ICMP ATÖLYESİ

ATÖLYENİN HEDEFİ:

Bu atölyede ICMP paketinin nasıl alındığını öğreneceksiniz.

ATÖLYENİN AMACI:

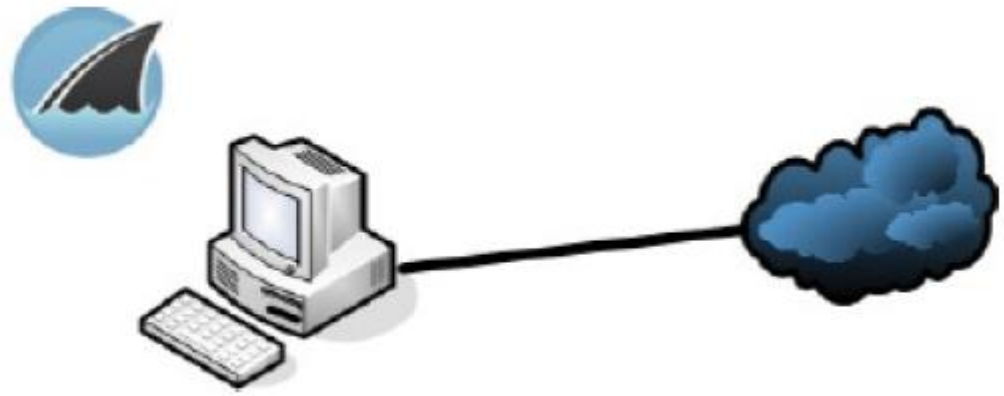
Internet Control Message Protocol (ICMP) ağ aygıtları tarafından güvenilirlik hakkında raporlama yapmak ve hata mesajları göndermek için kullanılır. ICMP, TCP/IP içindeki diğer protokollerin çoğundan farklıdır çünkü veri taşımak için kullanılmaz.

ATÖLYE ARACI:

Wireshark'ı ev bilgisayarınızda da aynı kolaylıkla çalıştırabilirsiniz.

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için aşağıdaki topolojiyi kullanmanız tavsiye edilir.



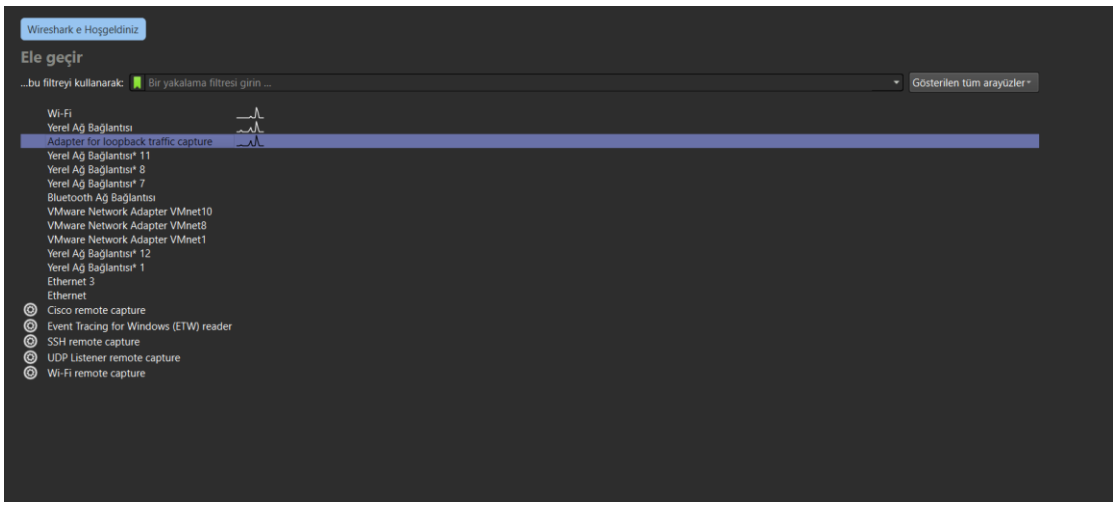
ATÖLYE ANLATIMI:

Adım1:

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

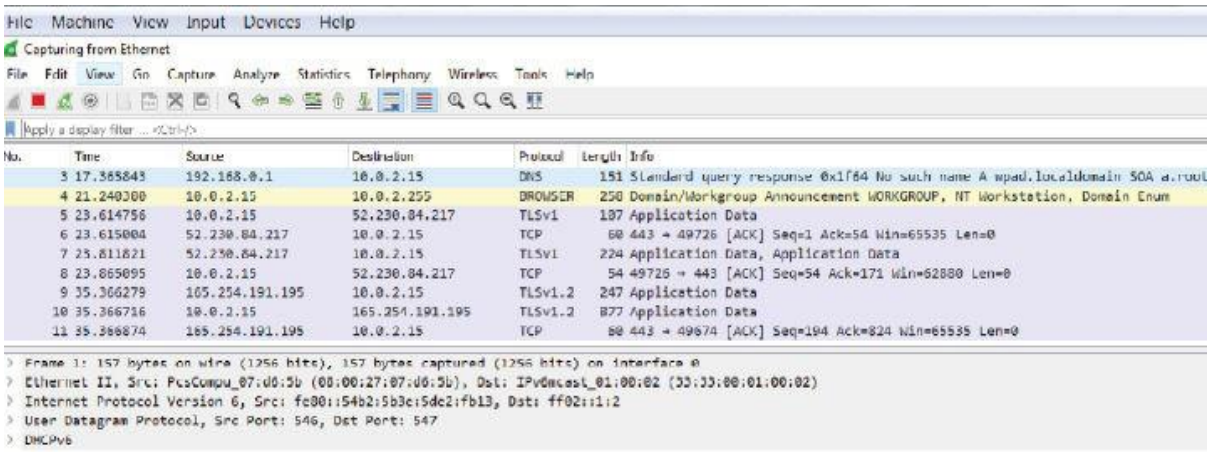
Adım2:

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



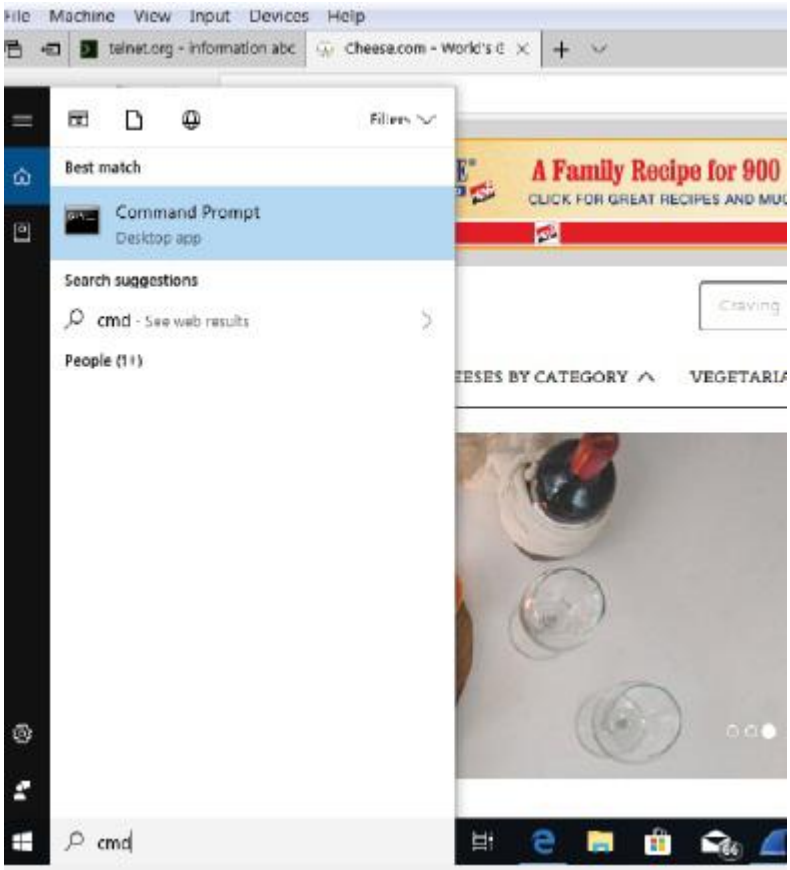
Adım 3:

Wireshark’ın trafiği yakaladığından emin olun.



