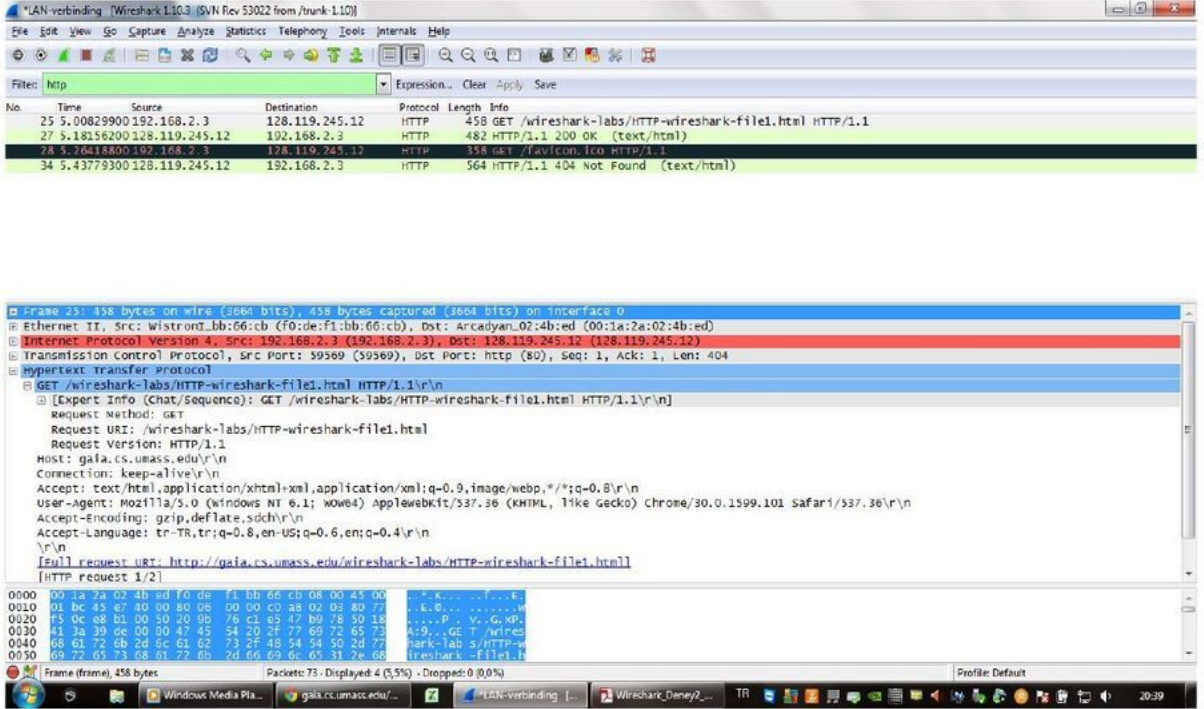


Bilgisayar Ağları Lab - 1

Rapor

1) <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> için sorulan sorular

1-) Benim browserım HTTP 1.1 kullanıyor. Bunu ilk yazılan URL de göderinin yanında "HTTP/1.1 " yazmasından anlıyoruz.Serverda da " request version: HTTP/ 1.1 " yazmasından serverında HTTP1.1 kullandığını anlıyoruz.



2-) Yukarıdaki print screen de de gösterildiği gibi language kısmında ;

Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4\r\n

Yazmaktadır.Buda bize ingilizce ve türkçe kullanımın olduğunu göstermektedir.

