



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



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.	Src	Dest Address	Summary	Len (B)	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]	①	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]	mail.nj.edu.cn	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	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]	mail.nj.edu.cn	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	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.a	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.in-addr.a	149	0:00:04.281
17	[202.113.64.133]	mail.nj.edu.cn	ICMP: Echo	106	0:00:05.261
18	# [202.113.77.253]	[202.113.64.133]	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	70	0:00:05.261
19	[202.113.64.133]	mail.nj.edu.cn	ICMP: Echo	106	0:00:05.265
20	# [202.113.77.253]	[202.113.64.133]	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	70	0:00:05.265

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 Address	Summary	Len (B)	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]	①	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]	mail.nj.edu.cn	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	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]	mail.nj.edu.cn	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	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.a	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.in-addr.a	149	0:00:04.281
17	[202.113.64.133]	mail.nj.edu.cn	ICMP: Echo	106	0:00:05.261
18	# [202.113.77.253]	[202.113.64.133]	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	70	0:00:05.261
19	[202.113.64.133]	mail.nj.edu.cn	ICMP: Echo	106	0:00:05.265
20	# [202.113.77.253]	[202.113.64.133]	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	70	0:00:05.265

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 。



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。

Decode, 18/97 Ethernet Frames						
No.	Src[Source Address]	Dest[Dest Address]	Summary	Len[Byte]	Rel Time	
5 #	[202.113.64.133]	[202.113.64.71]	[DNS] C ID=23868 OP=QUERY NAME=mail.nj.edu.cn	74	0:00:04.267	
6 #	[202.113.64.71]	[202.113.64.133]	[DNS] R ID=23868 OP=QUERY STAT=OK NAME=mail.nj.edu.cn	115	0:00:04.276	
7 #	[202.113.64.133]	[202.113.64.71]	[DNS] C ID=45720 OP=QUERY NAME=mail.nj.edu.cn	74	0:00:04.276	
8 #	[202.113.64.71]	[202.113.64.133]	[DNS] R ID=45720 OP=QUERY STAT=OK NAME=mail.nj.edu.cn	168	0:00:04.274	
9 #	[202.113.64.133]	(①)	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]	(②)	Expert: Time-to-live exceeded (Time to live exceeded in transmit)	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]	mail.nj.edu.cn	Expert: Time-to-live expiring	106	0:00:04.275	
14 #	[202.113.64.129]	[202.113.64.133]	ICMP Echo	70	0:00:04.275	
15 #	[202.113.64.133]	[202.113.64.71]	ICMP: Time exceeded (Time to live exceeded in transmit)	87	0:00:04.280	
16 #	[202.113.64.71]	[202.113.64.133]	[DNS] C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr.a	149	0:00:04.281	
17 #	[202.113.64.133]	mail.nj.edu.cn	[DNS] R ID=33660 OP=QUERY STAT=Name error NAME=129.64.113.202.in-addr.a	106	0:00:05.265	
18 #	[202.113.77.253]	[202.113.64.133]	ICMP: Time exceeded (Time to live exceeded in transmit)	70	0:00:05.265	
19 #	[202.113.64.133]	mail.nj.edu.cn	ICMP Echo	106	0:00:05.266	
20 #	[202.113.77.253]	[202.113.64.133]	Expert: Time-to-live exceeded in transmit	70	0:00:05.265	

Decode /

ICMP: Identification = 4413
ICMP: Flags = OK
ICMP: 0... = may fragment
ICMP: ...0 = last fragment
ICMP: Fragment offset = 0 bytes
ICMP: Time to live = 1 seconds/hops
ICMP: Protocol = 1 (①)
ICMP: Header checksum = B548 (correct)
ICMP: Source address = [②]
ICMP: Destination address = [218.81.20.208].③
ICMP: No options
ICMP

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①~⑤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/Mac	Dest Address	Summary	Len [B]	Rel. Time
5	[202.113.64.133]	[202.113.64.71]	DNS: C ID=23868 OP=QUERY NAME=mail.nj.edu.cn	74	0:00:04.267
6	[202.113.64.133]	[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]	[202.113.64.71]	DNS: C ID=45720 OP=QUERY NAME=mail.nj.edu.cn	74	0:00:04.273
8	[202.113.64.71]	[202.113.64.133]	DNS: R ID=45720 OP=QUERY STAT=OK NAME=mail.nj.edu.cn	160	0:00:04.276
9	# [202.113.64.133]	①	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]	mail.nj.edu.cn	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	# [202.113.64.129]	mail.nj.edu.cn	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]	[202.113.64.71]	ICMP: Time exceeded (Time to live exceeded in transi	97	0:00:04.280
16	[202.113.64.71]	[202.113.64.133]	DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addrs	149	0:00:04.281
17	[202.113.64.133]	mail.nj.edu.cn	DNS: R ID=33660 OP=QUERY STAT=Name error NAME=129.64.113.202.in-addrs	106	0:00:04.286
18	[202.113.77.253]	[202.113.64.133]	ICMP: Echo	70	0:00:05.240
19	[202.113.64.133]	mail.nj.edu.cn	ICMP: Time exceeded (Time to live exceeded in transi	106	0:00:05.266
20	# [202.113.77.253]	[202.113.64.133]	ICMP: Echo	70	0:00:05.266

