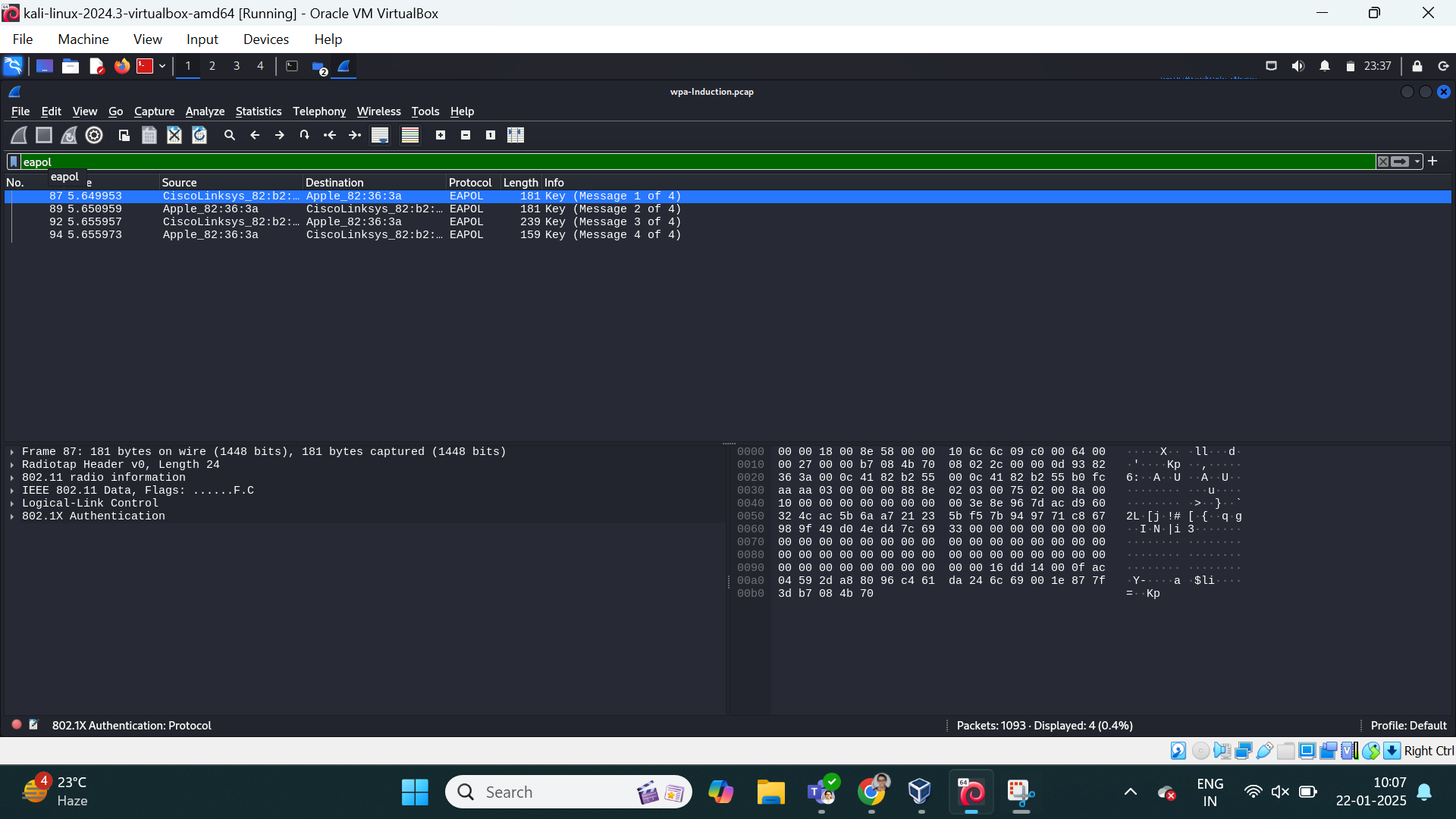
## \*\*Lab Exercises\*\*

### \*\*Exercise 1: Analyzing Wireless Traffic Using Wireshark\*\*

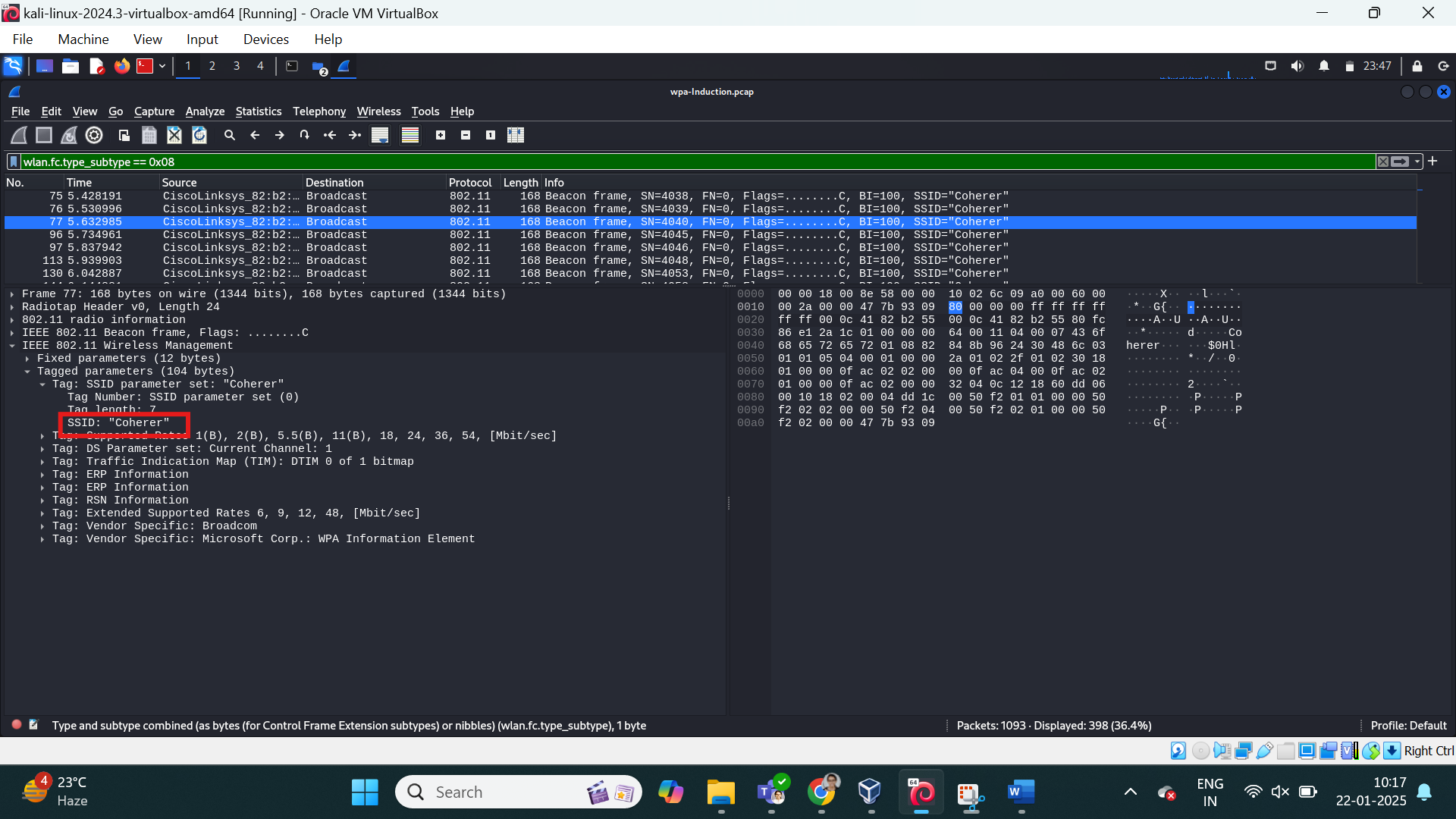
#### \*\*Objective\*\*:  
Learn how to open and analyze pre-captured wireless network traffic.

