



© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.

## Network Traffic Analysis

### DNS (Easy)

This challenge evaluates the contestant's ability to understand a packet capture containing network traffic using the DNS protocol. Use [Wireshark](#) to solve the challenge.

Questions 1 and 2 can be solved by looking for a packet with "Standard query" in the info column (packet #4). Once found, the Wireshark dissector will yield the answers.

```
> Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: CadmusCo_97:3f:45 (08:00:27:97:3f:45), Dst: CadmusCo_38:db:ed (08:00:27:38:db:ed)
> Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
> Transmission Control Protocol, Src Port: 1042 (1042), Dst Port: 53 (53), Seq: 1, Ack: 1, Len: 30
▼ Domain Name System (query)
  [Response In: 5]
  Length: 28
  Transaction ID: 0x0000
  > Flags: 0x0000 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > etas.com: type AXFR, class IN
```

© 2017 Cyber Skyline



© 2017 Cyber Skyline. All Rights Reserved.  
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Questions 3 – 5 can be solved by looking for a packet with “Standard query response” in the info column (packet #5). Once found, the Wireshark dissector will yield the answers.

```

▼ Domain Name System (response)
  [Request In: 4]
  [Time: 0.000778000 seconds]
  Length: 195
  Transaction ID: 0x0000
  > Flags: 0x8080 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    > etas.com: type AXFR, class IN
  ▼ Answers
    ▼ etas.com: type SOA, class IN, mname training2003p
      Name: etas.com
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 3600
      Data length: 47
      Primary name server: training2003p
      Responsible authority's mailbox: hostmaster
      Serial Number: 3
      Refresh Interval: 60 (1 minute)
      Retry Interval: 600 (10 minutes)
      Expire limit: 86400 (1 day)
      Minimum TTL: 3600 (1 hour)
    > etas.com: type NS, class IN, ns training2003p
    > welcome.etas.com: type A, class IN, addr 1.1.1.1
    > etas.com: type SOA, class IN, mname training2003p
  
```

Question	Answer
What was the type of the DNS query requested?	AXFR
What domain was requested?	etas.com
How many items were in the response?	4
What is the TTL for all of the records?	3600
What is the IP address for the "welcome" subdomain?	1.1.1.1