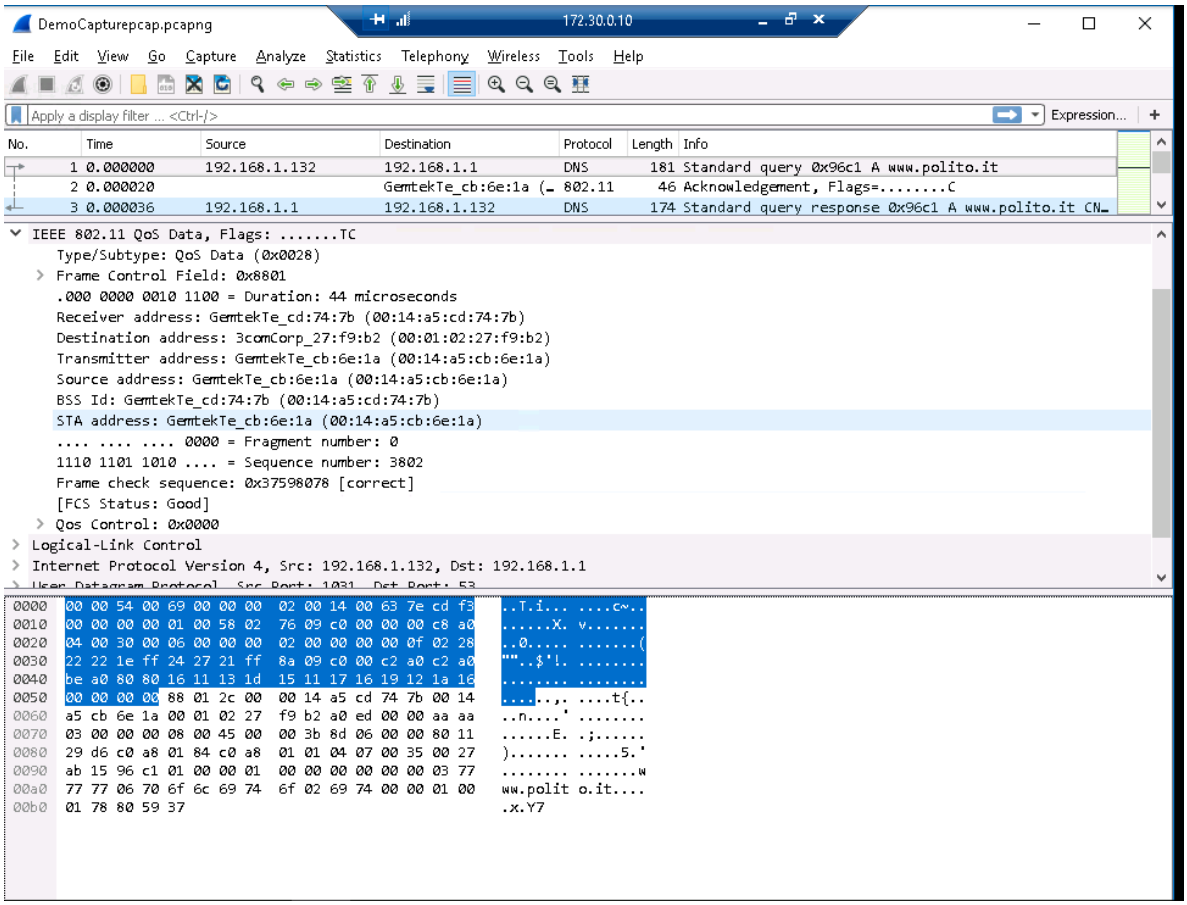
Lab 2 💻

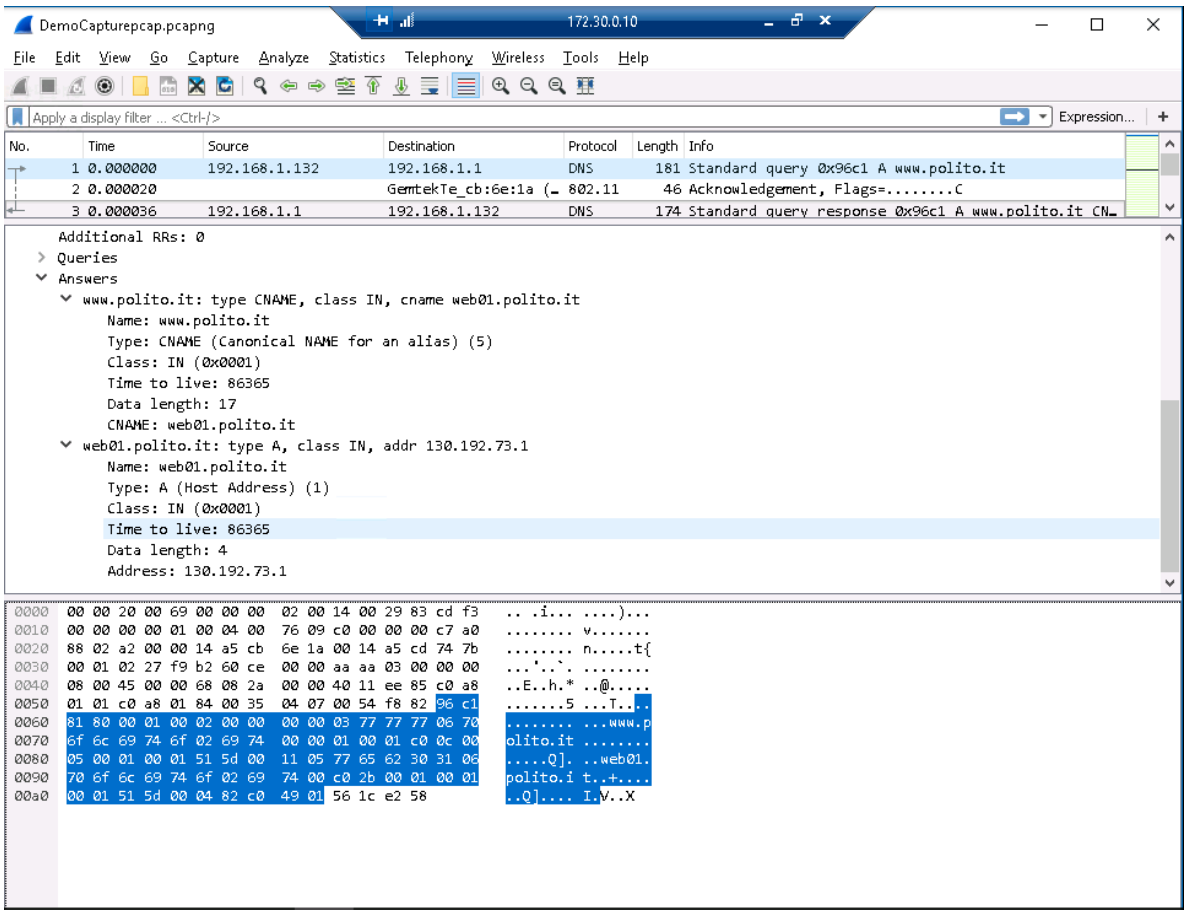
Authors: Daniel Gisolfi, James Ekstract

Section 1

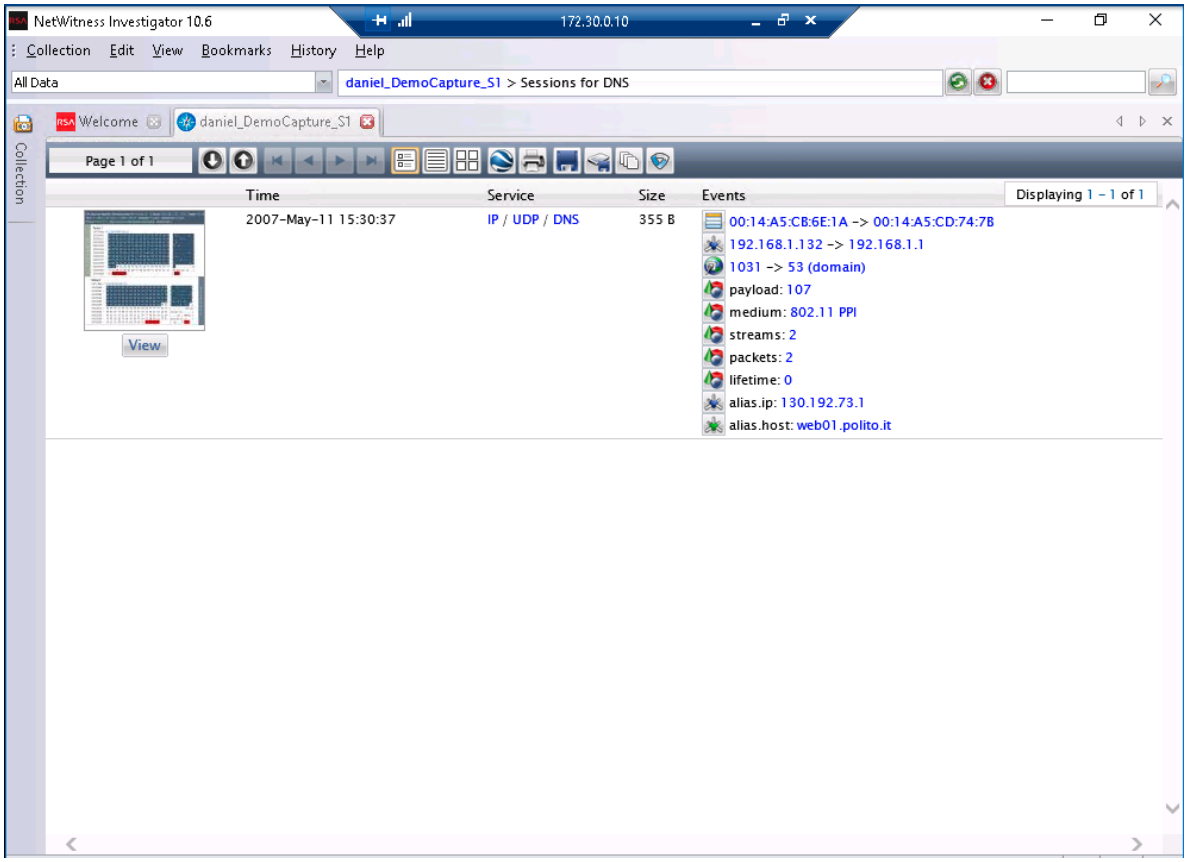
