Exploring North Korea’s Surveillance Technology

Florian Grunow & Niklaus Schiess

ERNW GmbH

Disclaimer

- We never visited DPRK
  - What we say about DPRK is mostly speculation or
  - based on publications of others.
- This is not about making fun of them
  - Not about the developers …
  - … and certainly not about the people of DPRK
- No focus on security in this talk -> Privacy

Agenda

- Introduction
- Surveillance
- Censorship
- Conclusions

Motivation

- Shed some light on repressive technology, even in 2017
- Overview of technical abilities to perform
  - Surveillance of their citizens
  - Censorship on a large scale
- Lack of public, in-depth research about technology by DPRK
- Disclosure to the public of potential surveillance and censorship

Previous Research

- Research done by us
  - Lifting the fog on Red Star OS (32C3)
  - Woolim: Lifting the fog on DPRK's latest tablet PC (33C3)

Previous Research

- Research done by us
  - Lifting the fog on Red Star OS (32C3)
  - Woolim: Lifting the fog on DPRK's latest tablet PC (33C3)
- Research done by others
  - Multiple publications concerning Red Star OS security (@hackerfantastic)
  - Art based on our Red Star OS research: Inter Alias (www.interalias.org)
  - Compromising Connectivity: Information Dynamics between the State & Society in a Digitizing North Korea - U.S.-Korea Institute (USKI) at SAIS

NO
SPY

Modern Devices in a Repressive State

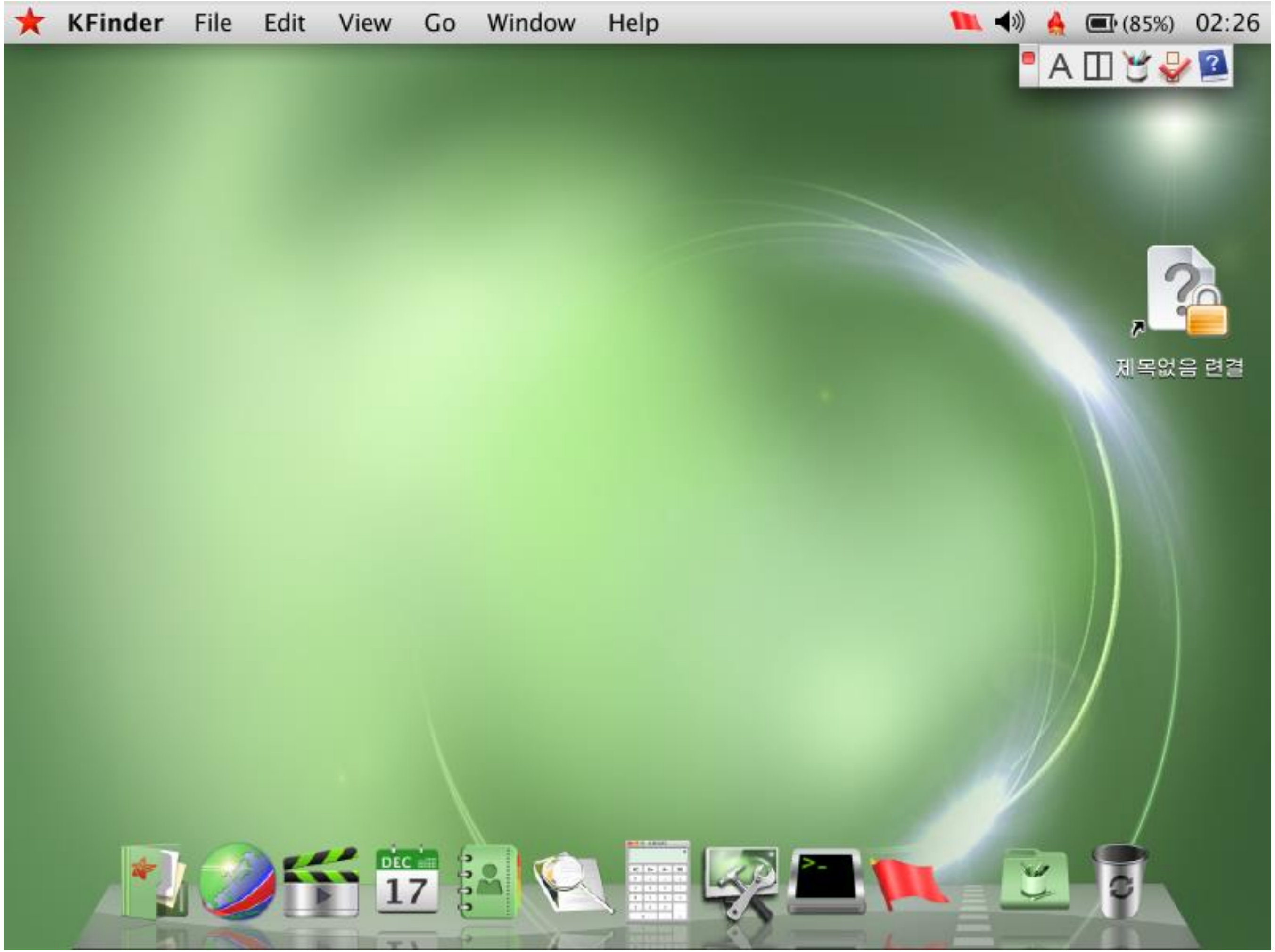
- DPRK started at around ~2000
- PCs, tablet PCs, mobile phones
- The problem: devices allow
  - access to media (photos, videos, audio),
  - sharing of media files and
  - potentially access information from outside of DPRK.
- Potential solutions:
  - Surveillance: tracking the distribution of unwanted/impure media
  - Censorship: prevent the distribution of unwanted/impure media

Red Star OS

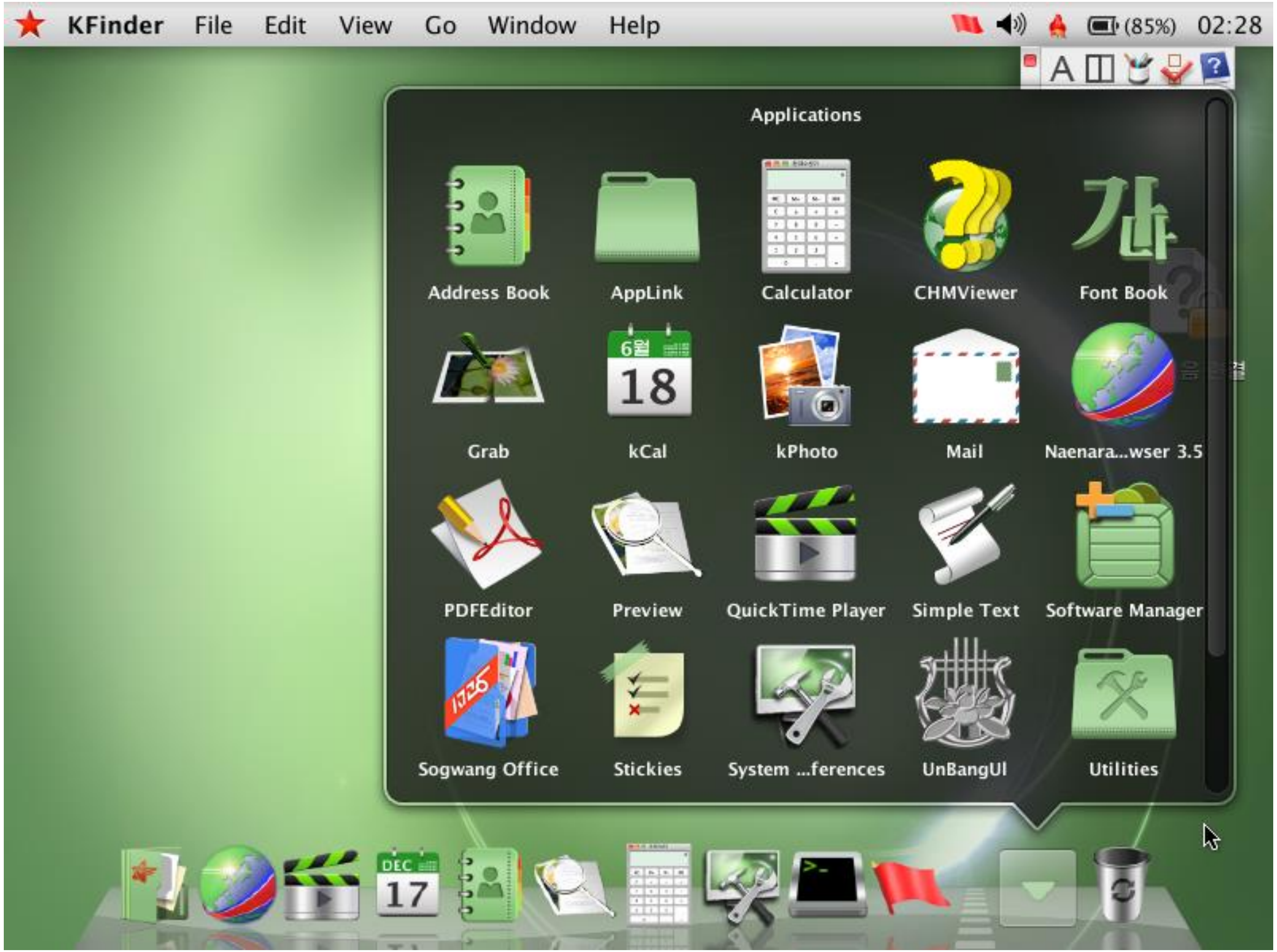
Tracking the distribution of media files

