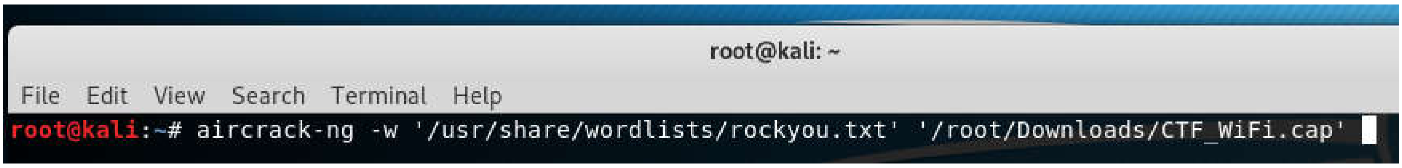
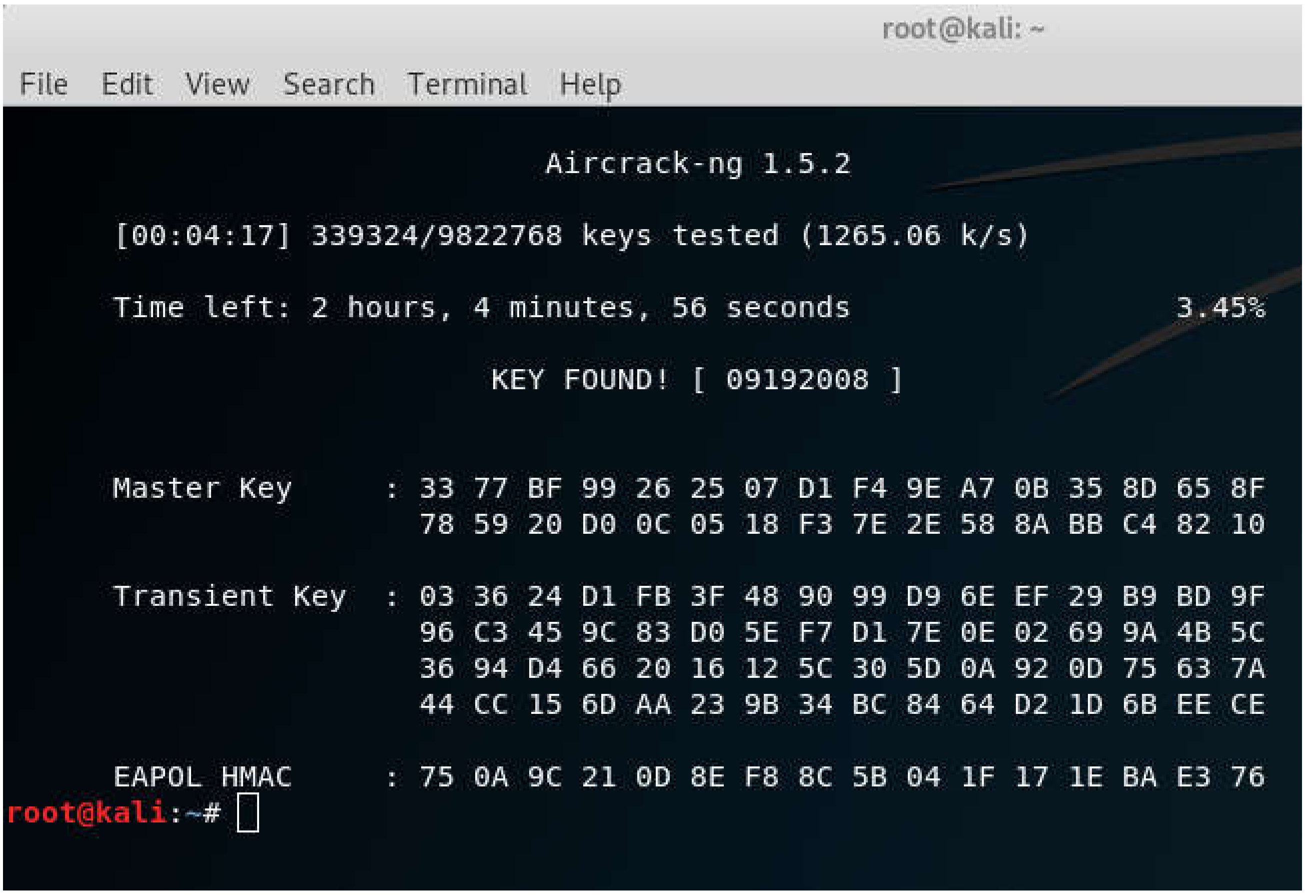
Krok 1: odwrócenie hasha WPA. albo poprzez domyślny wordlist w Kali albo najprostszą maskę ?d?d?d?d?d?d?d?d w hashcat -m2500 po wcześniejszym eksporcie handshake.

