Wireshark Homework

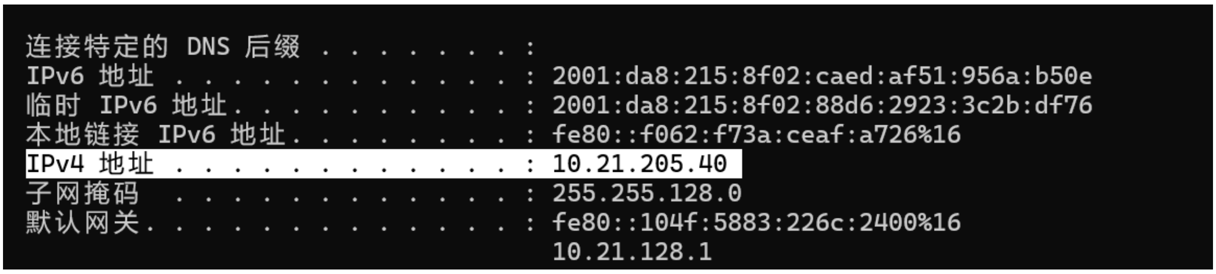
Wireshark Homework

任志诚 2023212020

2025-06-17 13:21:04

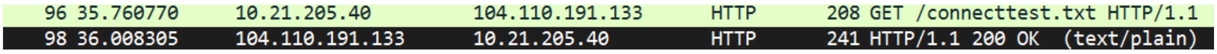
Contents

提取的请求信息



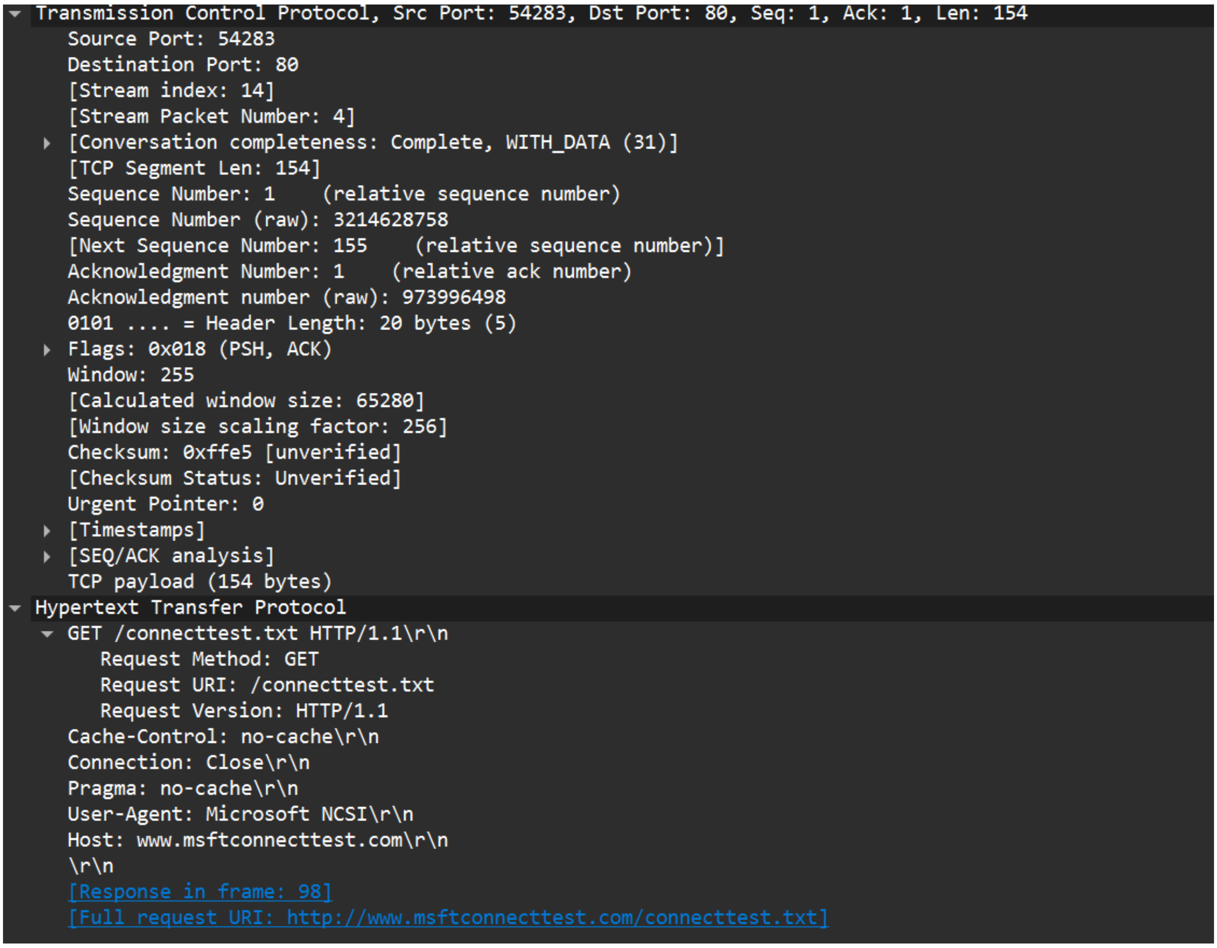
```
连接特定的 DNS 后缀 . . . . . . . :
IPv6 地址 . . . . . . . . . . . . : 2001:da8:215:8f02:caed:af51:956a:b50e
临时 IPv6 地址. . . . . . . . . . : 2001:da8:215:8f02:88d6:2923:3c2b:df76
本地链接 IPv6 地址. . . . . . . . : fe80::f062:f73a:ceaf:a726%16
IPv4 地址 . . . . . . . . . . . . : 10.21.205.40
子网掩码  . . . . . . . . . . . . : 255.255.128.0
默认网关. . . . . . . . . . . . . : fe80::104f:5883:226c:2400%16
                                    10.21.128.1
```

