**SSN College of Engineering,**
**Department of Computer Science and Engineering**
**CS6711 Security Laboratory**

**Exercise 12:**

To perform wireless audit on an access point or a router and decrypt WEP

**Introduction:**

- Components of a Wireless Network
  - Wireless network interface cards (WNICs), which transmit and receive wireless signals,
  - Access points (APs), which are the bridge between wired and wireless networks. An access point (AP) is a radio transceiver that connects to a network via an Ethernet cable and bridges a wireless LAN (WLAN) with a wired network. An AP is where RF channels are configured.
  - APs are what hackers look for when they drive around with an antenna and a laptop computer scanning for access.
  - A service set identifier (SSID) is the name used to identify a WLAN, much the same way a workgroup is used on a Windows network.
  - An SSID is configured on the AP as a unique, 1-to 32-character, case-sensitive alphanumeric name.
  - The AP usually beacons (broadcasts) the SSID several times a second so that users who have WNICs can see a display of all WLANs within range of the AP's signal
  - WEP is the acronym for Wired Equivalent Privacy. It was developed for IEEE 802.11 WLAN standards. Its goal was to provide the privacy equivalent to that provided by wired networks. WEP works by encrypting the data been transmitted over the network to keep it safe from eavesdropping.
  - WPA is the acronym for Wi-Fi Protected Access. It is a security protocol developed by the Wi-Fi Alliance in response to the weaknesses found in WEP. It is used to encrypt data on 802.11 WLANs. It uses higher Initial Values 48 bits instead of the 24 bits that WEP uses. It uses temporal keys to encrypt packets.
  -
- Wireless network surveys, or audits aim at both identifying security and performance issues in the network.

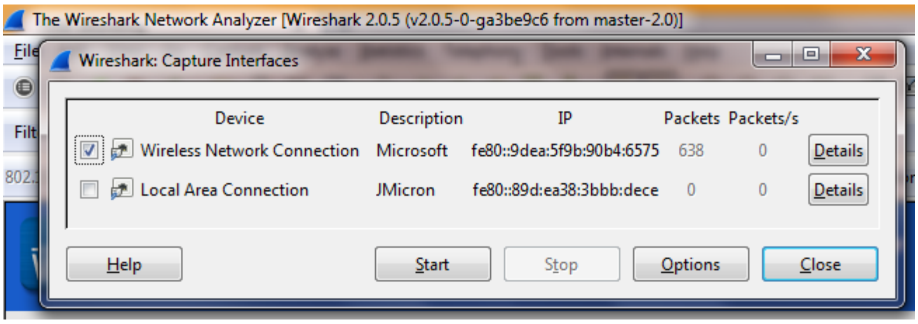
- Wireshark is network protocol analyzer that captures packets, decodes & analyzes contents

**Setting Up a wireshark**

1. Step 1: Start Wireshark
   download wireshark for windows and follow the install instructions.

2. Capture data and Hack WiFi using Wireshark:

   - First of all, we have to configure Wireshark. For proper configuration, change the wireless interface to 802.11 client device. To do this, click the Capture menu, choose Options, and select the appropriate interface.
   -



The Wireshark Network Analyzer [Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0)]

