# OLD DOMINION UNIVERSITY CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Ean Miller

01239018

## Task A ---- Get started with Wireshark

# You should keep Wireshark running in the background while performing the following

#### tasks.

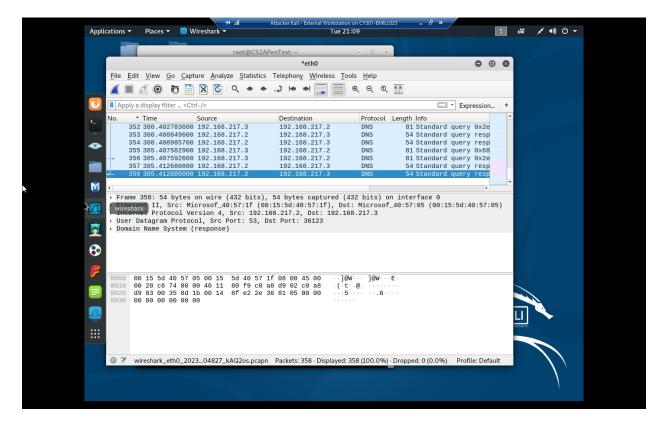
- 1. Open Wireshark on External Kali and listen on interface "eth0."
- 2. Open a new terminal then ping <u>Ubuntu VM</u> for 5-10 seconds.

## 3. Stop capturing (the red button on the tool bar).

Now, answer the following questions. You need to provide a screenshot that contains the

answers to each question.

Q1. How many packets are captured in total? How many packets are displayed?



Wire shark has captured 358 packets

**Q2.** Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).

| Applications 🔻  | Places 🔻   | 📶 Wireshark 🔻   | • al   | Attacker Kali - External \   | Workstation on CY301-EMILL<br>Tue 21:11 | 023 <u>- 6 ×</u>             |                                 | 1 2 18   | ≠ ⊕ (@ ◄ |
|---|--|---|--|--|---|------------------------------|---------------------------------|----------|----------|
| -   |  | _   |  |  |   |                              |                                 |          |          |
|   |  |   | root@CS2A  |  | - 🗆 x                                   |                              |                                 |          |          |
|   |  |   |  | *eth0  |   |                              | • •                             |          |          |
| <u>F</u> ile <u>E</u> di  | t <u>V</u> iew <u>G</u> o  | <u>Capture</u> <u>Analyz</u>  | e <u>S</u> tatistics   | Telephony Wire   |   |                              |                                 |          |          |
|   | 100  | i 🗋 🖹 🎑   | ०, ♦ ⇒   | ⊅ l∉ ⇒l 📮  |   | **                           |                                 |          |          |
| 🥑 🔳 icmp  |  |   |  |  |   | $\bowtie$                    | <ul> <li>Expression.</li> </ul> | .   +    |          |
|   | <ul> <li>Time</li> </ul>   | Source  |  | Destination  | Protocol                                | Length Info                  |                                 | -        |          |
| 32  |  | 7500 192.168.   |  | 192.168.10.1   |   | 98 Echo (pin                 |                                 |          |          |
|   |  | 5400 192.168.<br>4700 192.168.  |  | 192.168.217.<br>192.168.10.1   |   | 98 Echo (pin<br>98 Echo (pin |                                 |          |          |
|   |  | 4700 192.108.<br>8500 192.168.  |  | 192.168.217  |   | 98 Echo (pin                 |                                 |          |          |
|   |  | 3100 192.168.   |  | 192.168.10.1   |   | 98 Echo (pin                 |                                 |          |          |
|   |  | 5300 192.168.   |  | 192.168.217.   |   | 98 Echo (pin                 |                                 |          |          |
|   |  | 3600 192.168.   |  | 192.168.10.1   |   | 98 Echo (pin                 |                                 |          |          |
| M <sup>▲⊥</sup> 33.   | 2 360.24724:   | 1900 192.168.   | 10.10  | 192.168.217.   | .3 ICMP                                 | 98 Echo (pin                 | g) reply                        | <b>•</b> |          |
| ₽   |  |   |  |  |   |                              |                                 |          |          |
| 0000  |  |   |  | Lf 08 00 45 00   | ··]@W···]@W···                          |                              |                                 |          |          |
| 0010 0<br>0020 d  | 00 54 38 e9<br>19 03 00 00   | 00 00 3f 01<br>ce 37 07 3f  | de 61 c0 a<br>00 0d d5 7   | a8 0a 0a c0 a8<br>75 f5 63 00 00   | -T8?-a<br>7-?u-c                        |                              |                                 |          |          |
| 0010 C<br>0020 d<br>0030 C  | 00 54 38 e9<br>19 03 00 00<br>00 00 a0 cf  | 00 00 3f 01<br>ce 37 07 3f<br>00 00 00 00                               | de 61 c0 a<br>00 0d d5 7<br>00 00 10 1                             | a8 0a 0a c0 a8<br>75 f5 63 00 00<br>11 12 13 14 15   | -T8?-a<br>7-?u-c                        | · · ·                        |                                 |          |          |
| 0010 0<br>0020 d<br>0030 0<br>0040 1  | 00 54 38 e9<br>19 03 00 00<br>00 00 a0 cf<br>16 17 18 19   | 00 00 3f 01<br>ce 37 07 3f<br>00 00 00 00<br>1a 1b 1c 1d                | de 61 c0 a<br>00 0d d5 7<br>00 00 10 1<br>1e 1f 20 2               | a8 0a 0a c0 a8<br>75 f5 63 00 00   | -T8?-a<br>7-?u-c                        | :<br>:<br>:\$%               |                                 |          |          |
| 0010 0<br>0020 d<br>0030 0<br>0040 1<br>0050 2<br>0060 3                                | 90       54       38       e9         19       03       00       00         90       00       a0       cf         16       17       18       19         26       27       28       29  | 00 00 3f 01<br>ce 37 07 3f<br>00 00 00 00<br>1a 1b 1c 1d                | de 61 c0 a<br>00 0d d5 7<br>00 00 10 1<br>1e 1f 20 2               | a8 0a 0a c0 a8<br>75 f5 63 00 00<br>11 12 13 14 15<br>21 22 23 24 25   | -T8?-a<br>7-?u-c                        | :<br>:<br>:\$%               |                                 |          |          |
| 0000 d<br>0020 d<br>0030 d<br>0040 1<br>0050 2<br>0060 3                                | 00         54         38         e9           19         03         00         00         00           00         00         a0         cf         16         17         18         19           26         27         28         29         36         37 | 00 00 3f 01<br>ce 37 07 3f<br>00 00 00 00<br>1a 1b 1c 1d<br>2a 2b 2c 2d | de 61 c0 a<br>00 0d d5 7<br>00 00 10 1<br>1e 1f 20 2<br>2e 2f 30 3 | a8         0a         0a         c0         a8           75         f5         63         00         00         11         12         13         14         15           21         22         23         24         25         31         32         33         34         35 |   | \$%<br>445                   | Profile: Defa                   |          |          |
| 00100 0<br>0010 0<br>0020 d<br>0020 d<br>0020 d<br>0020 d<br>0020 1<br>0050 2<br>0060 3 | 00         54         38         e9           19         03         00         00         00           00         00         a0         cf         16         17         18         19           26         27         28         29         36         37 | 00 00 3f 01<br>ce 37 07 3f<br>00 00 00 00<br>1a 1b 1c 1d<br>2a 2b 2c 2d | de 61 c0 a<br>00 0d d5 7<br>00 00 10 1<br>1e 1f 20 2<br>2e 2f 30 3 | a8         0a         0a         c0         a8           75         f5         63         00         00         11         12         13         14         15           21         22         23         24         25         31         32         33         34         35 |   | \$%<br>445                   | Profile: Defa                   | ult      |          |

Wireshark has captured 33 packets with the protocol ICMP

**Q3.** Select an Echo (replay) message from the list. What are the source and destination IPs of

this packet? What are the sequence number and the size of the data? What is the response

time?

