



دانشکده مهندسی
کامپیوتر و فناوری اطلاعات

دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

آزمایشگاه شبکه های کامپیوتری

(پاییز ۱۴۰۰)

جلسه سوم

راه اندازی سرویس های Web و FTP

محمد چوپان ۹۸۳۱۱۲۵

۱- راه‌اندازی سرویس‌های Web و FTP

۱-۱- هدف آزمایش

هدف این آزمایش، آشنایی با تنظیمات مقدماتی مربوط به راه‌اندازی سرویس‌های Web و FTP و تحلیل بسته‌های HTTP و FTP است.

۲-۱- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز در این آزمایش عبارت‌اند از:

- کامپیوتر شخصی با سیستم‌عامل ویندوز 7 به بعد برای هر شخص
- برنامه Filezilla آخرین نسخه

۳-۱- شرح آزمایش

۱-۳-۱- تنظیمات سرور Web

۱. آدرس سایت خود را در مرورگر وارد کنید بسته‌های مربوط به سایت را پیدا کنید. بر روی یکی از آن‌ها کلیک راست کرده و follow HTTP Stream را انتخاب کنید. شکلی مشابه شکل (۱-۱) نمایش داده خواهد شد.

No.	Time	Source	Destination	Protocol	Length	Info
58	5.996343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=65495 SACK_PERM=1
59	5.996343	127.0.0.1	127.0.0.1	TCP	40	80 → 7391 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=65495 SACK_PERM=1
60	5.996343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=1 Ack=1 Win=0 Len=0
61	5.996343	127.0.0.1	127.0.0.1	HTTP	500	GET / HTTP/1.1
62	5.996343	127.0.0.1	127.0.0.1	TCP	40	80 → 7391 [ACK] Seq=1 Ack=541 Win=7652 Len=0
63	5.998343	127.0.0.1	127.0.0.1	HTTP	337	HTTP/1.1 200 OK (text/html)
64	5.998343	127.0.0.1	127.0.0.1	TCP	40	7391 → 80 [ACK] Seq=541 Ack=290 Win=7895 Len=0

سوال ۱: آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

پنجره نمایش داده شده :

No.	Time	Source	Destination	Protocol	Length	Info
97	2.549539	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	1317	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
98	2.549575	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49159 [ACK] Seq=1083 Ack=262 Win=2160896 Len=0
99	2.550629	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	318	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
100	2.550677	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49159 → boinc-client(1043) [ACK] Seq=262 Ack=1357 Win=2159872 Len=0
101	2.551098	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	331	Application Data
102	2.551128	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49159 [ACK] Seq=1357 Ack=549 Win=2160640 Len=0
103	2.552177	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	233	afrog(1042) → 51587 [PSH, ACK] Seq=508 Ack=1 Win=8439 Len=189
104	2.552214	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	51587 → afrog(1042) [ACK] Seq=1 Ack=757 Win=8345 Len=0
105	2.552471	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	1004	Application Data
106	2.552501	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49159 → boinc-client(1043) [ACK] Seq=549 Ack=2317 Win=2158848 Len=0
107	2.553195	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	75	Encrypted Alert
108	2.553227	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49159 [ACK] Seq=2317 Ack=580 Win=2160640 Len=0
109	2.553340	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49159 → boinc-client(1043) [FIN, ACK] Seq=580 Ack=2317 Win=2158848 Len=0
110	2.553356	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49159 [ACK] Seq=2317 Ack=581 Win=2160640 Len=0
111	2.553478	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49159 [FIN, ACK] Seq=2317 Ack=581 Win=2160640 Len=0
112	2.553530	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49159 → boinc-client(1043) [ACK] Seq=581 Ack=2318 Win=2158848 Len=0
113	2.556264	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	608	GET / HTTP/1.1
114	2.556331	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	http(80) → 49156 [ACK] Seq=817 Ack=1554 Win=2159616 Len=0
115	2.558859	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	317	HTTP/1.1 304 Not Modified
116	2.558941	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49156 → http(80) [ACK] Seq=1554 Ack=1090 Win=2160128 Len=0
117	2.608976	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	469	GET /docs/5.0/assets/brand/bootstrap-logo.svg HTTP/1.1
118	2.609026	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	http(80) → 49156 [ACK] Seq=1090 Ack=1979 Win=2159184 Len=0
119	2.609028	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	588	HTTP/1.1 404 Not Found (text/html)
120	2.609923	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49156 → http(80) [ACK] Seq=1979 Ack=1632 Win=2159616 Len=0
121	3.325809	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	45	51588 → 9013 [ACK] Seq=1 Ack=1 Win=8441 Len=1
122	3.325841	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	96	9013 → 51588 [ACK] Seq=1 Ack=2 Win=8439 Len=0 SLE=1 SRE=2

