به نام خدا

درس شبکه های کامپیوتری

تمرین دوم عملی : Wireshark

مدرس : دکتر موحدی

سارا سادات یونسی-۹۸۵۳۳۰۵۳

سؤال ۱

پاسخ درست ۱

B

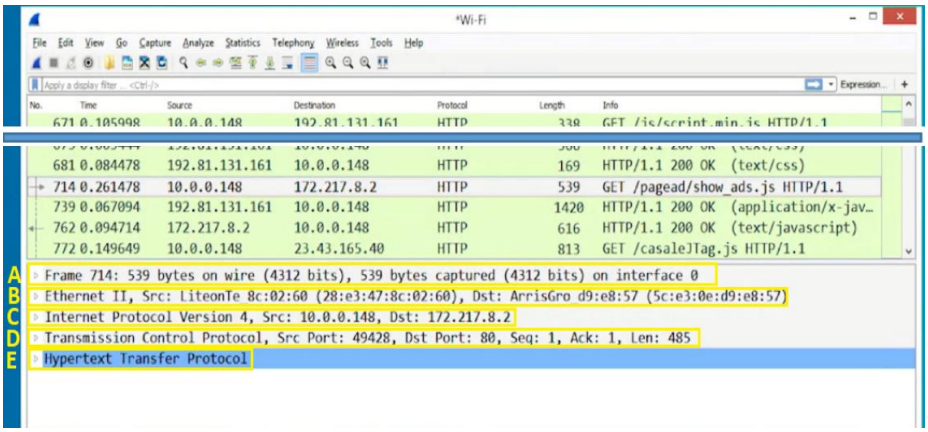
این یک فریم http است و شامل اطلاعات مبدا و مقصد می باشد .Ethernet II ,src/dest

چون فریم http توسط پروتکل Ethernet در نتورک راه پیدا می کنند و این هدر شامل اطلاعاتی مانند آدرس MAC مبدا و مقصد و نوع پروتکل استفاده شده یا همان تایپ که HTTP است را نشان می دهد . در نتیجه می توان گفت که هدر ایترنت به هدر فریم HTTP در قسمت اول این شکل است.

توضیحاتی درباره ی این HEADER:

اترنت(Ethernet) ، پروتکل استاندارد یا تکنولوژی است از خانواده ی شبکه های کامپیوتری که معمولا در شبکه های LAN (Local area network)و MAN (Metropolitan area network مورد استفاده قرار می گیرد. تجهیزاتی که از طریق اترنت ارتباط برقرار می کنند داده ها را به قسمت های کوچکتری به اسم قالب (Frame) تبدیل می کنند. با طول مشخص ۶۴ تا ۱۵۱۸هر استاندارد ممکن است ساختار خاصی را برای فریم تعریف کرده باشد. یک فریم از چندین بخش (field) تشکیل می گردد. و دارای آدرس فرستنده و گیرنده و اطلاعات خطایابی (error-checking) است، هر فیلد نیز از مجموعه ای بایت تشکیل شده است .همچنین در لایه Data link layer قرار می گیرد و شامل اطلاعات کنترلی من جمله چک سام برای اطمینان از درستی ان مجموعه هست.

گزینه A به کل هدر اشاره می کند اما ۱۴ بایت اولیه ی ما توسط B نمایش داده شد.

