

Wireshark Practical

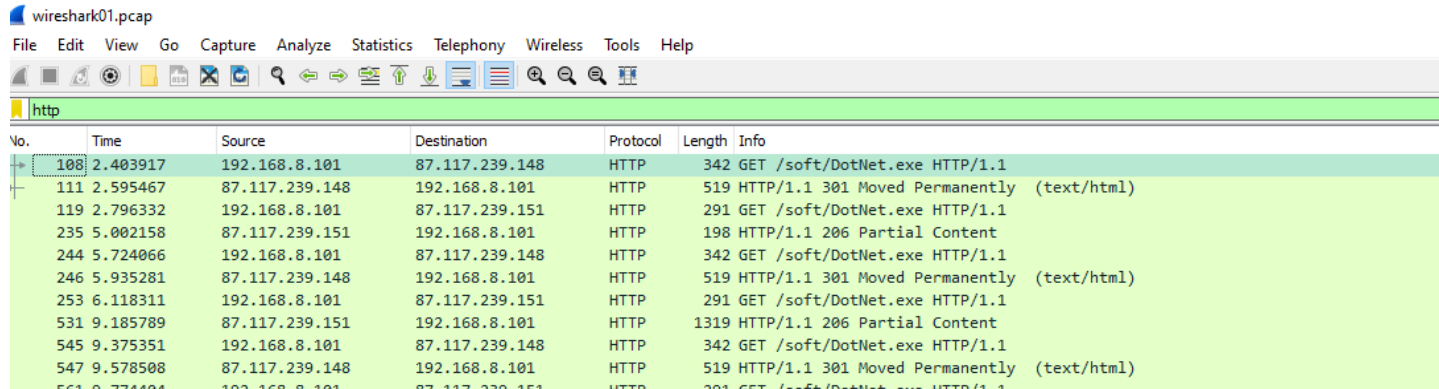
IS2111

Practical 05

B.G.S.S.W.Jayaweera
Index : 19020376

1. Enter following simple protocol names as filters and check whether such packets exist. Once you apply one filter, don't forget to click the clear button before applying another filter. Just deleting the text you entered does not clear the previous filter unless you click on the clear button.

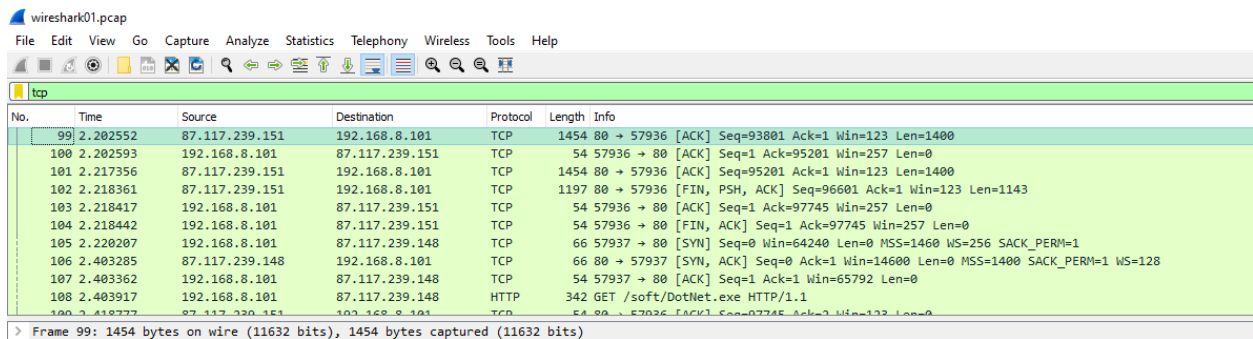
http



The screenshot shows the Wireshark interface with the packet capture filter set to 'http'. The packet list displays several HTTP GET requests from 192.168.8.101 to 87.117.239.148 and 87.117.239.151. The packet details pane shows the selected packet's structure, including the GET method and the requested resource.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 108 | 2.403917 | 192.168.8.101 | 87.117.239.148 | HTTP | 342 | GET /soft/DotNet.exe HTTP/1.1 |
| 111 | 2.595467 | 87.117.239.148 | 192.168.8.101 | HTTP | 519 | HTTP/1.1 301 Moved Permanently (text/html) |
| 119 | 2.796332 | 192.168.8.101 | 87.117.239.151 | HTTP | 291 | GET /soft/DotNet.exe HTTP/1.1 |
| 235 | 5.002158 | 87.117.239.151 | 192.168.8.101 | HTTP | 198 | HTTP/1.1 206 Partial Content |
| 244 | 5.724066 | 192.168.8.101 | 87.117.239.148 | HTTP | 342 | GET /soft/DotNet.exe HTTP/1.1 |
| 246 | 5.935281 | 87.117.239.148 | 192.168.8.101 | HTTP | 519 | HTTP/1.1 301 Moved Permanently (text/html) |
| 253 | 6.118311 | 192.168.8.101 | 87.117.239.151 | HTTP | 291 | GET /soft/DotNet.exe HTTP/1.1 |
| 531 | 9.185789 | 87.117.239.151 | 192.168.8.101 | HTTP | 1319 | HTTP/1.1 206 Partial Content |
| 545 | 9.375351 | 192.168.8.101 | 87.117.239.148 | HTTP | 342 | GET /soft/DotNet.exe HTTP/1.1 |
| 547 | 9.578508 | 87.117.239.148 | 192.168.8.101 | HTTP | 519 | HTTP/1.1 301 Moved Permanently (text/html) |