که به علت وجود docker و vm به شکل بالا در آمده است .

در اصل تمامی آدرس ها 127.0.0.1 است.

سوال ۱: آدرس پورت‌های مبدا و مقصد چیست؟ روند برقراری ارتباط در پروتکل HTTP چگونه است؟ وب سرور چگونه آدرس سایت درخواستی شما را تشخیص می‌دهد؟

No.	Time	Source	Destination	Protocol	Length	Info
41	0.102550	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	1004	Application Data
42	0.102610	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49641 → boinc-client(1043) [ACK] Seq=549 Ack=2317 Win=2158848 Len=0
43	0.103643	kubernetes.docker.inte...	kubernetes.docker.inte...	TLSv1..	75	Encrypted Alert
44	0.103683	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49641 [ACK] Seq=2317 Ack=580 Win=2160640 Len=0
45	0.103872	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49641 → boinc-client(1043) [FIN, ACK] Seq=580 Ack=2317 Win=2158848 Len=0
46	0.103900	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 49641 [ACK] Seq=2317 Ack=580 Win=2160640 Len=0
47	0.103935	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49641 → boinc-client(1043) [ACK] Seq=581 Ack=2318 Win=2158848 Len=0
48	0.411401	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	[TCP Retransmission] 49641 → boinc-client(1043) [FIN, ACK] Seq=580 Ack=2318 Win=2158848 Len=0
49	0.411441	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	[TCP ZeroWindow] boinc-client(1043) → 49641 [ACK] Seq=2318 Ack=581 Win=0 Len=0
50	4.430805	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	49652 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
51	4.430912	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	http(80) → 49652 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
52	4.430983	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49652 → http(80) [ACK] Seq=1 Ack=1 Win=2161152 Len=0
53	4.431054	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	49653 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
54	4.431755	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	http(80) → 49653 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
55	4.431820	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49653 → http(80) [ACK] Seq=1 Ack=1 Win=2161152 Len=0
56	4.437336	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	576	GET / HTTP/1.1
57	4.437386	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	http(80) → 49652 [ACK] Seq=1 Ack=533 Win=2160640 Len=0
58	4.440096	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	741	HTTP/1.1 200 OK (text/html)
59	4.440860	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49652 → http(80) [ACK] Seq=533 Ack=698 Win=2160384 Len=0
60	5.225473	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	45	51588 → 9013 [ACK] Seq=1 Ack=1 Win=8441 Len=1
61	5.225502	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	9013 → 51588 [ACK] Seq=1 Ack=2 Win=8439 Len=0 SLE=1 SRE=2
62	5.508010	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	434	GET /favicon.ico HTTP/1.1
63	5.508067	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	http(80) → 49652 [ACK] Seq=698 Ack=923 Win=2160384 Len=0
64	5.501716	kubernetes.docker.inte...	kubernetes.docker.inte...	HTTP	586	HTTP/1.1 404 Not Found (text/html)
65	5.501829	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	49652 → http(80) [ACK] Seq=923 Ack=1240 Win=2159872 Len=0
66	7.553421	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	52	9487 → 52942 [PSH, ACK] Seq=1 Ack=1 Win=8382 Len=0
67	7.553464	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	52942 → 9487 [ACK] Seq=1 Ack=9 Win=8333 Len=0

