



# DHCP'DEN HTTPS'YE

## BEU CYBER TEAM

| Betül YILMAZ | Bayramcan ÖZGÜL | Nisa ÇİBİK |

<https://www.linkedin.com/in/c4nbayram/>

<https://www.linkedin.com/in/nisa-%C3%A7ibik-3a821224a/>

<https://www.linkedin.com/in/bet%C3%BCI-y%C4%B1lmaz-b42807237/>

## Table of Contents

ÖN SÖZ .....	2
DHCP'den TLS'ye .....	3
HAZIRLIK .....	4
IP ADRESİNİN ATANMASI .....	4
DHCP .....	4
IP ADRESİNİN MAC ADRESİ İLE EŞLENMESİ .....	6
ARP .....	6
NAT ÇEVİRME GÖREVİ .....	8
NAT .....	8
SİTEYE İSTEK .....	10
DOMAIN ADINI BİR IP ADRESİNE ÇEVİRME .....	10
DNS .....	10
Nslookup'ı nasıl kullanabilirim? .....	12
SUNUCU İLE GÜVENLİ BİR TCP BAĞLANTISI KURMA .....	15
TCP .....	15
HTTP İSTEĞİ .....	16
HTTP .....	16
HTTPS İSTEĞİ .....	17
HTTPS .....	17
SUNUCUNUN SSL/TSL İLE ŞİFRELİ BİR BAĞLANTI KURMASI .....	18
SSL/TLS .....	18

## ÖN SÖZ

Bu rapor, bir bilgisayarın internete bağlanması ve Google.com'a erişimi sırasında yaşanan olayların detaylı bir analizini sunmaktadır. Eminim ki hepimiz, internete bağlanıp bir web sitesine erişmek için neler olduğunu merak ediyoruzdur. Bu raporumuzda, bu süreci açıklayarak, internet bağlantısı sırasında neler olup bittiğine dair kafanızda bir fikir oluşturmaya çalışacağız.

Rapor, bir bilgisayara internet takıldığında, veri iletimi için hangi ağ cihazlarına bağlandığını, bu cihazların birbirleriyle nasıl etkileşimde bulunduğunu ve sonuç olarak kullanıcının Google.com'a nasıl eriştiğini açıklamaktadır. Bu bilgiler, ağ teknolojileri hakkında daha geniş bir anlayış edinmek isteyenler için de oldukça yararlıdır.

Umarız bu raporumuz, internet teknolojisi hakkında meraklı olanlara, bilgisayarlarından Google.com'a erişim sürecini anlamalarında yardımcı olur.

<https://www.linkedin.com/in/c4nbayram/>

<https://www.linkedin.com/in/nisa-%C3%A7ibik-3a821224a/>

<https://www.linkedin.com/in/bet%C3%BCI-y%C4%Bılmaz-b42807237/>

BİR BİLGİSAYARA İNTERNET BAĞLANIP 'https://google[.]com' ADRESİNE GİRİLDİĞİNDE ARKADA NELER DÖNER VE HANGİ PROTOKOLLER ÇALIŞIR?

## DHCP'den TLS'ye

Hiç merak ettiniz mi, internet bağlantısıyla birlikte gerçekleşen veri transferi sürecinde hangi protokoller kullanılır ve arka planda neler yaşanır?

Öncelikle bir bilgisayar internete bağlandığında adım adım neler yaşanıyor:

1. İlk olarak, bilgisayar internete bağlandığında, Ethernet veya wifi adaptörü bir sinyal işareti algılar.
2. Ethernet veya Wifi bağlanması tamamlanır.
3. Ardından, DHCP sunucusu tarafından bir IP adresi atanır.
4. Sonrasında ARP protokolü IP adresiyle eşleşen bir fiziksel ana bilgisayar veya MAC adresi bulur.

NAT yönlendiricisi IP çevirme işlemini gerçekleştirir. NAT tablosuna bakarak, özel IP adresini genel bir IP adresine çevirir ve bu şekilde dış ağlara ya da İnternete çıkmış olur.

125 3.6643...	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0xde8faa27
132 6.2010...	192.168.1.1	255.255.255.255	DHCP	377 DHCP Offer	- Transaction ID 0xde8faa27
133 6.2030...	0.0.0.0	255.255.255.255	DHCP	364 DHCP Request	- Transaction ID 0xde8faa27
135 6.7210...	192.168.1.1	255.255.255.255	DHCP	377 DHCP ACK	- Transaction ID 0xde8faa27

Daha sonra [https://google\[.\]com](https://google[.]com) eriştiğinizde, aşağıdaki olaylar gerçekleşir:

1. Bilgisayar, okunabilir URL'yi bir IP adresine çevirmek için DNS isteği gönderir.
2. DNS sunucusu, Google'ın sunucusunun IP adresiyle yanıt verir.
3. Bilgisayar, IP adresini kullanarak web sayfası için bir HTTPS isteği gönderir.
4. Bilgisayar, sunucuyla TCP bağlantısı kurar.
5. Güvenli bir bağlantı kurmak için tarayıcı ve sunucu, şifreli bir bağlantı kuran bir SSL/TLS el sıkışması başlatır.
6. Sunucu, tarayıcının kodunu çözdüğü ve işlediği şifrelenmiş HTML içeriğiyle yanıt verir.

# HAZIRLIK

## IP ADRESİNİN ATANMASI

### DHCP

DHCP (Dynamic Host Configuration Protocol), ağdaki aygıtlara IP adresleri ve diğer ağ yapılandırmaları atamak için kullanılan bir ağ protokolüdür.

