EXPERIMENT 6: NETWORK HEALTH MONITORING USING WIRESHARK PACKET SNIFFER

TEAM 9

AIM

To monitor network health using the Wireshark packet sniffer tool.

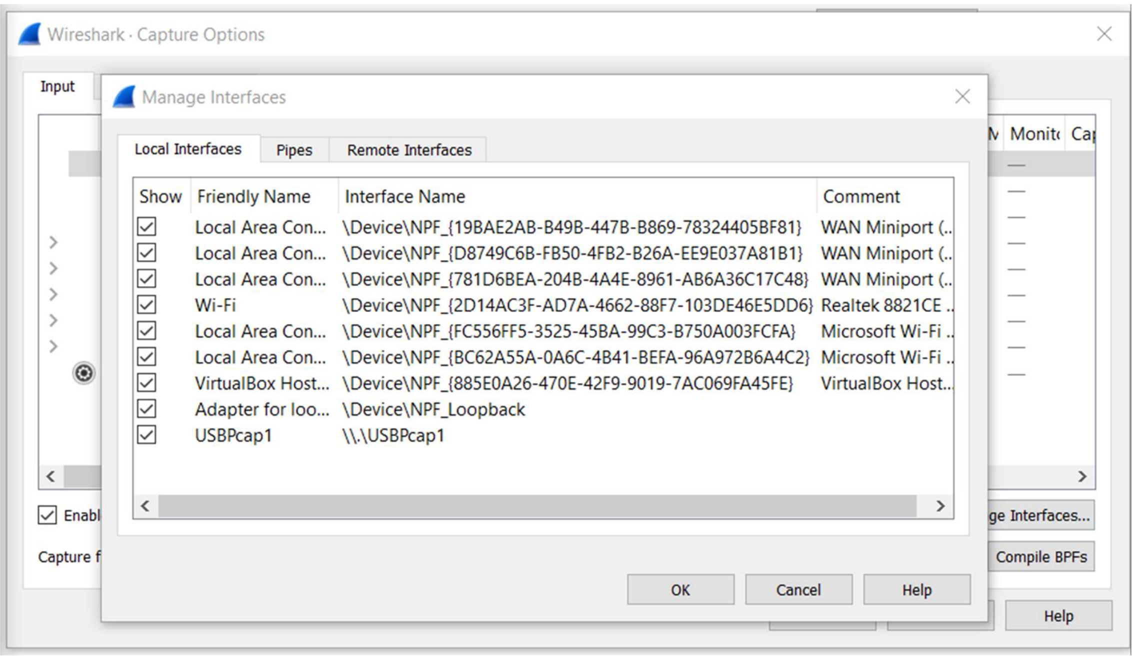
SOFTWARES REQUIRED

Wireshark 4.0.2 64-bit, the Wireshark Developer Community

Running on 64-bit Windows 10 (21H2), build 19044, with 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz (with SSE4.2), with 7926 MB of physical memory, with GLib 2.72.3, with PCRE2 10.40 2022-04-14, with Qt 5.15.2, with Npcap version 1.71, based on libpcap version 1.10.2-PRE-GIT, with c-ares 1.18.1, with GnuTLS 3.6.3, with Gcrypt 1.10.1, with nghttp2 1.46.0, with brotli 1.0.9, with LZ4 1.9.3, with Zstandard 1.5.2, without AirPcap, with light display mode, without HiDPI, with LC_TYPE=English_India.utf8, binary plugins supported.

