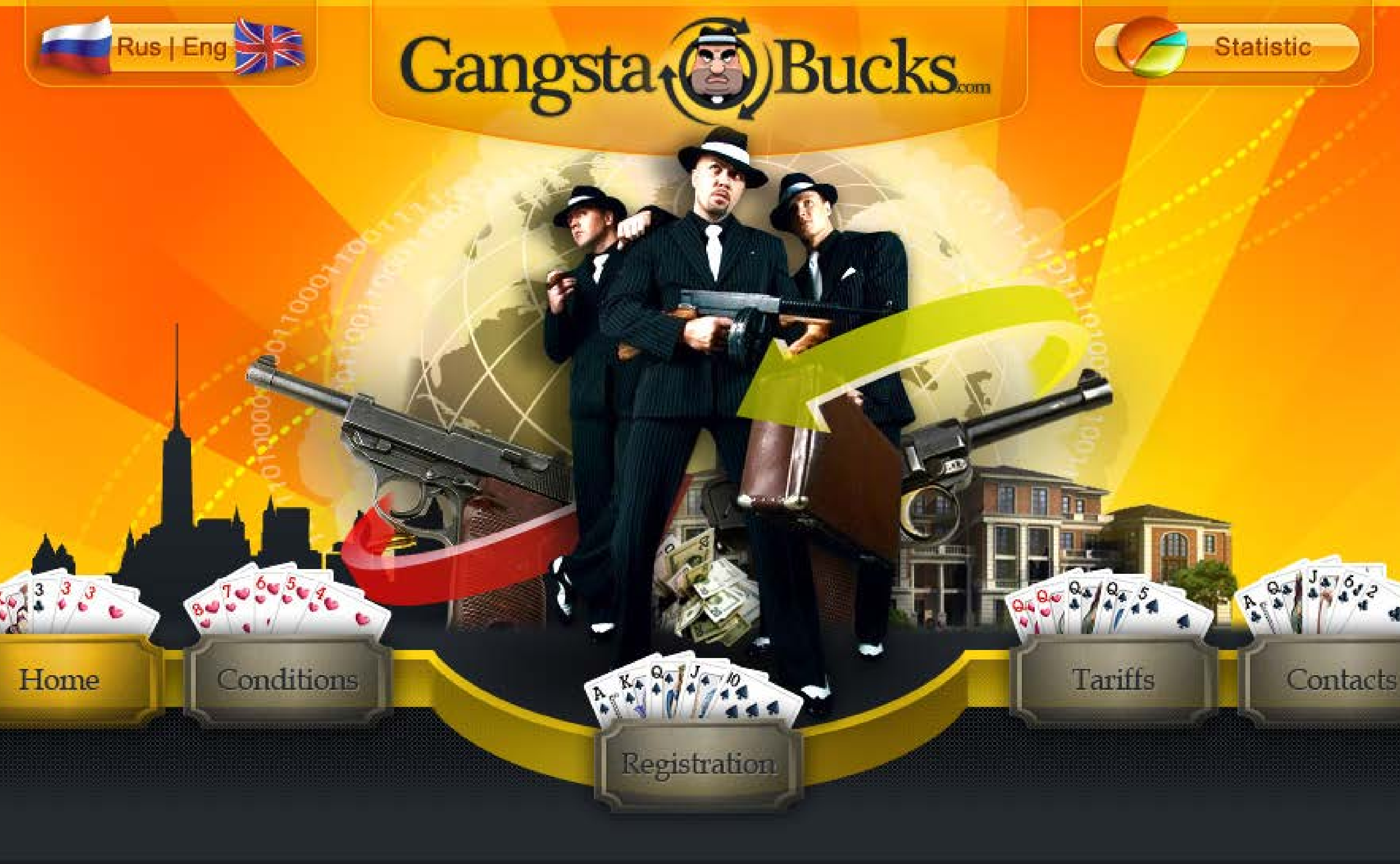
KEYNOTE
FIRST 2011

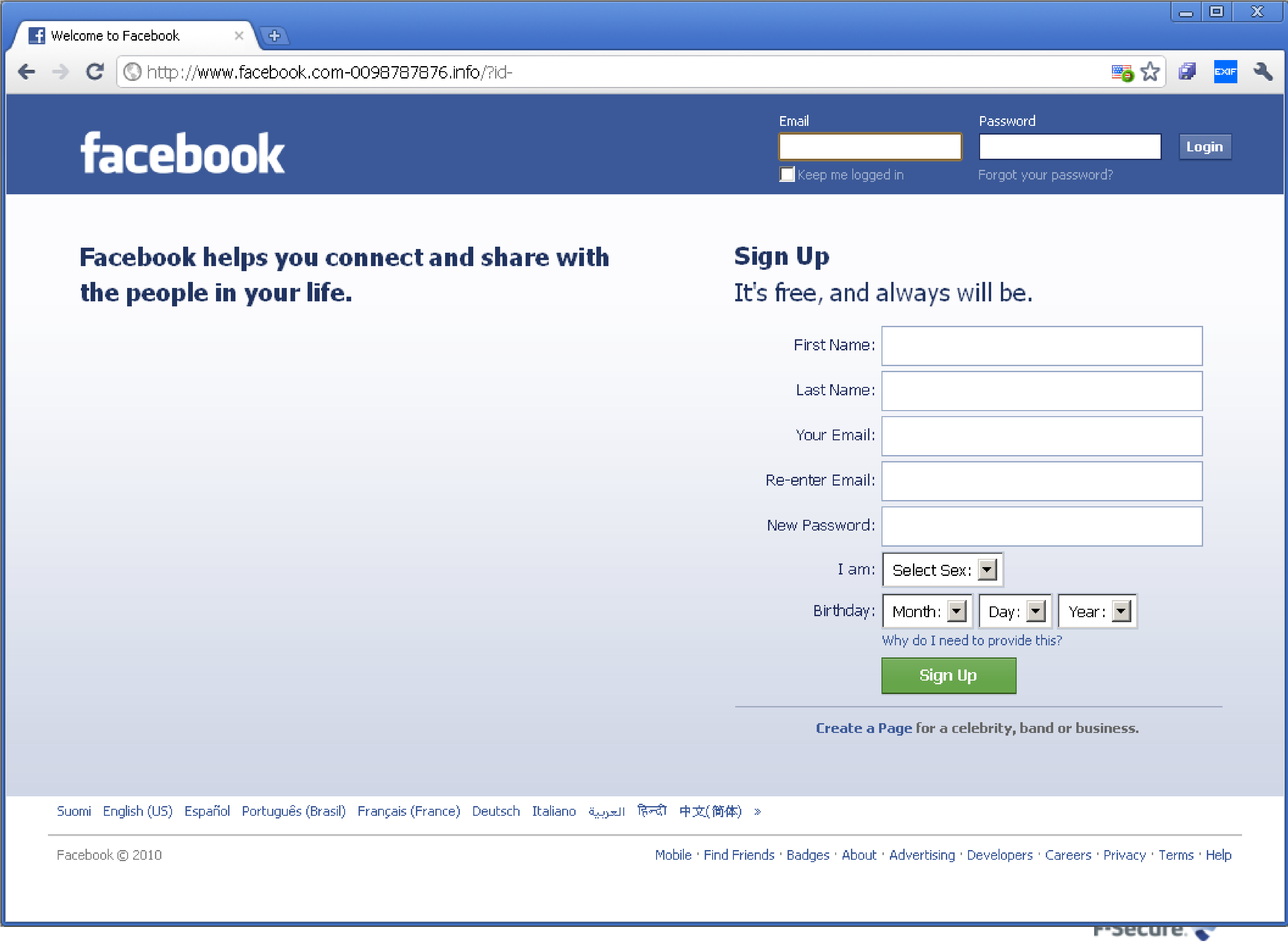
Mikko Hypponen
CRO
F-Secure Corp

BASF
Diskette Extra 5.25" · 2S/2D
Two sided · Double density
Sectors soft · 1ød/hole
Order code: Extra
5.25 2S/2D Plus
VIRUSVAARA!
Älä käytä!
BRAIN.A
Microsoft



GangstaBucks.com - it pays on time!
We pay for all installs!

facebook
