

شبکه‌های کامپیوتری

تمرین اول عملی

نام دانشجو: آرش یادگاری

شماره دانشجویی: ۹۹۱۰۵۸۱۵

سوال ۱:

بخش اول

۱. با استفاده از دستور زیر client تلنت را بر روی سیستم خود نصب می‌کنیم.

```
$sudo apt install telnet
```

۲. با استفاده از دستور زیر با استفاده از کاربر telnet به دامنه telehack.com و بر روی پورت ۲۳ متصل می‌شویم. (دقت شود که ممکن است این پورت اشغال باشد و در نتیجه port forwarding رخ دهد)

```
$telnet -l telnet telehack.com 23
```

```
Trying 64.13.139.230...
Connected to telehack.com.
Escape character is '^J'.

Connected to TELEHACK port 151

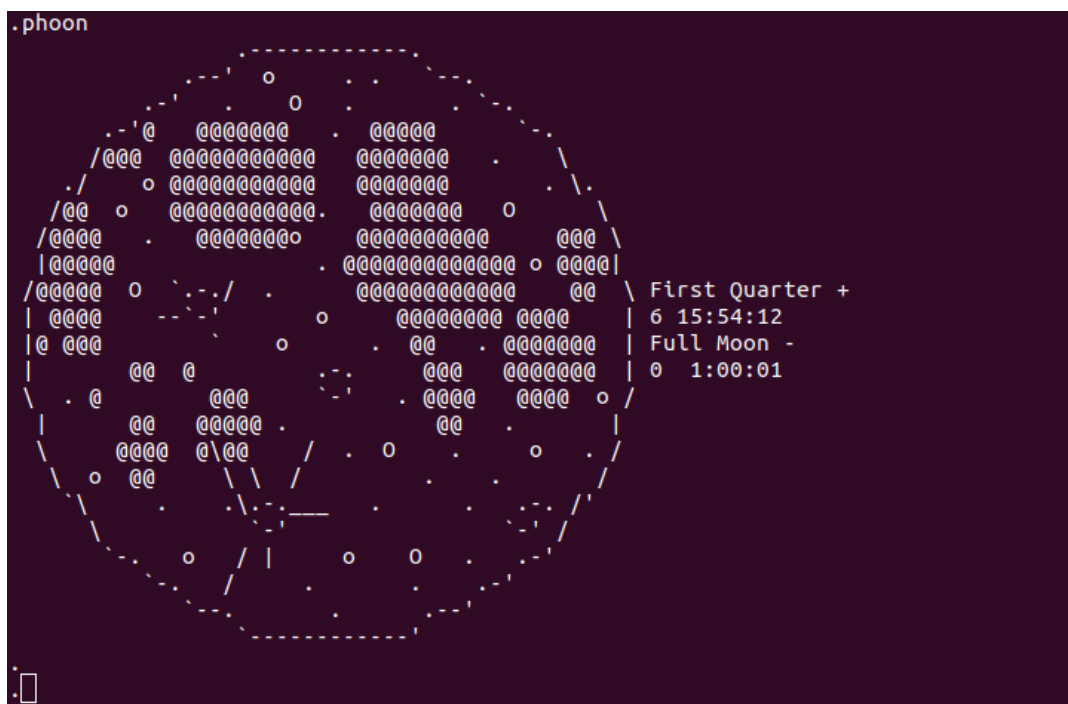
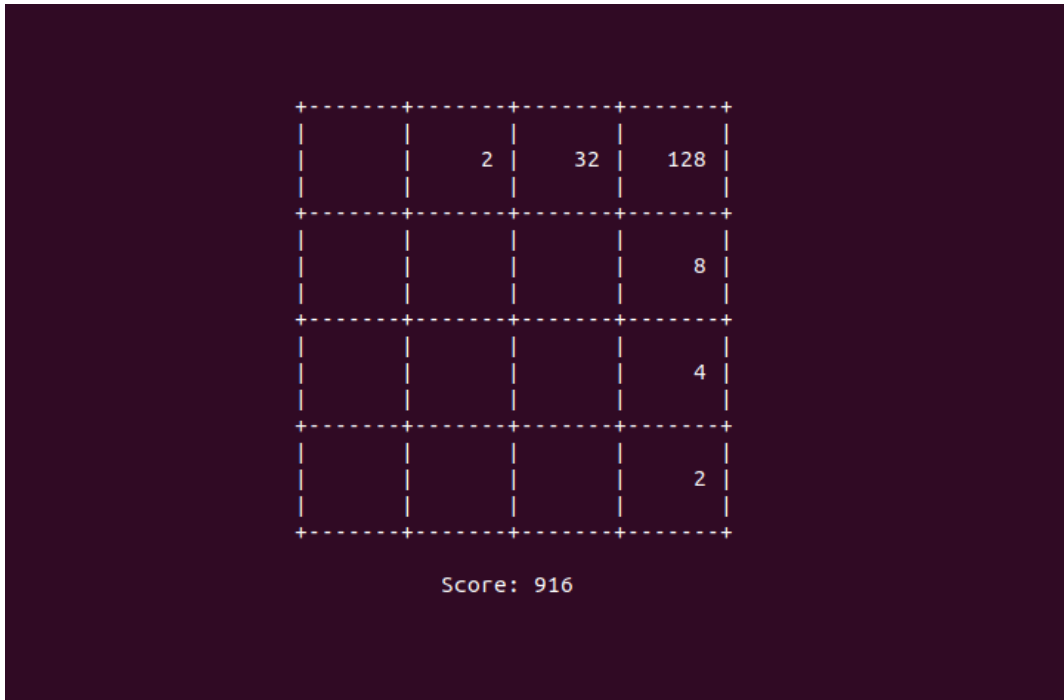
It is 11:59 am on Saturday, October 28, 2023 in Mountain View, California, USA.
There are 112 local users. There are 26647 hosts on the network.

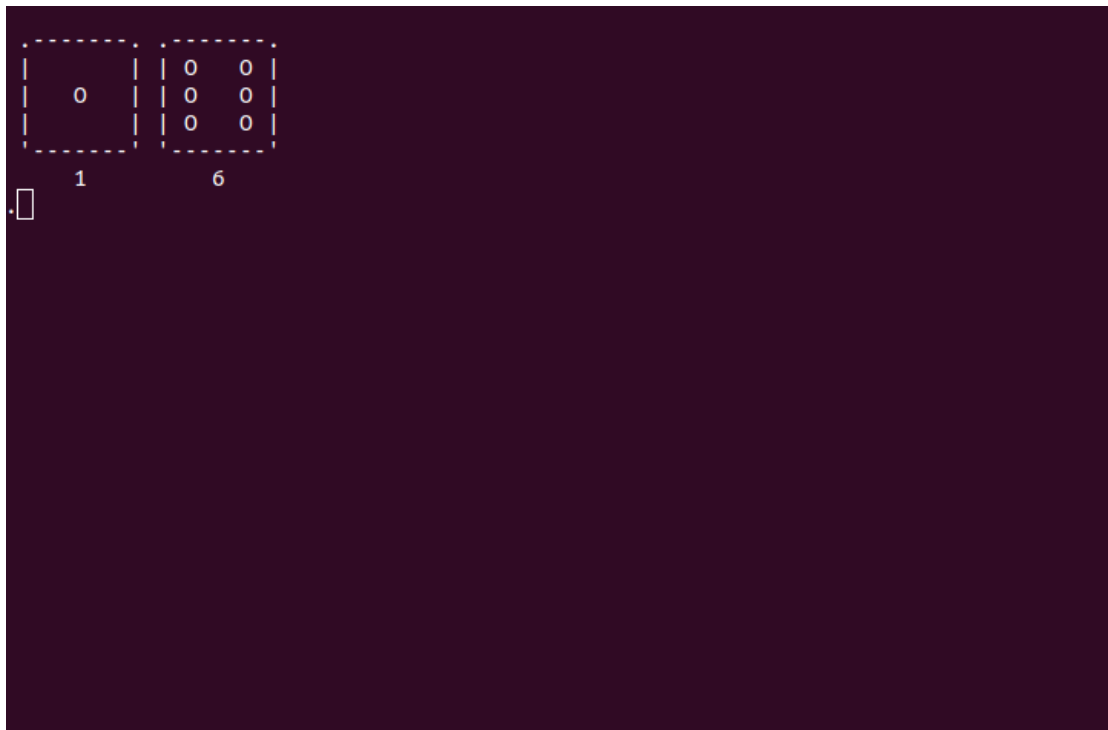
May the command line live forever.

Command, one of the following:
2048      ac      advent  aquarium  bf      c8
calc      callsign  ching   clear     clock   cowsay
date      dir      echo    eliza     exit    factor
file      fnord    geoip   gif        ipaddr  liff
login     md5      more    morse     netstat newuser
notes     octopus  phoon   pig        ping    primes
privacy   qr       rain    rand       rig     rockets
roll      rot13    run     salvo      sleep   starwars
sudoku    tail     traceroute typespeed  units   usenet
users     uumap    uupath  uuplot     weather zc

More commands available after login. Type HELP for a detailed command list.
Type NEWUSER to create an account. Press control-C to interrupt any command.
.exitConnection closed by foreign host.
```

