Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 02

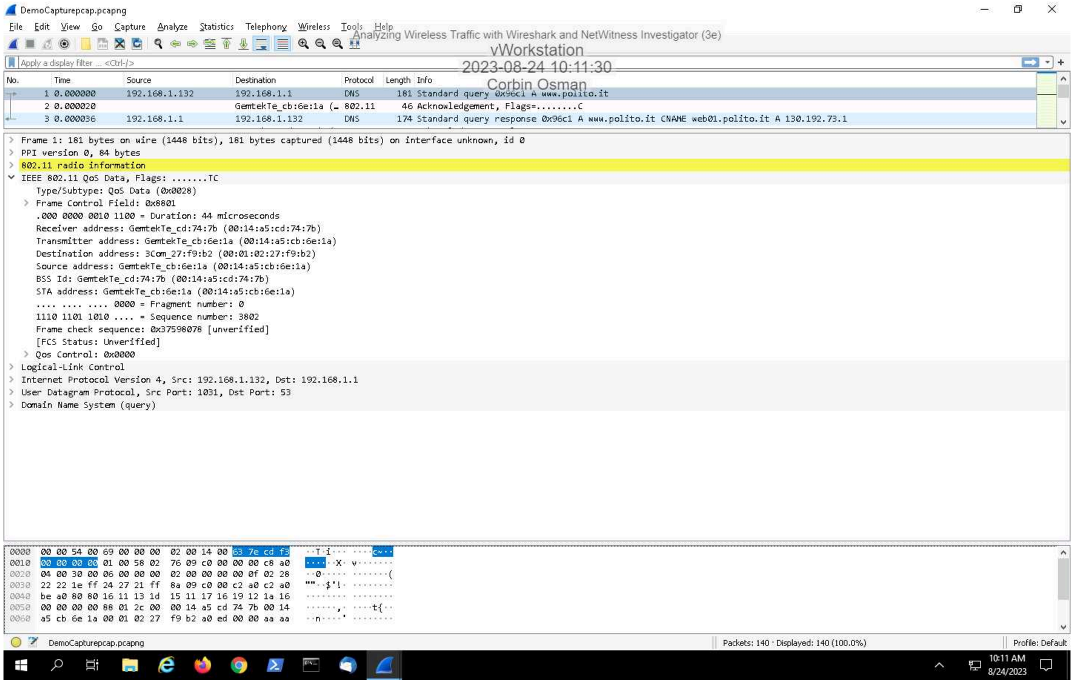
Student: Corbin Osman	Email: corbin.osman@mycampus.apus.edu
Time on Task: 2 hours, 15 minutes	Progress: 80%

Report Generated: Thursday, August 24, 2023 at 1:52 PM

Section 1: Hands-On Demonstration

Part 1: Analyze Wireless Traffic with Wireshark

16. **Make a screen capture** showing the **detail found in the IEEE 802.11 QoS Data fields**.

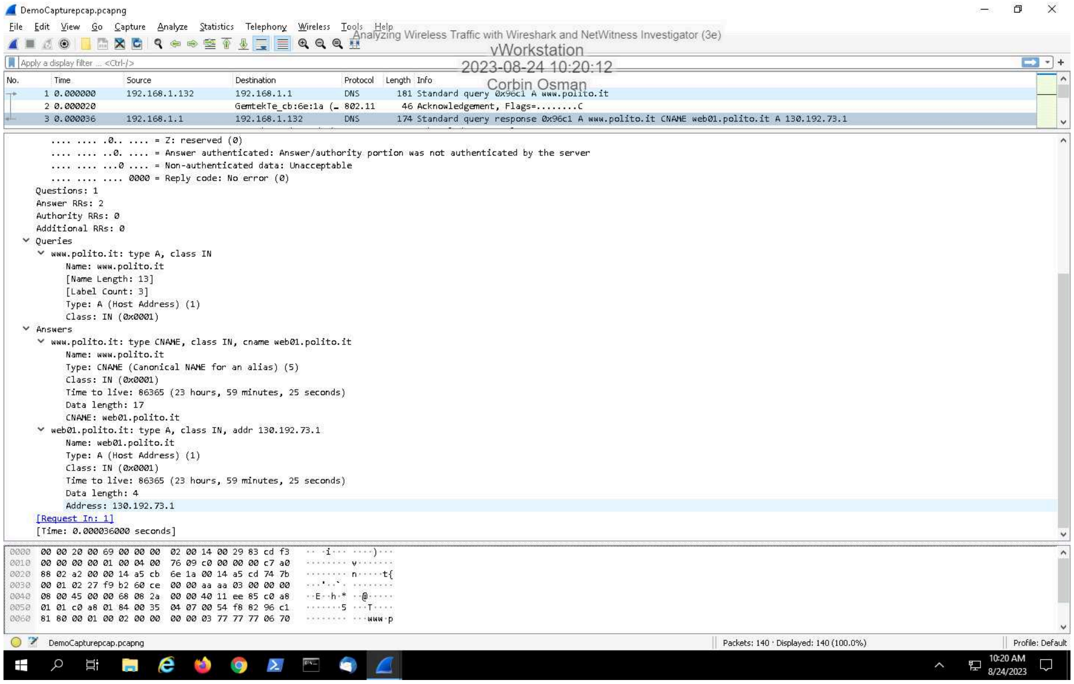

DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:11:30
Corbin Osman
Apply a display filter ... <Ctrl-/>

```
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 unknown, id 0
> PPI version 0, 84 bytes
> 802.11 radio information
v 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)
    Transmitter address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    Destination address: 3Com_27:f9:b2 (00:01:02:27:f9:b2)
    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 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
> 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)
```

```
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 a0   ······X· v·······
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ··0····· ·······(
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 16   ········ ········
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ······,· ····t{··
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ··n····' ········
```

35. **Make a screen capture** showing the **query name** (www.polito.it)**, the source IP address, and the destination IP address**.


DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
DemoCapturepcap.pcapng
Profile: Default
10:20 AM
8/24/2023

Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:20:12
Corbin Osman

```
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
```

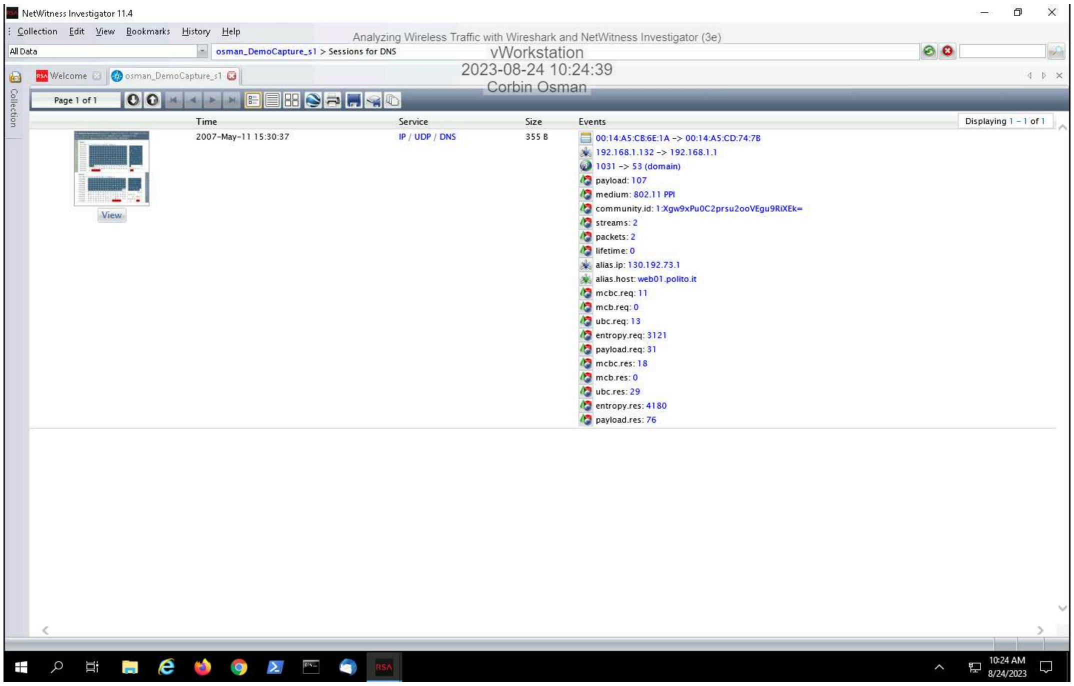
```
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    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)
  ˅ 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 (23 hours, 59 minutes, 25 seconds)
          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 (23 hours, 59 minutes, 25 seconds)
          Data length: 4
          Address: 130.192.73.1
    [Request In: 1]
    [Time: 0.000036000 seconds]
```

```
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·* ··@·····
0050  01 01 c0 a8 01 84 00 35  04 07 00 54 f8 82 96 c1   ·······5 ···T····
0060  81 80 00 01 00 02 00 00  00 00 03 77 77 77 06 70   ········ ···www·p
```

