CYBER SECURITY LAB REPORT

LAB 2 : WIRESHARK

Devi Jagannadh Kotha

06-02-2021

18BCN7079

INTRODUCTION

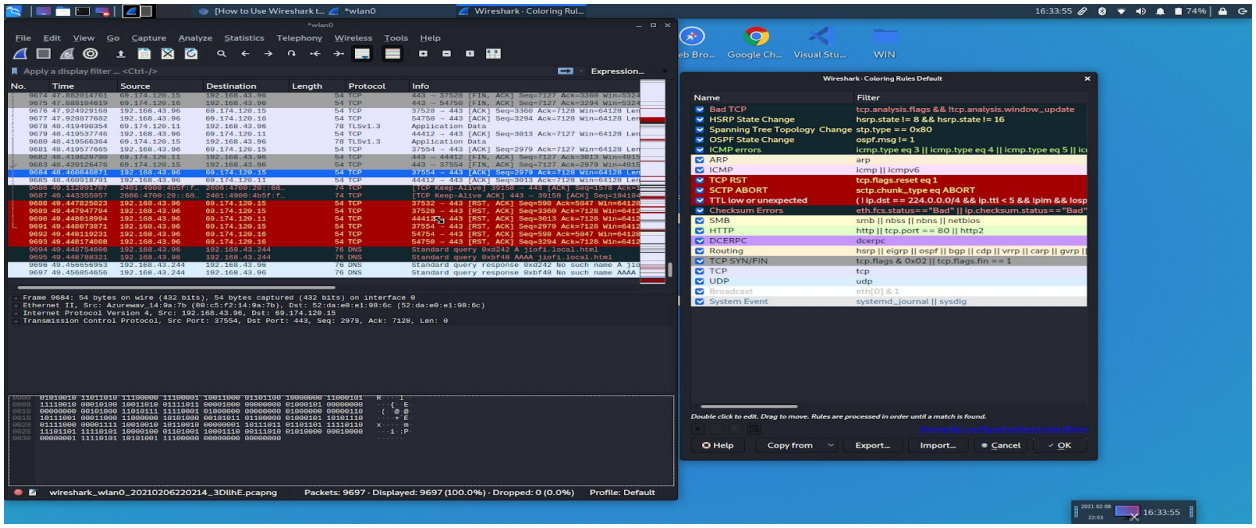
Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

