

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА



Институт радиоэлектроники и информационных технологий
Кафедра вычислительные системы и технологии

Лабораторная работа № 5

ОТЧЕТ

по лабораторной работе

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

_____ Гай В.Е.

СТУДЕНТ:

_____ Сапожников В.О.
19-В-1

Работа защищена «__» _____

С оценкой _____

Нижний Новгород 2021

Задание

Работа с анализатором протоколов tcpdump

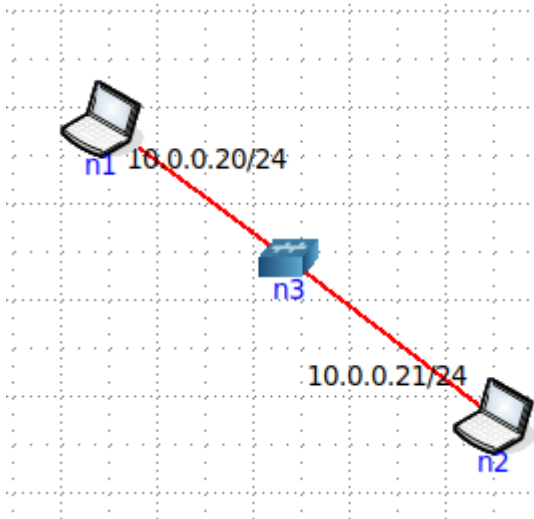
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.
2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).
3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.
5. Прочитать программой tcpdump созданный в предыдущем пункте файл.
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

Работа с анализатором протоколов wireshark

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.
3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.
4. Прочитать файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

Tcpdump

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



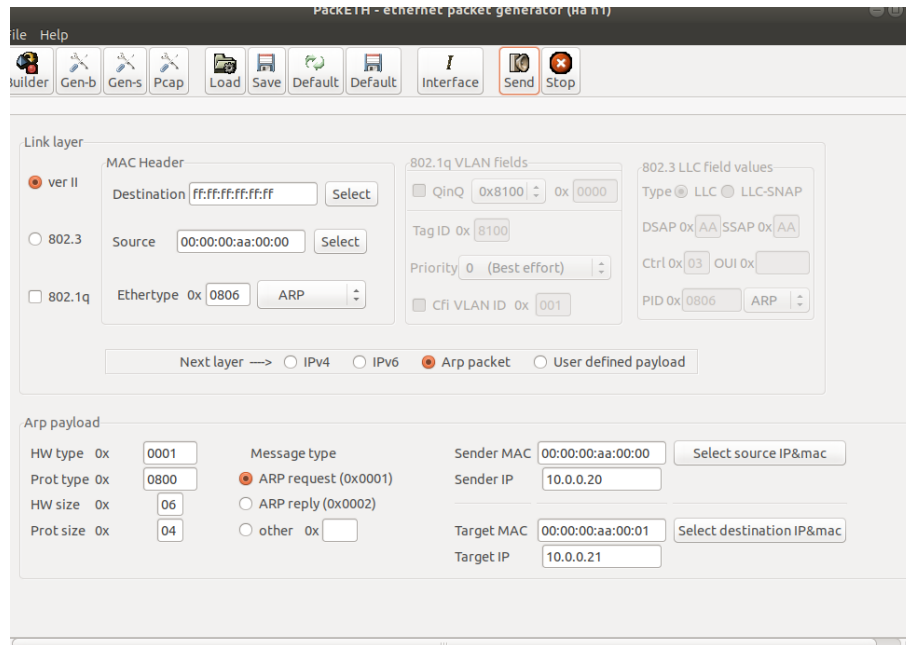
```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.43895/n1.conf# ping 10.0.0.21
PING 10.0.0.21 (10.0.0.21) 56(84) bytes of data:
 64 bytes from 10.0.0.21: icmp_seq=1 ttl=64 time=0.040 ms
 64 bytes from 10.0.0.21: icmp_seq=2 ttl=64 time=0.091 ms
 64 bytes from 10.0.0.21: icmp_seq=3 ttl=64 time=0.048 ms
 64 bytes from 10.0.0.21: icmp_seq=4 ttl=64 time=0.042 ms
 64 bytes from 10.0.0.21: icmp_seq=5 ttl=64 time=0.045 ms
 64 bytes from 10.0.0.21: icmp_seq=6 ttl=64 time=0.050 ms
 64 bytes from 10.0.0.21: icmp_seq=7 ttl=64 time=0.037 ms
 64 bytes from 10.0.0.21: icmp_seq=8 ttl=64 time=0.046 ms
 64 bytes from 10.0.0.21: icmp_seq=9 ttl=64 time=0.038 ms
 64 bytes from 10.0.0.21: icmp_seq=10 ttl=64 time=0.037 ms
 64 bytes from 10.0.0.21: icmp_seq=11 ttl=64 time=0.036 ms
 64 bytes from 10.0.0.21: icmp_seq=12 ttl=64 time=0.097 ms
 64 bytes from 10.0.0.21: icmp_seq=13 ttl=64 time=0.042 ms
 64 bytes from 10.0.0.21: icmp_seq=14 ttl=64 time=0.035 ms
 64 bytes from 10.0.0.21: icmp_seq=15 ttl=64 time=0.037 ms
 64 bytes from 10.0.0.21: icmp_seq=16 ttl=64 time=0.050 ms
 64 bytes from 10.0.0.21: icmp_seq=17 ttl=64 time=0.048 ms
 64 bytes from 10.0.0.21: icmp_seq=18 ttl=64 time=0.051 ms
^Z
[1]+  Остановлен    ping 10.0.0.21
root@n1:/tmp/pycore.43895/n1.conf#
```