Red Star OS

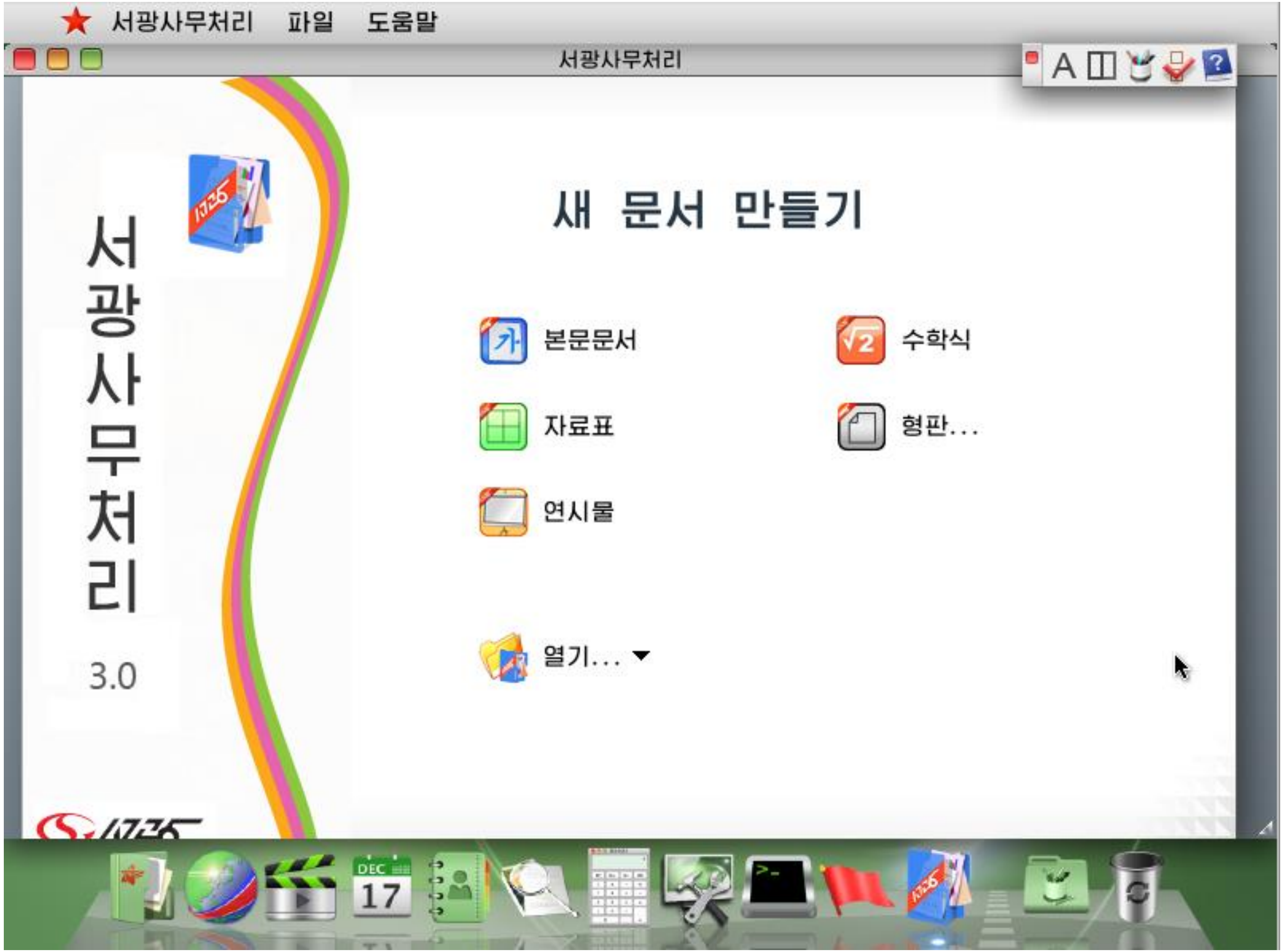
- Different leaked versions
  - Server (3.0) and Desktop (2.0 (and 2.5?) and 3.0)
  - We focused on Desktop 3.0
- General purpose desktop system based on Fedora and KDE
  - Look and Feel of Mac OS X
  - Email client, calendar, word processor, media player…
- Latest package builds in 2013
- Public leak in December 2014



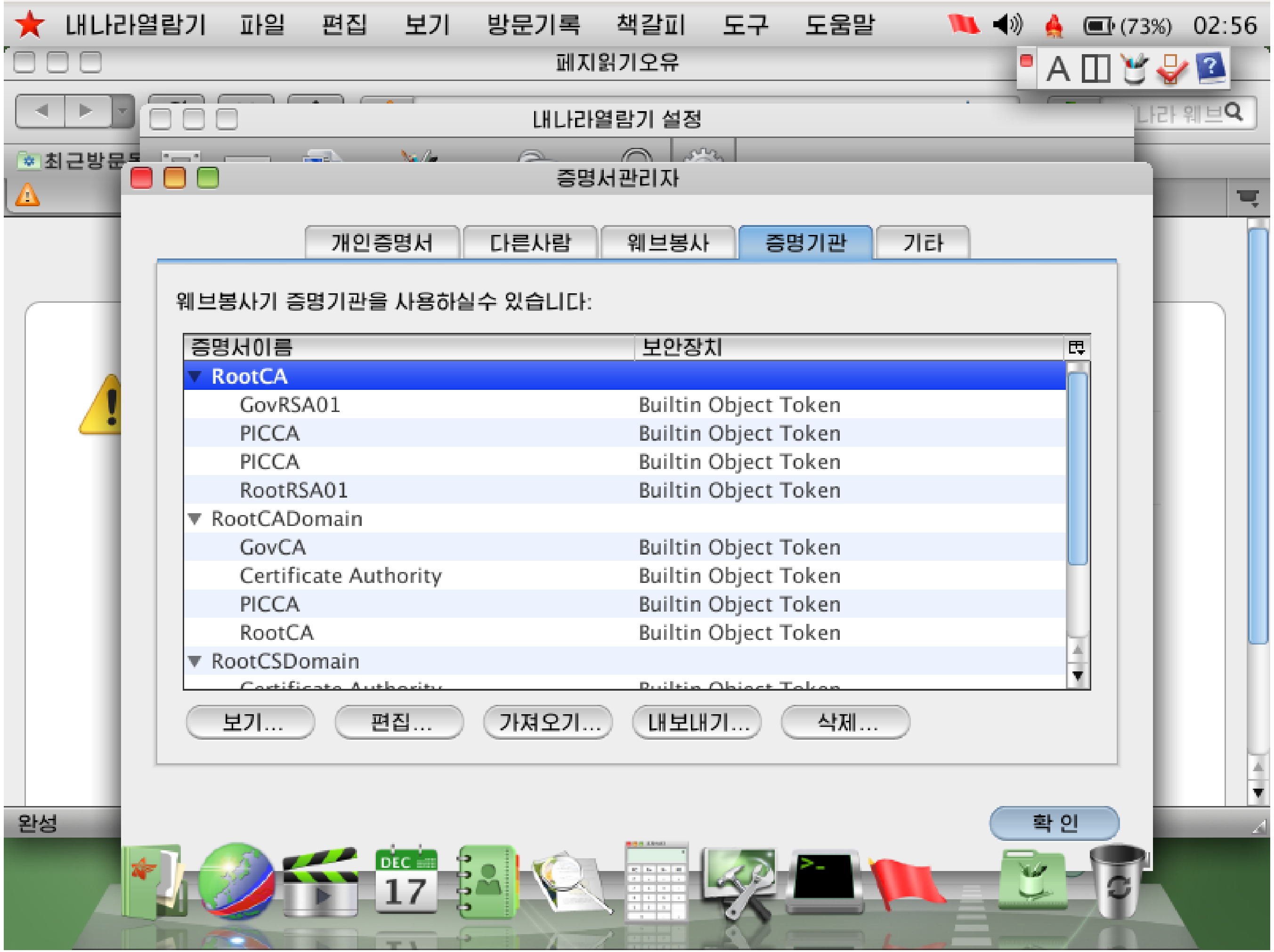
NO SPY


KFinder
File
Edit
View
Go
Window
Help
(85%)
02:28
Applications
Address Book
AppLink
Calculator
CHMViewer
Font Book
Grab
kCal
kPhoto
Mail
Naenara...wser 3.5
PDFEditor
Preview
QuickTime Player
Simple Text
Software Manager
Sogwang Office
Stickies
System ...ferences
UnBangUI
Utilities

