

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

Homework Lab 3

Table of Contents

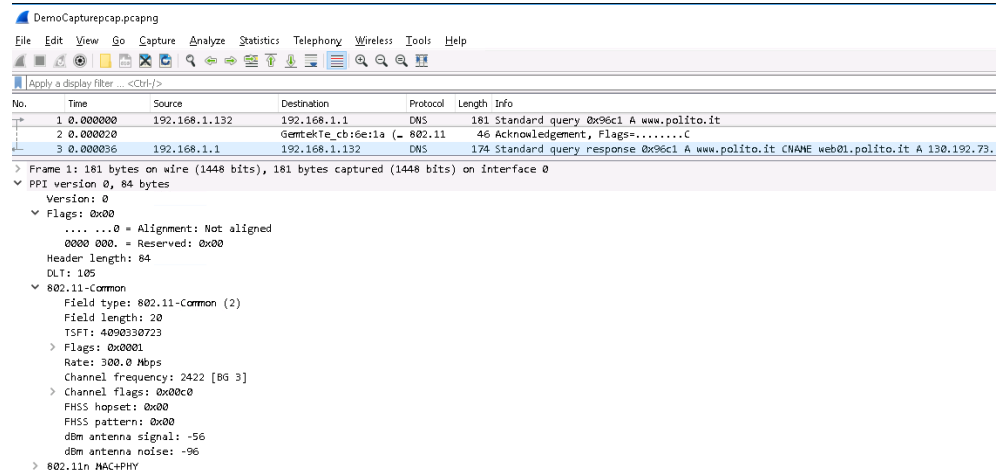
1 Part 1: Wireshark Analysis	3
1.1 Step #10: Frame Details - PPI Expanded	3
1.2 Step #12: Destination address.....	3
1.3 Step #14: Queries expanded	4
1.4 Step #20: DNS Answers expanded	4
2 Part 2: NetWitness Analysis	5
2.1 Step #10: DNS View	5
2.2 Step #11: Netwitness vs. Wireshark - DNS view	5
2.3 Step #13: Netwitness vs. Wireshark - Ethernet Source/Destination	6
2.3.1 Comparison Images	6
3 Part 3: Challenge Question	8