Klasyka podpowiada zwykły aircrack-ng:)

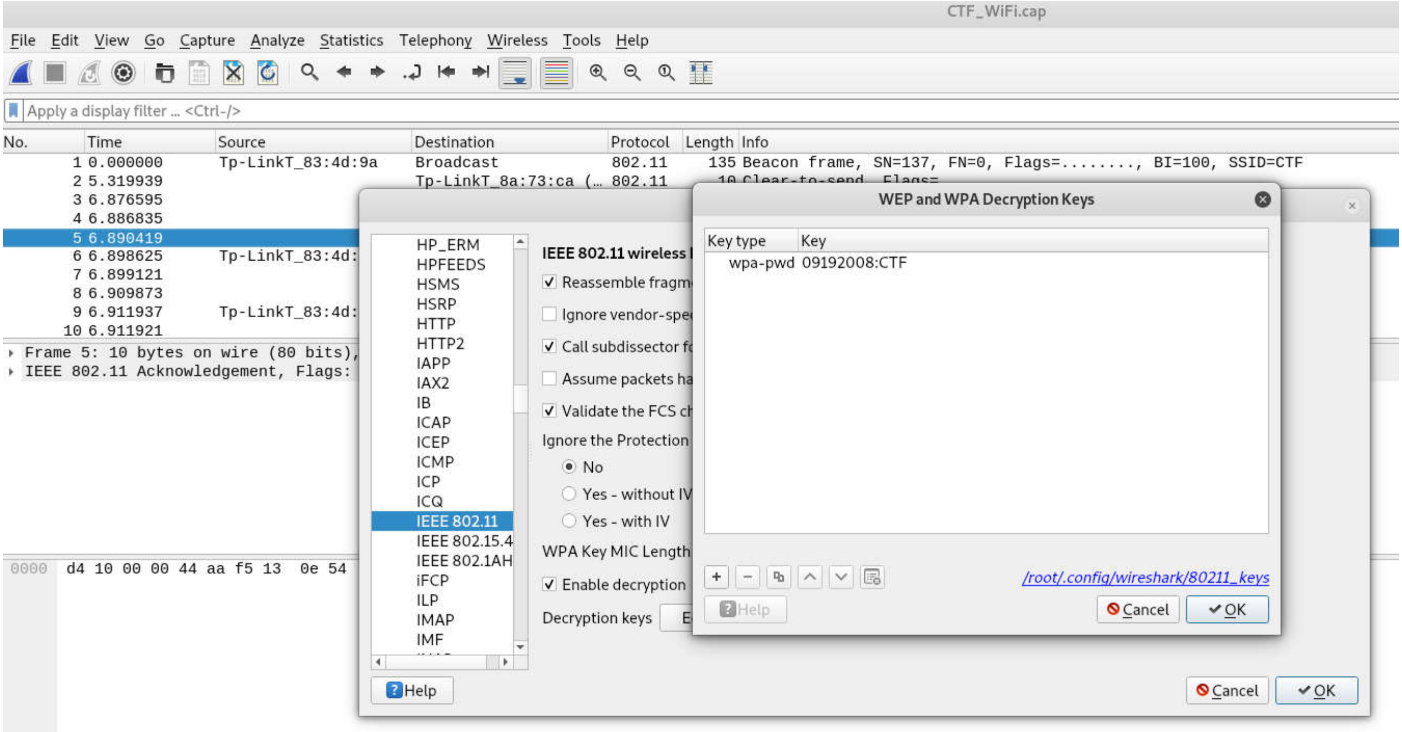


```
root@kali:~# aircrack-ng -w '/usr/share/wordlists/rockyou.txt' '/root/Downloads/CTF_WiFi.cap'
```



```
                               Aircrack-ng 1.5.2

      [00:04:17] 339324/9822768 keys tested (1265.06 k/s)

      Time left: 2 hours, 4 minutes, 56 seconds                  3.45%

                           KEY FOUND! [ 09192008 ]


      Master Key     : 33 77 BF 99 26 25 07 D1 F4 9E A7 0B 35 8D 65 8F
                       78 59 20 D0 0C 05 18 F3 7E 2E 58 8A BB C4 82 10

      Transient Key  : 03 36 24 D1 FB 3F 48 90 99 D9 6E EF 29 B9 BD 9F
                       96 C3 45 9C 83 D0 5E F7 D1 7E 0E 02 69 9A 4B 5C
                       36 94 D4 66 20 16 12 5C 30 5D 0A 92 0D 75 63 7A
                       44 CC 15 6D AA 23 9B 34 BC 84 64 D2 1D 6B EE CE

      EAPOL HMAC     : 75 0A 9C 21 0D 8E F8 8C 5B 04 1F 17 1E BA E3 76
root@kali:~# 
```