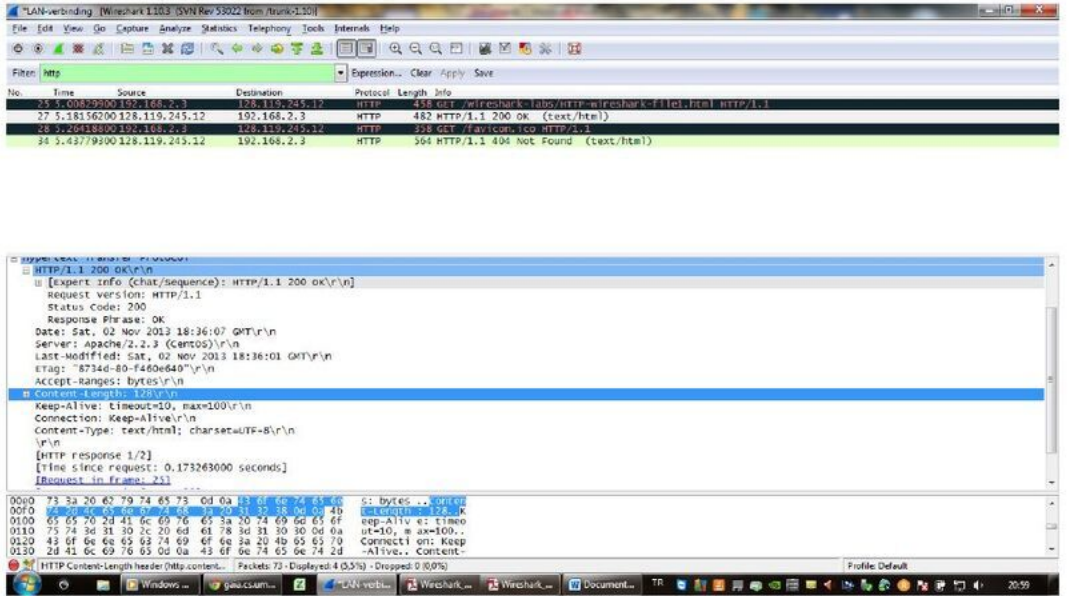
wireshark-file1.html HTTP/1.1

Burada 192.168.2.3 IP adresi benim bilgisayarına ait iken ; 128.119.245.12 IP adresi Server a aittir.

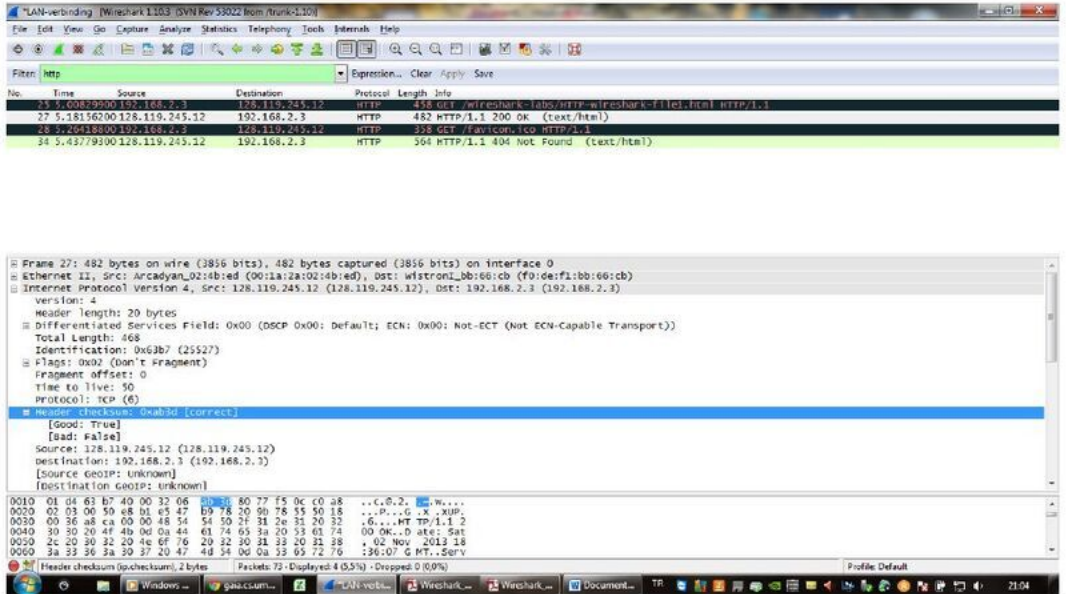
4-) Status kod olarak "HTTP/1.1 200 OK (text/html)" gönderilmiştir.

