# ATTACK DEFENSE

by PentesterAcademy

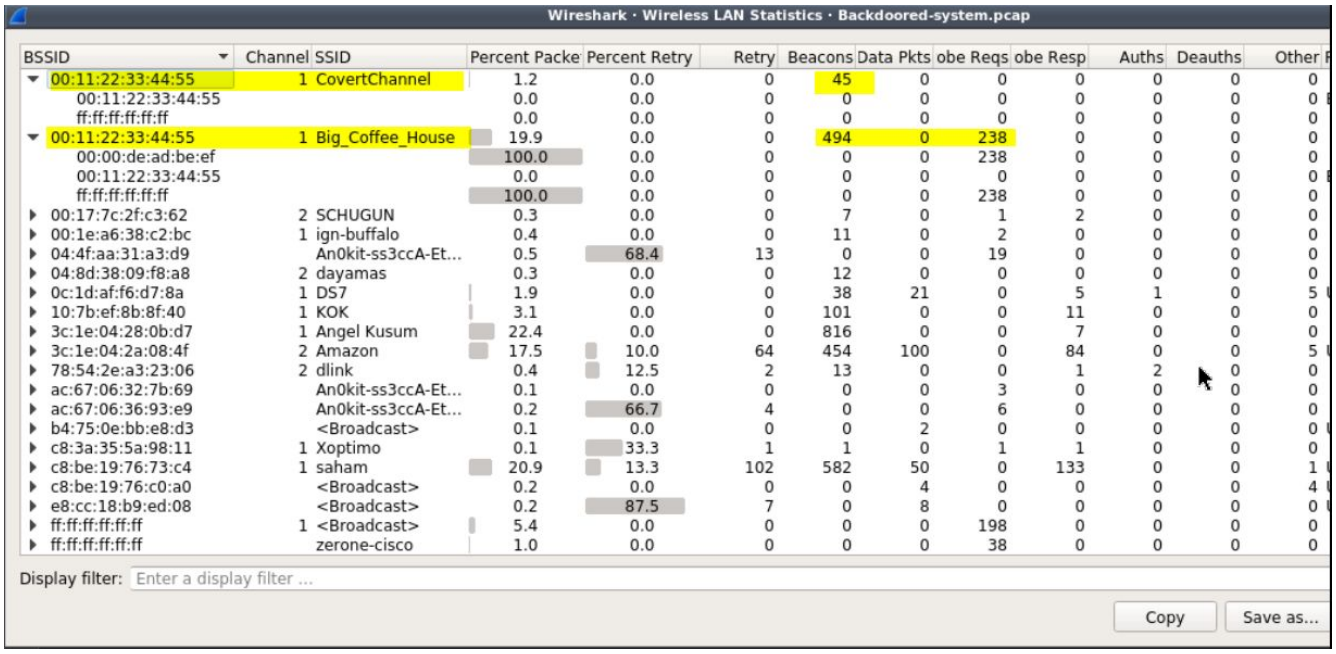
| Name | Backdoored System |
|---|---|
| URL | https://www.attackdefense.com/challengedetails?cid=65 |
| Type | Forensics : WiFi |