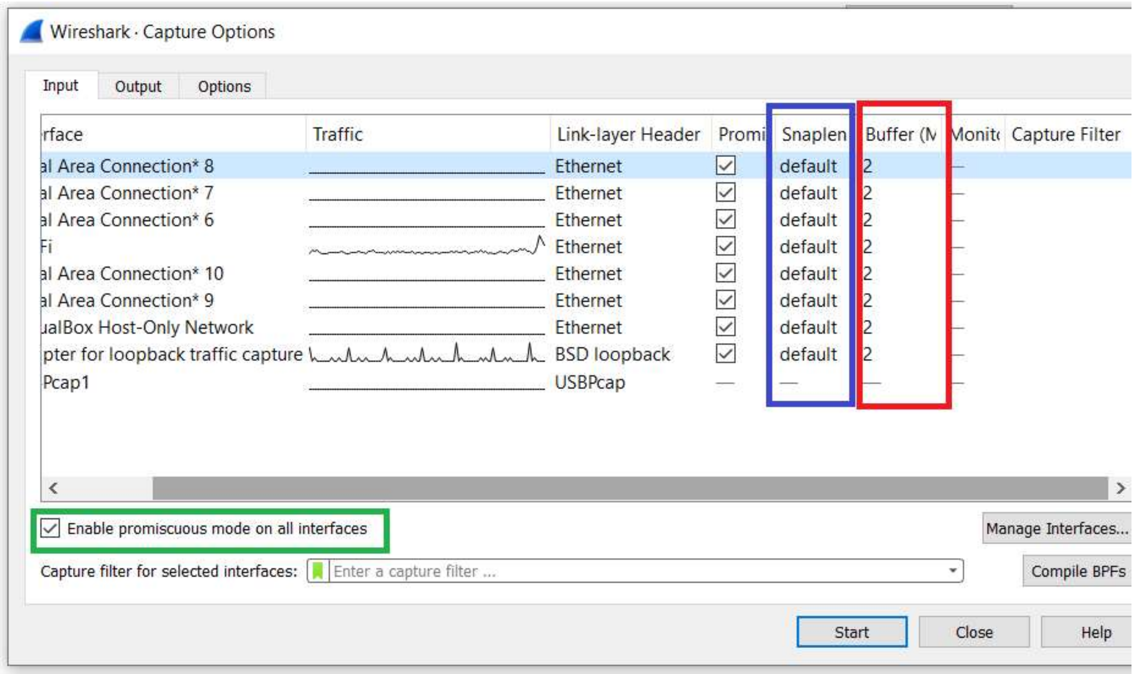
THEORY & SCREENSHOTS OF I/O

(i) Capturing & Analysing Ethernet Networks



Show	Friendly Name	Interface Name	Comment
☑	Local Area Con...	\Device\NPF_{19BAE2AB-B49B-447B-B869-78324405BF81}	WAN Miniport (..
☑	Local Area Con...	\Device\NPF_{D8749C6B-FB50-4FB2-B26A-EE9E037A81B1}	WAN Miniport (..
☑	Local Area Con...	\Device\NPF_{781D6BEA-204B-4A4E-8961-AB6A36C17C48}	WAN Miniport (..
☑	Wi-Fi	\Device\NPF_{2D14AC3F-AD7A-4662-88F7-103DE46E5DD6}	Realtek 8821CE ..
☑	Local Area Con...	\Device\NPF_{FC556FF5-3525-45BA-99C3-B750A003FCFA}	Microsoft Wi-Fi ..
☑	Local Area Con...	\Device\NPF_{BC62A55A-0A6C-4B41-BEFA-96A972B6A4C2}	Microsoft Wi-Fi ..
☑	VirtualBox Host...	\Device\NPF_{885E0A26-470E-42F9-9019-7AC069FA45FE}	VirtualBox Host..
☑	Adapter for loo...	\Device\NPF_Loopback	
☑	USBPcap1	\\.\USBPcap1	

Figure 1 – Manage Interfaces



rface	Traffic	Link-layer Header	Promi	Snaplen	Buffer (M	Monit	Capture Filter
al Area Connection* 8		Ethernet	☑	default	2	—	
al Area Connection* 7		Ethernet	☑	default	2	—	
al Area Connection* 6		Ethernet	☑	default	2	—	
Fi		Ethernet	☑	default	2	—	
al Area Connection* 10		Ethernet	☑	default	2	—	
al Area Connection* 9		Ethernet	☑	default	2	—	
ualBox Host-Only Network		Ethernet	☑	default	2	—	
pter for loopback traffic capture		BSD loopback	☑	default	2	—	
Pcap1		USBPcap	—	—	—	—	

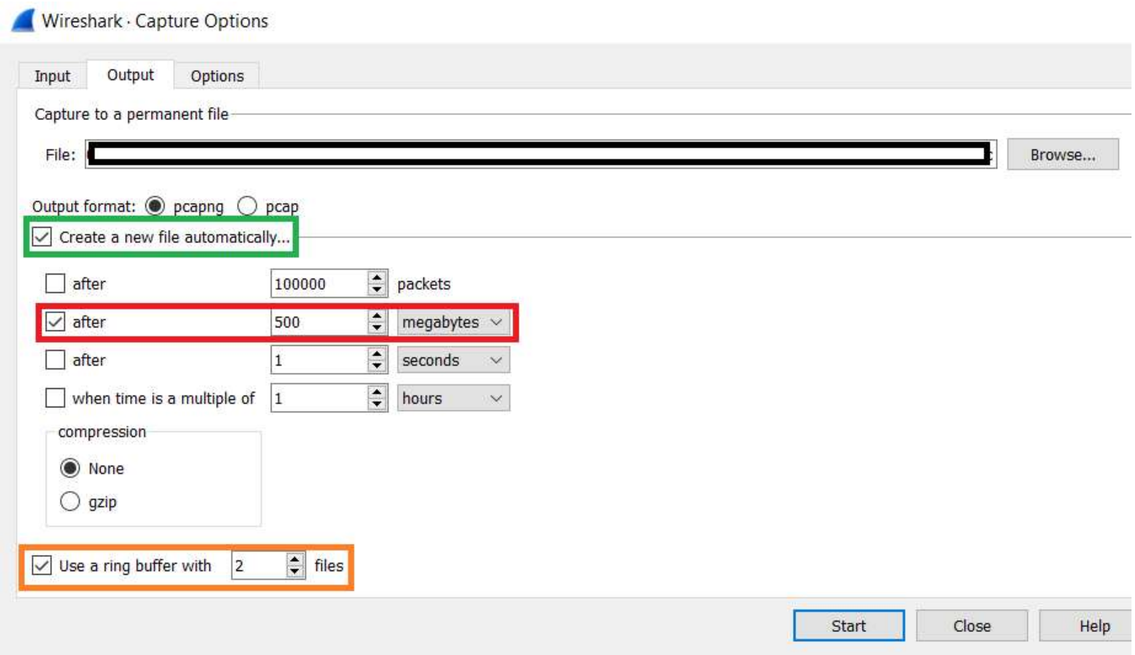
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 2 – Capture Options (Input)

As a practice, navigate to manage interfaces in the Wireshark capture options and check only the ones that you would use.

- Snaplength – It captures only a certain amount of data per frame instead of the entire payload, say the first 64 bytes of the frame, which includes most of the information that one needs such as the Ethernet part of the frame, the IP packet information, IP & TCP headers. One needs to be careful with that since there are possibilities of under-capturing certain data.
- Buffer – 2 megabytes of kernel buffer for a capture process. This is usually enough unless working in a high throughput environment.
- Enable promiscuous mode on all interfaces – It allows Wireshark to capture traffic not just to and from itself but also to other machines that are unicasting traffic among each other.



Wireshark · Capture Options

Input | Output | Options

Capture to a permanent file

File: [redacted] Browse...

Output format: ● pcapng ○ pcap

☑ Create a new file automatically...

