Forensics Challenge 0.0.1

Manual data recovery

CIRCL *TLP:WHITE*

info@circl.lu

Edition EC3

Current Situation

Simulation based on a real case

1. Small company
2. Ransomware outbreak
3. All data encrypted
4. File name extension `.rans` added
5. Backups on external disk
   - 5.1 Daily full backup of all data
   - 5.2 All data stored in individual ZIP archives
   - 5.3 Available backups:

```
    50832 Jun 14 10:53 backup_2019-02-08.zip.rans*
  2175110 Jun 14 10:57 backup_2019-02-12.zip.rans*
 11896585 Jun 14 11:01 backup_2019-02-13.zip.rans*
 11896763 Jun 14 11:10 backup_2019-02-14.zip.rans*

file *
    backup_2019-02-08.zip.rans: data
    backup_2019-02-12.zip.rans: data
    backup_2019-02-13.zip.rans: data
    backup_2019-02-14.zip.rans: data
```

→ Goal: Data recovery

Start investigation

How strong is the encryption?

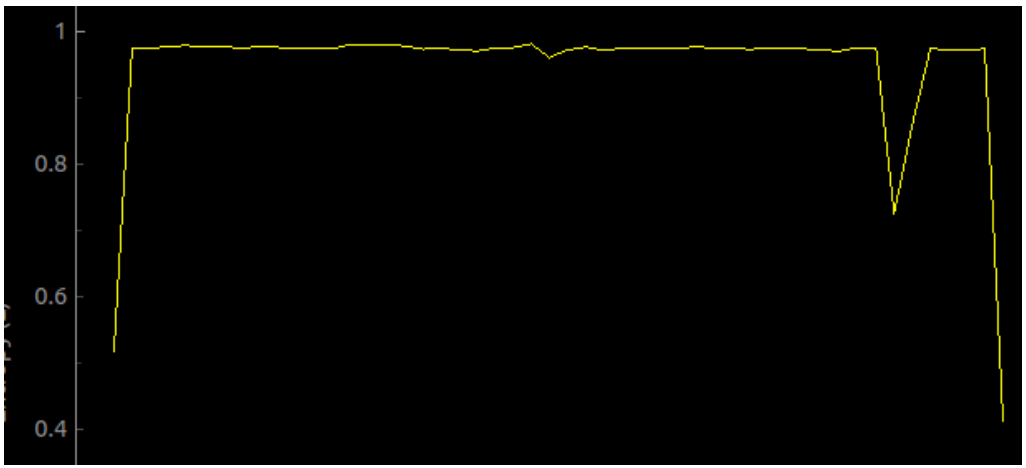
Calculate entropy

```
ent backup_2019-02-08.zip.rans      --> Entropy = 7.925631 bits per byte.
ent backup_2019-02-12.zip.rans      --> Entropy = 7.998791 bits per byte.
ent backup_2019-02-13.zip.rans      --> Entropy = 7.998055 bits per byte.
ent backup_2019-02-14.zip.rans      --> Entropy = 7.998011 bits per byte.
```

→ Dont look good

→ But wait we have ZIP files

```
binwalk -E backup_2019-02-08.zip.rans | less
```



Start investigation

Investigate with hex-viewer and strings

What do you think about this?

```
xxd backup_2019-02-08.zip.rans | less
```

```
00000000: 504b 0304 1400 0000 0000 7b59 484e 0000  PK........{YHN..
00000010: 0000 0000 0000 0000 0000 0900 0000 5069  ..............Pi
00000020: 6374 7572 6573 2f00 0000 0000 0000 0000  ctures/.........
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
.....
```

What do you think about this?

```
strings -n 10 backup_2019-02-* | less
```

```
$B-.jOA0|(
Pictures/CIRCL-Logo.png
<)&\8HVL+S
Documents/PK
Documents/Education_Programme_Flyer.pdf
Q<|D;y0eBxP
*i=u6:\?wW
Documents/forensics-101.pdf
6yK@@CB1,j
.....
```

What is the conclusion?

