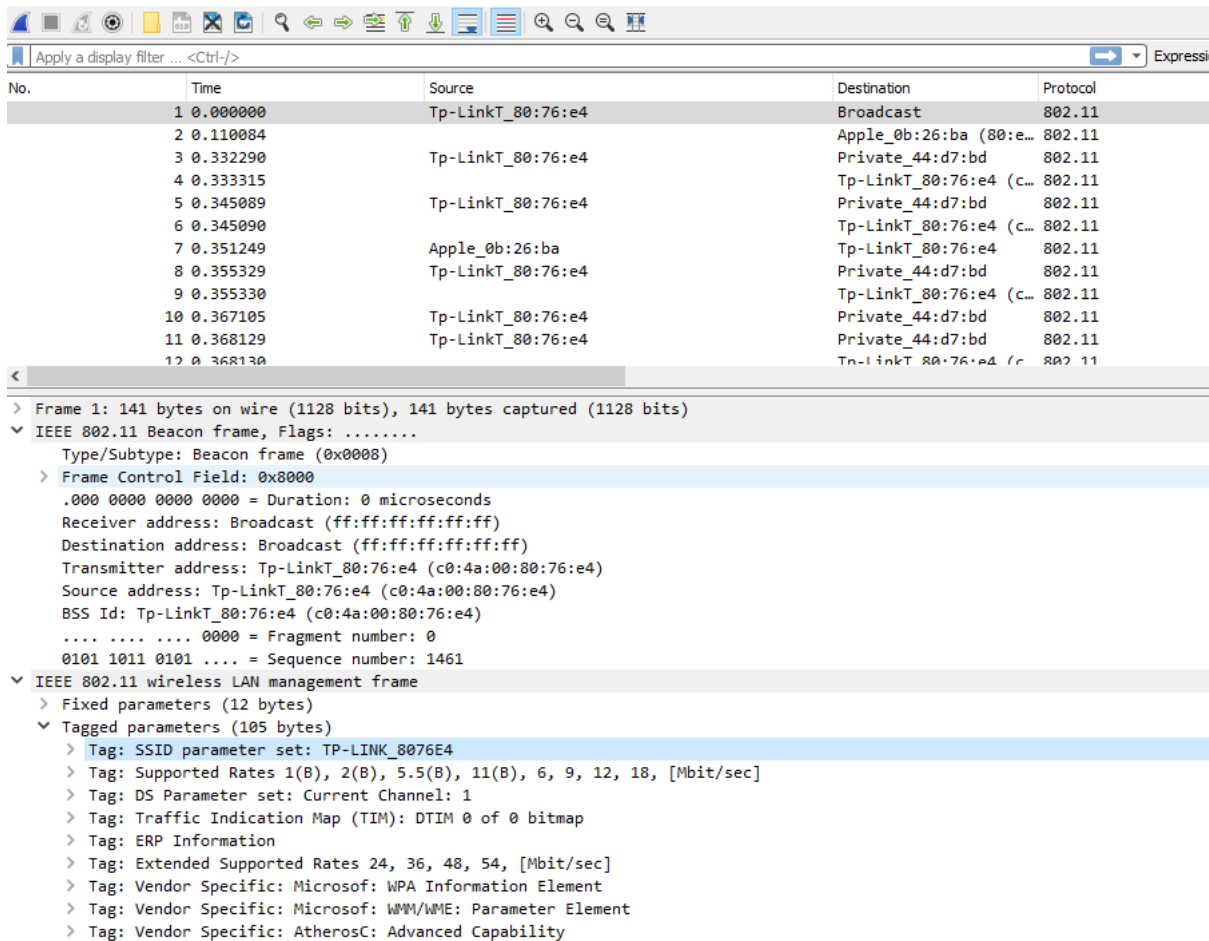


## Wireless Access Exploitation

### PCAP 3 (Hard)

This challenge evaluates the contestant's ability to crack WPA encryption given a packet capture. The [aircrack-ng](#) Linux tool can be used to solve this challenge. In addition, the [rockyou wordlist](#) is useful for cracking the password.

Questions 1 and 2 can be solved by analyzing the packet capture in Wireshark. Since only access points are supposed to send beacon frames, the access point can be easily identified.



