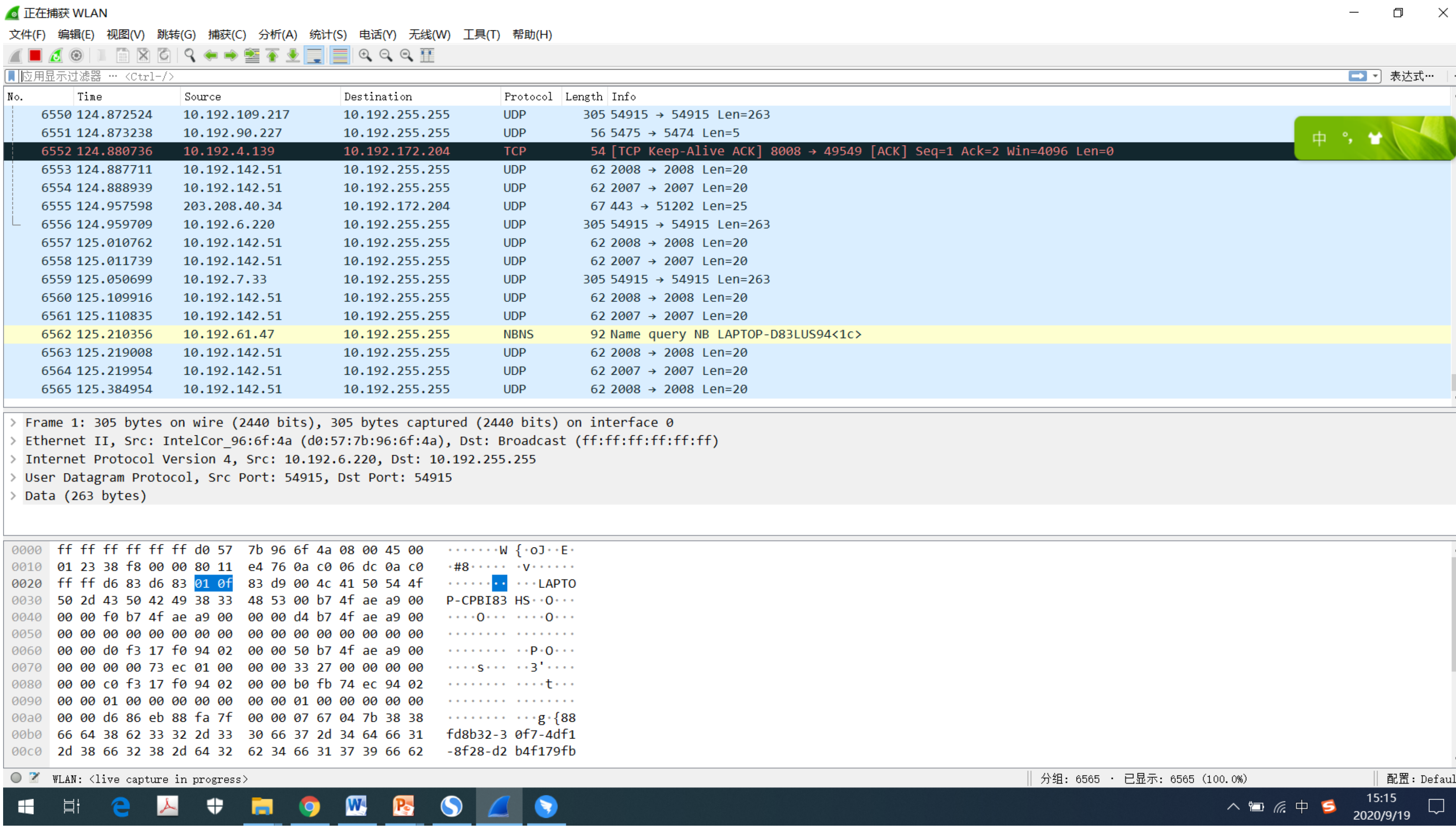
Wireshark

Dr. Xiqun Lu
College of Computer Science and Technology, Zhejiang University, Hangzhou

WireShark

- https://www.wireshark.org/
- The new version Wireshark 3.4.8 (Aug. 25, 2021)
- Extension include: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, Icap, mplog, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.

