Übung - DNS-Datenverkehr entdecken

Ziele

Teil 1: DNS-Datenverkehr erfassen

Teil 2: Erkunden des DNS-Abfrageverkehrs

Teil 3: Durchsuchen des DNS-Abfrageverkehrs

Hintergrund/Szenario

Wireshark ist ein Open-Source-Werkzeug zur Paketerfassung und -analyse. Wireshark liefert eine detaillierte Analyse des Netzwerkprotokollstapels. Mit Wireshark können Sie Datenverkehr für die Fehlerbehebung im Netzwerk filtern, Sicherheitsprobleme untersuchen und Netzwerkprotokolle analysieren. Da Wireshark die Möglichkeit bietet, die Paketdetails einzusehen, kann es von einem Angreifer als Erkundungstool verwendet werden.

In dieser Übung werden Sie Wireshark auf einem Windows-System installieren und Wireshark verwenden, um DNS-Pakete zu filtern und sich die Details von DNS-Abfrage- und Antwortpaketen anzusehen.

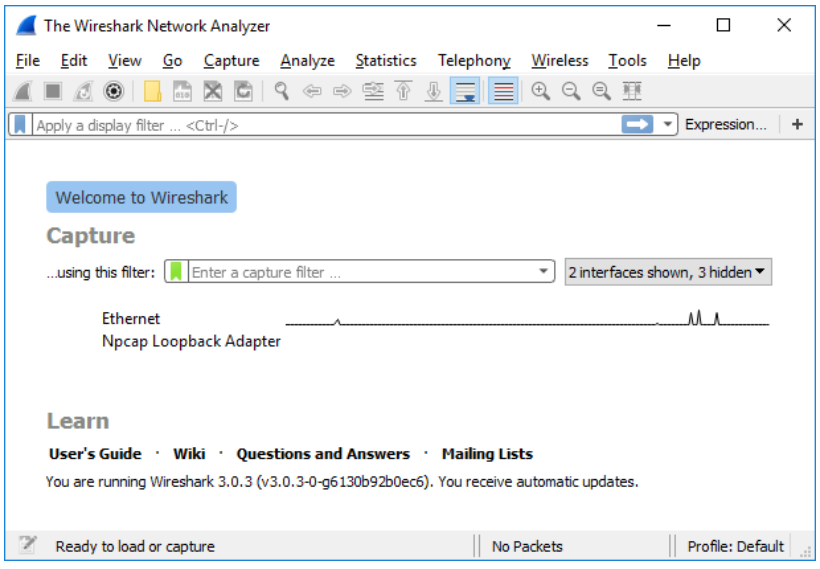
Benötigte Ressourcen

- 1 Windows-PC mit Internetzugang und installiertem Wireshark

Anleitung

Schritt 1: Erfassen Sie den DNS-Verkehr.

a. Öffnen Sie **Wireshark** und starten eine Wireshark-Aufzeichnung, indem Sie auf eine Netzwerkschnittstelle mit Datenverkehr doppelklicken.



b. Geben Sie in der Eingabeaufforderung **ipconfig /flushdns** ein, um den DNS-Cache zu löschen.

```
C:\Users\Student> ipconfig /flushdns
```

```
Windows IP Configuration

Der DNS-Resolver-Cache wurde erfolgreich geleert.
```

c. Geben Sie in der Eingabeaufforderung **nslookup** ein, um den interaktiven Modus von nslookup aufzurufen.

