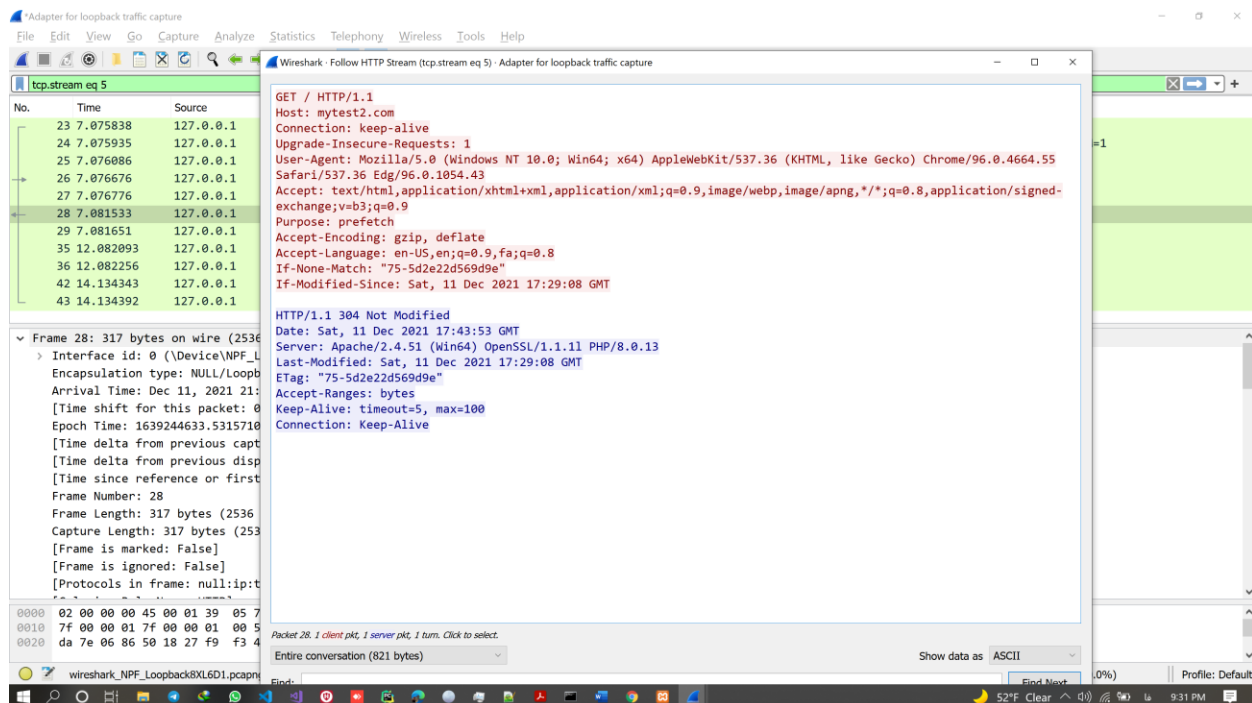


آرتا اسدی
9731006

تمرین web-ftp



سوال 1 :

آدرس هردو، لوکالهاست یا همان 127.0.0.1 است.
 در این پروتکل، ابتدا کلاینت یک ارتباط TCP با ساختن سوکت با سرور برقرار میکند. سرور ارتباط TCP از طرف کاربر را قبول میکند. سپس کلاینت درخواست خود را برای دریافت یک آبجکت به سرور میدهد و سرور به او پاسخ میدهد و در پاسخ آبجکت در خواستی را اگر موجود باشد برای کاربر ارسال میکند.
 یافتن آدرس صفحات وب از طریق اتصال به DNS و کوئری گرفتن از آن رخ میدهد.

سوال 2 :

GET / HTTP/1.1

Host: mytest2.com

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/96.0.4664.55 Safari/537.36 Edg/96.0.1054.43

مقدار user-agent بیانگر مواردی از قبیل سیستم عامل و مرورگر مورداستفاده و vender و ورژن مورداستفاده کاربر (کلاینت) است.