> Frame 51: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{...} id 0

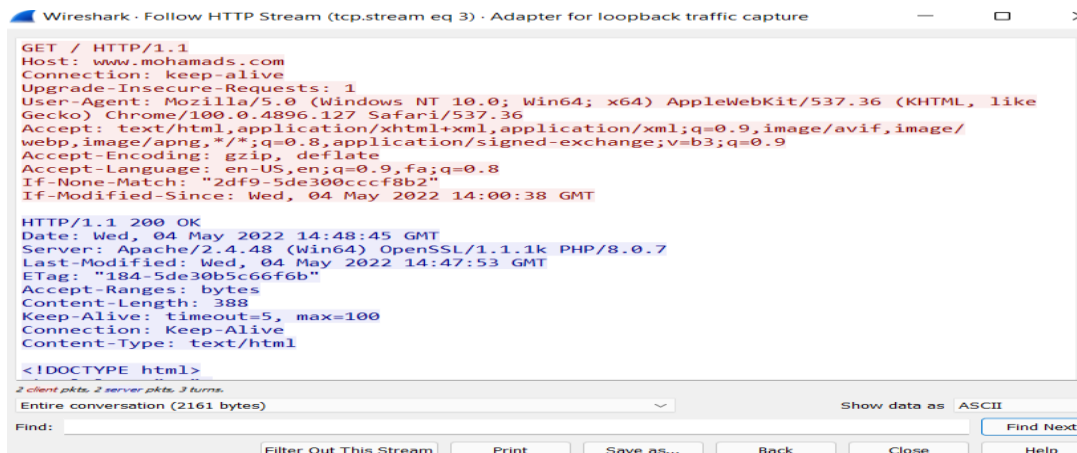
> Null/Loopback

> Internet Protocol Version 4, Src: kubernetes.docker.internal (127.0.0.1), Dst: kubernetes.docker.internal (127.0.0.1)

> Transmission Control Protocol, Src Port: http (80), Dst Port: 49652 (49652), Seq: 0, Ack: 1, Len: 0

آدرس های مبدا و مقصد هر دو 127.0.0.1 است و پورت مبدا نیز ۸۰ است.

آدرس سایت ما www.mohamads.com می باشد.



```
GET / HTTP/1.1
Host: www.mohamads.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fa;q=0.8
If-None-Match: "2df9-5de300ccc8b2"
If-Modified-Since: Wed, 04 May 2022 14:00:38 GMT

HTTP/1.1 200 OK
Date: Wed, 04 May 2022 14:48:45 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
Last-Modified: Wed, 04 May 2022 14:47:53 GMT
ETag: "184-5de30b5c66f6b"
Accept-Ranges: bytes
Content-Length: 388
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

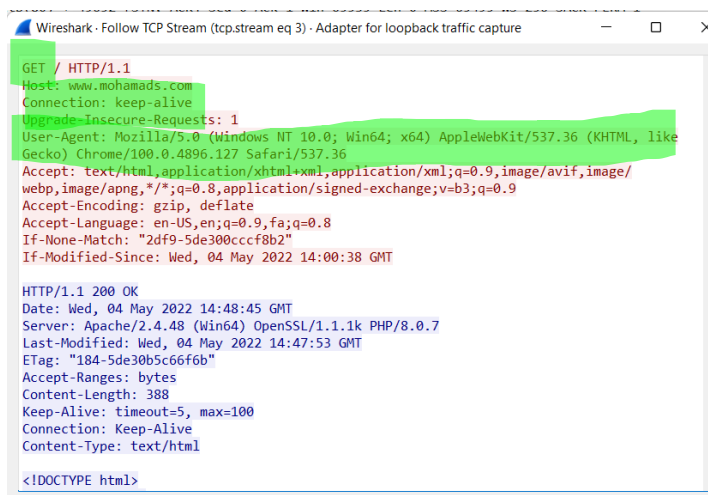
<!DOCTYPE html>
```

