|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |
| --- | --- |

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления\_\_\_\_\_\_\_\_\_\_\_

Отчет по лабораторной работе № 7  
**«Работа с программным анализатором протоколов**

**tcpdump»**по дисциплине «Сети и телекоммуникации»

Студент ИУ5-51Б Т.А. Цыпышев

(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель А.И. Антонов

(Подпись, дата) (И.О.Фамилия)

**Москва**

**2024**

### 1. Запуск tcpdump для захвата всех пакетов, проходящих по сети

Чтобы захватывать все пакеты в сети без фильтрации, используйте команду:

sudo tcpdump -c 7

* -c 7 — ограничивает количество захватываемых пакетов до 7.

tcpdump: verbose output suppressed, use -v[v]... for full protocol decode

listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes

03:21:29.351614 IP ttsypyshev-Modern-14-B11MOU.43978 > lh-in-f95.1e100.net.https: Flags [P.], seq 2805534563:2805534602, ack 1157091356, win 407, options [nop,nop,TS val 2053612174 ecr 584189844], length 39

03:21:29.351840 IP ttsypyshev-Modern-14-B11MOU.43978 > lh-in-f95.1e100.net.https: Flags [FP.], seq 39:63, ack 1, win 407, options [nop,nop,TS val 2053612174 ecr 584189844], length 24

03:21:29.450004 IP ttsypyshev-Modern-14-B11MOU.57814 > \_gateway.domain: 14905+ PTR? 95.161.233.64.in-addr.arpa. (44)

03:21:29.632502 IP \_gateway.domain > ttsypyshev-Modern-14-B11MOU.57814: 14905 1/0/0 PTR lh-in-f95.1e100.net. (77)

03:21:29.633522 IP ttsypyshev-Modern-14-B11MOU.33525 > \_gateway.domain: 28769+ PTR? 189.43.168.192.in-addr.arpa. (45)

03:21:29.636289 IP \_gateway.domain > ttsypyshev-Modern-14-B11MOU.33525: 28769 NXDomain 0/0/0 (45)

03:21:29.637635 IP ttsypyshev-Modern-14-B11MOU.41285 > \_gateway.domain: 571+ PTR? 108.43.168.192.in-addr.arpa. (45)

7 packets captured

8 packets received by filter

0 packets dropped by kernel

### 2. Запуск tcpdump для перехвата широковещательного трафика

Для фильтрации широковещательного трафика по MAC-адресу FF:FF:FF:FF:FF:FF и IP-адресу, который можно узнать с помощью ifconfig, используйте следующую команду:

sudo tcpdump -c 5 '(ether broadcast or ip broadcast)' -X

* -c 5 — ограничение захвата до 5 пакетов.
* ether broadcast — фильтрует по широковещательному MAC-адресу.
* ip broadcast — фильтрует по широковещательному IP-адресу.
* -X — выводит пакет в шестнадцатеричной и ASCII форме.

03:11:57.863705 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from dc:56:e7:47:70:e3 (oui Unknown), length 300

