Principios Básicos de Lockpicking

low[noise]
col hack. research

F4Lc0N – LNHG

falcon@lownoisehg.org

Twitter: @falcon_lownoise

http://www.lownoisehg.org/

Campus Party 2011 – BarCamp
Bogotá, D. C. – Colombia

Junio 2011

¿ Qué es LowNoise HG ?

- Grupo de Investigación (Hacking only)
- Creado en 1995
- Multidisciplinario (No sólo Ingenieros)
- Objetivo Común:

  Seguridad vs. Inseguridad
- Sin Ánimo de Lucro
- Recursos Propios
- Sin Afiliación a Empresas/Entidades

¿ Qué es LowNoise HG ?

Investigaciones actuales en:

- **RFID**
- **GSM / GPRS**
- **SIM cards / SmartCards**
- **Telefonía Fija (SS7)**
- **Muchas otras …**

Más información en:

- **http://www.lownoisehg.org/**

¿ Quién es F4Lc0N ?

- Investigador Líder de LowNoise HG
- Hacker 7 x 24 x 365 … x 16 (y contando …)
- Speaker desde 2004 …
- Afinidades básicas:
  - Linux (otros OSs)
  - uCs y uPs, FPGAs, comunicaciones
  - Ciframiento (3DES, Rijndael, etc.)
  - Bandas magnéticas, IR, BT, telefonía fija, TDMA, CDMA, GSM, lockpicking, etc.

DISCLAIMER

- Todo lo que se hable y se muestre en esta charla es el resultado de investigaciones con fines educativos.
- Todo descubrimiento realizado, ha sido y será usado de forma legal, por LNHG.
- La audiencia debe asumir todo lo se exponga hoy, como “falso” y “sin fundamento” hasta que lo compruebe personalmente.
- F4Lc0N no es el autor directo de ninguno de los descubrimientos expuestos, ni de las herramientas demostradas, ni los conoce.

YO = Alguien más

¿ Qué vamos a ver hoy ?

NIVEL DE LA CHARLA: Básico
DURACIÓN: 30 minutos

- Qué es Lockpicking ?
- Qué NO es Lockpicking ?
- Funcionamiento de una Cerradura Básica
- Herramientas “Básicas” y “No Tan Básicas”
- Uso de las Herramientas Básicas
- Demos

¿ Qué es Lockpicking ?

Lock picking is the art of unlocking a lock by analyzing and manipulating the components of the lock device, without the original key. Although lock picking can be associated with criminal intent, it is an essential skill for a locksmith. Lock picking is the ideal way of opening a lock without the correct key, while not damaging the lock, allowing it to be rekeyed for later use, which is especially important with antique locks that would be impossible to replace if destructive entry methods were used. **(Fuente: Wikipedia en Inglés)**

¿ Qué es Lockpicking ?

PUNTOS CRÍTICOS DE LA DEFINICIÓN:

Crackeo de passwords !≈ Lockpicking

LP: No hay cabida para la fuerza bruta

¿ Qué es Lockpicking ?

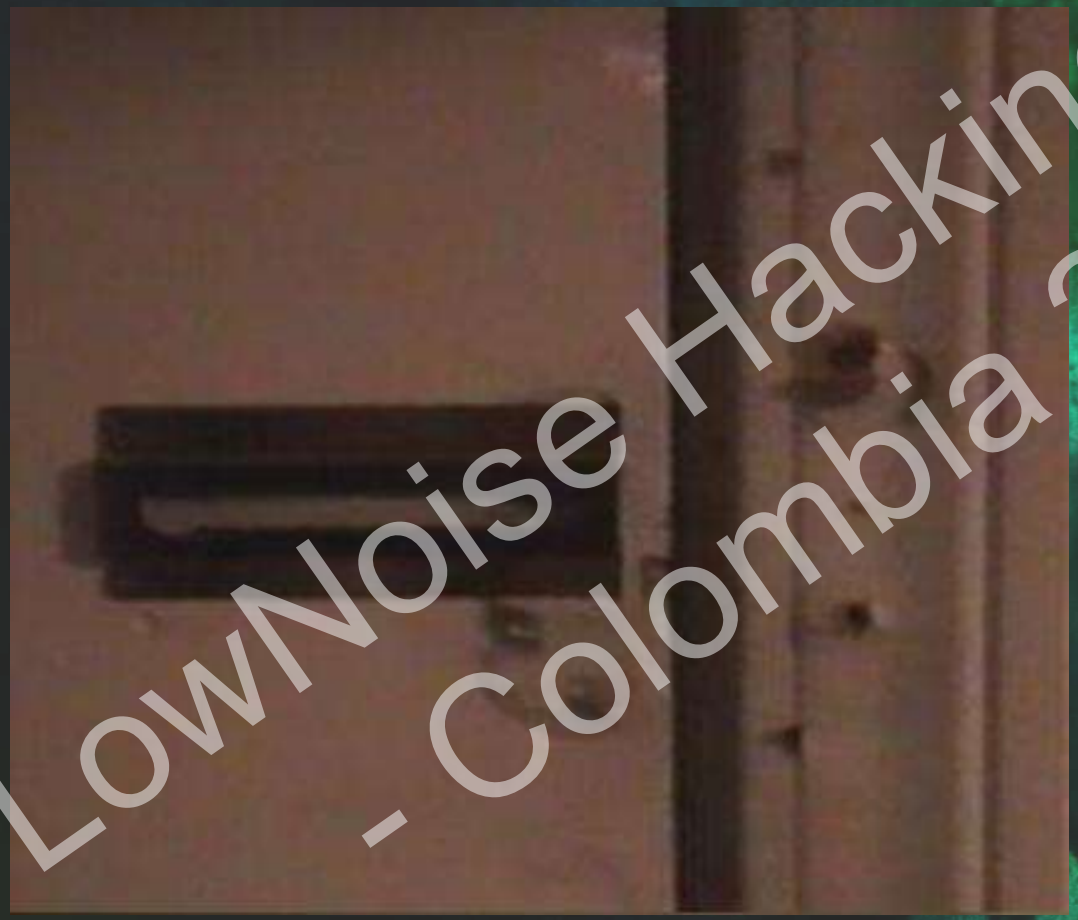
PUNTOS CRÍTICOS DE LA DEFINICIÓN:

- Es un **ARTE**
- El objetivo es **DESHABILITAR** el mecanismo de cierre
- **SIN** alterar o dañar la cerradura
- **SIN** dejar evidencia de manipulación
- **NADA ILEGAL !!!!**

¿ Qué NO es Lockpicking ?

¿ Qué NO es Lockpicking ?

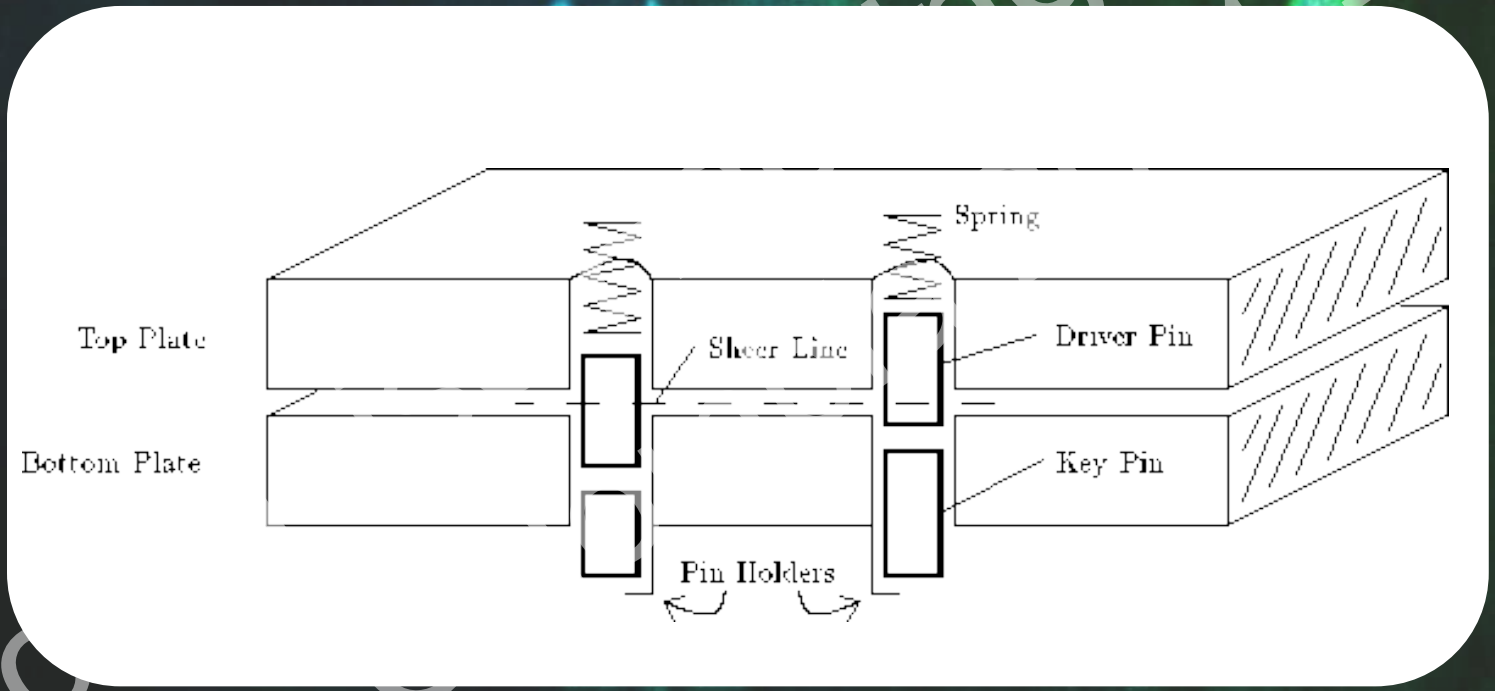
¿ Qué NO es Lockpicking ?