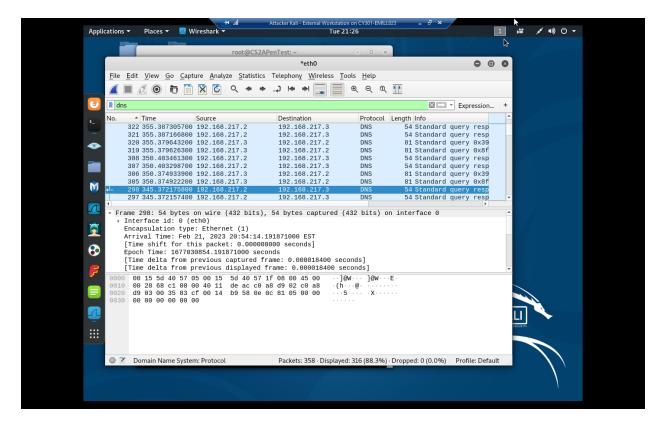
| Applications 🔻 | Places 🔻                 |                                  | al 4         | Attacker Kali - E  |          | ation on CY301-EMILLO | 23 _ 🗗             | ×            |             | 1     | <b>,</b> 2 | × • | 》(1) - |
|----------------|--------------------------|----------------------------------|--------------|--------------------|----------|-----------------------|--------------------|--------------|-------------|-------|------------|-----|--------|
|                |                          | <u> </u>                         | root@CS2AP   | anTest: ~          |          | - • ×                 |                    |              |             |       |            |     |        |
|                |                          |                                  | 1001@002711  |                    | thO      |                       |                    |              | 00          | 8     |            |     |        |
| File Edit      | t View Go                | <u>Capture</u> Analyz            | e Statistics | Telephony          | Wireless | Tools Help            |                    |              |             | -     |            |     |        |
|                |                          |                                  | -            | ريندي<br>⇒ ⇒ا (ل.  |          |                       | π                  |              |             |       |            |     |        |
|                |                          |                                  | ~ ~ ~        | - P 4              |          | ~~~~                  |                    |              |             |       |            |     |        |
| 🥑 🔳 icmp       |                          |                                  |              |                    |          |                       | $\times$           | <b>—</b> • E | xpression   | .   + |            |     |        |
|                | <ul> <li>Time</li> </ul> | Source                           |              | Destinatio         |          |                       | Length Info        |              |             | *     |            |     |        |
| 299            |                          | 3600 192.168.                    |              | 192.168            |          | ICMP                  | 98 Echo            |              |             |       |            |     |        |
| - 300          | 348.22203                | 32200 192.168.                   | L0.10        | 192.168<br>192.168 |          | ICMP<br>ICMP          | 98 Echo<br>98 Echo |              |             |       |            |     |        |
| 💽 🛛 Zenmap     | (as root) 4515           | 0300 192.168.2<br>8900 192.168.2 | 217.3        | 192.168            |          | ICMP                  | 98 Echo            |              |             |       |            |     |        |
| 303            |                          | 7100 192.168.2                   |              | 192.168            |          | ICMP                  | 98 Echo            |              |             |       |            |     |        |
| 304            | 4 350.27242              | 3700 192.168.                    | L0.10        | 192.168            | .217.3   | ICMP                  | 98 Echo            | (ping)       | reply       |       |            |     |        |
|                |                          | 00600 192.168.2                  |              | 192.168            |          | ICMP                  | 98 Echo            |              |             |       |            |     |        |
| 310            | 9 351.22627              | 1400 192.168.                    | L0.10        | 192.168            | .217.3   | ICMP                  | 98 Echo            | (ping)       | reply       | Ψ.    |            |     |        |
| 8              |                          |                                  |              |                    |          |                       |                    |              |             |       |            |     |        |
| 0000 00        |                          |                                  | 5d 40 57 05  |                    |          | ]@W···]@W···E         |                    |              |             |       |            |     |        |
|                |                          | 40 00 40 01<br>ed a3 07 3f       | b0 fb c0 a8  |                    |          | %0@·@·····            |                    |              |             |       |            |     |        |
|                |                          | 00 00 00 00                      |              |                    | 15       | .0                    |                    |              |             |       |            |     |        |
|                |                          | 1a 1b 1c 1d                      |              |                    |          | !"#\$                 |                    |              |             |       |            |     |        |
|                | 6 27 28 29               | 2a 2b 2c 2d                      | 2e 2f 30 3   | 1 32 33 34         |          | ()*+,/01234           | 45                 |              |             |       |            |     |        |
|                | 6 37                     |                                  |              |                    |          |                       |                    |              |             |       |            |     |        |
| 0060 3         | 6 37                     |                                  |              |                    | 67       |                       |                    |              |             |       | ECURITY    |     |        |
| 0060 3         | 6 37                     |                                  |              |                    | 67       |                       |                    |              |             |       | ECURITY    |     |        |
| 0060 3         | 6 37                     |                                  |              |                    | 67       |                       |                    |              |             |       | LECURITY   |     |        |
| 0060 30        |                          | 0_20230204827                    | _kAQ2os.pcap | ng Packets         |          |                       | Dropped: 0 (0.0    | 0%) Pr       | ofile: Defa | ult   | SECURITY   |     |        |
| 0060 30        |                          | 0_20230204827                    | _kAQ2os.pcap | ng Packets         |          |                       | Dropped: 0 (0.0    | 0%) Pr       | ofile: Defa | ult   | SECURITY   |     |        |
| 0060 30        |                          | 0_20230204827                    | _kAQ2os.pcap | ng Packets         |          |                       | Dropped: 0 (0.0    | 0%) Pr       | ofile: Defa | ılt   | SECURITY   |     |        |
| 0060 30        |                          | 0_20230204827                    | _kAQ2os.pcap | ng Packets         |          |                       | Dropped: 0 (0.0    | D%) Pr       | ofile: Defa | ult   | BECURITY   |     |        |

I chose packet number 299 and the source IP is 192.168.217.3 and the destination IP is

