

ICMP ATÖLYESİ

ATÖLYENİN HEDEFİ:

Bu atölyede ICMP paketinin nasıl alındığını öğreneceksiniz.

ATÖLYENİN AMACI:

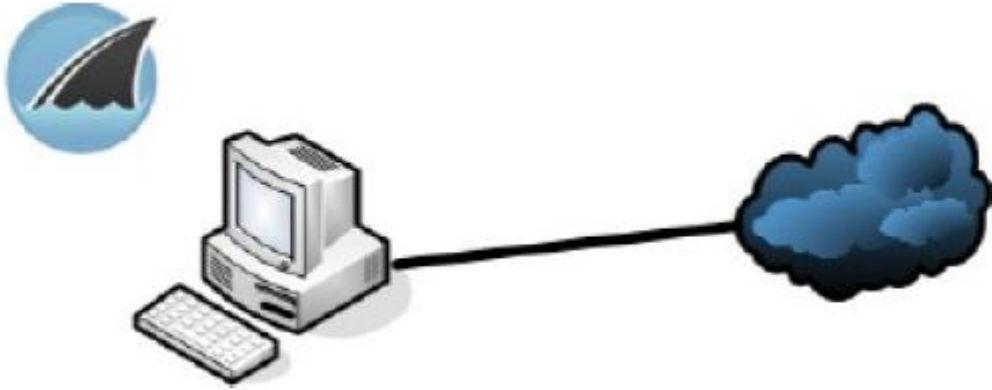
Internet Control Message Protocol (ICMP) ağ aygıtları tarafından güvenilirlik hakkında raporlama yapmak ve hata mesajları göndermek için kullanılır. ICMP, TCP/IP içindeki diğer protokollerin çoğundan farklıdır çünkü veri taşımak için kullanılmaz.

ATÖLYE ARACI:

Wireshark'ı ev bilgisayarınızda da aynı kolaylıkla çalıştırabilirsiniz.

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.



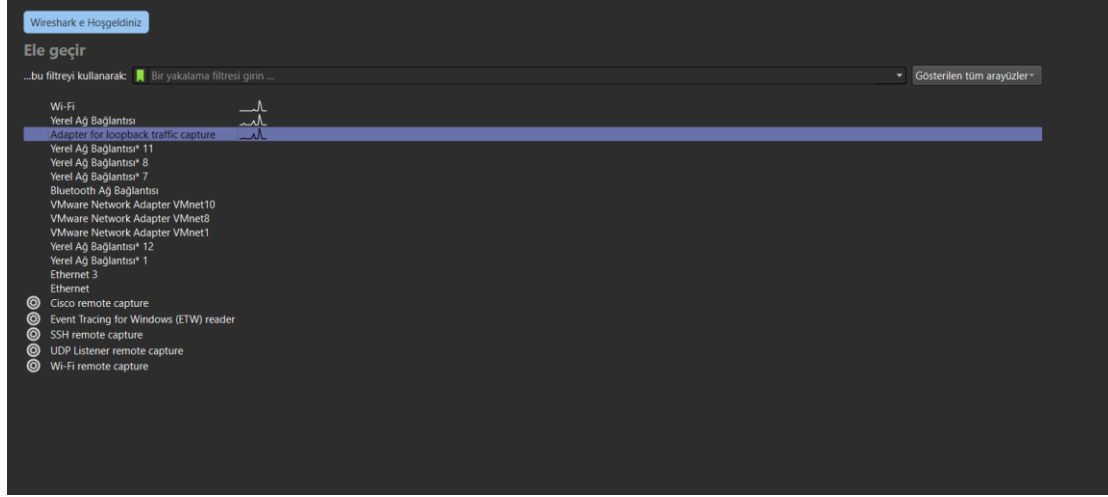
ATÖLYE ANLATIMI:

Adım1:

<https://www.wireshark.org/download.html> Adresine giderek sisteminize uygun wireshark'ı indirin ve bilgisayarınıza kurun.

