Curteanu Gabriel

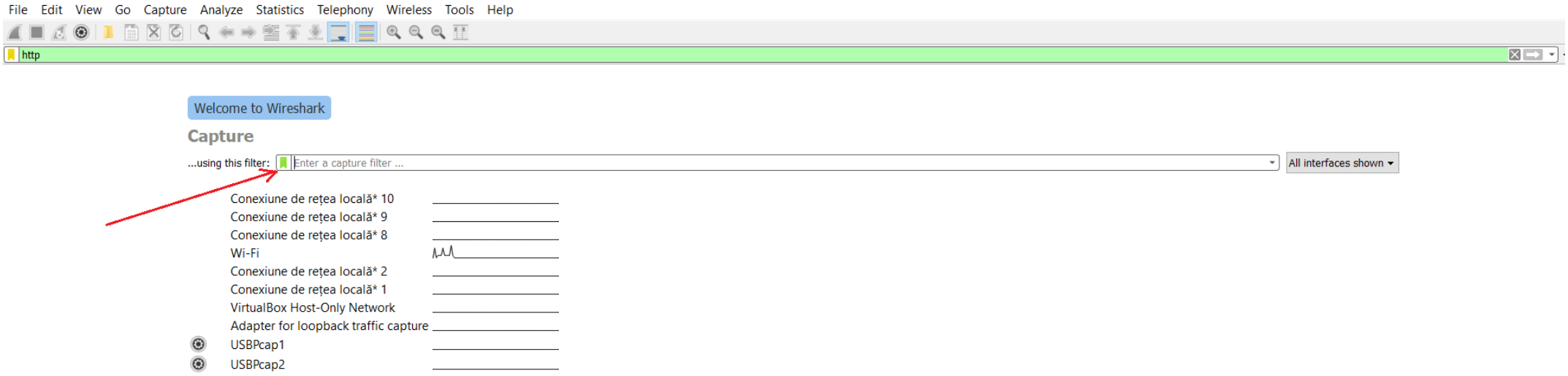
Captura și analiza traficului specific protocoalelor de nivel aplicație

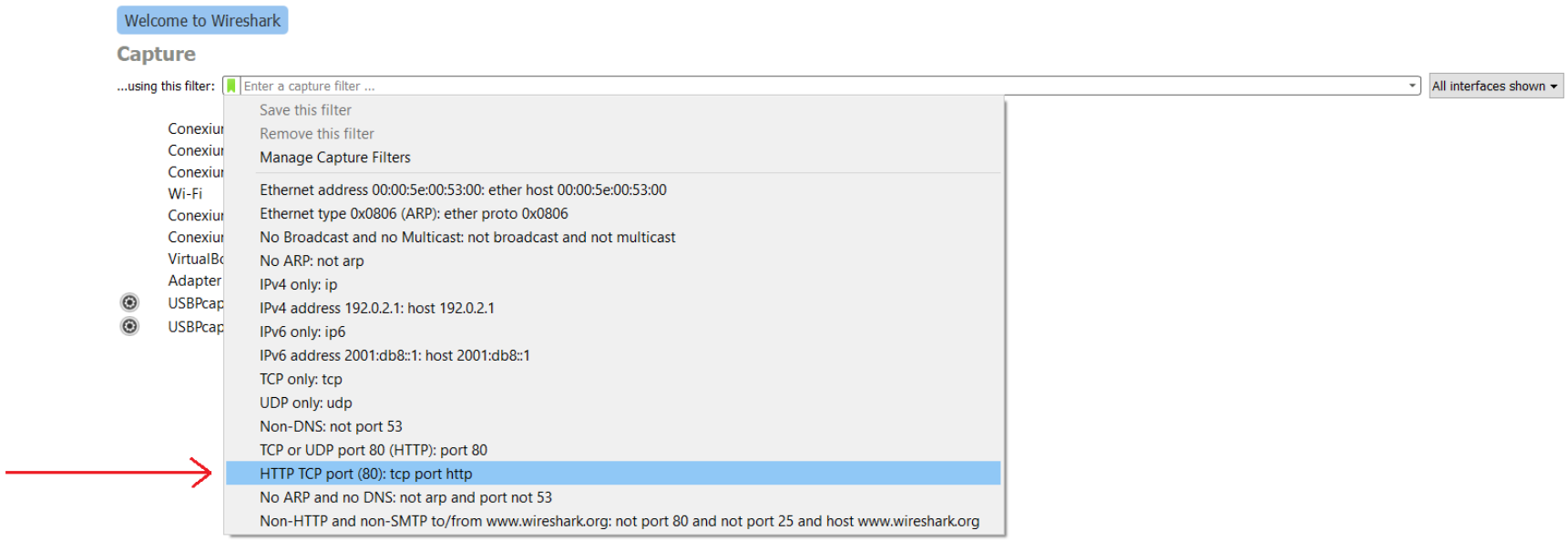
Protocoalele HTTP, FTP, DNS

1)HTTP

Pentru analiza pachetelor care țin de protocolul HTTP trebuie filtrat traficul. In campul care apare sub zona indicata de cuvantul *Capture* se poate introduce o descriere a conditiilor pe baza carora este selectat traficul respectiv, sau prin apasarea *bookmark-ului* de culoare verde se poate selecta un filtru de captura.

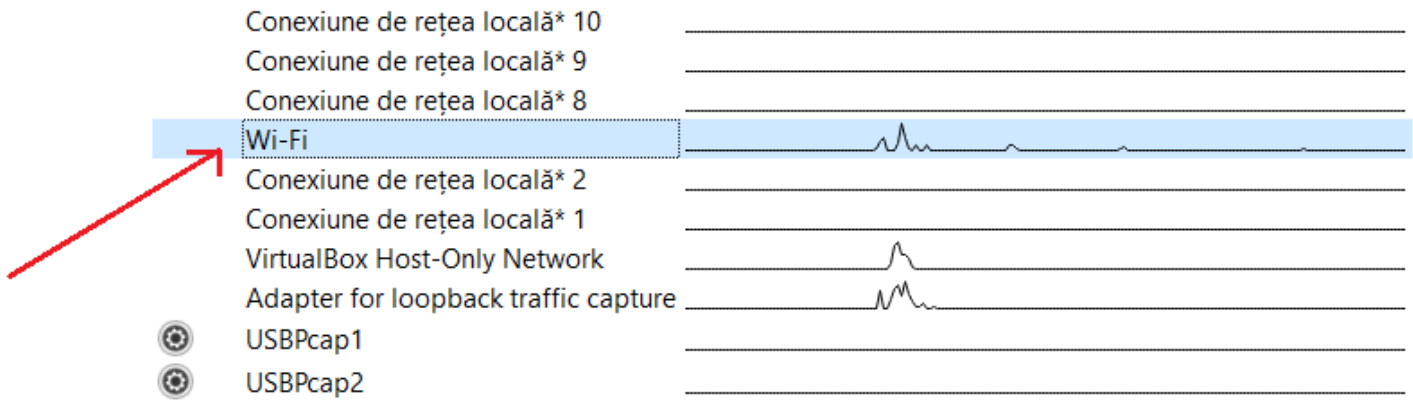
In cazul de față se selecteaza *HTTP TCP port(80): tcp port http.* 80 este numărul de port implicit pentru HTTP.



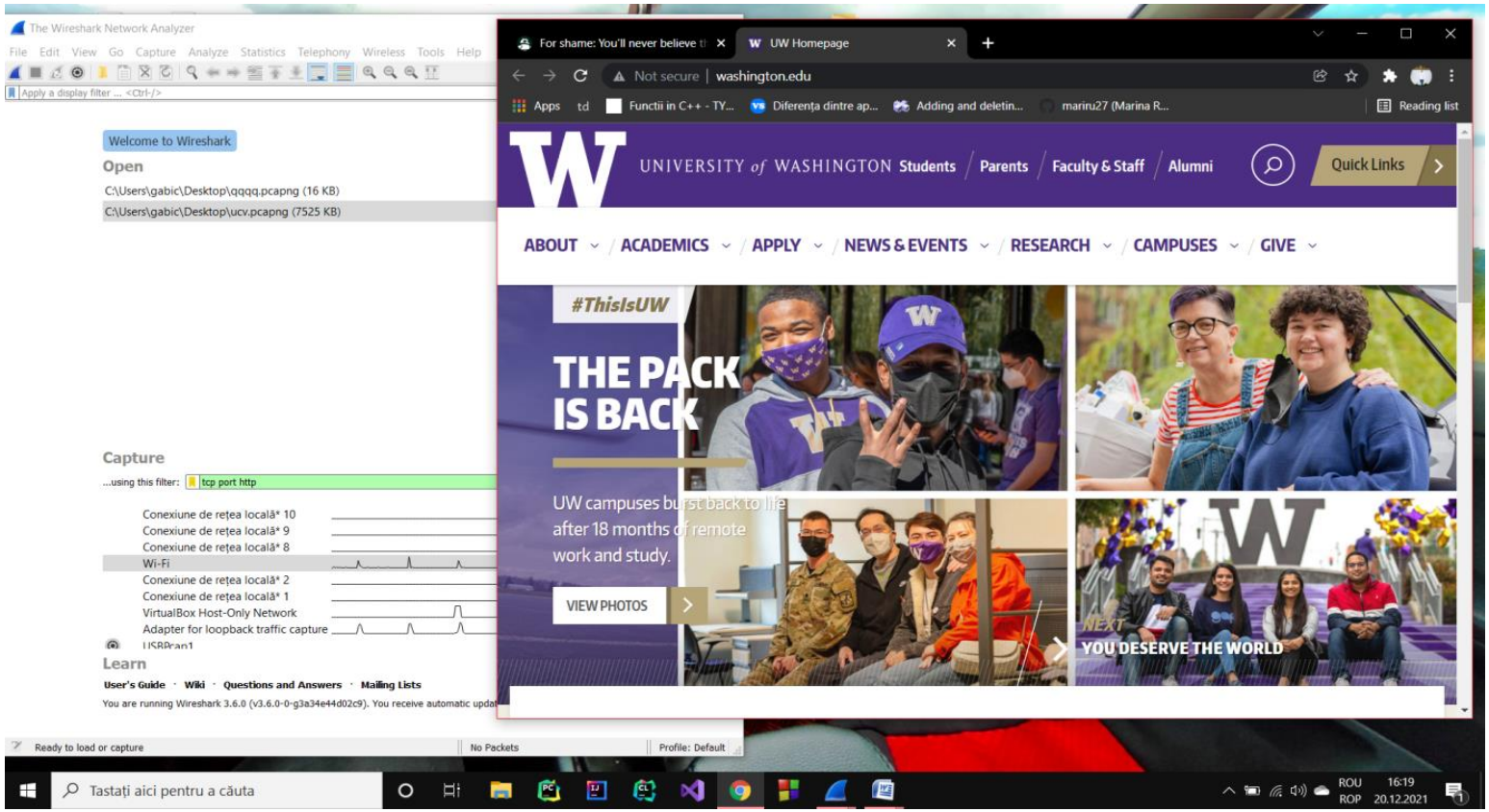

Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Save this filter
Remove this filter
Manage Capture Filters
Ethernet address 00:00:5e:00:53:00: ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): ether proto 0x0806
No Broadcast and no Multicast: not broadcast and not multicast
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: host 192.0.2.1
IPv6 only: ip6
IPv6 address 2001:db8::1: host 2001:db8::1
TCP only: tcp
UDP only: udp
Non-DNS: not port 53
TCP or UDP port 80 (HTTP): port 80
HTTP TCP port (80): tcp port http
No ARP and no DNS: not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org: not port 80 and not port 25 and host www.wireshark.org
Wi-Fi
USBPcap
USBPcap


Capture
...using this filter:
tcp port http
All interfaces shown

Acum ca filtrul este precizat, se lanseaza prin dublu click captura pe o interfata de retea; in cazul de față se foloseste W-Fi.

