GAMERS, YOU'RE THE NEW BOTNETS

(MALWARE DETECTION FOR TEENAGERS)

Julie Gommes – A.K.A. JujuSete

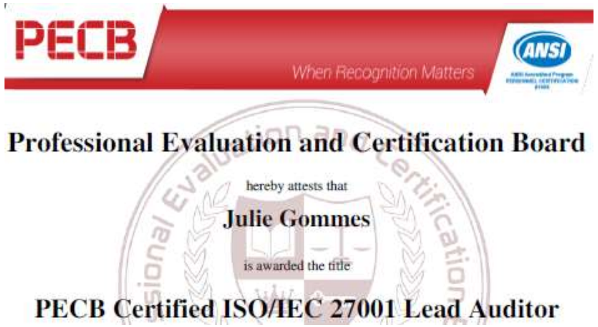
Owasp BENELUX 2016

March, 18th

WHO I AM

IT Security and governance consultant

- ❑ Risk analysis
- ❑ 27001 audits
- ❑ Risk management
- ❑ Security gap analysis



PECB

When Recognition Matters

ANSI

Professional Evaluation and Certification Board

hereby attests that

Julie Gommes

is awarded the title

PECB Certified ISO/IEC 27001 Lead Auditor

Find me there

Jujusete on IRC (freenode, geeknode, europnet…)

@JujuSete on Twitter

https://fr.linkedin.com/in/juliegommes

PREVIOUS TALKS, PAPERS AND TRAININGS

Cryptography and jihadism, from software to hardware

Hackfest – Quebec, november 16

DeepSec & Bsides – Vienna, november 16

How NGOs can encrypt their communication **- Ritimo** - Paris, Sept. 15

Social networks, practices and issues for NGOs - **Ritimo** - Paris, may 15

Free softwares, alternatives to Skype, google, Dropbox and others - **Ritimo** - Paris, may 15

Information Security for journalists

HITBSecConf – Amsterdam, may 14 / **DefCamp** – Bucarest, oct. 14 /

MRMCD – Darmstadt, sept. 14 / **PSES** – Paris, june 14 / ***NDH*** (Workshop) – Paris, june 14

Free software and (h)activism - **Ritimo** – feb. 2014

Social engineering for journalists - **NDH** – Paris, june 13 / ***Ubuntu Party*** – Paris, may 13

CONTENT

❑Aims of this talk

❑Disclaimer

❑Somewhere, there is a computer

❑What the hell your computer is doing without your permission ?

❑Where are your datas going ?

❑Your computer ? A botnet ?

❑Good practices for tomorrow

AIMS OF THIS TALK

❑I want young (o not so young) gamers to know how to check whether their computer is compromised using user friendly tools

❑I want them to be aware that best approaches to security exist

❑… And also i want to play with my own games

DISCLAIMER

- In France, the « illegal » downloading of a game protected by copiright can expose yourself to criminal sanctions.
- Sentence can be up to 3 years and 300,000 euros for penalty.

SOMEWHERE, A COMPUTER

One day, I found this computer in my living room.

It was soooooo many games cracked, downloaded via peer to peer conections

But this computer, <u>not mine</u>, was on MY network !!!

WHAT THE HELL YOUR COMPUTER IS DOING WITHOUT YOUR PERMISSION ?

BEFORE PLAYING

First step, istall wireshark

…

(yes, from offical website)

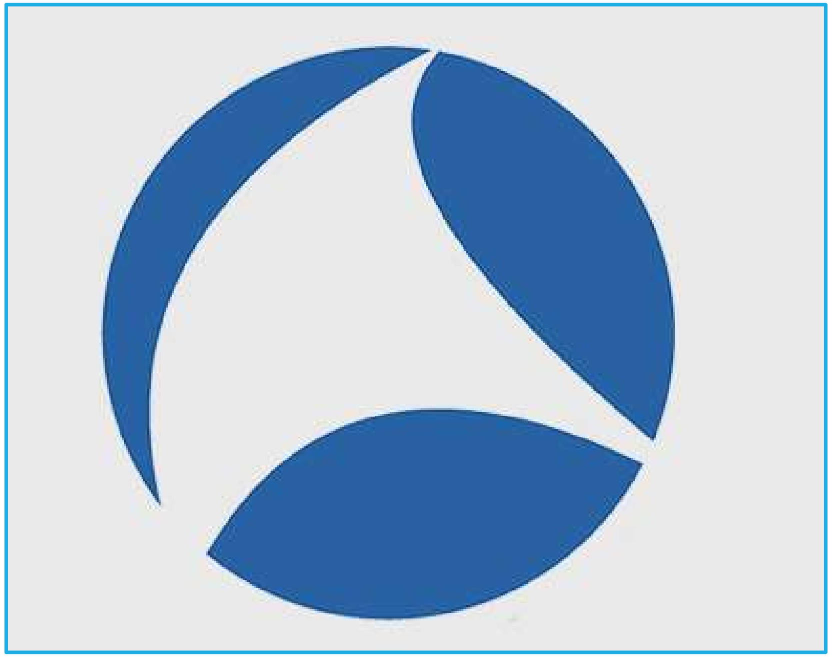
Then, stop applications that launch when your computer is starting.

…

(yes, all of them)

And restart your computer

LAUNCH WIRESHARK



Why wireshark ?

