The Dude
Sistema de monitoreo

Potente, practico y gratuito

https://mikrotik.com/thedude

DaveNISC
Expertos en seguridad informática

David Vega

Analista de seguridad informática

Cisco CCNA Cyber Ops - Security Analyst Nessus - ISO/IEC 27001

www.davenisc.com

Historia:

- Inicios en 2004 hasta 2009 en Apartado Antioquia **PSSPC** taller de mantenimiento.
- Luego en 2010 hasta 2018 en Bogotá **NISC** (Network Integration Services Colombia) Licenciamiento y Telecomunicaciones
- Actualmente 2019 en Bogotá **DaveNISC** Analista de seguridad informática, licenciamiento, telecomunicaciones, hacking ético, programación, asesorías, charlas, entre otros.

2019

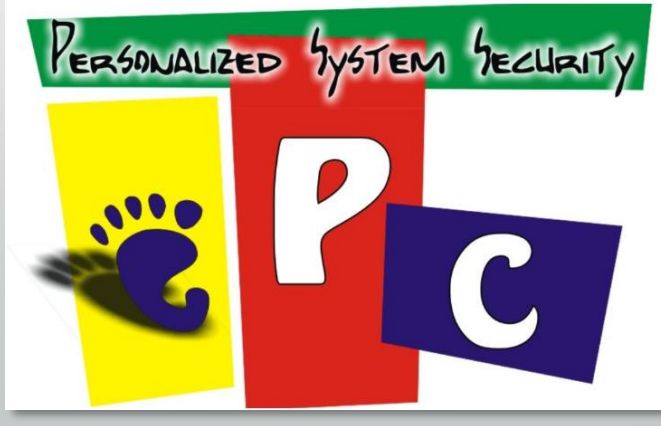
DaveNISC

Expertos en seguridad informática

2010 - 2018

Seguridad informática al alcance de todos

2004 - 2009



DaveNISC
Expertos en seguridad informática

3
Países

36
Clientes

Agenda

1. Ventajas the-dude
2. Instalación en Windows y Linux
3. Interfaz web
4. ¿Que se puede monitorear con the-dude?
5. Sistema de alertas
6. Notificaciones con Telegram

Sistema de monitoreo con The Dude

Ventajas:

1. Fácil integración con RB Mikrotik
2. Instalación en Windows o Linux
3. Interfaz web
4. Monitoreo en tiempo real
5. Sistema de alertas

Instalación

Sistemas recomendados
Windows 10 y 7

Sistemas recomendados
Ubuntu y Debian

Requisitos del sistema

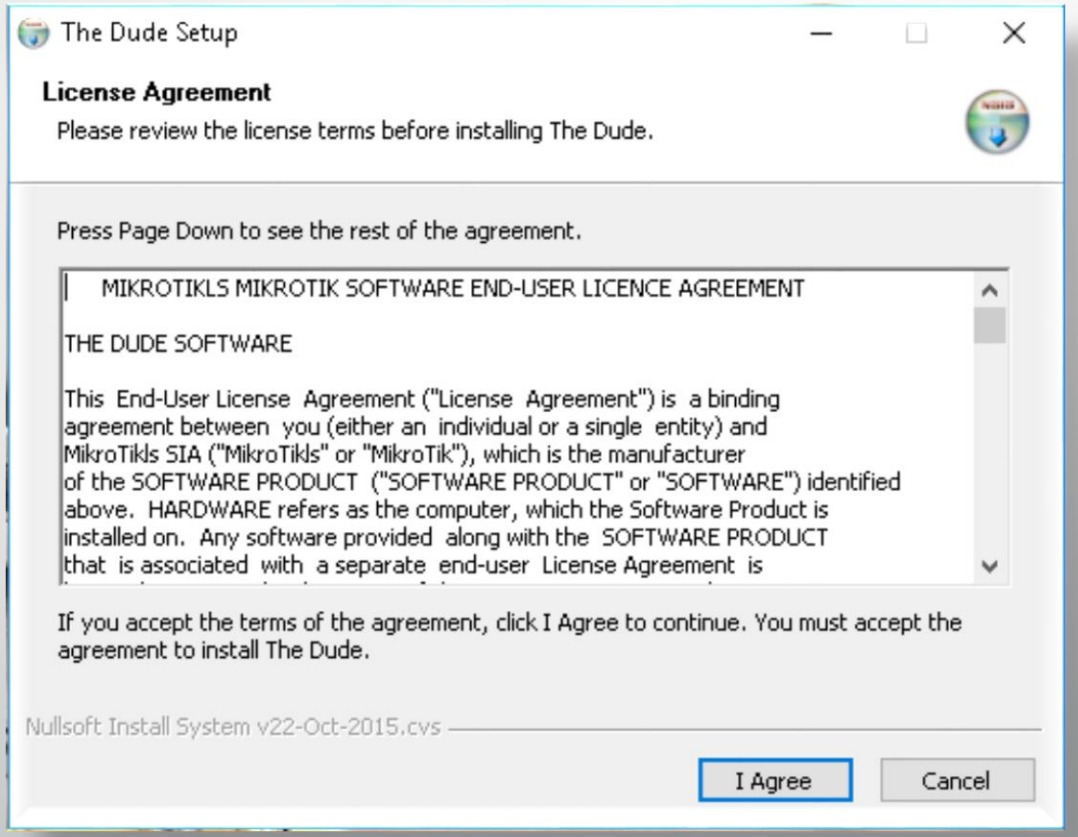
RouterOS:

- v6.34rc13 o superior

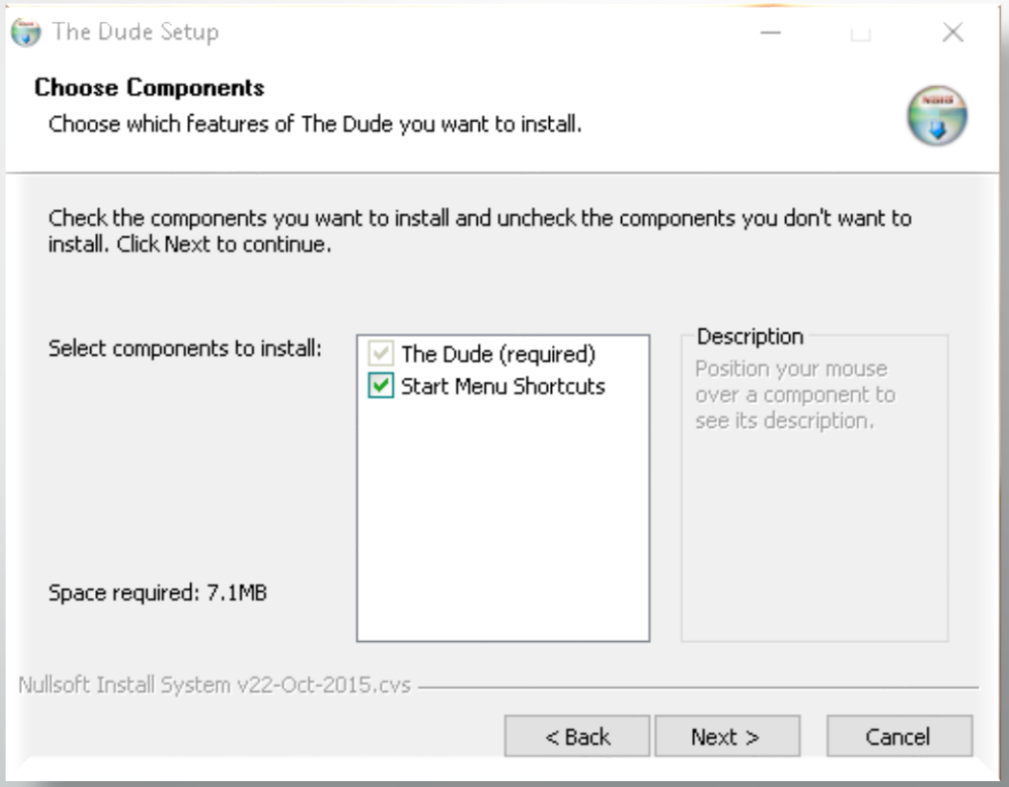
Hardware:

- TILE devices;
- ARM devices;
- MMIPS devices;
- RouterOS x86 installations;
- RouterOS CHR environment
- NO con SMIPS → hAP mini y hAP lite

