IST 623 - Intro to Information Security

Homework Lab 3

Ryan Timbrook
NetID: RTIMBROO
Term: Winter, 2020
Date: 3/3/2020
Topic: Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic

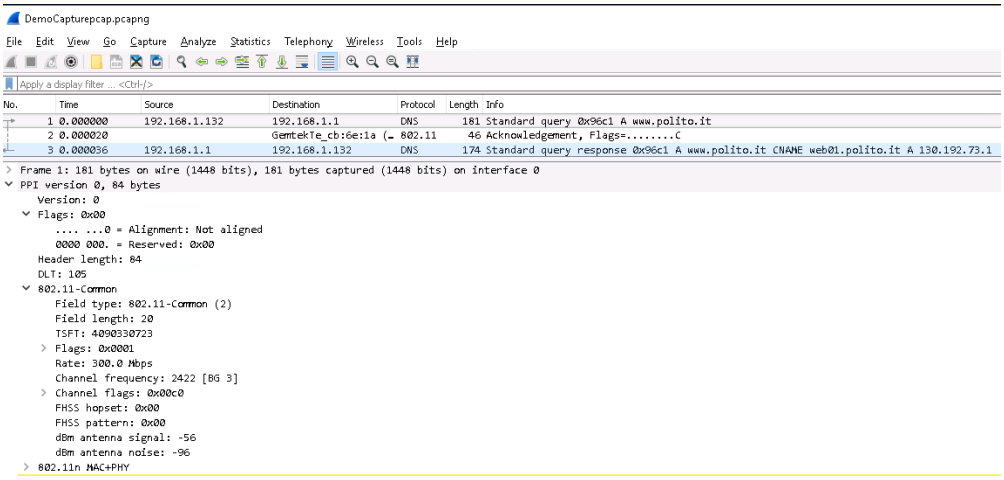
Table of Contents

Homework Lab 3

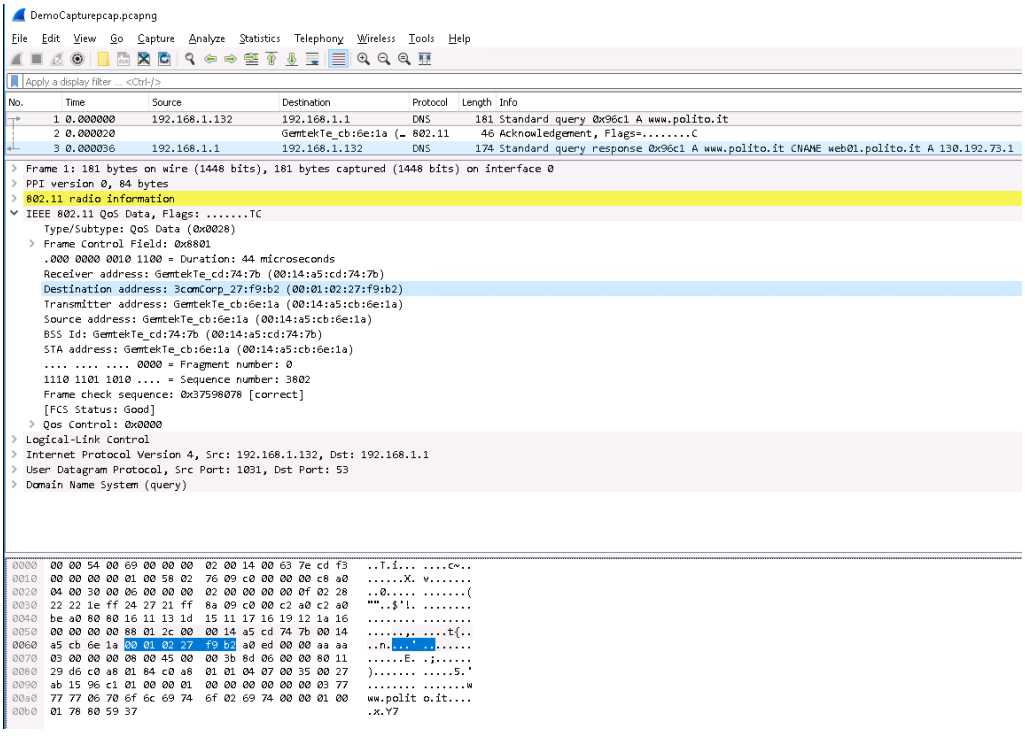
1 Part 1: Wireshark Analysis

Capture screenshots from Part 1: Steps #10, #12, #14, and #20

1.1 Step #10: Frame Details - PPI Expanded

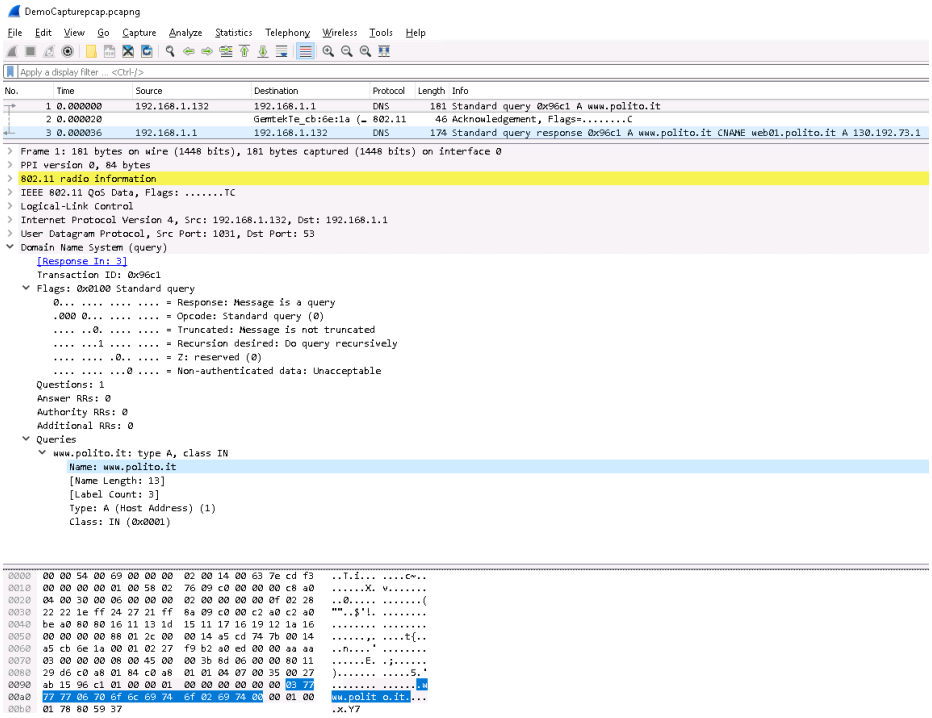


1.2 Step #12: Destination address

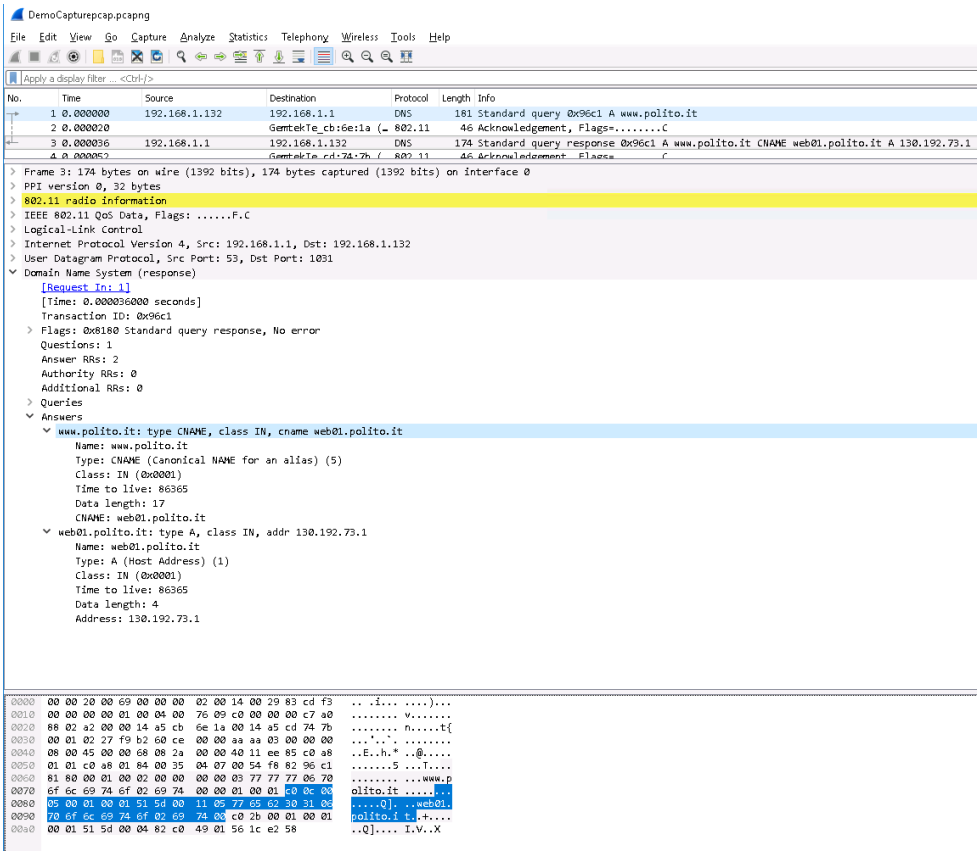


Homework Lab 3

1.3 Step #14: Queries expanded



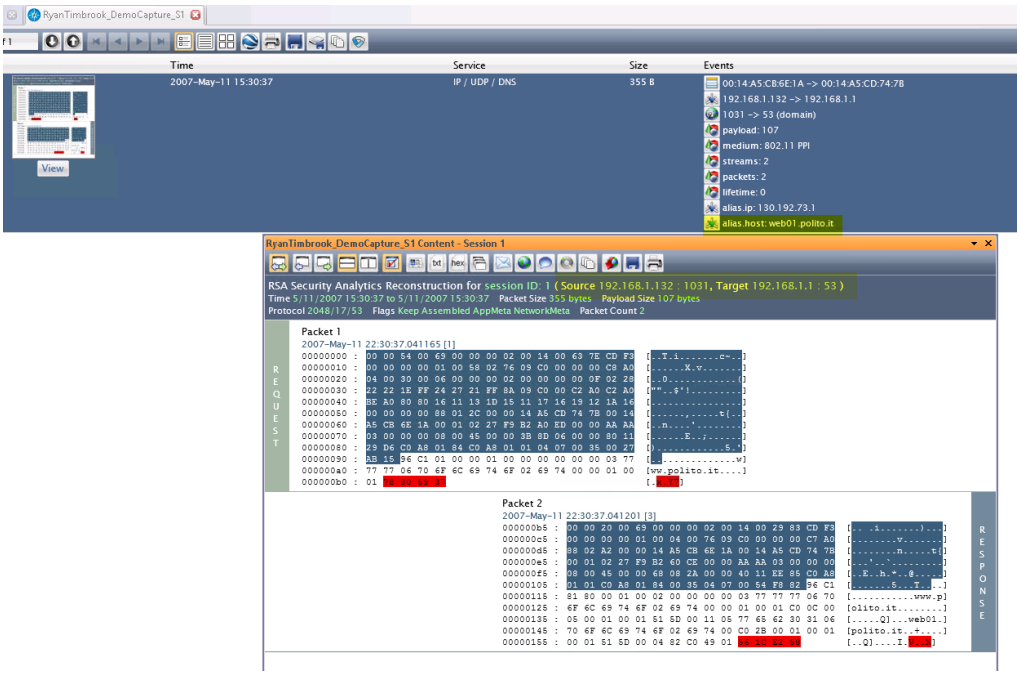
1.4 Step #20: DNS Answers expanded



2 Part 2: NetWitness Analysis

- Capture screenshots from Part 1: Steps #10
- Summary from Step #11
- Summary from Step #13

2.1 Step #10: DNS View



2.2 Step #11: Netwitness vs. Wireshark - DNS view

Question: Compare the information provided by NetWitness to the screen capture taken in part 1, Step #20

Response:

From the data captured in Wireshark under the 'Domain Name System (report)' header shown in section 2.4 above, compared to the image captured from Netwitness DNS analysis shown in section 3.1, both tools provide mostly the same information, where Netwitness does not have some of the low-level wireless information, such as command and control, but it provides a simpler, graphical display of the data. Netwitnesses graphical display allows you to view the DNS request and response packet information side-by-side with the events aggregated summary. This view makes it easy and and saves time in finding things like the alias host name and IP address, whereas in Wireshark it takes more time and experience in identifying these features. In Wireshark you'd have to know that CNAME (Canonical Name for an alias) translates to the alias host name the request was targeting. Netwitness also displays in its event window attributes that are buried in Wireshark under other headers than DNS that make it challenging to navigate. One example would be the source and destination mac addresses found in the first line of the Netwitness

DNS event window shown above. In Wireshark you'd have to search in other section headers to find this critical information.