NO SPY


서광사무처리
파일
도움말
서광사무처리
서광사무처리
3.0
새 문서 만들기
본문문서
수학식
자료표
형판...
연시물
열기...
DEC
17

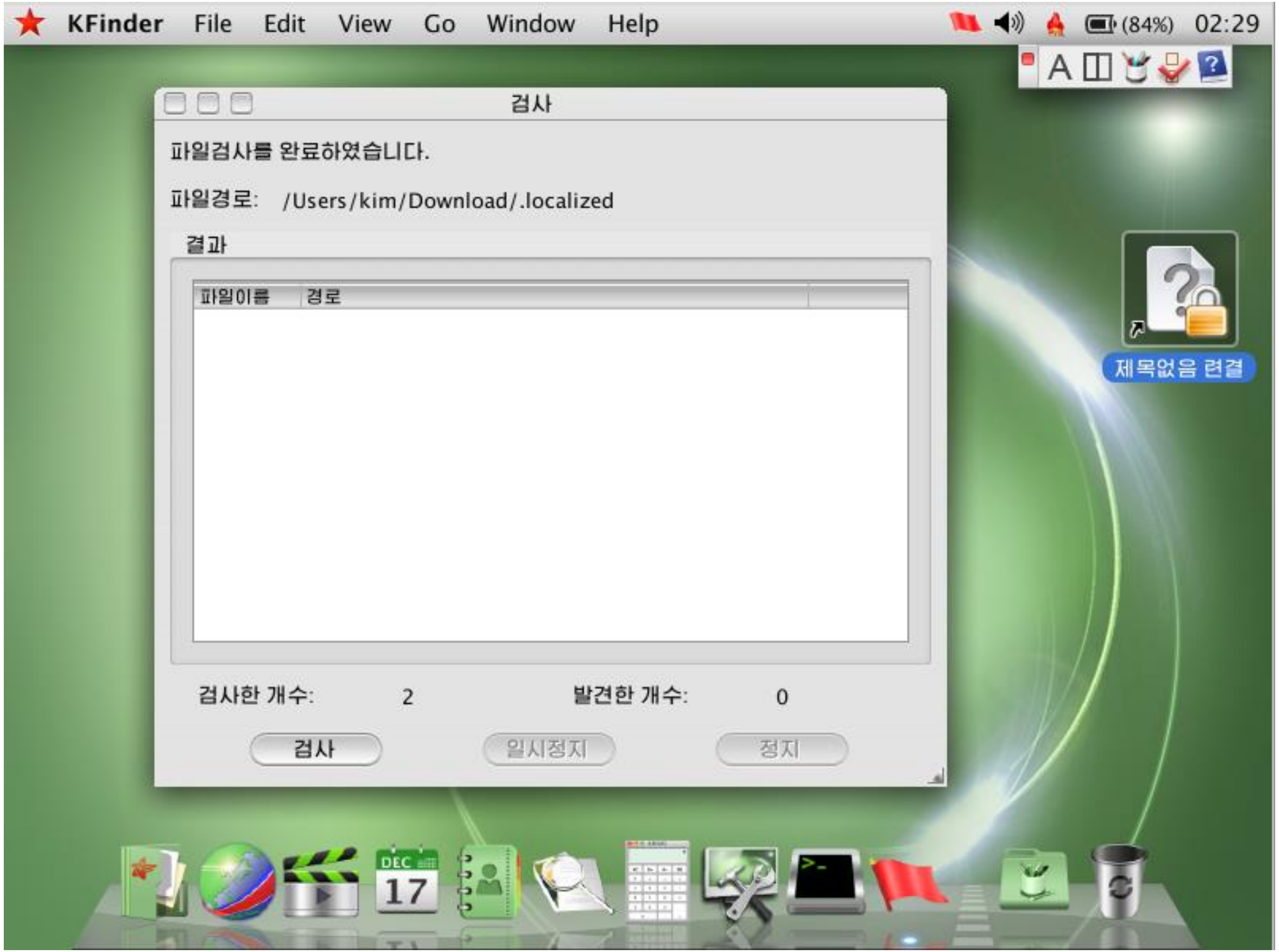
NO SPY



웨브봉사기 증명기관을 사용하실수 있습니다:

증명서이름	보안장치
▼ RootCA	
GovRSA01	Builtin Object Token
PICCA	Builtin Object Token
PICCA	Builtin Object Token
RootRSA01	Builtin Object Token
▼ RootCADomain	
GovCA	Builtin Object Token
Certificate Authority	Builtin Object Token
PICCA	Builtin Object Token
RootCA	Builtin Object Token
▼ RootCSDomain	
Certificate Authority	Builtin Object Token

NO SPY



검사

파일검사를 완료하였습니다.

파일경로: /Users/kim/Download/.localized

결과

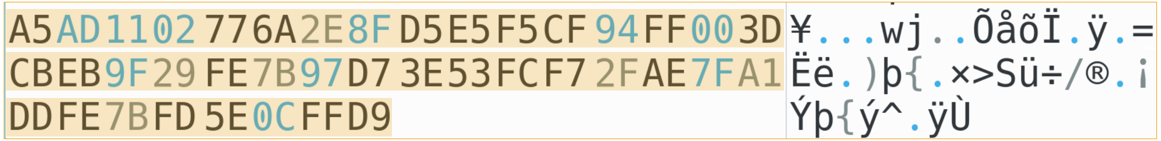
파일이름	경로

검사한 개수: 2

발견한 개수: 0

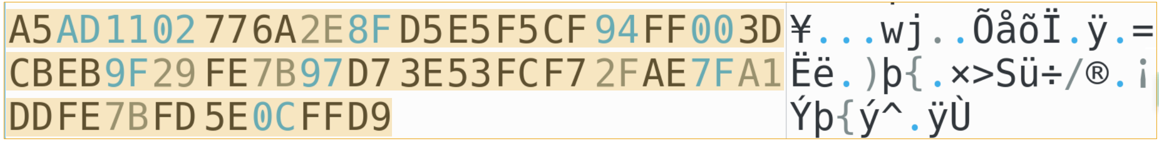
NO SPY

Original

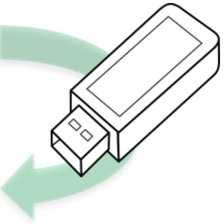


```
A5AD1102776A2E8FD5E5F5CF94FF003D¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9                Ýþ{ý^.ÿÙ
```

