



# 计算机三级网络技术

## 综合题4 解题技巧

主讲人：大头



### 考点清单

- 考点1：DNS域名解析
- 考点2：TCP三次握手
- 考点3：FTP简单文本传输协议
- 考点4：ICMP控制文本传输协议
- 考点5：HTTP超文本传输协议

公众号：大头计算机二级

微博/B站：@大头博士先生



# DNS域名解析

Internet上的主机可以使用IP地址进行识别，但通常都使用主机名识别，如www.bupt.edu.cn、abc.com等，这些名字便于记忆并且易于被人们所接受。但是当Internet中的计算机间进行通信时，必须使用对方的IP地址，这就必须将主机名转换为IP地址。主机名字到IP地址的转换过程被称为名字解析。

公众号：大头计算机二级

微博/B站：@大头博士先生



# DNS域名解析

## 得分点1：客户机/DNS服务器地址

一般会有四条报文，我们重点看第一条

第一条报文里，源地址为客户机地址，目的地址为DNS服务器地址，信息里会出现需要解析的域名。

公众号：大头计算机二级

微博/B站：@大头博士先生



15、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| No. | State | Source Address   | Destination Address | Summary  | Len | Rel. Time   |
|-----|-------|------------------|---------------------|--|-----|-------------|
| 5   |       | [202.113.64.133] | [202.113.64.7]      | DNS: C ID=23868 OP=QUERY NAME=mail.nj.edu.cn                 | 74  | 0:00:04.267 |
| 6   |       | [202.113.64.7]   | [202.113.64.133]    | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.nj.edu.cn         | 115 | 0:00:04.270 |
| 7   |       | [202.113.64.133] | [202.113.64.7]      | DNS: C ID=45720 OP=QUERY NAME=mail.nj.edu.cn                 | 74  | 0:00:04.273 |
| 8   |       | [202.113.64.7]   | [202.113.64.133]    | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.nj.edu.cn         | 160 | 0:00:04.274 |
| 9   |       | [202.113.64.133] | [202.113.64.133]    | Expert: Time-to-live expiring                                | 106 | 0:00:04.276 |
| 10  |       | [202.113.64.129] | [202.113.64.133]    | ICMP: Echo   | 70  | 0:00:04.276 |
| 11  |       | [202.113.64.133] | [202.113.64.133]    | ICMP: Time exceeded (Time to live exceeded in transit)       | 106 | 0:00:04.276 |
| 12  |       | [202.113.64.129] | [202.113.64.133]    | Expert: Time-to-live expiring                                | 70  | 0:00:04.276 |
| 13  |       | [202.113.64.129] | [202.113.64.133]    | ICMP: Time exceeded (Time to live exceeded in transit)       | 106 | 0:00:04.276 |
| 14  |       | [202.113.64.129] | [202.113.64.133]    | ICMP: Echo   | 70  | 0:00:04.276 |
| 15  |       | [202.113.64.133] | [202.113.64.7]      | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202 in-add          | 87  | 0:00:04.280 |
| 16  |       | [202.113.64.7]   | [202.113.64.133]    | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64.113.202 | 149 | 0:00:04.281 |
| 17  |       | [202.113.64.133] | [202.113.64.133]    | ICMP: Echo   | 106 | 0:00:05.268 |
| 18  |       | [202.113.77.253] | [202.113.64.133]    | Expert: Time-to-live exceeded in transit                     | 70  | 0:00:05.268 |
| 19  |       | [202.113.64.133] | [202.113.64.133]    | ICMP: Echo   | 106 | 0:00:05.268 |
| 20  |       | [202.113.77.253] | [202.113.64.133]    | Expert: Time-to-live exceeded in transit                     | 70  | 0:00:05.268 |

|                           |                        |
|---------------------------|------------------------|
| ICMP: Identification      | = 4413                 |
| ICMP: Flags               | = 0X                   |
| ICMP: .0. ....            | = any fragment         |
| ICMP: .0. ....            | = last fragment        |
| ICMP: Fragment offset     | = 0 bytes              |
| ICMP: Time to live        | = 1 seconds/hops       |
| ICMP: Protocol            | = 1 ( )                |
| ICMP: Header checksum     | = B548 (correct)       |
| ICMP: Source address      | = [ ]                  |
| ICMP: Destination address | = [218.91.20.208], [ ] |
| ICMP: No options          |                        |

请根据图中信息回答下列问题。

- (1) 该主机上执行的命令是 1 , 该主机上配置的DNS服务器的IP地址是 2 。
- (2) 图中的①~④删除了部分显示信息, 其中②处应该是 3 , ③处应该是 4 , ④处应该是 5 。



15、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| No. | State | Source Address   | Destination Address | Summary  | Len | Rel. Time   |
|-----|-------|------------------|---------------------|--|-----|-------------|
| 5   |       | [202.113.64.133] | [202.113.64.7]      | DNS: C ID=23868 OP=QUERY NAME=mail.nj.edu.cn                 | 74  | 0:00:04.267 |
| 6   |       | [202.113.64.7]   | [202.113.64.133]    | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.nj.edu.cn         | 115 | 0:00:04.270 |
| 7   |       | [202.113.64.133] | [202.113.64.7]      | DNS: C ID=45720 OP=QUERY NAME=mail.nj.edu.cn                 | 74  | 0:00:04.273 |
| 8   |       | [202.113.64.7]   | [202.113.64.133]    | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.nj.edu.cn         | 160 | 0:00:04.274 |
| 9   |       | [202.113.64.133] | [202.113.64.133]    | Expert: Time-to-live expiring                                | 106 | 0:00:04.276 |
| 10  |       | [202.113.64.129] | [202.113.64.133]    | ICMP: Echo   | 70  | 0:00:04.276 |
| 11  |       | [202.113.64.133] | [202.113.64.133]    | ICMP: Time exceeded (Time to live exceeded in transit)       | 106 | 0:00:04.276 |
| 12  |       | [202.113.64.129] | [202.113.64.133]    | Expert: Time-to-live expiring                                | 70  | 0:00:04.276 |
| 13  |       | [202.113.64.129] | [202.113.64.133]    | ICMP: Time exceeded (Time to live exceeded in transit)       | 106 | 0:00:04.276 |
| 14  |       | [202.113.64.129] | [202.113.64.133]    | ICMP: Echo   | 70  | 0:00:04.276 |
| 15  |       | [202.113.64.133] | [202.113.64.7]      | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202 in-add          | 87  | 0:00:04.280 |
| 16  |       | [202.113.64.7]   | [202.113.64.133]    | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64.113.202 | 149 | 0:00:04.281 |
| 17  |       | [202.113.64.133] | [202.113.64.133]    | ICMP: Echo   | 106 | 0:00:05.268 |
| 18  |       | [202.113.77.253] | [202.113.64.133]    | Expert: Time-to-live exceeded in transit                     | 70  | 0:00:05.268 |
| 19  |       | [202.113.64.133] | [202.113.64.133]    | ICMP: Echo   | 106 | 0:00:05.268 |
| 20  |       | [202.113.77.253] | [202.113.64.133]    | Expert: Time-to-live exceeded in transit                     | 70  | 0:00:05.268 |

|                           |                        |
|---------------------------|------------------------|
| ICMP: Identification      | = 4413                 |
| ICMP: Flags               | = 0X                   |
| ICMP: .0. ....            | = any fragment         |
| ICMP: .0. ....            | = last fragment        |
| ICMP: Fragment offset     | = 0 bytes              |
| ICMP: Time to live        | = 1 seconds/hops       |
| ICMP: Protocol            | = 1 ( )                |
| ICMP: Header checksum     | = B548 (correct)       |
| ICMP: Source address      | = [ ]                  |
| ICMP: Destination address | = [218.91.20.208], [ ] |
| ICMP: No options          |                        |

请根据图中信息回答下列问题。

- (1) 该主机上执行的命令是 1 , 该主机上配置的DNS服务器的IP地址是 2 202.113.64.7 。
- (2) 图中的①~④删除了部分显示信息, 其中②处应该是 3 , ③处应该是 4 , ④处应该是 5 。





# DNS域名解析

## 得分点2：tracert命令

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP数据包访问目标所采取的路径。

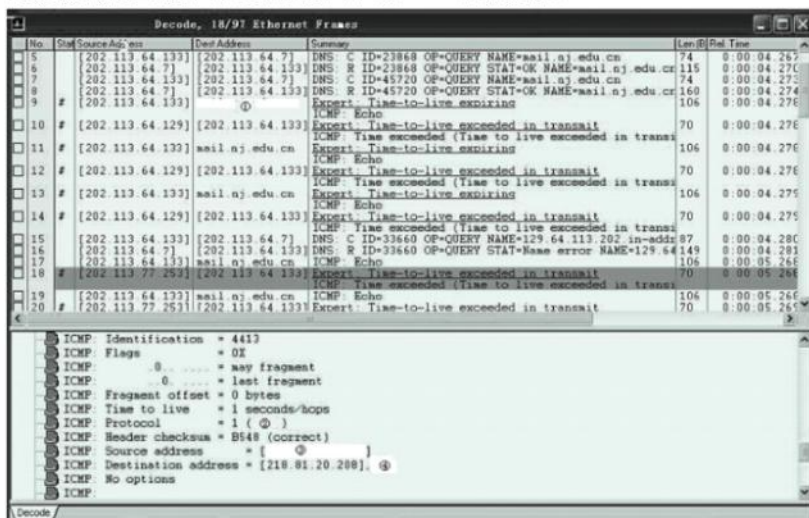
tracert <域名/IP地址>

公众号：大头计算机二级

微博/B站：@大头博士先生



15、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。



请根据图中信息回答下列问题。

- (1) 该主机上执行的命令是 1，该主机上配置的DNS服务器的IP地址是 2。
- (2) 图中的①~④删除了部分显示信息，其中②处应该是 3，③处应该是 4，④处应该是 5。



