

Bilgi Toplama

Necmettin ÇARKACI – Ahmet Alperen BULUT

Biz kimiz

İstihbarat Çeşitleri

Pasif Bilgi Toplama

- Hedef sistemden bağımsız

Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek

Aktif Bilgi Toplama

Traceroute

- ⌚ Traceroute bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösteren programdır.

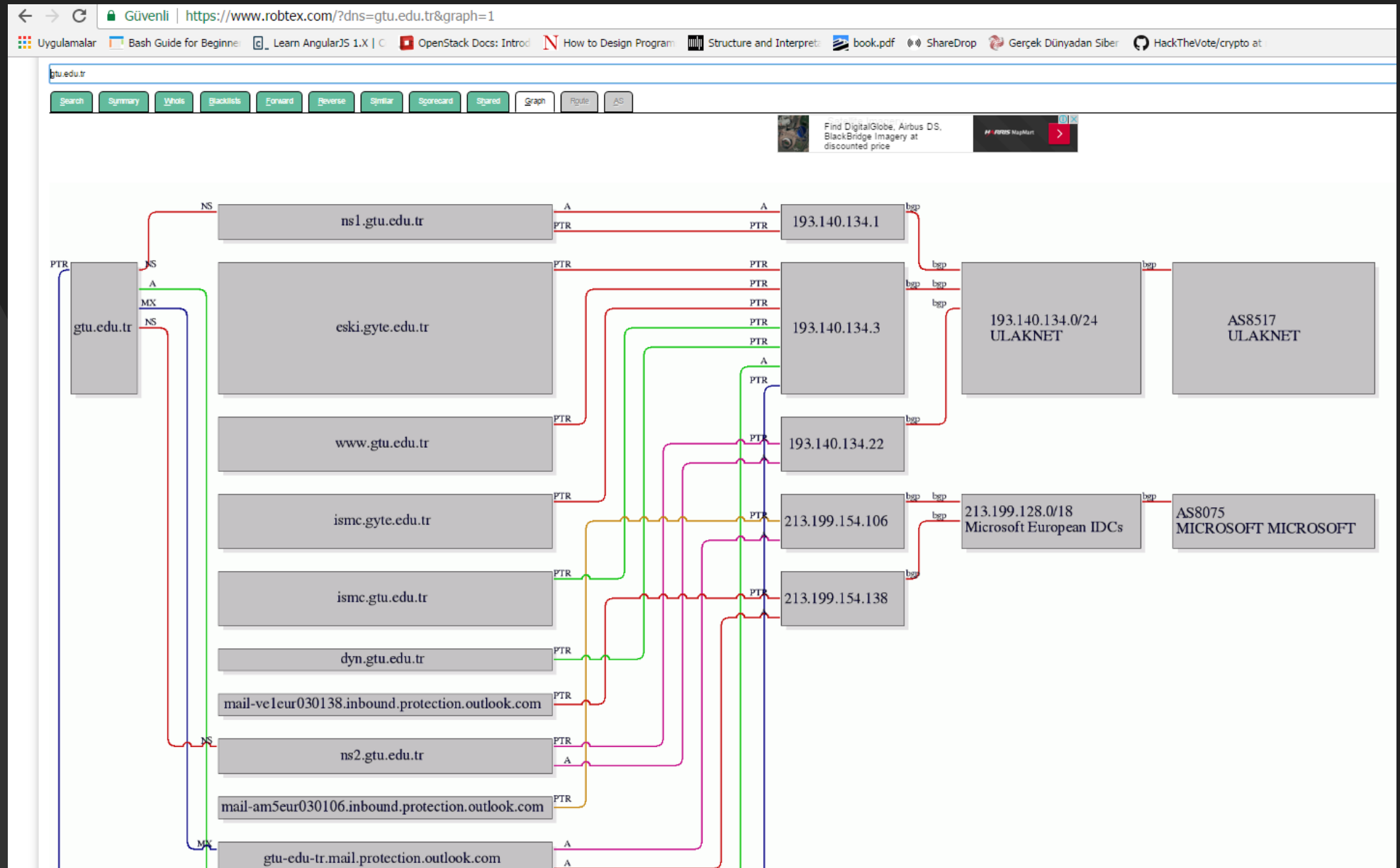
Dig

- ⌚ Detaylı DNS sorgulaması yapan gelişmiş bir araçtır.

Dirbuster

- ⌚ Hedef adresin alt dizinlerini bulmak için kullanılır.

