Clash Royale黑盒分析

和千风 cfc4n@cnxct.com

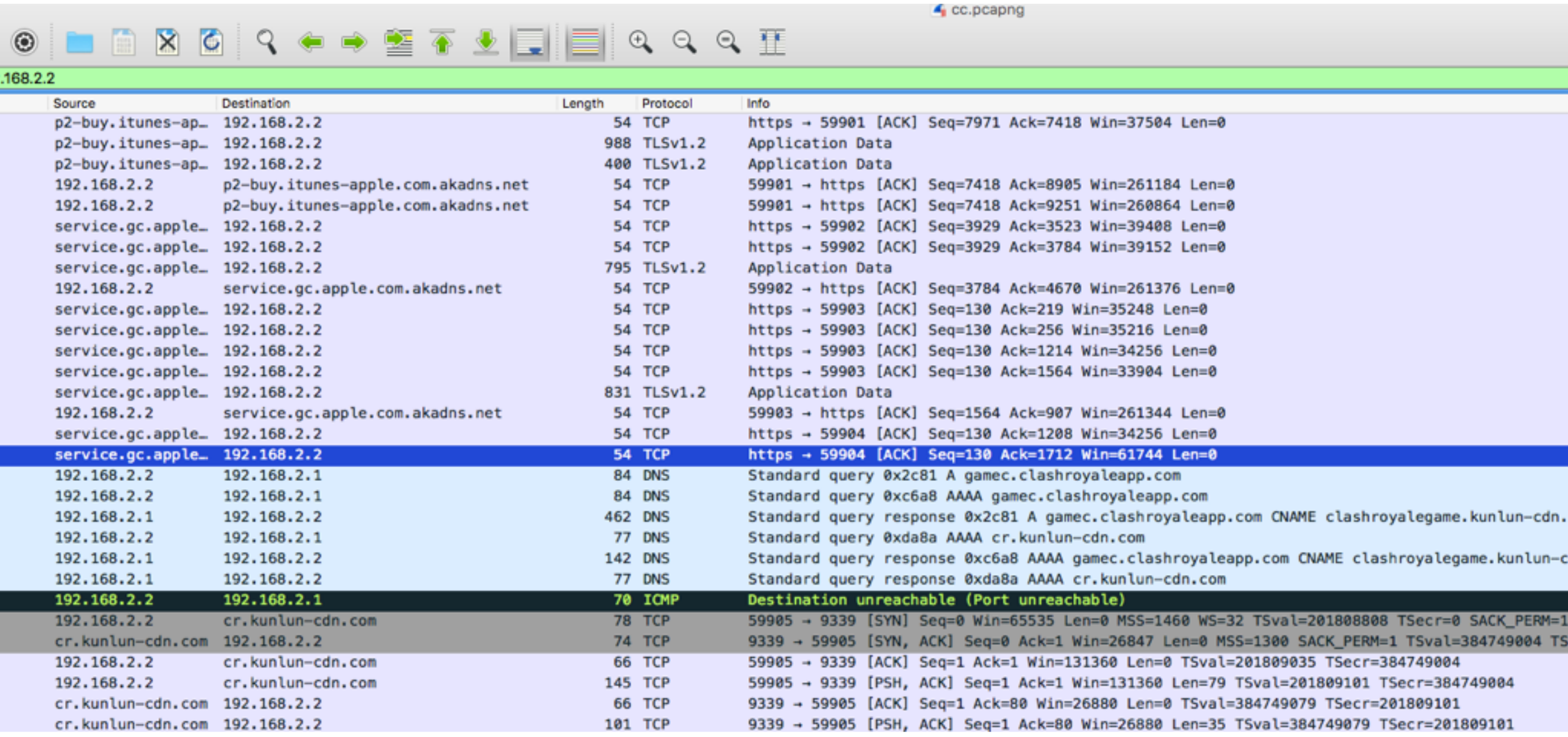
环境

- ios设备一部，并安装该游戏
- 有WIFI+有线网络的PC一台（借用了前端发布机MAC PRO）
- 后来在genymotion虚拟机上部署了环境

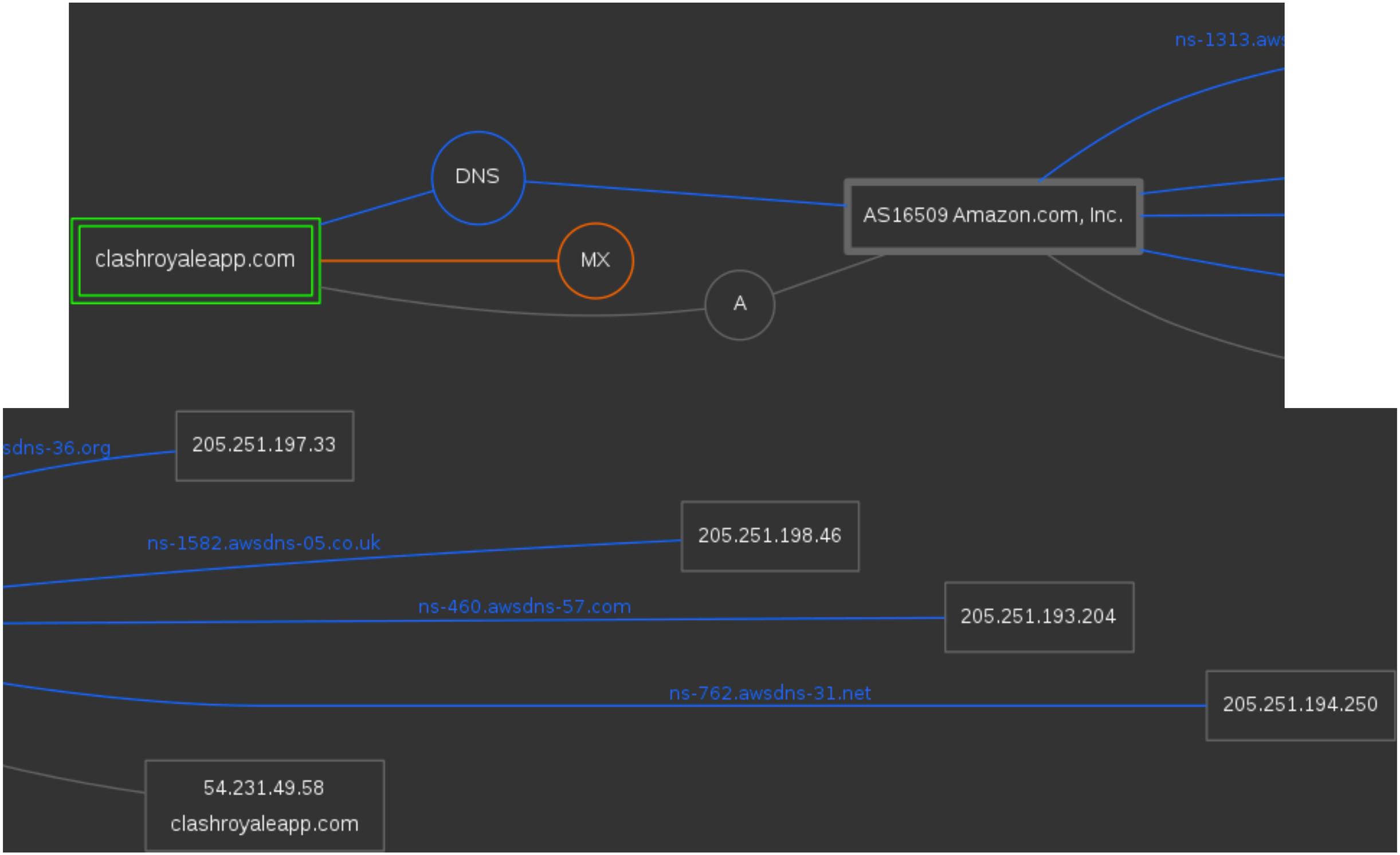
抓包步骤

- wifi开共享，用有线连接外网
- 手机连接共享的WIFI SSID
- 在mac pro上开wireshark抓包
- 手机登录游戏，玩一会游戏

查找服务器IP


cc.pcapng
.168.2.2
Source Destination Length Protocol Info
p2-buy.itunes-ap… 192.168.2.2 54 TCP https → 59901 [ACK] Seq=7971 Ack=7418 Win=37504 Len=0
p2-buy.itunes-ap… 192.168.2.2 988 TLSv1.2 Application Data
p2-buy.itunes-ap… 192.168.2.2 400 TLSv1.2 Application Data
192.168.2.2 p2-buy.itunes-apple.com.akadns.net 54 TCP 59901 → https [ACK] Seq=7418 Ack=8905 Win=261184 Len=0
192.168.2.2 p2-buy.itunes-apple.com.akadns.net 54 TCP 59901 → https [ACK] Seq=7418 Ack=9251 Win=260864 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59902 [ACK] Seq=3929 Ack=3523 Win=39408 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59902 [ACK] Seq=3929 Ack=3784 Win=39152 Len=0
service.gc.apple… 192.168.2.2 795 TLSv1.2 Application Data
192.168.2.2 service.gc.apple.com.akadns.net 54 TCP 59902 → https [ACK] Seq=3784 Ack=4670 Win=261376 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59903 [ACK] Seq=130 Ack=219 Win=35248 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59903 [ACK] Seq=130 Ack=256 Win=35216 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59903 [ACK] Seq=130 Ack=1214 Win=34256 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59903 [ACK] Seq=130 Ack=1564 Win=33904 Len=0
service.gc.apple… 192.168.2.2 831 TLSv1.2 Application Data
192.168.2.2 service.gc.apple.com.akadns.net 54 TCP 59903 → https [ACK] Seq=1564 Ack=907 Win=261344 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59904 [ACK] Seq=130 Ack=1208 Win=34256 Len=0
service.gc.apple… 192.168.2.2 54 TCP https → 59904 [ACK] Seq=130 Ack=1712 Win=61744 Len=0
192.168.2.2 192.168.2.1 84 DNS Standard query 0x2c81 A gamec.clashroyaleapp.com
192.168.2.2 192.168.2.1 84 DNS Standard query 0xc6a8 AAAA gamec.clashroyaleapp.com
192.168.2.1 192.168.2.2 462 DNS Standard query response 0x2c81 A gamec.clashroyaleapp.com CNAME clashroyalegame.kunlun-cdn.
192.168.2.2 192.168.2.1 77 DNS Standard query 0xda8a AAAA cr.kunlun-cdn.com
192.168.2.1 192.168.2.2 142 DNS Standard query response 0xc6a8 AAAA gamec.clashroyaleapp.com CNAME clashroyalegame.kunlun-c
192.168.2.1 192.168.2.2 77 DNS Standard query response 0xda8a AAAA cr.kunlun-cdn.com
192.168.2.2 192.168.2.1 70 ICMP Destination unreachable (Port unreachable)
192.168.2.2 cr.kunlun-cdn.com 78 TCP 59905 → 9339 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=201808808 TSecr=0 SACK_PERM=1
cr.kunlun-cdn.com 192.168.2.2 74 TCP 9339 → 59905 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1300 SACK_PERM=1 TSval=384749004 TS
192.168.2.2 cr.kunlun-cdn.com 66 TCP 59905 → 9339 [ACK] Seq=1 Ack=1 Win=131360 Len=0 TSval=201809035 TSecr=384749004
192.168.2.2 cr.kunlun-cdn.com 145 TCP 59905 → 9339 [PSH, ACK] Seq=1 Ack=1 Win=131360 Len=79 TSval=201809101 TSecr=384749004
cr.kunlun-cdn.com 192.168.2.2 66 TCP 9339 → 59905 [ACK] Seq=1 Ack=80 Win=26880 Len=0 TSval=384749079 TSecr=201809101
cr.kunlun-cdn.com 192.168.2.2 101 TCP 9339 → 59905 [PSH, ACK] Seq=1 Ack=80 Win=26880 Len=35 TSval=384749079 TSecr=201809101

确认域名


ns-1313.aws
DNS
clashroyaleapp.com
MX
A
AS16509 Amazon.com, Inc.
sdns-36.org
205.251.197.33
ns-1582.awsdns-05.co.uk
205.251.198.46
ns-460.awsdns-57.com
205.251.193.204
ns-762.awsdns-31.net
205.251.194.250
54.231.49.58
clashroyaleapp.com

域名相关

- A记录?
- NS记录?
- CNAME?

whois

- Domain Name: clashroyaleapp.com
- Registry Domain ID: 1970575925_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.comlaude.com
- Registrar URL: http://www.comlaude.com
- Updated Date: 2016-02-15T11:01:48Z
- Creation Date: 2015-10-21T16:11:09Z
- Registrar Registration Expiration Date: 2016-10-21T00:00:00Z
- Registrar: NOM-IQ Ltd dba Com Laude
- Registrar IANA ID: 470
- Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
- Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
- Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
- Registry Registrant ID:
- Registrant Name: Domain Manager

whois

- 设置域名保护
- 注册商为伦敦comlaude
- 排除国内代理商的域名，多数为SuperCell

Name Server

- NS-1313.AWSDNS-36.ORG
- NS-1582.AWSDNS-05.CO.UK
- NS-460.AWSDNS-57.COM
- NS-762.AWSDNS-31.NET
- 都为亚马逊云的服务器

A记录

- Bangkok, Thailand 54.231.49.82
- Auckland, New Zealand 54.231.82.129
- Toronto, Canada 54.231.49.249
- Paris, France 54.231.48.42
- Frankfurt, Germany 54.231.50.49
- Arizona, United States 54.231.1.188
- Washington DC, United States 54.231.48.106
- Sydney, Australia 54.231.0.172
- Beijing, China 54.231.14.140
- Tokyo, Japan 54.231.12.164
- Monterrey, Mexico 54.231.18.244
- Johannesburg, South Africa 54.231.9.188
- Moscow, Russia 54.231.19.20
- Manchester, United Kingdom 54.231.17.52

海外用哪个域名?

- 常识性排除主域名

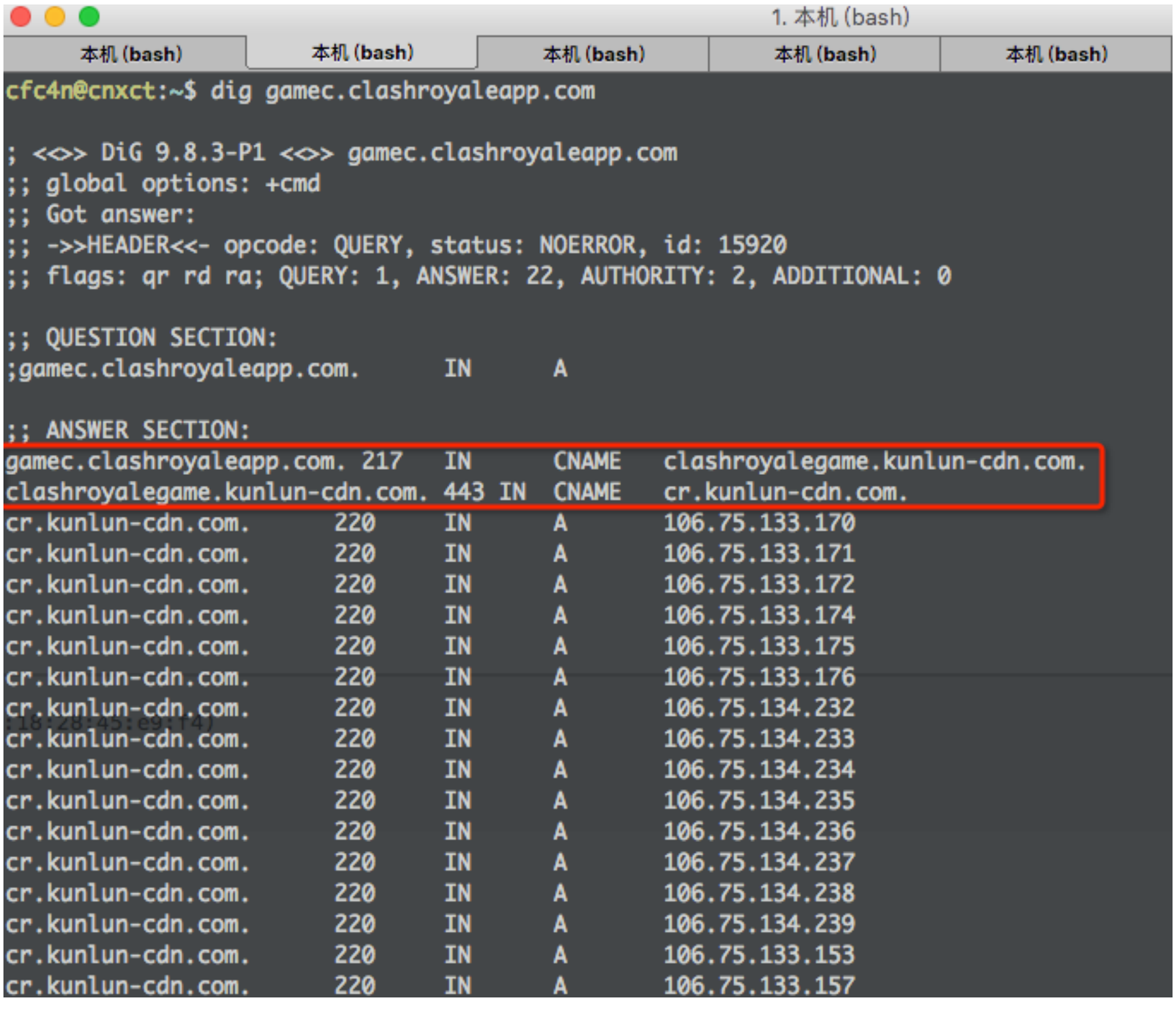
- 暂停，先分析下抓包得到的二级域名

分析专属域名

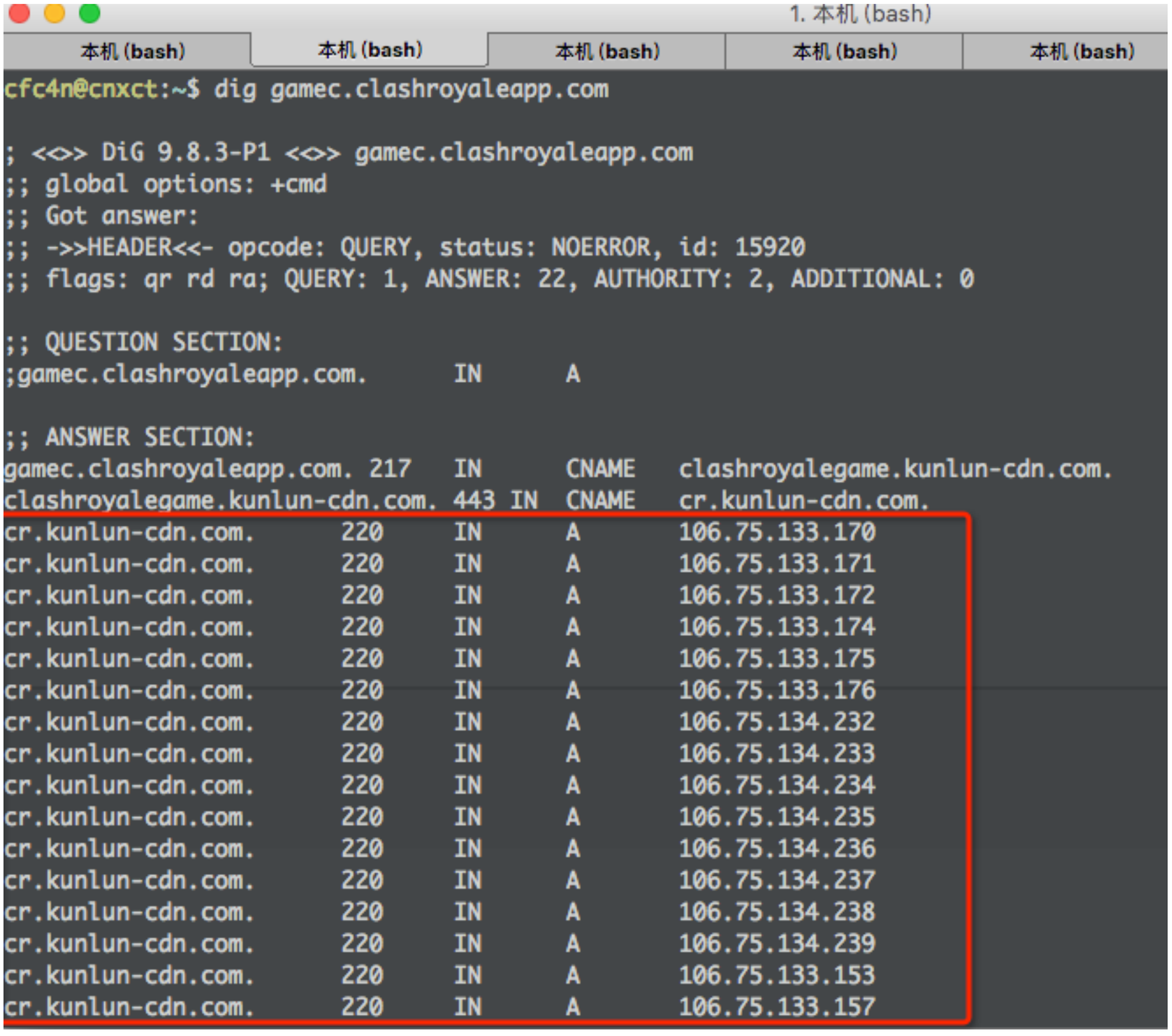
- 从结果来看游戏发起A 记录gamec.clashroyaleapp.com查询

- 查询结果为CNAME记录，CNAME到clashroyalegame.kunlun-cdn.com ， 再CNAME到 cr.kunlun-cdn.com

CNAME


1. 本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
cfc4n@cnxct:~$ dig gamec.clashroyaleapp.com
; <<>> DiG 9.8.3-P1 <<>> gamec.clashroyaleapp.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15920
;; flags: qr rd ra; QUERY: 1, ANSWER: 22, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;gamec.clashroyaleapp.com. IN A
;; ANSWER SECTION:
gamec.clashroyaleapp.com. 217 IN CNAME clashroyalegame.kunlun-cdn.com.
clashroyalegame.kunlun-cdn.com. 443 IN CNAME cr.kunlun-cdn.com.
cr.kunlun-cdn.com. 220 IN A 106.75.133.170
cr.kunlun-cdn.com. 220 IN A 106.75.133.171
cr.kunlun-cdn.com. 220 IN A 106.75.133.172
cr.kunlun-cdn.com. 220 IN A 106.75.133.174
cr.kunlun-cdn.com. 220 IN A 106.75.133.175
cr.kunlun-cdn.com. 220 IN A 106.75.133.176
cr.kunlun-cdn.com. 220 IN A 106.75.134.232
cr.kunlun-cdn.com. 220 IN A 106.75.134.233
cr.kunlun-cdn.com. 220 IN A 106.75.134.234
cr.kunlun-cdn.com. 220 IN A 106.75.134.235
cr.kunlun-cdn.com. 220 IN A 106.75.134.236
cr.kunlun-cdn.com. 220 IN A 106.75.134.237
cr.kunlun-cdn.com. 220 IN A 106.75.134.238
cr.kunlun-cdn.com. 220 IN A 106.75.134.239
cr.kunlun-cdn.com. 220 IN A 106.75.133.153
cr.kunlun-cdn.com. 220 IN A 106.75.133.157

DNS轮训


1. 本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
cfc4n@cnxct:~$ dig gamec.clashroyaleapp.com
; <<>> DiG 9.8.3-P1 <<>> gamec.clashroyaleapp.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15920
;; flags: qr rd ra; QUERY: 1, ANSWER: 22, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;gamec.clashroyaleapp.com. IN A
;; ANSWER SECTION:
gamec.clashroyaleapp.com. 217 IN CNAME clashroyalegame.kunlun-cdn.com.
clashroyalegame.kunlun-cdn.com. 443 IN CNAME cr.kunlun-cdn.com.
cr.kunlun-cdn.com. 220 IN A 106.75.133.170
cr.kunlun-cdn.com. 220 IN A 106.75.133.171
cr.kunlun-cdn.com. 220 IN A 106.75.133.172
cr.kunlun-cdn.com. 220 IN A 106.75.133.174
cr.kunlun-cdn.com. 220 IN A 106.75.133.175
cr.kunlun-cdn.com. 220 IN A 106.75.133.176
cr.kunlun-cdn.com. 220 IN A 106.75.134.232
cr.kunlun-cdn.com. 220 IN A 106.75.134.233
cr.kunlun-cdn.com. 220 IN A 106.75.134.234
cr.kunlun-cdn.com. 220 IN A 106.75.134.235
cr.kunlun-cdn.com. 220 IN A 106.75.134.236
cr.kunlun-cdn.com. 220 IN A 106.75.134.237
cr.kunlun-cdn.com. 220 IN A 106.75.134.238
cr.kunlun-cdn.com. 220 IN A 106.75.134.239
cr.kunlun-cdn.com. 220 IN A 106.75.133.153
cr.kunlun-cdn.com. 220 IN A 106.75.133.157

所有可见服务器

- 106.75.133.* 「20台」中国广东广州 ucloud.cn 电信/联通
- 106.75.134.* 「10台」中国广东广州 ucloud.cn 电信/联通
- 106.75.135.* 「7台」中国广东广州 ucloud.cn 电信/联通
- 106.75.140.* 「3台」中国广东广州 ucloud.cn 电信/联通

截止至2016-03-17

Name Server

cfc4n@cnxct:~$ dig gamec.clashroyaleapp.com

;; AUTHORITY SECTION:

kunlun-cdn.com. 22379 IN NS ns3.dnsv5.com.

kunlun-cdn.com. 22379 IN NS ns4.dnsv5.com.

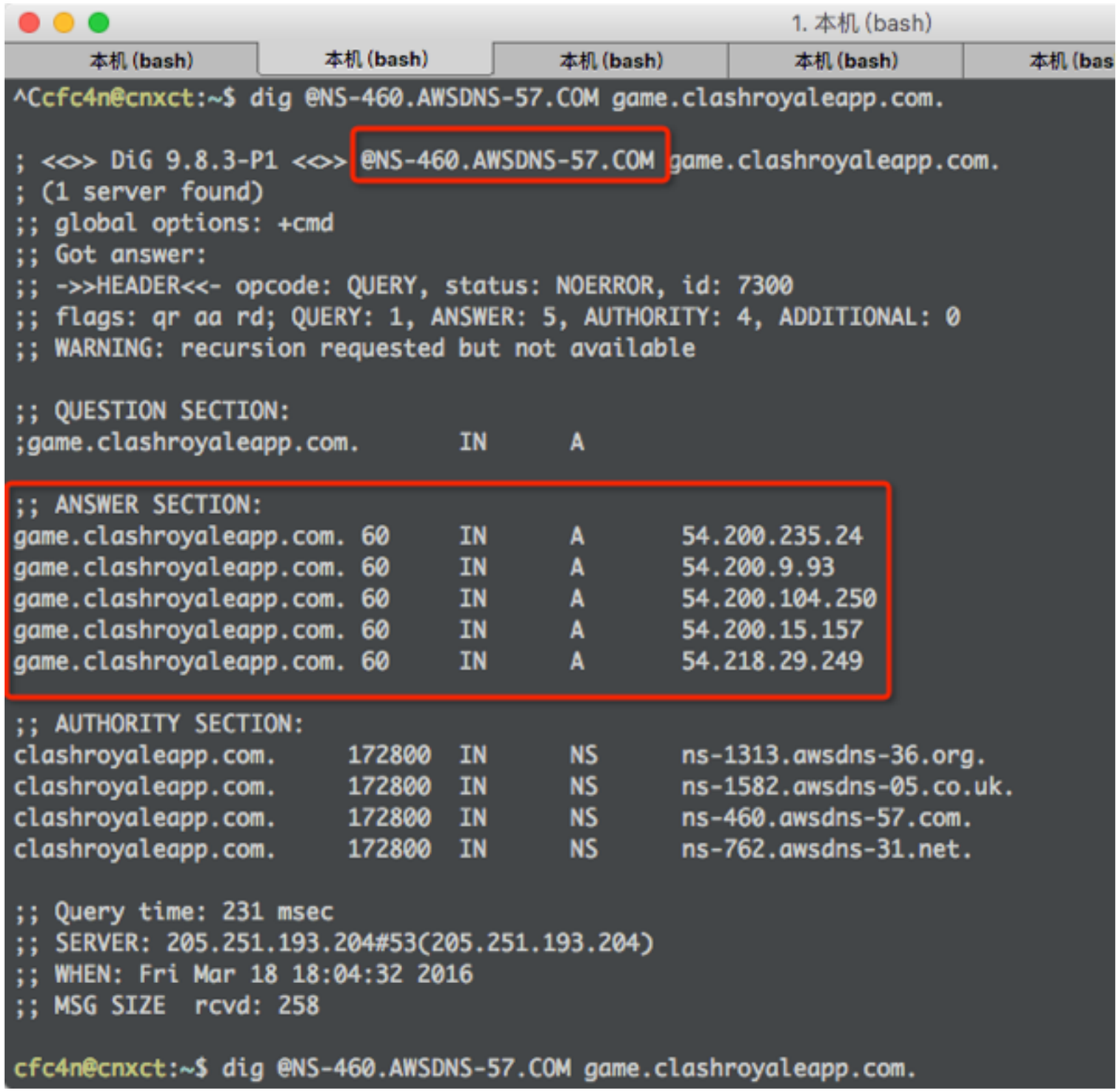
如何查询所有子域名

- 域名组织规定，不允许查询子域名列表
- 现存子域名查询，依赖搜索引擎收录，再汇总
- 非常规手段

子域名列表

- gamec.clashroyaleapp.com （国内3月16日15点左右半小时DNS查询次数400W）
- game.clashroyaleapp.com （国内3月16日15点左右半小时DNS查询次数17W）
- game.clashroyaleapp.com.ad***.to***
- game.clashroyaleapp.com.bel***
- game.clashroyaleapp.com.dh***
- game.clashroyaleapp.com.ho***
- game.clashroyaleapp.com.lo***
- game.clashroyaleapp.com.ral***
- game.clashroyaleapp.com.wor***

海外访问域名


1. 本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
本机 (bash)
本机 (bas
^Ccfc4n@cnxct:~$ dig @NS-460.AWSDNS-57.COM game.clashroyaleapp.com.
; <<>> DiG 9.8.3-P1 <<>> @NS-460.AWSDNS-57.COM game.clashroyaleapp.com.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7300
;; flags: qr aa rd; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 0
;; WARNING: recursion requested but not available
;; QUESTION SECTION:
;game.clashroyaleapp.com. IN A
;; ANSWER SECTION:
game.clashroyaleapp.com. 60 IN A 54.200.235.24
game.clashroyaleapp.com. 60 IN A 54.200.9.93
game.clashroyaleapp.com. 60 IN A 54.200.104.250
game.clashroyaleapp.com. 60 IN A 54.200.15.157
game.clashroyaleapp.com. 60 IN A 54.218.29.249
;; AUTHORITY SECTION:
clashroyaleapp.com. 172800 IN NS ns-1313.awsdns-36.org.
clashroyaleapp.com. 172800 IN NS ns-1582.awsdns-05.co.uk.
clashroyaleapp.com. 172800 IN NS ns-460.awsdns-57.com.
clashroyaleapp.com. 172800 IN NS ns-762.awsdns-31.net.
;; Query time: 231 msec
;; SERVER: 205.251.193.204#53(205.251.193.204)
;; WHEN: Fri Mar 18 18:04:32 2016
;; MSG SIZE rcvd: 258
cfc4n@cnxct:~$ dig @NS-460.AWSDNS-57.COM game.clashroyaleapp.com.