Interface of Wireshark

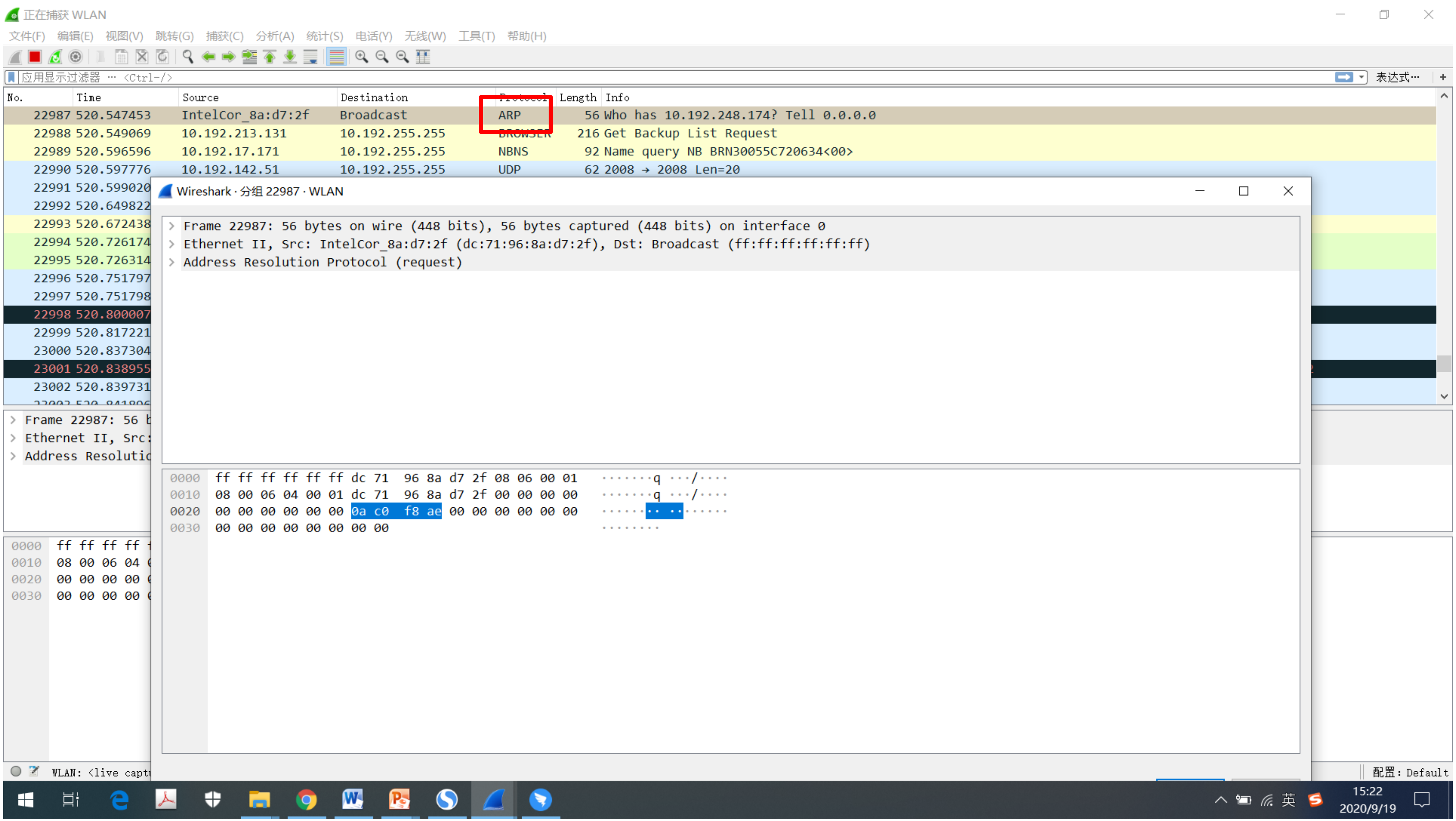


- Wireshark三个面板：“Packet List”面板（分组列表），“Packet Detail”(分组详情)，“Packet Byte”(分组包字节流)

Interface of Wireshark

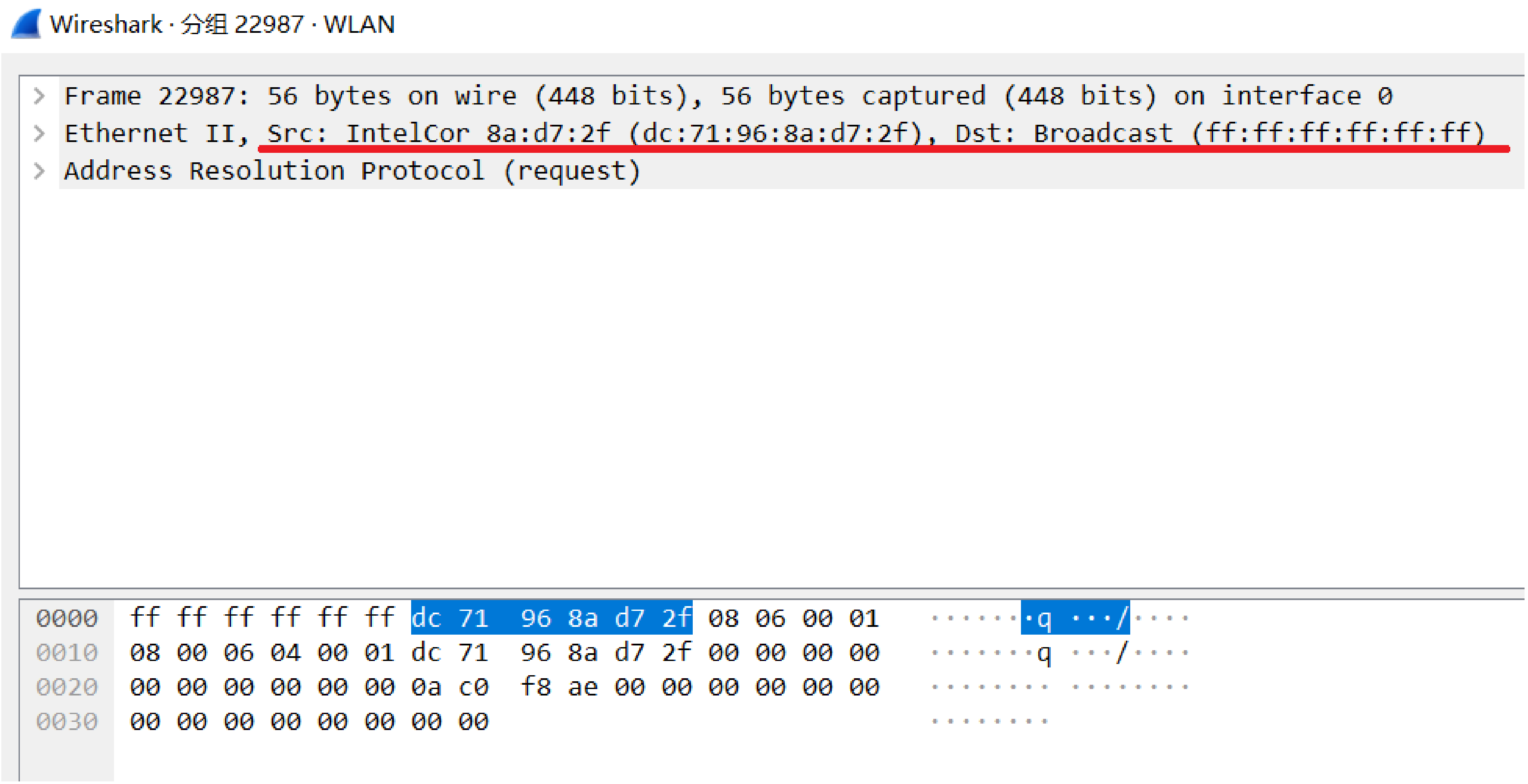
- Wireshark三个面板：“Packet List”面板（分组列表），“Packet Detail”(分组详情)，“Packet Byte”(分组包字节流)
- 列表中的每行显示捕捉文件的一个包。如果您选择其中一行，该包的更多情况会显示在"Packet Detail/分组详情"，"Packet Byte/分组字节流"面板。在分析(解剖)分组时，Wireshark会将协议信息放到各个列。因为高层协议通常会覆盖底层协议，您通常在包列表面板看到的都是每个包的最高层协议描述。（在这里高层是应用层，底层是数据链路层）

