



网络攻防实践——网络流量分析

华中科技大学
网络空间安全学院
肖凌

lingx@hust.edu.cn



◆实验目的

- ◆ 了解掌握Wireshark网络流量分析的基本功能
- ◆ 了解掌握网络流量分析的基本方法和步骤

◆实验环境

- ◆ 操作系统: Windows
- ◆ 实验工具: Wireshark 3.0.3



◆实验内容：

本次实验要完成6个小的任务：

- ◆ 5个单项任务主要完成对Wireshark网络流量分析基本功能的学习和训练。
- ◆ 综合任务面对实际问题，分析产生问题的原因并解决之。

◆实验要求

- ◆ 在“学习通”中回答问题并提交实验过程截图
- ◆ 提交阅读、整理的资料

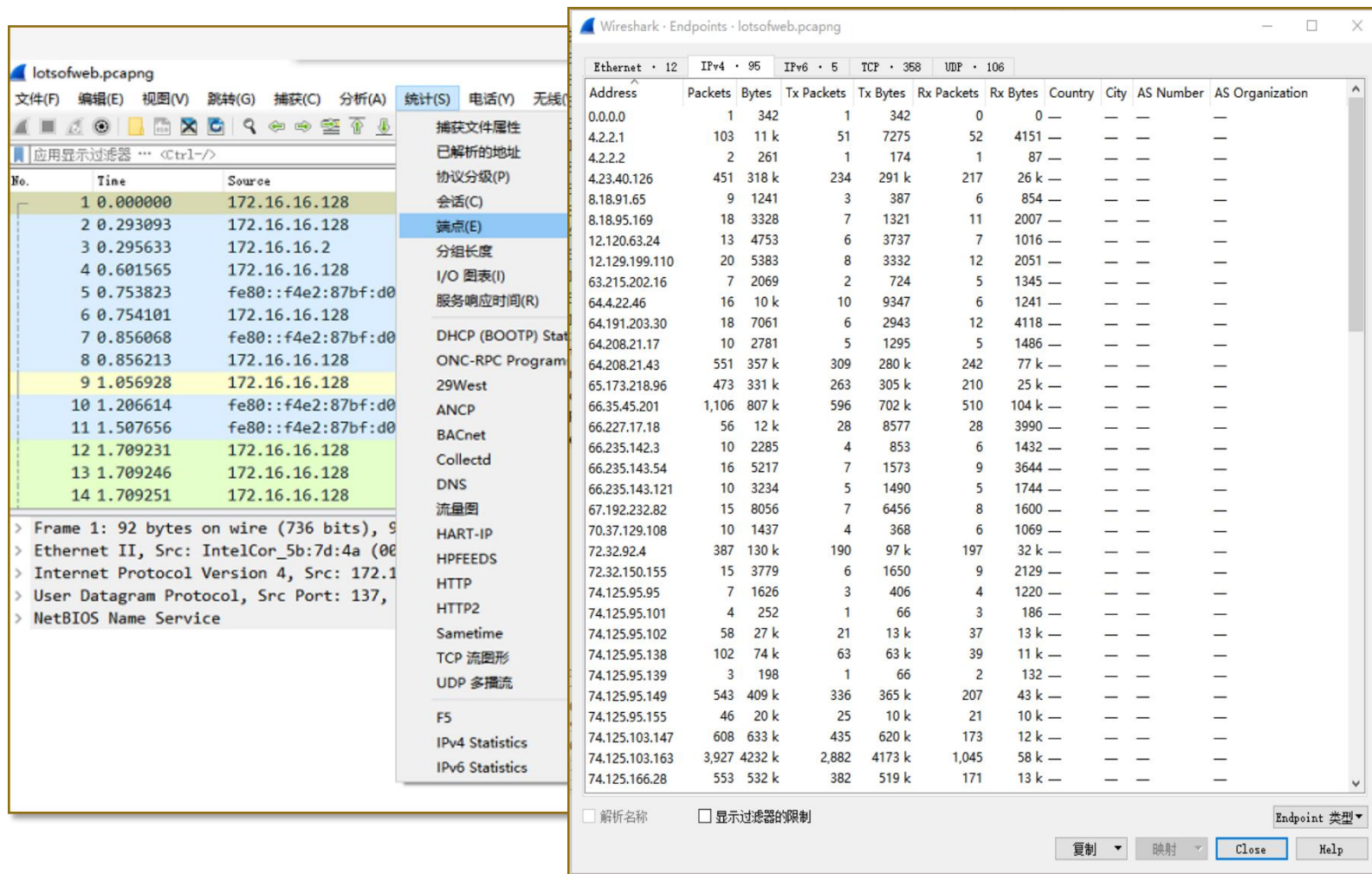


任务1 端点和会话统计分析

- 端点：网络中能够发送、接受数据的一台设备。
- 会话：网络中两个端点之间的数据交换。

分析网络流量时，当觉察到可以将问题定位到一个特定的端点上去，就可以使用**端点统计**功能

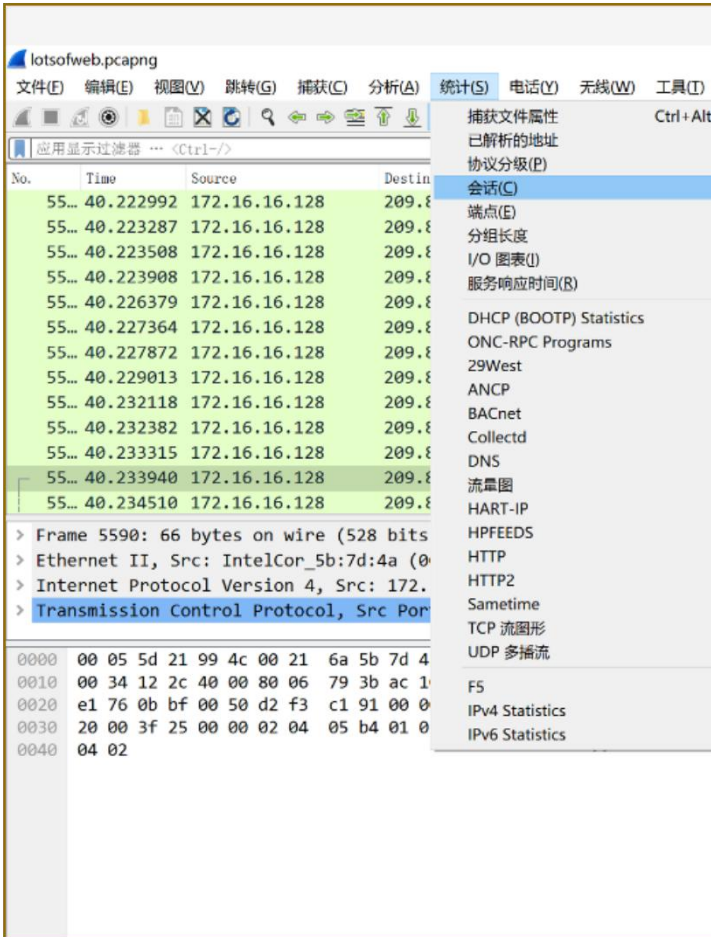
任务1 端点和会话统计分析



The image shows the Wireshark Endpoints window for the file 'lotsofweb.pcapng'. The window displays a table of endpoints with columns for Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, Rx Bytes, Country, City, AS Number, and AS Organization. The table is sorted by Address. The 'Endpoints' menu is open, showing options like '捕获文件属性', '已解析的地址', '协议分级(P)', '会话(C)', '端点(E)', '分组长度', 'I/O 图表(I)', '服务响应时间(R)', 'DHCP (BOOTP) Stat', 'ONC-RPC Program', '29West', 'ANCP', 'BACnet', 'Collectd', 'DNS', '流量图', 'HART-IP', 'HPFEEDS', 'HTTP', 'HTTP2', 'Sametime', 'TCP 流图形', 'UDP 多播流', 'F5', 'IPv4 Statistics', and 'IPv6 Statistics'. The '端点(E)' option is selected. The table shows data for various IP addresses, including 0.0.0.0, 4.2.2.1, 4.2.2.2, 4.23.40.126, 8.18.91.65, 8.18.95.169, 12.120.63.24, 12.129.199.110, 63.215.202.16, 64.4.22.46, 64.191.203.30, 64.208.21.17, 64.208.21.43, 65.173.218.96, 66.35.45.201, 66.227.17.18, 66.235.142.3, 66.235.143.54, 66.235.143.121, 67.192.232.82, 70.37.129.108, 72.32.92.4, 72.32.150.155, 74.125.95.95, 74.125.95.101, 74.125.95.102, 74.125.95.138, 74.125.95.139, 74.125.95.149, 74.125.95.155, 74.125.103.147, 74.125.103.163, and 74.125.166.28. The table also shows statistics for each endpoint, such as Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, Rx Bytes, Country, City, AS Number, and AS Organization.

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS Number | AS Organization |
|----------------|---------|--------|------------|----------|------------|----------|---------|------|-----------|-----------------|
| 0.0.0.0 | 1 | 342 | 1 | 342 | 0 | 0 | — | — | — | — |
| 4.2.2.1 | 103 | 11 k | 51 | 7275 | 52 | 4151 | — | — | — | — |
| 4.2.2.2 | 2 | 261 | 1 | 174 | 1 | 87 | — | — | — | — |
| 4.23.40.126 | 451 | 318 k | 234 | 291 k | 217 | 26 k | — | — | — | — |
| 8.18.91.65 | 9 | 1241 | 3 | 387 | 6 | 854 | — | — | — | — |
| 8.18.95.169 | 18 | 3328 | 7 | 1321 | 11 | 2007 | — | — | — | — |
| 12.120.63.24 | 13 | 4753 | 6 | 3737 | 7 | 1016 | — | — | — | — |
| 12.129.199.110 | 20 | 5383 | 8 | 3332 | 12 | 2051 | — | — | — | — |
| 63.215.202.16 | 7 | 2069 | 2 | 724 | 5 | 1345 | — | — | — | — |
| 64.4.22.46 | 16 | 10 k | 10 | 9347 | 6 | 1241 | — | — | — | — |
| 64.191.203.30 | 18 | 7061 | 6 | 2943 | 12 | 4118 | — | — | — | — |
| 64.208.21.17 | 10 | 2781 | 5 | 1295 | 5 | 1486 | — | — | — | — |
