

به نام آفریننده بیت‌ها



## پروژه دوم

شبکه‌های کامپیوتری

نیم‌سال دوم ۱۴۰۰ - ۱۴۰۱

دانشکده‌ی برق و کامپیوتر

دانشگاه صنعتی اصفهان

---

تیر ماه ۱۴۰۱

دانیال خراسانی‌زاده

ملیکا فتوحی

استاد درس:

دکتر محمدرضا حیدرپور



## فهرست مطالب

۲	۱ ارسال هر بسته دلخواه
۵	۲ ارسال بسته‌های TCP SYN
۷	۳ مینی وایر-شارک
۸	۴ مینی-انمپ



## ۱ ارسال هر بسته دلخواه

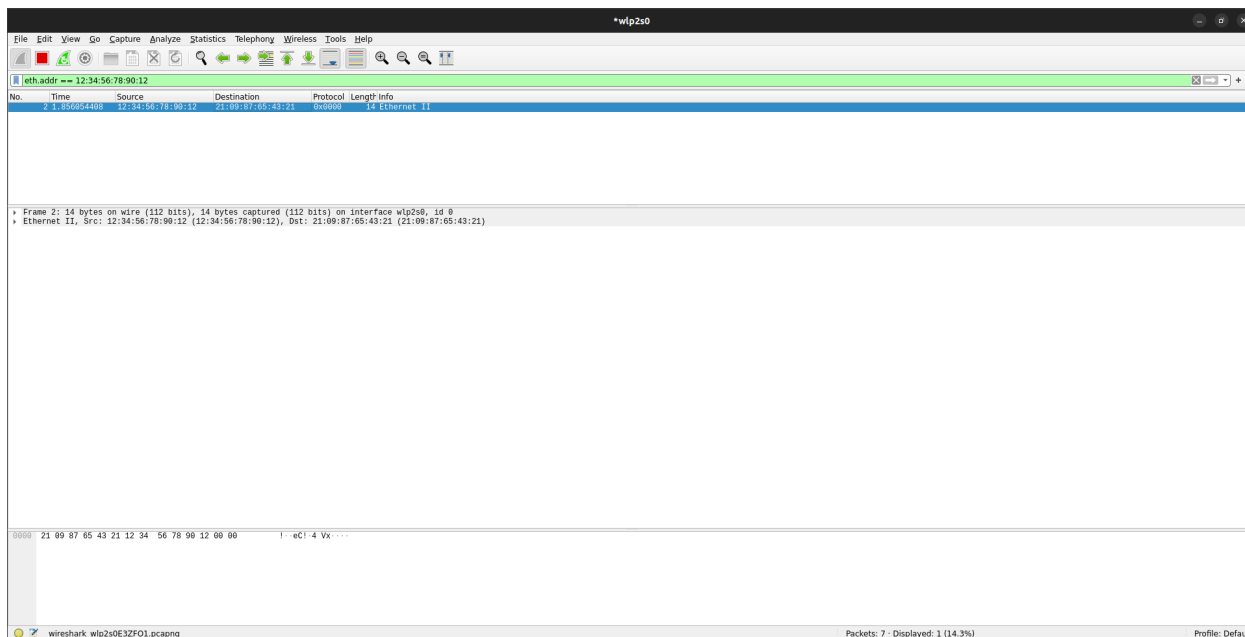
۱. ۱۴ بایت - این مقدار حداقل طول یک فریم اترنت سالم است.

۲. باید به فرمت استاندارد بسته اترنت باشد یعنی به ترتیب دارای ۶ بایت آدرس فیزیکی مقصد - ۶ بایت آدرس فیزیکی مبدا و ۲ بایت طول یا نوع پروتوکل باشد.

۳.