Figure 1: my ipconfig



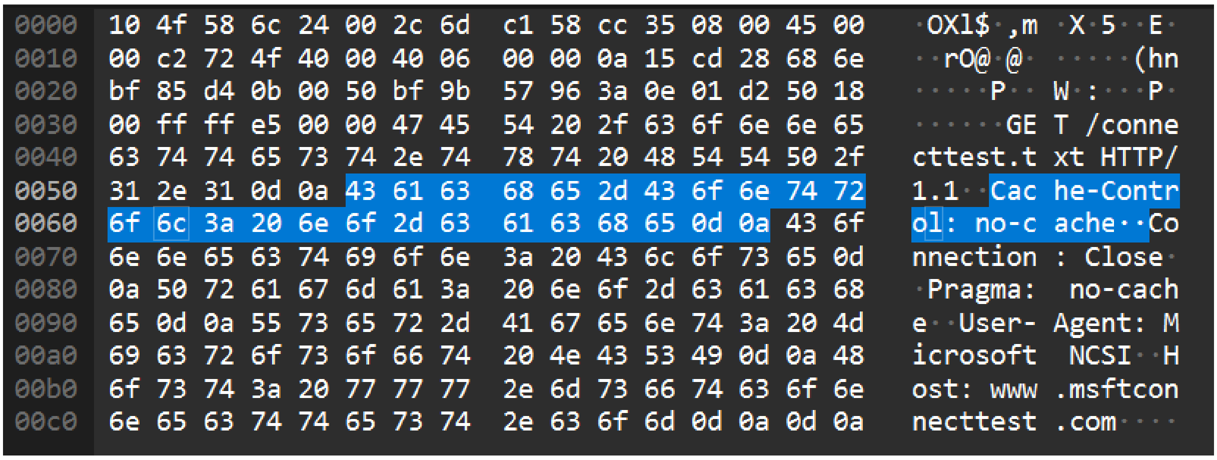
```
  96 35.760770     10.21.205.40        104.110.191.133     HTTP     208 GET /connecttest.txt HTTP/1.1
  98 36.008305     104.110.191.133     10.21.205.40        HTTP     241 HTTP/1.1 200 OK  (text/plain)
```

Figure 2: a request and its response



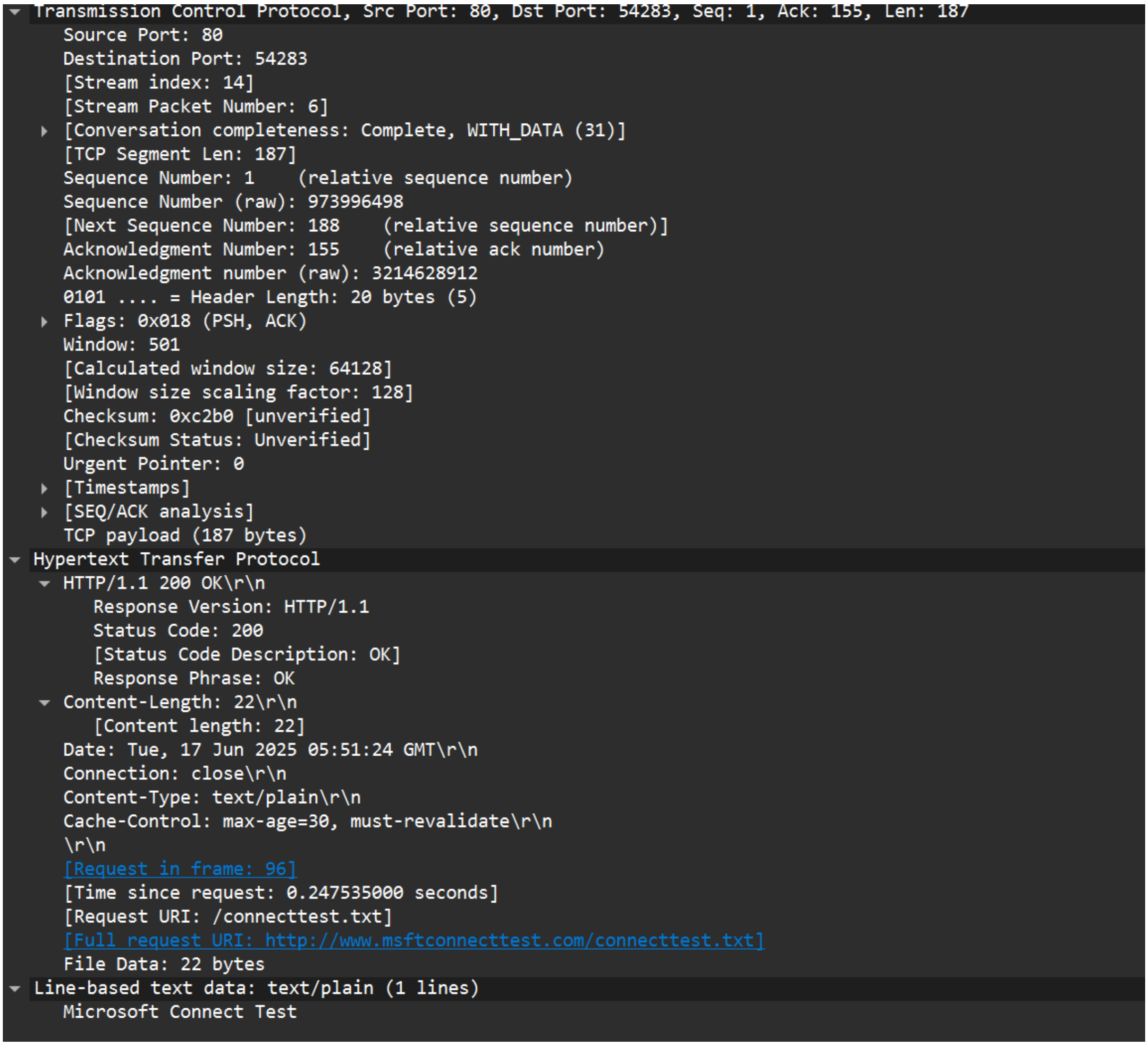
```
▾ Transmission Control Protocol, Src Port: 54283, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
    Source Port: 54283
    Destination Port: 80
    [Stream index: 14]
    [Stream Packet Number: 4]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 154]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3214628758
    [Next Sequence Number: 155    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 973996498
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0xffe5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (154 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /connecttest.txt HTTP/1.1\r\n
        Request Method: GET
        Request URI: /connecttest.txt
        Request Version: HTTP/1.1
    Cache-Control: no-cache\r\n
    Connection: Close\r\n
    Pragma: no-cache\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
    \r\n
    [Response in frame: 98]
    [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
```

