

图 3: 下载网页截图

三、Wireshark 抓包的几种协议

1、ARP（地址解析协议）

ARP 是用于解析网络层（通常是 IPv4）地址和链路层（MAC）地址之间映射关系的协议。主机发送信息时将包含目标 IP 地址的 ARP 请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址。收到返回消息后将该 IP 地址和物理地址存入本机 ARP 缓存中并保留一定时间，下次请求时直接查询 ARP 缓存就可以节约资源。

| | | | | |
|----------------|-------------------|-------------------|-----|--|
| 47 0.151894082 | 10.0.0.1 | 210.76.211.10 | TCP | 54 43698 → 443 [ACK] Seq=641 ACK=38589 |
| 48 5.111441583 | 36:b0:d0:bb:1b:9d | ee:b7:c2:da:4a:fb | ARP | 42 Who has 10.0.0.3? Tell 10.0.0.1 |
| 49 5.111929307 | ee:b7:c2:da:4a:fb | 36:b0:d0:bb:1b:9d | ARP | 42 Who has 10.0.0.1? Tell 10.0.0.3 |
| 50 5.111946819 | 36:b0:d0:bb:1b:9d | ee:b7:c2:da:4a:fb | ARP | 42 10.0.0.1 is at 36:b0:d0:bb:1b:9d |
| 51 5.112101208 | ee:b7:c2:da:4a:fb | 36:b0:d0:bb:1b:9d | ARP | 42 10.0.0.3 is at ee:b7:c2:da:4a:fb |

26:b0:d0:bb:1b:9d 对应本地 IP 为 10.0.0.1 的 MAC 地址。ee:b7:c2:da:4a:fb 对应本地 IP 为 10.0.0.3 的 MAC 地址。

2、DNS（域名系统）

DNS 是用于将易记的域名（例如 www.example.com）映射到 IP 地址（例如 292.268.2.2）的分布式数据库系统。

| | | | | |
|---------------|----------|---------------|-----|---|
| 1 0.000000000 | 10.0.0.1 | 1.2.4.8 | DNS | 74 Standard query 0x6499 A www.ucas.ac.cn |
| 2 0.000066044 | 10.0.0.1 | 1.2.4.8 | DNS | 74 Standard query 0xd69d AAAA www.ucas.ac.cn |
| 3 0.009739670 | 1.2.4.8 | 10.0.0.1 | DNS | 132 Standard query response 0xd69d AAAA www.ucas.ac.cn SOA gsns.gscas.ac.cn |
| 4 0.010087783 | 1.2.4.8 | 10.0.0.1 | DNS | 98 Standard query response 0x6499 A www.ucas.ac.cn A 210.76.211.10 |
| 5 0.010247316 | 10.0.0.1 | 210.76.211.10 | TCP | 74 54060 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 TSval=36548552 |

上图首先由本地 IP10.0.0.1 作为 source，向目标地址 1.2.4.8 即 DNS 服务器发送查询请求。1.2.4.8 返回本地 IP 解析结果，根据上图可以看出为 210.76.211.10。

3、TCP（传输控制协议）

TCP 是一种面向连接的、可靠的协议，用于在网络上传输数据。它确保数据的有序传输和可靠交付，通过使用三次握手来建立连接，并使用滑动窗口和确认机制来管理数据流。TCP 也处理数据分段、错误检测和恢复以及流量控制。它用于大多数应用程序的可靠通信，如网页浏览、文件下载和电子邮件。

| | | | | |
|----------------|---------------|---------------|-----|--|
| 13 0.059560267 | 210.76.211.10 | 10.0.0.1 | TCP | 58 443 → 43650 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 7 0.016019671 | 10.0.0.1 | 210.76.211.10 | TCP | 54 54060 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0 |
| 11 0.030470638 | 10.0.0.1 | 210.76.211.10 | TCP | 54 54060 → 80 [ACK] Seq=130 Ack=369 Win=41972 Len=0 |
| 36 0.134011810 | 10.0.0.1 | 210.76.211.10 | TCP | 54 54060 → 80 [ACK] Seq=131 Ack=370 Win=41972 Len=0 |
| 28 0.112404252 | 10.0.0.1 | 210.76.211.10 | TCP | 54 54060 → 80 [FIN, ACK] Seq=130 Ack=369 Win=41972 Len=0 |
| 5 0.010247316 | 10.0.0.1 | 210.76.211.10 | TCP | 74 54060 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 TSval=3654855259 TSecr=0 WS=512 |
| 9 0.016751983 | 210.76.211.10 | 10.0.0.1 | TCP | 54 80 → 54060 [ACK] Seq=1 Ack=130 Win=64240 Len=0 |
| 29 0.112744801 | 210.76.211.10 | 10.0.0.1 | TCP | 54 80 → 54060 [ACK] Seq=369 Ack=131 Win=64239 Len=0 |
| 35 0.133948492 | 210.76.211.10 | 10.0.0.1 | TCP | 54 80 → 54060 [FIN, PSH, ACK] Seq=369 Ack=131 Win=64239 Len=0 |
| 6 0.015976484 | 210.76.211.10 | 10.0.0.1 | TCP | 58 80 → 54060 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |

