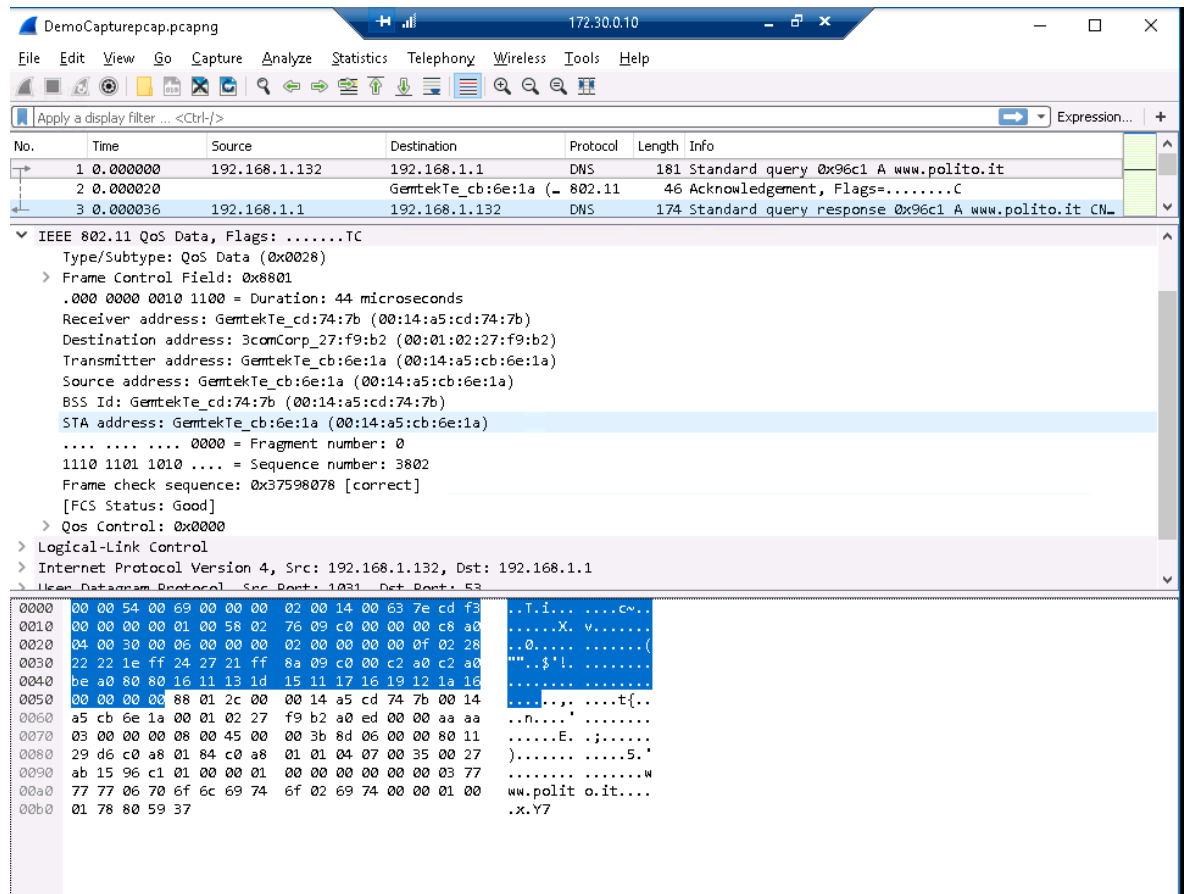


Lab 2

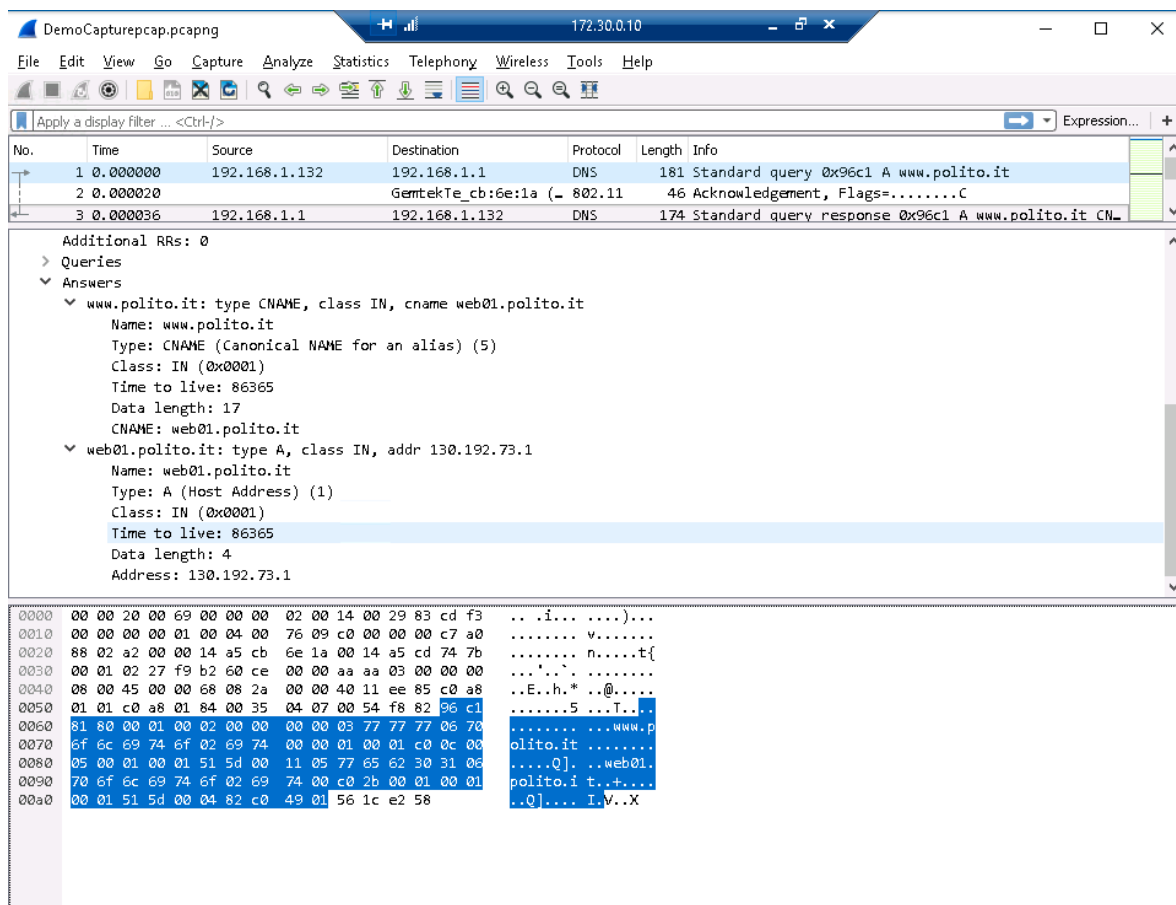
Authors: Daniel Gisolfi, James Ekstract

Section 1

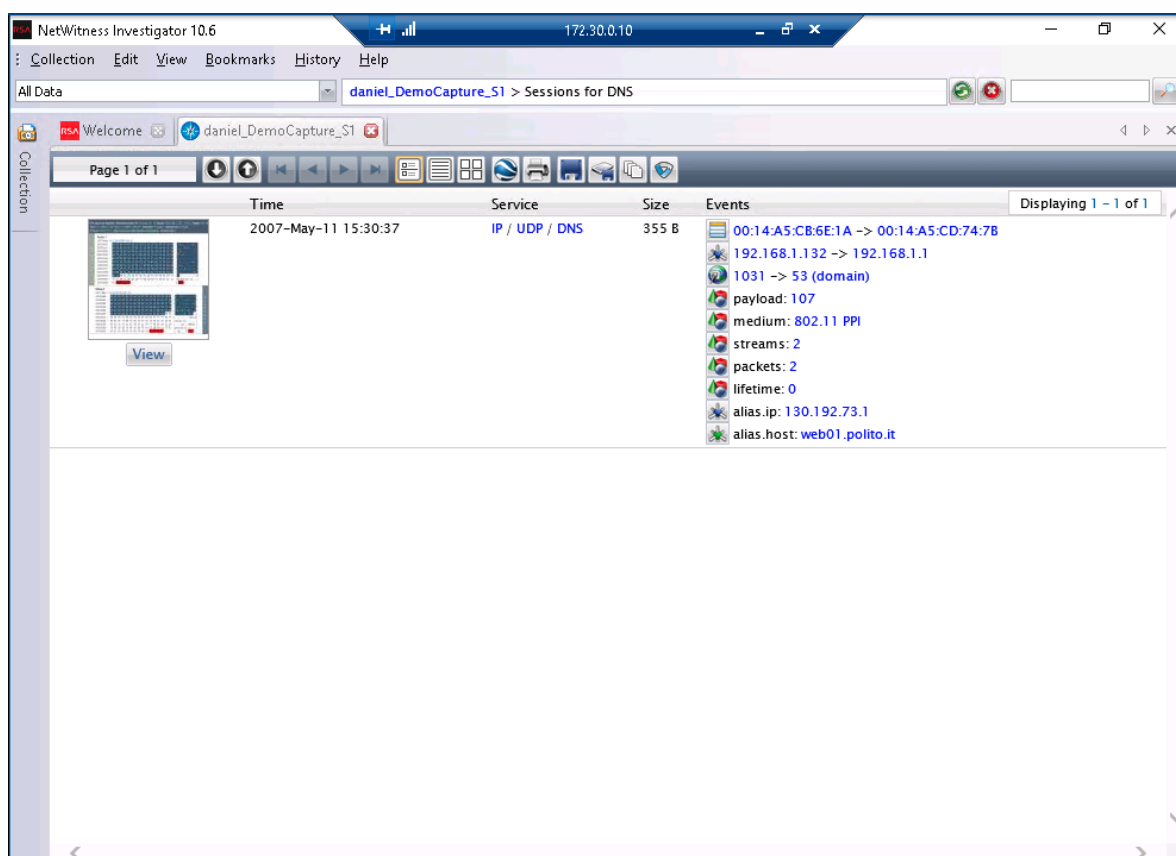
A screen capture showing the detail found in the IEEE 802.11 QoS Data fields



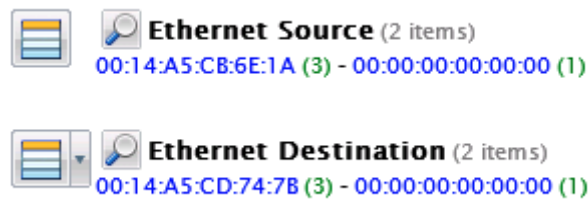
A screen capture showing the query name (www.polito.it), the source IP address, and the destination IP address



A screen capture of the DNS query showing the Hostname Alias, the Source IP Address, and the Destination IP Address fields



A screen capture showing the Ethernet source and Ethernet destination addresses



Looking at the same information viewed in wire shark from Part 1, Step 18. The view in netwitness investigator is a much higher level view in this case as the destination address is shown as 00:00:00:00:00:00 rather than the value seen in the wireshark screenshot displaying the destination as 00:01:02:27:f9:b2

Section 2

Part 1

The list of protocols used in frame 7 displayed in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
7	1.794591	95.136.242.99	109.6.1.72	PPP LCP	68	Echo Request
8	1.819663	109.6.1.72	95.136.242.99	PPP LCP	70	Echo Reply
9	3.047733	95.136.242.99	109.6.1.72	L2TP	70	Control Message

> Frame 7: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)						
> Ethernet II, Src: Sfr_18:c2:73 (e0:a1:d7:18:c2:73), Dst: Sfr_61:00:00 (00:17:33:61:00:00)						
> PPP-over-Ethernet Session						
> Point-to-Point Protocol						
> Internet Protocol Version 4, Src: 95.136.242.99, Dst: 109.6.1.72						
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701						
> Layer 2 Tunneling Protocol						
> Point-to-Point Protocol						
> PPP Link Control Protocol						