Wireshark: Capture Interfaces

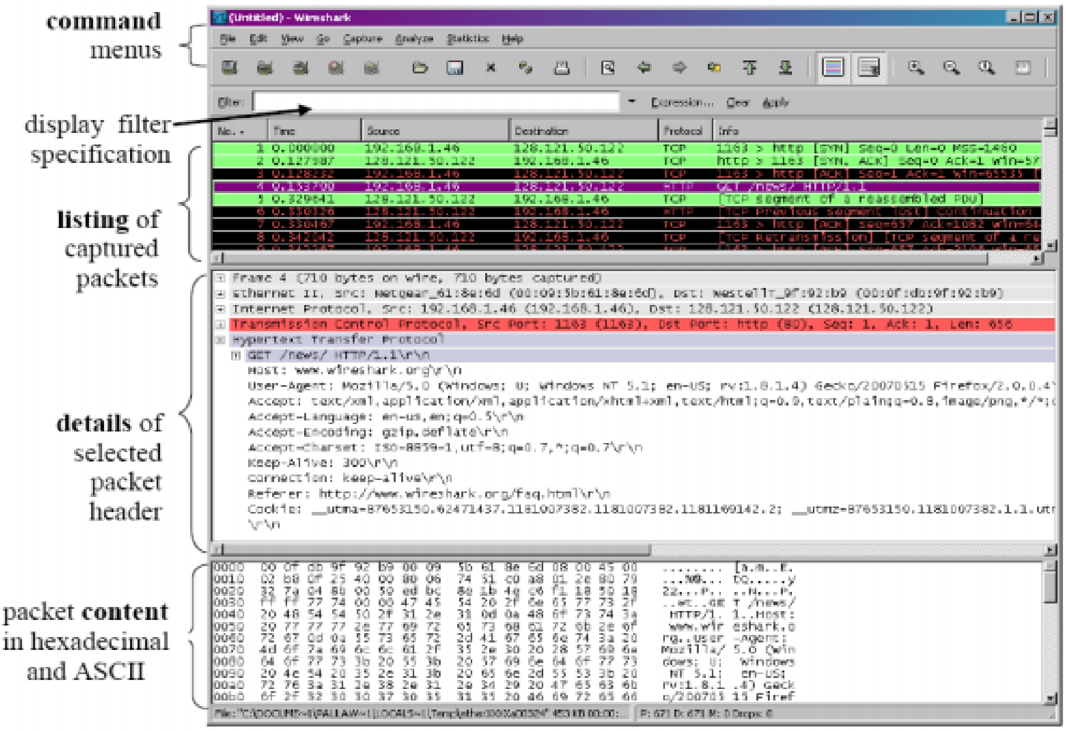
| | Device | Description | IP | Packets | Packets/s | |
|---|---|---|---|---|---|---|
| ☑ | Wireless Network Connection | Microsoft | fe80::9dea:5f9b:90b4:6575 | 638 | 0 | Details |
| □ | Local Area Connection | JMicron | fe80::89d:ea38:3bbb:dece | 0 | 0 | Details |

3. You can also choose filters if you need one. Filters are used to capture a particular packet data for outgoing traffic. To set a filter, click the Capture menu, choose Options, and click Capture Filter. The Wireshark Capture Filter window will appear and now you can set various filters according to your needs.

4. We are now ready for capturing network traffic to hack WiFi using Wireshark.

5. Now we will start Packet capturing process to Hack WiFi. To do so, click the capture menu and choose start. You will see that **Wireshark is capturing traffic** and it will continue until its buffer is filled up. If you think that you have enough packets, click the Capture menu and choose Stop.

6. Capture Interface Options


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply

```
No. -  Time        Source           Destination      Protocol  Info
     1 0.000000    192.168.1.46     128.121.50.122   TCP       1163 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.127987    128.121.50.122   192.168.1.46     TCP       http > 1163 [SYN, ACK] Seq=0 Ack=1 Win=57
     3 0.128232    192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=1 Ack=1 Win=65535 [
     4 0.153700    192.168.1.46     128.121.50.122   HTTP      GET /news/ HTTP/1.1
     5 0.329841    128.121.50.122   192.168.1.46     TCP       [TCP segment of a reassembled PDU]
     6 0.330126    128.121.50.122   192.168.1.46     HTTP      [TCP Previous segment lost] Continuation
     7 0.330467    192.168.1.46     128.121.50.122   TCP       1163 > http [ACK] Seq=657 Ack=1082 Win=64
     8 0.342042    128.121.50.122   192.168.1.46     TCP       [TCP Retransmission] [TCP segment of a re
```

```
⊞ Frame 4 (710 bytes on wire, 710 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: Westell_9f:92:b9 (00:0f:db:9f:92:b9)
⊞ Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)
⊞ Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656
⊟ Hypertext Transfer Protocol
  ⊞ GET /news/ HTTP/1.1\r\n
    Host: www.wireshark.org\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://www.wireshark.org/faq.html\r\n
    Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utr
    \r\n
```

