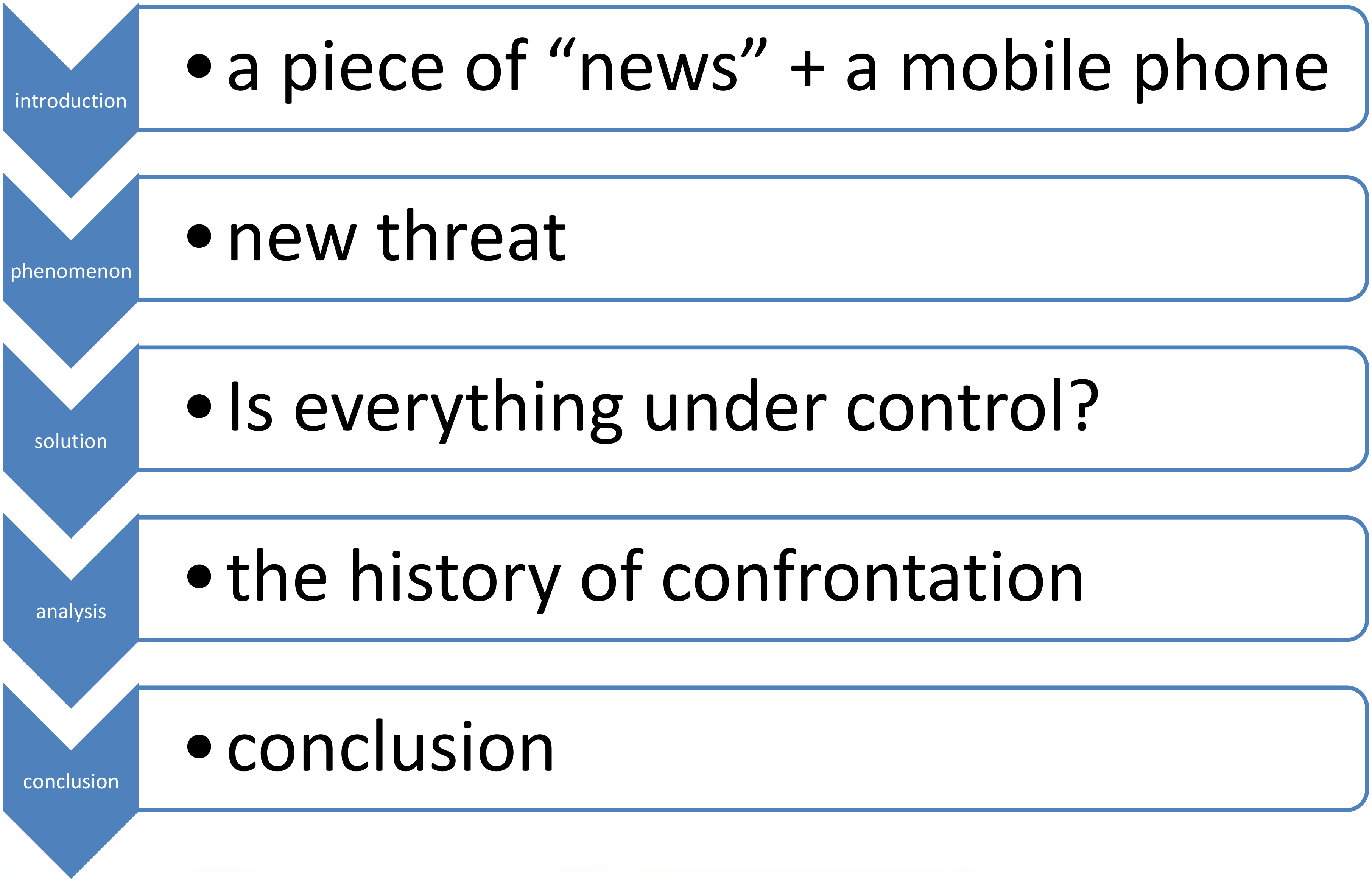
Malware in Mobile Platform from Panoramic Industrial View

Antiy Labs

Contents



introduction

- a piece of “news” + a mobile phone

phenomenon

- new threat

solution

- Is everything under control?

analysis

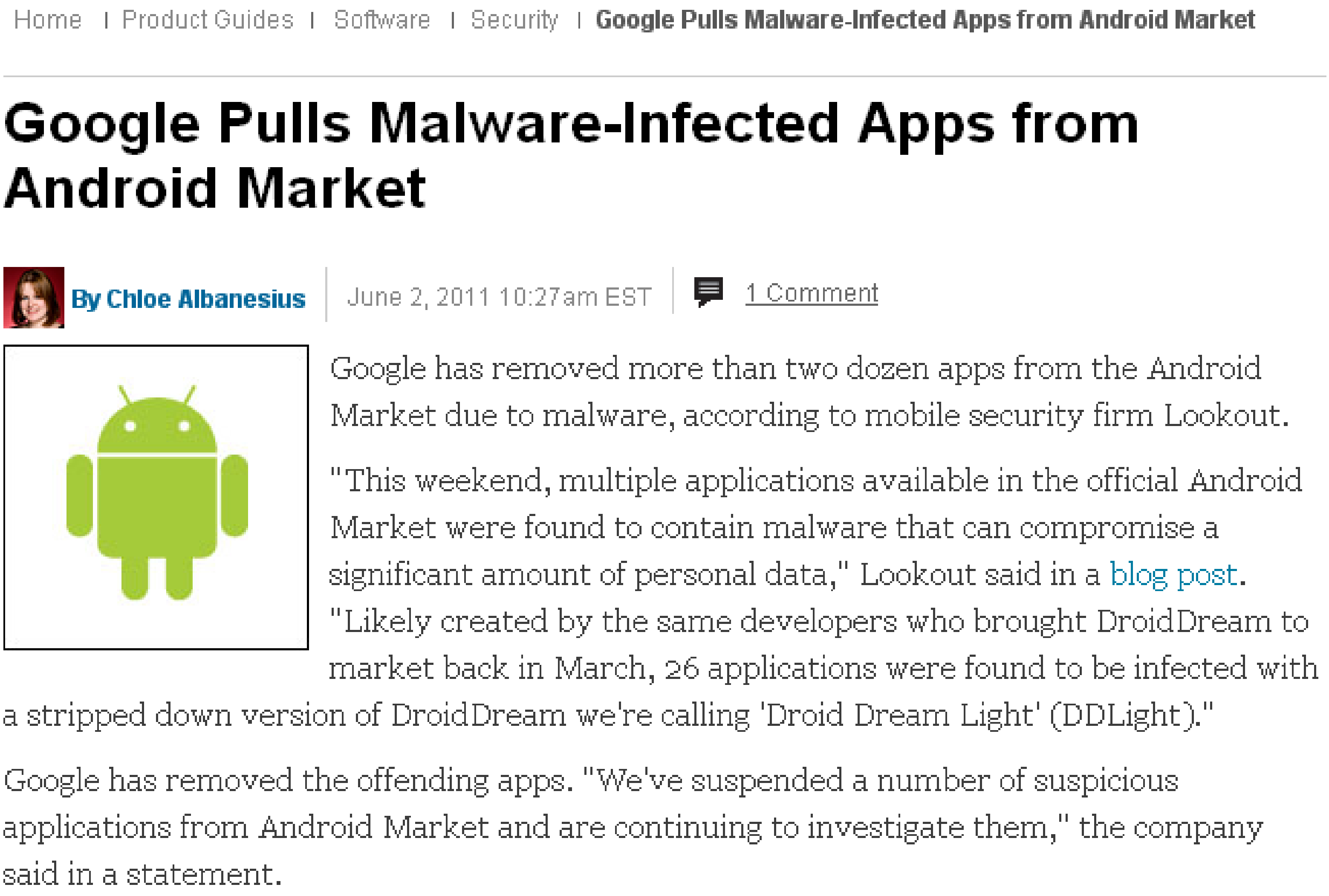
- the history of confrontation

conclusion

- conclusion

INTRODUCTION:
A PIECE OF “NEWS”+ A MOBILE PHONE

Talking From A Piece of “News”



Home | Product Guides | Software | Security | **Google Pulls Malware-Infected Apps from Android Market**

Google Pulls Malware-Infected Apps from Android Market

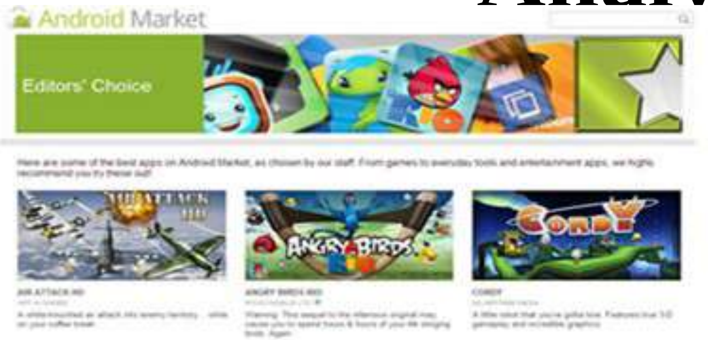
By Chloe Albanesius | June 2, 2011 10:27am EST | 1 Comment

Google has removed more than two dozen apps from the Android Market due to malware, according to mobile security firm Lookout.

"This weekend, multiple applications available in the official Android Market were found to contain malware that can compromise a significant amount of personal data," Lookout said in a blog post. "Likely created by the same developers who brought DroidDream to market back in March, 26 applications were found to be infected with a stripped down version of DroidDream we're calling 'Droid Dream Light' (DDLight)."

Google has removed the offending apps. "We've suspended a number of suspicious applications from Android Market and are continuing to investigate them," the company said in a statement.

Analysis



user channel

Android
Market

service provider

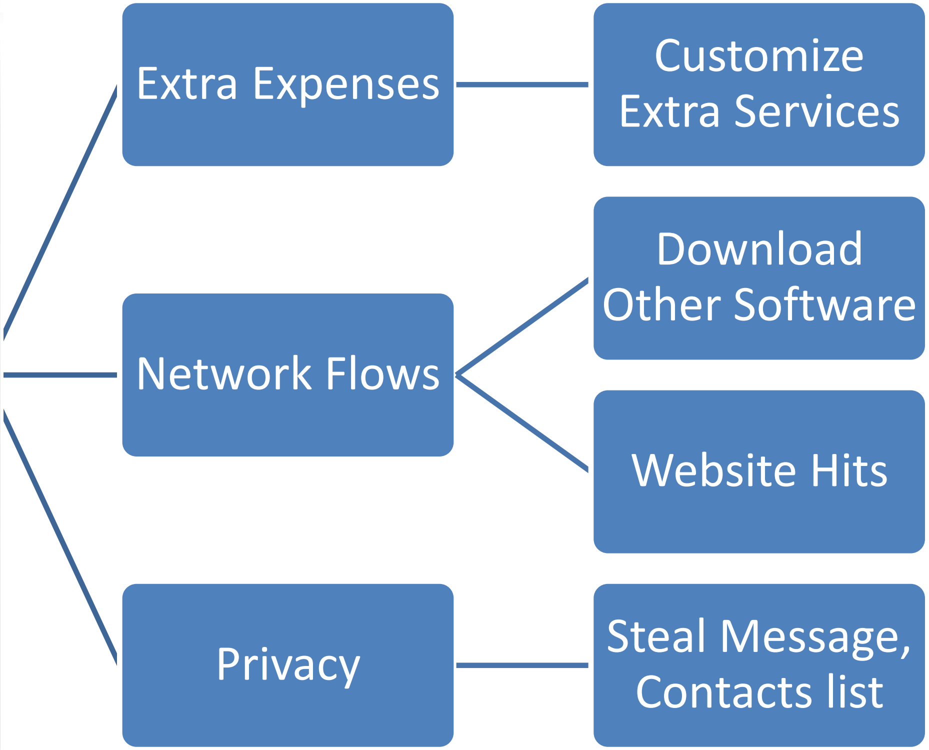
Google

consumer

smartphone vendor

mobile phone distributor

Taking from a Grey Mobile Phone



Extra Expenses

Customize Extra Services

Network Flows

Download Other Software

Website Hits

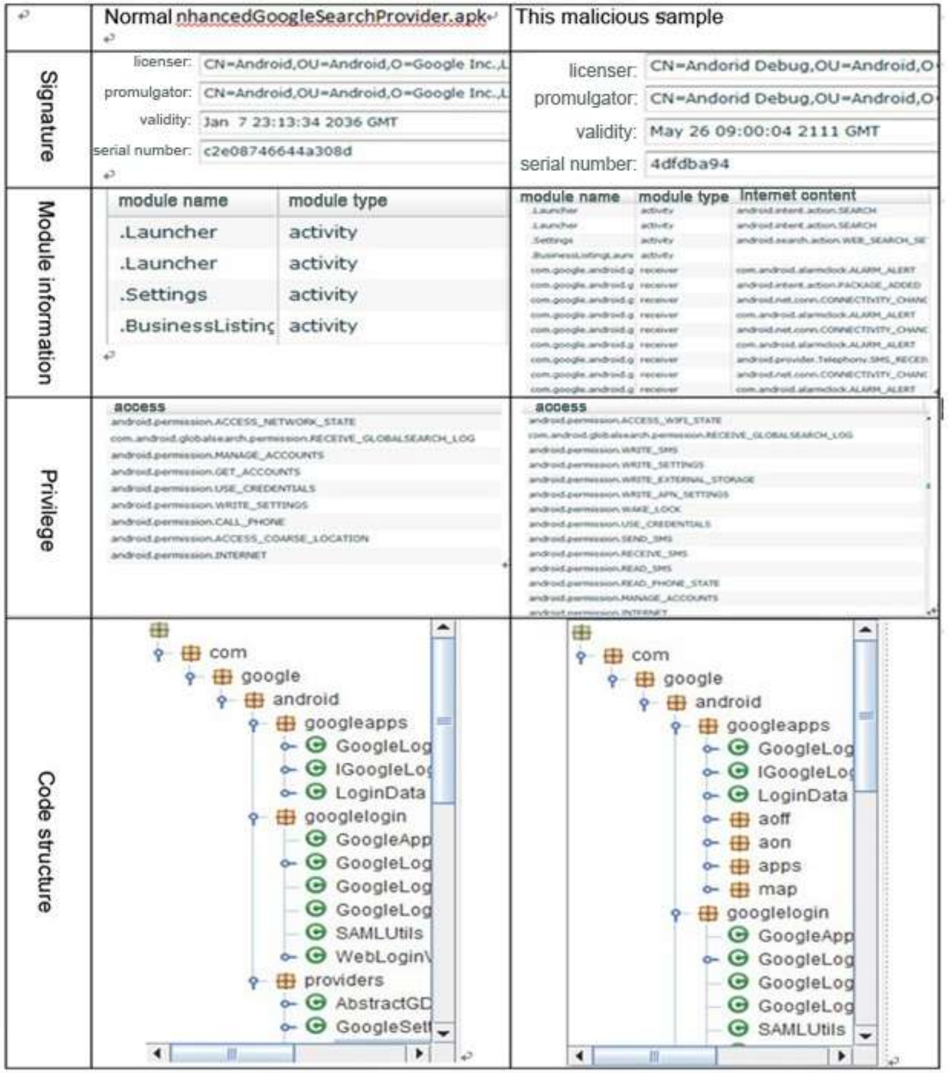
Privacy

Steal Message, Contacts list

Analysis on Malware

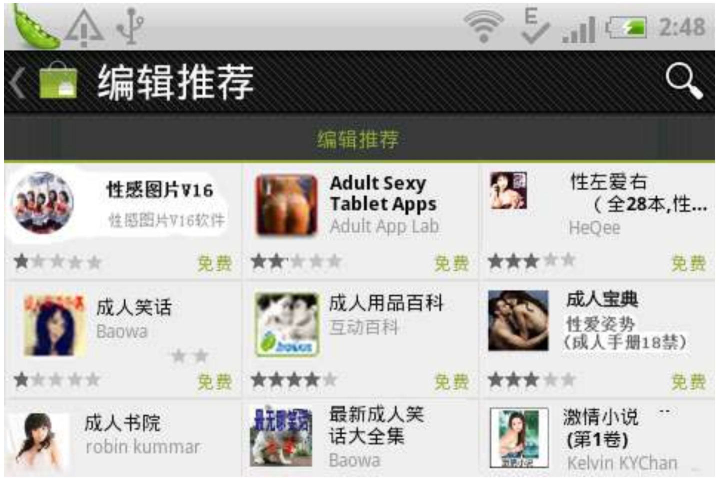
Information	
Name	com.google.android.providers.enhancedgooglesearch
Chinese Name	
Original Name	a.apk
URL Source	
Collection Source	
System Platform	Android
Format	apk
MD5 Value	BFBB58D0F8B487869393A0244AE71AFC
CRC32 Value	C1C12A99
SHA1 Value	59EE114166CDBCDDB88B38299934021080053D86
Bytes	

Malware Information	
Name	Trojan/Android.droiddg.a[rmt,sys]
CNCERT Name	a.remote.droiddg.a
Chines Name	
Other Names	None
Original/Tied	Firmware embedding
Threat type	remote system



	Normal nhancedGoogleSearchProvider.apk	This malicious sample
Signature	licenser: CN=Android,OU=Android,O=Google Inc.,L promulgator: CN=Android,OU=Android,O=Google Inc.,L validity: Jan 7 23:13:34 2036 GMT serial number: c2e08746644a308d	licenser: CN=Andorid Debug,OU=Android,O promulgator: CN=Andorid Debug,OU=Android,O validity: May 26 09:00:04 2111 GMT serial number: 4dfdba94
Module information	module name / module type .Launcher / activity .Launcher / activity .Settings / activity .BusinessListinç / activity	module name / module type / Internet content .Launcher / activity / android.intent.action.SEARCH .Launcher / activity / android.intent.action.SEARCH .Settings / activity / android.search.action.WEB_SEARCH_SE .BusinessListingLaun / activity / com.google.android.g / receiver / com.android.alarmclock.ALARM_ALERT com.google.android.g / receiver / android.intent.action.PACKAGE_ADDED com.google.android.g / receiver / android.net.conn.CONNECTIVITY_CHANC com.google.android.g / receiver / com.android.alarmclock.ALARM_ALERT com.google.android.g / receiver / android.net.conn.CONNECTIVITY_CHANC com.google.android.g / receiver / com.android.alarmclock.ALARM_ALERT com.google.android.g / receiver / android.provider.Telephony.SMS_RECEI com.google.android.g / receiver / android.net.conn.CONNECTIVITY_CHANC com.google.android.g / receiver / com.android.alarmclock.ALARM_ALERT
Privilege	access android.permission.ACCESS_NETWORK_STATE com.android.globalsearch.permission.RECEIVE_GLOBALSEARCH_LOG android.permission.MANAGE_ACCOUNTS android.permission.GET_ACCOUNTS android.permission.USE_CREDENTIALS android.permission.WRITE_SETTINGS android.permission.CALL_PHONE android.permission.ACCESS_COARSE_LOCATION android.permission.INTERNET	access android.permission.ACCESS_WIFI_STATE com.android.globalsearch.permission.RECEIVE_GLOBALSEARCH_LOG android.permission.WRITE_SMS android.permission.WRITE_SETTINGS android.permission.WRITE_EXTERNAL_STORAGE android.permission.WRITE_APN_SETTINGS android.permission.WAKE_LOCK android.permission.USE_CREDENTIALS android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.READ_SMS android.permission.READ_PHONE_STATE android.permission.MANAGE_ACCOUNTS android.permission.INTERNET
Code structure	com google android googleapps GoogleLog IGoogleLo LoginData googlelogin GoogleApp GoogleLog GoogleLog GoogleLog SAMLUtils WebLogin\ providers AbstractGD GoogleSet	com google android googleapps GoogleLog IGoogleLo LoginData aoff aon apps map googlelogin GoogleApp GoogleLog GoogleLog GoogleLog SAMLUtils

A Truely Funny Story



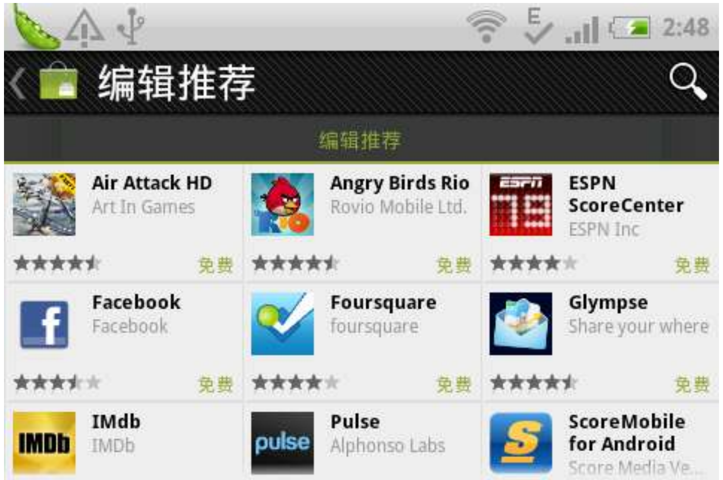
2:48

编辑推荐

编辑推荐

性感图片V16 性感图片V16软件 免费	Adult Sexy Tablet Apps Adult App Lab 免费	性左爱右 （全28本,性... HeQee 免费
成人笑话 Baowa 免费	成人用品百科 互动百科 免费	成人宝典 性爱姿势 （成人手册18禁） 免费
成人书院 robin kummar	最新成人笑话大全集 Baowa	激情小说 (第1卷) Kelvin KYChan

A sexy E-market



2:48

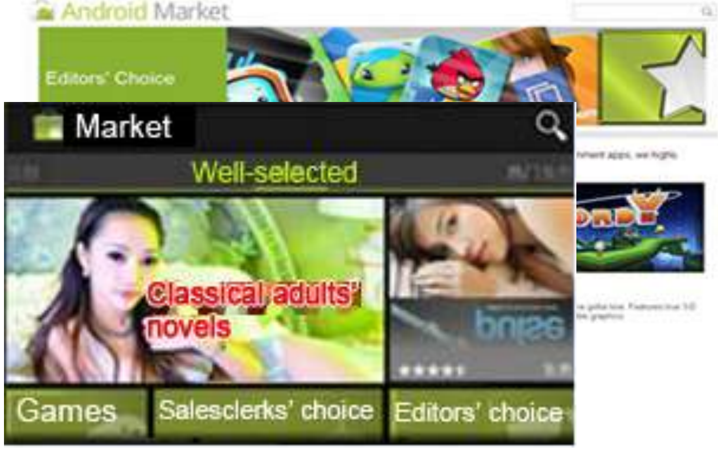
编辑推荐

编辑推荐

Air Attack HD Art In Games 免费	Angry Birds Rio Rovio Mobile Ltd. 免费	ESPN ScoreCenter ESPN Inc 免费
Facebook Facebook 免费	Foursquare foursquare 免费	Glympse Share your where 免费
IMdb IMDb	Pulse Alphonso Labs	ScoreMobile for Android Score Media Ve...

