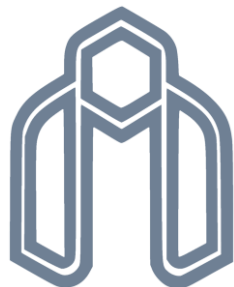


شبکه‌های کامپیوتری

تمرین دوم



دانشگاه صنعتی شاهرود

دکتر رضوانی

مصطفی فضلی - ۹۸۲۲۸۰۳

۱۳ اردیبهشت ماه ۱۴۰۱

سوال 1

حداقل 10 پروتکل از لایه کاربرد Application Layer را نام برده و مشخص کنید از کدام پروتکل لایه انتقال و چه پورتی استفاده می‌کنند.

- وب (the Web) HTTP <= پورت 80 و 8080 (TCP OR UDP)
- انتقال فایل (file transfer) FTP <= پورت 21 (TCP)
- ورود از راه دور (remote login) Telnet <= پورت 23 (TCP)
- اشتراک گذاری فایل بیت تورنت (BitTorrent file sharing) BitTorrent <= پورت 6969 (TCP)
- ایمیل (e-mail) SMTP <= پورت 25 و 587 (TCP)
- اداره پست ورژن 3 (Post Office Protocol v3) POP3 <= پورت 110 (TCP)
- دیمون چاپگر خطی (Line Printer Daemon) LPD <= پورت 515 (TCP)
- دسترسی به پیام اینترنتی (Internet Message Access) IMAP <= پورت 143 (TCP)
- انتقال فایل بی اهمیت (Trivial File transfer) TFTP <= پورت 69 (UDP)
- مدیریت شبکه ساده (Simple Network Management) SNMP <= پورت 161 (TCP) و 162 (UDP)
- سیستم نام دامنه (Domain Name System) DNS <= پورت 53 (TCP)

سوال 2

توضیح دهید که stateless بودن پروتکل HTTP به چه معنی است؟

پروتکل بدون حالت، پروتکلی ارتباطی است که در آن هیچ اطلاعاتی توسط گیرنده که معمولا یک سرور است ذخیره نمی‌شود. بدین معنا که در سمت سرور به ازای هر درخواست اطلاعاتی نظیر کوکی ذخیره نمی‌شود و اغلب در سمت کلاینت و مرورگر کاربر این اطلاعات ذخیره می‌شوند.

بدون حالت بودن در HTTP بدین معناست که هر پیام می‌تواند به صورت مجزا قابل درک باشد.

سوال 3

آیا یک سرور با یک نام مشخص می‌تواند بیش از یک آدرس IP داشته باشد؟ این موضوع چگونه می‌تواند به توزیع بار بر روی یک سرور کمک کند.

بله یک سرور با یک نام مشخص می‌تواند بیش از یک آدرس IP داشته باشد، این امر باعث می‌شود که خدمات یک سایت، از چندین میزبان باشد و آدرس نیز حفظ شود، همچنین در هنگامی که یک هاست در آن هنگام از کار افتاده باشد، می‌توان از دیگر هاست‌ها استفاده کرد تا این موضوع را جبران کنیم.

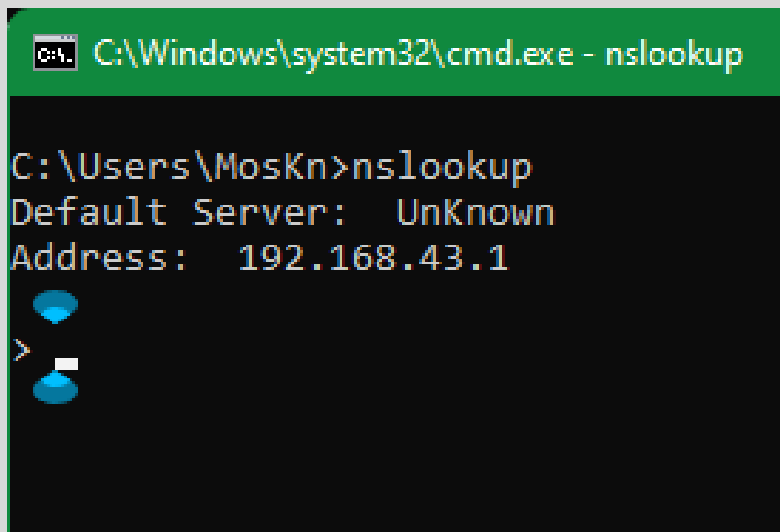
این پروتکل بدین دلیل که از DNS برای توزیع بار بین سرورهای تکراری استفاده می‌کند. سامانه‌های پر استفاده بر روی چندین سرور تکرار شده‌اند و هر یک روی یک دستگاه انتهایی متفاوت در حال اجرا هستند.