□ after 100000 packets

☑ after 500 megabytes

□ after 1 seconds

□ when time is a multiple of 1 hours

compression

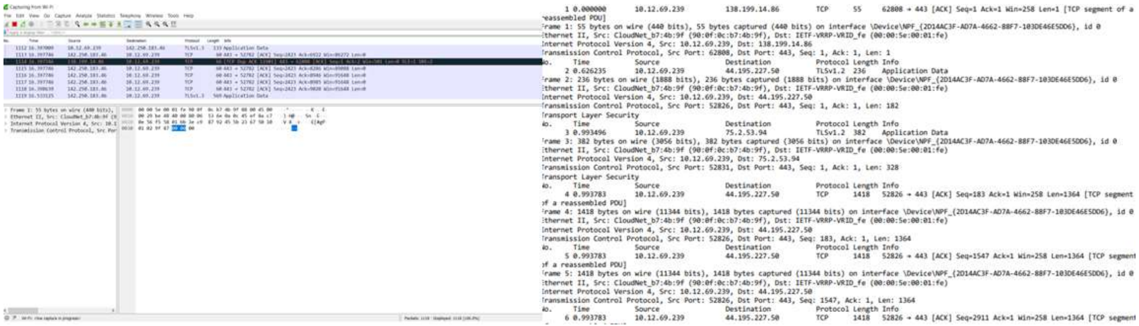
● None

○ gzip

☑ Use a ring buffer with 2 files

Figure 3 – Capture Options (Output)

Configure the place for Wireshark to save and configure some other settings that make Wireshark traffic easier to read. Two files will be overwritten continuously with 500 megabytes of data.



```
      1 0.000000       10.12.69.239          138.199.14.86         TCP      55     62808 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a
eassembled PDU]
rame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2D14AC3F-AD7A-4662-88F7-103DE46E5DD6}, id 0
thernet II, Src: CloudNet_b7:4b:9f (90:0f:0c:b7:4b:9f), Dst: IETF-VRRP-VRID_fe (00:00:5e:00:01:fe)
nternet Protocol Version 4, Src: 10.12.69.239, Dst: 138.199.14.86
ransmission Control Protocol, Src Port: 62808, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
o.     Time           Source                Destination           Protocol Length Info
      2 0.626235       10.12.69.239          44.195.227.50         TLSv1.2  236    Application Data
rame 2: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits) on interface \Device\NPF_{2D14AC3F-AD7A-4662-88F7-103DE46E5DD6}, id 0
thernet II, Src: CloudNet_b7:4b:9f (90:0f:0c:b7:4b:9f), Dst: IETF-VRRP-VRID_fe (00:00:5e:00:01:fe)
nternet Protocol Version 4, Src: 10.12.69.239, Dst: 44.195.227.50
ransmission Control Protocol, Src Port: 52826, Dst Port: 443, Seq: 1, Ack: 1, Len: 182
ransport Layer Security
o.     Time           Source                Destination           Protocol Length Info
      3 0.993496       10.12.69.239          75.2.53.94            TLSv1.2  382    Application Data
rame 3: 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits) on interface \Device\NPF_{2D14AC3F-AD7A-4662-88F7-103DE46E5DD6}, id 0
thernet II, Src: CloudNet_b7:4b:9f (90:0f:0c:b7:4b:9f), Dst: IETF-VRRP-VRID_fe (00:00:5e:00:01:fe)
nternet Protocol Version 4, Src: 10.12.69.239, Dst: 75.2.53.94
ransmission Control Protocol, Src Port: 52831, Dst Port: 443, Seq: 1, Ack: 1, Len: 328
ransport Layer Security
o.     Time           Source                Destination           Protocol Length Info
      4 0.993783       10.12.69.239          44.195.227.50         TCP      1418   52826 → 443 [ACK] Seq=183 Ack=1 Win=258 Len=1364 [TCP segment
f a reassembled PDU]
rame 4: 1418 bytes on wire (11344 bits), 1418 bytes captured (11344 bits) on interface \Device\NPF_{2D14AC3F-AD7A-4662-88F7-103DE46E5DD6}, id 0
thernet II, Src: CloudNet_b7:4b:9f (90:0f:0c:b7:4b:9f), Dst: IETF-VRRP-VRID_fe (00:00:5e:00:01:fe)
nternet Protocol Version 4, Src: 10.12.69.239, Dst: 44.195.227.50
ransmission Control Protocol, Src Port: 52826, Dst Port: 443, Seq: 183, Ack: 1, Len: 1364
o.     Time           Source                Destination           Protocol Length Info
      5 0.993783       10.12.69.239          44.195.227.50         TCP      1418   52826 → 443 [ACK] Seq=1547 Ack=1 Win=258 Len=1364 [TCP segment
f a reassembled PDU]
rame 5: 1418 bytes on wire (11344 bits), 1418 bytes captured (11344 bits) on interface \Device\NPF_{2D14AC3F-AD7A-4662-88F7-103DE46E5DD6}, id 0
thernet II, Src: CloudNet_b7:4b:9f (90:0f:0c:b7:4b:9f), Dst: IETF-VRRP-VRID_fe (00:00:5e:00:01:fe)
nternet Protocol Version 4, Src: 10.12.69.239, Dst: 44.195.227.50
ransmission Control Protocol, Src Port: 52826, Dst Port: 443, Seq: 1547, Ack: 1, Len: 1364
o.     Time           Source                Destination           Protocol Length Info
      6 0.993783       10.12.69.239          44.195.227.50         TCP      1418   52826 → 443 [ACK] Seq=2911 Ack=1 Win=258 Len=1364 [TCP segment
```

Figure 4 – Capturing from Wi-Fi

(ii) Capturing & Analysing 802.11 Wireless Networks

I. 802.11

- Institute of Electrical and Electronics Engineers' Standard for Wireless LAN communications.
- Standard is to define one medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity for fixed, portable, and moving stations (STAs) within a local area.

- Also offers regulatory bodies a means of standardizing access to one or more frequency bands for local area communication. Details the OSI Model's Layer 1 and Layer 2 protocols to be used for Wireless LAN.
- Uses radio waves as a physical layer and frames as a data link layer.