d. Geben Sie den Domain-Namen einer Website ein. In diesem Beispiel wird der Domainname www.cisco.com verwendet. Geben Sie in die Eingabeaufforderung **www.cisco.com** ein.

```
C:\Users\Student> nslookup
Default Server: UnKnown
Address: 68.105.28.16

> www.cisco.com
Server: UnKnown
Address: 68.105.28.16

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2001:578:28:68d::b33
          2001:578:28:685::b33
          96.7.79.147
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

e. Um den interaktiven Modus von nslookup zu beenden, geben Sie **exit** ein. Schließen Sie die Eingabeaufforderung.

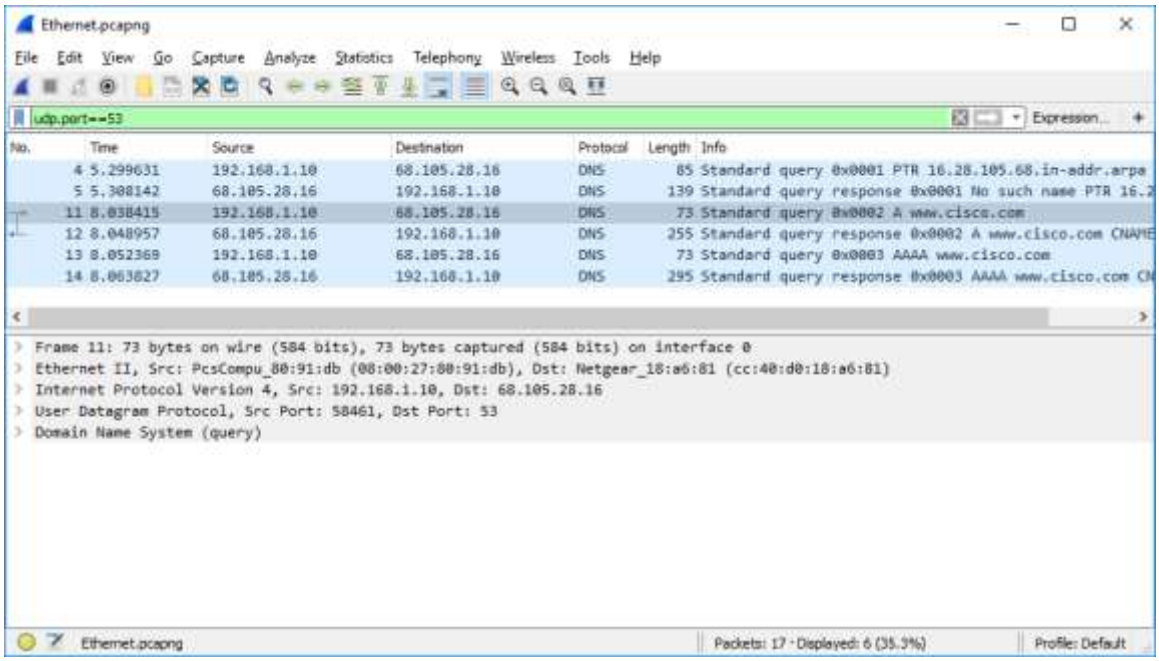
f. Klicken Sie auf **Stop capturing packets**, um die Wireshark-Aufzeichnung zu beenden.

