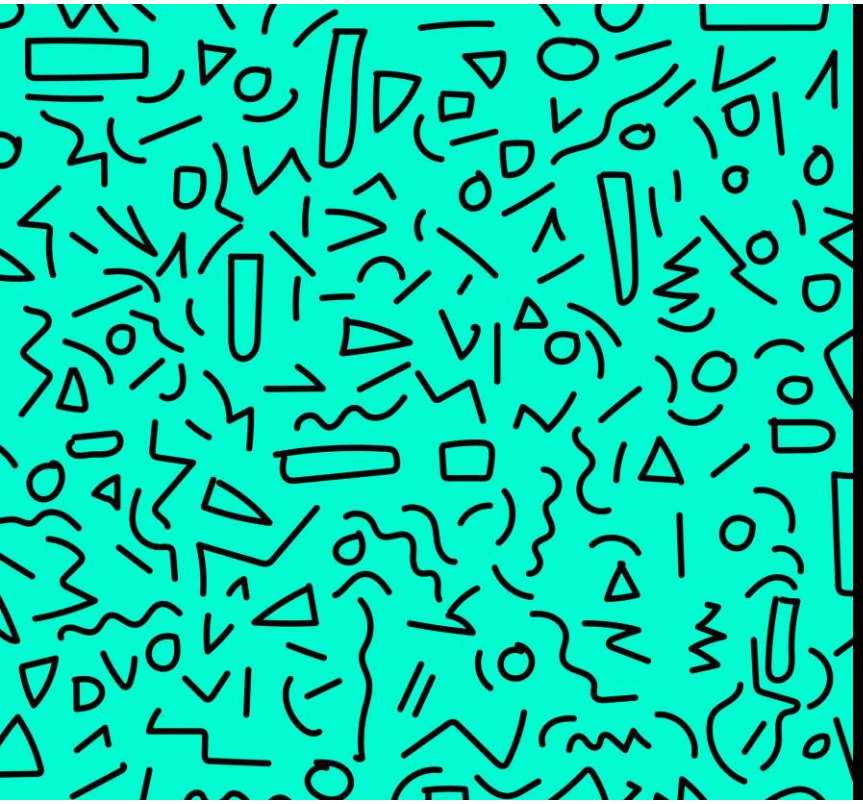


STEGANOGRAPHY IN ZIP FILE

Ignacy Szkudelski

SPIS TREŚCI

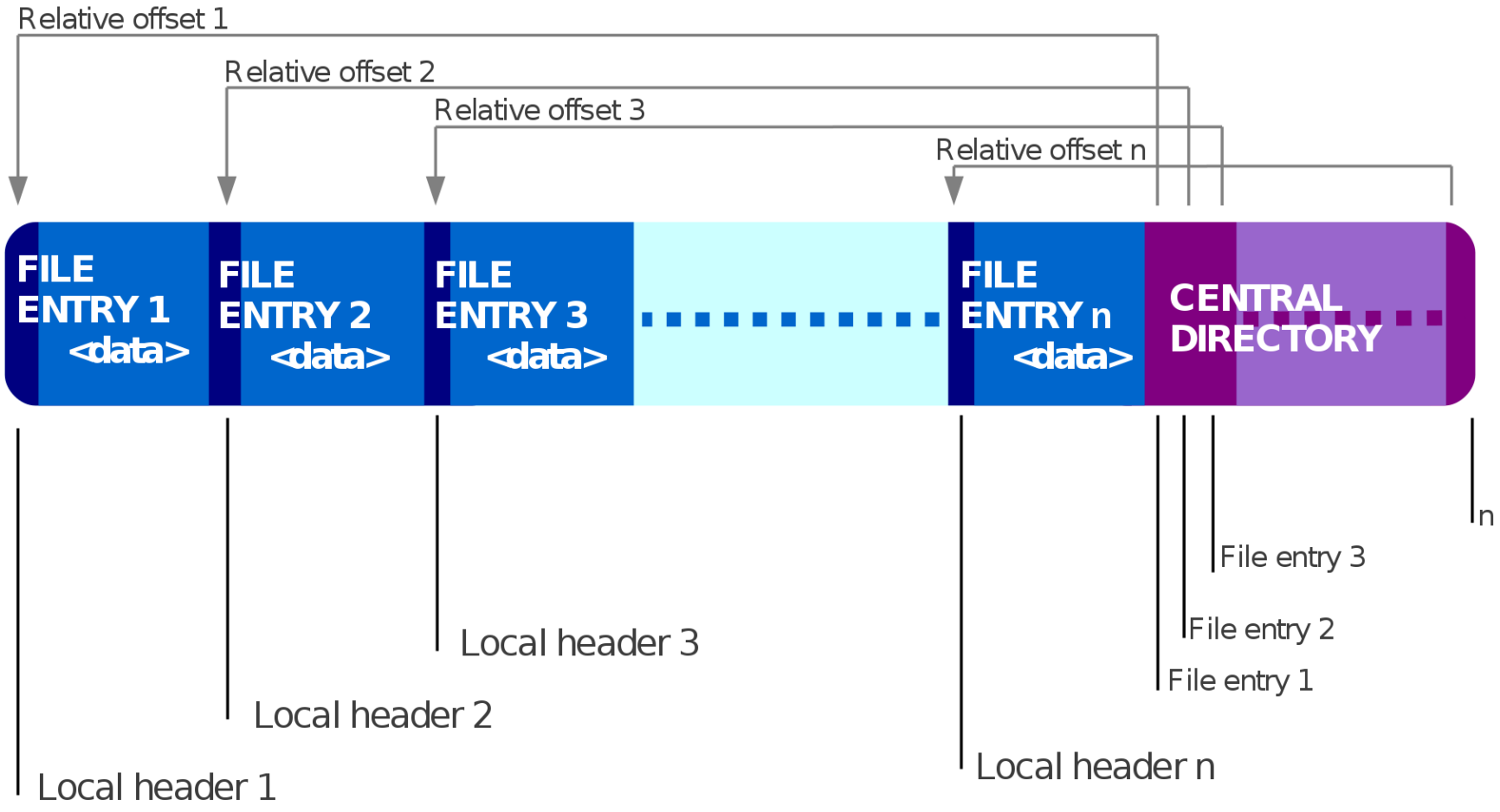
STEGANOGRAFIA

Ukrycie wiadomości tak aby nie było wiadomo że jest ona przesyłana

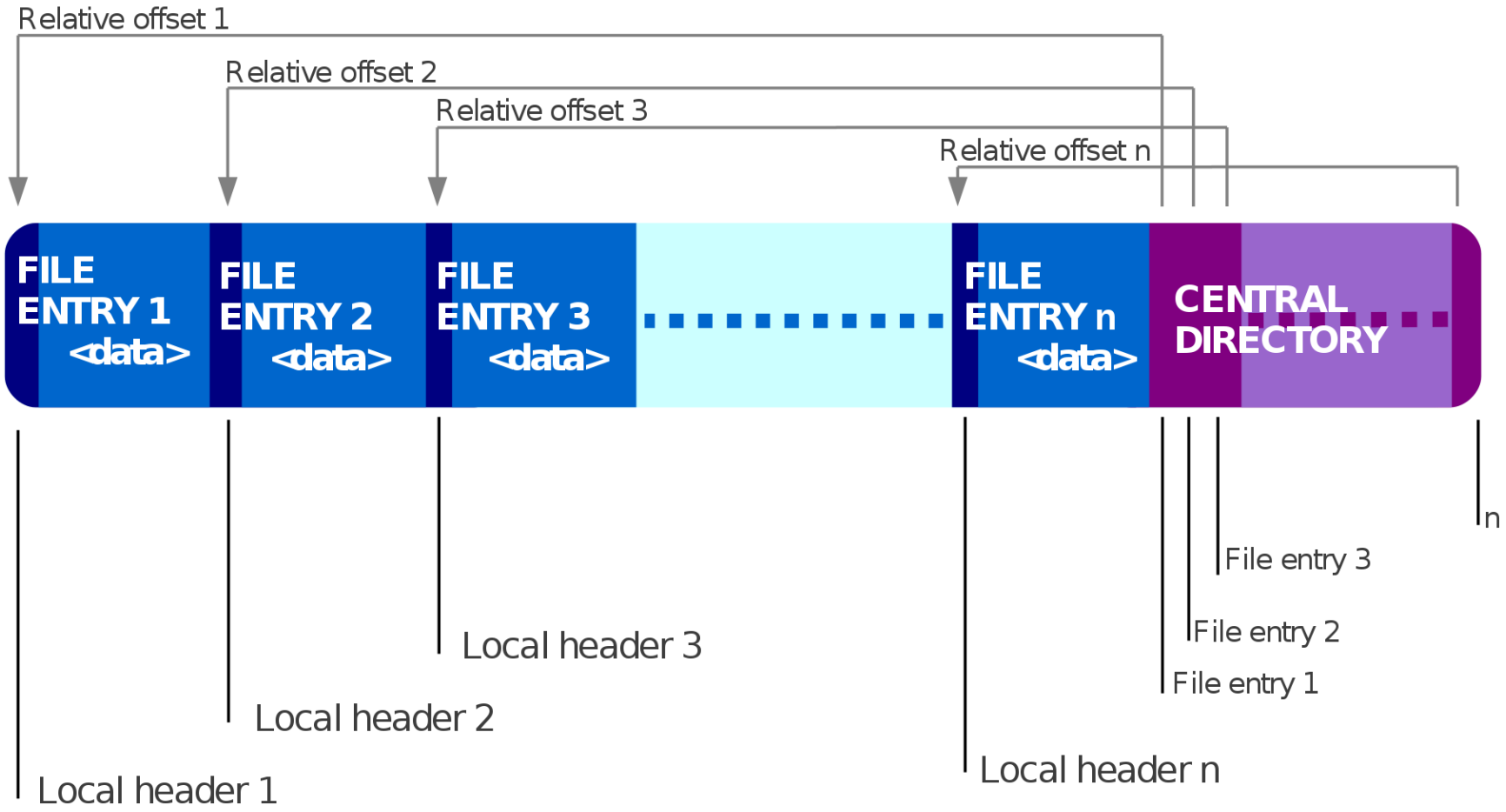
STEGANOGRAFIA

R	1	0	0	1	0	0	0	1
G	0	0	1	0	1	1	0	1
B	0	1	1	1	0	1	0	0

PLIK ZIP

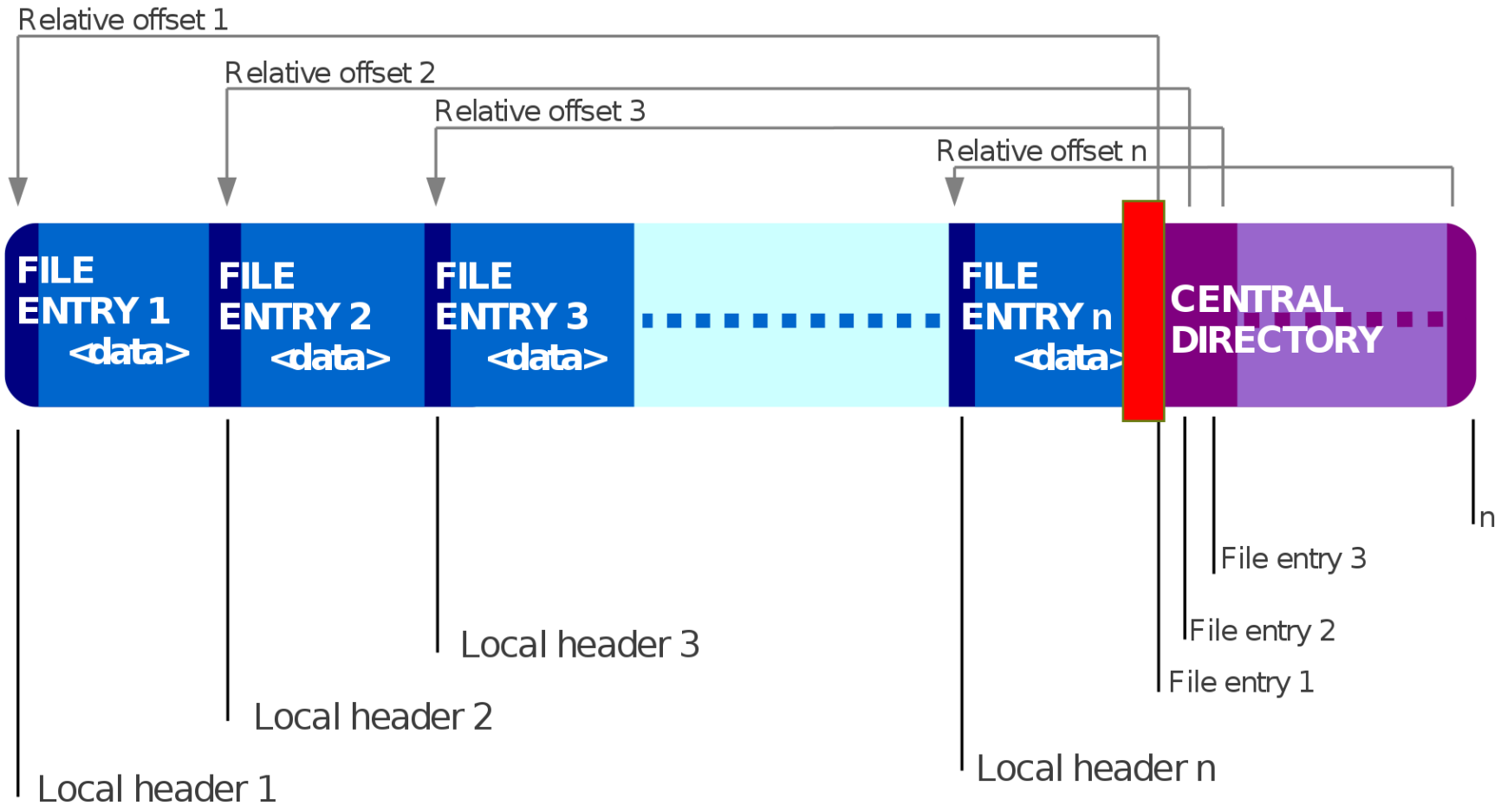

Relative offset 1
Relative offset 2
Relative offset 3