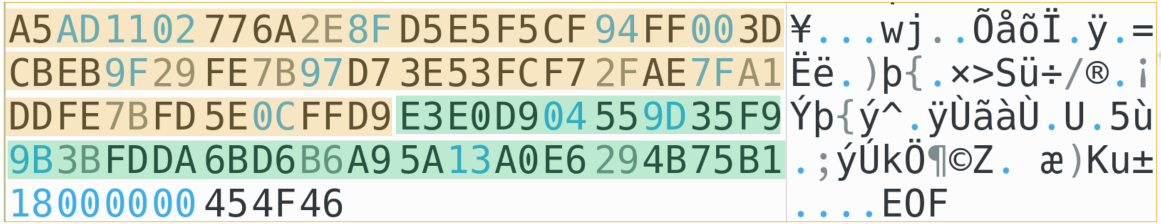
Original



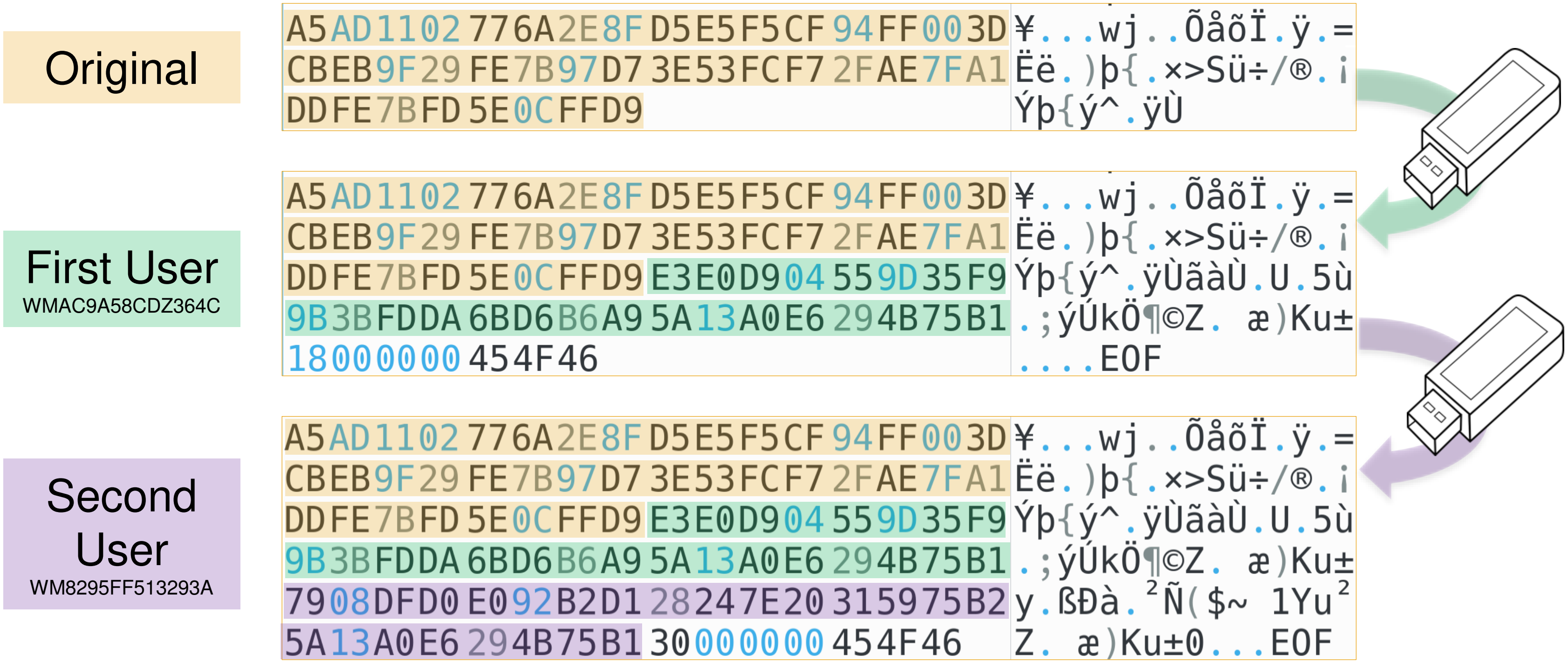
```
A5 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D ¥...wj..ÕåõÏ.ÿ.=
CB EB 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 Ëë.)þ{.×>Sü÷/®.¡
DD FE 7B FD 5E 0C FF D9                         Ýþ{ý^.ÿÙ
```



First User
WMAC9A58CDZ364C



```
A5 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D ¥...wj..ÕåõÏ.ÿ.=
CB EB 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 Ëë.)þ{.×>Sü÷/®.¡
DD FE 7B FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 Ýþ{ý^.ÿÙãàÙ.U.5ù
9B 3B FD DA 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 .;ýÚkÖ¶©Z. æ)Ku±
18 00 00 00 45 4F 46                            ....EOF
```



Original

```
A5AD1102 776A2E8F D5E5F5CF 94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29 FE7B97D7 3E53FCF7 2FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD 5E0CFFD9                   Ýþ{ý^.ÿÙ
```

First User
WMAC9A58CDZ364C

```
A5AD1102 776A2E8F D5E5F5CF 94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29 FE7B97D7 3E53FCF7 2FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD 5E0CFFD9 E3E0D904 559D35F9 Ýþ{ý^.ÿÙãàÙ.U.5ù
9B3BFDDA 6BD6B6A9 5A13A0E6 294B75B1 .;ýÚkÖ¶©Z. æ)Ku±
18000000 454F46                     ....EOF
```

Second User
WM8295FF513293A

```
A5AD1102 776A2E8F D5E5F5CF 94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29 FE7B97D7 3E53FCF7 2FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD 5E0CFFD9 E3E0D904 559D35F9 Ýþ{ý^.ÿÙãàÙ.U.5ù
9B3BFDDA 6BD6B6A9 5A13A0E6 294B75B1 .;ýÚkÖ¶©Z. æ)Ku±
7908DFD0 E092B2D1 28247E20 315975B2 y.ßÐà.²Ñ($~ 1Yu²
5A13A0E6 294B75B1 30000000 454F46   Z. æ)Ku±0...EOF
```

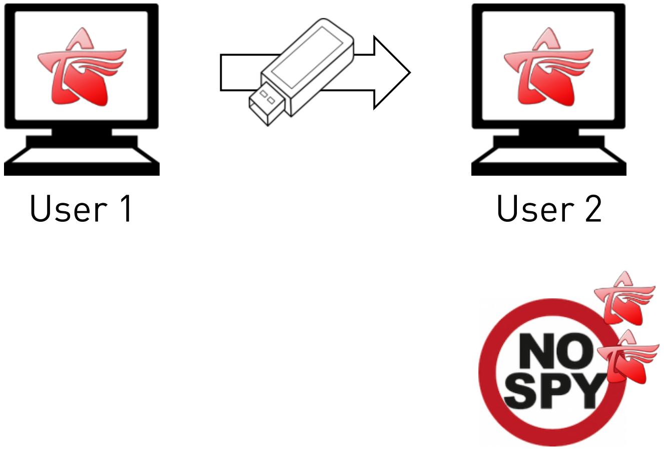
Decryption tool: https://github.com/takeshixx/redstar-tools

