Wireshark视角下的网络协议及网络特征分析

安天安全研究与应急处理中心

www.antiy.com

智者安天下

前言

1. 议题主要是通过真实案例展开

2. 部分案例源于工作，敏感部分技术细节已做模糊处理，敬请谅解。

3. 主要目的：

快速发现样本运行过程中产生的网络行为

掌握网络协议分析，解决网络故障

利于网络检测特征的提取和回放

识别可能的攻击或恶意活动……

AntiVirus is tough, But Wireshark makes it easy.

智者安天下

提纲

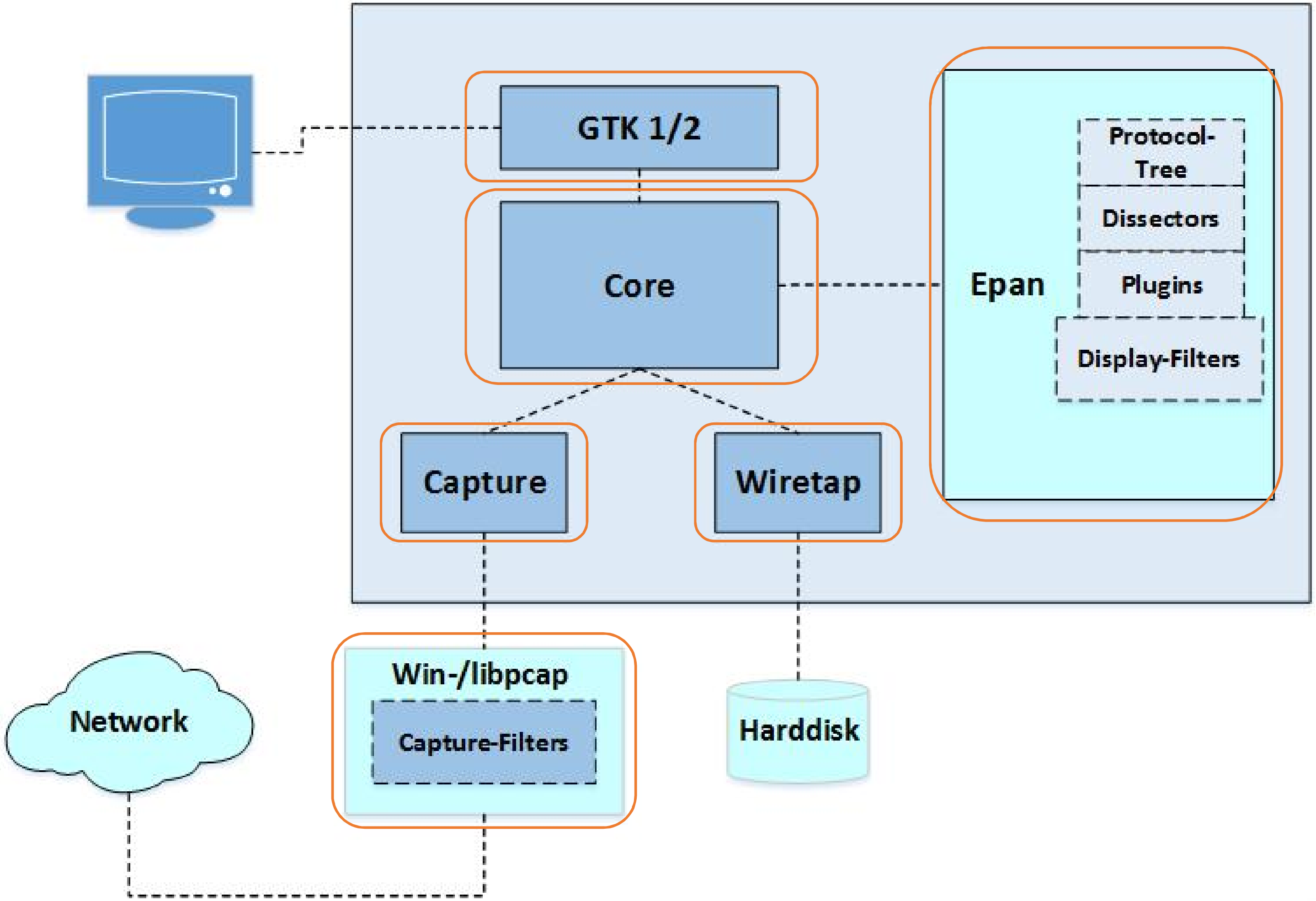
- Wireshark特性
- 网络协议分析
- 网络特征分析
- 案例分享
- 总结

智者安天下

Wireshark特性

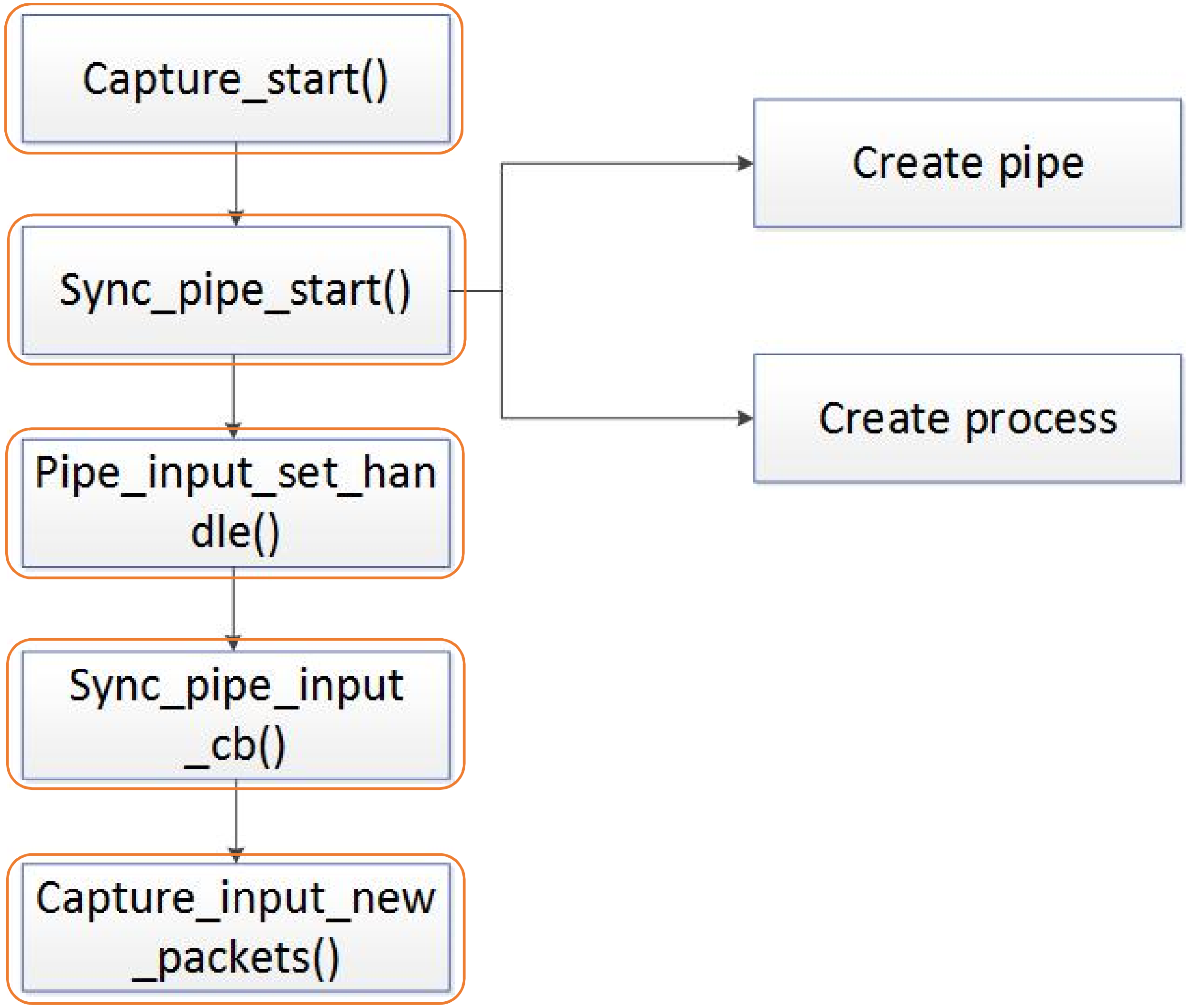
- 系统结构
- 捕获流程
- 解析原理

Wireshark系统结构

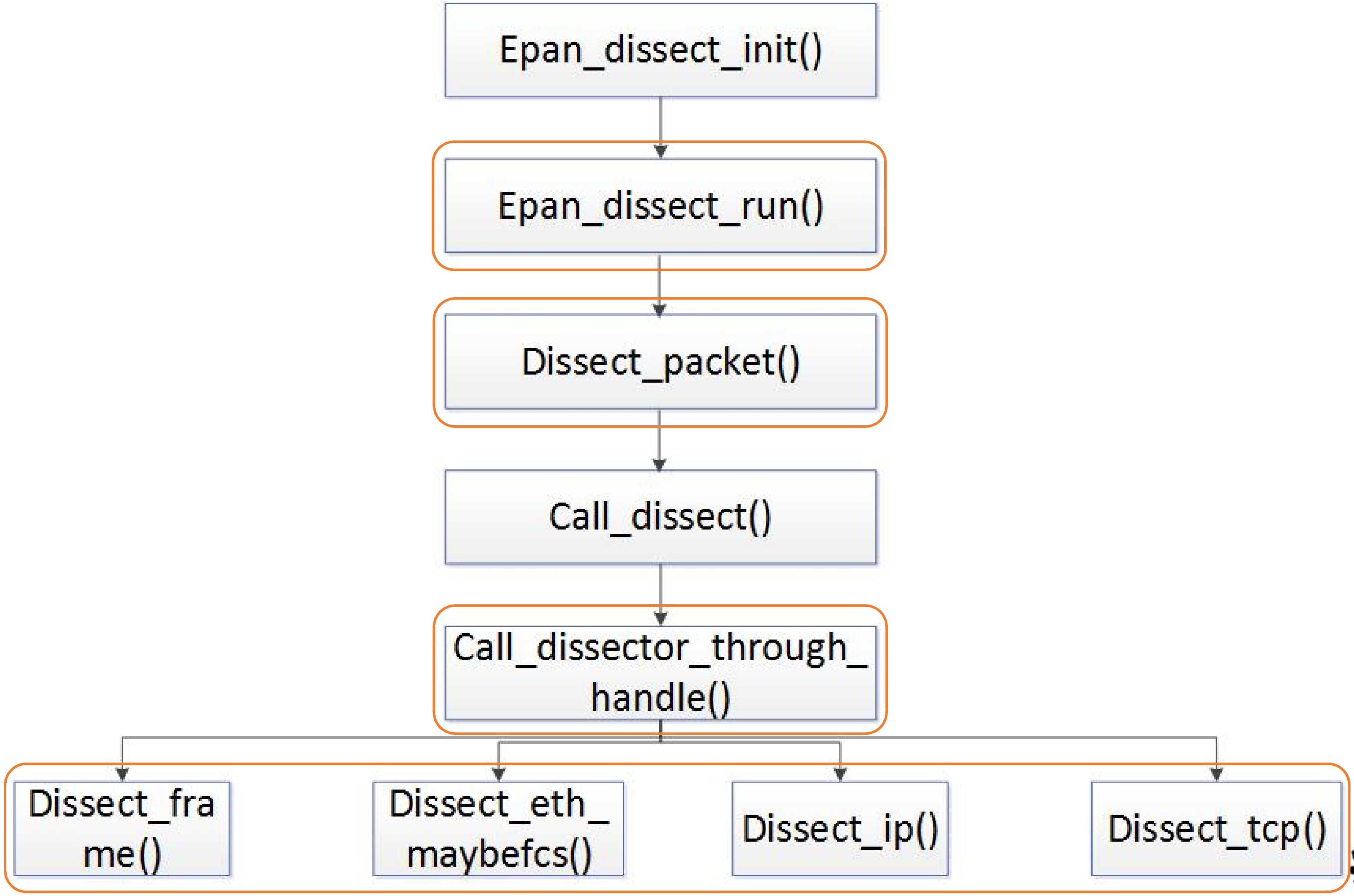


智者安天下

Wireshark数据捕获函数调用流程



Wireshark数据解析函数调用流程



Epan_dissect_init()

Epan_dissect_run()

Dissect_packet()

Call_dissect()

Call_dissector_through_handle()

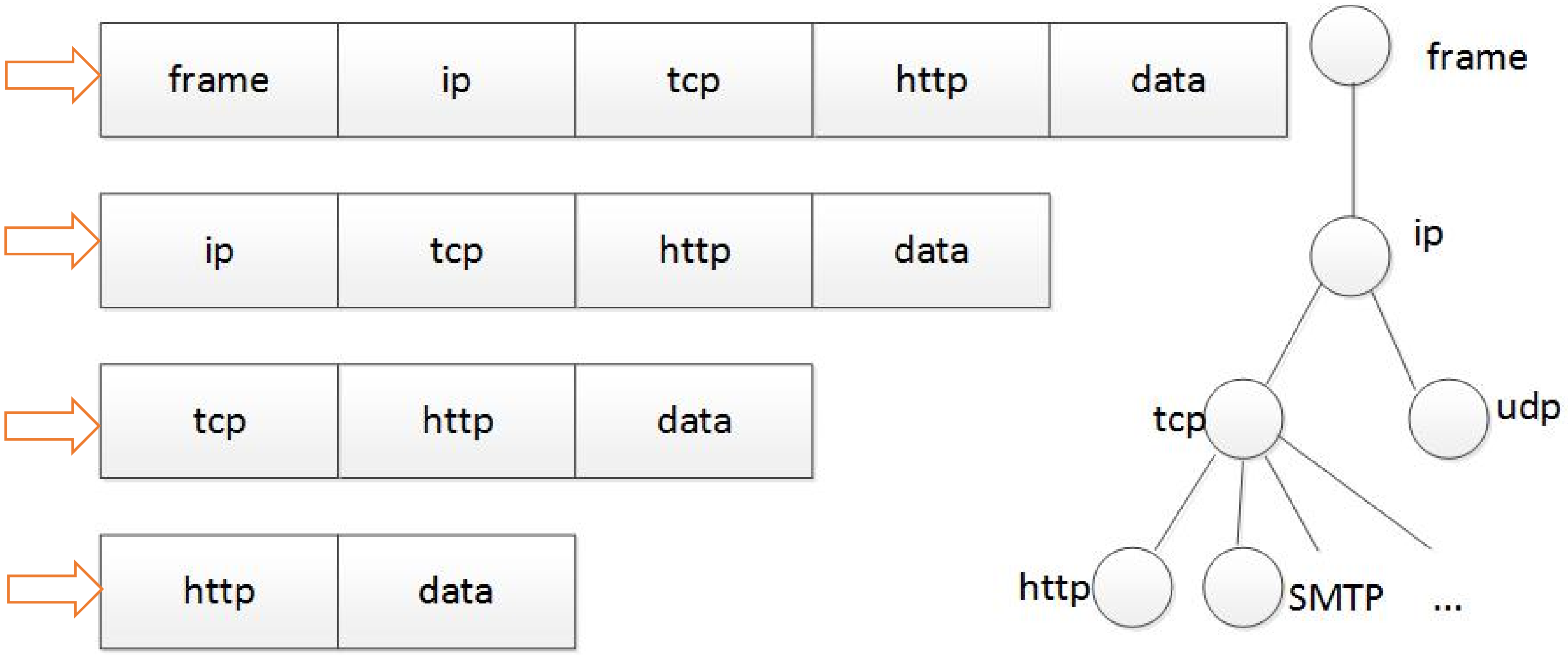
Dissect_frame()

Dissect_eth_maybefcs()

Dissect_ip()

Dissect_tcp()

Wireshark数据包协议解析工作原理



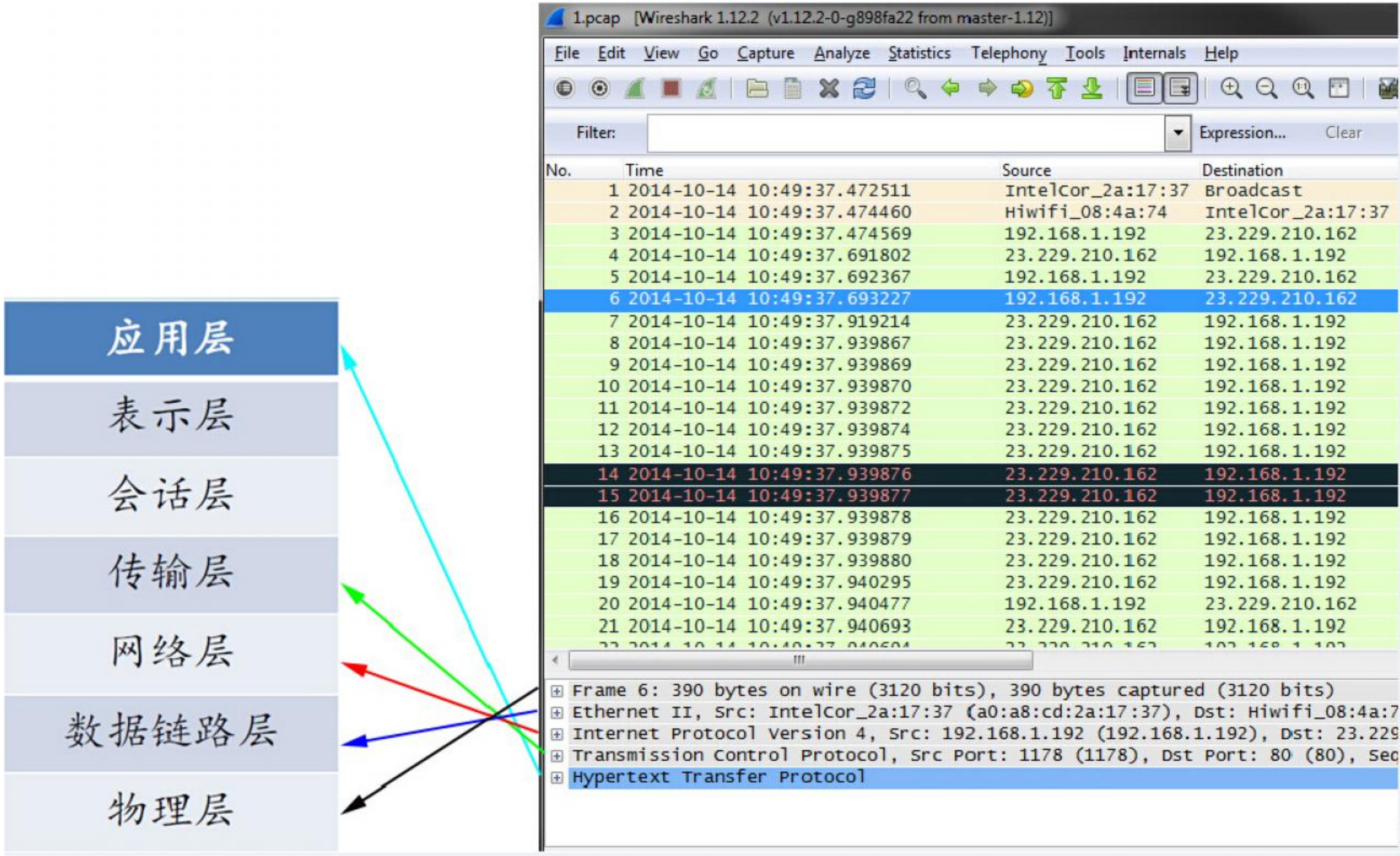
frame | ip | tcp | http | data

ip | tcp | http | data

tcp | http | data

http | data

Wireshark与OSI七层模型



应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

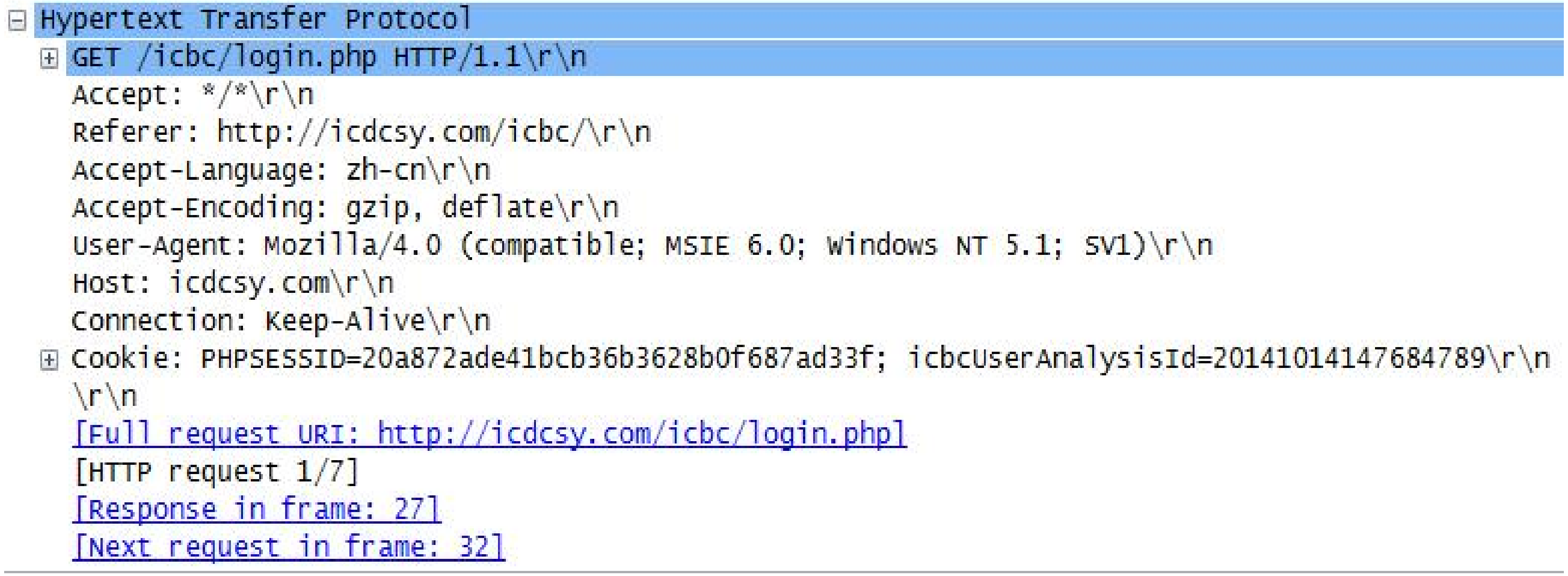
1.pcap [Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear

```
No.  Time                          Source             Destination
   1 2014-10-14 10:49:37.472511    IntelCor_2a:17:37  Broadcast
   2 2014-10-14 10:49:37.474460    Hiwifi_08:4a:74    IntelCor_2a:17:37
   3 2014-10-14 10:49:37.474569    192.168.1.192      23.229.210.162
   4 2014-10-14 10:49:37.691802    23.229.210.162     192.168.1.192
   5 2014-10-14 10:49:37.692367    192.168.1.192      23.229.210.162
   6 2014-10-14 10:49:37.693227    192.168.1.192      23.229.210.162
   7 2014-10-14 10:49:37.919214    23.229.210.162     192.168.1.192
   8 2014-10-14 10:49:37.939867    23.229.210.162     192.168.1.192
   9 2014-10-14 10:49:37.939869    23.229.210.162     192.168.1.192
  10 2014-10-14 10:49:37.939870    23.229.210.162     192.168.1.192
  11 2014-10-14 10:49:37.939872    23.229.210.162     192.168.1.192
  12 2014-10-14 10:49:37.939874    23.229.210.162     192.168.1.192
  13 2014-10-14 10:49:37.939875    23.229.210.162     192.168.1.192
  14 2014-10-14 10:49:37.939876    23.229.210.162     192.168.1.192
  15 2014-10-14 10:49:37.939877    23.229.210.162     192.168.1.192
  16 2014-10-14 10:49:37.939878    23.229.210.162     192.168.1.192
  17 2014-10-14 10:49:37.939879    23.229.210.162     192.168.1.192
  18 2014-10-14 10:49:37.939880    23.229.210.162     192.168.1.192
  19 2014-10-14 10:49:37.940295    23.229.210.162     192.168.1.192
  20 2014-10-14 10:49:37.940477    192.168.1.192      23.229.210.162
  21 2014-10-14 10:49:37.940693    23.229.210.162     192.168.1.192
  22 2014-10-14 10:49:37.940694    23.229.210.162     192.168.1.192
```

```
⊞ Frame 6: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)
⊞ Ethernet II, Src: IntelCor_2a:17:37 (a0:a8:cd:2a:17:37), Dst: Hiwifi_08:4a:7
⊞ Internet Protocol Version 4, Src: 192.168.1.192 (192.168.1.192), Dst: 23.229
⊞ Transmission Control Protocol, Src Port: 1178 (1178), Dst Port: 80 (80), Seq
⊞ Hypertext Transfer Protocol
```