TOOL USED

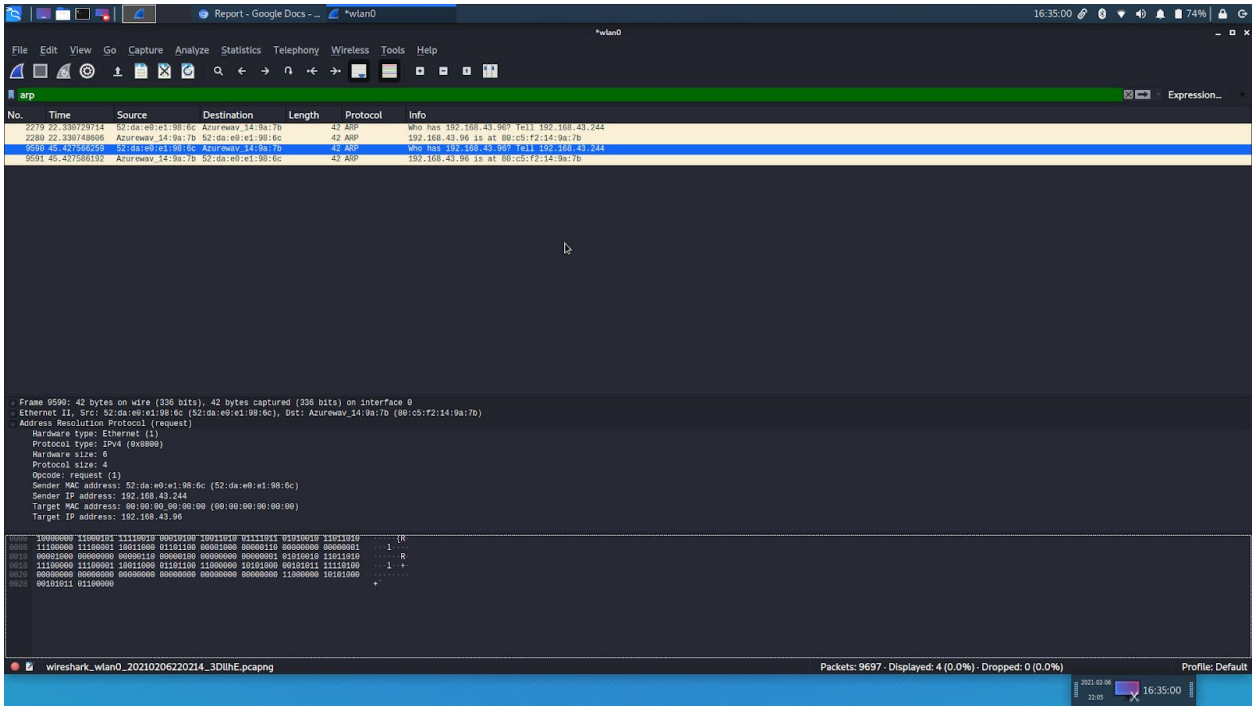
1. Wireshark

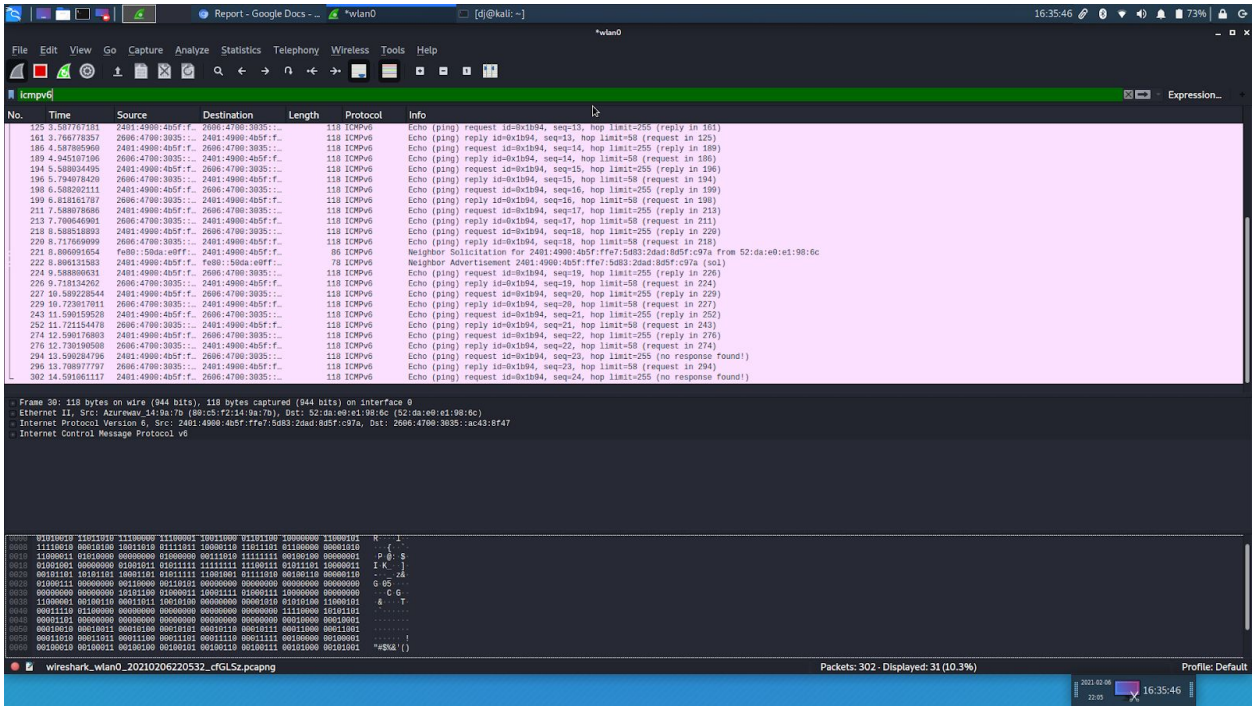
QUESTIONS

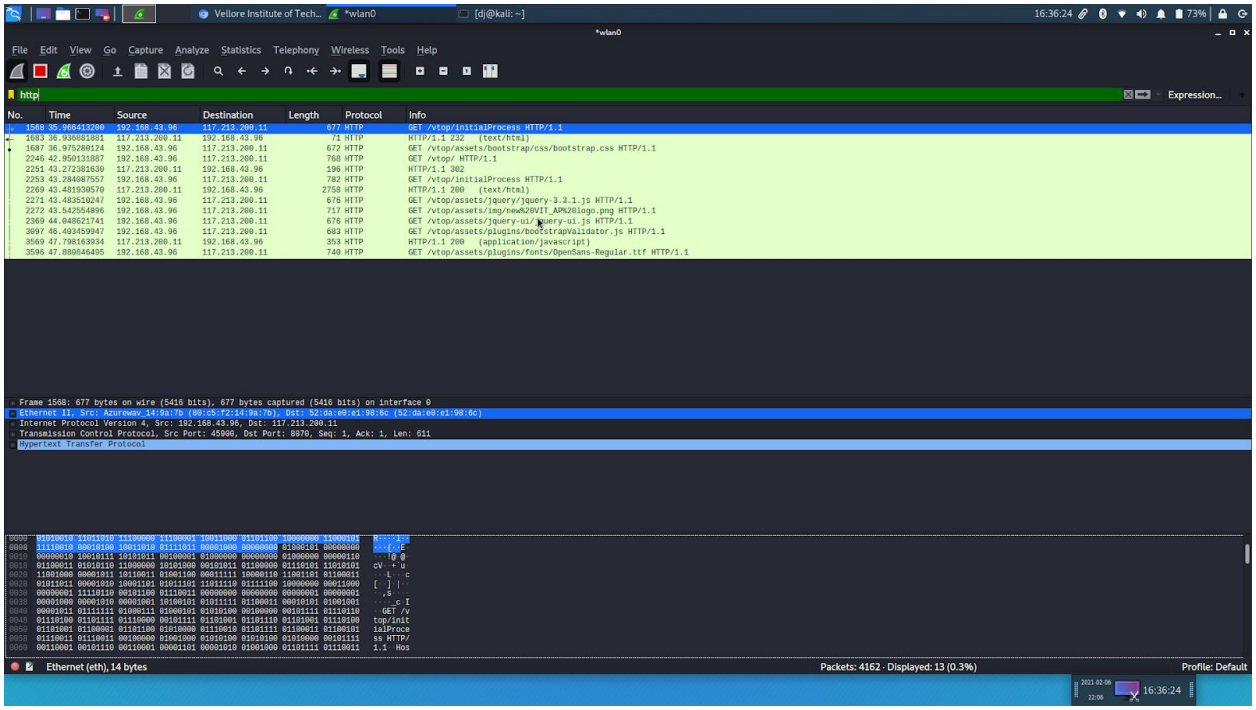
1. Each line in the top pane of the Wireshark window corresponds to a single packet seen on the network. The default display shows the time of the packet (relative to the initiation of the capture), the source and destination IP addresses, the protocol used and some information about the packet. Learn Wireshark color coding from help documents.

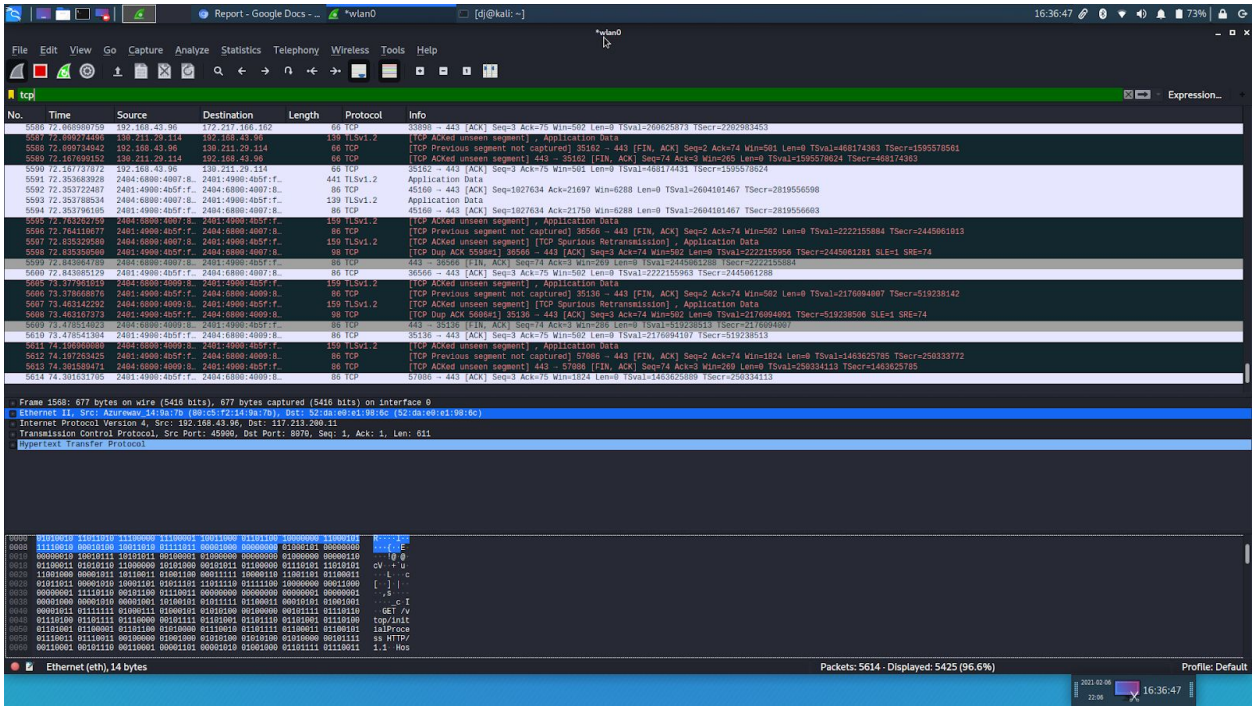


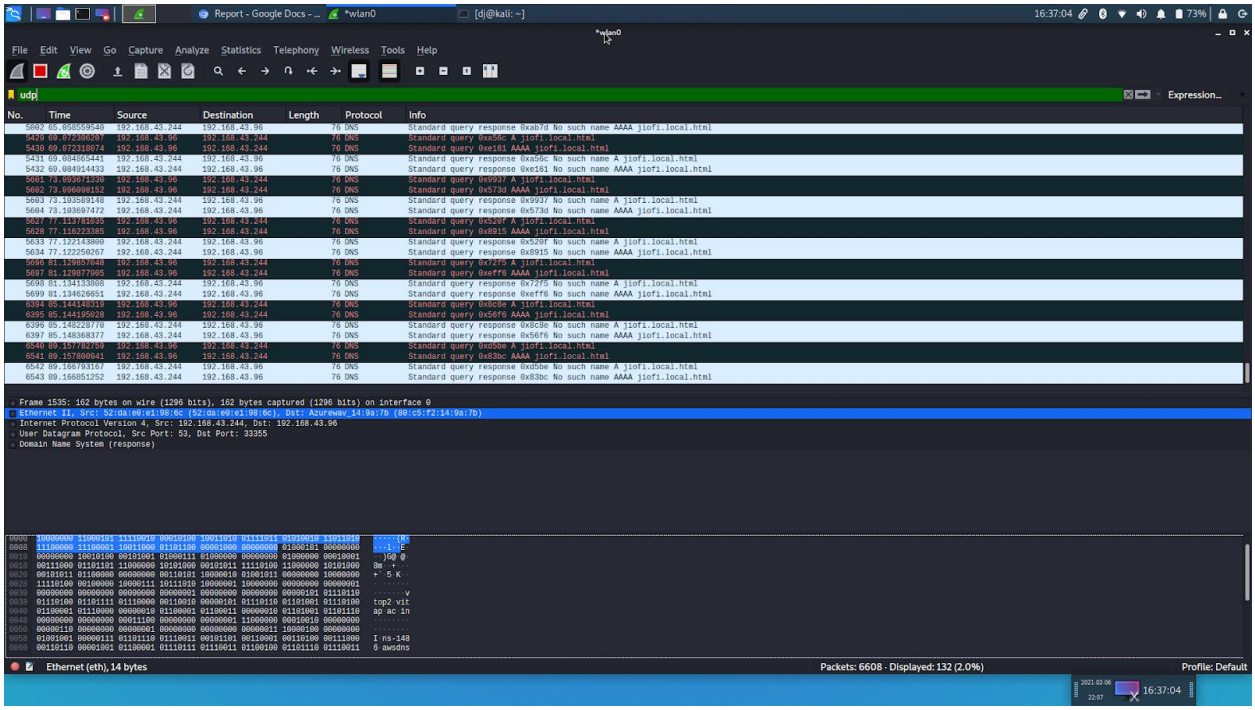
2. To locate specific packets related to individual requests or responses from a within larger capture containing more traffic, we can perform even more specific filtering using a variety of expressions relating to various header fields and their contents. Study how to apply a display filter to the captured packets.