Real E-market

Diverted Industrial Chain



Android Market

service provider

Google

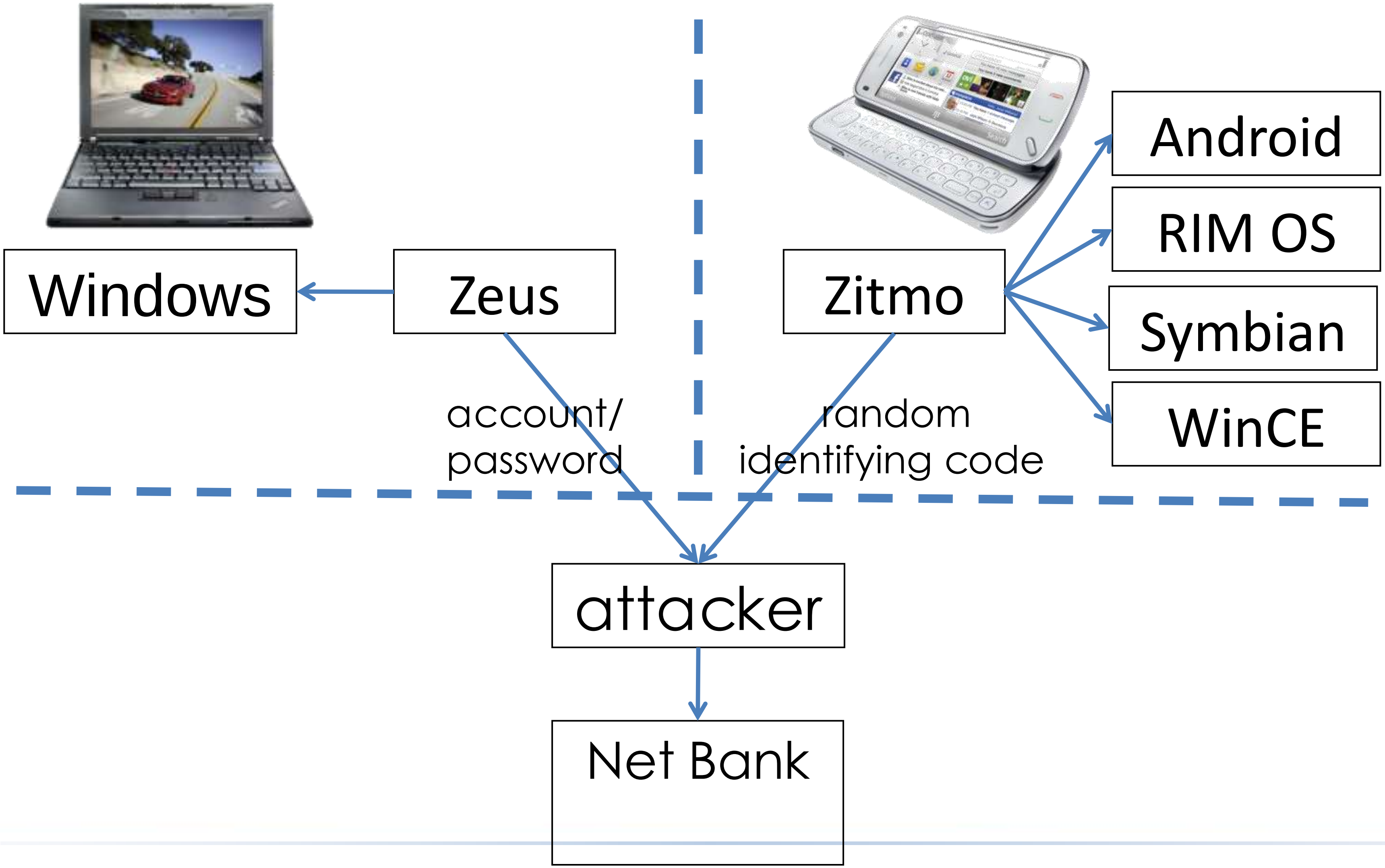
consumer

smartphone vendor

mobile phone distributor

INTERPRETATIONS OF NEW THREATS

Crossing the System Platform(**Zitmo**)



Windows

Zeus

account/ password

Zitmo

Android

RIM OS

Symbian

WinCE

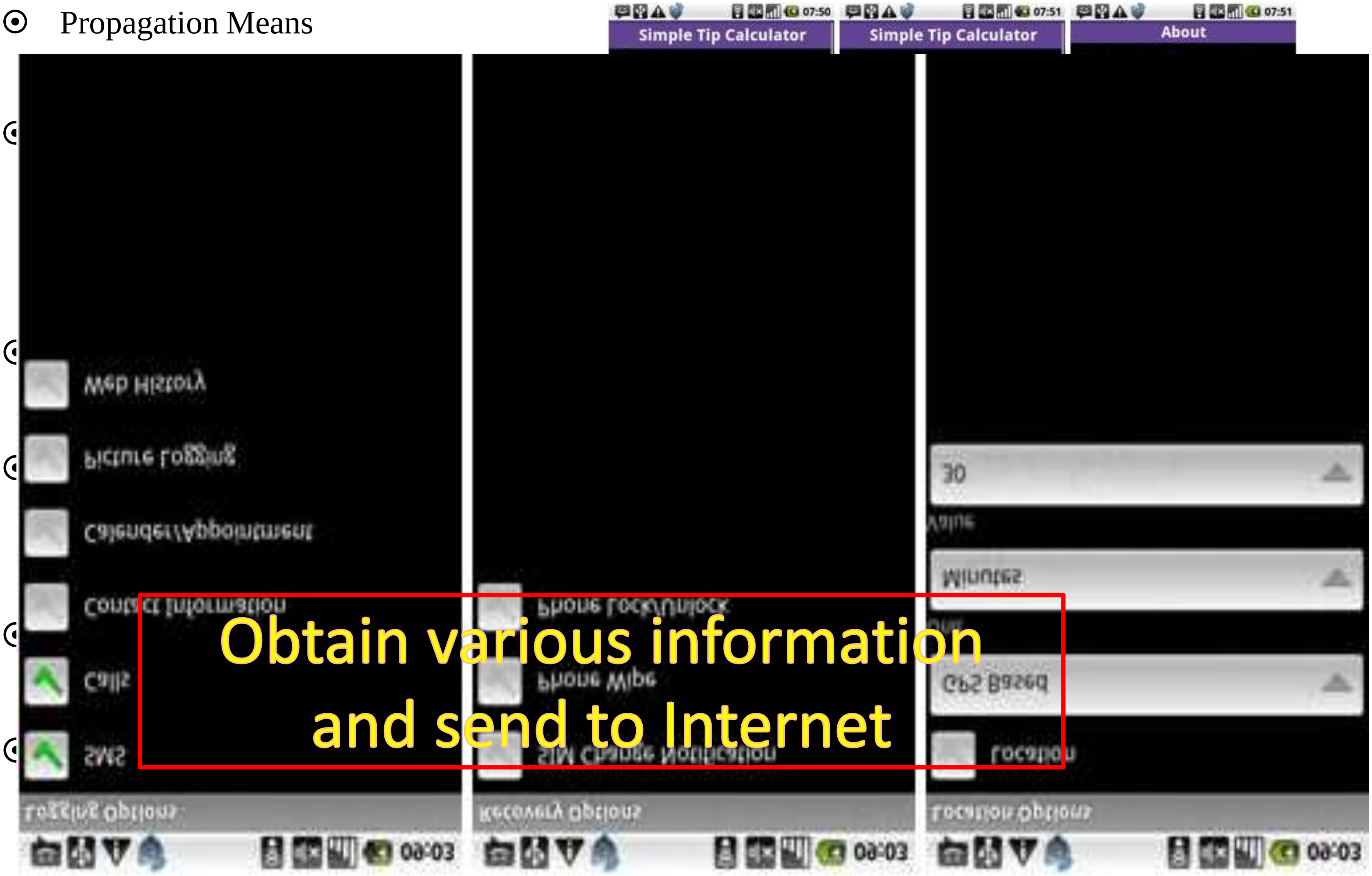
random identifying code

attacker

Net Bank

Steal Message and Contacts List (SW.Spyware)

- Propagation Means

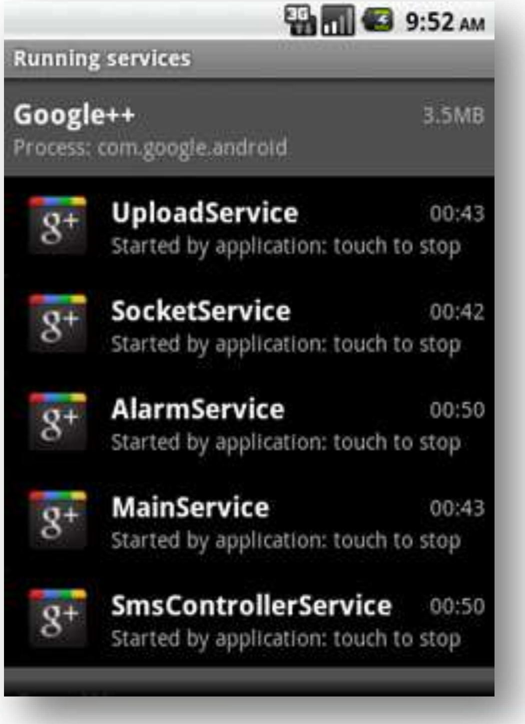


Obtain various information and send to Internet

Spycall (Nickispy)

- Spycall and send back
- Disguise as Google+

in the First Time


9:52 AM

Running services

Google++ 3.5MB
Process: com.google.android

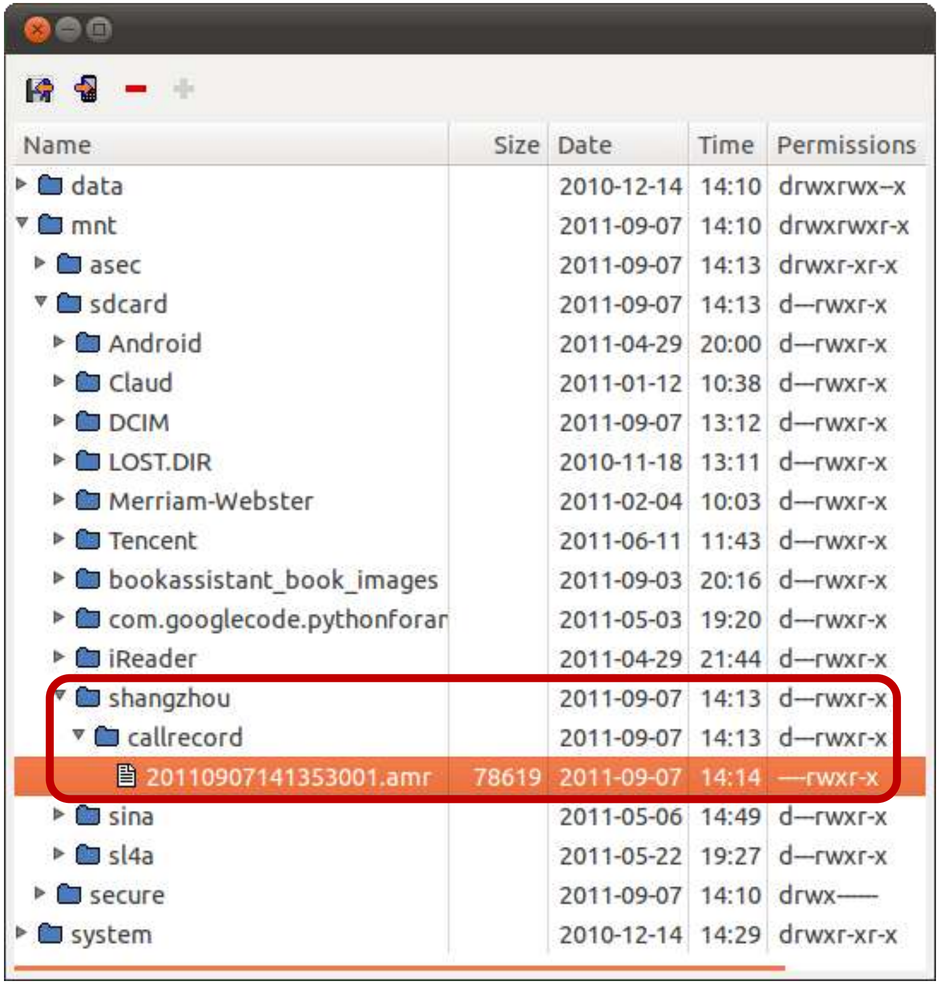
UploadService 00:43
Started by application: touch to stop

SocketService 00:42
Started by application: touch to stop

AlarmService 00:50
Started by application: touch to stop

MainService 00:43
Started by application: touch to stop

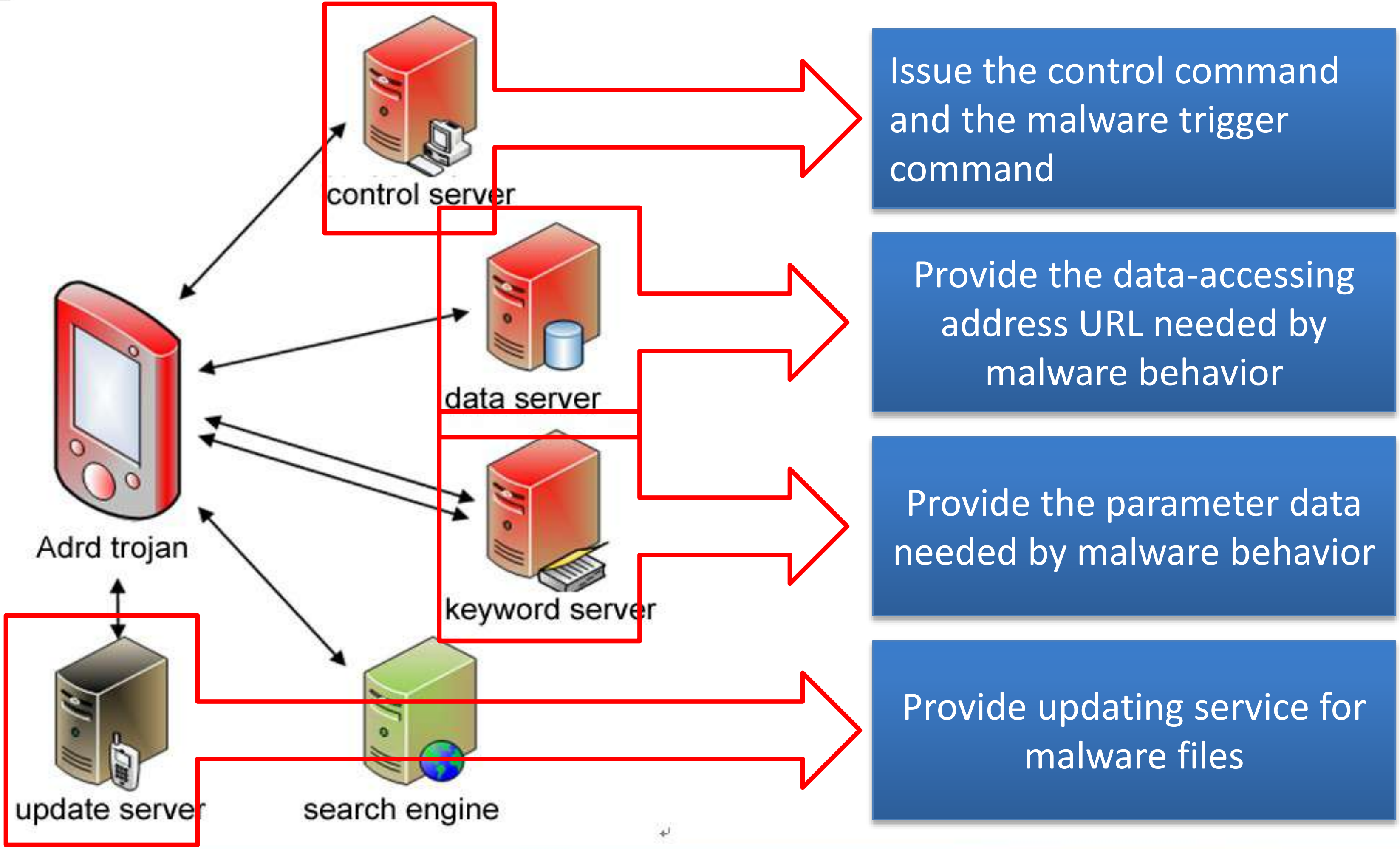
SmsControllerService 00:50
Started by application: touch to stop



Name	Size	Date	Time	Permissions
data		2010-12-14	14:10	drwxrwx–x
mnt		2011-09-07	14:10	drwxrwxr-x
asec		2011-09-07	14:13	drwxr-xr-x
sdcard		2011-09-07	14:13	d—rwxr-x
Android		2011-04-29	20:00	d—rwxr-x
Claud		2011-01-12	10:38	d—rwxr-x
DCIM		2011-09-07	13:12	d—rwxr-x
LOST.DIR		2010-11-18	13:11	d—rwxr-x
Merriam-Webster		2011-02-04	10:03	d—rwxr-x
Tencent		2011-06-11	11:43	d—rwxr-x
bookassistant_book_images		2011-09-03	20:16	d—rwxr-x
com.googlecode.pythonforar		2011-05-03	19:20	d—rwxr-x
iReader		2011-04-29	21:44	d—rwxr-x
shangzhou		2011-09-07	14:13	d—rwxr-x
callrecord		2011-09-07	14:13	d—rwxr-x
20110907141353001.amr	78619	2011-09-07	14:14	—rwxr-x
sina		2011-05-06	14:49	d—rwxr-x
sl4a		2011-05-22	19:27	d—rwxr-x
secure		2011-09-07	14:10	drwx——
system		2010-12-14	14:29	drwxr-xr-x

Form Control System(Adrd)

- Trojan/Android.Adrd.a[exp]



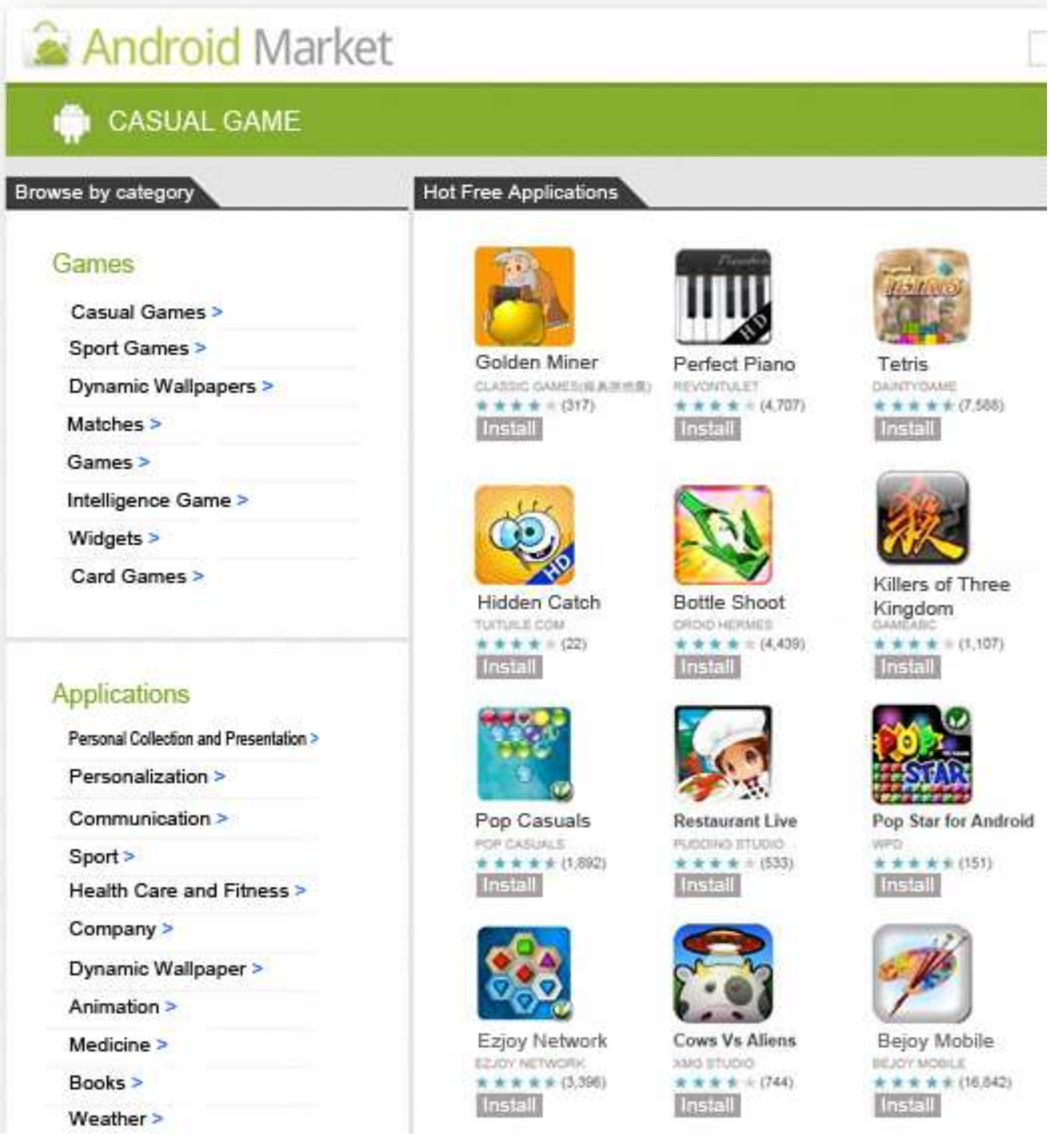
Issue the control command and the malware trigger command