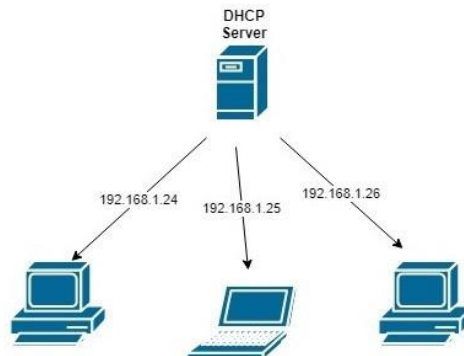
Şu şekilde çalışır:

1. Bir cihaz bir ağa bağlandığında, IP adresi isteyen bir yayın (DHCP DISCOVER) mesajı gönderir.
2. Genellikle bir ağ yönlendiricisinde veya ayrılmış sunucuda bulunan DHCP sunucusu isteği alır.
3. DHCP sunucusu, alt ağ maskesi, varsayılan ağ geçidi bilgileriyle birlikte cihaza ağda benzersiz bir IP adresi (DHCP OFFER) teklif eder.
4. Cihaz, DHCP sunucusunun göndermiş olduğu benzersiz IP adresi teklifini (DHCP REQUEST) kabul eder.
5. DHCP sunucusu gelen DHCP REQUEST talebini (DHCP ACK) mesajı ile tamamlar.

125 3.6643...	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0xde8faa27
132 6.2010...	192.168.1.1	255.255.255.255	DHCP	377 DHCP Offer	- Transaction ID 0xde8faa27
133 6.2030...	0.0.0.0	255.255.255.255	DHCP	364 DHCP Request	- Transaction ID 0xde8faa27
135 6.7210...	192.168.1.1	255.255.255.255	DHCP	377 DHCP ACK	- Transaction ID 0xde8faa27

### Sistem kaydı

```
udhcpd[2435]: Sending OFFER of 192.168.1.163 to (c4:d9:87: )  
udhcpd[2435]: Sending ACK to 192.168.1.163 (c4:d9:87: )
```



DHCP'nin avantajı IP adresleri atama işlemini otomatikleştirmesidir böylece ağ yöneticilerinin her aygıtı manuel bir şekilde yapılandırmaları gerekmez. Ayrıca DHCP sunucusu gerektiğinde IP adreslerini dinamik olarak yeniden atayabildiğinden aygıtlar ağa eklenirken veya ağdan kaldırılırken IP adreslerini yönetmeyi kolaylaştırır.

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x37b9c8b9
0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x37b9c8b9
192.168.1.1	192.168.1.33	DHCP	316	DHCP ACK - Transaction ID 0x37b9c8b9

Resim 1.1

Burada gördüğünüz üzere aygıtı daha önce DHCP tarafından benzersiz bir IP adresi atandığı için (DHCP DISCOVER) ve (DHCP OFFER) adımlarına gerek duyulmamış ve daha önce DHCP tarafından verilen IP kullanılmıştır.

- DHCP REQUEST: Aygıt, sunulan ağ yapılandırmalarını onaylamak ve DHCP sunucusunun sunduğu IP adresini ayırması için DHCP sunucusuna istek iletisi gönderir. / Resim 1.1
- DHCP ACK: Bu mesaj, ağ cihazının istemiş olduğu IP adresi ve ağ yapılandırmalarının sunucu tarafından onaylandığını belirtir. Bu, ağ üzerindeki cihazların eşsiz bir IP adresi olmasını sağlar. / Resim 1.1

**NOT:** DHCP sunucusu aygıtları MAC adresleri ile tanımlar eğer daha önce tanımadığı bir MAC adresi ise yeni ve benzersiz bir IP adresi verir.

...



## IP ADRESİNİN MAC ADRESİ İLE EŞLENMESİ

### ARP

ARP (Address Resolution Protocol), IP adresini ağdaki fiziksel (MAC) bir adresle eşleyen bir ağ protokolüdür.

Bu şekilde çalışır:

1. Bir aygıt aynı ağdaki başka bir aygıtı paket göndermek istediğinde önce ARP önbelleğindeki hedef IP adresini arar.
2. Hedef IP adresi önbellekte bulunmazsa cihaz ağa IP adresiyle ilişkili fiziksel adresini (MAC adresi) isteyen bir ARP yayın iletisi gönderir.
3. Ağdaki tüm cihazlar ARP yayını alır ancak yalnızca eşleşen IP adresine sahip cihaz MAC adresiyle yanıt verir.
4. Mac adres yanıtını alan cihaz MAC adresini gelen kaynak IP adresi ile kendi ARP önbelleğinde saklar.

Resim 1.1 de de görebileceğiniz gibi arp protokolü hedef IP adresini önbellekte arıyor.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.0009...	6c:5b:4c: [redacted]	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.1.1? Tell 192.168.1.82
3	0.0020...	00:02:61: [redacted]	6c:5b:4c: [redacted]	ARP	42	192.168.1.1 is at 00:02:61: [redacted]

Resim 1.1

Resim 1.2 de ise bu arama isteğinin paket içeriği bulunmakta.

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 6c:5b:4c: [redacted]
  Sender IP address: 192.168.1.82
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.1.1
```

Resim 1.2

Resim 1.3 deki paket içeriğinde ise önbellekte bulunan hedef IP adresinin eşleştirildiği MAC adresi bulunmakta.

```
▼ Ethernet II, Src: ZyxelCom_69:25:de (98:0d:67:69:25:de), Dst: Micro-St_f7:9a:a0 (d8:bb:c1:f7:9a:a0)
  > Destination: Micro-St_f7:9a:a0 (d8:bb:c1:f7:9a:a0)
  > Source: ZyxelCom_69:25:de (98:0d:67:69:25:de)
  Type: ARP (0x0806)
  > Trailer: 9aa00000000000001000000000000000000000000000000000000000000000000000
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: ZyxelCom_ [redacted] (98:0d:67: [redacted])
  Sender IP address: 192.168.1. [redacted]
  Target MAC address: Micro-St_ [redacted] (d8:bb:c1: [redacted])
  Target IP address: 192.168.1.33
```

Resim 1.3