Relative offset n
FILE ENTRY 1 <data>
FILE ENTRY 2 <data>
FILE ENTRY 3 <data>
FILE ENTRY n <data>
CENTRAL DIRECTORY
Local header 1
Local header 2
Local header 3
Local header n
File entry 1
File entry 2
File entry 3
n

GDZIE UKRYĆ WIADOMOŚĆ?



1. GDZIE UKRYĆ WIADOMOŚĆ?
(METODA 1)

MIĘDZY PLIKAMI A KATALOGIEM CENTRALNYM



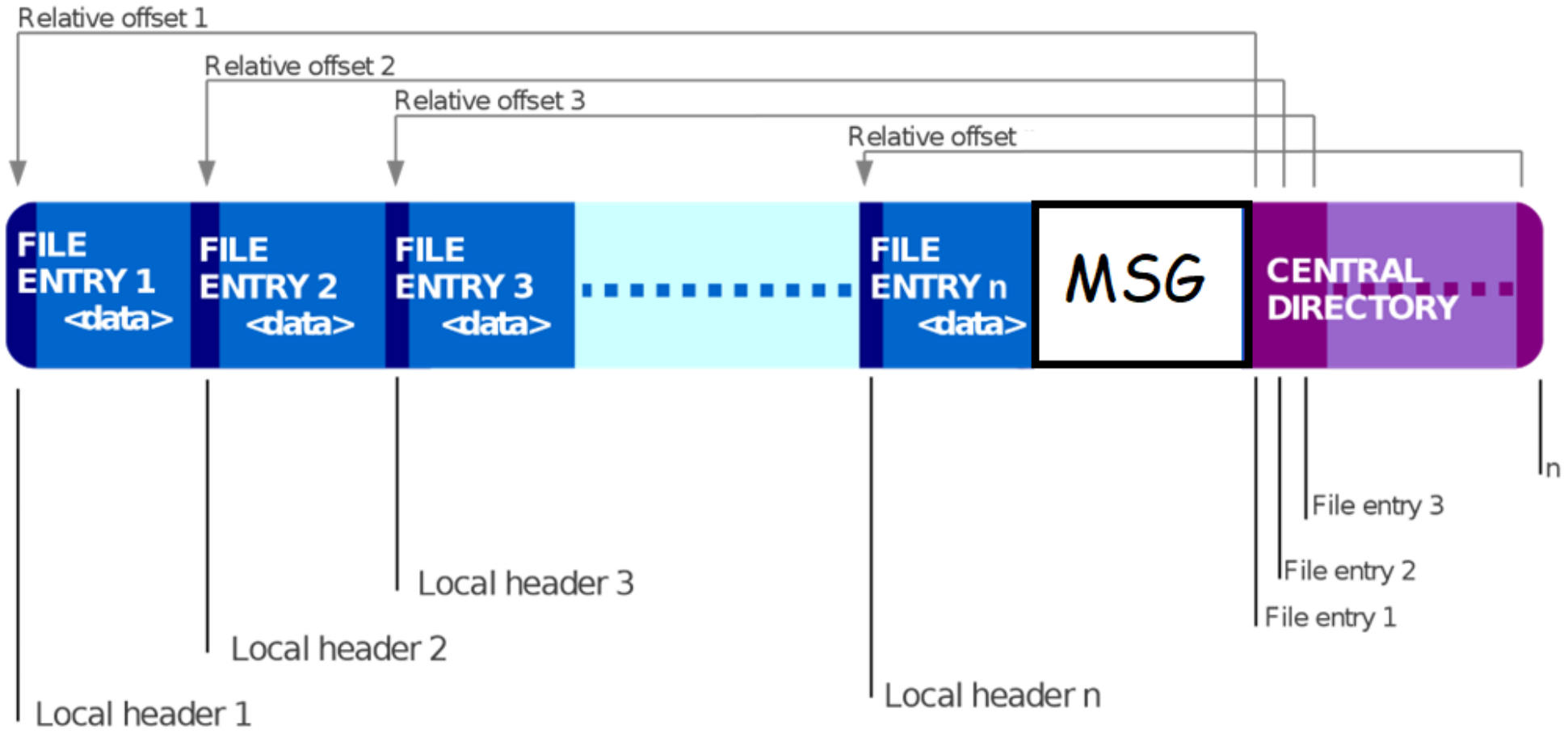
MIĘDZY PLIKAMI A KATALOGIEM CENTRALNYM

```
from zipfile import ZipFile
```