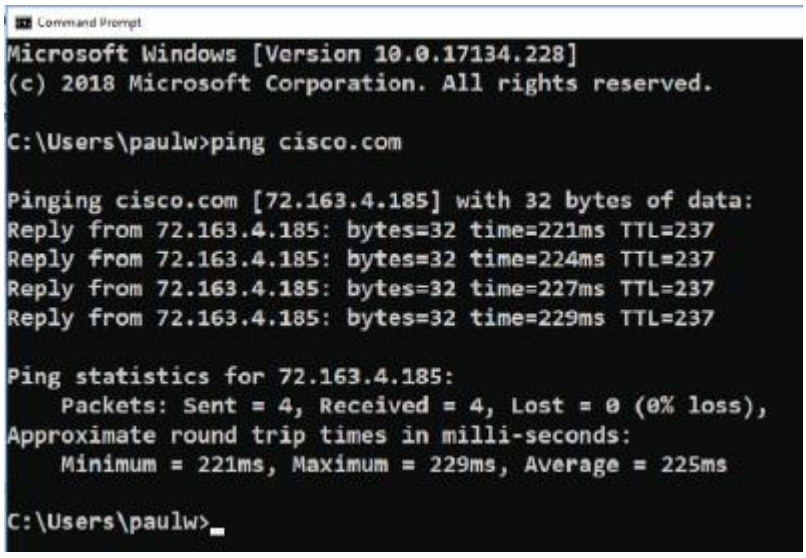
Adım 4:

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



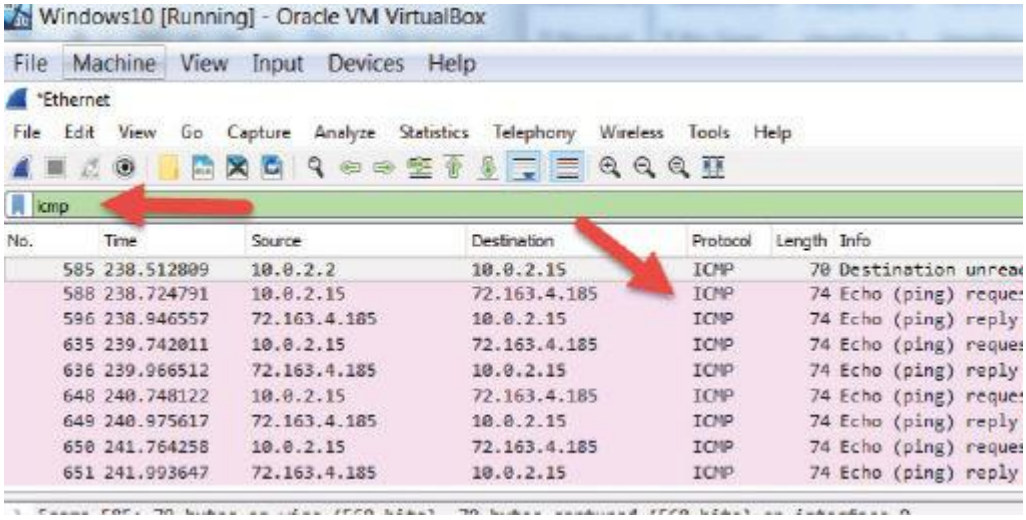
Adım 5:

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).



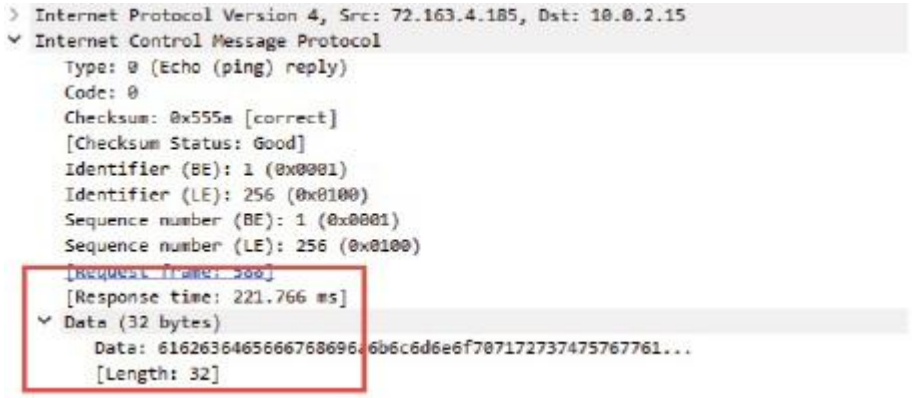
Adım 6:

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.