15、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| No. | Src              | Dest             | Summary  | Len | Rel. Time   |
|-----|------------------|------------------|--|-----|-------------|
| 5   | [202.113.64.133] | [202.113.64.7]   | DNS: C ID=23868 OP=QUERY NAME=mail.sj.edu.cn                         | 74  | 0:00:04.267 |
| 6   | [202.113.64.7]   | [202.113.64.133] | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.sj.edu.cn                 | 115 | 0:00:04.270 |
| 7   | [202.113.64.133] | [202.113.64.7]   | DNS: C ID=45720 OP=QUERY NAME=mail.sj.edu.cn                         | 74  | 0:00:04.273 |
| 8   | [202.113.64.7]   | [202.113.64.133] | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.sj.edu.cn                 | 160 | 0:00:04.276 |
| 9   | [202.113.64.133] | [202.113.64.133] | Expert: Time-to-live expiring  | 106 | 0:00:04.276 |
| 10  | [202.113.64.129] | [202.113.64.133] | ICMP: Echo   | 70  | 0:00:04.276 |
| 11  | [202.113.64.133] | [202.113.64.133] | Expert: Time-to-live exceeded in transit                             | 106 | 0:00:04.276 |
| 12  | [202.113.64.129] | [202.113.64.133] | ICMP: Echo   | 70  | 0:00:04.276 |
| 13  | [202.113.64.133] | [202.113.64.133] | Expert: Time-to-live exceeded in transit                             | 106 | 0:00:04.276 |
| 14  | [202.113.64.129] | [202.113.64.133] | ICMP: Echo   | 70  | 0:00:04.276 |
| 15  | [202.113.64.133] | [202.113.64.7]   | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr                 | 87  | 0:00:04.280 |
| 16  | [202.113.64.7]   | [202.113.64.133] | DNS: R ID=33660 OP=QUERY STAT=Base error NAME=129.64.113.202.in-addr | 149 | 0:00:04.281 |
| 17  | [202.113.64.133] | [202.113.64.133] | ICMP: Echo   | 106 | 0:00:05.261 |
| 18  | [202.113.77.253] | [202.113.64.133] | Expert: Time-to-live exceeded in transit                             | 70  | 0:00:05.261 |
| 19  | [202.113.64.133] | [202.113.64.133] | ICMP: Echo   | 106 | 0:00:05.261 |
| 20  | [202.113.77.253] | [202.113.64.133] | Expert: Time-to-live exceeded in transit                             | 70  | 0:00:05.261 |

tracert <域名>

请根据图中信息回答下列问题。

- (1) 该主机上执行的命令是 ① tracert mail.nj.edu.cn, 该主机上配置的DNS服务器的IP地址是 ② 。
- (2) 图中的①~④删除了部分显示信息, 其中②处应该是 ③, ③处应该是 ④, ④处应该是 ⑤。



## DNS域名解析

得分点3：根据tracert命令确认域名对应的IP地址

公众号：大头计算机二级

微博/B站：@大头博士先生



| NetworkMiner 16/07 Ethernet Frames |                  |                  |   |          |               |
|------------------------------------|------------------|------------------|---|----------|---------------|
| No                                 | Time             | Source Address   | Destination Address                                       | Protocol | Length/Offset |
| 9                                  | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=23648 OP=QUERY NAME=mail.t3.edu.cn              | 74       | 0.00:04.26    |
| 10                                 | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=17864 OP=QUERY STAT=OK NAME=mail.t3.edu.cn      | 118      | 0.00:04.27    |
| 11                                 | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=45720 OP=QUERY NAME=mail.t3.edu.cn              | 74       | 0.00:04.27    |
| 12                                 | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=45720 OP=QUERY NAME=mail.t3.edu.cn              | 118      | 0.00:04.27    |
| 13                                 | [202.113.64.137] | [202.113.64.3]   | Request: Time-to-live exceeded in transmit                | 106      | 0.00:04.27    |
| 14                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:04.27    |
| 15                                 | [202.113.64.137] | mail.t3.edu.cn   | Request: Time-to-live exceeded in transmit                | 106      | 0.00:04.27    |
| 16                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:04.27    |
| 17                                 | [202.113.64.137] | mail.t3.edu.cn   | Request: Time-to-live exceeded in transmit                | 106      | 0.00:04.27    |
| 18                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:04.27    |
| 19                                 | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=33640 OP=QUERY NAME=119.64.113.202.in-addr.arpa | 118      | 0.00:04.28    |
| 20                                 | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=33640 OP=QUERY NAME=119.64.113.202.in-addr.arpa | 149      | 0.00:04.29    |
| 21                                 | [202.113.64.137] | mail.t3.edu.cn   | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 22                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 23                                 | [202.113.64.137] | mail.t3.edu.cn   | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 24                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 25                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 26                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 27                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 28                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 29                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 30                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 31                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 32                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 33                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 34                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 35                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 36                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 37                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 38                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 39                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 40                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 41                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 42                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 43                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 44                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 45                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 46                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 47                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 48                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 49                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
| 50                                 | [202.113.64.137] | [202.113.64.137] | Request: Time-to-live exceeded in transmit                | 106      | 0.00:05.26    |
|                                    |                  |                  |   |          |               |

(1) 该主机上执行的命令是 ① \_\_\_\_\_。

(2) 图中的①~④删除了部分显示信息，其中①处应该是 ② \_\_\_\_\_，②处应该是 ③ \_\_\_\_\_，③处应该是 ④ \_\_\_\_\_。

(3) 主机mail.tj.edu.cn对应的IP地址是 ⑤ \_\_\_\_\_。



Wireshark packet capture showing a successful TCP connection from 192.113.64.137 to 192.113.64.129 on port 80. The connection is established via a SYN-ACK exchange. The packet list shows the initial SYN packet (seq=21648) and the corresponding SYN-ACK packet (seq=45720, ack=21649). The packet details show the TCP header with flags SYN, ACK, and Seq=45720. The packet bytes show the raw TCP segment structure.

| No. | Time     | Source Address | Destination Address | Protocol | Length | Info                                | Time     |
|-----|----------|----------------|---------------------|----------|--------|-------------------------------------|----------|
| 9   | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [RST] Seq=21648 Win=0 Len=0 | 0.000000 |
| 10  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 11  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 12  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 13  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 14  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 15  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 16  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 17  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 18  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 19  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 20  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 21  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 22  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 23  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 24  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 25  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 26  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 27  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 28  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 29  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 30  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 31  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 32  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 33  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 34  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 35  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 36  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 37  | 0.000000 | 192.113.64.137 | 192.113.64.129      | TCP      | 60     | 80 → 80 [ACK] Seq=45720 Win=0 Len=0 | 0.000000 |
| 38  | 0.000000 | 192.113.64.129 | 192.113.64.137      | TCP      | 60     | 80 → 80                             |          |

(1) 该主机上执行的命令是 ① nslookup。

(2) 图中的①~④删除了部分显示信息，其中①处应该是 ② Server: 192.168.1.1，②处应该是 ③ Address: 211.81.20.208，③处应该是 ④ 211.81.20.208。

(3) 主机mail.tj.edu.cn对应的IP地址是 ⑤ 211.81.20.208。



# DNS域名解析

## 得分点4：确认IP地址和MAC地址

### wireshark抓包

根据DNS信息的第一句，可以判断客户机和DNS服务器的IP地址，而后根据详细信息里，可以得到src表示源地址，dst表示目的地址；

两句话源地址和目的地址是对应的

```
> Frame 1212: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
> Ethernet II, Src: Hangzhou_5a:66:84 (58:6a:b1:5a:66:84), Dst: Dell_9d:27:05 (48:4d:7e:9d:27:05)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 59.67.152.250
> User Datagram Protocol, Src Port: 53, Dst Port: 60786
```

公众号：大头计算机二级

微博/B站：@大头博士先生



22、下图是校园网某台主机在命令行模式执行某个命令时用wireshark捕获的数据包。

The screenshot shows a Wireshark capture of a DNS query and response. The packet list shows a query for www.12306.cn and a response from 12306.adns.cache.ounglob.com. The packet details show the query and response structure.