The structure of a PKZip file

General structure:

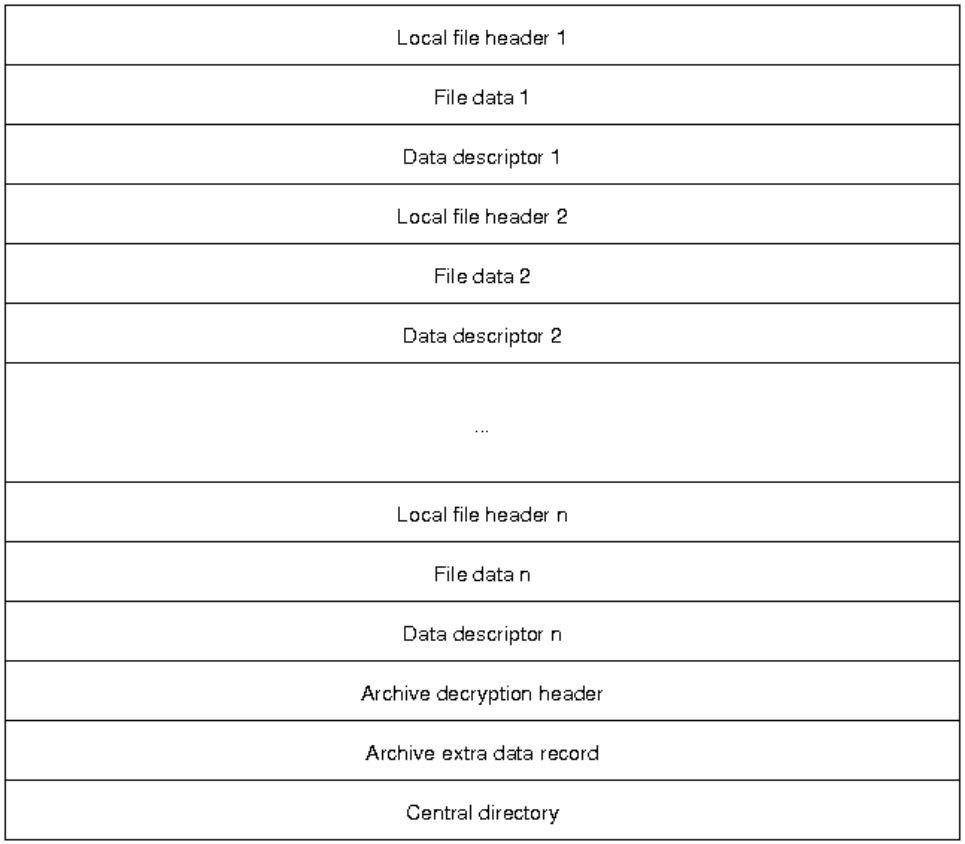


Image (c) jmu.edu - Image used solely for illustration purposes - https://users.cs.jmu.edu/buchhofp/forensics/formats/pkzip.html

The structure of a PKZip file

Local file headers:

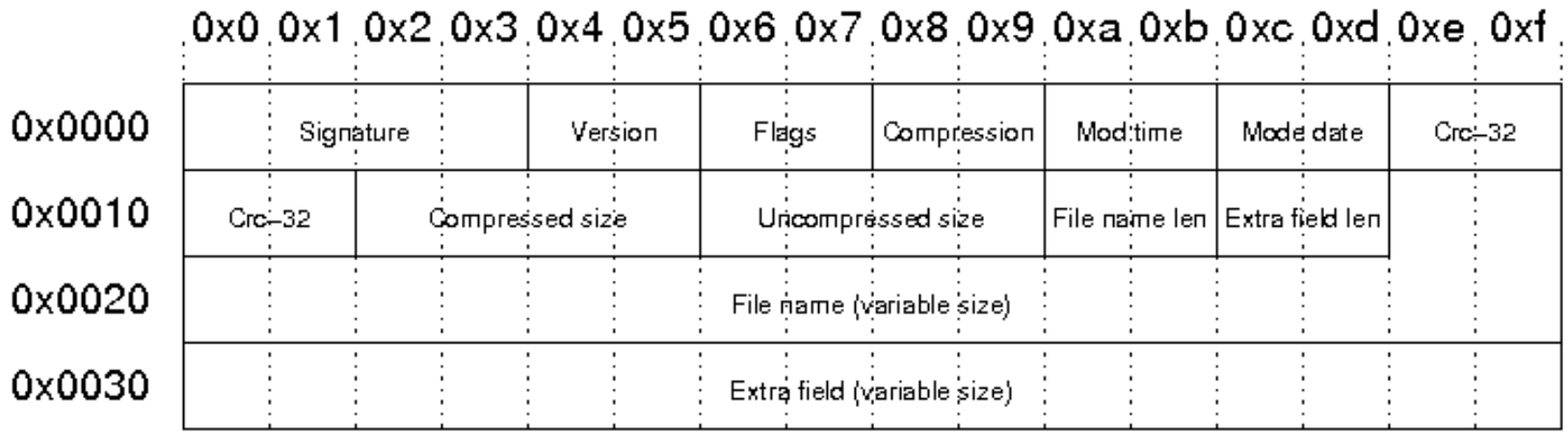
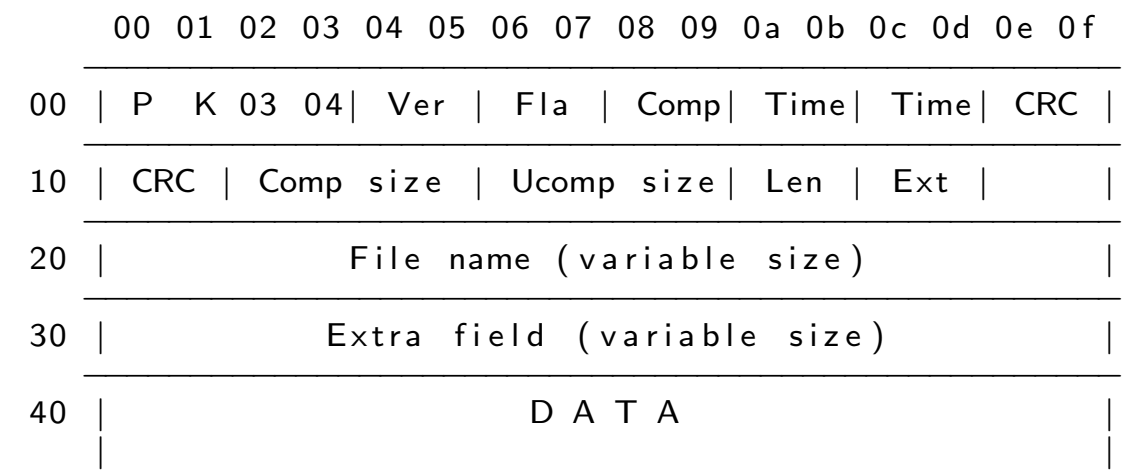


Image (c) jmu.edu - Image used solely for illustration purposes - https://users.cs.jmu.edu/buchhofp/forensics/formats/pkzip.html

