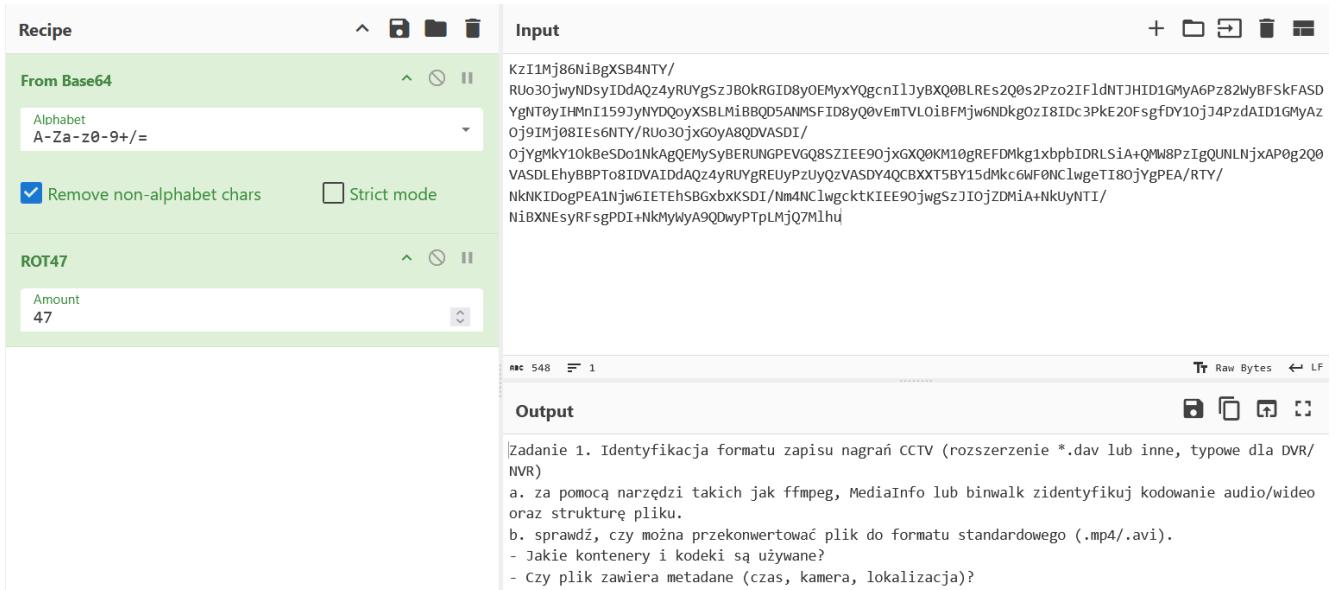


<b>POLITECHNIKA WROCŁAWSKA</b>  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
<b>CBESI0053G Informatyka śledcza – Laboratorium 12</b>	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 26.05.2025	
Data oddania sprawozdania: 01.06.2025	

## 1. Cel ćwiczenia

Analiza pliku .dav.