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

**Question 1:** How is information is getting leaked out?

**Solution:**

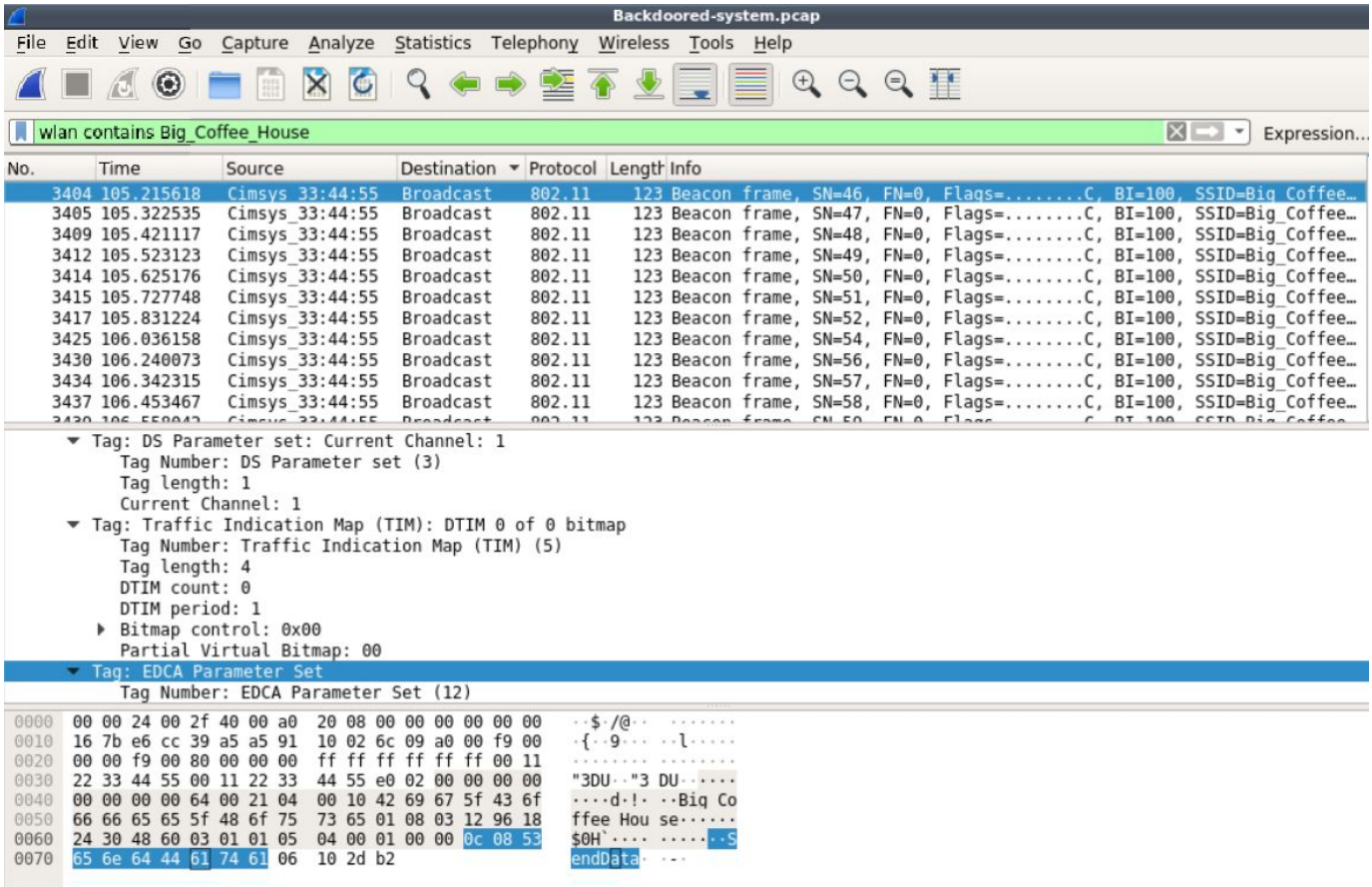
The best way to start WiFi Forensics with Wireshark is to start with macro view. Check WLAN summary using Wireless > WLAN Traffic.




