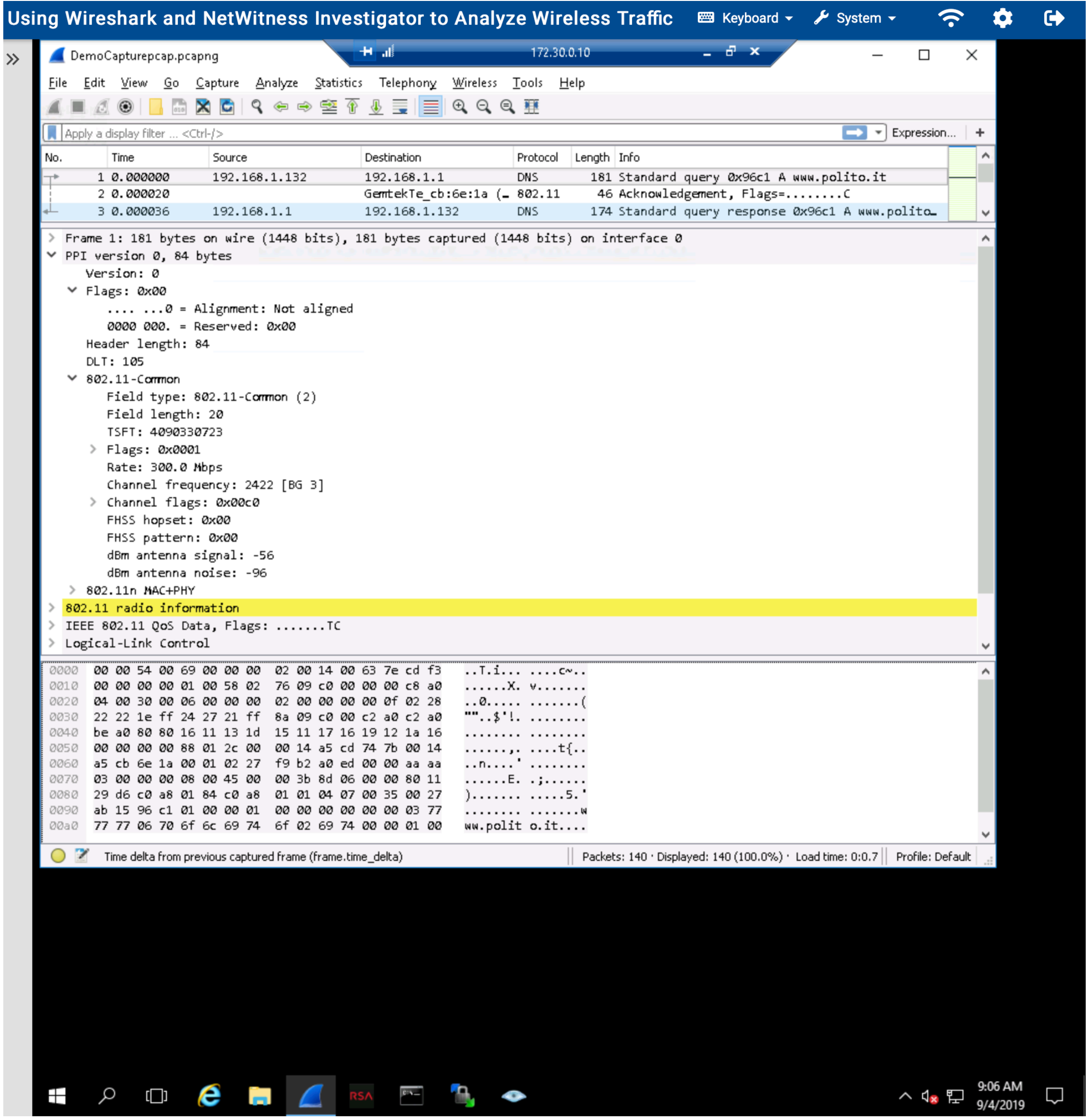
Lab #3: Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