December 2010



facebook

Email

Password

☐ Keep me logged in

Forgot your password?

Facebook helps you connect and share with the people in your life.

Sign Up

It's free, and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am:

Birthday:

Why do I need to provide this?

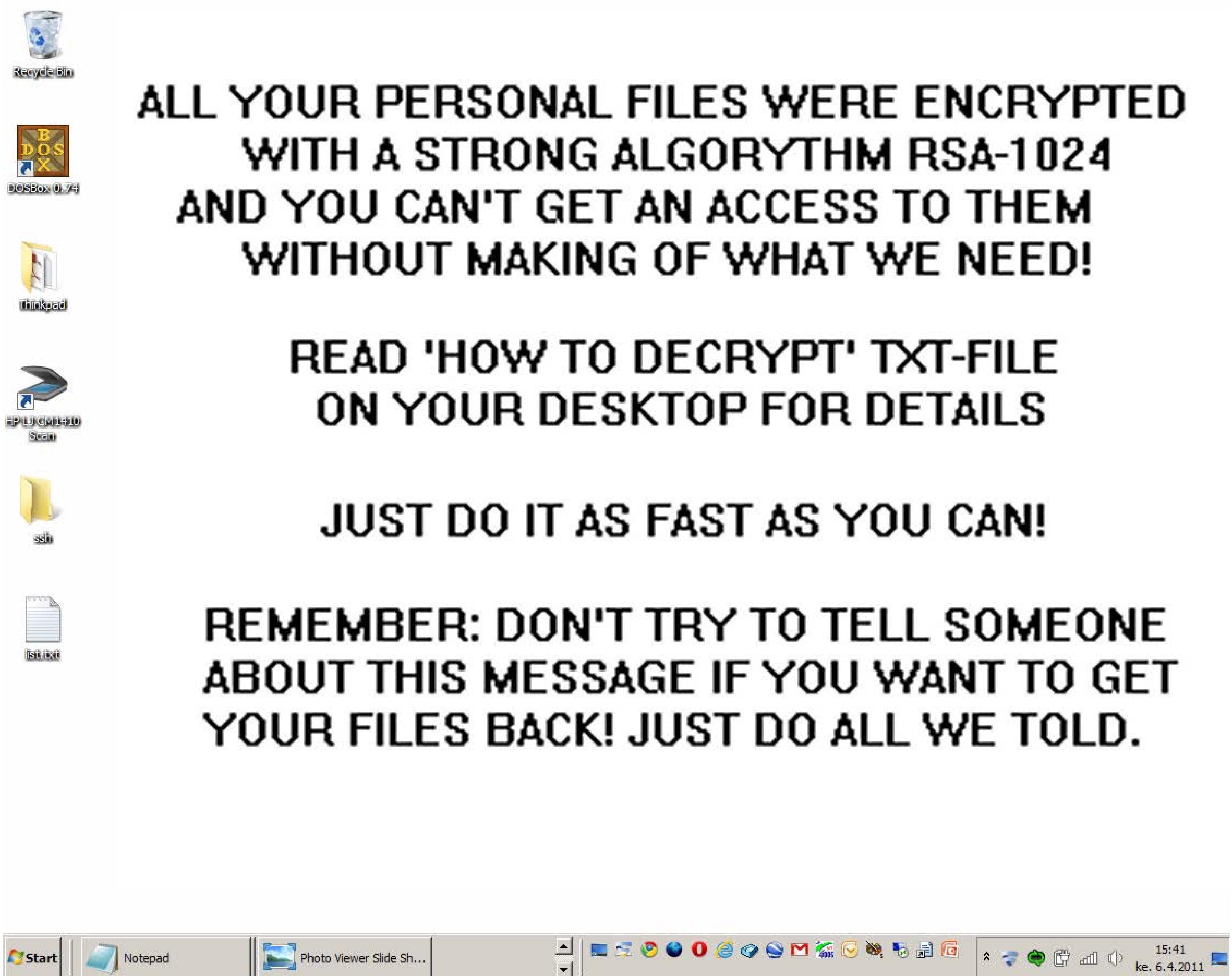
Create a Page for a celebrity, band or business.

