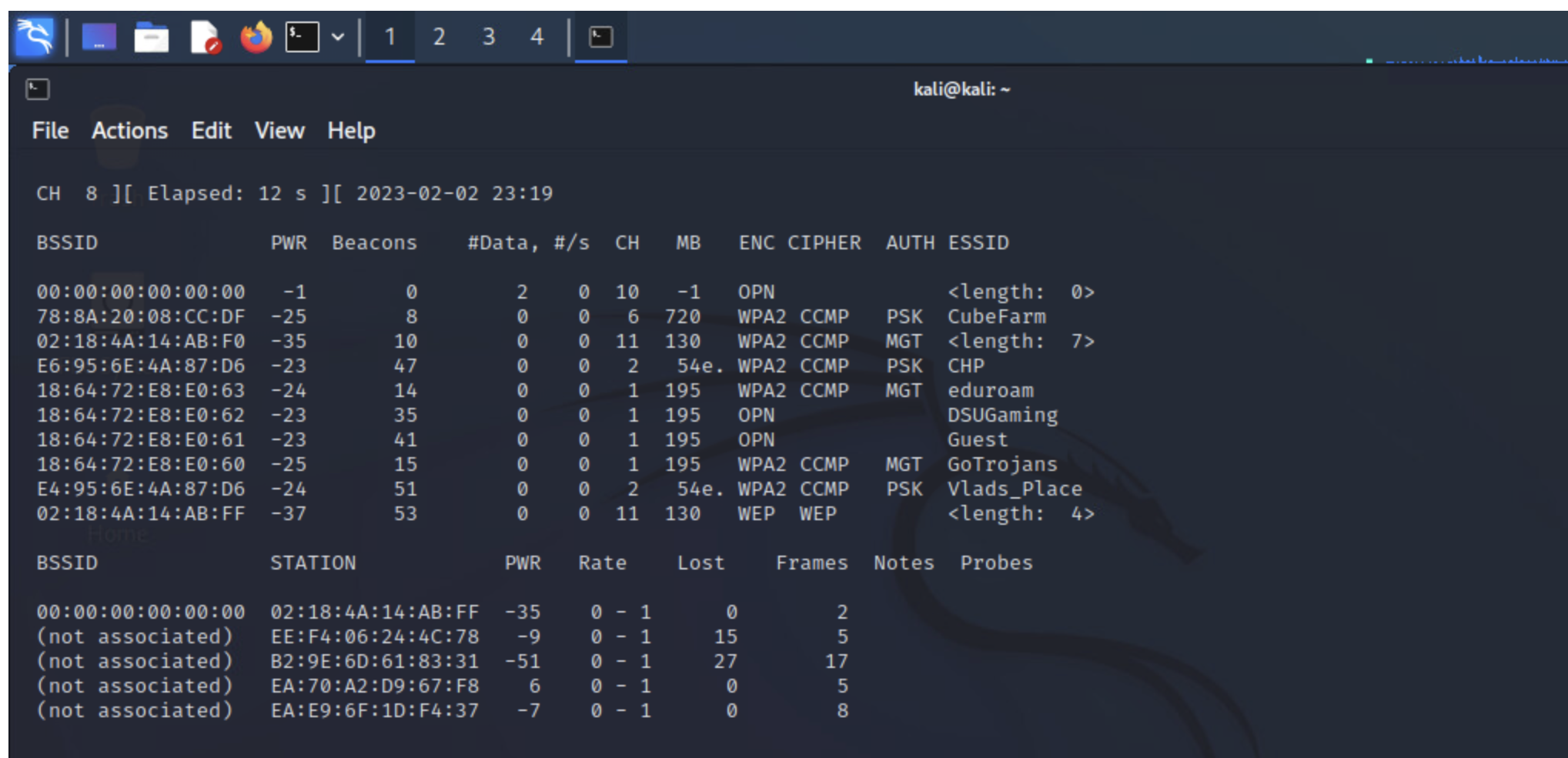
Lab 03 - Beacon Scavenger Hunt



## Locate a beacon that’s hiding its SSID. What is the SSID length?

BSSID -- 00:00:00:00:00:00

Channel -- 10

Length -- 0

BSSID -- 02:18:4A:14:AB:F0

Channel -- 11

Length -- 7

BSSID -- 02:18:4A:14:AB:FF

Channel -- 11

Length -- 4

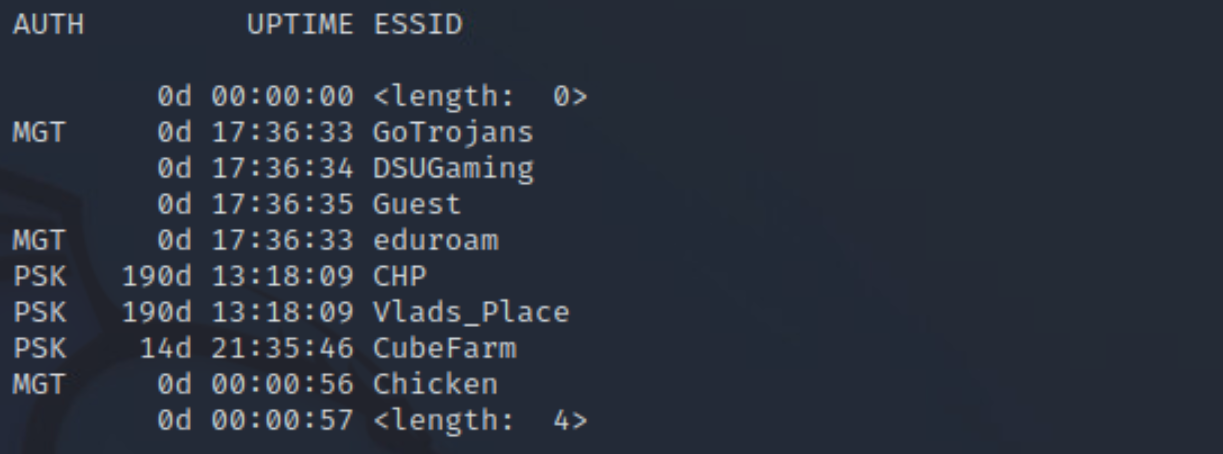