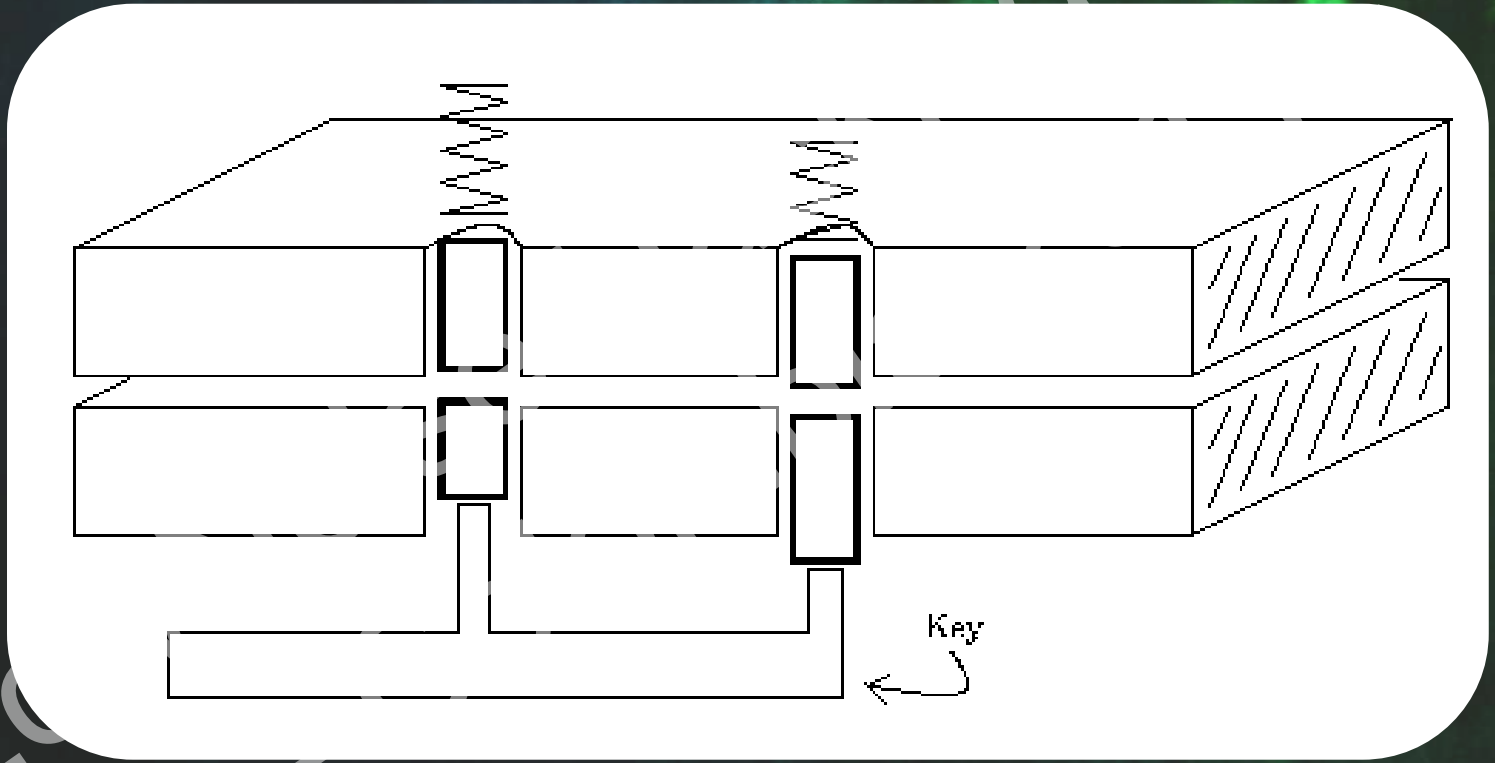
¿ Qué NO es Lockpicking ?

¿ Qué NO es Lockpicking ?