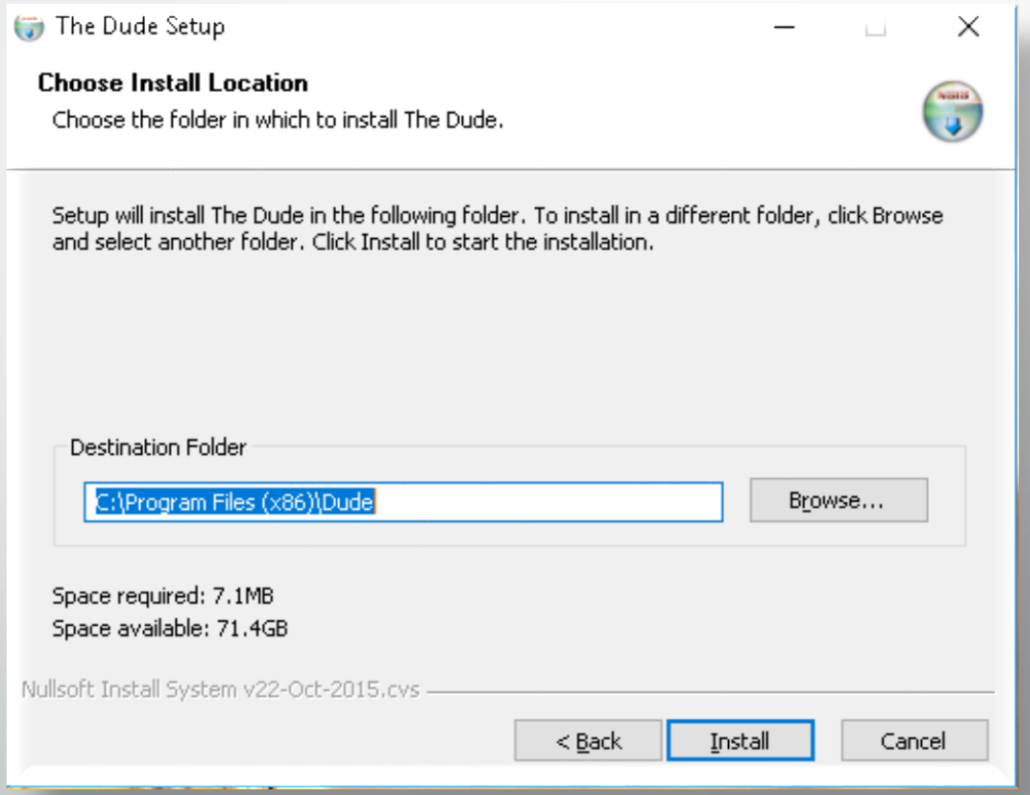
Instalación en Windows



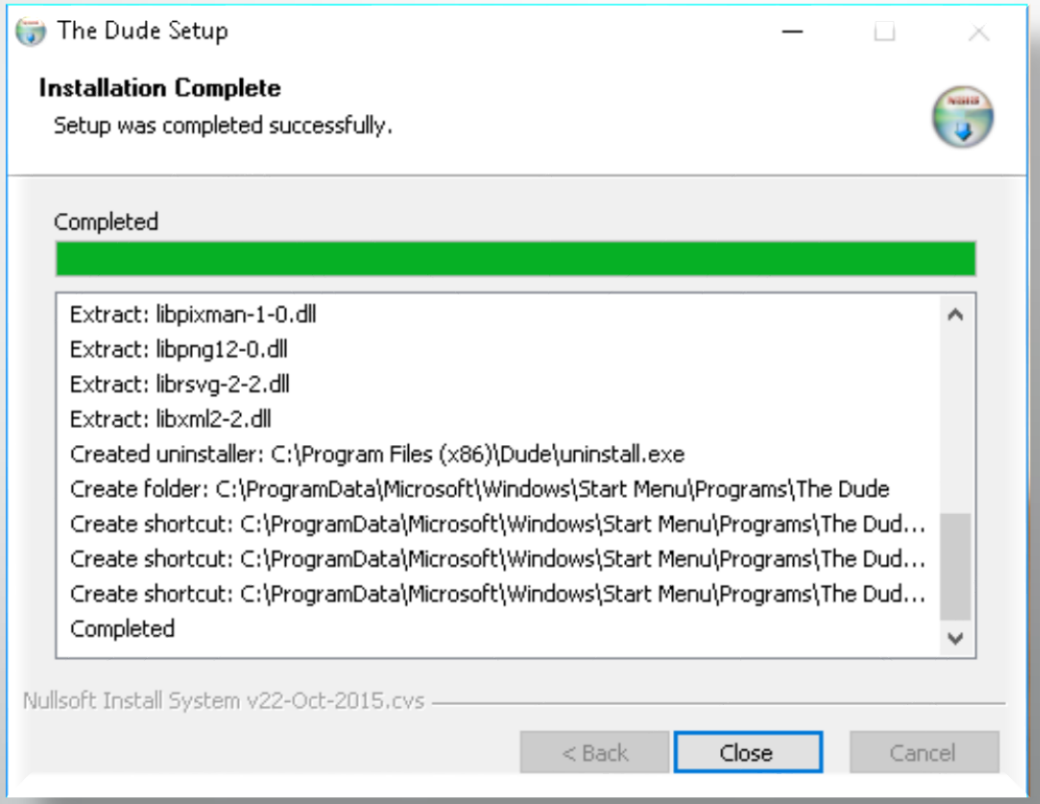
Instalación en Windows



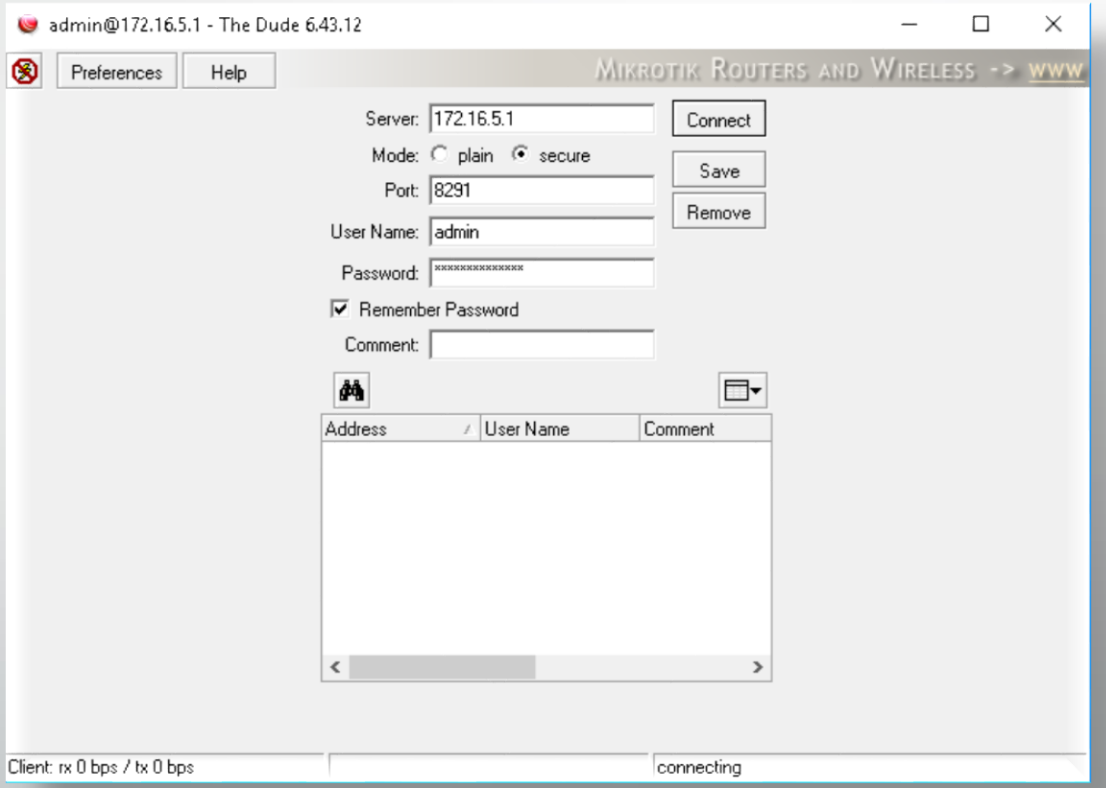
Instalación en Windows



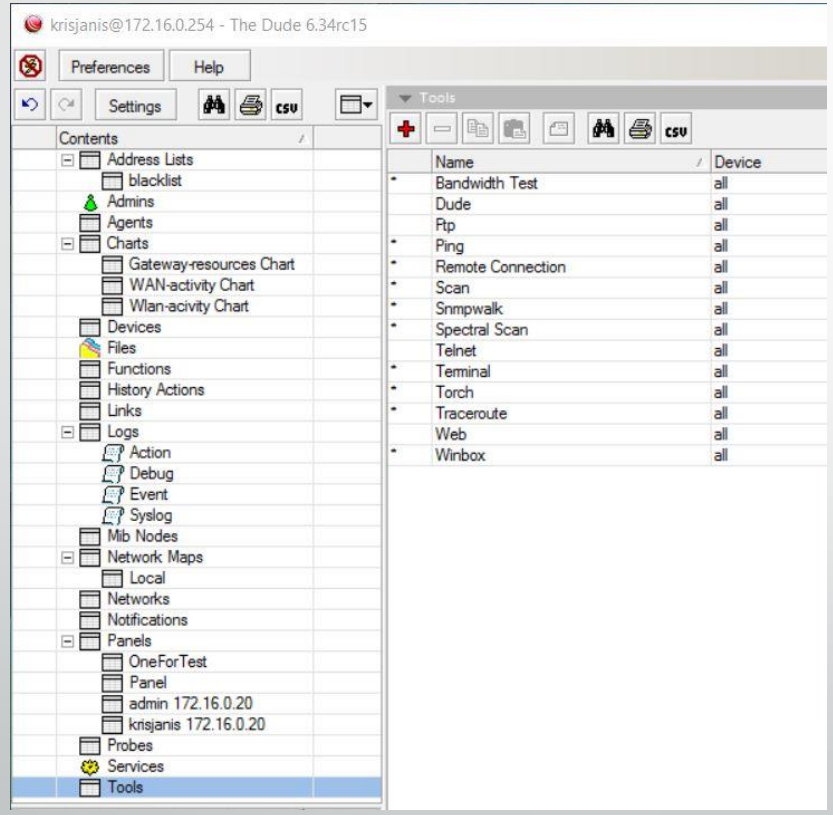
Instalación en Windows

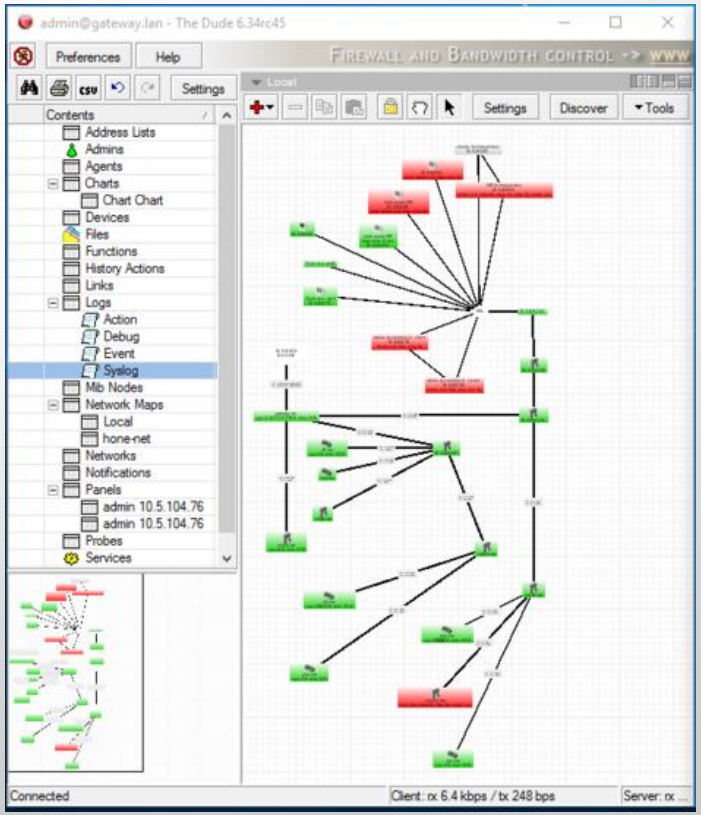


Instalación en Windows

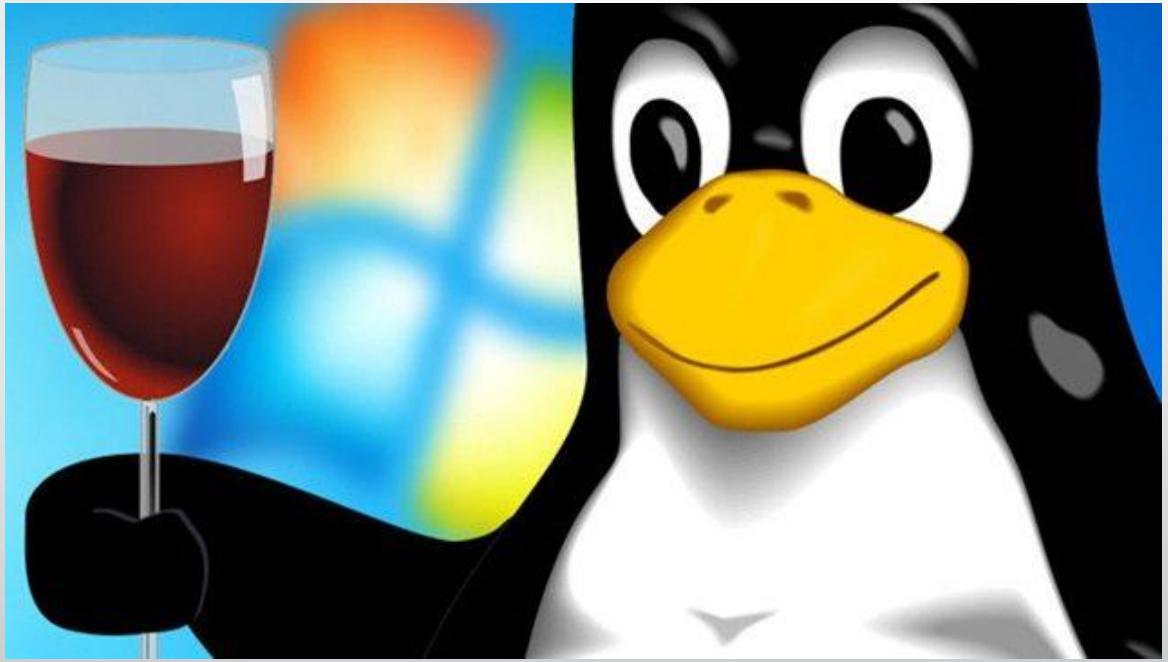


Instalación en Windows





Instalación en Linux



Instalación de wine en Ubuntu

- 1) Agregamos el soporte a la arquitectura de 64 bits.

→ sudo dpkg --add-architecture i386

- 2) Agregamos la clave de verificación.

→ wget -nc https://dl.winehq.org/wine-builds/Release.key

→ sudo apt-key add Release.key

Instalación wine

- 3) Agregamos el repositorio.

→ Ubuntu: sudo apt-add-repository https://dl.winehq.org/wine-builds/ubuntu/

- 4) Actualizamos

→ sudo apt update

Instalación wine

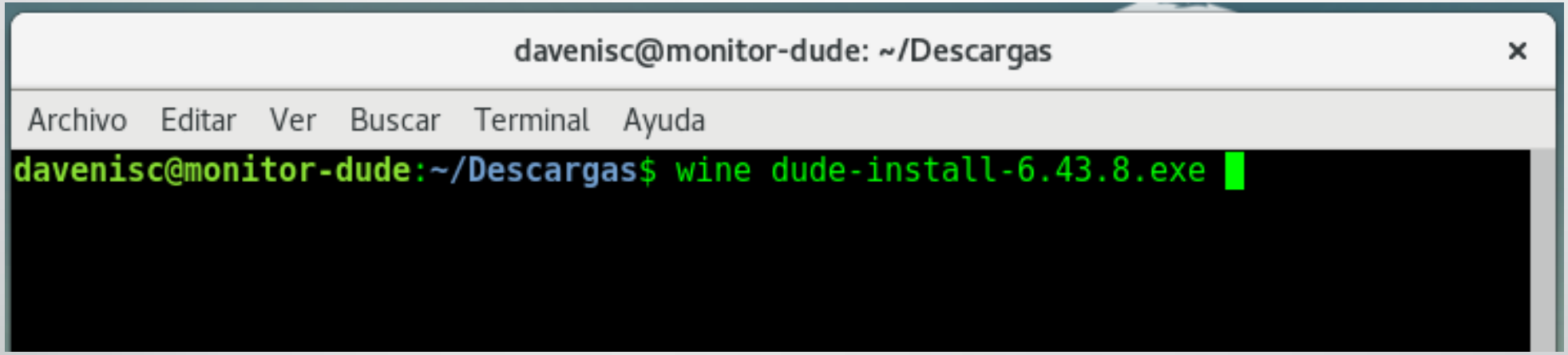
- 5) Instalamos la versión estable:

→ sudo apt install --install-recommends winehq-stable

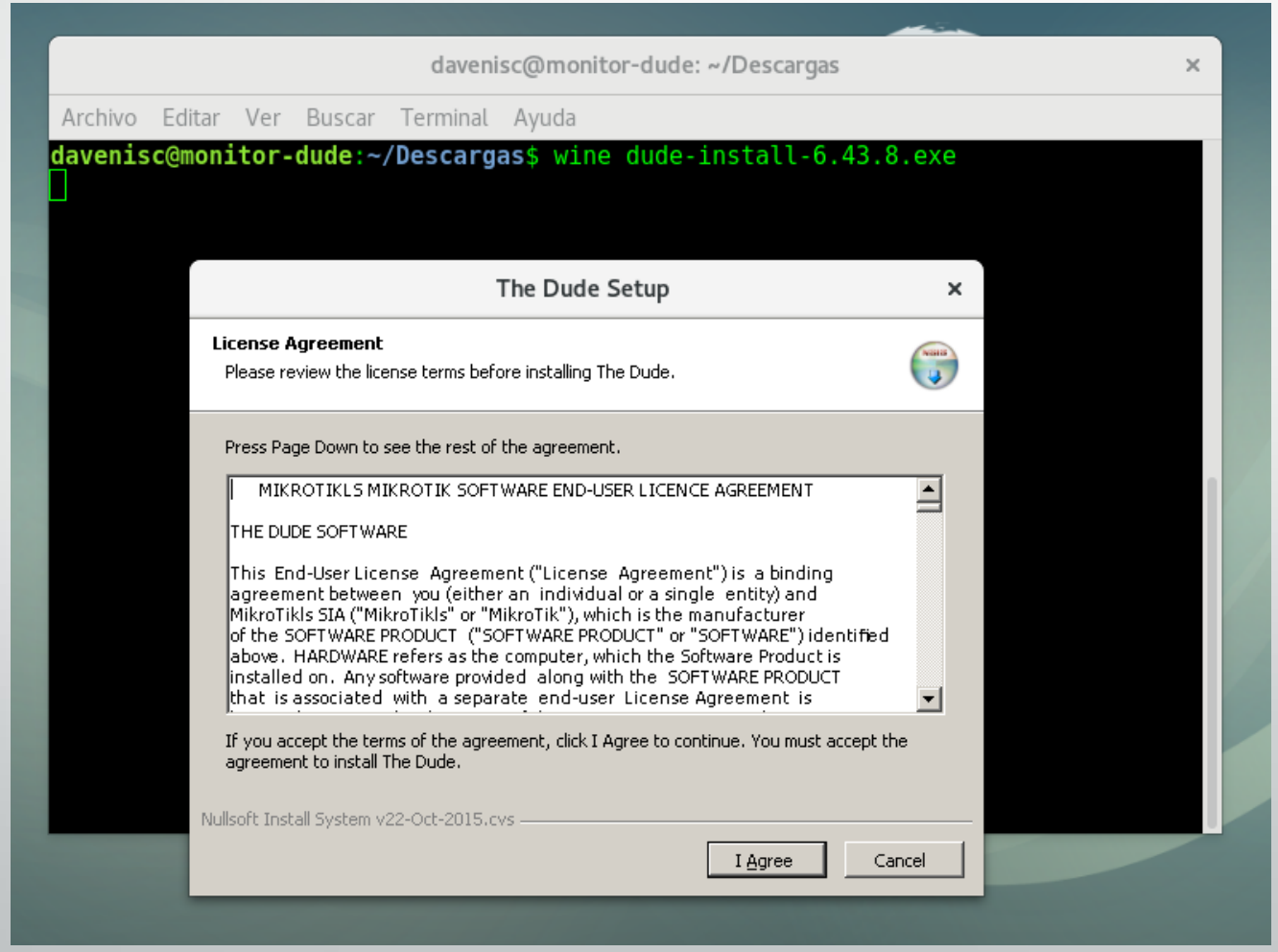
- 6) Corregimos errores de instalación

→ sudo apt-get install -f

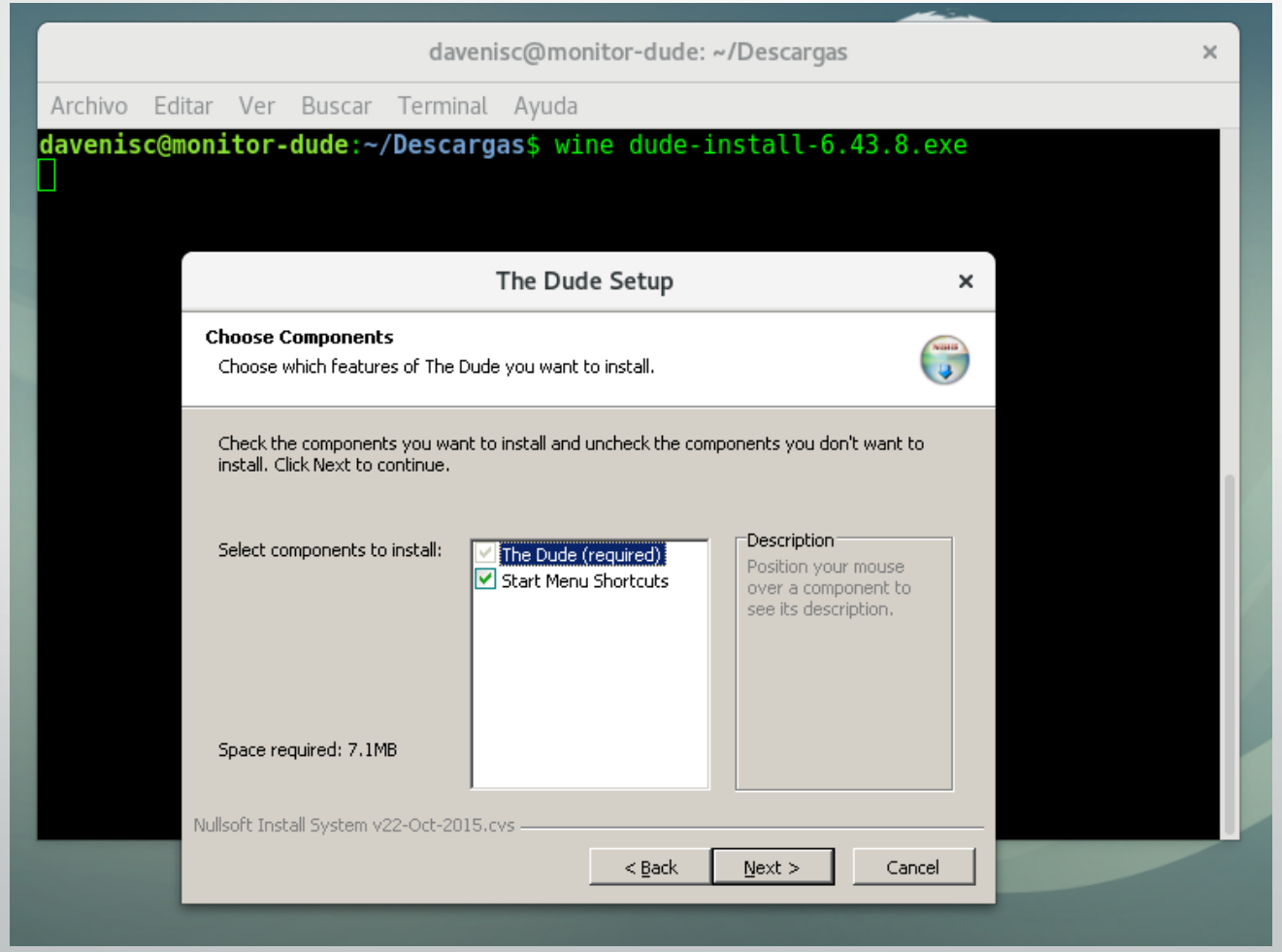
Instalación dude con wine



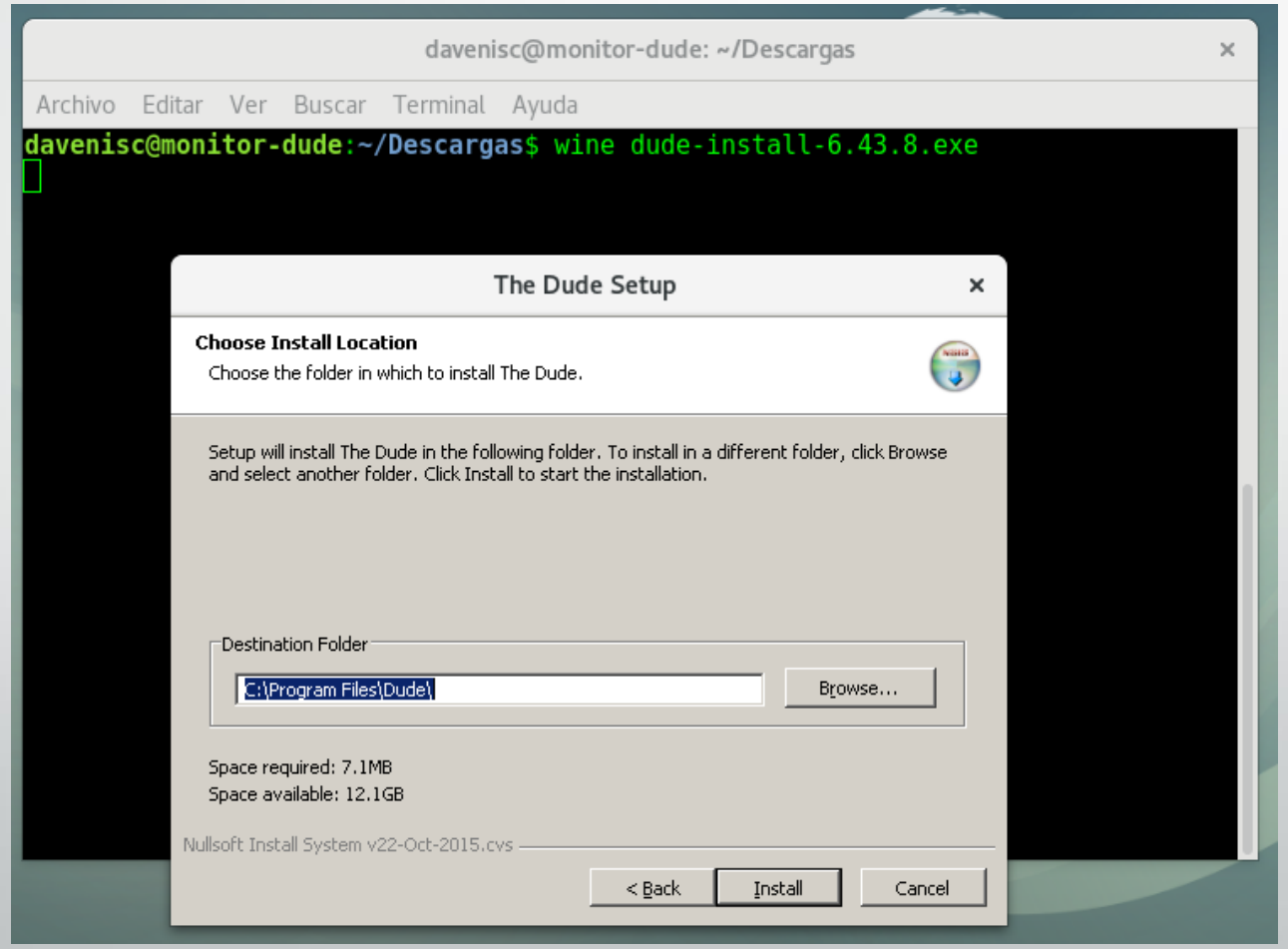
Instalación dude con wine



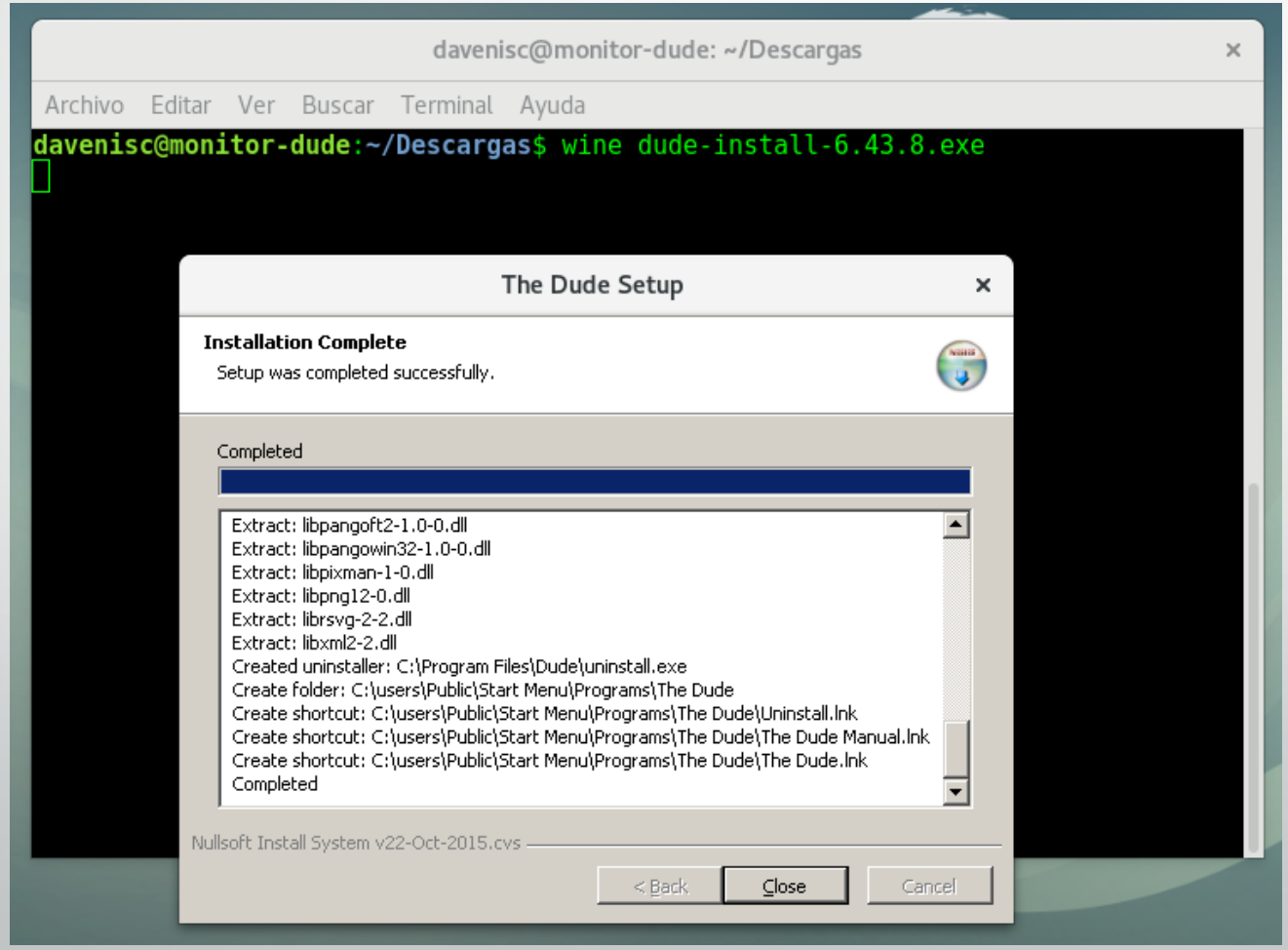
Instalación dude con wine



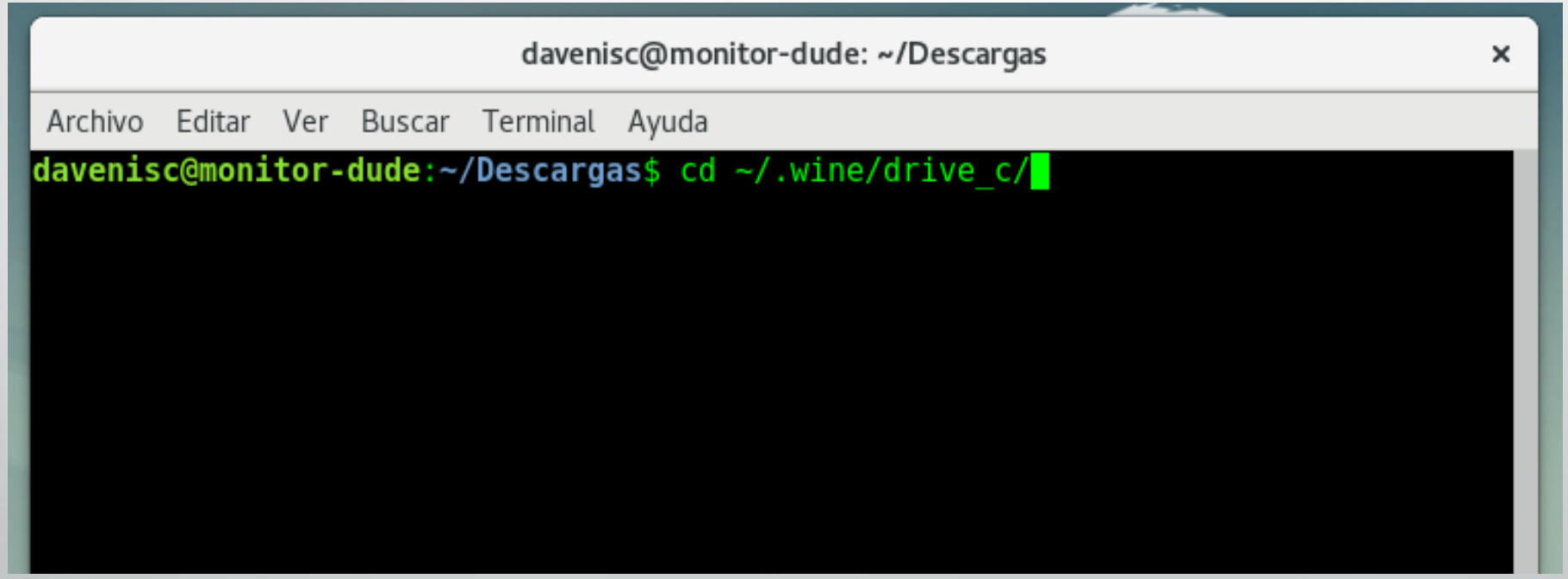
Instalación dude con wine



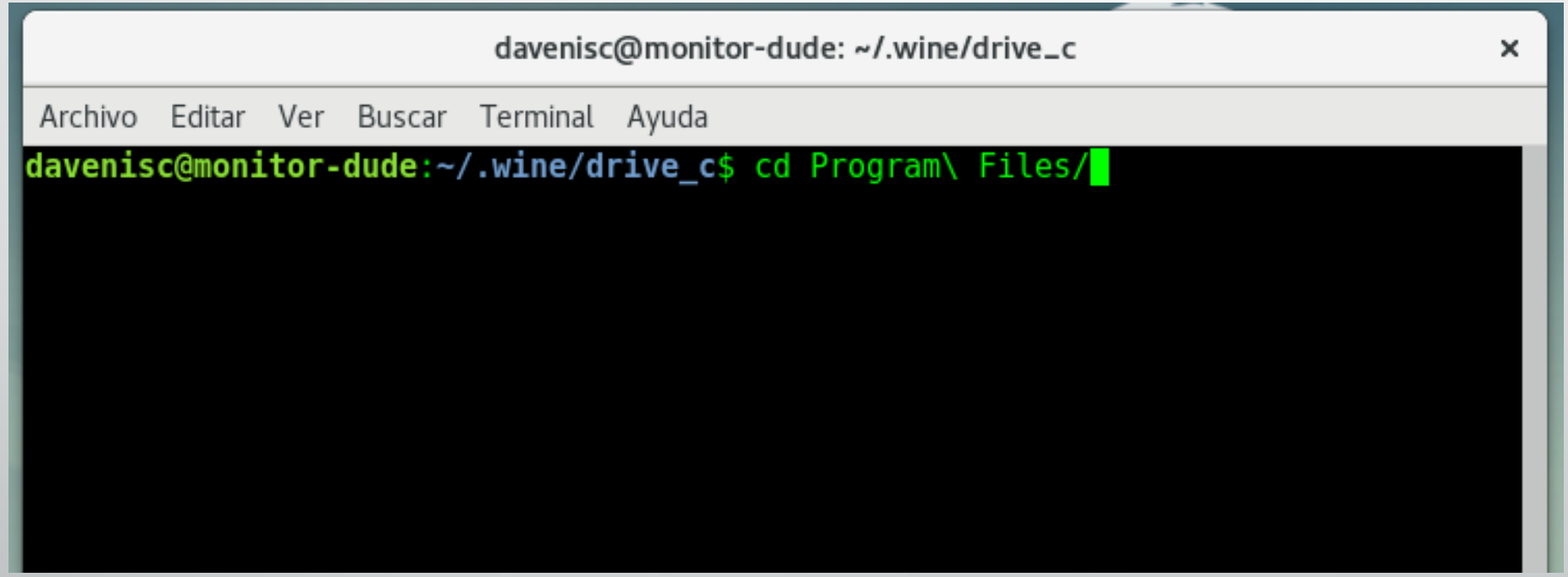
Instalación dude con wine



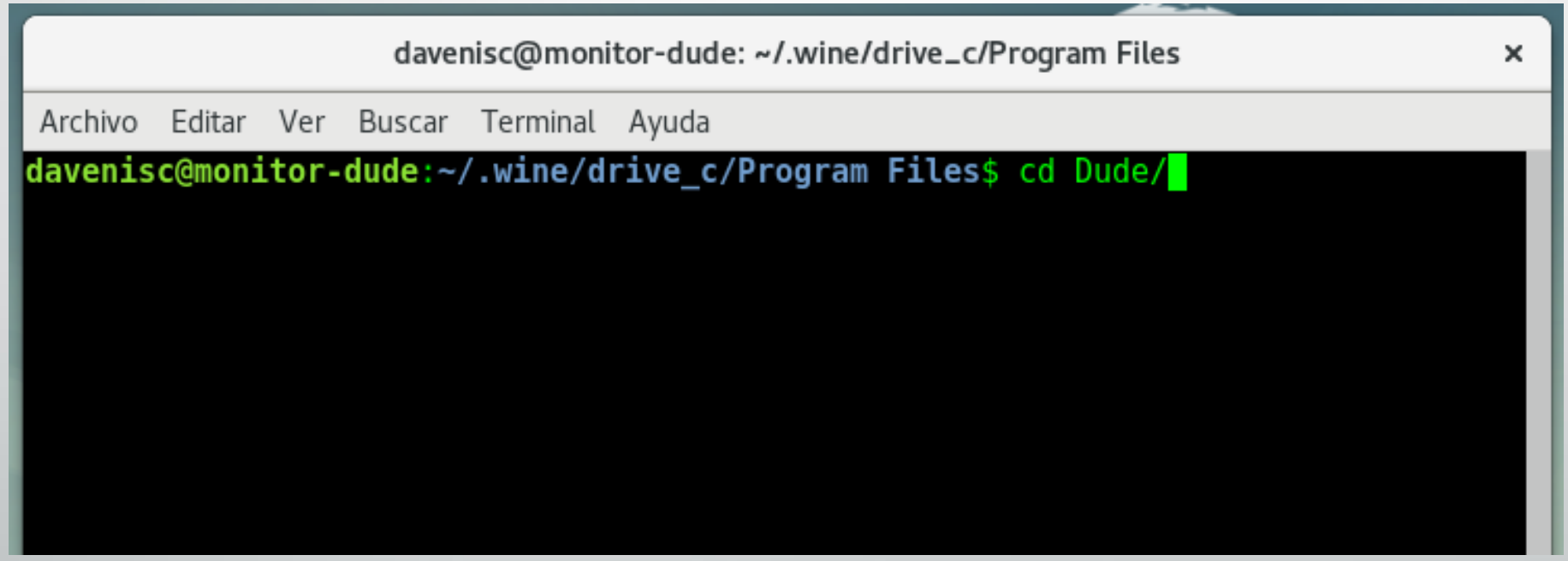
Entrar a la carpeta wine



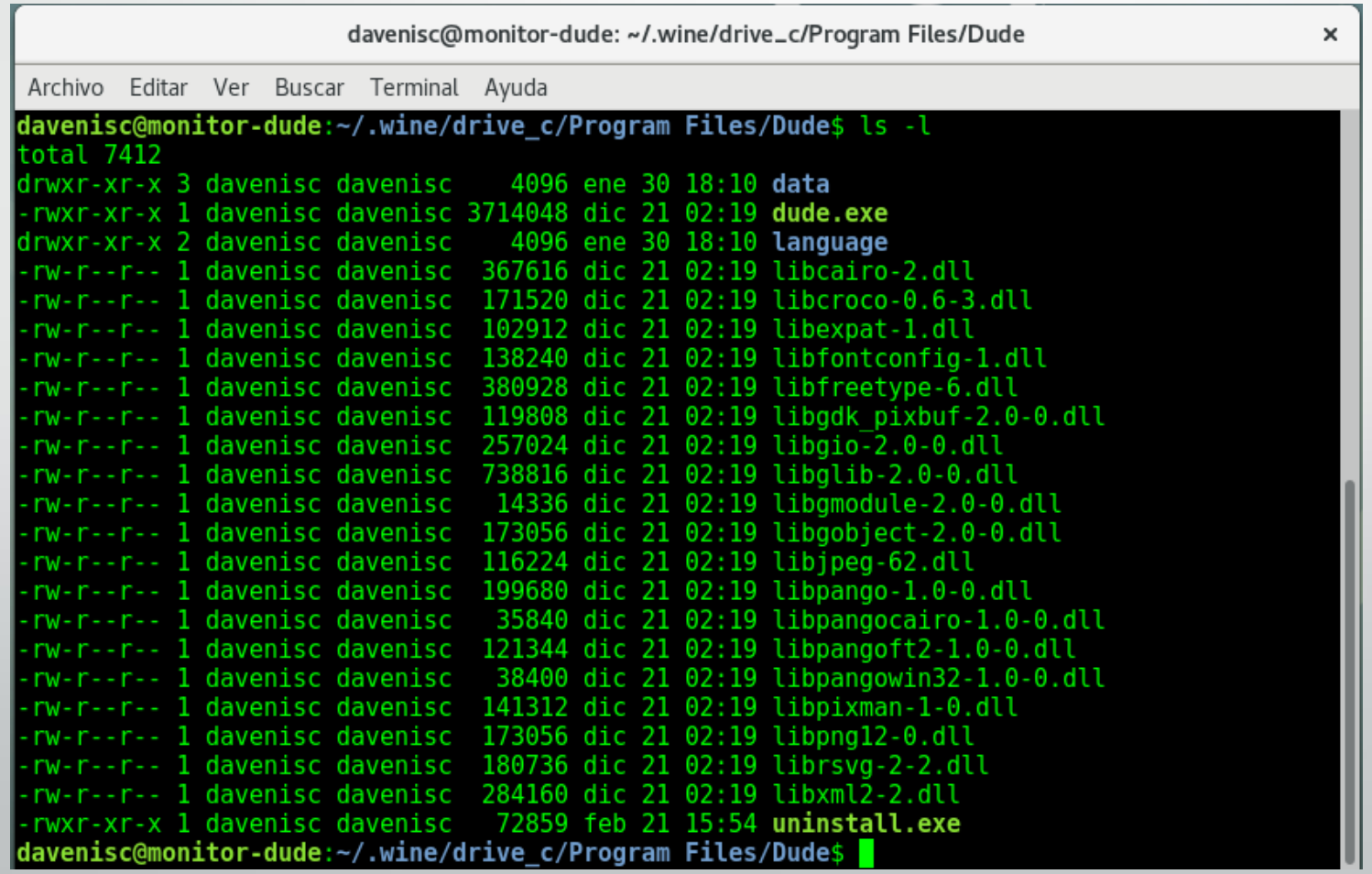
Entrar a Program\ Files/



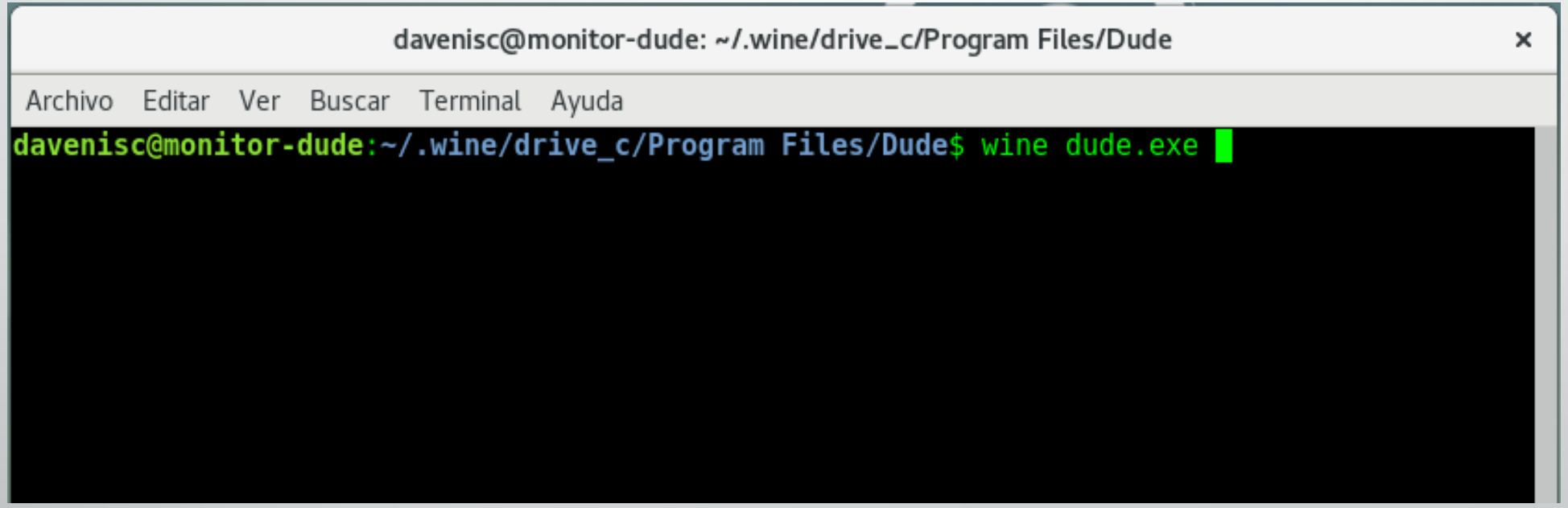