```
Interface: 192.168.1.60 --- 0x14
Internet Address      Physical Address      Type
192.168.1.1          00-02-61- [redacted]   dynamic
192.168.1.157        f8-77-b8- [redacted]   dynamic
192.168.1.163        c4-d9-87- [redacted]   dynamic
224.0.0.7            01-00-5e- [redacted]   static
224.0.0.22          01-00-5e- [redacted]   static
224.0.0.251          01-00-5e- [redacted]   static
224.0.0.252          01-00-5e- [redacted]   static
239.255.255.250      01-00-5e- [redacted]   static
255.255.255.255      ff-ff-ff- [redacted]   static
```

Resim 1.4

Resim 1.4 Bu resimde ise cmd üzerinden 'arp -a' komutunu kullanarak aygıtın arp tablosunu görüntüledik.



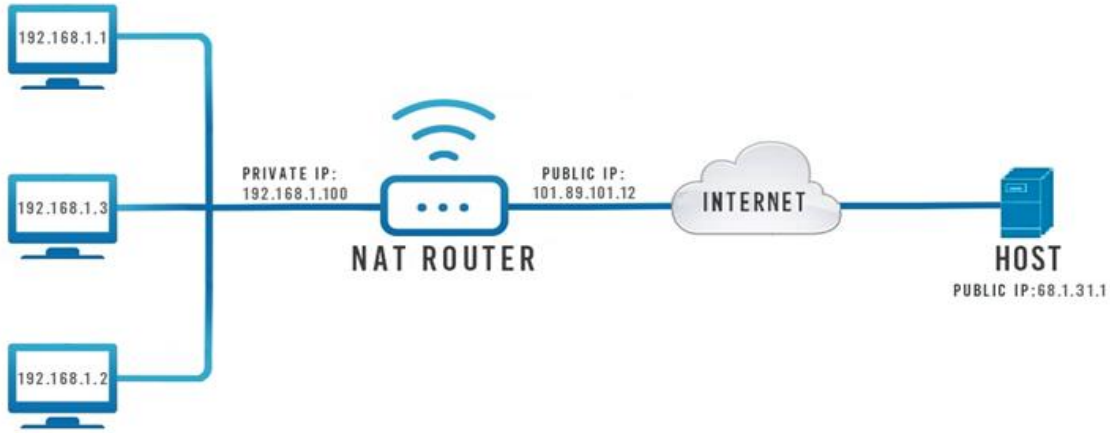
## NAT ÇEVİRME GÖREVİ

### NAT

NAT (Network Address Translation), internet üzerindeki yapılar arasında fiziksel IP adresi sınırlılığını aşmak için ortaya çıkmış bir teknolojidir. Aynı ağ içerisinde bulunan birden fazla cihazın aynı IP'yi kullanarak internete erişebilmesini sağlar.

Oluşturulan iç ağda her cihaza bir IP adresi (private IP) verilir. Ancak bunlar sadece iç ağ iletişimi için geçerlidir. İnternete bağlanırken NAT sahip olduğu gerçek IP (public IP) sayesinde veri alışverişini yapar.

Eğer NAT olmasaydı, ağdaki cihazlar açık ve görünür internet IP adresleri kullanmak zorunda kalacaklardı. IPv4 IP atama kapasitesi hızlı bir şekilde tükenecek ve bu durum ağ güvenliğini sınırlandıracaktı, ağdaki cihazlar ise internet üzerindeki saldırılara açık hale gelecekti.



NAT TABLE		
INSIDE PRIVATE IP:PORT	INSIDE PUBLIC IP:PORT	OUTSIDE PUBLIC IP:PORT
192.168.1.1:9688	101.89.101.12:8801	68.1.31.1:23
192.168.1.2:1253	101.89.101.12:5123	68.1.31.1:23
192.168.1.3:1025	101.89.101.12:102	68.1.31.1:23

NAT adımları şunlardır:

1. Ağdaki bir cihaz internete bağlanmak ister.
2. Yönlendirici üzerindeki NAT servisi, cihazın bağlantı isteğini alır.
3. İç ağdaki bir cihaz, internete bir veri paketi gönderir. NAT servisi, gönderilen bu veri paketinin kaynağı olan private IP adresini değiştirir ve router'ın kendi paylaşılan internet IP adresi olan public IP adresini kullanır.
4. Değiştirilmiş bu veri paketi, internet üzerinden hedef cihaza gönderilir.
5. Hedef cihaz, veri paketini alır ve cevap olarak bir veri paketi gönderir.
6. NAT servisi, gelen veri paketinin hedef IP adresini tekrar private IP adresine çevirir ve orijinal istemciye gönderir.
7. İç ağdaki istemci, veri paketini alır ve işlem tamamlanmış olur.

BU ADIMLAR, YÖNLENDİRİCİ NAT SERVİSİ TARAFINDAN OTOMATİK OLARAK YAPILIR VE KULLANICININ MANUEL OLARAK YAPMASI GEREKMEZ.

...

# SİTEYE İSTEK

## DOMAIN ADINI BİR IP ADRESİNE ÇEVİRME

### DNS

İnternet ortamındaki her birim IP adresleri ile tanımlıdır ancak insanların bu kadar çok IP adresini akılda tutması mümkün değildir. Bu sorunu çözmek için de alan adı sistemi oluşturulmuş ve sistemde çalışan DNS sunucuları ile sorun ortadan kaldırılmıştır.

DNS adımları şu şekildedir:

1. Kullanıcı bir domain adı yazdığında (örneğin www.google.com), bilgisayar tarafından bu domain adının IP adresine dönüştürülmesi istenir.
2. İlk olarak bilgisayarın yerel DNS ön belleği kontrol edilir. Eğer istenen bilgi burada varsa kullanılır.
3. Eğer yerel DNS ön belleğinde bilgi yoksa, istemci, yerel DNS sunucusuna (genellikle İnternet Servis Sağlayıcısı tarafından sağlanan) bir DNS isteği gönderir.
4. Yerel DNS sunucusu, ön belleğinde belirli bir domain adının çözümlenmiş bir IP adresi var mı kontrol eder.
5. Eğer ön bellekte IP adresi yoksa, yerel DNS sunucusu diğer DNS sunucularına sorgu yapar ve belirli bir domain adının IP adresini çözmeye çalışır.
6. İstemeyi karşılayan DNS sunucusu, belirli bir domain adının IP adresini bulur ve bu bilgiyi yerel DNS sunucusuna geri gönderir.
7. Yerel DNS sunucusu, istemciye belirli bir domain adının çözümlenmiş IP adresini geri gönderir.
8. Bulunan IP adresi kullanıcının bilgisayarına gönderilir ve kullanıcı istenen web sitesine erişebilir.
9. Bulunan IP adresi yerel DNS ön belleğine kaydedilir ve tekrar istenildiğinde buradan hızlı bir şekilde kullanılabilir.

Source	Destination	Protocol	Length	Info
192.168.1.33	192.168.1.1	DNS	74	Standard query 0x55a3 A www.google.com
192.168.1.1	192.168.1.33	DNS	90	Standard query response 0x55a3 A www.google.com A 216.239.38.120
192.168.1.33	192.168.1.1	DNS	74	Standard query 0xba94 A www.google.com
192.168.1.33	192.168.1.1	DNS	74	Standard query 0x682e HTTPS www.google.com
192.168.1.1	192.168.1.33	DNS	90	Standard query response 0xba94 A www.google.com A 216.239.38.120

Resim 1.4

Resim 1.4 de ise bu adımların WİRESHARK ile analiz görüntüsü alınmıştır.

Domain Name System (query)

Transaction ID: 0xa9a5

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

discord.com: type A, class IN

Name: discord.com

[Name Length: 11]

[Label Count: 2]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

discord.com: type A, class IN, addr 162.159.136.232

discord.com: type A, class IN, addr 162.159.128.233

discord.com: type A, class IN, addr 162.159.135.232

discord.com: type A, class IN, addr 162.159.138.232

discord.com: type A, class IN, addr 162.159.137.232

Name: discord.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 59 (59 seconds)

Data length: 4

Address: 162.159.137.232

Resim 1.5

Resim 1.5 de yapılan analizin paket içeriği görüntülenmekte.

Bahsedilen DNS önbelleginin içeriğini görüntülemek istersek;/Resim 1.6