| BSSID | Channel | SSID | Percent Packe | Percent Retry | Retry | Beacons | Data Pkts | obe Reqs | obe Resp | Auths | Deauths | Other F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00:11:22:33:44:55 | 1 | CovertChannel | 1.2 | 0.0 | 0 | 45 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00:11:22:33:44:55 | | | 0.0 | 0.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ff:ff:ff:ff:ff:ff | | | 0.0 | 0.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 00:11:22:33:44:55 | 1 | Big_Coffee_House | 19.9 | 0.0 | 0 | 494 | 0 | 238 | 0 | 0 | 0 | 0 |
| 00:00:de:ad:be:ef | | | 100.0 | 0.0 | 0 | 0 | 0 | 238 | 0 | 0 | 0 | 0 |
| 00:11:22:33:44:55 | | | 0.0 | 0.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ff:ff:ff:ff:ff:ff | | | 100.0 | 0.0 | 0 | 0 | 0 | 238 | 0 | 0 | 0 | 0 |
| 00:17:7c:2f:c3:62 | 2 | SCHUGUN | 0.3 | 0.0 | 0 | 7 | 0 | 1 | 2 | 0 | 0 | 0 |
| 00:1e:a6:38:c2:bc | 1 | ign-buffalo | 0.4 | 0.0 | 0 | 11 | 0 | 2 | 0 | 0 | 0 | 0 |
| 04:4f:aa:31:a3:d9 | | An0kit-ss3ccA-Et... | 0.5 | 68.4 | 13 | 0 | 0 | 19 | 0 | 0 | 0 | 0 |
| 04:8d:38:09:f8:a8 | 2 | dayamas | 0.3 | 0.0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0c:1d:af:f6:d7:8a | 1 | DS7 | 1.9 | 0.0 | 0 | 38 | 21 | 0 | 5 | 1 | 0 | 5 |
| 10:7b:ef:8b:8f:40 | 1 | KOK | 3.1 | 0.0 | 0 | 101 | 0 | 0 | 11 | 0 | 0 | 0 |
| 3c:1e:04:28:0b:d7 | 1 | Angel Kusum | 22.4 | 0.0 | 0 | 816 | 0 | 0 | 7 | 0 | 0 | 0 |
| 3c:1e:04:2a:08:4f | 2 | Amazon | 17.5 | 10.0 | 64 | 454 | 100 | 0 | 84 | 0 | 0 | 5 |
| 78:54:2e:a3:23:06 | 2 | dlink | 0.4 | 12.5 | 2 | 13 | 0 | 0 | 1 | 2 | 0 | 0 |
| ac:67:06:32:7b:69 | | An0kit-ss3ccA-Et... | 0.1 | 0.0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| ac:67:06:36:93:e9 | | An0kit-ss3ccA-Et... | 0.2 | 66.7 | 4 | 0 | 0 | 6 | 0 | 0 | 0 | 0 |
| b4:75:0e:bb:e8:d3 | | <Broadcast> | 0.1 | 0.0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| c8:3a:35:5a:98:11 | 1 | Xoptimo | 0.1 | 33.3 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| c8:be:19:76:73:c4 | 1 | saham | 20.9 | 13.3 | 102 | 582 | 50 | 0 | 133 | 0 | 0 | 1 |
| c8:be:19:76:c0:a0 | | <Broadcast> | 0.2 | 0.0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 4 |
| e8:cc:18:b9:ed:08 | | <Broadcast> | 0.2 | 87.5 | 7 | 0 | 8 | 0 | 0 | 0 | 0 | 0 |
| ff:ff:ff:ff:ff:ff | 1 | <Broadcast> | 5.4 | 0.0 | 0 | 0 | 0 | 198 | 0 | 0 | 0 | 0 |
| ff:ff:ff:ff:ff:ff | | zerone-cisco | 1.0 | 0.0 | 0 | 0 | 0 | 38 | 0 | 0 | 0 | 0 |

The first two listings “CovertChannel” and “Big_Coffee_House” doesn’t have any data packets but only management packets (beacons and probe requests). This doesn’t happen in any normal network. It can happen if the network is not in use. But, it gives the investigator a reason to look into it. If we apply a filter to only check packets from “Big_Coffee_House”.