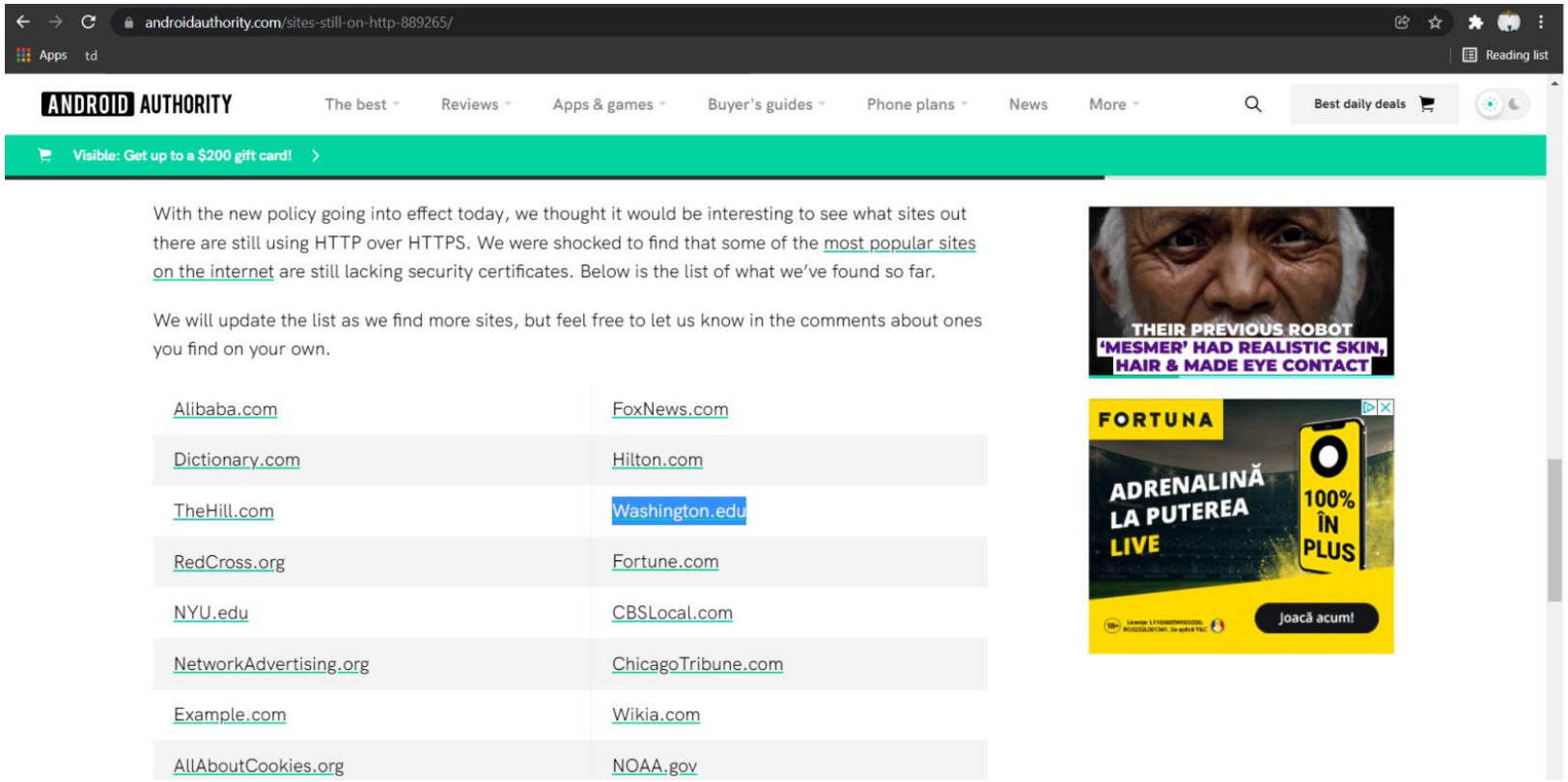


Site-ul ales pentru experimentele care vor implica folosirea protocolului HTTP este cel al Washington.edu (http://www.washington.edu/).

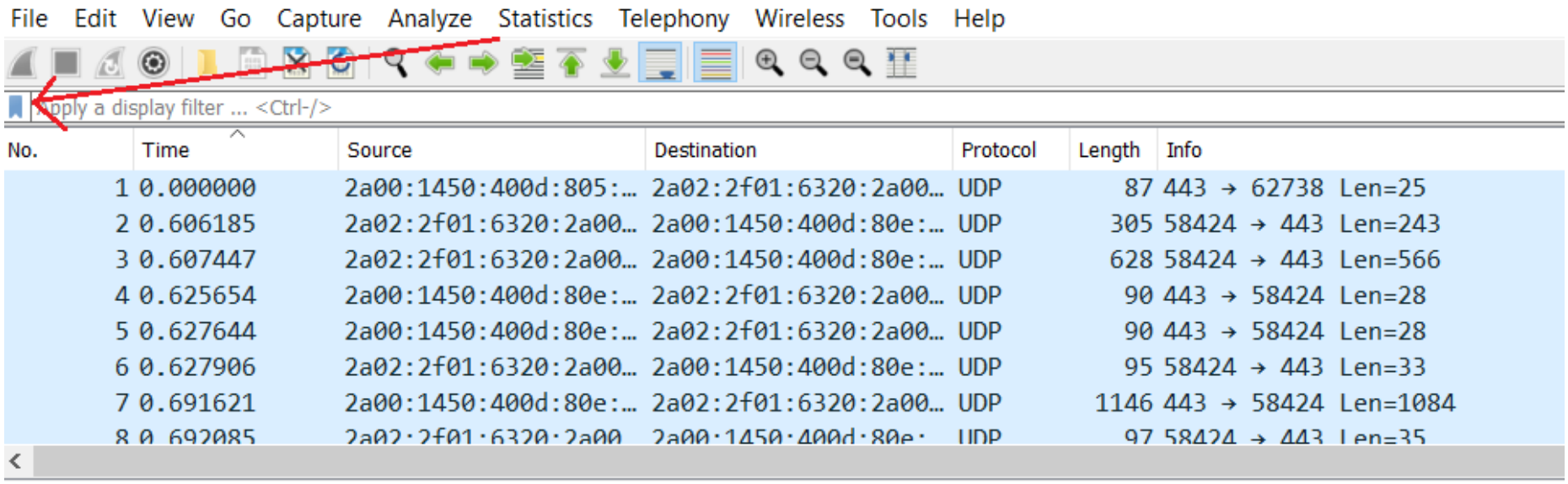


Site-ul a fost ales dintr-o lista de site-uri HTTP.

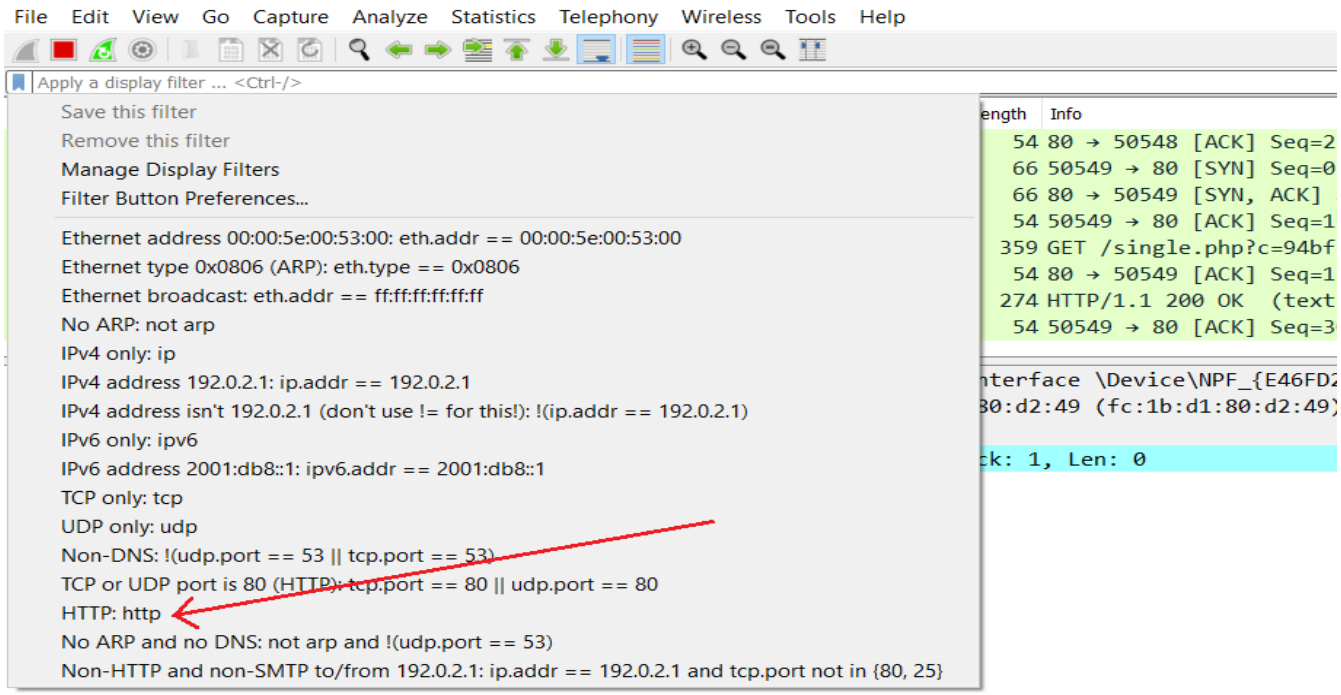
Lista se poate găsi la adresa https://www.androidauthority.com/sites-still-on-http-889265/.

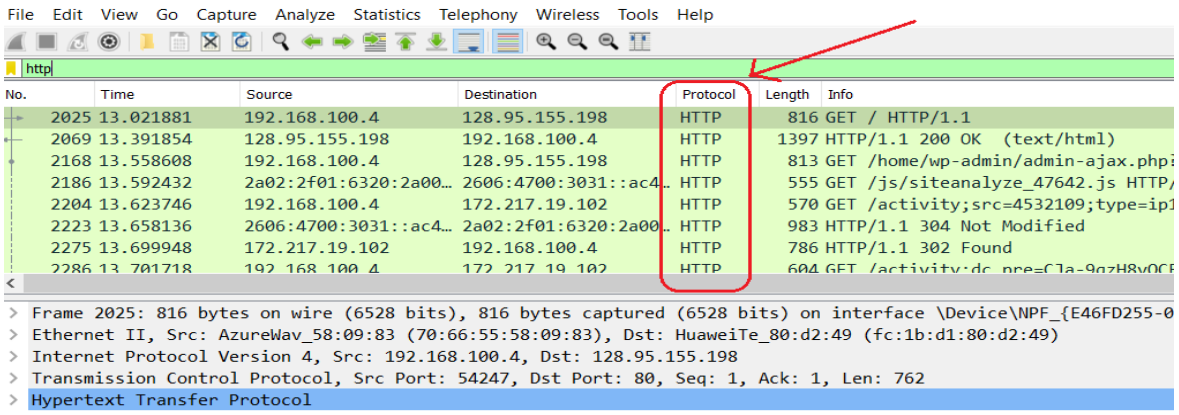


S-a incarcat site-ul si traficul a inceput sa circule. Pentru a se afisa doar traficul HTTP, se dă click pe *bookmark-ul* albastru deschis si se selecteaza traficul HTTP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a00:1450:400d:805:…	2a02:2f01:6320:2a00…	UDP	87	443 → 62738 Len=25
2	0.606185	2a02:2f01:6320:2a00…	2a00:1450:400d:80e:…	UDP	305	58424 → 443 Len=243
3	0.607447	2a02:2f01:6320:2a00…	2a00:1450:400d:80e:…	UDP	628	58424 → 443 Len=566
4	0.625654	2a00:1450:400d:80e:…	2a02:2f01:6320:2a00…	UDP	90	443 → 58424 Len=28
5	0.627644	2a00:1450:400d:80e:…	2a02:2f01:6320:2a00…	UDP	90	443 → 58424 Len=28
6	0.627906	2a02:2f01:6320:2a00…	2a00:1450:400d:80e:…	UDP	95	58424 → 443 Len=33
7	0.691621	2a00:1450:400d:80e:…	2a02:2f01:6320:2a00…	UDP	1146	443 → 58424 Len=1084
8	0.692085	2a02:2f01:6320:2a00	2a00:1450:400d:80e:	UDP	97	58424 → 443 Len=35