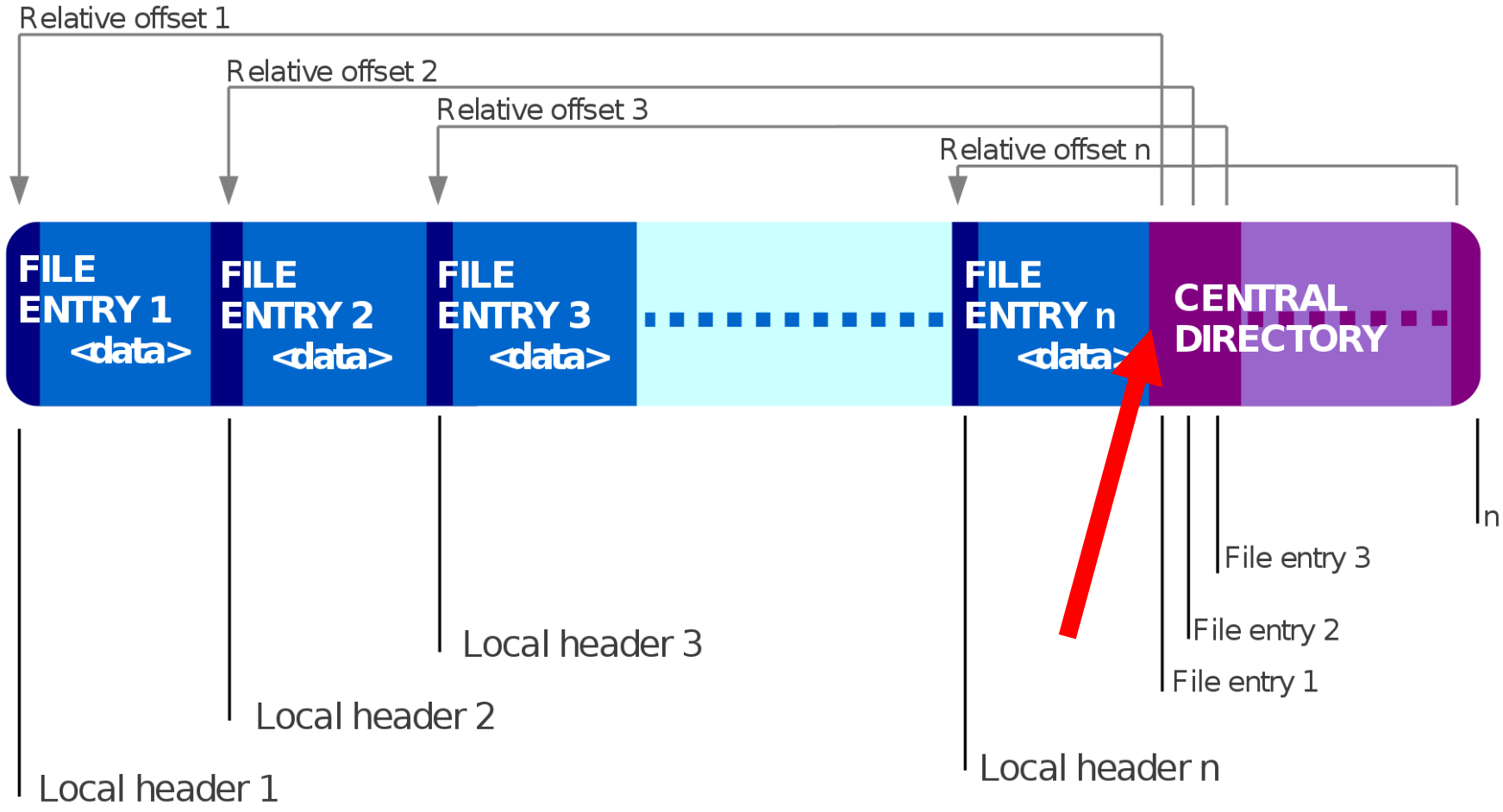
```
def close(self):
    """Close the file, and for mode 'w', 'x' and 'a' write the ending
    records."""
```

```
try:
    if self.mode in (
    'w', 'x', 'a') and self._didModify:  # write ending records
        with self._lock:
            if self._seekable:
                self.fp.seek(self.start_dir)
            self._write_end_record()
```

