|  |
| --- |
|  |
| Bilgisayar Ağları Lab. – 3 DNS |
| Rapor |
|  |
|  |
|  |

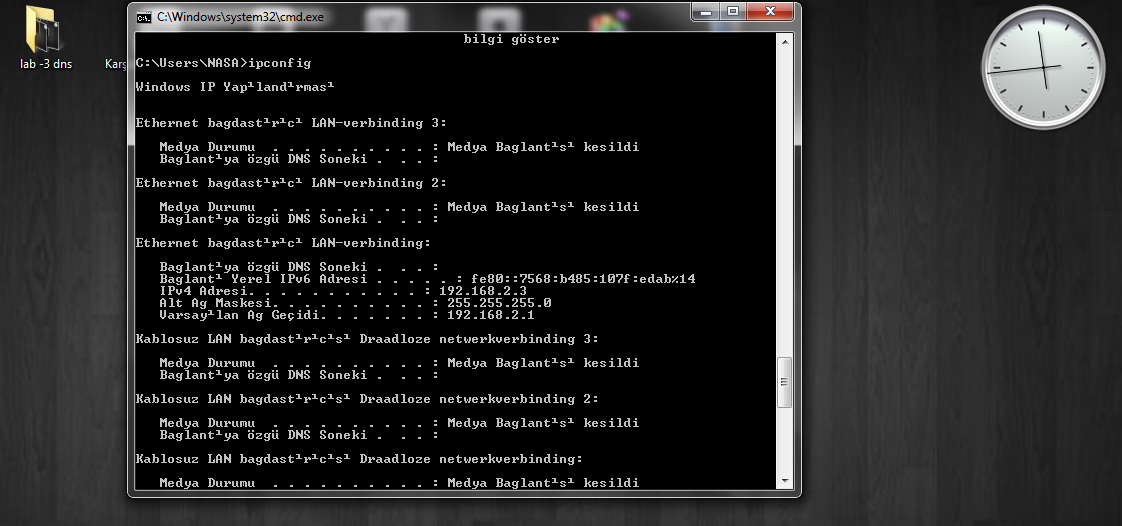
AD : Canberk ŞAHİN

NUMARA: 21095835

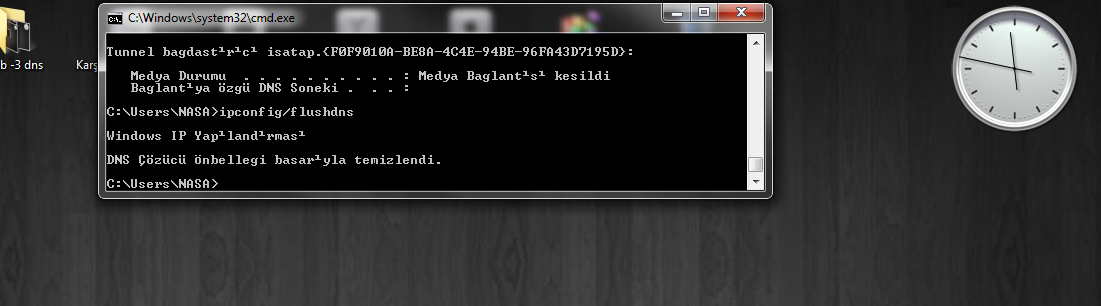
**Bilgisayar Ağları Lab - 1**

**Rapor**

* Nslookup [www.mit.edu](http://www.mit.edu) yazıldığında ;
* Nslookup –type = NS mit.edu yazıldığında ;
* Nslookup [www.aiit.or.kr](http://www.aiit.or.kr) bitsy.mit.edu
* İpconfig/all



