

Laboratório - Explore o tráfego DNS

Objetivos

Parte 1: Capturar tráfego DNS

Parte 2: Explore o tráfego de consulta DNS

Parte 3: Explore o tráfego de resposta do DNS

Histórico/Cenário

O Wireshark é uma ferramenta de captura e análise de pacotes de código aberto. O Wireshark fornece uma análise detalhada da pilha de protocolos de rede. O Wireshark permite filtrar o tráfego para solucionar problemas de rede, investigar problemas de segurança e analisar protocolos de rede. Como o Wireshark permite visualizar os detalhes do pacote, ele pode ser usado como uma ferramenta de reconhecimento para um invasor.

Neste laboratório, você instalará o Wireshark e usará o Wireshark para filtrar pacotes DNS e visualizar os detalhes dos pacotes de consulta e resposta DNS.

Recursos necessários

- 1 PC com acesso à internet e Wireshark instalado

Instruções

Parte 1: Capture o tráfego DNS

Etapa 1: Baixe e instale o Wireshark.

- a. Baixe a última versão estável do Wireshark em www.wireshark.org. Escolha a versão do software necessária com base na arquitetura e no sistema operacional do PC.
- b. Siga as instruções na tela para instalar o Wireshark. Se você for solicitado a instalar o USBPcap, **NÃO** instale o USBPcap para captura de tráfego normal. O USBPcap é experimental e pode causar problemas USB no seu PC.

Etapa 2: Capture o tráfego DNS

- a. Inicie o Wireshark. Selecione uma interface ativa com tráfego para captura de pacotes.
- b. Limpe o cache DNS.
 - 1) No Windows, digite **ipconfig /flushdns** no prompt de comando.
 - 2) Para a maioria das distribuições Linux, um dos seguintes utilitários é usado para cache de DNS: Systemd -Resolved, DNSMasq e NSCD. Se a sua distribuição Linux não usar um dos utilitários listados, faça uma pesquisa na Internet para o utilitário de cache DNS para sua distribuição Linux.
 - (i) Identifique o utilitário usado na sua distribuição Linux verificando o status:

Systemd-Resolved: **systemctl status systemd-resolved.service**

DnsMasq: **systemctl status dnsmasq.service**

NSCD: **statussystemctl nscd.service**

Laboratório - Explore o tráfego DNS

- (ii) Se você estiver usando o sistema resolvido, digite **systemd-resolve —flush-caches** para liberar o cache para Systemd-Resolved antes de reiniciar o serviço. Os comandos a seguir reiniciam o serviço associado usando privilégios elevados:

Systemd-Resolved: **sudo systemctl restart systemd-resolved.service**

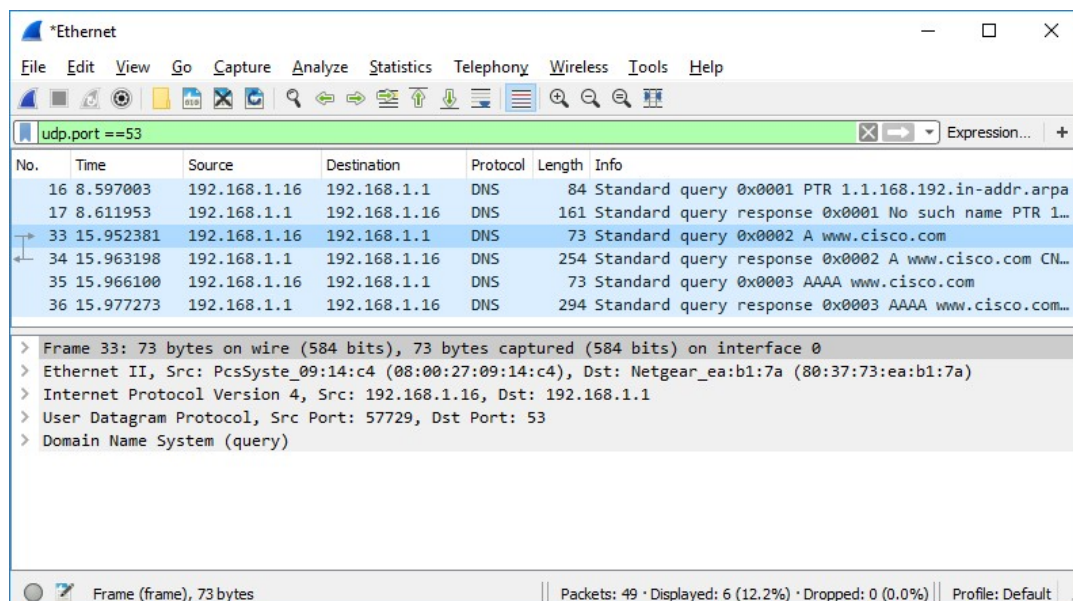
DNSMasq: **sudo systemctl restart dnsmasq.service**

