# 相关标准

## HTTP 1.1

RFC 7230：Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing

RFC 7231：Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

RFC 7232：Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests

RFC 7233：Hypertext Transfer Protocol (HTTP/1.1): Range Requests

RFC 7234：Hypertext Transfer Protocol (HTTP/1.1): Caching

RFC 7235：Hypertext Transfer Protocol (HTTP/1.1): Authentication

## HTTP 2.0

RFC 7540：Hypertext Transfer Protocol Version 2 (HTTP/2)

# 有用的软件

## Wireshark

https://www.wireshark.org/

## Fiddler

<https://www.telerik.com/fiddler>

## RawCap

<https://www.netresec.com/?page=RawCap>

## tcpdump

<http://www.tcpdump.org/>

## curl

<https://curl.se/>

## 浏览器

F12，开发者工具

# HTTP 1.1消息例子

## 获取CRL

### 请求

GET /crl/ServerCA.crl HTTP/1.1

User-Agent: Wget/1.19.4 (linux-gnu)

Accept: \*/\*

Accept-Encoding: identity

Host: classaca1.cnca.net

Connection: Keep-Alive

### 响应

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 09 Nov 2020 03:16:45 GMT

Content-Type: application/pkix-crl

Content-Length: 1794

Connection: keep-alive

Last-Modified: Mon, 09 Nov 2020 03:00:04 GMT

ETag: "702-5b3a3c2473243"

Accept-Ranges: bytes

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Content-Security-Policy: frame-src 'self' combo.b.qq.com

具体的CRL的DER编码



## chunked传输编码

### 请求

GET / HTTP/1.1

User-Agent: Wget/1.19.4 (linux-gnu)

Accept: \*/\*

Accept-Encoding: identity

Host: www.cnca.net

Connection: Keep-Alive

### 响应

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 09 Nov 2020 02:56:32 GMT

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

Connection: keep-alive

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=0aj6d453lcfidfeuejdvtj4dk1; path=/; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: private

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Content-Security-Policy: frame-src 'self' combo.b.qq.com

712c

0x712c字节的网页

0



## 重定向

### 请求

GET / HTTP/1.1

User-Agent: Wget/1.19.4 (linux-gnu)

Accept: \*/\*

Accept-Encoding: identity

Host: www.qq.com

Connection: Keep-Alive

### 响应

HTTP/1.1 302 Moved Temporarily

Server: stgw/1.3.12.4\_1.13.5

Date: Mon, 09 Nov 2020 09:04:09 GMT

Content-Type: text/html

Content-Length: 169

Connection: keep-alive

Location: https://www.qq.com/

XXX

通常接着客户端会继续访问<https://www.qq.com>



## POST表单

POST /test/Echo HTTP/1.1

Host: 127.0.0.1:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 41

Origin: http://127.0.0.1:8080

Connection: keep-alive

Referer: http://127.0.0.1:8080/test/1.html

Upgrade-Insecure-Requests: 1

name=%E5%BC%A0%E4%B8%89&password=12345678

### 响应

HTTP/1.1 200

Content-Type: text/html;charset=UTF-8

Content-Length: 80

Date: Tue, 10 Nov 2020 09:06:47 GMT

Keep-Alive: timeout=20

Connection: keep-alive

具体的响应数据



## 文件上传

### 请求

POST /test/Upload HTTP/1.1

Host: 127.0.0.1:8080

Connection: keep-alive

Content-Length: 1192

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://127.0.0.1:8080

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLyd9aAAlJiaV5uJJ

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Edg/86.0.622.63

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: http://127.0.0.1:8080/test/2.html

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

------WebKitFormBoundaryLyd9aAAlJiaV5uJJ

Content-Disposition: form-data; name="memo"

Memo域的值

------WebKitFormBoundaryLyd9aAAlJiaV5uJJ

Content-Disposition: form-data; name="uploadFile"; filename="root.cer"

Content-Type: application/x-x509-ca-cert

上传的文件内容

------WebKitFormBoundaryLyd9aAAlJiaV5uJJ--



## 代理

### 请求

注意：请求是发送给代理服务器的

GET http://www.cnca.net/ HTTP/1.1

Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, \*/\*

Accept-Language: zh-CN

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; InfoPath.3; .NET CLR 3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729)

Accept-Encoding: gzip, deflate

Host: www.cnca.net

DNT: 1

Proxy-Connection: Keep-Alive

Cookie: pgv\_pvi=4996771840

### 响应

HTTP/1.1 200 OK

Server: nginx

Date: Wed, 24 Jun 2020 02:35:39 GMT

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

Connection: keep-alive

Vary: Accept-Encoding

Set-Cookie: PHPSESSID=d7hjd3ecfih08s655i035c7m66; path=/; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: private

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Content-Security-Policy: frame-src 'self' combo.b.qq.com

Content-Encoding: gzip

chunked编码的数据



## 断点续传

### 第一次请求

GET /crl/ServerCA.crl HTTP/1.1

Host: classaca1.cnca.net

User-Agent: NETCA-HTTP-CLIENT2/1.0

Connection: close

### 第一次响应

HTTP/1.1 200 OK

Server: nginx

Date: Wed, 09 Dec 2020 03:05:58 GMT

Content-Type: application/pkix-crl

Content-Length: 1759

Connection: close

Last-Modified: Wed, 09 Dec 2020 03:00:04 GMT

ETag: "6df-5b5ff418cee19"

Accept-Ranges: bytes

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Content-Security-Policy: frame-src 'self' combo.b.qq.com

具体的CRL的DER编码

强行在没有获取完就断开连接

### 断点续传请求

GET /crl/ServerCA.crl HTTP/1.1

Host: classaca1.cnca.net

User-Agent: NETCA-HTTP-CLIENT2/1.0

Connection: close

Range: bytes=512-1758

### 断点续传响应

HTTP/1.1 206 Partial Content

Server: nginx

Date: Wed, 09 Dec 2020 03:06:15 GMT

Content-Type: application/pkix-crl

Content-Length: 1247

Connection: close

Last-Modified: Wed, 09 Dec 2020 03:00:04 GMT

ETag: "6df-5b5ff418cee19"

Accept-Ranges: bytes

Content-Range: bytes 512-1758/1759

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Content-Security-Policy: frame-src 'self' combo.b.qq.com

第512字节到1758字节（包括），序号从0算起



# TLS抓包

如果是使用RSA加密预主密钥的方式，拿到私钥即可

Fiddler代理

Firefox使用环境变量SSLKEYLOGFILE的值记录TLS相关的密钥信息