海外访问域名

- 无CNAME记录
- 只有A记录
- 根据4个Name Server响应,A记录均指向亚马逊美国机房
- A记录总数未统计，也为DNS轮训方式

小结

- 游戏服务器海外一个中心，部署集中在亚马逊美国俄亥俄州
- 国内一个中心，部署在广州Ucloud机房
- 国内至少约40台服务器，半小时活跃用户400W
- DNS轮训方式（建议用http dns来实现）

游戏通讯

```
625  6.370   192.168.2.2       192.168.2.1       77  DNS   Standard query 0xda8a AAAA cr.kunlun-cdn.com
626  6.370   192.168.128.47    192.168.1.6       77  DNS   Standard query 0x5c78 AAAA cr.kunlun-cdn.com
627  6.371   192.168.1.6       192.168.128.47    77  DNS   Standard query response 0x5c78 AAAA cr.kunlun-cdn.com
628  6.371   192.168.2.1       192.168.2.2      142  DNS   Standard query response 0xc6a8 AAAA gamec.clashroyaleapp.com CNA
629  6.371   192.168.2.1       192.168.2.2       77  DNS   Standard query response 0xda8a AAAA cr.kunlun-cdn.com
630  6.374   192.168.2.2       192.168.2.1       70  ICMP  Destination unreachable (Port unreachable)
631  6.375   192.168.2.2       cr.kunlun-cdn.com 78  TCP   59905 → 9339 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=20
632  6.375   192.168.128.47    cr.kunlun-cdn.com 78  TCP   45070 → 9339 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=20
633  6.454   a23-7-132-12.dep… 192.168.128.47  1494  TCP   [TCP segment of a reassembled PDU]
634  6.454   a23-7-132-12.dep… 192.168.128.47  1494  TCP   [TCP segment of a reassembled PDU]
635  6.454   192.168.128.47    a23-7-132-12.deploy.static.akamaite… 66  TCP   52323 → https [ACK] Seq=1 Ack=94249 Win=4006 Len=0 TSval=1559020
636  6.454   192.168.128.47    a23-7-132-12.deploy.static.akamaite… 66  TCP   [TCP Window Update] 52323 → https [ACK] Seq=1 Ack=94249 Win=4096
637  6.473   1.na.dl.wireshar… 192.168.128.47  1494  TCP   [TCP Previous segment not captured] [TCP segment of a reassemble
638  6.473   192.168.128.47    1.na.dl.wireshark.org 78  TCP   [TCP Window Update] 51866 → https [ACK] Seq=1 Ack=187069 Win=409
639  6.473   1.na.dl.wireshar… 192.168.128.47  1494  TCP   [TCP segment of a reassembled PDU]
640  6.473   192.168.128.47    1.na.dl.wireshark.org 78  TCP   [TCP Dup ACK 619#1] 51866 → https [ACK] Seq=1 Ack=187069 Win=409
641  6.473   1.na.dl.wireshar… 192.168.128.47  1494  TCP   [TCP segment of a reassembled PDU]
642  6.473   192.168.128.47    1.na.dl.wireshark.org 78  TCP   [TCP Dup ACK 619#2] 51866 → https [ACK] Seq=1 Ack=187069 Win=409
643  6.473   1.na.dl.wireshar… 192.168.128.47  1494  TCP   [TCP segment of a reassembled PDU]
644  6.473   192.168.128.47    1.na.dl.wireshark.org 78  TCP   [TCP Dup ACK 619#3] 51866 → https [ACK] Seq=1 Ack=187069 Win=409
```

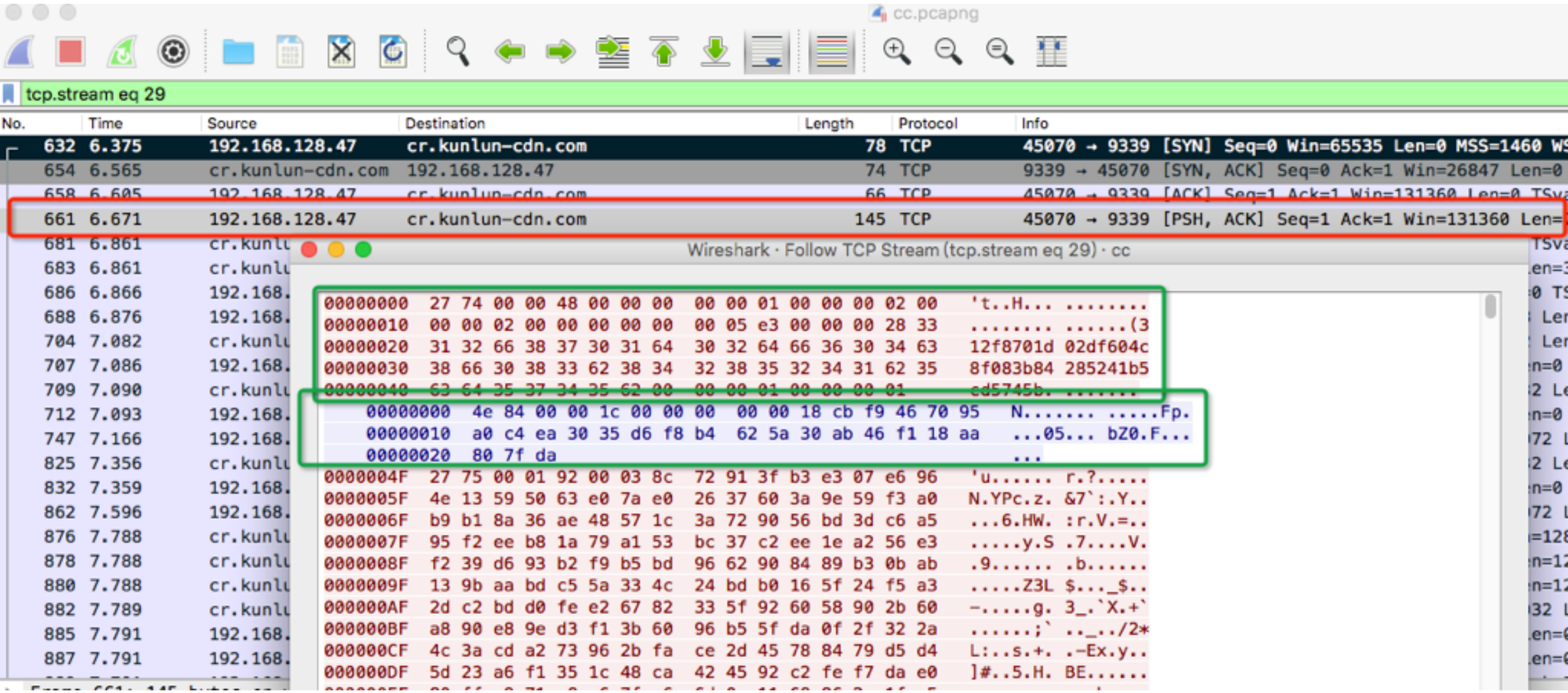
```
▶ Frame 631: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 1 (inbound)
▶ Ethernet II, Src: Apple_45:e9:f4 (a0:18:28:45:e9:f4), Dst: MS-NLB-PhysServer-32_1e:e1:4c:a9:64 (02:3e:e1:4c:a9:64)
▶ Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: cr.kunlun-cdn.com (106.75.134.234)
▼ Transmission Control Protocol, Src Port: 59905 (59905), Dst Port: 9339 (9339), Seq: 0, Len: 0
    Source Port: 59905 (59905)
    Destination Port: 9339 (9339)
    [Stream index: 28]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
```

游戏通讯

- 端口9339

- 似曾相识

游戏通讯


cc.pcapng
tcp.stream eq 29
No. Time Source Destination Length Protocol Info
632 6.375 192.168.128.47 cr.kunlun-cdn.com 78 TCP 45070 → 9339 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
654 6.565 cr.kunlun-cdn.com 192.168.128.47 74 TCP 9339 → 45070 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0
661 6.671 192.168.128.47 cr.kunlun-cdn.com 145 TCP 45070 → 9339 [PSH, ACK] Seq=1 Ack=1 Win=131360 Len=
681 6.861 cr.kunlu
683 6.861 cr.kunlu
686 6.866 192.168.
688 6.876 192.168.
704 7.082 cr.kunlu
707 7.086 192.168.
709 7.090 cr.kunlu
712 7.093 192.168.
747 7.166 192.168.
825 7.356 cr.kunlu
832 7.359 192.168.
862 7.596 192.168.
876 7.788 cr.kunlu
878 7.788 cr.kunlu
880 7.788 cr.kunlu
882 7.789 cr.kunlu
885 7.791 192.168.
887 7.791 192.168.
Wireshark · Follow TCP Stream (tcp.stream eq 29) · cc
00000000 27 74 00 00 48 00 00 00 00 00 01 00 00 00 02 00 't..H... ....
00000010 00 00 02 00 00 00 00 00 00 05 e3 00 00 00 28 33 ....(3
00000020 31 32 66 38 37 30 31 64 30 32 64 66 36 30 34 63 12f8701d 02df604c
00000030 38 66 30 38 33 62 38 34 32 38 35 32 34 31 62 35 8f083b84 285241b5
00000040 63 64 35 37 34 35 62 00 00 00 01 00 00 00 01 cd5745b. ....
00000000 4e 84 00 00 1c 00 00 00 00 00 18 cb f9 46 70 95 N....... .....Fp.
00000010 a0 c4 ea 30 35 d6 f8 b4 62 5a 30 ab 46 f1 18 aa ...05... bZ0.F...
00000020 80 7f da ...
0000004F 27 75 00 01 92 00 03 8c 72 91 3f b3 e3 07 e6 96 'u...... r.?.....
0000005F 4e 13 59 50 63 e0 7a e0 26 37 60 3a 9e 59 f3 a0 N.YPc.z. &7`:.Y..
0000006F b9 b1 8a 36 ae 48 57 1c 3a 72 90 56 bd 3d c6 a5 ...6.HW. :r.V.=..
0000007F 95 f2 ee b8 1a 79 a1 53 bc 37 c2 ee 1e a2 56 e3 .....y.S .7....V.
0000008F f2 39 d6 93 b2 f9 b5 bd 96 62 90 84 89 b3 0b ab .9...... .b......
0000009F 13 9b aa bd c5 5a 33 4c 24 bd b0 16 5f 24 f5 a3 .....Z3L $..._$..
000000AF 2d c2 bd d0 fe e2 67 82 33 5f 92 60 58 90 2b 60 -.....g. 3_.`X.+`
000000BF a8 90 e8 9e d3 f1 3b 60 96 b5 5f da 0f 2f 32 2a ......;` .._../2*
000000CF 4c 3a cd a2 73 96 2b fa ce 2d 45 78 84 79 d5 d4 L:..s.+. .-Ex.y..
000000DF 5d 23 a6 f1 35 1c 48 ca 42 45 92 c2 fe f7 da e0]#..5.H. BE......

Wireshark · Follow TCP Stream (tcp.stream eq 29) · cc

```
    00010BD1  00 2f 47 46 81 20 42 c5  1e 90                    ./GF. B. ..
000006CD  27 7c 00 00 10 00 00 79  39 e2 ce a2 19 55 6f 2c   '|.....y 9....Uo,
000006DD  15 54 f3 72 c3 ad 96                               .T.r...
    00010BDB  4e 8c 00 00 10 00 00 26  f1 18 42 97 ca 06 a4 f3   N......& ..B.....
    00010BEB  9e 56 fc 42 75 43 c0                               .V.BuC.
000006E4  27 7b 00 00 19 00 00 72  e0 58 83 f2 82 25 34 56   '{.....r .X...%4V
000006F4  c9 68 41 e2 94 51 bb 50  59 d4 a0 17 40 eb d9 2c   .hA..Q.P Y...@..,
00000704  27 7c 00 00 10 00 00 55  7f 76 a5 d9 fe 66 b9 24   '|.....U .v...f.$
00000714  21 9f 2b 5d 25 d1 35                               !.+]%.5
    00010BF2  4e 8c 00 00 10 00 00 25  bb 99 94 08 74 7a 5f 05   N......% ....tz_.
    00010C02  ee 71 e0 01 80 e1 b0                               .q.....
0000071B  27 7b 00 00 19 00 00 ca  61 c6 0f 1c 40 f8 5d 47   '{...... a...@.]G
0000072B  ee a9 34 a8 43 13 45 a7  fb 6a f6 26 43 c1 0d 17   ..4.C.E. .j.&C...
0000073B  37 16 00 00 2b 00 00 49  f3 7e ad 9f d9 51 15 96   7...+..I .~...Q..
0000074B  90 95 e8 34 27 4b 93 10  c4 4c 0d bb 59 44 af f4   ...4'K.. .L..YD..
0000075B  47 f1 6a 50 b8 57 a4 0c  35 eb cc 8a 51 1b f6 00   G.jP.W.. 5...Q...
0000076B  be b2                                              ..
0000076D  37 16 00 00 1a 00 00 3c  83 05 6b 55 88 71 21 26   7......< ..kU.q!&
0000077D  c0 32 d0 18 93 ed 90 96  84 b1 5c dd 5b c0 11 c9   .2...... ..\.[...
0000078D  51                                                 Q
    00010C09  5e f8 00 00 3f 00 00 47  56 f2 6b fc be bf 5e 9e   ^...?..G V.k...^.
    00010C19  fc a3 30 7e 2f 6c c3 45  e9 76 e5 aa 1d bf ca 64   ..0~/l.E .v.....d
    00010C29  79 8e 90 c7 de b2 2c 7f  b1 df b3 6b 31 c9 2f 6b   y.....,. ...k1./k
    00010C39  56 72 03 fa 9b 37 10 76  d3 98 72 0e 48 32 14 4c   Vr...7.v ..r.H2.L
    00010C49  a6 7a 9e 6f 7c ad                                  .z.o|.
    00010C4F  5e fe 00 00 18 00 00 06  41 bd 50 72 54 2b 86 d9   ^....... A.PrT+..
    00010C5F  51 ab 87 df 2b 34 59 fd  b8 6c 7b 87 28 b0 7d      Q...+4Y. .l{.(.}
0000078E  27 7c 00 00 10 00 00 31  e4 e3 56 20 a7 2f c3 5b   '|.....1 ..V ./.[
0000079E  39 68 cd 6b f1 6a fd                               9h.k.j.
    00010C6E  4e 8c 00 00 10 00 00 c4  ea f5 95 10 7a 54 a1 28   N....... ....zT.(
    00010C7E  12 34 e5 63 de db a1                               .4.c...
000007A5  27 7b 00 00 19 00 00 56  bb 45 1a 85 65 17 cb 13   '{.....V .E..e...
000007B5  79 c3 ae ee 50 ff c8 9c  e0 97 dd 09 8e ab e5 99   y...P... ........
```

Packet 7085. 49 client pkt(s), 71 server pkt(s), 44 turn(s). Click to select.

Entire conversation (70 kB) | Show data as Hex Dump | Stream 29

Find: | Find Next

Help | Hide this stream | Print | Save as... | Close

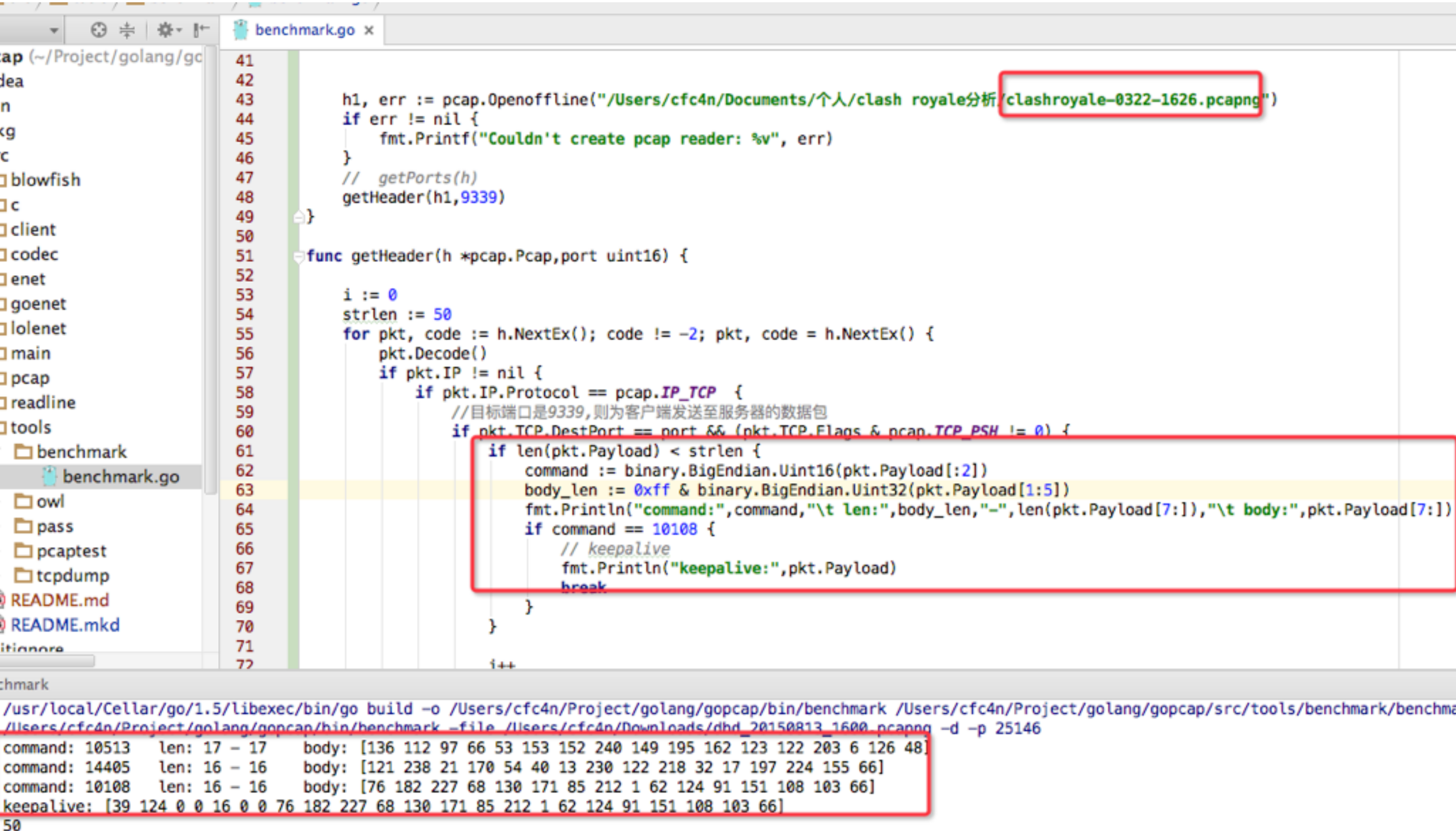
游戏通讯

- 27 7c 00 00 10 00 00 79
- 27 7b 00 00 19 00 00 72
- 27 7b 00 00 19 00 00 ca
- 37 16 00 00 1a 00 00 3c
- 27 7c 00 00 10 00 00 31
- 27 7b 00 00 19 00 00 56

根据经验

- IP\TCP等协议，均以固定包头格式
- 包头内包含后续包长度
- 猜测不变（或少变）部分为包头
- 查找包长度字段

pcapng协议包自动分析



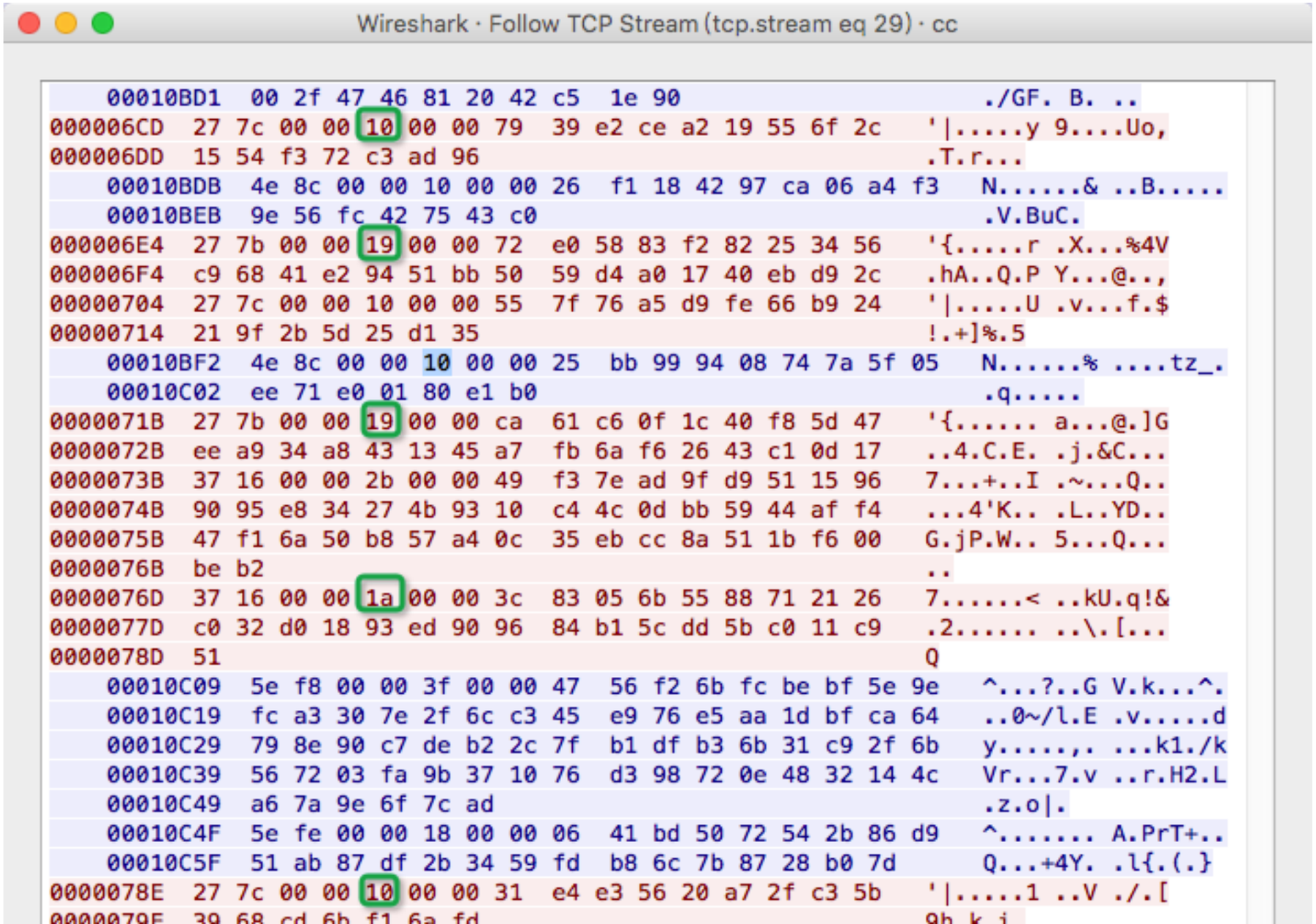
先捏软柿子 最短包入手

- 肉眼一个一个找?
- 程序处理wirshark数据包文件
- 遍历所有包，最短为23字节

- [39 124 0 0 16 0 0 135 29 244 121 46 116 184 61 65 103 17 224 73 143 189 48]
- [39 124 0 0 16 0 0 25 80 113 190 45 125 228 66 148 62 222 192 195 74 184 150]
- [39 124 0 0 16 0 0 138 215 9 252 5 252 4 96 135 136 71 30 168 52 19 201]

显然

- 第五字节为后面包长度



协议头-长度

27 7c 00 00 10 00 00 79 39 e2 ce a2 19 55 6f 2c

15 54 f3 72 c3 ad 96

第5字节0x10为第7-N的总长度

长度验证

- 一个字节的最大整数是8<<1 ,也就是0XFF,即255

- 选择大于255的包验证

Wireshark · Follow TCP Stream (tcp.stream eq 29) · cc

```
00000000  27 74 00 00 48 00 00 00  00 00 01 00 00 00 02 00   't..H... ........
00000010  00 00 02 00 00 00 00 00  00 05 e3 00 00 00 28 33   ........ ......(3
00000020  31 32 66 38 37 30 31 64  30 32 64 66 36 30 34 63   12f8701d 02df604c
00000030  38 66 30 38 33 62 38 34  32 38 35 32 34 31 62 35   8f083b84 285241b5
00000040  63 64 35 37 34 35 62 00  00 00 01 00 00 00 01      cd5745b. .......
    00000000  4e 84 00 00 1c 00 00 00  00 00 18 cb f9 46 70 95   N....... .....Fp.
    00000010  a0 c4 ea 30 35 d6 f8 b4  62 5a 30 ab 46 f1 18 aa   ...05... bZ0.F...
    00000020  80 7f da                                          ...
0000004F  27 75 00 01 92 00 03 8c  72 91 3f b3 e3 07 e6 96   'u...... r.?.....
0000005F  4e 13 59 50 63 e0 7a e0  26 37 60 3a 9e 59 f3 a0   N.YPc.z. &7`:.Y..
0000006F  b9 b1 8a 36 ae 48 57 1c  3a 72 90 56 bd 3d c6 a5   ...6.HW. :r.V.=..
0000007F  95 f2 ee b8 1a 79 a1 53  bc 37 c2 ee 1e a2 56 e3   .....y.S .7....V.
0000008F  f2 39 d6 93 b2 f9 b5 bd  96 62 90 84 89 b3 0b ab   .9...... .b......
0000009F  13 9b aa bd c5 5a 33 4c  24 bd b0 16 5f 24 f5 a3   .....Z3L $..._$..
000000AF  2d c2 bd d0 fe e2 67 82  33 5f 92 60 58 90 2b 60   -.....g. 3_.`X.+`
000000BF  a8 90 e8 9e d3 f1 3b 60  96 b5 5f da 0f 2f 32 2a   ......;` .._../2*
000000CF  4c 3a cd a2 73 96 2b fa  ce 2d 45 78 84 79 d5 d4   L:..s.+. .-Ex.y..
000000DF  5d 23 a6 f1 35 1c 48 ca  42 45 92 c2 fe f7 da e0   ]#..5.H. BE......
000000EF  80 ff e9 71 e8 c6 7f e6  6d 0e 11 68 86 2e 1f e5   ...q.... m..h....
000000FF  5b 2d af f1 5c 21 a2 9b  b7 41 aa 8a 31 95 48 c4   [-..\!.. .A..1.H.
0000010F  bc c4 9b a8 ba 1d 48 0b  8b 9e f8 ee e6 56 86 44   ......H. .....V.D
0000011F  fb b2 2a b7 03 14 38 a3  ae dd 7a 13 76 30 c9 61   ..*...8. ..z.v0.a
0000012F  6b 2d 18 97 34 54 d3 85  a5 ad 5d cd 52 6d f4 a0   k-..4T.. ..].Rm..
0000013F  e3 06 f7 4d 94 b4 18 d8  64 1c 87 c1 ef 51 83 fc   ...M.... d....Q..
0000014F  e7 2b 24 b7 61 a7 cb 79  12 fe 6b 5a 40 8a 0b b8   .+$.a..y ..kZ@...
0000015F  d7 3c 1f a9 a8 11 a4 fa  64 dd ad e8 95 e7 c1 d6   .<...... d.......
0000016F  38 2c a1 5f 3a 60 6d d8  3c 28 c2 05 eb ca b2 19   8,._:`m. <(......
0000017F  80 52 2c bc 08 ec da 18  63 7e cd 7e c1 bf 62 e9   .R,..... c~.~..b.
0000018F  ab 0b a1 58 38 54 56 b0  30 34 3c 12 8d cd 13 34   ...X8TV. 04<....4
0000019F  4c a1 cc 2a 73 30 0e df  6d be 9d d8 c3 a8 e4 f4   L..*s0.. m.......
000001AF  02 03 83 b4 b0 e3 2c 2f  87 ca 53 11 ac 6d d3 86   ......,/ ..S..m..
000001BF  e1 7d b2 e2 8a dd 07 fe  7d ff f5 ac d3 e5 b1 51   .}...... }......Q
000001CF  40 17 88 f2 44 8c 95 07  11 60 48 96 ce 39 fa b2   @...D... .`H..9..
000001DF  18 52 ec 03 99 c7 b6 4b  63                      .R.....K c
    00000023  4e 88 00 00 e6 00 01 c6  e7 51 f2 17 3c 35 a8 79   N....... .Q..<5.y
```

Packet 661. 49 client pkt(s), 71 server pkt(s), 44 turn(s). Click to select.

Entire conversation (70 kB) | Show data as Hex Dump | Stream 29

Find: | Find Next

Help | Hide this stream | Print | Save as... | Close

长度验证

- 第7字节往后是402个字节
- 对应第4、第5字节，即0x0192的值
- 确认长度含义正确，且为4-5字节(可能继续往前增长)
- 增长方式从后往前增长
- Big Endian模式

通讯协议头

- 0-3未确定
- 4-5确定为包体长度，大端
- 6-7一直为0x00，用意不明

通讯协议头

- 0-2 command 指令
- 3-5确定为包体长度，大端
- 6-7一直为0x00，用意不明

继续?