Schritt 2: Durchsuchen des DNS-Abfrageverkehrs

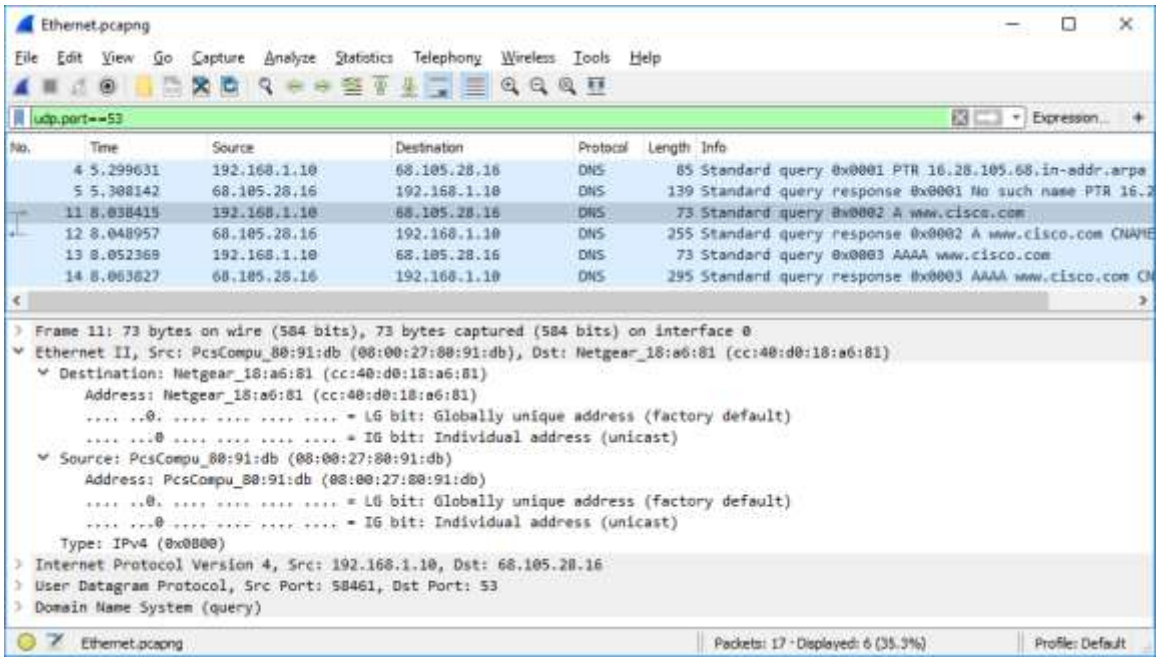
a. Beobachten Sie den erfassten Datenverkehr im Ausschnitt "Wireshark Packet List". Geben Sie **udp.port == 53** in das Filterfeld ein und klicken Sie auf den Pfeil (oder drücken Sie die Eingabetaste), um sich nur DNS-Pakete anzeigen zu lassen.

b. Wählen Sie das DNS-Paket mit der Bezeichnung **Standard query 0x0002 A www.cisco.com**.

Im Bereich "Paketdetails" sehen Sie, dass dieses Paket Ethernet II, Internet Protocol Version 4, User Datagram Protocol und Domain Name System (Abfrage) enthält.

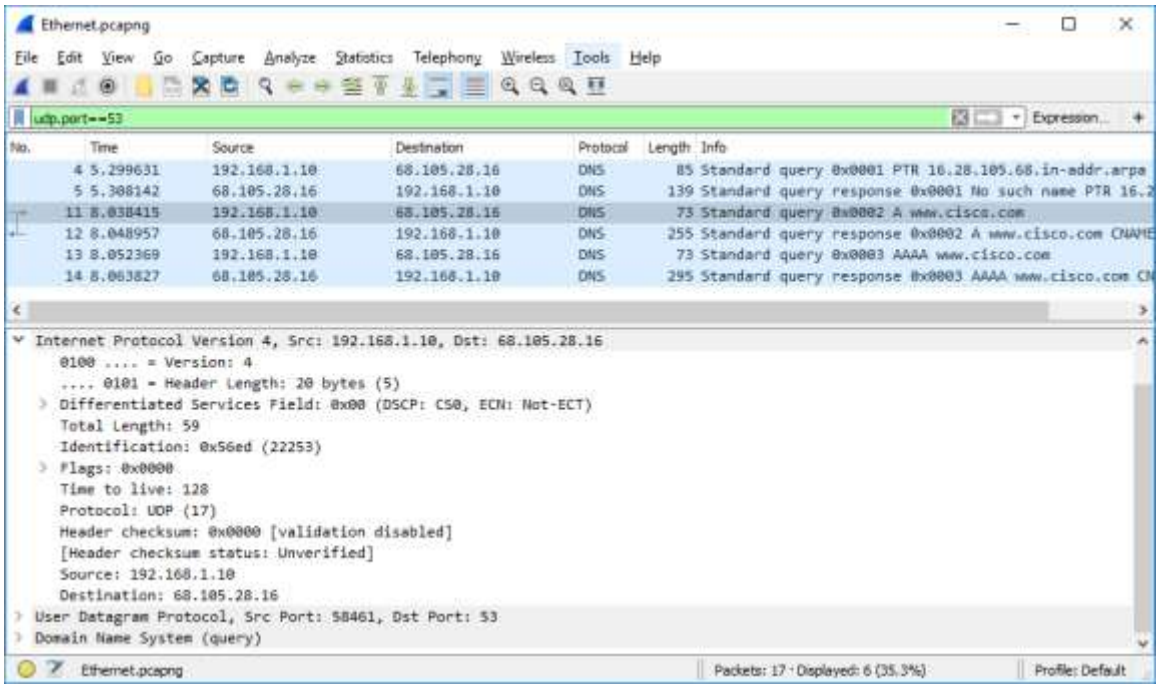


c. Öffnen Sie **Ethernet II**, um sich die Details anzusehen. Beachten Sie die Felder Quelle und Ziel.