| 64.208.21.43 | 551 | 357 k | 309 | 280 k | 242 | 77 k | — | — | — | — |
| 65.173.218.96 | 473 | 331 k | 263 | 305 k | 210 | 25 k | — | — | — | — |
| 66.35.45.201 | 1,106 | 807 k | 596 | 702 k | 510 | 104 k | — | — | — | — |
| 66.227.17.18 | 56 | 12 k | 28 | 8577 | 28 | 3990 | — | — | — | — |
| 66.235.142.3 | 10 | 2285 | 4 | 853 | 6 | 1432 | — | — | — | — |
| 66.235.143.54 | 16 | 5217 | 7 | 1573 | 9 | 3644 | — | — | — | — |
| 66.235.143.121 | 10 | 3234 | 5 | 1490 | 5 | 1744 | — | — | — | — |
| 67.192.232.82 | 15 | 8056 | 7 | 6456 | 8 | 1600 | — | — | — | — |
| 70.37.129.108 | 10 | 1437 | 4 | 368 | 6 | 1069 | — | — | — | — |
| 72.32.92.4 | 387 | 130 k | 190 | 97 k | 197 | 32 k | — | — | — | — |
| 72.32.150.155 | 15 | 3779 | 6 | 1650 | 9 | 2129 | — | — | — | — |
| 74.125.95.95 | 7 | 1626 | 3 | 406 | 4 | 1220 | — | — | — | — |
| 74.125.95.101 | 4 | 252 | 1 | 66 | 3 | 186 | — | — | — | — |
| 74.125.95.102 | 58 | 27 k | 21 | 13 k | 37 | 13 k | — | — | — | — |
| 74.125.95.138 | 102 | 74 k | 63 | 63 k | 39 | 11 k | — | — | — | — |
| 74.125.95.139 | 3 | 198 | 1 | 66 | 2 | 132 | — | — | — | — |
| 74.125.95.149 | 543 | 409 k | 336 | 365 k | 207 | 43 k | — | — | — | — |
| 74.125.95.155 | 46 | 20 k | 25 | 10 k | 21 | 10 k | — | — | — | — |
| 74.125.103.147 | 608 | 633 k | 435 | 620 k | 173 | 12 k | — | — | — | — |
| 74.125.103.163 | 3,927 | 4232 k | 2,882 | 4173 k | 1,045 | 58 k | — | — | — | — |
| 74.125.166.28 | 553 | 532 k | 382 | 519 k | 171 | 13 k | — | — | — | — |

任务1 端点和会话统计分析



Wireshark · Conversations · lotsofweb.pcapng

Ethernet · 13 IPv4 · 103 IPv6 · 4 TCP · 279 UDP · 93

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A |
|-------------------|-------------------|---------|--------|---------------|-------------|---------------|
| 00:05:5d:21:99:4c | 00:21:6a:5b:7d:4a | 12,754 | 9909 k | 7,794 | 8971 k | 4,960 |
| 00:05:5d:21:99:4c | ff:ff:ff:ff:ff:ff | 1 | 342 | 1 | 342 | 0 |
| 00:1d:7e:2d:64:96 | 00:21:6a:5b:7d:4a | 2 | 818 | 2 | 818 | 0 |
| 00:1d:7e:2d:64:96 | 01:00:5e:7f:ff:fa | 21 | 8227 | 21 | 8227 | 0 |
| 00:21:6a:5b:7d:4a | ff:ff:ff:ff:ff:ff | 43 | 3956 | 43 | 3956 | 0 |
| 00:21:6a:5b:7d:4a | 01:00:5e:7f:ff:fa | 2 | 350 | 2 | 350 | 0 |
| 00:21:6a:5b:7d:4a | 01:00:5e:00:01:3c | 1 | 86 | 1 | 86 | 0 |
| 00:21:6a:5b:7d:4a | 33:33:00:01:00:03 | 28 | 2408 | 28 | 2408 | 0 |
| 00:21:6a:5b:7d:4a | 01:00:5e:00:00:fc | 28 | 1848 | 28 | 1848 | 0 |
| 00:21:6a:5b:7d:4a | 33:33:00:00:00:0c | 2 | 2304 | 2 | 2304 | 0 |
| 00:21:6a:5b:7d:4a | 33:33:00:01:00:02 | 2 | 308 | 2 | 308 | 0 |
| 00:25:bc:46:65:bb | ff:ff:ff:ff:ff:ff | 7 | 594 | 7 | 594 | 0 |
| 00:25:bc:46:65:bb | 01:00:5e:00:00:fb | 8 | 892 | 8 | 892 | 0 |

☐ 解析名称
 ☐ 显示过滤器的限制
 ☐ 绝对开始时间
 Conversation 类型 ▼

复制 ▼ Follow Stream... Graph... Close Help



任务1 端点和会话统计分析

异常流量**溯源**的基本步骤：

- 1、通过端点窗口找到发送/接受数据包最多、最大的端点
- 2、打开会话窗口验证通信数据包最多、最大的端点的通信行为，找到它们之间是否存在通信
- 3、直接将该会话作为筛选过滤器，在数据包列表面板中进行进一步的分析