Suomi English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) »

Facebook © 2010

Mobile · Find Friends · Badges · About · Advertising · Developers · Careers · Privacy · Terms · Help

RANSOM
TROJANS

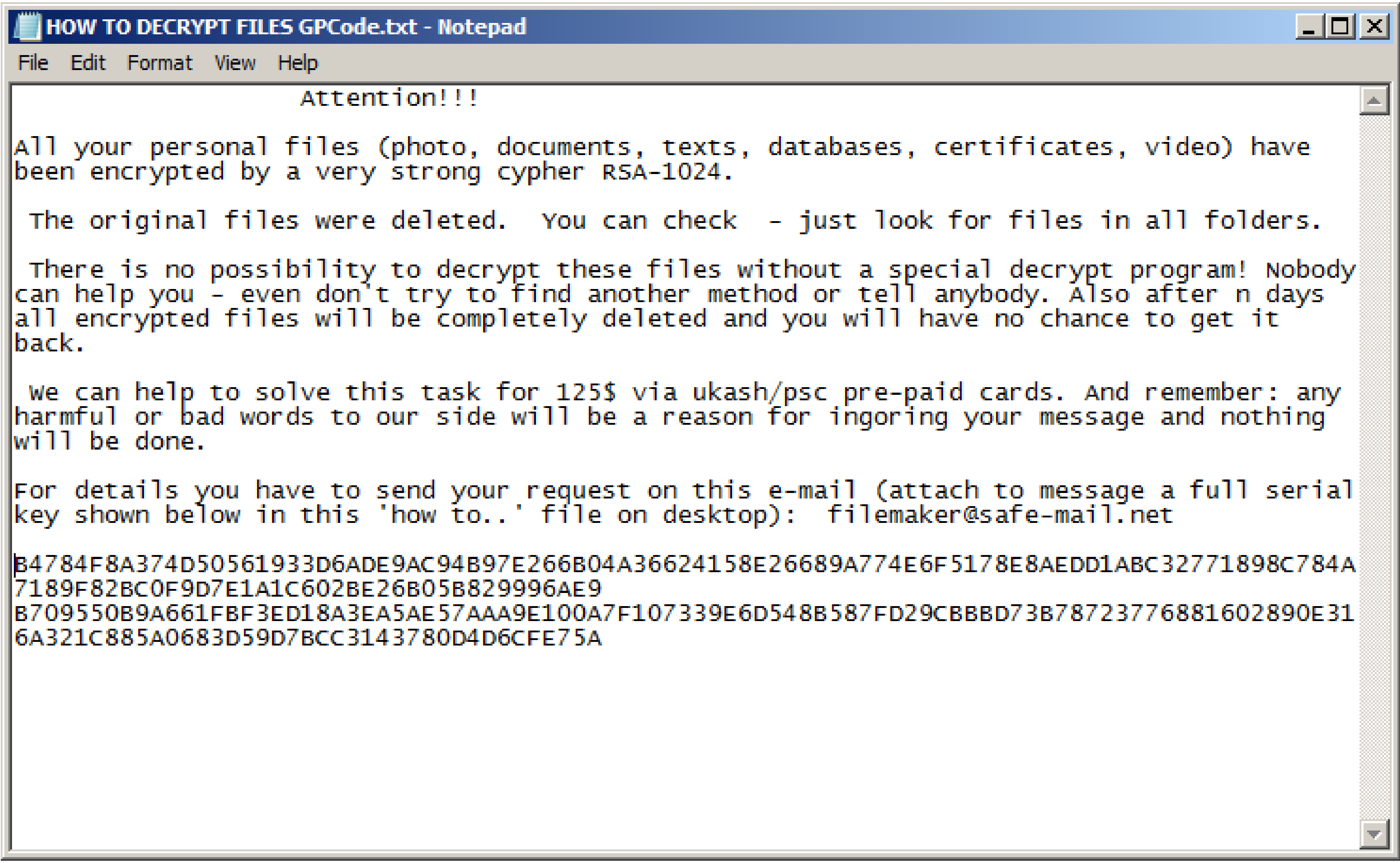


ALL YOUR PERSONAL FILES WERE ENCRYPTED
WITH A STRONG ALGORYTHM RSA-1024
AND YOU CAN'T GET AN ACCESS TO THEM
WITHOUT MAKING OF WHAT WE NEED!