-c <число> - tcpdump завершит работу после получения указанного числа пакетов

```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.43895/n2.conf# tcpdump -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
09:46:48.442630 IP 10.0.0.20 > n2: ICMP echo request, id 39, seq 3, length 64
09:46:48.442646 IP n2 > 10.0.0.20: ICMP echo reply, id 39, seq 3, length 64
09:46:49.466579 IP 10.0.0.20 > n2: ICMP echo request, id 39, seq 4, length 64
09:46:49.466594 IP n2 > 10.0.0.20: ICMP echo reply, id 39, seq 4, length 64
09:46:50.490641 IP 10.0.0.20 > n2: ICMP echo request, id 39, seq 5, length 64
09:46:50.490658 IP n2 > 10.0.0.20: ICMP echo reply, id 39, seq 5, length 64
09:46:51.514630 IP 10.0.0.20 > n2: ICMP echo request, id 39, seq 6, length 64
09:46:51.514646 IP n2 > 10.0.0.20: ICMP echo reply, id 39, seq 6, length 64
09:46:51.578531 ARP, Request who-has 10.0.0.20 tell n2, length 28
09:46:51.578637 ARP, Request who-has n2 tell 10.0.0.20, length 28
10 packets captured
12 packets received by filter
0 packets dropped by kernel
root@n2:/tmp/pycore.43895/n2.conf#
```

2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

Для создания широковещательного потока воспользуемся утилитой packETH



Широковещательный MAC адрес: `ff:ff:ff:ff:ff:ff`

`ether dst <ehost>` - будут выбираться все кадры, в которых поле MAC адресов получателя содержат значения `ehost`

-xx распечатка пакета в шестнадцатеричной системе

```
root@n2:/tmp/pycore.43895/n2.conf# tcpdump -c 5 ether dst ff:ff:ff:ff:ff:ff -xx
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:26:10.309863 ARP, Request who-has n2 (00:00:00:aa:00:01 (oui Ethernet)) tell 10.0.0.20,
length 46
  0x0000:  ffff ffff ffff 0000 00aa 0000 0806 0001
  0x0010:  0800 0604 0001 0000 00aa 0000 0a00 0014
  0x0020:  0000 00aa 0001 0a00 0015 0000 0000 0000
  0x0030:  0000 0000 0000 0000 0000 0000
10:26:10.678034 ARP, Request who-has n2 (00:00:00:aa:00:01 (oui Ethernet)) tell 10.0.0.20,
length 46
  0x0000:  ffff ffff ffff 0000 00aa 0000 0806 0001
  0x0010:  0800 0604 0001 0000 00aa 0000 0a00 0014
  0x0020:  0000 00aa 0001 0a00 0015 0000 0000 0000
  0x0030:  0000 0000 0000 0000 0000 0000
10:26:11.038012 ARP, Request who-has n2 (00:00:00:aa:00:01 (oui Ethernet)) tell 10.0.0.20,
length 46
  0x0000:  ffff ffff ffff 0000 00aa 0000 0806 0001
  0x0010:  0800 0604 0001 0000 00aa 0000 0a00 0014
  0x0020:  0000 00aa 0001 0a00 0015 0000 0000 0000
  0x0030:  0000 0000 0000 0000 0000 0000
10:26:11.398046 ARP, Request who-has n2 (00:00:00:aa:00:01 (oui Ethernet)) tell 10.0.0.20,
length 46
  0x0000:  ffff ffff ffff 0000 00aa 0000 0806 0001
  0x0010:  0800 0604 0001 0000 00aa 0000 0a00 0014
  0x0020:  0000 00aa 0001 0a00 0015 0000 0000 0000
  0x0030:  0000 0000 0000 0000 0000 0000
10:26:11.757620 ARP, Request who-has n2 (00:00:00:aa:00:01 (oui Ethernet)) tell 10.0.0.20,
length 46
  0x0000:  ffff ffff ffff 0000 00aa 0000 0806 0001
  0x0010:  0800 0604 0001 0000 00aa 0000 0a00 0014
  0x0020:  0000 00aa 0001 0a00 0015 0000 0000 0000
  0x0030:  0000 0000 0000 0000 0000 0000
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@n2:/tmp/pycore.43895/n2.conf#
```

3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

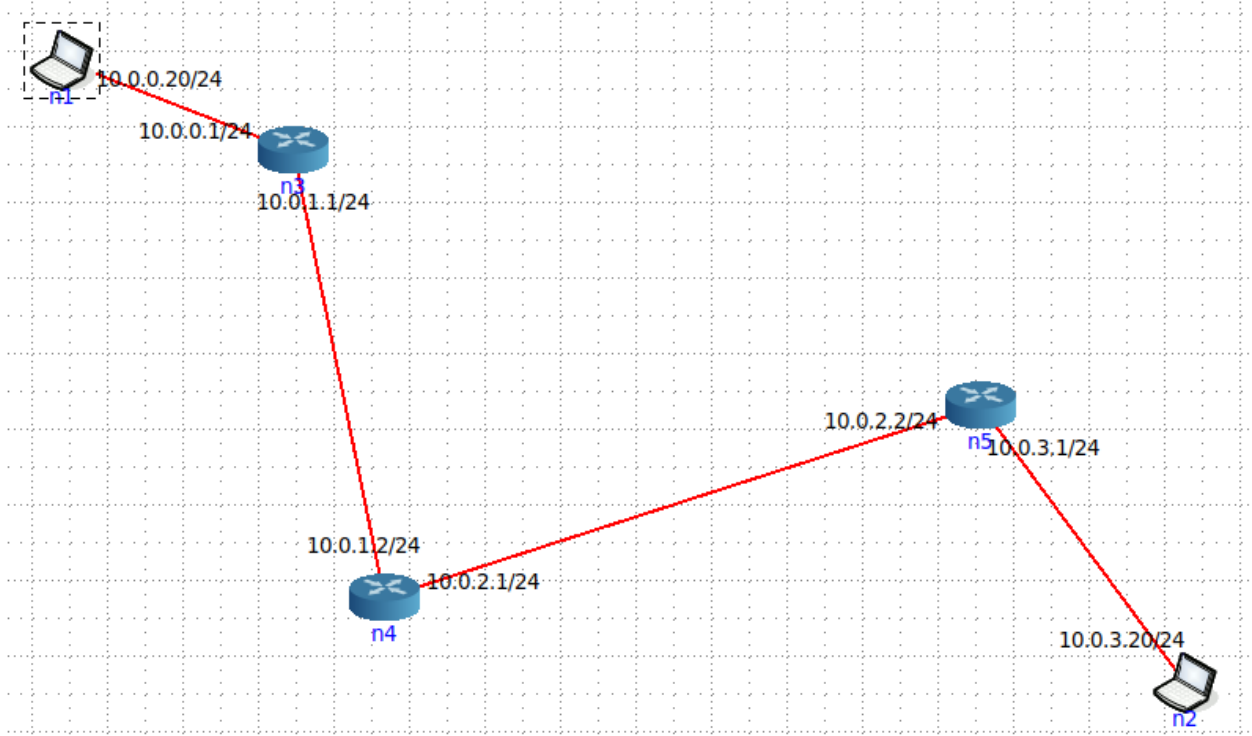
-c <число> - tcpdump завершит работу после получения указанного числа пакетов

-XX выводит пакет в ASCII и hex формате.

