

# کار با کاربردهای وب، DNS و سوکت

## سوال ۱

```
nic-hdl: ab590-irnic
person: alireza bagheri
e-mail: soft98.ir@gmail.com
address: Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR
phone: 0912 3549940
source: IRNIC # Filtered
```

- نام: علیرضا باقری
- آدرس holder domain: ایران - تهران - خیابان شریعتی - میرزاپور - مهر سوم غربی - پلاک ۲۰

## سوال ۲

```
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
```

## سوال ۳

### MX

این رکورد در واقع server mail ای را مشخص میکند که email های این دامنه را میپذیرد.

i	MX Records	Your Mail eXchanger (MX) records are:  0 soft98.ir. [TTL=14400]
---	------------	---

### NS

این نوع از رکورد ها یک دامنه را به authoritative DNS که دربردارنده ی اطلاعات آن دامنه است map میکنند . این رکورد قابلیت های مختلفی میتواند داشته باشد . ( نام در این رکورد ها domain و value همان hostname مربوط به server authoritative دامنه است)

i	NS records listed at parent servers	Nameserver records returned by the parent servers are:  ir1.hostdl.com. [NO GLUE] [TTL=1440] ir2.hostdl.com. [NO GLUE] [TTL=1440]  This information was kindly provided by a.nic.ir.
---	-------------------------------------	---

i	NS records at your local servers	NS records retrieved from your local nameservers were:  ir1.hostdl.com. [NO GLUE] [TTL=86400] ir2.hostdl.com. [NO GLUE] [TTL=86400]
---	----------------------------------	--

### A

این نوع از رکورد ها یک logical domain name را به IP address آن map میکند (name در این رکورد ها hostname و value همان IP address است).

i	WWW record	www.soft98.ir A records are:  www.soft98.ir. CNAME soft98.ir. [TTL=14400] soft98.ir. A 79.127.127.35 [TTL=14400]
---	------------	---

## TXT

این رکورد ها شامل اطلاعاتی به صورت متن برای سورس های خارج از دامنه هستند و استفاده های متعدد و مختلفی دارند.

سایت [viewdns.info](http://viewdns.info) در مورد این رکورد اطلاعاتی نداشت. در نتیجه برای بدست آوردن آن از سایت [mxtoolbox.com](http://mxtoolbox.com) استفاده کردیم:

Type	Domain Name	TTL	Record
TXT	soft98.ir	4 hrs	v=spf1 ip4:79.127.127.23 ip4:79.127.127.33 +a +mx +ip4:79.127.127.1/24 +ip4:185.120.222.1/24 +ip4:79.127.127.1/24 +ip4:185.120.222.1/24 +ip4:185.49.85.1/24 ~all

## سوال ۴

برای میل سرور به سراغ MX میرویم:

i	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
---	------------	--

که نشان میدهد میل سرور دانشگاه asg.aut.ac.ir میباشد.

برای آدرس IP به رکورد A نگاه میکنیم:

i	WWW record	www.aut.ac.ir A records are: www.aut.ac.ir. A 185.211.88.131 [TTL=3600]
---	------------	--

پس این آدرس برابر است با ۱۸۵.۲۱۱.۸۸.۱۳۱

## سوال ۵

Reverse IP results for farsnews.ir (178.22.78.1, 178.22.78.2, 178.22.78.3, 178.22.78.4)  
=====

Domain	Last Resolved Date
farsnews.com	2020-01-24
farsnews.ir	2021-04-24
farsnews.net	2020-01-24
farsnews.org	2020-01-24
fna.ir	2021-04-24