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.c, 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



19、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/Source Address	Dst/Address	Summary	Len/Bits	Raw Time
1	[202.113.64.137]	[202.113.64.21]	DNS C 1D=23868 OP=QUERY NAME=mail.tj.edu.cn	74	0.00 04.265
2	[202.113.64.137]	[202.113.64.21]	DNS C 1D=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn	74	0.00 04.271
3	[202.113.64.137]	[202.113.64.21]	DNS C 1D=45720 OP=QUERY NAME=mail.tj.edu.cn	74	0.00 04.271
4	[202.113.64.137]	[202.113.64.21]	DNS C 1D=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn	74	0.00 04.271
5	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.271
6	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.271
7	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transit	70	0.00 04.276
8	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded (Time to live exceeded in transit)	106	0.00 04.276
9	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transmit	70	0.00 04.276
10	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded (Time to live exceeded in transmit)	106	0.00 04.276
11	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.276
12	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.276
13	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transmit	70	0.00 04.276
14	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded (Time to live exceeded in transmit)	106	0.00 04.276
15	[202.113.64.137]	[202.113.64.21]	DNS C 1D=33660 OP=QUERY NAME=129.64.113.202.in-addr.a	87	0.00 04.286
16	[202.113.64.137]	[202.113.64.21]	DNS C 1D=33660 OP=QUERY STAT=Name error NAME=129.64.113.202.in-addr.a	87	0.00 04.286
17	[202.113.64.137]	[202.113.64.21]	DNS C 1D=33660 OP=QUERY NAME=error	108	0.00 04.286
18	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.286
19	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.286
20	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transmit	70	0.00 04.286

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) 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) 主机mail.tj.edu.cn对应的IP地址是 ⑤



19、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/Source Address	Dst/Address	Summary	Len/Bits	Raw Time
1	[202.113.64.137]	[202.113.64.21]	DNS C 1D=23868 OP=QUERY NAME=mail.tj.edu.cn	74	0.00 04.265
2	[202.113.64.137]	[202.113.64.21]	DNS C 1D=23868 OP=QUERY STAT=OK NAME=mail.tj.edu.cn	74	0.00 04.271
3	[202.113.64.137]	[202.113.64.21]	DNS C 1D=45720 OP=QUERY NAME=mail.tj.edu.cn	74	0.00 04.271
4	[202.113.64.137]	[202.113.64.21]	DNS C 1D=45720 OP=QUERY STAT=OK NAME=mail.tj.edu.cn	74	0.00 04.271
5	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.271
6	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.271
7	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transit	70	0.00 04.276
8	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded (Time to live exceeded in transit)	106	0.00 04.276
9	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.276
10	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.276
11	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transit	70	0.00 04.276
12	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded (Time to live exceeded in transit)	106	0.00 04.276
13	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.276
14	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.276
15	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transit	70	0.00 04.276
16	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded (Time to live exceeded in transit)	106	0.00 04.276
17	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.276
18	[202.113.64.137]	[202.113.64.21]	ICMP Echo reply	64	0.00 04.276
19	[202.113.64.137]	[202.113.64.21]	ICMP Time exceeded in transmit	70	0.00 04.286
20	[202.113.64.137]	[202.113.64.21]	ICMP Echo request	64	0.00 04.286

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) 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) 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: 59.67.152.258
  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。