- ❑No need to use CLI,
- ❑User friendly for windows users

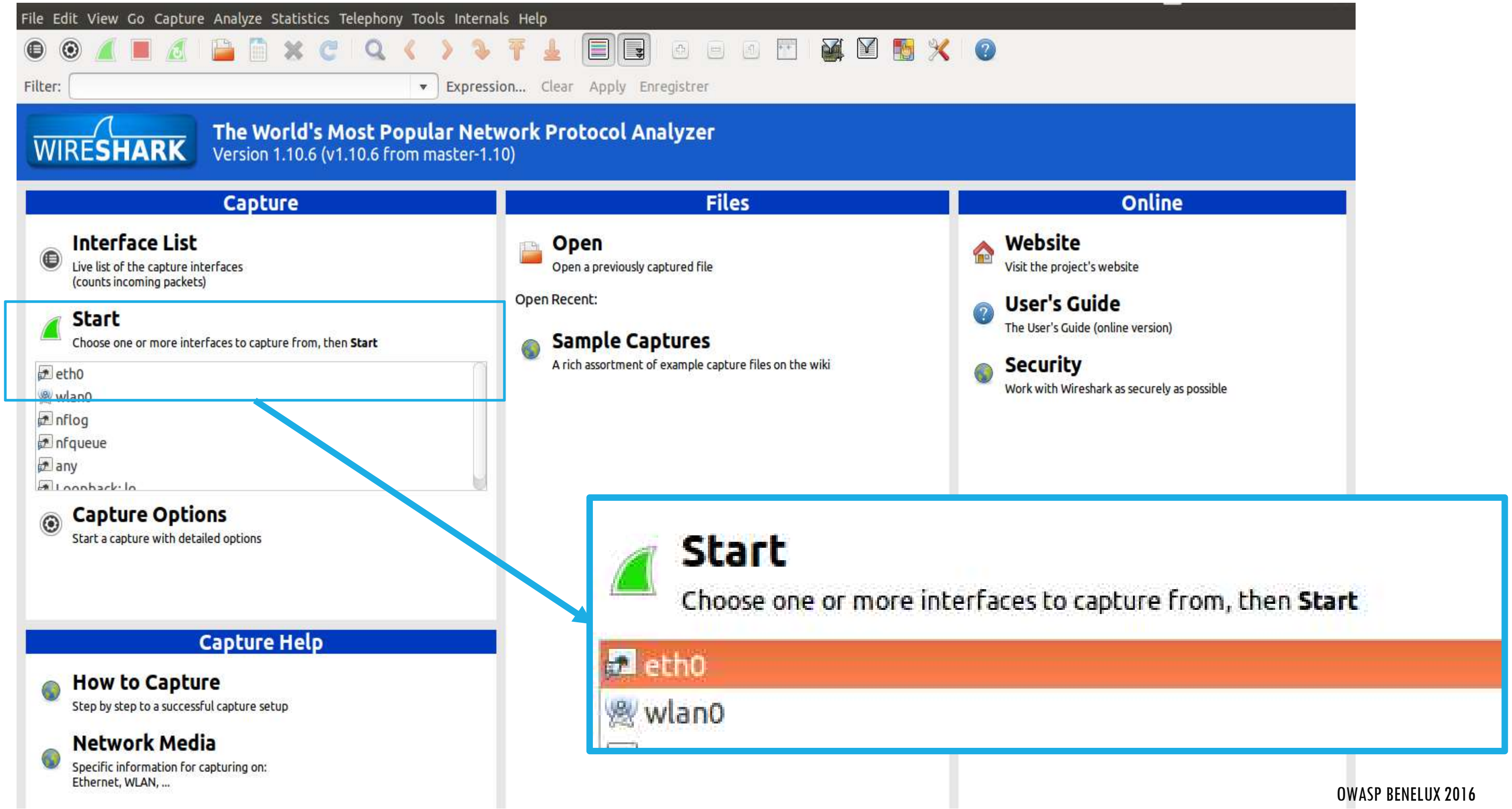
What is wireshark ?

- ❑Network packet analyzer

Why do you need to use it ?

- ❑This app will try to capture network packets and display thak packets as detailled as possible.

START WIRESHARK



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Enregistrer
WIRESHARK

The World's Most Popular Network Protocol Analyzer
Version 1.10.6 (v1.10.6 from master-1.10)

Capture

Interface List
Live list of the capture interfaces
(counts incoming packets)

Start
Choose one or more interfaces to capture from, then **Start**

eth0
wlan0
nflog
nfqueue
any
Loopback: lo

Capture Options
Start a capture with detailed options

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on:
Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wiki

Online

Website
Visit the project's website

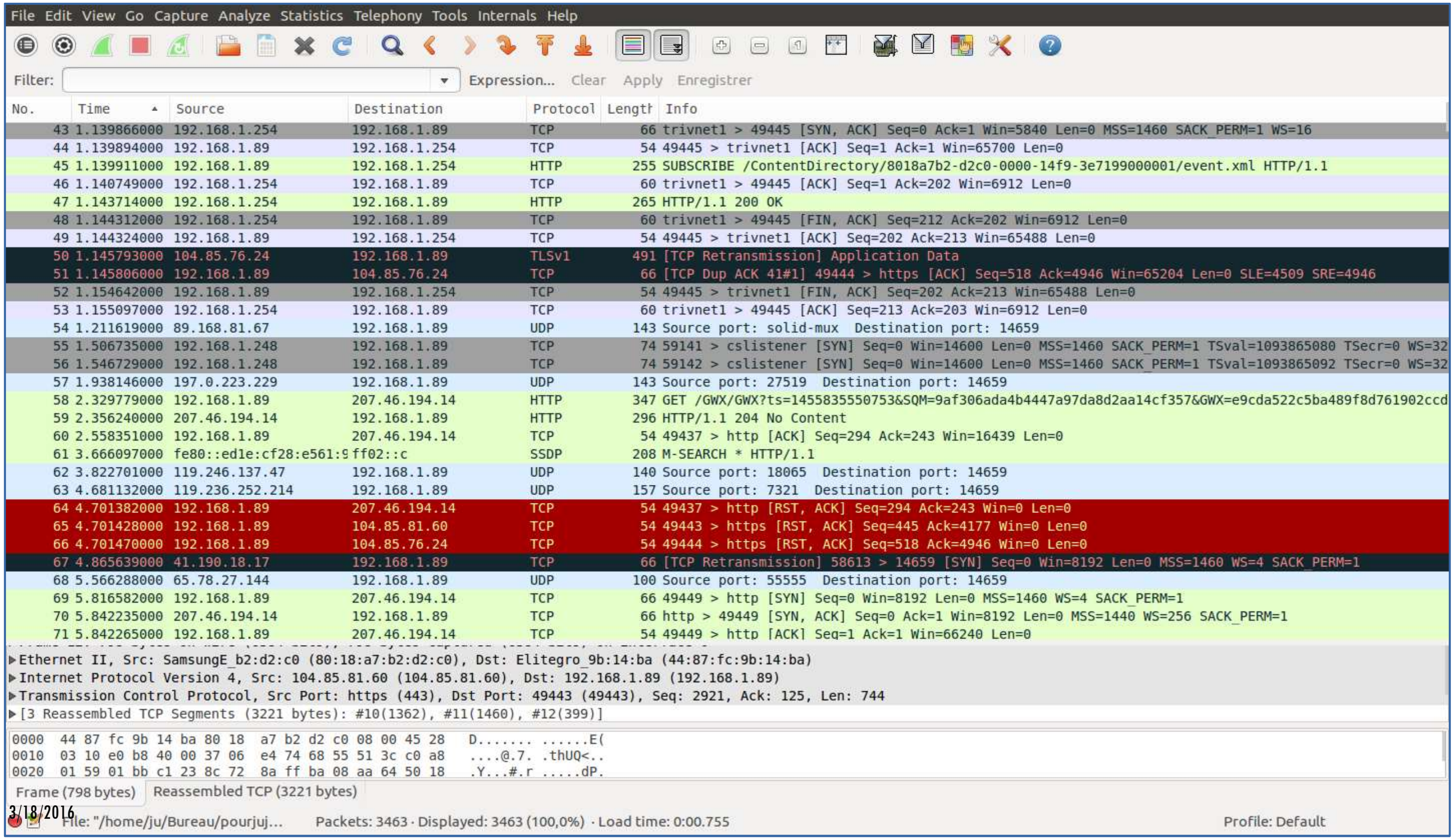
User's Guide
The User's Guide (online version)