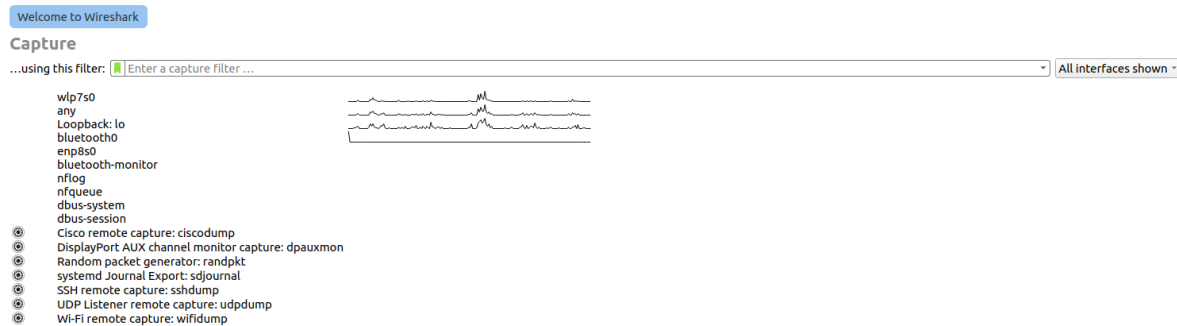
۳. به طور مثال بازی ۲۰۴۸, roll و phoon را اجرا می‌کنیم.





بخش دوم

۱. ابتدا با استفاده از پنجره capture بر روی interface مدنظر، پکت‌ها را ضبط می‌کنیم. (در اینجا wlp7s0)



سپس کامند تلنت را زده و در فیلتر telnet را جستجو می‌کنیم.

telnet						
No.	Time	Source	Destination	Protocol	Length	Info
1059	95.639859405	64.13.139.230	192.168.100.179	TELNET	69	Telnet Data ...
1061	95.640053533	192.168.100.179	64.13.139.230	TELNET	69	Telnet Data ...
1066	95.968415610	64.13.139.230	192.168.100.179	TELNET	335	Telnet Data ...
1068	95.968509118	192.168.100.179	64.13.139.230	TELNET	93	Telnet Data ...
1069	96.272014882	64.13.139.230	192.168.100.179	TELNET	963	Telnet Data ...
1074	96.599394961	64.13.139.230	192.168.100.179	TELNET	80	Telnet Data ...
1076	96.599577300	192.168.100.179	64.13.139.230	TELNET	92	Telnet Data ...
1097	106.487085924	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1099	106.827719730	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1100	106.827678419	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1102	107.339551895	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1109	108.295361781	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1111	108.587446843	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1114	108.809651363	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1115	108.875054195	64.13.139.230	192.168.100.179	TELNET	69	Telnet Data ...
1119	109.276076218	64.13.139.230	192.168.100.179	TELNET	70	Telnet Data ...
1122	109.550934549	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1135	112.921428631	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1141	113.457186351	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1142	113.457145235	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1144	113.870868508	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1150	114.510178434	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1152	114.900958819	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1168	116.865298793	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...

۲. از آنجا که telnet رمزنگاری نشده است، دیتاهای پکت به صورت plain text قابل مشاهده می‌باشد. همچنین هدر شامل آی‌پی، اترنت و همچنین یک هدر TCP می‌باشد که بر روی port ۲۳ گوش می‌ایستد.

۳.