Provide the data-accessing address URL needed by malware behavior

Provide the parameter data needed by malware behavior

Provide updating service for malware files

the interdisciplinary use of leak and social engineering



Android Market

CASUAL GAME

Browse by category

Games

- Casual Games >
- Sport Games >
- Dynamic Wallpapers >
- Matches >
- Games >
- Intelligence Game >
- Widgets >
- Card Games >

Applications

- Personal Collection and Presentation >
- Personalization >
- Communication >
- Sport >
- Health Care and Fitness >
- Company >
- Dynamic Wallpaper >
- Animation >
- Medicine >
- Books >
- Weather >

Hot Free Applications

Golden Miner
CLASSIC GAMES([illegible])
★★★★☆ (317)
Install

Perfect Piano
REVONTULET
★★★★☆ (4,707)
Install

Tetris
DAINTYGAME
★★★★★ (7,588)
Install

Hidden Catch
TUITUILE.COM
★★★★☆ (22)
Install

Bottle Shoot
DROID HERMES
★★★★☆ (4,439)
Install

Killers of Three Kingdom
GAMEABC
★★★★☆ (1,107)
Install

Pop Casuals
POP CASUALS
★★★★★ (1,892)
Install

Restaurant Live
PUDDING STUDIO
★★★★☆ (533)
Install

Pop Star for Android
WPD
★★★★★ (151)
Install

Ezjoy Network
EZJOY NETWORK
★★★★★ (3,396)
Install

Cows Vs Aliens
XMG STUDIO
★★★★☆ (744)
Install

Bejoy Mobile
BEJOY MOBILE
★★★★★ (16,842)
Install

1. Replace normal application by means of Google application download bug

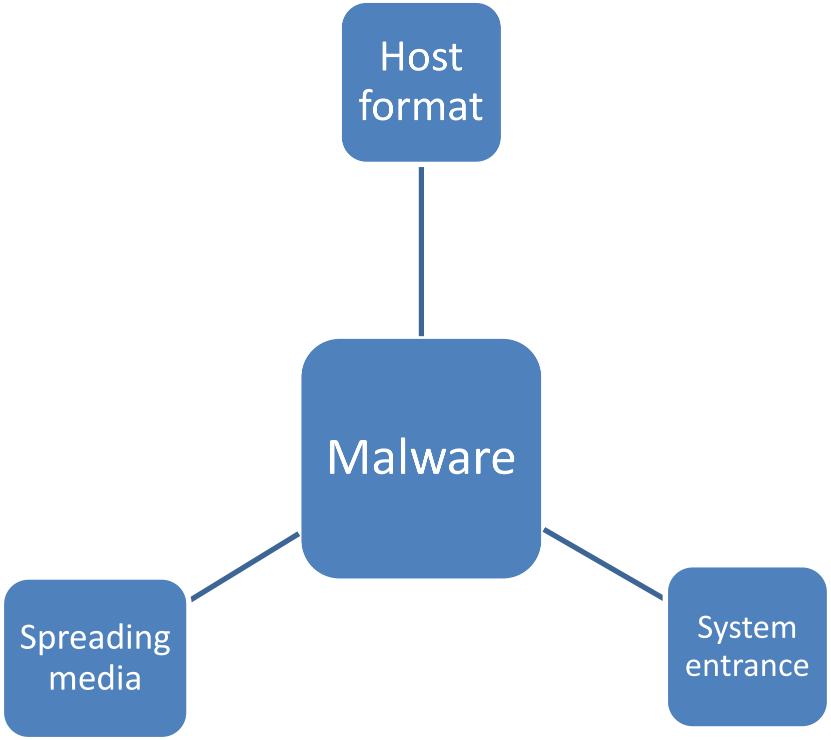
2. Consumers download bootleg applications which are actually malware, with 200 thousand victims.

3.Google clears out malware by remote upgrade interplay and provides security software

4.The malware attacker disguises as Google security software

SOLUTION：
IS EVERYTHING UNDER CONTROL

Traditional view

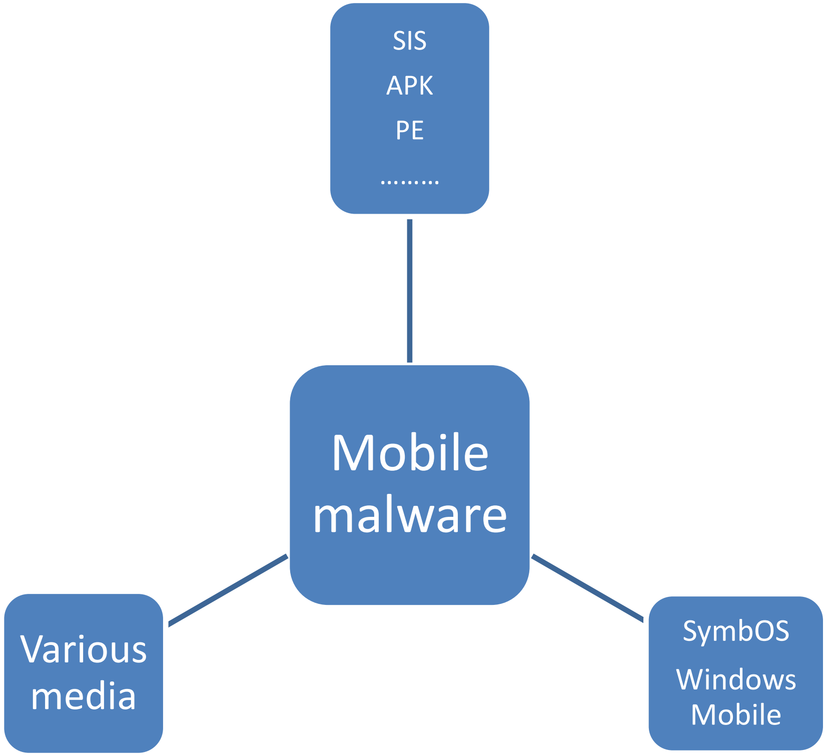


Host format

Malware

Spreading media

System entrance



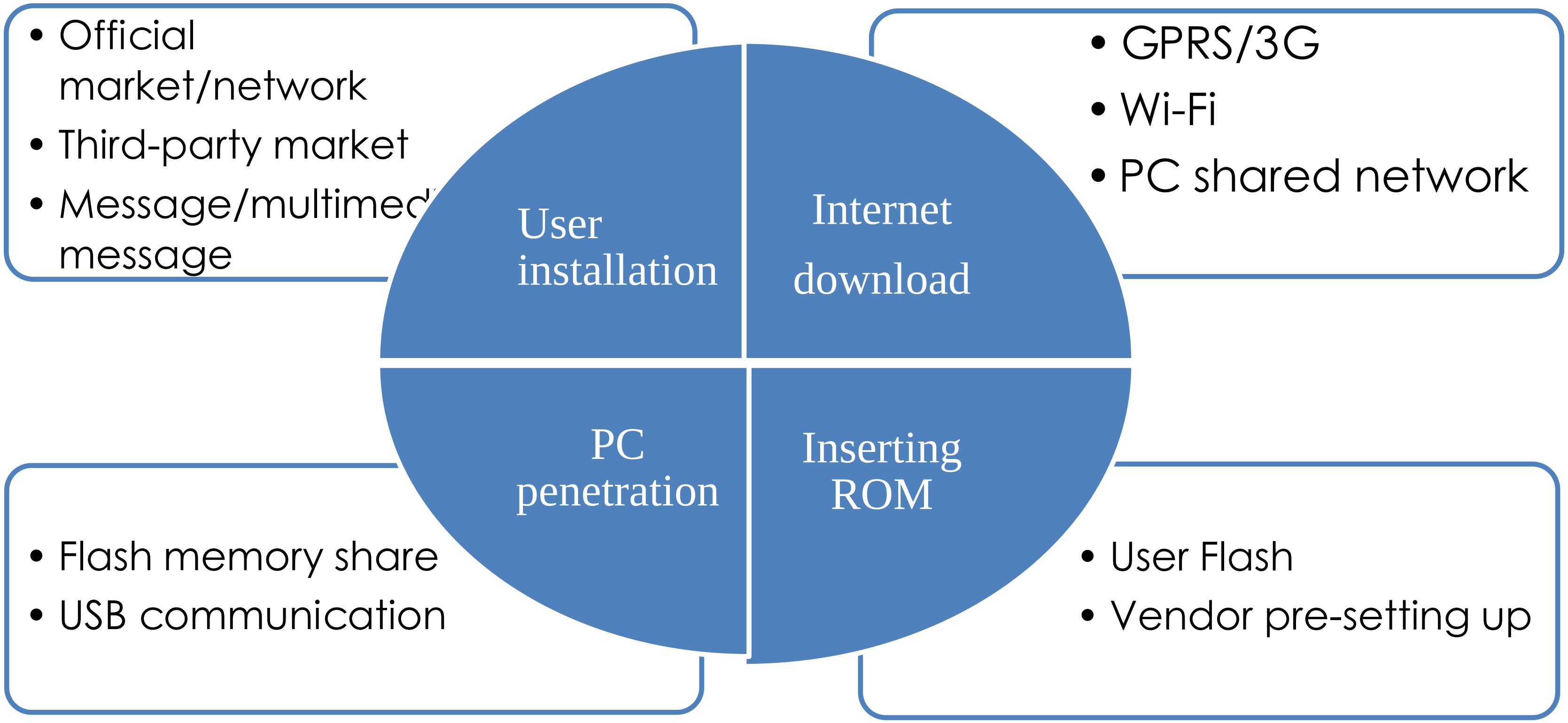
SIS
APK
PE
………

Mobile malware

Various media

SymbOS
Windows Mobile

Major Spreading Approaches



User installation

- Official market/network
- Third-party market
- Message/multimedi message

Internet download

- GPRS/3G
- Wi-Fi
- PC shared network

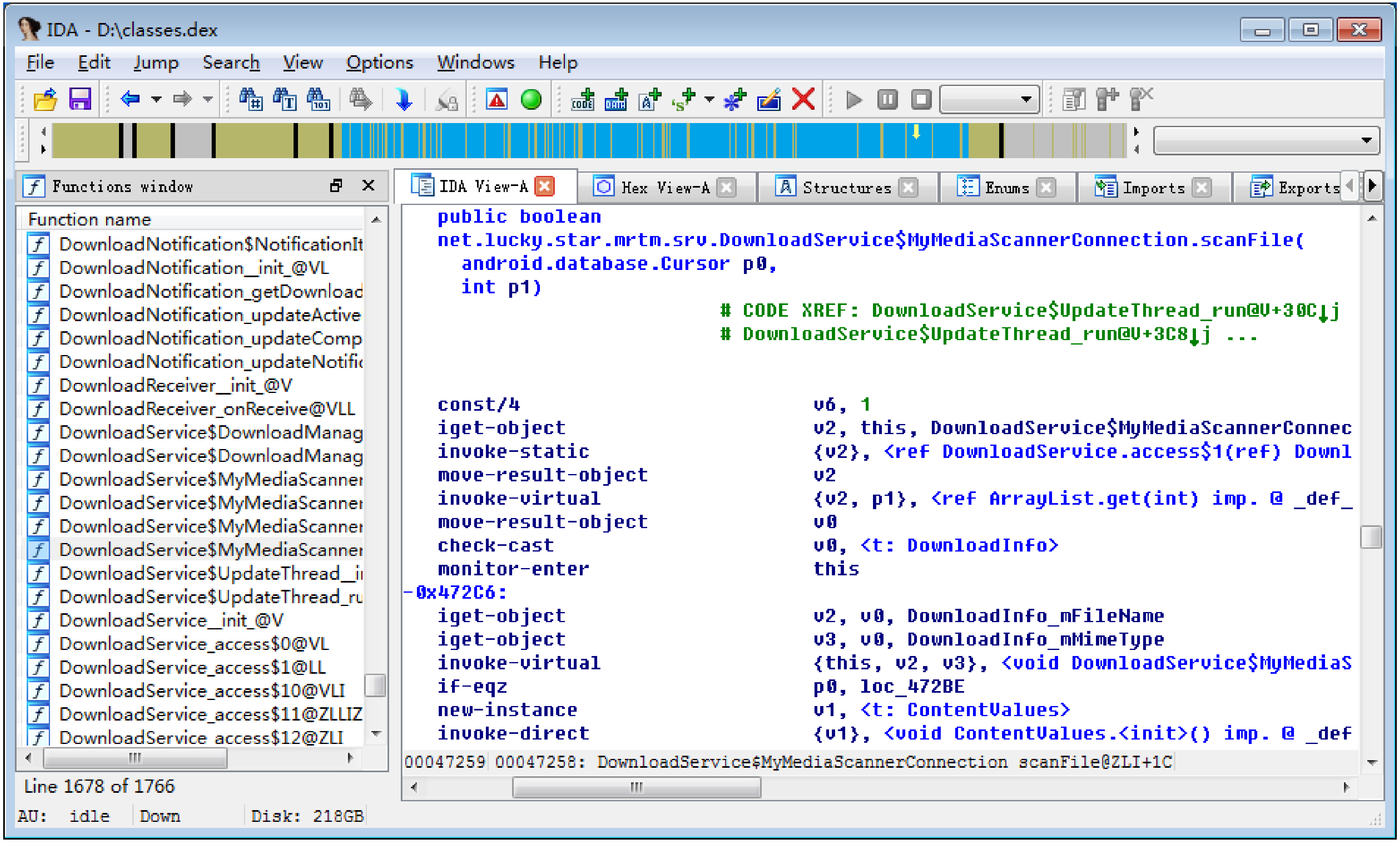
PC penetration

- Flash memory share
- USB communication

Inserting ROM

- User Flash
- Vendor pre-setting up

Dalvik Disassembling: IDA Pro



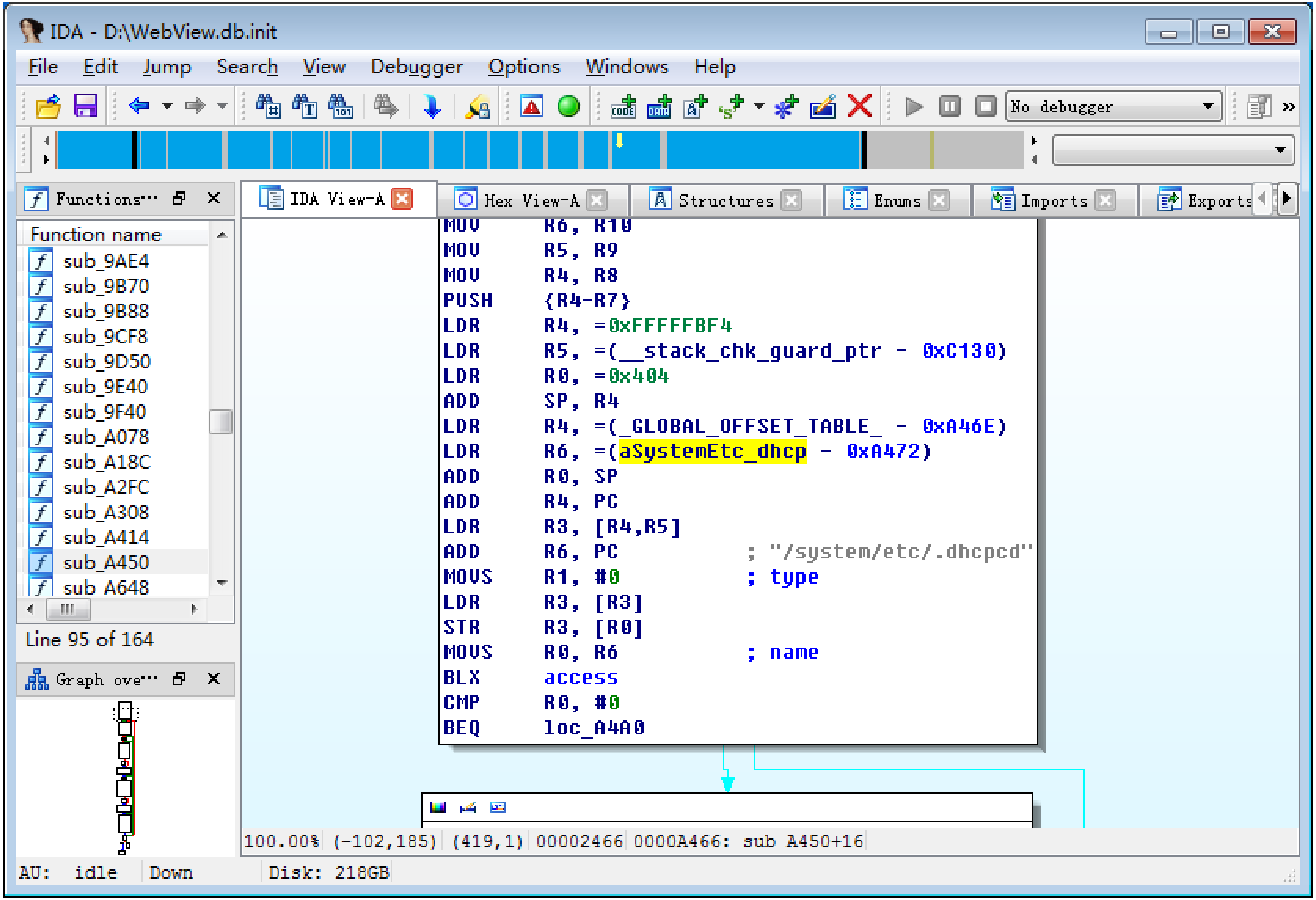
```
Function name
DownloadNotification$NotificationIt
DownloadNotification__init_@VL
DownloadNotification_getDownload
DownloadNotification_updateActive
DownloadNotification_updateComp
DownloadNotification_updateNotific
DownloadReceiver__init_@V
DownloadReceiver_onReceive@VLL
DownloadService$DownloadManag
DownloadService$DownloadManag
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$UpdateThread_i
DownloadService$UpdateThread_ru
DownloadService__init_@V
DownloadService_access$0@VL
DownloadService_access$1@LL
DownloadService_access$10@VLI
DownloadService_access$11@ZLLIZ
DownloadService_access$12@ZLI
```

Line 1678 of 1766

```
  public boolean
  net.lucky.star.mrtm.srv.DownloadService$MyMediaScannerConnection.scanFile(
    android.database.Cursor p0,
    int p1)
                        # CODE XREF: DownloadService$UpdateThread_run@V+30C↓j
                        # DownloadService$UpdateThread_run@V+3C8↓j ...


  const/4                          v6, 1
  iget-object                      v2, this, DownloadService$MyMediaScannerConnec
  invoke-static                    {v2}, <ref DownloadService.access$1(ref) Downl
  move-result-object               v2
  invoke-virtual                   {v2, p1}, <ref ArrayList.get(int) imp. @ _def_
  move-result-object               v0
  check-cast                       v0, <t: DownloadInfo>
  monitor-enter                    this
-0x472C6:
  iget-object                      v2, v0, DownloadInfo_mFileName
  iget-object                      v3, v0, DownloadInfo_mMimeType
  invoke-virtual                   {this, v2, v3}, <void DownloadService$MyMediaS
  if-eqz                           p0, loc_472BE
  new-instance                     v1, <t: ContentValues>
  invoke-direct                    {v1}, <void ContentValues.<init>() imp. @ _def
00047259 00047258: DownloadService$MyMediaScannerConnection scanFile@ZLI+1C
```