- 除client->server的首包未加密以外，其他均加密
- 似曾相识？SuperCell的一贯传统?
- coc-proxy 借用
- 查找libg.so中的公钥
- （细节先跳过，后面会提到）

解密完成，消息结构有待解码

```
connection from 192.168.2.3:59379 ...
connected to 106.75.133.160:9339 ... // client
ClientHandshake: {
  "unknown_0": 1,
  "unknown_1": 2,
  "majorVersion": 2,
  "unknown_3": 0,
  "minorVersion": 1507,
  "masterHash": "312f8701d02df604c8f083b84285241b5cd5745b",
  "unknown_6": 2,
  "unknown_7": 2
}
ServerHandshake: {
  "sessionKey": "9f38d039ce50adb2e9fbb6aa71462a824ee4903b4bb4a7db"
}
10101 Error: Read buffer out of data.
10101 27750000bf000300000006002549850000028396833 6a7a376464796338706d36366e396d7963336234326e6e77773979683336736387a676a6b0200a317000000283
38343238353234316235636435373435620000000000000000ffffffff0000000c436f6f6c7
0616420353839300000000000000005342e312e32010000000000000000f32363737303166336313036633162000000027a6801090000000000000000020000000000000000
20104 Error: Read buffer out of data.
20104 4e880000910001000000060025498500000006002549850000028396833 6a7a376464796338706d36366e396d7963336234326e6e77773979683336736387a676a6b1
a908000000010313437353236383738363131323433330000000d31343538363334383737363230000000d31343538363330353136303030 00ffffffff
24101 Error: Read buffer out of data.
24101 5e2500016f000000000060025498501009 4bcc8019cf1d201be8492ef0a00030880eae51881eae5188deae51881fcd91a80fcd91a83eae5180000880eae51881eae51
1881eae5188deae51881fcd91a80fcd91a83eae51800003f1a0001000000000 1a0100001000000 1a0d000001000000 1c010100000000 1c000000100000 1a0300001000
ef0a00007f011307010000 7f00000094bcc8019cf1d201be8492ef0a000000 7f0100000000000000002013600ac8bc0d30c0303a89843a89843bfaf8bef0a031a0d001a12001a0
aa020685a6aa020685a6aa020000000007f3600000000000000000000006040501a901050202050301050 5a90100033c07063c08063c0906000105080605 1a00041a01041a0
f4aacfd603
24447 Error: 'Message definition missing (24447).'
24447 5f7f000004000000000001
10513 Error: 'Message definition missing (10513).'
10513 2911000001000000
20105 Error: 'Message definition missing (20105).'
20105 4e8900000800000000000100000000
14405 Error: 'Message definition missing (14405).'
14405 38450000000000
AvatarStream: {
  "entries": []
}
```

统一框架的利弊

- COC、Hey Day、Boom Beach、Clash Royale都是同一台服务端框架
- 性能高、稳定性高
- 人员学习成本低
- 缺点：一损俱损

解码消息结构

- 很漫长的工程，对每个command都要解码

- 解码方式跟二进制文件资源(美术资源)还原类似

资源文件解密

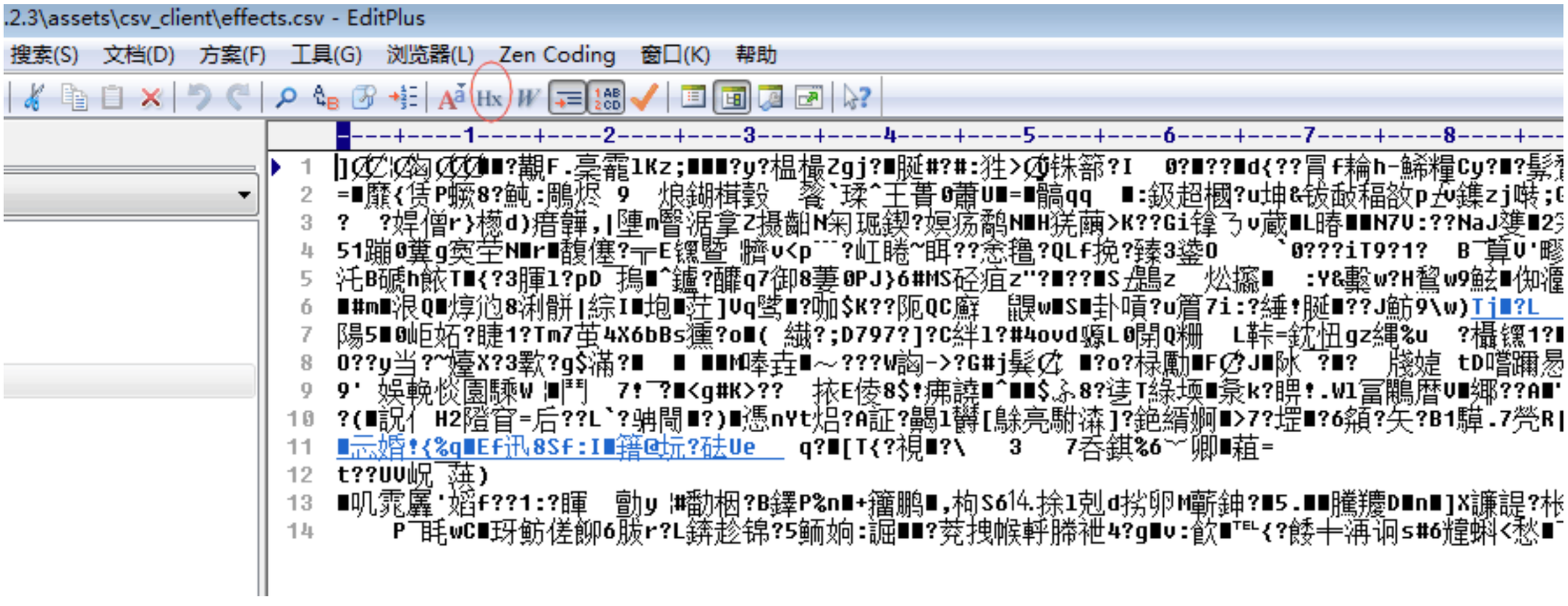
- csv配置文件

- sc未知格式文件

包的解压

- android包是 apk
- ios是ipa
- 为什么改成zip拓展名后，可以直接解压?
- 先看csv文件的解码

csv文件解码



乱码？为什么会乱码？

如何区分文本/二进制文件

- 拓展名是做什么用的?
- 1.jpg改名为1.png、1.gif还能正常显示吗？为什么?
- 它们是如何被存储到文件中的?

上传文件的图片判断

- 图片不合法又能怎样?
- 图片如何判断格式合法?
- 拓展名?
- 文件头(magic Number)？
- 然后呢?

文件的Magic Number

Some examples:

- Compiled Java class files (bytecode) and Mach-O binaries start with hex `CAFEBABE`. When compressed with Pack200 the bytes are changed to `CAFED00D`.
- GIF image files have the ASCII code for "GIF89a" (`47` `49` `46` `38` `39` `61`) or "GIF87a" (`47` `49` `46` `38` `37` `61`)
- JPEG image files begin with `FF` `D8` and end with `FF` `D9`. JPEG/JFIF files contain the ASCII code for "JFIF" (`4A` `46` `49` `46`) as a null terminated string. JPEG/Exif files contain the ASCII code for "
  followed by more metadata about the file.
- PNG image files begin with an 8-byte signature which identifies the file as a PNG file and allows detection of common file transfer problems: `\211` `P` `N` `G` `\r` `\n` `\032` `\n` (`89` `50` `4E` `47` `0D`
  characters to permit detecting unwarranted automated newline conversions, such as transferring the file using FTP with the *ASCII* transfer mode instead of the *binary* mode.[5]
- Standard MIDI audio files have the ASCII code for "MThd" (`4D` `54` `68` `64`) followed by more metadata.
- Unix or Linux scripts may start with a "shebang" (`#!`, `23` `21`) followed by the path to an interpreter, if the interpreter is likely to be different from the one from which the script was invoked.
- ELF executables start with `7F` `E` `L` `F`
- PostScript files and programs start with "%!" (`25` `21`).
- PDF files start with "%PDF" (hex `25` `50` `44` `46`).
- DOS MZ executable files and the EXE stub of the Microsoft Windows PE (Portable Executable) files start with the characters "MZ" (`4D` `5A`), the initials of the designer of the file format, Mark Zbikowski. Th
  dosZMXP, a non-PE EXE.[6]
- The Berkeley Fast File System superblock format is identified as either `19` `54` `01` `19` or `01` `19` `54` depending on version; both represent the birthday of the author, Marshall Kirk McKusick.
- The Master Boot Record of bootable storage devices on almost all IA-32 IBM PC compatibles has a code of `55` `AA` as its last two bytes.
- Executables for the Game Boy and Game Boy Advance handheld video game systems have a 48-byte or 156-byte magic number, respectively, at a fixed spot in the header. This magic number encodes a b
- Amiga software executable Hunk files running on Amiga classic 68000 machines all started with the hexadecimal number $000003f3, nicknamed the "Magic Cookie."
- In the Amiga, the only absolute address in the system is hex $0000 0004 (memory location 4), which contains the start location called SysBase, a pointer to exec.library, the so-called kernel of Amiga.
- PEF files, used by Mac OS and BeOS for PowerPC executables, contain the ASCII code for "Joy!" (`4A` `6F` `79` `21`) as a prefix.
- TIFF files begin with either `II` or `MM` followed by 42 as a two-byte integer in little or big endian byte ordering. `II` is for Intel, which uses little endian byte ordering, so the magic number is `49` `49` `2A`
  ordering, so the magic number is `4D` `4D` `00` `2A`.
- Unicode text files encoded in UTF-16 often start with the Byte Order Mark to detect endianness (`FE` `FF` for big endian and `FF` `FE` for little endian). And on Microsoft Windows, UTF-8 text files often sta
  `EF` `BB` `BF`.
- LLVM Bitcode files start with `BC` (0x42, 0x43)
- WAD files start with `IWAD` or `PWAD` (for *Doom*), `WAD2` (for *Quake*) and `WAD3` (for *Half-Life*).
- Microsoft Compound File Binary Format (mostly known as one of the older formats of Microsoft Office documents) files start with `D0` `CF` `11` `E0`, which is visually suggestive of the word "DOCFILE0".
- Headers in ZIP files begin with "PK" (`50` `4B`), the initials of Phil Katz, author of DOS compression utility PKZIP.

Detection

The Unix utility program `file` can read and interpret magic numbers from files, and indeed, the file which is used to parse the information is called *magic*. The Windows utility TrID has a similar purpose.

协议中的Magic Number

- LLVM bitcode files start with `BC` (0x42, 0x43)
- WAD files start with `IWAD` or `PWAD` (for *Doom*), `WAD2` (for *Quake*) and `WAD3` (for *Half-Life*).
- Microsoft Compound File Binary Format (mostly known as one of the older formats of Microsoft Office documents) files start with `D0` `CF` `11` `E0`, which is visually suggestive of the word "DOCFILE0".
- Headers in ZIP files begin with "PK" (`50` `4B`), the initials of Phil Katz, author of DOS compression utility PKZIP.

Detection

The Unix utility program `file` can read and interpret magic numbers from files, and indeed, the file which is used to parse the information is called *magic*. The Windows utility TrID has a similar purpose.

Magic numbers in protocols [edit]

Examples

- The OSCAR protocol, used in AIM/ICQ, prefixes requests with `2A`.
- In the RFB protocol used by VNC, a client starts its conversation with a server by sending "RFB" (`52` `46` `42`, for "Remote Frame Buffer") followed by the client's protocol version number.
- In the SMB protocol used by Microsoft Windows, each SMB request or server reply begins with '`FF` `53` `4D` `42`', or `"\xFFSMB"` at the start of the SMB request.
- In the MSRPC protocol used by Microsoft Windows, each TCP-based request begins with `05` at the start of the request (representing Microsoft DCE/RPC Version 5), followed immediately by a `00` or `01` fo first byte is always `04`.
- In COM and DCOM marshalled interfaces, called OBJREFs, always start with the byte sequence "MEOW" (`4D` `45` `4F` `57`). Debugging extensions (used for DCOM channel hooking) are prefaced with the
- Unencrypted BitTorrent tracker requests begin with a single byte containing the value `19` representing the header length, followed immediately by the phrase "BitTorrent protocol" at byte position 1.
- eDonkey2000/eMule traffic begins with a single byte representing the client version. Currently `E3` represents an eDonkey client, `C5` represents eMule, and `D4` represents compressed eMule.
- SSL transactions always begin with a "client hello" message. The record encapsulation scheme used to prefix all SSL packets consists of two- and three- byte header forms. Typically an SSL version 2 client he response to a client hello begins with `16` (though this may vary).
- DHCP packets use a "magic cookie" value of '`0x63` `0x82` `0x53` `0x63`' at the start of the options section of the packet. This value is included in all DHCP packet types.
- HTTP/2 connections are opened with the preface '`0x505249202a20485454502f322e300d0a0d0a534d0d0a0d0a`' or '`PRI * HTTP/2.0\r\n\r\nSM\r\n\r\n`'. The preface is designed to avoid the support earlier versions of HTTP but not 2.0.

Magic numbers in other uses [edit]

Examples

- The default MAC address on Texas Instruments SOCs is DE:AD:BE:EF:00:00 [7]

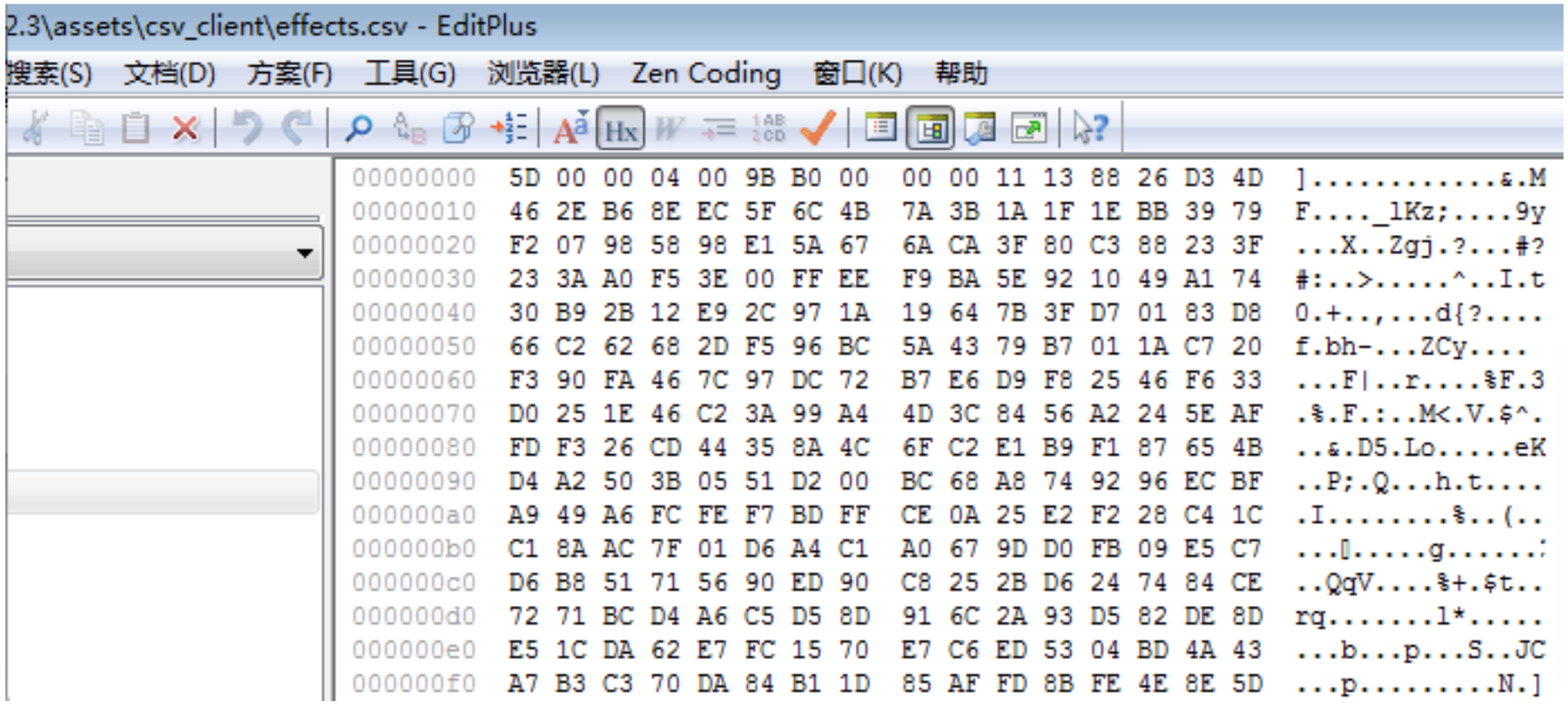
机智的你，一定秒懂为什么http的Magic Number可以是那两种咯?

比如

```
-rw-r--r--   1 cfc4n  staff  128578  4 22 16:27 反调试-trace进程判断.png
-rw-r--r--   1 cfc4n  staff   14154  4 22 18:27 分析草稿
-rw-r--r--@  1 cfc4n  staff   36202  4 26 16:32 字母频率.png
cfc4n@cnxct:~/Documents/个人/DHD分析$ hexdump 1.jpg |head -n 2
0000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00
0000010 00 00 00 00 ff db 00 43 00 06 04 05 06 05 04 06
cfc4n@cnxct:~/Documents/个人/DHD分析$
```

```
0000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 00
0000010 00 00 00 00 ff db 00 43 00 06 04 05 06 05 04 06
cfc4n@cnxct:~/Documents/个人/DHD分析$ hexdump 1.gif |head -n 2
0000000 47 49 46 38 39 61 5a 00 46 00 87 5a 00 02 02 02
0000010 01 81 1b 85 00 00 84 84 84 29 21 62 91 92 92 be
cfc4n@cnxct:~/Documents/个人/DHD分析$
```

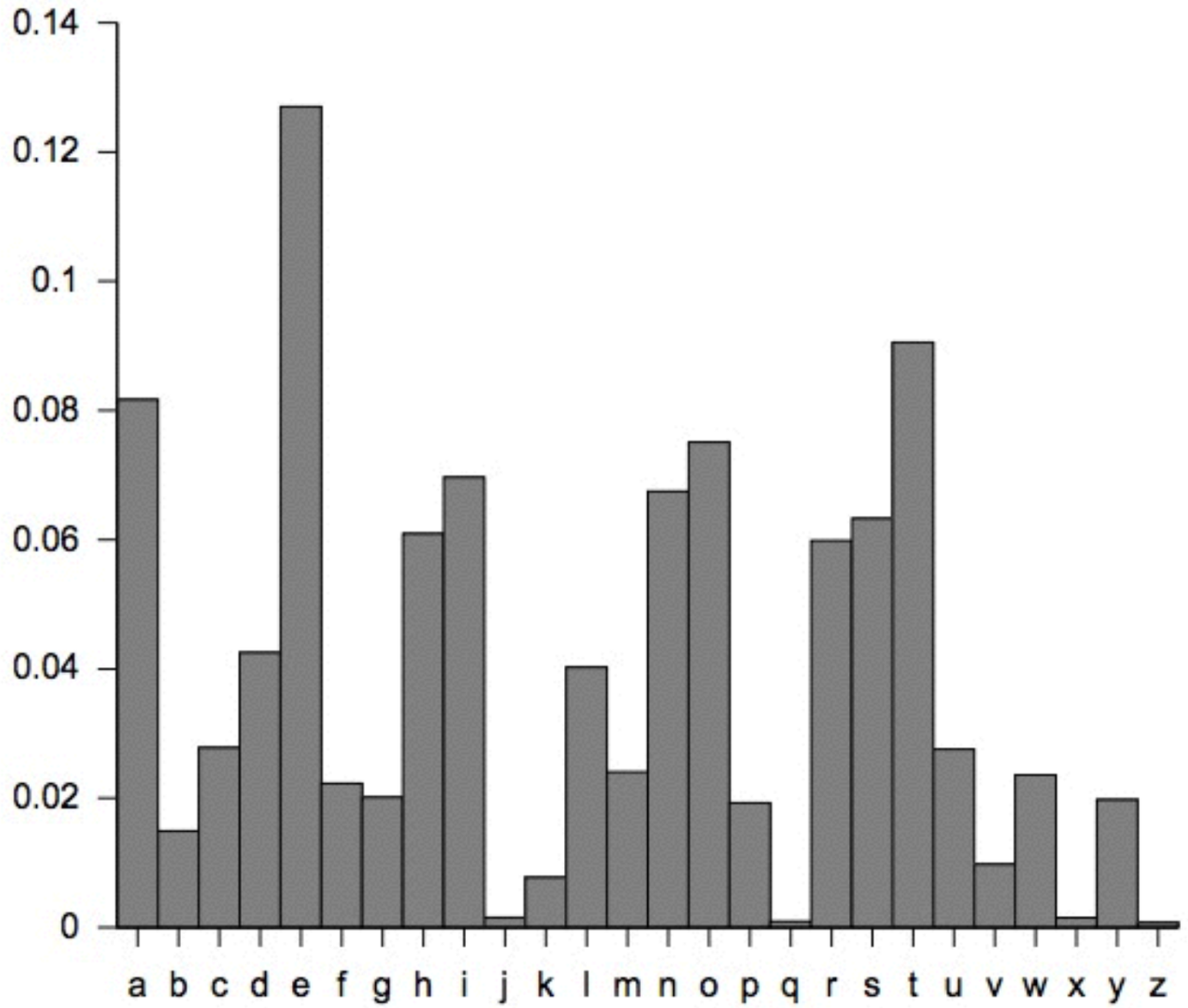
回到主题


2.3\assets\csv_client\effects.csv - EditPlus
搜索(S) 文档(D) 方案(F) 工具(G) 浏览器(L) Zen Coding 窗口(K) 帮助
00000000 5D 00 00 04 00 9B B0 00 00 00 11 13 88 26 D3 4D].............&.M
00000010 46 2E B6 8E EC 5F 6C 4B 7A 3B 1A 1F 1E BB 39 79 F...._lKz;....9y
00000020 F2 07 98 58 98 E1 5A 67 6A CA 3F 80 C3 88 23 3F ...X..Zgj.?...#?
00000030 23 3A A0 F5 3E 00 FF EE F9 BA 5E 92 10 49 A1 74 #:..>.....^..I.t
00000040 30 B9 2B 12 E9 2C 97 1A 19 64 7B 3F D7 01 83 D8 0.+..,...d{?....
00000050 66 C2 62 68 2D F5 96 BC 5A 43 79 B7 01 1A C7 20 f.bh-...ZCy....
00000060 F3 90 FA 46 7C 97 DC 72 B7 E6 D9 F8 25 46 F6 33 ...F|..r....%F.3
00000070 D0 25 1E 46 C2 3A 99 A4 4D 3C 84 56 A2 24 5E AF .%.F.:..M<.V.$^.
00000080 FD F3 26 CD 44 35 8A 4C 6F C2 E1 B9 F1 87 65 4B ..&.D5.Lo.....eK
00000090 D4 A2 50 3B 05 51 D2 00 BC 68 A8 74 92 96 EC BF ..P;.Q...h.t....
000000a0 A9 49 A6 FC FE F7 BD FF CE 0A 25 E2 F2 28 C4 1C .I........%..(..
000000b0 C1 8A AC 7F 01 D6 A4 C1 A0 67 9D D0 FB 09 E5 C7 ...[.....g......
000000c0 D6 B8 51 71 56 90 ED 90 C8 25 2B D6 24 74 84 CE ..QqV....%+.$t..
000000d0 72 71 BC D4 A6 C5 D5 8D 91 6C 2A 93 D5 82 DE 8D rq.......l*.....
000000e0 E5 1C DA 62 E7 FC 15 70 E7 C6 ED 53 04 BD 4A 43 ...b...p...S..JC
000000f0 A7 B3 C3 70 DA 84 B1 1D 85 AF FD 8B FE 4E 8E 5D ...p.........N.]

文件头(magic number)是什么?

- 怎么确定一个未知文件的文件头?
- 怎么确定其长度?
- 祖先是如何划分二十四节气?
- 每日周期可以通过日出日落，月呢？年呢？如何设计日历的?

凯撒密码如何被破解的



隐形的指纹—字母频率

密码的破译

- 单个特征重复频率
- 更多的样本，公有部分
- 最短的密文

csv文件解码

```
credits.csv:  5D 00 00 04 00 4F 02 00  00 00 11 13 88 26 D3 4D    46 2E C5 BA A5 53 6B 56  08 84 CF 8B 5B 2E D8 7C
effects.csv:  5D 00 00 04 00 9B B0 00  00 00 11 13 88 26 D3 4D    46 2E B6 8E EC 5F 6C 4B  7A 3B 1A 1F 1E BB 39 79
  music.csv:  5D 00 00 04 00 BE 03 00  00 00 11 13 88 26 D3 4D    46 2E B6 8A 1F 5E 04 B3  2F A2 F7 83 07 D2 03 39
 sounds.csv:  5D 00 00 04 00 86 84 00  00 00 11 13 88 26 D3 4D    46 2E B6 8A 1F 5E 04 B0  76 5C 57 E7 BA 60 89 20
```

5d 00 00 04 file heaher\magic number\file signature
5d 00 00 file heaher\magic number\file signature

LZMA
0x5d at the beginning (it's a flag), a 32bit field (size of the dictionary) and the lzma data.
The raw lzma stream usually starts with a 0x00 (offset 0x5)
Note: if you use "comptype lzma_compress" in QuickBMS to compress data, your output will start with 0x2c instead

Code:

```
5d 00 00 00 08 00 44 94 a6 b1 a9 14 37 65 03 e8   ].....D.....7e..
61 4e b5 0a 29 f7 bc f4 0a 39 10 76 ec 9c fe 41   aN..)....9.v...A
1a 6a 07 81 ce e1 e0 58 3f 2f a1 6a c9 03 2d 24   .j.....X?/.j..-$
38 74 b0 3d 19 ab 33 0c 73 57 75 94 da 8a ac 7e   8t.=..3.sWu....~
```

lzma 86 head
As before with a 64bit uncompressed size field before the compressed data.

Code:

```
5d 00 00 00 08 cf 07 00 00 00 00 00 00 00 44 94   ]..............D.
a6 b1 a9 14 37 65 03 e8 61 4e b5 0a 29 f7 bc f4   ....7e..aN..)...
0a 39 10 76 ec 9c fe 41 1a 6a 07 81 ce e1 e0 58   .9.v...A.j.....X
3f 2f a1 6a c9 03 2d 24 38 74 b0 3d 19 ab 33 0c   ?/.j..-$8t.=..3.
```

lzma 86 dec
One byte more than lzma.

Code:

```
5d 00 00 00 08 00 00 44 94 a6 b1 a9 14 37 65 03   ].....D.....7e.
e8 61 4e b5 0a 29 f7 bc f4 0a 39 10 76 ec 9c fe   .aN..)....9.v...
41 1a 6a 07 81 ce e1 e0 58 3f 2f a1 6a c9 03 2d   A.j.....X?/.j..-
24 38 74 b0 3d 19 ab 33 0c 73 57 75 94 da 8a ac   $8t.=..3.sWu....
```

lzma 86 dec head
All the fields seen before.

Code:

```
5d 00 00 00 08 00 cf 07 00 00 00 00 00 00 00 44   ]..............D
94 a6 b1 a9 14 37 65 03 e8 61 4e b5 0a 29 f7 bc   .....7e..aN..)..
f4 0a 39 10 76 ec 9c fe 41 1a 6a 07 81 ce e1 e0   ..9.v...A.j.....
58 3f 2f a1 6a c9 03 2d 24 38 74 b0 3d 19 ab 33   X?/.j..-$8t.=..3
```

lzma efs
Used by the ZIP file format.

