Syracuse University

IST-623 Lab#3

Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

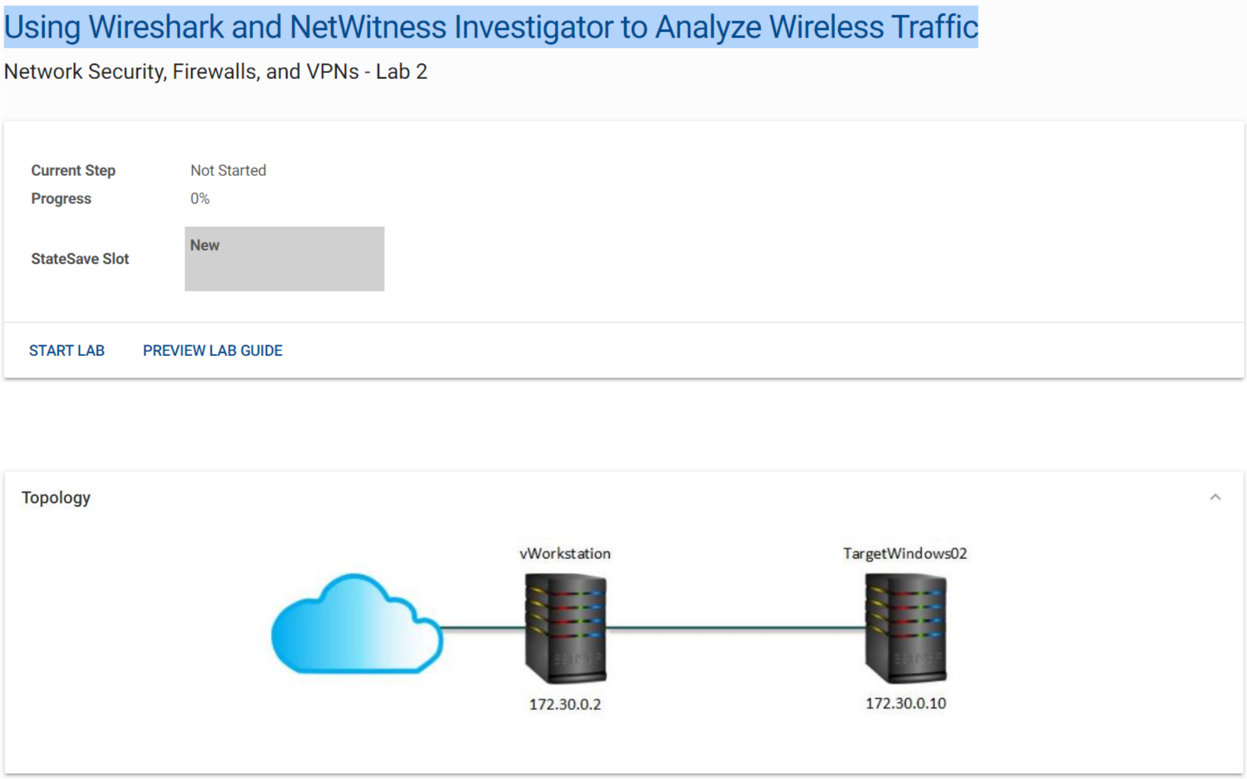
ThulasiRam RuppaKrishnan

IST 623

Professor Joon Park

Contents

Lab Environment

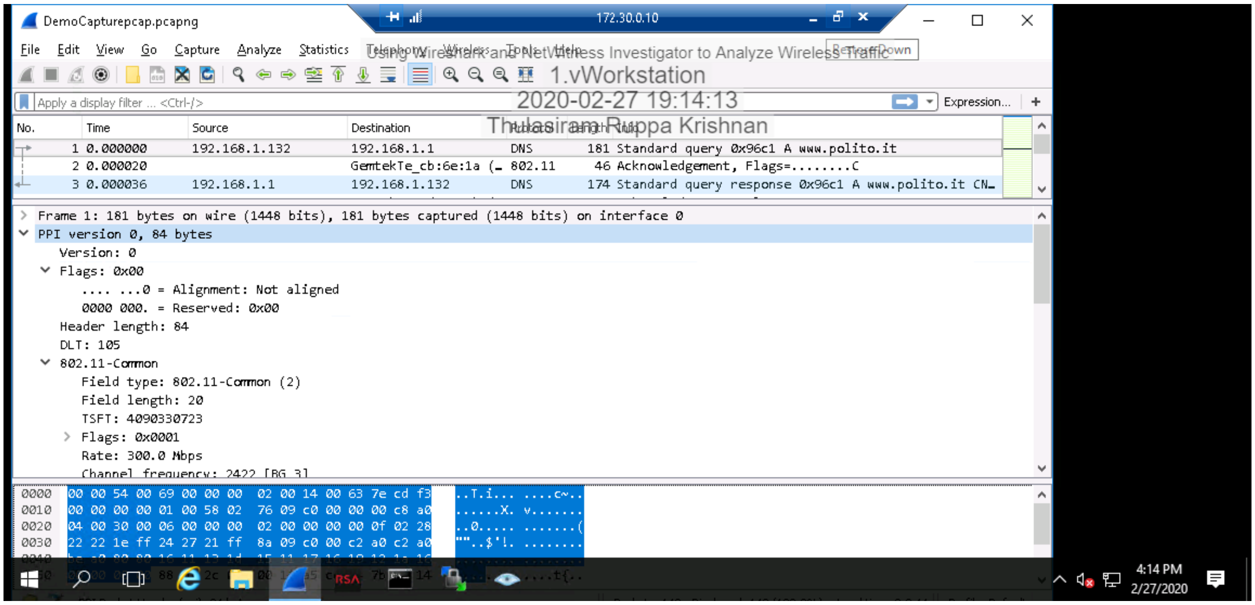


Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

Network Security, Firewalls, and VPNs - Lab 2

Current Step	Not Started
Progress	0%
StateSave Slot	New

Part 1: Analyze Wireless Traffic with Wireshark