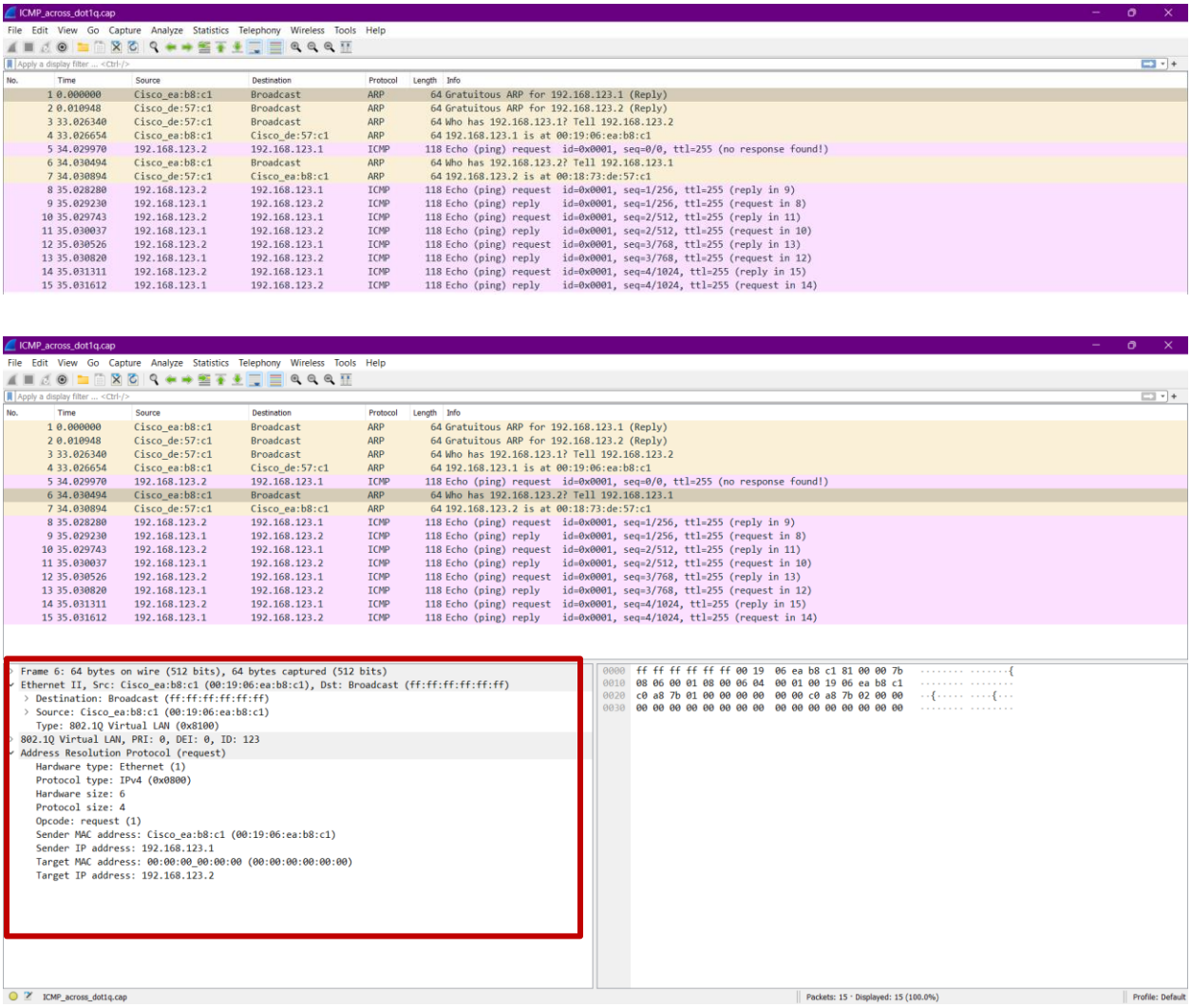


۱.شکل صورت سوال

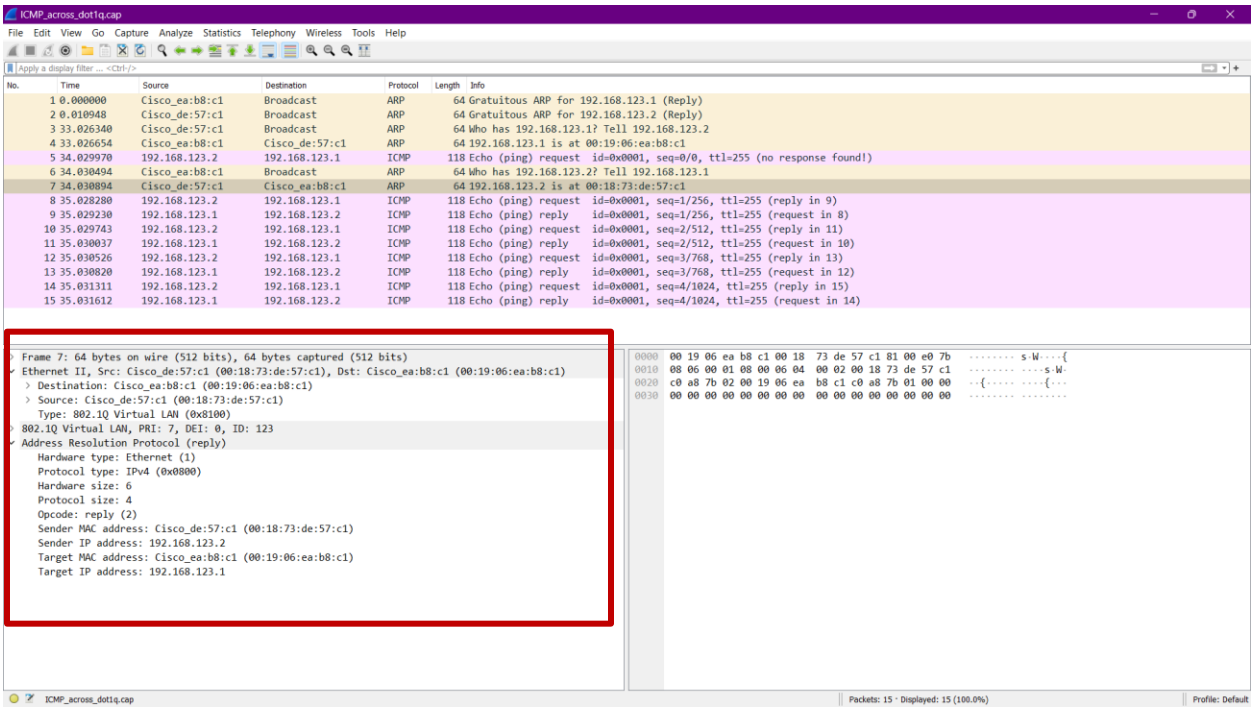
سؤال ۲

پاسخ درست ۲

الف)



۲.شکل ICMP request



۳.شکل ICMP reply

Request :
Source IP address : 192.168.123.1
Destination IP address : 192.168.123.2
Source MAC address : (Cisco_ea:b8:c1)00:19:06:ea:b8:c1
Destination MAC address : Broadcast (ff:ff:ff:ff:ff:ff)

Reply :
Source IP address : 192.168.123.2
Destination IP address : 192.168.123.1
Source MAC address : (Cisco_de:57:c1)00:18:73:de:57:c1
Destination MAC address : (Cisco_ea:b8:c1) 00:19:06:ea:b8:c1

قسمت های نارنجی جداول جواب نهایی و موردنظر هستند.

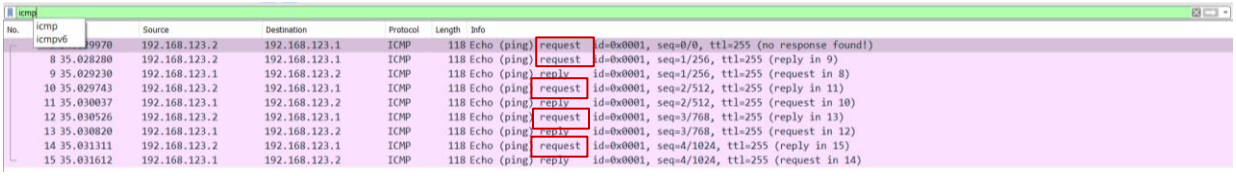
برای یافتن بسته رکوئست از بین broadcast شده ها آن هایی که gratuitous نباشند و با مک ادرس سوال مطابقت داشته باشند را در نظر میگیریم و به بسته