Homework Lab 3

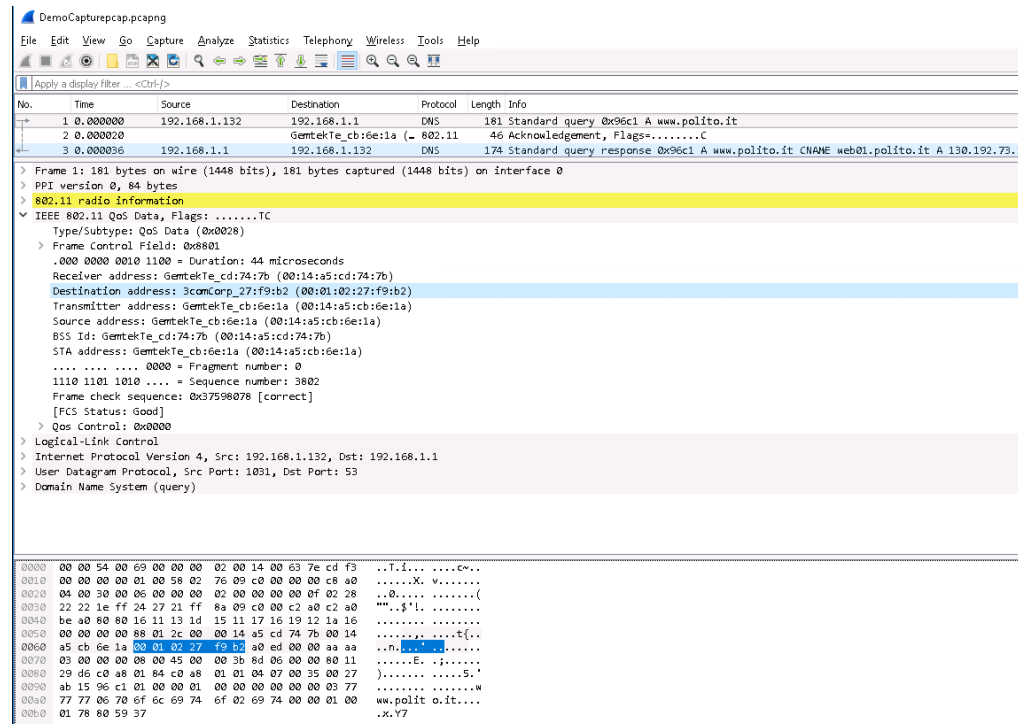
1 Part 1: Wireshark Analysis

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

DemoCapturecap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>

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 web01.polito.it A 130.192.73.1

> 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

> Domain Name System (query)

[Request In: 3]

Transaction ID: 0x96c1

Flags: 0x0100 Standard query

0... .. = Response: Message is a query

... .. = Opcode: Standard query (0)

... .. = Truncated: Message is not truncated

... .. = Recursion desired: Do query recursively

... .. = Z: reserved (0)

... .. = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

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)

0000 00 00 54 00 69 00 00 00 02 00 14 00 63 7e cd f3 ...T.i... ..Cm..

0010 00 00 00 00 01 00 58 02 76 09 c0 00 00 c8 a0X. V.....

0020 04 00 30 00 06 00 00 00 02 00 00 00 0f 02 28 ...0.....(

0030 22 22 1e ff 24 27 21 ff 8a 09 c0 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 88 01 2c 00 00 14 a5 cd 74 7b 00 14{..

0060 a5 cb 6e 1a 00 01 02 27 f9 b2 a0 ed 00 00 aa aa ...f.....

0070 03 00 00 00 08 00 45 00 00 3b 8d 00 00 80 11E. j.....

0080 29 d0 c0 a8 01 84 c0 a8 01 01 08 07 00 35 00 275..

0090 ab 15 96 c1 01 00 00 01 00 00 00 00 00 00 77LW

00a0 77 77 06 70 6f 6c 69 74 6f 02 69 74 00 00 01 00 ww.polito.it... ..

00b0 01 78 80 59 37X.Y7

1.4 Step #20: DNS Answers expanded

DemoCapturecap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>

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 web01.polito.it A 130.192.73.1
4	0.000052		GemtekTe.cb:74:7b (- 802.11)	46	Acknowledgement, Flags=.....C	

> Frame 3: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0

> PPI version 0, 92 bytes

> **802.11 radio information**

> IEEE 802.11 QoS Data, Flags:F.C

> Logical-Link Control

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.132

> User Datagram Protocol, Src Port: 53, Dst Port: 1031

> Domain Name System (response)

[Request In: 1]

[Time: 0.00006000 seconds]

Transaction ID: 0x96c1

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

Queries

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 c7 a0V.....

0020 88 82 a2 00 00 14 a5 cb 6e 1a 00 14 a5 cd 74 7bt(

0030 00 01 02 27 f9 b2 69 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 c15...T.....

0060 81 80 00 01 00 02 00 00 00 00 03 77 77 06 70www.p

0070 6f 6c 69 74 6f 02 69 74 00 01 00 01 00 00 00 olito.it.....

0080 05 00 01 03 01 51 54 00 11 05 77 65 62 30 31 03Q]..web01

0090 70 6f 6c 69 74 6f 02 69 74 00 c0 2b 00 01 00 01 polito.it.....