II. 802.11 Radio Wave Frequency Bands

- Several types of Wi-Fi standards exist - 802.11b, 802.11g, 802.11n, 802.11ah, etc. All standard occurs in the 2.4 GHz and 5 GHz frequency bands.
- The frequency band is divided into channels of equal bandwidth. To avoid interference, Wi-Fi devices can be configured to use different channels.
- Each standard uses different types of frequency modulation techniques.

III. 802.11 Frames

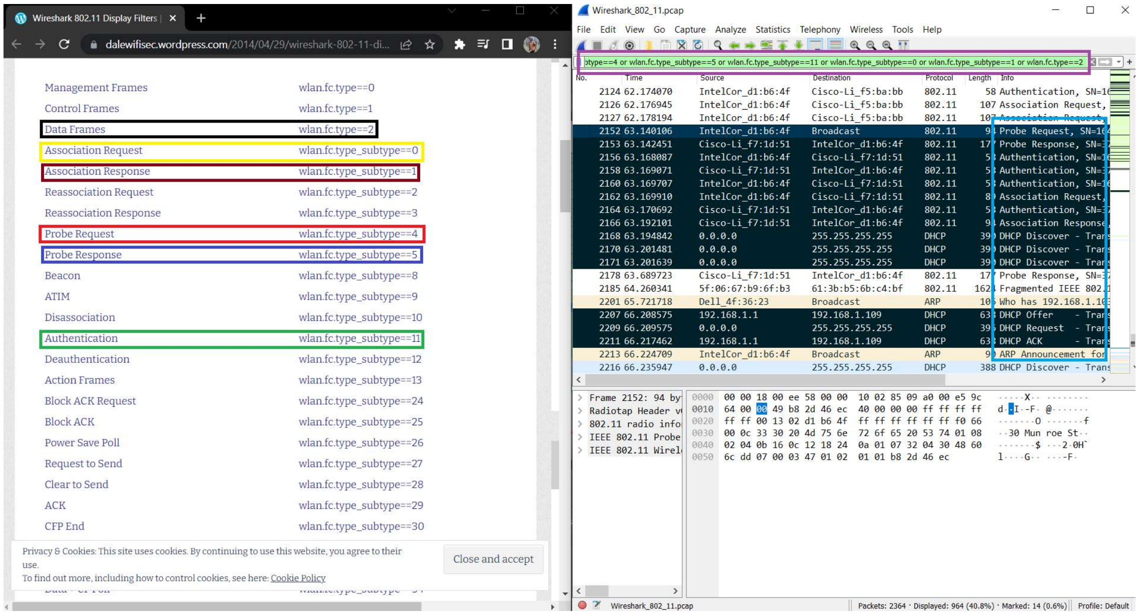
- Management Frames – Used for authentication, start, tearing-down and maintenance of Wi-Fi communications.
- Control Frames – Used to ease the flow of traffic. For example, signal if the medium is clear to send/receive data frames or acknowledge the receipt of error-free data frames.
- Data Frames – Encapsulate the actual data packets that need to be transmitted.

IV. 802.11 Regulations

- All Wi-Fi devices need to meet legal regulations about transmitter power, channels and interference. The is defined as a regdomain by IEEE. Each country or region (EU) can have its own set of regulations.

V. 802.11 Association Process

- The three 802.11 connection states are –
  - Not authenticated or associated.
  - Authenticated but not yet associated.
  - Authenticated and associated.
- A mobile station must be in the authenticated or associated state before data transmission can occur.



Wireshark 802.11 Display Filters |
dalewifisec.wordpress.com/2014/04/29/wireshark-802-11-di...
Close and accept
Wireshark_802_11.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Management Frames	wlan.fc.type==0
Control Frames	wlan.fc.type==1
Data Frames	wlan.fc.type==2
Association Request	wlan.fc.type_subtype==0
Association Response	wlan.fc.type_subtype==1
Reassociation Request	wlan.fc.type_subtype==2
Reassociation Response	wlan.fc.type_subtype==3
Probe Request	wlan.fc.type_subtype==4
Probe Response	wlan.fc.type_subtype==5
Beacon	wlan.fc.type_subtype==8
ATIM	wlan.fc.type_subtype==9
Disassociation	wlan.fc.type_subtype==10
Authentication	wlan.fc.type_subtype==11
Deauthentication	wlan.fc.type_subtype==12
Action Frames	wlan.fc.type_subtype==13
Block ACK Request	wlan.fc.type_subtype==24
Block ACK	wlan.fc.type_subtype==25
Power Save Poll	wlan.fc.type_subtype==26
Request to Send	wlan.fc.type_subtype==27
Clear to Send	wlan.fc.type_subtype==28
ACK	wlan.fc.type_subtype==29
CFP End	wlan.fc.type_subtype==30

Privacy & Cookies: This site uses cookies. By continuing to use this website, you agree to their use.
To find out more, including how to control cookies, see here: Cookie Policy

