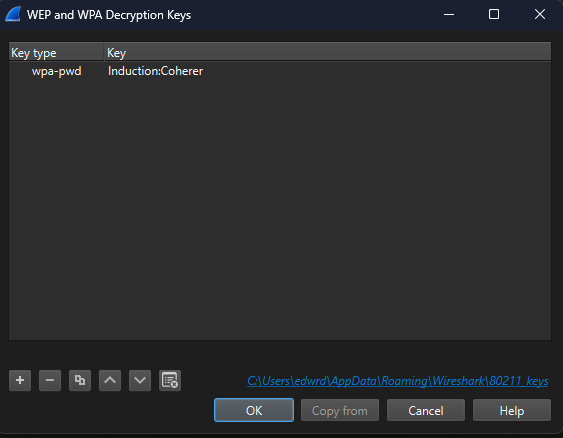
**Lab4**

1. Inspect capture and decrypt WPA encrypted traffic
2. Download and inspect the capture
3. Enter the WPA key and decrypt the traffic

Edit -> Preferences -> Protocols -> IEEE 802.11

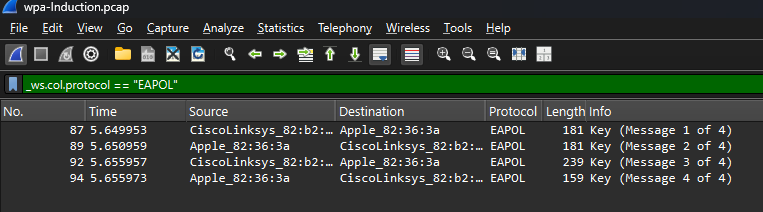
Edit Decrypytion Keys -> Enter “Induction:Coherer” of type wpa-pwd key

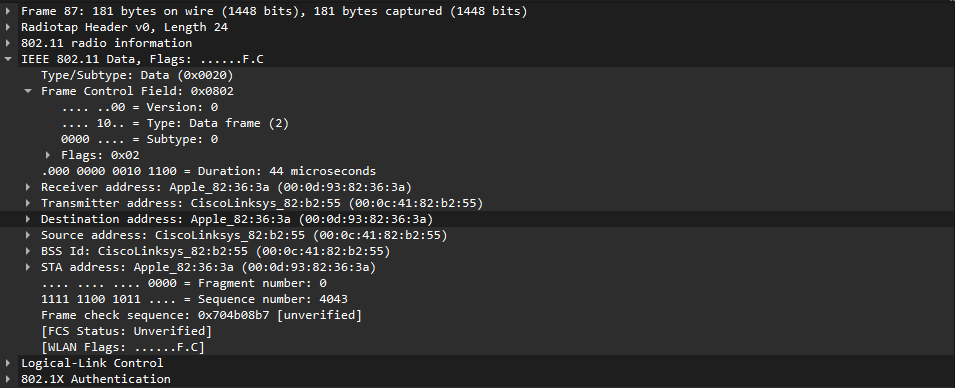


1. Identify a client and an Access Point (AP). Find the corresponding MAC addresses.

EAPOL stands for Extensible Authentication Protocol over LAN. It's used in WPA/WPA2 Wi-Fi authentication between the Access Point (AP) and the Client (STA). During WPA/WPA2 connection setup, EAPOL is the protocol used to exchange keys in what's called the **4-Way Handshake**.

Apply the filter EAPOL to the protocol column (\_ws.col.protocol == "EAPOL").



