

# Android Installer Encryption feature

1. Introduction.
2. What change we've made?
3. What data are now encrypted?
4. How to active the encryption in the installer?
5. How to check on phone?
6. Screen shot.

## 1. Introduction:

Encryption function to make our product more security. It protects our information like: UserName, UserPass, IMEI, UDID when we face with hacker. Some software to hack and detect information in our phone is:

+ Hack phone by root: <http://www.addictivetips.com/mobile/how-to-root-your-android-phone-device/>

+ SHARK : <http://www.appbrain.com/app/shark-for-root/lv.n3o.shark>

⇒ Install in Android phone to get information

+ Wincap: <http://www.wincap.org/install/default.htm> wincap v4.1.2

+ NetworkMiner: <http://sourceforge.net/projects/networkminer/> NetworkMiner v1.0

⇒ Installer in PC to analysis

## 2. What change we've made?

We use **Advanced Encryption Standard (AES)** to encrypt our information and **Base64** to encode and decode internet transfer protocol. Read link below for more details:

[http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

<http://en.wikipedia.org/wiki/Base64>

## 3. What data are now encrypted?

GLIVE:

<http://livewebapp.gameloft.com/glive/?>

lg=EN&

country=LkaKk/Yrhg30NsFvTIDUrVD1ENkvNoVcrGXq7CvZ1Oo=

&d=OrJQXGe6RCc4lvVJGa2xk/7HZsVHsO2sDNTzkEyqREfJ1XFBLbk5jE1MaYdBc3PKUPUQ2S82hVysZersK9nU6g==

&f=GRBQqqNBFCRbe7QjZ+ymslD1ENkvNoVcrGXq7CvZ1Oo=

&udid=uwQvKoQGaOA+EV543g3lf1D1ENkvNoVcrGXq7CvZ1Oo=

&GGI=6hjuwE43GwHKBw5nJ/pH11D1ENkvNoVcrGXq7CvZ1Oo=

&device\_token=

&username=UPUQ2S82hVysZersK9nU6g==

&pass=UPUQ2S82hVysZersK9nU6g==

&remember\_me=&type=ANDROID&height=800&fb=1&enc=1

#### **+ TRACKING:**

<http://ingameads.gameloft.com/redir/hdloading.php>

?game=UNHM&country=US&lg=en&ver=2.1&device=samsung\_NexusS&f=2.3.4

&udid=aya9vYE7sEMrs/p3N2e97VD1ENkvNoVcrGXq7CvZ1Oo=

&g\_ver=334

&line\_number=0yGLz2ZZOdOqtR7somRwsVD1ENkvNoVcrGXq7CvZ1Oo=

&check=2&enc=1

#### **+ IGP:**

<http://ingameads.gameloft.com/redir/android/index.php>

?from=GAME\_CODE&lg=EN

&udid= aya9vYE7sEMrs/p3N2e97VD1ENkvNoVcrGXq7CvZ1Oo=

&d=DEVICE\_ANDROID&f=FIRMWARE\_ANDROID&ver=GAME\_VERSION&country=COUNTRY\_DETECTED& height=DEVICE\_HEIGHT"

&enc=1

+ JP\_HD\_SUBSCRIPTION

[http://confirmation.gameloft.com/jp\\_hd\\_subscription/validate.php](http://confirmation.gameloft.com/jp_hd_subscription/validate.php)

&ticket= ZZOdOqtR7somRwsVD1ENkvNoVcrGXq7CvZ1

&imei= uwQvKoQGaOA+adaEV543g3lf1DERDrGXq7CvZ1Oo=

&enc=1

#### 4. How to active the encryption in the installer?

+ Update newest installer version and check flag : USE\_ENCRYPTION.

+ Edit "config.bat" to set: USE\_ENCRYPTION=1

+ Build and check

#### 5. How to check on phone?

To analyze network packet...

1. Install "**wincap**" and "**NetworkMiner**" on PC

<http://www.winpcap.org/install/default.htm> wincap v4.1.2

<http://sourceforge.net/projects/networkminer/> NetworkMiner v1.0

2. Do **rooting** the device. : <http://www.addictivetips.com/mobile/how-to-root-your-android-phone-device/>

3. Install "**Shark for Root**" on device from Android market.

[https://market.android.com/details?id=lv.n3o.shark&feature=search\\_result](https://market.android.com/details?id=lv.n3o.shark&feature=search_result)

4. Launch application (Ex: Asphalt 6) and go out to springboard.

5. Perform the "Shark for Root" and touch "start"

6. Back to the game then make progress until it is enough progression to create \*.pcap file.

7. Back to the "Shark for Root" and touch "stop" to save \*.pcap to root folder in SD card.

8. Copy \*.pcap file to PC and analyze it using the "NetworkMiner".

Done.

**6. Screen shot:**

Hosts [60]	Frames [10xx]	Files [182]	Images [258]	Messages	Credentials [7]	Sessions [27]	DNS [46]	Parameters [218]	Keywords	Cleartext	Anomalies
Parameter...	Parameter value	Details									
b	MXmYwXA8jZnWajN8vhFWedm5KZnYKtmYqJxlfFWXxmWwWhD8dFSXxm3WtB8jZn8b	HTTP QueryString									
v	1	HTTP QueryString									
lg	KR	HTTP QueryString									
country	KR	HTTP QueryString									
d	samsung_SHW-M250K	HTTP QueryString									
f	2.3.3	HTTP QueryString									
udid	pMBApEFBAQYk4o1d82zJVD1ENkVNoVcrGxq7CvZ10o=	HTTP QueryString									
GGI	25157	HTTP QueryString									
username	UPUQ2S82hVysZersK9nU6g==	HTTP QueryString									
pass	UPUQ2S82hVysZersK9nU6g==	HTTP QueryString									
type	ANDROID	HTTP QueryString									
height	800	HTTP QueryString									
fb	1	HTTP QueryString									
enc	1	HTTP QueryString									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
udid	357470040668406	HTTP QueryString									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
username	yukichan2000	HTTP POST									
pass	1qaz2wsx	HTTP POST									
remember_me	on	HTTP POST									
Connect	connect,connect	HTTP POST									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									
PHPSESSID	1728ee4d4d69bbd2c40f4c2a6ea585d8	HTTP Cookie									