Part 1: Analyze Wireless Traffic with Wireshark

Step #10



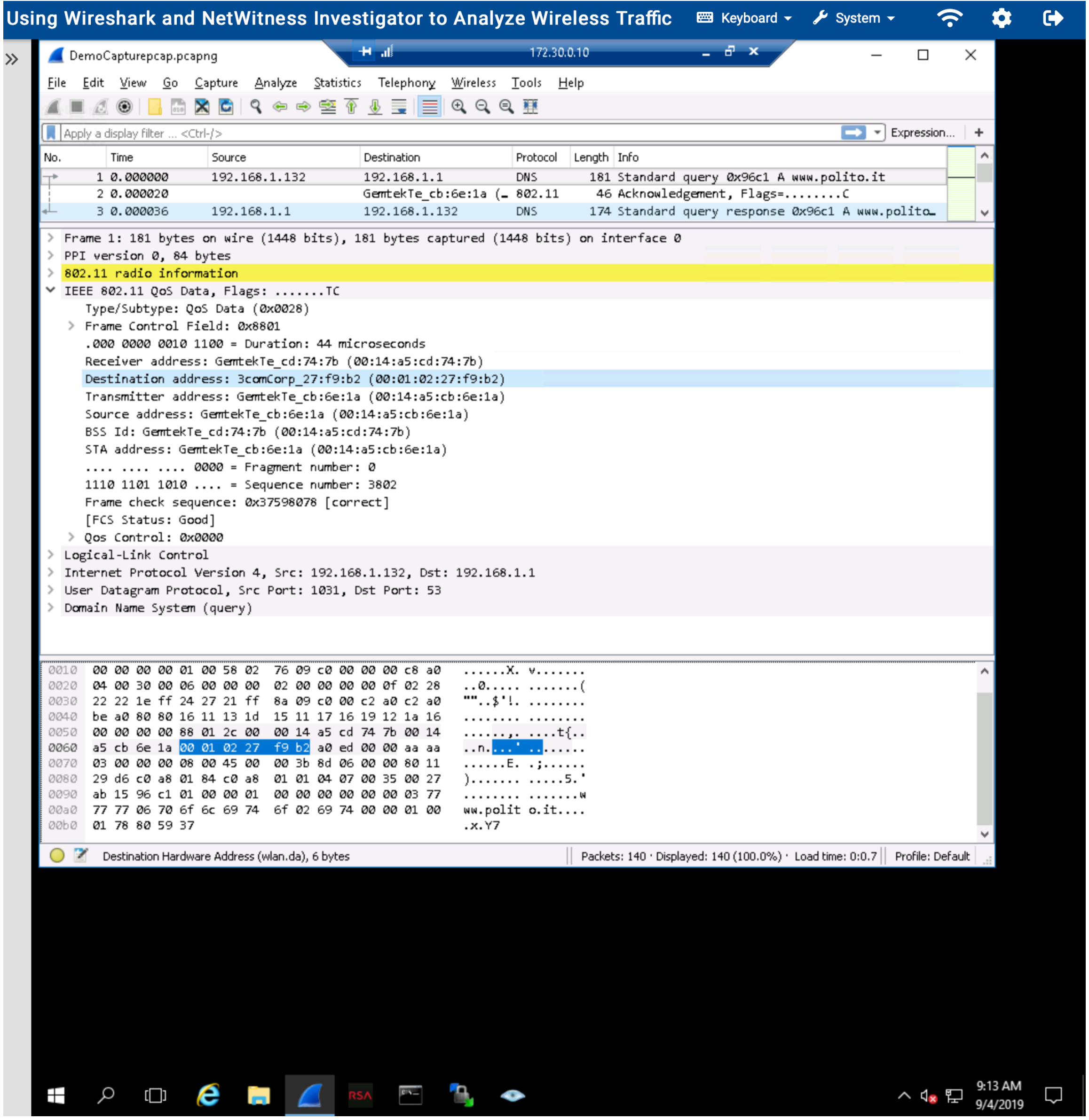
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.132	192.168.1.1	DNS	181	Standard query 0x96c1 A www.polito.it
2	0.000020		GemtekTe_cb:6e:1a (…	802.11	46	Acknowledgement, Flags=........C
3	0.000036	192.168.1.1	192.168.1.132	DNS	174	Standard query response 0x96c1 A www.polito…

```
> Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
v PPI version 0, 84 bytes
     Version: 0
   v Flags: 0x00
        .... ...0 = Alignment: Not aligned
        0000 000. = Reserved: 0x00
     Header length: 84
     DLT: 105
   v 802.11-Common
        Field type: 802.11-Common (2)
        Field length: 20
        TSFT: 4090330723
      > Flags: 0x0001
        Rate: 300.0 Mbps
        Channel frequency: 2422 [BG 3]
      > Channel flags: 0x00c0
        FHSS hopset: 0x00
        FHSS pattern: 0x00
        dBm antenna signal: -56
        dBm antenna noise: -96
   > 802.11n MAC+PHY
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
```

```
0000  00 00 54 00 69 00 00 00  02 00 14 00 63 7e cd f3   ..T.i... ....c~..
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
```

Time delta from previous captured frame (frame.time_delta) | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.7 | Profile: Default

Step #12


Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
Keyboard
System
DemoCapturepcap.pcapng
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
9:13 AM
9/4/2019