Packets: 140 · Displayed: 140 (100.0%)

Part 2: Analyze Wireless Traffic with NetWitness Investigator

9. **Make a screen capture** of the DNS query showing the **Hostname Alias, the Source IP Address, and the Destination IP Address fields**.



Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:24:39
Corbin Osman

osman_DemoCapture_s1 > Sessions for DNS

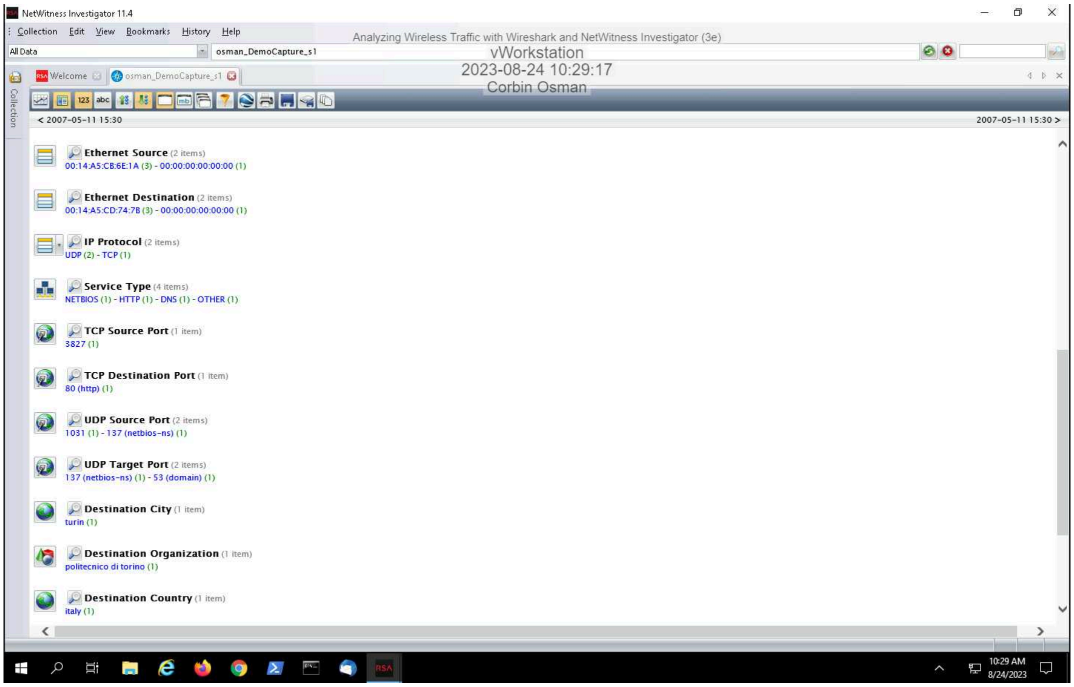
Displaying 1 – 1 of 1

Time	Service	Size	Events
2007–May–11 15:30:37	IP / UDP / DNS	355 B	00:14:A5:CB:6E:1A -> 00:14:A5:CD:74:7B 192.168.1.132 -> 192.168.1.1 1031 -> 53 (domain) payload: 107 medium: 802.11 PPI community.id: 1:Xgw9xPu0C2prsu2ooVEgu9RiXEk= streams: 2 packets: 2 lifetime: 0 alias.ip: 130.192.73.1 alias.host: web01.polito.it mcbc.req: 11 mcb.req: 0 ubc.req: 13 entropy.req: 3121 payload.req: 31 mcbc.res: 18 mcb.res: 0 ubc.res: 29 entropy.res: 4180 payload.res: 76

10. **Compare** the information provided by NetWitness to the screen capture you made of the query name (www.polito.it), the source IP address, and the destination IP address in Wireshark.

The query name of www.polito.it remained the same, and as found in Wireshark, packet one uses the 192.168.1.132 as the source with 192.168.1.1 as the destination. Packet three in Wireshark is the inverse. In NetWitness we see the DNS packet with the alias host as web01.polito.it, and it had the same source and destination IPs as Packet one from Wireshark.

13. **Make a screen capture** showing the **Ethernet source and Ethernet destination addresses**.



Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:29:17
Corbin Osman

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)

IP Protocol (2 items)
UDP (2) - TCP (1)

Service Type (4 items)
NETBIOS (1) - HTTP (1) - DNS (1) - OTHER (1)

TCP Source Port (1 item)
3827 (1)

TCP Destination Port (1 item)
80 (http) (1)

UDP Source Port (2 items)
1031 (1) - 137 (netbios-ns) (1)

UDP Target Port (2 items)
137 (netbios-ns) (1) - 53 (domain) (1)

Destination City (1 item)
turin (1)

Destination Organization (1 item)
politecnico di torino (1)

Destination Country (1 item)
italy (1)

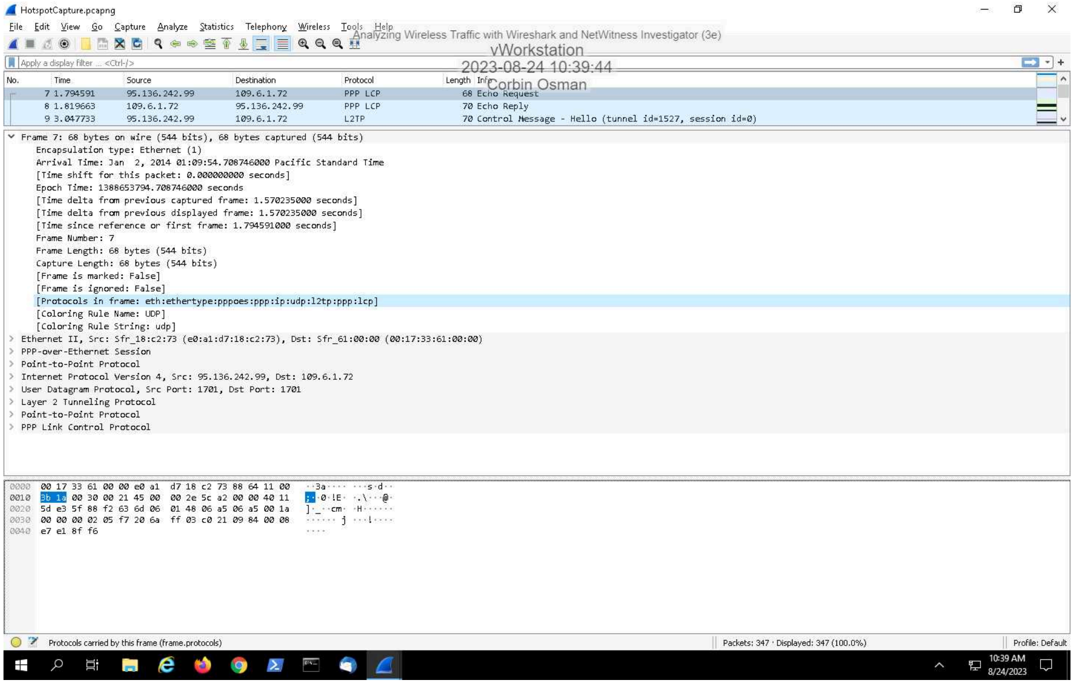
14. **Compare** the information provided by NetWitness to the screen capture you made of the detail found in the IEEE 802.11 QoS Data fields in Wireshark.