این کلاینت معمولاً درخواست خود را که از جنس http است به آدرس IP ارسال میکند، آنگاه برنامه DNS از طریق یک چرخه به توزیع ترافیک در بین سرورهای متفاوت می‌پردازد.

سوال 4

در سیستم عامل ویندوز و در command prompt می‌توانید با کمک دستور nslookup درخواست (query) DNS ارسال نمایید. در این تمرین با کمک این دستور پاسخ سوالات زیر را بدهید. برای هر سوال لازم است که حداقل یک دستور nslookup اجرا نمایید. لذا تصویر دستور اجرا شده در کامپیوتر خود را نیز ضمیمه کنید. دقت نمایید که کامپیوتر شما باید به اینترنت متصل باشد.

A. نحوه اتصال کامپیوتر شما به اینترنت چگونه است (برای نمونه از طریق ADSL یا شبکه اینترنت دانشگاه و یا موبایل متصل شده‌اید)



```
C:\Windows\system32\cmd.exe - nslookup

C:\Users\MosKn>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

>
```

نحوه اتصال سیستم بنده به اینترنت از طریق تلفن همراه است، به همین دلیل در هنگام nslookup گرفتن، آیدی از آدرس 192.168.43.1 می‌باشد، هر چه دستگاه های دیگری به این تلفن همراه متصل بشوند، رقم آخر این بخش بیشتر میگردد. اگر از طریق دانشگاه یا با استفاده از ADSL به اینترنت متصل بشویم، این آیدی عوض شده و همچنین ممکن است نام آن عوض بشود.

سوال 4

B. لیست DNS Server ها تنظیم شده بر روی کامپیوتر خود را ارائه کنید.

```
Select C:\Windows\system32\cmd.exe

C:\Users\MosKn>ipconfig /all

Windows IP Configuration

Host Name . . . . . : MosFazli
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 00-2B-67-A4-F8-BF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Unknown adapter Local Area Connection 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Windscribe Windtun420
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Unknown adapter ProtonVPN TUN:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : ProtonVPN Tunnel
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Unknown adapter HotspotShield Network Adapter:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : HotspotShield TAP-Windows Adapter V9
Physical Address. . . . . : 00-FF-01-99-15-77
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-04
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Enabled

Unknown adapter Local Area Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

با استفاده از دستور ipconfig و آپشن /all میتوانیم لیست تمامی DNS سرور های تنظیم شده روی کامپیوتر را بررسی کنیم.



سوال 4

C. لیست آدرس‌های IP را برای نام `www.yahoo.com` استخراج نمایید. نام واقعی این سرور را مشخص نمایید. کدام DNS Server پاسخ query شما را ارائه نموده است.

با استفاده از دستور `nslookup` می‌توان تمامی آدرس‌های IP را برای نام آدرس www.yahoo.com استخراج نمائیم، نام واقعی این سرور در بخش دوم `new-fp-shed.wg1.b.yahoo.com` نوشته شده است، برای این که پاسخ کوئری کدام DNS است، در بخش بالای Non-authoritative answer این بخش آمده است.

همچنین با آپشن `type=any` سایر آدرس‌ها نیز مشاهده می‌شوند.