**Filter:** wlan contains Big_Coffee_House



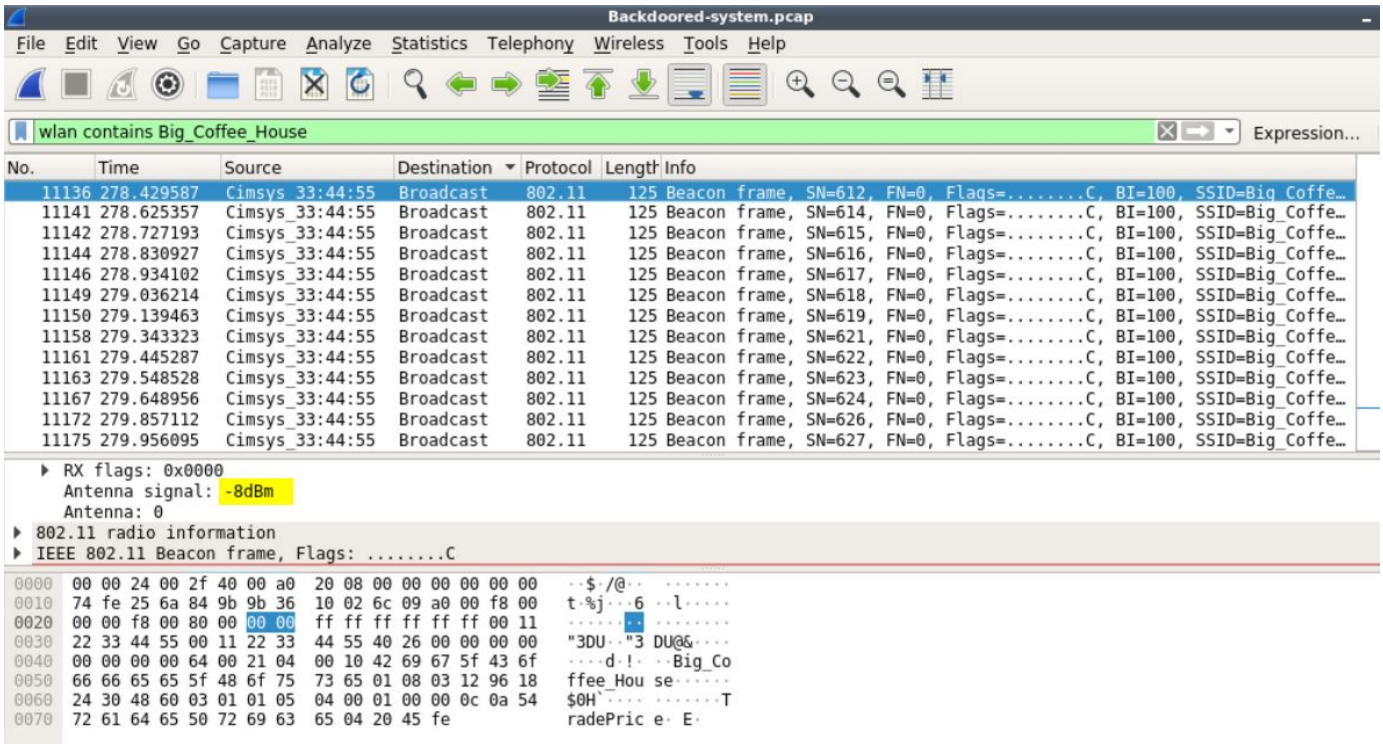

Scrolling through the packets, we can observe some content being passed as the unknown IEs payload.

**Answer:** Backdoor is using beacon and probe request frames to get commands and send information out.

**Question 2:** Can you tell something about the attacker or the attacker machine?

**Solution:**

The MAC (BSSI) address and RSSI strength from the packets can help in drawing conclusions on that.




**Answer:**

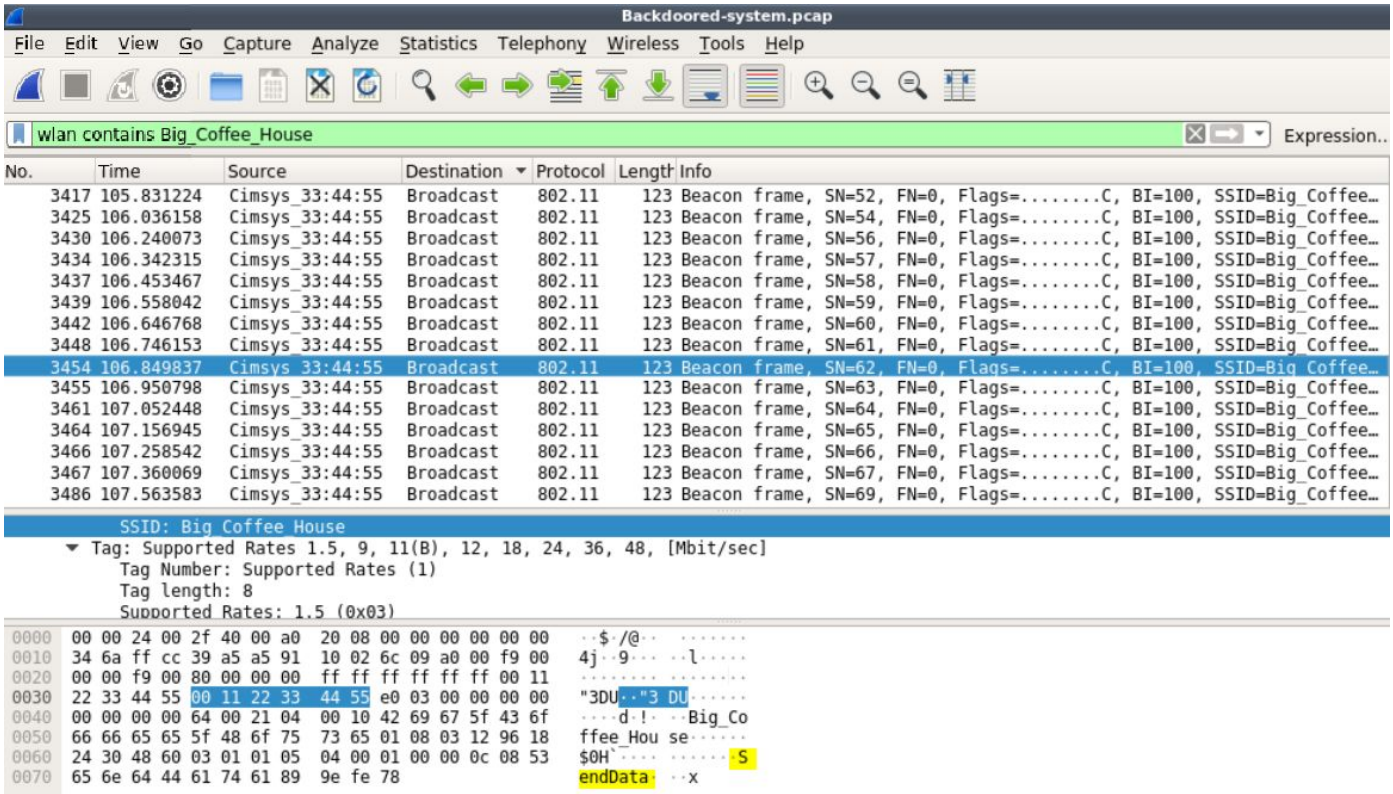
- Attacker machine's MAC is 00:11:22:33:44:55 which seems fake.
- The RSSI of beacon frames is very high (in range of one digit i.e. -9 dBm). Hence, it is possible that attacker's transmitter is just outside the boundary, most probably just opposite to a wall from the sensor and can be high power and directional. So, it is possible that attacker is just above floor (above the ceiling on which the sensor is installed).

