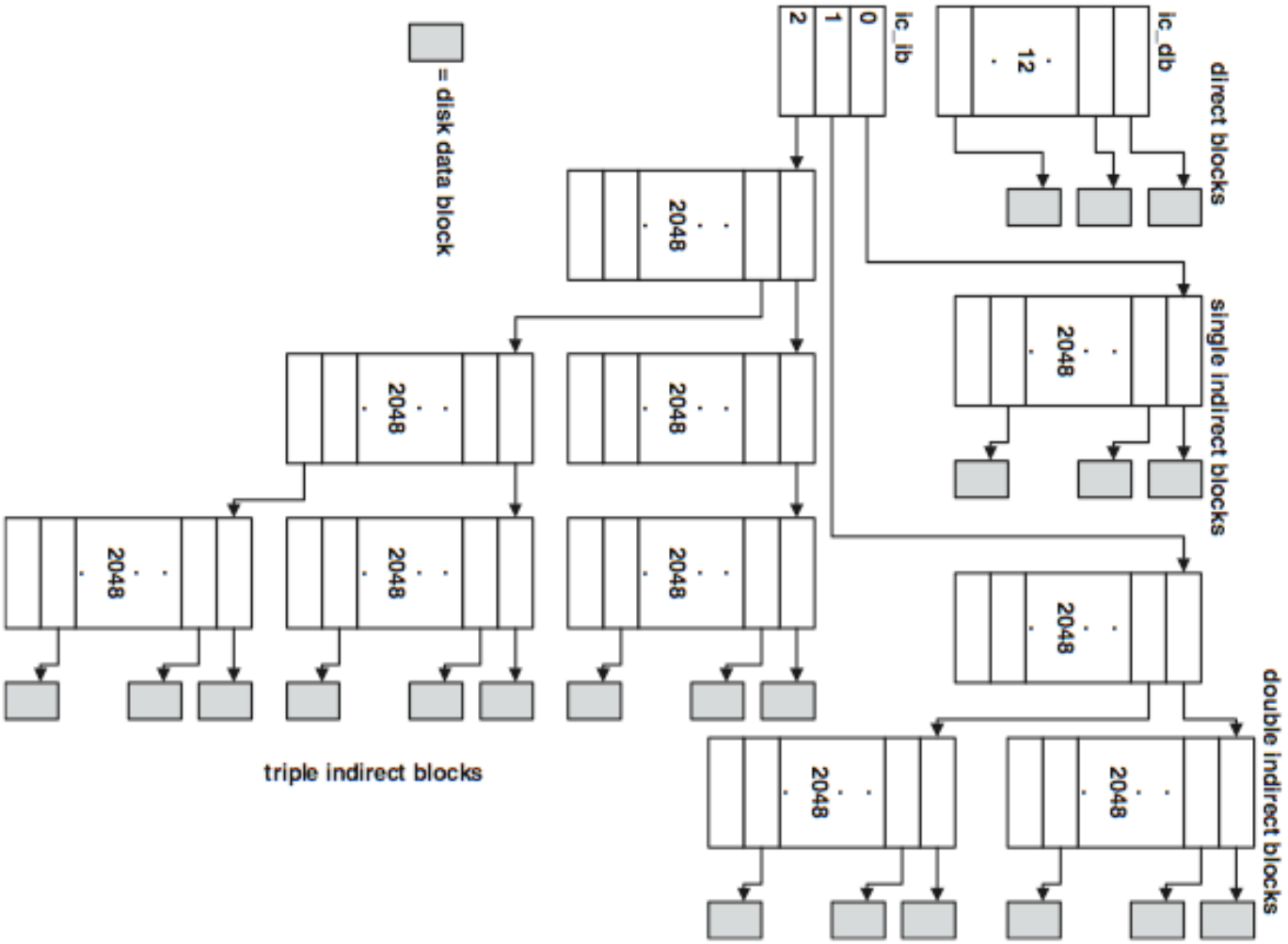


UFS – indeksno vozlišče

```
struct dinode {
  u_int16_t        di_mode;         /*   0: IFMT, permissions; see below. */
  int16_t          di_nlink;        /*   2: File link count. */
  union {
    u_int16_t oldids[2];            /*   4: Ffs: old user and group ids. */
    int32_t   inumber;              /*   4: Lfs: inode number. */
  } di_u;
  u_int64_t        di_size;         /*   8: File byte count. */
  int32_t          di_atime;        /*  16: Last access time. */
  int32_t          di_atimensec;    /*  20: Last access time. */
  int32_t          di_mtime;        /*  24: Last modified time. */
  int32_t          di_mtimensec;    /*  28: Last modified time. */
  int32_t          di_ctime;        /*  32: Last inode change time. */
  int32_t          di_ctimensec;    /*  36: Last inode change time. */
  ufs_daddr_t      di_db[NDADDR];   /*  40: Direct disk blocks. */
  ufs_daddr_t      di_ib[NIADDR];   /*  88: Indirect disk blocks. */
  u_int32_t        di_flags;        /* 100: Status flags (chflags). */
  int32_t          di_blocks;       /* 104: Blocks actually held. */
  int32_t          di_gen;          /* 108: Generation number. */
  u_int32_t        di_uid;          /* 112: File owner. */
  u_int32_t        di_gid;          /* 116: File group. */
  int32_t          di_spare[2];     /* 120: Reserved; currently unused */
}
```