Tracking the Distribution of Media Files

User 1

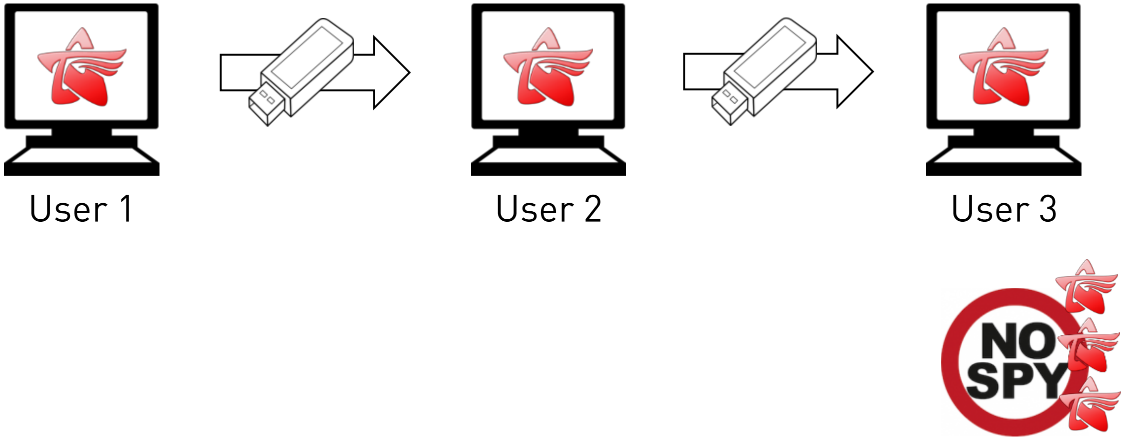
no-spy.jpg

Tracking the Distribution of Media Files



no-spy.jpg

Tracking the Distribution of Media Files



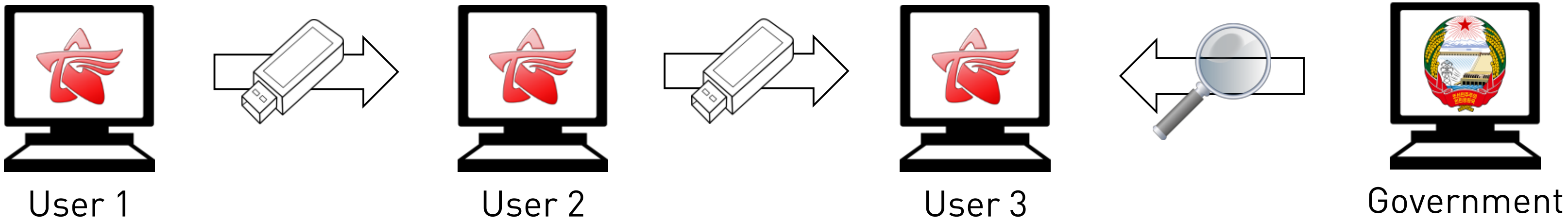
User 1

User 2

User 3

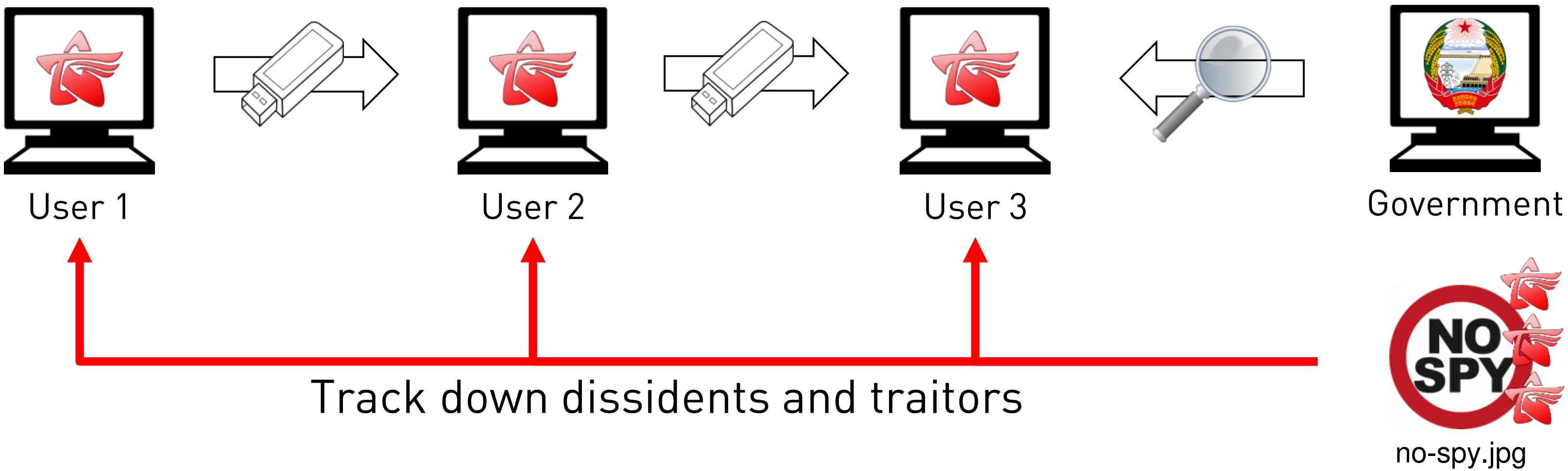
no-spy.jpg

Tracking the Distribution of Media Files



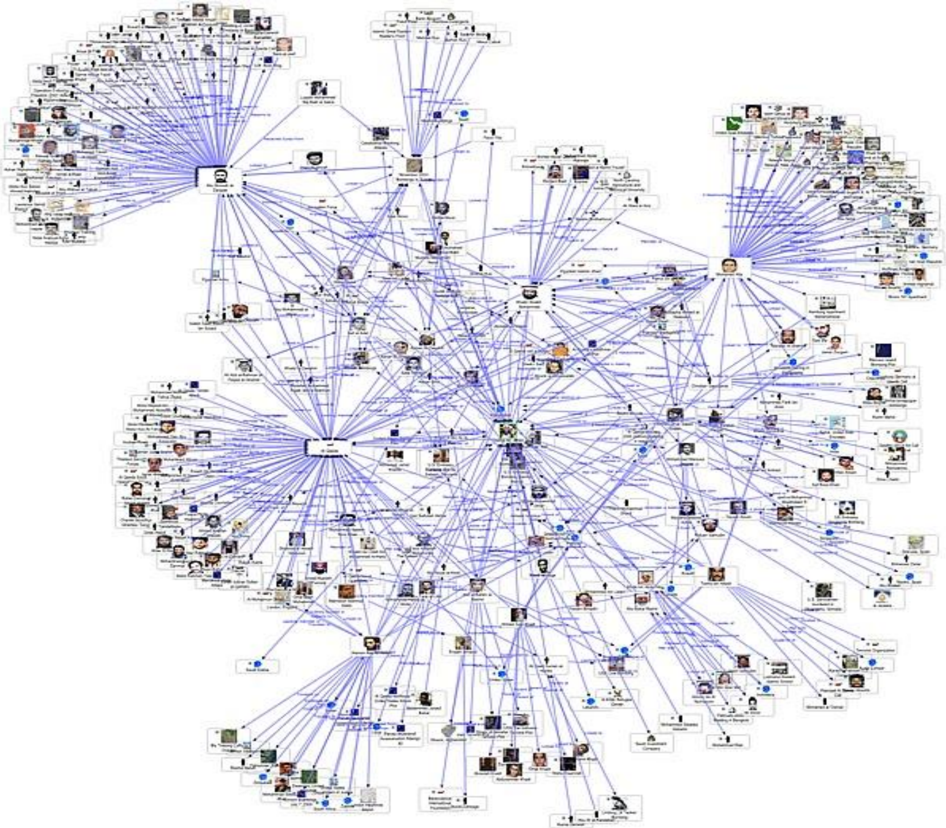
no-spy.jpg

Tracking the Distribution of Media Files



Tracking the Distribution of Media Files

- Create social networks
- Construct connections between dissidents
- Track down sources that create/import media files
- Shutdown dissidents/traitors



Source: https://i.stack.imgur.com/xWMRJ.jpg

Problems with Red Star OS Watermarking

- Only affects media files
  - No binaries/applications -> users can install software
- Not really sophisticated
  - Can be removed/bypassed easily
- “AntiVirus” could prevent distribution of certain files
- Watermarking only allows to **track** the distribution of media
  - Does **not prevent** distribution of media

Woolim

Prevent the distribution of media files

Source: http://bilder4.n-tv.de/img/incoming/crop10413391/8721322747-cImg_16_9-w1200/RTR3EQ0B.jpg

Woolim

- Name of a waterfall in DPRK
- Manufacturer: Hoozo (Z100) from China
- Similar products sell for ~180€ to ~260€ online
- Software from/modified by DPRK
- System Information
  - Allwinner A33 (ARMv7) SoC
  - 8GB SK Hynix flash
  - MicroSD and power plug
- Android 4.4.2 with Kernel 3.4.39
- Connectivity only available via dongles (no WIFI/Bluetooth built-in)

Source: http://s.newsweek.com/sites/www.newsweek.com/files/2015/02/23/0227kimjongun01.jpg

Woolim is More Restrictive

- Introduces file signatures
  - Using asymmetric cryptography (RSA)
  - Goal: **PREVENT** the distribution of media files

Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Woolim is More Restrictive

- Introduces file signatures
  - Using asymmetric cryptography (RSA)
  - Goal: **PREVENT** the distribution of media files
- Government has full control over signatures
  - Absolute control over media sources

Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Exploring “This is not signed file.”

- Introduces file signatures
  - Using asymmetric cryptography (RSA)
  - Goal: **PREVENT** the distribution of media files
- Government has full control over signatures
  - Absolute control over media sources
- Explicit signature checks on Woolim
  - Apps have to take care of checks
  - Unlike Red Star OS’s kernel module

Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Signature Checking

- Java interface with native JNI library
  - Called by apps e.g. during file opening/saving
  - Sometimes concealed as “license checks”

Signature Checking

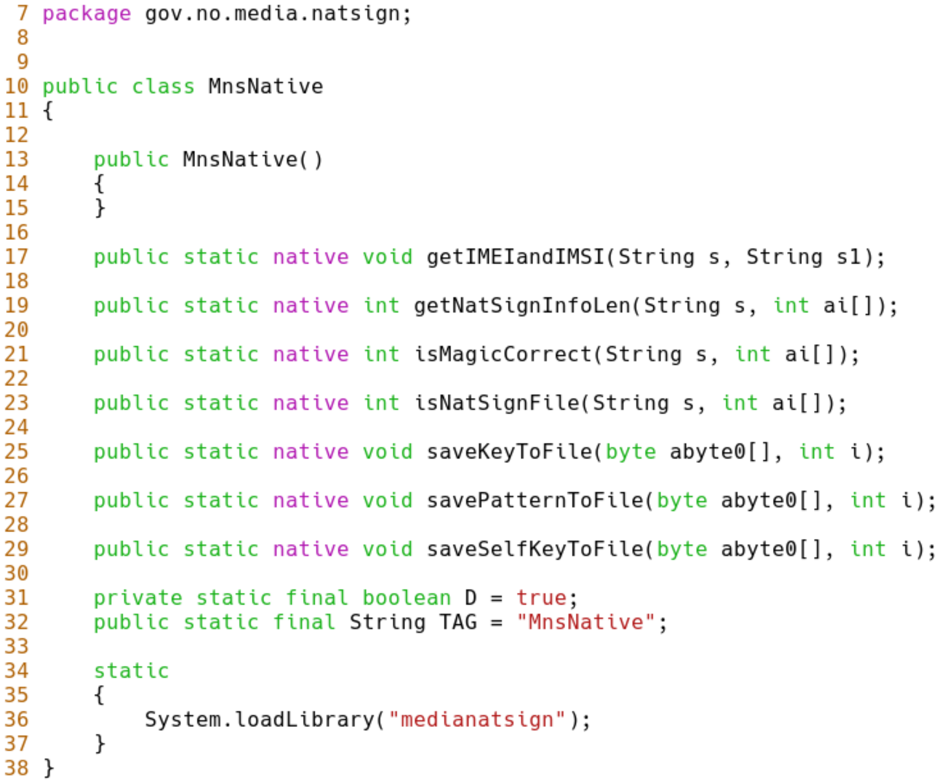
- Java interface with native JNI library
  - Called by apps e.g. during file opening/saving
  - Sometimes concealed as “license checks”
- Multiple ways of signing
  - NATISIGN: Files signed by the government
  - SELFSIGN: Files signed by the device itself

Signature Checking

- Java interface with native JNI library
  - Called by apps e.g. during file opening/saving
  - Sometimes concealed as “license checks”
- Multiple ways of signing
  - **NATISIGN**: Files signed by the government
  - **SELFSIGN**: Files signed by the device itself
- Files without proper signatures cannot be opened
  - By apps that do signature checks

