WIRESHARK

WHAT IS HTTP?

Hypertext Transfer Protocol: It is a text-based protocol used when communicating with websites.

Communicating with a website, when a website is entered (for example: http://example.com), the browser sends a request to that site. This request goes to the server where that site is located over the internet.

This communication takes place over the HTTP protocol. In other words, it can be thought of as a regular spoken language.

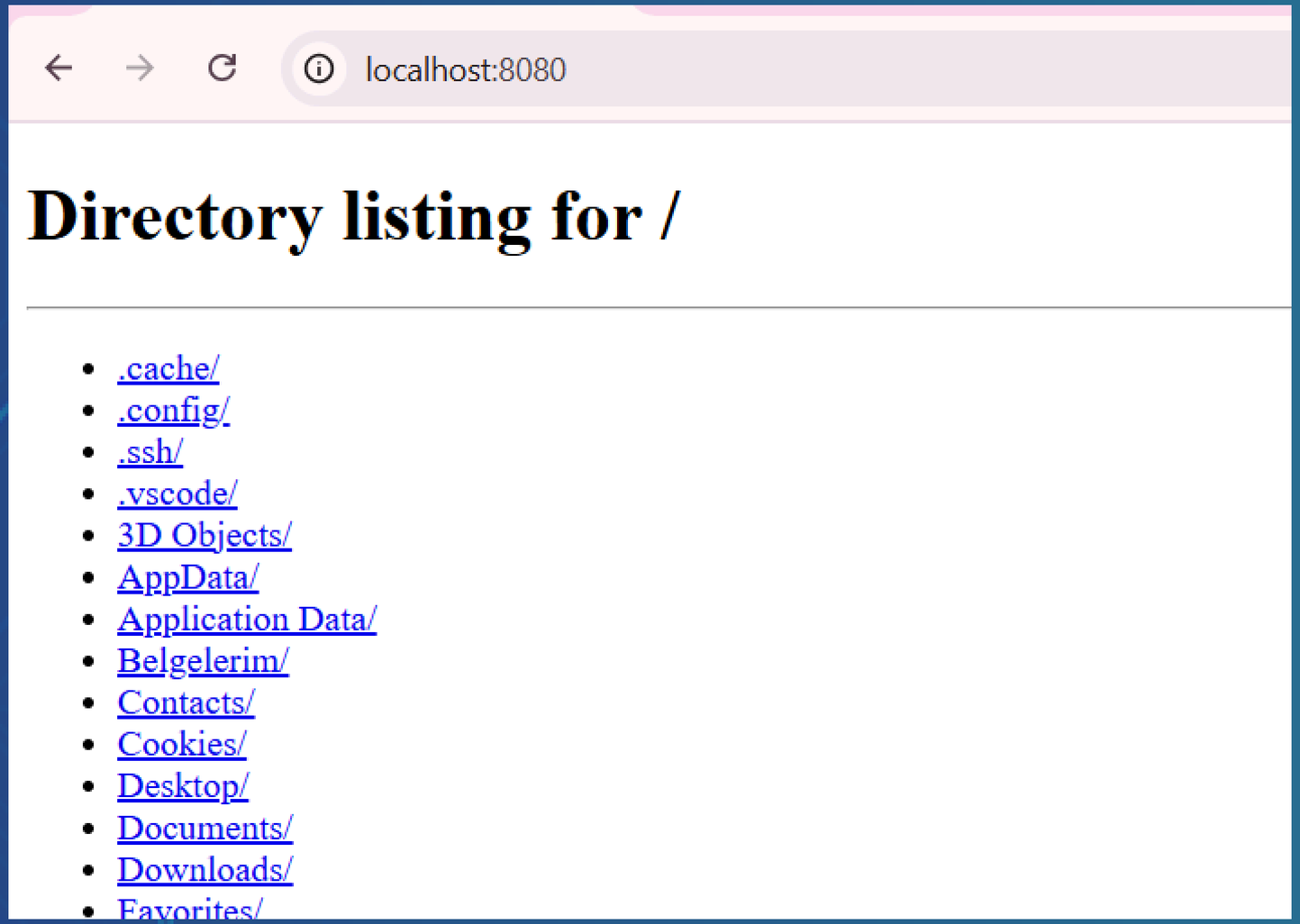
Unlike HTTPS, it does not include encryption.

