# 计算机网络实验2报告

马成 20307130112

1. 分析HTTP GET请求分组中各个字段的含义，以及你还知道哪些其他字段，列出并指明含义。
    - Host：主机名
    - Connection：是否需要持久的连接
    - User-Agent：用户代理，一种向访问网站提供你所使用的浏览器类型及版本、操作系统及版本、浏览器内核、等信息的标识。
    - Accept：描述客户端希望接收的响应body 数据类型
    - Accept-Encoding：声明浏览器支持的编码类型
    - Accept-language：表示客户端可以接收的语言类型
    - Cookie：分配给客户端的Cokkie编号
    - Cache-Control：缓存配置

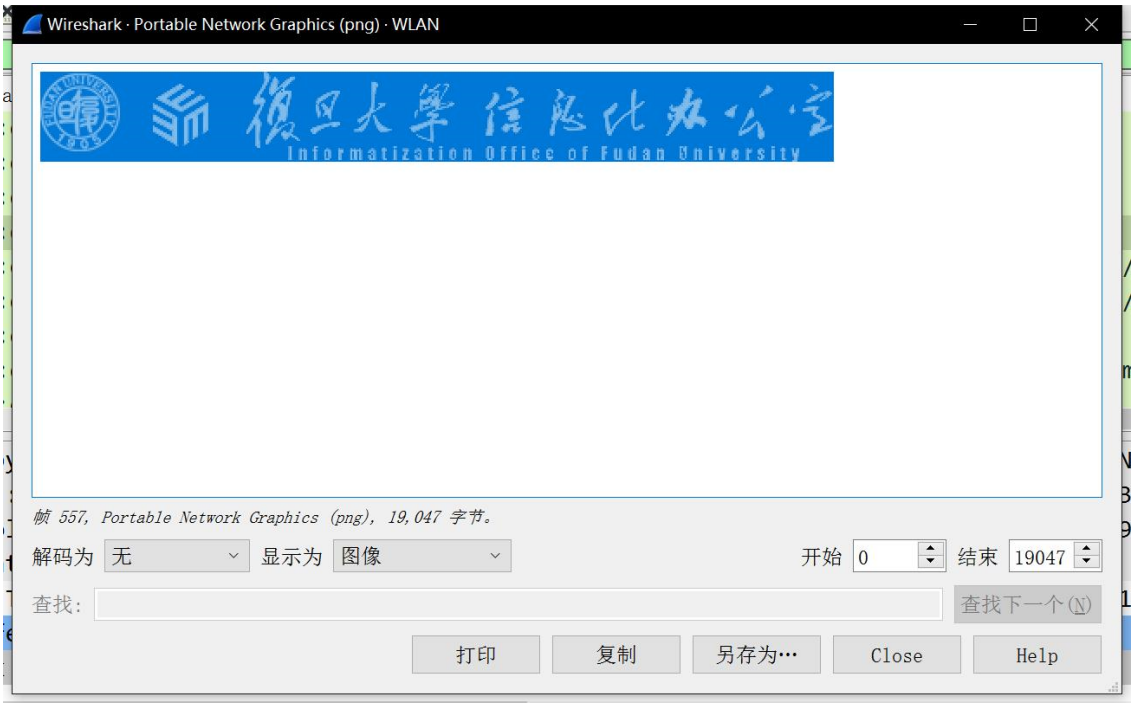
---

```
··Host: www.ecam (KHTML, like Ge
pus.fuda n.edu.cn cko) Chr ome/102.
··Connec tion: ke 0.0.0 Sa fari/537
ep-alive ··Upgrad .36··Acc ept: tex
e-Insecu re-Reque t/html,a pplicati
sts: 1·· User-Age on/xhtml +xml,app
nt: Mozi lla/5.0 lication /xml;q=0
(Windows NT 10.0 .9,image /avif,im
; Win64; x64) Ap age/webp ,image/a
pleWebKi t/537.36 png,*/*; q=0.8,ap
(KHTML, like Ge plicatio n/signed
cko) Chr ome/102. -exchang e;v=b3;q
0.0.0 Sa fari/537 =0.9··Ac cept-Enc
.36··Acc ept: tex oding: g zip, def
t/html,a pplicati late··Ac cept-Lan
on/xhtml +xml,app guage: z h-CN,zh;
lication /xml;q=0 q=0.9··C ookie: _
.9,image /avif,im ga=GA1.3 .3480343
age/webp ,image/a 62.16533 34214···
png,*/*; q=0.8,ap ·
```

