

2020-07-31-traffic-analysis-exercise.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

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

No.	Time	Source	Destination	Protocol	Length	Info
520	69.046350	10.7.31.7	10.7.31.101	TCP	54	3268 → 49749 [ACK] Seq=2827 Ack=2373 Win=2102272 Len=0
518	69.046186	10.7.31.101	10.7.31.7	TCP	1514	49749 → 3268 [ACK] Seq=351 Ack=2827 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
517	69.041763	10.7.31.101	10.7.31.7	TCP	54	49749 → 3268 [ACK] Seq=351 Ack=2827 Win=262656 Len=0
515	69.041099	10.7.31.7	10.7.31.101	TCP	1514	3268 → 49749 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
513	69.035956	10.7.31.101	10.7.31.7	TCP	54	49749 → 3268 [ACK] Seq=1 Ack=1 Win=262656 Len=0
512	69.034282	10.7.31.7	10.7.31.101	TCP	66	3268 → 49749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
511	69.033987	10.7.31.101	10.7.31.7	TCP	66	49749 → 3268 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
506	67.943078	10.7.31.101	10.7.31.7	TCP	54	49745 → 49667 [RST, ACK] Seq=3672 Ack=1870 Win=0 Len=0
505	67.942977	10.7.31.101	10.7.31.7	TCP	54	49744 → 135 [RST, ACK] Seq=497 Ack=453 Win=0 Len=0
504	67.382876	10.7.31.101	10.7.31.7	TCP	66	49744 → 135 [ACK] Seq=497 Ack=453 Win=262144 Len=0 SLE=281 SRE=453
503	67.382815	10.7.31.101	10.7.31.7	TCP	66	49745 → 49667 [ACK] Seq=3672 Ack=1870 Win=262656 Len=0 SLE=1730 SRE=1870
502	67.368328	10.7.31.7	10.7.31.101	TCP	54	389 → 49746 [RST, ACK] Seq=3528 Ack=2870 Win=0 Len=0
500	67.368081	10.7.31.7	10.7.31.101	TCP	54	389 → 49747 [RST] Seq=3595 Win=0 Len=0
499	67.367992	10.7.31.101	10.7.31.7	TCP	54	49747 → 389 [FIN, ACK] Seq=2376 Ack=3595 Win=262400 Len=0
498	67.367784	10.7.31.7	10.7.31.101	TCP	54	389 → 49747 [RST, ACK] Seq=3595 Ack=2376 Win=0 Len=0
494	67.366829	10.7.31.101	10.7.31.7	TCP	54	49747 → 389 [ACK] Seq=2109 Ack=3345 Win=262656 Len=0
492	67.366683	10.7.31.7	10.7.31.101	TCP	1514	389 → 49747 [ACK] Seq=1671 Ack=2109 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
491	67.366675	10.7.31.7	10.7.31.101	TCP	1514	389 → 49747 [ACK] Seq=211 Ack=2109 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
488	67.365155	10.7.31.7	10.7.31.101	TCP	54	389 → 49747 [ACK] Seq=1 Ack=2023 Win=2102272 Len=0
486	67.365031	10.7.31.101	10.7.31.7	TCP	1514	49747 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
485	67.362999	10.7.31.101	10.7.31.7	TCP	54	49747 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
484	67.362826	10.7.31.7	10.7.31.101	TCP	66	389 → 49747 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
483	67.362677	10.7.31.101	10.7.31.7	TCP	66	49747 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
475	67.357199	10.7.31.7	10.7.31.101	TCP	54	389 → 49746 [ACK] Seq=2827 Ack=2373 Win=2102272 Len=0
473	67.357082	10.7.31.101	10.7.31.7	TCP	1514	49746 → 389 [ACK] Seq=351 Ack=2827 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
472	67.355208	10.7.31.101	10.7.31.7	TCP	54	49746 → 389 [ACK] Seq=351 Ack=2827 Win=262656 Len=0
470	67.355101	10.7.31.7	10.7.31.101	TCP	1514	389 → 49746 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
468	67.354010	10.7.31.101	10.7.31.7	TCP	54	49746 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
467	67.353000	10.7.31.7	10.7.31.101	TCP	66	389 → 49746 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

▶ Frame 52: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

▶ Ethernet II, Src: Dell_c6:b1:73 (00:0d:56:c6:b1:73), Dst: ASUSTekCOMPU_12:af:38 (00:0c:6e:12:af:38)

▶ Internet Protocol Version 4, Src: 10.7.31.7, Dst: 10.7.31.101

▶ Transmission Control Protocol, Src Port: 88, Dst Port: 49731, Seq: 1748, Ack: 1765, Len: 0

0000 00 0c 6e 12 af 38 00 0d 56 c6 b1 73 08 00 45 00 n 8 V s E

0010 00 28 07 45 40 00 80 06 a1 11 0a 07 1f 07 0a 07 (E@

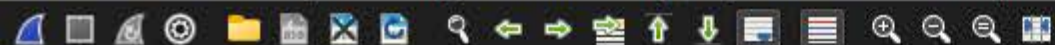
0020 1f 65 00 58 c2 43 98 0a 20 c2 1f bd 94 55 50 14 e X C UP