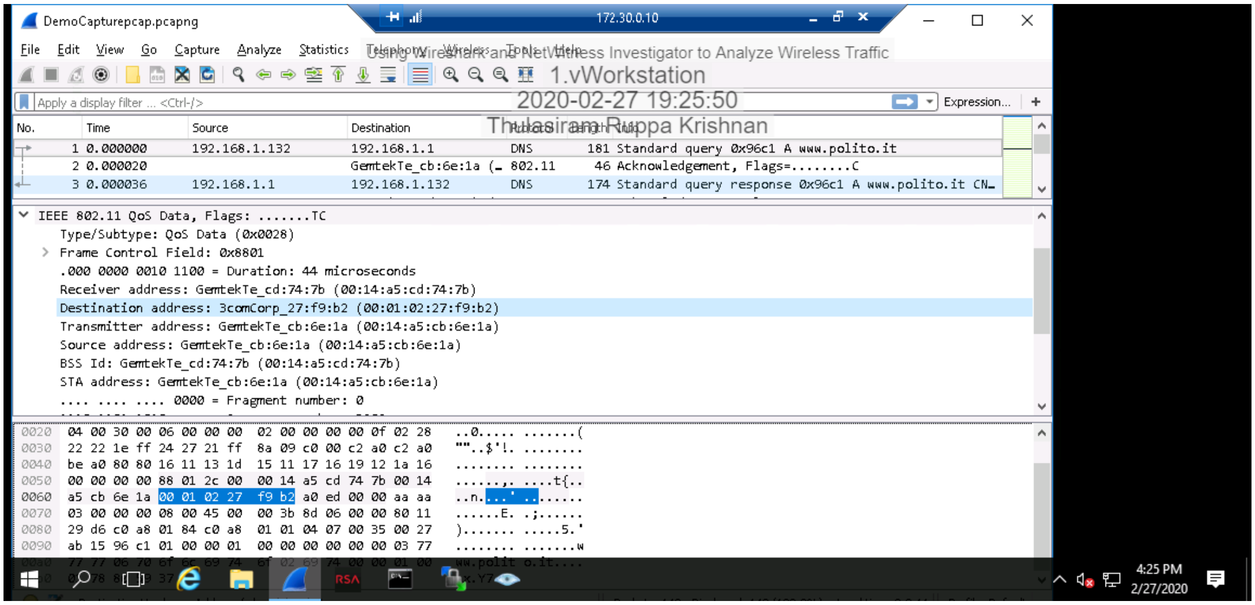

DemoCapturepcap.pcapng
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
4:14 PM
2/27/2020

Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
1.vWorkstation
2020-02-27 19:14:13
Thulasiram Ruppa Krishnan

```
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 CN…
```

```
> 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]
```

```
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   ""..$'!. ........
```