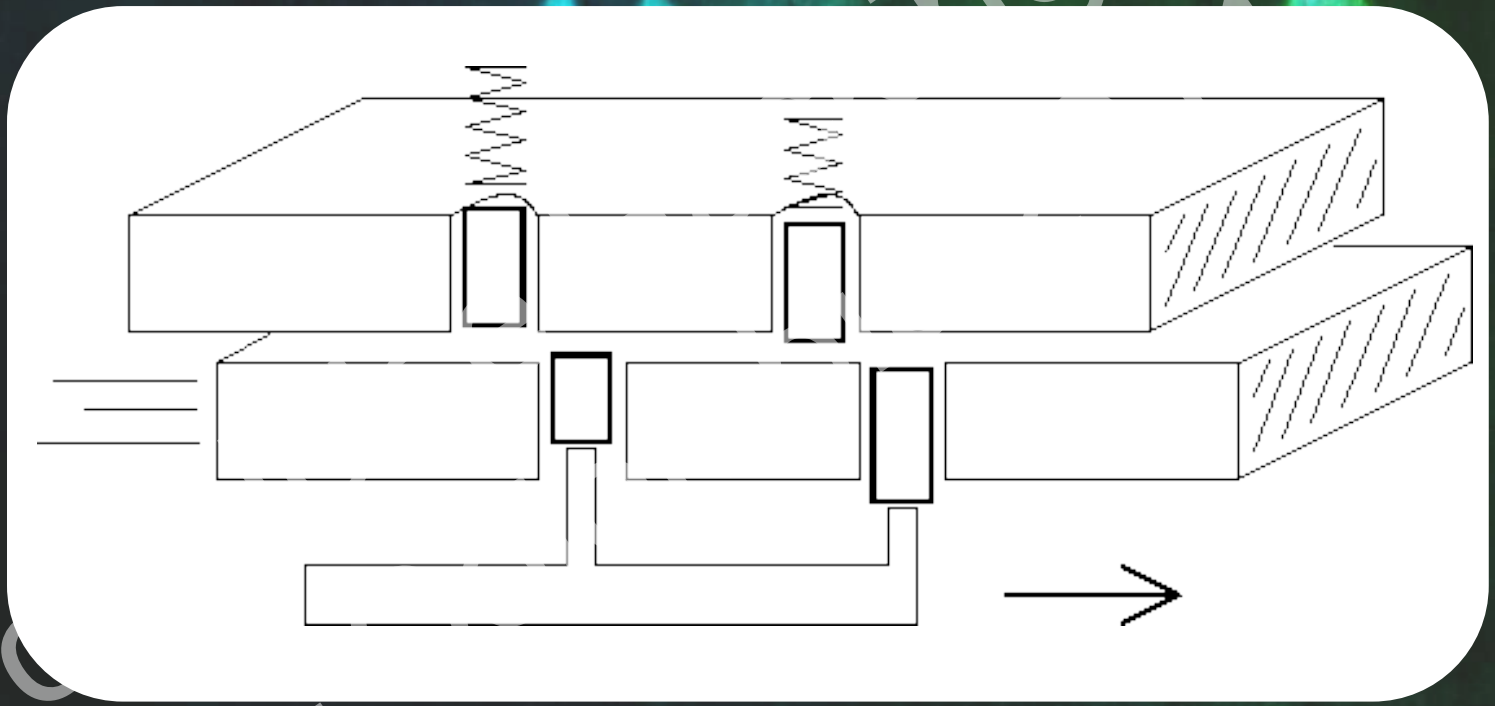
Funcionamiento de una Cerradura Básica



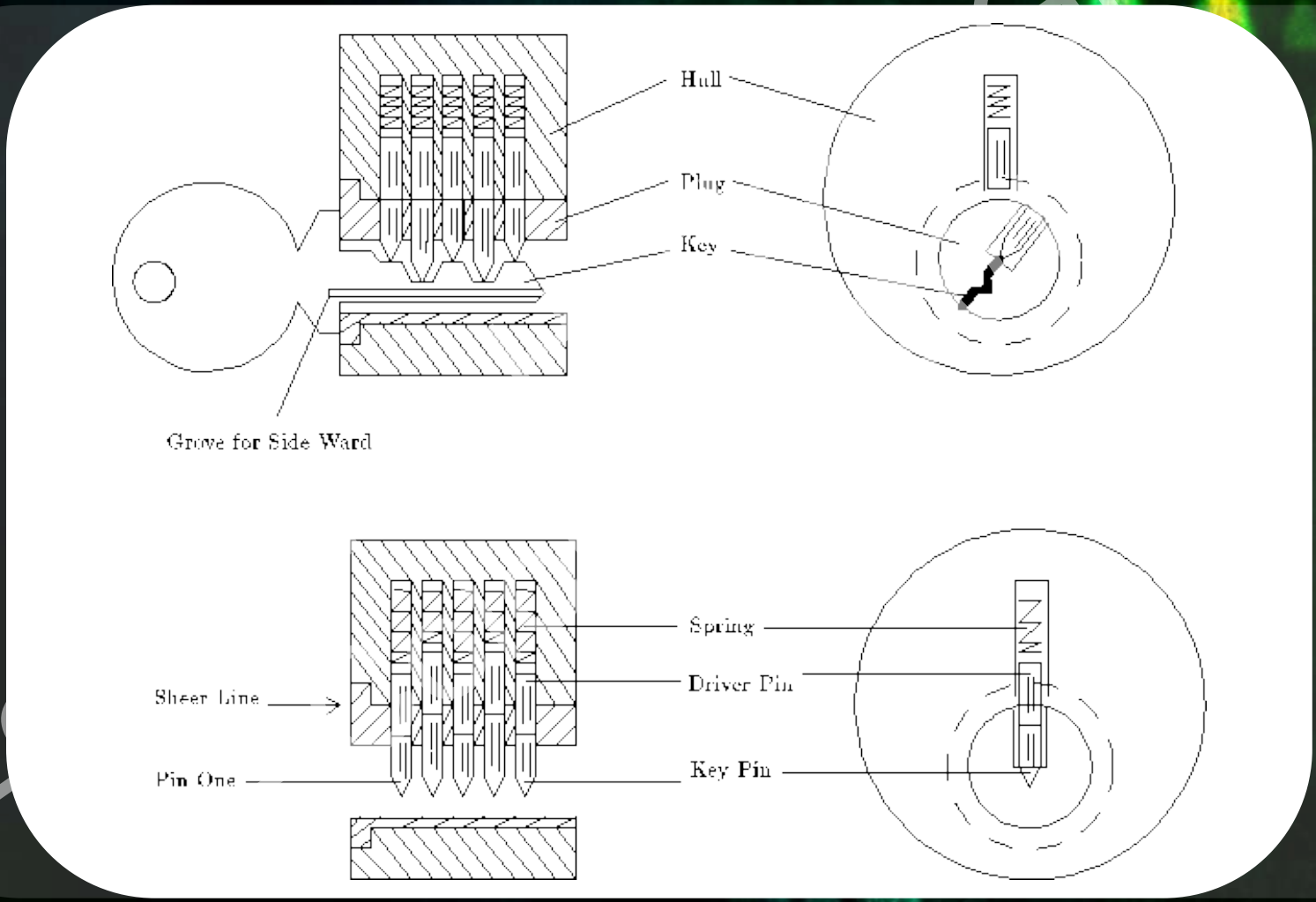
Funcionamiento de una Cerradura Básica



Funcionamiento de una Cerradura Básica



Funcionamiento de una Cerradura Básica



Funcionamiento de una Cerradura Básica

Herramientas Básicas

- **Tensores/Llaves de Torsión y Picks (ganzúas?)**

Herramientas Básicas

Herramientas Básicas

Herramientas Básicas

Herramientas Básicas

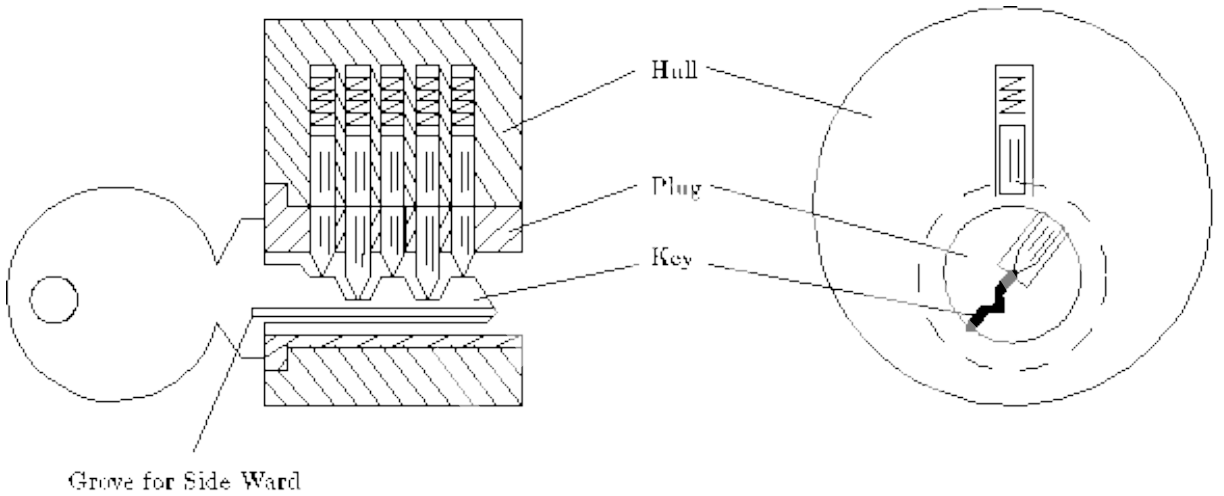