192.168.10.10, and the sequence number is 1/256 and the size of the data is 98 bytes or 784

bits, and the response time is 348.208873600 seconds

**Q4.** Apply "DNS" as a display filter in Wireshark. How many packets are displayed?



The amount of packets that are displayed is 322 packets

**Q5.** Find a DNS query packet. What is the domain name this host is trying to resolve? What is

the source IP and port number, destination IP and port number? Please express in the format:

IP:port

| Nuccion  | Appli        | cations •             | P DI:          | ices 🔻        | 🗖 W           | ireshark        | H al   |                   | Atta   | acker Ka | ili - Exte  | ernal W        | orkstatio<br>Tue 2 |       | Y301-EM      | ILL023  |        | - 6     | ×      |          |       | N I       | 18   | 1       | 》〇    | -        |
|--|--------------|-----------------------|----------------|---------------|---------------|-----------------|--------|-------------------|--------|----------|-------------|----------------|--------------------|-------|--------------|---------|--------|---------|--------|----------|-------|-----------|------|---------|-------|----------|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Lools Help         Image: Control Contrectic Contentic Control Control Control Control Contro  | , the second |                       |                | ices          |               | resnarie        |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       | P.C.      |      |         |       |          |
| Image: Source       Destination       Protocol length info       Image: Source       Protocol length info         192.168.217.3       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.3       192.168.217.2       192.168.217.3       192.168.217.3       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      | 9       | Θ     | ×        |
| Ima       Image: Construction of the second of   |              | <u>F</u> ile <u>I</u> | dit <u>V</u> i | ew <u>G</u> o | <u>C</u> aptu | ire <u>A</u> na | alyze  | <u>S</u> tatistic | s Te   | elepho   | ny <u>\</u> | <u>N</u> irele | ss <u>T</u> e      | ols   | <u>H</u> elp |         |        |         |        |          |       |           |      |         |       |          |
| Image: Control of the standard guery (withink 4.2.debian.pool.ntp.org)         192.168.217.3       192.168.217.2       015       81 Standard guery (withink 4.2.debian.pool.ntp.org)         192.168.217.2       192.168.217.3       015.100       81 Standard guery (withink 4.2.debian.pool.ntp.org)         192.168.217.2       192.168.217.2       015.100       81 Standard guery (withink 4.2.debian.pool.ntp.org)         192.168.217.2       192.168.217.3       015.54 Standard guery response 0x58bd Refused         192.168.217.2       192.168.217.2       015.54 Standard guery (withink 4.2.debian.pool.ntp.org)         192.168.217.2       192.168.217.2       015.54 Standard guery response 0x58bd Refused         192.168.217.2       192.168.217.3       015.54 Standard guery response 0x58bd Refused         192.168.217.2       192.168.217.3       015.54 Standard guery response 0x58bd Refused         192.168.217.2       192.168.217.3       015.54 Standard guery response 0x58bd Refused         192.168.217.2       192.168.217.2       015.54 Standard guery response 0x57bd Refused         192.168.217.2   |              |                       |                | (i)           | -             | 8               | Q      |                   | ٠      | J I€     | ⇒           |                |                    | ۲     | Θ            | D 🖡     | E      |         |        |          |       |           |      |         |       |          |
| Source       Destination       Protocol Length Info         192.166.217.3       192.166.217.2       DNS       81 Standard query 0x95b4 A 2.debian.pool.ntp.org         192.166.217.2       192.166.217.2       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.2       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.3       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.3       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.3       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.2       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.2       DNS       54 Standard query response 0x95b4 Refused         192.166.217.3       192.166.217.3       DNS       54 Standard query response 0x676b Refused         192.166.217.2       192.166.217.3       DNS       54 Standard query response 0x676b Refused         192.166.217.2       192.166.217.3       DNS       54 Standard query response 0x676e Refused         192.166.217.2       192.166.217.3       DNS       54 Standard query response 0x676e Refused         192.166.217.2       192.166.217.3       DNS   |              |                       |                | •             | · []          | (E13)           |        |                   |        |          |             | -              |                    | `     | <u>`</u>     | `       |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.3       192.168.217.2       DNS       61 Standard query 0xf5h4 A.2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf5h4 Azdebian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xf5h4 Azdebian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xf5h4 Azdebian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0xf5h4 Azdebian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0xf5h4 Azdebian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0xf5h4 Azdebian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf6h4 Azdebian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf6h4 Azdebian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf6h4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xf6h4 Refused         192.168.217.3       DNS       54 Standard query response 0xf6h4 Refused       192.168.217.2         192.168.217.2       DNS       54 Standard   |              | 📕 dns                 |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       | × =       |      | Express | ion   | +        |
| 192.168.217.3       192.168.217.2       DNS       81 Standard query 0x98bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x98bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x98bd AAAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query 0x95bd AAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x95bd AAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x95bd AAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query 0x96bd AAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x96bd AAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x96bd AAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x96bd AA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x96bd AA 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x96bd Refused         192.168.217.2       DNS       54 Standard query response 0x96  |              | Source                | :e             |               | ſ             | Destinat        | ion    |                   | 1      | Protoc   | ol L        | .ength         | Info               |       |              |         |        |         |        |          |       |           |      |         |       | -        |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 6xf6b4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query forsbuk A2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query forsbuk A2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query forsbuk AA2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query forsbuk AA2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query forsbuk AAA2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query forsbuk AAA3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 6x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 6x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 6x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query forsborse 6x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query forsborse 6x60e8 Refused         192.168.217.3       DNS       54 Standard query forsborse 6x60e8 Refused       192.168.217.3   | 9            |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x98bd Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x75b4 A 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x75b4 A 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x75b4 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x75b4 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query 0x760e4 A 3.debian.pool.ntp.org         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x760e4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x760e4 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x760e8 Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x760e8 Refused         192.168.217.4       192.168.217.3       DNS       54 Standard query response 0x760e8 A 3.debian.pool.ntp.org         192.168.217.4       192.168.217.4       192.168.217.4       192.168.217.4       192.168.217.4         192.168.217.4       192.168.217.4       192.168.217.4       192.168.217.4       192.168.2   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       | ntp.or    | rg   |         |       |          |
