

# Informatyka śledcza Laboratorium nr 3

## Raport – Nikodem Jakubowski

### Zadanie 1 – Base64 jako narzędzie do kodowania i dekodowania.

Rozwiązana łamigłówka.



Tworzę plik na pulpicie.

```
user@user: ~/Desktop
File Actions Edit View Help
GNU nano 7.2 laby_03.txt
Polska jest krajem położonym w Europie Środkowej, znana ze swojej bogatej historii i pięknych krajobrazów.
W Warszawie, stolicy Polski, można odwiedzić Zamek Królewski i spacerować po malowniczym Starym Mieście.
Polska kuchnia słynie z smacznych potraw, takich jak pierogi, bigos i kiełbasa.
W Tatrach, na granicy między Polską a Słowacją, znajdują się imponujące góry.
Kraków to inny popularny punkt turystyczny, gdzie można podziwiać historyczne zabytki, takie jak Wawel.
```

Korzystam z pozostałych narzędzi.

```
(user@user)~[~/Desktop]
$ file laby_03.txt
laby_03.txt: Unicode text, UTF-8 text

(user@user)~[~/Desktop]
$ base64 laby_03.txt > ~/Desktop/laby_03-encoded.txt

(user@user)~[~/Desktop]
$ file laby_03-encoded.txt
laby_03-encoded.txt: ASCII text

(user@user)~[~/Desktop]
$ cat laby_03-encoded.txt
UG9sc2thIGplc3Qga3JhamVtIHVxY3VxbXVnbHltIHcgRXVyb3BpZSDFmnJvZGtvd2VqLCB6bmFu
YSB6ZSBzd29qZWogYm9vYXRlaBoaXN0b3JpaSBpIH8pxJlrbnljaC8rcmFqb2JyYXRdS3cuCgpX
IFdhcnN6YXdpZSwgc3RvbG1jeSBQb2xza2ksIG1vxbXUySBvZhdDZWR6acSHIFphbWVrIETyw7Ns
ZXda2kgaSBzcGFjZXJvd2HEhyBwbyBtYWxvd25pY3p5bSBtdGFyeW0gTWllxZtJawUuCGpQb2xz
a2Ega3VjaG5pYSBzcyJ5bmltIHogc2lhY3pueWNoIHVvdHJhdWgdGFraWNoIGphayBwaWVyb2dp
LCBlaWdvcyBpIGtpZCWCYmFzYS4KClcgVG0cmFjaCwgbmEgZ3JhbmljeSBtY2Zp5IFBvbHNR
xIUgYSBtYXJvd2FjasSFLCB6bmFqZHVqxiUgc2nEmSBpbXBvbnVqxIVjZSBnw7NyeS4KCKtyYWVd
s3cgdG8gaW5ueSBwb3B1bGFybnkgcHVua3QgdHVyeXN0eWN6bnksIGdkemllIG1vxbXUySBwb2R6
aXdpYcSHIGhpc3RvcnJjem5LIHphYnlt0a2ksIHRha2llIGphayBXYXdlbC4K
```

```
(user@user)~[~/Desktop]
$ base64 -d laby_03-encoded.txt > ~/Desktop/laby_03-decoded.txt

(user@user)~[~/Desktop]
$ file laby_03-decoded.txt
laby_03-decoded.txt: Unicode text, UTF-8 text
```

```
(user@user)-[~/Desktop]
$ strings laby_03.txt
Polska jest krajem po
onym w Europie
rodkowej, znana ze swojej bogatej historii i pi
knych krajobraz
W Warszawie, stolicy Polski, mo
na odwiedzi
Zamek Kr
lewski i spacerowa
po malowniczym Starym Mie
cie.
Polska kuchnia s
ynie z smacznych potraw, takich jak pierogi, bigos i kie
basa.
W Tatrach, na granicy mi
dzy Polsk
a S
owacj
, znajduj
imponuj
ce g
Krak
w to inny popularny punkt turystyczny, gdzie mo
na podziwia
historyczne zabytki, takie jak Wawel.

(user@user)-[~/Desktop]
$ strings laby_03-decoded.txt
Polska jest krajem po
onym w Europie
rodkowej, znana ze swojej bogatej historii i pi
knych krajobraz
W Warszawie, stolicy Polski, mo
na odwiedzi
Zamek Kr
lewski i spacerowa
po malowniczym Starym Mie
cie.
Polska kuchnia s
ynie z smacznych potraw, takich jak pierogi, bigos i kie
basa.
W Tatrach, na granicy mi
dzy Polsk
a S
owacj
, znajduj
imponuj
ce g
Krak
w to inny popularny punkt turystyczny, gdzie mo
na podziwia
historyczne zabytki, takie jak Wawel.
```