Krok 2: odszyfrowanie ruchu wersja A



```
No.   Time       Source              Destination            Protocol Length Info
    1 0.000000   Tp-LinkT_83:4d:9a   Broadcast              802.11     135 Beacon frame, SN=137, FN=0, Flags=........, BI=100, SSID=CTF
    2 5.319939                       Tp-LinkT_8a:73:ca (…   802.11      10 Clear-to-send, Flags=
    3 6.876595
    4 6.886835
    5 6.890419
    6 6.898625   Tp-LinkT_83:4d:
    7 6.899121
    8 6.909873
    9 6.911937   Tp-LinkT_83:4d:
   10 6.911921
▸ Frame 5: 10 bytes on wire (80 bits),
▸ IEEE 802.11 Acknowledgement, Flags:
0000  d4 10 00 00 44 aa f5 13  0e 54
```

IEEE 802.11 wireless l

☑ Reassemble fragm

☐ Ignore vendor-spec

☑ Call subdissector fc

☐ Assume packets ha

☑ Validate the FCS ch

Ignore the Protection

● No

○ Yes - without IV

○ Yes - with IV

WPA Key MIC Length

☑ Enable decryption

Decryption keys E

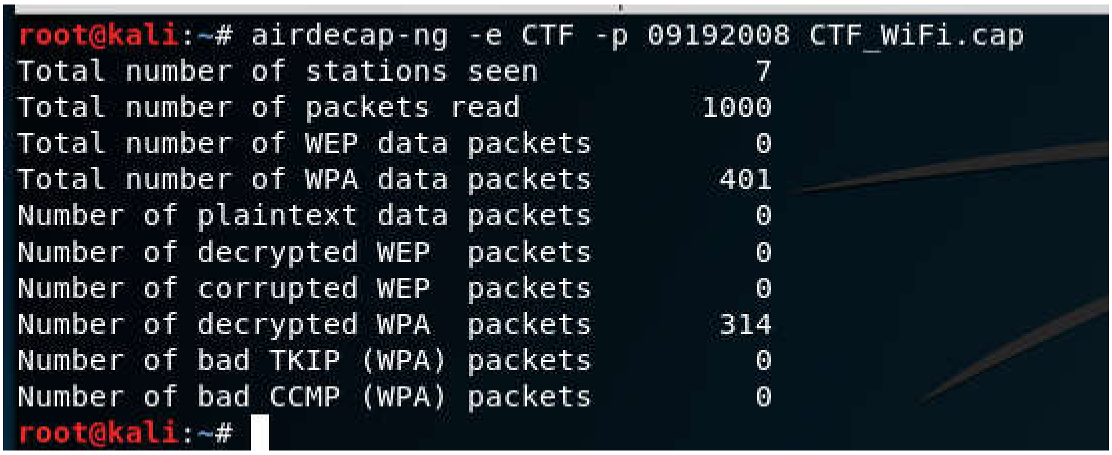
WEP and WPA Decryption Keys

Key type	Key
wpa-pwd	09192008:CTF

/root/.config/wireshark/80211_keys

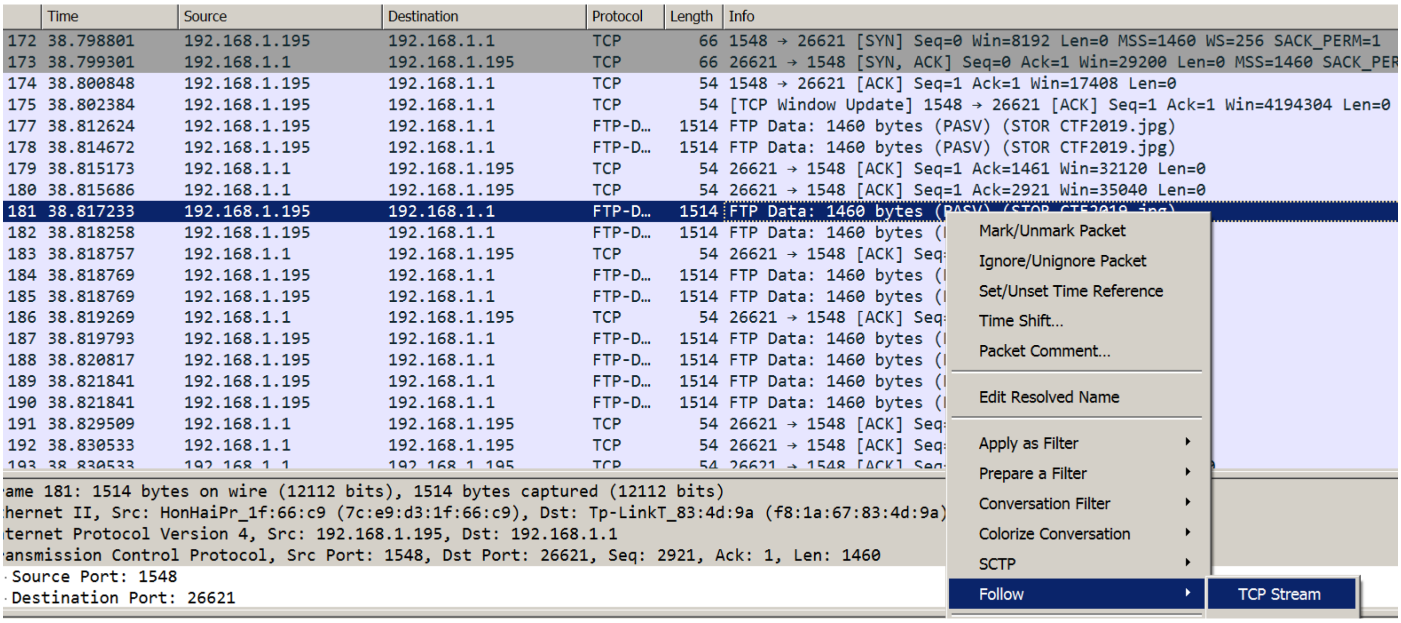
Help · Cancel · ✓OK

Krok 2: odszyfrowanie ruchu wersja B:



```
root@kali:~# airdecap-ng -e CTF -p 09192008 CTF_WiFi.cap
Total number of stations seen            7
Total number of packets read          1000
Total number of WEP data packets         0
Total number of WPA data packets       401
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets       314
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
root@kali:~# 
```

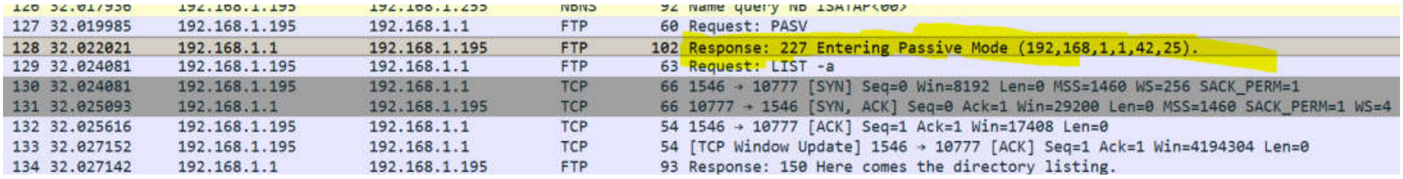
Krok 3: odnalezienie zawartości w ruchu ftp



