



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

به نام ایزد یکتا



دانشکده مهندسی کامپیوتر

آزمایش سوم درس آزمایشگاه شبکه‌های کامپیوتری

گروه دوم

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

No.	Time	Source	Destination	Protocol	Length	Info
465	31.858084	127.0.0.1	127.0.0.1	TCP	45	10731 → 10730 [PSH, ACK] Seq=149 Ack=1 Win=65535 Len=1
466	31.858113	127.0.0.1	127.0.0.1	TCP	44	10730 → 10731 [ACK] Seq=1 Ack=150 Win=64309 Len=0
467	31.858187	127.0.0.1	127.0.0.1	TCP	45	10731 → 10730 [PSH, ACK] Seq=150 Ack=1 Win=65535 Len=1
468	31.858210	127.0.0.1	127.0.0.1	TCP	44	10730 → 10731 [ACK] Seq=1 Ack=151 Win=64308 Len=0
469	31.858253	127.0.0.1	127.0.0.1	TCP	45	10731 → 10730 [PSH, ACK] Seq=151 Ack=1 Win=65535 Len=1
470	31.858273	127.0.0.1	127.0.0.1	TCP	44	10730 → 10731 [ACK] Seq=1 Ack=152 Win=64307 Len=0
471	31.858450	127.0.0.1	127.0.0.1	HTTP	464	GET / HTTP/1.1
472	31.858478	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [ACK] Seq=1 Ack=421 Win=525568 Len=0
473	31.860800	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
474	31.860863	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=421 Ack=247 Win=525312 Len=0
475	31.861028	127.0.0.1	127.0.0.1	TCP	45	10731 → 10730 [PSH, ACK] Seq=152 Ack=1 Win=65535 Len=1
476	31.861055	127.0.0.1	127.0.0.1	TCP	44	10730 → 10731 [ACK] Seq=1 Ack=153 Win=64306 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
376	31.239621	127.0.0.1	127.0.0.1	TCP	56	13210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PERM=1
377	31.239652	127.0.0.1	127.0.0.1	TCP	56	80 → 13210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
378	31.239724	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
471	31.858450	127.0.0.1	127.0.0.1	HTTP	464	GET / HTTP/1.1
472	31.858478	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [ACK] Seq=1 Ack=421 Win=525568 Len=0
473	31.860800	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
474	31.860863	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=421 Ack=247 Win=525312 Len=0
608	36.861728	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [FIN, ACK] Seq=247 Ack=421 Win=525568 Len=0
609	36.861838	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=421 Ack=248 Win=525312 Len=0
610	36.862046	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [FIN, ACK] Seq=421 Ack=248 Win=525312 Len=0
611	36.862120	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [ACK] Seq=248 Ack=422 Win=525568 Len=0

Wireshark · Follow HTTP Stream (tcp.stream eq 6) · Adapter for loopback traffic capture

```

GET / HTTP/1.1
Host: www.exomah.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 21 May 2021 15:10:53 GMT
If-None-Match: "88-5c2d8774aa938"

HTTP/1.1 304 Not Modified
Date: Fri, 21 May 2021 15:47:18 GMT
Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/8.0.6
Last-Modified: Fri, 21 May 2021 15:10:53 GMT
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```

سوال (۱)

- > Frame 471: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface \Device\NPF_{Loopback}, id 0
- > Null/Loopback
- > Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- > Transmission Control Protocol, Src Port: 13210, Dst Port: 80, Seq: 1, Ack: 1, Len: 420
- > Hypertext Transfer Protocol

شماره پورت مبدا: ۱۳۳۱۰

شماره پورت مقصد: ۸۰

در ابتدای برقراری اتصال http یک کانکشن tcp ایجاد می‌شود و پس از آن html base file از سرور درخواست و دریافت می‌شود و پس از آن با توجه به فایل html، درخواستهایی برای دریافت آبجکت‌های وب فرستاده می‌شود. آدرس ip سایت درخواستی برای وب سرور فرستاده می‌شود و از این راه می‌تواند سایت درخواستی را تشخیص دهد.

(سوال ۲)

No.	Time	Source	Destination	Protocol	Length	Info
376	31.239621	127.0.0.1	127.0.0.1	TCP	56	13210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=65495 WS=256 SACK_PERM=1
377	31.239652	127.0.0.1	127.0.0.1	TCP	56	80 → 13210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
378	31.239724	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
471	31.858450	127.0.0.1	127.0.0.1	HTTP	464	GET / HTTP/1.1
472	31.858478	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [ACK] Seq=1 Ack=421 Win=525568 Len=0
473	31.860800	127.0.0.1	127.0.0.1	HTTP	290	HTTP/1.1 304 Not Modified
474	31.860863	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=421 Ack=247 Win=525312 Len=0
608	36.861728	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [FIN, ACK] Seq=247 Ack=421 Win=525568 Len=0
609	36.861838	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [ACK] Seq=421 Ack=248 Win=525312 Len=0
610	36.862046	127.0.0.1	127.0.0.1	TCP	44	13210 → 80 [FIN, ACK] Seq=421 Ack=248 Win=525312 Len=0
611	36.862120	127.0.0.1	127.0.0.1	TCP	44	80 → 13210 [ACK] Seq=248 Ack=422 Win=525568 Len=0