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Save this filter
Remove this filter
Manage Display Filters
Filter Button Preferences...
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): eth.type == 0x0806
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!): !(ip.addr == 192.0.2.1)
IPv6 only: ipv6
IPv6 address 2001:db8::1: ipv6.addr == 2001:db8::1
TCP only: tcp
UDP only: udp
Non-DNS: !(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP): tcp.port == 80 || udp.port == 80
HTTP: http
No ARP and no DNS: not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1: ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
ength Info
54 80 → 50548 [ACK] Seq=2
66 50549 → 80 [SYN] Seq=0
66 80 → 50549 [SYN, ACK]
54 50549 → 80 [ACK] Seq=1
359 GET /single.php?c=94bf
54 80 → 50549 [ACK] Seq=1
274 HTTP/1.1 200 OK (text
54 50549 → 80 [ACK] Seq=3
nterface \Device\NPF_{E46FD2
80:d2:49 (fc:1b:d1:80:d2:49)
ck: 1, Len: 0


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
2025 13.021881 192.168.100.4 128.95.155.198 HTTP 816 GET / HTTP/1.1
2069 13.391854 128.95.155.198 192.168.100.4 HTTP 1397 HTTP/1.1 200 OK (text/html)
2168 13.558608 192.168.100.4 128.95.155.198 HTTP 813 GET /home/wp-admin/admin-ajax.php
2186 13.592432 2a02:2f01:6320:2a00… 2606:4700:3031::ac4… HTTP 555 GET /js/siteanalyze_47642.js HTTP/
2204 13.623746 192.168.100.4 172.217.19.102 HTTP 570 GET /activity;src=4532109;type=ip1
2223 13.658136 2606:4700:3031::ac4… 2a02:2f01:6320:2a00… HTTP 983 HTTP/1.1 304 Not Modified
2275 13.699948 172.217.19.102 192.168.100.4 HTTP 786 HTTP/1.1 302 Found
Frame 2025: 816 bytes on wire (6528 bits), 816 bytes captured (6528 bits) on interface \Device\NPF_{E46FD255-0
Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
Internet Protocol Version 4, Src: 192.168.100.4, Dst: 128.95.155.198
Transmission Control Protocol, Src Port: 54247, Dst Port: 80, Seq: 1, Ack: 1, Len: 762
Hypertext Transfer Protocol

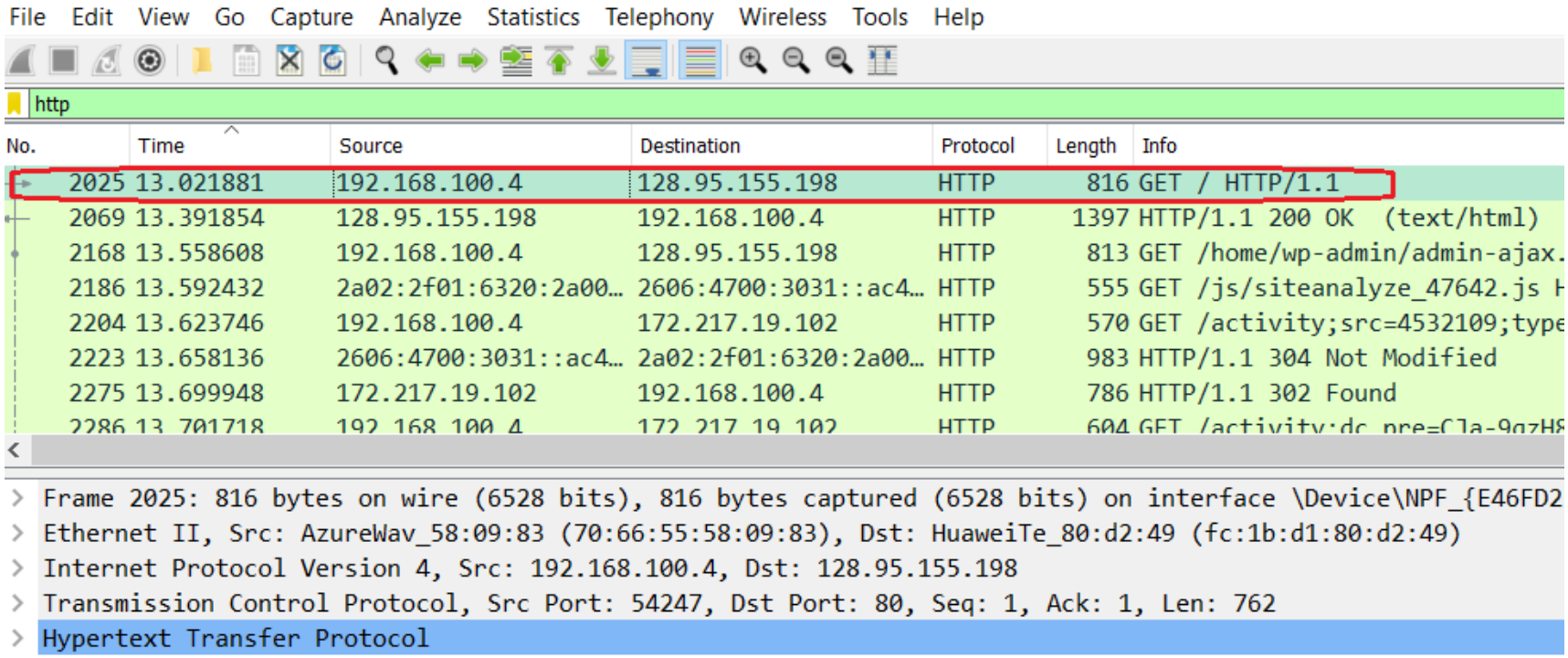
Protocolul HTTP foloseste TCP ca si protocol de transport.

Există două tipuri de mesaje HTTP: mesaje de solicitare (cerere) și mesaje de răspuns, ambele fiind discutate în cele ce urmează.

Prima data se analizeaza un pachet cerere.

Pachet de tip cerere:

Se selecteaza un pachet din cele afisate si se despacheteaza pentru a i se observa continutul. Pentru experiment se selecteaza primul pachet.



Sectiunea *Hypertext Transfer Protocol* afiseaza continutul pachetului.

Cand este expandat randul, se vor afisa urmatoarele:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2168	13.558608	192.168.100.4	128.95.155.198	HTTP	813	GET /home,
2186	13.592432	2a02:2f01:6320:2a00…	2606:4700:3031::ac4…	HTTP	555	GET /js/s
2204	13.623746	192.168.100.4	172.217.19.102	HTTP	570	GET /acti
2223	13.658136	2606:4700:3031::ac4…	2a02:2f01:6320:2a00…	HTTP	983	HTTP/1.1
2275	13.699948	172.217.19.102	192.168.100.4	HTTP	786	HTTP/1.1
2286	13.701718	192.168.100.4	172.217.19.102	HTTP	604	GET /acti
2320	13.747613	128.95.155.198	192.168.100.4	HTTP/J…	969	HTTP/1.1
2354	13.769159	172.217.19.102	192.168.100.4	HTTP	785	HTTP/1.1

```
> Frame 2025: 816 bytes on wire (6528 bits), 816 bytes captured (6528 bits) on interface
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 128.95.155.198
> Transmission Control Protocol, Src Port: 54247, Dst Port: 80, Seq: 1, Ack: 1, Len: 762
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: www.washington.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ro-RO,ro;q=0.9,en-US;q=0.8,en;q=0.7,de;q=0.6,fr;q=0.5\r\n
    v Cookie: _gcl_au=1.1.1668584188.1639740734; _ga=GA1.2.1718338852.1639740734; nmstat=
        Cookie pair: _gcl_au=1.1.1668584188.1639740734
        Cookie pair: _ga=GA1.2.1718338852.1639740734
        Cookie pair: nmstat=13eaedf5-f01a-b081-53f2-57ea8ad6d0a9
        Cookie pair: _mkto_trk=id:131-AQO-225&token:_mch-washington.edu-1639740738270-95
    If-None-Match: "f0aac-fa92-5d34876df3940"\r\n
    If-Modified-Since: Thu, 16 Dec 2021 19:31:09 GMT\r\n
    \r\n
```

Mesaj de tip cerere(request) reprezentat de comanda GET. Are urmatorii parametrii:

Tipul mesajului: cerere

Resursa asupra căreia se aplică cererea

Versiunea de protocol HTTP

Adresa host-ului

Tipul conexiunii: keep-alive, permite ca o singură conexiune TCP să rămână deschisă pentru mai multe solicitări/răspunsuri HTTP

Acest header trimite un mesaj către server care exprimă dorința clientului pentru un răspuns criptat și autentificat

Tipul de browser care face cererea către server

Acest header indica limba si locatia preferate de client

Aceasta sectiune verifica cooki-urile

Mesajul merge catre nivelul transport unde protocolul TCP il transforma intr-un segment.

Pentru a putea vizualiza continutul segmentului se expandeaza randul *Transmission Control Protocol*.

```
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 128.95.155.198
v Transmission Control Protocol, Src Port: 54247, Dst Port: 80, Seq: 1, Ack: 1, Len: 762
    Source Port: 54247
    Destination Port: 80
    [Stream index: 47]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 762]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2852692853
    [Next Sequence Number: 763    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 921177961
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····AP···]
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0x248f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.182255000 seconds]
      [Time since previous frame in this TCP stream: 0.000353000 seconds]
  > [SEQ/ACK analysis]
    TCP payload (762 bytes)
> Hypertext Transfer Protocol
```

Numarul portului sursa: 54247

Numarul portului destinatie: 80, portul implicit HTTP

Se foloseşte un număr (47 aici) pentru a identifica în mod unic un flux TCP

Nivelul de completare a conversatiei; este completa

Dimensiunea datelor conţinute în acest pachet

Numarul secventei

Numarul secventei care este defapt trimis pachetului

Este numărul de secvenţă curent + lungimea datelor din pachetul curent

Linia reprezintă numărul total de octeţi pe care gazda (host-ul) curent i-a primit din cealaltă parte

Numărul real de confirmare (acknowledgment)

Lungimea antetului TCP exprimata in octeti (20)

Flag-urile arata serverului care trimite mesajul ce actiuni trebuie sa indeplineasca serverul care primeste mesajul

Acest flag recunoaste datele pe care le-a primit de la celalalt server

Gazda care primeşte mesajul trebuie să transmită datele aplicaţiei care primeşte mesajul cât mai repede posibil

