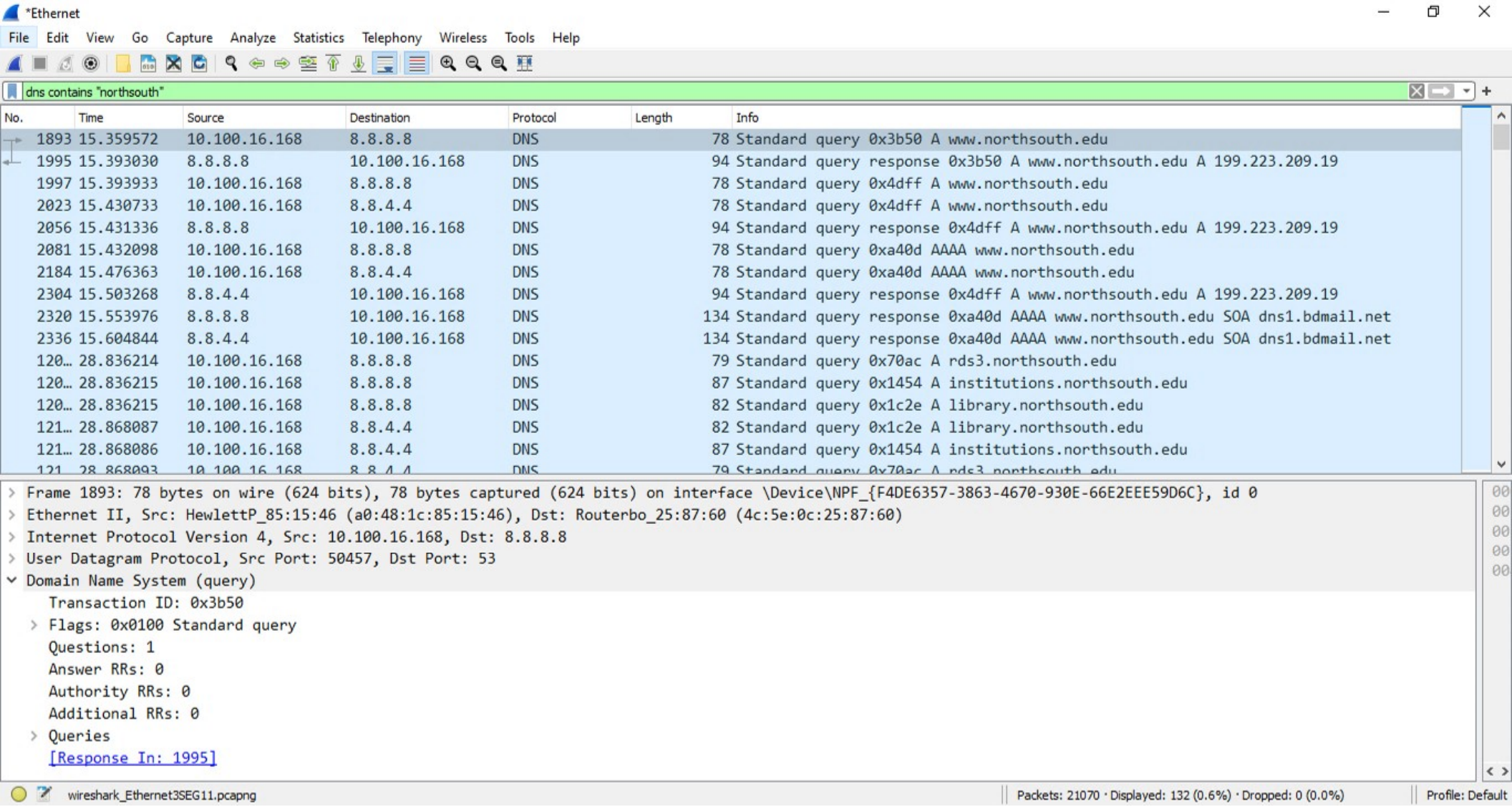
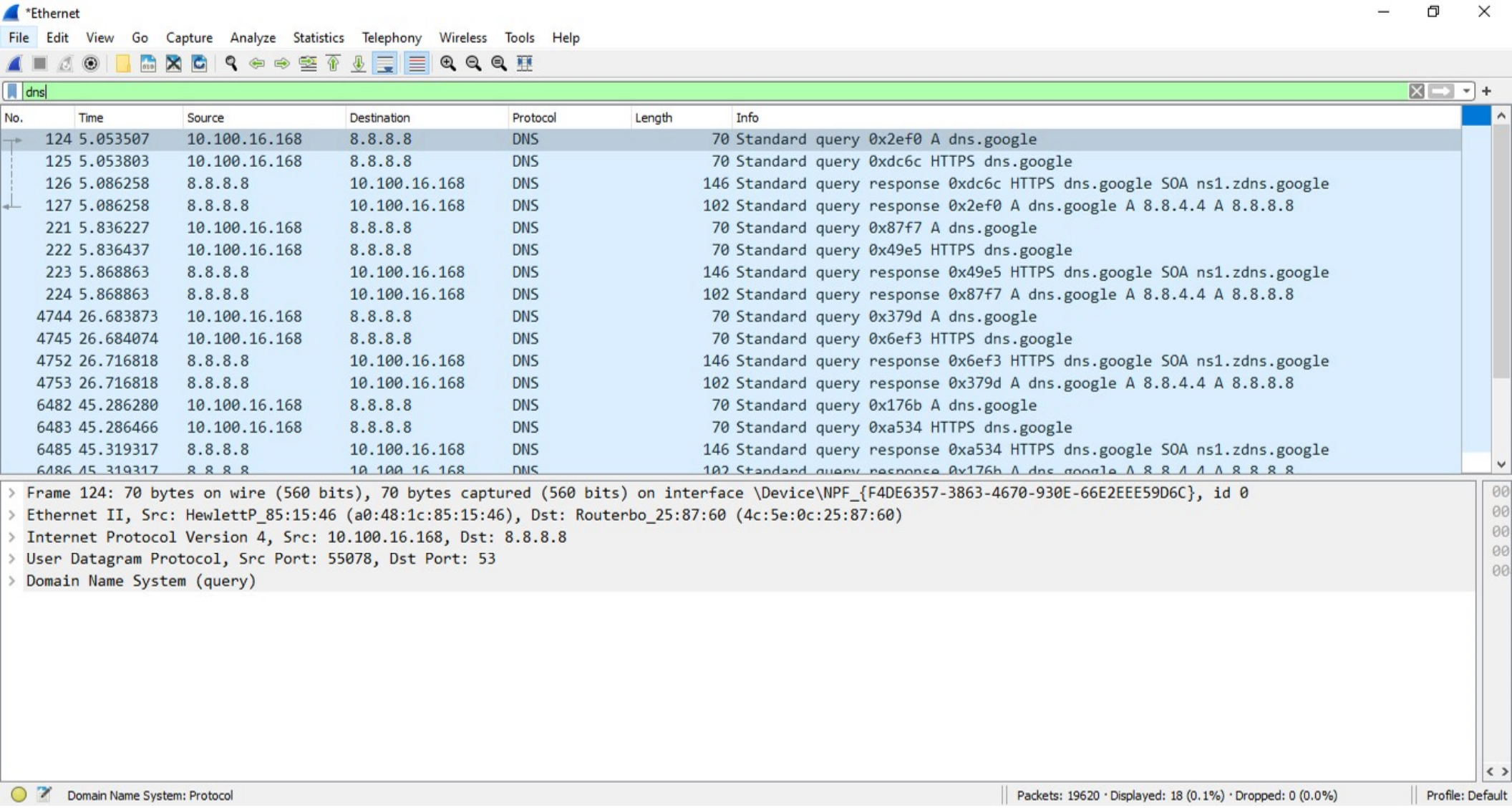
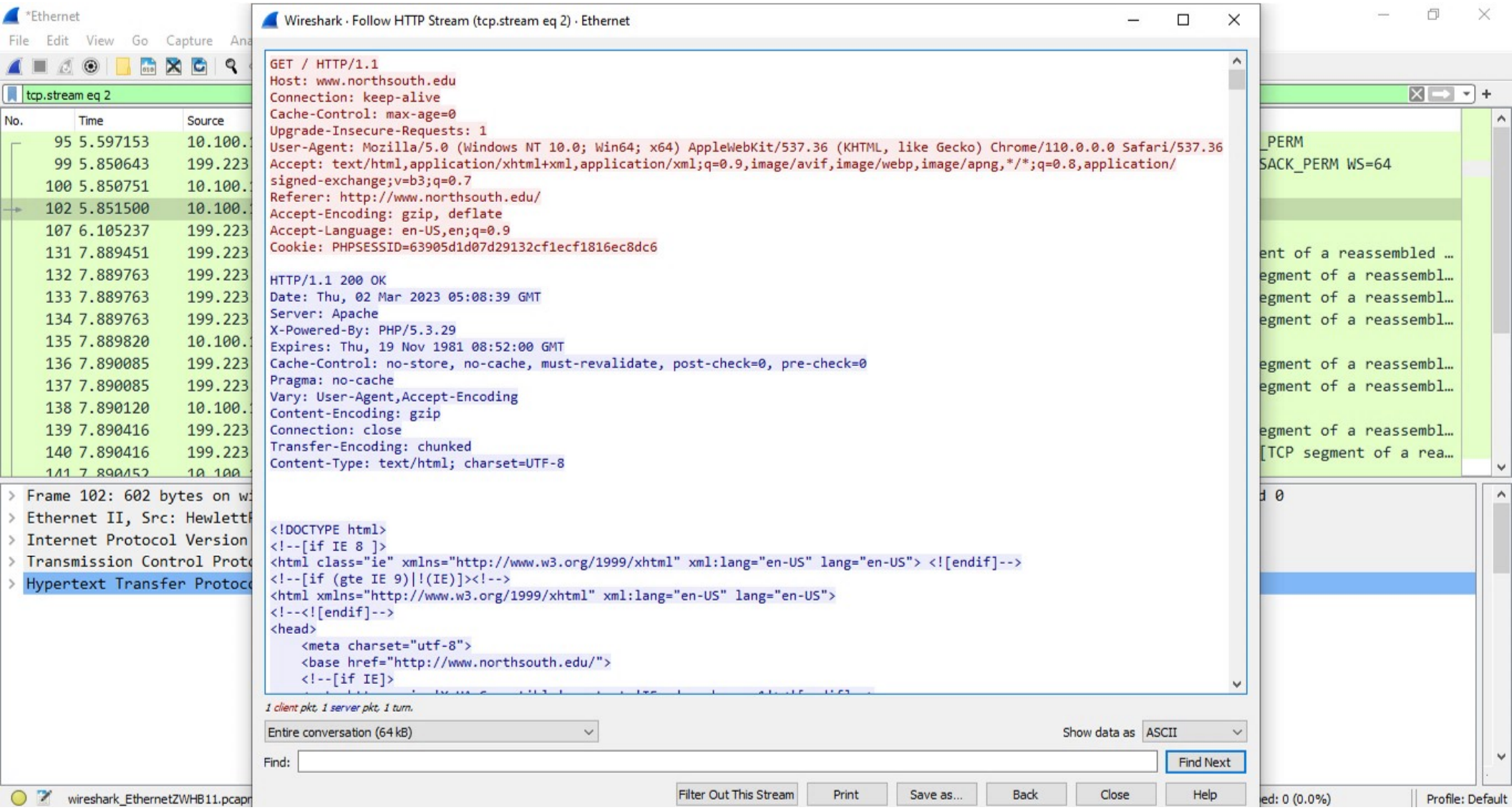
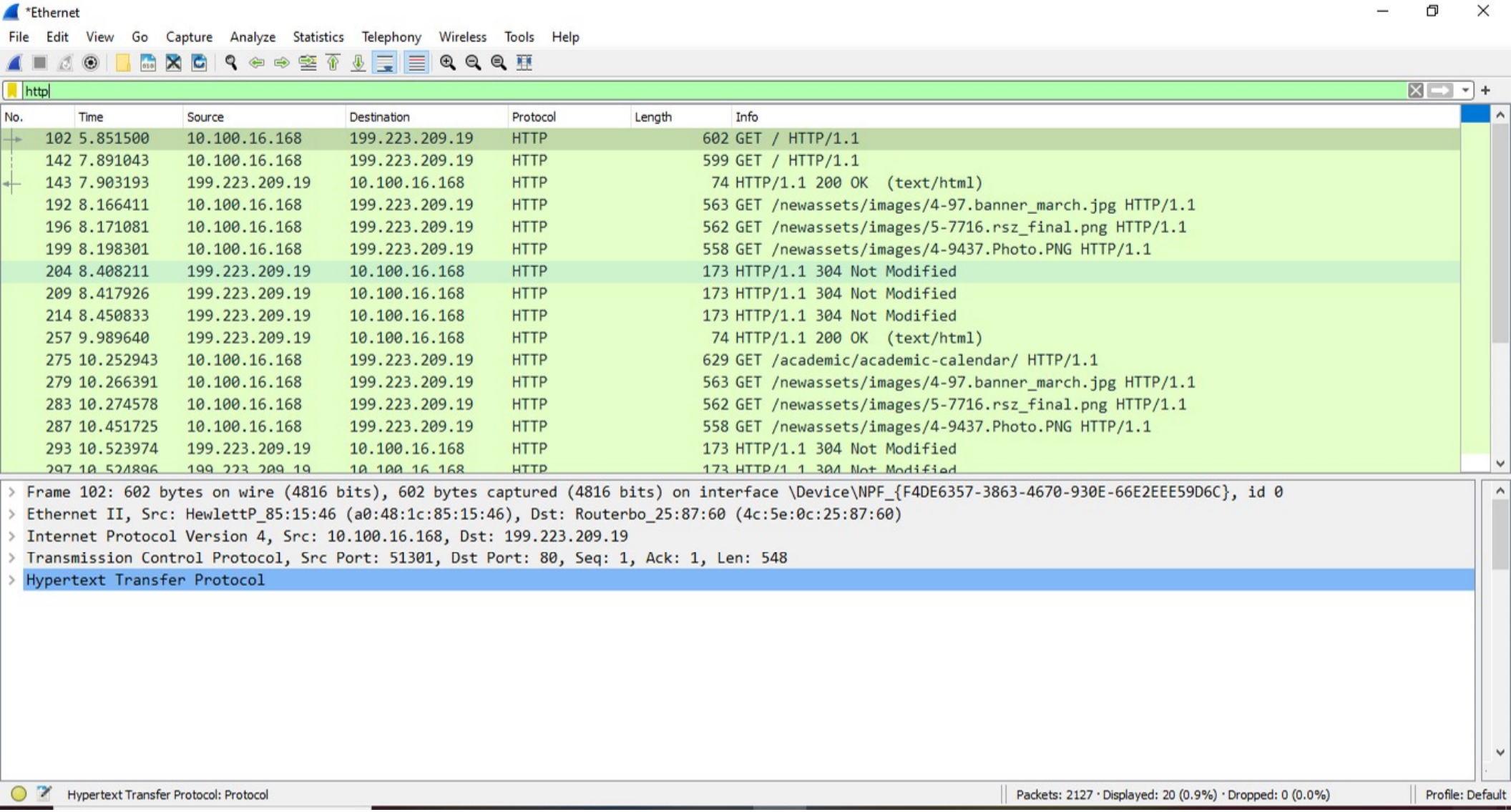
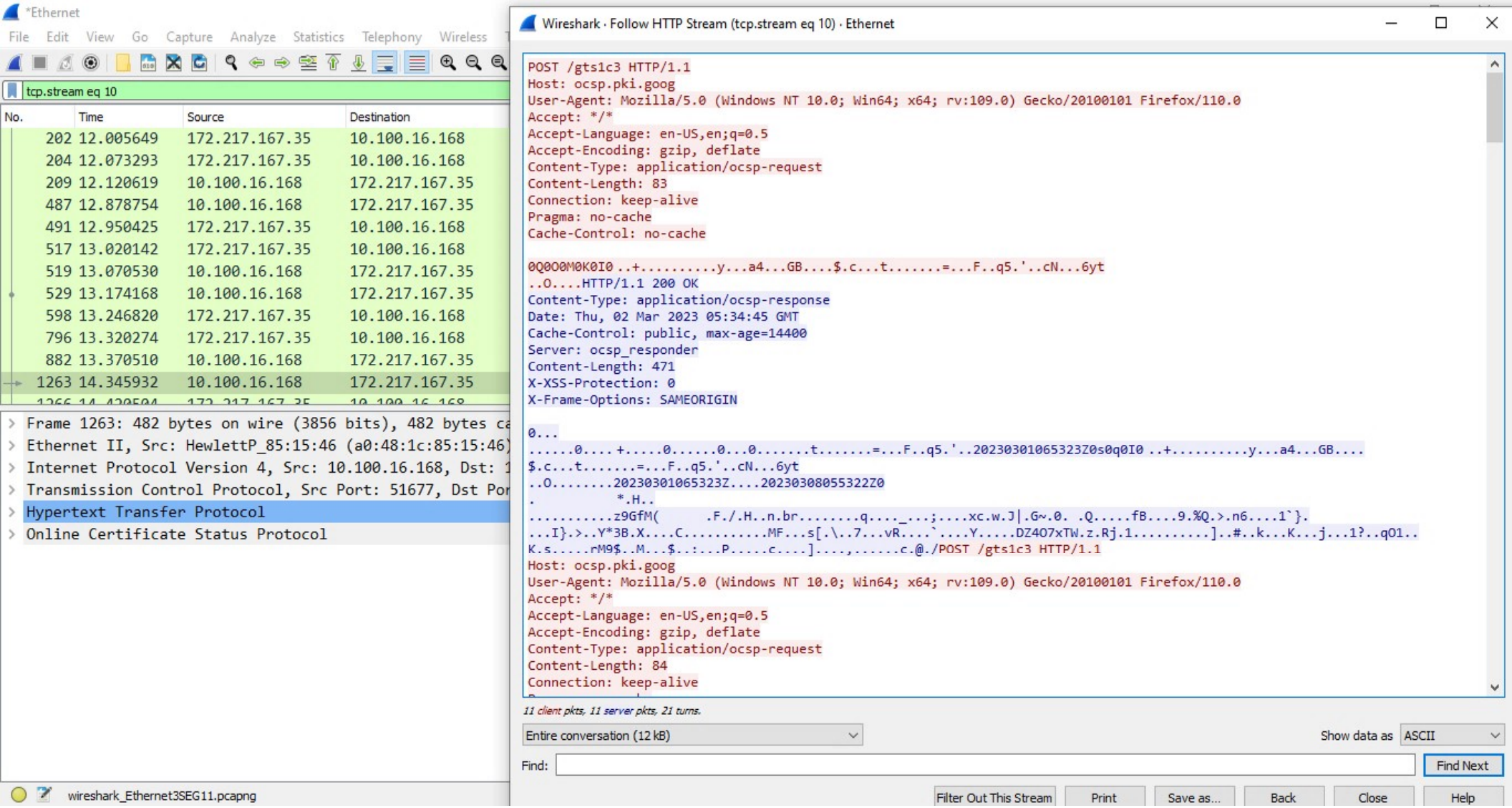
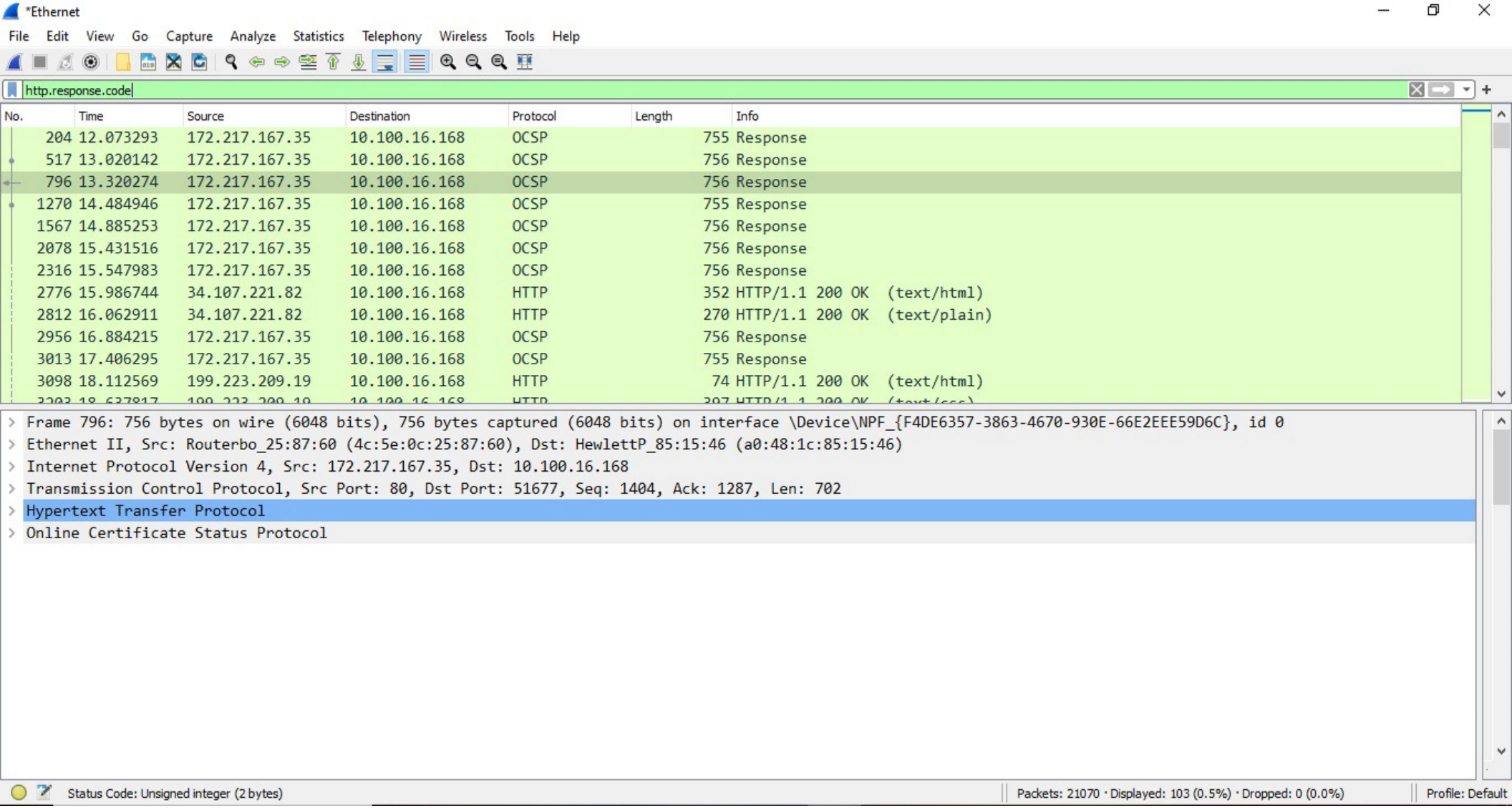