## Locate two beacons that are operating on a channel other than 1, 6 or 11

CHP ch2

Vlads\_Place ch2

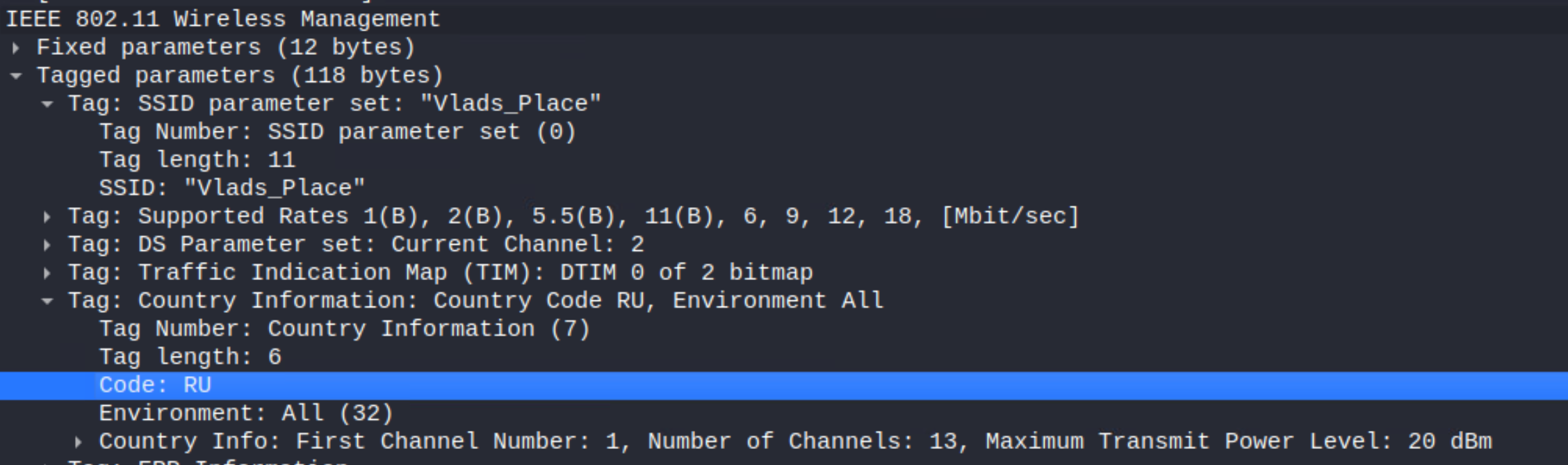
<Hidden> ch10 length0

## The timestamps for the official DSU networks are all very consistent, find a non-DSU beacon containing a timestamp that is significantly different



All of the DSU APs use MGT auth and the CubeFarm ESSID has an uptime of +04:00:00 compared to the other DSU APs.