Dimensiunea buffer-ului de recepţie

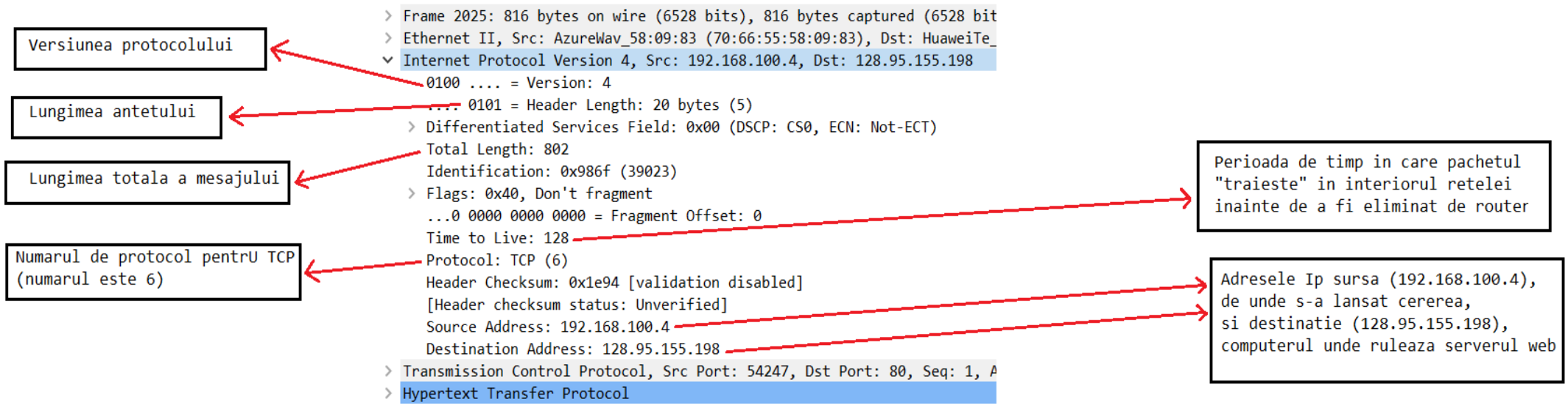
In timp ce pachetele sunt capturate, fiecare pachet este inregistrat intr-un "marcaj temporal". Aceste marcaje sunt salvate in fisierul de captura pentru a putea fi folosite in viitoarele analize

Secventele TCP (SEQ) si (ACK) ajuta la activarea unui transfer de date ordonat si fiabil

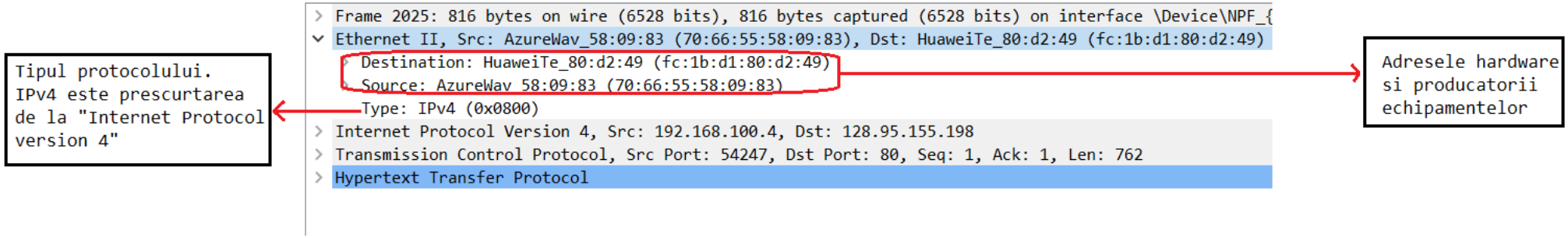
TCP Payload reprezinta corpul pachetului unde se gaseste tot continutul mesajului din antetul HTTP

Segmentul TCP este predat nivelului retea in protocolul Internet (Internet Protocol). Acest protocol face posibila partea de adresare.

In acest antet se obtine datagrama. Acest antet impreuna cu segmentul TCP formeaza datagrama de nivel retea.



In antetul *Ethernet II* se pot vedea adresele hardware (sursa si destinatie). Se pot identifica si producatorii acestor echipamente.



Datagrama de nivel retea este transmisa nivelului legatura de date in cadru (frame), care cuprinde intregul pachet.

ID-ul interfetei

Numele interfetei

Tipul interfetei, care in exemplu este Wi-Fi

Tipul de incapsulare: Ethernet (10) este o valoare interna care reprezinta tipul de antet al legaturii pentru pachetul respectiv

```
Frame 2025: 816 bytes on wire (6528 bits), 816 bytes captured (6528 bits) on interface \Device\NPF_{E4
  Interface id: 0 (\Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26})
    Interface name: \Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26}
    Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 20, 2021 16:11:04.793611000 GTB, oră standard
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1640009464.793611000 seconds
  [Time delta from previous captured frame: 0.000353000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 13.021881000 seconds]
  Frame Number: 2025
  Frame Length: 816 bytes (6528 bits)
  Capture Length: 816 bytes (6528 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
Internet Protocol Version 4, Src: 192.168.100.4, Dst: 128.95.155.198
Transmission Control Protocol, Src Port: 54247, Dst Port: 80, Seq: 1, Ack: 1, Len: 762
Hypertext Transfer Protocol
```

Momentul cand cererea a fost trimisa

Numarul cadrului

Lungimea Cadrului

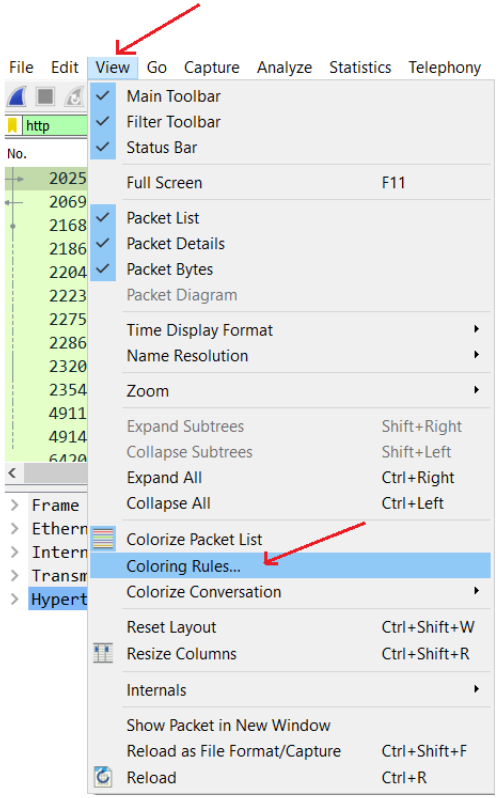
Numarul de octeti capturati

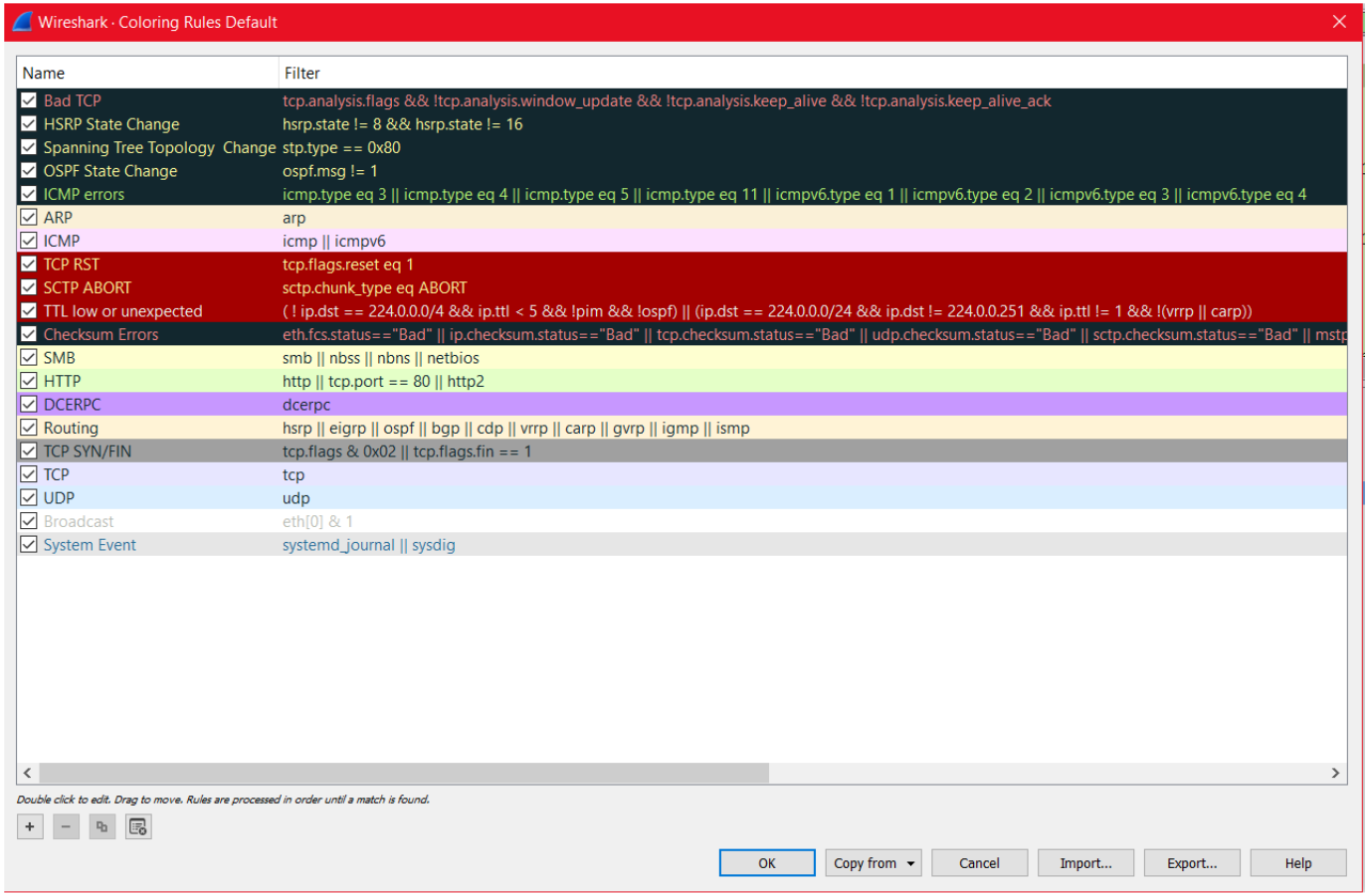
Protocoalele folosite in cadru

Culoarea pachetului selectat (verde) si numele filtrului

ICMP errors	icmp.type eq 3 || icmp
ARP	arp
ICMP	icmp || icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq AB
TTL low or unexpected	(! ip.dst == 224.0.0.0/4
Checksum Errors	eth.fcs.status=="Bad" |
SMB	smb || nbss || nbns || ne
HTTP	http || tcp.port == 80 || http2
DCERPC	dcerpc
Routing	hsrp || eigrp || ospf || bgp || cd
TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin
TCP	tcp
UDP	udp

Pentru a putea vizualiza culorile pachetelor se selecteaza *View -> Coloring Rules*





Pachet de tip raspuns:

Se selecteaza un pachet din cele afisate si se despacheteaza pentru a i se observa continutul. Pentru experiment se selecteaza al doilea pachet.