Wireshark视角下的网络分层之应用层

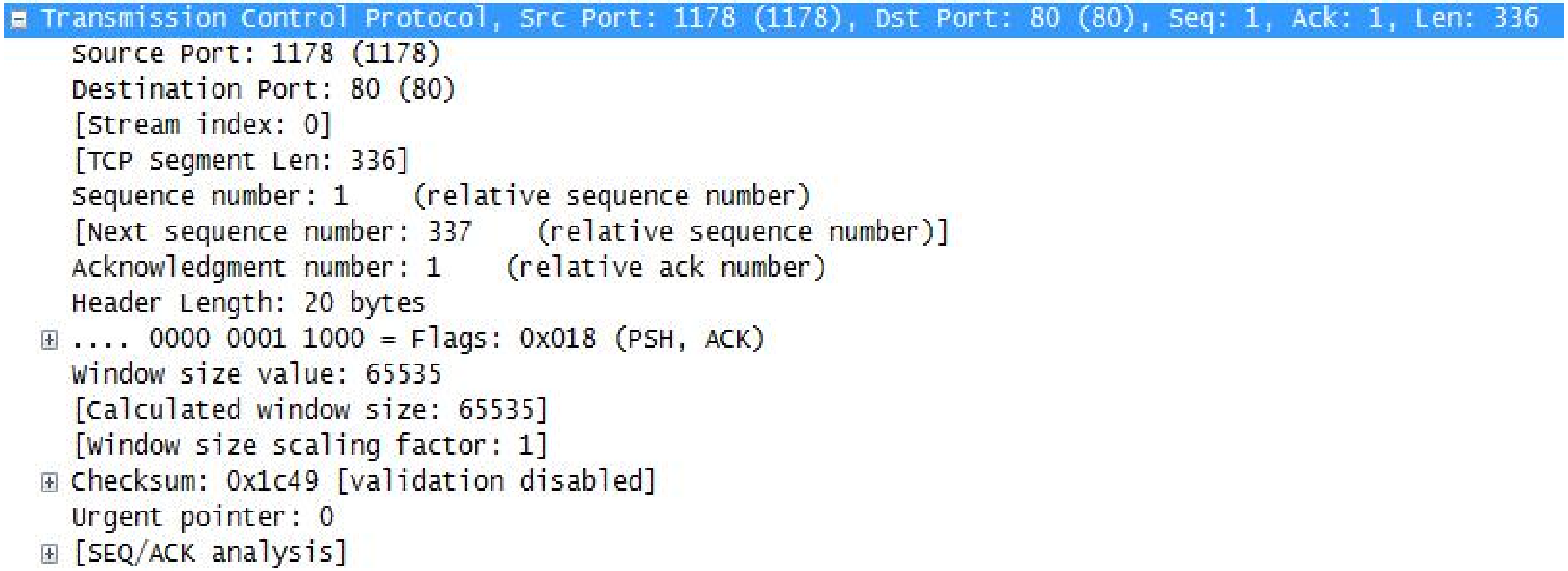


```
⊟ Hypertext Transfer Protocol
  ⊞ GET /icbc/login.php HTTP/1.1\r\n
    Accept: */*\r\n
    Referer: http://icdcsy.com/icbc/\r\n
    Accept-Language: zh-cn\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: icdcsy.com\r\n
    Connection: Keep-Alive\r\n
  ⊞ Cookie: PHPSESSID=20a872ade41bcb36b3628b0f687ad33f; icbcUserAnalysisId=20141014147684789\r\n
    \r\n
    [Full request URI: http://icdcsy.com/icbc/login.php]
    [HTTP request 1/7]
    [Response in frame: 27]
    [Next request in frame: 32]
```

应用层：HTTP是应用层协议，专注与超文本文件的传输，而对数据流传输一无所知。HTTP协议的通信是一次**request-responce**交流。客户端(guest)向服务器发出**请求**(request)，服务器(server)**回复**(response)客户端。

智者安天下

Wireshark视角下的网络分层之传输层

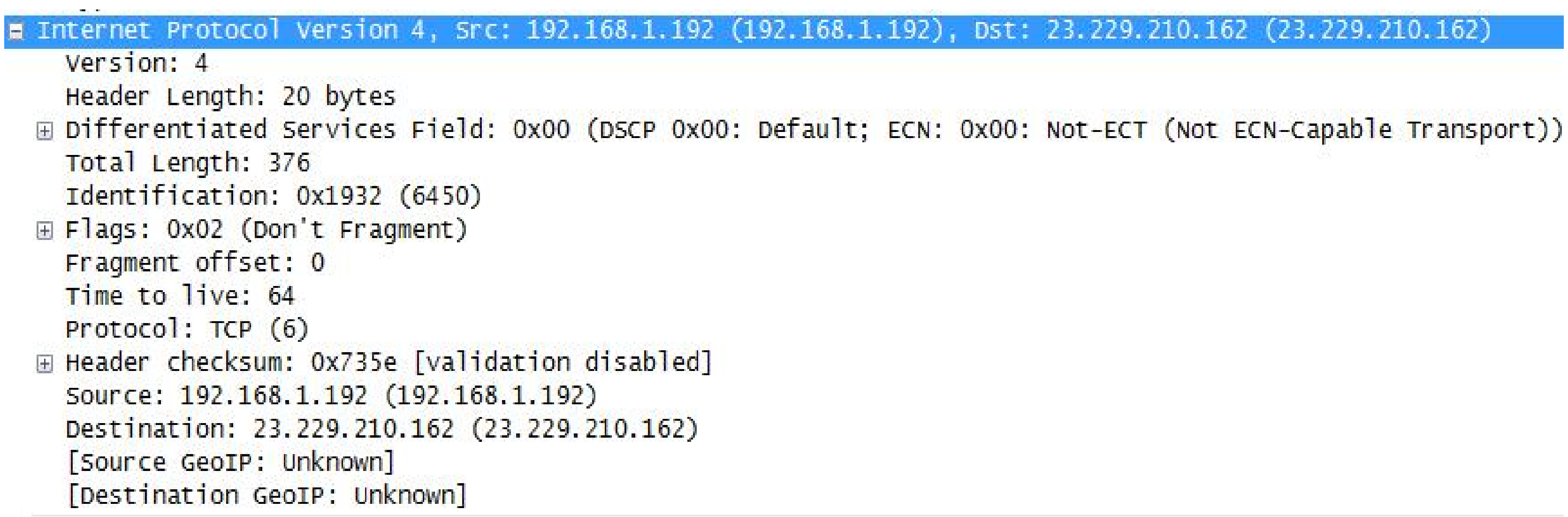


```
⊟ Transmission Control Protocol, Src Port: 1178 (1178), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 336
    Source Port: 1178 (1178)
    Destination Port: 80 (80)
    [Stream index: 0]
    [TCP Segment Len: 336]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 337    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ⊞ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: 1]
  ⊞ Checksum: 0x1c49 [validation disabled]
    Urgent pointer: 0
  ⊞ [SEQ/ACK analysis]
```

传输层：TCP协议，应用层所产生的数据就是通过TCP控制传输的。在Wireshark中，可以发现用于排序、重传、流量控制的Seq号和Ack号等相关信息Tips：虽名为“传输层”，但它并不是把网络包从一个设备传到另一个，而只是**对传输行为进行控制**。真正负责设备间传输的是下面两层。

智者安天下

Wireshark视角下的网络分层之网络层

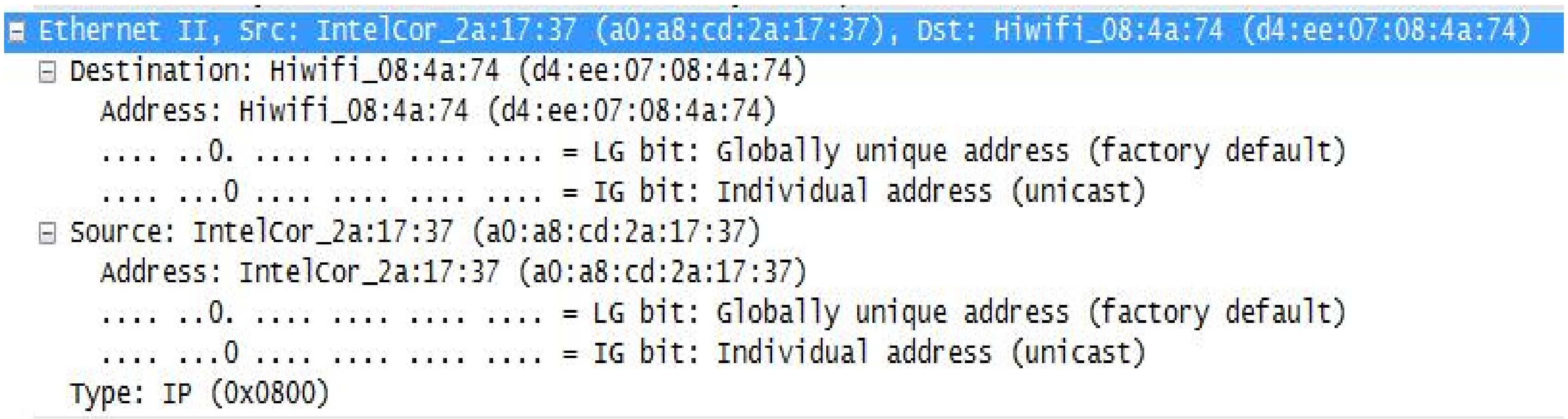


```
⊟ Internet Protocol Version 4, Src: 192.168.1.192 (192.168.1.192), Dst: 23.229.210.162 (23.229.210.162)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 376
    Identification: 0x1932 (6450)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
  ⊞ Header checksum: 0x735e [validation disabled]
    Source: 192.168.1.192 (192.168.1.192)
    Destination: 23.229.210.162 (23.229.210.162)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

网络层：本层的主要任务是将TCP层传下来的数据与目标地址和源地址结合起来。目标地址用于确定接收方，源地址用于确定发送方。

智者安天下

Wireshark视角下的网络分层之数据链路层

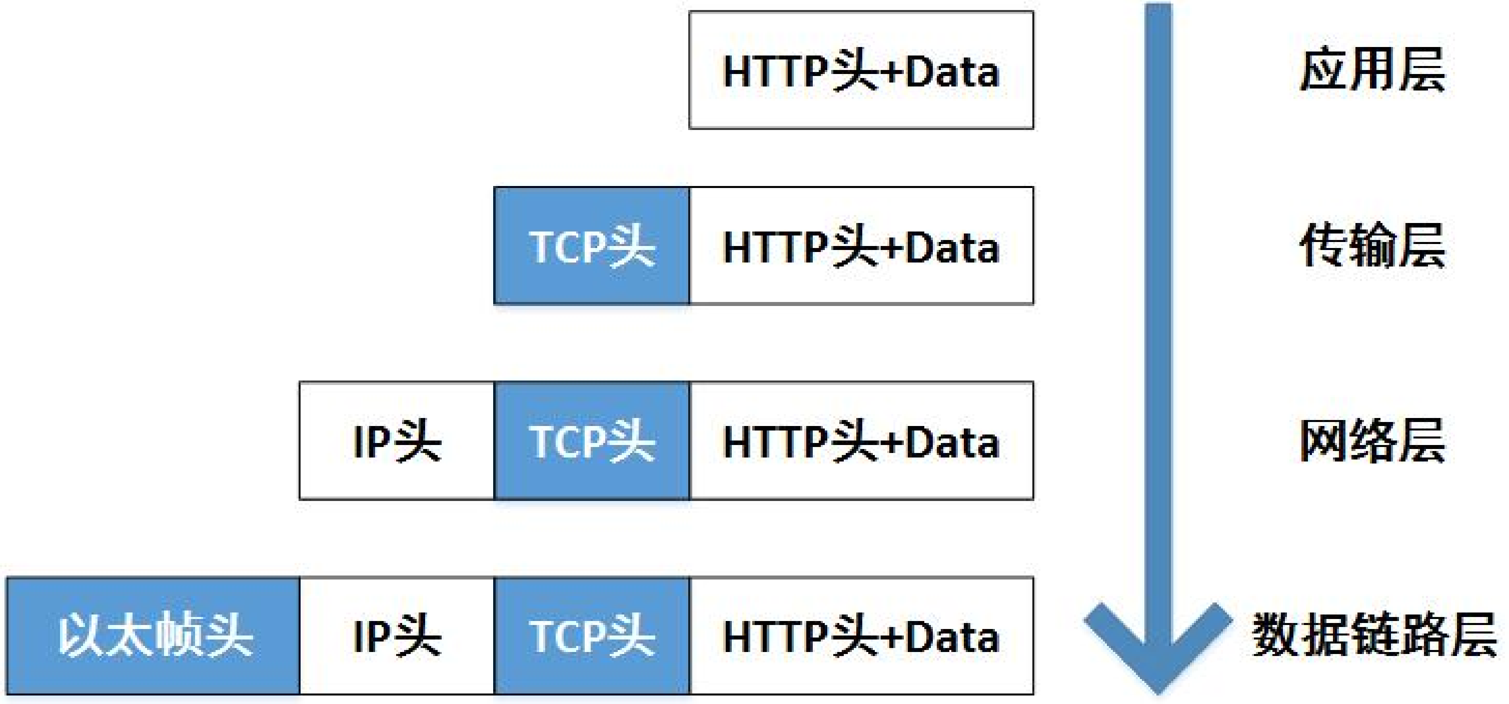


```
⊟ Ethernet II, Src: IntelCor_2a:17:37 (a0:a8:cd:2a:17:37), Dst: Hiwifi_08:4a:74 (d4:ee:07:08:4a:74)
  ⊟ Destination: Hiwifi_08:4a:74 (d4:ee:07:08:4a:74)
      Address: Hiwifi_08:4a:74 (d4:ee:07:08:4a:74)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: IntelCor_2a:17:37 (a0:a8:cd:2a:17:37)
      Address: IntelCor_2a:17:37 (a0:a8:cd:2a:17:37)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
```

数据链路层：即网络接口层，从图中可以看到相邻两个设备的MAC地址，因此该网络包才能以接力的方式送达目标地址。

智者安天下

Wireshark视角下的网络分层之数据重组

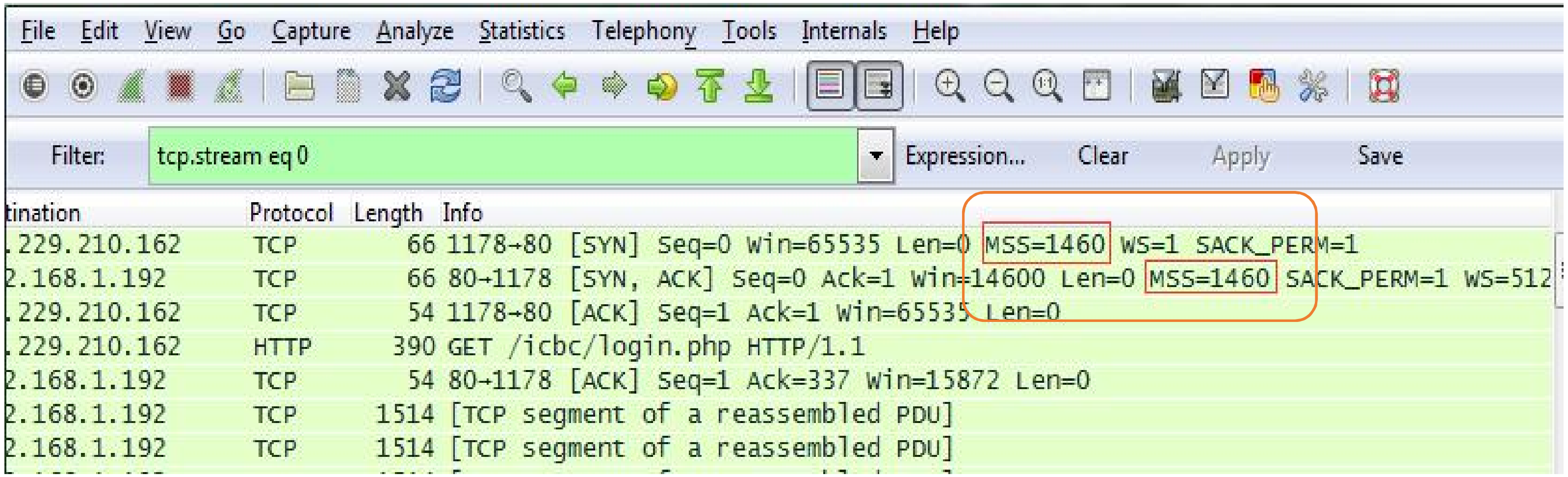


每一层各司其职，分工明确，逐层递进，最终形成一个完整的网络数据包

智者安天下

Q&A

- 如果传输数据比较大，比如8765字节，TCP层该如何处理？是否也是简单的加上TCP头之后交给网络层呢？



Filter: tcp.stream eq 0

