Southern University of Science and Technology

Computer Networking Lab Report

Name: 吴培霖 **Student Number:** 11711717

Major: None

Time: 2018/10/8

Introduction:

Assignment 1 Session Hijack: (Try to capture session cookie of pms.sustc.edu.cn (yours or your classmates')

(1) How did you capture the cookie?
(2) How did you set your cookie into target values?
(3) Did you success hijack the session?

Assignment 2 DNS Inspection: (Capture DNS query sent from your computer)

(1) Where did the query send?
(2) What did the query said?
(3) Does the server support recursive query?
(4) What did the response said?

Procedure:

Assignment 1 Session Hijack:

(1) How did you capture the cookie?

First, open the Wireshark, select WiFi to monitor. (fig.1)

Second, input the string "http.host == "pms.sustc.edu.cn"" into the filter. (fig.2)

Third, open IE Explorer, login in the web page. Finally, we can get cookie from the Wireshark. (fig.3,4)

(2) How did you set your cookie into target values?

First, open chrome, open the web page: http://pms.sustc.edu.cn/

Second, open the extension EditThisCookie, add a new cookie which name is

SessionID, and the value of it is the SessionID we get from fig.4 : SessionID=636745953135231536, Logined=1 then click submit. (fig.5,6,7)

(3) Did you success hijack the session?

Yes, we can use this account to print file or inquiry the usage log. (fig.8)

Assignment 2 DNS Inspection:

(5) Where did the query send?

First, open the Wireshark, set the udp port 53, select WiFi.(fig.9)

Second, select the certain item such that the item showed in the fig.10.

The query send to destination **172.18.1.92** probably our university's DNS server.

(6) What did the query said?

The query said "www.baidu.com: type A, class IN" (fig.11). Probably the host want to get the IP address corresponding to the domain name www.baidu.com.

(7) Does the server support recursive query?

Yes, the fig.12 shows that the server return the response "Server can do recursive queries".

(8) What did the response said?

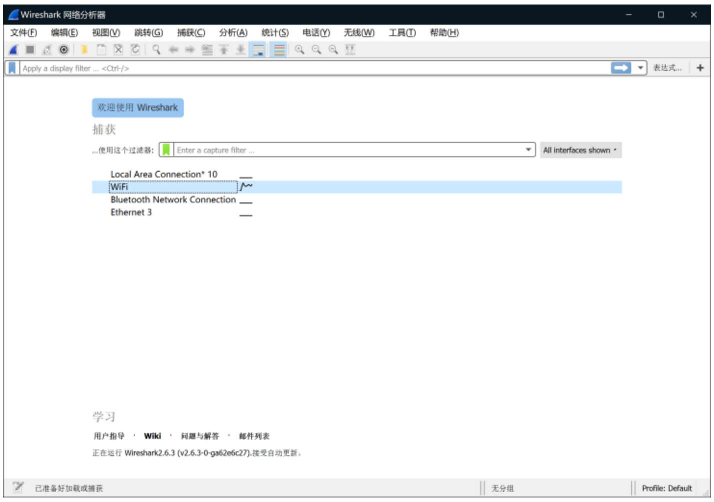
It gives answers: (showed in fig.13)

```
www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
    Name: www.baidu.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 146
    Data length: 15
    CNAME: www.a.shifen.com
www.a.shifen.com: type A, class IN, addr 119.75.213.61
    Name: www.a.shifen.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 146
    Data length: 4
    Address: 119.75.213.61
```

The address 119.75.213.61 is the IP address of the domain www.baidu.com.

Result:

Assignment 1:



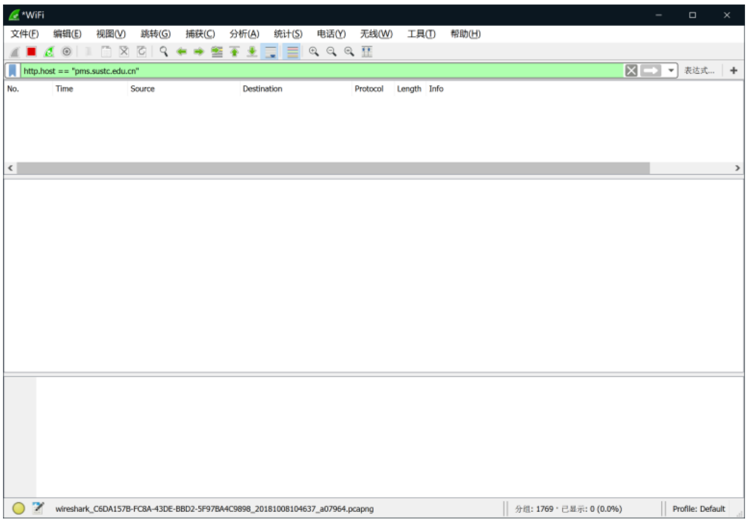
Wireshark 网络分析器
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...
欢迎使用 Wireshark
捕获
...使用这个过滤器:
Enter a capture filter ...
All interfaces shown
学习
用户指导 · Wiki · 问题与解答 · 邮件列表