2. 观察第一个请求的HTTP响应分组，指出这个HTTP响应分组是由多少个TCP报文段（segment）组成，并截图。 有38个分组(我给出的是第一个GET请求的分组数)

```
[38 Reassembled TCP Segments (47853 bytes): #38(278), #39(1400), #40(1400), #41(1304), #42(240), #43(1254), #44
    [Frame: 38, payload: 0-277 (278 bytes)]
    [Frame: 39, payload: 278-1677 (1400 bytes)]
    [Frame: 40, payload: 1678-3077 (1400 bytes)]
    [Frame: 41, payload: 3078-4381 (1304 bytes)]
    [Frame: 42, payload: 4382-4621 (240 bytes)]
    [Frame: 43, payload: 4622-5875 (1254 bytes)]
```

3. 观察一个带有明文图片的分组，通过“显示分组细节”，在wireshark中显示图片，并在浏览器中找出。





4. 在 `http://www.ecampus.fudan.edu.cn/` 网站搜索关键词，并使用wireshark抓包，观察并记录http是如何通过POST方法发送数据的。

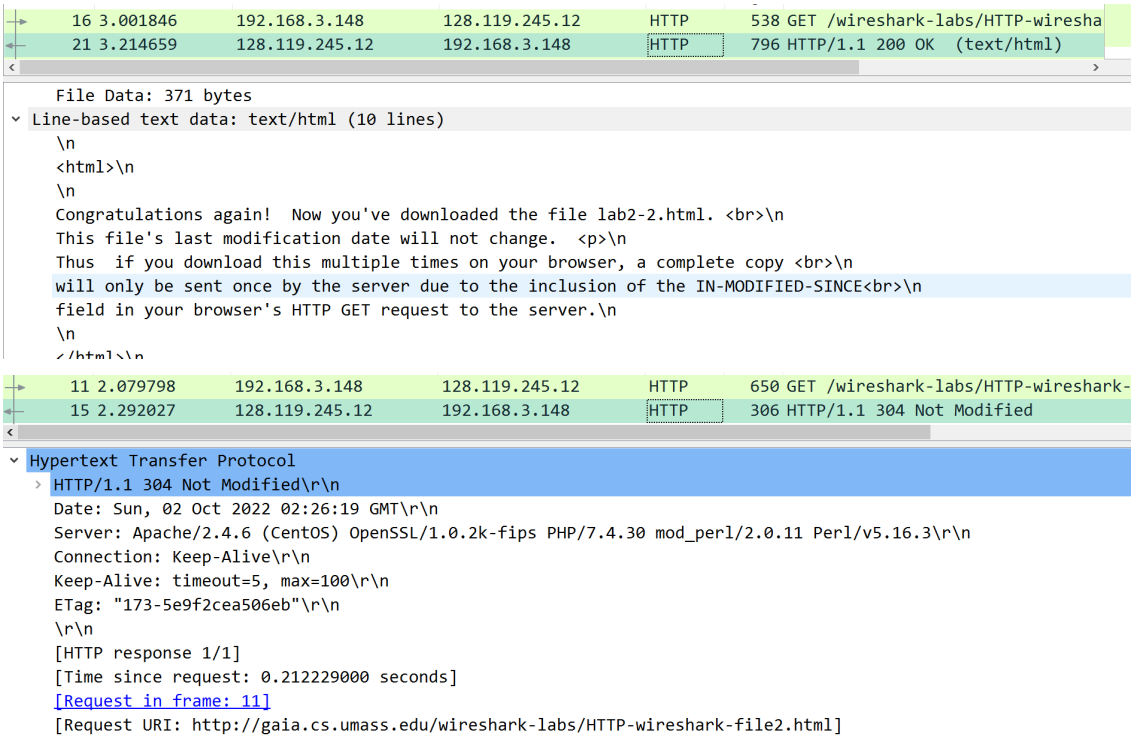
```
    51 4.722054      192.168.3.148         202.120.224.114       HTTP      906 POST /_web/search/doSearch.do?lo
> Frame 51: 906 bytes on wire (7248 bits), 906 bytes captured (7248 bits) on interface \Device\NPF_{0136C1D0-4A
> Ethernet II, Src: IntelCor_25:e3:ba (28:16:ad:25:e3:ba), Dst: HuaweiDe_db:47:a6 (bc:1a:e4:db:47:a6)
> Internet Protocol Version 4, Src: 192.168.3.148, Dst: 202.120.224.114
> Transmission Control Protocol, Src Port: 51245, Dst Port: 80, Seq: 2, Ack: 1, Len: 840
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "keyword" = "计算机"
```