Example I: ARP



ARP: Address Resolution Protocol [2]

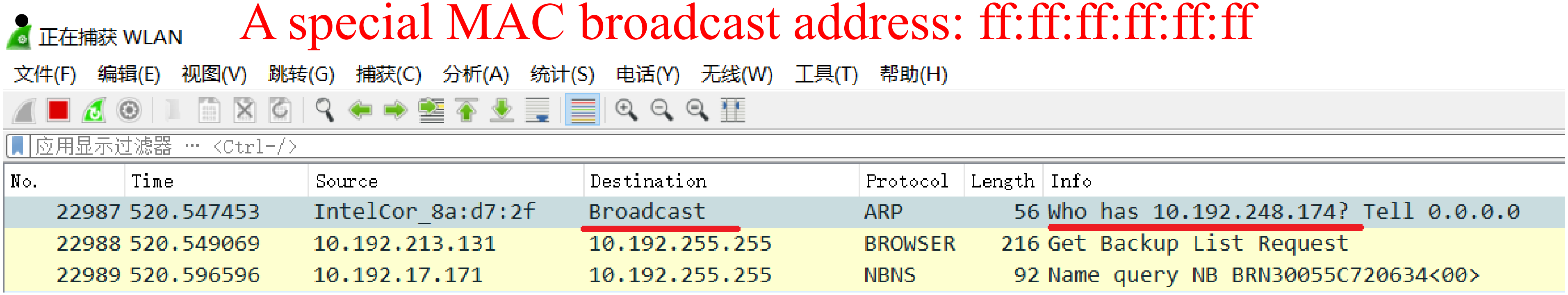
- Because there are both *network-layer addresses* (for example, Internet **IP addresses**) and *link-layer addresses* (that is, **MAC addresses**), there is a need to translate between them. For the Internet, this is the job of the **Address Resolution Protocol** (**ARP**) [RFC826]



ARP: Address Resolution Protocol [2]

- The purpose of the ARP query packet is to query all the other nodes on the subnet to determine the MAC address corresponding to the IP address that is being resolved.
- An ARP query packet (In this example: it give the IP address: 10.192.248.174, want to know the MAC address of the IP address. A IPv4 address has 32 bits and expressed in decimals (十进制) ×××.×××.×××.×××)
- The MAC addresses are 6 bytes long, giving 2^{48} possible MAC addresses, and are expressed in hexadecimal (十六进制). (In this example: the MAC address of the source is dc:71:96:8a:d7:2f)