مورد نظر می رسیم برای یافتن ریپلای هم دنبال arp های ریپلای دار و ان هایی که address resolution protocol کنار آن ها ریپلای نوشته است می پردازیم که با میدا ما سینک باشد.

و سپس اطلاعات لازم را از آدرس های مک و ای پی های رکوئست و ریپلای پیدا می کنیم .

A source MAC address is the address of the device sending the packet, and you can usually see it in the packet's Ethernet header

When a device is forwarding a message to an Ethernet network, the Ethernet header includes the following: Source MAC address: This is the MAC address of the source device NIC. Destination MAC address: This is the MAC address of the destination device NIC.

ب) براساس icmp فیلتر می کنیم که در نهایت ۵ تا ICMP REQUEST خواهیم داشت.



سؤال ۳

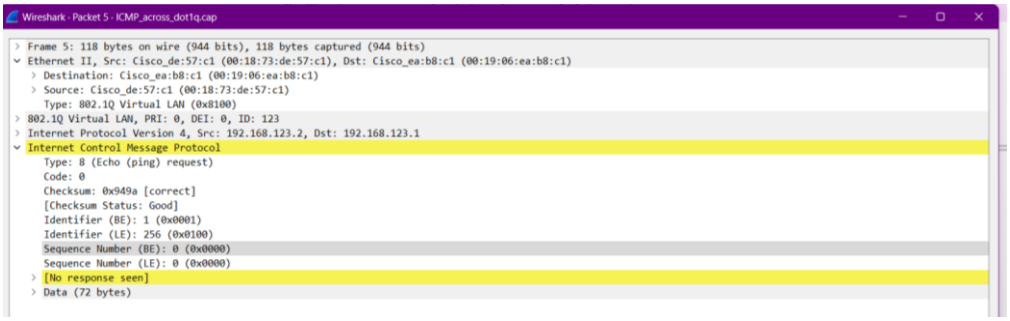
پاسخ درست ۳

توضیحی درباره ی RTT :