NSCD: **sudo systemctl reiniciar nscd.service**

- 3) Para o macOS, digite **sudo killall -HUP mDNSResponder** para limpar o cache DNS no Terminal. Execute uma pesquisa na Internet para os comandos para limpar o cache DNS de um sistema operacional mais antigo.
- c. Em um prompt de comando ou terminal, digite **nslookup** enter o modo interativo.
- d. Insira o nome do domínio. O nome do domínio www.cisco.com É usado neste exemplo.
- e. Digite **exit** quando terminar. Feche o prompt de comando.
- f. Clique em **Para a captura de pacotes** para parar a captura do Wireshark.

Parte 2: Explore o tráfego de consulta DNS

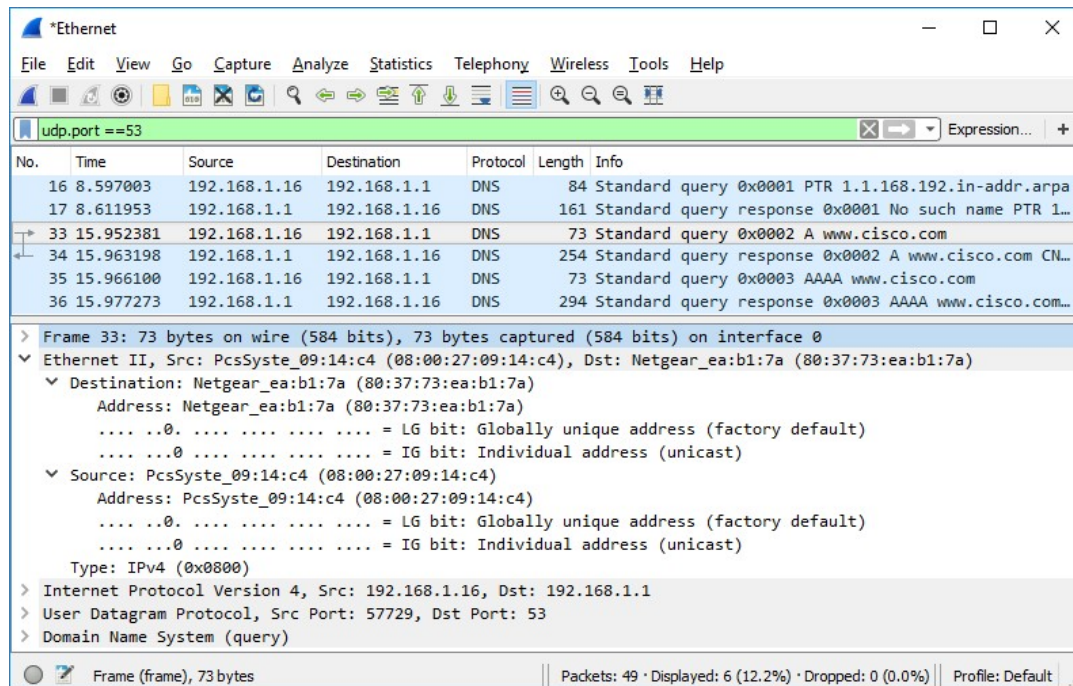
- a. Observe o tráfego capturado no painel Wireshark Packet List. Entre com **udp.port == 53** na caixa de filtro e clique na seta (ou pressione Enter) para exibir apenas pacotes DNS. **Observação:** As capturas de tela fornecidas são apenas exemplos. Sua saída talvez um pouco diferente.