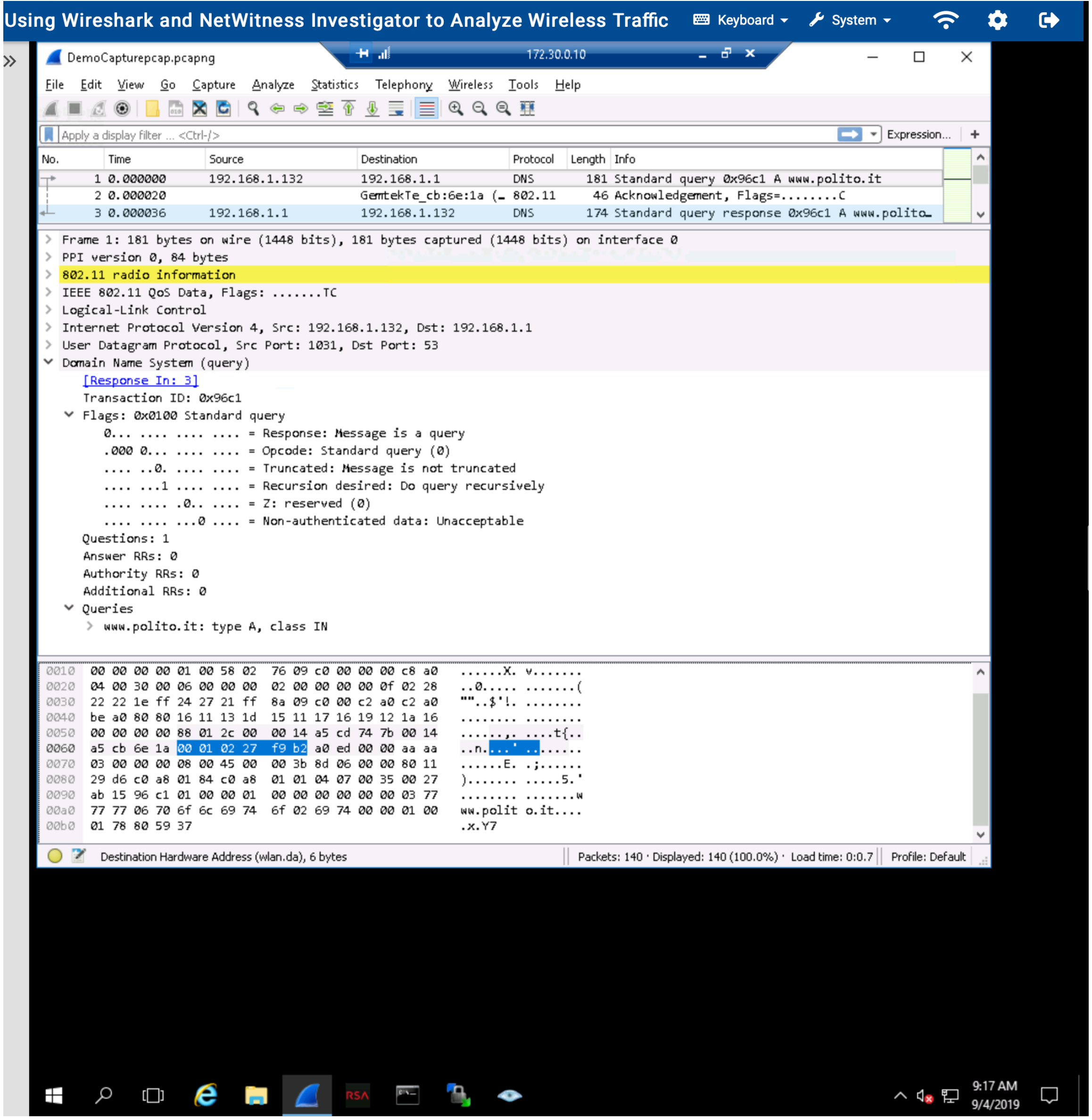
```
No.  Time       Source          Destination            Protocol  Length  Info
  1  0.000000   192.168.1.132   192.168.1.1            DNS          181  Standard query 0x96c1 A www.polito.it
  2  0.000020                   GemtekTe_cb:6e:1a (…   802.11        46  Acknowledgement, Flags=........C
  3  0.000036   192.168.1.1     192.168.1.132          DNS          174  Standard query response 0x96c1 A www.polito…
```

```
> Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
> PPI version 0, 84 bytes
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    Destination address: 3comCorp_27:f9:b2 (00:01:02:27:f9:b2)
    Transmitter address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    Source address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    BSS Id: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    STA address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    .... .... .... 0000 = Fragment number: 0
    1110 1101 1010 .... = Sequence number: 3802
    Frame check sequence: 0x37598078 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.132, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 1031, Dst Port: 53
> Domain Name System (query)
```

```
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   "".$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                     .x.Y7
```

Destination Hardware Address (wlan.da), 6 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.7 | Profile: Default

Step #14



Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
Keyboard
System
DemoCapturepcap.pcapng
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
9:17 AM
9/4/2019