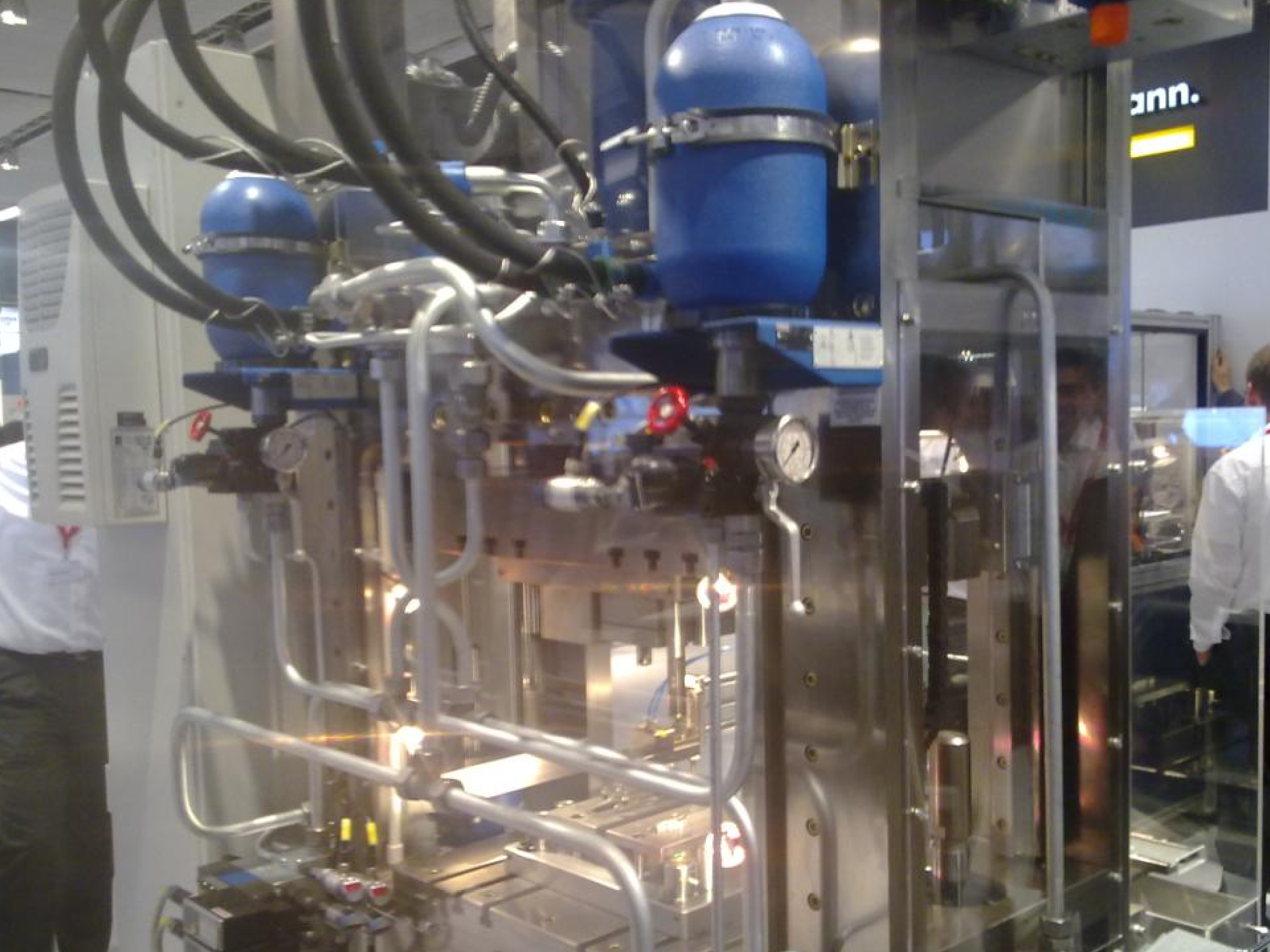
READ 'HOW TO DECRYPT' TXT-FILE
ON YOUR DESKTOP FOR DETAILS

JUST DO IT AS FAST AS YOU CAN!

REMEMBER: DON'T TRY TO TELL SOMEONE
ABOUT THIS MESSAGE IF YOU WANT TO GET
YOUR FILES BACK! JUST DO ALL WE TOLD.

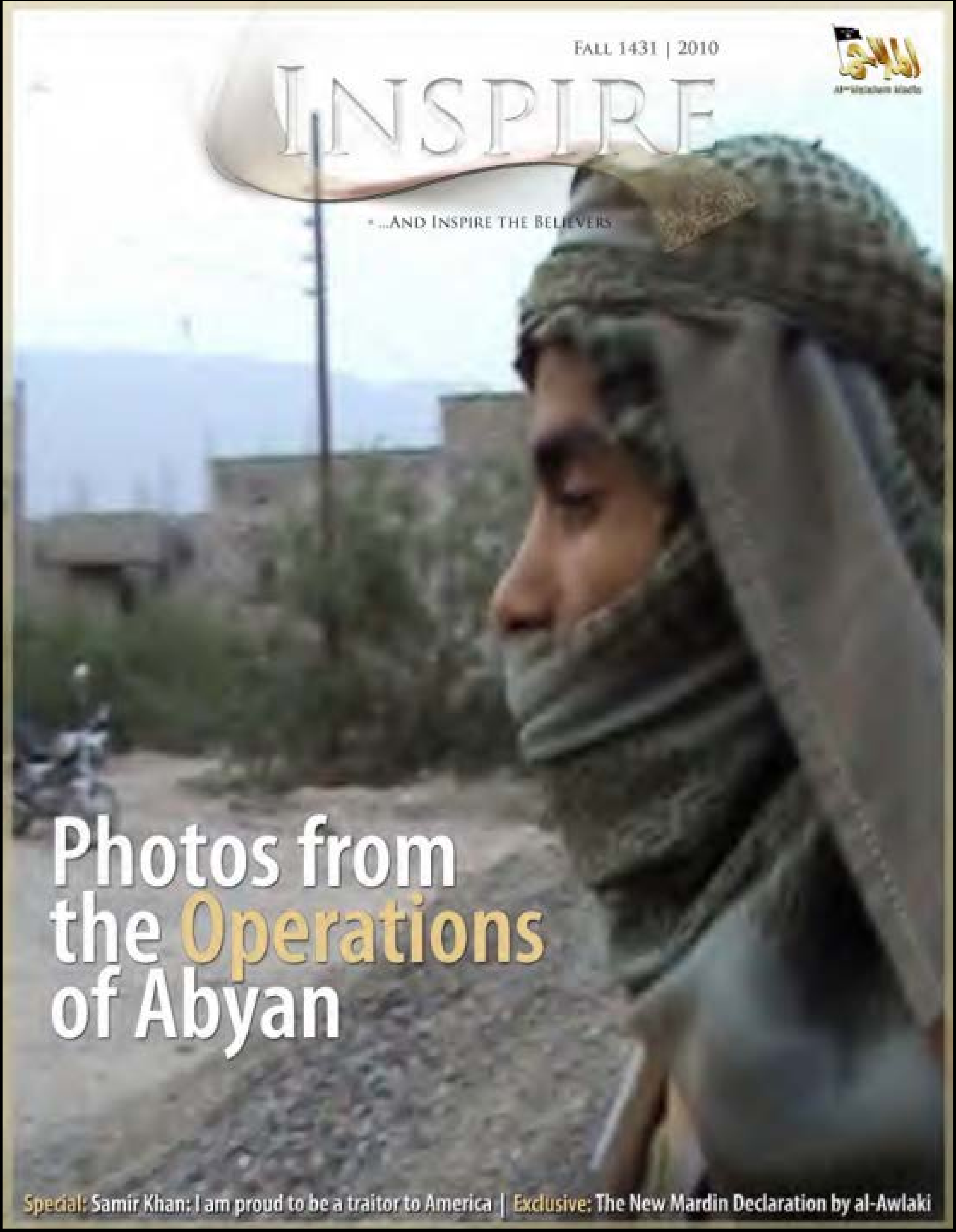


```
                   Attention!!!

All your personal files (photo, documents, texts, databases, certificates, video) have
been encrypted by a very strong cypher RSA-1024.

 The original files were deleted.  You can check  - just look for files in all folders.

 There is no possibility to decrypt these files without a special decrypt program! Nobody
can help you - even don't try to find another method or tell anybody. Also after n days
all encrypted files will be completely deleted and you will have no chance to get it
back.

 We can help to solve this task for 125$ via ukash/psc pre-paid cards. And remember: any
harmful or bad words to our side will be a reason for ingoring your message and nothing
will be done.

For details you have to send your request on this e-mail (attach to message a full serial
key shown below in this 'how to..' file on desktop):  filemaker@safe-mail.net

B4784F8A374D50561933D6ADE9AC94B97E266B04A36624158E26689A774E6F5178E8AEDD1ABC32771898C784A
7189F82BC0F9D7E1A1C602BE26B05B829996AE9
B709550B9A661FBF3ED18A3EA5AE57AAA9E100A7F107339E6D548B587FD29CBBBD73B787237768816028 90E31
6A321C885A0683D59D7BCC3143780D4D6CFE75A
```