5-) Son yenileme tarihi " Last-Modified: Sat, 02 Nov 2013 18:36:01 GMT\r\n " burda da belirtildiği gibi 2 Kasım 2013 Saat:18:36 dir.

6-)Content length aşağıdaki print screen de de gösterildiği gibi 128 b dir.

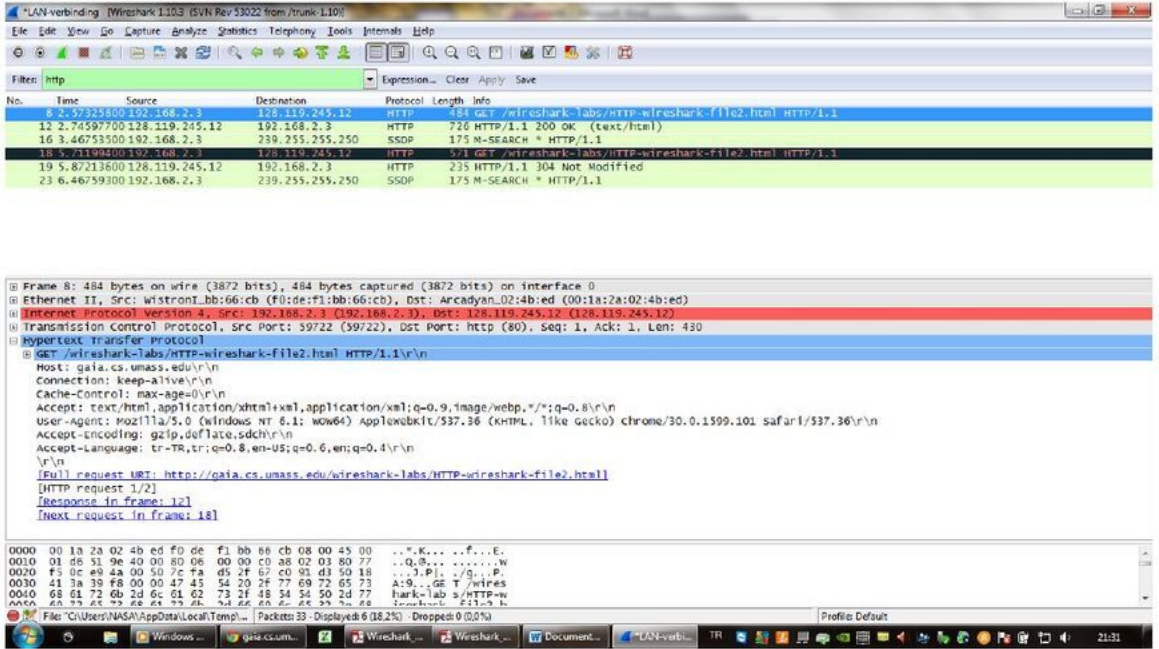


7-)Header lar listeden bakıldığında gözükmesede paket içeriğine girildiğinde hepsinin header ı vardır ve gözükmektedir. Örneğin ; Aşağıdaki print screen de işaretli kısım header ı göstermektedir.



2) <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> için sorulan sorular:

8-) Hayır IF – Modified – Since satırını görmedim.