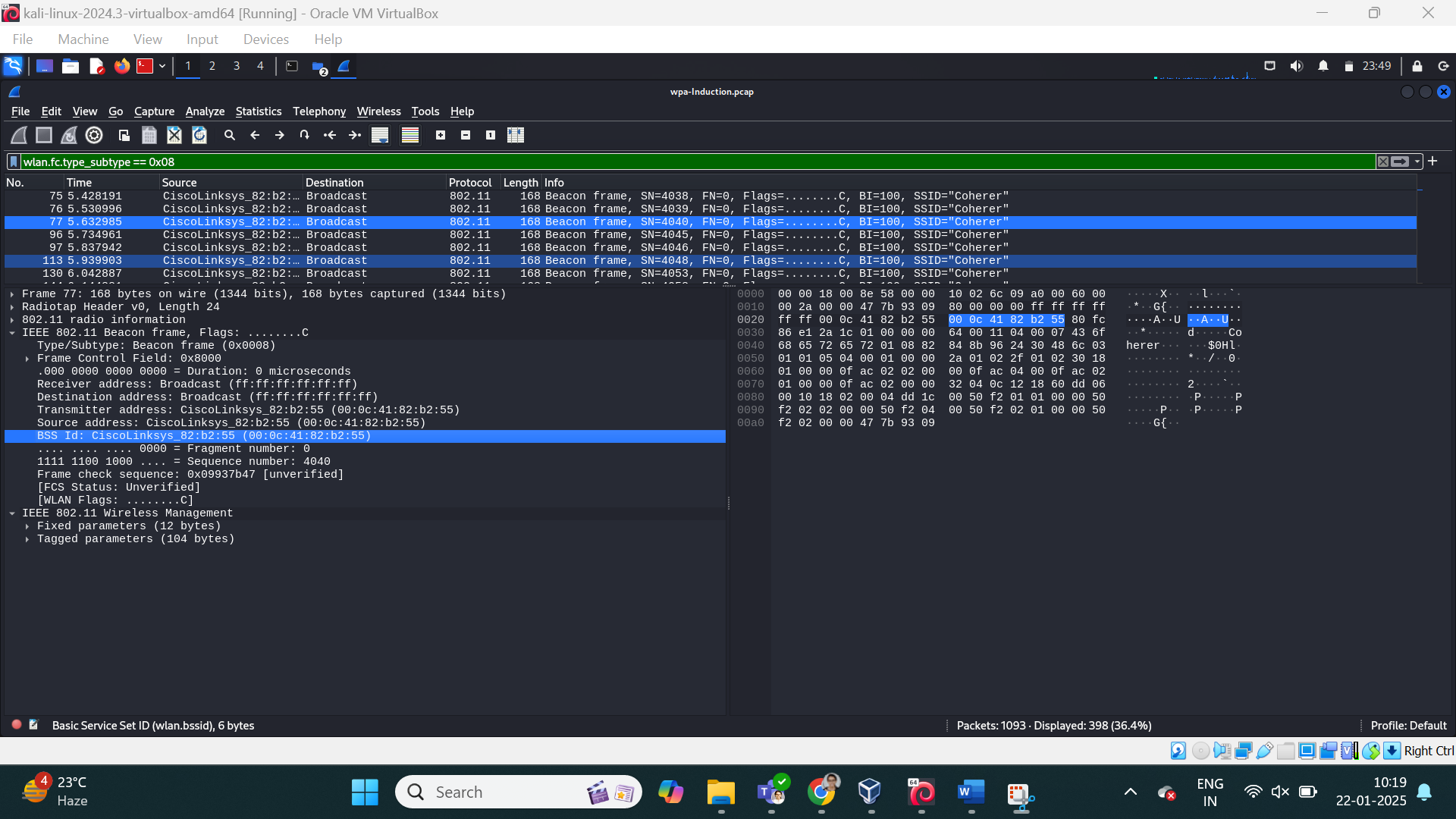
#### \*\*Steps\*\*:  
1. \*\*Open Wireshark\*\*:  
   - Launch Wireshark on your computer.  
   - Load a pre-captured file (e.g., WPA handshake):  