۴. همانطور که قبل تر مشخص شد، داده‌های پکت‌ها رمزنگاری نشده است در نتیجه ارسال اطلاعات از طریق این پروتکل به راحتی قابل ردیابی و مشاهده است. با توجه به قدیمی بودن این پروتکل، در بسیاری از سیستم‌ها از آن استفاده شده است. برای ارتباطاتی که نیاز به سرعت دارد و اورهد کمی مدنظر هست، این پروتکل مناسب است (local area network)

۵. تفاوت‌های اصلی:

(A) رمزنگاری داده

(B) بدون نیاز به احراز هویت

۶. یک نکته جالبی که دیدم این بود که اولین پکتی که از طریق این پروتکل فرستاده شده توسط سرور telehack هست و نه سیستم من که عجیب بنظر رسید. در نتیجه تمام ip‌هایی که مقصد آنها telehack هست را فیلتر کردم و مشاهده کردم که قبل از ارسال داده‌ها از طریق telnet، یک handshake با استفاده از پروتکل TCP انجام می‌گیرد و سپس چند پکت اول (در اینجا ۲) برای ست کردن یک سری option ارسال شده و پکت‌های بعدی نیز درخواست‌ها و پاسخ‌ها می‌باشد.

No.	Time	Source	Destination	Protocol	Length	Info
1051	95.058814242	192.168.100.179	64.13.139.230	TCP	74	55290 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1310162547 TSecr=0 WS=128
1057	95.349344954	64.13.139.230	192.168.100.179	TCP	74	23 → 55290 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1392 SACK_PERM TSval=13079911749 TSecr=1310162547 WS=128
1058	95.349405410	192.168.100.179	64.13.139.230	TCP	66	55290 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1310162837 TSecr=3979911749
1059	95.639859405	64.13.139.230	192.168.100.179	TELNET	69	Telnet Data ...
1060	95.639904110	192.168.100.179	64.13.139.230	TCP	66	55290 → 23 [ACK] Seq=1 Ack=4 Win=64256 Len=0 TSval=1310163128 TSecr=3979912041
1061	95.640053533	192.168.100.179	64.13.139.230	TELNET	69	Telnet Data ...
1066	95.968415610	64.13.139.230	192.168.100.179	TELNET	335	Telnet Data ...
1067	95.968415697	64.13.139.230	192.168.100.179	TCP	66	[TCP Dup ACK 1066#1] 23 → 55290 [ACK] Seq=273 Ack=4 Win=65280 Len=0 TSval=3979912359 TSecr=1310163128
1068	95.968509118	192.168.100.179	64.13.139.230	TELNET	93	Telnet Data ...
1069	95.272614082	64.13.139.230	192.168.100.179	TELNET	963	Telnet Data ...
1070	95.312601234	192.168.100.179	64.13.139.230	TCP	66	55290 → 23 [ACK] Seq=31 Ack=1170 Win=64128 Len=0 TSval=1310163801 TSecr=3979912656
1074	95.599394961	64.13.139.230	192.168.100.179	TELNET	80	Telnet Data ...
1075	95.599444163	192.168.100.179	64.13.139.230	TCP	66	55290 → 23 [ACK] Seq=31 Ack=1184 Win=64128 Len=0 TSval=1310164087 TSecr=3979913002
1076	95.599577390	192.168.100.179	64.13.139.230	TELNET	92	Telnet Data ...
1077	95.939194800	64.13.139.230	192.168.100.179	TCP	66	23 → 55290 [ACK] Seq=1184 Ack=57 Win=65280 Len=0 TSval=3979913329 TSecr=1310164088
1097	106.487085924	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1098	106.827078990	64.13.139.230	192.168.100.179	TCP	66	23 → 55290 [ACK] Seq=1184 Ack=58 Win=65280 Len=0 TSval=3979923175 TSecr=1310173975
1099	106.827719730	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1100	106.827678419	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1101	106.868695789	192.168.100.179	64.13.139.230	TCP	66	55290 → 23 [ACK] Seq=59 Ack=1185 Win=64128 Len=0 TSval=1310174357 TSecr=3979923176
1102	107.339551895	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...
1103	107.339592406	192.168.100.179	64.13.139.230	TCP	66	55290 → 23 [ACK] Seq=59 Ack=1186 Win=64128 Len=0 TSval=1310174828 TSecr=3979923556
1109	108.295361781	192.168.100.179	64.13.139.230	TELNET	67	Telnet Data ...
1111	108.587446843	64.13.139.230	192.168.100.179	TELNET	67	Telnet Data ...