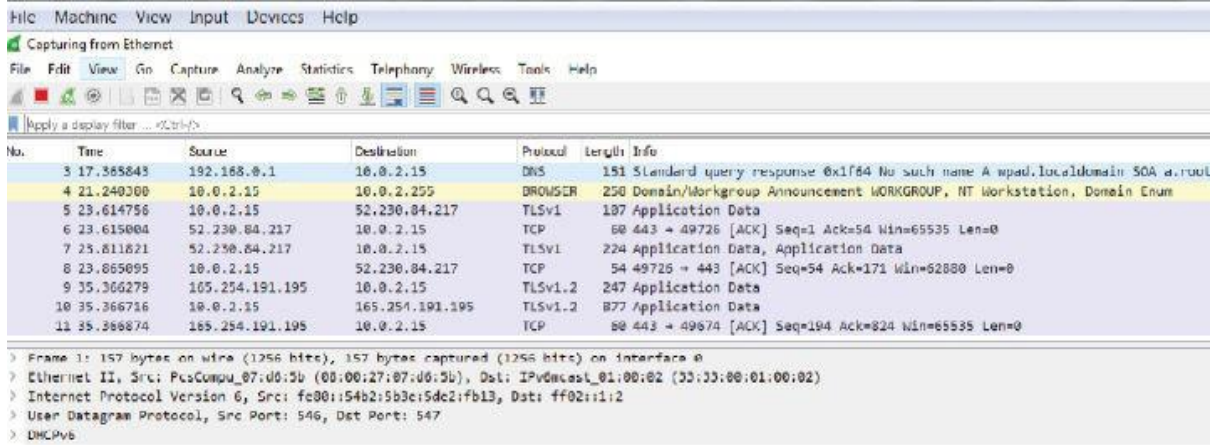
Adım2:

Wireshark'ı açarak yakalamak istediğimiz bağlantıyı seçelim. Ben “yerel ağ bağlantısı”nı seçtim.



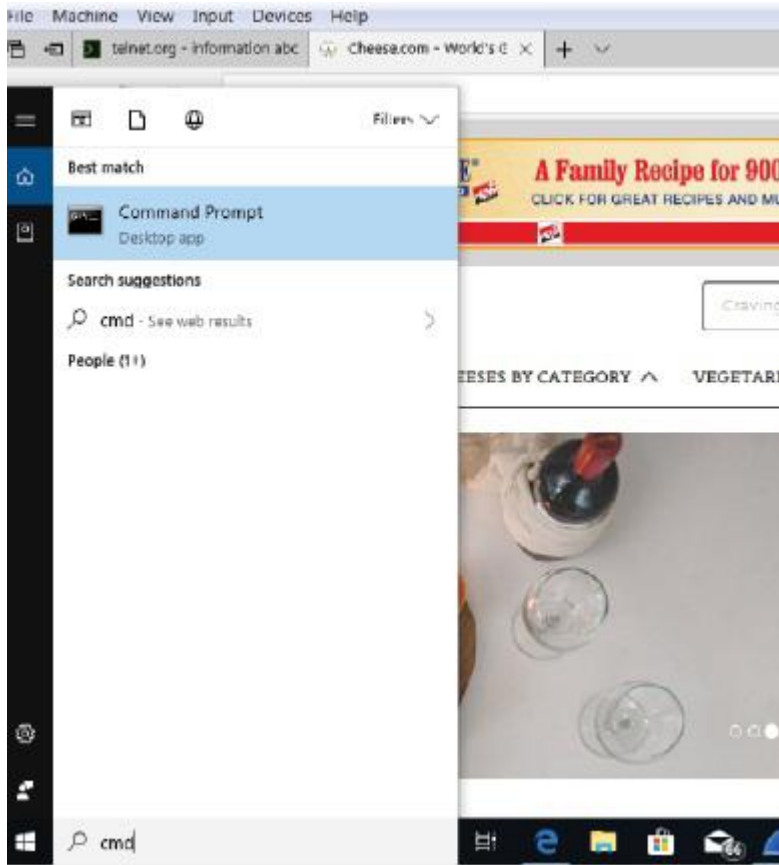
Adım 3:

Wireshark'ın trafiği yakaladığından emin olun.



Adım 4:

Arama çubuğuna 'cmd' yazarak bir komut satırı penceresi açın.