Code:

```
5d 00 00 00 08 00 00 05 00 00 44 94 a6 b1 a9 14   ].........D.....
37 65 03 e8 61 4e b5 0a 29 f7 bc f4 0a 39 10 76   7e..aN..)....9.v
```

LZMA file format

The LZMA header is not well documented. It's also a bit usual: it doesn't appear to have a magic byte prefix, as one would expect from a modern file format, and it not word-aligned. Nevertheless:

```
Offset Size  Description
  0     1    lc, lp and pb in encoded form
  1     4    dictSize (little endian)
  5     8    uncompressed size (little endian)
```

For the nine compression levels above, the five magic bytes are:

```
-1   5d 00 00 01 00
-2   5d 00 00 10 00
-3   5d 00 00 08 00
-4   5d 00 00 10 00
-5   5d 00 00 20 00
-6   5d 00 00 40 00
-7   5d 00 00 80 00
-8   5d 00 00 00 01
-9   5d 00 00 00 02
```

The `.lzma86` format adds an optional extra filter to better compress x86 executables. It begins with a one-byte prefix, which is `0` for standard LZMA and `1` to indicate that the x86 filter is applied. The remainder of the format is the same. (This package doesn't support lzma86 de/compression.)

lzma是什么

- LZMA，（Lempel-Ziv-Markov chain-Algorithm的缩写），是一个Deflate和LZ77算法改良和优化后的压缩算法，开发者是Igor Pavlov，2001年被首次应用于7-Zip压缩工具中，是 2001年以来得到发展的一个数据压缩算法。它使用类似于 LZ77 的字典编码机制，在一般的情况下压缩率比 bzip2 为高，用于压缩的可变字典最大可达4GB。
- 多数路由器的bin更新包都是lzma压缩的
- http://sudo-kill-all.blogspot.tw/2015/06/tutorial-unpacking-cable-modem-firmware.html
- http://zenhax.com/viewtopic.php?t=27
- https://github.com/cscott/lzma-purejs/blob/master/FORMAT.md
- ftp://ftp.uni-bayreuth.de/pub/packages/tools/lzma/tukaani.org/lzma/header-format-12.txt

LZMA的RFC

ftp://ftp.uni-bayreuth.de/pub/packages/tools/lzma/
tukaani.org/lzma/header-format-12.txt

- the number of literal context bits (lc, [0, 8]);
- the number of literal position bits (lp, [0, 4]); and
- the number of position bits (pb, [0, 4]).

csv解码

- 样本：credits.csv:　5D 00 00 04 00 4F 02 00　00 00 11 13 88 26 D3 4D　46 2E C5 BA A5 53 6B 56 08 84 CF 8B 5B 2E D8 7C
- 5D 00 00 04 00　文件magic Number
- 4F 02 00　00 00 11 13 88 为未压缩之前的文件大小?但所有文件的文件头里都有11 13 88
- 难道未压缩之前的文件大小是11 13 88之前的?

csv解码

回顾之前的几个文件，找下11 13 88之前的字节流内容

4F 02 00 00 00

9B B0 00 00 00

BE 03 00 00 00

86 84 00 00 00

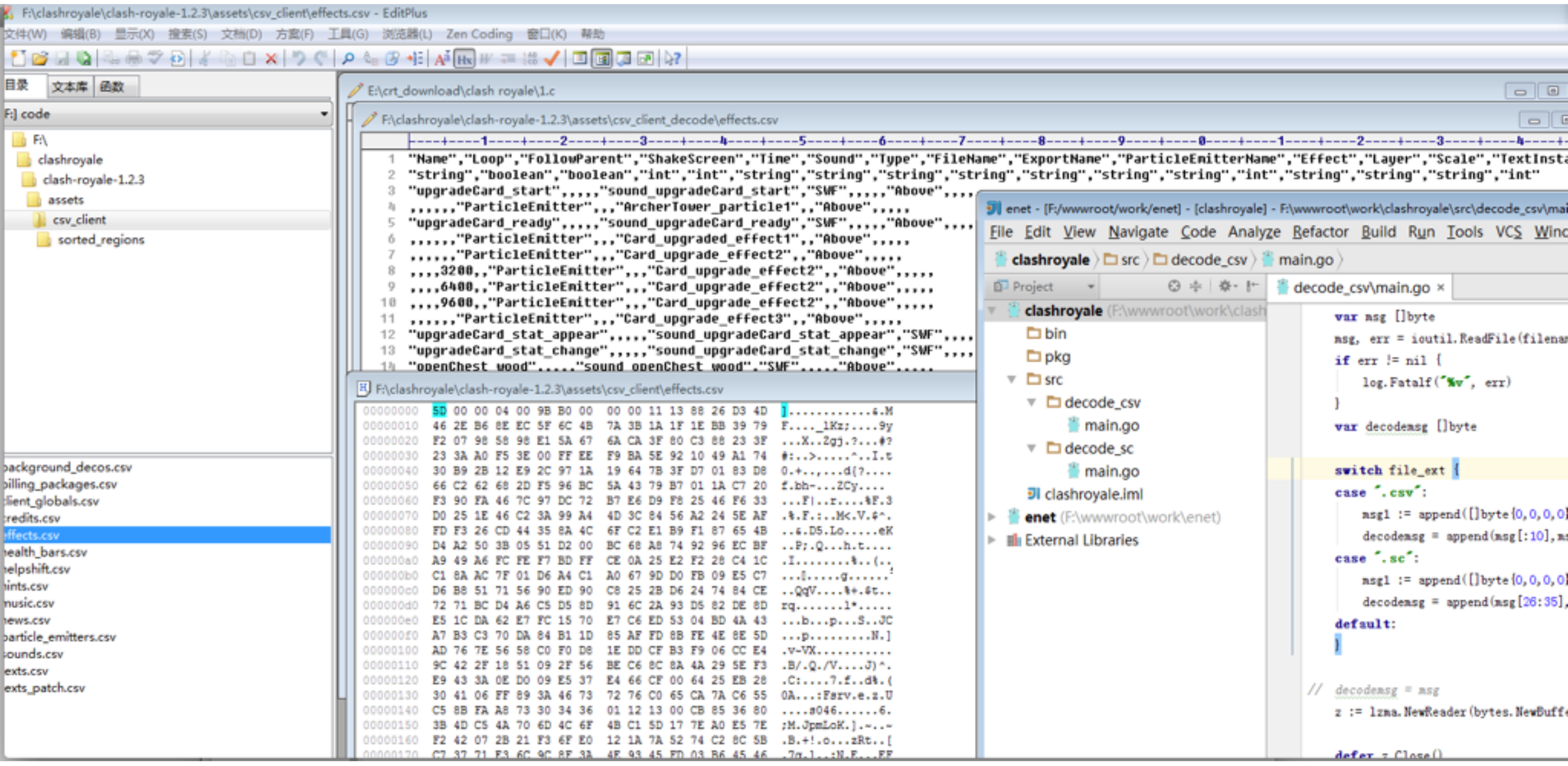
csv解码

- 小端处理之后分别是：591、2971、958、33926,好像数字很大?
- 但这单位是字节，实际上就是1K,3KB,1KB,33K的样子。
- 对照压缩后的大小，发现压缩比率也差不多。

csv解码

- 取前面5位作为length的值来解压试试?
- 开源的lzma类库都是8字节的长度，它这个是5字节，咋办?
- 改类库？好像挺麻烦。我补3个0x00呢?
- 还是不对...
- 会不会“4F 02 00 00 00”里的最后一位的00是literal position bits的部分呢?
- 补4个试试?
- 正确了...
- 但暴力尝试好像很傻....没办法，对lzma不熟悉

csv解码


F:\clashroyale\clash-royale-1.2.3\assets\csv_client\effects.csv - EditPlus
文件(W) 编辑(B) 显示(X) 搜索(S) 文档(D) 方案(F) 工具(G) 浏览器(L) Zen Coding 窗口(K) 帮助
目录 文本库 函数
F:) code
F:\
clashroyale
clash-royale-1.2.3
assets
csv_client
sorted_regions
background_decos.csv
billing_packages.csv
client_globals.csv
credits.csv
effects.csv
health_bars.csv
helpshift.csv
hints.csv
music.csv
news.csv
particle_emitters.csv
sounds.csv
texts.csv
texts_patch.csv
E:\crt_download\clash royale\1.c
F:\clashroyale\clash-royale-1.2.3\assets\csv_client_decode\effects.csv
1 "Name","Loop","FollowParent","ShakeScreen","Time","Sound","Type","FileName","ExportName","ParticleEmitterName","Effect","Layer","Scale","TextInsta
2 "string","boolean","boolean","int","int","string","string","string","string","string","string","string","int","string","string","string","int"
3 "upgradeCard_start",,,,,"sound_upgradeCard_start","SWF",,,,,"Above",,,,
4 ,,,,,,"ParticleEmitter",,,"ArcherTower_particle1",,"Above",,,,,
5 "upgradeCard_ready",,,,,"sound_upgradeCard_ready","SWF",,,,,"Above",,,,
6 ,,,,,,"ParticleEmitter",,,"Card_upgraded_effect1",,"Above",,,,,
7 ,,,,,,"ParticleEmitter",,,"Card_upgrade_effect2",,"Above",,,,,
8 ,,,,3200,,"ParticleEmitter",,,"Card_upgrade_effect2",,"Above",,,,,
9 ,,,,6400,,"ParticleEmitter",,,"Card_upgrade_effect2",,"Above",,,,,
10 ,,,,9600,,"ParticleEmitter",,,"Card_upgrade_effect2",,"Above",,,,,
11 ,,,,,,"ParticleEmitter",,,"Card_upgrade_effect3",,"Above",,,,,
12 "upgradeCard_stat_appear",,,,,"sound_upgradeCard_stat_appear","SWF",,,,
13 "upgradeCard_stat_change",,,,,"sound_upgradeCard_stat_change","SWF",,,,
14 "openChest_wood",,,,,"sound_openChest_wood","SWF",,,,,"Above",,,,,
F:\clashroyale\clash-royale-1.2.3\assets\csv_client\effects.csv
00000000 5D 00 00 04 00 9B B0 00 00 00 11 13 88 26 D3 4D]............&.M
00000010 46 2E B6 8E EC 5F 6C 4B 7A 3B 1A 1F 1E BB 39 79 F...._lKz;....9y
00000020 F2 07 98 58 98 E1 5A 67 6A CA 3F 80 C3 88 23 3F ...X..Zgj.?...#?
00000030 23 3A A0 F5 3E 00 FF EE F9 BA 5E 92 10 49 A1 74 #:..>.....^..I.t
00000040 30 B9 2B 12 E9 2C 97 1A 19 64 7B 3F D7 01 83 D8 0.+..,...d{?....
00000050 66 C2 62 68 2D F5 96 BC 5A 43 79 B7 01 1A C7 20 f.bh-...ZCy....
00000060 F3 90 FA 46 7C 97 DC 72 B7 E6 D9 F8 25 46 F6 33 ...F|..r....%F.3
00000070 D0 25 1E 46 C2 3A 99 A4 4D 3C 84 56 A2 24 5E AF .%.F.:..M<.V.$^.
00000080 FD F3 26 CD 44 35 8A 4C 6F C2 E1 B9 F1 87 65 4B ..&.D5.Lo.....eK
00000090 D4 A2 50 3B 05 51 D2 00 BC 68 A8 74 92 96 EC BF ..P;.Q...h.t....
000000a0 A9 49 A6 FC FE F7 BD FF CE 0A 25 E2 F2 28 C4 1C .I........%..(..
000000b0 C1 8A AC 7F 01 D6 A4 C1 A0 67 9D D0 FB 09 E5 C7 .....g.....
000000c0 D6 B8 51 71 56 90 ED 90 C8 25 2B D6 24 74 84 CE ..QqV....%+.$t..
000000d0 72 71 BC D4 A6 C5 D5 8D 91 6C 2A 93 D5 82 DE 8D rq.......l*.....
000000e0 E5 1C DA 62 E7 FC 15 70 E7 C6 ED 53 04 BD 4A 43 ...b...p...S..JC
000000f0 A7 B3 C3 70 DA 84 B1 1D 85 AF FD 8B FE 4E 8E 5D ...p.........N.]
00000100 AD 76 7E 56 58 C0 F0 D8 1E DD CF B3 F9 06 CC E4 .v~VX...........
00000110 9C 42 2F 18 51 09 2F 56 BE C6 8C 8A 4A 29 5E F3 .B/.Q./V....J)^.
00000120 E9 43 3A 0E D0 09 E5 37 E4 66 CF 00 64 25 EB 28 .C:....7.f..d%.(
00000130 30 41 06 FF 89 3A 46 73 72 76 C0 65 CA 7A C6 55 0A...:Fsrv.e.z.U
00000140 C5 8B FA A8 73 30 34 36 01 12 13 00 CB 85 36 80 ....s046......6.
00000150 3B 4D C5 4A 70 6D 4C 6F 4B C1 5D 17 7E A0 E5 7E ;M.JpmLoK.].~..~
00000160 F2 42 07 2B 21 F3 6F E0 12 1A 7A 52 74 C2 8C 5B .B.+!.o...zRt..[
00000170 C7 37 71 F3 6C 9C 8F 3A 4F 93 45 FD 03 B6 45 46 .7q.l..:N.E...EF
enet - [F:/wwwroot/work/enet] - [clashroyale] - F:\wwwroot\work\clashroyale\src\decode_csv\mai
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Winc
clashroyale src decode_csv main.go
Project
clashroyale (F:\wwwroot\work\clash
bin
pkg
src
decode_csv
main.go
decode_sc
main.go
clashroyale.iml
enet (F:\wwwroot\work\enet)
External Libraries
decode_csv\main.go ×
var msg []byte
msg, err = ioutil.ReadFile(filena
if err != nil {
log.Fatalf("%v", err)
}
var decodemsg []byte
switch file_ext {
case ".csv":
msg1 := append([]byte{0,0,0,0
decodemsg = append(msg[:10],ms
case ".sc":
msg1 := append([]byte{0,0,0,0
decodemsg = append(msg[26:35],
default:
}
// decodemsg = msg
z := lzma.NewReader(bytes.NewBuff
defer z.Close()

另一种

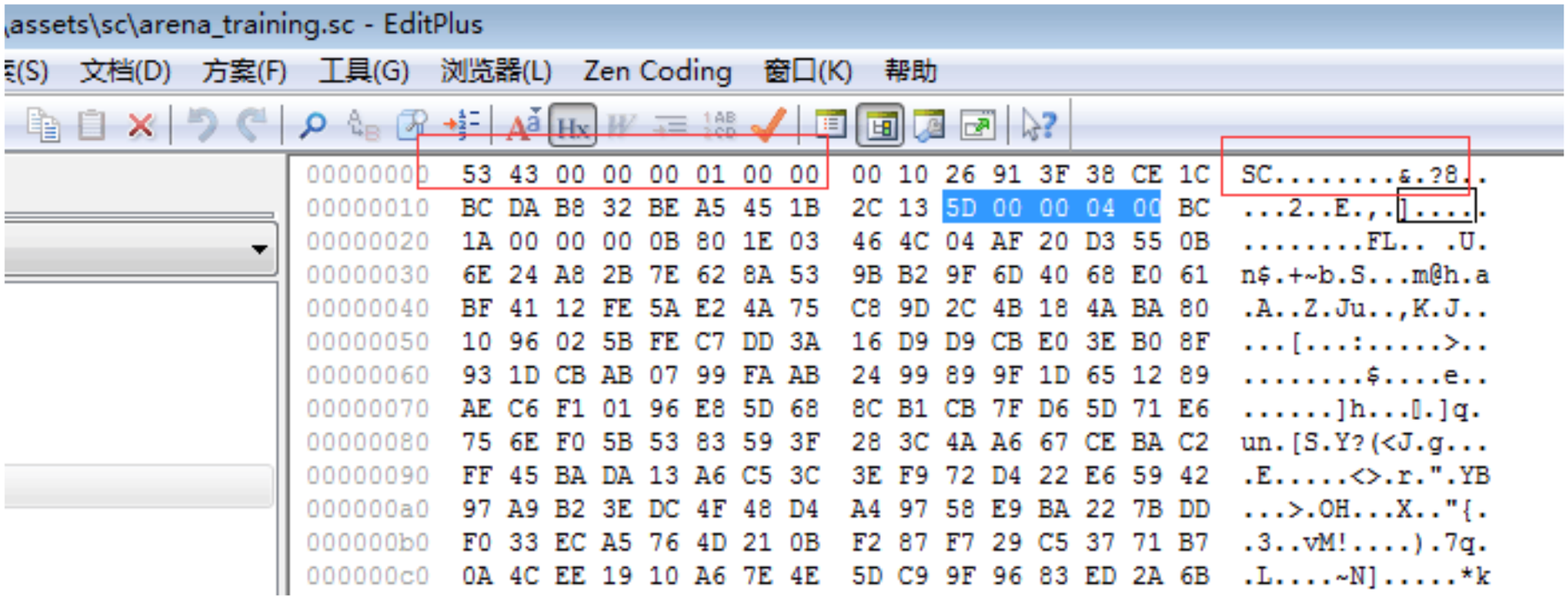
- 若样本数量少，或者所有文件都“加密”在一个文件中呢?
- 很大的文件头，记录文件总数，以及每个文件的长度?
- 按照段落存储每个文件? 参见我对LOL OB录像文件存储格式解密http://www.cnxct.com/how-to-watch-lol-tencent-ob-on-mac-osx/
- 他们自己的程序总要读取吧? （动态调试）

SC文件解码

- 照葫芦画瓢
- 直接看文件头?

```
building_barbarian_hut.sc :53 43 00 00 00 01 00 00  00 10 C7 3E 67 9D AC 90
building_bomb_tower.sc    :53 43 00 00 00 01 00 00  00 10 50 2F AB B7 BF 78
building_mortar.sc        :53 43 00 00 00 01 00 00  00 10 17 80 6D 53 C1 F3
```

SC文件解码




```
building_barbarian_hut.sc :53 43 00 00 00 01 00 00  00 10 C7 3E 67 9D AC 90
building_bomb_tower.sc    :53 43 00 00 00 01 00 00  00 10 50 2F AB B7 BF 78
building_mortar.sc        :53 43 00 00 00 01 00 00  00 10 17 80 6D 53 C1 F3
```

SC文件解码

- Magic Number:53 43 00 00 00 01 00 00 00 10
- 公开资料中，根本搜不到这种文件头的规范
- 是SuperCell自定义的?
- 0x53\0x43是什么?
- ASCII中对应S、C

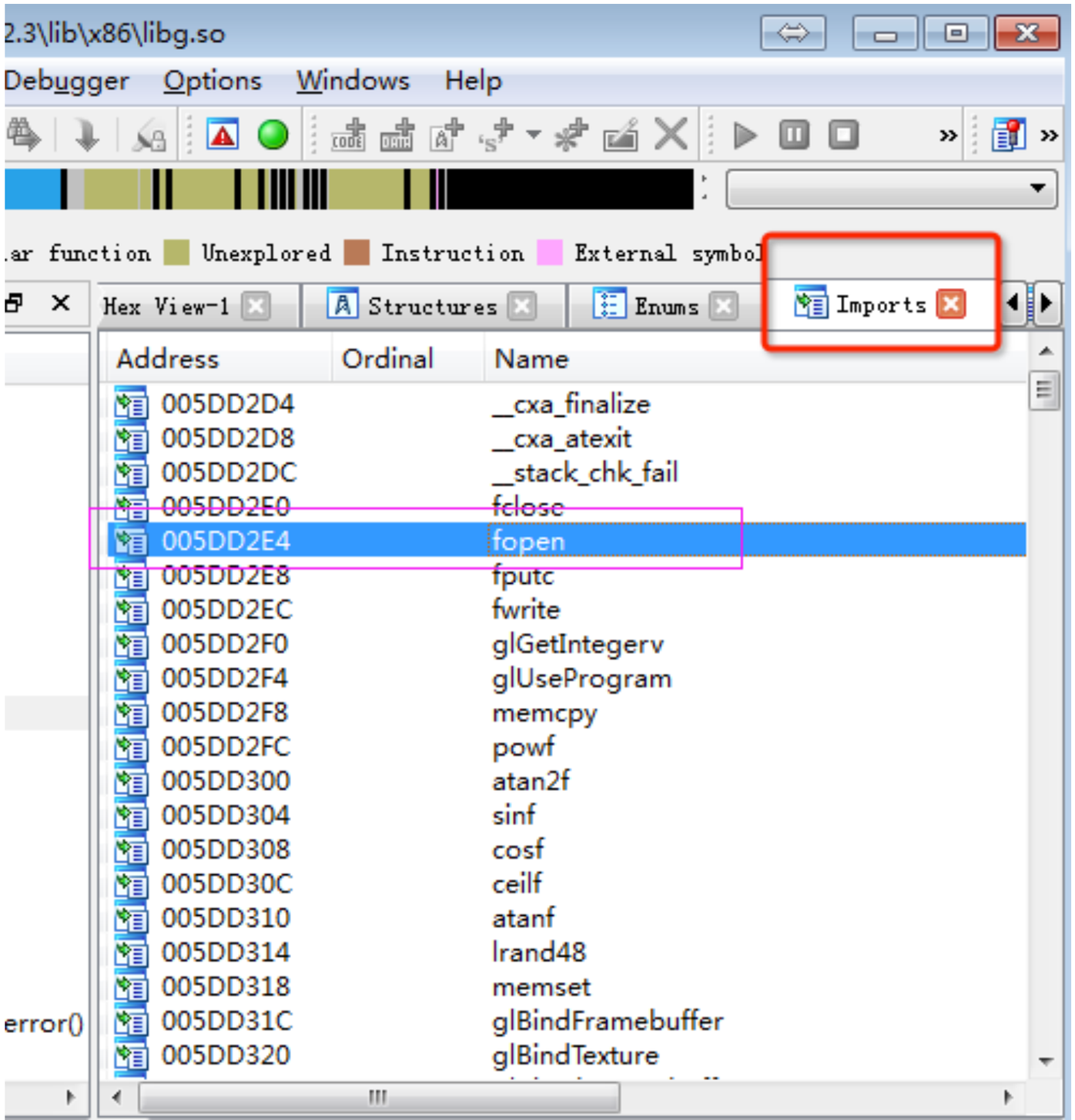
解铃还须系铃人

- 它自己总要读的吧
- 静态分析
- 动态调试分析
- 手游，一般调试android，你懂的
- android的java代码反编译，相信大家都搞得定
- 多数软件会把核心代码写到SO动态链接库中

代码是如何编写的

- Linux C中读文件是fopen
- 写个函数封装下fopen
- 再写个函数调用下刚刚的函数
- 打开文件后，读取
- 读取后，解码还原

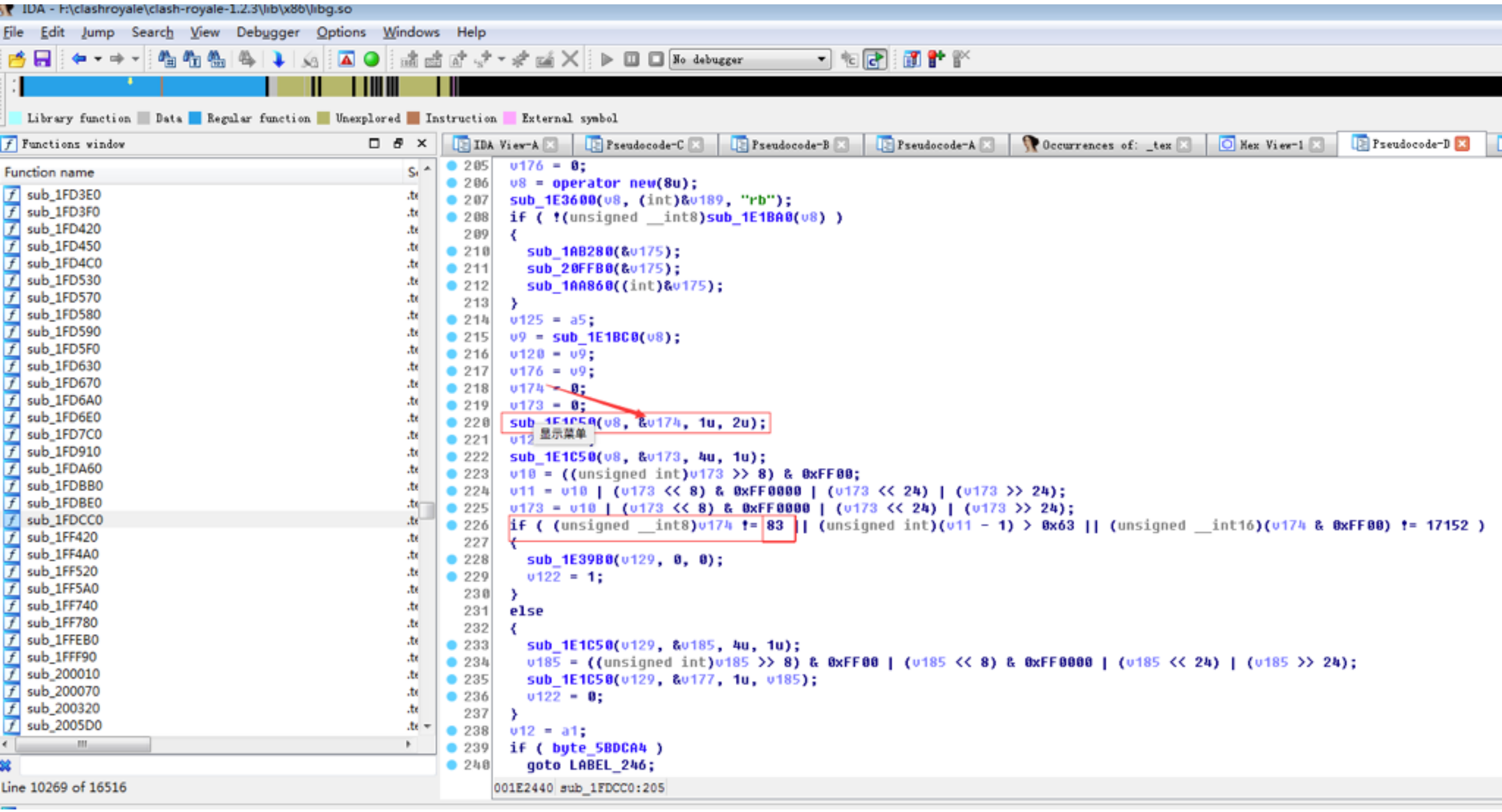
那我们从fopen开始吧



艰难的过程

- 调用 fopen的函数可能会很多
- 调用封装fopen函数的函数也会很多
- 如何筛选
- 调用时，总得传文件名吧?
- 万一是遍历目录呢？文件名是动态的。
- 但目录你总得传吧
- 配合多种信息，定位到目标函数

功夫不负有心人


IDA - F:\clashroyale\clash-royale-1.2.3\lib\x86\libg.so
File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
sub_1FD3E0
sub_1FD3F0
sub_1FD420
sub_1FD450
sub_1FD4C0
sub_1FD530
sub_1FD570
sub_1FD580
sub_1FD590
sub_1FD5F0
sub_1FD630
sub_1FD670
sub_1FD6A0
sub_1FD6E0
sub_1FD7C0
sub_1FD910
sub_1FDA60
sub_1FDBB0
sub_1FDBE0
sub_1FDCC0
sub_1FF420
sub_1FF4A0
sub_1FF520
sub_1FF5A0
sub_1FF740
sub_1FF780
sub_1FFEB0
sub_1FFF90
sub_200010
sub_200070
sub_200320
sub_2005D0
Line 10269 of 16516
IDA View-A
Pseudocode-C
Pseudocode-B
Pseudocode-A
Occurrences of: _tex
Hex View-1
Pseudocode-D
205 v176 = 0;
206 v8 = operator new(8u);
207 sub_1E3600(v8, (int)&v189, "rb");
208 if (!(unsigned __int8)sub_1E1BA0(v8))
209 {
210 sub_1AB280(&v175);
211 sub_20FFB0(&v175);
212 sub_1AA860((int)&v175);
213 }
214 v125 = a5;
215 v9 = sub_1E1BC0(v8);
216 v120 = v9;
217 v176 = v9;
218 v174 = 0;
219 v173 = 0;
220 sub_1E1C50(v8, &v174, 1u, 2u);
显示菜单
222 sub_1E1C50(v8, &v173, 4u, 1u);
223 v10 = ((unsigned int)v173 >> 8) & 0xFF00;
224 v11 = v10 | (v173 << 8) & 0xFF0000 | (v173 << 24) | (v173 >> 24);
225 v173 = v10 | (v173 << 8) & 0xFF0000 | (v173 << 24) | (v173 >> 24);
226 if ((unsigned __int8)v174 != 83 || (unsigned int)(v11 - 1) > 0x63 || (unsigned __int16)(v174 & 0xFF00) != 17152)
227 {
228 sub_1E39B0(v129, 0, 0);
229 v122 = 1;
230 }
231 else
232 {
233 sub_1E1C50(v129, &v185, 4u, 1u);
234 v185 = ((unsigned int)v185 >> 8) & 0xFF00 | (v185 << 8) & 0xFF0000 | (v185 << 24) | (v185 >> 24);
235 sub_1E1C50(v129, &v177, 1u, v185);
236 v122 = 0;
237 }
238 v12 = a1;
239 if (byte_5BDCA4)
240 goto LABEL_246;
001E2440 sub_1FDCC0:205

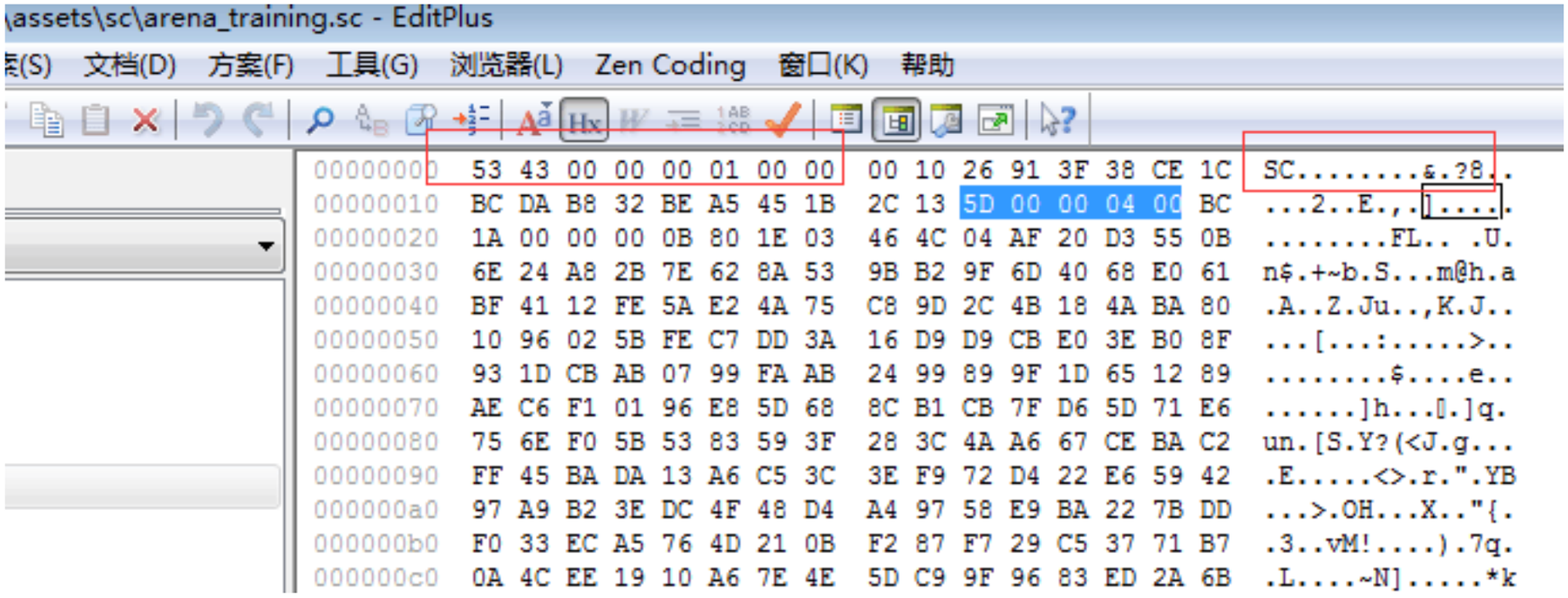
sc文件读取函数

- 以clash royale android 1.2.3为例(国外版),函数名是IDA根据所处文件中的位置给的
- 函数定位在sub_1FDCC0处
- 读取文件函数是sub_1E1C50
- 是它吗?
- v174 !=83 ， 记得刚刚的SC文件的magic number吗?
- 字母S，ASCII是0x53， 十进制是?