Herramientas No Tan Básicas

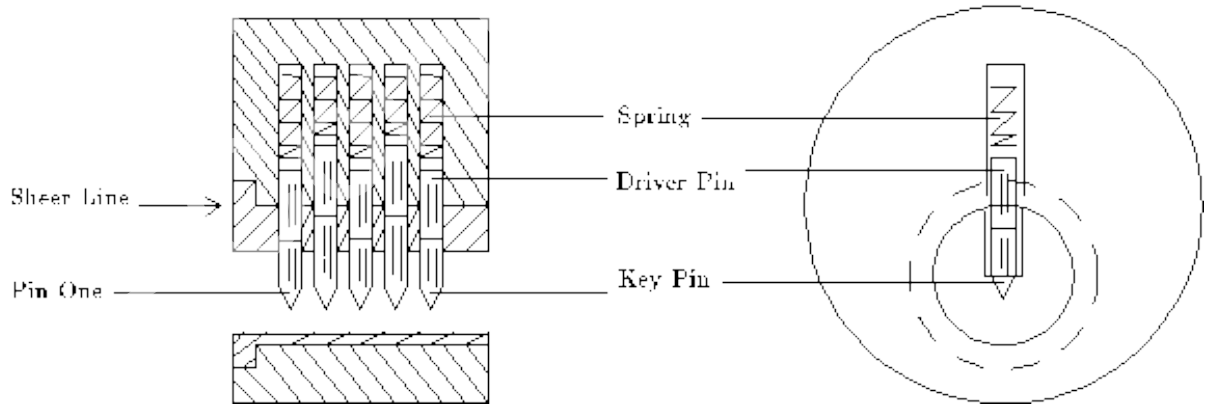
Herramientas No Tan Básicas

Herramientas No Tan Básicas

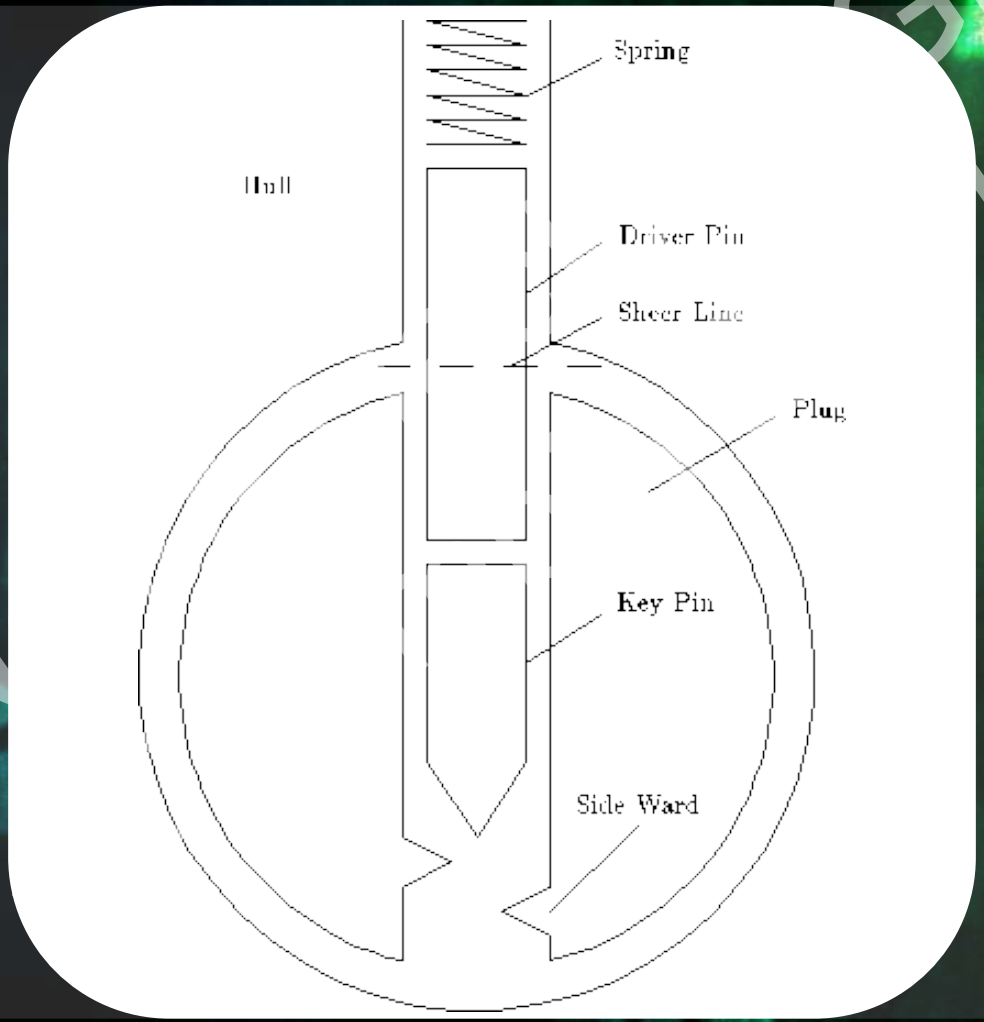
Herramientas No Tan Básicas

Uso de las Herramientas Básicas

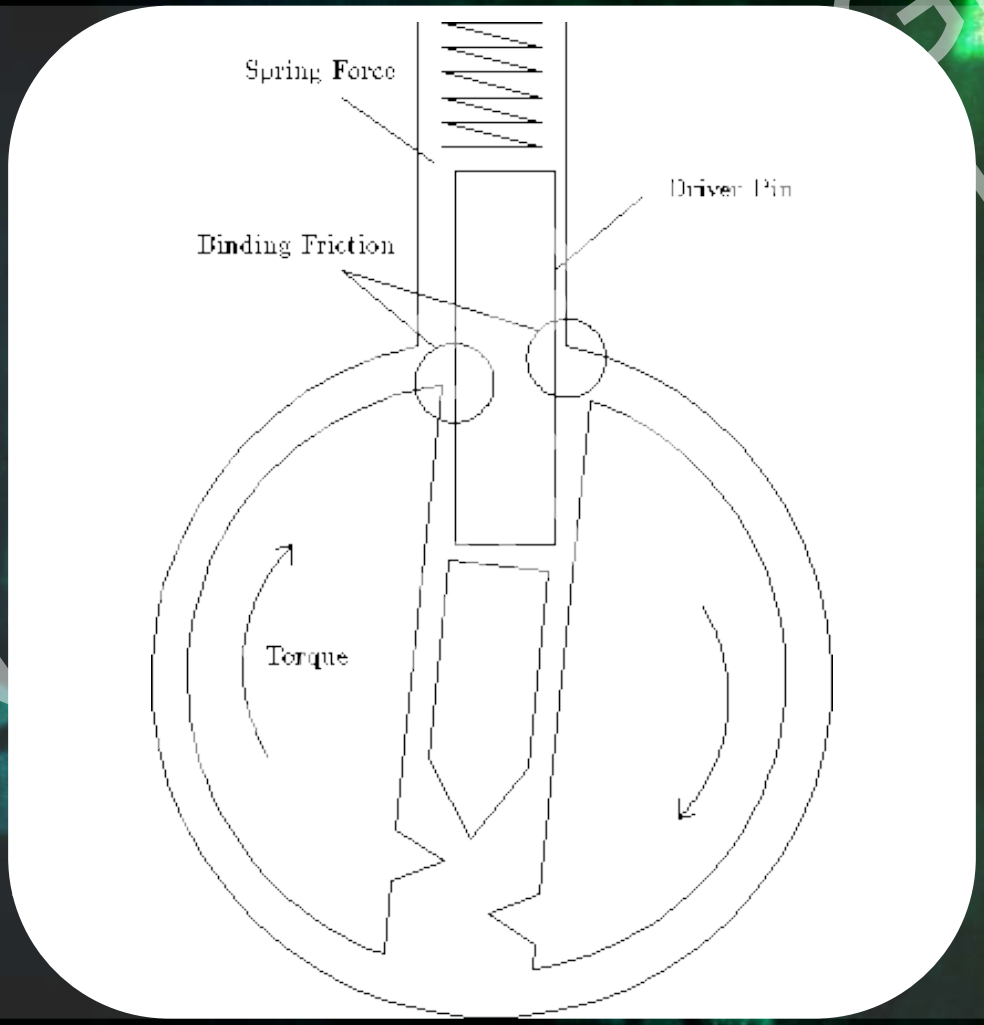




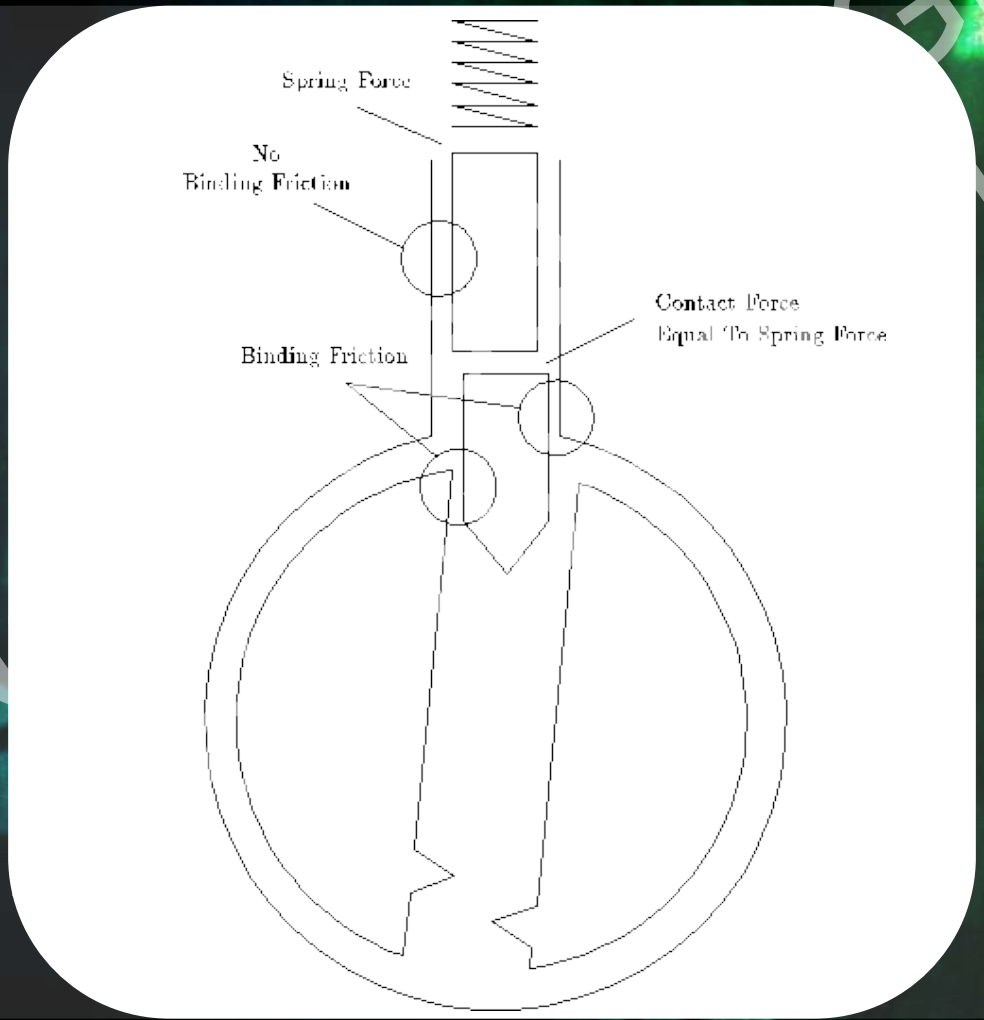
Uso de las Herramientas Básicas



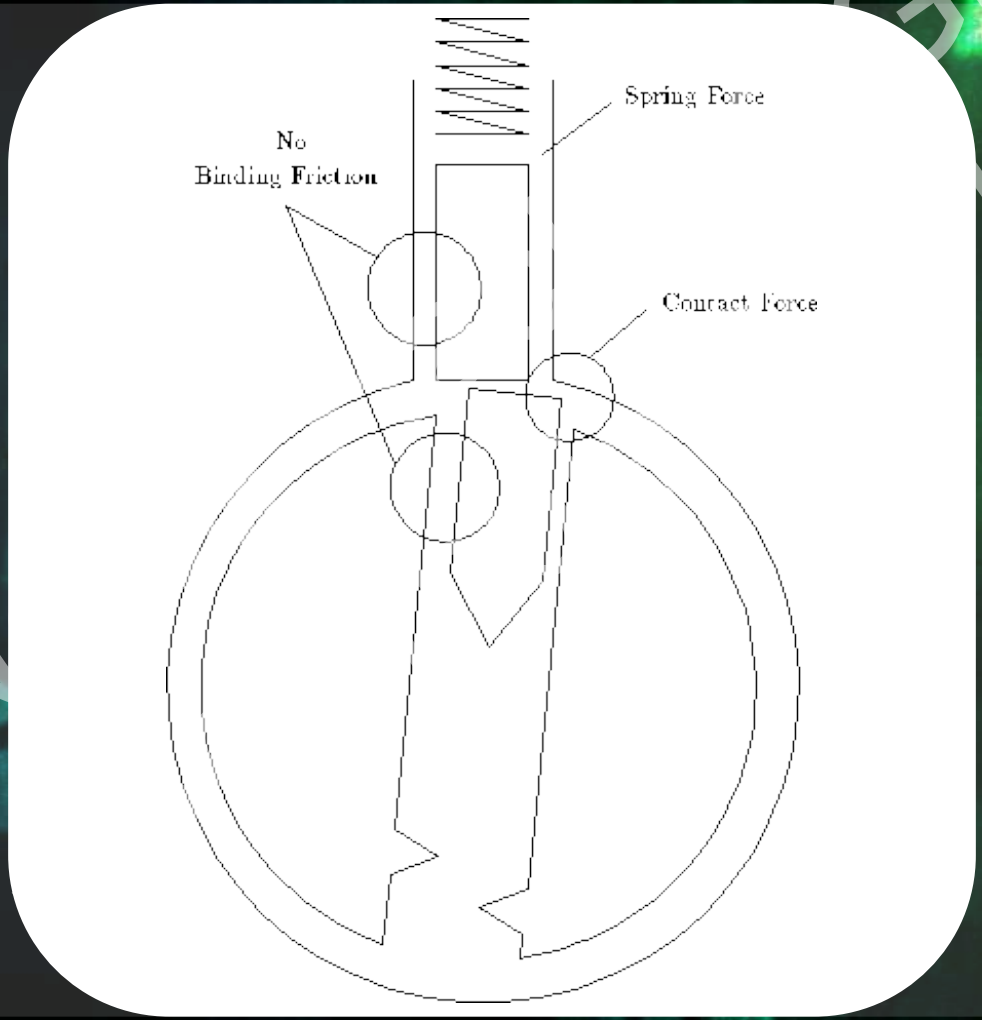
Uso de las Herramientas Básicas



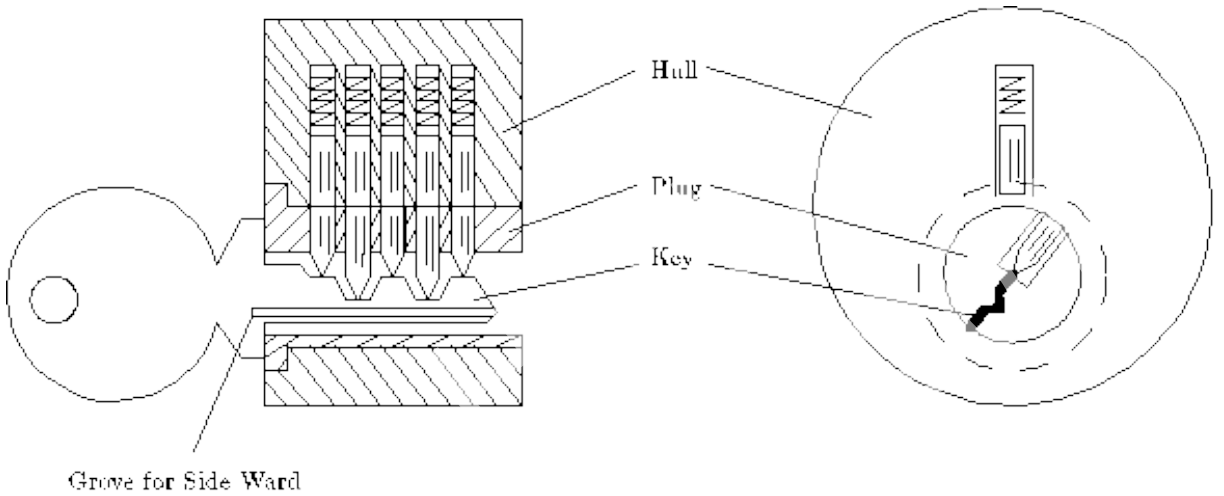
Uso de las Herramientas Básicas