- b. Selecione o pacote DNS contém **consulta padrão** e **A www.cisco.com** na coluna Informações.
- c. No painel Detalhes do Pacote, observe que este pacote possui Ethernet II, Internet Protocol Versão 4, User Datagram Protocol e Domain Name System (consulta).

Laboratório - Explore o tráfego DNS

- d. Expanda **Ethernet II** para ver os detalhes. Observe os campos de origem e destino.



The screenshot shows the Wireshark interface with a capture filter of `udp.port == 53`. The packet list displays several DNS packets. Packet 33 is selected, and its details are expanded, showing the Ethernet II header with source MAC `PcsSyste_09:14:c4` and destination MAC `Netgear_ea:b1:7a`.

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

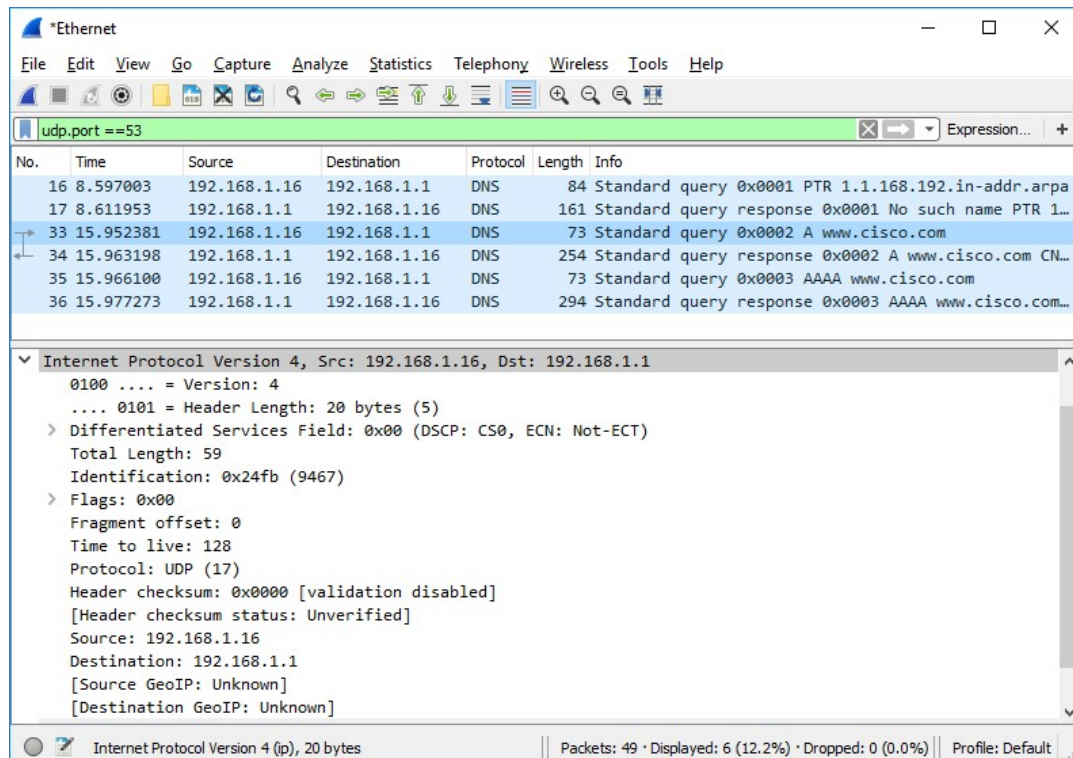
- Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Source: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
 - Address: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 57729, Dst Port: 53
- Domain Name System (query)

Frame (frame), 73 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Quais são os endereços MAC de origem e destino? A quais interfaces de rede esses endereços MAC estão associados?