     - Go to `File` > `Open` > Select the `.pcap` file.

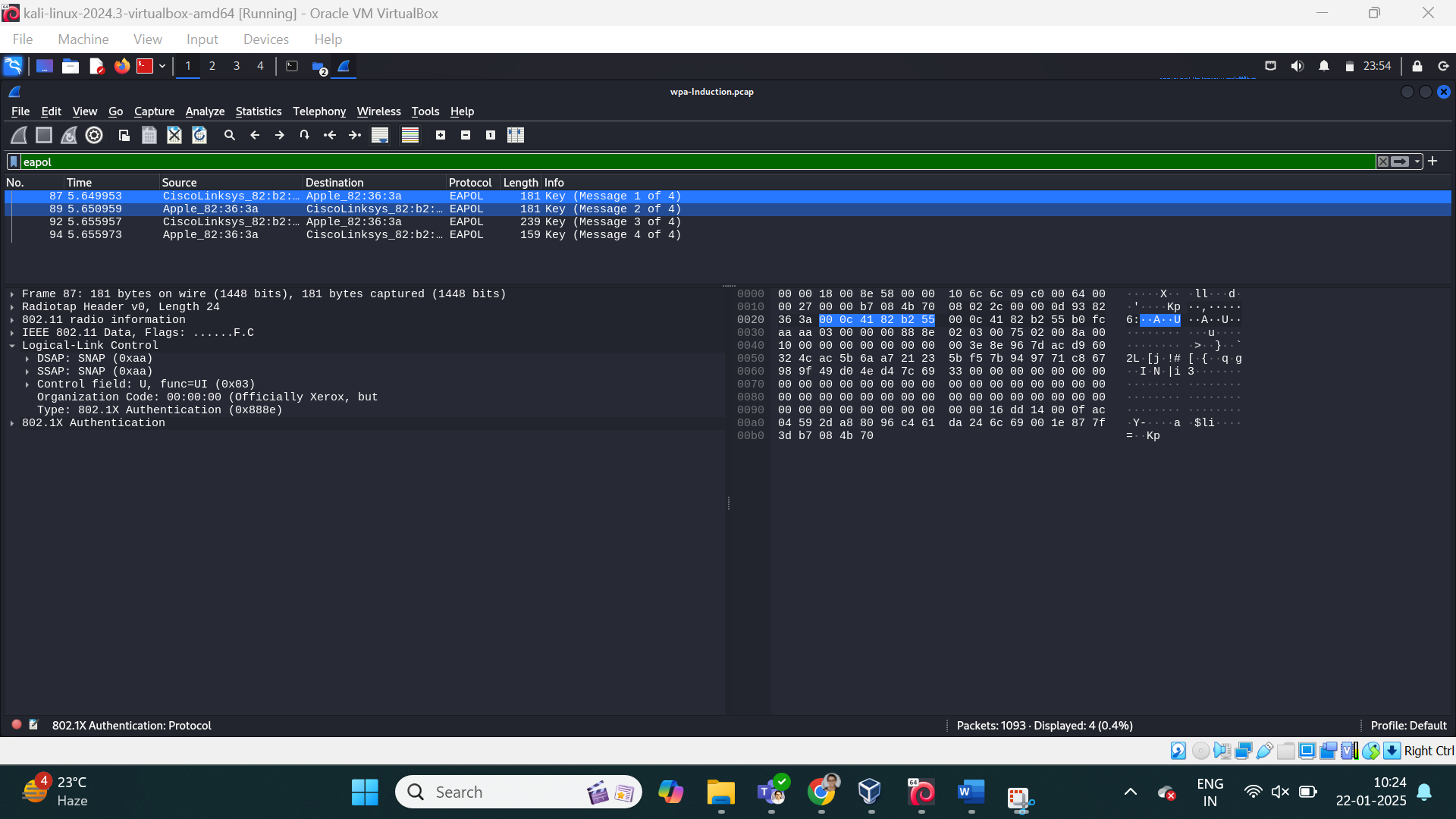
2. \*\*Filter Wireless Traffic\*\*:  
   - Use filters to isolate wireless packets:  
     - For WPA handshake: `eapol`.



