T.C.
SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BSM 435

İNTERNET MÜHENDİSLİĞİ

DNS PROTOKOLÜ

U161210008 Elif Cansu DÜZGÜN
G161210068 Enes Furkan YAVUZ
B1109.10007 Samet ORUÇ

Fakülte Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ

Öğretim Üyesi : Dr.Öğr.Üyesi MUSA BALTA

1. DNS NEDİR?

DNS (***D**omain Name **S**ystem*, **Alan Adı Sistemi**), internet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan, bilgisayar, servis, internet veya özel bir ağa bağlı herhangi bir kaynak için hiyerarşik dağıtılmış bir adlandırma sistemidir.

İnternet ağını oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri kullanıcıların kullanımı için www.site_ismi.com gibi kolay hatırlanır adreslere karşılık düşürülür. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır.

Katılımcı kuruluşların her birine atanmış alan adları çeşitli bilgileri ilişkilendirir. En belirgin olarak, insanlar tarafından kolayca ezberlenebilen alan adlarını, dünya çapında bilgisayar servisleri ve cihazlar için gerekli sayısal IP adreslerine çevirir (dönüştürür). DNS, çoğu internet servisinin işlevselliği için temel bir bileşendir, çünkü internetin temel yönetici servisidir.

Alan Adı Sistemi DNS her alan için yetkili ad sunucuları atayarak alan adlarını atama ve bu adların IP adreslerine haritalanması sorumluluğunu verir. Yetkili ad sunucuları desteklenen alanları için sorumlu olmakla görevlidirler ve diğer ad sunucuları yerine alt alanlara yetki (otorite) verebilirler. Bu mekanizma dağıtılmış ve arızaya toleranslı servis sağlar ve tek bir merkezi veri tabanına ihtiyacı önlemek için tasarlanmıştır.

DNS aynı zamanda özünde (çekirdekte) bulunan veritabanı servisinin teknik işlevselliğini de belirtir. DNS protokolünü – DNS'de kullanılan veri yapılarının ve veri iletişim alışverişinin (değiş tokuş) detaylı tanımlaması- İnternet Protocol Suite'in bir parçası olarak tanımlar. Tarihsel olarak DNS' den önceki yönetici servisleri orijinal olarak metin dosyalarına ve belirgin bir şekilde HOSTS.TXT çözücüsüne dayandığı için büyük veya küresel yöneticilere göre ölçeklenebilir değildi. DNS 1980' den bu yana yaygın olarak kullanılır olmuştur.

İnternet hiyerarşi alan adı ve İnternet Protokol (IP) adres boşluğu olmak üzere iki ana ad boşluğunu sağlar. DNS sistemi alan adı hiyerarşisi sağlar ve onunla adres boşluğu arasında çeviri servisi sağlar. İnternet adı sunucuları ve iletişim protokolü Domain Name Sistemini etkin kılar. Bir DNS ad sunucusu, alan DNS kayıtlarını alan adı için depolayan bir sunucudur; DNS ad sunucusu veri tabanına karşı sorulara cevaplarla karşılık verir.

DNS veri tabanında depolanan en yaygın kayıt türleri; DNS bölgesinin yetkisi otoritesi (SOA), IP adresleri (A ve AAAA), SMTP posta değiştiriciler (MX), ad sunucuları (NS), ters DNS aramaları için işaretçiler (PTR) ve alan adı takma isimleridir (CNAME).

Genel amaçlı bir veri tabanı olmak için tasarlanmamasına rağmen, DNS diğer veri türleri için DNSSEC kayıtları gibi şeyler için otomatik makine aramalarını ya da Sorumlu kişi (RP)

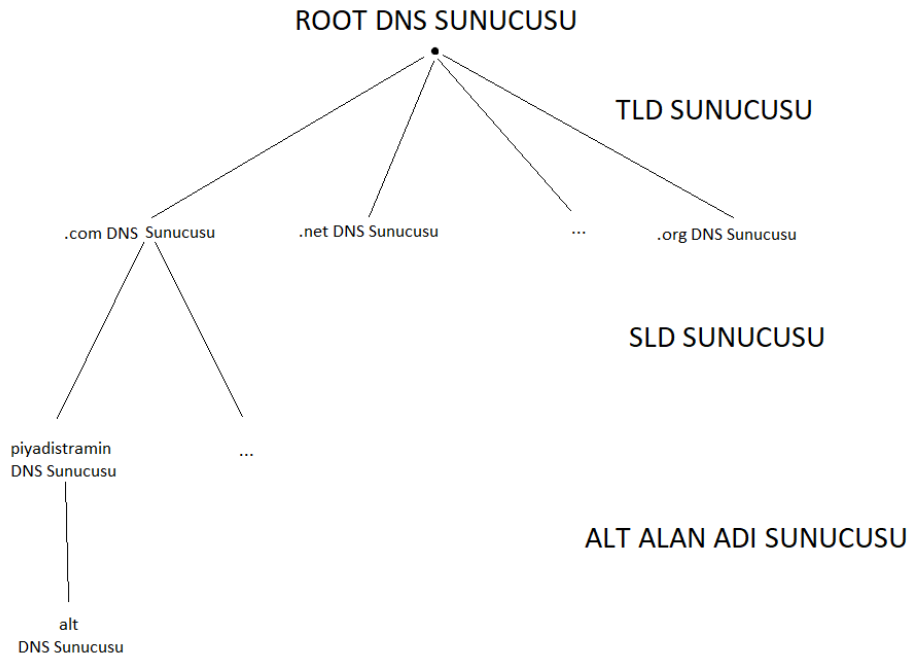
kayıtları gibi insan sorularını da depolayabilir. DNS kayıt türlerinin tam listesi için, DNS kayıt türlerinin listesi bakın. Genel amaçlı veritabanı olarak, DNS veri tabanında saklanan gerçek zamanlı kara delik listesi kullanılarak istenmeyen e-posta (Spam) ile mücadelede kullanımında da DNS görülebilir. İnternet adlandırma için veya genel amaçlı kullanımlar için olsun, DNS veritabanı, yapılandırılmış bölge dosyasında geleneksel olarak depolanır.