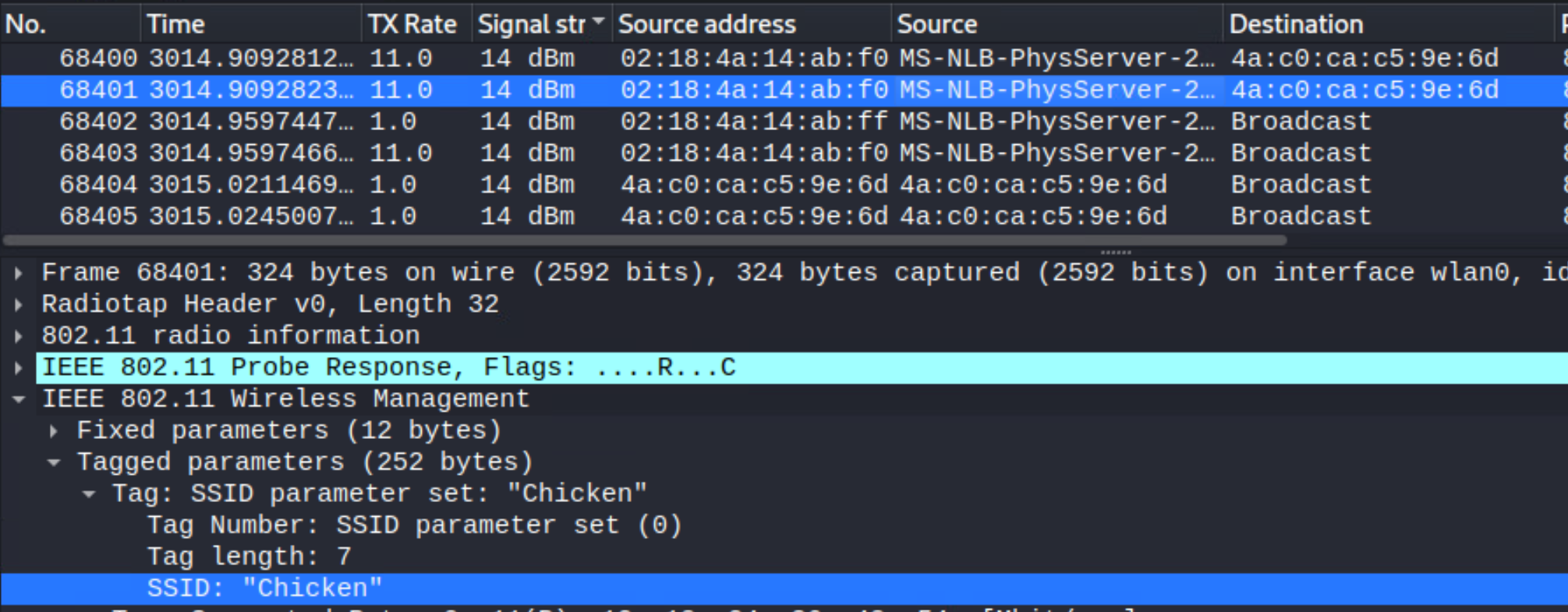
## Many AP’s do not beacon any regulatory domain information, but one does. Can you find it?



