Raport 3: Systemy operacyjne – pliki

Zadanie 1:

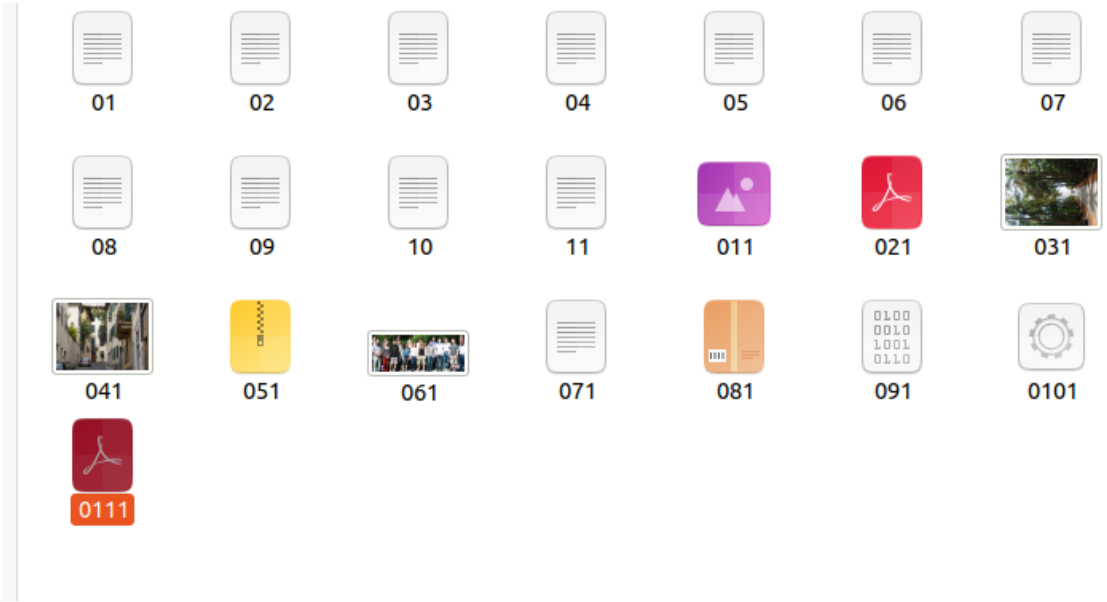
Pobierz plik item-03x01.tar.gz i rozpakuj go komendą

```
sansforensics@siftworkstation: ~
$ cd Downloads
sansforensics@siftworkstation: ~/Downloads
$ tar -xvf item-03x01.tar.gz
pliki/
pliki/03
pliki/07
pliki/08
pliki/06
pliki/04
pliki/10
pliki/11
pliki/01
pliki/02
pliki/09
pliki/05
sansforensics@siftworkstation: ~/Downloads
```

Użyto komendy base64 dla każdego z plików 01-11, a dla ułatwienia zadania przeniesiono odkodowaną zawartość do innego pliku przy użyciu komendy, ponieważ w terminalu byłoby to skomplikowanym zadaniem.

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 01 > 011
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 02 > 021
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 03 > 031
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 04 > 041
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 05 > 051
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 05 > 051
bash: 051: cannot overwrite existing file
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 06 > 061
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 07 > 071
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 08 > 081
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 09 > 091
sansforensics@siftworkstation: ~/Downloads/pliki
$ base64 -d 10 > 0101
sansforensics@siftworkstation: ~/Downloads/pliki
```

Uzyskano pliki o różnych typach.



Następnie używam komendy file w celu ustalenia jakie są typy konkretnych plików oraz komendy strings aby wydobyć informacje tekstowe z pliku.

Plik 011

file:

```
$ file 011
011: TIFF image data, big-endian, direntries=15, height=38, bps=0, compression=L
ZW, PhotometricIntepretation=RGB, orientation=upper-left, width=174
```

strings:

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ strings 011
DbQ8
HdR9$
LfS9
NgRI\
PhT:%
XlV;$
u<a
((<|
h9##
QtiQG
```