In Wireshark, the receiver address is the same as the ethernet destination address in NetWitness (00:14:A5:CD:74:7B), and the transmitter address is the same as the ethernet source address in NetWitness (00:14:A5:CB:6E:1A).

Section 2: Applied Learning

Part 1: Analyze Wireless Traffic with Wireshark

6. **Make a screen capture** showing **all protocols used in Packet 7**.



Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:39:44
Corbin Osman

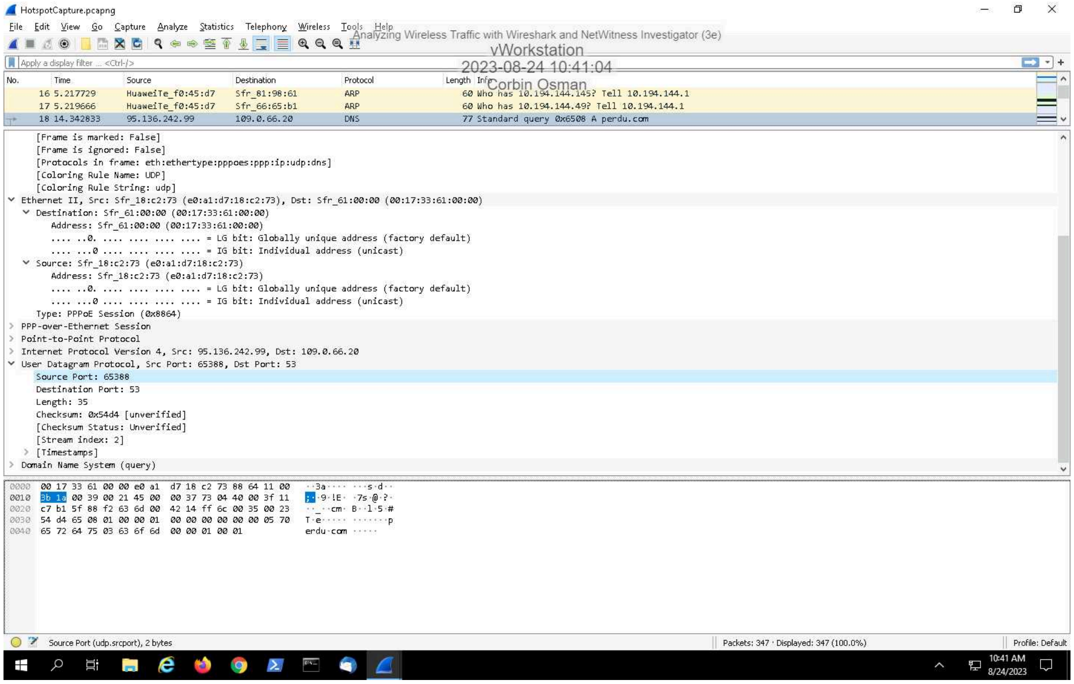
```
No.  Time       Source           Destination     Protocol   Length Info
   7 1.794591   95.136.242.99    109.6.1.72      PPP LCP        68 Echo Request
   8 1.819663   109.6.1.72       95.136.242.99   PPP LCP        70 Echo Reply
   9 3.047733   95.136.242.99    109.6.1.72      L2TP           70 Control Message - Hello (tunnel id=1527, session id=0)
```

```
v Frame 7: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan  2, 2014 01:09:54.708746000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1388653794.708746000 seconds
    [Time delta from previous captured frame: 1.570235000 seconds]
    [Time delta from previous displayed frame: 1.570235000 seconds]
    [Time since reference or first frame: 1.794591000 seconds]
    Frame Number: 7
    Frame Length: 68 bytes (544 bits)
    Capture Length: 68 bytes (544 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:l2tp:ppp:lcp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> 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
```

```
0000  00 17 33 61 00 00 e0 a1  d7 18 c2 73 88 64 11 00   ··3a····  ···s·d··
0010  3b 1a 00 30 00 21 45 00  00 2e 5c a2 00 00 40 11   ;··0·!E·  ·.\···@·
0020  5d e3 5f 88 f2 63 6d 06  01 48 06 a5 06 a5 00 1a   ]·_··cm·  ·H······
0030  00 00 00 02 05 f7 20 6a  ff 03 c0 21 09 84 00 08   ······ j  ···!····
0040  e7 e1 8f f6                                        ····
```

Protocols carried by this frame (frame.protocols) | Packets: 347 · Displayed: 347 (100.0%) | Profile: Default

12. **Make a screen capture** showing the **source port number used in Packet 18**.



Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:41:04
Corbin Osman

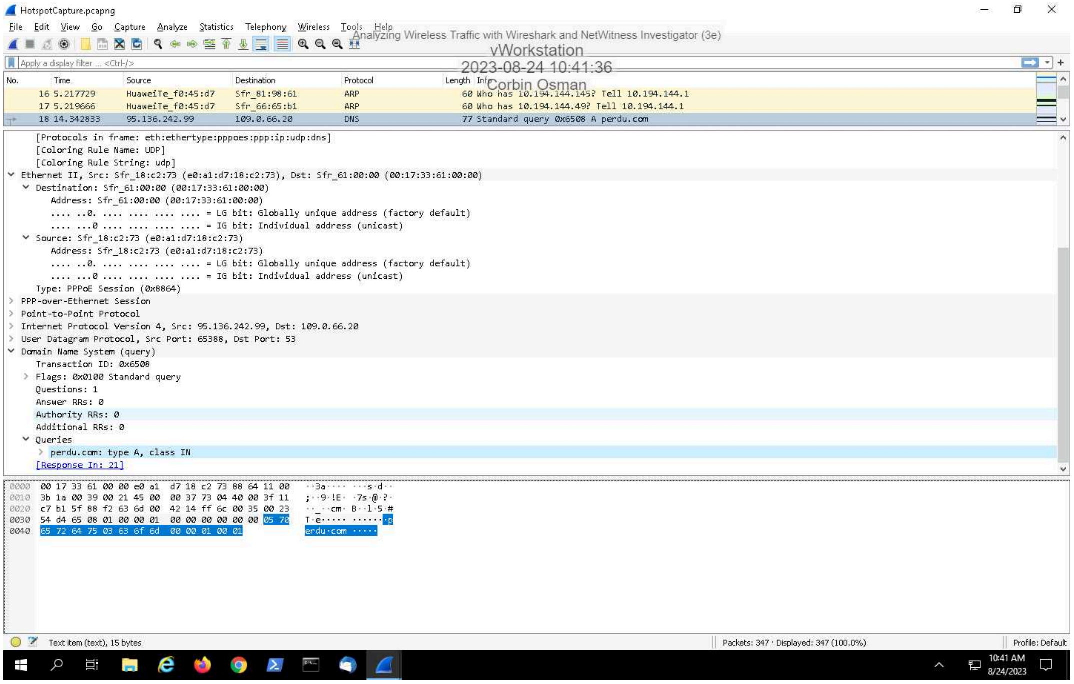
```
No.  Time       Source              Destination     Protocol   Length Info
  16 5.217729   HuaweiTe_f0:45:d7   Sfr_81:98:61    ARP            60 Who has 10.194.144.145? Tell 10.194.144.1
  17 5.219666   HuaweiTe_f0:45:d7   Sfr_66:65:b1    ARP            60 Who has 10.194.144.49? Tell 10.194.144.1
  18 14.342833  95.136.242.99       109.0.66.20     DNS            77 Standard query 0x6508 A perdu.com
```

```
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: Sfr_18:c2:73 (e0:a1:d7:18:c2:73), Dst: Sfr_61:00:00 (00:17:33:61:00:00)
  v Destination: Sfr_61:00:00 (00:17:33:61:00:00)
      Address: Sfr_61:00:00 (00:17:33:61:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v 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
v 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]
  > [Timestamps]
> Domain Name System (query)
```

```
0000  00 17 33 61 00 00 e0 a1  d7 18 c2 73 88 64 11 00   ··3a····  ···s·d··
0010  3b 1a 00 39 00 21 45 00  00 37 73 04 40 00 3f 11   ;··9·!E·  ·7s·@·?·
0020  c7 b1 5f 88 f2 63 6d 00  42 14 ff 6c 00 35 00 23   ··_··cm·  B··l·5·#
0030  54 d4 65 08 01 00 00 01  00 00 00 00 00 00 05 70   T·e·····  ·······p
0040  65 72 64 75 03 63 6f 6d  00 00 01 00 01            erdu·com  ·····
```