سوال 3 :

Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	44	55808 → 80 [FIN, ACK] Seq=1 Ack=1 Win=10233 Len=0
2	0.000056	127.0.0.1	127.0.0.1	TCP	44	80 → 55808 [ACK] Seq=1 Ack=2 Win=10233 Len=0
3	0.000100	127.0.0.1	127.0.0.1	TCP	44	80 → 55808 [FIN, ACK] Seq=1 Ack=2 Win=10233 Len=0
4	0.000136	127.0.0.1	127.0.0.1	TCP	44	55807 → 80 [FIN, ACK] Seq=1 Ack=1 Win=10233 Len=0

[Next Sequence Number: 2 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 1825583770
 0101 = Header Length: 20 bytes (5)
 ▾ **Flags: 0x011 (FIN, ACK)**
 000. = Reserved: Not set
 ...0 = Nonce: Not set
0... = Congestion Window Reduced (CWR): Not set
0... = ECN-Echo: Not set
0... = Urgent: Not set
1... = Acknowledgment: Set
0... = Push: Not set
0... = Reset: Not set
0... = Syn: Not set
 ▾1... = Fin: Set
 ▾ [Expert Info (Chat/Sequence): Connection finish (FIN)]
 [Connection finish (FIN)]
 [Severity level: Chat]
 [Group: Sequence]
 [TCP Flags:A...F]
 Window: 10233
 [Calculated window size: 10233]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0x0000 (unverified)
 0000 02 00 00 00 45 00 00 28 05 56 40 00 80 06 00 00E...V@....
 0010 7f 00 00 01 7f 00 00 01 da 00 00 50 2f 7a e4 beP/z...
 0020 6c d0 32 9a 50 11 27 f9 fb e3 00 00 1:2:P... ..

wireshark_NPF_Loopback8XL6D1.pcapng | Packets: 58 · Displayed: 58 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

سوال 4 :

Etag و host با هم فرق دارند. (سایت دیگر خود با نام mytest1 را باز کردم)

Warning: Potential Security Risk Ahead

mytest1

https://mytest1.com

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to mytest1.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

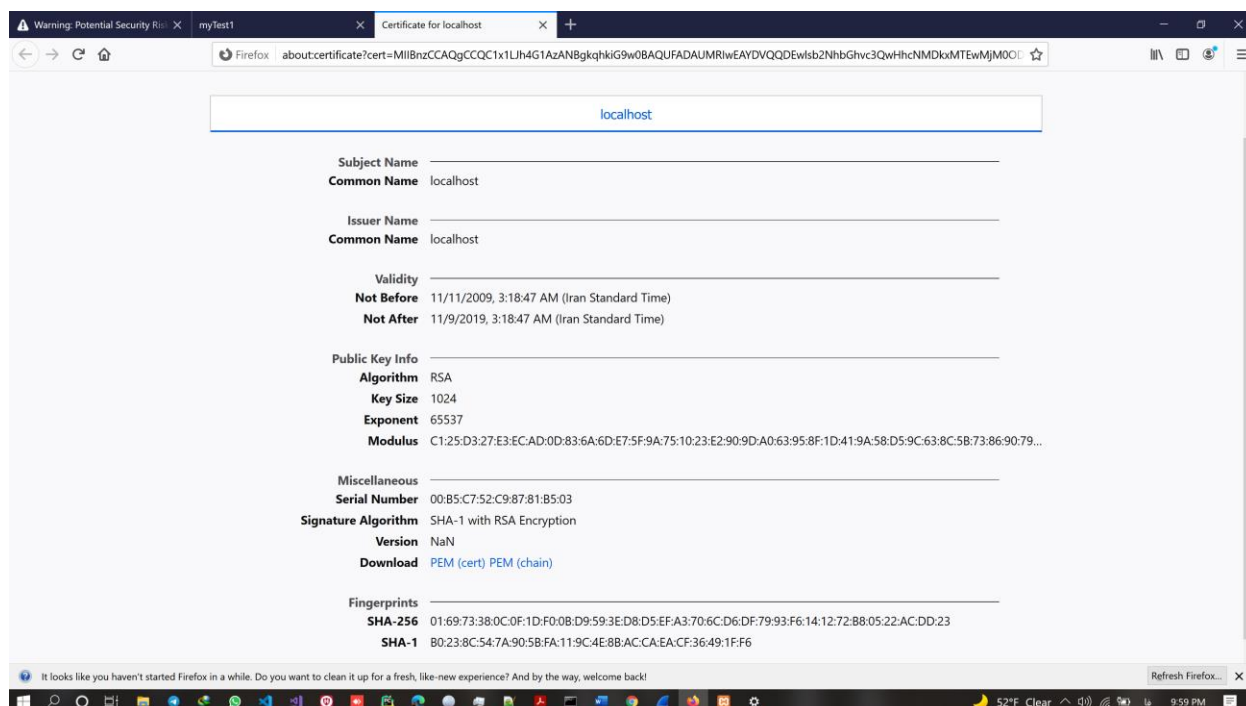
[Go Back \(Recommended\)](#) [Advanced...](#)

