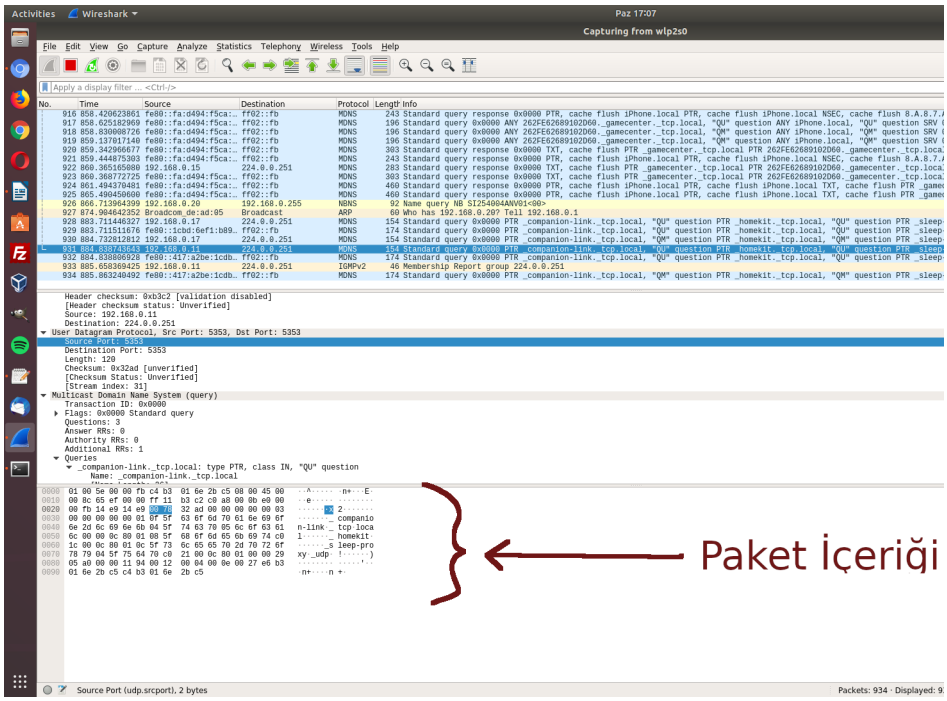
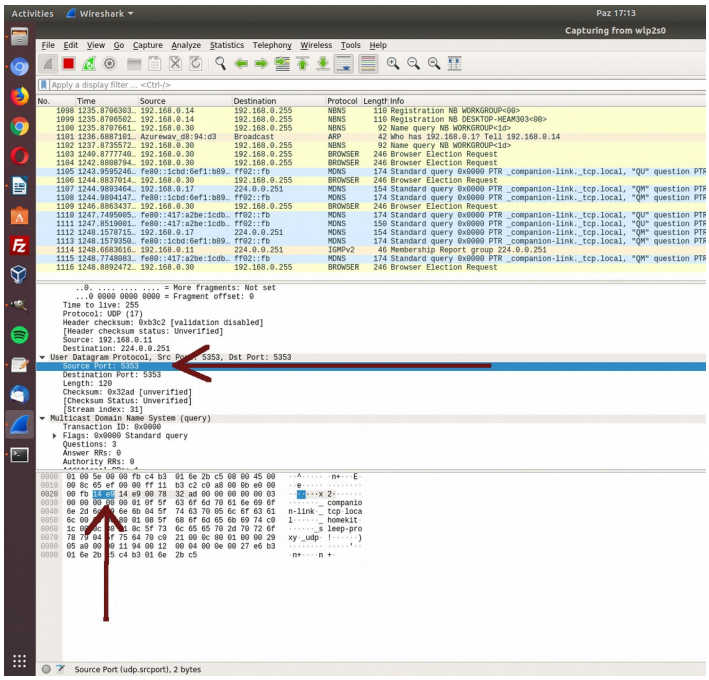
Wireshark Paket İçeriği (Raw Data) Neden Hex Gösterime Sahip?

Soru: Wireshark v.b Yazılımlar Neden Paket İçeriği Olarak Hex Gösterim Sunarlar?

Wireshark'ta trafiği dinlerken ekrana düşen paketlere tıkladığımızda alt bölüme paket içeriğindeki ham veri (raw data) yansır:



Wireshark v.b. bu yazılımlarda paket içeriği gösterilirken ham veri (raw data) hex gösterilir. Çünkü Wireshark'tan ilerleyecek olursak baktığımız paketin başlığını seçmemiz sonrası onun paket ham verisinde (raw data'sında), yani binary'sinde nereye tekabül ettiğini paket binary'si üzerinde direk göstermek yerine paket binary'si üzerinde ilgili binary ifadelerin hex halde özetlenmiş halini bize gösterir.