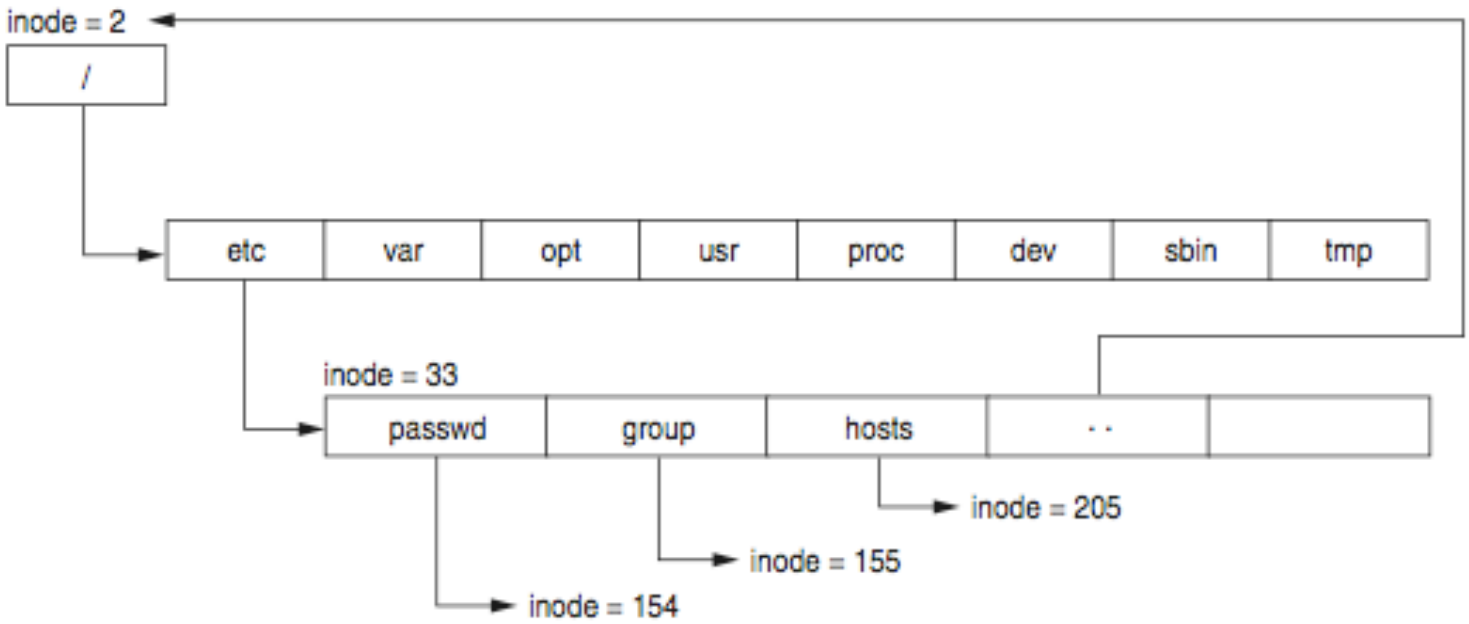
ufs/dinode.h

UFS – datotečni sistemi



UFS – imeniška datoteka

- posebna datoteka, ki sestoji iz delov imenika
- System V je imel predoločeno velikost imenika
- korenski imenik je opisan v inode 2
- vsak imenik ima poseben vnos .., ki pove, kje je starš



UFS – imeniški vnos

```
#define    MAXNAMLEN 255
struct direct {
  u_int32_t d_ino;       /* inode number of entry */
  u_int16_t d_reclen;    /* length of this record */
  u_int8_t  d_type;      /* file type, see below */
  u_int8_t  d_namlen;    /* length of string in d_name */
  char      d_name[MAXNAMLEN + 1];
                         /* name with length <= MAXNAMLEN */
};
```

ufs/dir.h

- *Izziv:* čemu je namenjen zapis reclen? Se to da izkoristiti za skrivanje podatkov?
- *Izziv:* kaj je to ACL? Kako je implementiran pri ufs?

