

## Wireshark Egzersiz – 2

**Son Teslim Tarihi: 27.04.2020 13:00 (Moodle)**

**Web site adresi:** [http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)

Yukarıdaki web site adresini istediğiniz bir internet tarayıcısının adres kısmına giriniz ve Wireshark programı üzerinden aşağıda istenen maddelere göre trafik akışını dinleyiniz.

1. Öncelikle tarayıcınızın önbelleğini temizlediğinizden emin olun. Geçmiş temizlerken aynı zamanda çerezleri ve önbelleği de temizlemelisiniz veya gizli sekme üzerinden işleminizi gerçekleştirebilirsiniz.
2. Wireshark programını çalıştırınız (sadece http mesajlarını dinleyiniz) ve yukarıda verilen url'i tarayıcınızın adres kısmına giriniz.
3. Verilen web sayfasını adres çubuğuna girdikten sonra sizden kullanıcı adı ve şifre isteyecek. Bu alanları şu şekilde doldurunuz:
  - a. **Kullanıcı Adı:** wireshark-students
  - b. **Şifre:** network
4. Kullanıcı adı ve şifreyi doğru bir şekilde girdikten sonra sizi, başarılı bir şekilde giriş yaptığınızı belirten bir web sayfası karşılayacak. Bu sayfayı gördükten sonra Wireshark paket dinleyiciyi durdurabilirsiniz.
5. Bu süreçte kadar yakaladığınız paketleri göz önüne alarak aşağıdaki soruları cevaplayınız:
  - a. Tarayıcınızdan gönderilen ilk HTTP GET mesajına sunucunun yanıtı (durum kodu) nedir?
  - b. Bu durum kodunun ne anlama geldiğini kısa bir şekilde açıklayınız.
  - c. Tarayıcı tarafından HTTP GET mesajı ikinci kez gönderildiğinde, HTTP GET mesajında hangi yeni alan bulunur? (**İpucu:** Hypertext Transfer Protocol sekmesini kontrol edin ve ilgili alanın resmini ekleyin)
  - d. Belirlediğiniz bu yeni HTTP header ne için kullanılmaktadır? Kısaca açıklayınız.
  - e. Bu HTTP header iki farklı parametre almaktadır. Bu parametrelerin neleri ifade ettiğini açıklayınız. İlk parametrenin alabileceği farklı fonksiyonlar vardır. Bu fonksiyonların sadece 2 tanesinin ismini yazınız.