

آزمایش دوم آزمایشگاه شبکه‌های کامپیوتری

رضا عبدالله زاده 97106132 (گروه 2)

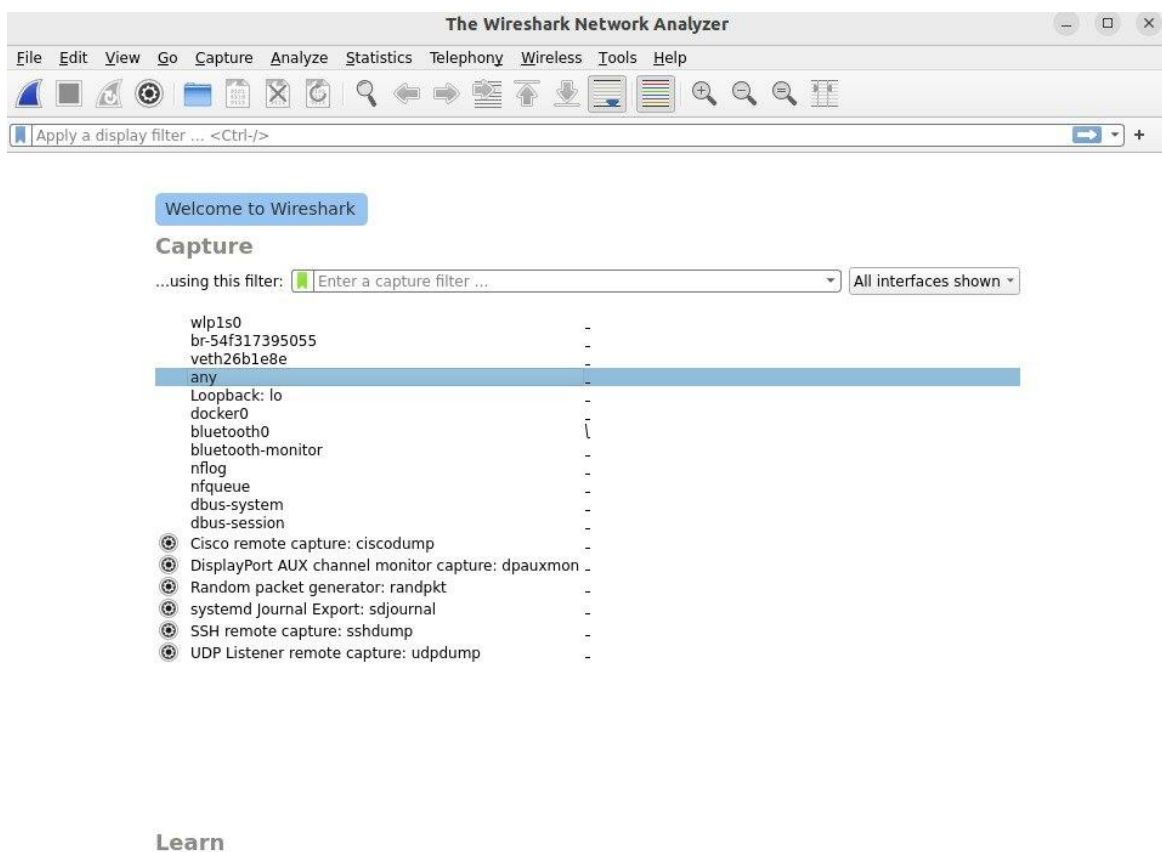
امین مقراضی 97106273 (گروه 2)

مجید طاهرخانی 97106108 (گروه 1)

بخش اول:

ابتدا wireshark را نصب میکنیم و گزینه‌ی any را انتخاب میکنیم و بعد capture میکنیم به صورت