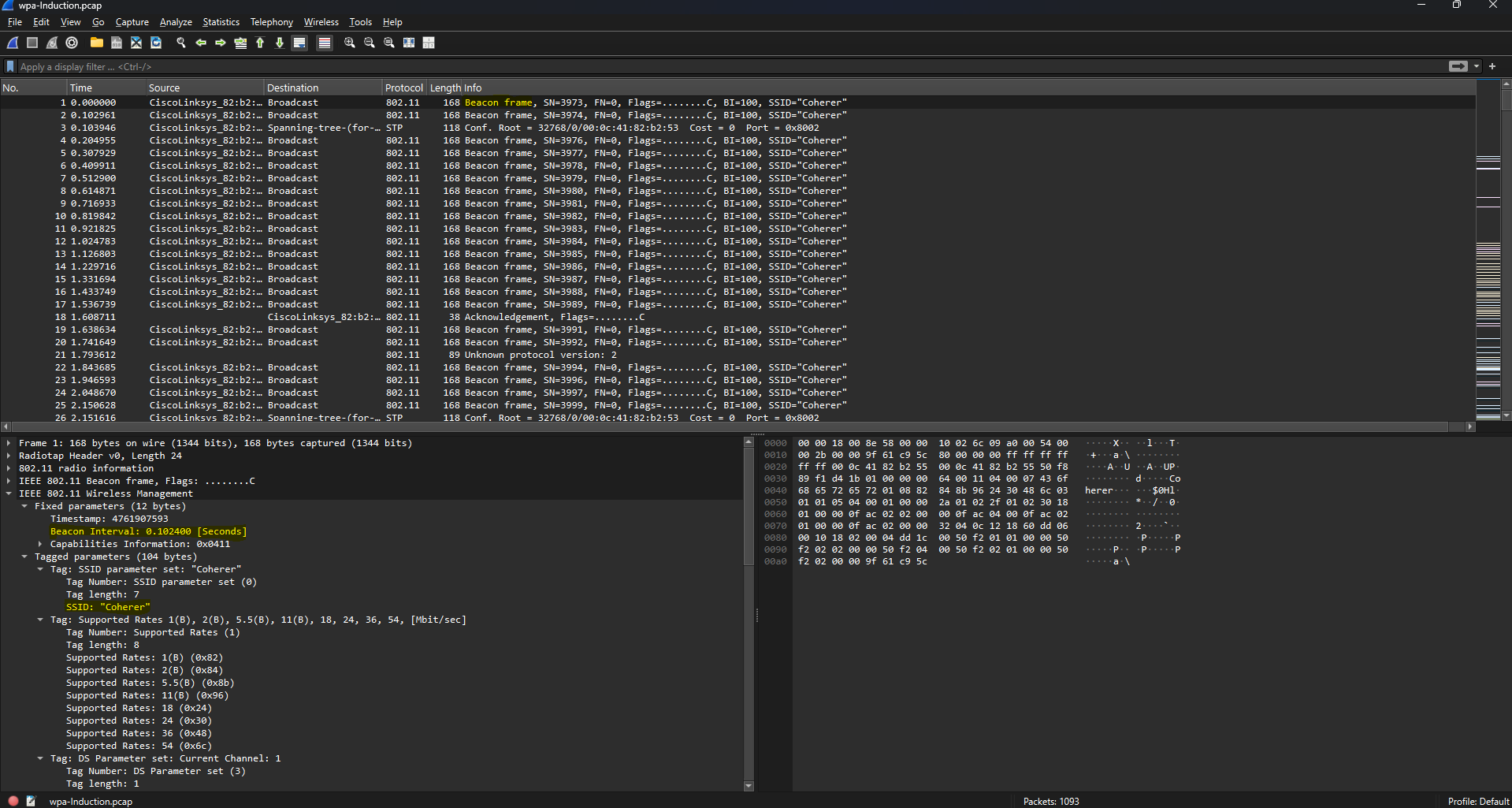


* Access Point (AP): 00:0c:41:82:b2:55 (Source address)
* Client: 00:0d:93:82:36:3a (Destination address)

1. Identify the broadcast messages sent by the AP. Which is the SSID? Which is the beacon interval?

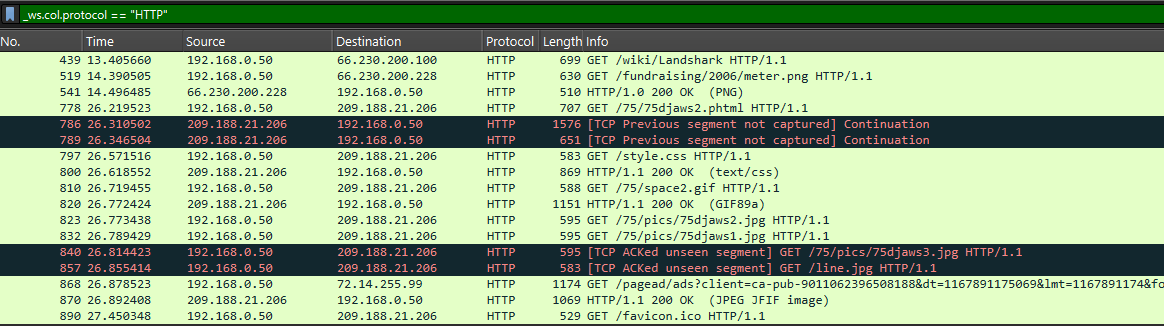
Click any beacon frame -> Expand IEEE 802.11 Wireless Management