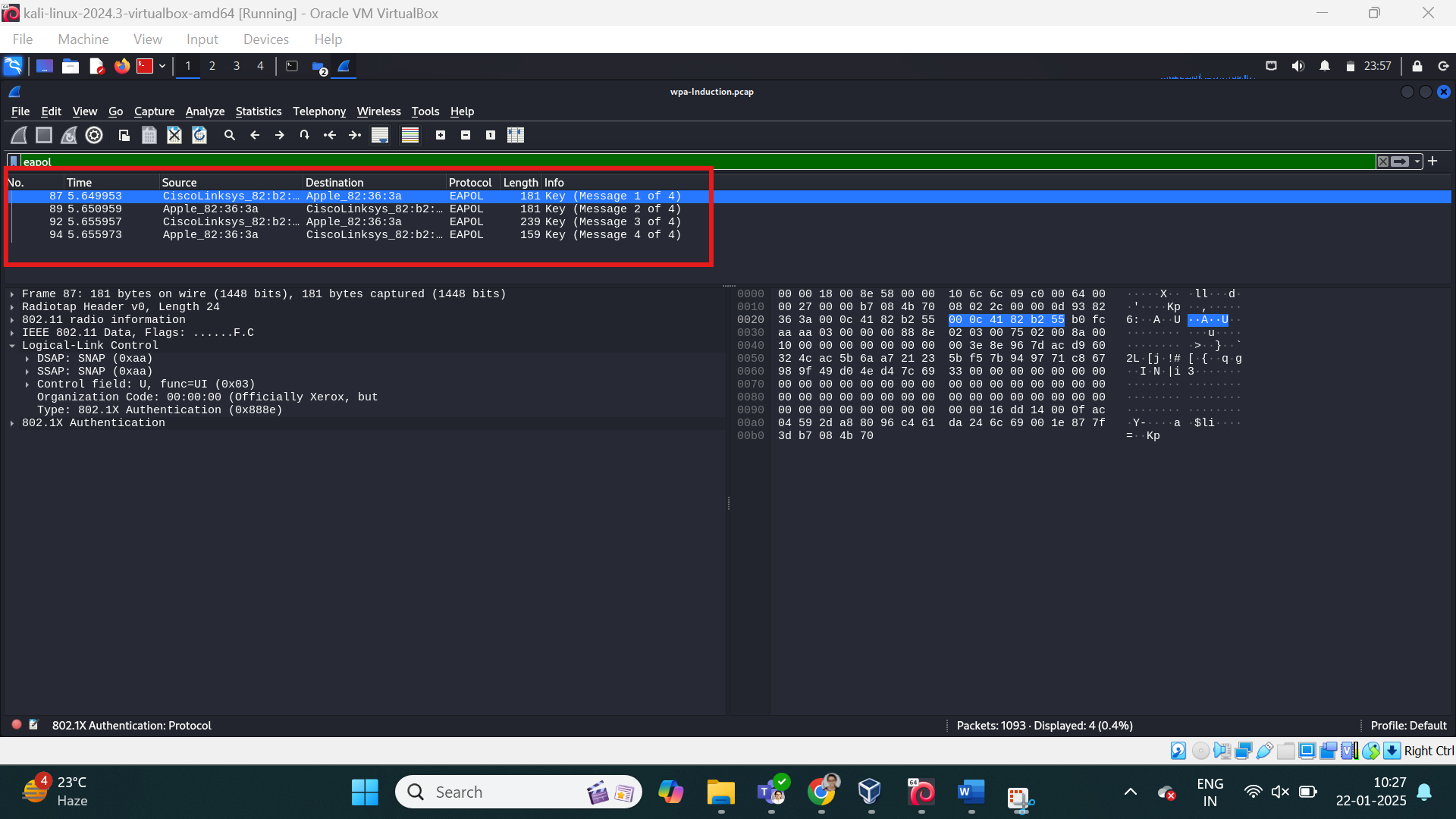
3. \*\*Analyze Packets\*\*:  
   - Identify the following components in the capture:  
     - \*\*SSID\*\*: The network name.