Signature: `0x50 0x4b 0x03 0x04`

Exercise 1: Recover a directory

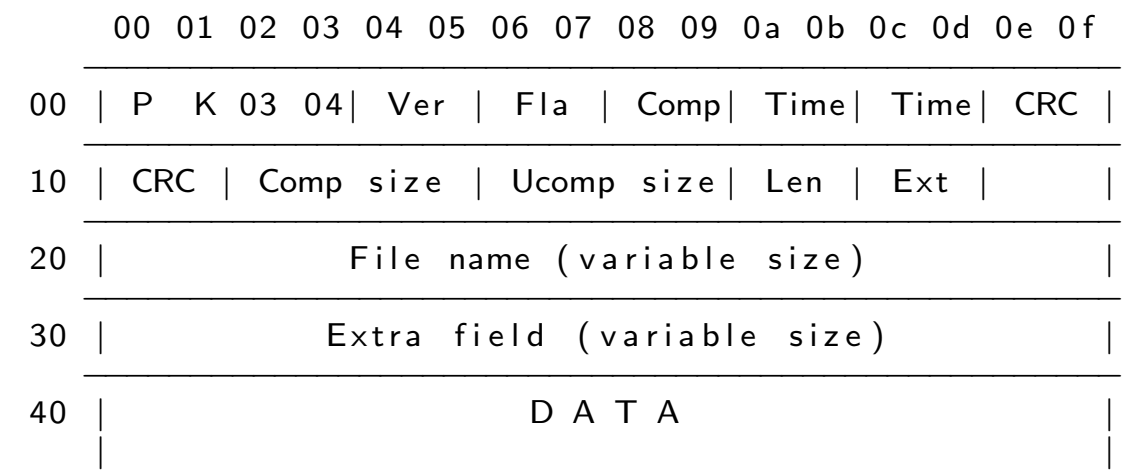



```
xxd backup_2019-02-14.zip.rans | less
    00000000: 504b 0304 1400 0000 0000 777c 4e4e 0000  PK........w|NN..
    00000010: 0000 0000 0000 0000 0000 0a00 0000 446f  ..............Do
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
```

Compressed size:	—>	—>
Lenght file name:	—>	—>
Extra field:	—>	—>
Start of data:		—>
End of data:		—>
Recovery begin (head begin):		—>
Recover size header + data:		—>

Command:

Exercise 1: Recover a directory

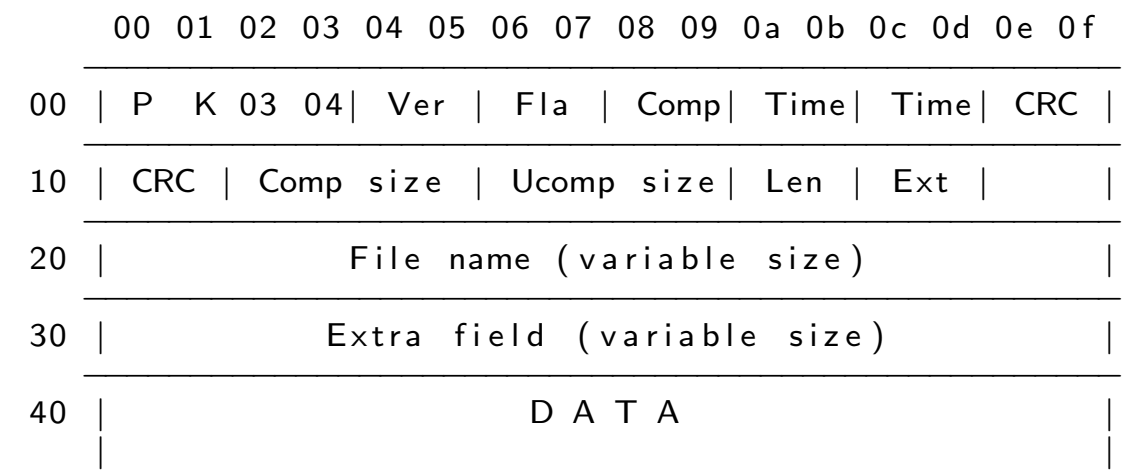



```
xxd backup_2019-02-14.zip.rans | less
    00000000: 504b 0304 1400 0000 0000 777c 4e4e 0000  PK........w|NN..
    00000010: 0000 0000 0000 0000 0000 0a00 0000 446f  ..............Do
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
```

```
              Compressed size: 00 00  ---->  00 00  ---->     0
            Lenght file name: 0a 00  ---->  00 0a  ---->    10
                 Extra field: 00 00  ---->  00 00  ---->     0
               Start of data:       30 + 10 + 0   ---->    40
                 End of data:              40 + 0  ---->    40
Recovery begin (head begin):                 00  ---->     0
 Recover size header + data:              40 + 0  ---->    40

  Command: dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=  skip=  count=   seek=
```