Security
Work with Wireshark as securely as possible

Start
Choose one or more interfaces to capture from, then **Start**

eth0
wlan0

AFTER 13 MINUTES, 3463 CONNECTIONS


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Enregistrer

```
No.     Time          Source                Destination       Protocol Length Info
     43 1.139866000 192.168.1.254         192.168.1.89      TCP        66 trivnet1 > 49445 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=16
     44 1.139894000 192.168.1.89          192.168.1.254     TCP        54 49445 > trivnet1 [ACK] Seq=1 Ack=1 Win=65700 Len=0
     45 1.139911000 192.168.1.89          192.168.1.254     HTTP      255 SUBSCRIBE /ContentDirectory/8018a7b2-d2c0-0000-14f9-3e7199000001/event.xml HTTP/1.1
     46 1.140749000 192.168.1.254         192.168.1.89      TCP        60 trivnet1 > 49445 [ACK] Seq=1 Ack=202 Win=6912 Len=0
     47 1.143714000 192.168.1.254         192.168.1.89      HTTP      265 HTTP/1.1 200 OK
     48 1.144312000 192.168.1.254         192.168.1.89      TCP        60 trivnet1 > 49445 [FIN, ACK] Seq=212 Ack=202 Win=6912 Len=0
     49 1.144324000 192.168.1.89          192.168.1.254     TCP        54 49445 > trivnet1 [ACK] Seq=202 Ack=213 Win=65488 Len=0
     50 1.145793000 104.85.76.24          192.168.1.89      TLSv1     491 [TCP Retransmission] Application Data
     51 1.145806000 192.168.1.89          104.85.76.24      TCP        66 [TCP Dup ACK 41#1] 49444 > https [ACK] Seq=518 Ack=4946 Win=65204 Len=0 SLE=4509 SRE=4946
     52 1.154642000 192.168.1.89          192.168.1.254     TCP        54 49445 > trivnet1 [FIN, ACK] Seq=202 Ack=213 Win=65488 Len=0
     53 1.155097000 192.168.1.254         192.168.1.89      TCP        60 trivnet1 > 49445 [ACK] Seq=213 Ack=203 Win=6912 Len=0
     54 1.211619000 89.168.81.67          192.168.1.89      UDP       143 Source port: solid-mux  Destination port: 14659
     55 1.506735000 192.168.1.248         192.168.1.89      TCP        74 59141 > cslistener [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1093865080 TSecr=0 WS=32
     56 1.546729000 192.168.1.248         192.168.1.89      TCP        74 59142 > cslistener [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1093865092 TSecr=0 WS=32
     57 1.938146000 197.0.223.229         192.168.1.89      UDP       143 Source port: 27519  Destination port: 14659
     58 2.329779000 192.168.1.89          207.46.194.14     HTTP      347 GET /GWX/GWX?ts=1455835550753&SQM=9af306ada4b4447a97da8d2aa14cf357&GWX=e9cda522c5ba489f8d761902ccd
     59 2.356240000 207.46.194.14         192.168.1.89      HTTP      296 HTTP/1.1 204 No Content
     60 2.558351000 192.168.1.89          207.46.194.14     TCP        54 49437 > http [ACK] Seq=294 Ack=243 Win=16439 Len=0
     61 3.666097000 fe80::ed1e:cf28:e561:9 ff02::c          SSDP      208 M-SEARCH * HTTP/1.1
     62 3.822701000 119.246.137.47        192.168.1.89      UDP       140 Source port: 18065  Destination port: 14659
     63 4.681132000 119.236.252.214       192.168.1.89      UDP       157 Source port: 7321  Destination port: 14659
     64 4.701382000 192.168.1.89          207.46.194.14     TCP        54 49437 > http [RST, ACK] Seq=294 Ack=243 Win=0 Len=0
     65 4.701428000 192.168.1.89          104.85.81.60      TCP        54 49443 > https [RST, ACK] Seq=445 Ack=4177 Win=0 Len=0
     66 4.701470000 192.168.1.89          104.85.76.24      TCP        54 49444 > https [RST, ACK] Seq=518 Ack=4946 Win=0 Len=0
     67 4.865639000 41.190.18.17          192.168.1.89      TCP        66 [TCP Retransmission] 58613 > 14659 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     68 5.566288000 65.78.27.144          192.168.1.89      UDP       100 Source port: 55555  Destination port: 14659
     69 5.816582000 192.168.1.89          207.46.194.14     TCP        66 49449 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     70 5.842235000 207.46.194.14         192.168.1.89      TCP        66 http > 49449 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
     71 5.842265000 192.168.1.89          207.46.194.14     TCP        54 49449 > http [ACK] Seq=1 Ack=1 Win=66240 Len=0

▶Ethernet II, Src: SamsungE_b2:d2:c0 (80:18:a7:b2:d2:c0), Dst: Elitegro_9b:14:ba (44:87:fc:9b:14:ba)
▶Internet Protocol Version 4, Src: 104.85.81.60 (104.85.81.60), Dst: 192.168.1.89 (192.168.1.89)
▶Transmission Control Protocol, Src Port: https (443), Dst Port: 49443 (49443), Seq: 2921, Ack: 125, Len: 744
▶[3 Reassembled TCP Segments (3221 bytes): #10(1362), #11(1460), #12(399)]

0000  44 87 fc 9b 14 ba 80 18  a7 b2 d2 c0 08 00 45 28   D....... ......E(
0010  03 10 e0 b8 40 00 37 06  e4 74 68 55 51 3c c0 a8   ....@.7. .thUQ<..
0020  01 59 01 bb c1 23 8c 72  8a ff ba 08 aa 64 50 18   .Y...#.r .....dP.
```

File: "/home/ju/Bureau/pourjuj... Packets: 3463 · Displayed: 3463 (100,0%) · Load time: 0:00.755 Profile: Default

HOW TO USE THAT ?

Let’s play with all those IP adresses you just discovered befor to play with the informations…

If you’re not travelling, your datas could be good guides.

If you’re not using command line, you can connect to https://www.whois.net/ and try to figure out where those IP adresses come from.

Ready for a world trip ?

WHERE ARE YOUR DATAS GOING ?

WELCOME TO THE WORLD!