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns contains "northsouth"
No. Time Source Destination Protocol Length Info
1893 15.359572 10.100.16.168 8.8.8.8 DNS 78 Standard query 0x3b50 A www.northsouth.edu
1995 15.393030 8.8.8.8 10.100.16.168 DNS 94 Standard query response 0x3b50 A www.northsouth.edu A 199.223.209.19
1997 15.393933 10.100.16.168 8.8.8.8 DNS 78 Standard query 0x4dff A www.northsouth.edu
2023 15.430733 10.100.16.168 8.8.4.4 DNS 78 Standard query 0x4dff A www.northsouth.edu
2056 15.431336 8.8.8.8 10.100.16.168 DNS 94 Standard query response 0x4dff A www.northsouth.edu A 199.223.209.19
2081 15.432098 10.100.16.168 8.8.8.8 DNS 78 Standard query 0xa40d AAAA www.northsouth.edu
2184 15.476363 10.100.16.168 8.8.4.4 DNS 78 Standard query 0xa40d AAAA www.northsouth.edu
2304 15.503268 8.8.4.4 10.100.16.168 DNS 94 Standard query response 0x4dff A www.northsouth.edu A 199.223.209.19
2320 15.553976 8.8.8.8 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
2336 15.604844 8.8.4.4 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
120… 28.836214 10.100.16.168 8.8.8.8 DNS 79 Standard query 0x70ac A rds3.northsouth.edu
120… 28.836215 10.100.16.168 8.8.8.8 DNS 87 Standard query 0x1454 A institutions.northsouth.edu
120… 28.836215 10.100.16.168 8.8.8.8 DNS 82 Standard query 0x1c2e A library.northsouth.edu
121… 28.868087 10.100.16.168 8.8.4.4 DNS 82 Standard query 0x1c2e A library.northsouth.edu
121… 28.868086 10.100.16.168 8.8.4.4 DNS 87 Standard query 0x1454 A institutions.northsouth.edu
Frame 1893: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: HewlettP_85:15:46 (a0:48:1c:85:15:46), Dst: Routerbo_25:87:60 (4c:5e:0c:25:87:60)
Internet Protocol Version 4, Src: 10.100.16.168, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 50457, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x3b50
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 1995]
wireshark_Ethernet3SEG11.pcapng
Packets: 21070 · Displayed: 132 (0.6%) · Dropped: 0 (0.0%)
Profile: Default