A screen capture showing the detail found in the IEEE 802.11 QoS Data fields



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



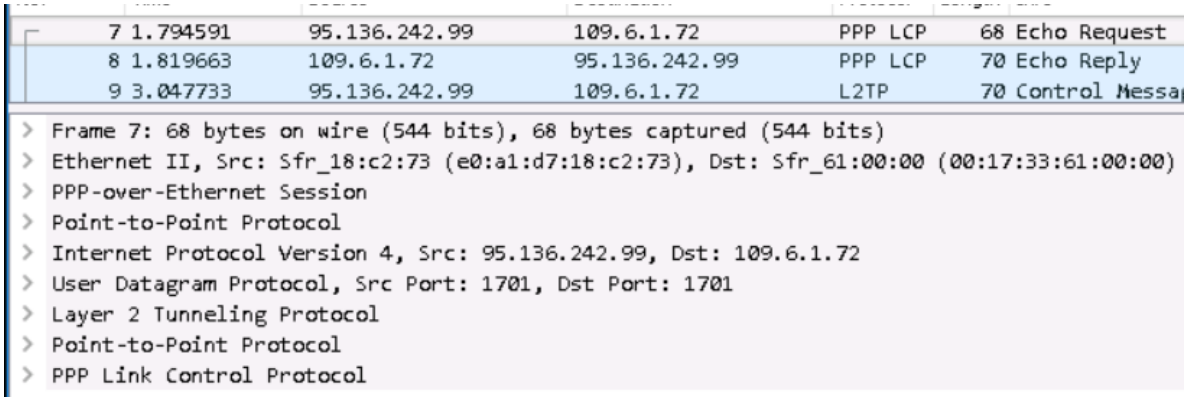
A screen capture showing the Ethernet source and Ethernet destination addresses

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 desitination adress 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`