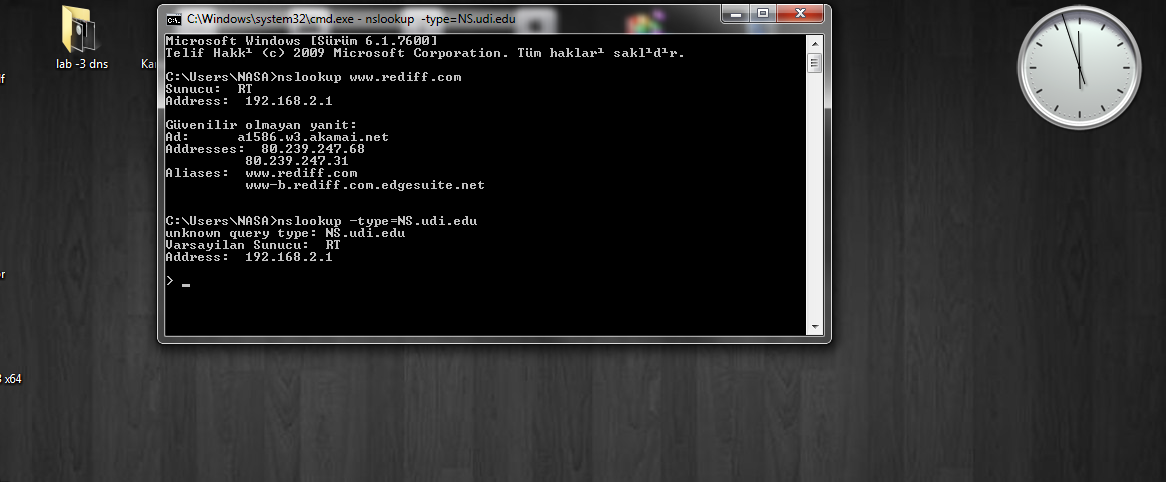
* İpconfig /flushdns



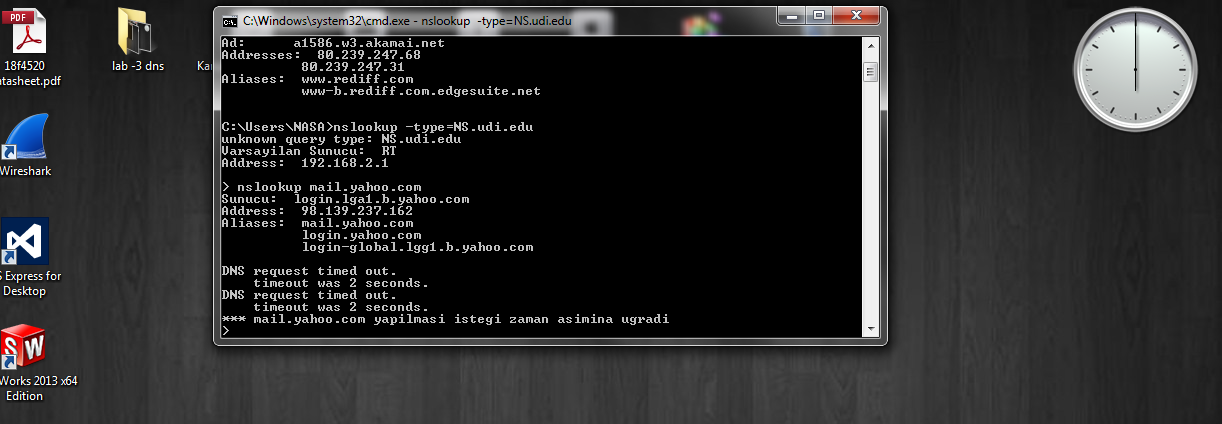
1-)Asia için [www.rediff.com](http://www.rediff.com) denendiğinde nslookup aşağıdaki gibi olmaktadır.