```
C:\Windows\system32\cmd.exe
C:\Users\MosKn>nslookup www.yahoo.com
Server: UnKnown
Address: 192.168.43.1

Non-authoritative answer:
Name: new-fp-shed.wg1.b.yahoo.com
Addresses: 2a00:1288:110:c305::1:8000
           2a00:1288:110:c305::1:8001
           87.248.100.214
Aliases: www.yahoo.com

C:\Users\MosKn>
```

سوال 4

D. لیست آدرس های IP برای نام `golestan.shahroodut.ac.ir` استخراج نمائید. برای این بخش باید DNS Server خود را به 4.2.2.4 تغییر دهید. دقت نمائید که نباید تنظیمات شبکه ای خود را تغییر دهید. تنها کافیست در زمان اجرای دستور `nslookup`، آدرس IP سرور جدید را بدهید.

```
C:\Windows\system32\cmd.exe

C:\Users\MosKn>nslookup golestan.shahroodut.ac.ir 4.2.2.4
Server:  d.resolvers.level3.net
Address:  4.2.2.4

Non-authoritative answer:
Name:    golestan.shahroodut.ac.ir
Address: 185.123.68.16

C:\Users\MosKn>
```

لیست آدرس های IP با استفاده از DNS Server مشخص شده
و تغییر یافته 4.2.2.4 به شکل زیر است. دستور آن نیز به طور کامل در کد
آمده است

185.123.68.16

سوال 4

E. نام واقعی سرور ایمیل را برای mail.google.com پیدا نمایید. برای این منظور باید نوع query را به MX تغییر دهید.

برای این منظور دستور فوق را میزنیم تا بخش مورد نظر با توجه به زیر بیاید، nslookup -type=mx mail.google.com بدین صورت می توان عبارت primary name server که نوشته شده است ns1.google.com است، نام واقعی سرور ایمیل است.

```
C:\Windows\system32\cmd.exe

C:\Users\MosKn>nslookup -type=mx mail.google.com
Server: UnKnown
Address: 192.168.43.1

google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 446669762
    refresh = 900 (15 mins)
    retry = 900 (15 mins)
    expire = 1800 (30 mins)
    default TTL = 60 (1 min)

C:\Users\MosKn>
```

سوال 4

F. آدرس IP سرور ایمیل را برای mail.google.com پیدا نمایید. ابتدا از بخش E نام واقعی سرور ایمیل را پیدا نموده و سپس یک query از نوع A ارسال نمایید تا آدرس IP را برگرداند.

ابتدا از بخش قبل نام واقعی را به دست آورده و سپس با استفاده از مشابه کوئری که در قسمت A به دست آمده است، کوئری را وارد میکنیم و بدین شکل خواهیم داشت:

```
C:\Windows\system32\cmd.exe

C:\Users\MosKn>nslookup -type=a ns1.google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     ns1.google.com
Address:  216.239.32.10