0x0000: ffff ffff ffff dc56 e747 70e3 0800 4500

0x0010: 0148 42bd 0000 ff11 77e8 0000 0000 ffff

0x0020: ffff 0044 0043 0134 cec6 0101 0600 8458

0x0030: 85c5 0000 0000 0000 0000 0000 0000 0000

0x0040: 0000 0000 0000 dc56 e747 70e3 0000 0000

0x0050: 0000 0000 0000 0000 0000 0000 0000 0000

0x0060: 0000 0000 0000 0000 0000 0000 0000 0000

0x0070: 0000 0000 0000 0000 0000 0000 0000 0000

0x0080: 0000 0000 0000 0000 0000 0000 0000 0000

0x0090: 0000 0000 0000 0000 0000 0000 0000 0000

0x00a0: 0000 0000 0000 0000 0000 0000 0000 0000

0x00b0: 0000 0000 0000 0000 0000 0000 0000 0000

0x00c0: 0000 0000 0000 0000 0000 0000 0000 0000

0x00d0: 0000 0000 0000 0000 0000 0000 0000 0000

0x00e0: 0000 0000 0000 0000 0000 0000 0000 0000

0x00f0: 0000 0000 0000 0000 0000 0000 0000 0000

0x0100: 0000 0000 0000 0000 0000 0000 0000 0000

0x0110: 0000 0000 0000 6382 5363 3501 0337 0901

0x0120: 7903 060f 6c72 77fc 3902 05dc 3d07 01dc

0x0130: 56e7 4770 e332 04c0 a800 8f33 0400 76a7

0x0140: 000c 0d41 7070 6c65 2d54 562d 3435 3635

0x0150: ff00 0000 0000

03:11:57.863747 ARP, Request who-has Apple-TV-4565.Dlink tell Apple-TV-4565.Dlink, length 46

0x0000: ffff ffff ffff dc56 e747 70e3 0806 0001

0x0010: 0800 0604 0001 dc56 e747 70e3 c0a8 008f

0x0020: 0000 0000 0000 c0a8 008f 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

03:11:57.863747 ARP, Request who-has 169.254.255.255 tell Apple-TV-4565.Dlink, length 46

0x0000: ffff ffff ffff dc56 e747 70e3 0806 0001

0x0010: 0800 0604 0001 dc56 e747 70e3 c0a8 008f

0x0020: 0000 0000 0000 a9fe ffff 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

03:11:57.961130 ARP, Request who-has dlinkrouter.Dlink tell Apple-TV-4565.Dlink, length 46

0x0000: ffff ffff ffff dc56 e747 70e3 0806 0001

0x0010: 0800 0604 0001 dc56 e747 70e3 c0a8 008f

0x0020: 0000 0000 0000 c0a8 0001 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

03:11:58.116899 ARP, Request who-has 169.254.255.255 tell Apple-TV-4565.Dlink, length 46

0x0000: ffff ffff ffff dc56 e747 70e3 0806 0001

0x0010: 0800 0604 0001 dc56 e747 70e3 c0a8 008f

0x0020: 0000 0000 0000 a9fe ffff 0000 0000 0000

0x0030: 0000 0000 0000 0000 0000 0000

5 packets captured

9 packets received by filter

0 packets dropped by kernel

### 3. Запуск tcpdump для перехвата пакетов ICMP

Чтобы перехватывать пакеты ICMP, отправленные на IP-адрес одного из лабораторных ПК, используйте:

sudo tcpdump -c 8 icmp and host <IP-адрес лабораторного ПК> -XX

* icmp — фильтрует только ICMP-пакеты.
* -XX — выводит пакеты в шестнадцатеричной и ASCII форме.

03:16:42.511258 IP ttsypyshev-Modern-14-B11MOU.Dlink > HP7C4D8F7677F4.Dlink: ICMP echo request, id 7792, seq 28, length 64

0x0000: 7c4d 8f76 77f4 4c44 5b39 8415 0800 4500 |M.vw.LD[9....E.

0x0010: 0054 8374 4000 4001 346d c0a8 00bf c0a8 .T.t@.@.4m......

0x0020: 00b8 0800 c31d 1e70 001c ea4e 6b67 0000 .......p...Nkg..

0x0030: 0000 facc 0700 0000 0000 1011 1213 1415 ................

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:42.515684 IP HP7C4D8F7677F4.Dlink > ttsypyshev-Modern-14-B11MOU.Dlink: ICMP echo reply, id 7792, seq 28, length 64

0x0000: 4c44 5b39 8415 7c4d 8f76 77f4 0800 4500 LD[9..|M.vw...E.

0x0010: 0054 823f 0000 ff01 b6a1 c0a8 00b8 c0a8 .T.?............

0x0020: 00bf 0000 cb1d 1e70 001c ea4e 6b67 0000 .......p...Nkg..

0x0030: 0000 facc 0700 0000 0000 1011 1213 1415 ................

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:43.513028 IP ttsypyshev-Modern-14-B11MOU.Dlink > HP7C4D8F7677F4.Dlink: ICMP echo request, id 7792, seq 29, length 64

0x0000: 7c4d 8f76 77f4 4c44 5b39 8415 0800 4500 |M.vw.LD[9....E.