Entrar a la carpeta Dude/



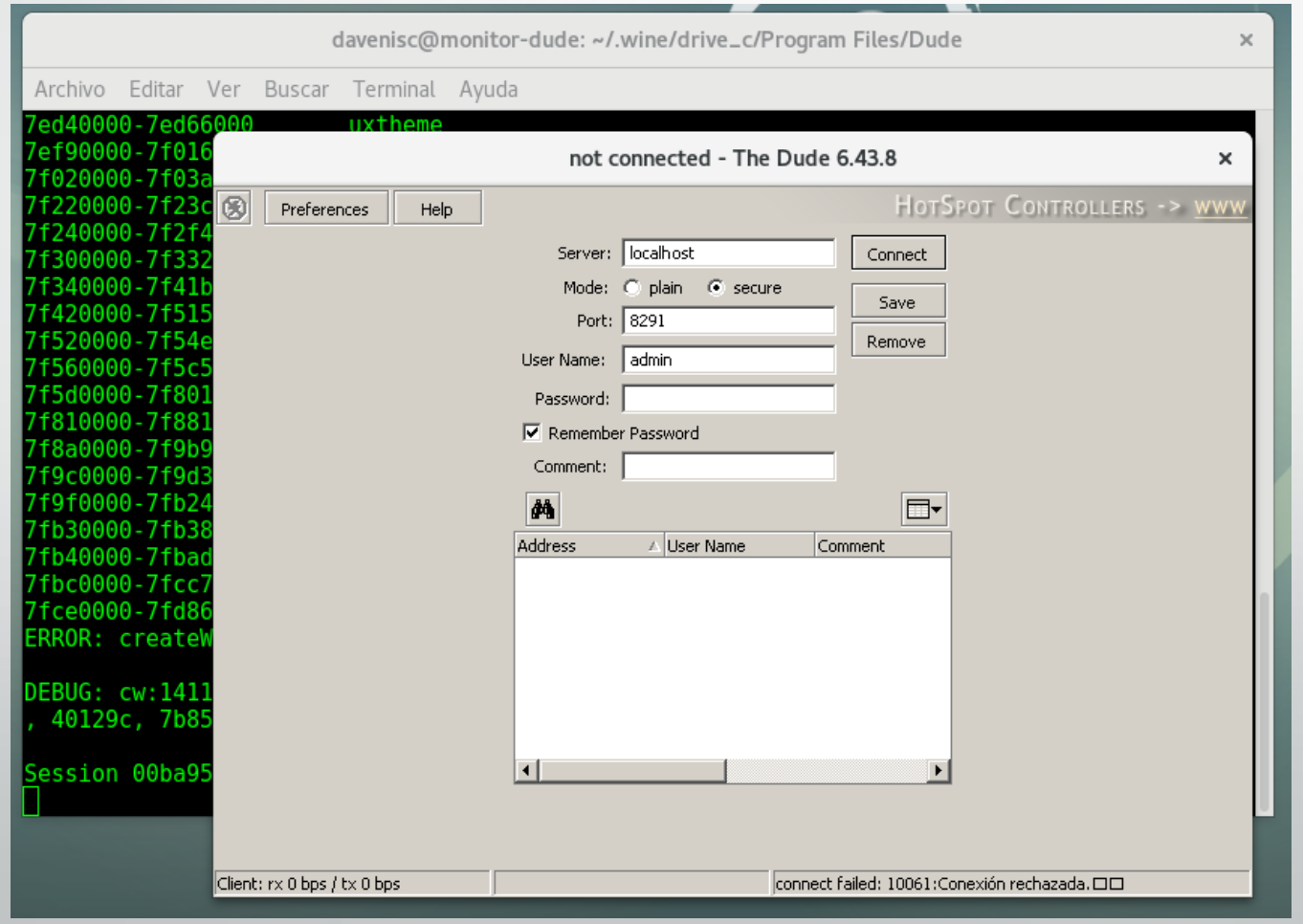
Listar archivos ls -l



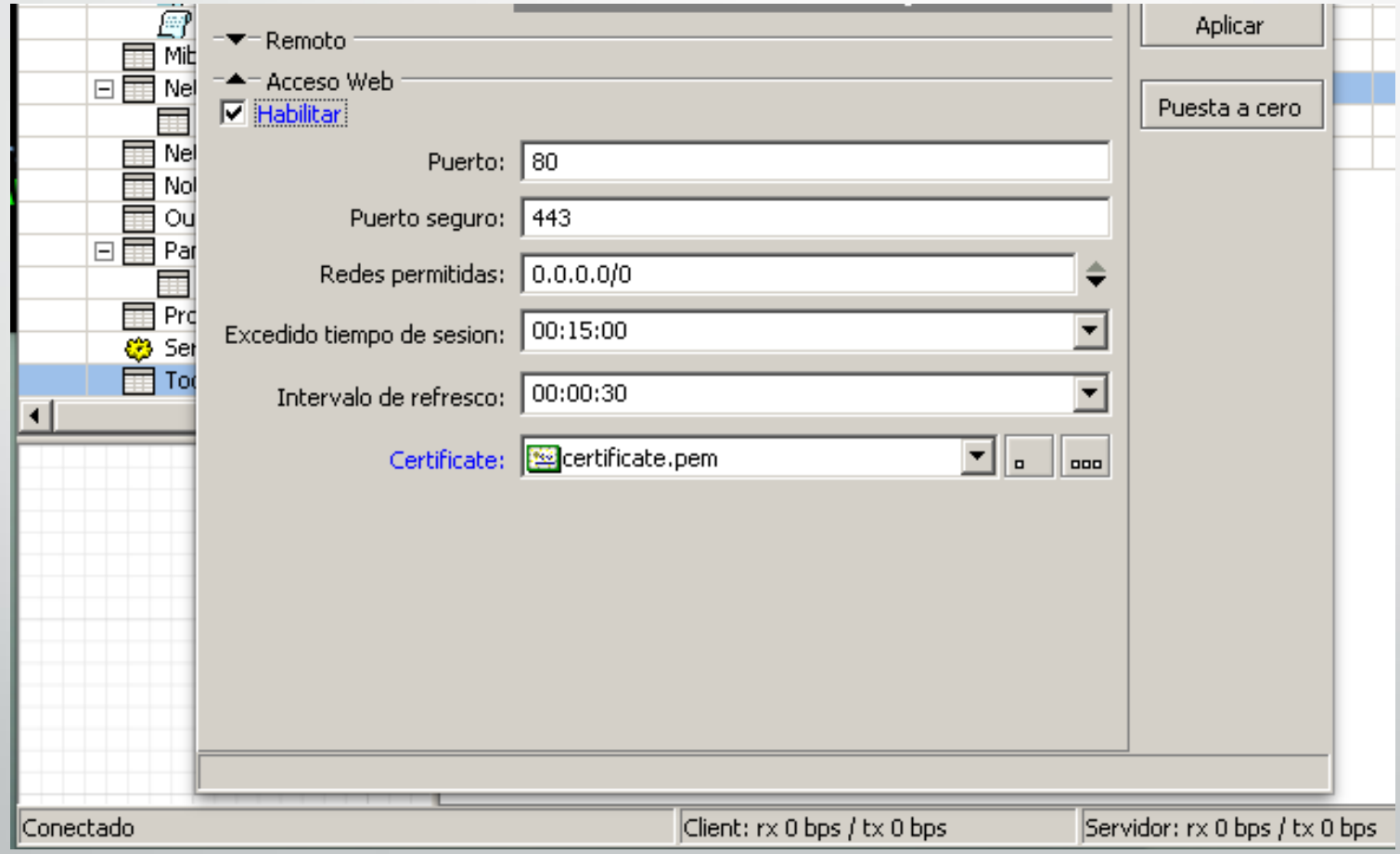
Ejecutar dude con wine



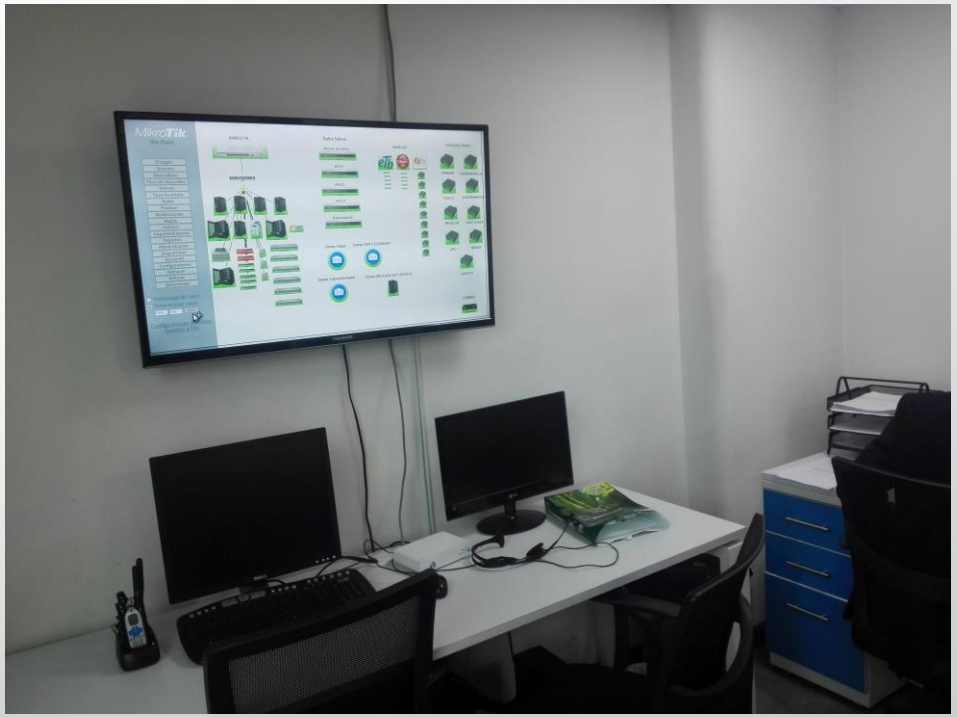
The dude con wine



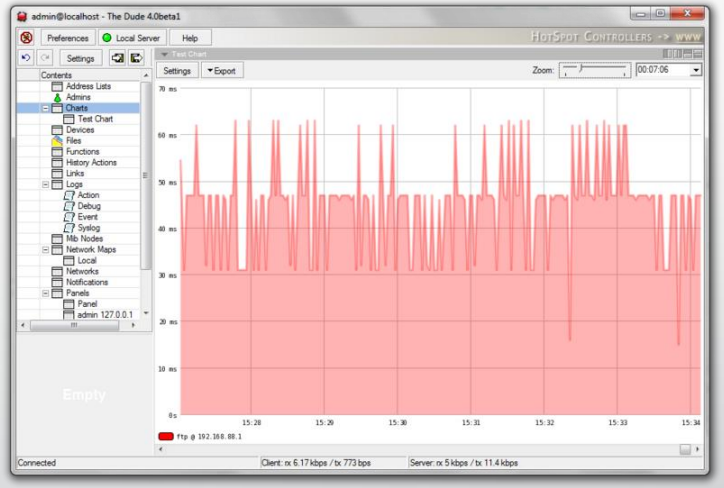
Interfaz web

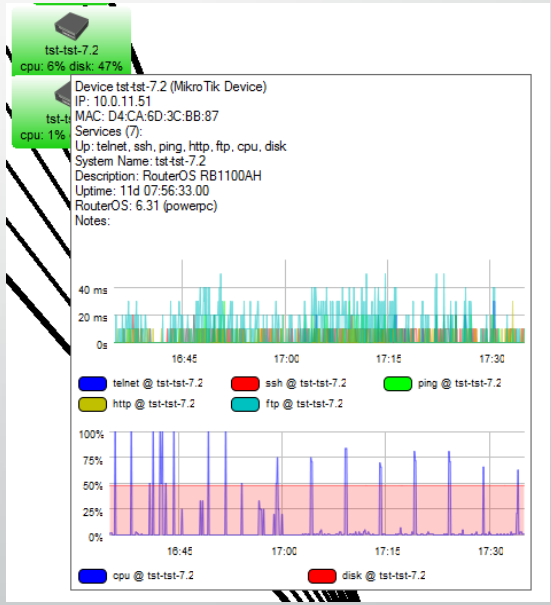


Interfaz web



Monitoreo en tiempo real



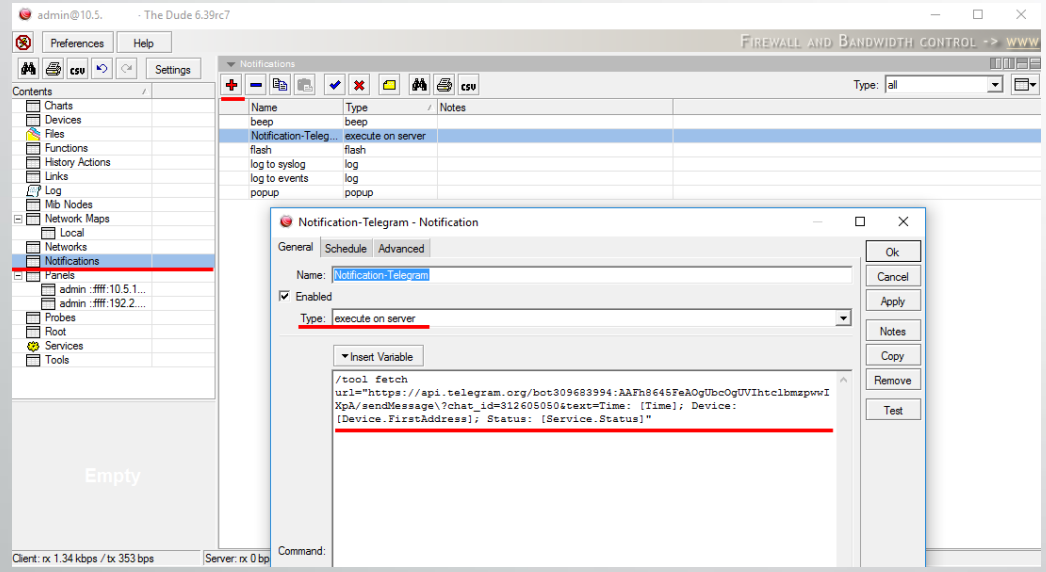


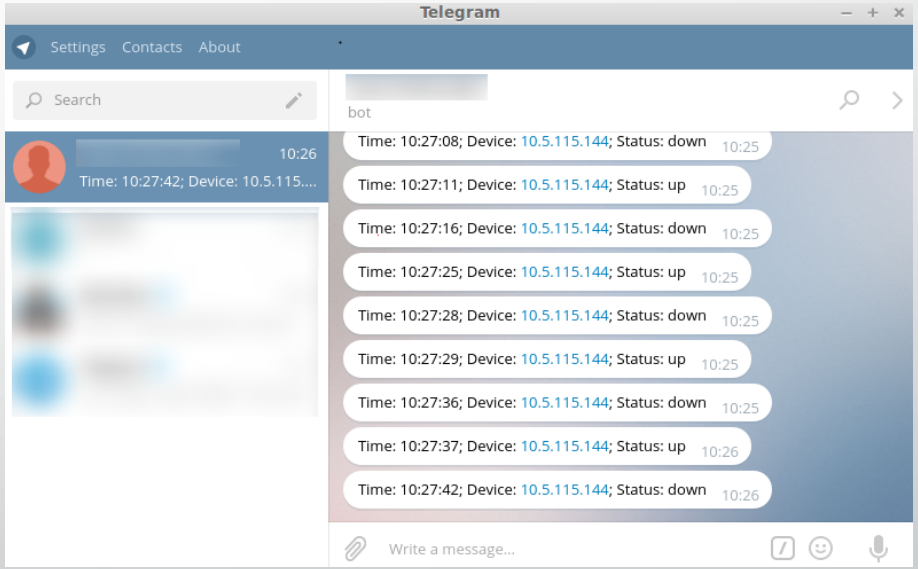
Sistema de alertas

Alertas
Correo electrónico

Alertas
Telegram

Notificaciones con Telegram





https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Dude_Telegram_Example

Notificaciones con Telegram

