

Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

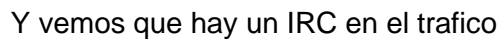
**Lab33 - Detect Suspicious
Protocols or Applications**

Prof. Ismael Jiménez Sánchez

**Alumno(a). Laury del Rosario Mex
Martin**

Ciclo 2020-B

Primero entraremos en Estadísticas| Jerarquía de Protocolo y nos saldrá una ventana en donde vemos los protocolos que aparecieron en el trafico



The figure displays a Wireshark network traffic analysis window titled "general101c.pcapng". It shows a list of captured packets in the top pane and a detailed view of selected packets in the bottom pane.

Packets List:

| No. | Time | TCP Delta | Source | Destination | Protocol | Host | Info |
|-----|----------|-------------|---------------|---------------|----------|------|--|
| 566 | 0.004936 | 0.004936000 | 24.6.173.220 | 67.220.66.111 | IRC | | Request (CAP) |
| 569 | 0.001637 | 0.028091000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (NOTICE) (NOTICE) |
| 570 | 0.000129 | 0.000129000 | 24.6.173.220 | 67.220.66.111 | IRC | | Request (NICK) (USER) |
| 579 | 0.000001 | 0.044202000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (NOTICE) |
| 581 | 0.073444 | 0.073585000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (NOTICE) (CAP) |
| 583 | 0.006503 | 0.006503000 | 24.6.173.220 | 67.220.66.111 | IRC | | Request (CAP) |
| 584 | 0.038451 | 0.038451000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (CAP) |
| 585 | 0.000348 | 0.000348000 | 24.6.173.220 | 67.220.66.111 | IRC | | Request (CAP) |
| 586 | 0.026163 | 0.026163000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (PING) |
| 587 | 0.000459 | 0.000459000 | 24.6.173.220 | 67.220.66.111 | IRC | | Request (PONG) |
| 588 | 0.027775 | 0.027775000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (001) (002) (003) (004) (005) (006) (042) (251) (252) |
| 589 | 0.001404 | 0.001404000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (ne) (254) (255) (265) (266) (250) (375) (372) (372) (372) (372) (372) (372) (372) (372) (372) |
| 591 | 0.000843 | 0.000843000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (-----) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) |
| 592 | 0.000002 | 0.000002000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (-----) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) |
| 593 | 0.000002 | 0.000002000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) |
| 595 | 0.000004 | 0.000004000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (rd) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) |
| 596 | 0.000004 | 0.000004000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (cleak) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) (372) |
| 598 | 0.000778 | 0.000778000 | 67.220.66.111 | 24.6.173.220 | IRC | | Request (USERHOST) |
| 603 | 0.001195 | 0.00112000 | 24.6.173.220 | 67.220.66.111 | IRC | | Response (302) |
| 604 | 0.031730 | 0.031730000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (NOTICE) (NOTICE) (NOTICE) (NOTICE) |
| 605 | 0.017595 | 0.017595000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (nterprises,) |
| 606 | 0.000009 | 0.000009000 | 67.220.66.111 | 24.6.173.220 | IRC | | Request (LIST) |
| 655 | 0.026767 | 0.026767000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (321) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) |
| 656 | 0.026767 | 0.026767000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (iterations!) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) |
| 657 | 0.001804 | 0.001804000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (net) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) |
| 658 | 0.000003 | 0.000003000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (new) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) |
| 659 | 0.000007 | 0.000007000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (lomew.2600.net) |
| 660 | 0.000006 | 0.000006000 | 67.220.66.111 | 24.6.173.220 | IRC | | Response (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) (322) |
| 661 | 0.000002 | 0.0 | | | | | |

The screenshot shows a Wireshark capture of a 2600net IRC session. The packet list on the left shows various messages. The packet details pane on the right shows the structure of an IRC message. The packet bytes pane on the right shows the raw data. The main packet list pane shows a series of messages from bartholomew.2600.net to mregion, including a welcome message and a list of server statistics.