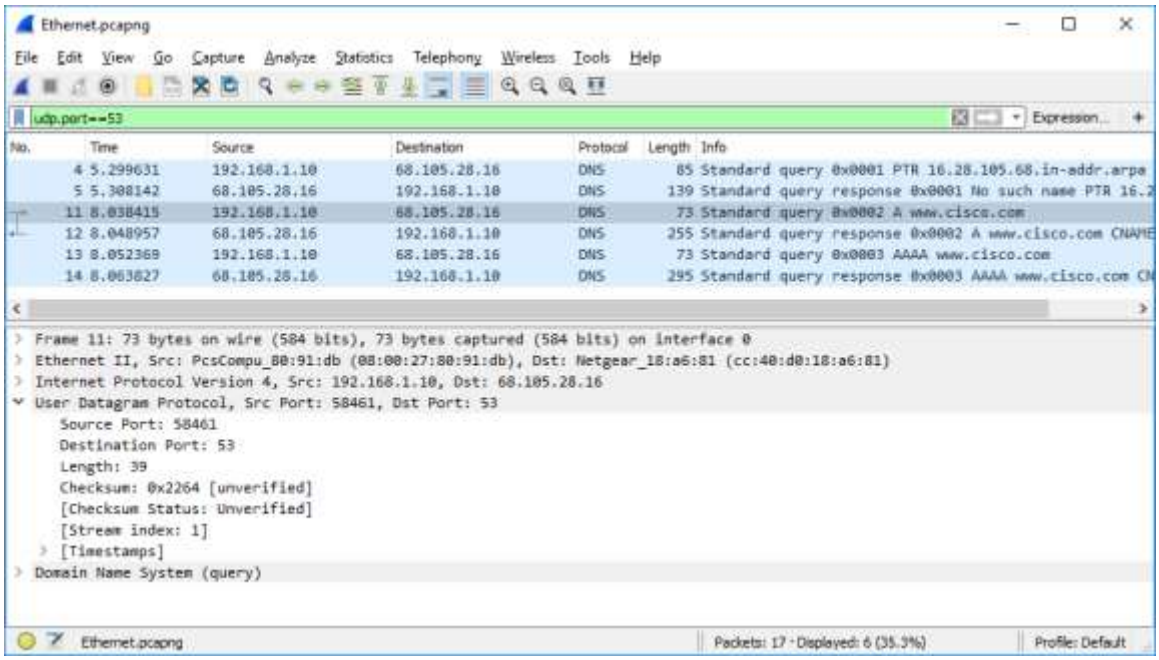
Wie lauten die MAC-Adressen von Quelle und Ziel? Welchen Netzwerkschnittstellen sind diese MAC-Adressen zugeordnet?

a. Öffnen Sie **Internet Protocol Version 4**. Beachten Sie die Quell- und Ziel-IPv4-Adressen.



Wie lauten die Adressen von Quelle und Ziel? Welchen Netzwerkschnittstellen sind diese Adressen zugeordnet?

b. Öffnen Sie das **User Datagram Protocol**. Beachten Sie die Quell- und Zielports.



Wie lauten die Quell- und Ziel-Ports? Wie lautet die Standard-DNS-Portnummer?

c. Öffnen Sie eine Eingabeaufforderung und geben Sie **arp -a** und **ipconfig /all** ein, um die MAC- und IP-Adressen des PCs aufzuzeichnen.