2.DNS ÇALIŞMA YAPISI

DNS, kullanıcıların web sitesi alan adına istek göndermesi ile çalışmaya başlar. Web sitelerine ulaşmak için kullanılan alan adları ve bu alan adlarının temsil ettiği IP adresleri DNS Server adı verilen sunucularda tutulmaktadır. Tarayıcı ile DNS sunucusuna bağlanılır ve alan adının temsil ettiği IP adresi bulunarak bu adrese istek gönderilir.

2.1 DNS YAPISI

DNS Yapısı en üstten başlayarak aşağıya doğru inen, hiyerarşik yapıya sahip bir veritabanıdır.



Şekil 1: DNS Hiyerarşik yapısı

DNS sisteminde, root nokta (.) ile gösterilir. Veritabanı üzerindeki her bir alt nokta “domain”; bu domainden kollara ayrılan her bir parça ise “subdomain” olarak adlandırılır. Bir alan adı en alttan root’a gelecek şekilde gösterilir. Şekil 1 incelendiğinde kök sunucudan itibaren başlayarak, hiyerarşik yapı sırasıyla aşağı doğru .com, piyadistramin ve alt olacak şekilde sıralanmıştır. Bu düğümlerin her biri DNS sunucusunda birer dizindir. Bu dosyaların adları en alttan en üste ilerlenecek şekilde birleştirilerek okunur. Şekil 1’ de gösterilen yapıya göre, yukarıdan aşağı, sırasıyla .com, piyadistramin ve alt olarak sıralanmış bu dizinler **alt.piyadistramin.com** olarak okunur ve bu isme **FQDN (Fully Qualified Domain Name- Tam Nitelikli Alan Adı)**denir.

2.1.1 ROOT SUNUCULAR

Alan adı — IP çözümlemesi, ilk olarak root sunucularda başlar. Root sunucular, gelen istekleri, adreslerini bildiği, hiyerarşinin sonraki seviyesi olan TLD (Top-Level Domain) sunucularına yönlendirirler. Dünya üzerinde 13 adet root sunucusu bulunmaktadır. Şekil 2’de bu sunucuların bilgisayar adlarını, IP adreslerini ve yönetildikleri kuruluşları inceleyebilirsiniz

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Şekil 2: DNS Root Sunucuları

2.1.2 ROOT SUNUCULAR

DNS yapısındaki bir sonraki seviye TLD (Top Level Domain-Üst Düzey Alan Adları) sunucularıdır. DNS alan adı uzayında ilk görev paylaşımı, TLD seviyesinde gerçekleşir. TLD

jenerik ve ülke kodlu alan adları olmak üzere ikiye ayrılmaktadır. Jenerik Alan Adları (gTLD — Generic TLD), 20 adettir ve yönetimi InterNIC(Internet Network Information Center- İnternet Ağı Bilgi Merkezi) tarafından yapılmaktadır. Ülke Kodlu Alan Adları (ccTLD- Country Code TLD) ise 248 tanedir ve ISO (International Organization for Standardization) kodları ile tanımlanmıştır. Ülke Kodlu Alan Adları'nın yönetimi ülkelere göre değişiklik göstermektedir. Türkiye bu yönetim ODTÜ tarafındanyapılmaktadır.

Örnek; .gov, .com, .org , .com.tr , .com.it

Resim 3' de belli başlı üst düzey alan adları gösterilmek

com	Ticari Kuruluşlar	tr	Türkiye
org	Ticari Olmayan Kuruluşlar	us	Amerika
mil	Askeri Kurumlar	gb	İngiltere
net	Network (Ağ) Organizasyonları	de	Almanya
edu	Eğitim Kurumları	au	Avustralya
gov	Hükümet Kurumları	fr	Fransa
int	Uluslararası Kurumlar	it	İtalya
info	Bilgi Servisleri	ca	Kanada
name	Bireysel Kullanım	ru	Rusya
tel	İnternet, İletişim Servisleri	es	İspanya

Şekil 3: Belli Başlı TLD Örnekleri

2.1.3 SLD SUNUCULAR

TLD seviyesinden sonraki seviye olan İkinci Seviye Alan Adı (SLD-Second Level Domain) sunucuları, kişilere veya kurumlara verilen farklı uzunluklardaki alan adlarını tutarlar. Bu alan adlarının yönetimi yine ülkelere göre değişiklik göstermektedir ve Türkiye'de ODTÜ tarafından yapılmaktadır.

Örnek; a.com, test.net

2.1.4 ALT ALAN SUNUCULARI

Alt alan adı, alan adına tanımlanmış bir alt alan adıyla, web alanı içerisindeki herhangi bir klasöre direkt olarak ulaşmayı sağlayan bir özelliktir. Örnek olarak; piyadist.com adlı bir web

sitesinin alt alan adı olan alt.piyadist.com adresi, alanda bulunan test klasörüne ulaşmak anlamına gelmektedir. Alt alan adları, alan adı sunucularında tutulur.

2.1.5 ANA BİLGİSAYAR ADI

DNS ağacında bir yaprağa karşı gelen isimler ve kaynak kayıtlarıdır. DNS alan adlandırmasında en sonda yer alırlar. "Sunucu Adı — Host Name" terimi bilgisayar ağlarında bir makine adına karşılık gelir. Bu makine basit bir bilgisayar olabileceği gibi bir ağ yazıcısı, fax makinası, modem, sunucu vb. ağa bağlanabilen herhangi bir araç olabilir. Bu makinaların her birine özgün bir sunucu adı atanabilir. DNS sisteminde ağ üzerindeki makinalar sunucu adı ve alan adı birleşmesiyle adlandırılırlar. FQDN(Fully Qualified Domain Name) denen bu yapıda her alan adı maksimum 63 karakterden oluşabilir ve toplamda da 255 karakteri aşamaz.