图中在进行握手连接，服务端向客户端发送 SYN，客户端向服务端发送 ACK，FIN 表示关闭连接，PSH 代表存在数据传输。

3、HTTP（超文本传输协议）

HTTP 是一种应用层协议，用于在 Web 上传输超文本文档，如网页。HTTP 是无状态的，每个请求和响应之间是独立的，它使用不同的 HTTP 方法来执行不同的操作。HTTP 主要在 Web 浏览器上运行，当用户进入网站域并打算访问它时，HTTP 提供访问权限。

| | | | | |
|------------------|--------------------|---------------|---------|--|
| 15 0.061516771 | 10.0.0.1 | 210.76.211.10 | TLSv1.3 | 462 Client Hello |
| 8 0.016295348 | 10.0.0.1 | 210.76.211.10 | HTTP | 183 GET / HTTP/1.1 |
| 10 0.038415567 | 210.76.211.10 | 10.0.0.1 | HTTP | 422 HTTP/1.1 302 Moved Temporarily (text/html) |
| NR 133 022011828 | fe8b::2a5e:67ff:fe | ff62::2 | ICMPv6 | 76 Router Solicitation from 26:5e:67:ee:43:84 |

出现 GET 请求。

5、HTTPS

HTTPS 是 HTTP 的安全版本，它代表 HTTP Secure，它使用 TLS/SSL 协议来加密数据传输。这种加密确保数据在客户端和服务端之间的传输是安全的，无法被窃取或篡改。HTTPS 使用公钥加密和证书验证来确保通信的安全性。它在安全性方面比 HTTP 更可靠，因此在处理敏感信息（如信用卡号、登录凭据等）的网站上广泛使用。

6、DNS 和 HTTP 在应用层，IP 在网络层，TCP 在传输层，ARP 在数据链路层。这也就有了不同层次的协议封装，即 Ethernet<IP<TCP<HTTP。如下图可见。

```
Frame 10: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface h1-eth0, id 0
Ethernet II, Src: ee:b7:c2:da:4a:fb (ee:b7:c2:da:4a:fb), Dst: 36:b0:d0:bb:1b:9d (36:b0:d0:bb:1b:9d)
Internet Protocol Version 4, Src: 210.76.211.10, Dst: 10.0.0.1
Transmission Control Protocol, Src Port: 80, Dst Port: 54060, Seq: 1, Ack: 130, Len: 368
Hypertext Transfer Protocol
Line-based text data: text/html (8 lines)
```

四、下载 ucas 页面的过程

修改 h1 主机的 DNS 设置，将 DNS 服务器设置为 1.2.4.8。首先由 DNS 发送查询请求，解析 IP 地址为 210.76.211.10，而后 TCP 进行握手连接，服务端第一次发送 SYN，第二次发送 SYN+ACK，第三次发送 ACK，h1 主机接收到 ucas 网站的响应，则连接已建立。握手成功后显示 PSH 代表存在数据传输。

实验二：流完成时间实验

一、复现图像

1、原始数据

表 2：不同带宽文件大小下流完成时间

| | 2MB | 20MB | 200MB |
|---------|------|------|-------|
| 20Mbps | 2.5 | 9.4 | 88 |
| 50Mbps | 2.3 | 3.94 | 23.4 |
| 200Mbps | 2.27 | 3.58 | 24.4 |
| 500Mbps | 2.2 | 3.2 | 5.5 |