Report - Google Docs - ...
*wlan0
[dj@kali: ~]
16:35:46
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmpv6
Expression...
No. Time Source Destination Length Protocol Info
125 3.507767181 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=13, hop limit=255 (reply in 161)
161 3.766778357 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=13, hop limit=58 (request in 125)
186 4.587805960 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=14, hop limit=255 (reply in 189)
189 4.945107106 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=14, hop limit=58 (request in 186)
194 5.588024495 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=15, hop limit=255 (reply in 196)
196 5.794078420 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=15, hop limit=58 (request in 194)
198 6.588202111 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=16, hop limit=255 (reply in 199)
199 6.818161787 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=16, hop limit=58 (request in 198)
211 7.588078686 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=17, hop limit=255 (reply in 213)
213 7.700646901 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=17, hop limit=58 (request in 211)
218 8.588518893 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=18, hop limit=255 (reply in 220)
220 8.717669099 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=18, hop limit=58 (request in 218)
221 8.806091654 fe80::50da:e0ff:... 2401:4900:4b5f:f... 86 ICMPv6 Neighbor Solicitation for 2401:4900:4b5f:ffe7:5d83:2dad:8d5f:c97a from 52:da:e0:e1:98:6c
222 8.806131583 2401:4900:4b5f:f... fe80::50da:e0ff:... 78 ICMPv6 Neighbor Advertisement 2401:4900:4b5f:ffe7:5d83:2dad:8d5f:c97a (sol)
224 9.588806631 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=19, hop limit=255 (reply in 226)
226 9.718134262 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=19, hop limit=58 (request in 224)
227 10.589228544 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=20, hop limit=255 (reply in 229)
229 10.723017011 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=20, hop limit=58 (request in 227)
243 11.590159528 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=21, hop limit=255 (reply in 252)
252 11.721154478 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=21, hop limit=58 (request in 243)
274 12.590176803 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=22, hop limit=255 (reply in 276)
276 12.730190508 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=22, hop limit=58 (request in 274)
294 13.590284796 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=23, hop limit=255 (no response found!)
296 13.708977797 2606:4700:3035::... 2401:4900:4b5f:f... 118 ICMPv6 Echo (ping) reply id=0x1b94, seq=23, hop limit=58 (request in 294)
302 14.591061117 2401:4900:4b5f:f... 2606:4700:3035::... 118 ICMPv6 Echo (ping) request id=0x1b94, seq=24, hop limit=255 (no response found!)
Frame 30: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
Ethernet II, Src: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b), Dst: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Internet Protocol Version 6, Src: 2401:4900:4b5f:ffe7:5d83:2dad:8d5f:c97a, Dst: 2606:4700:3035::ac43:8f47
Internet Control Message Protocol v6
wireshark_wlan0_20210206220532_cfGLSz.pcapng
Packets: 302 · Displayed: 31 (10.3%)
Profile: Default
16:35:46


Vellore Institute of Tech...
*wlan0
[dj@kali: ~]
16:36:24
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Length Protocol Info
1568 35.966413200 192.168.43.96 117.213.200.11 677 HTTP GET /vtop/initialProcess HTTP/1.1
1683 36.193881851 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 222 (text/html)
1687 36.975280124 192.168.43.96 117.213.200.11 672 HTTP GET /vtop/assets/bootstrap/css/bootstrap.css HTTP/1.1
2246 42.950131887 192.168.43.96 117.213.200.11 768 HTTP GET /vtop/ HTTP/1.1
2251 43.272381630 117.213.200.11 192.168.43.96 196 HTTP HTTP/1.1 302
2253 43.284087557 192.168.43.96 117.213.200.11 782 HTTP GET /vtop/initialProcess HTTP/1.1
2269 43.481930570 117.213.200.11 192.168.43.96 2758 HTTP HTTP/1.1 200 (text/html)
2271 43.483510247 192.168.43.96 117.213.200.11 676 HTTP GET /vtop/assets/jquery/jquery-3.3.1.js HTTP/1.1
2272 43.542554896 192.168.43.96 117.213.200.11 717 HTTP GET /vtop/assets/img/new%20VIT_AP%20logo.png HTTP/1.1
2369 44.048621741 192.168.43.96 117.213.200.11 676 HTTP GET /vtop/assets/jquery-ui/jquery-ui.js HTTP/1.1
3097 46.493459947 192.168.43.96 117.213.200.11 683 HTTP GET /vtop/assets/plugins/bootstrapValidator.js HTTP/1.1
3569 47.798163934 117.213.200.11 192.168.43.96 353 HTTP HTTP/1.1 200 (application/javascript)
3596 47.880846495 192.168.43.96 117.213.200.11 740 HTTP GET /vtop/assets/plugins/fonts/OpenSans-Regular.ttf HTTP/1.1
Frame 1568: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface 0
Ethernet II, Src: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b), Dst: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Internet Protocol Version 4, Src: 192.168.43.96, Dst: 117.213.200.11
Transmission Control Protocol, Src Port: 45900, Dst Port: 8070, Seq: 1, Ack: 1, Len: 611
Hypertext Transfer Protocol
Ethernet (eth), 14 bytes
Packets: 4162 · Displayed: 13 (0.3%)
Profile: Default
16:36:24


Report - Google Docs - ...
*wlan0
[dj@kali: ~]
16:36:47
73%
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
No. Time Source Destination Length Protocol Info
5586 72.000000759 192.168.43.96 172.217.168.162 66 TCP 38898 → 443 [ACK] Seq=3 Ack=75 Win=502 Len=0 TSval=269625873 TSecr=2202983453
5587 72.099274496 130.211.29.114 192.168.43.96 139 TLSv1.2 [TCP ACKed unseen segment] , Application Data
5588 72.099734942 192.168.43.96 130.211.29.114 66 TCP [TCP Previous segment not captured] 35162 → 443 [FIN, ACK] Seq=2 Ack=74 Win=501 Len=0 TSval=468174363 TSecr=1595578561
5589 72.167699152 130.211.29.114 192.168.43.96 66 TCP [TCP ACKed unseen segment] 443 → 35162 [FIN, ACK] Seq=74 Ack=3 Win=265 Len=0 TSval=1595578824 TSecr=468174363
5590 72.197737872 192.168.43.96 130.211.29.114 66 TCP 35162 → 443 [ACK] Seq=3 Ack=75 Win=501 Len=0 TSval=468174431 TSecr=1595578824
5591 72.353683928 2404:6800:4007:8... 2401:4900:4b5f:f... 441 TLSv1.2 Application Data
5592 72.353722487 2401:4900:4b5f:f... 2404:6800:4007:8... 86 TCP 45160 → 443 [ACK] Seq=1027634 Ack=21697 Win=6288 Len=0 TSval=2604101467 TSecr=2819556598
5593 72.353788534 2404:6800:4007:8... 2401:4900:4b5f:f... 139 TLSv1.2 Application Data
5594 72.353796105 2401:4900:4b5f:f... 2404:6800:4007:8... 86 TCP 45160 → 443 [ACK] Seq=1027634 Ack=21750 Win=6288 Len=0 TSval=2604101467 TSecr=2819556603
5595 72.763262759 2404:6800:4007:8... 2401:4900:4b5f:f... 159 TLSv1.2 [TCP ACKed unseen segment] , Application Data
5596 72.764110677 2401:4900:4b5f:f... 2404:6800:4007:8... 86 TCP [TCP Previous segment not captured] 36566 → 443 [FIN, ACK] Seq=2 Ack=74 Win=502 Len=0 TSval=2222155884 TSecr=2445061013
5597 72.835320500 2404:6800:4007:8... 2401:4900:4b5f:f... 159 TLSv1.2 [TCP ACKed unseen segment] [TCP Spurious Retransmission] , Application Data
5598 72.835358500 2401:4900:4b5f:f... 2404:6800:4007:8... 98 TCP [TCP Dup ACK 5596#1] 36566 → 443 [ACK] Seq=3 Ack=74 Win=502 Len=0 TSval=2222155956 TSecr=2445061281 SLE=1 SRE=74
5599 72.843064789 2404:6800:4007:8... 2401:4900:4b5f:f... 86 TCP 443 → 36566 [FIN, ACK] Seq=74 Ack=3 Win=269 Len=0 TSval=2445061288 TSecr=2222155884
5600 72.843085129 2401:4900:4b5f:f... 2404:6800:4007:8... 86 TCP 36566 → 443 [ACK] Seq=3 Ack=75 Win=502 Len=0 TSval=2222155963 TSecr=2445061288
5605 73.376061816 2404:6800:4009:8... 2401:4900:4b5f:f... 159 TLSv1.2 [TCP ACKed unseen segment] , Application Data
5606 73.376668876 2401:4900:4b5f:f... 2404:6800:4009:8... 86 TCP [TCP Previous segment not captured] 35136 → 443 [FIN, ACK] Seq=2 Ack=74 Win=502 Len=0 TSval=2176094007 TSecr=519238142
5607 73.463142292 2404:6800:4009:8... 2401:4900:4b5f:f... 159 TLSv1.2 [TCP ACKed unseen segment] [TCP Spurious Retransmission] , Application Data
5608 73.463167373 2401:4900:4b5f:f... 2404:6800:4009:8... 98 TCP [TCP Dup ACK 5606#1] 35136 → 443 [ACK] Seq=3 Ack=74 Win=502 Len=0 TSval=2176094091 TSecr=519238506 SLE=1 SRE=74
5609 73.471558792 2401:4900:4b5f:f... 2404:6800:4009:8... 86 TCP 443 → 35136 [FIN, ACK] Seq=74 Ack=3 Win=269 Len=0 TSval=519243534 TSecr=2176097107
5610 73.478541304 2401:4900:4b5f:f... 2404:6800:4009:8... 86 TCP 35136 → 443 [ACK] Seq=3 Ack=75 Win=502 Len=0 TSval=2176094107 TSecr=519238513
5611 74.196060088 2404:6800:4009:8... 2401:4900:4b5f:f... 159 TLSv1.2 [TCP ACKed unseen segment] , Application Data
5612 74.197263425 2401:4900:4b5f:f... 2404:6800:4009:8... 86 TCP [TCP Previous segment not captured] 57086 → 443 [FIN, ACK] Seq=2 Ack=74 Win=1824 Len=0 TSval=1463625785 TSecr=250333772
5613 74.301589471 2404:6800:4009:8... 2401:4900:4b5f:f... 86 TCP [TCP ACKed unseen segment] 443 → 57086 [FIN, ACK] Seq=74 Ack=3 Win=269 Len=0 TSval=250334113 TSecr=1463625785
5614 74.301631705 2401:4900:4b5f:f... 2404:6800:4009:8... 86 TCP 57086 → 443 [ACK] Seq=3 Ack=75 Win=1824 Len=0 TSval=1463625889 TSecr=250334113
Frame 1568: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface 0
Ethernet II, Src: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b), Dst: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Internet Protocol Version 4, Src: 192.168.43.96, Dst: 117.213.200.11
Transmission Control Protocol, Src Port: 45900, Dst Port: 8070, Seq: 1, Ack: 1, Len: 611
Hypertext Transfer Protocol
Ethernet (eth), 14 bytes
Packets: 5614 · Displayed: 5425 (96.6%)
Profile: Default
16:36:47