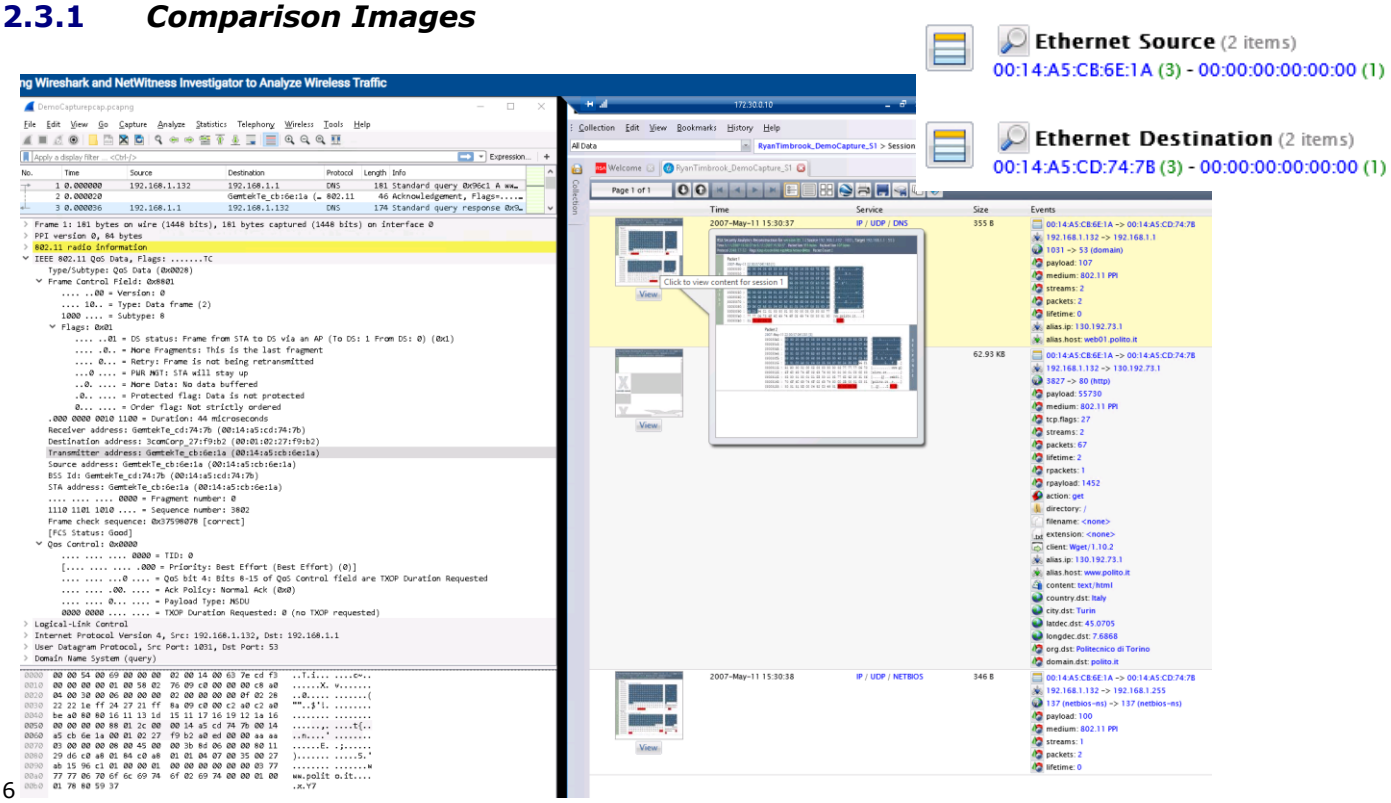
2.3 Step #13: Netwitness vs. Wireshark - Ethernet Source/Destination

Question: Compare the information seen in Netwitness Ethernet Source and Ethernet Destination categories with Wireshark 'Frame Address Information'.