2-) nslookup –type=NS.udi.org Avrupadaki bi üniversite sitesi

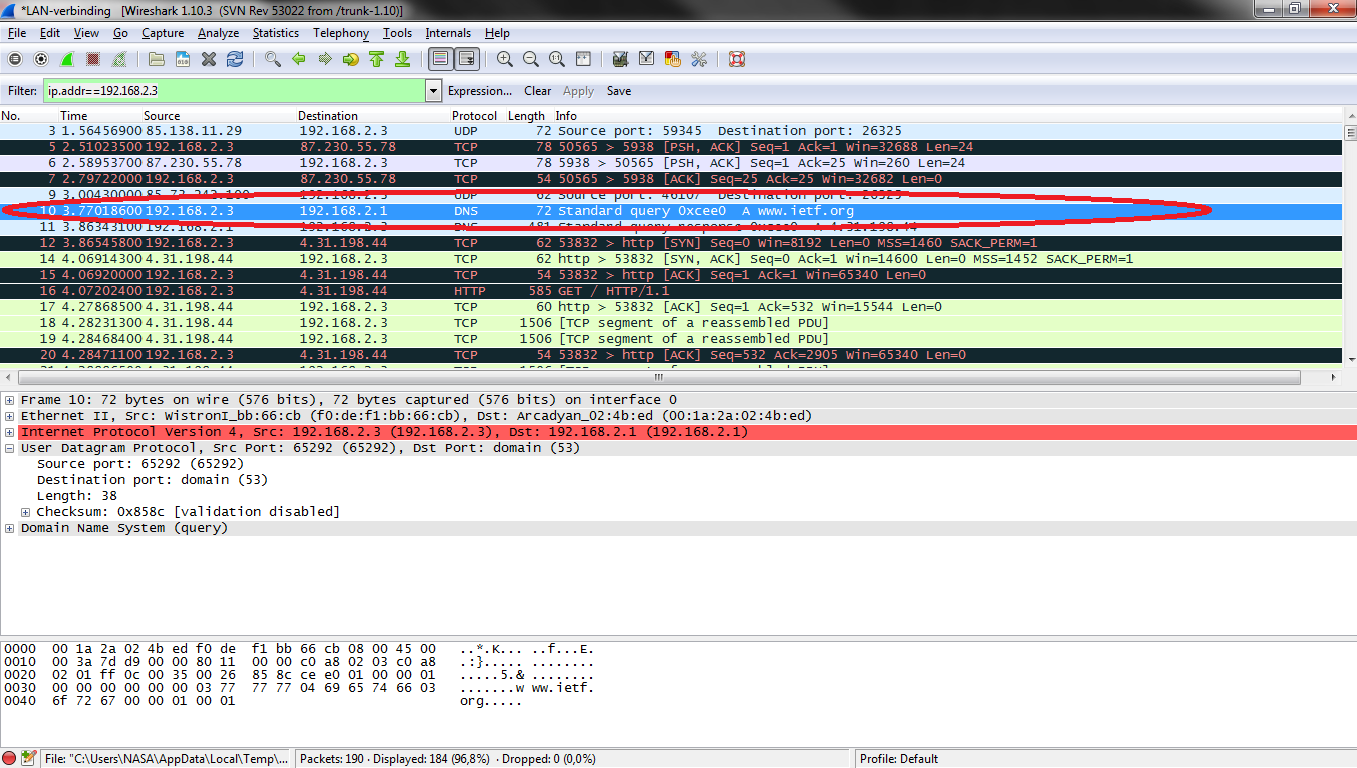


3-) nslookup mail.yahoo.com ya baktığımızda ;



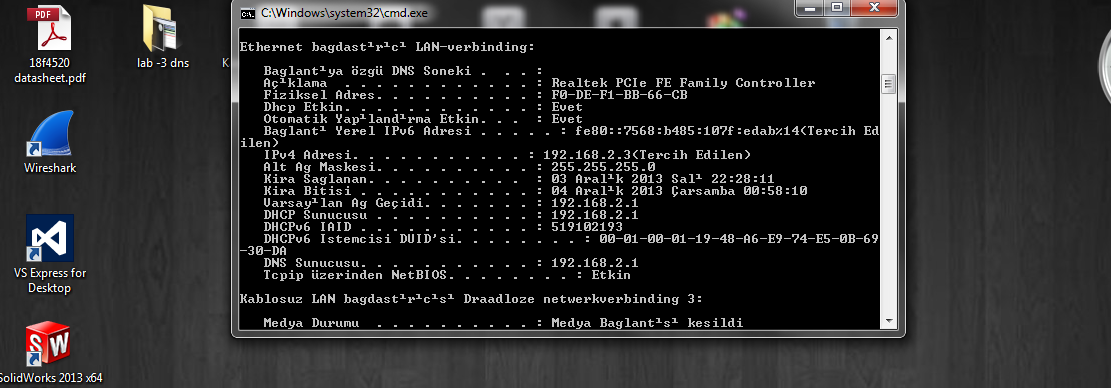
3. Kısım ilk işlemi;

4)