```

C:\Users\asinc>ipconfig /displaydns

Windows IP Configuration

sentry.io
-----
Record Name . . . . . : sentry.io
Record Type . . . . . : 1
Time To Live . . . . . : 2582
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 35.188.42.15

sslwidget.criteo.com
-----
Record Name . . . . . : sslwidget.criteo.com
Record Type . . . . . : 5
Time To Live . . . . . : 21
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : widget.par.vip.prod.criteo.com

```

Resim 1.6

Cmd aracılığıyla "ipconfig /displaydns" komutunu kullanmak yeterli olacaktır.

Peki bir alan adının IP adresini öğrenmek veyahut farklı işlemler için neler yapabiliriz buna bir göz atalım;

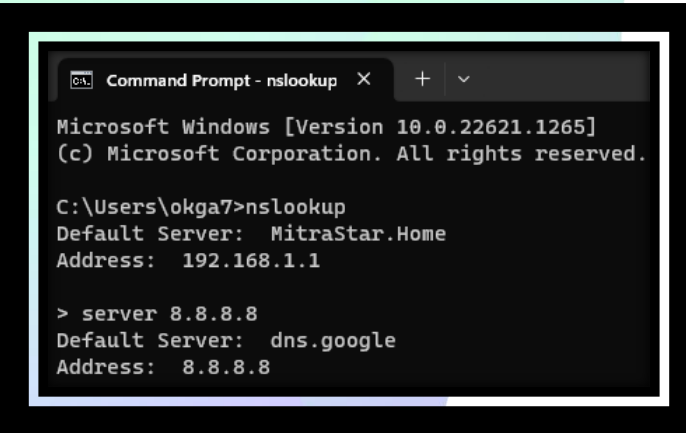
Öncelikle alan adını IP adresine çevirme işlemini yapan ya da farklı işlevleri olan birçok site bulunmakta fakat biz en güvenli yöntemlerden biri olan ve kendi sistemimizden erişebildiğimiz NSLookup aracını inceleyeceğiz.

### Nslookup’ı nasıl kullanabilirim?

İlk olarak komut istemcisini açmalıyız ardından ‘nslookup’ yazarak aracımızın içine gireceğiz.

Nslookup aracının farklı kullanımları ve parametreleri var bunlara bir göz gezdirelim;

- server: Bu parametre, sorguların hangi DNS sunucusuna yönlendirileceğini belirlemek için kullanılır. /Resim 1.7



```
Command Prompt - nslookup X + v
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\okga7>nslookup
Default Server:  MitraStar.Home
Address:  192.168.1.1

> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8
```

Resim 1.7

- set: NSLOOKUP aracı için çeşitli ayarları yapmamızı sağlar ve bu parametre bir çok komutu içinde barındırır bunlardan bahsedecek olursak;

“set type=mx”

MX (Mail Exchanger) girilen alan adına ait mail adreslerinin çalıştığı mail sunucularını adresleyen DNS kayıtlarıdır.

Resim 1.8 de google.com için bir sorgu yaptık fakat herhangi bir kayıt bulunamadı.

```
> set type=mx
> google.com
Server: myhome.mynet
Address: 192.168.1.1

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com
```

Resim 1.8

“set type=ns”

NS (Name Server) girilen alan adının sorgulanmasında kullanılan isim sunucularıdır IP adresine göre sorgulama yapar ve IP adresinin bulunduğu sunucuyu size sunar.

Resim 1.9 da Google.com için alan adı sorgulaması yaptık ve bize IP adresinin bulunduğu sunucu bilgilerini verdi.