🇵🇱 83.23.44.147 Poland

🇷🇴 188.27.116.117 Romania, Bucharest DC (port 21228)

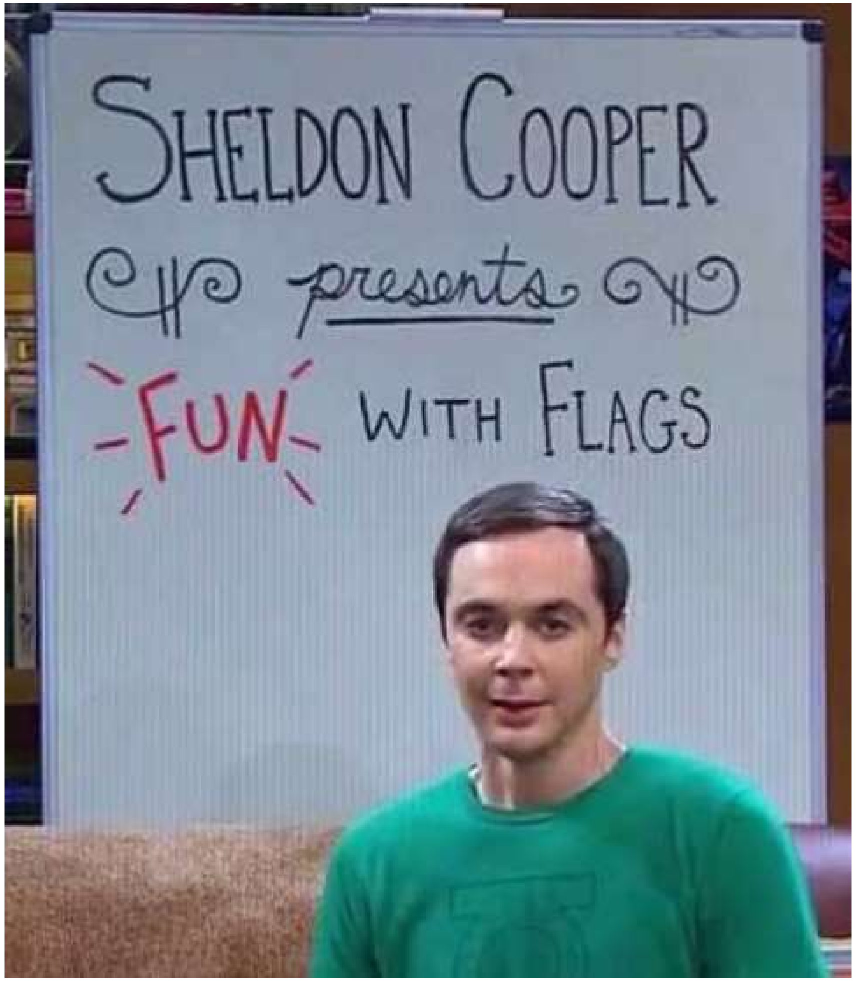
🇷🇺 176.226.129.185 Intersvyaz
JSC Network Operation Center, Russia (port 6881)

🇹🇷 92.45.227.153 Ankara, Turquie (port 14659)

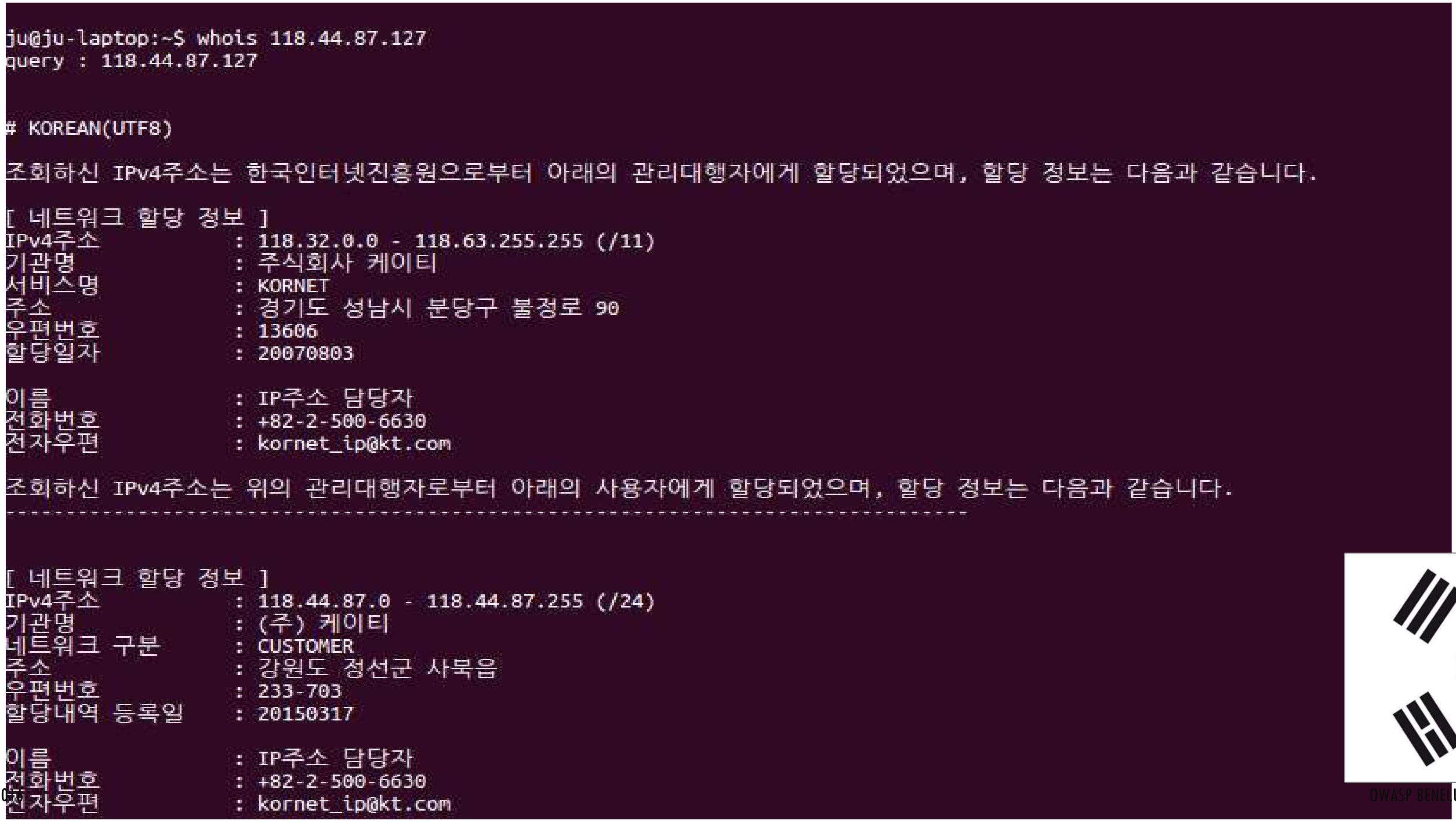
🇬🇧 90.215.255.255 London (port 14659)

🇯🇵 180.220.246.102 Japan

🇪🇪 85.253.105.245 Estonia (port 14659)