Figure 3: get request



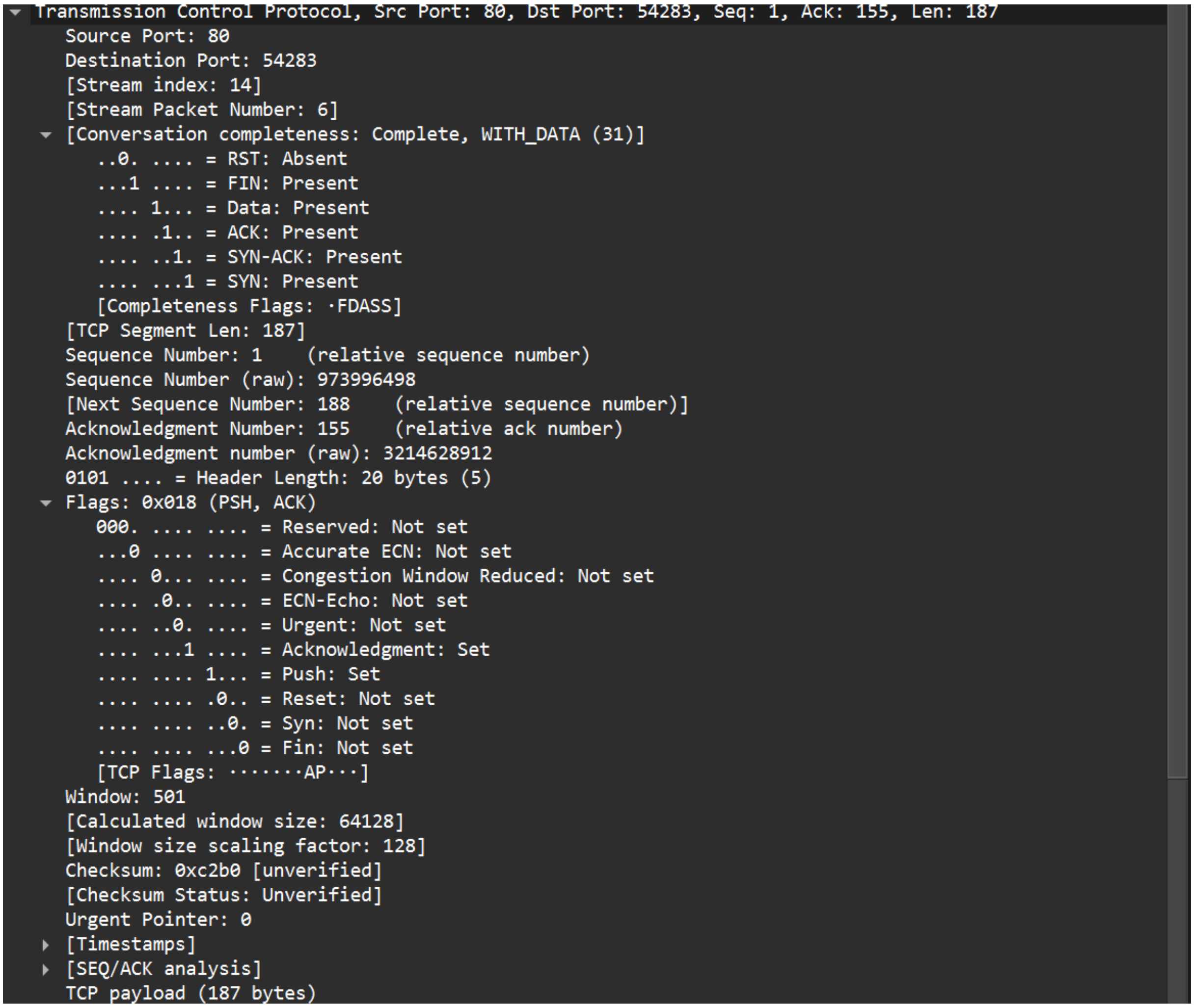
```
0000  10 4f 58 6c 24 00 2c 6d  c1 58 cc 35 08 00 45 00   ·OXl$·,m ·X·5··E·
0010  00 c2 72 4f 40 00 40 06  00 00 0a 15 cd 28 68 6e   ··rO@·@· ·····(hn
0020  bf 85 d4 0b 00 50 bf 9b  57 96 3a 0e 01 d2 50 18   ·····P·· W·:···P·
0030  00 ff ff e5 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ······GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   1.1··Cac he-Contr
0060  6f 6c 3a 20 6e 6f 2d 63  61 63 68 65 0d 0a 43 6f   ol: no-c ache··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 43 6c 6f 73 65 0d   nnection : Close·
0080  0a 50 72 61 67 6d 61 3a  20 6e 6f 2d 63 61 63 68   ·Pragma:  no-cach
0090  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
00a0  69 63 72 6f 73 6f 66 74  20 4e 43 53 49 0d 0a 48   icrosoft  NCSI··H
00b0  6f 73 74 3a 20 77 77 77  2e 6d 73 66 74 63 6f 6e   ost: www .msftcon
00c0  6e 65 63 74 74 65 73 74  2e 63 6f 6d 0d 0a 0d 0a   necttest .com····
```