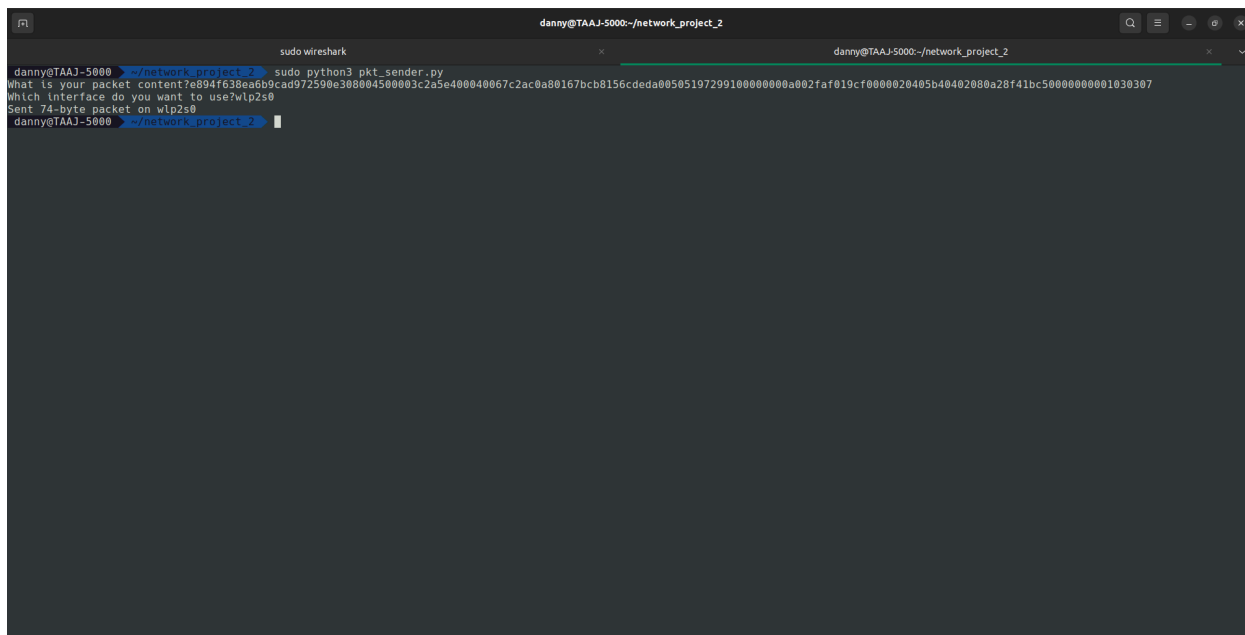
```
danny@TAAJ-5000:~/network_project_2$ sudo wireshark
danny@TAAJ-5000:~/network_project_2$ sudo python3 pkt_sender.py
What is your packet content?22109876543211234567890120000
Which interface do you want to use?wlp2s0
Sent 14-byte packet on wlp2s0
danny@TAAJ-5000:~/network_project_2$
```

شکل ۱: ارسال فریم اترنت خالی

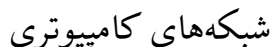


شکل ۲: کیچر فریم ارسال شده در برنامه وایرشارک

۴.



شکل ۳: ارسال بسته TCP



## پروژه دوم

شکل ۴: کیچر بسته در برنامه وایرشارک (بسته شماره ۱۳۷ بسته اصلی و بسته شماره ۳۷۷ بسته تکراری ارسال شده است)

۵. حمله Replay Attack یک نوع حمله در شبکه است که در آن ارسال یک بسته صحیح با اهداف بدخواهانه چندین بار تکرار می‌شود. با توجه به اینکه می‌توان با استفاده از برنامه‌ای که در این قسمت نوشتیم هر بسته‌ای را ارسال کرد، اگر به یک بسته صحیح دست پیدا کنیم می‌توانیم بارها آن را ارسال کرده و باعث ایجاد اختلال بشویم که این کار دقیقاً همان حمله بازپخش است.



## ۲ ارسال بسته‌های TCP SYN

۱. فیلدهای ID و TTL در هدر IP و فیلدهای Sequence Number و Acknowledgment Number در هدر TCP می‌توانند دلخواه باشند. البته مقدار TTL باید مقدار درستی باشد و اگر خیلی کم باشد ممکن است بسته به مقصد نرسد و اگر خیلی زیاد باشد ممکن است باعث ایجاد ترافیک ناخواسته در شبکه شود.