```

> Frame 471: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 13210, Dst Port: 80, Seq: 1, Ack: 1, Len: 420
> Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.exomah.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Fri, 21 May 2021 15:10:53 GMT\r\n
    If-None-Match: "88-5c2d8774aa938"\r\n
  \r\n
  
```

مقدار بخش keep alive: connection (یعنی ارتباط tcp بسته نشود این نوع ارتباط http از نوع پایا یا persistent می‌باشد)

درخواست از نوع GET است. مقدار UA که در شکل نیز مشخص شده است بیانگر مشخصات مرورگر مبدا است.

```

Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
✓ Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...0 = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....S.]
Window: 64240
[Calculated window size: 64240]

```

0000	02 00 00 00 45 00 00 34	29 2e 40 00 80 06 00 00E..4).@.....
0010	7f 00 00 01 7f 00 00 01	33 9a 00 50 33 b4 38 b93..P3.8.
0020	00 00 00 00 80 02 fa f0	db a1 00 00 02 04 ff d7
0030	01 03 03 08 01 01 04 02	

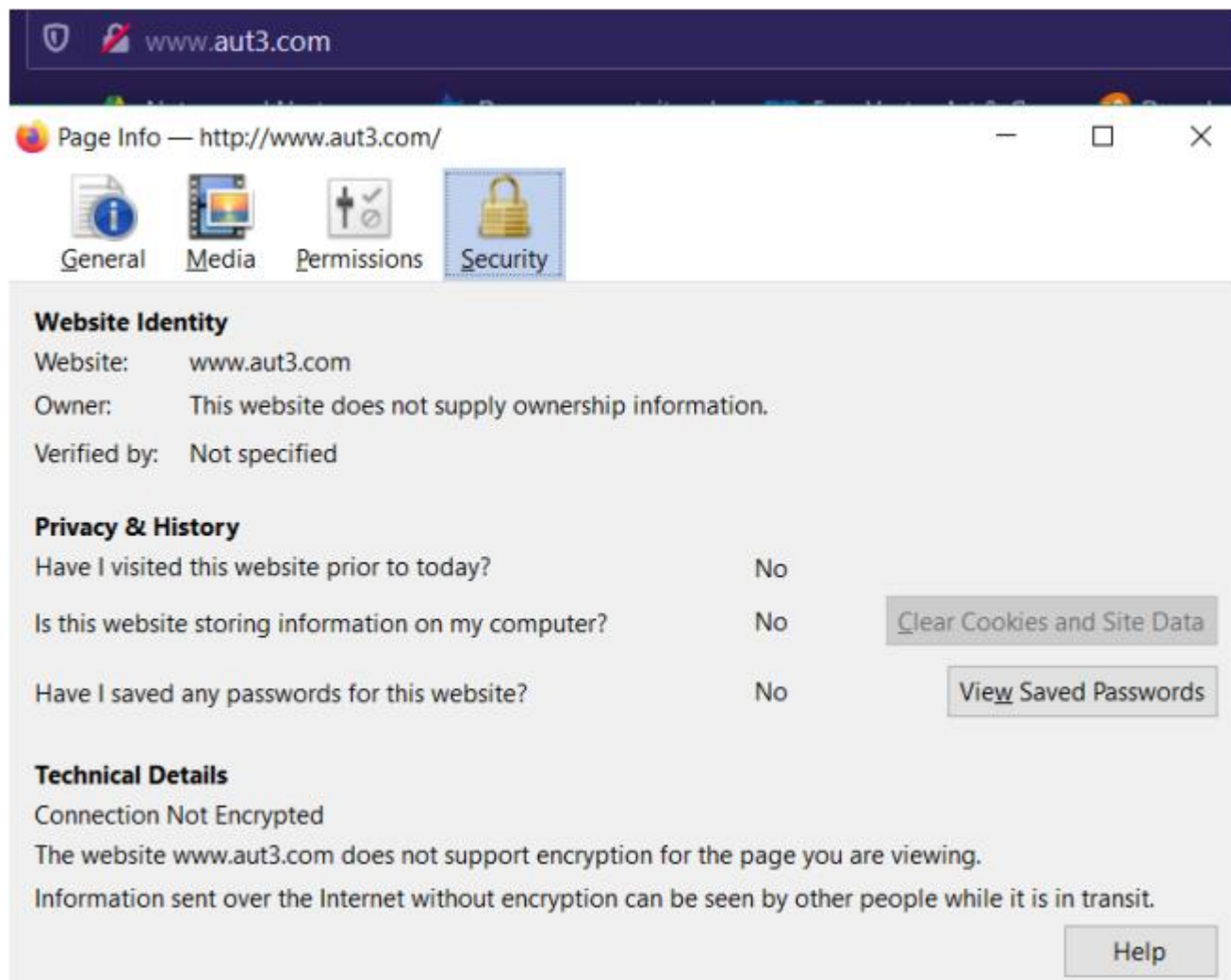
مقدار flag هایی که در اولین بسته‌ی پروتکل TCP ست شده‌اند در تصویر بالا قابل مشاهده است.