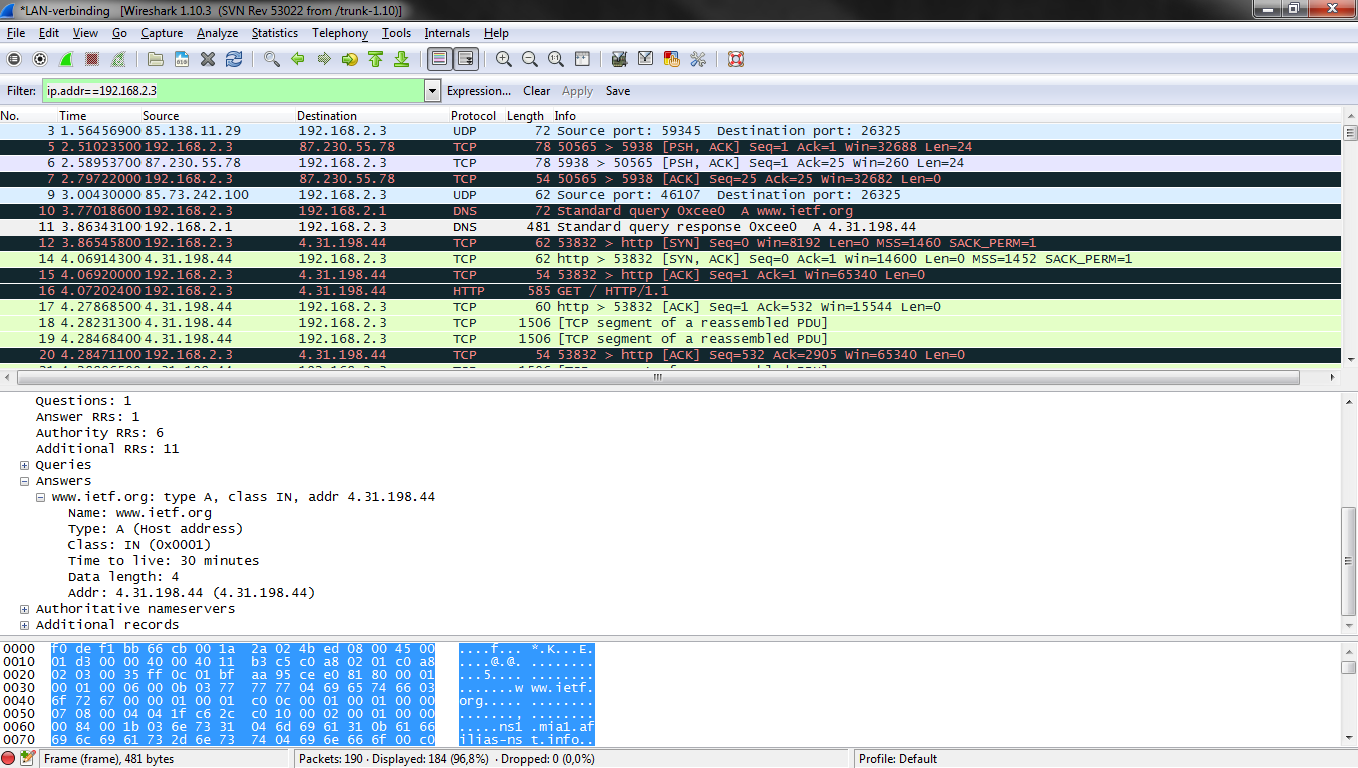
[www.ietf.com](http://www.ietf.com) için wireshark ta bakıldığında aşağıda kırmızıyla belirttiğim gibi User Datagram Protocol yani UDP kullanılmıştır.

5)Yukarıdaki screenshotta da görüldüğü gibi Source port (Scr port ) = 65292 ve Destination port yani Dst = 53 üncü porttadır.

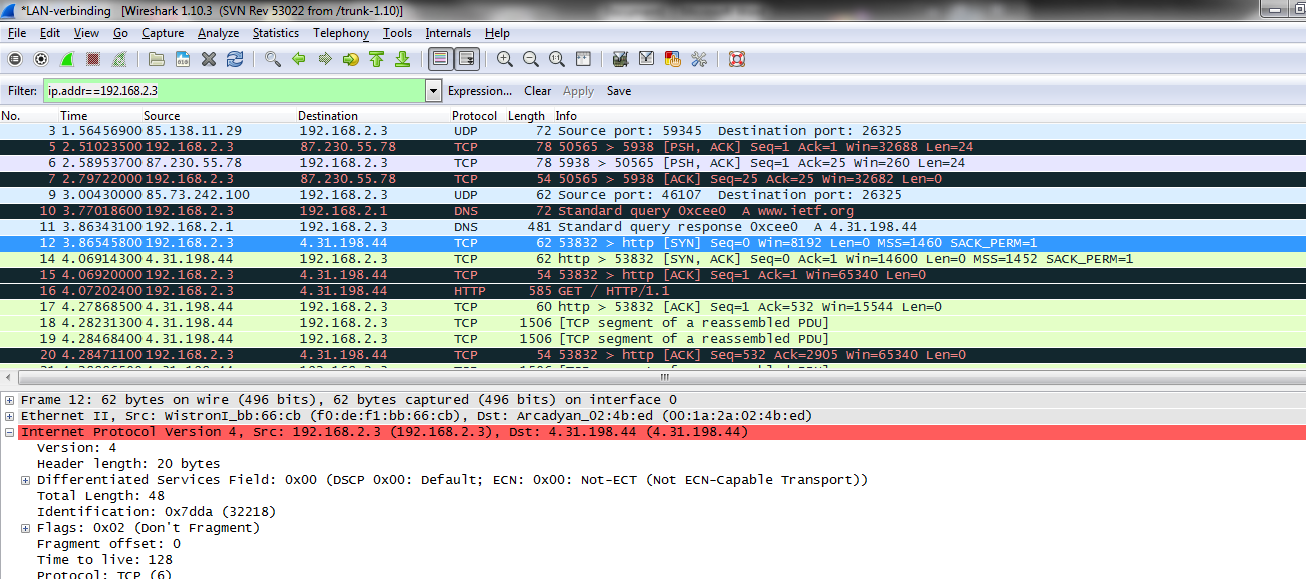
6) Aşağıda da gösterdiğim gibi Varsayılan ağ geçidi ve DHCP sunucusu IP si 192.168.2.1 dir.Wire shar ta da görülmektedir. Benim Ip adresimde 192.168.2.3 dür.