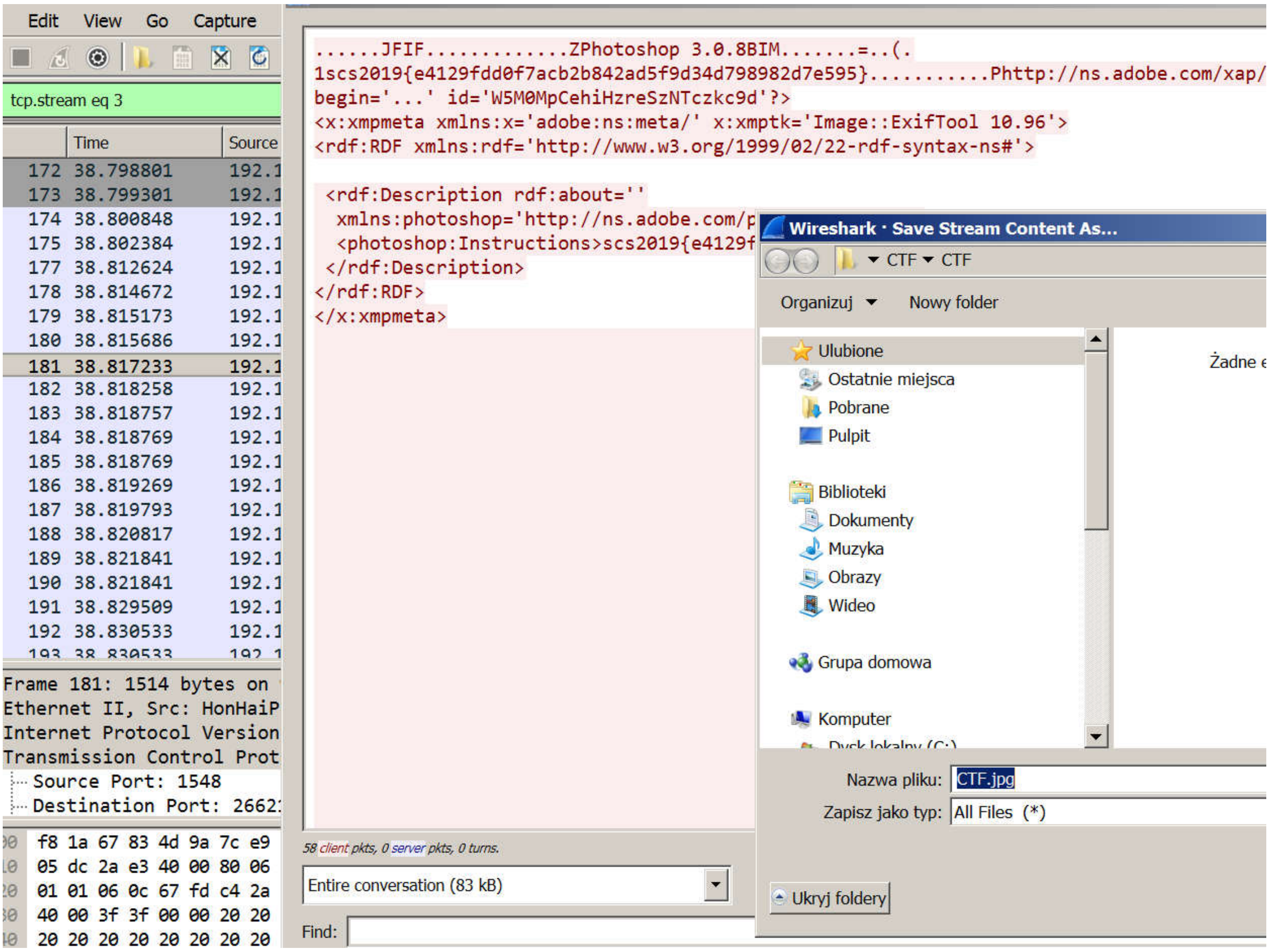
```
    Time        Source         Destination    Protocol  Length  Info
172 38.798801   192.168.1.195  192.168.1.1    TCP         66 1548 → 26621 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
173 38.799301   192.168.1.1    192.168.1.195  TCP         66 26621 → 1548 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PER
174 38.800848   192.168.1.195  192.168.1.1    TCP         54 1548 → 26621 [ACK] Seq=1 Ack=1 Win=17408 Len=0
175 38.802384   192.168.1.195  192.168.1.1    TCP         54 [TCP Window Update] 1548 → 26621 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
177 38.812624   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (PASV) (STOR CTF2019.jpg)
178 38.814672   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (PASV) (STOR CTF2019.jpg)
179 38.815173   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq=1 Ack=1461 Win=32120 Len=0
180 38.815686   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq=1 Ack=2921 Win=35040 Len=0
181 38.817233   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (PASV) (STOR CTF2019.jpg)
182 38.818258   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
183 38.818757   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq
184 38.818769   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
185 38.818769   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
186 38.819269   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq
187 38.819793   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
188 38.820817   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
189 38.821841   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
190 38.821841   192.168.1.195  192.168.1.1    FTP-D…    1514 FTP Data: 1460 bytes (
191 38.829509   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq
192 38.830533   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq
193 38.830533   192.168.1.1    192.168.1.195  TCP         54 26621 → 1548 [ACK] Seq
```

```
ame 181: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
hernet II, Src: HonHaiPr_1f:66:c9 (7c:e9:d3:1f:66:c9), Dst: Tp-LinkT_83:4d:9a (f8:1a:67:83:4d:9a)
ternet Protocol Version 4, Src: 192.168.1.195, Dst: 192.168.1.1
ansmission Control Protocol, Src Port: 1548, Dst Port: 26621, Seq: 2921, Ack: 1, Len: 1460
 Source Port: 1548
 Destination Port: 26621
```

Krok 4: eksport obrazka



```
126 32.017936  192.168.1.195  192.168.1.255  NBNS   92 Name query NB ISATAP<00>
127 32.019985  192.168.1.195  192.168.1.1    FTP    60 Request: PASV
128 32.022021  192.168.1.1    192.168.1.195  FTP   102 Response: 227 Entering Passive Mode (192,168,1,1,42,25).
129 32.024081  192.168.1.195  192.168.1.1    FTP    63 Request: LIST -a
130 32.024081  192.168.1.195  192.168.1.1    TCP    66 1546 → 10777 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
131 32.025093  192.168.1.1    192.168.1.195  TCP    66 10777 → 1546 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=4
132 32.025616  192.168.1.195  192.168.1.1    TCP    54 1546 → 10777 [ACK] Seq=1 Ack=1 Win=17408 Len=0
133 32.027152  192.168.1.195  192.168.1.1    TCP    54 [TCP Window Update] 1546 → 10777 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
134 32.027142  192.168.1.1    192.168.1.195  FTP    93 Response: 150 Here comes the directory listing.
```