Report - Google Docs - ...
*wlan0
[dj@kali: ~]
16:37:04
73%
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression...
No. Time Source Destination Length Protocol Info
5002 65.058559540 192.168.43.244 192.168.43.96 76 DNS Standard query response 0xab7d No such name AAAA jiofi.local.html
5429 69.071200297 192.168.43.96 192.168.43.244 76 DNS Standard query 0xab7d A jiofi.local.html
5430 69.072318074 192.168.43.96 192.168.43.244 76 DNS Standard query 0xe161 AAAA jiofi.local.html
5431 69.084865441 192.168.43.244 192.168.43.96 76 DNS Standard query response 0xa56c No such name A jiofi.local.html
5432 69.084914433 192.168.43.244 192.168.43.96 76 DNS Standard query response 0xe161 No such name AAAA jiofi.local.html
5601 73.093697438 192.168.43.96 192.168.43.244 76 DNS Standard query 0x993f A jiofi.local.html
5602 73.096098152 192.168.43.96 192.168.43.244 76 DNS Standard query 0x573d AAAA jiofi.local.html
5603 73.103589148 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x993f No such name A jiofi.local.html
5604 73.103697472 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x573d No such name AAAA jiofi.local.html
5627 77.115718103 192.168.43.96 192.168.43.244 76 DNS Standard query 0x520f A jiofi.local.html
5628 77.116223385 192.168.43.96 192.168.43.244 76 DNS Standard query 0x8915 AAAA jiofi.local.html
5633 77.122143800 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x520f No such name A jiofi.local.html
5634 77.122250267 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x8915 No such name AAAA jiofi.local.html
5696 81.122689148 192.168.43.96 192.168.43.244 76 DNS Standard query 0x72f5 A jiofi.local.html
5697 81.129877985 192.168.43.96 192.168.43.244 76 DNS Standard query 0xeff6 AAAA jiofi.local.html
5698 81.134133808 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x72f5 No such name A jiofi.local.html
5699 81.134626651 192.168.43.244 192.168.43.96 76 DNS Standard query response 0xeff6 No such name AAAA jiofi.local.html
6394 85.144145317 192.168.43.96 192.168.43.244 76 DNS Standard query 0x6c8e A jiofi.local.html
6395 85.144195028 192.168.43.96 192.168.43.244 76 DNS Standard query 0x56f6 AAAA jiofi.local.html
6396 85.148228770 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x6c8e No such name A jiofi.local.html
6397 85.148368377 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x56f6 No such name AAAA jiofi.local.html
6540 89.157782759 192.168.43.96 192.168.43.244 76 DNS Standard query 0xdbde A jiofi.local.html
6541 89.157800941 192.168.43.96 192.168.43.244 76 DNS Standard query 0x83bc AAAA jiofi.local.html
6542 89.166793167 192.168.43.244 192.168.43.96 76 DNS Standard query response 0xd5be No such name A jiofi.local.html
6543 89.166851252 192.168.43.244 192.168.43.96 76 DNS Standard query response 0x83bc No such name AAAA jiofi.local.html
Frame 1535: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
Ethernet II, Src: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c), Dst: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b)
Internet Protocol Version 4, Src: 192.168.43.244, Dst: 192.168.43.96
User Datagram Protocol, Src Port: 53, Dst Port: 33355
Domain Name System (response)
Ethernet (eth), 14 bytes
Packets: 6608 · Displayed: 132 (2.0%)
Profile: Default
16:37:04

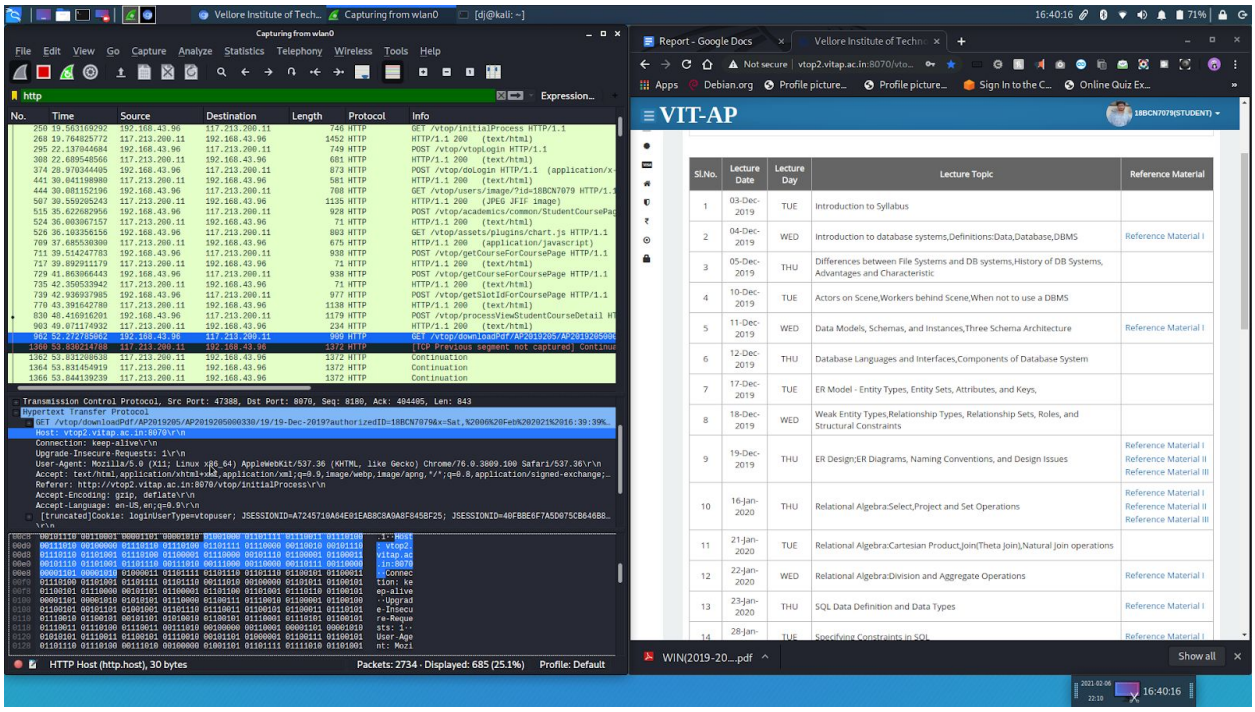
3. Use your Web browser to access a file from a Web server. Using Wireshark captures the packets arriving at your computer. Also download a Wireshark-readable packet trace from the Web server from which you downloaded the file. Using this server trace

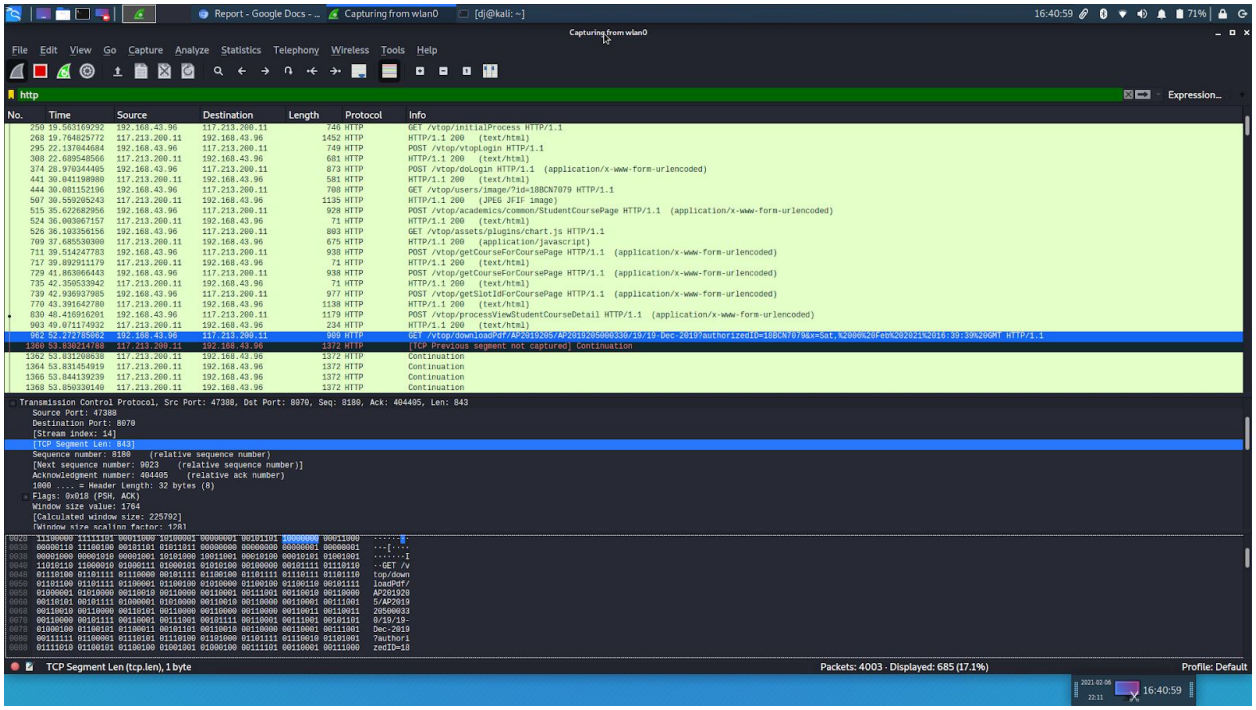
- Find the packets that were generated by your own access of the Web server.

