



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Aula  
Virtual

cidead

Ciberseguridad en Entornos de las Tecnologías de la Información

Módulo 5021 – Incidentes de Ciberseguridad

Ejercicio – Troyanos de Acceso Remoto a Móvil y a PC

# Pliego de Descargo

- Los ejercicios y conocimientos contenidos en el Módulo 5021, *Incidentes de Ciberseguridad*, tienen un propósito exclusivamente formativo, por lo que **nunca se deberán utilizar con fines maliciosos o delictivos**.
- Ni el Ministerio de Educación y Formación Profesional como organismo oficial, ni el CIDEAD como área integrada en el mismo, serán responsables en ningún caso de los daños directos o indirectos que pudieran derivarse del uso inadecuado de las herramientas de hacking ético utilizadas en dichos ejercicios.



cidead



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Aula  
Virtual

cidead

## Índice de contenidos

1. RAT Móvil – AhMyth RAT
2. RAT PC – Quasar RAT



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Aula  
Virtual

cidead

## 1. RAT Móvil – AhMyth RAT

# Ataque a un Móvil con un RAT

- En este ejercicio atacaremos un móvil Android con un Troyano de Acceso Remoto, instalaremos en el dispositivo una puerta trasera y capturaremos toda la información de la víctima.
- Utilizaremos para ello el troyano AhMyth, que es de código abierto y se puede manipular con mucha facilidad para elaborar otras cepas más sofisticadas.
- El servidor de AhMyth se puede instalar sobre Windows (opción elegida para este ejercicio) o sobre las distribuciones Linux más populares (este último S.O. resulta ideal para modificar el código y crear nuevos troyanos derivados de AhMyth, más potentes e indetectables).
- El cliente de AhMyth contiene la puerta trasera y se instala en el móvil Android. AhMyth está muy extendido y su cliente original es detectado con facilidad por el filesystem, por el instalador, y por los antivirus habituales en Android, por lo que otro reto diferente será incrustarlo dentro de un vector para que no sea detectado en ningún momento, ni antes de la instalación ni después de la misma.



# Ataque a un Móvil con un RAT

- La sigla RAT puede significar *Remote Administration Tool* (control remoto normal con fines administrativos o de mantenimiento) ó *Remote Access Trojan* (control remoto malicioso con fines dolosos). En ambos casos se requiere que propietario del dispositivo autorice la instalación del cliente correspondiente en el móvil, hecho que se produce expresamente en el primer caso, y mediante un vector de infección en el segundo caso.
- La frontera entre ambos tipos de control remoto es muy delgada, por lo que siempre se habrá de tener en cuenta que esta práctica se imparte sólo a efectos formativos y que nunca se deberán utilizar estos conocimientos con fines maliciosos o delictivos.

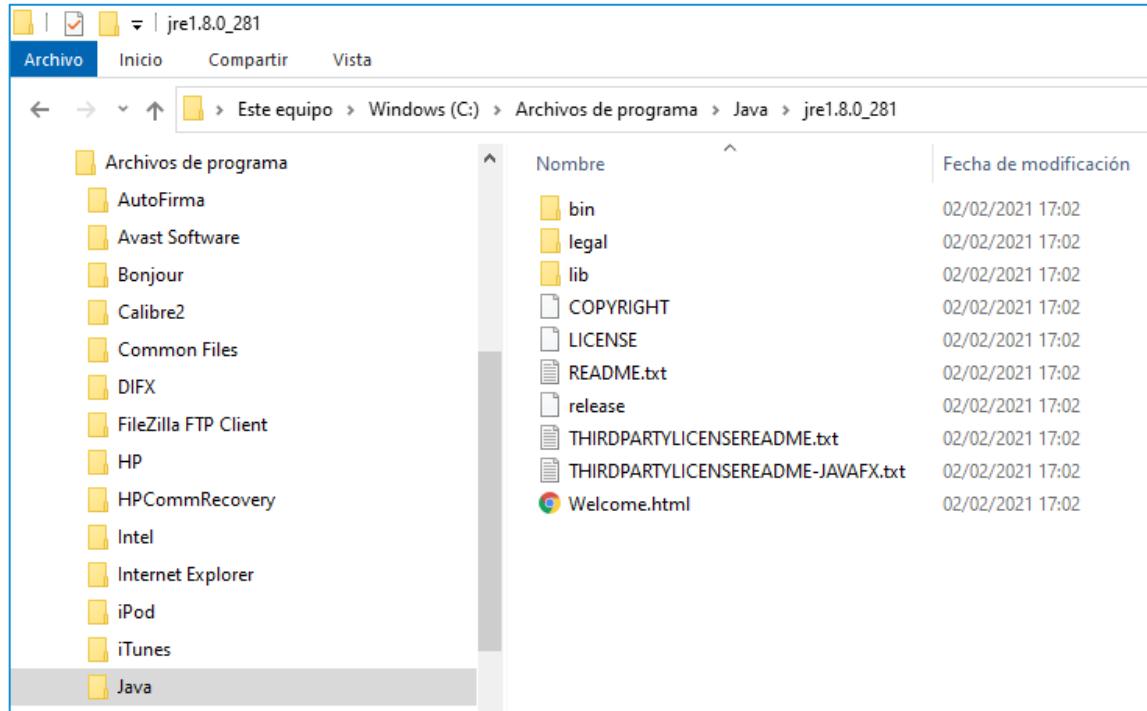
# Instalación de Java en Windows

- Pasamos a describir la secuencia de pasos que permitirán habilitar el SW del RAT.
- En primer lugar, revisaremos la instalación de Java en Windows, o bien, la actualizaremos a la última versión.

The image shows the official Java website homepage. At the top, there is a red header with the Java logo, a search bar, and 'Descargar' and 'Ayuda' buttons. Below the header, a large white banner features the text 'JAVA Y TÚ, DESCARGAR HOY' in a large, bold, sans-serif font. Underneath the banner, there is a red button labeled 'Descarga gratuita de Java'. Further down, there are links for '¿Qué es Java?' and '¿Necesita ayuda?'. A section titled 'Acerca de Java (sitio en inglés)' contains icons for various Java-related resources: 'go.java', 'Alice', 'Greenfoot', 'JavaOne', 'Oracle Academy', and 'Java Magazine'. The 'Java Magazine' icon includes the text 'Get it now for FREE!'. The bottom right corner of the page has a watermark that says 'cidead'.

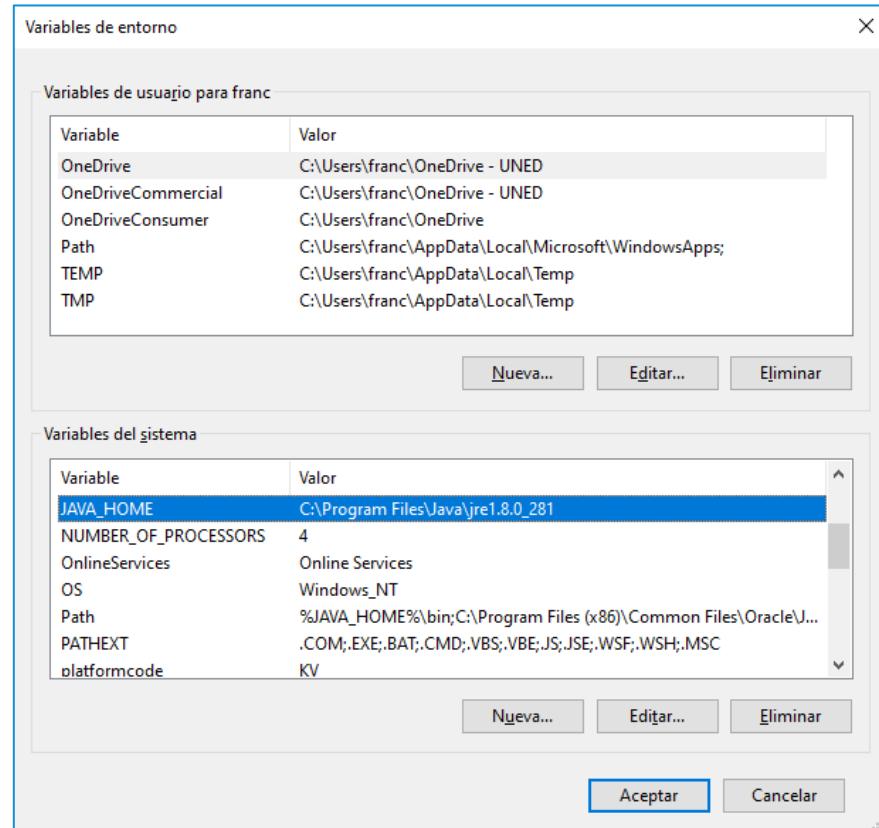
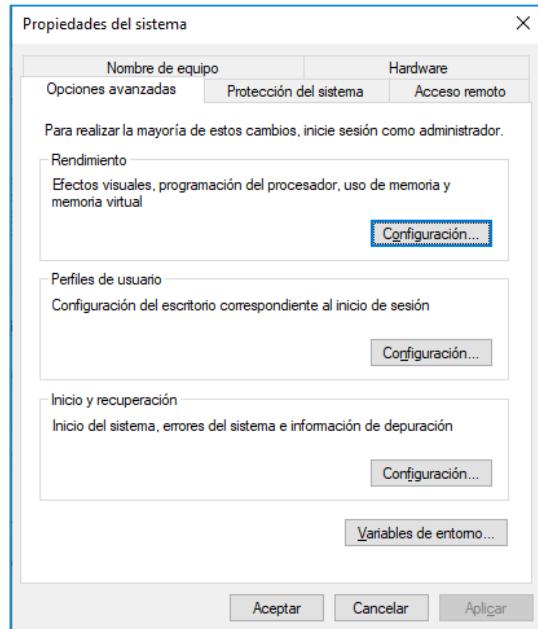
# Configuración del JRE

- Después localizaremos la ruta de instalación del Java Runtime Environment (JRE).



# Configuración del JRE

- Iremos a Configuración Avanzada del Sistema, Variables de Entorno.
- Crearemos la variable JAVA\_HOME con la ruta anterior y la incluiremos al principio del PATH.



# Descarga de AhMyth desde GitHub

- Descargaremos la versión para Windows del servidor AyMyth desde GitHub.
- <https://github.com/AhMyth/AhMyth-Android-RAT>

## Getting Started

You have two options to install it

1) From source code

Prerequisite :

- Electron (to start the app)
- Java (to generate apk backdoor)
- Electron-builder and electron-packer (to build binaries for (OSX,WINDOWS,LINUX))

```
1. git clone https://github.com/AhMyth/AhMyth-Android-RAT.git
2. cd AhMyth-Android-RAT/AhMyth-Server
3. npm start
```

2) From binaries

Prerequisite :

- Download a binary from <https://github.com/AhMyth/AhMyth-Android-RAT/releases>
- Java (to generate apk backdoor)

## AhMyth Beta Version

 AhMyth released this on 7 Jul 2017 · 51 commits to master since this release

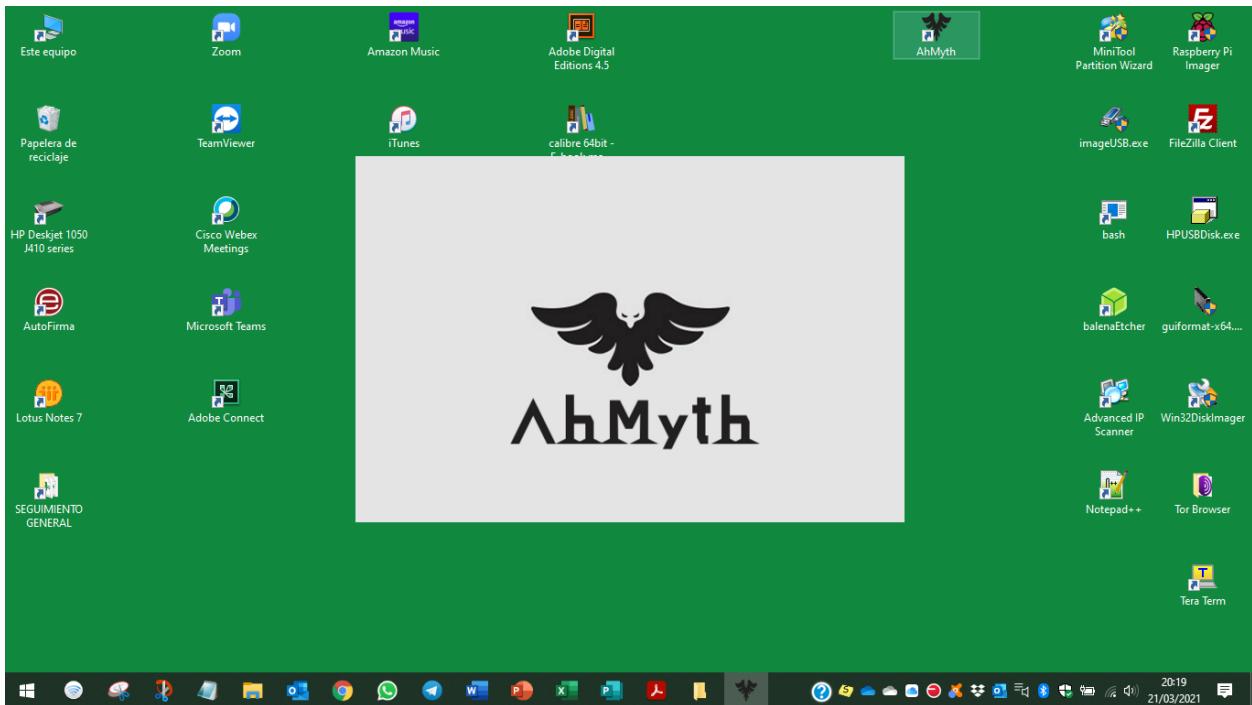
v1.0-beta.1  
beta version

▼ Assets 6

-  [AhMyth\\_linux32.deb](#)
-  [AhMyth\\_linux64.deb](#)
-  [AhMyth\\_Win32.exe](#)
-  [AhMyth\\_Win64.exe](#)
-  [Source code \(zip\)](#)
-  [Source code \(tar.gz\)](#)

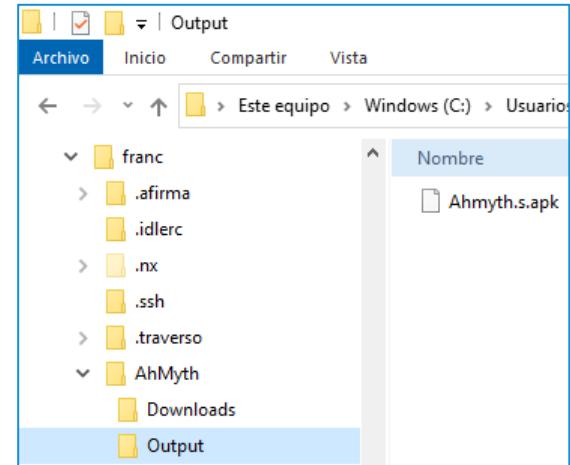
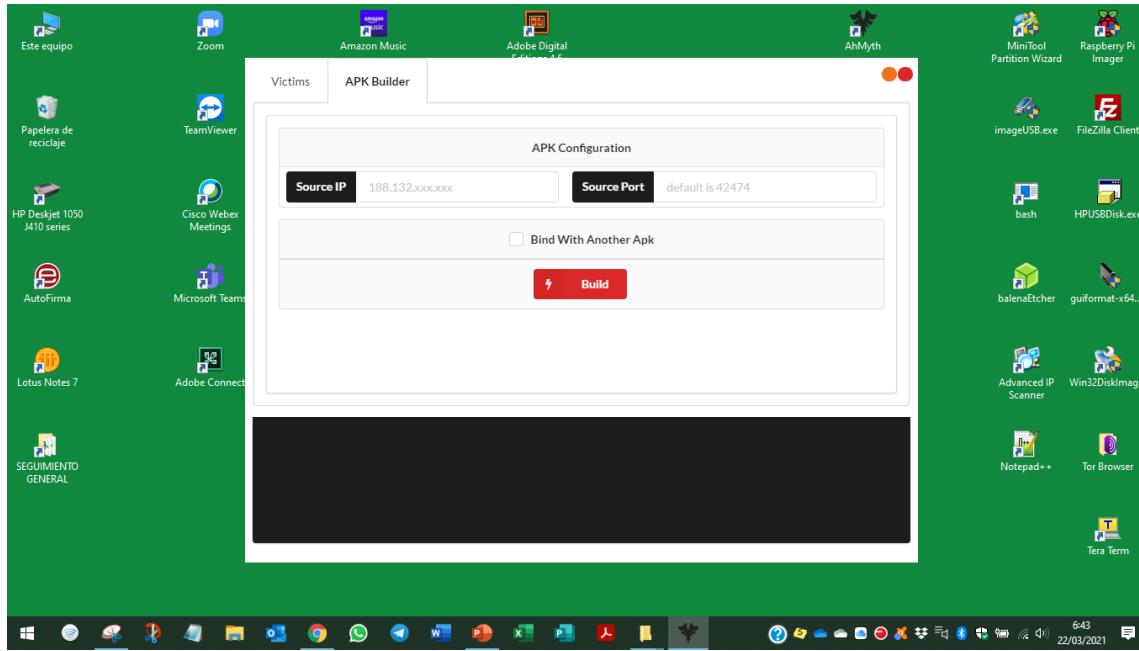
# Instalación de AhMyth en Windows

- Instalaremos el servidor AhMyth en Windows ejecutando el fichero descargado, y arrancaremos la aplicación servidora.



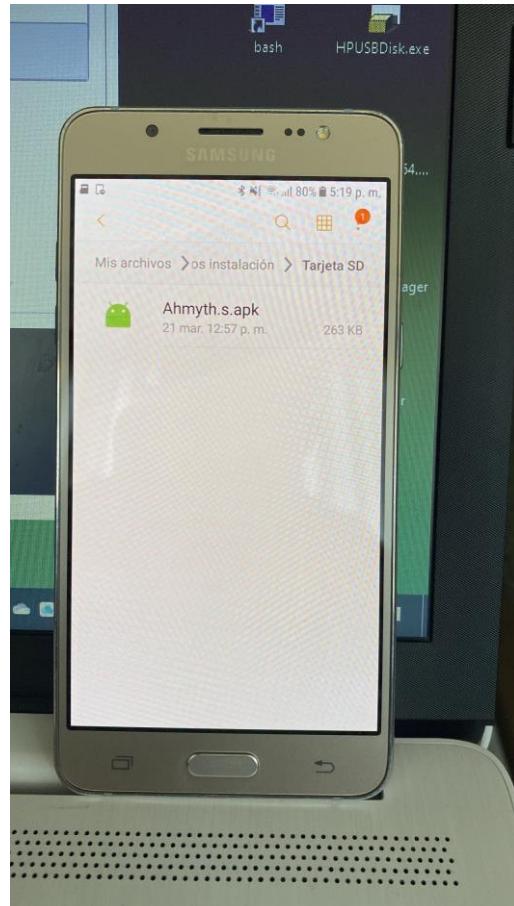
# Generación de la APK Cliente desde AhMyth Server

- Generaremos la APK cliente para el móvil rellenando la dirección IP de la máquina que la atacará y usando el puerto que nos propone AhMyth (u otro contiguo).