```

> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 13884, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
▼ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.aut3.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.aut3.com/]
    [HTTP request 1/2]
    [Response in frame: 6354]

```

این بار از ادرس aut3.com استفاده کردیم. همانطوری که مشاهده میکنید آدرس پورت مبدا متفاوت است تا بتوان بستههای مربوط به آنها را از هم جدا کرد. طول بستههای آنها نیز متفاوت است. پارامترهای acknowledge number و sequence number هر دو که به صورت raw تنظیم شدهاست هم متفاوت است.



حالا برای کانکشن https برای همین دامنه، اطلاعات مربوط به certificate :

localhost

Subject Name

Common Name localhost

Issuer Name

Common Name localhost

صادر شده توسط: localhost
برای: localhost

Validity

Not Before Tue, 10 Nov 2009 23:48:47 GMT
Not After Fri, 08 Nov 2019 23:48:47 GMT

مدت زمان اعتبار
منقضی شده

Public Key Info

Algorithm RSA
Key Size 1024
Exponent 65537
Modulus C1:25:D3:27:E3:EC:AD:0D:83:6A:6D:E7:5F:9A:75:10:23:E2:90:9D:A0:63:95:8F:1D:4...

Miscellaneous

Serial Number 00:B5:C7:52:C9:87:81:B5:03
Signature Algorithm SHA-1 with RSA Encryption
Version NaN
Download PEM (cert) PEM (chain)

Fingerprints

SHA-256 01:69:73:38:0C:0F:1D:F0:0B:D9:59:3E:D8:D5:EF:A3:70:6C:D6:DF:79:93:F6:14:12:72:....
SHA-1 B0:23:8C:54:7A:90:5B:FA:11:9C:4E:8B:AC:CA:EA:CF:36:49:1F:F6

سوال (۶)

No.	Time	Source	Destination	Protocol	Length	Info
102	6.319135	127.0.0.1	127.0.0.1	TLSv1.3	561	Client Hello
108	6.320061	127.0.0.1	127.0.0.1	TLSv1.3	906	Server Hello, Change Cipher Spec, Appl
> Frame 108: 906 bytes on wire (7248 bits), 906 bytes captured (7248 bits) on interface \Device\NPF_{Loopback}, id 0 > Null/Loopback > Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 > Transmission Control Protocol, Src Port: 443, Dst Port: 14487, Seq: 1, Ack: 518, Len: 862 > Transport Layer Security						
> TLSv1.3 Record Layer: Handshake Protocol: Server Hello Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 122 > Handshake Protocol: Server Hello						
> TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec Content Type: Change Cipher Spec (20) Version: TLS 1.2 (0x0303) Length: 1 Change Cipher Spec Message						
> TLSv1.3 Record Layer: Application Data Protocol: http-over-tls Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 38 Encrypted Application Data: c57fd94a52940ca01a7afafd6c305f256adf50ce15257a16d4e61e17245813c15029a5e0... [Application Data Protocol: http-over-tls]						
> TLSv1.3 Record Layer: Application Data Protocol: http-over-tls Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 449 Encrypted Application Data: 30c014d8f75e7df09560156b0465f090099a4d2f300b371d2435b7ee19eb580da14499d0... [Application Data Protocol: http-over-tls]						
> TLSv1.3 Record Layer: Application Data Protocol: http-over-tls Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 153 Encrypted Application Data: e3ee513871579509e3dabcc498d435ac5336d9b73ccade6cb50f4218f625d61a9f31338d... [Application Data Protocol: http-over-tls]						