"dst host <хост> and ip proto \icmp" –перехватить пакеты ICMP на хост

```
.<.conf# tcpdump -c 3 -XX 'dst host 10.0.0.21 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:43:39.263833 IP 10.0.0.20 > n2: ICMP echo request, id 59, seq 1, length 64
0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
0x0010: 0054 c437 4000 4001 6249 0a00 0014 0a00 .T.7@.@.bI.....
0x0020: 0015 0800 02ba 003b 0001 abce 1d62 0000 .....;.....b..
0x0030: 0000 6906 0400 0000 0000 1011 1213 1415 ..i.....
0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!".$%
0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
0x0060: 3637 67
10:43:40.265726 IP 10.0.0.20 > n2: ICMP echo request, id 59, seq 2, length 64
0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
0x0010: 0054 c4e7 4000 4001 6199 0a00 0014 0a00 .T..@.@.a.....
0x0020: 0015 0800 b2b1 003b 0002 acce 1d62 0000 .....;.....b..
0x0030: 0000 b80d 0400 0000 0000 1011 1213 1415 .....
0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!".$%
0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
0x0060: 3637 67
10:43:41.274555 IP 10.0.0.20 > n2: ICMP echo request, id 59, seq 3, length 64
0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
0x0010: 0054 c4f9 4000 4001 6187 0a00 0014 0a00 .T..@.@.a.....
0x0020: 0015 0800 088e 003b 0003 adce 1d62 0000 .....;.....b..
0x0030: 0000 6130 0400 0000 0000 1011 1213 1415 ..a0.....
0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!".$%
0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
0x0060: 3637 67
3 packets captured
3 packets received by filter
0 packets dropped by kernel
root@n2:/tmp/pycore.43895/n2.conf#
```

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.



Отправка 7 ICMP пакетов при помощи traceroute

```

11:18 Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.43895/n2.conf# traceroute -q 7 -I 10.0.0.20
traceroute to 10.0.0.20 (10.0.0.20), 64 hops max
 1  10.0.3.1  0,002ms  0,002ms  0,002ms  0,002ms  0,002ms  0,002ms  0,002ms  *
 2  10.0.2.1  0,002ms  0,002ms  0,001ms  0,001ms  0,001ms  0,001ms  0,001ms  *
 3  10.0.1.1  0,010ms  0,007ms  0,007ms  0,012ms  0,511ms  0,008ms  0,008ms  *
 4  10.0.0.20 0,010ms  0,008ms  0,007ms  0,011ms  0,008ms  0,008ms  0,007ms
root@n2:/tmp/pycore.43895/n2.conf#
  
```

Запись пакетов

-w сохраняет данные tcpdump в двоичном формате.

```

Терминал
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.43895/n1.conf# tcpdump -c 7 -w lab1.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
7 packets captured
19 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.43895/n1.conf#
  
```


5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

```
root@n1:/tmp/pycore.43895/n1.conf# tcpdump -r lab1.cap -XX
reading from file lab1.cap, link-type EN10MB (Ethernet)
11:18:31.871012 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
    0x0000:  0100 5e00 0005 0000 00aa 0001 0800 45c0  ..^.....E.
    0x0010:  0040 d6e1 0000 0159 f7bd 0a00 0001 e000  .@.....Y.....
    0x0020:  0005 0201 002c 0a00 0001 0000 0000 f1c8  .....,.....
    0x0030:  0000 0000 0000 0000 0000 0000 0000 0002  .....
    0x0040:  0201 0000 0006 0000 0000 0000 0000  .....
11:18:33.871216 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
    0x0000:  0100 5e00 0005 0000 00aa 0001 0800 45c0  ..^.....E.
    0x0010:  0040 d6e3 0000 0159 f7bb 0a00 0001 e000  .@.....Y.....
    0x0020:  0005 0201 002c 0a00 0001 0000 0000 f1c8  .....,.....
    0x0030:  0000 0000 0000 0000 0000 0000 0000 0002  .....
    0x0040:  0201 0000 0006 0000 0000 0000 0000  .....
11:18:35.872303 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
    0x0000:  0100 5e00 0005 0000 00aa 0001 0800 45c0  ..^.....E.
    0x0010:  0040 d6e5 0000 0159 f7b9 0a00 0001 e000  .@.....Y.....
    0x0020:  0005 0201 002c 0a00 0001 0000 0000 f1c8  .....,.....
    0x0030:  0000 0000 0000 0000 0000 0000 0000 0002  .....
    0x0040:  0201 0000 0006 0000 0000 0000 0000  .....
11:18:37.872642 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
    0x0000:  0100 5e00 0005 0000 00aa 0001 0800 45c0  ..^.....E.
    0x0010:  0040 d6e7 0000 0159 f7b7 0a00 0001 e000  .@.....Y.....
    0x0020:  0005 0201 002c 0a00 0001 0000 0000 f1c8  .....,.....
    0x0030:  0000 0000 0000 0000 0000 0000 0000 0002  .....
    0x0040:  0201 0000 0006 0000 0000 0000 0000  .....
11:18:38.715152 IP 10.0.3.20 > n1: ICMP echo request, id 80, seq 21, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  .....E.
    0x0010:  0034 300c 4000 0101 3296 0a00 0314 0a00  .40.@...2.....
    0x0020:  0014 0800 f423 0050 0015 0800 0000 0000  .....#.P.....
    0x0030:  0000 0700 0000 0000 0000 c044 deb2 557f  .....D..U.
    0x0040:  0000  .....
11:18:38.715351 IP 10.0.3.20 > n1: ICMP echo request, id 80, seq 22, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  .....E.
    0x0010:  0034 300d 4000 0101 3295 0a00 0314 0a00  .40.@...2.....
    0x0020:  0014 0800 4fdd 0050 0016 f8b7 86b2 557f  ....0..P.....U.
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a  ..ZZZZZZZZZZZZZZ
    0x0040:  5a5a  ZZ
root@n1:/tmp/pycore.43895/n1.conf#
```

