



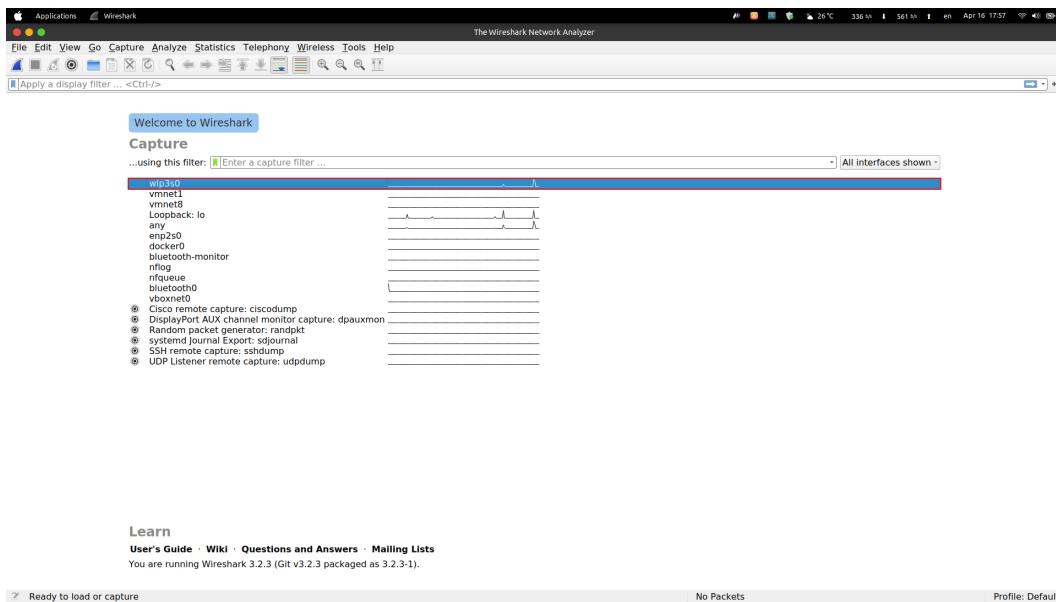
## گزارش آزمایش چهارم

مریم سعیدمهر  
شماره دانشجویی : ۹۶۲۹۳۷۳

### فهرست مطالب

۱	آزمایش ۱-۱-۱ : گرفتن بسته‌های پیام	۱
۱.۱	سوال اول	۱
۲.۱	سوال دوم	۱
۳.۱	سوال سوم	۱
۲	آزمایش ۱-۱-۲ : پروتکل HTTP	۲
۱.۲	سوال اول	۲
۲.۲	سوال دوم	۲
۳.۲	سوال سوم	۲
۴.۲	سوال چهارم	۲
۵.۲	سوال پنجم	۲
۶.۲	سوال ششم	۲
۳	آزمایش ۳-۱ : ردیابی DNS توسط wireshark	۳
۱.۳	سوال اول	۳
۲.۳	سوال دوم	۳
۳.۳	سوال سوم	۳
۴.۳	سوال چهارم	۳
۵.۳	سوال پنجم	۳
۶.۳	سوال ششم	۳
۷.۳	سوال هفتم	۳
۴	آزمایش ۱-۱-۳ : ردیابی بسته‌های ICMP	۴
۵	فایل‌های pcapng خروجی وایرشارک	۵
۱۶		

## ۱ آزمایش ۱-۱-۱ : گرفتن بسته های پیام



شکل ۱: انتخاب کارت شبکه مناسب (wlp3s0)

```
TX packets 16596 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.215.1 netmask 255.255.255.0 broadcast 192.168.215.255
inet6 fe80::250:56ff:fe08:8 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:c0:00:08 txqueuelen 1000 (Ethernet)
RX packets 1004 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16644 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.7 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::c126:e295:4a06:e3a4 prefixlen 64 scopeid 0x20<link>
ether 34:41:5d:91:af:3c txqueuelen 1000 (Ethernet)
RX packets 9500797 bytes 11193180367 (11.1 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 7358900 bytes 2005042104 (2.0 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

شکل ۲: خروجی دستور ifconfig و اطمینان از درستی کارت شبکه انتخاب شده در وایرشارک

## ۱.۱ سوال اول

- ARP
- TCP
- UDP
- TLSv1.2
- DNS
- HTTP
- TLSv1.3
- SSLv2

## ۲.۱ سوال دوم

No.	Time	Source	Destination	Protocol	Length	Info
775	26.683717847	192.168.1.7	176.101.52.155	HTTP	502	GET / HTTP/1.1
793	26.683717847	176.101.52.155	192.168.1.7	HTTP	410	HTTP/1.1 410 Moved Permanently (text/html)

> Frame 783: 446 bytes on wire (352 bits), 446 bytes captured (352 bits) on interface wlp3s0, id 0
Ethernet II, Src: ASUSTek-C8_8a:d4 (00:0c:41:5d:91:af), Dst: IntelCor_91:af:3c (34:41:5d:91:af:3c)
Internet Protocol Version 4, Src: 176.101.52.155, Dst: 192.168.1.7
Transmission Control Protocol, Src Port: 80, Dst Port: 52844, Seq: 1, Ack: 449, Len: 362
HyperText Transfer Protocol
HTTP/1.1 410 Moved Permanently
Server: nginx/1.18.0v/n
Date: Fri, 16 Apr 2021 15:15:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 169
Connection: keep-alive
Location: https://iut.ac.ir/yr
Vary: Accept-Encoding
[HTTP response 1/1]
[Time since request: 0.073843905 seconds]
[Request Headers]
[Request URI: http://iut.ac.ir/]
File Data: 169 bytes
Line-based text data: text/html (7 lines)

شکل ۳: فاصله زمانی برابر با ۰.۰۷۳۸۴۳۹۰ HTTP Response تا HTTP GET (26.757561752 – 26.683717847 = ۰.۰۷۳۸۴۳۹۰ seconds = 73.8439 ms)

## ۳.۱ سوال سوم

بعد از وارد کردن iut.ac.ir در browse و زدن دکمه جستجو ، ابتدا یک درخواست dns server به dns server محلی شبکه من ارسال میشود تا آدرس IP به iut.ac.ir بترجمه شود.

No.	Time	* Source	Destination	Protocol	Length	Info
118	0.065344972	192.168.1.1	192.168.1.1	DNS	96	Standard query response 0x12b7 A adservice.google.com A 172.217.109.226
141	0.243884538	192.168.1.1	192.168.1.1	DNS	79	Standard query 0x007e A client.google.com
159	0.243884538	192.168.1.1	192.168.1.1	DNS	111	Standard query response 0x007e A client.google.com CNAME clients.l.google.com A 172.217.109.238
257	0.887532083	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x1ef7 A fonts.gstatic.com
258	0.888623879	192.168.1.1	192.168.1.1	DNS	132	Standard query response 0x1ef7 A fonts.gstatic.com CNAME gstaticadsssl1.google.com A 216.58.209.131
329	0.888623879	192.168.1.1	192.168.1.1	DNS	96	Standard query 0x1ef7 A fonts.gstatic.com
329	0.124972492	192.168.1.1	192.168.1.1	DNS	102	Standard query response 0xbff0 A encrypted-thin.gstatic.com A 172.217.10.142
340	0.388188848	192.168.1.1	192.168.1.1	DNS	85	Standard query 0xbcc0 A mobile-gtalk.l.google.com
342	0.425154939	192.168.1.1	192.168.1.1	DNS	101	Standard query response 0xbcc0 A mobile-gtalk.l.google.com A 108.177.15.188
367	0.388188848	192.168.1.1	192.168.1.1	DNS	83	Standard query 0xbcc0 A mobile-gtalk.l.google.com
368	0.735785646	192.168.1.1	192.168.1.1	DNS	97	Standard query response 0xb1ab A update.googleapis.com A 172.217.18.191
445	0.918492024	192.168.1.1	192.168.1.1	DNS	77	Standard query 0x1c21 A www.l.google.com
449	0.918492024	192.168.1.1	192.168.1.1	DNS	93	Standard query response 0x1c21 A www.l.google.com A 172.217.109.238
506	0.751578155	192.168.1.1	192.168.1.1	DNS	75	Standard query 0xd065 A www.gstatic.com
507	0.751720287	192.168.1.1	192.168.1.1	DNS	75	Standard query 0x6ceb A ssl.gstatic.com
508	0.918492024	192.168.1.1	192.168.1.1	DNS	77	Standard query 0xc44 A plus.l.google.com
512	0.708937775	192.168.1.1	192.168.1.1	DNS	91	Standard query response 0x1c00 A www.gstatic.com A 172.217.109.227
514	0.79897176	192.168.1.1	192.168.1.1	DNS	91	Standard query response 0x1ceb A ssl.gstatic.com A 172.217.18.131
515	0.791209234	192.168.1.1	192.168.1.1	DNS	93	Standard query response 0xc44 A plus.l.google.com A 216.58.209.142
523	0.918492024	192.168.1.1	192.168.1.1	DNS	79	Standard query response 0x1c00 A www.gstatic.com
534	0.905488595	192.168.1.1	192.168.1.1	DNS	93	Standard query response 0x1e7e A play.google.com A 172.217.18.142
751	0.633904526	192.168.1.1	192.168.1.1	DNS	69	Standard query 0xf728 A iut.ac.ir
761	0.708937775	192.168.1.1	192.168.1.1	DNS	89	Standard query response 0x1c00 A www.iut.ac.ir A 176.101.52.155
779	0.701637799	192.168.1.1	192.168.1.1	DNS	75	Standard query response 0x13ff A sbl.google.com
781	0.7408336548	192.168.1.1	192.168.1.1	DNS	91	Standard query response 0x13ff A sbl.google.com A 216.58.209.142
1616	0.8151664951	192.168.1.1	192.168.1.1	DNS	79	Standard query response 0x1cf7 A materials.iut.ac.ir
1783	0.828032963	192.168.1.1	192.168.1.1	DNS	93	Standard query response 0x7e70 A materials.iut.ac.ir A 176.101.52.155

> Frame 781: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface wlp3s0, id 0
Ethernet II, Src: IntelCor_91:af:3c (34:41:5d:91:af:3c), Dst: ASUSTek-C8_8a:d4 (00:0c:41:5d:91:af:3d)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 39543, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xf728
Question: 1
Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
iut.ac.ir: type A, class IN
[Response In: 706]

شکل ۴: اولین درخواست خروجی از سیستم از کلاینت مربوط به پروتکل dns است.

همان طور که از تصویر ۴ پیداست ، این درخواست به آدرس 192.168.1.1 رفته است. که همان dns server محلی شبکه من هست.