در پروتکل HTTP ابتدا کاربر یک ارتباط TCP با یک وب سوکت برقرار میکند. سپس این ارتباط توسط سرور قبول می شود و یا در مواردی رد. پس از آن کاربر درخواست گرفتن یک صفحه که در اینجا همان صفحه اول ما است را میکند و در صورتی که این صفحه وجود داشته باشد توسط سرور برای کاربر ارسال می شود در غیر این صورت خطای ۴۰۴ توسط سرور برگردانده می شود.

حال آدرس IP صفحه ما توسط DNS انجام می شود و از با گرفتن یک کوئری که در آزمایش های پیش روند آن را دیدیم انجام می شود.

۲. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش های مختلف پروتکل HTTP را مشاهده کنید.

سوال ۲: مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟



```
GET / HTTP/1.1
Host: www.mohamads.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,fa;q=0.8
If-None-Match: "2df9-5de300ccc8b2"
If-Modified-Since: Wed, 04 May 2022 14:00:38 GMT

HTTP/1.1 200 OK
Date: Wed, 04 May 2022 14:48:45 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
Last-Modified: Wed, 04 May 2022 14:47:53 GMT
ETag: "184-5de30b5c66f6b"
Accept-Ranges: bytes
Content-Length: 388
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
```

مقدار Connection برابر با keep-alive است که یعنی در خواست مورد نظر را بعد از پاسخ قطع نکند یا نبندد. درخواست ما از نوع GET بوده است و مقدار user-agent هم در تصویر مشخص شده است. که این مقدار بیانگر سیستم عامل مورد استفاده فرد و مرورگر آن و ورژن های آن ها است.

سوال ۳: در پنجره باز شده، اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

```
✓ Flags: 0x40, Don't fragment
0... .... = Reserved bit: Not set
.1... .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
```

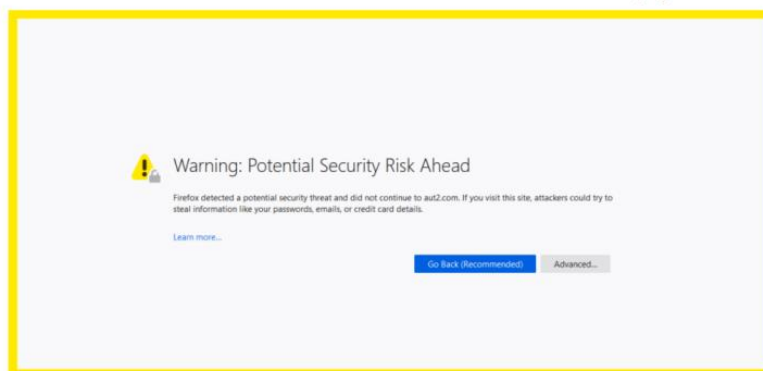
مقادیر flag تنظیم شده .

سوال ۴: یک سایت دیگر با نام دلخواه ایجاد کنید و بسته‌های مربوط به آن را شنود کنید. چه تفاوتی بین این دو سایت وجود دارد؟

علاوه بر آدرس دو سایت و محتوای آن ها پروتکل های دیگری مانند UDP نیز مشاهده می شود.

۳. حال آدرس <https://www.example.com> را در مرورگر خود باز کنید. دقت کنید که به جای test.com آدرس سایت خود را قرار دهید.

۴. سایت را در مرورگر باز کنید. خطای نشان داده شده در شکل (۲-۱) نمایش داده می شود.



شکل (۲-۱) خطای نمایش داده شده

۵. بر روی Advanced کلیک کرده و دکمه View Certificate را فشار دهید.

سوال ۵: مشخص کنید که گواهی را چه کسی برای چه کسی صادر کرده، مدت زمان اعتبار گواهی چقدر است، کلید عمومی صادرکننده چیست و امضای دیجیتال انجام شده با چه الگوریتم‌هایی انجام شده است.

