

Lockpicking 101

O como enseñar a un grupo de colegas
a hacer el mal con un par de hierritos y
algo de práctica.



Índice

Bienvenidos

Disclaimer

¿que es lockpicking?

- Herramientas
- Anatomía de una cerradura
- Técnicas
 - Pin a pin
 - ◇ Pines de seguridad
 - Rastrillado
 - Pincho
 - Otras cerraduras
- Candados de combinación
 - Apertura manual
 - Padlock shim
- Cerraduras Tubulares
 - Apertura manual
 - Apertura tubular
- Cerraduras de disco
 - Apertura manual
- Puertas de emergencia
 - Hooks

Bienvenidos!

LOCKPICKING

QUE VENIMOS A APRENDER?

**COMO DELINCUENTES!!!
JUJU EQUISIDE**

**¿COMO NOS
HACE SENTIR?**

imgflip.com

Disclaimer

- Se que no hace falta decirlo, pero por si acaso preferimos curarnos en salud:
- **TODO LO EXPLICADO EN ESTA CHALA ES MATERIAL DE APRENDIZAJE PARA FINES EDUCATIVOS.**
- **SE PIDE A LOS ASISTENTES QUE USEN LOS CONOCIMIENTOS CON CUIDADO Y ETICA SIEMPRE EN ENTORNOS CONTROLADOS Y NUNCA PARA COMETER ILEGALIDADES.**
- Dicho esto, que es de cajón... no nos responsabilizamos del uso que den los asistentes a los conocimientos adquiridos ... sentaos y disfrutad del viaje pues el Hacking es un mundo muy extenso y lleno de rincones oscuros para mentes inquietas.

Who am I?

Ah mierda que ya lo sabéis, ya la costumbre...

- Username : Alvaro Alonso (A.K.A. - Nebu73)
- Twitter/Telegram : @Nebu_73
- Pentester / Hacker ético
- Cibercooperante de Incibe (I4SK)
- Master en Ciberseguridad - Cybersoc de Deloitte
- Experto en Seguridad de la Información - UCLM
- Certified Ethical Hacker - EC Council
- OSWP - Offensive Security Wireless Professional
- Administrador y escritor del blog de Seguridad Informática - 
- Actualmente Red Teamer en :  Profesor del master de Ciberseguridad de de kyndryl
- Ponente en :



¿Lockpicking?

100
89
rage

Lock Picking in Movies/TV Shows Starter Pack

Jiggling a single lock pick instead of a rake and the lock instantly opens



inserts two random tools
instant unlocking sound
"we're in"



Inserting two picks and no tension tool, lock opens in seconds



Inserts the correct tools for once and you think it's going to be a realistic scene

proceeds to rapidly jiggle the correct tools up and down
unlocking sound
"got it"

Esto no es...



¿Qué es el lock picking?

Lock picking es la habilidad de abrir una cerradura mediante el análisis y manipulación de sus componentes internos sin utilizar la llave original. Algunas personas disfrutan de esto de manera recreacional, lo cual consiste en el estudio y el aprendizaje de cómo derrotar los sistemas de seguridad internos de las cerraduras para lograr su apertura sin daño alguno de sus componentes internos.

Por tanto lo que
pretendo es
que tras este
taller paséis de
una situación
así....



A una así...

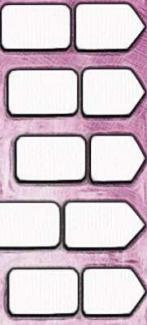


TYPES OF Lock PICKS

¿Qué herramientas
se utilizan?

THE CITY RAKE

THE CITY RAKE GETS ITS NAME FROM ITS RESEMBLANCE TO A CITY SKYLINE! IT IS A POWERFUL TOOL AGAINST PIN ARRANGEMENTS WHERE THERE ARE SHORTER PINS IN THE MIDDLE AND LONGER PINS IN THE FRONT AND BACK.



¿Qué
herramientas se
utilizan?

TYPES OF Lock Picks

THE GEM

THE GEM IS ANOTHER VERY POPULAR PICK THAT SIMPLY ADDS A SHORT, BUT POINTY, TIP TO THE END OF THE SHORT HOOK. THIS GIVES US A LITTLE MORE REACH WITHOUT SACRIFICING ANY OF THE MANEUVERABILITY AND AGILENESS OF THE BELOVED SHORT HOOK.



- Ganzúa de gancho
 - Los hay más cortos, más largos, con más curva y con menos pero sirven para ir levantando pin a pin.

¿Qué? ¿Qué es un pin?



¿Qué herramientas se utilizan?

- EL TENSOR porque levantar pinos esta divertido si pero..... habrá que simular la tensión de giro dentro del bombín no? Pues para eso se usa esta herramienta.