ann.

SIEMENS
INTF
BAF
BATT1F
BATT2F
DC 5V
DC 24V
SIMATIC
S7-400
C S7-400
7-3
443-1 adv.
ATIC ET 200S
SIEMENS

CAUTION
CAUTION
VACON
CAUTION



Fall 1431 | 2010

Inspire

"...And Inspire the Believers"

Photos from the Operations of Abyan

Special: Samir Khan: I am proud to be a traitor to America | Exclusive: The New Mardin Declaration by al-Awlaki

THE DUST WILL NEVER SETTLE DOWN

LARS VILKS

FLEMMING ROSE

CARSTEN JUSTE

GIRT WILDERS

SALMAN RUSHDIE

KURT WESTERGAARD

AYAAN HIRSI ALI

ULF JOHANNSON

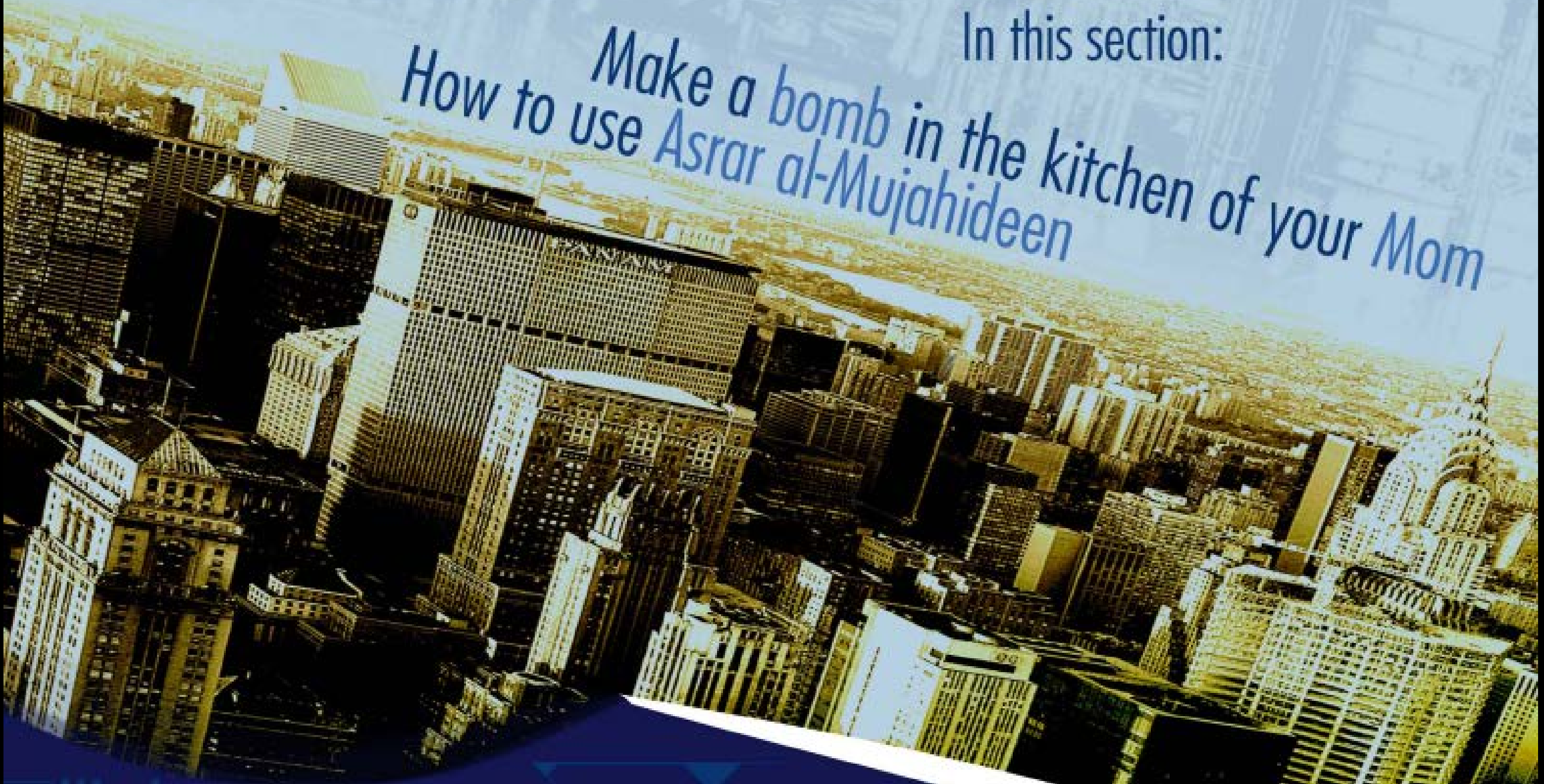
MOLLY NORRIS

Open Source Jihad

In this section:

Make a bomb in the kitchen of your Mom

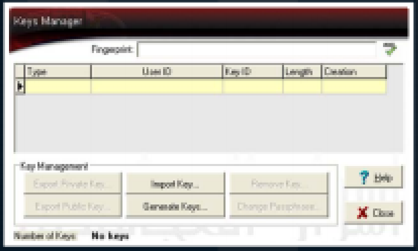
How to use Asrar al-Mujahideen



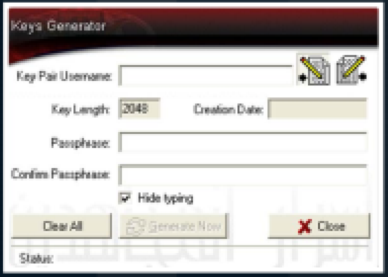
How to use Asrar al-Mujahideen: Sending & Receiving Encrypted Messages

Sending an important message in the old days only required a piece of paper, a writing utensil, and a trustworthy messenger that knows the location of the party you need to reach. Today, this is still an effective method if such a messenger is available and can get around without anyone stopping him. However, for the most part, this method has slowly evaporated and is now replaced with the Internet. Its benefit is that if there is no messenger that