زیر



بعد سایت sharif.edu را سرچ میکنیم و بعد از لود شدن ضبط را متوقف میکنیم

| *any | | | | | |
|--|--------------|-----------------|-----------------|----------|--|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | |
| Apply a display filter ... <Ctrl-/> | | | | | |
| No. | Time | Source | Destination | Protocol | Length Info |
| 963 | 12.937354070 | 127.0.0.53 | 127.0.0.1 | DNS | 124 Standard query response 0xd090 A optimizationg |
| 964 | 12.937921027 | 192.168.43.176 | 142.250.184.234 | QUIC | 1294 Initial, DCID=c927de3a7b7b339f, PKN: 1, PADDING |
| 965 | 13.142528057 | 142.250.184.234 | 192.168.43.176 | QUIC | 1294 Initial, SCID=c927de3a7b7b339f, PKN: 1, ACK, CR |
| 966 | 13.144615533 | 192.168.43.176 | 142.250.184.234 | QUIC | 1294 Initial, DCID=c927de3a7b7b339f, PKN: 2, ACK, PA |
| 967 | 13.341348477 | 192.168.43.176 | 152.89.13.54 | TCP | 68 36416 → 80 [FIN, ACK] Seq=491 Ack=324 Win=64128 |
| 968 | 13.341458278 | 192.168.43.176 | 216.239.38.120 | TCP | 68 38080 → 443 [FIN, ACK] Seq=582 Ack=4290 Win=641 |
| 969 | 13.341505356 | 192.168.43.176 | 216.239.38.120 | TCP | 68 38086 → 443 [FIN, ACK] Seq=582 Ack=4290 Win=641 |
| 970 | 13.341537835 | 192.168.43.176 | 216.239.38.120 | TCP | 68 38082 → 443 [FIN, ACK] Seq=582 Ack=4289 Win=641 |
| 971 | 13.341755900 | 192.168.43.176 | 142.250.184.234 | TCP | 76 47724 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |
| 972 | 13.346322002 | 142.250.184.234 | 192.168.43.176 | QUIC | 1256 Handshake, SCID=c927de3a7b7b339f |
| 973 | 13.346323399 | 142.250.184.234 | 192.168.43.176 | QUIC | 104 Protected Payload (KP0) |
| 974 | 13.347815770 | 192.168.43.176 | 142.250.184.234 | QUIC | 85 Handshake, DCID=c927de3a7b7b339f |

▶ Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface any, id 0
 ▶ Linux cooked capture v1
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
 ▶ User Datagram Protocol, Src Port: 43037, Dst Port: 53
 ▶ Domain Name System (query)

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0000 | 00 00 03 04 00 06 00 00 | 00 00 00 00 00 00 08 00 | |
| 0010 | 45 00 00 56 74 28 40 00 | 40 11 c8 38 7f 00 00 01 | E..Vt(@.0..8.... |
| 0020 | 7f 00 00 35 a8 1d 00 35 | 00 42 fe 89 54 52 01 20 | ...5...5..B...TR |
| 0030 | 00 01 00 00 00 00 00 01 | 0e 63 6c 69 65 6e 74 73 |c.clients |
| 0040 | 65 72 76 69 63 65 73 0a | 67 6f 6f 67 6c 65 61 70 | ervices..googleap |
| 0050 | 69 73 03 63 6f 6d 00 00 | 01 00 01 00 00 29 04 b0 | is.com.....) |
| 0060 | 00 00 00 00 00 00 | | |

کل پکت ها را مشاهده میکنیم

اگر در قسمت فیلتر بزیم http، این ریکویست ها را میبینیم

| *any | | | | | |
|--|-------------|----------------|----------------|----------|------------------------|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | |
| http | | | | | |
| No. | Time | Source | Destination | Protocol | Length Info |
| 578 | 4.795590080 | 192.168.43.176 | 152.89.13.54 | HTTP | 558 GET / HTTP/1.1 |
| 582 | 4.911107741 | 152.89.13.54 | 192.168.43.176 | HTTP | 390 HTTP/1.1 302 Found |

▶ Frame 578: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface any, id 0
 ▶ Linux cooked capture v1
 ▶ Internet Protocol Version 4, Src: 192.168.43.176, Dst: 152.89.13.54
 ▶ Transmission Control Protocol, Src Port: 36416, Dst Port: 80, Seq: 1, Ack: 1, Len: 490
 ▶ Hypertext Transfer Protocol