> TLSv1.3 Record Layer: Application Data Protocol: http-over-tls Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303)						

خیر. از آنجایی که از پروتکل tls استفاده شده است، متن این ارتباط قابل خواندن نیست. پروتکل tls وظیفه رمزگذاری encryption ارتباط بین سرور و کلاینت را به عهده دارد.

سوال (۷)

نتایج مشاهده‌ی certificate سایت گوگل:

www.google.com		GTS CA 101	GlobalSign
Subject Name			Miscellaneous
Country	US		Serial Number 00:FE:DD:8D:C7:EE:F6:EB:49:05:00:00:00:87:CC:17
State/Province	California		Signature Algorithm SHA-256 with RSA Encryption
Locality	Mountain View		Version 3
Organization	Google LLC		Download PEM (cert) PEM (chain)
Common Name	www.google.com		
Issuer Name			Fingerprints
Country	US		SHA-256 6E:AF:ED:04:94:61:BD:EA:B7:A3:20:7E:72:F8:0E:0C:9D:4C:79:80:6C:E4:43:DE:3B:29...
Organization	Google Trust Services		SHA-1 67:E9:C1:B1:15:CA:6F:E9:E7:35:1A:B2:B6:C7:36:06:97:52:E6:CE
Common Name	GTS CA 101		
Validity			Basic Constraints
Not Before	Mon, 03 May 2021 11:24:19 GMT		Certificate Authority No
Not After	Mon, 26 Jul 2021 11:24:18 GMT		
Subject Alt Names			Key Usages
DNS Name	www.google.com		Purposes Digital Signature
Public Key Info			Extended Key Usages
Algorithm	Elliptic Curve		Purposes Server Authentication
Key Size	256		
Curve	P-256		
Public Value	04:35:A6:91:67:2A:BE:DA:F0:95:EA:D0:20:87:A4:35:1D:30:42:E1:34:E3:2A:3F:A9:8...		Subject Key ID
			Key ID DB:77:7F:18:75:36:1E:7C:DF:DF:5D:D4:43:37:D2:6A:52:B2:41:57
			Authority Key ID
			Key ID 98:D1:F8:6E:10:EB:CF:9B:EC:60:9F:18:90:1B:A0:EB:7D:09:FD:2B

CRL Endpoints	
Distribution Point	http://crl.pki.goog/GTS101core.crl
Authority Info (AIA)	
Location	http://ocsp.pki.goog/gts1o1core
Method	Online Certificate Status Protocol (OCSP)
Location	http://pki.goog/gsr2/GTS101.crt
Method	CA Issuers
Certificate Policies	
Policy	Certificate Type (2.23.140.1.2.2)
Value	Organization Validation
Policy	Statement Identifier (1.3.6.1.4.1)
Value	1.3.6.1.4.1.11129.2.5.3
Embedded SCTs	
Log ID	44:94:65:2E:B0:EE:CE:AF:C4:40:07:D8:A8:FE:28:C0:DA:E6:82:BE:D8:CB:31:B5:3F:D3...
Name	Cloudflare "Nimbus2021"
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 03 May 2021 12:24:20 GMT
Log ID	F6:5C:94:2F:D1:77:30:22:14:54:18:08:30:94:56:8E:E3:4D:13:19:33:BF:DF:0C:2F:20:0...
Name	Google "Argon2021"
Signature Algorithm	SHA-256 ECDSA
Version	1
Timestamp	Mon, 03 May 2021 12:24:20 GMT

این مدرک، اطلاعات بیشتری را شامل میشود. به عنوان اولین تفاوت می توان به تفاوت صادر کننده و دریافت کننده مدرک اشاره کرد و اینکه مدرک گوگل منقضی نشده است و تا تاریخ 26 جوالی 2021 اعتبار دارد. الگوریتم به کار رفته برای امضا نیز متفاوت می باشد.

(سوال ۸)

15311	651.574861	127.0.0.1	127.0.0.1	FTP	51 Request: CWD /
15316	651.575011	127.0.0.1	127.0.0.1	FTP	91 Response: 250 CWD successful. "/" is current directory.
15330	651.575691	127.0.0.1	127.0.0.1	FTP	50 Request: LIST
15332	651.577653	127.0.0.1	127.0.0.1	FTP	69 Response: 150 Connection accepted
15351	651.577999	127.0.0.1	127.0.0.1	FTP	61 Response: 226 Transfer OK