```
tination         Protocol  Length  Info
.229.210.162      TCP        66 1178→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 SACK_PERM=1
2.168.1.192       TCP        66 80→1178 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
.229.210.162      TCP        54 1178→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
.229.210.162      HTTP      390 GET /icbc/login.php HTTP/1.1
2.168.1.192       TCP        54 80→1178 [ACK] Seq=1 Ack=337 Win=15872 Len=0
2.168.1.192       TCP      1514 [TCP segment of a reassembled PDU]
2.168.1.192       TCP      1514 [TCP segment of a reassembled PDU]
```

结论：发包的大小取决于MTU较小的一方

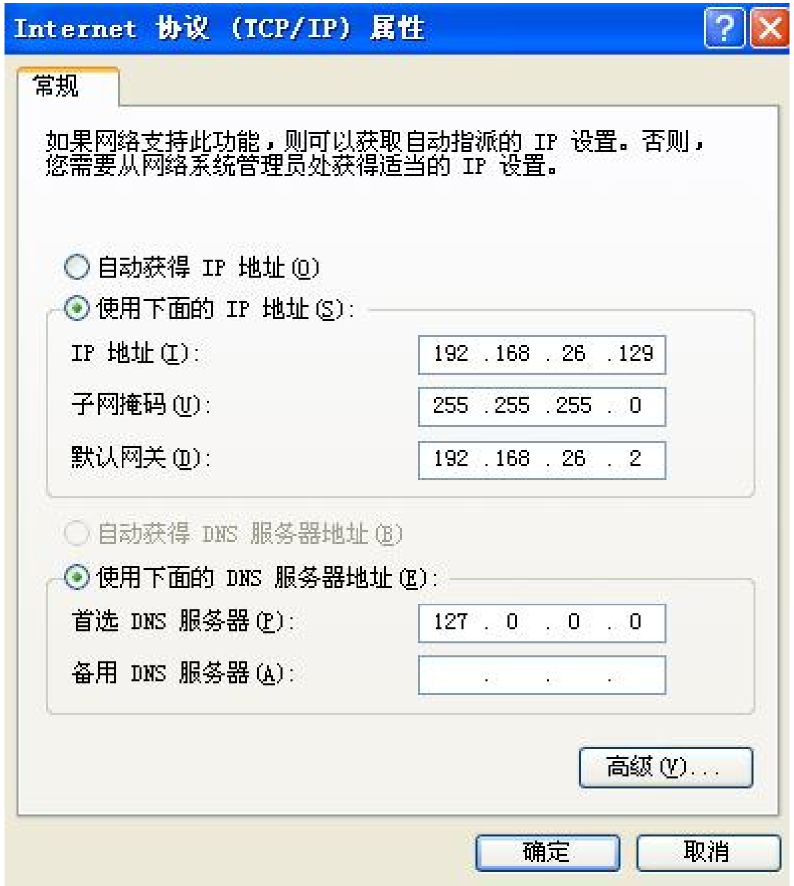
智者安天下

网络协议解析

- TCP
- UDP
- HTTP

Appetizer

主机 A



Internet 协议 (TCP/IP) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

○ 自动获得 IP 地址(O)

● 使用下面的 IP 地址(S):

IP 地址(I): 192 .168 . 26 .129

子网掩码(U): 255 .255 .255 . 0

默认网关(D): 192 .168 . 26 . 2

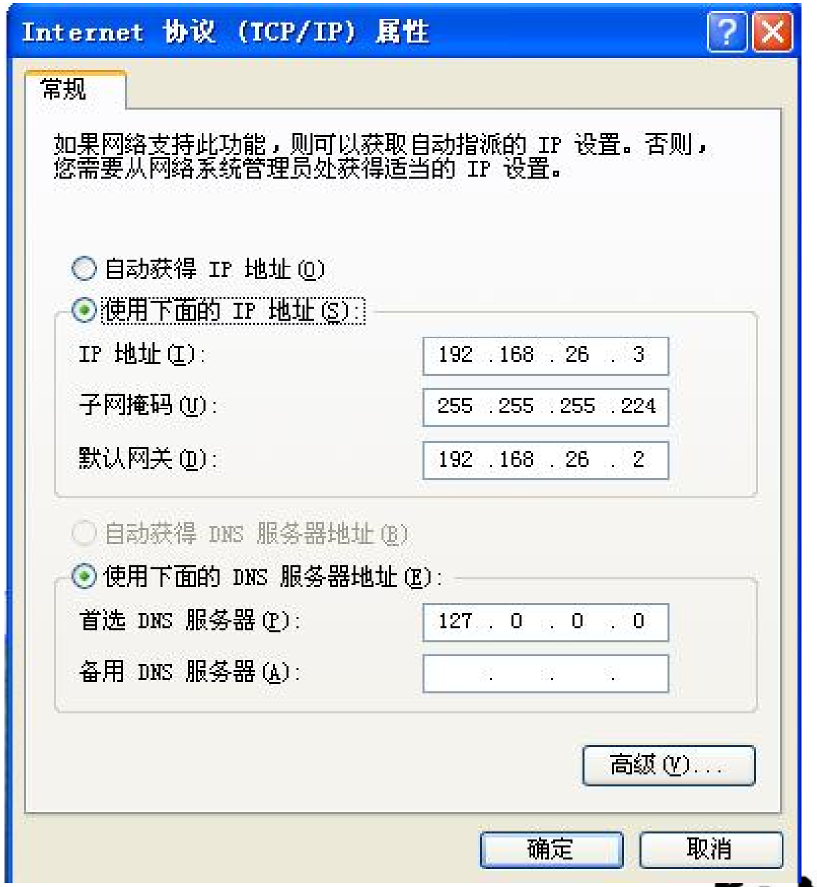
○ 自动获得 DNS 服务器地址(B)

● 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): 127 . 0 . 0 . 0

备用 DNS 服务器(A): . . .

主机 B



Internet 协议 (TCP/IP) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

○ 自动获得 IP 地址(O)

● 使用下面的 IP 地址(S):

IP 地址(I): 192 .168 . 26 . 3

子网掩码(U): 255 .255 .255 .224

默认网关(D): 192 .168 . 26 . 2

○ 自动获得 DNS 服务器地址(B)

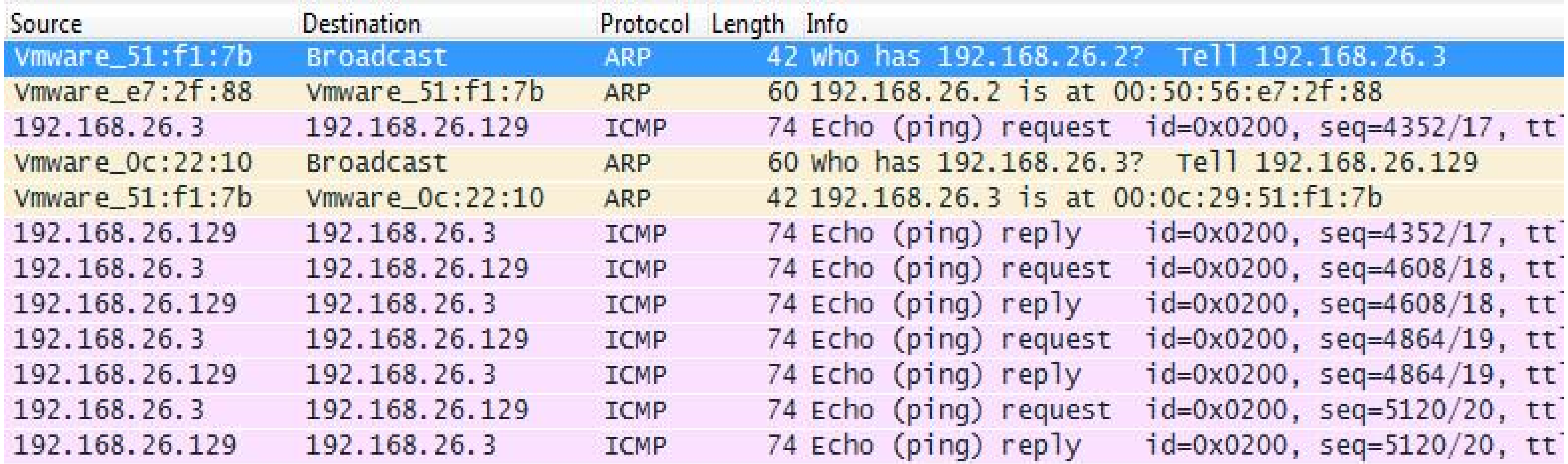
● 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): 127 . 0 . 0 . 0

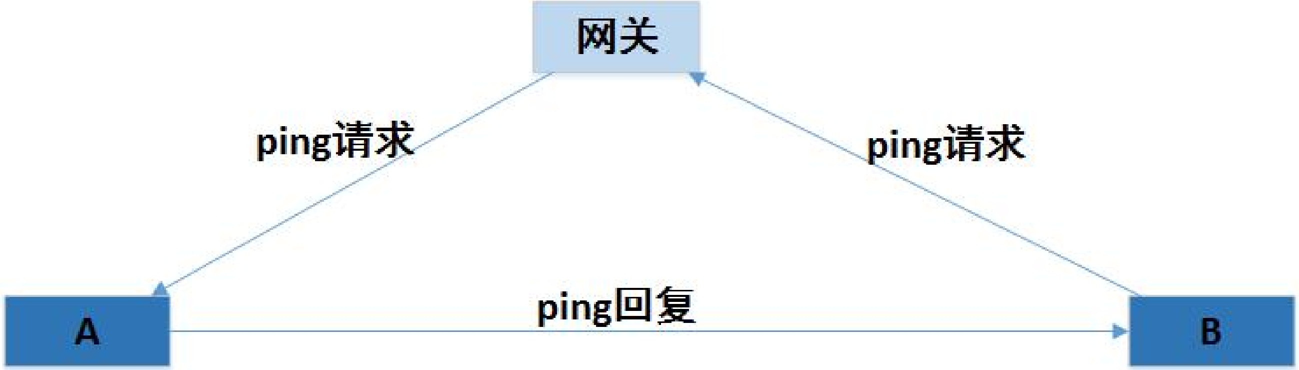
备用 DNS 服务器(A): . . .

智者安天下

通信过程



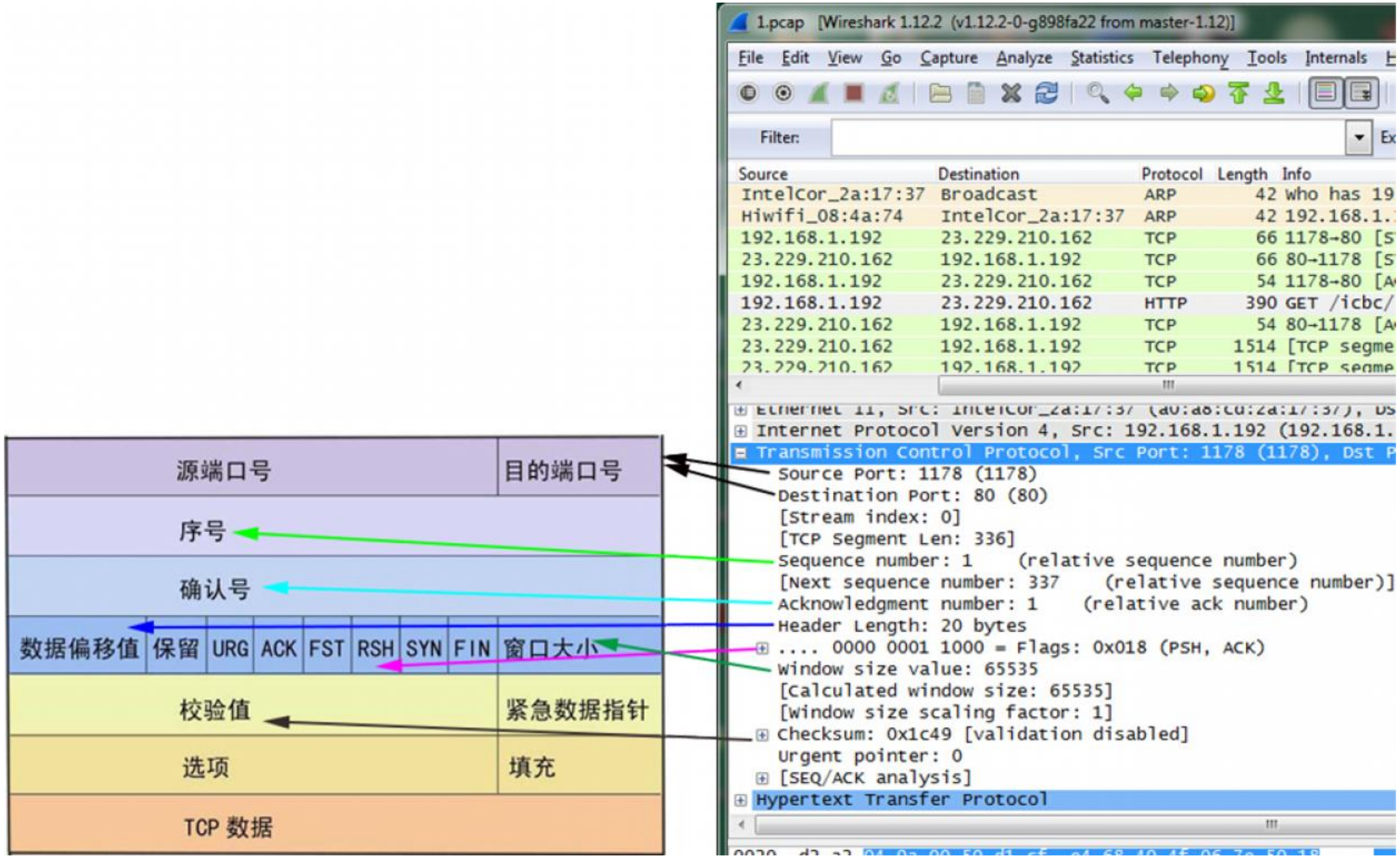
```
Source            Destination       Protocol  Length  Info
Vmware_51:f1:7b   Broadcast         ARP       42 Who has 192.168.26.2?  Tell 192.168.26.3
Vmware_e7:2f:88   Vmware_51:f1:7b   ARP       60 192.168.26.2 is at 00:50:56:e7:2f:88
192.168.26.3      192.168.26.129    ICMP      74 Echo (ping) request  id=0x0200, seq=4352/17, tt
Vmware_0c:22:10   Broadcast         ARP       60 Who has 192.168.26.3?  Tell 192.168.26.129
Vmware_51:f1:7b   Vmware_0c:22:10   ARP       42 192.168.26.3 is at 00:0c:29:51:f1:7b
192.168.26.129    192.168.26.3      ICMP      74 Echo (ping) reply    id=0x0200, seq=4352/17, tt
192.168.26.3      192.168.26.129    ICMP      74 Echo (ping) request  id=0x0200, seq=4608/18, tt
192.168.26.129    192.168.26.3      ICMP      74 Echo (ping) reply    id=0x0200, seq=4608/18, tt
192.168.26.3      192.168.26.129    ICMP      74 Echo (ping) request  id=0x0200, seq=4864/19, tt
192.168.26.129    192.168.26.3      ICMP      74 Echo (ping) reply    id=0x0200, seq=4864/19, tt
192.168.26.3      192.168.26.129    ICMP      74 Echo (ping) request  id=0x0200, seq=5120/20, tt
192.168.26.129    192.168.26.3      ICMP      74 Echo (ping) reply    id=0x0200, seq=5120/20, tt
```



通信过程：主机B先将Ping请求交给默认网关，默认网关再转发给主机A，A收到请求后直接把ping回复给B

智者安天下

Wireshark与TCP报文对应字段



源端口号 | 目的端口号

序号

确认号

数据偏移值 | 保留 | URG | ACK | FST | RSH | SYN | FIN | 窗口大小

校验值 | 紧急数据指针

选项 | 填充

TCP 数据

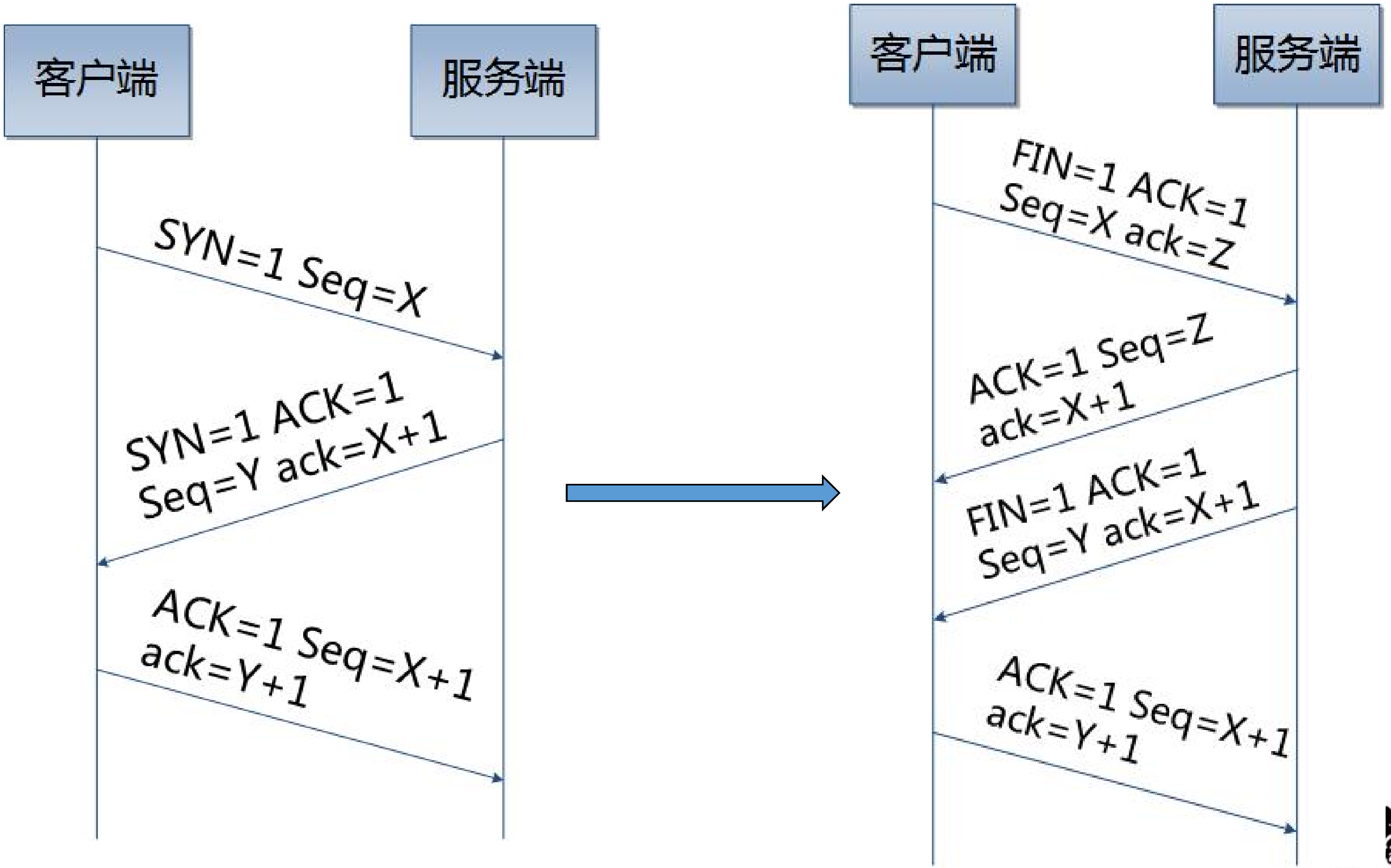
1.pcap [Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)]

```
Source             Destination        Protocol Length Info
IntelCor_2a:17:37  Broadcast          ARP          42 Who has 19
Hiwifi_08:4a:74    IntelCor_2a:17:37  ARP          42 192.168.1.
192.168.1.192      23.229.210.162     TCP          66 1178→80 [S
23.229.210.162     192.168.1.192      TCP          66 80→1178 [S
192.168.1.192      23.229.210.162     TCP          54 1178→80 [A
192.168.1.192      23.229.210.162     HTTP        390 GET /icbc/
23.229.210.162     192.168.1.192      TCP          54 80→1178 [A
23.229.210.162     192.168.1.192      TCP        1514 [TCP segme
23.229.210.162     192.168.1.192      TCP        1514 [TCP segme
```

```
⊞ Ethernet II, Src: IntelCor_2a:17:37 (a0:a8:cd:2a:17:37), Ds
⊞ Internet Protocol Version 4, Src: 192.168.1.192 (192.168.1.
⊟ Transmission Control Protocol, Src Port: 1178 (1178), Dst P
    Source Port: 1178 (1178)
    Destination Port: 80 (80)
    [Stream index: 0]
    [TCP Segment Len: 336]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 337    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ⊞ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: 1]
  ⊞ Checksum: 0x1c49 [validation disabled]
    Urgent pointer: 0
  ⊞ [SEQ/ACK analysis]
⊞ Hypertext Transfer Protocol
```

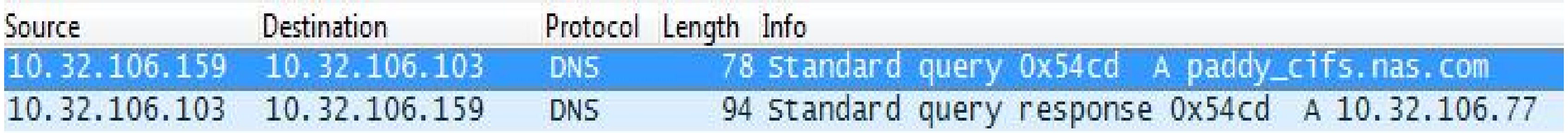
智者安天下

TCP三次握手与四次挥手示意图



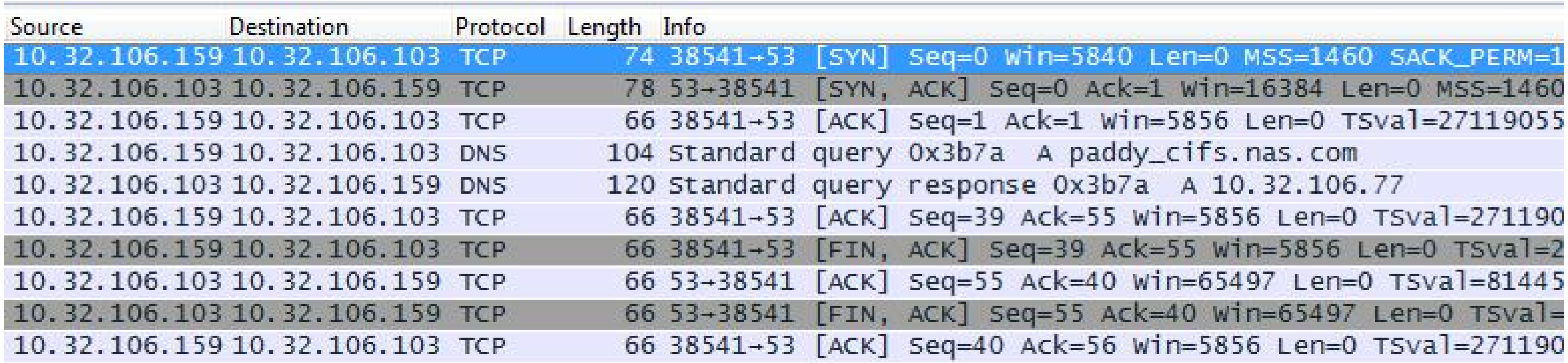
UDP

- 基于UDP的DNS查询：



Source	Destination	Protocol	Length	Info
10.32.106.159	10.32.106.103	DNS	78	Standard query 0x54cd A paddy_cifs.nas.com
10.32.106.103	10.32.106.159	DNS	94	Standard query response 0x54cd A 10.32.106.77

- 基于TCP的DNS查询：



Source	Destination	Protocol	Length	Info
10.32.106.159	10.32.106.103	TCP	74	38541→53 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
10.32.106.103	10.32.106.159	TCP	78	53→38541 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
10.32.106.159	10.32.106.103	TCP	66	38541→53 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=27119055
10.32.106.159	10.32.106.103	DNS	104	Standard query 0x3b7a A paddy_cifs.nas.com
10.32.106.103	10.32.106.159	DNS	120	Standard query response 0x3b7a A 10.32.106.77
10.32.106.159	10.32.106.103	TCP	66	38541→53 [ACK] Seq=39 Ack=55 Win=5856 Len=0 TSval=271190
10.32.106.159	10.32.106.103	TCP	66	38541→53 [FIN, ACK] Seq=39 Ack=55 Win=5856 Len=0 TSval=2
10.32.106.103	10.32.106.159	TCP	66	53→38541 [ACK] Seq=55 Ack=40 Win=65497 Len=0 TSval=81445
10.32.106.103	10.32.106.159	TCP	66	53→38541 [FIN, ACK] Seq=55 Ack=40 Win=65497 Len=0 TSval=
10.32.106.159	10.32.106.103	TCP	66	38541→53 [ACK] Seq=40 Ack=56 Win=5856 Len=0 TSval=271190

UDP协议优缺点

优点：

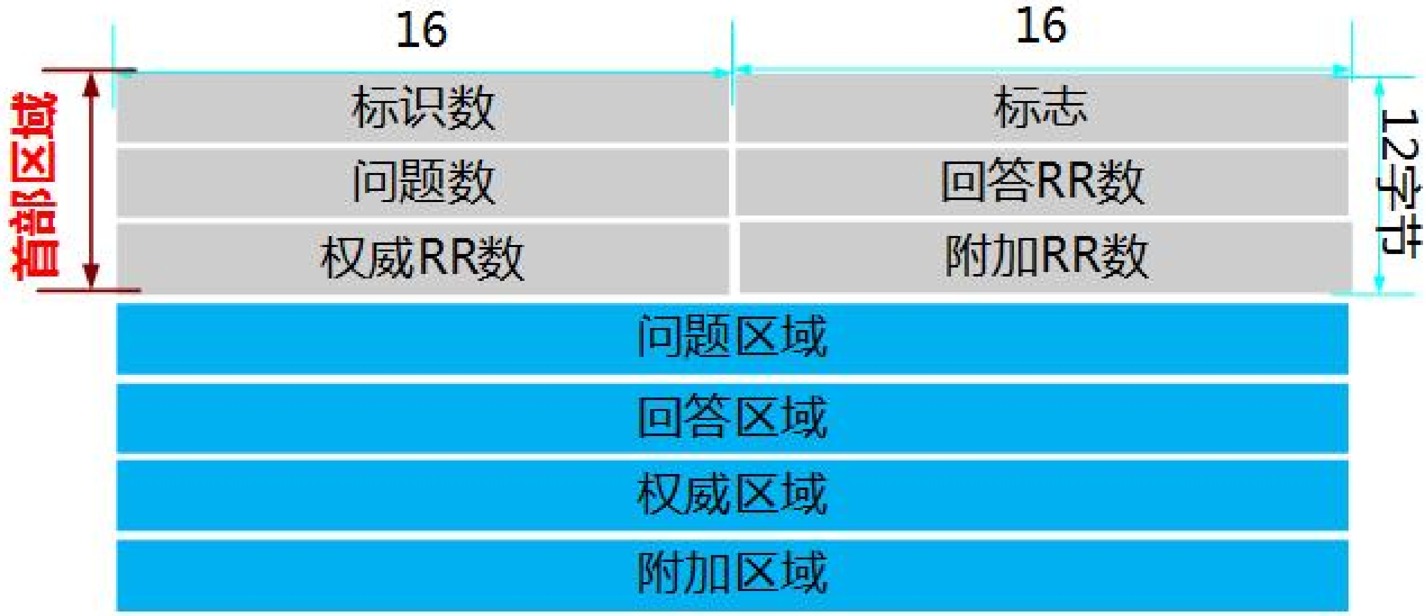
- UDP包携带的净数据较多
- 无需维持连接（DNS查询为例）

缺点：

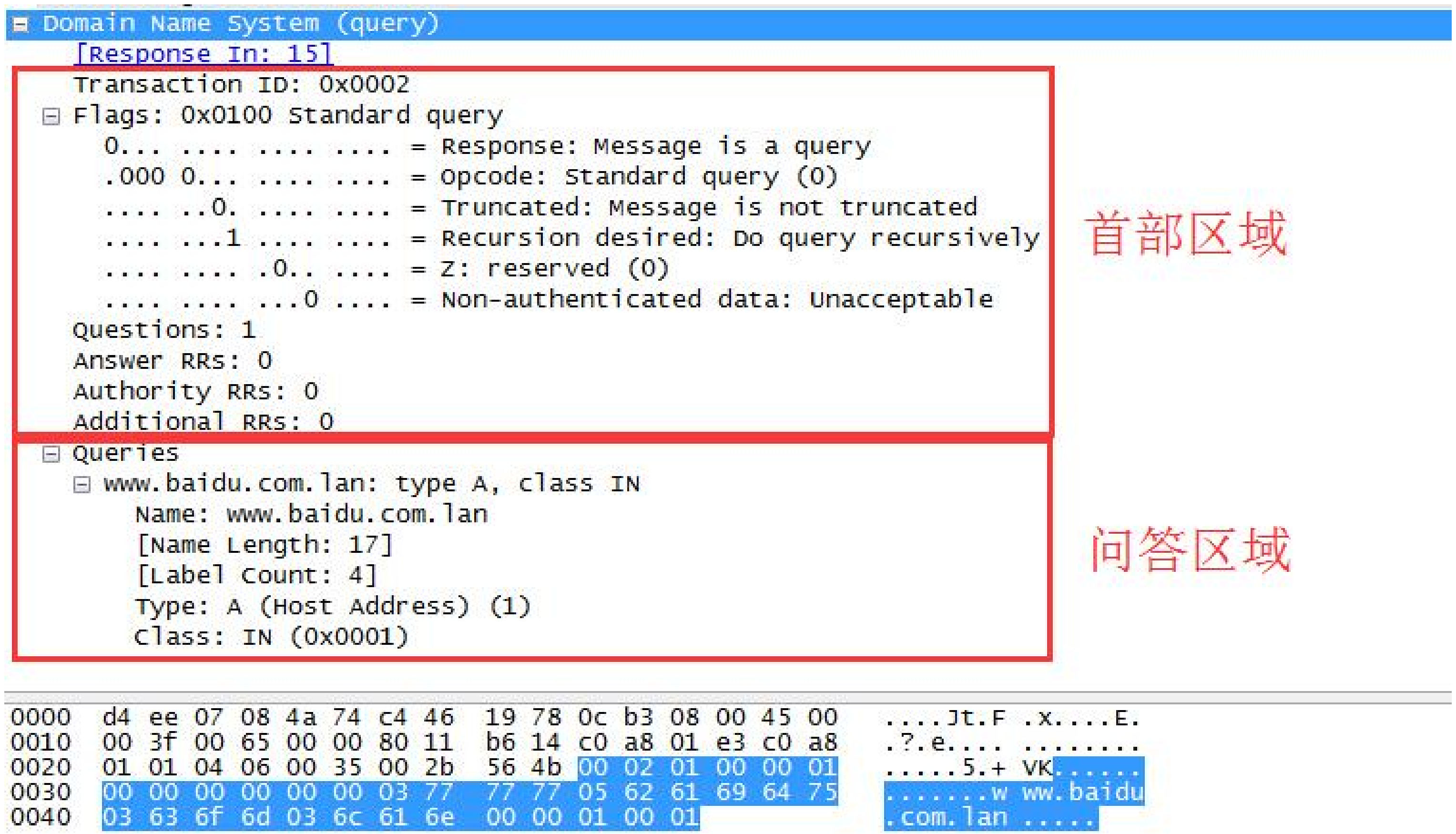
- 不考虑MTU大小
- 没有重传机制

智者安天下

DNS报文格式：查询报文和回答报文，两者格式相同



Wireshark眼中的DNS查询报文



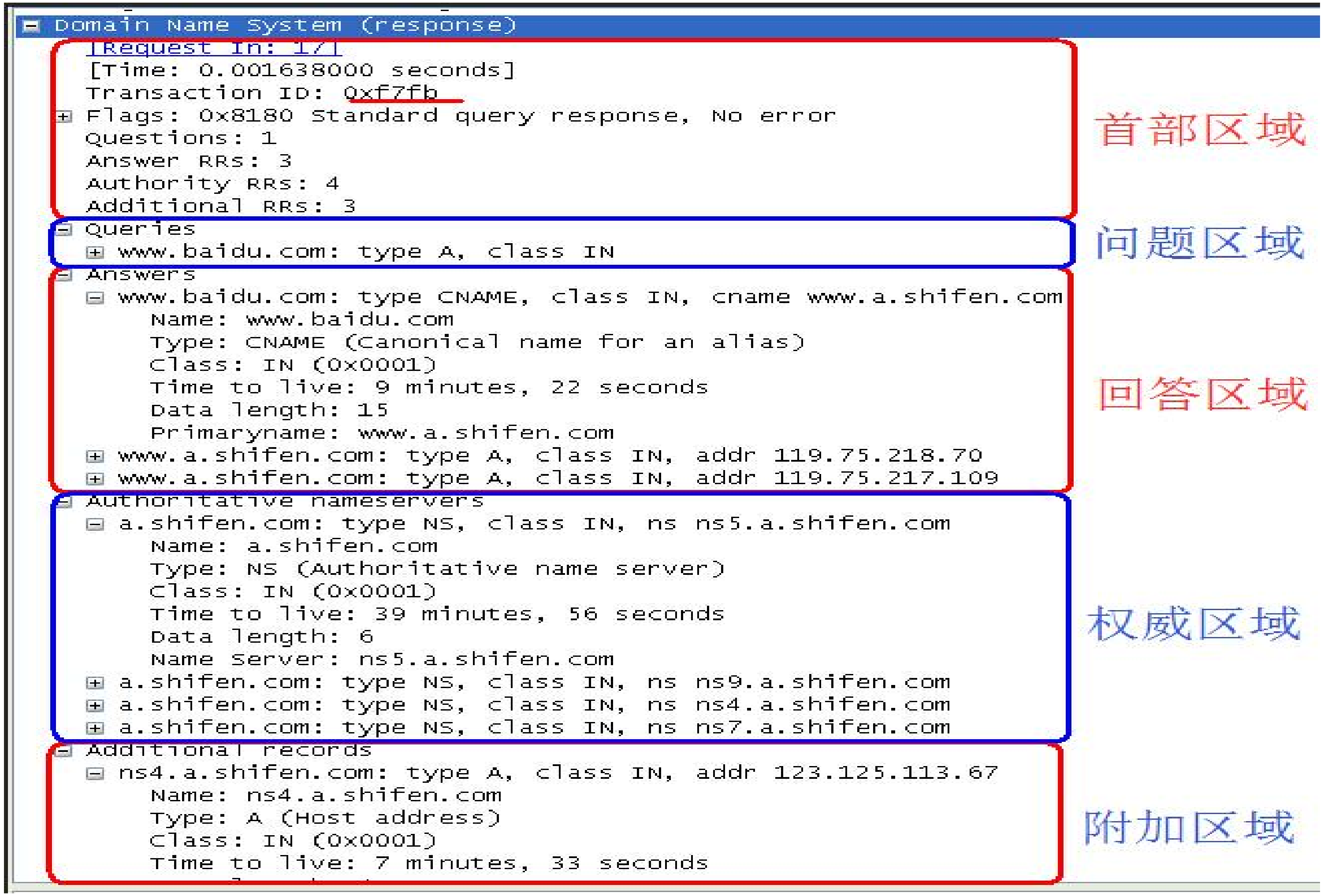
```
⊟ Domain Name System (query)
    [Response In: 15]
    Transaction ID: 0x0002
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...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.lan: type A, class IN
        Name: www.baidu.com.lan
        [Name Length: 17]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