http

No.	Time	Source	Destination	Protocol	Length	Info
2025	13.021881	192.168.100.4	128.95.155.198	HTTP	816	GET / HTTP/1.1
2069	13.391854	128.95.155.198	192.168.100.4	HTTP	1397	HTTP/1.1 200 OK (text/html)
2168	13.558608	192.168.100.4	128.95.155.198	HTTP	813	GET /home/wp-admin/admin-ajax.php
2186	13.592432	2a02:2f01:6320:2a00…	2606:4700:3031::ac4…	HTTP	555	GET /js/siteanalyze_47642.js HTTP/
2204	13.623746	192.168.100.4	172.217.19.102	HTTP	570	GET /activity;src=4532109;type=ip
2223	13.658136	2606:4700:3031::ac4…	2a02:2f01:6320:2a00…	HTTP	983	HTTP/1.1 304 Not Modified
2275	13.699948	172.217.19.102	192.168.100.4	HTTP	786	HTTP/1.1 302 Found
2286	13.701718	192.168.100.4	172.217.19.102	HTTP	604	GET /activity;dc_pre=CJa-9qzH8vQC
2320	13.747613	128.95.155.198	192.168.100.4	HTTP/J…	969	HTTP/1.1 200 OK , JavaScript Obje
2354	13.769159	172.217.19.102	192.168.100.4	HTTP	785	HTTP/1.1 302 Found
4911	23.218490	128.95.155.198	192.168.100.4	HTTP	266	HTTP/1.0 408 Request Time-out (t
4914	23.265692	128.95.155.198	192.168.100.4	HTTP	266	HTTP/1.0 408 Request Time-out (t
6420	37.382904	192.168.100.4	185.141.63.172	HTTP	359	GET /single.php?c=94bf3661c794e3e
6423	37.475692	185.141.63.172	192.168.100.4	HTTP	274	HTTP/1.1 200 OK (text/html)
7677	75.251360	192.168.100.4	192.28.147.68	HTTP	728	POST /webevents/visitWebPage?_mch
7698	75.438713	192.28.147.68	192.168.100.4	HTTP	365	HTTP/1.1 200 OK (text/plain)

Se observa continutul HTML al paginii:

```
> Frame 2069: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits) on interface \Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26}, id 0
> Ethernet II, Src: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49), Dst: AzureWav_58:09:83 (70:66:55:58:09:83)
> Internet Protocol Version 4, Src: 128.95.155.198, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 54247, Seq: 14121, Ack: 763, Len: 1343
> [11 Reassembled TCP Segments (15463 bytes): #2032(1412), #2033(1412), #2035(1412), #2036(1412), #2038(1412), #2039(1412), #2041(1412), #2042(1412), #2044(1412), #2045(1412), #2069(1343)]
> Hypertext Transfer Protocol
v Line-based text data: text/html (20 lines)
    [truncated]<!DOCTYPE html><html class="no-js" lang="en"><head><meta content="IE=edge" http-equiv="X-UA-Compatible"/><title> UW Homepage </title><meta charset="utf-8"/><meta content="University of Washingt…
  \tvar gtm4wp_datalayer_name = "dataLayer";\n
  \tvar dataLayer = dataLayer || [];\n
  //]]>\n
    [truncated]</script><!-- End Google Tag Manager for WordPress by gtm4wp.com --><link href="//www.washington.edu" rel="dns-prefetch"/><link href="//fonts.googleapis.com" rel="dns-prefetch"/><link href="//s…
  /* <![CDATA[ */\n
  var style_dir = "http:\/\/www.washington.edu\/home";\n
    [truncated]var jetpackCarouselStrings = {"widths":[370,700,1000,1200,1400,2000],"is_logged_in":"","lang":"en","ajaxurl":"http:\/\/www.washington.edu\/home\/wp-admin\/admin-ajax.php","nonce":"d30c9fe0ed","…
  var apiKey = {"local":"","network":"AIzaSyAtyy_XX9al6Xyq2KVHt8q949BkAwsI48c"};\n
  /* ]]> */\n
    [truncated]</script><script src="//www.washington.edu/static/home/wp-content/themes/uw-2014/js/site.js?ver=2.3.3" type="text/javascript"></script><script src="//www.washington.edu/static/home/wp-content/t…
  \tvar dataLayer_content = {"siteID":"81","siteName":"UW Homepage","pagePostType":"frontpage"};\n
  \tdataLayer.push( dataLayer_content );//]]>\n
  </script><script data-cfasync="false">//<![CDATA[\n
  (function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':\n
  new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],\n
  j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=\n
  '//www.googletagmanager.com/gtm.'+'js?id='+i+dl;f.parentNode.insertBefore(j,f);\n
  })(window,document,'script','dataLayer','GTM-KQ6QQBT');//]]>\n
    [truncated]</script><!-- End Google Tag Manager --><!-- End Google Tag Manager for WordPress by gtm4wp.com --> <style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margi…
```

La inspectarea sursei paginii se observa ca se aseamana codurile HTML:

UW Homepage | view-source:www.washington.edu

Not secure | view-source:www.washington.edu

Apps td | Reading list

Line wrap

```
<!DOCTYPE html><html class="no-js" lang="en"><head><meta content="IE=edge" http-equiv="X-UA-Compatible"/><title> UW Homepage </title><meta charset="utf-8"/><meta content="University of Washington" name="descr
    var gtm4wp_datalayer_name = "dataLayer";
    var dataLayer = dataLayer || [];
//]]>
</script><!-- End Google Tag Manager for WordPress by gtm4wp.com --><link href="//www.washington.edu" rel="dns-prefetch"/><link href="//fonts.googleapis.com" rel="dns-prefetch"/><link href="//s.w.org" rel="dn
/* <![CDATA[ */
var style_dir = "http:\/\/www.washington.edu\/home";
var jetpackCarouselStrings = {"widths":[370,700,1000,1200,1400,2000],"is_logged_in":"","lang":"en","ajaxurl":"http:\/\/www.washington.edu\/home\/wp-admin\/admin-ajax.php","nonce":"1cf697d05b","display_exif":"
var apiKey = {"local":"","network":"AIzaSyAtyy_XX9al6Xyq2KVHt8q949BkAwsI48c"};
/* ]]> */
</script><script id="site-js" src="//www.washington.edu/static/home/wp-content/themes/uw-2014/js/site.js?ver=2.3.3" type="text/javascript"></script><script id="homepage-js" src="//www.washington.edu/static/ho
    var dataLayer_content = {"siteID":"81","siteName":"UW Homepage","pagePostType":"frontpage"};
    dataLayer.push( dataLayer_content );//]]>
</script><script data-cfasync="false">//<![CDATA[
(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'//www.googletagmanager.com/gtm.'+'js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-KQ6QQBT');//]]>
</script><!-- End Google Tag Manager --><!-- End Google Tag Manager for WordPress by gtm4wp.com --><style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}
```

Sectiunea *Hypertext Transfer Protocol* afiseaza continutul raspunsului:

```
> Frame 2069: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176
> Ethernet II, Src: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49), Dst: AzureWav_5
> Internet Protocol Version 4, Src: 128.95.155.198, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 54247, Seq: 14121
> [11 Reassembled TCP Segments (15463 bytes): #2032(1412), #2033(1412), #2
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 20 Dec 2021 14:11:04 GMT\r\n
    Server: Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.1e-fips PHP/7
    Last-Modified: Mon, 20 Dec 2021 00:27:10 GMT\r\n
    ETag: "180c17-f609-5d388f308b380"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding,User-Agent\r\n
    Content-Encoding: gzip\r\n
  v Content-Length: 15087\r\n
      [Content length: 15087]
    Content-Type: text/html\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.369973000 seconds]
    [Request in frame: 2025]
    [Next request in frame: 2168]
    [Next response in frame: 2320]
    [Request URI: http://www.washington.edu/]
    Content-encoded entity body (gzip): 15087 bytes -> 62985 bytes
    File Data: 62985 bytes
> Line-based text data: text/html (20 lines)
```

Linia indică data și ora când răspunsul HTTP a fost creat și trimis de către server.

Versiunea protocolului

Codul de stare 200 arata ca totul este in regula

Mesajul de stare "OK" semnifica faptul ca serverul a gasit si trimite obiectul solicitat

Linia de antet indică faptul că mesajul a fost generat de un server web Apache instalat pe o distribuție Unix

Antetul arata data și ora când obiectul a fost creat sau modificat ultima dată

Numărul de octeți din obiectul trimis

Linia indica faptul ca obiectul din corpul mesajului este text HTML

Nivelul transport divide mesajul pe care il primeste de la nivelul aplicatie in segmente. Din cauza marimii mesajului care nu incape intr-un singur pachet de informatii, protocolul TCP imparte mesajul de raspuns in segmente egale (fiecare are 1412 octeti) pe care le v-a reasambla la destinatie cand v-a fi afisat mesajul final.

```
> Frame 2069: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits) on int
> Ethernet II, Src: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49), Dst: AzureWav_58:09:83 (70:
> Internet Protocol Version 4, Src: 128.95.155.198, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 54247, Seq: 14121, Ack: 763,
v [11 Reassembled TCP Segments (15463 bytes): #2032(1412), #2033(1412), #2035(1412), #
    [Frame: 2032, payload: 0-1411 (1412 bytes)]
    [Frame: 2033, payload: 1412-2823 (1412 bytes)]
    [Frame: 2035, payload: 2824-4235 (1412 bytes)]
    [Frame: 2036, payload: 4236-5647 (1412 bytes)]
    [Frame: 2038, payload: 5648-7059 (1412 bytes)]
    [Frame: 2039, payload: 7060-8471 (1412 bytes)]
    [Frame: 2041, payload: 8472-9883 (1412 bytes)]
    [Frame: 2042, payload: 9884-11295 (1412 bytes)]
    [Frame: 2044, payload: 11296-12707 (1412 bytes)]
    [Frame: 2045, payload: 12708-14119 (1412 bytes)]
    [Frame: 2069, payload: 14120-15462 (1343 bytes)]
    [Segment count: 11]
    [Reassembled TCP length: 15463]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c2032
> Hypertext Transfer Protocol
> Line-based text data: text/html (20 lines)
```

Segmentele

Numarul de segmente

La nivelul retea, adresa sursa si adresa destinatie se inverseaza; mesajul cerere este trimis catre destinatie, iar mesajul raspuns este trimis la sursa, care devine noua destinatie, dupa cum se observa:

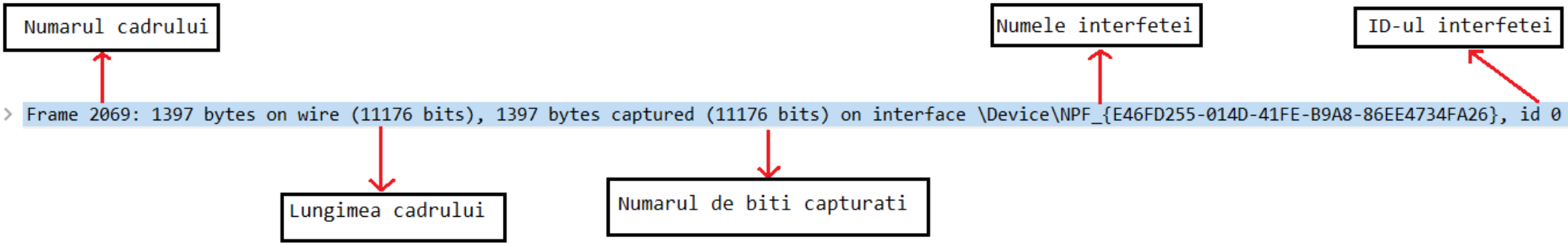
Cerere

```
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 128.95.155.198
> Transmission Control Protocol, Src Port: 54247, Dst Port: 80, Seq: 1, Ack: 1, Len: 762
```

Raspuns

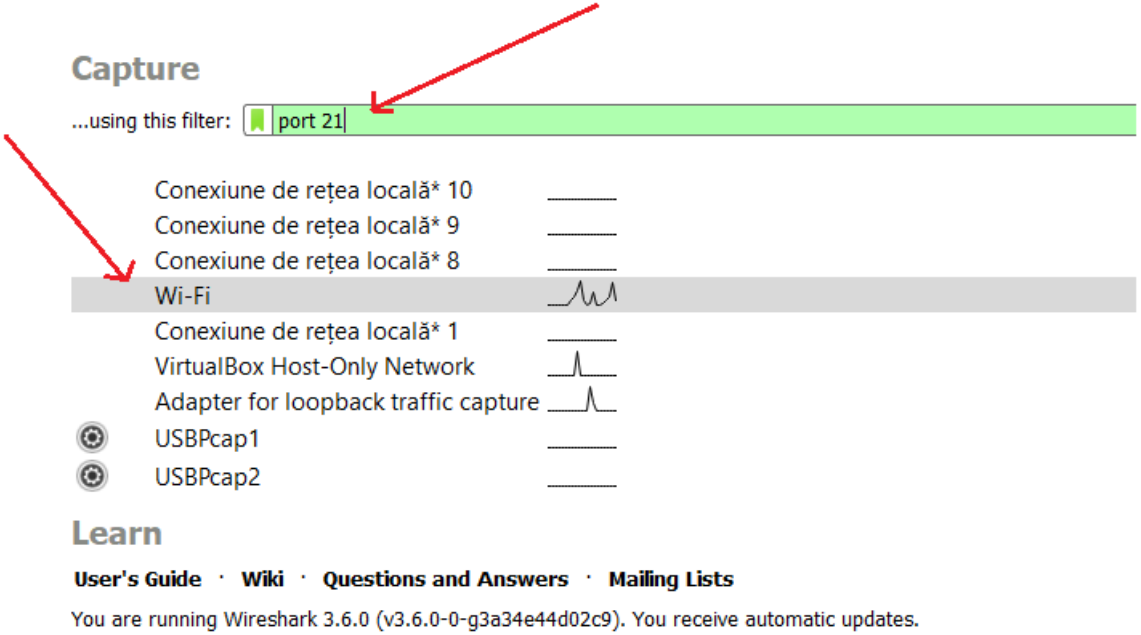
```
> Internet Protocol Version 4, Src: 128.95.155.198, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 80, Dst Port: 54247, Seq: 14121, Ack: 763, Len: 1343
```

In cadru(frame) se afla pachetul primit ca raspuns.