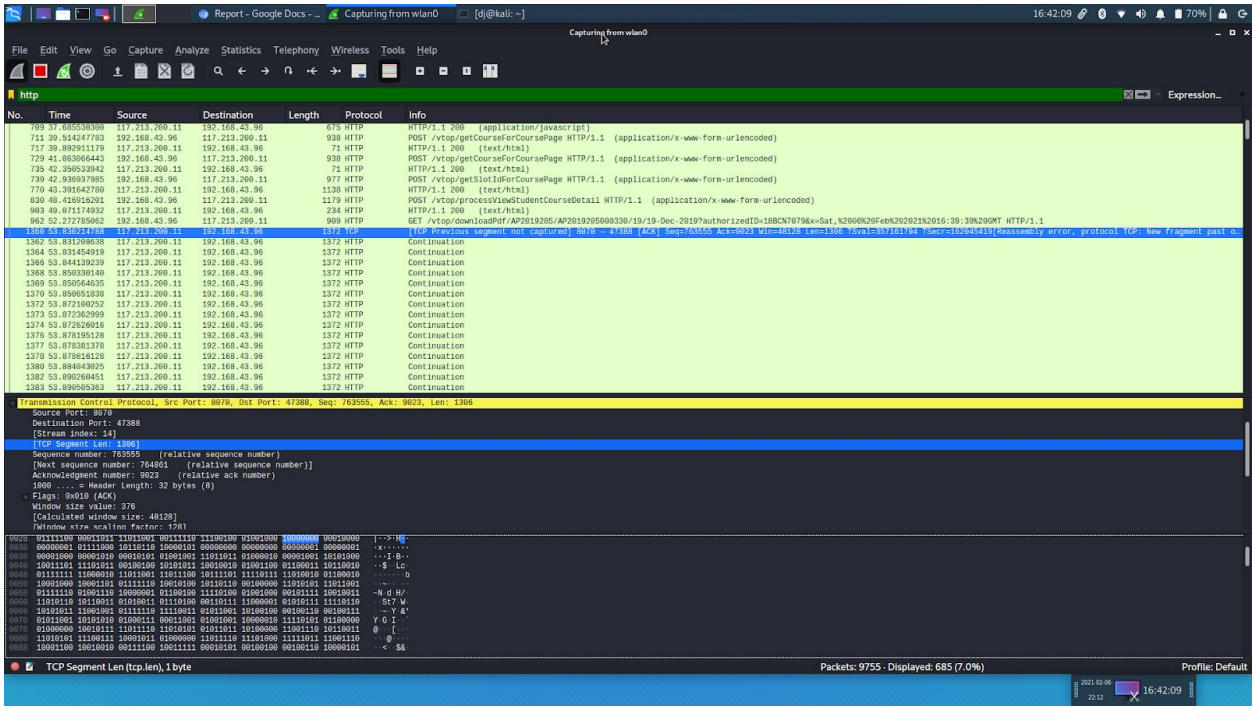
- Analyze the client- and server-side traces to explore aspects of TCP.

- Evaluate the performance of the TCP connection between your computer and the Web server.

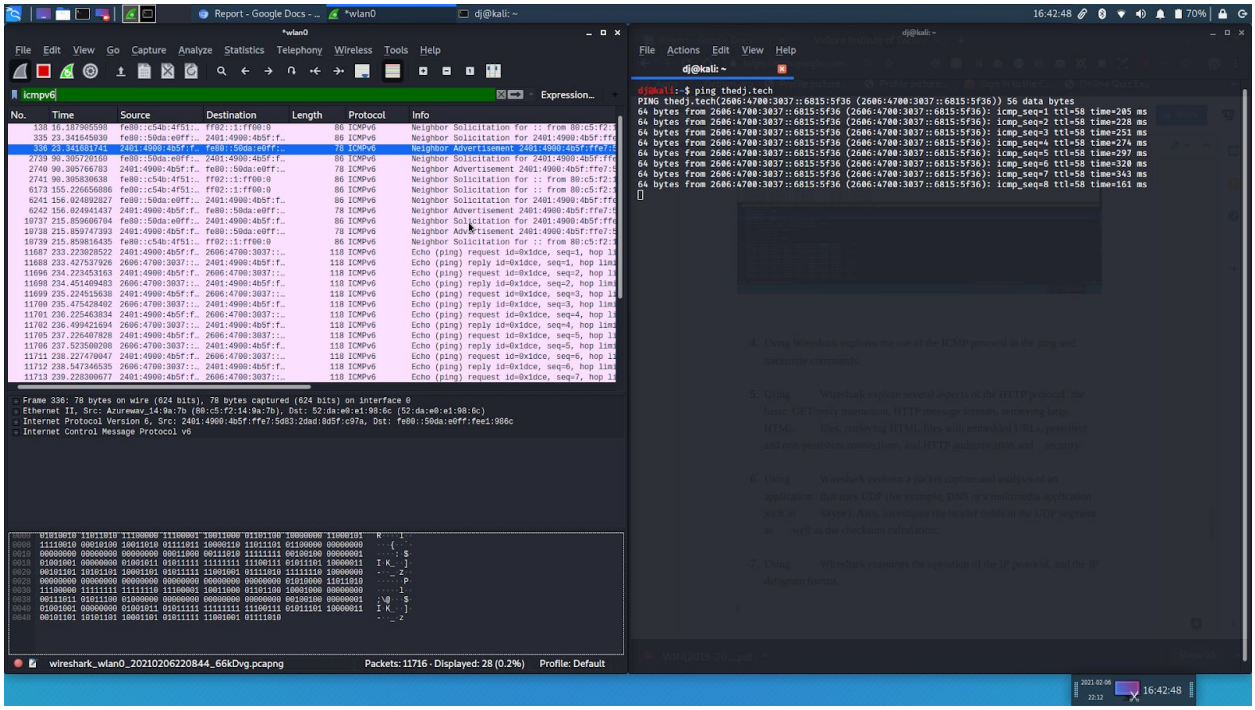
- Trace TCP's window behavior, and infer packet loss, retransmission, flow control and congestion control behavior, and estimated roundtrip time.