```

> Frame 15330: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 14917, Dst Port: 21, Seq: 76, Ack: 501, Len: 6
v File Transfer Protocol (FTP)
  LIST\r\n
    Request command: LIST
[Current working directory: /]

```

از دستور LIST برای گرفتن لیست فایلها استفاده میشود. نام کاربری استفاده شده در اینجا test است (همانطوری که در تنظیمات FileZilla ایجادش کردیم و با آن الگین کردیم)

15157	645.628147	127.0.0.1	127.0.0.1	FTP	89 Response: 220-1164118 Server version 0.3.41 beta
15159	645.628209	127.0.0.1	127.0.0.1	FTP	89 Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
15164	645.628274	127.0.0.1	127.0.0.1	FTP	105 Response: 220 Please visit http://sourceforge.net/projects/filezilla/
15178	651.567471	127.0.0.1	127.0.0.1	FTP	55 Request: USER test
15180	651.568051	127.0.0.1	127.0.0.1	FTP	76 Response: 331 Password required for test
15190	651.569113	127.0.0.1	127.0.0.1	FTP	56 Request: PASS 12345
15192	651.569550	127.0.0.1	127.0.0.1	FTP	59 Response: 230 Logged on
15202	651.570922	127.0.0.1	127.0.0.1	FTP	50 Request: SYST