ENTONCES COMO RESUMEN

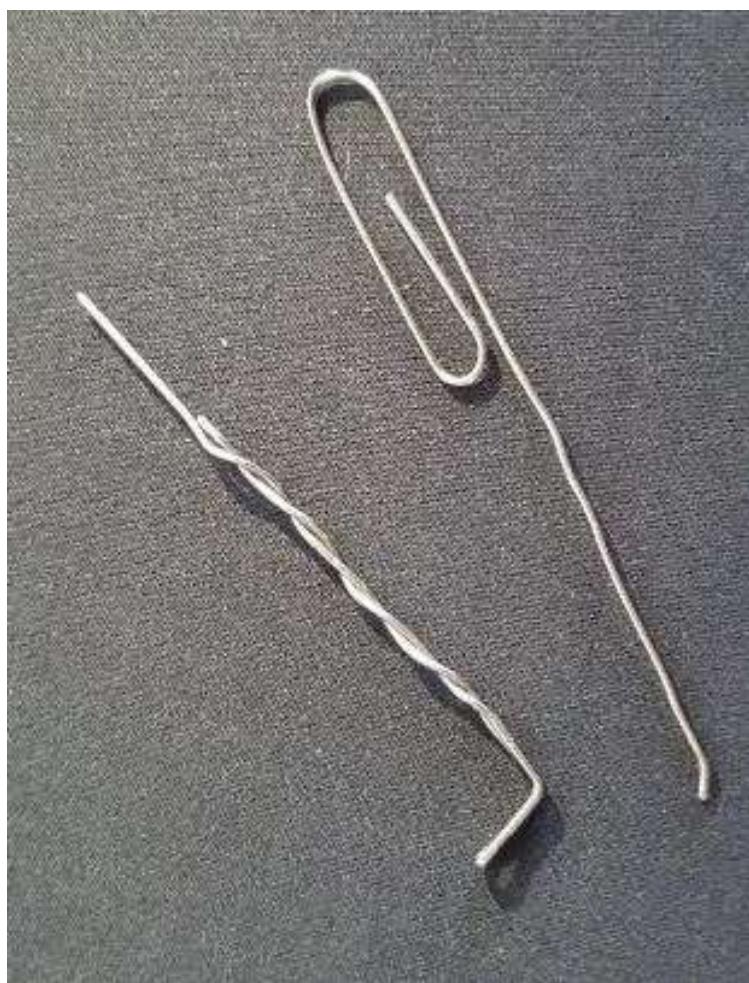
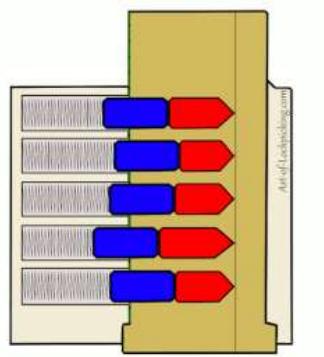
— ¿Sabrías decirme si jugamos a quien es quien?

MAS REFERNCIAS! => <https://www.facebook.com/artoflockpicking/photos>

BRICO-Picking

- Hay veces que no dispones de tus amadas ganzúas (mal! Llévalas encima o será un...)
- Por ello es recomendable llevar tanto una navaja multiusos como unos clips o unas horquillas ;P.