WSTRZYKNIĘCIE WIADOMOŚCI



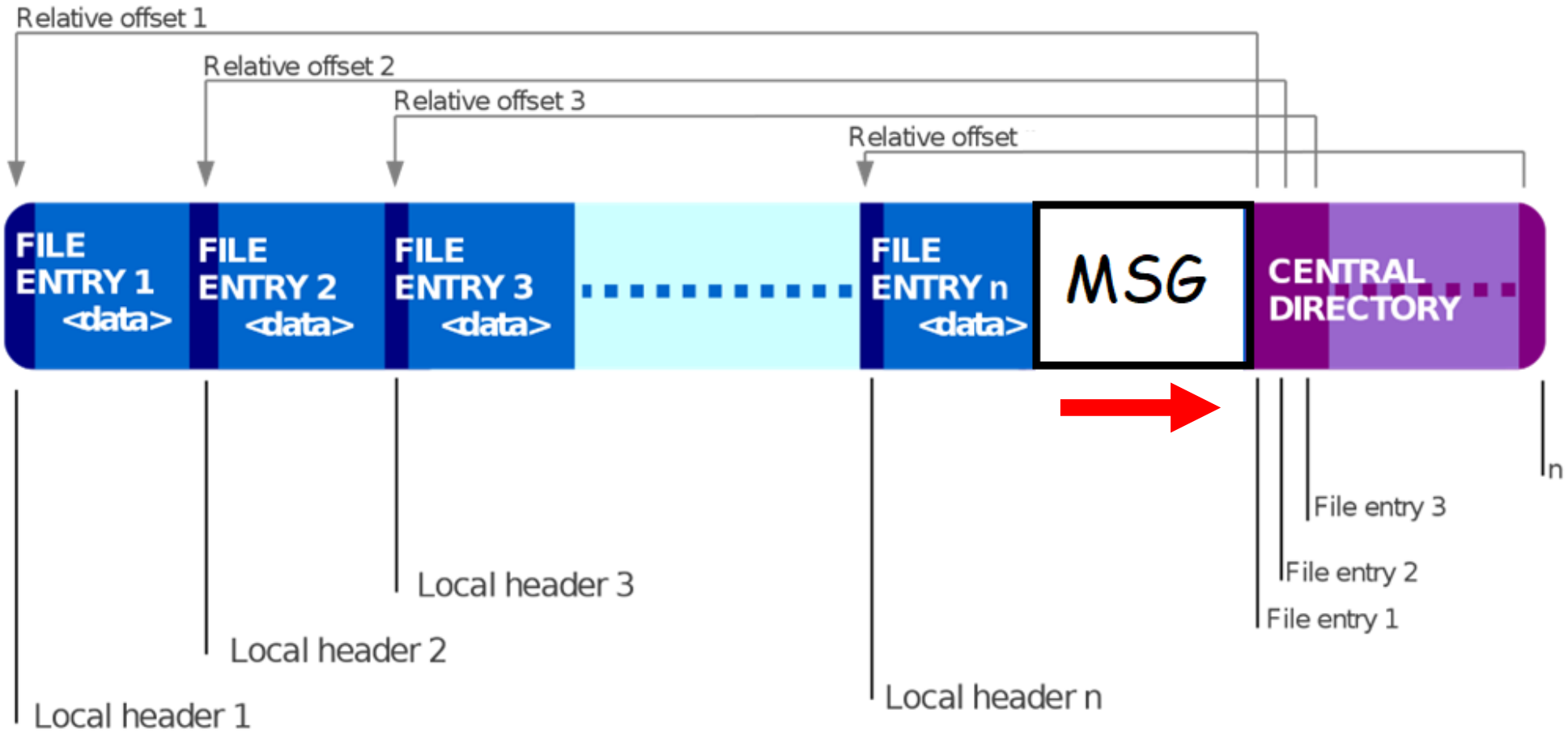
POCZĄTEK KATALOGU GŁÓWNEGO



POCZĄTEK KATALOGU GŁÓWNEGO

```
self.fp.seek(self.start_dir)
```

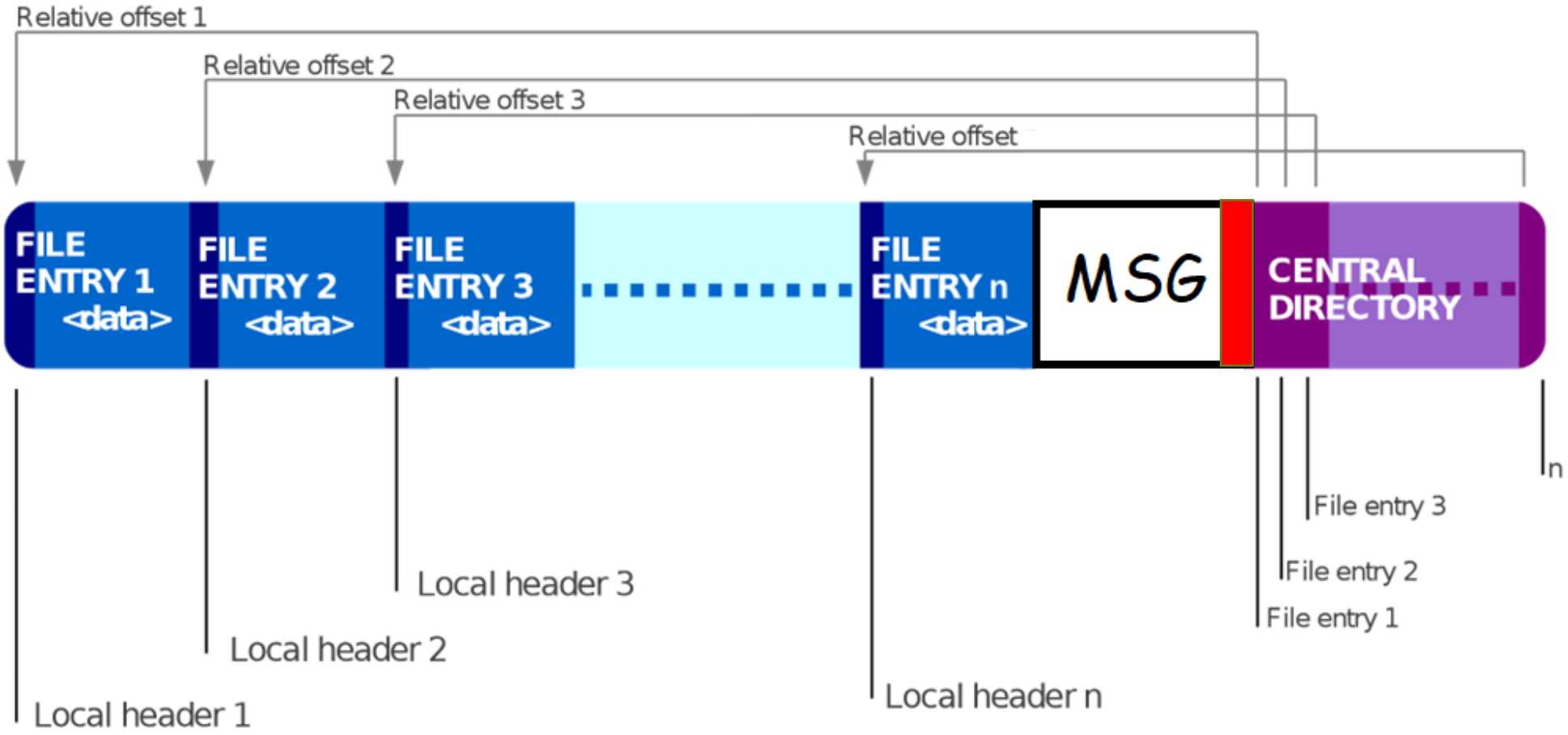
ZAPISANIE WIADOMOŚCI



ZAPISANIE WIADOMOŚCI

```
self.fp.write(self._message)
```

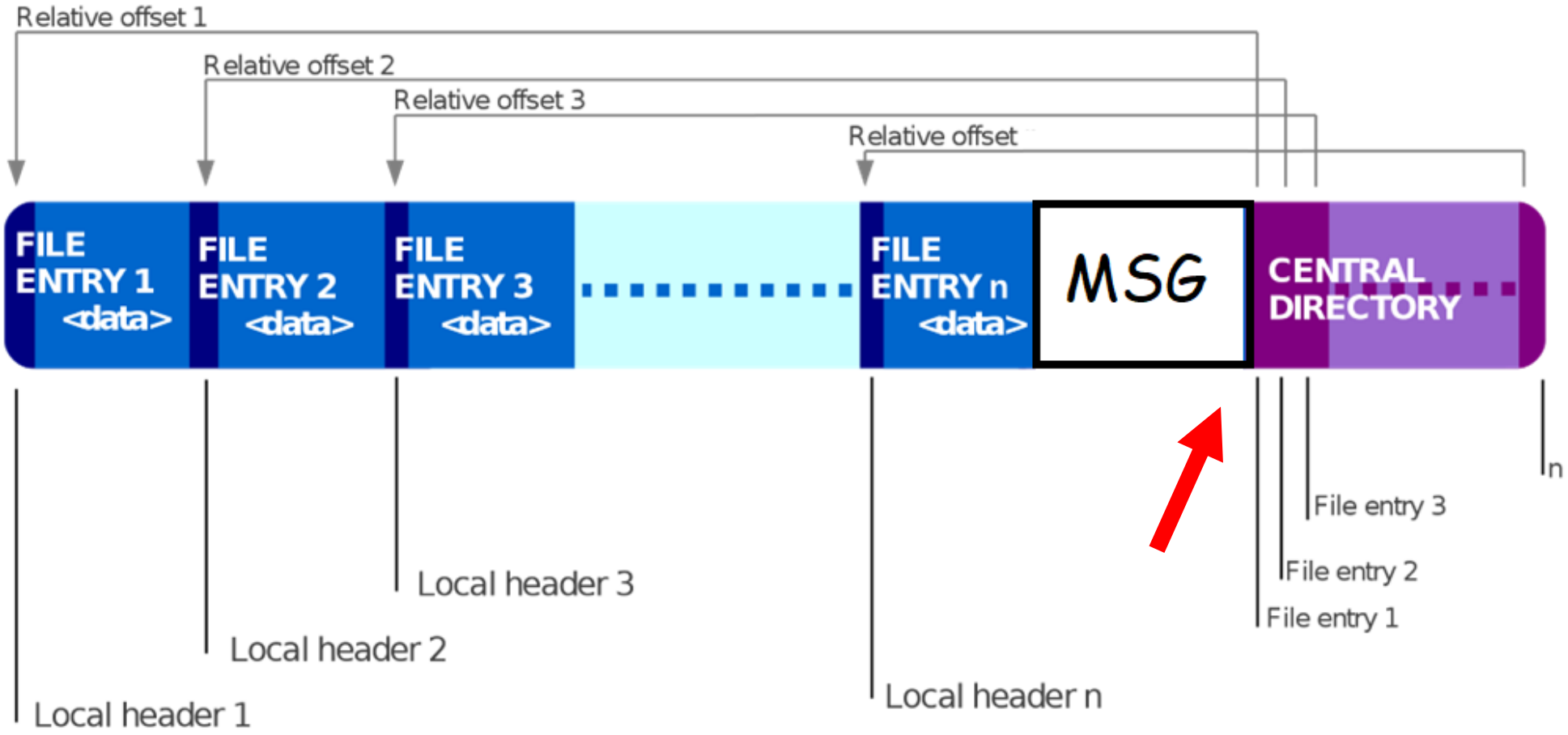
ZAPISANIE INFORMACJI O DŁUGOŚCI WIADOMOŚCI



ZAPISANIE INFORMACJI O DŁUGOŚCI WIADOMOŚCI

```
msg_len_info = str(msg_len).zfill(10)
self.fp.write(msg_len_info.encode(ENC))
```