سوال ۲

بخش اول

۱. کافی است دستور داده شده را در ترمینال اجرا کنیم تا خروجی زیر را مشاهده کنیم.

```
curl -v info.cern.ch
* Trying 188.184.100.182:80...
* Trying 2001:1458:d00:35::100:222:80...
* Immediate connect fail for 2001:1458:d00:35::100:222: Network is unreachable
* Connected to info.cern.ch (188.184.100.182) port 80 (#0)
> GET / HTTP/1.1
> Host: info.cern.ch
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 30 Oct 2023 09:00:10 GMT
< Server: Apache
< Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT
< ETag: "286-4f1aadb3105c0"
< Accept-Ranges: bytes
< Content-Length: 646
< Connection: close
< Content-Type: text/html
<
<html><head></head><body><header>
<title>http://info.cern.ch</title>
</header>

<h1>http://info.cern.ch - home of the first website</h1>
<p>From here you can:</p>
```

```

<ul>
<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the
first website</a></li>
<li><a
href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse
the first website using the line-mode browser simulator</a></li>
<li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the
birth of the web</a></li>
<li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics
laboratory where the web was born</a></li>
</ul>
</body></html>
* Closing connection 0

```

همانطور که مشاهده می‌کنید از پروتکل HTTP با ورژن ۱.۱ استفاده شده است. همچنین آدرس و پورت مقصد برابر است با 188.184.100.182:80 می‌باشد. همچنین اطلاعاتی مانند دامنه و همچنین ورژنی با توجه به نوع سیستم عامل و دیگر مشخصات درخواست کننده تعیین می‌شود.

در پاسخ کد ۲۰۰ ارسال شده است که به معنی آن است که درخواست به درستی پاسخ داده شده است. در ادامه تگ‌هایی مثل تاریخ، سایز، نوع اتصال و ... آمده است و در انتها فایل html به صورت استرینگ نمایش داده شده است.

۲. پکت‌های ارسالی با استفاده از wireshark و اعمال فیلتر پورت ۸۰ (HTTP default) به این صورت می‌باشد.

1779...	2077.5440149...	172.17.103.161	188.184.100.182	TCP	74	54854 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=559567189 TSecr=0 WS=128
1779...	2077.8479305...	188.184.100.182	172.17.103.161	TCP	74	80 → 54854 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=3923028431 TSecr=559567189 WS=128
1779...	2077.8479846...	172.17.103.161	188.184.100.182	TCP	66	54854 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=559567493 TSecr=3923028431
1779...	2077.8481660...	172.17.103.161	188.184.100.182	HTTP	142	GET / HTTP/1.1
1779...	2077.9504438...	188.184.100.182	172.17.103.161	TCP	66	80 → 54854 [ACK] Seq=1 Ack=77 Win=29056 Len=0 TSval=3923028737 TSecr=559567493
1779...	2077.9536511...	188.184.100.182	172.17.103.161	HTTP	944	HTTP/1.1 200 OK (text/html)
1779...	2077.9536514...	188.184.100.182	172.17.103.161	TCP	66	80 → 54854 [FIN, ACK] Seq=879 Ack=77 Win=29056 Len=0 TSval=3923028738 TSecr=559567493
1779...	2077.9536961...	172.17.103.161	188.184.100.182	TCP	66	54854 → 80 [ACK] Seq=77 Ack=879 Win=64128 Len=0 TSval=559567599 TSecr=3923028738
1779...	2077.9540826...	172.17.103.161	188.184.100.182	TCP	66	54854 → 80 [FIN, ACK] Seq=77 Ack=880 Win=64128 Len=0 TSval=559567599 TSecr=3923028738
1779...	2078.0526308...	188.184.100.182	172.17.103.161	TCP	66	80 → 54854 [ACK] Seq=880 Ack=78 Win=29056 Len=0 TSval=3923028841 TSecr=559567599

همانطور که مشخص است پس از عمل handshake، درخواست HTTP get برای دریافت ارسال شده است و سپس در پاسخ نیز داده‌ها ارسال شده است.