APIs de telegramas

Ofrecemos dos tipos de API para desarrolladores. El Bot API le permite crear fácilmente programas que usan mensajes de Telegram para una interfaz. La API de Telegram y TDLib le permiten crear sus propios clientes de Telegram personalizados. Le invitamos a utilizar ambas API de forma gratuita.

También puede agregar Telegram Widgets a su sitio web.

API API

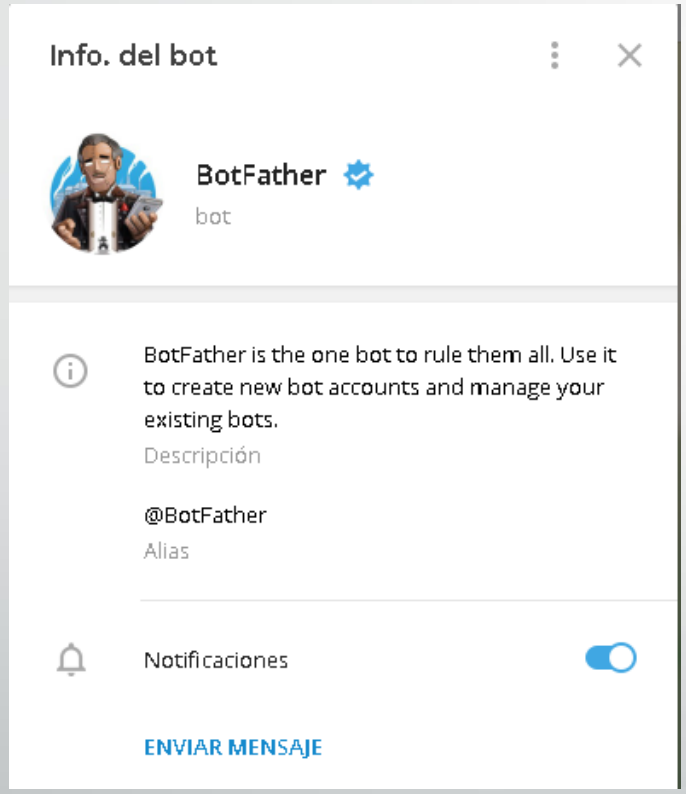
Esta API le permite conectar bots a nuestro sistema. **Los Telegram Bots** son cuentas especiales que no requieren un número de teléfono adicional para configurar. Estas cuentas sirven como una interfaz para el código que se ejecuta en algún lugar de su servidor.

