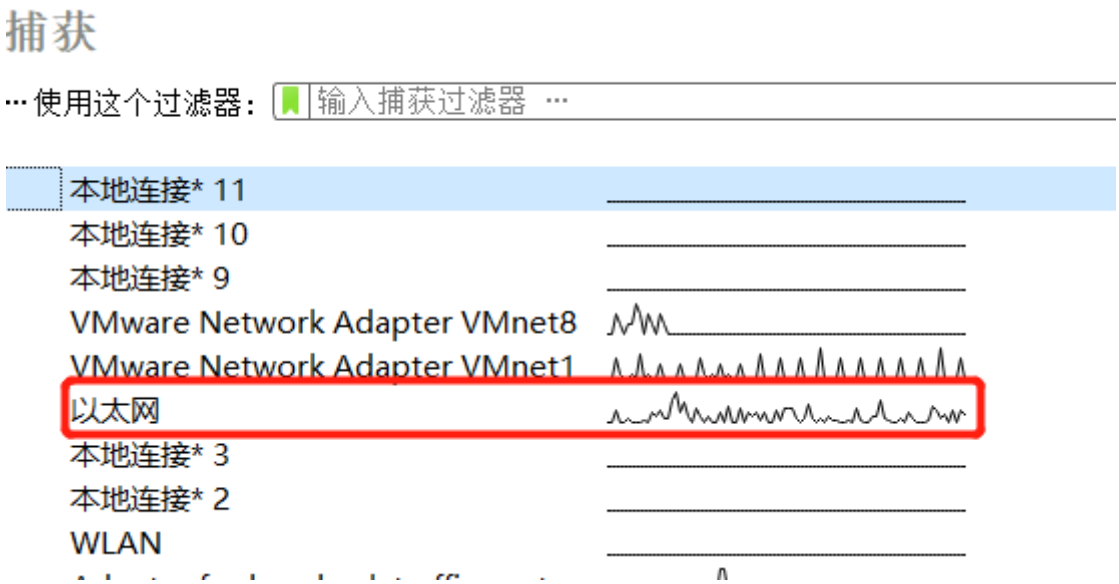
抓包实践及pcap包分析

1. 脉脉App抓包分析

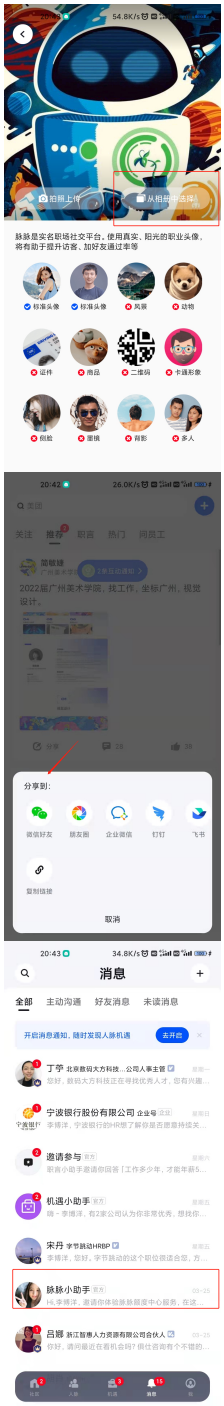
   由于校园网内的无关流量非常多，因此手机连接热点之后首先wireshark收集无关背景流量，找到热点所在的网卡“以太网”，进行抓包操作。



   分析无关背景流量可以看出存在大量的 BroadCast，Ipv6地址数据包，都是局域网内的数据包，与数据传输没有关系。

108.987665	Tp-LinkT_5a:08:5c	Broadcast	ARP
109.067032	BeijingX_ee:f0:60	Broadcast	ARP
0.339422	fe80::46f9:71ff:fe7…	ff02::1:2	DHCPv6
0.346402	fe80::46f9:71ff:fe7…	ff02::1:2	DHCPv6
0.385369	fe80::520f:f5ff:fee…	ff02::1:2	DHCPv6
1.167653	fe80::520f:f5ff:fed…	ff02::1:2	DHCPv6
1.582290	fe80::520f:f5ff:fea…	ff02::1:2	DHCPv6
1.714169	fe80::addc:369e:4ae…	ff02::1:2	DHCPv6
2.001871	fe80::520f:f5ff:fea…	ff02::1:2	DHCPv6

   随即进行特定应用的网络通信的数据抓包，第一个指定的app是脉脉，对脉脉进行登录转发帖子，查看消息，以及上传头像等操作。



接着对这一系列操作进行抓包后保存为pcap文件 。接着将无关流量的特征筛选出关于进行网络通信的相关流量。可以得到的关于脉脉app的网络协议报文有DNS（udp），TLS，HTTP，TCP协议报文。因此将其分类对其分析内容。