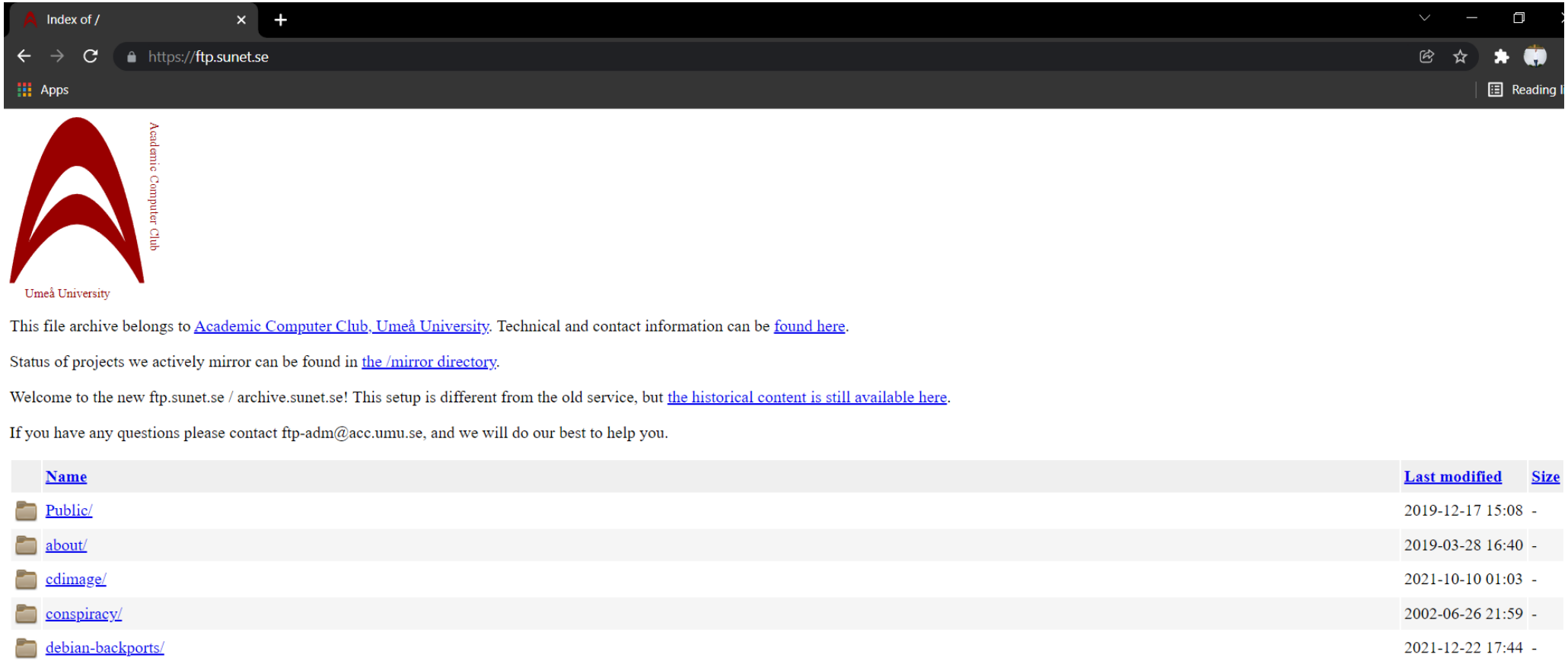
2)FTP

Pentru analiza pachetelor care țin de protocolul FTP se introduce numarul *port 21* in caseta folosita pentru filtrare.



Protocolul FTP folosește TCP ca protocol de transport.

Site-ul ales pentru experimentul FTP este https://ftp.sunet.se/.



Conexiunea la site se face din Linia de comanda, folosind comanda *ftp.*

Se realizeaza conexiunea catre site

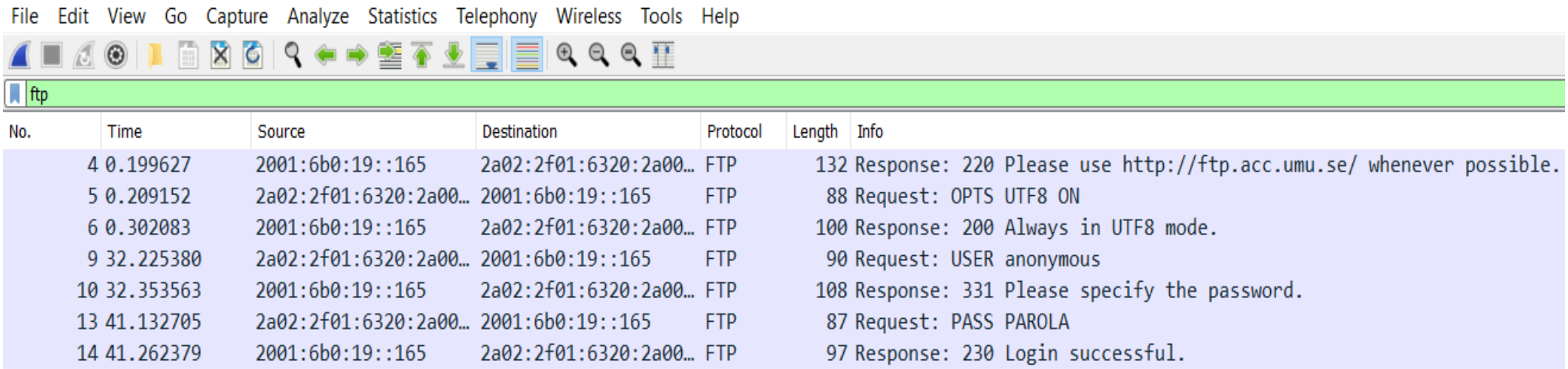
```
Microsoft Windows [Version 10.0.19041.685]
(c) 2020 Microsoft Corporation. Toate drepturile rezervate.

C:\Users\gabic>ftp ftp.sunet.se
Connected to sunet.ftp.acc.umu.se.
220 Please use http://ftp.acc.umu.se/ whenever possible.
200 Always in UTF8 mode.
User (sunet.ftp.acc.umu.se:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

Se introduce un username, de preferat anonim

Se introduce o parola. Cea folosita in experiment este PAROLA

Autentificarea are loc cu succes

Se observa protocoalele FTP, filtrate cu portul 21:



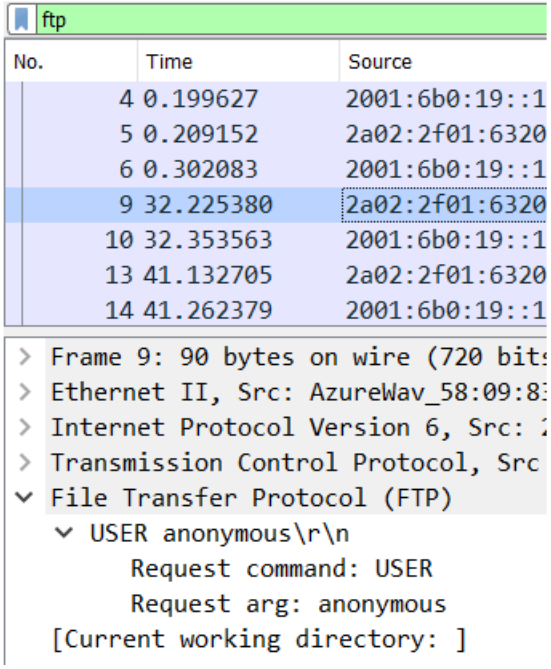
No.	Time	Source	Destination	Protocol	Length	Info
4	0.199627	2001:6b0:19::165	2a02:2f01:6320:2a00…	FTP	132	Response: 220 Please use http://ftp.acc.umu.se/ whenever possible.
5	0.209152	2a02:2f01:6320:2a00…	2001:6b0:19::165	FTP	88	Request: OPTS UTF8 ON
6	0.302083	2001:6b0:19::165	2a02:2f01:6320:2a00…	FTP	100	Response: 200 Always in UTF8 mode.
9	32.225380	2a02:2f01:6320:2a00…	2001:6b0:19::165	FTP	90	Request: USER anonymous
10	32.353563	2001:6b0:19::165	2a02:2f01:6320:2a00…	FTP	108	Response: 331 Please specify the password.
13	41.132705	2a02:2f01:6320:2a00…	2001:6b0:19::165	FTP	87	Request: PASS PAROLA
14	41.262379	2001:6b0:19::165	2a02:2f01:6320:2a00…	FTP	97	Response: 230 Login successful.

Exista mesaje de tip cerere si raspuns.

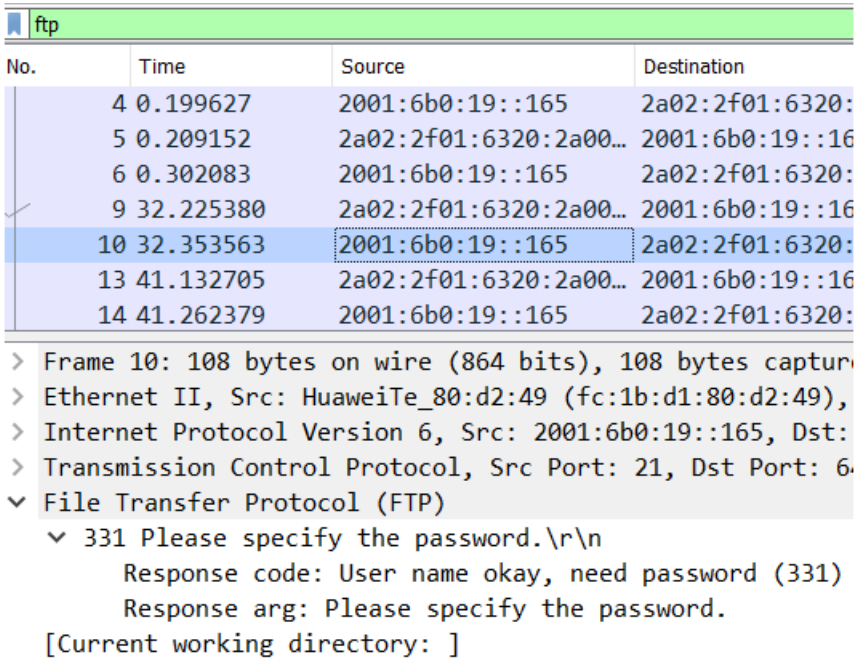
Pentru inceput se verifica doua pachete cerere si doua pachete raspuns pentru a se vedea continutul antetului *File Transfer Protocol (FTP)*, mai exact pachetele de la liniile 9, 10, 13, 14.

9	32.225380	2a02:2f01:6320:2a00…	2001:6b0:19::165	FTP
10	32.353563	2001:6b0:19::165	2a02:2f01:6320:2a00…	FTP
13	41.132705	2a02:2f01:6320:2a00…	2001:6b0:19::165	FTP
14	41.262379	2001:6b0:19::165	2a02:2f01:6320:2a00…	FTP

Linia 9:



Linia 10:



Antetul FTP contine este un mesaj de tip cerere care solicita clientului numele de utilizator al acestuia

Antetul FTP contine un mesaj de tip raspuns care spune ca username-ul este corect si ca are nevoie de parola

Linia 13