زمان رفت و برگشت (RTT) در شبکه، که به عنوان زمان تأخیر رفت و برگشت (RTD) نیز شناخته می‌شود، معیاری است که برحسب میلی ثانیه (ms) مدت زمان ارسال یک بسته داده، به اضافه مدت زمان دریافت تأییدیه سیگنال آن را نشان می‌دهد.به عبارت دیگر، RTTاز زمانی که مرورگر درخواستی را به سرور ارسال می‌کند تا زمانی که پاسخی از سرور دریافت می‌کند، محاسبه می‌شود. عدد حاصل از این محاسبه برای برنامه‌های کاربردی وب بسیار مهم است RTT .به همراه TTFB از اصلی‌ترین معیارهای اندازه‌گیری زمان بارگذاری صفحه و تأخیر شبکه محسوب می‌شود.در این بسته های ICMP نیز به همان معنای ارسال و دریافت یک بسته و یا request و reply زده شده دریافت شده را محسوب می کنیم.

فریم های مورد بررسی :

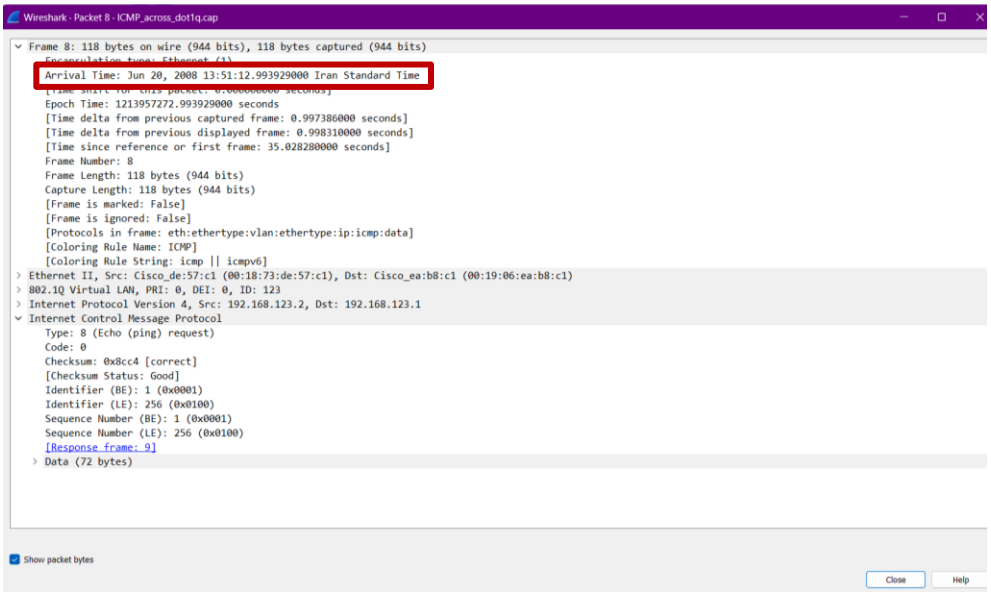
Arrival time دو بسته ی رکوئست و ریپلای فریم را از هم کم می کنیم و حاصل را پیدا می کنیم یا می توانیم از عددی که برای ریسپانس تایم گذاشته شده استفاده کنیم ..برای بسته ی ۵ محاسبه نمی شود چون فاقد ریپلای است.