Fingerprints	
SHA-256	69:BF:E2:6B:61:59:6F:0B:85:35:84:88:AA:21:FC:18:EE:B0:9F:5C:9C:D8:2C:1F:47:...
SHA-1	F0:5B:AA:FB:46:71:17:5C:BB:46:C1:FC:4A:47:00:53:DF:E8:92:A2
Basic Constraints	
Certificate Authority	Yes
Subject Key ID	
Key ID	82:C3:20:2B:D8:E5:23:EB:68:27:51:DF:C6:75:57:98:FB:1B:CE:0D
Authority Key ID	
Key ID	82:C3:20:2B:D8:E5:23:EB:68:27:51:DF:C6:75:57:98:FB:1B:CE:0D

Certificate	
Subject Name	
Country	US
Locality	Palo Alto
Organizational Unit	VMware
Common Name	VMware
Email Address	none@vmware.com
Issuer Name	
Country	US
Locality	Palo Alto
Organizational Unit	VMware
Common Name	VMware
Email Address	none@vmware.com
Validity	
Not Before	Tue, 12 Oct 2021 11:33:45 GMT
Not After	Wed, 12 Oct 2022 11:33:45 GMT
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	F5:3F:53:E3:E6:A0:7E:5E:AA:1D:C4:63:52:2E:7D:B6:40:34:E2:1E:A2:BE:77:0B:07:F...
Miscellaneous	
Serial Number	00:AF:68:26:7B:93:83:C4:E7
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

مقادیر خواسته شده در تصاویر خط کشیده شده است .

Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	F5:3F:53:E3:E6:A0:7E:5E:AA:1D:C4:63:52:2E:7D:B6:40:34:E2:1E:A2:BE:77:0B:07:F 9:43:18:51:71:A7:93:2B:23:48:84:39:FD:A6:50:9A:C9:F2:9D:8B:F0:21:FF:B1:98:49: 13:45:C8:C8:2F:AB:70:67:0A:96:F1:AF:53:4D:59:05:D6:D7:86:6F:5B:A2:45:53:0A: BD:C6:19:E1:EE:AC:B2:71:0F:25:27:31:7D:F8:B9:3B:96:A6:C4:77:10:13:6D:F3:50:3 A:17:C0:42:35:F6:D0:D3:AD:0A:41:97:19:8D:08:E5:0E:31:E5:71:8E:39:62:30:DB:B 4:15:84:56:E2:CB:43:5E:7B:89:5E:8B:10:CD:06:8A:1B:C2:9B:35:AD:E5:1B:E9:90:26: 71:3D:41:D5:11:F6:B0:3A:D9:15:4D:65:FC:51:73:EE:59:E1:EE:97:E0:15:63:B0:8B:5 9:53:1E:72:A3:6E:25:5F:F3:E6:1A:0F:A6:C7:CC:81:67:0A:77:F5:5E:9C:D9:71:E2:C 6:75:41:D0:9A:14:11:37:F1:C8:CB:B9:A5:1D:84:24:61:2D:EC:0B:4C:CE:9F:A2:2D:4 B:84:65:26:FA:1E:BE:47:D1:23:FC:AA:94:9B:50:7F:9D:9E:DA:F6:EC:24:0A:20:08:2 B:6D:90:17

مقدار کامل کلید عمومی در تصویر بالا قابل مشاهده است .

۶. حال ارتباط را با وایرشارک شنود کنید. بر روی بسته TLS مربوط به این ارتباط کلیک راست کرده و Follow SSL Stream را انتخاب کنید. صفحه‌ای مطابق شکل (۳-۱) نمایش داده می‌شود.