```

Link 3 (wlp3s0)
  Current Scopes: DNS
  DefaultRoute setting: yes
    LLMNR setting: yes
  MulticastDNS setting: no
    DNSOverTLS setting: no
      DNSSEC setting: no
      DNSSEC supported: no
  Current DNS Server: 192.168.1.1
  DNS Servers: 192.168.1.1
  DNS Domain: ~.

Link 2 (enp2s0)
  Current Scopes: none
  DefaultRoute setting: no
    LLMNR setting: yes
  MulticastDNS setting: no
    DNSOverTLS setting: no
      DNSSEC setting: no
      DNSSEC supported: no

```

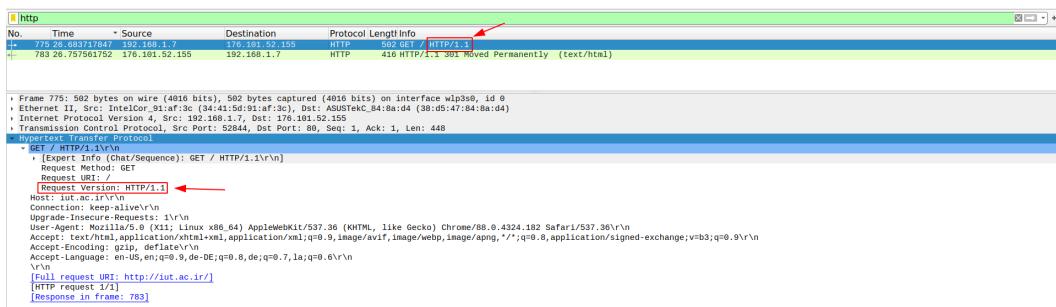
🕒 26s ⏳ 21:34:30

شکل ۵: خروجی دستور `systemd-resolve -status` در لینوکس

## ۲ آزمایش 1-1-2 : پروتکل HTTP

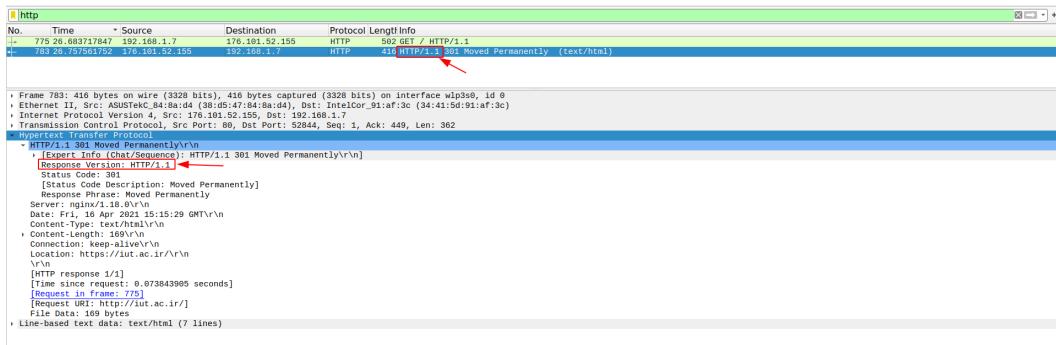
### ۱.۲ سوال اول

- نسخه پشتیبانی شده در مرورگر :



شکل ۶: نسخه پشتیبانی شده HTTP در مرورگر

- نسخه پشتیبانی شده در سرور :



شکل ۷: نسخه پشتیبانی شده HTTP در سرور

#### ۰ تفاوت ۱.۰ با HTTP ۱.۱ :

به عنوان کاربر اینترنت، باید از HTTP استفاده کرده باشید. این یکی از متدائل ترین نامه ها به ویژه برای میلیون ها صفحه است که در حال حاضر بصورت آنلاین اداره می شوند. در اینجا موضوع مورد بحث است. ظاهراً اگر چیزی راجع به HTTP می دانید، دو نسخه ۱.۰ و ۱.۱ وجود دارد. منظور از این دو نسخه چیست؟ در زیر یک مرحله به مرحله مرور HTTP ۱.۰ و HTTP ۱.۱ آورده شده است.

اصطلاح HTTP به پروتکل انتقال متن Hyper اشاره دارد. این به عنوان پروتکل مشتری و سرور عمل می کند که نحوه انتقال پیام ها در قالب شبکه جهانی را مشخص می کند. HTTP ۱.۰ در اوایل سال ۱۹۹۶ هنگامی که شروع شرکت هایی که به صورت آنلاین برای تجارت حرکت می کردند، معرفی شد. محبوبیت استفاده از HTTP

با بیش از ۷۵ درصد ترافیک در اینترنت که فقط به آن متکی است افزایش یافته است.

HTTP ۱.۰ فقط می تواند تا ۱۶ کد وضعیت را تعریف کند که یک شماره رزرو شده بود. محدودیت اصلی استفاده از ۱۶ کد وضعیت این بود که گزارشگری با وضوح ضعیف وجود داشت که مورد توجه قارگرفت و بنابراین نیاز به تهیه ۱.۱ Http وجود دارد. ۱.۱ با ۲۴ کد وضعیت همراه بود که قادر به حل محدودیت های قبلی که ۱.۱ Http با آن روپرتو بود، بود. گزارش خطاب سریعتر انجام شد و تشخیص آسان خطاهای هنگام بروز رخ داد.

یکی دیگر از مواردی که با استفاده از ۱.۱ Http به وجود آمد هدر هشدار دهنده ای بود که قابلیت انجام چندین هشدار وضعیت ثانویه را داشت. هدف اصلی از نشانه های وضعیت ثانویه در ۱.۱ Http توجه به دریافت کننده یک مشکل در هنگام درخواست موفقیت آمیز بود. درخواستهای هشدار دهنده که در ۱.۱ Http مطرح شده اند می توانند به دو طبقه تقسیم شوند. کلاسها بر اساس رقم اول بود که روی کد سه رقمی ارائه شد. در یک کلاس، هشدار پس از تأیید موفقیت آمیز که در حافظه پنهان حذف شد. کلاس دوم یکی بود که حفظ شد و همراه با ورود مجدد آن به حافظه پنهان است.

استفاده از HTTP ۱.۰ فقط با اجازه ای برای تأیید هویت اساسی همراه است، با این کار با چالش نام های کاربری و کلمه های عبوری که از آنها رمزگذاری نشده استفاده می شود. این همانطور که به درستی فرض می کنید، عامل خطر جریمه شدن را به وجود می آورد. HTTP ۱.۰ همچنین وابستگی ندارد و بنابراین اطلاعات جمع آوری شده توسط فعالیت جنبالی می تواند بعدا در آینده مورد استفاده قرار گیرد. ورود ۱.۱ Http این مسئله را اصلاح کرد و استفاده از تأیید هویت Digest Access را ارائه داد. این قابلیت تأیید هویت اساسی است و برای سرورهای برتر امکان استفاده از یک مقدار onetime را فراهم می آورد که در واقع دستیابی چرت زدن دشوار است. چک رمز عبور، نام کاربری و یک بار مقدار ساخته شده است و همه اینها رمزگذاری شده اند. بنابراین می توانید اطمینان داشته باشید که هنگام استفاده از ۱.۱ Http هیچ گونه جریمه ای امکان پذیر نیست.

طراحی HTTP ۱.۰ برای هر درخواستی که از طریق آن انجام شود، نیاز به اتصال TCP جدید دارد. این امر باعث ایجاد چالش شد زیرا هزینه و زمان برقراری اتصال TCP جدید با هر درخواست وجود دارد، و اتصال بسیار کند می شود. برای مقابله با این ۱.۱ Http با استفاده از اتصالات مدام و همچنین استفاده از درخواست های خط لوله برای کار بر روی اتصالات پایدار آمده است.

**خلاصه :**

HTTP به معنی پروتکل انتقال متن Hyper است. HTTP ۱.۱ به طور کلی ارتقاء محدودیت های HTTP ۱.۰ است. HTTP ۱.۰ می تواند کدهای ۱۶status را تعریف کند. HTTP ۱.۰ می تواند ۲۴ کد وضعیت را تعریف کند.

- 1.1 Http دارای یک هشدار است که قادر به تولید هشدارهای وضعیت ثانویه است
- 1.0 Http احراز هویت نامن است زیرا رمزگذاری نشده است
- 1.1 Http امن است زیرا از چک لیست نام کاربری ، رمزعبور و مقدار یکبار استفاده می کند.

۲۰۲ سوال دوم