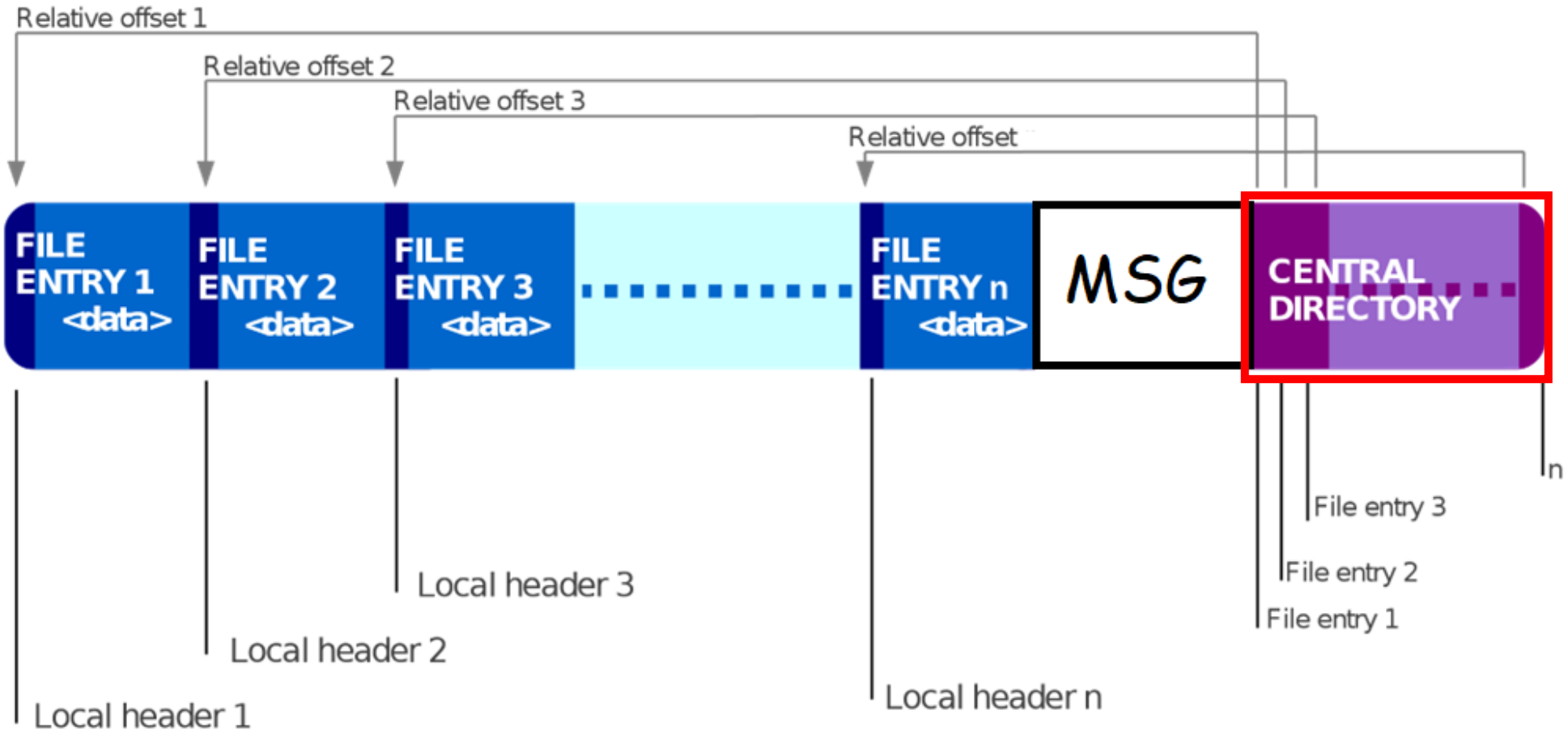
UAKTUALNIENIE WSKAŹNIKA POCZĄTKU KATALOGU GŁÓWNEGO



UAKTUALNIENIE WSKAŹNIKA POCZĄTKU KATALOGU GŁÓWNEGO

```
shift = len(self._message) + len(msg_len_info)
self.start_dir += shift
self.fp.seek(self.start_dir)
```

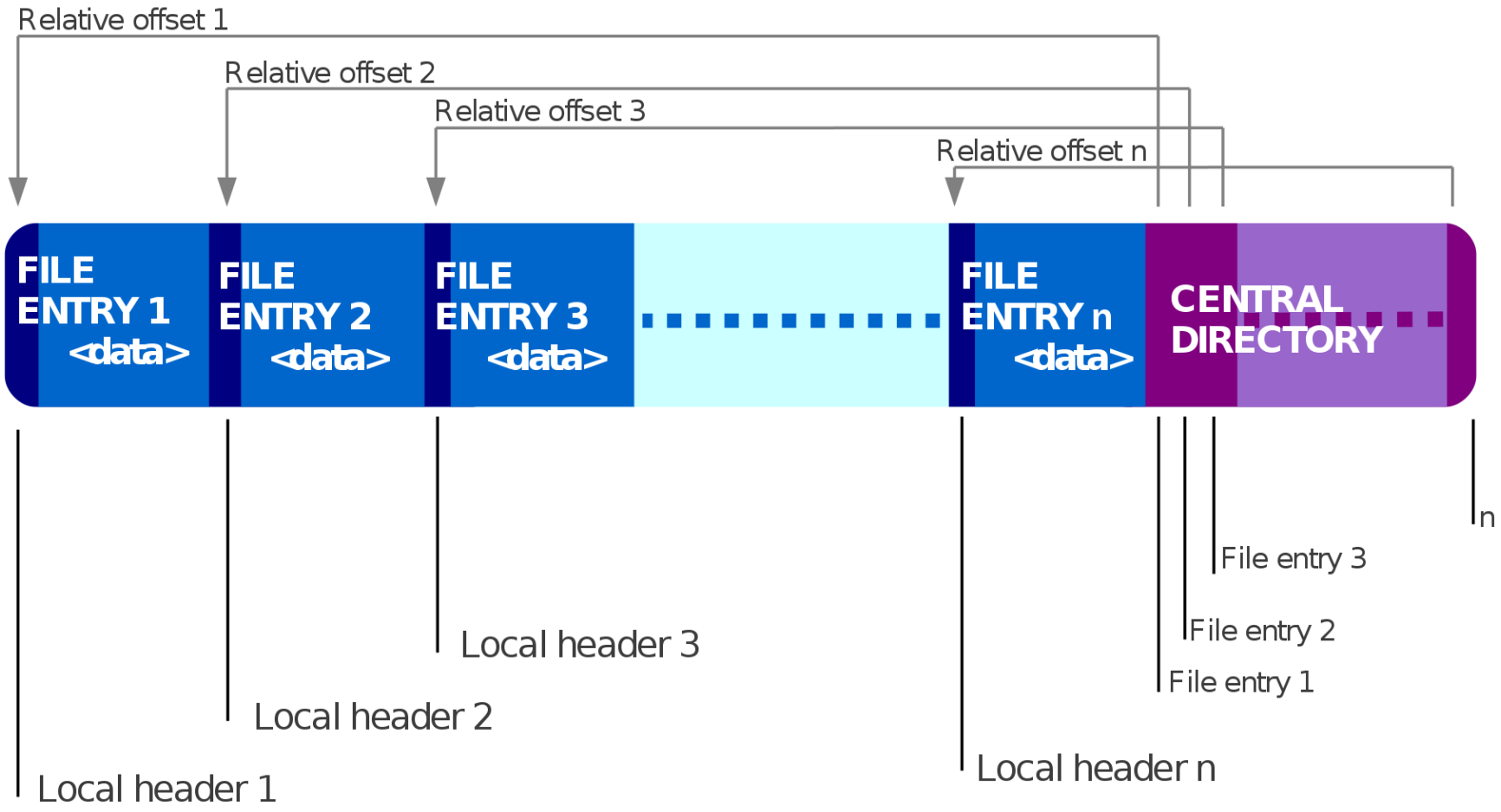
DOŁĄCZENIE KATALOGU GŁÓWNEGO



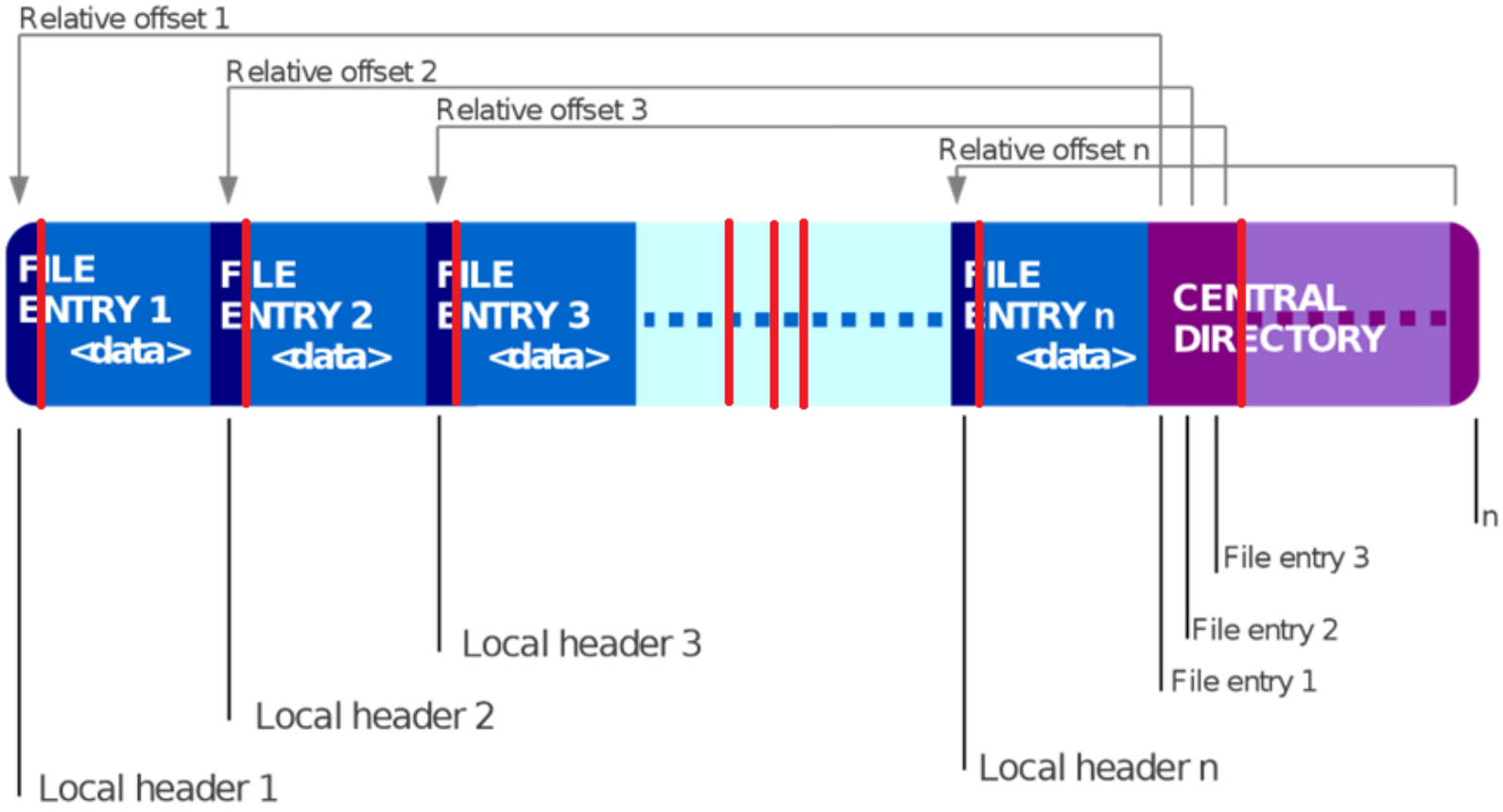
DOŁĄCZENIE KATALOGU GŁÓWNEGO

```
self._write_end_record()
```