Plik 021

file:

```
$ file 021
021: PDF document, version 1.4
```

strings:

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ strings 021
%PDF-1.4
381 0 obj
<</Linearized 1/L 438681/O 383/E 115213/N 2/T 430945/H [ 1276 344]>>
endobj

xref
381 49
0000000016 00000 n
0000001804 00000 n
0000001951 00000 n
0000002520 00000 n
```

Plik 031

file:

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ file 031
031: JPEG image data, Exif standard: [TIFF image data, little-endian, direntries
=12, description=OLYMPUS DIGITAL CAMERA         , manufacturer=OLYMPUS IMAGING C
ORP.   , model=u1020,S1020     , orientation=upper-left, xresolution=1008, yresol
ution=1016, resolutionunit=2, software=Version 1.0                    , datetime
=2015:09:08 11:02:17], baseline, precision 8, 3648x2736, components 3
```

strings:

```
$ strings 031 |head
JFIF
]Exif
OLYMPUS DIGITAL CAMERA
OLYMPUS IMAGING CORP.
u1020,S1020
Version 1.0
2015:09:08 11:02:17
PrintIM
0300
0221
```

Plik 041

file:

```
$ file 041
041: JPEG image data, Exif standard: [TIFF image data, little-endian, direntries
=12, description=                               , manufacturer=NIKON, model=COOL
PIX P6000, orientation=upper-left, xresolution=210, yresolution=218, resolutionu
nit=2, software=Nikon Transfer 1.1 W, datetime=2008:11:01 21:15:09, GPS-Data], b
aseline, precision 8, 640x480, components 3
```

strings:

```
$ strings 041
Exif

NIKON
COOLPIX P6000
Nikon Transfer 1.1 W
:2008:11:01 21:15:09
0220
0100
2008:10:22 16:46:53
2008:10:22 16:46:53
ASCII
```

Plik 051

file:

```
$ file 051
051: Microsoft Excel 2007+
```

strings:

```
$ strings 051
[Content_Types].xml
|v~6}
qFz,
BKPN
J=IB
1"o^
_rels/.rels
b"gi
4Mox/
```

Plik 061

file:

```
$ file 061
061: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segme
nt length 16, Exif Standard: [TIFF image data, little-endian, direntries=9, manu
facturer=Canon, model=Canon EOS 450D, orientation=upper-left, xresolution=144, y
resolution=152, resolutionunit=2, datetime=2013:06:06 16:02:24], baseline, preci
sion 8, 3699x1718, components 3
```

strings:

```
$ strings 061 |head
JFIF
60Exif
Canon
Canon EOS 450D
2013:06:06 16:02:24
0221
0100
2013:06:06 16:02:24
2013:06:06 16:02:24
Canon EOS 450D
```

Plik 071

file:

```
$ file 071
071: ISO-8859 text, with CRLF line terminators
```

strings:

```
$ strings 071
30/04/2015      "TRANSAKCJA KART
ATNICZ
"       "LIDL KOCMYRZOWSKA Krakow 31109507 000000000135053"     "-27,79 PLN"
28/04/2015      "PRZELEW INTERNET M/B"  "UPC Polska Sp.z o.o. al. Jana Paw
a II 27 Warszawa 00-867 nr abonenta 3551021"    "-139,77 PLN"
28/04/2015      "TRANSAKCJA KART
ATNICZ
"       "CARREFOUR HIPERMARKET KRAKOW 24204500 1051241444"      "-129,66 PLN"
28/04/2015      "PRZELEW INTERNET"      "DotPay ul. Wielicka 72 Krak
w 30-552 M1283-2524 Zam
```

Plik 081

file:

```
$ file 081
081: POSIX tar archive (GNU)
```

strings:

```
$ strings 081
messages
0000644
0000000
0000000
00000020132
07747776253
011334
ustar
root
root
```

Plik 091

file:

```
$ file 091
091: data
```

strings:

```
$ strings 091 |head
$J'i
d       o3g
9%gW    $k
O@iNc
I)[Q
2fcs
|iHV
ecr[[
/lt0
.5[1,
```