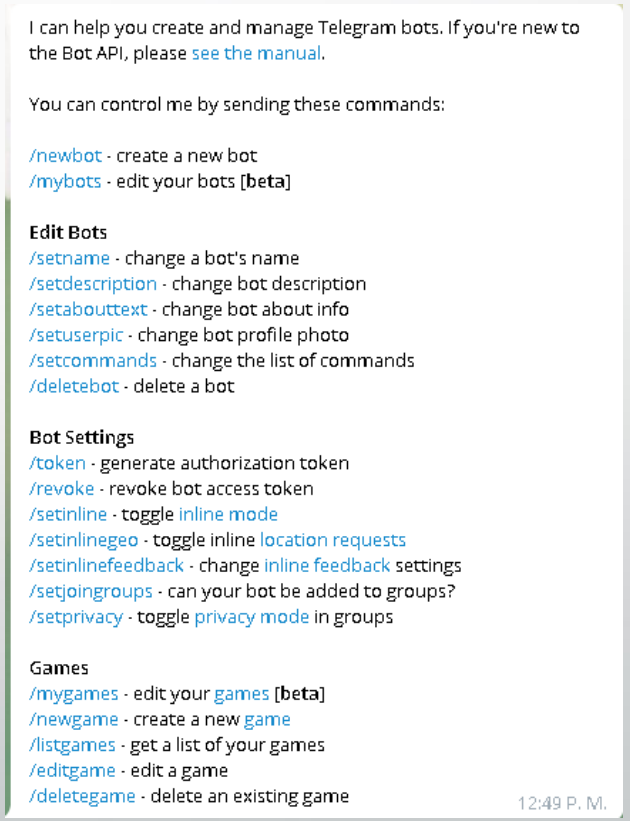
Para usar esto, no necesita saber nada sobre cómo funciona nuestro protocolo de cifrado MTProto; nuestro servidor intermediario se encargará de todo el cifrado y la comunicación con la API de Telegram. Se comunica con este servidor a través de una interfaz simple HTTPS que ofrece una versión simplificada de la API de Telegram.

> **Obtenga más información sobre la API de Bot aquí »**

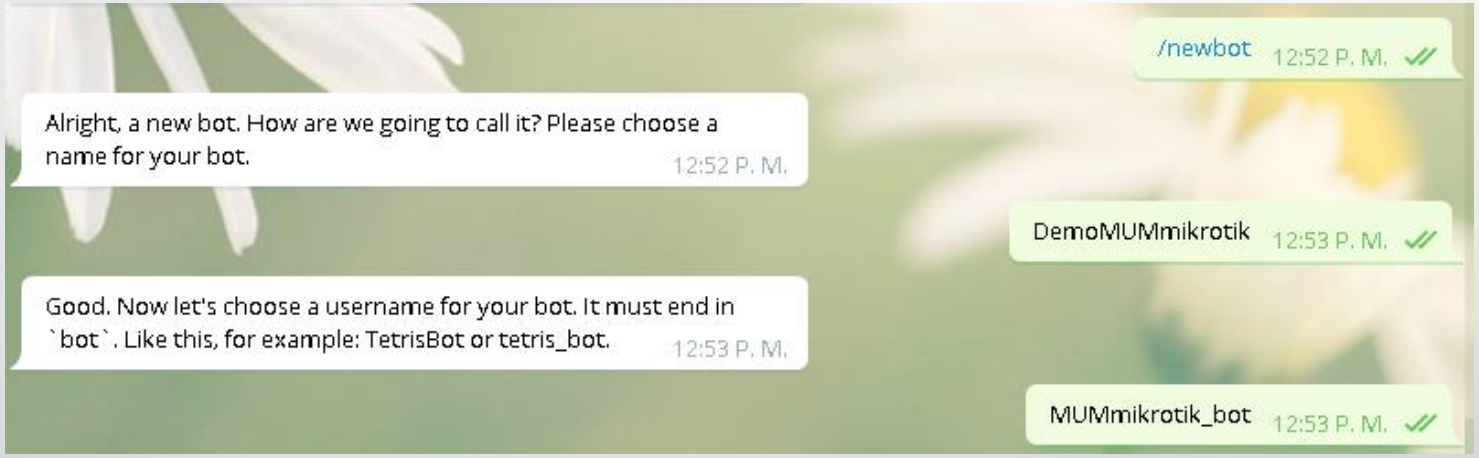
Los desarrolladores de bot también pueden utilizar nuestra **API de pagos** para aceptar **pagos** de usuarios de Telegram en todo el mundo.

Crear Bot con Telegram

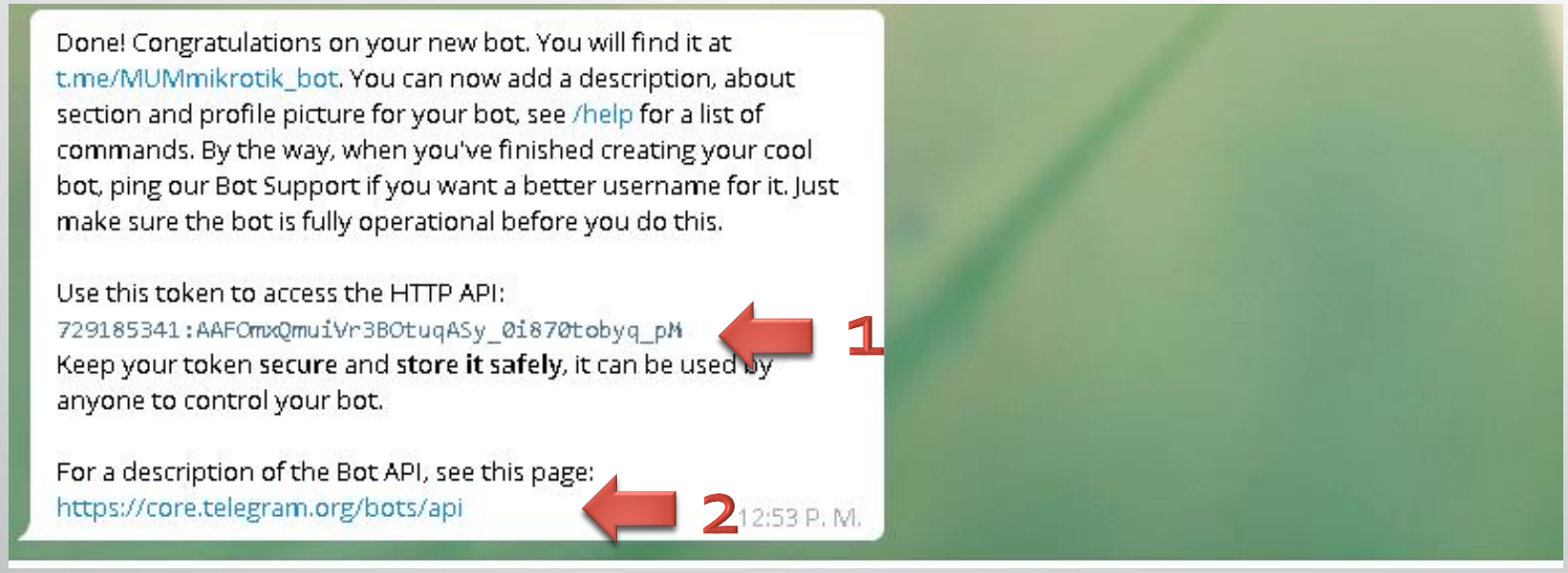




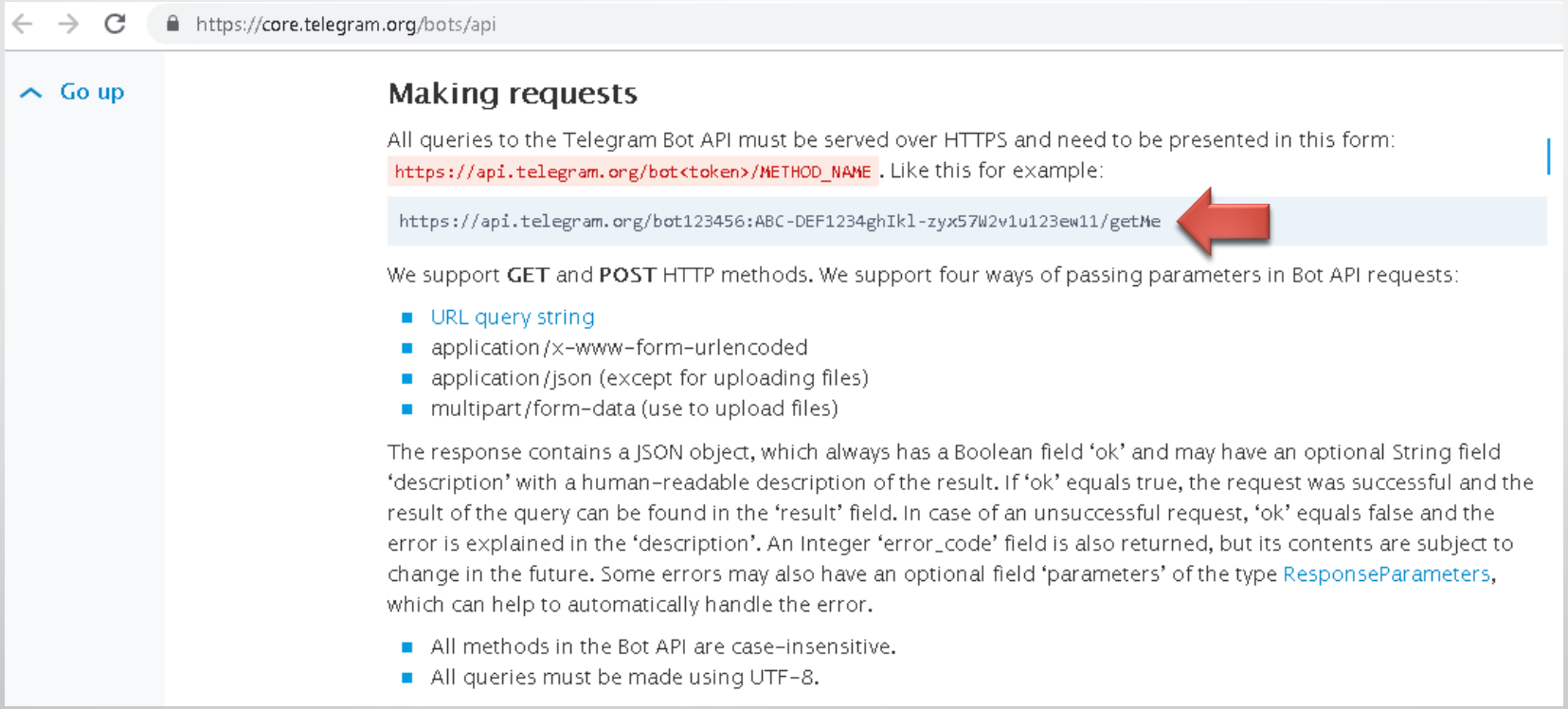
Crear Bot con Telegram



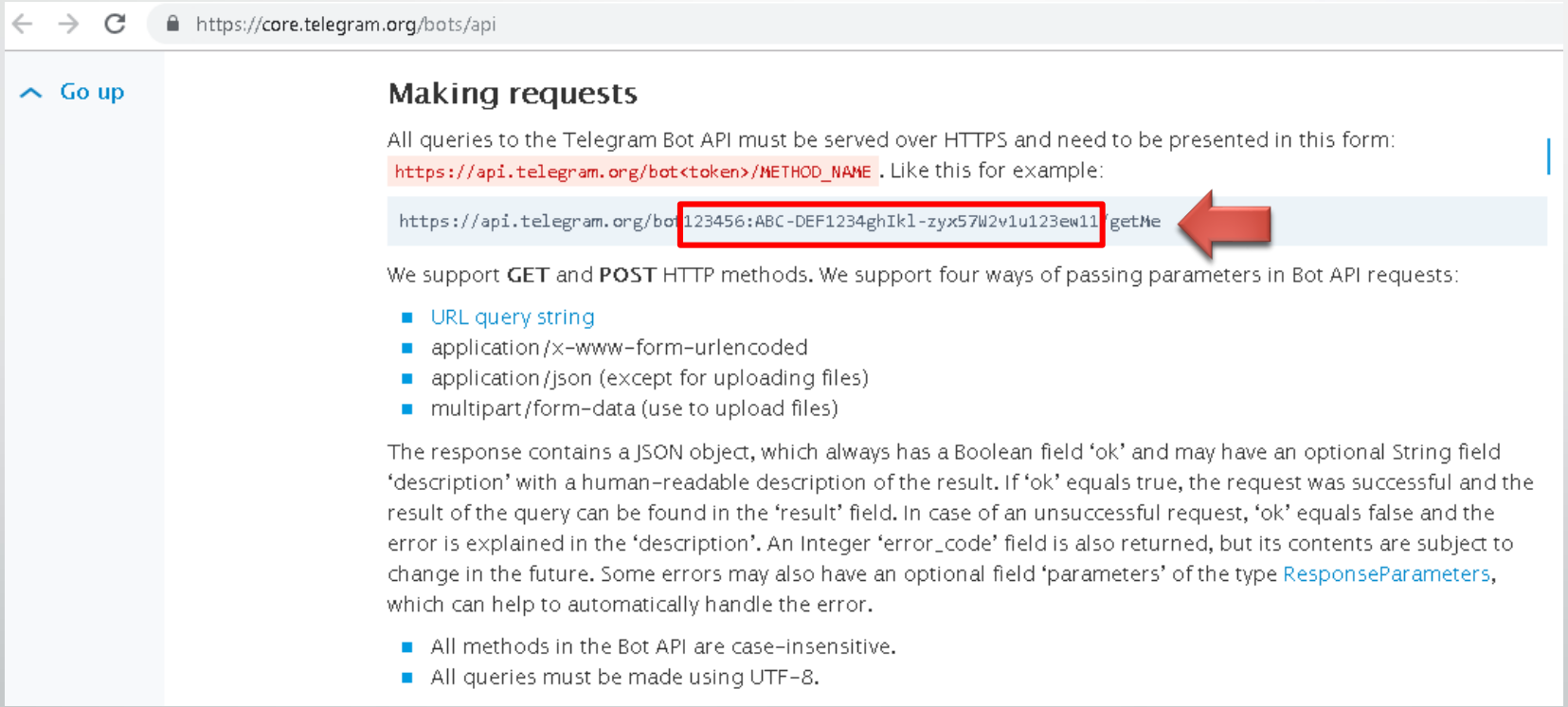
Token


Done! Congratulations on your new bot. You will find it at t.me/MUMmikrotik_bot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.
Use this token to access the HTTP API:
729185341:AAFOmxQmuiVr3BOtuqASy_0i870tobyq_pM
1
Keep your token secure and store it safely, it can be used by anyone to control your bot.
For a description of the Bot API, see this page:
https://core.telegram.org/bots/api
2
12:53 P. M.

