

Wireshark Analysis for DWD <file> command for all encryption

Server Port = 49154

Caesar Cipher (Shift = 12)

Table of alphabets and their shifted by 12 versions

Letter	Letter shifted by 13
a/A	m/M
b/B	n/N
c/C	o/O
d/D	p/P
e/E	q/Q
f/F	r/R
g/G	s/S
h/H	t/T
i/I	u/U
j/J	v/V
k/K	w/W
l/L	x/X
m/M	y/Y
n/N	z/Z
o/O	a/A
p/P	b/B
q/Q	c/C
r/R	d/D
s/S	e/E
t/T	f/F

u/U	g/G
v/V	h/H
x/X	i/I
y/Y	j/J
z/Z	k/K

```
(kali㉿kali)-[~/Downloads/newproj/client]
$ python client.py
Socket Created at client end
Connected to Server IP= 127.0.0.1
DWD server_test_file.txt
STATUS: OK
□
```

Firstly we are sending the command from client to server

Also for the command we are sending i.e. DWD server_test_file.txt

We expect ca-PIP eqdhqd_fdef_ruxq.fif

```

▶ Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface lo, id 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ Transmission Control Protocol, Src Port: 39108, Dst Port: 49154, Seq: 1, Ack: 1, Len: 27
▼ Data (27 bytes)
  Data: 63612d504950206571646871645f667165665f727578712e666a66
  [Length: 27]

0000  00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 4f d2 c6 40 00 40 06 69 e0 7f 00 00 01 7f 00  .O..@.@.i.....
0020  00 01 98 c4 c0 02 82 8f 1f e5 7c 95 a3 61 80 18  .....|..a..
0030  02 00 fe 43 00 00 01 01 08 0a 28 b5 da 76 28 b5  ...C.....(..v(
0040  8a c7 63 61 2d 50 49 50 20 65 71 64 68 71 64 5f  ..ca-PIP eqdhqd
0050  66 71 65 66 5f 72 75 78 71 2e 66 6a 66          fqef_rux q.fjf

```

Here we see that source protocol is random port but the destination port is 49154

We have an encrypted command on the dump which matches our expectations.

Now for contents of server_test_file.txt are

Today I connected with about 15 clients. I am so happy that I served them.

We expect encrypted text to be

Fapmk U oazzqofqp iuft mnagf 15 oxuqzfe. U my ea tmbbk ftmf U eqdhqp ftqy.

```
Frame 8: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49154, Dst Port: 39108, Seq: 9, Ack: 28, Len: 77
Data (77 bytes)
Data: 63612d4661706d6b2055206f617a7a716f6671702069756674206d6e616766203135206f...
[Length: 77]

0020  00 01 c0 02 98 c4 7c 95 a3 69 82 8f 20 00 80 18 .....|.i.
0030  02 00 fe 75 00 00 01 01 08 0a 28 b5 da 76 28 b5 ...u...(-v(
0040  da 76 63 61 2d 46 61 70 6d 6b 20 55 20 6f 61 7a ..vca-Fap mk U oaz
0050  7a 71 6f 66 71 70 20 69 75 66 74 20 6d 6e 61 67 zqofqp i uft mnag
0060  66 20 31 35 20 6f 78 75 71 7a 66 65 2e 20 55 20 f 15 oxu qzfe. U
0070  6d 79 20 65 61 20 74 6d 62 62 6b 20 66 74 6d 66 my ea tm bbk ftmf
0080  20 55 20 65 71 64 68 71 70 20 66 74 71 79 2e U eqdhq p ftqy.
```

Text in the dump is same as what we expected.

Now we look for response footer

```
Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49154, Dst Port: 50484, Seq: 86, Ack: 28, Len: 10
Data (10 bytes)
Data: 63612d70697064717a70
[Length: 10]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010  00 3e e5 dd 40 00 40 06 56 da 7f 00 00 01 7f 00 ->..@.@. V.....
0020  00 01 c0 02 c5 34 2c 61 59 df e1 1d 02 94 80 18 .....4,a Y.....
0030  02 00 fe 32 00 00 01 01 08 0a 29 0b 3f 9b 29 0b ...2.....)?)..
0040  3b ad 63 61 2d 70 69 70 64 71 7a 70 ; ca-pip dqzp
```