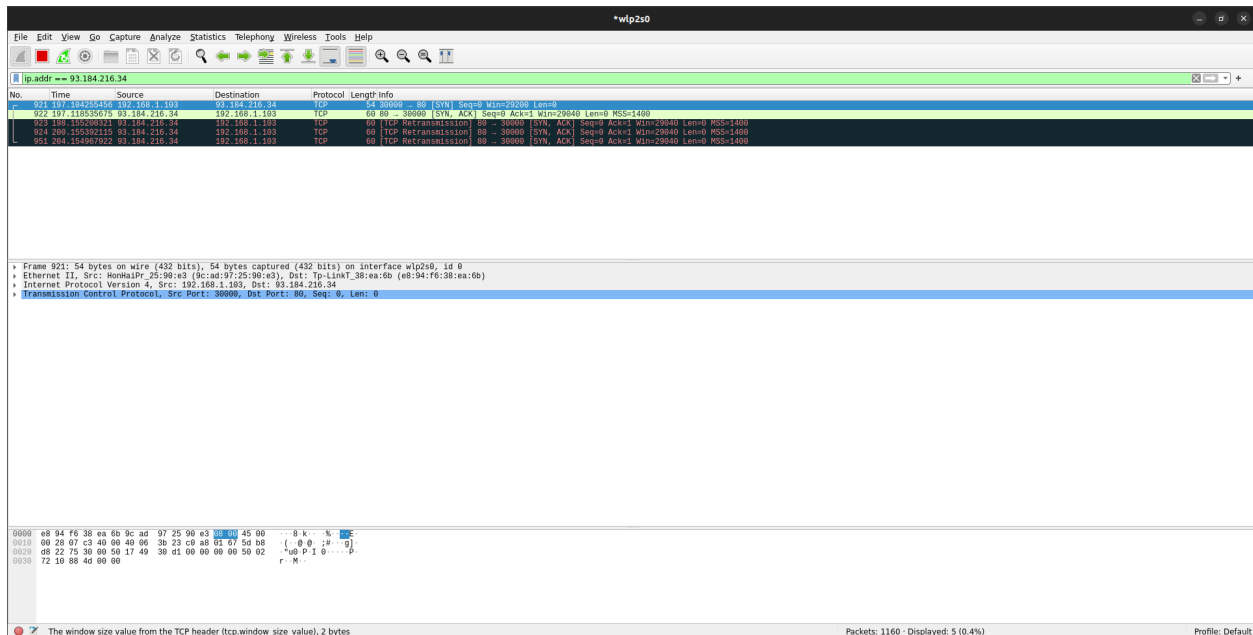
۲.

```
danny@TAAJ-5000:~/network_project_2
sudo wireshark
danny@TAAJ-5000:~/network_project_2 nslookup example.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   example.com
Address: 93.184.216.34
Name:   example.com
Address: 2606:2800:220:1:248:1893:25c8:1946

danny@TAAJ-5000:~/network_project_2 ./lftinfo.sh 93.184.216.34 80 wlp2s0 30000
danny@TAAJ-5000:~/network_project_2 sudo python3 tcp_syn_sender.py
Sent 54-byte TCP SYN packet on wlp2s0
danny@TAAJ-5000:~/network_project_2
```

شکل ۵: ارسال بسته TCP SYN به وبسایت example.com



شکل ۶: کپچر کردن بسته TCP SYN ارسال شده در برنامه وایرشارک

۳. اولین بسته بعد از بسته ارسالی پاسخ SYN ACK سرور به بسته‌ای است که ما ارسال کردیم، با توجه به اینکه پروتکل TCP اتصال گرا است اگر برای بسته‌ای که ارسال کرده ACK دریافت نکند، بسته را بازارسال می‌کند. در اینجا نیز با توجه به اینکه به SYN ACK سرور پاسخی نمی‌دهیم، سرور چندین بار آن را باز ارسال می‌کند تا اگر مشکلی در ارسال بسته اول بوده در نهایت بسته به دست ما برسد.

