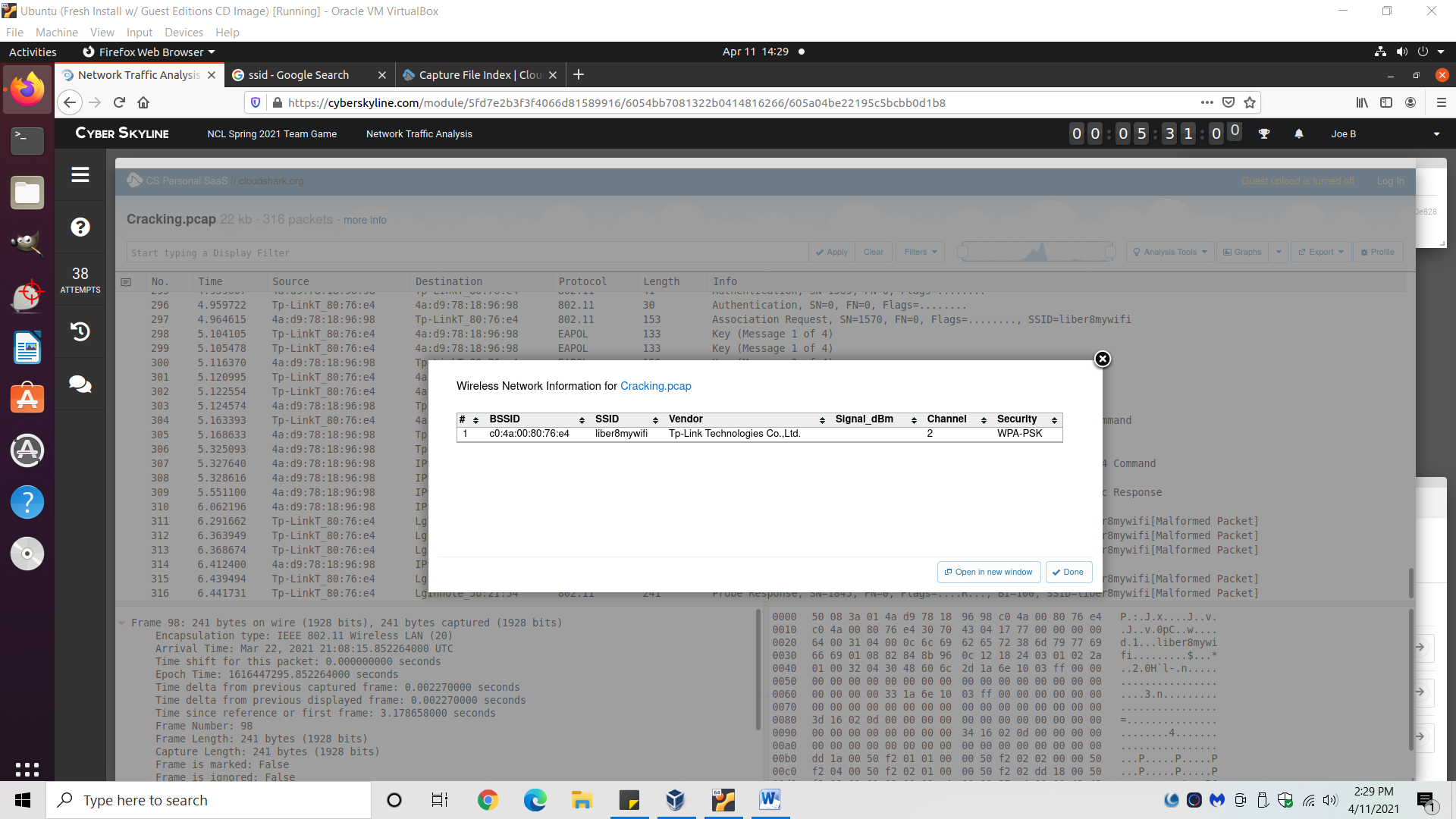
**Cracking (Medium)**

**A wireless network was hacked. See if you can figure out what happened.**

**What channel was the victim network operating on?**

1. Go to “Analysis Tools” on the top right-hand side and click on “Wireless Networks.”



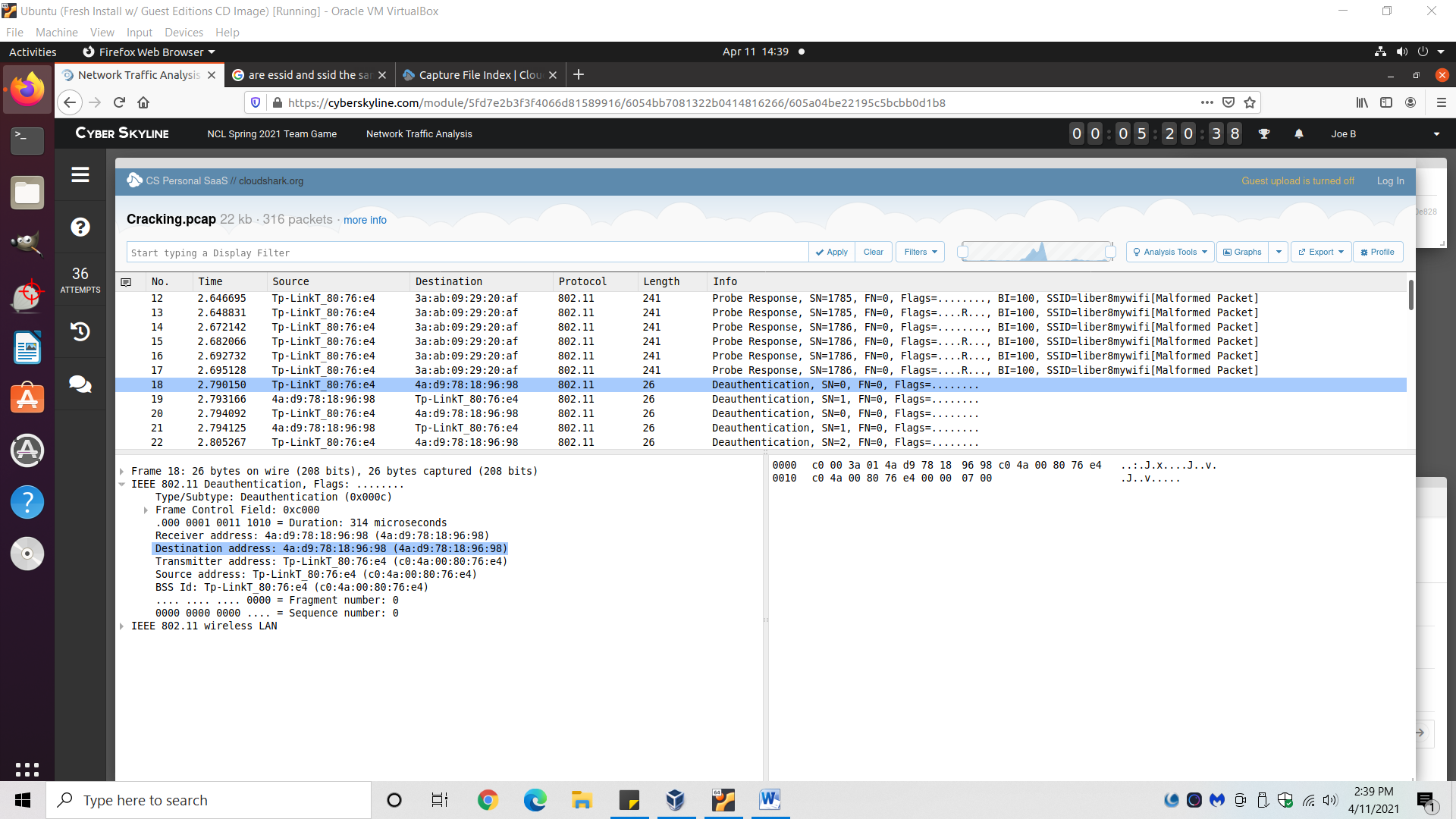
1. Observe that there’s a single Wi-Fi channel, on channel 2.
2. Answer: 2

**What is the ESSID of the wifi network that was hacked?**

1. Same steps as above.
2. SSID is the service set identifier or network name for the basic service set(BSS). ESSID is the same as the SSID but is used across multiple access points as part of the same WLAN. ... BSSID is the MAC address of the AP's radio for that service set.
3. Answer: liber8mywifi