```
[http]
No. Time * Source Destination Protocol Length Info
1+ 773.24.75.71.7 176.161.52.155 HTTP/1.1 502 Bad Gateway / HTTP/1.1
4+ 783.22.75.75.752 176.161.52.155 HTTP/1.1 301 Moved Permanently (text/html)

[+] Frame 1: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface wlp3s0, id 0
[Ethernet II Src: IntelPro_91af:3c (38:11:91:af:3c:00) Dst: CiscoTekC_84:8a:1d (38:05:47:84:8a:1d)
[Transmission Control Protocol, Src Port: 80, Dst Port: 80, Seq: 1, Ack: 1, Len: 448
[HyperText Transfer Protocol
- [GET /index.html]
  [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
  Request-Method: GET
  Request-URI: /
  Request-Version: HTTP/1.1
  Host: iut.ac.ir\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8, application/xsigned-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,de-DE;q=0.8,de;q=0.7,la;q=0.6\r\n
  \r\n
  [Full request URI: http://iut.ac.ir/]
  [HTTP request line]
  [Response in Frame: 783]
```

شکل ۸: زبان های مورد قبول مورگر : en-US,en;q=0.9,de-DE;q=0.8,de;q=0.7,la;q=0.6

٣٠٢ سوال سوم

اگر به درخواست HTTP GET دقت کنیم، این همان درخواستی است که از سمت مرورگر من به مقصد ارسال شده است. پس به این ترتیب، آدرس IP همان Source کامپیوتر من است و آدرس IP همان Destination سرور مقصود است.

No.	Time	Source	Destination	Protocol	Length	Info
775	26.683717847	192.168.1.7	176.101.52.155	HTTP	502	GET / HTTP/1.1
793	26.752561752	176.101.52.155	192.168.1.7	HTTP	416	HTTP/1.1 301 Moved Permanently (text/html)

شکا ۹: آدرس IP کامپوتو من عیارت است از ۱۹۲.۱۶۸.۱.۷

No.	Time	Source	Destination	Protocol	Length	Info
775	26.683717847	192.168.1.7	176.161.52.155	HTTP	502	GET / HTTP/1.1
783	26.757561752	176.161.52.155	192.168.1.7	HTTP	416	HTTP/1.1 301 Moved Permanently (text/html)

شکل ۱۰: آدرس IP سرور مقصد عیارت است از ۱۵۵.۱۵۲.۵۲.۱۰۱.۱۷۶

همچنین محضر احتیاط مستوانیم IP خودمان را با دستور ifconfig چک کنیم:

```

TX packets 339 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.215.1 netmask 255.255.255.0 broadcast 192.168.215.255
inet6 fe80::250:56ff:fe00:8 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:c0:00:08 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 341 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.7 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::c126:e295:4a06:e3a4 prefixlen 64 scopeid 0x20<link>
ether 34:41:5d:91:af:3c txqueuelen 1000 (Ethernet)
RX packets 169085 bytes 214698951 (214.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 116927 bytes 15709670 (15.7 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

🕒 22:33:45

شکل ۱۱: آدرس IP کامپیوتر من 192.168.1.7 میباشد.