Figure 4: request right



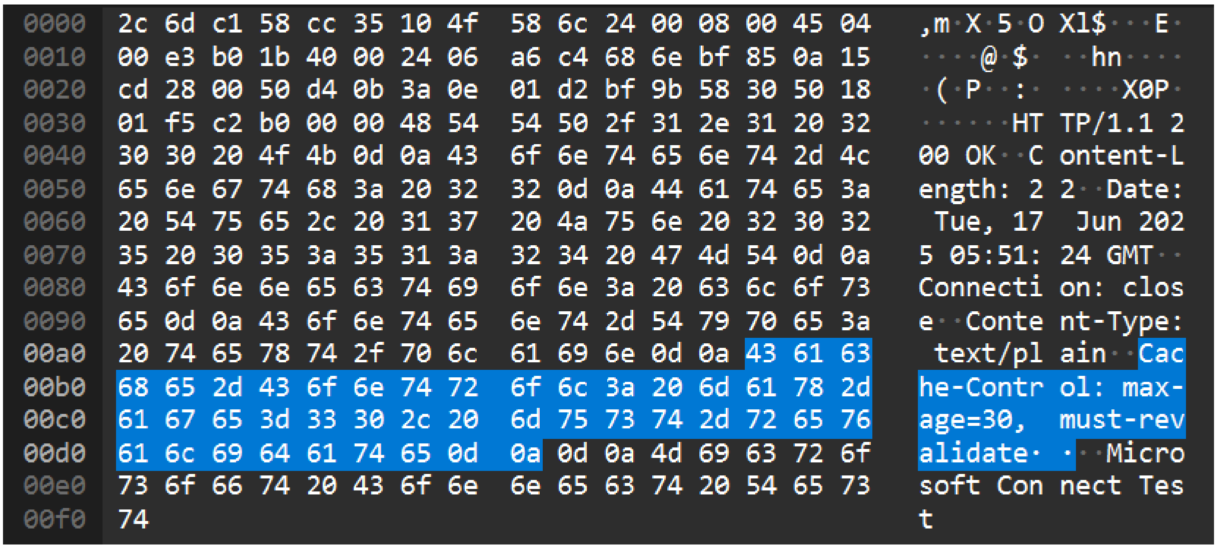
```
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 54283, Seq: 1, Ack: 155, Len: 187
     Source Port: 80
     Destination Port: 54283
     [Stream index: 14]
     [Stream Packet Number: 6]
   ▸ [Conversation completeness: Complete, WITH_DATA (31)]
     [TCP Segment Len: 187]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 973996498
     [Next Sequence Number: 188    (relative sequence number)]
     Acknowledgment Number: 155    (relative ack number)
     Acknowledgment number (raw): 3214628912
     0101 .... = Header Length: 20 bytes (5)
   ▸ Flags: 0x018 (PSH, ACK)
     Window: 501
     [Calculated window size: 64128]
     [Window size scaling factor: 128]
     Checksum: 0xc2b0 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   ▸ [Timestamps]
   ▸ [SEQ/ACK analysis]
     TCP payload (187 bytes)
▾ Hypertext Transfer Protocol
   ▾ HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
   ▾ Content-Length: 22\r\n
        [Content length: 22]
     Date: Tue, 17 Jun 2025 05:51:24 GMT\r\n
     Connection: close\r\n
     Content-Type: text/plain\r\n
     Cache-Control: max-age=30, must-revalidate\r\n
     \r\n
     [Request in frame: 96]
     [Time since request: 0.247535000 seconds]
     [Request URI: /connecttest.txt]
     [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
     File Data: 22 bytes
▾ Line-based text data: text/plain (1 lines)
     Microsoft Connect Test
```

Figure 5: response



```
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 54283, Seq: 1, Ack: 155, Len: 187
    Source Port: 80
    Destination Port: 54283
    [Stream index: 14]
    [Stream Packet Number: 6]
  ▾ [Conversation completeness: Complete, WITH_DATA (31)]
       ..0. .... = RST: Absent
       ...1 .... = FIN: Present
       .... 1... = Data: Present
       .... .1.. = ACK: Present
       .... ..1. = SYN-ACK: Present
       .... ...1 = SYN: Present
       [Completeness Flags: ·FDASS]
    [TCP Segment Len: 187]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 973996498
    [Next Sequence Number: 188    (relative sequence number)]
    Acknowledgment Number: 155    (relative ack number)
    Acknowledgment number (raw): 3214628912
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x018 (PSH, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Accurate ECN: Not set
       .... 0... .... = Congestion Window Reduced: Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...1 .... = Acknowledgment: Set
       .... .... 1... = Push: Set
       .... .... .0.. = Reset: Not set
       .... .... ..0. = Syn: Not set
       .... .... ...0 = Fin: Not set
       [TCP Flags: ·······AP···]
    Window: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0xc2b0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (187 bytes)
```

Figure 6: response more details



```
0000  2c 6d c1 58 cc 35 10 4f  58 6c 24 00 08 00 45 04   ,m·X·5·O Xl$···E·
0010  00 e3 b0 1b 40 00 24 06  a6 c4 68 6e bf 85 0a 15   ····@·$·  ··hn····
0020  cd 28 00 50 d4 0b 3a 0e  01 d2 bf 9b 58 30 50 18   ·(·P··:·  ····X0P·
0030  01 f5 c2 b0 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2 2··Date:
0060  20 54 75 65 2c 20 31 37  20 4a 75 6e 20 32 30 32    Tue, 17  Jun 202
0070  35 20 30 35 3a 35 31 3a  32 34 20 47 4d 54 0d 0a   5 05:51: 24 GMT··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f 73   Connecti on: clos
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61 63    text/pl ain··Cac
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65 76   age=30,  must-rev
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72 6f   alidate· ···Micro
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65 73   soft Con nect Tes
00f0  74                                                 t
```

Figure 7: response right

源和目标 IP 地址

- 源 **IP** 地址: 10.21.205.40（本机 IP，如 ipconfig 截图所示）
- 目标 **IP** 地址: 104.110.191.133（服务器 IP）