| 192.168.217.3       192.168.217.2       DNS       #1 Standard query @x98bd AAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query @x98bd AAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query @x98bd AAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query @x98bd AAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       51 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query @x76e AAA 3.debian.pool.ntp.org         192.168.217.4       Y       Y       Y <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.3       192.168.217.2       DNS       Al Standard query 0x08bd AxAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       S Standard query 0x08bd AxAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       S Standard query 0x08bd AxAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       S Standard query 0x08bd AxAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       S Standard query 0x08bd AxAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       S Standard query 0x08bd AxAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       S Standard query response 0x0688       A S.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       S Standard query response 0x0688       A S.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       S Standard query response 0x0688       A S.debian.pool.ntp.org         192.168.217.2       DNS       R Standard query response 0x0688       A S.debian.pool.ntp.org         192.168.217.3       DNS       S Standard query response 0x0688       A S.debian.pool.ntp.org         192.168.217.3       DNS       S Standard query response 0x0688       A S.debian.pool.ntp.org         Usersentation Port: 531   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x98b4 Refused         192.168.217.3       192.168.217.2       DNS       61 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x67ee AAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       DNS       54 Standard query response 0x60e8 Refused       192.168.217.2         192.168.217.2       DNS       54 Standard query response 0x60e8 Refused       192.168.217.2         192.168.217.2       DNS       54 Standard query response 0x60e8 Refused       192.168.217.2         192.168.217.2       DNS       54 Standard query response 0x60e8 Refused       192.168.217.2         Use   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x98bd Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x96e8 A 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x96e8 A 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x96e8 A 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x96e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x96e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x76e Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x76e Refused         192.168.217.3       192.168.217.3       DNS       51 Standard query externed the standard query ex   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       | ntp.or    | rg   |         |       |          |
| 192.168.217.3       192.168.217.2       DNS       81 Standard query 0xc5e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query 0xc5e8 AAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xc6e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xc6e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xc6e8 A 3.debian.pool.ntp.org         192.168.217.3       DNS       54 Standard query response 0xc6e8 Refused       192.168.217.3         192.168.217.3       DNS       54 Standard query response 0xc6e8 A 3.debian.pool.ntp.org         192.168.217.3       DNS       54 Standard query response 0xc6e8 Refused         192.168.217.3       DNS       54 Standard query response 0xc6e8 A 3.debian.pool.ntp.org         192.168.217.3       DNS       54 Standard query response 0xc6e8 Refused         192.168.217.3       DNS       54 Standard query response 0xc6e8 Refused         192.168.217.3       DNS       51 Standard query response 0xc6e8 Refused         192.168.217.3       DNS       51 Standard query response 0xc6e8 Refused         192.168.217.3       DNS       51 Standard query response 0xc6e8 Refused         192.168.217.2       DNS  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.3       192.168.217.2       DNS       81 Standard query 0xe7ee AAAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.3       DNS       51 Standard query response 0x60e8 Refused         192.168.217.3       DNS       51 Standard query response 0x60e8 Refused         192.168.217.3       DNS       51 Standard query response 0x60e8 Refused         Source Port: 55117       Destination Port: 53       Source Port: 5517         Destination Port: 53       Length: 47       Checksum 6x3398 [unverified]       [Stream index: 0]         [Stream index: 0]       DNS       54 Standard 0x Standard 0   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.2       DNS       54 Standard query response 0x67ee Refused          192.168.217.2       DNS       54 Standard query response 0x67ee Refused          192.168.217.2       DNS       54 Standard query response 0x67ee Refused          192.168.217.2       User Datagram Protocol, Screptified            192.168.217.3       DNS       54 Standard query response 0x68e8 A 3, debian.nool.ntn.org           192.168.217.2       DNS       54 Standard query response 0x68e8 A 3, debian.nool.ntn.org  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 192.168.217.2       192.168.217.3       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.2       192.168.217.2       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.3       192.168.217.2       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.2       192.168.217.3       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.2       192.168.217.3       DNS       54 Standard Query response 0xe7ee Refused         192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2         192.168.217.2       192.168.217.2       192.168.217.2       192.168.217.2         192.168.217.3       DNS       192.168.217.3       192.168.217.2         192.168.217.4       192.168.217.2       192.168.217.2       192.168.217.2         192.168.217.4       192.168.217.2       192.168.217.2       192.168.217.2         192.168.217.4       192.168.217.2       192.168.217.2       192.168.217.2  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       | ntp.or    | rg   |         |       |          |
| 192.168.217.3       192.168.217.2       DNS       R1 Standard ouerv 0x60e8 A 3.debian.pool.ntp.org         * Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2       *         * User Datagram Protocol, Src Port: 55117, Dst Port: 53         Source Port: 55117         Destination Port: 53         Length: 47         Checksum Status: Unverified]         [Stream index: 0]         > Domain Name System (query)         ************************************   | 1            |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| <pre>     Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2     User Datagram Protocol, Src Port: 55117, Dst Port: 53     Source Port: 55117     Destination Port: 53     Length: 47     Checksum: 6x3398 [unverified]     [Checksum Status: Unverified]     [Checksum status: Unverified]     [Checksum status: 0]     Domain Name System (query)     0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00     vomain Name System (query)     vomain Name Syst</pre> |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| <pre>&gt; Internet Protocol version 4, SrC: 192.106.217.3, USC: 192.106.217.2<br/>&gt; User Datagram Protocol, Src Port: 5517<br/>Destination Port: 53<br/>Length: 47<br/>Checksum: 6v33988 [unverified]<br/>[Checksum Status: Unverified]<br/>[Stream index: 0]<br/>&gt; Domain Name System (query)<br/>0000 00 15 5d 40 57 1f 99 15 5d 40 57 05 08 00 45 00<br/>&gt; 0000 00 15 5d 40 57 1f 99 15 5d 40 57 05 08 00 45 00<br/>&gt; 0000 00 43 6a 06 40 00 40 11 9d 4c c6 a8 d9 03 c6 a8<br/>&gt;M.5./ 3<br/>0030 00 00 00 00 00 00 00 132 06 64 652 69 01 00<br/>0044 78 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00<br/>0050 01</pre>  |              | 192.                  | 168.21         | 7.3           | -             | 192.16          | 8.217  | .2                |        | DNS      |             | 81             | Star               | ndard | quer         | v 0x    | 60e8   | A 3.0   | lebia  | n.noo    | 1.ntn | .ora      |      |         | •     | <b>T</b> |