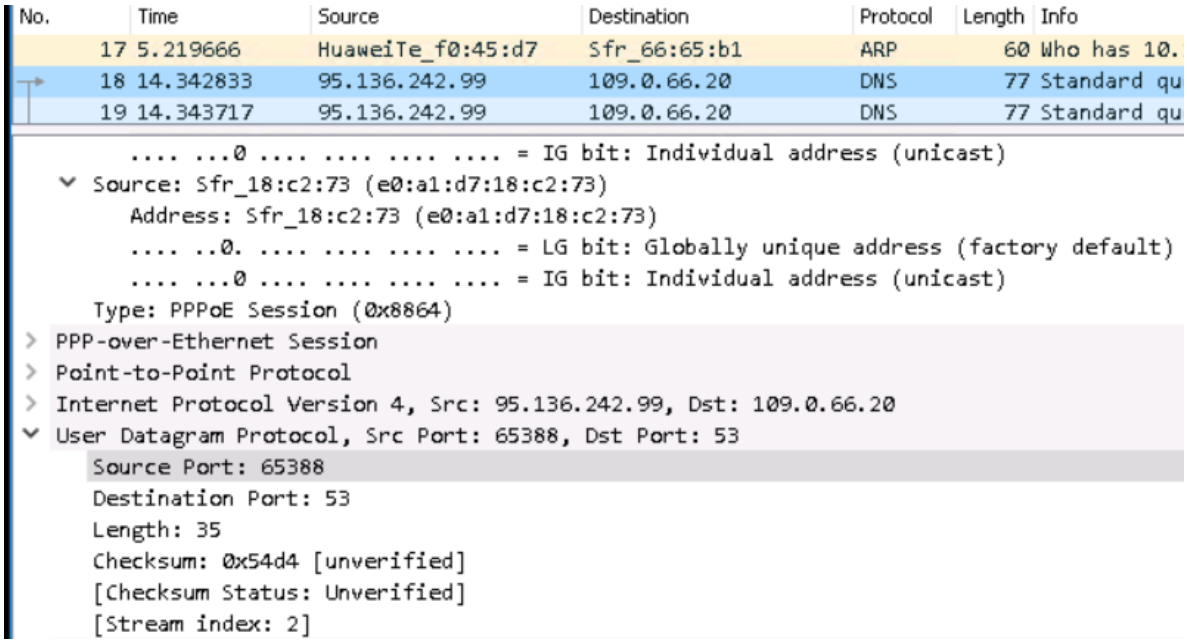
Section 2

Part 1

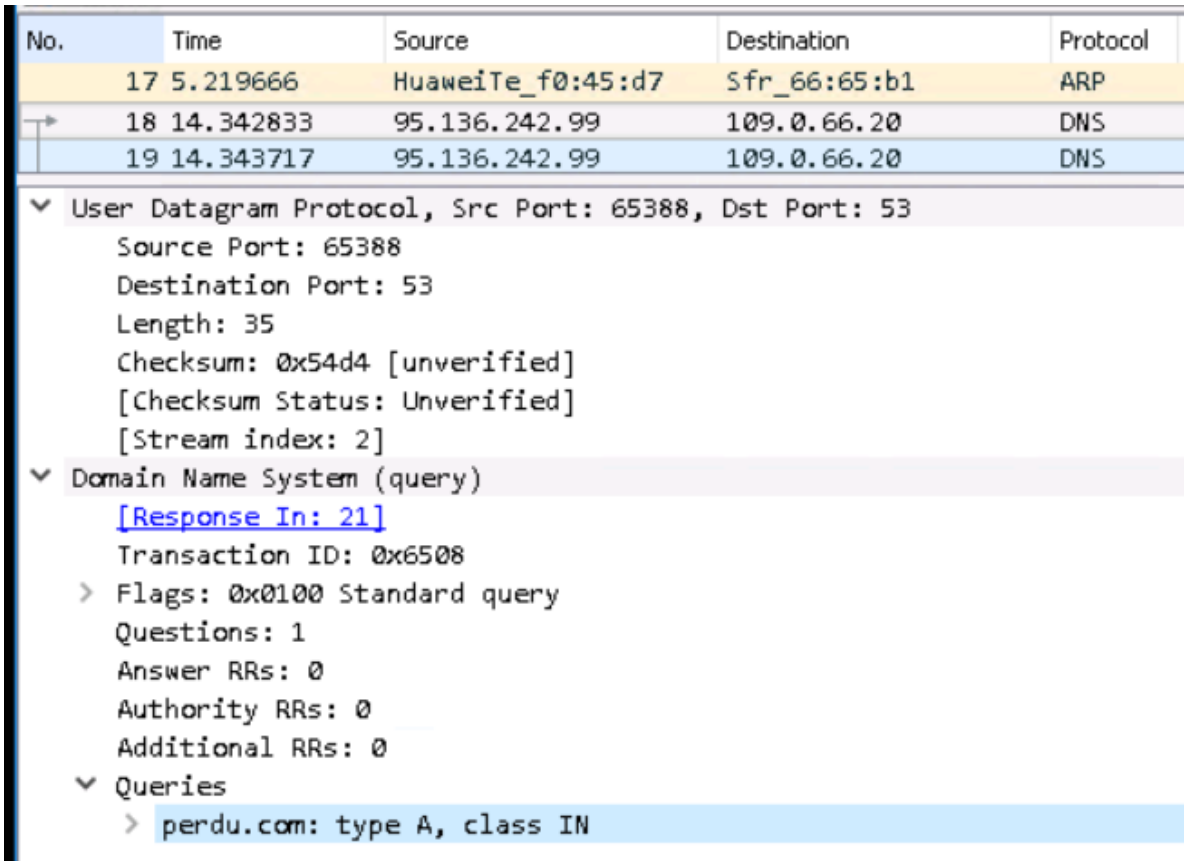
The list of protocols used in frame 7 displayed in Wireshark



