Q1: (Layer 4) Protocol is:

A1: The protocol can be explained as below

* Ethernet II – Since field offset 12-13 has 0x0800
* IPv4 – Because field offset 14 = 45, 4 is for IPv4
* UDP – As field offset 23 has 11hex = 17dec which for UDP

Layer 4 or transport layer in this case is UDP.

Q2: Source MAC address:

A2: Apple\_00:0d:fa (b8:8d:12:00:0d:fa)

Q3: Destination MAC address:

A3: Cisco\_b5:49:40 (00:11:bc:b5:49:40)

Q4: Source IP address:

A4: Field offset 26-29 has 0A 07 03 1A (hex) = 10.7.3.26

Q5: Destination IP address:

A5: Field offset 30-33 has 42 AA E8 41(hex) = 66.170.232.65

Q6: Source (Layer 4) Port #:

A6: Source Port: Field offset 34-35 = C719(hex) = 50969

Q7: Destination (Layer 4) Port # :

A7: Destination Port: Field offset 36-37 = 0035(hex) = 53

Q8: (Application Layer) Payload description:

A8: Application layer in this case is DNS, because destination port of layer 4 is 53. The payload is :

* Transaction ID: 0x0290
* **Flags: 0x0100 Standard query**
  + 0... .... .... .... = Response: Message is a query
  + .000 0... .... .... = Opcode: Standard query (0)
  + .... ..0. .... .... = Truncated: Message is not truncated
  + .... ...1 .... .... = Recursion desired: Do query recursively
  + .... .... .0.. .... = Z: reserved (0)
  + .... .... ...0 .... = Non-authenticated data: Unacceptable
* Questions: 1
* Answer RRs: 0
* Authority RRs: 0
* Additional RRs: 0
* **Queries**
  + **mitre.org: type A, class IN**
    - Name: mitre.org
    - Name Length: 9
    - Label Count: 2
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)

Reference:

<https://hpd.gasmi.net/>