C:\Users\MosKn>
```

سوال 5

A. از هنگامیکه کلاینت روی لینک کلیک میکند تا زمانیکه شی مورد نظرش را دریافت می کند چه مدت زمانی به طول می انجامد؟

به طور معمول با توجه به اطلاعات داده شده در سوال مدت زمان به این اندازه است :

$$RTT_1 + RTT_2 + \dots + RTT_n$$

اگر زمان در RTT_0 را در نظر بگیریم، با توجه به اینکه برای ارسال و دریافت (برقراری ارتباط) میان کلاینت و سرور دو بار تکرار میشود داریم :

$$2RTT_0 + RTT_1 + RTT_2 + \dots + RTT_n$$

سوال 5

B. حال با فرض اینکه فایل HTML به 8 شئی بسیار کوچک روی همان سرور ارجاع دهد و پروتکل HTTP گذرا باشد و اتصالات TCP به صورت سری برقرار شود قسمت a را حل کنید.

$$RTT_1 + \dots + RTT_n + 2RTT_o + 8 \cdot 2RTT_o \\ = 18RTT_o + RTT_1 + \dots + RTT_n$$

C. قسمت b را فرض آنکه پروتکل HTTP گذرا باشد و مرورگر برای 5 اتصال موازی پیکر بندی شده باشد حل کنید.

$$RTT_1 + \dots + RTT_n + 2RTT_o + 2 \cdot 2RTT_o \\ = 6RTT_o + RTT_1 + \dots + RTT_n$$

D. با فرض اینکه فایل HTML به 8 شئی بسیار کوچک باشد و پروتکل HTTP ماندگار باشد مسئله را حل کنید.

•Persistent-pipelining

$$RTT_1 + \dots + RTT_n + 2RTT_o + RTT_o \\ = 3RTT_o + RTT_1 + \dots + RTT_n$$

Persistent connection without pipelining, without parallel connections.

$$RTT_1 + \dots + RTT_n + 2RTT_o + 8RTT_o \\ = 10RTT_o + RTT_1 + \dots + RTT_n$$

سوال 6

اگر چه web cache منجر به کاهش مدت زمان درخواست کاربر می‌شود ولی مشکل جدیدی را ایجاد می‌کند. یک کپی از شیء object در Cache ذخیره می‌شود که ممکن است قدیمی باشد. به عبارتی دیگر در حالی که کپی شیء در حافظه Cache ذخیره می‌شود ممکن است شیء مقیم در سرور وب دچار تغییراتی شده باشد. حال توضیح دهید که این مشکل چگونه توسط پروتکل HTTP حل می‌شود؟

بوسیله درخواست شرطی، سرور کش با استفاده از این هدر در پروتکل معلوم بررسی میکند که آیا از تاریخی که شیء ذخیره شده در سرور تغییری کرده است یا خیر، اگر این فایل تغییری کرده باشد، سرور شیء را دوباره ارسال میکند، در غیر اینصورت پیغام 304 not modified را ارسال میکند تا سرور کش از فایل درون دیتابیس خود استفاده کند.

سوال 7

پایدار:

$$d_{\text{nodal}} = d_{\text{queue}} + d_{\text{prop}} + d_{\text{trans}} + d_{\text{proc}}$$

$$d_{\text{prop}} + d_{\text{trans}} = \left(\frac{7.2}{1.8}\right) \times 2RTT + \left(\frac{7.2 \times 1000 \times 8}{1 \text{ mbps}}\right) = 4 \times 2 \times 40 + 57.6 = 320 + 57.6 = 3.7 \times 10^2 \text{ ms}$$

$$d_{\text{prop}} + d_{\text{trans}} = \left(\frac{3.6}{1.8}\right) \times 5 \times 2RTT + \left(\frac{1.8 \times 8 \times 1000}{1 \text{ mbps}}\right) =$$

$$2 \times 5 \times 2 \times 40 + 14.4 = 800 + 14.4 = 8.1 \times 10^2 \text{ ms}$$

$$(3.7 + 8.1) \times 10^2 = 11.8 \times 10^2$$

ناپایدار:

$$N \text{ segment} = \left(\frac{7.2}{1.8}\right) + \left(\frac{3.6}{1.8}\right) \times 5 = 14 \quad d_{\text{prop}} = 15RTT = 15 \times 40 = 6 \times 10^2 \text{ ms}$$

$$d_{\text{trans}} = (7.2 + 3.6 \times 5) \times 8 / 1 \text{ mbps} = 201.6 \text{ kbit} / 1 \text{ mbps} = 2 \times 10^2 \text{ ms}$$

$$6 + 2 = 8 \times 10^2 \text{ ms}$$

سوال 8

```
mosfazli@knight:~ | 146x30 | pts/0
(20:46:22)→ telnet
telnet> open shahroodut.ac.ir 80
Trying 85.185.67.248...
Connected to shahroodut.ac.ir.
Escape character is '^]'.
GET / HTTP/1.1
if-Modified_Since: Wed, 20 June 2012 10:15:22 GMT
Host: shahroodut.ac.ir