سوال ۶: آیا می‌توانید متن ارتباط را بخوانید؟ چرا؟



```

Wireshark · Follow TCP Stream (tcp.stream eq 15) · Adapter for loopback traffic capture
.....j.P.....xq.T2v....:Z.O2
...^jj|.c..(5.-I@{..VF^...e>.B.....q....+./,0...../5....JJ.....www.mohamads.com.....
.
..ZZ.....#.....h2.http/1.1.....
.....3.+.)ZZ.....YSM~S....L....5$.~.Y.....k.-....
+.....Di.....h2.....
.....9...5...+Rb.A..v..A.=Y^").59.
g..GI.....i..0..
.....0...0.....h&{...0
.
*.H..
.....0c1.0 ..U....US1.0...U... Palo Alto1.0
..U....VMware1.0
..U....VMware1.0.. *.H..
...none@vmware.com0..
211012113345Z.
221012113345Z0c1.0 ..U....US1.0...U... Palo Alto1.0
..U....VMware1.0
..U....VMware1.0.. *.H..
...none@vmware.com0..0
*.H..
.....0..
.....?S...~^...cR.},@4....w...C.Qq..+H.9..P.....I..I.E../.pg
...SMY....0[.ES
.....q.%'1}...;...w..m.Pr...B5....
A.....1.q.9b0...V..C^{.^.....5.....&q=A.....:Me.Qs.Y.....c..YS.r.n%_.....g
w.^..q..uA...7.....$a-.L...K.e&...G.#....P.....$
..+m.....0..0...U.....+.#..h'Q..uW....
0....U.#...0.....+..#..h'Q..uW....

```

خیر نمی‌توان زیرا داده‌های ارسال شده با این پروتکل رمزنگاری شده‌اند و قابل مشاهده نیستند.

سوال ۷: گواهی آن سایت با گواهی شما چه تفاوت‌هایی دارد؟

Certificate			
www.google.com	GTS CA 1C3	GTS Root R1	GlobalSign Root CA
Subject Name			
Common Name	www.google.com		
Issuer Name			
Country	US		
Organization	Google Trust Services LLC		
Common Name	GTS CA 1C3		
Validity			
Not Before	Mon, 11 Apr 2022 09:43:41 GMT		
Not After	Mon, 04 Jul 2022 09:43:40 GMT		
Subject Alt Names			
DNS Name	www.google.com		
Public Key Info			
Algorithm	Elliptic Curve		
Key Size	256		
Curve	P-256		
Public Value	04:AB:0E:2D:19:04:9A:90:A4:E1:65:66:A2:43:1D:3E:51:2E:DA:8E:91:CD:26:AC:DF:E2...		
Miscellaneous			
Serial Number	50:69:89:19:16:59:07:17:0A:54:D0:54:F5:95:1D:38		
Signature Algorithm	SHA-256 with RSA Encryption		
Version	3		
Download	PEM (cert) PEM (chain)		
Fingerprints			
SHA-256	97:DD:A6:7B:71:09:11:7C:8F:5E:CF:09:75:91:86:2C:3A:87:28:A0:09:7D:06:90:3B...		
SHA-1	85:58:C5:DE:23:81:8D:85:5A:3C:E7:9C:E5:F5:F9:47:53:65:3F:71		
Basic Constraints			

همانطور که میبینیم ۳ نوع گواهی دارد که مواردی مانند صادر کننده آن ها کلید عمومی و تاریخ اعتبار آن با ما متفاوت است.

۱-۳-۲- تنظیمات سرور FTP

۷. ابتدا از طریق XAMPP ماژول FileZilla را استارت کنید. سپس طبق آموزش یک اکانت با رمز عبور دلخواه ایجاد کنید. سپس مسیر دلخواه برای به اشتراک‌گذاری را مشخص کنید.

۸. به آدرس <ftp://127.0.0.1> بروید. ارتباط را با وایرشارک شنود کنید.

سوال ۸: مشخص کنید چه دستوری برای لیست کردن فایل‌های دایرکتوری استفاده شده است. مشخص کنید چه نام کاربری برای دسترسی به سایت استفاده شده است. پروتکل لایه Transport استفاده شده برای این بسته‌ها چیست؟ آدرس پورت مبدا و مقصد ارتباط را مشخص کنید.