Robtex



Wireshark

Ralink Technology Inc. (Microsoft's Packet Scheduler) : Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:

Current Wireless Interface: None 802.11 Channel: FC5 Filter: Decryption Mode: Wireless Settings... Decryption Keys...

No.	Time	Source	Destination *	Protocol	Info
56	6.565943	192.168.1.2	80.93.212.86	TCP	1857 > http [FIN, ACK] Seq=8 Ack=29686 win=63556 Len=0
55	6.527297	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=29686 win=63556 Len=0
53	6.521441	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=28981 win=64260 Len=0
50	6.498083	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=26461 win=64260 Len=0
48	6.486681	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=25201 win=64260 Len=0
45	6.463445	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=22681 win=64260 Len=0
43	6.452057	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=21421 win=64260 Len=0
40	6.428705	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=18901 win=64260 Len=0
38	6.416944	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=17641 win=64260 Len=0
35	6.393781	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=15121 win=64260 Len=0
33	6.382065	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=13861 win=64260 Len=0
30	6.359078	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=11341 win=64260 Len=0

Genel Protokol Bilgisi

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 80.93.212.86 (80.93.212.86)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 - 00.. = ECN-Capable Transport (ECT): 0
 - 00.. = ECN-CE: 0
- Total Length: 40
- Identification: 0x31a2 (12706)
- Flags: 0x04 (Don't Fragment)
 - 0... = Reserved bit: Not set
 - 1... = Don't fragment: Set
 - ..0. = More fragments: Not set
- Fragment offset: 0
- Time to live: 222
- Protocol: TCP (0x06)
- Header checksum: 0x84cf [correct]
 - [Good: True]
 - [Bad: False]
- Source: 192.168.1.2 (192.168.1.2)
- Destination: 80.93.212.86 (80.93.212.86)

Protokol Detayı

Transmission Control Protocol, Src Port: 1857 (1857), Dst Port: http (80), Seq: 8, Ack: 29686, Len: 0

- Source port: 1857 (1857)
- Destination port: http (80)
- Sequence number: 8 (relative sequence number)
- Acknowledgement number: 29686 (relative ack number)
- Header length: 20 bytes
- Flags: 0x11 (FIN, ACK)
 - 0... .. = Congestion window Reduced (CWR): Not set
 - ..0. = ECN-Echo: Not set
 - ..0. = Urgent: Not set
 - ...1 = Acknowledgment: Set
 - 0... .. = Push: Not set

Wireshark: Capture from Ralink Technolo...

Captured Packets

Total	% of total
57	100,0%
SCTP	0 0,0%
TCP	57 100,0%
UDP	0 0,0%
ICMP	0 0,0%
ARP	0 0,0%
OSPF	0 0,0%
GRE	0 0,0%
NetBIOS	0 0,0%
IPX	0 0,0%
VINES	0 0,0%
Other	0 0,0%