0x0010: 0054 86fe 4000 4001 30e3 c0a8 00bf c0a8 .T..@.@.0.......

0x0020: 00b8 0800 d915 1e70 001d eb4e 6b67 0000 .......p...Nkg..

0x0030: 0000 e3d3 0700 0000 0000 1011 1213 1415 ................

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:43.516361 IP HP7C4D8F7677F4.Dlink > ttsypyshev-Modern-14-B11MOU.Dlink: ICMP echo reply, id 7792, seq 29, length 64

0x0000: 4c44 5b39 8415 7c4d 8f76 77f4 0800 4500 LD[9..|M.vw...E.

0x0010: 0054 8917 0000 ff01 afc9 c0a8 00b8 c0a8 .T..............

0x0020: 00bf 0000 e115 1e70 001d eb4e 6b67 0000 .......p...Nkg..

0x0030: 0000 e3d3 0700 0000 0000 1011 1213 1415 ................

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:44.514783 IP ttsypyshev-Modern-14-B11MOU.Dlink > HP7C4D8F7677F4.Dlink: ICMP echo request, id 7792, seq 30, length 64

0x0000: 7c4d 8f76 77f4 4c44 5b39 8415 0800 4500 |M.vw.LD[9....E.

0x0010: 0054 8917 4000 4001 2eca c0a8 00bf c0a8 .T..@.@.........

0x0020: 00b8 0800 fe0d 1e70 001e ec4e 6b67 0000 .......p...Nkg..

0x0030: 0000 bdda 0700 0000 0000 1011 1213 1415 ................

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:44.520039 IP HP7C4D8F7677F4.Dlink > ttsypyshev-Modern-14-B11MOU.Dlink: ICMP echo reply, id 7792, seq 30, length 64

0x0000: 4c44 5b39 8415 7c4d 8f76 77f4 0800 4500 LD[9..|M.vw...E.

0x0010: 0054 8cef 0000 ff01 abf1 c0a8 00b8 c0a8 .T..............

0x0020: 00bf 0000 060e 1e70 001e ec4e 6b67 0000 .......p...Nkg..

0x0030: 0000 bdda 0700 0000 0000 1011 1213 1415 ................

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:45.516422 IP ttsypyshev-Modern-14-B11MOU.Dlink > HP7C4D8F7677F4.Dlink: ICMP echo request, id 7792, seq 31, length 64

0x0000: 7c4d 8f76 77f4 4c44 5b39 8415 0800 4500 |M.vw.LD[9....E.

0x0010: 0054 8b8d 4000 4001 2c54 c0a8 00bf c0a8 .T..@.@.,T......

0x0020: 00b8 0800 9606 1e70 001f ed4e 6b67 0000 .......p...Nkg..

0x0030: 0000 24e1 0700 0000 0000 1011 1213 1415 ..$.............

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

03:16:45.524016 IP HP7C4D8F7677F4.Dlink > ttsypyshev-Modern-14-B11MOU.Dlink: ICMP echo reply, id 7792, seq 31, length 64

0x0000: 4c44 5b39 8415 7c4d 8f76 77f4 0800 4500 LD[9..|M.vw...E.

0x0010: 0054 94d7 0000 ff01 a409 c0a8 00b8 c0a8 .T..............

0x0020: 00bf 0000 9e06 1e70 001f ed4e 6b67 0000 .......p...Nkg..

0x0030: 0000 24e1 0700 0000 0000 1011 1213 1415 ..$.............

0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 ...........!"#$%

0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()\*+,-./012345

0x0060: 3637 67

8 packets captured

8 packets received by filter

0 packets dropped by kernel

Используйте ping, чтобы сгенерировать ICMP-запросы на лабораторный ПК.