Source Port (udp.srcport), 2 bytes | Packets: 347 · Displayed: 347 (100.0%) | Profile: Default

14. **Make a screen capture** showing the **domain queried in Packet 18**.


HotspotCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:41:36
Corbin Osman
10:41 AM
8/24/2023

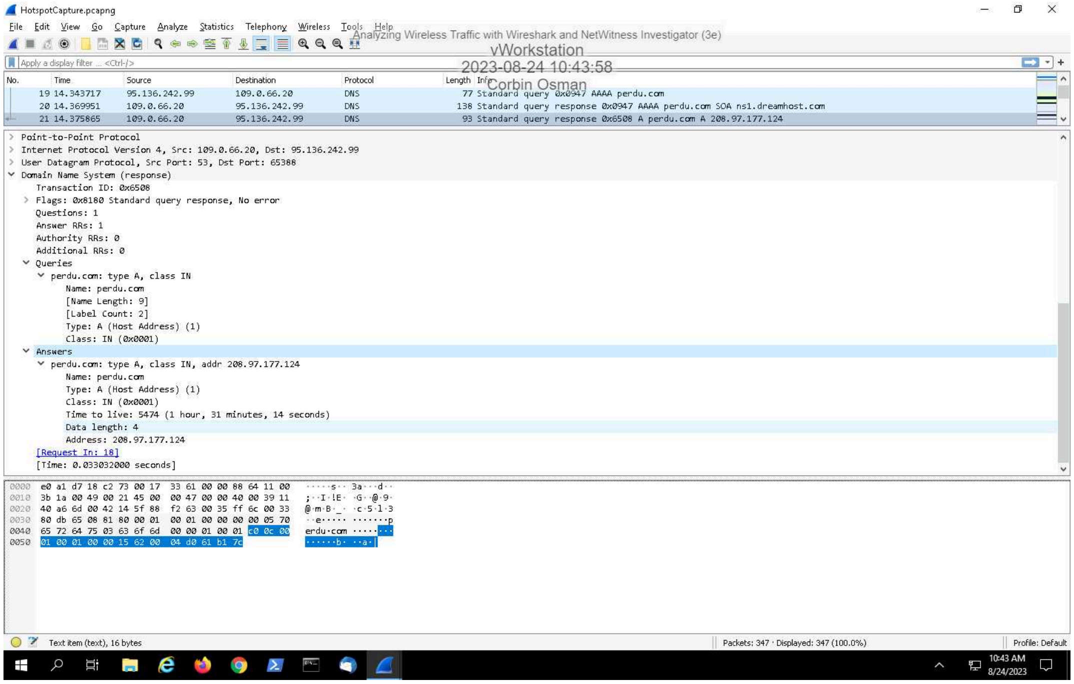
```
No.   Time        Source            Destination     Protocol   Length  Info
   16 5.217729    HuaweiTe_f0:45:d7 Sfr_81:98:61    ARP            60  Who has 10.194.144.145? Tell 10.194.144.1
   17 5.219666    HuaweiTe_f0:45:d7 Sfr_66:65:b1    ARP            60  Who has 10.194.144.49? Tell 10.194.144.1
   18 14.342833   95.136.242.99     109.0.66.20     DNS            77  Standard query 0x6508 A perdu.com
```

```
    [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: Sfr_18:c2:73 (e0:a1:d7:18:c2:73), Dst: Sfr_61:00:00 (00:17:33:61:00:00)
  v Destination: Sfr_61:00:00 (00:17:33:61:00:00)
      Address: Sfr_61:00:00 (00:17:33:61:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v 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
v Domain Name System (query)
    Transaction ID: 0x6508
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > perdu.com: type A, class IN
    [Response In: 21]
```

```
0000  00 17 33 61 00 00 e0 a1  d7 18 c2 73 88 64 11 00   ··3a····  ···s·d··
0010  3b 1a 00 39 00 21 45 00  00 37 73 04 40 00 3f 11   ;··9·!E·  ·7s·@·?·
0020  c7 b1 5f 88 f2 63 6d 00  42 14 ff 6c 00 35 00 23   ··_··cm·  B··l·5·#
0030  54 d4 65 08 01 00 00 01  00 00 00 00 00 00 05 70   T·e·····  ·······p
0040  65 72 64 75 03 63 6f 6d  00 00 01 00 01            erdu·com  ·····
```

```
Text item (text), 15 bytes          Packets: 347 · Displayed: 347 (100.0%)          Profile: Default
```

18. **Make a screen capture** showing the **address details in the related packet**.


HotspotCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:43:58
Corbin Osman
10:43 AM
8/24/2023