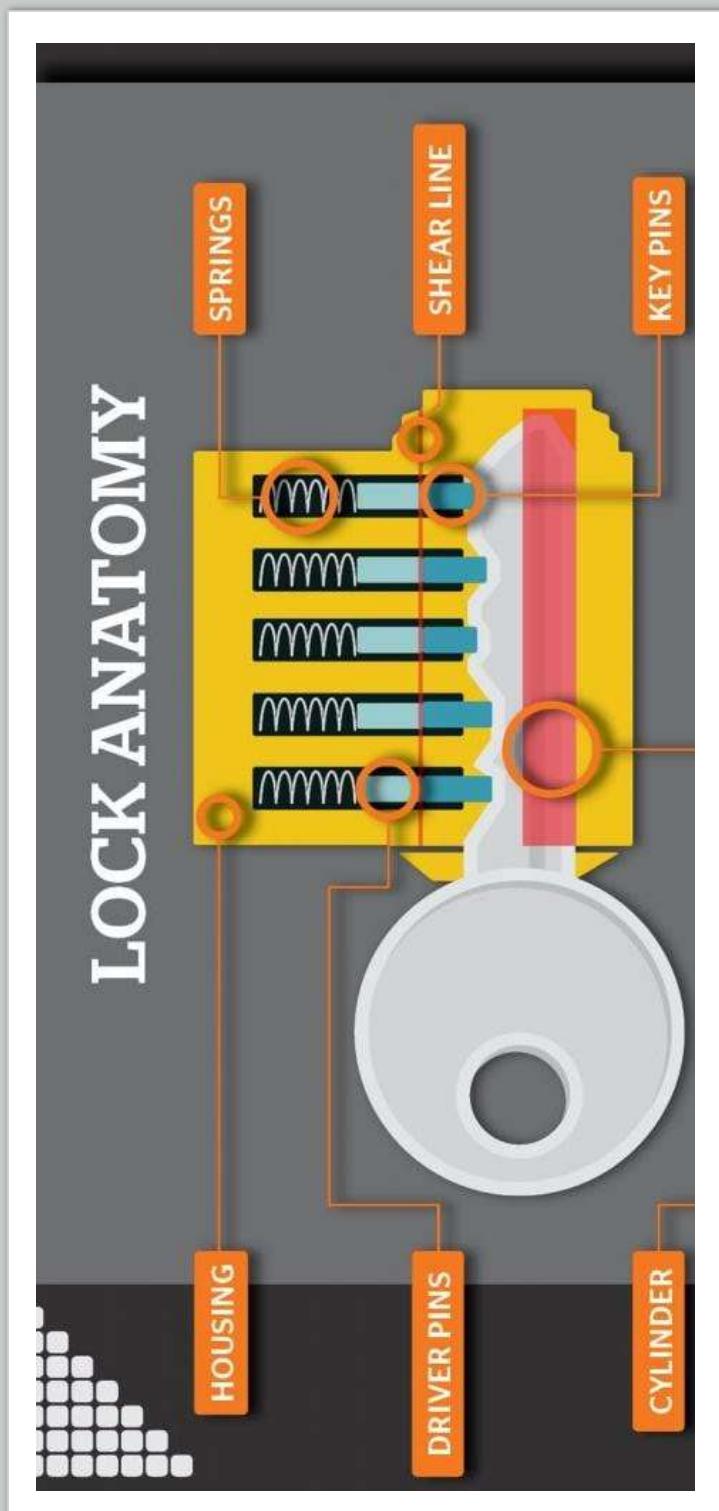


El bombín

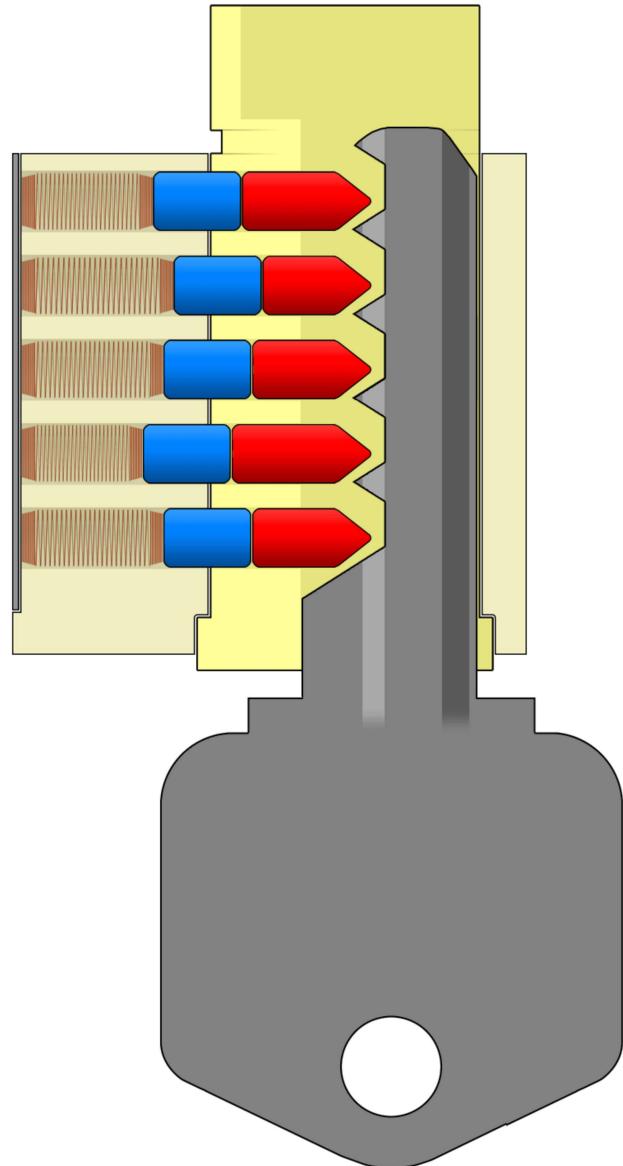


- Vale, hemos hablado de las herramientas pero nos queda hablar de lo importante, de la cerradura/bombín, llámalo como quieras... y sobre todo de su anatomía.

Anatomía de una cerradura



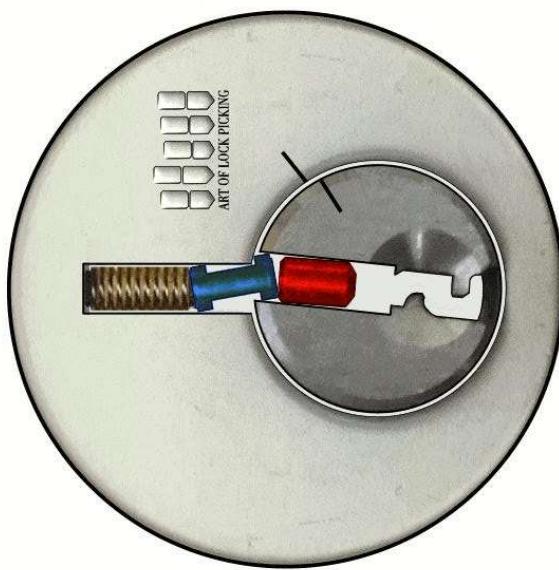
MECANISMO



- Al introducir la llave, los picos que tiene, empujan los pinos hacia arriba para hacer que coincidan con la línea del shear, desbloqueando el mecanismo y haciendo que se permita el giro.