Local Area Connection* 10
WiFi
Bluetooth Network Connection
Ethernet 3

正在运行 Wireshark2.6.3 (v2.6.3-0-ga62e6c27).接受自动更新。

已准备好加载或捕获 | 无分组 | Profile: Default

(fig.1 Open Wireshark, choose WiFi)

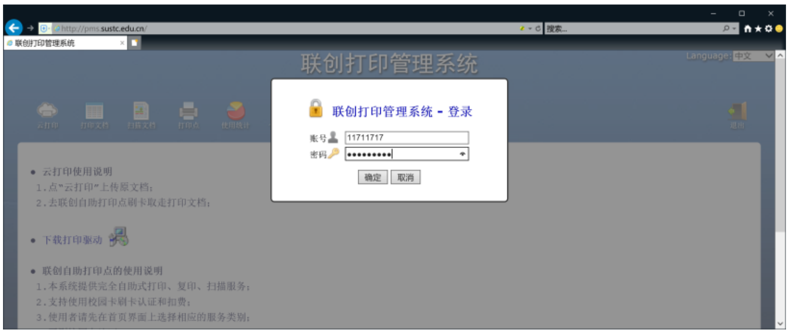


*WiFi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式...
No. Time Source Destination Protocol Length Info

http.host == "pms.sustc.edu.cn"

wireshark_C6DA157B-FC8A-43DE-BBD2-5F97BA4C9898_20181008104637_a07964.pcapng | 分组: 1769 · 已显示: 0 (0.0%) | Profile: Default

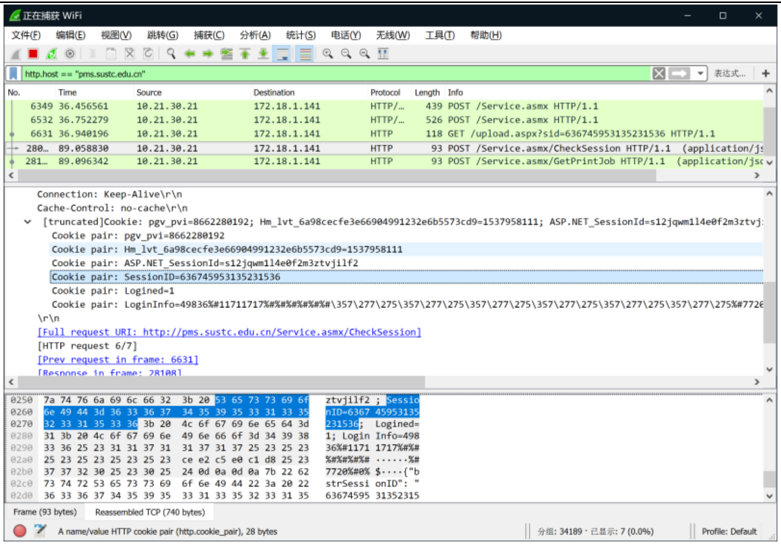
(fig.2 use filter to filt the information)



账号 11711717
密码 ••••••••••

- 云打印使用说明
  1.点"云打印"上传原文档;
  2.去联创自助打印点刷卡取走打印文档;
- 下载打印驱动
- 联创自助打印点的使用说明
  1.本系统提供完全自助式打印、复印、扫描服务;
  2.支持使用校园卡刷卡认证和扣费;
  3.使用者请先在首页界面上选择相应的服务类别;

(fig.3 use IE Explorer to login the pms.sustc.edu.cn)


正在捕获 WiFi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

http.host == "pms.sustc.edu.cn"

```
No.    Time       Source        Destination   Protocol Length Info
  6349 36.456561  10.21.30.21   172.18.1.141  HTTP/…    439 POST /Service.asmx HTTP/1.1
  6532 36.752279  10.21.30.21   172.18.1.141  HTTP/…    526 POST /Service.asmx HTTP/1.1
  6631 36.940196  10.21.30.21   172.18.1.141  HTTP      118 GET /upload.aspx?sid=636745953135231536 HTTP/1.1
 280…  89.058830  10.21.30.21   172.18.1.141  HTTP       93 POST /Service.asmx/CheckSession HTTP/1.1  (application/js
 281…  89.096342  10.21.30.21   172.18.1.141  HTTP       93 POST /Service.asmx/GetPrintJob HTTP/1.1  (application/jsc
```