HTTP/1.1 302 Found
Date: Tue, 10 May 2022 16:16:42 GMT
Server: Apache
Location: https://shahroodut.ac.ir/
Content-Length: 209
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="https://shahroodut.ac.ir/">here</a>.</p>
</body></html>
Connection closed by foreign host.
(20:46:59)→
```

با استفاده از دستور telnet میتوان برای بازکردن یک کانکشن دانشگاه صنعتی شاهرود و تعیین پورت 80 برای HTTP درخواستی از نوع GET فرستاد. سپس با تعیین سرآیند if-modified-sience آخرین اطلاعات کش شده از سرور به دست می آید.

سوال 9

به پیام‌های دریافتی در ایمیل خود نگاه کنید. آیا می‌توانید از سرآیند یک پیام، آدرس IP سیستمی که پیام از آنجا ارسال شده است را استخراج نمایید؟ یک نمونه سرآیند را نوشته و پاسخ خود توضیح دهید.

```
E4b6y/JAfzsKnG247oaxKtb8EujOxslfSvY9sDXaiCjNH#b0fSd4A2So+yxQUuURlMmB
MeB++xwhQUHyTrIgnuft2a+c5Pkm3lhr7BhmQ241BynU9Rm117WQ6suBB2x6FAwKFKV6
M5AKQVCvVh2EGa6znImpj/WH6A+t00fFc+JrYKf0zIpxXE6uNzK/QFD1LcJf0w5w6bx5
ZcdFwREHCBQ/7CFRwSHc1+vnpTXh6FWL3W2cFFL7X70+t/oc5GTU4bsYDoHjg+HTZUtS
YcHA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=content-transfer-encoding:message-id:user-agent:references
:in-reply-to:subject:to:from:date:mime-version:dkim-signature;
bh=+pv8m9RChBEv7Y0s5CRwp95/uxx099mzX0ChZU2pyMw==;
b=IfK03qdEt7wmSK11aQnhP9aLtBK24GK9gtHGAbJWYuQ9ucrJN+ONAsbZS/e4NRgyQ
ioFoOrLfJZc9nPe4WGFry9Xv2TbcLJg0vAhS2G5Pvcpg59vI2ZMUrqsYVrV/Xoa4LJbI
G5teAxlNifvY7sPbAd3AkceTbQ82MkICTAVOXzVfX7Ex2s07RLJ7DX8YLiKfwtGaTFKz
X8mlqJpLzSQ50QoadE6l9Q8gOpI8ki4crx635W0QumghdFGm2kGBgEdXuDeK+JiAIN04
TLowXsvglyhP/tuBqvqberk7CRKvQ8LL1Hhkh36104GlnC3C7CAko8Vr/qldagE6cX
w19w==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@suigle.com header.s=default header.b=Lvp00iQA;
spf=pass (google.com: domain of zahedi@suigle.com designates 184.170.148.112 as permitted sender) smtp.mailfrom=zahedi@suigle.com
Return-Path: <zahedi@suigle.com>
Received: from mail-server205.webhostingbuzz.com (mail-server205.webhostingbuzz.com. [184.170.148.112])
by mx.google.com with ESMTPS id w8-20020a05622a190800b002f1d4ac0d12s16173108qtc.498.2022.05.01.23.59.30
for <mosfazli@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDHE-AES128-GCM-SHA256 bits=128/128);
Sun, 01 May 2022 23:59:30 -0700 (PDT)
Received-SPF: pass (google.com: domain of zahedi@suigle.com designates 184.170.148.112 as permitted sender) client-ip=184.170.148.112;
Authentication-Results: mx.google.com;
dkim=pass header.i=@suigle.com header.s=default header.b=Lvp00iQA;
spf=pass (google.com: domain of zahedi@suigle.com designates 184.170.148.112 as permitted sender) smtp.mailfrom=zahedi@suigle.com
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=suigle.com; s=default; h=Content-Transfer-Encoding:Content-Type:Message-ID:References:In-Reply-To:Subject:To:From:Date:MIME-