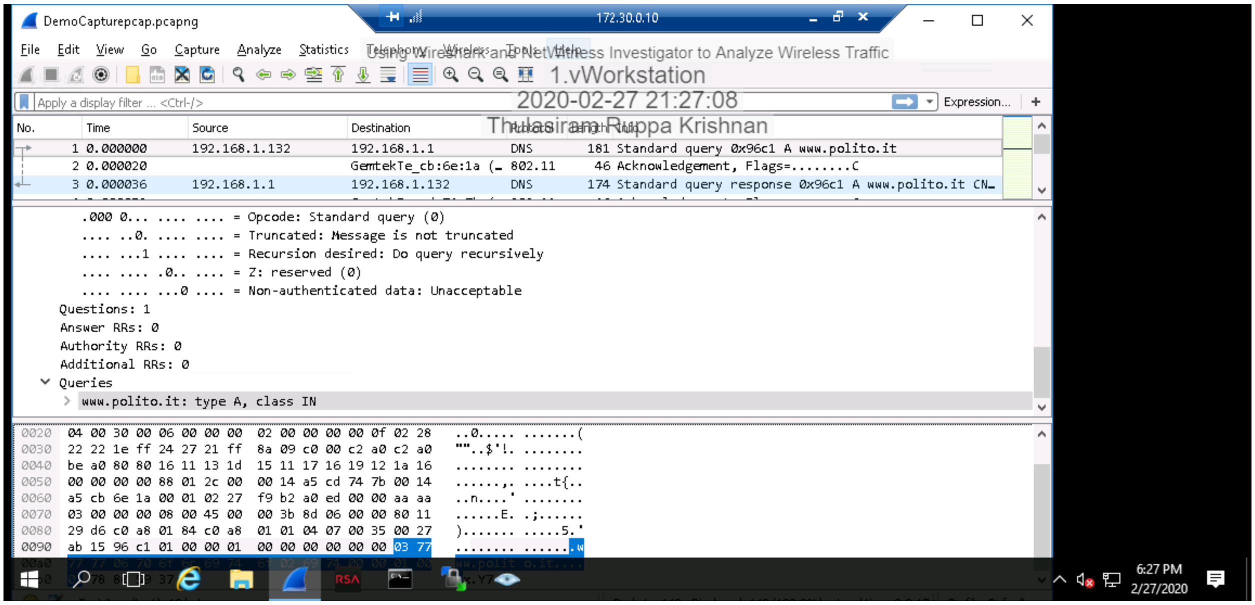

DemoCapturepcap.pcapng
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
4:25 PM
2/27/2020

Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
1.vWorkstation
2020-02-27 19:25:50
Thulasiram Ruppa Krishnan

```
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 CN…
```

```
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
```

```
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
```

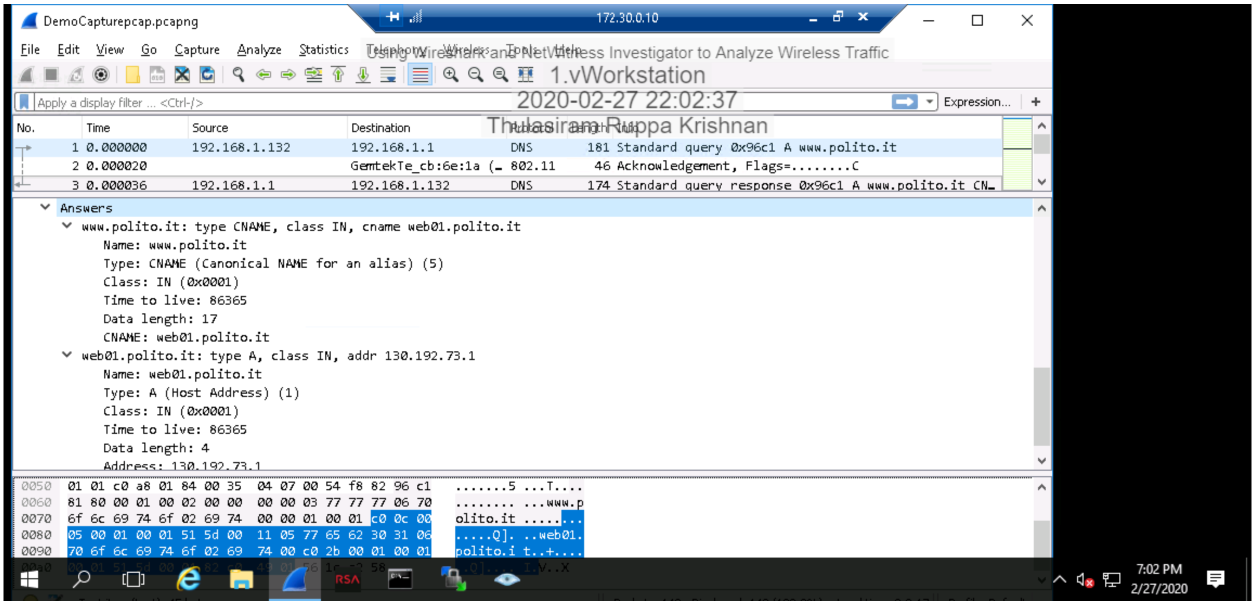


Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
1.vWorkstation
2020-02-27 21:27:08
Thulasiram Ruppa Krishnan

```
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 CN…
```

```
        .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
  ˅ Queries
    > www.polito.it: type A, class IN
```

```
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
```