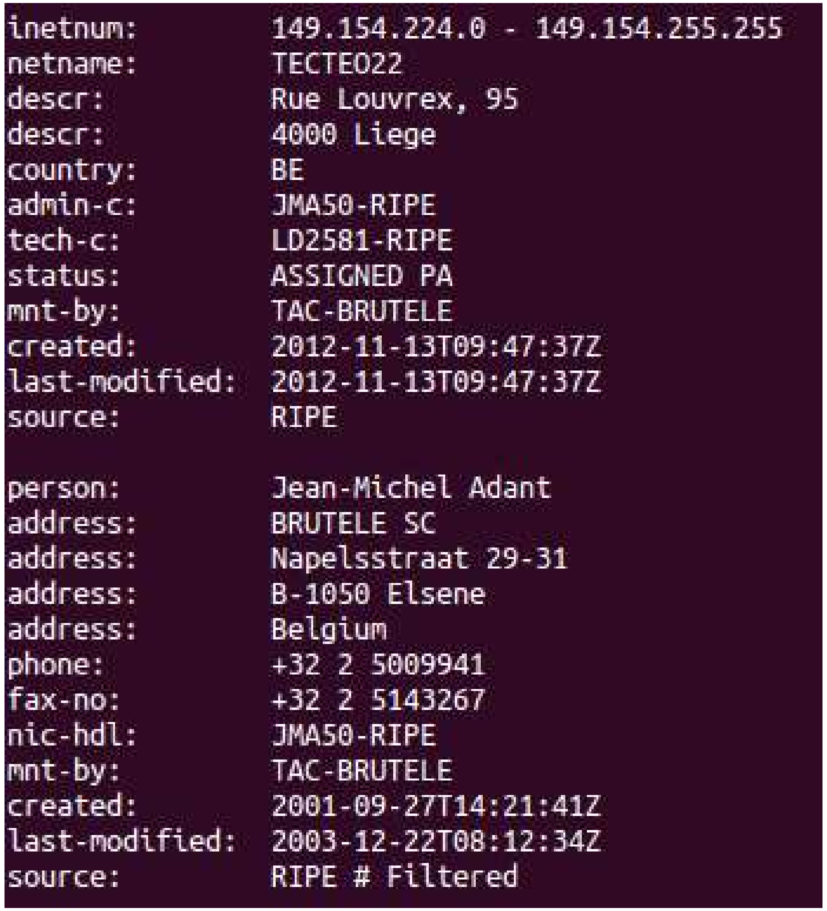


118.44.87.127   WELCOME TO KOREA!



```
ju@ju-laptop:~$ whois 118.44.87.127
query : 118.44.87.127


# KOREAN(UTF8)

조회하신 IPv4주소는 한국인터넷진흥원으로부터 아래의 관리대행자에게 할당되었으며, 할당 정보는 다음과 같습니다.

[ 네트워크 할당 정보 ]
IPv4주소           : 118.32.0.0 - 118.63.255.255 (/11)
기관명             : 주식회사 케이티
서비스명           : KORNET
주소               : 경기도 성남시 분당구 불정로 90
우편번호           : 13606
할당일자           : 20070803

이름               : IP주소 담당자
전화번호           : +82-2-500-6630
전자우편           : kornet_ip@kt.com

조회하신 IPv4주소는 위의 관리대행자로부터 아래의 사용자에게 할당되었으며, 할당 정보는 다음과 같습니다.
--------------------------------------------------------------------------------


[ 네트워크 할당 정보 ]
IPv4주소           : 118.44.87.0 - 118.44.87.255 (/24)
기관명             : (주) 케이티
네트워크 구분      : CUSTOMER
주소               : 강원도 정선군 사북읍
우편번호           : 233-703
할당내역 등록일    : 20150317

이름               : IP주소 담당자
전화번호           : +82-2-500-6630
전자우편           : kornet_ip@kt.com
```

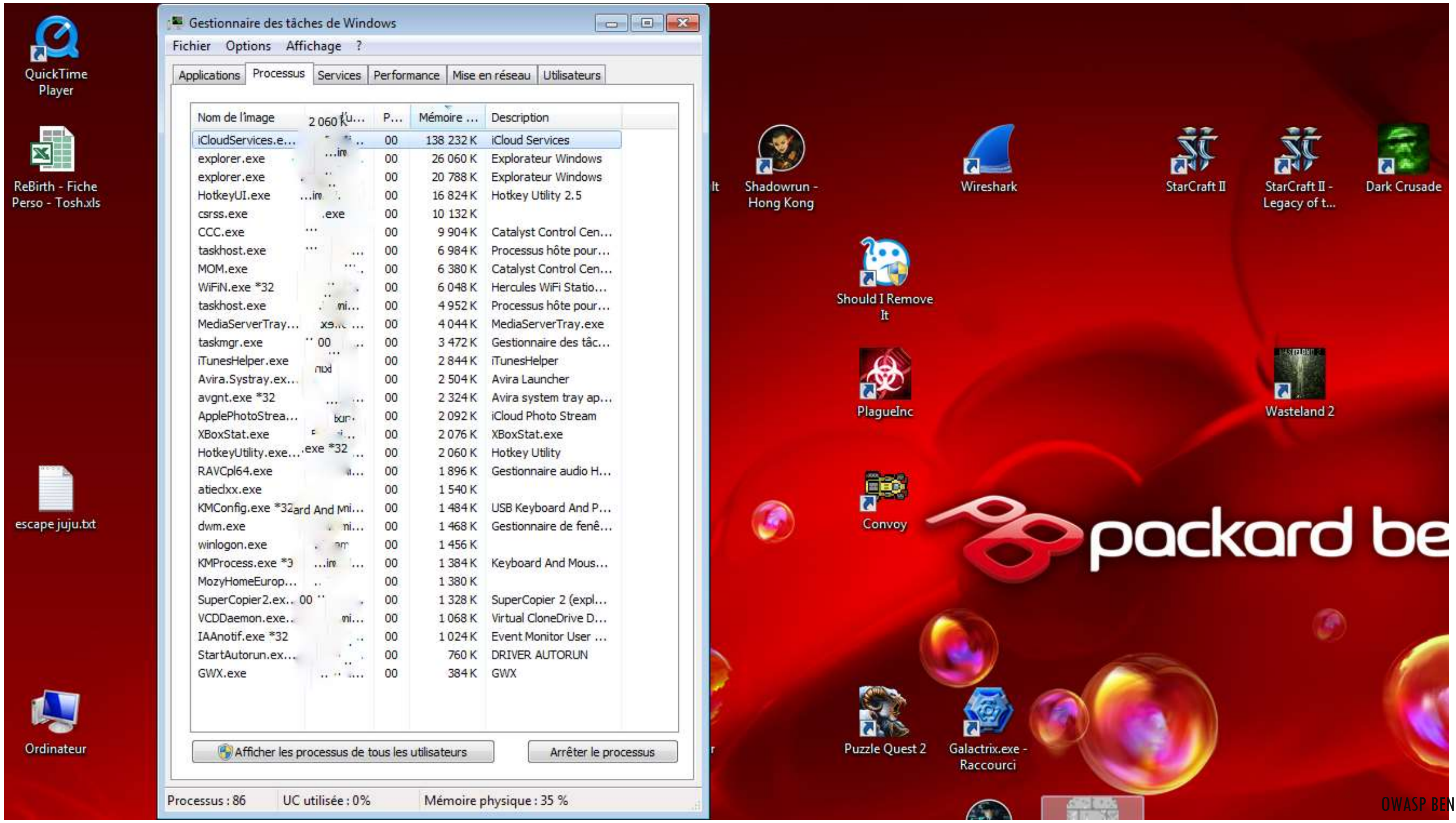
149.154.224.15
OUR FAVORITE NEIGHBOUR!



```
inetnum:        149.154.224.0 - 149.154.255.255
netname:        TECTEO22
descr:          Rue Louvrex, 95
descr:          4000 Liege
country:        BE
admin-c:        JMA50-RIPE
tech-c:         LD2581-RIPE
status:         ASSIGNED PA
mnt-by:         TAC-BRUTELE
created:        2012-11-13T09:47:37Z
last-modified:  2012-11-13T09:47:37Z
source:         RIPE

person:         Jean-Michel Adant
address:        BRUTELE SC
address:        Napelsstraat 29-31
address:        B-1050 Elsene
address:        Belgium
phone:          +32 2 5009941
fax-no:         +32 2 5143267
nic-hdl:        JMA50-RIPE
mnt-by:         TAC-BRUTELE
created:        2001-09-27T14:21:41Z
last-modified:  2003-12-22T08:12:34Z
source:         RIPE # Filtered
```