The image shows a Wireshark packet capture analysis. The top pane displays a list of 12 packets. Packet 1 is an IEEE 802.11 Beacon frame from Tp-LinkT\_80:76:e4 to Broadcast. The bottom pane shows the detailed view of this beacon frame, including its structure and various information elements.

No.	Time	Source	Destination	Protocol
1	0.000000	Tp-LinkT_80:76:e4	Broadcast	802.11
2	0.110084		Apple_0b:26:ba (80:e...	802.11
3	0.332290	Tp-LinkT_80:76:e4	Private_44:d7:bd	802.11
4	0.333315		Tp-LinkT_80:76:e4 (c...	802.11
5	0.345089	Tp-LinkT_80:76:e4	Private_44:d7:bd	802.11
6	0.345090		Tp-LinkT_80:76:e4 (c...	802.11
7	0.351249	Apple_0b:26:ba	Tp-LinkT_80:76:e4	802.11
8	0.355329	Tp-LinkT_80:76:e4	Private_44:d7:bd	802.11
9	0.355330		Tp-LinkT_80:76:e4 (c...	802.11
10	0.367105	Tp-LinkT_80:76:e4	Private_44:d7:bd	802.11
11	0.368129	Tp-LinkT_80:76:e4	Private_44:d7:bd	802.11
12	0.368130		Tp-LinkT_80:76:e4 (c...	802.11

**Frame 1: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)**

- IEEE 802.11 Beacon frame, Flags: .....
  - Type/Subtype: Beacon frame (0x0008)
  - Frame Control Field: 0x8000
    - .000 0000 0000 0000 = Duration: 0 microseconds
    - Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    - Transmitter address: Tp-LinkT\_80:76:e4 (c0:4a:00:80:76:e4)
    - Source address: Tp-LinkT\_80:76:e4 (c0:4a:00:80:76:e4)
    - BSS Id: Tp-LinkT\_80:76:e4 (c0:4a:00:80:76:e4)
    - .... .... 0000 = Fragment number: 0
    - 0101 1011 0101 .... = Sequence number: 1461
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (12 bytes)
  - Tagged parameters (105 bytes)
    - Tag: SSID parameter set: TP-LINK\_8076E4
    - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    - Tag: DS Parameter set: Current Channel: 1
    - Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    - Tag: ERP Information
    - Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    - Tag: Vendor Specific: Microsoft: WPA Information Element
    - Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element
    - Tag: Vendor Specific: AtherosC: Advanced Capability



© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Question 3 can be solved by running aircrack-ng on the packet capture.

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt -b C0:4A:00:80:76:E4 NCL-2015-PCAP3.cap
```

```
[00:02:29] 185752 keys tested (1266.94 k/s)

KEY FOUND! [ blueberry muffin ]

Master Key   : 5A 75 D7 85 D4 01 7C 70 20 E9 65 FD FC E5 45 4B
              DD DC 99 33 93 23 81 52 D7 FD CA 4E A8 34 82 C0

Transient Key : 29 AE 08 6D 9C 01 BD 98 D3 AB 2E 2B 25 1B FE 2C
              45 1A AD D7 79 B7 02 FB 5E 25 A3 44 3B 82 DB B5
              19 6C EA 12 1A 5D 15 51 29 0F C0 22 CA 16 10 6B
              E0 49 44 D4 1A CF D4 04 A3 17 E9 6C B0 12 9C 83

EAPOL HMAC   : 11 F0 85 20 D7 F6 B5 BB A6 69 61 9C 04 DC 50 AB
root@kali:~/Desktop/ncl# aircrack-ng -w /usr/share/wordlists/rockyou.txt -b C0:4A:00:80:76:E4 NCL-2015-PCAP3.cap
```

© 2017 Cyber Skyline



© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.



© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Questions 4 – 11 can be solved by using the previously acquired WPA key to decrypt traffic in Wireshark. This can be done by selecting “Edit > Preferences > Protocols > IEEE 802.11” and then checking “Enable decryption” and adding the decryption key.

Questions 4 – 9 can be solved by following various TCP streams for HTTP traffic between a user and the router’s admin panel.