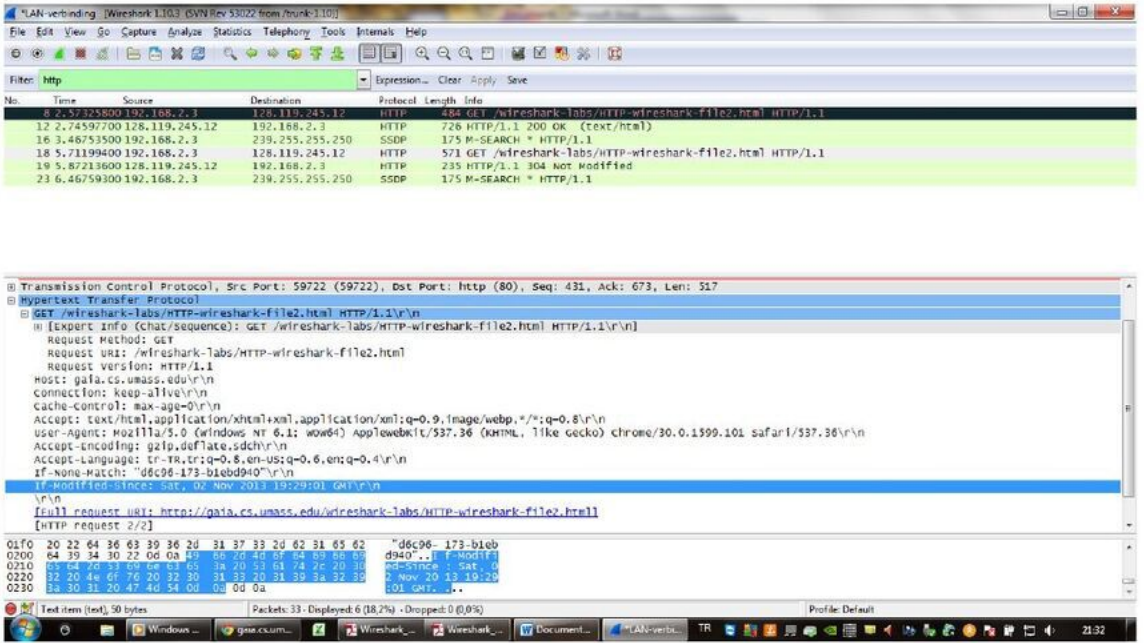
9-) Evet server kesin olarak text cevabı verdi bunu da serverın verdiği cevabın içindeki bu yapıdan anlayabiliriz. Çünkü bu sekmenin içerisinde Line-based text data: text/html kısmında

“Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.”

Bu yazı yer almaktadır.

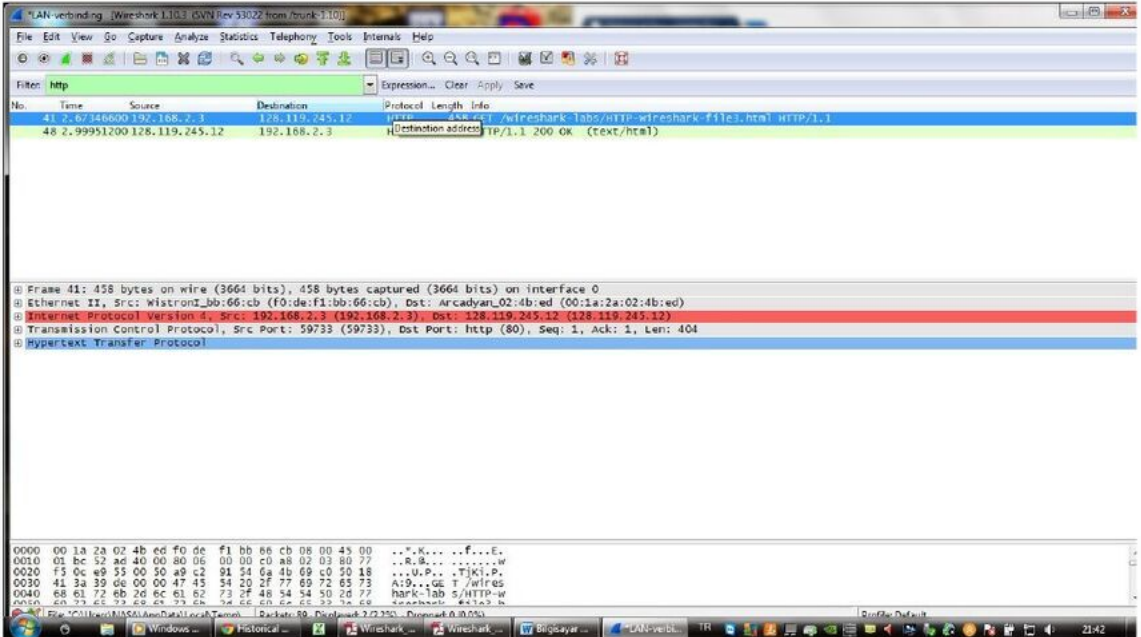
10-) İkinci GET de İF – MODİFİED – SINCE yazısı bulunmaktadır. Aşağıdaki print screen de de gösterilmektedir. Print screen e göre en son 2 kasım 2013 saat : 19:29:01 de modified edilmiştir.