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0000 | 00 04 00 01 00 06 74 4c | a1 6e fa 01 00 01 08 00 |tL.n..... |
| 0010 | 45 00 02 1e a6 f5 40 00 | 40 06 ff fc c0 a8 2b b0 | E.....@. @.....+ |
| 0020 | 98 59 0d 36 8e 40 00 50 | c5 82 f0 ca 2d f9 1f cc | Y.6.@P.....- |
| 0030 | 80 18 01 f6 b5 42 00 00 | 01 01 08 0a cc 32 7c f1 |B.....2].. |
| 0040 | 80 74 75 7c 47 45 54 20 | 2f 20 48 54 54 50 2f 31 | tu GET / HTTP/1 |
| 0050 | 2e 31 0d 0a 48 6f 73 74 | 3a 20 73 68 61 72 69 66 | .1..Host : sharif |
| 0060 | 2e 65 64 75 0d 0a 43 6f | 6e 6e 65 63 74 69 6f 6e | .edu..Co nnection |
| 0070 | 3a 20 6b 65 65 70 2d 61 | 6c 69 76 65 0d 0a 55 70 | : keep-a live-Up |
| 0080 | 67 72 61 64 65 2d 49 6e | 73 65 63 75 72 65 2d 52 | grade-In secure-R |
| 0090 | 65 71 75 65 73 74 73 3a | 20 31 0d 0a 65 73 65 72 | equests: 1..User |

اگر ادرس destination را در بروزر بزنیم این سایت بالا میاید:

152.89.13.54

بیت الکترونیک
sina.sharif.edu
دانشگاه صنعتی شریف

Vclass Net2 Register VPN

ریاست دانشگاهآموزشپژوهشدانشجویفرهنگیاداری و مالیپررئیس هاآموزشهای الکترونیکفرم هاپهوندها

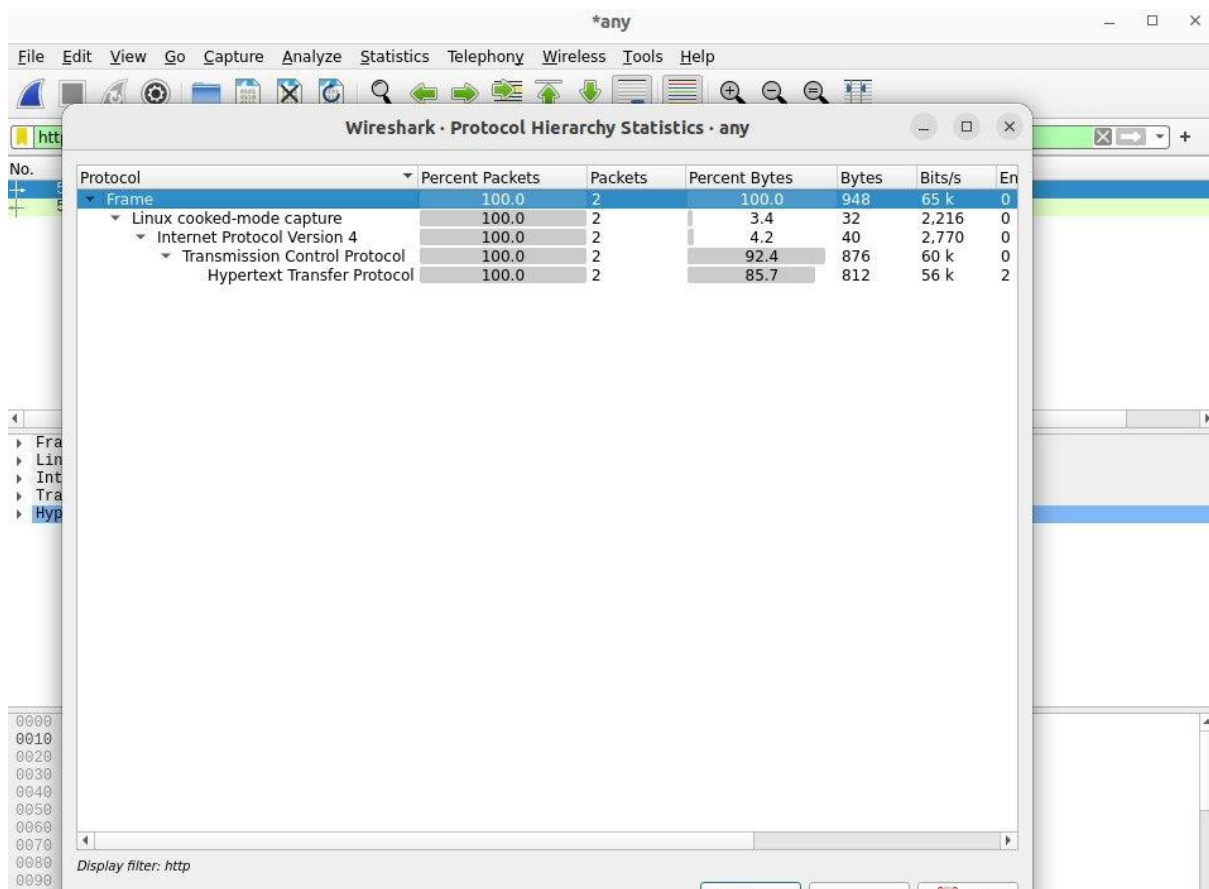
انوماسیون اداری
فایل سرور SUT-FTP
مدیران دانشگاه
امور مالی
حقوق و دستمزد
وب سایت شخصی و ایمییل اساتید
شماره تلفن کارکنان