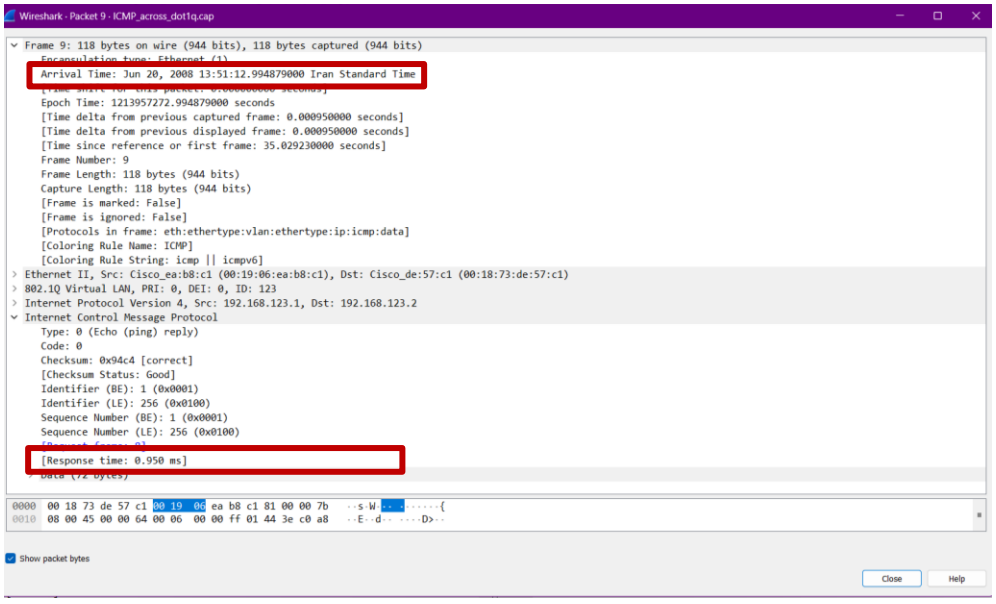
۴.شکل فریم ۵

برای

Request :8 → Reply :**9** **0.994879-0.993929=0.950ms**

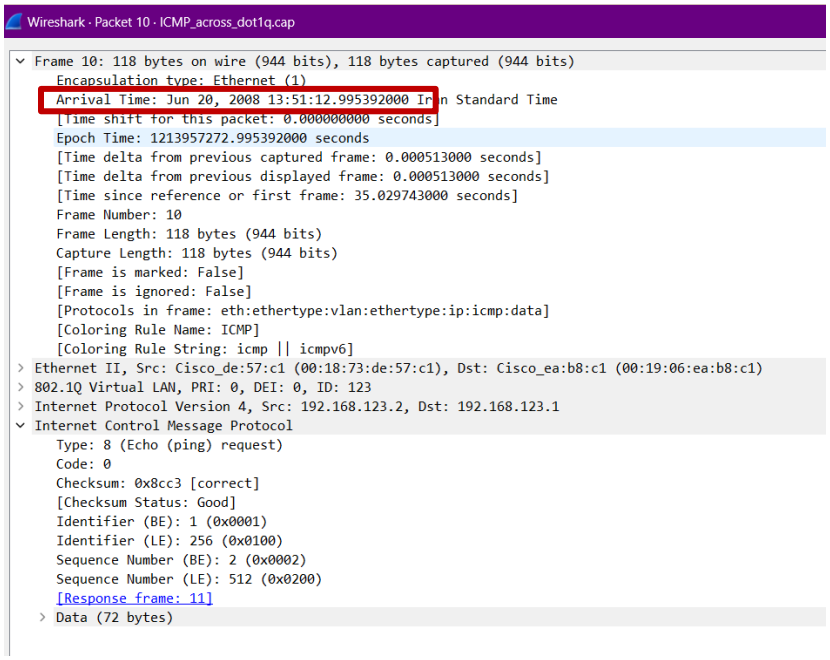


۵. شکل فریم ۸ درخواست

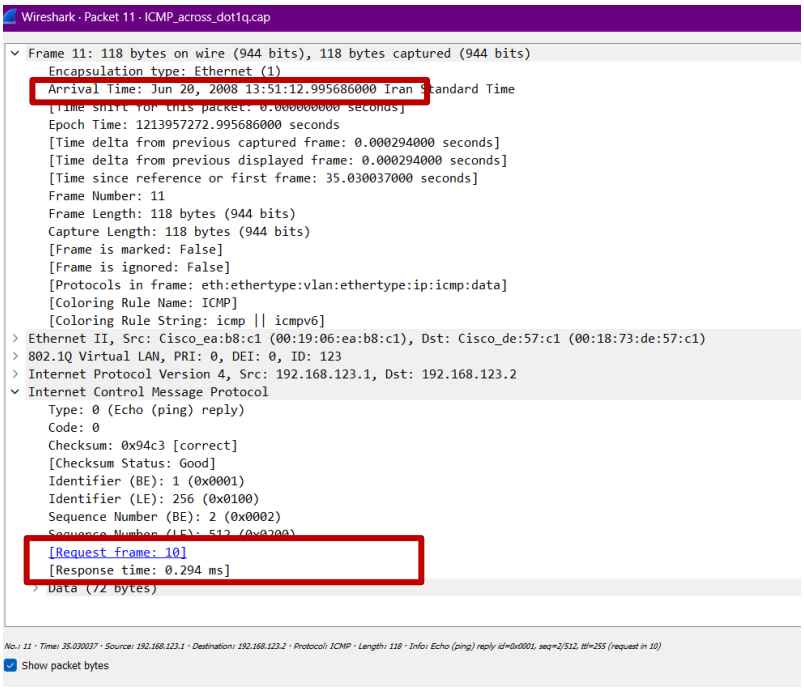


۶. شکل فریم ۹ پاسخ

Request : 10 → Reply : 11 0.995686-0.995392=0.294ms

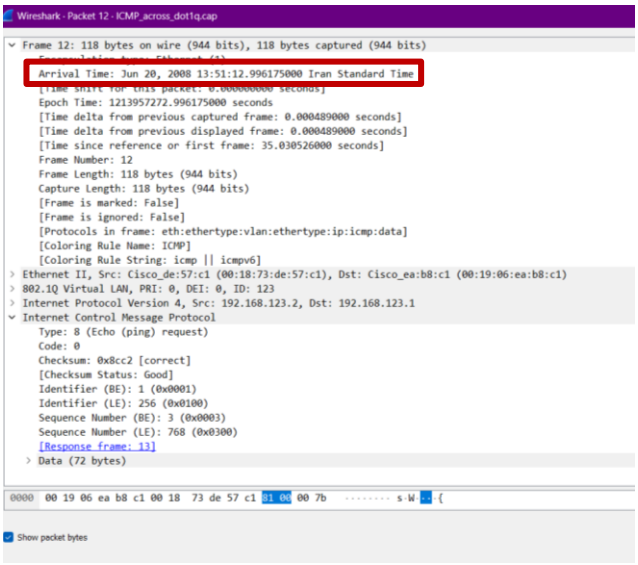


۷. شکل فریم ۱۰ درخواست

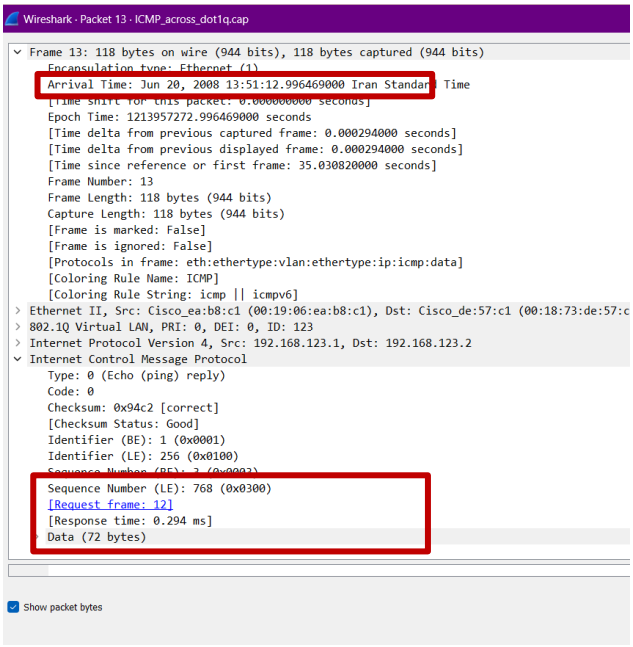


۸. شکل فریم ۱۱ پاسخ

Request : 12 → Reply : 13 0.996469-0.996175=0.294ms

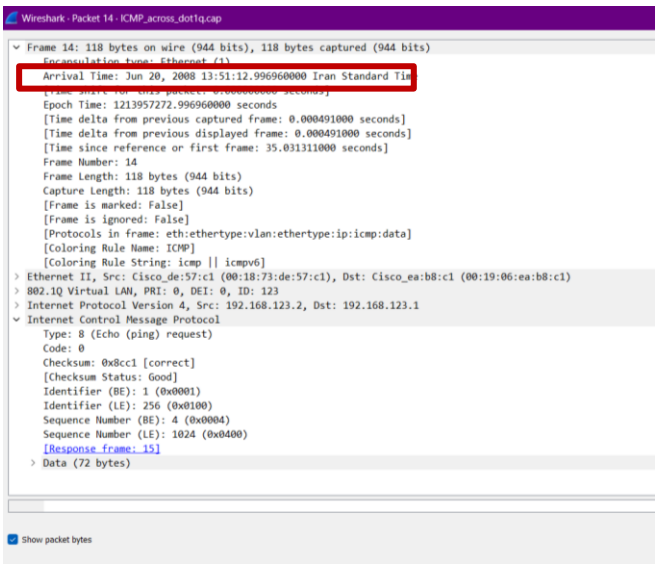


۹. شکل فریم ۱۲ درخواست

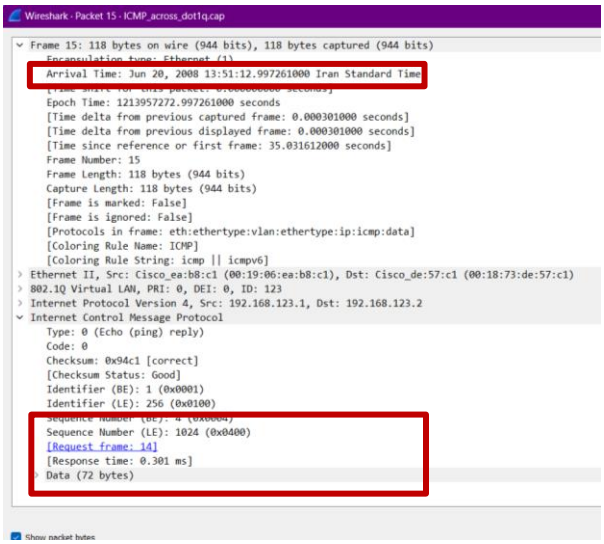


۱۰. شکل فریم ۱۳ پاسخ

Request : 14 → Reply : 15 0.997261-0.996960=0.301ms



۱۱. شکل فریم ۱۴ درخواست



۱۲. شکل فریم ۱۵ پاسخ

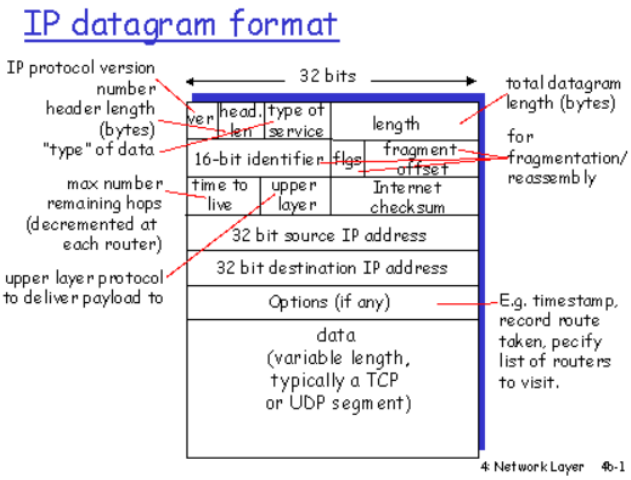