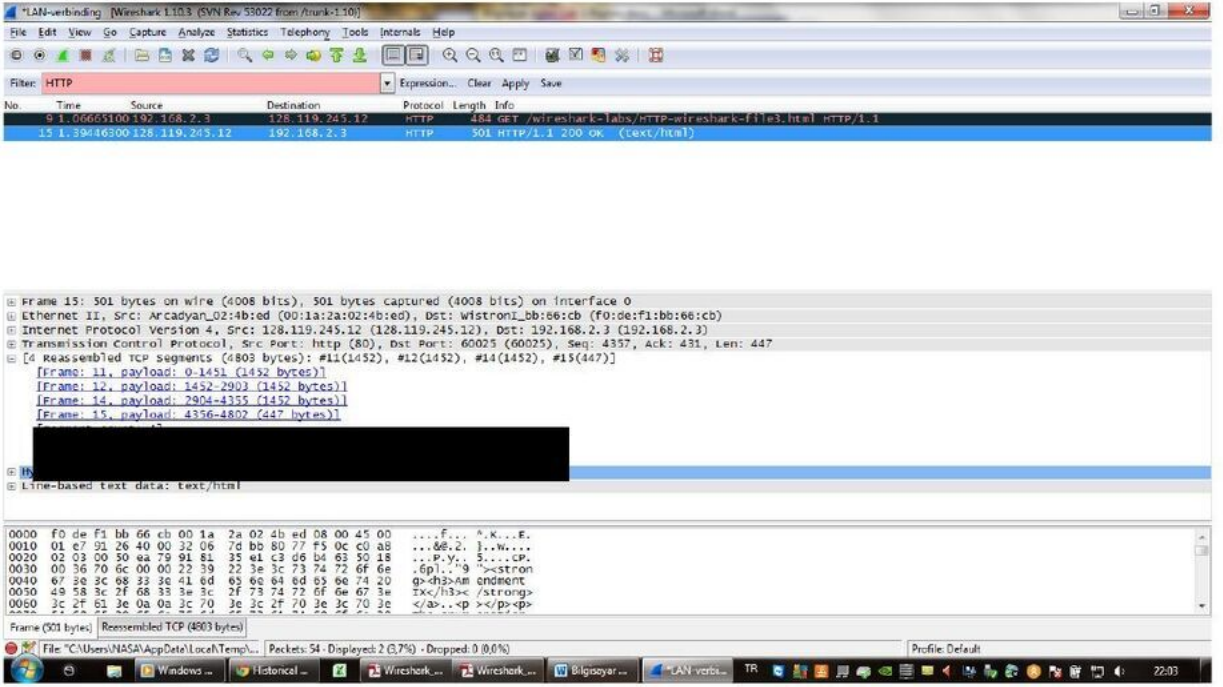
11-) HTTP status ikinci get ten sonra 304 yani => Message: HTTP/1.1 304 Not Modified\r\n
Serverdaki bilgide bir deęişiklik olmadığı için ilk get te yüklenen yazı cache den çağırılmıştır.

3) <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> için olan soruların cevapları :

12-) Print screen de de görüldüğü gibi 1 tane GET mesajı var.



13-) TCP sekmesinden baktığımızda alttaki print screen de olduğu gibi 1452,1452,1452,447 byte kullanıyor.Tcp 4 data paketi taşıyor ve toplam boyut Content – lenght 4500 byte.