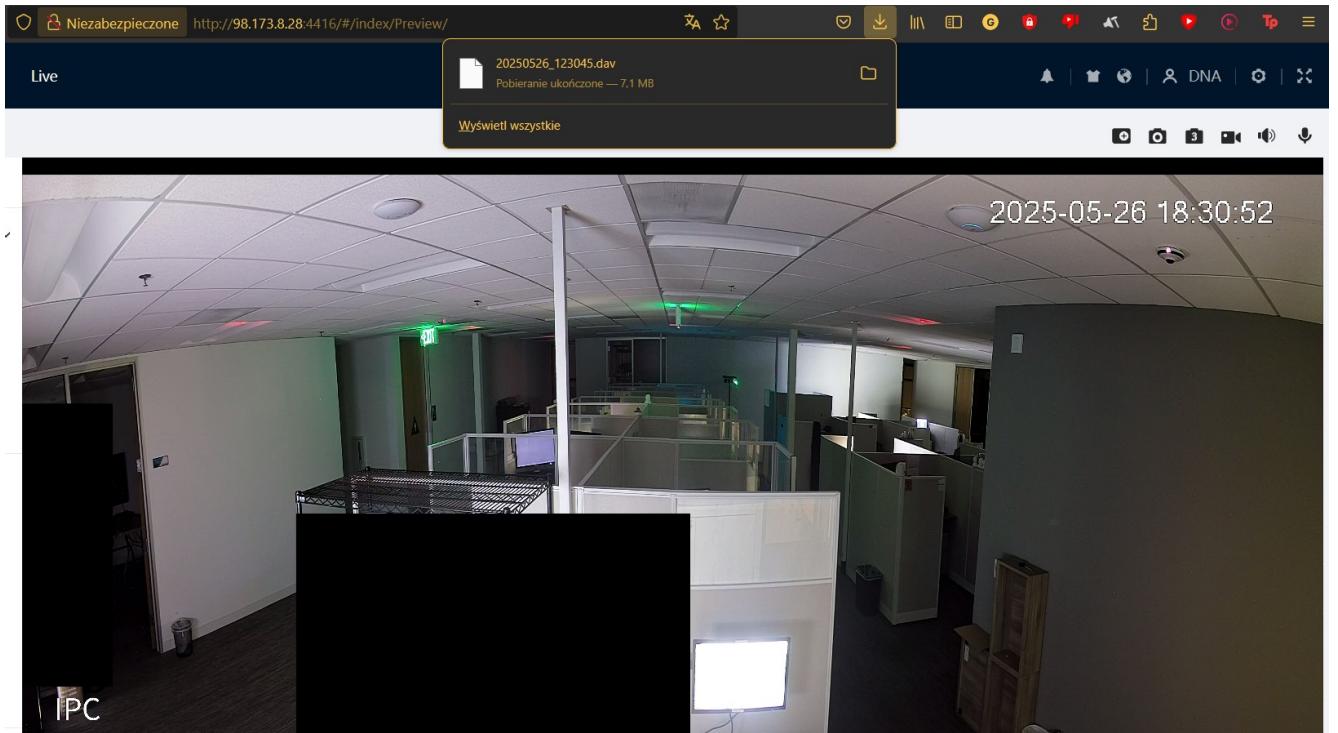
## 2. Rozszyfrowanie instrukcji laboratoryjnej



Rysunek 1: CyberChef

## 3. Realizacja zadań laboratoryjnych

**Zadanie 1. Identyfikacja formatu zapisu nagrań CCTV (rozszerzenie \*.dav lub inne, typowe dla DVR/NVR)**



Rysunek 2: pobranie pliku .dav za pośrednictwem strony [https://dahuawiki.com/Live\\_Demo](https://dahuawiki.com/Live_Demo)

a) za pomocą narzędzi takich jak ffmpeg, MediaInfo lub binwalk zidentyfikuj kodowanie audio/video oraz strukturę pliku.

```
(kali㉿kali)-[~/Desktop]
$ exiftool 20250526_123045.dav
ExifTool Version Number : 13.00
File Name : 20250526_123045.dav
Directory : .
File Size : 7.5 MB
File Modification Date/Time : 2025:05:26 06:41:56-04:00
File Access Date/Time : 2025:05:26 06:44:12-04:00
File Inode Change Date/Time : 2025:05:26 06:41:56-04:00
File Permissions : -rwxrwx—
Error : Unknown file type

(kali㉿kali)-[~/Desktop]
$ binwalk 20250526_123045.dav
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
```

