

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: KỸ THUẬT GIÁM SÁT AN TOÀN MẠNG
Phân tích gói tin DNS sử dụng Tshark

Sinh viên thực hiện: Nguyễn Tuấn Đạt – B21DCAT058

Giảng viên hướng dẫn: THs. Ninh Thị Thu Trang

HÀ NỘI 3-2025

Mục lục

1. Mục đích	3
2. Yêu cầu đối với sinh viên	3
3. Nội dung thực hành.....	3
4. Kết thúc bài lab:	3

Nội dung và hướng dẫn bài thực hành

1. Mục đích

Giúp sinh viên hiểu rõ cách phân tích gói tin DNS và nắm vững kỹ năng phân tích lưu lượng mạng.

2. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ Tshark.

3. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

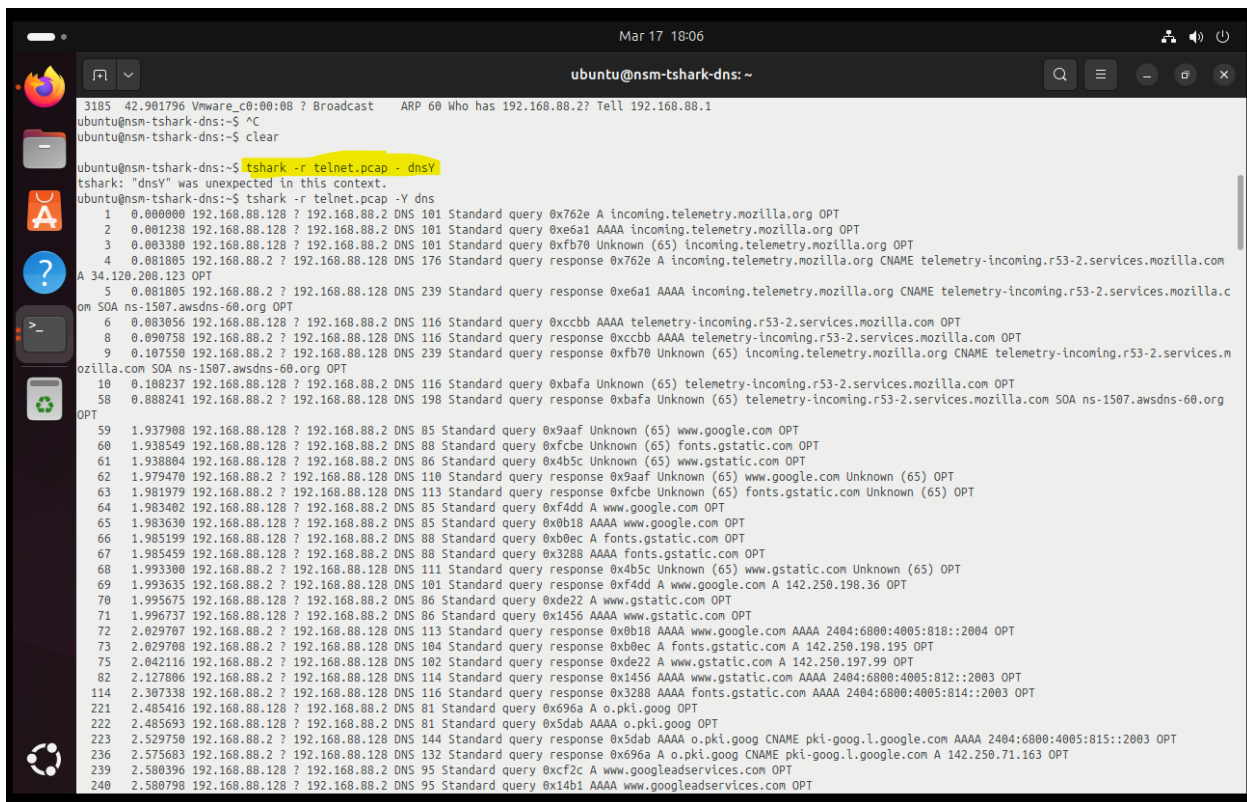
labtainer -r nsm-tshark-dns

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong terminal ảo sẽ xuất hiện.