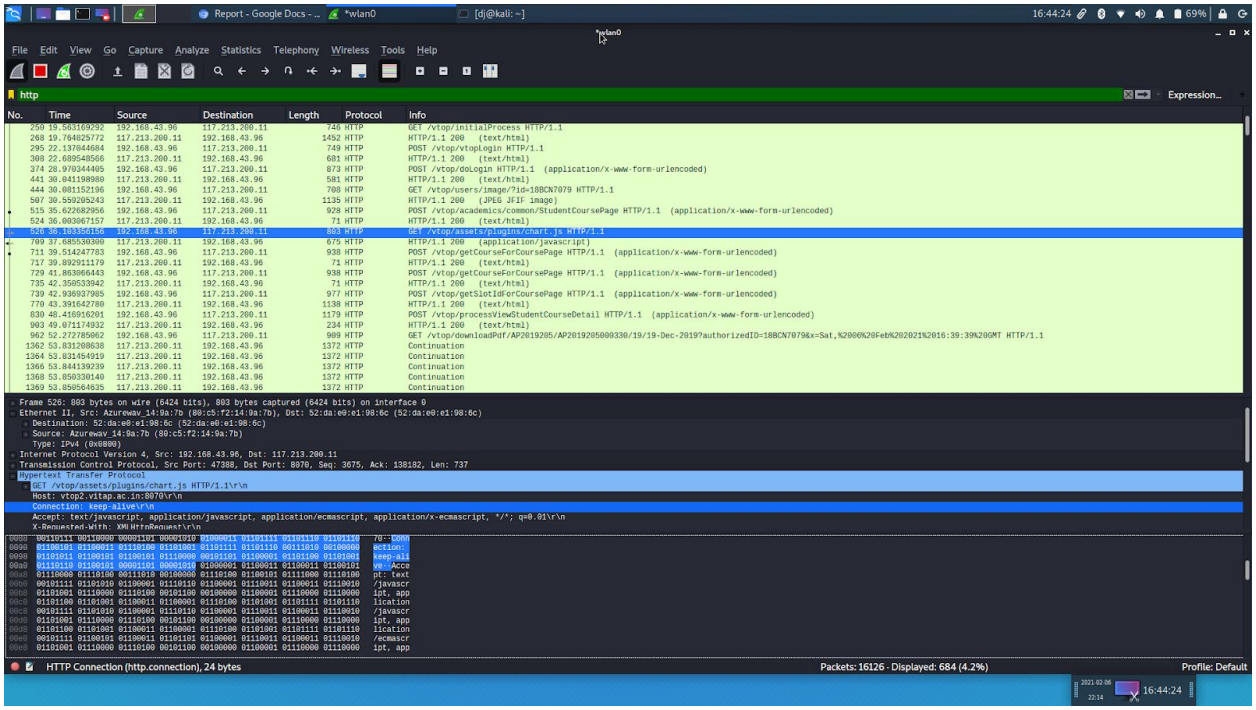

Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Length Protocol Info
250 19.568169292 192.168.43.96 117.213.200.11 746 HTTP GET /vtop/initialProcess HTTP/1.1
268 19.764825772 117.213.200.11 192.168.43.96 1452 HTTP HTTP/1.1 200 (text/html)
295 22.137044684 192.168.43.96 117.213.200.11 749 HTTP POST /vtop/vtopLogin HTTP/1.1
308 22.689548566 117.213.200.11 192.168.43.96 601 HTTP HTTP/1.1 200 (text/html)
374 28.970344405 192.168.43.96 117.213.200.11 873 HTTP POST /vtop/doLogin HTTP/1.1 (application/x-www-form-urlencoded)
441 30.041198980 117.213.200.11 192.168.43.96 581 HTTP HTTP/1.1 200 (text/html)
444 30.081152196 192.168.43.96 117.213.200.11 708 HTTP GET /vtop/users/image/?id=18BCN7079 HTTP/1.1
507 30.559205243 117.213.200.11 192.168.43.96 1135 HTTP HTTP/1.1 200 (JPEG JFIF image)
515 35.622682956 192.168.43.96 117.213.200.11 928 HTTP POST /vtop/academics/common/StudentCourseCopy HTTP/1.1 (application/x-www-form-urlencoded)
524 36.003067157 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
526 36.103356156 192.168.43.96 117.213.200.11 803 HTTP GET /vtop/assets/plugins/chart.js HTTP/1.1
709 37.685530300 117.213.200.11 192.168.43.96 675 HTTP HTTP/1.1 200 (application/javascript)
711 39.514247783 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
717 39.892911179 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
729 41.863066443 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
735 42.350533942 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
739 42.936937985 192.168.43.96 117.213.200.11 977 HTTP POST /vtop/getSlotIdForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
770 43.391642780 117.213.200.11 192.168.43.96 1138 HTTP HTTP/1.1 200 (text/html)
830 48.416916201 192.168.43.96 117.213.200.11 1179 HTTP POST /vtop/processViewStudentCourseDetail HTTP/1.1 (application/x-www-form-urlencoded)
903 49.071174932 117.213.200.11 192.168.43.96 234 HTTP HTTP/1.1 200 (text/html)
962 52.272785062 192.168.43.96 117.213.200.11 909 HTTP GET /vtop/downloadPdf/AP2019205000330/19/19-Dec-2019?authorizedID=18BCN7079&x=Sat,%2006%20Feb%202021%2016:39:39%20GMT HTTP/1.1
1360 53.830214788 117.213.200.11 192.168.43.96 1372 HTTP [TCP Previous segment not captured] Continuation
1362 53.831208638 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1364 53.831454919 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1366 53.844139239 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1368 53.850330140 117.213.200.11 192.168.43.96 1372 HTTP Continuation
Transmission Control Protocol, Src Port: 47388, Dst Port: 8070, Seq: 8180, Ack: 404405, Len: 843
Source Port: 47388
Destination Port: 8070
[Stream index: 14]
[TCP Segment Len: 843]
Sequence number: 8180 (relative sequence number)
[Next sequence number: 9023 (relative sequence number)]
Acknowledgment number: 404405 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window size value: 1764
[Calculated window size: 225792]
[Window size scaling factor: 128]
TCP Segment Len (tcp.len), 1 byte
Packets: 4003 · Displayed: 685 (17.1%)
Profile: Default
16:40:59

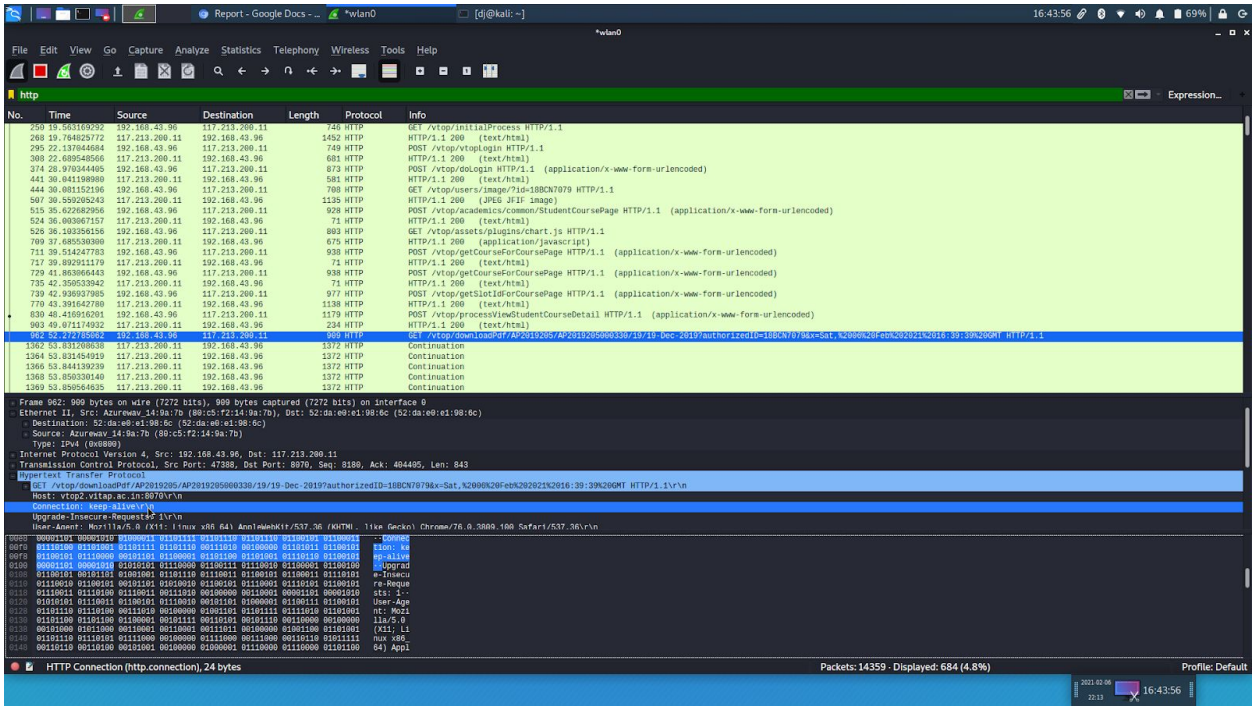

Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Length Protocol Info
709 37.685530300 117.213.200.11 192.168.43.96 675 HTTP HTTP/1.1 200 (application/javascript)
711 39.514247783 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
717 39.892911179 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
729 41.863066443 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
735 42.350533942 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
739 42.936937985 192.168.43.96 117.213.200.11 977 HTTP POST /vtop/getSlotIdForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
770 43.391642780 117.213.200.11 192.168.43.96 1138 HTTP HTTP/1.1 200 (text/html)
830 48.416916201 192.168.43.96 117.213.200.11 1179 HTTP POST /vtop/processViewStudentCourseDetail HTTP/1.1 (application/x-www-form-urlencoded)
903 49.071174932 117.213.200.11 192.168.43.96 234 HTTP HTTP/1.1 200 (text/html)
962 52.272785062 192.168.43.96 117.213.200.11 909 HTTP GET /vtop/downloadPdf/AP2019205000330/19/19-Dec-2019?authorizedID=18BCN7079&x=Sat,%2006%20Feb%202021%2016:39:39%20GMT HTTP/1.1
1360 53.830214788 117.213.200.11 192.168.43.96 1372 TCP [TCP Previous segment not captured] 8070 → 47388 [ACK] Seq=763555 Ack=9023 Win=48128 Len=1306 TSval=3571611704 TSecr=102045419[Reassembly error, protocol TCP: New fragment past o
1362 53.831208638 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1364 53.831454919 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1366 53.844139239 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1368 53.850330140 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1369 53.850564635 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1370 53.850651838 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1372 53.872100252 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1373 53.872362999 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1374 53.872626016 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1376 53.878195128 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1377 53.878381378 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1378 53.878616128 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1380 53.884043025 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1382 53.890260451 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1383 53.890505363 117.213.200.11 192.168.43.96 1372 HTTP Continuation
Transmission Control Protocol, Src Port: 8070, Dst Port: 47388, Seq: 763555, Ack: 9023, Len: 1306
Source Port: 8070
Destination Port: 47388
[Stream index: 14]
[TCP Segment Len: 1306]
Sequence number: 763555 (relative sequence number)
[Next sequence number: 764861 (relative sequence number)]
Acknowledgment number: 9023 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 376
[Calculated window size: 48128]
[Window size scaling factor: 128]
TCP Segment Len (tcp.len), 1 byte
Packets: 9755 · Displayed: 685 (7.0%)
Profile: Default
16:42:09