۳. در قسمت data پکت ارسال شده با HTTP مشاهده می‌شود که داده‌ها به صورت text و بدون encryption ارسال شده‌اند در نتیجه امنیتی پایینی داشته و به طور مثال برای خرید از یک فروشگاه آنلاین بسیار خطرناک است چرا که رمز کارت‌های شما ممکن است افشا شود.

```

▼ Line-based text data: text/html (13 lines)
<html><head></head><body><header>\n
<title>http://info.cern.ch</title>\n
</header>\n
\n
<h1>http://info.cern.ch - home of the first website</h1>\n
<p>From here you can:</p>\n
<ul>\n
<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first website</a></li>\n
<li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the first website u:
<li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the web</a></li>\n
<li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory where the web \
</ul>\n
</body></html>\n

```

بخش دوم

دستورات زیر را در ترمینال اجرا می‌کنیم.

```

$nc -v www.example.com 80
Connection to www.example.com (93.184.216.34) 80 port [tcp/http] succeeded!
GET / HTTP/1.1
host: example.com

```

در پاسخ، صفحه html ارسال می‌شود

```

HTTP/1.1 200 OK
Age: 282575
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Mon, 30 Oct 2023 10:56:58 GMT
Etag: "3147526947+ident"
Expires: Mon, 06 Nov 2023 10:56:58 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (dcb/7F3C)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256

<!doctype html>
<html>
<head>
  <title>Example Domain</title>

```

```
<meta charset="utf-8" />
<meta http-equiv="Content-type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<style type="text/css">
body {
    background-color: #f0f0f2;
    margin: 0;
    padding: 0;
    font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe
UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
}
div {
    width: 600px;
    margin: 5em auto;
    padding: 2em;
    background-color: #fdfdff;
    border-radius: 0.5em;
    box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
}
a:link, a:visited {
    color: #38488f;
    text-decoration: none;
}
@media (max-width: 700px) {
    div {
        margin: 0 auto;
        width: auto;
    }
}
</style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You
may use this
    domain in literature without prior coordination or asking for
    permission.</p>
    <p><a href="https://www.iana.org/domains/example">More
    information...</a></p>
```



```
</div>
</body>
</html>
```

بخش سوم

۱. با استفاده از این دستور curl در ترمینال، یک درخواست HTTPS به www.github.com ارسال می‌کنیم.

همچنین packet ها را در wireshark ضبط می‌کنیم.

No.	Time	Source	Destination	Protocol	Length	Info
271	7.763839292	172.27.52.174	140.82.121.4	TCP	74	40020 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2833516378 TSecr=0 WS=128
273	7.996173983	140.82.121.4	172.27.52.174	TCP	74	443 → 40020 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM TSval=2755866655 TSecr=2833516378 WS=1924
274	7.996243229	172.27.52.174	140.82.121.4	TCP	66	40020 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2833516591 TSecr=2755866655
275	8.084596629	172.27.52.174	140.82.121.4	TLSPv1.3	583	Client Hello
284	8.609733284	140.82.121.4	172.27.52.174	TLSPv1.3	2880	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
285	8.609795375	172.27.52.174	140.82.121.4	TCP	66	40020 → 443 [ACK] Seq=518 Ack=2815 Win=62976 Len=0 TSval=2833517284 TSecr=2755867259
286	8.610165534	172.27.52.174	140.82.121.4	TLSPv1.3	130	Change Cipher Spec, Application Data
287	8.610227570	172.27.52.174	140.82.121.4	TLSPv1.3	161	Application Data, Application Data
288	8.661477398	172.27.52.174	140.82.121.4	TLSPv1.3	159	Application Data, Application Data
289	9.197946770	172.27.52.174	140.82.121.4	TCP	159	[TCP Retransmission] 40020 → 443 [PSH, ACK] Seq=677 Ack=2815 Win=64128 Len=93 TSval=2833517792 TSecr=2755867259
305	9.224901924	140.82.121.4	172.27.52.174	TLSPv1.3	145	Application Data
306	9.224902229	140.82.121.4	172.27.52.174	TLSPv1.3	145	Application Data
307	9.224902329	140.82.121.4	172.27.52.174	TLSPv1.3	130	Application Data
308	9.224902411	140.82.121.4	172.27.52.174	TLSPv1.3	3760	Application Data, Application Data, Application Data
309	9.224902493	140.82.121.4	172.27.52.174	TLSPv1.3	5762	Application Data, Application Data, Application Data, Application Data
310	9.225104868	172.27.52.174	140.82.121.4	TCP	66	40020 → 443 [ACK] Seq=770 Ack=12427 Win=54528 Len=0 TSval=2833517820 TSecr=2755867845
311	9.225450834	172.27.52.174	140.82.121.4	TLSPv1.3	97	Application Data
312	9.318950517	140.82.121.4	172.27.52.174	TCP	78	[TCP Dup ACK 305#1] 443 → 40020 [ACK] Seq=12427 Ack=770 Win=67584 Len=0 TSval=2755868089 TSecr=2833517792 SLE=677 SRE=770
313	9.337471444	140.82.121.4	172.27.52.174	TLSPv1.3	1490	Application Data
314	9.337944926	140.82.121.4	172.27.52.174	TLSPv1.3	4338	Application Data, Application Data, Application Data
315	9.337987465	172.27.52.174	140.82.121.4	TCP	66	40020 → 443 [ACK] Seq=801 Ack=18123 Win=61696 Len=0 TSval=2833517933 TSecr=2755868086
316	9.348817295	140.82.121.4	172.27.52.174	TLSPv1.3	7186	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
317	9.349007258	140.82.121.4	172.27.52.174	TLSPv1.3	1490	Application Data

