

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "TOOL BOX", "PENTESTING", "RED TEAM", "HACKER", "TRAINING", "ACCESS POINT", "WORLD-CLASS TRAINERS", "PATV", "TEAM LABS", "SPENTESTER", "ACADEMY", "ATTACKDEFENSE LABS", "COURSES ACCESS POINT PENTESTER", "ACCESS POINT TOOL BOX WORLD-CLASS TRAINERS", "ATTACKDEFENSE LABS TRAINING COURSES SPATV ACCESS", "PENTESTER ACADEMY RED TEAM LABS", "ATTACKDEFENSE LABS COURSES PENTESTER ACADEMY", "COURSES PENTESTER ACADEMY TOOL BOX PENTESTI", "SS POINT WORLD-CLASS TRAINERS TRAINING HACKER", "TOOL BOX", "HACKER PENTESTING", "RED TEAM LABS", "PENTESTER ACADEMY ATTACKDEFENSE LABS", "COURSES PENTESTER ACA", "PENTESTER ACADEMY ATTACKDEFENSE LABS", "TOOL BOX WORLD-CI", "WORLD-CLASS TRAINERS", "RED TEAM", "TRAINING CO", "PENTESTER ACADEMY", "TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and most central, with "ATTACK" in red and "DEFENSE" in dark blue. Below them, the phrase "by PentesterAcademy" is written in black. The background is white, and the overall design is clean and modern.

Name	Wi-Fi: SSIDs and BSSIDs
URL	https://www.attackdefense.com/challengedetails?cid=50
Type	Traffic Analysis: Tshark Fu

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. Also, note that the IP addresses and domain names might be different in your lab.

Q1. Find the number of beacon frames present in WiFi_traffic.pcap

Answer: 5868 Beacon Frames

Command: tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' | wc

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' | wc
5868   77912  816220
student@attackdefense:~$
```

Q2. Print unique list of all AP BSSIDs in WiFi_traffic.pcap

Command: tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' -T fields -e wlan.bssid | sort | uniq

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' -T fields -e wlan.bssid | sort | uniq
00:1e:40:ed:4b:0f
3c:1e:04:28:0b:d7
54:b8:0a:58:0b:34
6c:19:8f:5f:81:74
6c:72:20:6b:e3:ad
94:44:52:74:e6:7a
bc:ae:c5:c3:5e:01
bc:f6:85:4d:b2:93
c4:12:f5:bf:de:54
c8:be:19:79:31:90
e8:de:27:16:87:18
ec:22:80:c3:4a:68
fc:b0:c4:91:71:e0
fc:b0:c4:91:71:e1
fc:b0:c4:91:71:e2
fc:b0:c4:91:71:e3
student@attackdefense:~$
```

Q3. Print unique list of all AP SSIDs in WiFi_traffic.pcap

Command: tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' -T fields -e wlan.ssid | sort | uniq

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' -T fields -e wlan.ssid | sort | uniq
Amazon Wood
Angel Kusum
BinarySecuritySolutions
GUNEEV
Home_Network
Incredible Holidays
LazyArtists
Logistics
Nirmall
SecurityTube_Open
Shubha
belkin.367a
dg_patel
student@attackdefense:~$
```

Q4. In (3) change the filter so only non-null SSIDs are printed

Command: tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008 && !(wlan.tag.length ==0)' -T fields -e wlan.ssid | sort | uniq

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008 && !(wlan.tag.length ==0)' -T fields -e wlan.ssid | sort | uniq
Amazon Wood
Angel Kusum
BinarySecuritySolutions
GUNEEV
Home_Network
Incredible Holidays
LazyArtists
Logistics
Nirmall
SecurityTube_Open
Shubha
belkin.367a
dg_patel
student@attackdefense:~$
```

Q5. Print the unique list of SSID and BSSIDs side by side for all AP networks in WiFi_traffic.pcap

Command: tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' -T fields -e wlan.ssid -e wlan.bssid | sort | uniq

```
student@attackdefense:~$ tshark -r WiFi_traffic.pcap -Y 'wlan.fc.type_subtype == 0x0008' -T fields -e wlan.ssid -e wlan.bssid | sort | uniq
fc:b0:c4:91:71:e1
fc:b0:c4:91:71:e2
fc:b0:c4:91:71:e3
Amazon Wood      c8:be:19:79:31:90
Angel Kusum      3c:1e:04:28:0b:d7
BinarySecuritySolutions bc:ae:c5:c3:5e:01
GUNEEV 54:b8:0a:58:0b:34
Home_Network     6c:19:8f:5f:81:74
Incredible Holidays c4:12:f5:bf:de:54
LazyArtists      fc:b0:c4:91:71:e0
Logistics        6c:72:20:6b:e3:ad
Nirmall bc:f6:85:4d:b2:93
SecurityTube_Open e8:de:27:16:87:18
Shubha 00:1e:40:ed:4b:0f
belkin.367a      94:44:52:74:e6:7a
dg_patel         ec:22:80:c3:4a:68
student@attackdefense:~$
```



References:

1. Tshark (<https://www.wireshark.org/docs/man-pages/tshark.html>)
2. Wireshark (<https://www.wireshark.org/>)