Laboratório - Explore o tráfego DNS

- e. Expanda **Internet Protocol Version 4**. Observe os endereços IPv4 de origem e destino.



The screenshot shows the Wireshark interface with a packet capture on the Ethernet interface. The filter is set to `udp.port == 53`. The packet list shows several DNS queries and responses. The packet details pane for the selected packet (No. 33) shows the Internet Protocol Version 4 header with source and destination IP addresses.

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1...
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN...
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com...

Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

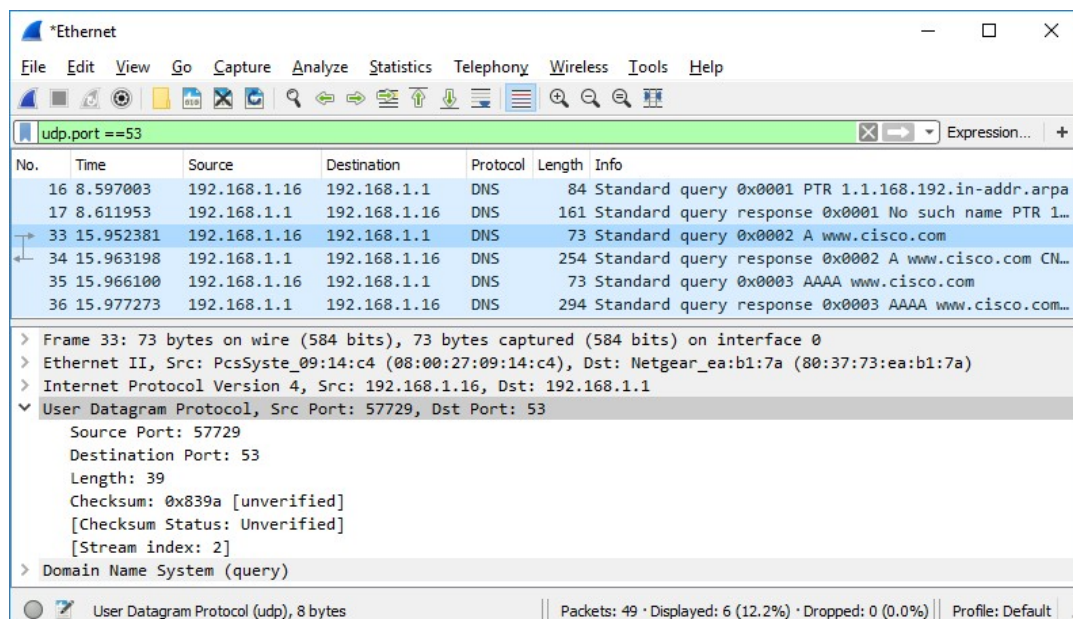
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 59
- Identification: 0x24fb (9467)
- > Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: UDP (17)
- Header checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.16
- Destination: 192.168.1.1
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Internet Protocol Version 4 (ip), 20 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Quais são os endereços IP de origem e destino? A quais interfaces de rede esses endereços IP estão associados?

Laboratório - Explore o tráfego DNS

- f. Expanda a aba **User Datagram Protocol**. Observe os campos de origem e destino.



Quais são os valores das portas origem e destino? Qual é o número da porta DNS padrão?

- g. Determine o endereço IP e MAC do PC.
- 1) Em um prompt de comando do Windows, digite **arp -a** e **ipconfig /all** para registrar os endereços MAC e IP do PC.
 - 2) Para Linux e macOS PC, digite **ifconfig** ou **ip address** em um terminal.

Compare os endereços MAC e IP nos resultados do Wireshark com os endereços IP e MAC. O que você observa?

- h. Expanda o **Domain Name System (query)** no painel Detalhes do pacote. Então expanda também **Flags** e **Queries**.