我搞不下去了

- 我逆向接触少，不太熟，对这个函数的反编译结果的理解，找了做二进制的大神帮忙
- 大神告诉我，前面的N字节只是用来存储该文件是否过期，是否变动之类，本身不含加密解密部分
- 大神很忙，甩给我一句话，就走了

再难还是要继续



再看SC文件的HEX格式内容，机智的你，肯定看到蓝色选中部分是多么的面熟，嗯，LZMA

LZMA解压之后

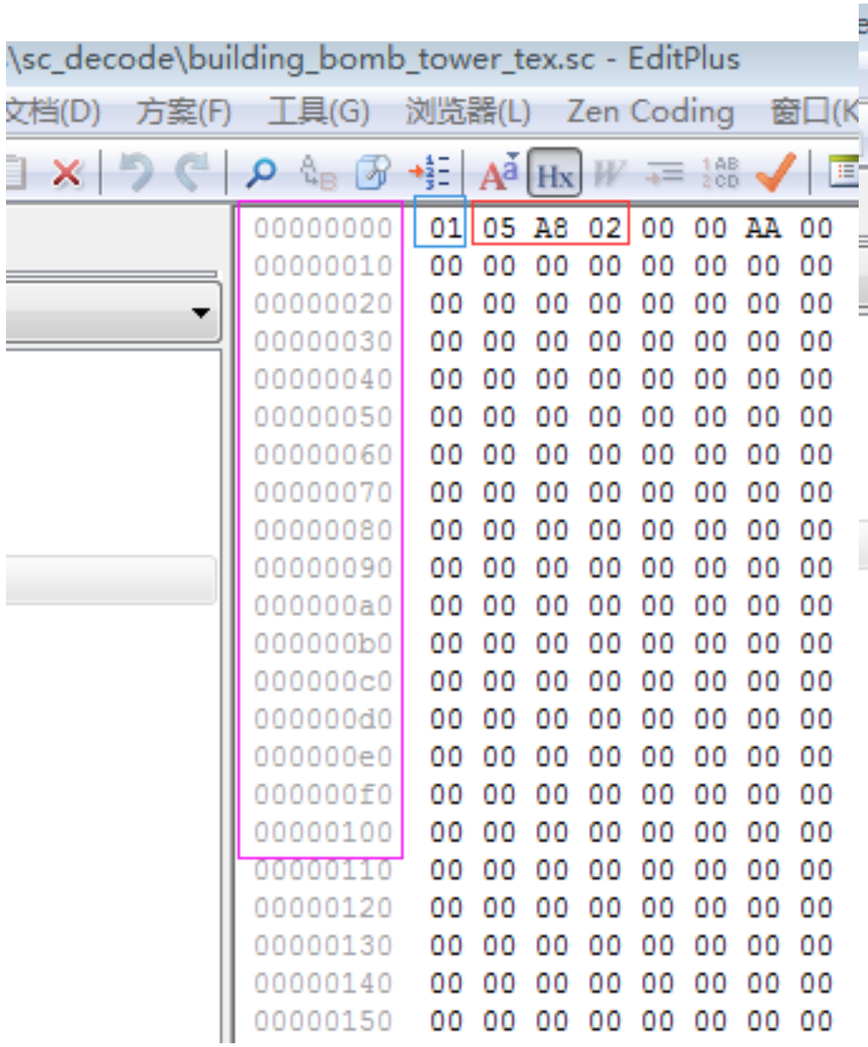
- 下面是多个文件存储在一个文件中了
- 如何解码呢
- 嗯，这是SuperCell的游戏
- 嗯，我还记得Clash Royale的协议上是雷同COC的
- 嗯，那这个SC文件格式，是不是也类似COC呢
- 嗯，是的，又可以站在大神的肩膀上了

也并不是一样

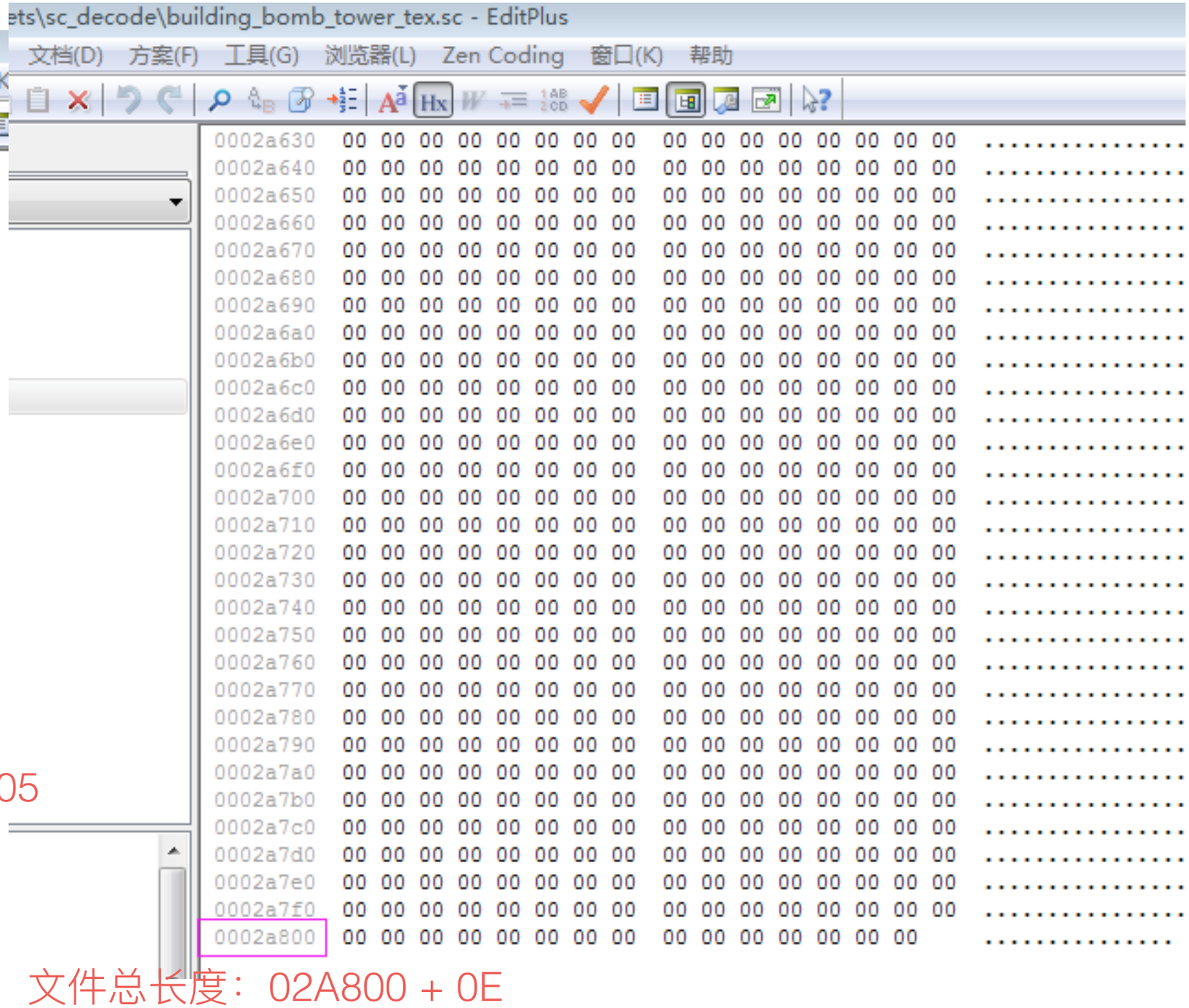
- IDA的静态分析过程中，看到过针对_tex.sc文件名与不是以这个结束的文件的分开处理

- _tex.sc与COC的lzma之后的内容存储拼装格式一致

_tex.sc文件



Little endian 02 A8 05

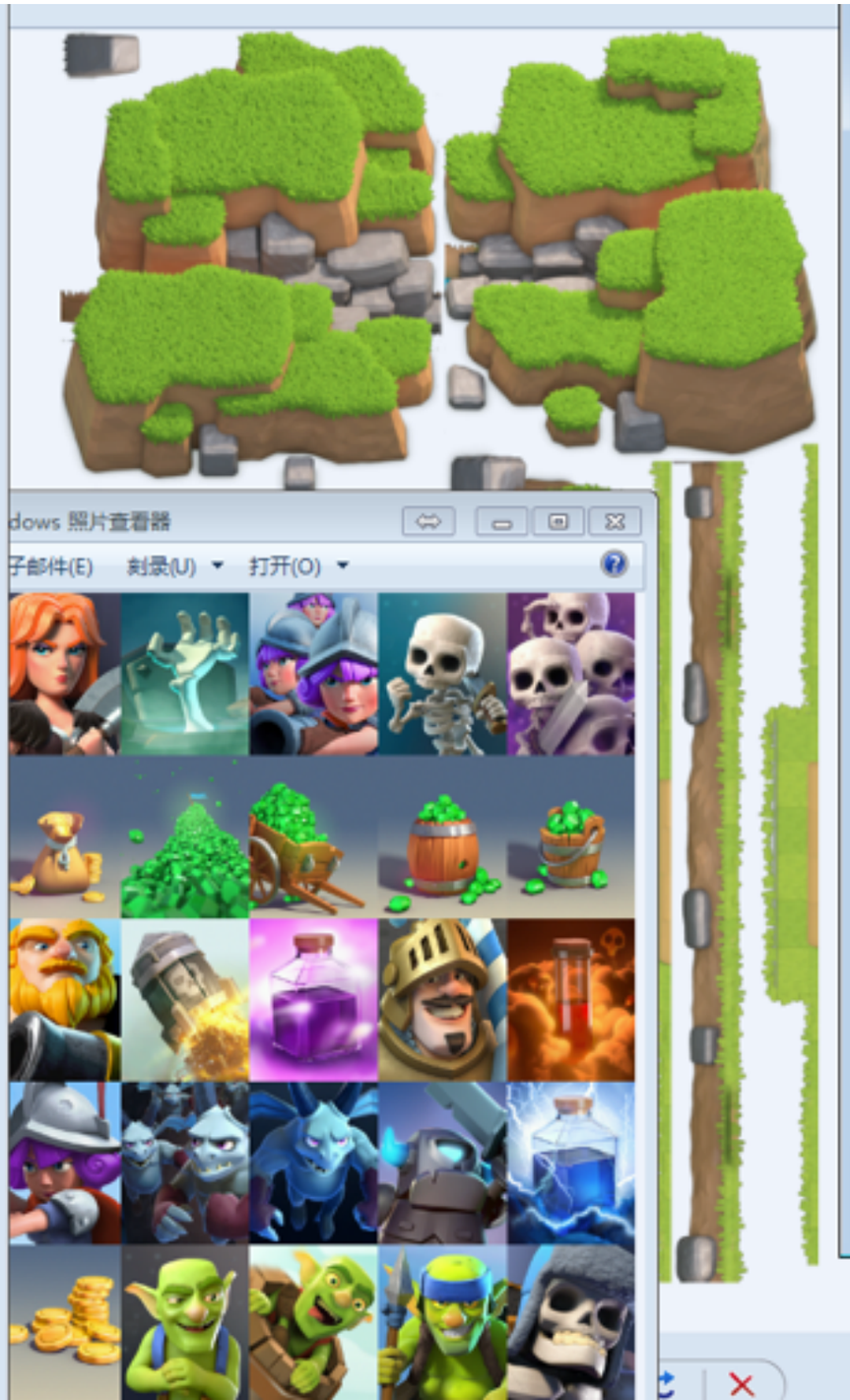


文件总长度：02A800 + 0E

SC文件的结果

- SC存的是图片文件，包括PNG等，一个SC可能存多个
- 正好上周做了PNG文件的读取，正好用到

SC文件解码预览



分析目的与作用

- 资源保护
- 资源压缩，减少包大小
- 资源借鉴(读书人的事，不能算偷)
- 协议安全设计
- 文件组成格式了解
- 知己知彼，百(zuo)战(de)不(geng)殆(hao)。

压缩的意义

- SC目录解压前大小57M
- 解压后大小326M
- 压缩率17%

本质

- 根本都没有二进制文件、文本文件一说，伪命题
- 不管消息包还是文件，都是字节流
- 字节流存储的都是字节
- 看或者不看，它都在那里
- 它一直都是字节流，看你(关联的软件)怎么解读
- 文本文件，图片文件，甚至so链接库、exe二进制都一样

内部产品检测

- 《大皇帝》、《少三》lua脚本加密
- 《大皇帝》、《少三》美术资源加密
- 通讯协议部分暂时还没时间去看

E:\迅雷下载\大皇帝OL_游族_1.3.0_release\assets\src\28a27819a94d19e8616e3bbc58b55346_app.luac - EditPlus

文件(W) 编辑(B) 显示(X) 搜索(S) 文档(D) 方案(F) 工具(G) 浏览器(L) Zen Coding 窗口(K) 帮助

目录 文本库 函数

[E:]

- E:\
  - 迅雷下载
    - 大皇帝OL_游族_1.3.0_release
      - assets
        - src
          - basic
          - cocos
          - common
          - config
          - packages
          - platform
          - plugin_activityoperations
          - plugin_activityplatform
          - plugin_caochuan
          - plugin_challenge
          - plugin_city
          - plugin_citywar
          - plugin_crossarena
          - plugin_fight
          - plugin_gvg
          - plugin_haremnew
          - plugin_hero
          - plugin_huarongdao
          - plugin_jieting

28a27819a94d19e8616e3bbc58b55346_app.luac
766d43465e6af9f02ac061c0f8be5808_clear.luac
7b13b0e19639b43425f65c439dda414e_framework.luac
config.luac
main.luac

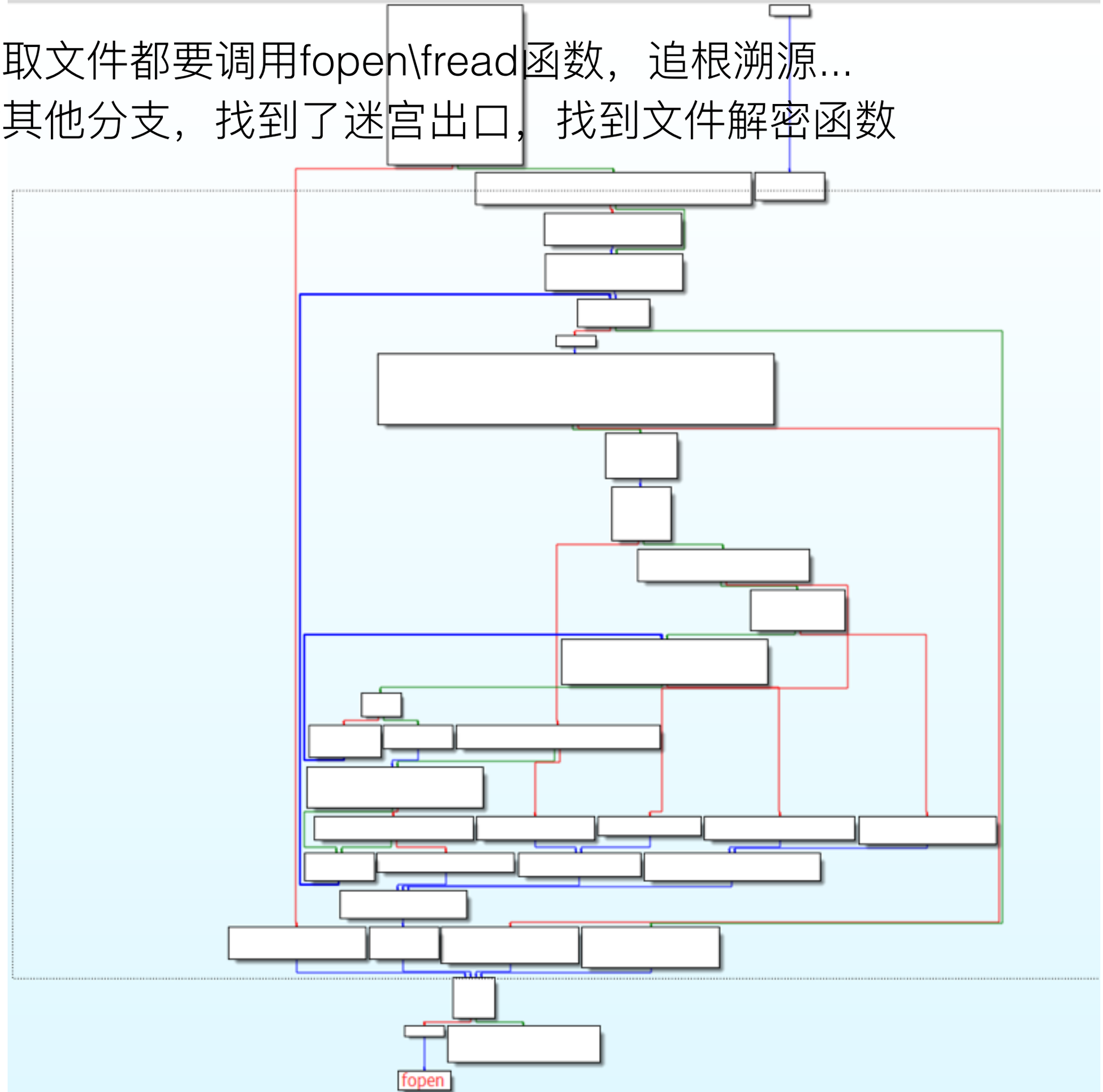
```
00000000  58 58 54 45 41 31 42 03  A7 A9 B5 D2 83 62 87 91  XXTEA1B......b..
00000010  EB 50 90 4C 6D 4A CE 52  59 F8 3C 11 94 8C 80 8F  .P.LmJ.RY.<.....
00000020  B8 A9 18 D9 8B 1A 32 60  62 67 CA 43 23 C8 EE BE  ......2`bg.C#...
00000030  CB B8 3B DE D4 F7 90 64  37 09 A2 3A F8 8A D2 77  ..;....d7..:...w
00000040  D3 AF 6C 1F 5E A4 4B 2E  17 89 82 3F 36 1D E8 4C  ..l.^.K....?6..L
00000050  5E C1 0F 8A BA 62 1C AB  79 AE FC 7A 86 37 C7 4C  ^....b..y..z.7.L
00000060  E4 0E DE BE 21 75 AE 77  FF 64 13 21 82 7C EE 89  ....!u.w.d.!.|..
00000070  DC 6F 30 10 A6 32 E7 54  F1 50 6A 5C AD 4E F5 C9  .o0..2.T.Pj\.N..
00000080  6A 47 6E 89 55 3F C8 1C  1A E7 B8 BE 88 42 80 06  jGn.U?.......B..
00000090  2F 48 C6 75 0B 8E 75 2B  8D BF DE 07 FA 02 9F 1E  /H.u..u+........
000000a0  96 0F 6C CC 2C 91 84 62  18 D2 A3 33 BA E0 58 0E  ..l.,..b...3..X.
000000b0  7C 79 10 1C 3C 7F AF 01  62 9D CE BA 8D ED 43 BD  |y..<[..b.....C.
000000c0  86 1E AA 07 70 03 E2 A3  59 F0 49 4A 43 36 B8 73  ....p...Y.IJC6.s
000000d0  C7 DA 0C C3 9A CC 3F E4  5E 7A AB 24 5B 0B D5 F5  ......?.^z.$[...
000000e0  E3 A7 4A F1 C0 7C F1 71  9A C2 3C E4 43 0E F3 D0  ..J..|.q..<.C...
000000f0  DF 8B 81 BD 3A 38 B8 FD  D5 66 1A B0 EC 78 16 16  ....:8...f...x..
00000100  22 F2 B7 77 A6 C2 00 E0  2E E8 B1 FC CD 54 2F 16  "..w.........T/.
00000110  8E 11 9F EC 4E 43 08 A9  C1 47 F8 4D 5E ED 71 62  ....NC...G.M^.qb
00000120  76 0B 1F A9 F8 3B FA 59  CC 35 A7 4A 7D A4 47 1C  v....;.Y.5.J}.G.
00000130  9C D5 B1 5D E2 B0 3E 76  7B 21 BB 8D B4 C2 63 1D  ...]..>v{!....c.
00000140  94 52 1A 91 85 55 BD 78  BD F1 83 FC 66 F5 85 48  .R...U.x....f..H
00000150  F7 05 55 F5 96 73 89 B3  DE EE 96 96 43 0A 30 9D  ..U..s......C.0.
00000160  C4 21 60 C2 92 7C CE 99  5F 51 F4 02 FA 17 78 E0  .!`..|.._Q....x.
00000170  AC 3E EF 36 30 0A 1A E4  02 EC 0C FE 41 D0 C0 19  .>.60.......A...
00000180  5D 67 A4 04 BA D2 60 CC  26 D1 C3 D1 D3 21 DD 81  ]g....`.&....!..
00000190  A9 07 03 75 04 EF 4D 9A  BB 63 E7 62 F2 2F 1D BF  ...u..M..c.b./..
000001a0  D4 77 C9 04 73 81 9A 76  6D 37 7C C1 D1 70 71 94  .w..s..vm7|..pq.
000001b0  F0 85 35 8B 8B 8C C1 4B  CB 29 88 7C 34 E9 68 10  ..5....K.).|4.h.
000001c0  6F 70 11 E1 B3 EB 47 8A  D2 3C 16 47 03 ED A1 07  op....G..<.G....
000001d0  A1 7F 96 26 04 EB 2D B7  A9 7F EC 72 0B C5 DE F3  .[.&..-..[.r....
000001e0  4D C4 4C 57 2F 5C 38 EF  4B 6F 36 EA 3E 2F 97 0B  M.LW/\8.Ko6.>/..
000001f0  4C D3 3C 5D 97 92 B9 77  CC EE 4C 43 3E BA CC BD  L.<]...w..LC>...
00000200  4C E7 0F 17 96 8D C2 BD  12 74 1B 3A 57 E7 41 26  L........t.:W.A&
00000210  2E 95 78 86 8E 09 DB B2  B1 6E 9A FE 1A 9D 59 6F  ..x......n....Yo
00000220  23 23 F1 71 CD 5D A8 1E  28 78 C7 FE 52 68 68 2B  ##.q.]..(x..Rhh+
00000230  E0 1E 8A 8D 38 11 EF D3  C9 BC CA A4 A0 29 5F 99  ....8........)_.
00000240  67 86 2D E3 B6 9A 25 20  F1 DA 99 DF DF DF 29 97  g.-...% ......).
00000250  E5 50 D6 37 E4 41 FC 79  E2 3A FF DB 14 D7 1D B5  .P.7.A.y.:......
00000260  4B 25 7B D5 2E A8 C5 42  C8 FA 6B 03 0E 97 04 B4  K%{....B..k.....
00000270  22 A3 18 05 30 B5 9F E8  59 2E 2F 7A D4 5A D3 E0  "...0...Y./z.Z..
00000280  AB 07 0F 5E 12 3E 11 A8  FA C2 39 A3 FF 22 5A 11  ...^.>....9.."Z.
00000290  BA A1 23 0C 3E 45 C0 D4  96 F5 07 D9 67 C0 9E FD  ..#.>E......g...
000002a0  D5 09 04 72 D5 A0 C5 8F  22 6E 6E 36 86 AE B9 8E  ...r....."nn6....
```

现状分析

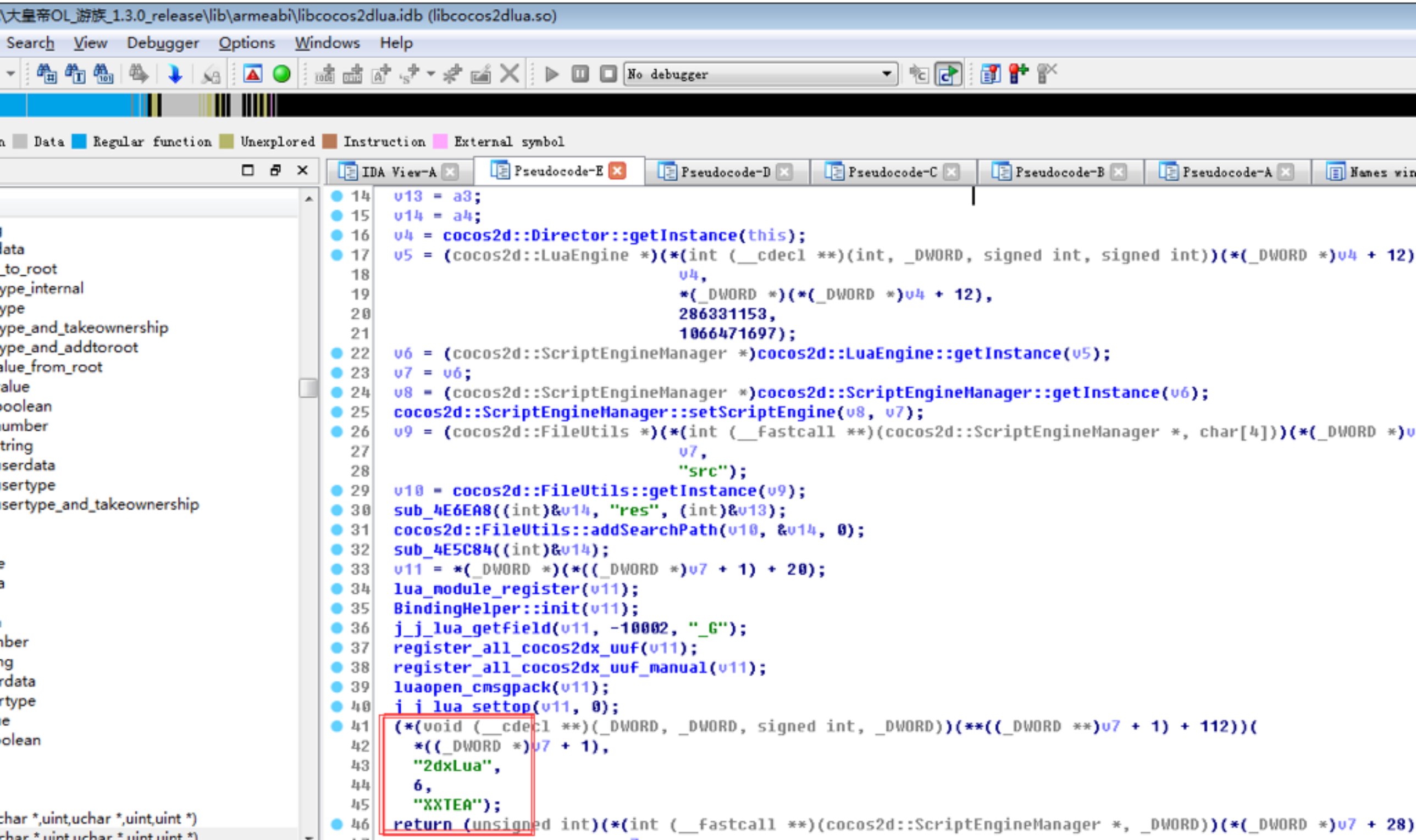
- luac文件magic number为58 58 54 45
- 一番检索，发现这都不是常规文件头
- 先进行静态分析，尝试找出解密方式
- 再进行动态分析，确认解密函数

读取文件都要调用fopen\fread函数，追根溯源...