A)Min = 0.294 ms

B)Max =0. 950 ms

C)Avg = 0.45975 ms

سؤال ٤

پاسخ درست ۴



Note: for each packet, the first 14 Bytes are the Ethernet header.

```
01 00 5e 00 00 fc 60 eb  69 4d 97 3f 08 00 46 00
00 20 07 32 00 00 01 02  33 d7 ac 11 5c c1 e0 00
00 fc 94 04 00 00 16 00  09 03 e0 00 00 fc 00 00
00 00 00 00 00 00 00 00  00 00 00 00
```

Header : 14 bit

ip source address : ac 11 5c c1 → 172.17.92.193

ip destination address: e0 00 00 fc → 224.0.0.252

ip protocol : 02 → IGMP

فیلد پروتوکل در بایت ۲۴ ام قرار دارد که همانطور که مشاهده می کنیم ۰۲ است که نماد پروتوکل Internet Group Management Protocol

در لایه ی سوم مدل tcp / ip قرار دارد

IGMP(Internet Group Management Protocol)پروتکلی است که عضویت هاست در گروه های IP multicast موجود در یک بخش (Segment) از شبکه مدیریت میکند. یک گروه IP Multicast که با نام یک host group هم شناخته میشود، مجموعه ای از هاست‌ها است که به ترافیک های آدرس دهی شده با آدرس IP multicast در شبکه گوش میدهند. ترافیک IP multicast در واقع به یک آدرس MAC فرستاده اما توسط چندین هاست پردازش میشود.

```
01 00 5e 00 00 01 64 31  50 0e 0a 2f 08 00 45 00
00 3c 2c a3 00 00 80 01  25 77 ac 11 5c 94 e0 00
00 01 08 00 2d de 00 01  0a 90 42 69 74 44 65 66
65 6e 64 65 72 20 46 69  72 65 77 61 6c 6c 20 42
72 6f 61 64 63 61 73 74  00 00
```

ip source address : ac 11 5c 94 → 172.17.92.148

ip destination address: e0 00 00 01 → 224.0.0.1

ip protocol : 01 → ICMP

فیلد پروتوکل در بایت ۲۴ ام قرار دارد که همانطور که مشاهده می کنیم ۰۱ است که نماد پروتوکل Internet Control Message Protocol