The source port used by UDP in frame 18, displayed in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
17	5.219666	HuaweiTe_f0:45:d7	Sfr_66:65:b1	ARP	60	Who has 10.
18	14.342833	95.136.242.99	109.0.66.20	DNS	77	Standard qu
19	14.343717	95.136.242.99	109.0.66.20	DNS	77	Standard qu

.... 0 = IG bit: Individual address (unicast)						
▼ Source: Sfr_18:c2:73 (e0:a1:d7:18:c2:73)						
Address: Sfr_18:c2:73 (e0:a1:d7:18:c2:73)						
.... 0 = LG bit: Globally unique address (factory default)						
.... 0 = IG bit: Individual address (unicast)						
Type: PPPoE Session (0x8864)						
> PPP-over-Ethernet Session						
> Point-to-Point Protocol						
> Internet Protocol Version 4, Src: 95.136.242.99, Dst: 109.0.66.20						
▼ User Datagram Protocol, Src Port: 65388, Dst Port: 53						
Source Port: 65388						
Destination Port: 53						
Length: 35						
Checksum: 0x54d4 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 2]						

The domain queried in frame 18, displayed in Wireshark

No.	Time	Source	Destination	Protocol
17	5.219666	HuaweiTe_f0:45:d7	Sfr_66:65:b1	ARP
18	14.342833	95.136.242.99	109.0.66.20	DNS
19	14.343717	95.136.242.99	109.0.66.20	DNS

▼ User Datagram Protocol, Src Port: 65388, Dst Port: 53

Source Port: 65388

Destination Port: 53

Length: 35

Checksum: 0x54d4 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

▼ Domain Name System (query)

[\[Response In: 21\]](#)

Transaction ID: 0x6508

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> perdu.com: type A, class IN

The address details shown in frame 21 (the response to frame 18) displayed in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
20	14.369951	109.0.66.20	95.136.242.99	DNS	138	Standard query response 0x0947 AAAA perdu.com SOA...
21	14.375865	109.0.66.20	95.136.242.99	DNS	93	Standard query response 0x6508 A perdu.com A 208...
22	14.393000	95.136.242.99	109.0.66.20	DNS	87	Standard query 0xe69b A hotspot.wifi.sfr.fr

[Time: 0.033032000 seconds]

Transaction ID: 0x6508

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

▼ Queries

> perdu.com: type A, class IN

▼ Answers

▼ perdu.com: type A, class IN, addr 208.97.177.124

Name: perdu.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 5474

Data length: 4

Address: 208.97.177.124

The authoritative nameserver in frame 20, displayed in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
20	14.369951	109.0.66.20	95.136.242.99	DNS	138	Standard query response 0x0947 AAAA perdu.com SOA...
21	14.375865	109.0.66.20	95.136.242.99	DNS	93	Standard query response 0x6508 A perdu.com A 208...
22	14.393000	95.136.242.99	109.0.66.20	DNS	87	Standard query 0xe69b A hotspot.wifi.sfr.fr

Additional RRs: 0

- Queries
 - > perdu.com: type AAAA, class IN
- Authoritative nameservers
 - > perdu.com: type SOA, class IN, mname ns1.dreamhost.com
 - Name: perdu.com
 - Type: SOA (Start Of a zone of Authority) (6)
 - Class: IN (0x0001)
 - Time to live: 3555
 - Data length: 49
 - Primary name server: ns1.dreamhost.com
 - Responsible authority's mailbox: hostmaster.dreamhost.com
 - Serial Number: 2013012600
 - Refresh Interval: 18339 (5 hours, 5 minutes, 39 seconds)
 - Retry Interval: 1800 (30 minutes)
 - Expire limit: 1814400 (21 days)
 - Minimum TTL: 14400 (4 hours)