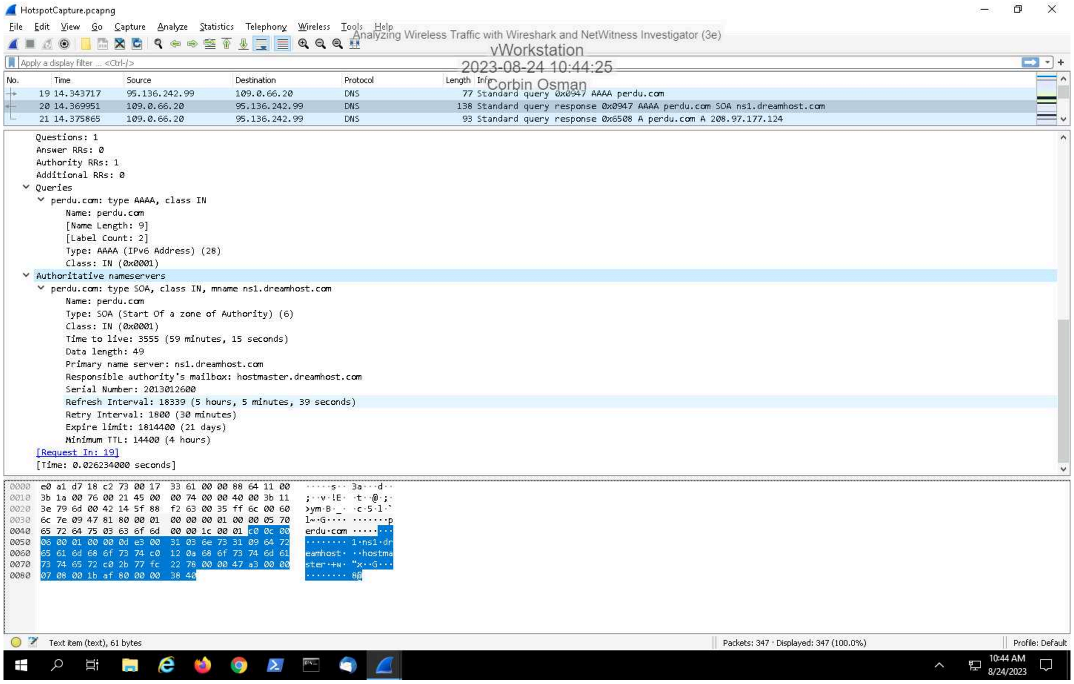
```
No.   Time        Source            Destination     Protocol   Length  Info
   19 14.343717   95.136.242.99     109.0.66.20     DNS            77  Standard query 0x0947 AAAA perdu.com
   20 14.369951   109.0.66.20       95.136.242.99   DNS           138  Standard query response 0x0947 AAAA perdu.com SOA ns1.dreamhost.com
   21 14.375865   109.0.66.20       95.136.242.99   DNS            93  Standard query response 0x6508 A perdu.com A 208.97.177.124
```

```
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 109.0.66.20, Dst: 95.136.242.99
> User Datagram Protocol, Src Port: 53, Dst Port: 65388
v Domain Name System (response)
    Transaction ID: 0x6508
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v perdu.com: type A, class IN
        Name: perdu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    v 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 (1 hour, 31 minutes, 14 seconds)
        Data length: 4
        Address: 208.97.177.124
    [Request In: 18]
    [Time: 0.033032000 seconds]
```

```
0000  e0 a1 d7 18 c2 73 00 17  33 61 00 00 88 64 11 00   ·····s··  3a···d··
0010  3b 1a 00 49 00 21 45 00  00 47 00 00 40 00 39 11   ;··I·!E·  ·G··@·9·
0020  40 a6 6d 00 42 14 5f 88  f2 63 00 35 ff 6c 00 33   @·m·B·_·  ·c·5·l·3
0030  80 db 65 08 81 80 00 01  00 01 00 00 00 00 05 70   ··e·····  ·······p
0040  65 72 64 75 03 63 6f 6d  00 00 01 00 01 c0 0c 00   erdu·com  ········
0050  01 00 01 00 00 15 62 00  04 d0 61 b1 7c            ······b·  ·a·|
```

```
Text item (text), 16 bytes          Packets: 347 · Displayed: 347 (100.0%)          Profile: Default
```

20. **Make a screen capture** showing the **authoritative nameserver in Packet 20**.


HotspotCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:44:25
Corbin Osman

```
No.  Time       Source          Destination     Protocol  Length Info
  19 14.343717  95.136.242.99   109.0.66.20     DNS           77 Standard query 0x0947 AAAA perdu.com
  20 14.369951  109.0.66.20     95.136.242.99   DNS          138 Standard query response 0x0947 AAAA perdu.com SOA ns1.dreamhost.com
  21 14.375865  109.0.66.20     95.136.242.99   DNS           93 Standard query response 0x6508 A perdu.com A 208.97.177.124
```

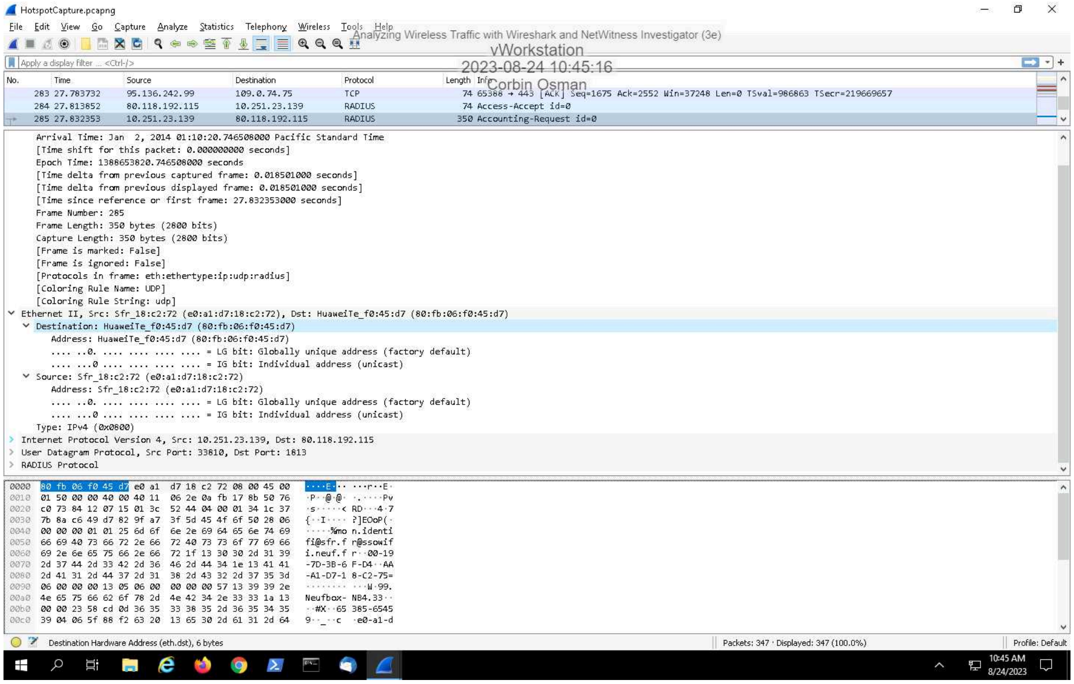
```
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v perdu.com: type AAAA, class IN
        Name: perdu.com
        [Name Length: 9]
        [Label Count: 2]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
  v Authoritative nameservers
    v 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 (59 minutes, 15 seconds)
        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)
    [Request In: 19]
    [Time: 0.026234000 seconds]
```

```
0000  e0 a1 d7 18 c2 73 00 17  33 61 00 00 88 64 11 00   ·····s·· 3a···d··
0010  3b 1a 00 76 00 21 45 00  00 74 00 00 40 00 3b 11   ;··v·!E· ·t··@·;·
0020  3e 79 6d 00 42 14 5f 88  f2 63 00 35 ff 6c 00 60   >ym·B·_· ·c·5·l·`
0030  6c 7e 09 47 81 80 00 01  00 00 00 01 00 00 05 70   l~·G···· ·······p
0040  65 72 64 75 03 63 6f 6d  00 00 1c 00 01 c0 0c 00   erdu·com ········
0050  06 00 01 00 00 0d e3 00  31 03 6e 73 31 09 64 72   ········ 1·ns1·dr
0060  65 61 6d 68 6f 73 74 c0  12 0a 68 6f 73 74 6d 61   eamhost· ··hostma
0070  73 74 65 72 c0 2b 77 fc  22 78 00 00 47 a3 00 00   ster·+w· "x··G···
0080  07 08 00 1b af 80 00 00  38 40                     ········ 8@
```

Text item (text), 61 bytes | Packets: 347 · Displayed: 347 (100.0%) | Profile: Default

10:44 AM
8/24/2023

22. **Make a screen capture** showing the **destination MAC address in Packet 285**.


HotspotCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:45:16
Corbin Osman

```
No.  Time       Source          Destination     Protocol  Length Info
 283 27.783732  95.136.242.99   109.0.74.75     TCP           74 65388 → 443 [ACK] Seq=1675 Ack=2552 Win=37248 Len=0 TSval=986863 TSecr=219669657
 284 27.813852  80.118.192.115  10.251.23.139   RADIUS        74 Access-Accept id=0
 285 27.832353  10.251.23.139   80.118.192.115  RADIUS       350 Accounting-Request id=0
```

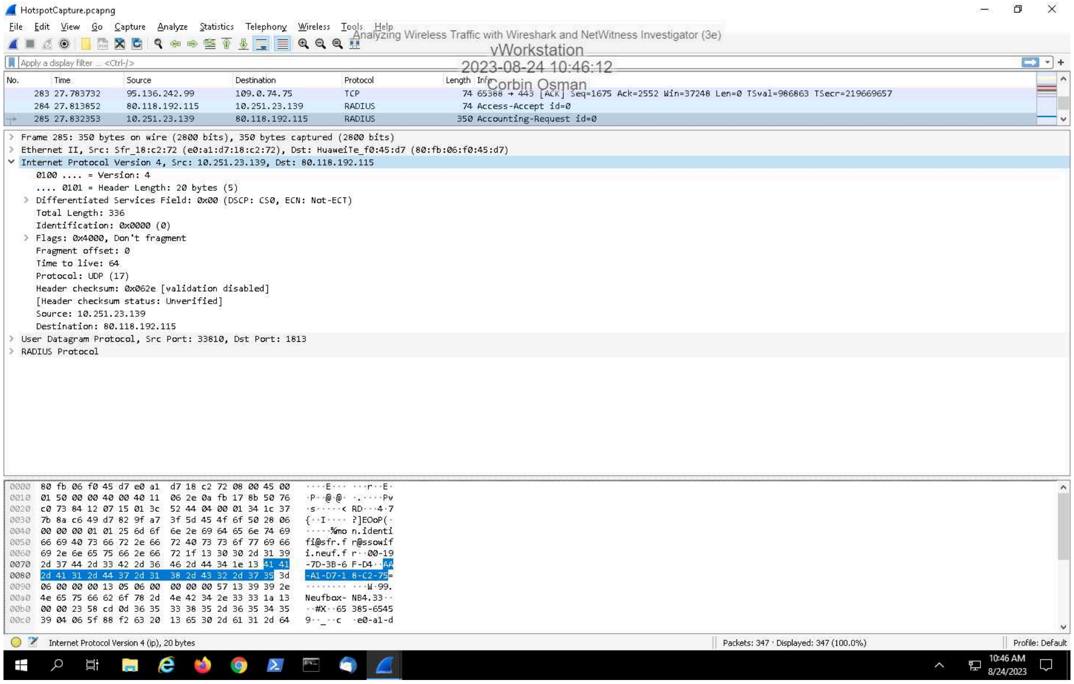
```
    Arrival Time: Jan  2, 2014 01:10:20.746508000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1388653820.746508000 seconds
    [Time delta from previous captured frame: 0.018501000 seconds]
    [Time delta from previous displayed frame: 0.018501000 seconds]
    [Time since reference or first frame: 27.832353000 seconds]
    Frame Number: 285
    Frame Length: 350 bytes (2800 bits)
    Capture Length: 350 bytes (2800 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:radius]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
  v Destination: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
      Address: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Sfr_18:c2:72 (e0:a1:d7:18:c2:72)
      Address: Sfr_18:c2:72 (e0:a1:d7:18:c2:72)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.251.23.139, Dst: 80.118.192.115
> User Datagram Protocol, Src Port: 33810, Dst Port: 1813
> RADIUS Protocol
```

```
0000  80 fb 06 f0 45 d7 e0 a1  d7 18 c2 72 08 00 45 00   ····E··· ···r··E·
0010  01 50 00 00 40 00 40 11  06 2e 0a fb 17 8b 50 76   ·P··@·@· ·.····Pv
0020  c0 73 84 12 07 15 01 3c  52 44 04 00 01 34 1c 37   ·s·····< RD···4·7
0030  7b 8a c6 49 d7 82 9f a7  3f 5d 45 4f 6f 50 28 06   {··I···· ?]EOoP(·
0040  00 00 00 01 01 25 6d 6f  6e 2e 69 64 65 6e 74 69   ·····%mo n.identi
0050  66 69 40 73 66 72 2e 66  72 40 73 73 6f 77 69 66   fi@sfr.f r@ssowif
0060  69 2e 6e 65 75 66 2e 66  72 1f 13 30 30 2d 31 39   i.neuf.f r··00-19
0070  2d 37 44 2d 33 42 2d 36  46 2d 44 34 1e 13 41 41   -7D-3B-6 F-D4··AA
0080  2d 41 31 2d 44 37 2d 31  38 2d 43 32 2d 37 35 3d   -A1-D7-1 8-C2-75=
0090  06 00 00 00 13 05 06 00  00 00 00 57 13 39 39 2e   ········ ···W·99.
00a0  4e 65 75 66 62 6f 78 2d  4e 42 34 2e 33 33 1a 13   Neufbox- NB4.33··
00b0  00 00 23 58 cd 0d 36 35  33 38 35 2d 36 35 34 35   ··#X··65 385-6545
00c0  39 04 06 5f 88 f2 63 20  13 65 30 2d 61 31 2d 64   9··_··c  ·e0-a1-d
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 347 · Displayed: 347 (100.0%) | Profile: Default

10:45 AM
8/24/2023

24. **Make a screen capture** showing the **source port and destination port in Packet 285**.


HotspotCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

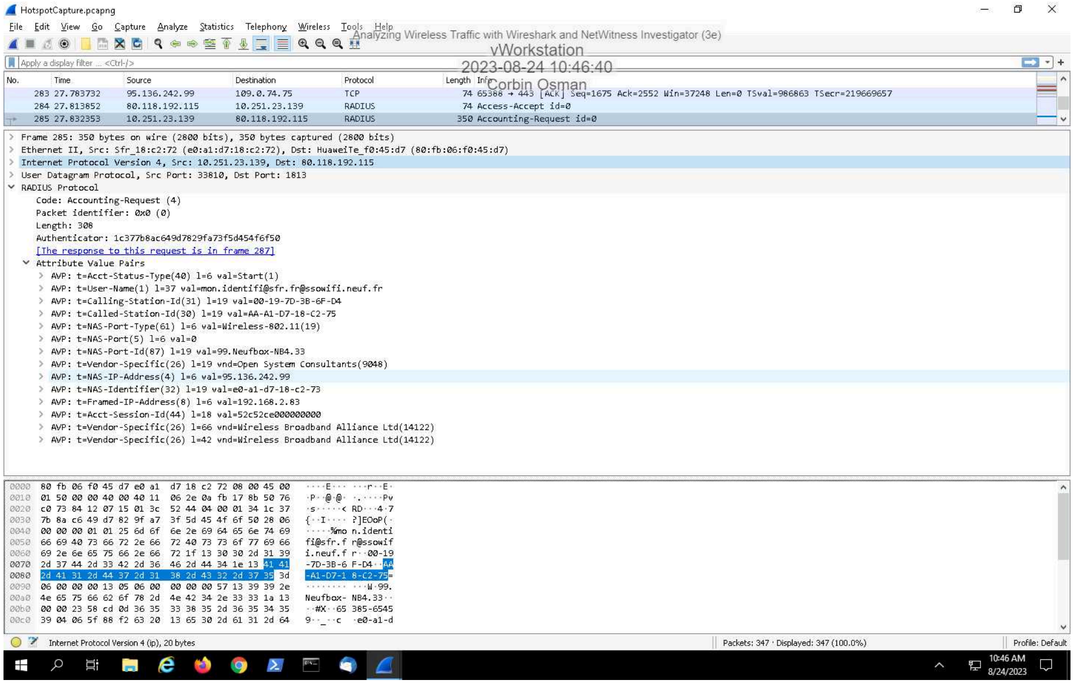
```
No.   Time        Source          Destination     Protocol  Length Info
  283 27.783732   95.136.242.99   109.0.74.75     TCP         74 65388 → 443 [ACK] Seq=1675 Ack=2552 Win=37248 Len=0 TSval=986863 TSecr=219669657
  284 27.813852   80.118.192.115  10.251.23.139   RADIUS      74 Access-Accept id=0
  285 27.832353   10.251.23.139   80.118.192.115  RADIUS     350 Accounting-Request id=0
```

```
> Frame 285: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)
> Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
v Internet Protocol Version 4, Src: 10.251.23.139, Dst: 80.118.192.115
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 336
    Identification: 0x0000 (0)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x062e [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.251.23.139
    Destination: 80.118.192.115
> User Datagram Protocol, Src Port: 33810, Dst Port: 1813
> RADIUS Protocol
```