MY COMPUTER ? A BOTNET ?

LET'S CHECK AT THE PROCESSES

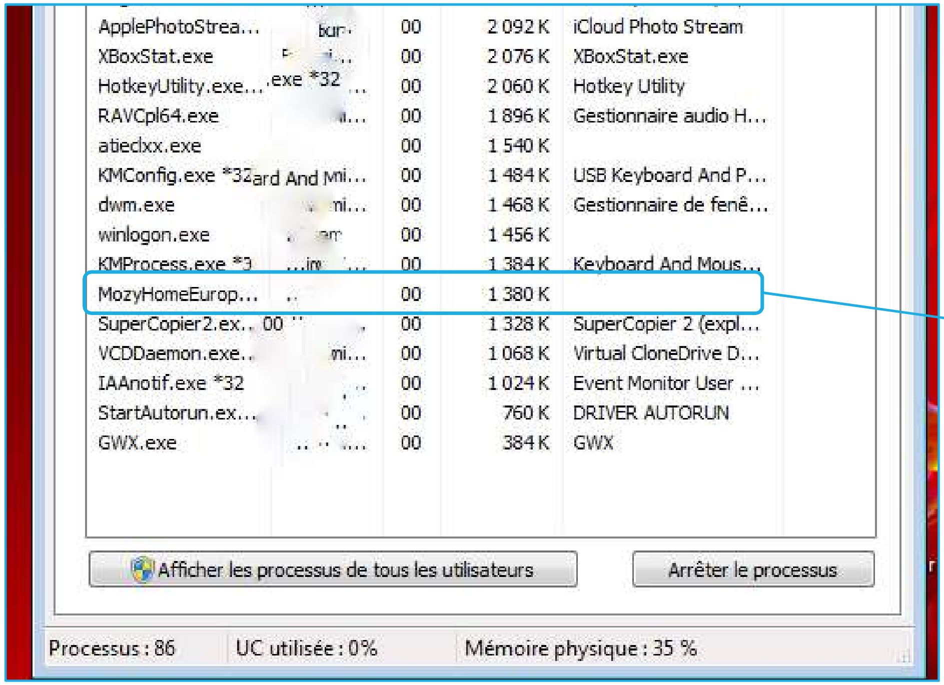


Gestionnaire des tâches de Windows

Nom de l'image	U...	P...	Mémoire ...	Description
iCloudServices.e...	[redacted]	00	138 232 K	iCloud Services
explorer.exe	[redacted]	00	26 060 K	Explorateur Windows
explorer.exe	[redacted]	00	20 788 K	Explorateur Windows
HotkeyUI.exe	[redacted]	00	16 824 K	Hotkey Utility 2.5
csrss.exe	[redacted]	00	10 132 K	
CCC.exe	[redacted]	00	9 904 K	Catalyst Control Cen...
taskhost.exe	[redacted]	00	6 984 K	Processus hôte pour...
MOM.exe	[redacted]	00	6 380 K	Catalyst Control Cen...
WiFiN.exe *32	[redacted]	00	6 048 K	Hercules WiFi Statio...
taskhost.exe	[redacted]	00	4 952 K	Processus hôte pour...
MediaServerTray...	[redacted]	00	4 044 K	MediaServerTray.exe
taskmgr.exe	[redacted]	00	3 472 K	Gestionnaire des tâc...
iTunesHelper.exe	[redacted]	00	2 844 K	iTunesHelper
Avira.Systray.ex...	[redacted]	00	2 504 K	Avira Launcher
avgnt.exe *32	[redacted]	00	2 324 K	Avira system tray ap...
ApplePhotoStrea...	[redacted]	00	2 092 K	iCloud Photo Stream
XBoxStat.exe	[redacted]	00	2 076 K	XBoxStat.exe
HotkeyUtility.exe...	[redacted]	00	2 060 K	Hotkey Utility
RAVCpl64.exe	[redacted]	00	1 896 K	Gestionnaire audio H...
atiedxx.exe	[redacted]	00	1 540 K	
KMConfig.exe *32	[redacted]	00	1 484 K	USB Keyboard And P...
dwm.exe	[redacted]	00	1 468 K	Gestionnaire de fenê...
winlogon.exe	[redacted]	00	1 456 K	
KMProcess.exe *3	[redacted]	00	1 384 K	Keyboard And Mous...
MozyHomeEurop...	[redacted]	00	1 380 K	
SuperCopier2.ex...	[redacted]	00	1 328 K	SuperCopier 2 (expl...
VCDDaemon.exe...	[redacted]	00	1 068 K	Virtual CloneDrive D...
IAAnotif.exe *32	[redacted]	00	1 024 K	Event Monitor User ...
StartAutorun.ex...	[redacted]	00	760 K	DRIVER AUTORUN
GWX.exe	[redacted]	00	384 K	GWX

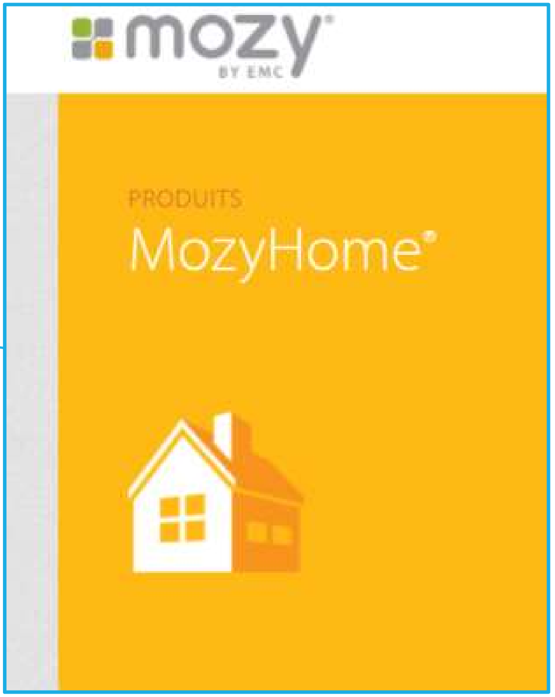
Processus : 86 UC utilisée : 0% Mémoire physique : 35 %