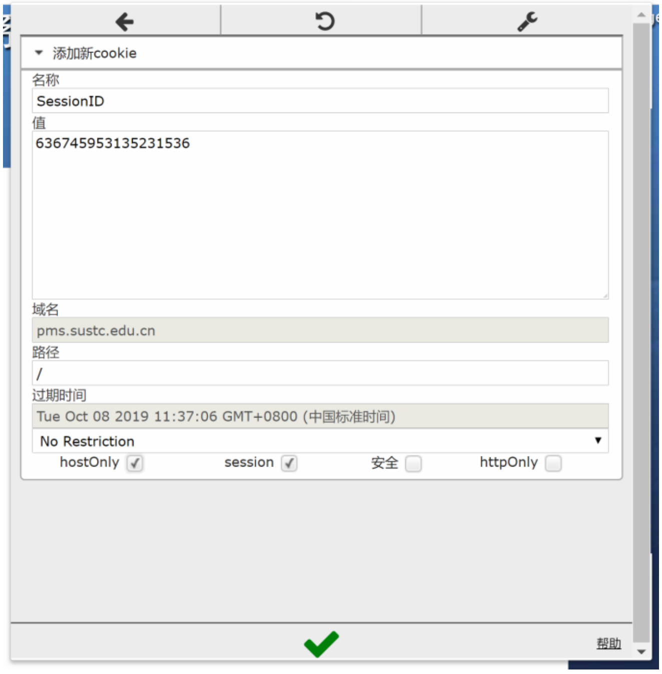
```
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
  [truncated]Cookie: pgv_pvi=8662280192; Hm_lvt_6a98cecfe3e66904991232e6b5573cd9=1537958111; ASP.NET_SessionId=s12jqwm1l4e0f2m3ztvj:
      Cookie pair: pgv_pvi=8662280192
      Cookie pair: Hm_lvt_6a98cecfe3e66904991232e6b5573cd9=1537958111
      Cookie pair: ASP.NET_SessionId=s12jqwm1l4e0f2m3ztvjilf2
      Cookie pair: SessionID=636745953135231536
      Cookie pair: Logined=1
      Cookie pair: LoginInfo=49836%#11711717%#%#%#%#%#%#\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275%#7726
    \r\n
    [Full request URI: http://pms.sustc.edu.cn/Service.asmx/CheckSession]
    [HTTP request 6/7]
    [Prev request in frame: 6631]
    [Response in frame: 28108]
```

```
0250  7a 74 76 6a 69 6c 66 32  3b 20 53 65 73 73 69 6f   ztvjilf2 ; Sessio
0260  6e 49 44 3d 36 33 36 37  34 35 39 35 33 31 33 35   nID=6367 45953135
0270  32 33 31 35 33 36 3b 20  4c 6f 67 69 6e 65 64 3d   231536;  Logined=
0280  31 3b 20 4c 6f 67 69 6e  49 6e 66 6f 3d 34 39 38   1; Login Info=498
0290  33 36 25 23 31 31 37 31  31 37 31 37 25 23 25 23   36%#1171 1717%#%#
02a0  25 23 25 23 25 23 25 23  ce e2 c5 e0 c1 d8 25 23   %#%#%#%# ······%#
02b0  37 37 32 30 25 23 30 25  24 0d 0a 0d 0a 7b 22 62   7720%#0% $····{"b
02c0  73 74 72 53 65 73 73 69  6f 6e 49 44 22 3a 20 22   strSessi onID": "
02d0  36 33 36 37 34 35 39 35  33 31 33 35 32 33 31 35   63674595 31352315
```

Frame (93 bytes) Reassembled TCP (740 bytes)

A name/value HTTP cookie pair (http.cookie_pair), 28 bytes 分组: 34189 · 已显示: 7 (0.0%) Profile: Default

(fig.4 use WireShark to catch the cookie)