端口号

- 源端口: 54283（随机分配的客户端端口）
- 目标端口: 80（标准 HTTP 端口）

Host 字段

- **Host**: `www.msftconnecttest.com`

User-Agent 字段

- **User-Agent**: Microsoft NCSI

提取的响应信息

状态码

- 状态码: 200 OK

Content-Type 字段

- **Content-Type**: text/plain

Server 字段

- 在提供的截图中没有明确显示 Server 字段，该字段可能不存在于此 HTTP 响应中，或位于未捕获到的响应头部分

问题思考

HTTP 请求的目标端口通常是多少？

HTTP 请求的标准目标端口是 **80**，如截图中所示。HTTPS 则使用 443 端口。

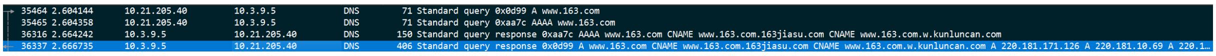
报文中的字段形式是怎样的？

HTTP 报文使用纯文本格式，以”字段名: 字段值”的形式组织，每行一个字段，如截图中所示：- `Host: www.msftconnecttest.com` - `User-Agent: Microsoft NCSI` - `Content-Type: text/plain`

Wireshark 同时提供了三种查看方式：1. 解析后的纯文本视图（HTTP 协议字段被解析为易读形式）2. 十六进制原始数据视图（数据包的二进制表现形式）3. 结构化协议树（按协议层级组织的视图）

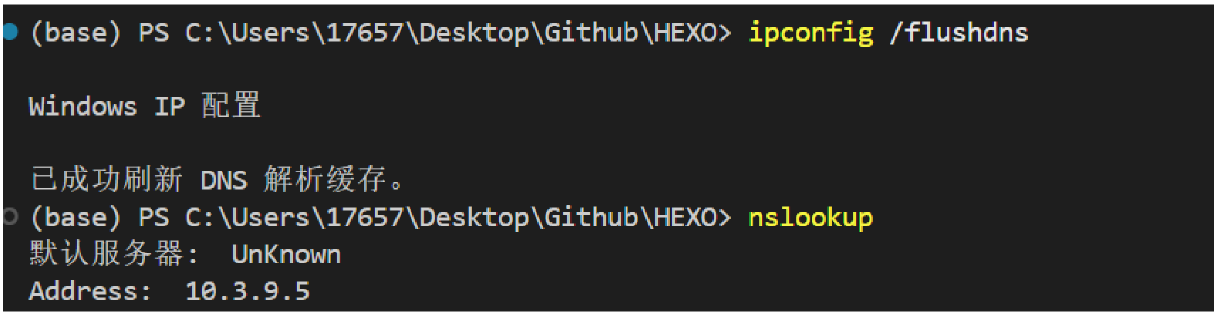
在 Wireshark 中可以看到，虽然在网络上传输时是二进制字节流，但 HTTP 协议本身是基于文本的协议。

DNS



```
35464 2.604144   10.21.205.40   10.3.9.5       DNS    71 Standard query 0x0d99 A www.163.com
35465 2.604358   10.21.205.40   10.3.9.5       DNS    71 Standard query 0xaa7c AAAA www.163.com
36316 2.664242   10.3.9.5       10.21.205.40   DNS   150 Standard query response 0xaa7c AAAA www.163.com CNAME www.163.com.163jiasu.com CNAME www.163.com.w.kunluncan.com
36337 2.666735   10.3.9.5       10.21.205.40   DNS   406 Standard query response 0x0d99 A www.163.com CNAME www.163.com.163jiasu.com CNAME www.163.com.w.kunluncan.com A 220.181.171.126 A 220.181.10.69 A 220.1…
```

Figure 8: 四条信息

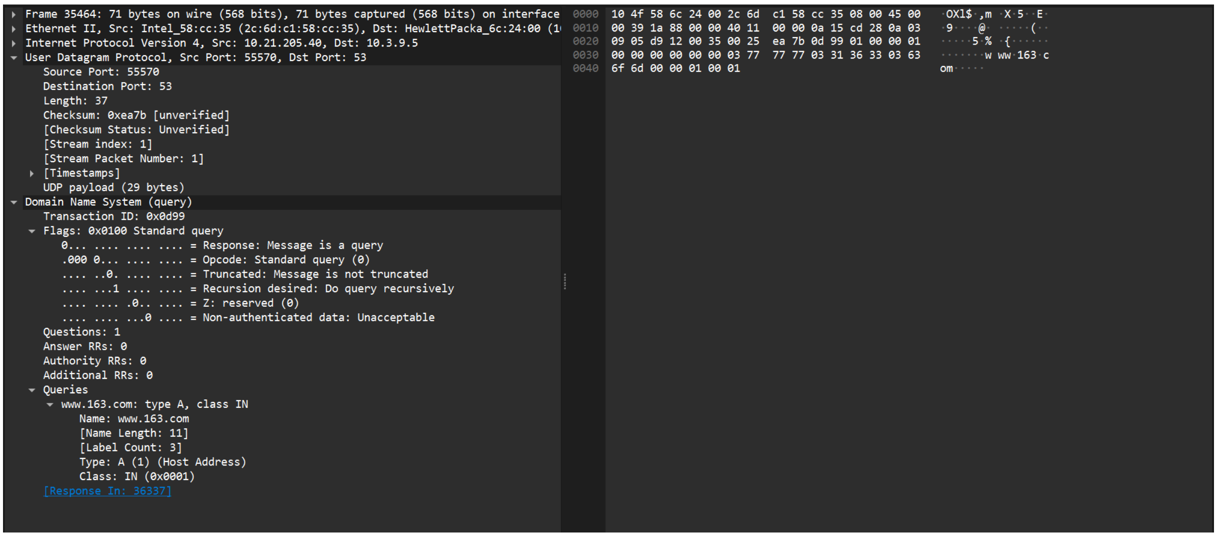


```
(base) PS C:\Users\17657\Desktop\Github\HEXO> ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
(base) PS C:\Users\17657\Desktop\Github\HEXO> nslookup
默认服务器:  UnKnown
Address:  10.3.9.5
```