MOZY HOME EUROP

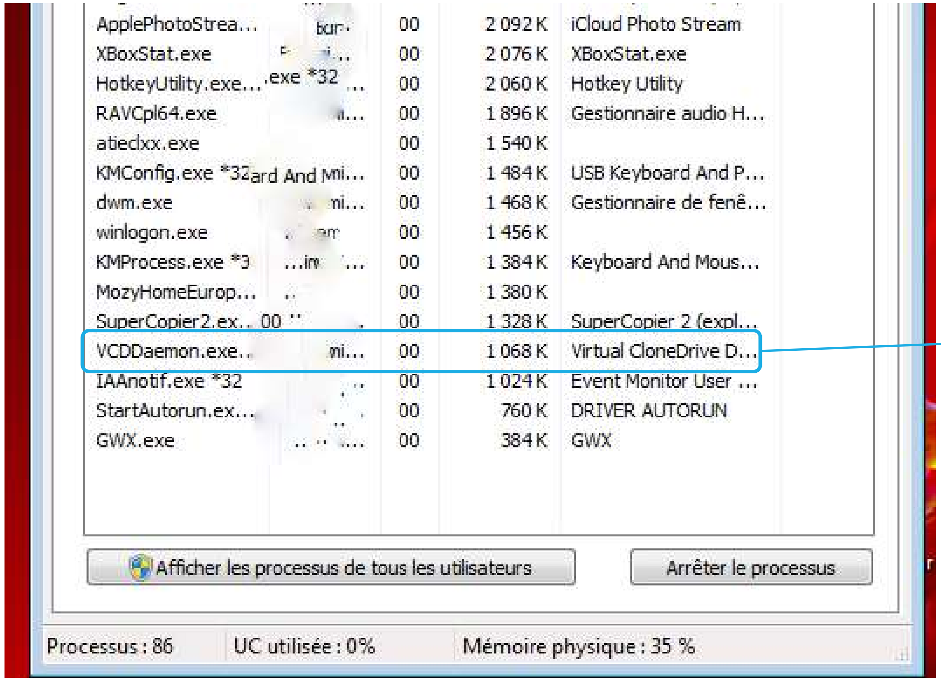


```
ApplePhotoStrea...          00   2 092 K   iCloud Photo Stream
XBoxStat.exe                00   2 076 K   XBoxStat.exe
HotkeyUtility.exe... .exe *32 ...   00   2 060 K   Hotkey Utility
RAVCpl64.exe                00   1 896 K   Gestionnaire audio H...
atieclxx.exe                00   1 540 K
KMConfig.exe *32ard And Mi...   00   1 484 K   USB Keyboard And P...
dwm.exe                     00   1 468 K   Gestionnaire de fenê...
winlogon.exe                00   1 456 K
KMProcess.exe *3            00   1 384 K   Keyboard And Mous...
MozyHomeEurop...            00   1 380 K
SuperCopier2.ex.. 00        00   1 328 K   SuperCopier 2 (expl...
VCDDaemon.exe..             00   1 068 K   Virtual CloneDrive D...
IAAnotif.exe *32            00   1 024 K   Event Monitor User ...
StartAutorun.ex...          00     760 K   DRIVER AUTORUN
GWX.exe                     00     384 K   GWX
```

Processus : 86   UC utilisée : 0%   Mémoire physique : 35 %



VCDDAEMON.EXE



ApplePhotoStrea…	bur…	00	2 092 K	iCloud Photo Stream
XBoxStat.exe	…i…	00	2 076 K	XBoxStat.exe
HotkeyUtility.exe…	.exe *32 …	00	2 060 K	Hotkey Utility
RAVCpl64.exe	…i…	00	1 896 K	Gestionnaire audio H…
atieclxx.exe		00	1 540 K	
KMConfig.exe *32	ard And Mi…	00	1 484 K	USB Keyboard And P…
dwm.exe	…mi…	00	1 468 K	Gestionnaire de fenê…
winlogon.exe	…em	00	1 456 K	
KMProcess.exe *3	…in …	00	1 384 K	Keyboard And Mous…
MozyHomeEurop…	..	00	1 380 K	
SuperCopier2.ex…	00 …	00	1 328 K	SuperCopier 2 (expl…
VCDDaemon.exe…	mi…	00	1 068 K	Virtual CloneDrive D…
IAAnotif.exe *32	..	00	1 024 K	Event Monitor User …
StartAutorun.ex…	…	00	760 K	DRIVER AUTORUN
GWX.exe	…	00	384 K	GWX

Processus : 86 UC utilisée : 0% Mémoire physique : 35 %

Some malware appear as VCDDaemon.exe, including those found in the C:\windows or C:\windows\system32.

Check the VCDDaemon.exe process on your PC.

LET'S SCAN PORTS

If you use CLI, do that with Nmap, if not, you can find lots of ports scanners online.

Port	Service	comment
21	FTP	Open, no password…
137/139	Netbios-ns/ssn	Can't close because of printer, network, etc. but can be used for an attack