名称
SessionID

值
636745953135231536

域名
pms.sustc.edu.cn

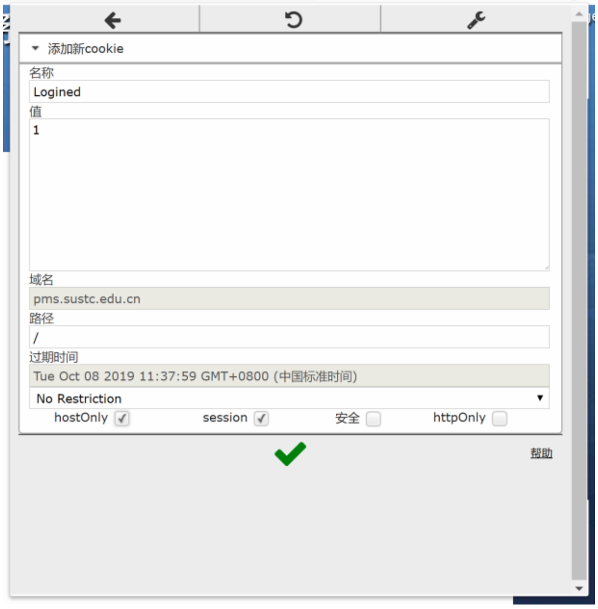
路径
/

过期时间
Tue Oct 08 2019 11:37:06 GMT+0800 (中国标准时间)

No Restriction ▾

hostOnly ☑ session ☑ 安全 ☐ httpOnly ☐

(fig.5 input SessionID cookie via EditThisCookie)


▾ 添加新cookie

名称
Logined

值
1

域名
pms.sustc.edu.cn

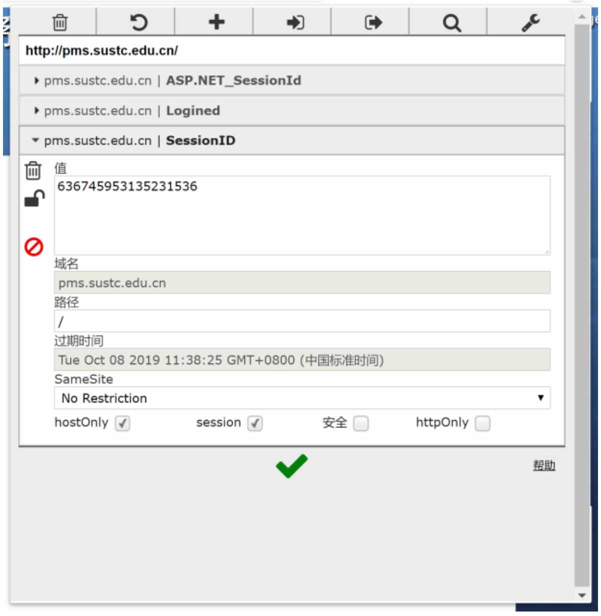
路径
/

过期时间
Tue Oct 08 2019 11:37:59 GMT+0800 (中国标准时间)

No Restriction ▾

hostOnly ☑ session ☑ 安全 □ httpOnly □

(fig.6 input Logined cookie via EditThisCookie)


http://pms.sustc.edu.cn/

▸ pms.sustc.edu.cn | **ASP.NET_SessionId**

▸ pms.sustc.edu.cn | **Logined**

▾ pms.sustc.edu.cn | **SessionID**

值
636745953135231536

域名
pms.sustc.edu.cn

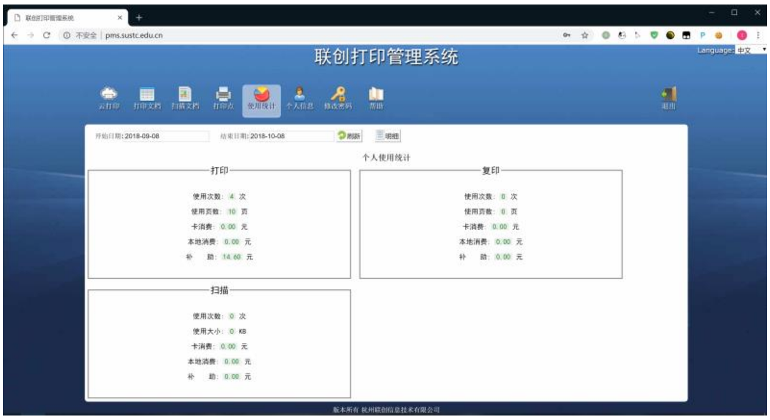
路径
/

过期时间
Tue Oct 08 2019 11:38:25 GMT+0800 (中国标准时间)

SameSite
No Restriction ▾

hostOnly ☑ session ☑ 安全 □ httpOnly □

(fig.7 click submit)