tcp.stream eq 3

```
    Time       Source
172 38.798801  192.1
173 38.799301  192.1
174 38.800848  192.1
175 38.802384  192.1
177 38.812624  192.1
178 38.814672  192.1
179 38.815173  192.1
180 38.815686  192.1
181 38.817233  192.1
182 38.818258  192.1
183 38.818757  192.1
184 38.818769  192.1
185 38.818769  192.1
186 38.819269  192.1
187 38.819793  192.1
188 38.820817  192.1
189 38.821841  192.1
190 38.821841  192.1
191 38.829509  192.1
192 38.830533  192.1
193 38.830533  192.1
```

```
Frame 181: 1514 bytes on
Ethernet II, Src: HonHaiP
Internet Protocol Version
Transmission Control Prot
  Source Port: 1548
  Destination Port: 2662
```

```
00  f8 1a 67 83 4d 9a 7c e9
10  05 dc 2a e3 40 00 80 06
20  01 01 06 0c 67 fd c4 2a
30  40 00 3f 3f 00 00 20 20
40  20 20 20 20 20 20 20 20
```

```
......JFIF.............ZPhotoshop 3.0.8BIM.......=..(.
1scs2019{e4129fdd0f7acb2b842ad5f9d34d798982d7e595}...........Phttp://ns.adobe.com/xap/
begin='...' id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x='adobe:ns:meta/' x:xmptk='Image::ExifTool 10.96'>
<rdf:RDF xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'>

 <rdf:Description rdf:about=''
  xmlns:photoshop='http://ns.adobe.com/p
  <photoshop:Instructions>scs2019{e4129f
 </rdf:Description>
</rdf:RDF>
</x:xmpmeta>
```

58 client pkts, 0 server pkts, 0 turns.

Entire conversation (83 kB)

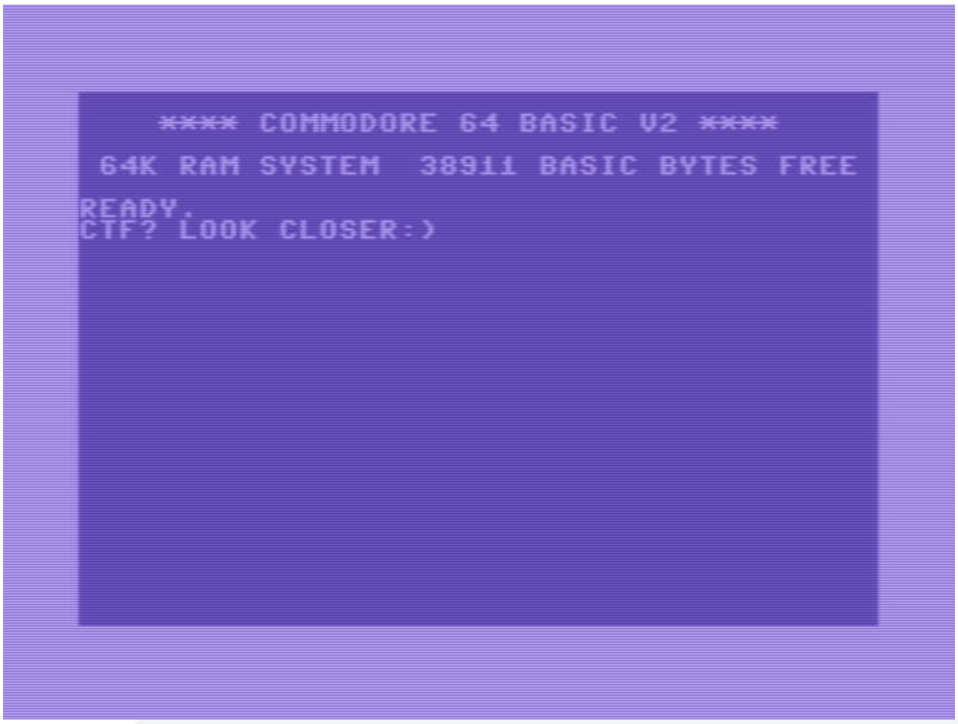
Find:

Wireshark · Save Stream Content As...