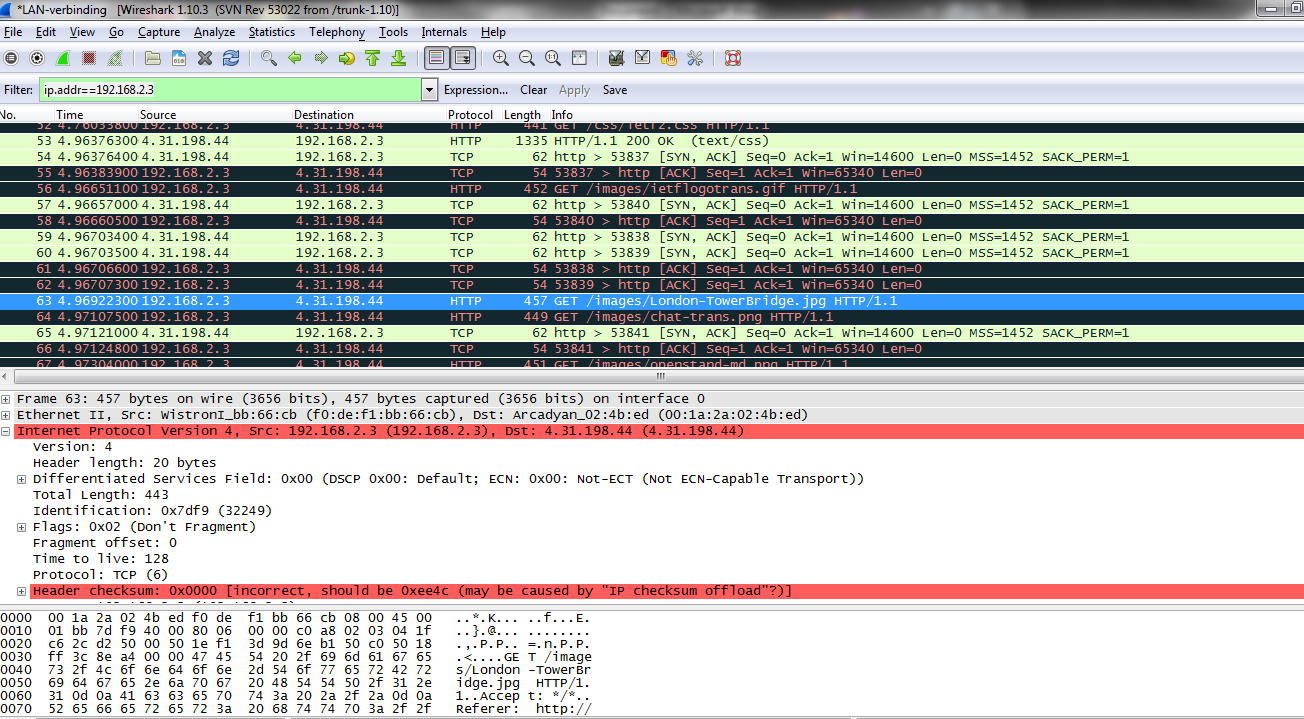
7) Bu standart bir query mesaj ve herhangi bir veri içermemektedir. Yukarıdaki screenshotta da görülmektedir.

8) Aşağıda da gösterildiği gibi TYPE A class IN addres 4.31.198.44 ve DNS sekmesini açtığımızda answer =1 görülmektedir.