| <pre>- User Datagram Protocol, src Port: 5517, Dst Port: 53 Source Port: 5517 Destination Port: 53 Length: 47 Checksum: 6v3398 [unverified] [Checksum: 6v3398 [unverified] [Stream index: 0] Domain Name System (query) 0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00 0010 00 43 6a 06 40 06 40 11 9d 4c C6 a8 d9 03 c0 a8 0020 40 03 60 02 f 33 98 f5 b4 01 00 00 01 0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00 001 ntp org 0050 01 001 00 10 00 10 00 10 00 10 00 00 01 00 001 ntp org 0020 00 01 00 00 01 00 00 00 01 00 001 ntp org 0020 01 01 0020 01 01 0020 01 01 0020 02 07 40 05 00 02 01 00 0020 00 00 00 01 32 06 64 65 62 09 01 60 01 0020 00 01 00 00 01 00 0020 00 00 00 01 32 06 64 65 62 09 01 00 001 ntp org 0020 01 01 0020 01 01 0020 01 01 0020 01 01 0020 01 01 0020</pre>             | 9            | . Int.                | ornot          | rotoc         |               | cion (          | 1 Sro  | 102               | 169    | 217      | 2 0         | ct · ·         | 102 1              | 60 2. | 17 2         |         |        |         |        |          |       |           |      |         |       |          |
| Source Port: 55117         Destination Port: 53         Length: 47         Checksum: 0x3398 [unverified]         [Checksum: status: Unverified]         [Stream index: 0]         Domain Name System (query)         ************************************  |              |                       |                |               |               |                 |        |                   |        |          |             |                | 192.1              | 00.2. | 11.2         |         |        |         |        |          |       |           |      |         |       |          |
| Destination Port: 53<br>Length: 47<br>Checksum: 0x3398 [unverified]<br>[Checksum Status: Unverified]<br>[Stream index: 0]<br>Domain Name System (query)<br>0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00<br>0020 d0 43 6a 06 40 00 35 00 2f 33 98 f5 b4 01 00 00 01<br>0020 00 00 00 00 00 01 32 06 64 65 62 69 61 66 04<br>0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00<br>0050 01   | <b>.</b>     |                       |                |               |               | , one           | , 1010 |                   | ., .   | /3L I    | 01          | 00             |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| Length: 47<br>Checksum: 0x3398 [unverified]<br>[Stream index: 0]         Domain Name System (query)         0000       00 15 5d 40 57 1f 00 15 5d 40 57 95 08 00 45 00<br>0020 d0 02 07 4d 00 35 00 2f 33 98 f5 b4 10 00 00 61<br>0020 d0 00 00 00 00 00 00 26 6d 65 02 69 61 60 4<br>0020 d0 00 00 00 00 00 00 00 32 66 6d 65 02 69 61 60 4<br>0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00<br>0050 01  | ~            |                       |                |               |               | 53              |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| Checksum: 0x3398 [unverified]<br>[Checksum Status: Unverified]<br>[Stream index: 0]<br>Domain Name System (query)<br>0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00<br>0020 40 02 d7 4d 00 35 00 2f 33 98 f5 b4 01 00 00 00 1<br>0020 40 00 20 d7 4d 00 35 00 2f 33 98 f5 b4 01 00 00 01<br>0030 00 00 00 00 00 01 32 06 64 65 62 69 61 66 04<br>0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00<br>0050 01<br>01<br>01<br>01<br>01<br>01<br>01<br>01<br>01<br>01   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| [Checksum Status: Unverified]<br>[Stream index: 0]<br>Domain Name System (query)<br>0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00<br>0020 00 43 6a 66 40 00 40 11 9d 4c c0 88 d9 03 c0 88<br>0020 00 00 40 00 35 00 21 33 98 f5 b4 01 00 00 80 1<br>0030 00 00 00 00 00 13 2 06 64 65 62 69 61 68 04<br>0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00<br>0056 61<br>   | <b>9</b>     |                       |                |               | 398 Fi        | inveri          | fiedl  |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| [Stream index: 0]           [Stream index: 0]             Domain Name System (query)           [Outopic content index: 0]             Otopic content index: 0]           [Outopic content index: 0]             Otopic content index: 0]           [Outopic content index: 0]             Outopic content index: 0]           [Outopic content index: 0]             [Outopic content index: 0]           [Outopic content index: 0]             [Outopic content index: 0]           [Outopic content index: 0]   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 90000       000 155 0d 40 577 16       00 60 15 50 40 577 05       00 80 00 45 00       • .004 <td< td=""><td>-</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>   | -            |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 0000       00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00<br>004 3 6a 66 40 00 40 11 9d 4c c0 a8 d9 03 c0 a8<br>0020 d9 02 07 4d 00 35 00 2f 33 98 f5 64 00 00 01<br>0030 00 00 00 00 00 00 00 01 32 64 65 62 96 61 00<br>0044 78 6f 6f 6c 03 6e 74 78 03 6f 72 67 00 00 01 00<br>01      ]@w]@w  | ٣.           |                       |                |               |               | uerv)           |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 0010       006       43       63       06       40       011       9d       4c       c0       8d       09       03       c3       06       43       63       06       40       01       9d       02       d9       02       d7       d4       06       35       06       43       08       43       64       60       06  |              |                       |                |               |               | ,               |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       | -        |
| 0920       d9 02 d7 dd 00 35 00 2f 33 98 f5 b4 01 00 00 01       33 98 f5 b4 01 00 00 01 01 32 06 64 65 62 69 61 66 04         0940       00 00 00 00 00 13 2 06 64 65 62 69 61 66 04  | F.           |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 0030 00 00 00 00 01 32 06 64 65 62 69 61 6e 04<br>0046 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00<br>0050 01  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00 pool-ntp .org   | 2            |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 0050 <b>01</b>   |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
|  | ••           |                       |                | 01 00         | 03 00         | e /4 /          | 0 03   | 01 72             | 07     | 00 00    | 9 01        | 00             | p00.               | · nrb | ·org         |         |        |         |        |          |       |           |      |         |       |          |
| Source or Destination Hardware Address (eth.addr), 6 bytes Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%) Profile: Default  |              | 0030                  | 01             |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| Source or Destination Hardware Address (eth.addr), 6 bytes Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%) Profile: Default  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| <ul> <li>Source or Destination Hardware Address (eth.addr), 6 bytes</li> <li>Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)</li> </ul>  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| <ul> <li>Z Source or Destination Hardware Address (eth.addr), 6 bytes</li> <li>Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)</li> <li>Profile: Default</li> </ul>  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| <ul> <li>Source or Destination Hardware Address (eth.addr), 6 bytes</li> <li>Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)</li> <li>Profile: Default</li> </ul>  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| <ul> <li>Source or Destination Hardware Address (eth.addr), 6 bytes</li> <li>Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)</li> </ul>  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
| 🕘 🍸 Source or Destination Hardware Address (eth.addr), 6 bytes 🛛 Packets: 358 - Displayed: 316 (88.3%) - Dropped: 0 (0.0%) 📄 Profile: Default  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        |          |       |           |      |         |       |          |
|  |              | 0 7                   | Source         | or Dest       | ination       | Hardwa          | re Add | ress (etl         | h.addr | r), 6 by | /tes        |                |                    | Р     | ackets       | : 358 · | Displa | ayed: 3 | 16 (88 | .3%) · I | Dropp | ed: 0 (0. | .0%) | Profi   | e: De | fault    |
|  |              |                       |                |               |               |                 |        |                   |        |          |             |                |                    |       |              |         |        |         |        | .,       |       |           | ,    |         |       |          |