Laboratório - Explore o tráfego DNS

- i. Observe os resultados. O sinalizador está configurado para fazer a consulta recursivamente para procurar o endereço IP em `www.cisco.com`.

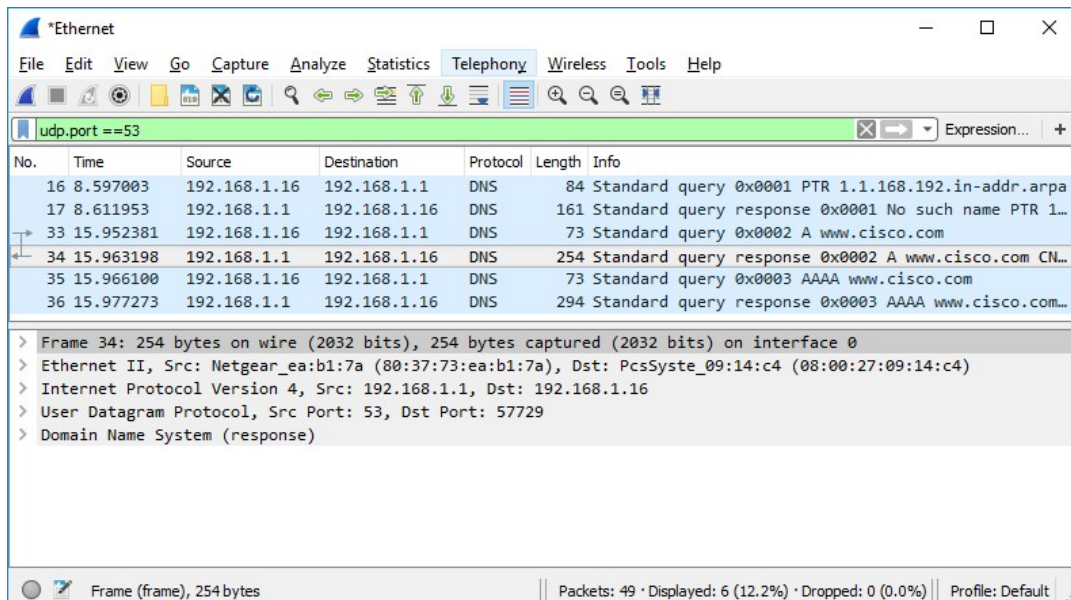
The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar at the top is set to "udp.port == 53". The packet list shows several DNS packets. Packet 34 is selected, showing a standard query response for "www.cisco.com". The packet details pane shows the following information:

- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 57729, Dst Port: 53
- Domain Name System (query)
 - [Response In: 34]
 - Transaction ID: 0x0002
 - Flags: 0x0100 Standard query
 - 0... .. = Response: Message is a query
 - .000 0... .. = Opcode: Standard query (0)
 - = Truncated: Message is not truncated
 -1 ... = Recursion desired: Do query recursively
 -0.. .. = Z: reserved (0)
 -00 .. = Non-authenticated data: Unacceptable
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.cisco.com: type A, class IN
 - Name: www.cisco.com
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

The status bar at the bottom indicates "Domain Name System (dns), 31 bytes" and "Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default".

Parte 3: Explore o tráfego de resposta do DNS

- Selecione a resposta correspondente. O pacote DNS tem uma resposta de consulta padrão e A **www.cisco.com** na coluna Info.