WİRESHARK İLE DOSYA ELE GEÇİRME (HTTP ÜZERİNDEN)

Localde, 8080 portunda bir sunucu başlatmak için;

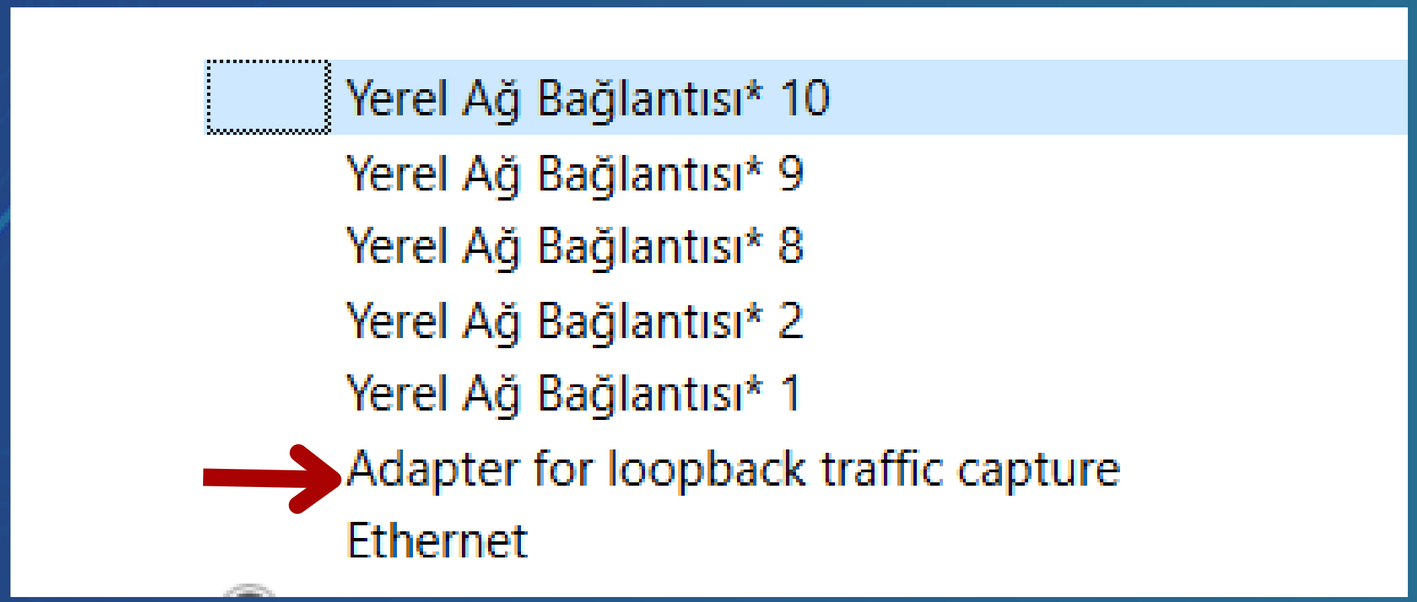
```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Melek> python -m http.server 8080
Serving HTTP on :: port 8080 (http://[::]:8080/) ...
```

When we type “localhost:8080” into the browser, we should encounter a screen like the one below.



WİRESHARK SİDE

To monitor traffic via Wireshark, we select the “Adapter for loopback capture” interface.



WİRESHARK SİDE

The connection was established and the client requested the page from the server. And the server returned the page.