Exercise 1: Recover a directory




```
xxd backup_2019-02-14.zip.rans | less
    00000000: 504b 0304 1400 0000 0000 777c 4e4e 0000  PK........w|NN..
    00000010: 0000 0000 0000 0000 0000 0a00 0000 446f  ..............Do
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
```

```
                Compressed size: 00 00  ---->  00 00  ---->     0
              Lenght file name: 0a 00  ---->  00 0a  ---->    10
                   Extra field: 00 00  ---->  00 00  ---->     0
                 Start of data:      30 + 10 + 0   ---->    40
                   End of data:             40 + 0  ---->    40
Recovery begin (head begin):                   00  ---->     0
 Recover size header + data:             40 + 0  ---->    40
```

Command: `dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=0 count=40 seek=0`

Exercise 2: Recover your first file

```
     00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
    ------------------------------------------------
 00 | P  K 03 04| Ver | Fla | Comp| Time| Time| CRC |
    ------------------------------------------------
 10 | CRC | Comp size | Ucomp size| Len | Ext |     |
    ------------------------------------------------
 20 |           File name (variable size)           |
    ------------------------------------------------
 30 |                                               |
```

```
xxd backup_2019-02-14.zip.rans | less
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
    00000030: 0800 1c80 4c4e 85b6 6965 7f6b 0200 ccbd  ....LN..ie.k....
    00000040: 0200 2700 0000 446f 6375 6d65 6e74 732f  ..'...Documents/
    00000050: 4564 7563 6174 696f 6e5f 5072 6f67 7261  Education_Progra
    00000060: 6d6d 655f 466c 7965 722e 7064 66dc 5a05  mme_Flyer.pdf.Z.
    00000070: 5494 cf16 ff08 1109 2905 41a4 a543 ba41  T.......).A..C.A
```

```
              Compressed size:          -->          -->
             Lenght file name:          -->          -->
                  Extra field:          -->          -->
                Start of data:                       -->
                  End of data:                       -->
 Recovery begin (head begin):                        -->
  Recover size header + data:                        -->
```

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=  skip=   count=       seek=
```

Exercise 2: Recover your first file

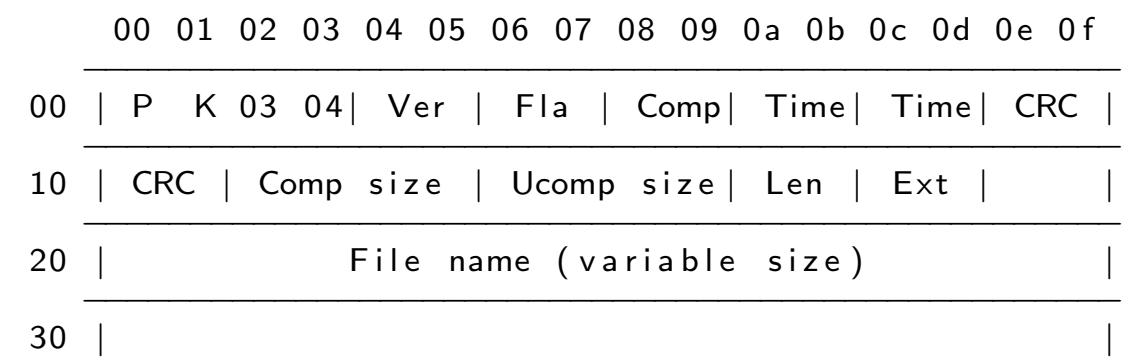
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	P	K	03	04	Ver		Fla		Comp		Time		Time		CRC	
10	CRC				Comp size				Ucomp size				Len		Ext	
20	File name (variable size)															
30																