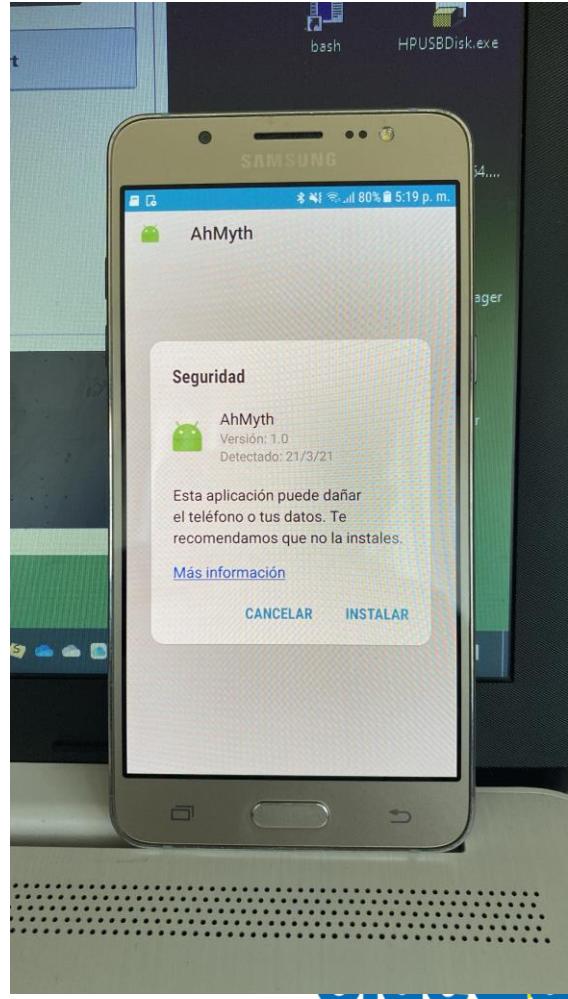
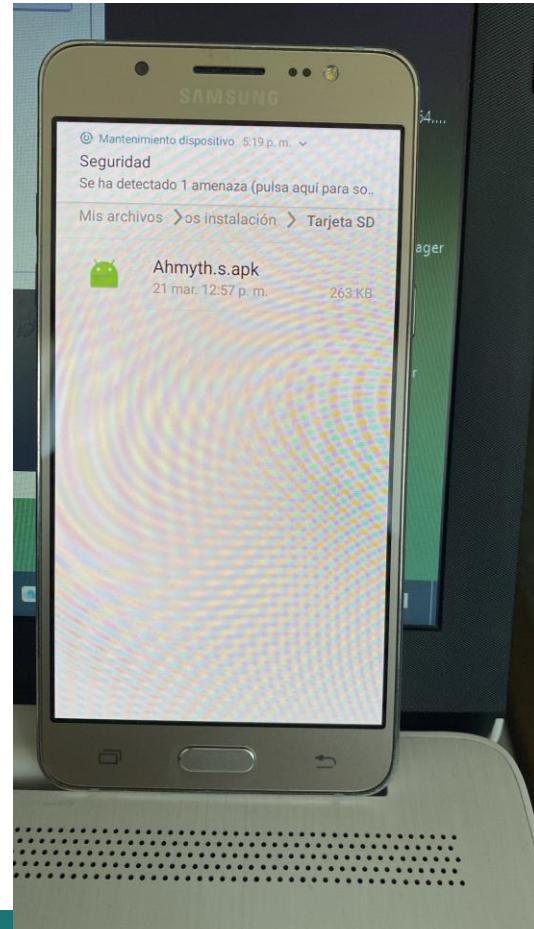
# Inoculación del Vector APK en el Móvil

- Para poder continuar rápidamente con el ejercicio, grabaremos el fichero en la tarjeta SD del móvil, pues cualquier aplicación de correo electrónico detectará el virus y no nos dejará enviar este fichero.
- Whatsapp detectará también el virus, pero nos permitirá enviar y descargar el fichero avisándonos de que es peligroso.
- Este SW es ampliamente conocido y detectado por muchos programas, pero también es el germen de otros RATs mucho más sofisticados e indetectables, que se han elaborado partiendo de un Branch de su código abierto.



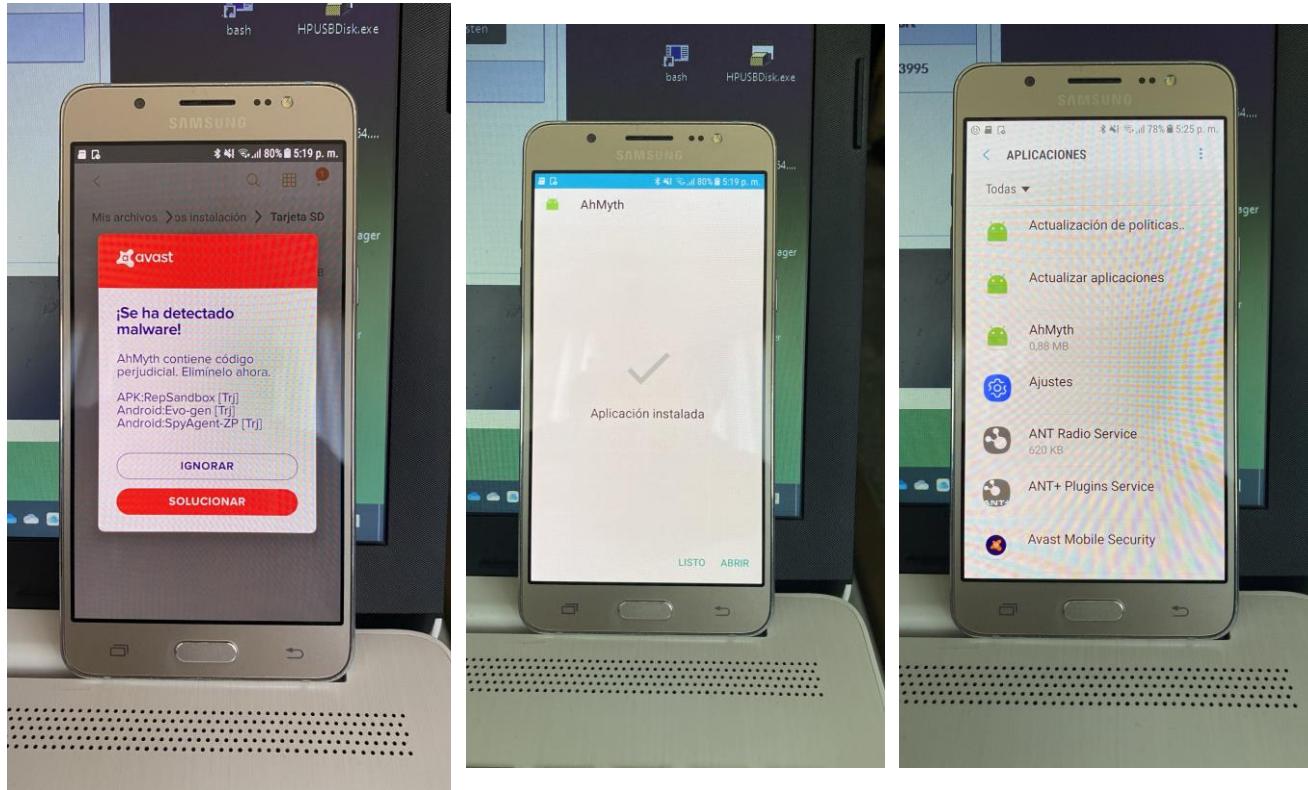
# Detección del Vector

- Unos segundos después de introducir la tarjeta SD, el móvil detecta que el fichero es peligroso y lo muestra en el File System Manager.
- Al intentar instalarlo, nos vuelve a avisar de que se trata de un fichero con riesgo, nos da opción de cancelar la instalación y, en caso de proseguir, nos obliga a autorizar la instalación de aplicaciones con origen desconocido en los ajustes.



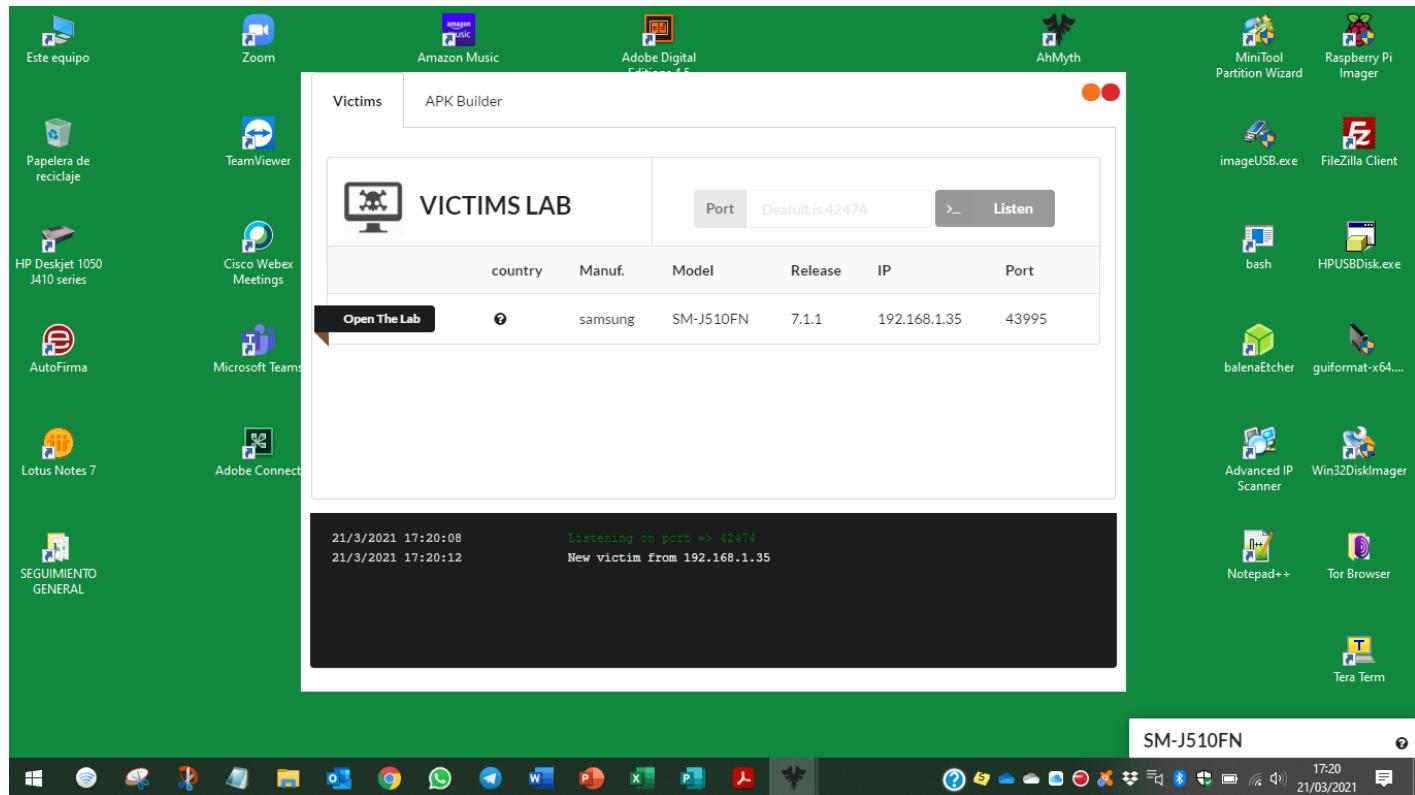
# Aviso del Antivirus

- Si hay instalado un antivirus en el móvil, también nos avisará del peligro y nos dará opción de cancelar la instalación.



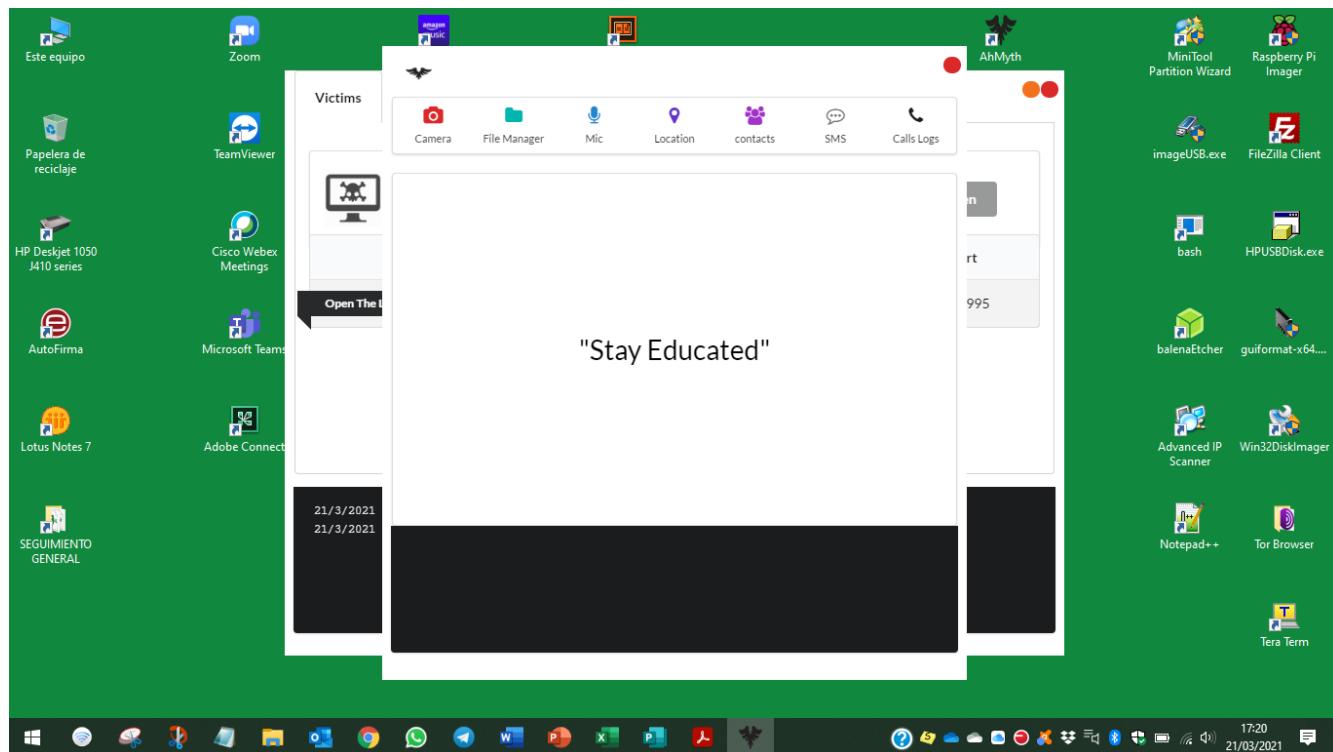
# Víctima Activa

- En cuanto esté en ejecución la APK en el móvil, aparecerá en el servidor una línea indicando que la víctima está activa.



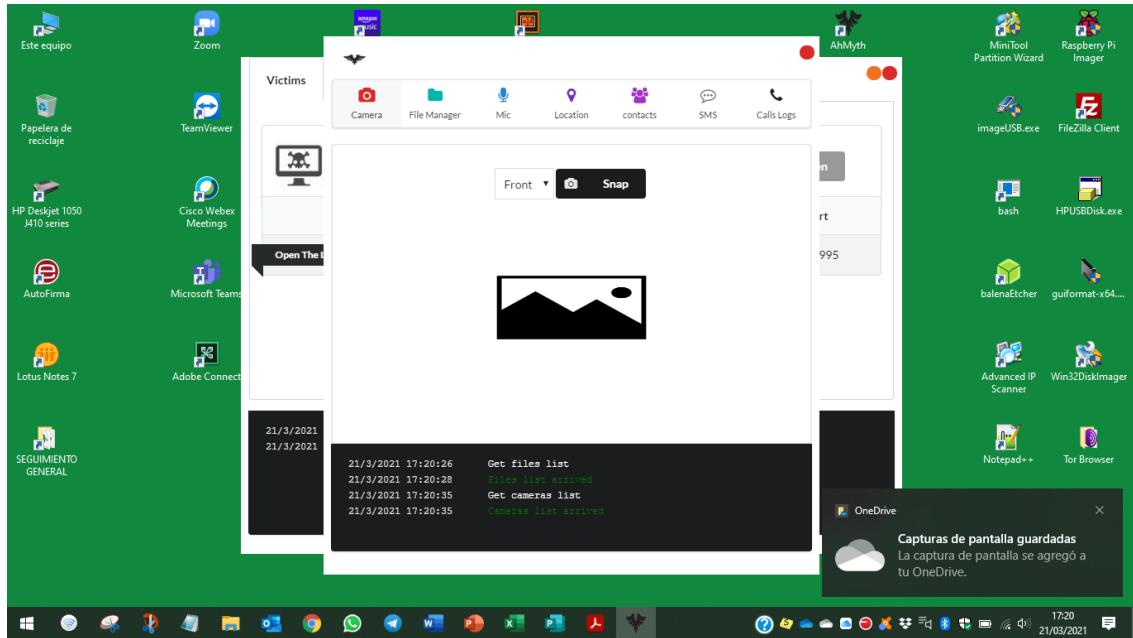
# Apertura del Panel de Control

- Procederemos a abrir el panel de control de la víctima en el que, de entrada, se nos pide que mantengamos la compostura.



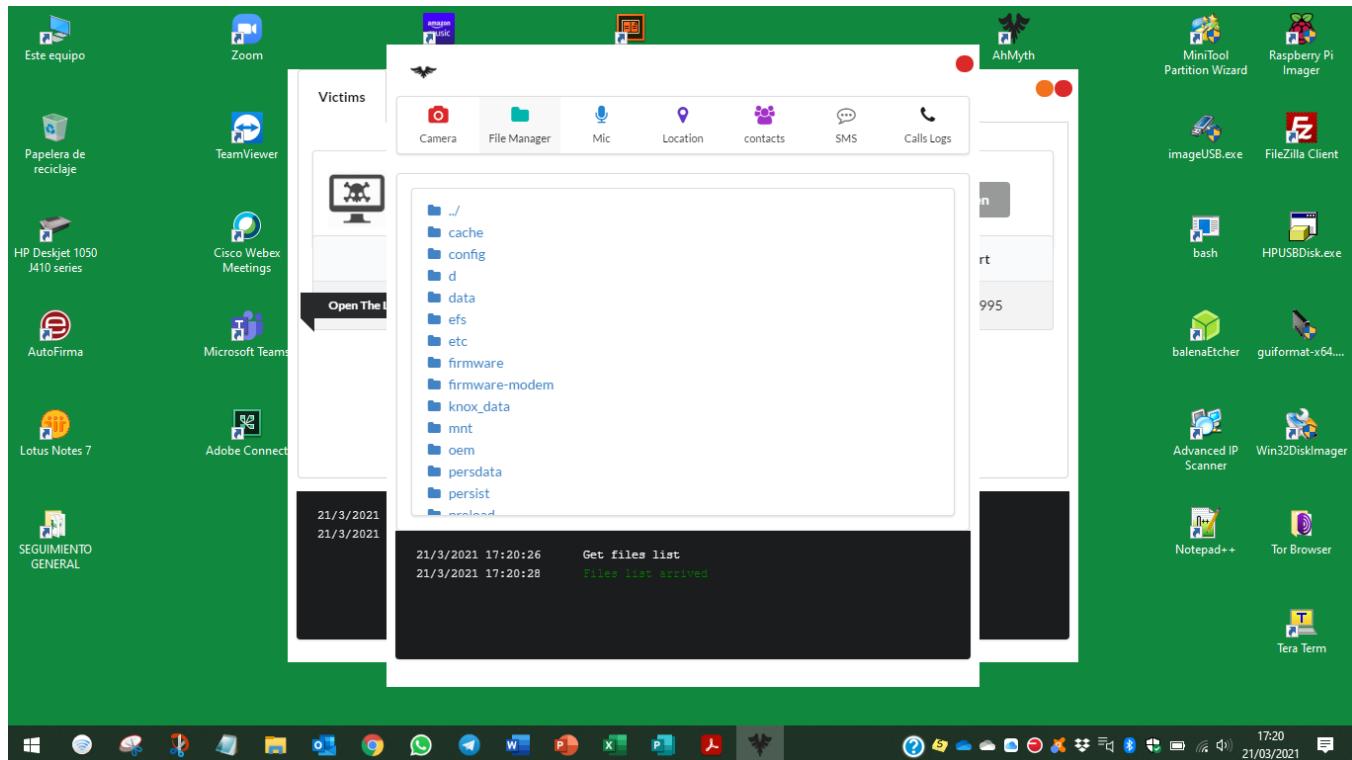
# Acceso a la Cámara de la Víctima

- La primera opción es acceder a la cámara de la víctima.
- Esta opción estuvo activa durante un tiempo, pero ahora viene desactivada por defecto, dado el peligro que conlleva.
- En cualquier caso, al disponer de los fuentes, se puede modificar el código para activarla de nuevo.