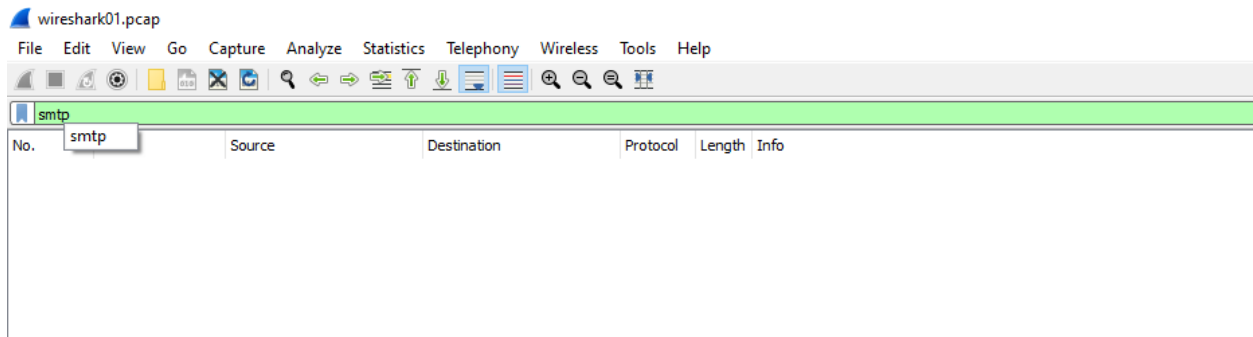
tcp



The screenshot shows the Wireshark interface with the packet capture filter set to 'tcp'. The packet list displays several TCP packets, including ACKs and a FIN packet. The packet details pane shows the selected packet's structure, including the TCP header and the application data.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 99 | 2.202552 | 87.117.239.151 | 192.168.8.101 | TCP | 1454 | 80 → 57936 [ACK] Seq=93801 Ack=1 Win=123 Len=1400 |
| 100 | 2.202593 | 192.168.8.101 | 87.117.239.151 | TCP | 54 | 57936 → 80 [ACK] Seq=1 Ack=95201 Win=257 Len=0 |
| 101 | 2.217356 | 87.117.239.151 | 192.168.8.101 | TCP | 1454 | 80 → 57936 [ACK] Seq=95201 Ack=1 Win=123 Len=1400 |
| 102 | 2.218361 | 87.117.239.151 | 192.168.8.101 | TCP | 1197 | 80 → 57936 [FIN, PSH, ACK] Seq=96601 Ack=1 Win=123 Len=1143 |
| 103 | 2.218417 | 192.168.8.101 | 87.117.239.151 | TCP | 54 | 57936 → 80 [ACK] Seq=1 Ack=97745 Win=257 Len=0 |
| 104 | 2.218442 | 192.168.8.101 | 87.117.239.151 | TCP | 54 | 57936 → 80 [FIN, ACK] Seq=1 Ack=97745 Win=257 Len=0 |
| 105 | 2.220207 | 192.168.8.101 | 87.117.239.148 | TCP | 66 | 57937 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 106 | 2.403285 | 87.117.239.148 | 192.168.8.101 | TCP | 66 | 80 → 57937 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1 WS=128 |
| 107 | 2.403362 | 192.168.8.101 | 87.117.239.148 | TCP | 54 | 57937 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0 |
| 108 | 2.403917 | 192.168.8.101 | 87.117.239.148 | HTTP | 342 | GET /soft/DotNet.exe HTTP/1.1 |

smtp



The screenshot shows the Wireshark interface with the packet capture filter set to 'smtp'. The packet list is currently empty, indicating that no SMTP packets were captured in the selected time range.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------|--------|-------------|----------|--------|------|
|-----|------|--------|-------------|----------|--------|------|

arp

wireshark01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-----------|-------------------|-------------------|----------|--------|---|
| 158 | 3.217254 | HuaweiTe_5f:3e:b9 | HonHaiPr_30:92:7b | ARP | 42 | Who has 192.168.8.101? Tell 192.168.8.1 |
| 159 | 3.217269 | HonHaiPr_30:92:7b | HuaweiTe_5f:3e:b9 | ARP | 42 | 192.168.8.101 is at 74:40:bb:30:92:7b |
| 6098 | 50.136303 | HuaweiTe_5f:3e:b9 | HonHaiPr_30:92:7b | ARP | 42 | Who has 192.168.8.101? Tell 192.168.8.1 |
| 6099 | 50.136319 | HonHaiPr_30:92:7b | HuaweiTe_5f:3e:b9 | ARP | 42 | 192.168.8.101 is at 74:40:bb:30:92:7b |
| 10089 | 94.459400 | HuaweiTe_5f:3e:b9 | HonHaiPr_30:92:7b | ARP | 42 | Who has 192.168.8.101? Tell 192.168.8.1 |
| 10090 | 94.459419 | HonHaiPr_30:92:7b | HuaweiTe_5f:3e:b9 | ARP | 42 | 192.168.8.101 is at 74:40:bb:30:92:7b |