联创打印管理系统

开始日期: 2018-09-08 结束日期: 2018-10-08

个人使用统计

打印

使用次数: 4 次
使用页数: 10 页
卡消费: 0.00 元
本地消费: 0.00 元
补 助: 14.60 元

复印

使用次数: 0 次
使用页数: 0 页
卡消费: 0.00 元
本地消费: 0.00 元
补 助: 0.00 元

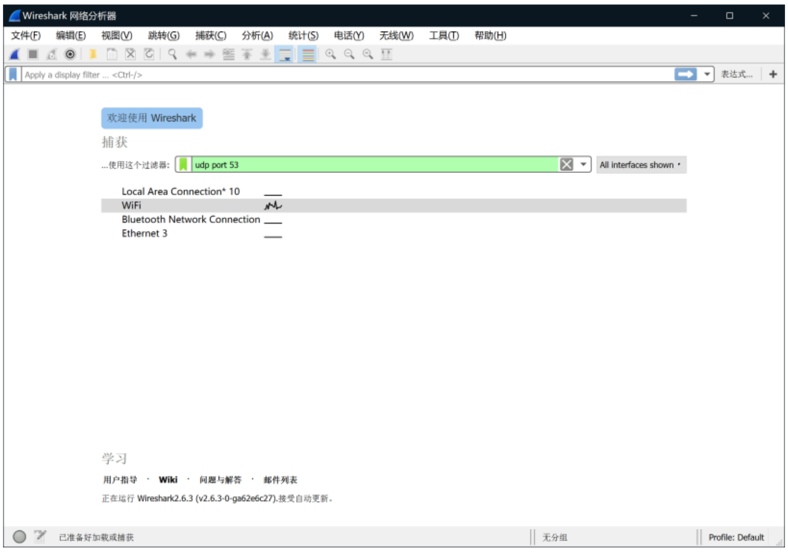
扫描

使用次数: 0 次
使用大小: 0 KB
卡消费: 0.00 元
本地消费: 0.00 元
补 助: 0.00 元

版本所有 杭州联创信息技术有限公司

(fig.8 use the account to do something)

Assignment 2:


Wireshark 网络分析器
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter … <Ctrl-/>
表达式…
欢迎使用 Wireshark
捕获
学习
用户指导 · Wiki · 问题与解答 · 邮件列表

…使用这个过滤器: udp port 53

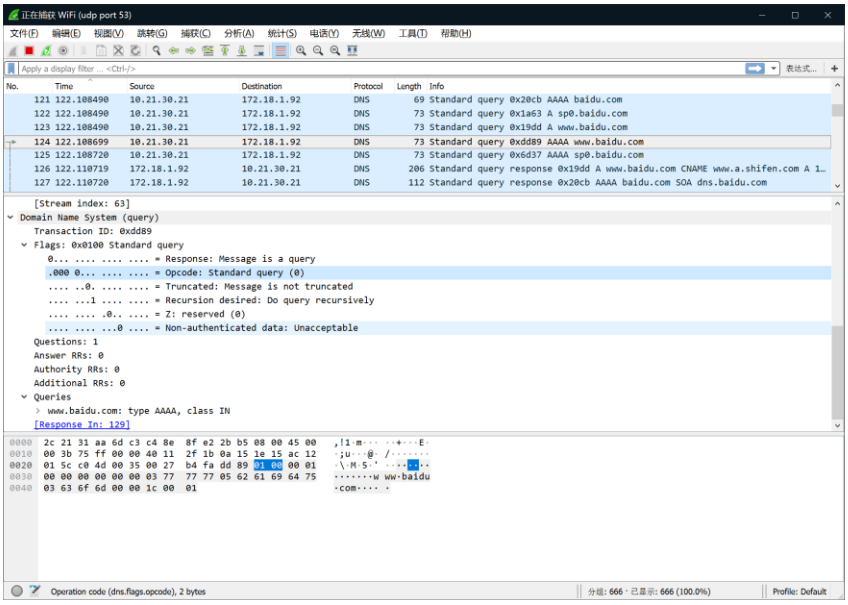
All interfaces shown

Local Area Connection* 10
WiFi
Bluetooth Network Connection
Ethernet 3

正在运行 Wireshark2.6.3 (v2.6.3-0-ga62e6c27).接受自动更新。

已准备好加载或捕获 | 无分组 | Profile: Default

(fig.9 open Wireshark, set udp port 53, select WiFi)


正在捕获 WiFi (udp port 53)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter … <Ctrl-/>
表达式…