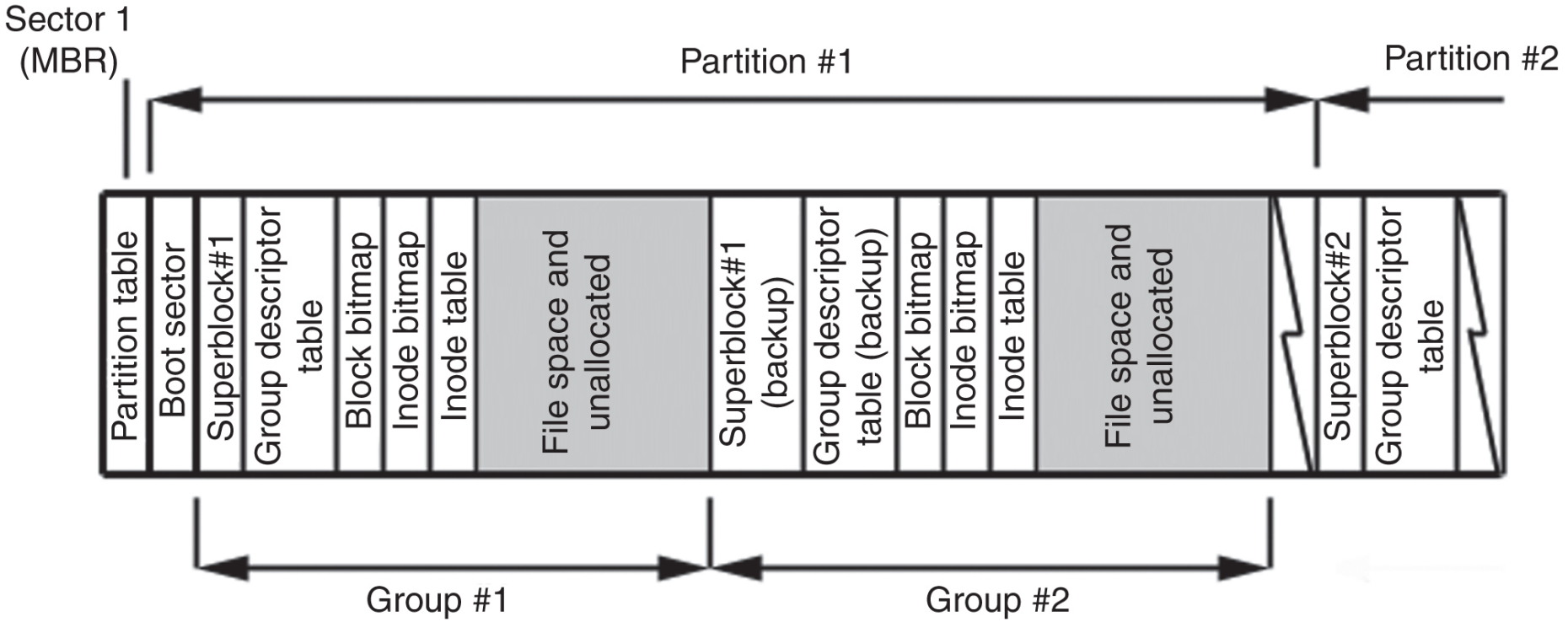
UFS – nadblok

- nadblok (*superblock*) hrani opis konfiguracije skupine cilindrov
- raztreseno po disku – na začetku vsake skupine cilindrov
  - da se ohrani knfiguracija, če se en zapis izgubi
- orodje **`dumpfs`**

- *Izziv:* poiščite strukturo nadbloka. Kako vemo, da imamo opravka z UFS datotečnim sistemom? Kje to piše? Preberite superblock z vašega unix datotečnega sistema in v njem ugotovite, za kateri datotečni sistem gre.

Datotečni sistem ext2

- osnovna struktura podobna kot pri ufs
- namesto skupin cilindrov, govorimo o skupinah blokov
- imeniki in indeksna vozlišča – kot pri UFS



Datotečni sistem ext2

- orodje za pregledovanje diska: Linux Disk Editor (LDE) (http://lde.sourceforge.net/)

```
                                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
```

Datotečni sistem ext2

```
                        lde v2.6.0 : ext2 : /dev/hdd2
Inode:     229505 (0x00038081)  Block:          0 (0x00000000)

-rw-r--r--   1 root     root         1186  Tue Sep 24 08:57:40 2002

TYPE: regular file  LINKS:   1              DIRECT BLOCKS=0x000703F9
MODE: \0644         FLAGS: \10
UID: 00000(root)    GID: 00000(root)
SIZE: 1186          SIZE(BLKS): 8

ACCESS TIME:        Tue Nov 26 11:10:18 2002
CREATION TIME:      Tue Sep 24 08:57:40 2002
MODIFICATION TIME:  Tue Sep 24 08:57:40 2002
DELETION TIME:      Wed Dec 31 19:00:00 1969
```