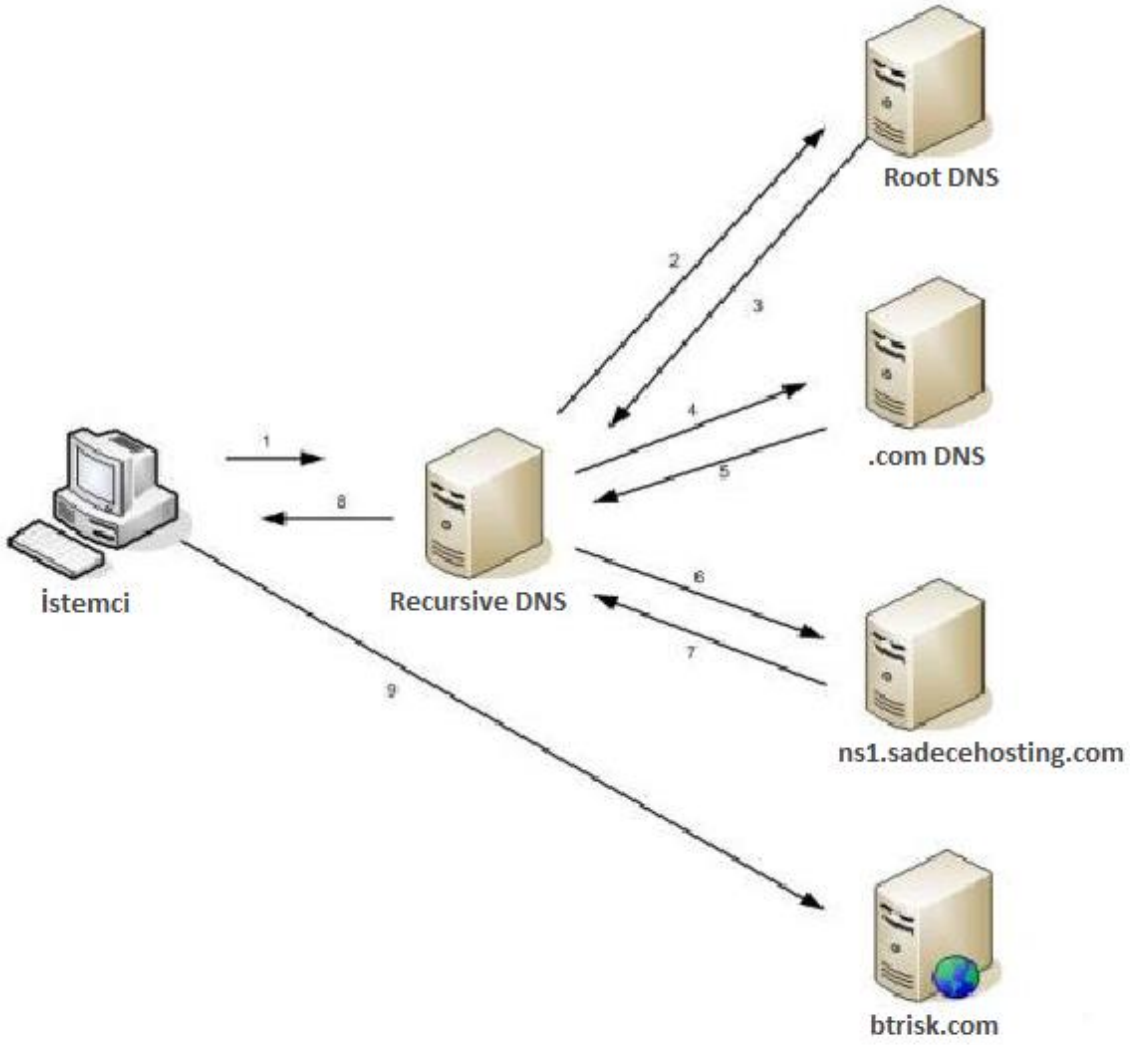
3.DNS İSİM ÇÖZÜMLEMESİ

DNS sunucuları sorumlu olduğu ve de başka yollar ile öğrendiği bütün FQDN'leri ve IP adreslerinin listesini belleğinde saklar. İstemcilerin öğrenmek istediği IP ve FQDN'leri öğrenebilmesi için sorgusunda FQDN/IP, sorgu çeşidini (Kaynak Kaydı(Resource Record)) belirtmesi gerekir.

İstemci tarafından yapılan bir DNS sorgusunun işleyişi şu şekilde gerçekleşir:

1. DNS Name Cache: Önce cache adı verilen önbelleğe bakılır. Eğer erişmek isteyen bilgisayar, sunucuya daha önce eriştiyse bunu cache'de tutar ve burada tuttuğu bilgiyi kullanarak bu bilgisayara erişir. DNS cache'i ipconfig /displaydns komutu ile öğrenilebilir.
2. Host file: C:\Windows\system32\drivers\etc altında bulunan host dosyası notepad ile açılırsa çözülmesi istenen adresin karşılığındaki IP adresinin tutulduğunu göreceksiniz. Bu dosyayı değiştirip adresin istediğiniz IP'ye gitmesini sağlamak mümkündür.
3. Eğer DNS sunucusu sorguyu host dosyasından cevap bulamazsa, belleğinde kayıtlı Root(Kök) DNS sunucularına sorguyu yönlendirir.
4. Kök sunucuları sorguyu ilgili TLD sunucularına yönlendirir.