Not:

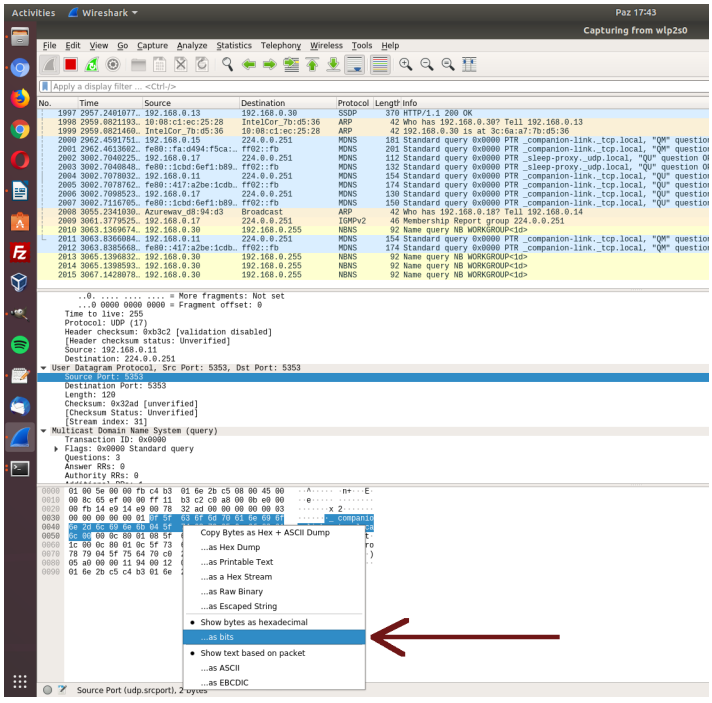
i) Aynı şekilde OllyDebug yazılımında tersine mühendislikle incelenen bir executable programın / yazılımın çözümlenebilen kaynak kodları üzerinde gezinirken çözümlenen kodların executable program içersisinde (raw data'sında), yani binary'sinde nereye denk geldiğini yazılım binary'si üzerinde direk göstermek yerine yazılım binary'si üzerinde ilgili binary ifadelerin hex halde özetlenmiş gösterimlerini bize gösterir.

Normalde internette trafikte TCP/IP paket içerikleri 1 ve 0 bit dizisi halinde gelir ve giderler. Neden o zaman paket içeriği olarak Wireshark v.b. yazılımlar hex kullanmaktadır?

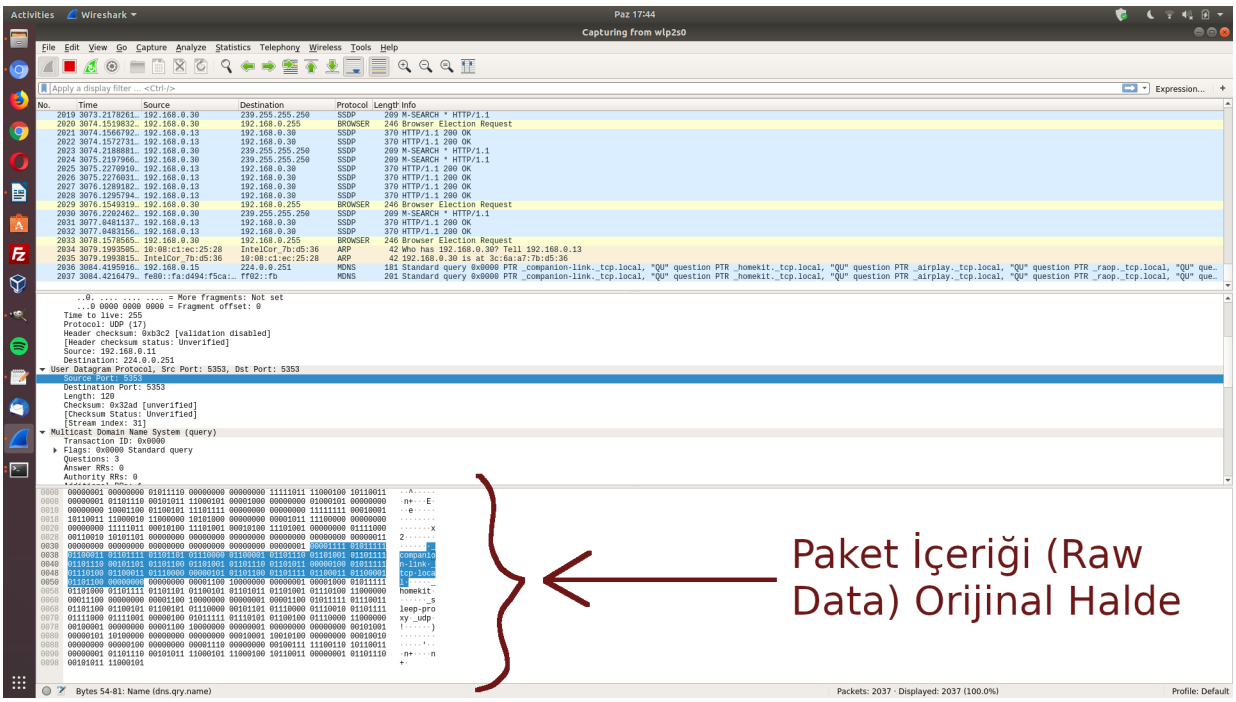
Cevap:

Okunurluk açısından 0 ve 1 bit dizilerini ekrana basmak yığınla veri ekrana basmak olacağından, işlevsiz görüneceğinden okunurluk açısından bunun bir üst level'ı olan hex formatında paket içerikleri gösterilmektedir. Hex formatı ikili formatın bir tık üstünde bir okunurluk sunduğunduğundan ve olabildiğince low level olduğundan dolayı paket içeriği olarak bu format seçilmekte.

Örneğin istenirse Wireshark'da paket içeriği (raw data) gösterimi için default olarak gelen hex özeti halinde göster seçeneği yerine birebir paket ham verisini (orijinal halini) göster seçilebilir:



(Paket içeriğine sağ tık yapıp ...as bits seçilir)



(Paket içeriği orijinal halde görüntülenir)

Kaynaklar

Benim Not

https://osqa-ask.wireshark.org/questions/62161/export-capture-file-as-hex-dump