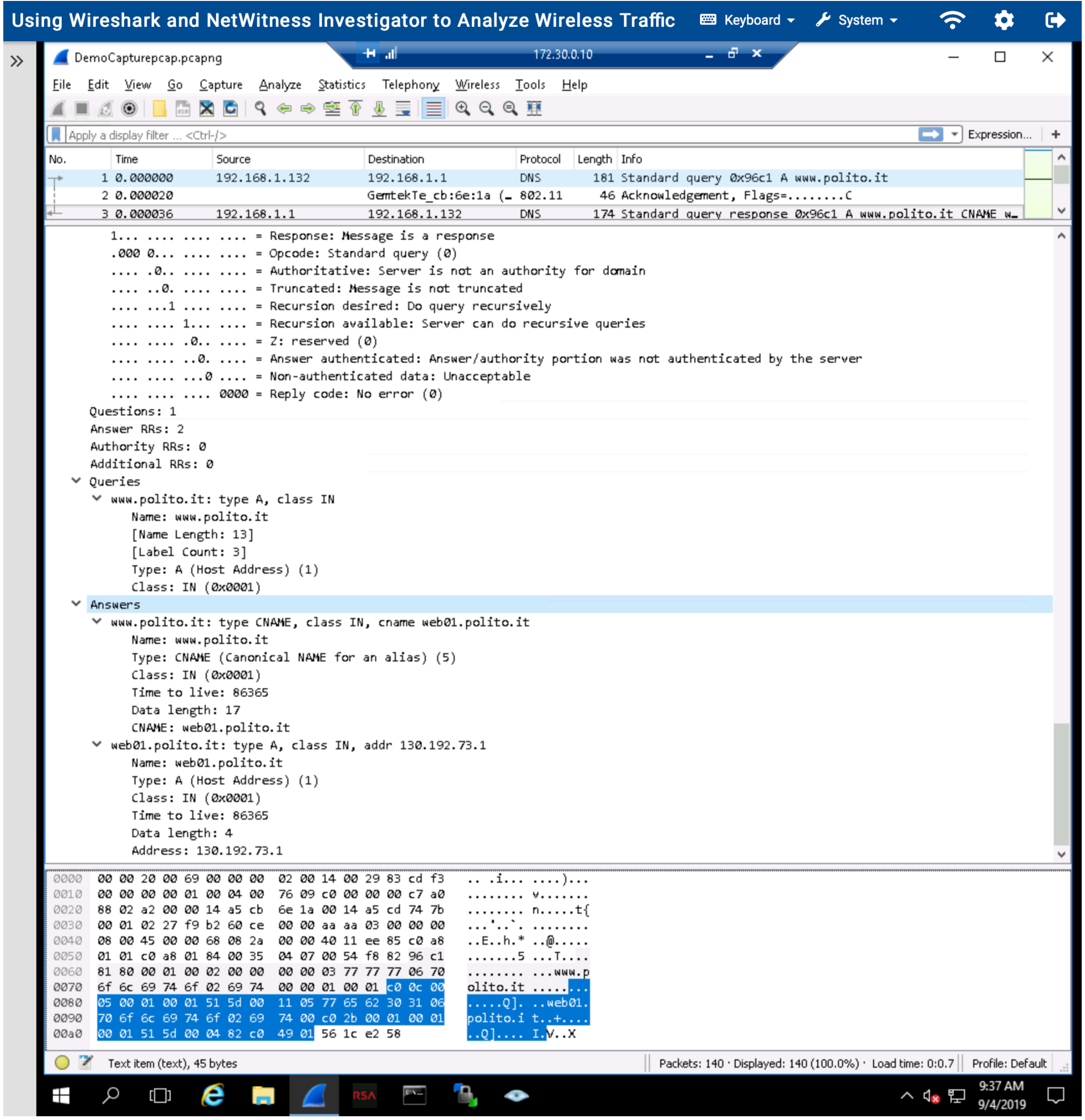
```
No.  Time      Source         Destination          Protocol Length Info
   1 0.000000  192.168.1.132  192.168.1.1          DNS         181 Standard query 0x96c1 A www.polito.it
   2 0.000020                 GemtekTe_cb:6e:1a (… 802.11       46 Acknowledgement, Flags=........C
   3 0.000036  192.168.1.1    192.168.1.132        DNS         174 Standard query response 0x96c1 A www.polito…
```

```
> Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
> PPI version 0, 84 bytes
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.132, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 1031, Dst Port: 53
v Domain Name System (query)
    [Response In: 3]
    Transaction ID: 0x96c1
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.polito.it: type A, class IN
```

```
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                     .x.Y7
```

Destination Hardware Address (wlan.da), 6 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.7 | Profile: Default