### 4. Перехват трафика утилиты traceroute

Для перехвата трафика, генерируемого утилитой traceroute, сначала получите IP-адрес узла с помощью утилиты nslookup:

nslookup <domain\_name>

Затем используйте команду tcpdump для перехвата трафика traceroute:

sudo tcpdump -c 7 udp and host <IP-адрес узла> -X

* udp — фильтрует трафик UDP, который используется утилитой traceroute.

listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes

03:20:25.455925 IP ttsypyshev-Modern-14-B11MOU.Dlink.52456 > lo-in-f139.1e100.net.33434: UDP, length 32

0x0000: 4500 003c 748e 0000 0111 f76d c0a8 00bf E..<t......m....

0x0010: adc2 de8b cce8 829a 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.455978 IP ttsypyshev-Modern-14-B11MOU.Dlink.35194 > lo-in-f139.1e100.net.33435: UDP, length 32

0x0000: 4500 003c 28b8 0000 0111 4344 c0a8 00bf E..<(.....CD....

0x0010: adc2 de8b 897a 829b 0028 4def 4041 4243 .....z...(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456001 IP ttsypyshev-Modern-14-B11MOU.Dlink.52220 > lo-in-f139.1e100.net.33436: UDP, length 32

0x0000: 4500 003c c8b4 0000 0111 a347 c0a8 00bf E..<.......G....

0x0010: adc2 de8b cbfc 829c 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456023 IP ttsypyshev-Modern-14-B11MOU.Dlink.60432 > lo-in-f139.1e100.net.33437: UDP, length 32

0x0000: 4500 003c 4fdf 0000 0211 1b1d c0a8 00bf E..<O...........

0x0010: adc2 de8b ec10 829d 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456045 IP ttsypyshev-Modern-14-B11MOU.Dlink.53439 > lo-in-f139.1e100.net.33438: UDP, length 32

0x0000: 4500 003c 1946 0000 0211 51b6 c0a8 00bf E..<.F....Q.....

0x0010: adc2 de8b d0bf 829e 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456067 IP ttsypyshev-Modern-14-B11MOU.Dlink.33820 > lo-in-f139.1e100.net.33439: UDP, length 32

0x0000: 4500 003c a1e2 0000 0211 c919 c0a8 00bf E..<............

0x0010: adc2 de8b 841c 829f 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456089 IP ttsypyshev-Modern-14-B11MOU.Dlink.52950 > lo-in-f139.1e100.net.33440: UDP, length 32

0x0000: 4500 003c 4e3a 0000 0311 1bc2 c0a8 00bf E..<N:..........

0x0010: adc2 de8b ced6 82a0 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

7 packets captured

34 packets received by filter

0 packets dropped by kernel

### 5. Перехват пакетов TCP с флагом SYN

Для отбора TCP-сегментов с флагом SYN, используйте команду:

sudo tcpdump -c 2 -lvnnSXX 'tcp[tcpflags] & tcp-syn != 0'

* -c 2 — захватить только два пакета.
* 'tcp[tcpflags] & tcp-syn != 0' — фильтрует пакеты, где установлен флаг SYN.
* -S — отображает реальные номера последовательности.
* -X — выводит данные пакета в шестнадцатеричной и ASCII формах.

>....

03:20:25.455925 IP ttsypyshev-Modern-14-B11MOU.Dlink.52456 > lo-in-f139.1e100.net.33434: UDP, length 32

0x0000: 4500 003c 748e 0000 0111 f76d c0a8 00bf E..<t......m....

0x0010: adc2 de8b cce8 829a 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.455978 IP ttsypyshev-Modern-14-B11MOU.Dlink.35194 > lo-in-f139.1e100.net.33435: UDP, length 32

0x0000: 4500 003c 28b8 0000 0111 4344 c0a8 00bf E..<(.....CD....

0x0010: adc2 de8b 897a 829b 0028 4def 4041 4243 .....z...(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456001 IP ttsypyshev-Modern-14-B11MOU.Dlink.52220 > lo-in-f139.1e100.net.33436: UDP, length 32

0x0000: 4500 003c c8b4 0000 0111 a347 c0a8 00bf E..<.......G....

0x0010: adc2 de8b cbfc 829c 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456023 IP ttsypyshev-Modern-14-B11MOU.Dlink.60432 > lo-in-f139.1e100.net.33437: UDP, length 32

0x0000: 4500 003c 4fdf 0000 0211 1b1d c0a8 00bf E..<O...........