Co ciekawe \$file rozpoznaje plik zakodowany w Base64 jako ASCII, a \$strings nie rozpoznaje polskich znaków i wypisuje zamiast nich znak nowej linii.

## Zadanie 2 – W zakładce pliki do przedmiotu Informatyka Śledcza znajduje się katalog File.zip, który zawiera przykładowe pliki o różnych rozszerzeniach.

Użycie komendy \$file oraz \$pdffinfo.

```
(user@user)-[~/Desktop/infos-lab03]
$ pdffinfo D19910350Lj.pdf
Title: Akt prawny
Author: Władysław Baksza
Creator: Microsoft® Word 2013
Producer: Microsoft® Word 2013
CreationDate: Tue Oct 12 13:08:08 2021 CEST
ModDate: Tue Oct 12 13:08:08 2021 CEST
Custom Metadata: no
Metadata Stream: no
Tagged: yes
UserProperties: no
Suspects: no
Form: none
JavaScript: no
Pages: 351
Encrypted: no
Page size: 595.32 x 841.92 pts (A4)
Page rot: 0
File size: 2601654 bytes
Optimized: no
PDF version: 1.5

(user@user)-[~/Desktop/infos-lab03]
$ pdffinfo D2020000211201.pdf
Title: Ustawa z dnia 28 października 2020 r. o zmianie niektórych u
staw w związku z przeciwdziałaniem sytuacji kryzysowej związanym z wystąpien
iem COVID-19
Author: RCL
Creator: Microsoft® Word 2010
Producer: Microsoft® Word 2010; modified using iText 2.1.7 by iText
CreationDate: Sat Nov 28 18:39:52 2020 CET
ModDate: Sat Nov 28 18:40:01 2020 CET
Custom Metadata: no
Metadata Stream: yes
Tagged: yes
UserProperties: no
Suspects: no
Form: AcroForm
JavaScript: no
Pages: 18
Encrypted: no
Page size: 595.32 x 841.92 pts (A4)
Page rot: 0
File size: 487654 bytes
Optimized: no
PDF version: 1.5

(user@user)-[~/Desktop/infos-lab03]
$ ls
D19910350Lj.pdf D2020000211201.pdf Text

(user@user)-[~/Desktop/infos-lab03]
$ file D19910350Lj.pdf
D19910350Lj.pdf: PDF document, version 1.5, 351 pages

(user@user)-[~/Desktop/infos-lab03]
$ file D2020000211201.pdf
D2020000211201.pdf: PDF document, version 1.5, 18 pages

(user@user)-[~/Desktop/infos-lab03]
$ file Text
Text: ASCII text, with no line terminators
```

Następnie informacje z \$pdffinfo.

### D19910350Lj.pdf

Title: Akt prawny

Author: Władysław Baksza

Creator: Microsoft® Word 2013  
Producer: Microsoft® Word 2013  
CreationDate: Tue Oct 12 13:08:08 2021 CEST  
ModDate: Tue Oct 12 13:08:08 2021 CEST  
Custom Metadata: no  
Metadata Stream: no  
Tagged: yes  
UserProperties: no  
Suspects: no  
Form: none  
JavaScript: no  
Pages: 351  
Encrypted: no  
Page size: 595.32 x 841.92 pts (A4)  
Page rot: 0  
File size: 2601654 bytes  
Optimized: no  
PDF version: 1.5