  
     - \*\*BSSID\*\*: The MAC address of the access point.

  
     - \*\*Handshake Packets\*\*: Look for EAPOL packets.



4. \*\*Document Observations\*\*:  
   - Note the time, source, destination, and protocol of key packets.



---

### \*\*Exercise 2: Cracking WEP Encryption Using Pre-Captured Files\*\*

#### \*\*Objective\*\*:  
Simulate cracking a WEP-encrypted network using Aircrack-ng.

#### \*\*Steps\*\*:  
1. \*\*Download a WEP Capture File\*\*:  
   - Obtain a `.cap` file containing WEP packets (e.g., from GitHub).

**Found .cap file from**: <https://www.aircrack-ng.org/downloads.html?utm_source=chatgpt.com>

2. \*\*Analyze the Capture\*\*:  
   - Open the file in Wireshark to ensure it contains WEP-encrypted traffic.

**This filters encrypted wireless traffic**

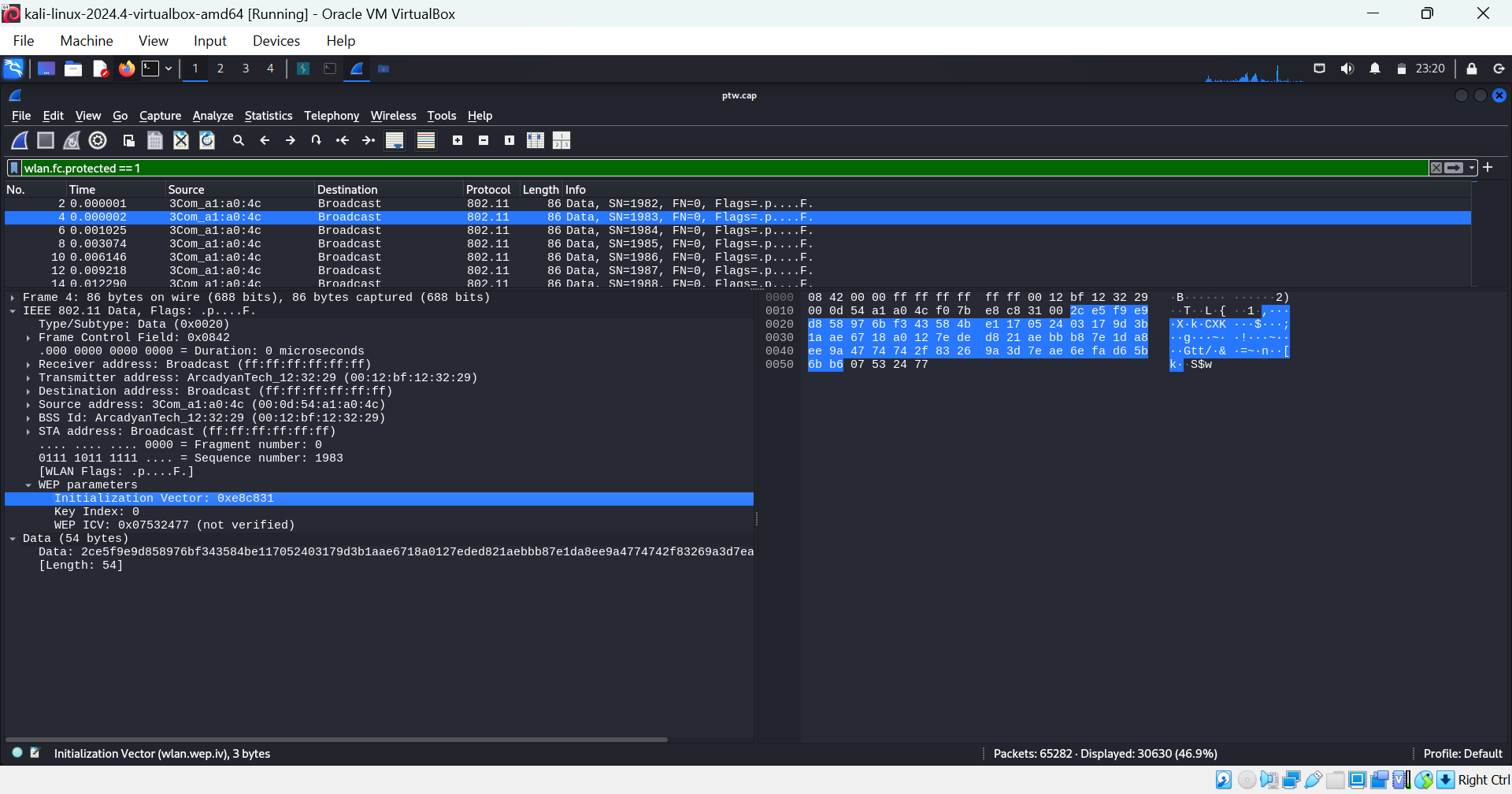
wlan.fc.protected == 1

 **Check Encryption Type**:

* Look at the **Protocol** column for 802.11 frames.
* Click on a captured packet and expand the **IEEE 802.11** section.
* Look for **"WEP"** under **"Security"** or **"Protected Data"**.
* If present, the traffic is WEP-encrypted.

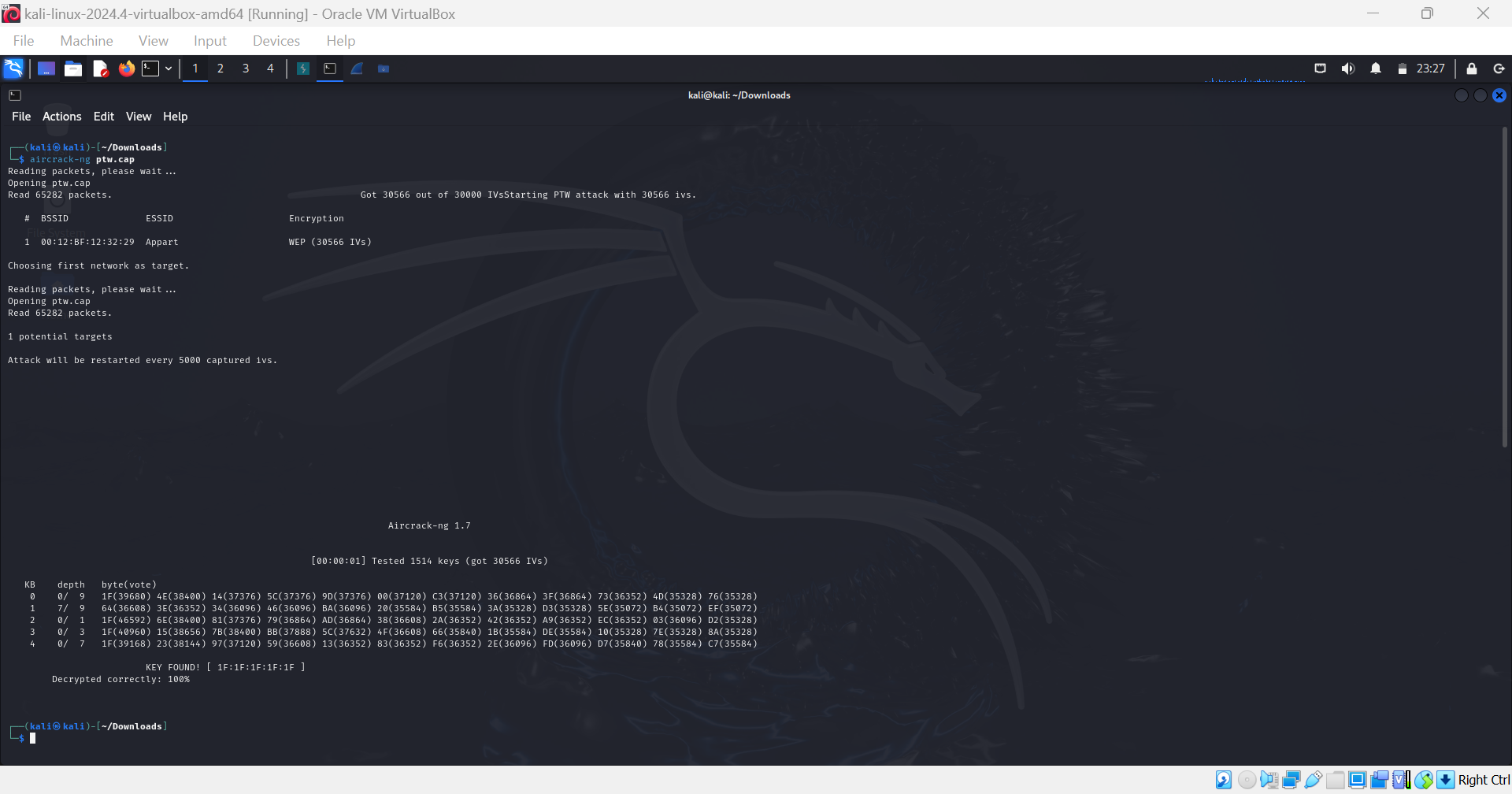
 **Verify IVs (Initialization Vectors)**:

* Look for a field named **IV** (Initialization Vector) in WEP-encrypted packets.
* WEP uses IVs for encryption, and repeated IVs indicate vulnerability.