**What is the MAC address of the victim that was deauthenticated?**

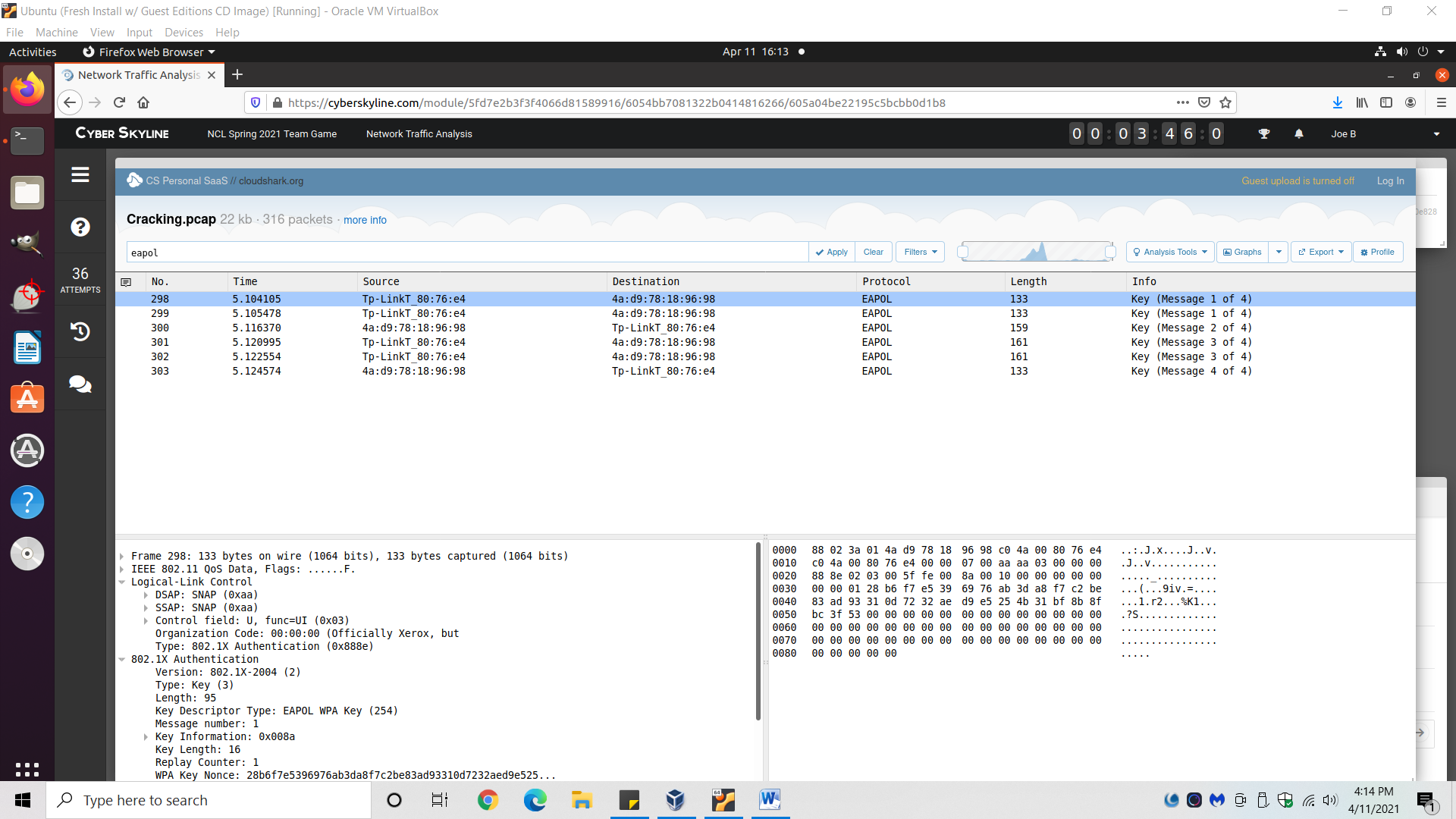
1. Scroll through packets until you see the first packet that has “deauthenitaction” in the info section.
2. Expand “I.EEE 802.11 Deauthentication…”



1. There’s a MAC address in the “Destination Address” info.
2. Answer: 4A:D9:78:18:96:98

**What is the wireless password?**

1. Reference video on password cracking below. This is only one video in a 3 part series by “thenewboston” on YouTube. Look up videos 7-9 in the series for a complete understanding: <https://www.youtube.com/watch?v=En6XRMqg3aA&list=PL6gx4Cwl9DGC04FAovs0lswXTPXeomORn&index=9>
2. The attacker used a deauthentication attack to boot a user off the Wi-Fi, forcing them to log on again. Form here, the attacker can capture the 4-way handshake used by the WPA-2 security, and then crack the Wi-Fi passcode from the info contained within the captures.
   1. Wikipedia article on deauthentication attacks: <https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack>
3. Filter the frames by “eapol” which is the protocol that WPA-2 uses to conduct the 4-way handshake.



1. Download the eapol frames as a .pcap file.
2. Open terminal and type in *aircrack-ng Cracking.pcap -w rockyou.txt*
   1. Note: You have to type in the file paths for both files within the command; it just so happened I had both files in my *pwd*.
   2. Download aircrack-ng via the terminal with *sudo apt-get install aircrack-ng*.
   3. Download the “rockyou.txt” online.
3. Answer: \*My computer is too slow and doesn’t have enough resources to password crack (hahaha!). Try it yourself!
   1. Check different pages on aircrack-ng’s website to learn tips to speed-up and minimize resources for password cracking: https://www.aircrack-ng.org/doku.php?id=aircrack-ng