```
0000  80 fb 06 f0 45 d7 e0 a1  d7 18 c2 72 08 00 45 00   ····E··· ···r··E·
0010  01 50 00 00 40 00 40 11  06 2e 0a fb 17 8b 50 76   ·P··@·@· ·.····Pv
0020  c0 73 84 12 07 15 01 3c  52 44 04 00 01 34 1c 37   ·s·····< RD···4·7
0030  7b 8a c6 49 d7 82 9f a7  3f 5d 45 4f 6f 50 28 06   {··I···· ?]EOoP(·
0040  00 00 00 01 01 25 6d 6f  6e 2e 69 64 65 6e 74 69   ·····%mo n.identi
0050  66 69 40 73 66 72 2e 66  72 40 73 73 6f 77 69 66   fi@sfr.f r@ssowif
0060  69 2e 6e 65 75 66 2e 66  72 1f 13 30 30 2d 31 39   i.neuf.f r··00-19
0070  2d 37 44 2d 33 42 2d 36  46 2d 44 34 1e 13 41 41   -7D-3B-6 F-D4··AA
0080  2d 41 31 2d 44 37 2d 31  38 2d 43 32 2d 37 35 3d   -A1-D7-1 8-C2-75=
0090  06 00 00 00 13 05 06 00  00 00 00 57 13 39 39 2e   ········ ···W·99.
00a0  4e 65 75 66 62 6f 78 2d  4e 42 34 2e 33 33 1a 13   Neufbox- NB4.33··
00b0  00 00 23 58 cd 0d 36 35  33 38 35 2d 36 35 34 35   ··#X··65 385-6545
00c0  39 04 06 5f 88 f2 63 20  13 65 30 2d 61 31 2d 64   9··_··c  ·e0-a1-d
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 347 · Displayed: 347 (100.0%) | Profile: Default

26. **Make a screen capture** showing the **Attribute Value Pairs in Packet 285**.


HotspotCapture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source          Destination     Protocol  Length Info
  283 27.783732   95.136.242.99   109.0.74.75     TCP         74 65388 → 443 [ACK] Seq=1675 Ack=2552 Win=37248 Len=0 TSval=986863 TSecr=219669657
  284 27.813852   80.118.192.115  10.251.23.139   RADIUS      74 Access-Accept id=0
  285 27.832353   10.251.23.139   80.118.192.115  RADIUS     350 Accounting-Request id=0
```

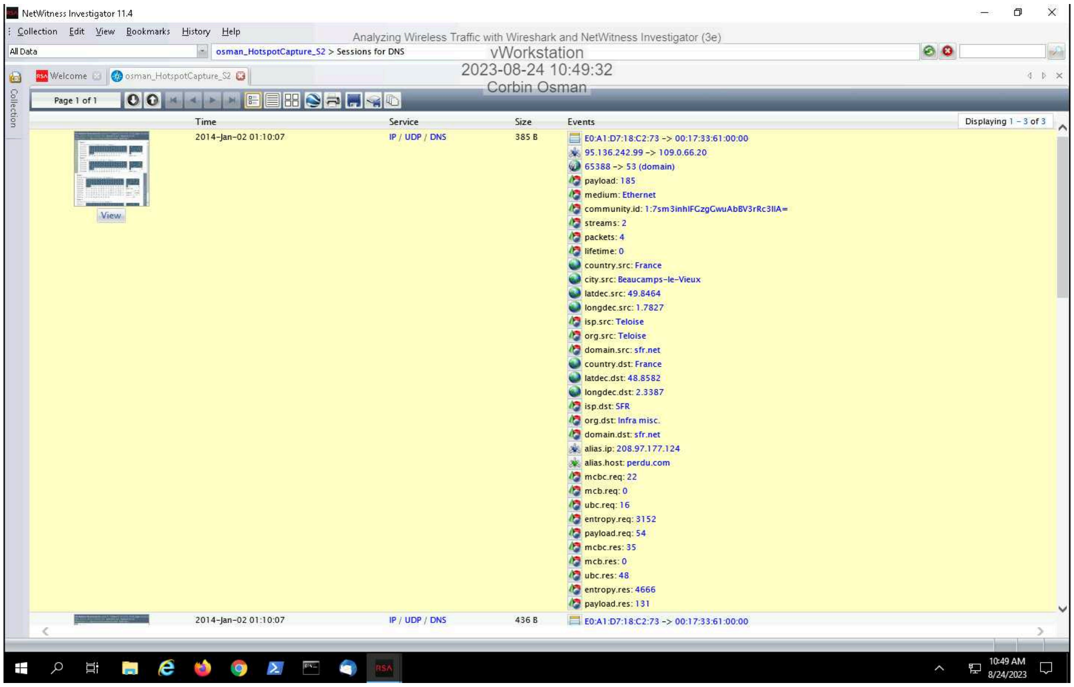
```
> Frame 285: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits)
> Ethernet II, Src: Sfr_18:c2:72 (e0:a1:d7:18:c2:72), Dst: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
> Internet Protocol Version 4, Src: 10.251.23.139, Dst: 80.118.192.115
> User Datagram Protocol, Src Port: 33810, Dst Port: 1813
v RADIUS Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0x0 (0)
    Length: 308
    Authenticator: 1c377b8ac649d7829fa73f5d454f6f50
    [The response to this request is in frame 287]
  v Attribute Value Pairs
    > AVP: t=Acct-Status-Type(40) l=6 val=Start(1)
    > AVP: t=User-Name(1) l=37 val=mon.identifi@sfr.fr@ssowifi.neuf.fr
    > AVP: t=Calling-Station-Id(31) l=19 val=00-19-7D-3B-6F-D4
    > AVP: t=Called-Station-Id(30) l=19 val=AA-A1-D7-18-C2-75
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=NAS-Port(5) l=6 val=0
    > AVP: t=NAS-Port-Id(87) l=19 val=99.Neufbox-NB4.33
    > AVP: t=Vendor-Specific(26) l=19 vnd=Open System Consultants(9048)
    > AVP: t=NAS-IP-Address(4) l=6 val=95.136.242.99
    > AVP: t=NAS-Identifier(32) l=19 val=e0-a1-d7-18-c2-73
    > AVP: t=Framed-IP-Address(8) l=6 val=192.168.2.83
    > AVP: t=Acct-Session-Id(44) l=18 val=52c52ce000000000
    > AVP: t=Vendor-Specific(26) l=66 vnd=Wireless Broadband Alliance Ltd(14122)
    > AVP: t=Vendor-Specific(26) l=42 vnd=Wireless Broadband Alliance Ltd(14122)
```

```
0000  80 fb 06 f0 45 d7 e0 a1  d7 18 c2 72 08 00 45 00   ····E··· ···r··E·
0010  01 50 00 00 40 00 40 11  06 2e 0a fb 17 8b 50 76   ·P··@·@· ·.····Pv
0020  c0 73 84 12 07 15 01 3c  52 44 04 00 01 34 1c 37   ·s·····< RD···4·7
0030  7b 8a c6 49 d7 82 9f a7  3f 5d 45 4f 6f 50 28 06   {··I···· ?]EOoP(·
0040  00 00 00 01 01 25 6d 6f  6e 2e 69 64 65 6e 74 69   ·····%mo n.identi
0050  66 69 40 73 66 72 2e 66  72 40 73 73 6f 77 69 66   fi@sfr.f r@ssowif
0060  69 2e 6e 65 75 66 2e 66  72 1f 13 30 30 2d 31 39   i.neuf.f r··00-19
0070  2d 37 44 2d 33 42 2d 36  46 2d 44 34 1e 13 41 41   -7D-3B-6 F-D4··AA
0080  2d 41 31 2d 44 37 2d 31  38 2d 43 32 2d 37 35 3d   -A1-D7-1 8-C2-75=
0090  06 00 00 00 13 05 06 00  00 00 00 57 13 39 39 2e   ········ ···W·99.
00a0  4e 65 75 66 62 6f 78 2d  4e 42 34 2e 33 33 1a 13   Neufbox- NB4.33··
00b0  00 00 23 58 cd 0d 36 35  33 38 35 2d 36 35 34 35   ··#X··65 385-6545
00c0  39 04 06 5f 88 f2 63 20  13 65 30 2d 61 31 2d 64   9··_··c  ·e0-a1-d
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 347 · Displayed: 347 (100.0%) | Profile: Default

Part 2: Analyze Wireless Traffic with NetWitness Investigator

6. **Make a screen capture** showing the **Hostname Alias, the Source IP Address, the Destination IP Address, and source city fields of the perdu.com DNS session**.