No.	Time	Sources	Destinations	Protocol	Length	Info
1	1210 3.279465	59.67.152.258	8.8.8.8	DNS	72	Standard query 0x1617 A www.12306.cn
2	1210 3.279465	59.67.152.258	8.8.8.8	DNS	72	Standard query 0x1617 A www.12306.cn.jobs.com CNHPE www.12306.cn.jobs.com CNHPE 12306.xdcache.org108.com
1212	3.279511	8.8.8.8	59.67.152.258	DNS	143	Standard query response 0x1617 A www.12306.cn.jobs.com CNHPE www.12306.cn.jobs.com CNHPE 12306.xdcache.org108.com
1214	3.280225	8.8.8.8	59.67.152.258	DNS	233	Standard query response 0x1617 A www.12306.cn.jobs.com CNHPE www.12306.cn.jobs.com CNHPE 12306.xdcache.org108.com
1215	3.280225	59.67.152.258	43.226.162.67	ICMP	74	Echo (ping) request 0x00001, seq=273/4353, ttl=128 (reply in 1225)
1216	3.291382	43.226.162.67	59.67.152.258	ICMP	74	Echo (ping) reply 0x00001, seq=273/4353, ttl=53 (request in 1215)
1639	4.291232	59.67.152.258	43.226.162.67	ICMP	74	Echo (ping) request 0x00001, seq=274/4369, ttl=128 (reply in 1648)
1640	4.293273	43.226.162.67	59.67.152.258	ICMP	74	Echo (ping) reply 0x00001, seq=274/4369, ttl=53 (request in 1639)
1995	5.295095	59.67.152.258	43.226.162.67	ICMP	74	Echo (ping) request 0x00001, seq=275/4385, ttl=128 (reply in 1995)
1996	5.297982	43.226.162.67	59.67.152.258	ICMP	74	Echo (ping) reply 0x00001, seq=275/4385, ttl=53 (request in 1994)
2344	6.297345	59.67.152.258	43.226.162.67	ICMP	74	Echo (ping) request 0x00001, seq=276/5121, ttl=128 (reply in 2345)
2345	6.299298	43.226.162.67	59.67.152.258	ICMP	74	Echo (ping) reply 0x00001, seq=276/5121, ttl=53 (request in 2344)
6343	15.279160	59.67.152.258	51.255.41.275	ICMP	483	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:66:84 (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: 59.67.152.258
User Datagram Protocol, Src Port: 53, Dst Port: 60786
  Source Port: 53
  Destination Port: 60786
  Length: 128
  Checksum: 0x6d5a [Unverified]
    [Checksum Status: Unverified]
  [Stream index: 19]
  Domain Name System (response)
    [Request Id: 12306]
    [Time: 0.001960000 seconds]
    Transaction ID: 0x1617
    Flags: 0x0100 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 CNHPE, class IN, cname www.12306.cn.lxdns.com
    > www.12306.cn.lxdns: type CNHPE, class IN, cname 12306.xdcache.org108.com
    > 12306.xdcache.org108.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 ，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。

Frame 1212: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 8
Interface 8, Src: Hangzhou_Sat:60:84 (5e:0:1:1:1:1) [Bridged Adapter], Dst: 59.67.152.250
User Datagram Protocol, Src Port: 53, Dst Port: 67000
Source Port: 53
Destination Port: 67000
Length: 128
Checksum: 0x6d61 [verified]
[Checksum Status: Unverified]
[Stream Index: 19]
Domain Name System (response)
Request ID: 12101
[Time: 0.001986800 seconds]
Transaction ID: 0x1d17
Flags: 0x8100 Standard query response, No error
Question: 1
Authority: 0
Additional: 0
Queries:
www.12306.cn type A, class IN
Answers:
www.12306.cn type CNAME, cname www.12306.cn.lndns.com
www.12306.cn.lndns.com type CNAME, cname 12306.xbdcache.ourglb0.com
12306.xbdcache.ourglb0.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。