Wireshark · Conversations · http_espn_fail.pcapng

| Ethernet · 1 | IPv4 · 8 | IPv6 | TCP · 16 | UDP · 7 | | | | | | | |
|---------------|---------------|---------|----------|---------------|-------------|---------------|-------------|-----------|----------|--------------|--------------|
| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
| 72.246.56.35 | 172.16.16.154 | 247 | 106 k | 124 | 188 k | 112 | 8315 | 0.527902 | 90.8063 | 16 k | |
| 172.16.16.154 | 203.0.113.9 | | | | | | | 0 | 0.430071 | 94.5936 | 572 |
| 72.21.91.8 | 172.16.16.1 | | | | | | | 3170 | 0.526867 | 60.5532 | 8863 |
| 172.16.16.154 | 199.181.13. | | | | | | | 47 k | 0.238547 | 91.0836 | 171 |
| 72.246.56.83 | 172.16.16.1 | | | | | | | 1518 | 0.659868 | 45.3449 | 3384 |
| 69.31.75.194 | 172.16.16.154 | | | | | | | 1007 | 0.579477 | 90.6593 | 789 |
| 4.2.2.1 | 172.16.16.154 | 14 | 1627 | | | | | 521 | 0.000000 | 0.6639 | 13 k |
| 68.71.212.158 | 172.16.16.154 | 13 | 2032 | | | | | 832 | 0.027167 | 90.8752 | 105 |

作为过滤器应用

选中

非选中

准备过滤器

查找

着色

...and Selected

...or Selected

...and not Selected

...or not Selected

A ↔ B

A → B

B → A

A ↔ Any

A → Any

Any → A

Any ↔ B

Any → B

B → Any



任务1 端点和会话统计分析

验证试验-1

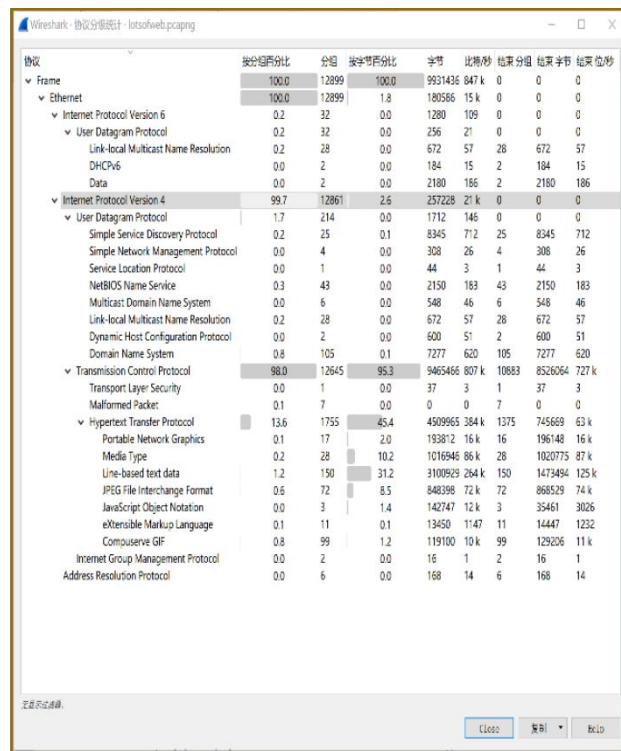
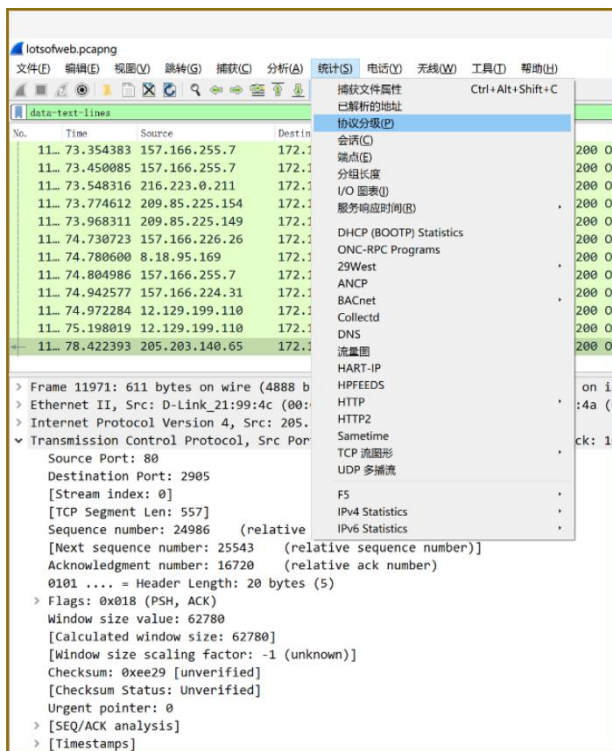
管理员用Wireshark进行了数据包嗅探捕获产生*lotsofweb.pcapng*捕获文件，请对该数据包捕获文件进行分析，并回答下列问题：