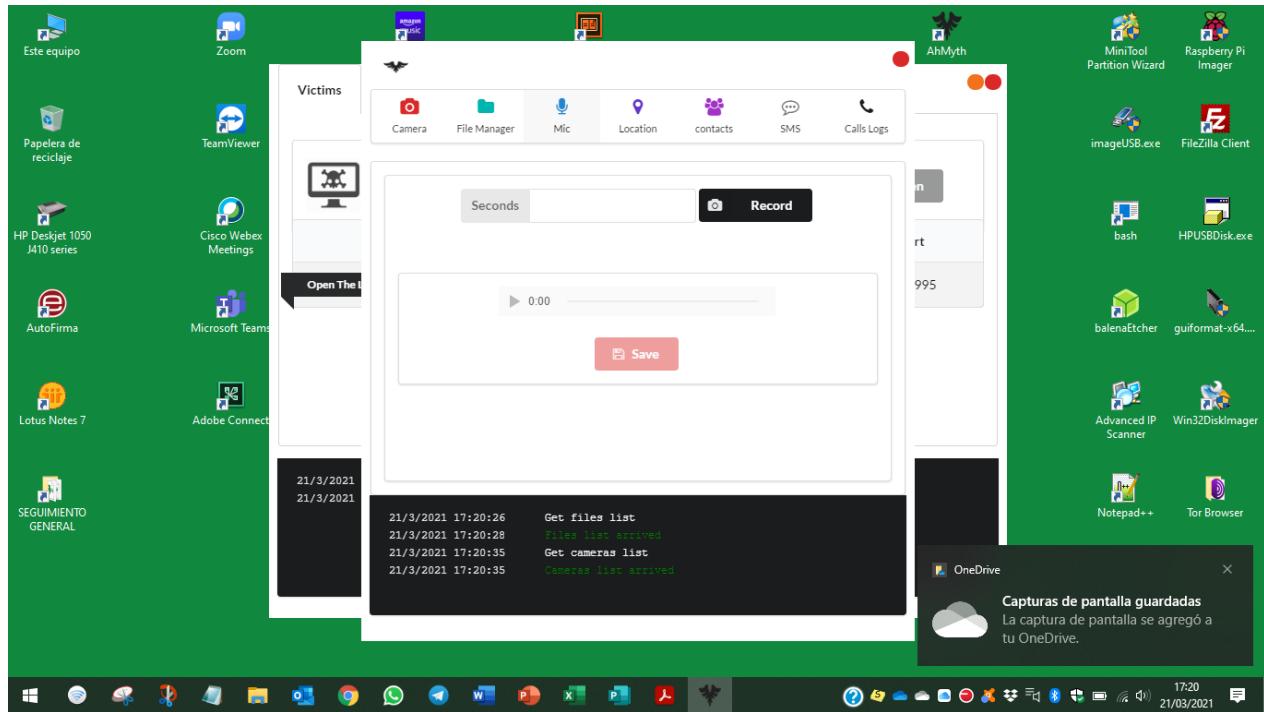
# Opción File Manager

Mediante la opción File Manager se puede acceder a cualquier fichero del teléfono y descargarlo en local.



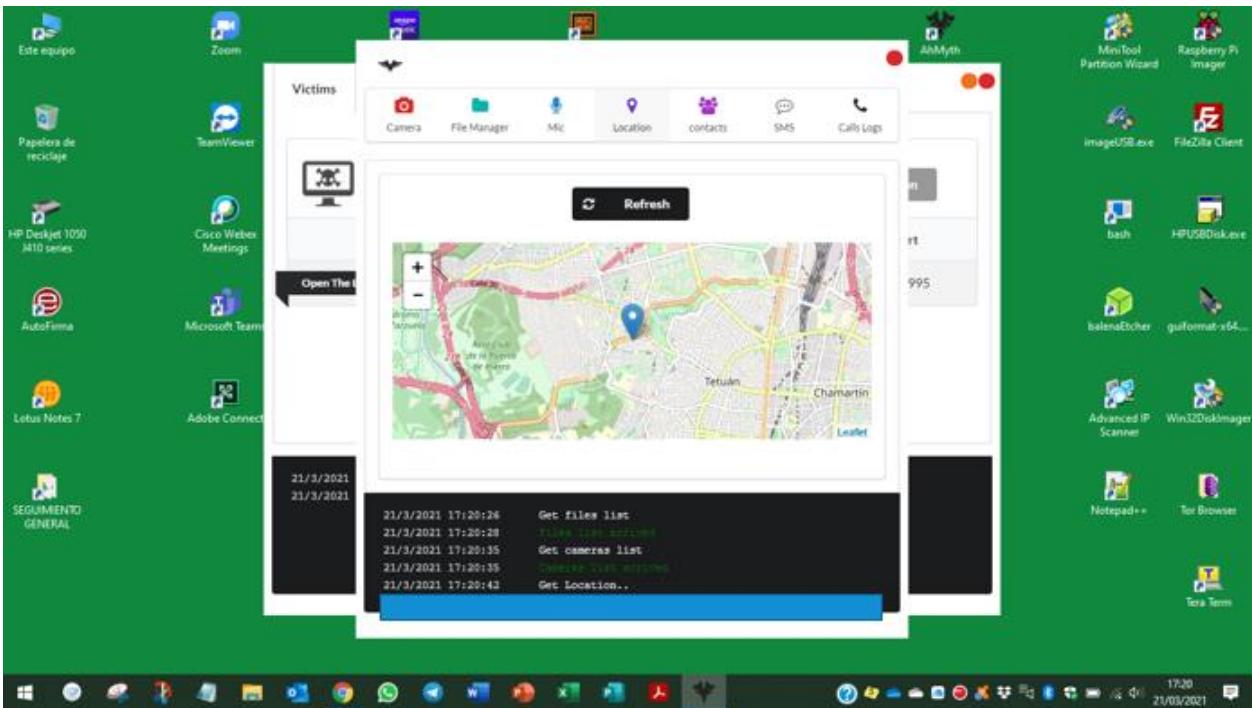
# Acceso al Micrófono de la Víctima

Con el micrófono ocurre lo mismo que con la cámara, esto es, viene desactivado por defecto y hay que modificar los fuentes para activarlo, dado que se trata de una opción muy peligrosa.



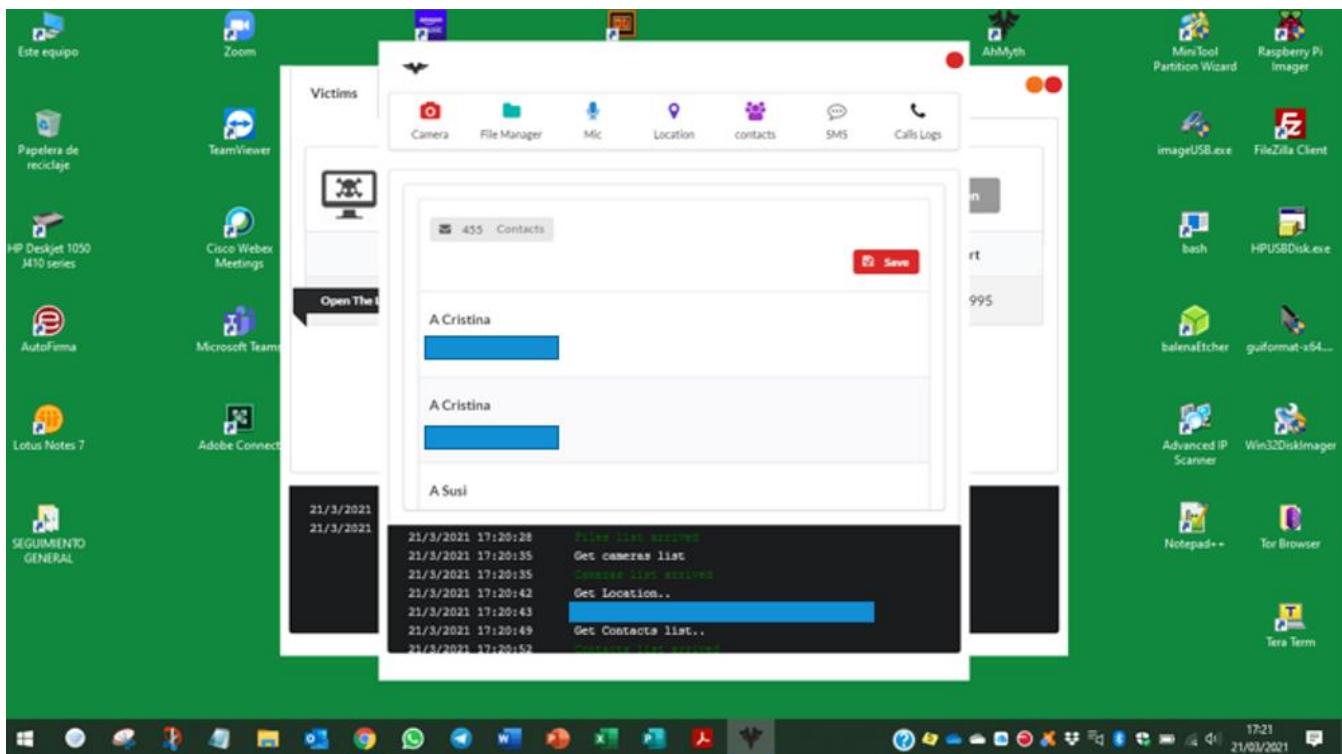
# Acceso a la Ubicación Detallada

Con la opción de ubicación, se obtiene la posición detallada del dispositivo en un mapa, en caso de que dicho dispositivo disponga de GPS y lo tenga activado.



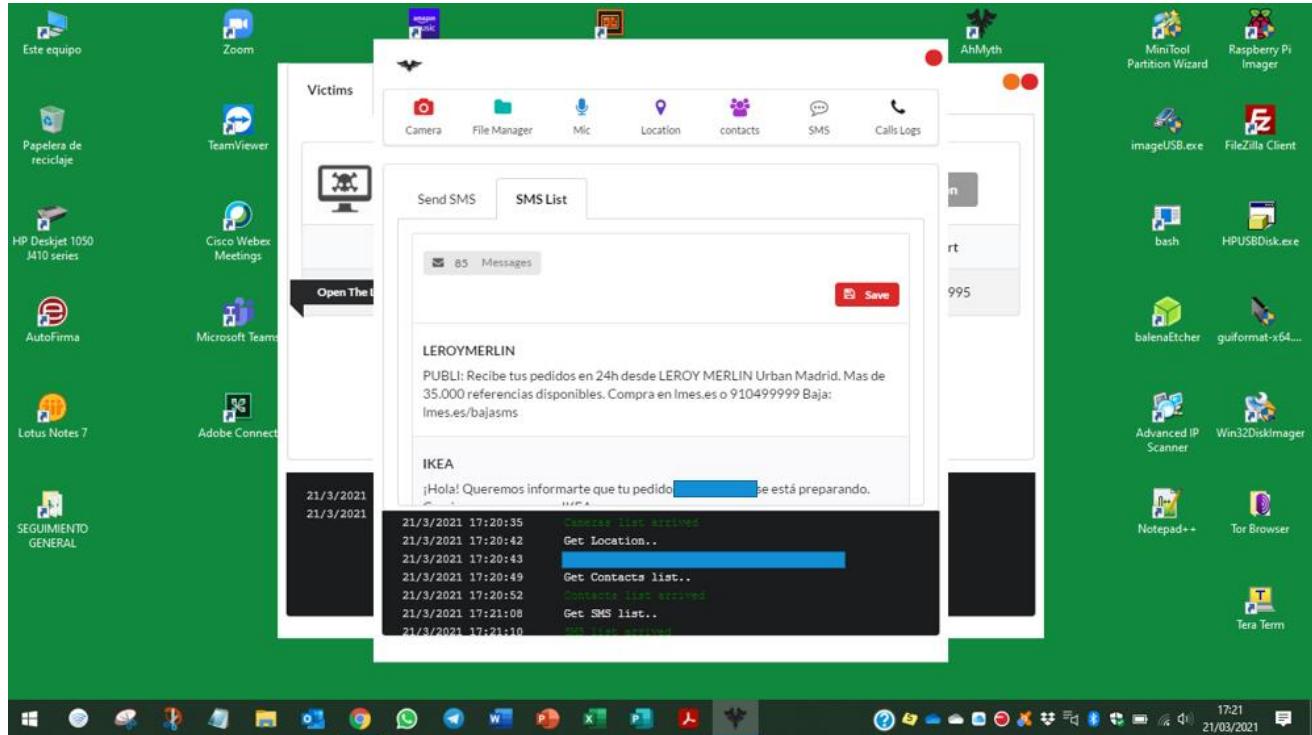
# Acceso a los Contactos

También es posible acceder a los contactos del móvil y descargar la lista completa en el PC en formato csv, fácilmente manejable en una hoja de cálculo.



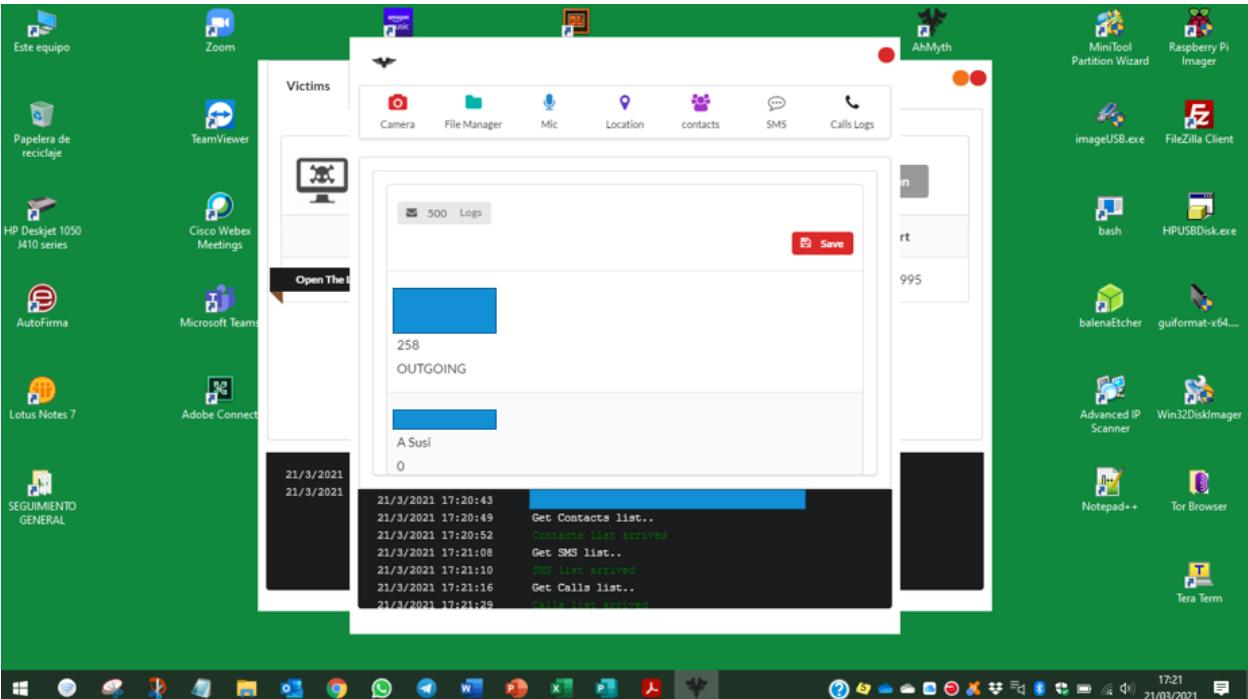
# Acceso a la Función SMS

- Se puede visualizar la lista de SMS del móvil y también descargarlos en local.
- También es posible redactar y enviar un SMS desde el móvil. Esta opción es también muy peligrosa.



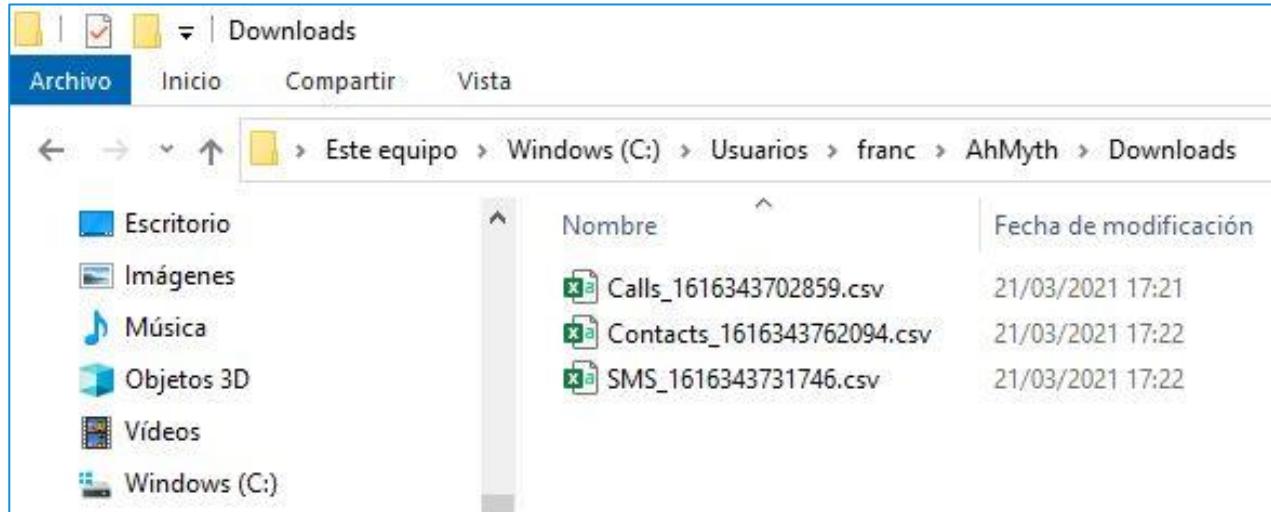
# Acceso a la Lista de Llamadas Telefónicas

- Y finalmente, también es posible acceder a la lista de llamadas y salvarla en local.
- Existen muchas más posibilidades de manipulación de datos, no obstante, para ello se precisan conocimientos avanzados de programación, que quedan fuera del alcance de este ejercicio.