-r читает данные tcpdump в двоичном формате, сохранённые ранее при использовании ключа -w

6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ARP, отправленные на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой ping. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 5.

```
root@n2:/tmp/pycore.43895/n2.conf# ping 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=64 time=1.45 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=64 time=0.176 ms
64 bytes from 10.0.0.20: icmp_seq=3 ttl=64 time=0.098 ms
64 bytes from 10.0.0.20: icmp_seq=4 ttl=64 time=0.117 ms
64 bytes from 10.0.0.20: icmp_seq=5 ttl=64 time=0.114 ms
64 bytes from 10.0.0.20: icmp_seq=6 ttl=64 time=0.115 ms
64 bytes from 10.0.0.20: icmp_seq=7 ttl=64 time=0.109 ms
64 bytes from 10.0.0.20: icmp_seq=8 ttl=64 time=0.106 ms
64 bytes from 10.0.0.20: icmp_seq=9 ttl=64 time=0.111 ms
64 bytes from 10.0.0.20: icmp_seq=10 ttl=64 time=0.103 ms
64 bytes from 10.0.0.20: icmp_seq=11 ttl=64 time=0.116 ms
64 bytes from 10.0.0.20: icmp_seq=12 ttl=64 time=0.111 ms
64 bytes from 10.0.0.20: icmp_seq=13 ttl=64 time=0.063 ms
64 bytes from 10.0.0.20: icmp_seq=14 ttl=64 time=0.068 ms
64 bytes from 10.0.0.20: icmp_seq=15 ttl=64 time=0.071 ms
64 bytes from 10.0.0.20: icmp_seq=16 ttl=64 time=0.110 ms
64 bytes from 10.0.0.20: icmp_seq=17 ttl=64 time=0.043 ms
64 bytes from 10.0.0.20: icmp_seq=18 ttl=64 time=0.046 ms
64 bytes from 10.0.0.20: icmp_seq=19 ttl=64 time=0.117 ms
64 bytes from 10.0.0.20: icmp_seq=20 ttl=64 time=0.110 ms
64 bytes from 10.0.0.20: icmp_seq=21 ttl=64 time=0.114 ms
```

```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.43895/n1.conf# tcpdump -c 5 -XX 'ether proto \arp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:37:08.900892 ARP, Request who-has n1 tell 10.0.0.21, length 28
    0x0000:  ffff ffff ffff 0000 00aa 0001 0806 0001  .....
    0x0010:  0800 0604 0001 0000 00aa 0001 0a00 0015  .....
    0x0020:  0000 0000 0000 0a00 0014  .....
11:37:08.900907 ARP, Reply n1 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
    0x0000:  0000 00aa 0001 0000 00aa 0000 0806 0001  .....
    0x0010:  0800 0604 0002 0000 00aa 0000 0a00 0014  .....
    0x0020:  0000 00aa 0001 0a00 0015  .....
11:37:14.042977 ARP, Request who-has 10.0.0.21 tell n1, length 28
    0x0000:  0000 00aa 0001 0000 00aa 0000 0806 0001  .....
    0x0010:  0800 0604 0001 0000 00aa 0000 0a00 0014  .....
    0x0020:  0000 0000 0000 0a00 0015  .....
11:37:14.043096 ARP, Reply 10.0.0.21 is-at 00:00:00:aa:00:01 (oui Ethernet), length 28
    0x0000:  0000 00aa 0000 0000 00aa 0001 0806 0001  .....
    0x0010:  0800 0604 0002 0000 00aa 0001 0a00 0015  .....
    0x0020:  0000 00aa 0000 0a00 0014  .....
11:37:32.475006 ARP, Request who-has n1 tell 10.0.0.21, length 28
    0x0000:  0000 00aa 0000 0000 00aa 0001 0806 0001  .....
    0x0010:  0800 0604 0001 0000 00aa 0001 0a00 0015  .....
    0x0020:  0000 0000 0000 0a00 0014  .....
5 packets captured
6 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.43895/n1.conf#
```


Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, отправленные на определенный IP-адрес. Количество захватываемых пакетов ограничить 7. Для генерирования пакетов воспользоваться утилитой traceroute.

```
root@n2:/tmp/pycore.43895/n2.conf# traceroute -q 7 10.0.1.20
traceroute to 10.0.1.20 (10.0.1.20), 64 hops max
 1  10.0.3.1  0,003ms  0,002ms  0,002ms  0,002ms  0,002ms  0,002ms
*
 2  10.0.2.1  0,011ms  0,008ms  0,008ms  0,007ms  0,010ms  0,008ms
*
 3  10.0.1.20  0,010ms  0,008ms  0,008ms  0,011ms  0,008ms  0,008ms
*
root@n2:/tmp/pycore.43895/n2.conf#
```

```
tcpdump -c 7 -xx -dst host 10.0.1.20 and ip proto (udp)
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:46:57.133457 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd2 4000 0111 d1ce 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
11:46:57.133658 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd3 4000 0111 d1cd 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
11:46:57.133796 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd4 4000 0111 d1cc 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
11:46:57.134017 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd5 4000 0111 d1cb 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
11:46:57.134174 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd6 4000 0111 d1ca 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
11:46:57.134308 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd7 4000 0111 d1c9 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
11:46:57.134441 IP 10.0.3.20.54898 > n1.33436: UDP, length 9
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  ....E.
    0x0010:  0025 8fd8 4000 0111 d1c8 0a00 0314 0a00  .%..@.....
    0x0020:  0114 d672 829c 0011 575f 5355 5045 524d  ...r....W_SUPERM
    0x0030:  414e 00                                AN.
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.43895/n1.conf#
```

Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Для генерирования пакетов воспользоваться утилитой traceroute.

```
root@n2:/tmp/pycore.43895/n2.conf# traceroute -q 7 -I 10.0.1.20
traceroute to 10.0.1.20 (10.0.1.20), 64 hops max
 1  10.0.3.1  0,002ms  0,002ms  0,001ms  0,002ms  0,001ms  0,002ms  0,002ms  *
 2  10.0.2.1  0,008ms  0,006ms  0,006ms  0,006ms  0,006ms  0,006ms  0,006ms  *
 3  10.0.1.20  0,014ms  0,008ms  0,007ms  0,008ms  0,007ms  0,008ms  0,011ms

root@n2:/tmp/pycore.43895/n2.conf#
```

```
Терминал
Файл Правка Вид Поиск Терминал Справка
< -c 7 -xx 'dst host 10.0.1.20 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:59:39.898935 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 14, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd41 4000 0101 8460 0a00 0314 0a00
    0x0020:  0114 0800 b014 0055 000e 0800 0000 0000
    0x0030:  0000 0700 0000 0000 0000 c004 eb03 8d7f
    0x0040:  0000
11:59:39.899148 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 15, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd42 4000 0101 845f 0a00 0314 0a00
    0x0020:  0114 0800 0bce 0055 000f f877 9303 8d7f
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a
    0x0040:  5a5a
11:59:39.899278 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 16, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd43 4000 0101 845e 0a00 0314 0a00
    0x0020:  0114 0800 0bcd 0055 0010 f877 9303 8d7f
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a
    0x0040:  5a5a
11:59:39.899403 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 17, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd44 4000 0101 845d 0a00 0314 0a00
    0x0020:  0114 0800 0bcc 0055 0011 f877 9303 8d7f
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a
    0x0040:  5a5a
11:59:39.899529 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 18, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd45 4000 0101 845c 0a00 0314 0a00
    0x0020:  0114 0800 0bcb 0055 0012 f877 9303 8d7f
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a
    0x0040:  5a5a
11:59:39.899655 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 19, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd46 4000 0101 845b 0a00 0314 0a00
    0x0020:  0114 0800 0bca 0055 0013 f877 9303 8d7f
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a
    0x0040:  5a5a
11:59:39.899781 IP 10.0.3.20 > n1: ICMP echo request, id 85, seq 20, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500
    0x0010:  0034 dd47 4000 0101 845a 0a00 0314 0a00
    0x0020:  0114 0800 0bc9 0055 0014 f877 9303 8d7f
    0x0030:  0000 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a 5a5a
    0x0040:  5a5a
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.43895/n1.conf#
```

Wireshark

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

```

Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.43895/n2.conf# ping 10.0.1.255 -b
WARNING: pinging broadcast address
PING 10.0.1.255 (10.0.1.255) 56(84) bytes of data.

```

Capturing from veth5.0.dc

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 10.0.1.255

No.	Time	Source	Destination	Protocol	Length	Info
3	0.882702220	10.0.1.22	10.0.1.255	ICMP	98	Echo (ping) request
4	1.907372127	10.0.1.22	10.0.1.255	ICMP	98	Echo (ping) request
6	2.931087012	10.0.1.22	10.0.1.255	ICMP	98	Echo (ping) request
7	3.955094726	10.0.1.22	10.0.1.255	ICMP	98	Echo (ping) request
9	4.979436986	10.0.1.22	10.0.1.255	ICMP	98	Echo (ping) request
13	6.003062526	10.0.1.22	10.0.1.255	ICMP	98	Echo (ping) request

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 10.0.1.22, Dst: 10.0.1.255

Internet Control Message Protocol

```

0000  ff ff ff ff ff ff 00 00 00 aa 00 05 08 00 45 00  .....E.
0010  00 54 00 00 40 00 40 01 23 95 0a 00 01 16 0a 00  .T..@..#.....
0020  01 ff 08 00 e2 89 00 31 00 14 4c 32 1e 62 00 00  .....1..L2.b..
0030  00 00 eb c9 00 00 00 00 00 00 10 11 12 13 14 15  .....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37                                           67

```

veth5.0.dc: <live capture in progress> Packets: 13 · Displayed: 6 (46.2%) Profile: Default