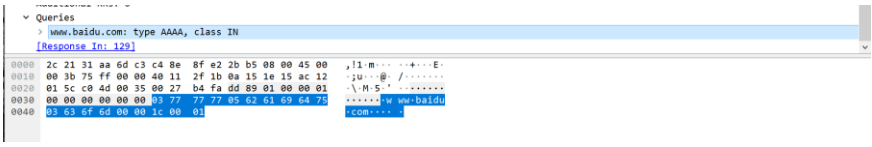
```
No.  Time        Source        Destination   Protocol Length Info
 121 122.108490  10.21.30.21   172.18.1.92   DNS       69 Standard query 0x20cb AAAA baidu.com
 122 122.108490  10.21.30.21   172.18.1.92   DNS       73 Standard query 0x1a63 A sp0.baidu.com
 123 122.108490  10.21.30.21   172.18.1.92   DNS       73 Standard query 0x19dd A www.baidu.com
 124 122.108699  10.21.30.21   172.18.1.92   DNS       73 Standard query 0xdd89 AAAA www.baidu.com
 125 122.108720  10.21.30.21   172.18.1.92   DNS       73 Standard query 0x6d37 AAAA sp0.baidu.com
 126 122.110719  172.18.1.92   10.21.30.21   DNS      206 Standard query response 0x19dd A www.baidu.com CNAME www.a.shifen.com A 1…
 127 122.110720  172.18.1.92   10.21.30.21   DNS      112 Standard query response 0x20cb AAAA baidu.com SOA dns.baidu.com
```

```
    [Stream index: 63]
˅ Domain Name System (query)
    Transaction ID: 0xdd89
  ˅ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
    > www.baidu.com: type AAAA, class IN
    [Response In: 129]
```

```
0000  2c 21 31 aa 6d c3 c4 8e  8f e2 2b b5 08 00 45 00   ,!1·m··· ··+···E·
0010  00 3b 75 ff 00 00 40 11  2f 1b 0a 15 1e 15 ac 12   ·;u···@· /·······
0020  01 5c c0 4d 00 35 00 27  b4 fa dd 89 01 00 00 01   ·\·M·5·' ········
0030  00 00 00 00 00 00 03 77  77 77 05 62 61 69 64 75   ·······w ww·baidu
0040  03 63 6f 6d 00 00 1c 00  01                        ·com···· ·
```

Operation code (dns.flags.opcode), 2 bytes | 分组: 666 · 已显示: 666 (100.0%) | Profile: Default

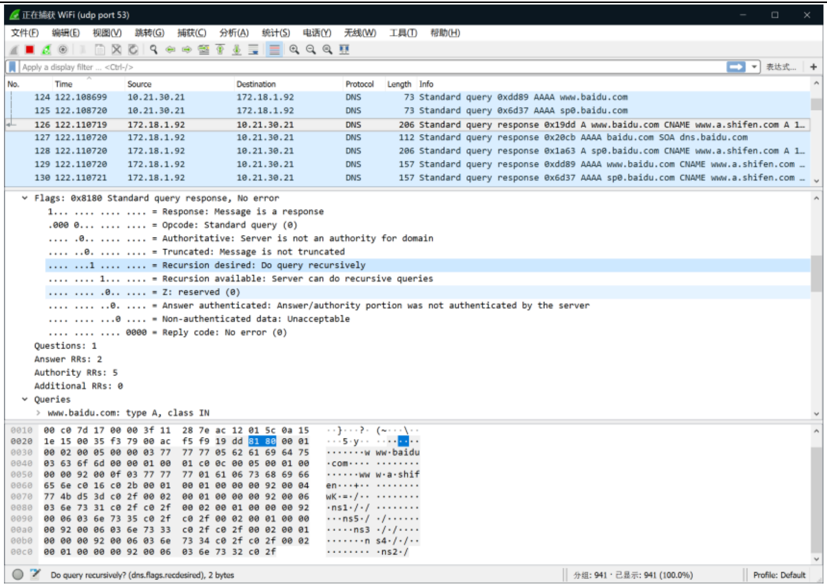
(fig.10 select a item, the information says it is a query)



```
  ˅ Queries
    > www.baidu.com: type AAAA, class IN
    [Response In: 129]
```

```
0000  2c 21 31 aa 6d c3 c4 8e  8f e2 2b b5 08 00 45 00   ,!1·m··· ··+···E·
0010  00 3b 75 ff 00 00 40 11  2f 1b 0a 15 1e 15 ac 12   ·;u···@· /·······
0020  01 5c c0 4d 00 35 00 27  b4 fa dd 89 01 00 00 01   ·\·M·5·' ········
0030  00 00 00 00 00 00 03 77  77 77 05 62 61 69 64 75   ·······w ww·baidu
0040  03 63 6f 6d 00 00 1c 00  01                        ·com···· ·
```

(fig.11 query said it need the IP address of www.baidu.com)


正在捕获 WiFi (udp port 53)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...

