

[illegible]

<b>Name</b>	WiFi Addict
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=72">https://www.attackdefense.com/challengedetails?cid=72</a>
<b>Type</b>	Forensics : WiFi

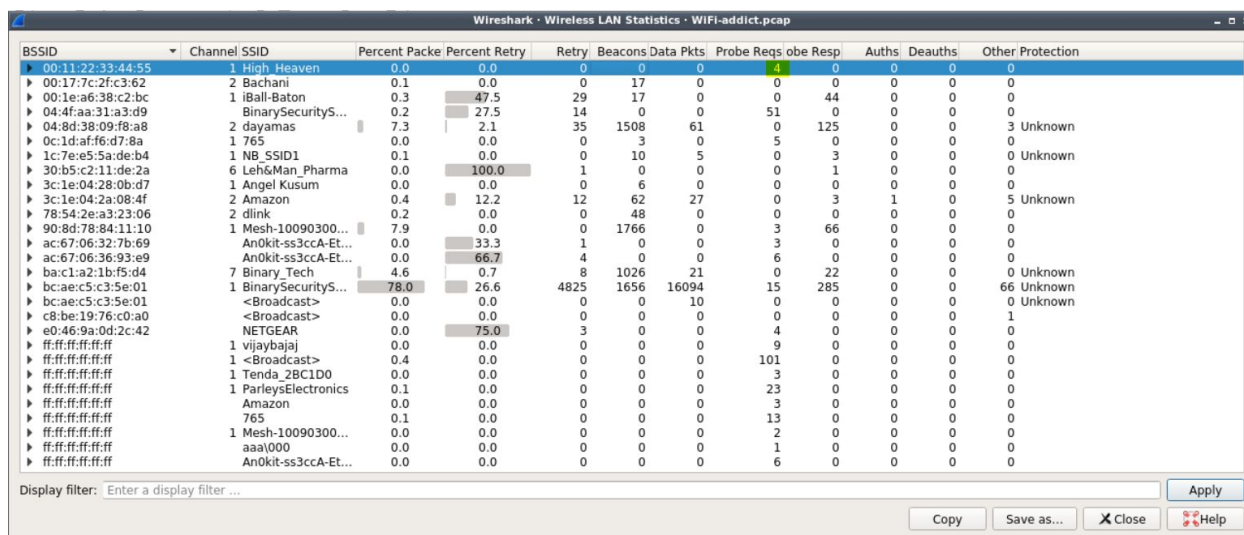
**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on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

**Question 1:** Who among the above is guilty?

**Solution:**

Check WiFi traffic summary using Wireless > WLAN Traffic option.

Some probe requests are present for High\_heaven cafe. From the case statement, one can correlate that the High Heaven was the cafe of the hotel, where the meeting took place.