- 1、通信量最大、最活跃的端点有哪些？
- 2、最大的数据通信量来自于哪些端点的通信？
- 3、对最大的数据通信特点进行分析，有什么特点呢？

任务1 端点和会话统计分析

协议分层结构的统计

有时候需要知道数据包捕获文件中协议的分布情况，也就是捕获文件中TCP、IP、DHCP等所占百分比的多少





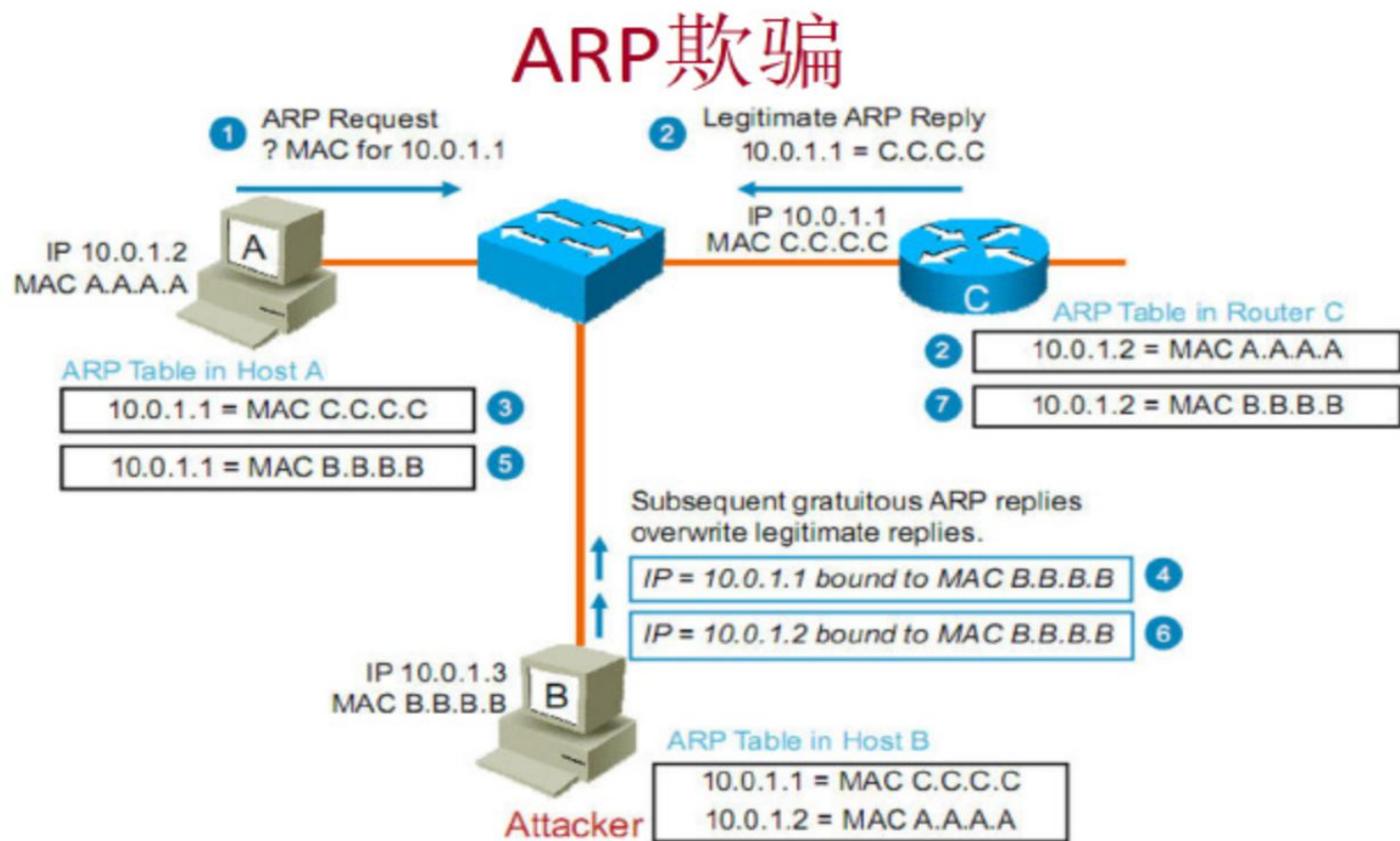
任务1 端点和会话统计分析

验证试验-2

通过Wireshark的协议分层结构统计功能发现某一段时间内ARP数据包的数量大增，利用过滤器将这一段时间内的arp数据包过滤出来，保存在捕获文件 *lotsofarp.pcapng* 中，请你对该捕获文件进行分析，你有什么猜测或者结论呢？

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|---|
| 1 | 0.000000 | 00:0c:29:91:c4:10 | ff:ff:ff:ff:ff:ff | ARP | 42 | Who has 192.168.3.1? Tell 192.168.3.25 |
| 2 | 0.003261 | f4:a5:9d:5b:8f:44 | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f4:a5:9d:5b:8f:44 |
| 3 | 5.027210 | f4:a5:9d:5b:8f:44 | 00:0c:29:91:c4:10 | ARP | 60 | Who has 192.168.3.25? Tell 192.168.3.1 |
| 4 | 5.027235 | 00:0c:29:91:c4:10 | f4:a5:9d:5b:8f:44 | ARP | 42 | 192.168.3.25 is at 00:0c:29:91:c4:10 |
| 5 | 12.807236 | 50:57:9c:b7:c0:6a | ff:ff:ff:ff:ff:ff | ARP | 60 | Gratuitous ARP for 192.168.3.10 (Request) |
| 6 | 12.807263 | f4:a5:9d:5b:8f:44 | ff:ff:ff:ff:ff:ff | ARP | 60 | Who has 192.168.3.10? Tell 192.168.3.1 |
| 7 | 37.281489 | f4:a5:9d:5b:8f:44 | ff:ff:ff:ff:ff:ff | ARP | 60 | Who has 192.168.3.2? Tell 192.168.3.1 |
| 8 | 37.588185 | 70:8a:09:93:bc:b2 | ff:ff:ff:ff:ff:ff | ARP | 60 | Who has 192.168.3.1? Tell 192.168.3.2 |
| 9 | 38.687971 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 10 | 38.688904 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 11 | 38.688924 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 12 | 38.689079 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 13 | 38.689358 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 14 | 38.689614 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 15 | 38.690665 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 16 | 38.690679 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 17 | 38.690684 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |
| 18 | 38.690688 | f8:e4:e3:b0:ea:6e | 00:0c:29:91:c4:10 | ARP | 60 | 192.168.3.1 is at f8:e4:e3:b0:ea:6e |