分析 DNS报文内容，可以用明文查看其查询域名和响应报文的地址。

登陆时，dns报文查询获得的域名向域名服务器查询(api.taou.com和open.taou.com)

```
1 0.000000      10.211.18.135        8.8.8.8              DNS         72 Standard query 0xf0c6 A api.taou.com
2 0.000017      10.211.18.135        8.8.8.8              DNS         73 Standard query 0x3220 A open.taou.com
3 0.000139      10.211.18.135        8.8.8.8              DNS         73 Standard query 0x1358 A open.taou.com
1: protocol:dns src=10.211.18.135:61475 dst=8.8.8.8:53
.api.taou.com.....
2: protocol:dns src=10.211.18.135:61476 dst=8.8.8.8:53
.open.taou.com.....
3: protocol:dns src=10.211.18.135:61477 dst=8.8.8.8:53
.open.taou.com.....
```

同理，域名服务器分别返回域名的ip地址并且都指向maimai.cn

```
4: protocol:dns src=8.8.8.8:53 dst=10.211.18.135:61475
.api.taou.com.................maimai.cn..*.........106:75:23:100:
5: protocol:dns src=8.8.8.8:53 dst=10.211.18.135:61477
.open.taou.com.................maimai.cn..+.........106:75:23:100:
6: protocol:dns src=8.8.8.8:53 dst=10.211.18.135:61476
.open.taou.com.............!...maimai.cn..+.......1.106:75:23:100:
Standard query response 0xf0c6 A api.taou.com CNAME maimai.cn A 106.75.23.100
Standard query response 0x1358 A open.taou.com CNAME maimai.cn A 106.75.23.100
Standard query response 0x3220 A open.taou.com CNAME maimai.cn A 106.75.23.100
```

在接下来的转发帖子，查看消息以及上传头像的操作中。dns报文都去查询以下的cdn服务器(七牛和金山云)，进行数据传输和接受。

```
7: protocol:dns src=10.211.18.135:61481 dst=8.8.8.8:53
.i9.taou.com.....
8: protocol:dns src=8.8.8.8:53 dst=10.211.18.135:61481
.i9.taou.com.............".
7xi2l68u.v5.com.z0.glb.qiniudns...).......D...opencdnqiniustaticv6.jomodns...W.........
14:29:98:41:.W.........111:170:26:41:
Standard query 0xdc62 A i9.taou.com
Standard query response 0xdc62 A i9.taou.com CNAME 7xi2l68u.v5.com.z0.glb.qiniudns.com CNAME opencdnqini…
```

```
11: protocol:dns src=10.211.18.135:61491 dst=8.8.8.8:53
.maimai.cn.....
12: protocol:dns src=10.211.18.135:61492 dst=8.8.8.8:53
.dl.taou.com.....
13: protocol:dns src=8.8.8.8:53 dst=10.211.18.135:61491
.maimai.cn..............3.106:75:23:100:
14: protocol:dns src=8.8.8.8:53 dst=10.211.18.135:61492
.dl.taou.com.................dl116:97:111:117:.com.download.ks-
cdn...).......X...k1103:115:108:98:.ksyuncdn...S.......c.116:130:197:1:.S.......c.
0xe3f6 A maimai.cn
0x6f1f A dl.taou.com
response 0xe3f6 A maimai.cn A 106.75.23.100
response 0x6f1f A dl.taou.com CNAME dl.taou.com.download.ks-cdn.com CNAME k1.gslb.ksyuncd…
```

接着分析HTTP报文中文本。因为是明文传输，解析其中的host，content-type等信息通过文本匹配的方式解析其中内容，得到如下文本。

```
8: protocol:tcp src=10.211.18.135:61572 dst=47.95.50.1:80 header length:20  tcp flags:PSH_ACK
host::daa.shuzilm.cn
contentype:  application/json
User-Agent:
9: protocol:tcp src=47.95.50.1:80 dst=10.211.18.135:61572 header length:20  tcp flags:PSH_ACK
host::daa.shuzilm.cn
contentype:  application/json;32charset=utf8
User-Agent:
```

Wireshark · 分组 8 · http.pcap

```
    Sequence Number (raw): 1926830859
    [Next Sequence Number: 968    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2744785204
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 128
    [Calculated window size: 128]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x7a60 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (967 bytes)
v Hypertext Transfer Protocol
  > POST /report?v=1.1&c=1&e=1&p=4EAA6523E31E4CA7F19C919BB82DA869 HTTP/1.1\r\n
    Accept: application/json\r\n
    Content-Type: application/json\r\n
  > Content-Length: 768\r\n
    Host: daa.shuzilm.cn\r\n
    Connection: Keep-Alive\r\n
```