* Beacon interval is found under Fixed parameters: 0.102400 (seconds)
* SSID is found under Tagged parameters: “Coherer”

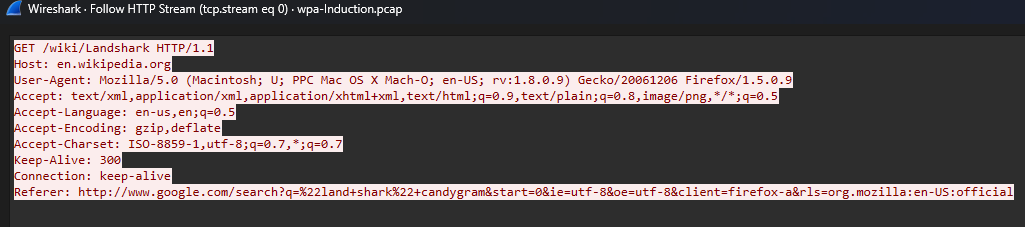


1. Search for HTTP traffic. Find and follow a TCP or HTTP stream. Name a website the client visits.

Apply the filter HTTP to the protocol column (\_ws.col.protocol == "HTTP").



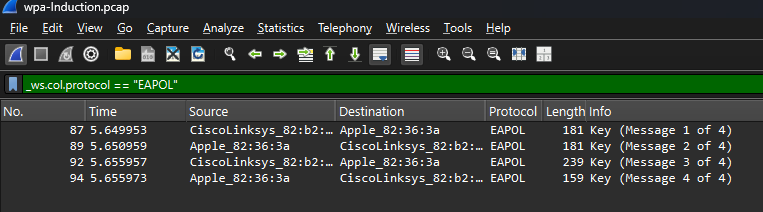
Right-click on a HTTP packet -> Follow -> HTTP Stream



* en.wikipedia.org

1. 4-Way Handshake
2. Identify the four frames of the EAPOL handshake.

Apply the filter EAPOL to the protocol column (\_ws.col.protocol == "EAPOL").



* AP → Client (ANonce sent)
* Client → AP (SNonce sent)
* AP → Client (GTK sent, MIC present)
* Client → AP (Acknowledgment)

1. Find the values of the two nonces further used in the key agreement.

**ANonce (Authenticator Nonce)** is sent by the **Access Point** in **Message 1** of the 4-Way Handshake and it is used to help derive encryption keys.

Click on the first EAPOL packet -> Expand 802.1x Authentication

* WPA Key Nonce: 3e8e967dacd960324cac5b6aa721235bf57b949771c867989f49d04ed47c6933

**SNonce (Supplicant Nonce)** is sent by the **Client (Supplicant)** in **Message 2** and it is combined with the ANonce and the password to derive the **Pairwise Transient Key (PTK)**.

Click on the second EAPOL packet -> Expand 802.1x Authentication

* WPA Key Nonce: cdf405ceb9d889ef3dec42609828fae546b7add7baecbb1a394eac5214b1d386

1. Find the value of the GTK.

**GTK (Group Temporal Key)** is a **key used to encrypt broadcast/multicast traffic** on the Wi-Fi network and it is sent by the AP to the client in **Message 3**, **encrypted** using the **KEK** (Key Encryption Key).

Click on the third EAPOL packet -> Expand 802.1x Authentication -> Expand WPA Key Data

* GTK: ee22041a83853263474c38811352282071c122359b7c35a7e7d034f3cd6ac565

1. Which of the four frames is integrity protected?

* All except the first one (Key MIC – Message Integrity Code != 0)

1. Which of the four frames contains encrypted data? Why?

* The third frame is encrypted using KEK because it includes GTK

1. Find the values of the two EAPOL keys Key Confirmation Key (KCK) and Key Encryption Key (KEK). What are these used for?

**KCK (Key Confirmation Key)**

* Integrity protection.
* Generate and verify the **Message Integrity Code (MIC)** on EAPOL-Key frames.
* Ensures messages haven’t been tampered with.
* [KCK: b1cd792716762903f723424cd7d16511]

**KEK (Key Encryption Key)**

* Encryption of key material.
* Encrypt the **GTK** (Group Temporal Key) and other sensitive key data in Message 3.
* Ensures confidentiality of keys during transmission.
* [KEK: 82a644133bfa4e0b75d96d2308358433]