5. TLD sunucuları sorguyu ilgili sunuculara yönlendirerek istemciye cevap dönülmesi sağlanır.



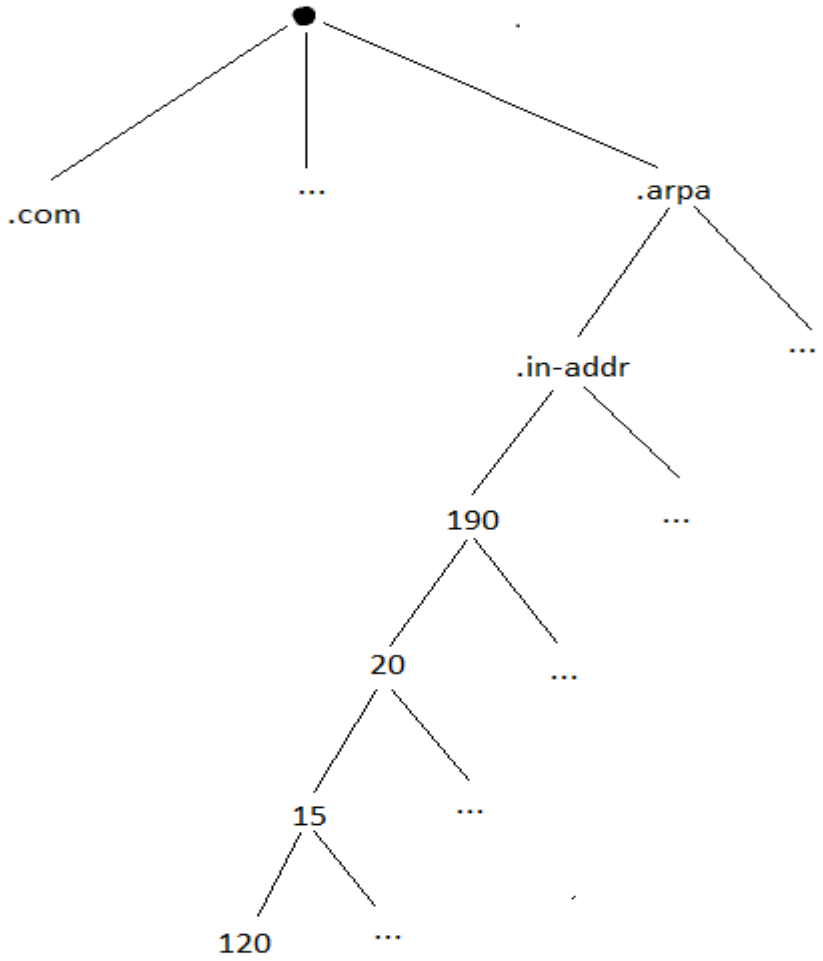
Şekil 4.DNS İsim Çözümleme

4.TERS DNS ÇÖZÜMLEMESİ

Ters DNS Çözümlemesi, DNS çözümlemesinin tersi işlemi olan, IP adresinden alan adı bulma işlemini gerçekleştirir

IP adresleri alan adları gibi birbirine bağımlı değildir. Örneğin; alt.piyadistramin.com alan adı, piyadistramin.com alan adının bir alt alanıdır ve birbirine bağımlıdır. Ama 10.10.10.10 IP

adresi ile 10.10.10.11 IP adresi ile birbirine alan adı açısından bağımlı değildir. Yani 10.10.10.10 IP adresi a.com adlı adresi temsil ederken, 10.10.10.11 IP adresi çok daha farklı olan b.com adlı adresi temsil edebilir. Durum böyle olunca, mantıken bir alan adının IP adresinin bulunması tüm IP adreslerinin incelenmesini gerektirir ve bu ömre bedel bir işlemdir. Fakat bu sorun ARPA tarafından, alan adlarında olduğu gibi IP adreslerinin de hiyerarşik bir yapı alması ile çözülmüştür.



Şekil 5. DNS Alan Adı Çözümlemesi

Şekil 5 ‘ te inceleyecek olursak, hiyerarşik bir yapı görmekteyiz. TLD sunucularına .arpa adlı bir alan eklenmiştir. Bu alanın alt alanı olarak da in-addr eklenmiştir. IP adresleri bulunacağı zaman tıpkı alan adlarının bulunduğu gibi arpa adından başlayarak aşağı doğru ilerler. Bu yapıya göre IP adreslerine ulaşılıp alan adların bulunması işlemi kolaylaştırılmıştır. Dikkat edilmesi gereken başka bir durum ise IP adreslerinin hiyerarşiye göre .in-addr.arpa

adıyla FQDN gibi isimlendirilmesi işlemidir. Şekilde görülen IP 190.15.20.120 iken, hiyerarşiye göre 120.20.15.190.in-addr.arpa olarak adlandırılır.

5. DNS ZONE

DNS zone, DNS sunucularında oluşturulan alan adlarının bilgilerinin tutulduğu dosyalardır. Üst kısımda alan adlarının hiyerarşik yapısı ve her düğümün bir dizini temsil ettiğini söylemiştim. İşte bu dizin bir bölgeyi(zone) temsil eder ve zone olarak adlandırılır.

DNS Zone, Forward Lookup Zone ve Reverse Lookup Zone olarak ikiye ayrılır. Forward Lookup Zone, alan adından IP adresinin bulunması için oluşturulan alanlardır. Reverse Lookup Zone ise tersine, IP adresinin hangi alan adını temsil ettiğinin çözümlenmesi için oluşturulan alanlardır. Forward Lookup Zone ve Reverse Lookup Zone 3 şekilde oluşturulur:

5.1 PRIMARY ZONE (BİRİNCİL BÖLGE)

Yazılabilir, okunabilir ve yönetilebilir zone tipidir. Bu zone tipinde; yeni bir kayıt ekleme, kayıtlar üzerinde değişiklik yapma gibi işlemler yapılabilir.

5.2 SECONDARY ZONE (İKİNCİL BÖLGE)

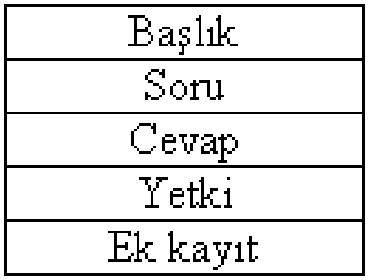
Secondary Zone Primary Zone sunucularından verilerin kopyalanıp, başka bölgede kurulan DNS sunucularına kopyalanması ve yazma, yönetme işlemleri yapılmasına izin verilmeden sadece okuma işlemi yapılması için oluşturulan zone tipidir. Alan adı ve IP adresi çözümlemeleri için uzak konumda bulunan sunucuların sürekli Primary Zone olan DNS sunucularına gitmesi yerine daha yakın konumdaki sunucularla haberleşebilmesi için Secondary Zone kullanılır.

5.3 STUB ZONE

Stub Zone, yardımcı DNS diyebiliriz. En çok aranan isimler burada yer alır. İlk sorgu bu zone tipinde gerçekleşir. Eğer Stub Zone’da aranan isim bulunamazsa Primary veya Secondary Zone’da arama yapılır.

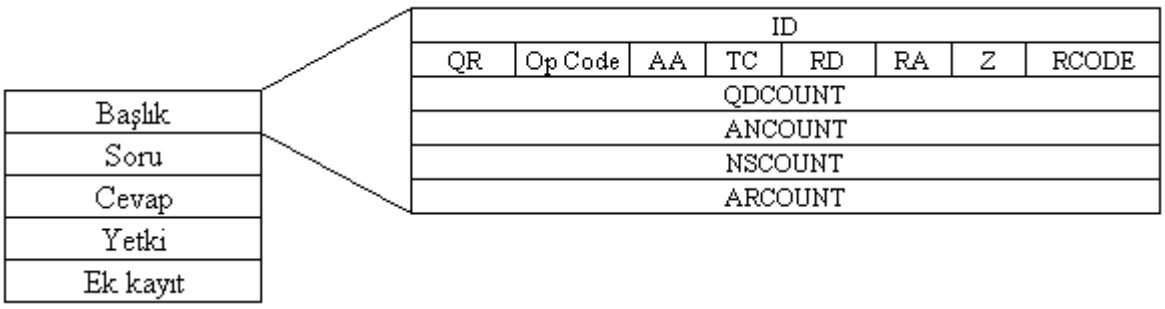
6.DNS MESAJLARI

Şekil 6'da bir DNS mesajının formatı verilmiştir. Mesajlar isim sunucular arasında RR'lerin güncelleştirilmesi için transfer edilir. Netice olarak, mesajın bazı alanları RR formatına benzerdir.