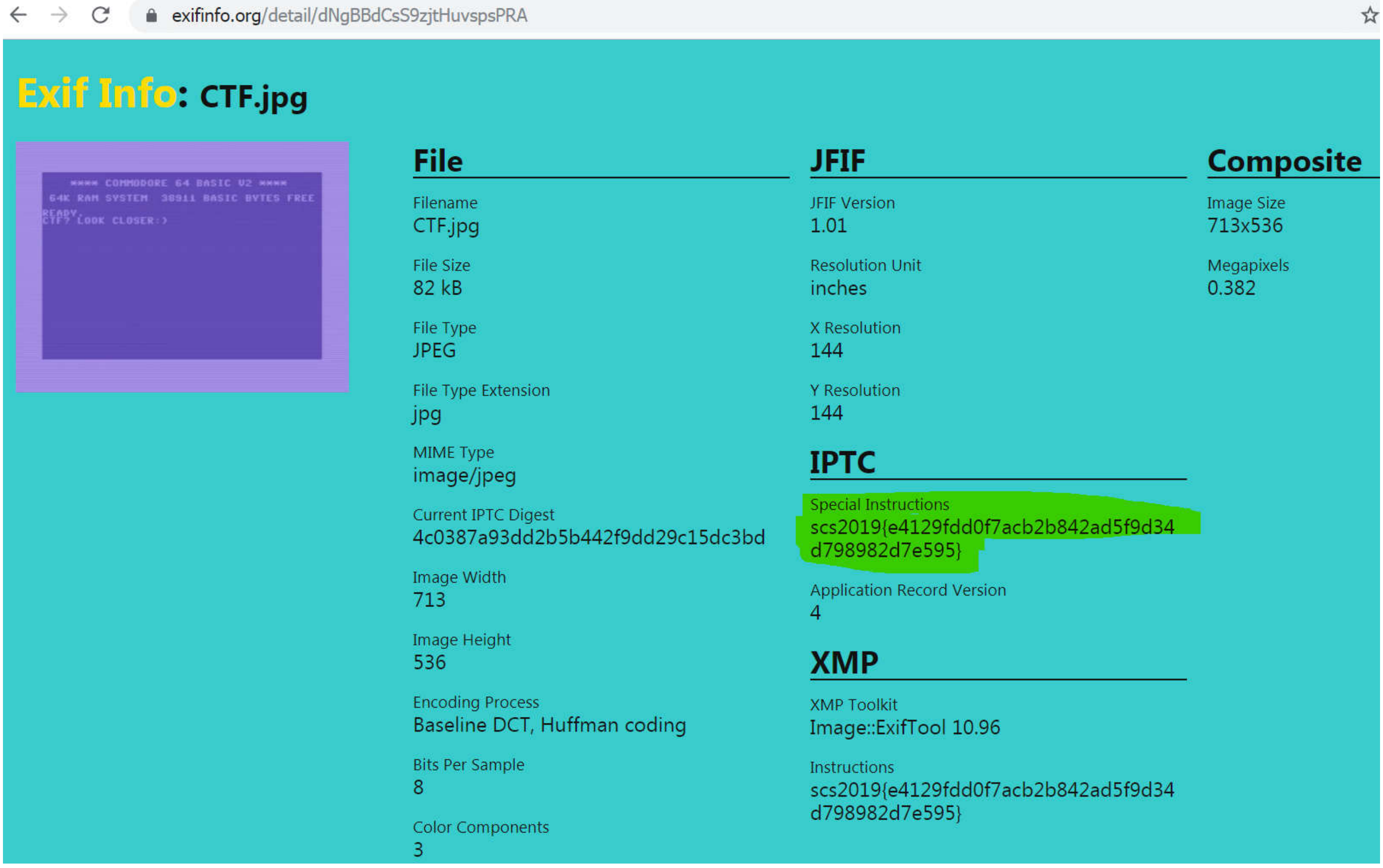
Nazwa pliku: CTF.jpg

Zapisz jako typ: All Files (*)

Krok 5: Metadane w pliku



```
**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM  38911 BASIC BYTES FREE
READY.
CTF? LOOK CLOSER:)
```