از پروتوکل های اصلی بسته پروتکل های اینترنت

پروتکل icmp که مخفف عبارت internet control message protocol است که در فارسی آن را پروتکل کنترل پیام های اینترنتی ترجمه می کنند. icmp جهت خطایابی در کامپیوترها ، روترها و هاست، بررسی وجود سیگنال و به طور کلی بررسی وضعیت ارتباطی بین روتر و سرور ها مورد استفاده قرار می گیرد.

در مدل ۵ لایه ای شبکه، این پروتکل همانند پروتکل ip در لایه ی network (شبکه) قرار می گیرد، اما نوع کارکرد آن شبیه پروتکل های لایه ی transport (انتقال) می باشد.

سؤال ۵

پاسخ درست ۵

الف) بسته ICMP دارای پورت مبدا و مقصد نیست زیرا برای network-layer information طراحی شده است.

و این دیتا ها بین روتر و هاست جا به جا می شوند نه برای فرایند های applications layer

هر بسته ICMP یک "نوع" و یک "کد" دارد. ترکیب نوع/کد پیام خاص در حال دریافت را مشخص می کند. از آنجایی که خود نرم افزار شبکه همه چیز را تفسیر می کند پیام های ICMP، برای هدایت پیام ICMP به یک لایه برنامه application layer ، به شماره پورتی نیاز نیست

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

ب)request

ping request: type: 8 code number: 0

Data sectionبا سایز متغیر خواهیم داشت ودیتای خالص را به ما نشان می دهد و هدر ۸ بایتی که این هدر شامل ایتم های زیر می باشد:

Type : مشخص کننده ی نوع پیام ICMP و یک بایت را شامل می شود در اینجا برابر ۸

Code : در اینجا برابر با صفر اطلاعات بیش تری درباره ی تایپ پیام در اختیار ما می گذارد و دراینجا جزئیاتی همچون زیر نوع ها و خطاها را مشخص می کند که در اینجا به معنای فرستادن یک پینگ مشخص و درخواست ارسال پاسخ است. شامل یک بایت

Checksum : 2 بایت برای اطمینان از درستی پکت

Identifier : ۲ بایت برای بایند کردن رکوئست به ریپلای

Sequence number :شماره توالی خام مقدار واقعی تخصیص داده شده به بسته است. WireShark جلسات TCP را گروه بندی می کند و به آنها اعداد توالی نسبی (و تایید) اختصاص می دهد که از ۰ شروع می شود (و به نظر می رسد برای هر بسته بعدی ۱ افزایش می یابد) تا کاربر بتواند توالی رویدادها را شناسایی کند.

2بایت

ث)reply

type: 0 code number: 0

Type : مشخص کننده ی نوع پیام ICMP و یک بایت را شامل می شود در اینجا برابر 0

نوع پیام ICMP اینجا اکو ریپلای و برابر صفر و کد آن هم برابر صفر می باشد.

Code : در اینجا برابر با صفر اطلاعات بیش تری درباره ی تایپ پیام در اختیار ما می گذارد و دراینجا جزئیاتی همچون زیر نوع ها و خطاها را مشخص می کند که در اینجا به معنای فرستادن یک پینگ مشخص و درخواست ارسال پاسخ است. شامل یک بایت

Checksum : 2 بایت برای اطمینان از درستی پکت

Identifier : ۲ بایت برای بایند کردن رکوئست به ریپلای

Sequence number :شماره توالی خام مقدار واقعی تخصیص داده شده به بسته است. WireShark جلسات TCP را گروه بندی می کند و به آنها اعداد توالی نسبی (و تایید) اختصاص می دهد که از ۰ شروع می شود (و به نظر می رسد برای هر بسته بعدی ۱ افزایش می یابد) تا کاربر بتواند توالی رویدادها را شناسایی کند.

2بایت

```
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xde69 [correct]
[Checksum Status: Good]
Identifier (BE): 2 (0x0002)
Identifier (LE): 512 (0x0200)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
```

رکوئست

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xe669 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
```

ریپلای