exists, access to the other party is only a few clicks of a mouse button away. Its harm is that the spies are actively paying attention to the Emails, especially if you are an individual that is known to be jihādī-minded. So how does one go about sending important messages without it being noticed by the enemy? Following is one method and that is by using an encryption software.

One such software is a program created by our brothers called Asrar al-Mujahideen 2.0. Here, we will discuss how to use this program, how to create your key, how to send and receive the public key of the other party, and how to check if your version of the software is forfeited or not. There are many things you can do with this program besides sending and receiving encrypted messages; we will cover those aspects in later issue, *In Shā’*



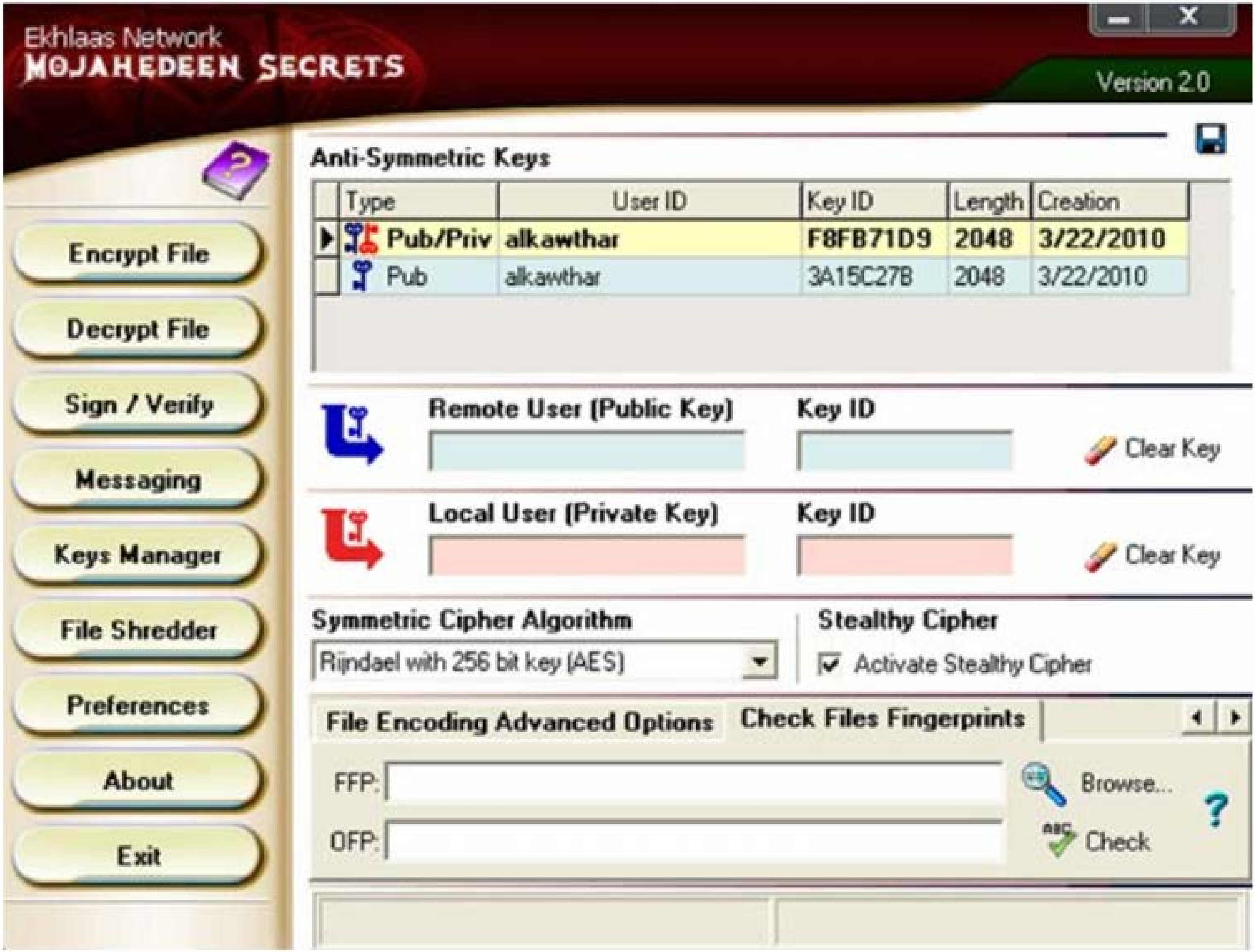
Number of Keys: No keys



Key Length: 2048

☑ Hide typing

In the first field, you type in your username that you would like to use; it has to be at least 5 characters. If you would like to use Arabic, you just have to click on the button to the far right to change the language. Then for the passphrase, enter in a password that is easy for you to remember, but difficult for anyone to figure out; it has to be at least 8