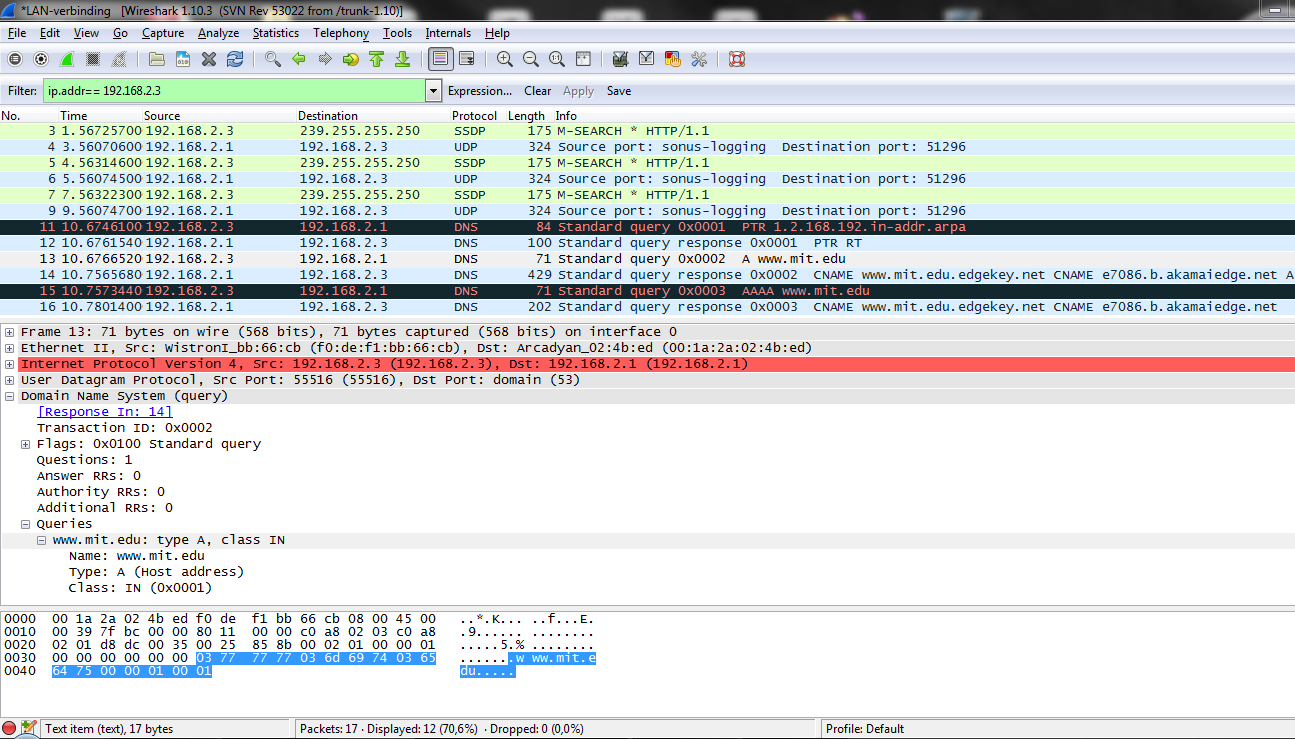
9)ilk SYN paketinde 4.31.198.44 IP adresinden cevap gönderilmiştir.



10) Aşağıda da görüldüğü gibi web sitesindeki resimler için yeni bir DNS query oluşturulmamıştır.



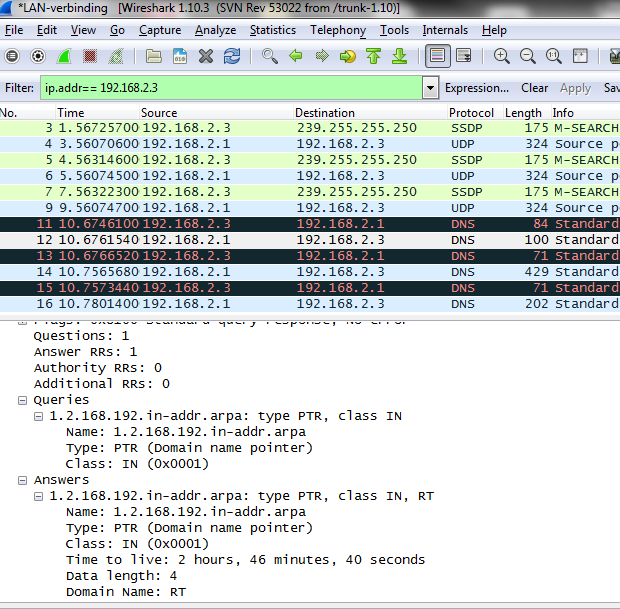
\*\* nslookup cmd kısmından [www.mit.edu](http://www.mit.edu) yaptığımızda aşağıdaki çıktıyı görmekteyiz.