روی این دامنه ها ping میزنیم تا IP آنها را بدست آوریم:

```
C:\Users\Asus>ping farsnews.com
```

```
Pinging farsnews.com [178.22.78.1] with 32 bytes of data:
Reply from 178.22.78.1: bytes=32 time=26ms TTL=52
Reply from 178.22.78.1: bytes=32 time=25ms TTL=52
Reply from 178.22.78.1: bytes=32 time=26ms TTL=52
Reply from 178.22.78.1: bytes=32 time=25ms TTL=52
```

```
Ping statistics for 178.22.78.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 26ms, Average = 25ms
```

```
C:\Users\Asus>ping farsnews.ir
```

```
Pinging farsnews.ir [178.22.78.3] with 32 bytes of data:
Reply from 178.22.78.3: bytes=32 time=27ms TTL=52
Reply from 178.22.78.3: bytes=32 time=24ms TTL=52
Reply from 178.22.78.3: bytes=32 time=25ms TTL=52
Reply from 178.22.78.3: bytes=32 time=26ms TTL=52
```

```
Ping statistics for 178.22.78.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 27ms, Average = 25ms
```

```
C:\Users\Asus>ping farsnews.net
```

```
Ping request could not find host farsnews.net. Please check the name and try again.
```

```
C:\Users\Asus>ping farsnews.org
```

```
Ping request could not find host farsnews.org. Please check the name and try again.
```

```
C:\Users\Asus>ping fna.ir
```

```
Pinging fna.ir [178.22.78.1] with 32 bytes of data:
Reply from 178.22.78.1: bytes=32 time=25ms TTL=52
Reply from 178.22.78.1: bytes=32 time=39ms TTL=52
Reply from 178.22.78.1: bytes=32 time=25ms TTL=52
Reply from 178.22.78.1: bytes=32 time=26ms TTL=52
```

```
Ping statistics for 178.22.78.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 39ms, Average = 28ms
```

## سوال ۶

زمانی که ما برای وبسایتی درخواست میفرستیم ابتدا با استفاده از سلسله مراتب DNS ها (ابتدا درخواست به local dns server می رود و اگر IP درخواستی موجود نبود درخواست به DNS root server میرود و DNS root به ما TLD DNS server را که دامنه ی ما را شامل میشود میدهد و سپس TLD DNS server به ما آدرس authoritative server مناسب را میدهد تا از آن پرس و جو کنیم .)

آدرس وبسایت درخواستی ما در request packet موجود است و هر یک از DNS server ها جدول هایی دارند که دامنه های مختلف و یا سرور های یک دامنه ی خاص در آن ها موجود است بنابراین در هر دامنه وب سرور های مختلفی میتوانند وجود داشته باشند که وقتی درخواست

به آن سرور میرسد در آن table جستجو انجام شده و IP address آن سرور به دست می آید و میتوان این روش را به نوعی multiplexing به شمار آورد چرا که وب سایت های مختلفی در یک DNS میتوانند موجود باشند و DNS با جست و جوی table های خود یکی از IP address ها یا نام یک DNS server را برمیگرداند . پس زمانی که IP address آن سرور را داریم به نحوی مانند آن است که به سمت آن multiplexing کرده ایم.

## بررسی مورد چهار



### Trace DNS Delegation

Tracing DNS delegation for "aut.ac.ir":

```
Loading root server list (static data):
-> a.root-servers.net (198.41.0.4)
-> b.root-servers.net (192.228.79.201)
-> c.root-servers.net (192.33.4.12)
-> d.root-servers.net (128.8.10.90)
-> e.root-servers.net (192.203.230.10)
-> f.root-servers.net (192.5.5.241)
-> g.root-servers.net (192.112.36.4)
-> h.root-servers.net (128.63.2.53)
-> i.root-servers.net (192.36.148.17)
-> j.root-servers.net (192.58.128.30)
-> k.root-servers.net (193.0.14.129)
-> l.root-servers.net (199.7.83.42)
-> m.root-servers.net (202.12.27.33)
```

## سوال ۷

از دستور netstat -b استفاده میکنیم.

```
C:\WINDOWS\system32>netstat -b

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:7115           tonec:7116              ESTABLISHED
] Dropbox.exe[
TCP    127.0.0.1:7116           tonec:7115              ESTABLISHED
] Dropbox.exe[
TCP    127.0.0.1:7674           tonec:7675              ESTABLISHED
] Dropbox.exe[
TCP    127.0.0.1:7675           tonec:7674              ESTABLISHED
...
] SearchApp.exe[
TCP    192.168.1.3:9223         111.221.29.254:https    TIME_WAIT
```

## سوال ۸

از دستور netstat -n استفاده میکنیم.