Anti-Symmetric Keys

Type	User ID	Key ID	Length	Creation
Pub/Priv	alkawthar	F8FB71D9	2048	3/22/2010
Pub	alkawthar	3A15C27B	2048	3/22/2010

Remote User (Public Key) | Key ID

Local User (Private Key) | Key ID

Symmetric Cipher Algorithm: Rijndael with 256 bit key (AES)

Stealthy Cipher: ☑ Activate Stealthy Cipher

FFP:

OFP:

﴿ وَأَعِدُّوا لَهُم مَّا اسْتَطَعْتُم مِّن قُوَّةٍ وَمِن رِّبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ ﴾

١

المجاهد التقني

العدد الأول - شهر ذو القعدة
سنة ١٤٢٧ هجرية

مجلة دورية تصدر عن مركز الفجر للإعلام

مركز الفجر للإعلام

المجلة تنشر حصريا في الحسبة والإخلاص والبراق والفردوس

4) التشغيل و التجارب

نعود ونكرر أن هذه العملية ليست للمبتدئين، وأن التشغيل في بعض الحالات قد يؤدي إلى مشاكل لا تُحمد عقباها.

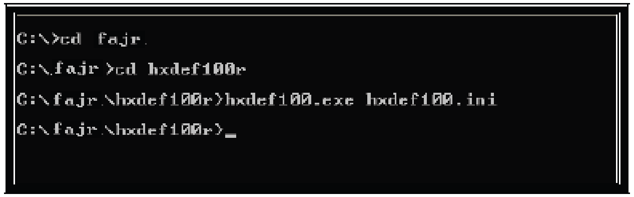
بعد إعداد ملف الخيارات كما هو موضّح في القسم السابق نكون جاهزين لمرحلة التشغيل.

a) تشغيل الملف

يتم باستخدام الأمر التالي :

hxdef100.exe [inifile]

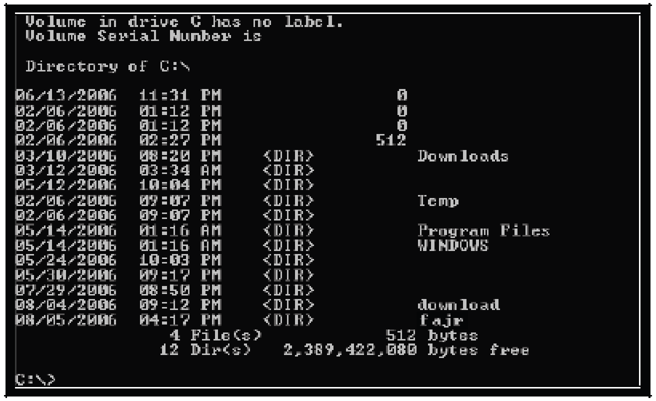
و الـــ **[inifile]** هو اسم ملف الإعدادات، وهنا في المثال المرفق اسمه **hxdef100.ini**



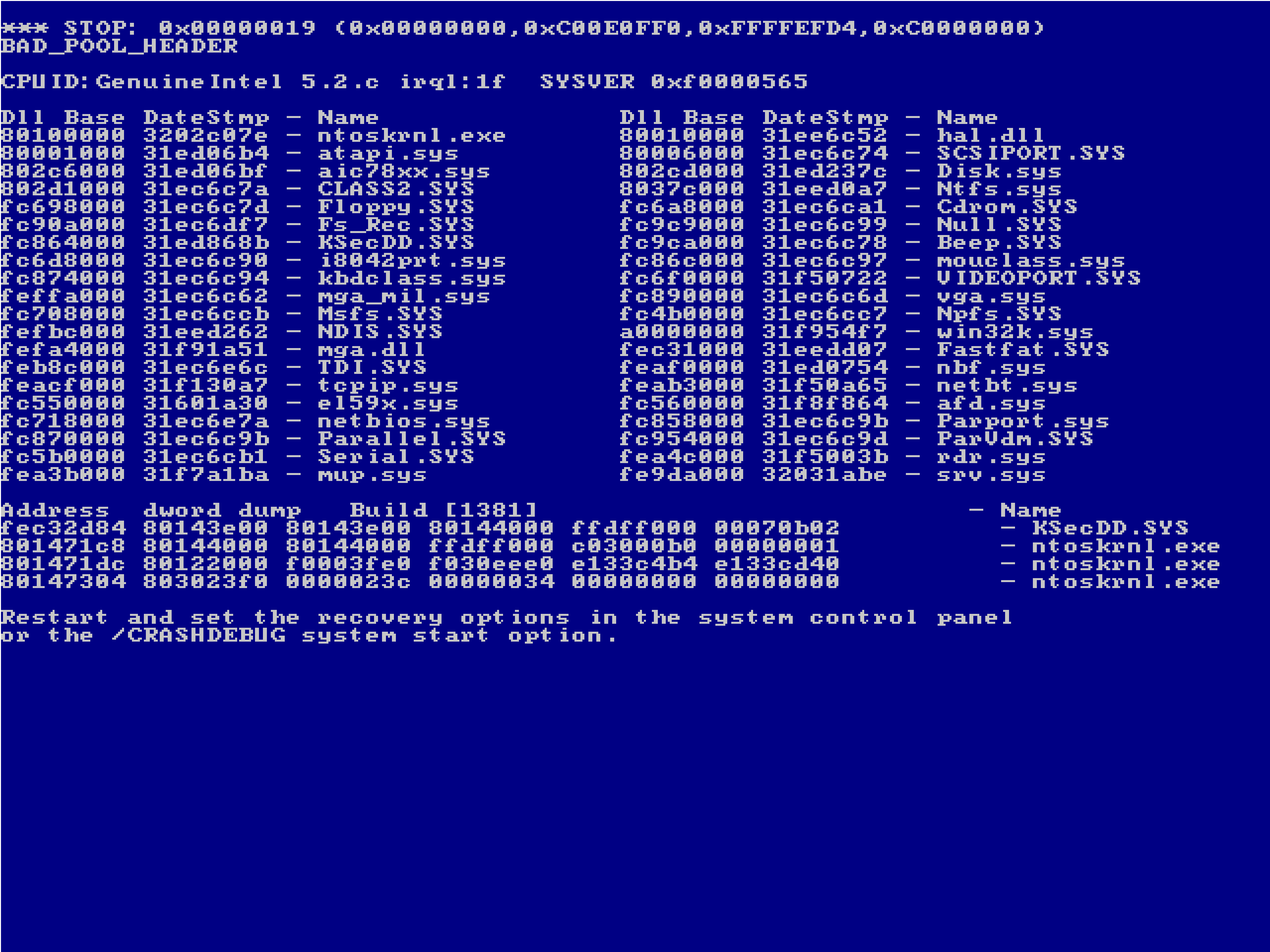
```
C:\>cd fajr
C:\fajr>cd hxdef100r
C:\fajr\hxdef100r>hxdef100.exe hxdef100.ini
C:\fajr\hxdef100r>_
```