5. 分析HTTP中GET方法与POST方法有哪些区别

   - get方法会把数据都放在头部url里而post会放在请求体中，因为get方法数据都暴露在url中因此post方法比get更加安全
   - get是从服务器上获取数据，post是向服务器传送数据
   - get方法在浏览器回退时是无害的而post会再次提交表单
   - get方法产生的url可以被bookmark，post不会
   - get方法会被浏览器主动cache，post不会除非手动设置
   - get方法只能进行url编码，post支持多种编码
   - get方法参数会完整保留在历史记录里而post中的参数不会
   - get方法在url中传颂的参数是有长度限制的，post没有对参数的数据类型get只接受ASCII字符，post不是
   - get安全性非常低，post安全性较高。

- 由于get方法会把请求头和数据一并发送服务器响应200只会产生一个tcp包，而post会先发送一个请求头服务器响应100continue之后再发送数据服务器响应200因此会产生两个tcp包

6. 访问`http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html`，之后，再次访问改地址，观察分析两次请求以及应答的区别

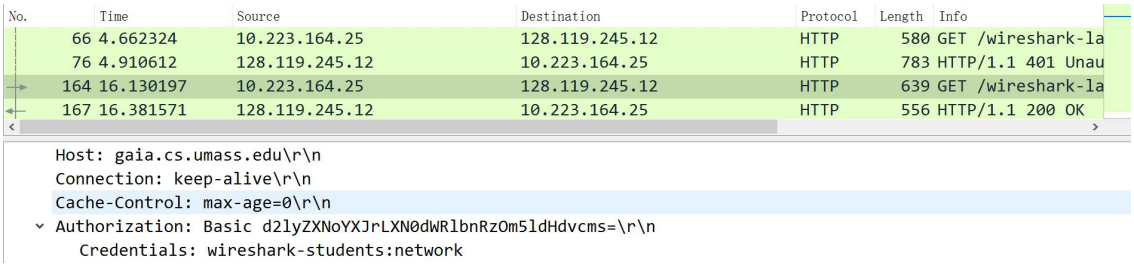



第一次请求的时候返回的是这个网页的详细信息，给出了这个网页的HTML代码，但是第二次访问的时候只是返回了304Not Modified 表示该网页没有变化，直接从缓存中读取数据不用想远端服务器请求完整数据

7. 结合这两次请求与应答，分析HTTP 条件GET的工作方式

用户先访问代理服务器，如果代理服务器中有这个数据的缓存，那么就向服务器发送给一个请求得到该数据最后一次被更改的时间。如果更改的时间在缓存的时间之后则让服务器传回完整数据，否则直接将缓存过的数据返回给客户。如果没有这个数据的缓存则让服务器传回完整数据给客户。降低了客户端的请求相应时间也减少了一个机构内部网络与Internet接入链路上的流量

8. 通过wireshark抓包，找到输入的用户名与密码。（提示：传输使用了base64编码）




9. 将地址中的“http”改为“https”，再次输入用户名与密码，比较两次通信的区别，改为”https”后，还能否通过抓包捕获密码

不能了，似乎没有找到哪一个请求是真正需要的请求