Şekil 6. DNS Mesajının Formatı

Şekilde görüldüğü gibi mesaj beş ana bölümden oluşur. Başlık (ki her zaman bulunur) sorgu ve cevabın doğası ile ilgili alanlar içerir. Soru (question) bölümü isim sunucusuna sorgu gönderilmede kullanılan verileri içerir. Cevap (answer) bölümü soruların cevapları ile yenilenen RR değerlerini içerir. Yetki (authority) bölümü yetkili isim sunucularını işaret eden RR'ler içerir. Ek kayıt (additional record) sorguya asistanlık yapan RR'ler içerir; bu RR'ler özellikle soruların cevapları ile ilgili değildir.



Şekil 7. DNS Mesajının Başlığı

Şekil 7'de başlık bölümünün formatı gösterilmiştir. İlk alan ID alanıdır ve 16-bitten oluşur. Bu tanımlayıcı hem sorguda hem cevapta kullanılır ve ikisinin eşleşmesini sağlar. QR alanı bir bitlik alandır ve mesajın sorgu (0) veya cevap (1) olduğunu belirtir.

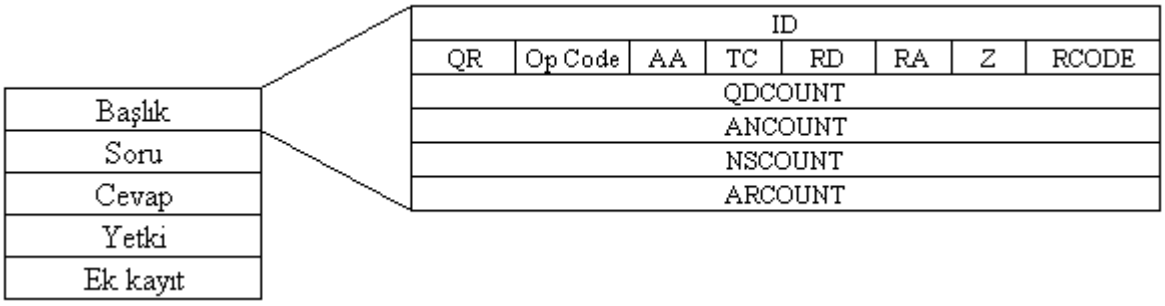
Opcode 4 bitten oluşur. Değerlerinin karşılığı şöyledir: 0 = standart sorgu, 1 = ters sorgu, 2 = sunucu statü isteği ve 3'den 15'e = rezerve edilmiştir.

AA (yetkili cevap) bir cevap için 1 değerine set edilirse cevaplayan isim sunucusunun sorgulanan domain name'i için yetkili olduğunu belirtir. TC (truncation-kesici) 1'e set edilerek mesajın çok uzun olduğu için kesildiği belirtilir. Kesme iletim linkinin izin verdiği veri birimi uzunluğu ile ilgilidir. RD (tekrarlamalı işlem istendi) biti 1'e set edilerek isim sunucusuna bir tekrarlamalı sorgu yap direktifi verilir. RA (tekrarlamalı yapılabilir) biti bir cevap mesajıdır. Eğer isim sunucusu bir tekrarlamalı sorgu yapabilecekse RA ile bunu gösterir. Z alanı üç bittir ve ileride kullanılmak üzere rezerve edilmiştir.

RCODE aşağıdaki değerlere set edilebilen 4 bit içerir:

- 0 = Hiç bir hata oluşmadı
- 1 = Bir format hatası oluştu ve isim sunucu sorguyu anlayamadı.
- 2 = İsim sunucusunda bir sorun var.
- 3 = Sorgudaki domain referansında bir sorun var; sunucu bunu bulamaz.
- 4 = İsim sunucu bu tip sorguyu desteklemiyor.
- 5 = İsim sunucu yönetim veya güvenlik sebebi ile işlem yapmıyor.
- 6'dan 15'e = İleride kullanılmak üzere rezerve edilmiştirler.

QDCOUNT 16-bitten oluşur ve soru bölümündeki girişlerin sayısını belirtir. ANCOUNT 16-bitten oluşur ve cevap bölümündeki RR'lerin sayısını belirtir. NSCOUNT 16-bitten oluşur ve yetkili kayıt bölümündeki sunucu kaynak kayıtlarının sayısını belirtir. ARCOUNT 16-bitten oluşur ve ek kayıt bölümündeki kaynak kayıtlarının sayısını belirler. Bu son dört alan mesajı alan birime, dört alanın sınırlarını nasıl belirleyeceğinin bildirir.



Şekil 8. DNS Mesajının diğer Alanlarının Formatı

Şekil 8'de bu dört bölümün formatı gösterilmiştir. Soru bölümü üç girişten oluşur. Bu bölümün sorgu mesajlarının sorularını taşıdığını söylemiştik. QNAME domain ismini içerir. QTYPE alanı sorgunun tipini belirtir. QCLASS sorgu sınıfını belirtir. Tipik olarak, bu değer Internet için IN olur.

Şekil 8'de görüldüğü gibi DNS mesajının Cevap, Yetki ve Ek Kayıt bölümleri aynı formatı içerirler. Bu formattaki alanlar şöyledir:

- İSİM: Kaynak kaydınca belirtilen domain ismini tanımlar.
- TİP: RR tip kodlarından birini içerir.
- SINIF: RDATA alanında bulunan veri sınıfını belirler.
- TTL: Daha önce öğrendik.
- RD Uzunluğu: Alan uzunluğunu belirtir.
- RDATA: Kaynakla ilgili bilgiyi içerir. İçeriği kaynak kaydının tipi ve sınıfı ile ilgilidir. Örneğin, bir Internet adresi olabilir.