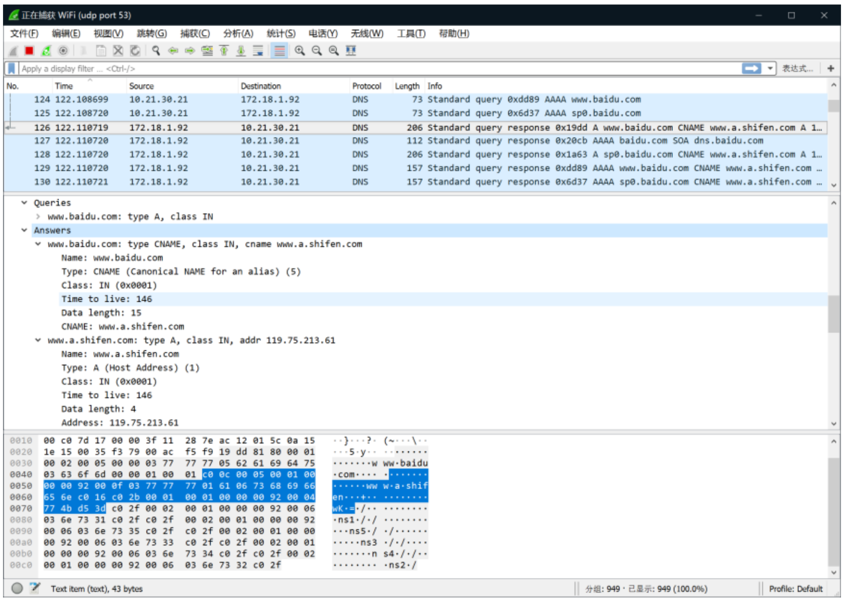
```
No.  Time        Source        Destination   Protocol Length Info
 124 122.108699  10.21.30.21   172.18.1.92   DNS       73 Standard query 0xdd89 AAAA www.baidu.com
 125 122.108720  10.21.30.21   172.18.1.92   DNS       73 Standard query 0x6d37 AAAA sp0.baidu.com
 126 122.110719  172.18.1.92   10.21.30.21   DNS      206 Standard query response 0x19dd A www.baidu.com CNAME www.a.shifen.com A 1…
 127 122.110720  172.18.1.92   10.21.30.21   DNS      112 Standard query response 0x20cb AAAA baidu.com SOA dns.baidu.com
 128 122.110720  172.18.1.92   10.21.30.21   DNS      206 Standard query response 0x1a63 A sp0.baidu.com CNAME www.a.shifen.com A 1…
 129 122.110720  172.18.1.92   10.21.30.21   DNS      157 Standard query response 0xdd89 AAAA www.baidu.com CNAME www.a.shifen.com …
 130 122.110721  172.18.1.92   10.21.30.21   DNS      157 Standard query response 0x6d37 AAAA sp0.baidu.com CNAME www.a.shifen.com …
```

```
  Flags: 0x8180 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .0.. .... .... = Authoritative: Server is not an authority for domain
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive queries
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 2
  Authority RRs: 5
  Additional RRs: 0
  Queries
    > www.baidu.com: type A, class IN
```

```
0010  00 c0 7d 17 00 00 3f 11  28 7e ac 12 01 5c 0a 15   ··}···?· (~···\··
0020  1e 15 00 35 f3 79 00 ac  f5 f9 19 dd 81 80 00 01   ···5·y·· ········
0030  00 02 00 05 00 00 03 77  77 77 05 62 61 69 64 75   ·······w ww·baidu
0040  03 63 6f 6d 00 00 01 00  01 c0 0c 00 05 00 01 00   ·com···· ········
0050  00 00 92 00 0f 03 77 77  77 01 61 06 73 68 69 66   ······ww w·a·shif
0060  65 6e c0 16 c0 2b 00 01  00 01 00 00 00 92 00 04   en···+·· ········
0070  77 4b d5 3d c0 2f 00 02  00 01 00 00 00 92 00 06   wK·=·/·· ········
0080  03 6e 73 31 c0 2f c0 2f  00 02 00 01 00 00 00 92   ·ns1·/·/ ········
0090  00 06 03 6e 73 35 c0 2f  c0 2f 00 02 00 01 00 00   ···ns5·/ ·/······
00a0  00 92 00 06 03 6e 73 33  c0 2f c0 2f 00 02 00 01   ·····ns3 ·/·/····
00b0  00 00 00 92 00 06 03 6e  73 34 c0 2f c0 2f 00 02   ·······n s4·/·/··
00c0  00 01 00 00 00 92 00 06  03 6e 73 32 c0 2f         ········ ·ns2·/
```

