





Security Apps with P4 Programmable Switches

### Mitigating DNS amplification attack in P4

Ali AlSabeh, Jorge Crichigno University of South Carolina http://ce.sc.edu/cyberinfra

University of South Carolina (USC) Energy Sciences Network (ESnet)

September 18, 2023

### Lab 8: Detecting and Mitigating the DNS Amplification Attack

### Domain Name System (DNS)

- The Domain Name System (DNS) is an essential component of the internet
- It is responsible for translating humanreadable domain names into IP addresses that can be understood by devices connected to the internet<sup>1</sup>



### **DNS** Amplification

- Due its frequent use on the Internet, the DNS is susceptible to many attacks
- DNS amplification is an attack that exploits the infrastructure of the DNS to create a Distributed Denial of Service (DDoS) on a target victim
  - > Thus, rendering the victim unresponsive due to the large amount of traffic received



# **DNS Amplification**

- In a DNS amplification attach, the attacker sends DNS requests with spoofed source IP address
  of the target victim
- The DNS server responds to all the requests and send them to the target victim
- Typically, a valid response is much larger than the request



### **Attack Scenario**

- The attacker performs a DNS amplification attack using the source IP address of the victim
- The DNS server responds to the DNS requests and sends them to the victim
- The P4 switch drops all the DNS replies that do not associate with DNS requests issued by the victim
- The P4 switch forwards legitimate DNS replies requested by the victim



### **DNS Header Fields**

- UDP packets with source or destination port 53 are DNS packets
- The transaction ID is generated by the client upon sending a DNS request
- The DNS *qr* flag indicates that the DNS packet is request (*qr*=0) or response (*qr*=1)



# Lab Topology

The topology consists of:

- Host h1 representing the victim of the DNS amplification attack
- Host h2 representing the attacker and the DNS resolver
- Programmable switch s1 that forwards traffic and protects against DNS amplification attack