请根据图中信息回答下列问题。

(1) 该主机上执行的命令是 (1)

(2) 该主机上使用的DNS服务器的IP地址是 (2)

(3) 该主机的IP地址是 (3)，该主机的MAC地址是 (4)

(4) 主机www.12306.cn对应的IP地址是 (5)



22、下图是校园网某台主机在命令行模式执行某个命令时用wireshark捕获的数据包。

| No.  | Time      | Source        | Destination   | Protocol | Length | Info   |
|------|-----------|---------------|---------------|----------|--------|--|
| 1210 | 0.274645  | 59.67.152.250 | 8.8.8.8       | DNS      | 72     | Standard query 0x1617 A www.12306.cn   |
| 1211 | 0.274661  | 59.67.152.250 | 8.8.8.8       | DNS      | 72     | Standard query 0x50fd AAAA www.12306.cn  |
| 1212 | 0.274661  | 8.8.8.8       | 59.67.152.250 | DNS      | 162    | Standard query response 0x1617 A www.12306.cn CNAME www.12306.cn.1dns.com CNAME 12306.xdscache.org10b.com ...    |
| 1214 | 0.280225  | 8.8.8.8       | 59.67.152.250 | DNS      | 213    | Standard query response 0x50fd AAAA www.12306.cn CNAME www.12306.cn.1dns.com CNAME 12306.xdscache.org10b.com ... |
| 1215 | 0.289202  | 59.67.152.250 | 43.226.162.67 | ICMP     | 74     | Echo (ping) request 10=0x0001, seq=273/4353, ttl=128 (reply in 1216)   |
| 1216 | 0.291302  | 43.226.162.67 | 59.67.152.250 | ICMP     | 74     | Echo (ping) reply 10=0x0001, seq=273/4353, ttl=53 (request in 1215)  |
| 1639 | 4.291132  | 59.67.152.250 | 43.226.162.67 | ICMP     | 74     | Echo (ping) request 10=0x0001, seq=274/4609, ttl=128 (reply in 1640)   |
| 1640 | 4.293273  | 43.226.162.67 | 59.67.152.250 | ICMP     | 74     | Echo (ping) reply 10=0x0001, seq=274/4609, ttl=53 (request in 1639)  |
| 1994 | 5.295005  | 59.67.152.250 | 43.226.162.67 | ICMP     | 74     | Echo (ping) request 10=0x0001, seq=275/4805, ttl=128 (reply in 1995)   |
| 1995 | 5.297902  | 43.226.162.67 | 59.67.152.250 | ICMP     | 74     | Echo (ping) reply 10=0x0001, seq=275/4805, ttl=53 (request in 1994)  |
| 2344 | 6.297245  | 59.67.152.250 | 43.226.162.67 | ICMP     | 74     | Echo (ping) request 10=0x0001, seq=276/5121, ttl=128 (reply in 2345)   |
| 2345 | 6.299296  | 43.226.162.67 | 59.67.152.250 | ICMP     | 74     | Echo (ping) reply 10=0x0001, seq=276/5121, ttl=53 (request in 2344)  |
| 6383 | 15.079506 | 59.67.152.250 | 51.255.41.135 | ICMP     | 48     | Destination unreachable (Port unreachable)   |

|   |
|---|
| Frame 1212: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0        |
| Ethernet II, Src: Hangzhou_5a:66:04 (58:69:ad:a3:66:04), Dst: Dell_9d:27:05 (48:4d:7e:9d:27:05) |
| Internet Protocol Version 4, Src: 8.8.8.8, Dst: 59.67.152.250                                   |
| User Datagram Protocol, Src Port: 53, Dst Port: 53  |
| Source Port: 53   |
| Destination Port: 53  |
| Length: 128   |
| Checksum: 0x6f5a [unverified]   |
| [Checksum Status: Unverified]   |
| [Stream Index: 19]  |
| Domain Name System (response)   |
| Request ID: 1212  |
| Time: 0.001560000 seconds   |
| Transaction ID: 0x1617  |
| Flags: 0x1800 Standard query response, No error   |
| Questions: 1  |
| Answer RRs: 3   |
| Authority RRs: 0  |
| Additional RRs: 0   |
| Queries   |
| www.12306.cn: type A, class IN  |
| Answers   |
| www.12306.cn: type CNAME, class IN, cname www.12306.cn.1dns.com                                 |
| www.12306.cn.1dns.com: type CNAME, class IN, cname 12306.xdscache.org10b.com                    |
| 12306.xdscache.org10b.com: type A, class IN, addr 43.226.162.67                                 |

请根据图中信息回答下列问题。

(1) 该主机上执行的命令是 1

(2) 该主机上使用的DNS服务器的IP地址是 2

(3) 该主机的IP地址是 3 59.67.152.250，该主机的MAC地址是 4 48:4d:7e:9d:27:05。

(4) 主机www.12306.cn对应的IP地址是 5

## DNS域名解析

得分点5：确认输入的url

wireshark抓包

根据DNS信息，判断用户访问的路径，注意题目选中的是哪一条报文。

| No.  | Time     | Source         | Destination   | Protocol | Length | Info  |
|------|----------|----------------|---------------|----------|--------|---|
| 119  | 0.250929 | 172.64.135.5   | 59.67.152.250 | HTTP     | 386    | HTTP/1.1 400 Bad Request (text/html)  |
| 206  | 0.520169 | 172.64.135.5   | 59.67.152.250 | HTTP     | 386    | HTTP/1.1 400 Bad Request (text/html)  |
| 1082 | 1.904747 | 59.67.152.250  | 8.8.8.8       | DNS      | 73     | Standard query 0x50be A qur1.f.360.cn   |
| 1083 | 1.904747 | 59.67.152.250  | 8.8.8.8       | DNS      | 73     | Standard query 0x467 AAAA qur1.f.360.cn   |
| 1084 | 1.905704 | 59.67.152.250  | 8.8.8.8       | DNS      | 77     | Standard query 0x46c A www.enorth.com.cn  |
| 1085 | 1.905704 | 59.67.152.250  | 8.8.8.8       | DNS      | 77     | Standard query 0xc2c9 AAAA www.enorth.com.cn  |
| 1086 | 1.906380 | 8.8.8.8        | 59.67.152.250 | DNS      | 133    | Standard query response 0x50be A qur1.f.360.cn CNAME qur1.fh-1b.com A 111.206.62.164 A 111.206.62.169           |
| 1087 | 1.907595 | 8.8.8.8        | 59.67.152.250 | DNS      | 201    | Standard query response 0x46c AAAA www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd.  |
| 1088 | 1.909468 | 8.8.8.8        | 59.67.152.250 | DNS      | 210    | Standard query response 0xc2c9 AAAA www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd. |
| 1090 | 1.911046 | 8.8.8.8        | 59.67.152.250 | DNS      | 101    | Standard query response 0x467 AAAA qur1.f.360.cn CNAME qur1.fh-1b.com   |
| 1094 | 1.911836 | 59.67.152.250  | 220.194.79.33 | HTTP     | 583    | GET / HTTP/1.1  |
| 1134 | 1.920010 | 220.194.79.33  | 59.67.152.250 | HTTP     | 221    | HTTP/1.1 200 OK (text/html)   |
| 1139 | 1.920210 | 111.206.62.164 | 59.67.152.250 | HTTP     | 772    | POST /wdinfo.php HTTP/1.1 (application/octet-stream)  |
| 1140 | 1.929537 | 220.194.79.33  | 59.67.152.250 | HTTP     | 389    | GET /sys/share/jquery-1.10.2.min.js HTTP/1.1  |
| 1174 | 1.934093 | 59.67.152.250  | 220.194.79.33 | HTTP     | 390    | GET /css/gg201409.css HTTP/1.1  |
| 1178 | 1.937266 | 220.194.79.33  | 59.67.152.250 | HTTP     | 880    | HTTP/1.1 200 OK (text/css)  |
| 1212 | 1.943181 | 220.194.79.33  | 59.67.152.250 | HTTP     | 1180   | HTTP/1.1 200 OK (application/javascript)  |
| 1225 | 1.971121 | 59.67.152.250  | 220.194.79.33 | HTTP     | 383    | GET /sys/online_calc.js?ver=1 HTTP/1.1  |

公众号：大头计算机二级

微博/B站：@大头博士先生





23、下图是校园网某台主机使用浏览器访问某个网站时用wireshark捕获的数据包。

| No.  | Time     | Source        | Destination    | Protocol | Length | Info  |
|------|----------|---------------|----------------|----------|--------|---|
| 119  | 0.250929 | 172.64.135.5  | 59.67.152.250  | HTTP     | 386    | HTTP/1.1 400 Bad Request (text/html)  |
| 286  | 0.320569 | 172.64.135.5  | 59.67.152.250  | HTTP     | 386    | HTTP/1.1 400 Bad Request (text/html)  |
| 1062 | 1.904747 | 59.67.152.250 | 8.8.8.8        | DNS      | 73     | Standard query 0x5b6e & qurl.f.360.cn   |
| 1063 | 1.904747 | 59.67.152.250 | 8.8.8.8        | DNS      | 73     | Standard query 0x5b6f & AAAA qurl.f.360.cn  |
| 1064 | 1.905704 | 59.67.152.250 | 8.8.8.8        | DNS      | 77     | Standard query 0xf43c & www.enorth.com.cn   |
| 1065 | 1.905704 | 59.67.152.250 | 8.8.8.8        | DNS      | 77     | Standard query 0xf43c & www.enorth.com.cn   |
| 1066 | 1.906380 | 8.8.8.8       | 59.67.152.250  | DNS      | 133    | Standard query response 0x5b6e & qurl.f.360.cn CNAME qurl.qh-1b.com & 111.206.62.164 & 111.206.62.169             |
| 1067 | 1.907595 | 8.8.8.8       | 59.67.152.250  | DNS      | 201    | Standard query response 0xf43c & www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd-      |
| 1068 | 1.909468 | 8.8.8.8       | 59.67.152.250  | DNS      | 210    | Standard query response 0xc2c9 & AAAA www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd- |
| 1090 | 1.911046 | 8.8.8.8       | 59.67.152.250  | DNS      | 181    | Standard query response 0x9467 & AAAA qurl.f.360.cn CNAME qurl.qh-1b.com  |
| 1094 | 1.911836 | 59.67.152.250 | 220.194.79.33  | HTTP     | 583    | GET / HTTP/1.1  |
| 1134 | 1.920010 | 220.194.79.33 | 59.67.152.250  | HTTP     | 221    | HTTP/1.1 200 OK (text/html)   |
| 1139 | 1.920210 | 59.67.152.250 | 111.206.62.164 | HTTP     | 772    | POST /userinfo.php HTTP/1.1 (application/octet-stream)  |
| 1168 | 1.929537 | 59.67.152.250 | 220.194.79.33  | HTTP     | 389    | GET /sys/share/jquery-1.12.2.min.js HTTP/1.1  |
| 1174 | 1.934093 | 59.67.152.250 | 220.194.79.33  | HTTP     | 390    | GET /css/gg201409.css HTTP/1.1  |
| 1178 | 1.937266 | 220.194.79.33 | 59.67.152.250  | HTTP     | 880    | HTTP/1.1 200 OK (text/css)  |
| 1212 | 1.943181 | 220.194.79.33 | 59.67.152.250  | HTTP     | 1580   | HTTP/1.1 200 OK (application/javascript)  |
| 1225 | 1.971121 | 59.67.152.250 | 220.194.79.33  | HTTP     | 383    | GET /sys/online_cal.js?ver=1 HTTP/1.1   |
| 1225 | 1.971121 | 59.67.152.250 | 220.194.79.33  | HTTP     | 383    | GET /sys/online_cal.js?ver=1 HTTP/1.1   |