Sinh viên thực hiện lọc các gói tin chứa giao thức DNS:

tshark -r telnet.pcap -Y 'dns'



```
3185 42.981796 Vmware_c0:00:00 ? Broadcast ARP 60 Who has 192.168.88.2? Tell 192.168.88.1
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y dns
tshark: "dnsY" was unexpected in this context.
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y dns
1 0.000000 192.168.88.128 ? 192.168.88.2 DNS 101 Standard query 0x762e A incoming.telemetry.mozilla.org OPT
2 0.001238 192.168.88.128 ? 192.168.88.2 DNS 101 Standard query 0xe6a1 AAAA incoming.telemetry.mozilla.org OPT
3 0.003380 192.168.88.128 ? 192.168.88.2 DNS 101 Standard query 0xfb70 Unknown (65) incoming.telemetry.mozilla.org OPT
4 0.001805 192.168.88.2 ? 192.168.88.128 DNS 176 Standard query response 0x762e A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com
5 0.001805 192.168.88.2 ? 192.168.88.128 DNS 239 Standard query response 0xe6a1 AAAA incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com
6 0.003056 192.168.88.128 ? 192.168.88.2 DNS 116 Standard query 0xcbb AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
8 0.090758 192.168.88.2 ? 192.168.88.128 DNS 116 Standard query response 0xcbb AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
9 0.107550 192.168.88.2 ? 192.168.88.128 DNS 239 Standard query response 0xfb70 Unknown (65) incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com
10 0.108237 192.168.88.128 ? 192.168.88.2 DNS 116 Standard query 0xbafa Unknown (65) telemetry-incoming.r53-2.services.mozilla.com OPT
58 0.888241 192.168.88.2 ? 192.168.88.128 DNS 198 Standard query response 0xbafa Unknown (65) telemetry-incoming.r53-2.services.mozilla.com SOA ns-1507.awsdns-60.org OPT
59 1.937908 192.168.88.128 ? 192.168.88.2 DNS 85 Standard query 0x9aaf Unknown (65) www.google.com OPT
60 1.938549 192.168.88.128 ? 192.168.88.2 DNS 88 Standard query 0xfcbe Unknown (65) fonts.gstatic.com OPT
61 1.938804 192.168.88.128 ? 192.168.88.2 DNS 86 Standard query 0x4b5c Unknown (65) www.gstatic.com OPT
62 1.979470 192.168.88.2 ? 192.168.88.128 DNS 110 Standard query response 0x9aaf Unknown (65) www.google.com Unknown (65) OPT
63 1.981979 192.168.88.2 ? 192.168.88.128 DNS 113 Standard query response 0xfcbe Unknown (65) fonts.gstatic.com Unknown (65) OPT