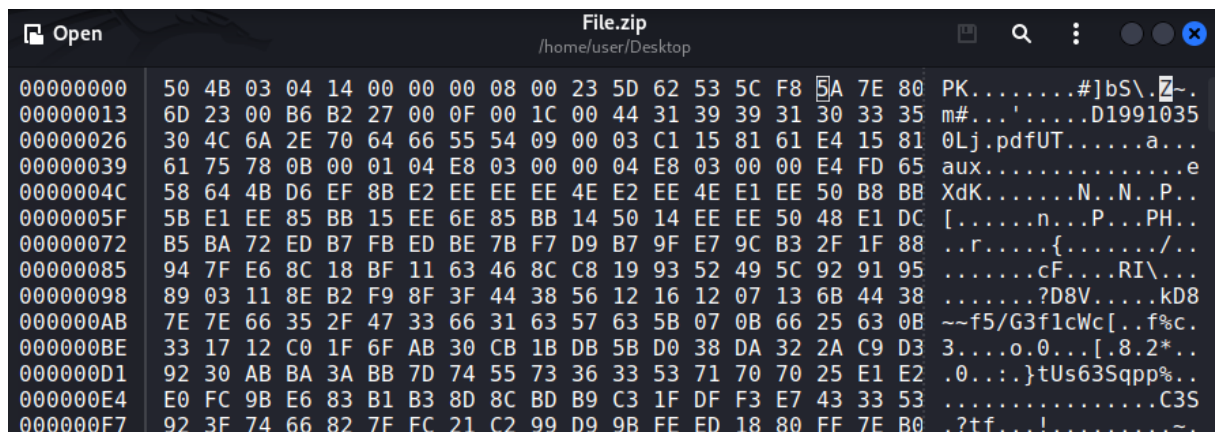
**D2020000211201.pdf**

Title: Ustawa z dnia 28 października 2020 r. o zmianie niektórych ustaw w związku z przeciwdziałaniem sytuacjom kryzysowym związanym z wystąpieniem COVID-19  
Author: RCL  
Creator: Microsoft® Word 2010  
Producer: Microsoft® Word 2010; modified using iText 2.1.7 by 1T3XT  
CreationDate: Sat Nov 28 18:39:52 2020 CET  
ModDate: Sat Nov 28 18:40:01 2020 CET  
Custom Metadata: no  
Metadata Stream: yes  
Tagged: yes  
UserProperties: no  
Suspects: no

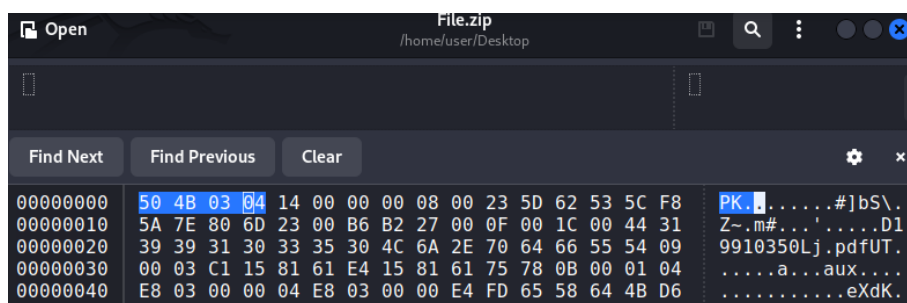
Form: AcroForm  
JavaScript: no  
Pages: 18  
Encrypted: no  
Page size: 595.32 x 841.92 pts (A4)  
Page rot: 0  
File size: 407654 bytes  
Optimized: no  
PDF version: 1.5

### Zadanie 3 – Właściwości narzędzia GHex.

Informacja o rozszerzeniu archiwum znajduje się w pierwszym wierszu.