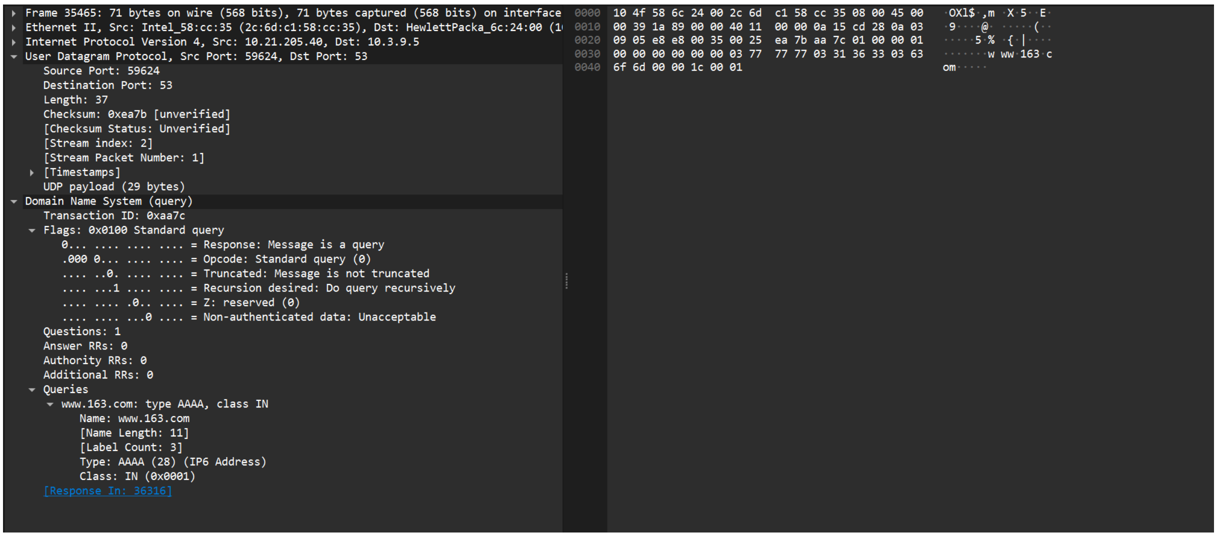
Figure 9: config



```
Frame 35464: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface
Ethernet II, Src: Intel_58:cc:35 (2c:6d:c1:58:cc:35), Dst: HewlettPacka_6c:24:00 (1
Internet Protocol Version 4, Src: 10.21.205.40, Dst: 10.3.9.5
User Datagram Protocol, Src Port: 55570, Dst Port: 53
    Source Port: 55570
    Destination Port: 53
    Length: 37
    Checksum: 0xea7b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (29 bytes)
Domain Name System (query)
    Transaction ID: 0x0d99
    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
        www.163.com: type A, class IN
            Name: www.163.com
            [Name Length: 11]
            [Label Count: 3]
            Type: A (1) (Host Address)
            Class: IN (0x0001)
    [Response In: 36337]
```

```
0000  10 4f 58 6c 24 00 2c 6d  c1 58 cc 35 08 00 45 00   ·OXl$·,m ·X·5··E·
0010  00 39 1a 88 00 00 40 11  00 00 0a 15 cd 28 0a 03   ·9····@· ·····(··
0020  09 05 d9 12 00 35 00 25  ea 7b 0d 99 01 00 00 01   ·····5·% ·{······
0030  00 00 00 00 00 00 03 77  77 77 03 31 36 33 03 63   ·······w ww·163·c
0040  6f 6d 00 00 01 00 01                               om·····
```

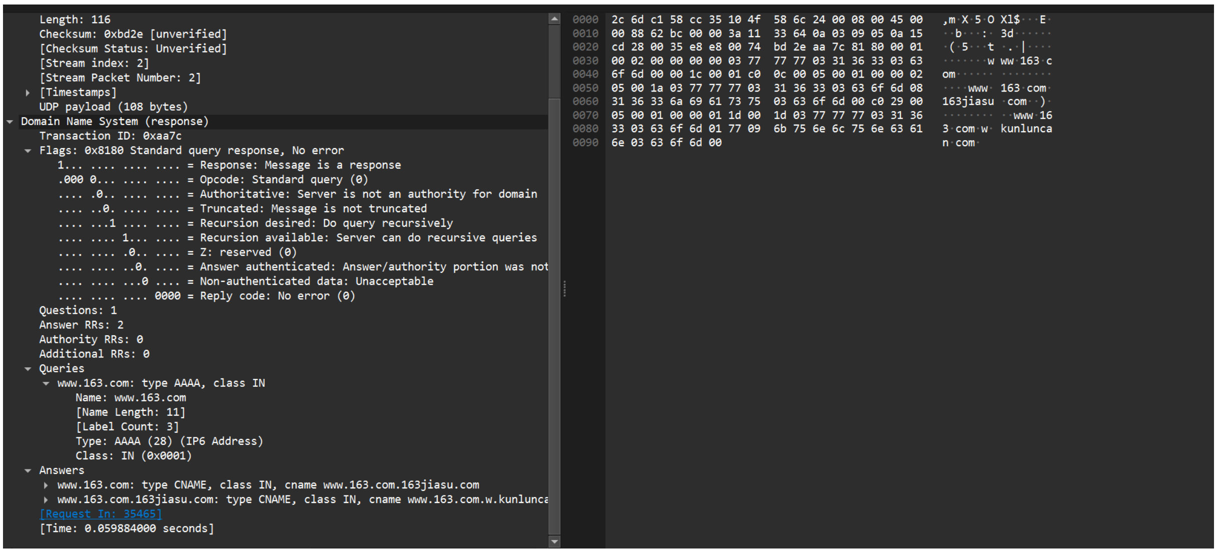
Figure 10: A request



```
▸ Frame 35465: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface
▸ Ethernet II, Src: Intel_58:cc:35 (2c:6d:c1:58:cc:35), Dst: HewlettPacka_6c:24:00 (1
▸ Internet Protocol Version 4, Src: 10.21.205.40, Dst: 10.3.9.5
▾ User Datagram Protocol, Src Port: 59624, Dst Port: 53
    Source Port: 59624
    Destination Port: 53
    Length: 37
    Checksum: 0xea7b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (29 bytes)
▾ Domain Name System (query)
    Transaction ID: 0xaa7c
  ▾ 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
    ▾ www.163.com: type AAAA, class IN
        Name: www.163.com
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
    [Response In: 36316]
```

```
0000  10 4f 58 6c 24 00 2c 6d  c1 58 cc 35 08 00 45 00   ·OXl$·,m ·X·5··E·
0010  00 39 1a 89 00 00 40 11  00 00 0a 15 cd 28 0a 03   ·9····@· ·····(··
0020  09 05 e8 e8 00 35 00 25  ea 7b aa 7c 01 00 00 01   ·····5·% ·{·|····
0030  00 00 00 00 00 00 03 77  77 77 03 31 36 33 03 63   ·······w ww·163·c
0040  6f 6d 00 00 1c 00 01                               om·····
```