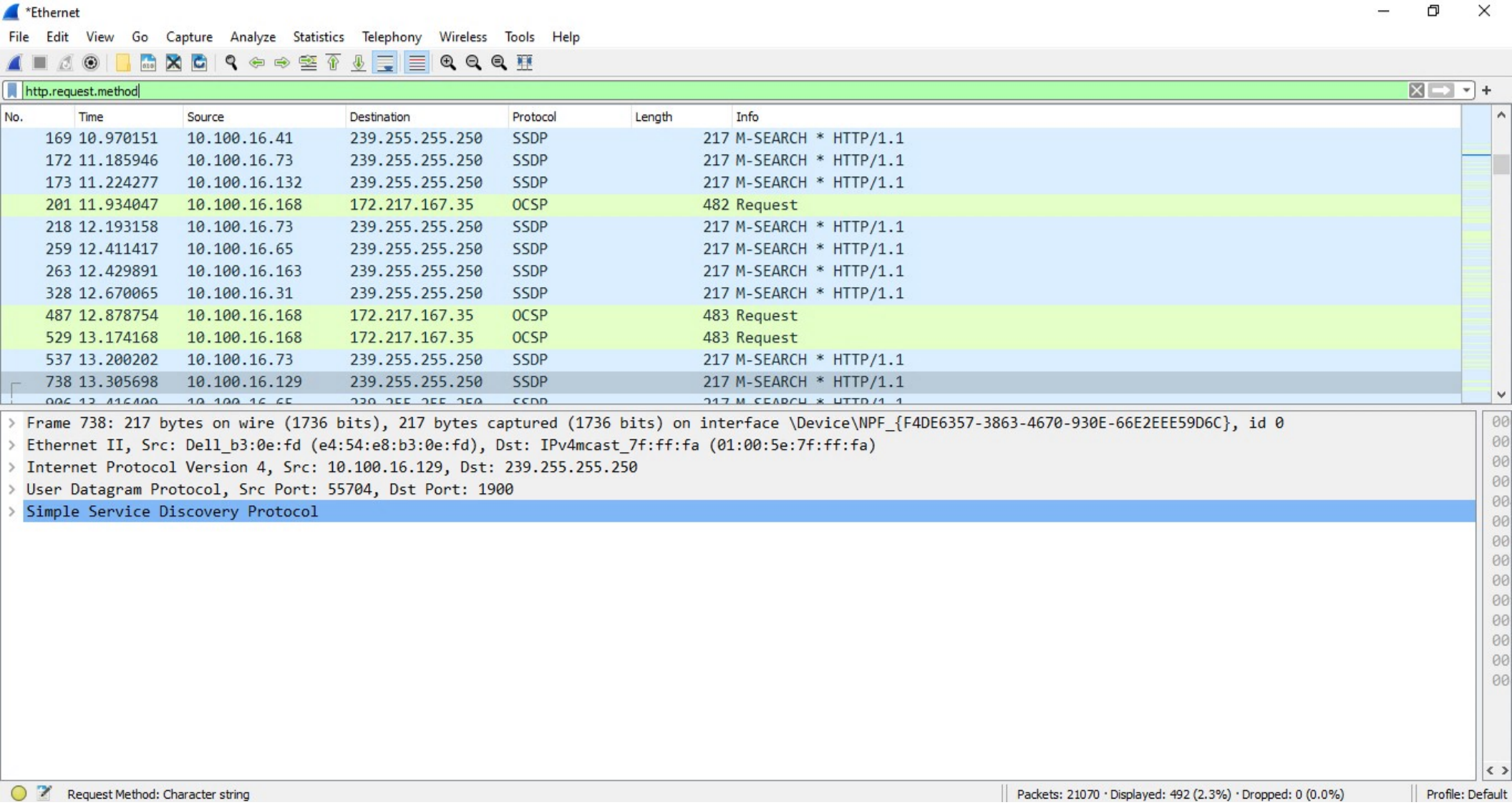

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
124 5.053507 10.100.16.168 8.8.8.8 DNS 70 Standard query 0x2ef0 A dns.google
125 5.053803 10.100.16.168 8.8.8.8 DNS 70 Standard query 0xdc6c HTTPS dns.google
126 5.086258 8.8.8.8 10.100.16.168 DNS 146 Standard query response 0xdc6c HTTPS dns.google SOA ns1.zdns.google
127 5.086258 8.8.8.8 10.100.16.168 DNS 102 Standard query response 0x2ef0 A dns.google A 8.8.4.4 A 8.8.8.8
221 5.836227 10.100.16.168 8.8.8.8 DNS 70 Standard query 0x87f7 A dns.google
222 5.836437 10.100.16.168 8.8.8.8 DNS 70 Standard query 0x49e5 HTTPS dns.google
223 5.868863 8.8.8.8 10.100.16.168 DNS 146 Standard query response 0x49e5 HTTPS dns.google SOA ns1.zdns.google
224 5.868863 8.8.8.8 10.100.16.168 DNS 102 Standard query response 0x87f7 A dns.google A 8.8.4.4 A 8.8.8.8
4744 26.683873 10.100.16.168 8.8.8.8 DNS 70 Standard query 0x379d A dns.google
4745 26.684074 10.100.16.168 8.8.8.8 DNS 70 Standard query 0x6ef3 HTTPS dns.google
4752 26.716818 8.8.8.8 10.100.16.168 DNS 146 Standard query response 0x6ef3 HTTPS dns.google SOA ns1.zdns.google
4753 26.716818 8.8.8.8 10.100.16.168 DNS 102 Standard query response 0x379d A dns.google A 8.8.4.4 A 8.8.8.8
6482 45.286280 10.100.16.168 8.8.8.8 DNS 70 Standard query 0x176b A dns.google
6483 45.286466 10.100.16.168 8.8.8.8 DNS 70 Standard query 0xa534 HTTPS dns.google
6485 45.319317 8.8.8.8 10.100.16.168 DNS 146 Standard query response 0xa534 HTTPS dns.google SOA ns1.zdns.google
Frame 124: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: HewlettP_85:15:46 (a0:48:1c:85:15:46), Dst: Routerbo_25:87:60 (4c:5e:0c:25:87:60)
Internet Protocol Version 4, Src: 10.100.16.168, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 55078, Dst Port: 53
Domain Name System (query)
Domain Name System: Protocol
Packets: 19620 · Displayed: 18 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

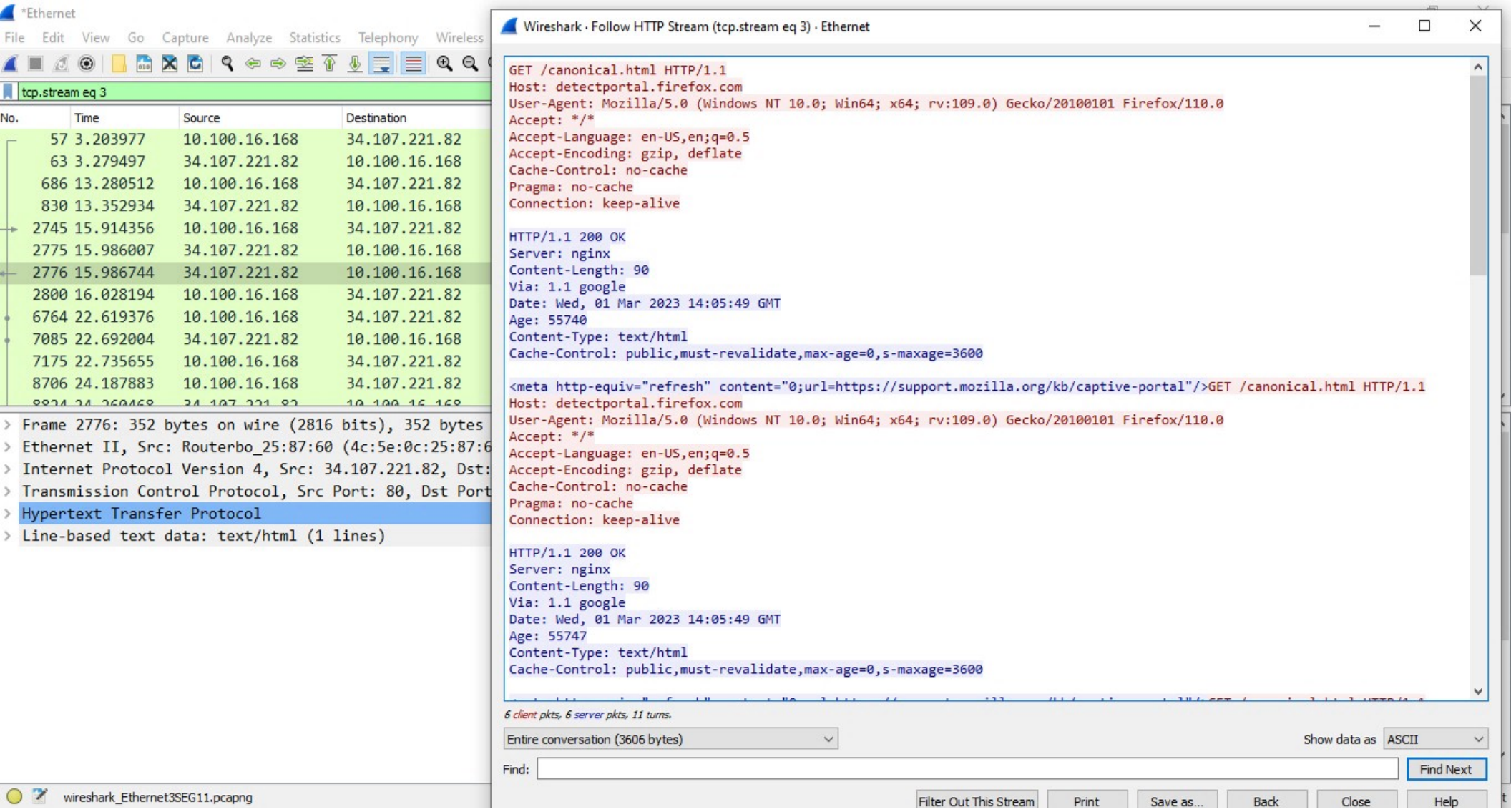

*Ethernet
File Edit View Go Capture Ana
tcp.stream eq 2
No. Time Source
95 5.597153 10.100.
99 5.850643 199.223
100 5.850751 10.100.
102 5.851500 10.100.
107 6.105237 199.223
131 7.889451 199.223
132 7.889763 199.223
133 7.889763 199.223
134 7.889763 199.223
135 7.889820 10.100.
136 7.890085 199.223
137 7.890085 199.223
138 7.890120 10.100.
139 7.890416 199.223
140 7.890416 199.223
Frame 102: 602 bytes on wi
Ethernet II, Src: HewlettP
Internet Protocol Version
Transmission Control Proto
Hypertext Transfer Protoco
wireshark_EthernetZWHB11.pcapn
_PERM
SACK_PERM WS=64
ent of a reassembled …
egment of a reassembl…
egment of a reassembl…
egment of a reassembl…
egment of a reassembl…
egment of a reassembl…
egment of a reassembl…
[TCP segment of a rea…
d 0
ed: 0 (0.0%)
Profile: Default
Wireshark · Follow HTTP Stream (tcp.stream eq 2) · Ethernet
GET / HTTP/1.1
Host: www.northsouth.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Referer: http://www.northsouth.edu/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=63905d1d07d29132cf1ecf1816ec8dc6
HTTP/1.1 200 OK
Date: Thu, 02 Mar 2023 05:08:39 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: User-Agent,Accept-Encoding
Content-Encoding: gzip
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<!--[if IE 8]>
<html class="ie" xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-US" lang="en-US"> <![endif]-->
<!--[if (gte IE 9)|!(IE)]><!-->
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-US" lang="en-US">
<!--<![endif]-->
<head>
<meta charset="utf-8">
<base href="http://www.northsouth.edu/">
<!--[if IE]>
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (64 kB)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