```
> set type=ns
> google.com
Server: myhome.mynet
Address: 192.168.1.1

Non-authoritative answer:
google.com      nameserver = ns3.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
```

Resim 1.9

“set type=a”

A kaydı, bir alan adının IP adresine çözümlendiği kayıttır.Yani, ‘set type=a’ komutunu kullanarak nslookup ile bir alan adının hangi IP adresine çözümlendiğini öğrenebilirsiniz.

Resim 2.0 da ise google.com alan adının A kayıtlarını sorguladık.

```
> set type=a
> google.com
Server:  MitraStar.Home
Address:  192.168.1.1

Non-authoritative answer:
Name:     google.com
Address:  216.239.38.120
```

Resim 2.0

“set debug”

Ayrıntılı çıktılar için hata ayıklama modunu açar.

“set timeout=10”

Cevap beklenirken geçen süreyi belirler.

“set domain=google.com”

Varsayılan DNS bölgesini belirler.

“set all”

Tüm sorgu sonuçlarını listeler. /Resim 2.1

“set recurse”

Yaptığımız sorunun yanıtını alana kadar tekrarlar.

‘HELP’ VEYA ‘-?’ NSLOOKUP ARACININ KULLANIMI HAKKINDA YARDIM  
BİLGİLERİNİ GÖRÜNTÜLER.

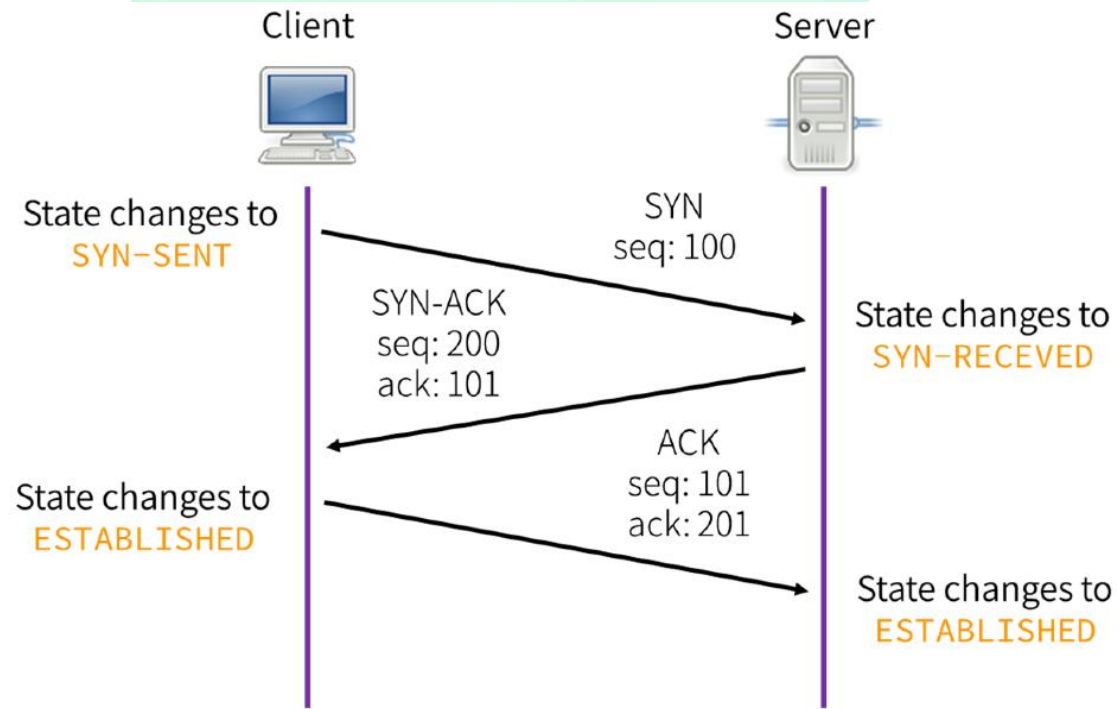


## SUNUCU İLE GÜVENLİ BİR TCP BAĞLANTISI KURMA

### TCP

TCP (Transmission Control Protocol) bilgisayarlar arasındaki iletişimin, küçük paketler hâlinde ve kayıpsız olarak gerçekleştirilmesini sağlayan bir protokoldür. Aslında TCP protokolünün en önemli özelliği kimlik doğrulaması yapması ve veriyi karşı tarafa gönderirken veya alırken verinin bütünlüğünü sağlamasıdır. Gelişmiş bilgisayar ağlarında ortaya çıkan kayıpları önlemek için TCP protokolü yazılmıştır. **HTTP, HTTPS, POP3, SSH, SMTP, TELNET ve FTP** gibi günlük hayatta sıkça kullandığımız protokollerin veri iletimi TCP vasıtasıyla yapılır.

Bir TCP bağlantısı yapılırken üçlü el sıkışma adı verilen (3-Way Handshake) işlemi gerçekleştirilir. / Resim 2.1



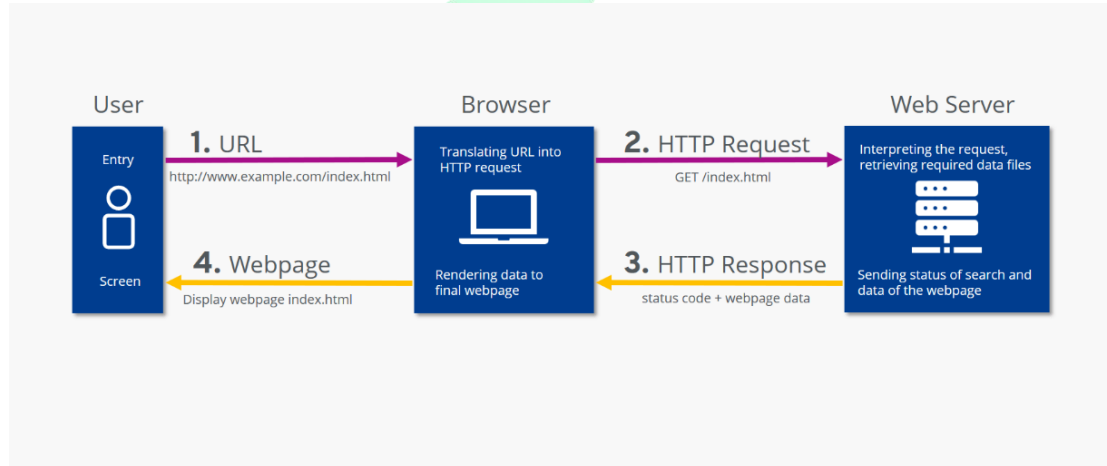
Resim 2.1

## HTTP İSTEĞİ

### HTTP

HTTP (Hypertext Transfer Protocol), internet üzerinden veri iletmek için kullanılan bir iletişim protokolüdür. İnternetteki web sayfalarını ve diğer içerikleri görüntülemek için bir web sunucusundan bir web tarayıcısına veri aktarmak için kullanılır.

HTTP istek/yanıt (request/response) modeli şu adımlardan oluşur:



1. Kullanıcı, tarayıcısından bir web adresi girer (örneğin `http://www.google.com`).
2. Tarayıcı, girilen web adresindeki verilere erişmek için bir HTTP isteği oluşturur ve sunucuya gönderir.
3. Web sunucusu, tarayıcının gönderdiği HTTP isteğini alır ve işler.
4. Sunucu, isteğe uygun bir HTTP yanıtı oluşturur. Yanıt, sunucunun isteği nasıl işlediğini ve sunucunun yanıt verme durumunu belirtir (örneğin, 200 OK durum kodu).