## ۴.۲ سوال چهارم

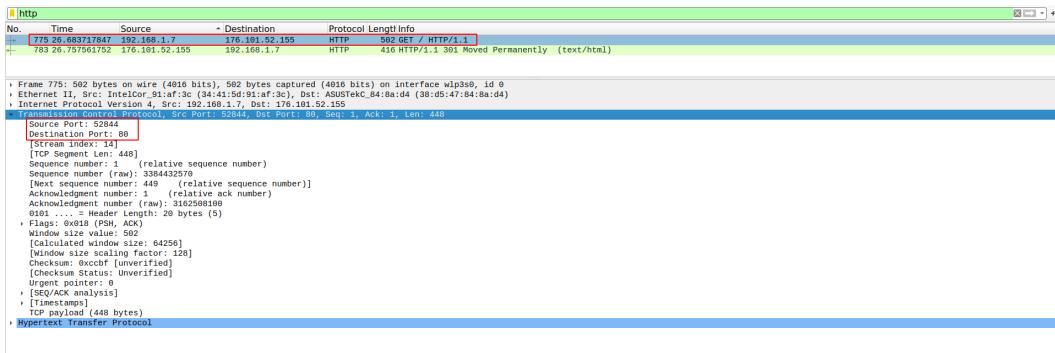
پروتکل استفاده شده در لایه انتقال TCP است.

No.	Time	Source	Destination	Protocol	Length	Info
783	20.12.2016 17:52:00	192.168.1.7	192.168.1.7	HTTP	416	HTTP /1.1 301 Moved Permanently (text/html)
775	26.08.2016 17:52:00	192.168.1.7	192.168.1.7	HTTP	502	GET / HTTP/1.1

Frame 783: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface wlp3s0, id 0
 Ethernet II, Src: Intel(R) Dual Band Wireless-AC (00:50:56:c0:00:08), Dst: Intel(R) Dual Band Wireless-AC (34:41:5d:91:af:3c)
 Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.7
 0100 ... = Version: 4
 ... = Header length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 402
 Identification: 55898
 Flags: 0x0000, Don't fragment
 Fragment offset: 0
 Time to live: 68
 [Protocol: **HTTP**]
 Header checksum: 0xbcb0 [validation disabled]
 [Header checksum status: Unverified]
 Source port: 52844
 Destination port: 80
 Destination: 192.168.1.7
 [Transmission Control Protocol]
 Src Port: 80, Dst Port: 52844, Seq: 1, Ack: 449, Len: 362
 Source Port: 52844
 Destination Port: 80
 [Stream index: 14]
 [TCP Segment Len: 362]
 Sequence number (raw): 3162588108
 [Next sequence number: 363 (relative sequence number)]
 Acknowledgment number (raw): 3384433818
 Acknowledgment number (raw): 3384433818
 0101 .... = Header Length: 20 bytes (5)
 Flags: 0x18 (PSH, ACK)
 Window size scaling factor: 256
 Checksum: 0x0000 [Unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 [Urgent pointer analysis]
 [Timestamp]
 TCP payload (362 bytes)
 Hypertext Transfer Protocol
 Line-based text data: text/html (7 lines)

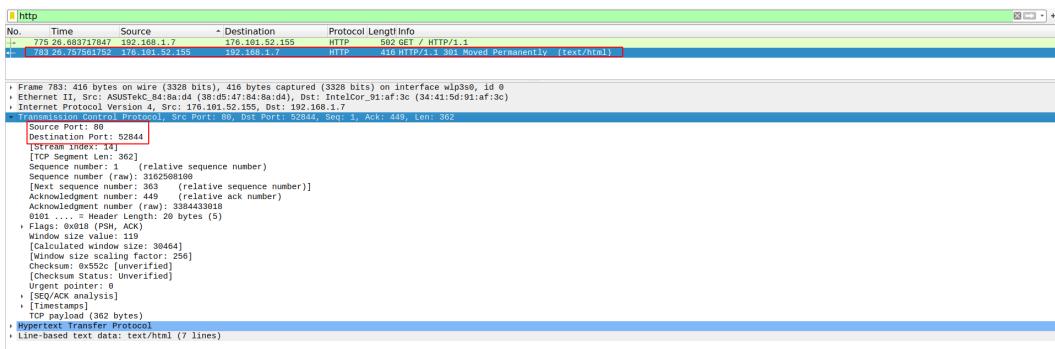
## ۵.۲ سوال پنجم

• HTTP GET •



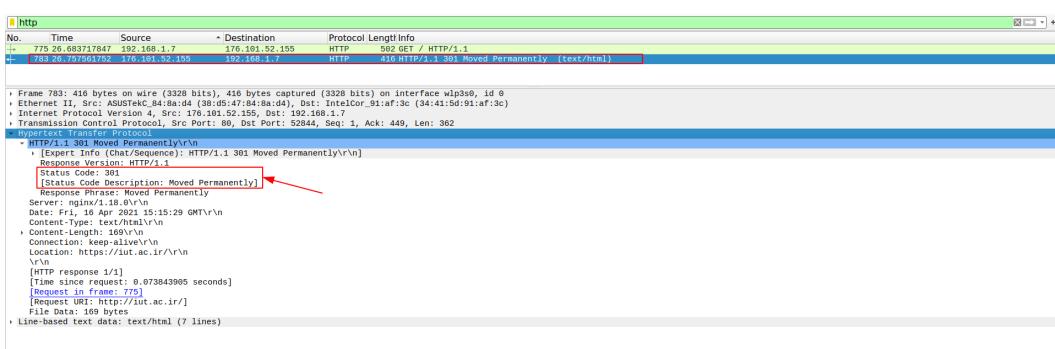
شکل ۱۲: شماره پورت مبدأ 52844 و شماره پورت مقصد 80

• HTTP Response •



شکل ۱۳: شماره پورت مبدأ 80 و شماره پورت مقصد 52844

## ۶.۲ سوال ششم



شکل ۱۴: 301 Moved Permanently status code با یاری 301 بوده و به معنای Moved Permanently است.

## ۳ آزمایش 1-3 : ردیابی DNS توسط wireshark

### ۱.۳ سوال اول

• آدرس فرستنده 192.168.1.7 : DNS query •

No.	Time	Source	Destination	Protocol	Length	Info
1616 28.151664951	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x7e7d A materials.iut.ac.ir	
779 26.791653799	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x13ff A sb.1.google.com	
779 26.833984926	192.168.1.7	192.168.1.1	DNS	65	Standard query 0x13ff A iut.ac.ir	
522 28.127252296	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xecc7e A www.gstatic.com	
568 8.752133249	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xcc44 A plus.l.google.com	
507 8.751729887	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A www.gstatic.com	
506 8.761878136	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A www.gstatic.com	
445 9.961946063	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A www.gstatic.com	
367 5.697226768	192.168.1.7	192.168.1.1	DNS	81	Standard query 0x9lab A update.googleapis.com	
349 5.398188840	192.168.1.7	192.168.1.1	DNS	85	Standard query 0x6c30 A mobile-gtalk.1.google.com	
325 5.329834757	192.168.1.7	192.168.1.1	DNS	89	Standard query 0xdxf1 A clientservices.googleapis.com	
1783 28.320822963	192.168.1.1	192.168.1.7	DNS	95	Standard query response 0x7e7d A materials.iut.ac.ir A 176.101.52.155	
768 28.442983166	192.168.1.1	192.168.1.7	DNS	89	Standard query response 0x6ceb A iut.ac.ir A 176.101.52.155	
534 9.065488953	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0xece7e A play.google.com A 172.217.18.142	
534 9.065488953	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x6ceb A play.google.com A 172.217.18.142	
514 8.798767776	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0x6ceb A ssl.gstatic.com A 172.217.18.131	
512 8.788667775	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0xd6e5 A www.gstatic.com A 172.217.169.227	
446 7.099321233	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x1c21 A www.l.google.com A 172.217.169.238	
369 8.925154985	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x1c21 A www.l.google.com A 172.217.169.131	
342 5.429515498	192.168.1.1	192.168.1.7	DNS	101	Standard query response 0xb38 A mobile-gtalk.1.google.com A 188.177.15.188	
326 5.124972492	192.168.1.1	192.168.1.7	DNS	102	Standard query response 0xf5f9 A encrypted-tbm.gstatic.com A 172.217.18.142	
258 5.329834757	192.168.1.1	192.168.1.7	DNS	121	Standard query response 0x13ff A www.gstatic.com A 216.58.289.142	
153 8.438298989	192.168.1.1	192.168.1.7	DNS	119	Standard query response 0xdxf1 A clients4.google.com CNNAME clients.1.google.com A 172.217.108.288	
119 8.065488953	192.168.1.1	192.168.1.7	DNS	119	Standard query response 0xd6e5 A www.accounts.google.com A 172.217.140.266	