The domain name of this packet is Standard query 0xf5b4 A 2.debian.pool.ntp.org, the source

IP and port number is 192.168.217.3:55117 and the destination IP and port number is

#### 192.168.217.2:53

**Q6.** Find the **corresponding** DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

| <pre>teid     teid     teid</pre>  | Applicat  | tions <b>T</b> P          | Places ▼        | H ull<br>Wireshark ▼           | Attacker Kali - E | cternal Workstation on C<br>Tue 21:44 | Y301-EMILL0  | 023 –         | в×            |            |              | ((اله محمر | ( <sup>1</sup> ) 🔻 |
|--|-----------|---------------------------|-----------------|--------------------------------|-------------------|---------------------------------------|--------------|---------------|---------------|------------|--------------|------------|--------------------|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help         Image: Statistics Telephony Wireless Tools Tools         Statistics Telephony Wireless Tools         Image: Statistics Telephony Wireless Tools         Image: Statistics Telephony Wireless Tools         Image: Tools  | rippileur |                           | uces            |                                |                   |                                       |              |               |               |            |              |            |                    |
| Image: Source       Destination       Protocol Length Info         192.168.217.3       192.168.217.2       DNS       61 Standard query 0x56bd AAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       61 Standard query response 0x56bd Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x56bd Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x56bd Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x56bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x56bd Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x56bd Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x68bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x68bd Refused         192.168.217.3       192.168.217.2       DNS       64 Standard query response 0x76bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x76bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x76bd Refused         192.168.217.3       DNS       54 Standard  |           |                           |                 |                                |                   | *eth0                                 |              |               |               |            |              |            | • •                |
| Image: Source       Destination       Protocol Length Info         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x95b4 A 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x95bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x95b4 AFUsed         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x95b4 AFUsed         192.168.217.2       192.168.217.2       DNS       81 Standard query response 0x95b4 AFUsed         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x95b4 AFUsed         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x95b4 AFUsed         192.168.217.3       192.168.217.2       DNS       84 Standard query response 0x95b4 AFUsed         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x95b4 AFUsed         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x95b4 AFUsed         192.168.217.2       192.168.217.2       DNS       81 Standard query response 0x95b4 AFUsed         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x80bd Refused         192.168.217.2       192.168.217.2       DN  | Ē         | ile <u>E</u> dit <u>V</u> | /iew <u>G</u> o | Capture Analyze Statistics     | Telephony         | Wireless Tools                        | <u>H</u> elp |               |               |            |              |            |                    |
| Image: Construction       Protocol Length Info         Source       Destination       Protocol Length Info         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x98bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.2       DNS       81 Standard query response 0x98bd Refused         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x95bd AFused         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x95bd AFused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x95bd AFused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x95bd AFused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x95bd Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x95bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x95bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x95bd Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x95bd Refused         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x95bd Refused <td></td> <td></td> <td></td> <td></td> <td>1 14 4</td> <td></td> <td>0</td> <td>**</td> <td></td> <td></td> <td></td> <td></td> <td></td>  |           |                           |                 |                                | 1 14 4            |                                       | 0            | **            |               |            |              |            |                    |
| Source         Destination         Protocol         Length         Info           192.168.217.3         192.168.217.2         DNS         81 Standard         query 0xf5b4 A 2.debian.pool.ntp.org           192.168.217.3         192.168.217.2         DNS         83 Standard         query 0xf5b4 A 2.debian.pool.ntp.org           192.168.217.2         192.168.217.3         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.3         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.3         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.2         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.3         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.3         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.2         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.2         192.168.217.2         DNS         54 Standard         query response 0xf5b4 Refused           192.168.217.2         192.168.217.2         DNS         54   |           |                           |                 |                                | ·*) I = =         |                                       | વવ           | 11            |               |            |              |            |                    |
| 192.168.217.3       192.168.217.2       DNS       81 Standard query 0xf5b4 A 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       63 Standard query 0xf5b4 A 2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0xf5b4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.2       192.168.217.2       DNS       81 Standard query response 0xf5b4 Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0xf5b4 Refused         192.168.217.2       DNS       61 Standard query response 0xf5b4 Refused       192.168.217.3         192.168.217.   |           | dns                       |                 |                                |                   |                                       |              |               |               |            |              | Expressio  | 1 +                |
| 192.168.217.3       192.168.217.2       DNS       64 Standard query 0x98bd AAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x15b4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x15b4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x15b4 Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x98bd AAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x98bd AAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x15b4 Refused         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x98bd Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x98bd Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x608e Refused         192.168.217.3       192.168.217.2       DNS       64 Standard query response 0x608e Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x608e Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x608e Refused <t< td=""><td></td><td>Source</td><td></td><td>Destination</td><td>Protocol</td><td>Length Info</td><td></td><td></td><td></td><td></td><td></td><td></td><td><b></b></td></t<>   |           | Source                    |                 | Destination                    | Protocol          | Length Info                           |              |               |               |            |              |            | <b></b>            |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query vresponse 6x4554 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x45b4 A 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       61 Standard query 0x45b4 A 2.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       61 Standard query 0x49bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x49bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x49bd AAAA 2.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query 0x49bd AAAA 2.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query 0x49bd AAAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x6698 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x6698 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x6698 Refused         192.168.217.2       192.168.217.2       DNS       64 Standard query response 0x6698 Refused         192.168.217.2       192.168.217.2       DNS       64 Standard query response 0x6698 Ref   | 9         | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               | 81 Standard                           | query (      | 0xf5b4 A      | 2.debian      | .pool.ntp  | .org         |            |                    |