Java Native Interface Libraries

- Check if file has a proper signature
- Used by various applications, e.g.:
  - FileBrowser.apk
  - Gallery2.apk
  - Music.apk
  - PackageInstaller.apk
  - PDFViewer.apk
  - RedFlag.apk
  - SoundRecorder.apk
  - TextEditor.apk



```java
package gov.no.media.natsign;


public class MnsNative
{

    public MnsNative()
    {
    }

    public static native void getIMEIandIMSI(String s, String s1);

    public static native int getNatSignInfoLen(String s, int ai[]);

    public static native int isMagicCorrect(String s, int ai[]);

    public static native int isNatSignFile(String s, int ai[]);

    public static native void saveKeyToFile(byte abyte0[], int i);

    public static native void savePatternToFile(byte abyte0[], int i);

    public static native void saveSelfKeyToFile(byte abyte0[], int i);

    private static final boolean D = true;
    public static final String TAG = "MnsNative";

    static
    {
        System.loadLibrary("medianatsign");
    }
}
```

NATISIGN

- Files that have been approved by the government
  - Also referred to as “gov_sign”
- Files are signed with a 2048 bit RSA key
- Device holds the public key to verify signatures
  - Deployed on the device (0.dat)
- Code does some additional obfuscation
  - Probably to make manual signing harder

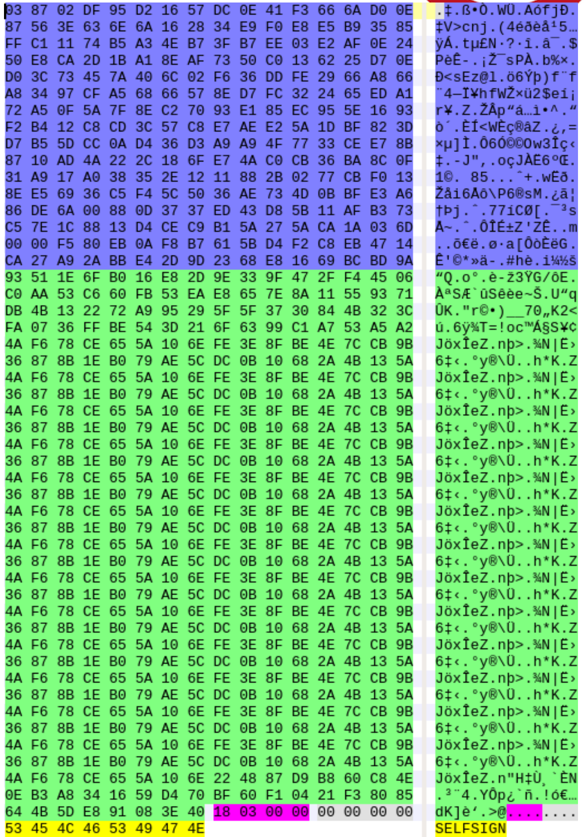
Source: https://en.wikipedia.org/wiki/North_Korea#/media/File:Emblem_of_North_Korea.svg

SELFSIGN’ing

- Combination of
  - Symmetric encryption (Rijndael 256)
  - Asymmetric signatures (RSA)
  - Hashing (SHA224/SHA256)
- Device identity stored in legalref.dat
  - Comprised of IMEI and IMSI
  - Each device‘s „legal reference“
- Files created on the device itself can be opened
  - Camera images, office documents, PDFs, etc.

SELFSIGN Signatures

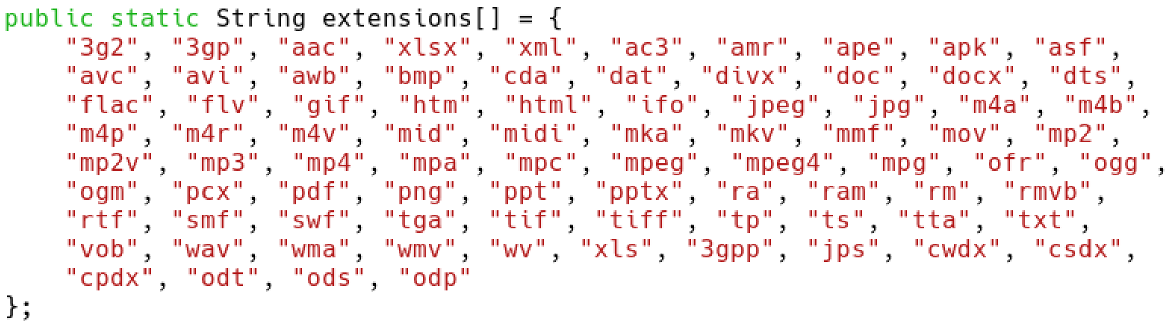
- RSA signature of file hash
- Encrypted device identity
  - Rijndael 256 (key and blocks)
  - IMEI and IMSI
- Trailer
  - Signature size
  - ASCII suffix “SELFSIGN“
- Fixed size of 792 bytes



```
03 87 02 DF 95 D2 16 57 DC 0E 41 F3 66 6A D0 0E  .‡.ß•Ò.WÜ.AófjÐ.
87 56 3E 63 6E 6A 16 28 34 E9 F0 E8 E5 B9 35 85  ‡V>cnj.(4éðèå¹5…
FF C1 11 74 B5 A3 4E B7 3F B7 EE 03 E2 AF 0E 24  ÿÁ.tµ£N·?·î.â¯.$
50 E8 CA 2D 1B A1 8E AF 73 50 C0 13 62 25 D7 0E  PèÊ-.¡Ž¯sPÀ.b%×.
D0 3C 73 45 7A 40 6C 02 F6 36 DD FE 29 66 A8 66  Ð<sEz@l.ö6Ýþ)f¨f
A8 34 97 CF A5 68 66 57 8E D7 FC 32 24 65 ED A1  ¨4—Ï¥hfWŽ×ü2$eí¡
72 A5 0F 5A 7F 8E C2 70 93 E1 85 EC 95 5E 16 93  r¥.Z.ŽÂp“á…ì•^.“
F2 B4 12 C8 CD 3C 57 C8 E7 AE E2 5A 1D BF 82 3D  ò´.ÈÍ<WÈç®âZ.¿‚=
D7 B5 5D CC 0A D4 36 D3 A9 A9 4F 77 33 CE E7 8B  ×µ]Ì.Ô6Ó©©Ow3Îç‹
87 10 AD 4A 22 2C 18 6F E7 4A C0 CB 36 BA 8C 0F  ‡.-J",.oçJÀË6ºŒ.
31 A9 17 A0 38 35 2E 12 11 88 2B 02 77 CB F0 13  1©. 85...ˆ+.wËð.
8E E5 69 36 C5 F4 5C 50 36 AE 73 4D 0B BF E3 A6  Žåi6Åô\P6®sM.¿ã¦
86 DE 6A 00 88 0D 37 37 ED 43 D8 5B 11 AF B3 73  †Þj.ˆ.77íCØ[.¯³s
C5 7E 1C 88 13 D4 CE C9 B1 5A 27 5A CA 1A 03 6D  Å~.ˆ.ÔÎÉ±Z'ZÊ..m
00 00 F5 80 EB 0A F8 B7 61 5B D4 F2 C8 EB 47 14  ..õ€ë.ø·a[ÔòÈëG.
CA 27 A9 2A BB E4 2D 9D 23 68 E8 16 69 BC BD 9A  Ê'©*»ä-.#hè.i¼½š
93 51 1E 6F B0 16 E8 2D 9E 33 9F 47 2F F4 45 06  “Q.o°.è-ž3ŸG/ôE.
C0 AA 53 C6 60 FB 53 EA E8 65 7E 8A 11 55 93 71  ÀªSÆ`ûSêèe~Š.U“q
DB 4B 13 22 72 A9 95 29 5F 5F 37 30 84 4B 32 3C  ÛK."r©•)__70„K2<
FA 07 36 FF BE 54 3D 21 6F 63 99 C1 A7 53 A5 A2  ú.6ÿ¾T=!oc™Á§S¥¢
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B  JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A  6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E 22 48 87 D9 B8 60 C8 4E  JöxÎeZ.n"H‡Ù¸`ÈN
0E B3 A8 34 16 59 D4 70 BF 60 F1 04 21 F3 80 85  .³¨4.YÔp¿`ñ.!ó€…
64 4B 5D E8 91 08 3E 40 18 03 00 00 00 00 00 00  dK]è‘.>@........
53 45 4C 46 53 49 47 4E                          SELFSIGN
```

Files Types Affected by Signing

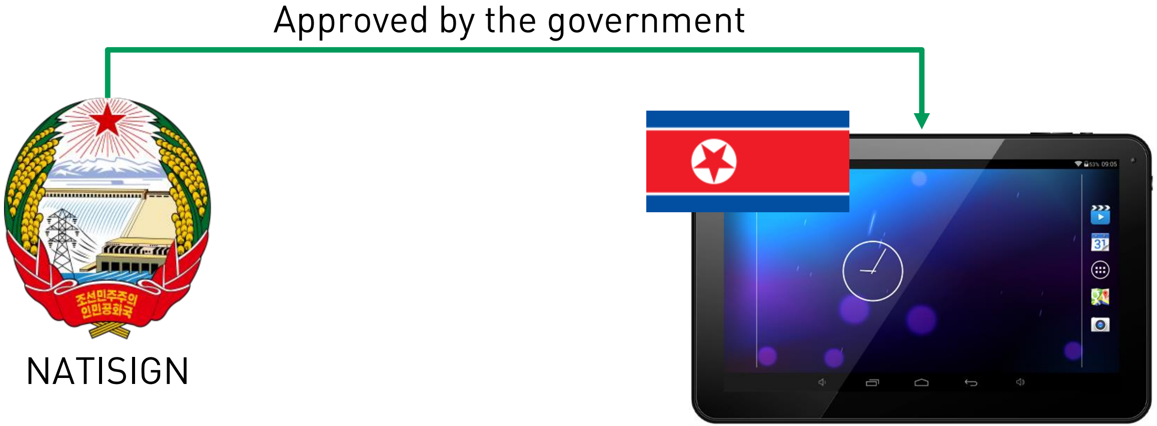
- All kinds of media files
- Text and HTML files
- Even APKs…