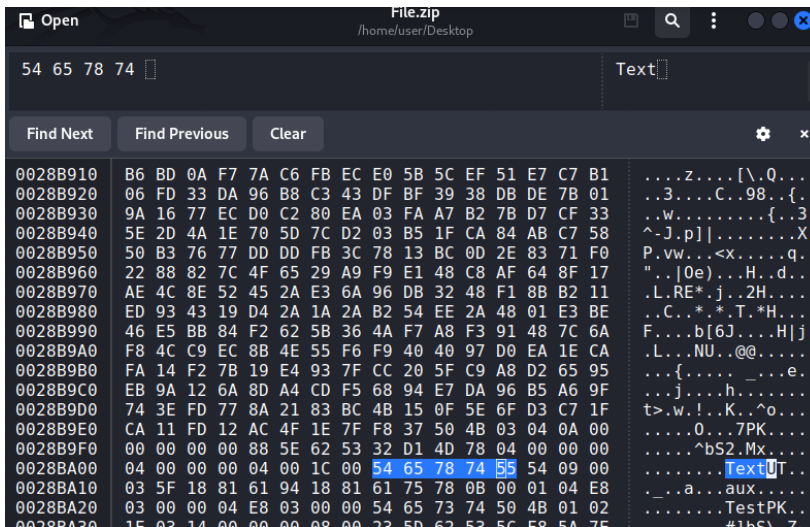
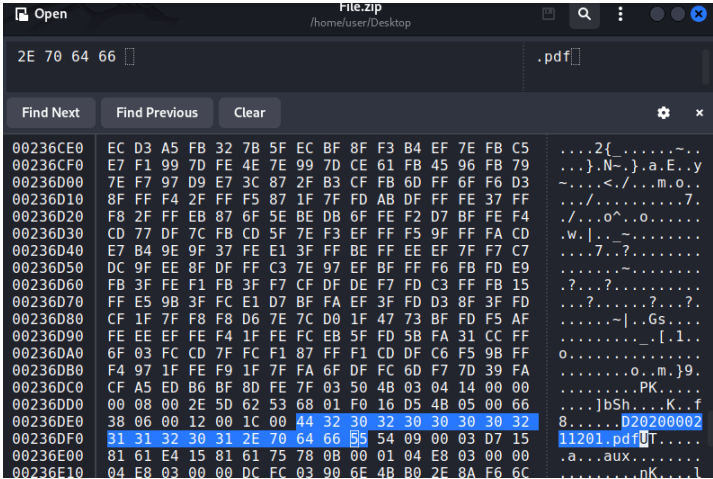


Sygnatura pliku .zip.

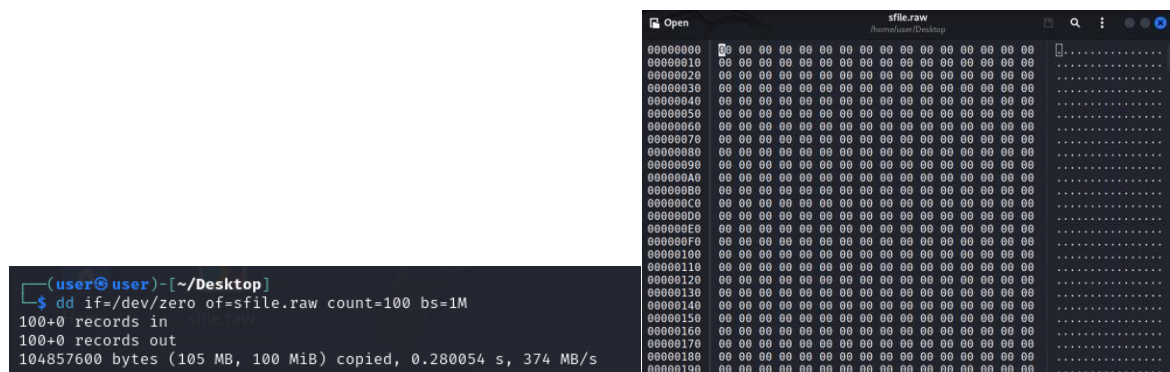


Sygnatura pliku ZIP to czterobajtowy nagłówek, który występuje na początku każdego pliku ZIP. Sygnatura ta ma postać: 50 4B 03 04. Gdzie każda liczba to reprezentacja szesnastkowa jednego bajtu. Odpowiada to ASCII dla liter "PK", to skrót od "Phil Katz" - twórcy formatu ZIP.

