

A.mukesh
1920115051

Ethical Hacking for mobile applications - ITA1437

Ex.No. 6 - Use WireShark sniffer to capture network traffic and analyze

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The packet list pane on the left shows a list of captured packets, with the selected packet (No. 2750) highlighted in green. The packet details pane on the right shows the selected packet's details, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
2286	8.636728	20.189.173.7	172.18.64.198	TCP	60	443 → 61346 [ACK] Seq=1 Ack=229 Win=30336 Len=0
2580	9.883881	140.82.112.26	172.18.64.198	TLSv1.2	79	Application Data
2581	9.885530	172.18.64.198	140.82.112.26	TLSv1.2	83	Application Data
2582	9.891925	140.82.112.26	172.18.64.198	TCP	60	443 → 61124 [ACK] Seq=26 Ack=30 Win=277 Len=0
2714	10.440053	20.189.173.7	172.18.64.198	TCP	1514	443 → 61346 [PSH, ACK] Seq=1 Ack=229 Win=30336 Len=14
2715	10.440232	172.18.64.198	20.189.173.7	TCP	54	61346 → 443 [ACK] Seq=229 Ack=1461 Win=262144 Len=0
2718	10.442702	20.189.173.7	172.18.64.198	TCP	1514	443 → 61346 [ACK] Seq=1461 Ack=229 Win=30336 Len=1460
2719	10.443162	172.18.64.198	20.189.173.7	TCP	54	61346 → 443 [ACK] Seq=229 Ack=2921 Win=262144 Len=0
2725	10.446749	20.189.173.7	172.18.64.198	TCP	1514	443 → 61346 [ACK] Seq=2921 Ack=229 Win=30336 Len=1460
2726	10.447164	172.18.64.198	20.189.173.7	TCP	54	61346 → 443 [ACK] Seq=229 Ack=4381 Win=262144 Len=0
2743	10.453901	20.189.173.7	172.18.64.198	TCP	1514	443 → 61346 [ACK] Seq=4381 Ack=229 Win=30336 Len=1460
2744	10.454602	172.18.64.198	20.189.173.7	TCP	54	61346 → 443 [ACK] Seq=229 Ack=5841 Win=262144 Len=0
2746	10.454808	20.189.173.7	172.18.64.198	TLSv1.2	454	Server Hello, Certificate, Certificate Status, Server
2747	10.455503	172.18.64.198	20.189.173.7	TCP	54	61346 → 443 [ACK] Seq=229 Ack=6241 Win=261632 Len=0
2750	10.480841	172.18.64.198	111.119.15.0	TCP	66	61348 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
2751	10.487016	111.119.15.0	172.18.64.198	TCP	66	80 → 61348 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
2752	10.487294	172.18.64.198	111.119.15.0	TCP	54	61348 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

0000 38 90 a5 c8 4d 47 14 13 33 5e dd 6b 08 00 45 00 8...MG...3^k...E-
0010 01 1d 7f af 40 00 80 06 0e dc ac 12 40 c6 6f 77 ...@... ..@.ow
0020 0f 00 ef a4 00 50 0e 9b 5f f3 c9 6b e1 2c 50 18P... ..k.,P.
0030 02 01 e3 8f 00 00 47 45 54 20 2f 6d 73 64 6f 77GE T /msdow
0040 6e 6c 6f 61 64 2f 75 70 64 61 74 65 2f 76 33 2f nload/up date/v3/

Transmission Control Protocol: Protocol | Packets: 21788 · Displayed: 249 (1.1%) | Profile: Default