首部区域

问答区域

```
0000  d4 ee 07 08 4a 74 c4 46  19 78 0c b3 08 00 45 00   ....Jt.F .x....E.
0010  00 3f 00 65 00 00 80 11  b6 14 c0 a8 01 e3 c0 a8   .?.e.... ........
0020  01 01 04 06 00 35 00 2b  56 4b 00 02 01 00 00 01   .....5.+ VK......
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 03 6c 61 6e  00 00 01 00 01            .com.lan .....
```

Wireshark眼中的DNS回答报文



```
⊟ Domain Name System (response)
    [Request In: 17]
    [Time: 0.001638000 seconds]
    Transaction ID: 0xf7fb
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 4
    Additional RRs: 3
  ⊟ 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)
        Class: IN (0x0001)
        Time to live: 9 minutes, 22 seconds
        Data length: 15
        Primaryname: www.a.shifen.com
    ⊞ www.a.shifen.com: type A, class IN, addr 119.75.218.70
    ⊞ www.a.shifen.com: type A, class IN, addr 119.75.217.109
  ⊟ Authoritative nameservers
    ⊟ a.shifen.com: type NS, class IN, ns ns5.a.shifen.com
        Name: a.shifen.com
        Type: NS (Authoritative name server)
        Class: IN (0x0001)
        Time to live: 39 minutes, 56 seconds
        Data length: 6
        Name Server: ns5.a.shifen.com
    ⊞ a.shifen.com: type NS, class IN, ns ns9.a.shifen.com
    ⊞ a.shifen.com: type NS, class IN, ns ns4.a.shifen.com
    ⊞ a.shifen.com: type NS, class IN, ns ns7.a.shifen.com
  ⊟ Additional records
    ⊟ ns4.a.shifen.com: type A, class IN, addr 123.125.113.67
        Name: ns4.a.shifen.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 7 minutes, 33 seconds
```

首部区域

问题区域

回答区域

权威区域

附加区域

智者安天下

DNS攻击方式

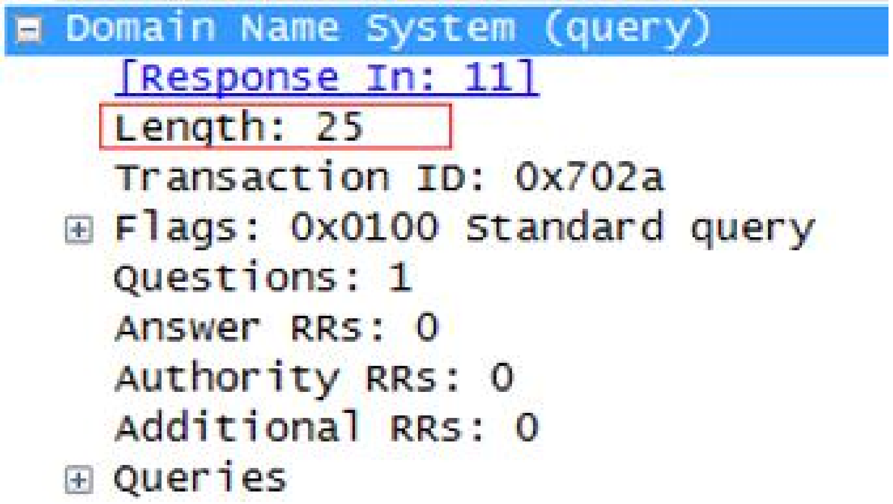
1. 域名劫持
2. 缓存投毒
3. DNS欺骗
4. **放大攻击**

正常的DNS查询：源IP地址 -----DNS查询----> DNS服务器 -----DNS回复包----> 源IP地址

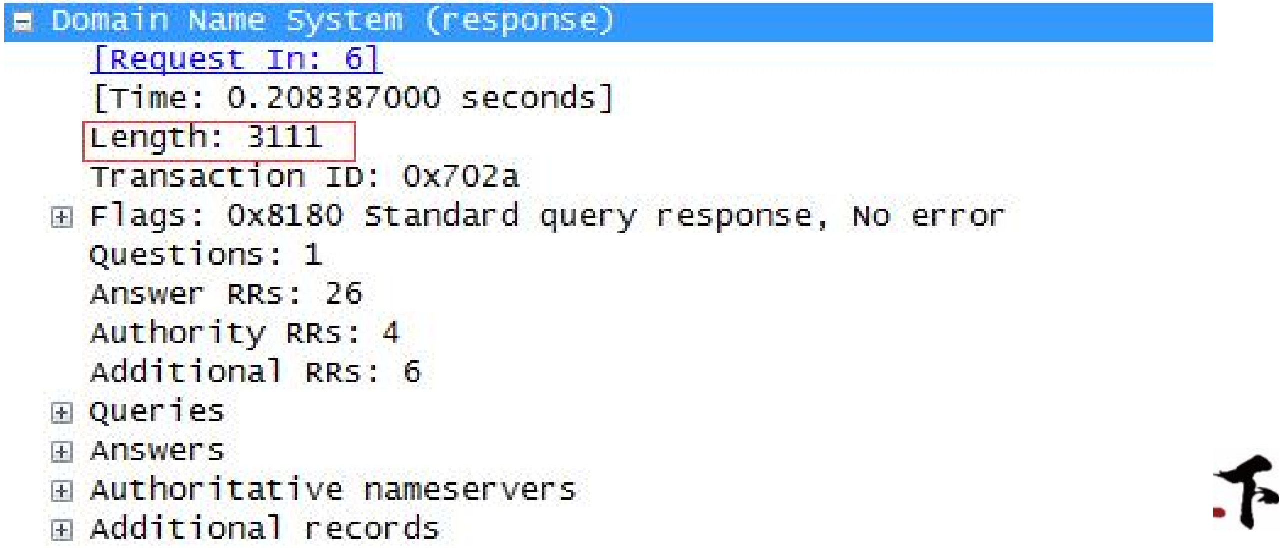
DNS放大攻击：伪造IP地址 -----DNS查询----> DNS服务器 -----DNS回复包----> 伪造的IP地址（攻击目标）

智者安天下

DNS放大攻击

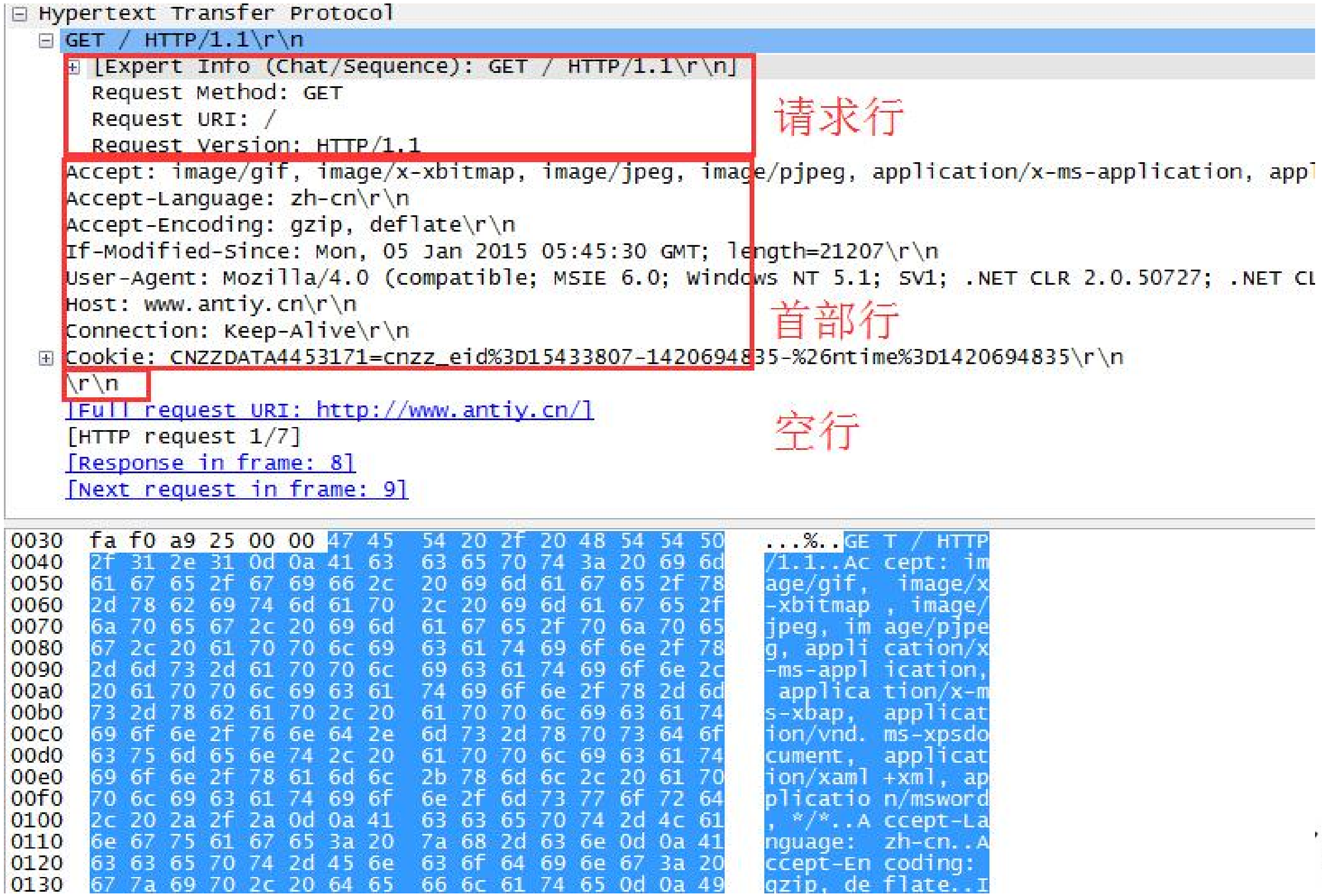


```
⊟ Domain Name System (query)
    [Response In: 11]
    Length: 25
    Transaction ID: 0x702a
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
```



```
⊟ Domain Name System (response)
    [Request In: 6]
    [Time: 0.208387000 seconds]
    Length: 3111
    Transaction ID: 0x702a
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 26
    Authority RRs: 4
    Additional RRs: 6
  ⊞ Queries
  ⊞ Answers
  ⊞ Authoritative nameservers
  ⊞ Additional records
```

Wireshark眼中的HTTP请求报文



```
⊟ Hypertext Transfer Protocol
  ⊟ GET / HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-application, appl
    Accept-Language: zh-cn\r\n
    Accept-Encoding: gzip, deflate\r\n
    If-Modified-Since: Mon, 05 Jan 2015 05:45:30 GMT; length=21207\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CL
    Host: www.antiy.cn\r\n
    Connection: Keep-Alive\r\n
  ⊞ Cookie: CNZZDATA4453171=cnzz_eid%3D15433807-1420694835-%26ntime%3D1420694835\r\n
    \r\n
    [Full request URI: http://www.antiy.cn/]
    [HTTP request 1/7]
    [Response in frame: 8]
    [Next request in frame: 9]
```

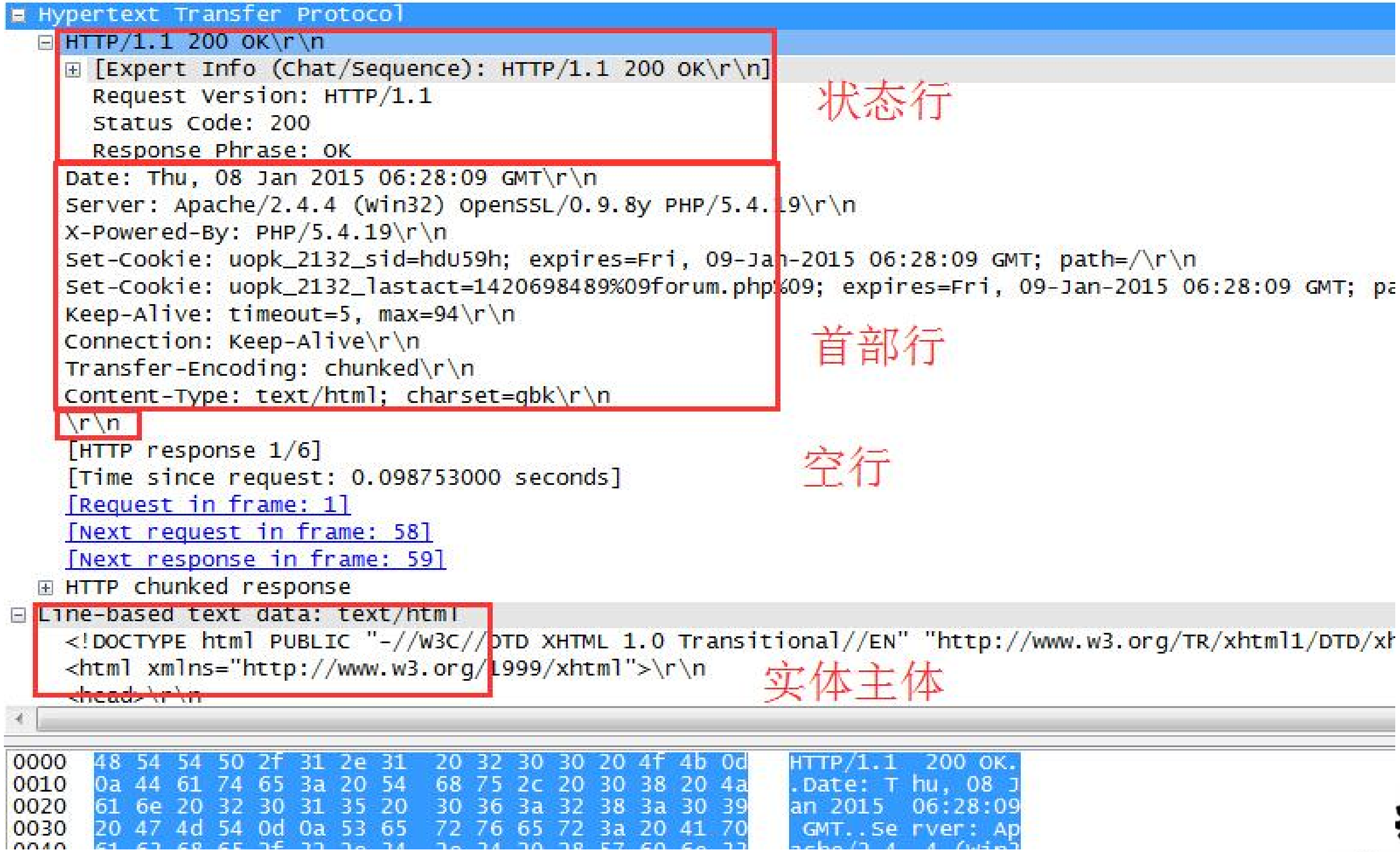
请求行

首部行

空行

```
0030  fa f0 a9 25 00 00 47 45  54 20 2f 20 48 54 54 50   ...%..GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 69 6d   /1.1..Ac cept: im
0050  61 67 65 2f 67 69 66 2c  20 69 6d 61 67 65 2f 78   age/gif,  image/x
0060  2d 78 62 69 74 6d 61 70  2c 20 69 6d 61 67 65 2f   -xbitmap , image/
0070  6a 70 65 67 2c 20 69 6d  61 67 65 2f 70 6a 70 65   jpeg, im age/pjpe
0080  67 2c 20 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   g, appli cation/x
0090  2d 6d 73 2d 61 70 70 6c  69 63 61 74 69 6f 6e 2c   -ms-appl ication,
00a0  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 6d    applica tion/x-m
00b0  73 2d 78 62 61 70 2c 20  61 70 70 6c 69 63 61 74   s-xbap,  applicat
00c0  69 6f 6e 2f 76 6e 64 2e  6d 73 2d 78 70 73 64 6f   ion/vnd. ms-xpsdo
00d0  63 75 6d 65 6e 74 2c 20  61 70 70 6c 69 63 61 74   cument,  applicat
00e0  69 6f 6e 2f 78 61 6d 6c  2b 78 6d 6c 2c 20 61 70   ion/xaml +xml, ap
00f0  70 6c 69 63 61 74 69 6f  6e 2f 6d 73 77 6f 72 64   plicatio n/msword
0100  2c 20 2a 2f 2a 0d 0a 41  63 63 65 70 74 2d 4c 61   , */*..A ccept-La
0110  6e 67 75 61 67 65 3a 20  7a 68 2d 63 6e 0d 0a 41   nguage:  zh-cn..A
0120  63 63 65 70 74 2d 45 6e  63 6f 64 69 6e 67 3a 20   ccept-En coding:
0130  67 7a 69 70 2c 20 64 65  66 6c 61 74 65 0d 0a 49   gzip, de flate..I
```

Wireshark眼中的HTTP响应报文

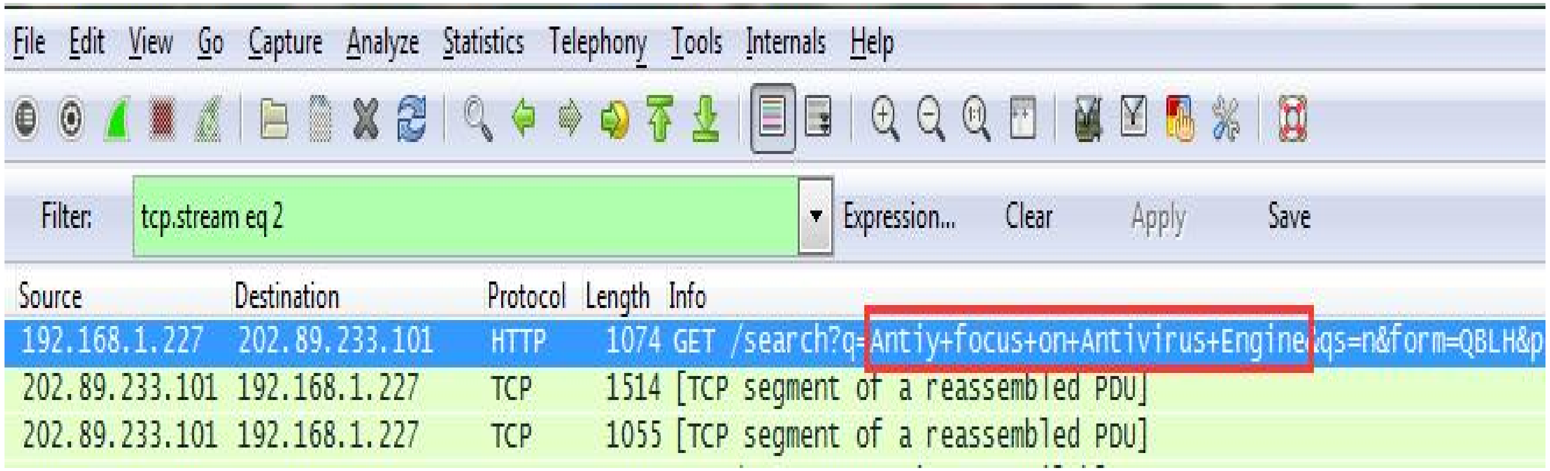


```
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Thu, 08 Jan 2015 06:28:09 GMT\r\n
    Server: Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.19\r\n
    X-Powered-By: PHP/5.4.19\r\n
    Set-Cookie: uopk_2132_sid=hdu59h; expires=Fri, 09-Jan-2015 06:28:09 GMT; path=/\r\n
    Set-Cookie: uopk_2132_lastact=1420698489%09forum.php%09; expires=Fri, 09-Jan-2015 06:28:09 GMT; pa
    Keep-Alive: timeout=5, max=94\r\n
    Connection: Keep-Alive\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: text/html; charset=gbk\r\n
    \r\n
    [HTTP response 1/6]
    [Time since request: 0.098753000 seconds]
    [Request in frame: 1]
    [Next request in frame: 58]
    [Next response in frame: 59]
  ⊞ HTTP chunked response
⊟ Line-based text data: text/html
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xh
    <html xmlns="http://www.w3.org/1999/xhtml">\r\n
    <head>\r\n

0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 54  68 75 2c 20 30 38 20 4a   .Date: T hu, 08 J
0020  61 6e 20 32 30 31 35 20  30 36 3a 32 38 3a 30 39   an 2015  06:28:09
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 34 20 28 57 69 6e 33   ache/2.4 .4 (Win3
```