**Question 3:** What information has been exchanged?

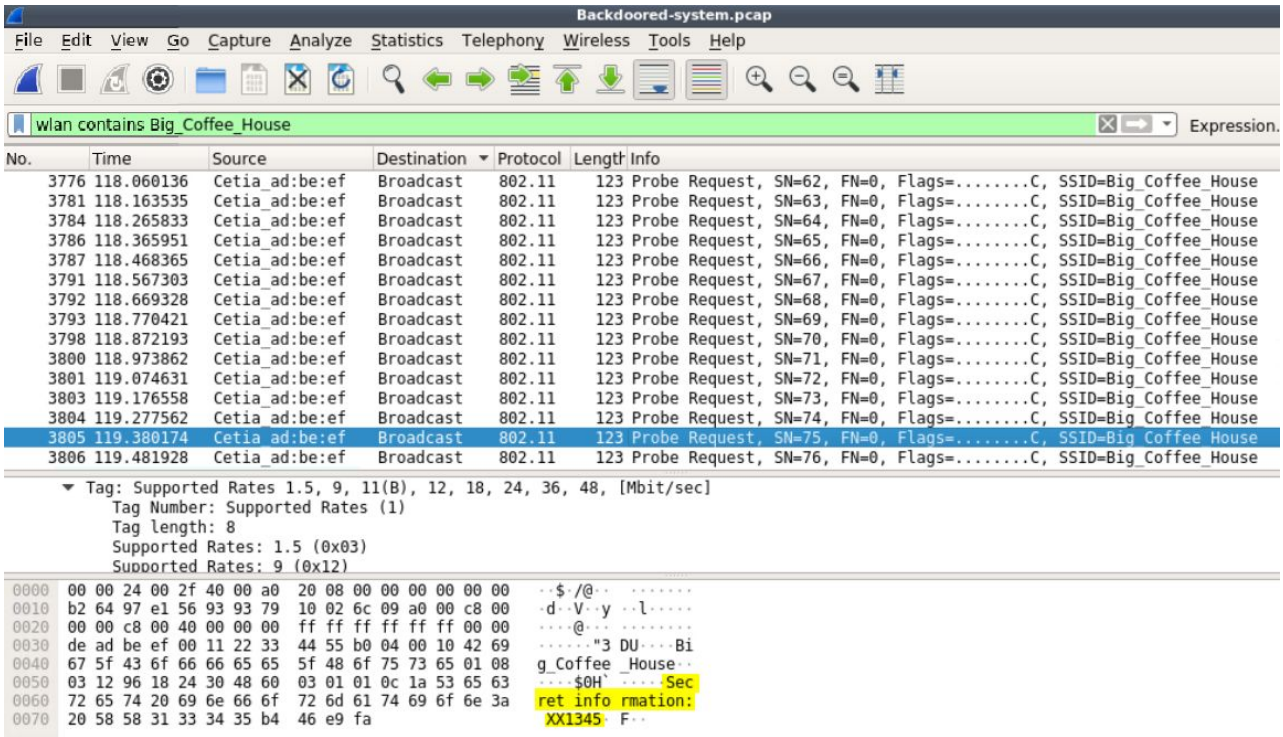
**Solution:**

We have to check the payload of different packets, also you will notice the same payload/message in multiple packets.