7. DNS KAYIT TÜRLERİ

DNS kayıtları, bir alan adını açıklayan bilgi kümeleridir. DNS kayıtları, zone file olarak bilinen veri dosyalarına dahildir. Bu kayıtları, alan adını yönetebilmek için DNS sağlayıcıları sunar.

7.1. A KAYDI

Adres kaydı ya da kısaltılmış adı ile A kaydı, en temel ve en yaygın olan kayıt türüdür. A kaydı alan adları ile IP adreslerini eşleştirmek için kullanılır. 32 bit olan IPv4 adreslerini alan adları ile eşleştirmek için A kayıt türü kullanılır.

7.2. AAAA KAYDI

AAAA kaydı da A kaydı gibi, alan adı ile IP adreslerini eşleştirmek için kullanılır. Fakat AAAA kaydı, A kaydından farklı olarak 128 bitlik IPv6 adreslerini alan adları ile eşleştirmek için kullanılır.

7.3. ATMA KAYDI

ATM(Asynchronous Transfer Mode) adres kaydıdır. Alan adı alanında geçen DNS adresini atm address alanında geçen ATM adresine eşler.

7.4. CNAME KAYDI

CNAME kaydı, alan adlarını tek bir alan adında birleştirmek ve bir alan adını farklı bir alan adına yönlendirmek için kullanılır. Örneğin; www.piyadistramin.com ve piyadistramin.com alan adlarını CNAME ile www.piyadistramin.com adında birleştirebilir. Aynı zamanda a.com gibi bir alan adına gönderilen istekleri piyadistramin.com'a yönlendirebiliriz.

7.5. HINFO KAYDI

HINFO (Host Information-Ana bilgisayar ismi) bilgisayar bilgileri kaydıdır. Alan adı kısmındaki DNS adresinin bulunduğu bilgisayar üzerindeki işlemci ve işletim sistemlerine ait bilgileri verir.

7.6. ISDN KAYDI

ISDN (Integrated Services Digital Network- Bütünleştirilmiş Sayısal Ağ Hizmetleri) kaydıdır. Alan adını bir telefon numarasına eşler.

7.7. MX KAYDI

Mail sunucularının IP adreslerini tutmak için MX (Mail Exchanger-Posta Değiştirici) kaydı kullanılır. MX kayıtları, e-posta adreslerine gelen e-postaları, e-posta adresi kayıtlarının olduğu sunucuya göndermek için kullanılır. Mailleri mail sunucusuna yönlendirmek için mail sunucusuna ait alan adının A kaydı tanımlanır ve A kaydı ile MX kaydı oluşturulur.

7.8. NS KAYDI

NS (Name Server-İsim Sunucusu) kaydı ile ağ üzerinde bulunan diğer DNS sunucuları tanımlanır ve bu kayıt sayesinde DNS sunucuları arasında haberleşme sağlanır.

7.9 SRV KAYDI

SRV kayıt tipi sunucu tarafından sunulan bir servisin adres, protokol ve port bilgisini döner. **Service**: Hizmetin simgesel adı. Alt çizgi karakteri (_) her zaman hizmet adının başına eklenir.

Protocol (Protokol): İnternet protokolünün simgesel adı; genellikle TCP veya UDP'dir. Alt çizgi karakteri (_) her zaman protokol adının başına eklenir.

Priority (Öncelik) : hedefte belirtilen bilgisayar için öncelik değeri belirtir.

Weight (Ağırlık): Öncelik değeri aynı olan sunucular için yük dengeleme yapmak için kullanılır. Değerleri aynı olan ama birbirinden farklı değere sahip sunucu bilgisayarlar olursa, önce en yüksek değere sahip bilgisayar işleme alınır.

Port (Bağlantı Noktası): Hizmetin TCP veya UDP bağlantı noktasıdır. Bağlantı noktası numarası değeri 0–65535 arası 16 bitlik bir tamsayıdır. Internet Assigned Numbers Authority (IANA — İnternet Atanmış Numaralar Yetkilisi), belirli hizmetlere atanan bağlantı noktası numaralarının resmi listesini tutar.

Target (Hedef): Hizmet alanında belirtilen hizmeti sağlayan sunucunun domain adıdır. Sunucunun SRV kaydıyla aynı etki alanında bulunması gerekmez.

7.10 PTR KAYDI

Bir nevi A kaydının yaptığı işlemin tersini yapar. PTR kaydı, IP adresine ait alan adının kaydını tutmak için kullanılır. Alan adı ile .in-addr.arpa uzantılı IP adresini birbirine eşler.

7.11 SOA KAYDI

Tüm bölgelerdeki ilk kayıttır. Bir DNS sunucusunun sahip olduğu zone'nun kaydını tutar. SOA kayıtları aşağıdaki parametrelerde tutulur.

Serial Number:Seri numarası değerini tutar. Zone transferleri bu numaraya bakılarak yapılır.

Refresh Interval: Secondary Zone DNS sunucusunda, zone bilgisinin yenilenmesi gereken süre belirtilir.

Retry İnterval: Bir şekilde tamamlanamamış zone yenileme denemesinden sonra beklenen süredir.

Expiration: Zone bilgisinin yenilemediği durumlarda, secondary zone'nun yetkilerinin sonlanması için gereken süredir.

Minimum TTL: İkincil sunucunun zone dosyasını önbellekte tutma süresidir

7.12 SPF & TXT KAYDI

SPF kaydı, hangi mail sunucusu üzerinden mail gönderilebileceği kaydını tutar. Örneğin bir sunucuya mail gönderildiğinde, o sunucu o mail adresinin @ işaretinden sonraki alan adı ile IP adres kaydını kendi SPF kayıtlarından kontrol eder. Eğer kendi kayıtlarıyla eşleşme sağlayamazsa SPAM bildirir. Bu SPF kayıtlarını tanımlamak için TXT kaydı kullanılır.

7.13 RP KAYDI

RP (Sorumlu Kişi-Responsible Person) kaydı DNS sunucusunda sorumlu kişinin bilgilerinin tutulması için kullanılır.