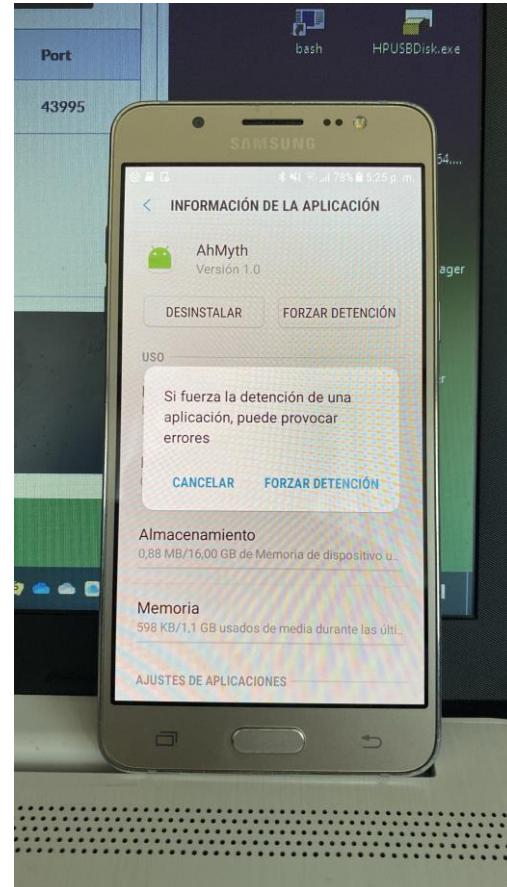
# Ficheros de Descargas de Información de la Víctima

- Los ficheros de descargas de información de la víctima se almacenan en el directorio “Downloads” de la Carpeta “AhMyth”.



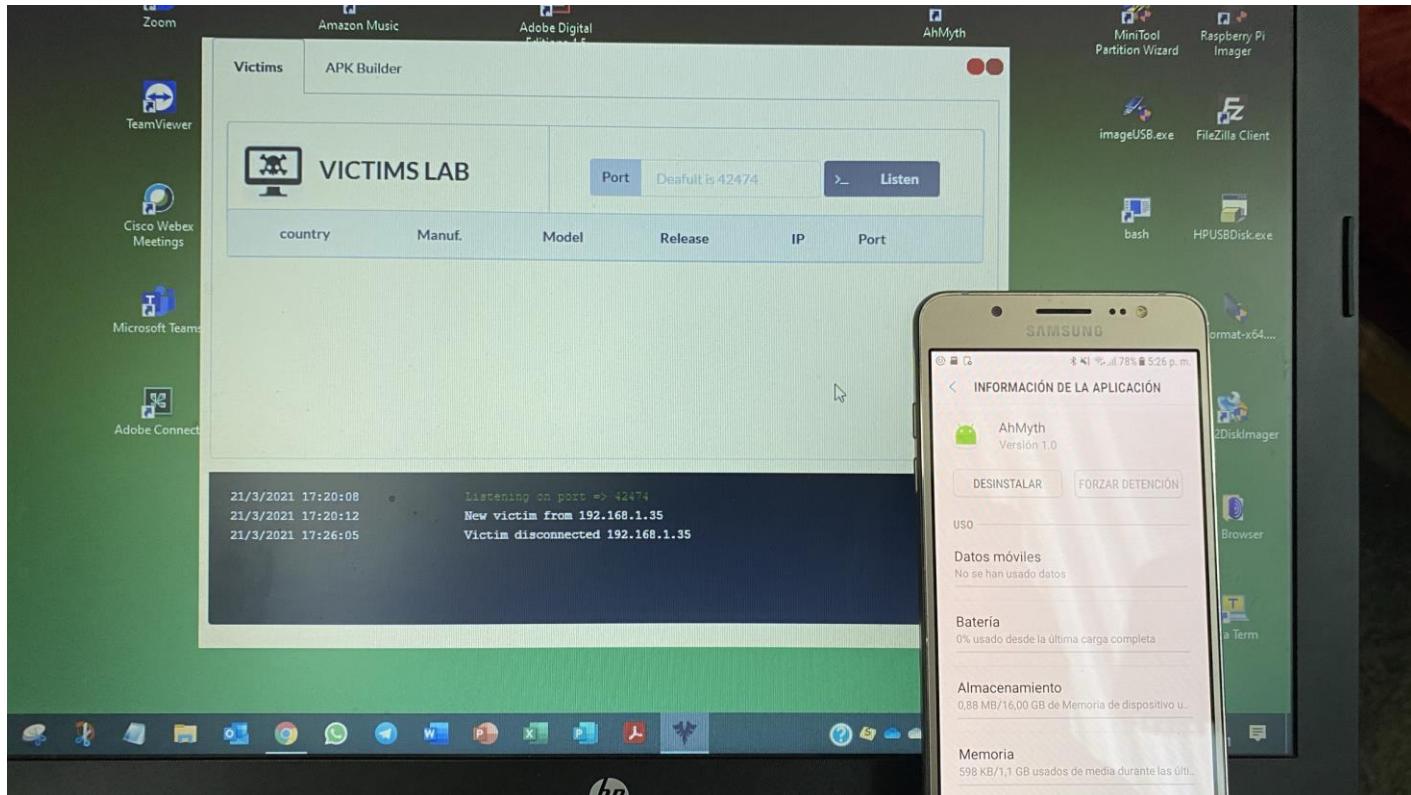
# Detención de la Aplicación Cliente

- Tras realizar el ejercicio, forzamos la detención de la aplicación cliente en el móvil.



# Desaparición del Panel de Control de la Víctima

Tras forzar la detención, automáticamente desaparece el panel de control de la víctima del servidor AhMyth, y damos por finalizado el ejercicio.





GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN  
Y FORMACIÓN PROFESIONAL



Aula  
Virtual

cidead

## 2. RAT PC – Quasar RAT

GitHub - quasar/Quasar: Remote +

https://github.com/quasar/Quasar

WORK Ciberseguridad Educación Oficial Telefónica Sociales Finanzas Comercial Salud Seguros Suministros Nubes Multimedia Lectura Ofimática »

Why GitHub? Team Enterprise Explore Marketplace Pricing Search Sign in Sign up

quasar / Quasar

Code Issues Pull request

master 2 branches

- MaxXor Merge branch 'dev'
- .github/ISSUE\_TEMPLATE
- Images
- Licenses
- Quasar.Client Merge branch 'dev'
- Quasar.Common.Tests Revert Version
- Quasar.Common Revert Version
- Quasar.Server Revert Version
- .gitattributes Added .gitattributes

Para instalar Quasar RAT, en primer lugar localizaremos el proyecto correspondiente en GitHub.

Al visualizar el fichero README del proyecto, veremos que para trabajar en Windows habrá que tener instalados previamente el entorno de Visual Studio y el Framework .net, ambos en sus versiones más recientes.

Security Insights

Go to file Code

34702 on 8 Feb 1,294 commits

11 months ago  
11 months ago  
10 months ago  
2 months ago  
8 months ago  
8 months ago  
8 months ago  
7 years ago

About

Remote Administration Tool for Windows

windows c-sharp security  
remote-control administration Topic: security  
protobuf dotnet mono remote  
rat net remote-desktop red-team

Readme MIT License

Releases 10

Quasar v1.4.0 Latest

16:24 09/04/2021

GitHub - quasar/Quasar: Remote +

https://github.com/quasar/Quasar

WORK Ciberseguridad Educación Oficial Telefónica Sociales Finanzas Comercial Salud Seguros Suministros Nubes Multimedia Lectura Ofimática »

Why GitHub? Team Enterprise Explore Marketplace Pricing Search Sign in Sign up

quasar / Quasar

Code

Issues 124

Pull requests 9

Actions

Projects

Wiki

Security

Insights

master

2 branches

10 tags

Go to file

Code

Clone

HTTPS GitHub CLI

<https://github.com/quasar/Quasar.git>

Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

Download ZIP

8 months ago

8 months ago

7 years ago

MaxXor Merge branch 'dev'

Para descargar el proyecto en nuestro PC tenemos dos opciones:

- Descargar el ZIP y descomprimirlo (para nuestra práctica elegiremos esta alternativa).
- Si tenemos habilitado el núcleo Linux de Windows, podemos clonar el directorio con el comando "git clone".

Quasar.Server

Revert version

.gitattributes

Added .gitattributes

About

Remote Administration Tool for Windows

windows c-sharp security

remote-control administration

protobuf dotnet mono remote

rat net remote-desktop red-team

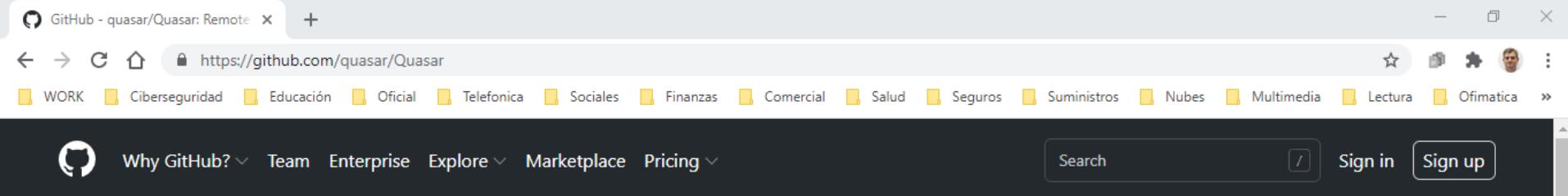
Readme

MIT License

Releases 10

Quasar v1.4.0 Latest

5 Jun 2020



quasar / Quasar

Code Issues 124 Pull requests 9 Actions Projects Wiki Security Insights

master 2 branches 10 tags

MaxXor Merge branch 'dev'

- .github/ISSUE
- Images
- Licenses
- Quasar.Cli
- Quasar.Cor
- Quasar.Cor
- Quasar.Ser

Quasar-master.zip

Clone

HTTPS GitHub CLI

<https://github.com/quasar/Quasar.git>

Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

Download ZIP

Activar todos los escudos (13 desactivado)

Desactivar durante 10 minutos

Desactivar durante 1 hora

Desactivar hasta que se reinicie el equipo

Desactivar permanentemente

About

Remote Administration Tool for Windows

windows c-sharp security  
remote-control administration  
protobuf dotnet mono remote  
rat net remote-desktop red-team

Abrir interfaz de usuario de Avast

Control de escudos de Avast  
Modo silencioso  
Baúl de virus  
Actualizar  
Activar modo sin conexión  
Información sobre la suscripción  
Acerca de Avast

09/04/2021

En caso de que optemos por descargar el fichero ZIP, es probable que nuestro antivirus detecte el código potencialmente malicioso y bloquee la descarga, como ocurre con el antivirus Avast. Así pues, antes de iniciar dicha descarga inhabilitaremos el antivirus durante un periodo acotado.

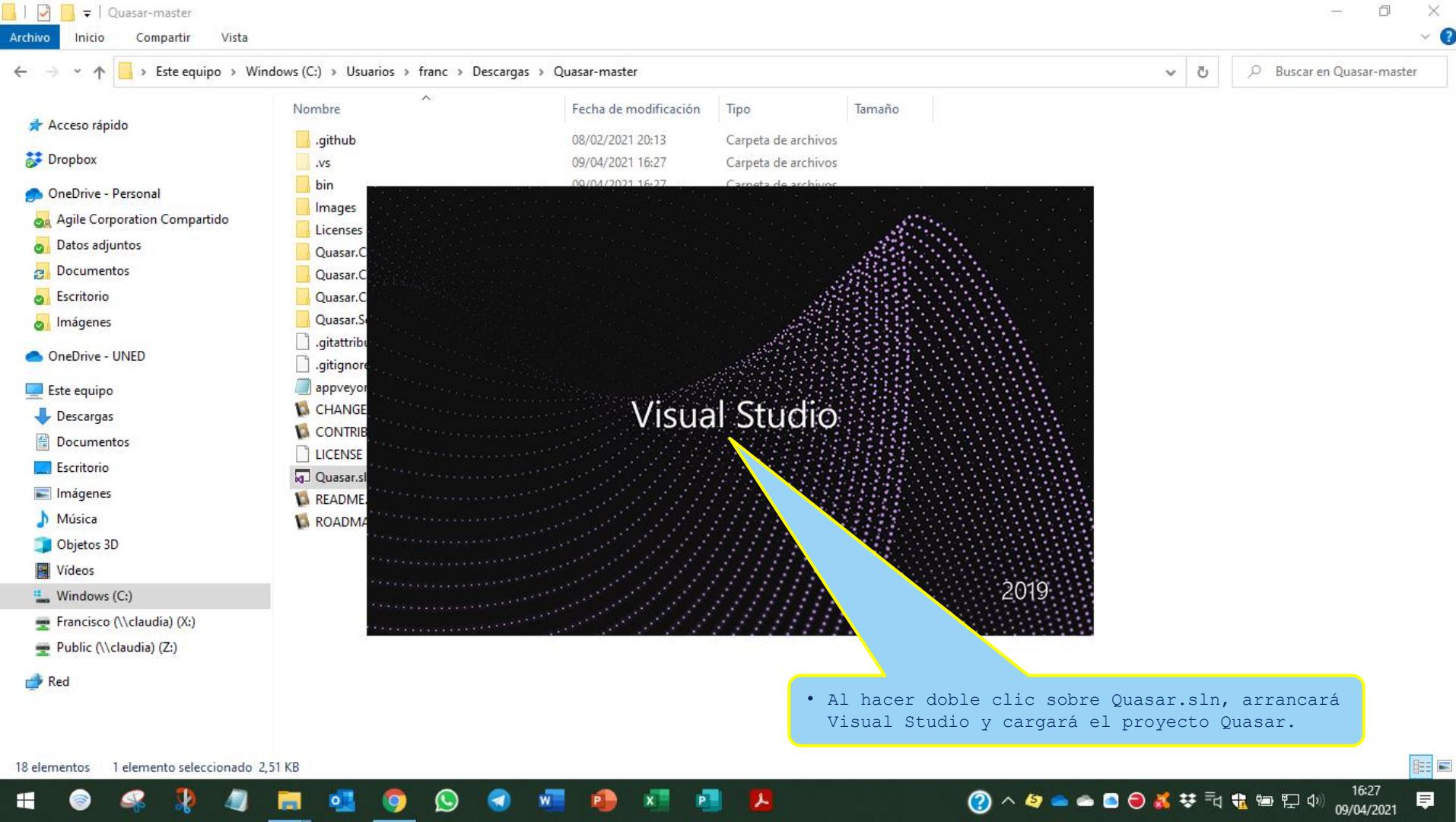
Este equipo > Windows (C:) > Usuarios > franc > Descargas > Quasar-master >

Nombre	Fecha de modificación	Tipo	Tamaño
.github	08/02/2021 20:13	Carpetas de archivos	
Images	08/02/2021 20:13	Carpetas de archivos	
Licenses	08/02/2021 20:13	Carpetas de archivos	
Quasar.Client	08/02/2021 20:13	Carpetas de archivos	
Quasar.Common	08/02/2021 20:13	Carpetas de archivos	
Quasar.Common.Tests	08/02/2021 20:13	Carpetas de archivos	
Quasar.Server	08/02/2021 20:13	Carpetas de archivos	
.gitattributes	08/02/2021 20:13	Archivo GITATTRIB...	1 KB
.gitignore	08/02/2021 20:13	Archivo GITIGNORE	3 KB
appveyor.yml	08/02/2021 20:13	Archivo YML	1 KB
CHANGELOG.md	08/02/2021 20:13	Documento MD	5 KB
CONTRIBUTING.md	08/02/2021 20:13	Documento MD	1 KB
LICENSE	08/02/2021 20:13	Archivo	2 KB
Quasar.sln	08/02/2021 20:13	Visual Studio Solu...	3 KB
README.md	08/02/2021 20:13	Documento MD	4 KB
ROADMAP.md	08/02/2021 20:13	Documento MD	2 KB

• Una vez finalizada la descarga, localizaremos el fichero Quasar.sln para construir el RAT en Visual Studio.

16 elementos 1 elemento seleccionado 2,51 KB

16:26 09/04/2021



- Al hacer doble clic sobre Quasar.sln, arrancará Visual Studio y cargará el proyecto Quasar.

Archivo Editar Ver Git Proyecto Compilar Depurar Prueba Analizar Herramientas Extensiones Ventana Ayuda Buscar (Ctrl+Q) Quasar Live Share

Explorador de servidores Cuadro de herramientas Orígenes de datos

Debug AnyCPU Quasar.Server Quasar.Server

Release Administrador de configuración...

• Una vez haya arrancado el entorno, seleccionaremos la opción "Release" para construir el RAT.

• Si seleccionamos la opción "Debug", se generará una versión enriquecida orientada a desarrolladores, no obstante, no contará con toda la funcionalidad (por ejemplo, no permitirá construir el SW a instalar en el PC remoto que se desea controlar).

Salida

Mostrar salida de: Compilación

Operación Limpiar iniciada...