64 1.983402 192.168.88.128 ? 192.168.88.2 DNS 85 Standard query 0xf4dd A www.google.com OPT
65 1.983638 192.168.88.128 ? 192.168.88.2 DNS 85 Standard query 0xb18 AAAA www.google.com OPT
66 1.985199 192.168.88.128 ? 192.168.88.2 DNS 88 Standard query 0xb0ec A fonts.gstatic.com OPT
67 1.985459 192.168.88.128 ? 192.168.88.2 DNS 88 Standard query 0x3200 AAAA fonts.gstatic.com OPT
68 1.993300 192.168.88.2 ? 192.168.88.128 DNS 111 Standard query response 0x4b5c Unknown (65) www.gstatic.com Unknown (65) OPT
69 1.993635 192.168.88.2 ? 192.168.88.128 DNS 101 Standard query response 0xf4dd A www.google.com A 142.250.198.36 OPT
70 1.995675 192.168.88.128 ? 192.168.88.2 DNS 86 Standard query 0xde22 A www.gstatic.com OPT
71 1.996737 192.168.88.128 ? 192.168.88.2 DNS 86 Standard query 0x1456 AAAA www.gstatic.com OPT
72 2.029707 192.168.88.2 ? 192.168.88.128 DNS 113 Standard query response 0xb18 AAAA www.google.com AAAA 2404:6800:4005:818::2004 OPT
73 2.029708 192.168.88.2 ? 192.168.88.128 DNS 104 Standard query response 0xb0ec A fonts.gstatic.com A 142.250.198.195 OPT
74 2.042116 192.168.88.2 ? 192.168.88.128 DNS 102 Standard query response 0xde22 A www.gstatic.com A 142.250.197.99 OPT
75 2.127806 192.168.88.2 ? 192.168.88.128 DNS 114 Standard query response 0x1456 AAAA www.gstatic.com AAAA 2404:6800:4005:812::2003 OPT
114 2.307338 192.168.88.2 ? 192.168.88.128 DNS 116 Standard query response 0x3288 AAAA fonts.gstatic.com AAAA 2404:6800:4005:814::2003 OPT
221 2.485416 192.168.88.128 ? 192.168.88.2 DNS 81 Standard query 0x696a A o.pki.goog OPT
222 2.485693 192.168.88.128 ? 192.168.88.2 DNS 81 Standard query 0x5dab AAAA o.pki.goog OPT
223 2.529750 192.168.88.2 ? 192.168.88.128 DNS 144 Standard query response 0x5dab AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4005:815::2003 OPT
236 2.575683 192.168.88.128 ? 192.168.88.2 DNS 132 Standard query response 0x696a A o.pki.goog CNAME pki-goog.l.google.com A 142.250.71.163 OPT
239 2.580396 192.168.88.128 ? 192.168.88.2 DNS 95 Standard query 0xcf2c A www.googleadservices.com OPT
240 2.580798 192.168.88.128 ? 192.168.88.2 DNS 95 Standard query 0x14b1 AAAA www.googleadservices.com OPT
```