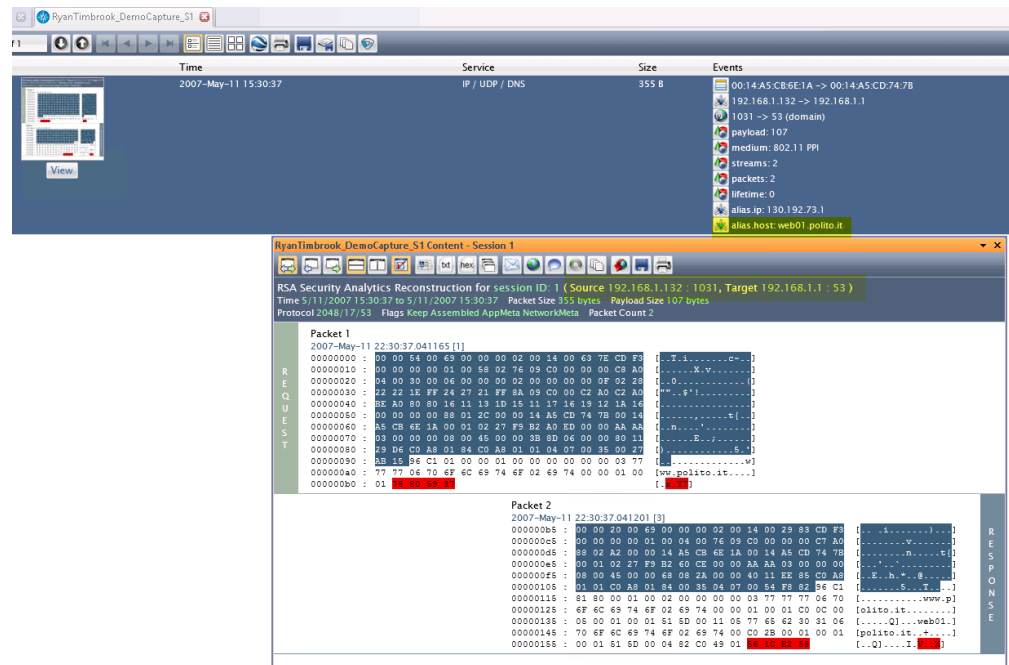
00a0 00 01 51 5d 00 04 82 c0 49 01 56 1c e2 58Q]....I.V..X

Homework Lab 3

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. NetWitness 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 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

Homework Lab 3

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

The image displays a side-by-side comparison of two network analysis tools: Wireshark (left) and Netwitness (right).

Wireshark (Left): The interface shows a packet capture of a DNS query. The 'Frame 1: 181 bytes on wire (1444 bits), 181 bytes captured (1444 bits) on interface 0' is selected. The 'Details' pane shows the 'Ethernet II, Src: Intel Corp. (08:00:00:00:00:00), Dst: Intel Corp. (08:00:00:00:00:00)' and 'Internet Protocol Version 4, Src: 192.168.1.132, Dst: 192.168.1.1'. The 'Payload' pane shows a 'Standard query query' from 192.168.1.132 to 192.168.1.1.

Netwitness (Right): The interface shows a list of events. The 'Ethernet Source' and 'Ethernet Destination' categories are expanded, showing a list of events with details such as 'Time', 'Service', 'Size', and 'Events'. The 'Ethernet Source' event shows a source IP of 00:14:A5:CB:6E:1A (3) and a destination IP of 00:00:00:00:00:00 (1). The 'Ethernet Destination' event shows a source IP of 00:14:A5:CD:74:7B (3) and a destination IP of 00:00:00:00:00:00 (1).

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 NOT: 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
[.... ..0000 = Priority: Best Effort (Best Effort) (0)]
.... ..0000 = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
.... ..0000 = Ack Policy: Normal Ack (0x0)
.... ..0000 = Payload Type: MSDU
0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)

```

Netwitness - Ethernet Source / Destination

**Ethernet Source** (2 items)

00:14:A5:CB:6E:1A (3) - 00:00:00:00:00:00 (1)

**Ethernet Destination** (2 items)

00:14:A5:CD:74:7B (3) - 00:00:00:00:00:00 (1)

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.
 - o 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.
 - o 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:
 - o 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
 - o 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>