补充知识：ARP协议及ARP欺骗



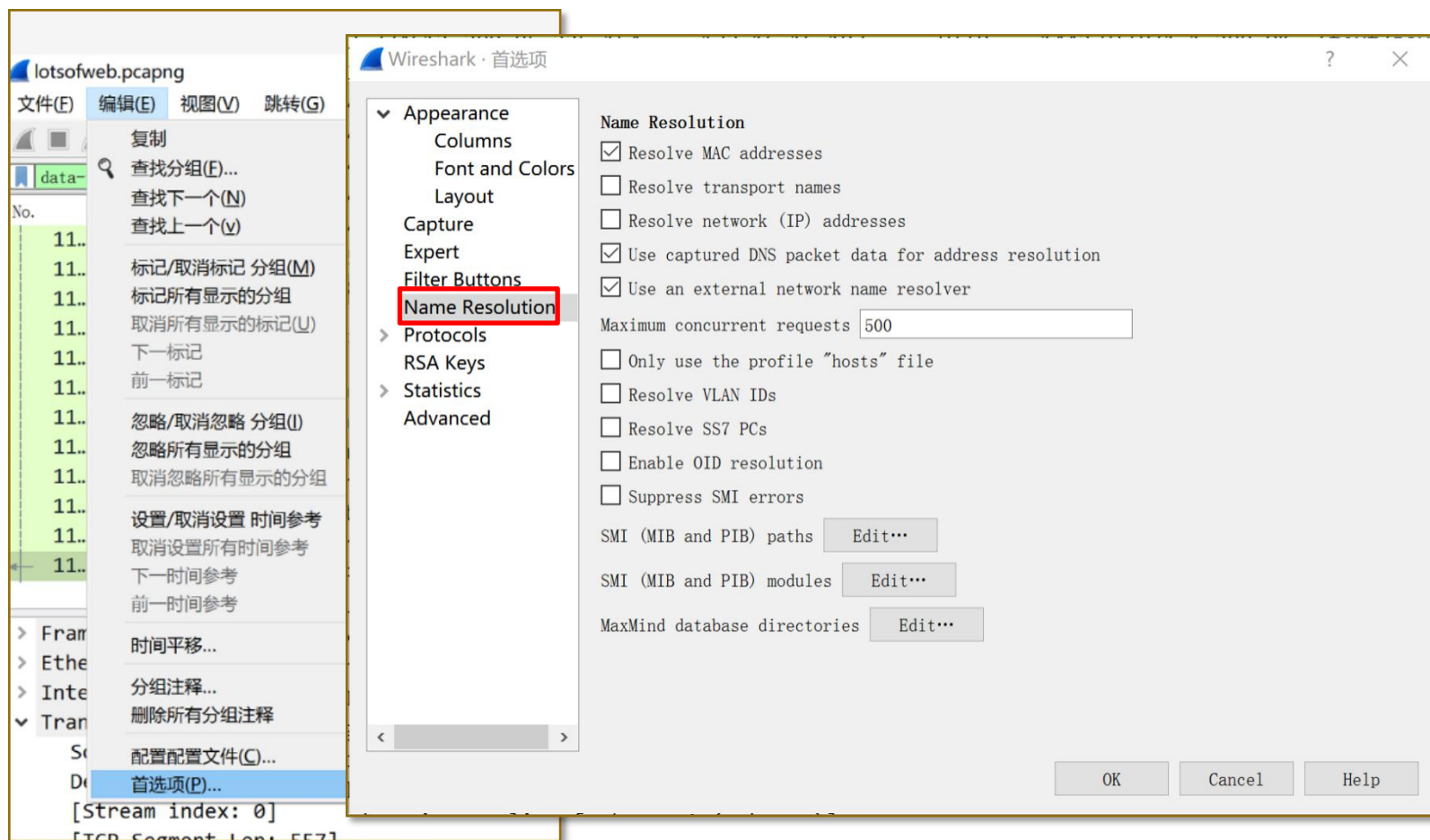


任务2 名称解析

将一个独特的地址**转换**为另外地址，其目的是为了更方便记忆和使用

Wireshark在分析捕获的数据包是，往往使用名称解析来**简化**分析过程，避免用户在一大堆让人头晕眼花的地址中绕来绕去。

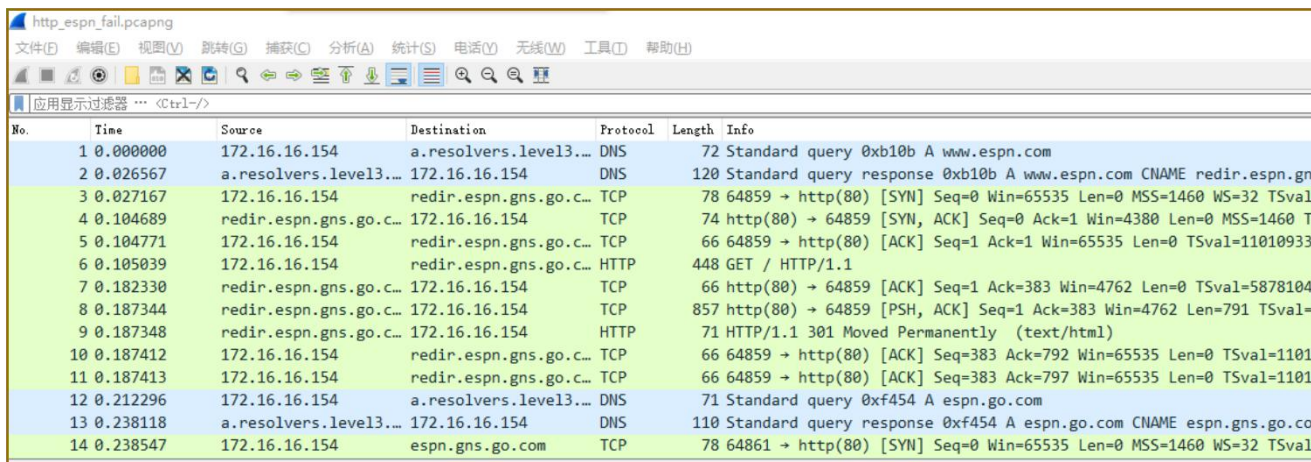
任务2 名称解析



任务2 名称解析

验证试验-3

用Wireshark打开捕获文件`lotsofweb.pcapng`，通过设置名字解析的相关选项和参数，使得数据包列表面板中的source或者destination列中出现与IP地址对应的名字



The screenshot shows the Wireshark interface with the file `http_espn_fail.pcapng` open. The packet list pane displays 14 packets. The 'Name' column is visible, showing the resolved hostnames for the source and destination IP addresses.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|--|
| 1 | 0.000000 | 172.16.16.154 | a.resolvers.level3... | DNS | 72 | Standard query 0xb10b A www.espn.com |
| 2 | 0.026567 | a.resolvers.level3... | 172.16.16.154 | DNS | 120 | Standard query response 0xb10b A www.espn.com CNAME redir.espn.gn |
| 3 | 0.027167 | 172.16.16.154 | redir.espn.gns.go.c... | TCP | 78 | 64859 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval= |
| 4 | 0.104689 | redir.espn.gns.go.c... | 172.16.16.154 | TCP | 74 | http(80) → 64859 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 TS |
| 5 | 0.104771 | 172.16.16.154 | redir.espn.gns.go.c... | TCP | 66 | 64859 → http(80) [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=11010933 |
| 6 | 0.105039 | 172.16.16.154 | redir.espn.gns.go.c... | HTTP | 448 | GET / HTTP/1.1 |
| 7 | 0.182330 | redir.espn.gns.go.c... | 172.16.16.154 | TCP | 66 | http(80) → 64859 [ACK] Seq=1 Ack=383 Win=4762 Len=0 TSval=5878104 |
| 8 | 0.187344 | redir.espn.gns.go.c... | 172.16.16.154 | TCP | 857 | http(80) → 64859 [PSH, ACK] Seq=1 Ack=383 Win=4762 Len=791 TSval= |
| 9 | 0.187348 | redir.espn.gns.go.c... | 172.16.16.154 | HTTP | 71 | HTTP/1.1 301 Moved Permanently (text/html) |
| 10 | 0.187412 | 172.16.16.154 | redir.espn.gns.go.c... | TCP | 66 | 64859 → http(80) [ACK] Seq=383 Ack=792 Win=65535 Len=0 TSval=11010 |
| 11 | 0.187413 | 172.16.16.154 | redir.espn.gns.go.c... | TCP | 66 | 64859 → http(80) [ACK] Seq=383 Ack=797 Win=65535 Len=0 TSval=11010 |
| 12 | 0.212296 | 172.16.16.154 | a.resolvers.level3... | DNS | 71 | Standard query 0xf454 A espn.go.com |
| 13 | 0.238118 | a.resolvers.level3... | 172.16.16.154 | DNS | 110 | Standard query response 0xf454 A espn.go.com CNAME espn.gns.go.co |
| 14 | 0.238547 | 172.16.16.154 | espn.gns.go.com | TCP | 78 | 64861 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval= |