Version:Sender:Reply-To:Cc:Content-ID: Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc :Resent-Message-ID:List-Id:List-Help:List-Unsubscribe:List-Subscribe: List-Post:List-
Owner:List-Archive; bh=+pv8m9RChBEv7Y0s5CRwp95/uxx099mzX0ChZU2pyMw==; b=Lvp00iQAaIawKj149BNGRVZqa uti7Mq0f7uLtuK7of0fHyXH1lenmM88c+UURhY3TmZ07hLKkaAFzxLPXonQeIXAAdNHfMbsXftD1aGi
Lr90MOMy8kQqpsr/G0ENDz/nk1UzXJN1fKt10ZmrJpikvf7adkM6SH7bej3voEj18GwKd30P189zb IM+haPNvu4FSLp2J8Q/d4WvzdPxhUedZ8hwIPLZaCveOAaw4jyfEWvkvNoXQIXEGavNyR6MgaXgcLN
tp7+Utt9W4xnl9nbM6pAxHvvrF8DIKFCvf73VwLJAPOf+HAe+Rc3YVXZeGyuBGStmMRz5N0Ni92D SBHxaENA==;
Received: from [::1] (port=55146 helo=server205.webhostingbuzz.com) by server205.webhostingbuzz.com with esmtpa (Exim 4.95) (envelope-from <zahedi@suigle.com>) id 1nlQ1q-00057w-Ks for mosfazli@gmail.com; Mon, 02
May 2022 02:59:30 -0400
MIME-Version: 1.0
Date: Mon, 02 May 2022 11:29:29 +0430
From: zahedi@suigle.com
To: Mostafa Fazli <mosfazli@gmail.com>
Subject: Re: درخواست شنید جهت تمرین طراحی نوشت
In-Reply-To: <CANnu_v1wZCT0F8Ajc+1+Lr0eo4FkZ1X+OKtPZhTfPqUxpc3Bww@mail.gmail.com>
References: <CANnu_v1wZCT0F8Ajc+1+Lr0eo4FkZ1X+OKtPZhTfPqUxpc3Bww@mail.gmail.com>
User-Agent: Roundcube Webmail/1.4.12
Message-ID: <74287fbfec75680e787d838bde6e7789@suigle.com>
X-Sender: zahedi@suigle.com
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - server205.webhostingbuzz.com
X-AntiAbuse: Original Domain - gmail.com
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
X-AntiAbuse: Sender Address Domain - suigle.com
X-Get-Message-Sender-Via: server205.webhostingbuzz.com: authenticated_id: zahedi@suigle.com
X-Authenticated-Sender: server205.webhostingbuzz.com: zahedi@suigle.com
X-Source:
X-Source-Args:
```

هنگامی که به بخش show original مراجعه کنیم، بخشی باز می شود که سرآیند یا هدری دارد که اطلاعاتی درباره آییی فرستنده و بخش ها و توضیحات دیگر همراه آن نوشته شده است.

همچنین میتوان با استفاده از سایت whois آی پی مورد نظر را رهگیری کرد.



سوال 10

برروي آدرس سايت دانشگاه دستور nslookup را با سوييچ مربوطه انجام داده و آدرس mail server آن را پيدا كنيد.
سپس آي پي آن و محل جغرافيايي آدرس سرور آن را پيدا كنيد.(اسكرين شات هاي هرمرحله را ضميمه كنيد).

C:\Windows\system32\cmd.exe

```
C:\Users\MosKn>nslookup -type=mx shahroodut.ac.ir
```

```
Server:  dns.google
```

```
Address:  8.8.8.8
```

```
Non-authoritative answer:
```

```
shahroodut.ac.ir      MX preference = 10, mail exchanger = mail.shahroodut.ac.ir
```

```
C:\Users\MosKn>
```

سپس با استفاده از سايت های رهگیری آيپی محل جغرافيايي آدرس سرور آن را پيدا می كنيم.

سوال 10

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.613]
(c) Microsoft Corporation. All rights reserved.

C:\Users\MosKn>nslookup mail.shahroodut.ac.ir
Server: UnKnown
Address: 192.168.255.191

Non-authoritative answer:
Name: mail.shahroodut.ac.ir
Address: 185.123.68.17

C:\Users\MosKn>
```