Plik 0101

file:

```
$ file 0101
0101: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked
, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=55bab91499d24ed0c2183d3
0cacb2c30e3c41caf, for GNU/Linux 3.2.0, stripped
```

strings:

```
$ strings 0101
/lib64/ld-linux-x86-64.so.2
librhythmbox-core.so.10
g_type_check_instance_cast
g_log
g_object_unref
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
rb_application_run
rb_threads_init
```

Plik 0111

file:

```
$ file 0111
0111: PDF document, version 1.4
```

strings:

```
$ strings 0111
%PDF-1.4
2 0 obj
<</Length 3 0 R/Filter/FlateDecode>>
stream
pExMt
AMXX
,rOX
+uOh
HG:qV
^tKf
```

Następnie dla poszczególnych plików użyto komend *pdfinfo* i *exiftool*.

Pdfinfo użyto dla plików 0111 i 021.

Przykładowe użycie:

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ pdfinfo -meta 021 > 021pdf
```

Uzyskany efekt:

Open 021pdf ~/Downloads/pliki

```
<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c014 79.156797, 2014/08/20-09:53:02        ">
   <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
      <rdf:Description rdf:about=""
            xmlns:xmp="http://ns.adobe.com/xap/1.0/"
            xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/"
            xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#"
            xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#"
            xmlns:dc="http://purl.org/dc/elements/1.1/"
            xmlns:pdf="http://ns.adobe.com/pdf/1.3/">
         <xmp:CreateDate>2015-01-16T18:46:36Z</xmp:CreateDate>
         <xmp:MetadataDate>2015-01-16T18:46:38Z</xmp:MetadataDate>
         <xmp:ModifyDate>2015-01-16T18:46:38Z</xmp:ModifyDate>
         <xmp:CreatorTool>Adobe InDesign CC 2014 (Macintosh)</xmp:CreatorTool>
         <xmpMM:InstanceID>uuid:919574e2-d77a-6944-980f-afdb086b32bf</xmpMM:InstanceID>
         <xmpMM:OriginalDocumentID>xmp.did:BB151BA4DEAFDF118F3BA536721FFC27</xmpMM:OriginalDocumentID>
         <xmpMM:DocumentID>xmp.id:a8d2f34f-784d-446d-9efa-0d5e7ea771d7</xmpMM:DocumentID>
         <xmpMM:RenditionClass>proof:pdf</xmpMM:RenditionClass>
         <xmpMM:DerivedFrom rdf:parseType="Resource">
            <stRef:instanceID>xmp.iid:1622d6b2-5b3b-d842-8402-08d0b564beca</stRef:instanceID>
            <stRef:documentID>xmp.did:1622d6b2-5b3b-d842-8402-08d0b564beca</stRef:documentID>
            <stRef:originalDocumentID>xmp.did:BB151BA4DEAFDF118F3BA536721FFC27</stRef:originalDocumentID>
            <stRef:renditionClass>default</stRef:renditionClass>
         </xmpMM:DerivedFrom>
         <xmpMM:History>
            <rdf:Seq>
               <rdf:li rdf:parseType="Resource">
                  <stEvt:action>converted</stEvt:action>
                  <stEvt:parameters>from application/x-indesign to application/pdf</stEvt:parameters>
                  <stEvt:softwareAgent>Adobe InDesign CC 2014 (Macintosh)</stEvt:softwareAgent>
                  <stEvt:changed>/</stEvt:changed>
                  <stEvt:when>2015-01-16T18:46:36Z</stEvt:when>
               </rdf:li>
            </rdf:Seq>
         </xmpMM:History>
         <dc:format>application/pdf</dc:format>
         <pdf:Producer>Adobe PDF Library 11.0</pdf:Producer>
         <pdf:Trapped>False</pdf:Trapped>
      </rdf:Description>
   </rdf:RDF>
</x:xmpmeta>
<?xpacket end="r"?>
```

Z kolei *exiftool* użyto dla plików 011, 031, 041 i 061.

Przykładowe użycie:

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ exiftool 011 > 011_exif
```