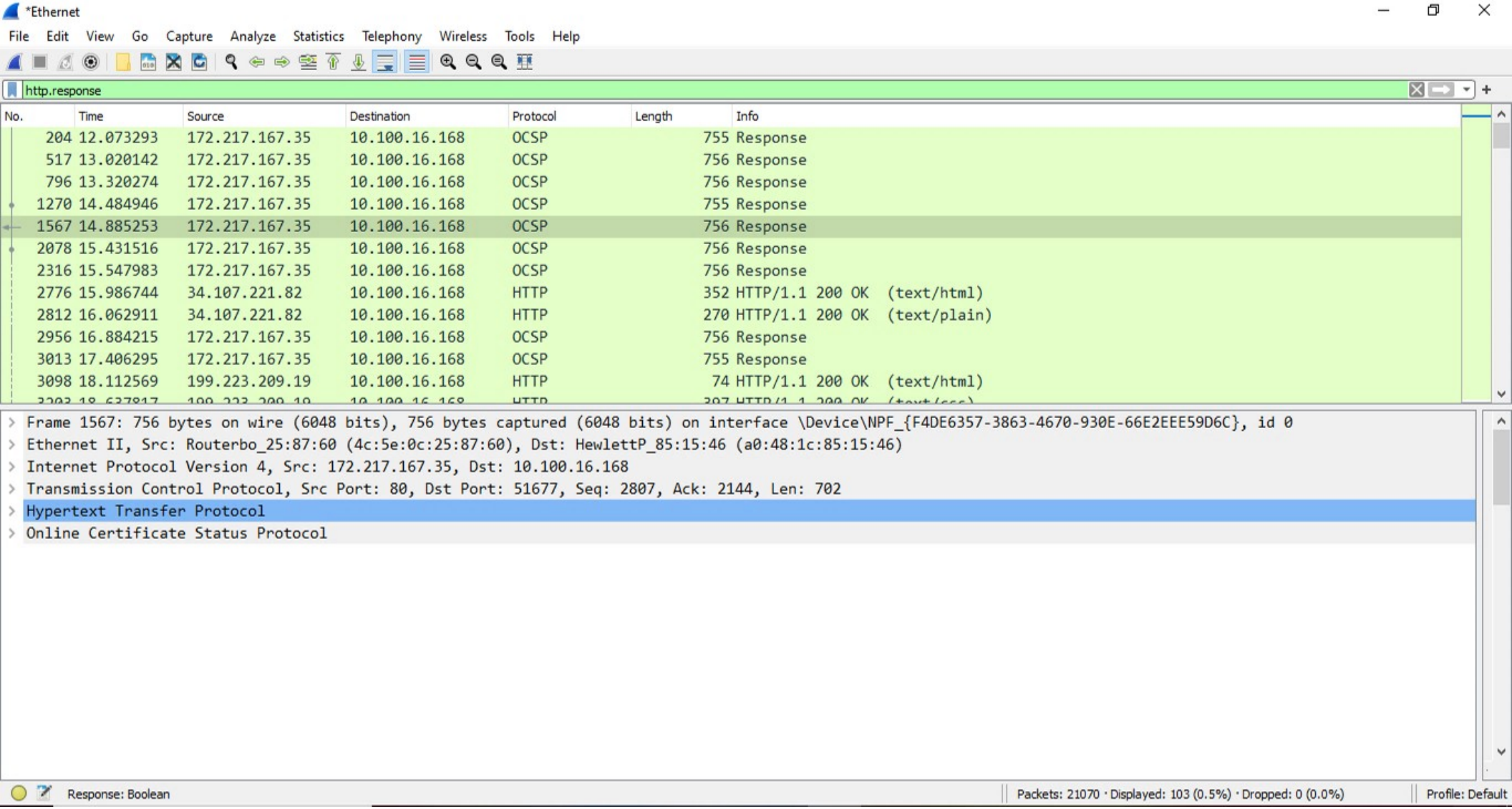

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
102 5.851500 10.100.16.168 199.223.209.19 HTTP 602 GET / HTTP/1.1
142 7.891043 10.100.16.168 199.223.209.19 HTTP 599 GET / HTTP/1.1
143 7.903193 199.223.209.19 10.100.16.168 HTTP 74 HTTP/1.1 200 OK (text/html)
192 8.166411 10.100.16.168 199.223.209.19 HTTP 563 GET /newassets/images/4-97.banner_march.jpg HTTP/1.1
196 8.171081 10.100.16.168 199.223.209.19 HTTP 562 GET /newassets/images/5-7716.rsz_final.png HTTP/1.1
199 8.198301 10.100.16.168 199.223.209.19 HTTP 558 GET /newassets/images/4-9437.Photo.PNG HTTP/1.1
204 8.408211 199.223.209.19 10.100.16.168 HTTP 173 HTTP/1.1 304 Not Modified
209 8.417926 199.223.209.19 10.100.16.168 HTTP 173 HTTP/1.1 304 Not Modified
214 8.450833 199.223.209.19 10.100.16.168 HTTP 173 HTTP/1.1 304 Not Modified
257 9.989640 199.223.209.19 10.100.16.168 HTTP 74 HTTP/1.1 200 OK (text/html)
275 10.252943 10.100.16.168 199.223.209.19 HTTP 629 GET /academic/academic-calendar/ HTTP/1.1
279 10.266391 10.100.16.168 199.223.209.19 HTTP 563 GET /newassets/images/4-97.banner_march.jpg HTTP/1.1
283 10.274578 10.100.16.168 199.223.209.19 HTTP 562 GET /newassets/images/5-7716.rsz_final.png HTTP/1.1
287 10.451725 10.100.16.168 199.223.209.19 HTTP 558 GET /newassets/images/4-9437.Photo.PNG HTTP/1.1
293 10.523974 199.223.209.19 10.100.16.168 HTTP 173 HTTP/1.1 304 Not Modified
Frame 102: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: HewlettP_85:15:46 (a0:48:1c:85:15:46), Dst: Routerbo_25:87:60 (4c:5e:0c:25:87:60)
Internet Protocol Version 4, Src: 10.100.16.168, Dst: 199.223.209.19
Transmission Control Protocol, Src Port: 51301, Dst Port: 80, Seq: 1, Ack: 1, Len: 548
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol
Packets: 2127 · Displayed: 20 (0.9%) · Dropped: 0 (0.0%)
Profile: Default

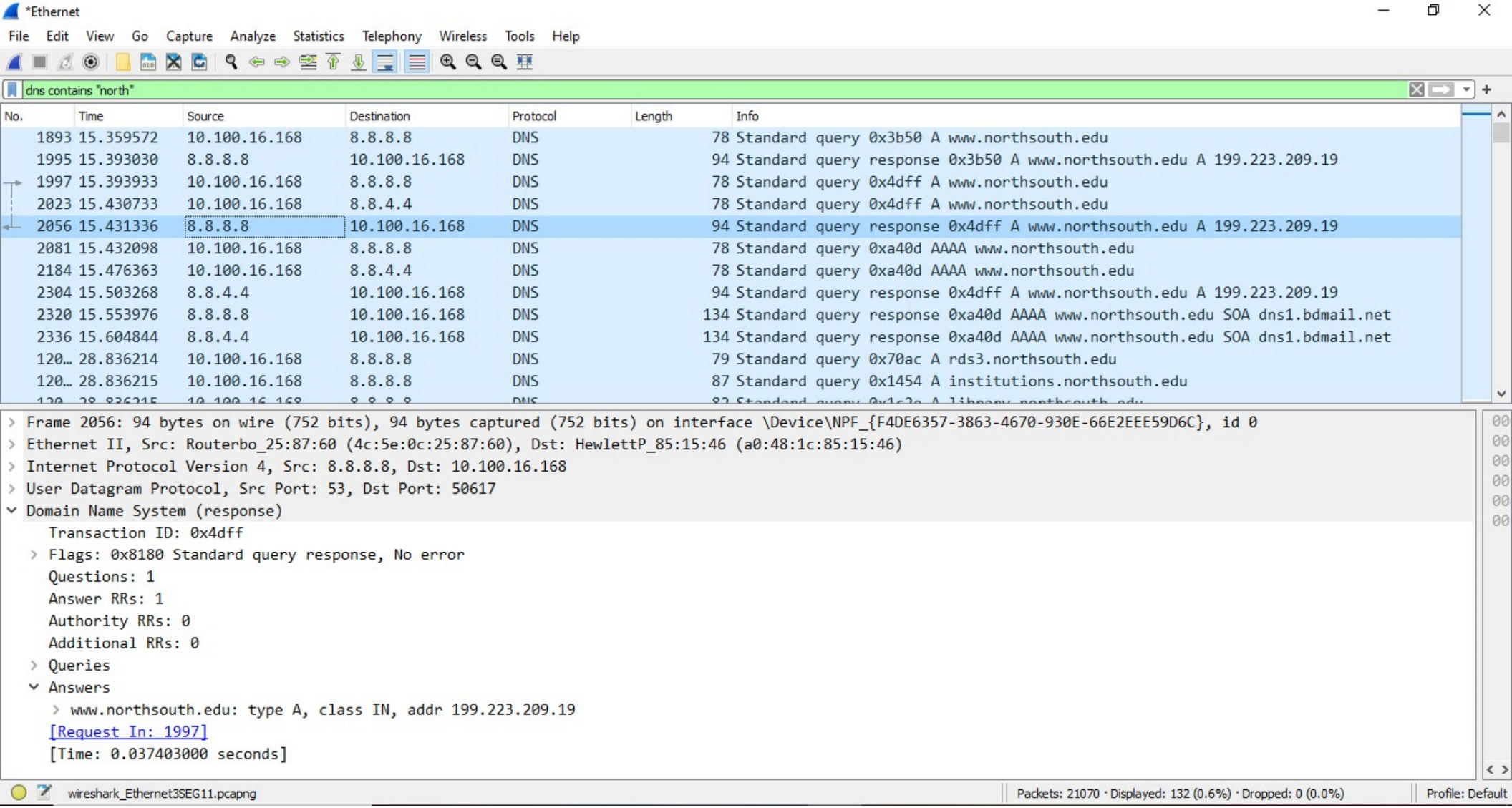

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless
tcp.stream eq 10
No. Time Source Destination
202 12.005649 172.217.167.35 10.100.16.168
204 12.073293 172.217.167.35 10.100.16.168
209 12.120619 10.100.16.168 172.217.167.35
487 12.878754 10.100.16.168 172.217.167.35
491 12.950425 172.217.167.35 10.100.16.168
517 13.020142 172.217.167.35 10.100.16.168
519 13.070530 10.100.16.168 172.217.167.35
529 13.174168 10.100.16.168 172.217.167.35
598 13.246820 172.217.167.35 10.100.16.168
796 13.320274 172.217.167.35 10.100.16.168
882 13.370510 10.100.16.168 172.217.167.35
1263 14.345932 10.100.16.168 172.217.167.35
Frame 1263: 482 bytes on wire (3856 bits), 482 bytes ca
Ethernet II, Src: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 10.100.16.168, Dst: 1
Transmission Control Protocol, Src Port: 51677, Dst Por
Hypertext Transfer Protocol
Online Certificate Status Protocol
wireshark_Ethernet3SEG11.pcapng
Wireshark · Follow HTTP Stream (tcp.stream eq 10) · Ethernet
POST /gts1c3 HTTP/1.1
Host: ocsp.pki.goog
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
0Q0O0M0K0I0 ..+.....y...a4...GB....$.c...t.....=...F..q5.'..cN...6yt
..O....HTTP/1.1 200 OK
Content-Type: application/ocsp-response
Date: Thu, 02 Mar 2023 05:34:45 GMT
Cache-Control: public, max-age=14400
Server: ocsp_responder
Content-Length: 471
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
0...
.....0....+.....0.....0...0.....t.....=...F..q5.'..20230301065323Z0s0q0I0 ..+.....y...a4...GB....
$.c...t.....=...F..q5.'..cN...6yt
..O.....20230301065323Z....20230308055322Z0
. *.H..
.....z9GfM(.F./.H..n.br.....q...._...;....xc.w.J|.G~.0. .Q.....fB....9.%Q.>.n6....1`}.
...I}.>..Y*3B.X....C.....MF...s[.\..7...vR....`....Y.....DZ4O7xTW.z.Rj.1.....]..#..k...K...j...1?..qO1..
K.s.....rM9$..M...$..:...P.....c....]...,.....c.@./POST /gts1c3 HTTP/1.1
Host: ocsp.pki.goog
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 84
Connection: keep-alive
11 client pkts, 11 server pkts, 21 turns.
Entire conversation (12 kB)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