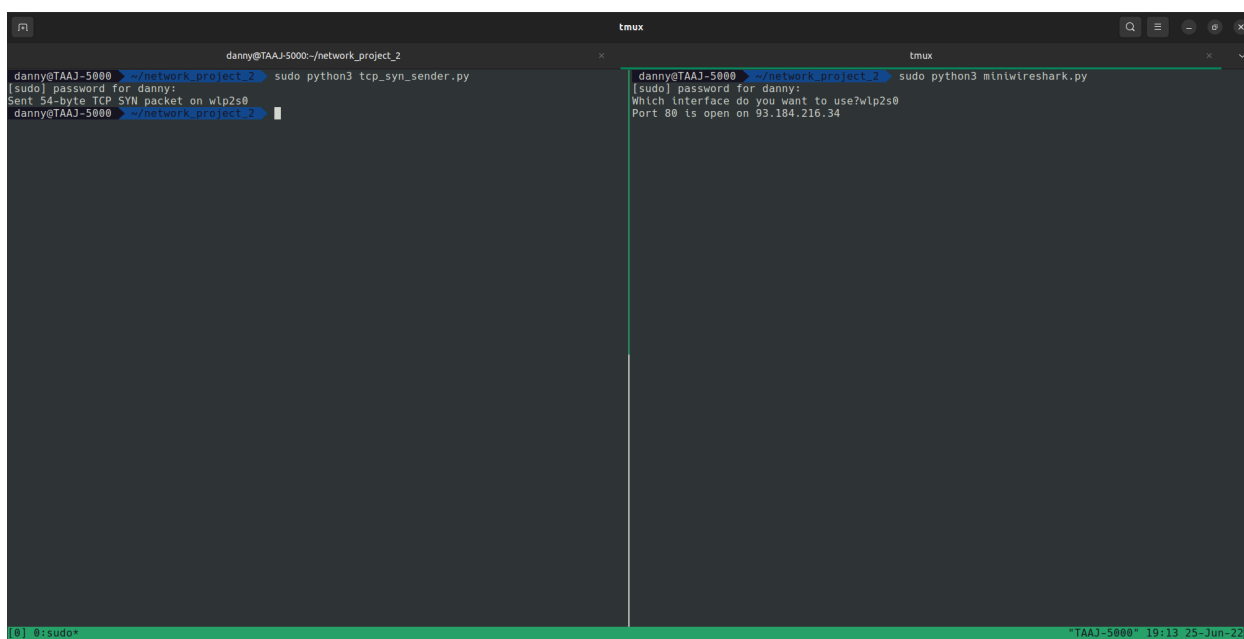
۴. در شکل ۵ نحوه کار این برنامه نشان داده شده.

### ۳ مینی وایر-شارک

۱. طول هدر Ethernet ۱۴ بایت، حداقل طول هدر IP ۲۰ بایت و حداکثر طول آن ۶۰ بایت، حداقل طول هدر TCP ۲۰ بایت و حداکثر طول آن ۶۰ بایت است.

۲. با چک کردن فیلد Flags در هدر TCP و یک بودن بیت‌های SYN و ACK در این فیلد می‌توانیم مطمئن شویم که بسته دریافتی SYN ACK است.

۳.



```
danny@TAAJ-5000:~/network_project_2$ sudo python3 tcp_syn_sender.py
[sudo] password for danny:
Sent 54-byte TCP SYN packet on wlp2s0
danny@TAAJ-5000:~/network_project_2$

danny@TAAJ-5000:~/network_project_2$ sudo python3 miniwireshark.py
[sudo] password for danny:
Which interface do you want to use?wlp2s0
Port 80 is open on 93.184.216.34
```

شکل ۷: همکاری دو برنامه TCP SYN sender و Mini Wireshark





## ۴ مینی-انمپ

۱. پورت‌های 25، 80، 110، 143، 443، 465، 587، 993، 995 روی این سرور باز هستند.

```
tmux
sudo wireshark
danny@TAAJ-5000 ~/network_project_2 sudo python3 miniwreshark.py
Which interface do you want to use?wlp2s0

danny@TAAJ-5000 ~/network_project_2 sudo python3 mininmap_sender.py
What is the target IP address?176.101.52.70
Which ports do you want to scan?20-2000
Sent 54-byte TCP SYN packet to port 0
Sent 54-byte TCP SYN packet to port 1
Sent 54-byte TCP SYN packet to port 2
Sent 54-byte TCP SYN packet to port 3
Sent 54-byte TCP SYN packet to port 4
Sent 54-byte TCP SYN packet to port 5
Sent 54-byte TCP SYN packet to port 6
Sent 54-byte TCP SYN packet to port 7
Sent 54-byte TCP SYN packet to port 8
Sent 54-byte TCP SYN packet to port 9
Sent 54-byte TCP SYN packet to port 10
Sent 54-byte TCP SYN packet to port 11
Sent 54-byte TCP SYN packet to port 12
Sent 54-byte TCP SYN packet to port 13
Sent 54-byte TCP SYN packet to port 14
Sent 54-byte TCP SYN packet to port 15
Sent 54-byte TCP SYN packet to port 16
Sent 54-byte TCP SYN packet to port 17
Sent 54-byte TCP SYN packet to port 18
```

