

Lab Report #3: Network Security, Firewalls, and VPNs

Section 1 Part 1:

IEEE 802.11 QoS Data fields

DemoCapturecap.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	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

> PPI version 0, 84 bytes

> 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

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 a0X. v.....

0020 04 00 30 00 06 00 00 00 02 00 00 00 00 0f 02 28 ..0.... n.....t{

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 16E..h.*..@.....

Query name (www.polito.it) The source IP address, and the destination IP address

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.....

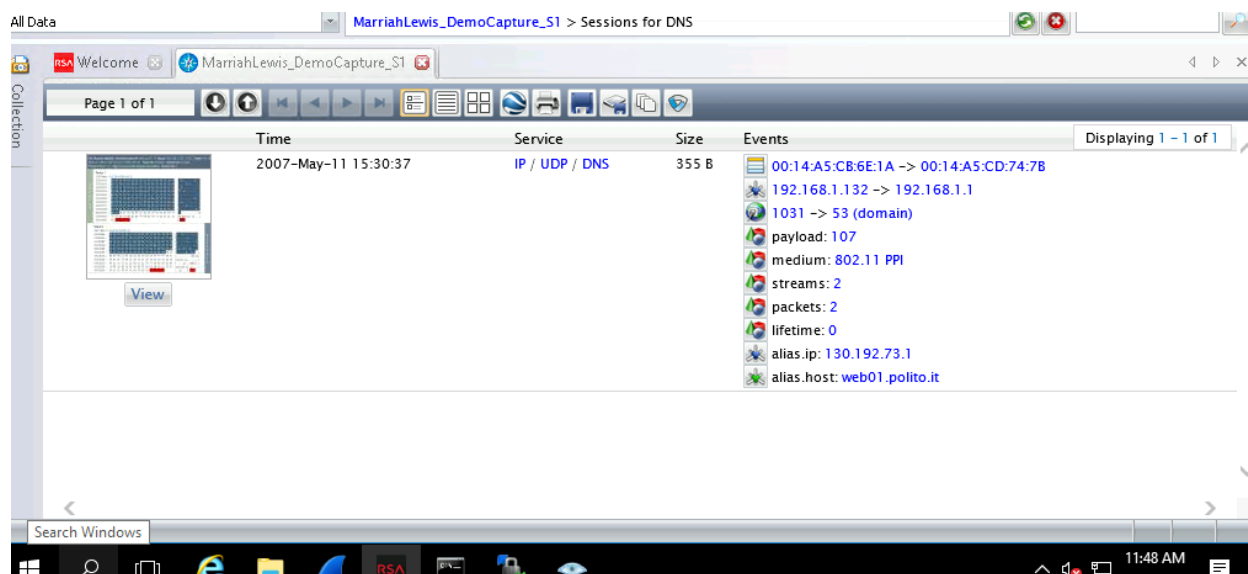
0020 88 02 a2 00 00 14 a5 cb 6e 1a 00 14 a5 cd 74 7b n.....t{

0030 00 01 02 27 f9 b2 60 ce 00 00 aa aa 03 00 00 00 ...'..`.....

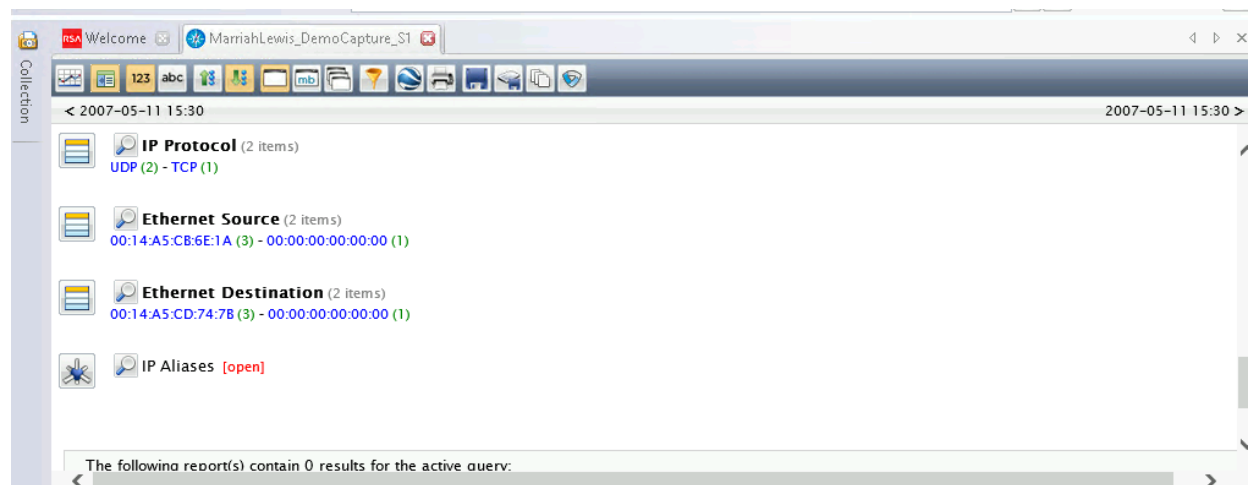
0040 08 00 45 00 00 68 08 2a 00 00 40 11 ee 85 c0 a8 ..E..h.*..@.....

Section 1 Part 2: Analyze Wireless Traffic with NetWitness Investigator

Hostname Alias, the Source IP Address, and the Destination IP Address



Ethernet source and Ethernet destination addresses



Netwitness vs Wireshark- DNS view

Both applications provide essentially the same information, with the exception that Netwitness lacks some of the low-level wireless information, such as command and control, but it does it in a more user-friendly, graphical fashion. The DNS request and response packet information can be viewed side-by-side with the events aggregated summary on the Netwitness graphical display. Finding items like the alias host name and IP address is simple and quick with this approach but

recognizing similar details in Wireshark takes more time and skill. In Wireshark, the user must know the Canonical Name for an alias, which corresponds to the alias host name for which the request was made. In addition, Netwitness exposes attributes that are buried in Wireshark under other headers than DNS, making it difficult to traverse. The source and destination mac addresses in the first line of the Netwitness DNS event window displayed above is an example. In Wireshark, the user would have to search in other sections headers to find this critical information.

Netwitness vs Wireshark- Ethernet Source/Destination

The source/destination data is grouped in Netwitness for easy viewing of the detailed data components. The source information in the Netwitness window is divided down into three-service protocols that illustrate the communication hierarchy. Under the HTTP service, the user can observe briefly high-level information about the transmission that could be used for forensic investigation, such as country.dst, city.dst, latdec.dst, longdec.dst, domain.dst. Notwithstanding those fields, other applicable data like payload, medium, packet counts, lifetime, and more are displayed for fast investigation, while in Wireshark these fields are found in other segment headers making the task time intensive to pinpoint and difficult to understand what is going on in the communication. Nonetheless, Wireshark has lower-level data not showed in Netwitness, for example, Flags where the user can see that in the source information it shows that the 'Protected flag: data is not protected'.