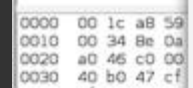
Running 00:01:20

Help Stop

Don't fragment (ip.flags.df), 1 byte

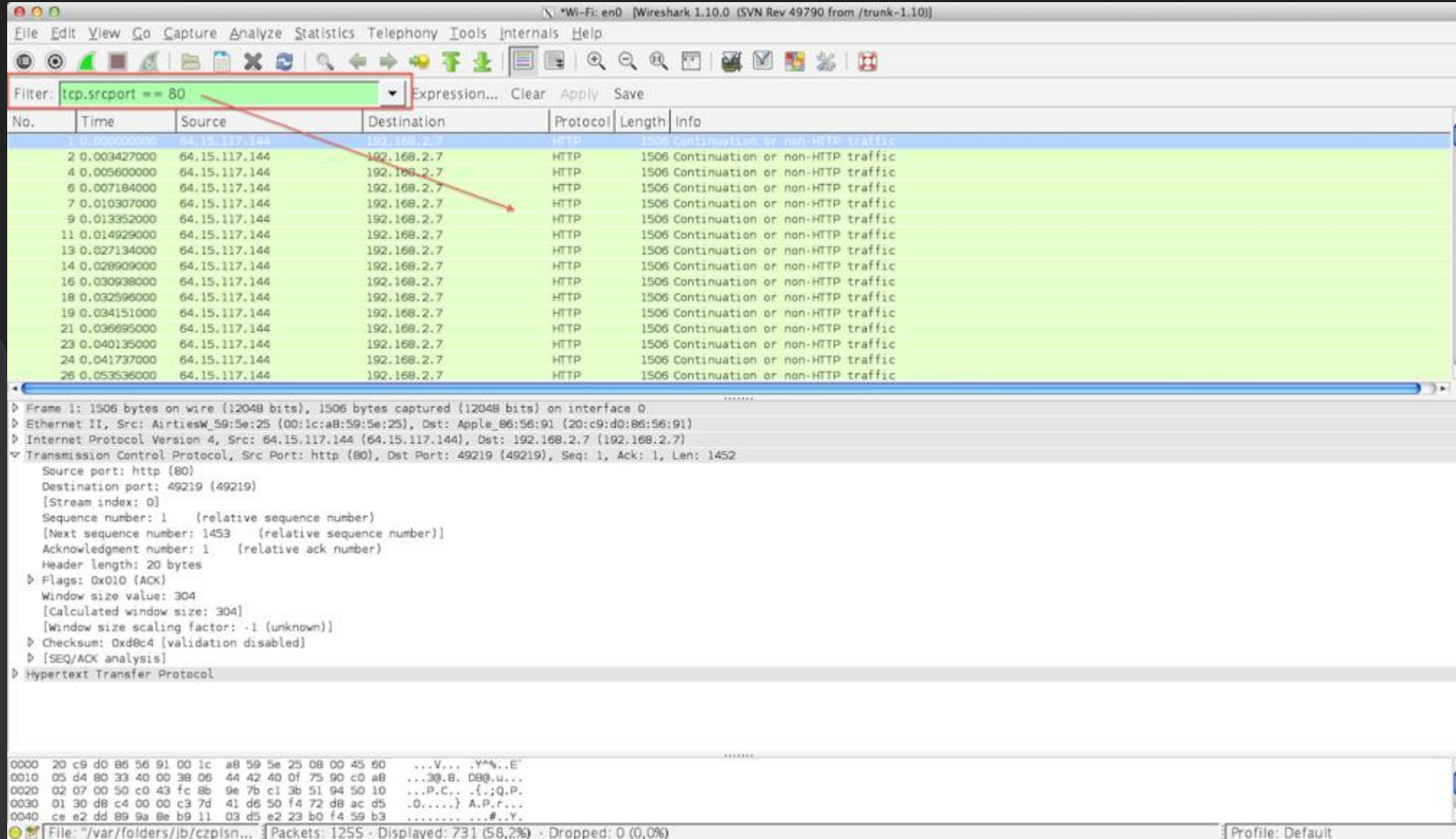
P: 57 D: 57 M: 0

Wireshark



Display Filter: Yakalanan paketlerin içerisinde istenilen özelliklerdeki paketlerin ayıklanması kısmında kullanılabilir.

Wireshark



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window is divided into three panes. The top pane shows a list of captured packets, with a display filter of 'tcp.srcport == 80' applied. The filter is highlighted with a red box, and a red arrow points from it to the 'tcp' column of the first packet. The packet list shows 26 packets, all of which are HTTP continuation requests from 64.15.117.144 to 192.168.2.7. The middle pane shows the details of the selected packet (Frame 1), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
2	0.003427000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
4	0.005600000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
6	0.007184000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
7	0.010307000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
9	0.013352000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
11	0.014929000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
13	0.027134000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
14	0.028909000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
16	0.030938000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
18	0.032596000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
19	0.034151000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
21	0.036695000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
23	0.040135000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
24	0.041737000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
26	0.053536000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic

Frame 1: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface 0
Ethernet II, Src: AirtiesW_59:5e:25 (00:1c:a8:59:5e:25), Dst: Apple_86:56:91 (20:c9:d0:86:56:91)
Internet Protocol Version 4, Src: 64.15.117.144 (64.15.117.144), Dst: 192.168.2.7 (192.168.2.7)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49219 (49219), Seq: 1, Ack: 1, Len: 1452
Source port: http (80)
Destination port: 49219 (49219)
[Stream index: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1453 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x010 (ACK)
Window size value: 304
[Calculated window size: 304]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xd8c4 [validation disabled]
[SEQ/ACK analysis]
Hypertext Transfer Protocol

0000 20 c9 d0 86 56 91 00 1c a8 59 5e 25 08 00 45 60 ...V...Y%..E
0010 05 d4 80 33 40 00 38 06 44 42 40 0f 75 90 c0 a8 ...38.B. D80.u...
0020 02 07 00 50 c0 43 fc 8b 9e 7b c1 3b 51 94 50 10 ...P.C...{:;Q.P.
0030 01 30 d8 c4 00 00 c3 7d 41 d6 50 f4 72 d8 ac d5 .0.....} A.P.r...
0040 ce e2 dd 89 9a 8e b9 11 03 d5 e2 23 b0 f4 59 b3#..Y..