### **DNS Amplification without Mitigation**

#### Performing DNS amplification

|   |  |   |  |  |  | 1 <b>* *</b>                                    |   |
|---|--|---|--|--|--|---|---|
| <u>C</u>  |  |   | Host: h2   |  | - 0 ×  | Device h1-e                                     | th0 [10.0.0.1] (1/2):                   |
| oot@lubuntu   | u-vm:/home   | /admin# ./perf  | orm_DNS  | _amplification.sh  |  | <pre>====================================</pre> |   |
|   |  |   |  |  |  |   | ####################################### |
|   |  |   |  |  |  |   | ####################################### |
|   |  |   |  |  |  |   | ####################################### |
|   |  | am  | plification.p  | ocap   | - 2 X  |   | ****                                    |
| le Edit View Go   | Capture Analyze  | a Statistics Telephony  | Wireless Tools   | Help   |  |   | *************************************** |
|   |  |   |  |  |  |   | *****                                   |
|   |  | i I 🍳 듲 🔿 🔜 7   | F 生 📃 I  |  |  |   | ####################################### |
|   |  |   |  |  |  |   | ####################################### |
| Apply a display filte   | r <ctrl-></ctrl->  |   |  |  |  |   | ****                                    |
| Time  | Source   | Destination   | Protocol   | Length Info  | A  |   |   |
| 1 0.000000  | 10.0.0.2   | 10.0.0.1  | DNS  | 135 Standard query response 0xa0ff A   | NY fonts.googlea   |   | *****                                   |
| 2 0.077750  | 10.0.0.2   | 10.0.0.1  | DNS  | 1128 Standard query response 0xc872 A  | NY google.com A  | Outgoing:                                       |   |
| 3 0.116868  | 10.0.0.2   | 10.0.0.1  | DNS  | 513 Standard query response 0xa952 A   | NY youtube.com /   |   |   |
| 4 0.205087  | 10.0.0.2   | 10.0.0.1  | IPv4   | 1514 Fragmented IP protocol proto=UD   | P 17, off=0, ID=   |   |   |
| 5 0.282926  | 10.0.0.2   | 10.0.0.1  | DNS  | 775 Standard query response 0x13f5 A   | NY instagram.com   |   |   |
|   | 40 0 0 0   | 10 0 0 1  | DNS  | 311 Standard guery response Avadah A   | WV googlatageon  |   |   |
| 6 0.322254  | 10.0.0.2   | 10.0.1  | DNO  | SII Scandard query response bravab A   | NY googretagmana   |   |   |
| 6 0.322254<br>7 0.420935  | 10.0.0.2   | 10.0.0.1  | DNS  | 94 Standard query response 0x7793 A  | NY googlelagmana<br>NY s.w.org A 192   |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951  | 10.0.0.2<br>10.0.0.2<br>10.0.0.2   | 10.0.0.1<br>10.0.0.1<br>10.0.0.1  | DNS  | 94 Standard query response 0x7793 A<br>104 Standard query response 0xc5e1 A  | NY googletagmana<br>NY s.w.org A 192<br>NY linkedin.com  |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951<br>9 0.589614  | 10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2   | 10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1  | DNS<br>DNS<br>DNS  | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7591 A<br>214 Standard query response 0x0397 A  | NY GOOGLELAGMANA<br>NY s.w.org A 192<br>NY linkedin.com<br>NY gmpg.org SOA   |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951<br>9 0.589614<br>10 0.633033   | 10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2   | 10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1  | DNS<br>DNS<br>DNS<br>DNS<br>DNS                                    | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7593 A<br>214 Standard query response 0x0397 A<br>134 Standard query response 0x0397 A  | NY googletagmana<br>NY s.w.org A 192<br>NY linkedin.com<br>NY gmpg.org SOA<br>NY ajax.googlea  |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951<br>9 0.589614<br>10 0.633033<br>11 0.721982  | 10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2   | 10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1  | DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS                             | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7793 A<br>214 Standard query response 0x0397 A<br>134 Standard query response 0x39b6 A<br>124 Standard query response 0x15b0 A  | NY googletamana<br>NY s.w.org A 192<br>NY linkedin.com<br>NY gmpg.org SOA<br>NY ajax.googlea<br>NY fonts.gstatic   |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951<br>9 0.589614<br>10 0.633033<br>11 0.721982<br>12 0.794274                               | 10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2<br>10.0.0.2   | $10.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.$ | DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS               | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7793 A<br>214 Standard query response 0x0397 A<br>134 Standard query response 0x39b6 A<br>124 Standard query response 0x15b0 A<br>277 Standard query response 0x6dd9 A  | NY googletagman<br>NY s.w.org A 192<br>NY linkedin.com<br>NY gmpg.org SOA<br>NY ajax.googlea<br>NY fonts.gstatic<br>NY plus.google.c   |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951<br>9 0.589614<br>10 0.633033<br>11 0.721982<br>12 0.794274<br>13 0.837086                | 10.0.0.2 $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$   | $10.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.1 \\ 10.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0.0.0.0 \\ 10.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.$   | DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS               | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7593 A<br>214 Standard query response 0x0397 A<br>134 Standard query response 0x396 A<br>124 Standard query response 0x15b0 A<br>277 Standard query response 0x5602 A<br>294 Standard query response 0x5602 A   | NY googletagman<br>NY s.w.org A 19:<br>NY linkedin.com<br>NY gmpg.org SOA<br>NY ajax.googlea<br>NY fonts.gstatic<br>NY plus.google.c   |   |   |
| 6 0.322254<br>7 0.420935<br>8 0.514951<br>9 0.589614<br>10 0.633033<br>11 0.721982<br>12 0.794274<br>13 0.837086<br>14 0.926681 | 10.0.0.2 $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$ $10.0.0.2$   | 10.0.0.1 $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$   | DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7793 A<br>104 Standard query response 0x0597 A<br>134 Standard query response 0x39b6 A<br>124 Standard query response 0x3b6 A<br>277 Standard query response 0x6dd9 A<br>294 Standard query response 0x6dd9 A<br>582 Standard query response 0x33a9 A | NY googletagman<br>NY s.w.org A 192<br>NY linkedin.com<br>NY gmpg.org SOA<br>NY ajax.googlea<br>NY fonts.gstatic<br>NY fonts.gstatic<br>NY plus.google.c<br>NY maps.google.c<br>NY youtu.be A 1. |   |   |
| 6 0.32254<br>7 0.420935<br>8 0.514951<br>9 0.589614<br>10 0.633033<br>11 0.721982<br>12 0.794274<br>13 0.837086<br>14 0.926681  | $\begin{array}{c} 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ 10.0.0.2\\ \end{array}$ | 10.0.0.1 $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$ $10.0.0.1$   | DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS<br>DNS        | 94 Standard query response 0x7793 A<br>104 Standard query response 0x7793 A<br>104 Standard query response 0x0397 A<br>134 Standard query response 0x39b6 A<br>124 Standard query response 0x3bb6 A<br>277 Standard query response 0x5b0 A<br>294 Standard query response 0x50d2 A<br>582 Standard query response 0x33a9 A | NY googletagman<br>NY s.w.org A 192<br>NY linkedin.com<br>NY gmpg.org SOA<br>NY ajax.googlea<br>NY fonts.gstatic<br>NY plus.google.c<br>NY maps.google.c<br>NY youtu.be A 1                      |   |   |