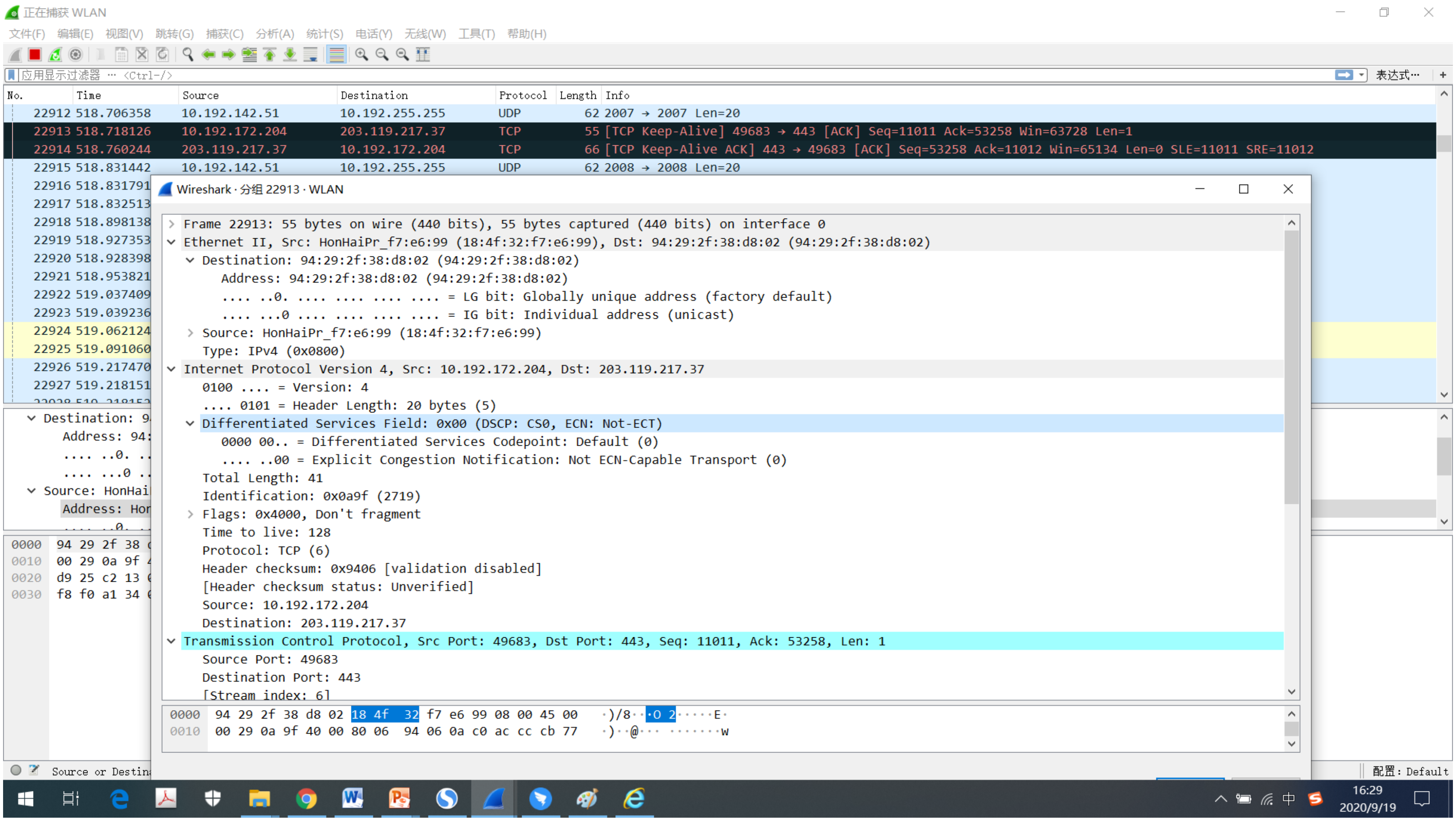
A special MAC broadcast address: ff:ff:ff:ff:ff:ff



ARP: Address Resolution Protocol [2]

- Each node (host and router) has **an ARP table** in its memory, which contains mappings of IP addresses to MAC addresses.
- The ARP table contains a time-to-live (**TTL**) value, which indicates when each mapping will be deleted from the table.
  - A typical expiration time for an entry is 20 minutes from when an entry is placed in an ARP table.
- ARP vs. DNS
  - ARP resolves an IP address to a MAC address only for nodes on the same subnet.
  - DNS resolves host names to IP addresses for hosts anywhere in the Internet.
- ARP is probably best considered a protocol that straddles the boundary between the link and network layers.