Rysunek 3: wynik exiftool i binwalk

```
(kali㉿kali)-[~/Desktop]
$ mediainfo 20250526_123045.dav
General
Complete name : 20250526_123045.dav
Format : HEVC
Format/Info : High Efficiency Video Coding
File size : 7.11 MiB
Frame rate : 25.000 FPS
FileExtension_Invalid : hevc h265 265

Video
Format : HEVC
Format/Info : High Efficiency Video Coding
Format profile : Main@L6@Main
Width : 4 096 pixels
Height : 1 800 pixels
Display aspect ratio : 2.25:1
Frame rate : 25.000 FPS
Color space : YUV
Chroma subsampling : 4:2:0
Bit depth : 8 bits
```

Rysunek 4: wynik mediainfo

```
(kali㉿kali)-[~/Desktop]
└─$ ffmpeg -i 20250526_123045.dav
ffmpeg version 7.1-4 Copyright (c) 2000-2024 the FFmpeg developers
  built with gcc 14 (Debian 14.2.0-17)
configuration: --prefix=/usr --extra-version=4 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu --incdir=/usr/include/x86_64-linux-gnu --arch=amd64
--enable-gpl --disable-stripping --disable-libmfx --enable-gnutls --enable-libaom --enable-libbs2b --enable-libcdio --enable-libc
odec2 --enable-libdavid --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi --enable-libglslang --enable-libgme --enable-libgsm
--enable-libharfbuzz --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopennpt --enable-libopus --enable-librubberband --enable-libshine
--enable-libsnappy --enable-libsoxr --enable-libspeex --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libw
ebp --enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzimg --enable-openal --enable-opengl --enable-sndio --enable-libvpl --
enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint --enable-frei0r --enable-ladspa --enable-libbluray --enable-libcaca --enable-libdvd
nav --enable-libdvdread --enable-libjack --enable-libpulse --enable-librabbitmq --enable-librist --enable-libsrt --enable-libssh --enable-libstvav1 --enable-l
ibx264 --enable-libzmq --enable-libzvbi --enable-lv2 --enable-sdl2 --enable-libplacebo --enable-libravie --enable-pocketsphinx --enable-librsvg --enable-libj
pg --enable-shared

libavutil      59. 39.100 / 59. 39.100
libavcodec     61. 19.100 / 61. 19.100
libavformat    61.  7.100 / 61.  7.100
libavdevice    61.  3.100 / 61.  3.100
libavfilter     10.  4.100 / 10.  4.100
libswscale      8.  3.100 /  8.  3.100
libswresample   5.  3.100 /  5.  3.100
libpostproc    58.  2.100 / 58.  2.100

[dhav @ 0x5641457fc40] Unknown type: B8, skipping rest of header.
Last message repeated 127 times
Input #0, dhav, from '20250526_123045.dav':
  Duration: 00:00:18.00, start: 1748284191.000000, bitrate: 3314 kb/s
  Stream #0:0: Video: hevc (Main), yuv420p(tv), 4096x1800, 25 fps, 25 tbr, 1k tbn
At least one output file must be specified
```

Rysunek 5: wynik ffmpeg

Komentarz: Narzędzia *binwalk* oraz *exiftool* nie podają praktycznie żadnych użytecznych informacji o pliku, poza jego rozmiarem (*exiftool*). Narzędzia *mediainfo* oraz *ffmpeg* zgodnie informują o:

- FPS = 25
- Kodowaniu wideo – HEVC
- Rozdzielczości = 2096\*1800

Ponadto *mediainfo* informuje o modelu barw: YUV a *ffmpeg* o czasie trwania nagrania: 18s.