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

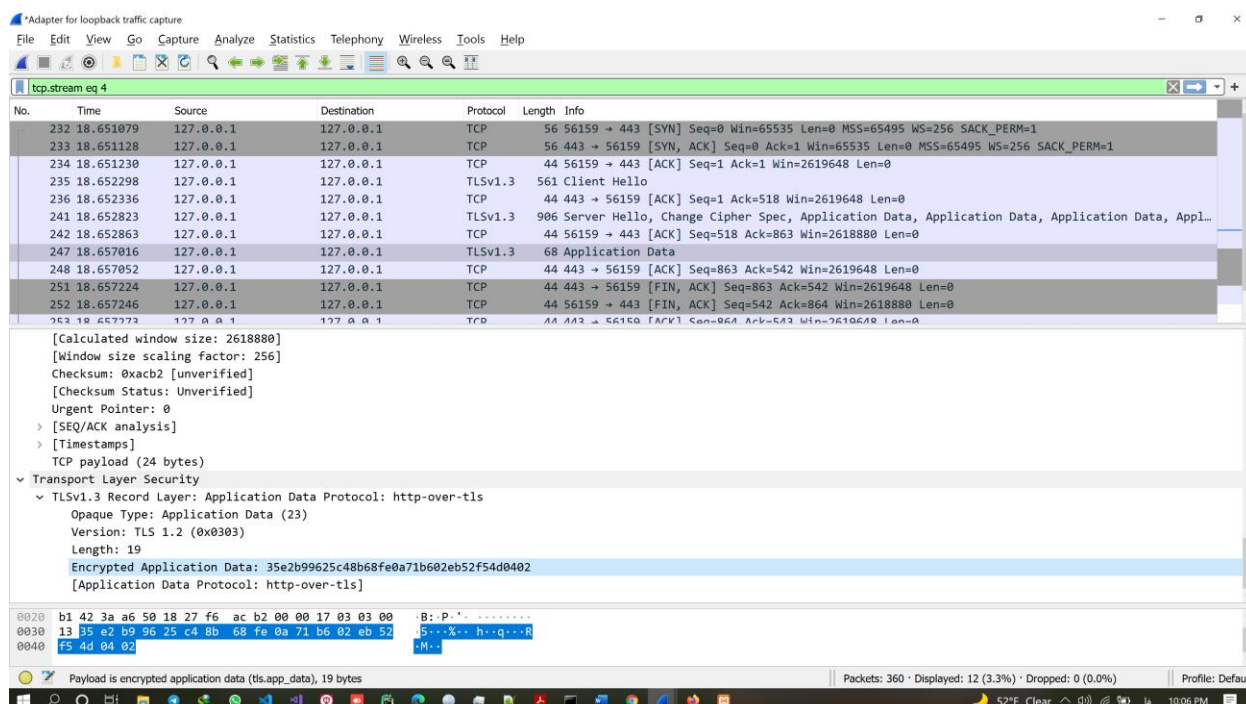
سوال 5 :

این گواهی توسط localhost برای localhost صادر شده. اعتبار آن از 2009/11/11 تا 2019/9/11 است. کلید عمومی آن RSA(1024 bytes) است و الگوریتم امضا RSA encrypting می باشد.