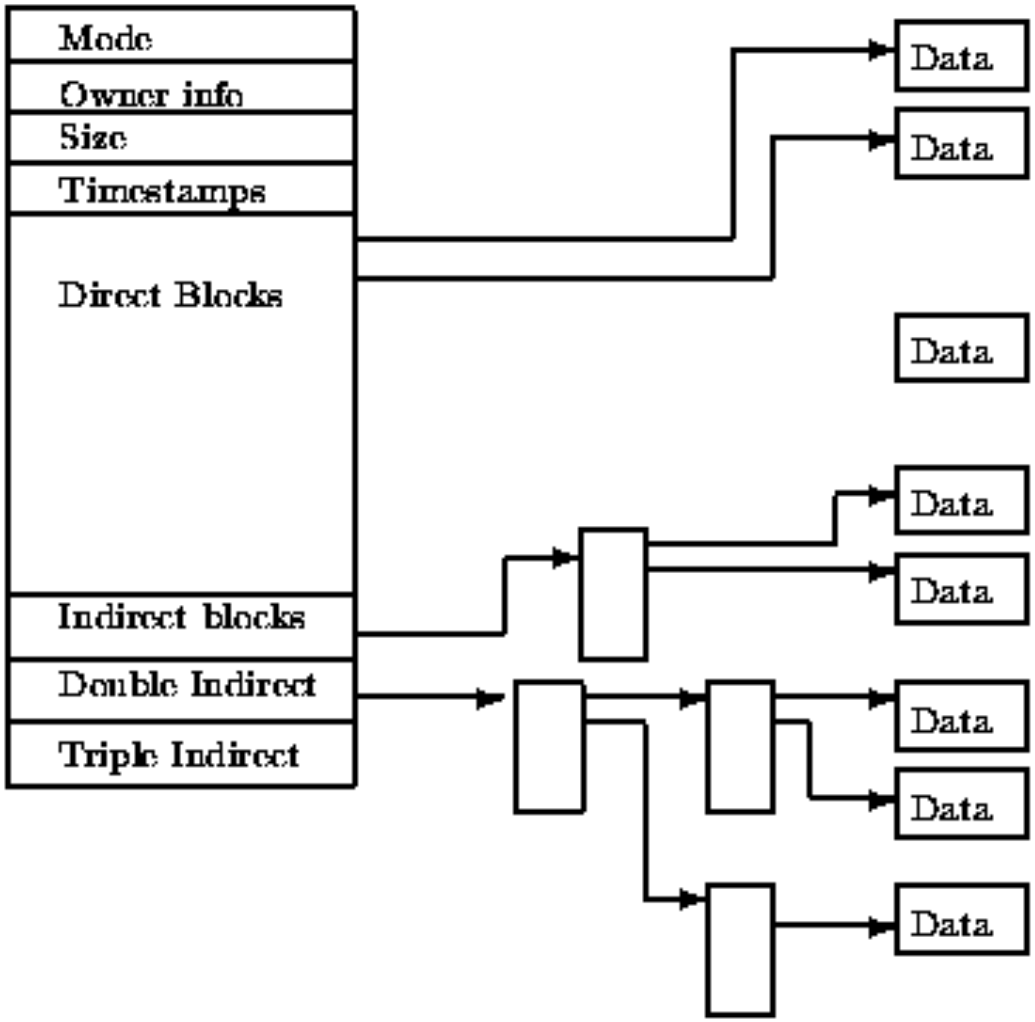
```
INDIRECT BLOCK=
2x INDIRECT BLOCK=
3x INDIRECT BLOCK=
```

ext2 – indeksno vozlišče

```
struct ext2_inode {
   __u16   i_mode;         /*   0: File mode */
   __u16   i_uid;          /*   2: Owner Uid */
   __u32   i_size;         /*   4: Size in bytes */
   __u32   i_atime;        /*   8: Access time */
   __u32   i_ctime;        /*  12: Creation time */
   __u32   i_mtime;        /*  16: Modification time */
   __u32   i_dtime;        /*  20: Deletion Time */
   __u16   i_gid;          /*  24: Group Id */
   __u16   i_links_count;  /*  26: Links count */
   __u32   i_blocks;       /*  28: Blocks count */
   __u32   i_flags;        /*  32: File flags */
   __u32   l_i_reserved1;  /*  36: OS dependent 1 */
   __u32   i_block[EXT2_N_BLOCKS];/* 40: Pointers to blocks */
   __u32   i_generation;   /* 100: File version (for NFS) */
   __u32   i_file_acl;     /* 104: File ACL */
   __u32   i_dir_acl;      /* 108: Directory ACL */
   __u32   i_faddr;        /* 112:  Fragment address */
   __u8    l_i_frag;       /* 116:  Fragment number */
   __u8    l_i_fsize;      /* 117:   Fragment size */
   __u16   i_pad1;         /* 118:   */
   __u32   l_i_reserved2[2]; /* 120: OS dependent 2 */
};
```