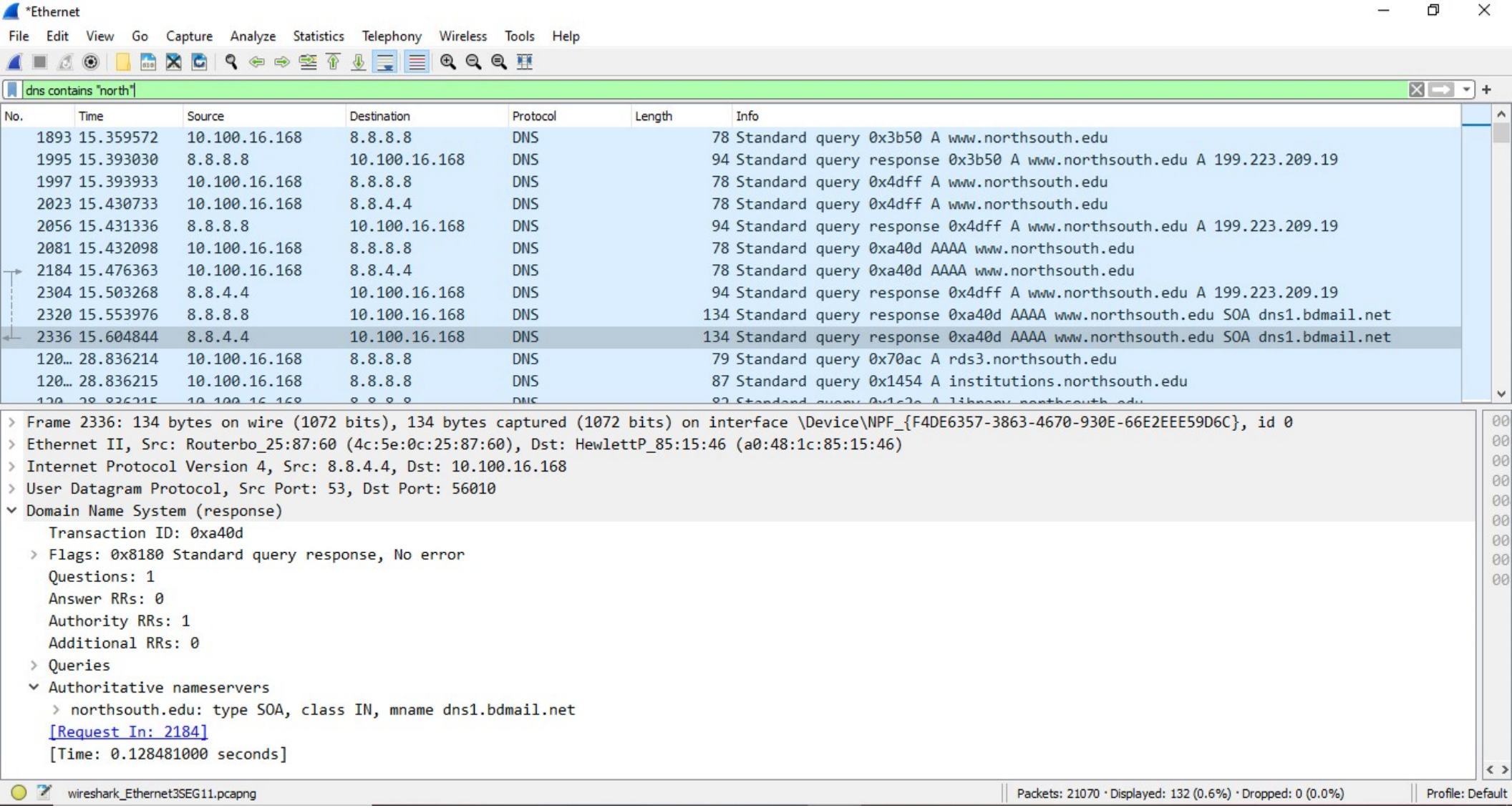

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response.code
No. Time Source Destination Protocol Length Info
204 12.073293 172.217.167.35 10.100.16.168 OCSP 755 Response
517 13.020142 172.217.167.35 10.100.16.168 OCSP 756 Response
796 13.320274 172.217.167.35 10.100.16.168 OCSP 756 Response
1270 14.484946 172.217.167.35 10.100.16.168 OCSP 755 Response
1567 14.885253 172.217.167.35 10.100.16.168 OCSP 756 Response
2078 15.431516 172.217.167.35 10.100.16.168 OCSP 756 Response
2316 15.547983 172.217.167.35 10.100.16.168 OCSP 756 Response
2776 15.986744 34.107.221.82 10.100.16.168 HTTP 352 HTTP/1.1 200 OK (text/html)
2812 16.062911 34.107.221.82 10.100.16.168 HTTP 270 HTTP/1.1 200 OK (text/plain)
2956 16.884215 172.217.167.35 10.100.16.168 OCSP 756 Response
3013 17.406295 172.217.167.35 10.100.16.168 OCSP 755 Response
3098 18.112569 199.223.209.19 10.100.16.168 HTTP 74 HTTP/1.1 200 OK (text/html)
Frame 796: 756 bytes on wire (6048 bits), 756 bytes captured (6048 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 172.217.167.35, Dst: 10.100.16.168
Transmission Control Protocol, Src Port: 80, Dst Port: 51677, Seq: 1404, Ack: 1287, Len: 702
Hypertext Transfer Protocol
Online Certificate Status Protocol
Status Code: Unsigned integer (2 bytes)
Packets: 21070 · Displayed: 103 (0.5%) · Dropped: 0 (0.0%)
Profile: Default

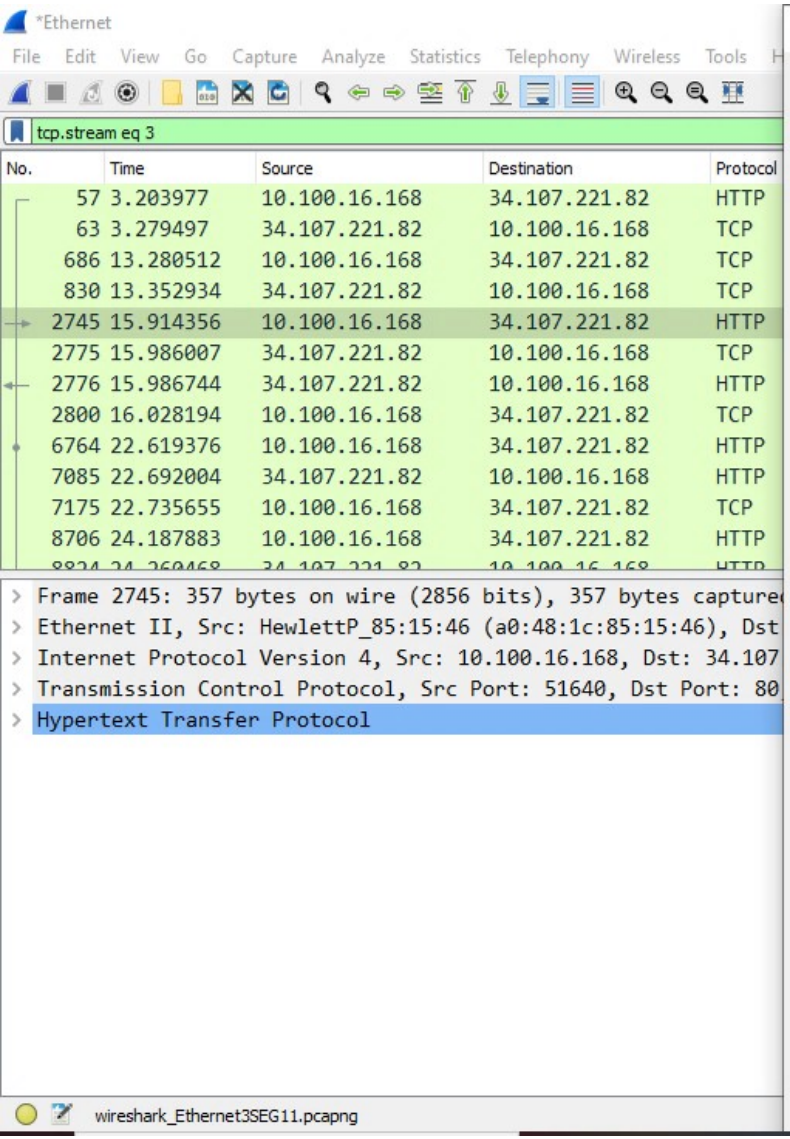

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method
No. Time Source Destination Protocol Length Info
169 10.970151 10.100.16.41 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
172 11.185946 10.100.16.73 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
173 11.224277 10.100.16.132 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
201 11.934047 10.100.16.168 172.217.167.35 OCSP 482 Request
218 12.193158 10.100.16.73 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
259 12.411417 10.100.16.65 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
263 12.429891 10.100.16.163 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
328 12.670065 10.100.16.31 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
487 12.878754 10.100.16.168 172.217.167.35 OCSP 483 Request
529 13.174168 10.100.16.168 172.217.167.35 OCSP 483 Request
537 13.200202 10.100.16.73 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
738 13.305698 10.100.16.129 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
Frame 738: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Dell_b3:0e:fd (e4:54:e8:b3:0e:fd), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 10.100.16.129, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 55704, Dst Port: 1900
Simple Service Discovery Protocol
Request Method: Character string
Packets: 21070 · Displayed: 492 (2.3%) · Dropped: 0 (0.0%)
Profile: Default

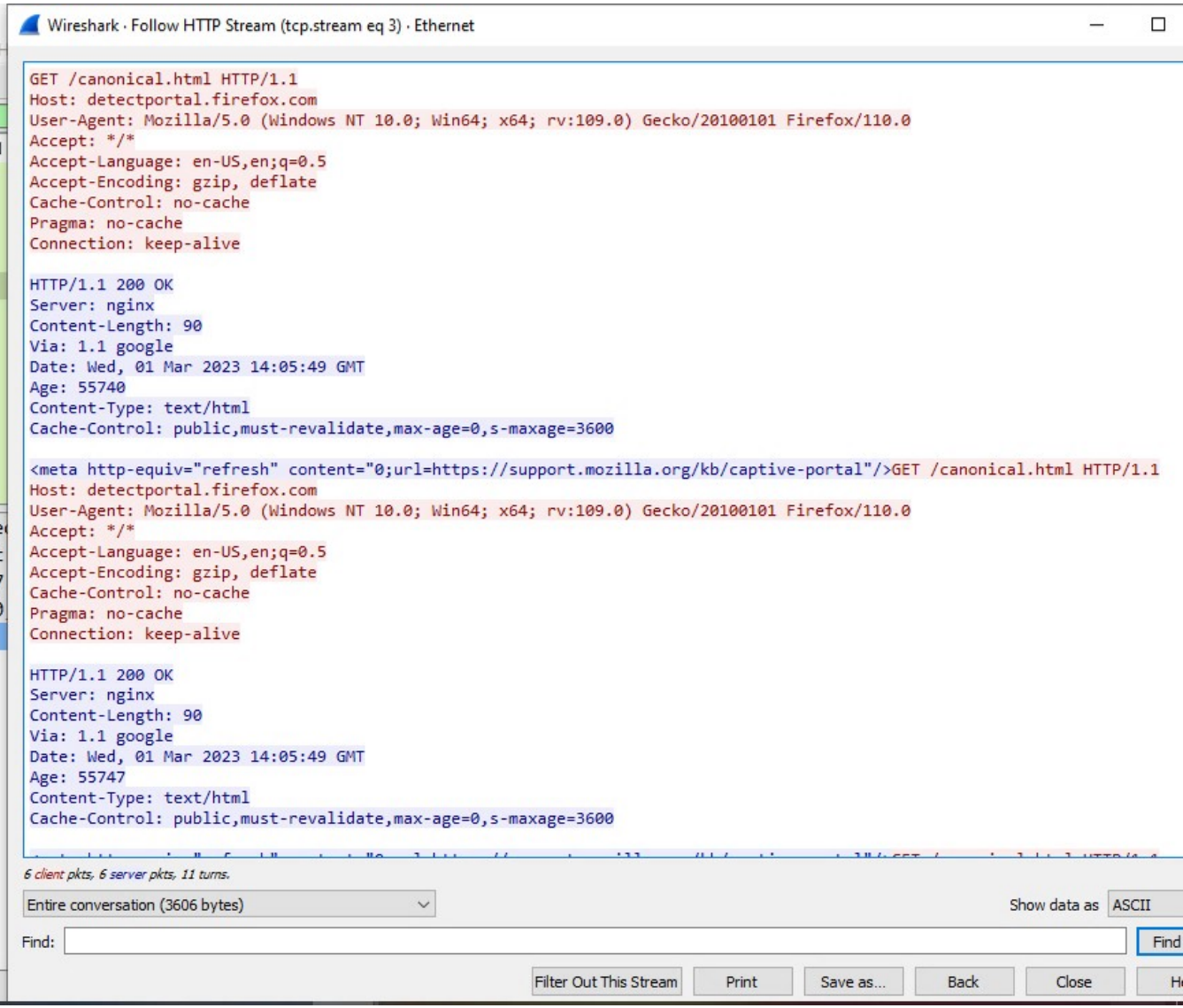

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless
tcp.stream eq 3
No. Time Source Destination
57 3.203977 10.100.16.168 34.107.221.82
63 3.279497 34.107.221.82 10.100.16.168
686 13.280512 10.100.16.168 34.107.221.82
830 13.352934 34.107.221.82 10.100.16.168
2745 15.914356 10.100.16.168 34.107.221.82
2775 15.986007 34.107.221.82 10.100.16.168
2776 15.986744 34.107.221.82 10.100.16.168
2800 16.028194 10.100.16.168 34.107.221.82
6764 22.619376 10.100.16.168 34.107.221.82
7085 22.692004 34.107.221.82 10.100.16.168
7175 22.735655 10.100.16.168 34.107.221.82
8706 24.187883 10.100.16.168 34.107.221.82
Frame 2776: 352 bytes on wire (2816 bits), 352 bytes
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:6
Internet Protocol Version 4, Src: 34.107.221.82, Dst:
Transmission Control Protocol, Src Port: 80, Dst Port
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
wireshark_Ethernet3SEG11.pcapng
Wireshark · Follow HTTP Stream (tcp.stream eq 3) · Ethernet
GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive
HTTP/1.1 200 OK
Server: nginx
Content-Length: 90
Via: 1.1 google
Date: Wed, 01 Mar 2023 14:05:49 GMT
Age: 55740
Content-Type: text/html
Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600
<meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal"/>GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive
HTTP/1.1 200 OK
Server: nginx
Content-Length: 90
Via: 1.1 google
Date: Wed, 01 Mar 2023 14:05:49 GMT
Age: 55747
Content-Type: text/html
Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600
6 client pkts, 6 server pkts, 11 turns.
Entire conversation (3606 bytes)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