AU: idle   Down   Disk: 218GB

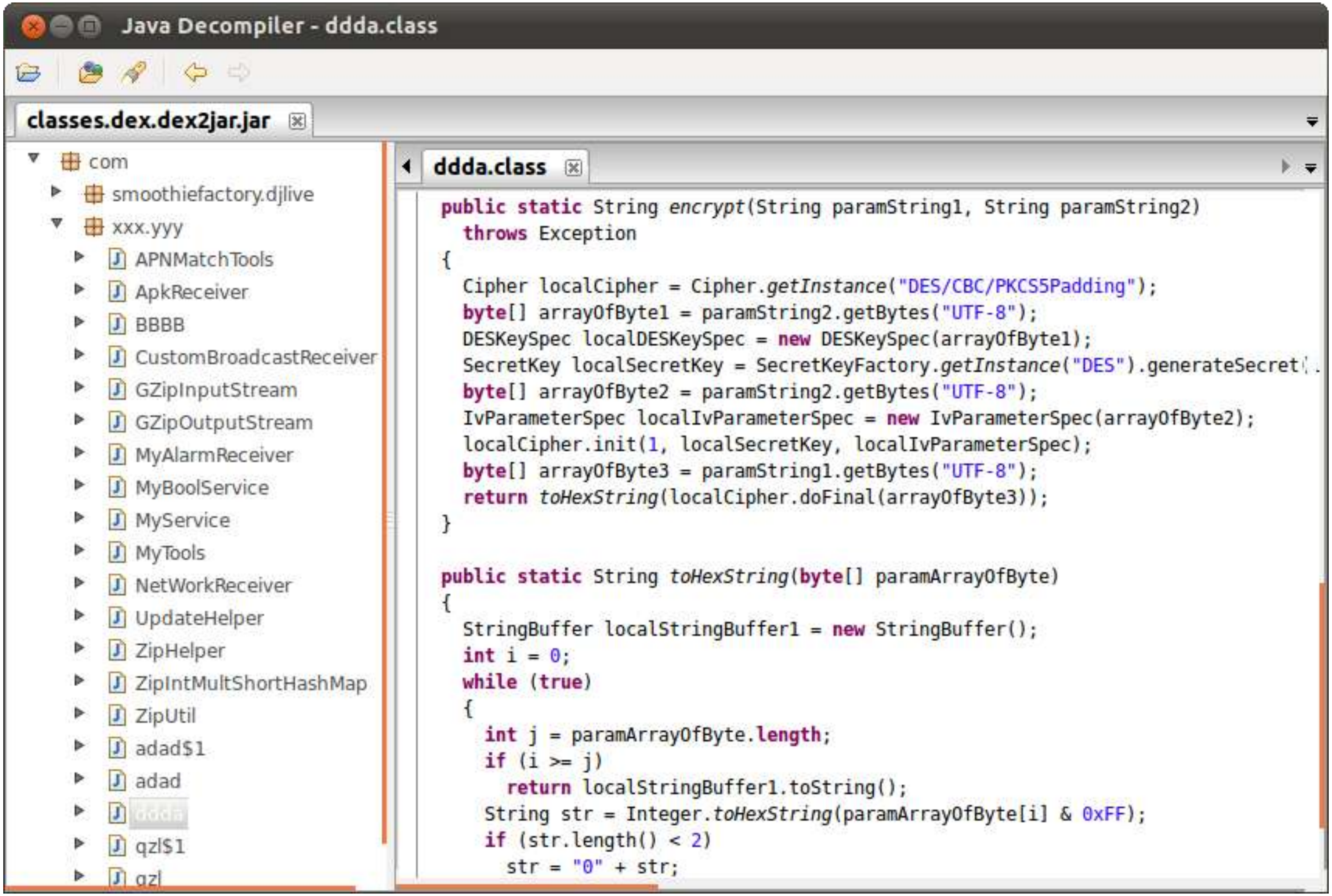
Static Analysis: ARM Disassembling



```
MOV     R6, R10
MOV     R5, R9
MOV     R4, R8
PUSH    {R4-R7}
LDR     R4, =0xFFFFFBF4
LDR     R5, =(__stack_chk_guard_ptr - 0xC130)
LDR     R0, =0x404
ADD     SP, R4
LDR     R4, =(_GLOBAL_OFFSET_TABLE_ - 0xA46E)
LDR     R6, =(aSystemEtc_dhcp - 0xA472)
ADD     R0, SP
ADD     R4, PC
LDR     R3, [R4,R5]
ADD     R6, PC              ; "/system/etc/.dhcpcd"
MOVS    R1, #0              ; type
LDR     R3, [R3]
STR     R3, [R0]
MOVS    R0, R6              ; name
BLX     access
CMP     R0, #0
BEQ     loc_A4A0
```

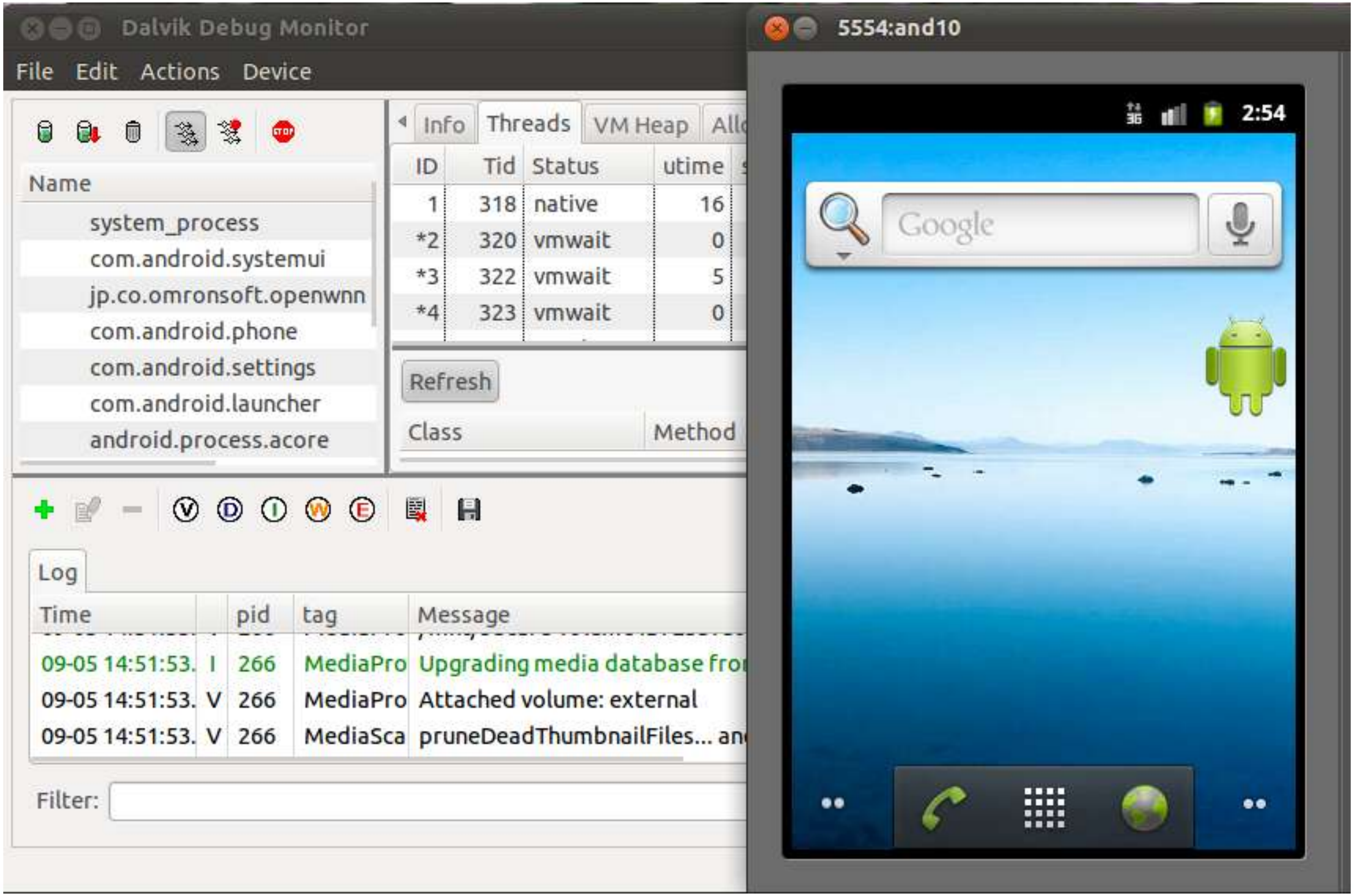
```
100.00% (-102,185) (419,1) 00002466 0000A466: sub_A450+16
AU:  idle   Down      Disk: 218GB
```

Static Analysis: Java Decompilation



```
public static String encrypt(String paramString1, String paramString2)
  throws Exception
{
  Cipher localCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
  byte[] arrayOfByte1 = paramString2.getBytes("UTF-8");
  DESKeySpec localDESKeySpec = new DESKeySpec(arrayOfByte1);
  SecretKey localSecretKey = SecretKeyFactory.getInstance("DES").generateSecret(
  byte[] arrayOfByte2 = paramString2.getBytes("UTF-8");
  IvParameterSpec localIvParameterSpec = new IvParameterSpec(arrayOfByte2);
  localCipher.init(1, localSecretKey, localIvParameterSpec);
  byte[] arrayOfByte3 = paramString1.getBytes("UTF-8");
  return toHexString(localCipher.doFinal(arrayOfByte3));
}

public static String toHexString(byte[] paramArrayOfByte)
{
  StringBuffer localStringBuffer1 = new StringBuffer();
  int i = 0;
  while (true)
  {
    int j = paramArrayOfByte.length;
    if (i >= j)
      return localStringBuffer1.toString();
    String str = Integer.toHexString(paramArrayOfByte[i] & 0xFF);
    if (str.length() < 2)
      str = "0" + str;
```

Dynamic Analysis: SDK Simulator

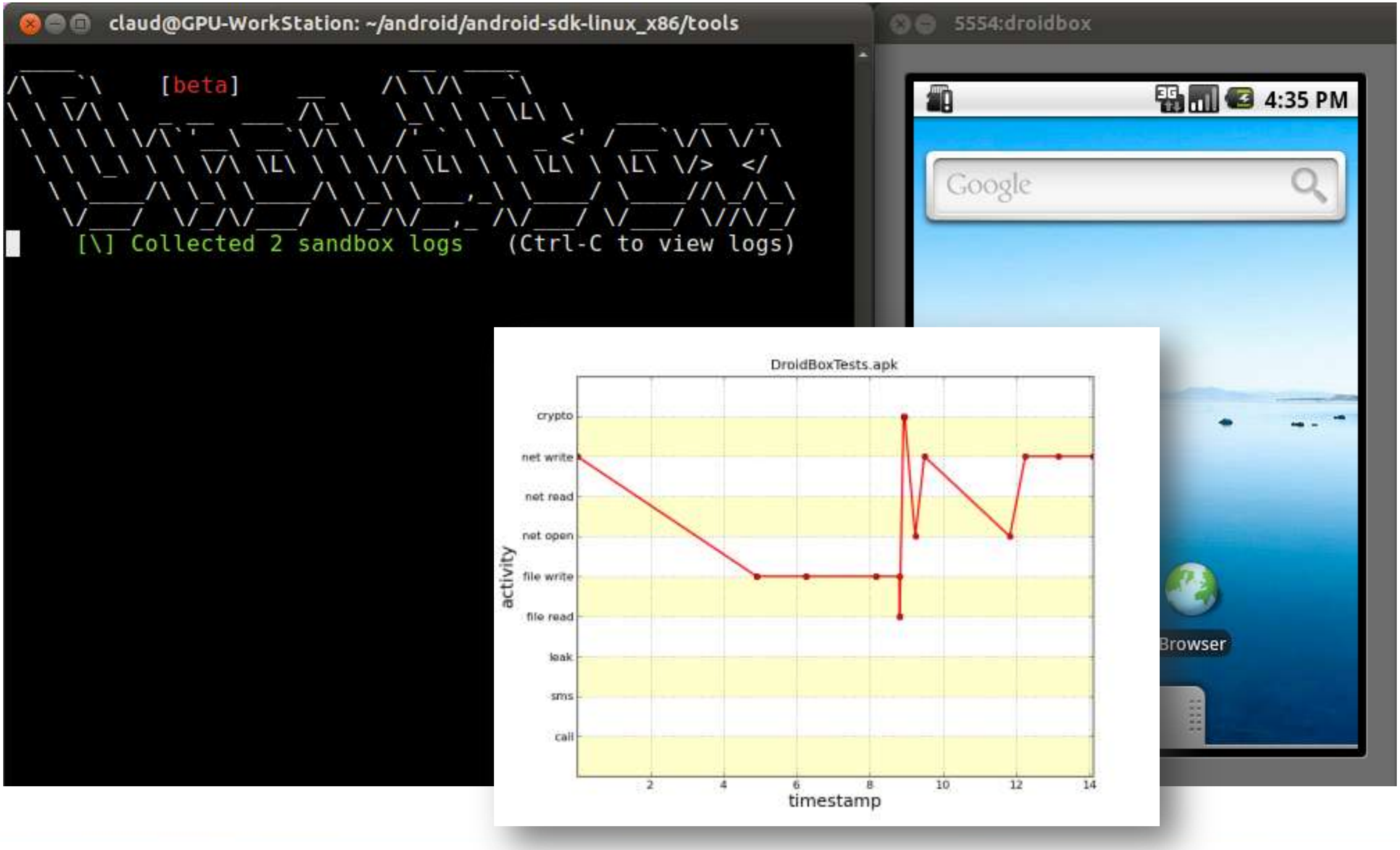


Name
- system_process
- com.android.systemui
- jp.co.omronsoft.openwnn
- com.android.phone
- com.android.settings
- com.android.launcher
- android.process.acore

ID	Tid	Status	utime
1	318	native	16
*2	320	vmwait	0
*3	322	vmwait	5
*4	323	vmwait	0

```
Time              pid  tag       Message
09-05 14:51:53. I  266  MediaPro  Upgrading media database fro
09-05 14:51:53. V  266  MediaPro  Attached volume: external
09-05 14:51:53. V  266  MediaSca  pruneDeadThumbnailFiles... an
```

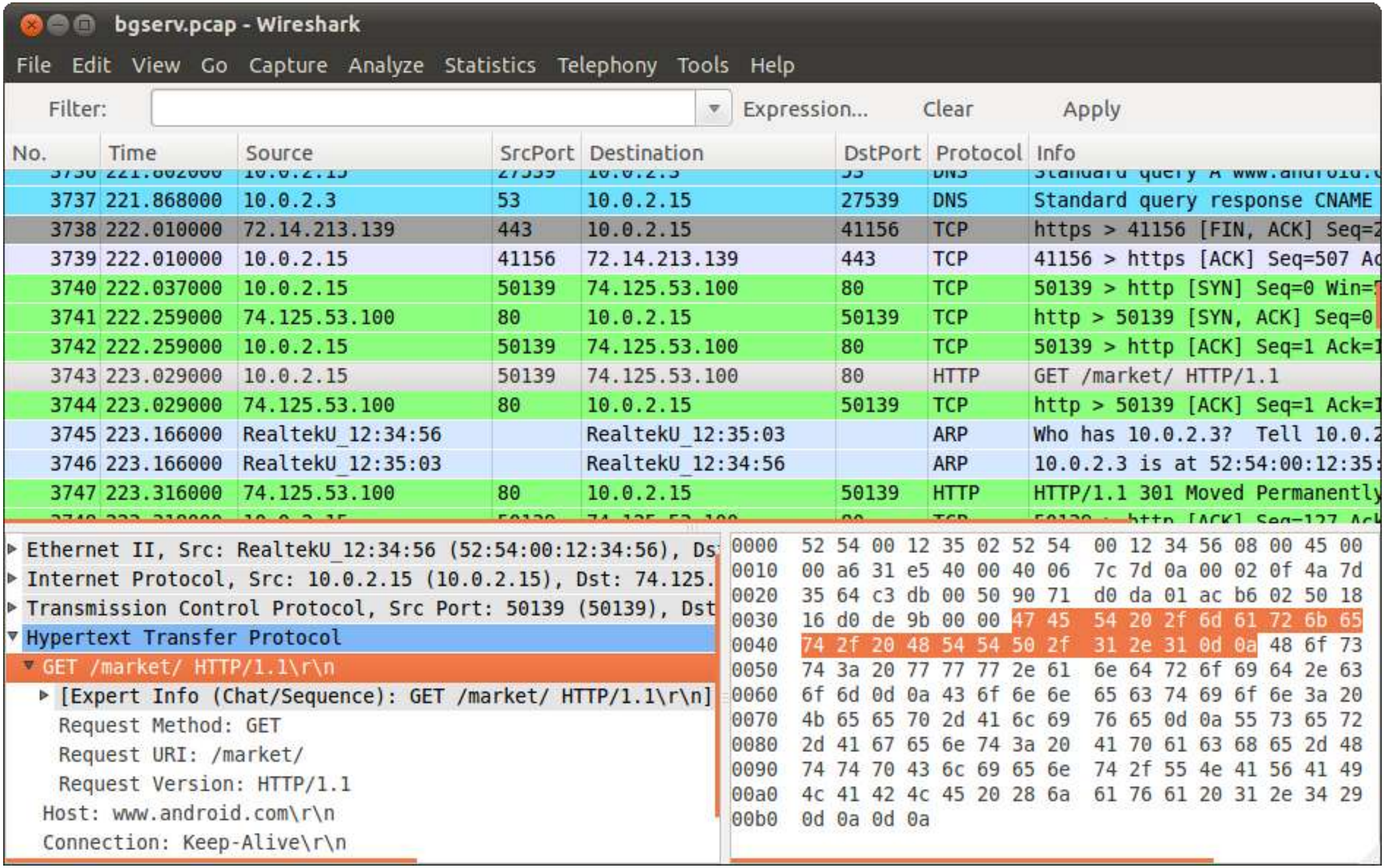
Dynamic Analysis: Behavior Monitor



claud@GPU-WorkStation: ~/android/android-sdk-linux_x86/tools

```
 ____                               __  ____
/\  _`\      [beta]       __       /\ \/\  _`\
\ \ \/\ \  _ __  ___ /\_\      \_\ \ \ \L\ \    ___   __  _
 \ \ \ \ \/\`'__\ __`\/\ \  /'_` \ \  _ <' / __`\/\ \/'\
  \ \ \_\ \ \ \/\ \L\ \ \ \/\ \L\ \ \ \L\ \/\ \L\ \/>  </
   \ \____/\ \_\ \____/\ \_\ \___,_\ \____/\ \____//\_/\_\
    \/___/  \/_/\/___/  \/_/\/__,_ /\/___/  \/___/ \//\/_/
     [\] Collected 2 sandbox logs   (Ctrl-C to view logs)
```

Network Analysis



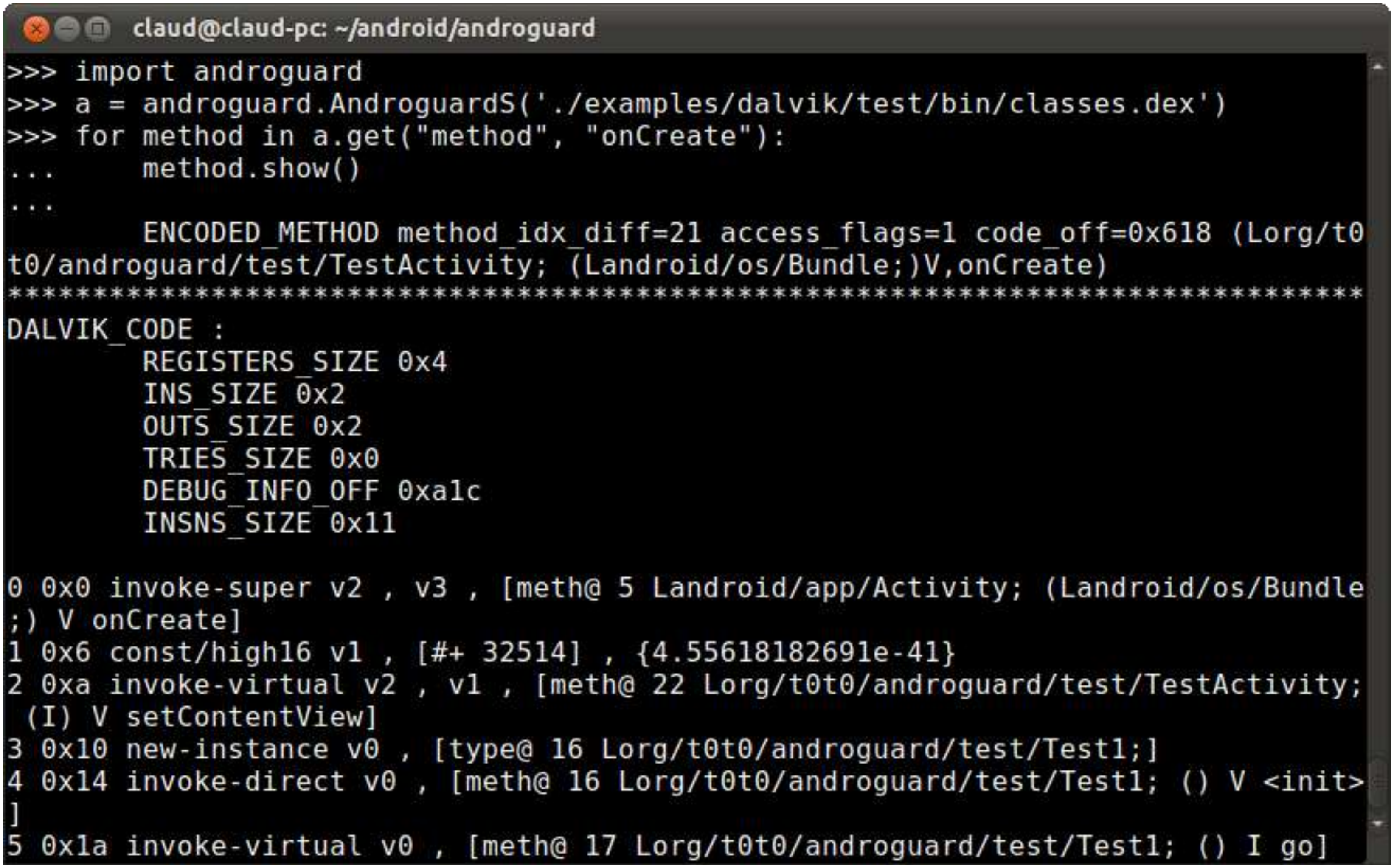
bgserv.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Info
3736	221.862000	10.0.2.15	27539	10.0.2.3	53	DNS	Standard query A www.android.c
3737	221.868000	10.0.2.3	53	10.0.2.15	27539	DNS	Standard query response CNAME
3738	222.010000	72.14.213.139	443	10.0.2.15	41156	TCP	https > 41156 [FIN, ACK] Seq=2
3739	222.010000	10.0.2.15	41156	72.14.213.139	443	TCP	41156 > https [ACK] Seq=507 Ac
3740	222.037000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [SYN] Seq=0 Win=
3741	222.259000	74.125.53.100	80	10.0.2.15	50139	TCP	http > 50139 [SYN, ACK] Seq=0
3742	222.259000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [ACK] Seq=1 Ack=1
3743	223.029000	10.0.2.15	50139	74.125.53.100	80	HTTP	GET /market/ HTTP/1.1
3744	223.029000	74.125.53.100	80	10.0.2.15	50139	TCP	http > 50139 [ACK] Seq=1 Ack=1
3745	223.166000	RealtekU_12:34:56		RealtekU_12:35:03		ARP	Who has 10.0.2.3? Tell 10.0.2
3746	223.166000	RealtekU_12:35:03		RealtekU_12:34:56		ARP	10.0.2.3 is at 52:54:00:12:35:
3747	223.316000	74.125.53.100	80	10.0.2.15	50139	HTTP	HTTP/1.1 301 Moved Permanently
3748	223.318000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [ACK] Seq=127 Ack

```
▶ Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Ds
▶ Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 74.125.
▶ Transmission Control Protocol, Src Port: 50139 (50139), Dst
▼ Hypertext Transfer Protocol
  ▼ GET /market/ HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /market/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /market/
      Request Version: HTTP/1.1
    Host: www.android.com\r\n
    Connection: Keep-Alive\r\n
```