2. GDZIE UKRYĆ WIADOMOŚĆ?
(METODA 2)



W KOMENTARZACH PLIKU ZIP



PODZIAŁ WIADOMOŚCI NA TYLE CZĘŚCI W ILE MIEJSC MOŻNA WPISAĆ KOMENTARZ

```python
def split_msg(msg, n):
    len_msg = len(msg)
    part_len = max(len_msg // n, 1)
    parts = [msg[i*part_len:i*part_len+part_len] for i in range(n-1)]
    parts.append(msg[(n-1)*part_len:])
    return parts
```

ZAPIANIE POSZCZEGÓLNYCH CZĘŚCI WIADOMOŚCI W KOMENTARZE

```
def hide_msg(file_name, msg: str):
    msg = bytes(msg, encoding=ENC)
    with zipfile.ZipFile(file_name, 'a') as zip_file:
        n_places = len(zip_file.namelist()) + 1
        msg_parts = split_msg(msg, n_places)
        for file_path, comment in zip(zip_file.namelist(), msg_parts):
            zip_file.getinfo(file_path).comment = comment

        zip_file.comment = msg_parts[-1]
```

3. UKRYCIE JAWNEGO TEKSTU ZMIANA FORMATOWANIA

UTF-8 → IBM039

```
>>> "WIADOMOSC MA ALE".encode("utf-8")
b'WIADOMOSC MA ALE'
>>> "WIADOMOSC MA ALE".encode("IBM039")
b'\xe6\xc9\xc1\xc4\xd6\xd4\xd6\xe2\xc3@\xd4\xc1@\xc1\xd3\xc5'
```

4. URUCHAMIANIE PLIKU EXE UKRYTEGO W PLIKU ZIP

UKRYWANIE PLIKU EXE

```
def hide_exe_in_zip(exe_name, zip_name, method):
    bin_exe = _read_exe(exe_name)
    str_exe_base64 = base64.b64encode(bin_exe)
    str_exe_ibm039 = str_exe_base64.decode(ENC)
    hide_msg(zip_name, str_exe_ibm039, method)
```

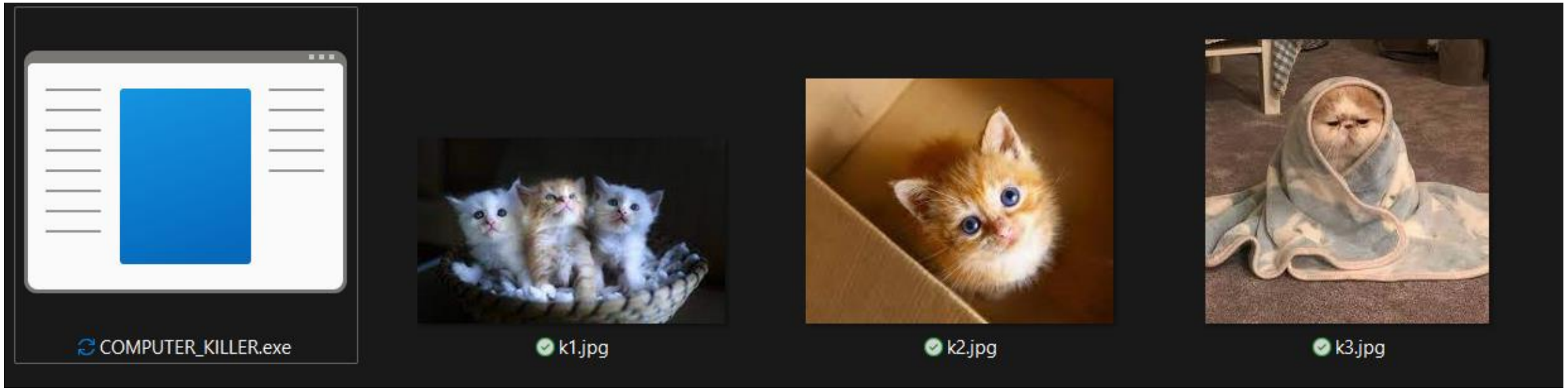
ODCZYTANIE UKRYTEGO PLIKU EXE

```
def _load_exe_from_zip(zip_name, method):
    str_exe = show_msg(zip_name, method)
    bytes_exe = str_exe.encode(ENC)
    bin_exe = _decode_base64_string(bytes_exe)
    return bin_exe
```

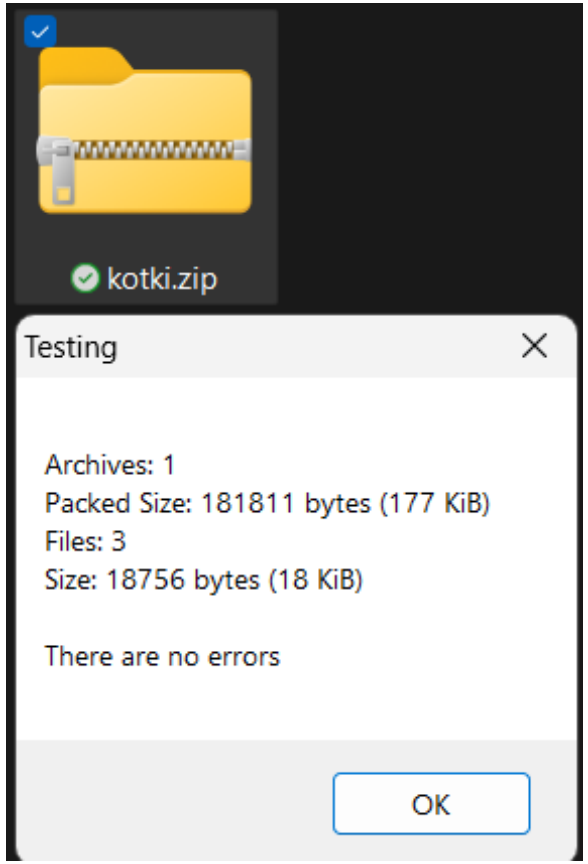
WYKONANIE PLIKU EXE

```
def run_exe_from_zip(zip_name, method):
    exe_bytes = _load_exe_from_zip(zip_name, method)
    with tempfile.NamedTemporaryFile(suffix='.exe', delete=False) as temp_file:
        temp_file.write(exe_bytes)
    subprocess.run(temp_file.name, shell=False)
    temp_file.close()
```