```
13 41.132705     2a02:2f01:
14 41.262379     2001:6b0:1

> Frame 13: 87 bytes on wire (696
> Ethernet II, Src: AzureWav_58:0
> Internet Protocol Version 6, Sr
> Transmission Control Protocol,
v File Transfer Protocol (FTP)
  v PASS PAROLA\r\n
      Request command: PASS
      Request arg: PAROLA
  [Current working directory: ]
```

Linia 14

```
14 41.262379     2001:6b0:19::165     2a02:2f01

> Frame 14: 97 bytes on wire (776 bits), 97 bytes ca
> Ethernet II, Src: HuaweiTe_80:d2:49 (fc:1b:d1:80:d
> Internet Protocol Version 6, Src: 2001:6b0:19::165
> Transmission Control Protocol, Src Port: 21, Dst P
v File Transfer Protocol (FTP)
  v 230 Login successful.\r\n
      Response code: User logged in, proceed (230)
      Response arg: Login successful.
  [Current working directory: ]
```

Antetul FTP este de tip cerere si solicita serverului parola (se afiseaza si parola corecta care este PAROLA, cum a fost specificat mai sus)

Antetul FTP contine raspunsul care confirma ca autentificarea a avut loc cu succes

Se continua cu linia 9.

Segmentul TCP este predat nivelului retea in protocolul Internet (Internet Protocol).

```
Transmission Control Protocol, Src Port: 64335, Dst Port: 21, Seq:
    Source Port: 64335
    Destination Port: 21
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 16]
    Sequence Number: 15    (relative sequence number)
    Sequence Number (raw): 2712948859
    [Next Sequence Number: 31    (relative sequence number)]
    Acknowledgment Number: 85    (relative ack number)
    Acknowledgment number (raw): 287814924
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 8108
    [Calculated window size: 8108]
    [Window size scaling factor: 1]
    Checksum: 0xf2b2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (16 bytes)
```

Portul sursa si portul destinatie

Lungimea segmentului TCP

Nivelul de completare a conversatiei: incomplet; conexiunea a fost intrerupta

Lungimea antetului

Pachetului este trimis unei ferestre TCP de 8108 octeți și folosește un factor de scalare (scaling factor) de 1. Dimensiunea reală a ferestrei este de 8108 x 1.

TCP payload detine tot continutul mesajului

Mesajul este transmis mai departe in protocolul internet:

```
> Frame 9: 90 bytes on wire (720 bits), 90 bytes captured (720
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst:
v Internet Protocol Version 6, Src: 2a02:2f01:6320:2a00:ec42:c1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0
    .... 0101 1111 1001 1010 1000 = Flow Label: 0x5f9a8
    Payload Length: 36
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2a02:2f01:6320:2a00:ec42:c134:1b9f:8a4f
    Destination Address: 2001:6b0:19::165
```

Versiunea protocolului internet

Lungimea protocolului payload

Adresele sursa si destinatie

Pentru a se asigura că pachetele IP au o durată de viață limitată în rețea, acestea au un câmp de antet (Hop Limit in acest caz) și o valoare care specifică numărul maxim de hopuri (64 aici) care pot fi parcurse către destinație

Antetul Ethernet II contine adresele hardware sursa si destinatie, precum si tipul protocolului de internet (IPv6).

```
Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
  Destination: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
  Source: AzureWav_58:09:83 (70:66:55:58:09:83)
  Type: IPv6 (0x86dd)
```

Mesajul ajunge in final in frame.

ID-ul interfetei

Numele interfetei

Tipul interfetei (Wi-Fi)

```
Frame 9: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on in
    Interface id: 0 (\Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26})
        Interface name: \Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 22, 2021 20:44:39.207009000 GTB, oră standard
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1640198679.207009000 seconds
    [Time delta from previous captured frame: 31.918711000 seconds]
    [Time delta from previous displayed frame: 31.923297000 seconds]
    [Time since reference or first frame: 32.225380000 seconds]
    Frame Number: 9
    Frame Length: 90 bytes (720 bits)
    Capture Length: 90 bytes (720 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:ftp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

Momentul in care cererea a fost trimisa

Numarul cadrului

Lungimea cadrului

Numarul de octeti capturati

Protocoalele folosite in pachet

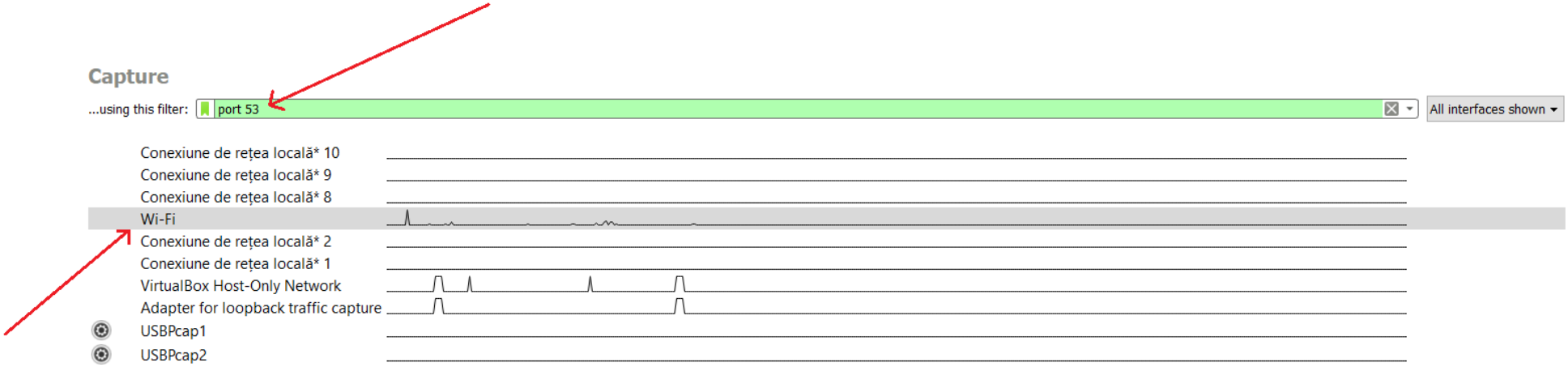
Culoarea pachetului (gri) si filtrul protocolului

TCP tcp

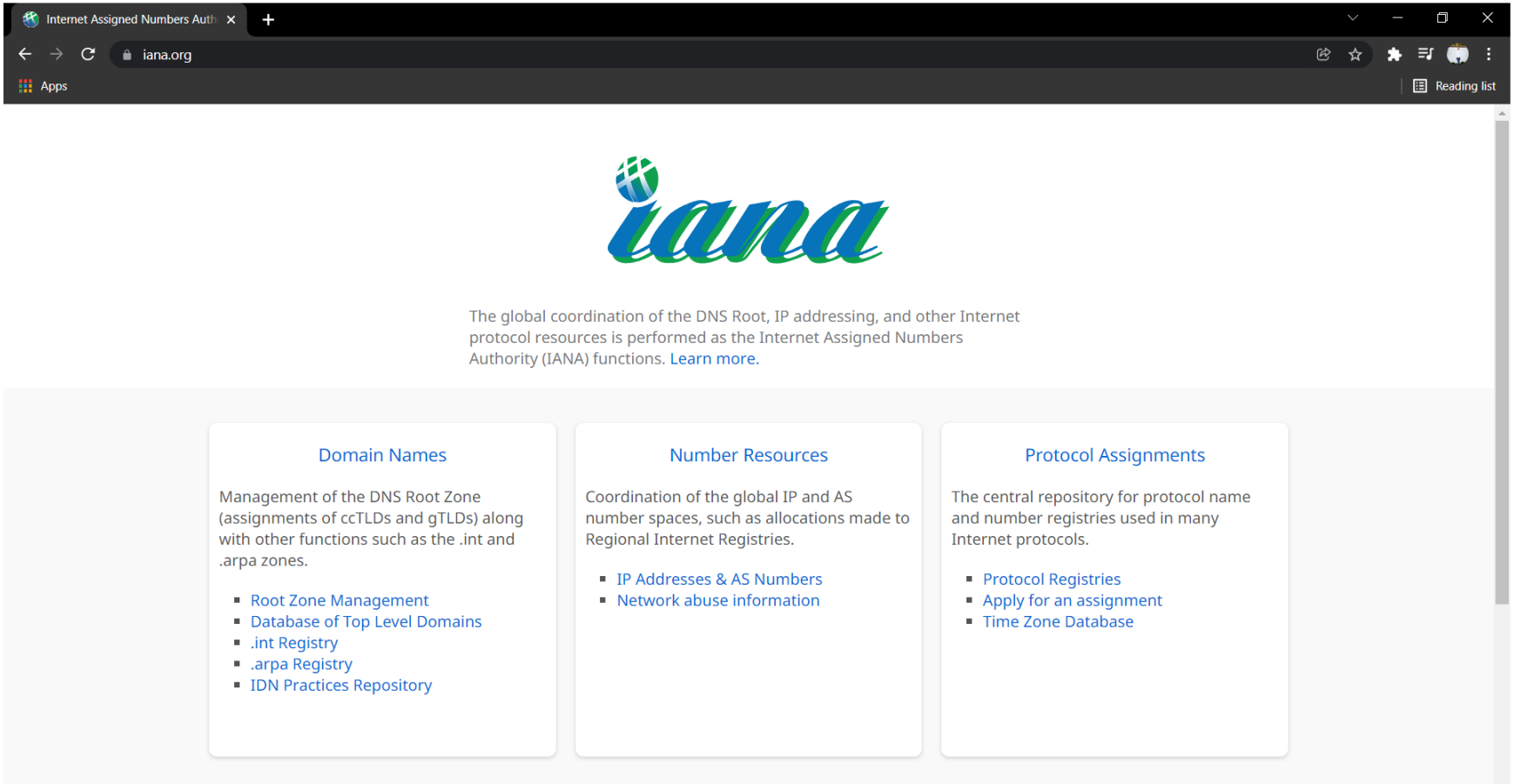
3)DNS

Pentru analiza pachetelor care țin de protocolul DNS se introduce numarul *port 53* in caseta folosita pentru filtrare, 53 fiind portul implicit pentru DNS.

Se alege o interfata de retea pentru a se captura pachetul (in experiment se foloseste Wi-Fi).



Site-ul ales pentru experiment este iana.org.