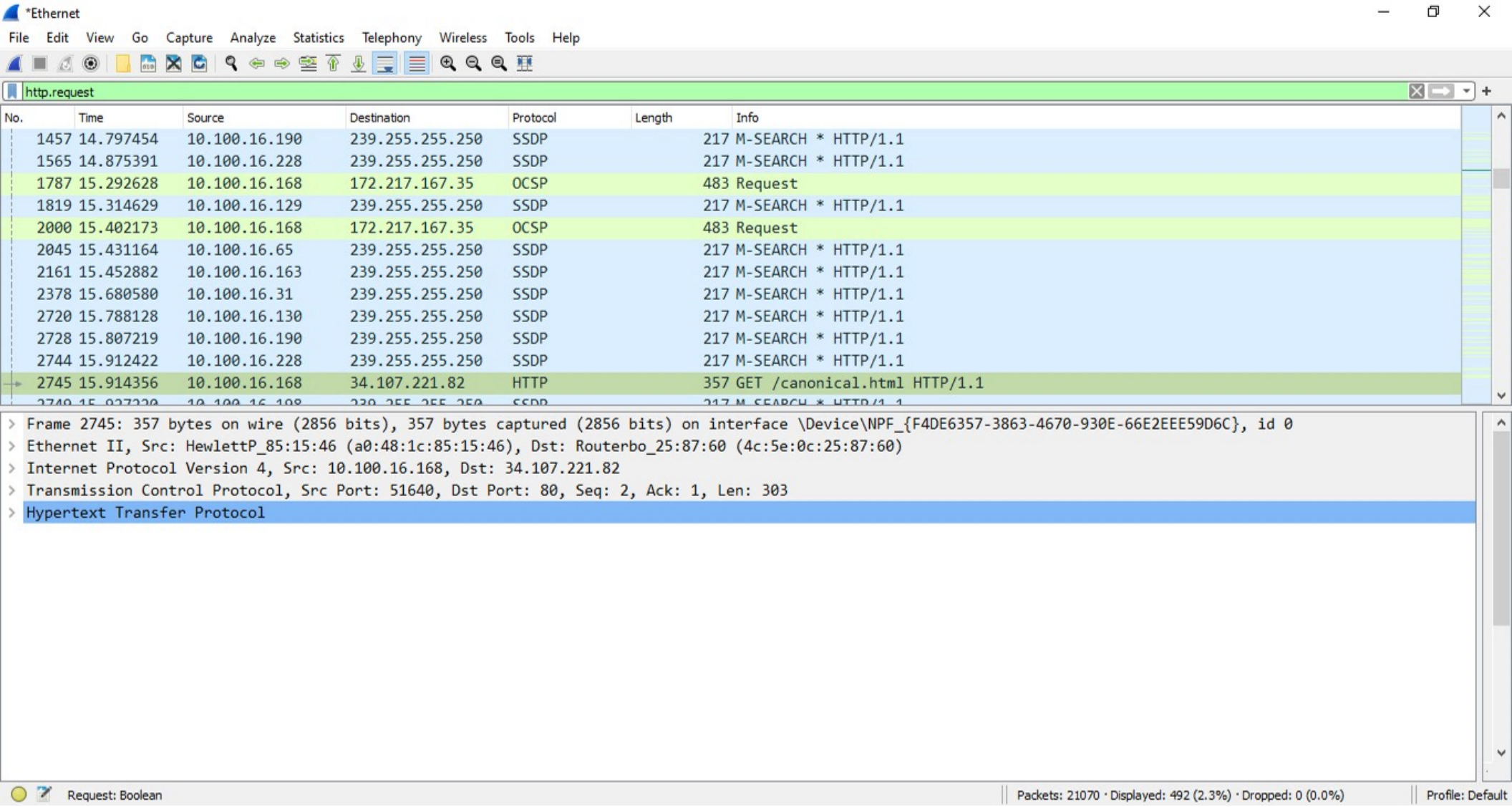

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.response
No. Time Source Destination Protocol Length Info
204 12.073293 172.217.167.35 10.100.16.168 OCSP 755 Response
517 13.020142 172.217.167.35 10.100.16.168 OCSP 756 Response
796 13.320274 172.217.167.35 10.100.16.168 OCSP 756 Response
1270 14.484946 172.217.167.35 10.100.16.168 OCSP 755 Response
1567 14.885253 172.217.167.35 10.100.16.168 OCSP 756 Response
2078 15.431516 172.217.167.35 10.100.16.168 OCSP 756 Response
2316 15.547983 172.217.167.35 10.100.16.168 OCSP 756 Response
2776 15.986744 34.107.221.82 10.100.16.168 HTTP 352 HTTP/1.1 200 OK (text/html)
2812 16.062911 34.107.221.82 10.100.16.168 HTTP 270 HTTP/1.1 200 OK (text/plain)
2956 16.884215 172.217.167.35 10.100.16.168 OCSP 756 Response
3013 17.406295 172.217.167.35 10.100.16.168 OCSP 755 Response
3098 18.112569 199.223.209.19 10.100.16.168 HTTP 74 HTTP/1.1 200 OK (text/html)
Frame 1567: 756 bytes on wire (6048 bits), 756 bytes captured (6048 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 172.217.167.35, Dst: 10.100.16.168
Transmission Control Protocol, Src Port: 80, Dst Port: 51677, Seq: 2807, Ack: 2144, Len: 702
Hypertext Transfer Protocol
Online Certificate Status Protocol
Response: Boolean
Packets: 21070 · Displayed: 103 (0.5%) · Dropped: 0 (0.0%)
Profile: Default

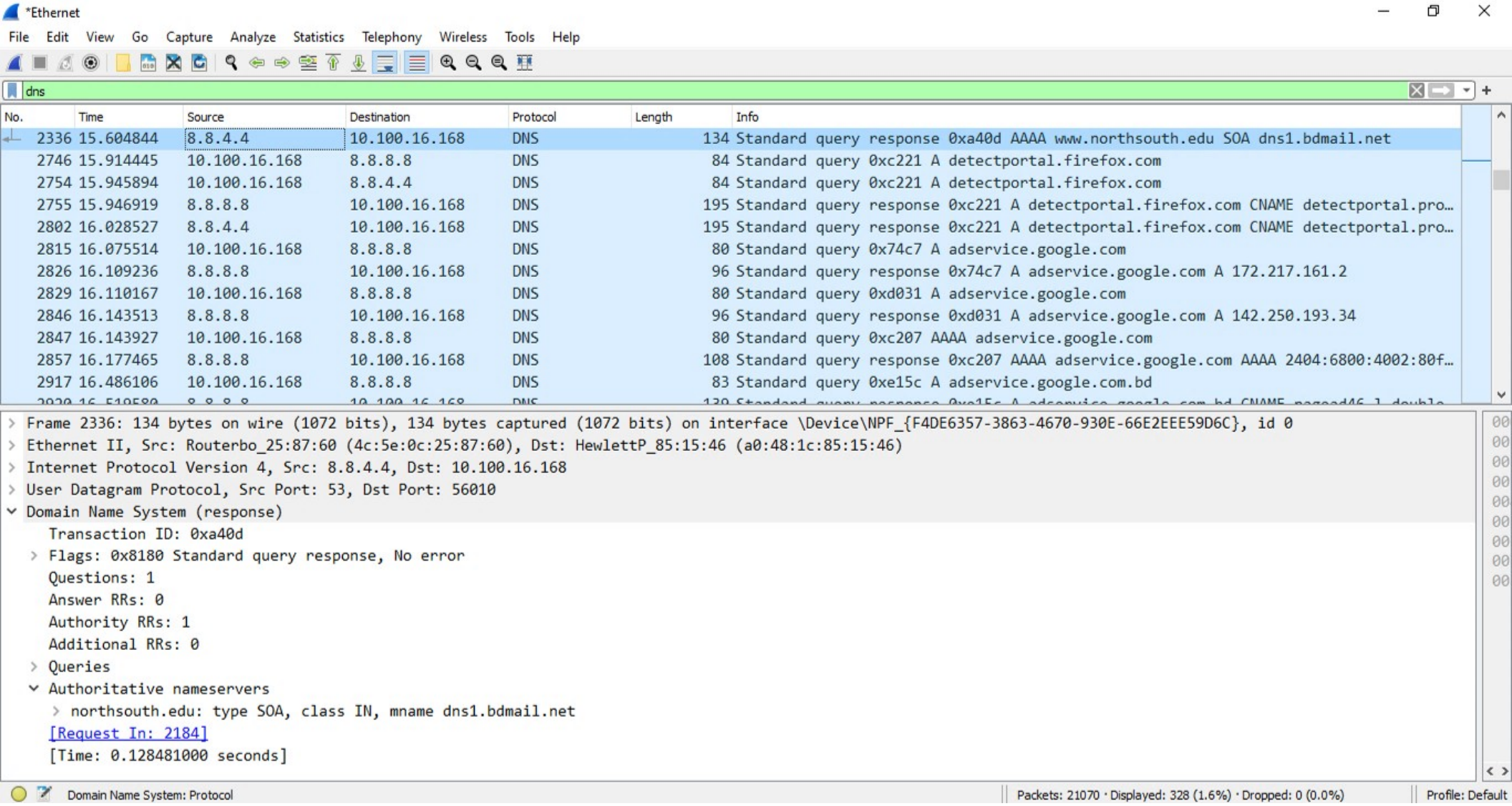

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns contains "north"
No. Time Source Destination Protocol Length Info
1893 15.359572 10.100.16.168 8.8.8.8 DNS 78 Standard query 0x3b50 A www.northsouth.edu
1995 15.393030 8.8.8.8 10.100.16.168 DNS 94 Standard query response 0x3b50 A www.northsouth.edu A 199.223.209.19
1997 15.393933 10.100.16.168 8.8.8.8 DNS 78 Standard query 0x4dff A www.northsouth.edu
2023 15.430733 10.100.16.168 8.8.4.4 DNS 78 Standard query 0x4dff A www.northsouth.edu
2056 15.431336 8.8.8.8 10.100.16.168 DNS 94 Standard query response 0x4dff A www.northsouth.edu A 199.223.209.19
2081 15.432098 10.100.16.168 8.8.8.8 DNS 78 Standard query 0xa40d AAAA www.northsouth.edu
2184 15.476363 10.100.16.168 8.8.4.4 DNS 78 Standard query 0xa40d AAAA www.northsouth.edu
2304 15.503268 8.8.4.4 10.100.16.168 DNS 94 Standard query response 0x4dff A www.northsouth.edu A 199.223.209.19
2320 15.553976 8.8.8.8 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
2336 15.604844 8.8.4.4 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
120… 28.836214 10.100.16.168 8.8.8.8 DNS 79 Standard query 0x70ac A rds3.northsouth.edu
120… 28.836215 10.100.16.168 8.8.8.8 DNS 87 Standard query 0x1454 A institutions.northsouth.edu
Frame 2056: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.100.16.168
User Datagram Protocol, Src Port: 53, Dst Port: 50617
Domain Name System (response)
Transaction ID: 0x4dff
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
www.northsouth.edu: type A, class IN, addr 199.223.209.19
[Request In: 1997]
[Time: 0.037403000 seconds]
wireshark_Ethernet3SEG11.pcapng
Packets: 21070 · Displayed: 132 (0.6%) · Dropped: 0 (0.0%)
Profile: Default