b) نتائج ما بعد التشغيل

في هذه الصورة تظهر الملفات قبل الإخفاء :



```
 Volume in drive C has no label.
 Volume Serial Number is

 Directory of C:\

06/13/2006  11:31 PM                 0
02/06/2006  01:12 PM                 0
02/06/2006  01:12 PM                 0
02/06/2006  02:27 PM               512
03/10/2006  08:20 PM    <DIR>          Downloads
03/12/2006  03:34 AM    <DIR>
05/12/2006  10:04 PM    <DIR>
02/06/2006  09:07 PM    <DIR>          Temp
02/06/2006  09:07 PM    <DIR>
05/14/2006  01:16 AM    <DIR>          Program Files
05/14/2006  01:16 AM    <DIR>          WINDOWS
05/24/2006  10:03 PM    <DIR>
05/30/2006  09:17 PM    <DIR>
07/29/2006  08:50 PM    <DIR>
08/04/2006  09:12 PM    <DIR>          download
08/05/2006  04:17 PM    <DIR>          fajr
               4 File(s)            512 bytes
              12 Dir(s)   2,389,422,080 bytes free

C:\>
```



```
*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFEFD4,0xC0000000)
BAD_POOL_HEADER

CPUID:GenuineIntel 5.2.c irql:1f  SYSVER 0xf0000565

Dll Base DateStmp - Name               Dll Base DateStmp - Name
80100000 3202c07e - ntoskrnl.exe       80010000 31ee6c52 - hal.dll
80001000 31ed06b4 - atapi.sys          80006000 31ec6c74 - SCSIPORT.SYS
802c6000 31ed06bf - aic78xx.sys        802cd000 31ed237c - Disk.sys
802d1000 31ec6c7a - CLASS2.SYS         8037c000 31eed0a7 - Ntfs.sys
fc698000 31ec6c7d - Floppy.SYS         fc6a8000 31ec6ca1 - Cdrom.SYS
fc90a000 31ec6df7 - Fs_Rec.SYS         fc9c9000 31ec6c99 - Null.SYS
fc864000 31ed868b - KSecDD.SYS         fc9ca000 31ec6c78 - Beep.SYS
fc6d8000 31ec6c90 - i8042prt.sys       fc86c000 31ec6c97 - mouclass.sys
fc874000 31ec6c94 - kbdclass.sys       fc6f0000 31f50722 - VIDEOPORT.SYS
feffa000 31ec6c62 - mga_mil.sys        fc890000 31ec6c6d - vga.sys
fc708000 31ec6ccb - Msfs.SYS           fc4b0000 31ec6cc7 - Npfs.SYS
fefbc000 31eed262 - NDIS.SYS           a0000000 31f954f7 - win32k.sys
fefa4000 31f91a51 - mga.dll            fec31000 31eedd07 - Fastfat.SYS
feb8c000 31ec6e6c - TDI.SYS            feaf0000 31ed0754 - nbf.sys
feacf000 31f130a7 - tcpip.sys          feab3000 31f50a65 - netbt.sys
fc550000 31601a30 - el59x.sys          fc560000 31f8f864 - afd.sys
fc718000 31ec6e7a - netbios.sys        fc858000 31ec6c9b - Parport.sys
fc870000 31ec6c9b - Parallel.SYS       fc954000 31ec6c9d - ParVdm.SYS
fc5b0000 31ec6cb1 - Serial.SYS         fea4c000 31f5003b - rdr.sys
fea3b000 31f7a1ba - mup.sys            fe9da000 32031abe - srv.sys

Address  dword dump   Build [1381]                           - Name
fec32d84 80143e00 80143e00 80144000 ffdff000 00070b02          - KSecDD.SYS
801471c8 80144000 80144000 ffdff000 c03000b0 00000001          - ntoskrnl.exe
801471dc 80122000 f0003fe0 f030eee0 e133c4b4 e133cd40          - ntoskrnl.exe
80147304 803023f0 0000023c 00000034 00000000 00000000          - ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.
```

KEYNOTE FIRST 2011

Mikko Hypponen
CRO
F-Secure Corp