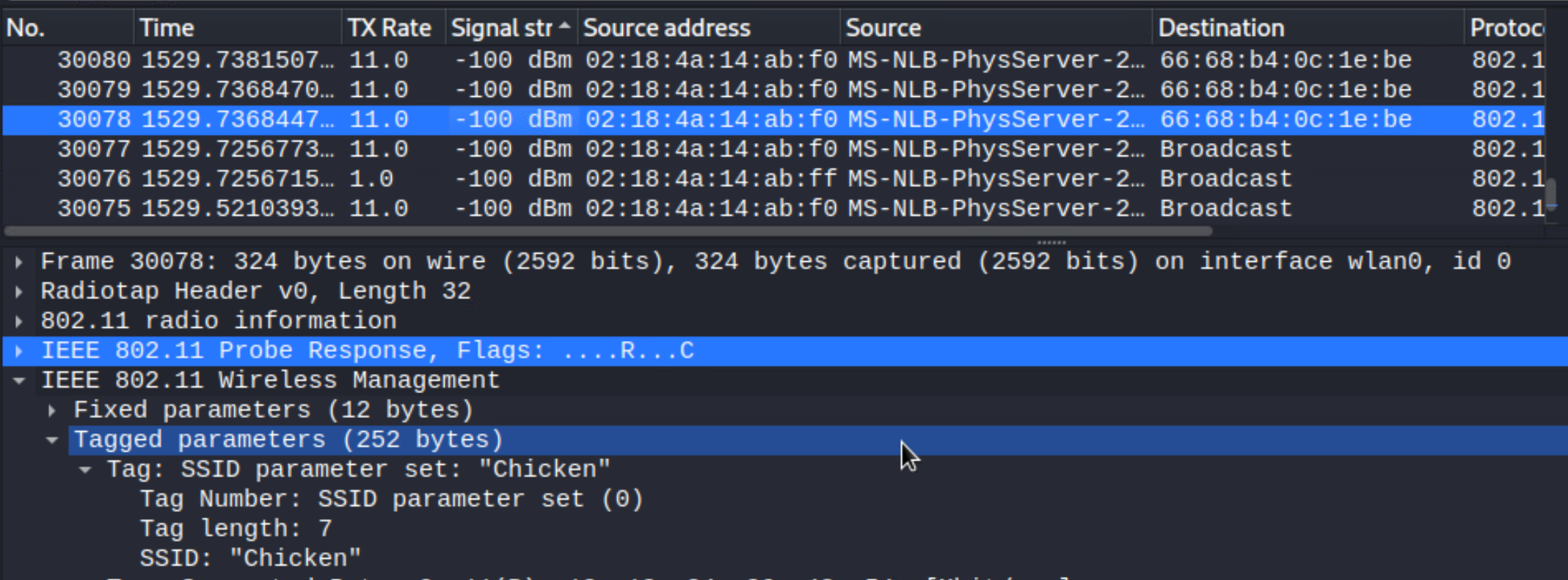
Vlads\_Place advertises country information code “RU”

## Create two screenshots, one with the best, one with the worst signal strength you can find ---- (Going off of Signal Strength in dBm and not TX rate)