119 1.250929 172.64.135.5 59.67.152.250 HTTP 386 HTTP/1.1 400 Bad Request (text/html)
286 0.520569 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 0x5bbe & qurl.f.360.cn
1083 1.904747 59.67.152.250 8.8.8.8 DNS 73 Standard query 0x9467 AAAA qurl.f.360.cn
1084 1.905704 59.67.152.250 8.8.8.8 DNS 77 Standard query 0x4f9c A www.enorth.com.cn
1085 1.905704 59.67.152.250 8.8.8.8 DNS 77 Standard query 0x4f9c AAAA www.enorth.com.cn
1086 1.906380 8.8.8.8 59.67.152.250 DNS 133 Standard query response 0x5bbe www.enorth.com.cn A 111.206.62.164 www.enorth.com.cn
1087 1.907595 8.8.8.8 59.67.152.250 DNS 201 Standard query response 0x4f9c www.enorth.com.cn CNAME www.enorth.com.cn.dns1.com CNAME 287911.v2.cd.
1088 1.909468 8.8.8.8 59.67.152.250 DNS 210 Standard query response 0x4f9c www.enorth.com.cn A 111.206.62.164 www.enorth.com.cn
1089 1.911846 8.8.8.8 59.67.152.250 DNS 301 Standard query response 0x9467 AAAA qurl.f.360.com CNAME qurl.qh-lb.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 223 HTTP/1.1 200 OK (text/html)
1139 1.920210 59.67.152.250 111.206.62.164 HTTP 772 POST /wdinfo.php HTTP/1.1 (application/octet-stream)
1168 1.929537 59.67.152.250 220.194.79.33 HTTP 389 GET /sys/share/jquery-1.10.2.min.js HTTP/1.1
1174 1.934093 59.67.152.250 220.194.79.33 HTTP 390 GET /css/gz201409.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 381 GET /sys/online_calc.js?ver=1 HTTP/1.1
1250 1.971121 59.67.152.250 220.194.79.33 HTTP 381 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	Data
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)
1882	1.894747	59.67.152.250	8.8.8.8	DNS	73	Standard query 0xb5be A qu1.f.368.cn
1883	1.894747	59.67.152.250	8.8.8.8	DNS	73	Standard query 0x9467 AAAA qu1.f.368.cn
1884	1.895704	59.67.152.250	8.8.8.8	DNS	77	Standard query 0x4f9c A www.enorth.com.cn
1885	1.895704	59.67.152.250	8.8.8.8	DNS	77	Standard query 0xc2c9 AAAA www.enorth.com.cn
1886	1.896380	8.8.8.8	59.67.152.250	HTTP	133	Standard query response 0xb5be A qu1.f.368.cn CNAME qu1.qh-lb.com A 111.200.62.164 A 111.200.62.169
1887	1.897595	8.8.8.8	59.67.152.250	DNS	201	Standard query response 0x4f9c A www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd...
1888	1.899468	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...
1890	1.911846	8.8.8.8	59.67.152.250	DNS	181	Standard query response 0x9467 AAAA qu1.f.368.cn CNAME qu1.qh-lb.com
1894	1.911836	59.67.152.250	228.194.79.33	HTTP	583	GET / HTTP/1.1
1134	1.920810	228.194.79.33	59.67.152.250	HTTP	221	HTTP/1.1 200 OK (text/html)
1135	1.920810	59.67.152.250	111.200.62.164	HTTP	772	POST /winfo.php HTTP/1.1 (application/octet-stream)
1168	1.929337	59.67.152.250	228.194.79.33	HTTP	389	GET /js/share/jquery-1.18.2.min.js HTTP/1.1
1174	1.934893	59.67.152.250	228.194.79.33	HTTP	390	GET /css/ggIndex.css HTTP/1.1
1178	1.937266	228.194.79.33	59.67.152.250	HTTP	388	HTTP/1.1 200 OK (text/html)
1212	1.943181	228.194.79.33	59.67.152.250	HTTP	1188	HTTP/1.1 200 OK (application/javascript)
1225	1.971121	59.67.152.250	228.194.79.33	HTTP	383	GET /js/online_calc.js?ver=1 HTTP/1.1
1226	1.971121	228.194.79.33	59.67.152.250	HTTP	384	GET /js/online_calc.js?ver=1 HTTP/1.1

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	Data
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)
1882	1.894747	59.67.152.250	8.8.8.8	DNS	73	Standard query 0xb5be A qu1.f.368.cn
1883	1.894747	59.67.152.250	8.8.8.8	DNS	73	Standard query 0x9467 AAAA qu1.f.368.cn
1884	1.895704	59.67.152.250	8.8.8.8	DNS	77	Standard query 0x4f9c A www.enorth.com.cn
1885	1.895704	59.67.152.250	8.8.8.8	DNS	77	Standard query 0xc2c9 AAAA www.enorth.com.cn
1886	1.896380	8.8.8.8	59.67.152.250	HTTP	133	Standard query response 0xb5be A qu1.f.368.cn CNAME qu1.qh-lb.com A 111.200.62.164 A 111.200.62.169
1887	1.897595	8.8.8.8	59.67.152.250	DNS	201	Standard query response 0x4f9c A www.enorth.com.cn CNAME www.enorth.com.cn.cdn.dnsv1.com CNAME 287911.s2.cd...
1888	1.899468	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...
1890	1.911846	8.8.8.8	59.67.152.250	DNS	181	Standard query response 0x9467 AAAA qu1.f.368.cn CNAME qu1.qh-lb.com
1894	1.911836	59.67.152.250	228.194.79.33	HTTP	583	GET / HTTP/1.1
1134	1.920810	228.194.79.33	59.67.152.250	HTTP	221	HTTP/1.1 200 OK (text/html)
1135	1.920810	59.67.152.250	111.200.62.164	HTTP	772	POST /winfo.php HTTP/1.1 (application/octet-stream)
1168	1.929337	59.67.152.250	228.194.79.33	HTTP	389	GET /js/share/jquery-1.18.2.min.js HTTP/1.1
1174	1.934893	59.67.152.250	228.194.79.33	HTTP	390	GET /css/ggIndex.css HTTP/1.1
1178	1.937266	228.194.79.33	59.67.152.250	HTTP	388	HTTP/1.1 200 OK (text/html)
1212	1.943181	228.194.79.33	59.67.152.250	HTTP	1188	HTTP/1.1 200 OK (application/javascript)
1225	1.971121	59.67.152.250	228.194.79.33	HTTP	383	GET /js/online_calc.js?ver=1 HTTP/1.1
1226	1.971121	228.194.79.33	59.67.152.250	HTTP	384	GET /js/online_calc.js?ver=1 HTTP/1.1