Los Pines

- La gran mayoría de las cerraduras, traen pines lisos sin mas historia pero las que son consideradas de "seguridad" traen pines especiales con surcos que hacen mas complicado su ganzuado o apertura.





NOW
THE...•



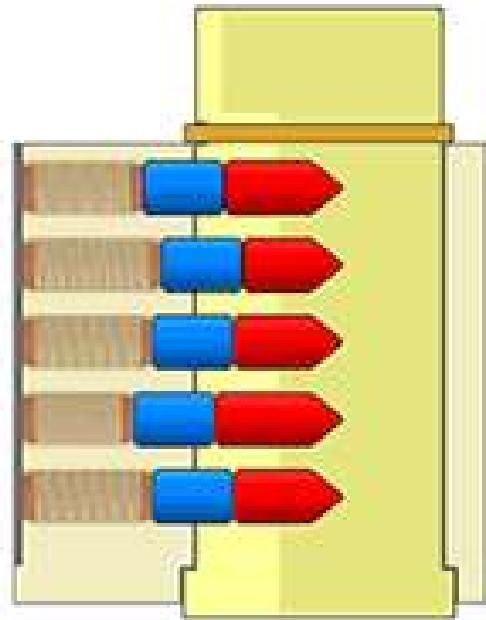
Las presentaciones

Aquí la cerradura de prácticas, aquí mis alumnos deseosos de aprender el mal.

Esta cerradura ha sido preparada para ser modificada según vayáis avanzando. Como veréis la vuestra esta ya montada por completo y tiene en la parte inferior unos tornillos allen.

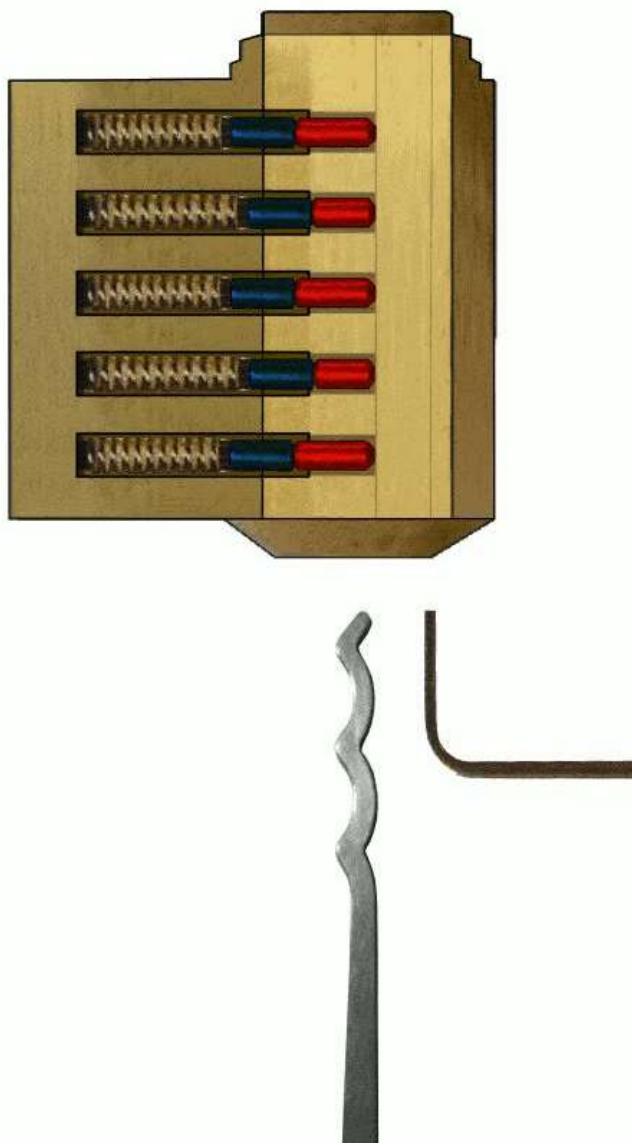
Aparte tenéis una bolsita con muelles, pines y contrapines para ir modificándolo y haciéndolo un pelín más difícil.

Técnica 1: Levantar pin a Pin



- Utilizando la llave de tensión, la introducimos por la abertura de la llave (por la parte donde no se ven los pinos) y hacemos fuerza para que simule una llave girando.
- Cogemos el gancho y lo introducimos donde se ven los pinos, ya que vamos a utilizarlo para empujarlos hasta que se alineen con el shear y así nos permita liberar el mecanismo.
- En el caso de añadir más pinos, es simple, seguir haciendo clics hasta que ceda. De ahí, los tornillos allen, podéis añadirle hasta 5 pinos más en el orden que queráis para ir aprendiendo.