```
C:\Users\Student> arp -a

Interface: 192.168.1.10 --- 0x4
  Internet Address Physical Address Type
  192.168.1.1 cc-40-d0-18-a6-81 dynamic
  192.168.1.122 b0-a7-37-46-70-bb dynamic
  192.168.1.255 ff-ff-ff-ff-ff-ff static
  224.0.0.22 01-00-5e-00-00-16 static
  224.0.0.252 01-00-5e-00-00-fc static
  239.255.255.250 01-00-5e-7f-ff-fa static
  255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\Studuent> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP
   Primary Dns Suffix . . . . . . . :
   Knotentyp. . . . . . . . . . . . : Hybrid
```

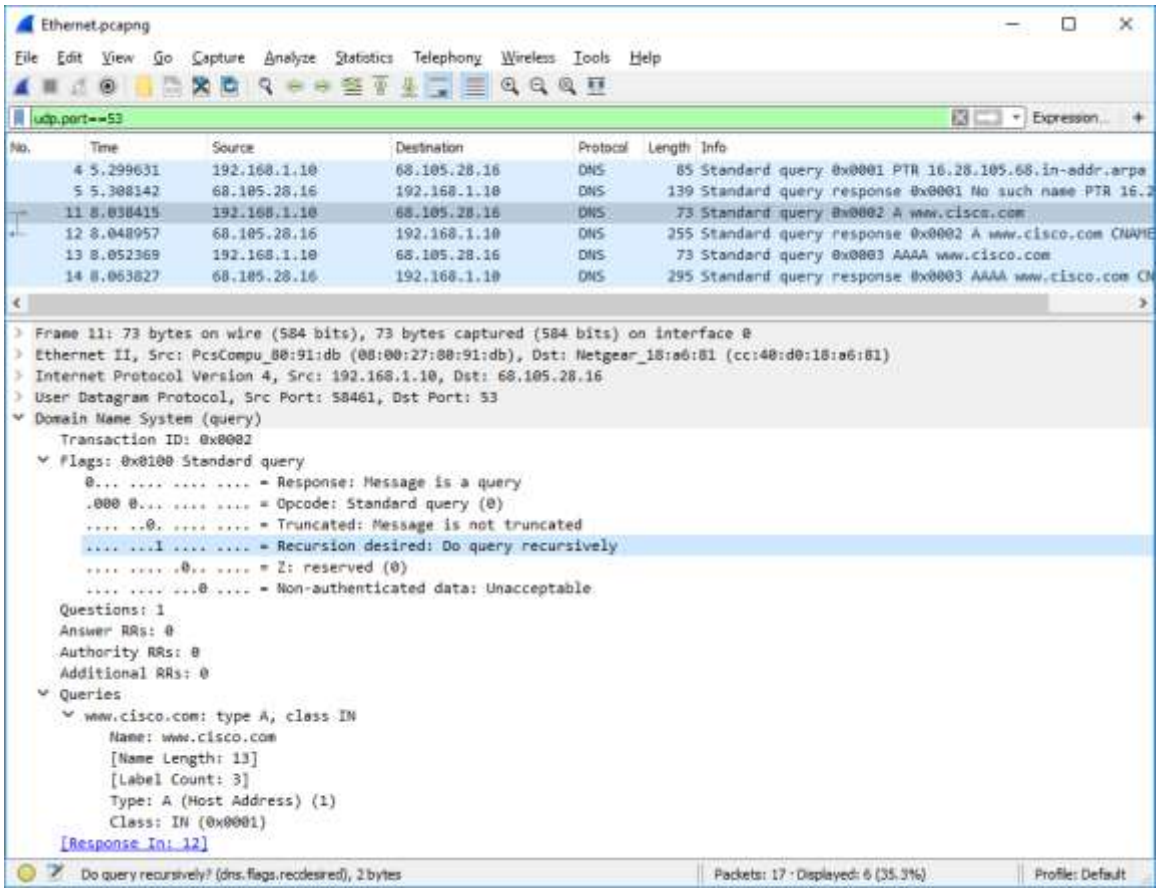


```
   IP Routing Enabled. . . . . . . . : No
   WINS-Proxy aktiviert. . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-80-91-DB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, August 20, 2019 5:39:51 PM
   Lease Expires . . . . . . . . . . : Wednesday, August 21, 2019 5:39:50 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 50855975
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
   DNS Servers . . . . . . . . . . . : 68.105.28.16
                                       68.105.29.16
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Vergleichen Sie die MAC- und IP-Adressen in den Wireshark-Ergebnissen mit den Ergebnissen aus dem Befehl **ipconfig /all**. Welche Unterschiede stellen Sie fest?