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	60	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: 0.003.489	
217		[202.113.78.123]	www.bupt.edu.cn	ICMP: Echo	1066	0:00:0: 0.396.605	
218		www.bupt.edu.cn	[202.113.78.123]	ICMP: Echo reply	1066	0:00:1 0.003.429	

请根据图中信息回答下列问题。

- (1) 该主机上执行的命令完整内容是 ① 。
- (2) 主机59.67.148.5的功能是 ② ，其提供服务的缺省端口是 ③ 。
- (3) 图中①处删除了部分显示信息，该信息应该是 ④ 。
- (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: 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	60	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 E? 跟 .1.abcdef
00000030 57 60 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghi;jklmnopqrstuvwxyz
00000040 77 65 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdeghijklmno
00000050 70 61 62 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrsuvwxyzabcdgfh
00000060 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnopqrstuvwxyz

\Expert \Decode \Matrix \Host Table \Protocol Dist. \Statistics \Filtered 10

请根据图中信息回答下列问题。

- (1) 该主机上执行的命令完整内容是 ① 。
- (2) 主机59.67.148.5的功能是 ② DNS 其提供服务的缺省端口是 ③ 。
- (3) 图中①处删除了部分显示信息，该信息应该是 ④ 。
- (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sniffer捕获的数据包。

The screenshot shows a list of network frames captured by Sniffer Portable. Frame 14 is highlighted, showing an FTP control connection from JACKSON to the server. The details pane shows the following information for frame 14:

IP	... 0 ...	last fragment
IP:	Fragment offset	= 0 bytes
IP:	Time to live	= 128 seconds/hop
IP:	Protocol	= 6 (TCP)
IP:	Header checksum	* C6DB (correct)
IP:	Source address	= [202.113.78.113]: JACKSON
IP:	Destination address	* [211.69.71.80]. @
IP:	No options	
TCP Header		
TCP:	Source port	= 1039
TCP:	Destination port	= 21 (FTP-ctrl)
TCP:	Sequence number	= 577568801
TCP:	Next expected Seq number	= 577568802
TCP:	Acknowledgment number	= 2951764892
TCP:	Data offset	= 20 bytes

The hex dump pane shows the raw data of the captured frame.

请根据图中信息回答下列问题。

(1) 该URL是 ①

577568801-1

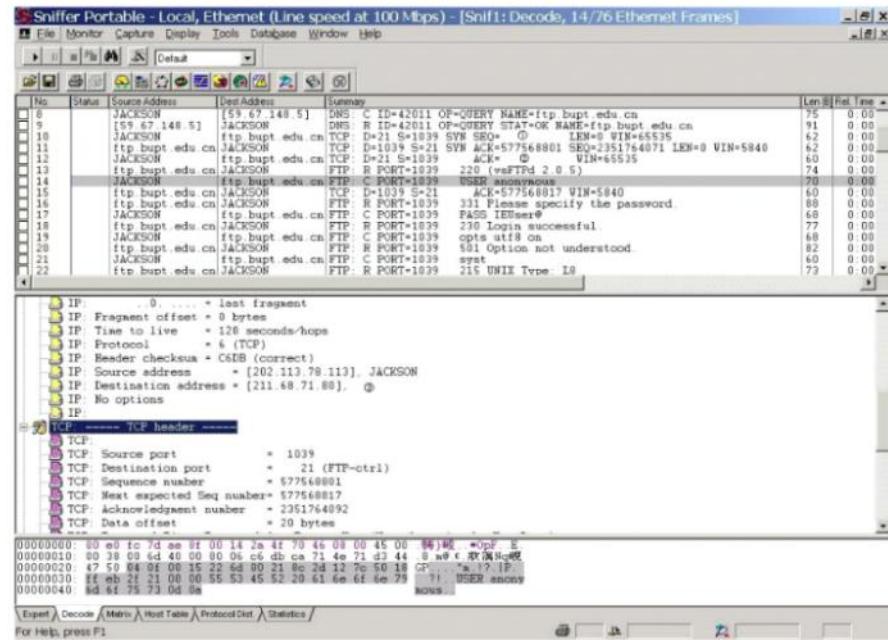
(2) 该主机的IP地址是 ②

(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。

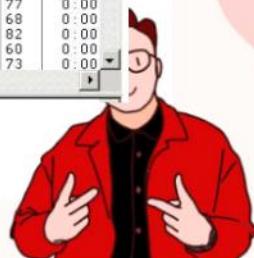
- (1) 该URL是 ①
- (2) 该主机的IP地址是 ②
- (3) 图中的①②③删除了部分显示信息，其中①应该是 ③，②应该是 ④
- (4) 该主机配置的DNS服务器的IP地址是 ⑤



TCP得分点

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

No.	Status	Source Address	Dest Address	Summary	Len [B]	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	JACKSON		ftp.bupt.edu.cn	TCP: D=21 S=1039 SYN SEQ= ① 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= ② LEN=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.	68	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。

The screenshot shows a network traffic capture window. The list pane shows several frames, with frame 23 selected. The details pane shows the TCP header for frame 23:

TCP	Source port	= 2263
TCP	Destination port	= 21 (FTP-ctrl)
TCP	Initial sequence number	= 3176842225
TCP	Next expected Seq number	= 3176842226
TCP	Data offset	= 20 bytes (4 bits)
TCP	Reserved Bits: Reserved for Future Use (6 bits)	= 02
TCP	Flags	= 02
TCP	0	= (Congestion Window Reduced (CWR) NOT set)
TCP	n	= (ECN Eahn NOT Set)

The raw data pane shows the hex and ASCII representation of the captured frame.