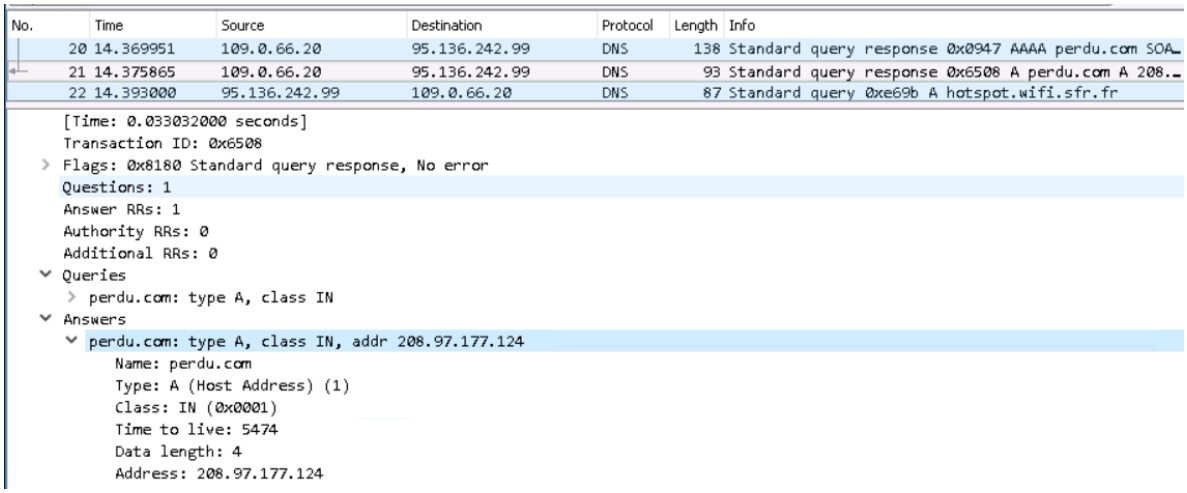
The source port used by UDP in frame 18, displayed in Wireshark



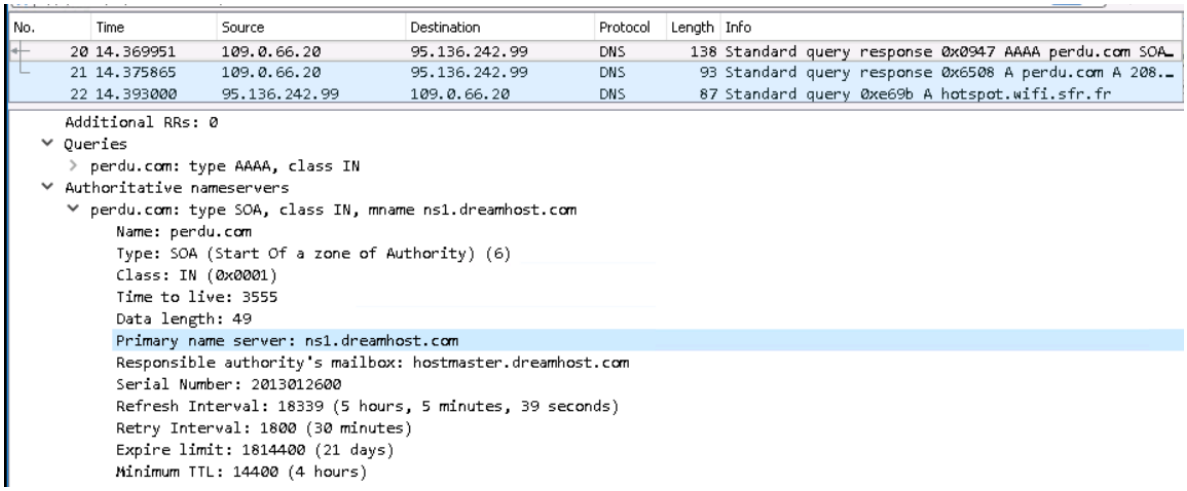
The domain queried in frame 18, displayed in Wireshark