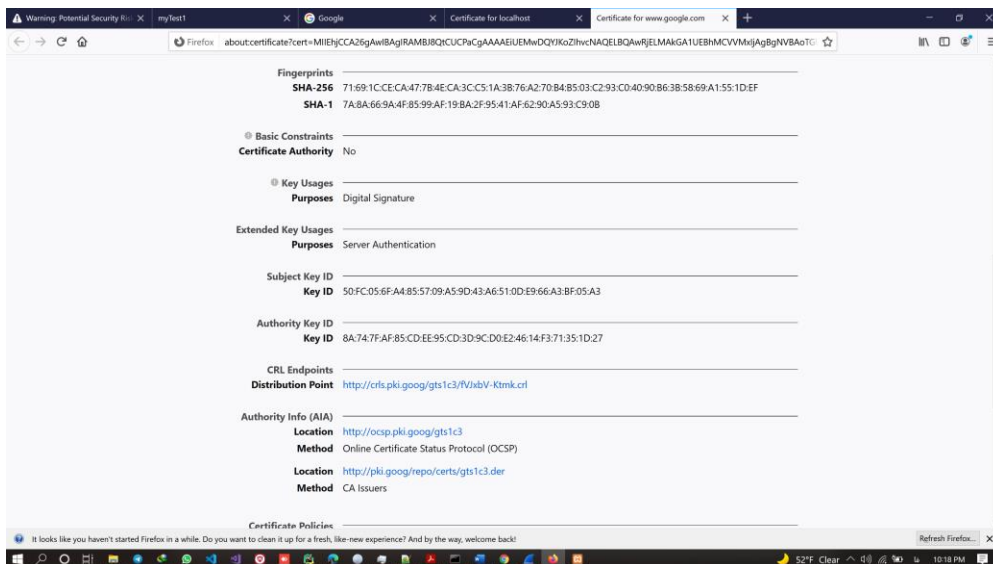
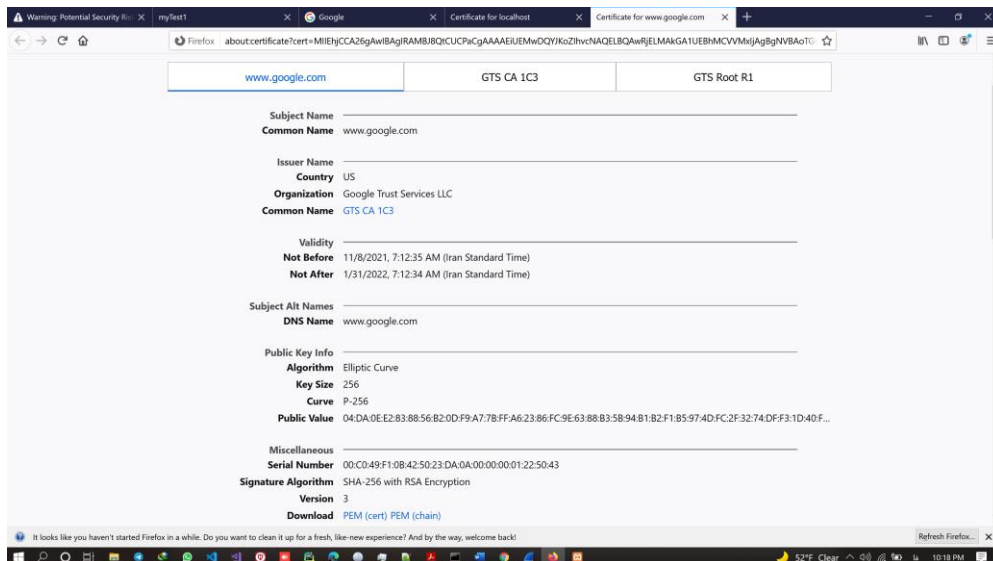
سوال 6 :