请根据图中信息回答下列问题。

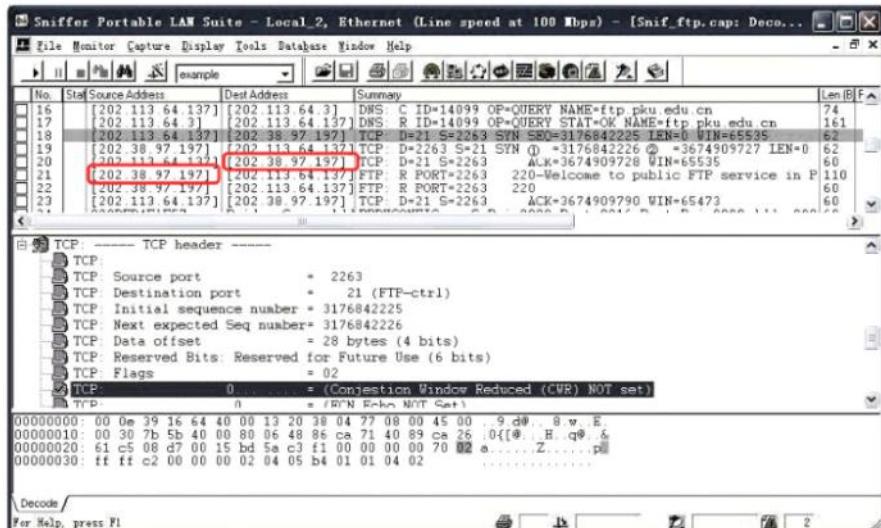
(1) 该主机上配置的域名服务器的IP地址是 ① 。

(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。

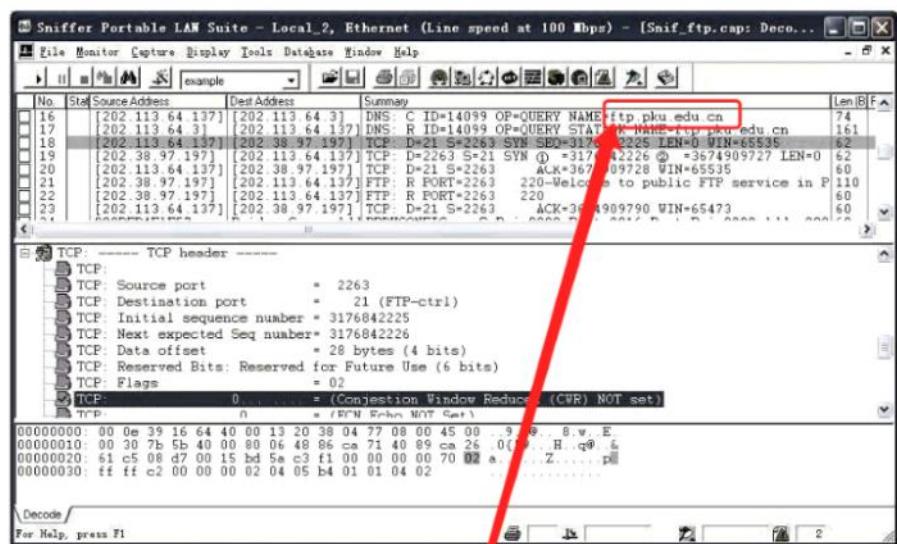
(1) 该主机上配置的域名服务器的IP地址是 ① 。

(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 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 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



No.	Src	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	0:00:04.278
				ICMP: Echo		
10	#	[202.113.64.129]	[202.113.64.137]	Expert: Time-to-live_exceeded_in_transmit ICMP: Time_exceeded (Time to live exceeded in transi	70	0:00:04.278
11	#	[202.113.64.137]	mail.tj.edu.cn	Expert: Time-to-live_expiring	106	0:00:04.278
12	#	[202.113.64.129]	[202.113.64.137]	Expert: Time-to-live_exceeded_in_transmit ICMP: Time_exceeded (Time to live exceeded in transi	70	0:00:04.278
13	#	[202.113.64.137]	mail.tj.edu.cn	Expert: Time-to-live_expiring	106	0:00:04.278
14	#	[202.113.64.129]	[202.113.64.137]	Expert: Time-to-live_exceeded_in_transmit ICMP: Time_exceeded (Time to live exceeded in transi	70	0:00:04.278
15		[202.113.64.137]	[202.113.64.3]	DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addi	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 ICMP: Time_exceeded (Time to live exceeded in transi	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_transmit	70	0:00:05.269

```
ICMP: Identification = 4413
ICMP: Flags = 0x0
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 = BS48 (correct)
ICMP: Source address = [③]
ICMP: Destination address = [211.81.20.208].④
ICMP: No options
ICMP:
```