شکل ۸: شروع کار برنامه Mini Nmap

```
tmux
sudo wireshark
danny@TAAJ-5000 ~/network_project_2 sudo python3 miniwreshark.py
Which interface do you want to use?wlp2s0
Port 25 is open on 176.101.52.70
Port 80 is open on 176.101.52.70
Port 110 is open on 176.101.52.70
Port 143 is open on 176.101.52.70
Port 443 is open on 176.101.52.70
Port 465 is open on 176.101.52.70
Port 587 is open on 176.101.52.70
Port 993 is open on 176.101.52.70
Port 995 is open on 176.101.52.70

Sent 54-byte TCP SYN packet to port 1957
Sent 54-byte TCP SYN packet to port 1958
Sent 54-byte TCP SYN packet to port 1959
Sent 54-byte TCP SYN packet to port 1960
Sent 54-byte TCP SYN packet to port 1961
Sent 54-byte TCP SYN packet to port 1962
Sent 54-byte TCP SYN packet to port 1963
Sent 54-byte TCP SYN packet to port 1964
Sent 54-byte TCP SYN packet to port 1965
Sent 54-byte TCP SYN packet to port 1966
Sent 54-byte TCP SYN packet to port 1967
Sent 54-byte TCP SYN packet to port 1968
Sent 54-byte TCP SYN packet to port 1969
Sent 54-byte TCP SYN packet to port 1970
Sent 54-byte TCP SYN packet to port 1971
Sent 54-byte TCP SYN packet to port 1972
Sent 54-byte TCP SYN packet to port 1973
Sent 54-byte TCP SYN packet to port 1974
Sent 54-byte TCP SYN packet to port 1975
Sent 54-byte TCP SYN packet to port 1976
Sent 54-byte TCP SYN packet to port 1977
Sent 54-byte TCP SYN packet to port 1978
Sent 54-byte TCP SYN packet to port 1979
Sent 54-byte TCP SYN packet to port 1980
Sent 54-byte TCP SYN packet to port 1981
Sent 54-byte TCP SYN packet to port 1982
Sent 54-byte TCP SYN packet to port 1983
Sent 54-byte TCP SYN packet to port 1984
Sent 54-byte TCP SYN packet to port 1985
Sent 54-byte TCP SYN packet to port 1986
Sent 54-byte TCP SYN packet to port 1987
Sent 54-byte TCP SYN packet to port 1988
Sent 54-byte TCP SYN packet to port 1989
Sent 54-byte TCP SYN packet to port 1990
Sent 54-byte TCP SYN packet to port 1991
Sent 54-byte TCP SYN packet to port 1992
Sent 54-byte TCP SYN packet to port 1993
Sent 54-byte TCP SYN packet to port 1994
Sent 54-byte TCP SYN packet to port 1995
Sent 54-byte TCP SYN packet to port 1996
Sent 54-byte TCP SYN packet to port 1997
Sent 54-byte TCP SYN packet to port 1998
Sent 54-byte TCP SYN packet to port 1999
Sent 54-byte TCP SYN packet to port 2000
danny@TAAJ-5000 ~/network_project_2
```

شکل ۹: پایان کار برنامه Mini Nmap و لیست پورت‌های باز در سرور انتخاب شده  
دانیال خراسانی‌زاده  
۸  
ملیکا فتوحی

۲.

Port	Service
25	SMTP
80	HTTP
110	POP3
143	IMAP
443	HTTPS
465	SMTPS
587	SMTP
993	IMPAS
995	POP3S

۳. با توجه به اینکه این برنامه فرایند ایجاد یک اتصال TCP را به طور کامل انجام می‌دهد، عملکرد کندتری نسبت به برنامه اصلی ما خواهد داشت اما نتیجه کار آن یکسان خواهد بود.