5. Sunucu, tarayıcıya HTTP yanıtını gönderir.
6. Tarayıcı, sunucudan gelen yanıtı alır ve tarayıcı tarafından istenen web sayfasını görüntüler.

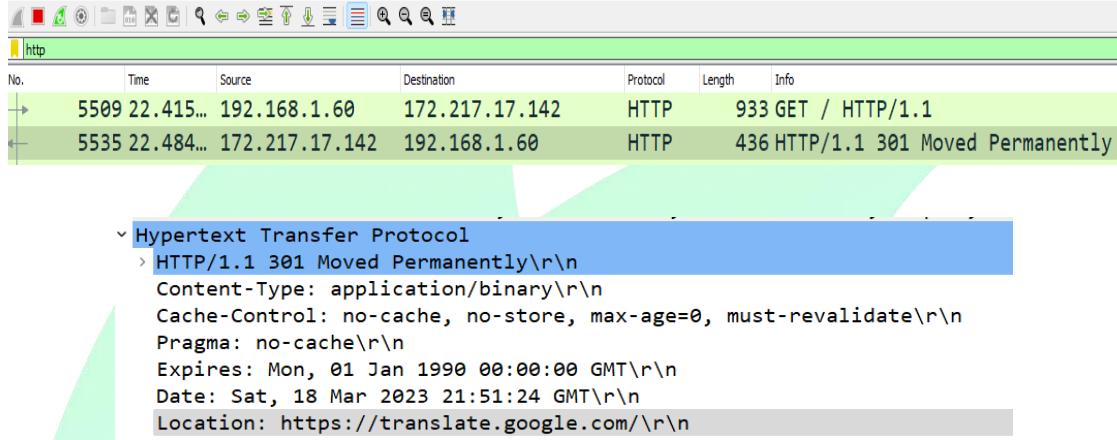
Bu adımlar bir HTTP isteğinin nasıl yapıldığını açıklar. Her bir web sayfasının yüklenmesi için tekrar tekrar yapılır ve her bir HTTP isteği/yanıtı eşlemesi, tarayıcı ve sunucu arasındaki veri alışverişini yönetir.

**Eğer sunucu HTTP yerine HTTPS kullanıyorsa paketi 443 portuna yönlendirir ve tls el sıkışması başlar.**

## HTTPS İSTEĞİ

### HTTPS

Çoğu web sunucusu, HTTPS protokolü kullanarak iletişim kurmayı tercih eder. Bu nedenle, bir kullanıcı HTTP protokolü kullanarak bir istekte bulunduğunda, web sunucusu tarafından bir yönlendirme yapılır ve kullanıcının HTTPS protokolü kullanarak tekrar istekte bulunması istenir. Bu yönlendirme, kullanıcının iletişim kurmak için HTTPS protokolünü kullanmasını sağlar ve daha güvenli bir bağlantı sağlar.



No.	Time	Source	Destination	Protocol	Length	Info
5509	22.415...	192.168.1.60	172.217.17.142	HTTP	933	GET / HTTP/1.1
5535	22.484...	172.217.17.142	192.168.1.60	HTTP	436	HTTP/1.1 301 Moved Permanently

▼ Hypertext Transfer Protocol

- HTTP/1.1 301 Moved Permanently\r\n
- Content-Type: application/binary\r\n
- Cache-Control: no-cache, no-store, max-age=0, must-revalidate\r\n
- Pragma: no-cache\r\n
- Expires: Mon, 01 Jan 1990 00:00:00 GMT\r\n
- Date: Sat, 18 Mar 2023 21:51:24 GMT\r\n
- Location: https://translate.google.com/\r\n

HTTPS (Hypertext Transfer Protocol Secure), internet üzerinde verilerin güvenli bir şekilde transfer edilmesini sağlamak için SSL/TLS tarafından şifrelenerek kullanılan bir protokoldür ve aşağıdaki adımları içermektedir:

1. Bağlantı kurma: Tarama isteği gönderilen tarayıcı, web sunucusuyla güvenli bir bağlantı kurar.
2. SSL/TLS handshake: Tarayıcı ve web sunucusu, birbirlerine güvenli bir şekilde bağlantı kurmak için SSL/TLS protokolüne göre bir "handshake" işlemi yaparlar. Bu işlem, tarayıcının web sunucusunun SSL/TLS sertifikasını doğrulamasını ve anahtar değişimini içerir.
3. Veri şifreleme: Tarayıcı, web sunucusundan istek gönderir ve veriler şifreli olarak gönderilir.
4. Veri gönderme: Şifreli veriler, web sunucusundan tarayıcıya güvenli bir şekilde gönderilir.
5. Veri çözme: Tarayıcı, aldığı şifreli verileri çözer ve kullanıcıya görüntüler.



## SUNUCUNUN SSL/TSL İLE ŞİFRELİ BİR BAĞLANTI KURMASI

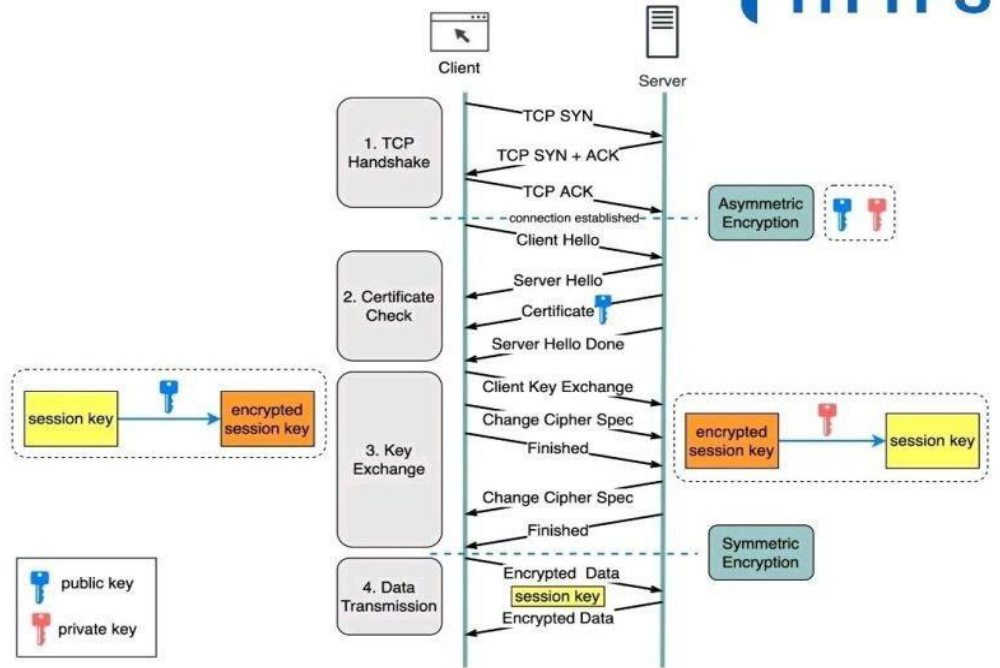
### SSL/TLS

TLS(Secure Sockets Layer) ve TLS (Transport Layer Security), internet üzerinde verilerin güvenli bir şekilde transfer edilmesini sağlamaya yarayan şifreleme protokolleridir.