File: "/var/folders/jb/czplsn... Packets: 1255 · Displayed: 731 (58,2%) · Dropped: 0 (0,0%) Profile: Default

Kelime arama : İzlenen trafik içerisinde kelime arama;

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main packet list on the left shows a series of packets. Packet 264 is highlighted, showing it is a DNS Standard query response from 192.168.2.7 to 8.8.8.8. The packet details pane on the right shows the structure of this DNS response, including the transaction ID (0xa2a2) and the query name (berbergokmen.com). A search dialog box titled 'Wireshark: Find Packet' is open in the center, with the search criteria set to 'String' and the search text 'berbergokmen'. The search results show that the word 'berbergokmen' is found in the packet bytes of packet 264. The status bar at the bottom indicates that 9872 packets are displayed out of 9872 captured.

No.	Time	Source	Destination	Protocol	Length	Info
257	4.504274000	192.168.2.7	173.194.39.206	TLSv1	107	Encrypted Handshake Message
258	4.504451000	192.168.2.7	173.194.39.206	TLSv1	1203	Application Data
259	4.537153000	173.194.39.206	192.168.2.7	TCP	66	https > 49714 [ACK] Seq=134 Ack=226 Win=42368 Len=0 TSval=1573130431 TSecr=871760693
260	4.590256000	173.194.39.206	192.168.2.7	TCP	66	https > 49714 [ACK] Seq=134 Ack=1363 Win=42304 Len=0 TSval=1573130485 TSecr=871760693
261	4.606608000	173.194.39.206	192.168.2.7	TLSv1	505	Application Data
262	4.606756000	192.168.2.7	173.194.39.206	TCP	66	49714 > https [ACK] Seq=1363 Ack=573 Win=131296 Len=0 TSval=871760794 TSecr=1573130500
263	4.870551000	Apple_86:56:91	Broadcast	ARP	42	Who has 6.6.6.254? Tell 6.6.6.113
264	4.893195000	192.168.2.7	8.8.8.8	DNS	76	Standard query response 0xa2a2 A berbergokmen.com
265	5.005994000	8.8.8.8	192.168.2.7	DNS	62	Standard query response 0xa2a2 A 178.210.160.70
266	5.006572000	192.168.2.7	178.210.160.70	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
267	5.016842000	178.210.160.70	192.168.2.7	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
268	5.017051000	192.168.2.7	178.210.160.70	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
269	5.019271000	192.168.2.7	178.210.160.70	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
270	5.037164000	178.210.160.70	192.168.2.7	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
271	5.062309000	178.210.160.70	192.168.2.7	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1

Wireshark: Find Packet

Find:

By: ☐ Display filter ☐ Hex value ☒ String

Filter: ☒ Filter: berbergokmen

Search In:

☐ Packet list ☐ Packet details ☒ Packet bytes

String Options:

☐ Case sensitive

Character width:

Direction: ☐ Up ☒ Down

Help Cancel Find

Query Name (dns.qry.name),... Packets: 9872 · Displayed: 9872 (100,0%) · Dropped: 0 (0,0%) Profile: Default

Protokol detayı : Protokol detaylarının gösterilmesi. Özellikle DDOS saldırılarında saldırı tipini belirlemek için kullanılır.

Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A red box highlights the 'Protocol Hierarchy Statistics' window, which provides a detailed breakdown of the captured traffic by protocol.

Protocol Hierarchy Statistics (Display filter: none)