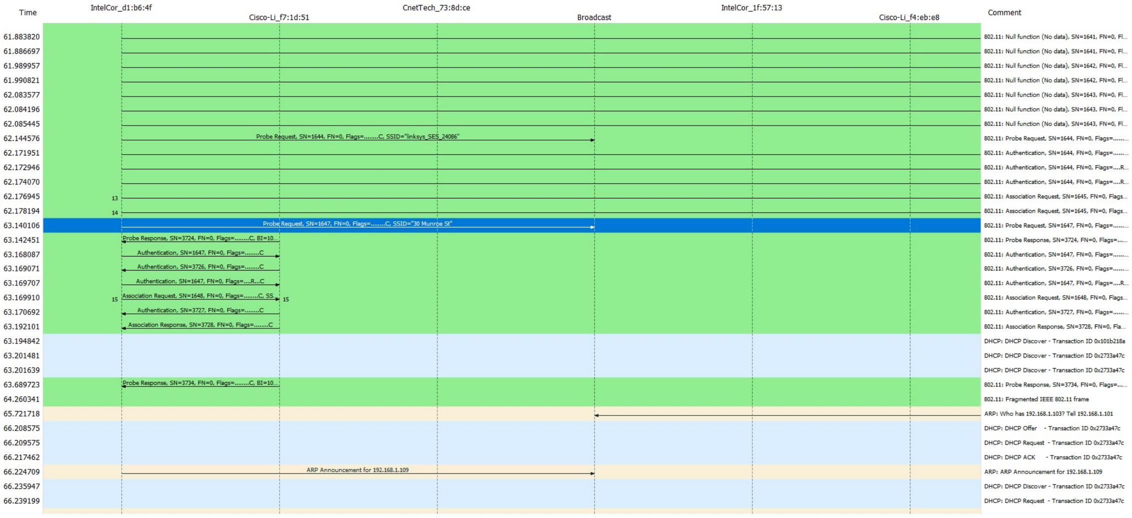
```
btype==4 or wlan.fc.type_subtype==5 or wlan.fc.type_subtype==11 or wlan.fc.type_subtype==0 or wlan.fc.type_subtype==1 or wlan.fc.type==2
```

```
No.    Time       Source              Destination         Protocol  Length Info
  2124 62.174070  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb   802.11      58 Authentication, SN=1
  2126 62.176945  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb   802.11     107 Association Request,
  2127 62.178194  IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb   802.11     107 Association Request,
  2152 63.140106  IntelCor_d1:b6:4f   Broadcast           802.11      94 Probe Request, SN=16
  2153 63.142451  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11     177 Probe Response, SN=3
  2156 63.168087  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51   802.11      58 Authentication, SN=1
  2158 63.169071  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11      58 Authentication, SN=3
  2160 63.169707  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51   802.11      58 Authentication, SN=1
  2162 63.169910  IntelCor_d1:b6:4f   Cisco-Li_f7:1d:51   802.11      8  Association Request,
  2164 63.170692  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11      58 Authentication, SN=3
  2166 63.192101  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11      9  Association Response
  2168 63.194842  0.0.0.0             255.255.255.255     DHCP       39  DHCP Discover - Tran
  2170 63.201481  0.0.0.0             255.255.255.255     DHCP       39  DHCP Discover - Tran
  2171 63.201639  0.0.0.0             255.255.255.255     DHCP       39  DHCP Discover - Tran
  2178 63.689723  Cisco-Li_f7:1d:51   IntelCor_d1:b6:4f   802.11     177 Probe Response, SN=3
  2185 64.260341  5f:06:67:b9:6f:b3   61:3b:b5:6b:c4:bf   802.11    162  Fragmented IEEE 802.1
  2201 65.721718  Dell_4f:36:23       Broadcast           ARP        10  Who has 192.168.1.10
  2207 66.208575  192.168.1.1         192.168.1.109       DHCP       63  DHCP Offer    - Tran
  2209 66.209575  0.0.0.0             255.255.255.255     DHCP       39  DHCP Request  - Tran
  2211 66.217462  192.168.1.1         192.168.1.109       DHCP       63  DHCP ACK      - Tran
  2213 66.224709  IntelCor_d1:b6:4f   Broadcast           ARP         9  ARP Announcement for
  2216 66.235947  0.0.0.0             255.255.255.255     DHCP      388 DHCP Discover - Trans
```

```
> Frame 2152: 94 by      0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e5 9c   ·····X·· ········
> Radiotap Header v      0010  64 00 00 49 b8 2d 46 ec  40 00 00 00 ff ff ff ff   d··I·-F· @·······
> 802.11 radio info      0020  ff ff 00 13 02 d1 b6 4f  ff ff ff ff ff ff f0 66   ·······O ·······f
> IEEE 802.11 Probe      0030  00 0c 33 30 20 4d 75 6e  72 6f 65 20 53 74 01 08   ··30 Mun roe St··
> IEEE 802.11 Wirel      0040  02 04 0b 16 0c 12 18 24  0a 01 07 32 04 30 48 60   ·······$ ···2·0H`
                         0050  6c dd 07 00 03 47 01 02  01 01 b8 2d 46 ec         l····G·· ···-F·
```

Wireshark_802_11.pcap | Packets: 2364 · Displayed: 964 (40.8%) · Marked: 14 (0.6%) | Profile: Default