```
xxd backup_2019-02-14.zip.rans | less
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
    00000030: 0800 1c80 4c4e 85b6 6965 7f6b 0200 ccbd  ....LN..ie.k....
    00000040: 0200 2700 0000 446f 6375 6d65 6e74 732f  ..'...Documents/
    00000050: 4564 7563 6174 696f 6e5f 5072 6f67 7261  Education_Progra
    00000060: 6d6d 655f 466c 7965 722e 7064 66dc 5a05  mme_Flyer.pdf.Z.
    00000070: 5494 cf16 ff08 1109 2905 41a4 a543 ba41  T.......).A..C.A
```

Compressed size:	7f6b 0200 ⟶	0002 6b7f ⟶	158,591
Lenght file name:	2700 ⟶	0027 ⟶	39
Extra field:	0000 ⟶	0000 ⟶	0
Start of data:	40 + 30 + 39 + 0 ⟶		109
End of data:	109 + 158,591 ⟶		158,700
Recovery begin (head begin):	28 ⟶		40
Recover size header + data:	30 + 39 + 158,591 ⟶		158,660

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs= skip= count= seek=
```

Exercise 2: Recover your first file



	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	P	K	03	04	Ver		Fla		Comp		Time		Time		CRC	
10	CRC				Comp size				Ucomp size				Len		Ext	
20	File name (variable size)															
30																

```
xxd backup_2019-02-14.zip.rans | less
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
    00000030: 0800 1c80 4c4e 85b6 6965 7f6b 0200 ccbd  ....LN..ie.k....
    00000040: 0200 2700 0000 446f 6375 6d65 6e74 732f  ..'...Documents/
    00000050: 4564 7563 6174 696f 6e5f 5072 6f67 7261  Education_Progra
    00000060: 6d6d 655f 466c 7965 722e 7064 66dc 5a05  mme_Flyer.pdf.Z.
    00000070: 5494 cf16 ff08 1109 2905 41a4 a543 ba41  T.......).A..C.A
```

Compressed size:	7f6b 0200	⟶ 0002 6b7f	⟶ 158,591
Lenght file name:	2700	⟶ 0027	⟶ 39
Extra field:	0000	⟶ 0000	⟶ 0
Start of data:		40 + 30 + 39 + 0	⟶ 109
End of data:		109 + 158,591	⟶ 158,700
Recovery begin (head begin):		28	⟶ 40
Recover size header + data:		30 + 39 + 158,591	⟶ 158,660

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=40 count=158660 seek=40
```

Exercise 3: Recover the next file

```
     00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
   ┌──────────────────────────────────────────────────┐
00 | P  K 03 04| Ver | Fla | Comp| Time| Time| CRC |
   ├──────────────────────────────────────────────────┤
10 | CRC | Comp size | Ucomp size| Len | Ext |      |
   ├──────────────────────────────────────────────────┤
20 |           File name (variable size)              |
   ├──────────────────────────────────────────────────┤
30 |                                                  |
```

```
xxd backup_2019-02-14.zip.rans | less
    00026be0: 20b1 9523 e3e5 9557 5320 fb01 504b 0304   ..#...WS ..PK..
    00026bf0: 1400 0000 0800 2b80 4c4e 911e 00e9 f497   ......+.LN......
    00026c00: 0d00 12a9 0e00 1b00 0000 446f 6375 6d65   ..........Docume
    00026c10: 6e74 732f 666f 7265 6e73 6963 732d 3130   nts/forensics-10
    00026c20: 312e 7064 66bc 5a75 54db 4f12 bf83 16a7   1.pdf.ZuT.O.....
```

```
              Compressed size:          -->          -->
             Lenght file name:          -->          -->
                  Extra field:          -->          -->
                Start of data:                       -->
                  End of data:                       -->
 Recovery begin (head begin):                        -->
  Recover size header + data:                        -->
```

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=       count=       seek=
```