0x0010: adc2 de8b ec10 829d 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456045 IP ttsypyshev-Modern-14-B11MOU.Dlink.53439 > lo-in-f139.1e100.net.33438: UDP, length 32

0x0000: 4500 003c 1946 0000 0211 51b6 c0a8 00bf E..<.F....Q.....

0x0010: adc2 de8b d0bf 829e 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456067 IP ttsypyshev-Modern-14-B11MOU.Dlink.33820 > lo-in-f139.1e100.net.33439: UDP, length 32

0x0000: 4500 003c a1e2 0000 0211 c919 c0a8 00bf E..<............

0x0010: adc2 de8b 841c 829f 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

03:20:25.456089 IP ttsypyshev-Modern-14-B11MOU.Dlink.52950 > lo-in-f139.1e100.net.33440: UDP, length 32

0x0000: 4500 003c 4e3a 0000 0311 1bc2 c0a8 00bf E..<N:..........

0x0010: adc2 de8b ced6 82a0 0028 4def 4041 4243 .........(M.@ABC

0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS

0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^\_

7 packets captured

34 packets received by filter

0 packets dropped by kernel

### 6. Отбор дейтаграмм UDP между ПК и сервером на портах DNS и диапазоне 10000–65535

Для фильтрации UDP-пакетов между локальным ПК и сервером, отправленных с порта DNS (порт 53), на диапазон портов назначения 10000–65535:

sudo tcpdump -c 10 udp and src port 53 and dst portrange 10000-65535

* src port 53 — фильтрует по исходному порту DNS.
* dst portrange 10000-65535 — фильтрует по диапазону портов назначения.

03:24:02.200486 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.57004: 47313 3/0/1 CNAME detectportal.prod.mozaws.net., CNAME prod.detectportal.prod.cloudops.mozgcp.net., A 34.107.221.82 (167)

03:24:02.259484 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.54923: 9613 1/0/1 A 93.184.215.14 (56)

03:24:02.262173 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.47409: 15382 1/0/1 HTTPS (120)

03:24:02.262179 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.43086: 44062 1/0/1 AAAA 2606:2800:21f:cb07:6820:80da:af6b:8b2c (68)

03:24:02.266308 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.42444: 13527 2/0/1 A 192.0.0.170, A 192.0.0.171 (74)

03:24:02.268398 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.46839: 45911 0/1/1 (99)

03:24:02.268398 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.37648: 22219 1/0/1 AAAA 2600:1901:0:38d7:: (99)

03:24:03.369050 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.35091: 25322 1/0/1 A 76.76.2.22 (61)

03:24:03.485950 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.52373: 63747 NXDomain 0/1/1 (142)

03:24:03.486767 IP6 fe80::a2ab:1bff:fe30:f46.domain > ttsypyshev-Modern-14-B11MOU.39024: 6996 NXDomain 0/1/1 (142)

10 packets captured

12 packets received by filter

0 packets dropped by kernel

### 7. Отбор дейтаграмм TCP с исходным портом менее 1024

Для отбора TCP-пакетов, исходящие порты которых меньше 1024, используйте:

sudo tcpdump -c 2 'tcp and src portrange 1-1023'

* src port <1024 — фильтрует по исходным портам менее 1024.

03:25:12.843950 IP dlinkrouter.Dlink.http > ttsypyshev-Modern-14-B11MOU.Dlink.44404: Flags [S.], seq 1314790735, ack 3738168633, win 14480, options [mss 1460,nop,nop,TS val 13914019 ecr 1872172244,nop,wscale 3], length 0

03:25:12.846508 IP dlinkrouter.Dlink.http > ttsypyshev-Modern-14-B11MOU.Dlink.44404: Flags [.], ack 460, win 1944, options [nop,nop,TS val 13914020 ecr 1872172251], length 0

2 packets captured

5 packets received by filter

0 packets dropped by kernel

### 8. Отбор дейтаграмм с портами назначения больше 1024

Для отбора пакетов с номерами портов назначения, превышающими 1024, используйте:

sudo tcpdump -c 2 '(tcp or udp) and dst portrange 1025-65535'

* dst port > 1024 — фильтрует по портам назначения, большими 1024.