C:\Users\Asus&gt;netstat -n

## Active Connections

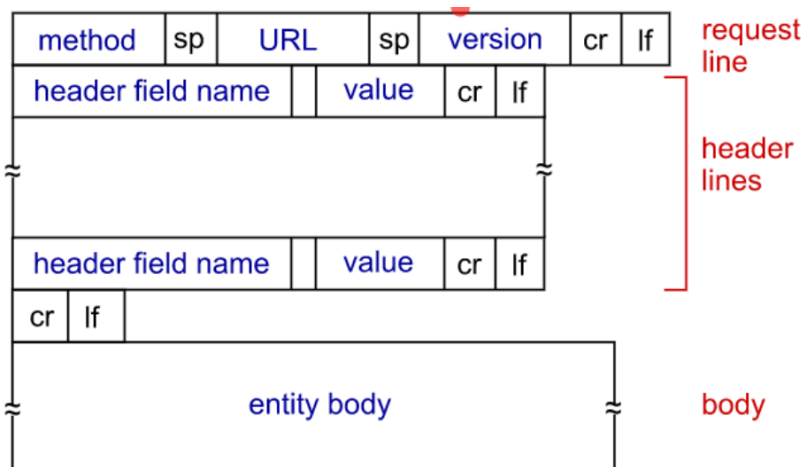
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:7115	127.0.0.1:7116	ESTABLISHED
TCP	127.0.0.1:7116	127.0.0.1:7115	ESTABLISHED
TCP	127.0.0.1:7674	127.0.0.1:7675	ESTABLISHED
TCP	127.0.0.1:7675	127.0.0.1:7674	ESTABLISHED
TCP	127.0.0.1:13737	127.0.0.1:13738	ESTABLISHED
TCP	127.0.0.1:13738	127.0.0.1:13737	ESTABLISHED
TCP	127.0.0.1:13739	127.0.0.1:13740	ESTABLISHED
TCP	127.0.0.1:13740	127.0.0.1:13739	ESTABLISHED
TCP	127.0.0.1:13741	127.0.0.1:13742	ESTABLISHED
TCP	127.0.0.1:13742	127.0.0.1:13741	ESTABLISHED
TCP	127.0.0.1:13745	127.0.0.1:13746	ESTABLISHED
TCP	127.0.0.1:13746	127.0.0.1:13745	ESTABLISHED
TCP	127.0.0.1:13754	127.0.0.1:13755	ESTABLISHED
TCP	127.0.0.1:13755	127.0.0.1:13754	ESTABLISHED
TCP	127.0.0.1:13837	127.0.0.1:13838	ESTABLISHED
TCP	127.0.0.1:13838	127.0.0.1:13837	ESTABLISHED
TCP	192.168.1.3:2006	95.101.14.38:443	ESTABLISHED
TCP	192.168.1.3:2090	18.221.82.221:443	ESTABLISHED
TCP	192.168.1.3:2119	18.221.82.221:443	ESTABLISHED
TCP	192.168.1.3:7270	64.233.167.188:5228	ESTABLISHED
TCP	192.168.1.3:7316	40.119.211.203:443	ESTABLISHED
TCP	192.168.1.3:7375	212.16.77.188:443	ESTABLISHED
TCP	192.168.1.3:8038	216.58.210.67:443	ESTABLISHED
TCP	192.168.1.3:8163	64.233.167.108:993	ESTABLISHED
TCP	192.168.1.3:8164	172.217.169.234:443	ESTABLISHED
TCP	192.168.1.3:8165	78.47.111.159:443	CLOSE_WAIT
TCP	192.168.1.3:8166	151.139.128.14:80	CLOSE_WAIT
TCP	192.168.1.3:8168	151.139.128.14:80	CLOSE_WAIT
TCP	192.168.1.3:8249	185.173.105.157:443	ESTABLISHED
TCP	192.168.1.3:8457	18.221.82.221:443	ESTABLISHED
TCP	192.168.1.3:8572	162.125.19.131:443	ESTABLISHED
TCP	192.168.1.3:8576	162.125.19.131:443	ESTABLISHED
TCP	192.168.1.3:8581	162.125.19.9:443	ESTABLISHED
TCP	192.168.1.3:8620	162.125.19.131:443	ESTABLISHED
TCP	192.168.1.3:8648	13.224.194.218:443	ESTABLISHED
TCP	192.168.1.3:8651	52.88.142.33:443	ESTABLISHED
TCP	192.168.1.3:8656	216.58.208.78:443	ESTABLISHED
TCP	192.168.1.3:8657	52.114.128.69:443	TIME_WAIT
TCP	192.168.1.3:8661	52.114.128.69:443	ESTABLISHED
TCP	192.168.1.3:8662	212.16.77.189:443	CLOSE_WAIT