3. \*\*Use Aircrack-ng\*\*:  
   - Launch Kali Linux.  
   - Run Aircrack-ng on the capture file:  
     ```bash  
     aircrack-ng -b [BSSID] -w /usr/share/wordlists/rockyou.txt wep\_capture.cap  
     ```

4. \*\*Crack the Key\*\*:  
   - If successful, Aircrack-ng will display the WEP key in plaintext.



**Result:** KEY FOUND! [ 1F:1F:1F:1F:1F ]

#### \*\*Expected Outcome\*\*:  
Understand how WEP encryption is vulnerable and why it is deprecated.

---

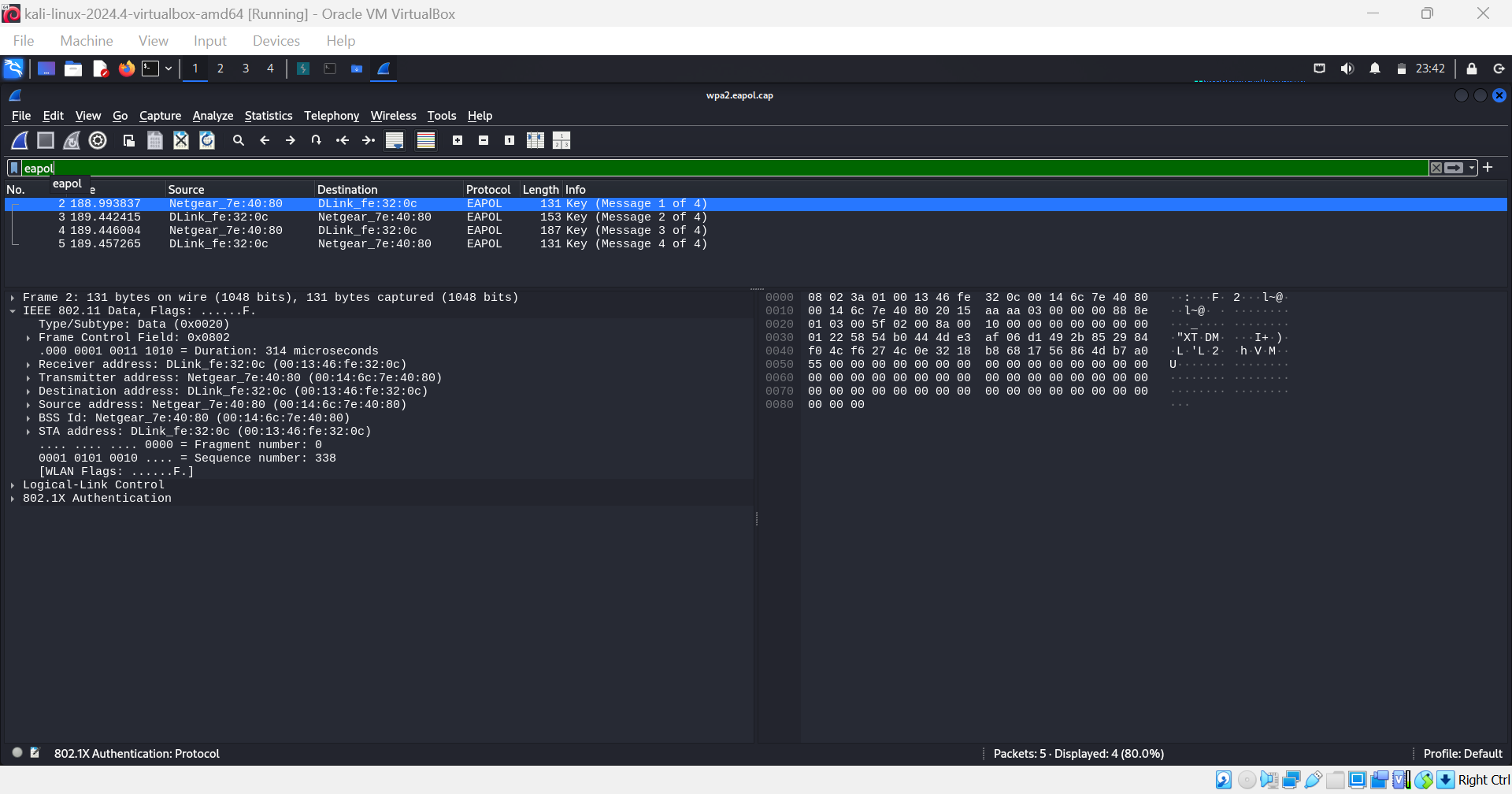
### \*\*Exercise 3: Cracking WPA/WPA2 Encryption Using a Pre-Captured Handshake\*\*

#### \*\*Objective\*\*:  
Simulate cracking a WPA/WPA2-encrypted network using a captured handshake and dictionary attack.