0030 00 00 2d dc 00 00

2020-07-31-traffic-analysis-exercise.pcap

Packets: 4593 · Displayed: 4593 (100.0%)

Profile: Default



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

No.	Time	Source	Destination	Protocol	Length	Info
444	67.341886	10.7.31.7	10.7.31.101	TCP	66	49667 → 49745 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
443	67.341717	10.7.31.101	10.7.31.7	TCP	66	49745 → 49667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
438	67.336967	10.7.31.101	10.7.31.7	TCP	54	49744 → 135 [ACK] Seq=1 Ack=1 Win=262656 Len=0
437	67.336027	10.7.31.7	10.7.31.101	TCP	66	135 → 49744 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
436	67.335817	10.7.31.101	10.7.31.7	TCP	66	49744 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
435	61.010713	10.7.31.101	10.7.31.7	TCP	54	49741 → 49667 [RST, ACK] Seq=3650 Ack=1870 Win=0 Len=0
434	61.010412	10.7.31.101	10.7.31.7	TCP	54	49740 → 135 [RST, ACK] Seq=497 Ack=453 Win=0 Len=0
433	61.008333	10.7.31.7	10.7.31.101	TCP	54	389 → 49742 [RST] Seq=3528 Win=0 Len=0
432	61.008252	10.7.31.101	10.7.31.7	TCP	54	49742 → 389 [FIN, ACK] Seq=2848 Ack=3528 Win=261888 Len=0
431	61.008171	10.7.31.7	10.7.31.101	TCP	54	389 → 49742 [RST, ACK] Seq=3528 Ack=2848 Win=0 Len=0
429	61.008016	10.7.31.7	10.7.31.101	TCP	54	389 → 49743 [RST] Seq=3595 Win=0 Len=0
428	61.007870	10.7.31.7	10.7.31.101	TCP	54	389 → 49743 [RST, ACK] Seq=3595 Ack=2354 Win=0 Len=0
427	61.007863	10.7.31.101	10.7.31.7	TCP	54	49743 → 389 [FIN, ACK] Seq=2354 Ack=3595 Win=262400 Len=0
423	61.006930	10.7.31.101	10.7.31.7	TCP	54	49743 → 389 [ACK] Seq=2087 Ack=3345 Win=262656 Len=0
421	61.006777	10.7.31.7	10.7.31.101	TCP	1514	389 → 49743 [ACK] Seq=1671 Ack=2087 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
420	61.006768	10.7.31.7	10.7.31.101	TCP	1514	389 → 49743 [ACK] Seq=211 Ack=2087 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
417	61.005433	10.7.31.7	10.7.31.101	TCP	54	389 → 49743 [ACK] Seq=1 Ack=2001 Win=2102272 Len=0
415	61.005289	10.7.31.101	10.7.31.7	TCP	1514	49743 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
414	61.004384	10.7.31.101	10.7.31.7	TCP	54	49743 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
413	61.004210	10.7.31.7	10.7.31.101	TCP	66	389 → 49743 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
412	61.004048	10.7.31.101	10.7.31.7	TCP	66	49743 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
404	61.000044	10.7.31.7	10.7.31.101	TCP	54	389 → 49742 [ACK] Seq=2827 Ack=2351 Win=2102272 Len=0
402	60.999910	10.7.31.101	10.7.31.7	TCP	1514	49742 → 389 [ACK] Seq=351 Ack=2827 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
401	60.999228	10.7.31.101	10.7.31.7	TCP	54	49742 → 389 [ACK] Seq=351 Ack=2827 Win=262656 Len=0
399	60.999088	10.7.31.7	10.7.31.101	TCP	1514	389 → 49742 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
397	60.998138	10.7.31.101	10.7.31.7	TCP	54	49742 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
396	60.998050	10.7.31.7	10.7.31.101	TCP	66	389 → 49742 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
395	60.997868	10.7.31.101	10.7.31.7	TCP	66	49742 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
377	60.086220	10.7.31.7	10.7.31.101	TCP	54	49667 → 49741 [ACK] Seq=1 Ack=2110 Win=2102272 Len=0

▶ Frame 52: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ Ethernet II, Src: Dell_c6:b1:73 (00:0d:56:c6:b1:73), Dst: ASUSTekCOMPU_12:af:38 (00:0c:6e:12:af:38)
▶ Internet Protocol Version 4, Src: 10.7.31.7, Dst: 10.7.31.101
▶ Transmission Control Protocol, Src Port: 88, Dst Port: 49731, Seq: 1748, Ack: 1765, Len: 0

```
0000  00 0c 6e 12 af 38 00 0d 56 c6 b1 73 08 00 45 00  .n.8.V.s.E
0010  00 28 07 45 40 00 80 06 a1 11 0a 07 1f 07 0a 07  (.E@.....
0020  1f 65 00 58 c2 43 98 0a 20 c2 1f bd 94 55 50 14  .e.XC.....UP
0030  00 00 2d dc 00 00
```