Frame 1067: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface 0  
 Ethernet II, Src: Hengzhou\_Sa166:84 (58:ea:b1:5a:16:84), Dst: Dell\_9d:27:05 (48:6d:7e:9d:27:05)  
 Internet Protocol Version 4, Src: 8.8.8.8, Dst: 59.67.152.250  
 User Datagram Protocol, Src Port: 53, Dst Port: 49425  
 Domain Name System (response)  
 [Request ID: 3084]  
 [Time: 0.001891000 seconds]  
 Transaction ID: 0xf43c  
 Flags: 0x0100 Standard query response, No error  
 Questions: 1  
 Answer RRs: 5  
 Authority RRs: 0  
 Additional RRs: 0  
 Queries  
 Answers  
 > www.enorth.com.cn: type CNAME, class IN, cname www.enorth.com.cn.cdn.dnsv1.com  
 > www.enorth.com.cn.cdn.dnsv1.com: type CNAME, class IN, cname 287911.s2.cdntip.com  
 > 287911.s2.cdntip.com: type A, class IN, addr 220.194.79.33  
 > 287911.s2.cdntip.com: type A, class IN, addr 220.194.79.34  
 > 287911.s2.cdntip.com: type A, class IN, addr 125.39.132.236

以访问 (live capture in progress)

过滤: 10000 · 已捕获: 527 (2.9K)

配置文件: Default

请根据图中信息回答下列问题。

- (1) 在浏览器中输入的URL是 1
- (2) 该主机上使用的DNS服务器的IP地址是 2
- (3) 该主机的IP地址是 3，该主机的MAC地址是 4
- (4) 域名www.enorth.com.cn对应的IP地址是 5

23、下图是校园网某台主机使用浏览器访问某个网站时用wireshark捕获的数据包。

| No.  | Time     | Source        | Destination    | Protocol | Length | Info  |
|------|----------|---------------|----------------|----------|--------|---|
| 119  | 0.250929 | 172.64.135.5  | 59.67.152.250  | HTTP     | 386    | HTTP/1.1 400 Bad Request (text/html)  |
| 286  | 0.320569 | 172.64.135.5  | 59.67.152.250  | HTTP     | 386    | HTTP/1.1 400 Bad Request (text/html)  |
| 1062 | 1.904747 | 59.67.152.250 | 8.8.8.8        | DNS      | 73     | Standard query 0x5b6e & qurl.f.360.cn   |
| 1063 | 1.904747 | 59.67.152.250 | 8.8.8.8        | DNS      | 73     | Standard query 0x5b6f & AAAA qurl.f.360.cn  |
| 1064 | 1.905704 | 59.67.152.250 | 8.8.8.8        | DNS      | 77     | Standard query 0xf43c & www.enorth.com.cn   |
| 1065 | 1.905704 | 59.67.152.250 | 8.8.8.8        | DNS      | 77     | Standard query 0xf43c & www.enorth.com.cn   |
| 1066 | 1.906380 | 8.8.8.8       | 59.67.152.250  | DNS      | 133    | Standard query response 0x5b6e & qurl.f.360.cn CNAME qurl.qh-1b.com & 111.206.62.164 & 111.206.62.169             |
| 1067 | 1.907595 | 8.8.8.8       | 59.67.152.250  | DNS      | 201    | Standard query response 0xf43c & www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd-      |
| 1068 | 1.909468 | 8.8.8.8       | 59.67.152.250  | DNS      | 210    | Standard query response 0xc2c9 & AAAA www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd- |
| 1090 | 1.911046 | 8.8.8.8       | 59.67.152.250  | DNS      | 181    | Standard query response 0x9467 & AAAA qurl.f.360.cn CNAME qurl.qh-1b.com  |
| 1094 | 1.911836 | 59.67.152.250 | 220.194.79.33  | HTTP     | 583    | GET / HTTP/1.1  |
| 1134 | 1.920010 | 220.194.79.33 | 59.67.152.250  | HTTP     | 221    | HTTP/1.1 200 OK (text/html)   |
| 1139 | 1.920210 | 59.67.152.250 | 111.206.62.164 | HTTP     | 772    | POST /userinfo.php HTTP/1.1 (application/octet-stream)  |
| 1168 | 1.929537 | 59.67.152.250 | 220.194.79.33  | HTTP     | 389    | GET /sys/share/jquery-1.12.2.min.js HTTP/1.1  |
| 1174 | 1.934093 | 59.67.152.250 | 220.194.79.33  | HTTP     | 390    | GET /css/gg201409.css HTTP/1.1  |
| 1178 | 1.937266 | 220.194.79.33 | 59.67.152.250  | HTTP     | 880    | HTTP/1.1 200 OK (text/css)  |
| 1212 | 1.943181 | 220.194.79.33 | 59.67.152.250  | HTTP     | 1580   | HTTP/1.1 200 OK (application/javascript)  |
| 1225 | 1.971121 | 59.67.152.250 | 220.194.79.33  | HTTP     | 383    | GET /sys/online_cal.js?ver=1 HTTP/1.1   |
| 1225 | 1.971121 | 59.67.152.250 | 220.194.79.33  | HTTP     | 383    | GET /sys/online_cal.js?ver=1 HTTP/1.1   |

Frame 1067: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits) on interface 0  
 Ethernet II, Src: Hengzhou\_Sa166:84 (58:ea:b1:5a:16:84), Dst: Dell\_9d:27:05 (48:6d:7e:9d:27:05)  
 Internet Protocol Version 4, Src: 8.8.8.8, Dst: 59.67.152.250  
 User Datagram Protocol, Src Port: 53, Dst Port: 49425  
 Domain Name System (response)  
 [Request ID: 3084]  
 [Time: 0.001891000 seconds]  
 Transaction ID: 0xf43c  
 Flags: 0x0100 Standard query response, No error  
 Questions: 1  
 Answer RRs: 5  
 Authority RRs: 0  
 Additional RRs: 0  
 Queries  
 Answers  
 > www.enorth.com.cn: type CNAME, class IN, cname www.enorth.com.cn.cdn.dnsv1.com  
 > www.enorth.com.cn.cdn.dnsv1.com: type CNAME, class IN, cname 287911.s2.cdntip.com  
 > 287911.s2.cdntip.com: type A, class IN, addr 220.194.79.33  
 > 287911.s2.cdntip.com: type A, class IN, addr 220.194.79.34  
 > 287911.s2.cdntip.com: type A, class IN, addr 125.39.132.236

以访问 (live capture in progress)

过滤: 10000 · 已捕获: 527 (2.9K)

配置文件: Default

请根据图中信息回答下列问题。

- (1) 在浏览器中输入的URL是 1 www.enorth.com.cn
- (2) 该主机上使用的DNS服务器的IP地址是 2
- (3) 该主机的IP地址是 3，该主机的MAC地址是 4
- (4) 域名www.enorth.com.cn对应的IP地址是 5

# DNS域名解析

## 得分点6：根据IP地址判断功能

题目给一个IP地址，需要判断其为什么对象的IP地址，进而判断其功能

公众号：大头计算机二级

微博/B站：@大头博士先生



3、下图是一台主机在命令行模式下执行某个命令时用sniffer捕获的数据包。

| No. | State | Source Address    | Dest Address     | Summary   | Len (Bytes) | Rel. Time | Delta Time |
|-----|-------|-------------------|------------------|---|-------------|-----------|------------|
| 158 |       | [202.113.78.123]  | [59.67.148.5]    | DNS: C ID=20353 OP=QUERY NAME=www.bupt.edu.cn             | 75          | 0:00:0    | 3.321.717  |
| 159 |       | [59.67.148.5]     | [202.113.78.123] | DNS: R ID=20353 OP=QUERY STAT=OK NAME=www.bupt.edu.cn     | 91          | 0:00:0    | 0.007.784  |
| 160 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0:00:0    | 0.002.452  |
| 161 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0:00:0    | 0.003.882  |
| 163 |       | [184.168.124.135] | [202.113.78.123] | TCP: D=10556 S=80 SYN ACK=1642834386 SEQ=320707678 LEN=60 | 0           | 0:00:0    | 0.440.005  |
| 175 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0:00:0    | 0.554.387  |
| 176 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0:00:0    | 0.003.432  |
| 196 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0:00:0    | 0.996.602  |
| 197 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0:00:0    | 0.003.469  |
| 217 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0:00:1    | 0.996.605  |
| 218 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0:00:1    | 0.003.429  |

IP:

ICMP: ----- ICMP header -----

ICMP:

ICMP: Type = 8 ( ① )

ICMP: Code = 0

ICMP: Checksum = D844 (correct)

ICMP: Identifier = 512

ICMP: Sequence number = 26880

ICMP: [1024 bytes of data]

ICMP:

ICMP: [Normal end of "ICMP header".]