از دستور List استفاده شده است .

NO.	Time	Source	Destination	Protocol	Length	Info
53	2.340760	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	52	Response: 200 OK
57	2.340926	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	51	Request: CWD /
61	2.341472	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	91	Response: 250 CWD successful. "/" is current directory.
63	2.341656	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	52	Request: TYPE A
69	2.343183	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	63	Response: 200 Type set to A
75	2.343599	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	50	Request: PASV
79	2.344795	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	90	Response: 227 Entering Passive Mode (127,0,0,1,207,13)
84	2.345238	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	50	Request: LIST
92	2.348073	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	69	Response: 150 Connection accepted
104	2.350098	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP	61	Response: 226 Transfer OK
96	2.348398	kubernetes.docker.inte...	kubernetes.docker.inte...	FTP-D...	6289	FTP Data: 6245 bytes (PASV) (LIST)
1	0.000000	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	53002 → boinc-client(1043) [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
2	0.000106	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	56	boinc-client(1043) → 53002 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
3	0.000177	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	53002 → boinc-client(1043) [ACK] Seq=1 Ack=1 Win=2161152 Len=0
5	0.024757	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 53002 [ACK] Seq=1 Ack=169 Win=2161152 Len=0
7	0.038569	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	53002 → boinc-client(1043) [ACK] Seq=169 Ack=1083 Win=2160128 Len=0
9	0.041050	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 53002 [ACK] Seq=1083 Ack=262 Win=2160896 Len=0
11	0.042544	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	53002 → boinc-client(1043) [ACK] Seq=262 Ack=1357 Win=2159872 Len=0
13	0.043120	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	44	boinc-client(1043) → 53002 [ACK] Seq=1357 Ack=549 Win=2160640 Len=0
14	0.044611	kubernetes.docker.inte...	kubernetes.docker.inte...	TCP	233	afrop(1042) → 51587 [PSH, ACK] Seq=1 Ack=1 Win=8439 Len=189

> Frame 84: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_{...} id 0

> Null/Loopback

> Internet Protocol Version 4, Src: kubernetes.docker.internal (127.0.0.1), Dst: kubernetes.docker.internal (127.0.0.1)

> Transmission Control Protocol, Src Port: 52981 (52981), Dst Port: ftp (21), Seq: 28, Ack: 121, Len: 6

> File Transfer Protocol (FTP)

[Current working directory: /]

[Command response frames: 1]

[Command response bytes: 6245]

[Command response first frame: 96]

[Command response last frame: 96]

[Setup frame: 79]

پورت مبدا و مقصد در شکل مشخص شده است. پروتکل لایه Transport نیز TCP است.

```

Wireshark · Follow TCP Stream (tcp.stream eq 9) · Adapter for loopback traffic capture

220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
USER mohamad
331 Password required for mohamad
PASS 123
230 Logged on
opts utf8 on
200 UTF8 mode enabled
syst
215 UNIX emulated by FileZilla
site help
504 Command not implemented for that parameter
PWD
257 "/" is current directory.

```

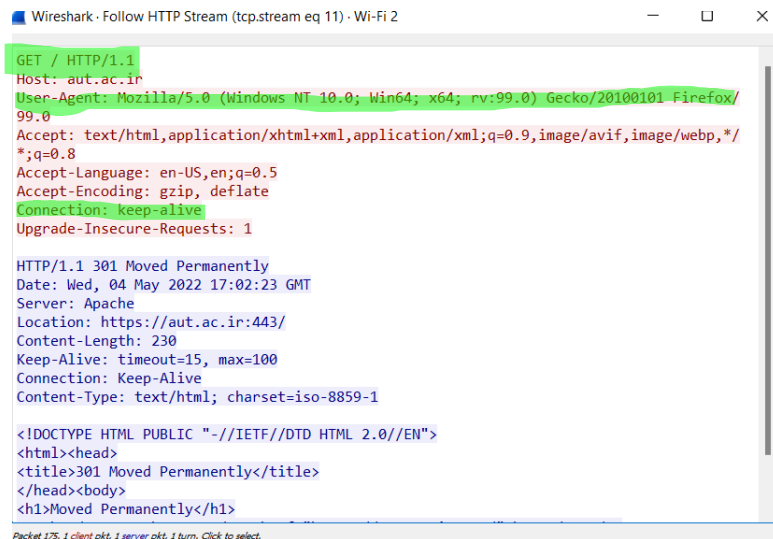
مشخصات هم در شکل بالا دیده می شود.

