دستور کار سری 4

عرفان رفیعی اسکویی - 98243027

بخش اول)

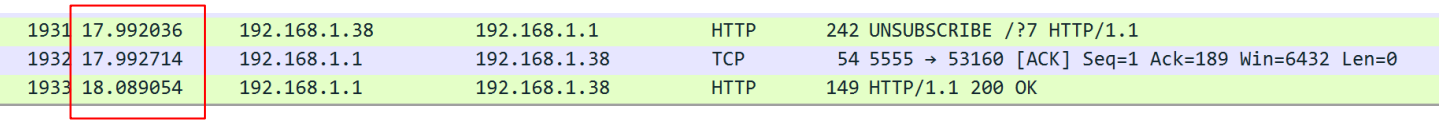
1)

پروتکل ها :

TCP SSL SSDP MDNS LLMNR IGMPv3 ICMPv6 HTTP DNS ARP

TLSv1.3 TLSv1.2

2) زمان ارسال تا ok :



1931	17.992036	192.168.1.38	192.168.1.1	HTTP	242 UNSUBSCRIBE /?7 HTTP/1.1
1932	17.992714	192.168.1.1	192.168.1.38	TCP	54 5555 → 53160 [ACK] Seq=1 Ack=189 Win=6432 Len=0
1933	18.089054	192.168.1.1	192.168.1.38	HTTP	149 HTTP/1.1 200 OK

3) اولین پروتکلی که فعال میشود DNS است.

خروجی سیستم از DNS query به آدرس IP سرور DNS در ماشین محلی یا شبکه می رود. این آدرس IP متعلق به سرور DNS است که معمولاً توسط یک ارائه دهنده خدمات اینترنتی (ISP) یا یک سازمان نگهداری می شود.

هنگامی که سرور DNS query را دریافت کرد، یا با آدرس IP دامنه درخواستی پاسخ می دهد یا اگر اطلاعات لازم را نداشته باشد، درخواست را به سرور DNS دیگری ارسال می کند. سپس کامپیوتر از آدرس IP برای برقراری ارتباط با وب سرور میزبان وب سایت استفاده می کند.

بخش دوم)

1) همانطور که در عکس مشخص است مرورگر نسخه http 1 را اجرا میکند :

http

No.	Time	Source	Destination	Protocol	Length	Info
1442	9.260823	192.168.1.38	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
1445	9.261635	192.168.1.38	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
1448	9.414844	13.107.4.52	192.168.1.38	HTTP	593	HTTP/1.1 200 OK (text/plain)
1453	9.419528	13.107.4.52	192.168.1.38	HTTP	593	HTTP/1.1 200 OK (text/plain)
1636	44.778740	192.168.1.38	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
1639	44.780530	192.168.1.38	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
1648	44.928589	13.107.4.52	192.168.1.38	HTTP	593	HTTP/1.1 200 OK (text/plain)
1653	44.934555	13.107.4.52	192.168.1.38	HTTP	593	HTTP/1.1 200 OK (text/plain)

2) در شکل زیر ادرس ip کامپیوتر source و ادرس ip مقصد destination هست :

Source	Destination	Protocol
192.168.1.38	13.107.4.52	HTTP

3) و 4)

```
> Hypertext Transfer Protocol
```

```
v Transmission Control Protocol, Src Port: 57148, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
    Source Port: 57148
    Destination Port: 80
```

5)

درWireshark ، status code در پاسخ HTTP به کد سه رقمی ارسال شده توسط سرور برای نشان دادن وضعیت درخواست مشتری اشاره دارد. این status code ها به پنج کلاس گروه بندی می شوند که هر کلاس نشان دهنده نوع متفاوتی از پاسخ است. این پنج کلاس عبارتند از:

1xx : پاسخ های اطلاعاتی (به عنوان مثال، 100 ادامه)

2xx : پاسخ‌های موفق) مثلاً 200(OK

3xx : پیام های تغییر مسیر (به عنوان مثال، 301 به طور دائم منتقل شده است)

4xx : خطاهای مشتری (به عنوان مثال، 404 یافت نشد)

5xx : خطاهای سرور (به عنوان مثال، 500 خطای داخلی سرور)

کد وضعیت معمولاً در خط اول هدر پاسخ HTTP به همراه نسخه پروتکل HTTP استفاده شده یافت می شود. در مثال ما خروجی اینگونه است :

```
HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
     [HTTP/1.1 200 OK\r\n]
     [Severity level: Chat]
     [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
```

در این مثال، کد وضعیت 200 است که نشان می دهد سرور با موفقیت درخواست مشتری را انجام داده است.

بخش سوم)

1) به وسیله TCP فرستاده شده اند.

2)

```
User Datagram Protocol, Src Port: 64751, Dst Port: 53
```

این پورت 53 است که مربوط به سرویس زیر است :

Port(s)	Protocol	Service
53	tcp,udp	DNS

3) ادرس ip مقصد :

```
fe80::1          DNS        96 Standard query 0x7f20 A www.varzesh3.com
```

4)

```
Queries
  www.varzesh3.com: type HTTPS, class IN
      Name: www.varzesh3.com
      [Name Length: 16]
      [Label Count: 3]
      Type: HTTPS (HTTPS Specific Service Endpoints) (65)
      Class: IN (0x0001)
  [Response In: 529]
```

5) بله مثلا به عنوان مثال یک ویدیو در سایت بود که query به این صورت آن را نشان داده:

```
DNS        99 Standard query 0xf4d2 HTTPS static2.farakav.com
DNS       103 Standard query 0x3916 A video-vcdn.varzesh3.com
DNS       103 Standard query 0x9e0f HTTPS video-vcdn.varzesh3.com
```

بخش چهارم)

1) دستور :

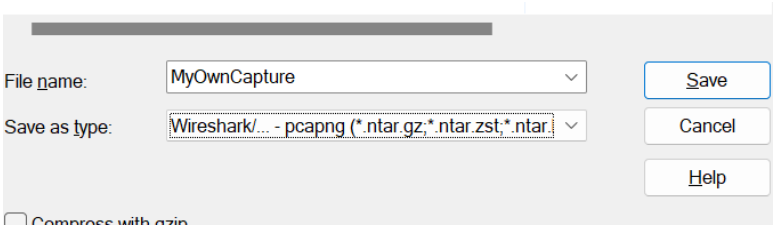
```
C:\Users\efnos>ping www.google.com

Pinging www.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=63ms TTL=110
Reply from 216.239.38.120: bytes=32 time=62ms TTL=110
Reply from 216.239.38.120: bytes=32 time=63ms TTL=110
Reply from 216.239.38.120: bytes=32 time=62ms TTL=110

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 63ms, Average = 62ms

C:\Users\efnos>
```

نتیجه :

119	10.091961	192.168.1.38	216.239.38.120	ICMP	74 Echo (ping) request id=0x0001, seq=3316/62476, ttl=128 (reply in 120)
120	10.154094	216.239.38.120	192.168.1.38	ICMP	74 Echo (ping) reply id=0x0001, seq=3316/62476, ttl=110 (request in 119)
121	14.232435	fe80::1	fe80::f139:42ba:d86…	ICMPv6	86 Neighbor Solicitation for fe80::f139:42ba:d86e:b991 from e4:18:6b:db:51:88
122	14.232539	fe80::f139:42ba:d86…	fe80::1	ICMPv6	86 Neighbor Advertisement fe80::f139:42ba:d86e:b991 (sol, ovr) is at 90:e8:68:41:4f:6f

2) پروتکل icmp فعال میشود.

3)



4)

مورد خواسته شده را انجام داده و save میکنیم.