ICMP:

00000020: 45 fe 08 00 d8 44 02 00 69 00 61 62 63 64 65 66 E7 00 i.abcdef

00000030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv

00000040: 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 wabdefghijklmno

00000050: 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 pqrstuvwxyzabdefgh

00000060: 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 ijklmnopqrstuvwa

请根据图中信息回答下列问题。

- 该主机上执行的命令完整内容是 ① 。
- 主机59.67.148.5的功能是 ② ，其提供服务的缺省端口是 ③ 。
- 图中①处删除了部分显示信息，该信息应该是 ④ 。
- 如果用Sniffer统计网络流量中各种应用的分布情况，应打开的窗口是 ⑤ 。

3、下图是一台主机在命令行模式下执行某个命令时用sniffer捕获的数据包。

| No. | State | Source Address    | Dest Address     | Summary   | Len (Bytes) | Rel. Time      | Delta Time |
|-----|-------|-------------------|------------------|---|-------------|----------------|------------|
| 158 |       | [202.113.78.123]  | [59.67.148.5]    | DNS: C ID=20353 OP=QUERY NAME=www.bupt.edu.cn           | 75          | 0.00:0.321.717 |            |
| 159 |       | [59.67.148.5]     | [202.113.78.123] | DNS: R ID=20353 OP=QUERY STAT=OK NAME=www.bupt.edu.cn   | 91          | 0.00:0.007.784 |            |
| 160 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0.00:0.002.452 |            |
| 161 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0.00:0.003.882 |            |
| 162 |       | [184.168.124.135] | [202.113.78.123] | TCP: D=10556 S=80 SYN ACK=1642834386 SEQ=320707678 LEN= | 60          | 0.00:0.040.005 |            |
| 175 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0.00:0.054.387 |            |
| 176 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0.00:0.003.432 |            |
| 196 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0.00:0.096.602 |            |
| 197 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0.00:0.003.469 |            |
| 217 |       | [202.113.78.123]  | www.bupt.edu.cn  | ICMP: Echo  | 1066        | 0.00:0.096.605 |            |
| 218 |       | www.bupt.edu.cn   | [202.113.78.123] | ICMP: Echo reply  | 1066        | 0.00:0.003.429 |            |

IP:

ICMP: ICMP header

ICMP:

ICMP: Type = 8 ( ① )

ICMP: Code = 0

ICMP: Checksum = D844 (correct)

ICMP: Identifier = 512

ICMP: Sequence number = 26880

ICMP: [1024 bytes of data]

ICMP:

ICMP: [Normal end of "ICMP header".]

ICMP:

00000020: 45 fe 08 00 d8 44 02 00 69 00 61 62 63 64 65 66 E? 00 i abcdef  
00000030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuv  
00000040: 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 ef wabcedefghijklmno  
00000050: 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 pqrstuvwxyzabcedefgh  
00000060: 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 6f ijklmnopqrstuvwa

请根据图中信息回答下列问题。

- 该主机上执行的命令完整内容是 ① 。
- 主机59.67.148.5的功能是 ② DNS ，其提供服务的缺省端口是 ③ 。
- 图中①处删除了部分显示信息，该信息应该是 ④ 。
- 如果用Sniffer统计网络流量中各种应用的分布情况，应打开的窗口是 ⑤ 。

## TCP

传输控制协议 (TCP, Transmission Control Protocol) 是为了在不可靠的互联网络上提供可靠的端到端字节流而专门设计的一个传输协议。

公众号：大头计算机二级

微博/B站：@大头博士先生





# TCP三次握手



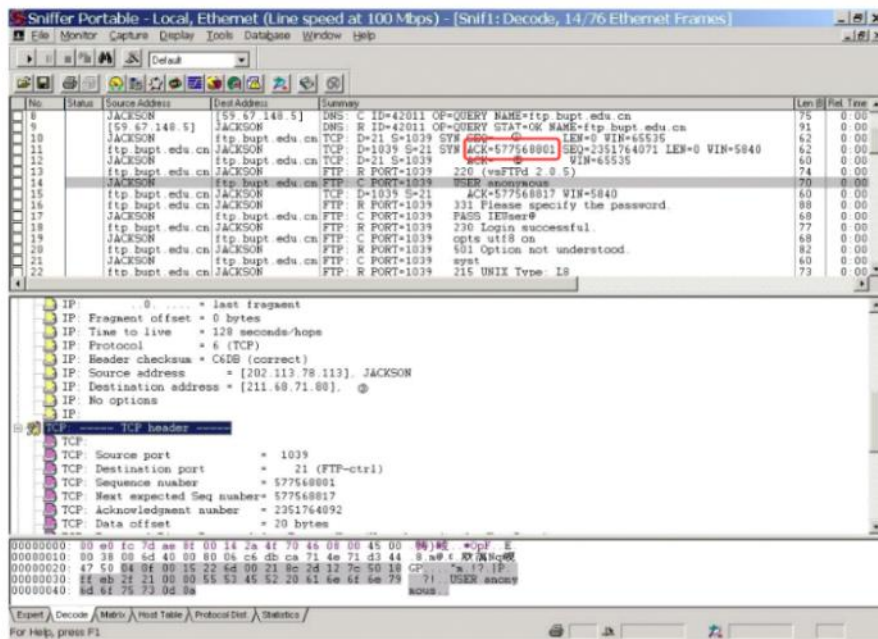
建立连接时, TCP FLAG=02

公众号: 大头计算机二级

微博/B站: @大头博士先生



1. 下图是校园网某台主机使用浏览器访问某个网站, 在地址栏键入其URL时用miffler捕获的数据包。

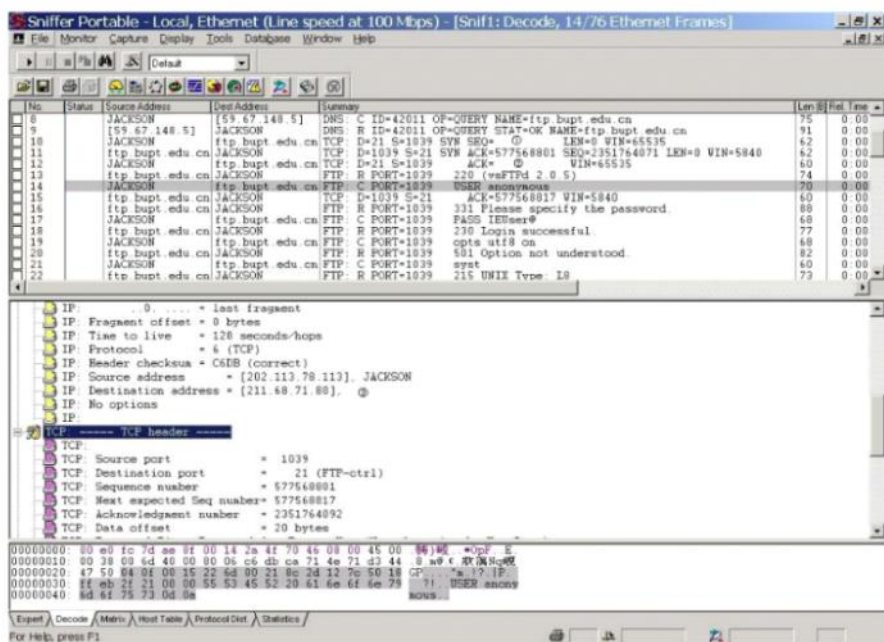


请根据图中信息回答下列问题。

- (1) 该URL是 577568801-1。
- (2) 该主机的IP地址是 2。
- (3) 图中的①②③删除了部分显示信息, 其中①应该是 3 577568800, ②应该是 4。
- (4) 该主机配置的DNS服务器的IP地址是 5。



- 1、下图是校园网某台主机使用浏览器访问某个网站，在地址栏键入其URL时用sniffer捕获的数据包。



请根据图中信息回答下列问题。

- (1) 该URL是 ①。
- (2) 该主机的IP地址是 ②。
- (3) 图中的①②③删除了部分显示信息，其中①应该是 ③，②应该是 ④。
- (4) 该主机配置的DNS服务器的IP地址是 ⑤。

## TCP得分点

- 1、建立连接时，TCP FLAG=02
- 2、seq与ack值计算
- 3、连接后，只需要有ACK即可

| No. | Status | Source Address  | Dest Address    | Summary  | Len | Rel. Time |
|-----|--------|-----------------|-----------------|--|-----|-----------|
| 8   |        | JACKSON         | [59.67.148.5]   | DNS: C ID=42011 OP=QUERY NAME=ftp.bupt.edu.cn                    | 75  | 0.00      |
| 9   |        | [59.67.148.5]   | JACKSON         | DNS: R ID=42011 OP=QUERY STAT=OK NAME=ftp.bupt.edu.cn            | 91  | 0.00      |
| 10  |        | ftp.bupt.edu.cn | JACKSON         | TCP: D=21 S=1039 SYN SEQ= 0 LEN=0 WIN=65535                      | 62  | 0.00      |
| 11  |        | ftp.bupt.edu.cn | JACKSON         | TCP: D=1039 S=21 SYN ACK=577568801 SEQ=2351764071 LEN=0 WIN=5840 | 62  | 0.00      |
| 12  |        | JACKSON         | ftp.bupt.edu.cn | TCP: D=21 S=1039 ACK= 0 WIN=65535                                | 60  | 0.00      |
| 13  |        | ftp.bupt.edu.cn | JACKSON         | FTP: R PORT=1039 220 (vsFTPd 2.0.5)                              | 74  | 0.00      |
| 14  |        | JACKSON         | ftp.bupt.edu.cn | FTP: C PORT=1039 USER anonymous                                  | 70  | 0.00      |
| 15  |        | ftp.bupt.edu.cn | JACKSON         | TCP: D=1039 S=21 ACK=577568817 WIN=5840                          | 60  | 0.00      |
| 16  |        | ftp.bupt.edu.cn | JACKSON         | FTP: R PORT=1039 331 Please specify the password.                | 88  | 0.00      |
| 17  |        | JACKSON         | ftp.bupt.edu.cn | FTP: C PORT=1039 PASS IEUser@                                    | 68  | 0.00      |
| 18  |        | ftp.bupt.edu.cn | JACKSON         | FTP: R PORT=1039 230 Login successful.                           | 77  | 0.00      |
| 19  |        | JACKSON         | ftp.bupt.edu.cn | FTP: C PORT=1039 opts utf8 on                                    | 68  | 0.00      |
| 20  |        | ftp.bupt.edu.cn | JACKSON         | FTP: R PORT=1039 501 Option not understood.                      | 82  | 0.00      |
| 21  |        | JACKSON         | ftp.bupt.edu.cn | FTP: C PORT=1039 syst  | 60  | 0.00      |
| 22  |        | ftp.bupt.edu.cn | JACKSON         | FTP: R PORT=1039 215 UNIX Type: L8                               | 73  | 0.00      |