Adım 5:

cisco.com gibi genel bir URL'ye ping atın. Birçok site ICMP'yi engellemiştir. Bu yüzden bunu engellememiş bir websitesi bulun (veya ağınızdaki dahili bir makineye ping atın).

```
Command Prompt
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\paulw>ping cisco.com

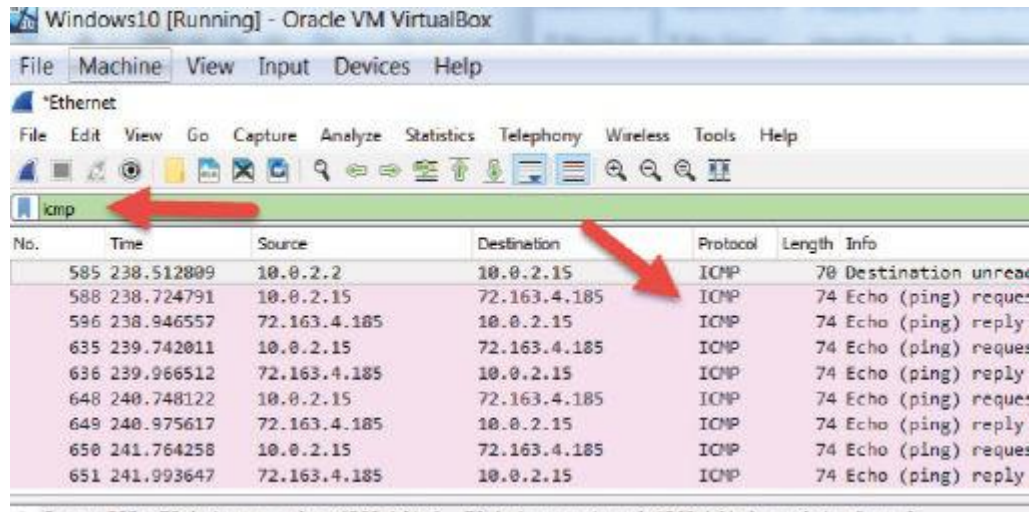
Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=221ms TTL=237
Reply from 72.163.4.185: bytes=32 time=224ms TTL=237
Reply from 72.163.4.185: bytes=32 time=227ms TTL=237
Reply from 72.163.4.185: bytes=32 time=229ms TTL=237

Ping statistics for 72.163.4.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 221ms, Maximum = 229ms, Average = 225ms

C:\Users\paulw>
```

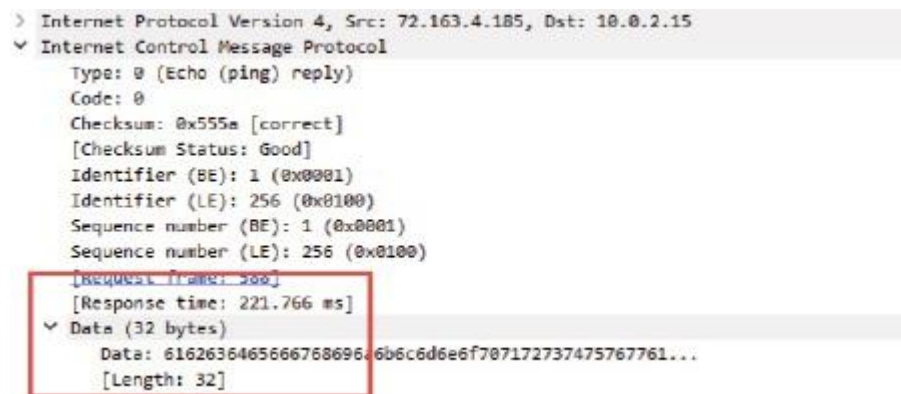
Adım 6:

Sonuçları daraltmak ve ICMP trafiğini kullanmak için Wireshark filtre çubuğunu kullanın. Yalnızca küçük harfle yazın.



Adım 7:

Ping'in ICMP echo isteği ve echo yanıt paketlerini kullandığını unutmayın. Yanıt süresini, uzunluğunu vb. bulun.



Adım 8:

Time To Live'i (TTL) IP başlığı altında bulun.