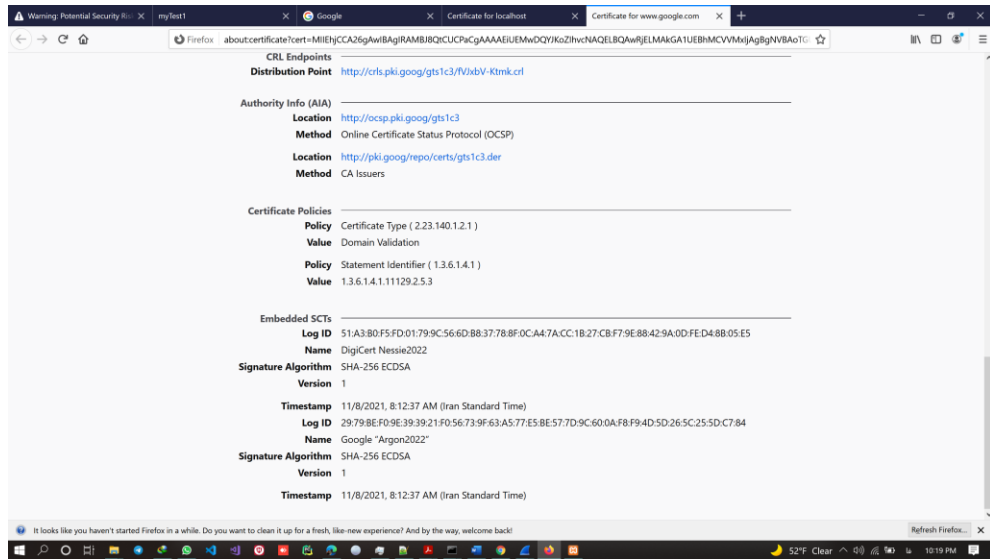
خیر نمی توان خواند زیرا این ارتباط رمز گذاری شده و داده به صورت رمز گذاری شده است. (متن هایلایت شده)



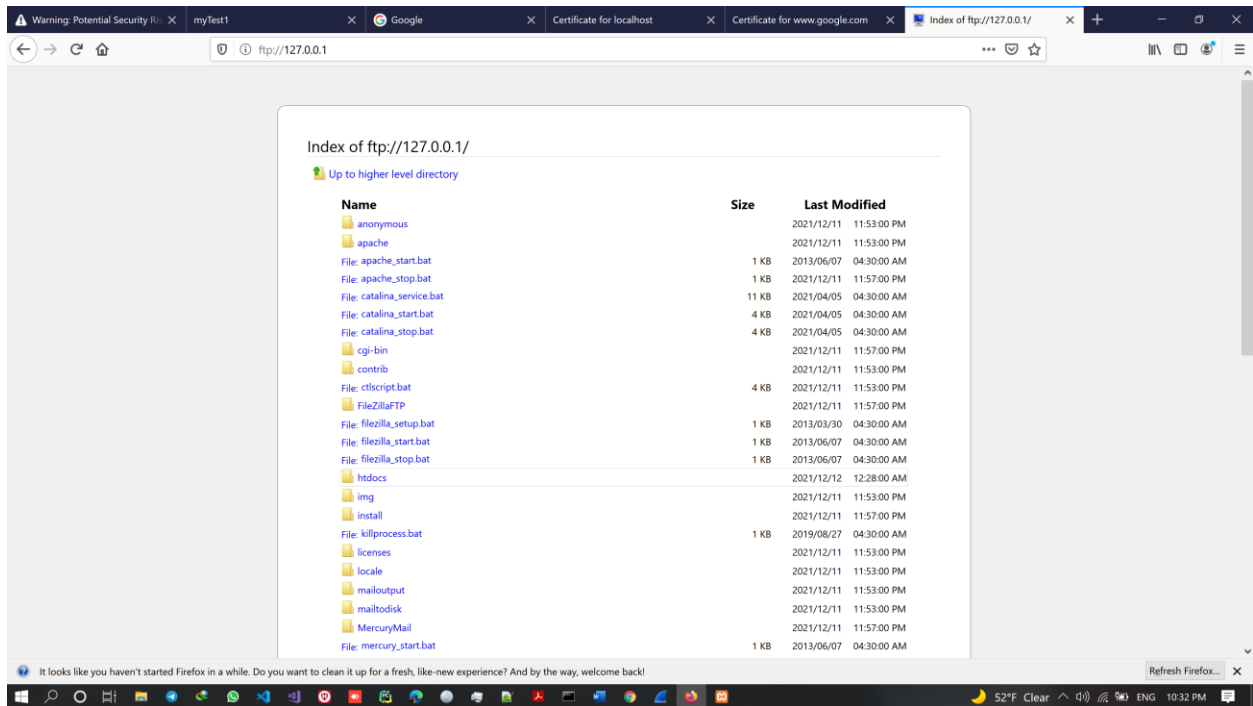
سوال 7 :