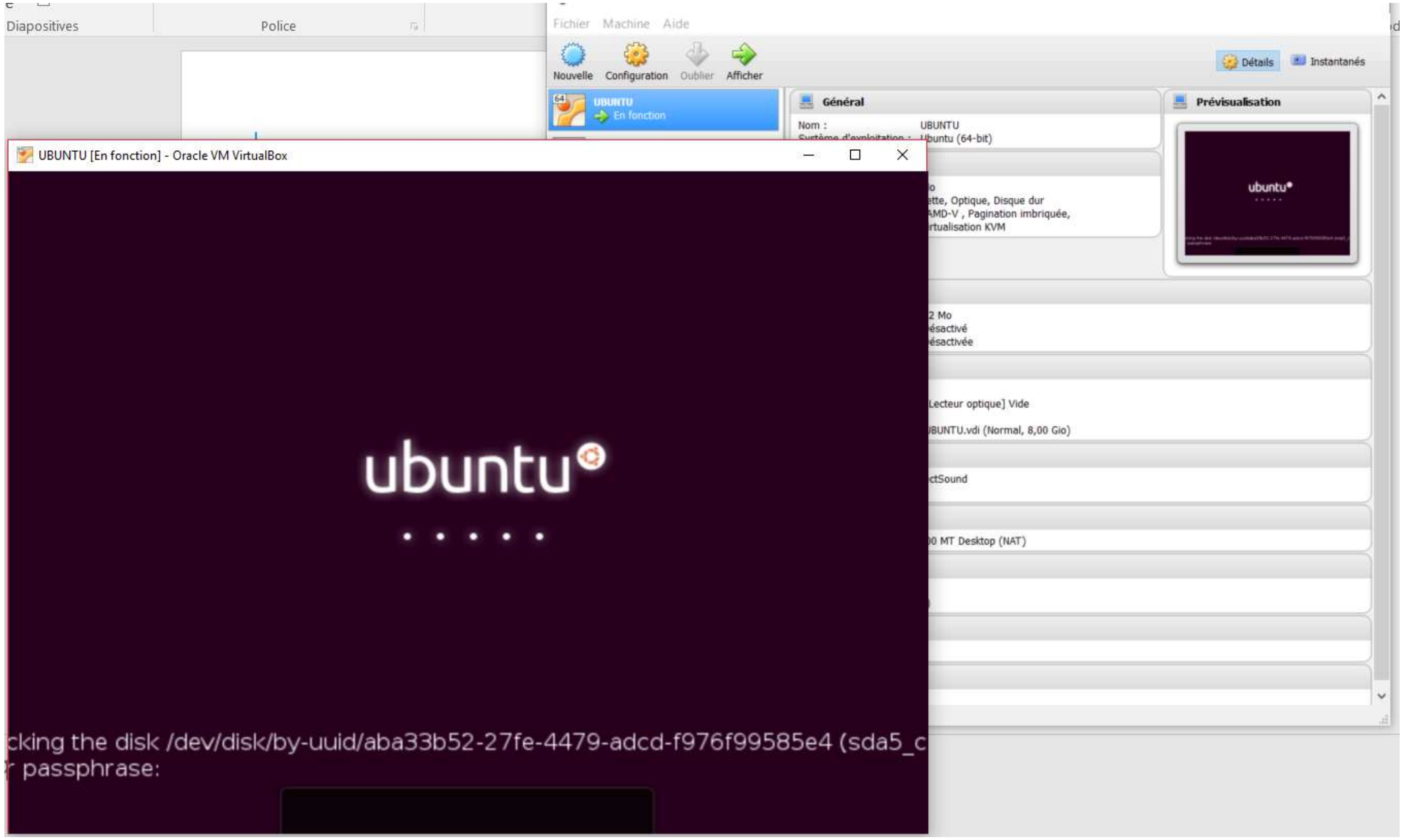
Port	Service	Comment
79	finger	Finger is not dangerous but leave it in listening without really need is a mistake. finger gives too much information about the system users
119	nntp	Vulnerability has been identified in several versions of Windows; which could be exploited by an attacker. The problem is due to an error in the Network News Transfer Protocol that does not properly handling certain malicious requests
135	Epmap	Port used by BLASTER virus - vidéo
1214/ 4662/ 4663	Kazaa & eDokey	Port used by Peer-to-Peer applications for the exchange of files. Unfortunately, their use in a network can lead to security problems and unnecessarily consume bandwidth
3127	CTX Bridge	Used by lots of viruses : MyDoom, Novarg…

GOOD PRACTICES FOR TOMORROW

(KILL THIS COMPUTER WITH FIRE!!!)

RE-INSTALL ALL
(BUT NOT THE CRACKED GAMES)
... EVEN BY DEFAULT

VIRTUALIZATION ?



Nom : UBUNTU
Système d'exploitation : Ubuntu (64-bit)

o
ette, Optique, Disque dur
AMD-V , Pagination imbriquée,
rtualisation KVM

2 Mo
ésactivé
ésactivée

Lecteur optique] Vide
BUNTU.vdi (Normal, 8,00 Gio)

ctSound

0 MT Desktop (NAT)

```
cking the disk /dev/disk/by-uuid/aba33b52-27fe-4479-adcd-f976f99585e4 (sda5_c
r passphrase:
```

KEEP AN EYE
ON YOUR RUNNING PROCESSES

❑ But it's not enought…

USING TWO DIFFERENT OS?

❑DUAL BOOT, like one for gaming (Windows) and an other for doing everithing else (Ubuntu ?)

❑There also vwill be a problem if the 2 different OS are sharing the same disk or part of disk, you have to separate the two universes

❑Problem of resources can be the same as virtualizing

AND WHAT ABOUT A DEDICATED MACHINE ?

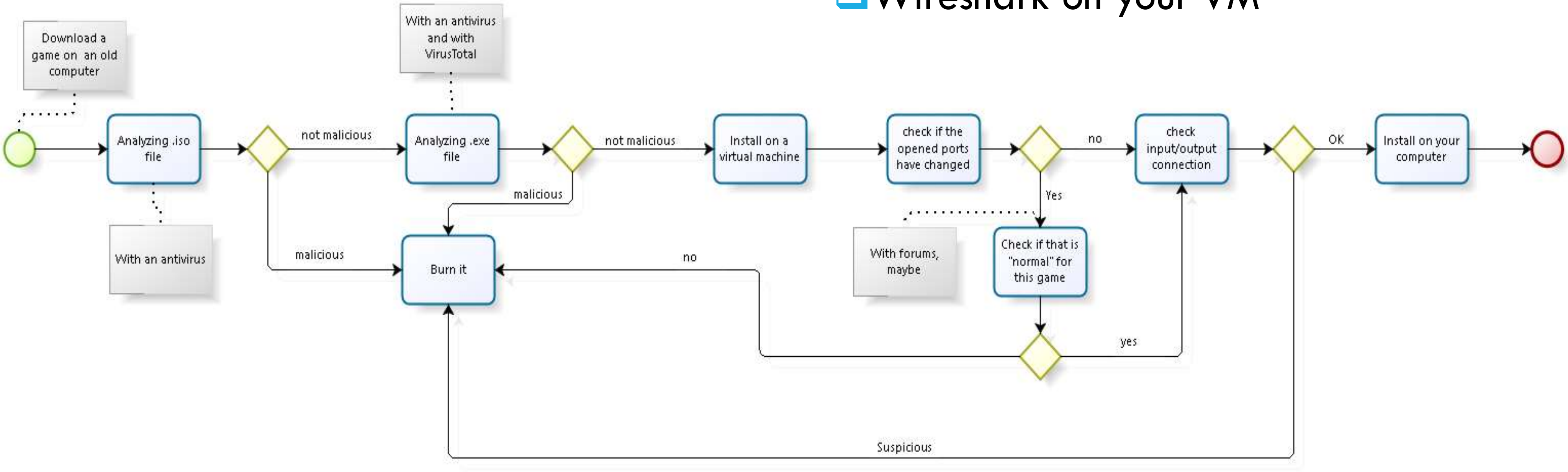
□ Not connected to local network

□ Not connected to internet

The problem is gamers sometimes need to play online

CREATING A PROCESS

- ❑An old computer connected to Internet
- ❑An updated antivirus
- ❑A virtual machine
- ❑Wireshark on your VM



Download a game on an old computer
Analyzing .iso file
With an antivirus
not malicious
malicious
With an antivirus and with VirusTotal
Analyzing .exe file
malicious
not malicious
Burn it
Install on a virtual machine
check if the opened ports have changed
no
Yes
With forums, maybe
Check if that is "normal" for this game
no
yes
check input/output connection
OK
Install on your computer
Suspicious

THANK YOU ! QUESTIONS ?