

Wifi MÓDULO: INTRODUCCIÓN AL PROTOCOLO 802.11

Taller 1

Actividad de aprendizaje:

El siguiente taller tiene como objetivo que el Aprendiz analice un archivo de captura de tráfico de una red inalámbrica con autenticación 802.11 y comprenda aspectos básicos de los paquetes.

Para esta actividad el aprendiz deberá:

Tener máquina virtual Kali Linux actualizada con la herramienta Wireshark.

Actividades del taller

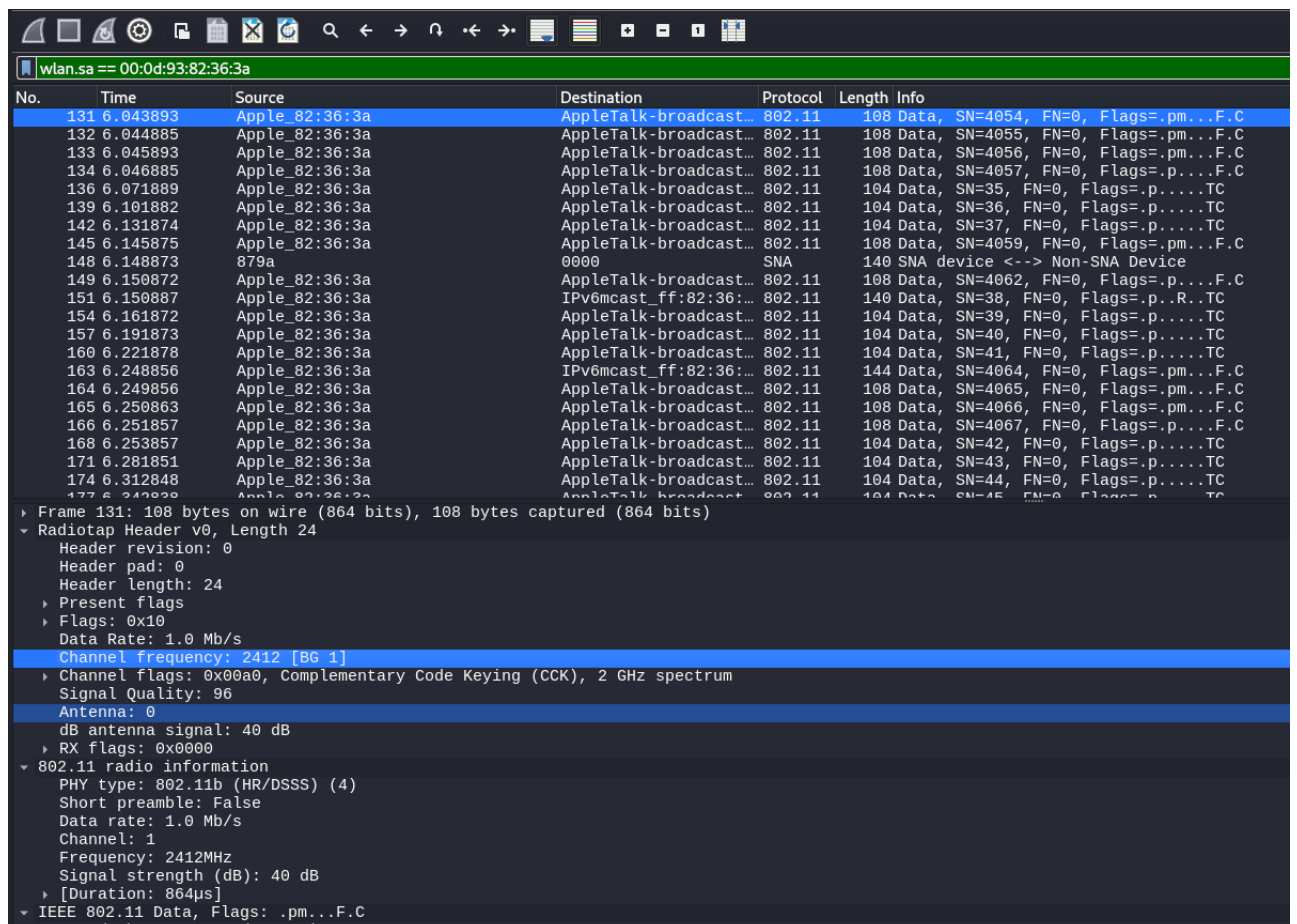
1. iniciar máquina virtual Kali
2. Descargar archivo de captura sobre el cual se realizará el análisis
3. abrir la herramienta Wireshark
4. abrir el archivo de captura con extensión .pcap
5. analizar los diferentes dispositivos identificados, relacionarlos en una tabla
6. analizar los diferentes protocolos identificados, relacionarlos en una tabla
7. analizar los diferentes flags identificados dentro de los paquetes y protocolo (escoja 5 paquetes o trazas aleatorias)

El objetivo de este taller es comprender cómo se ve una traza de red 802.11, aprender a analizar e identificar aspectos necesarios para una investigación o revisión de redes.

