MODULO ETHERNET Gruppo _____ Classe _____

LAB: WIRESHARK & ETHERNET T =100' Data_____

Obiettivi: analizzare le schermate (pannelli) dell'applicativo Wireshark (W), potente e diffuso "sniffer" per reti locali con lo scopo di apprendere nei dettagli il protocollo studiato (Ethernet in questo caso).

Seguire le istruzioni e rispondere ai quesiti della scheda prepara alla verifica pratica su Wireshark&Ethernet.

Premessa: consultare il tutorial "Wireshark Intro" presente in eLearning.

PARTE I

1. Wireshark presenta: un menu in alto; la barra dei pulsanti; la barra dei filtri di visualizzazione; 3 pannelli: Packet List -- Packet Details -- Packet Bytes; la barra di stato. Individuare esattamente queste sezioni di Wireshark
2. Selezionare il frame n°1. Quali info vengono sinteticamente esposte nel Packet Details a destra di "> Frame 1:" ? Cosa succede se espandiamo la riga cliccando sul segno ">" ?
3. Selezionare il frame n°1. Quali info vengono sinteticamente esposte nel Packet Details a destra di "> Ethernet 2" ? qual è il significato dei byte (0c:3b: ….) ? Qual è il significato della stringa Micro-St ? (cercare di rispondere anche cercando su Internet)
4. Espandete la riga cliccando su ">". Quali indicazioni appaiono? Sapete ricondurle ai campi del protocollo studiati a teoria?
5. Quali info vengono mostrate espandendo il campo "Destination"? Osservate come vengono decodificate le informazioni, senza sforzo alcuno da parte dell'utente; cosa c'è di interessante?
6. Espandete ora il campo "Source"; che differenze trovate rispetto al campo "Destination" ?
7. Cliccate sulle info, una ad una, mostrate nel pannello Packet Details; cosa appare nel pannello Packet Bytes? Che informazioni vengono fornite? A sinistra e a destra.
8. Quali informazioni vengono rappresentate nel pannello Packet List? In particolare: Quale informazione è esposta nelle colonne "Source" e "Destination"? Quale informazione è rappresentata nella colonna "protocol"? La colonna length di quale grandezza tratta?
9. Frame 18: Qual è il tipo del frame Ethernet? Espandere la 2ª riga (IEEE…); l'indicazione "Length" riporta un numero: giustificarlo esattamente; corrisponde alla lunghezza del frame? Cosa viene trascurato? Consultare il pannello Packet Bytes e trovare corrispondenze col pannello Packet Details. Fate la stessa analisi per l'indicazione "padding"
10. Qual è il protocollo trasportato dal frame n° 18?
11. Partendo dal frame n° 18 cercare un altro pacchetto LLC
12. Come dovrebbe essere letta l'informazione rappresentata nel campo "source" del frame n° 5?
13. Considerare un frame a caso e reperire le informazioni richieste analizzando i pannelli di Wireshark nel dettaglio: da quanti byte è costituito il frame secondo Wireshark? In questi byte sono conteggiati preambolo, SFD e FCS?

PARTE II

14. Per pochi secondi catturate traffico dalla propria scheda di rete.
15. Stoppare la cattura e analizzare il traffico. Qual è l'indirizzo MAC della NIC montata sul tuo PC? Chi ha costruito la tua NIC?

16. Trascrivere il nome di 3 OUI, con il loro codice
17. Esistono frame multicast nel file di cattura che stai esaminando?
18. Consulta le dispense fornite in eLearning e trova altri particolari che Wireshark offre
19. Decodificare i campi dell'header Ethernet del frame 14//3 (scrivere qlcs del tipo: campo1=valore, campo2=…)
20. Cosa rappresenta il campo Protocol della packet list window?
21. Quali sono le dimensioni del payload del frame Ethernet n° 2 ?
22. Individuare un frame 802.3
23. Nella packet list window quali indirizzi sono riportati come source e destination? A che livello fanno riferimento? Con quali protocolli (indicarne almeno 1) viene mostrato l'indirizzo MAC? Sai dare una motivazione?
24. Perché Wireshark mostra l'indirizzo MAC effettivo degli host locali, ma non l'indirizzo MAC effettivo degli host remoti?
25. Voglio togliere dai frame nel pannello Packet List quelli che segnalati col protocollo ARP? Quale filtro devo utilizzare (consulta il materiale su Elearning→Ethernet)? Come faccio a rimuovere il filtro appena applicato?
26. Come si possono filtrare i frame che partono-arrivano alla NIC con indirizzo 30:9c:23:0c:3B:A9? (scrivere il filtro)
27. Chi è il destinatario del frame 3? Motivare o consultare il Panel Details per la risposta corretta.