图中数据已经过五次平均

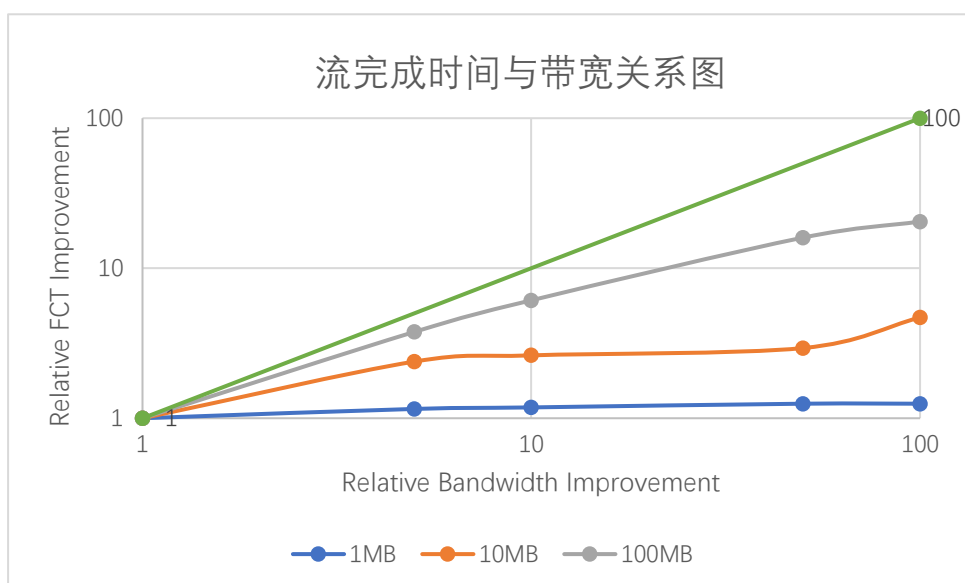
2、处理后的数据

表 2：处理后的数据

| | 2MB | 20MB | 200MB |
|----|----------|----------|---------|
| 2 | 2 | 2 | 2 |
| 5 | 2.253846 | 2.385787 | 3.76068 |
| 20 | 2.2822 | 2.625698 | 6.22222 |
| 50 | 2.25 | 2.9375 | 26 |

其中 x 轴处理公式为后续的带宽大小处于实验最小带宽，y 轴处理公式为同一文件大小下，最慢时间除以当前时间。

3、图像



横纵坐标均为 log 坐标

二、解释图像

首先这些文件的下载涉及到 TCP 传输。TCP 传输通过将数据拆分成称为数据包的小块来工作，然后在发送端和接收端之间交换这些数据包。首先，在两台计算机之间建立 TCP 连接需要进行三次握手过程，以确保双方都准备好进行通信。同时，TCP 具有拥塞控制机制，用于监测网络拥塞并相应地调整传输速率，以确保网络的稳定性和效率。

而慢启动机制是拥塞控制的一部分，它是在开始传输数据时以较低的速率开始，然后逐渐增加传输速率，直到达到网络的最大容量。在连接刚建立时，慢启动会将初始拥塞窗口设置为一个较小的值，通常为 1 到 10 个数据包大小。每当发送方接收到确认的数据包而不出现超时，拥塞窗口大小指数增长，从而导致发送速率的增加。如果出现超时或拥塞，发送方会将拥塞窗口减小，并重新开始慢启动。然后，它会以线性增长的方式逐渐增加拥塞窗口的大小。

该图像的数据均经过处理。可以看出，在文件大小为 1MB 时，平均下载速率并未随着带宽增加而有显著提升，而文件大小为 100MB 时，平均下载速率随带宽显著提升。因此，文件越大，下载时间随带宽增大越有明显减少，平均下载速率越明显增大。结合 TCP 传输工作原理，可以猜到，由于文件大小较小，拥塞窗口的作用不大，考虑到握手时间等因素，传输受其他因素影响较大。

而三条不同文件大小的曲线随着文件大小变大逐渐逼近 $y=x$ 曲线。这是由于随着文件大小增加，其他因素的影响减少，拥塞窗口大小成指数增长，发送速率在建立连接后迅速增加，带宽成为主要限制因素。较大文件的下载速率更接近实际带宽的能力，此时下载速率与文件大小之间的关系趋于线性。