۲. چند پکت اول و پکت hello client که در آن server name آورده شده است رمزنگاری نشده‌اند. علت آن است

که رمزنگاری که انجام می‌شود بسته به certifiacte ای است که توسط origin server به سمت کاربر ارسال می‌شود. کاربر با استفاده از public key موجود در این certificate درخواست خود را ارسال می‌کند و با استفاده از کلید اختصاصی این درخواست رمزگشایی می‌شود. تا زمانی که مشخص نباشد که کاربر به چه سروری قصد ارسال و دریافت داده دارد، رمزنگاری TLS/SSL امکان پذیر نمی‌باشد.

۳. از آنجا که origin server ممکن است چندین دامنه مختلف را پوشش دهد، ارسال IP به تنهایی کافی نمی‌باشد و ممکن است SSL/TLS certificate اشتباهی ارسال شود و ارتباط را قطع کند. در نتیجه در مرحله handshake، دامنه نیز ارسال می‌شود.

۵. از آنجا که https از پروتکل TLS استفاده می‌کند، کاربر می‌تواند از صحت certificate اطمینان حاصل کند و همچنین اطلاعات آن با استفاده از public key رمزنگاری می‌شود و برخلاف http در صورت نداشتن private key غیرقابل رمزگشایی است.

سوال ۳

۱. خروجی زیر در ترمینال مشاهده می‌شود

```
halfblood@Halfblood:~$ dig -t NS ce.sharif.edu +noall +answer
ce.sharif.edu.      60      IN      NS      ns1.sharif.ir.
ce.sharif.edu.      60      IN      NS      ns2.sharif.ir.
```

دستور dig، یک کامند DNS Lookup می‌باشد خروجی‌های این دستور، name server هایی هستند که در صورتی که دامنه مورد جستجو شامل ce.sharif.edu باشد به آنها جهت برگرداندن اطلاعاتی مانند IP مراجعه می‌شود. NS نشان‌دهنده نوع سرورهاست (name server) و IN نیز نوع کلس داده‌های ذخیره شده در این سرورهاست. دو عدد آمده نیز TTL هستند.

۲.

```
halfblood@Halfblood:~$ dig ce.sharif.edu MX +noall +answer
ce.sharif.edu.      60      IN      MX      5 mx1.sharif.ir.
ce.sharif.edu.      60      IN      MX      5 mx2.sharif.ir.
```

مشخصات سرورهایی که مسئول دریافت و انتقال ایمیل هستند را نشان می‌دهد. MX نشان‌گر mail exchanger می‌باشد، مقدار ۵ نشان‌دهنده اولویت می‌باشد باقی موارد مشابه قسمت قبل است.