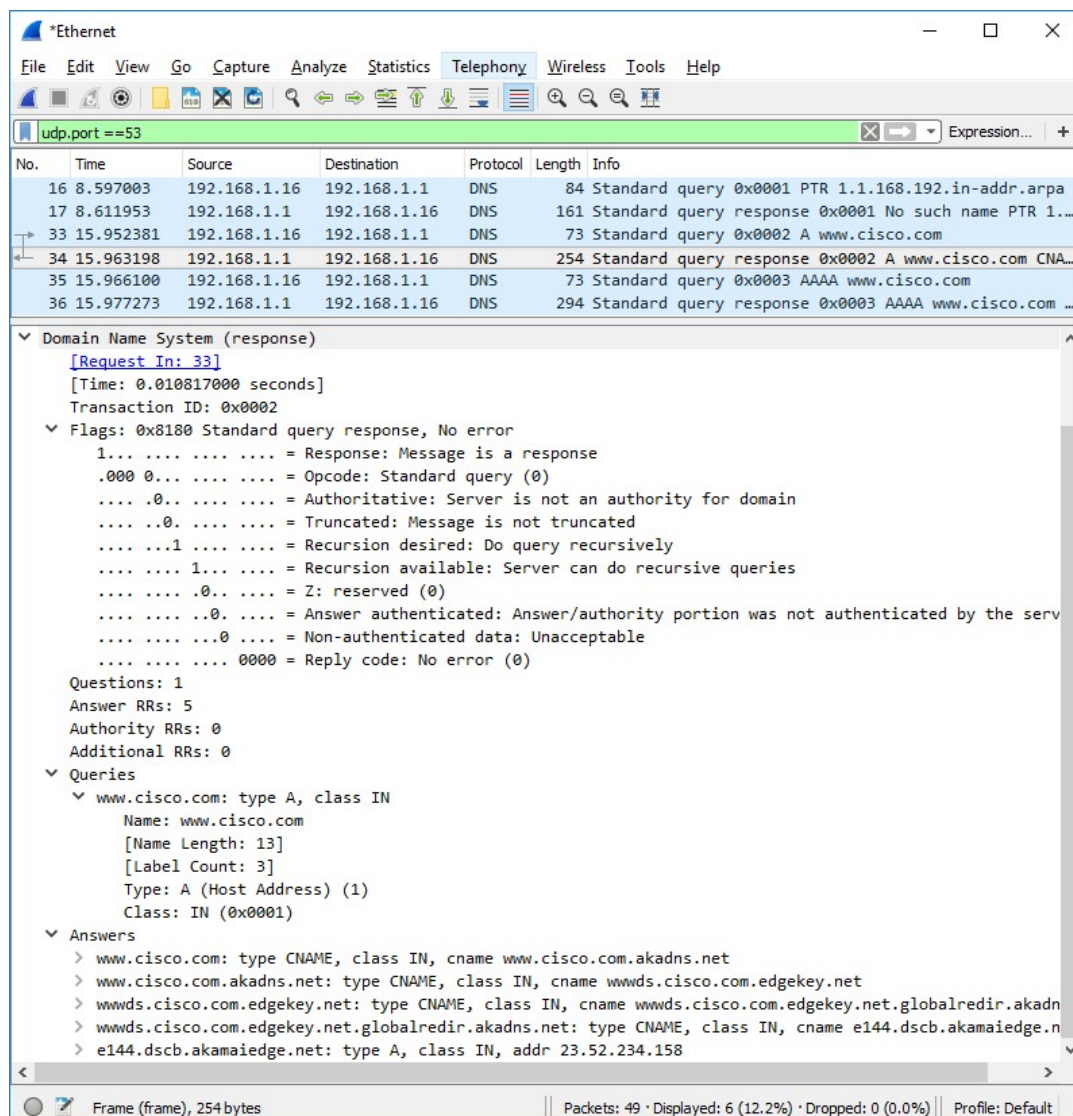


Quais são os endereços MAC e IP de origem e destino e os números de porta? Como eles se comparam aos endereços nos pacotes de consulta DNS?

.

- Expanda **Domain Name System (response)**. Então expanda **Flags**, **Queries**, e **Answers**.
- Observe os resultados.
- O servidor DNS pode fazer consultas recursivas?

Laboratório - Explore o tráfego DNS



d. Observe os registros CNAME e A nos detalhes das Respostas.

Como os resultados se comparam aos resultados do nslookup?

Reflexão

1. A partir dos resultados do Wireshark, o que mais você pode aprender sobre a rede ao remover o filtro?

2. Como um invasor pode usar o Wireshark para comprometer a segurança da sua rede?