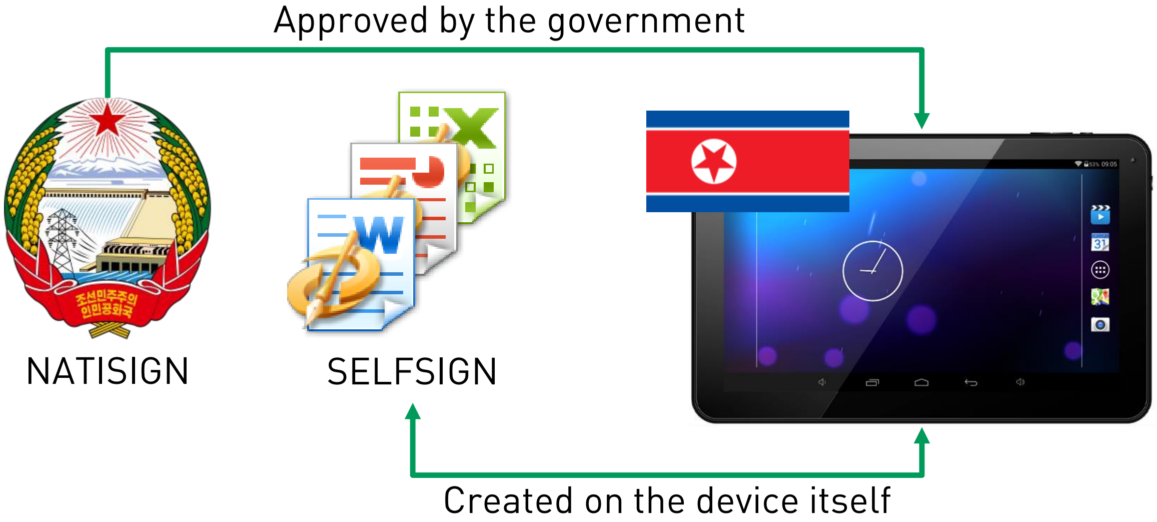
```
public static String extensions[] = {
    "3g2", "3gp", "aac", "xlsx", "xml", "ac3", "amr", "ape", "apk", "asf",
    "avc", "avi", "awb", "bmp", "cda", "dat", "divx", "doc", "docx", "dts",
    "flac", "flv", "gif", "htm", "html", "ifo", "jpeg", "jpg", "m4a", "m4b",
    "m4p", "m4r", "m4v", "mid", "midi", "mka", "mkv", "mmf", "mov", "mp2",
    "mp2v", "mp3", "mp4", "mpa", "mpc", "mpeg", "mpeg4", "mpg", "ofr", "ogg",
    "ogm", "pcx", "pdf", "png", "ppt", "pptx", "ra", "ram", "rm", "rmvb",
    "rtf", "smf", "swf", "tga", "tif", "tiff", "tp", "ts", "tta", "txt",
    "vob", "wav", "wma", "wmv", "wv", "xls", "3gpp", "jps", "cwdx", "csdx",
    "cpdx", "odt", "ods", "odp"
};
```