Zawartość archiwum (typu .zip czy .rar) jest możliwa do wykrycia. Poniżej znalezione sygnatury.



Wykonuję po kolei polecenia. Różnica – plik jest zapełniony zerami.





Po wykonaniu `$mkfs.fat`, plik dostał dodatkową informację.

```
Open sfile.raw /home/user/Desktop
00000000  B 3C 90 6D 6B 66 73 2E 66 61 74 00 02 04 04 00  <.mkfs.fat....
00000010  02 00 02 00 00 F8 C8 00 20 00 08 00 00 00 00 00  .....
00000020  00 20 03 00 80 00 29 86 56 54 D2 4E 4F 20 4E 41  .....).VT.NO NA
00000030  4D 45 20 20 20 20 46 41 54 31 36 20 20 20 0E 1F  ME FAT16 ..
00000040  BE 5B 7C AC 22 C0 74 0B 56 B4 0E BB 07 00 CD 10  .[|".t.V.....
00000050  5E EB F0 32 E4 CD 16 CD 19 EB FE 54 68 69 73 20  ^..2.....This
00000060  69 73 20 6E 6F 74 20 61 20 62 6F 6F 74 61 62 6C  is not a bootabl
00000070  65 20 64 69 73 6B 2E 20 20 50 6C 65 61 73 65 20  e disk. Please
00000080  69 6E 73 65 72 74 20 61 20 62 6F 6F 74 61 62 6C  insert a bootabl
00000090  65 20 66 6C 6F 70 70 79 20 61 6E 64 0D 0A 70 72  e floppy and..pr
000000A0  65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 74  ess any key to t
000000B0  72 79 20 61 67 61 69 6E 20 2E 2E 2E 20 00 0A 00  ry again ... ..
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Po wykonaniu `$mkfs.ext4`.

```
(user@user)~[~/Desktop]
$ mkfs.ext4 sfile.raw
mkfs.ext4 sfile.raw
mke2fs 1.47.0 (5-Feb-2023)
sfile.raw contains a vfat file system
Proceed anyway? (y,N) y
Discarding device blocks: done
Creating filesystem with 102400 1k blocks and 25584 inodes
Filesystem UUID: 0d4d9daf-3583-4b9c-86fe-c535abe815fe
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```

„Superbloki” zostały utworzone na blokach: 8193, 24577, 40961, 57345, 73729.

Użycie `$dumpe2fs`.

```
(user@user)~[~/Desktop]
$ dumpe2fs sfile.raw
dumpe2fs 1.47.0 (5-Feb-2023)
Filesystem volume name: <none>
Last mounted on: <not available>
Filesystem UUID: 0d4d9daf-3583-4b9c-86fe-c535abe815fe
Filesystem magic number: 0xEF53
Filesystem revision #: 1 (dynamic)
Filesystem features: has_journal ext_attr resize_inode dir_index filetype extent 64bit flex_bg sparse_super lar
ge_file huge_file dir_nlink extra_isize metadata_csum
Filesystem flags: signed_directory_hash
Default mount options: user_xattr acl
Filesystem state: clean
Errors behavior: Continue
Filesystem OS type: Linux
Inode count: 25584
Block count: 102400
Reserved block count: 5120
Overhead clusters: 12067
Free blocks: 98319
Free inodes: 25573
Super blocks: 1
```

Parsowane informacje poniżej.

Magiczny numer: 0xEF53,

Numer UUID: 0d4d9daf-3583-4b9c-86fe-c535abe815fe,

Wielkość bloku: 1024,

Liczba wolnych bloków: 4095,

Podaj „checksum” typ: crc32c,

Wolne bloki w gr. 12: 98305-102399.