سوال ۴

بخش اول

کافی است فایل باینری را دانلود کنیم. و با دستور زیر یک پروکسی لوکال ایجاد کنیم.

```
$/gost -L=:8080
```

بخش دوم

تصویر لاگ و wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	33134 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=2589941584 TSecr=0 WS=128
2	0.000000328	127.0.0.1	127.0.0.1	TCP	74	8080 → 33134 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65486 SACK_PERM TSval=2589941584 TSecr=2589941584 WS=128
3	0.000014321	127.0.0.1	127.0.0.1	TCP	60	33134 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2589941584 TSecr=2589941584
4	0.000058123	127.0.0.1	127.0.0.1	HTTP	187	GET http://sharif.edu/ HTTP/1.1
5	0.000060256	127.0.0.1	127.0.0.1	TCP	60	8080 → 33134 [ACK] Seq=1 Ack=122 Win=65488 Len=0 TSval=2589941584 TSecr=2589941584
6	0.000069708	127.0.0.1	127.0.0.1	DNS	81	Standard query 0x2458 AAAA sharif.edu OPT
7	0.000440535	127.0.0.1	127.0.0.53	DNS	81	Standard query 0x3c1c A sharif.edu OPT
8	0.029725887	127.0.0.53	127.0.0.1	DNS	97	Standard query response 0x3c1c A sharif.edu A 152.89.13.54 OPT
9	0.271819507	127.0.0.53	127.0.0.1	DNS	141	Standard query response 0x2458 AAAA sharif.edu SOA ns1.sharif.ir OPT
10	0.285490803	127.0.0.1	127.0.0.1	HTTP	569	HTTP/1.1 301 Moved Permanently (text/html)
11	0.285518767	127.0.0.1	127.0.0.1	TCP	66	33134 → 8080 [ACK] Seq=122 Ack=504 Win=65152 Len=0 TSval=2589941869 TSecr=2589941869
12	0.285858118	127.0.0.1	127.0.0.1	TCP	66	33134 → 8080 [FIN, ACK] Seq=122 Ack=504 Win=65536 Len=0 TSval=2589941870 TSecr=2589941869
13	0.286227561	127.0.0.1	127.0.0.1	TCP	66	8080 → 33134 [FIN, ACK] Seq=504 Ack=123 Win=65536 Len=0 TSval=2589941870 TSecr=2589941870
14	0.286266021	127.0.0.1	127.0.0.1	TCP	66	33134 → 8080 [ACK] Seq=123 Ack=505 Win=65536 Len=0 TSval=2589941870 TSecr=2589941870

```

halfblood@Halfblood:~/gost/gost-linux-amd64-2.11.5$ ./gost-linux-amd64 -L=:8080
2023/10/31 22:00:43 route.go:695: auto://:8080 on [::]:8080
2023/10/31 22:00:56 http.go:161: [http] 127.0.0.1:58110 -> auto://:8080 -> www.example.com:80
2023/10/31 22:00:56 http.go:256: [route] 127.0.0.1:58110 -> auto://:8080 -> www.example.com:80
2023/10/31 22:00:56 http.go:311: [http] 127.0.0.1:58110 <-> www.example.com:80
2023/10/31 22:00:57 http.go:313: [http] 127.0.0.1:58110 >-< www.example.com:80
2023/10/31 22:04:03 http.go:161: [http] 127.0.0.1:33134 -> auto://:8080 -> sharif.edu:80
2023/10/31 22:04:03 http.go:256: [route] 127.0.0.1:33134 -> auto://:8080 -> sharif.edu:80
2023/10/31 22:04:04 http.go:311: [http] 127.0.0.1:33134 <-> sharif.edu:80
2023/10/31 22:04:04 http.go:313: [http] 127.0.0.1:33134 >-< sharif.edu:80

```

ابتدا یک handshake بین پورت ۸۰۸۰ (پروکسی) و یک پورت لوکال رندوم (در اینجا 33134) اتفاق می‌افتد و سپس درخواست‌های 33134 به پورت ۸۰۸۰ زده میشه و ۸۰۸۰ پس از دریافت جواب، داده را برای این پورت ارسال می‌کند. در فلش اول هندشیک و در فلش دوم اک دریافت جواب توسط پورت ۳۳۱۳۴ دیده می‌شود.

سوال ۵

۱. کانکشن‌های موجود در فایل q5.1 ذخیره شده است.

```
$netstat
```

۲. کانکشن‌های موجود در فایل q5.2 ذخیره شده است.

```
$netstat -t
```

۳. کانکشن‌های موجود در فایل q5.3 ذخیره شده است.

```
$netstat -ul
```

۴. کانکشن‌های موجود در فایل q5.4 ذخیره شده است.

```
$netstat -r all
```

مشورت:

عرفان مجیبی