Figure 5 – Sort Packet Captures

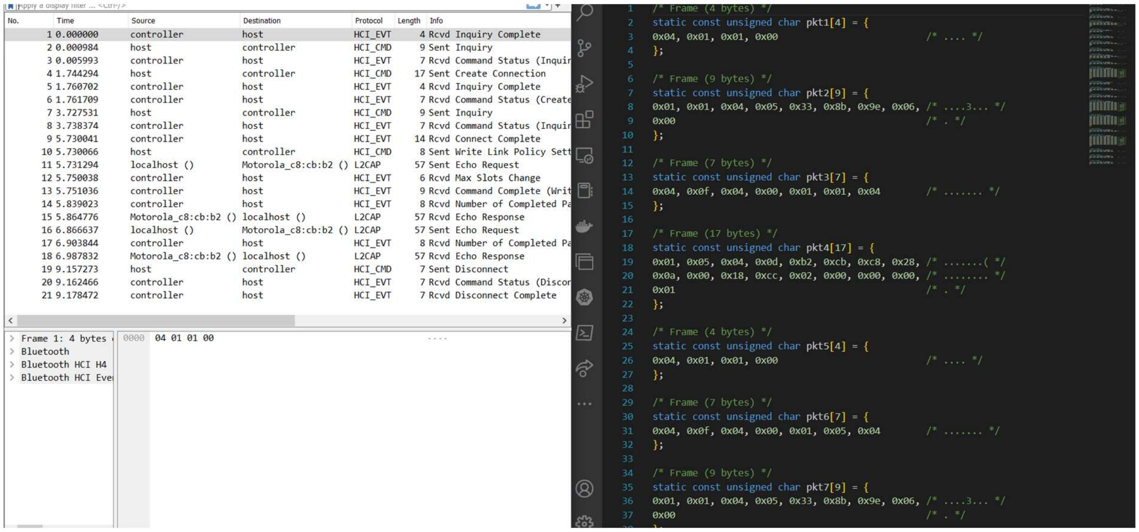


IntelCor_d1:b6:4f
Cisco-Li_f7:1d:51
CnetTech_73:8d:ce
Broadcast
IntelCor_1f:57:13
Cisco-Li_f4:eb:e8
Probe Request, SN=1644, FN=0, Flags=........C, SSID="linksys_SES_24086"
13
14
Probe Request, SN=1647, FN=0, Flags=........C, SSID="30 Munroe St"
Probe Response, SN=3724, FN=0, Flags=........C, BI=10...
Authentication, SN=1647, FN=0, Flags=........C
Authentication, SN=3726, FN=0, Flags=........C
Authentication, SN=1647, FN=0, Flags=....R...C
15
Association Request, SN=1648, FN=0, Flags=........C, SS...
15
Authentication, SN=3727, FN=0, Flags=........C
Association Response, SN=3728, FN=0, Flags=........C
Probe Response, SN=3734, FN=0, Flags=........C, BI=10...
ARP Announcement for 192.168.1.109

Time	Comment
61.883820	802.11: Null function (No data), SN=1641, FN=0, Fl...
61.886697	802.11: Null function (No data), SN=1641, FN=0, Fl...
61.989957	802.11: Null function (No data), SN=1642, FN=0, Fl...
61.990821	802.11: Null function (No data), SN=1642, FN=0, Fl...
62.083577	802.11: Null function (No data), SN=1643, FN=0, Fl...
62.084196	802.11: Null function (No data), SN=1643, FN=0, Fl...
62.085445	802.11: Null function (No data), SN=1643, FN=0, Fl...
62.144576	802.11: Probe Request, SN=1644, FN=0, Flags=........
62.171951	802.11: Authentication, SN=1644, FN=0, Flags=........
62.172946	802.11: Authentication, SN=1644, FN=0, Flags=....R...
62.174070	802.11: Authentication, SN=1644, FN=0, Flags=....R...
62.176945	802.11: Association Request, SN=1645, FN=0, Flags...
62.178194	802.11: Association Request, SN=1645, FN=0, Flags...
63.140106	802.11: Probe Request, SN=1647, FN=0, Flags=........
63.142451	802.11: Probe Response, SN=3724, FN=0, Flags=......
63.168087	802.11: Authentication, SN=1647, FN=0, Flags=........
63.169071	802.11: Authentication, SN=3726, FN=0, Flags=........
63.169707	802.11: Authentication, SN=1647, FN=0, Flags=....R...
63.169910	802.11: Association Request, SN=1648, FN=0, Flags...
63.170692	802.11: Authentication, SN=3727, FN=0, Flags=........
63.192101	802.11: Association Response, SN=3728, FN=0, Fla...
63.194842	DHCP: DHCP Discover - Transaction ID 0x101b218a
63.201481	DHCP: DHCP Discover - Transaction ID 0x2733a47c
63.201639	DHCP: DHCP Discover - Transaction ID 0x2733a47c
63.689723	802.11: Probe Response, SN=3734, FN=0, Flags=......
64.260341	802.11: Fragmented IEEE 802.11 frame
65.721718	ARP: Who has 192.168.1.103? Tell 192.168.1.101
66.208575	DHCP: DHCP Offer - Transaction ID 0x2733a47c
66.209575	DHCP: DHCP Request - Transaction ID 0x2733a47c
66.217462	DHCP: DHCP ACK - Transaction ID 0x2733a47c
66.224709	ARP: ARP Announcement for 192.168.1.109
66.235947	DHCP: DHCP Discover - Transaction ID 0x2733a47c
66.239199	DHCP: DHCP Request - Transaction ID 0x2733a47c