1>----- Operación Limpiar iniciada: proyecto: Quasar.Common.Tests, configuración: Debug Any CPU -----  
2>----- Operación Limpiar iniciada: proyecto: Quasar.Client, configuración: Debug Any CPU -----  
2>C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\MSBuild\Current\Bin\Microsoft.Common.CurrentVersion.targets(5424,5): w  
2>Compilación del proyecto "Quasar.Client.csproj" terminada.  
3>----- Operación Limpiar iniciada: proyecto: Quasar.Server, configuración: Debug Any CPU -----  
4>----- Operación Limpiar iniciada: proyecto: Quasar.Common, configuración: Debug Any CPU -----  
4>C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\MSBuild\Current\Bin\Microsoft.Common.CurrentVersion.targets(5424,5): w  
4>Compilación del proyecto "Quasar.Common.csproj" terminada.  
===== Limpiar: 4 correctos, 0 incorrectos, 0 omitidos =====

Lista de errores Salida

Explorador de soluciones

Buscar en Explorador de soluciones (Ctrl+P)

Solución "Quasar" (4 de 4 proyectos)  
Quasar.Client  
Quasar.Common  
Quasar.Common.Tests  
Quasar.Server

Explorador de soluciones Cambios de GIT: Quasar

Propiedades

Quasar.Server Propiedades del proyecto

Misc

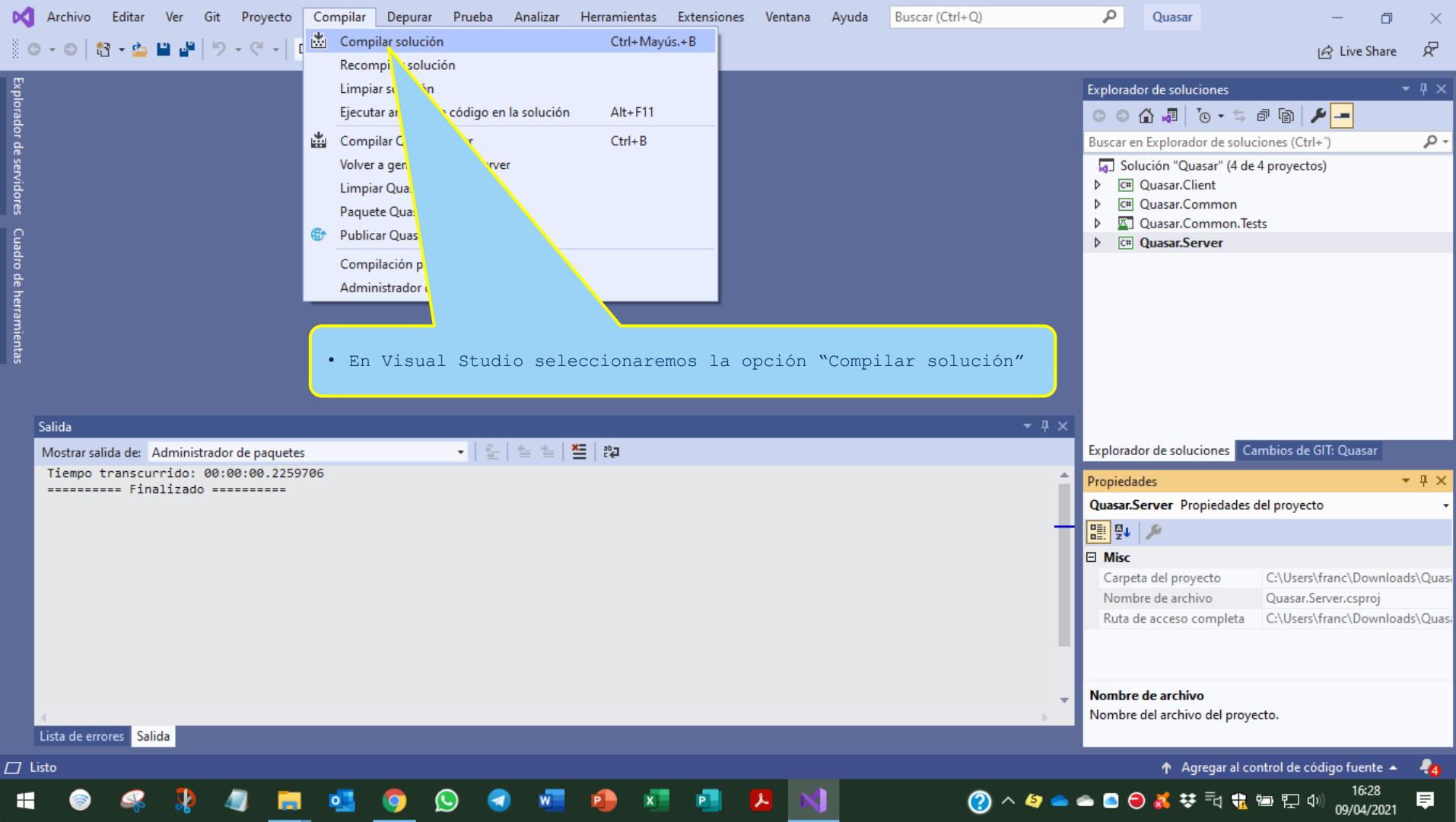
Carpetas del proyecto	C:\Users\franc\Downloads\Quasar
Nombre de archivo	Quasar.Server.csproj
Ruta de acceso completa	C:\Users\franc\Downloads\Quasar

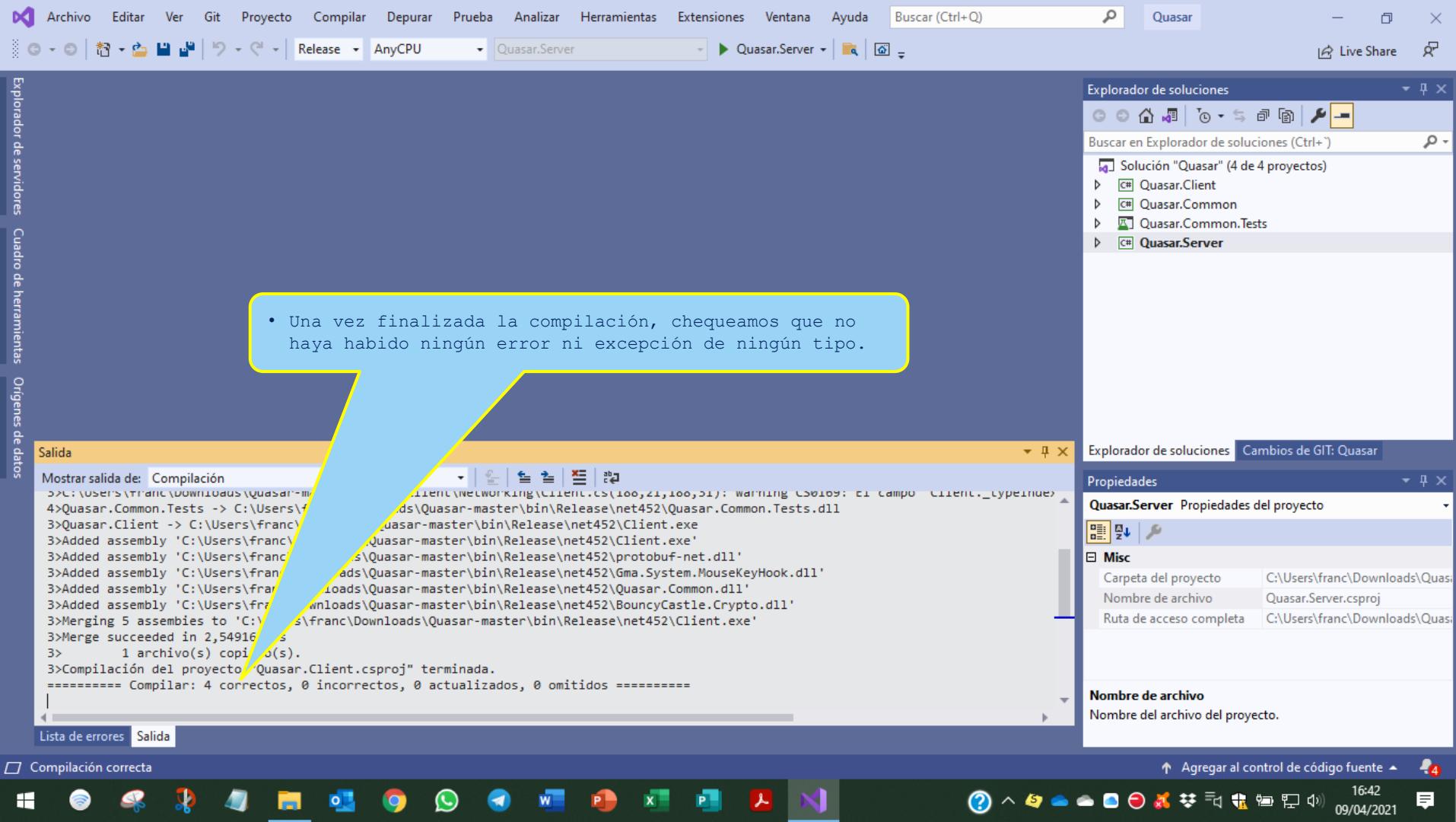
Nombre de archivo

Nombre del archivo del proyecto.

Operación Limpiar finalizada correctamente Agregar al control de código fuente

16:42 09/04/2021





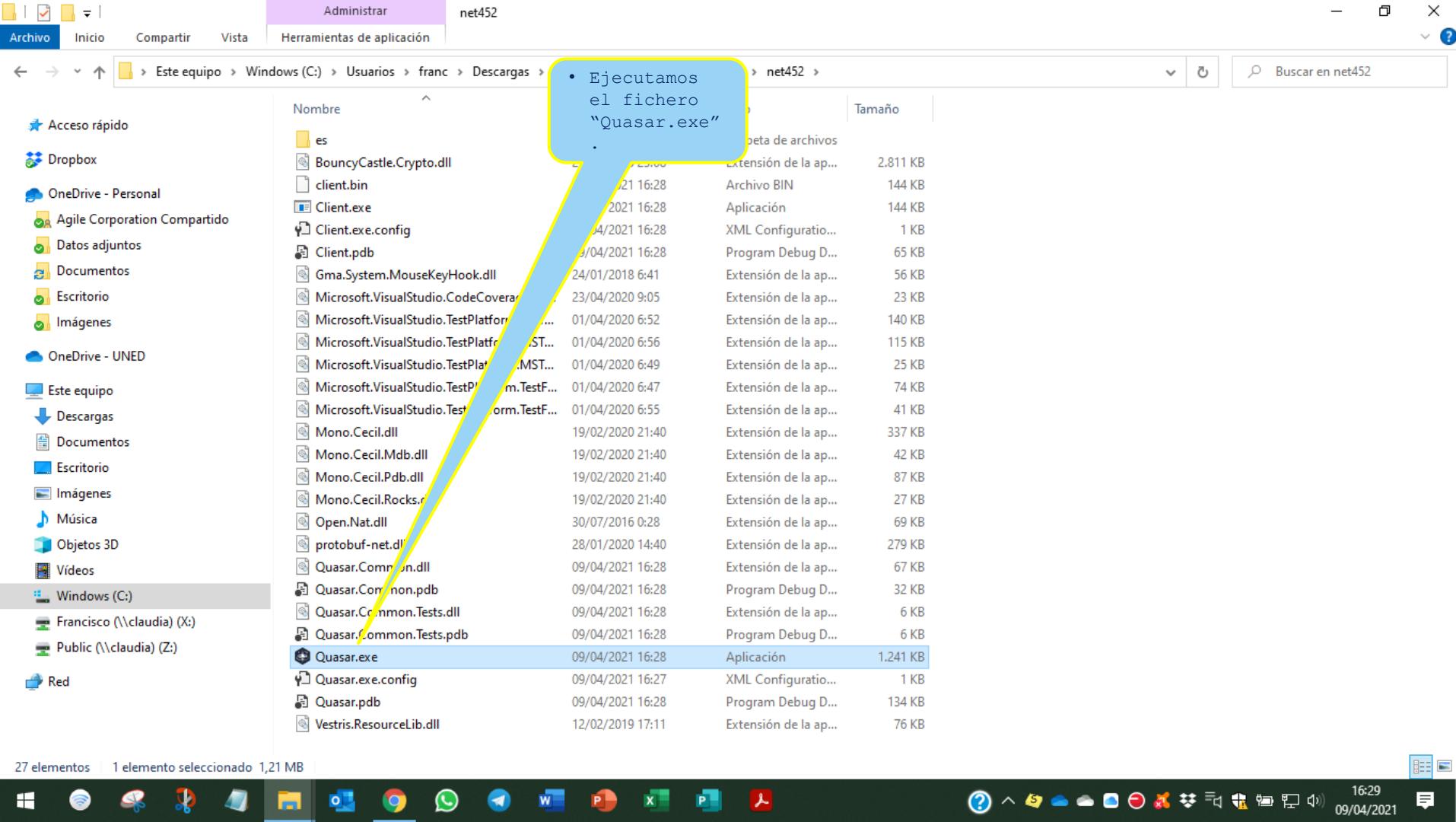
Este equipo > Descargas > Quasar-master > bin >

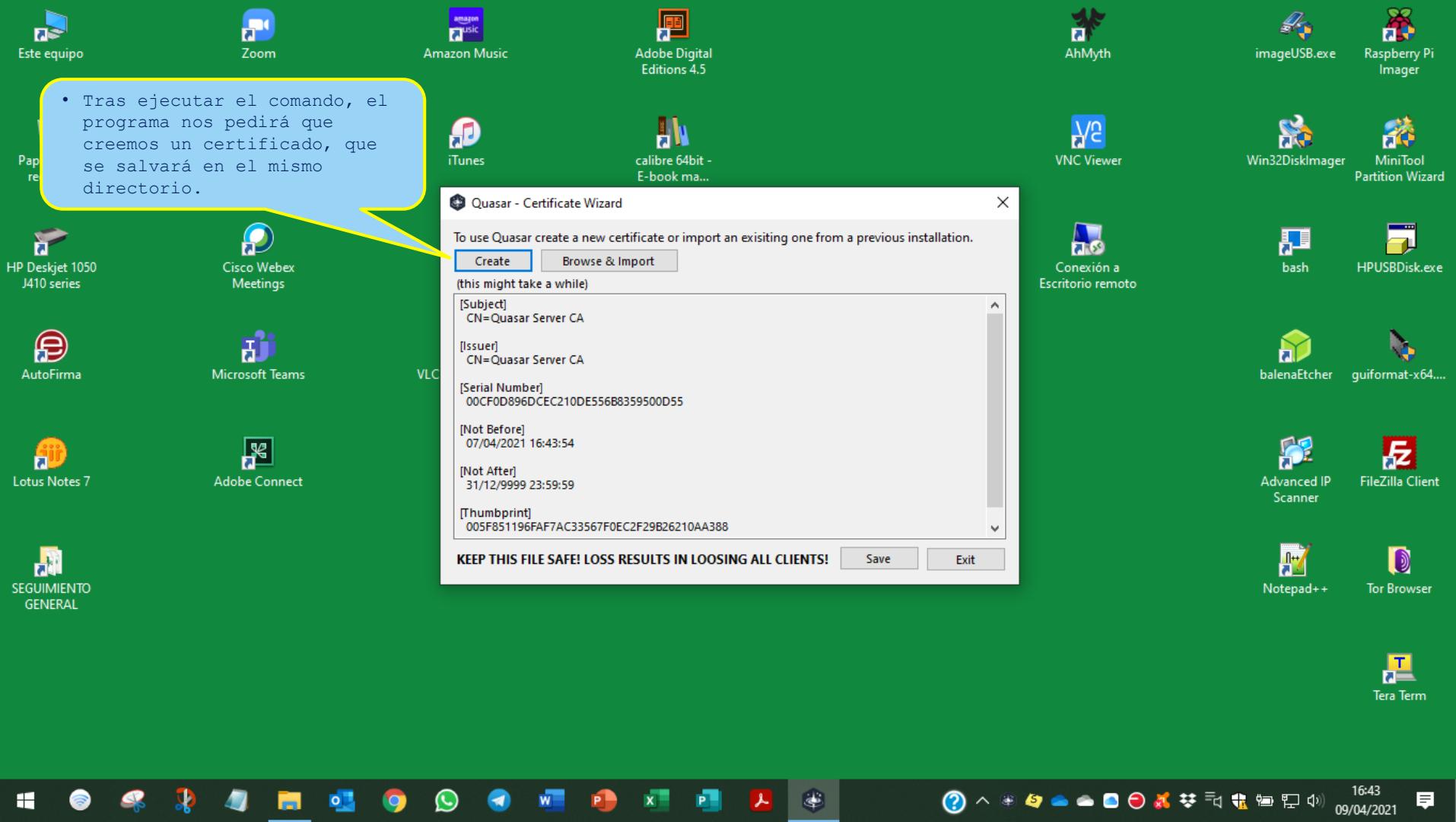
Nombre	Fecha de modificación	Tipo
Debug	09/04/2021 16:27	Carpeta de archivos
Release	09/04/2021 16:42	Carpeta de archivos

• Chequeamos que se haya creado el directorio "Release", lo abrimos y localizamos el fichero "Quasar.exe".  
• En este caso hemos compilado dos veces con las opciones Debug y Release, aunque esto no es necesario para la práctica.

2 elementos 1 elemento seleccionado

16:43 09/04/2021





net452

Archivo Inicio Compartir Vista

Este equipo > Windows (C:) > Usuarios > franc > Descargas > Quasar-master > bin > Release > net452 >

Buscar en net452

Acceso rápido

- Dropbox
- OneDrive - Personal
- OneDrive - UNED
- Este equipo
- Descargas
- Documentos
- Escritorio
- Imágenes
- Música
- Objetos 3D
- Vídeos
- Windows (C:)
- Francisco (\claudia) (X:)
- Public (\claudia) (Z:)