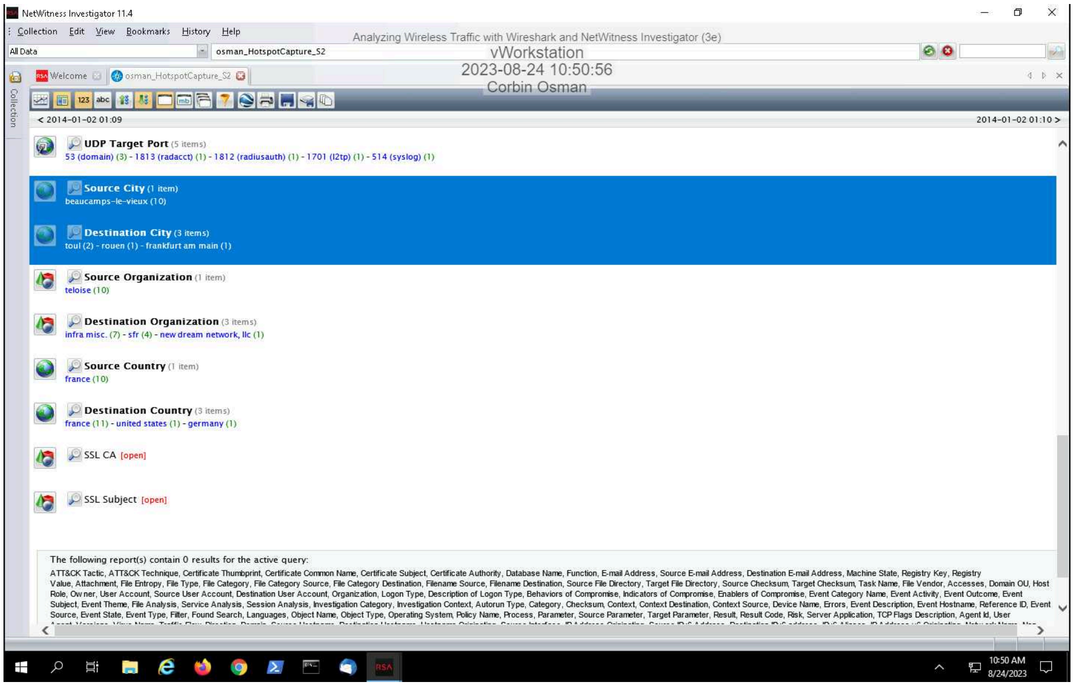

NetWitness Investigator 11.4
Collection Edit View Bookmarks History Help
All Data
osman_HotspotCapture_S2 > Sessions for DNS
Welcome
osman_HotspotCapture_S2
Page 1 of 1
Collection
View
10:49 AM
8/24/2023

Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:49:32
Corbin Osman

Time	Service	Size	Events
2014-Jan-02 01:10:07	IP / UDP / DNS	385 B	E0:A1:D7:18:C2:73 -> 00:17:33:61:00:00 95.136.242.99 -> 109.0.66.20 65388 -> 53 (domain) payload: 185 medium: Ethernet community.id: 1:7sm3inhIFGzgGwuAbBV3rRc3IIA= streams: 2 packets: 4 lifetime: 0 country.src: France city.src: Beaucamps-le-Vieux latdec.src: 49.8464 longdec.src: 1.7827 isp.src: Teloise org.src: Teloise domain.src: sfr.net country.dst: France latdec.dst: 48.8582 longdec.dst: 2.3387 isp.dst: SFR org.dst: Infra misc. domain.dst: sfr.net alias.ip: 208.97.177.124 alias.host: perdu.com mcbc.req: 22 mcb.req: 0 ubc.req: 16 entropy.req: 3152 payload.req: 54 mcbc.res: 35 mcb.res: 0 ubc.res: 48 entropy.res: 4666 payload.res: 131
2014-Jan-02 01:10:07	IP / UDP / DNS	436 B	E0:A1:D7:18:C2:73 -> 00:17:33:61:00:00

Displaying 1 – 3 of 3

9. **Make a screen capture** showing the **source and destination cities**.



Analyzing Wireless Traffic with Wireshark and NetWitness Investigator (3e)
vWorkstation
2023-08-24 10:50:56
Corbin Osman

< 2014-01-02 01:09 — 2014-01-02 01:10 >

UDP Target Port (5 items)
53 (domain) (3) - 1813 (radacct) (1) - 1812 (radiusauth) (1) - 1701 (l2tp) (1) - 514 (syslog) (1)

Source City (1 item)
beaucamps-le-vieux (10)

Destination City (3 items)
toul (2) - rouen (1) - frankfurt am main (1)

Source Organization (1 item)
teloise (10)

Destination Organization (3 items)
infra misc. (7) - sfr (4) - new dream network, llc (1)

Source Country (1 item)
france (10)

Destination Country (3 items)
france (11) - united states (1) - germany (1)

SSL CA [open]

SSL Subject [open]

The following report(s) contain 0 results for the active query:
ATT&CK Tactic, ATT&CK Technique, Certificate Thumbprint, Certificate Common Name, Certificate Subject, Certificate Authority, Database Name, Function, E-mail Address, Source E-mail Address, Destination E-mail Address, Machine State, Registry Key, Registry Value, Attachment, File Entropy, File Type, File Category, File Category Source, File Category Destination, Filename Source, Filename Destination, Source File Directory, Target File Directory, Source Checksum, Target Checksum, Task Name, File Vendor, Accesses, Domain OU, Host Role, Ow ner, User Account, Source User Account, Destination User Account, Organization, Logon Type, Description of Logon Type, Behaviors of Compromise, Indicators of Compromise, Enablers of Compromise, Event Category Name, Event Activity, Event Outcome, Event Subject, Event Theme, File Analysis, Service Analysis, Session Analysis, Investigation Category, Investigation Context, Autorun Type, Category, Checksum, Context, Context Destination, Context Source, Device Name, Errors, Event Description, Event Hostname, Reference ID, Event Source, Event State, Event Type, Filter, Found Search, Languages, Object Name, Object Type, Operating System, Policy Name, Process, Parameter, Source Parameter, Target Parameter, Result, Result Code, Risk, Server Application, TCP Flags Description, Agent Id, User

Section 3: Challenge and Analysis

Part 1: Research Network Forensics Tools

Provide a **brief summary** of three other solutions. Be sure to include the product name, key features, cost (or if it is freely available), and any other relevant details that would make it a popular choice among network forensics investigators.

Incomplete

Part 2: Investigate Suspicious Web Traffic

Using Wireshark and NetWitness, **identify** the IP address that was resolved for the www.perdu.com website, as well as the destination port number.

Incomplete

Using Wireshark and NetWitness, **identify** the actual geographic location of the web server that hosts perdu.com.

Incomplete

Part 3: Create a Visual Presentation of Your Findings

Make a screen capture showing the **geographic location of the IP address associated with perdu.com in Google Earth**.

Incomplete