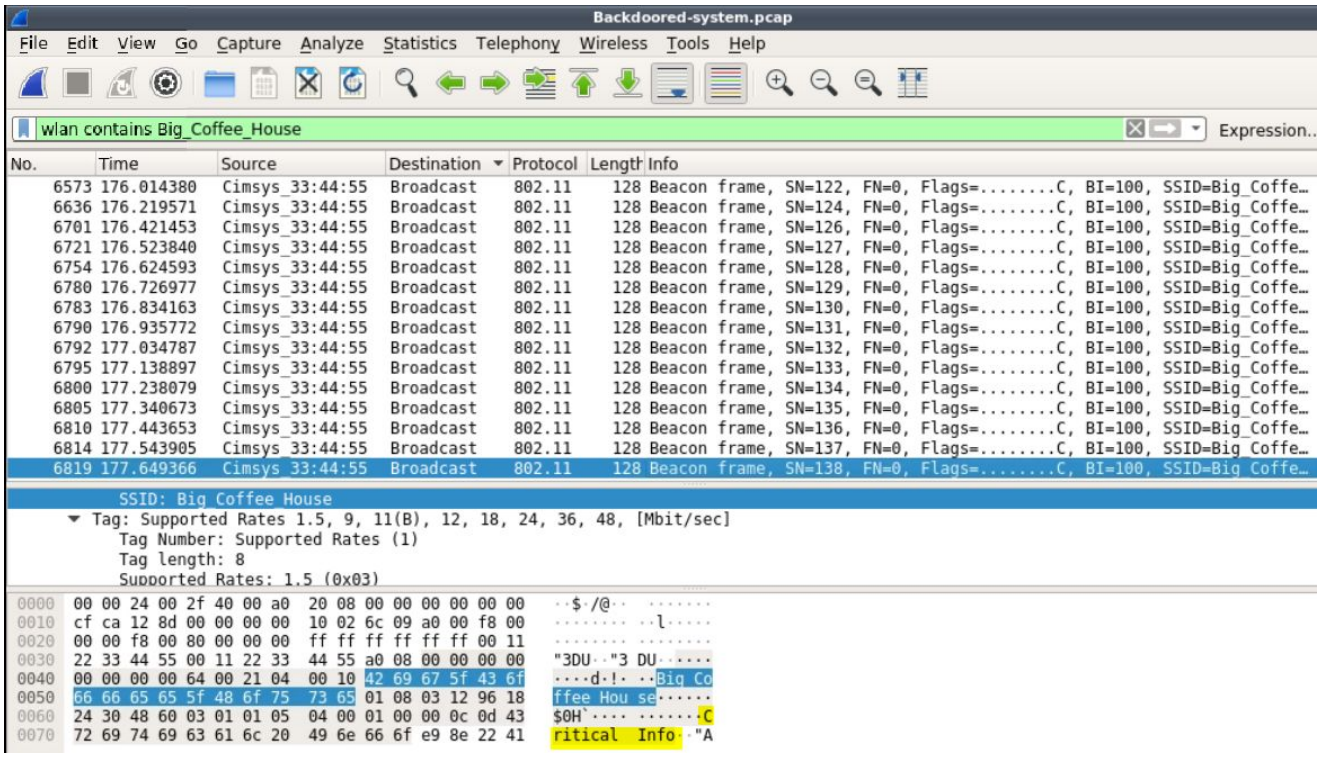
**Payload 1**



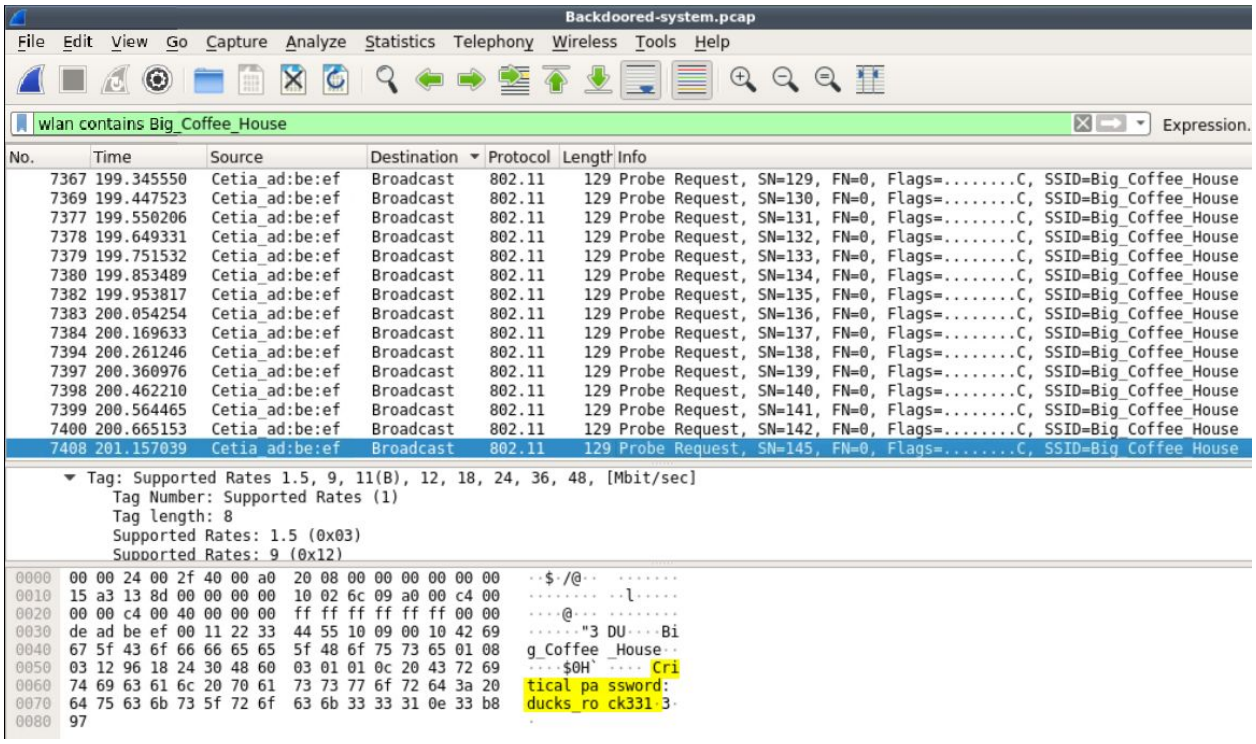
## Payload 2



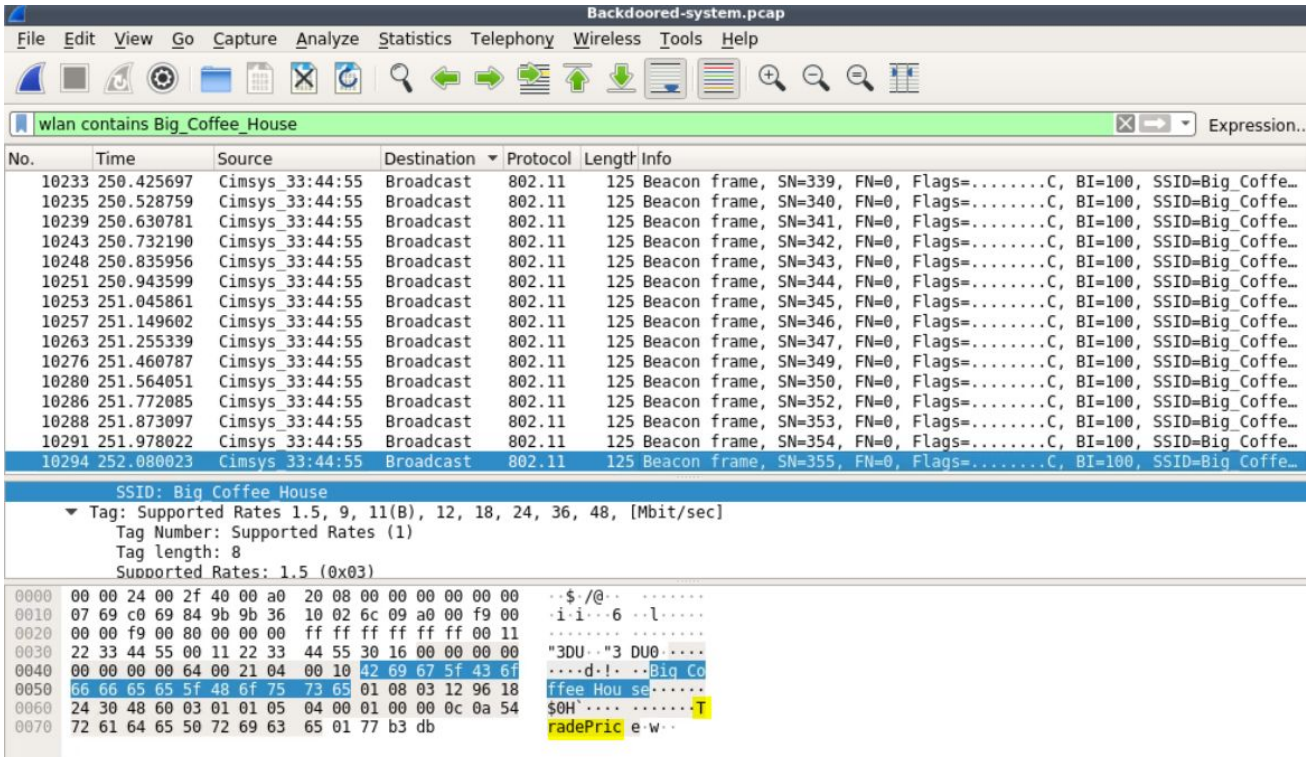

## Payload 3



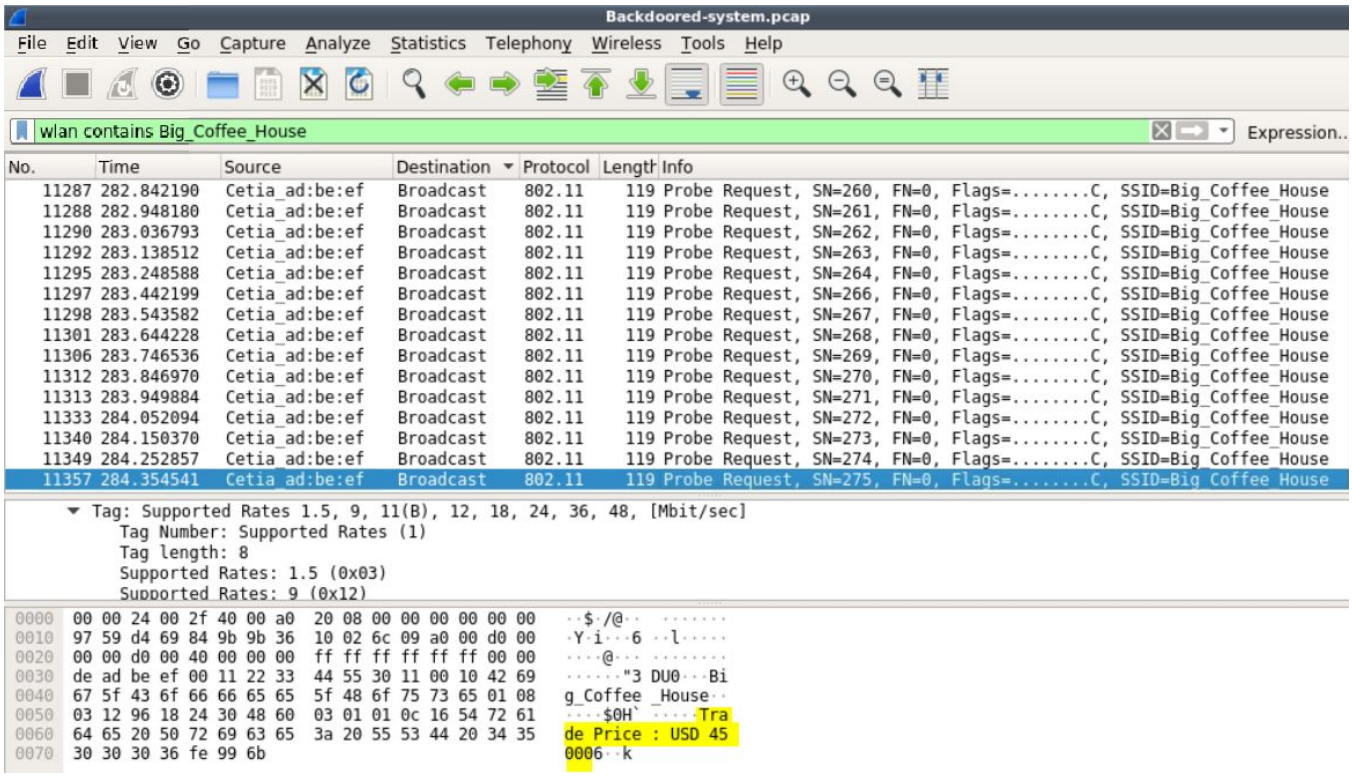
## Payload 4




## Payload 5



**Payload 6**




**Answer:** We found 3 rounds of message exchange. Given below:

- Attacker -> Backdoored machine: SendData
- Backdoored machine -> Attacker: Secret information: XX1345
- Attacker -> Backdoored machine: Critical Info
- Backdoored machine -> Attacker: Critical password:ducks_rock331
- Attacker -> Backdoored machine: TradePrice
- Backdoored machine -> Attacker: Trade Price : USD 45000