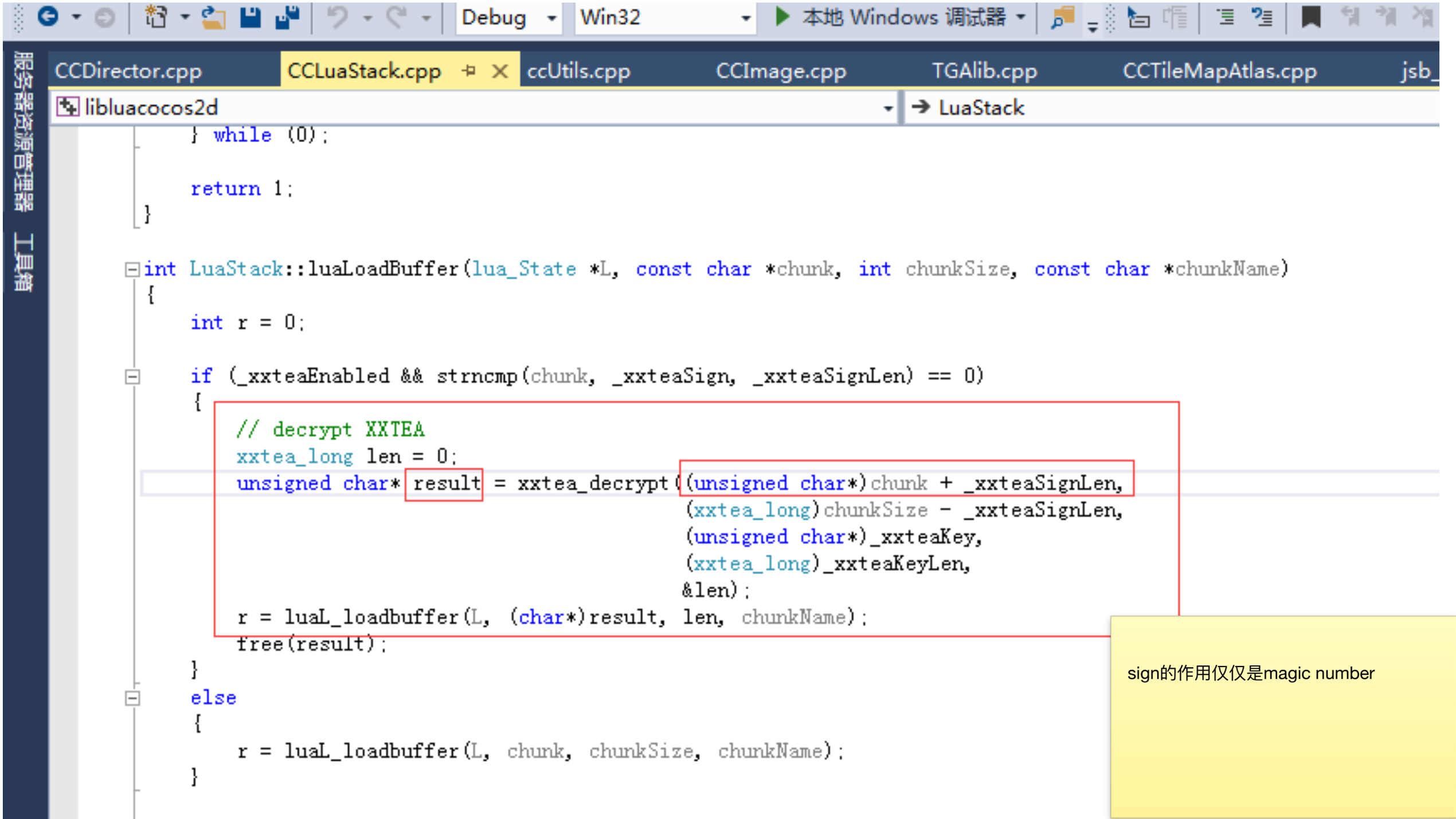
排除其他分支，找到了迷宫出口，找到文件解密函数



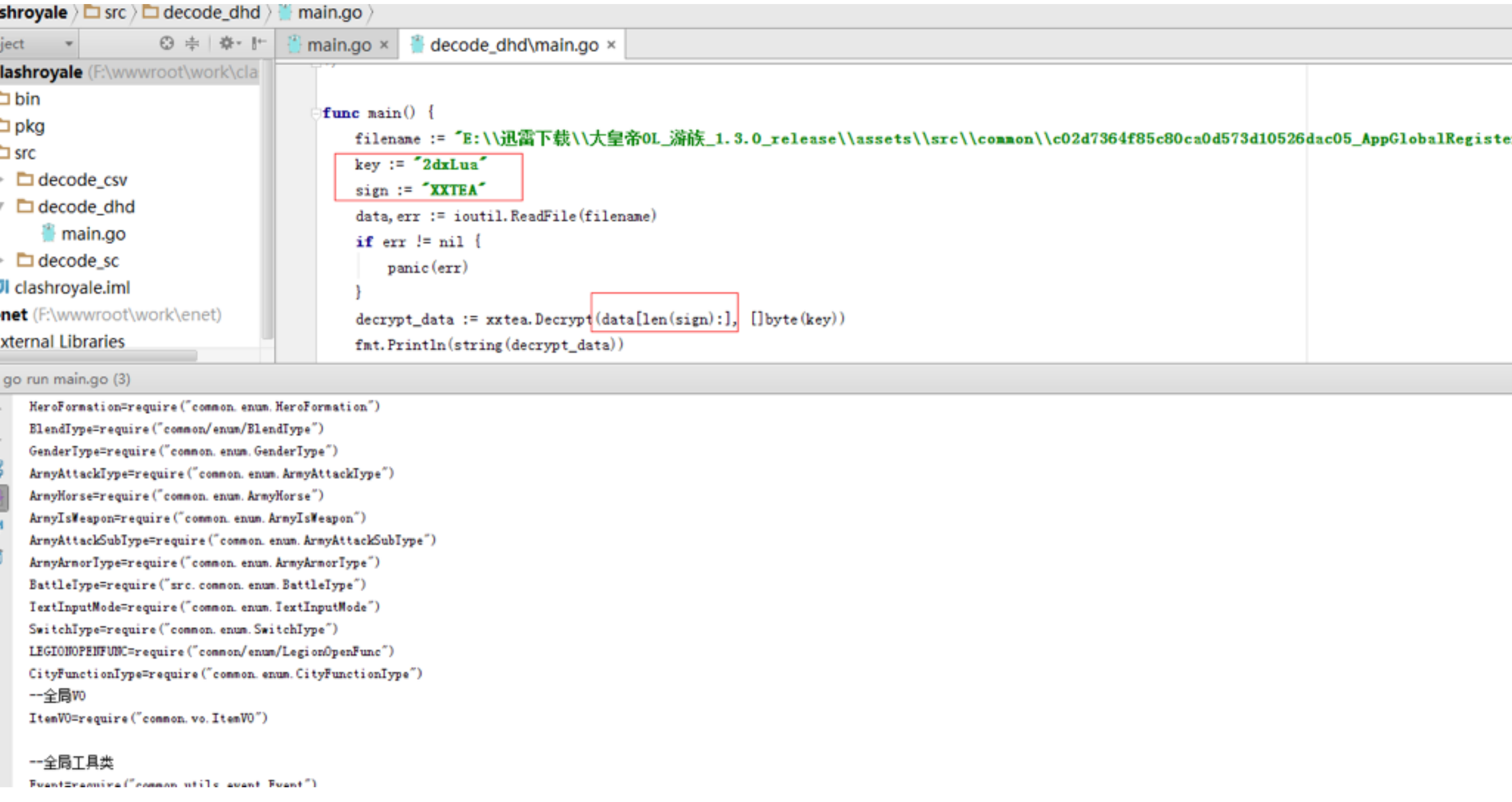
lua的加密


\大皇帝OL_游族_1.3.0_release\lib\armeabi\libcocos2dlua.idb (libcocos2dlua.so)
Search View Debugger Options Windows Help
No debugger
Data Regular function Unexplored Instruction External symbol
IDA View-A Pseudocode-E Pseudocode-D Pseudocode-C Pseudocode-B Pseudocode-A Names win
v13 = a3;
v14 = a4;
v4 = cocos2d::Director::getInstance(this);
v5 = (cocos2d::LuaEngine *)(*(int (__cdecl **)(int, _DWORD, signed int, signed int))(*(_DWORD *)v4 + 12)
v4,
*(_DWORD *)(*(_DWORD *)v4 + 12),
286331153,
1066471697);
v6 = (cocos2d::ScriptEngineManager *)cocos2d::LuaEngine::getInstance(v5);
v7 = v6;
v8 = (cocos2d::ScriptEngineManager *)cocos2d::ScriptEngineManager::getInstance(v6);
cocos2d::ScriptEngineManager::setScriptEngine(v8, v7);
v9 = (cocos2d::FileUtils *)(*(int (__fastcall **)(cocos2d::ScriptEngineManager *, char[4]))(*(_DWORD *)v
v7,
"src");
v10 = cocos2d::FileUtils::getInstance(v9);
sub_4E6EA8((int)&v14, "res", (int)&v13);
cocos2d::FileUtils::addSearchPath(v10, &v14, 0);
sub_4E5C84((int)&v14);
v11 = *(_DWORD *)(*((_DWORD *)v7 + 1) + 20);
lua_module_register(v11);
BindingHelper::init(v11);
j_j_lua_getfield(v11, -10002, "_G");
register_all_cocos2dx_uuf(v11);
register_all_cocos2dx_uuf_manual(v11);
luaopen_cmsgpack(v11);
j_j_lua_settop(v11, 0);
(*(void (__cdecl **)(_DWORD, _DWORD, signed int, _DWORD))(**((_DWORD **)v7 + 1) + 112))(
*((_DWORD *)v7 + 1),
"2dxLua",
6,
"XXTEA");
return (unsigned int)(*(int (__fastcall **)(cocos2d::ScriptEngineManager *, _DWORD))(*(_DWORD *)v7 + 28)
data
_to_root
ype_internal
ype
ype_and_takeownership
ype_and_addtoroot
alue_from_root
alue
oolean
umber
tring
serdata
sertype
sertype_and_takeownership
char *,uint,uchar *,uint,uint *)

查找源码验证猜测


Debug
Win32
本地 Windows 调试器
CCDirector.cpp
CCLuaStack.cpp
ccUtils.cpp
CCImage.cpp
TGAlib.cpp
CCTileMapAtlas.cpp
jsb_
libluacocos2d
LuaStack
} while (0);
return 1;
}
int LuaStack::luaLoadBuffer(lua_State *L, const char *chunk, int chunkSize, const char *chunkName)
{
int r = 0;
if (_xxteaEnabled && strncmp(chunk, _xxteaSign, _xxteaSignLen) == 0)
{
// decrypt XXTEA
xxtea_long len = 0;
unsigned char* result = xxtea_decrypt((unsigned char*)chunk + _xxteaSignLen,
(xxtea_long)chunkSize - _xxteaSignLen,
(unsigned char*)_xxteaKey,
(xxtea_long)_xxteaKeyLen,
&len);
r = luaL_loadbuffer(L, (char*)result, len, chunkName);
free(result);
}
else
{
r = luaL_loadbuffer(L, chunk, chunkSize, chunkName);
}
sign的作用仅仅是magic number

解密LUA脚本


shroyale 〉 src 〉 decode_dhd 〉 main.go 〉
ject
main.go ×
decode_dhd\main.go ×
lashroyale (F:\wwwroot\work\cla
bin
pkg
src
decode_csv
decode_dhd
main.go
decode_sc
clashroyale.iml
net (F:\wwwroot\work\enet)
xternal Libraries
func main() {
filename := "E:\\迅雷下载\\大皇帝OL_游族_1.3.0_release\\assets\\src\\common\\c02d7364f85c80ca0d573d10526dac05_AppGlobalRegiste
key := "2dxLua"
sign := "XXTEA"
data,err := ioutil.ReadFile(filename)
if err != nil {
panic(err)
}
decrypt_data := xxtea.Decrypt(data[len(sign):], []byte(key))
fmt.Println(string(decrypt_data))
go run main.go (3)
HeroFormation=require("common.enum.HeroFormation")
BlendType=require("common/enum/BlendType")
GenderType=require("common.enum.GenderType")
ArmyAttackType=require("common.enum.ArmyAttackType")
ArmyHorse=require("common.enum.ArmyHorse")
ArmyIsWeapon=require("common.enum.ArmyIsWeapon")
ArmyAttackSubType=require("common.enum.ArmyAttackSubType")
ArmyArmorType=require("common.enum.ArmyArmorType")
BattleType=require("src.common.enum.BattleType")
TextInputMode=require("common.enum.TextInputMode")
SwitchType=require("common.enum.SwitchType")
LEGIONOPENFUNC=require("common/enum/LegionOpenFunc")
CityFunctionType=require("common.enum.CityFunctionType")
--全局VO
ItemVO=require("common.vo.ItemVO")
--全局工具类

大皇帝的美术资源

- 图片资源magic number为F9 43 5A
- 跳过了隐性指纹（规律）的查找
- 静态分析确认图片处理函数initWithImageData
- 直接动态调试，在initWithImageData函数上下断点
- 对于无法识别的函数，sub_XXXXX为其在so的偏移地址+so在内存中的基址，在对应的内存段上下断点即可

E:\迅雷下载\大皇帝OL_游族_1.3.0_release\assets\res\imgs\06ec2a07bcabd6502803936bddd8eb75_citymap3.ud - EditPlus

文件(W) 编辑(B) 显示(X) 搜索(S) 文档(D) 方案(F) 工具(G) 浏览器(L) Zen Coding 窗口(K) 帮助

目录 文本库 函数

[E:]

- E:\
- 迅雷下载
  - 大皇帝OL_游族_1.3.0_release
    - assets
      - res
        - imgs

033471ded48fe02228a6eedffd639d1b_liuliangBg.ud
06ec2a07bcabd6502803936bddd8eb75_citymap3.ud
07853ce5fdbccbe9b7530263fcd0a6f8_bg8.ud
171a0a8f4fce60678208569f0d7162c3_fight_bg_cn.ud
1b02bc6459824df90ee533676be8e004_bg11.ud
2b2ebc9af9848a324ac6741cfbc4a510_loginBg1.ud
2ce596ad0c6a137117ee05fe104dba72_troopdrill_bg_2.

```
00000000  F9 43 5A 21 00 00 00 02  00 00 00 00 00 0D 48 88  .CZ!..........H.
00000010  78 9C AC BD 4D 8F 5B 57  B2 2D 58 DD 6D 83 BC 42  x...M.[W.-X.m...
00000020  7B 6D D9 28 7A D2 E8 81  24 FA 49 1A 3C A0 27 35  {m.(z...$.I.<.'5
00000030  2C 03 D6 3D 74 49 85 86  D0 E8 41 0E 59 A8 34 3F  ,..=tI....A.Y.4?
00000040  4A 6E E0 9D 21 87 AC 97  69 8A 69 DF 81 73 98 B8  Jn..!...i.i..s..
00000050  67 24 9B F4 43 F9 FD 08  3F 51 49 5D 74 FD 85 1E  g$..C...?QI]t...
00000060  DC 6A 66 65 FA 07 F4 B0  4F C4 8A 15 11 FB 90 29  .jfe....O......)
00000070  BB 2E DA 07 56 66 F2 9B  E7 EC BD F6 8A 15 2B 62  ....Vf........+b
00000080  FF 2F BF FA D5 AF 3E F9  EF 7E F5 AB FF F1 BF FD  ./....>..~......
00000090  95 FE F7 3F 34 FF FF 6F  D5 3F FE EA BF 97 3F FE  ...?4..o.?....?.
000000a0  DF 5F FD EA FF EE FC EA  57 FF 13 EE FA D5 FF FA  ._......W.......
000000b0  BF BF FA 9F FF 9B E6 E7  7F FD CD 77 BF FE D3 AF  ........[..w....
000000c0  7F FF EF 71 CC 7E FD DD  AF 7F FC CD C7 9F 36 C7  [..q.~...[....6.
000000d0  E7 ED E3 5F 7F C3 23 EE  7D D8 1C F2 EF F3 57 0F  ..._[.#.}.....W.
000000e0  3F 7F 24 C7 AB 87 7A DB  F1 AB D3 A3 D3 A3 93 A3  ?[$...z.........
000000f0  E7 AF 9E BF 3A 6E 7E 1E  BF C2 2D 72 C8 6D 72 9C  ....:n~...-r.mr.
00000100  1E 5D 0E 36 83 DD 60 37  BE 6E 8E 77 CD EF 72 2C  .].6..`7.n.w..r,
00000110  E5 B6 71 77 82 63 37 5E  DA 2D BB E6 DF CB E6 95  ..qw.c7^.-......
00000120  CA E3 72 A0 FF EA CF E3  E6 95 8F 5F 3D 6A FE DF  ..r........_=j..
00000130  F8 6B 35 87 7E 8E CD A0  F3 7B 79 B5 E6 35 F4 F5  .k5.~....{y..5..
00000140  E4 B5 E4 73 E1 5E 79 46  F3 6E BF 97 DB 3F A9 FB  ...s.^yF.n...?..
00000150  CD F1 49 2D B7 6C 9A 57  95 D7 90 E7 EC EC 35 AF  ..I-.l.W......5.
00000160  9B 43 7E 6F 3E 73 F3 DA  F2 0A CD FD 47 97 F6 28  .C~o>s......G..(
00000170  39 4E 9B 67 5D 8F 3F A9  7B 75 6F D2 F1 EF 20 8F  9N.g].?.{uo... .
00000180  95 4F D8 9C AD E6 8C 7C  D1 FC 8E 33 B4 D4 43 CE  .O.....|...3..C.
00000190  CF B1 DD F6 6E 20 AF 2C  B7 9C 34 7F 1D E3 BE E6  ....n .,..4[....
000001a0  7B 3D 2F 8E 87 7A A6 F3  2D F2 EC E3 F4 F7 C9 11  {=/..z..-.......
000001b0  5F 45 DE 01 E7 6E C9 F3  D5 3A 8F CB A3 0D AE 45  _E...n...:.....E
000001c0  73 FF 67 AF E4 78 A4 EF  FA BC F9 F9 50 5F EB C4  s.g..x......P_..
000001d0  5E 0B 07 CE AE BC 9E FC  76 62 67 F2 54 EF C3 B7  ^.......vbg.T...
000001e0  C0 B7 91 67 E1 56 BE A7  9C AB 4B 3D 7F BC 3E 4B  ...g.V....K=[.>K
000001f0  7D 15 9C 21 7C C6 78 ED  A5 1D 27 B8 5A 83 65 BA  }..!|.x...'.Z.e.
00000200  65 D9 BC C6 3B 79 95 A3  A5 7D 07 DE 8E 31 63 8F  e...;y...}...1c.
00000210  6C 3E 6B 6F D2 AB E5 2A  F8 F8 C2 59 18 6C FC D8  l>ko...*...Y.l..
00000220  C9 F5 9F 6C F4 93 61 DC  61 14 7E A2 63 E1 93 7A  ...l..a.a.~.c..z
00000230  54 BF 99 76 27 D7 63 19  1B 3D 1D 99 CD D5 AD F5  T..v'.c..=......
00000240  E7 A4 EB 07 6F FB 87 E6  19 DD 5A 46 75 BE AF EF  ....o.....ZFu...
00000250  47 F3 79 26 55 73 5B BF  79 DD 71 BD 98 CA F1 7D  G.y&Us[.y.q....}
00000260  71 2C A6 6F A6 E3 E6 BE  37 CD 4F B9 57 7E D7 A3  q,.o....7.O.W~..
00000270  F9 ED 73 3D F4 95 26 9F  E8 21 9F AC 39 9F CD D9  ..s=..&..!..9...
00000280  78 67 F3 88 DF 5D CF F6  11 CF EC B1 5D D3 FD E3  xg...]......]...
00000290  A1 CD 64 3D 3E E5 F1 D1  A7 31 E7 E5 F8 B1 39 BE  ..d=>....1....9.
000002a0  6B FE CF 98 21 88 21 98  F1 D1 41 CC F8 F8 D3 36  k...!.!...A....6
000002b0  62 04 66 3C F2 F1 8B 91  8C F1 6E 9F D2 C7 E5 69  b.f<......n....i
```

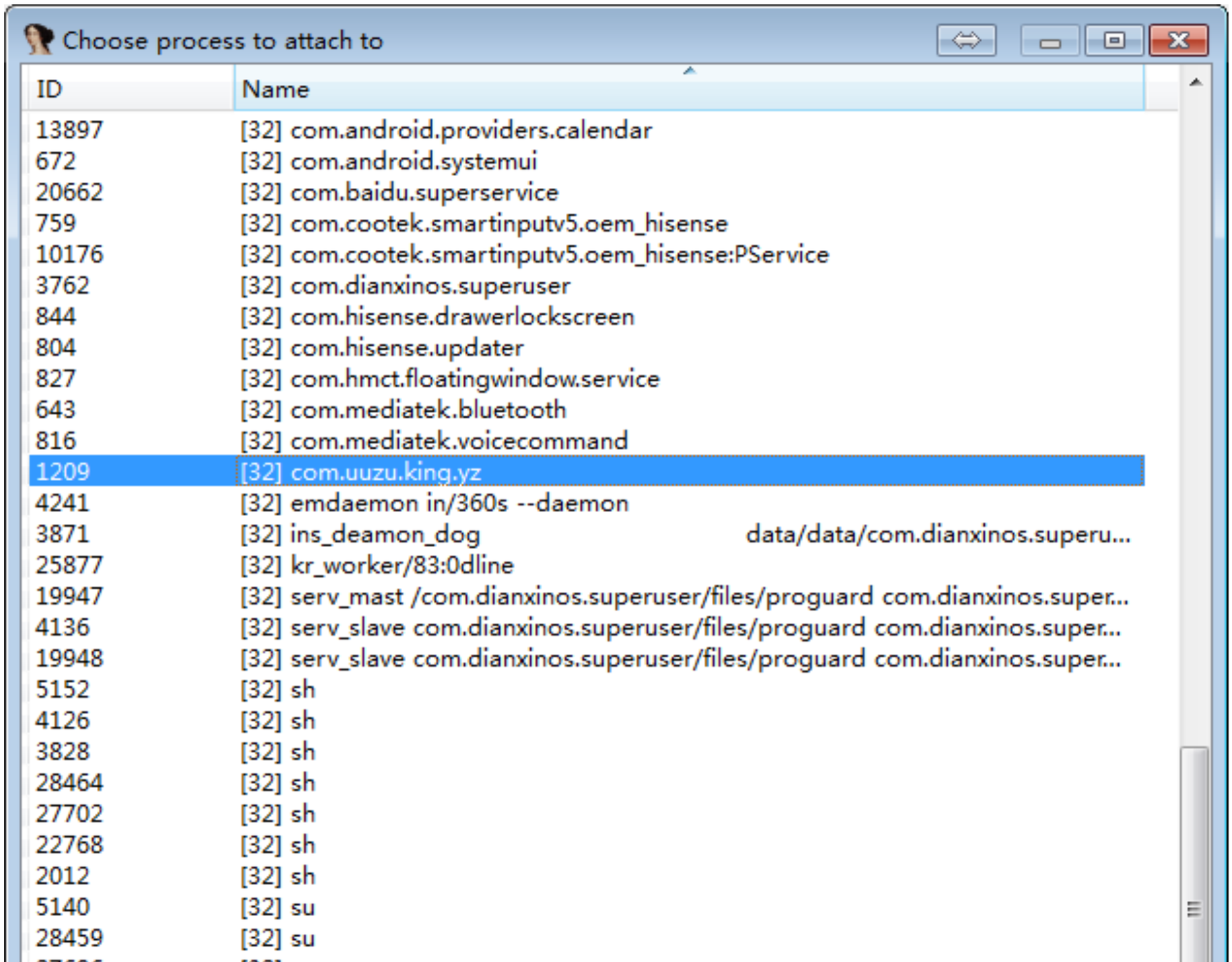
android动态调试环境

- IDA pro (>6.6版本支持android调试)
- 大皇帝、少三只支持ARM CPU架构，不能用模拟器
- IDA pro的android_server为ARM的程序，不能在X86上运行，不能用模拟器
- android调试同用户的进程，需要su权限（真机要越狱）

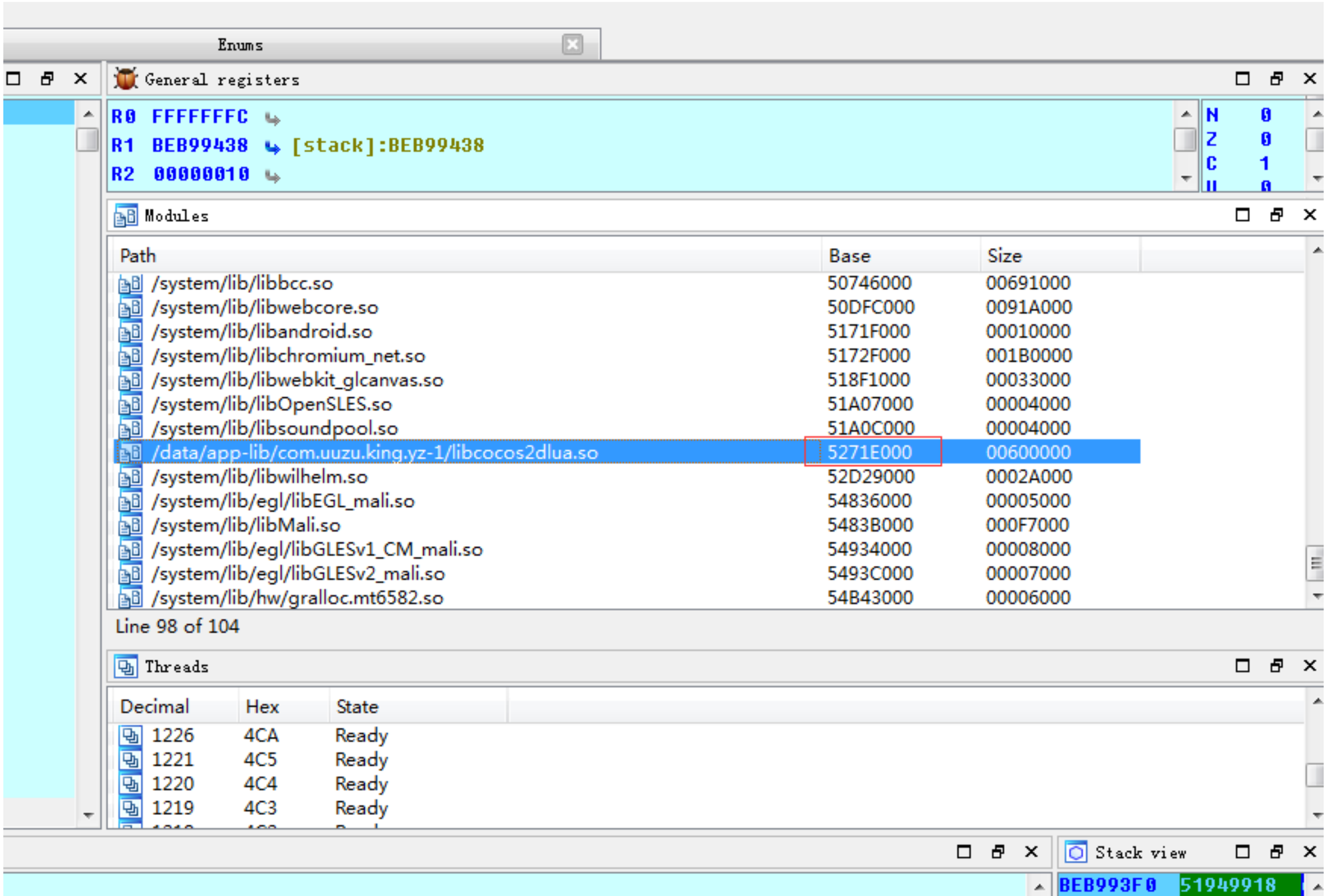
android动态调试步骤

- 调试设备上安装游戏（好像是废话）
- android_server推送至调试手机
- adb forward tcp:xxx 转发设备端口到本机
- adb shell ， su，执行android_server
- 在手机中运行游戏
- attach进程，进程名为包名

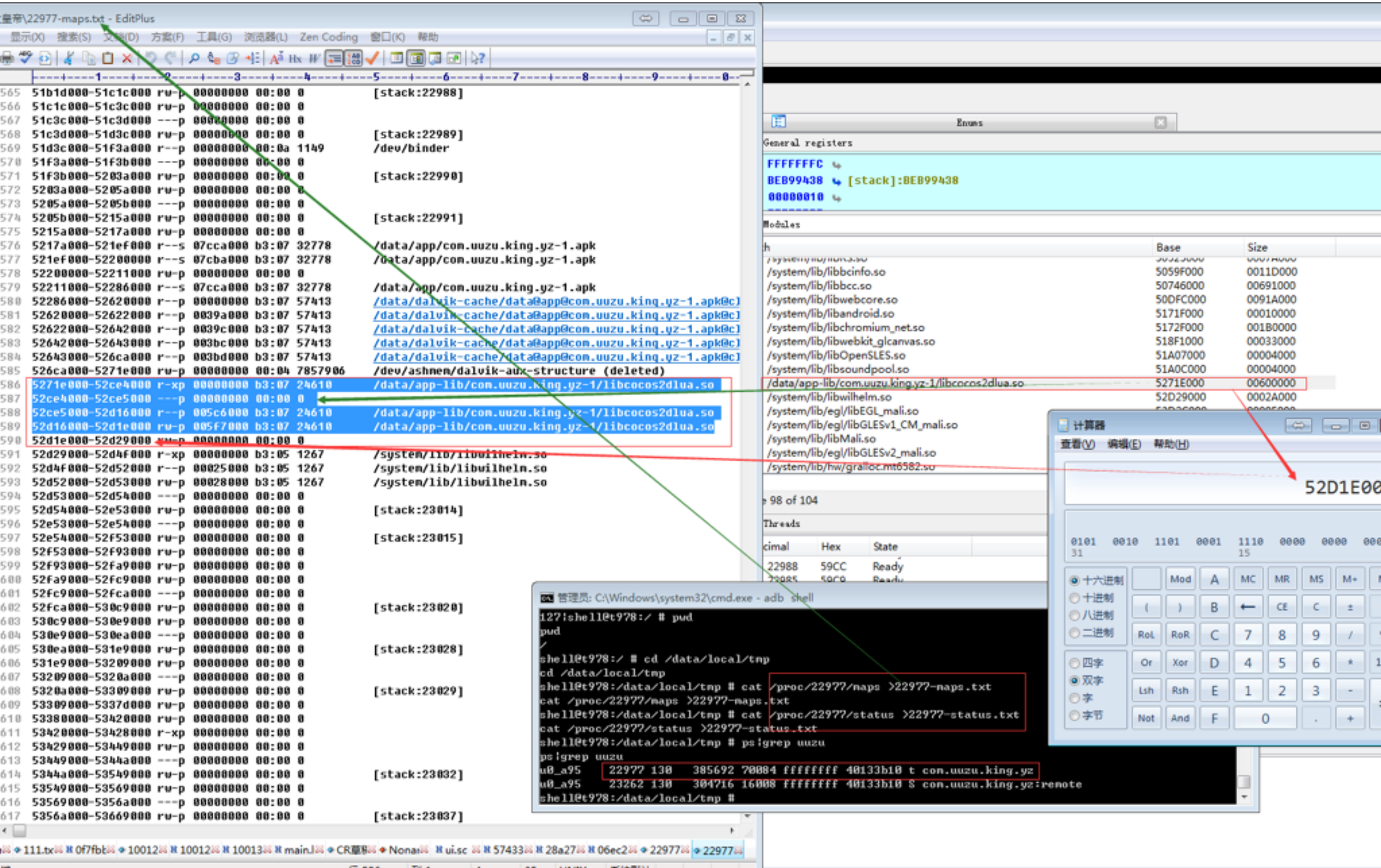
attach到android进程



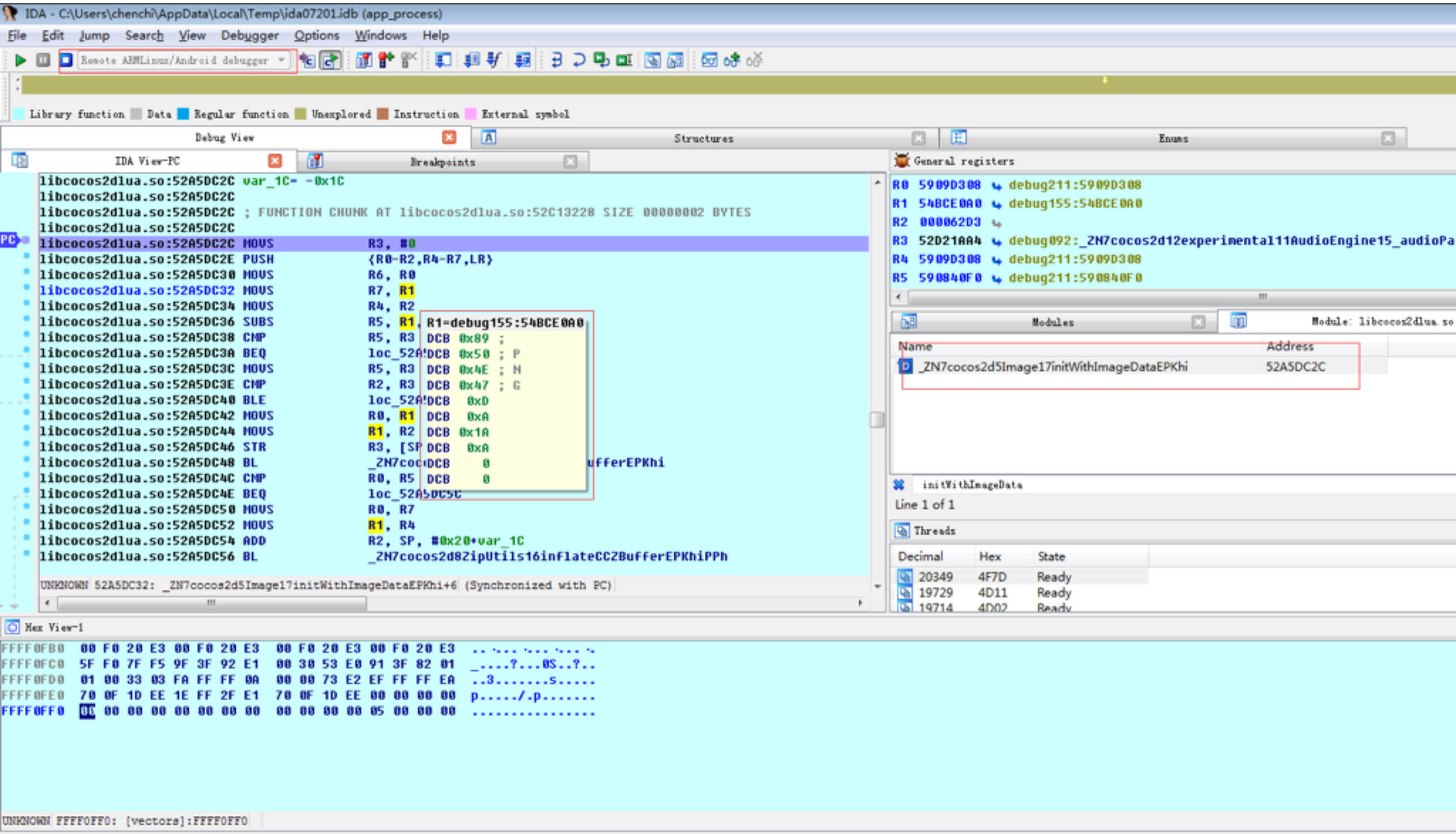
游戏运行时


Enums
General registers
R0 FFFFFFFC
R1 BEB99438 [stack]:BEB99438
R2 00000010
N 0
Z 0
C 1
Modules
Path
Base
Size
/system/lib/libbcc.so 50746000 00691000
/system/lib/libwebcore.so 50DFC000 0091A000
/system/lib/libandroid.so 5171F000 00010000
/system/lib/libchromium_net.so 5172F000 001B0000
/system/lib/libwebkit_glcanvas.so 518F1000 00033000
/system/lib/libOpenSLES.so 51A07000 00004000
/system/lib/libsoundpool.so 51A0C000 00004000
/data/app-lib/com.uuzu.king.yz-1/libcocos2dlua.so 5271E000 00600000
/system/lib/libwilhelm.so 52D29000 0002A000
/system/lib/egl/libEGL_mali.so 54836000 00005000
/system/lib/libMali.so 5483B000 000F7000
/system/lib/egl/libGLESv1_CM_mali.so 54934000 00008000
/system/lib/egl/libGLESv2_mali.so 5493C000 00007000
/system/lib/hw/gralloc.mt6582.so 54B43000 00006000
Line 98 of 104
Threads
Decimal
Hex
State
1226 4CA Ready
1221 4C5 Ready
1220 4C4 Ready
1219 4C3 Ready
Stack view
BEB993F0 51949918