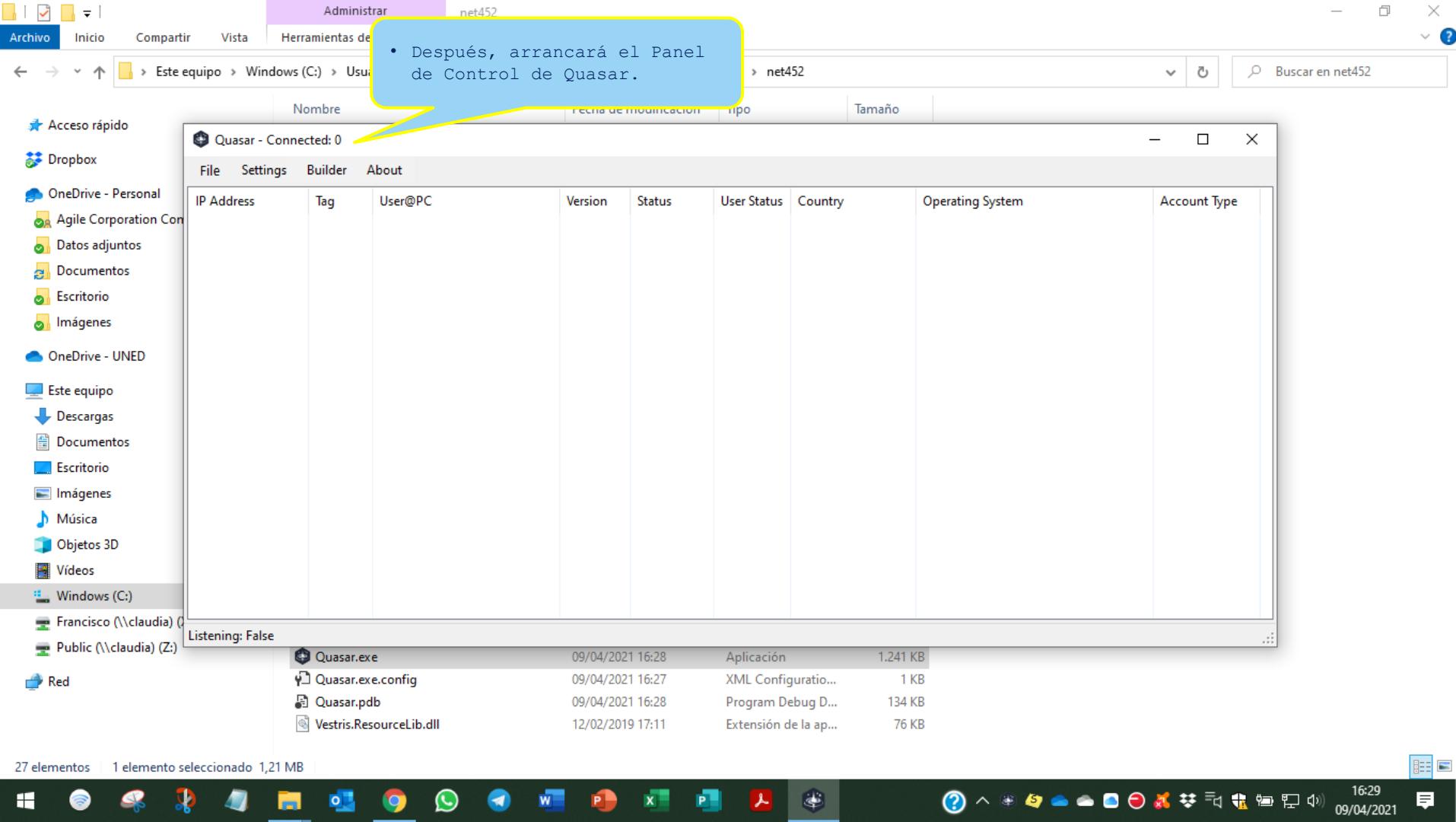
Red

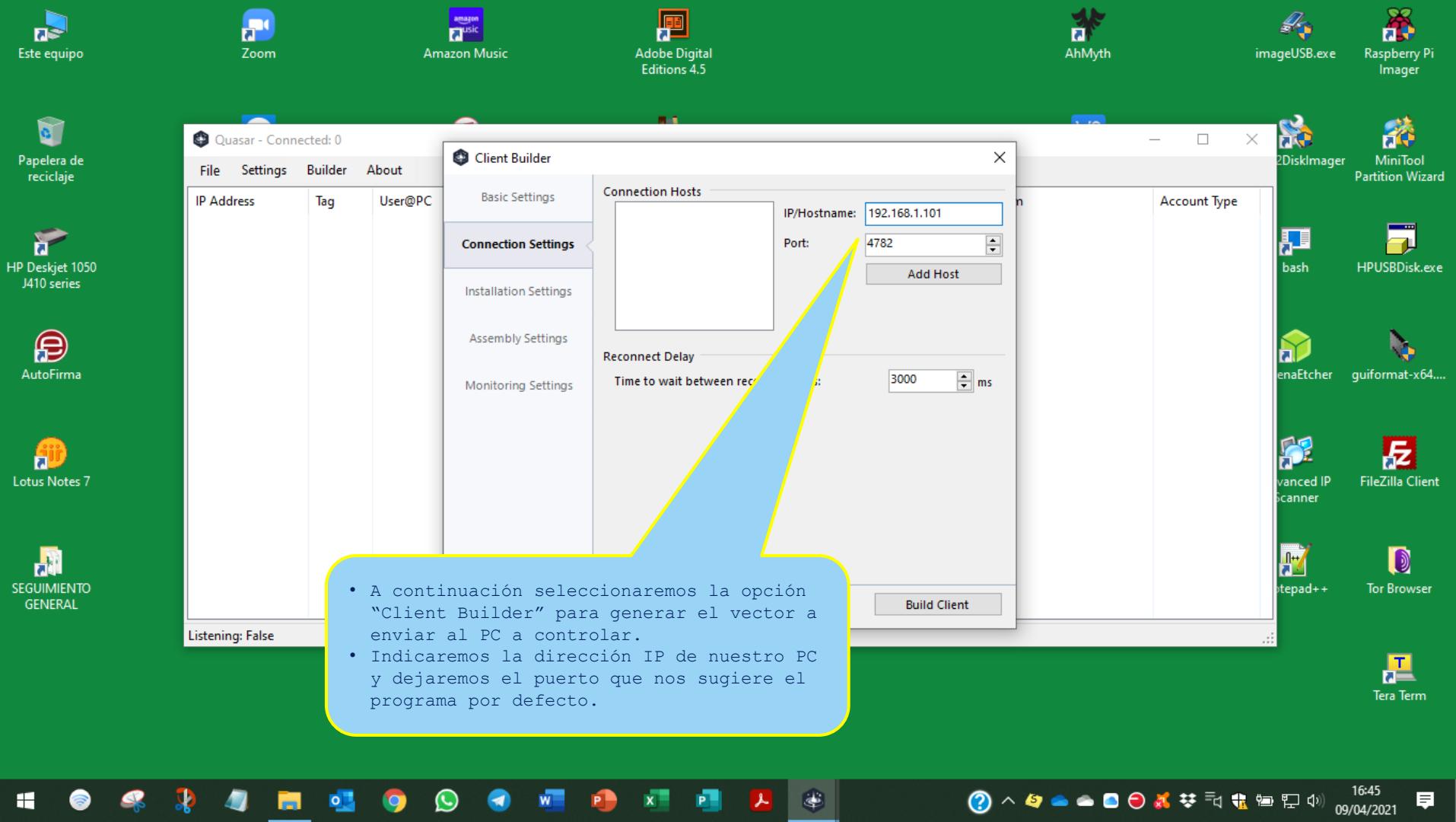
Nombre	Fecha de modificación	Tipo	Tamaño
es	09/04/2021 16:42	Carpeta de archivos	
BouncyCastle.Crypto.dll	29/03/2020 23:08	Extensión de la ap...	2.811 KB
client.bin	09/04/2021 16:42	Archivo BIN	2.844 KB
Client.exe	09/04/2021 16:42	Aplicación	2.844 KB
Client.exe.config	09/04/2021 16:42	XML Configuratio...	1 KB
Gma.System.MouseKeyHook.dll	24/01/2018 6:41	Extensión de la ap...	56 KB
Microsoft.VisualStudio.CodeCoverage.Sh...	23/04/2020 9:05	Extensión de la ap...	23 KB
Microsoft.VisualStudio.TestPlatform.MST...	01/04/2020 6:52	Extensión de la ap...	140 KB
Microsoft.VisualStudio.TestPlatform.MST...	01/04/2020 6:56	Extensión de la ap...	115 KB
Microsoft.VisualStudio.TestPlatform.MST...	01/04/2020 6:49	Extensión de la ap...	25 KB
Microsoft.VisualStudio.TestPlatform.TestF...	01/04/2020 6:47	Extensión de la ap...	74 KB
Microsoft.VisualStudio.TestPlatform.TestF...	01/04/2020 6:55	Extensión de la ap...	41 KB
Mono.Cecil.dll	19/02/2020 21:40	Extensión de la ap...	337 KB
Mono.Cecil.Mdb.dll	19/02/2020 21:40	Extensión de la ap...	42 KB
Mono.Cecil.Pdb.dll	19/02/2020 21:40	Extensión de la ap...	87 KB
Mono.Cecil.Rocks.dll	19/02/2020 21:40	Extensión de la ap...	27 KB
Open.Nat.dll	30/07/2016 0:28	Extensión de la ap...	69 KB
protobuf-net.dll	28/01/2020 14:40	Extensión de la ap...	279 KB
Quasar.Common.dll	09/04/2021 16:42	Extensión de la ap...	63 KB
Quasar.Common.Tests.dll	09/04/2021 16:42	Extensión de la ap...	6 KB
Quasar.exe	09/04/2021 16:42	Aplicación	1.221 KB
Quasar.exe.config	09/04/2021 16:42	XML Configuratio...	1 KB
quasar.p12	09/04/2021 16:44	Personal Informati...	5 KB
Vestrис.ResourceLib.dll	12/02/2019 17:11	Extensión de la ap...	76 KB

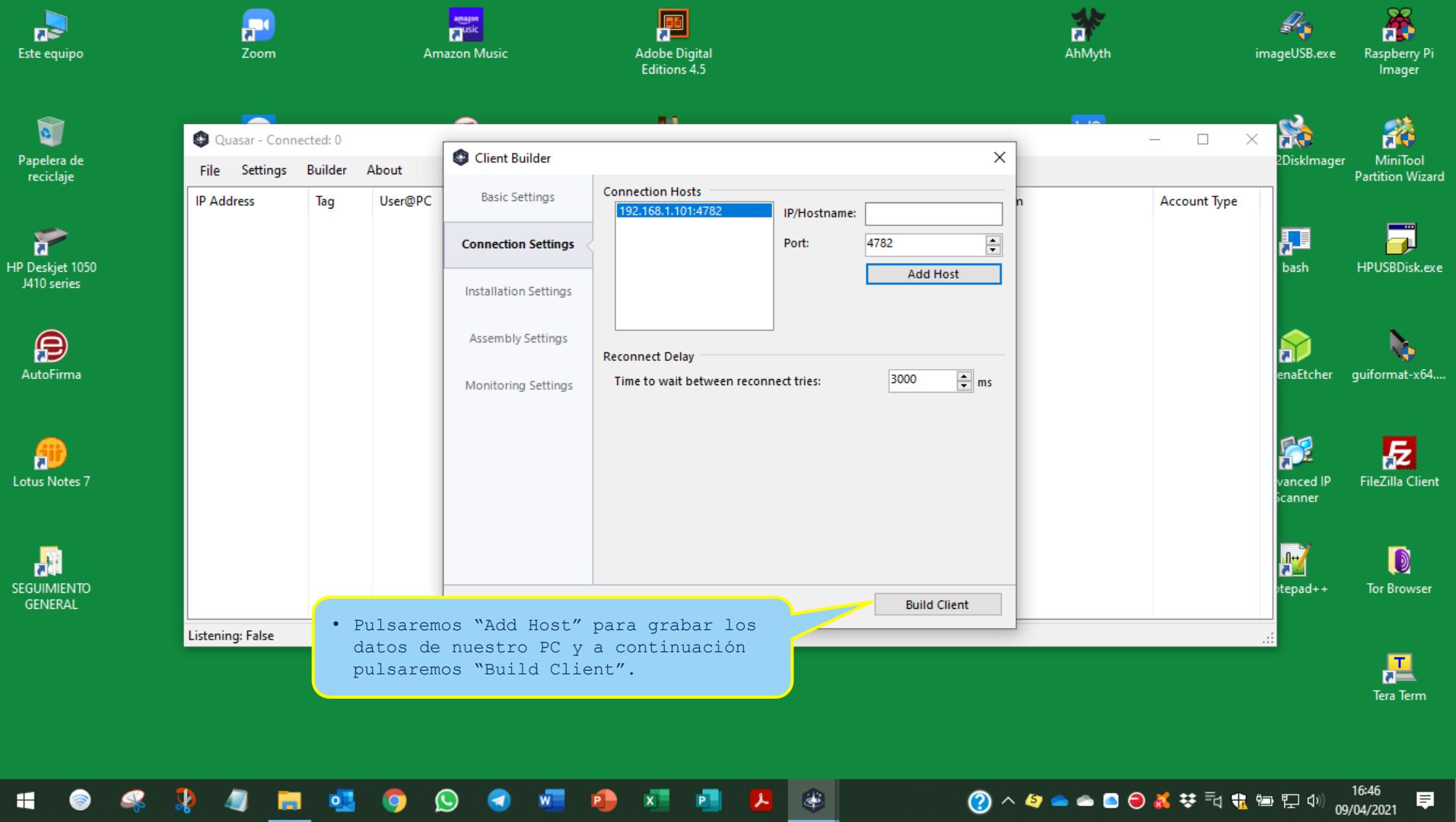
24 elementos 1 elemento seleccionado 4,16 KB

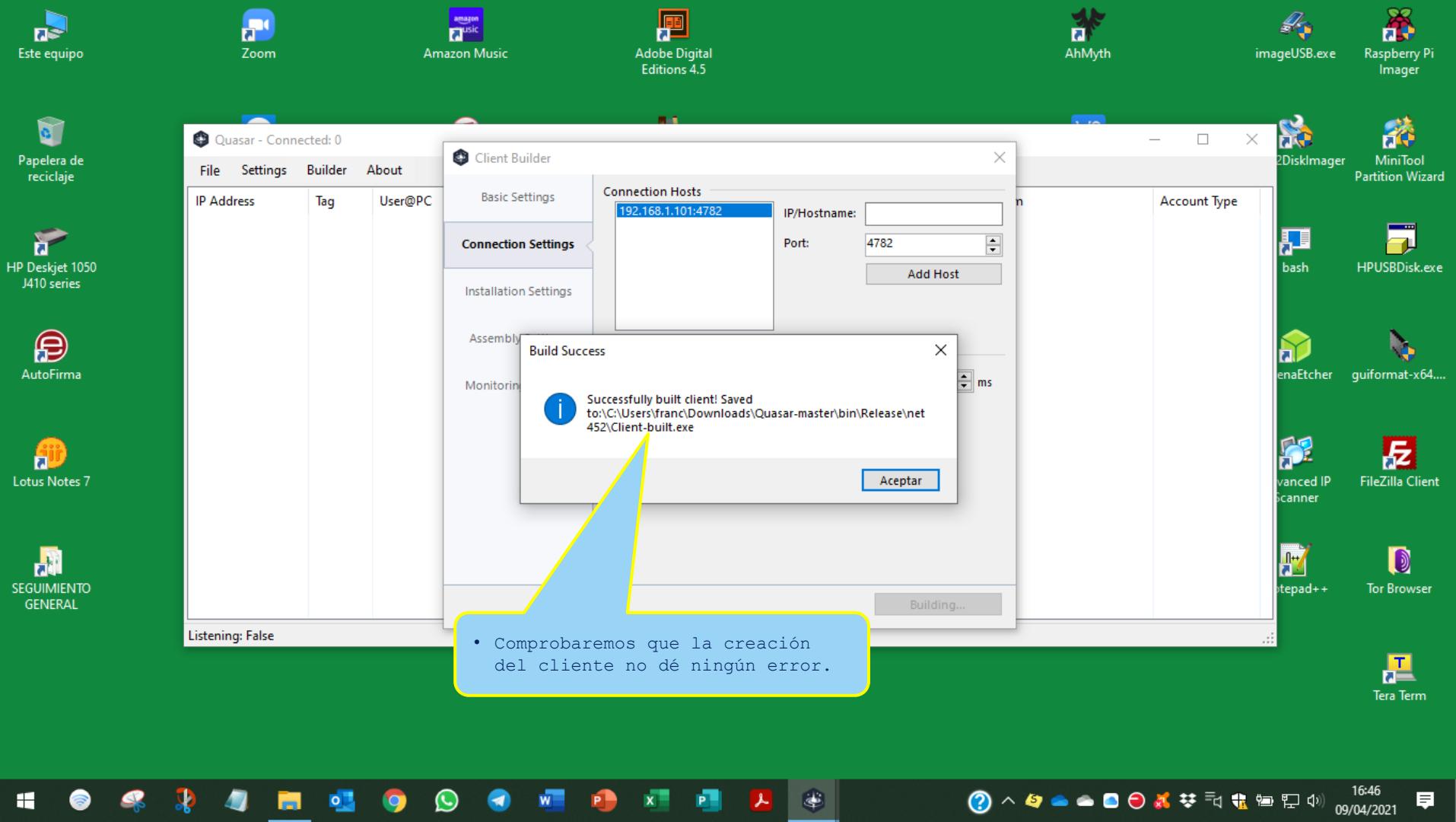
16:44 09/04/2021

- Conviene respaldar el certificado, pues si se pierde o se daña se perderá también la conexión con todos los PCs clientes.









- Comprobaremos que la creación del cliente no dé ningún error.

Administrador net452

Archivo Inicio Compartir Vista Herramientas de aplicación

PAKO\_8GB (D:) > Quasar-master > bin > Release > net452 >

Buscar en net452

Acceso rápido

- Dropbox
- OneDrive - Personal
- OneDrive - UNED
- Este equipo
- Descargas
- Documentos
- Escritorio
- Imágenes
- Música
- Objetos 3D
- Vídeos
- Windows (C:)
- PAKO\_8GB (D:)
- Francisco (\claudia) (X:)
- Public (\claudia) (Z:)
- PAKO\_8GB (D:)
- Red

Nombre	Fecha de modificación	Tipo	Tamaño
es	09/04/2021 16:47	Carpeta de archivos	
Profiles	09/04/2021 16:47	Carpeta de archivos	
BouncyCastle.Crypto.dll	29/03/2020 23:08	Extensión de la ap...	2.811 KB
client.bin	09/04/2021 16:42	Archivo BIN	2.844 KB
Client.exe	09/04/2021 16:42	Aplicación	2.844 KB
Client.exe.config	09/04/2021 16:42	XML Configuratio...	1 KB
<b>Client-built.exe</b>	<b>09/04/2021 16:46</b>	<b>Aplicación</b>	<b>2.831 KB</b>
Gma.System.MouseKeyHook.dll	24/01/2018 6:41	Extensión de la ap...	56 KB
Microsoft.VisualStudio.CodeCoverage.Sh...	23/04/2020 9:05	Extensión de la ap...	23 KB
Microsoft.VisualStudio.TestPlatform.M...	01/04/2020 6:52	Extensión de la ap...	140 KB
Microsoft.VisualStudio.TestPlatform.MST...	01/04/2020 6:56	Extensión de la ap...	115 KB
Microsoft.VisualStudio.TestPlatform.MST...	01/04/2020 6:56	Extensión de la ap...	25 KB
Microsoft.VisualStudio.TestPlatform.TestF...	01/04/2020 6:56	Extensión de la ap...	74 KB
Microsoft.VisualStudio.TestPlatform.TestF...	01/04/2020 6:55	Extensión de la ap...	41 KB
Mono.Cecil.dll	19/02/2020 21:40	Extensión de la ap...	337 KB
Mono.Cecil.Mdb.dll	19/02/2020 21:40	Extensión de la ap...	12 KB
Mono.Cecil.Pdb.dll	19/02/2020 21:40	Extensión de la ap...	
Mono.Cecil.Rocks.dll	19/02/2020 21:40	Extensión de la ap...	
Open.Nat.dll	30/07/2016 0:28	Extensión de la ap...	
protobuf-net.dll	28/01/2020 14:40	Extensión de la ap...	
Quasar.Common.dll	09/04/2021 16:42	Extensión de la ap...	63 KB
Quasar.Common.Tests.dll	09/04/2021 16:42	Extensión de la ap...	6 KB
Quasar.exe	09/04/2021 16:42	Aplicación	1.221 KB
Quasar.exe.config	09/04/2021 16:42	XML Configuratio...	1 KB
quasar.p12	09/04/2021 16:44	Personal Informati...	5 KB
Vestris.ResourceLib.dll	12/02/2019 17:11	Extensión de la ap...	76 KB

26 elementos 1 elemento seleccionado 2,76 MB

16:48 09/04/2021

• Comprobaremos que se ha creado el fichero "Client-built.exe" en el mismo directorio.