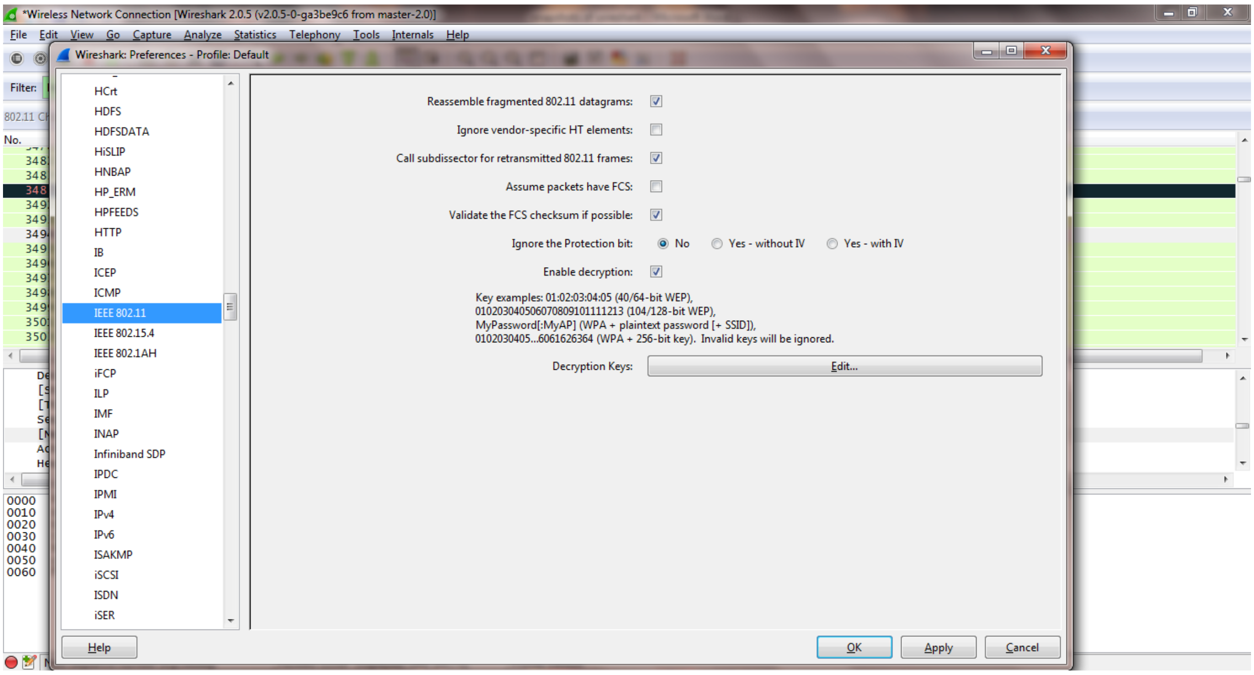
```
0000  00 0f db 9f 92 b9 00 09  5b 61 8e 6d 08 00 45 00   ........ [a.m..E.
0010  02 b8 0f 25 40 00 80 06  74 51 c0 a8 01 2e 80 79   ...%@... tQ.....y
0020  32 7a 04 8b 00 50 ed bc  8e 1b 4e c6 f1 18 50 18   2z...P.. ..N...P.
0030  ff ff 77 74 00 00 47 45  54 20 2f 6e 65 77 73 2f   ..wt..GE T /news/
0040  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0050  20 77 77 77 2e 77 69 72  65 73 68 61 72 6b 2e 6f    www.wir eshark.o
0060  72 67 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   rg..User -Agent:
0070  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0080  64 6f 77 73 3b 20 55 3b  20 57 69 6e 64 6f 77 73   dows; U;  Windows
0090  20 4e 54 20 35 2e 31 3b  20 65 6e 2d 55 53 3b 20    NT 5.1;  en-US;
00a0  72 76 3a 31 2e 38 2e 31  2e 34 29 20 47 65 63 6b   rv:1.8.1 .4) Geck
00b0  6f 2f 32 30 30 37 30 35  31 35 20 46 69 72 65 66   o/200705 15 Firef
```

File: "C:\DOCUME~1\PALLAW~1\LOCALS~1\Temp\etherXXXXa00324" 453 KB 00:00:... P: 671 D: 671 M: 0 Drops: 0

7. **How to Decrypt 802.11:** Wireshark can decrypt WEP and WPA/WPA2.

    - You can add decryption keys using Wireshark's 802.11 preferences or by using the wireless toolbar. Up to 64 keys are supported.