| 102:106:217:2       102:106:217:3       005       54 Standard query response 0x9bbd Refused         192:106:217:3       192:106:217:3       192:106:217:2       DNS       81 Standard query response 0x9bbd Refused         192:106:217:3       192:106:217:3       192:106:217:3       DNS       64 Standard query response 0x9bbd Refused         192:106:217:3       192:106:217:3       DNS       64 Standard query response 0x9bbd Refused         192:106:217:2       192:106:217:3       DNS       54 Standard query response 0x9bbd Refused         192:106:217:2       192:106:217:3       DNS       54 Standard query response 0x9bbd Refused         192:106:217:2       192:106:217:3       DNS       54 Standard query response 0x9bbd Refused         192:106:217:2       192:106:217:3       DNS       54 Standard query response 0x60e8 Refused         192:106:217:2       192:106:217:3       DNS       54 Standard query response 0x60e8 Refused         192:106:217:2       192:106:217:3       DNS       54 Standard query response 0x60e8 A 3.debian.pool.ntp.org         192:106:217:3       DNS       54 Standard query response 0x60e8 A 3.debian.pool.ntp.org         192:106:217:3       DNS       54 Standard query response 0x60e8 A 3.debian.pool.ntp.org         192:106:217:3       DNS       54 Standard query response 0x60e8 A 3.debian.pool.ntp.org  |           | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               | 81 Standard                           | query (      | 0x98bd AA     | AAA 2.deb     | ian.pool.  | ntp.org      |            |                    |
| <ul> <li>192.168.217.3 192.168.217.2 DNS &amp;1 Standard query @xf5b4 A 2.debian.pool.ntp.org</li> <li>192.168.217.3 192.168.217.2 DNS &amp;1 Standard query @xf5b4 A 2.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.3 DNS 54 Standard query @x69b4 AAA.2.debian.pool.ntp.org</li> <li>192.168.217.3 192.168.217.3 DNS 54 Standard query @x69b4 AAA.2.debian.pool.ntp.org</li> <li>192.168.217.3 192.168.217.3 DNS 54 Standard query @x69b4 AAA.3.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.2 DNS 61 Standard query @x69b6 A A.3.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.2 DNS 61 Standard query @x87ee AAAA 3.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.3 DNS 54 Standard query @x87ee AAAA 3.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.3 DNS 54 Standard query @x87ee AAAA 3.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.3 DNS 54 Standard query @x87ee AAAA 3.debian.pool.ntp.org</li> <li>192.168.217.2 192.168.217.2 DNS 81 Standard query @x87ee Refused</li> <li>192.168.217.3 192.168.217.2 DNS 81 Standard query @x87ee Refused</li> <li>192.168.217.3 192.168.217.2 DNS 81 Standard query @x869e A A 3.debian.pool.ntp.org</li> <li>192.168.217.3 DNS 54 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.4 DNS 81 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.5 DNS 81 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.3 DNS 54 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.4 DNS 81 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.5 DNS 81 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.4 DNS 81 Standard query @x869e A 3.debian.pool.ntp.org</li> <li>192.168.217.2 DNS 81</li></ul>  | s         | 192.168.2                 | 217.2           | 192.168.217.3                  | DNS               | 54 Standard                           | query        | response      | 0xf5b4 R      | lefused    |              |            |                    |
| <ul> <li>192.168.217.3 192.168.217.2 DNS 81 Standard query exsBnd AAAA 2.debian.pool.ntp.org<br/>192.168.217.2 192.168.217.3 DNS 54 Standard query response 0x5b4 Refused<br/>192.168.217.2 192.168.217.3 DNS 54 Standard query response 0x5b4 Refused<br/>192.168.217.3 192.168.217.2 DNS 81 Standard query response 0x8bd Refused<br/>192.168.217.3 192.168.217.2 DNS 81 Standard query response 0x8be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 54 Standard query response 0x8be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 54 Standard query response 0x8be8 Refused<br/>192.168.217.3 192.168.217.3 DNS 54 Standard query response 0x8be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 54 Standard query response 0x8be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 54 Standard query response 0x8be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 54 Standard query response 0x7be8 Refused<br/>192.168.217.3 192.168.217.3 DNS 54 Standard query response 0x7be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 51 Standard query response 0x7be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 51 Standard query response 0x7be8 Refused<br/>192.168.217.3 192.168.217.2 DNS 54 Standard query response 0x7be8 Refused<br/>192.168.217.2 DNS 55 Standard query response 0x7be8 Refused<br/>192.168.217.2 DNS 55 Standard query respon</li></ul> |           | 192.168.2                 | 217.2           | 192.168.217.3                  | DNS               |                                       |              |               |               |            |              |            |                    |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x5b4 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x5b4 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query response 0x5b4 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       54 Standard query 0x7ee AAAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x60e8 A 4.00         192.168.217.3       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x67ee Refused         192.168.217.3       DNS       54 Standard query 0x60e8 A 3.debian.nool.ntn.org         192.168.217.3       DNS <td></td> <td>192.168.2</td> <td>217.3</td> <td>192.168.217.2</td> <td>DNS</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>   |           | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               |                                       |              |               |               |            |              |            |                    |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query esponse 0x38bd Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x7ee AAA 3. debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x7ee AAA 3. debian.pool.ntp.org         192.168.217.2       192.168.217.2       DNS       54 Standard query 0x7ee AAA 3. debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query exponse 0x50e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query exponse 0x50e8 Refused         192.168.217.2       192.168.217.2       DNS       54 Standard query exponse 0x50e8 Refused         192.168.217.3       192.168.217.2       DNS       54 Standard query exponse 0x50e8 Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.3       DNS       54 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3       DNS       51 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3       DNS       51 Standard query 0x60e8 A 3.debian.pool.ntp.org         192.168.217.3 <t< td=""><td></td><td>192.168.2</td><td>217.3</td><td>192.168.217.2</td><td>DNS</td><td></td><td></td><td></td><td></td><td></td><td>ntp.org</td><td></td><td></td></t<>   |           | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               |                                       |              |               |               |            | ntp.org      |            |                    |
| 192.168.217.3       192.168.217.2       DNS       81 Standard query 0x0e84 A 3.debian.pool.ntp.org         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x7ee AAAA 3.debian.pool.ntp.org         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query response 0x67ee Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query exponse 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query exponse 0x67ee Refused         192.168.217.3       192.168.217.3       DNS       51 Standard query exponse 0x67ee Refused         192.168.217.3       DNS       51 Standard query exponse 0x67ee Refused          192.168.217.3       DNS       51 Standard query exponse 0x67ee Refused          192.168.217.3       DNS       51 Standard query exponse 0x67ee Refused          192.168.217.3       DNS   |           | 192.168.2                 | 217.2           | 192.168.217.3                  | DNS               |                                       |              |               |               |            |              |            |                    |
| 192.168.217.3       192.168.217.2       DNS       81 Standard query expose 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x60e8 Refused         192.168.217.3       DNS       54 Standard query response 0x60e8 Refused         Viser Datagram Protocol, src Port: 53       Dst Port: 55117         Source Port: 53       Dst Port: 55117         Length: 20       Checksum: 6x7e31 [unverified]         [Checksum: dx1au: Unverified]       [Stream index: 0]         > Domain Name System (response)       ·(•)@viseE.         0010       60 28 ac 84 60 00 40 41 19 a e9 c0 a8 d9 62 c6 a8       ·(•)@viseE.         0038       80 60 60 80 60 60       ·· <td></td> <td>192.168.2</td> <td>217.2</td> <td>192.168.217.3</td> <td>DNS</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>  |           | 192.168.2                 | 217.2           | 192.168.217.3                  | DNS               |                                       |              |               |               |            |              |            |                    |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x80e8 Refused         192.168.217.2       192.168.217.3       DNS       54 Standard query response 0x80e8 Refused         192.168.217.2       192.168.217.2       DNS       54 Standard query response 0x80e8 Refused         192.168.217.2       192.168.217.2       DNS       81 Standard query response 0x80e8 A 3.debian.nool.ntn.org         Internet Protocol Version 4, Src: 192.168.217.2, DSt: 192.168.217.3       Issure Port: 53       Dst Port: 55117         Source Port: 53       Destination Port: 55117       Ength: 20         Checksum: Sore31 [unverified]       [Checksum Status: Unverified]       [Checksum Status: Unverified]         [Stream index: 0]       Domain Name System (response)       Image: 100 Image: 1  |           | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               |                                       |              |               |               |            |              |            |                    |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query esponse 0xe7ee Refused         192.168.217.3       192.168.217.3       DNS       54 Standard query 0x60e8 A 3.debian.nool.nto.org         Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3       Surce Port: 53, Dst Port: 55117       Surce Port: 55         Source Port: 53       Destination Port: 55117       Length: 20         Checksum: 8x7e31 [unverified]       [Checksum Status: Unverified]         [Stream index: 0]       Domain Name System (response)         0000       00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00      [00         0010       02 8a c84 00 00 40 11 9a e9 c0 a8 d9 92 cc0 a8      [00         0030       06 00 00 00 00       00 11 7 531 5b 481 05 00 00      [00  |           | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               |                                       |              |               |               |            | ntp.org      |            |                    |