#### Inspecting resource usage at the victim

"Host: h1"

| Curr: | 1.15 kBit/s  |
|-------|--------------|
| Avg:  | 1.34 kBit/s  |
| Min:  | 0.00 Bit/s   |
| Max:  | 18.27 kBit/s |
| Ttl:  | 104.48 kByte |

- 2 X

\_\_\_\_\_

: 41.05 MBit/s 17.76 MBit/s 0.00 Bit/s 45.44 MBit/s 337.19 MByte

### **DNS Amplification Mitigation with P4**

#### Defining DNS header

#### headers.p4 - lab8 - Visual Studio Code parser.p4 - lab8 - Visual Studio Code File Edit Selection View Go Run Terminal Help File Edit Selection View Go Run Terminal Help G = parser.p4 • EXPLORER headers.p4 EXPLORER headers.p4 LAB8 ≡ parser.p4 V LAB8 ≡ headers.p4 23 state parse ipv4 { 34 {} basic.json C {} basic.json 33 packet.extract(hdr.ipv4); 24 basic.p4 ≡ basic.p4 header udp t { transition select(hdr.ipv4.protocol) { 34 25 basic.p4i ≡ basic.p4i 35 bit<16> srcPort; 26 TYPE UDP: parse udp; checksum.p4 default: accept; 36 bit<16> dstPort; 27 ≡ checksum.p4 deparser.p4 28 bit<16> len; 37 deparser.p4 egress.p4 29 38 bit<16> checksum; egress.p4 30 state parse udp { 39 headers.p4 headers.p4 31 packet.extract(hdr.udp); 40 ingress.p4 transition select(hdr.udp.srcPort, hdr.udp.dstPort) { 32 ingress.p4 /\* Define the DNS header below\*/ 41 lab8.mn (TYPE DNS, ): parse dns; 33 🗉 lab8.mn 42 header dns t { parser.p4 34 (,TYPE DNS): parse dns; bit<16> transaction id; 43 parser.p4 35 ( , ): accept; 44 bit<1> qr flag; 36 45 bit<7> padding; 37 46 38 state parse dns { 47 packet.extract(hdr.dns); 39 48 struct metadata { 40 transition accept; 49 /\*empty\*/ 41 50 42

Transitioning and extracting DNS header

## DNS Amplification Mitigation with P4

Defining a function that computes a unique flow ID based on the 5-tuple (used for DNS requests)

| ⊲              |                          |          | 🌒 ingress.p4 - lab8 - Visual Studio Code                         |
|----------------|--------------------------|----------|--|
| File           | Edit Selection View Go   | Run Term | inal Help  |
| C1             | EXPLORER                 | ≣ header | rs.p4 $\equiv$ parser.p4 $\equiv$ ingress.p4 $\bullet$           |
|                | $\sim$ LAB8              | ≡ ingres | is.p4  |
| Q              | <pre>{} basic.json</pre> | 29       |  |
|                | ≣ basic.p4               | 30       | <pre>register<bit<16>&gt;(65535) transaction_ids;</bit<16></pre> |
| Ŷ٥             | ≣ basic.p4i              | 31       | <pre>bit&lt;16&gt; idx;</pre>                                    |
| 8              | ≣ checksum.p4            | 32       | antian annuts flow id/) (f                                       |
| ~              | ≡ deparser.p4            | 33       | action compute_flow_id()   |
| ±,>            | ≡ egress.p4              | 34       | idy  |
|                | ≡ headers.p4             | 36       | HashAlgorithm.crc16.   |
| R <sup>O</sup> | ≡ ingress.p4             | 37       | (bit<1>)0,   |
| 9              | ≡ lab8.mn                | 38       | {  |
|                | = narser n/              | 39       | hdr.ipv4.srcAddr,  |
|                | = parser.p4              | 40       | hdr.ipv4.dstAddr,  |
|                |                          | 41       | hdr.udp.srcPort,   |
|                |                          | 42       | hdr.udp.dstPort,   |
|                |                          | 43       | hdr.ipv4.protocol  |
|                |                          | 44       |  |
|                |                          | 45       | (D1T<10>) 05535  |
|                |                          | 40       | li l                         |
|                |                          | 4/       | N  |
|                |                          | 40       |  |