Decode

分区 综合题解题技巧 的第 16 页

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。

No.	Src 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	0:00:04.276
14	# [202.113.64.129]	[202.113.64.137]	ICMP: Echo	70	0:00:04.276
15	[202.113.64.137]	[202.113.64.3]	Expert: Time-to-live exceeded in transit	87	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	149	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	106	0:00:05.266
18	# [202.113.77.253]	[202.113.64.137]	Expert: 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	0:00:05.266

Decoded /

ICMP: Identification = 4413
ICMP: Flags = OK
ICMP: may fragment
ICMP: last fragment
ICMP: Fragment offset = 0 bytes
ICMP: Time to live = 1 seconds/hops
ICMP: Protocol = 1 (<2>)
ICMP: Header checksum = B548 (correct)
ICMP: Source address = [③]
ICMP: Destination address = [211.81.20.208]. ④
ICMP: No options
ICMP:

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 。 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	Src/Mac Address	Dst/Mac 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 transmit	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 transmit	106	0:00:04.276
14	# [202.113.64.129]	[202.113.64.137]	ICMP: Echo	70	0:00:04.276
15	[202.113.64.137]	[202.113.64.3]	ICMP: Time exceeded (Time to live exceeded in transmit)	87	0:00:04.290
16	[202.113.64.3]	[202.113.64.137]	DNS C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr.a	149	0:00:04.291
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.a	106	0:00:05.268
18	# [202.113.77.253]	[202.113.64.137]	ICMP: Echo	70	0:00:05.268
19	[202.113.64.137]	mail.tj.edu.cn	ICMP: Time exceeded (Time to live exceeded in transmit)	106	0:00:05.268
20	# [202.113.77.253]	[202.113.64.137]	ICMP: Time exceeded (Time to live exceeded in transmit)	70	0:00:05.268

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 ICMP ④ 。
- (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	Stat	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	0:00:04.274
10	#	[202.113.64.129]	[202.113.64.137]	ICMP: Echo	70	0:00:04.275
11	#	[202.113.64.137]	mail.tj.edu.cn	Expert: Time-to-live exceeded in transmit	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 transmit	106	0:00:04.276
14	#	[202.113.64.129]	[202.113.64.137]	ICMP: Echo	70	0:00:04.276
15		[202.113.64.137]	[202.113.64.3]	DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr.a	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 transmit	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 transmit	70	0:00:05.266

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	Stat	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	0:00:04.274
10	#	[202.113.64.129]	[202.113.64.137]	ICMP: Echo	70	0:00:04.275
11	#	[202.113.64.137]	mail.tj.edu.cn	Expert: Time-to-live exceeded in transmit	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 transmit	106	0:00:04.276
14	#	[202.113.64.129]	[202.113.64.137]	ICMP: Echo	70	0:00:04.276
15		[202.113.64.137]	[202.113.64.3]	DNS: C ID=33660 OP=QUERY NAME=129.64.113.202.in-addr.a	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 transmit	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 transmit	70	0:00:05.266

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。

No.	Size	Source Address	Dest Address	Summary	Len (B)	Pkt Time
1	#	[202.113.64.129]	[202.113.64.129]	ICMP: C IP=236460 OP=QUERY NAME=mail.tj.edu.cn	116	0:00:04.247
2	#	[202.113.64.129]	[202.113.64.129]	ICMP: R IP=236460 OP=QUERY STAT=OK NAME=mail.tj.edu.cn	116	0:00:04.275
3	#	[202.113.64.129]	[202.113.64.129]	ICMP: C IP=47220 OP=QUERY NAME=mail.tj.edu.cn	74	0:00:04.275
4	#	[202.113.64.129]	[202.113.64.129]	ICMP: R IP=47220 OP=QUERY STAT=OK NAME=mail.tj.edu.cn	74	0:00:04.275
5	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded	106	0:00:04.276
6	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	70	0:00:04.276
7	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	106	0:00:04.276
8	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	70	0:00:04.276
9	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	106	0:00:04.276
10	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	70	0:00:04.276
11	#	[202.113.64.129]	[mail.tj.edu.cn]	ICMP: Eseqpt Time-to-live exceeded	106	0:00:04.276
12	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	70	0:00:04.276
13	#	[202.113.64.129]	[mail.tj.edu.cn]	ICMP: Eseqpt Time-to-live exceeded	106	0:00:04.276
14	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	70	0:00:04.276
15	#	[202.113.64.129]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	87	0:00:04.280
16	#	[202.113.64.129]	[202.113.64.129]	ICMP: C IP=336460 OP=QUERY NAME=129.64.113.202.in-addr.a	149	0:00:04.280
17	#	[202.113.64.129]	[202.113.64.129]	ICMP: R IP=336460 OP=QUERY STAT=Name error NAME=129.64.113.202	106	0:00:05.264
18	#	[202.113.77.203]	[202.113.64.129]	ICMP: Echo	79	0:00:05.264
19	#	[202.113.77.203]	[202.113.64.129]	ICMP: Echo	136	0:00:05.264
20	#	[202.113.77.203]	[202.113.64.129]	ICMP: Eseqpt Time-to-live exceeded in transmit	136	0:00:05.264