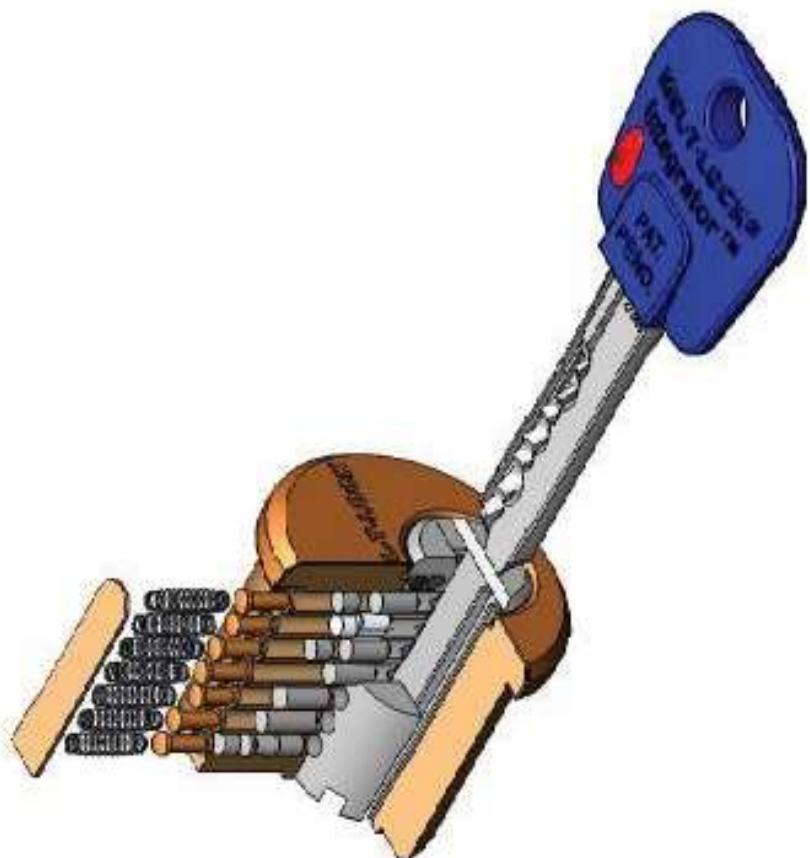
Técnica 2: Rastrillado



- Se utiliza un rastrillo con varios puntos elevados y se introduce en la cerradura, a la vez que se genera tensión con el tensor. Se mueve hacia delante y hacia detrás haciendo presión sobre los pines para ir liberando el cilindro.

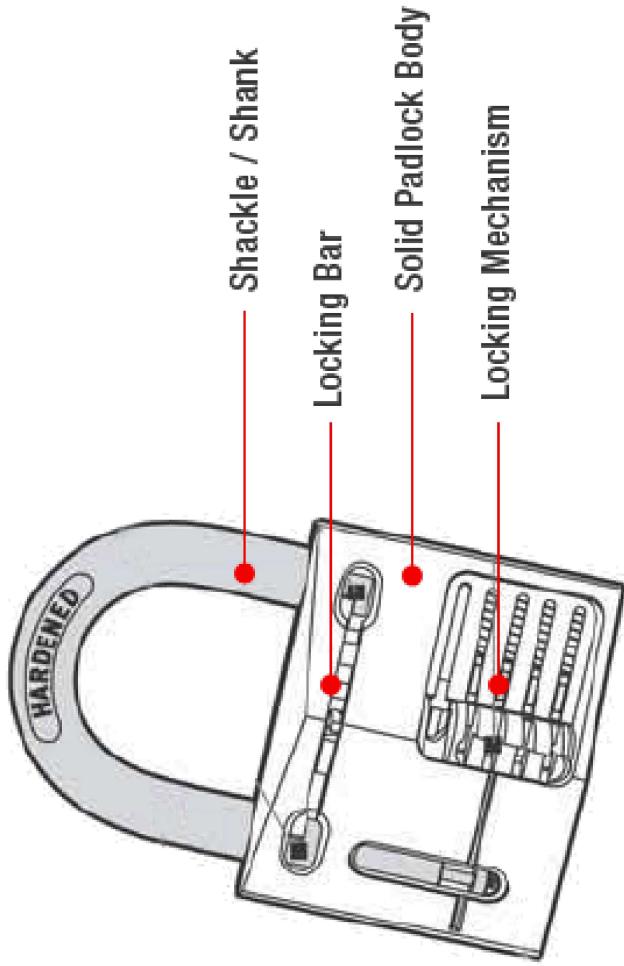
Otras cerraduras de pines

- Multilock
 - No dejan de ser cerraduras con pines, si quizás con más pines, lo más probable que con pines de seguridad, pero... pines a fin de cuentas por tanto se pueden abrir con algo de paciencia.



Candados

- En los candados todo funciona como en el resto de cerraduras, hay pines y se tiene que tensionar junto con levantar los pines uno a uno.
- Pero también existen problemas de diseño que permiten aperturas más imaginativas.