Step #20



Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
Keyboard
System
DemoCapturepcap.pcapng
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source          Destination         Protocol Length Info
   1 0.000000  192.168.1.132   192.168.1.1         DNS         181 Standard query 0x96c1 A www.polito.it
   2 0.000020                  GemtekTe_cb:6e:1a (… 802.11      46 Acknowledgement, Flags=........C
   3 0.000036  192.168.1.1     192.168.1.132       DNS         174 Standard query response 0x96c1 A www.polito.it CNAME w…
```

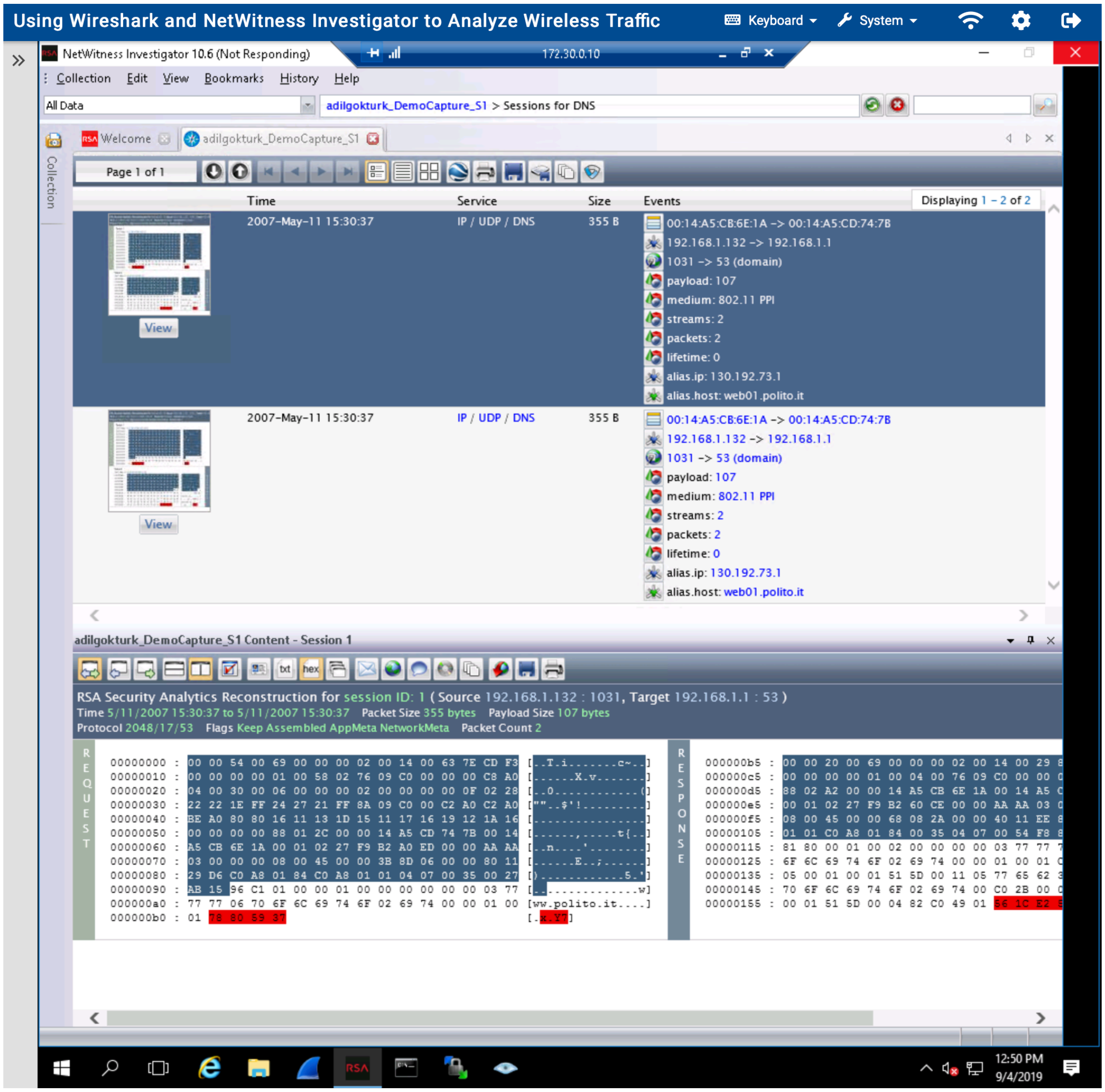
```
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 0
   ∨ Queries
     ∨ www.polito.it: type A, class IN
           Name: www.polito.it
           [Name Length: 13]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
   ∨ Answers
     ∨ www.polito.it: type CNAME, class IN, cname web01.polito.it
           Name: www.polito.it
           Type: CNAME (Canonical NAME for an alias) (5)
           Class: IN (0x0001)
           Time to live: 86365
           Data length: 17
           CNAME: web01.polito.it
     ∨ web01.polito.it: type A, class IN, addr 130.192.73.1
           Name: web01.polito.it
           Type: A (Host Address) (1)
           Class: IN (0x0001)
           Time to live: 86365
           Data length: 4
           Address: 130.192.73.1
```

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 29 83 cd f3   .. .i... ....)...
0010  00 00 00 00 01 00 04 00  76 09 c0 00 00 00 c7 a0   ........ v.......
0020  88 02 a2 00 00 14 a5 cb  6e 1a 00 14 a5 cd 74 7b   ........ n.....t{
0030  00 01 02 27 f9 b2 60 ce  00 00 aa aa 03 00 00 00   ...'..`. ........
0040  08 00 45 00 00 68 08 2a  00 00 40 11 ee 85 c0 a8   ..E..h.* ..@.....
0050  01 01 c0 a8 01 84 00 35  04 07 00 54 f8 82 96 c1   .......5 ...T....
0060  81 80 00 01 00 02 00 00  00 00 03 77 77 77 06 70   ........ ...www.p
0070  6f 6c 69 74 6f 02 69 74  00 00 01 00 01 c0 0c 00   olito.it ........
0080  05 00 01 00 01 51 5d 00  11 05 77 65 62 30 31 06   .....Q]. ..web01.
0090  70 6f 6c 69 74 6f 02 69  74 00 c0 2b 00 01 00 01   polito.i t..+....
00a0  00 01 51 5d 00 04 82 c0  49 01 56 1c e2 58         ..Q].... I.V..X
```