Dzięki wykonaniu `$fsck.ext4` wiemy, że wykorzystano około 12 % bloków.

```
(user@user)-[~/Desktop]
$ fsck.ext4 sfile.raw
e2fsck 1.47.0 (5-Feb-2023)
sfile.raw: clean, 11/25584 files, 12081/102400 blocks
```

## Zadanie 5 – Znaczenie superbloku w odzyskiwaniu danych.

Po użyciu \$losetup zostało przydzielone /dev/loop0.

```
(root@user)-[/home/user/Desktop]
# sudo mount /dev/loop0 /mnt/hgfs
```

```
(root@user)-[/home/user/Desktop]
# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
loop0 7:0 0 100M 0 loop /mnt/hgfs
sda 8:0 0 25G 0 disk
├─sda1 8:1 0 24G 0 part /
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 975M 0 part [SWAP]
sr0 11:0 1 1024M 0 rom
```

```
(root@user)-[/home/user/Desktop]
# ls -li /mnt/hgfs
total 12
11 drwx----- 2 root root 12288 Nov 16 19:21 lost+found
```

Katalog "lost+found" jest standardowym katalogiem w systemie plików ext2/ext3/ext4. Jest to miejsce, gdzie system przechowuje pliki, które zostały uszkodzone lub nie mają właściwych atrybutów.

```
(root@user)-[/mnt/hgfs]
# touch newitem

(root@user)-[/mnt/hgfs]
# ls
lost+found newitem
```

```
(root@user)-[/mnt/hgfs]
# dd if=/dev/zero of=/dev/loop0 count=1 bs=1024 seek=1
1+0 records in
1+0 records out
1024 bytes (1.0 kB, 1.0 KiB) copied, 0.00636488 s, 161 kB/s
```

Po tym jest pusto.

```
(root@user)-[/mnt/hgfs]
# ls -a
```

Próba odmontowania kończy się niepowodzeniem, trzeba „zabić” proces.

```
(root@user)-[/mnt/hgfs]
# umount /dev/loop0
umount: /mnt/hgfs: target is busy.
```

Zabicie procesu.

```
(root@user)-[/mnt/hgfs]
# ls /mnt/hgfs
ls: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
ls: WARNING: can't stat() fuse.portel file system /run/user/1000/doc
Output information may be incomplete.
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
zsh 33542 root cwd DIR 7,0 1024 2 /mnt/hgfs
ls 39040 root cwd DIR 7,0 1024 2 /mnt/hgfs
ls 39041 root cwd DIR 7,0 1024 2 /mnt/hgfs

(root@user)-[/mnt/hgfs]
#
(root@user)-[/mnt/hgfs]
# sudo kill -9 33542
zsh: Killed sudo -s

(user@user)-[/mnt/tmp]
# sudo -s
(root@user)-[/mnt/tmp]
# umount /dev/loop0
```

Próba zamontowania kończy się niepowodzeniem, „zły superblock”.

```
(root@user)-[/mnt/tmp]
# mount /dev/loop0 /mnt/hgfs
mount: /mnt/hgfs: wrong fs type, bad option, bad superblock on /dev/loop0, missing codepage or helper program, or other error.
       dmesg(1) may have more information after failed mount system call.
```

Rezultat odzyskanych danych.

```
(root@user)-[/mnt/tmp]
# fsck -f -y -b 8193 /dev/loop0 /mnt/hgfs
fsck from util-linux 2.39.2
e2fsck 1.47.0 (5-Feb-2023)
e2fsck 1.47.0 (5-Feb-2023)
fsck.ext2: Is a directory while trying to open /mnt/hgfs

The superblock could not be read or does not describe a valid ext2/ext3/ext4
filesystem. If the device is valid and it really contains an ext2/ext3/ext4
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>
or
    e2fsck -b 32768 <device>

Superblock needs_recovery flag is clear, but journal has data.
Recovery flag not set in backup superblock, so running journal anyway.
/dev/loop0: recovering journal
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
Block bitmap differences:  +(8193--8450) +(24577--24834) +(40961--41218) +(57345--57602) +(73729--73986)
Fix? yes

Free inodes count wrong for group #0 (1957, counted=1956).
Fix? yes

Free inodes count wrong (25573, counted=25572).
Fix? yes

Padding at end of inode bitmap is not set. Fix? yes

/dev/loop0: ***** FILE SYSTEM WAS MODIFIED *****
/dev/loop0: 12/25584 files (0.0% non-contiguous), 12081/102400 blocks
```

Tutaj odzyskany wolumen.