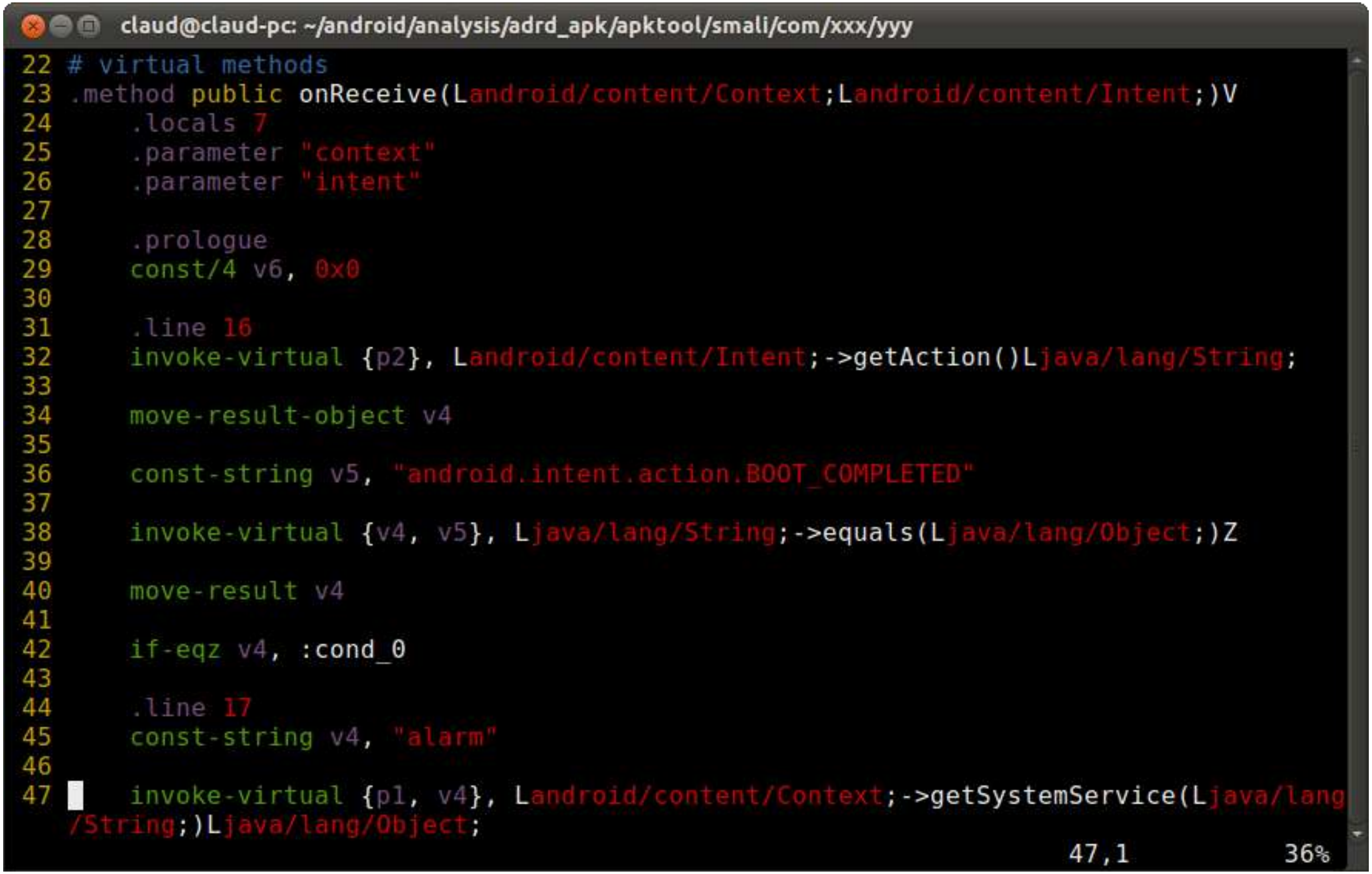
```
0000  52 54 00 12 35 02 52 54  00 12 34 56 08 00 45 00
0010  00 a6 31 e5 40 00 40 06  7c 7d 0a 00 02 0f 4a 7d
0020  35 64 c3 db 00 50 90 71  d0 da 01 ac b6 02 50 18
0030  16 d0 de 9b 00 00 47 45  54 20 2f 6d 61 72 6b 65
0040  74 2f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73
0050  74 3a 20 77 77 77 2e 61  6e 64 72 6f 69 64 2e 63
0060  6f 6d 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20
0070  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 55 73 65 72
0080  2d 41 67 65 6e 74 3a 20  41 70 61 63 68 65 2d 48
0090  74 74 70 43 6c 69 65 6e  74 2f 55 4e 41 56 41 49
00a0  4c 41 42 4c 45 20 28 6a  61 76 61 20 31 2e 34 29
00b0  0d 0a 0d 0a
```

Automatic Analysis



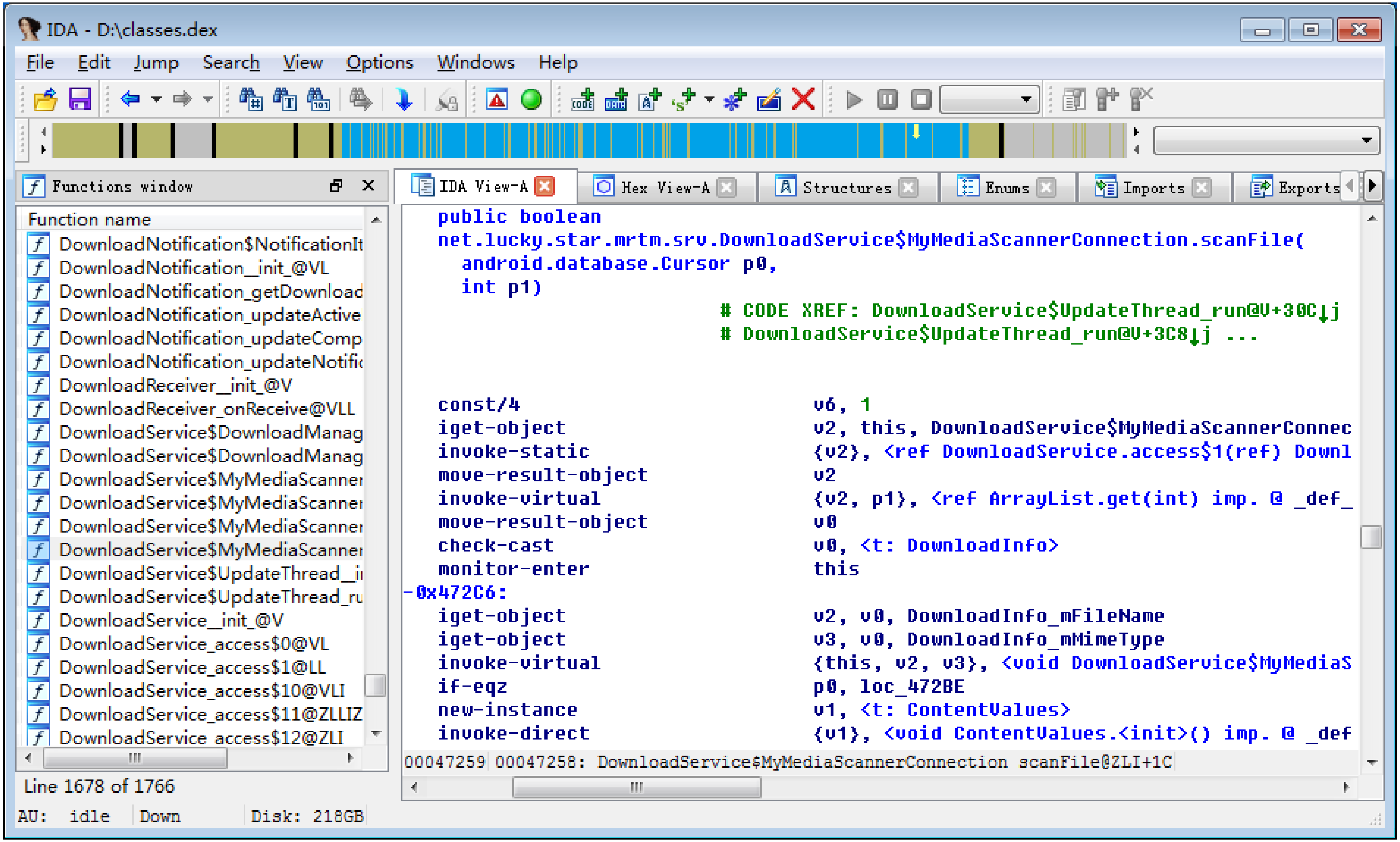
```
>>> import androguard
>>> a = androguard.AndroguardS('./examples/dalvik/test/bin/classes.dex')
>>> for method in a.get("method", "onCreate"):
...     method.show()
...
        ENCODED_METHOD method_idx_diff=21 access_flags=1 code_off=0x618 (Lorg/t0
t0/androguard/test/TestActivity; (Landroid/os/Bundle;)V,onCreate)
********************************************************************************
DALVIK_CODE :
        REGISTERS_SIZE 0x4
        INS_SIZE 0x2
        OUTS_SIZE 0x2
        TRIES_SIZE 0x0
        DEBUG_INFO_OFF 0xa1c
        INSNS_SIZE 0x11

0 0x0 invoke-super v2 , v3 , [meth@ 5 Landroid/app/Activity; (Landroid/os/Bundle
;) V onCreate]
1 0x6 const/high16 v1 , [#+ 32514] , {4.55618182691e-41}
2 0xa invoke-virtual v2 , v1 , [meth@ 22 Lorg/t0t0/androguard/test/TestActivity;
 (I) V setContentView]
3 0x10 new-instance v0 , [type@ 16 Lorg/t0t0/androguard/test/Test1;]
4 0x14 invoke-direct v0 , [meth@ 16 Lorg/t0t0/androguard/test/Test1; () V <init>
]
5 0x1a invoke-virtual v0 , [meth@ 17 Lorg/t0t0/androguard/test/Test1; () I go]
```

Disassembling Dalvik Code


claud@claud-pc: ~/android/analysis/adrd_apk/apktool/smali/com/xxx/yyy

```
# virtual methods
.method public onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 7
    .parameter "context"
    .parameter "intent"

    .prologue
    const/4 v6, 0x0

    .line 16
    invoke-virtual {p2}, Landroid/content/Intent;->getAction()Ljava/lang/String;

    move-result-object v4

    const-string v5, "android.intent.action.BOOT_COMPLETED"

    invoke-virtual {v4, v5}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result v4

    if-eqz v4, :cond_0

    .line 17
    const-string v4, "alarm"

    invoke-virtual {p1, v4}, Landroid/content/Context;->getSystemService(Ljava/lang/String;)Ljava/lang/Object;
                                                                          47,1          36%
```

Disassembling Dalvik Code



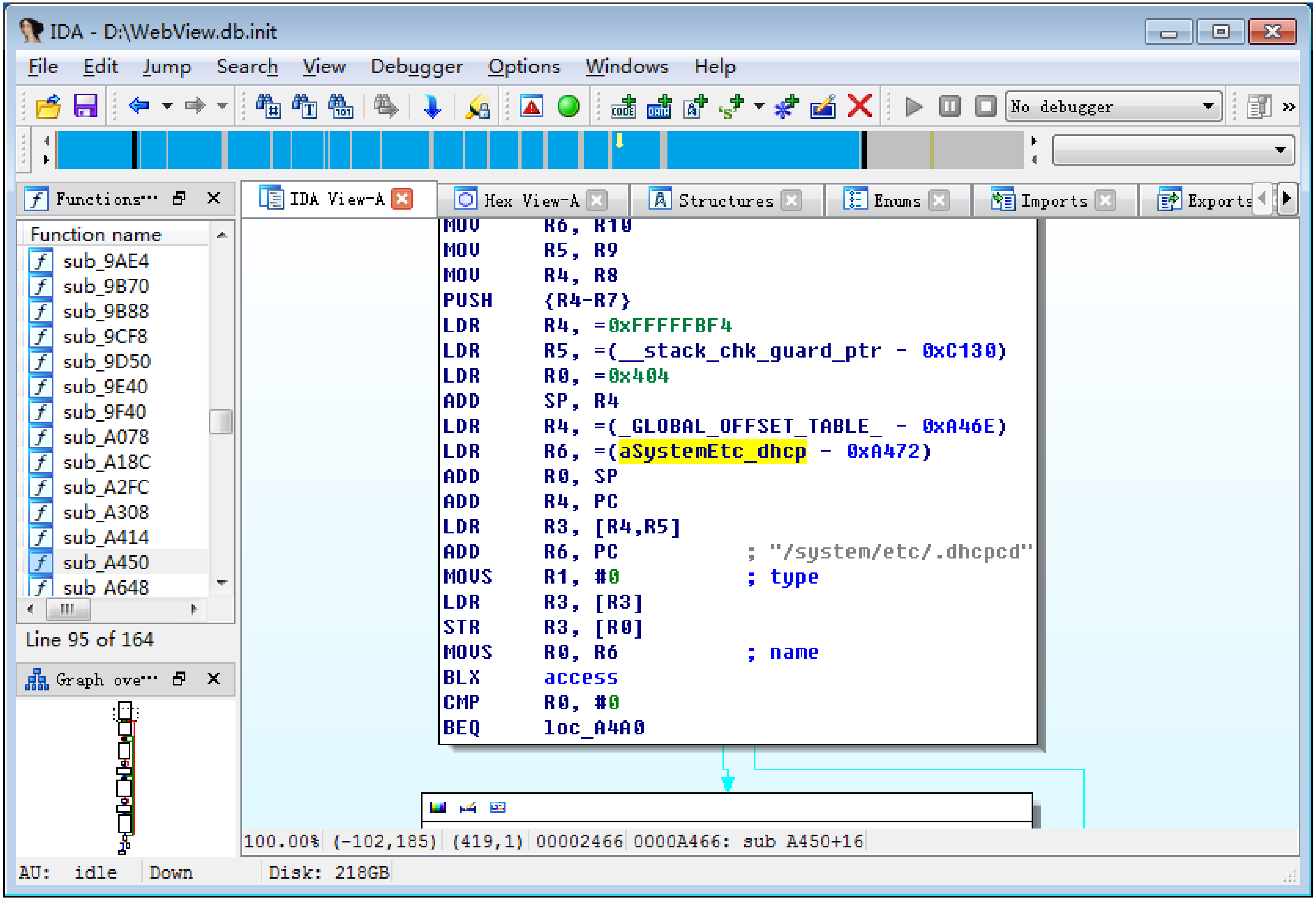
```
DownloadNotification$NotificationIt
DownloadNotification__init_@VL
DownloadNotification_getDownload
DownloadNotification_updateActive
DownloadNotification_updateComp
DownloadNotification_updateNotifi
DownloadReceiver__init_@V
DownloadReceiver_onReceive@VLL
DownloadService$DownloadManag
DownloadService$DownloadManag
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$UpdateThread__i
DownloadService$UpdateThread_ru
DownloadService__init_@V
DownloadService_access$0@VL
DownloadService_access$1@LL
DownloadService_access$10@VLI
DownloadService_access$11@ZLLIZ
DownloadService_access$12@ZLI
```

```
  public boolean
  net.lucky.star.mrtm.srv.DownloadService$MyMediaScannerConnection.scanFile(
    android.database.Cursor p0,
    int p1)
                                   # CODE XREF: DownloadService$UpdateThread_run@V+30C↓j
                                   # DownloadService$UpdateThread_run@V+3C8↓j ...


  const/4                         v6, 1
  iget-object                     v2, this, DownloadService$MyMediaScannerConnec
  invoke-static                   {v2}, <ref DownloadService.access$1(ref) Downl
  move-result-object              v2
  invoke-virtual                  {v2, p1}, <ref ArrayList.get(int) imp. @ _def_
  move-result-object              v0
  check-cast                      v0, <t: DownloadInfo>
  monitor-enter                   this
-0x472C6:
  iget-object                     v2, v0, DownloadInfo_mFileName
  iget-object                     v3, v0, DownloadInfo_mMimeType
  invoke-virtual                  {this, v2, v3}, <void DownloadService$MyMediaS
  if-eqz                          p0, loc_472BE
  new-instance                    v1, <t: ContentValues>
  invoke-direct                   {v1}, <void ContentValues.<init>() imp. @ _def
00047259 00047258: DownloadService$MyMediaScannerConnection scanFile@ZLI+1C
```

Line 1678 of 1766

AU: idle   Down   Disk: 218GB

Disassembling ARM Code



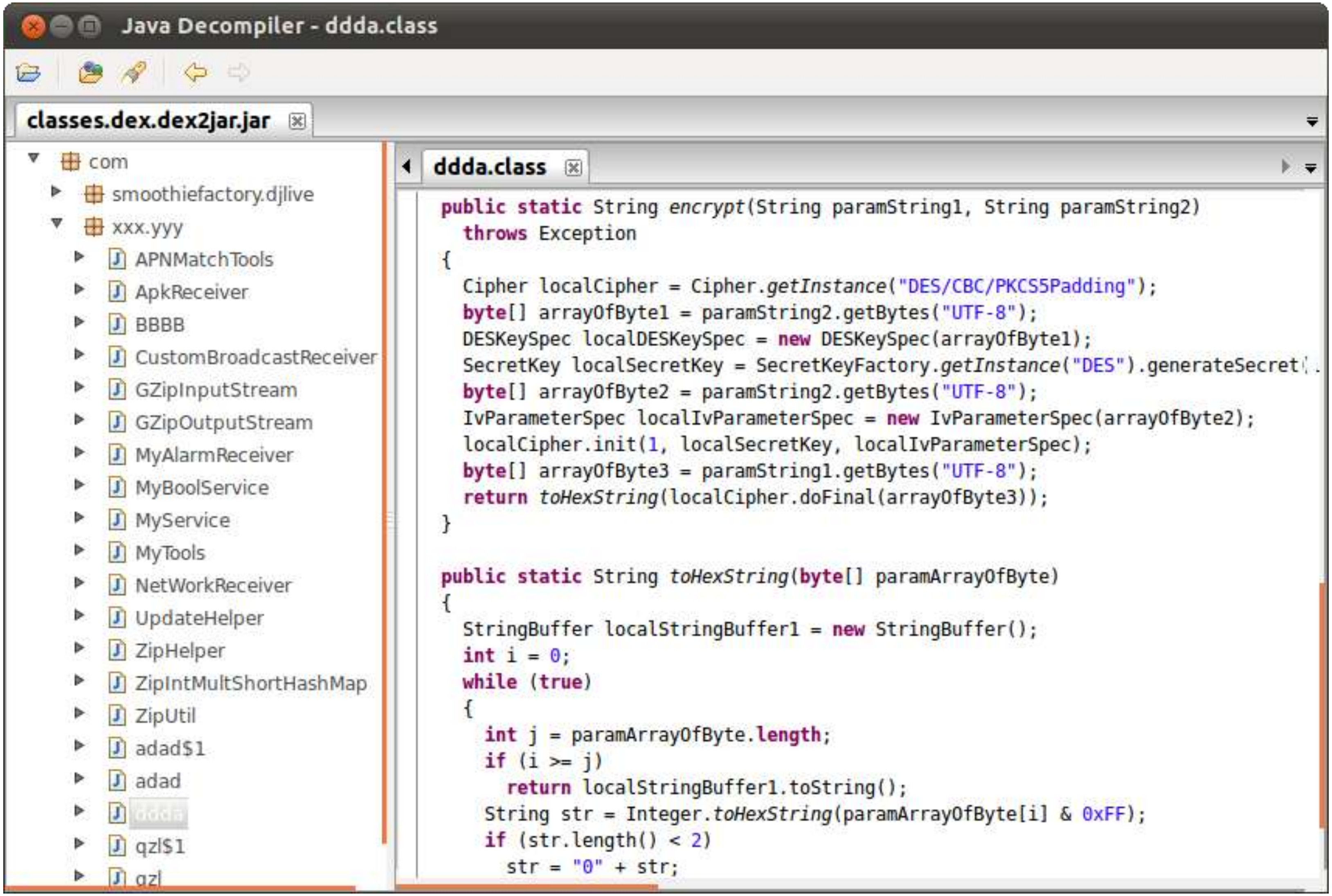
Function name
- sub_9AE4
- sub_9B70
- sub_9B88
- sub_9CF8
- sub_9D50
- sub_9E40
- sub_9F40
- sub_A078
- sub_A18C
- sub_A2FC
- sub_A308
- sub_A414
- sub_A450
- sub_A648