Uzyskany efekt:

Open 011_exif ~/Downloads/pliki

```
ExifTool Version Number         : 11.88
File Name                       : 011
Directory                       : .
File Size                       : 6.8 kB
File Modification Date/Time     : 2022:03:21 13:05:45+00:00
File Access Date/Time           : 2022:03:22 13:53:15+00:00
File Inode Change Date/Time     : 2022:03:21 13:05:45+00:00
File Permissions                : rw-rw-r--
File Type                       : TIFF
File Type Extension             : tif
MIME Type                       : image/tiff
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Width                     : 174
Image Height                    : 38
Bits Per Sample                 : 8 8 8 8
Compression                     : LZW
Photometric Interpretation      : RGB
Strip Offsets                   : 8
Orientation                     : Horizontal (normal)
Samples Per Pixel               : 4
Rows Per Strip                  : 38
Strip Byte Counts               : 6391
Planar Configuration            : Chunky
Predictor                       : Horizontal differencing
Extra Samples                   : Associated Alpha
Sample Format                   : Unsigned; Unsigned; Unsigned; Unsigned
XMP Toolkit                     : XMP Core 5.1.2
Image Size                      : 174x38
Megapixels                      : 0.007
```

Dla pozostałych plików nie mamy komendy, która pozwala na wypisanie i analizę metadanych.

Metadane dotyczące pliku 031(obrazek został obrócony):

File Type: JPEG

Camera Model Name: u1020, s1020

Orientation: Horizontal(normal)

Software: Version 1.0

Local Length: 6.6 mm

Modify Date: 2015:09:08 11:02:17

Exposure Program: Creative (slow speed)

Camera ID: OLYMPUS DIGITAL CAMERA

Color Space: sRGB

File Source: Digital Camera

Custom Rendered: Normal

Exposure Mode: Auto

White Balance: Auto

Digital Zoom Ratio: 1

Contrast: Normal

Saturation: Normal

Compression: JPEG (old-style)

Image Width: 2736

Image Height: 3648

Image Size: 2736x3648

Megapixels: 10.0

Shutter Speed: 1/250

Analiza 10 wybranych parametrów metadanych:

1. Orientation – określa pozycję pliku, najczęściej graficznego lub video, ale ten parametr określa się również dla plików takich jak pdf czy doc. W większości przypadków jego wartość to „poziomy" lub „pionowy".
2. Megapixels – liczba megapikseli, które tworzą dany plik.
3. File Type – synonim wyrażenia „format pliku". Opisuje ono sposób w jaki dany plik jest przechowywany na komputerze, a także podaje informacje w jaki sposób powinien zostać otworzony.
4. Image Size – określa rozmiar obrazu – jego szerokość i wysokość liczoną w pikselach
5. Color Space – informacja o tym jaki model wyświetlania kolorów został zastosowany.
6. Compression – metoda kompresji jaka została zastosowana dla pliku
7. Camera Model Name – daje informacje o tym jaki model aparatu został użyty do uchwycenia obrazu.
8. Image Width – szerokość obrazu.
9. Image Height – wysokość zdjęcia.
10. White Balance – określa stan balansu bieli(proces usuwania nierealistycznych przebarwień, dzięki czemu obiekty wyglądające na białe na zdjęciu stają się białe na zdjęciu).

Komentarz:

Biorąc pod uwagę model aparatu można stwierdzić, że autor zdjęcia jest raczej amatorem fotografii. Olympus u1020, s1020 jest skierowany do standardowych użytkowników robiących zdjęcia na przykład na rodzinnej uroczystości. Nie posiada wielu zaawansowanych funkcji, których potrzebowałby zawodowy fotograf. Dodatkowo parametry takie jak balans bieli czy ustawienia trybu ekspozycji są automatyczne więc nie zostały dostosowane przez osobę wykonującą zdjęcie.

