

No.	Time	Source	Destination	Protocol	Length	Info
1658	2024-05-14 13:49:02,888992	10.2.238.160	10.2.4.53	DNS	71	Standard query 0x0004 A www.mit.edu

Frame 1658: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{1C783651-C779-4443-B85A-5E2C5079BE75}, id 0

Ethernet II, Src: Microsoft\_66:9e:ab (70:bc:10:66:9e:ab), Dst: Fortinet\_09:00:1e (00:09:0f:09:00:1e)

Internet Protocol Version 4, Src: 10.2.238.160, Dst: 10.2.4.53

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 57

Identification: 0xd7c0 (55232)

000. .... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x5c1a [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.2.238.160

Destination Address: 10.2.4.53

User Datagram Protocol, Src Port: 64920, Dst Port: 53

Source Port: 64920

Destination Port: 53

Length: 37

Checksum: 0xa84d [unverified]

[Checksum Status: Unverified]

[Stream index: 10]

[Timestamps]

UDP payload (29 bytes)

Domain Name System (query)