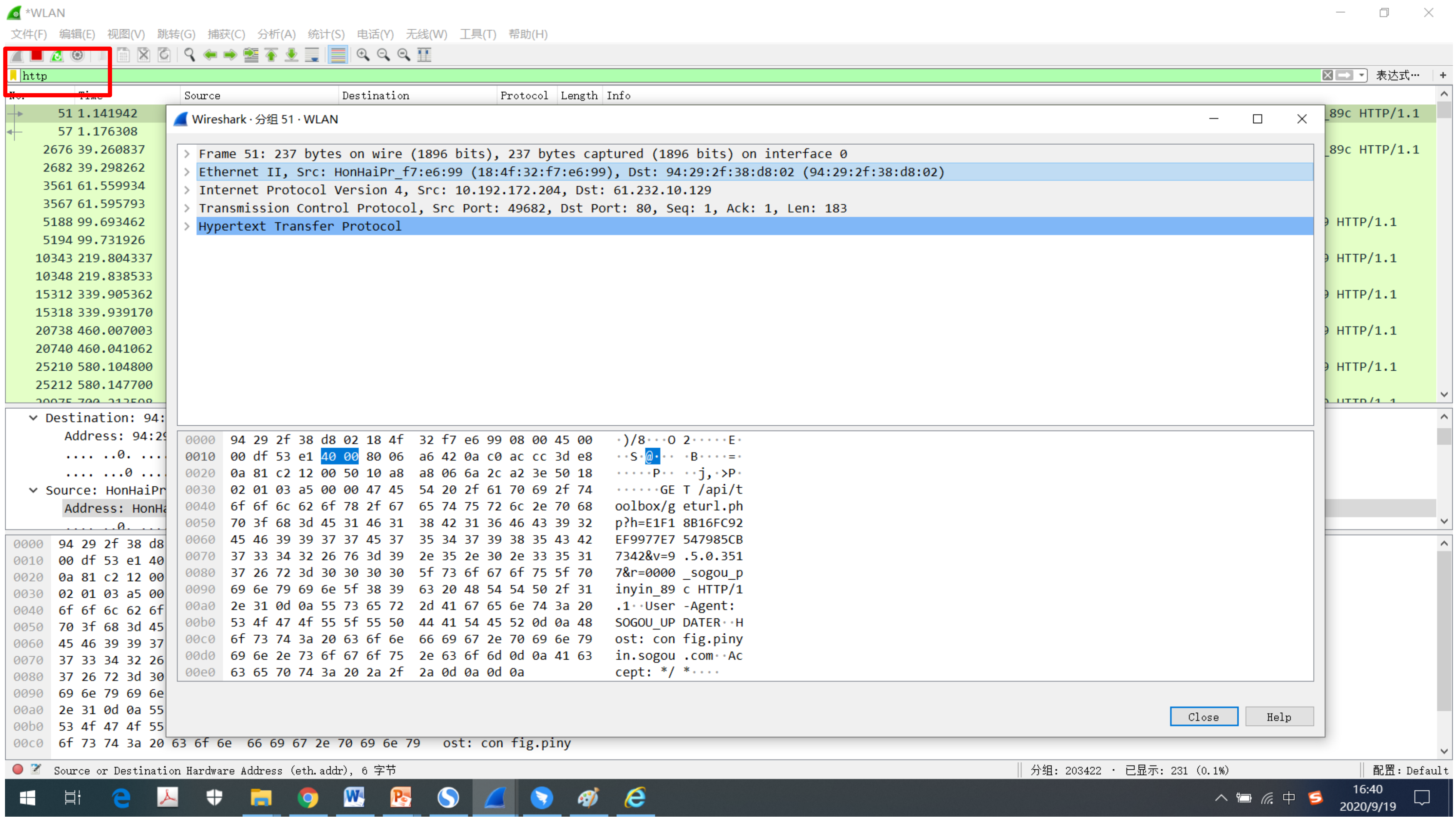
Example II: TCP



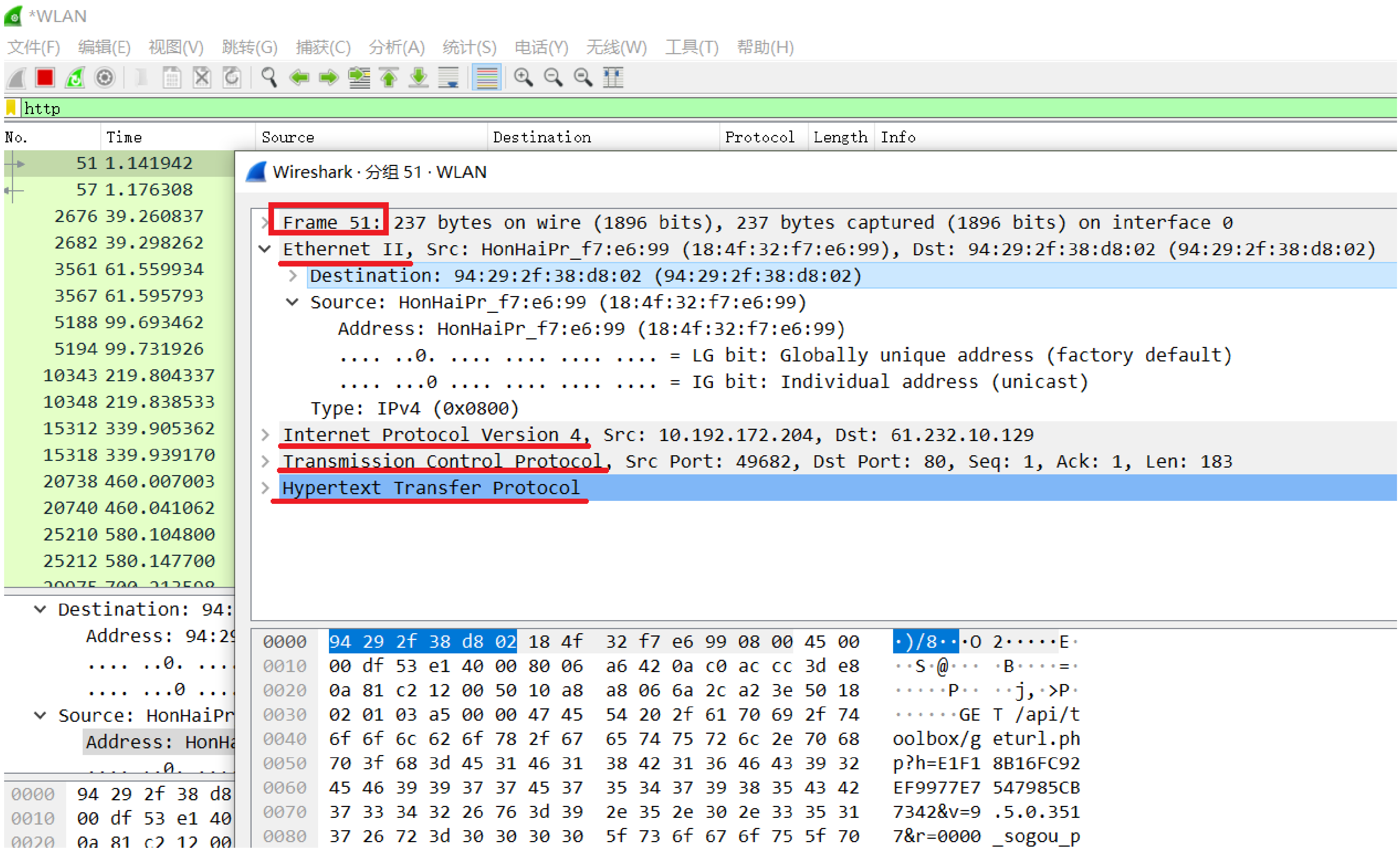
Example II: TCP

```
1442    10.192.142.51    10.192.255.255    UDP    62 2008 → 2008 Len=20

Wireshark · 分组 22913 · WLAN

> Frame 22913: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
v Ethernet II, Src: HonHaiPr_f7:e6:99 (18:4f:32:f7:e6:99), Dst: 94:29:2f:38:d8:02 (94:29:2f:38:d8:02)
  v Destination: 94:29:2f:38:d8:02 (94:29:2f:38:d8:02)
      Address: 94:29:2f:38:d8:02 (94:29:2f:38:d8:02)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: HonHaiPr_f7:e6:99 (18:4f:32:f7:e6:99)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.192.172.204, Dst: 203.119.217.37
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 41
    Identification: 0x0a9f (2719)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x9406 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.192.172.204
    Destination: 203.119.217.37
v Transmission Control Protocol, Src Port: 49683, Dst Port: 443, Seq: 11011, Ack: 53258, Len: 1
    Source Port: 49683
    Destination Port: 443
    [Stream index: 6]

0000   94 29 2f 38 d8 02 18 4f  32 f7 e6 99 08 00 45 00   ·)/8··O 2·····E·
```