We found footer as pipdqzp which encrypted version of dwrend

Now we look for status response

```
Frame 12: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49154, Dst Port: 50484, Seq: 96, Ack: 28, Len: 18
Data (18 bytes)
Data: 63612d727069702045464d4647453a204157
[Length: 18]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010  00 46 e5 de 40 00 40 06 56 d1 7f 00 00 01 7f 00 .F..@.@. V.....
0020  00 01 c0 02 c5 34 2c 61 59 e9 e1 1d 02 94 80 18 .....4,a Y.....
0030  02 00 fe 3a 00 00 01 01 08 0a 29 0b 43 84 29 0b ...:.. ..)C..
0040  3f 9b 63 61 2d 72 70 69 70 20 45 46 4d 46 47 45 ? ca-rpi p EFMFGE
0050  3a 20 41 57 : AW
```

We found status response as rpip EFMFGE: AW which is encrypted version of fdwd STATUS:
OK

Transpose

Our command is DWD server_test_file.txt and we are expecting encrypted command to be DWD txt.elif_tset_revres

```

> Frame 6: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 57316, Dst Port: 49154, Seq: 1, Ack: 1, Len: 27
> Data (27 bytes)
  Data: 74722d445744207478742e656c696665f747365745f726576726573
  [Length: 27]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 4f 1d 8e 40 00 40 06 1f 19 7f 00 00 01 7f 00  .O.@.@.....
0020  00 01 df e4 c0 02 3a a1 67 d3 f5 b0 2d ce 80 18  .....:g....
0030  02 00 fe 43 00 00 01 01 08 0a 28 d9 a0 df 28 d9  ...C.....(..(
0040  68 fe 74 72 2d 44 57 44 20 74 78 74 2e 65 6c 69  h.tr-DWD txt.eli
0050  66 5f 74 73 65 74 5f 72 65 76 72 65 73         f_tset_r evres

```

Encrypted command in the dump is the same as what we expected.

We look for response header

```

> Frame 8: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49154, Dst Port: 57316, Seq: 1, Ack: 28, Len: 7
> Data (7 bytes)
  Data: 74722d72647764
  [Length: 7]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 3b 43 47 40 00 40 06 f9 73 7f 00 00 01 7f 00  .;CG@.@.s....
0020  00 01 c0 02 df e4 f5 b0 2d ce 3a a1 67 ee 80 18  .....-:g....
0030  02 00 fe 2f 00 00 01 01 08 0a 28 d9 a0 df 28 d9  .../.....(..(
0040  a0 df 74 72 2d 72 64 77 64                      ..tr-rdw d

```

Originally we expect it to be dwdr but it is reversed

Now for contents of server_test_file.txt are

Today I connected with about 15 clients. I am so happy that I served them.

We expect encrypted text to be

yad-oT I detcennoc htiw tuoba 51 .neilc I ma os yppah tath I devsres .meht

```

> Frame 10: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49154, Dst Port: 57316, Seq: 8, Ack: 28, Len: 77
~ Data (77 bytes)
  Data: 74722d7961646f5420492064657463656e6e6f6320687469772074756f6261203531202e...
  [Length: 77]

0020  00 01 c0 02 df e4 f5 b0 2d d5 3a a1 67 ee 80 18  ....:..g...
0030  02 00 fe 75 00 00 01 01 08 0a 28 d9 a1 42 28 d9  ..u.....(..B(
0040  a0 df 74 72 2d 79 61 64 6f 54 20 49 20 64 65 74  ..tr-yad oT I det
0050  63 65 6e 6e 6f 63 20 68 74 69 77 20 74 75 6f 62  cennoc h tiw tuob
0060  61 20 35 31 20 2e 73 74 6e 65 69 6c 63 20 49 20  a 51 .st neilc I
0070  6d 61 20 6f 73 20 79 70 70 61 68 20 74 61 68 74  ma os yp pah taht
0080  20 49 20 64 65 76 72 65 73 20 2e 6d 65 68 74    I devre s .meht

```

The response file matches our expectations also we see a tr in front which indicates that data is transposed

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  ....E.
0010  00 3e 43 49 40 00 40 06 f9 6e 7f 00 00 01 7f 00  .>CI@.@. .n.....
0020  00 01 c0 02 df e4 f5 b0 2e 22 3a a1 67 ee 80 18  ....:..g...
0030  02 00 fe 32 00 00 01 01 08 0a 28 d9 a5 e5 28 d9  ..2.....(....(
0040  a1 42 74 72 2d 64 6e 65 72 64 77 64             .Btr-dne rdwd

```

We also see a response footer encrypted version of dwdrend

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  ....E.
0010  00 46 43 4a 40 00 40 06 f9 65 7f 00 00 01 7f 00  .FCJ@.@. .e.....
0020  00 01 c0 02 df e4 f5 b0 2e 2c 3a a1 67 ee 80 18  ....:..g...
0030  02 00 fe 3a 00 00 01 01 08 0a 28 d9 a9 d6 28 d9  ..:.....(....(
0040  a5 e5 74 72 2d 64 77 64 66 20 3a 53 55 54 41 54  ..tr-dwd f :SUTAT
0050  53 20 4b 4f                                     S KO

