Seminari Wireshark

Configuració: Edit → Preferences

1. Escollim la interfície

Funciona a partir de directors → Prog / DLL

- Oficial (Director) (ethernet...) [ETH → IP → TCP → HTTP]
- Heurístic

Filtres:

- De captura: Aplicats al trànsit d'entrada

[not] primitiva [and / or] [not] primitiva

↳ primitiva:
- tipus: host, net, port
- direcció: src, dst, inbound...
- protocol: ether, ip, udp...

. src host 192.168.1.10 and icmp [icmptype] != icmp-echo

. ip[2:2] > 576 and tcp[13] & 3 = 0

- De visualització: Aplicats al trànsit capturat

expressió [and (&&) / or (||) / xor (^^) / in / [...]] expressió...

Wireshark:

- Name Resolution: Tot unchecked
- Protocols:
  - Ethernet: Tot unchecked
  - IPv4 i v6: Reassemble fragmented ⇒ Unchecked [2]; Show IPv4 summary ⇒ Checked [3]
  - TCP: Show TCP ✓ [1]; [2-6] X i demés; Calculate conversation: ✓

UDP: Show UDP Summary: ✓
Calculate conversations
Demés: X

Exemples:

tcp.flags.fin == 1 ← A la part superior o menú contextual

http ← No captura tots els paquets http !http and tcp.port == 80

↳ tcp.port == 80

tcp.flags.syn ⇒ tcp.flags.syn == 1 ← els syn activats

Menú Analyze:

Seleccionar un paquet ⇒ Analyse ⇒ Apply as filter ⇒ Selected
⇒ Prepare as a filter
⇒ Conversation filter
⇒ Follow

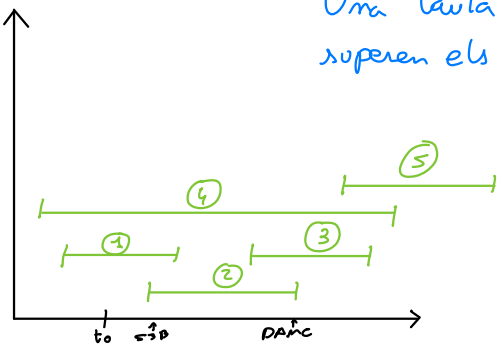
Menú Satistics:

⇒ Capture file statistics
⇒ Protocol Hierarchy
⇒ Conversations
⇒ I/O Graphics
⇒ Flow Graph

Pràctica 3:

Una taula de 18 i l'altra de 15, les demés no superen els 8 items.

Gràfic de pastís > 0%. !!!



⇒ És una