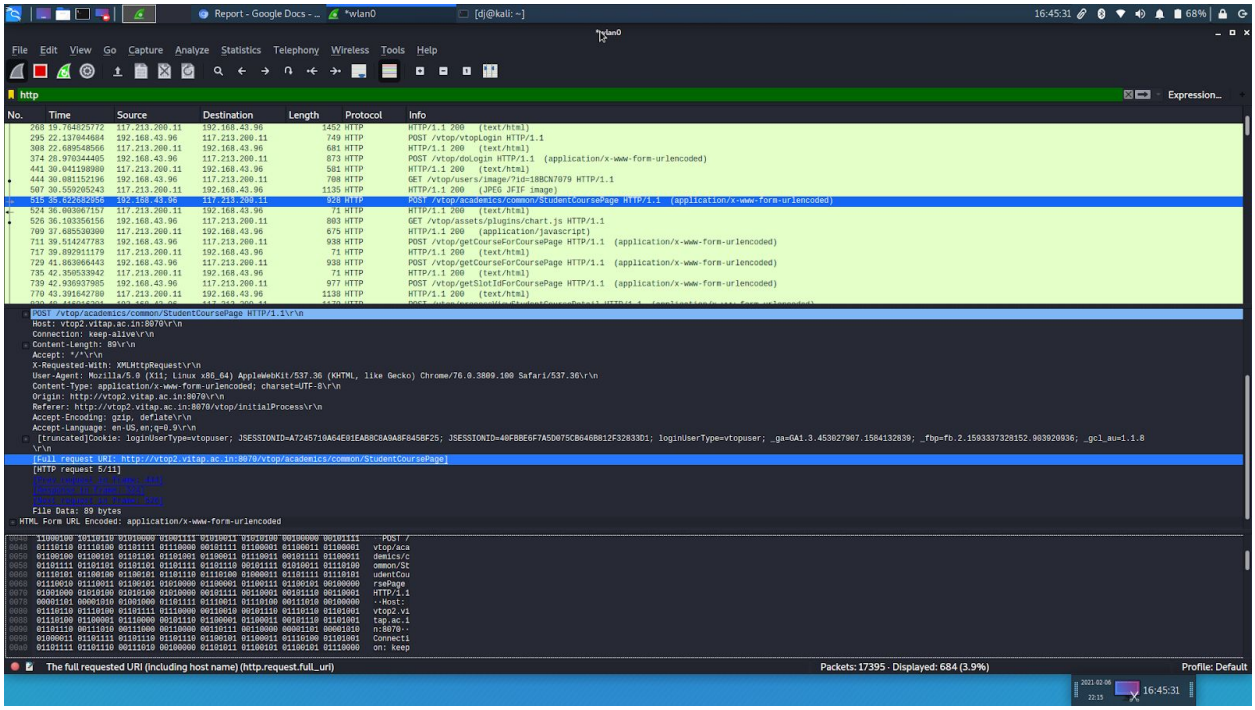
4. Using Wireshark explores the use of the ICMP protocol in the ping and traceroute commands.



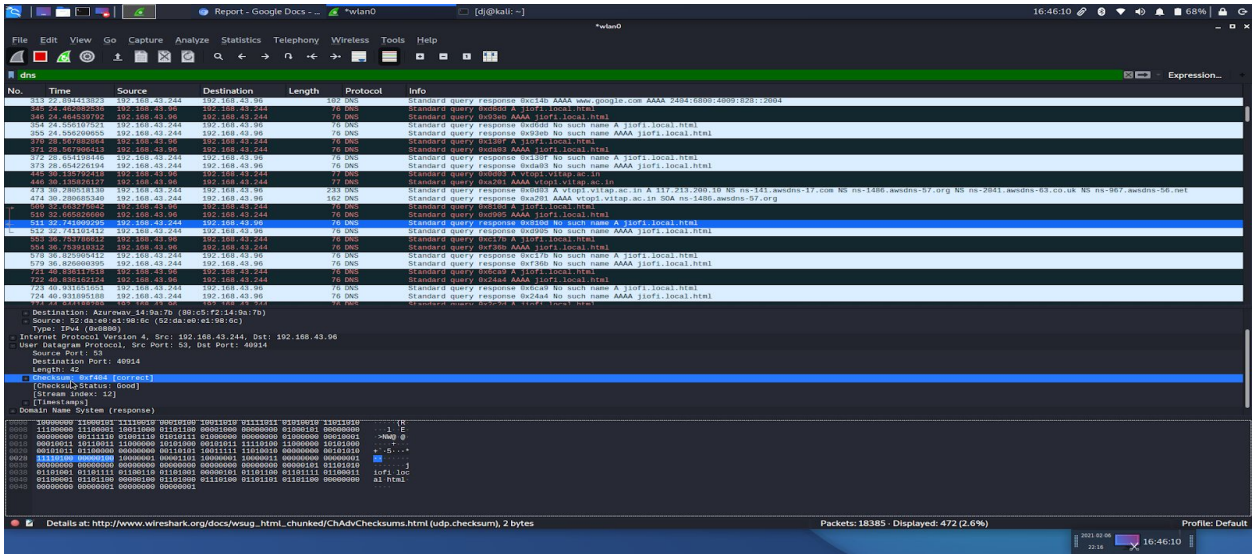
5. Using Wireshark explore several aspects of the HTTP protocol: the basic GET/reply interaction, HTTP message formats, retrieving large HTML files, retrieving HTML files with embedded URLs, persistent and non-persistent connections, and HTTP authentication and security.


Report - Google Docs - ...
*wlan0
[dj@kali: ~]
16:44:24
69%
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Length Protocol Info
250 19.563169292 192.168.43.96 117.213.200.11 746 HTTP GET /vtop/initialProcess HTTP/1.1
268 19.764825772 117.213.200.11 192.168.43.96 1452 HTTP HTTP/1.1 200 (text/html)
295 22.137044684 192.168.43.96 117.213.200.11 749 HTTP POST /vtop/vtopLogin HTTP/1.1
308 22.689548566 117.213.200.11 192.168.43.96 681 HTTP HTTP/1.1 200 (text/html)
374 28.970344405 192.168.43.96 117.213.200.11 873 HTTP POST /vtop/doLogin HTTP/1.1 (application/x-www-form-urlencoded)
441 30.041198980 117.213.200.11 192.168.43.96 581 HTTP HTTP/1.1 200 (text/html)
444 30.081152196 192.168.43.96 117.213.200.11 708 HTTP GET /vtop/users/image/?id=18BCN7079 HTTP/1.1
507 30.559205243 117.213.200.11 192.168.43.96 1135 HTTP HTTP/1.1 200 (JPEG JFIF image)
515 35.622682956 192.168.43.96 117.213.200.11 928 HTTP POST /vtop/academics/common/StudentCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
524 36.003067157 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
526 36.103356156 192.168.43.96 117.213.200.11 803 HTTP GET /vtop/assets/plugins/chart.js HTTP/1.1
709 37.685530300 117.213.200.11 192.168.43.96 675 HTTP HTTP/1.1 200 (application/javascript)
711 39.514247783 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
717 39.892911179 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
729 41.863066443 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
735 42.350533942 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
739 42.936937985 192.168.43.96 117.213.200.11 977 HTTP POST /vtop/getSlotIdForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
770 43.391642780 117.213.200.11 192.168.43.96 1138 HTTP HTTP/1.1 200 (text/html)
830 48.416916201 192.168.43.96 117.213.200.11 1179 HTTP POST /vtop/processViewStudentCourseDetail HTTP/1.1 (application/x-www-form-urlencoded)
903 49.071174932 117.213.200.11 192.168.43.96 234 HTTP HTTP/1.1 200 (text/html)
962 52.272785062 192.168.43.96 117.213.200.11 909 HTTP GET /vtop/downloadPdf/AP2019205/AP2019205000330/19/19-Dec-2019?authorizedID=18BCN7079&x=Sat,%2006%20Feb%202021%2016:39:39%20GMT HTTP/1.1
1362 53.831208638 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1364 53.831454919 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1366 53.844139239 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1368 53.850330140 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1369 53.850564635 117.213.200.11 192.168.43.96 1372 HTTP Continuation
Frame 526: 803 bytes on wire (6424 bits), 803 bytes captured (6424 bits) on interface 0
Ethernet II, Src: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b), Dst: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Destination: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Source: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.96, Dst: 117.213.200.11
Transmission Control Protocol, Src Port: 47388, Dst Port: 8070, Seq: 3675, Ack: 138182, Len: 737
Hypertext Transfer Protocol
GET /vtop/assets/plugins/chart.js HTTP/1.1\r\n
Host: vtop2.vitap.ac.in:8070\r\n
Connection: keep-alive\r\n
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01\r\n
X-Requested-With: XMLHttpRequest\r\n
HTTP Connection (http.connection), 24 bytes
Packets: 16126 · Displayed: 684 (4.2%)
Profile: Default
16:44:24