برای مشاهده سایر پروتکل ها باید از netstat -an استفاده کنیم. برای این حالت قسمتی از ترمینال را نشان داده ایم:

TCP	192.168.1.3:9268	212.16.77.189:443	CLOSE_WAIT
TCP	192.168.1.3:9269	216.58.209.142:443	ESTABLISHED
TCP	192.168.1.3:9270	52.109.28.63:443	TIME_WAIT
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:1536	[::]:0	LISTENING
TCP	[::]:1537	[::]:0	LISTENING
TCP	[::]:1538	[::]:0	LISTENING
TCP	[::]:1539	[::]:0	LISTENING
TCP	[::]:1542	[::]:0	LISTENING
TCP	[::]:1771	[::]:0	LISTENING
TCP	[::]:5357	[::]:0	LISTENING
TCP	[::]:17500	[::]:0	LISTENING
TCP	[::1]:1541	[::]:0	LISTENING
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:3702	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	

## سوال ۹

علت وارد کردن دو enter آن است که زمانی که ارتباط TCP باز میکنیم میتوانیم پشت هم درخواست بفرستیم و این درخواست ها ممکن است چند خطی باشند. بنابراین باید تمایزی میان رفتن به خط بعدی و رفتن به درخواست بعدی وجود داشته باشد.



بنابراین یک enter به معنای رفتن به خط بعدی است این در حالی است که دو enter به معنای پایان درخواست فعلی و ارسال آن و رفتن به درخواست بعدی است.

## سوال ۱۰

```
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Sun, 25 Apr 2021 07:12:47 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
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>
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>
</body></html>
```