Do query recursively? (dns.flags.recdesired), 2 bytes | 分组: 941 · 已显示: 941 (100.0%) | Profile: Default

(fig.12 server responses “Server can do recursive queries”)


正在捕获 WiFi (udp port 53)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Apply a display filter ... <Ctrl-/>
表达式...

```
No.  Time        Source        Destination   Protocol Length Info
 124 122.108699  10.21.30.21   172.18.1.92   DNS       73 Standard query 0xdd89 AAAA www.baidu.com
 125 122.108720  10.21.30.21   172.18.1.92   DNS       73 Standard query 0x6d37 AAAA sp0.baidu.com
 126 122.110719  172.18.1.92   10.21.30.21   DNS      206 Standard query response 0x19dd A www.baidu.com CNAME www.a.shifen.com A 1…
 127 122.110720  172.18.1.92   10.21.30.21   DNS      112 Standard query response 0x20cb AAAA baidu.com SOA dns.baidu.com
 128 122.110720  172.18.1.92   10.21.30.21   DNS      206 Standard query response 0x1a63 A sp0.baidu.com CNAME www.a.shifen.com A 1…
 129 122.110720  172.18.1.92   10.21.30.21   DNS      157 Standard query response 0xdd89 AAAA www.baidu.com CNAME www.a.shifen.com …
 130 122.110721  172.18.1.92   10.21.30.21   DNS      157 Standard query response 0x6d37 AAAA sp0.baidu.com CNAME www.a.shifen.com …
```

```
  Queries
    > www.baidu.com: type A, class IN
  Answers
    www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 146
      Data length: 15
      CNAME: www.a.shifen.com
    www.a.shifen.com: type A, class IN, addr 119.75.213.61
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 146
      Data length: 4
      Address: 119.75.213.61
```

```
0010  00 c0 7d 17 00 00 3f 11  28 7e ac 12 01 5c 0a 15   ··}···?· (~···\··
0020  1e 15 00 35 f3 79 00 ac  f5 f9 19 dd 81 80 00 01   ···5·y·· ········
0030  00 02 00 05 00 00 03 77  77 77 05 62 61 69 64 75   ·······w ww·baidu
0040  03 63 6f 6d 00 00 01 00  01 c0 0c 00 05 00 01 00   ·com···· ········
0050  00 00 92 00 0f 03 77 77  77 01 61 06 73 68 69 66   ······ww w·a·shif
0060  65 6e c0 16 c0 2b 00 01  00 01 00 00 00 92 00 04   en···+·· ········
0070  77 4b d5 3d c0 2f 00 02  00 01 00 00 00 92 00 06   wK·=·/·· ········
0080  03 6e 73 31 c0 2f c0 2f  00 02 00 01 00 00 00 92   ·ns1·/·/ ········
0090  00 06 03 6e 73 35 c0 2f  c0 2f 00 02 00 01 00 00   ···ns5·/ ·/······
00a0  00 92 00 06 03 6e 73 33  c0 2f c0 2f 00 02 00 01   ·····ns3 ·/·/····
00b0  00 00 00 92 00 06 03 6e  73 34 c0 2f c0 2f 00 02   ·······n s4·/·/··
00c0  00 01 00 00 00 92 00 06  03 6e 73 32 c0 2f         ········ ·ns2·/
```

Text item (text), 43 bytes | 分组: 949 · 已显示: 949 (100.0%) | Profile: Default

(fig.13 server gives the answer)

Analysis(including answer of question)：

Assignment 1: We need not only the SessionID but also need to set Logined=1 in case the server close this SessionID.

Conclusion and Experience：

After studying the Wireshark and cookie, we can learn how to do a simple hijack and we can prevent the hijack done by others since we can find some ways to prevent it. It is also useful for us to do some tests when we do the socket programing. Also, from the assignment 2, we can learn the principle how the host to get the IP address from the DNS server. It helps us to understand the computer networking well.

Tips：