Plik nie posiada znanej sygnatury: „DHA”

**b) sprawdź, czy można przekonwertować plik do formatu standardowego (.mp4/.avi).**

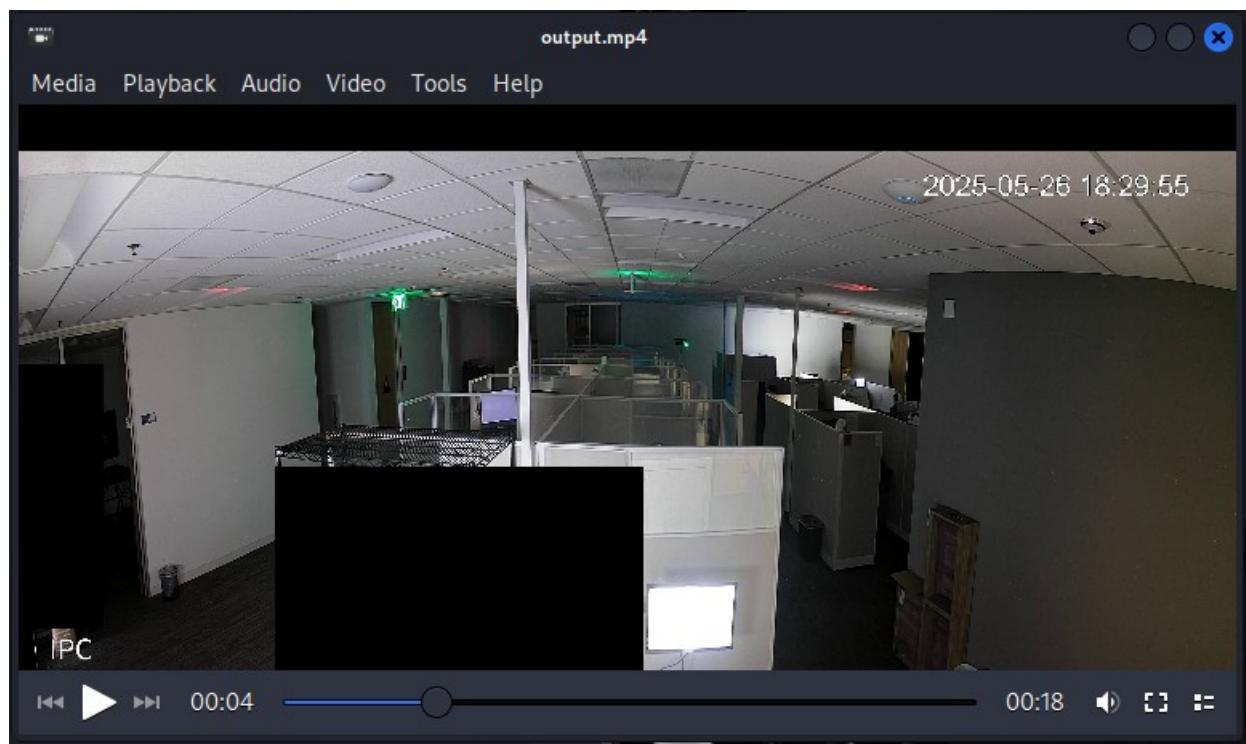
```

kali@kali: ~/Desktop
File Actions Edit View Help
└$ ffmpeg -i 20250526_123045.dav -c copy output.mp4
ffmpeg version 7.1-4 Copyright (c) 2000-2024 the FFmpeg developers
  built with gcc 14 (Debian 14.2.0-17)
  configuration: --prefix=/usr --extra-version=4 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu --incdir=/usr/include/x86_64-linux-gnu --arch=amd64 --enable-gpl --disable-stripping --disable-libmfx --disable-omx --enable-gnutls --enable-libaom --enable-libass --enable-libbs2b --enable-libcdio --enable-libcodec2 --enable-libdavid --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi --enable-libglslang --enable-libgme --enable-libgsms --enable-libharfbuzz --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopenmpt --enable-libopus --enable-librubberband --enable-libshine --enable-libsnappy --enable-libsoxr --enable-libspeex --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libwebp --enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzimg --enable-openal --enable-opengl --enable-sndio --enable-libvpl --enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint --enable-frei0r --enable-ladspa --enable-libbluray --enable-libcaca --enable-libdvda --enable-libdvdread --enable-libjack --enable-libpulse --enable-librabitmq --enable-librist --enable-libsrt --enable-libssh --enable-libsvtav1 --enable-libx264 --enable-libzmq --enable-libzvbi --enable-lv2 --enable-sdl2 --enable-libplacebo --enable-libravie --enable-pocketsphinx --enable-librsvg --enable-libjxl --enable-shared
libavutil      59. 39.100 / 59. 39.100
libavcodec     61. 19.100 / 61. 19.100
libavformat    61.  7.100 / 61.  7.100
libavdevice    61.  3.100 / 61.  3.100
libavfilter     10.  4.100 / 10.  4.100
libswscale      8.  3.100 /  8.  3.100
libswresample   5.  3.100 /  5.  3.100
libpostproc    58.  3.100 / 58.  3.100
[dhav @ 0x5627c24e8cc0] Unknown type: B8, skipping rest of header.
Last message repeated 127 times
Input #0, dhav, from '20250526_123045.dav':
  Duration: 00:00:18.00, start: 1748284191.000000, bitrate: 3314 kb/s
  Stream #0:0: Video: hevc (Main), yuv420p(tv), 4096x1800, 25 fps, 25 tbr, 1k tbn
File 'output.mp4' already exists. Overwrite? [y/N] ■