شکل ۱۵: آدرس فرستنده 192.168.1.7

• آدرس(ها)ی پاسخ : iut.ac.ir: type A, class IN, addr 176.101.52.155

No.	Time	Source	Destination	Protocol	Length	Info
1616 28.151664951	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x7e7d A materials.iut.ac.ir	
779 26.791653799	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x13ff A sb.1.google.com	
779 26.833984926	192.168.1.7	192.168.1.1	DNS	65	Standard query 0x13ff A iut.ac.ir	
522 28.127252296	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xecc7e A www.gstatic.com	
568 8.752133249	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xcc44 A plus.l.google.com	
507 8.751729887	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A www.gstatic.com	
506 8.761878136	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A www.gstatic.com	
445 9.961946063	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A www.gstatic.com	
367 5.697226768	192.168.1.7	192.168.1.1	DNS	81	Standard query 0x9lab A update.googleapis.com	
349 5.398188840	192.168.1.7	192.168.1.1	DNS	85	Standard query 0x6c30 A mobile-gtalk.1.google.com	
325 5.329834757	192.168.1.7	192.168.1.1	DNS	89	Standard query 0xdxf1 A clientservices.googleapis.com	
1783 28.320822963	192.168.1.1	192.168.1.7	DNS	95	Standard query response 0x7e7d A materials.iut.ac.ir A 176.101.52.155	
768 28.442983166	192.168.1.1	192.168.1.7	DNS	89	Standard query response 0x6ceb A iut.ac.ir A 176.101.52.155	
534 9.065488953	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0xece7e A play.google.com A 172.217.18.142	
534 9.065488953	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x6ceb A play.google.com A 172.217.18.142	
514 8.798767776	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0x6ceb A ssl.gstatic.com A 172.217.18.131	
512 8.788667775	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0xd6e5 A www.gstatic.com A 172.217.169.227	
446 7.099321233	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x1c21 A www.l.google.com A 172.217.169.238	
369 8.925154985	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x1c21 A www.l.google.com A 172.217.169.131	
342 5.429515498	192.168.1.1	192.168.1.7	DNS	101	Standard query response 0xb38 A mobile-gtalk.1.google.com A 188.177.15.188	
326 5.124972492	192.168.1.1	192.168.1.7	DNS	102	Standard query response 0xf5f9 A encrypted-tbm.gstatic.com A 172.217.18.142	
258 5.329834757	192.168.1.1	192.168.1.7	DNS	121	Standard query response 0x13ff A www.gstatic.com A 216.58.289.142	
153 8.438298989	192.168.1.1	192.168.1.7	DNS	119	Standard query response 0xdxf1 A clients4.google.com CNNAME clients.1.google.com A 172.217.108.288	
119 8.065488953	192.168.1.1	192.168.1.7	DNS	119	Standard query response 0xd6e5 A www.accounts.google.com A 172.217.140.266	

شکل ۱۶: آدرس(ها)ی پاسخ : iut.ac.ir: type A, class IN, addr 176.101.52.155

No.	Time	Source	Destination	Protocol	Length	Info
1610 28.1516649951	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x7e7d A materials.iut.ac.ir	
779 26.781663799	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A sbl.google.com	
780 26.781663799	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A sbl.google.com	
781 26.781663799	192.168.1.7	192.168.1.1	DNS	69	Standard query 0xf120 A iut.ac.ir	
522 0.965221210	192.168.1.7	192.168.1.1	DNS	75	Standard query 0xece7e A play.google.com	
508 0.752133249	192.168.1.7	192.168.1.1	DNS	75	Standard query 0xc44 A plus.l.google.com	
507 0.751720287	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A ssl.gstatic.com	
508 0.751578135	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ed5 A www.gstatic.com	
445 1.091840263	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x121 A www.gstatic.com	
367 5.697226769	192.168.1.7	192.168.1.1	DNS	81	Standard query 0x13ab A update.googleapis.com	
349 0.381388649	192.168.1.7	192.168.1.1	DNS	85	Standard query 0xbce30 A mobile-gtalk.l.google.com	
325 9.123532683	192.168.1.7	192.168.1.1	DNS	80	Standard query 0x13ff A www.gstatic.com	
297 0.87532683	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x13ff7 A fonts.gstatic.com	
141 3.243864838	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xcd7e A clients4.google.com	

شکل ۱۷: از پروتکل UDP استفاده میکند (در DNS query)

No.	Time	Source	Destination	Protocol	Length	Info
141 3.243864838	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xcede A clients4.google.com	
113 0.965442899	192.168.1.7	192.168.1.1	DNS	80	Standard query 0x13ff A adservice.google.com	
168 2.925246429	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xb654 A www.google.com	
82 0.579386562	192.168.1.7	192.168.1.1	DNS	94	Standard query 0x5ec2 A oauthaccountmanager.googleapis.com	
45 2.177252296	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x1489 A accounts.google.com	
14 2.177252296	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x1489 A accounts.google.com	
3 3.329834757	192.168.1.7	192.168.1.1	DNS	89	Standard query 0xd2f1 A clientservices.googleapis.com	
1783 28.320922863	192.168.1.1	192.168.1.7	DNS	95	Standard query response 0x7fd A materials.iut.ac.ir A 176.101.52.155	
759 26.781663799	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x13ff A materials.iut.ac.ir A 176.101.52.145	
760 26.781663799	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x13ff A materials.iut.ac.ir A 176.101.52.145	
534 0.86548856	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0xece7e A play.google.com A 172.217.18.142	
516 0.86548856	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0xc44 A plus.l.google.com A 216.58.299.142	
514 0.780707111	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0x6ceb A ssl.gstatic.com A 172.217.18.142	

شکل ۱۸: از پروتکل UDP استفاده میکند (در DNS response)

## ۲.۳ سوال دوم

No.	Time	Source	Destination	Protocol	Length	Info
1610 28.1516649951	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x7e7d A materials.iut.ac.ir	
779 26.781663799	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A sbl.google.com	
780 26.781663799	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A sbl.google.com	
781 26.781663799	192.168.1.7	192.168.1.1	DNS	69	Standard query 0xf120 A iut.ac.ir	
522 0.965221210	192.168.1.7	192.168.1.1	DNS	75	Standard query 0xece7e A play.google.com	
508 0.752133249	192.168.1.7	192.168.1.1	DNS	75	Standard query 0xc44 A plus.l.google.com	
507 0.751720287	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A ssl.gstatic.com	
508 0.751578135	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ed5 A www.gstatic.com	
445 1.091840263	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x121 A www.gstatic.com	
367 5.697226769	192.168.1.7	192.168.1.1	DNS	81	Standard query 0x13ab A update.googleapis.com	
349 0.381388649	192.168.1.7	192.168.1.1	DNS	85	Standard query 0xbce30 A mobile-gtalk.l.google.com	
325 9.123532683	192.168.1.7	192.168.1.1	DNS	80	Standard query 0x13ff A www.gstatic.com	
297 0.87532683	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x13ff7 A fonts.gstatic.com	
141 3.243864838	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xcd7e A clients4.google.com	