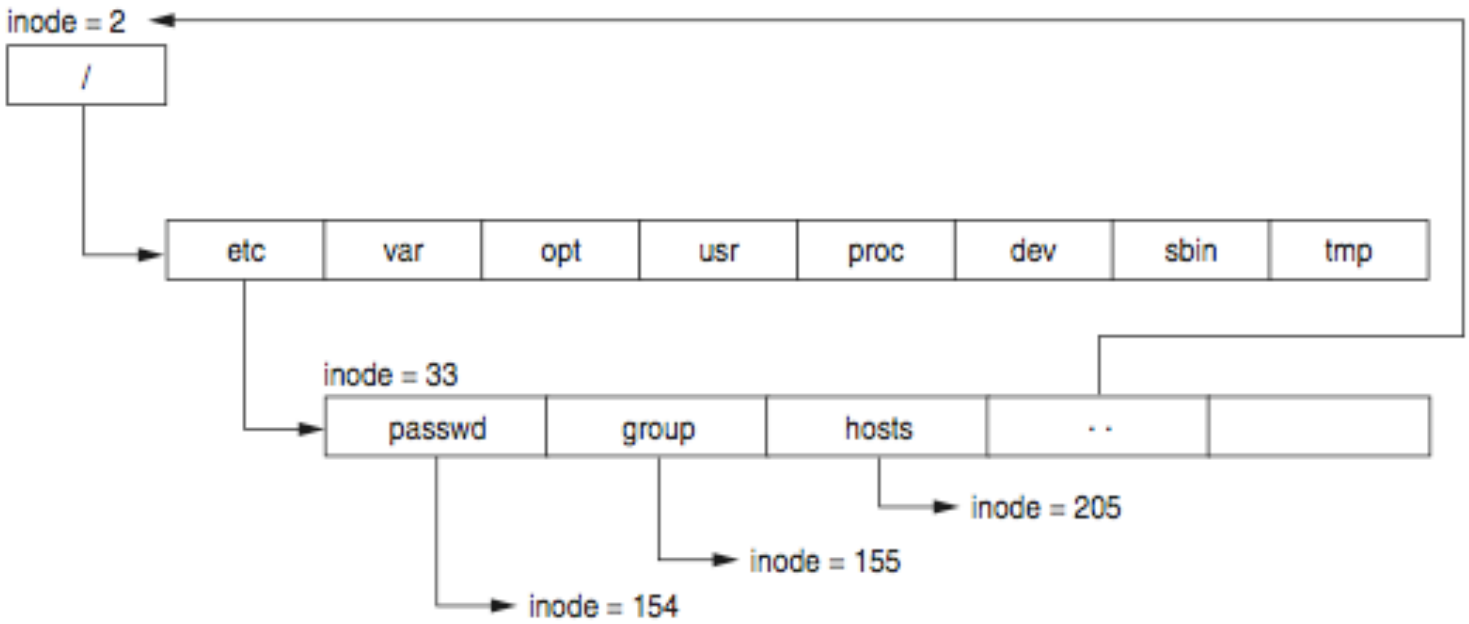
ext2fs/ext2_fs.h

ext2 – indeksno vozlišče



Imeniška datoteka

- posebna datoteka, ki sestoji iz delov imenika
- System V je imel predoločeno velikost imenika
- korenski imenik je opisan v inode 2
- vsak imenik ima poseben vnos .., ki pove, kje je starš



ext2 – imeniški vnos

```
#define    EXT2FS_MAXNAMLEN 255
struct  ext2fs_direct {
  u_int32_t e2d_ino;       /* inode number of entry */
  u_int16_t e2d_reclen;    /* length of this record */
  u_int8_t e2d_namlen;     /* length of string in d_name */
  u_int8_t e2d_type;       /* file type */
  char     e2d_name[EXT2FS_MAXNAMLEN];
                           /* name with length <=
 EXT2FS_MAXNAMLEN */
};
```

ext2fs/ext2fs_dir.h

ext2 – nadblok

- nadblok (*superblock*) hrani opis konfiguracije skupine blokov
- raztreseno po disku – na začetku vsake skupine blokov
  - da se ohrani knfiguracija, če se en zapis izgubi
- orodje **`dumpfs`**

- *Izziv:* poiščite strukturo nadbloka ext2. Primerjajte jo s strukturo UFS superbloka.

Datotečni sistem ext3

- avtor Stephen Tweedie 1999 / 2000 / 2001
- osnovna struktura enaka kot pri datotečnem sistemu ext2
  - razdelitev na skupine blokov vključno z nadblokom (*superblock*)
  - imeniki in indeksna vozlišča
  - vodenje evidence o disku
- dodana je možnost hranjenja dnevniške strukture
- osnovni datotečni sistem OS Linux

Dnevniki ext3

- v dnevnikih se hranijo zapisi o vseh spremembah v datotečnem sistemu
- dnevniška struktura omogoča tri vrste vodenja dnevnika:
  - celovit dnevnik (*journal*): hrani se vse; tako metapodatke kot vsebino – najbolj varno
  - zaporedno (*ordered*): hranijo se samo metapodatki vendar se shranijo po uspešno opravljeni operaciji – srednje varno
  - zapiši (*writeback*): podobno kot zaporedni, le da se shranjujejo dnevniški zapisi hkrati z dejanskimi zapisi – najmanj varno

Dnevniki ext3

- dnevnik je zaporedna datoteka
- zapisi so shranjeni pred prvo skupino blokov
- dnevniška skupina je sestavljena podobno kot bločna skupina:
  - dnevniški nadblok
  - opisi transakcij

Dnevniki ext3

- opis transakcij vsebuje tri vrste blokov:
  - opisni blok (descriptor block): začetek transakcije
  - metadata bloki: opisi transakcije
  - zaključni blok (*commit block*): zaključek transakcije
  - preklicni blok (revoke block): če pride do napake in vsebuje seznam blokov v datotečnem sistemu, ki jih je potrebno ponovno namestiti (restavrirati)
- vsi (tudi nadblok) se prično z magično številko:

  JFS_DESCRIPTOR_BLOCK 1
  JFS_COMMIT_BLOCK 2
  JFS_SUPERBLOCK_V1 3
  JFS_SUPERBLOCK_V2 4
  JFS_REVOKE_BLOCK 5

Dnevniki ext3

- *Izziv:* preučite strukturo nadbloka (npr. http://linuxsoftware.co.nz/wiki/ext3) . Pridobite blok iz svojega datotečnega sistema in komentirajte njegovo vsebino.
- *Izziv:* Kako dobiti nazaj izbrisano datoteko v sistemu ext2 in kako v ext3? Kaj pa v ufs?