IP Details For: 185.123.68.17

Decimal:	3111863313
Hostname:	webmail.shahroodut.ac.ir. 17.68.123.185.in-addr.arpa domain name pointer mail.shahroodut.ac.ir
ASN:	5627
ISP:	Shahrood University
Services:	Likely mail server
Assignment:	Likely Static IP
Country:	Iran (Islamic Republic of)
State/Region:	Kermanshah
City:	Kermanshah

سوال 11

The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets, with packet 17 selected. The middle pane shows the details of the selected packet, which is a DNS query for 'shahroodut.ac.ir'. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1.178864		192.168.43.201	192.168.43.1	DNS	76	Standard query 0x8b73 A shahroodut.ac.ir
1.476807		192.168.43.1	192.168.43.201	DNS	92	Standard query response 0x8b73 A shahroodut.ac.ir A 85.185.67.248
1.481349		192.168.43.201	192.168.43.1	DNS	83	Standard query 0x8a99 A safebrowsing.google.com
1.547889		192.168.43.1	192.168.43.201	DNS	118	Standard query response 0x8a99 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.16.14
2.575271		192.168.43.201	192.168.43.1	DNS	72	Standard query 0x2f92 A a.unscart.in
2.673587		192.168.43.1	192.168.43.201	DNS	88	Standard query response 0x2f92 A a.unscart.in A 157.245.109.76

Details of packet 17 (DNS query):

- Ethernet II, Src: IntelCor_61:8f:b9 (34:cf:f6:61:8f:b9), Dst: XiaomiCo_13:43:1f (94:87:e0:13:43:1f)
- Internet Protocol Version 4, Src: 192.168.43.201, Dst: 192.168.43.1
- User Datagram Protocol, Src Port: 49635, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x8b73
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - shahroodut.ac.ir: type A, class IN

Raw packet data (hex and ASCII):

```
0000  94 87 e0 13 43 1f 34 cf f6 61 8f b9 08 00 45 00  ....C-4- .a....E-
0010  00 3e f3 ac 00 00 80 11 6e e7 c0 a8 2b c9 c0 a8  ->.....n...+...
0020  2b 01 c1 e3 00 35 00 2a df f4 8b 73 01 00 00 01  +----5.*...s...
0030  00 00 00 00 00 00 0a 73 68 61 68 72 6f 6f 64 75  ....ts hahroodu
0040  74 02 61 63 02 69 72 00 00 01 00 01  ....t-ac.ir....
```

مبدأ و مقصد آیی را با توجه به این روی پروتکل DNS قرار دارد، request and response را در این بخش پیدا میکنیم، اطلاعات مختلفی را در لایه های این بخش می توان یافت. برای مثال اینکه آخرین پکت ارسال شده است یا خیر، از طریق چه اینترنتی این پکت ارسال شده است و نوع کوئری و تبدیل آیی به نام و بالعکس آن را می توان در این قسمت مشاهده کرد.



سوال 12

خیر، با توجه به اینکه تعداد سایت هایی که رکورد آنها ذخیره میشود، با تعداد عکس هایی که نمایش داده می شود همخوانی ندارد، می توان این نتیجه را گرفت. همچنین با توجه به اینکه این بخش در خود chache ذخیره میکند.