```
GET /userRpm/StatusRpm.htm HTTP/1.1
Host: 192.168.0.254
Connection: keep-alive
Authorization: Basic YWRtaW46TkNMLVJDSkQtNjI4MQ==
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36
DNT: 1
Referer: http://192.168.0.254/userRpm/StatusRpm.htm
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4
```

```
HTTP/1.1 200 OK
Server: Router
Connection: close
Content-Type: text/html
WWW-Authenticate: Basic realm="TP-LINK Wireless N Nano Router WR702N"
```

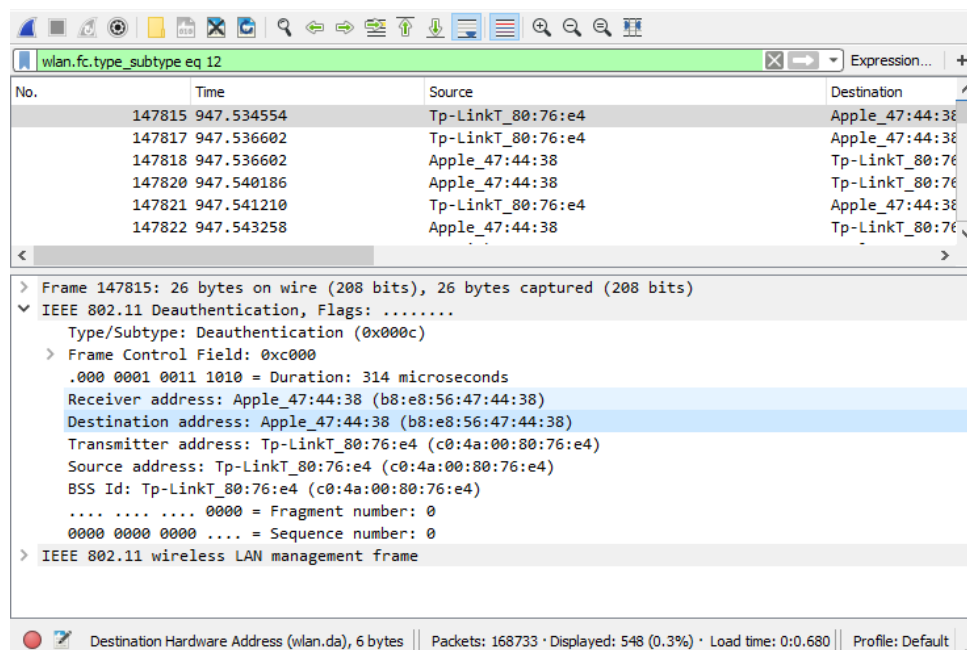
```
<SCRIPT language="javascript" type="text/javascript">
var statusPara = new Array(
1,
1,
21,
15000,
392,
"4.19.1 Build 130528 Rel.52704n ",
"WR702N 1.0 00000000",
1,
0,0 );
</SCRIPT>
<SCRIPT language="javascript" type="text/javascript">
var lanPara = new Array(
"C0-4A-00-80-76-E4",
"192.168.0.254",
"255.255.255.0",
0,0 );
</SCRIPT>
<SCRIPT language="javascript" type="text/javascript">
var wlanPara = new Array(
1,
"TP-LINK_8076E4",
1,
5,
"C0-4A-00-80-76-E4",
"192.168.0.254",
2,
7,
0,
1,
6,
0,0 );
</SCRIPT>
```



© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Questions 10 and 1 can be solved by using the filter:

wlan.fc.type\_subtype eq 12



Question	Answer
What is the MAC address of the router?	C0:4A:00:80:76:E4
What is the ESSID of the router?	TP-LINK_8076E4
What is the password for the wireless network?	blueberrymuffin
What is the IP address of the router?	192.168.0.254
What company manufactured the router?	TP-LINK
What is the model of the router?	WR702N
What firmware version is installed on the router?	4.19.1
What release number is the router using?	52704n
What is the IP address of the user who logged into the router admin panel?	192.168.0.101
What is the MAC address of the first victim of the deauthentication attack?	B8:E8:56:47:44:38
What is the MAC address of the second victim of the deauthentication attack?	80:E6:50:0B:26:BA