Administrador net452

Archivo Inicio Compartir Vista Herramientas de aplicación

PAKO\_8GB (D:) > Quasar-master > bin > Release > net452 >

Buscar en net452

Acceso rápido

- Dropbox
- OneDrive - Personal
- OneDrive - UNED
- Este equipo
- Descargas
- Documentos
- Escritorio
- Imágenes
- Música
- Objetos 3D
- Vídeos
- Windows (C:)
- PAKO\_8GB (D:)
- Francisco (\claudia) (X:)
- Public (\claudia) (Z:)
- PAKO\_8GB (D:)
- Red

Nombre	Fecha de modificación	Tipo	Tamaño
es	09/04/2021 16:47	Carpeta de archivos	
Profiles	09/04/2021 16:47	Carpeta de archivos	
BouncyCastle.Crypto.dll	29/03/2020 23:08	Extensión de la ap...	2.811 KB
client.bin	09/04/2021 16:42	Archivo BIN	2.844 KB
Client.exe	09/04/2021 16:42	Aplicación	2.844 KB
Client.exe.config	09/04/2021 16:42	XML Configuratio...	1 KB
Client-built.exe	09/04/2021 16:46	Aplicación	2.831 KB
EJECUTAME.exe	09/04/2021 16:46	Aplicación	2.831 KB
Gma.System.MouseKeyHook.dll	24/01/2018 6:41	Extensión de la ap...	56 KB
Microsoft.VisualStudio.CodeCoverage.Sh...	23/04/2020 9:05	Extensión de la ap...	23 KB
Microsoft.VisualStudio.TestPlatform.MST...	01/04/2020 6:52	Extensión de la ap...	140 KB
Microsoft.VisualStudio.TestTools.UITestForm.MST...	01/04/2020 6:56	Extensión de la ap...	115 KB
Microsoft.VisualStudio.TestTools.UnitTesting.MST...	01/04/2020 6:49	Extensión de la ap...	25 KB
Microsoft.VisualStudio.TestTools.UnitTesting.MST...	01/04/2020 6:47	Extensión de la ap...	74 KB
Microsoft.VisualStudio.TestTools.UnitTesting.MST...	01/04/2020 6:55	Extensión de la ap...	41 KB
Mono.Cecil.dll	21/04/2018 21:40	Extensión de la ap...	337 KB

Este fichero es el vector que tendremos que conseguir que se ejecute en el PC remoto, por lo que es conveniente darle un nombre adecuado.

Cuando se usa Quasar para mantenimiento remoto, se pide al usuario que ejecute este fichero voluntariamente.

En los ejercicios de Penetration Testing, este fichero se suele disimular lo mejor posible para que el usuario lo ejecute inadvertidamente (su ejecución es rapidísima y sin ninguna respuesta).

**NOTA IMPORTANTE.** Aprovechamos para recordar que esta práctica tiene fines exclusivamente formativos, y que las técnicas descritas en ella deberán usarse siempre con buen fin.

27 elementos 1 elemento seleccionado 2,76 MB

16:49 09/04/2021



Este equipo



Zoom



Amazon Music



Adobe Digital  
Editions 4.5



AhMyth



imageUSB.exe



Raspberry Pi  
Imager



Papelera de  
reciclaje



HP Deskjet 1050  
J410 series



AutoFirma



Lotus Notes 7



SEGUIMIENTO  
GENERAL

Quasar - Connected: 1

File Settings Builder About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
192.168.1.55	pc_obj...	franc@PC-CRISTINA-HP	1.4.0	Connected	Active	España [ES]	Windows 10 Home 64 Bit	User

Listening on port 4782.

• En cuanto se ejecute el vector, el PC remoto aparecerá inmediatamente en el Panel de Control de Quasar y una ventana emergente nos notificará este hecho.

Quasar Server

i Client connected from España!  
IP Address: 192.168.1.55  
Operating System: Windows 10 Home  
64 Bit



Este equipo



Zoom



Amazon Music



Adobe Digital Editions 4.5



AhMyth



imageUSB.exe



Raspberry Pi Imager



Papelera de reciclaje

HP Deskjet 1050  
J410 series

AutoFirma



Lotus Notes 7

SEGUIMIENTO  
GENERAL

Quasar - Connected: 1 [Selected: 1]

File Settings Builder About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
192.168.1.55	pc_obj...	franc@PC-CRISTINA-HD	1.4.0	Connected	Active	España [ES]	Windows 10 Home 64 Bit	User

Administration ▾

- System Information
- File Manager
- Startup Manager
- Task Manager
- Remote Shell
- TCP Connections
- Reverse Proxy
- Registry Editor
- Remote Execute ▾
- Actions ▾

Listening on port 4782.

Pulsando con el botón derecho del ratón sobre el PC remoto, se desplegará el menú de control, que mostrará las diferentes acciones que se pueden ejecutar.

En esta imagen se muestra el menú "Administración".



Tera Term



Este equipo



Zoom



Amazon Music



Adobe Digital Editions 4.5



AhMyth



imageUSB.exe



Raspberry Pi Imager



Papelera de reciclaje

HP Deskjet 1050  
J410 series

AutoFirma



Lotus Notes 7

SEGUIMIENTO  
GENERAL

Quasar - Connected: 1 [Selected: 1]

File   Settings   Builder   About

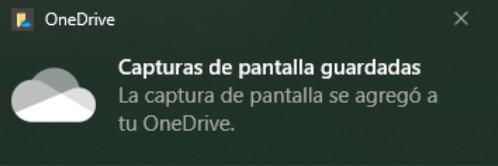
IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
192.168.1.55	pc_obj...	franc@PC-CRISTINA-HP	1.4.0	Connected	Active	España [ES]	Windows 10 Home 64 Bit	User

Administration

- Monitoring
- User Support
- Client Management
- Select All

• Menú “Monitorización”.

Listening on port 4782.





Este equipo



Zoom



Amazon Music



Adobe Digital Editions 4.5



AhMyth



imageUSB.exe



Raspberry Pi Imager



Papelera de reciclaje

HP Deskjet 1050  
J410 series

AutoFirma



Lotus Notes 7

SEGUIMIENTO  
GENERAL

Quasar - Connected: 1 [Selected: 1]

File   Settings   Builder   About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
192.168.1.55	pc_obj...	franc@PC-CRISTINA-HP	1.4.0	Connected	Active	España [ES]	Windows 10 Home 64 Bit	User

Administration

Monitoring

User Support

Client Management

All

Show Messagebox

Remote Desktop

Send to Website

• Menú "Soporte al Usuario".

Listening on port 4782.





Este equipo



Zoom



Amazon Music



Adobe Digital Editions 4.5



AhMyth



imageUSB.exe

Raspberry Pi  
ImagerPapelera de  
reciclajeHP Deskjet 1050  
J410 series

AutoFirma



Lotus Notes 7

SEGUIMIENTO  
GENERAL

Quasar - Connected: 1 [Selected: 1]

File Settings Builder About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
192.168.1.55	pc_obj...	franc@PC-CRISTINA-HP	1.4.0	Connected	Active	España [ES]	Windows 10 Home 64 Bit	User

Administration

Monitoring

User Support

Client Management

Elevate Client Permissions

Update

Reconnect

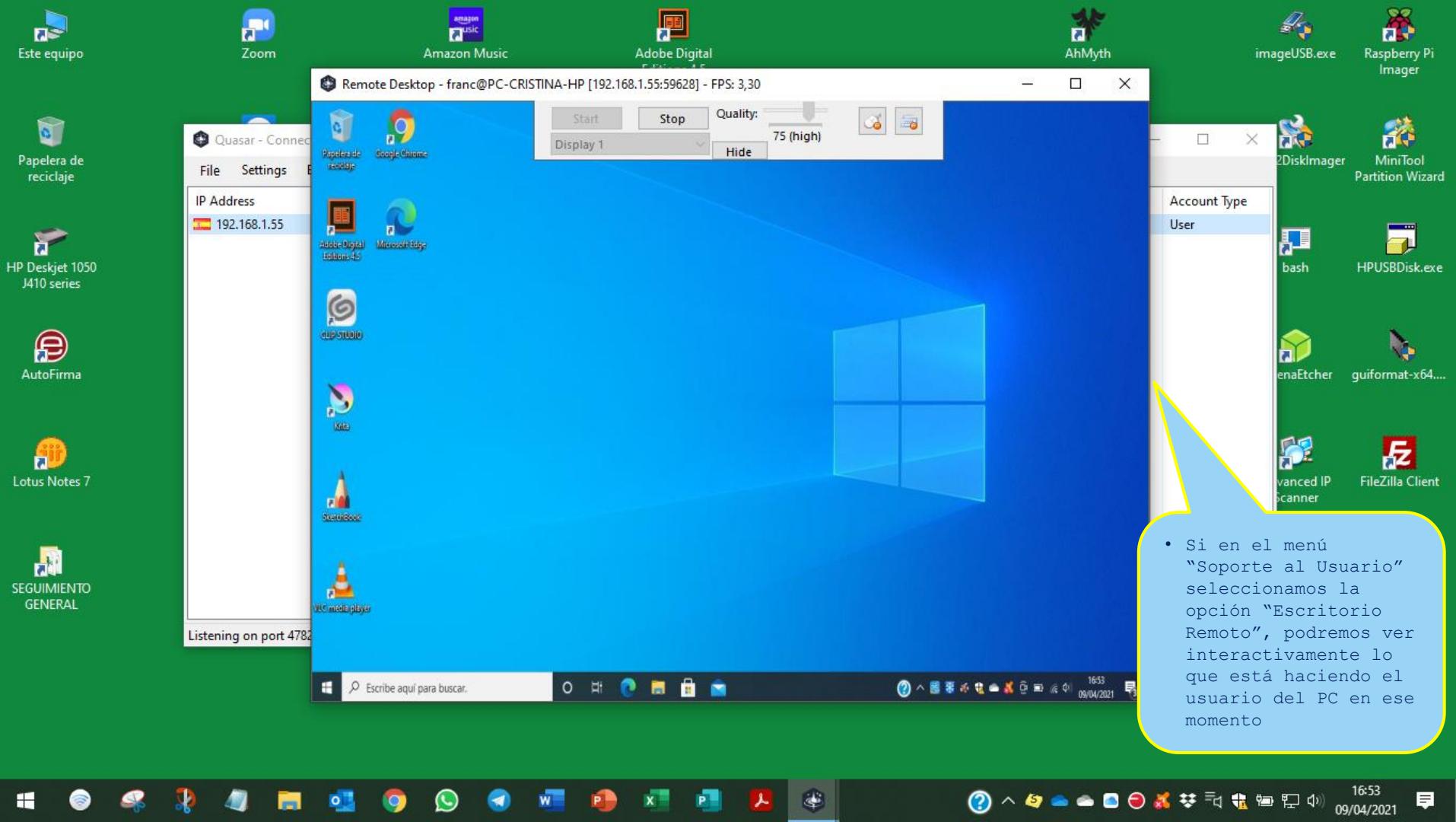
Disconnect

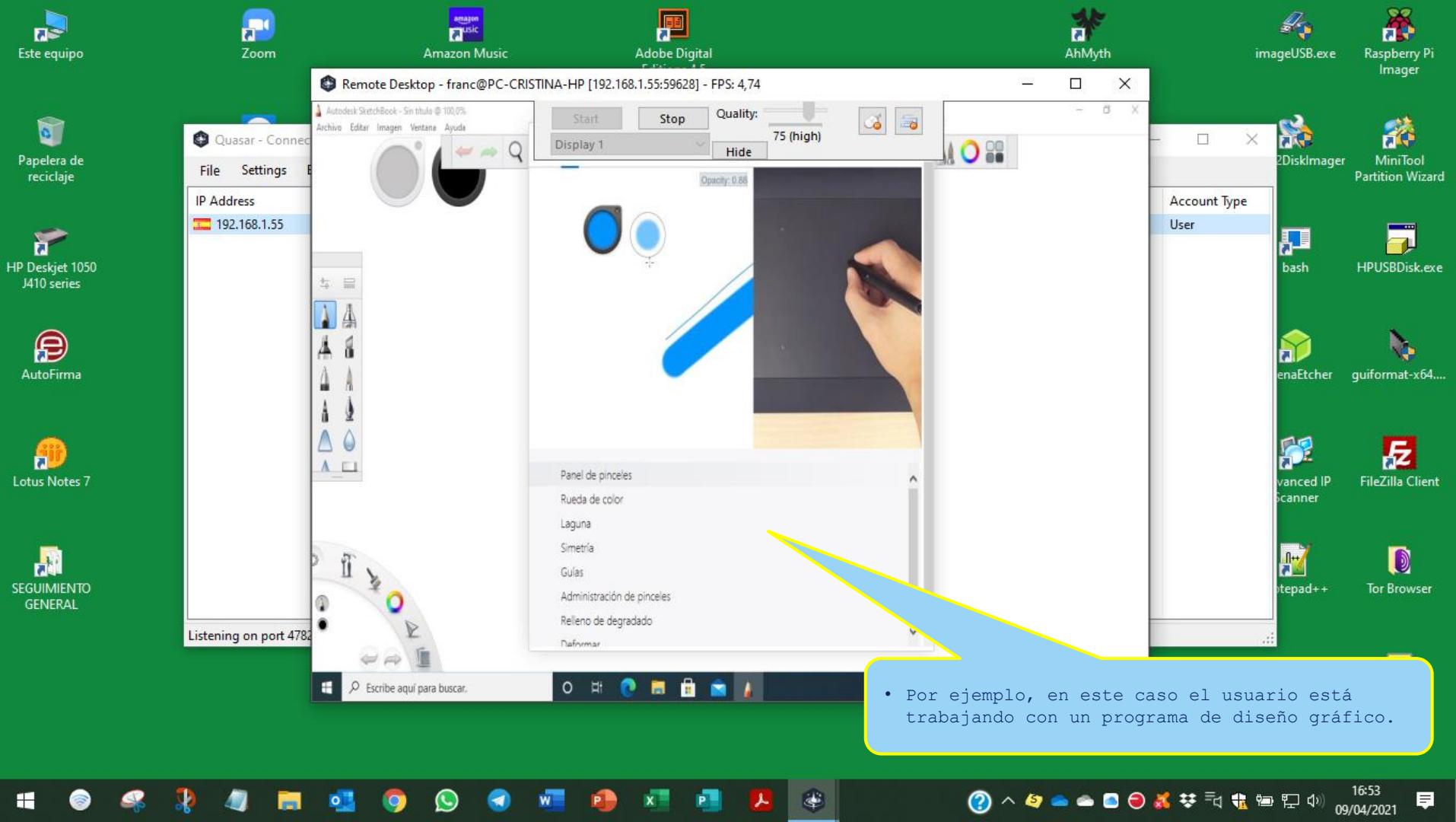
Uninstall

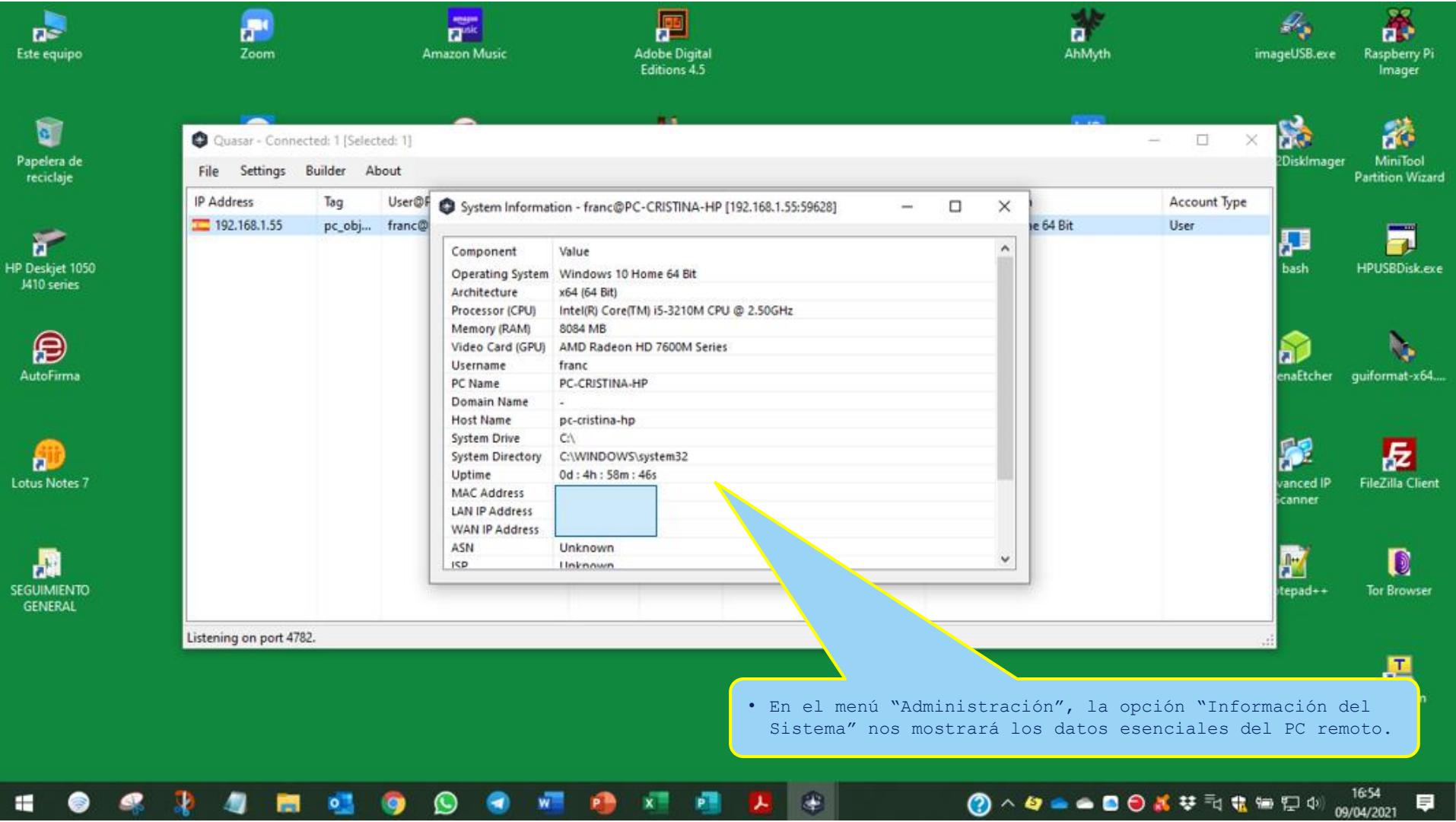
• Menú "Gestión del Cliente".

Listening on port 4782.