接着通过分析http包中的User-Agent，则能得到当前报文的发送用户的设备信息，可以得到如下

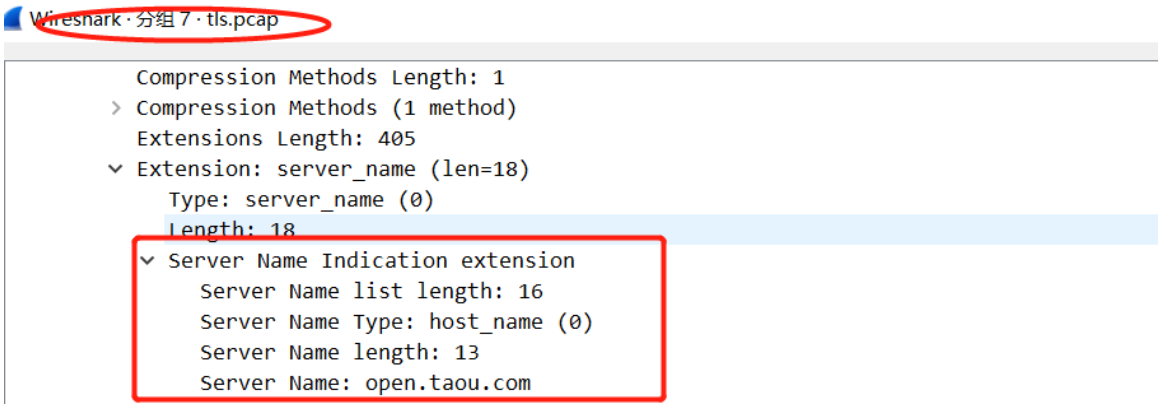
```
37: protocol:tcp src=10.211.18.135:61580 dst=8.131.112.227:80 header length:20  tcp flag
host::8.131.112.227
contentype:  application/octet-stream
User-Agent:     Dalvik/2.1.032(Linux;32U;32Android3212;32Mi321032Build/SKQ1.211230.001)
38: protocol:tcp src=8.131.112.227:80 dst=10.211.18.135:61580 header length:20  tcp flag
host::8.131.112.227
contentype:  application/octet-stream
User-Agent:     Dalvik/2.1.032(Linux;32U;32Android3212;32Mi321032Build/SKQ1.211230.001)
```

与实现操作的移动设备系统设备一致，mi10，Android12(图中的32是ascii码，在http文本中为空格)

接下来解析 加密报文TLS，TLS本身就是TCP协议报文，所以会解析基本的报文信息，分析tcp的报文ip，端口以及当前报文的flags。接下来解析TLS报文中的cipher suite。当client发出hello请求时，client发送的报文的中携带着client可以使用的cipher suite集合。而当server回应之后，会回应之后通信使用的cipher，并且解析。在Hello报文的TLS层的扩展中，有固定格式的server name内容。如图：

```
7: protocol:tcp src=10.211.18.135:61480 dst=106.75.23.100:443 header length:32  tcp flags:PSH_ACK
client hello    client cipher suite:no.0: 1301 no.1: 1302 no.2: 1303 no.3: ffffc02b no.4: ffffc02c no.5:
ffffcba9 no.6: ffffc02f no.7: ffffc030 no.8: ffffcba8 no.9: ffffc013 no.10: ffffc014 no.11: ffffff9c no.12:
ffffff9d no.13: 2f no.14: 35
server name:open.taou.com
8: protocol:tcp src=106.75.23.100:443 dst=10.211.18.135:61478 header length:32  tcp flags:ACK
server hello    server cipher suite:server response cipher: 1301
```

分别是client hello和server hello报文，client发送的cipher suite有15个cipher，最终server回应0x1301的cipher方式。同时client hello中打印出extension中的server name。