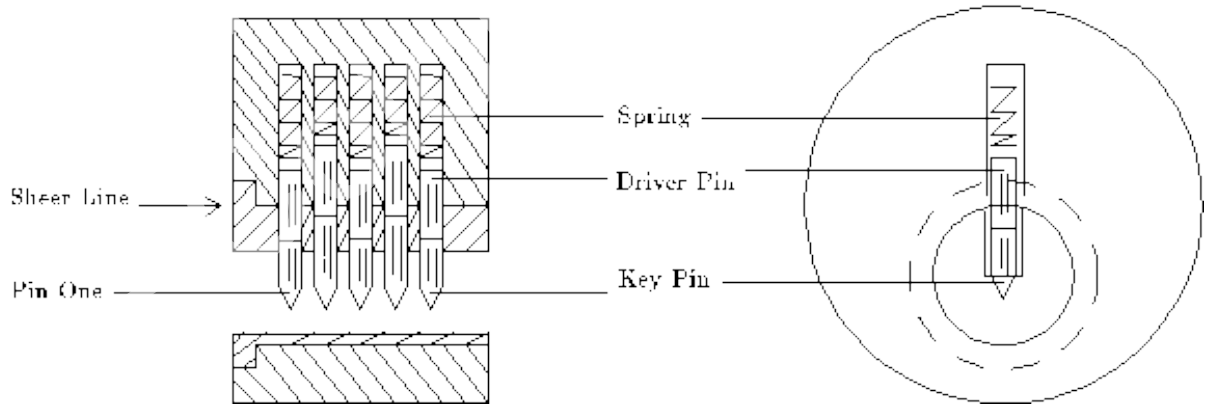


Uso de las Herramientas Básicas

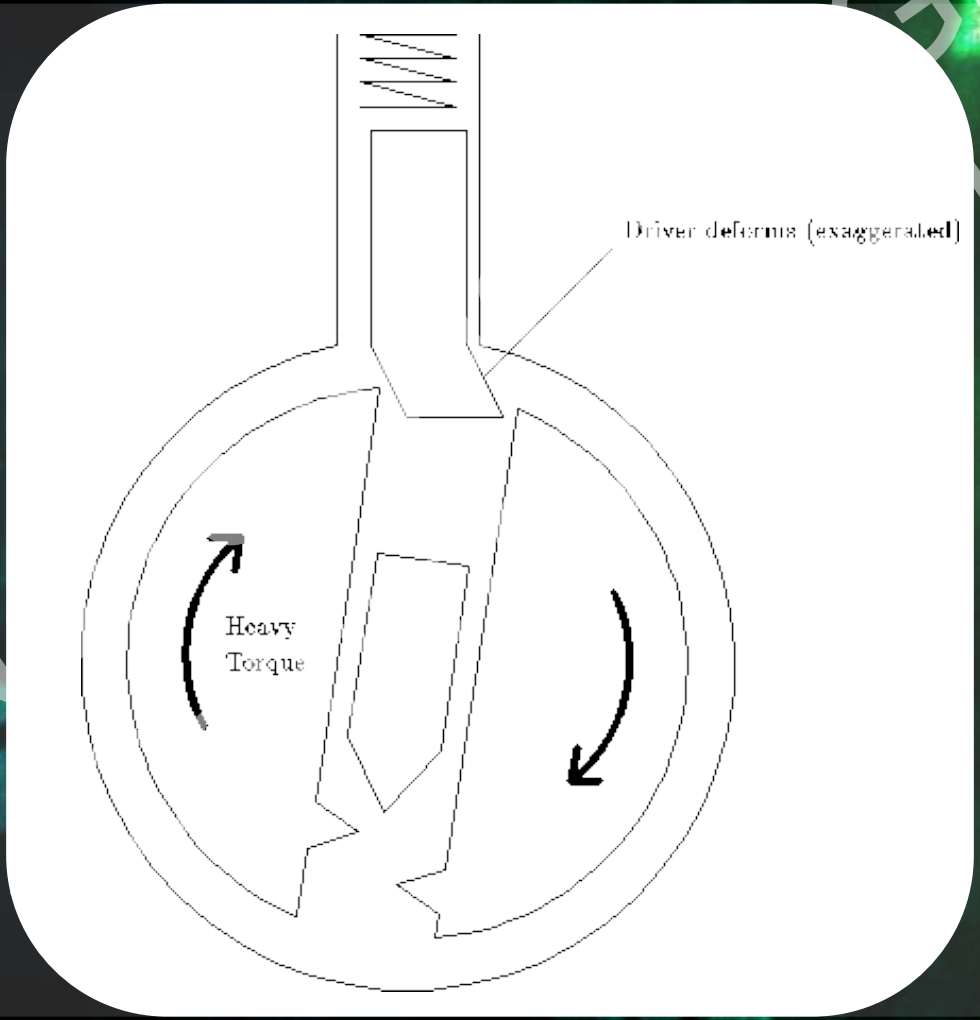


Uso de las Herramientas Básicas

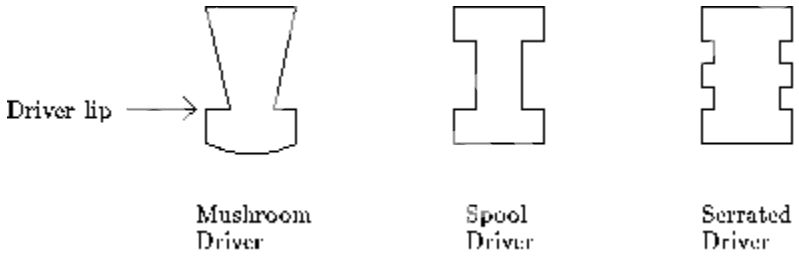




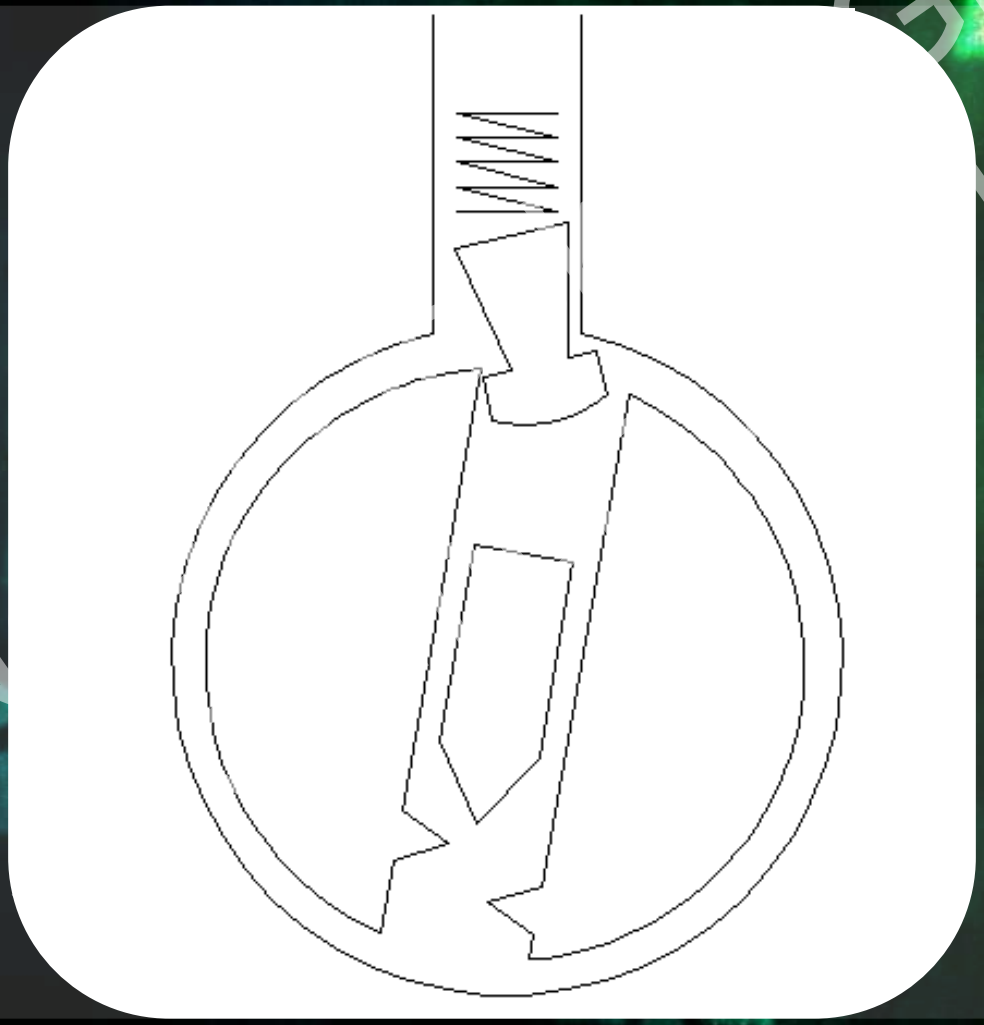
Uso de las Herramientas Básicas



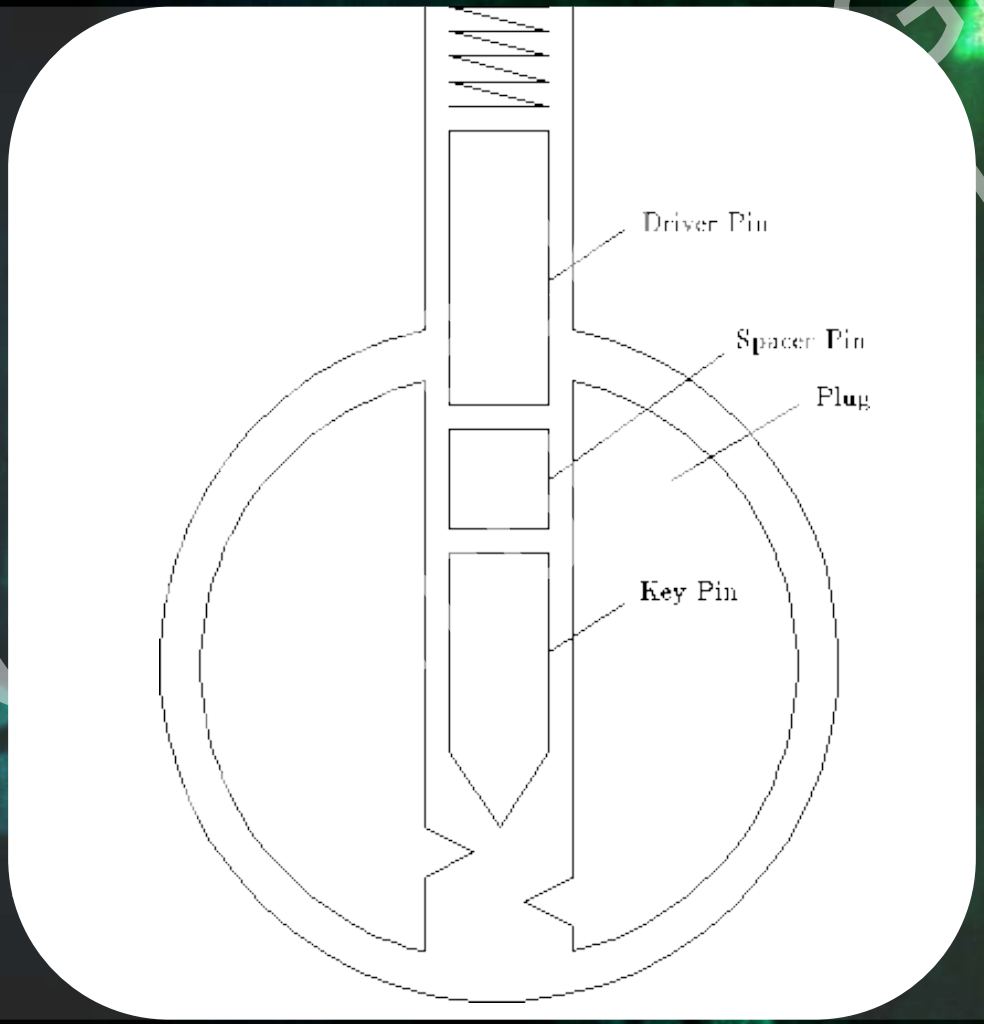
Uso de las Herramientas Básicas



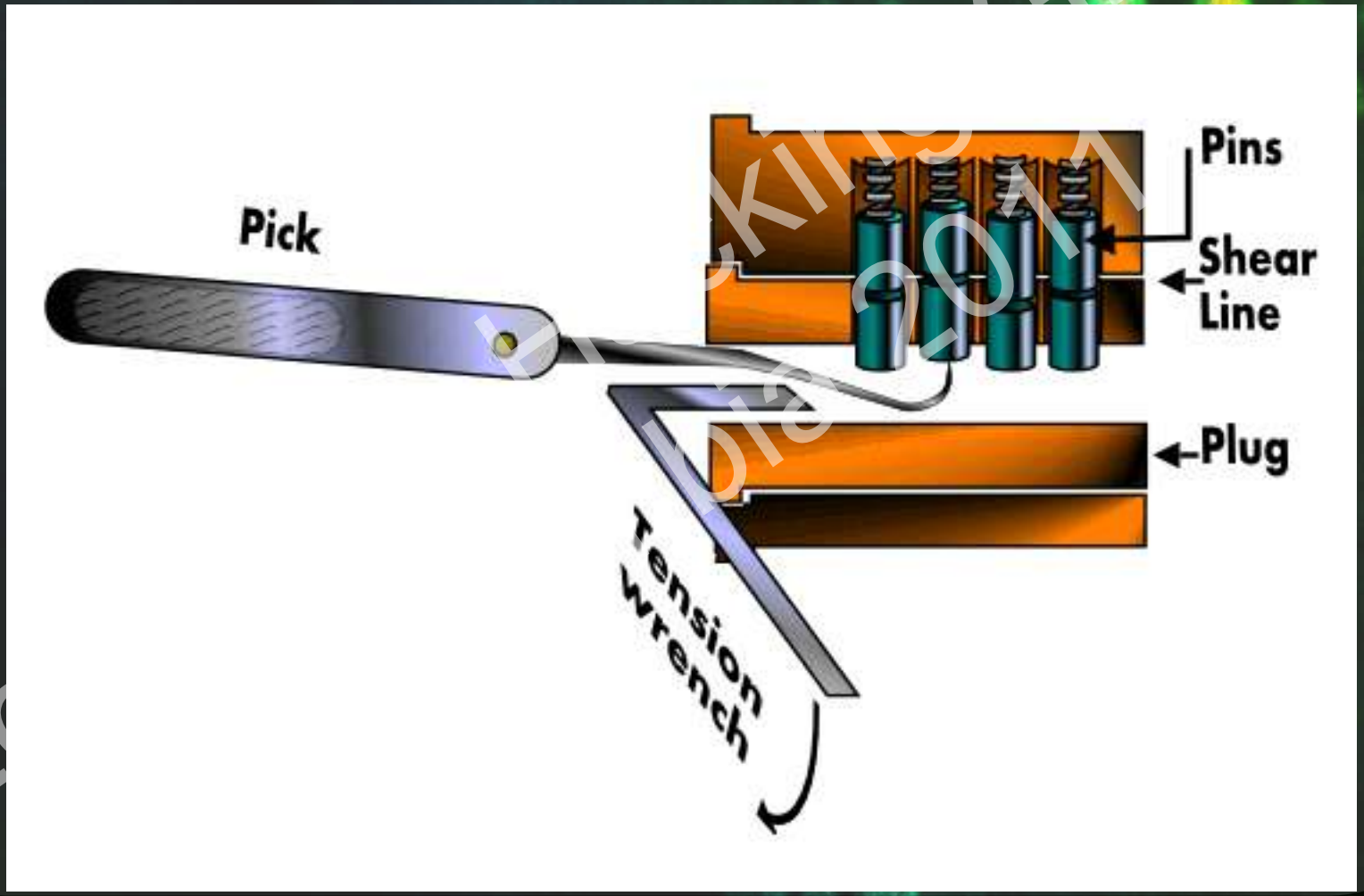
Uso de las Herramientas Básicas



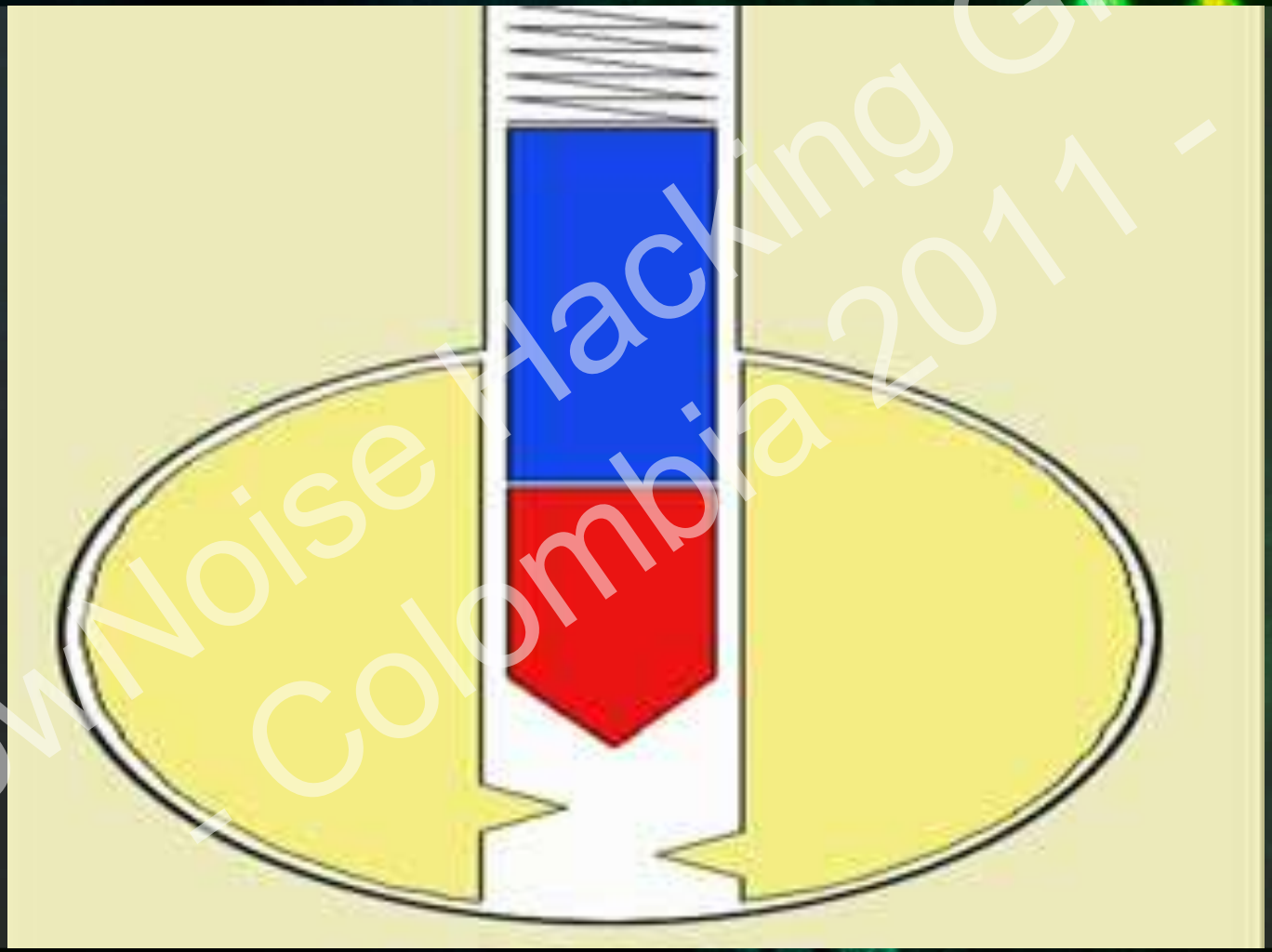
Uso de las Herramientas Básicas