03:26:46.322731 IP 206.253.89.88.https > ttsypyshev-Modern-14-B11MOU.Dlink.55500: Flags [.], ack 594918022, win 21, options [nop,nop,TS val 1693288547 ecr 1070131005], length 0

03:26:46.358180 IP dlinkrouter.Dlink.http > ttsypyshev-Modern-14-B11MOU.Dlink.43942: Flags [S.], seq 572375827, ack 3407497231, win 14480, options [mss 1460,nop,nop,TS val 13923337 ecr 1872265763,nop,wscale 3], length 0

2 packets captured

9 packets received by filter

0 packets dropped by kernel

### 9. Отбор UDP-пакетов с размером от 50 до 100 байт

Чтобы отобрать UDP-пакеты, размер которых больше 50 байт, но не превышает 100 байт:

sudo tcpdump -c 10 udp and greater 50 and less 100

* greater 50 — фильтрует пакеты больше 50 байт.
* less 100 — фильтрует пакеты меньше 100 байт.

03:27:32.026373 IP ttsypyshev-Modern-14-B11MOU.Dlink.35827 > 168.207.110.34.bc.googleusercontent.com.https: UDP, length 31

03:27:32.048918 IP 168.207.110.34.bc.googleusercontent.com.https > ttsypyshev-Modern-14-B11MOU.Dlink.35827: UDP, length 31

03:27:32.049262 IP ttsypyshev-Modern-14-B11MOU.Dlink.35827 > 168.207.110.34.bc.googleusercontent.com.https: UDP, length 31

03:27:32.369008 IP ttsypyshev-Modern-14-B11MOU.Dlink.35827 > 168.207.110.34.bc.googleusercontent.com.https: UDP, length 37

03:27:32.408292 IP 168.207.110.34.bc.googleusercontent.com.https > ttsypyshev-Modern-14-B11MOU.Dlink.35827: UDP, length 27

03:27:32.436416 IP ttsypyshev-Modern-14-B11MOU.Dlink.51176 > waw02s22-in-f1.1e100.net.https: UDP, length 40

03:27:32.452898 IP ttsypyshev-Modern-14-B11MOU.Dlink.51176 > waw02s22-in-f1.1e100.net.https: UDP, length 42

03:27:32.474115 IP ttsypyshev-Modern-14-B11MOU.Dlink.51176 > waw02s22-in-f1.1e100.net.https: UDP, length 44

03:27:32.477799 IP ttsypyshev-Modern-14-B11MOU.Dlink.51176 > waw02s22-in-f1.1e100.net.https: UDP, length 44

03:27:32.516545 IP ttsypyshev-Modern-14-B11MOU.Dlink.51176 > waw02s22-in-f1.1e100.net.https: UDP, length 47

10 packets captured

12 packets received by filter

0 packets dropped by kernel

### 10. Отбор IP-пакетов TCP с исходным портом менее 1024 и портом назначения более 10000, размером до 100 байт

Для отбора таких пакетов:

sudo tcpdump -c 2 'ip and tcp and src portrange 0-1023 and dst portrange 10000-65535 and less 100'

* src port <1024 — фильтрует по исходному порту меньше 1024.
* dst port >10000 — фильтрует по порту назначения больше 10000.
* less 100 — фильтрует по размеру пакетов меньше 100 байт.

03:29:15.219906 IP dlinkrouter.Dlink.http > ttsypyshev-Modern-14-B11MOU.Dlink.53394: Flags [.], ack 1956445712, win 1944, options [nop,nop,TS val 13938135 ecr 1872414623], length 0

03:29:15.988511 IP dlinkrouter.Dlink.http > ttsypyshev-Modern-14-B11MOU.Dlink.53408: Flags [S.], seq 2055158868, ack 140620388, win 14480, options [mss 1460,nop,nop,TS val 13938212 ecr 1872415392,nop,wscale 3], length 0

2 packets captured

4 packets received by filter

0 packets dropped by kernel

### TCP (Transmission Control Protocol)

TCP — протокол транспортного уровня в модели TCP/IP, обеспечивающий надежную передачу данных между приложениями. Он использует механизмы установления соединения, управления потоком, восстановления после ошибок и завершения соединения.