11) Source port 55516 ve Destination Port ta 53 dür. Yukarıdaki screen shottada görülmektedir.

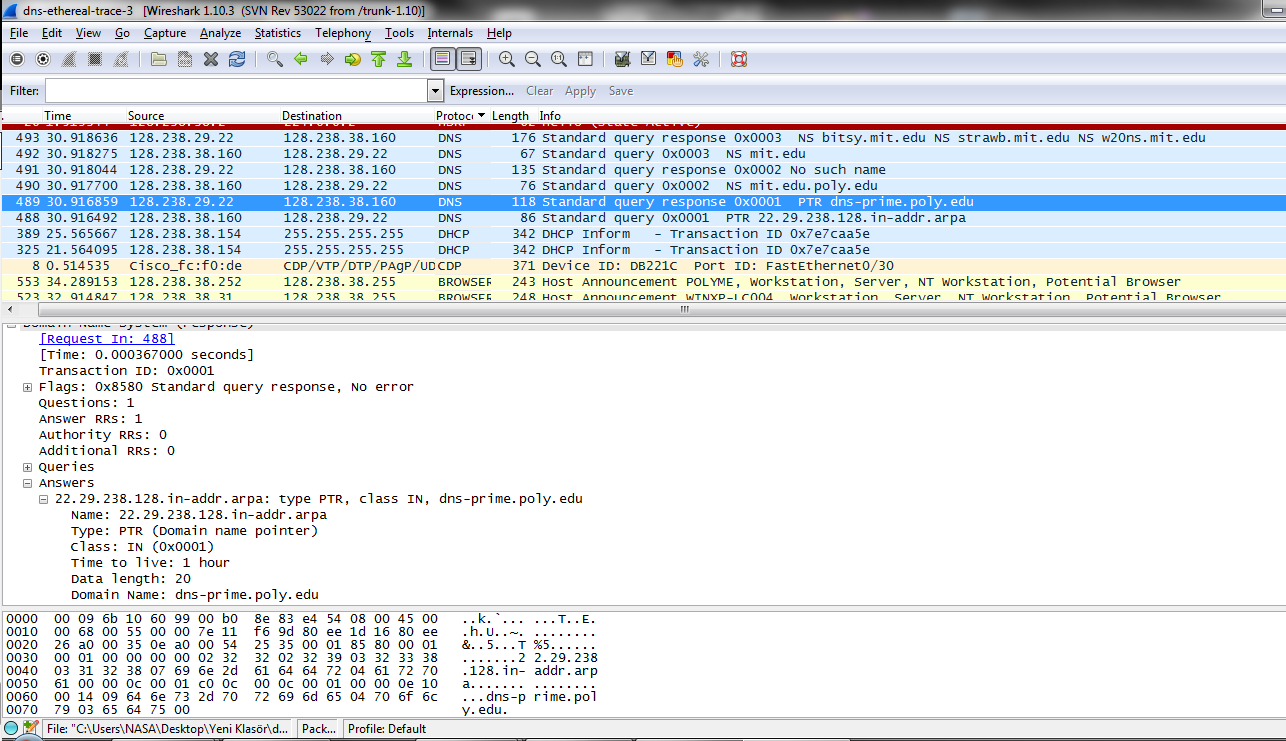
12) Daha önce ipconfig / all yaptığımızda da gördüğümüz gibi 192.168.2.1 IP adresi benim local default DNS server IP adresimdir.

13) Yukarıdaki screenshottada görüldüğü gibi TYPE A DNS türüdür. Ve Answer veya bi içerik içermez.

14) Aşağıdaki screenshottada görüldüğü gibi 1 cevap gelmiş ve içeriğide aşağıda belirtilmiştir.

16) Kendi bilgisayarımdan ve farklı bir bilgisayardan denememe rağmen nslookup-type=NS mit.edu DNS için timeout vermektedir.Bundan dolayı lab föyünden trace indirme kısmından edindiğim tracelerle devam etmekte dolayısıyla IP adreslerinde farklılıklar bulunmaktadır.\*\*

Aşağıdaki screenshot a göre DNS query mesajının IP adresi 128.238.29.22 dir.