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Ethernet	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Internet Protocol Version 4	99,07 %	6278	99,96 %	6154583	0,435	0	0	0,000
User Datagram Protocol	1,01 %	64	0,12 %	7296	0,001	0	0	0,000
Domain Name Service	0,98 %	62	0,11 %	6730	0,000	62	6730	0,000
Hypertext Transfer Protocol	0,03 %	2	0,01 %	566	0,000	2	566	0,000
Transmission Control Protocol	98,04 %	6213	99,84 %	6147217	0,435	6021	6068695	0,429
Secure Sockets Layer	2,30 %	146	0,70 %	42941	0,003	144	41111	0,003
Secure Sockets Layer	0,03 %	2	0,03 %	1830	0,000	2	1830	0,000
Hypertext Transfer Protocol	0,66 %	42	0,50 %	30937	0,002	24	18724	0,001
Media Type	0,27 %	17	0,18 %	11353	0,001	17	11353	0,001
Line-based text data	0,02 %	1	0,01 %	860	0,000	1	860	0,000
Malformed Packet	0,06 %	4	0,08 %	4644	0,000	4	4644	0,000
Internet Control Message Protocol	0,02 %	1	0,00 %	70	0,000	1	70	0,000
Address Resolution Protocol	0,93 %	59	0,04 %	2478	0,000	59	2478	0,000

The bottom status bar indicates: Text item (text), 31 bytes | Packets: 6337 - Displayed: 6337 (100,0%) - Dropped: 0 (0,0%) | Profile: Default

TCP follow : TCP oturumlarında paket birleştirme, HTTP bağlantısındaki tüm giden gelen paketlerin birleştirilip session hakkında bilgi verilmesi.

Wireshark

Birleştirilmek istenilen protokol paketi üzerinde sağ tıklanır ve "Follow TCP Stream" seçeneği seçilir.

The image shows the Wireshark 1.10.0 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for packet capture and analysis. The filter bar shows 'tcp.stream eq 6'. The packet list pane displays a list of captured packets, with packet 1475 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. A context menu is open over packet 1475, with the 'Follow TCP Stream' option highlighted. The status bar at the bottom shows 'File: /var/folders/jb/czplsn... | Packets: 6337 - Displayed: 2630 (41.5%) - Dropped: 0 (0.0%) | Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
1475	40.454889000	192.168.2.7	64.15.117.173	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1476	40.543435000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1477	41.418220000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1478	41.418359000	192.168.2.7	64.15.117.173	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1479	41.418931000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1480	41.419598000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1481	41.419647000	192.168.2.7	64.15.117.173	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1482	41.420712000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1483	41.420837000	192.168.2.7	64.15.117.173	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1484	41.421437000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1485	41.422449000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1486	41.422503000	192.168.2.7	64.15.117.173	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1487	41.423213000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1488	41.423437000	192.168.2.7	64.15.117.173	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1489	41.425061000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
1490	41.426357000	64.15.117.173	192.168.2.7	TCP	1162	1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0

Frame 1475: 1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0
Ethernet II, Src: Apple_08:00:27:00:00:00, Dst: AirtiesW_59:5e:25:00:00:00
Internet Protocol Version 4, Src: 192.168.2.7 (192.168.2.7), Dst: 64.15.117.173
Transmission Control Protocol, Src Port: 50540 (50540), Dst Port: http (80)
Source port: 50540 (50540)
Destination port: http (80)
[Stream index: 6]
Sequence number: 8121 (relative sequence number)
[Next sequence number: 9229 (relative sequence number)]
Acknowledgment number: 1479767 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 16384
[Calculated window size: 16384]
0000 00 1c a8 59 5e 25 20 c9 d0 06 56 91 08 00 45 00 ...Y...V...E.
0010 04 7c d9 1c 00 00 40 06 24 f4 c0 a8 02 07 40 0f ...|...@. \$.....@.
0020 75 ad c5 6c 00 50 18 cb 96 ef 40 82 8a e0 50 18 u..l.P.. ..@...P.
0030 40 00 84 b3 00 00 3d 31 33 37 36 33 38 30 32 33 @.....=1 37638023
0040 38 33 32 35 36 20 50 52 45 46 3d 48 49 44 44 45 8325; PR EF=HIDOE
0050 4e 5f 4d 41 53 54 48 45 41 44 5f 49 44 3d 33 4c N_MASTHE AD_ID=3L
0060 79 5f 66 73 46 64 52 45 49 26 61 6c 3d 74 72 2b y.fsF6RE I6altr+
0070 65 6e 26 66 76 3d 31 31 2e 37 2e 37 30 30 26 66 en&fv=11 .7.7006f
0080 34 3d 34 30 30 30 30 30 30 26 66 31 3d 35 30 30 4=400000 0&f1=500
0090 30 30 30 30 30 30 20 57 31 56 48 58 2e 72 65 73 00000; W 1VHX.res
00a0 75 6d 65 3d 56 5f 78 45 52 71 46 53 34 34 59 3a une=V_xE RqFS44Y:
00b0 31 31 35 33 2c 30 59 43 41 63 58 69 48 45 64 6b 1153,0YC ACXIHedk
00c0 3a 3d 30 38 34 2c 47 66 70 4c 65 61 39 4f 75 72 +20R6.Gf mlea90ur
Frame (1162 bytes) Reassembled TCP (2308 bytes)

İstek sayıları : http istek sayılarının görüntülenmesi.