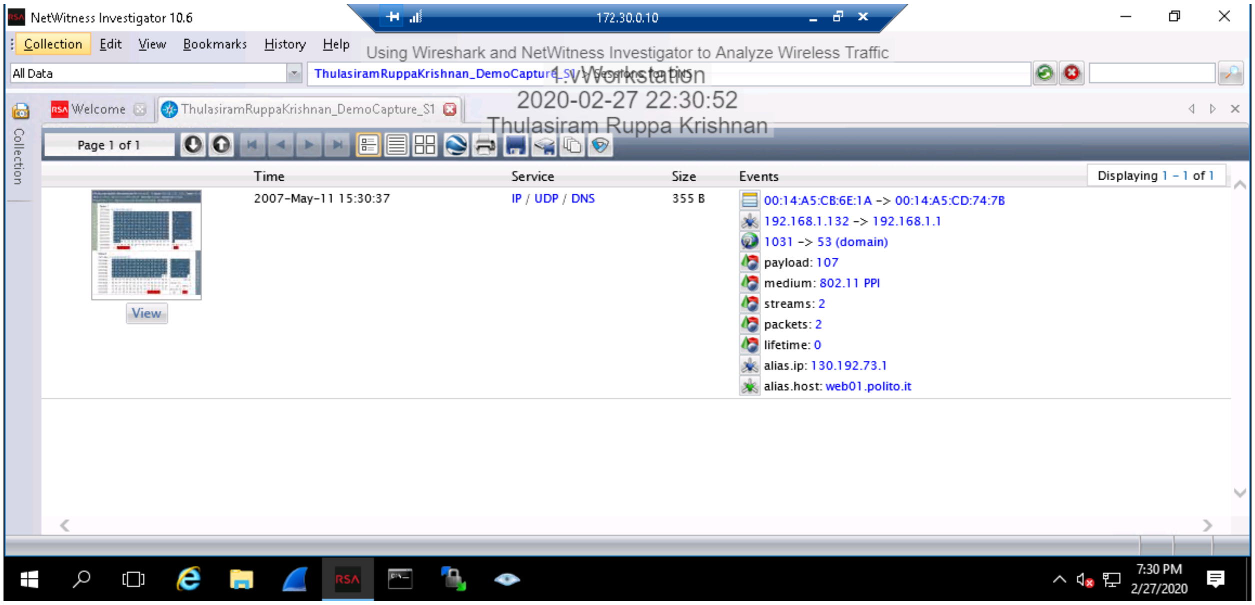
Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic
1.vWorkstation
2020-02-27 22:02:37
Thulasiram Ruppa Krishnan

```
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 CN…
```

```
  ˅ 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
```

```
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..+....
```

Part 2: Compare with NetWitness Investigator



Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

ThulasiramRuppaKrishnan_DemoCapture_S1 \ Sessions for DNS

1.VWorkstation

2020-02-27 22:30:52

Thulasiram Ruppa Krishnan

Displaying 1 – 1 of 1

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

Compare in 200 words the information provided by NetWitness to the screen capture you made with Wireshark (Part 1, Step#20).

In the Wireshark, it displays the name (host), colonial name (alias), class, time to live, data length and the ip address whereas in NetWitness it shows host, alias, medium, payload, domain, streams, packets and lifetime. The presentation in the NetWitness is neat and clear and easy to find information but on Wireshark it requires careful attention. Also, the graphical view helps to navigate through the information easily and quickly . with respect to data length and time to live the information in Wireshark is straight forward and in NetWitness I could not find the same value shown in Wireshark which is weird and not sure this information is available in NetWitness

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).

In the Wireshark, it displays source, destination, receiver and transmitter addresses and in NetWitness they are marked as categories. Wireshark displays transmitter/receiver addresses in both full hexadecimal (00:14:a5:cd:74:7b) and a kind of shorthand, in this case, GemtekTe_cd:74:7b. That shorthand code is Wireshark's translation of the first part of the receiver address (00:14:a5) into the manufacturer's name or alphanumeric designation (GemtekTe_).

Part 3: Challenge Question

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

- Wireshark requires elevated privileges, which can either be bad or good depending on your perspective.
- It has the standard disadvantage of capturing packets that might not reflect actual network traffic because the data is captured locally. Not a flaw of Wireshark, specifically, but of any locally run sniffing software.
- It can be confusing for new users to see all the columns and colors. You can do a lot of customization, but it takes some effort.
- It requires a lot of manual analysis to get the data a forensic investigator is searching for.
- Notifications will not make it evident if there is an intrusion in the network
- Can only gather information from the network, cannot send
- Wireshark has export restrictions
- Wireshark can decrypt the SSL traffic which can expose the private information