Sinh viên xác định số khung của bản ghi chứa truy vấn đầu tiên và tên miền được truy vấn:

tshark -r telnet.pcap -Y 'dns.qry.name' -T fields -e frame.number -e dns.qry.name | head -n 1



```
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y 'dns.qry.name' -T fields -e frame.number -e dns.qry.name | head -n 1
1 incoming.telemetry.mozilla.org
ubuntu@nsm-tshark-dns:~$
```

➔ Số khung : 1

➔ tên miền truy vấn : incoming.telemetry.mozilla.org

Xác định các tên miền được truy vấn trong các gói tin DNS chứa bản ghi A:

```
tshark -r telnet.pcap -Y 'dns.qry.type == 1' -T fields -e dns.qry.name
```

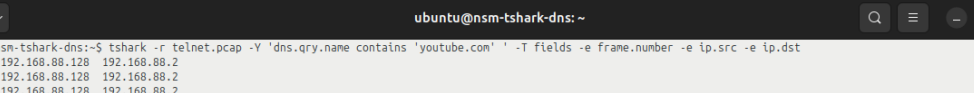
Mar 17 18:46

ubuntu@nsm-tshark-dns: ~

```
1      incoming.telemetry.mozilla.org
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y 'dns.qry.type == 1' -T fields -e dns.qry.name
incoming.telemetry.mozilla.org
incoming.telemetry.mozilla.org
www.google.com
fonts.gstatic.com
www.google.com
www.gstatic.com
fonts.gstatic.com
www.gstatic.com
o.pki.goog
o.pki.goog
www.googleleadservices.com
firefox.settings.services.mozilla.com
firefox.settings.services.mozilla.com
www.googleleadservices.com
id.google.com
id.google.com
csp.withgoogle.com
csp.withgoogle.com
ogads-pa.googleapis.com
ogads-pa.googleapis.com
play.google.com
play.google.com
accounts.firefox.com
accounts.firefox.com
incoming.telemetry.mozilla.org
incoming.telemetry.mozilla.org
detectportal.firefox.com
detectportal.firefox.com
example.org
ipv4only.arpa
example.org
ipv4only.arpa
contile.services.mozilla.com
firefox.settings.services.mozilla.com
firefox.settings.services.mozilla.com
content-signature-2.cdn.mozilla.net
content-signature-2.cdn.mozilla.net
r10.o.lencr.org
firefox-settings-attachments.cdn.mozilla.net
r10.o.lencr.org
firefox-settings-attachments.cdn.mozilla.net
www.youtube.com
www.facebook.com
```

Sinh viên thực hiện lọc và hiển thị số khung cùng với địa chỉ IP đích và IP nguồn được truy vấn trong các gói tin DNS có chứa tên miền 'youtube.com'

```
tshark -r telnet.pcap -Y 'dns.qry.name contains 'youtube.com'' -T fields -e frame.number -e ip.src -e ip.dst
```



The screenshot shows a terminal window titled 'ubuntu@nsm-tshark-dns: ~'. The command executed is `tshark -r telnet.pcap -Y 'dns.qry.name contains 'youtube.com' ' -T fields -e frame.number -e ip.src -e ip.dst`. The output displays a list of network packets with their frame numbers and source/destination IP addresses.

Frame Number	IP Source	IP Destination
1223	192.168.88.128	192.168.88.2
1224	192.168.88.128	192.168.88.2
1225	192.168.88.128	192.168.88.2
1231	192.168.88.2	192.168.88.128
1232	192.168.88.2	192.168.88.128
1357	192.168.88.2	192.168.88.128

Cột 1 biểu thị số khung

Cột 2 biểu thị địa chỉ nguồn

Cột 3 biểu thị địa chỉ đích

Tìm tên miền thu được nhiều nhất trong quá trình thu thập dữ liệu:

```
tshark -r telnet.pcap -Y 'dns.flags.response == 0' -T fields -e dns.qry.name | sort | uniq -c | sort -nr | head -n 1
```

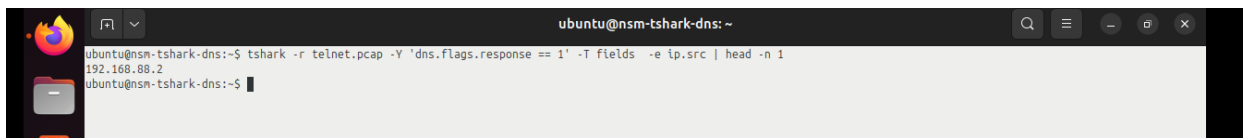


```
ubuntu@nsm-tshark-dns: ~  
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y 'dns.flags.response == 0' -T fields -e dns.qry.name | sort | uniq -c | sort -nr | head -n 1  
10 incoming.telemetry.mozilla.org  
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y 'dns.flags.response == 0' -T fields -e dns.qry.name | sort | uniq -c | sort -nr | head -n 5  
10 incoming.telemetry.mozilla.org  
8 telemetry.incoming.r53-2.services.mozilla.com  
6 Firefox.settings.services.mozilla.com  
5 twitter.com  
4 prod.remote-settings.prod.webservices.mozgcp.net  
ubuntu@nsm-tshark-dns:~$
```

- ➔ Tên miền được truy vấn nhiều nhất : **incoming.telemetry.mozilla.org**
- ➔ Với **10** lần truy vấn

Sinh viên tìm địa chỉ IP của máy chủ DNS nào đã trả lời truy vấn đầu tiên:

```
tshark -r telnet.pcap -Y 'dns.flags.response == 1' -T fields -e ip.src | head -n 1
```