Defining a function that computes a unique flow ID based on the 5-tuple (used for DNS replies)

| <₽  |   | ● ingress.p4 - lab8 - Visual Studio Code   |
|---|---|--|
| File Edit Selection View Go   | Run Terminal Hel  | p  |
| EXPLORER  | ≣ headers.p4  | $\equiv$ parser.p4 $\equiv$ ingress.p4 $\bullet$   |
| V LAB8  | ≡ ingress.p4  |  |
| <ul> <li>♀</li> <li>♀</li></ul> | 46<br>47<br>48<br>49<br>50<br>51<br>52<br>53<br>54<br>55<br>56<br>57<br>58<br>59<br>60<br>61<br>62<br>63<br>64<br>}<br> | <pre>);<br/>ion compute_reverse_flow_id() {     hash(         idx,         HashAlgorithm.crc16,         (bit&lt;1&gt;)0,         {             hdr.ipv4.dstAddr,             hdr.ipv4.srcAddr,             hdr.udp.dstPort,             hdr.udp.srcPort,             hdr.ipv4.protocol         },         (bit&lt;16&gt;) 65535 );</pre> |

## DNS Amplification Mitigation with P4

Using the flow ID to save the transaction ID of DNS request in a P4 register

| ≺    |                          |    |           |         |                            | ● ingress.p4 - lab8 - Visual Studio Code                                  |
|------|--------------------------|----|-----------|---------|----------------------------|---|
| File | Edit Selection View      | Go | Run Termi | inal He |                            |   |
| G    | EXPLORER                 |    | ≣ header  | s.p4    | ≣ parser.p4                | ≣ ingress.p4 ●  |
|      | V LAB8                   |    | ≡ ingres  | s.p4    |                            | 12 I.   |
| Q    | <pre>{} basic.json</pre> |    | 54        |         | {                          |   |
|      | ≡ basic.p4               |    | 55        |         | hdr.i                      | .pv4.dstAddr,   |
| 90   | ≣ basic.p4i              |    | 56        |         | hdr.i                      | pv4.srcAddr,  |
| 5    | ≡ checksum.p4            |    | 57        |         | hdr.u                      | dp.dstPort,   |
|      | deparser.p4              |    | 58        |         | hdr.u                      | dp.srcPort,   |
| ±,>  | ≡ egress.p4              |    | 59        |         | ndr.1                      | pv4.protocol  |
|      | = headers.p4             |    | 61        |         | },<br>(hit<165)            | 65525   |
| - A- | $\equiv$ ingress p4      |    | 62        |         |                            | 0000  |
|      | = lab8 mn                |    | 63        | 3       | ,                          |   |
|      |                          |    | 64        | ,       |                            |   |
|      | ≞ parser.p4              |    | 65        | app     | {                          |   |
|      |                          |    | 66        |         | <mark>f (</mark> hdr.dns.i | sValid()) {   |
|      |                          |    | 67        |         | if (hdr.d                  | ns.qr_flag == 0) {  |
|      |                          |    | 68        |         | compu                      | <pre>ite_flow_id();</pre>   |
|      |                          |    | 69        |         | trans                      | <pre>action_ids.write((bit&lt;32&gt;) idx, hdr.dns.transaction_id);</pre> |
|      |                          |    | 70        |         | forwa                      | rding.apply();  |
|      |                          |    | 71        |         | }                          |   |
|      |                          |    | 72        |         |                            |   |
|      |                          |    | 73        | }       |                            |   |
|      |                          |    | 74 }      |         |                            |   |