Q&A

- 基于HTTP协议的通信过程，对于传输的内容是否会被窃取？
- 解决措施？

搜索内容：Antiy focus on Antivirus Engine

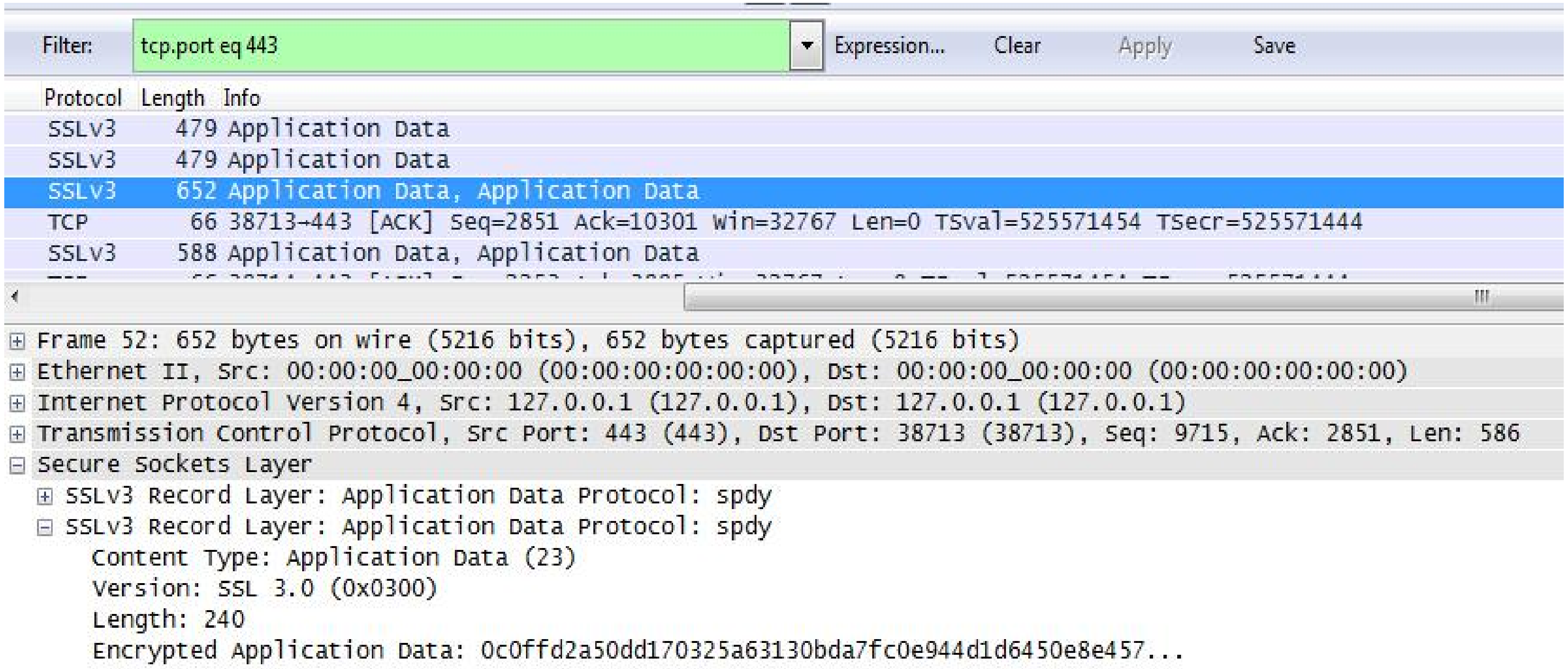


Filter: tcp.stream eq 2

```
Source         Destination    Protocol Length Info
192.168.1.227  202.89.233.101 HTTP     1074 GET /search?q=Antiy+focus+on+Antivirus+Engine&qs=n&form=QBLH&p
202.89.233.101 192.168.1.227  TCP      1514 [TCP segment of a reassembled PDU]
202.89.233.101 192.168.1.227  TCP      1055 [TCP segment of a reassembled PDU]
```

智者安天下

防范措施：HTTPS



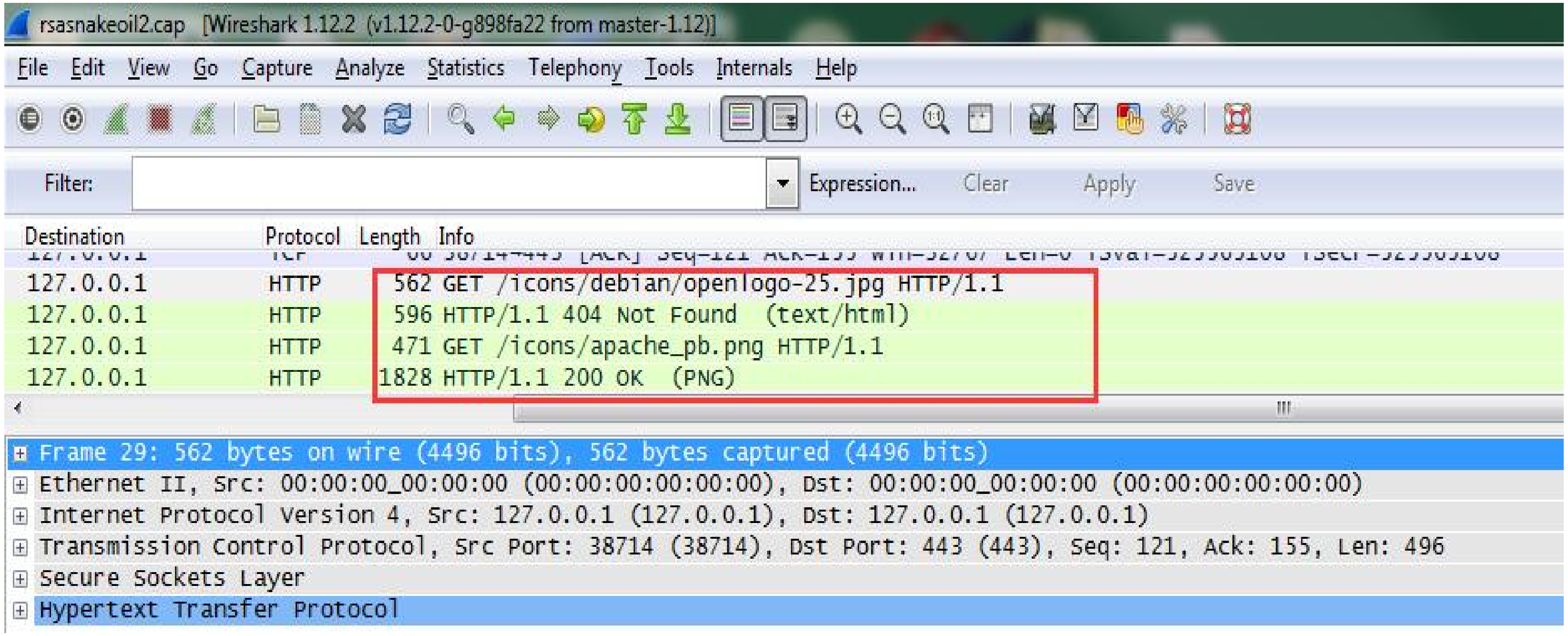
```
Protocol Length Info
SSLv3      479 Application Data
SSLv3      479 Application Data
SSLv3      652 Application Data, Application Data
TCP         66 38713→443 [ACK] Seq=2851 Ack=10301 Win=32767 Len=0 TSval=525571454 TSecr=525571444
SSLv3      588 Application Data, Application Data
```

```
⊞ Frame 52: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
⊞ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊞ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 38713 (38713), Seq: 9715, Ack: 2851, Len: 586
⊟ Secure Sockets Layer
  ⊞ SSLv3 Record Layer: Application Data Protocol: spdy
  ⊟ SSLv3 Record Layer: Application Data Protocol: spdy
      Content Type: Application Data (23)
      Version: SSL 3.0 (0x0300)
      Length: 240
      Encrypted Application Data: 0c0ffd2a50dd170325a63130bda7fc0e944d1d6450e8e457...
```

https数据包，报文内容均为加密状态，如何进行解密？

智者安天下

解密HTTPS数据包


rsasnakeoil2.cap [Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
Destination         Protocol  Length  Info
127.0.0.1           TCP         66 38714→443 [ACK] Seq=121 Ack=155 Win=32767 Len=0 TSval=525505108 TSecr=525505108
127.0.0.1           HTTP       562 GET /icons/debian/openlogo-25.jpg HTTP/1.1
127.0.0.1           HTTP       596 HTTP/1.1 404 Not Found  (text/html)
127.0.0.1           HTTP       471 GET /icons/apache_pb.png HTTP/1.1
127.0.0.1           HTTP      1828 HTTP/1.1 200 OK  (PNG)

⊞ Frame 29: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
⊞ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊞ Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
⊞ Transmission Control Protocol, Src Port: 38714 (38714), Dst Port: 443 (443), Seq: 121, Ack: 155, Len: 496
⊞ Secure Sockets Layer
⊞ Hypertext Transfer Protocol
```

在Wireshark中导入对应的key文件，即可解密该数据包

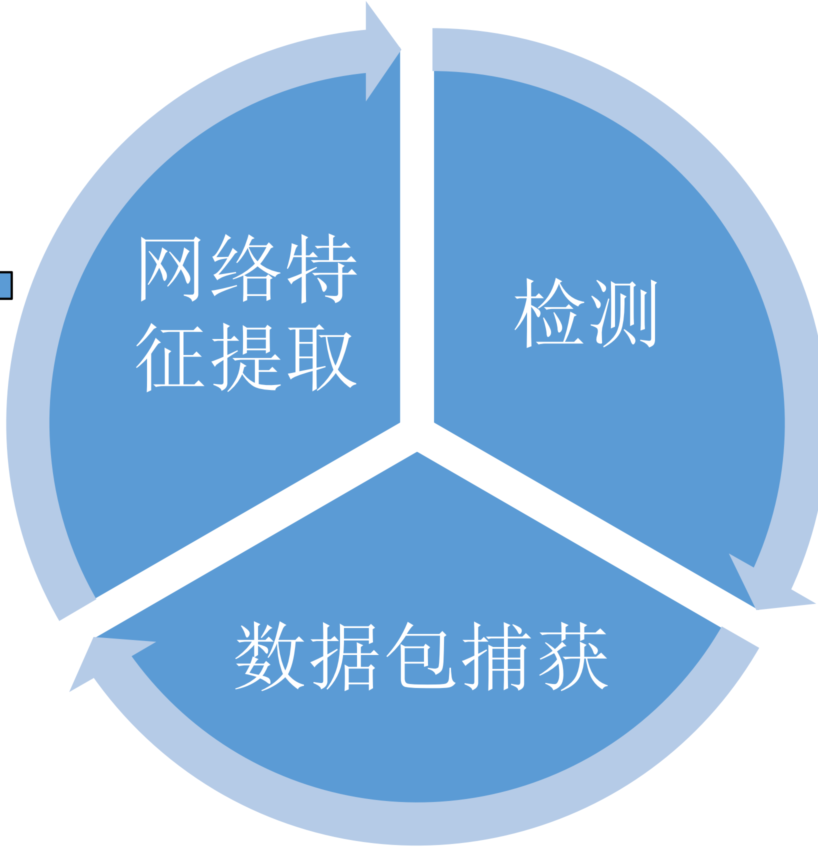
网络特征分析

- 特征分析流程
- 特征匹配及实例
- 特征提取实例
- 网络特征库

主要流程

1. 数据包包头信息

2. 数据包载荷（payload）……



智者安天下

网络特征匹配

- 字符串匹配
- 协议匹配
- 长度（大小）匹配
- 数量匹配
- 逻辑匹配（eg. 正则表达式）

常见的匹配算法：Rabin-Karp算法、Boyer-Moore算法和Aho-Corasick算法等

智者安天下

网络特征匹配——以Snort为例

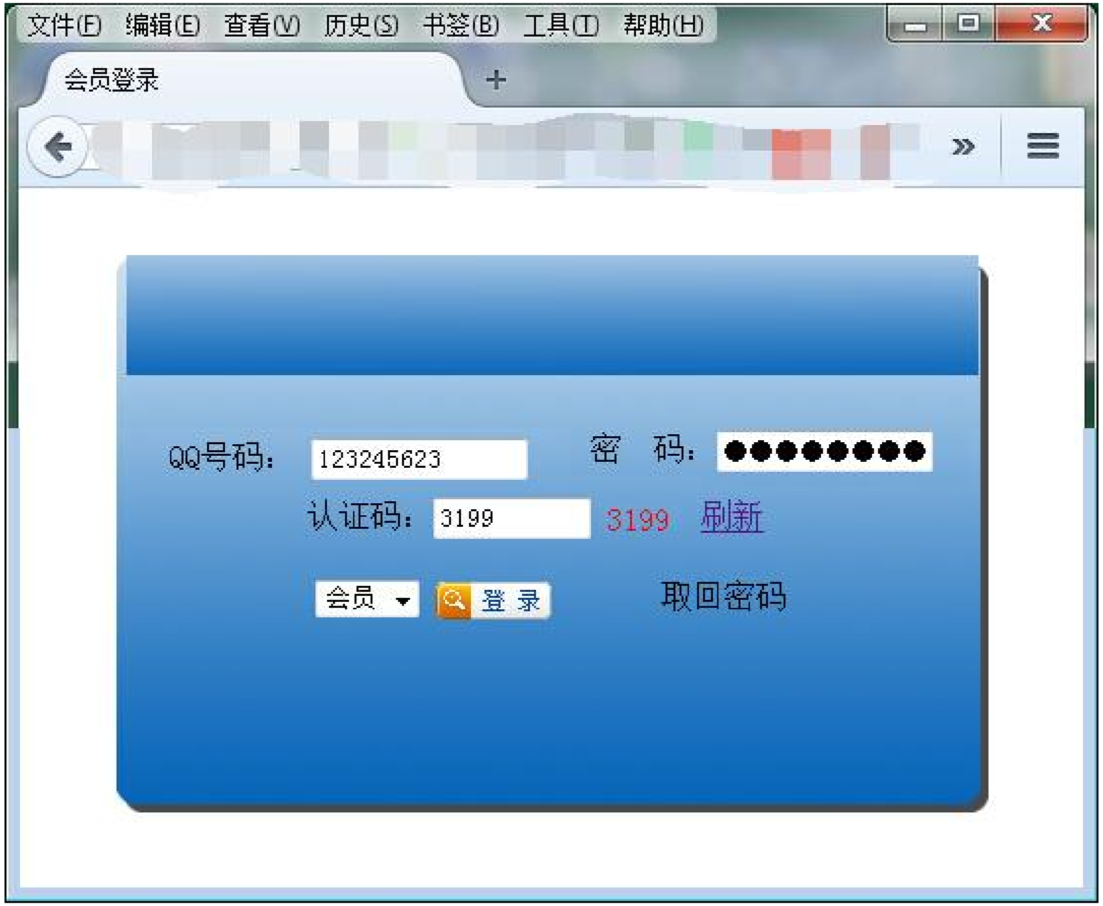
- Snort网络特征：

```
alert tcp any any -> any 80 (msg:"Test alert";
classtype:misc-attack; uricontent:"?";sid:20140925;
rev:1;)
```

- 特征描述：

任何访问部署特征机器80端口且请求中包含“？”的网络流量，都会匹配成功，发生警报，并且可以查看对应的警报类型以及提示信息。

网络特征——以钓鱼网站为例



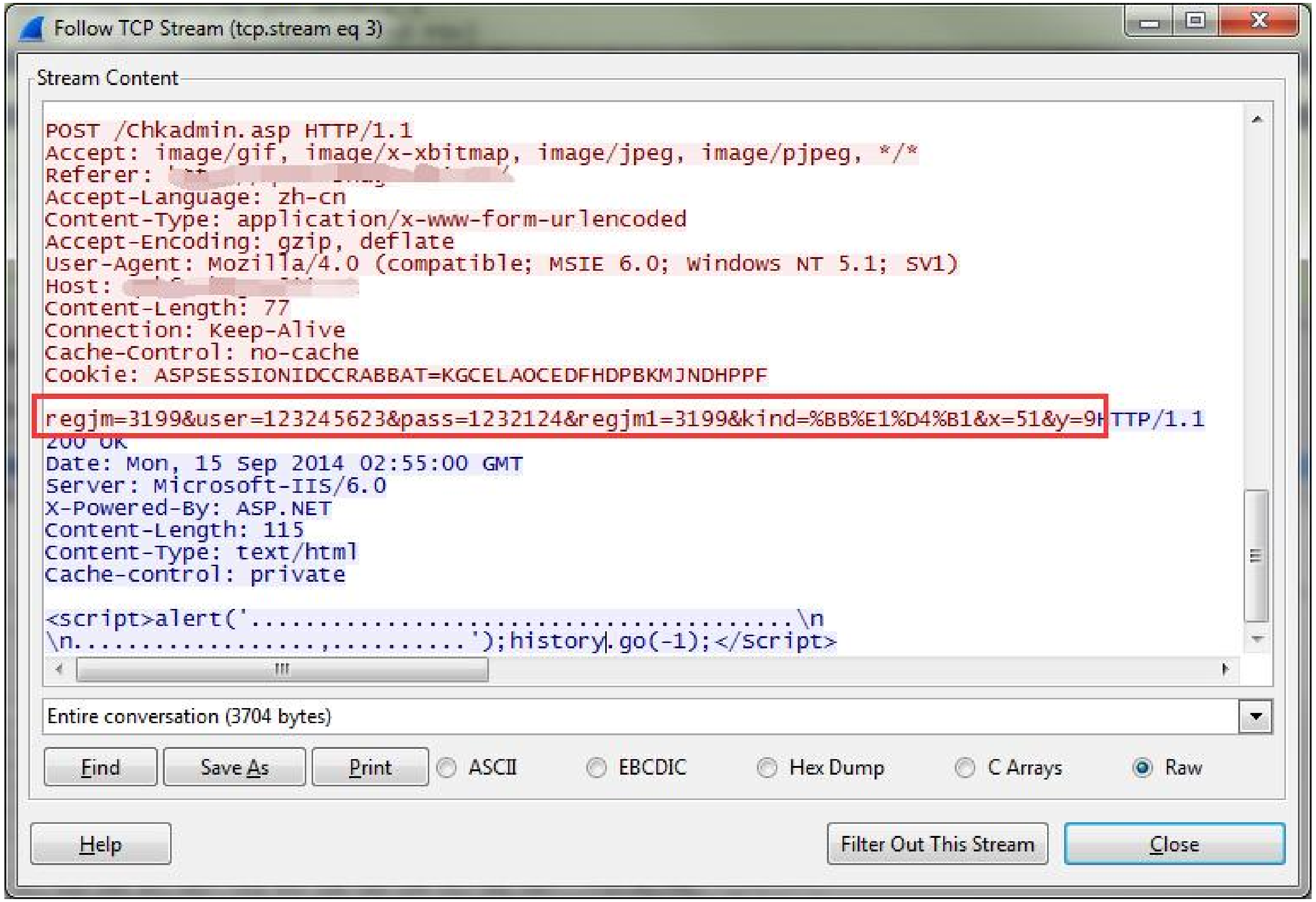
QQ号码：123245623 密　码：●●●●●●●●●

认证码：3199 3199 刷新

会员 ▾ 登 录　取回密码

智者安天下

网络特征——以钓鱼网站为例



```
POST /Chkadmin.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Referer: [redacted]
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: [redacted]
Content-Length: 77
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDCCRABBAT=KGCELAOCEDFHDPBKMJNDHPPF

regjm=3199&user=123245623&pass=1232124&regjm1=3199&kind=%BB%E1%D4%B1&x=51&y=9HTTP/1.1
200 OK
Date: Mon, 15 Sep 2014 02:55:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 115
Content-Type: text/html
Cache-control: private

<script>alert('........................................\n
\n..................,..........');history.go(-1);</script>
```

Entire conversation (3704 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

智者安天下

网络特征——以钓鱼网站为例

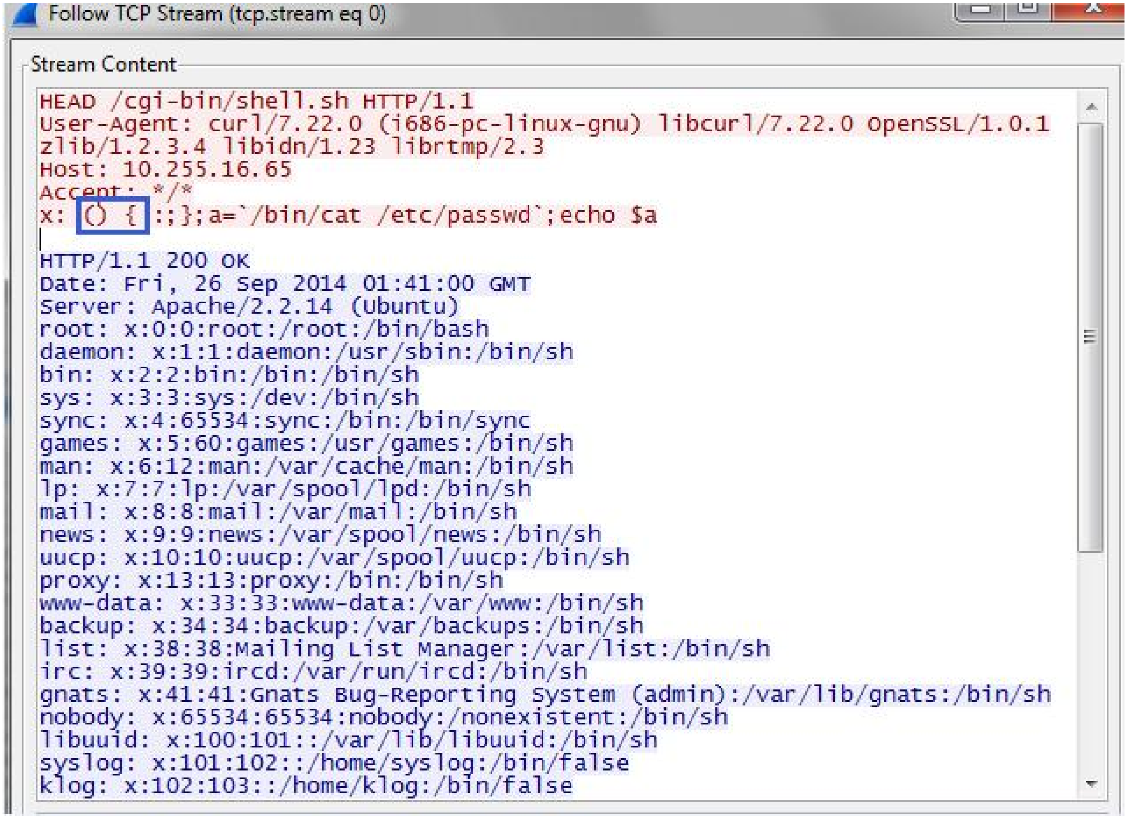
可以作为特征的内容：

- 方法：POST
- 包含文件名：.asp
- 主体字段： “regjm”，“user”，“pass”，“regjm1” ，“kind”……

网络特征——以“破壳”为例

- 如果通过HTTP检测验证漏洞或攻击，可以根据host、UserAgent、header等头信息字符串“() { ”进行检测。

- 特征规则：\x28\x29\x20\x7b\x20



```
HEAD /cgi-bin/shell.sh HTTP/1.1
User-Agent: curl/7.22.0 (i686-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1
zlib/1.2.3.4 libidn/1.23 librtmp/2.3
Host: 10.255.16.65
Accept: */*
x: () { :;};a=`/bin/cat /etc/passwd`;echo $a