Text item (text), 45 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.7 | Profile: Default

Part 2: Compare with NetWitness Investigator

Step #10



Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

NetWitness Investigator 10.6 (Not Responding) — 172.30.0.10

All Data — adilgokturk_DemoCapture_S1 > Sessions for DNS

Page 1 of 1 — Displaying 1 – 2 of 2

Time	Service	Size	Events
2007–May–11 15:30:37	IP / UDP / DNS	355 B	00:14:A5:CB:6E:1A –> 00:14:A5:CD:74:7B 192.168.1.132 –> 192.168.1.1 1031 –> 53 (domain) payload: 107 medium: 802.11 PPI streams: 2 packets: 2 lifetime: 0 alias.ip: 130.192.73.1 alias.host: web01.polito.it
2007–May–11 15:30:37	IP / UDP / DNS	355 B	00:14:A5:CB:6E:1A –> 00:14:A5:CD:74:7B 192.168.1.132 –> 192.168.1.1 1031 –> 53 (domain) payload: 107 medium: 802.11 PPI streams: 2 packets: 2 lifetime: 0 alias.ip: 130.192.73.1 alias.host: web01.polito.it

adilgokturk_DemoCapture_S1 Content - Session 1

RSA Security Analytics Reconstruction for session ID: 1 (Source 192.168.1.132 : 1031, Target 192.168.1.1 : 53)
Time 5/11/2007 15:30:37 to 5/11/2007 15:30:37 Packet Size 355 bytes Payload Size 107 bytes
Protocol 2048/17/53 Flags Keep Assembled AppMeta NetworkMeta Packet Count 2

REQUEST

```
00000000 : 00 00 54 00 69 00 00 00 02 00 14 00 63 7E CD F3 [..T.i.......c~..]
00000010 : 00 00 00 00 01 00 58 02 76 09 C0 00 00 00 C8 A0 [......X.v.......]
00000020 : 04 00 30 00 06 00 00 00 02 00 00 00 00 0F 02 28 [..0............(]
00000030 : 22 22 1E FF 24 27 21 FF 8A 09 C0 00 C2 A0 C2 A0 [""..$'!.........]
00000040 : BE A0 80 80 16 11 13 1D 15 11 17 16 19 12 1A 16 [................]
00000050 : 00 00 00 00 88 01 2C 00 00 14 A5 CD 74 7B 00 14 [......,.....t{..]
00000060 : A5 CB 6E 1A 00 01 02 27 F9 B2 A0 ED 00 00 AA AA [..n....'........]
00000070 : 03 00 00 00 08 00 45 00 00 3B 8D 06 00 00 80 11 [......E..;......]
00000080 : 29 D6 C0 A8 01 84 C0 A8 01 01 04 07 00 35 00 27 [)............5.']
00000090 : AB 15 96 C1 01 00 00 01 00 00 00 00 00 00 03 77 [...............w]
000000a0 : 77 77 06 70 6F 6C 69 74 6F 02 69 74 00 00 01 00 [ww.polito.it....]
000000b0 : 01 78 80 59 37                                  [.x.Y7]
```

RESPONSE

```
000000b5 : 00 00 20 00 69 00 00 00 02 00 14 00 29 8
000000c5 : 00 00 00 00 01 00 04 00 76 09 C0 00 00 0
000000d5 : 88 02 A2 00 00 14 A5 CB 6E 1A 00 14 A5 C
000000e5 : 00 01 02 27 F9 B2 60 CE 00 00 AA AA 03 0
000000f5 : 08 00 45 00 00 68 08 2A 00 00 40 11 EE 8
00000105 : 01 01 C0 A8 01 84 00 35 04 07 00 54 F8 8
00000115 : 81 80 00 01 00 02 00 00 00 03 77 77 7
00000125 : 6F 6C 69 74 6F 02 69 74 00 00 01 00 01 C
00000135 : 05 00 01 00 01 51 5D 00 11 05 77 65 62 3
00000145 : 70 6F 6C 69 74 6F 02 69 74 00 C0 2B 00 0
00000155 : 00 01 51 5D 00 04 82 C0 49 01 56 1C E2 5
```