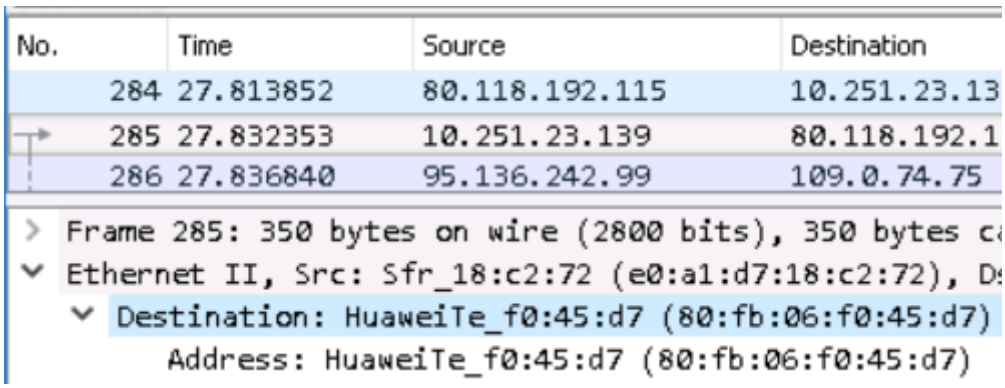
The address details shown in frame 21 (the response to frame 18) displayed in Wireshark



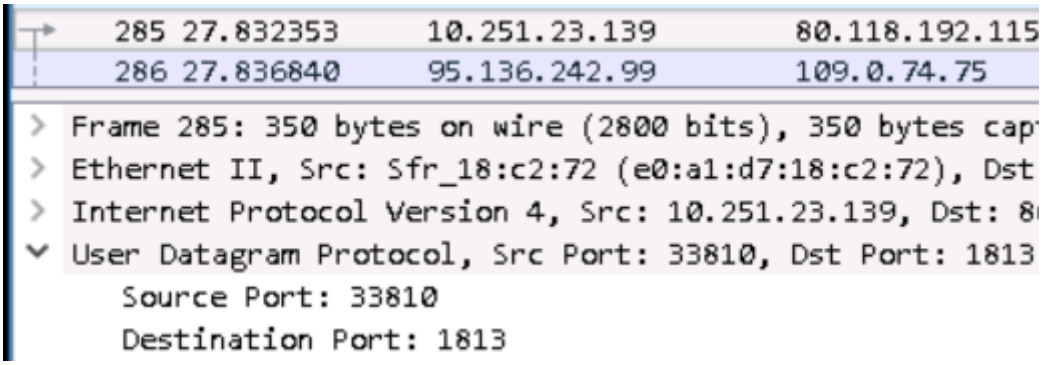
The authoritative nameserver in frame 20, displayed in Wireshark



The destination MAC address of frame 285, displayed in Wireshark



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



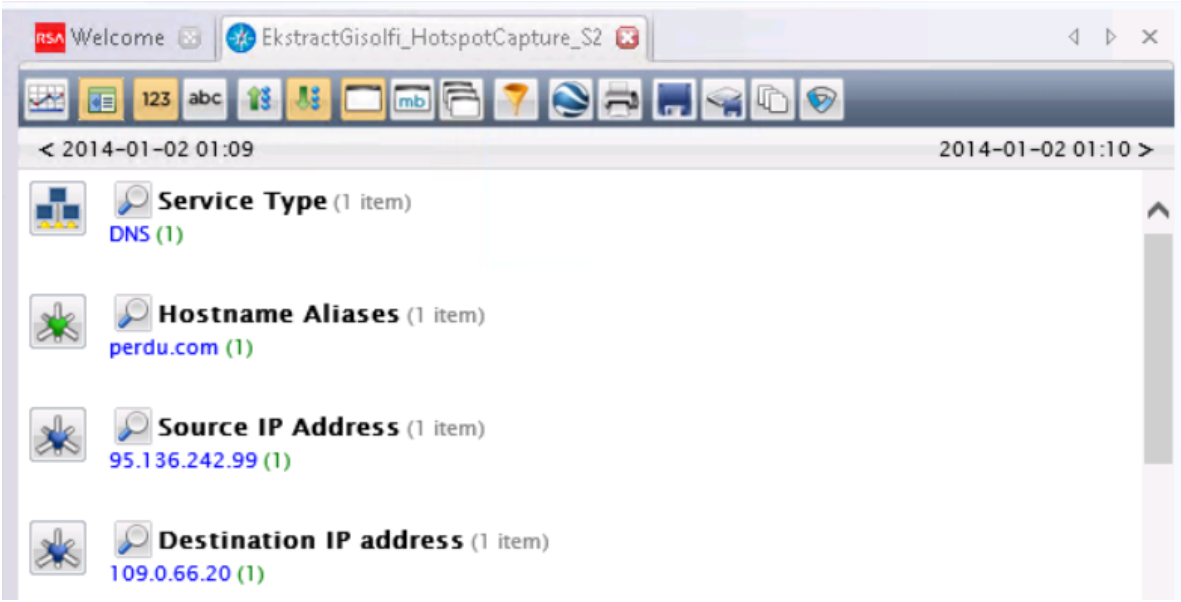
The attribute value pairs of frame 285, displayed in Wireshark