SSL, eski bir şifreleme protokolüdür ve 1999 yılında yerini TLS almıştır. Ancak, hala "SSL" terimi kullanılır ve anlaşılır.

TLS, verilerin şifrenmesi ve doğrulaması gibi özellikleri barındırır ve SSL'e göre daha güvenli ve güncel bir teknolojidir.

### How does HTTPS Work?



TCP bağlantısı olduktan sonra:

192.168.1.60	85.111.38.82	TCP	66 24932 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
85.111.38.82	192.168.1.60	TCP	54 443 → 24900 [ACK] Seq=1 Ack=2 Win=49152 Len=0
85.111.38.82	192.168.1.60	TCP	54 443 → 24904 [ACK] Seq=1 Ack=2 Win=22016 Len=0
85.111.38.82	192.168.1.60	TCP	66 443 → 24931 [SYN, ACK] Seq=0 Ack=1 Win=14520 Len=0 M
192.168.1.60	85.111.38.82	TCP	54 24931 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0

TLS için temelde 4 aşamadan söz edebiliriz:

### Sertifika Kontrolü:

İstemci tarayıcıya bir "istemci merhaba" ve bununla birlikte 17 tane şifre paketi içeren şifre paketleri gönderir. Bununla birlikte Sunucu bir "sunucu merhabası" ile yanıt verir. Sunucu TLS sertifikasının içerdiği ve gönderilen şifre paketlerinden birini seçer ortak anahtarlar (Public Key) birlikte TLS sertifikasının bir kopyasını tarayıcıya gönderir Tarayıcı sunucudan gelen anahtarı ve TLS sertifikasını kontrol eder. Anahtarın doğruluğunu, sertifikanın süresinin dolup dolmadığını ve o web siteye ait olup olmadığını kontrol eder.

478 3.8153...	192.168.1.60	85.111.38.82	TLSv1...	571 Client Hello
Transmission Control Protocol, Src Port: 24931, Dst Port: 443, Seq: 1, Ack: 1, Len: 517				
Transport Layer Security				
TLSv1.2 Record Layer: Handshake Protocol: Client Hello				
Content Type: Handshake (22)				
Version: TLS 1.0 (0x0301)				
Length: 512				
Handshake Protocol: Client Hello				
Handshake Type: Client Hello (1)				
Length: 508				
Version: TLS 1.2 (0x0303)				
Random: 678d628c1545c5c41019db4690d27439f81f9d176c4787c5b29da4c07aa320ef				
Session ID Length: 32				
Session ID: 479223a1b35d204616bd43cd91f14c533e022bfcf5163e35c76a522a369a612a				
Cipher Suites Length: 34				
Cipher Suites (17 suites)				
Cipher Suite: Reserved (GREASE) (0x4a4a)				
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)				
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)				
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)				
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)				
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)				
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)				

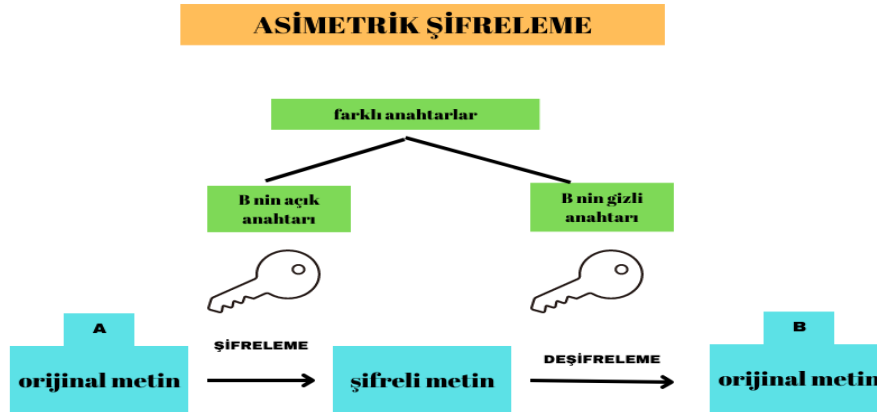
```