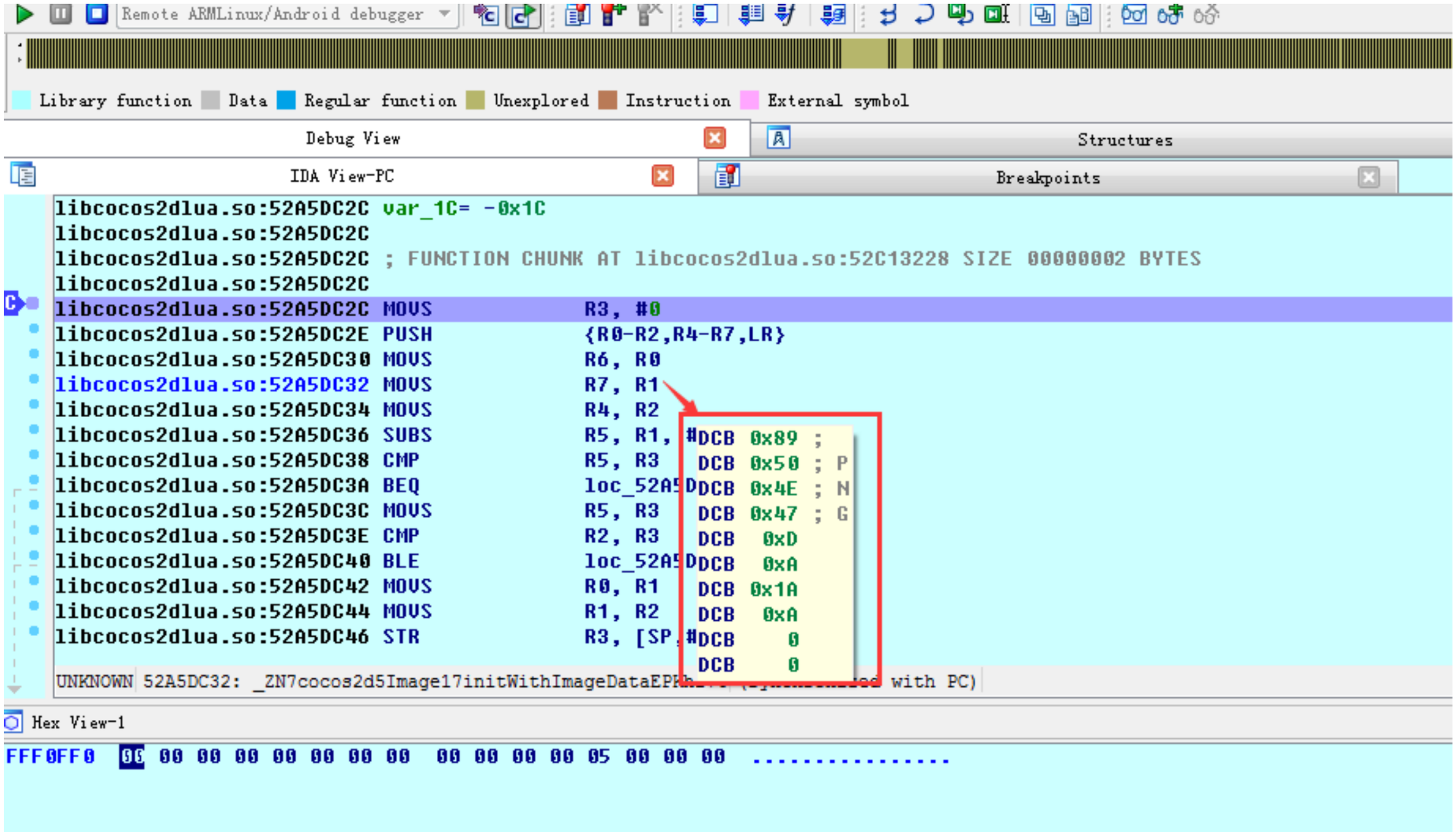
so文件内存段分布


量帝\22977-maps.txt - EditPlus
显示(X) 搜索(S) 文档(D) 方案(F) 工具(G) 浏览器(L) Zen Coding 窗口(K) 帮助
51b1d000-51c1c000 rw-p 00000000 00:00 0 [stack:22988]
51c1c000-51c3c000 rw-p 00000000 00:00 0
51c3c000-51c3d000 ---p 00000000 00:00 0
51c3d000-51d3c000 rw-p 00000000 00:00 0 [stack:22989]
51d3c000-51f3a000 r--p 00000000 00:0a 1149 /dev/binder
51f3a000-51f3b000 ---p 00000000 00:00 0
51f3b000-5203a000 rw-p 00000000 00:00 0 [stack:22990]
5203a000-5205a000 rw-p 00000000 00:00 0
5205a000-5205b000 ---p 00000000 00:00 0
5205b000-5215a000 rw-p 00000000 00:00 0 [stack:22991]
5215a000-5217a000 rw-p 00000000 00:00 0
5217a000-521ef000 r--s 07cca000 b3:07 32778 /data/app/com.uuzu.king.yz-1.apk
521ef000-52200000 r--s 07cba000 b3:07 32778 /data/app/com.uuzu.king.yz-1.apk
52200000-52211000 rw-p 00000000 00:00 0
52211000-52286000 r--s 07cca000 b3:07 32778 /data/app/com.uuzu.king.yz-1.apk
52286000-52620000 r--p 00000000 b3:07 57413 /data/dalvik-cache/data@app@com.uuzu.king.yz-1.apk@c
52620000-52622000 r--p 0039a000 b3:07 57413 /data/dalvik-cache/data@app@com.uuzu.king.yz-1.apk@c
52622000-52642000 r--p 0039c000 b3:07 57413 /data/dalvik-cache/data@app@com.uuzu.king.yz-1.apk@c
52642000-52643000 r--p 003bc000 b3:07 57413 /data/dalvik-cache/data@app@com.uuzu.king.yz-1.apk@c
52643000-526ca000 r--p 003bd000 b3:07 57413 /data/dalvik-cache/data@app@com.uuzu.king.yz-1.apk@c
526ca000-5271e000 rw-p 00000000 00:04 7857906 /dev/ashmem/dalvik-aux-structure (deleted)
5271e000-52ce4000 r-xp 00000000 b3:07 24610 /data/app-lib/com.uuzu.king.yz-1/libcocos2dlua.so
52ce4000-52ce5000 ---p 00000000 00:00 0
52ce5000-52d16000 r--p 005c6000 b3:07 24610 /data/app-lib/com.uuzu.king.yz-1/libcocos2dlua.so
52d16000-52d1e000 rw-p 005f7000 b3:07 24610 /data/app-lib/com.uuzu.king.yz-1/libcocos2dlua.so
52d1e000-52d29000 rw-p 00000000 00:00 0
52d29000-52d4f000 r-xp 00000000 b3:05 1267 /system/lib/libuilheln.so
52d4f000-52d52000 r--p 00025000 b3:05 1267 /system/lib/libuilheln.so
52d52000-52d53000 rw-p 00028000 b3:05 1267 /system/lib/libuilheln.so
52d53000-52d54000 ---p 00000000 00:00 0
52d54000-52e53000 rw-p 00000000 00:00 0 [stack:23014]
52e53000-52e54000 ---p 00000000 00:00 0
52e54000-52f53000 rw-p 00000000 00:00 0 [stack:23015]
52f53000-52f93000 rw-p 00000000 00:00 0
52f93000-52fa9000 rw-p 00000000 00:00 0
52fa9000-52fc9000 rw-p 00000000 00:00 0
52fc9000-52fca000 ---p 00000000 00:00 0
52fca000-530c9000 rw-p 00000000 00:00 0 [stack:23020]
530c9000-530e9000 rw-p 00000000 00:00 0
530e9000-530ea000 ---p 00000000 00:00 0
530ea000-531e9000 rw-p 00000000 00:00 0 [stack:23028]
531e9000-53209000 rw-p 00000000 00:00 0
53209000-5320a000 ---p 00000000 00:00 0
5320a000-53309000 rw-p 00000000 00:00 0 [stack:23029]
53309000-5337d000 rw-p 00000000 00:00 0
53380000-53420000 rw-p 00000000 00:00 0
53420000-53428000 r-xp 00000000 00:00 0
53429000-53449000 rw-p 00000000 00:00 0
53449000-5344a000 ---p 00000000 00:00 0
5344a000-53549000 rw-p 00000000 00:00 0 [stack:23032]
53549000-53569000 rw-p 00000000 00:00 0
53569000-5356a000 ---p 00000000 00:00 0
5356a000-53669000 rw-p 00000000 00:00 0 [stack:23037]
Enums
General registers
FFFFFFFC
BEB99438 [stack]:BEB99438
00000010
Modules
Base Size
/system/lib/libbcinfo.so 5059F000 0011D000
/system/lib/libbcc.so 50746000 00691000
/system/lib/libwebcore.so 50DFC000 0091A000
/system/lib/libandroid.so 5171F000 00010000
/system/lib/libchromium_net.so 5172F000 001B0000
/system/lib/libwebkit_glcanvas.so 518F1000 00033000
/system/lib/libOpenSLES.so 51A07000 00004000
/system/lib/libsoundpool.so 51A0C000 00004000
/data/app-lib/com.uuzu.king.yz-1/libcocos2dlua.so 5271E000 00600000
/system/lib/libwilhelm.so 52D29000 0002A000
/system/lib/egl/libEGL_mali.so
/system/lib/egl/libGLESv1_CM_mali.so
/system/lib/libMali.so
/system/lib/egl/libGLESv2_mali.so
/system/lib/hw/gralloc.mt6582.so
98 of 104
Threads
cimal Hex State
22988 59CC Ready
管理员: C:\Windows\system32\cmd.exe - adb shell
127|shell@t978:/ # pud
pud
/
shell@t978:/ # cd /data/local/tmp
cd /data/local/tmp
shell@t978:/data/local/tmp # cat /proc/22977/maps >22977-maps.txt
cat /proc/22977/maps >22977-maps.txt
shell@t978:/data/local/tmp # cat /proc/22977/status >22977-status.txt
cat /proc/22977/status >22977-status.txt
shell@t978:/data/local/tmp # ps|grep uuzu
ps|grep uuzu
u0_a95 22977 130 385692 70084 ffffffff 40133b10 t com.uuzu.king.yz
u0_a95 23262 130 304716 16008 ffffffff 40133b10 S com.uuzu.king.yz:remote
shell@t978:/data/local/tmp #
计算器
查看(V) 编辑(E) 帮助(H)
52D1E00
0101 0010 1101 0001 1110 0000 0000 000
31 15
十六进制 十进制 八进制 二进制
四字 双字 字 字节
Mod A MC MR MS M+
( ) B ← CE C ±
RoL RoR C 7 8 9 /
Or Xor D 4 5 6 *
Lsh Rsh E 1 2 3 -
Not And F 0 . +

在目标函数上下断点


IDA - C:\Users\chenchi\AppData\Local\Temp\ida07201.idb (app_process)
File Edit Jump Search View Debugger Options Windows Help
Remote ARMLinux/Android debugger
Library function Data Regular function Unexplored Instruction External symbol
Debug View
Structures
Enums
IDA View-PC
Breakpoints
General registers
libcocos2dlua.so:52A5DC2C var_1C= -0x1C
libcocos2dlua.so:52A5DC2C
libcocos2dlua.so:52A5DC2C ; FUNCTION CHUNK AT libcocos2dlua.so:52C13228 SIZE 00000002 BYTES
libcocos2dlua.so:52A5DC2C
libcocos2dlua.so:52A5DC2C MOVS R3, #0
libcocos2dlua.so:52A5DC2E PUSH {R0-R2,R4-R7,LR}
libcocos2dlua.so:52A5DC30 MOVS R6, R0
libcocos2dlua.so:52A5DC32 MOVS R7, R1
libcocos2dlua.so:52A5DC34 MOVS R4, R2
libcocos2dlua.so:52A5DC36 SUBS R5, R1,
libcocos2dlua.so:52A5DC38 CMP R5, R3
libcocos2dlua.so:52A5DC3A BEQ loc_52A
libcocos2dlua.so:52A5DC3C MOVS R5, R3
libcocos2dlua.so:52A5DC3E CMP R2, R3
libcocos2dlua.so:52A5DC40 BLE loc_52A
libcocos2dlua.so:52A5DC42 MOVS R0, R1
libcocos2dlua.so:52A5DC44 MOVS R1, R2
libcocos2dlua.so:52A5DC46 STR R3, [SP
libcocos2dlua.so:52A5DC48 BL _ZN7coc
libcocos2dlua.so:52A5DC4C CMP R0, R5
libcocos2dlua.so:52A5DC4E BEQ loc_52A5DC5C
libcocos2dlua.so:52A5DC50 MOVS R0, R7
libcocos2dlua.so:52A5DC52 MOVS R1, R4
libcocos2dlua.so:52A5DC54 ADD R2, SP, #0x20+var_1C
libcocos2dlua.so:52A5DC56 BL _ZN7cocos2d8ZipUtils16inflateCC2BufferEPKhiPPh
R1=debug155:54BCE0A0
DCB 0x89 ;
DCB 0x50 ; P
DCB 0x4E ; N
DCB 0x47 ; G
DCB 0xD
DCB 0xA
DCB 0x1A
DCB 0xA
DCB 0
DCB 0
ufferEPKhi
UNKNOWN 52A5DC32: _ZN7cocos2d5Image17initWithImageDataEPKhi+6 (Synchronized with PC)
R0 5909D308 debug211:5909D308
R1 54BCE0A0 debug155:54BCE0A0
R2 000062D3
R3 52D21AA4 debug092:_ZN7cocos2d12experimental11AudioEngine15_audioPa
R4 5909D308 debug211:5909D308
R5 590840F0 debug211:590840F0
Modules
Module: libcocos2dlua.so
Name
Address
_ZN7cocos2d5Image17initWithImageDataEPKhi
52A5DC2C
initWithImageData
Line 1 of 1
Threads
Decimal
Hex
State
20349 4F7D Ready
19729 4D11 Ready
19714 4D02 Ready
Hex View-1
FFFF0FB0 00 F0 20 E3 00 F0 20 E3 00 F0 20 E3 00 F0 20 E3
FFFF0FC0 5F F0 7F F5 9F 3F 92 E1 00 30 53 E0 91 3F 82 01
FFFF0FD0 01 00 33 03 FA FF FF 0A 00 00 73 E2 EF FF FF EA
FFFF0FE0 70 0F 1D EE 1E FF 2F E1 70 0F 1D EE 00 00 00 00
FFFF0FF0 05 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00
UNKNOWN FFFF0FF0: [vectors]:FFFF0FF0

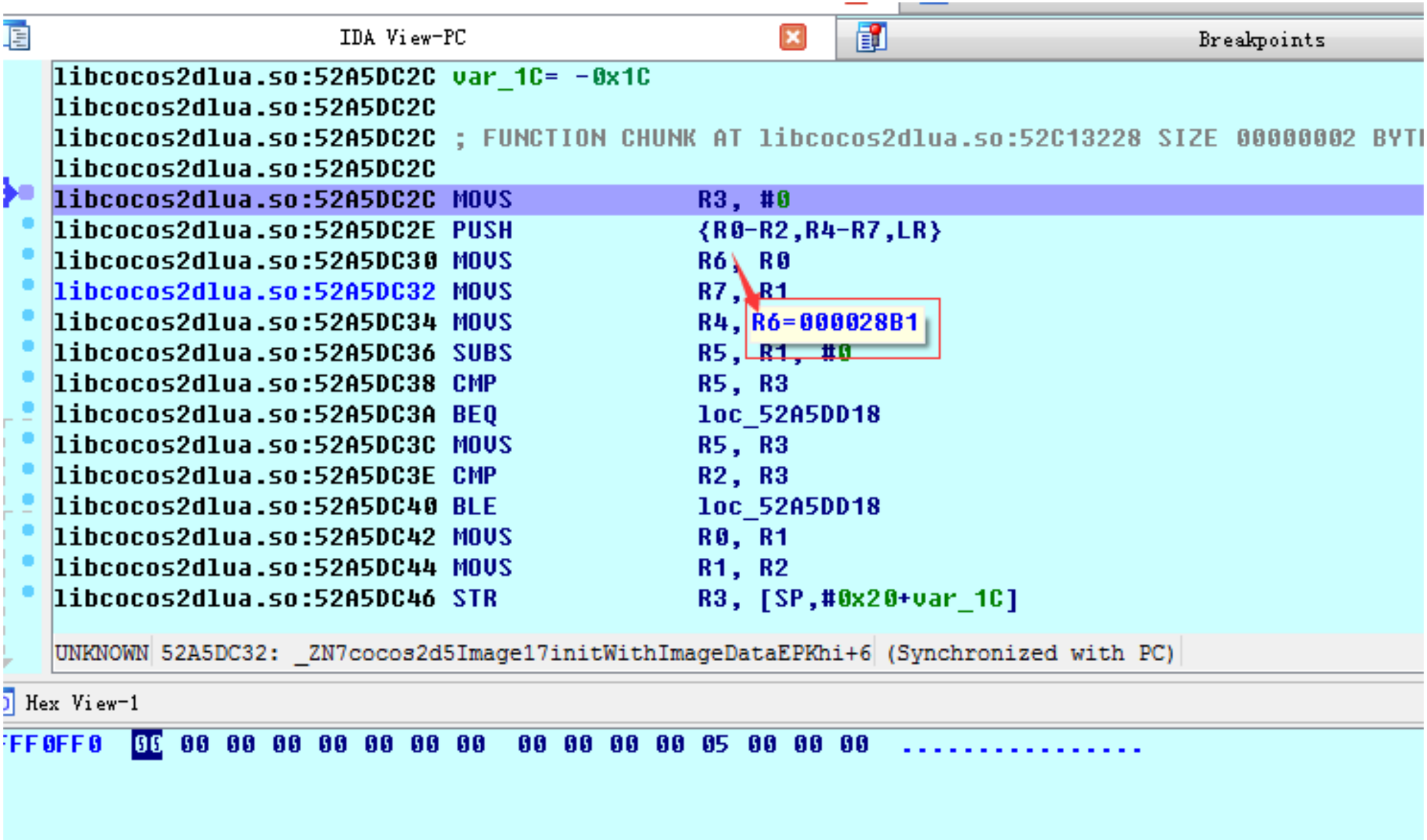
让程序运行到断点处


Remote ARMLinux/Android debugger
Library function
Data
Regular function
Unexplored
Instruction
External symbol
Debug View
Structures
IDA View-PC
Breakpoints
libcocos2dlua.so:52A5DC2C var_1C= -0x1C
libcocos2dlua.so:52A5DC2C
libcocos2dlua.so:52A5DC2C ; FUNCTION CHUNK AT libcocos2dlua.so:52C13228 SIZE 00000002 BYTES
libcocos2dlua.so:52A5DC2C
libcocos2dlua.so:52A5DC2C MOVS R3, #0
libcocos2dlua.so:52A5DC2E PUSH {R0-R2,R4-R7,LR}
libcocos2dlua.so:52A5DC30 MOVS R6, R0
libcocos2dlua.so:52A5DC32 MOVS R7, R1
libcocos2dlua.so:52A5DC34 MOVS R4, R2
libcocos2dlua.so:52A5DC36 SUBS R5, R1, #
libcocos2dlua.so:52A5DC38 CMP R5, R3
libcocos2dlua.so:52A5DC3A BEQ loc_52A5D
libcocos2dlua.so:52A5DC3C MOVS R5, R3
libcocos2dlua.so:52A5DC3E CMP R2, R3
libcocos2dlua.so:52A5DC40 BLE loc_52A5D
libcocos2dlua.so:52A5DC42 MOVS R0, R1
libcocos2dlua.so:52A5DC44 MOVS R1, R2
libcocos2dlua.so:52A5DC46 STR R3, [SP,#
DCB 0x89 ;
DCB 0x50 ; P
DCB 0x4E ; N
DCB 0x47 ; G
DCB 0xD
DCB 0xA
DCB 0x1A
DCB 0xA
DCB 0
DCB 0
UNKNOWN 52A5DC32: _ZN7cocos2d5Image17initWithImageDataEPh
with PC)
Hex View-1
FFF0FFF0 89 50 4E 47 0D 0A 1A 0A 00 00 00 00 05 00 00 00 .PNG............

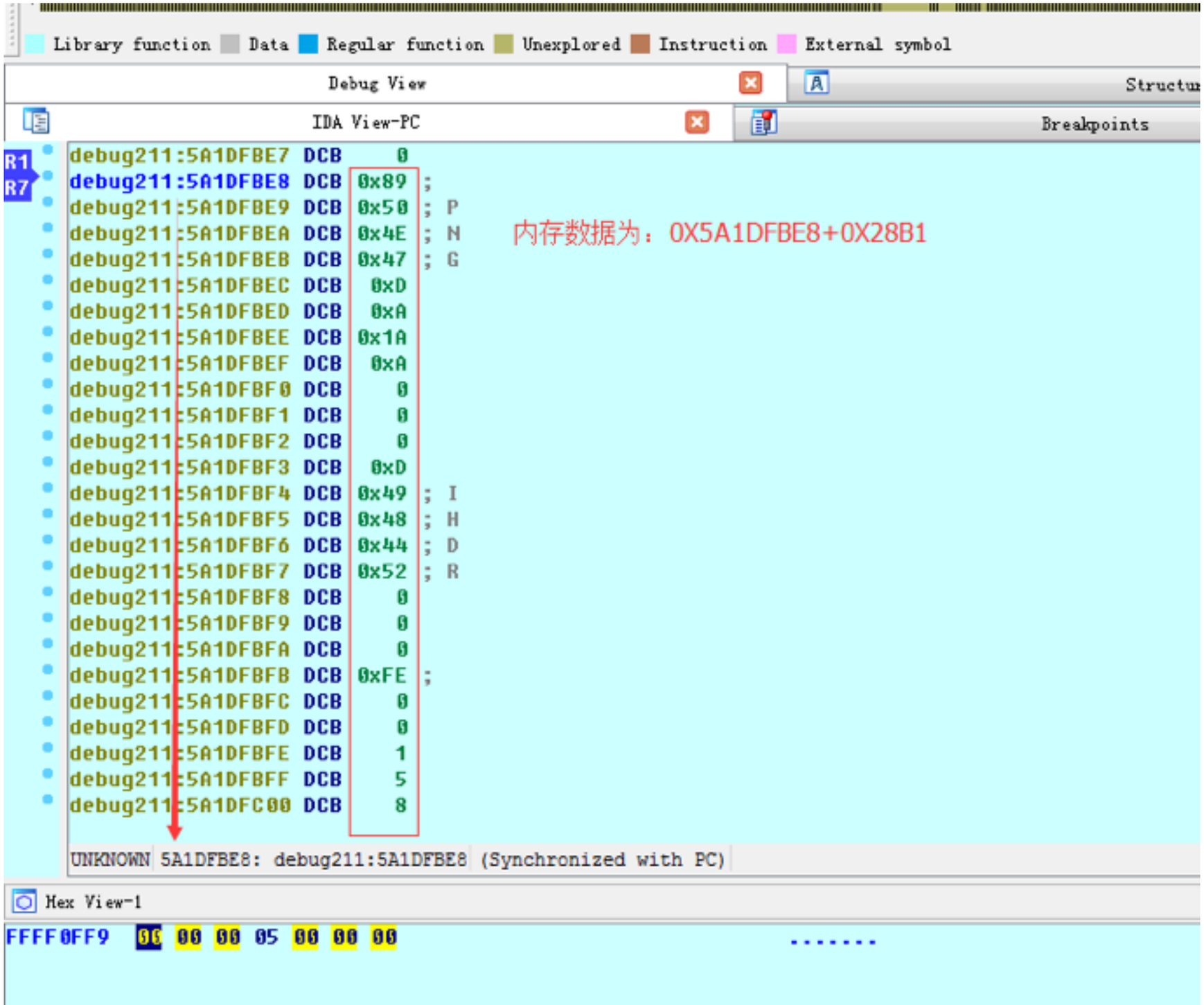
内存DUMP

- 还记得当年大明湖畔的magic number吗?
- png的magic number是什么来着?
- 上图中R1寄存器的前8个字节 89 50 4E 47
- 找到了png图片在内存中的开始地址
- 那结束地址（长度）呢

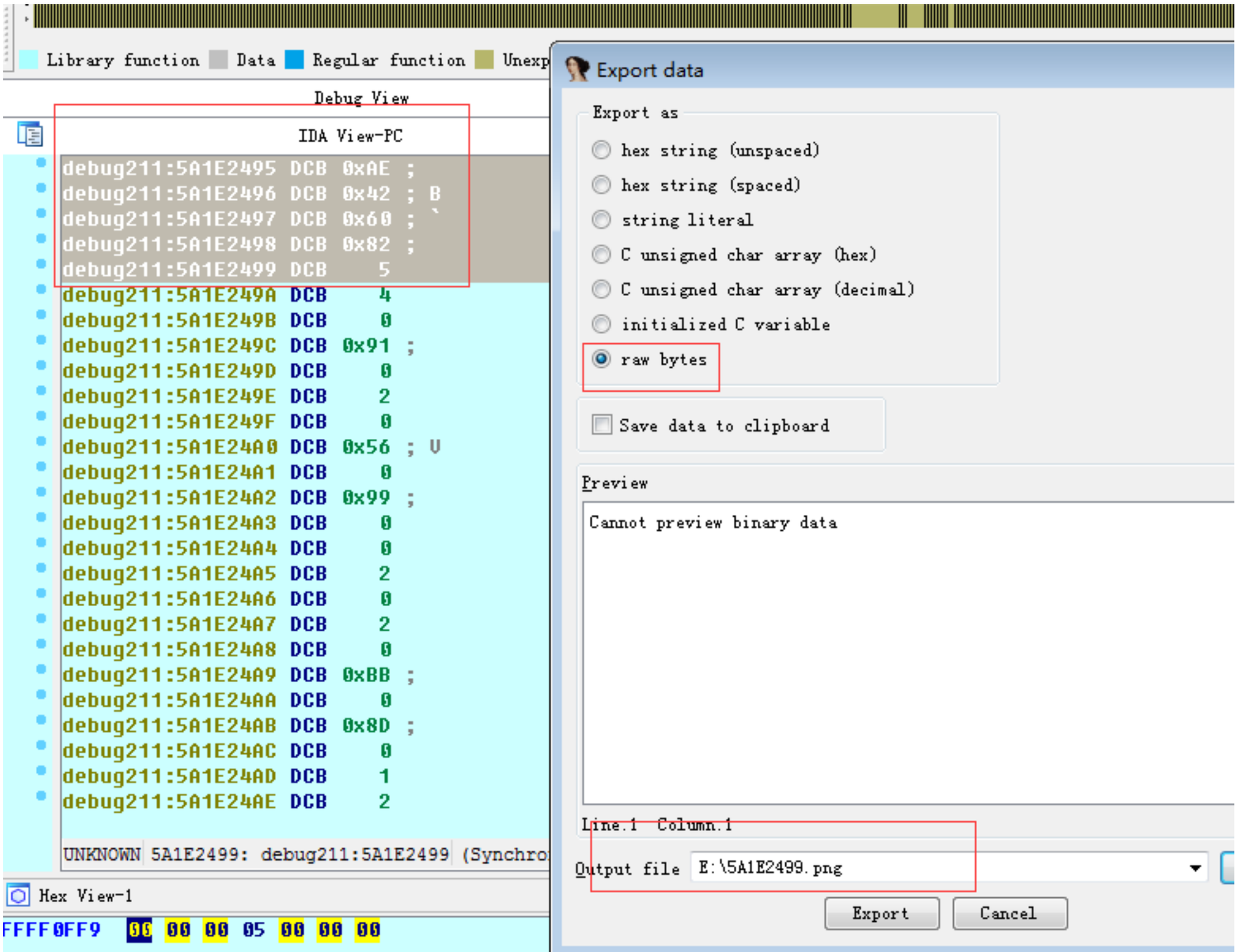
PNG数据长度


IDA View-PC
Breakpoints
libcocos2dlua.so:52A5DC2C var_1C= -0x1C
libcocos2dlua.so:52A5DC2C
libcocos2dlua.so:52A5DC2C ; FUNCTION CHUNK AT libcocos2dlua.so:52C13228 SIZE 00000002 BYTE
libcocos2dlua.so:52A5DC2C
libcocos2dlua.so:52A5DC2C MOVS R3, #0
libcocos2dlua.so:52A5DC2E PUSH {R0-R2,R4-R7,LR}
libcocos2dlua.so:52A5DC30 MOVS R6, R0
libcocos2dlua.so:52A5DC32 MOVS R7, R1
libcocos2dlua.so:52A5DC34 MOVS R4, R6=00028B1
libcocos2dlua.so:52A5DC36 SUBS R5, R1, #0
libcocos2dlua.so:52A5DC38 CMP R5, R3
libcocos2dlua.so:52A5DC3A BEQ loc_52A5DD18
libcocos2dlua.so:52A5DC3C MOVS R5, R3
libcocos2dlua.so:52A5DC3E CMP R2, R3
libcocos2dlua.so:52A5DC40 BLE loc_52A5DD18
libcocos2dlua.so:52A5DC42 MOVS R0, R1
libcocos2dlua.so:52A5DC44 MOVS R1, R2
libcocos2dlua.so:52A5DC46 STR R3, [SP,#0x20+var_1C]
UNKNOWN 52A5DC32: _ZN7cocos2d5Image17initWithImageDataEPKhi+6 (Synchronized with PC)
Hex View-1
FF0FF0 96 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 ....