5. SKAN PLIKU Z PLIKIEM EXE



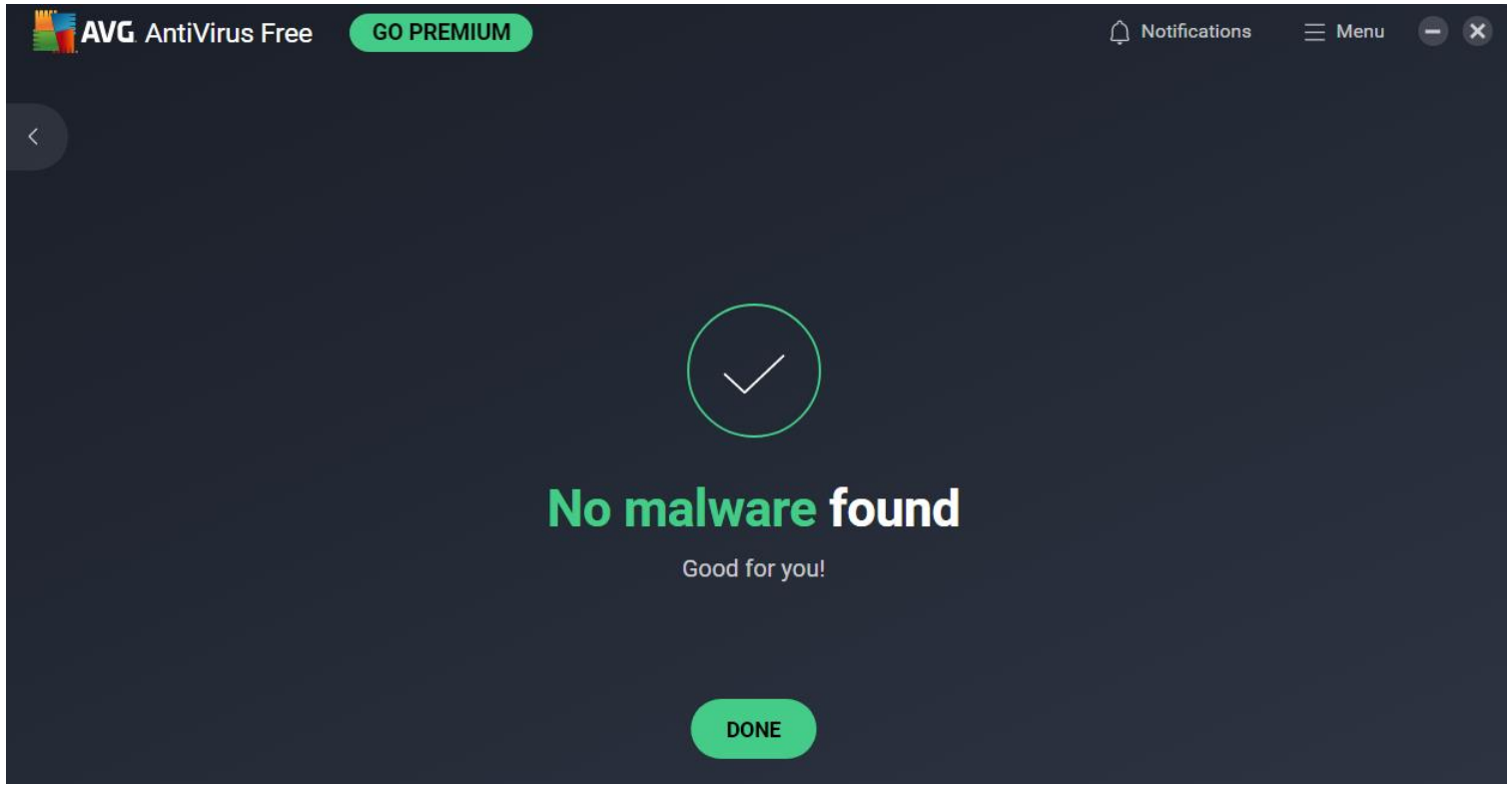
7-ZIP



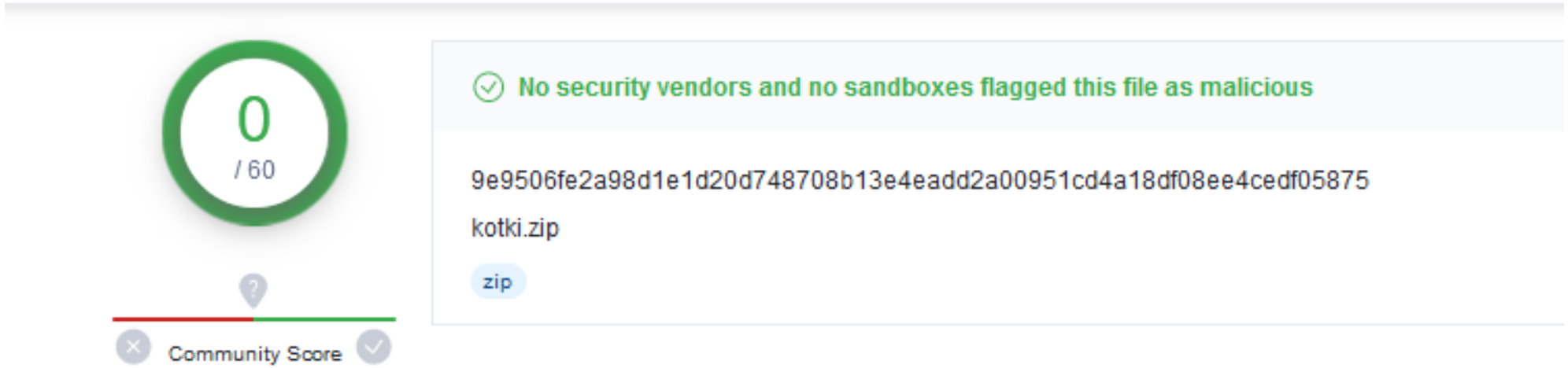
Size	18 756
Packed Size	18 663
Folders	0
Files	3
CRC	F4F542E3

Path	C:\Users\ignsz\OneDrive\STUDIA\MK\Steganography\files\kotki.zip
Type	zip
Physical Size	181 811
Comment	@¦‰_˜_@©•'-¦

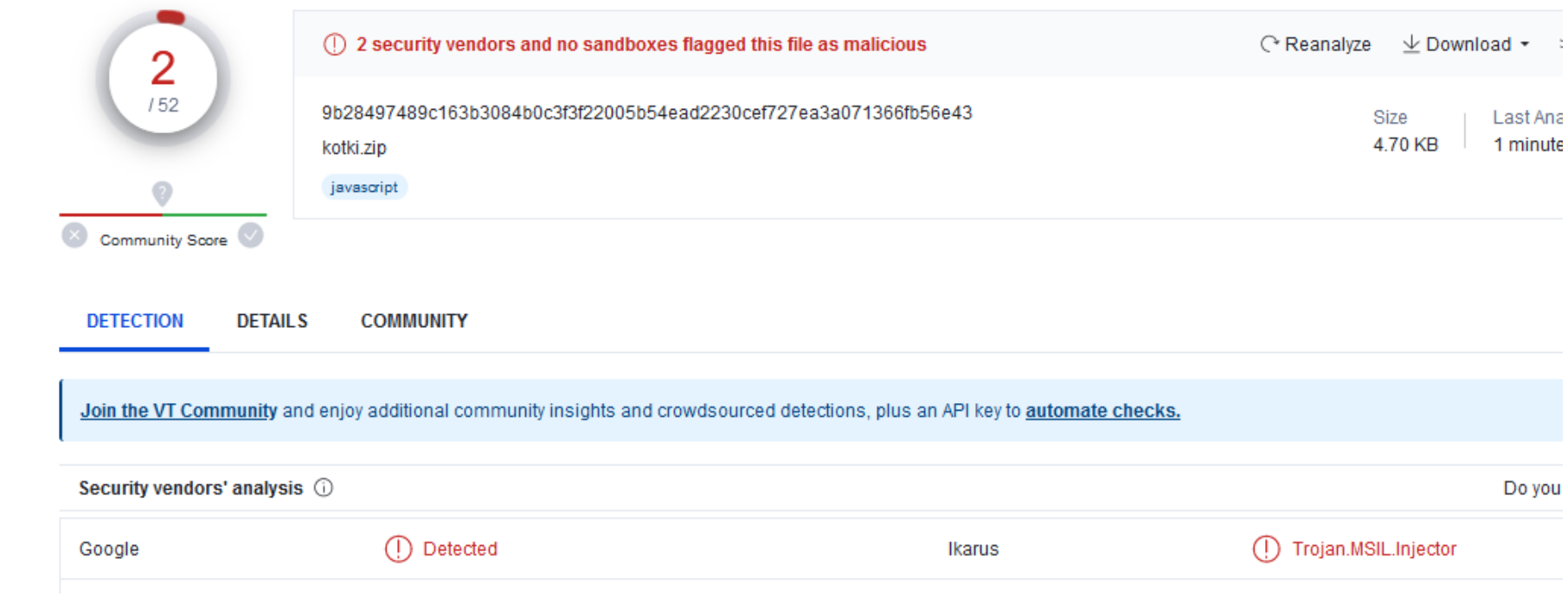
AVG


AVG AntiVirus Free
GO PREMIUM
Notifications
Menu
No malware found
Good for you!
DONE