任务2 名称解析

名称解析的潜在弊端：

- 1、名称解析可能失败，尤其是没有可用的DNS服务器时
- 2、名称解析会带来额外的开销
- 3、名称解析的数据包可能会影响到对捕获数据的分析

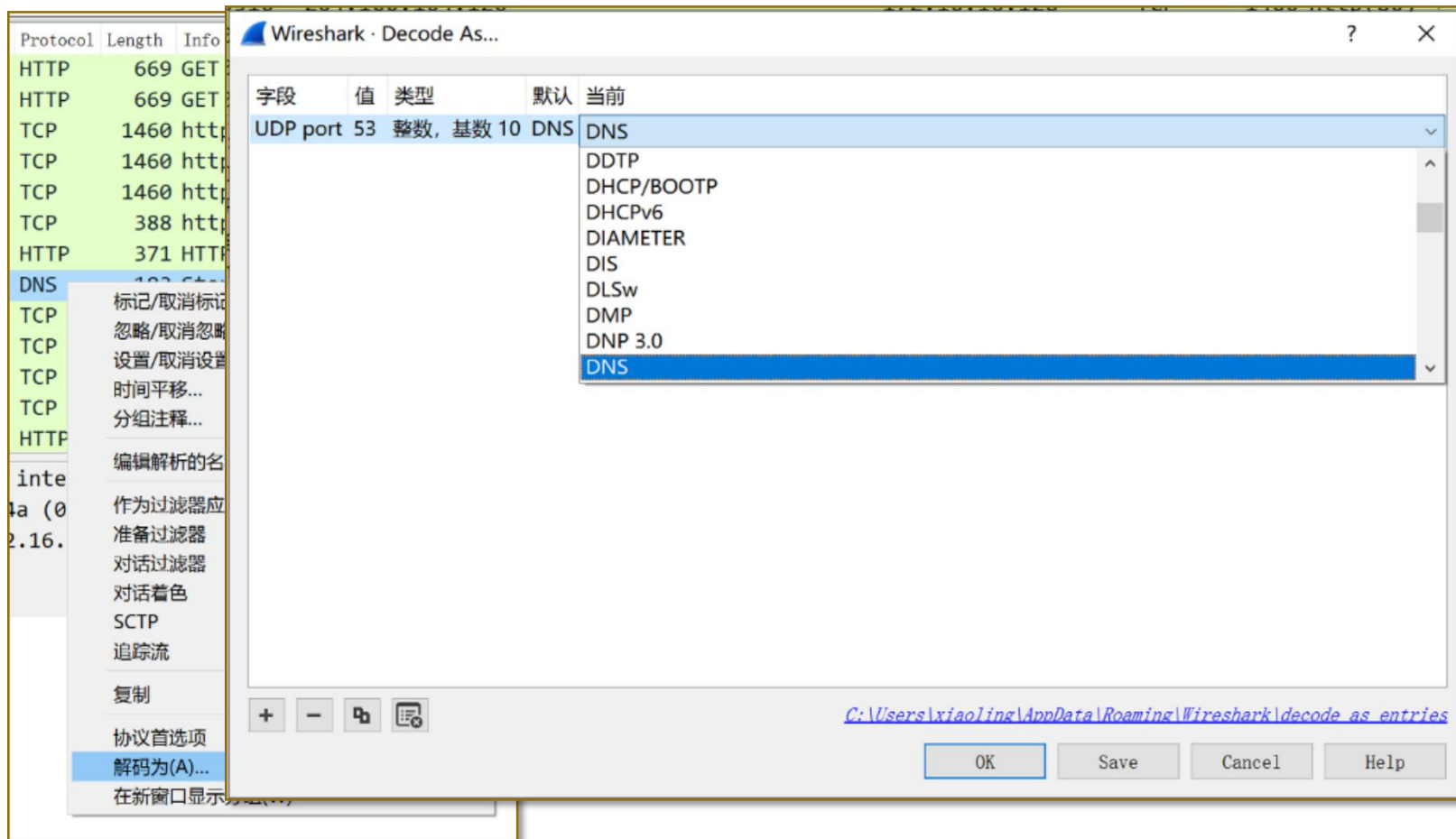


任务3 协议解析

Wireshark最大的优势在于对上千种协议解析的支持，协议解析器允许将数据包拆分成多个协议区段方便分析。

Wireshark**自动识别**每个数据包并决定如何显示该数据包，但是也并非每次都能够选择正确的协议解析器。特别是协议使用**非标准**的配置时。

任务3 协议解析





任务3 协议解析

验证试验-4

使用Wireshark打开捕获文件`wrongdissector.pcapng`，对数据包进行分析，并回答下列问题：

- 1、Wireshark是否选择了错误的协议解析器，为什么？
- 2、你认为正确的协议解析器应该是什么？为什么？
- 3、请为Wireshark的更换正确的协议解析器。
- 4、你认为本案例中Wireshark错误选择协议解析器的原因是什么



任务3 协议解析

是否保存更换的协议解析器？

将保存更换协议解析器配置这件事情忘在脑后是一件非常容易的事情。一旦出现这样的情况将引起一系列混乱。因此个人强烈建议**不**保存，以避免自己给自己挖了一个大坑。



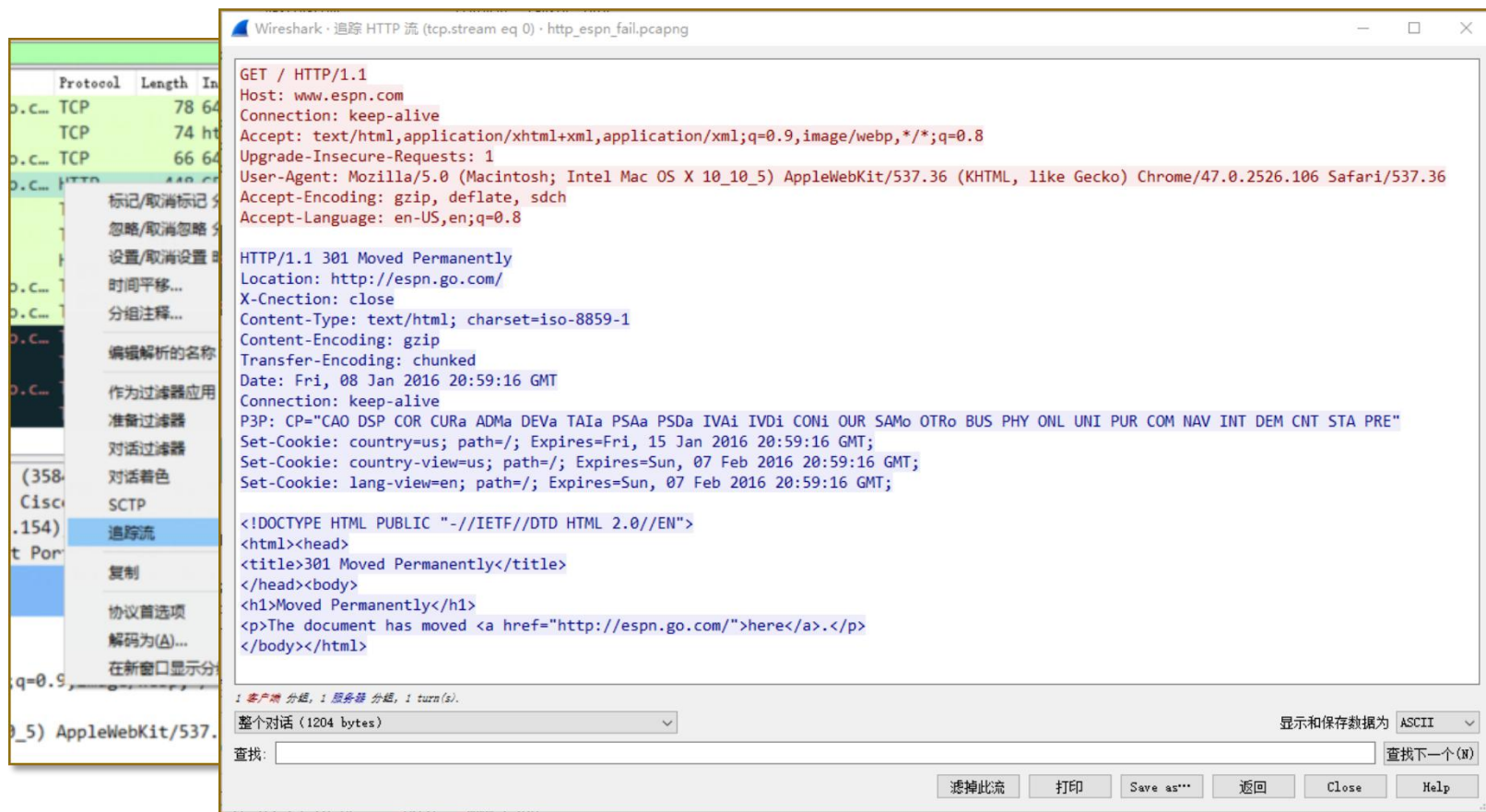
任务4 流追踪

Wireshark分析功能中令人满意的一点就是他能够将来自不同包的数据重组成**统一易读**的格式。

目前Wireshark可以跟踪4种类型的流：

- TCP流
- UDP流
- SSL流
- HTTP流。

任务4 流追踪





任务4 流追踪

验证试验-5

使用Wireshark打开捕获文件 *http_google.pcapng*，对数据包进行分析，完成下面的操作：

- 1、在Wireshark的数据包列表面板中找到第一个http请求数据包；
- 2、跟踪该http流，找到第一个http请求数据包的响应数据包；
- 3、该响应数据包响应了一个什么样的内容呢，从http的响应数据包提取服务器响应的对象，并使用浏览器查看之？