```

And we also have response fdwd STATUS: OK

Plain

Firstly we look for the command

```

> Frame 4: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 41640, Dst Port: 49154, Seq: 1, Ack: 1, Len: 27
~ Data (27 bytes)
  Data: 706c2d445744207365727665725f746573745f66696c652e747874
  [Length: 27]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 4f 58 a0 40 00 40 06 e4 06 7f 00 00 01 7f 00  .OX.@.
0020  00 01 a2 a8 c0 02 d9 89 8d cb f5 9f ea 3d 80 18  .....=..
0030  02 00 fe 43 00 00 01 01 08 0a 28 f2 f0 c0 28 f2  ...C....(....(
0040  bf 3d 70 6c 2d 44 57 44 20 73 65 72 76 65 72 5f  ..=pl-DWD server_
0050  74 65 73 74 5f 66 69 6c 65 2e 74 78 74          test_fil e.txt

```

We see the plain command DWD server_test_file.txt

Now we look for the response header

```

> Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49154, Dst Port: 41640, Seq: 1, Ack: 28, Len: 8
~ [Malformed Packet: LBMSRS]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 3c 2e d4 40 00 40 06 0d e6 7f 00 00 01 7f 00  .<..@.
0020  00 01 c0 02 a2 a8 f5 9f ea 3d d9 89 8d e6 80 18  .....-..
0030  02 00 fe 30 00 00 01 01 08 0a 28 f2 f0 c0 28 f2  ...0....(....(
0040  f0 c0 70 6c 2d 64 77 64 72 20                      ..pl-dwd r

```

We see the dwdr header

Now we look for response contents of the file

```

> Frame 8: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49154, Dst Port: 41640, Seq: 9, Ack: 28, Len: 77
~ Data (77 bytes)
  Data: 706c2d546f646179204920636f6e6e656374656420776974682061626f75742031352063...
  [Length: 77]

0020  00 01 c0 02 a2 a8 f5 9f ea 45 d9 89 8d e6 80 18  .....E.....
0030  02 00 fe 75 00 00 01 01 08 0a 28 f2 f0 c0 28 f2  ...u....(....(
0040  f0 c0 70 6c 2d 54 6f 64 61 79 20 49 20 63 6f 6e  ..pl-Tod ay I con
0050  6e 65 63 74 65 64 20 77 69 74 68 20 61 62 6f 75  nected w ith abou
0060  74 20 31 35 20 63 6c 69 65 6e 74 73 2e 20 49 20  t 15 cli ents. I
0070  61 6d 20 73 6f 20 68 61 70 70 79 20 74 68 61 74  am so ha ppy that
0080  20 49 20 73 65 72 76 65 64 20 74 68 65 6d 2e    I serve d them.

```

We have exact same contents of the file

Now we look for the response footer

```

> Frame 10: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49154, Dst Port: 41640, Seq: 86, Ack: 28, Len: 10
  Data (10 bytes)
    Data: 706c2d64776472656e64
    [Length: 10]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 3e 2e d6 40 00 40 06 0d e2 7f 00 00 01 7f 00  ->..@.@.....
0020  00 01 c0 02 a2 a8 f5 9f ea 92 d9 89 8d e6 80 18  .....
0030  02 00 fe 32 00 00 01 01 08 0a 28 f2 f4 a9 28 f2  ...2....(....(
0040  f0 c0 70 6c 2d 64 77 64 72 65 6e 64             ..pl-dwd rend

```

We found the footer as dwdrend

Now we look for Status response

```

> Frame 12: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 49154, Dst Port: 41640, Seq: 96, Ack: 28, Len: 18
  Data (18 bytes)
    Data: 706c2d66647764205354415455533a204f4b
    [Length: 18]

0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 46 2e d7 40 00 40 06 0d d9 7f 00 00 01 7f 00  .F.@.@.....
0020  00 01 c0 02 a2 a8 f5 9f ea 9c d9 89 8d e6 80 18  .....
0030  02 00 fe 3a 00 00 01 01 08 0a 28 f2 f8 95 28 f2  ...:....(....(
0040  f4 a9 70 6c 2d 66 64 77 64 20 53 54 41 54 55 53  ..pl-fdw d STATUS
0050  3a 20 4f 4b                                     : OK

```

We found the status as fdwd STATUS: OK