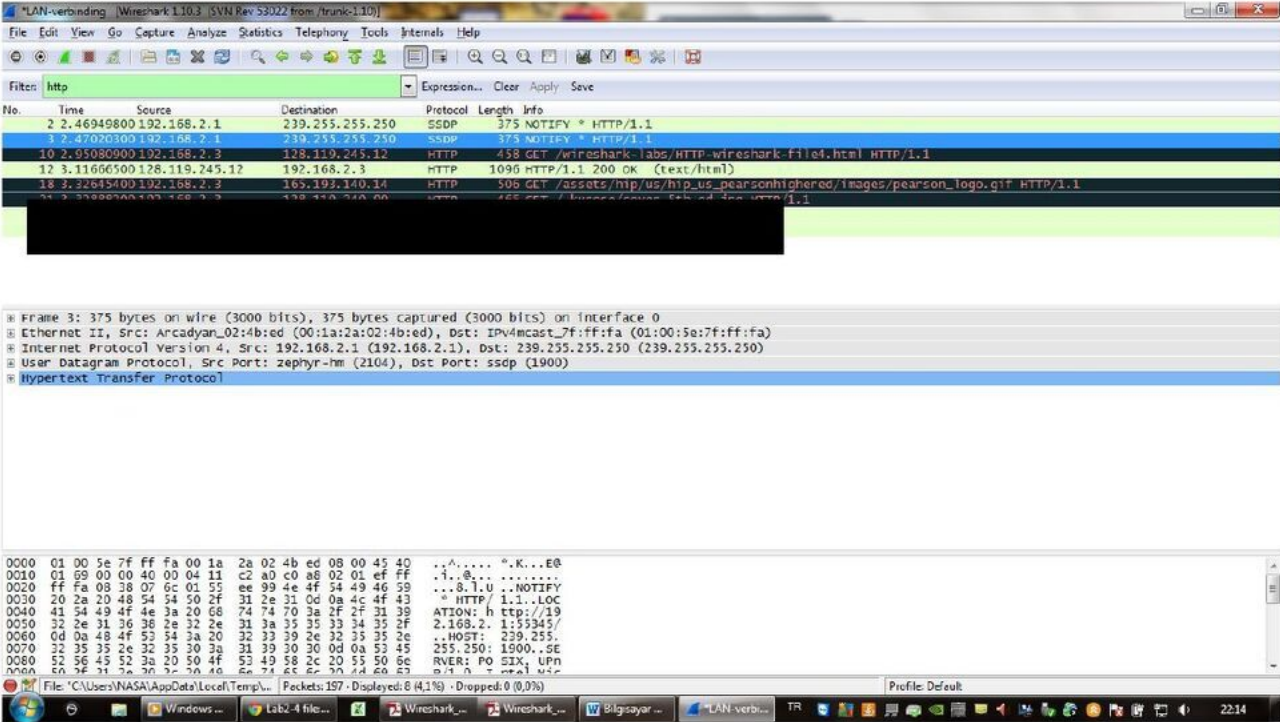


14-) Status Code: 200 yani OK konumunda

15-) Hayır , HTTP ve TCP de başka durum bildiren bir yapı yok .

4) <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> için olan soruların cevapları :

16-) Aşağıdaki print screen de de görüldüğü gibi 3 tane GET komutu bulunmaktadır. Bunlardan 3 tane geri dönen IP vardır bunlar 128.119.245.12 , 165.193.140.14 , 128.119.240.90



17-) Bu yapıya bakıldığında iki resim için iki TCP bağlantısı kullanıldığını görüyoruz ve bu da seri indirildiğini gösteriyor.