2. vimeo 网站 抓包实践分析

vimeo是一个美国的视频网站，因此在外网进行了登录，和观看视频的操作。

```
105: protocol:dns src=192.168.1.159:49231 dst=192.168.1.254:53
.vimeo.com..A..
106: protocol:dns src=192.168.1.159:52552 dst=192.168.1.254:53
.vimeo.com.....
107: protocol:dns src=192.168.1.159:56667 dst=192.168.1.254:53
.js-agent.newrelic.com..A..
108: protocol:dns src=192.168.1.159:56939 dst=192.168.1.254:53
.js-agent.newrelic.com.....
109: protocol:dns src=192.168.1.159:54489 dst=192.168.1.254:53
.cdn.cookielaw.org..A..
110: protocol:dns src=192.168.1.159:49236 dst=192.168.1.254:53
.cdn.cookielaw.org.....
111: protocol:dns src=192.168.1.159:52256 dst=192.168.1.254:53
.www.googleadservices.com..A..
112: protocol:dns src=192.168.1.159:59413 dst=192.168.1.254:53
.www.googleadservices.com.....
113: protocol:dns src=192.168.1.159:56692 dst=192.168.1.254:53
.cdn.pdst.fm..A..
114: protocol:dns src=192.168.1.159:58467 dst=192.168.1.254:53
.cdn.pdst.fm.....
115: protocol:dns src=192.168.1.159:52518 dst=192.168.1.254:53
.websdk.appsflyer.com..A..
116: protocol:dns src=192.168.1.159:52383 dst=192.168.1.254:53
.websdk.appsflyer.com.....
117: protocol:dns src=192.168.1.159:60289 dst=192.168.1.254:53
.cdn.taboola.com..A..
118: protocol:dns src=192.168.1.159:58256 dst=192.168.1.254:53
.cdn.taboola.com.....
119: protocol:dns src=192.168.1.159:58587 dst=192.168.1.254:53
.www.facebook.com..A..
120: protocol:dns src=192.168.1.159:57576 dst=192.168.1.254:53
.www.facebook.com.....
121: protocol:dns src=192.168.1.254:53 dst=192.168.1.159:49231
.vimeo.com..A.............A.ns-70.awsdns-08...awsdns-hostmaster.amazon..x..0:1:81:128:.....:....,
```

在登录vimeo使用google账号登录，因此直接得到googleservices的域名进行授权登录。并且不断查询合适的cdn服务器进行服务。

```
Standard query 0xeeb2 HTTPS vimeo.com
Standard query 0xb5d3 A vimeo.com
Standard query 0x0fd1 HTTPS js-agent.newrelic.com
Standard query 0xf3ae A js-agent.newrelic.com
Standard query 0x88f4 HTTPS cdn.cookielaw.org
Standard query 0x7f42 A cdn.cookielaw.org
Standard query 0xbe32 HTTPS www.googleadservices.com
Standard query 0x731f A www.googleadservices.com
Standard query 0x0ce3 HTTPS cdn.pdst.fm
Standard query 0xff0d A cdn.pdst.fm
Standard query 0x7b76 HTTPS websdk.appsflyer.com
Standard query 0x8b52 A websdk.appsflyer.com
Standard query 0xdf5c HTTPS cdn.taboola.com
Standard query 0x1da1 A cdn.taboola.com
```

在登陆时使用了tls协议报文进行加密通信交换登录信息密钥。

```
403: protocol:tcp src=192.168.1.159:56267 dst=146.75.0.217:443 header length:32  tcp flags:PSH_ACK
Client hello:   client cipher suite:no.1: ffffa9aa  no.2: 1301  no.3: 1302  no.4: 1303  no.5:
ffffc02c  no.6: ffffc02b  no.7: ffffcba9  no.8: ffffc030  no.9: ffffc02f  no.10: ffffcba8  no.11:
ffffc00a  no.12: ffffc009  no.13: ffffc014  no.14: ffffc013  no.15: ffffff9d  no.16: ffffff9c  no.
17: 0035  no.18: 002f  no.19: ffffc008  no.20: ffffc012  no.21: 000a
Server name:player.vimeo.com
```

可以解析tls报文 的 cipher suite，以及server name，该值指向player.vimeo.com。

在登录之后点击视频播放，播放过程中从服务器的端口443进行传输，并且是udp报文，因此在播放过程中vimeo使用quic协议进行加密传输视频。没有对quic协议进行揭秘分析。同样通过对http中的user-agent进行解析抓取可以得到设备信息

```
1028: protocol:quic src=192.168.1.159:64840 dst=172.224.38.133:443
1029: protocol:quic src=172.224.38.133:443 dst=192.168.1.159:64840
1030: protocol:quic src=172.224.38.133:443 dst=192.168.1.159:64840
1031: protocol:quic src=172.224.38.133:443 dst=192.168.1.159:64840
1032: protocol:quic src=172.224.38.133:443 dst=192.168.1.159:64840
```

```
2960: protocol:tcp src=142.250.187.99:80 dst=192.168.1.159:56277 hea
host::ocsp.pki.goog
contentype:  p response
User-Agent:     com.apple.trustd/2.2
2961: protocol:tcp src=142.250.187.174:443 dst=192.168.1.159:56297
```