HTTP/1.1 200 OK
Date: Fri, 26 Sep 2014 01:41:00 GMT
Server: Apache/2.2.14 (Ubuntu)
root: x:0:0:root:/root:/bin/bash
daemon: x:1:1:daemon:/usr/sbin:/bin/sh
bin: x:2:2:bin:/bin:/bin/sh
sys: x:3:3:sys:/dev:/bin/sh
sync: x:4:65534:sync:/bin:/bin/sync
games: x:5:60:games:/usr/games:/bin/sh
man: x:6:12:man:/var/cache/man:/bin/sh
lp: x:7:7:lp:/var/spool/lpd:/bin/sh
mail: x:8:8:mail:/var/mail:/bin/sh
news: x:9:9:news:/var/spool/news:/bin/sh
uucp: x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy: x:13:13:proxy:/bin:/bin/sh
www-data: x:33:33:www-data:/var/www:/bin/sh
backup: x:34:34:backup:/var/backups:/bin/sh
list: x:38:38:Mailing List Manager:/var/list:/bin/sh
irc: x:39:39:ircd:/var/run/ircd:/bin/sh
gnats: x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody: x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid: x:100:101::/var/lib/libuuid:/bin/sh
syslog: x:101:102::/home/syslog:/bin/false
klog: x:102:103::/home/klog:/bin/false
```

智者安天下

网络特征库

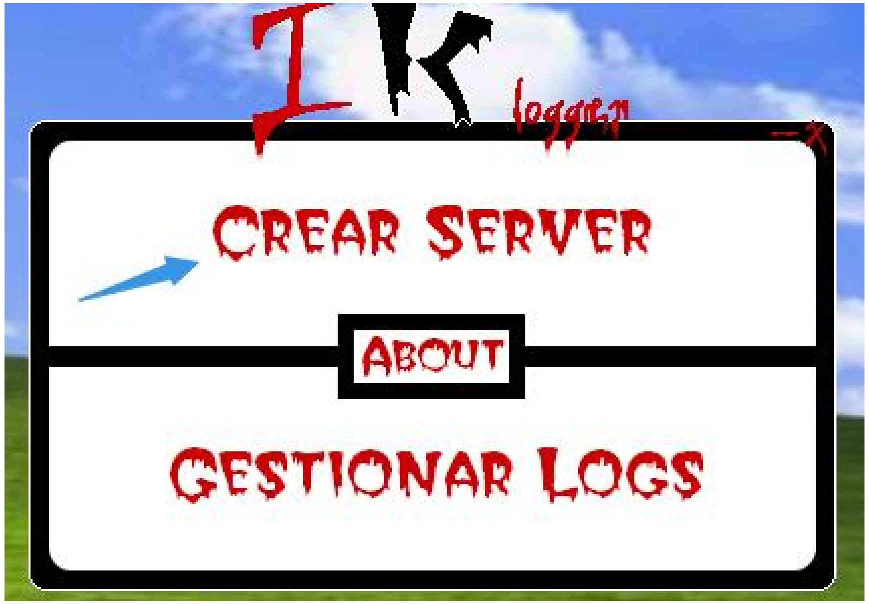
- 精确性：防止误报和漏报的发生
- 实时性：快速检测异常行为
- 可扩展性：根据网络异常行为的变化不定期更新特征库

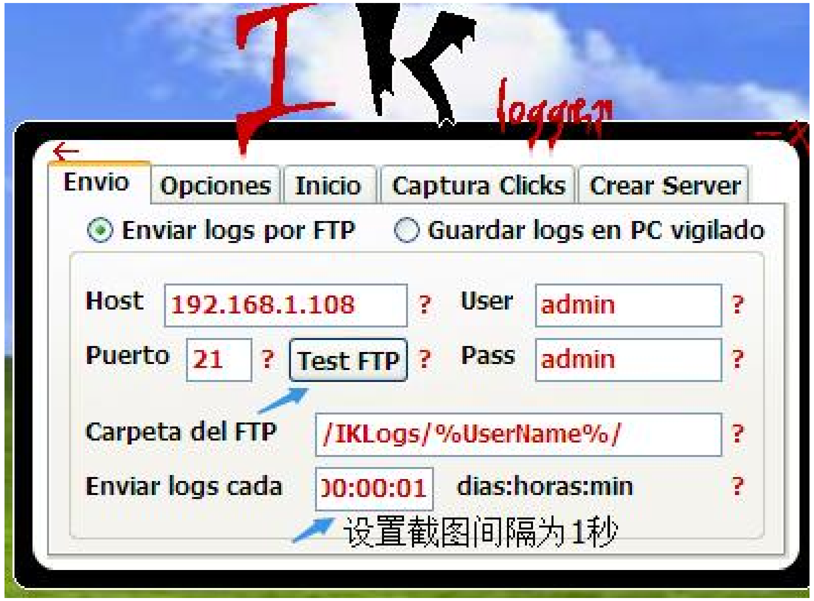
案例分享

- 银行盗号木马
- 非授权通信
- 美女黑客之约

案例分享之银行盗号木马

- 盗取银行的登录用户名和密码
- 通过FTP回传屏幕截图以及键盘记录





● Enviar logs por FTP ○ Guardar logs en PC vigilado

Host 192.168.1.108 ? User admin ?

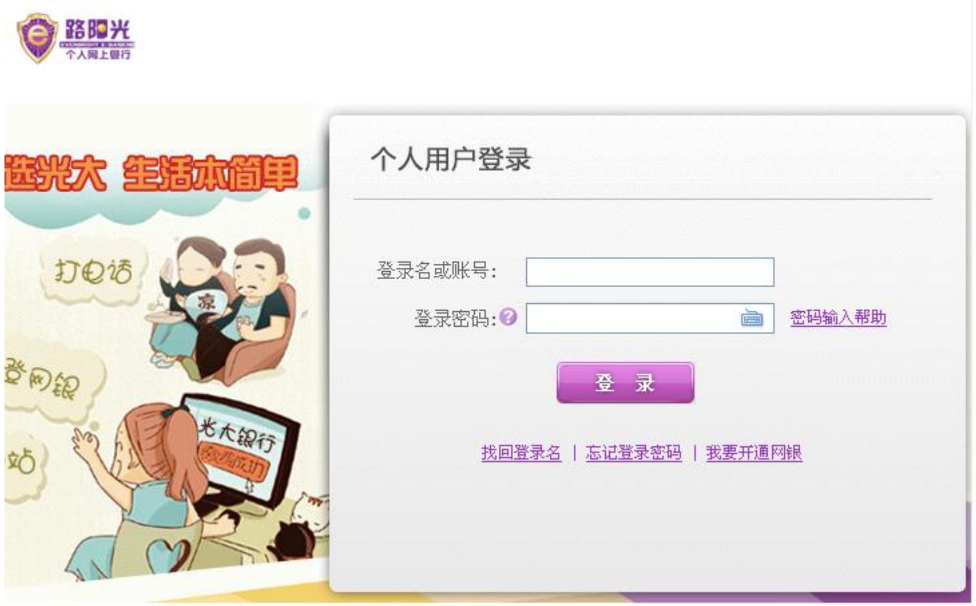
Puerto 21 ? Test FTP ? Pass admin ?

Carpeta del FTP /IKLogs/%UserName%/ ?

Enviar logs cada)0:00:01 dias:horas:min ?

设置截图间隔为1秒

案例分享之银行盗号木马



个人用户登录

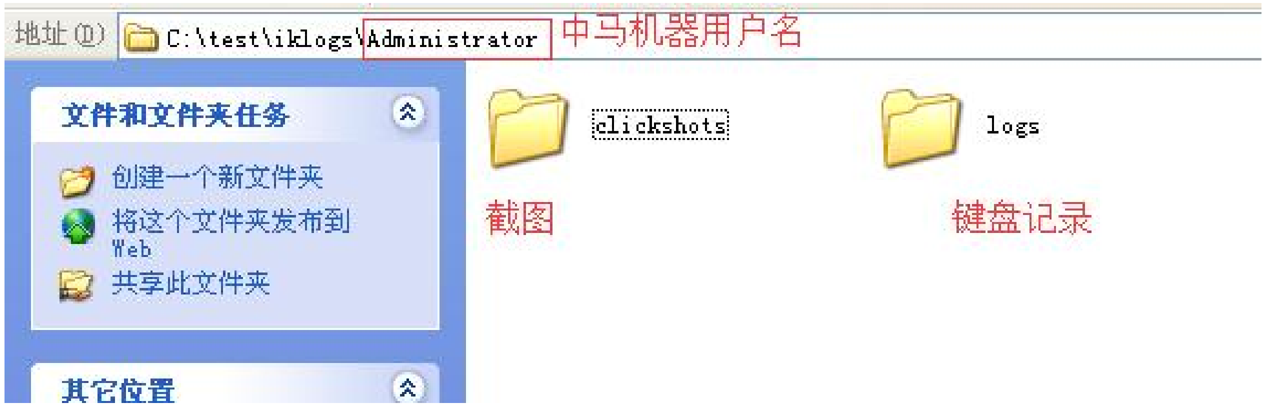
登录名或账号：

登录密码：

密码输入帮助

登 录

找回登录名 | 忘记登录密码 | 我要开通网银



地址(D) C:\test\iklogs\Administrator

中马机器用户名

文件和文件夹任务

- 创建一个新文件夹
- 将这个文件夹发布到Web
- 共享此文件夹

其它位置

clickshots

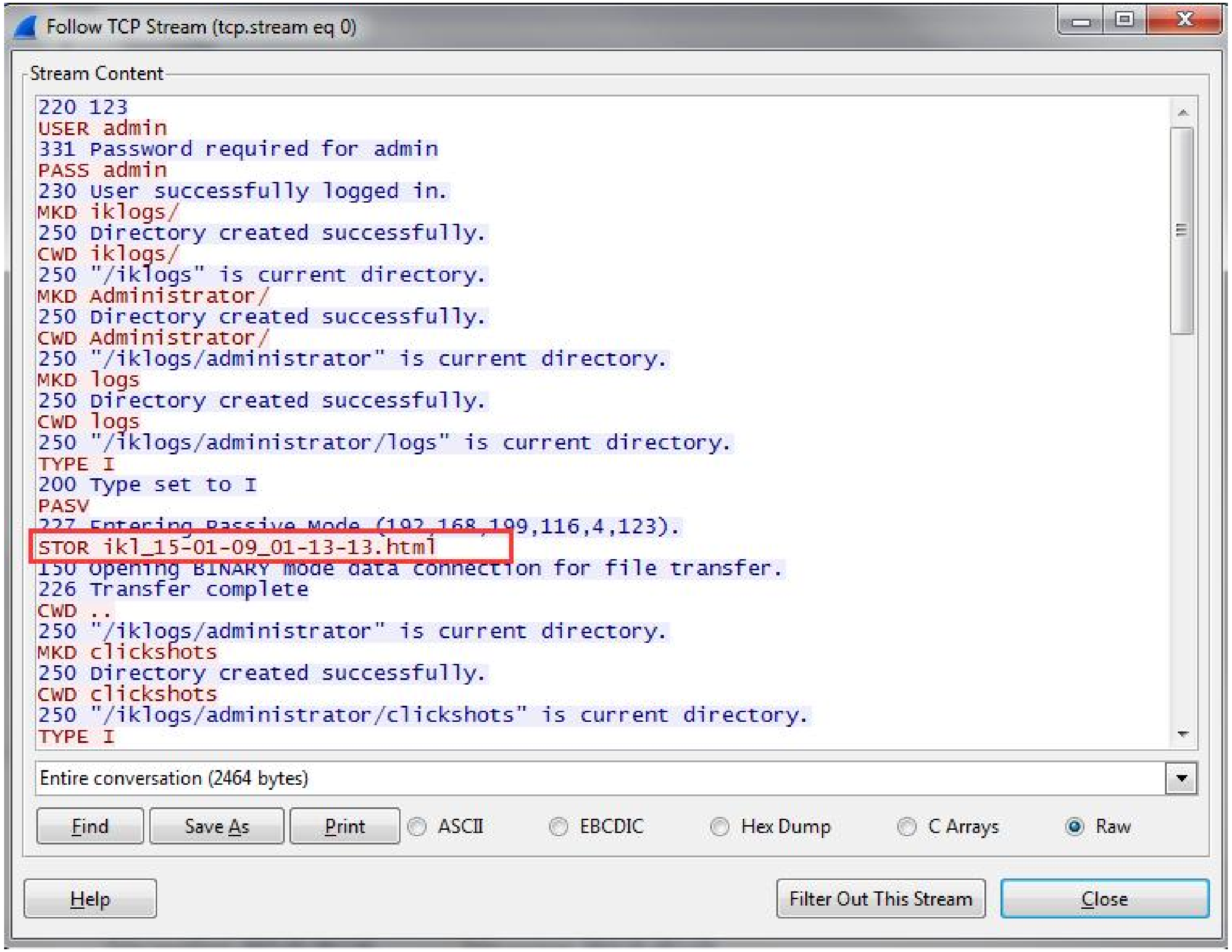
截图

logs

键盘记录

智者安天下

木马传输流程



Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
220 123
USER admin
331 Password required for admin
PASS admin
230 User successfully logged in.
MKD iklogs/
250 Directory created successfully.
CWD iklogs/
250 "/iklogs" is current directory.
MKD Administrator/
250 Directory created successfully.
CWD Administrator/
250 "/iklogs/administrator" is current directory.
MKD logs
250 Directory created successfully.
CWD logs
250 "/iklogs/administrator/logs" is current directory.
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (192,168,199,116,4,123).
STOR ikl_15-01-09_01-13-13.html
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
CWD ..
250 "/iklogs/administrator" is current directory.
MKD clickshots
250 Directory created successfully.
CWD clickshots
250 "/iklogs/administrator/clickshots" is current directory.
TYPE I
```

Entire conversation (2464 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

智者安天下

盗号木马网络特征提取

- 方法：FTP
- 目录名称：iklogs
- 键盘记录和屏幕截图：

ikl_ + [0-9-_]{5,17} + ^ “.html”

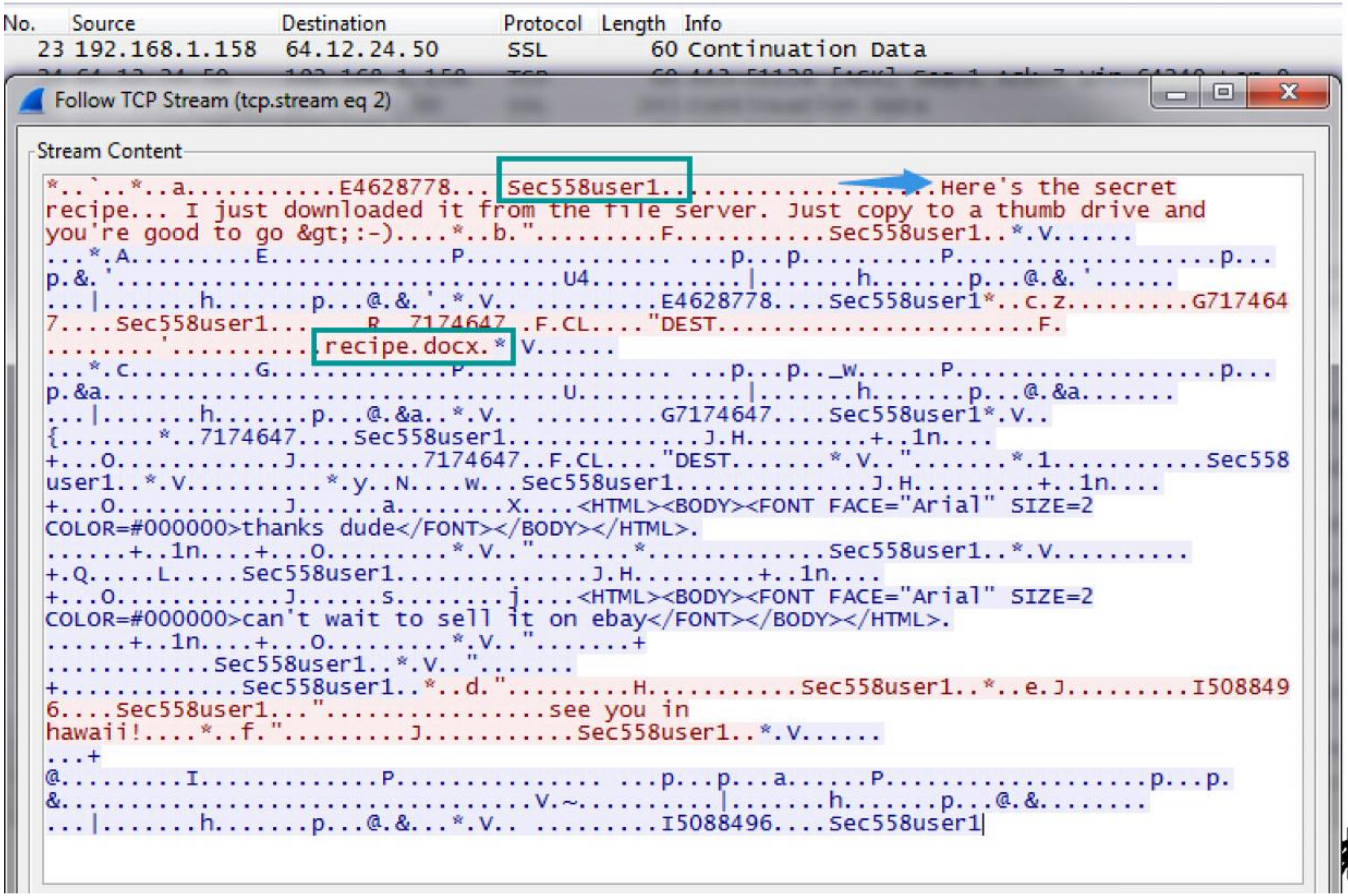
ikc_ + [0-9-_]{5,22} + ^ “.jpg”

案例分享之非授权通信

任务描述：

在企业网络监控试验中，我们捕获到一次非授权即时通信（IM），要求根据捕获到的网络数据包，分析出此次非授权通信的第一条会话信息内容，以及通信传输的文件名及其内容。

案例分享之非授权通信



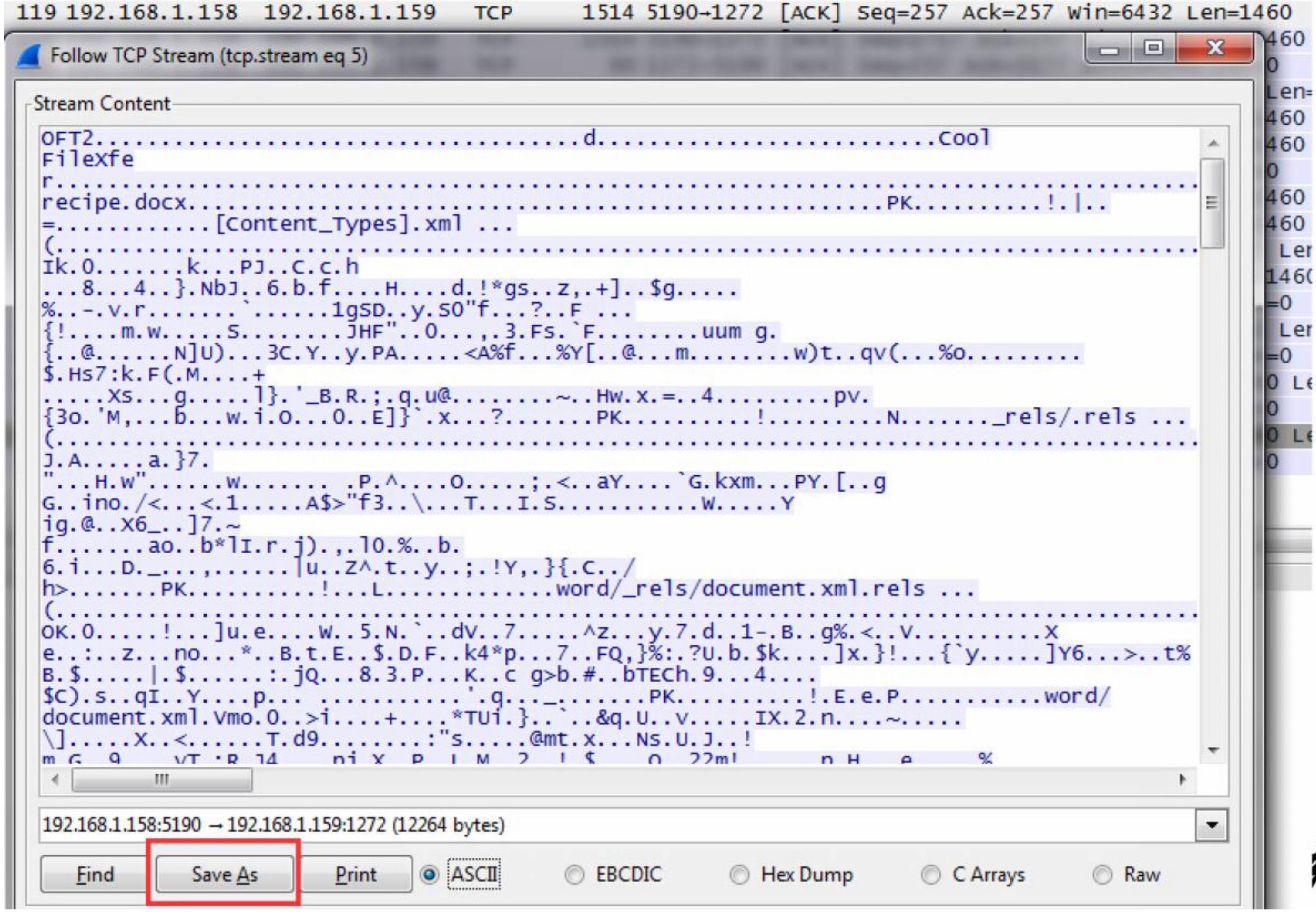
```
No.  Source          Destination    Protocol Length Info
  23 192.168.1.158   64.12.24.50    SSL          60 Continuation Data
```

Follow TCP Stream (tcp.stream eq 2)

Stream Content

```
*..`..*..a...........E4628778... Sec558user1..................Here's the secret
recipe... I just downloaded it from the file server. Just copy to a thumb drive and
you're good to go &gt;:-)....*..b."..........F...........Sec558user1..*.V......
...*.A.........E..............P................ ...p...p...........P....................p...
p.&.'...............................U4...........|.......h.......p...@.&.'......
...|.......h.......p...@.&.'.*.V.. ..........E4628778....Sec558user1*..c.z..........G717464
7....Sec558user1...     R  7174647 .F.CL...."DEST........................F.
........'...........recipe.docx.* V......
...*.c.........G..............P................ ...p...p.._w......P....................p...
p.&a................................U...........|.......h.......p...@.&a.......
...|.......h.......p...@.&a..*.V.. ..........G7174647....Sec558user1*.V..
{.......*..7174647....Sec558user1...............J.H..........+..1n....
+...O............J..........7174647..F.CL...."DEST.......*.V.."........*.1............Sec558
user1..*.V..........*.y..N....w...Sec558user1...............J.H..........+..1n....
+...O............J......a.........X....<HTML><BODY><FONT FACE="Arial" SIZE=2
COLOR=#000000>thanks dude</FONT></BODY></HTML>.
......+..1n....+...O.........*.V.."........*.............Sec558user1..*.V..........
+.Q.....L.....Sec558user1..............J.H..........+..1n....
+...O............J......s.........j....<HTML><BODY><FONT FACE="Arial" SIZE=2
COLOR=#000000>can't wait to sell it on ebay</FONT></BODY></HTML>.
......+..1n....+...O.........*.V.."........+
............Sec558user1..*.V.."........
+............Sec558user1..*..d."..........H...........Sec558user1..*..e.J..........I508849
6....Sec558user1..."..................see you in
hawaii!....*..f."..........J...........Sec558user1..*.V......
...+
@.........I.............P................ ...p...p...a......P....................p...p.
&...................................V.~...........|.......h.......p...@.&........
...|.......h.......p...@.&...*.V.. ..........I5088496....Sec558user1
```