17)

Type NS ve answer yani bir içerik bulunmamaktadır.

18)

İsim serverı bitsy, strawb and w20ns.

Additional kısmına bakar isek Ip adresini buluruz

Answers

mit.edu: type NS, class inet, ns bitsy.mit.edu

mit.edu: type NS, class inet, ns strawb.mit.edu

mit.edu: type NS, class inet, ns w20ns.mit.edu

Additional records

bitsy.mit.edu: type A, class inet, addr 18.72.0.3

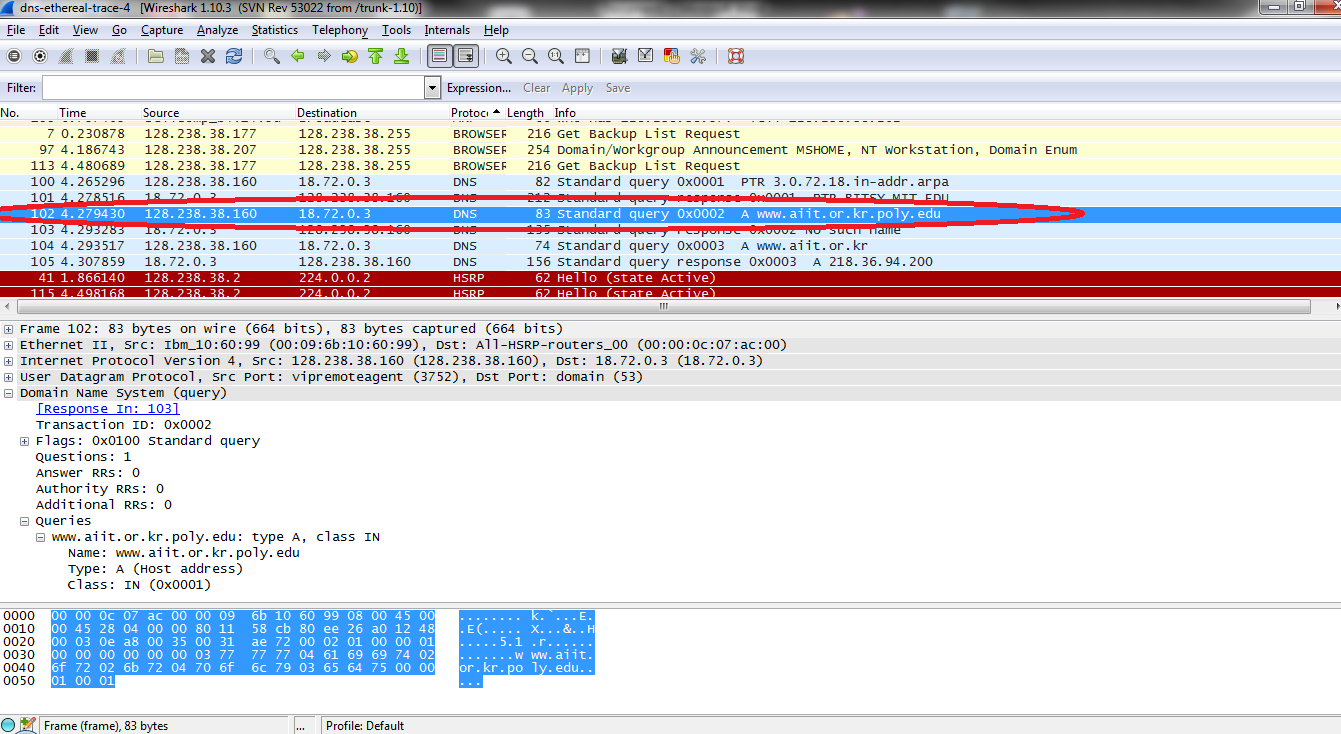
strawb.mit.edu: type A, class inet, addr 18.71.0.151

w20ns.mit.edu: type A, class inet, addr 18.70.0.160

20)

Bu soruda da aynı sıkıntı yaşandığı için aynı şekilde trace dosyasını föyde belirtilen siteden indirerek yaptım.\*\*

Aşağıdaki screenshotta da belirtildiği gibi IP = 18.72.0.3 dur. Hayır benim default local DNS serverım değil. Bu bitsy.mit.edu ya ait.



21)Yukarıda da görüldüğü gibi DNS TYPE A dır. Ve answer yoktur.

22) Aşağıdaki screenshot tada görüldüğü gibi 1 answer var ve bunun içeriğide screenshotta gösterilmiştir.