| 192.168.217.2       192.168.217.3       DNS       54 Standard query esponse 0xe7ee Refused         192.168.217.3       192.168.217.2       DNS       81 Standard query 0x60e8 A 3.debian.nool.ntn.org         Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3       Surce Port: 53       Dst port: 55117         Surce Port: 53       Destination Port: 55117       Destination Port: 55117         Length: 20       Checksum: Satus: Unverified]       [Checksum Status: Unverified]         [Checksum Name System (response)       0000       00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00      ]0WE.         0010       09 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8      ]0WE.       (0)   | M         | 192.168.2                 | 217.2           | 192.168.217.3                  | DNS               |                                       |              |               |               |            |              |            |                    |
| <ul> <li>Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3</li> <li>User Datagram Protocol, Src Port: 53, Dst Port: 55117<br/>Source Port: 53<br/>Destination Port: 55117<br/>Length: 20<br/>Checksum Status: Unverified]<br/>[Checksum Status: Unverified]<br/>[Checksum Status: Unverified]</li> <li>Domain Name System (response)</li> <li>0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00<br/>0010 00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8<br/>0010 00 28 ac 84 00 00 44 11 9a e9 c0 a8 d9 02 cc a8<br/>0030 06 00 00 00 00 14 7e 31 f5 b4 81 05 00 00<br/>0030 06 00 00 00 00 00</li> </ul>  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| <ul> <li>Internet Protocol version 4, Sr2: 192.108.217.2, USC: 192.108.217.3</li> <li>Internet Protocol, Src Port: 53, Dst Port: 55117</li> <li>Source Port: 53</li> <li>Destination Port: 55117</li> <li>Length: 20</li> <li>Checksum: 0x7e31 [unverified]</li> <li>[Stream index: 0]</li> <li>Domain Name System (response)</li> <li>0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00</li> <li>0000 00 15 5d 40 57 05 00 14 7e 31 f5 b4 81 05 00 00</li> <li>0000 00 00 00 00 00 00 00</li> </ul>  |           | 192.168.2                 | 217.3           | 192.168.217.2                  | DNS               | 81 Standard                           | auerv (      | 0x60e8 A      | 3.debian      | .nool.ntn  | .ora         |            |                    |
| <ul> <li>User Datagram Protocol, Src Port: 53, Dst Port: 55117<br/>Source Port: 53<br/>Destination Port: 55117<br/>Length: 29<br/>Checksum Status: Unverified]<br/>[Checksum Status: Unverified]<br/>[Checksum Status: Unverified]<br/>[Stream index: 0]</li> <li>Domain Name System (response)</li> <li>0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00<br/>0010 00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8<br/>0000 00 00 00 00 00 00 00 14 7e 31 f5 b4 81 05 00 00<br/>0030 00 00 00 00 00 00 00</li> <li></li></ul>  |           | T                         | Ductors         |                                | 0.017.0           | D-+- 400 400 0                        | 47.0         |               |               |            |              |            |                    |
| Source Port: 53         Destination Port: 5517         Length: 20         Checksum: 0x7e31 [unverified]         [Stream index: 0]         Domain Name System (response)         0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00         0010 00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8         0030 00 00 08 5d 7 4d 00 14 7e 31 f5 b4 81 05 00 00         0030 06 00 08 00 00 08   |           |                           |                 |                                |                   |                                       | 17.3         |               |               |            |              |            | <u>^</u>           |
| Destination Port: 55117         Length: 20         Checksum: 0x7e31 [unverified]         [Checksum: three right]         Stream index: 0]         Domain Name System (response)         0000       00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00         0010       600 28 ac 84 00 00 40 11 9a e9 c6 a8 d9 02 c6 a8         0030       00 00 00 00 00 00 00   | XXX I     |                           |                 |                                | SC POIL. 3        | 5117                                  |              |               |               |            |              |            |                    |
| Checksum: 0x7c31 [unverified]<br>[Checksum: 0x7c31 [unverified]<br>[Stream index: 0]         Domain Name System (response)         0000       00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00<br>0010       •··[0w·•··E·································   |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| Checksum: 0x7e31 [unverified]<br>[Checksum Status: Unverified]<br>[Stream index: 0]         Domain Name System (response)         0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00<br>0010 00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8<br>0030 00 00 00 5d 7 d4 00 14 7e 31 f5 b4 81 05 00 00<br>0030 06 00 06 00 00   | $\sim$    |                           |                 | 11. 55117                      |                   |                                       |              |               |               |            |              |            |                    |
| Image: Checksum Status: Unverified]         [Stream index: 0]         Domain Name System (response)         Image: Open index: 0]         0000       00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00         0010       00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8         0020       09 03 00 35 d7 4d 00 14 7e 31 f5 b4 81 05 00 00         0030       00 00 00 00 00 00 00   | 6         |                           |                 | 31 [unverified]                |                   |                                       |              |               |               |            |              |            |                    |
| Image: Stream index: 0]       Domain Name System (response)         Image: Stream index: 0]       Domain Name System (response)         Image: Stream index: 0]       Image: Stream index: 0]         Image: Stream index: 0]       Image: Stream index: 0]<   |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| Image: System (response)         Image: Sy  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| 0000         00 15 5d 40 57 65 00 15 5d 40 57 1f 08 00 45 00           0010         00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8           0020         d9 03 00 35 d7 4d 00 14 7e 31 f5 b4 81 05 00 00           0030         00 00 00 00 00 00  | Γ.        |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| 0010         00 28 ac 84 00 00 40 11 9a e9 c0 a8 d9 02 c0 a8         10 c0   | _         |                           |                 | (,                             |                   |                                       |              |               |               |            |              |            | -                  |
| 0010         002 8 ac 84 00 00 40 11         9a e9 c0 a8 d9 02 c0 a8         ((····))         (····)           0020         09 03 00 55 d7 4d 00 14         7e 31 f5 b4 81 05 00 00         ····································   |           | 0000 00 1                 | 15 5d 40        | 57 05 00 15 5d 40 57 1         | 6 08 00 45        | 5.00 ···1@W·••                        | 1@W-         | E.            |               |            |              |            |                    |
| 0020 0920 d9 03 00 35 d7 4d 00 14 7e 31 f5 b4 81 05 00 005.M. ~1   |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| 0030 00 00 00 00 00 00 00  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  | <b></b> e |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
|  |           |                           |                 |                                |                   |                                       |              |               |               |            |              |            |                    |
| Source or Destination Hardware Address (eth.addr), 6 bytes Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%) Profile: Defau  |           | 🔍 🗹 Sour                  | ce or Destir    | nation Hardware Address (eth.a | ddr), 6 bytes     | F                                     | ackets: 35   | 58 · Displaye | ed: 316 (88.) | 3%)∙Droppe | ed: 0 (0.0%) | Profile:   | Default            |

The source IP and port number is 192.168.217.2:53 and the destination IP and port number is

192.168.217.3:55117, the message is "Refused" with a flag of 0x8105