Figure 6 – Flow Graph Statistics

(iii) Capturing & Analysing Bluetooth Traffic

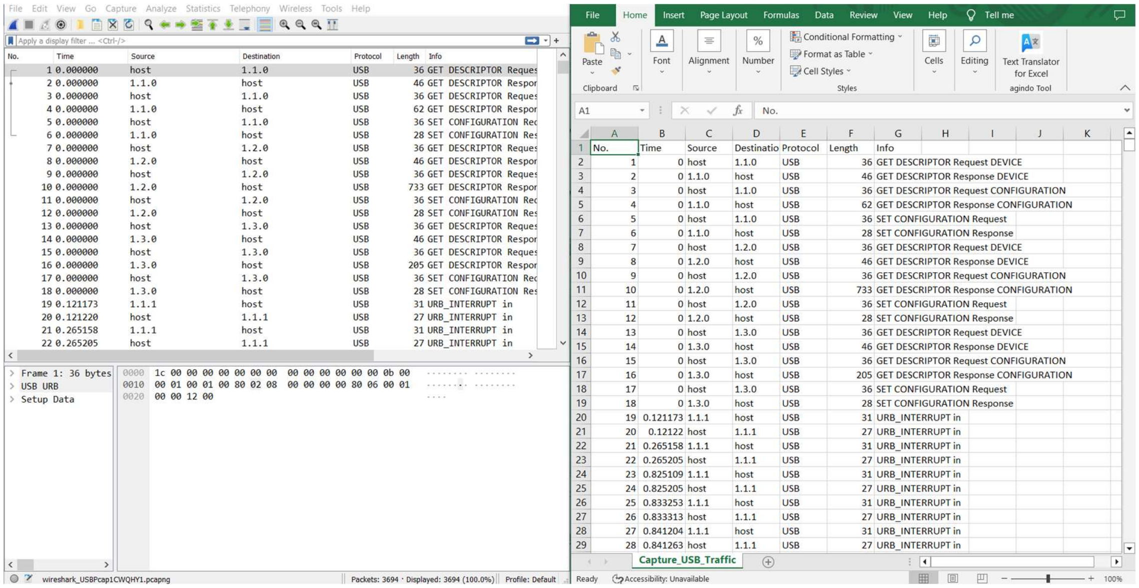


```
No.   Time      Source                 Destination            Protocol  Length Info
    1 0.000000  controller             host                   HCI_EVT     4 Rcvd Inquiry Complete
    2 0.000984  host                   controller             HCI_CMD     9 Sent Inquiry
    3 0.005993  controller             host                   HCI_EVT     7 Rcvd Command Status (Inquir
    4 1.744294  host                   controller             HCI_CMD    17 Sent Create Connection
    5 1.760702  controller             host                   HCI_EVT     4 Rcvd Inquiry Complete
    6 1.761709  controller             host                   HCI_EVT     7 Rcvd Command Status (Create
    7 3.727531  host                   controller             HCI_CMD     9 Sent Inquiry
    8 3.738374  controller             host                   HCI_EVT     7 Rcvd Command Status (Inquir
    9 5.730041  controller             host                   HCI_EVT    14 Rcvd Connect Complete
   10 5.730066  host                   controller             HCI_CMD     8 Sent Write Link Policy Sett
   11 5.731294  localhost ()           Motorola_c8:cb:b2 ()   L2CAP      57 Sent Echo Request
   12 5.750038  controller             host                   HCI_EVT     6 Rcvd Max Slots Change
   13 5.751036  controller             host                   HCI_EVT     9 Rcvd Command Complete (Writ
   14 5.839023  controller             host                   HCI_EVT     8 Rcvd Number of Completed Pa
   15 5.864776  Motorola_c8:cb:b2 ()   localhost ()           L2CAP      57 Rcvd Echo Response
   16 6.866637  localhost ()           Motorola_c8:cb:b2 ()   L2CAP      57 Sent Echo Request
   17 6.903844  controller             host                   HCI_EVT     8 Rcvd Number of Completed Pa
   18 6.987832  Motorola_c8:cb:b2 ()   localhost ()           L2CAP      57 Rcvd Echo Response
   19 9.157273  host                   controller             HCI_CMD     7 Sent Disconnect
   20 9.162466  controller             host                   HCI_EVT     7 Rcvd Command Status (Discor
   21 9.178472  controller             host                   HCI_EVT     7 Rcvd Disconnect Complete

> Frame 1: 4 bytes      0000  04 01 01 00                      ....
> Bluetooth
> Bluetooth HCI H4
> Bluetooth HCI Eve
```

```c
/* Frame (4 bytes) */
static const unsigned char pkt1[4] = {
0x04, 0x01, 0x01, 0x00                          /* .... */
};

/* Frame (9 bytes) */
static const unsigned char pkt2[9] = {
0x01, 0x01, 0x04, 0x05, 0x33, 0x8b, 0x9e, 0x06, /* ....3... */
0x00                                            /* . */
};

/* Frame (7 bytes) */
static const unsigned char pkt3[7] = {
0x04, 0x0f, 0x04, 0x00, 0x01, 0x01, 0x04        /* ....... */
};

/* Frame (17 bytes) */
static const unsigned char pkt4[17] = {
0x01, 0x05, 0x04, 0x0d, 0xb2, 0xcb, 0xc8, 0x28, /* .......( */
0x0a, 0x00, 0x18, 0xcc, 0x02, 0x00, 0x00, 0x00, /* ........ */
0x01                                            /* . */
};

/* Frame (4 bytes) */
static const unsigned char pkt5[4] = {
0x04, 0x01, 0x01, 0x00                          /* .... */
};

/* Frame (7 bytes) */
static const unsigned char pkt6[7] = {
0x04, 0x0f, 0x04, 0x00, 0x01, 0x05, 0x04        /* ....... */
};

/* Frame (9 bytes) */
static const unsigned char pkt7[9] = {
0x01, 0x01, 0x04, 0x05, 0x33, 0x8b, 0x9e, 0x06, /* ....3... */
0x00                                            /* . */
```

Figure 7 – Bluetooth Sample Capture File

(iv) Capturing & Analysing USB Traffic



```
No.   Time      Source   Destination  Protocol  Length Info
    1 0.000000  host     1.1.0        USB         36 GET DESCRIPTOR Reques
    2 0.000000  1.1.0    host         USB         46 GET DESCRIPTOR Respor
    3 0.000000  host     1.1.0        USB         36 GET DESCRIPTOR Reques
    4 0.000000  1.1.0    host         USB         62 GET DESCRIPTOR Respor
    5 0.000000  host     1.1.0        USB         36 SET CONFIGURATION Rec
    6 0.000000  1.1.0    host         USB         28 SET CONFIGURATION Res
    7 0.000000  host     1.2.0        USB         36 GET DESCRIPTOR Reques
    8 0.000000  1.2.0    host         USB         46 GET DESCRIPTOR Respor
    9 0.000000  host     1.2.0        USB         36 GET DESCRIPTOR Reques
   10 0.000000  1.2.0    host         USB        733 GET DESCRIPTOR Respor
   11 0.000000  host     1.2.0        USB         36 SET CONFIGURATION Rec
   12 0.000000  1.2.0    host         USB         28 SET CONFIGURATION Res
   13 0.000000  host     1.3.0        USB         36 GET DESCRIPTOR Reques
   14 0.000000  1.3.0    host         USB         46 GET DESCRIPTOR Respor
   15 0.000000  host     1.3.0        USB         36 GET DESCRIPTOR Reques
   16 0.000000  1.3.0    host         USB        205 GET DESCRIPTOR Respor
   17 0.000000  host     1.3.0        USB         36 SET CONFIGURATION Rec
   18 0.000000  1.3.0    host         USB         28 SET CONFIGURATION Res
   19 0.121173  1.1.1    host         USB         31 URB_INTERRUPT in
   20 0.121220  host     1.1.1        USB         27 URB_INTERRUPT in
   21 0.265158  1.1.1    host         USB         31 URB_INTERRUPT in
   22 0.265205  host     1.1.1        USB         27 URB_INTERRUPT in

> Frame 1: 36 bytes   0000  1c 00 00 00 00 00 00 00  00 00 00 00 00 00 0b 00   ........ ........
> USB URB             0010  00 01 00 01 00 80 02 08  00 00 00 00 80 06 00 01   ........ ........
> Setup Data          0020  00 00 12 00                                        ....

wireshark_USBPcap1CWQHY1.pcapng    Packets: 3694 · Displayed: 3694 (100.0%)    Profile: Default
```