پرتال پژوهشی
فعالتهای دانشکده ای و دروس اینترنتی
اجاد وب سایت شخصی و انتقال اطلاعات
مرکز آموزشهای الکترونیک
سیستم آموزش
سیستم تدارکات، انبار، اموال

Outlook
تنظیمات ایمییل
سامانه حضور و غیاب
تغییر کلمه رمز
اعتبار باقیمانده اینترنت
مدیریت امور اداری
سامانه پارکینگ
سامانه تغذیه

انرژی | برق | شیمی | شیمی و نفت | صنایع | علوم ریاضی | عمران | فیزیک | کامپیوتر | مدیریت و اقتصاد | مکانیک | مهندسی و علم مواد | هوا فضا

در قسمت statistics با انتخاب protocol hierarchy میتوانیم درصد پروتکول های مختلف را مشاهده کنیم، بصورت زیر:

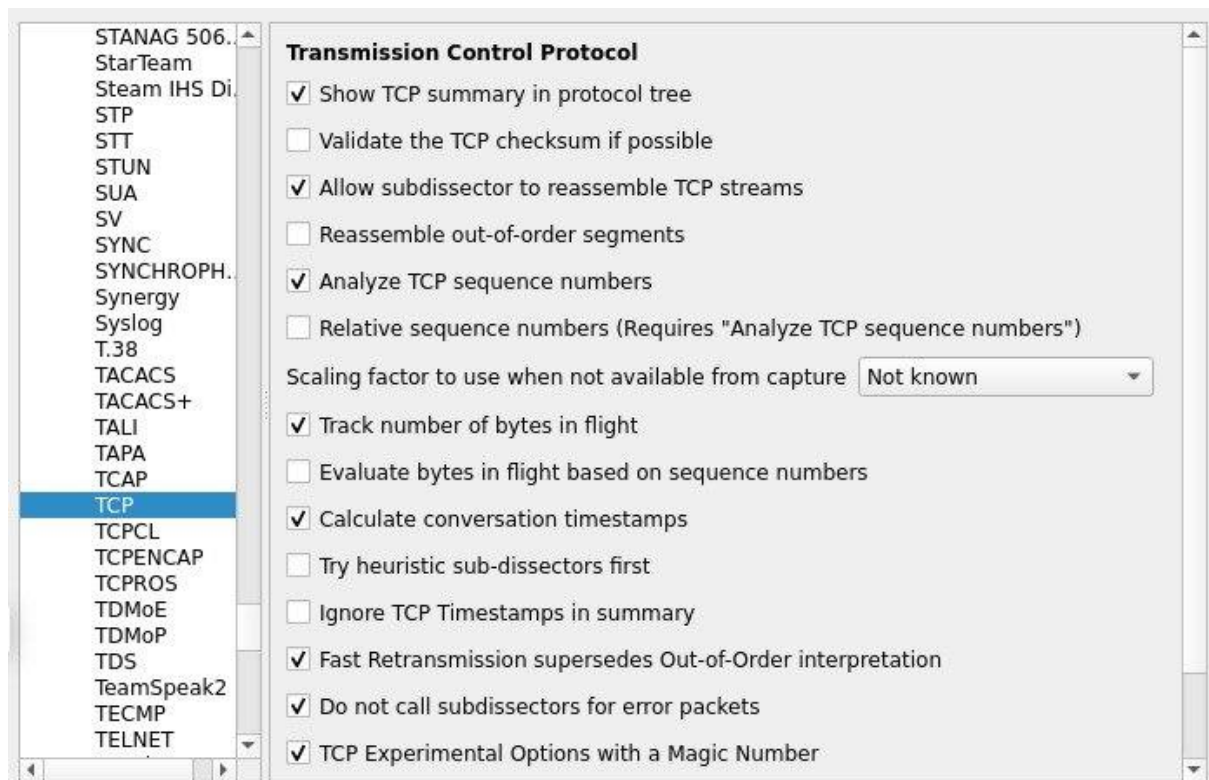


The image shows the 'Wireshark - Protocol Hierarchy Statistics - any' window. It displays a tree view of network protocols and their corresponding statistics. The table below represents the data shown in the window.

| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | En |
|-------------------------------|-----------------|---------|---------------|-------|--------|----|
| Frame | 100.0 | 2 | 100.0 | 948 | 65 k | 0 |
| Linux cooked-mode capture | 100.0 | 2 | 3.4 | 32 | 2,216 | 0 |
| Internet Protocol Version 4 | 100.0 | 2 | 4.2 | 40 | 2,770 | 0 |
| Transmission Control Protocol | 100.0 | 2 | 92.4 | 876 | 60 k | 0 |
| Hypertext Transfer Protocol | 100.0 | 2 | 85.7 | 812 | 56 k | 2 |

همانطور که در تصاویر مشاهده میکنید time برابر 4.79 است که میرویم در قسمت edit در preferences بصورت زیر تیک relative را برمیذاریم

در قسمت filter کلمه ی dns را سرچ میکنیم و مشاهده میکنیم.



برای استخراج عکس ها در بخش file در قسمت export object گزینه ی http را میزیم و میتوانیم عکس ها را انتخاب کنیم

بخش دوم:

به کمک putty به telehack.com تلنت زدیم و نتیجه به صورت زیر شد:

| telnet | | | | | | |
|---|-----------|----------------|----------------|----------|--------|-----------------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 4426 | 14.070338 | 172.27.170.224 | 64.13.139.230 | TELNET | 75 | Telnet Data ... |
| 4581 | 14.502584 | 64.13.139.230 | 172.27.170.224 | TELNET | 60 | Telnet Data ... |
| 4802 | 15.051509 | 64.13.139.230 | 172.27.170.224 | TELNET | 1194 | Telnet Data ... |
| 4803 | 15.051835 | 172.27.170.224 | 64.13.139.230 | TELNET | 63 | Telnet Data ... |
| 4804 | 15.051981 | 172.27.170.224 | 64.13.139.230 | TELNET | 65 | Telnet Data ... |
| 4805 | 15.052102 | 172.27.170.224 | 64.13.139.230 | TELNET | 57 | Telnet Data ... |
| 5034 | 15.577014 | 64.13.139.230 | 172.27.170.224 | TELNET | 60 | Telnet Data ... |
| 5242 | 16.133300 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 5317 | 16.314577 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 5375 | 16.481121 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 5425 | 16.602662 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 5449 | 16.664411 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 5605 | 17.067939 | 64.13.139.230 | 172.27.170.224 | TELNET | 56 | Telnet Data ... |
| 5776 | 17.524073 | 64.13.139.230 | 172.27.170.224 | TELNET | 60 | Telnet Data ... |
| 5980 | 18.292680 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 6027 | 18.629332 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 6054 | 18.750978 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 6067 | 18.800382 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 6109 | 18.914392 | 172.27.170.224 | 64.13.139.230 | TELNET | 55 | Telnet Data ... |
| 6318 | 19.556894 | 64.13.139.230 | 172.27.170.224 | TELNET | 56 | Telnet Data ... |
| 6692 | 20.688446 | 64.13.139.230 | 172.27.170.224 | TELNET | 60 | Telnet Data ... |
| 6968 | 21.247997 | 172.27.170.224 | 64.13.139.230 | TELNET | 56 | Telnet Data ... |
| 7383 | 22.216724 | 64.13.139.230 | 172.27.170.224 | TELNET | 56 | Telnet Data ... |
| > Frame 4426: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{66F0A3D...} > Ethernet II, Src: LiteonTe_23:d4:f7 (c8:ff:28:23:d4:f7), Dst: Cisco_b4:bb:ec (10:b3:c6:b4:bb:ec) > Internet Protocol Version 4, Src: 172.27.170.224, Dst: 64.13.139.230 > Transmission Control Protocol, Src Port: 2923, Dst Port: 23, Seq: 1, Ack: 1, Len: 21 > Telnet > Will Negotiate About Window Size Command: Will (251) Subcommand: Negotiate About Window Size > Will Terminal Speed Command: Will (251) Subcommand: Terminal Speed | | | | | | |