Técnica 3: El Pincho (candados)



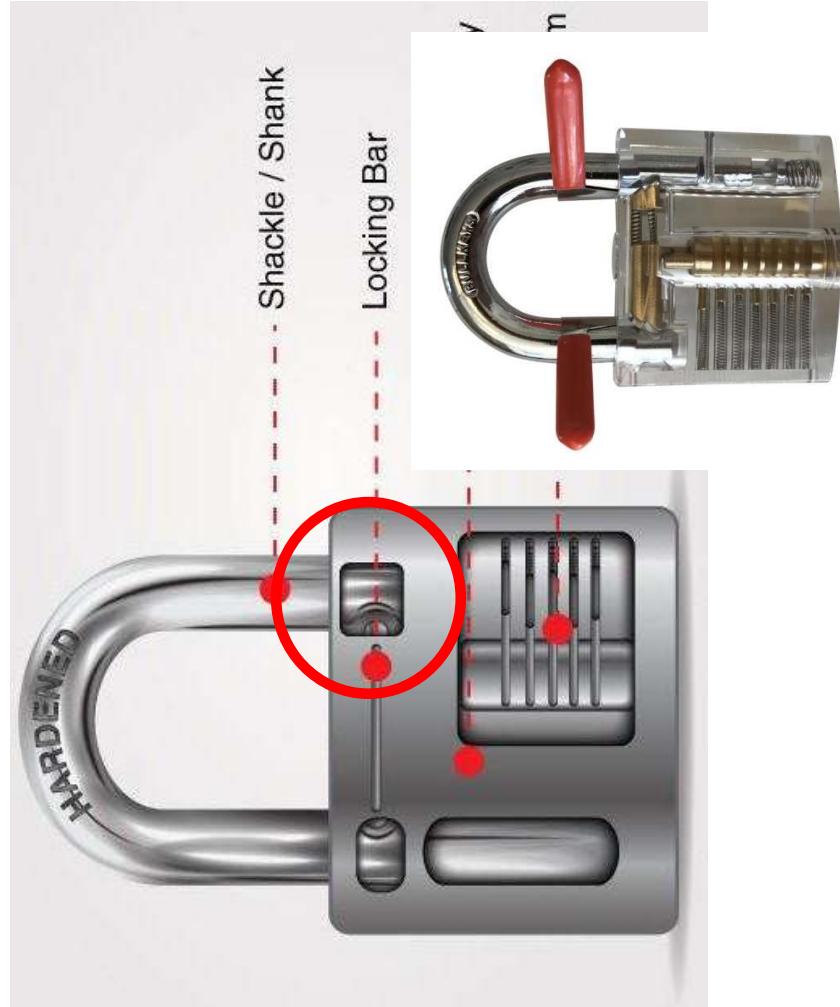
- Por fallos de diseño hay una herramienta que podríamos llamar "el pincho" que permite levantar el mecanismo de bloqueo del arco del candado haciendo que se abra sin necesidad de levantar pines.

[+] [VIDEO](#)

Técnica 4: Padlock Shim (Candado)

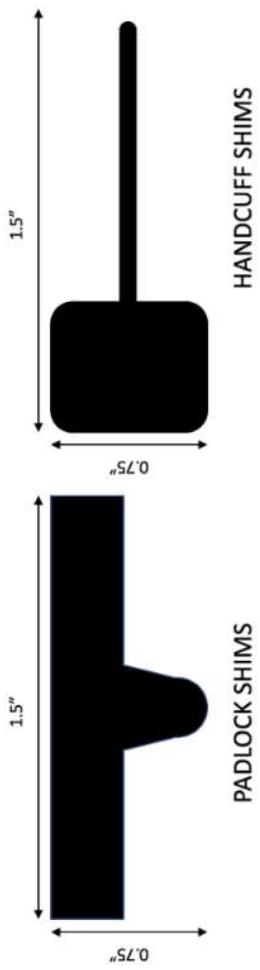
- Los candados disponen de 2 lengüetas que quedan liberadas al introducir y girar la llave. Estas lengüetas son las que mantienen el arco cerrado y sin opción a abrirse. Los padlock Shims son un pequeño bypass a la seguridad de la llave o combinación de desbloqueo, haciendo que las lengüetas queden liberadas y abriendo el candado.

[+] [VIDEO](#)