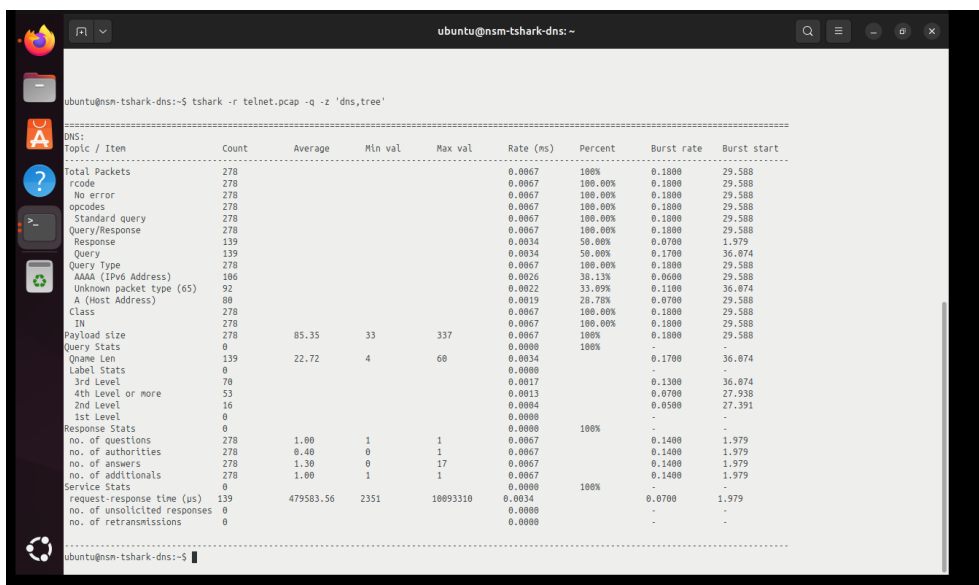


```
ubuntu@nsm-tshark-dns: ~  
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -Y 'dns.flags.response == 1' -T fields -e ip.src | head -n 1  
192.168.88.2  
ubuntu@nsm-tshark-dns:~$
```

- ➔ Địa chỉ IP trả lời truy vấn nhiều nhất : **192.168.88.2**

Thống kê chi tiết về truy vấn và phản hồi DNS dưới dạng cây:

```
tshark -r telnet.pcap -q -z 'dns,tree'
```



```
ubuntu@nsm-tshark-dns: ~  
ubuntu@nsm-tshark-dns:~$ tshark -r telnet.pcap -q -z 'dns,tree'
```

Topic / Item	Count	Average	Min val	Max val	Rate (ns)	Percent	Burst rate	Burst start
DNS:								
Total Packets	278				0.0007	100%	0.1000	29.588
rcode	278				0.0007	100.00%	0.1000	29.588
No error	278				0.0007	100.00%	0.1000	29.588
opcodes	278				0.0007	100.00%	0.1000	29.588
Standard query	278				0.0007	100.00%	0.1000	29.588
Query/Response	278				0.0007	100.00%	0.1000	29.588
Response	139				0.0034	50.00%	0.0700	1.979
Query	139				0.0034	50.00%	0.1700	36.074
Query Type	278				0.0007	100.00%	0.1000	29.588
AAAA (IPv6 Address)	106				0.0026	38.13%	0.0600	29.588
Unknown packet type (65)	92				0.0022	33.09%	0.1100	36.074
A (Host Address)	80				0.0019	28.78%	0.0700	29.588
Class	278				0.0007	100.00%	0.1000	29.588
IN	278				0.0007	100.00%	0.1000	29.588
Payload size	278	85.35	33	337	0.0007	100%	0.1000	29.588
Query Stats	0				0.0000	100%	-	-
Qname Len	139	22.72	4	60	0.0034	-	0.1700	36.074
Label Stats	0				0.0000	-	-	-
3rd Level	70				0.0017	0.1300	0.1300	36.074
4th Level or more	53				0.0013	0.0700	0.0700	27.330
2nd Level	16				0.0004	0.0500	0.0500	27.330
1st Level	0				0.0000	-	-	-
Response Stats	0				0.0000	100%	-	-
no. of questions	278	1.00	1	1	0.0007	0.1400	0.1400	1.979
no. of authorities	278	0.40	0	1	0.0007	0.1400	0.1400	1.979
no. of answers	278	1.30	0	17	0.0007	0.1400	0.1400	1.979
no. of additional	278	1.00	1	1	0.0007	0.1400	0.1400	1.979
Service Stats	0				0.0000	100%	-	-
request-response time (us)	139	479583.56	2351	10093310	0.0034	0.0700	0.0700	1.979
no. of unsolicited responses	0				0.0000	-	-	-
no. of retransmissions	0				0.0000	-	-	-