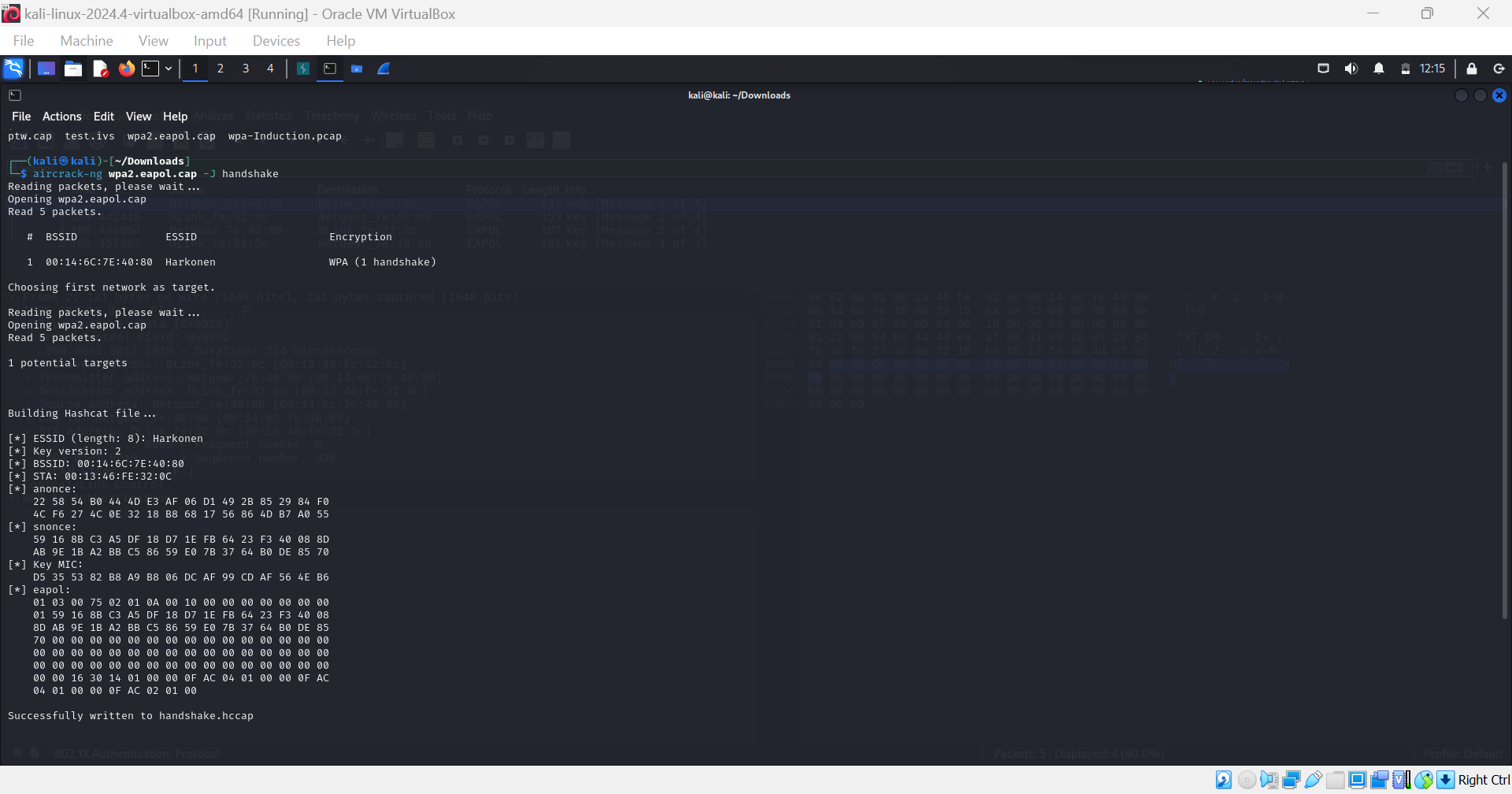
#### \*\*Steps\*\*:  
1. \*\*Download a WPA Handshake File\*\*:  
   - Obtain a `.cap` file with a valid handshake (e.g., from GitHub).  
**Obtained .cap file from**: <https://github.com/aircrack-ng/aircrack-ng/tree/master/test>

2. \*\*Verify the Handshake\*\*:  
   - Open the file in Wireshark.  
   - Use the filter `eapol` to ensure handshake packets are present.

If **4 EAPOL packets** are present, the handshake is complete and ready for cracking.



3. \*\*Convert the Capture File\*\*:  
   - Use `aircrack-ng` to convert the `.cap` file to `.hccapx` format for Hashcat (optional):  
     ```bash  
     aircrack-ng handshake.cap -J handshake  
     ```



4. \*\*Run Aircrack-ng\*\*:  
   - Attempt to crack the handshake using a dictionary file:  
     ```bash  
     aircrack-ng -w /usr/share/wordlists/rockyou.txt handshake.cap  
     ```