۱-۳-۳- پروتکل HTTP

۱. عمل شنود را آغاز کنید، مرورگر را باز کرده و به آدرس <http://aut.ac.ir> بروید. شنود را متوقف کرده و بسته‌ها را بررسی کنید:

۲. بر روی یکی از بسته‌های پروتکل HTTP کلیک راست کرده و Follow HTTP Stream را انتخاب کنید. اگر Wireshark شما این گزینه را ندارد آن را به روز کنید.

۳. بر روی اولین بسته در پنجره باز شده کلیک کنید. بخش‌های مختلف پروتکل HTTP را مشاهده کنید. مقدار بخش Connection چیست؟ درخواست HTTP از نوع GET بوده است یا از نوع POST؟ مقدار User Agent چیست؟ به نظر شما این مقدار بیانگر چه چیزی است؟



```
GET / HTTP/1.1
Host: aut.ac.ir
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 301 Moved Permanently
Date: Wed, 04 May 2022 17:02:23 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
```

مقادیر خواسته شده در شکل مشخص شده است .

مقدار Connection برابر با keep-alive است که یعنی در خواست مورد نظر را بعد از پاسخ قطع نکند یا نبندد. درخواست ما از نوع GET بوده است و مقدار user-agent هم در تصویر مشخص شده است . که این مقدار بیانگر سیستم عامل مورد استفاده فرد و مرورگر آن و ورژن های آن ها است.

۴. در پنجره باز شده، بسته‌هایی با پروتکل TCP هم مشخص شده است. اولین بسته را انتخاب کنید. سپس مقدار Flags در پروتکل TCP را مشاهده کنید. چه مقادیری برای این بسته تنظیم شده است؟

```

178 11.543750 aut.ac.ir 192.168.1.35 TCP 54 http(80) → 63836 [ACK] Seq=1 Ack=342 Win=30016 Len=0
179 11.544280 aut.ac.ir 192.168.1.35 HTTP 528 HTTP/1.1 301 Moved Permanently (text/html)
184 11.589378 192.168.1.35 aut.ac.ir TCP 54 63836 → http(80) [ACK] Seq=342 Ack=475 Win=64006 Len=0
8390 21.558785 192.168.1.35 aut.ac.ir TCP 55 [TCP Keep-Alive] 63836 → http(80) [ACK] Seq=341 Ack=475 Win=64006 Len=1
8487 21.635795 aut.ac.ir 192.168.1.35 TCP 66 [TCP Keep-Alive ACK] http(80) → 63836 [ACK] Seq=475 Ack=342 Win=30016 Len=0 SLE=341 SRE=342

```

```

Acknowledgment number (raw): 3866864833
0101 .... = Header Length: 20 bytes (5)
▼ Flags: 0x010 (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
.... .....0.. = Fin: Not set
[TCP Flags: .....A....]
Window: 30016
0000 94 00 53 59 ca e5 78 54 2e d9 6d 24 00 00 45 00  --SY--xt--ms--E--

```

```

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..]

```

برای بسته اول flag SYN تنظیم شده بود اما برای بقیه بسته ها flag ACK تنظیم شده بوده است که flag Syn به معنای شروع یک ارتباط TCP است. و flag ACK نیز برای ارسال اطلاعات است. که به معنای دریافت موفق یک بسته است.