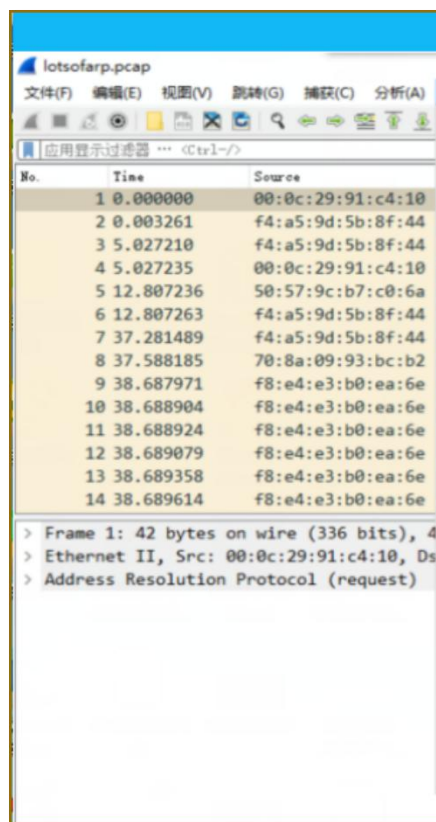


任务5 数据包长度

某些情况下，我们就可以通过捕获文件中数据包长度的分布情况，做一些对流量的合理猜测。

如果存在很多较大的数据包，那么很可能网络中在进行的大量的**数据传输**；如果绝大多数数据包都很小，我们便可以假设网络中此时存在**协议控制命令**，但是没有大规模的数据传输。

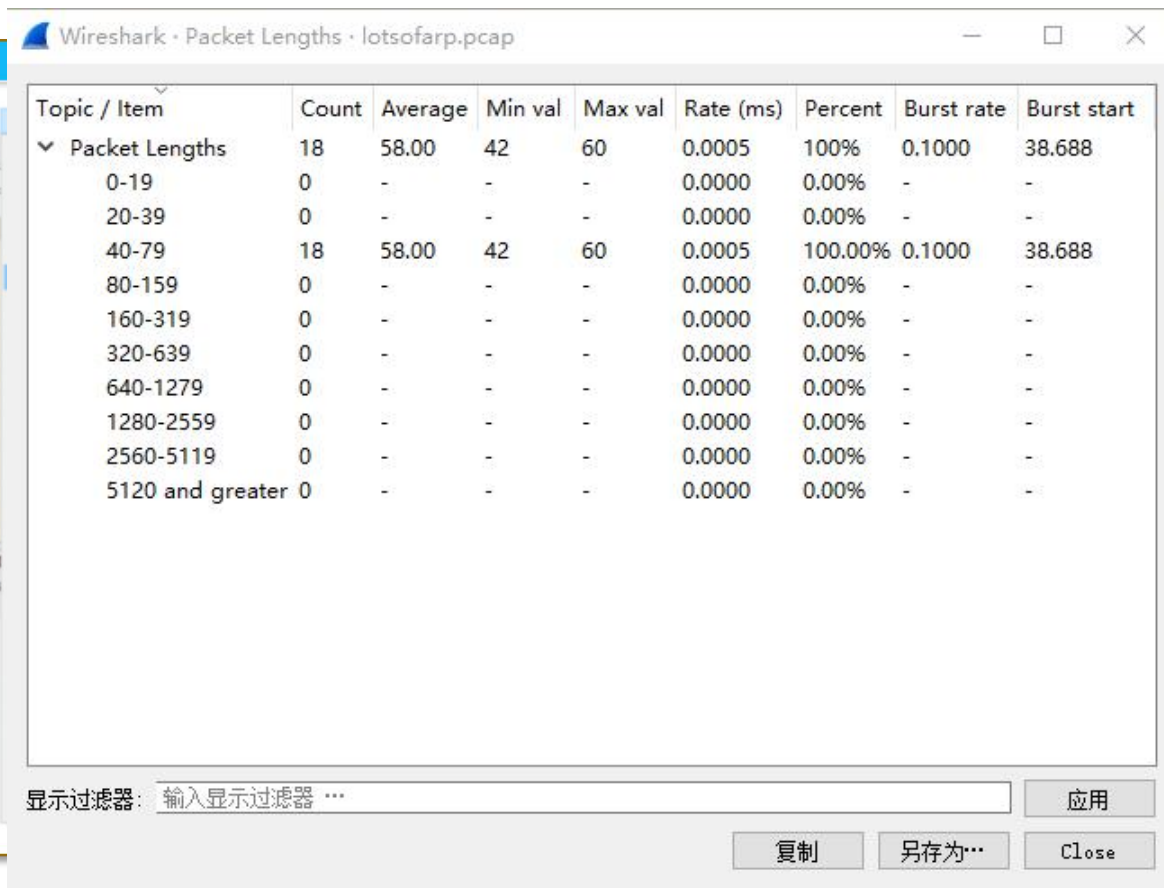
任务5 数据包长度



The image shows the Wireshark interface with the packet list and details panes. The packet list shows 14 packets, all from source 00:0c:29:91:c4:10. The details pane shows the structure of the first packet: Ethernet II, Src: 00:0c:29:91:c4:10, Dst: f8:e4:e3:b0:ea:6e, and Address Resolution Protocol (request).

| No. | Time | Source |
|-----|-----------|-------------------|
| 1 | 0.000000 | 00:0c:29:91:c4:10 |
| 2 | 0.003261 | f4:a5:9d:5b:8f:44 |
| 3 | 5.027210 | f4:a5:9d:5b:8f:44 |
| 4 | 5.027235 | 00:0c:29:91:c4:10 |
| 5 | 12.807236 | 50:57:9c:b7:c0:6a |
| 6 | 12.807263 | f4:a5:9d:5b:8f:44 |
| 7 | 37.281489 | f4:a5:9d:5b:8f:44 |
| 8 | 37.588185 | 70:8a:09:93:bc:b2 |
| 9 | 38.687971 | f8:e4:e3:b0:ea:6e |
| 10 | 38.688904 | f8:e4:e3:b0:ea:6e |
| 11 | 38.688924 | f8:e4:e3:b0:ea:6e |
| 12 | 38.689079 | f8:e4:e3:b0:ea:6e |
| 13 | 38.689358 | f8:e4:e3:b0:ea:6e |
| 14 | 38.689614 | f8:e4:e3:b0:ea:6e |

> Frame 1: 42 bytes on wire (336 bits), 4 captured (28 bits) on interface 0
> Ethernet II, Src: 00:0c:29:91:c4:10, Dst: f8:e4:e3:b0:ea:6e
> Address Resolution Protocol (request)



The image shows the 'Wireshark - Packet Lengths - lotsofarp.pcap' dialog box. It displays a table of packet length statistics. The 'Packet Lengths' section is expanded, showing a distribution of packet sizes. The 'Display filter' field is empty, and the 'Apply' button is highlighted.

| Topic / Item | Count | Average | Min val | Max val | Rate (ms) | Percent | Burst rate | Burst start |
|------------------|-------|---------|---------|---------|-----------|---------|------------|-------------|
| Packet Lengths | 18 | 58.00 | 42 | 60 | 0.0005 | 100% | 0.1000 | 38.688 |
| 0-19 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 20-39 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 40-79 | 18 | 58.00 | 42 | 60 | 0.0005 | 100.00% | 0.1000 | 38.688 |
| 80-159 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 160-319 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 320-639 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 640-1279 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 1280-2559 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 2560-5119 | 0 | - | - | - | 0.0000 | 0.00% | - | - |
| 5120 and greater | 0 | - | - | - | 0.0000 | 0.00% | - | - |

显示过滤器: 输入显示过滤器 ...