Datotečni sistemi

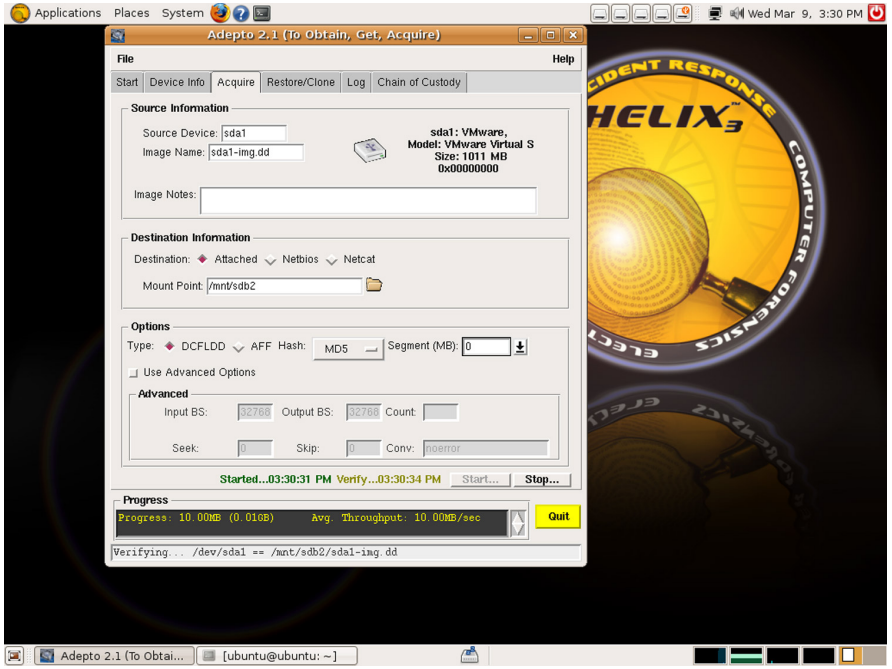
- obstajajo še drugi datotečni sistemi
  - reiserFS, XFS, gfs, afs, ext4, HSM, ...

- *Izziv:* naredite podobno analizo za omenjene sisteme kot smo jo naredili za ufs in ext.
- *Izziv:* Primerjajte opisane datotečne sisteme med seboj – v katerem lahko kje skrijemo kakšne podatke?
- *Izziv:* pripravite kolegu poljuben datotečni sistem in naj kolega ugotovi, za kateri sistem gre.

Forenzični viri

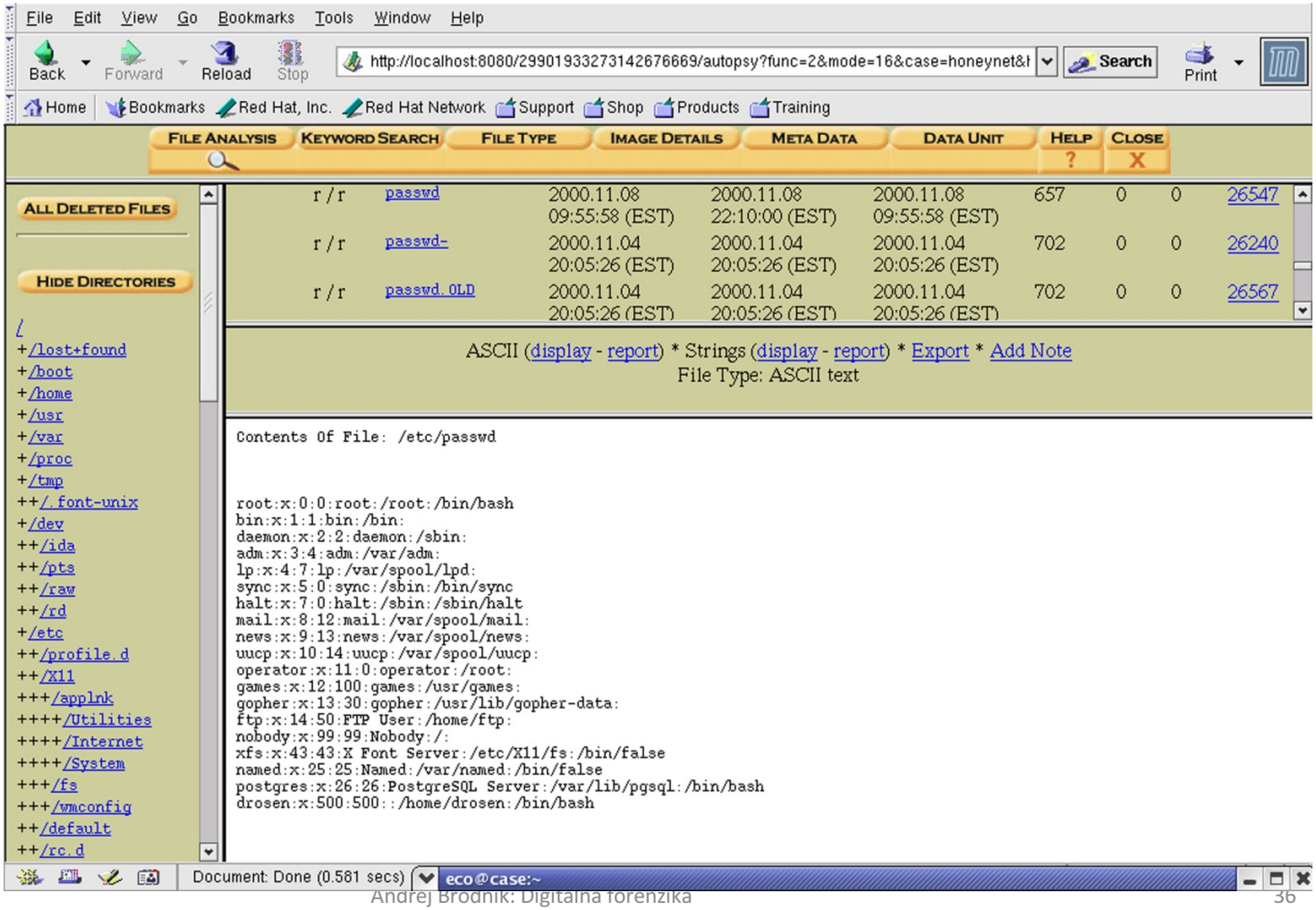
- za analizo slike diska uporabljamo samostoječe operacijske sisteme
- primer: Helix (Ubuntu)