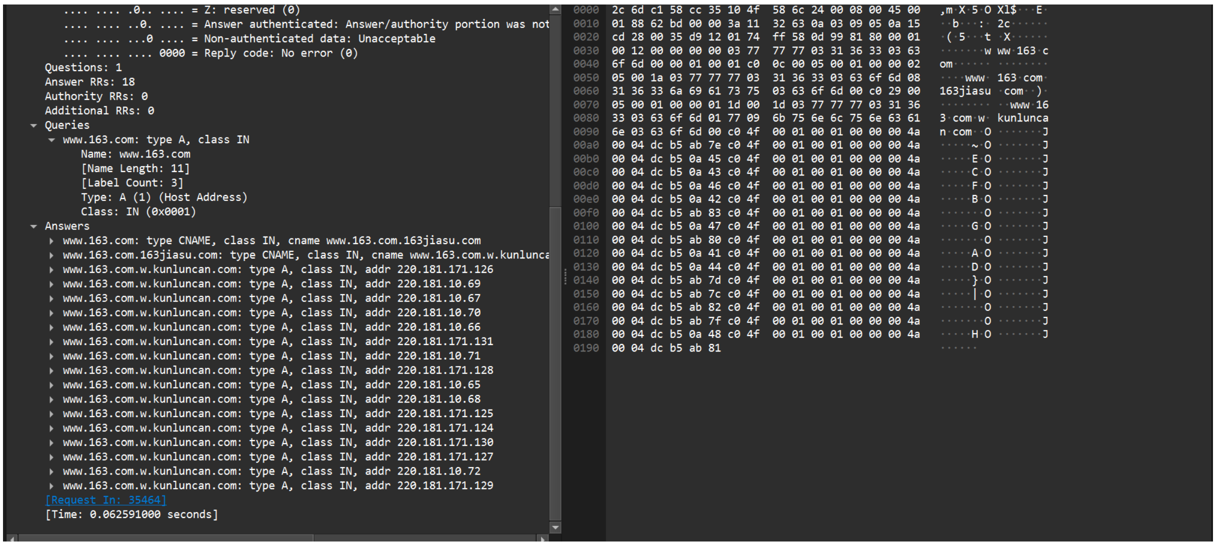
Figure 11: AAAA request



```
    Length: 116
    Checksum: 0xbd2e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 2]
  ▸ [Timestamps]
    UDP payload (108 bytes)
▾ Domain Name System (response)
    Transaction ID: 0xaa7c
  ▾ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.163.com: type AAAA, class IN
        Name: www.163.com
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▾ Answers
    ▸ www.163.com: type CNAME, class IN, cname www.163.com.163jiasu.com
    ▸ www.163.com.163jiasu.com: type CNAME, class IN, cname www.163.com.w.kunlunca
    [Request In: 35465]
    [Time: 0.059884000 seconds]
```

```
0000  2c 6d c1 58 cc 35 10 4f  58 6c 24 00 08 00 45 00   ,m·X·5·O Xl$···E·
0010  00 88 62 bc 00 00 3a 11  33 64 0a 03 09 05 0a 15   ··b···:· 3d······
0020  cd 28 00 35 e8 e8 00 74  bd 2e aa 7c 81 80 00 01   ·(·5···t ·.·|····
0030  00 02 00 00 00 00 03 77  77 77 03 31 36 33 03 63   ·······w ww·163·c
0040  6f 6d 00 00 1c 00 01 c0  0c 00 05 00 01 00 00 02   om······ ········
0050  05 00 1a 03 77 77 77 03  31 36 33 03 63 6f 6d 08   ····www· 163·com·
0060  31 36 33 6a 69 61 73 75  03 63 6f 6d 00 c0 29 00   163jiasu ·com··)·
0070  05 00 01 00 00 01 1d 00  1d 03 77 77 77 03 31 36   ········ ··www·16
0080  33 03 63 6f 6d 01 77 09  6b 75 6e 6c 75 6e 63 61   3·com·w· kunlunca
0090  6e 03 63 6f 6d 00                                  n·com·
```