BSSID	Channel	SSID	Percent Packets	Percent Retry	Retry	Beacons	Data Pkts	Probe Requests	Probe Responses	Auths	Deauths	Other	Protection
00:11:22:33:44:55	1	High Heaven	0.0	0.0	0	0	0	4	0	0	0	0	0
00:17:7c:2fc3:62	2	Bachani	0.1	0.0	0	17	0	0	0	0	0	0	0
00:1e:a6:38:c2:bc	1	iBall-Baton	0.3	47.5	29	17	0	0	44	0	0	0	0
04:4f:aa:31:a3:d9		BinarySecurityS...	0.2	27.5	14	0	0	51	0	0	0	0	0
04:8d:38:09:f8:a8	2	dayamas	7.3	2.1	35	1508	61	0	125	0	0	0	3 Unknown
0c:1d:af:f6:d7:8a	1	765	0.0	0.0	0	3	0	5	0	0	0	0	0
1c:7e:e5:5a:de:b4	1	NB_SSID1	0.1	0.0	0	10	5	0	3	0	0	0	0 Unknown
30:b5:c2:11:de:2a	6	Leh&Man_Pharma	0.0	100.0	1	0	0	0	1	0	0	0	0
3c:1e:04:28:0b:d7	1	Angel Kusum	0.0	0.0	0	6	0	0	0	0	0	0	0
3c:1e:04:2a:08:4f	2	Amazon	0.4	12.2	12	62	27	0	3	1	0	0	5 Unknown
78:54:2e:a3:23:06	2	dlink	0.2	0.0	0	48	0	0	0	0	0	0	0
90:8d:78:84:11:10	1	Mesh-10090300...	7.9	0.0	0	1766	0	3	66	0	0	0	0
ac:67:06:32:7b:69		Anokit-ss3ccA-Et...	0.0	33.3	1	0	0	3	0	0	0	0	0
ac:67:06:36:93:e9		Anokit-ss3ccA-Et...	0.0	66.7	4	0	0	6	0	0	0	0	0
ba:c1:a2:1b:f5:d4	7	Binary_Tech	4.6	0.7	8	1026	21	0	22	0	0	0	0 Unknown
bc:ae:c5:c3:5e:01	1	BinarySecurityS...	78.0	26.6	4825	1656	16094	15	285	0	0	0	66 Unknown
bc:ae:c5:c3:5e:01		<Broadcast>	0.0	0.0	0	0	10	0	0	0	0	0	0 Unknown
c8:be:19:76:c0:a0		<Broadcast>	0.0	0.0	0	0	0	0	0	0	0	0	1
e0:46:9a:0d:2c:42		NETGEAR	0.0	75.0	3	0	0	4	0	0	0	0	0
ff:ff:ff:ff:ff:ff	1	vijaybajaj	0.0	0.0	0	0	0	9	0	0	0	0	0
ff:ff:ff:ff:ff:ff	1	<Broadcast>	0.4	0.0	0	0	0	101	0	0	0	0	0
ff:ff:ff:ff:ff:ff	1	Tenda_2BC1D0	0.0	0.0	0	0	0	3	0	0	0	0	0
ff:ff:ff:ff:ff:ff	1	ParleysElectronics	0.1	0.0	0	0	0	23	0	0	0	0	0
ff:ff:ff:ff:ff:ff		Amazon	0.0	0.0	0	0	0	3	0	0	0	0	0
ff:ff:ff:ff:ff:ff		765	0.1	0.0	0	0	0	13	0	0	0	0	0
ff:ff:ff:ff:ff:ff	1	Mesh-10090300...	0.0	0.0	0	0	0	2	0	0	0	0	0
ff:ff:ff:ff:ff:ff		aaa0000	0.0	0.0	0	0	0	1	0	0	0	0	0
ff:ff:ff:ff:ff:ff		Anokit-ss3ccA-Et...	0.0	0.0	0	0	0	6	0	0	0	0	0

Check the sender MAC address for the probes sent for High Heaven's WiFi network i.e. High\_Heaven. The MAC belongs to Ms Hannah's device. This tells us that she has used this WiFi network which in turn states that she was at that venue.

**Filter:** wlan.ssid=="High\_Heaven"

The image shows a Wireshark capture of network traffic. The top pane displays a list of filtered packets (wlan.ssid=="High\_Heaven"). The middle pane shows the details of the selected packet (Frame 4058), including the IEEE 802.11 radio information and the probe request details. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4058	128.313741	Cetia_ad:be:ef	Broadcast	802.11	90	Probe Request, SN=1507, FN=0, Flags=.....C, SSID=High Heaven
28653	246.042036	Cetia_ad:be:ef	Broadcast	802.11	90	Probe Request, SN=1761, FN=0, Flags=.....C, SSID=High Heaven
29782	247.765542	Cetia_ad:be:ef	Broadcast	802.11	90	Probe Request, SN=1778, FN=0, Flags=.....C, SSID=High Heaven
80113	375.437349	Cetia_ad:be:ef	Broadcast	802.11	90	Probe Request, SN=2249, FN=0, Flags=.....C, SSID=High Heaven

Frame 4058: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0  
Radiotap Header v0, Length 36  
802.11 radio information  
IEEE 802.11 Probe Request, Flags: .....C  
Type/Subtype: Probe Request (0x0004)  
Frame Control Field: 0x4000  
Duration: 0 microseconds  
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)  
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)  
Transmitter address: Cetia\_ad:be:ef (00:00:de:ad:be:ef)  
Source address: Cetia\_ad:be:ef (00:00:de:ad:be:ef)  
BSS Id: Cimsys\_33:44:55 (00:11:22:33:44:55)  
Fragment number: 0  
Sequence number: 1507  
Frame check sequence: 0x546781b5 [correct]  
[FCS Status: Good]

One might argue that she might have gone there for some other reason. But, remember, we are only looking for a probable cause. We are not declaring her the culprit but giving the security team a reason to launch a proper investigation. The possible culprit is Ms. Hanna (SVP Production).

**Answer:** Ms. Hanna (SVP Production).