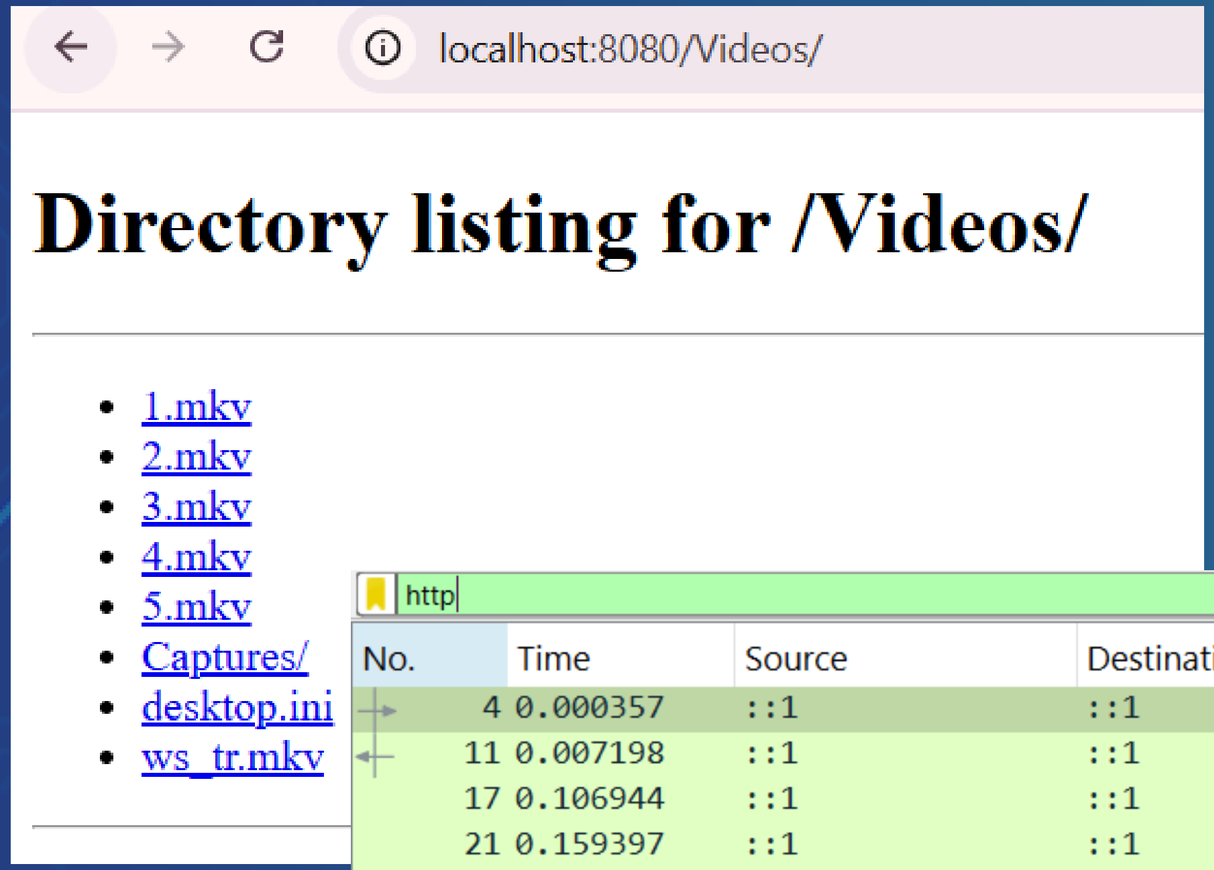
Source	Destination	Protocc	Length	Info
::1	::1	TCP	76	50581 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
::1	::1	TCP	76	8080 → 50581 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
::1	::1	TCP	64	50581 → 8080 [ACK] Seq=1 Ack=1 Win=2618880 Len=0
::1	::1	HTTP	749	GET / HTTP/1.1
::1	::1	TCP	64	8080 → 50581 [ACK] Seq=1 Ack=686 Win=2618880 Len=0
::1	::1	TCP	76	50582 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
::1	::1	TCP	76	8080 → 50582 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
::1	::1	TCP	64	50582 → 8080 [ACK] Seq=1 Ack=1 Win=2618880 Len=0
::1	::1	TCP	220	8080 → 50581 [PSH, ACK] Seq=1 Ack=686 Win=2618880 Len=156 [TCP PDU reassembled in 11]
::1	::1	TCP	64	50581 → 8080 [ACK] Seq=686 Ack=157 Win=2618624 Len=0
::1	::1	HTTP	2436	HTTP/1.0 200 OK (text/html)

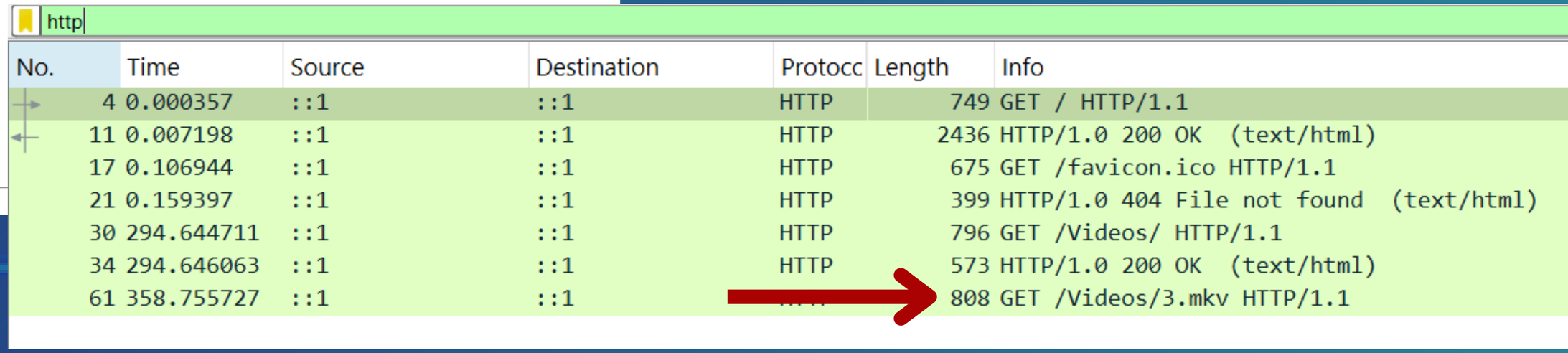
It can be examined by HTTP filtering.

http

No.	Time	Source	Destination	Protocc	Length	Info
4	0.000357	::1	::1	HTTP	749	GET / HTTP/1.1
11	0.007198	::1	::1	HTTP	2436	HTTP/1.0 200 OK (text/html)
17	0.106944	::1	::1	HTTP	675	GET /favicon.ico HTTP/1.1
21	0.159397	::1	::1	HTTP	399	HTTP/1.0 404 File not found (text/html)

We download any video by going to the videos section in the server section and we will capture it via Wireshark.





To download the video via Wireshark, we first stop the capture, select the video and click save. After saving, the video will be downloaded.