```

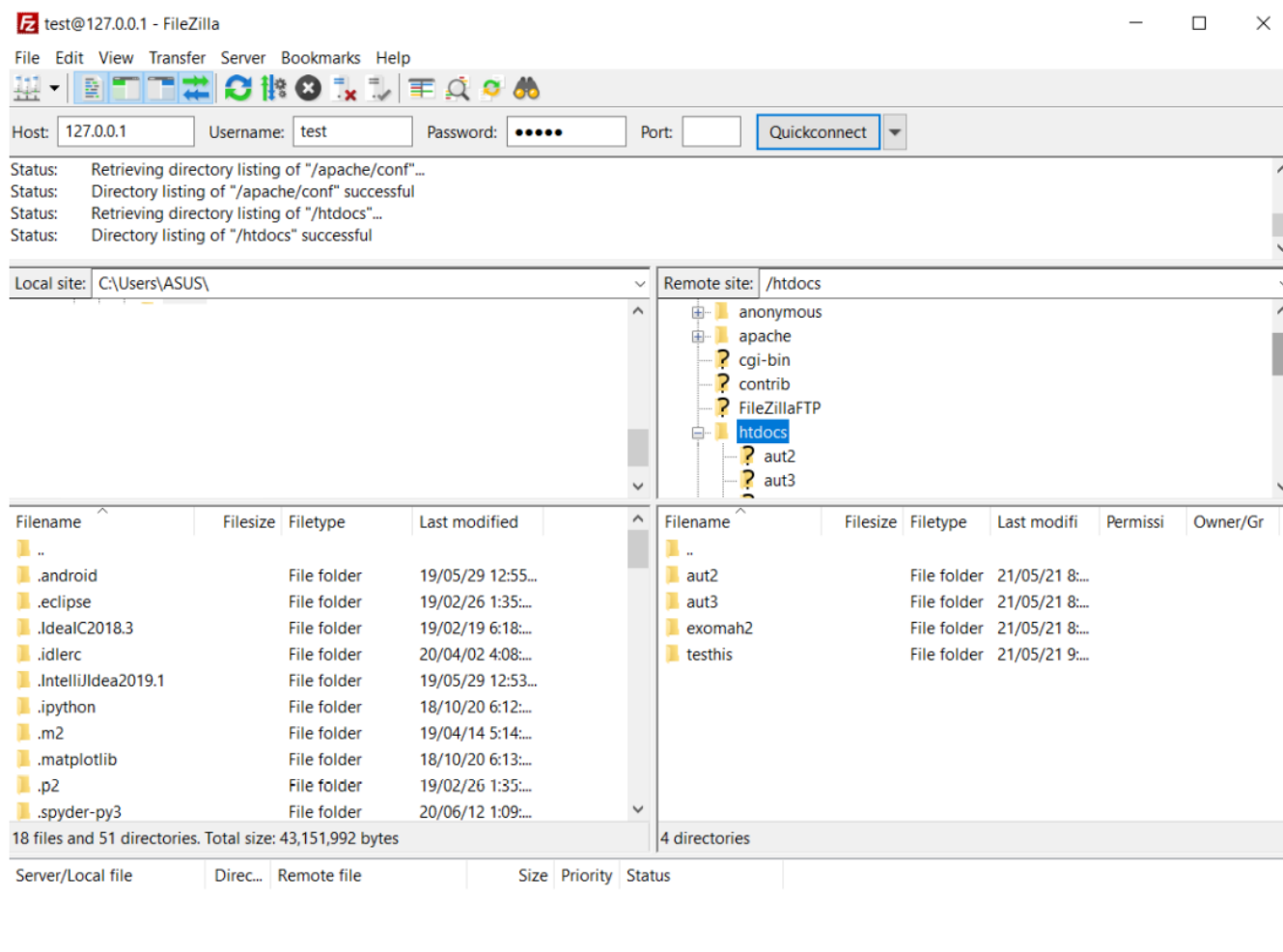
> Frame 15178: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{Loopback}, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 14917, Dst Port: 21, Seq: 1, Ack: 149, Len: 11
v File Transfer Protocol (FTP)
  USER test\r\n
    Request command: USER
    Request arg: test
[Current working directory: ]

```

در این ارتباطات از پروتکل TCP استفاده شده است، با شماره پورت مبدا 14917 و مقصد 21 که در تصاویر بال نیز مشخص شده است.

سوال ۹)

این بار دیگر سایت باز نمی‌شود و مرورگر پیام میدهد که برای اتصال باید از اپلیکیشن دیگری استفاده کنیم که در اینجا ما از FileZilla استفاده می‌کنیم.



اگر بسته‌های مربوط به این ارتباطات را از وایرشارک شنود کنیم، نمیتوانیم هیچ اطلاعاتی را از آن بخوانیم.

[illegible]

پروتوکل HTTP:

در اینجا، بسته‌های مربوط به follow HTTP Stream را مشاهده می‌کنیم.

No.	Time	Source	Destination	Protocol	Length	Info
838	178.550809	192.168.1.103	185.211.88.131	TCP	66	1369 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
842	178.587246	185.211.88.131	192.168.1.103	TCP	62	80 → 1369 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
845	178.587325	192.168.1.103	185.211.88.131	TCP	54	1369 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
847	178.587601	192.168.1.103	185.211.88.131	HTTP	1265	GET / HTTP/1.1
849	178.643500	185.211.88.131	192.168.1.103	TCP	60	80 → 1369 [ACK] Seq=1 Ack=1212 Win=31486 Len=0
850	178.644863	185.211.88.131	192.168.1.103	HTTP	528	HTTP/1.1 301 Moved Permanently (text/html)
852	178.684785	192.168.1.103	185.211.88.131	TCP	54	1369 → 80 [ACK] Seq=1212 Ack=475 Win=17046 Len=0
946	188.644974	192.168.1.103	185.211.88.131	TCP	55	[TCP Keep-Alive] 1369 → 80 [ACK] Seq=1211 Ack=475 Win=17046 Len=1
947	188.675630	185.211.88.131	192.168.1.103	TCP	66	[TCP Keep-Alive ACK] 80 → 1369 [ACK] Seq=475 Ack=1212 Win=31486 Len=0 SLE=1211 SRE=1212
958	193.659367	185.211.88.131	192.168.1.103	TCP	60	80 → 1369 [FIN, ACK] Seq=475 Ack=1212 Win=31486 Len=0
959	193.659513	192.168.1.103	185.211.88.131	TCP	54	1369 → 80 [ACK] Seq=1212 Ack=476 Win=17046 Len=0
960	193.659730	192.168.1.103	185.211.88.131	TCP	54	1369 → 80 [FIN, ACK] Seq=1212 Ack=476 Win=17046 Len=0
961	193.691526	185.211.88.131	192.168.1.103	TCP	60	80 → 1369 [ACK] Seq=476 Ack=1213 Win=31486 Len=0

اطلاعات مربوط به پروتکل tcp و فلگ‌ها: (در این کانکشن از این پروتکل لایه انتقال استفاده می‌شود)

Transmission Control Protocol, Src Port: 1369, Dst Port: 80, Seq: 1, Ack: 1, Len: 1211

Source Port: 1369

Destination Port: 80

[Stream index: 64]

[TCP Segment Len: 1211]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1380490331

[Next Sequence Number: 1212 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2664919712

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, 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

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:AP...]

Window: 17520

[Calculated window size: 17520]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0xafee [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

اطالعات مربوط به پروتکل http :