A1 | No.

	A	B	C	D	E	F	G	H	I	J	K
1	No.	Time	Source	Destinatio	Protocol	Length	Info				
2	1	0	host	1.1.0	USB	36	GET DESCRIPTOR Request DEVICE				
3	2	0	1.1.0	host	USB	46	GET DESCRIPTOR Response DEVICE				
4	3	0	host	1.1.0	USB	36	GET DESCRIPTOR Request CONFIGURATION				
5	4	0	1.1.0	host	USB	62	GET DESCRIPTOR Response CONFIGURATION				
6	5	0	host	1.1.0	USB	36	SET CONFIGURATION Request				
7	6	0	1.1.0	host	USB	28	SET CONFIGURATION Response				
8	7	0	host	1.2.0	USB	36	GET DESCRIPTOR Request DEVICE				
9	8	0	1.2.0	host	USB	46	GET DESCRIPTOR Response DEVICE				
10	9	0	host	1.2.0	USB	36	GET DESCRIPTOR Request CONFIGURATION				
11	10	0	1.2.0	host	USB	733	GET DESCRIPTOR Response CONFIGURATION				
12	11	0	host	1.2.0	USB	36	SET CONFIGURATION Request				
13	12	0	1.2.0	host	USB	28	SET CONFIGURATION Response				
14	13	0	host	1.3.0	USB	36	GET DESCRIPTOR Request DEVICE				
15	14	0	1.3.0	host	USB	46	GET DESCRIPTOR Response DEVICE				
16	15	0	host	1.3.0	USB	36	GET DESCRIPTOR Request CONFIGURATION				
17	16	0	1.3.0	host	USB	205	GET DESCRIPTOR Response CONFIGURATION				
18	17	0	host	1.3.0	USB	36	SET CONFIGURATION Request				
19	18	0	1.3.0	host	USB	28	SET CONFIGURATION Response				
20	19	0.121173	1.1.1	host	USB	31	URB_INTERRUPT in				
21	20	0.12122	host	1.1.1	USB	27	URB_INTERRUPT in				
22	21	0.265158	1.1.1	host	USB	31	URB_INTERRUPT in				
23	22	0.265205	host	1.1.1	USB	27	URB_INTERRUPT in				
24	23	0.825109	1.1.1	host	USB	31	URB_INTERRUPT in				
25	24	0.825205	host	1.1.1	USB	27	URB_INTERRUPT in				
26	25	0.833253	1.1.1	host	USB	31	URB_INTERRUPT in				
27	26	0.833313	host	1.1.1	USB	27	URB_INTERRUPT in				
28	27	0.841204	1.1.1	host	USB	31	URB_INTERRUPT in				
29	28	0.841263	host	1.1.1	USB	27	URB_INTERRUPT in				

Capture_USB_Traffic

Figure 8 – Capture USB Traffic

RESULT

Thus, monitored network health using the Wireshark packet sniffer. All the simulation results were verified successfully.

REFERENCES

1. Wireshark Lab: 802.11 Wi-Fi v8.0, Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross – http://www-net.cs.umass.edu/wireshark-labs/Wireshark_802.11_v8.0.pdf
2. "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012), vol., no., pp.1-3534, 14 Dec. 2016, DOI: 10.1109/IEEESTD.2016.7786995.
3. Understanding the IEEE 802.11 Standard for Wireless Networks – https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-80211.html
4. Wireshark 802.11 Display Filters – https://dalewifisec.wordpress.com/2014/04/29/wireshark-802-11-display-filters-2/
5. Bluetooth Wireshark Wiki – https://wiki.wireshark.org/Bluetooth
6. How to perform network traffic capture with Wireshark – https://www.youtube.com/watch?v=nWvscuxqais&t=306s&ab_channel=ChrisGreer
7. 802.11 Wireless Packet Capture – https://www.youtube.com/watch?v=3wKyUnFN7k8&ab_channel=AtishApajee
8. Capture USB Traffic with Wireshark – https://www.youtube.com/watch?v=Nix-QZ0gkOc&ab_channel=InformationSecurityNewspaper

CONTRIBUTION – TEAM 9

Name	Roll Number	Work Done – Wireshark & Corresponding Documentation
B Ambareesh	CB.EN.U4CCE20006	Capturing & Analysing 802.11 Bluetooth and USB Traffic
Narendran S	CB.EN.U4CCE20036	Capturing & Analysing Ethernet Networks
Narun T	CB.EN.U4CCE20037	
Pabbathi Greeshma	CB.EN.U4CCE20040	Capturing & Analysing 802.11 Wireless Networks
Santosh	CB.EN.U4CCE20053	

Postscript – B Ambareesh (CB.EN.U4CCE20006) gathered study materials and resources about Wireshark apart from the ones mentioned under references, i.e., the basic groundwork.