The destination MAC address of frame 285, displayed in Wireshark

No.	Time	Source	Destination
284	27.813852	80.118.192.115	10.251.23.139
285	27.832353	10.251.23.139	80.118.192.115
286	27.836840	95.136.242.99	109.0.74.75

> Frame 285: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface 0

▼ Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)

Address: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)

The source and destination ports of frame 285, displayed in Wireshark

285	27.832353	10.251.23.139	80.118.192.115
286	27.836840	95.136.242.99	109.0.74.75

> Frame 285: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface 0

> Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)

> Internet Protocol Version 4, Src: 10.251.23.139, Dst: 80.118.192.115

▼ User Datagram Protocol, Src Port: 33810, Dst Port: 1813

Source Port: 33810

Destination Port: 1813

The attribute value pairs of frame 285, displayed in Wireshark

285	27.832353	10.251.23.139	80.118.192.115	RADIUS	350 Accounting-Request(4) (id=0, 1)
286	27.836840	95.136.242.99	109.0.74.75	TLsv1	727 Application Data

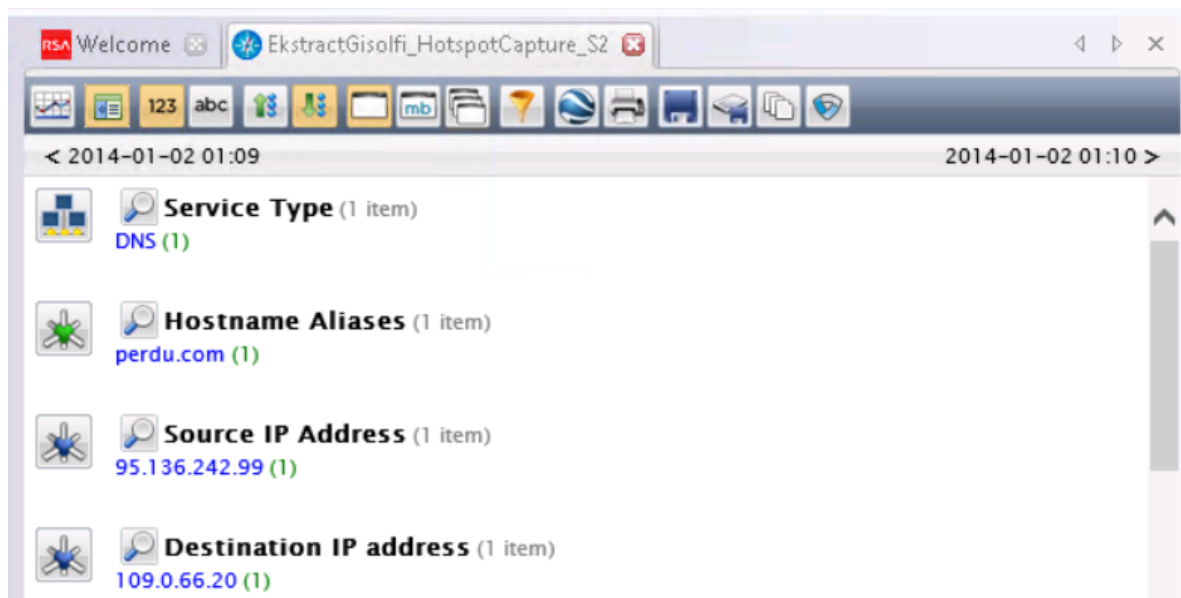
Authenticator: 1c377b8ac649d7829fa73f5d454f6f50
[\[The response to this request is in frame 287\]](#)