案例分享之非授权通信

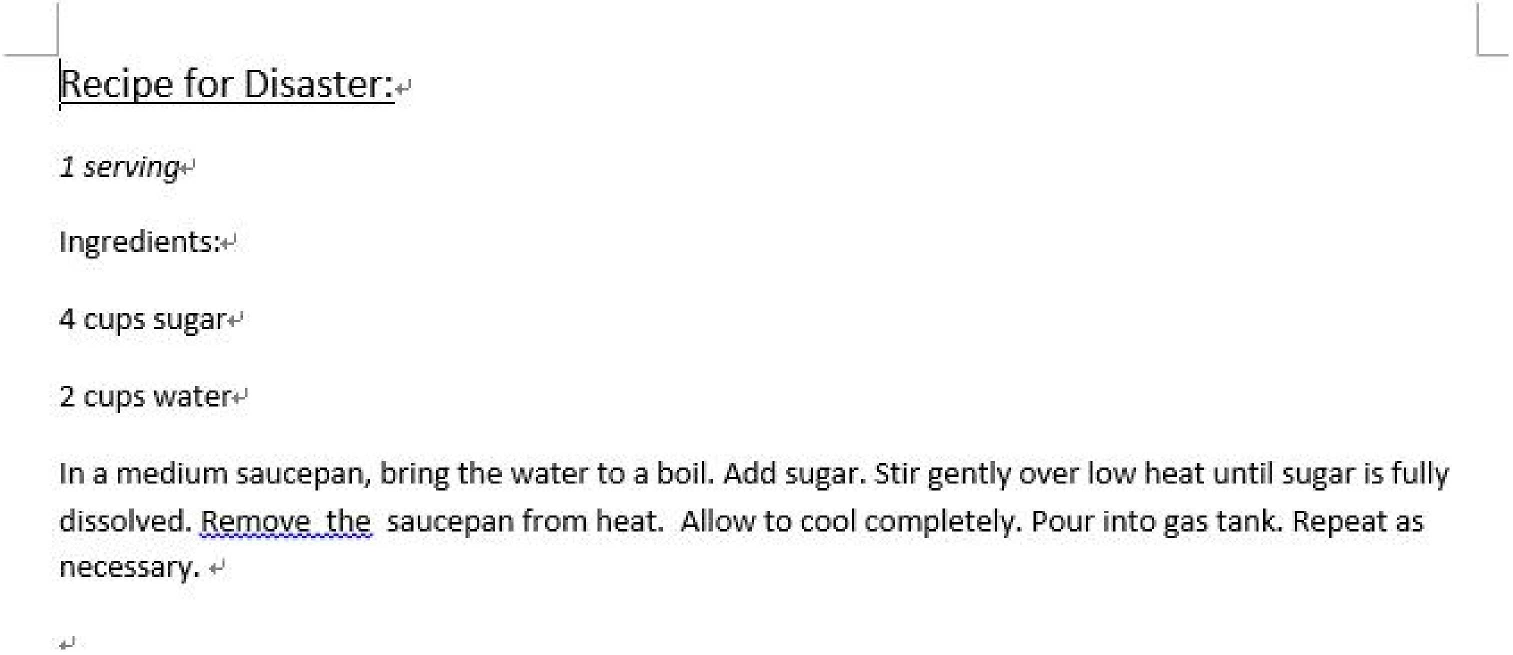


```
119 192.168.1.158   192.168.1.159   TCP     1514 5190→1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
```

```
OFT2...................................d..........................Cool
Filexfe
r..........................................................................................
recipe.docx...........................................PK...........!.|..
=............[Content_Types].xml ...
(..........................................................................................
Ik.O.......k...PJ..C.c.h
...8...4..}.NbJ..6.b.f....H....d.!*gs..z,.+]..$g.....
%..-.v.r.......`......1gSD..y.SO"f...?..F ...
{!....m.w.....S........JHF"..O...,.3.Fs.`F........uum g.
{..@......N]U)...3C.Y..y.PA.....<A%f...%Y[..@...m........w)t..qv(...%o.........
$.Hs7:k.F(.M....+
.....Xs...g.....]}.'_B.R.;.q.u@........~..Hw.x.=..4.........pv.
{3o.'M,...b...w.i.O...O..E]}`.x...?.......PK..........!.........N......._rels/.rels ...
(..........................................................................................
J.A.....a.}7.
"...H.w"......w.......  .P.^....O.....;.<..aY....`G.kxm...PY.[..g
G..ino./<...<.1.....A$>"f3..\...T...I.S...........W.....Y
ig.@..X6_..]7.~
f.......ao..b*lI.r.j).,.lO.%..b.
6.i...D._...,.......|u..Z^.t..y..;.!Y,.}{.C../
h>.......PK..........!...L.............word/_rels/document.xml.rels ...
(..........................................................................................
OK.O.....!...]u.e....W..5.N.`..dV..7.....^z...y.7.d..1-.B..g%.<..V..........X
e..:..z...no...*..B.t.E..$.D.F..k4*p...7..FQ,}%:.?U.b.$k....]x.}!...{`y.....]Y6...>..t%
B.$.....|.$......:.jQ...8.3.P...K..c g>b.#..bTECh.9...4....
$C).s..qI..Y....p...  ...........'.q..._.......PK..........!.E.e.P...........word/
document.xml.Vmo.O..>i....+....*TUi.}..`..&q.U..V.....IX.2.n....~.....
\].....X..<.......T.d9........:"s.....@mt.x...Ns.U.J..!
```

192.168.1.158:5190 → 192.168.1.159:1272 (12264 bytes)

案例分享之非授权通信



Recipe for Disaster:

1 serving

Ingredients:

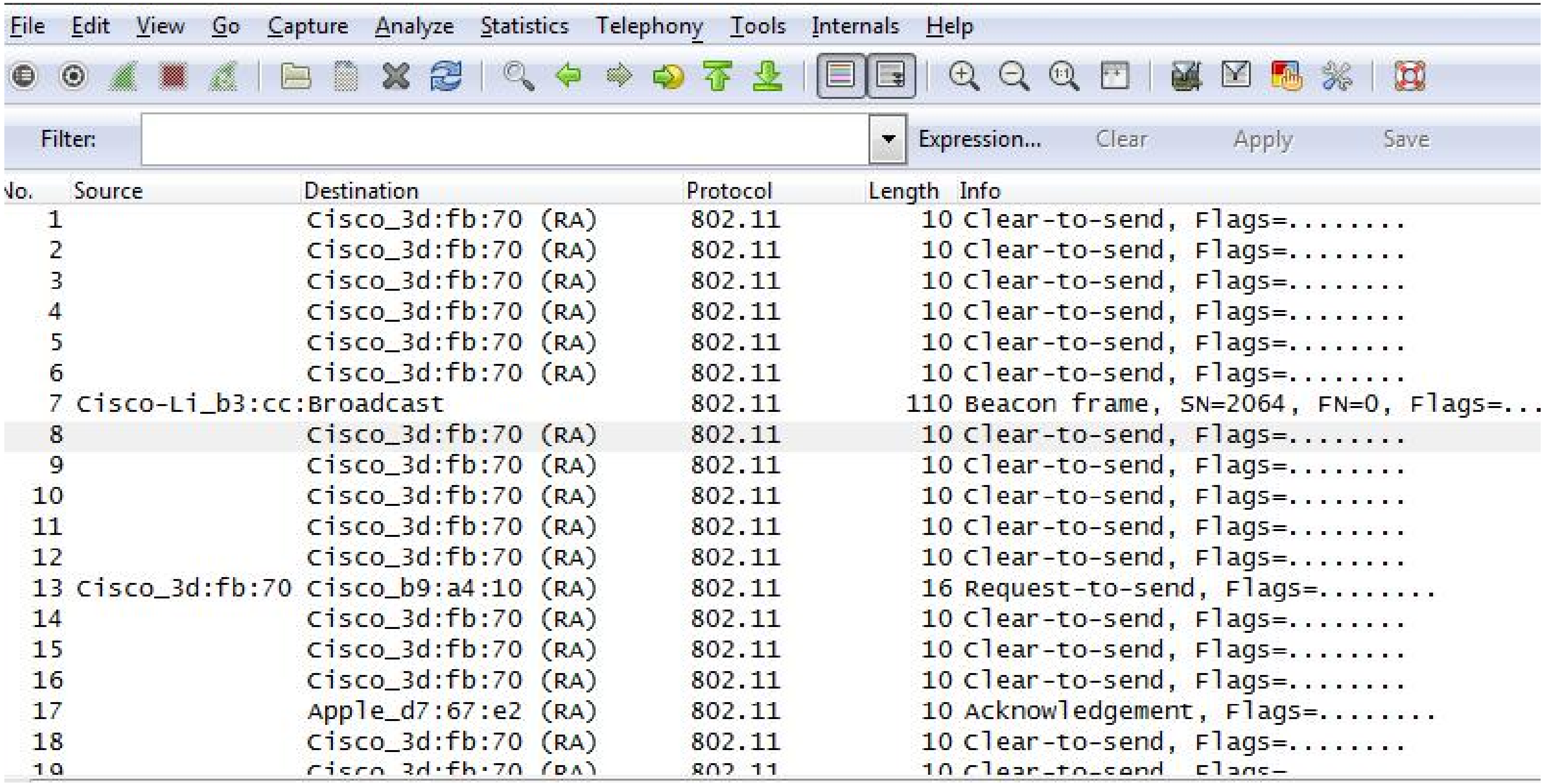
4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

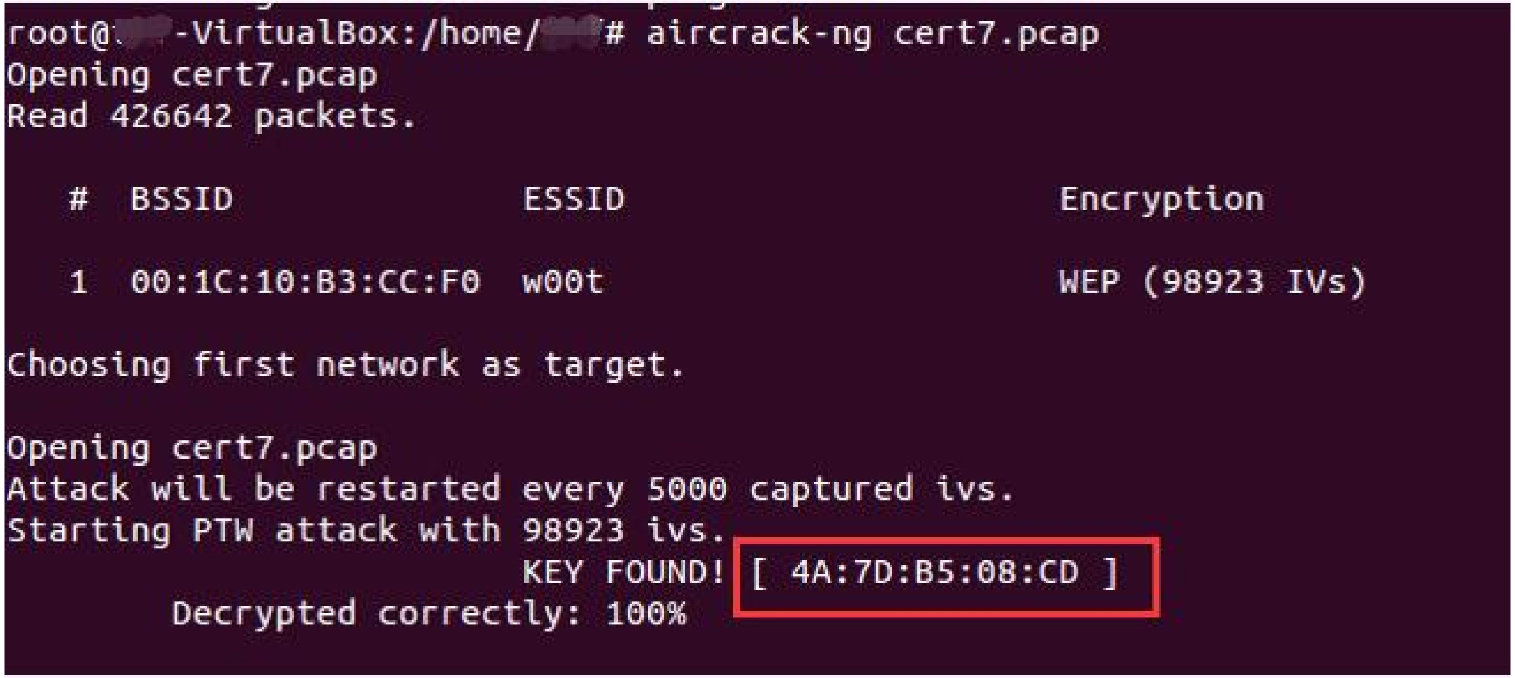
案例分享之我与美女黑客的约会

故事关键词：美女黑客；Dark Tangent ；俄罗斯

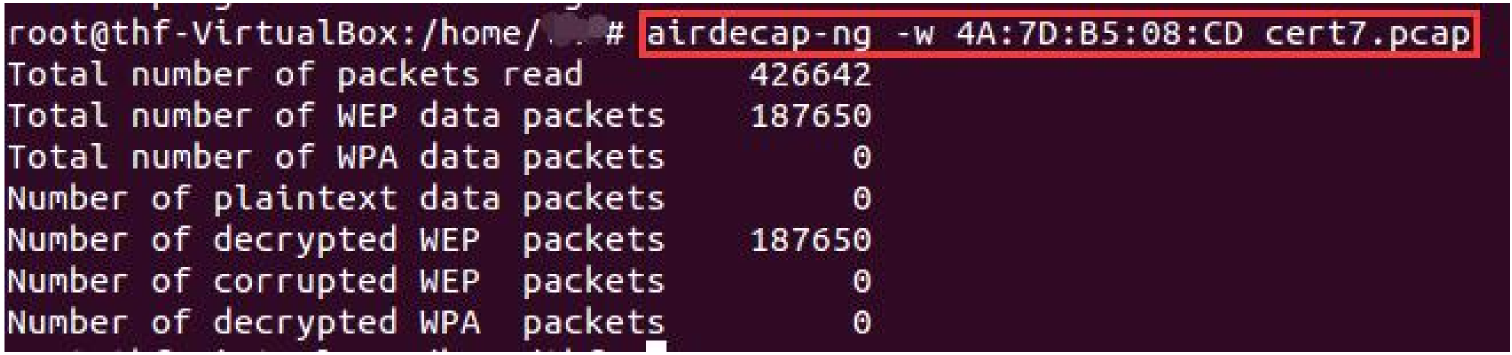


```
No.  Source           Destination           Protocol   Length  Info
  1                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  2                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  3                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  4                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  5                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  6                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  7 Cisco-Li_b3:cc:Broadcast                802.11       110 Beacon frame, SN=2064, FN=0, Flags=...
  8                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
  9                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 10                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 11                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 12                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 13 Cisco_3d:fb:70 Cisco_b9:a4:10 (RA)      802.11        16 Request-to-send, Flags=........
 14                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 15                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 16                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 17                   Apple_d7:67:e2 (RA)   802.11        10 Acknowledgement, Flags=........
 18                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=........
 19                   Cisco_3d:fb:70 (RA)   802.11        10 Clear-to-send, Flags=
```

案例分享之我与美女黑客的约会



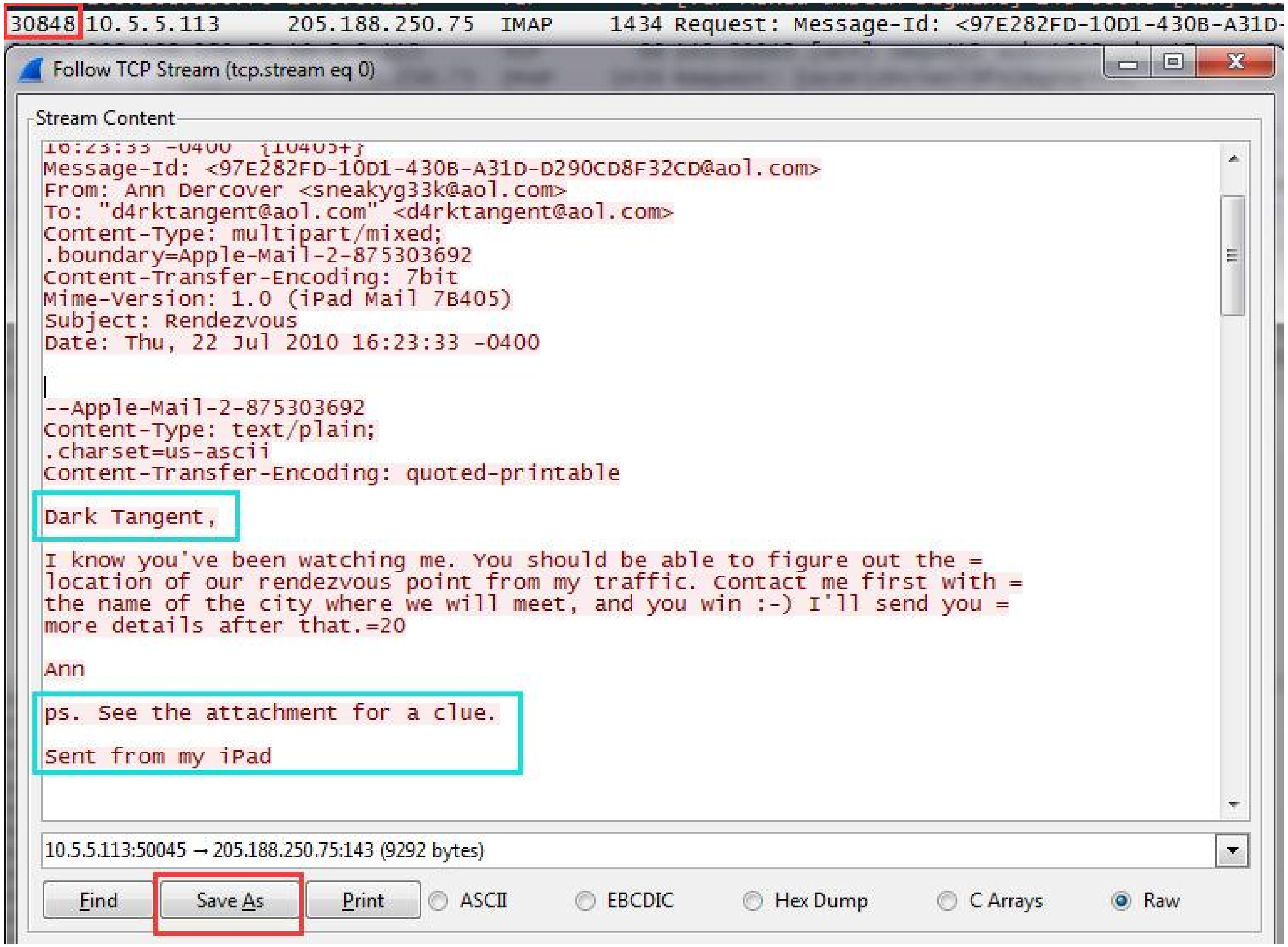
```
root@[redacted]-VirtualBox:/home/[redacted]# aircrack-ng cert7.pcap
Opening cert7.pcap
Read 426642 packets.

   #  BSSID              ESSID                      Encryption

   1  00:1C:10:B3:CC:F0  w00t                       WEP (98923 IVs)

Choosing first network as target.

Opening cert7.pcap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 98923 ivs.
                         KEY FOUND! [ 4A:7D:B5:08:CD ]
        Decrypted correctly: 100%
```



```
root@thf-VirtualBox:/home/[redacted]# airdecap-ng -w 4A:7D:B5:08:CD cert7.pcap
Total number of packets read        426642
Total number of WEP data packets    187650
Total number of WPA data packets         0
Number of plaintext data packets         0
Number of decrypted WEP  packets    187650
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
```

智者安天下

案例分享之我与美女黑客的约会

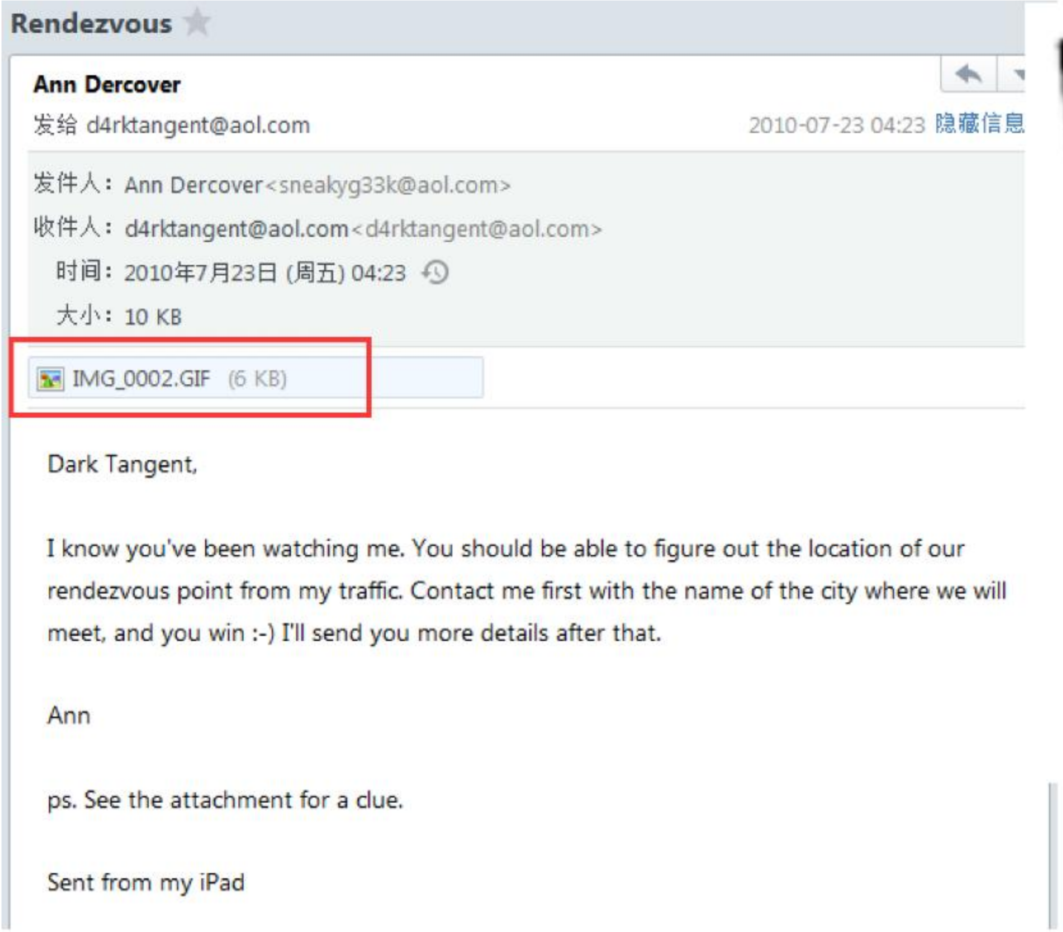


```
30848 10.5.5.113        205.188.250.75   IMAP    1434 Request: Message-Id: <97E282FD-10D1-430B-A31D-
```

```
16:23:33 -0400  {10405+}
Message-Id: <97E282FD-10D1-430B-A31D-D290CD8F32CD@aol.com>
From: Ann Dercover <sneakyg33k@aol.com>
To: "d4rktangent@aol.com" <d4rktangent@aol.com>
Content-Type: multipart/mixed;
.boundary=Apple-Mail-2-875303692
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (iPad Mail 7B405)
Subject: Rendezvous
Date: Thu, 22 Jul 2010 16:23:33 -0400


--Apple-Mail-2-875303692
Content-Type: text/plain;
.charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Dark Tangent,

I know you've been watching me. You should be able to figure out the =
location of our rendezvous point from my traffic. Contact me first with =
the name of the city where we will meet, and you win :-) I'll send you =
more details after that.=20

Ann

ps. See the attachment for a clue.

Sent from my iPad
```

10.5.5.113:50045 → 205.188.250.75:143 (9292 bytes)

案例分享之我与美女黑客的约会



Rendezvous ☆

Ann Dercover

发给 d4rktangent@aol.com 2010-07-23 04:23 隐藏信息

发件人：Ann Dercover<sneakyg33k@aol.com>

收件人：d4rktangent@aol.com<d4rktangent@aol.com>

时间：2010年7月23日 (周五) 04:23

大小：10 KB

IMG_0002.GIF (6 KB)

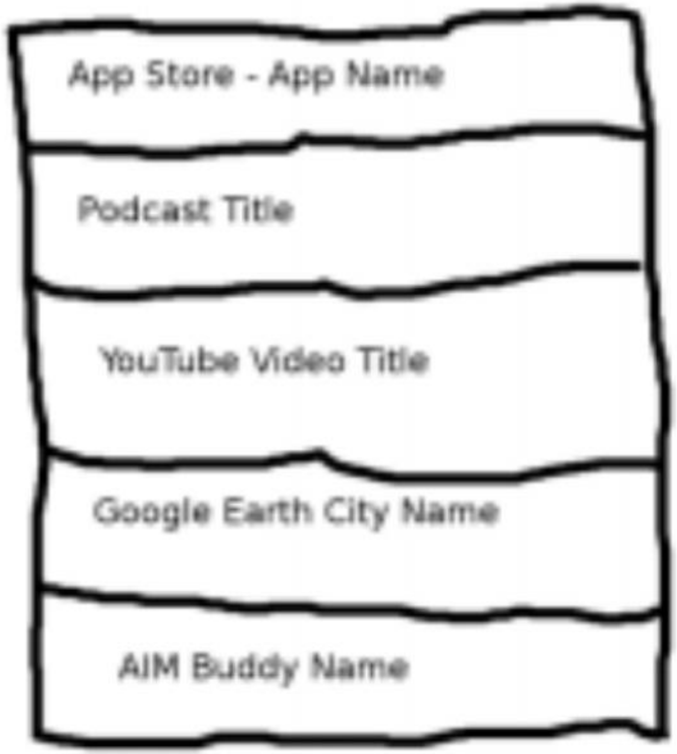
Dark Tangent,

I know you've been watching me. You should be able to figure out the location of our rendezvous point from my traffic. Contact me first with the name of the city where we will meet, and you win :-) I'll send you more details after that.

Ann

ps. See the attachment for a clue.