```

Rysunek 6: konwersja pliku .dat na .mp4

Komentarz: Tak, plik można przekonwertować do formatu standardowego programem ffmpeg.



Rysunek 7: plik .mp4

- Jakie kontenery i kodeki są używane?

```
Input #0, mov,mp4,m4a,3gp,3g2,mj2, from 'output.mp4':
  Metadata:
    major_brand     : isom
    minor_version   : 512
    compatible_brands: isomiso2mp41
    encoder         : Lavf61.7.100
  Duration: 00:00:18.00, start: 0.000000, bitrate: 3307 kb/s
  Stream #0:0[0x1](und): Video: hevc (Main) (hev1 / 0x31766568), yuv420p(tv),
  4096x1800, 3306 kb/s, 15.44 fps, 25 tbr, 16k tbn (default)
    Metadata:
      handler_name   : VideoHandler
      vendor_id      : [0][0][0][0]
At least one output file must be specified
```

Rysunek 8: wynik `ffmpeg -i output.mp4`

Kontener: MP4 (isom)

Kodek: HEVC

- Czy plik zawiera metadane (czas, kamera, lokalizacja)?

Plik `output.mp4` nie zawiera danych na temat czasu, kamery ani lokalizacji.

```
Poster Time : 0 s
Selection Time : 0 s
Selection Duration : 0 s
Current Time : 0 s
Next Track ID : 2
Track Header Version : 0
Track Create Date : 0000:00:00 00:00:00
Track Modify Date : 0000:00:00 00:00:00
Track ID : 1
Track Duration : 18.00 s
Track Layer : 0
Track Volume : 0.00%
Matrix Structure : 1 0 0 0 1 0 0 0 1
Image Width : 4096
Image Height : 1800
Media Header Version : 0
Media Create Date : 0000:00:00 00:00:00
Media Modify Date : 0000:00:00 00:00:00
Media Time Scale : 16000
Media Duration : 18.00 s
Media Language Code : und
Handler Description : VideoHandler
Graphics Mode : srcCopy
Op Color : 0 0 0
Compressor ID : hev1
Source Image Width : 4096
Source Image Height : 1800
X Resolution : 72
Y Resolution : 72
Bit Depth : 24
```

Rysunek 9: fragment wyniku exiftool

Komentarz: plik .mp4 zawiera różne metadane ale nie dotyczące czasu, kamery czy lokalizacja. *Media Create Date* lub *Track Create Date* mają zerowe wartości, a wpisów o sprzęcie czy lokalizacji nie ma wcale.

#### 4. Wnioski

Plik strumieniowy .dav można przekonwertować na bardziej standardowy format np. .mp4, którego analiza dostarcza większej ilości informacji o nagraniu.