8. DNS SORGULAMA

DNS; mail sunucuları, domain isimleri ve IP adresleri gibi bilgileri tutan hiyerarşik bir yapıdır. Bir DNS istemcisi, ad çözümlemesi yapmak için DNS sunucularını sorgular. DNS hizmetleri; kullanıcının girdiği bir DNS adını çözüp, IP adresi gibi o ad ile ilişkili bilgileri oluşturur.

DNS sorgulaması yapmadan önce yapılan bir tarama sonucunda, DNS bilgileri 'name servers(NS)' ya da 'domain servers' olarak görülür. Bu bilgiilerin erişiminden sonra DNS sorgulamasıyla daha fazla bilgiye ulaşılır.

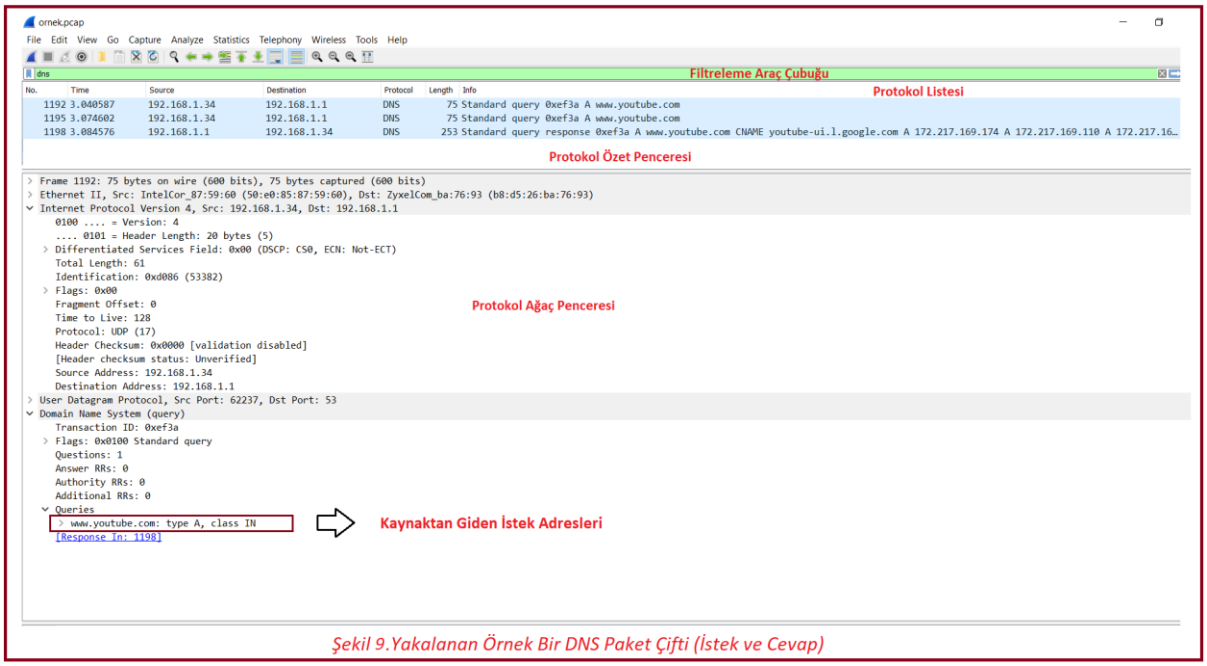
Yanlış yapılandırılmış bir DNS sunucusu sonucunda 'Bölge Transferi(Zone Transfer)' olarak bilinen atak yapılabilir. Bölge transferi ile DNS sorgusu yapılan hedefle ilgili birçok bilgiye ulaşılabilir. Bölge transferi; DNS sunucusunun çalıştığı domain ile ilgili bütün verileri içerir. Bu önemli bilgilerin içinde e-posta sunucusunun ismi, IP adresi, kullanılan işletim sistemi ile ilgili bilgiler vardır.

Bölge transferlerine karşı bir önlem olarak güvenlik duvarında(firewall) veya ağ geçitlerindeki yönlendiricilerde 53 numaralı TCP portu gelen tüm yetkisiz bağlantılara karşı kapalı tutulmalıdır.

DNS sorgulasından bir korunma yöntemi olarak alan adı bir domain değilse, -.tr uzantı ile sonlanmıyorsa 'private domain' haline getirmek bazı tehlikelerden korur. Private domain olan alan adlarında kişisel bilgiler 'Private' halini alır. Yani gerçek bilgiler gizlenir. Ama, private domain her domain sağlayıcıda yoktur.