Absolute Control of Woolim’s Media Sources

Absolute Control of Woolim’s Media Sources



Absolute Control of Woolim’s Media Sources



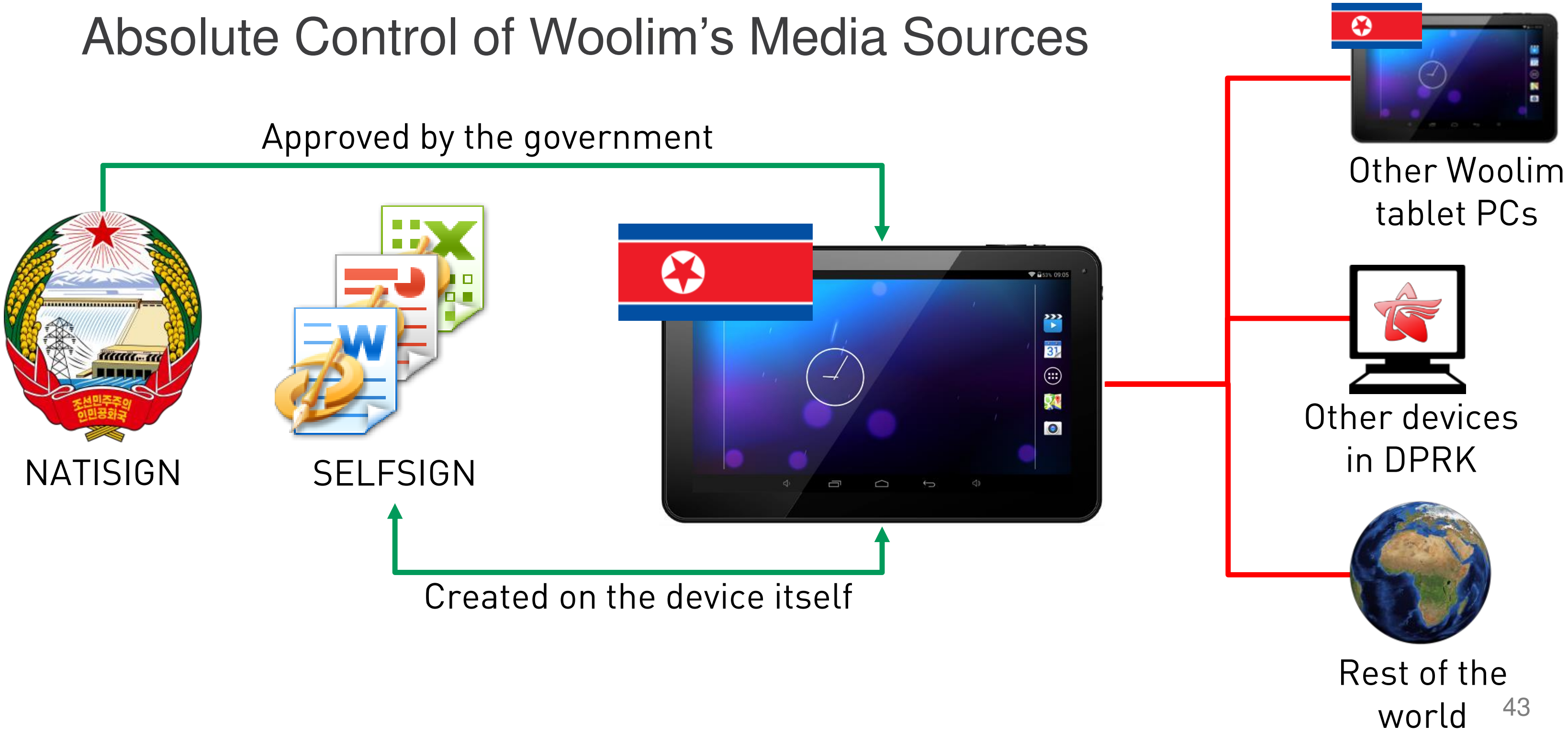
Approved by the government

NATISIGN

SELFSIGN

Created on the device itself

Absolute Control of Woolim's Media Sources



Approved by the government

NATISIGN

SELFSIGN

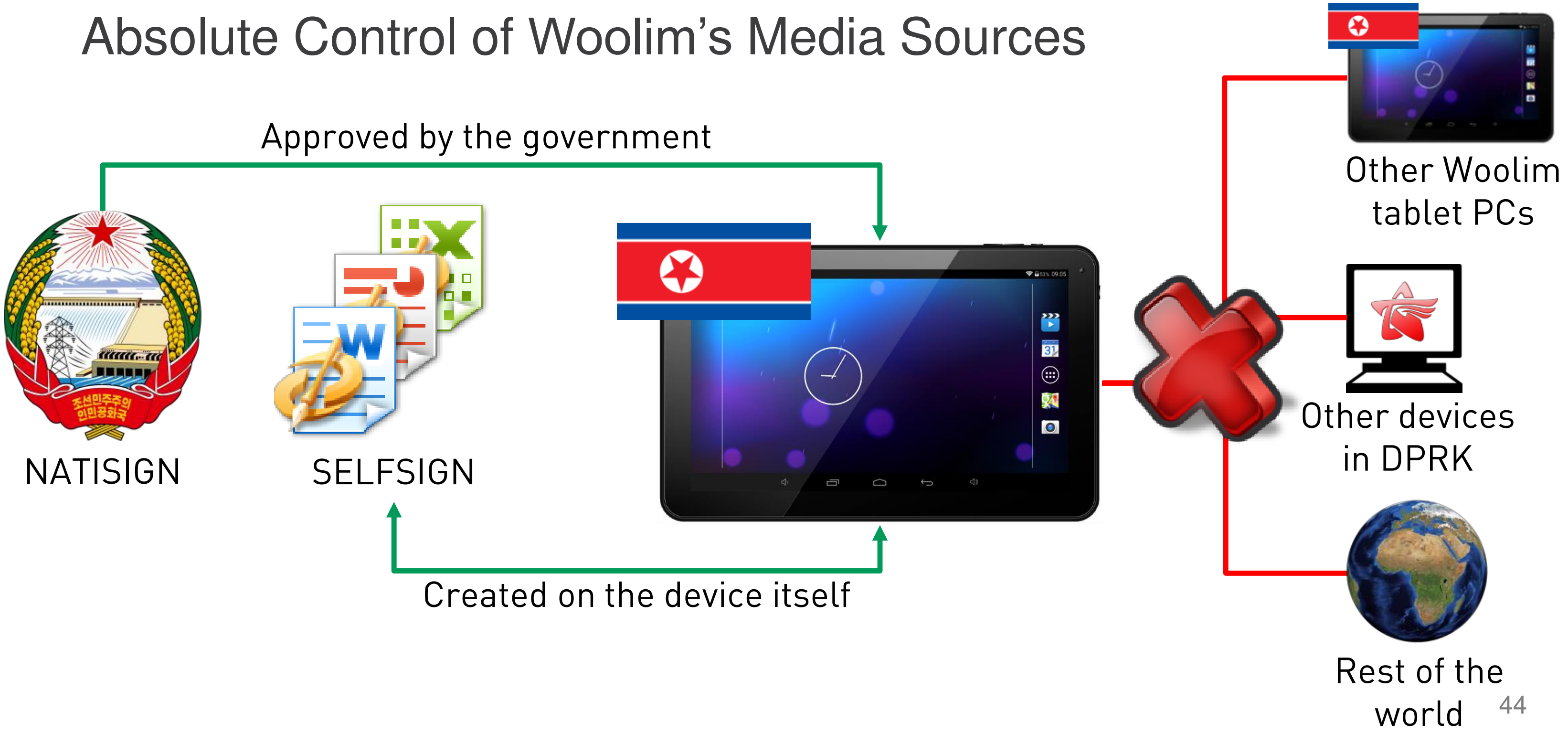
Created on the device itself

Other Woolim tablet PCs

Other devices in DPRK

Rest of the world

Absolute Control of Woolim's Media Sources



Approved by the government

NATISIGN

SELFSIGN

Created on the device itself

Other Woolim tablet PCs

Other devices in DPRK

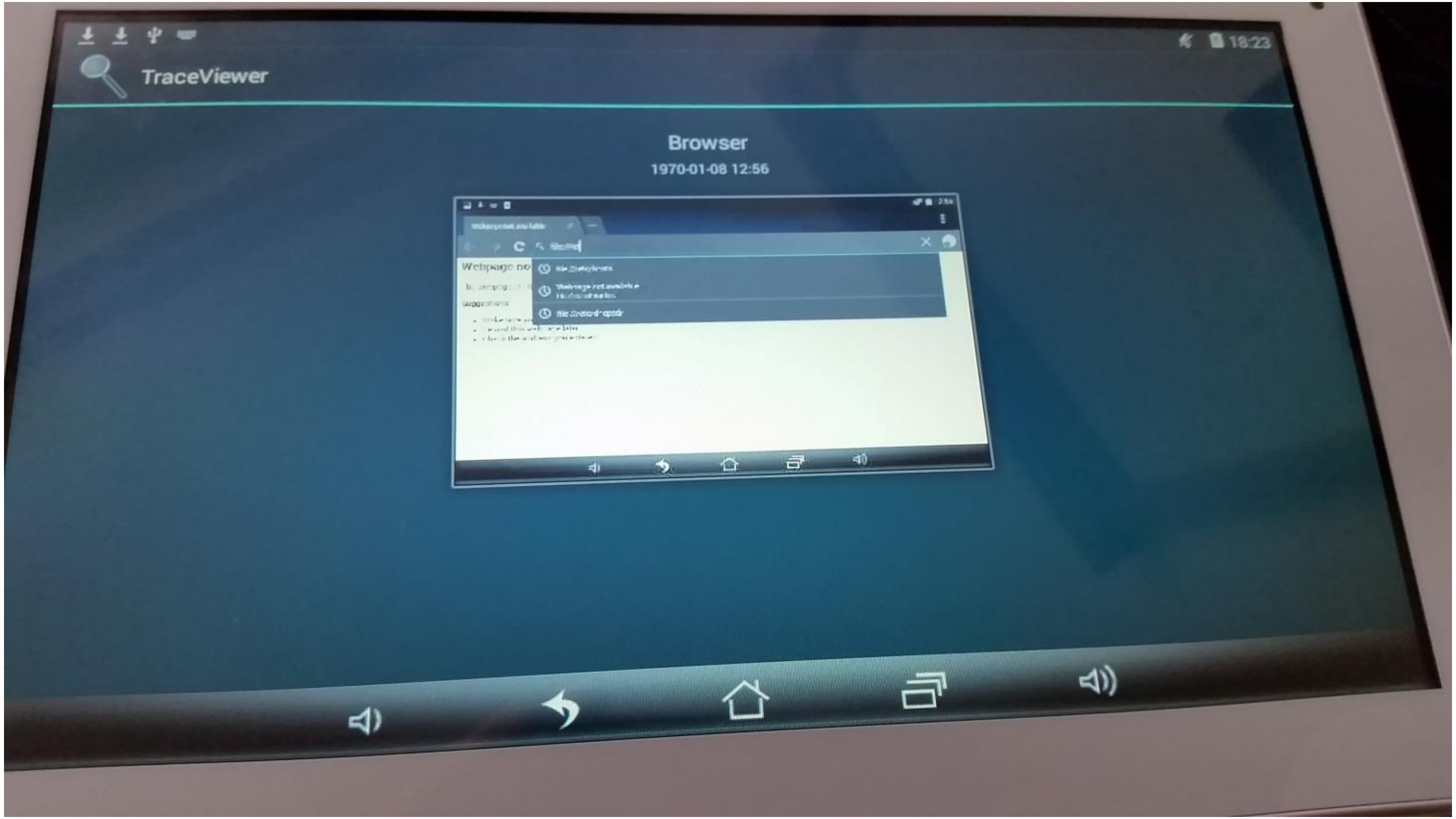
Rest of the world

Network-level Surveillance and Censorship

- Network is controlled by the government
- No Internet access for most users
- Route all traffic over central nodes/proxies
- Only a few government-owned Certificate Authorities

Human-level Surveillance

- Woolim includes TraceViewer
  - Take screenshots of apps
  - Records browser history
- Random physical inspections of mobile devices
  - Ranging from school teachers to members of special security units
  - Could identify inappropriate usage within minutes
- Prevents hiding impure files in removable media
  - Detecting inappropriate use is still possible if media will be removed
- Recorded histories and screenshots cannot be removed



TraceViewer

Browser

1970-01-08 12:56

Conclusions

Surveillance and Censorship

Source: https://www.zdf.de/assets/kim-jong-un-104~1920x1080

NO SPY

Surveillance and Censorship on Multiple Levels

- Network level
  - Government-controlled network
- Device level
  - Track distribution of media files via watermarks and signatures
  - Prevent distribution of media files with signatures
- Human level
  - Take screenshots and record browser histories
  - Make them easily accessible for random inspections via TraceViewer

How the Implementations Evolved

Red Star OS
2013

- Simple watermarking applied to media files
- Code for advanced watermarking (e.g. for audio filters) available, but not used.

Ryonghung
~2013

- Ported version of Red Star OS watermarking code (lots of similarities)
- Experimental version of signature checking available.

Woolim
~2015

- Same Red Star OS compatible code, but not used.
- Only advanced signature checking used

Thanks for Supporting our Research

- slipstream/RoL (@TheWack0lian)
  - For leaking the Red Star OS ISOs
- Will Scott (@willscott)
  - For translations and other information
- Iltaek
  - Translations
- ISFINK (www.isfink.org)
  - Freedom of Information in North Korea
  - Provided the tablet(s) -> Big thank you!

Future Work

- Dump of multiple devices (tablets and smartphones)
  - We don’t have access to these devices
- AntiVirus software

- Anybody got a smartphone from DPRK?
- Anybody got software from DPRK?
- “signed XP”?

→ We would love to take a look at more technology from DPRK!

Thank you for your Attention!

{fgrunow,nschiess}@ernw.de

@0x79
@_takeshix

www.ernw.de

www.insinuator.net