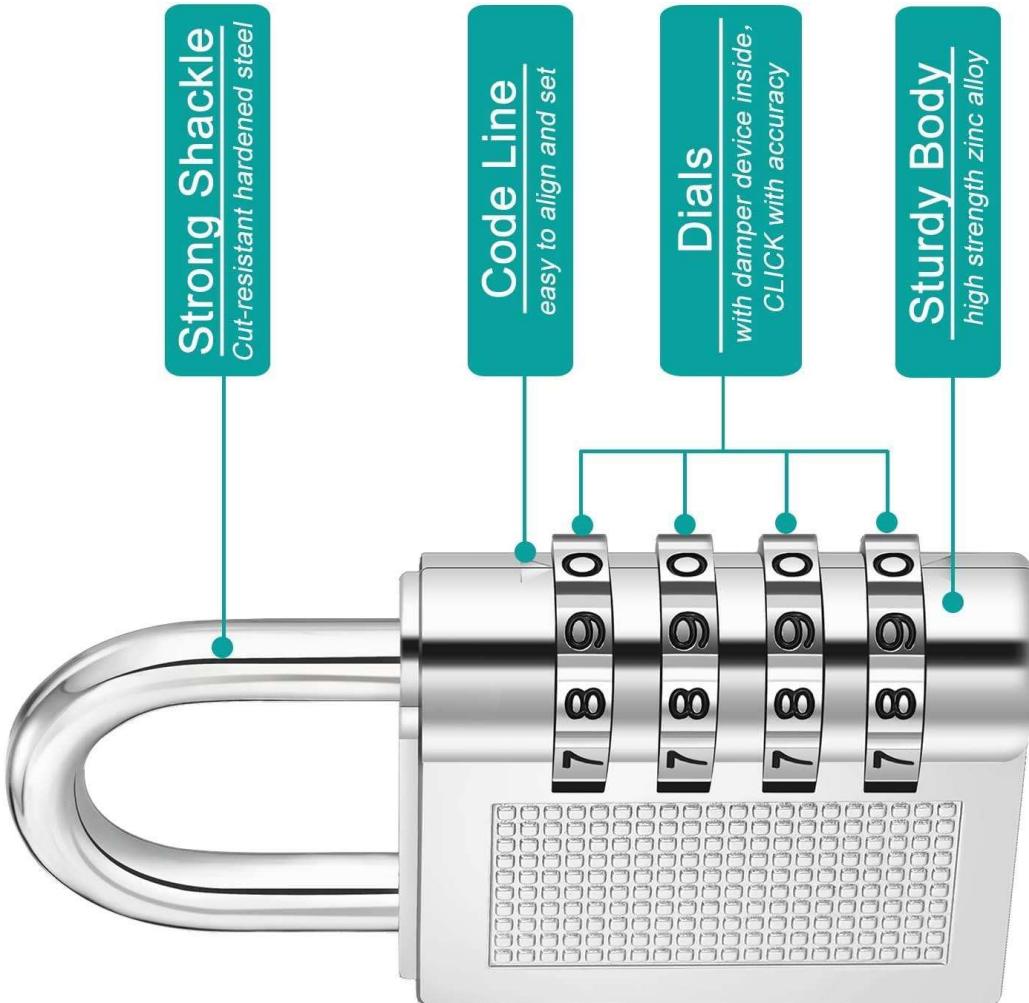
Brico-Picking

- Lo mismo que existen formas de crear ganzúas con objetos cotidianos, se pueden hacer Padlock Shims utilizando latas de refrescos, cuanto más finas mejor.



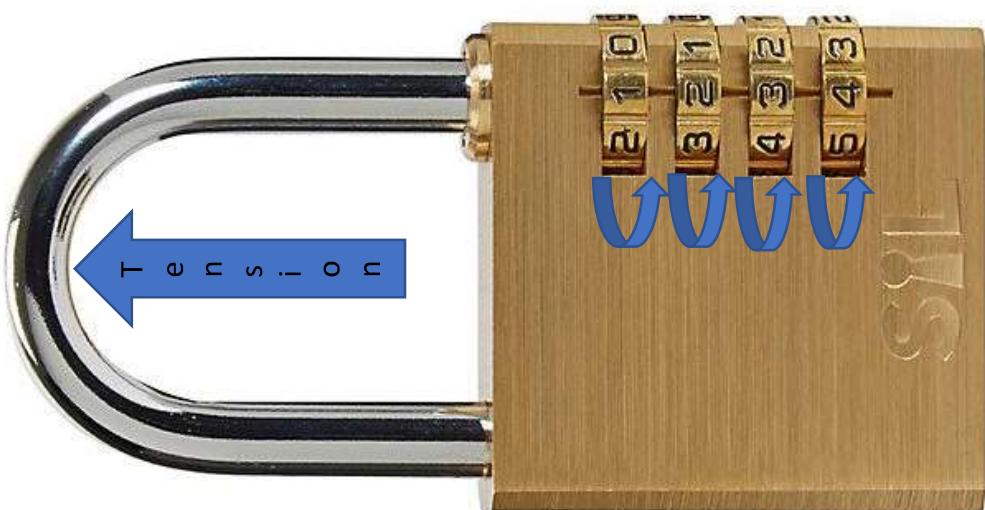
Candados de Combinacion

- Son candados que contienen diales numéricos o alfanuméricos en los que en vez de llave se dispone de una clave preconfigurable para su apertura.
- Internamente tienen una serie de discos que permiten que el mecanismo se libere en cuanto se pone la clave que se ha determinado para abrirlo.



Técnica 5: Apertura Manual

- El procedimiento es sencillo. Pondremos a 0 los diales del candado y tiraremos del arco de cierre hacia arriba generando tensión como si del tensor se tratase.
- Giramos los diales un poco hacia delante y hacia atrás buscando el que más tensión genera y comenzamos por ese.
- Iremos girando los diales poco a poco notando como giran en cada número hasta notar uno en el que el sonido o el tacto es diferente y si, se nota bastante además.
- Según vayamos avanzando se nota como se va liberando el arco cada vez más hasta liberarse del todo.