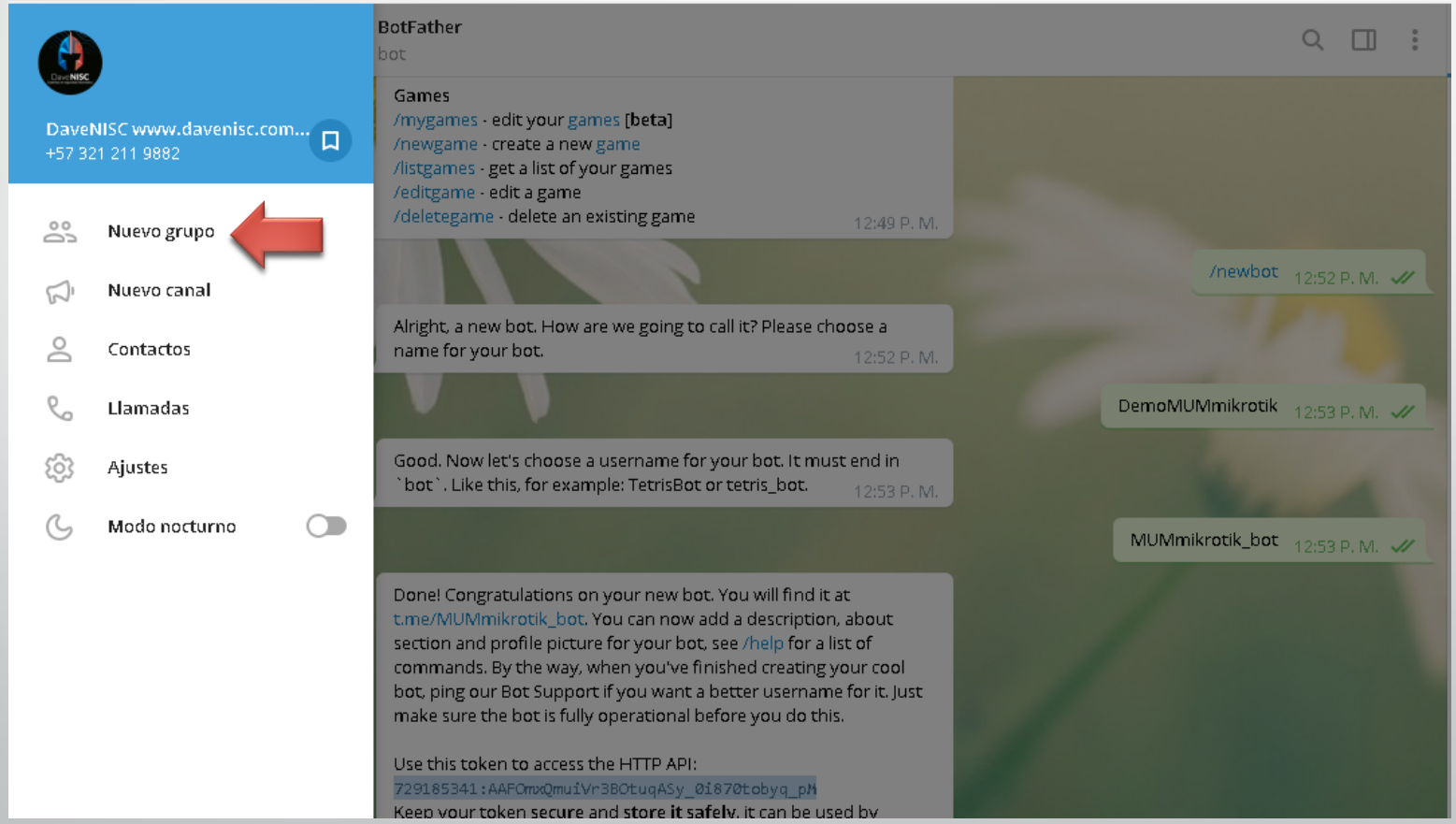
URL para obtener el ID de grupo



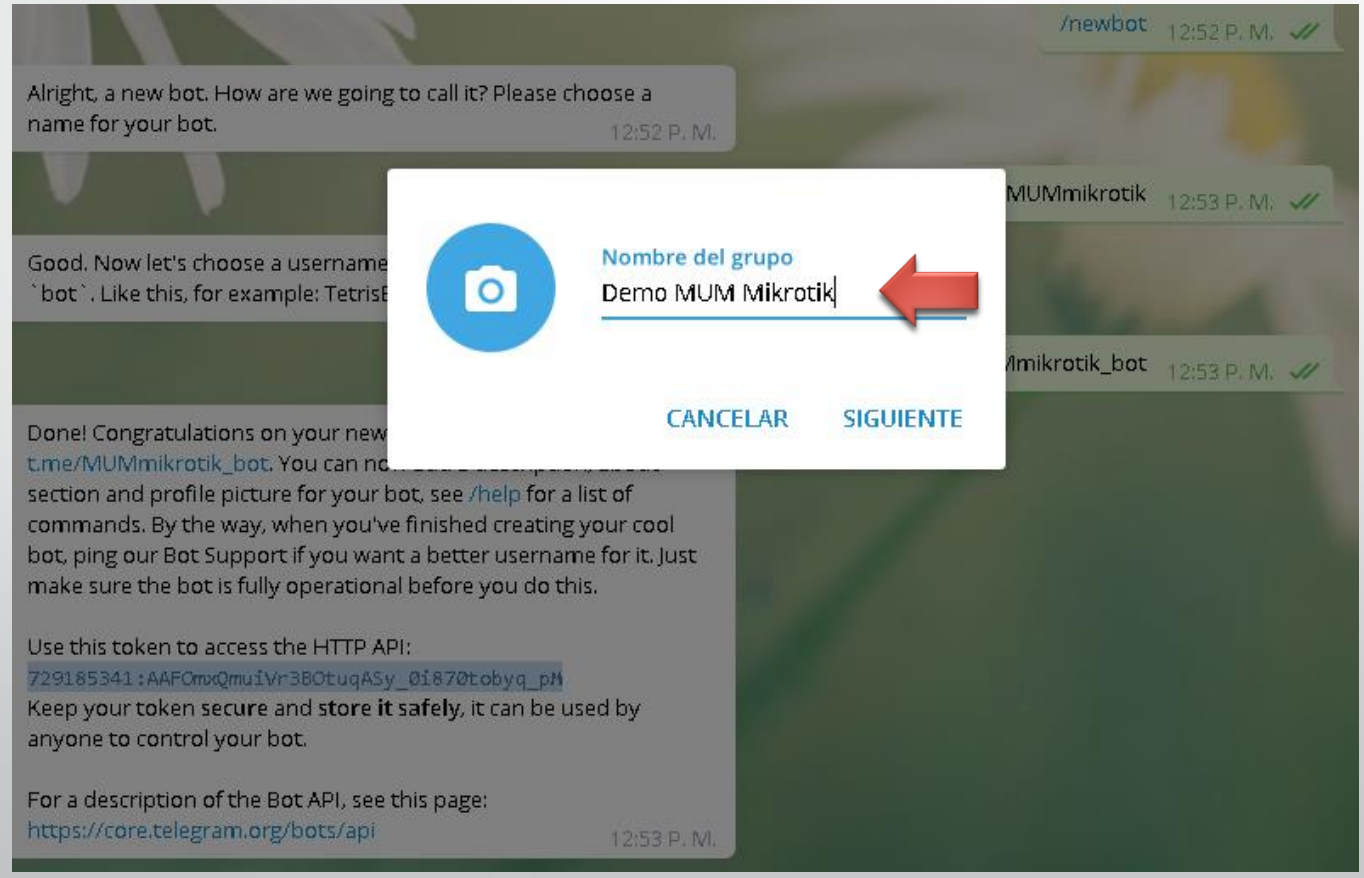
Crear Bot con Telegram



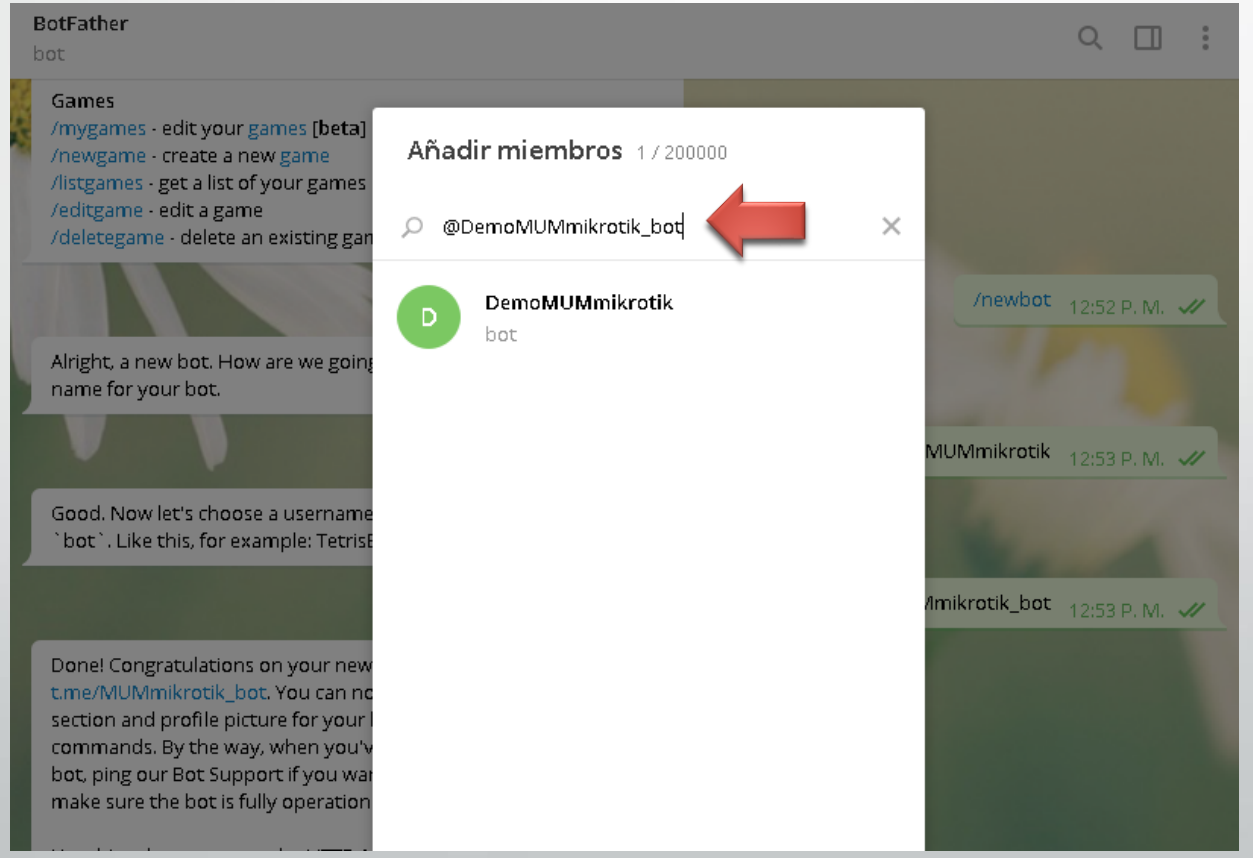
Crear un grupo en Telegram



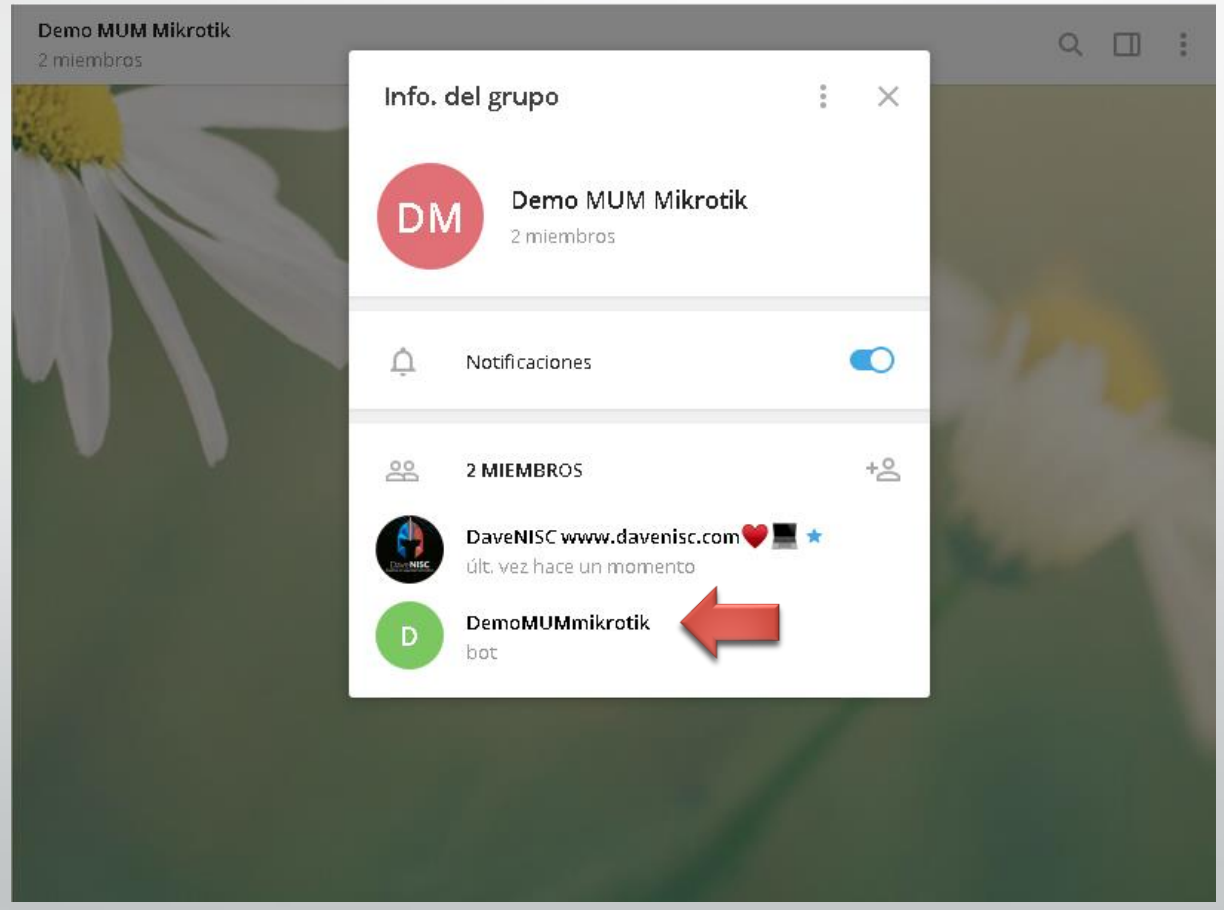
Nombre de grupo



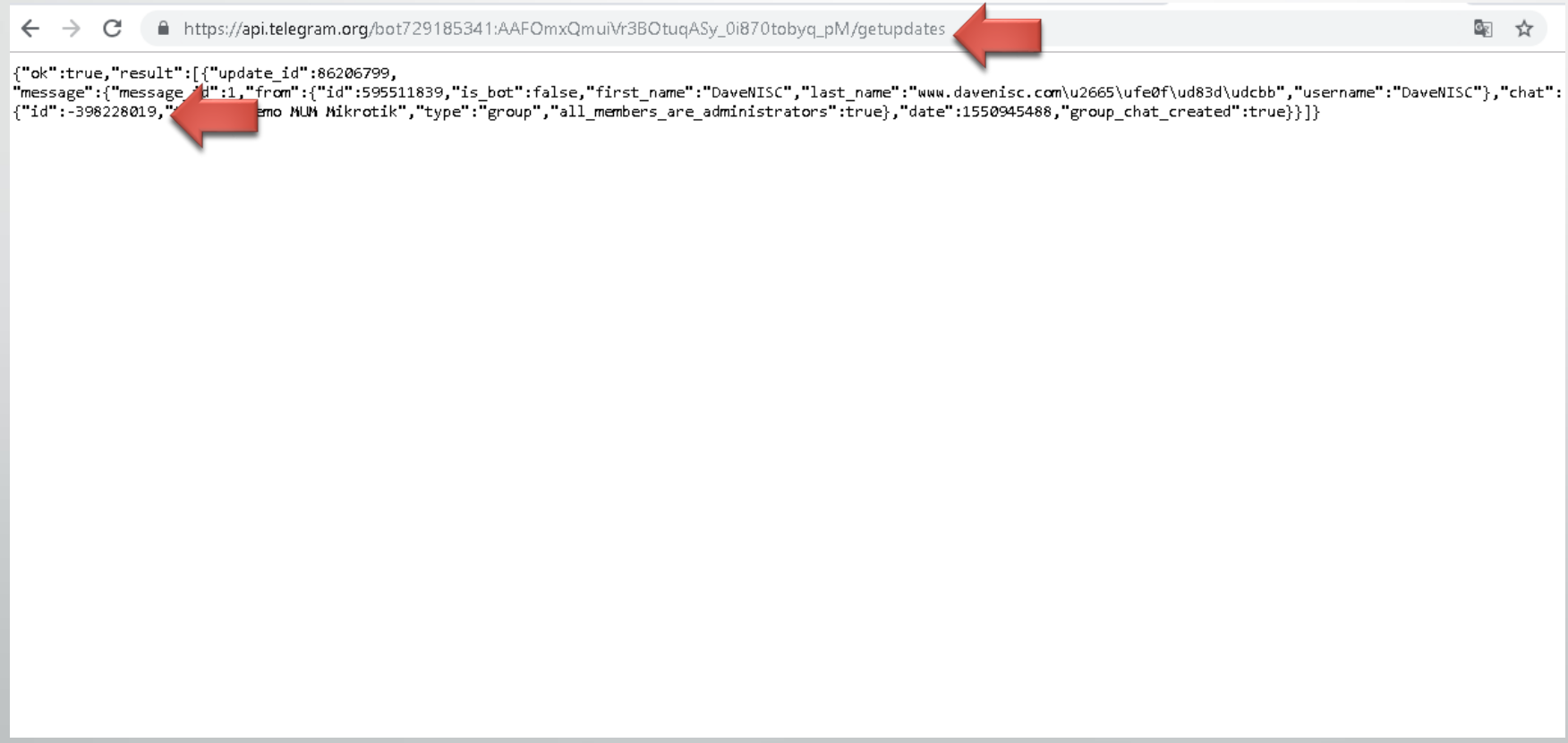
Unir Bot a grupo



Bot en el grupo



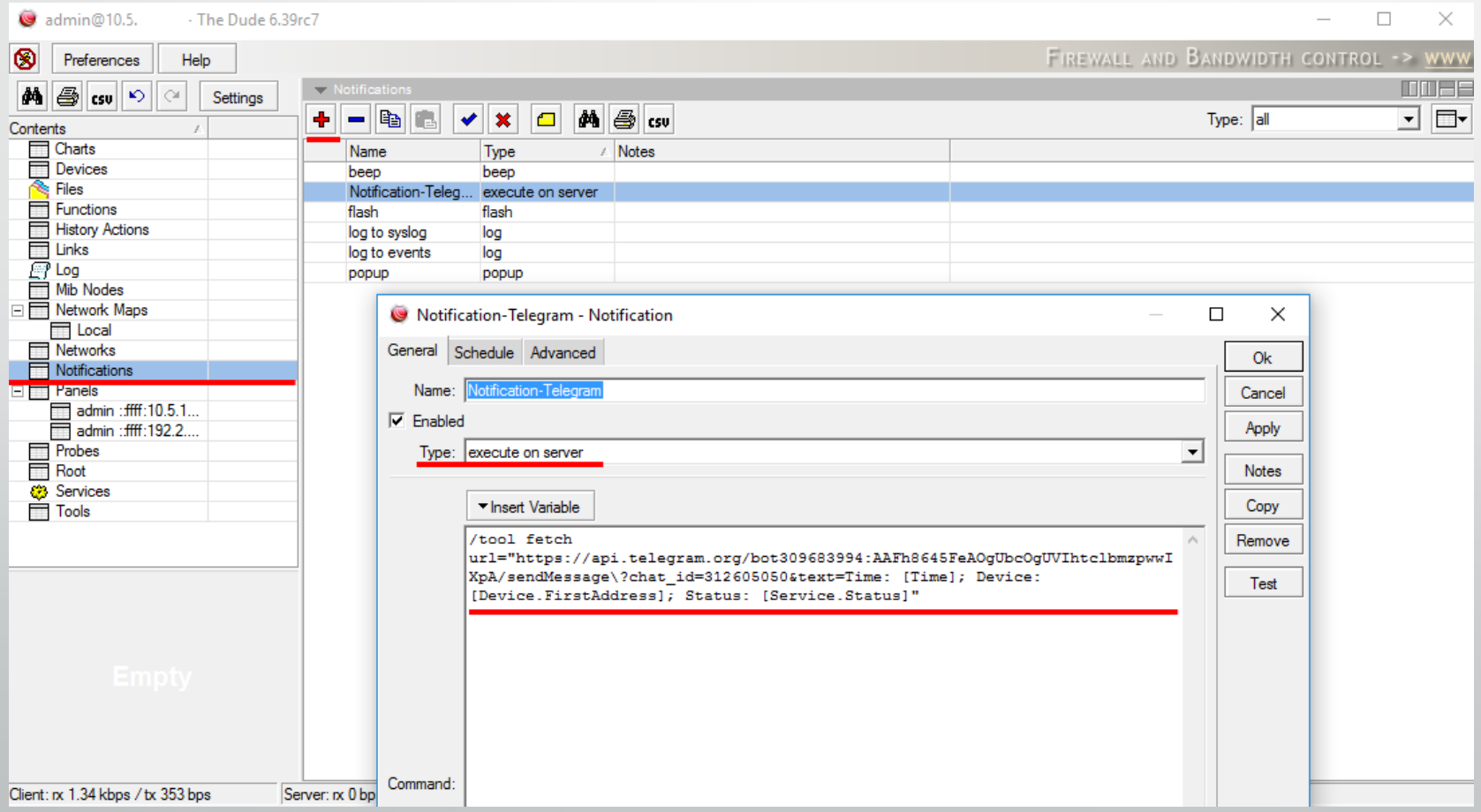
Crear Bot con Telegram



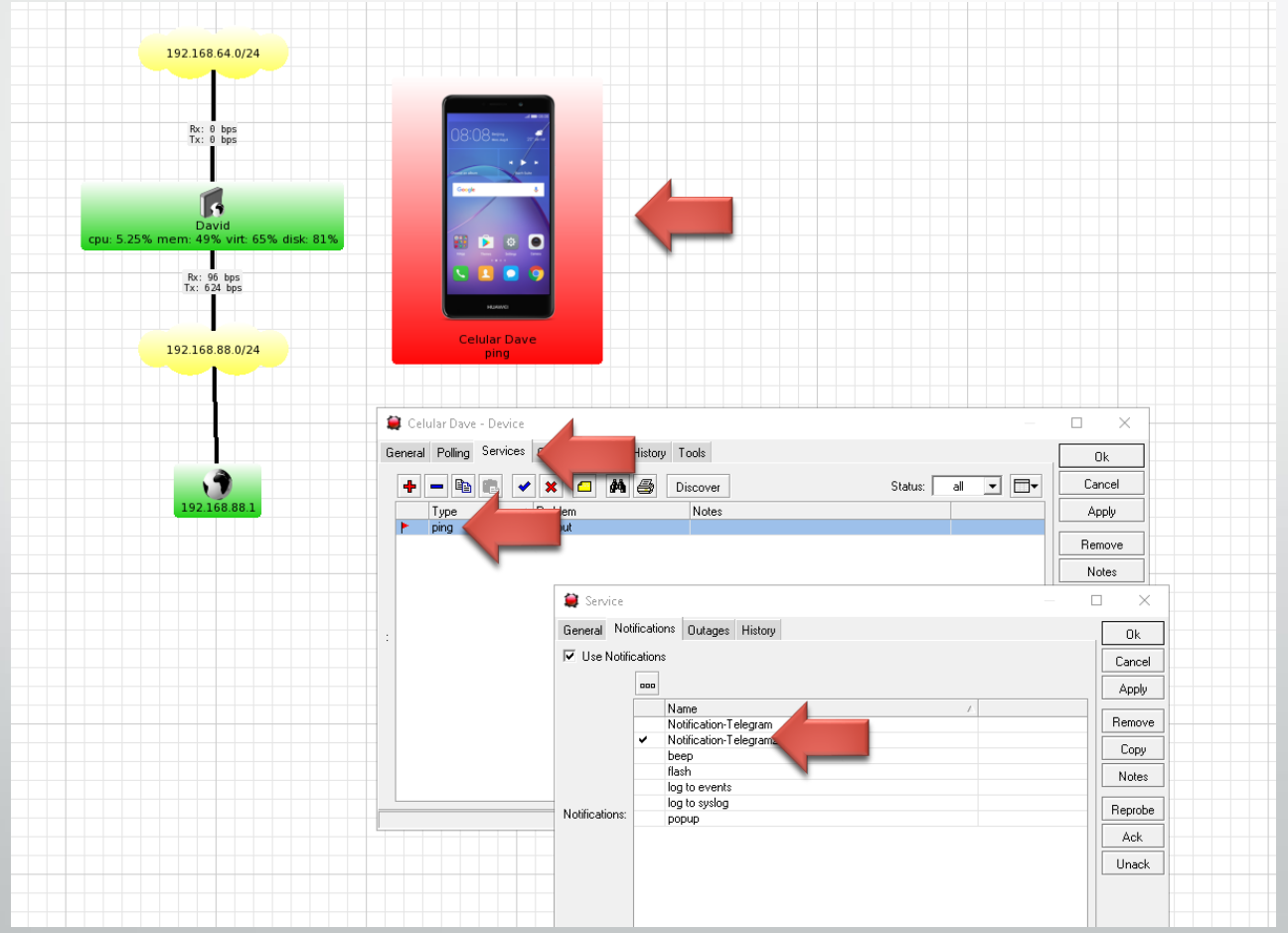
Crear Bot con Telegram

- 1. Token: 729185341:AAFOmxQmuiVr3BOtuqASy_oi870tobyq_pM
- 2. ID de grupo: -398228019
- 3."https://api.telegram.org/bot729185341:AAFOmxQmuiVr3BOtuqASy_oi870tobyq_pM/sendMessage?chat_id=-398228019&text=Time: [Time]; Device: [Device.FirstAddress]; Status: [Service.Status]"