```
Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
Host: aut.ac.ir\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
> [truncated]Cookie: _ga=GA1.3.234810661.1617441214; 969af8aywID_67c5c_mysid=1; HASH_969af8aywID_67c5c_mysid=9C42D581404D31E721F936995065138F04
\r\n
[Full request URI: http://aut.ac.ir/]
[HTTP request 1/1]
[Response in frame: 850]
```

همانطور که مشاهده می‌شود، اتصال از نوع keep-alive است که کانکشن tcp باز بماند. نوع پروتکل نیز get است. مقدار UA در تصویر مشخص شده است که نشان دهنده‌ی اطالعات مرورگر مبدا است.

پروتکل FTP: در اینجا بسته‌های مربوط به follow HTTP Stream را مشاهده می‌کنیم.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.276505	195.83.118.1	192.168.1.103	TCP	66	21 → 1403 [SYN, ACK] Seq=0 Ack=1 Win=13900 Len=0 MSS=1390 WS=1 SACK_PERM=1
9	0.276711	192.168.1.103	195.83.118.1	TCP	54	1403 → 21 [ACK] Seq=1 Ack=1 Win=66560 Len=0
16	0.600827	195.83.118.1	192.168.1.103	FTP	60	Response: 220-
17	0.640846	192.168.1.103	195.83.118.1	TCP	54	1403 → 21 [ACK] Seq=1 Ack=7 Win=66560 Len=0
18	0.734287	195.83.118.1	192.168.1.103	FTP	1038	Response: 70 Request: USER anonymous
19	0.735504	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=991 Ack=17 Win=13916 Len=0
20	0.768975	195.83.118.1	192.168.1.103	FTP	103	Response: 331 Guest login ok, type your name as password.
21	0.899015	195.83.118.1	192.168.1.103	FTP	80	Request: PASS mozilla@example.com
22	0.899333	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1040 Ack=43 Win=13942 Len=0
23	0.932364	195.83.118.1	192.168.1.103	FTP	60	Response: 230-
24	1.064791	195.83.118.1	192.168.1.103	TCP	54	1403 → 21 [ACK] Seq=43 Ack=1046 Win=65536 Len=0
25	1.105807	192.168.1.103	195.83.118.1	FTP	397	Response: \tVous etes dans la classe guest,
26	1.197508	195.83.118.1	192.168.1.103	FTP	60	Request: SYST
27	1.198546	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1389 Ack=49 Win=13948 Len=0
28	1.233274	195.83.118.1	192.168.1.103	FTP	103	Response: 215 UNIX Type: L8 Version: NetBSD-Ftpd 20110904
29	1.366802	195.83.118.1	192.168.1.103	FTP	60	Request: FEAT
30	1.367419	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1438 Ack=55 Win=13954 Len=0
31	1.398702	195.83.118.1	192.168.1.103	FTP	78	Response: 211-Features supported
32	1.530629	195.83.118.1	192.168.1.103	FTP	54	1403 → 21 [ACK] Seq=55 Ack=1462 Win=66560 Len=0
33	1.571597	192.168.1.103	195.83.118.1	FTP	140	Response: MDTM
34	1.662641	195.83.118.1	192.168.1.103	FTP	59	Request: PWD
35	1.663015	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1548 Ack=60 Win=13959 Len=0
36	1.693952	195.83.118.1	192.168.1.103	FTP	89	Response: 257 "/" is the current directory.
37	1.826344	195.83.118.1	192.168.1.103	FTP	62	Request: TYPE I
38	1.827525	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1583 Ack=68 Win=13967 Len=0
39	1.858477	195.83.118.1	192.168.1.103	FTP	74	Response: 200 Type set to I.
40	2.012069	195.83.118.1	192.168.1.103	FTP	60	Request: PASV
41	2.013487	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1603 Ack=74 Win=13973 Len=0
42	2.044954	195.83.118.1	192.168.1.103	FTP	103	Response: 227 Entering Passive Mode (195,83,118,1,195,33)
43	2.180099	195.83.118.1	192.168.1.103	FTP	61	Request: CWD /
44	2.181274	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1652 Ack=81 Win=13980 Len=0
46	2.213090	195.83.118.1	192.168.1.103	FTP	83	Response: 250 CWD command successful.
47	2.345489	195.83.118.1	192.168.1.103	FTP	60	Request: LIST
48	2.345988	192.168.1.103	195.83.118.1	FTP	60	21 → 1403 [ACK] Seq=1681 Ack=87 Win=13986 Len=0
51	2.376943	195.83.118.1	192.168.1.103	FTP	110	Response: 150 Opening BINARY mode data connection for '/bin/ls'.
52	2.516472	195.83.118.1	192.168.1.103	FTP	54	1403 → 21 [FIN, ACK] Seq=87 Ack=1737 Win=66304 Len=0