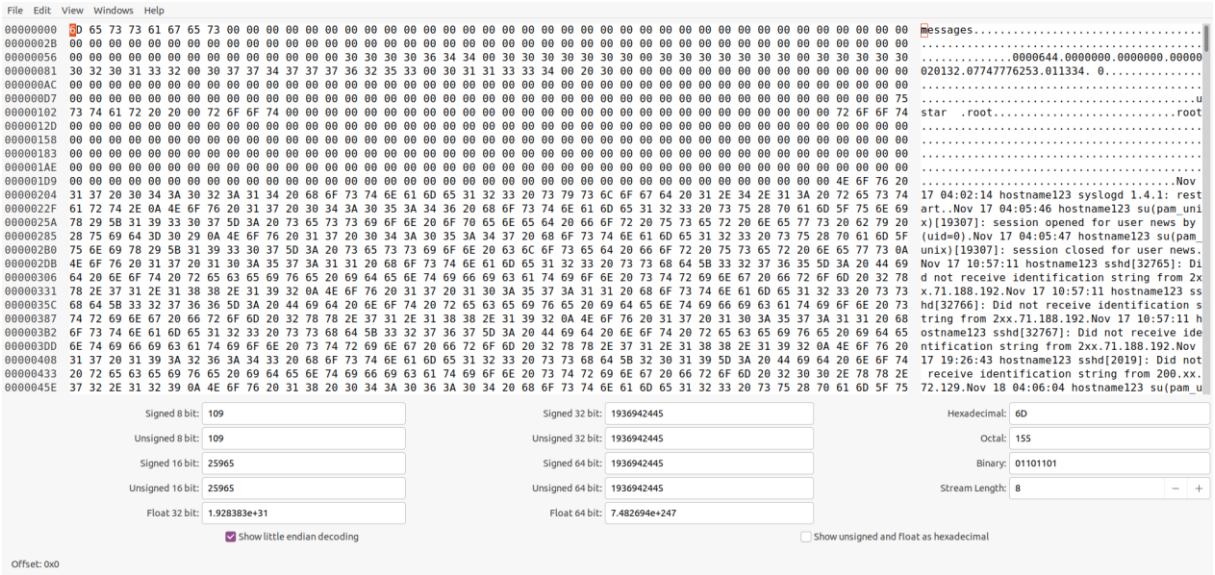
Zadanie 2

Użyto komendy xxd 081:

```
sansforensics@siftworkstation: ~/Downloads/pliki
$ xxd 081
00000000: 6d65 7373 6167 6573 0000 0000 0000 0000  messages........
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000060: 0000 0000 3030 3030 3634 3400 3030 3030  ....0000644.0000
00000070: 3030 3000 3030 3030 3030 3000 3030 3030  000.0000000.0000
00000080: 3030 3230 3133 3200 3037 3734 3737 3736  0020132.07747776
00000090: 3235 3300 3031 3133 3334 0020 3000 0000  253.011334. 0...
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000100: 0075 7374 6172 2020 0072 6f6f 7400 0000  .ustar  .root...
00000110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000120: 0000 0000 0000 0000 0072 6f6f 7400 0000  .........root...
00000130: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000140: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000150: 0000 0000 0000 0000 0000 0000 0000 0000
```

Po odczytaniu zawartości terminala można zauważyć, że archiwum składało się z 5 plików o nazwach: messages, messages1, messages2, messages3, messages4.

Alternatywnym rozwiązaniem jest zaimportowanie pliku do programu GHex (lub użycie komendy ghex 081):



Otrzymano tabelę:

Pole	Offset	Długość [B]	Wartość
File name	0x0	100	messages
File mode	0x64	8	0000644
Owner user ID	0x6c	8	0000000

Owner group ID	0x74	8	0000000
Length of file in bytes	0x7c	12	00000020132
Modify time of file	0x88	12	07747776253
Checksum for header	0x94	8	011334
Indicator for links	0x9c	1	0
Name of linked file	0x9d	100	
USTAR indicator	0x101	6	utar(+space)
USTAR version	0x107	2	space(+NULL)
Owner User name	0x109	32	root
Owner group name	0x129	32	root
Device major number	0x149	8	
Device minor number	0.151	8	
Prefix for file name	0x159	155	