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 _____。

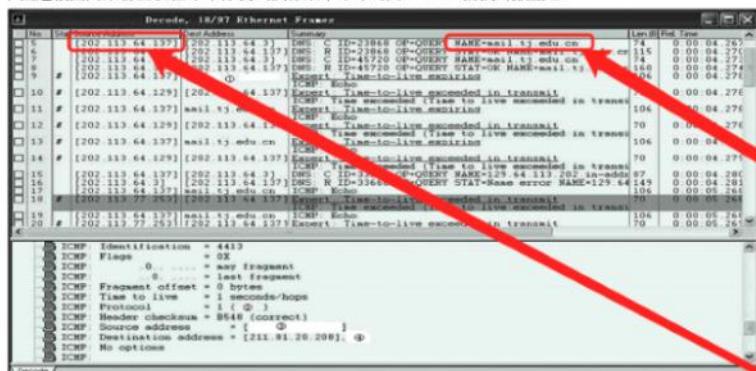
(2) 图中的①~④删除了部分显示信息，其中①处应该是 ② _____。

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_____。④处应该是 ④_____。

(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。

No.	Status	Source Address	DestAddress	Summary	Len[Byt]	Rel
31		[202 113 64 168 www.tjut.edu.cn	TCP D=80 S=1049 ACK=2656713554 WIN=6544 60			
32		[202 113 64 168 www.tjut.edu.cn	DNS C 10456287 OP=QUERY NAME=64.113.262.148			
33		dns.tjut.edu.cn [202 113 64 168 www.tjut.edu.cn	DNS R 10456287 OP=QUERY NAME=64.113.262.148			
34		000EED4EA5F7	Bridge_Group_Ad	BPDUCONFIG: S-Pri=8000 Port=8016 Root:Port=60		
35		000E39166440	Broadcast	ARP C PA=[202 113 64 159] PRO=IP	60	
36		000E39166440	Broadcast	ARP C PA=[202 113 64 159] PRO=IP	60	
37		[202 113 64 168 www.tjut.edu.cn	HTTP C Port=1049 GET /index.jsp HTTP/1.1 461			
38		① www.tjut.edu.cn [202 113 64 168	HTTP R Port=1049 HTTP/1.1 Status=OK 1514			
39		www.tjut.edu.cn [202 113 64 168 www.tjut.edu.cn	HTTP Continuation of frame 38 (1/2) 1460 B 1514			
40		[202 113 64 168 www.tjut.edu.cn	TCP D=80 S=1049 ③ -2656716474 WIN=6552 60			

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。

No.	Status	Source Address	DestAddress	Summary	Len[Byt]	Rel
31		[202 113 64 168 www.tjut.edu.cn	TCP D=80 S=1049 ACK=2656713554 WIN=6544 60			
32		[202 113 64 168 www.tjut.edu.cn	DNS C 10456287 OP=QUERY NAME=64.113.262.148			
33		dns.tjut.edu.cn [202 113 64 168 www.tjut.edu.cn	DNS R 10456287 OP=QUERY NAME=64.113.262.148			
34		000EED4EA5F7	Bridge_Group_Ad	BPDUCONFIG: S-Pri=8000 Port=8016 Root:Port=60		
35		000E39166440	Broadcast	ARP C PA=[202 113 64 159] PRO=IP	60	
36		000E39166440	Broadcast	ARP C PA=[202 113 64 159] PRO=IP	60	
37		[202 113 64 168 www.tjut.edu.cn	HTTP C Port=1049 GET /index.jsp HTTP/1.1 461			
38		① www.tjut.edu.cn [202 113 64 168	HTTP R Port=1049 HTTP/1.1 Status=OK 1514			
39		www.tjut.edu.cn [202 113 64 168 www.tjut.edu.cn	HTTP Continuation of frame 38 (1/2) 1460 B 1514			
40		[202 113 64 168 www.tjut.edu.cn	TCP D=80 S=1049 ③ -2656716474 WIN=6552 60			

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