489 3.8380... 85.111.38.82 192.168.1.60 TLSv1... 1502 Server Hello
> Frame 489: 1502 bytes on wire (12016 bits), 1502 bytes captured (12016 bits) on interface
> Ethernet II, Src: [redacted]
> Internet Protocol [redacted]
> Transmission Control Protocol, Src Port: 443, Dst Port: 24931, Seq: 1, Ack: 518, Len: 1448
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 80
  > Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 76
    Version: TLS 1.2 (0x0303)
  > Random: ca99e2d1145c2ac213e7906e926baa1e3024182d6807f118a0108842a1ca3e1b
    Session ID Length: 32
    Session ID: f14fec40fdc5db3a91fd6a075a91e7d03af565056b64aff11c6eb0a5fba1eea9
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)

```

### Asimetrik şifreleme:

Farklı bir anahtar çifti kullanarak şifreleme ve çözme işlemlerini gerçekleştiren şifreleme yöntemidir. Bu anahtar çifti, biri özel anahtar (private key) ve diğeri ise genel anahtar (public key) olarak adlandırılır. Genel anahtar herkese açık bir şekilde paylaşılabılırken, özel anahtar sadece anahtar sahibi tarafından bilinir.



### Anahtar Değişimi:

TLS sertifikasını doğruladıktan sonra, istemci bir oturum anahtarı oluşturur ve public key'i kullanarak şifreler. Sunucu şifrelenmiş oturum anahtarını alır ve private key ile şifresini

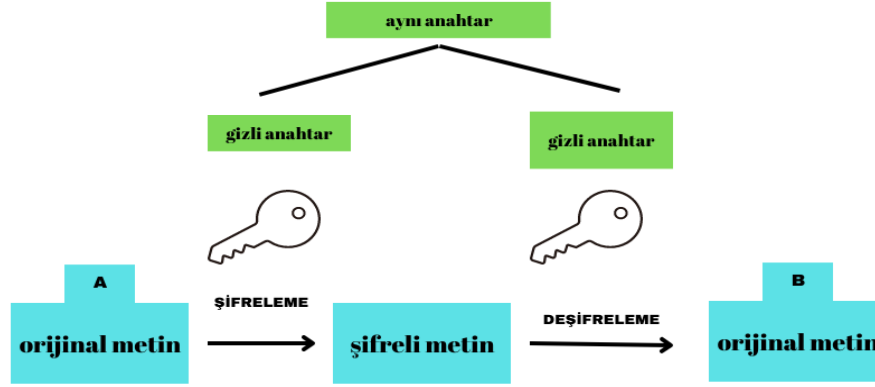
çözer. Artık hem istemci hem de sunucu aynı oturum anahtarına (simetrik şifreleme) sahip olduğundan, şifrelenmiş veriler güvenli bir çift yönlü kanalda iletilir.

The image displays two Wireshark packet captures related to a TLSv1.2 handshake. The top packet (Frame 493) is a 'Server Key Exchange' message. It shows the 'Handshake Protocol' section with details like 'Handshake Type: Server Key Exchange (12)', 'Length: 329', and 'EC Diffie-Hellman Server Params'. The 'Pubkey' is highlighted with a red box. The bottom packet (Frame 495) is a 'Client Key Exchange' message. It shows the 'Handshake Protocol' section with details like 'Handshake Type: Client Key Exchange (16)', 'Length: 66', and 'EC Diffie-Hellman Client Params'. The 'Client Key Exchange' section is highlighted with a red box. Both packets are part of a TLSv1.2 session between 192.168.1.60 and 85.111.38.82. The interface shows the 'Transport Layer Security' protocol tree on the left and the packet details on the right.

Simetrik Şifreleme, verilerin şifrelenmesinde kullanılır ve aynı anahtarın hem şifreleme hem de şifre çözme işlemleri için kullanıldığı bir şifreleme türüdür. Bu yöntemde verilerin şifrelenmesinde kullanılan anahtar verilerin çözülmesinde de kullanılır.



## SİMETRİK ŞİFRELEME



### Veri Aktarımı:

Gizli anahtar güvenli bir şekilde yerleştirildiğinde istemci ve sunucu artık şifreleme kullanarak güvenli bir şekilde bilgi alışverişinde bulunabilir. İstemci ve sunucu arasında iletilen tüm veriler, gizli anahtar kullanılarak şifrelenir ve şifresi çözülür.

BU ADIMLAR, TARAMA ESNASINDA VERİLERİN GÜVENLİ BİR ŞEKİLDE TRANSFER EDİLMESİNİ SAĞLAR VE VERİ GÜVENLİĞİNİN BOZULMASINI ÖNLER. BU NEDENLE, İNTERNET ÜZERİNDE GÜVENLİ BİR TARAMA YAPMAK İSTEYEN KULLANICILAR İÇİN HTTPS KULLANIMI ÖNERİLİR.

– Teşekkürler