Example III: HTTP



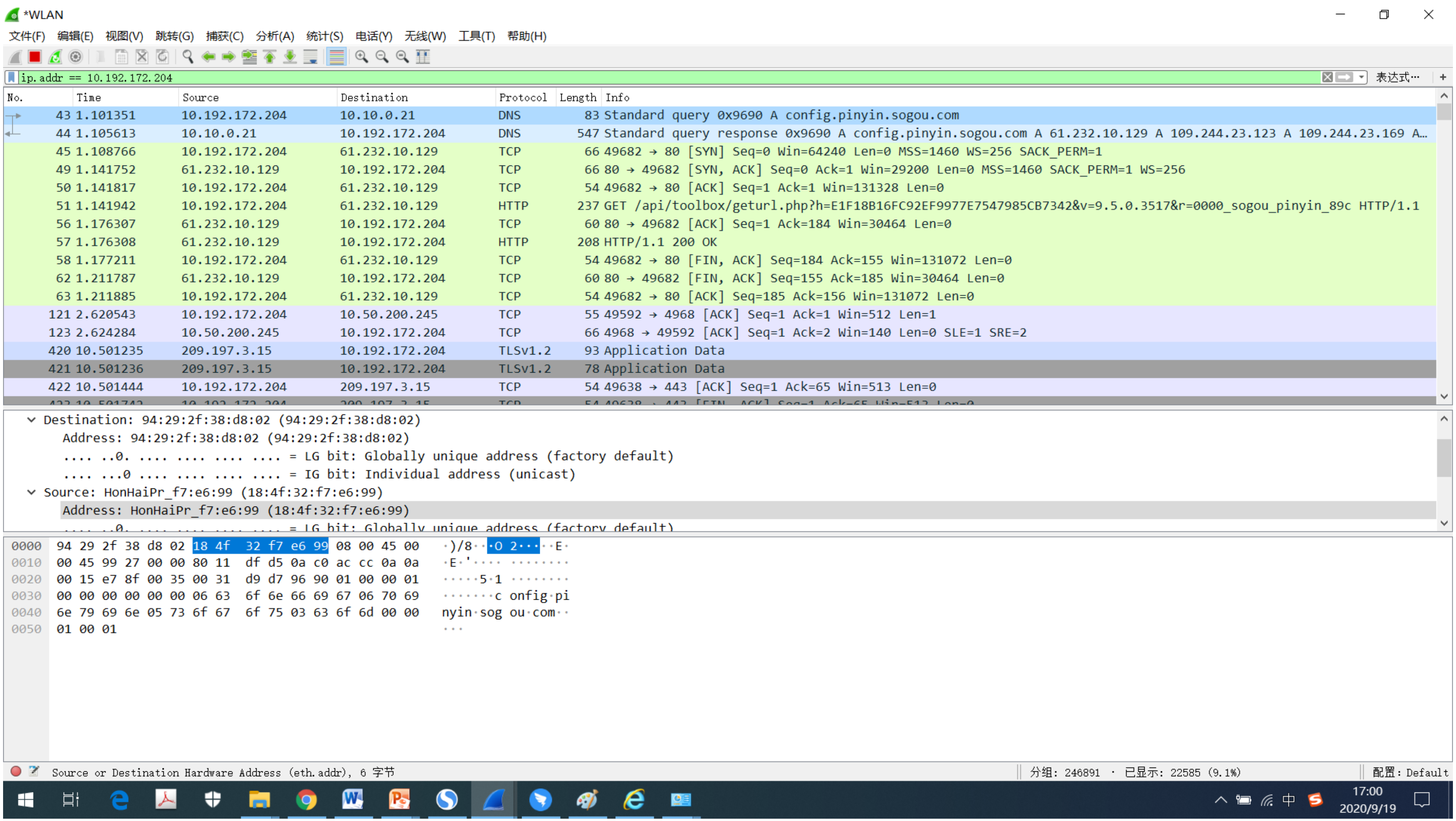
Example III: HTTP



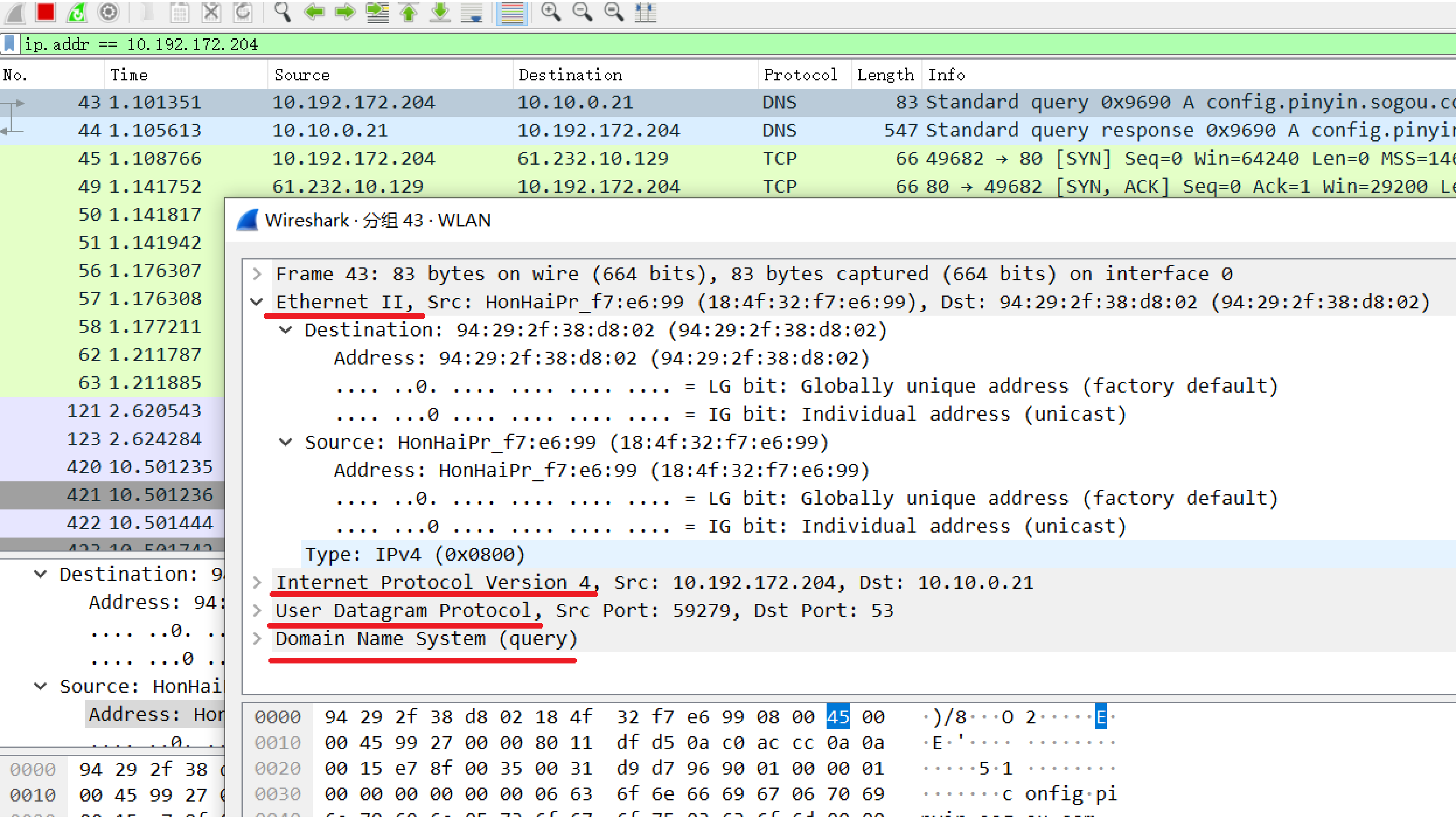
Example IV: ip.addr == 10.192.172.204

