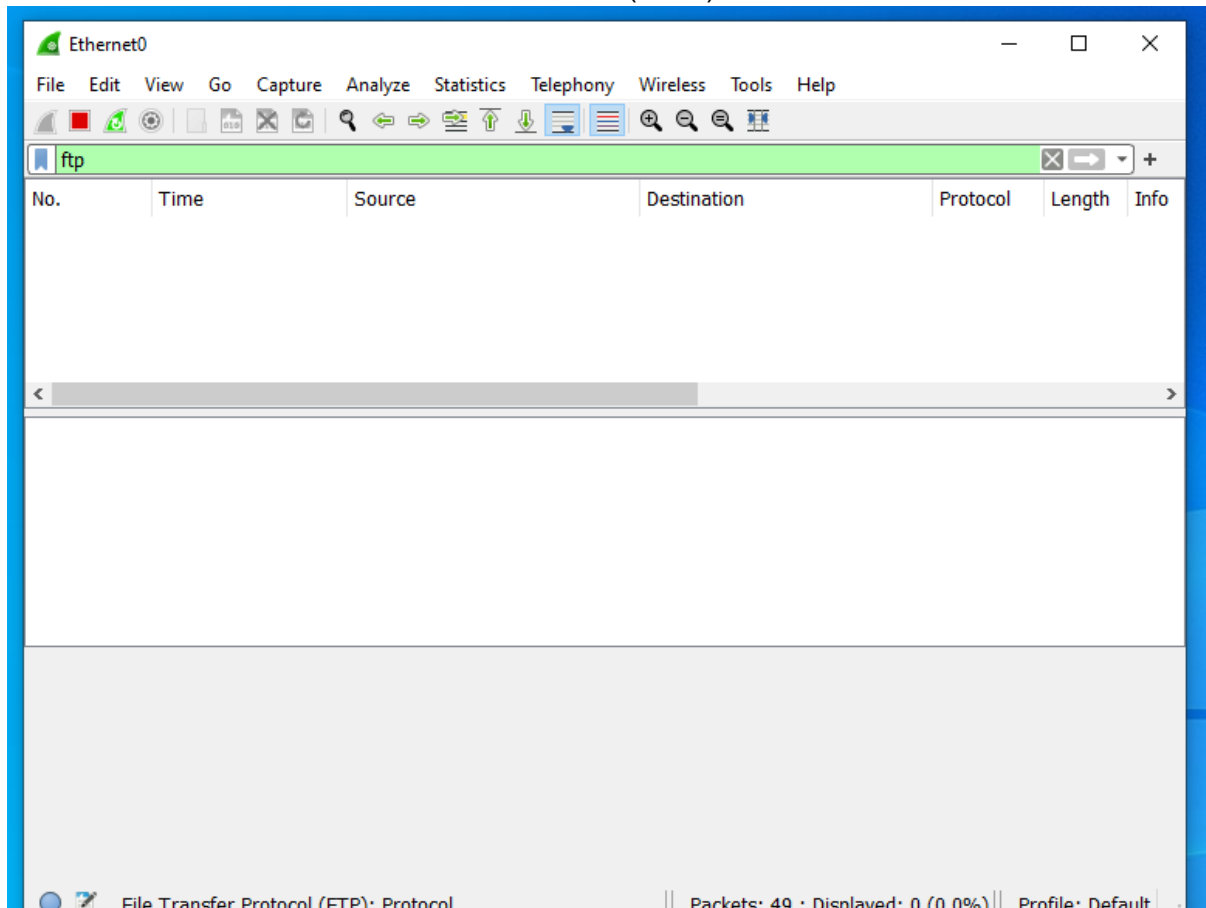


Capturing FTP in Wireshark

ביצוע לכידת FTP ב WIRESHARK

1. נפתח WIRESHARK במחשב האורח (Client) ונחפש תעבורת FTP:



כפי שאנו רואים כעת אין תעבורה של פרוטוקול FTP.

2. כעת אכנס לשרת FTP שביתי קודם לכן ונוכל לראות שלאחר הכניסה לשרת ה FTP ישנה תעבורת CLEAR TEXT (הפרוטוקול אינו מוצפן!) ב WIRESHARK

192.168.177.128

File Home Share View

The Internet > 192.168.177.128

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Music
- Videos
- OneDrive
- This PC
- Network

FTP Data

FTP Text File.txt

2 items

Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
85	134.922400	192.168.177.128	192.168.177.129	FTP	79	Response: 530 User cannot log in.
94	140.217223	192.168.177.128	192.168.177.129	FTP	81	Response: 220 Microsoft FTP Service
96	140.221422	192.168.177.129	192.168.177.128	FTP	74	Request: USER administrator
97	140.221937	192.168.177.128	192.168.177.129	FTP	77	Response: 331 Password required
99	140.222411	192.168.177.129	192.168.177.128	FTP	73	Request: PASS queQE123!@#
100	140.224960	192.168.177.128	192.168.177.129	FTP	75	Response: 230 User logged in.
102	140.225368	192.168.177.129	192.168.177.128	FTP	68	Request: opts utf8 on
103	140.225879	192.168.177.128	192.168.177.129	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding now ON.
105	140.226288	192.168.177.129	192.168.177.128	FTP	59	Request: PwD
106	140.226610	192.168.177.128	192.168.177.129	FTP	85	Response: 257 "/" is current directory.

> Frame 79: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{6C026246-0B1B-4067-BA72-CD8AA0C972A4}, id 0

> Ethernet II, Src: VMware_03:77:cd (00:0c:29:03:77:cd), Dst: VMware_42:74:ee (00:0c:29:42:74:ee)

> Internet Protocol Version 4, Src: 192.168.177.128, Dst: 192.168.177.129

> Transmission Control Protocol, Src Port: 21, Dst Port: 49840, Seq: 1, Ack: 1, Len: 27

> File Transfer Protocol (FTP)

[Current working directory:]

```

0000  00 0c 29 42 74 ee 00 0c 29 03 77 cd 00 00 45 00  ..)Bt... }w...E
0010  00 43 c0 b9 40 00 00 06 55 a8 c0 a0 b1 00 c0 a8  C-@... U....
0020  b1 81 00 15 c2 b0 2e 3b ad 2e c7 a1 81 11 50 16  ....;.....P
0030  20 03 29 8f 00 00 32 32 30 20 4d 69 63 72 6f 73  )...22 0 Micros
0040  6f 66 74 20 46 54 50 20 53 65 72 76 69 63 65 0d  oft FTP Service
0050  0a

```

File Transfer Protocol (FTP): Protocol

Packets: 160 · Displayed: 14 (8.8%)

Profile: Default