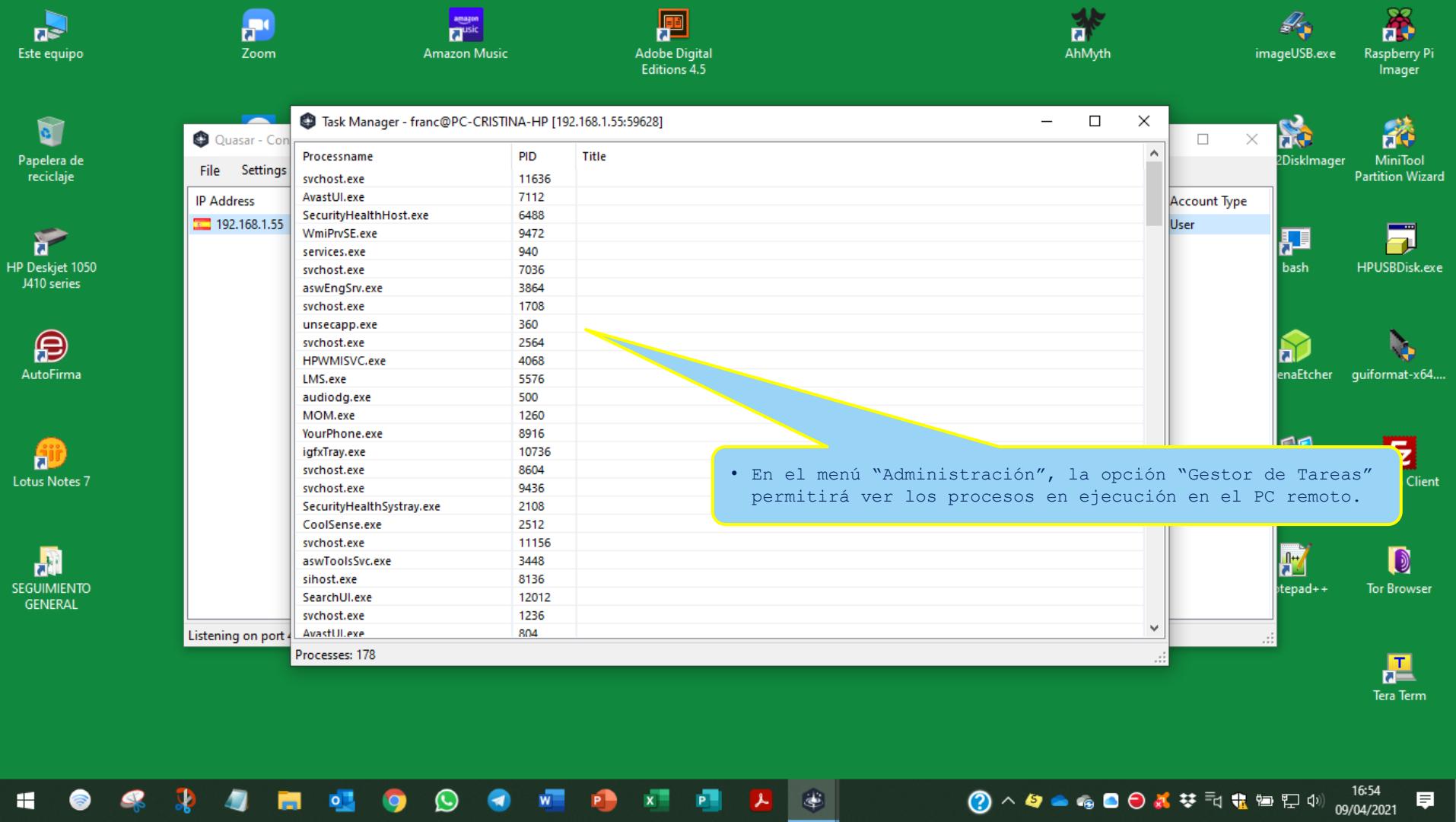


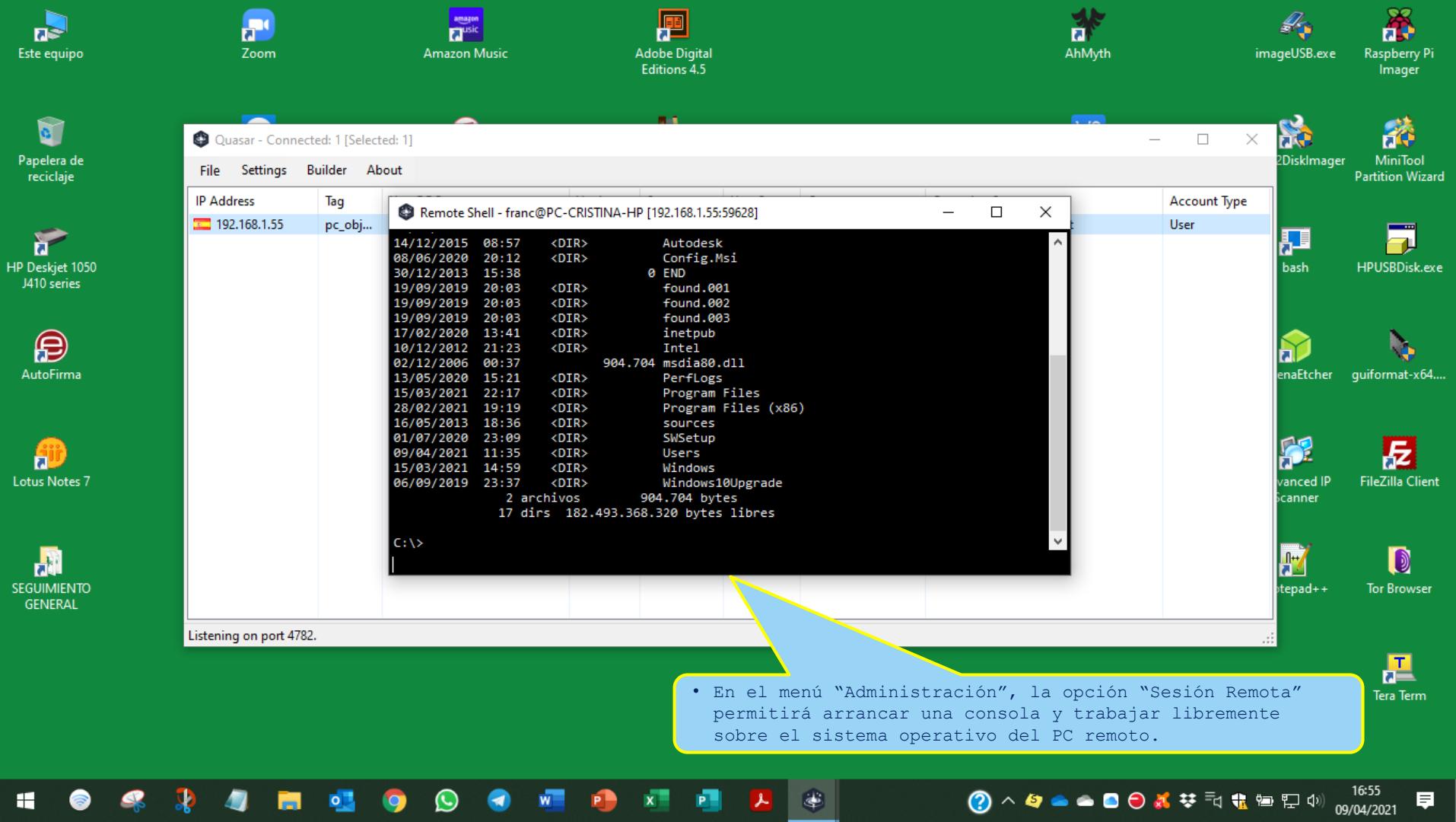


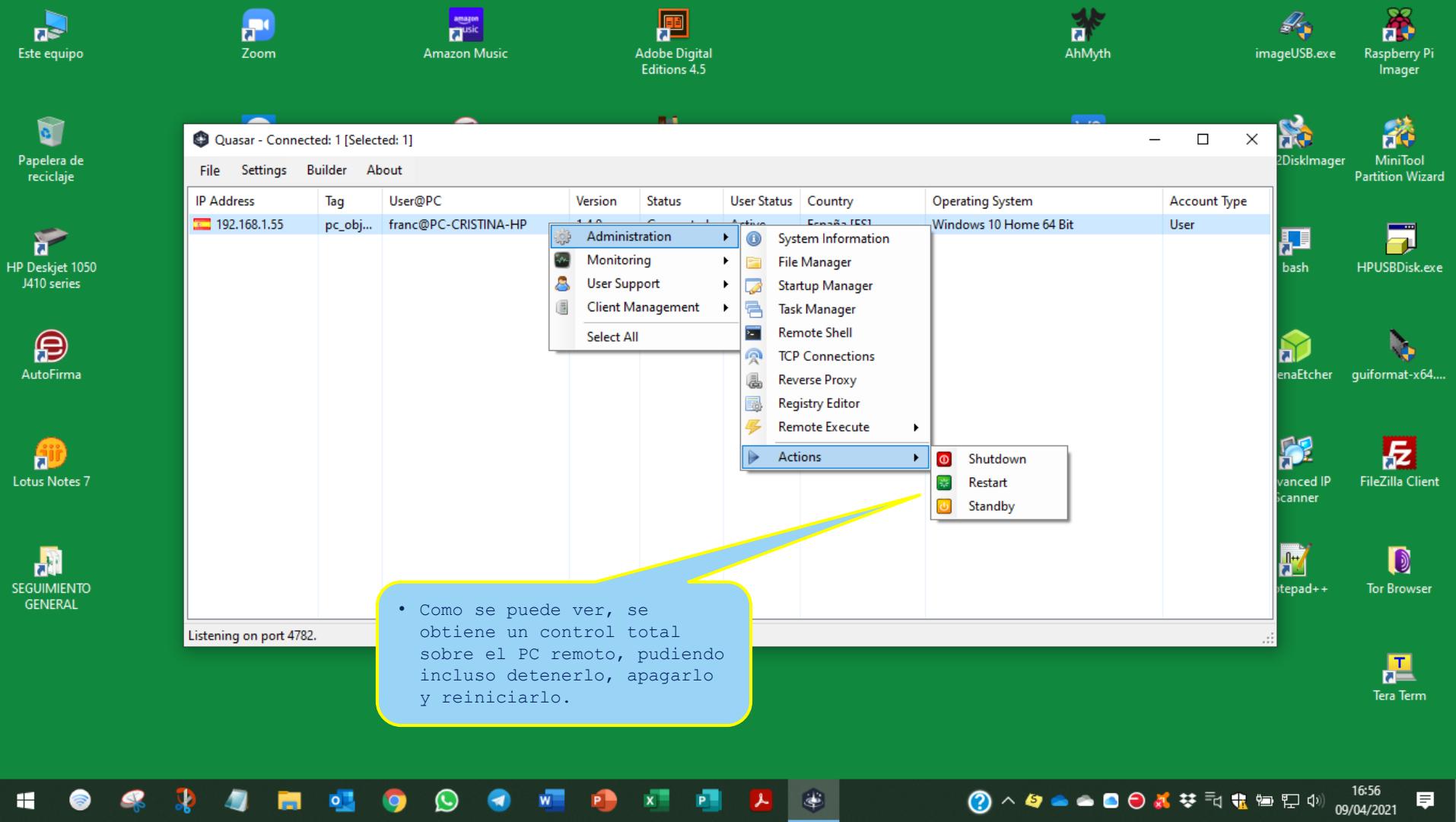


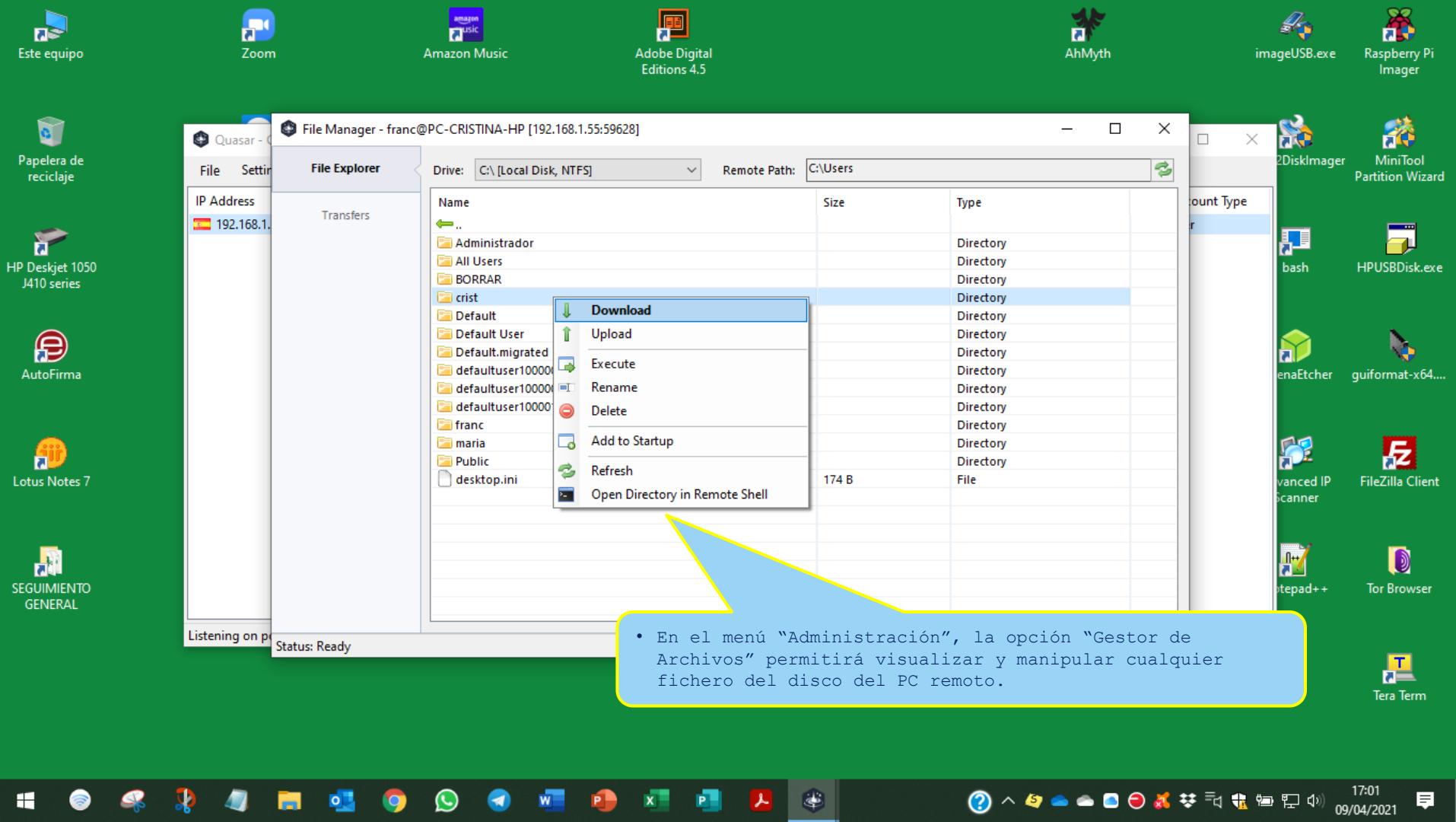


- En el menú "Administración", la opción "Información del Sistema" nos mostrará los datos esenciales del PC remoto.











Este equipo



Zoom



Amazon Music



Adobe Digital  
Editions 4.5



AhMyth



imageUSB.exe



Raspberry Pi  
Imager



Papelera de  
reciclaje



HP Deskjet 1050  
J410 series



AutoFirma



Lotus Notes 7



SEGUIMIENTO  
GENERAL

Quasar - Connected: 1 [Selected: 1]

File Settings Builder About

IP Address Tag

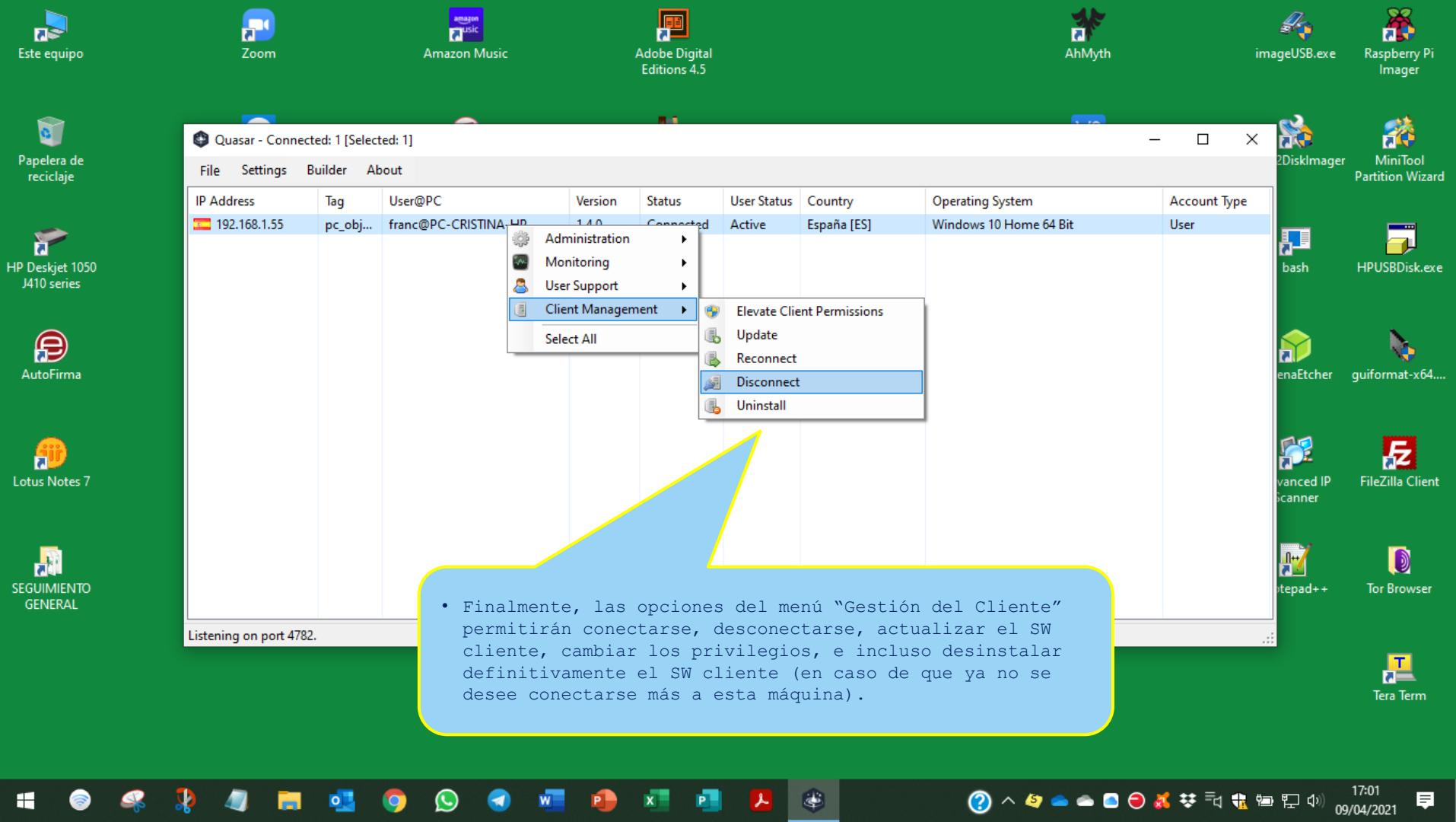
192.168.1.55	pc_obj.
--------------	---------

Startup Manager - franc@PC-CRISTINA-HP [192.168.1.55:59628]

Name	Path
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	C:\WINDOWS\system32\SecurityHealthSystray.exe
SecurityHealth	C:\WINDOWS\system32\SecurityHealthSystray.exe
AvastUI.exe	"C:\Program Files\AVAST Software\Avast\AvLaunch.exe" /gui
AdobeGCIInvoker-1.0	"C:\Program Files (x86)\Common Files\Adobe\AdobeGCCClient\AGCIInvokerUtility.exe"
AdobeAAMUpdater-1.0	"C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtili..."
SynTPEnh	C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	
OneDrive	"C:\Program Files (x86)\Microsoft OneDrive\OneDrive.exe" /background

Listening on port 4782.

- En el menú "Administración", la opción "Gestor de Arranque" permitirá ver cuáles son los procesos que se ejecutan en el arranque del PC.



# Bibliografía

- [www.kali.org](http://www.kali.org)
- [www.github.com](http://www.github.com)
- [www.incibe.es](http://www.incibe.es)
- [www.Microsoft.com](http://www.Microsoft.com)
- <https://github.com/AhMyth/AhMyth-Android-RAT>
- <https://github.com/quasar/Quasar.git>