Line 95 of 164

```
MOV     R6, R10
MOV     R5, R9
MOV     R4, R8
PUSH    {R4-R7}
LDR     R4, =0xFFFFFBF4
LDR     R5, =(__stack_chk_guard_ptr - 0xC130)
LDR     R0, =0x404
ADD     SP, R4
LDR     R4, =(_GLOBAL_OFFSET_TABLE_ - 0xA46E)
LDR     R6, =(aSystemEtc_dhcp - 0xA472)
ADD     R0, SP
ADD     R4, PC
LDR     R3, [R4,R5]
ADD     R6, PC              ; "/system/etc/.dhcpcd"
MOVS    R1, #0              ; type
LDR     R3, [R3]
STR     R3, [R0]
MOVS    R0, R6              ; name
BLX     access
CMP     R0, #0
BEQ     loc_A4A0
```

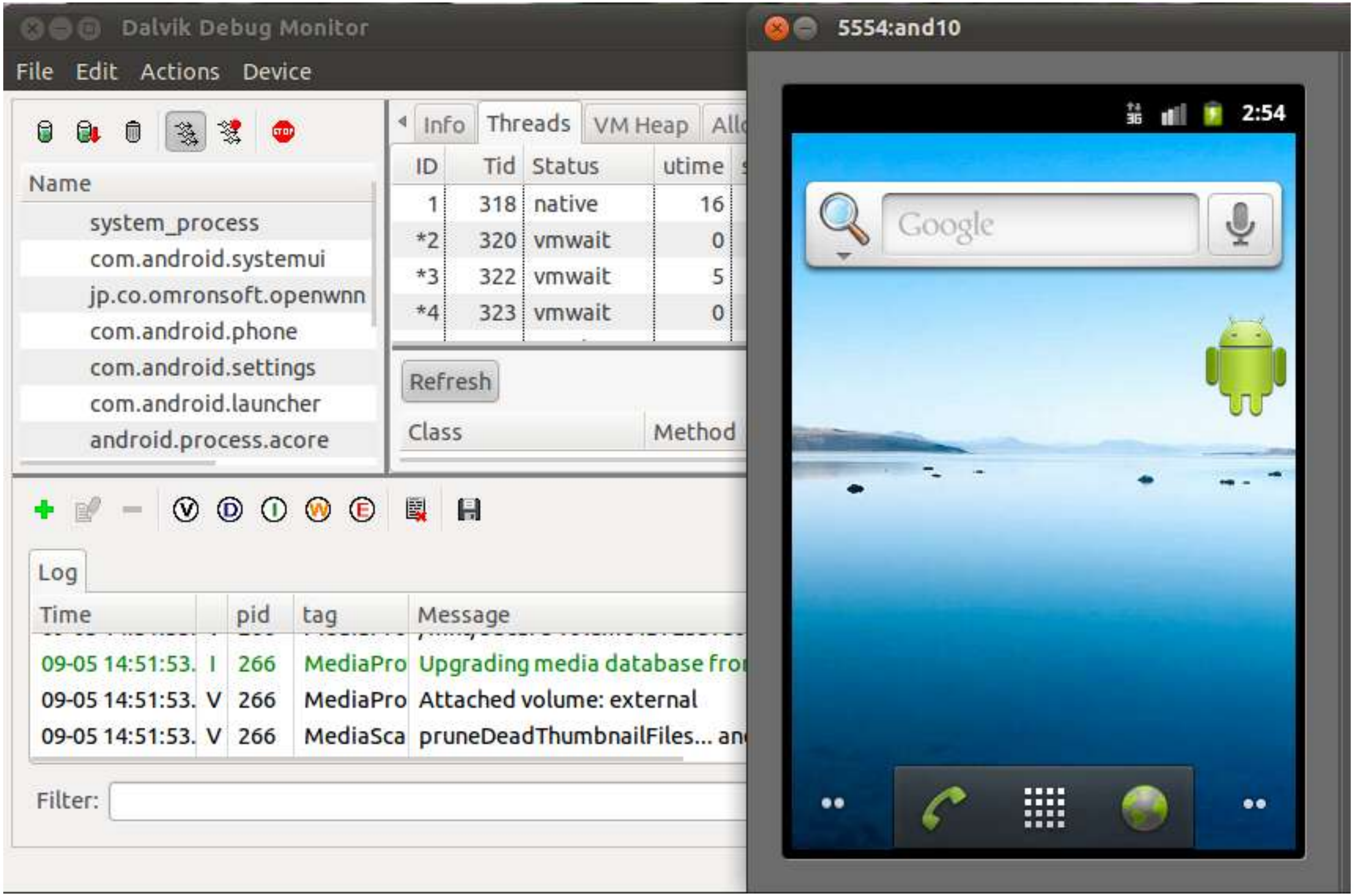
```
100.00% (-102,185) (419,1) 00002466 0000A466: sub_A450+16
AU:  idle   Down      Disk: 218GB
```

Decompilation as Java



```java
public static String encrypt(String paramString1, String paramString2)
  throws Exception
{
  Cipher localCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
  byte[] arrayOfByte1 = paramString2.getBytes("UTF-8");
  DESKeySpec localDESKeySpec = new DESKeySpec(arrayOfByte1);
  SecretKey localSecretKey = SecretKeyFactory.getInstance("DES").generateSecret(.
  byte[] arrayOfByte2 = paramString2.getBytes("UTF-8");
  IvParameterSpec localIvParameterSpec = new IvParameterSpec(arrayOfByte2);
  localCipher.init(1, localSecretKey, localIvParameterSpec);
  byte[] arrayOfByte3 = paramString1.getBytes("UTF-8");
  return toHexString(localCipher.doFinal(arrayOfByte3));
}

public static String toHexString(byte[] paramArrayOfByte)
{
  StringBuffer localStringBuffer1 = new StringBuffer();
  int i = 0;
  while (true)
  {
    int j = paramArrayOfByte.length;
    if (i >= j)
      return localStringBuffer1.toString();
    String str = Integer.toHexString(paramArrayOfByte[i] & 0xFF);
    if (str.length() < 2)
      str = "0" + str;
```

System Simulation

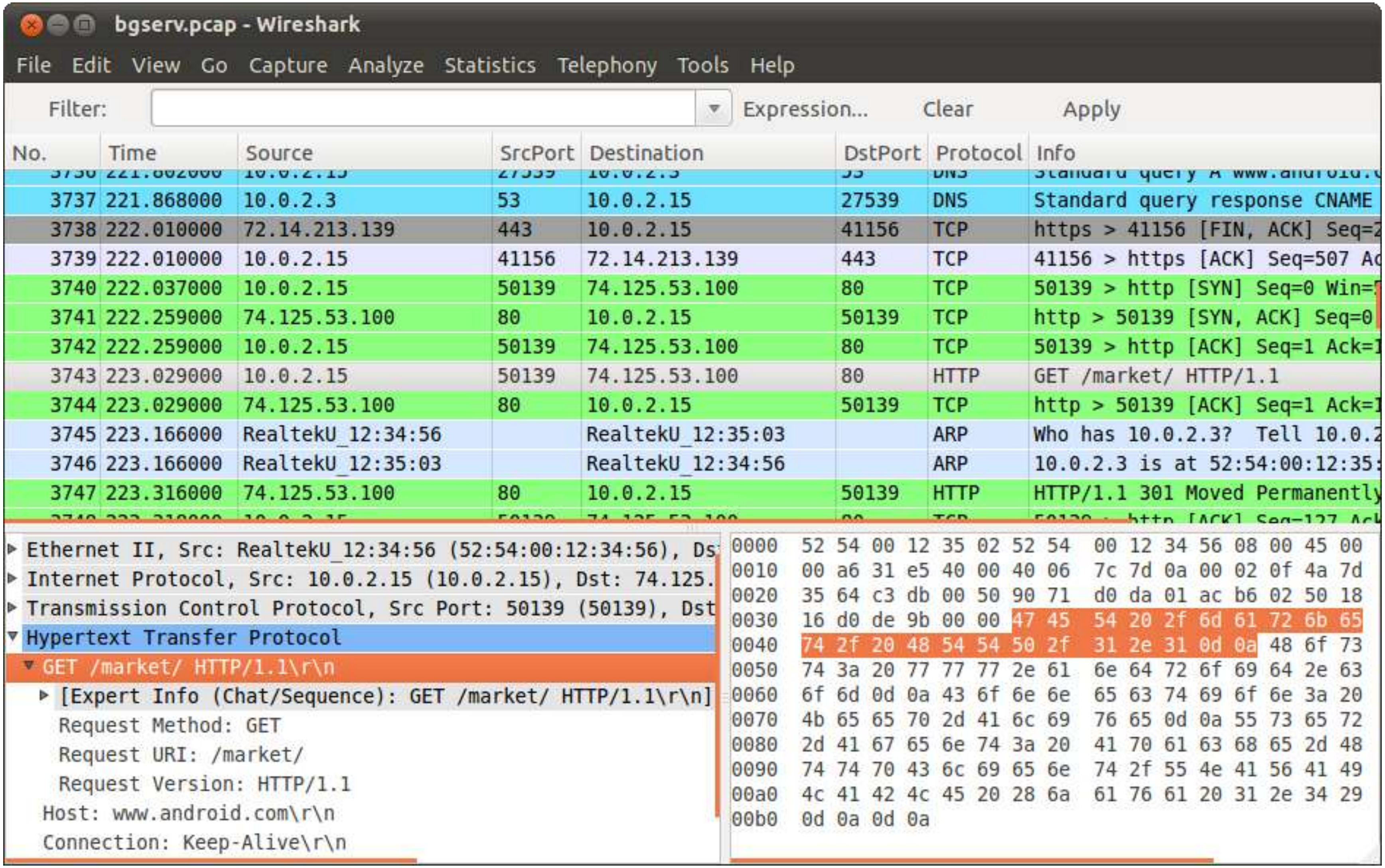


Name
system_process
com.android.systemui
jp.co.omronsoft.openwnn
com.android.phone
com.android.settings
com.android.launcher
android.process.acore

ID	Tid	Status	utime
1	318	native	16
*2	320	vmwait	0
*3	322	vmwait	5
*4	323	vmwait	0

```
Time             pid  tag       Message
09-05 14:51:53. I 266  MediaPro  Upgrading media database fro
09-05 14:51:53. V 266  MediaPro  Attached volume: external
09-05 14:51:53. V 266  MediaSca  pruneDeadThumbnailFiles... an
```

Network Data Analysis

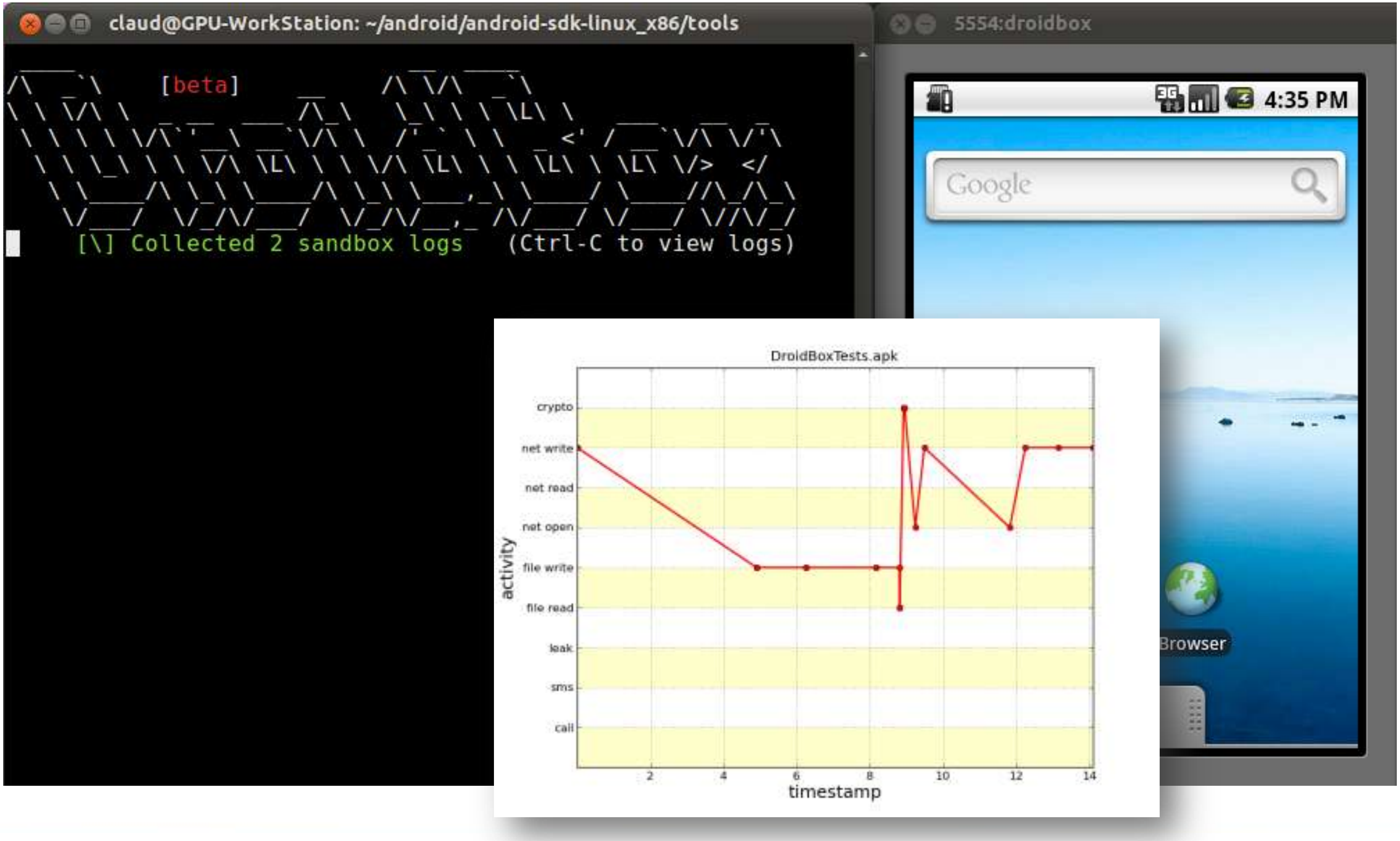


No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Info
3736	221.862000	10.0.2.15	27539	10.0.2.3	53	DNS	Standard query A www.android.c
3737	221.868000	10.0.2.3	53	10.0.2.15	27539	DNS	Standard query response CNAME
3738	222.010000	72.14.213.139	443	10.0.2.15	41156	TCP	https > 41156 [FIN, ACK] Seq=2
3739	222.010000	10.0.2.15	41156	72.14.213.139	443	TCP	41156 > https [ACK] Seq=507 Ac
3740	222.037000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [SYN] Seq=0 Win=
3741	222.259000	74.125.53.100	80	10.0.2.15	50139	TCP	http > 50139 [SYN, ACK] Seq=0
3742	222.259000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [ACK] Seq=1 Ack=1
3743	223.029000	10.0.2.15	50139	74.125.53.100	80	HTTP	GET /market/ HTTP/1.1
3744	223.029000	74.125.53.100	80	10.0.2.15	50139	TCP	http > 50139 [ACK] Seq=1 Ack=1
3745	223.166000	RealtekU_12:34:56		RealtekU_12:35:03		ARP	Who has 10.0.2.3? Tell 10.0.2
3746	223.166000	RealtekU_12:35:03		RealtekU_12:34:56		ARP	10.0.2.3 is at 52:54:00:12:35:
3747	223.316000	74.125.53.100	80	10.0.2.15	50139	HTTP	HTTP/1.1 301 Moved Permently
3748	223.316000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [ACK] Seq=127 Ack

```
▸ Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Ds
▸ Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 74.125.
▸ Transmission Control Protocol, Src Port: 50139 (50139), Dst
▾ Hypertext Transfer Protocol
  ▾ GET /market/ HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /market/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /market/
      Request Version: HTTP/1.1
    Host: www.android.com\r\n
    Connection: Keep-Alive\r\n
```

```
0000  52 54 00 12 35 02 52 54  00 12 34 56 08 00 45 00
0010  00 a6 31 e5 40 00 40 06  7c 7d 0a 00 02 0f 4a 7d
0020  35 64 c3 db 00 50 90 71  d0 da 01 ac b6 02 50 18
0030  16 d0 de 9b 00 00 47 45  54 20 2f 6d 61 72 6b 65
0040  74 2f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73
0050  74 3a 20 77 77 77 2e 61  6e 64 72 6f 69 64 2e 63
0060  6f 6d 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20
0070  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 55 73 65 72
0080  2d 41 67 65 6e 74 3a 20  41 70 61 63 68 65 2d 48
0090  74 74 70 43 6c 69 65 6e  74 2f 55 4e 41 56 41 49
00a0  4c 41 42 4c 45 20 28 6a  61 76 61 20 31 2e 34 29
00b0  0d 0a 0d 0a
```