همچنین میتوان تجربی و با آزمایش به این نتیجه دست یافت که تعداد پکت DNS های ارسالی متفاوت از تعداد عکس های موجود در یک سایت است.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
4.339422	192.168.43.201	192.168.43.1	DNS	72	Standard query 0x0f72 A a.unscart.in	
4.882462	192.168.43.201	192.168.43.1	DNS	76	Standard query 0x0ab3 A dns.msftncsi.com	
5.668142	192.168.43.201	192.168.43.1	DNS	82	Standard query 0xaf69 A client.wns.windows.com	
6.071694	192.168.43.201	192.168.43.1	DNS	95	Standard query 0x953e A optimizationguide-pa.googleapis.com	
6.075735	192.168.43.201	192.168.43.1	DNS	83	Standard query 0xeaca A safebrowsing.google.com	
6.084609	192.168.43.201	192.168.43.1	DNS	80	Standard query 0x723d A stu.shahroodut.ac.ir	
6.105646	192.168.43.201	192.168.43.1	DNS	82	Standard query 0xaf69 A client.wns.windows.com	
6.757369	192.168.43.1	192.168.43.201	DNS	111	Standard query response 0x953e A optimizationguide-pa.googleapis.com A 216.58.210.170	
6.769038	192.168.43.1	192.168.43.201	DNS	118	Standard query response 0xeaca A safebrowsing.google.com CNAME sb.l.google.com A 172.217.21.46	
6.775896	192.168.43.1	192.168.43.201	DNS	96	Standard query response 0x723d A stu.shahroodut.ac.ir A 85.185.67.201	
6.784329	192.168.43.1	192.168.43.201	DNS	92	Standard query response 0x0ab3 A dns.msftncsi.com A 131.107.255.255	
6.888171	192.168.43.201	192.168.43.1	DNS	86	Standard query 0x2c94 A mozilla.cloudflare-dns.com	
6.926322	192.168.43.1	192.168.43.201	DNS	88	Standard query response 0x0f72 A a.unscart.in A 157.245.109.76	
7.106517	192.168.43.201	192.168.43.1	DNS	82	Standard query 0xaf69 A client.wns.windows.com	
7.109773	192.168.43.1	192.168.43.201	DNS	141	Standard query response 0xaf69 A client.wns.windows.com CNAME wns.notify.trafficmanager.net A 20.199.120.182	
7.115497	192.168.43.1	192.168.43.201	DNS	141	Standard query response 0xaf69 A client.wns.windows.com CNAME wns.notify.trafficmanager.net A 20.199.120.182	
7.161113	192.168.43.1	192.168.43.201	DNS	118	Standard query response 0x2c94 A mozilla.cloudflare-dns.com A 104.16.248.249 A 104.16.249.249	
11.749559	192.168.43.201	192.168.43.1	DNS	74	Standard query 0x0ff0 A ogs.google.com	
12.187104	192.168.43.201	192.168.43.1	DNS	74	Standard query 0x0ff0 A ogs.google.com	
12.242534	192.168.43.201	192.168.43.1	DNS	82	Standard query 0x413b A client.wns.windows.com	
12.246788	192.168.43.1	192.168.43.201	DNS	141	Standard query response 0x413b A client.wns.windows.com CNAME wns.notify.trafficmanager.net A 20.199.120.182	

> Frame 5: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{5F40C480-567E-4EBC-B781-D232EB1111C0}, id 0

> Ethernet II, Src: IntelCor_61:8f:b9 (34:cf:f6:61:8f:b9), Dst: XiaomiCo_13:43:1f (94:87:e0:13:43:1f)

> Internet Protocol Version 4, Src: 192.168.43.201, Dst: 192.168.43.1

> User Datagram Protocol, Src Port: 52012, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x3427

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> v10.events.data.microsoft.com: type A, class IN

0000 94 87 e0 13 43 1f 34 cf f6 61 8f b9 08 00 45 00C-4-..a-...E-
0010 00 4b f4 64 00 00 80 11 6e 22 c0 a8 2b c9 00 a8 ..K.d....n":.+..
0020 0b 01 cb 2c 00 35 00 37 87 3a 34 27 01 00 00 01 ..,5-7-:4'.....
0030 00 00 00 00 00 00 03 76 31 30 06 65 76 65 74v 10 event
0040 73 04 64 61 74 61 09 6d 69 63 72 6f 73 6f 66 74 s data:m icrosoft
0050 03 63 6f 6d 00 00 01 00 01com.....

Text item (text), 35 bytes

Packets: 525 - Displayed: 38 (7.2%)

Profile: Default



Finish