58	2.522073	192.168.1.103	195.83.118.1	TCP		

پروتکل استفاده شده در این اتصال، پروتکل TCP است. پورت مقصد 21 و پورت مبدا 1403 است.

tcp.stream eq 0111

No.	Time	Source	Destination	Protocol	Length	Info
38	1.827525	192.168.1.103	195.83.118.1	FTP	62	Request: TYPE I
39	1.858477	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1583 Ack=68 Win=13967 Len=0
40	2.012069	195.83.118.1	192.168.1.103	FTP	74	Response: 200 Type set to I.
41	2.013487	192.168.1.103	195.83.118.1	FTP	60	Request: PASV
42	2.044954	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1603 Ack=74 Win=13973 Len=0
43	2.180099	195.83.118.1	192.168.1.103	FTP	103	Response: 227 Entering Passive Mode (195,83,118,1,195,33)
44	2.181274	192.168.1.103	195.83.118.1	FTP	61	Request: CWD /
46	2.213090	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1652 Ack=81 Win=13980 Len=0
47	2.345489	195.83.118.1	192.168.1.103	FTP	83	Response: 250 CWD command successful.
48	2.345988	192.168.1.103	195.83.118.1	FTP	60	Request: LIST
51	2.376943	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1681 Ack=87 Win=13986 Len=0
52	2.516472	195.83.118.1	192.168.1.103	FTP	110	Response: 150 Opening BINARY mode data connection for '/bin/ls'.
58	2.522073	192.168.1.103	195.83.118.1	TCP	54	1403 → 21 [FIN, ACK] Seq=87 Ack=1737 Win=66304 Len=0
59	2.552115	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1737 Ack=88 Win=13986 Len=0
60	2.653128	195.83.118.1	192.168.1.103	FTP	78	Response: 226 Transfer complete.
61	2.653196	192.168.1.103	195.83.118.1	TCP	54	1403 → 21 [RST, ACK] Seq=88 Ack=1761 Win=0 Len=0

> Frame 48: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{B7C9CAFE-7328-4144-A682-34275519EC33}, id 0
 > Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
 > Internet Protocol Version 4, Src: 192.168.1.103, Dst: 195.83.118.1
 > Transmission Control Protocol Src Port: 1403, Dst Port: 21, Seq: 81, Ack: 1681, Len: 6
 > File Transfer Protocol (FTP)
 [Current working directory: /]

مقدار یوزنیم و پسورد به ترتیب anonymous و com.exmapple@mozilla می باشد که در تصویر بعدی نیز مشخص شده است:

17	0.640840	192.168.1.103	195.83.118.1	TCP	54	1403 → 21 [ACK] Seq=1 Ack=/ Win=0 Len=0
18	0.734287	195.83.118.1	192.168.1.103	FTP	1038	Response:
19	0.735504	192.168.1.103	195.83.118.1	FTP	70	Request: USER anonymous
20	0.768975	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=991 Ack=17 Win=13916 Len=0
21	0.899015	195.83.118.1	192.168.1.103	FTP	103	Response: 331 Guest login ok, type your name as password.
22	0.899333	192.168.1.103	195.83.118.1	FTP	80	Request: PASS mozilla@example.com
23	0.932364	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1040 Ack=43 Win=13942 Len=0
24	1.064791	195.83.118.1	192.168.1.103	FTP	60	Response: 230-
25	1.105807	192.168.1.103	195.83.118.1	TCP	54	1403 → 21 [ACK] Seq=43 Ack=1046 Win=65536 Len=0
26	1.197508	195.83.118.1	192.168.1.103	FTP	397	Response: \tVous etes dans la classe guest,
27	1.198546	192.168.1.103	195.83.118.1	FTP	60	Request: SYST
28	1.233274	195.83.118.1	192.168.1.103	TCP	60	21 → 1403 [ACK] Seq=1389 Ack=49 Win=13948 Len=0

> Frame 19: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{B7C9CAFE-7328-4144-A682-34275519EC33}, id 0
 > Ethernet II, Src: AzureWav_1e:36:59 (80:c5:f2:1e:36:59), Dst: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60)
 > Internet Protocol Version 4, Src: 192.168.1.103, Dst: 195.83.118.1
 > Transmission Control Protocol, Src Port: 1403, Dst Port: 21, Seq: 1, Ack: 991, Len: 16
 > File Transfer Protocol (FTP)
 > USER anonymous\r\n
 Request command: USER
 Request arg: anonymous
 [Current working directory:]

اگر روی این بسته ها کلیک کنیم نیز همین مقادیر را به عنوان نام کاربری و رمز عبور مشاهده خواهیم کرد.