همینطور tcp stream آن در شکل زیر مشخص است:


```
Wireshark · Follow TCP Stream (tcp.stream eq 36) · Wi-Fi 2
.....
Connected to TELEHACK port 85
.....
It is 11:42 am on Monday, August 1, 2022 in Mountain View, California, USA.
There are 73 local users. There are 26642 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.
Press control-C to interrupt any command.

May the command line live forever.

Command, one of the following:
2048      ?      ac      advent      aquarium    basic
bf        cal     calc     callsign    ching       clear
clock     cowsay  ddate    echo        eliza       factor
figlet    finger  fnord    geoip       gif         help
ipaddr    joke    login    mac         md5         morse
newuser   notes   octopus  phoon       pig         ping
pong      primes  privacy  qr          rain        rand
rfc       rig     roll     sleep       starwars    traceroute
typespeed units   uptime   usenet      users       uumap
uupath    uuplot  when     zc          zork        zrun

.....P.....XTERM....$..$loginlogin dups dups

Password: dups*dups
*****
Logged in as user DUPS. Last login was 1m ago.

You have mail.
@ls
ls
advent.gam      againstip.txt  basic.man      bbslist.txt
big.bas         c8test.c8     changelog.txt  colossus.txt
command.txt     crackdown.txt do-well.txt    dojo.man
drunks.txt      escseq.bas    etewaf.txt     ferry.txt
finger.txt      fnord.txt     future.txt     hammurabi.bas
hckr_hnd.txt    ien137.txt    jfet.a2        johnnycode.txt
k-rad.txt       learncode.txt leaves.txt      lem.bas
like.bas        lostpig.gam   mastermind.bas matrix.bas
mud.exe         notes.txt     orange-book.txt oregon.bas
pman.man        porthack.exe  privacy.txt    rogue.gam
```

-۱

بر اساس خروجی wireshark آدرس آپی مبدا 172.27.170.224 و آدرس آپی مقصد 64.13.139.230 است.

۲- با جستجو به دستور لاگین در telehack می‌رسیم و با بررسی آن مقدار username و password به ترتیب برابر dups و dupsdups است. همانطور که قابل مشاهده است برای انتقال پسورد هیچ رمزگذاری انجام نشده است.

۳- در کنسول مقصد دستورات زیر به ترتیب اجرا شده است که در تصاویر زیر از طریق محیط wireshark نیز قابل مشاهده است:

Ls, date, clock

```

@ls
ls
advent.gam      againstip.txt  basic.man      bbslist.txt
big.bas         c8test.c8     changelog.txt  colossus.txt
command.txt     crackdown.txt  do-well.txt    dojo.man
drunks.txt     escseq.bas    etewaf.txt     ferry.txt
finger.txt     fnord.txt     future.txt     hammurabi.bas
hckr_hnd.txt   ien137.txt    jfet.a2        johnnycode.txt
k-rad.txt      learncode.txt  leaves.txt     lem.bas
like.bas       lostpig.gam   mastermind.bas matrix.bas
mud.exe        notes.txt     orange-book.txt oregon.bas
pman.man       porthack.exe  privacy.txt    rogue.gam
rootkit.exe    satcom.man    showrunning.txt smile.c8
snowing.vt     sstrek.bas    starwars.txt   sysmon.txt
telehack.txt   tetris.exe    ttest.vt       tunes.bas
underground.txt unix.txt       wardial.exe     wumpus.bas
xmas.vt        xmodem.exe    zork.gam