应用 复制 另存为... Close



任务5 数据包长度

验证试验-6

使用Wireshark打开捕获文件 *download_slow.pcapng*，对其数据包长度进行统计分析。这些网络流量中是否存在大规模的数据传输呢？

任务6 丢失的页面

当Peter和往常一样打开网站ESPN查看篮球比赛成绩的时候，他发现加载网页耗费了很长的时间，而当加载过程终于完成时，页面丢失了大部分图片和内容。

需要明确的是，这个问题只在Peter一个人的计算机上发生，并没有影响到其他人，因此我们在Peter的计算机上进行数据包嗅探工作，获取了数据包捕获文件 *[http_espn_fail.pcapng](#)*。





任务6 丢失的页面

1、首先，我们需要从大量的网络数据包中找到**http请求数据包**。

- 1) 设置过滤器筛选http请求报文;
- 2) http请求序列

实验7-1: 请提供两种方法过滤http请求数据包的截图



任务6 丢失的页面

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|----------------|----------|--------|----------------------------------|
| 6 | 0.105039 | 172.16.16.154 | 68.71.212.158 | HTTP | 448 | GET / HTTP/1.1 |
| 17 | 0.316340 | 172.16.16.154 | 199.181.133.61 | HTTP | 447 | GET / HTTP/1.1 |
| 71 | 0.554110 | 172.16.16.154 | 72.21.91.8 | HTTP | 398 | GET /js/310987714.js HTTP/1.1 |
| 74 | 0.565877 | 172.16.16.154 | 72.246.56.35 | HTTP | 511 | GET /combiner/i?img=%2Fphoto%2F2 |
| 202 | 0.616633 | 172.16.16.154 | 69.31.75.194 | HTTP | 491 | GET /i/columnists/kapadia_sheil_ |
| 387 | 0.700630 | 172.16.16.154 | 72.246.56.35 | HTTP | 490 | GET /combiner/i?img=%2Fphoto%2F2 |
| 390 | 0.702291 | 172.16.16.154 | 72.246.56.83 | HTTP | 594 | GET /combiner/i?img=%2Fmedia%2Fm |

Topic / Item

▼ HTTP Request Sequences

▼ http://www.espn.com/

▼ http://espn.go.com/

http://cdn.optimizely.com/js/310987714.js

http://assets.espn.go.com/i/columnists/kapadia_sheil_m.jpg

http://a4.espncdn.com/combiner/i?img=%2Fphoto%2F2014%2F0806%2F nfl_g_colts5_cr_1296x729.jpg&w=556&cquality

http://a2.espncdn.com/combiner/i?img=%2Fmedia%2Fmotion%2F2016%2F0108%2Fdm_160108_Trainer_should_get_the

http://a1.espncdn.com/combiner/i?img=%2Fphoto%2F2016%2F0108%2Fsubzero_5x2.png&w=1296&h=518&scale=cro



任务6 丢失的页面

2、在没有明确的目标会话的情况下，进行**协议层次统计**分析。这将帮助我们定位非预期的协议和通信过程中各种协议分布的异常。

实验7-2： 请提供对整个报文的协议分层统计分析的截图

任务6 丢失的页面

| 协议 | 按分组百分比 | 分组 | 按字节百分比 | 字节 | 比特/秒 | 结束 分组 | 结束 字节 | 结束 位/秒 |
|---------------------------------|--------|-----|--------|--------|------|-------|--------|--------|
| ▼ Frame | 100.0 | 569 | 100.0 | 357205 | 30 k | 0 | 0 | 0 |
| ▼ Ethernet | 100.0 | 569 | 2.2 | 7966 | 670 | 0 | 0 | 0 |
| ▼ Internet Protocol Version 4 | 100.0 | 569 | 3.2 | 11380 | 958 | 0 | 0 | 0 |
| ▼ User Datagram Protocol | 2.5 | 14 | 0.0 | 112 | 9 | 0 | 0 | 0 |
| Domain Name System | 2.5 | 14 | 0.3 | 1039 | 87 | 14 | 1039 | 87 |
| ▼ Transmission Control Protocol | 97.5 | 555 | 94.3 | 336702 | 28 k | 541 | 328718 | 27 k |
| ▼ Hypertext Transfer Protocol | 2.5 | 14 | 89.1 | 318310 | 26 k | 7 | 2917 | 245 |
| Portable Network Graphics | 0.2 | 1 | 41.4 | 147718 | 12 k | 1 | 148117 | 12 k |
| Line-based text data | 0.5 | 3 | 144.9 | 517527 | 43 k | 3 | 109488 | 9217 |
| JPEG File Interchange Format | 0.5 | 3 | 15.8 | 56573 | 4762 | 3 | 57788 | 4865 |



任务6 丢失的页面

3、对存在的7个HTTP会话进行逐个分析。

实验7-3：请使用Wireshark统计会话功能列出本案例捕获数据包中的所有会话，并提交截图



任务6 丢失的页面

| Ethernet · 1 | | IPv4 · 8 | | IPv6 | TCP · 16 | | UDP · 7 | | | | | |
|---------------|----------------|----------|-------|---------------|-------------|---------------|-------------|-----------|----------|--------------|--------------|--|
| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A | |
| 4.2.2.1 | 172.16.16.154 | 14 | 1627 | 7 | 1106 | 7 | 521 | 0.000000 | 0.6639 | 13 k | | |
| 68.71.212.158 | 172.16.16.154 | 13 | 2032 | 6 | 1200 | 7 | 832 | 0.027167 | 90.8752 | 105 | | |
| 69.31.75.194 | 172.16.16.154 | 19 | 9949 | 10 | 8942 | 9 | 1007 | 0.579477 | 90.6593 | 789 | | |
| 72.21.91.8 | 172.16.16.154 | 92 | 70 k | 49 | 67 k | 43 | 3170 | 0.526867 | 60.5532 | 8863 | | |
| 72.246.56.35 | 172.16.16.154 | 247 | 196 k | 134 | 188 k | 113 | 8315 | 0.527902 | 90.8063 | 16 k | | |
| 72.246.56.83 | 172.16.16.154 | 30 | 20 k | 15 | 19 k | 15 | 1518 | 0.659868 | 45.3449 | 3384 | | |
| 172.16.16.154 | 199.181.133.61 | 61 | 49 k | 24 | 1953 | 37 | 47 k | 0.238547 | 91.0836 | 171 | | |
| 172.16.16.154 | 203.0.113.94 | 93 | 6774 | 93 | 6774 | 0 | 0 | 0.430071 | 94.5936 | 572 | | |



任务6 丢失的页面

4、发现异常，使用流追踪功能重点分析异常会话

实验7-4: 请在Wireshark数据包列表面板中展示异常会话

任务6 丢失的页面

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|--------------|----------|--------|---|
| 25 | 0.430071 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | 64862 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1101093668 TSecr=0 SACK |
| 26 | 0.430496 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | 64863 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1101093668 TSecr=0 SACK |
| 27 | 0.431050 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | 64864 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1101093669 TSecr=0 SACK |
| 39 | 0.500663 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | 64865 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1101093737 TSecr=0 SACK |
| 40 | 0.500873 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | 64866 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1101093737 TSecr=0 SACK |
| 70 | 0.553964 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | 64869 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1101093787 TSecr=0 SACK |
| 456 | 1.460006 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64863 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 457 | 1.460006 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64862 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 458 | 1.461238 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64864 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 459 | 1.530278 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64866 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 460 | 1.530278 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64865 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 461 | 1.580145 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64869 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 462 | 2.461157 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64863 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |
| 463 | 2.461157 | 172.16.16.154 | 203.0.113.94 | TCP | 78 | [TCP Retransmission] 64862 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=11 |



任务6 丢失的页面

真相大白！