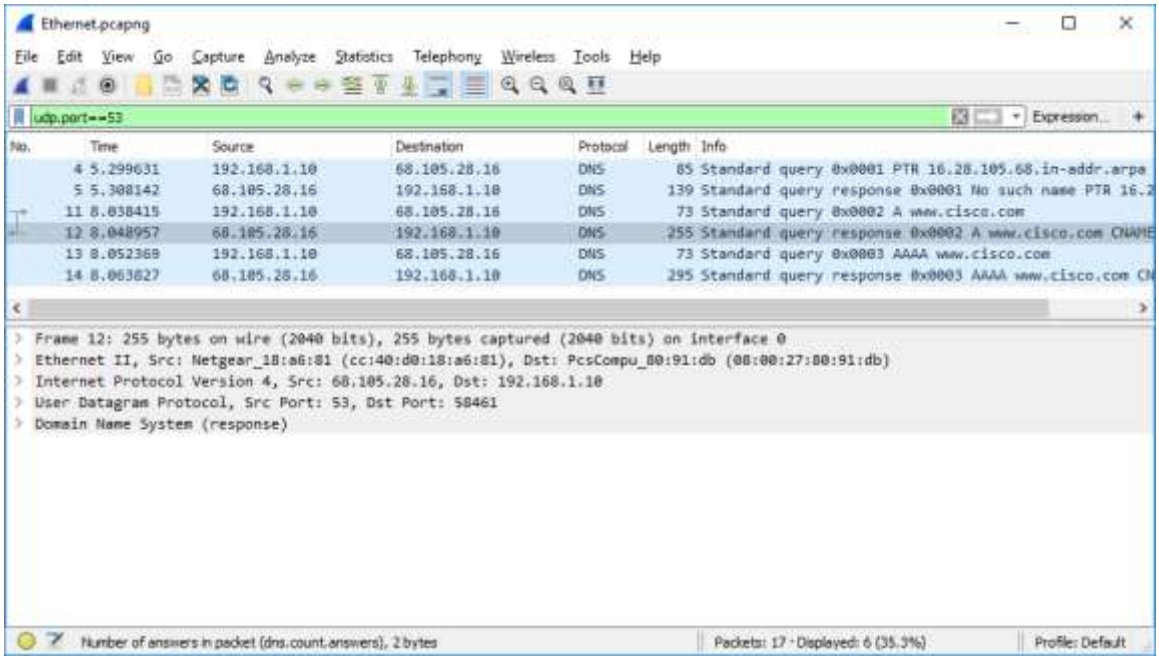
d. Öffnen Sie im Fensterbereich Paketdetails das Feld **Domain Name System (query)**. Erweitern Sie dann die **Flags** und **Queries**.

Beobachten Sie die Ergebnisse. Das Flag ist so gesetzt, dass die Abfrage rekursiv durchgeführt wird, um die IP-Adresse für die Adresse www.cisco.com abzufragen.



