## **Activity File: Analyzing Wireless Attacks**

In this activity, you will continue to play the role of a security analyst at Acme Corp.

* There is concern about one of the wireless routers detected in the Kansas City office, as it was found to have weak encryption.
* You are concerned that a hacker could decrypt the traffic from this wireless router.
* Your task is to see if you can obtain the wireless secret key and decrypt the wireless traffic to determine any associated security risks.
* <https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/UCI-VIRT-CYBER-PT-03-2022-U-LOL/-/tree/main/09-Networking-Fundamentals-II-and-CTF-Review/1/Activities/14_Wireless_Attacks/unsolved>

### **Instructions**

1. Open the kansascityWEP.pcap file in wireshark.
2. Use Aircrack-ng on the packet capture to determine the secret key
   1. Aircrack-ng kansascityWEP.pcap.
   2. Key found : 1F:1F:1F:1F:1F
3. Use the key to decrypt the traffic.
   1. Click view => wireless toolbar  
      => 802.11 preferences => Enable Decryption => Edit => “+” icon => select WEP and input key => select ok
4. Analyze the decrypted traffic and determine the associated security risks.
   1. ARP and IGMP protocols are decrypted
   2. Hackers can use ARP to determine private IP addresses