Using the flow ID to retrieve the transaction ID of DNS request saved in a P4 register and comparing it with the transaction ID of the received DNS reply

| ) ingress.p4 - lab8 - Visual Studio Code   |
|--|
| Terminal Help  |
| neaders.p4 $\equiv$ parser.p4 $\equiv$ ingress.p4 $\bullet$  |
| ingress.p4   |
| 4  |
| 5 apply {  |
| 6 if (hdr.dns.isValid()) {   |
| 7 if (hdr.dns.qr_flag == 0) {  |
| 8 compute_flow_id();   |
| <pre>g transaction_ids.write((bit&lt;32&gt;) idx, ndr.dns.transaction_id);<br/>forwarding_apply();</pre> |
| 1 Stwarding.appry();   |
| else if (hdr.dns.gr flag == 1) {   |
| 3 bit<16> transaction id;  |
| 4 compute reverse flow id();   |
| <pre>5 transaction ids.read(transaction id, (bit&lt;32&gt;) idx);</pre>                                  |
| <pre>6 if (transaction_id == hdr.dns.transaction_id) {</pre>   |
| <pre>7 forwarding.apply();</pre>   |
| 8 }  |
| 9 else {   |
| 0 drop();  |
|  |
|  |
|  |
| ++   J<br>5 }  |
|  |

# **DNS Amplification with Mitigation**

### Performing DNS amplification

|  |  |   |   | <u></u>  |                      | HUSLI III |  |
|--|--|---|---|--|----------------------|-----------|--|
| X  |  |   | "Host: h2"  | – 🗷 🗙 Device   | h1-eth0 [10.0.0.1] ( | 1/2):     |  |
| root@lubu  | ntu-vm:/home,  | /admin# ./per   | form_DNS_amplification.sh   | Incomi   | ng :                 |           |  |
| <u>File Edit V</u> iew   | <u>Go</u> <u>C</u> apture <u>A</u> nalyze  | am<br><u>S</u> tatistics Telephony  | nplification.pcap<br><u>W</u> ireless <u>T</u> ools <u>H</u> elp  | - ø ×  |                      |           | Curr: 0.00 Bit/s   |
| Apply a display  | ) 📄 🔝 🔀 🎑  | )   🤇 🗢 🔿 警 🤇   | <b>₹ ⊻ _ =</b> € € € ₩  |  |                      |           | Avg: 8.00 Bit/s<br>Min: 0.00 Bit/s<br>Max: 53.73 MBit/s  |
| No.         Time           10.00000         2           20.0775         3           30.11686         4           40.20508         5           50.28292         6           70.42093         8           80.51495         9           90.58961         10           100.63303         11           120.79427         13           130.83708 | Source           0         10.0.0.2           0         10.0.0.2           8         10.0.0.2           7         10.0.0.2           6         10.0.0.2           5         10.0.0.2           1         10.0.0.2           1         10.0.0.2           1         10.0.0.2           1         10.0.0.2           1         10.0.0.2           2         10.0.0.2           4         10.0.0.2           3         10.0.0.2           6         10.0.0.2           6         10.0.0.2 | Destination<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1<br>10.0.0.1 | Protocol Lendth InfoDNS135 Standard query response0x08DNS1128 Standard query response0x08DNS513 Standard query response0x08IPv41514 Fragmented IP protocolprotDNS311 Standard query response0x13DNS311 Standard query response0x49DNS311 Standard query response0x44DNS94 Standard query response0x47DNS104 Standard query response0x63DNS134 Standard query response0x39DNS124 Standard query response0x39DNS124 Standard query response0x36DNS277 Standard query response0x50DNS294 Standard query response0x50 | Iff ANY fonts.google;         772 ANY google.com A         52 ANY youtube.com A         52 ANY youtube.com A         o=UDP 17, off=0, ID:         175 ANY instagram.com         193 ANY s.w.org A 192         191 ANY jong.gorg SOA         196 ANY ajax.googlea;         190 ANY fonts.gstatic         193 ANY pas.google.com | ng :                 |           | Ttl: 472.57 MByte<br>Curr: 0.00 Bit/s<br>Avg: 0.00 Bit/s |
| 14 0.92668   | 1 10.0.0.2   | 10.0.0.1  | DNS 582 Standard query response 0x33  | ANY youtu.be A 17  |                      |           | Min: 0.00 Bit/s<br>Max: 27.54 kBit/s<br>Ttl: 42.41 kBvte |

#### Inspecting resource usage at the victim