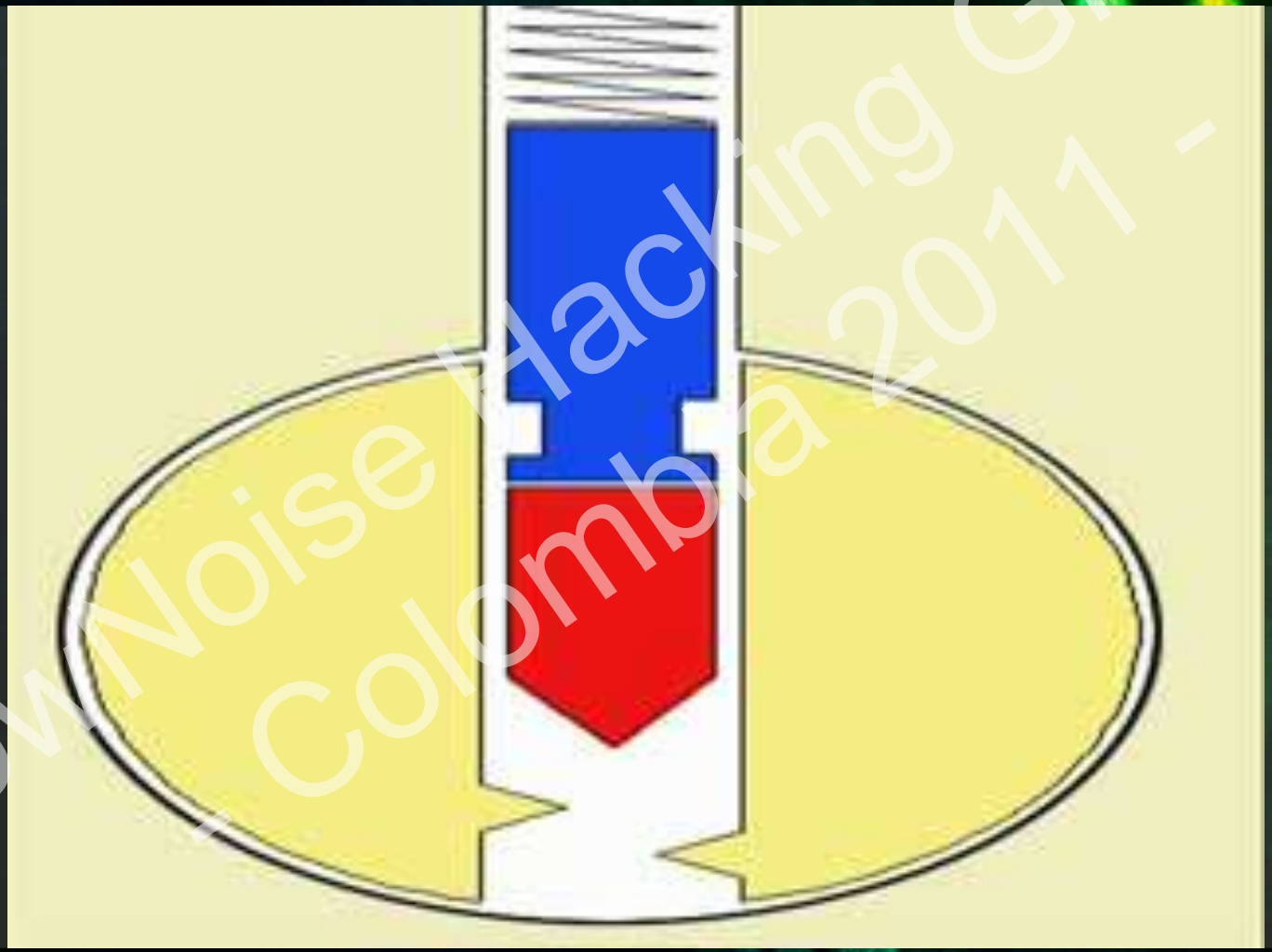
Uso de las Herramientas Básicas



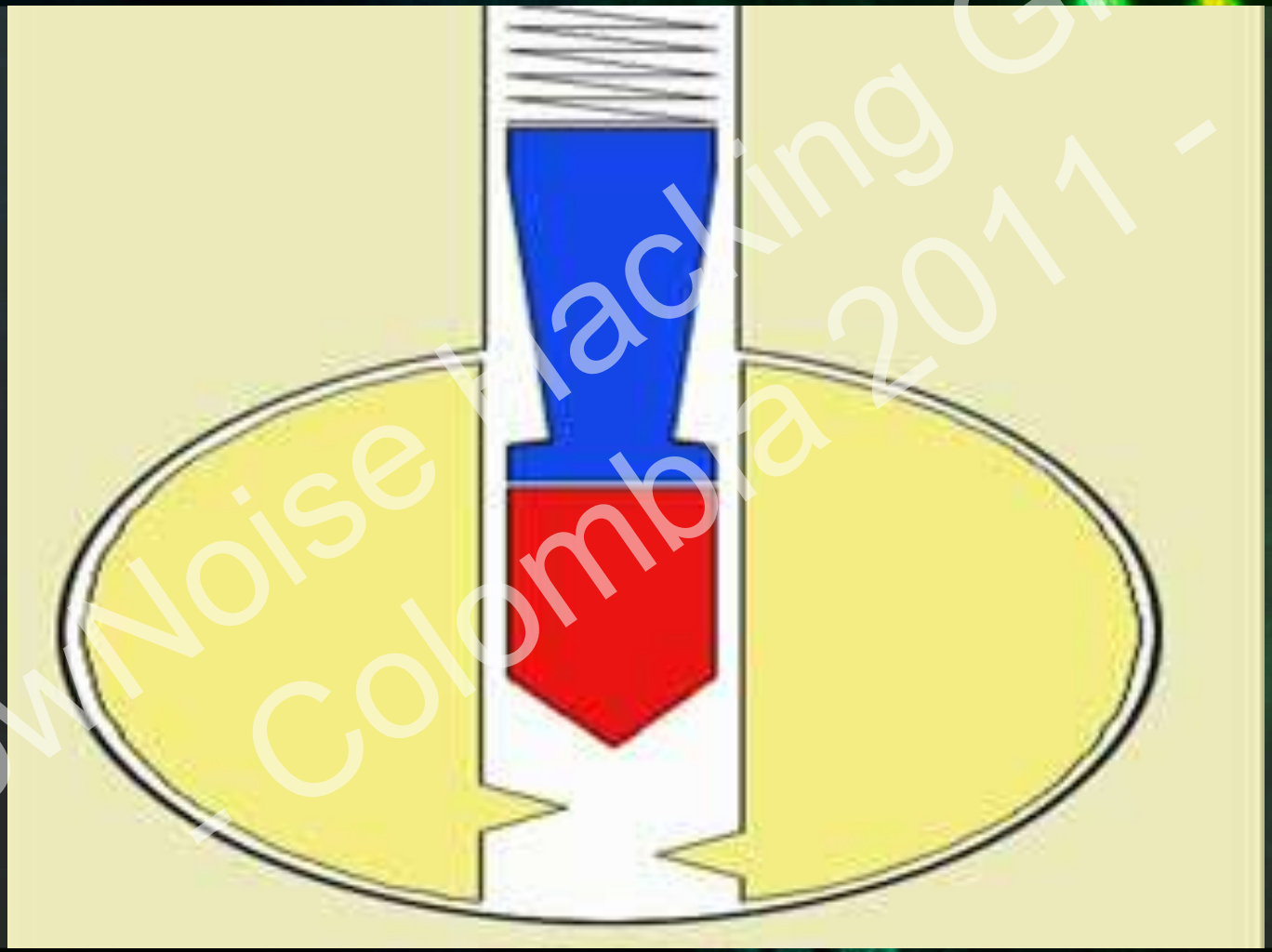
Uso de las Herramientas Básicas



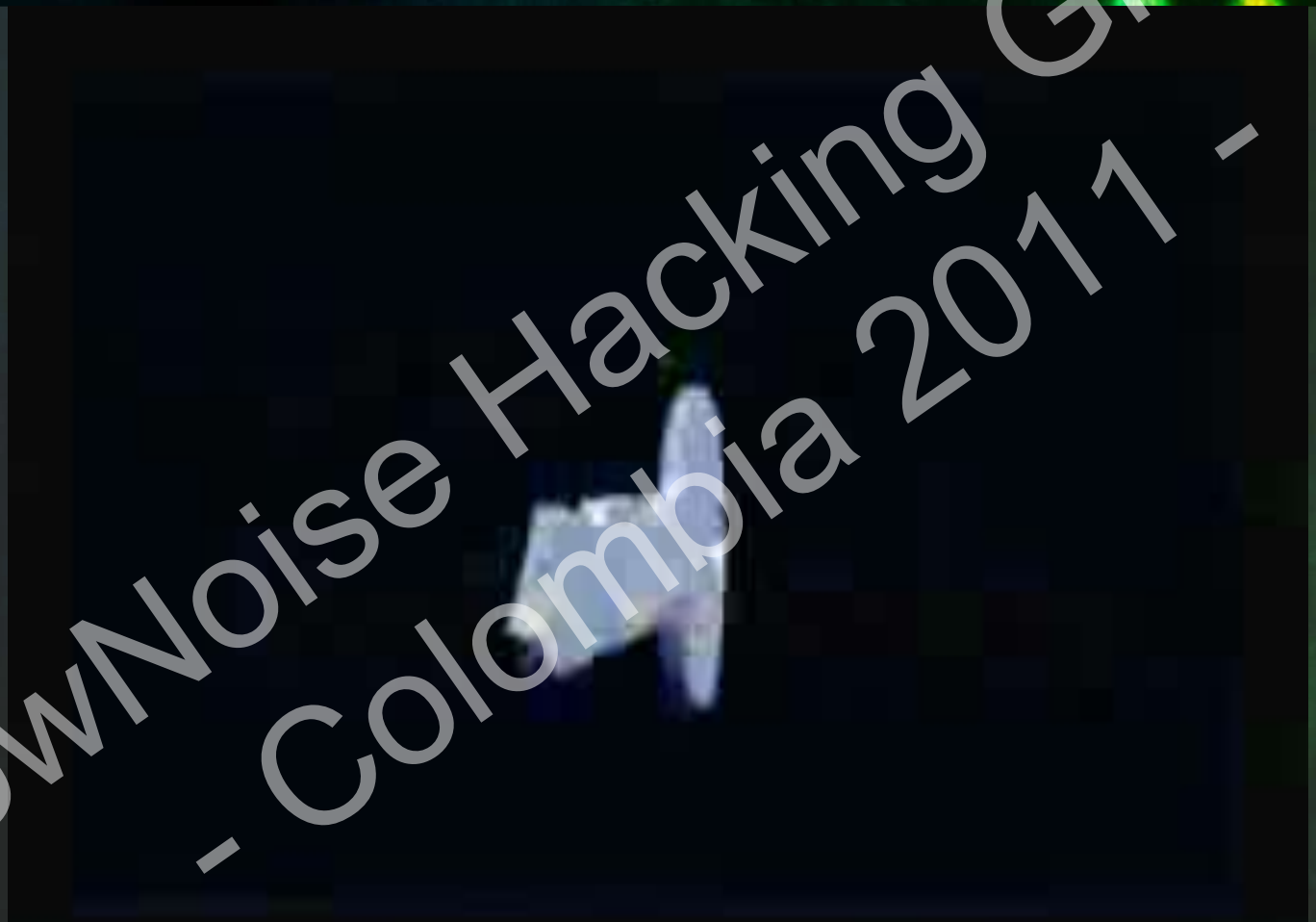
Uso de las Herramientas Básicas



Uso de las Herramientas Básicas



Uso de las Herramientas Básicas



Uso de las Herramientas Básicas

Demos

INMEDIATAMENTE A CONTINUACIÓN DE ESTA CHARLA, EN UNA MESA QUE CONSIGAMOS:

- **Varios tipos de cerraduras**
- **Varios tipos de herramientas**
- **Hands-on**
