Ödev - Ağ Trafiğini Görüntülemek için Wireshark Kullanma

Amaç: Yerel ve uzak ağlarda akan paketleri yakalama ve analiz etme

Gerekli kaynaklar

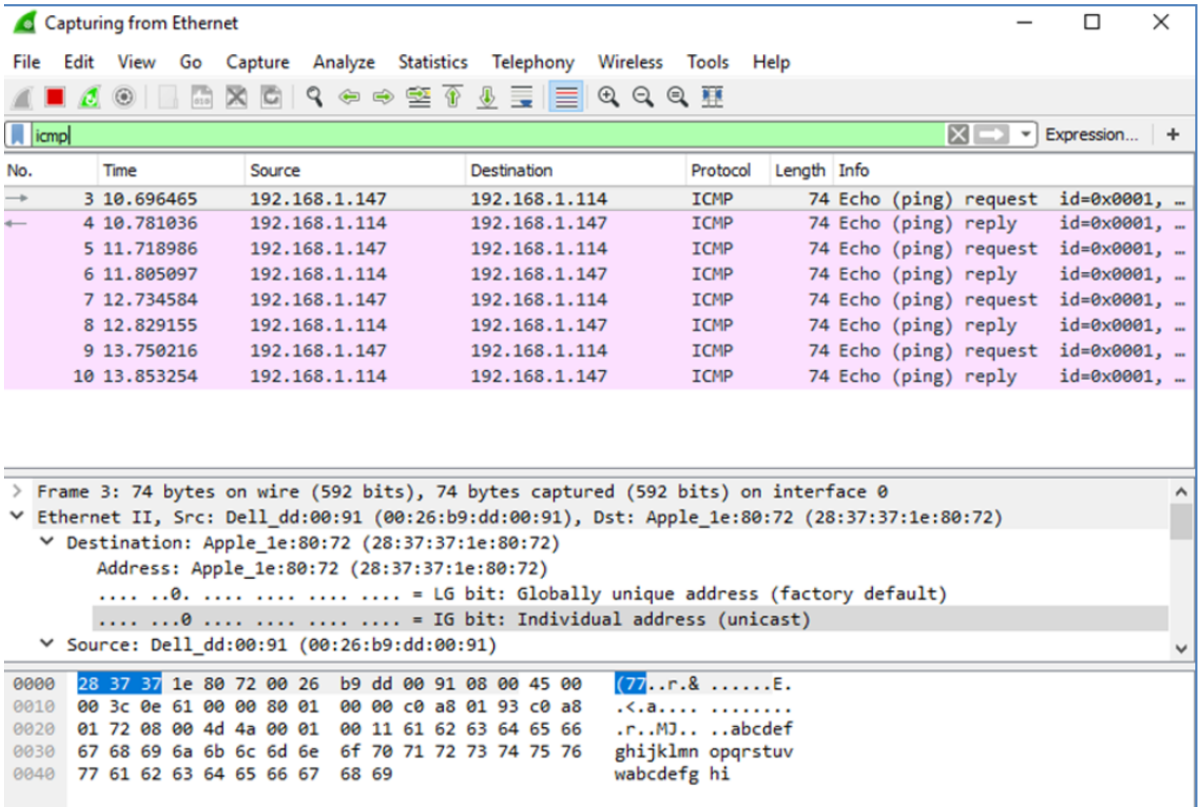
- 1 PC (internet erişimi olan)
- Yerel alan ağındaki (LAN) ek bilgisayarlar, ping isteklerini yanıtlamak için kullanılacaktır

Lab kapsamında öğrenciden istenenler

1) Komut satırında C:\> ping IPv4 adres girerek Wireshark ekranında akan ICMP paketlerini inceleyin

Not: Wireshark'ın üst kısmındaki Filtre kutusuna icmp yazarak trafiği filtreleyebilirsiniz

Filtreleyince aşağıdaki şekle yakın bir görünüm elde etmeniz gerekiyor



Not: Rahat analiz yapabilmek için belirli bir müddet sonra yakalamayı durdur simgesine tıklayarak veri yakalamayı durdurun.

Not: Wireshark verileri üç bölümde görüntülenir: 1) Üst bölüm, listelenen IP paket bilgilerinin bir özetiyle birlikte yakalanan PDU çerçevelerinin listesini görüntüler; 2) orta bölüm, ekranın üst kısmında seçilen çerçeve için PDU bilgilerini listeler ve yakalanan bir PDU çerçevesini protokol katmanlarına göre ayırır; ve 3) alt kısım, her katmanın ham verilerini görüntüler. Ham veriler hem onaltılık hem de ondalık biçimde görüntülenir.

2) Wireshark'ın üst kısmındaki ilk ICMP istek PDU çerçevelerine tıklayın. Kaynak sütununun bilgisayarınızın IP adresini, Hedef sütununun ise ping attığınız bilgisayarın IP adresini içerdiğine dikkat edin.

3) Üst bölümde bu PDU çerçevesi seçiliyken orta bölüme gidin. Hedef ve kaynak MAC adreslerini görüntülemek için Ethernet II satırının solundaki artı işaretine tıklayın.
4) Kaynak MAC adresi PC arabiriminizle eşleşiyor mu?
5) Wireshark'taki hedef MAC adresi, ping attığınız MAC adresiyle eşleşiyor mu?
6) Ping atılan PC'nin MAC adresi PC'niz tarafından nasıl alınır?

7) Aşağıdaki verilen sitelere tarayıcıdan erişin ve yukarıda gerçekleştirdiğiniz adımları burada da gerçekleştirerek paketleri inceleyiniz.

- www.google.com
- www.cisco.com