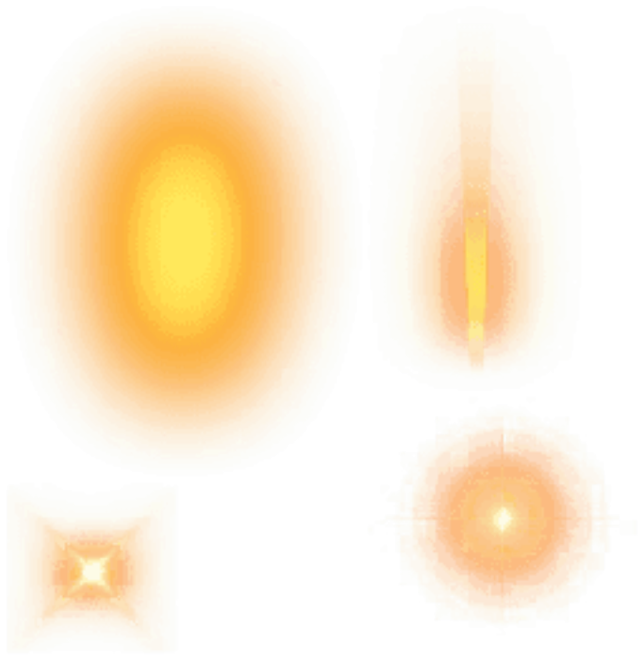
PNG在内存中范围


Library function
Data
Regular function
Unexplored
Instruction
External symbol
Debug View
Structu
IDA View-PC
Breakpoints
R1
R7
debug211:5A1DFBE7 DCB 0
debug211:5A1DFBE8 DCB 0x89 ;
debug211:5A1DFBE9 DCB 0x50 ; P
debug211:5A1DFBEA DCB 0x4E ; N
debug211:5A1DFBEB DCB 0x47 ; G
debug211:5A1DFBEC DCB 0xD
debug211:5A1DFBED DCB 0xA
debug211:5A1DFBEE DCB 0x1A
debug211:5A1DFBEF DCB 0xA
debug211:5A1DFBF0 DCB 0
debug211:5A1DFBF1 DCB 0
debug211:5A1DFBF2 DCB 0
debug211:5A1DFBF3 DCB 0xD
debug211:5A1DFBF4 DCB 0x49 ; I
debug211:5A1DFBF5 DCB 0x48 ; H
debug211:5A1DFBF6 DCB 0x44 ; D
debug211:5A1DFBF7 DCB 0x52 ; R
debug211:5A1DFBF8 DCB 0
debug211:5A1DFBF9 DCB 0
debug211:5A1DFBFA DCB 0
debug211:5A1DFBFB DCB 0xFE ;
debug211:5A1DFBFC DCB 0
debug211:5A1DFBFD DCB 0
debug211:5A1DFBFE DCB 1
debug211:5A1DFBFF DCB 5
debug211:5A1DFC00 DCB 8
内存数据为：0X5A1DFBE8+0X28B1
UNKNOWN 5A1DFBE8: debug211:5A1DFBE8 (Synchronized with PC)
Hex View-1
FFFF0FF9 00 00 00 05 00 00 00 ....

内存dump


Library function
Data
Regular function
Debug View
IDA View-PC
debug211:5A1E2495 DCB 0xAE ;
debug211:5A1E2496 DCB 0x42 ; B
debug211:5A1E2497 DCB 0x60 ; `
debug211:5A1E2498 DCB 0x82 ;
debug211:5A1E2499 DCB 5
debug211:5A1E249A DCB 4
debug211:5A1E249B DCB 0
debug211:5A1E249C DCB 0x91 ;
debug211:5A1E249D DCB 0
debug211:5A1E249E DCB 2
debug211:5A1E249F DCB 0
debug211:5A1E24A0 DCB 0x56 ; V
debug211:5A1E24A1 DCB 0
debug211:5A1E24A2 DCB 0x99 ;
debug211:5A1E24A3 DCB 0
debug211:5A1E24A4 DCB 0
debug211:5A1E24A5 DCB 2
debug211:5A1E24A6 DCB 0
debug211:5A1E24A7 DCB 2
debug211:5A1E24A8 DCB 0
debug211:5A1E24A9 DCB 0xBB ;
debug211:5A1E24AA DCB 0
debug211:5A1E24AB DCB 0x8D ;
debug211:5A1E24AC DCB 0
debug211:5A1E24AD DCB 1
debug211:5A1E24AE DCB 2
UNKNOWN 5A1E2499: debug211:5A1E2499 (Synchro
Hex View-1
FFFF0FF9 00 00 00 05 00 00 00
Export data
Export as
hex string (unspaced)
hex string (spaced)
string literal
C unsigned char array (hex)
C unsigned char array (decimal)
initialized C variable
raw bytes
Save data to clipboard
Preview
Cannot preview binary data
Line.1 Column.1
Output file
E:\5A1E2499.png
Export
Cancel

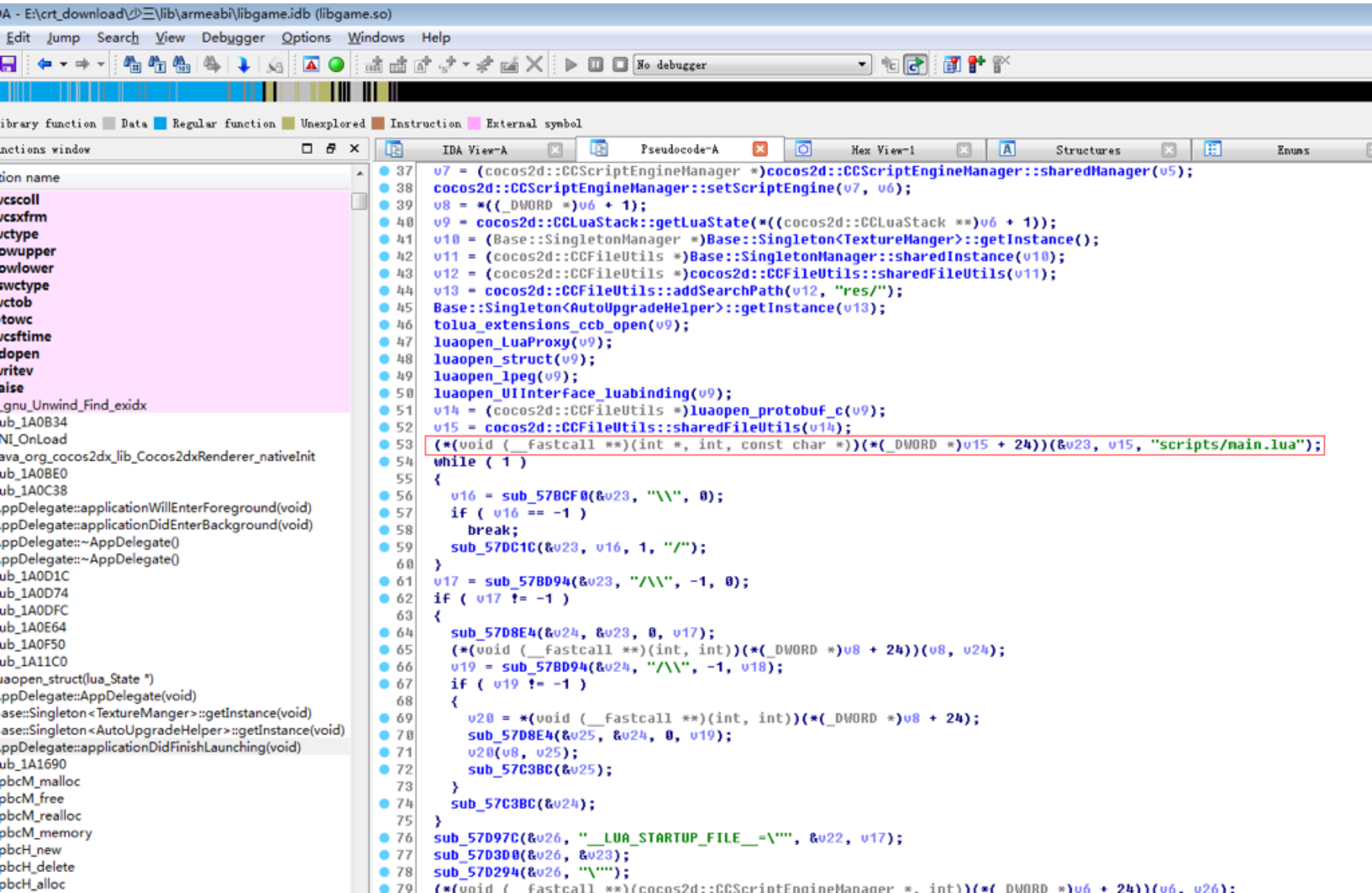
导出的图片



图片加密算法

- 我没时间继续跟下去
- 在stack栈列表里，往上追溯，找到调用该函数的地方，找到解密函数，找到解密算法
- 工头叫我去搬砖了...

少三的lua加密


A - E:\crt_download\少三\lib\armeabi\libgame.idb (libgame.so)
Edit Jump Search View Debugger Options Windows Help
No debugger
ibrary function Data Regular function Unexplored Instruction External symbol
nctions window
tion name
vcscoll
vcsxfrm
vctype
owupper
owlower
swctype
vctob
towc
vcsftime
dopen
vritev
aise
_gnu_Unwind_Find_exidx
ub_1A0B34
NI_OnLoad
ava_org_cocos2dx_lib_Cocos2dxRenderer_nativeInit
ub_1A0BE0
ub_1A0C38
ppDelegate::applicationWillEnterForeground(void)
ppDelegate::applicationDidEnterBackground(void)
ppDelegate::~AppDelegate()
ppDelegate::~AppDelegate()
ub_1A0D1C
ub_1A0D74
ub_1A0DFC
ub_1A0E64
ub_1A0F50
ub_1A11C0
uaopen_struct(lua_State *)
ppDelegate::AppDelegate(void)
ase::Singleton<TextureManger>::getInstance(void)
ase::Singleton<AutoUpgradeHelper>::getInstance(void)
ppDelegate::applicationDidFinishLaunching(void)
ub_1A1690
pbcM_malloc
pbcM_free
pbcM_realloc
pbcM_memory
pbcH_new
pbcH_delete
pbcH_alloc
IDA View-A
Pseudocode-A
Hex View-1
Structures
Enums
37 v7 = (cocos2d::CCScriptEngineManager *)cocos2d::CCScriptEngineManager::sharedManager(v5);
38 cocos2d::CCScriptEngineManager::setScriptEngine(v7, v6);
39 v8 = *((_DWORD *)v6 + 1);
40 v9 = cocos2d::CCLuaStack::getLuaState(*((cocos2d::CCLuaStack **)v6 + 1));
41 v10 = (Base::SingletonManager *)Base::Singleton<TextureManger>::getInstance();
42 v11 = (cocos2d::CCFileUtils *)Base::SingletonManager::sharedInstance(v10);
43 v12 = (cocos2d::CCFileUtils *)cocos2d::CCFileUtils::sharedFileUtils(v11);
44 v13 = cocos2d::CCFileUtils::addSearchPath(v12, "res/");
45 Base::Singleton<AutoUpgradeHelper>::getInstance(v13);
46 tolua_extensions_ccb_open(v9);
47 luaopen_LuaProxy(v9);
48 luaopen_struct(v9);
49 luaopen_lpeg(v9);
50 luaopen_UIInterface_luabinding(v9);
51 v14 = (cocos2d::CCFileUtils *)luaopen_protobuf_c(v9);
52 v15 = cocos2d::CCFileUtils::sharedFileUtils(v14);
53 (*(void (__fastcall **)(int *, int, const char *))(*(_DWORD *)v15 + 24))(&v23, v15, "scripts/main.lua");
54 while (1)
55 {
56 v16 = sub_57BCF0(&v23, "\\", 0);
57 if (v16 == -1)
58 break;
59 sub_57DC1C(&v23, v16, 1, "/");
60 }
61 v17 = sub_57BD94(&v23, "/\\", -1, 0);
62 if (v17 != -1)
63 {
64 sub_57D8E4(&v24, &v23, 0, v17);
65 (*(void (__fastcall **)(int, int))(*(_DWORD *)v8 + 24))(v8, v24);
66 v19 = sub_57BD94(&v24, "/\\", -1, v18);
67 if (v19 != -1)
68 {
69 v20 = *(void (__fastcall **)(int, int))(*(_DWORD *)v8 + 24);
70 sub_57D8E4(&v25, &v24, 0, v19);
71 v20(v8, v25);
72 sub_57C3BC(&v25);
73 }
74 sub_57C3BC(&v24);
75 }
76 sub_57D97C(&v26, "__LUA_STARTUP_FILE__=\"", &v22, v17);
77 sub_57D3D0(&v26, &v23);
78 sub_57D294(&v26, "\"");
79 (*(void (__fastcall **)(cocos2d::CCScriptEngineManager *, int))(*(_DWORD *)v6 + 24))(v6, v26);

少三lua加密的静态分析

- 没有明文存储密钥
- 大约分为N种magic number
- 提高了解密的成本

少三lua的动态分析

- 经过一番动态调试，发现并不是单一的密钥解密
- 每种文件头的解密KEY并不一样
- 也确定是XXTEA加密
- 对抗难度提高，但威胁也还在，也可以提高

E:\crt_download\少三\59B21008-59B69432.Dump - EditPlus

文件(W) 编辑(B) 显示(X) 搜索(S) 文档(D) 方案(F) 工具(G) 浏览器(L) Zen Coding 窗口(K) 帮助

文本库 函数

E:\
crt_download
少三
assets
lib
META-INF
res

21008-59B69432.Dump
10328_2106_2.4.20.zip
droidManifest.xml
ses.dex
ort_results.txt
ources.arsc

```
1  //cleint <--> scene
2  package cs;
3
4  message User {
5    required uint32 id = 1;
6    required string name = 2;
7    required uint32 level = 3;
8    required uint32 vit = 4; //体力
9    required uint32 spirit = 5; //精力
10   required uint32 refresh_vit_time
11   required uint32 refresh_spirit_ti
12   required uint32 exp = 8;
13   required uint32 money = 9;
14   required uint32 gold = 10;
15   required uint32 prestige = 11; //
16   optional uint32 skill_point = 12;
17   required uint32 medal = 13; //奖章
18   required uint32 tower_score = 14;
19   required uint32 fight_value = 15;
20   required uint32 battle_token = 16
21   required uint32 battle_token_time
22   optional uint32 essence = 18; //精
23   required uint32 forbid_battle_tim
24   optional uint32 guide_id = 20;
25   optional uint32 corp_point = 21;//
26   optional uint32 wheel_score = 22;
27   optional uint32 god_soul = 23; //
28   optional uint32 contest_point = 2
29   optional uint32 title_id = 25; //
30   repeated TitleInfo title_list = 2
31   optional uint32 spread_sum_score
32   optional uint32 coupon = 28; //团
33   optional uint32 fid = 29; // 头像
34   optional uint32 fight_score = 30;
35   optional uint32 cloth_id = 31;
36   optional uint32 cloth_time = 32;
37   optional bool   cloth_open = 33;
38   optional uint32 ksoul_point = 34;
39   optional uint32 cnt = 35;//改名次
40   optional uint32 ksoul_summon_scor
41   optional uint32 ksoul_fight_base
42   optional uint32 wid  = 38;//装备的
43   optional uint32 trade_point = 39;
44 }
45
46 message Knight {
47   required uint32 id = 1;
48   required uint32 base_id = 2;
49   required uint32 level = 3;
50   required uint32 exp = 4;
51   required uint32 time = 5;
52   required uint32 user_id = 6;
53   required KnightTraining training
54   required uint32 halo_level = 8;//
55   required uint32 halo_exp = 9;//光
```

文件 (*.*)

分析草稿 Noname1 111.txt 0f7fbba7e6ecb9 10012_fight.json 100

帮助，请按键盘 F1 键

IDA - C:\Users\chenchi\AppData\Local\Temp\ida56527.idb (app_process)

File Edit Jump Search View Debugger Options Windows Help

Remote ARMLinux/Android debugger

Library function Data Regular function Unexplored Instruction External symbol

Debug View | Structures

IDA View-PC | Pseudocode-C | Pseudocode-B | Pseudocode-A | Breakpoints

```
R0 debug170:59B21008 DCB 0x2F ; /
   debug170:59B21009 DCB 0x2F ; /
   debug170:59B2100A DCB 0x63 ; c
   debug170:59B2100B DCB 0x6C ; l
   debug170:59B2100C DCB 0x65 ; e
   debug170:59B2100D DCB 0x69 ; i
   debug170:59B2100E DCB 0x6E ; n
   debug170:59B2100F DCB 0x74 ; t
   debug170:59B21010 DCB 0x20
   debug170:59B21011 DCB 0x3C ; <
   debug170:59B21012 DCB 0x2D ; -
   debug170:59B21013 DCB 0x2D ; -
   debug170:59B21014 DCB 0x2D ; -
   debug170:59B21015 DCB 0x3E ; >
   debug170:59B21016 DCB 0x20
   debug170:59B21017 DCB 0x73 ; s
   debug170:59B21018 DCB 0x63 ; c
   debug170:59B21019 DCB 0x65 ; e
   debug170:59B2101A DCB 0x6E ; n
   debug170:59B2101B DCB 0x65 ; e
   debug170:59B2101C DCB  0xA
   debug170:59B2101D DCB 0x70 ; p
   debug170:59B2101E DCB 0x61 ; a
   debug170:59B2101F DCB 0x63 ; c
   debug170:59B21020 DCB 0x6B ; k
```

UNKNOWN 59B2100B: debug170:59B2100B (Synchronized with R1)

Hex View-1

```
BEB99FC0  41 43 45 3D 38 2C 34 39  36 36 34 00 41 4E 44 52  ACE=8,49664.ANDR
BEB99FD0  4F 49 44 5F 53 4F 43 4B  45 54 5F 7A 79 67 6F 74  OID_SOCKET_zygot
BEB99FE0  65 3D 39 00 2F 73 79 73  74 65 6D 2F 62 69 6E 2F  e=9./system/bin/
BEB99FF0  61 70 70 5F 70 72 6F 63  65 73 73 00 00 00 00 00  app_process.....
FFFF0000  00 00 9F EF DD 00 00 EA  10 F4 9F E5 BB 00 00 EA  ................
FFFF0010  9A 00 00 EA FA 00 00 EA  78 00 00 EA 00 C0 4F E1  ........x.....O.
FFFF0020  04 B0 4E E2 01 A0 5A E2  28 00 00 1A 00 58 2D E9  ..N...Z.(....X-.
FFFF0030  1C D0 4D E2 00 7F CD E8  00 F0 20 E3 FF 00 2D E9  ..M..... ...-.
```

UNKNOWN BEB99FD0: [stack]:BEB99FD0

Stack

```
52FAEA
52FAEA
52FAEA
52FAEA
52FAEA
52FAEA
52FAEA
```

UNKNOWN

Output window

```
Caching 'Modules'... ok
Caching 'Modules'... ok
Stored export results in E:\crt_download\少三\export_results.txt
--------------开始Dump数据--------------
StartAddres:0x59B21008  EndAddres:0x59B69432
SavePath:E:\crt_download\少三\59B21008-59B69432.Dump
--------------Dump数据成功--------------
```

IDC

AU: idle Down

在xxtea_decrypt函数部分，下断点，内存DUMP了，解密后的源码

lua被解密的危害

- 逻辑代码被泄露
- 改写逻辑代码，重新打包，实现内置外挂
- 改写控制的结果，比如客户端操作评分，枪枪爆头，刀刀刺杀
- lua里有通讯协议编码格式，协议外挂更容易被制作
- 影响游戏平衡，减少游戏生命周期，甚至拖死游戏

客户端密钥保护

- 代码中字符串编译后的存储
- 静态分析不可见
- 运行时计算出字符串
- 还原字符串时，利用文件名，长度等隐形特征，做相关运算。

客户端密钥保护

JEB -

File Edit Action Window Help

Manifest | Resources | Assets | Assembly | Decompiled Java | Strings | Constants | Notes

```
    private int foo() {  // has try-catch handlers
        AssetManager assman = this.getAssets();
        String v0 = MainActivity.decryptString(-31, -27, 0x34);  // 1.png
        Object[] v2 = new Object[1];
        v2[0] = v0;
        Class v0_1 = Class.forName(MainActivity.decryptString(0x11, 0, 0x15));  // android.content.res.AssetManager
        String v3 = MainActivity.decryptString(0x1F, -28, 0);  // open
        Class[] v4 = new Class[1];
        v4[0] = String.class;
        Object stream = v0_1.getMethod(v3, v4).invoke(assman, v2);
        Cipher cipher = Cipher.getInstance(MainActivity.decryptString(-15, -15, 5));  // AES/CFB/NoPadding
        cipher.init(2, new SecretKeySpec(new byte[]{0x32, -93, -33, 0x17, -36, 0x68, 0x76, -25, 0x27, -97, -90, 0x14, 0x2E
                , -46, -86, 0x6C}, MainActivity.decryptString(-15, -29, 3)), new IvParameterSpec(new byte[]{-87, 0x62, -45
                , 0x29, 0x5A, -112, -28, 0x7A, -14, 0x73, 0x6E, 0x73, -115, 0x3A, 5, -47}));
        return new CipherInputStream(((InputStream)stream), cipher).available();
    }
```

不要明文存储密钥，加密或混淆

资源保护

- 静态资源自定义格式加密
- 加密算法尽量不要太浪费CPU
- 密钥可分开存储，不要硬编码明文存储

什么是外挂

- 第一次听到外挂是什么时候?
- 首次接触的外挂是什么功能?
- 用到、碰到、写过哪些外挂，都是什么功能?

外挂分类

- 内存修改

遍历进程的内存地址，根据搜索的数值类型，按照对应字节长度的整型值比较，找出匹配的内存地址列表。金山游侠、cheat engine，八门神器等…

- 按键模拟

区块颜色值读取，下发键盘指令，比如按键精灵的分辨率强制，血条色块读取，进度百分比等。代表：按键精灵…

- 内存地址（函数）Call

内存地址读取，获得数值，Call 内存地址，调用程序已有函数，执行游戏指令。代表：LOL无限视距等…

- 协议外挂

俗称封包挂，脱机挂，根据通讯协议，模拟客户端，发送合法协议的客户端。代表：《传奇》早期的封包外挂

Cheat Engine

八门神器


八门神器: 艾诺迪亚4[1736]
搜索项1
1 25316408: 1060
2 4008FBC0: 1060
3 400AAAA0: 1060
4 41D115D4: 1060
5 41D2A7EC: 1060
6 41D2AFEC: 1060
Lv. 1
祭司
凯恩
技能点:0
1432 / 1432
HP
100%
144 / 200
MP
72%
1060 / 12802
EXP
8%
能力点:0
DW
力量 11
W
敏捷 7
W
体力 9
W
智力 9
W
精力 15
W
1
6
DMG 17
M.DMG 32
CRT 7.0%
H.RATE 98.0%
C.DMG 100.0%
DEF 21
P.RES 20.7%
M.RES 0.0%
AVD 17.1%
W.D.R 3.0%
S.D.R 12.0%
2
7
3
8
4
9
5
0

内存修改

- 目标值与某固定数值做亦或，躲避数值搜索

- 多处存储，存非整型的校验值，使用时与之校验

按键模拟

- 遍历进程列表，检测常见软件进程名
- 遍历进程列表的调用so列表，检测软件名的so链接库名
- android上比较难处理...

内存Call

- 运行时，开线程检测自身加载的so列表（被注入时，会有so链接库 attach到该进程）

- 好像无解...

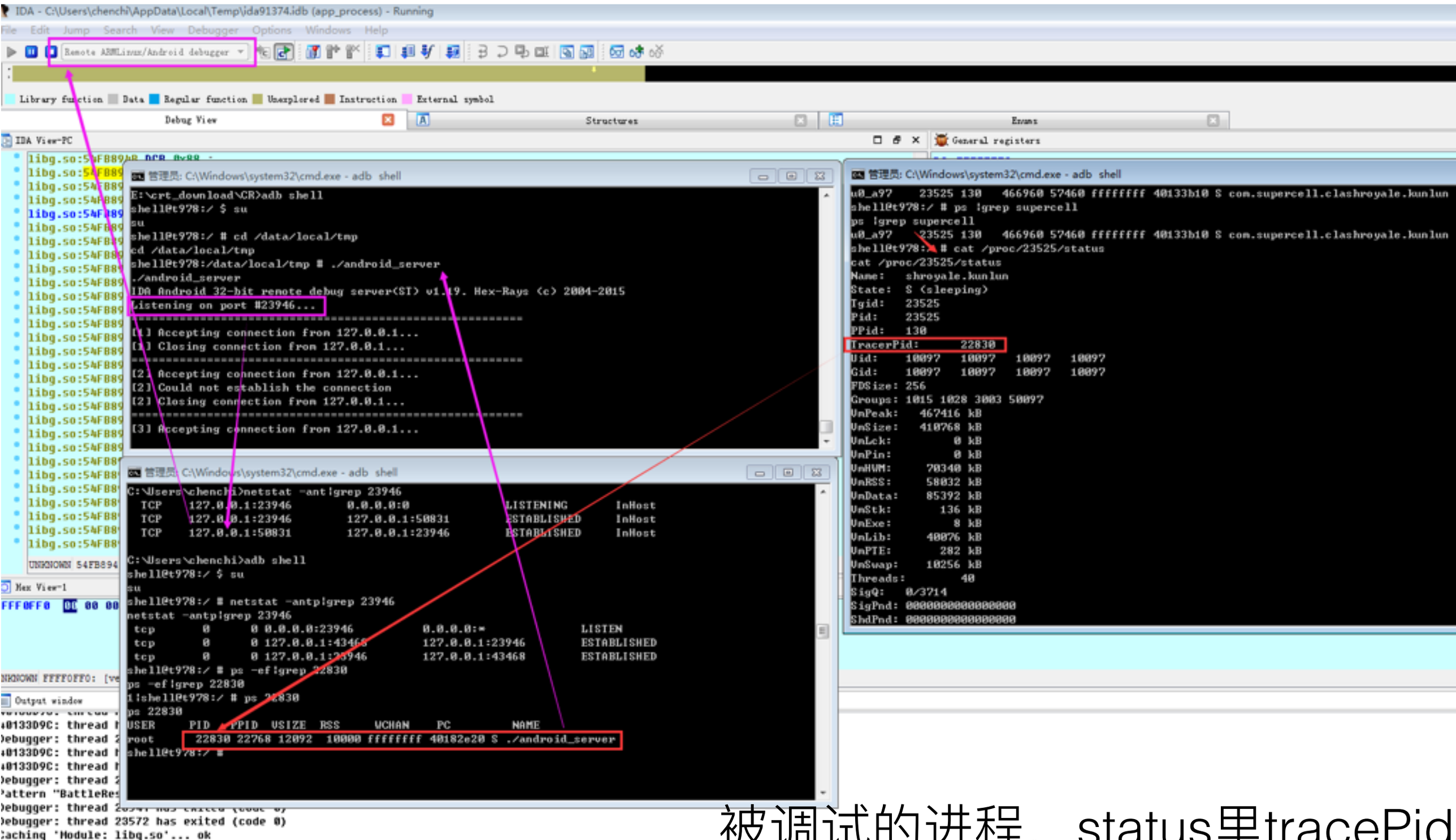
协议外挂

- 通讯协议加密，公钥私钥分开，每个用户、每次登录通讯加密的KEY都不一样

- 提高客户端反编译的难度，函数混淆，KEY等字符串加密

- 反调试，新开线程检测，参考下图（有点耗电）

反调试



被调试的进程，status里tracePid

反注入

- 性能分析时，常关注的 /proc/PID/maps 中内存分配
- 参考上面（进程加载的so在内存分布的图，96页左右）
- 检测异常so，决定是否继续运行程序

其他对抗方案

- 二次打包:关键文件的hash与服务器校验
- 二次打包:利用打包工具缺陷技巧（比如apktool打包png问题）
- 静态分析:畸形ELF格式文件构造等...
- 动态分析:反调试、反注入，检测后停止运行...

没有绝对安全

- 多点套路，少点真诚。
- 多点、多处、不定时，不同函数去校验检测
- 一切安全方案都是为了提高对抗成本
- 等做到Clash Royale这等规模后再说（先不着急，先出产品）
- 对抗是长期持续的工程，不能一劳永逸

移动软件保护产品

- 梆梆 :http://www.bangcle.com/ （COC）
- 爱加密 :https://www.ijiami.cn/ （花千骨）
- APKProtect :http://www.apkprotect.com/
- Shield4J :http://shield4j.com/
- DexGuard :http://www.saikoa.com/dexguard

完

业余爱好，如有不对，敬请斧正。

参考及资料

- COC的proxy：https://github.com/clugh/coc-proxy
- LOL Launcher通讯协议分析：http://www.cnxct.com/league-of-legends-launcher-of-osx/
- 文件头：https://en.wikipedia.org/wiki/Magic_number_(programming)
- 现代密码学 http://open.163.com/movie/2012/10/B/K/M99VIFJA6_M9A018BBK.html
- 资源加密：https://www.pnfsoftware.com/blog/dexguards-assets-encryption/
- APK保护：http://bbs.pediy.com/showthread.php?t=183116
- ELF修复的思考:http://bbs.pediy.com/showthread.php?t=192874