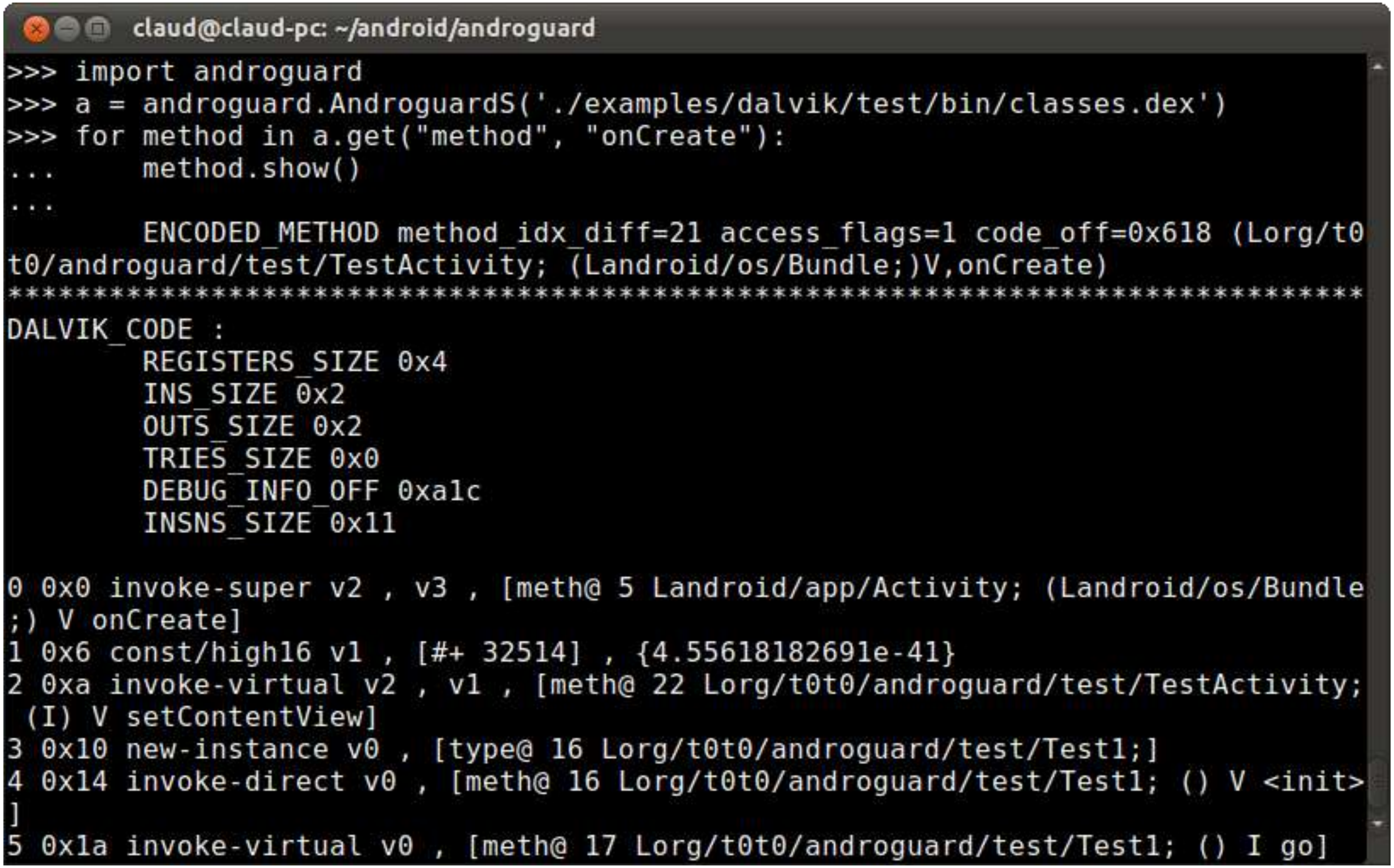
Dynamic Behavior Monitor



claud@GPU-WorkStation: ~/android/android-sdk-linux_x86/tools

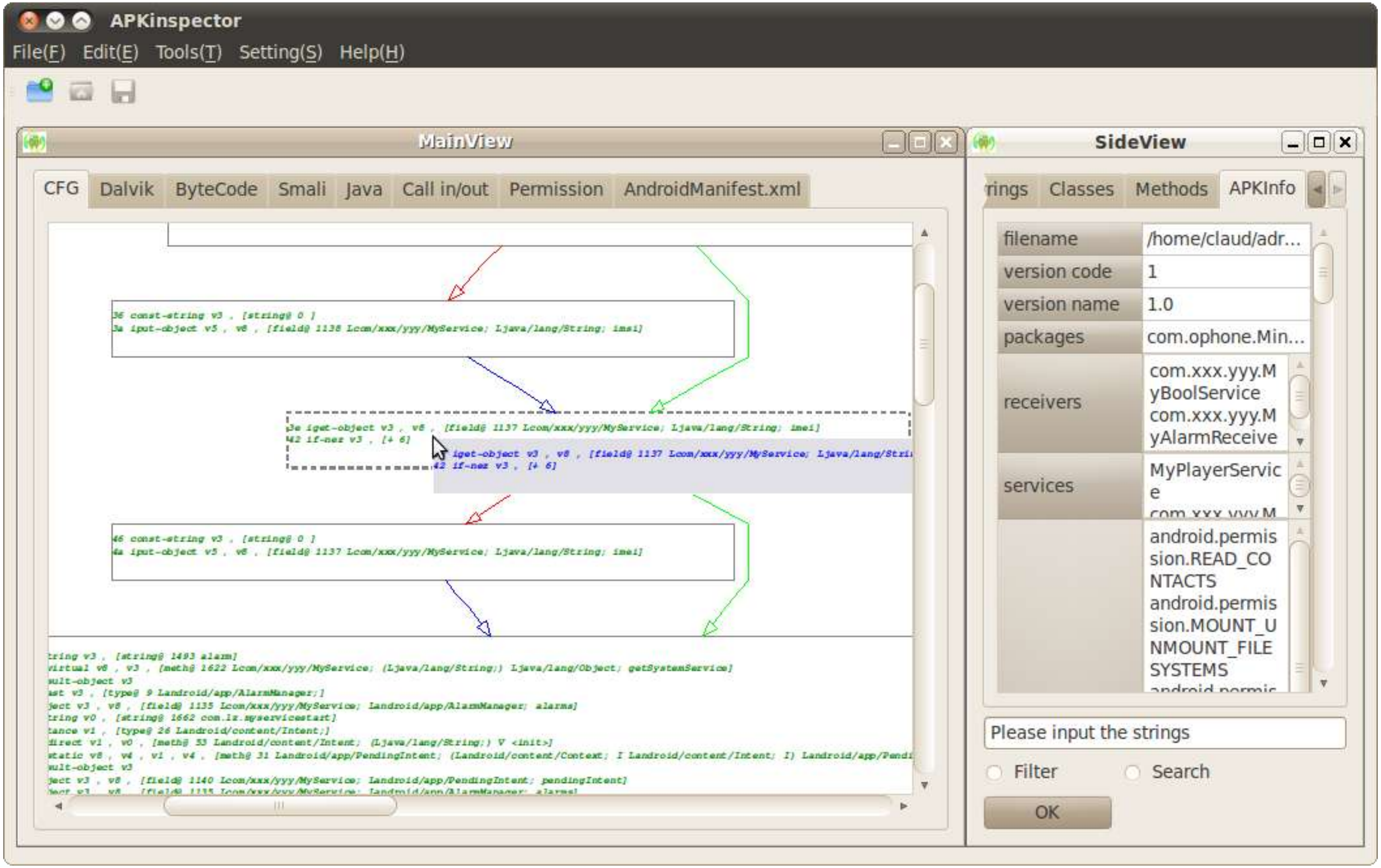
```
 ____                               __  ____
/\  _`\     [beta]       __        /\ \/\  _`\
\ \ \/\ \  _ __  ___ /\_\      \_\ \ \ \L\ \   ___   __  _
 \ \ \ \ \/\`'__\ __`\/\ \  /'_` \ \  _ <' / __`\/\ \/'\
  \ \ \_\ \ \ \/\ \L\ \ \ \/\ \L\ \ \ \L\ \/\ \L\ \/>  </
   \ \____/\ \_\ \____/\ \_\ \___,_\ \____/\ \____//\_/\_\
    \/___/  \/_/\/___/  \/_/\/__,_ /\/___/  \/___/ \//\/_/
     [\] Collected 2 sandbox logs   (Ctrl-C to view logs)
```

Automatic Comprehensive Analysis



```
>>> import androguard
>>> a = androguard.AndroguardS('./examples/dalvik/test/bin/classes.dex')
>>> for method in a.get("method", "onCreate"):
...     method.show()
...
        ENCODED_METHOD method_idx_diff=21 access_flags=1 code_off=0x618 (Lorg/t0
t0/androguard/test/TestActivity; (Landroid/os/Bundle;)V,onCreate)
********************************************************************************
DALVIK_CODE :
        REGISTERS_SIZE 0x4
        INS_SIZE 0x2
        OUTS_SIZE 0x2
        TRIES_SIZE 0x0
        DEBUG_INFO_OFF 0xa1c
        INSNS_SIZE 0x11

0 0x0 invoke-super v2 , v3 , [meth@ 5 Landroid/app/Activity; (Landroid/os/Bundle
;) V onCreate]
1 0x6 const/high16 v1 , [#+ 32514] , {4.55618182691e-41}
2 0xa invoke-virtual v2 , v1 , [meth@ 22 Lorg/t0t0/androguard/test/TestActivity;
 (I) V setContentView]
3 0x10 new-instance v0 , [type@ 16 Lorg/t0t0/androguard/test/Test1;]
4 0x14 invoke-direct v0 , [meth@ 16 Lorg/t0t0/androguard/test/Test1; () V <init>
]
5 0x1a invoke-virtual v0 , [meth@ 17 Lorg/t0t0/androguard/test/Test1; () I go]
```

Visualized Comprehensive Analysis



```
36 const-string v3 , [string@ 0 ]
3a iput-object v5 , v8 , [field@ 1138 Lcom/xxx/yyy/MyService; Ljava/lang/String; imsi]
```

```
3e iget-object v3 , v8 , [field@ 1137 Lcom/xxx/yyy/MyService; Ljava/lang/String; imei]
42 if-nez v3 , [+ 6]
```

```
 iget-object v3 , v8 , [field@ 1137 Lcom/xxx/yyy/MyService; Ljava/lang/Stri
42 if-nez v3 , [+ 6]
```

```
46 const-string v3 , [string@ 0 ]
4a iput-object v5 , v8 , [field@ 1137 Lcom/xxx/yyy/MyService; Ljava/lang/String; imei]
```

```
tring v3 , [string@ 1493 alarm]
virtual v8 , v3 , [meth@ 1622 Lcom/xxx/yyy/MyService; (Ljava/lang/String;) Ljava/lang/Object; getSystemService]
sult-object v3
ast v3 , [type@ 9 Landroid/app/AlarmManager;]
ject v3 , v8 , [field@ 1135 Lcom/xxx/yyy/MyService; Landroid/app/AlarmManager; alarms]
tring v0 , [string@ 1662 com.lz.myservicestart]
tance v1 , [type@ 26 Landroid/content/Intent;]
direct v1 , v0 , [meth@ 53 Landroid/content/Intent; (Ljava/lang/String;) V <init>]
static v8 , v4 , v1 , v4 , [meth@ 31 Landroid/app/PendingIntent; (Landroid/content/Context; I Landroid/content/Intent; I) Landroid/app/Pendi
sult-object v3
ject v3 , v8 , [field@ 1140 Lcom/xxx/yyy/MyService; Landroid/app/PendingIntent; pendingIntent]
ject v3 , v8 , [field@ 1135 Lcom/xxx/yyy/MyService; Landroid/app/AlarmManager; alarms]
```

filename	/home/claud/adr...
version code	1
version name	1.0
packages	com.ophone.Min...
receivers	com.xxx.yyy.MyBoolService com.xxx.yyy.MyAlarmReceive
services	MyPlayerService com.xxx.yyy.M
	android.permission.READ_CONTACTS android.permission.MOUNT_UNMOUNT_FILESYSTEMS android.permis

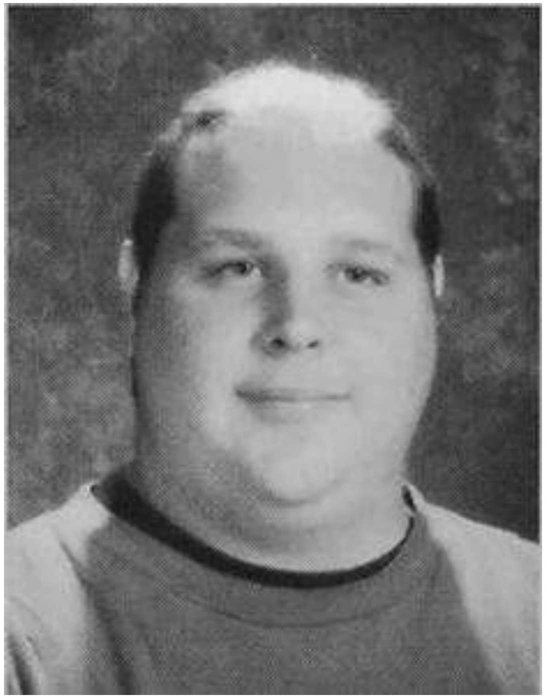
Please input the strings

○ Filter ○ Search

ANALYSIS:
THE HISTORY OF CONFRONTATION

Those Forgotten Grey Faces ？

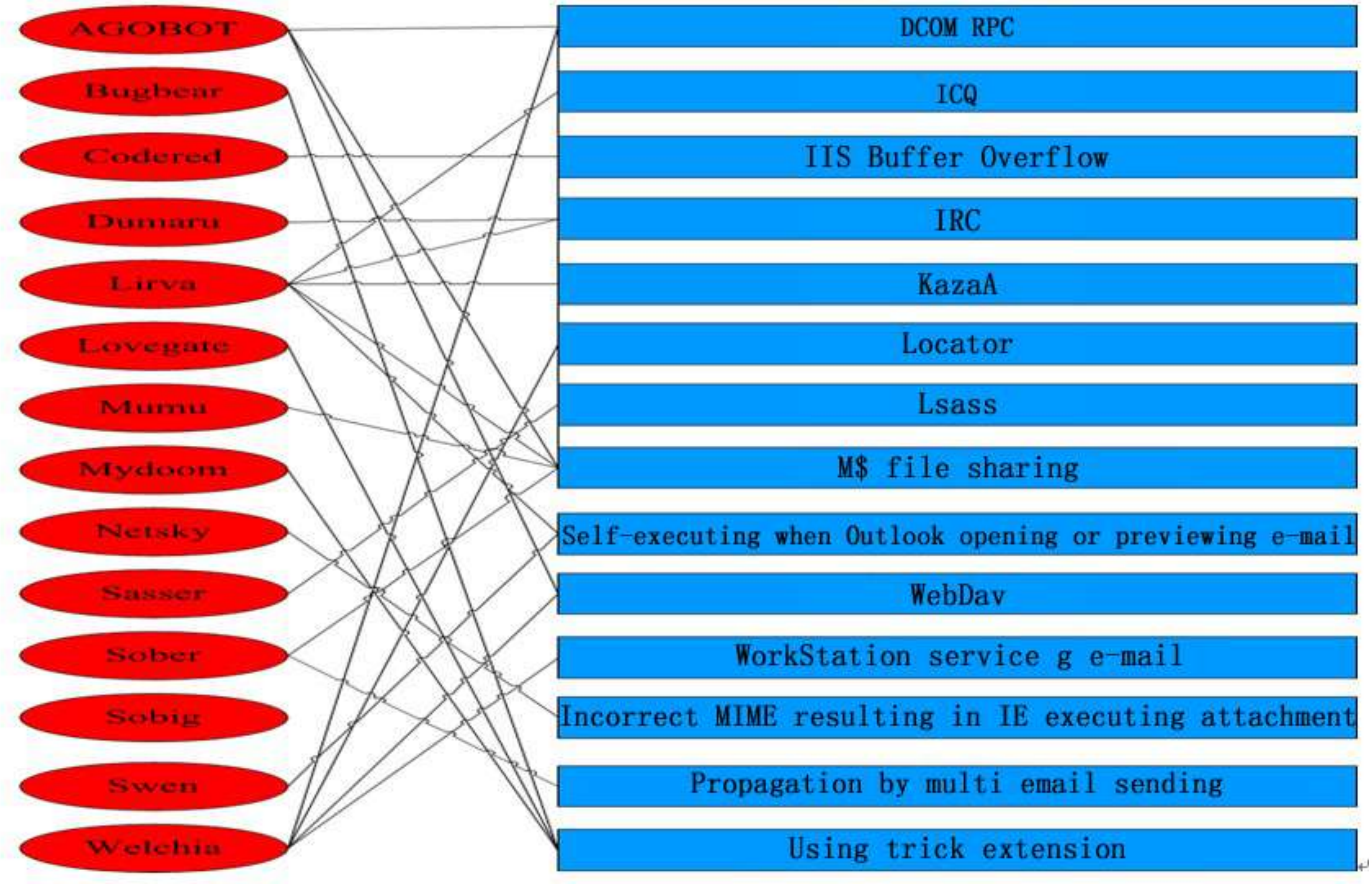
CIH
1998



Melisa
1999

Sasser
2004

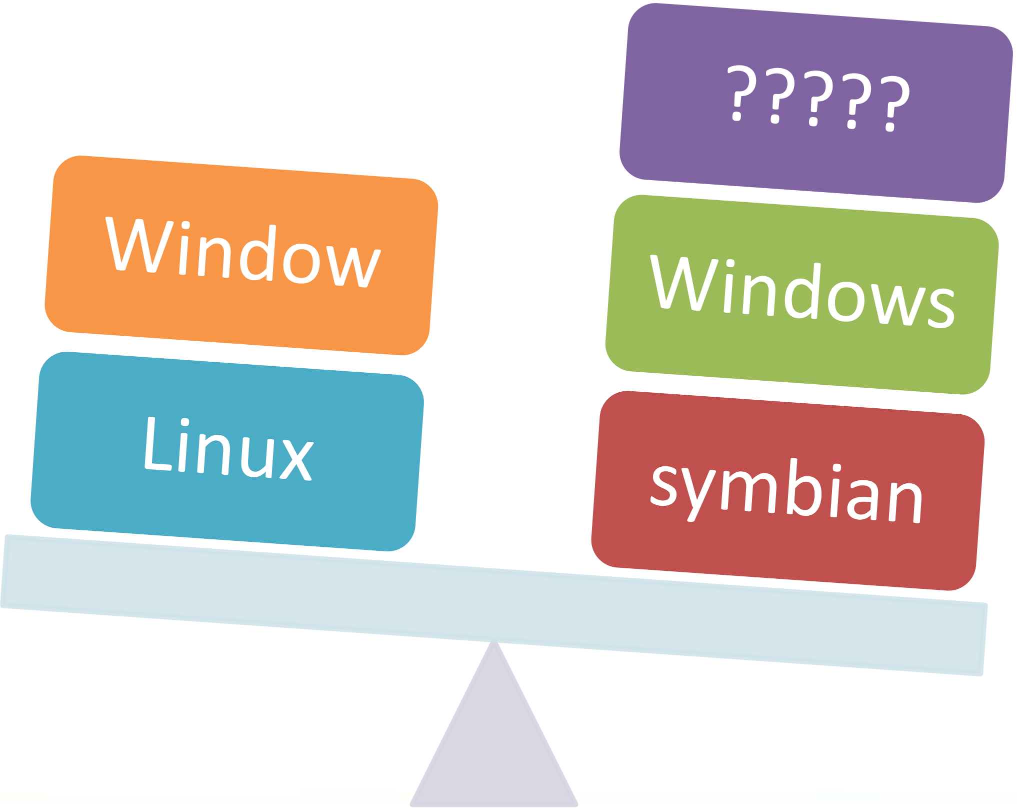
Those Forgotten Red Alert ？



A Cross-Platform Contrast

2001

2010



?????

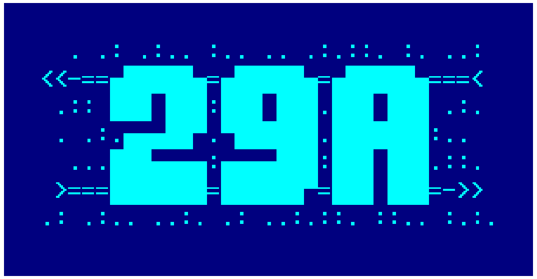
Window

Windows

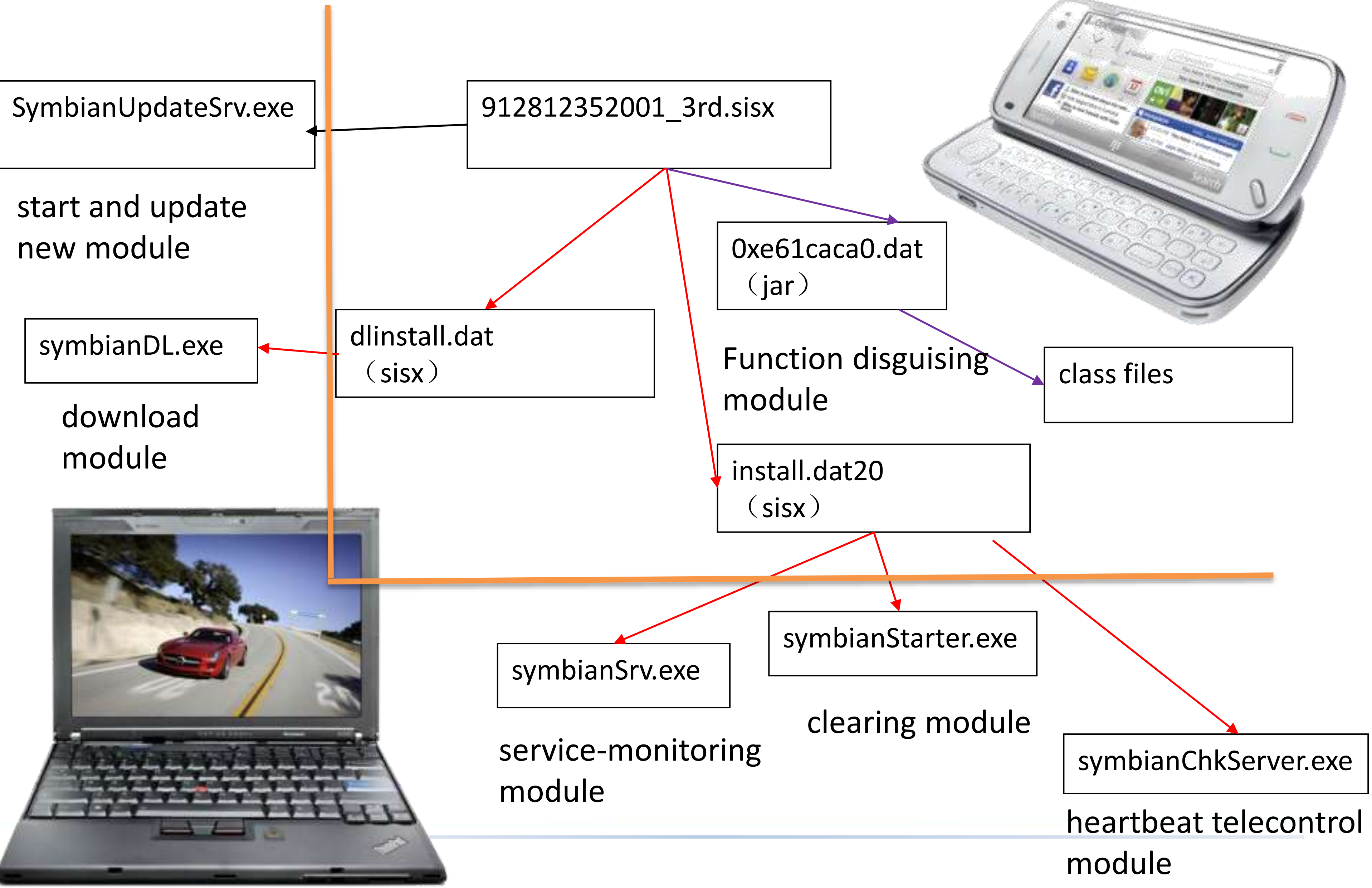
Linux

symbian

Winux (2001)