شکل ۱۹: پورت مقصد پیام 53 است

No.	Time	Source	Destination	Protocol	Length	Info
144	14:33:00.86409	192.168.1.7	192.168.1.1	DNS	70	Standard query @0x7e7 A clients4.google.com
137	5.064429589	192.168.1.7	192.168.1.1	DNS	80	Standard query @0x12D7 A adservice.google.com
108	2.925246420	192.168.1.7	192.168.1.1	DNS	74	Standard query @0x854 A www.google.com
82	2.157232602	192.168.1.7	192.168.1.1	DNS	94	Standard query @0x809 A authmanagement.googleapis.com
49	1.157232602	192.168.1.7	192.168.1.1	DNS	70	Standard query @0x1489 A accounts.google.com
15	1.856962867	192.168.1.7	192.168.1.1	DNS	78	Standard query @0x8C2 A www.googleapis.com
3	1.329834757	192.168.1.7	192.168.1.1	DNS	89	Standard query @0x2F1 A clientservices.googleapis.com
178	1.157232602	192.168.1.7	192.168.1.1	DNS	90	Standard query @0x14A0 A www.iut.ac.ir A 176.101.52.155
781	26.749386546	192.168.1.1	192.168.1.7	DNS	91	Standard query response @0x3FF A sh1.google.com A 216.58.289.142
1	Frame 769: 85 bytes on wire (688 bits), 85 bytes captured (688 bits) on interface wlp3s0, id 0					
	> Ethernet II, Src: ASUSTekC_84:8a:d4 (38:05:47:84:8a:d4), Dst: IntelCor_91:af:3c (34:41:5d:91:af:3c)					
	Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.7					
	> UDP, Src Port: 53, Dst Port: 53, Src Port: 39545					
	Source Port: 53					
	Destination Port: 39545					
	Length: 80					
	[Checksum: 0x8786 [unverified]]					
	[Checksum Status: Unverified]					
	[Stream index: 32]					
	[Timestamp]					
	Domain Name System (response)					

شکل ۲۰: پورت مبدأ پیام ۵۳ پورت DNS response ۵۳ است.

نتیجتاً پورت ۵۳ متعلق به سرویس DNS است.

### ۳.۳ سوال سوم

No.	Time	Source	Destination	Protocol	Length	Info
1616	28.151664695	192.168.1.7	192.168.1.1	DNS	79	Standard query @0x7e7d A materials.iut.ac.ir
779	26.781063709	192.168.1.7	192.168.1.1	DNS	79	Standard query @0x10ff A sh1.google.com
1	Frame 761: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface wlp3s0, id 0					
	> Ethernet II, Src: IntelCor_91:af:3c (34:41:5d:91:af:3c), Dst: ASUSTekC_84:8a:d4 (38:05:47:84:8a:d4)					
	Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1					
	0100 ... = Version: 4					
	... 0101 = Header Length: 20 bytes (5)					
	0000 0000 = Total Length: 690 bytes (552)					
	0000 0000 = Identification: 0x0000 (0SCP: CSH, ECN: Not-ECN)					
	Total Length: 55					
	Identification: 0x72ba (19370)					
	Flags: 0x0000 [Don't fragment]					
	Frag offset: 0					
	Time to live: 64					
	Protocol: UDP [17]					
	Header checksum: 0x44a0 [Validation disabled]					
	[Header checksum status: Unverified]					
	Source: 192.168.1.7					
	Destination: 192.168.1.1					
	Domain Name System (query)					

شکل ۲۱: پیام به آدرس 192.168.1.1 فرستاده شده است.

```

Link 3 (wlp3s0)
  Current Scopes: DNS
  DefaultRoute setting: yes
    LLMNR setting: yes
  MulticastDNS setting: no
    DNSOverTLS setting: no
      DNSSEC setting: no
      DNSSEC supported: no
  Current DNS Server: 192.168.1.1
  DNS Servers: 192.168.1.1
  DNS Domain: ~.

Link 2 (enp2s0)
  Current Scopes: none
  DefaultRoute setting: no
    LLMNR setting: yes
  MulticastDNS setting: no
    DNSOverTLS setting: no
      DNSSEC setting: no
      DNSSEC supported: no

```

شکل ۲۲: آدرس DNS server محلی شبکه من ۱۹۲.۱۶۸.۱.۱ است. (با استفاده از دستور `systemd-resolve --status` در لینوکس میتوان آن را پیدا کرد.)

متناسب با تصاویر ۲۱ و ۲۲ واضح هست که پیغام DNS query به همان DNS Server محلی شبکه من ارسال شده است.

#### ۴.۳ سوال چهارم

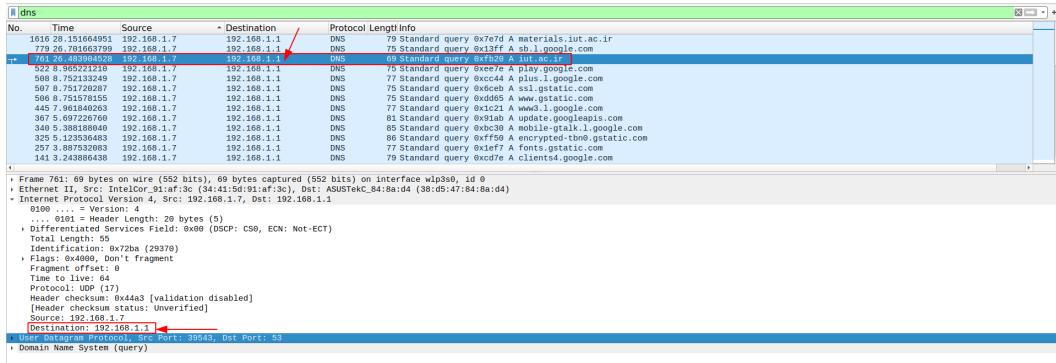
No.	Time	Source	Destination	Protocol	Length	Info
1616	28.1516640951	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x7e7d A materials.iut.ac.ir
779	28.701663799	192.168.1.7	192.168.1.1	DNS	79	Standard query 0x13ff A sb.1.google.com
781	28.4830984526	192.168.1.7	192.168.1.1	DNS	69	Standard query 0xf528 A iut.ac.ir
568	28.752133249	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xccc4 A www.google.com
568	28.751720287	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6ceb A plus.gsstatic.com
568	28.751578135	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6cbb A www.gsstatic.com
445	28.751578135	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x6c21 A static1.gsstatic.com
367	28.697226768	192.168.1.7	192.168.1.1	DNS	81	Standard query 0x91ab A update.gooleapis.com
349	28.388188049	192.168.1.7	192.168.1.1	DNS	89	Standard query 0xb330 A mobile-gtalk.l.google.com
325	28.388188049	192.168.1.7	192.168.1.1	DNS	89	Standard query 0xb330 A mobile-gtalk.l.gsstatic.com
257	28.887532083	192.168.1.7	192.168.1.1	DNS	77	Standard query 0x1ef7 A Fonts.gsstatic.com
1413	28.24386438	192.168.1.7	192.168.1.1	DNS	79	Standard query 0xc07e A clients4.google.com

Frame 781: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface wlp3s0, id 0
 ▷ Flags: 0x0100 [Standard query]
 ◁ Flags: 0x0100 [Standard query]
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 - Queries
 ▷ iut.ac.ir: type A, class IN
 Name: iut.ac.ir
 [Label Length: 3]
 [Label Count: 3]
 Type: A (Host Address) (1) ←
 Class: IN (0x0001)
 Response Id: 709

شکل ۲۳: پیغام DNS query ارسال شده از نوع A هست به این معنا که نام سایت برای DNS server فرستاده شده و منتظر دریافت آدرس IP متناظر با آن هستیم.