- 先在“控制面板”中打开网络中心，然后详细信息里有你电脑当前所使用的IP地址，你也可以看一下你电脑的物理地址（MAC地址）

Example IV: ip.addr == 10.192.172.204



Example V: DNS



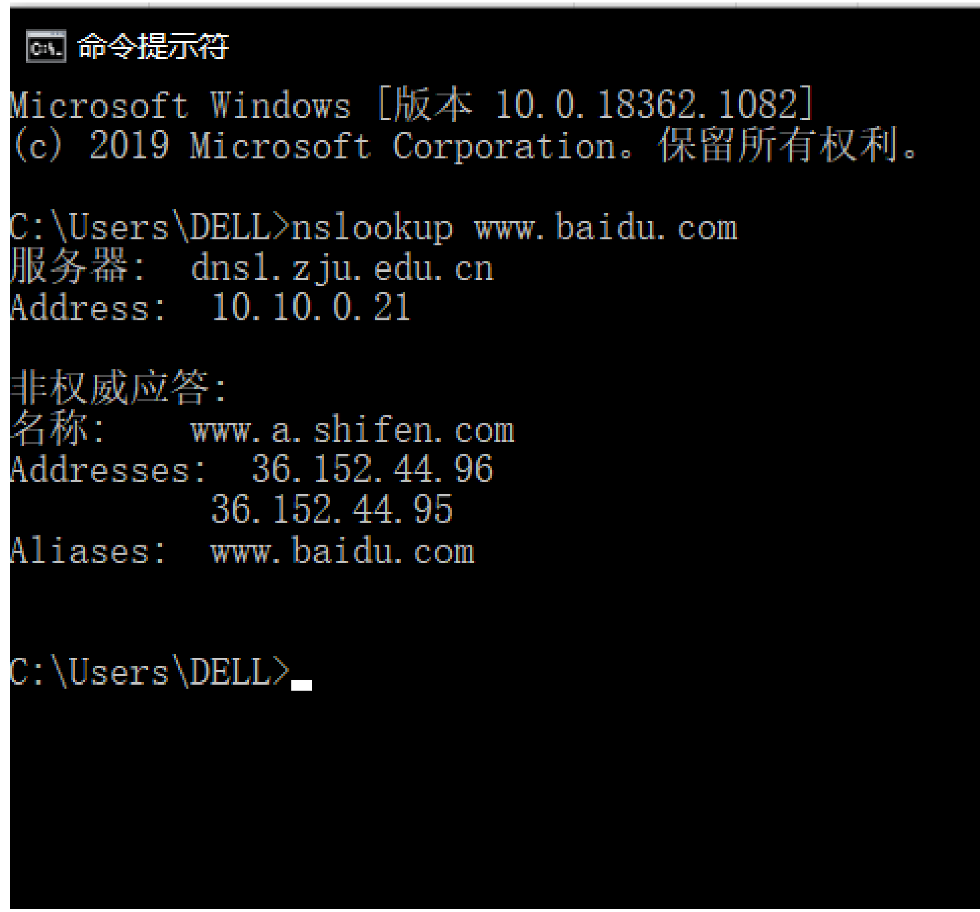
注意：在DNS数据包中传输层用的协议是UDP，不是TCP协议！Port number: 53