Response:

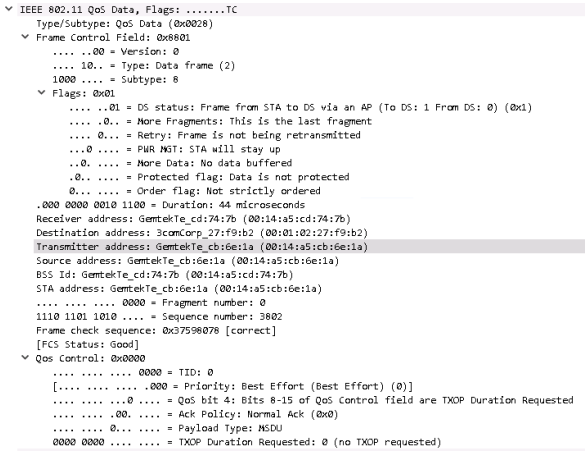
Comparing Netwitness's view of Ethernet Source/Destination information with Wireshark's Frame Detail data, see section 3.3.1 Comparison Images below for details, Netwitness groups the source/destination data for simple viewing of the detailed data elements. In the Netwitness window shown below on the right hand side of the image, the source information is broken down into the three service protocol that represent the hierarchy of the communication. In this view you are able to see at a glance high-level information about the transmission that could be used in forensic analysis such as country.dst, city.dst, latdec.dst, longdec.dst, org.dst, domain.dst, to name a few, under the HTTP Service. In addition to those fields, other relevant information such as payload, medium, packet counts, lifetime, etc. are shown for quick analysis, whereas in Wireshark these fields are found in other section headers making it time intensive to pinpoint and paint a picture of what's going on in the communication. However, Wireshark does have lower level information not displayed in Netwitness such as Flags where you can see that in the source data it shows that the 'Protected flag: Data is not protected'.

2.3.1 *Comparison Images*



Homework Lab 3

Wireshark - Frame Control



```
IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    Flags: 0x01
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .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
      .... .... .... 0000 = TID: 0
      [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
      .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
      0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
```

Netwitness - Ethernet Source / Destination

3 Part 3: Challenge Question

Question: Discuss current limitations of Wireshark.

While Wireshark has many positive attributes such as details on the granular level, dissecting packets to the maximum limit possible, it's availability on all operating systems, it's low load on the systems processor, and ability to listen on multiple NIC's at once and provide dumps allowing you to plug in and listen on all of them at once, it has it's limitations in a few areas. For one, it feel's "too in-depth" and can be overwhelming to look at. The tool lacks features that would aggregate the data into higher-level views for quick analysis and troubleshooting as seen in the NetWitness Investigator tool. Reports in Wireshark can not be exported in a graphical-intuitive format, only XML or RAW text, which is a con for anyone who has to present their findings to upper leadership who respond better to well laid out data visualizations.

Despite the fact that it allows you to monitor the network, it does not provide a mechanism to alert administrators in case of strange things happening in the network. It only measures data in the network but does not manipulate the data. Wireshark requires a lot of memory for large organizations with a busy network, it therefor may end up crushing it if it runs out of memory.

It is possible that in some cases Wireshark will not be able to capture wireless information or it can only capture the essence of the command and control information, but not the information itself. Packet capture add-ons, such as AirPcap, are frequently installed with Wireshark. These add-ons enable you to capture more wireless information, but again is an add-on that requires human time and effort to install and configure in the environment.

Additionally, Wireshark has a few name resolution drawbacks such as:

- Name resolution will often fail.
    - The name to be resolved might simply be unknown by the name servers asked, or the servers are just not available and the name is also not found in the Wireshark's configuration files.
- The resolved names are not stored in the capture file or somewhere else.
    - Resolved names might not be available if you open the capture file later or on a different machine. Each time you open a capture file it may look "slightly different" simply because you can't connect to the name server.
- DNS may add additional packets to your capture file:
    - You may see packets to/from your machine in your capture file, which are caused by name resolution network services of the machine Wireshark captures from.
- Resolved DSN names are cached by Wireshark
    - If the name resolution information should change while Wireshark is running, Wireshark won't notice a change in the name resolution information once it gets cached, e.g., a new DHCP lease takes effect, Wireshark won't notice it.
- https://www.wireshark.org/download/docs/user-guide.pdf