Для фильтрации для ip используется: `ip.dst == <нужный ip>`

```
Текстовый редактор Вт, 18:03
Открыть sharkARP1.txt [Только для чтения] /usr/local/lib/core Сохранить

-----+-----+
15:02:47,532,470 ETHER
0 |01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|35|98|00|00|01|59|98|07|0a|00|01|01|e0|
10|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
12|01|00|00|00|06|0a|00|01|01|00|00|00|00|

-----+-----+
15:02:47,987,881 ETHER
0 |ff|ff|ff|ff|ff|ff|00|00|00|aa|00|05|08|00|45|00|00|54|00|00|40|00|40|01|23|95|0a|00|01|16|0a|
10|01|ff|08|00|e5|36|00|3d|00|0f|97|35|1e|62|00|00|00|00|8f|12|0f|00|00|00|00|00|10|11|12|13|14|15|
16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|
17|

-----+-----+
15:02:49,011,623 ETHER
0 |ff|ff|ff|ff|ff|ff|00|00|00|aa|00|05|08|00|45|00|00|54|00|00|40|00|40|01|23|95|0a|00|01|16|0a|
10|01|ff|08|00|43|1b|00|3d|00|10|99|35|1e|62|00|00|00|00|3e|2d|00|00|00|00|00|00|10|11|12|13|14|15|
16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|
17|

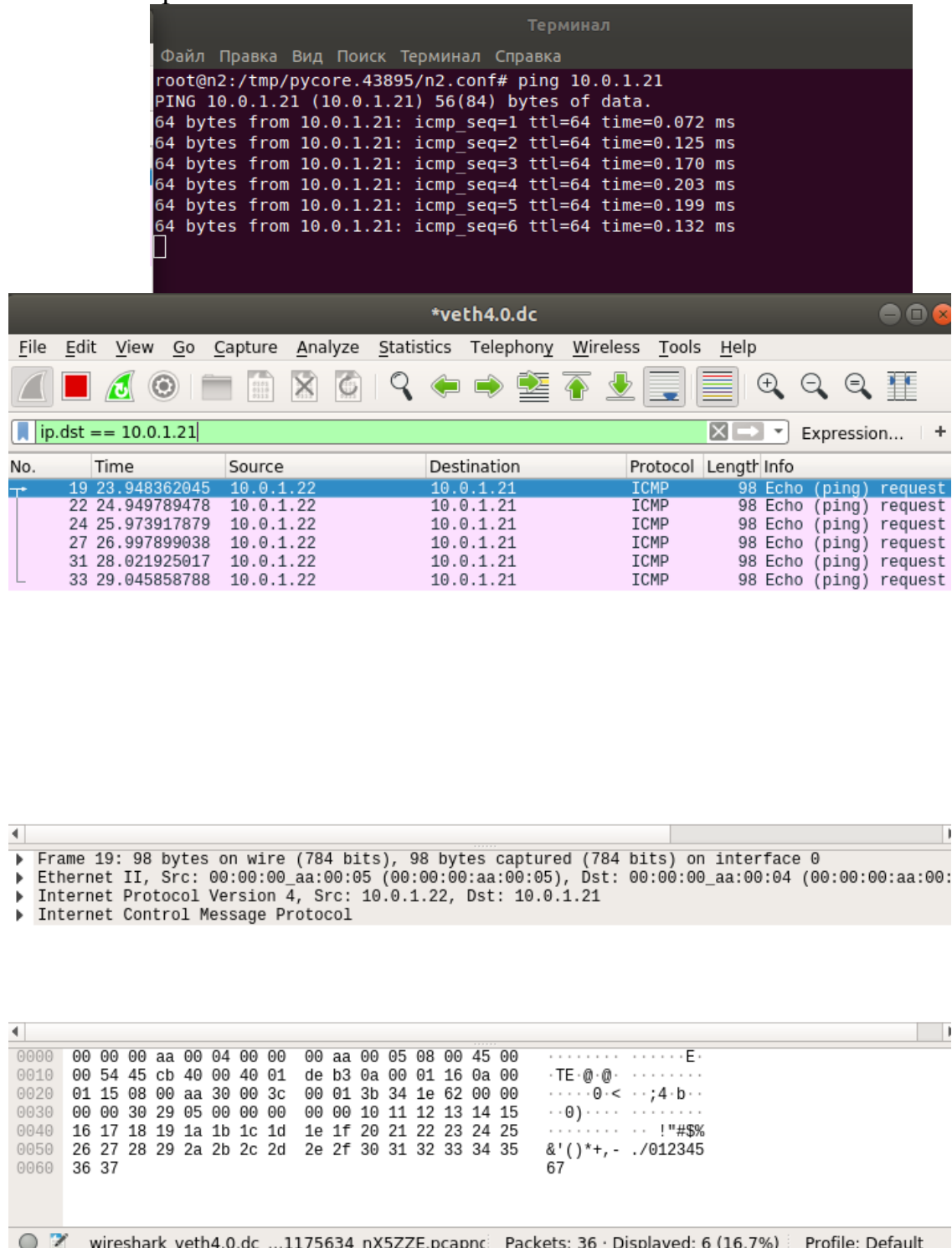
-----+-----+
15:02:49,533,238 ETHER
0 |01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|35|9a|00|00|01|59|98|05|0a|00|01|01|e0|
10|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
12|01|00|00|00|06|0a|00|01|01|00|00|00|00|

-----+-----+
15:02:50,035,793 ETHER
0 |ff|ff|ff|ff|ff|ff|00|00|00|aa|00|05|08|00|45|00|00|54|00|00|40|00|40|01|23|95|0a|00|01|16|0a|
10|01|ff|08|00|05|bc|00|3d|00|11|9a|35|1e|62|00|00|00|00|7a|8b|00|00|00|00|00|00|10|11|12|13|14|15|
16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|
17|

-----+-----+
15:02:51,059,569 ETHER
0 |ff|ff|ff|ff|ff|ff|00|00|00|aa|00|05|08|00|45|00|00|54|00|00|40|00|40|01|23|95|0a|00|01|16|0a|
10|01|ff|08|00|05|bc|00|3d|00|11|9a|35|1e|62|00|00|00|00|7a|8b|00|00|00|00|00|00|10|11|12|13|14|15|
16|17|18|19|1a|1b|1c|1d|1e|1f|20|21|22|23|24|25|26|27|28|29|2a|2b|2c|2d|2e|2f|30|31|32|33|34|35|36|
17|

Загрузка файла «/usr/local/lib/core/sharkARP1.txt»... Текст Ширина табуляции: 8 Стр 1, Стлб 1 ВСТ
```

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.



The image shows a terminal window and a Wireshark packet capture window. The terminal window displays the output of a ping command from a root user on a system named n2. The output shows six successful ping requests to 10.0.1.21, each receiving 64 bytes of data with varying response times. The Wireshark window shows a capture of these ICMP echo requests on interface 0. The packet list shows six packets, all of which are ICMP Echo (ping) requests from 10.0.1.22 to 10.0.1.21. The packet details pane shows the structure of the first packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol header.

Terminal Output:

```

root@n2:/tmp/pycore.43895/n2.conf# ping 10.0.1.21
PING 10.0.1.21 (10.0.1.21) 56(84) bytes of data.
64 bytes from 10.0.1.21: icmp_seq=1 ttl=64 time=0.072 ms
64 bytes from 10.0.1.21: icmp_seq=2 ttl=64 time=0.125 ms
64 bytes from 10.0.1.21: icmp_seq=3 ttl=64 time=0.170 ms
64 bytes from 10.0.1.21: icmp_seq=4 ttl=64 time=0.203 ms
64 bytes from 10.0.1.21: icmp_seq=5 ttl=64 time=0.199 ms
64 bytes from 10.0.1.21: icmp_seq=6 ttl=64 time=0.132 ms

```

Wireshark Packet Capture:

No.	Time	Source	Destination	Protocol	Length	Info
19	23.948362045	10.0.1.22	10.0.1.21	ICMP	98	Echo (ping) request
22	24.949789478	10.0.1.22	10.0.1.21	ICMP	98	Echo (ping) request
24	25.973917879	10.0.1.22	10.0.1.21	ICMP	98	Echo (ping) request
27	26.997899038	10.0.1.22	10.0.1.21	ICMP	98	Echo (ping) request
31	28.021925017	10.0.1.22	10.0.1.21	ICMP	98	Echo (ping) request
33	29.045858788	10.0.1.22	10.0.1.21	ICMP	98	Echo (ping) request

Packet Details (Frame 19):

- Frame 19: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
- Ethernet II, Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05), Dst: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
- Internet Protocol Version 4, Src: 10.0.1.22, Dst: 10.0.1.21
- Internet Control Message Protocol

Packet Bytes:

```

0000  00 00 00 aa 00 04 00 00 00 aa 00 05 08 00 45 00  .....E.
0010  00 54 45 cb 40 00 40 01 de b3 0a 00 01 16 0a 00  .TE.@@.
0020  01 15 08 00 aa 30 00 3c 00 01 3b 34 1e 62 00 00  ...0.<..;4.b.
0030  00 00 30 29 05 00 00 0c 00 00 10 11 12 13 14 15  ..0).....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....!""$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37                                           67

```

Wireshark veth4.0.dc ...1175634 nX5ZZE.pcapnc Packets: 36 · Displayed: 6 (16.7%) Profile: Default


```
Открыть sharkICMP1.txt [Только для чтения] Сохранить
/usr/local/lib/core

+-----+
14:56:35,389,921 ETHER
|0|01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|34|24|00|00|01|59|99|7b|0a|00|01|01|e0|
00|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
02|01|00|00|00|06|0a|00|01|01|00|00|00|00|

+-----+
14:56:37,390,278 ETHER
|0|01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|34|26|00|00|01|59|99|79|0a|00|01|01|e0|
00|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
02|01|00|00|00|06|0a|00|01|01|00|00|00|00|

+-----+
14:56:39,391,389 ETHER
|0|01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|34|28|00|00|01|59|99|77|0a|00|01|01|e0|
00|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
02|01|00|00|00|06|0a|00|01|01|00|00|00|00|

+-----+
14:56:41,391,997 ETHER
|0|01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|34|2a|00|00|01|59|99|75|0a|00|01|01|e0|
00|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
02|01|00|00|00|06|0a|00|01|01|00|00|00|00|

+-----+
14:56:43,246,554 ETHER
|0|33|33|00|00|00|05|00|00|00|aa|00|02|86|dd|6c|00|9c|a3|00|24|59|01|fe|80|00|00|00|00|00|00|02|
00|00|ff|fe|aa|00|02|ff|02|00|00|00|00|00|00|00|00|00|00|00|05|03|01|00|24|0a|00|00|01|00|00|
00|00|a5|81|41|00|00|00|00|60|01|00|01|13|00|0a|00|28|0a|00|00|01|00|00|00|00|

+-----+
14:56:43,393,070 ETHER
|0|01|00|5e|00|00|05|00|00|00|aa|00|02|08|00|45|c0|00|40|34|2c|00|00|01|59|99|73|0a|00|01|01|e0|
00|00|05|02|01|00|2c|0a|00|00|01|00|00|00|00|e7|c6|00|00|00|00|00|00|00|00|ff|ff|ff|00|00|02|
02|01|00|00|00|06|0a|00|01|01|00|00|00|00|
```

The figure displays a Wireshark capture of a traceroute from root@n3 to 10.0.0.20. The packet list shows a series of ICMP Echo (ping) requests. The packet details show the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol layers. The packet bytes show the raw data of the ICMP request.

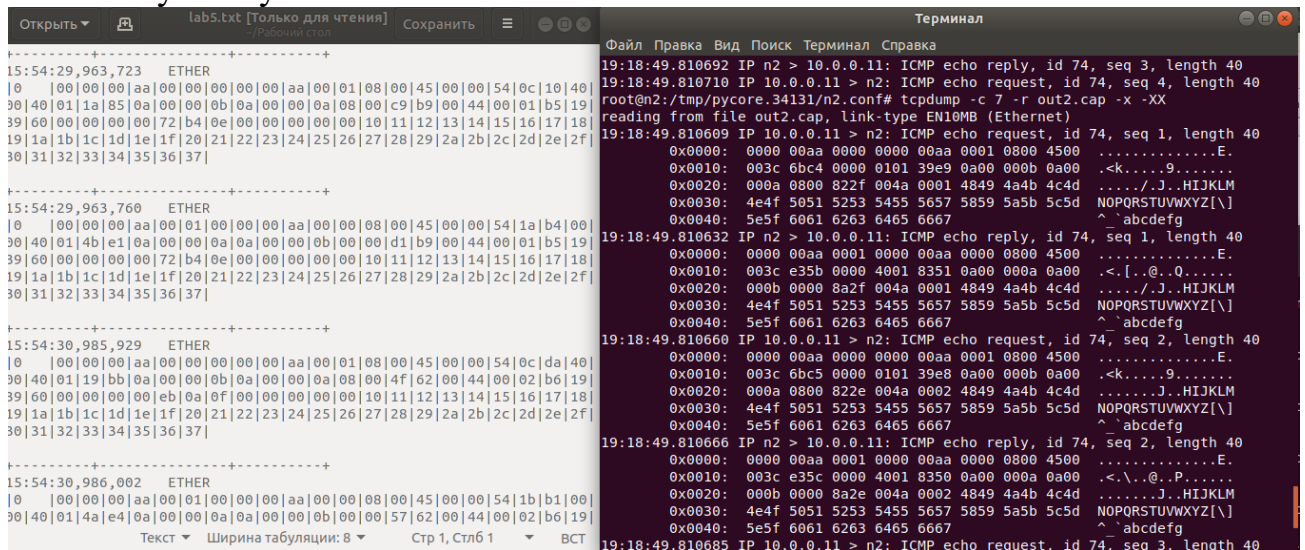
No.	Time	Source	Destination	Protocol	Length	Info
33	19.385123661	10.0.1.1	10.0.0.20	ICMP	94	time-to-live exceeded
34	19.385137547	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
40	22.387786473	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
41	22.387851062	10.0.1.1	10.0.1.20	ICMP	94	time-to-live exceeded
42	22.387935211	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
43	22.388000935	10.0.1.1	10.0.1.20	ICMP	94	time-to-live exceeded
44	22.388029008	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
45	22.388061001	10.0.1.1	10.0.1.20	ICMP	94	time-to-live exceeded
46	22.388139878	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
48	22.388372390	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
50	22.388483116	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
52	22.388658847	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
54	22.388793192	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
56	22.388902705	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
58	22.389019078	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
60	22.389117190	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
62	22.389224447	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request
64	22.389331324	10.0.1.20	10.0.0.20	ICMP	66	Echo (ping) request