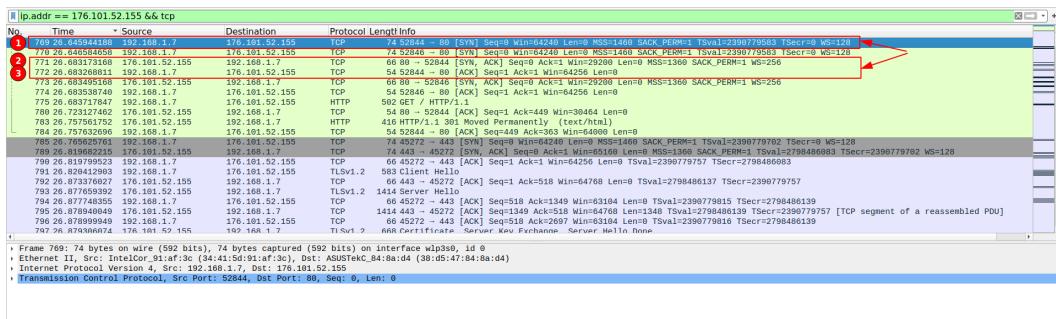
همچنین از تصویر فوق نیز پیداست که این پیغام حاوی جواب نیست (جواب در پیغام جداگانه ای تحت عنوان DNS response نمایش داده شد) به ما برمیگردد.

### ۵.۳ سوال پنجم



شکل ۲۴: قسمت Answer پیغام DNS response در مورد سایت iut.ac.ir تنها حاوی یک جواب است. (type A, class IN, addr 176.101.52.155)

### ۶.۳ سوال ششم



شکل ۲۵: three way handshaking

**توضیحات :** در تصویر ۲۵ از دو پورت ۵۲۸۴۴ و ۵۲۸۴۶ عملیات ۳ way handshaking HTTP تنها از پورت ۵۲۸۴۴ ادامه پیدا کرده است (طبق تصاویر ۱۲ و ۱۳) و این امر به دلیل آن بوده که من در مرورگر در دو tab جدا آدرس iut.ac.ir را وارد کرده بودم و سپس یکی از tab ها بستم.

آدرس مقصد بسته SYN دلیلاً همان آدرس آورده شده در قسمت Answer پیغام DNS response است (جوجع به تصویر ۲۴)(176.101.52.155)

### ۷.۳ سوال هفتم

بله ظاهرا سایت iut.ac.ir حاوی محتوایی از سایت material.iut.ac.ir بوده است.

No.	Time	Source	Destination	Protocol	Length	Info
341	13:42:51.000000000	192.168.1.7	192.168.1.1	DNS	60	Standard query 0xdca A mobile.talk.i.google.com
342	13:42:51.045945958	192.168.1.1	192.168.1.7	DNS	102	Standard query response 0xb03c8 A mobile.talk.i.google.com A 198.177.15.18
367	5.697226760	192.168.1.7	192.168.1.1	DNS	81	Standard query 0x91ab A update.googleapis.com
368	5.735785646	192.168.1.1	192.168.1.7	DNS	97	Standard query response 0x91ab A update.googleapis.com A 172.217.18.131
445	13:42:51.100000000	192.168.1.7	192.168.1.1	DNS	73	Standard query 0xc121 A www.3.l.google.com
446	1.999321333	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0xc121 A www.3.l.google.com A 172.217.169.238
596	6.751578133	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x0d05 A www.gstatic.com
597	5.751578133	192.168.1.1	192.168.1.7	DNS	75	Standard query response 0x0d05 A www.gstatic.com
598	6.752133249	192.168.1.7	192.168.1.1	DNS	77	Standard query 0xcc44 A plus1.google.com
512	6.788697775	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0xd6d5 A www.gstatic.com A 172.217.169.237
514	6.788697775	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0xd6d5 A s3l.gstatic.com A 172.217.169.131
515	6.791299293	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0xcc44 A plus1.google.com A 216.58.299.142
522	6.985221210	192.168.1.7	192.168.1.1	DNS	75	Standard query 0xee7e A play.google.com
534	6.065488500	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0xee7e A play.google.com A 172.217.18.142
762	26.644683166	192.168.1.7	192.168.1.1	DNS	69	Standard query 0xf2b0 A iut.ac.ir
768	26.644683166	192.168.1.1	192.168.1.7	DNS	85	Standard query response 0xf2b0 A iut.ac.ir A 176.101.52.155
779	26.781663799	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x1aff A sbl.google.com
780	26.781663799	192.168.1.1	192.168.1.7	DNS	93	Standard query response 0x1aff A sbl.google.com A 216.58.209.142
1816	176.101.52.155	192.168.1.7	192.168.1.1	DNS	95	Standard query response 0x7e7d A materials.iut.ac.ir A 176.101.52.155
1783	28.328922963	192.168.1.1	192.168.1.7	DNS	95	Standard query response 0x7e7d A materials.iut.ac.ir A 176.101.52.155

Frame 1616: 97 bytes on wire (632 bits), 97 bytes captured (632 bits) on interface wlp3s0, id 0  
Ethernet II, Src: Intel(R) Dual Band Wireless-AC (34:41:5d:91:a9:3c), Dst: ASUSTek\_C\_84:8a:d4 (38:05:47:84:8a:d4)  
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1  
User Datagram Protocol, Src Port: 38898, Dst Port: 53  
Domain Name System (query)  
    Transaction ID: 0x7e7d  
    Flag: Q  
    Question: Standard query  
        Questions: 1  
        Answer RRs: 0  
        Authority RRs: 0  
        Additional RRs: 0  
    Queries  
        materials.iut.ac.ir type A, class IN  
            Name: materials.iut.ac.ir  
            [Name Length: 19]  
            [Label Count: 4]  
            Type: A (1)  
            Class: IN (0x0001)  
        [Response Id: 1783]

### ۴ آزمایش ۱-۱-۳ : ردیابی بسته های ICMP

```
maryam@bitterocean:~
> ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=5.05 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=5.52 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=4.05 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=3.97 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=4.31 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=4.18 ms
^C
--- 192.168.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 3.967/4.511/5.524/0.573 ms
[ 5s ] ① 14:02:09
```

شکل ۲۶: اجرای دستور ping به آدرس 192.168.1.1

Apply a display filter: ... <Ctrl+>						
No.	Time	Source	Destination	Protocol	Length	Info
2	6.08808908908	129.168.14.86	138.199.14.86	TCP	60	[TCP ACKed unseen segment] 45911 - 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 Tsval=270936770 TSerr=366319485
3	5.563745883	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=1/256 ttl=64 (reply in 4)
4	5.563745883	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=1/256 ttl=64 (request in 3)
5	5.567145908	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=2/252 ttl=64 (reply in 6)
6	5.572176831	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=2/252 ttl=64 (request in 5)
7	5.598916603	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=3/768 ttl=64 (reply in 8)
8	5.603745883	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=3/768 ttl=64 (request in 7)
9	5.784406521	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=4/1024 ttl=64 (reply in 10)
10	5.74351446	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=4/1024 ttl=64 (request in 9)
11	5.74351446	192.168.1.7	224.0.2.51	MONS	183	Standard query 0x001a PTR _37F83649._sub._googlecast._tcp.local. "QM" question
12	5.72117717	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=5/1280 ttl=64 (reply in 13)
13	6.57632756	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0005 seq=5/1280 ttl=64 (request in 12)
14	7.574132723	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=6/1536 ttl=64 (reply in 15)
15	7.5782398087	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=6/1536 ttl=64 (request in 14)