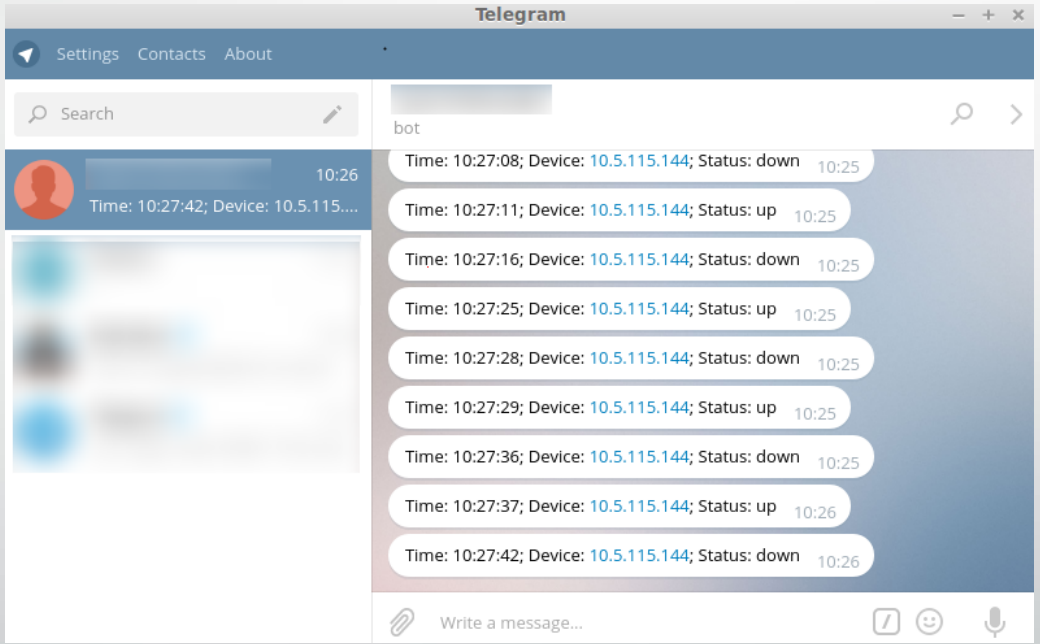
Notificaciones con Telegram



Aplicar notificación a cada host



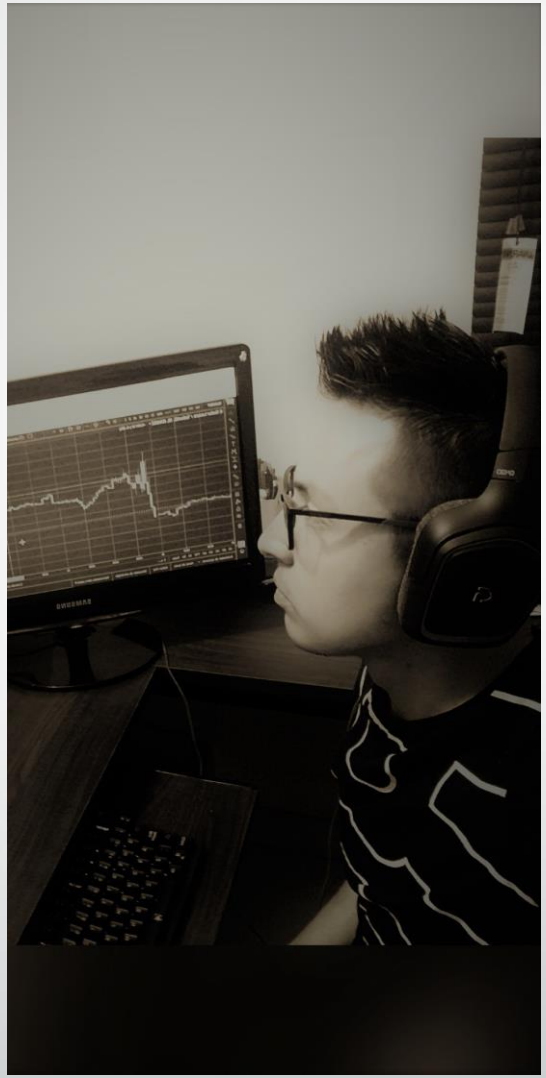
Notificaciones con Telegram



Referencias

* https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Dude_Telegram_Example
* https://core.telegram.org/api
* https://core.telegram.org/bots/api
* https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6
* https://mikrotik.com/download
* https://mikrotik.com/thedude
* https://mikrotik.com/

Gracias!



DaveNISC

Expertos en seguridad informática

@DaveNISC

- www.davenisc.com
- info@davenisc.com