三、部分实验测试截图

| "Node: h1" | "Node: h1" |
|--|--|
| <pre> root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:09:46-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.2' 1MB.dat.2 100%[=====] 1.00M 671KB/s in 1.5s 2023-09-14 19:09:51 (671 KB/s) - '1MB.dat.2' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# dd if=/dev/zero of=1MB.dat bs=1M count=1 1+0 records in 1+0 records out 1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.00490061 s, 214 MB/s root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:17:03-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.3' 1MB.dat.3 100%[=====] 1.00M 673KB/s in 1.5s 2023-09-14 19:17:05 (673 KB/s) - '1MB.dat.3' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:17:12-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.4' 1MB.dat.4 100%[=====] 1.00M 670KB/s in 1.5s 2023-09-14 19:17:14 (670 KB/s) - '1MB.dat.4' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:17:17-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.5' 1MB.dat.5 100%[=====] 1.00M 671KB/s in 1.5s 2023-09-14 19:17:19 (671 KB/s) - '1MB.dat.5' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:17:23-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.6' 1MB.dat.6 100%[=====] 1.00M 673KB/s in 1.5s 2023-09-14 19:17:25 (673 KB/s) - '1MB.dat.6' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# █ </pre> | <pre> root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:22:19-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.19' 1MB.dat.19 100%[=====] 1.00M 844KB/s in 1.2s 2023-09-14 19:22:21 (844 KB/s) - '1MB.dat.19' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:22:22-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.20' 1MB.dat.20 100%[=====] 1.00M 838KB/s in 1.2s 2023-09-14 19:22:24 (838 KB/s) - '1MB.dat.20' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:22:25-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.21' 1MB.dat.21 100%[=====] 1.00M 840KB/s in 1.2s 2023-09-14 19:22:27 (840 KB/s) - '1MB.dat.21' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:23:02-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.22' 1MB.dat.22 100%[=====] 1.00M 843KB/s in 1.2s 2023-09-14 19:23:03 (843 KB/s) - '1MB.dat.22' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat --2023-09-14 19:23:04-- http://10.0.0.2/1MB.dat Connecting to 10.0.0.2:80... connected. HTTP request sent, awaiting response... 200 OK Length: 1048576 (1.0M) [application/octet-stream] Saving to: '1MB.dat.23' 1MB.dat.23 100%[=====] 1.00M 841KB/s in 1.2s 2023-09-14 19:23:06 (841 KB/s) - '1MB.dat.23' saved [1048576/1048576] root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat </pre> |

```

root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat
--2023-09-14 19:30:40-- http://10.0.0.2/1MB.dat
Connecting to 10.0.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1048576 (1.0M) [application/octet-stream]
Saving to: '1MB.dat.30'

1MB.dat.30         100%[=====] 1.00M  844KB/s   in 1.2s

2023-09-14 19:30:41 (844 KB/s) - '1MB.dat.30' saved [1048576/1048576]

root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat
--2023-09-14 19:30:44-- http://10.0.0.2/1MB.dat
Connecting to 10.0.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1048576 (1.0M) [application/octet-stream]
Saving to: '1MB.dat.31'

1MB.dat.31         100%[=====] 1.00M  846KB/s   in 1.2s

2023-09-14 19:30:46 (846 KB/s) - '1MB.dat.31' saved [1048576/1048576]

root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat
--2023-09-14 19:30:47-- http://10.0.0.2/1MB.dat
Connecting to 10.0.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1048576 (1.0M) [application/octet-stream]
Saving to: '1MB.dat.32'

1MB.dat.32         100%[=====] 1.00M  843KB/s   in 1.2s

2023-09-14 19:30:49 (843 KB/s) - '1MB.dat.32' saved [1048576/1048576]

root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat
--2023-09-14 19:30:50-- http://10.0.0.2/1MB.dat
Connecting to 10.0.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1048576 (1.0M) [application/octet-stream]
Saving to: '1MB.dat.33'

1MB.dat.33         100%[=====] 1.00M  845KB/s   in 1.2s

2023-09-14 19:30:51 (845 KB/s) - '1MB.dat.33' saved [1048576/1048576]

root@leona-virtual-machine:/home/leona# wget http://10.0.0.2/1MB.dat
--2023-09-14 19:30:52-- http://10.0.0.2/1MB.dat
Connecting to 10.0.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1048576 (1.0M) [application/octet-stream]
Saving to: '1MB.dat.34'

1MB.dat.34         100%[=====] 1.00M  848KB/s   in 1.2s

2023-09-14 19:30:54 (848 KB/s) - '1MB.dat.34' saved [1048576/1048576]

```