12:50 PM
9/4/2019

Step #11

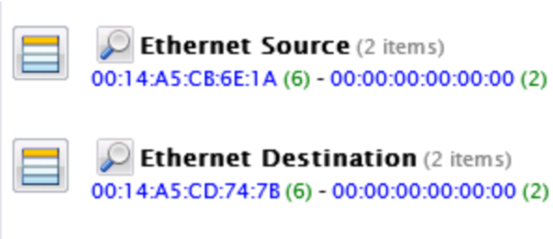
- In the Lab Report file, compare in 200 words the information provided by NetWitness to the screen capture you made with Wireshark (Part 1, Step#20).
  - It seems both NetWitness and Wireshark have similar function. Apparently, NetWitness seems more users friendly than Wireshark. Wireshark is a very good tool to analyze packets between two different networks that you're monitoring. I also found out that, it's especially powerful if you know how to identify network protocols such as TCP, DNS, and SFTP etc. Wireshark's filtering system seems extremely helpful.

- Another important difference between NetWitness and Wireshark is that Wireshark is available for free, it is often used for packet capture and for initial analysis. NetWitness Investigator, on the other hand, requires the purchase of a license for use, so only more senior often uses it, more skilled, and better-trained security analysts for specific types of analysis. Often, investigators, or even clients, with little training can capture needed information with the no-cost Wireshark while a more in-depth security-focused analysis is later done with NetWitness Investigator.

Step #13:
In the NetWitness Investigator window, use the scrollbar to locate the Ethernet Source and Ethernet Destination categories. Compare in 200 words the information you can get from these categories with the Frame Control information captured by Wireshark (See Figure 6 in Part 1).

Let's take a look at the screen shots first. Apparently, NetWitness clearly displays both Ethernet Source and Ethernet Destination categories as shown photo below.

NetWitness Screen

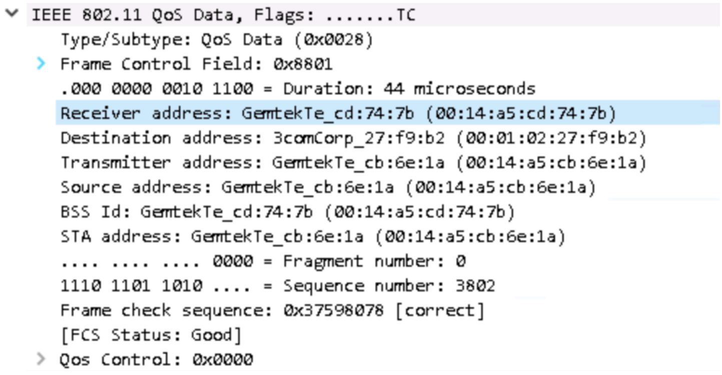


Ethernet Source (2 items)
00:14:A5:CB:6E:1A (6) - 00:00:00:00:00:00 (2)

Ethernet Destination (2 items)
00:14:A5:CD:74:7B (6) - 00:00:00:00:00:00 (2)

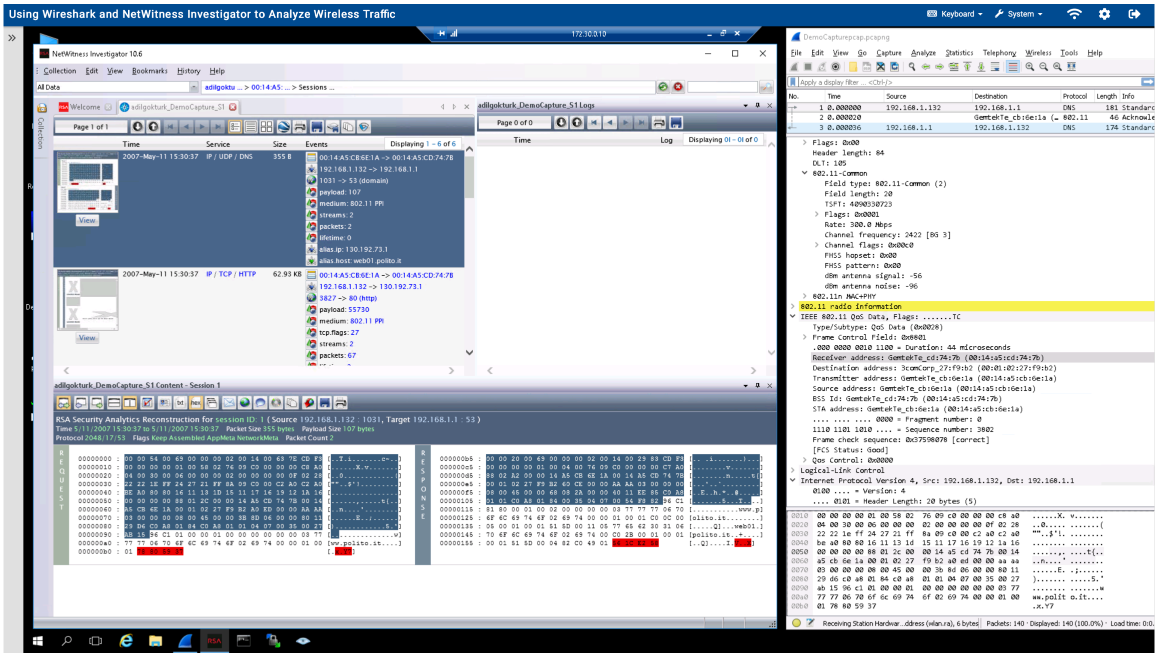
Wireshark also displays both Ethernet Source and Ethernet Destination categories as Receiver address and Transmitter address. But it is not clear as in NetWitness screen would. It needs a little bit more experience and users knowledge to see same information in a different way of depiction/display.