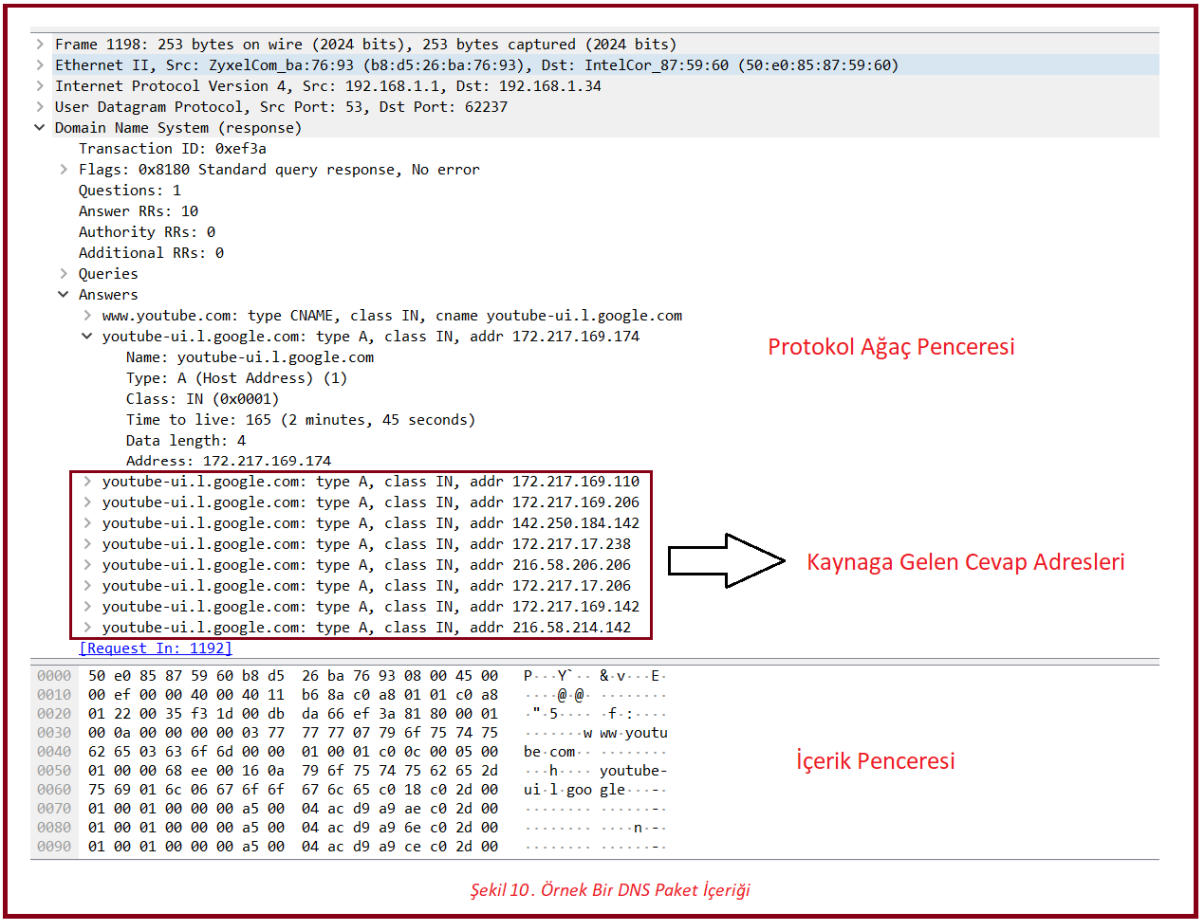
9.WİRESHARK İLE DNS PAKET ANALİZİ

Sekil 9'da görüldüğü gibi Wireshark ile bilgisayar ağ arayüzü dinlenmiş ve DNS paketleri Filtreleme Çubuğuna yazılan "dns" parametresi ile filtrelenmiş ve Sekil 9 daki örnek paketler yakalanmıştır.



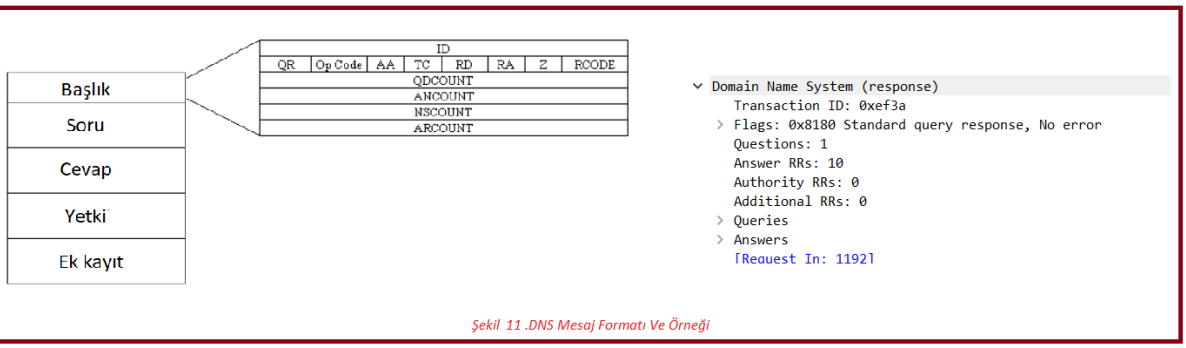
Şekil 9.Yakalanan Örnek Bir DNS Paket Çifti (İstek ve Cevap)

Yukarıda gösterilen paketlerden 1192 istek paketi,1198 numaralı paket ise bu isteğe bir cevap paketidir.Detaylı incelemek gerekirse kullanıcı 192.168.1.34 ip adresinden istediğini gönderiyor . İlk önce bilgisayarımız bu isteğimizi kendisinde tanımlı olan 192.168.1.1 ip adresli DNS sunucuya (Local Name Server) soruyor. Eğer sunucu bu adrese cevap vermeye yetkili değilse, kendisinde kayıtlı kendisinde kayıtlı olan, en üst seviyedeki alan adlarının (Top Level Domain Names) tanımlı olduğu Kök sunuculardan (Root Name Server) birine adresi soruyor. Kök sunucu adrese bakıyor, adresine cevap vermeye kendisi yetkili değil ama .com adreslerine cevap verebilecek sunucuyu biliyor ve sizin DNS sunucunuza bu adresi bildiriyor.Sunucunuz .com alan adlarını tanımlı olduğu sunucuya aynı soruyu soruyor. Cevabi o da bilmiyor ama youtube.com'un adresini biliyor.Sunucunuz, bu kez Youtube`nin DNS sunucusuna aynı soruyu soruyor . Youtube'un sunucusu, Youtube hakkında sorulan sorulara cevap vermeye yetkili olduğu için, sunucu üzerindeki tabloya bakıyor ve www adresinin Ip'sini sizin sunucunuza veriyor.192.168.1.1 ip adresli sunucumuz, gönderilen IP adresini,192.168.1.34 adresine gönderiyor.Bu şekilde istek cevaplanmış oluyor.



Şekil 10. Örnek Bir DNS Paket İçeriği

Paketlerin katman temelli yapısı ve içerikleri yukarıda gösterildiği (Şekil 10) gibi detaylı görüntülenebilir. Protokol ağaç ve protokol içerik pencereleri bu amaçla kullanılabilir. Bu pencerenin amacı protokol özet penceresinde seçili olan paket içeriğini katmanlı ağaç yapısı şeklinde göstermektir. Veri görüntüleme penceresinde ise seçili paket veya alanın bilgilerini onaltılık veya bit düzeyinde gösterir.



Şekil 11 .DNS Mesaj Formatı Ve Örneği

Şekil 11' de görüldüğü gibi mesaj beş ana bölümden oluşur. Başlık (ki her zaman bulunur) sorgu ve cevabın doğası ile ilgili alanlar içerir. Soru (question) bölümü isim sunucusuna

sorgu gönderilmede kullanılan verileri içerir. Cevap (answer) bölümü soruların cevapları ile yenilenen RR değerlerini içerir. Yetki (authority) bölümü yetkili isim sunucularını işaret eden RR'ler içerir. Ek kayıt (additional record) sorguya asistanlık yapan RR'ler içerir; bu RR'ler özellikle soruların cevapları ile ilgili değildir.