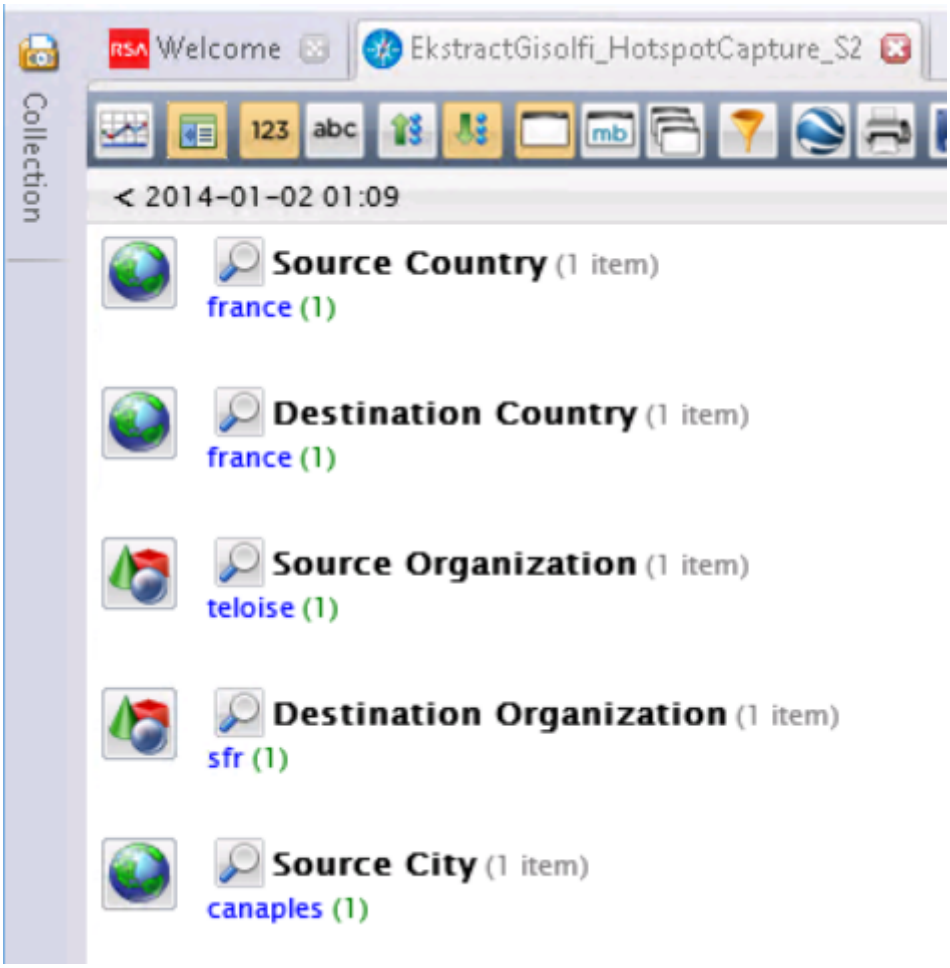
```
285 27.832353    10.251.23.139     80.118.192.115    RADIUS    350 Accounting-Request(4) (id=0, l
286 27.836840    95.136.242.99     109.0.74.75       TLSv1     727 Application Data

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