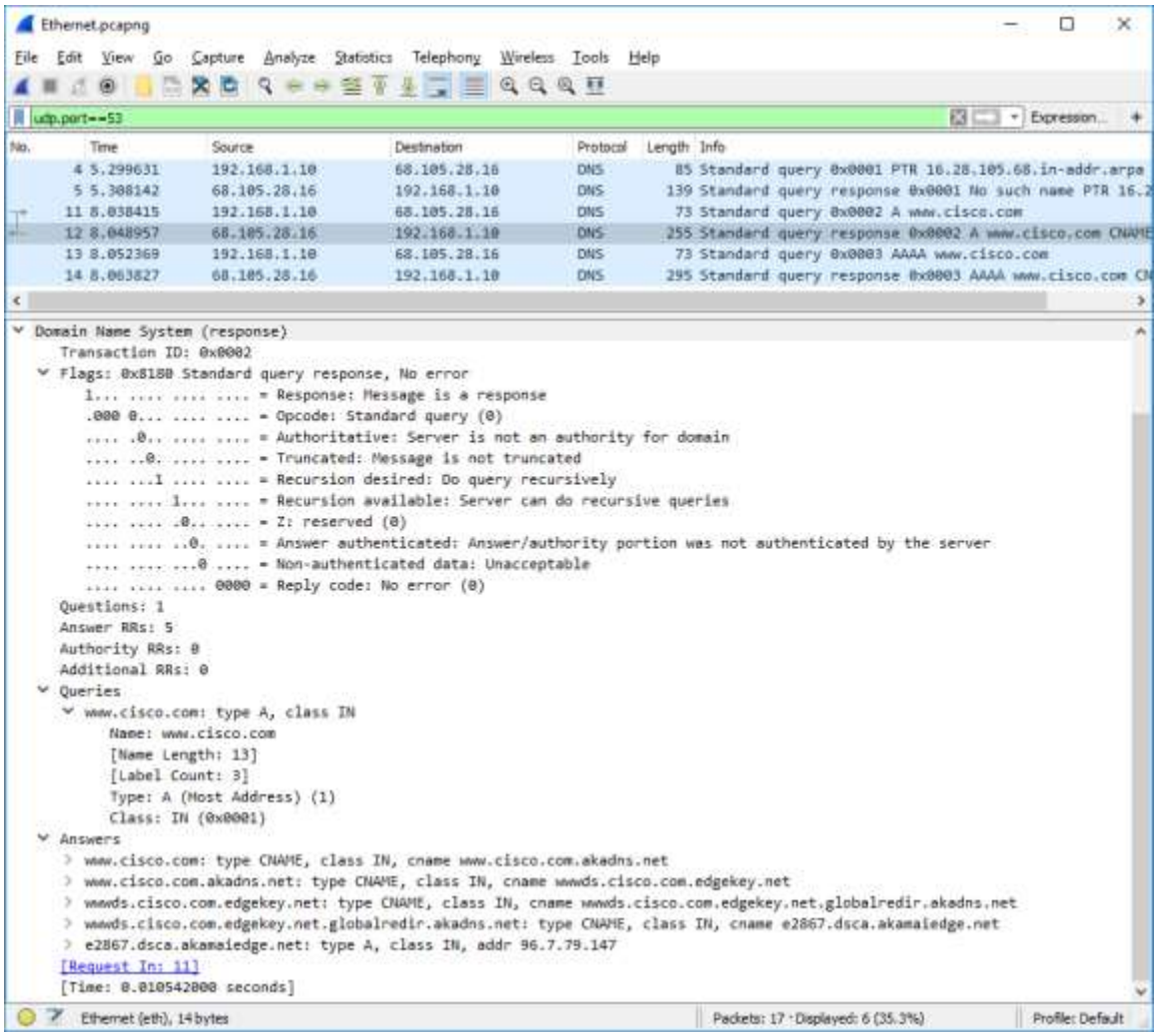
Schritt 3: Durchsuchen des DNS-Antwortverkehrs

a. Wählen Sie das entsprechende DNS-Antwortpaket mit der Bezeichnung **Standard query response 0x0002 A www.cisco.com**.



Wie lauten die Quell- und Ziel-MAC- und -IP-Adressen sowie die Portnummern? Wie stimmen sie mit den Adressen in den DNS-Abfragepaketen überein?

b. Erweitern Sie den Bereich **Domain Name System (response)**. Erweitern Sie dann die Bereiche **Flags**, **Queries** und **Answers**. Beobachten Sie die Ergebnisse.



Kann der DNS-Server rekursive Abfragen durchführen?

c. Beachten Sie die CNAME- und A-Records in den Details der Antworten.

Wie sind die Ergebnisse im Vergleich zu nslookup-Ergebnissen?

Verständnisfragen

1. Was können Sie anhand der Wireshark-Ergebnisse noch über das Netzwerk erfahren, wenn Sie den Filter entfernen?

2. Wie kann ein Angreifer Wireshark verwenden, um Ihre Netzwerksicherheit zu gefährden?