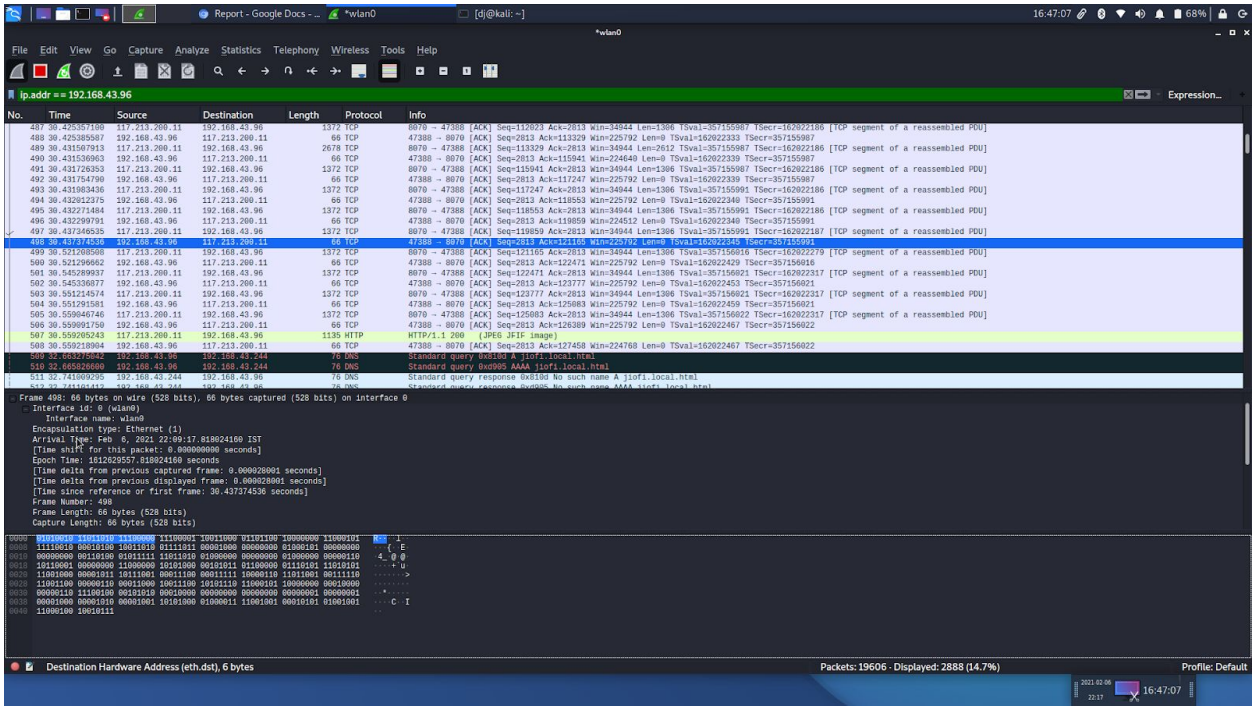

Report - Google Docs - ...
*wlan0
[dj@kali: ~]
16:43:56
69%
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Length Protocol Info
250 19.563169292 192.168.43.96 117.213.200.11 746 HTTP GET /vtop/initialProcess HTTP/1.1
268 19.764825772 117.213.200.11 192.168.43.96 1452 HTTP HTTP/1.1 200 (text/html)
295 22.137044684 192.168.43.96 117.213.200.11 749 HTTP POST /vtop/vtopLogin HTTP/1.1
308 22.689548566 117.213.200.11 192.168.43.96 681 HTTP HTTP/1.1 200 (text/html)
374 28.970344405 192.168.43.96 117.213.200.11 873 HTTP POST /vtop/doLogin HTTP/1.1 (application/x-www-form-urlencoded)
441 30.041198980 117.213.200.11 192.168.43.96 581 HTTP HTTP/1.1 200 (text/html)
444 30.081152196 192.168.43.96 117.213.200.11 708 HTTP GET /vtop/users/image/?id=18BCN7079 HTTP/1.1
507 30.559205243 117.213.200.11 192.168.43.96 1135 HTTP HTTP/1.1 200 (JPEG JFIF image)
515 35.622682956 192.168.43.96 117.213.200.11 928 HTTP POST /vtop/academics/common/StudentCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
524 36.003067157 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
526 36.103356156 192.168.43.96 117.213.200.11 803 HTTP GET /vtop/assets/plugins/chart.js HTTP/1.1
709 37.685530300 117.213.200.11 192.168.43.96 675 HTTP HTTP/1.1 200 (application/javascript)
711 39.514247783 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
717 39.892911179 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
729 41.863066443 192.168.43.96 117.213.200.11 938 HTTP POST /vtop/getCourseForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
735 42.350533942 117.213.200.11 192.168.43.96 71 HTTP HTTP/1.1 200 (text/html)
739 42.936937985 192.168.43.96 117.213.200.11 977 HTTP POST /vtop/getSlotIdForCoursePage HTTP/1.1 (application/x-www-form-urlencoded)
770 43.391642780 117.213.200.11 192.168.43.96 1138 HTTP HTTP/1.1 200 (text/html)
830 48.416916201 192.168.43.96 117.213.200.11 1179 HTTP POST /vtop/processViewStudentCourseDetail HTTP/1.1 (application/x-www-form-urlencoded)
903 49.071174932 117.213.200.11 192.168.43.96 234 HTTP HTTP/1.1 200 (text/html)
962 52.272785062 192.168.43.96 117.213.200.11 909 HTTP GET /vtop/downloadPdf/AP2019205/AP2019205000330/19/19-Dec-2019?authorizedID=18BCN7079&x=Sat,%2006%20Feb%202021%2016:39:39%20GMT HTTP/1.1
1362 53.831208638 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1364 53.831454919 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1366 53.844139239 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1368 53.850330140 117.213.200.11 192.168.43.96 1372 HTTP Continuation
1369 53.850564635 117.213.200.11 192.168.43.96 1372 HTTP Continuation
Frame 962: 909 bytes on wire (7272 bits), 909 bytes captured (7272 bits) on interface 0
Ethernet II, Src: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b), Dst: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Destination: 52:da:e0:e1:98:6c (52:da:e0:e1:98:6c)
Source: Azurewav_14:9a:7b (80:c5:f2:14:9a:7b)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.96, Dst: 117.213.200.11
Transmission Control Protocol, Src Port: 47388, Dst Port: 8070, Seq: 8180, Ack: 404405, Len: 843
Hypertext Transfer Protocol
GET /vtop/downloadPdf/AP2019205/AP2019205000330/19/19-Dec-2019?authorizedID=18BCN7079&x=Sat,%2006%20Feb%202021%2016:39:39%20GMT HTTP/1.1\r\n
Host: vtop2.vitap.ac.in:8070\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/537.36\r\n
HTTP Connection (http.connection), 24 bytes
Packets: 14359 · Displayed: 684 (4.8%)
Profile: Default
16:43:56



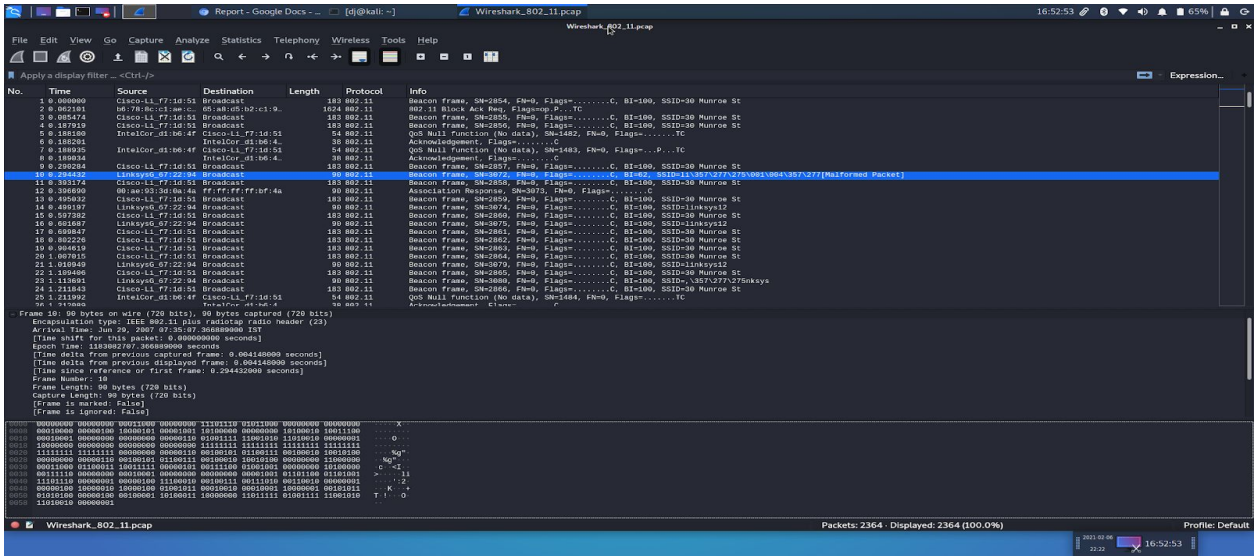
6. Using Wireshark perform a packet capture and analysis of an application that uses UDP (for example, DNS or a multimedia application such as Skype). Also, investigate the header fields in the UDP segment as well as the checksum calculation.



7. Using Wireshark examines the operation of the IP protocol, and the IP datagram format.



8. Using Wireshark lab perform capture and study the 802.11 frames exchanged between a wireless laptop and an access point.



CONCLUSION

We successfully experimented with WireShark.

REFERENCES

1. https://www.wireshark.org/
2. http://cs.gmu.edu/~astavrou/courses/ISA_674_F12/Wireshark-Tutorial.pdf
3. http://www-scf.usc.edu/~csci571/Special/Tutorials/wireshark_html/wireshark.html