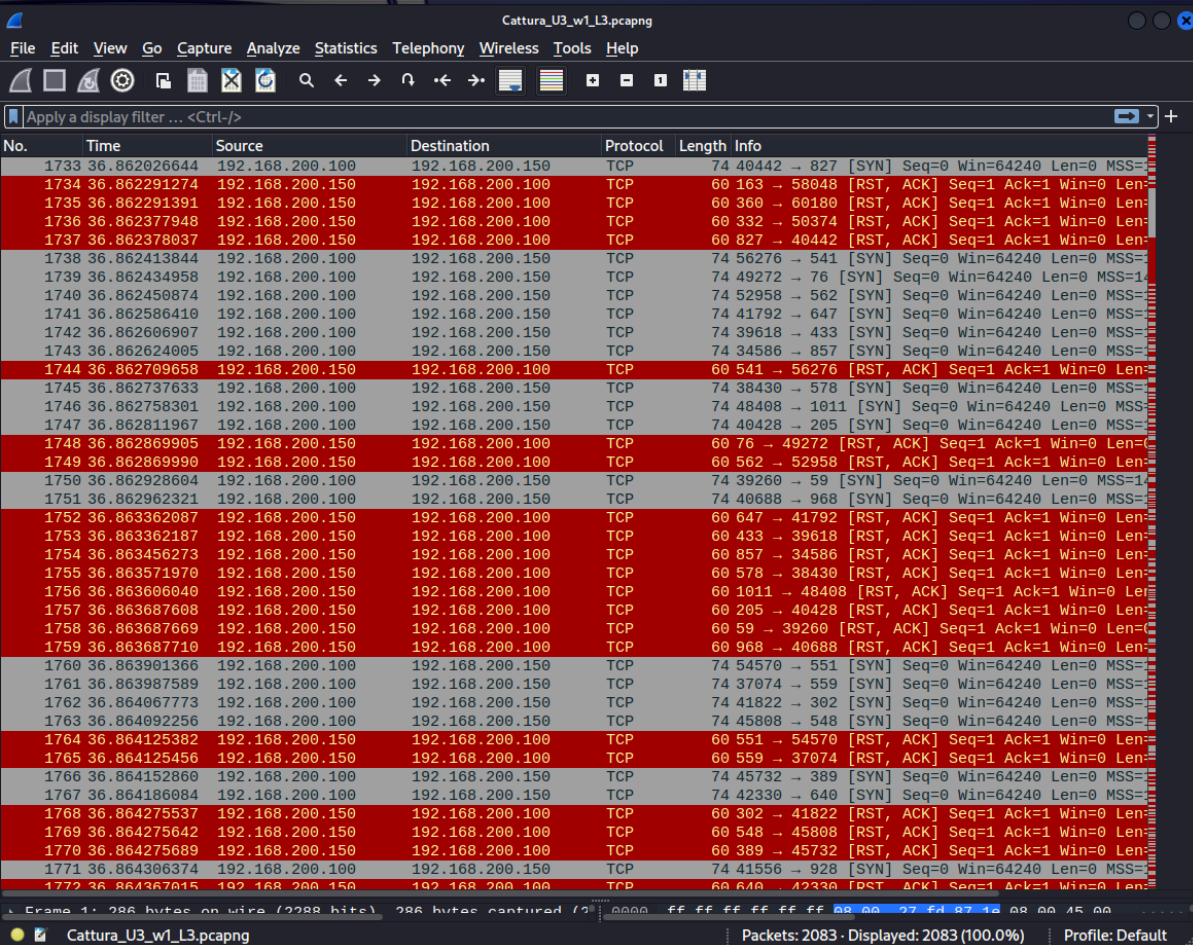


ESERCIZIO 3 SETTIMANA 9



The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows a series of TCP packets. The packet details pane on the right shows the structure of a selected packet, including the Ethernet II header, Internet Protocol header, and Transmission Control Protocol header. The packet list shows a series of TCP RST and ACK packets from 192.168.200.100 to 192.168.200.150. The packet details pane shows the structure of a selected packet, including the Ethernet II header, Internet Protocol header, and Transmission Control Protocol header.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|-----------------|-----------------|----------|--------|--|
| 1733 | 36.862026644 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40442 → 827 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1734 | 36.862291274 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 163 → 58048 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1735 | 36.862291391 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 360 → 60180 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1736 | 36.862377948 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 332 → 50374 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1737 | 36.862378037 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 827 → 40442 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1738 | 36.862413844 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 56276 → 541 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1739 | 36.862434958 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49272 → 76 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1740 | 36.862450874 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52958 → 562 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1741 | 36.862586410 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41792 → 647 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1742 | 36.862606907 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 39618 → 433 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1743 | 36.862624005 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34586 → 857 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1744 | 36.862709658 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 541 → 56276 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1745 | 36.862737633 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 38430 → 578 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1746 | 36.862758301 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 48408 → 1011 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1747 | 36.862811967 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40428 → 205 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1748 | 36.862869905 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 76 → 49272 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1749 | 36.862869990 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 562 → 52958 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1750 | 36.862928604 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 39260 → 59 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1751 | 36.862962321 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 40688 → 968 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1752 | 36.863362087 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 647 → 41792 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1753 | 36.863362187 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 433 → 39618 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1754 | 36.863456273 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 857 → 34586 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1755 | 36.863571970 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 578 → 38430 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1756 | 36.863606040 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 1011 → 48408 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1757 | 36.863687608 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 205 → 40428 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1758 | 36.863687669 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 59 → 39260 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1759 | 36.863687710 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 968 → 40688 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1760 | 36.863901366 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54570 → 551 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1761 | 36.863987589 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37074 → 559 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1762 | 36.864067773 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41822 → 302 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1763 | 36.864092256 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45808 → 548 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1764 | 36.864125382 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 551 → 54570 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1765 | 36.864125456 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 559 → 37074 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1766 | 36.864152860 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45732 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1767 | 36.864186084 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42330 → 640 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1768 | 36.864275537 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 302 → 41822 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1769 | 36.864275642 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 548 → 45808 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1770 | 36.864275689 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 389 → 45732 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |
| 1771 | 36.864306374 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41556 → 928 [SYN] Seq=0 Win=64240 Len=0 MSS= |
| 1772 | 36.864367015 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 640 → 42330 [RST, ACK] Seq=1 Ack=1 Win=0 Len= |

Identifichiamo vari IOC in questo screenshot, possiamo notare varie richieste TCP da parte dell'IP 192.168.200.100 tramite RST, ACK. Possiamo pensare che ci sia una scansione in atto. Potremmo configurare delle policy firewall per bloccare l'accesso a tutte le porte da parte di quel determinato attaccante, in modo tale da evitare che informazioni circa porta / servizi in ascolto finiscano nelle mani dell'attaccante.