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. A filter is applied to the packet list, showing only HTTP requests. The packet list shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
324	5.841010000	192.168.2.7	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
325	5.841807000	85.111.30.81	192.168.2.7	TCP	1494	[TCP Out-Of-Order] [TCP segment of a reassembled PDU]
326	5.841862000	192.168.2.7	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
327	5.842566000	85.111.30.81	192.168.2.7	TCP	1494	[TCP Out-Of-Order] [TCP segment of a reassembled PDU]
328	5.842662000	192.168.2.7	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
329	5.843803000	85.111.30.81	192.168.2.7	TCP	1494	[TCP Out-Of-Order] [TCP segment of a reassembled PDU]
330	5.843890000	192.168.2.7	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
331	5.845058000	85.111.30.77	192.168.2.7	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
332	5.845104000	192.168.2.7	173.194.39.2	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
333	5.848452000	173.194.39.2	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
334	5.852831000	85.111.30.81	192.168.2.7	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
335	5.854696000	85.111.30.81	192.168.2.7	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
336	5.854774000	192.168.2.7	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
337	5.855224000	85.111.30.81	192.168.2.7	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
338	5.855282000	192.168.2.7	85.111.30.81	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0
339	5.872665000	85.111.30.81	192.168.2.7	TCP	54	[TCP Dup ACK 238#2] 53128 > http [ACK] Seq=1465 Ack=6092 win=65535 Len=0

The packet details pane shows the following information for the selected packet (Frame 337):

- Frame 337: 639 bytes on wire (5112 bytes captured on interface)
- Ethernet II, Src: AirtiesW_59:5e:2d, Dst: 192.168.2.7
- Internet Protocol Version 4, Src: 85.111.30.81, Dst: 192.168.2.7
- Transmission Control Protocol, Src Port: 53128, Dst Port: 80, Seq: 1465, Win: 65535, Len: 0
- Hypertext Transfer Protocol
- JPEG File Interchange Format

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, TCP header, and the HTTP request body.

The HTTP/Requests with filter: window is open, showing a list of HTTP requests by host. The list is sorted by Count, Rate (ms), and Percent. The data is as follows:

Topic / Item	Count	Rate (ms)	Percent
HTTP Requests by HTTP Host	972	0,001136	
res.reklamport.com	15	0,000018	1,54%
www.sahibinden.com	30	0,000035	3,09%
banner2.sahibinden.com	90	0,000105	9,26%
image5.sahibinden.com	40	0,000047	4,12%
b.scorecardresearch.com	55	0,000064	5,66%
pubads.g.doubleclick.net	10	0,000012	1,03%
ad.reklamport.com	10	0,000012	1,03%
gatr.hit.gemius.pl	21	0,000025	2,16%
www.google-analytics.com	32	0,000037	3,29%
csi.gstatic.com	1	0,000001	0,10%
ds.serving-sys.com	1	0,000001	0,10%
kelebekgaleri.hurriyet.com.tr	50	0,000058	5,14%
www.hurriyet.com.tr	21	0,000025	2,16%
api1.hurpass.com	15	0,000018	1,54%
imgkelebek.hurriyet.com.tr	22	0,000026	2,26%
adonline.e-kolay.net	7	0,000008	0,72%
sayac.hurriyet.com.tr	9	0,000011	0,93%
ad.e-kolay.net	19	0,000022	1,95%
www.facebook.com	16	0,000019	1,65%

Uygulama : Paket yakalama

- ⌚ Tcp port 21 (FTP)
- ⌚ Tcp port 21 and tcp port 1982
- ⌚ Tcp port 22 and host bilmuh.gtu.edu.tr
- ⌚ Tcp port 21 (SMTP)

Uygulama : dsniff

Kaynakça

- ⌚ Paket/Protokol Analizi Amaçlı Wireshark Kullanımı,
http://wiki.bgasecurity.com/Paket/Protokol_Analizi_Amaçlı_Wireshark_Kullanımı
- ⌚ BGA, Beyaz şapkalı hacker eğitimi yardımcı ders notları - I