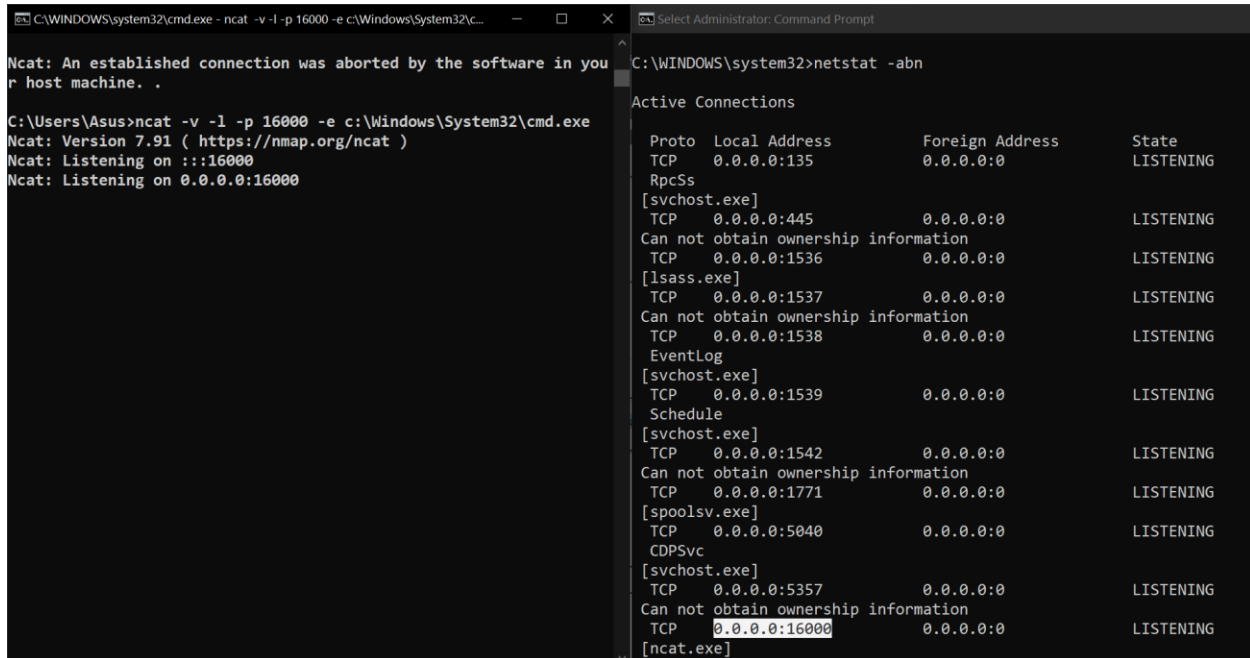
حال از طریق مرورگر امتحان میکنیم و در وایرشارک capture میکنیم:

433	13.727284	192.168.1.3	185.211.88.131	HTTP	1114 GET / HTTP/1.1
437	13.769716	185.211.88.131	192.168.1.3	HTTP	528 HTTP/1.1 301 Moved Permanently (text/html)

## سوال ۱۱

بله زیرا تا زمانی که **ctrl+c** را نزده ایم ارتباط برقرار می ماند و الزم است برای هر درخواست ارتباط را دوباره باز کنیم

## سوال ۱۲



```

C:\WINDOWS\system32\cmd.exe - ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: An established connection was aborted by the software in your host machine.

C:\Users\Asus>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000

C:\WINDOWS\system32>netstat -abn

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
RpcSs
[svchost.exe]
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
Can not obtain ownership information
TCP    0.0.0.0:1536             0.0.0.0:0               LISTENING
[lsass.exe]
TCP    0.0.0.0:1537             0.0.0.0:0               LISTENING
Can not obtain ownership information
TCP    0.0.0.0:1538             0.0.0.0:0               LISTENING
EventLog
[svchost.exe]
TCP    0.0.0.0:1539             0.0.0.0:0               LISTENING
Schedule
[svchost.exe]
TCP    0.0.0.0:1542             0.0.0.0:0               LISTENING
Can not obtain ownership information
TCP    0.0.0.0:1771             0.0.0.0:0               LISTENING
[spoolsv.exe]
TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING
CDPSvc
[svchost.exe]
TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING
Can not obtain ownership information
TCP    0.0.0.0:16000            0.0.0.0:0               LISTENING
[ncat.exe]

```

این port همانطور که در شکل مشاهده میشود به پورت ۰.۰.۰.۰ ، bind شده است.



```

C:\WINDOWS\system32\cmd.exe - ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: An established connection was aborted by the software in your host machine.

C:\Users\Asus>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
Ncat: Connection from 192.168.1.3.
Ncat: Connection from 192.168.1.3:9510.

C:\Users\Asus>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 4:

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

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2dd7:ef8b:8a22:36cd%22
    IPv4 Address. . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\Asus>ncat 192.168.1.3 16000
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asus>

```

سوال ۱۳

```

C:\WINDOWS\system32\cmd.exe
C:\Users\Asus>ncat -l -p 4444 < index.html
GET / HTTP/1.1
Host: 127.0.0.1:4444
Connection: keep-alive
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,fa;q=0.8

C:\Users\Asus>