Frame 22: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: 00:00:00:aa:00:03 (00:00:00:aa:00:03), Dst: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
 Internet Protocol Version 4, Src: 10.0.1.20, Dst: 10.0.0.20
 Internet Control Message Protocol

0000 00 00 00 aa 00 02 00 00 00 aa 00 03 08 00 45 00E
 0010 00 34 81 3f 40 00 01 01 e3 62 0a 00 01 14 0a 00 -4?.....b.....
 0020 00 14 08 00 e2 ef 00 1e 00 0a 0c 0f 04 b5 55U
 0030 00 00 00 8c 0f 04 b5 55 00 00 6e e3 93 c2 88 7fU..n.....
 0040 00 00



4. Прочитать файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.



```
Открыть lab5.txt [Только для чтения] Сохранить
15:54:29,963,723 ETHER
00 00 00 00 aa 00 00 00 00 00 00 aa 00 01 08 00 45 00 00 54 0c 10 40
30 40 01 1a 85 0a 00 00 0b 0a 00 00 0a 08 00 c9 b9 00 44 00 01 b5 19
39 60 00 00 00 00 72 b4 0e 00 00 00 00 00 10 11 12 13 14 15 16 17 18
19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f
30 31 32 33 34 35 36 37

15:54:29,963,760 ETHER
00 00 00 00 aa 00 01 00 00 00 00 aa 00 08 00 45 00 00 54 1a b4 00
30 40 01 4b e1 0a 00 00 0a 0a 00 00 0b 00 00 d1 b9 00 44 00 01 b5 19
39 60 00 00 00 00 72 b4 0e 00 00 00 00 00 10 11 12 13 14 15 16 17 18
19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f
30 31 32 33 34 35 36 37

15:54:30,985,929 ETHER
00 00 00 00 aa 00 00 00 00 00 00 aa 00 01 08 00 45 00 00 54 0c da 40
30 40 01 19 bb 0a 00 00 0b 0a 00 00 0a 08 00 4f 62 00 44 00 02 b6 19
39 60 00 00 00 00 eb 0a 0f 00 00 00 00 00 10 11 12 13 14 15 16 17 18
19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f
30 31 32 33 34 35 36 37

15:54:30,986,002 ETHER
00 00 00 00 aa 00 01 00 00 00 00 aa 00 08 00 45 00 00 54 1b b1 00
30 40 01 4a e4 0a 00 00 0a 0a 00 00 0b 00 00 57 62 00 44 00 02 b6 19

Текст Ширина таблицы: 8 Стр 1, Стлб 1 ВСТ

Файл Правка Вид Поиск Терминал Справка
19:18:49.810692 IP n2 > 10.0.0.11: ICMP echo reply, id 74, seq 3, length 40
19:18:49.810710 IP 10.0.0.11 > n2: ICMP echo request, id 74, seq 4, length 40
root@n2:/tmp/pycore.34131/n2.conf# tcpdump -c 7 -r out2.cap -x -XX
reading from file out2.cap, link-type EN10MB (Ethernet)
19:18:49.810609 IP 10.0.0.11 > n2: ICMP echo request, id 74, seq 1, length 40
0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
0x0010: 003c 6bc4 0000 0101 39e9 0a00 000b 0a00 .<k.....9.....
0x0020: 000a 0800 822f 004a 0001 4849 4a4b 4c4d ...../J..HIJKLM
0x0030: 4e4f 5051 5253 5455 5657 5859 5a5b 5c5d NOPQRSTUVWXYZ[\]
0x0040: 5e5f 6061 6263 6465 6667 ^_abcdefg
19:18:49.810632 IP n2 > 10.0.0.11: ICMP echo reply, id 74, seq 1, length 40
0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
0x0010: 003c e35b 0000 4001 8351 0a00 000a 0a00 .<.[...@..0.....
0x0020: 000b 0000 8a2f 004a 0001 4849 4a4b 4c4d ...../J..HIJKLM
0x0030: 4e4f 5051 5253 5455 5657 5859 5a5b 5c5d NOPQRSTUVWXYZ[\]
0x0040: 5e5f 6061 6263 6465 6667 ^_abcdefg
19:18:49.810660 IP 10.0.0.11 > n2: ICMP echo request, id 74, seq 2, length 40
0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
0x0010: 003c 6bc5 0000 0101 39e8 0a00 000b 0a00 .<k.....9.....
0x0020: 000a 0800 822e 004a 0002 4849 4a4b 4c4d ...../J..HIJKLM
0x0030: 4e4f 5051 5253 5455 5657 5859 5a5b 5c5d NOPQRSTUVWXYZ[\]
0x0040: 5e5f 6061 6263 6465 6667 ^_abcdefg
19:18:49.810666 IP n2 > 10.0.0.11: ICMP echo reply, id 74, seq 2, length 40
0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
0x0010: 003c e35c 0000 4001 8350 0a00 000a 0a00 .<.\...@..P.....
0x0020: 000b 0000 8a2e 004a 0002 4849 4a4b 4c4d ...../J..HIJKLM
0x0030: 4e4f 5051 5253 5455 5657 5859 5a5b 5c5d NOPQRSTUVWXYZ[\]
0x0040: 5e5f 6061 6263 6465 6667 ^_abcdefg
19:18:49.810685 IP 10.0.0.11 > n2: ICMP echo request, id 74, seq 3, length 40
```