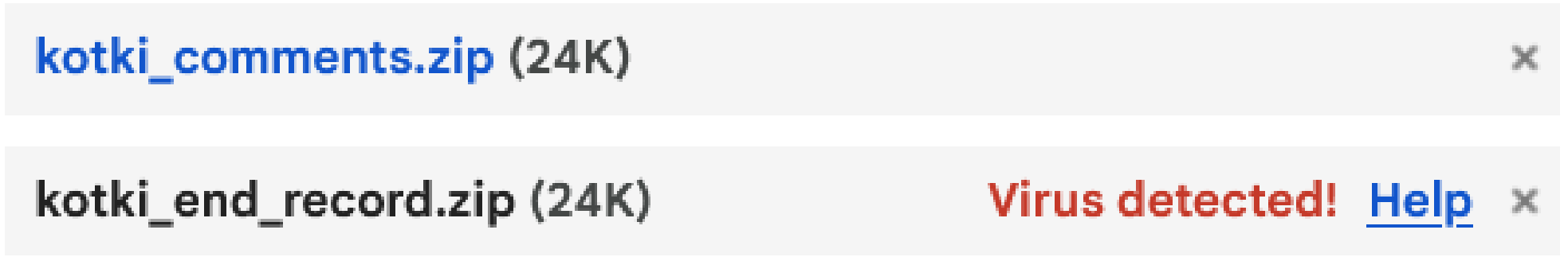
VIRUSTOTAL – COMMENTS



VIRUSTOTAL – END RECORD

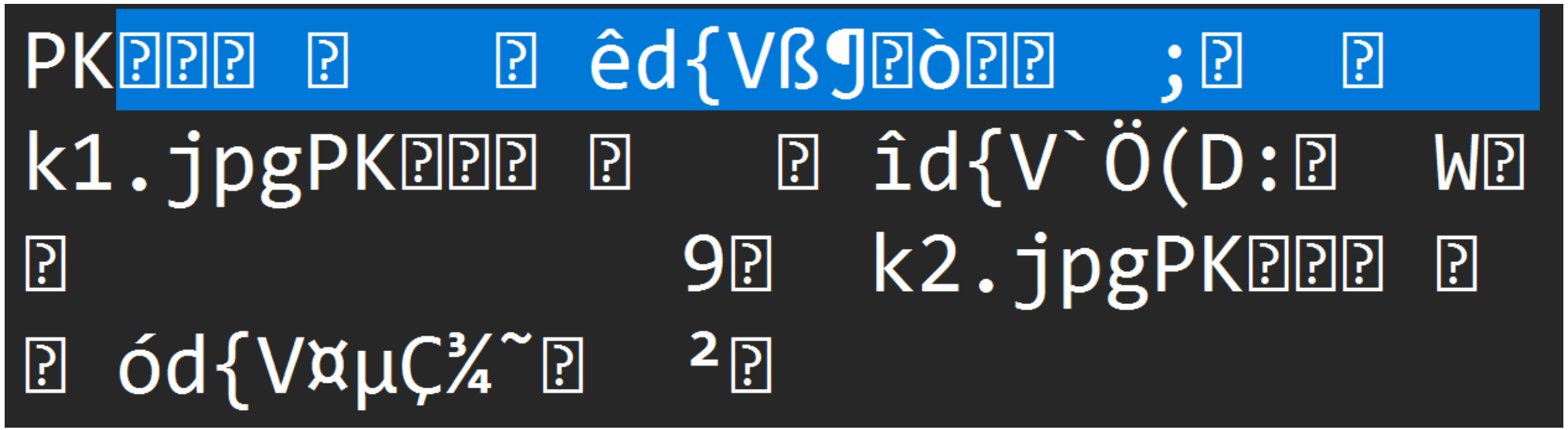


GMAIL

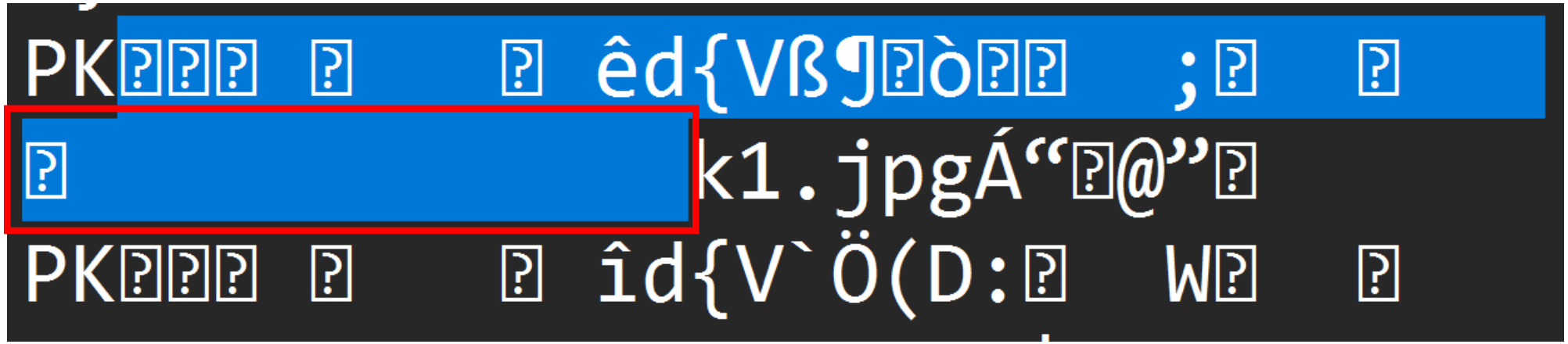

kotki_comments.zip (24K)
kotki_end_record.zip (24K)
Virus detected!
Help

6. PREZENTACJA DZIAŁANIA

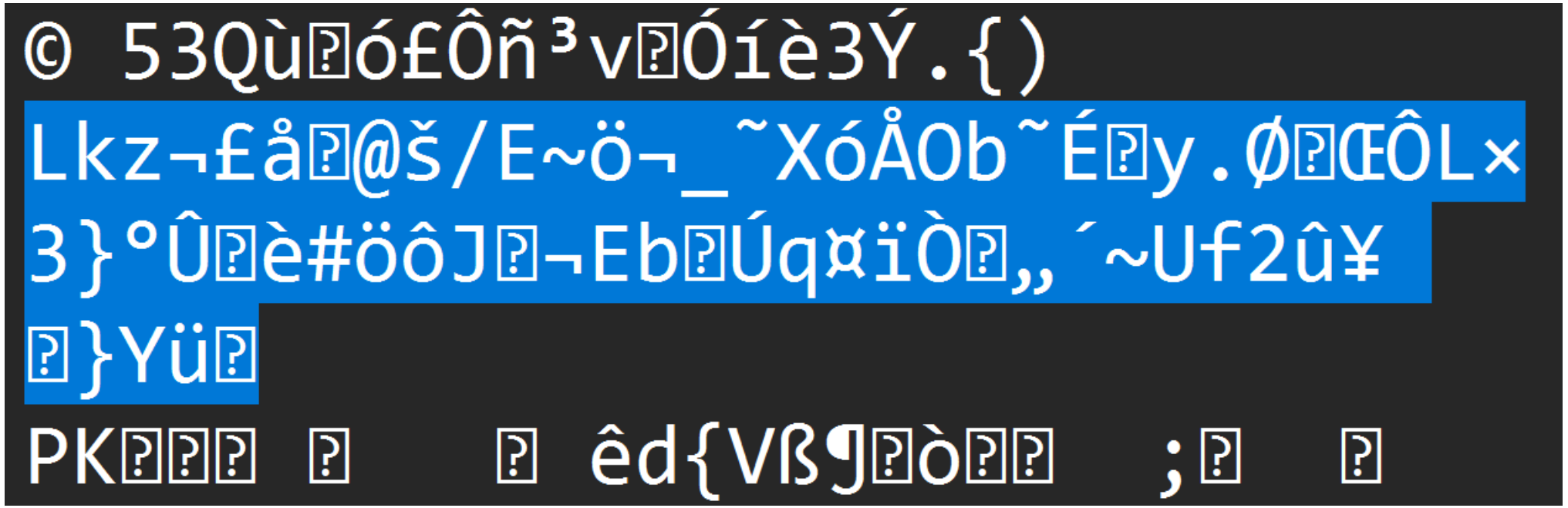
W BAJTACH - ORYGINALNY



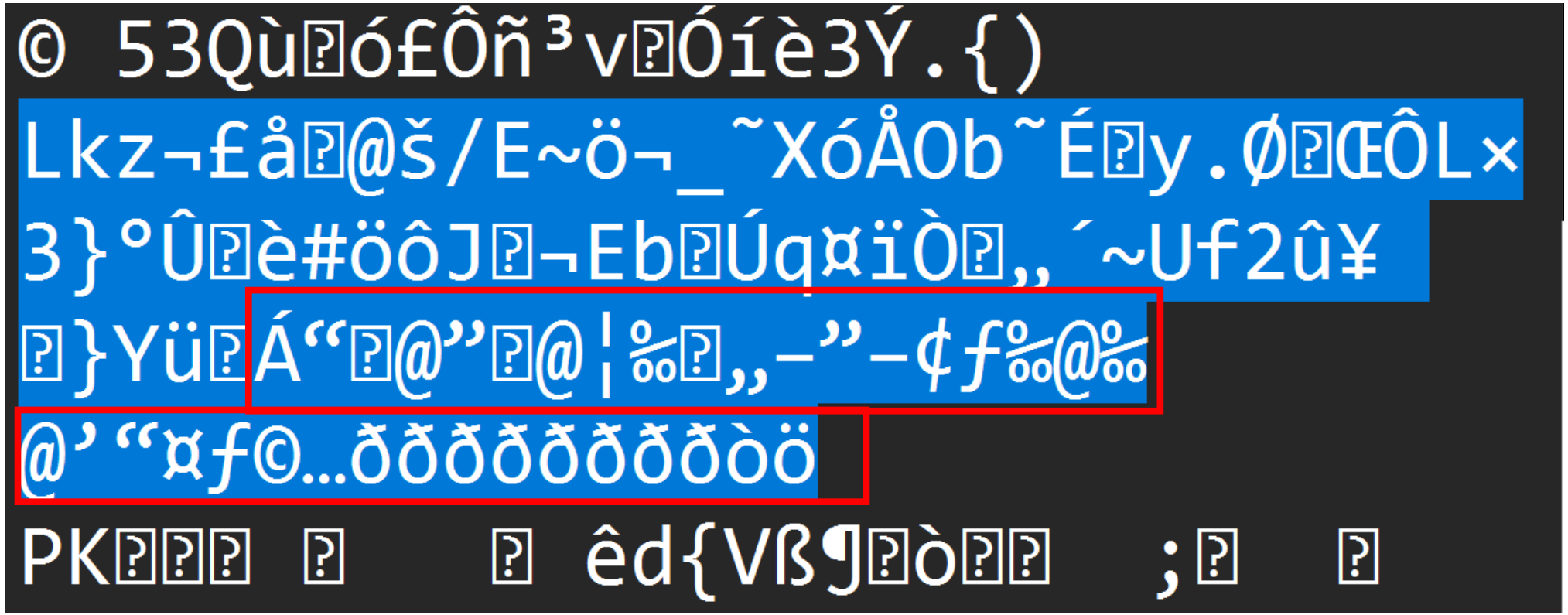
W BAJTACH – Z KOMENTARZM



W BAJTACH - ORYGINALNY



W BAJTACH – Z DODATKIEM PRZED REKORDEM KOŃCOWYM



DZIĘKI ZA UWAGĘ