```

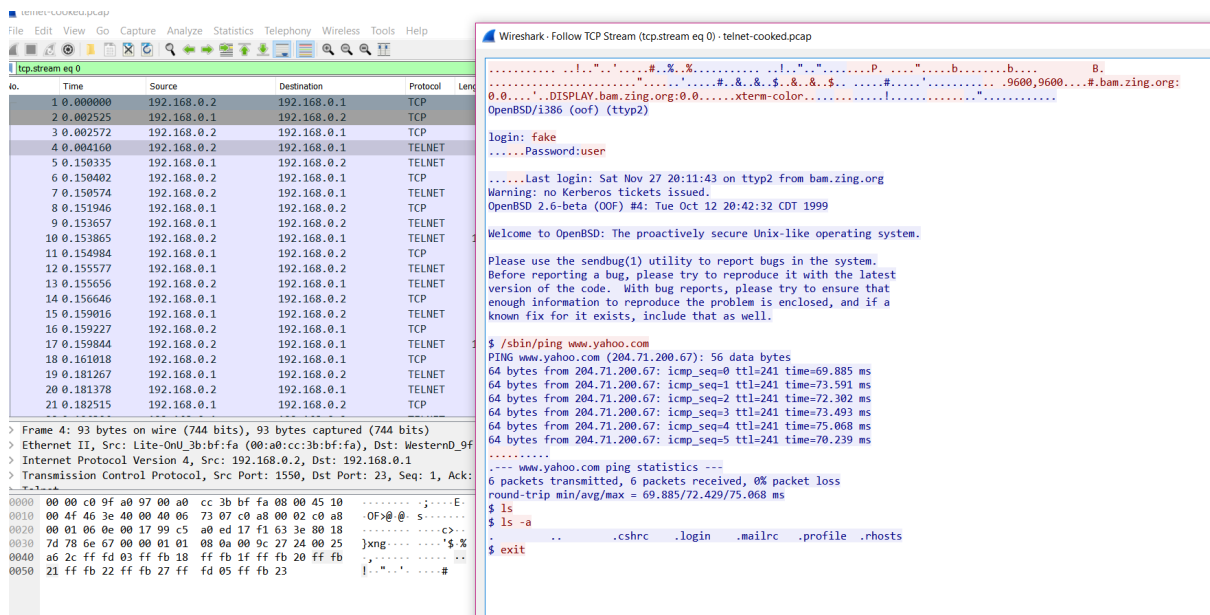
```

@date
date
Monday, August 1, 2022 11:12:41 PM +0430
@clocklock
. [?251.[H.[2]

```

پیوست بخش دوم:

در بخش قبل آزمایش را خودمان اجرا کردیم ولی با توجه به فایل ضمیمه شده و انجام مراحل پیشین که در شکل زیر مشخص است:



آیپی مبدا و مقصد به ترتیب 192.168.0.2 و 192.168.0.1 و مقدار یوزرنیم و پسورد به ترتیب fake و user است و دستورات `ls`، `ls -a`، `ping www.yahoo.com` و `exit` اجرا شده است.

```
login: fake
.....Password:user
```

```
$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms

--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
.
..
.cshrc
.profile
.rhosts
$ exit
```

بخش سوم:

1- بر اساس خروجی wireshark درخواست و پاسخ آن با سرور 172.26.146.34 رد و بدل می شود.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 698 | 7.421227 | 172.27.170.224 | 172.26.146.34 | DNS | 86 | Standard query 0x0001 PTR 34.146.26.172.in-addr.arpa |
| 706 | 7.748842 | 172.26.146.34 | 172.27.170.224 | DNS | 140 | Standard query response 0x0001 No such name PTR 34.146.26.172.in-addr.arpa SOA 26.172.IN-ADDR.ARPA |

2- header درخواست dns:

```
▼ Domain Name System (query)
  Transaction ID: 0x0004
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0.. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ google.com: type A, class IN
      Name: google.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 724]
```

Transaction ID مربوط به این درخواست برابر 0x0004 است که یک آیدی یونیک به نسبت داده

شده به هر بسته ی dns است که در ریسپانس نیز باید با همین مقدار موجود باشد.

محتوای این پیام بزرگ نبوده و در نتیجه truncate نشده است و بر اساس فلگ چهارم به صورت

بازگشتی درخواست dns داده می شود.

Header پاسخ dns:

```

▼ Domain Name System (response)
  Transaction ID: 0x0004
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .0... .. = Authoritative: Server is not an authority for domain
    .... ..0... .. = Truncated: Message is not truncated
    .... ...1... .. = Recursion desired: Do query recursively
    .... ....1... .. = Recursion available: Server can do recursive queries
    .... ....0... .. = Z: reserved (0)
    .... ....0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... ....0... .. = Non-authenticated data: Unacceptable
    .... ....0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ google.com: type A, class IN
      Name: google.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  > Answers
    [Request In: 718]
    [Time: 0.014830000 seconds]

```

مقدار Transaction ID برابر همان مقدار در ریکوئست یعنی 0x0004 است و بر اساس هدر، پاسخ نیز به صورت بازگشتی پردازش شده است. در بازیابی آیدی google.com اروری رخ نداده است و همانطور که قابل مشاهده است آدرس google.com از dns server اصلی آن بازیابی نشده است بلکه از یک non-authoritative server و به صورت کش شده بازیابی شده است.