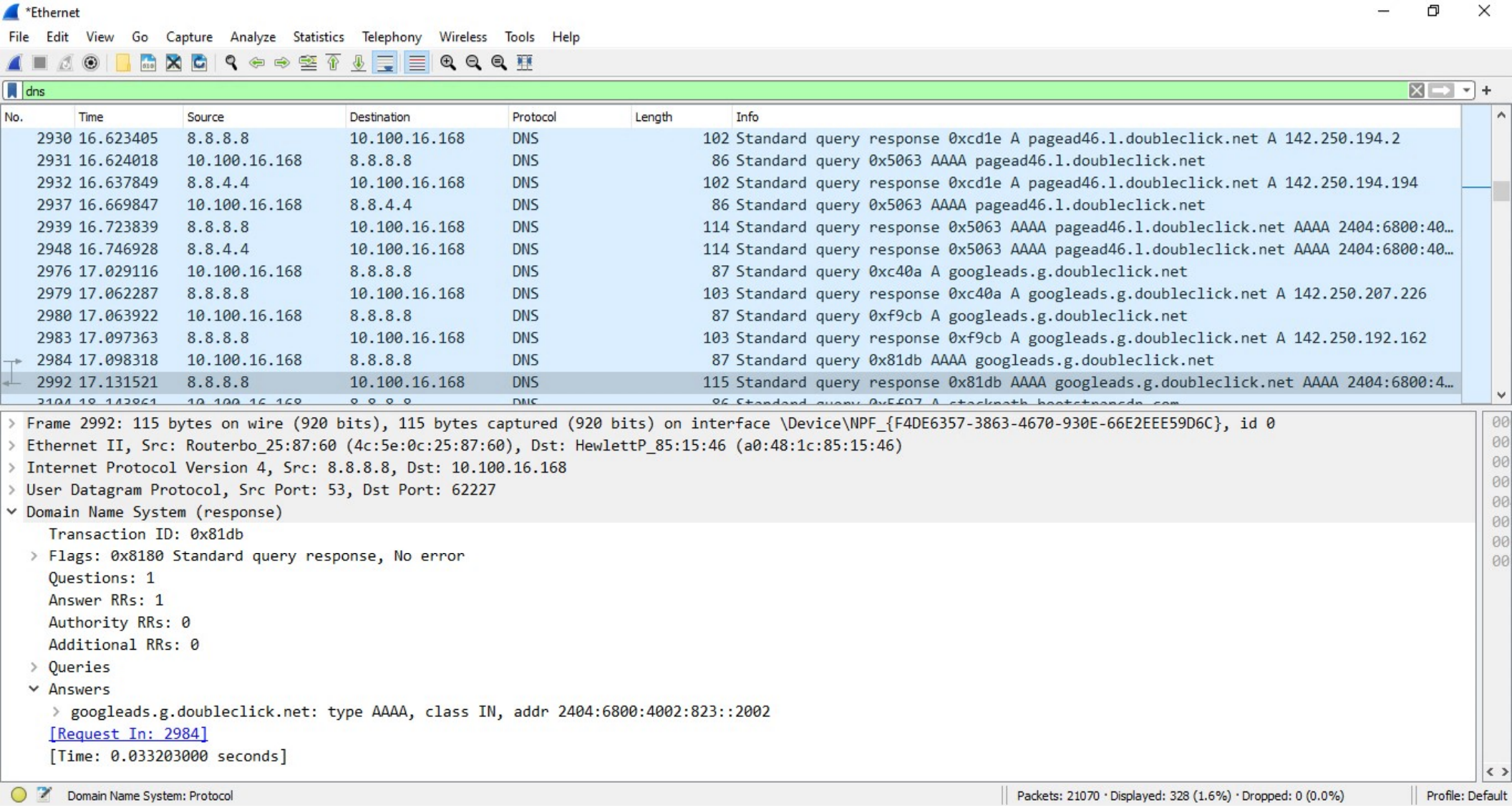

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns contains "north"
No. Time Source Destination Protocol Length Info
1893 15.359572 10.100.16.168 8.8.8.8 DNS 78 Standard query 0x3b50 A www.northsouth.edu
1995 15.393030 8.8.8.8 10.100.16.168 DNS 94 Standard query response 0x3b50 A www.northsouth.edu A 199.223.209.19
1997 15.393933 10.100.16.168 8.8.8.8 DNS 78 Standard query 0x4dff A www.northsouth.edu
2023 15.430733 10.100.16.168 8.8.4.4 DNS 78 Standard query 0x4dff A www.northsouth.edu
2056 15.431336 8.8.8.8 10.100.16.168 DNS 94 Standard query response 0x4dff A www.northsouth.edu A 199.223.209.19
2081 15.432098 10.100.16.168 8.8.8.8 DNS 78 Standard query 0xa40d AAAA www.northsouth.edu
2184 15.476363 10.100.16.168 8.8.4.4 DNS 78 Standard query 0xa40d AAAA www.northsouth.edu
2304 15.503268 8.8.4.4 10.100.16.168 DNS 94 Standard query response 0x4dff A www.northsouth.edu A 199.223.209.19
2320 15.553976 8.8.8.8 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
2336 15.604844 8.8.4.4 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
120… 28.836214 10.100.16.168 8.8.8.8 DNS 79 Standard query 0x70ac A rds3.northsouth.edu
120… 28.836215 10.100.16.168 8.8.8.8 DNS 87 Standard query 0x1454 A institutions.northsouth.edu
Frame 2336: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.100.16.168
User Datagram Protocol, Src Port: 53, Dst Port: 56010
Domain Name System (response)
Transaction ID: 0xa40d
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
Authoritative nameservers
northsouth.edu: type SOA, class IN, mname dns1.bdmail.net
[Request In: 2184]
[Time: 0.128481000 seconds]
wireshark_Ethernet3SEG11.pcapng
Packets: 21070 · Displayed: 132 (0.6%) · Dropped: 0 (0.0%)
Profile: Default

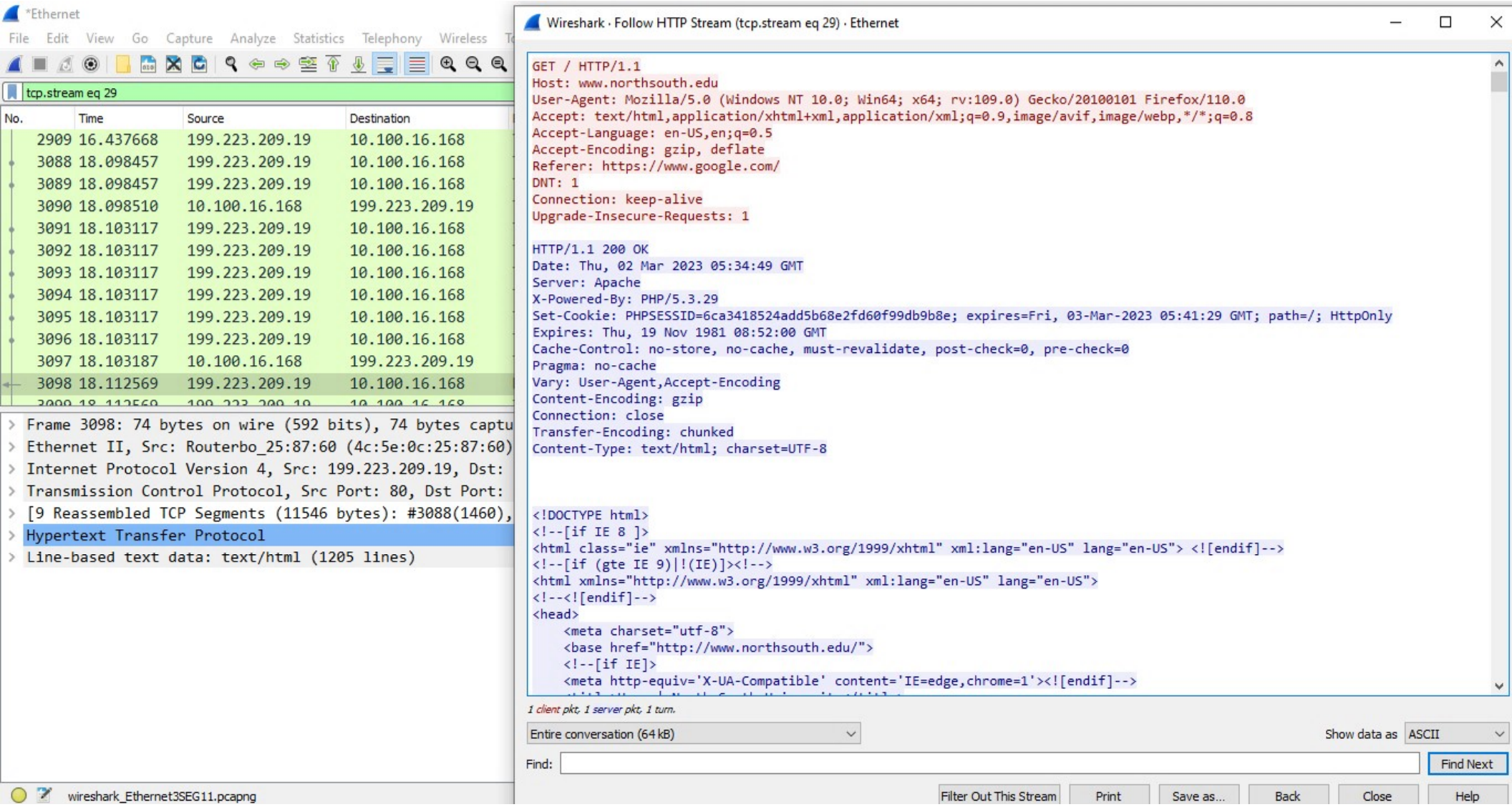

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools
tcp.stream eq 3
No. Time Source Destination Protocol
57 3.203977 10.100.16.168 34.107.221.82 HTTP
63 3.279497 34.107.221.82 10.100.16.168 TCP
686 13.280512 10.100.16.168 34.107.221.82 TCP
830 13.352934 34.107.221.82 10.100.16.168 TCP
2745 15.914356 10.100.16.168 34.107.221.82 HTTP
2775 15.986007 34.107.221.82 10.100.16.168 TCP
2776 15.986744 34.107.221.82 10.100.16.168 HTTP
2800 16.028194 10.100.16.168 34.107.221.82 TCP
6764 22.619376 10.100.16.168 34.107.221.82 HTTP
7085 22.692004 34.107.221.82 10.100.16.168 HTTP
7175 22.735655 10.100.16.168 34.107.221.82 TCP
8706 24.187883 10.100.16.168 34.107.221.82 HTTP
Frame 2745: 357 bytes on wire (2856 bits), 357 bytes capture
Ethernet II, Src: HewlettP_85:15:46 (a0:48:1c:85:15:46), Dst
Internet Protocol Version 4, Src: 10.100.16.168, Dst: 34.107
Transmission Control Protocol, Src Port: 51640, Dst Port: 80
Hypertext Transfer Protocol
wireshark_Ethernet3SEG11.pcapng