Wireshark Screen



```
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    Destination address: 3comCorp_27:f9:b2 (00:01:02:27:f9:b2)
    Transmitter address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    Source address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    BSS Id: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    STA address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    .... .... .... 0000 = Fragment number: 0
    1110 1101 1010 .... = Sequence number: 3802
    Frame check sequence: 0x37598078 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
```

As seen in the photo down below, NetWitness has a more users friendly, clear and more sophisticated visualization on both Ethernet Source and Ethernet Destination categories.


Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
Keyboard
System
NetWitness Investigator 10.6
Collection Edit View Bookmarks History Help
All Data
adilgoktu ... > 00:14:A5: ... > Sessions ...
Welcome
adilgokturk_DemoCapture_S1
Page 1 of 1
adilgokturk_DemoCapture_S1 Logs
Page 0 of 0
View
DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Time	Service	Size	Events
2007-May-11 15:30:37	IP / UDP / DNS	355 B	00:14:A5:CB:6E:1A -> 00:14:A5:CD:74:7B 192.168.1.132 -> 192.168.1.1 1031 -> 53 (domain) payload: 107 medium: 802.11 PPI streams: 2 packets: 2 lifetime: 0 alias.ip: 130.192.73.1 alias.host: web01.polito.it
2007-May-11 15:30:37	IP / TCP / HTTP	62.93 KB	00:14:A5:CB:6E:1A -> 00:14:A5:CD:74:7B 192.168.1.132 -> 130.192.73.1 3827 -> 80 (http) payload: 55730 medium: 802.11 PPI tcp.flags: 27 streams: 2 packets: 67

Displaying 1 – 6 of 6

adilgokturk_DemoCapture_S1 Content - Session 1

RSA Security Analytics Reconstruction for session ID: 1 (Source 192.168.1.132 : 1031, Target 192.168.1.1 : 53)
Time 5/11/2007 15:30:37 to 5/11/2007 15:30:37 Packet Size 355 bytes Payload Size 107 bytes
Protocol 2048/17/53 Flags Keep Assembled AppMeta NetworkMeta Packet Count 2

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.132	192.168.1.1	DNS	181	Standard
2	0.000020		GemtekTe_cb:6e:1a (…	802.11	46	Acknowle
3	0.000036	192.168.1.1	192.168.1.132	DNS	174	Standard

```
  > Flags: 0x00
    Header length: 84
    DLT: 105
  ˅ 802.11-Common
      Field type: 802.11-Common (2)
      Field length: 20
      TSFT: 4090330723
    > Flags: 0x0001
      Rate: 300.0 Mbps
      Channel frequency: 2422 [BG 3]
    > Channel flags: 0x00c0
      FHSS hopset: 0x00
      FHSS pattern: 0x00
      dBm antenna signal: -56
      dBm antenna noise: -96
  > 802.11n MAC+PHY
> 802.11 radio information
˅ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    Destination address: 3comCorp_27:f9:b2 (00:01:02:27:f9:b2)
    Transmitter address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    Source address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    BSS Id: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    STA address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    .... .... .... 0000 = Fragment number: 0
    1110 1101 1010 .... = Sequence number: 3802
    Frame check sequence: 0x37598078 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
> Logical-Link Control
˅ Internet Protocol Version 4, Src: 192.168.1.132, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

```
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   "".$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                      .x.Y7
```

Receiving Station Hardwar...ddress (wlan.ra), 6 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.

Part 3: Challenge Question

After research on the Wireshark tool, discuss its current limitation (in 200 words).

- Apparently the major difference between NetWitness and Wireshark is that Wireshark is available for free, it is often used for packet capture and for initial analysis. NetWitness Investigator, on the other hand, requires the purchase of a license for use, so only more senior often uses it, more skilled, and better-trained security analysts for specific types of analysis. Often, investigators, or even clients, with little training can capture needed information with the no-cost Wireshark while a more in-depth security-focused analysis is later done with NetWitness Investigator.
- As I mentioned before, it seems both NetWitness and Wireshark have similar functions. Apparently, NetWitness seems more users friendly than Wireshark.
- Another important point would be the preference of the program also depends on the research requirements. Sometimes, it could be more useful if we use both NetWitness and Wireshark to see a complex forensic investigation to see/show a complete picture.