- *Izziv:* pripravite si Helix CD in preverite, kakšna orodja so že na njem.
- *Izziv:* poiščite še kakšne druge podobne sisteme.

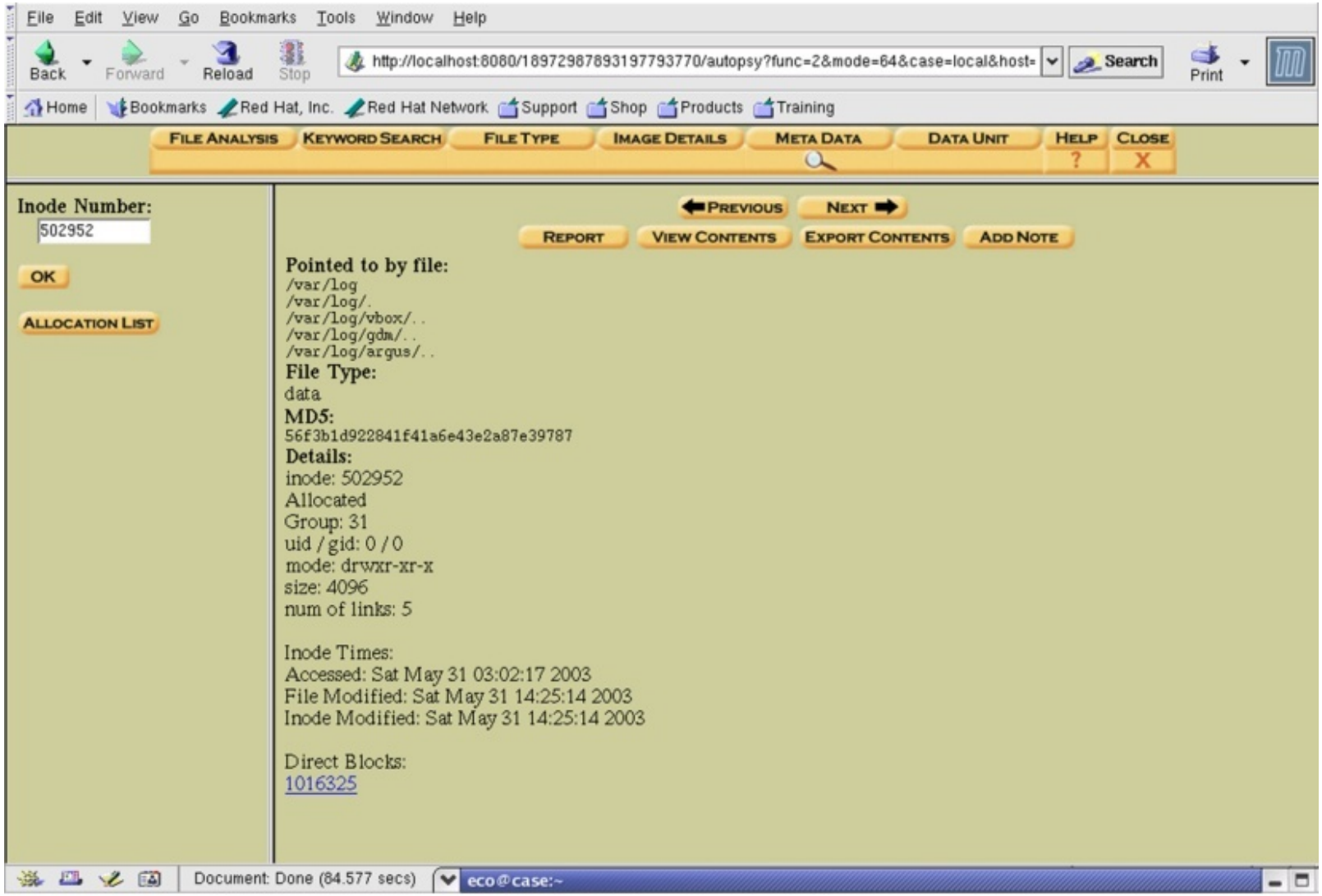


Forenzični viri

- orodje *SleuthKit* z *Autopsy Forensic Browser*

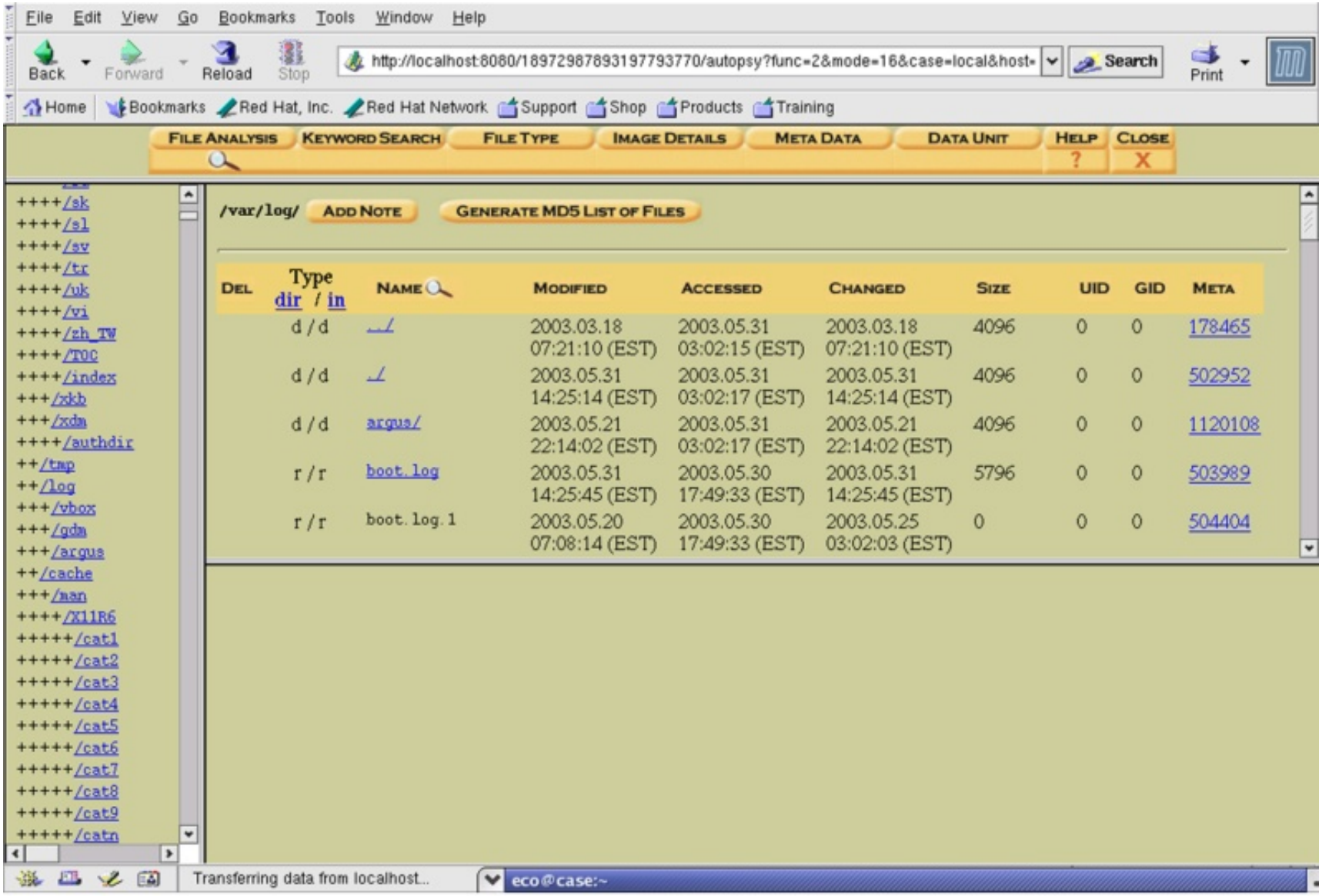


Forenzični viri – raziskava z *SleuthKit*



B

Forenzični viri – raziskava z *SleuthKit*



A

Forenzični viri

- video *File System Forensic Analysis* (*www.youtube.com/watch?v=rmG8yt1WpuA*)
- različne organizacije
  - SANS Institute (*Sysadmin, Audit, Networking, and Security*): tečaji, literatura, …
  - The Honeynet Project (http://www.honeynet.org/)

- *Izziv:* poglejte si izzive na http://www.honeynet.org/challenges in se lotite katerega od njih.

Forenzični viri

- nekaj zanimivih in bogatih referenc:
  - B. Carter, *File system forensic analysis*. Addison-Wesley, 2005.
  - Gregorio Narváez, *Taking advantage of Ext3 journaling file system in a forensic investigation*. SANS Institute, 2007.