Dado que no tengo una antena para poder utilizar el modo monitor de esta he tenido que descargarme uno de Wireshark Samples.

https://wiki.wireshark.org/uploads/__/moin_import_/attachments/SampleCaptures/wpa-Induction.pcap

Análisis.



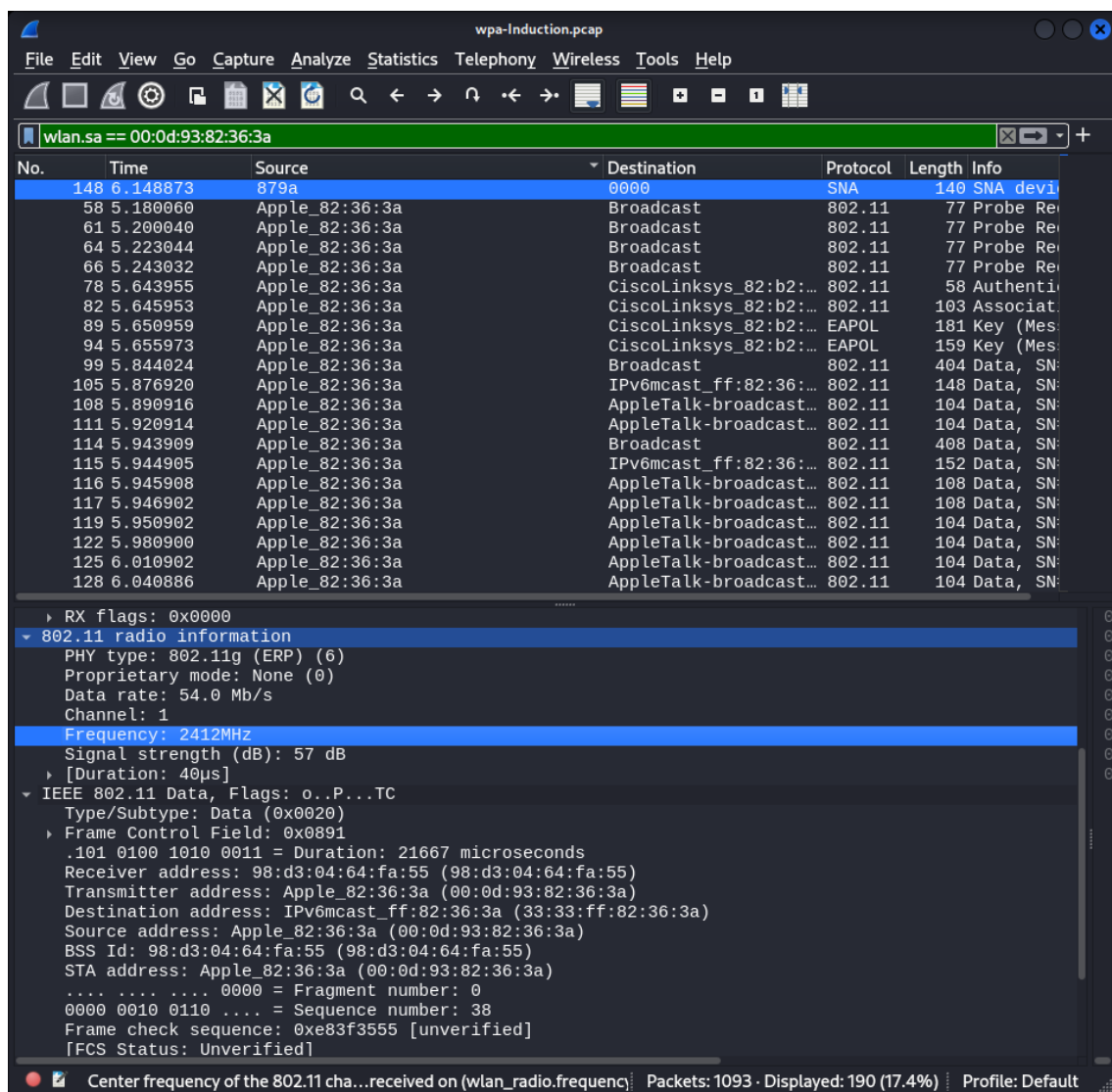
The image shows a Wireshark packet capture interface. The top bar indicates the capture source as 'wlan.sa == 00:0d:93:82:36:3a'. The packet list pane shows a series of packets from 131 to 174, all originating from 'Apple_82:36:3a' and destined for 'AppleTalk-broadcast...'. The packet details pane is expanded for packet 131, showing the following structure:

- Frame 131: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
- ▼ Radiotap Header v0, Length 24
 - Header revision: 0
 - Header pad: 0
 - Header length: 24
 - ▶ Present flags
 - Flags: 0x10
 - Data Rate: 1.0 Mb/s
 - Channel frequency: 2412 [BG 1]
 - ▶ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
 - Signal Quality: 96
 - Antenna: 0
 - dB antenna signal: 40 dB
 - ▶ RX flags: 0x0000
- ▼ 802.11 radio information
 - PHY type: 802.11b (HR/DSSS) (4)
 - Short preamble: False
 - Data rate: 1.0 Mb/s
 - Channel: 1
 - Frequency: 2412MHz
 - Signal strength (dB): 40 dB
 - ▶ [Duration: 864µs]
- ▼ IEEE 802.11 Data, Flags: .pm...F.C

Voy a seguir la traza de Apple_82:36:3a.

En la rama de Radiotap Header, puedo ver que la calidad de la señal es bastante alta por lo que intuyo que el dispositivo está bastante cerca del router o switch. Conectado con una frecuencia de 2.4 GHz a través del canal 1.

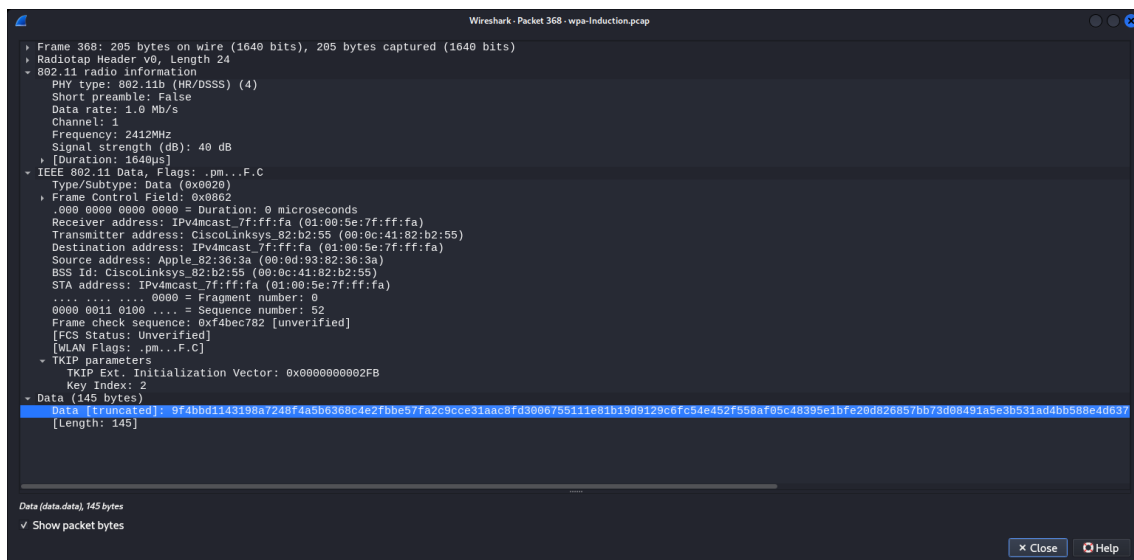
El router (CiscoLinksys_82:b2:55) le da una dirección IPv6 (00:0c:41:82:b2:55). También puedo observar que le proporciona distintos parámetros conforme se transmite la información en este caso TKIP con un Key Index 2. El protocolo usado es el 802.11b.



En esta segunda imagen analizaré el paquete 148 con nombre 879a.

Este paquete utiliza un tipo de circuito integrado 802.11g (ERP) por el canal 1 con una frecuencia de 2.4 GHz. Su señal no es tan alta como el anterior dispositivo.

El protocolo que utiliza es el SNA (Systems Network Architecture) diseñado por IBM en 1974 utilizada para la conectividad con hosts o mainframe de IBM (grandes ordenadores y servidores robustos que soportan millones de transacciones, generalmente usado en bancos. Estos la utilizan por considerarlo más seguro que el modelo TCP/IP. Es común que las redes de cajeros automáticos utilicen el protocolo SNA.



Esta imagen corresponde al stream del paquete 368.

Se basa en una transmisión del dispositivo Apple_82:36:3^a a IPv4mcast_7f:ff:fa.

Su circuito integrado es 802.11b (HR/DSSS), utiliza el canal 1 y una frecuencia de 2.4 GHz. En la rama de data podemos ver que está "truncada", con una longitud de 145.