In acest experiment se acceseaza site-ul din linia de comanda:

Se introduce comanda nslookup (comanda care verifica inregistrarile DNS pe Windows). Comanda este urmata de adresa site-ului ("iana.org") si de server-ul Google DNS 8.8.8.8

```
Microsoft Windows [Version 10.0.19041.685]
(c) 2020 Microsoft Corporation. Toate drepturile rezervate.

C:\Users\gabic>nslookup iana.org 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    iana.org
Addresses:  2001:500:88:200::8
          192.0.43.8


C:\Users\gabic>
```

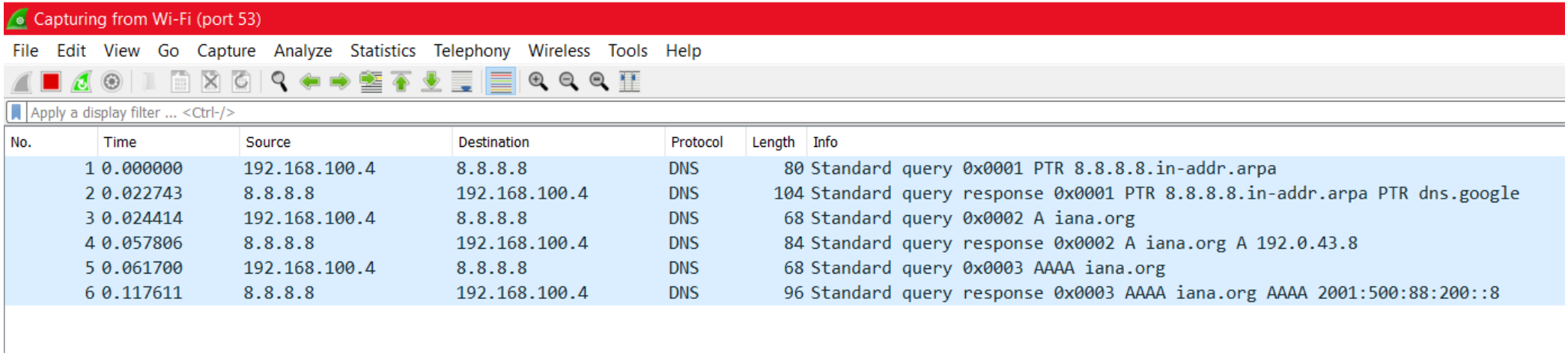
Serverul si adresa server-ului care a raspuns la interogare

Numele site-ului cautat

Adresele ipv6 si ipv4

Protocolul DNS folosește UDP ca protocol de transport.

In Wireshark se observa protocoalele DNS, filtrate cu portul 53:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
2	0.022743	8.8.8.8	192.168.100.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
3	0.024414	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0002 A iana.org
4	0.057806	8.8.8.8	192.168.100.4	DNS	84	Standard query response 0x0002 A iana.org A 192.0.43.8
5	0.061700	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0003 AAAA iana.org
6	0.117611	8.8.8.8	192.168.100.4	DNS	96	Standard query response 0x0003 AAAA iana.org AAAA 2001:500:88:200::8

In experiment se lucreaza cu pachete tip cerere si raspuns.

Se gasesc doua tipuri de perechi cerere – raspuns:

Mesaj care trimite o interogare (query) server-ului Google
si mesaj care primeste raspuns de la server

Capturing from Wi-Fi (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
2	0.022743	8.8.8.8	192.168.100.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
3	0.024414	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0002 A iana.org
4	0.057806	8.8.8.8	192.168.100.4	DNS	84	Standard query response 0x0002 A iana.org A 192.0.43.8
5	0.061700	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0003 AAAA iana.org
6	0.117611	8.8.8.8	192.168.100.4	DNS	96	Standard query response 0x0003 AAAA iana.org AAAA 2001:500:88:200::8

Mesaj care trimite o interogare (query) site-ul ales (iana.org)
si mesaj care primeste raspuns de la site

In experiment se analizeaza mesajele trimise catre iana.org.

Pachet de tip cerere/interogare

Se selecteaza al treilea pachet, cel de tip cerere (request). Se despacheteaza pentru a i se observa continutul.

Sectiunea *Domain Name System (DNS)* afiseaza continutul pachetului.

Cand este expandat randul, se vor afisa urmatoarele:

*Wi-Fi (port 53)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
2	0.022743	8.8.8.8	192.168.100.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
3	0.024414	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0002 A iana.org
4	0.057806	8.8.8.8	192.168.100.4	DNS	84	Standard query response 0x0002 A iana.org A 192.0.43.8
5	0.061700	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0003 AAAA iana.org

```
> Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26}, id 0
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 63782, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > iana.org: type A, class IN
    [Response In: 4]
```

Antetul DNS care contine un mesaj de tip interogare (query)

ID-ul de tranzacție (Transaction ID)
Pachetul selectat are acelasi ID de tranzacție cu cel de raspuns.
Tranzactiile celor doua pachete se potrivesc (ambele sunt 0x0002).
Acelasi caz si la pachetele cerere - respuns catre serverul Google 8.8.8.8, doar ca ID-ul lor este 0x0001.
Asa se pot uni interogarile cu raspunsurile.

Flag-ul care este activ semnifica faptul ca interogatia ii cere serverului sa caute recursiv in alte servere raspunsul

Numarul de intrebari (Questions) furnizează numărul de solicitări care sunt trimise în segmentul de interogări DNS.
În cazul de față este 1.

Raspunsul interogarii se afla la linia 4

4	0.057806	8.8.8.8	192.168.100.4	DNS	84	Standard query response 0x0002 A iana.org A 192.0.43.8

```
0020  08 08 f9 26 00 35 00 22  33 3f 00 02 01 00 00 01   ···&·5·" 3?·····
0030  00 00 00 00 00 00 04 69  61 6e 61 03 6f 72 67 00   ·******i ana·org·
```

UDP transforma mesajul intr-o datagrama in protocolul *User Datagram Protocol*.

```
> Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{E46FD
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 8.8.8.8
v User Datagram Protocol, Src Port: 63782, Dst Port: 53
    Source Port: 63782
    Destination Port: 53
    Length: 34
    Checksum: 0x333f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (26 bytes)
> Domain Name System (query)
```

Numarul portului sursa: 63782

Numarul portului destinatie: 53, portul implicit DNS

Acest câmp specifică lungimea în octeți a antetului și a datelor UDP

UDP payload reprezinta corpul pachetului unde se gaseste tot continutul mesajului din protocolul DNS

Mesajul este predat nivelului retea in protocolul Internet (Internet Protocol).

```
> Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{E46FD255-
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
v Internet Protocol Version 4, Src: 192.168.100.4, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 54
    Identification: 0xa0bc (41148)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x653e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.100.4
    Destination Address: 8.8.8.8
> User Datagram Protocol, Src Port: 63782, Dst Port: 53
> Domain Name System (query)
```

Versiunea protocolului

Lungimea antetului

Lungimea totala a mesajului

Reprezinta cantitatea de timp în care pachetul este setat să existe în interiorul rețelei înainte de a fi aruncat de către router

Numărul de protocol pentru UDP

Adresa IP a sursei

Adresa IP a destinatiei

In antetul *Ethernet II* se pot vedea adresele hardware (sursa si destinatie). Se pot identifica producatorii echipamentelor.

Versiunea Protocolului Internet

```
> Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{E46FD25
v Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
    > Destination: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
    > Source: AzureWav_58:09:83 (70:66:55:58:09:83)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 63782, Dst Port: 53
> Domain Name System (query)
```

In final, mesajul ajunge in cadru (frame).

Id-ul interfetei

Tipul de antet al legaturii pachetului

Momentul in care a fost trimisa interogarea

Numarul cadrului

Lungimea cadrului

Numarul de biti capturati

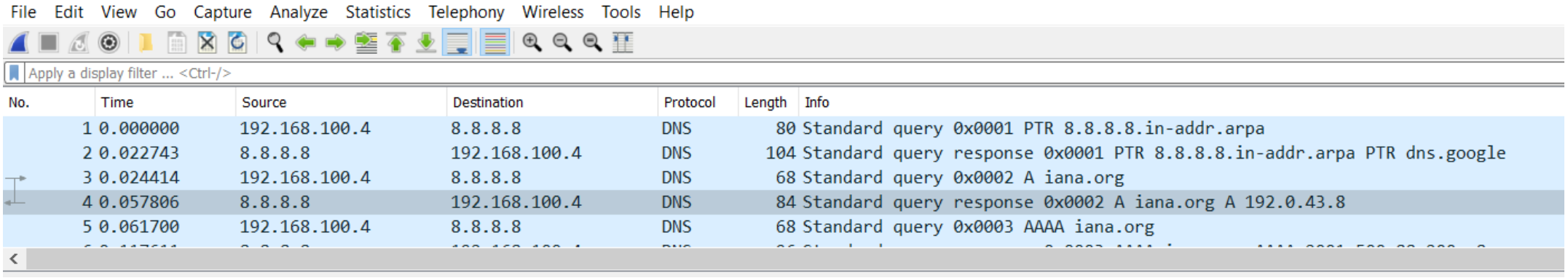
Protocoalele folosite in cadru

Culoarea pachetului care este albastru deschis

```
Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{E46FD255-0
  Interface id: 0 (\Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26})
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec 21, 2021 16:13:33.997692000 GTB, oră standard
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1640096013.997692000 seconds
  [Time delta from previous captured frame: 0.001671000 seconds]
  [Time delta from previous displayed frame: 0.001671000 seconds]
  [Time since reference or first frame: 0.024414000 seconds]
  Frame Number: 3
  Frame Length: 68 bytes (544 bits)
  Capture Length: 68 bytes (544 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 63782, Dst Port: 53
> Domain Name System (query)
```

Pachet de tip raspuns:

Se selecteaza al patrulea pachet, cel de tip raspuns. Se despacheteaza pentru a i se observa continutul.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
2	0.022743	8.8.8.8	192.168.100.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
3	0.024414	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0002 A iana.org
4	0.057806	8.8.8.8	192.168.100.4	DNS	84	Standard query response 0x0002 A iana.org A 192.0.43.8
5	0.061700	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0003 AAAA iana.org

Sectiunea *Domain Name System (DNS)* afiseaza continutul raspunsului:

ID-ul de tranzacție (Transaction ID). Raspunsul are acelasi ID de tranzacție ca si interogarea (0x0002).

```
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was no
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        iana.org: type A, class IN
    Answers
        iana.org: type A, class IN, addr 192.0.43.8
    [Request In: 3]
    [Time: 0.033392000 seconds]
```

Flag-ul arata ca mesajul pachetului este de tip raspuns

Flag-ul reprezinta o cerere catre server care ii cere sa caute recursiv in alte servere raspunsul

Flag-ul reprezinta un raspuns. Raspunsul se poate cauta recursiv

Numarul de interogari (este 1)

Raspunsul interogarii: Numărul de intrări din lista de înregistrare a resurselor de răspuns (RRs = Resource Record) care au fost returnate

Interogarea

Raspunsul interogarii, returneaza adresa site-ului

Cererea se afla la randul 3

3	0.024414	192.168.100.4	8.8.8.8	DNS	68	Standard query 0x0002 A iana.org

Mai departe, adresa sursa si adresa destinatie se inverseaza; interogatia este trimisa catre destinatie, iar mesajul raspuns este trimis la sursa, care devine noua destinatie, dupa cum se observa:

Interogare

```
> Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{E46FD255
> Ethernet II, Src: AzureWav_58:09:83 (70:66:55:58:09:83), Dst: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49)
> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 63782, Dst Port: 53
> Domain Name System (query)
```

Raspuns

```
> Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{E46FD2
> Ethernet II, Src: HuaweiTe_80:d2:49 (fc:1b:d1:80:d2:49), Dst: AzureWav_58:09:83 (70:66:55:58:09:83)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.100.4
> User Datagram Protocol, Src Port: 53, Dst Port: 63782
> Domain Name System (response)
```

In final, mesajul ajunge in cadru (frame).

Numarul cadrului

Numarul de octeti trimisi

Numele interfetei

ID-ul interfetei

```
> Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{E46FD255-014D-41FE-B9A8-86EE4734FA26}, id 0
```

Numarul de octeti capturati