Exercise 3: Recover the next file

```
     00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
   ┌──────────────────────────────────────────────────┐
00 | P  K 03 04| Ver | Fla | Comp| Time| Time| CRC |
   ├──────────────────────────────────────────────────┤
10 | CRC | Comp size | Ucomp size| Len | Ext |      |
   ├──────────────────────────────────────────────────┤
20 |           File name (variable size)              |
   ├──────────────────────────────────────────────────┤
30 |                                                  |
```

```
xxd backup_2019-02-14.zip.rans | less
    00026be0: 20b1 9523 e3e5 9557 5320 fb01 504b 0304   ..#...WS ..PK..
    00026bf0: 1400 0000 0800 2b80 4c4e 911e 00e9 f497   ......+.LN......
    00026c00: 0d00 12a9 0e00 1b00 0000 446f 6375 6d65   ..........Docume
    00026c10: 6e74 732f 666f 7265 6e73 6963 732d 3130   nts/forensics-10
    00026c20: 312e 7064 66bc 5a75 54db 4f12 bf83 16a7   1.pdf.ZuT.O.....

              Compressed size: f497 0d00  -->  000d 97f4  -->    890,868
            Lenght file name:      1b00  -->       001b  -->         27
                 Extra field:      0000  -->       0000  -->          0
               Start of data:   158,700 + 30 + 27 + 0  -->    158,757
                 End of data:       158,757 + 890,868  -->  1,049,625
 Recovery begin (head begin):                  026bec  -->    158,700
  Recover size header + data:       30 + 27 + 890,868  -->    890,925

dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=       count=       seek=
```

Exercise 3: Recover the next file

```
     00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
   ┌─────────────────────────────────────────────────┐
00 | P  K 03 04| Ver | Fla | Comp| Time| Time| CRC |
   ├─────────────────────────────────────────────────┤
10 | CRC | Comp size | Ucomp size| Len | Ext |     |
   ├─────────────────────────────────────────────────┤
20 |           File name (variable size)           |
   ├─────────────────────────────────────────────────┤
30 |                                               |
```

```
xxd backup_2019-02-14.zip.rans | less
    00026be0: 20b1 9523 e3e5 9557 5320 fb01 504b 0304   ..#...WS ..PK..
    00026bf0: 1400 0000 0800 2b80 4c4e 911e 00e9 f497   ......+.LN......
    00026c00: 0d00 12a9 0e00 1b00 0000 446f 6375 6d65   ..........Docume
    00026c10: 6e74 732f 666f 7265 6e73 6963 732d 3130   nts/forensics-10
    00026c20: 312e 7064 66bc 5a75 54db 4f12 bf83 16a7   1.pdf.ZuT.O.....

              Compressed size: f497 0d00  ──>  000d 97f4  ──>    890,868
            Lenght file name:      1b00  ──>       001b  ──>         27
                 Extra field:      0000  ──>       0000  ──>          0
               Start of data:   158,700 + 30 + 27 + 0     ──>    158,757
                 End of data:       158,757 + 890,868     ──>  1,049,625
 Recovery begin (head begin):                   026bec  ──>    158,700
  Recover size header + data:       30 + 27 + 890,868     ──>    890,925

dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=158700 count=890925 seek=158700
```

Final Command List

Already covered:

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=0 count=40 seek=0
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=158700 count=890925 seek=158700
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=40 count=158660 seek=40
```

Home work:

```
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=1049625 count=1074145 seek=104962
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=2123770 count=77 seek=2123770

dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=2123770 count=38 seek=2123847
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=2123808 count=113286 seek=212388
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=2237094 count=4806555 seek=223717
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=7043649 count=4801146 seek=704372
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=11844795 count=39 seek=11844872

dd if=backup_2019-02-12.zip.rans of=rescue.zip bs=1 skip=2123809 count=25464 seek=1184491
dd if=backup_2019-02-08.zip.rans of=rescue.zip bs=1 skip=25426 count=19260 seek=11870375
dd if=backup_2019-02-12.zip.rans of=rescue.zip bs=1 skip=2168533 count=5713 seek=11889635
```

Alternative methodes

- Carving
  - Carving
    - .....
  - ZIP -FF
    - .....