Cross Platform-Mobile + PC Bimorphism



912812352001_3rd.sisx

SymbianUpdateSrv.exe

start and update new module

dlinstall.dat（sisx）

symbianDL.exe

download module

0xe61caca0.dat（jar）

Function disguising module

class files

install.dat20（sisx）

symbianSrv.exe

service-monitoring module

symbianStarter.exe

clearing module

symbianChkServer.exe

heartbeat telecontrol module

The Confrontation History Since 1988

Normalized Confrontation

Systematical Confrontation

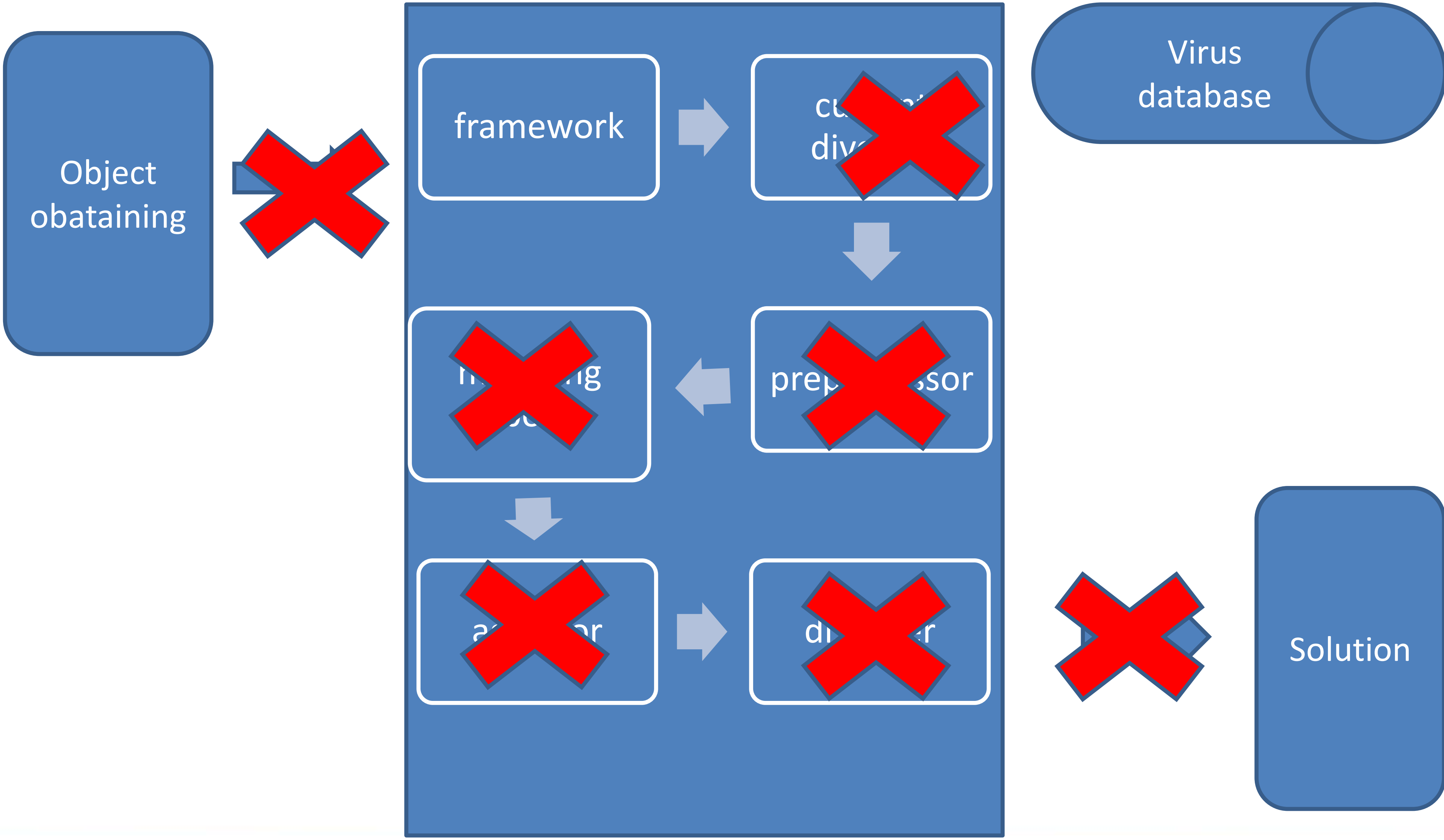
Industrial Confrontation

Notable Event and Typical Method of Normalized Confrontation

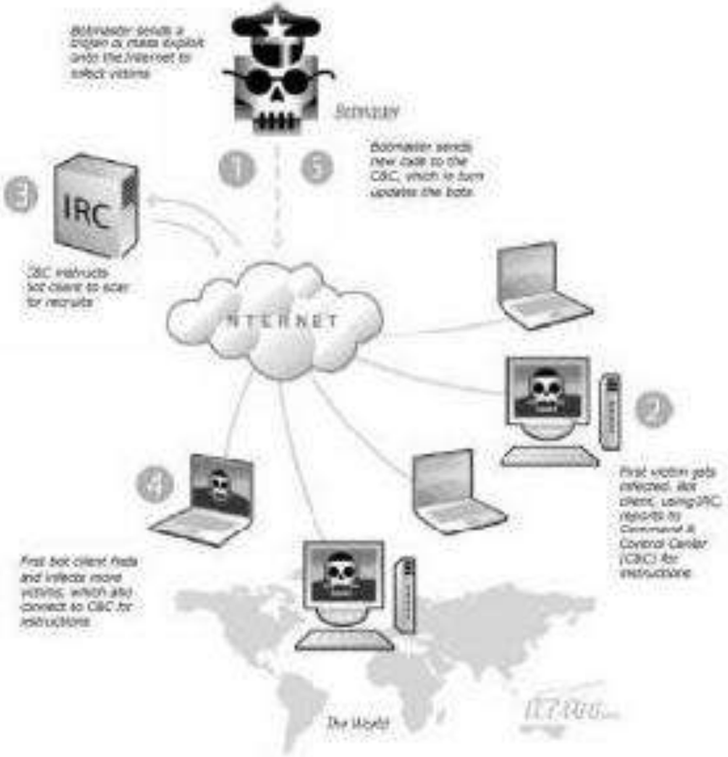
- Bouncing Ball Virus
- Encrypted Virus
- Metamorphic Virus
- Script Virus
- Macro Virus

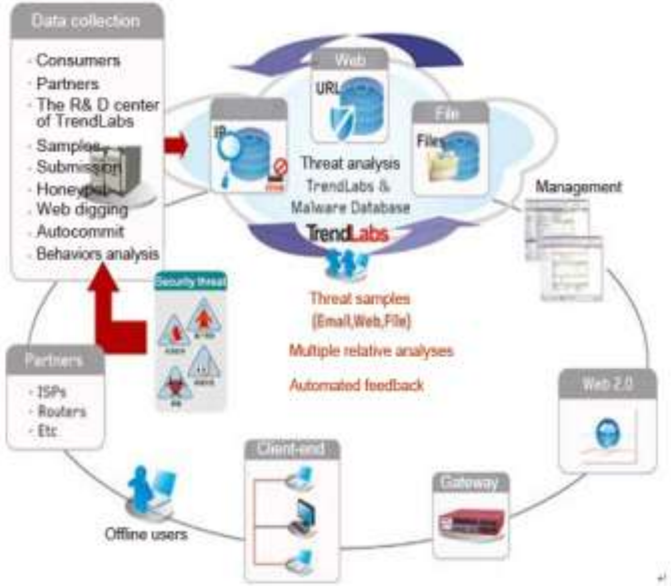
- Pattern Matching Penetrated
- Difficulty Promoted
- Direct Attack Mechanism
- Disrupting the Wording Chain
- Interfering Mechanism
- Normalized Confrontation

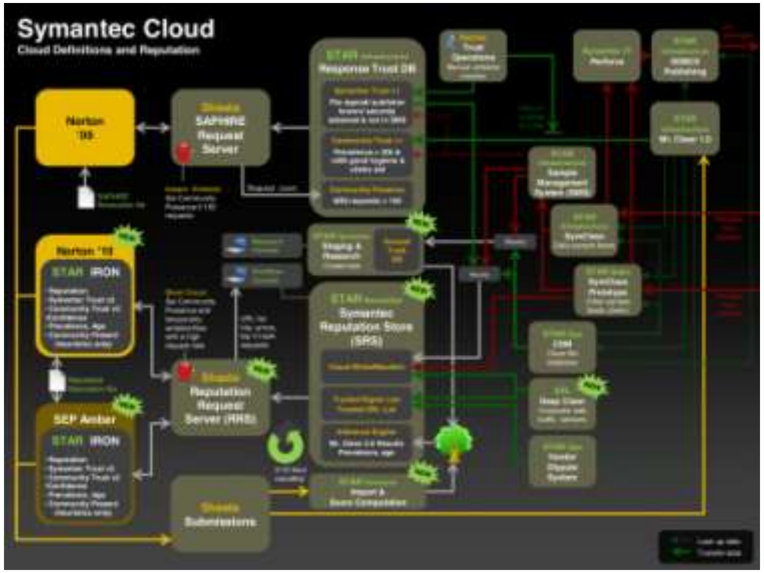
Normalized Confrontation



Systematical confrontation（2000～2005）


Botmaster sends a trojan or mass exploit onto the Internet to infect victims
Botmaster
1
5
Botmaster sends new code to the C&C, which in turn updates the bots.
3
IRC
C&C instructs bot client to scan for recruits
INTERNET
2
First victim gets infected; bot client, using IRC, reports to Command & Control Center (C&C) for instructions
4
First bot client finds and infects more victims, which also connect to C&C for instructions
The World

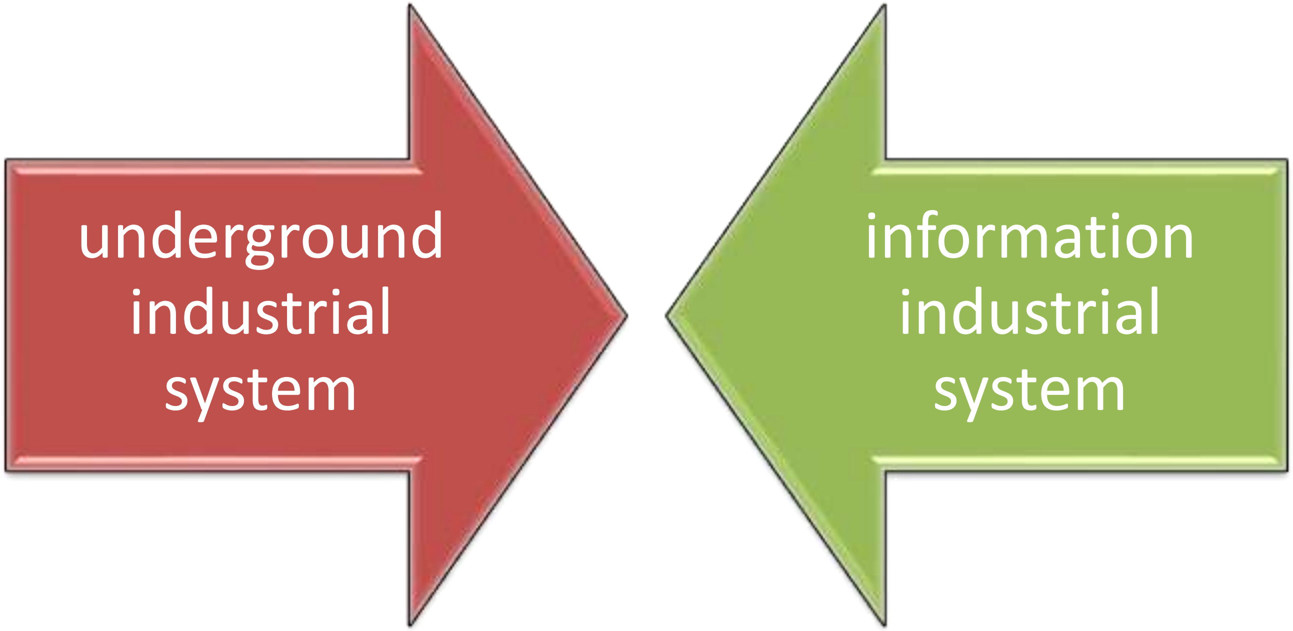




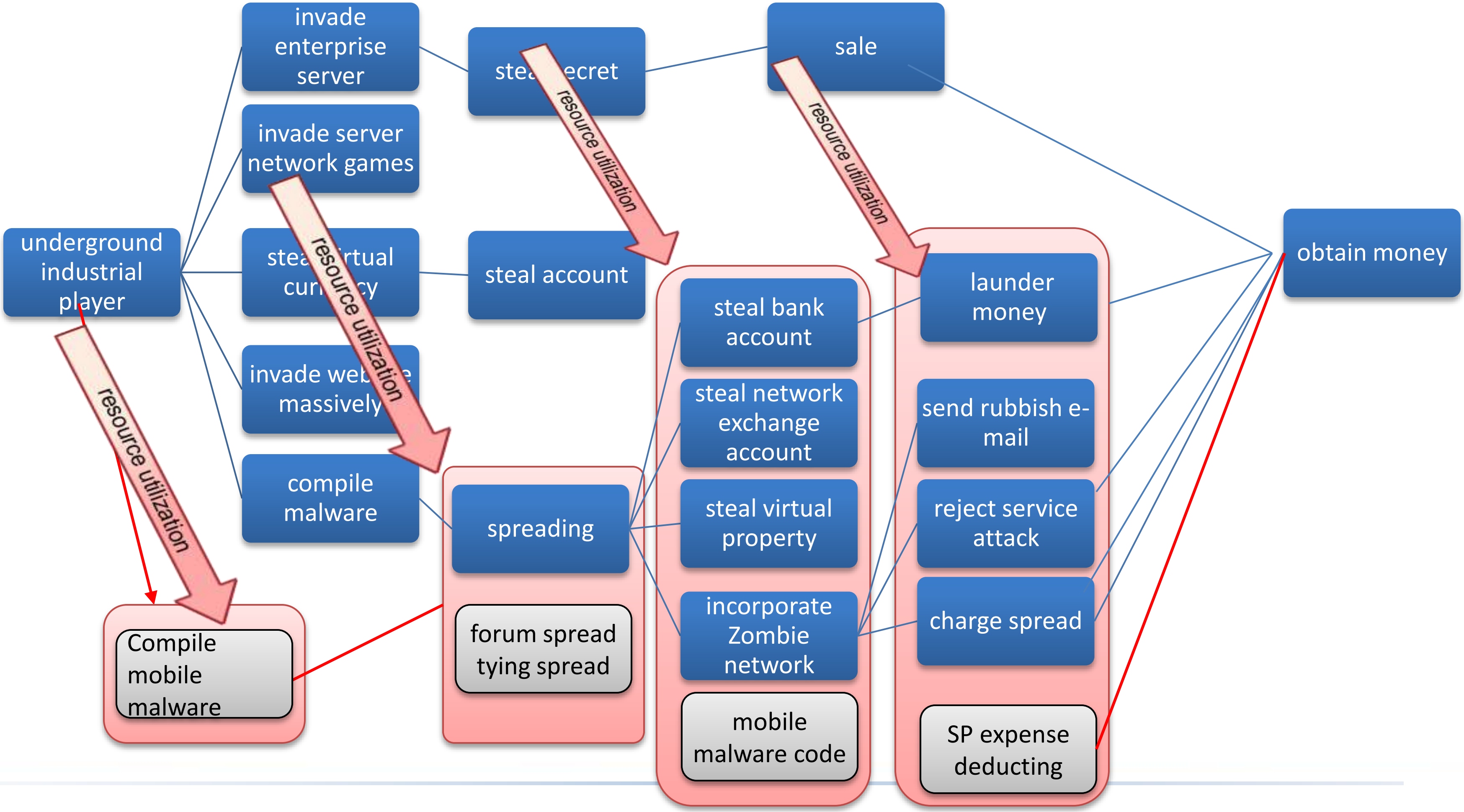
Systematical confrontation (notable event)

- The Emerge of P2P Zombie Network
- The Application of PKI System in Zombie Network
- Attack on VirusTotal by distributed DDos
- Shift from Client to Could Port

Industrial Confrontation (2005—Now)



An Integral Whole Seen from Underground Economy Chain



underground industrial player

invade enterprise server

invade server network games

steal virtual currency

invade website massively

compile malware

steal secret

steal account

sale

spreading

forum spread tying spread

steal bank account

steal network exchange account

steal virtual property

incorporate Zombie network

mobile malware code

launder money

send rubbish e-mail

reject service attack

charge spread

SP expense deducting

obtain money

Compile mobile malware

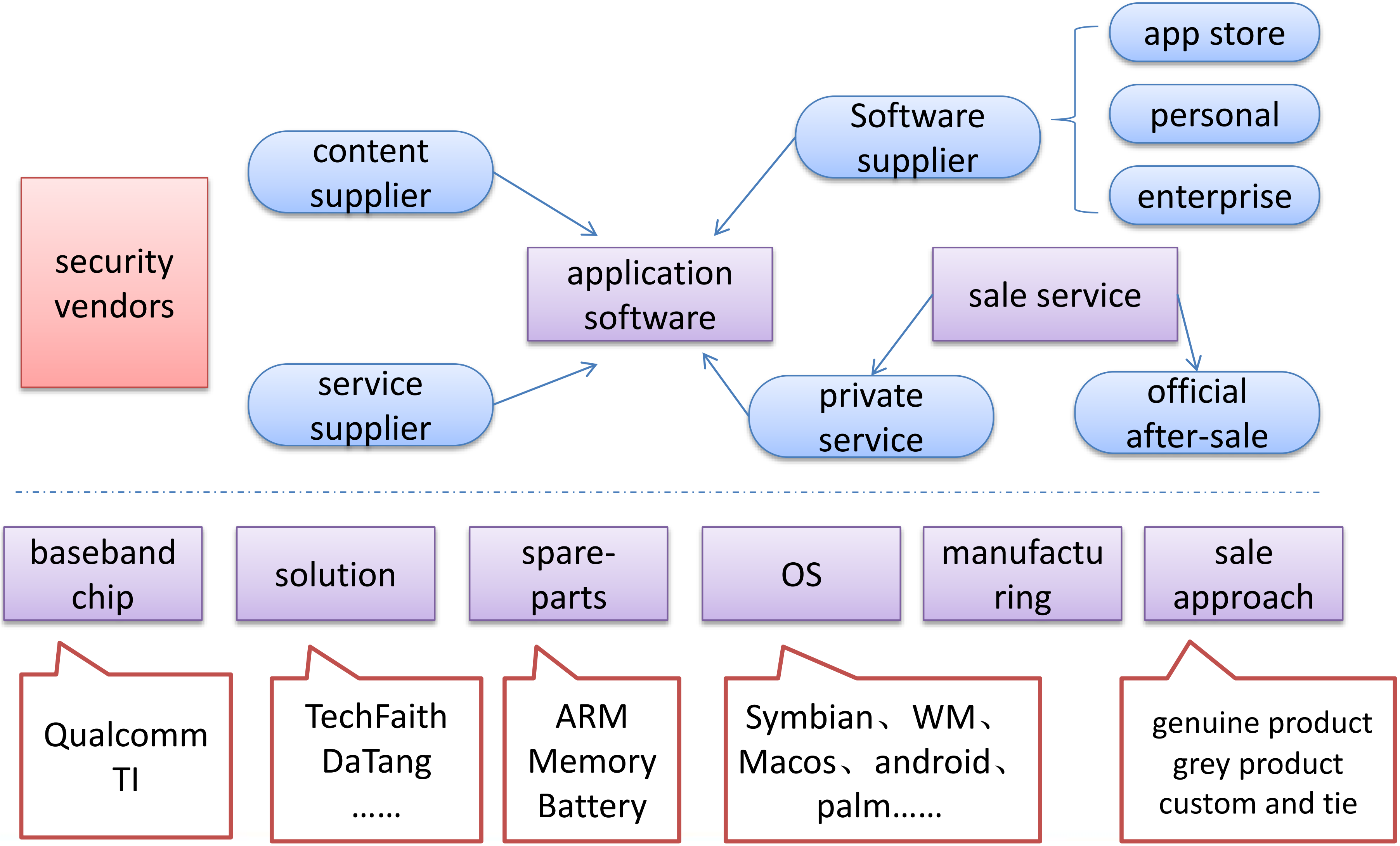
resource utilization

resource utilization

resource utilization

resource utilization

Industrial Chain: Complex and Interminable



security vendors

content supplier

service supplier

application software

Software supplier

app store

personal

enterprise

sale service

private service

official after-sale

baseband chip

solution

spare-parts

OS

manufacturing

sale approach

Qualcomm
TI

TechFaith
DaTang
……

ARM
Memory
Battery

Symbian、 WM、
Macos、 android、
palm……

genuine product
grey product
custom and tie

Summary

- Malware has developed and broke through the traditional single concept of program code. It has penetrated into the whole system of society, politics, economy and life. It is impossible to resist malware effectively only relying on anti-virus vendors. The battle against malware requires the management and resistance of the whole social system.
- Anti-virus men of all countries, unite!
- Thank you!
- seak@antiy.com