8. Adding Keys: 802.11 Preferences: Go to *Edit->Preferences->IEEE 802.11* or choose wireless tool bar in view menu.


*Wireless Network Connection [Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Wireshark: Preferences - Profile: Default
Filter:
No.
HCrt
HDFS
HDFSDATA
HiSLIP
HNBAP
HP_ERM
HPFEEDS
HTTP
IB
ICEP
ICMP
IEEE 802.11
IEEE 802.15.4
IEEE 802.1AH
iFCP
ILP
IMF
INAP
Infiniband SDP
IPDC
IPMI
IPv4
IPv6
ISAKMP
iSCSI
ISDN
iSER
Help
OK
Apply
Cancel

Reassemble fragmented 802.11 datagrams: ☑

Ignore vendor-specific HT elements: ☐

Call subdissector for retransmitted 802.11 frames: ☑

Assume packets have FCS: ☐

Validate the FCS checksum if possible: ☑

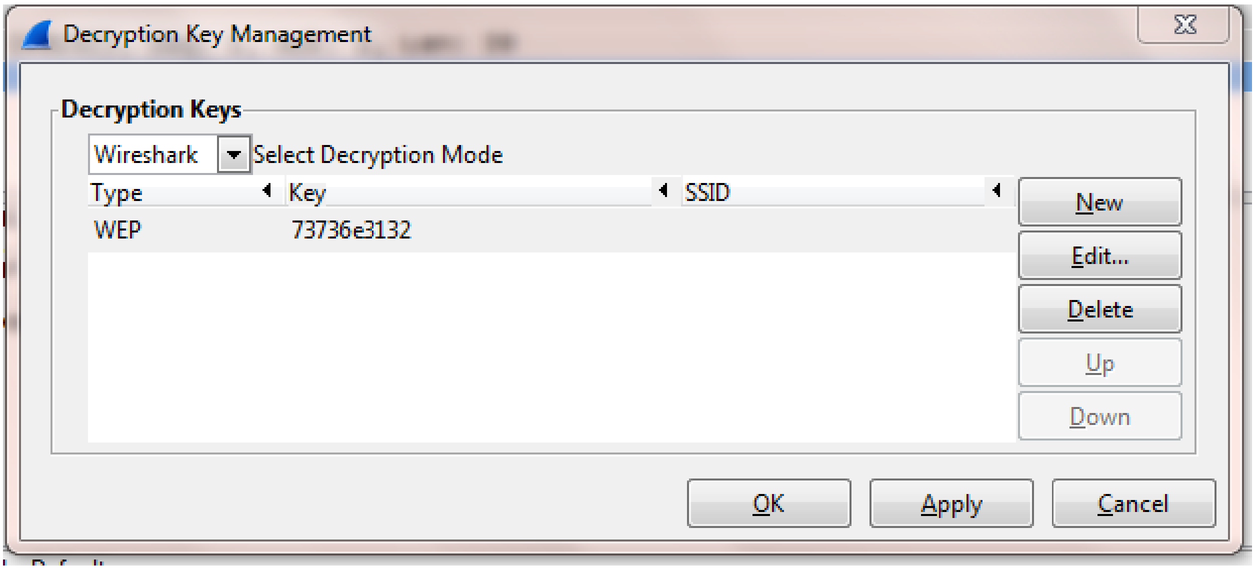
Ignore the Protection bit: ● No ○ Yes - without IV ○ Yes - with IV

Enable decryption: ☑

Key examples: 01:02:03:04:05 (40/64-bit WEP),
0102030405060708091011111213 (104/128-bit WEP),
MyPassword[:MyAP] (WPA + plaintext password [+ SSID]),
0102030405...6061626364 (WPA + 256-bit key). Invalid keys will be ignored.

Decryption Keys: Edit...

9. Select enable decryption and press the edit button against decryption keys. You will get a display as follows. Select the key type as WEP and provide the password of the wireless network under the key tab and press Apply and ok.



Decryption Key Management

Decryption Keys

Wireshark Select Decryption Mode

| Type | Key | SSID |
|---|---|---|
| WEP | 73736e3132 | |

10. Selecting **Wireshark** uses Wireshark's built-in decryption features and will pass the keys on to the AirPcap adapter so that 802.11 traffic is decrypted before it's passed on to Wireshark.