Figure 12: A response



```
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 18
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.163.com: type A, class IN
          Name: www.163.com
          [Name Length: 11]
          [Label Count: 3]
          Type: A (1) (Host Address)
          Class: IN (0x0001)
  ▾ Answers
    ▸ www.163.com: type CNAME, class IN, cname www.163.com.163jiasu.com
    ▸ www.163.com.163jiasu.com: type CNAME, class IN, cname www.163.com.w.kunlunca
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.126
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.69
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.67
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.70
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.66
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.131
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.71
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.128
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.65
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.68
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.125
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.124
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.130
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.127
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.10.72
    ▸ www.163.com.w.kunluncan.com: type A, class IN, addr 220.181.171.129
    [Request In: 35464]
    [Time: 0.062591000 seconds]
```

```
0000  2c 6d c1 58 cc 35 10 4f  58 6c 24 00 08 00 45 00   ,m·X·5·O Xl$···E·
0010  01 88 62 bd 00 00 3a 11  32 63 0a 03 09 05 0a 15   ··b···:· 2c······
0020  cd 28 00 35 d9 12 01 74  ff 58 0d 99 81 80 00 01   ·(·5···t ·X······
0030  00 12 00 00 00 00 03 77  77 77 03 31 36 33 03 63   ·······w ww·163·c
0040  6f 6d 00 00 01 00 01 c0  0c 00 05 00 01 00 00 02   om······ ········
0050  05 00 1a 03 77 77 77 03  31 36 33 03 63 6f 6d 08   ····www· 163·com·
0060  31 36 33 6a 69 61 73 75  03 63 6f 6d 00 c0 29 00   163jiasu ·com··)·
0070  05 00 01 00 00 01 1d 00  1d 03 77 77 77 03 31 36   ········ ··www·16
0080  33 03 63 6f 6d 01 77 09  6b 75 6e 6c 75 6e 63 61   3·com·w· kunlunca
0090  6e 03 63 6f 6d 00 c0 4f  00 01 00 01 00 00 00 4a   n·com··O ·······J
00a0  00 04 dc b5 ab 7e c0 4f  00 01 00 01 00 00 00 4a   ·····~·O ·······J
00b0  00 04 dc b5 0a 45 c0 4f  00 01 00 01 00 00 00 4a   ·····E·O ·······J
00c0  00 04 dc b5 0a 43 c0 4f  00 01 00 01 00 00 00 4a   ·····C·O ·······J
00d0  00 04 dc b5 0a 46 c0 4f  00 01 00 01 00 00 00 4a   ·····F·O ·······J
00e0  00 04 dc b5 0a 42 c0 4f  00 01 00 01 00 00 00 4a   ·····B·O ·······J
00f0  00 04 dc b5 ab 83 c0 4f  00 01 00 01 00 00 00 4a   ·······O ·······J
0100  00 04 dc b5 0a 47 c0 4f  00 01 00 01 00 00 00 4a   ·····G·O ·······J
0110  00 04 dc b5 ab 80 c0 4f  00 01 00 01 00 00 00 4a   ·······O ·······J
0120  00 04 dc b5 0a 41 c0 4f  00 01 00 01 00 00 00 4a   ·····A·O ·······J
0130  00 04 dc b5 0a 44 c0 4f  00 01 00 01 00 00 00 4a   ·····D·O ·······J
0140  00 04 dc b5 ab 7d c0 4f  00 01 00 01 00 00 00 4a   ·····}·O ·······J
0150  00 04 dc b5 ab 7c c0 4f  00 01 00 01 00 00 00 4a   ·····|·O ·······J
0160  00 04 dc b5 ab 82 c0 4f  00 01 00 01 00 00 00 4a   ·······O ·······J
0170  00 04 dc b5 ab 7f c0 4f  00 01 00 01 00 00 00 4a   ·······O ·······J
0180  00 04 dc b5 0a 48 c0 4f  00 01 00 01 00 00 00 4a   ·····H·O ·······J
0190  00 04 dc b5 ab 81                                  ······
```

Figure 13: AAAA response

清除 DNS 缓存

从终端截图可以看到，已使用命令`ipconfig /flushdns`成功清除了 DNS 缓存：- 终端显示：“已成功刷新 **DNS** 解析缓存” - 使用`nslookup`确认 DNS 服务器为 **10.3.9.5**

DNS 查询与响应报文分析

查询报文分析

根据截图，可以看到多个 DNS 查询：

1. 查询域名：www.163.com
2. 查询类型：
    - A 记录查询（IPv4 地址）- Type: A (1)
    - AAAA 记录查询（IPv6 地址）- Type: AAAA (28)
3. 查询特征：
    - Transaction ID: 0x8d99（A 记录查询）和 0xaa7c（AAAA 记录查询）
    - 源端口：55570、59624（随机客户端端口）
    - 目标端口：**53**（标准 DNS 端口）
    - 使用 **UDP** 协议传输

响应报文分析

1. 查询域名：www.163.com
2. 响应 **IP** 地址：多个 IP 地址返回，包括：
   - **IPv4** 地址（A 记录）：
     - 220.181.171.126
     - 220.181.10.69
     - 220.181.10.67
     - 220.181.10.70
     - 220.181.10.66
     - 等多个 IP 地址
   - **CNAME** 记录：
     - www.163.com.163jiasu.com
     - www.163.com.w.kunluncan.com

DNS 协议特性分析

DNS 使用的端口号

从截图中可以明确看到：- 服务器端口：53（固定标准端口）- 客户端端口：随机高位端口（如 55570、59624）

DNS 使用的传输协议

截图中可以看到：- 主要使用 **UDP** 协议，因为：- 数据包标识为”User Datagram Protocol” - 相比 TCP 更快速，适合简短的 DNS 查询 - 标准 DNS 查询通常小于 512 字节，适合 UDP 传输

DNS 特性	值	说明
查询域名	www.163.com	中国网易公司网站
查询类型	A 和 AAAA	分别查询 IPv4 和 IPv6 地址
客户端端口	55570、59624 等	随机高位端口
服务器端口	53	DNS 标准端口

DNS 特性	值	说明
传输协议	UDP	无连接、快速、适合短查询
查询事务 ID	0x8d99、0xaa7c	确保请求和响应匹配的唯一标识符

补充说明：虽然本次抓包显示使用 UDP，但 DNS 协议在某些情况下也会使用 TCP：- 当响应大小超过 512 字节时 - 进行区域传送 (AXFR) 等操作时 - 需要可靠连接时