5) http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html için olan soruların cevapları :

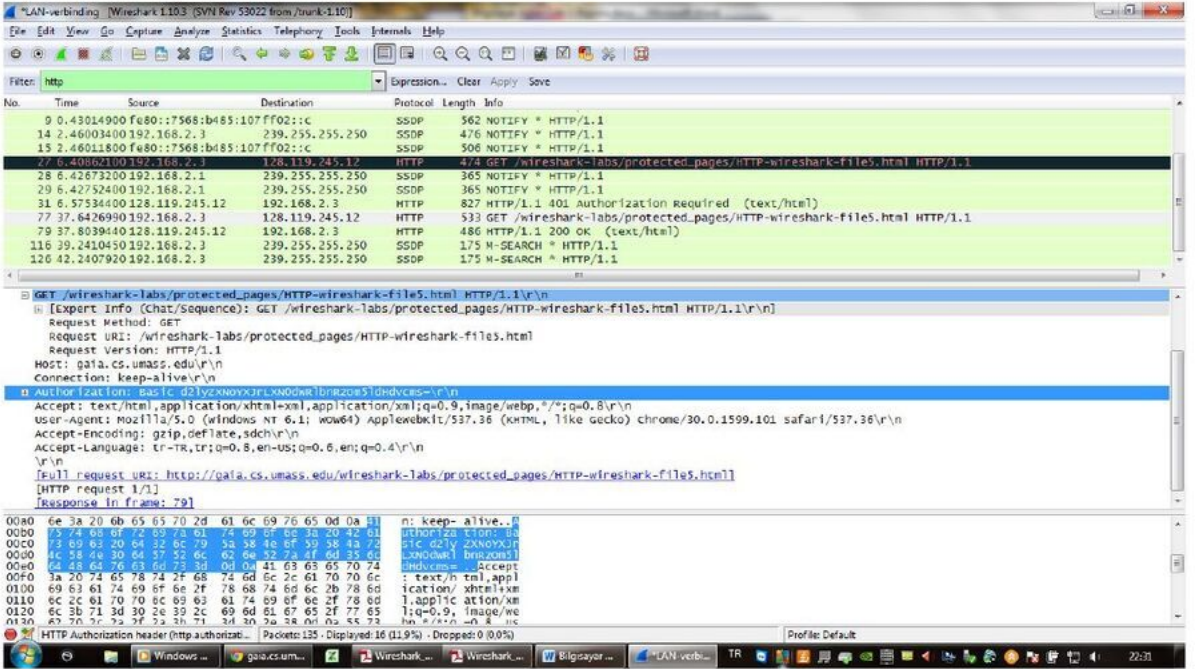
18-) HTTP GET in ilk status kodu aşağıda da belirttiğim gibi 401 yani “Authorization Required”

The screenshot shows the Wireshark 1.10.3 interface. The packet list on the left shows a series of SSDP and HTTP packets. The selected packet is packet 31, an HTTP 401 Authorization Required response. The packet details pane on the right shows the following information:

- Frame 31: 827 bytes on wire (6616 bits), 827 bytes captured (6616 bits) on interface 0
- Ethernet II, Src: Arcadyan_02:4b:ed (00:1a:2a:02:4b:ed), Dst: WistronI_bb:66:cb (f0:de:f1:bb:66:cb)
- Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.3 (192.168.2.3)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 60150 (60150), Seq: 1, Ack: 421, Len: 773
- Hypertext Transfer Protocol
 - HTTP/1.1 401 Authorization Required\r\n
 - [Export Info (Chat/Sequence): HTTP/1.1 401 Authorization Required\r\n]
 - Request version: HTTP/1.1
 - Status Code: 401
 - Response Phrase: Authorization Required
 - Date: Sat, 02 Nov 2013 20:26:55 GMT\r\n
 - Server: Apache/2.2.3 (CentOS)\r\n
 - WWW-Authenticate: Basic realm="wireshark-students only"\r\n
 - Content-Length: 486\r\n
 - Keep-Alive: timeout=10, max=100\r\n
 - Connection: Keep-Alive\r\n

The packet bytes pane at the bottom shows the raw data of the packet, including the HTTP status code and response headers.

19-) İkinci GET te ise şifre girildikten sonra ;



Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n böyle bir kısmını geliyor.

Lab sorularının alt kısmında da bu şifrelemenin kriptolu gönderilmediğini ve kriptolu örnekler için “HTTP Access Authentication Framework” kısmına bakmamız gerektiği belirtiliyor.