公众号：大头计算机二级

微博/B站：@大头博士先生

# FTP文本传输协议

文件传送协议（FTP）允许用户从服务器上获取文件副本并下载到本地计算机上、或将本地计算机上的一个文件上传到服务器。

FTP端口号为21

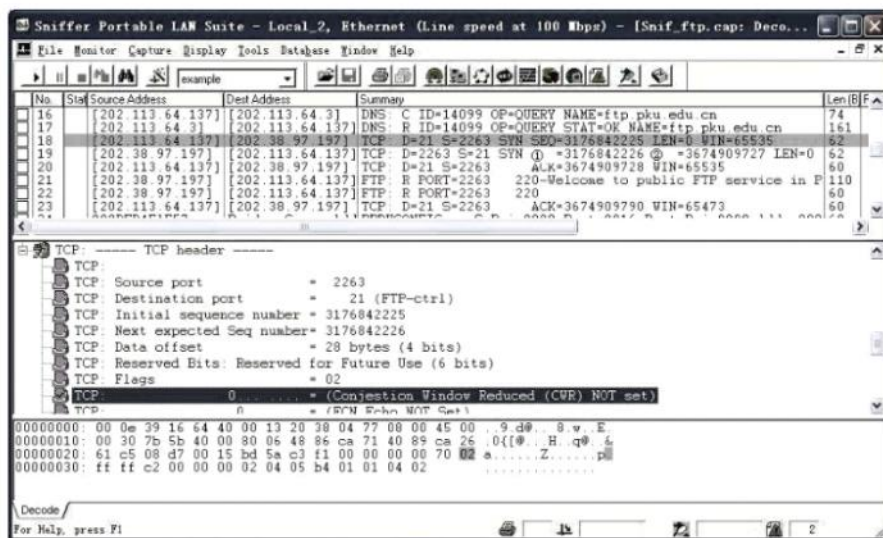
命令语句为：ftp <域名>



公众号：大头计算机二级

微博/B站：@大头博士先生

32、下图是一台Windows主机在命令行模式下执行某个命令时用Sniffer捕获到的数据包。

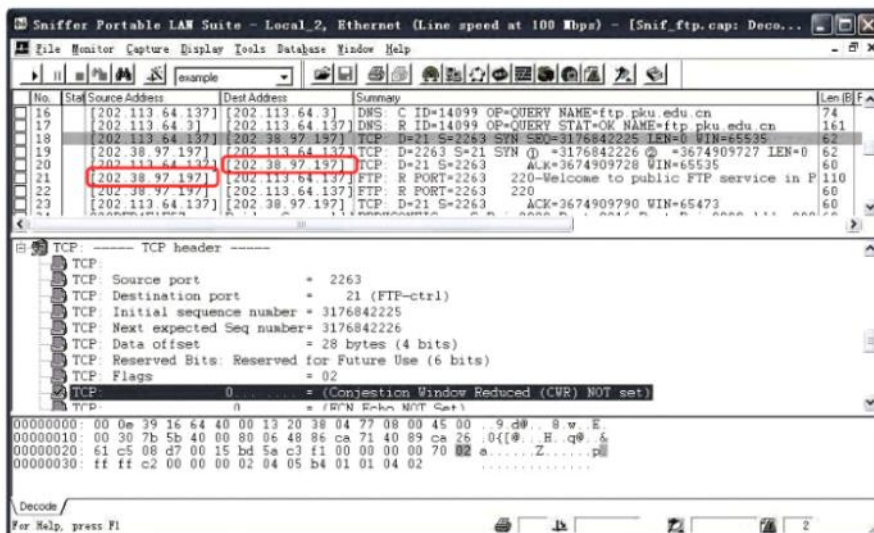


请根据图中信息回答下列问题。

- (1) 该主机上配置的域名服务器的IP地址是 ① 。
- (2) 图中的①和②删除了部分显示信息，其中①处的信息应该是 ② 。
- (3) 主机202.38.97.197是 ③ 服务器，其提供服务的端口是 ④ 。
- (4) 该主机上执行的命令是 ⑤ 。



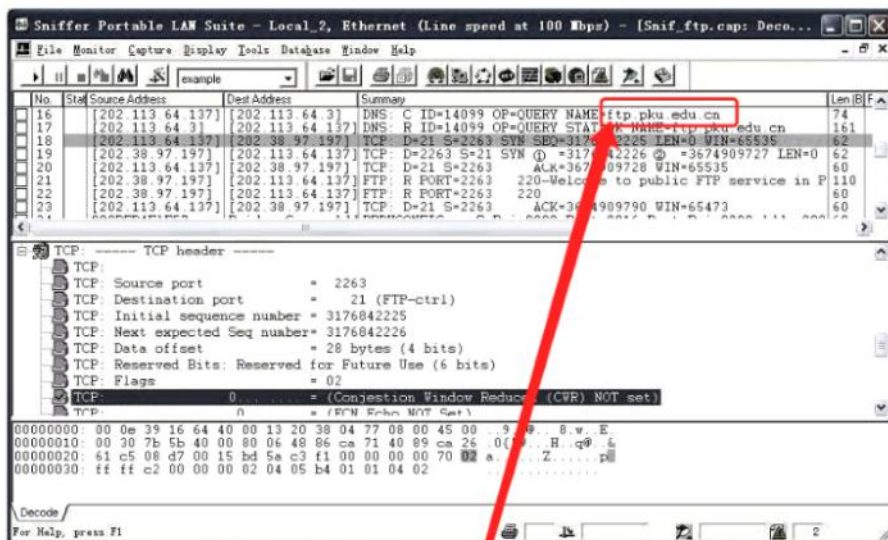
32、下图是一台Windows主机在命令行模式下执行某个命令时用Sniffer捕获到的数据包。



请根据图中信息回答下列问题。

- (1) 该主机上配置的域名服务器的IP地址是 ① 。
- (2) 图中的①和②删除了部分显示信息，其中①处的信息应该是 ② 。
- (3) 主机202.38.97.197是 ③ ftp 服务器，其提供服务的端口是 ④ 21 。
- (4) 该主机上执行的命令是 ⑤ 。

32、下图是一台Windows主机在命令行模式下执行某个命令时用Sniffer捕获到的数据包。



请根据图中信息回答下列问题。

- (1) 该主机上配置的域名服务器的IP地址是 ① 。
- (2) 图中的①和②删除了部分显示信息，其中①处的信息应该是 ② 。
- (3) 主机202.38.97.197是 ③ ftp 服务器，其提供服务的端口是 ④ 21 。
- (4) 该主机上执行的命令是 ⑤ ftp ftp.pku.edu.cn 。

# ICMP控制报文协议

ICMP协议主要用来检测网络通信故障和实现链路追踪

## 1、ping命令

ping是一种因特网包探索器，用于测试网络连接量的程序；默认发送4个ICMP报文，每个报文包含64字节数据

## 2、tracert命令

第一条报文：源地址是客户机地址，目的地址是网站地址

公众号：大头计算机二级

微博/B站：@大头博士先生



| Decode, 18/97 Ethernet Frames |     |                  |                  |  |        |             |
|-------------------------------|-----|------------------|------------------|--|--------|-------------|
| No.                           | Sta | Source Address   | Dest Address     | Summary  | Len(B) | Ret Time    |
| 5                             |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=23868 OP=QUERY NAME=mail.tj.edu.cn   | 74     | 0:00:04.267 |
| 6                             |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn   | 115    | 0:00:04.270 |
| 7                             |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=45720 OP=QUERY NAME=mail.tj.edu.cn   | 74     | 0:00:04.273 |
| 8                             |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn   | 160    | 0:00:04.274 |
| 9                             | #   | [202.113.64.137] | [202.113.64.137] | Expert: Time-to-live expiring<br>ICMP: Echo  | 106    | 0:00:04.276 |
| 10                            | #   | [202.113.64.129] | [202.113.64.137] | Expert: Time-to-live exceeded in transit<br>ICMP: Time exceeded (Time to live exceeded in transit) | 70     | 0:00:04.276 |
| 11                            | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live expiring<br>ICMP: Echo  | 106    | 0:00:04.276 |
| 12                            | #   | [202.113.64.129] | [202.113.64.137] | Expert: Time-to-live exceeded in transit<br>ICMP: Time exceeded (Time to live exceeded in transit) | 70     | 0:00:04.276 |
| 13                            | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live expiring<br>ICMP: Echo  | 106    | 0:00:04.279 |
| 14                            | #   | [202.113.64.129] | [202.113.64.137] | Expert: Time-to-live exceeded in transit<br>ICMP: Time exceeded (Time to live exceeded in transit) | 70     | 0:00:04.279 |
| 15                            |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr   | 87     | 0:00:04.280 |
| 16                            |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64   | 149    | 0:00:04.281 |
| 17                            |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo   | 106    | 0:00:05.266 |
| 18                            | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transit<br>ICMP: Time exceeded (Time to live exceeded in transit) | 70     | 0:00:05.266 |
| 19                            |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo   | 106    | 0:00:05.266 |
| 20                            | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transit   | 70     | 0:00:05.265 |

|                           |                      |
|---------------------------|----------------------|
| ICMP: Identification      | = 4413               |
| ICMP: Flags               | = 0X                 |
| ICMP: .0. ....            | = may fragment       |
| ICMP: .0. ....            | = last fragment      |
| ICMP: Fragment offset     | = 0 bytes            |
| ICMP: Time to live        | = 1 seconds/hops     |
| ICMP: Protocol            | = 1 ( @ )            |
| ICMP: Header checksum     | = B548 (correct)     |
| ICMP: Source address      | = [ ③ ]              |
| ICMP: Destination address | = [211.81.20.208]. ④ |
| ICMP: No options          |                      |