صادر کننده گواهی و مدت اعتبار آن متفاوت است. همین طور فیلد های بیشتری دارد و همین طور الگوریتم جدیدی برای رمز گذاری مشاهده می شود.





سوال 8 :



با دستوری به نام list دایرکتوری ها لیست می شوند.

Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
200	1.415090	127.0.0.1	127.0.0.1	FTP	75	Response: 257 "/" is current directory.
210	1.415494	127.0.0.1	127.0.0.1	FTP	52	Request: TYPE I
212	1.415670	127.0.0.1	127.0.0.1	FTP	63	Response: 200 Type set to I
222	1.416072	127.0.0.1	127.0.0.1	FTP	50	Request: PASV
224	1.416705	127.0.0.1	127.0.0.1	FTP	91	Response: 227 Entering Passive Mode (127,0,0,1,219,233)
240	1.417555	127.0.0.1	127.0.0.1	FTP	51	Request: CWD /
248	1.417992	127.0.0.1	127.0.0.1	FTP	91	Response: 250 CWD successful. "/" is current directory.
261	1.419487	127.0.0.1	127.0.0.1	FTP	50	Request: LIST
263	1.421156	127.0.0.1	127.0.0.1	FTP	69	Response: 150 Connection accepted
277	1.421664	127.0.0.1	127.0.0.1	FTP	61	Response: 226 Transfer OK
265	1.421316	127.0.0.1	127.0.0.1	FTP-DA	3299	FTP Data: 3255 bytes (PASV) (CWD /)
1	0.000000	127.0.0.1	127.0.0.1	TCP	45	56036 → 56035 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1
2	0.000023	127.0.0.1	127.0.0.1	TCP	44	56035 → 56036 [ACK] Seq=1 Ack=2 Win=60260 Len=0
3	0.000050	127.0.0.1	127.0.0.1	TCP	45	56036 → 56035 [PSH, ACK] Seq=2 Ack=1 Win=65535 Len=1
4	0.000074	127.0.0.1	127.0.0.1	TCP	44	56035 → 56036 [ACK] Seq=1 Ack=3 Win=60259 Len=0
5	0.000107	127.0.0.1	127.0.0.1	TCP	45	56036 → 56035 [PSH, ACK] Seq=3 Ack=1 Win=65535 Len=1

Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 127.0.0.1
Destination Address: 127.0.0.1

> Transmission Control Protocol, Src Port: 56296, Dst Port: 21, Seq: 74, Ack: 503, Len: 6

File Transfer Protocol (FTP)
LIST\r\n
Request command: LIST
[Current working directory: /]

0010 7f 00 00 01 7f 00 00 01 db e8 00 15 bc 94 c5 8f
0020 a7 b5 0f 4f 50 18 27 f7 c7 fe 00 00 4c 49 53 54 ...OP...LIST
0030 0d 0a ..