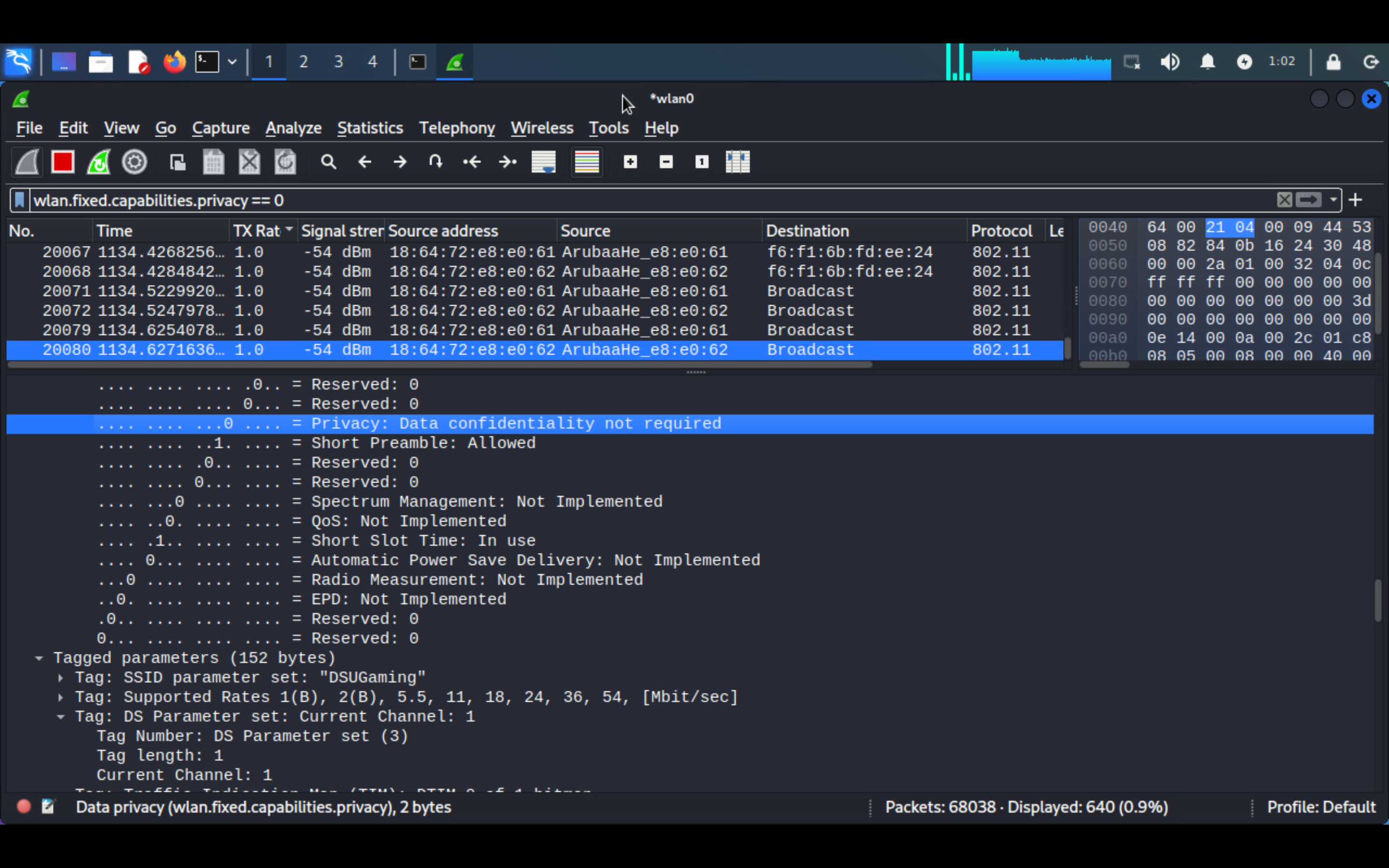
Most – Chicken w/ 14dBm



Least – Chicken w/ -100dBm

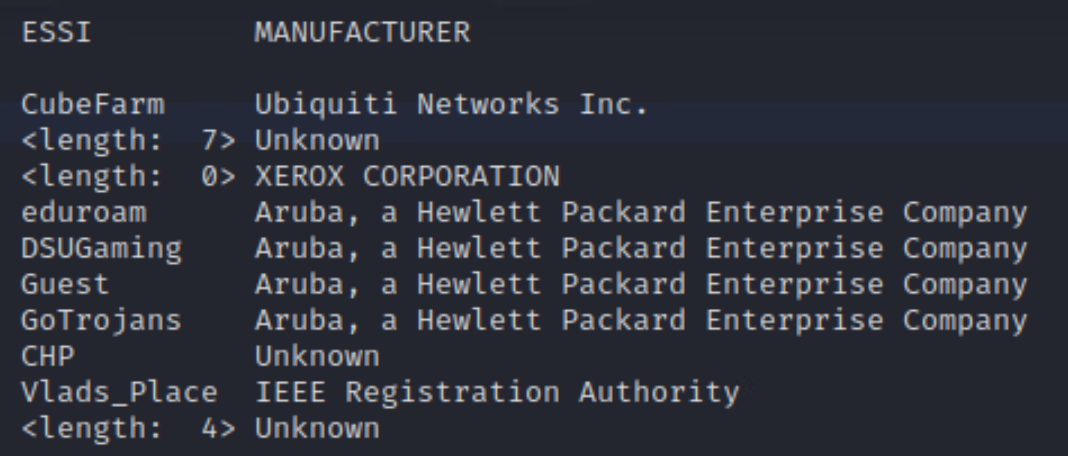


## Find a network that does not have the Privacy flag set

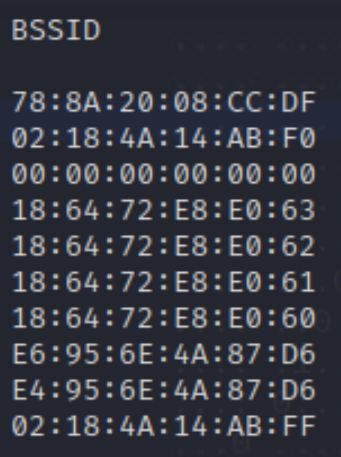


DSUGaming

## Display a list of all of the unique ESSID’s you can detect in a given area



## Display a list of all of the unique BSSID’s you can detect in a given area



## Many beacons contain “vendor specific” information, you can see this in Wireshark if you look at a beacon frame. What is this for?

It identifies the manufacturer of the network adapter used and helps determine vendor specific capabilities/elements.

## Researchy question! 802.11ax, marketed to the muggles as WiFi 6, is pretty neat. It’s introduced a lot of new features, they’re really only useful in dense environments. Advice: don’t bother upgrading to AX in order to improve your home’s wifi performance. To that end, one of the neat features that are introduced is the notion of “spatial reuse”. We achieve this through coloring (basic service set coloring or more broadly as a network color code). No crayons needed. What is this?

Basic service set coloring (BSSC) is a technique for marking shared frequencies within 802.11ax access points that allows a network to determine how much of a spectrum can be overlayed or reused. Knowing this method reduces interference due to congestion and ensures a quality connection despite highly dense user environments.

Possible applications for this technology being stadiums, hotels, or high-density housing (e.g., college dorms) where many unique access points might be deployed to enable greater access control per user(s) where spectrum might be limited and heavily overlapped.