# ICMP控制报文协议

## 得分点1：判断协议类型

可以根据报文详情分析，也可以根据协议端口号，ICMP协议端口号为1

公众号：大头计算机二级

微博/B站：@大头博士先生



18、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| Decode, 18/97 Ethernet Frames |     |                  |                  |  |                   |
|-------------------------------|-----|------------------|------------------|--|-------------------|
| No                            | Sta | Source Address   | Dest Address     | Summary  | Len [B] Ret. Time |
| 5                             |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=23868 OP=QUERY NAME=mail.tj.edu.cn                         | 74 0:00:04.257    |
| 6                             |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn                 | 115 0:00:04.270   |
| 7                             |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=45720 OP=QUERY NAME=mail.tj.edu.cn                         | 74 0:00:04.273    |
| 8                             |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn                 | 160 0:00:04.274   |
| 9                             | #   | [202.113.64.137] | ①                | Expert: Time-to-live expiring  | 106 0:00:04.275   |
| 10                            |     | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70 0:00:04.276    |
| 11                            | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live exceeded in transit                             | 106 0:00:04.276   |
| 12                            |     | [202.113.64.129] | [202.113.64.137] | ICMP: Time exceeded (Time to live exceeded in transit)               | 106 0:00:04.276   |
| 13                            | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live expiring  | 106 0:00:04.275   |
| 14                            |     | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70 0:00:04.275    |
| 15                            |     | [202.113.64.137] | [202.113.64.3]   | ICMP: Time exceeded (Time to live exceeded in transit)               | 106 0:00:04.280   |
| 16                            |     | [202.113.64.3]   | [202.113.64.137] | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr                 | 87 0:00:04.281    |
| 17                            |     | [202.113.64.137] | mail.tj.edu.cn   | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64.113.202.in-addr | 149 0:00:04.281   |
| 18                            | #   | [202.113.77.253] | [202.113.64.137] | ICMP: Echo   | 106 0:00:05.268   |
| 19                            |     | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live exceeded in transit                             | 70 0:00:05.268    |
| 20                            | #   | [202.113.77.253] | [202.113.64.137] | ICMP: Echo   | 106 0:00:05.268   |

|                           |                      |
|---------------------------|----------------------|
| ICMP: Identification      | = 4413               |
| ICMP: Flags               | = 0X                 |
| ICMP: ..0..               | = may fragment       |
| ICMP: ..0..               | = last fragment      |
| ICMP: Fragment offset     | = 0 bytes            |
| ICMP: Time to live        | = 1 seconds/hops     |
| ICMP: Protocol            | = 1 (ICMP)           |
| ICMP: Header checksum     | = B548 (correct)     |
| ICMP: Source address      | = [ ③ ]              |
| ICMP: Destination address | = [211.81.20.208], ④ |
| ICMP:                     | No options           |

请根据图中信息回答下列问题。

- (1) 该主机上配置的网关是 ① 。
- (2) IP地址为202.113.77.253的设备应具备的功能是 ② 。
- (3) 图中的①~④删除了部分显示信息，其中②处应该是 ③ ，④处应该是 ④ 。
- (4) 该主机上执行的命令是 ⑤ 。



18、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| No. | Sta | Source Address   | Dest Address     | Summary   | Len | Rel. Time   |
|-----|-----|------------------|------------------|---|-----|-------------|
| 5   |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=23868 OP=QUERY NAME=mail.tj.edu.cn            | 74  | 0:00:04.267 |
| 6   |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn    | 115 | 0:00:04.272 |
| 7   |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=45720 OP=QUERY NAME=mail.tj.edu.cn            | 74  | 0:00:04.273 |
| 8   |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn    | 160 | 0:00:04.274 |
| 9   | #   | [202.113.64.137] | ①                | Expert: Time-to-live expiring                           | 106 | 0:00:04.276 |
|     |     |                  |                  | ICMP: Echo  |     |             |
| 10  | #   | [202.113.64.129] | [202.113.64.137] | Expert: Time-to-live exceeded in transmit               | 70  | 0:00:04.276 |
|     |     |                  |                  | ICMP: Time exceeded (Time to live exceeded in transmit) |     |             |
| 11  | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live expiring                           | 106 | 0:00:04.278 |
|     |     |                  |                  | ICMP: Echo  |     |             |
| 12  | #   | [202.113.64.129] | [202.113.64.137] | Expert: Time-to-live exceeded in transmit               | 70  | 0:00:04.278 |
|     |     |                  |                  | ICMP: Time exceeded (Time to live exceeded in transmit) |     |             |
| 13  | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live expiring                           | 106 | 0:00:04.279 |
|     |     |                  |                  | ICMP: Echo  |     |             |
| 14  | #   | [202.113.64.129] | [202.113.64.137] | Expert: Time-to-live exceeded in transmit               | 70  | 0:00:04.279 |
|     |     |                  |                  | ICMP: Time exceeded (Time to live exceeded in transmit) |     |             |
| 15  |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr    | 87  | 0:00:04.280 |
| 16  |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64    | 149 | 0:00:04.281 |
| 17  |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo  | 106 | 0:00:05.268 |
| 18  | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transmit               | 70  | 0:00:05.268 |
|     |     |                  |                  | ICMP: Time exceeded (Time to live exceeded in transmit) |     |             |
| 19  |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo  | 106 | 0:00:05.268 |
| 20  | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transmit               | 70  | 0:00:05.268 |
|     |     |                  |                  | ICMP: Echo  |     |             |

|                           |                      |
|---------------------------|----------------------|
| ICMP: Identification      | = 4413               |
| ICMP: Flags               | = 0X                 |
| ICMP: .0. ....            | = may fragment       |
| ICMP: .0. ....            | = last fragment      |
| ICMP: Fragment offset     | = 0 bytes            |
| ICMP: Time to live        | = 1 seconds/hops     |
| ICMP: Protocol            | = ① ( ② )            |
| ICMP: Header checksum     | = B9 (correct)       |
| ICMP: Source address      | = ③                  |
| ICMP: Destination address | = [202.113.20.208] ④ |
| ICMP: No options          |                      |

请根据图中信息回答下列问题。

- 该主机上配置的网关是 ①。
- IP地址为202.113.77.253的设备应具备的功能是 ②。
- 图中的①~④删除了部分显示信息，其中②处应该是 ③ ICMP，③处应该是 ④。
- 该主机上执行的命令是 ⑤。

## ICMP控制报文协议

得分点2：网关

tracert探测到的第一个路由器，即为网关

公众号：大头计算机二级

微博/B站：@大头博士先生



18、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| No. | Sta | Source Address   | Dest Address     | Summary  | Len [B] | Rel. Time   |
|-----|-----|------------------|------------------|--|---------|-------------|
| 5   |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=23868 OP=QUERY NAME=mail.tj.edu.cn         | 74      | 0:00:04.267 |
| 6   |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn | 115     | 0:00:04.270 |
| 7   |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=45720 OP=QUERY NAME=mail.tj.edu.cn         | 74      | 0:00:04.273 |
| 8   |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn | 160     | 0:00:04.274 |
| 9   | #   | [202.113.64.137] | ①                | Expert: Time-to-live expiring                        | 106     | 0:00:04.276 |
| 10  | #   | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70      | 0:00:04.276 |
| 11  | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live exceeded in transit             | 106     | 0:00:04.276 |
| 12  | #   | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70      | 0:00:04.276 |
| 13  | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live exceeded in transit             | 106     | 0:00:04.275 |
| 14  | #   | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70      | 0:00:04.275 |
| 15  |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202 in-add  | 87      | 0:00:04.280 |
| 16  |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64 | 149     | 0:00:04.281 |
| 17  |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo   | 106     | 0:00:05.268 |
| 18  | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transit             | 70      | 0:00:05.268 |
| 19  |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo   | 106     | 0:00:05.268 |
| 20  | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transit             | 70      | 0:00:05.268 |

|                           |                      |
|---------------------------|----------------------|
| ICMP: Identification      | = 4413               |
| ICMP: Flags               | = 0X                 |
| ICMP: ..0..               | = may fragment       |
| ICMP: ..0..               | = last fragment      |
| ICMP: Fragment offset     | = 0 bytes            |
| ICMP: Time to live        | = 1 seconds/hops     |
| ICMP: Protocol            | = 1 ( @ )            |
| ICMP: Header checksum     | = B548 (correct)     |
| ICMP: Source address      | = [ @ ]              |
| ICMP: Destination address | = [211.81.20.208], ④ |
| ICMP: No options          |                      |

请根据图中信息回答下列问题。

- (1) 该主机上配置的网关是 ① 。
- (2) IP地址为202.113.77.253的设备应具备的功能是 ② 。
- (3) 图中的①~④删除了部分显示信息，其中②处应该是 ③ ，③处应该是 ④ 。
- (4) 该主机上执行的命令是 ⑤ 。