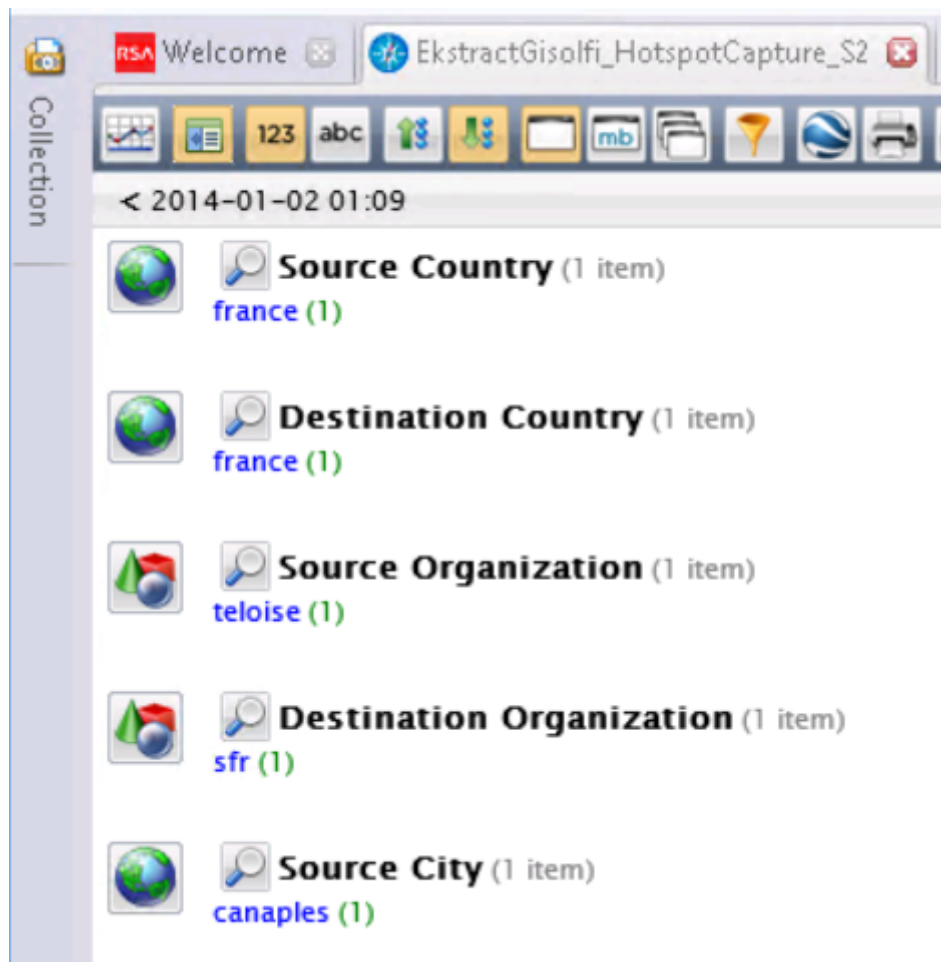
Attribute Value Pairs

- > AVP: l=6 t=Acct-Status-Type(40): Start(1)
- > AVP: l=37 t=User-Name(1): mon.identifi@sfr.fr@ssowifi.neuf.fr
- > AVP: l=19 t=Calling-Station-Id(31): 00-19-7D-3B-6F-D4
- > AVP: l=19 t=Called-Station-Id(30): AA-A1-D7-18-C2-75
- > AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
- > AVP: l=6 t=NAS-Port(5): 0
- > AVP: l=19 t=NAS-Port-Id(87): 99.Neufbox-NB4.33
- > AVP: l=19 t=Vendor-Specific(26) v=Open System Consultants(9048)
- > AVP: l=6 t=NAS-IP-Address(4): 95.136.242.99
- > AVP: l=19 t=NAS-Identifier(32): e0-a1-d7-18-c2-73
- > AVP: l=6 t=Framed-IP-Address(8): 192.168.2.83
- > AVP: l=18 t=Acct-Session-Id(44): 52c52ce000000000
- > AVP: l=66 t=Vendor-Specific(26) v=Wireless Broadband Alliance Ltd (formerly 'Wi-Fi Alliance')(14122)
- > AVP: l=42 t=Vendor-Specific(26) v=Wireless Broadband Alliance Ltd (formerly 'Wi-Fi Alliance')(14122)

Part 2

The hostname alias, source IP, destination IP , and source city fields of the perdu.com DNS session displayed in NetWitness Investigator





The source and destination cities from the packet capture, displayed in NetWitness Investigator