### Установление соединения: Три рукопожатия (3-way handshake)

Процесс три этапа:

1. **SYN** (synchronize): Клиент отправляет серверу сегмент с установленным флагом SYN, инициируя запрос на установление соединения.
   * Этот сегмент содержит начальный номер последовательности (ISN, Initial Sequence Number).
2. **SYN-ACK** (synchronize-acknowledge): Сервер отвечает, отправляя сегмент с флагами SYN и ACK.
   * Сервер указывает свой ISN и подтверждает получение ISN клиента.
3. **ACK** (acknowledge): Клиент подтверждает получение SYN-ACK сервера, устанавливая флаг ACK.

После этого соединение считается установленным.

### Завершение соединения (4-way handshake)

Процесс закрытия соединения TCP состоит из четырех шагов:

1. **FIN** (finish): Одна из сторон (обычно клиент) отправляет сегмент с флагом FIN, указывая на завершение передачи данных.
2. **ACK** (acknowledge): Другая сторона подтверждает получение FIN, отправляя сегмент с флагом ACK.
3. **FIN**: Сторона, подтвердившая получение FIN, отправляет свой сегмент с флагом FIN, завершая передачу данных с её стороны.
4. **ACK**: Первая сторона отправляет подтверждение (ACK), завершая соединение.

Как вы можете заметить, для завершения соединения потребовалось четыре сегмента, а не три, как в случае с рукопожатием. Схема выглядит чуть иначе, потому что при завершении соединения, собеседник (в нашем случае сервер) должен сперва уведомить приложение, использующее TCP, о том, что соединение вот-вот завершится. И когда это приложение будет готово к завершению, тогда TCP собеседника отправит свой FIN-пакет.

#### Почему нельзя обойтись 3 шагами?

Если завершение происходило бы за 3 шага, это могло бы привести к следующим проблемам:

* Потеря данных: Один из узлов может не успеть передать все данные перед закрытием соединения.
* Несогласованность: Узлы могли бы находиться в разных состояниях относительно завершения соединения, что создало бы неустойчивость и ошибки.

### Флаги TCP

В протоколе TCP (Transmission Control Protocol) флаги — это специальные поля в заголовке TCP-пакета, которые управляют состоянием соединения, синхронизацией и передачей данных. Каждое соединение TCP — это последовательность событий, которые управляются с помощью этих флагов.

TCP использует следующие флаги:

1. **SYN**: Инициация соединения.
2. **ACK**: Подтверждение получения данных.
3. **FIN**: Завершение соединения.
4. **RST**: Сброс соединения.
5. **PSH**: Принудительная передача данных, игнорируя буферизацию.
6. **URG**: Указывает, что данные являются срочными.
7. **ECE** и **CWR**: Используются для управления перегрузкой (в контексте ECN — Explicit Congestion Notification).

### Фильтрация по конкретным флагам:

**SYN**:  
tcpdump 'tcp[tcpflags] & tcp-syn != 0'

**ACK**:  
tcpdump 'tcp[tcpflags] & tcp-ack != 0'

**FIN**:  
tcpdump 'tcp[tcpflags] & tcp-fin != 0'

**RST**:  
tcpdump 'tcp[tcpflags] & tcp-rst != 0'

**PSH**:  
sudo tcpdump -i enp0s3 'tcp[13] & 8 != 0'

**URG**:  
tcpdump 'tcp[tcpflags] & tcp-urg != 0'

Показ всех пакетов с установленными флагами SYN и ACK:

tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-ack) == (tcp-syn|tcp-ack)'

### Заключение

В ходе лабораторной работы были продемонстрированы различные методы фильтрации и анализа сетевых пакетов с использованием инструмента tcpdump. Особое внимание было уделено фильтрации по флагам, размерам пакетов и портам, что позволяет эффективно анализировать сетевой трафик и выявлять важные особенности работы протоколов TCP и UDP.