- **Tenemos muy pocos kits de lockpicking**

Recomendación Legal

SOLAMENTE PRACTIQUE LOCKPICKING CON CERRADURAS PROPIAS !

Conclusiones

A seguir disfrutando de Campus Party ….

OJO -> La charla está en:
http://www.lownoisehg.org/CampusParty2011/

Otras Charlas de LowNoiseHG en CPCO4

Martes 28 de Junio - 3:30pm

F4Lc0N - Qué es SCADA y cómo me afecta su (in)seguridad ?

Miércoles 29 de Junio - 3:30pm

bytemare – Informática Forense e Investigaciones Digitales

Viernes 1 de Julio - 10:30am

tinpardo - Ataques Distribuidos de DoS a Sistemas Web

Viernes 1 de Julio - 1:30pm (**BarCamp CP**)

F4Lc0N - Principios Básicos de LockPicking

Viernes 1 de Julio - 3:30pm

bytemare – Computación Parasitaria

Viernes 1 de Julio - 8:30pm

nopbyte - Aseguramiento de Vuln. Web con Tecnologías OWASP

FIN

- Gracias por la paciencia
- Para investigaciones con LNHG:

falcon@lownoisehg.org

Twitter: @falcon_lownoise

http://www.lownoisehg.org/

- Para cosas más “serias”:

mrubio@itss.com.co