File Transfer Protocol (FTP) (ftp), 6 bytes

Packets: 305 · Displayed: 305 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

پروتکل لایه transport از نوع TCP است و پورت مبدا 56296 و پورت مقصد 21 می باشد.

همین طور نام کاربری test می باشد.

Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
117	1.402712	127.0.0.1	127.0.0.1	FTP	75	Response: 257 "/" is current directory.
127	1.408157	127.0.0.1	127.0.0.1	FTP	52	Request: TYPE I
129	1.408981	127.0.0.1	127.0.0.1	FTP	63	Response: 200 Type set to I
139	1.410553	127.0.0.1	127.0.0.1	FTP	50	Request: PASV
141	1.411187	127.0.0.1	127.0.0.1	FTP	91	Response: 227 Entering Passive Mode (127,0,0,1,219,233)
151	1.413249	127.0.0.1	127.0.0.1	FTP	51	Request: CWD /
153	1.413597	127.0.0.1	127.0.0.1	FTP	91	Response: 250 CWD successful. "/" is current directory.
156	1.413684	127.0.0.1	127.0.0.1	FTP	50	Request: LIST
158	1.413753	127.0.0.1	127.0.0.1	FTP	69	Response: 150 Connection accepted
160	1.413766	127.0.0.1	127.0.0.1	FTP	61	Response: 226 Transfer OK
162	1.413817	127.0.0.1	127.0.0.1	FTP-DA	3299	FTP Data: 3255 bytes (PASV) (CWD /)
163	1.413823	127.0.0.1	127.0.0.1	TCP	45	56036 → 56035 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1
164	1.413828	127.0.0.1	127.0.0.1	TCP	44	56035 → 56036 [ACK] Seq=1 Ack=2 Win=60260 Len=0
167	1.413844	127.0.0.1	127.0.0.1	TCP	45	56036 → 56035 [PSH, ACK] Seq=2 Ack=1 Win=65535 Len=1
170	1.413893	127.0.0.1	127.0.0.1	TCP	44	56035 → 56036 [ACK] Seq=1 Ack=3 Win=60259 Len=0
171	1.413896	127.0.0.1	127.0.0.1	TCP	45	56036 → 56035 [PSH, ACK] Seq=3 Ack=1 Win=65535 Len=1

Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000
[Header checksum status: Unverified]
Source Address: 127.0.0.1
Destination Address: 127.0.0.1

> Transmission Control Protocol, Src Port: 56296, Dst Port: 21, Seq: 74, Ack: 503, Len: 6

File Transfer Protocol (FTP)
331 Password required for test
PASS 123
230 Logged on
SYST
215 UNIX emulated by FileZilla
FEAT
211-Features:
MDTM
REST STREAM
SIZE
MLST type*;size*;modify*;
MLSD
UTF8
CLNT
MFMT
211 End
OPTS UTF8 ON
200 UTF8 mode enabled
PWD
257 "/" is current directory.
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (127,0,0,1,219,233)
CWD /
250 CWD successful. "/" is current directory.
LIST
150 Connection accepted
226 Transfer OK

Packet 117, 10 client pkts, 23 server pkts, 20 turns. Click to select.

Entire conversation (623 bytes)

Show data as ASCII

Find:

Stream 3

Find Next

Filter Out This Stream

Print

Save as...

Back

Close

Help

Packets: 0 (0.0%)

Profile: Default

پروتکل http :

مقدار connection برابر keep-alive است و همین طور user-agent برابر است با **Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0** که بیانگر مواردی مانند سیستم عامل و مرورگر مورد استفاده و vender و ورژن مورد استفاده کاربر است.