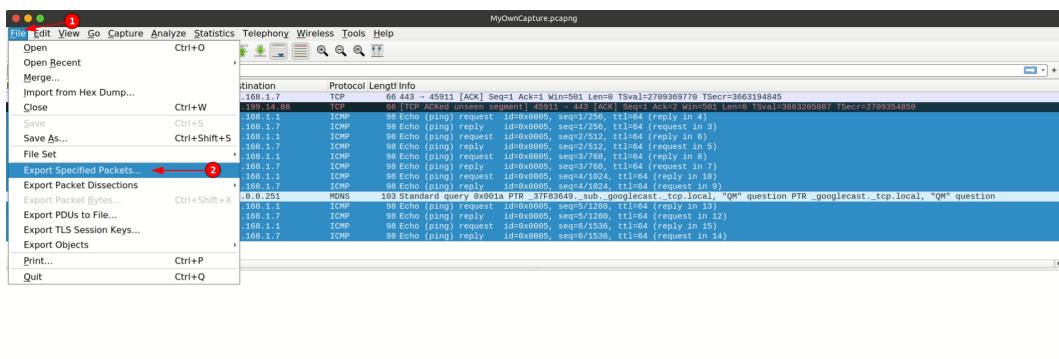
شکل ۲۷: وضعیت بسته های capture شده در حین اجرای ping به آدرس 192.168.1.1

اولین بسته یک ICMP است که از سیستم ما (192.168.1.7) به مقصد (192.168.1.1) روانه میشود و بعد از آن یک بسته ICMP replay است که از مبدأ 192.168.1.1 به سمت سیستم ما 192.168.1.7 ارسال شده است. و این روند به ازای هر ping تکرار میشود.(طبق تصویر ۲۶ من ۶ بسته ping فرستادم و هیچ loss هم نداشت و به همین دلیل در واپیشارک ۱۲ بسته ICMP جمع آوری شده است.)

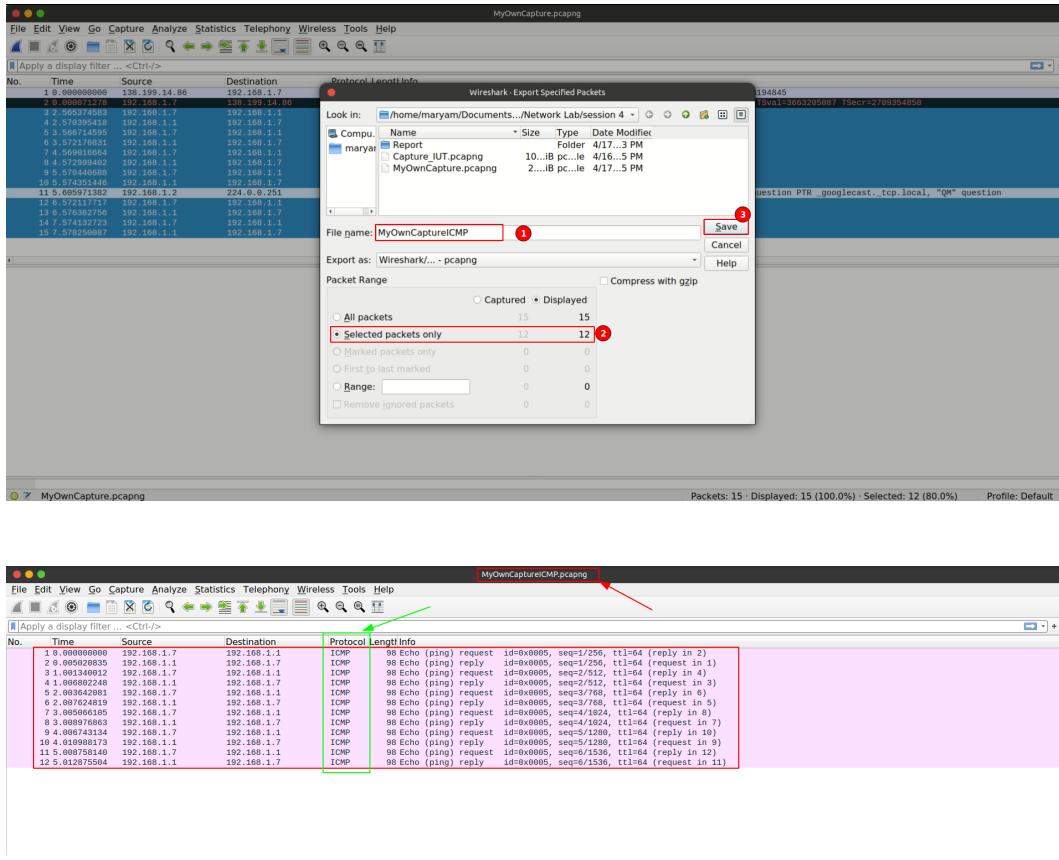
برای ذخیره کردن بسته های ICMP آنها را انتخاب میکنم (به کمک نگه داشتن دکمه Ctrl و کلیک روی بسته های مورد نظر) سپس از منوی File Export Specified Packets... گزینه... MyOwnICMP و بعد از انتخاب نام Save را میزنم. دکمه D

Apply a display filter: ... <Ctrl+>						
No.	Time	Source	Destination	Protocol	Length	Info
1	6.08808908908	138.199.14.86	192.168.1.7	TCP	60	[TCP ACKed unseen segment] 45911 - 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 Tsval=270936770 TSerr=3663194845
2	5.563745883	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=1/256 ttl=64 (reply in 4)
3	5.563745883	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=1/256 ttl=64 (request in 3)
5	5.567145908	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=2/252 ttl=64 (reply in 6)
6	5.572176831	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=2/252 ttl=64 (request in 5)
7	5.598916603	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=3/768 ttl=64 (reply in 8)
8	5.729994902	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=3/768 ttl=64 (request in 7)
9	5.784406521	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=4/1024 ttl=64 (reply in 10)
10	5.74351446	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=4/1024 ttl=64 (request in 9)
11	5.66591382	192.168.1.2	224.0.2.51	MONS	183	Standard query 0x001a PTR _37F83649._sub._googlecast._tcp.local. "QM" question
12	6.572117717	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=5/1280 ttl=64 (reply in 13)
13	6.57632756	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=5/1280 ttl=64 (request in 12)
14	7.574132723	192.168.1.7	192.168.1.1	ICMP	98	Echo (ping) request id=0x0005 seq=6/1536 ttl=64 (reply in 15)
15	7.5782398087	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) reply id=0x0005 seq=6/1536 ttl=64 (request in 14)

شکل ۲۸: انتخاب بسته های ICMP به کمک نگه داشتن دکمه Ctrl و کلیک روی بسته های مورد نظر



شکل ۲۹: برای ذخیره سازی به منوی File رفته و گزینه... Export Specified Packets... را انتخاب میکنیم.



شکل ۳۰: محتويات فایل MyOwnCaptureICMP.pcapng

## ۵ فایل های pcapng خروجی وایرشارک

- فایل capture کردن کلیه بسته ها در طی سرچ سایت iut.ac.ir در مرورگر :

- فایل capture کردن بسته ها در 192.168.1.1

- فایل حاوی بسته های ICMP در حین 192.168.1.1

**تذکر :** هر سه فایل فوق در پوشه آپلود شده در سامانه ضمیمه شده اند.