Sent from my iPad



App Store - App Name

Podcast Title

YouTube Video Title

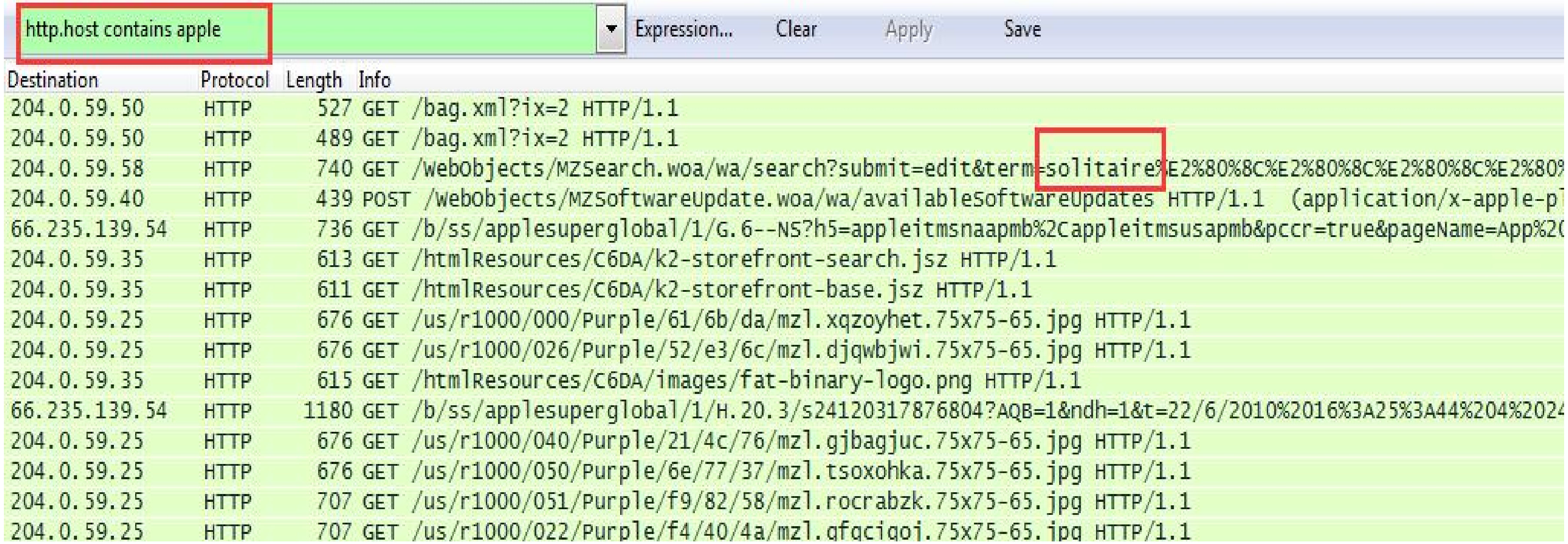
Google Earth City Name

AIM Buddy Name

智者安天下

案例分享之我与美女黑客的约会

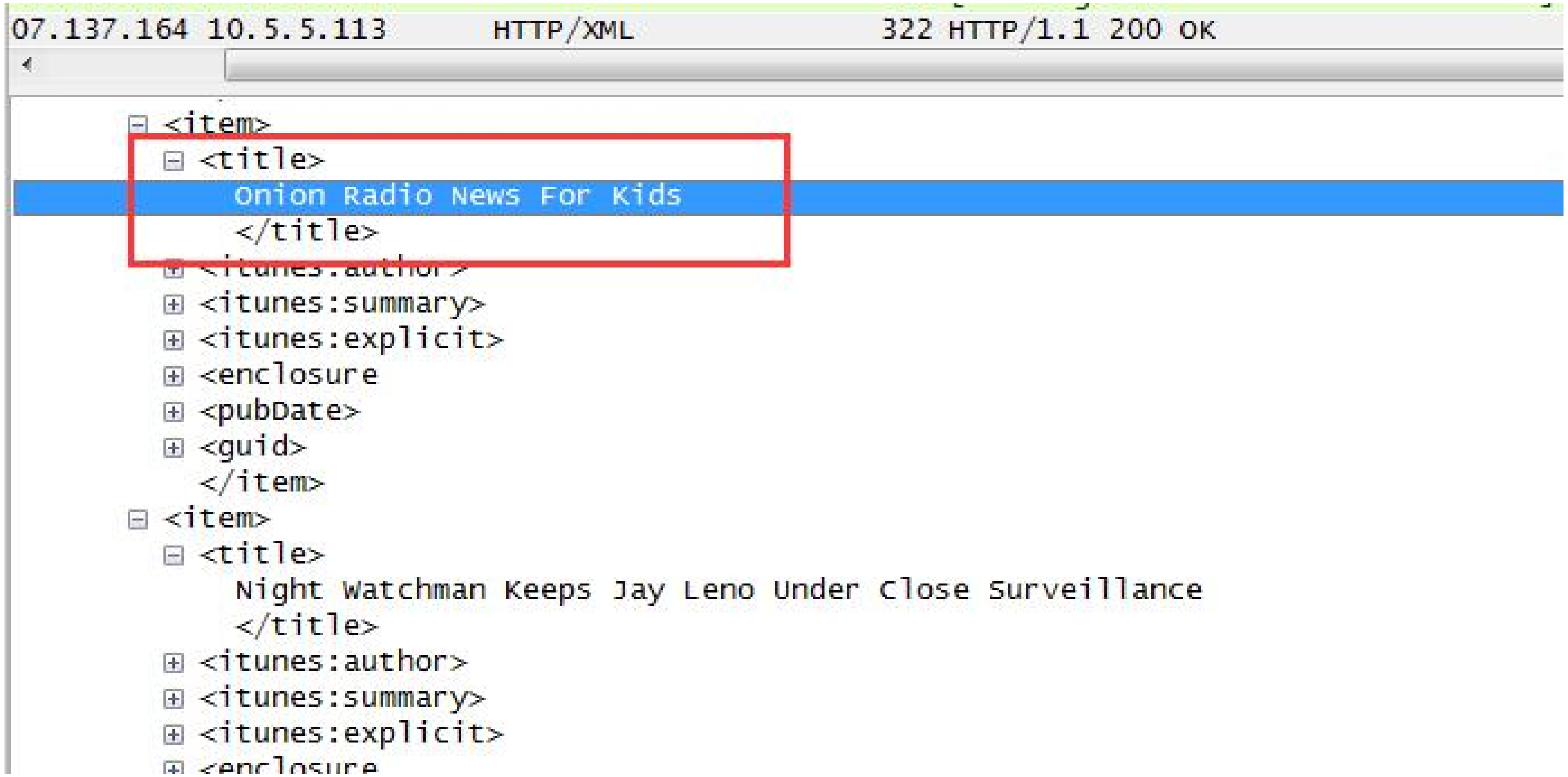
App Store – App Name → Solitaire



```
Destination     Protocol  Length  Info
204.0.59.50     HTTP       527 GET /bag.xml?ix=2 HTTP/1.1
204.0.59.50     HTTP       489 GET /bag.xml?ix=2 HTTP/1.1
204.0.59.58     HTTP       740 GET /WebObjects/MZSearch.woa/wa/search?submit=edit&term=solitaire%E2%80%8C%E2%80%8C%E2%80%8C%E2%80%
204.0.59.40     HTTP       439 POST /WebObjects/MZSoftwareUpdate.woa/wa/availableSoftwareUpdates HTTP/1.1  (application/x-apple-pl
66.235.139.54   HTTP       736 GET /b/ss/applesuperglobal/1/G.6--NS?h5=appleitmsnaapmb%2Cappleitmsusapmb&pccr=true&pageName=App%2
204.0.59.35     HTTP       613 GET /htmlResources/C6DA/k2-storefront-search.jsz HTTP/1.1
204.0.59.35     HTTP       611 GET /htmlResources/C6DA/k2-storefront-base.jsz HTTP/1.1
204.0.59.25     HTTP       676 GET /us/r1000/000/Purple/61/6b/da/mzl.xqzoyhet.75x75-65.jpg HTTP/1.1
204.0.59.25     HTTP       676 GET /us/r1000/026/Purple/52/e3/6c/mzl.djqwbjwi.75x75-65.jpg HTTP/1.1
204.0.59.35     HTTP       615 GET /htmlResources/C6DA/images/fat-binary-logo.png HTTP/1.1
66.235.139.54   HTTP      1180 GET /b/ss/applesuperglobal/1/H.20.3/s24120317876804?AQB=1&ndh=1&t=22/6/2010%2016%3A25%3A44%204%2024
204.0.59.25     HTTP       676 GET /us/r1000/040/Purple/21/4c/76/mzl.gjbagjuc.75x75-65.jpg HTTP/1.1
204.0.59.25     HTTP       676 GET /us/r1000/050/Purple/6e/77/37/mzl.tsoxohka.75x75-65.jpg HTTP/1.1
204.0.59.25     HTTP       707 GET /us/r1000/051/Purple/f9/82/58/mzl.rocrabzk.75x75-65.jpg HTTP/1.1
204.0.59.25     HTTP       707 GET /us/r1000/022/Purple/f4/40/4a/mzl.qfqcigoi.75x75-65.jpg HTTP/1.1
```

案例分享之我与美女黑客的约会

Podcast Title → Onion Radio News for Kids

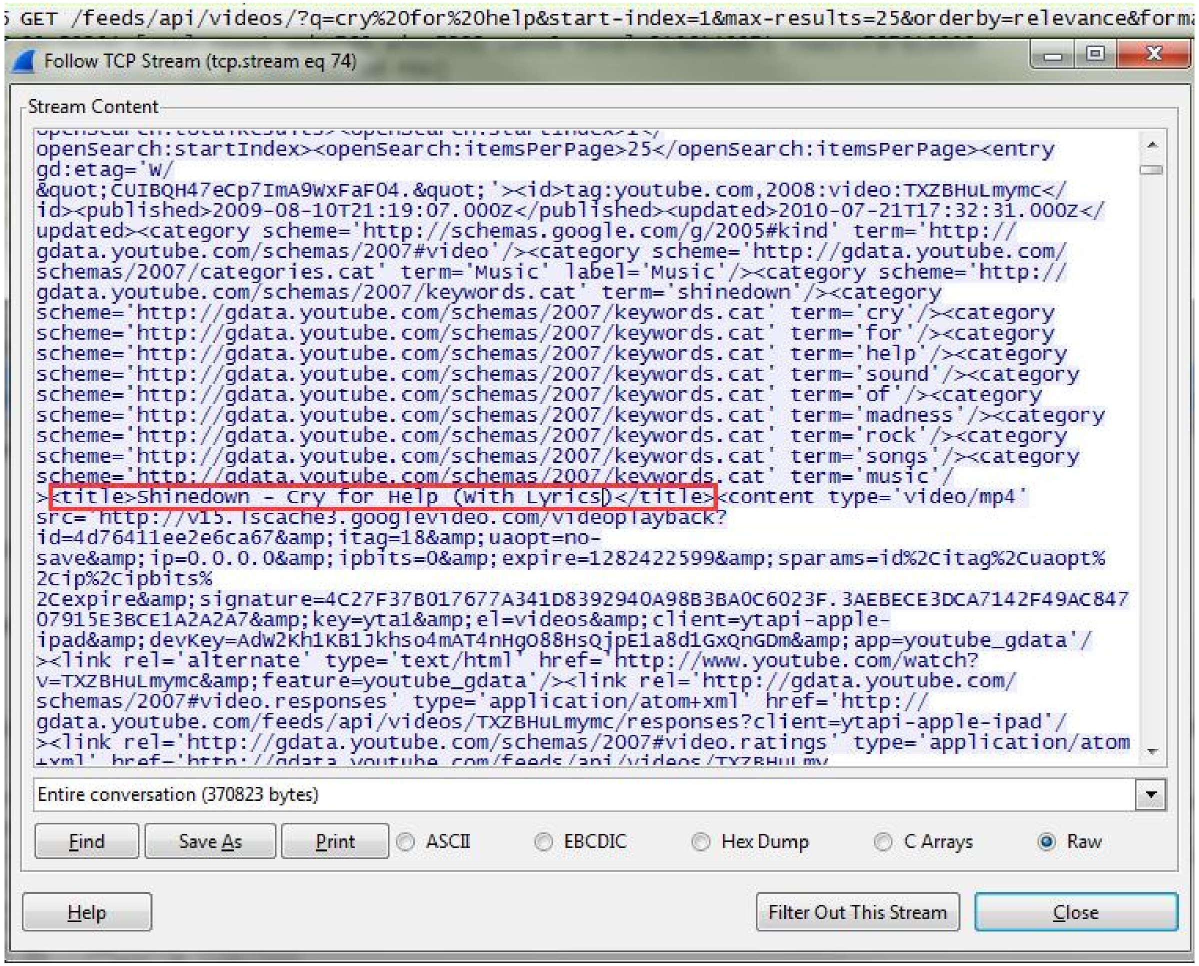


```
07.137.164 10.5.5.113        HTTP/XML                  322 HTTP/1.1 200 OK

      ⊟ <item>
        ⊟ <title>
            Onion Radio News For Kids
            </title>
        ⊞ <itunes:author>
        ⊞ <itunes:summary>
        ⊞ <itunes:explicit>
        ⊞ <enclosure
        ⊞ <pubDate>
        ⊞ <guid>
          </item>
      ⊟ <item>
        ⊟ <title>
            Night Watchman Keeps Jay Leno Under Close Surveillance
            </title>
        ⊞ <itunes:author>
        ⊞ <itunes:summary>
        ⊞ <itunes:explicit>
        ⊞ <enclosure
```

智者安天下

案例分享之我与美女黑客的约会

YouTube Video Title → Cry for Help



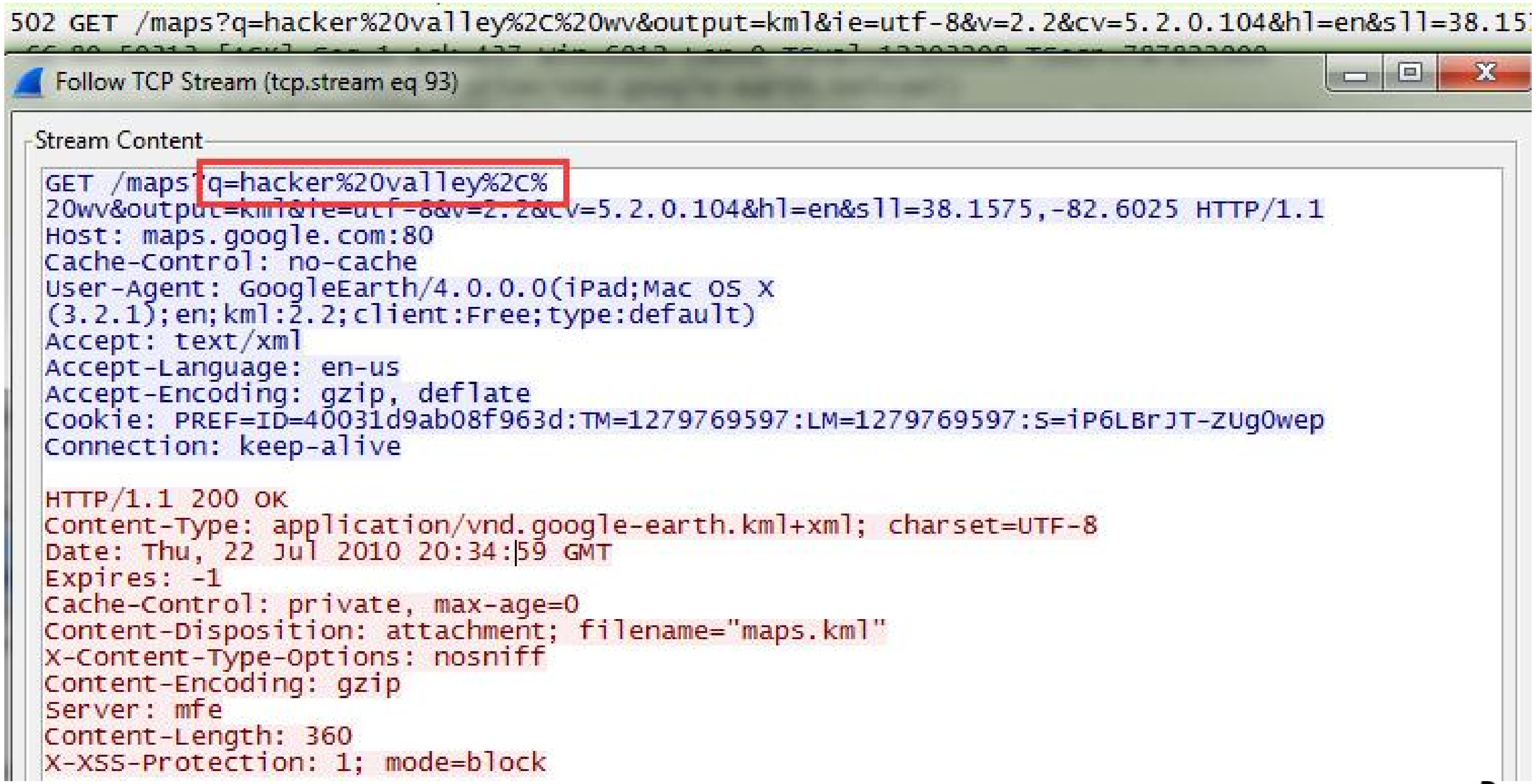
```
GET /feeds/api/videos/?q=cry%20for%20help&start-index=1&max-results=25&orderby=relevance&forma
```

```
openSearch:startIndex><openSearch:itemsPerPage>25</openSearch:itemsPerPage><entry
gd:etag='W/
&quot;CUIBQH47eCp7ImA9WxFaF04.&quot;'><id>tag:youtube.com,2008:video:TXZBHuLmymc</
id><published>2009-08-10T21:19:07.000Z</published><updated>2010-07-21T17:32:31.000Z</
updated><category scheme='http://schemas.google.com/g/2005#kind' term='http://
gdata.youtube.com/schemas/2007#video'/><category scheme='http://gdata.youtube.com/
schemas/2007/categories.cat' term='Music' label='Music'/><category scheme='http://
gdata.youtube.com/schemas/2007/keywords.cat' term='shinedown'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='cry'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='for'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='help'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='sound'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='of'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='madness'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='rock'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='songs'/><category
scheme='http://gdata.youtube.com/schemas/2007/keywords.cat' term='music'/
><title>Shinedown - Cry for Help (With Lyrics)</title><content type='video/mp4'
src='http://v15.lscache3.googlevideo.com/videoplayback?
id=4d76411ee2e6ca67&amp;itag=18&amp;uaopt=no-
save&amp;ip=0.0.0.0&amp;ipbits=0&amp;expire=1282422599&amp;sparams=id%2Citag%2Cuaopt%
2Cip%2Cipbits%
2Cexpire&amp;signature=4C27F37B017677A341D8392940A98B3BA0C6023F.3AEBECE3DCA7142F49AC847
07915E3BCE1A2A2A7&amp;key=yta1&amp;el=videos&amp;client=ytapi-apple-
ipad&amp;devKey=AdW2Kh1KB1Jkhso4mAT4nHgO88HsQjpE1a8d1GxQnGDm&amp;app=youtube_gdata'/
><link rel='alternate' type='text/html' href='http://www.youtube.com/watch?
v=TXZBHuLmymc&amp;feature=youtube_gdata'/><link rel='http://gdata.youtube.com/
schemas/2007#video.responses' type='application/atom+xml' href='http://
gdata.youtube.com/feeds/api/videos/TXZBHuLmymc/responses?client=ytapi-apple-ipad'/
><link rel='http://gdata.youtube.com/schemas/2007#video.ratings' type='application/atom
+xml' href='http://gdata.youtube.com/feeds/api/videos/TXZBHuLmy
```

Entire conversation (370823 bytes)

案例分享之我与美女黑客的约会

Google Earth City Name → Hacker Valley



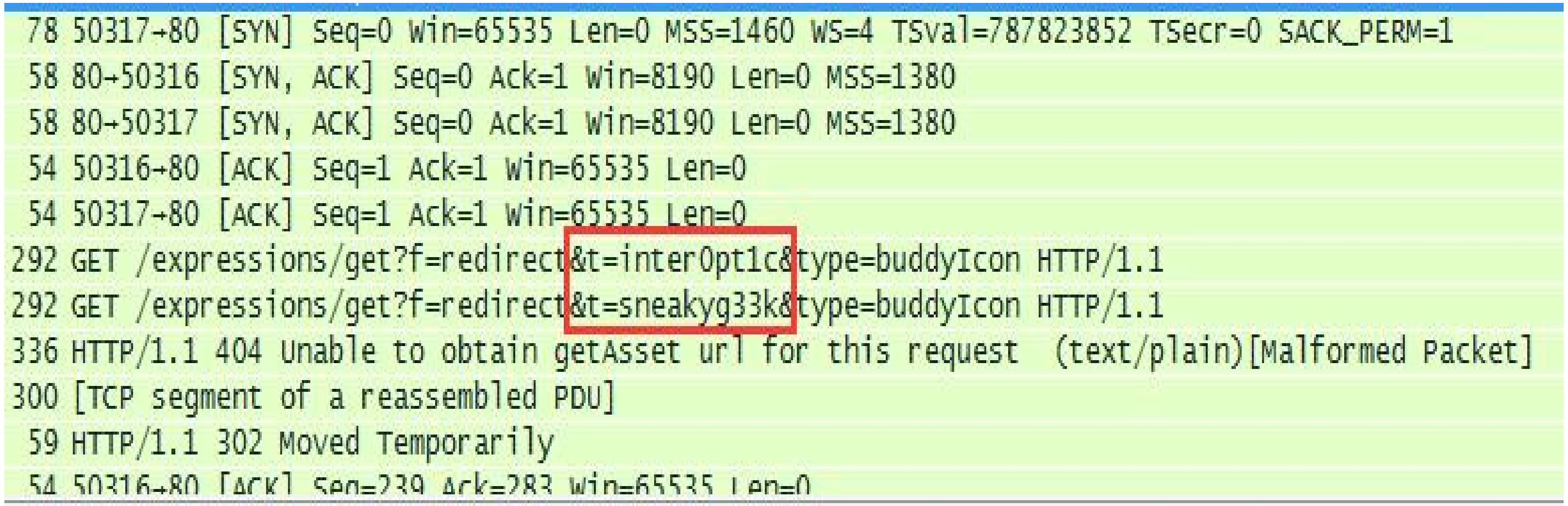
```
502 GET /maps?q=hacker%20valley%2C%20wv&output=kml&ie=utf-8&v=2.2&cv=5.2.0.104&hl=en&sll=38.15
```

```
GET /maps?q=hacker%20valley%2C%
20wv&output=kml&ie=utf-8&v=2.2&cv=5.2.0.104&hl=en&sll=38.1575,-82.6025 HTTP/1.1
Host: maps.google.com:80
Cache-Control: no-cache
User-Agent: GoogleEarth/4.0.0.0(iPad;Mac OS X
(3.2.1);en;kml:2.2;client:Free;type:default)
Accept: text/xml
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: PREF=ID=40031d9ab08f963d:TM=1279769597:LM=1279769597:S=iP6LBrJT-ZUg0wep
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: application/vnd.google-earth.kml+xml; charset=UTF-8
Date: Thu, 22 Jul 2010 20:34:59 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Disposition: attachment; filename="maps.kml"
X-Content-Type-Options: nosniff
Content-Encoding: gzip
Server: mfe
Content-Length: 360
X-XSS-Protection: 1; mode=block
```

智者安天下

案例分享之我与美女黑客的约会

AIM Buddy Name → Inter0pt1c或sneakyg33k



```
 78 50317→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 TSval=787823852 TSecr=0 SACK_PERM=1
 58 80→50316 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380
 58 80→50317 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380
 54 50316→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 54 50317→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
292 GET /expressions/get?f=redirect&t=inter0pt1c&type=buddyIcon HTTP/1.1
292 GET /expressions/get?f=redirect&t=sneakyg33k&type=buddyIcon HTTP/1.1
336 HTTP/1.1 404 Unable to obtain getAsset url for this request  (text/plain)[Malformed Packet]
300 [TCP segment of a reassembled PDU]
 59 HTTP/1.1 302 Moved Temporarily
 54 50316→80 [ACK] Seq=239 Ack=283 Win=65535 Len=0
```

智者安天下

案例分享之我与美女黑客的约会

App Store - App Name

Podcast Title

YouTube Video Title

Google Earth City Name

AIM Buddy Name

Solitaire

Onion Radio News for Kids

Cry for Help

Hacker Valley

Inter0pt1c或sneakyg33k

➔ SOCHI 或 SOCHS

智者安天下

总结

回顾

- Wireshark特性
  - 系统结构
  - 数据捕获及解析流程
  - OSI七层模型
- 网络协议分析
  - TCP
  - UDP
  - DNS
  - HTTP
- 网络特征分析
  - 特征分析流程
  - 特征匹配及实例
  - 特征提取实例
  - 网络特征库
- 案例分享
  - 银行盗号木马
  - 非授权通信
  - 美女黑客之约

智者安天下

感谢大家参与本次交流！

www.antiy.com

智者安天下