exifinfo.org/detail/dNgBBdCsS9zjtHuvspsPRA

Exif Info: CTF.jpg

File

Filename
CTF.jpg

File Size
82 kB

File Type
JPEG

File Type Extension
jpg

MIME Type
image/jpeg

Current IPTC Digest
4c0387a93dd2b5b442f9dd29c15dc3bd

Image Width
713

Image Height
536

Encoding Process
Baseline DCT, Huffman coding

Bits Per Sample
8

Color Components
3

JFIF

JFIF Version
1.01

Resolution Unit
inches

X Resolution
144

Y Resolution
144

IPTC

Special Instructions
scs2019{e4129fdd0f7acb2b842ad5f9d34d798982d7e595}

Application Record Version
4

XMP

XMP Toolkit
Image::ExifTool 10.96

Instructions
scs2019{e4129fdd0f7acb2b842ad5f9d34d798982d7e595}

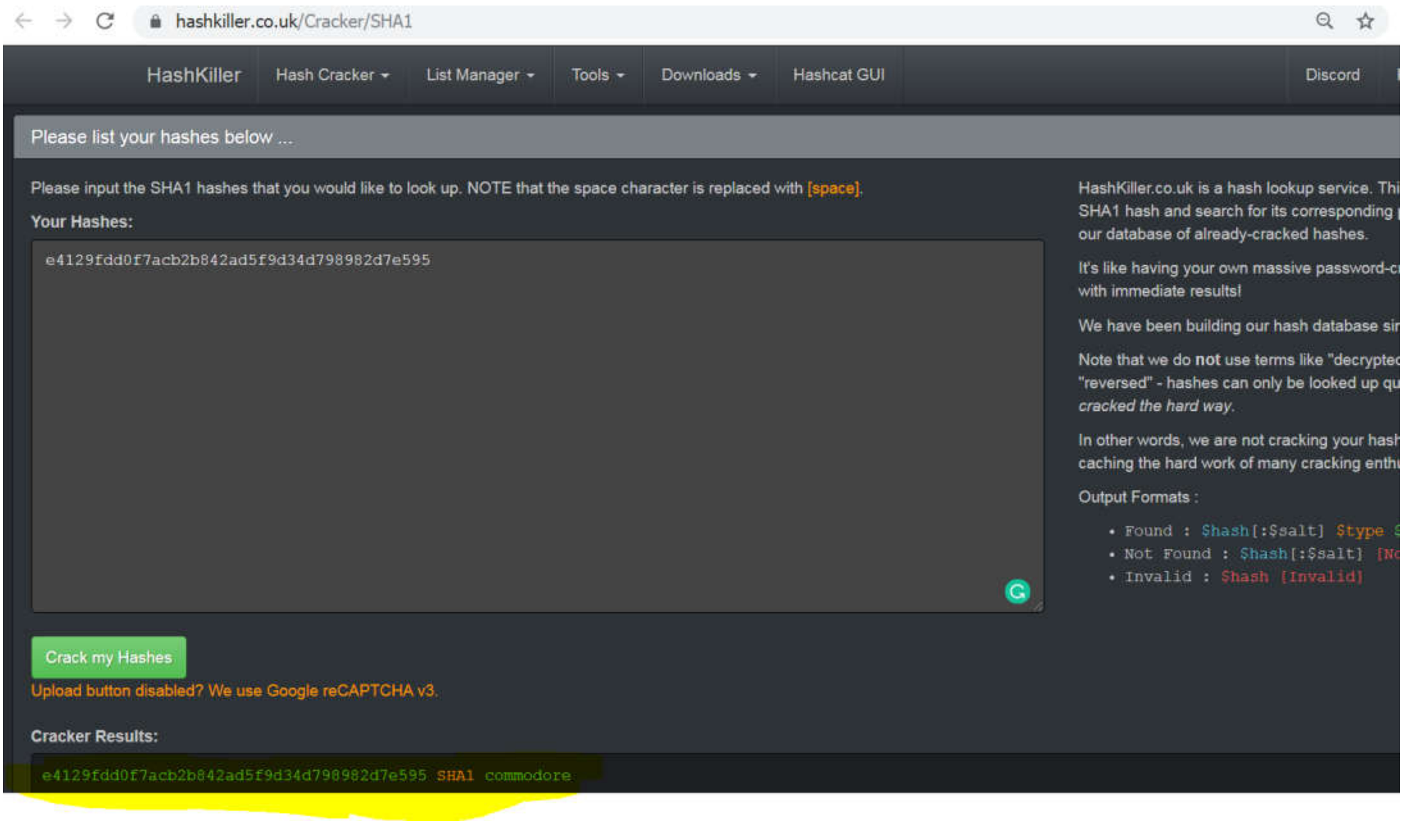
Composite

Image Size
713x536

Megapixels
0.382

Krok 6: Odwrócenie hasha

scs2019{e4129fdd0f7acb2b842ad5f9d34d798982d7e595}



Please list your hashes below ...

Please input the SHA1 hashes that you would like to look up. NOTE that the space character is replaced with [space].

Your Hashes:

```
e4129fdd0f7acb2b842ad5f9d34d798982d7e595
```

HashKiller.co.uk is a hash lookup service. Thi
SHA1 hash and search for its corresponding
our database of already-cracked hashes.

It's like having your own massive password-c
with immediate results!

We have been building our hash database sir

Note that we do **not** use terms like "decrypted
"reversed" - hashes can only be looked up qu
cracked the hard way.

In other words, we are not cracking your hash
caching the hard work of many cracking enthu

Output Formats :

```
• Found : $hash[:$salt] $type $
• Not Found : $hash[:$salt] [No
• Invalid : $hash [Invalid]
```

Upload button disabled? We use Google reCAPTCHA v3.

Cracker Results:

```
e4129fdd0f7acb2b842ad5f9d34d798982d7e595 SHA1 commodore
```

Krok7: commodore

:)

Konrad Jędrzejczyk