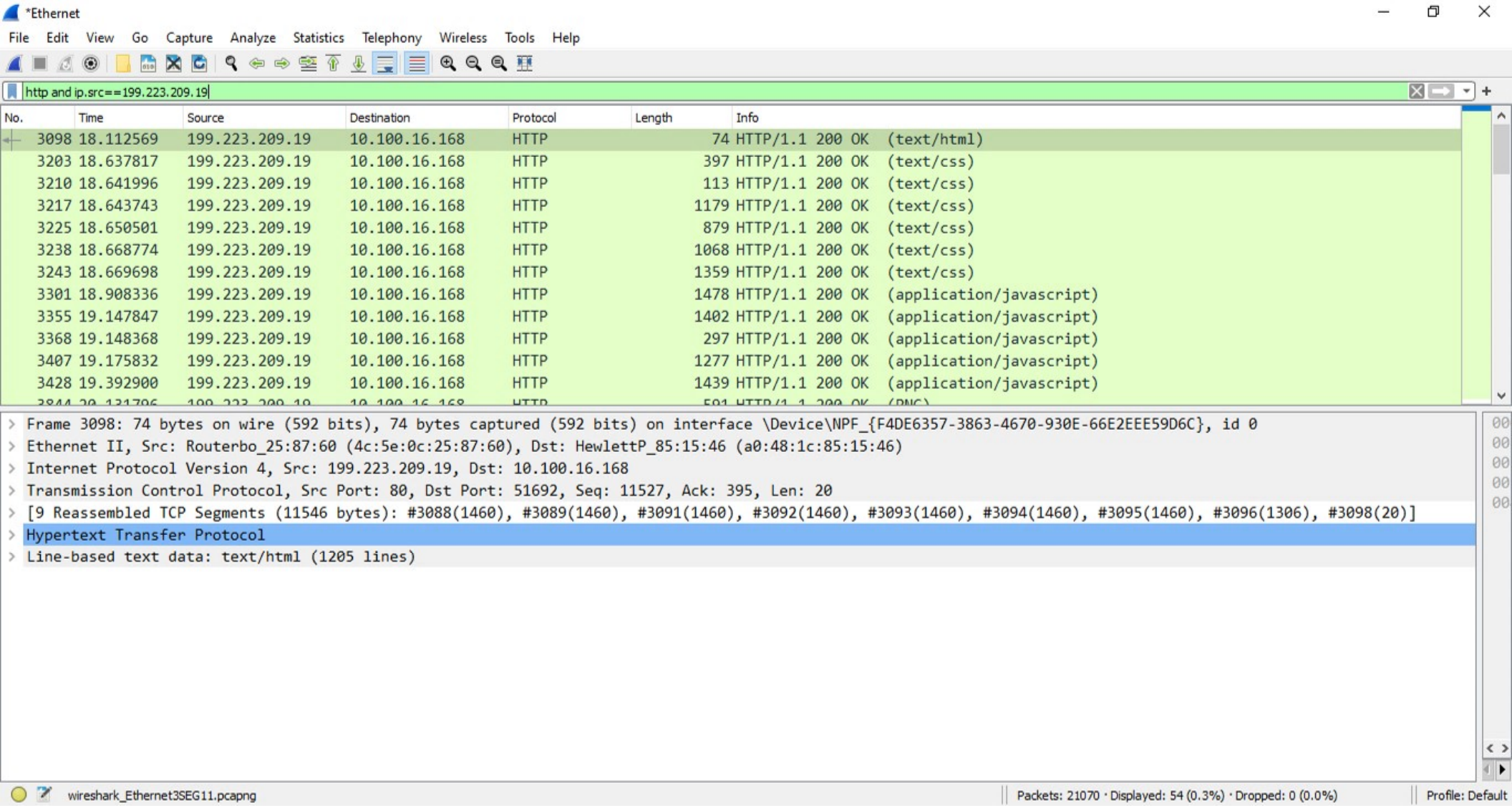

Wireshark · Follow HTTP Stream (tcp.stream eq 3) · Ethernet
GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive
HTTP/1.1 200 OK
Server: nginx
Content-Length: 90
Via: 1.1 google
Date: Wed, 01 Mar 2023 14:05:49 GMT
Age: 55740
Content-Type: text/html
Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600
<meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal"/>GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive
HTTP/1.1 200 OK
Server: nginx
Content-Length: 90
Via: 1.1 google
Date: Wed, 01 Mar 2023 14:05:49 GMT
Age: 55747
Content-Type: text/html
Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600
6 client pkts, 6 server pkts, 11 turns.
Entire conversation (3606 bytes)
Show data as ASCII
Find:
Find
Filter Out This Stream
Print
Save as...
Back
Close


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination Protocol Length Info
1457 14.797454 10.100.16.190 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
1565 14.875391 10.100.16.228 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
1787 15.292628 10.100.16.168 172.217.167.35 OCSP 483 Request
1819 15.314629 10.100.16.129 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2000 15.402173 10.100.16.168 172.217.167.35 OCSP 483 Request
2045 15.431164 10.100.16.65 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2161 15.452882 10.100.16.163 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2378 15.680580 10.100.16.31 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2720 15.788128 10.100.16.130 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2728 15.807219 10.100.16.190 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2744 15.912422 10.100.16.228 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2745 15.914356 10.100.16.168 34.107.221.82 HTTP 357 GET /canonical.html HTTP/1.1
Frame 2745: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: HewlettP_85:15:46 (a0:48:1c:85:15:46), Dst: Routerbo_25:87:60 (4c:5e:0c:25:87:60)
Internet Protocol Version 4, Src: 10.100.16.168, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 51640, Dst Port: 80, Seq: 2, Ack: 1, Len: 303
Hypertext Transfer Protocol
Request: Boolean
Packets: 21070 · Displayed: 492 (2.3%) · Dropped: 0 (0.0%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
2336 15.604844 8.8.4.4 10.100.16.168 DNS 134 Standard query response 0xa40d AAAA www.northsouth.edu SOA dns1.bdmail.net
2746 15.914445 10.100.16.168 8.8.8.8 DNS 84 Standard query 0xc221 A detectportal.firefox.com
2754 15.945894 10.100.16.168 8.8.4.4 DNS 84 Standard query 0xc221 A detectportal.firefox.com
2755 15.946919 8.8.8.8 10.100.16.168 DNS 195 Standard query response 0xc221 A detectportal.firefox.com CNAME detectportal.pro…
2802 16.028527 8.8.4.4 10.100.16.168 DNS 195 Standard query response 0xc221 A detectportal.firefox.com CNAME detectportal.pro…
2815 16.075514 10.100.16.168 8.8.8.8 DNS 80 Standard query 0x74c7 A adservice.google.com
2826 16.109236 8.8.8.8 10.100.16.168 DNS 96 Standard query response 0x74c7 A adservice.google.com A 172.217.161.2
2829 16.110167 10.100.16.168 8.8.8.8 DNS 80 Standard query 0xd031 A adservice.google.com
2846 16.143513 8.8.8.8 10.100.16.168 DNS 96 Standard query response 0xd031 A adservice.google.com A 142.250.193.34
2847 16.143927 10.100.16.168 8.8.8.8 DNS 80 Standard query 0xc207 AAAA adservice.google.com
2857 16.177465 8.8.8.8 10.100.16.168 DNS 108 Standard query response 0xc207 AAAA adservice.google.com AAAA 2404:6800:4002:80f…
2917 16.486106 10.100.16.168 8.8.8.8 DNS 83 Standard query 0xe15c A adservice.google.com.bd
Frame 2336: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 8.8.4.4, Dst: 10.100.16.168
User Datagram Protocol, Src Port: 53, Dst Port: 56010
Domain Name System (response)
Transaction ID: 0xa40d
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
Authoritative nameservers
northsouth.edu: type SOA, class IN, mname dns1.bdmail.net
[Request In: 2184]
[Time: 0.128481000 seconds]
Domain Name System: Protocol
Packets: 21070 · Displayed: 328 (1.6%) · Dropped: 0 (0.0%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
2930 16.623405 8.8.8.8 10.100.16.168 DNS 102 Standard query response 0xcd1e A pagead46.l.doubleclick.net A 142.250.194.2
2931 16.624018 10.100.16.168 8.8.8.8 DNS 86 Standard query 0x5063 AAAA pagead46.l.doubleclick.net
2932 16.637849 8.8.4.4 10.100.16.168 DNS 102 Standard query response 0xcd1e A pagead46.l.doubleclick.net A 142.250.194.194
2937 16.669847 10.100.16.168 8.8.4.4 DNS 86 Standard query 0x5063 AAAA pagead46.l.doubleclick.net
2939 16.723839 8.8.8.8 10.100.16.168 DNS 114 Standard query response 0x5063 AAAA pagead46.l.doubleclick.net AAAA 2404:6800:40…
2948 16.746928 8.8.4.4 10.100.16.168 DNS 114 Standard query response 0x5063 AAAA pagead46.l.doubleclick.net AAAA 2404:6800:40…
2976 17.029116 10.100.16.168 8.8.8.8 DNS 87 Standard query 0xc40a A googleads.g.doubleclick.net
2979 17.062287 8.8.8.8 10.100.16.168 DNS 103 Standard query response 0xc40a A googleads.g.doubleclick.net A 142.250.207.226
2980 17.063922 10.100.16.168 8.8.8.8 DNS 87 Standard query 0xf9cb A googleads.g.doubleclick.net
2983 17.097363 8.8.8.8 10.100.16.168 DNS 103 Standard query response 0xf9cb A googleads.g.doubleclick.net A 142.250.192.162
2984 17.098318 10.100.16.168 8.8.8.8 DNS 87 Standard query 0x81db AAAA googleads.g.doubleclick.net
2992 17.131521 8.8.8.8 10.100.16.168 DNS 115 Standard query response 0x81db AAAA googleads.g.doubleclick.net AAAA 2404:6800:4…
Frame 2992: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.100.16.168
User Datagram Protocol, Src Port: 53, Dst Port: 62227
Domain Name System (response)
Transaction ID: 0x81db
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
googleads.g.doubleclick.net: type AAAA, class IN, addr 2404:6800:4002:823::2002
[Request In: 2984]
[Time: 0.033203000 seconds]
Domain Name System: Protocol
Packets: 21070 · Displayed: 328 (1.6%) · Dropped: 0 (0.0%)
Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless
tcp.stream eq 29
No. Time Source Destination
2909 16.437668 199.223.209.19 10.100.16.168
3088 18.098457 199.223.209.19 10.100.16.168
3089 18.098457 199.223.209.19 10.100.16.168
3090 18.098510 10.100.16.168 199.223.209.19
3091 18.103117 199.223.209.19 10.100.16.168
3092 18.103117 199.223.209.19 10.100.16.168
3093 18.103117 199.223.209.19 10.100.16.168
3094 18.103117 199.223.209.19 10.100.16.168
3095 18.103117 199.223.209.19 10.100.16.168
3096 18.103117 199.223.209.19 10.100.16.168
3097 18.103187 10.100.16.168 199.223.209.19
3098 18.112569 199.223.209.19 10.100.16.168
Frame 3098: 74 bytes on wire (592 bits), 74 bytes captu
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60)
Internet Protocol Version 4, Src: 199.223.209.19, Dst:
Transmission Control Protocol, Src Port: 80, Dst Port:
[9 Reassembled TCP Segments (11546 bytes): #3088(1460),
Hypertext Transfer Protocol
Line-based text data: text/html (1205 lines)
wireshark_Ethernet3SEG11.pcapng
Wireshark · Follow HTTP Stream (tcp.stream eq 29) · Ethernet
GET / HTTP/1.1
Host: www.northsouth.edu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Thu, 02 Mar 2023 05:34:49 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
Set-Cookie: PHPSESSID=6ca3418524add5b68e2fd60f99db9b8e; expires=Fri, 03-Mar-2023 05:41:29 GMT; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: User-Agent,Accept-Encoding
Content-Encoding: gzip
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<!--[if IE 8]>
<html class="ie" xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-US" lang="en-US"> <![endif]-->
<!--[if (gte IE 9)|!(IE)]><!-->
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-US" lang="en-US">
<!--<![endif]-->
<head>
<meta charset="utf-8">
<base href="http://www.northsouth.edu/">
<!--[if IE]>
<meta http-equiv='X-UA-Compatible' content='IE=edge,chrome=1'><![endif]-->
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (64 kB)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http and ip.src==199.223.209.19
No. Time Source Destination Protocol Length Info
3098 18.112569 199.223.209.19 10.100.16.168 HTTP 74 HTTP/1.1 200 OK (text/html)
3203 18.637817 199.223.209.19 10.100.16.168 HTTP 397 HTTP/1.1 200 OK (text/css)
3210 18.641996 199.223.209.19 10.100.16.168 HTTP 113 HTTP/1.1 200 OK (text/css)
3217 18.643743 199.223.209.19 10.100.16.168 HTTP 1179 HTTP/1.1 200 OK (text/css)
3225 18.650501 199.223.209.19 10.100.16.168 HTTP 879 HTTP/1.1 200 OK (text/css)
3238 18.668774 199.223.209.19 10.100.16.168 HTTP 1068 HTTP/1.1 200 OK (text/css)
3243 18.669698 199.223.209.19 10.100.16.168 HTTP 1359 HTTP/1.1 200 OK (text/css)
3301 18.908336 199.223.209.19 10.100.16.168 HTTP 1478 HTTP/1.1 200 OK (application/javascript)
3355 19.147847 199.223.209.19 10.100.16.168 HTTP 1402 HTTP/1.1 200 OK (application/javascript)
3368 19.148368 199.223.209.19 10.100.16.168 HTTP 297 HTTP/1.1 200 OK (application/javascript)
3407 19.175832 199.223.209.19 10.100.16.168 HTTP 1277 HTTP/1.1 200 OK (application/javascript)
3428 19.392900 199.223.209.19 10.100.16.168 HTTP 1439 HTTP/1.1 200 OK (application/javascript)
Frame 3098: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F4DE6357-3863-4670-930E-66E2EEE59D6C}, id 0
Ethernet II, Src: Routerbo_25:87:60 (4c:5e:0c:25:87:60), Dst: HewlettP_85:15:46 (a0:48:1c:85:15:46)
Internet Protocol Version 4, Src: 199.223.209.19, Dst: 10.100.16.168
Transmission Control Protocol, Src Port: 80, Dst Port: 51692, Seq: 11527, Ack: 395, Len: 20
[9 Reassembled TCP Segments (11546 bytes): #3088(1460), #3089(1460), #3091(1460), #3092(1460), #3093(1460), #3094(1460), #3095(1460), #3096(1306), #3098(20)]
Hypertext Transfer Protocol
Line-based text data: text/html (1205 lines)
wireshark_Ethernet3SEG11.pcapng
Packets: 21070 · Displayed: 54 (0.3%) · Dropped: 0 (0.0%)
Profile: Default