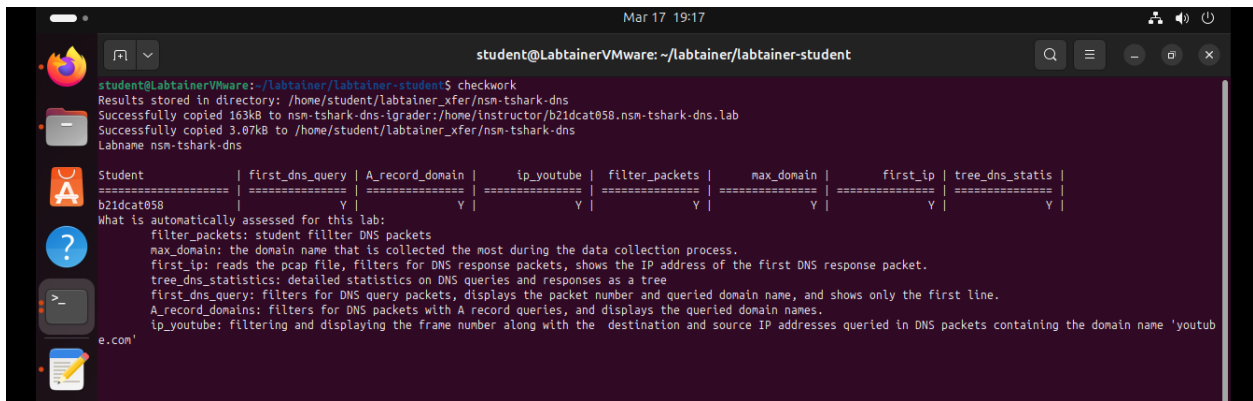
4. Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab nsm-tshark-dns

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Checkwork bài nsm-tshark-dns:



```
student@LabtainerVMware: ~/labtainer/labtainer-student
student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nsm-tshark-dns
Successfully copied 163kB to nsm-tshark-dns-igrader:/home/instructor/b2idcat058.nsm-tshark-dns.lab
Successfully copied 3.07kB to /home/student/labtainer_xfer/nsm-tshark-dns
Labname nsm-tshark-dns

Student | first_dns_query | A_record_domain | ip_youtube | filter_packets | max_domain | first_ip | tree_dns_status |
=====|=====|=====|=====|=====|=====|=====|=====|
b2idcat058 | | Y | Y | Y | Y | | Y |

What is automatically assessed for this lab:
filter_packets: student filter DNS packets
max_domain: the domain name that is collected the most during the data collection process.
first_ip: reads the pcap file, filters for DNS response packets, shows the IP address of the first DNS response packet.
tree_dns_statistics: detailed statistics on DNS queries and responses as a tree
first_dns_query: filters for DNS query packets, displays the packet number and queried domain name, and shows only the first line.
A_record_domains: filters for DNS packets with A record queries, and displays the queried domain names.
ip_youtube: filtering and displaying the frame number along with the destination and source IP addresses queried in DNS packets containing the domain name 'youtube.com'
```

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer -r nsm-tshark-dns