18、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。

| No. | Sta | Source Address   | Dest Address     | Summary  | Len [B] | Rel. Time   |
|-----|-----|------------------|------------------|--|---------|-------------|
| 5   |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=23868 OP=QUERY NAME=mail.tj.edu.cn         | 74      | 0:00:04.267 |
| 6   |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn | 115     | 0:00:04.270 |
| 7   |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=45720 OP=QUERY NAME=mail.tj.edu.cn         | 74      | 0:00:04.273 |
| 8   |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn | 160     | 0:00:04.274 |
| 9   | #   | [202.113.64.137] | ①                | Expert: Time-to-live expiring                        | 106     | 0:00:04.276 |
| 10  | #   | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70      | 0:00:04.276 |
| 11  | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live exceeded in transit             | 106     | 0:00:04.276 |
| 12  | #   | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70      | 0:00:04.276 |
| 13  | #   | [202.113.64.137] | mail.tj.edu.cn   | Expert: Time-to-live exceeded in transit             | 106     | 0:00:04.275 |
| 14  | #   | [202.113.64.129] | [202.113.64.137] | ICMP: Echo   | 70      | 0:00:04.275 |
| 15  |     | [202.113.64.137] | [202.113.64.3]   | DNS: C ID=33660 OP=QUERY NAME=129.64.113.202 in-add  | 87      | 0:00:04.280 |
| 16  |     | [202.113.64.3]   | [202.113.64.137] | DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64 | 149     | 0:00:04.281 |
| 17  |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo   | 106     | 0:00:05.268 |
| 18  | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transit             | 70      | 0:00:05.268 |
| 19  |     | [202.113.64.137] | mail.tj.edu.cn   | ICMP: Echo   | 106     | 0:00:05.268 |
| 20  | #   | [202.113.77.253] | [202.113.64.137] | Expert: Time-to-live exceeded in transit             | 70      | 0:00:05.268 |

|                           |                      |
|---------------------------|----------------------|
| ICMP: Identification      | = 4413               |
| ICMP: Flags               | = 0X                 |
| ICMP: ..0..               | = may fragment       |
| ICMP: ..0..               | = last fragment      |
| ICMP: Fragment offset     | = 0 byte             |
| ICMP: Time to live        | = 1 seconds/hops     |
| ICMP: Protocol            | = 1 ( @ )            |
| ICMP: Header checksum     | = B548 (correct)     |
| ICMP: Source address      | = [ @ ]              |
| ICMP: Destination address | = [211.81.20.208], ④ |
| ICMP: No options          |                      |

请根据图中信息回答下列问题。

- (1) 该主机上配置的网关是 ① 202.113.64.129 。
- (2) IP地址为202.113.77.253的设备应具备的功能是 ② 。
- (3) 图中的①~④删除了部分显示信息，其中②处应该是 ③ ，③处应该是 ④ 。
- (4) 该主机上执行的命令是 ⑤ 。

# ICMP控制报文协议

## 得分点3：ICMP源地址和目的地址

整个tracert过程，源地址一定是客户机的地址，目的地址是网站的地址

公众号：大头计算机二级

微博/B站：@大头博士先生



21、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。



请根据图中信息回答下列问题。

(1) 主机mail.tj.edu.cn对应的IP地址是 ① 。

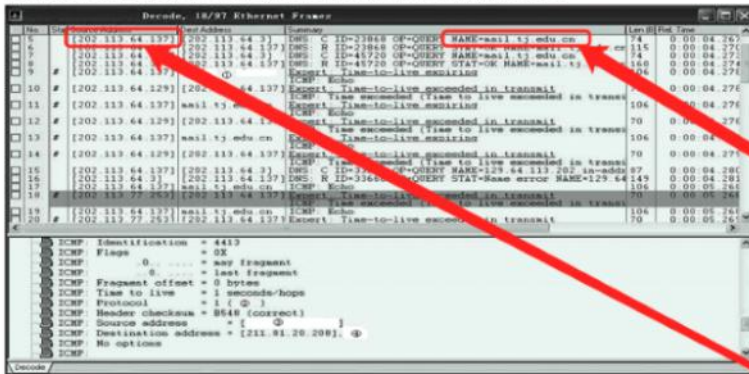
(2) 图中的①~④删除了部分显示信息，其中①处应该是 ② ，③处应该是 ③ ，④处应该是 ④ 。

(3) 该主机上执行的命令是 ⑤ 。





21、下图是校园网某台主机在命令行模式执行某个命令时用sniffer捕获的数据包。



请根据图中信息回答下列问题。

- (1) 主机mail.tj.edu.cn对应的IP地址是 ① 。
- (2) 图中的①~④删除了部分显示信息，其中①处应该是 ② ，③处应该是 ③ 202.113.64.137 ，④处应该是 ④ mail.tj.edu.cn 。
- (3) 该主机上执行的命令是 ⑤ 。



## HTTP超文本传输协议

超文本传输协议 (Hyper Text Transfer Protocol, HTTP) 是一个简单的请求-响应协议，它通常运行在TCP之上。它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。

get命令

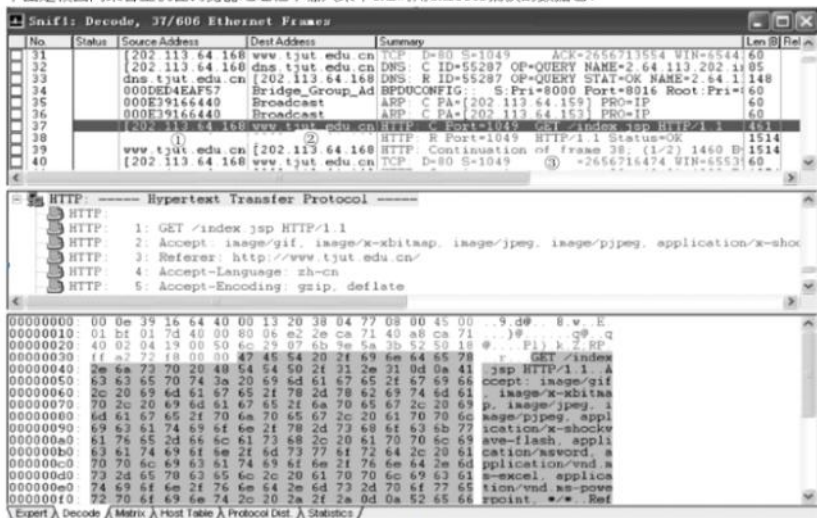
post命令

公众号：大头计算机二级

微博/B站：@大头博士先生



35、下图是校园网某台主机在浏览器地址栏中输入某个URL时用sniffer捕获的数据包。

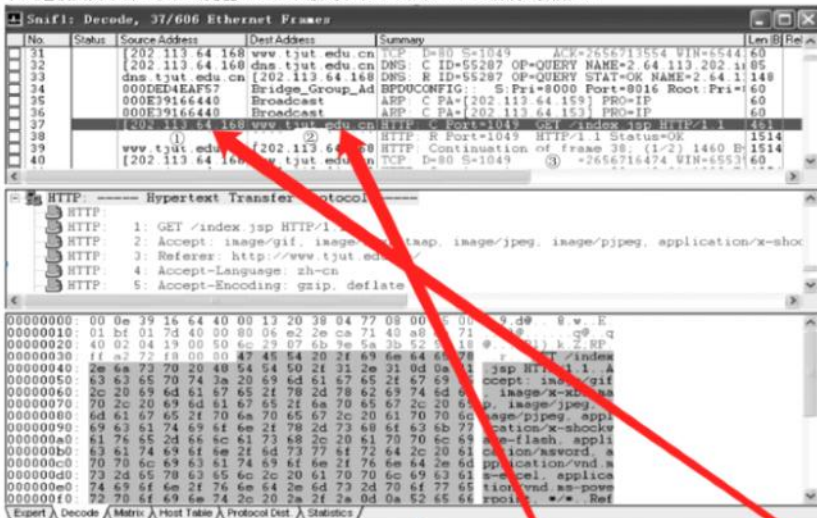


请根据图中信息回答下列问题。

- (1) 该主机的IP地址是 ① ，IP地址202.113.64.2对应的主机名是 ② 。
- (2) 图中的①~③删除了部分显示信息，其中①处应该是 ③ ，②处应该是 ④ ，③处应该是 ⑤ 。



35、下图是校园网某台主机在浏览器地址栏中输入某个URL时用sniffer捕获的数据包。



请根据图中信息回答下列问题。

- (1) 该主机的IP地址是 ① ，IP地址202.113.64.2对应的主机名是 ② 。
- (2) 图中的①~③删除了部分显示信息，其中①处应该是 ③ www.tjut.edu.cn ，②处应该是 ④ 202.113.64.168 ，③处应该是 ⑤ 。



# 那些奇奇怪怪的端口

ICMP协议端口：1

TCP协议端口：6

FTP协议端口：21

公众号：大头计算机二级

微博/B站：@大头博士先生



# E-mail基本概念

电子邮件系统是Internet上最重要的网络应用之一。电子邮件系统使用的协议主要有：简单邮件传送协议（SMTP），用于发送电子邮件，SMTP默认的TCP端口为25；邮局协议目前使用的是第三版本的邮局协议，即POP3，默认的TCP端口为110，用户可以使用POP3协议可以访问并读取邮件服务器上的邮件信息；Internet消息访问协议IMAP是用于客户端管理邮件服务器上邮件的协议，目前是IMAP4，默认的TCP端口为143。

公众号：大头计算机二级

微博/B站：@大头博士先生