```

```

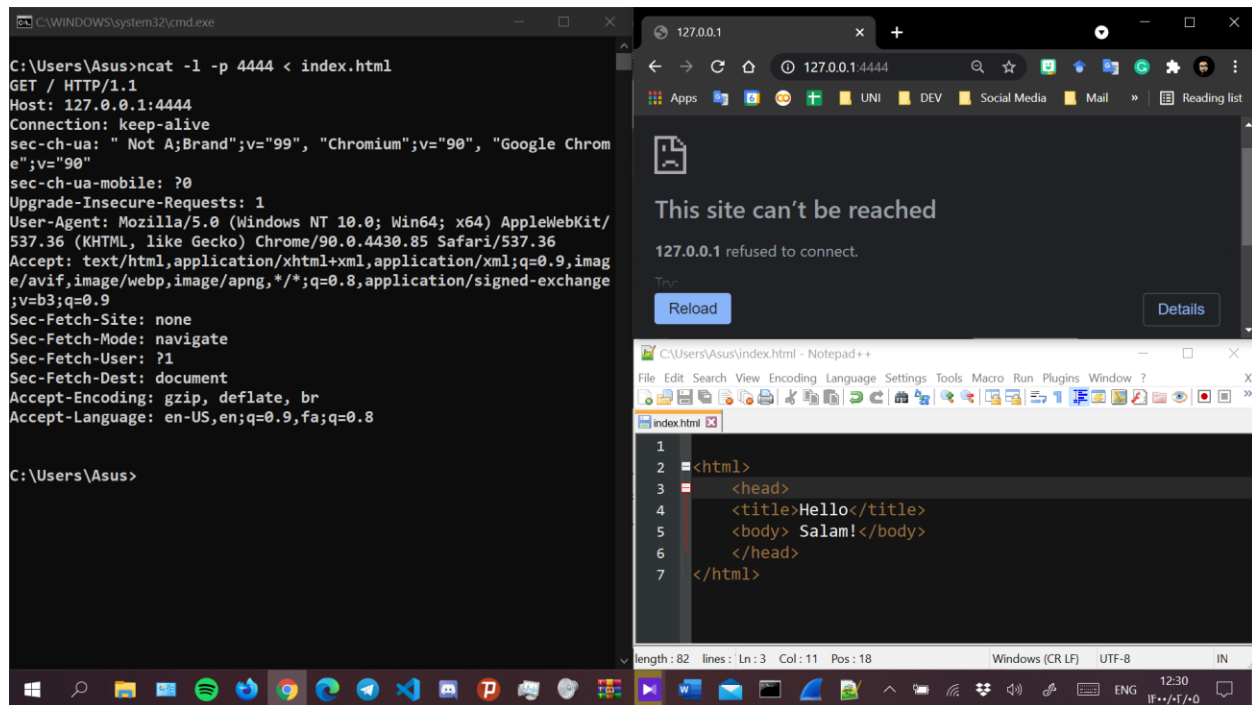
Hello
Salam!

```

```

C:\Users\Asus\index.html - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index.html
1 HTTP/1.1 200 OK
2
3 <html>
4   <head>
5     <title>Hello</title>
6   <body> Salam!</body>
7   </head>
8 </html>

```



اگر یک فایل دیگر بدون خط اول بسازیم و امتحان کنیم صفحه بالا نمی آید چرا که این خط به معنای وضعیت موفقیت آمیز در HTTP response است و در واقع در فایل باید چنین خطی موجود باشد که در هنگام پاسخ به درخواست اعالم کند که درخواست موفقیت آمیز بوده است و شی درخواست شده در ادامه ی پاسخ آمده است . اما اگر این خط نباشد سیستم درخواست دهنده متوجه نمیشود که شی درخواستی اش با موفقیت رسیده تا آن را دریافت کند و خطا دریافت میکنیم.

## سوال ۱۴

## سوال ۱۵

## سوال ۱۶