ip.addr == x.x.x.x vs. host.addr = x.x.x.x

- 实验中第4部分和第5部分相比，区别在于ip.addr == x.x.x.x是捕获所有数据包，但是只显示与ip地址为x.x.x.x有关的数据包，而host.addr = x.x.x.x只捕获ip地址为x.x.x.x的数据包。检查一下实验结果， host.addr = x.x.x.x命令下抓获数据包量要小很多。

nslookup

- 技巧：先退出Wireshark，然后重新打开，再运行“nslookup www.baidu.com”在命令行。



nslookup [4]

- 正向解析：通过域名查找ip；反向解析：通过ip查找域名；
- IP反向解析主要应用到邮件服务器中来阻拦垃圾邮件，特别是在国外。多数垃圾邮件发送者使用动态分配或者没有注册域名的IP地址来发送垃圾邮件，以逃避追踪，使用了域名反向解析后，就可以大大降低垃圾邮件的数量。
  - 比如你用 xxx@name.com 这个邮箱给我的邮箱 123@163.com 发了一封信。163邮件服务器接到这封信会查看这封信的信头文件，这封信的信头文件会显示这封信是由哪个IP地址发出来的。然后根据这个IP地址进行反向解析，如果反向解析到这个IP所对应的域名是 name.com 那么就接受这封邮件，如果反向解析发现这个IP没有对应到name.com，那么就拒绝这封邮件。

nslookup [4]

- 由于在域名系统中，一个IP地址可以对应多个域名，因此从IP出发去找域名，理论上应该遍历整个域名树，但这在Internet上是不现实的。
- 为了完成逆向域名解析，系统提供一个特别域，该特别域称为逆向解析域in-addr.arpa。这样欲解析的IP地址就会被表达成一种像域名一样的可显示串形式，后缀以逆向解析域域名“in-addr.arpa”结尾。　例如一个IP地址：222.211.233.244，其逆向域名表达方式为：244.233.221.222.in-addr.arpa两种表达方式中IP地址部分顺序恰好相反。
  - 因为域名结构是自底向上(从子域到域)，而IP地址结构是自顶向下(从网络到主机)的

nslookup [4]

- 通过ping 命令，我们看到我们只能获取上面通过nslookup获取的众多IP地址的一个，而且这个IP地址并不固定，同样也无法得知我们是通过哪个DNS 服务器获取的域名解析信息。ping 与nslookup的区别详细到此已经一目了然。

nslookup [4]

命令提示符

```
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
名称:    www.google.com
Addresses:  2001::1f0d:4808
          0.0.0.0
          127.0.0.1


C:\Users\DELL>nslookup -qt=ptr 36.152.44.96
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

*** dns1.zju.edu.cn 找不到 96.44.152.36.in-addr.arpa.: Non-existent domain

C:\Users\DELL>nslookup -qt=mx www.zju.edu.cn
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

zju.edu.cn
        primary name server = dns1.zju.edu.cn
        responsible mail addr = root.zju.edu.cn
        serial  = 2016112807
        refresh = 10800 (3 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 30 (30 secs)

C:\Users\DELL>
```

ping

```
命令提示符
Microsoft Windows [版本 10.0.18362.1082]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\DELL>ping www.baidu.com

正在 Ping www.a.shifen.com [36.152.44.95] 具有 32 字节的数据:
来自 36.152.44.95 的回复: 字节=32 时间=10ms TTL=55
来自 36.152.44.95 的回复: 字节=32 时间=10ms TTL=55
来自 36.152.44.95 的回复: 字节=32 时间=10ms TTL=55
来自 36.152.44.95 的回复: 字节=32 时间=10ms TTL=55

36.152.44.95 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 10ms，最长 = 10ms，平均 = 10ms

C:\Users\DELL>ping www.163.com

正在 Ping z163ipv6.v.qdyd03.longclouds.com [112.13.207.3] 具有 32 字节的数据:
来自 112.13.207.3 的回复: 字节=32 时间=5ms TTL=55
来自 112.13.207.3 的回复: 字节=32 时间=5ms TTL=55
来自 112.13.207.3 的回复: 字节=32 时间=5ms TTL=55
来自 112.13.207.3 的回复: 字节=32 时间=6ms TTL=55

112.13.207.3 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 5ms，最长 = 6ms，平均 = 5ms

C:\Users\DELL>
```

References

- [1] https://www.wireshark.org/
- [2] J. F. Kurose and K.W. Ross, Computer Networking — A Top-down Approach, 5th Edition, Pearson Education Inc., 2010.
- [3] https://blog.csdn.net/gui951753/article/details/83070180 (这个博客中有解释多个站点对应一个IP地址的问题。)
- [4] https://www.cnblogs.com/machangwei-8/p/10353137.html