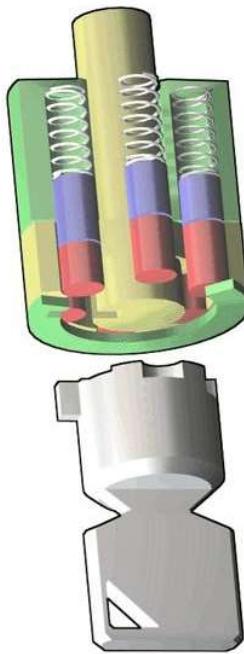
Herramientas

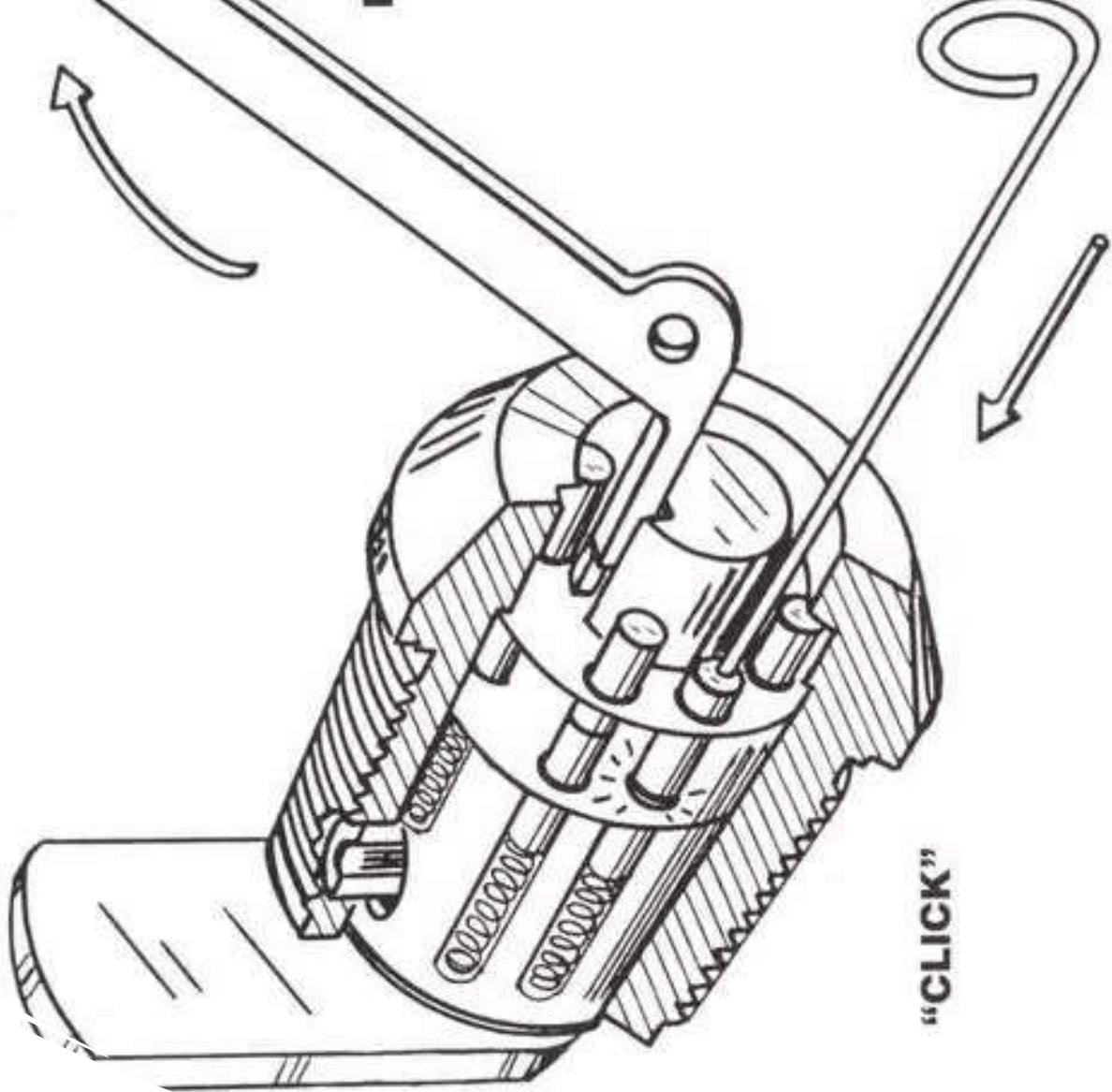


- Son ganzúas específicas para este tipo de cerraduras, que disponen de diferente número de agujas según la cantidad de pines de que disponga la cerradura.
- Y en algunos casos difiere el diámetro de la cerradura/ganzúa.

Cerraduras tubulares

- Las cerraduras tubulares son muy parecidas a las que hemos visto, se trata de cerraduras que tienen una forma tubular como su propio nombre indica.
- Típicas en buzones por ejemplo y que cuya llave suele ser una forma cilíndrica con una lengüeta pequeña.





Técnica 6: Apertura tubular pin a pin

- En este caso funcionaremos con una herramienta de tensión y por otro lado con una herramienta con la que ir empujando los pines y viendo cuales "piden" y cuáles no.
 - "PEDIR" quiere decir cuando se nota resistencia en un pin concreto. Los que "no piden" se notan totalmente sueltos. Al aplicar suficiente tensión sobre los pines que piden se nota un ligero CLICK que lo libera pudiendo pasar al siguiente.
- Como dato a tener en cuenta, las cerraduras de este tipo tienden a necesitar más de un ganezudo ya que tienen varias posiciones, por lo que las herramientas de tensión suelen quedar atrapadas hasta acabar el recorrido o volver a la posición original.

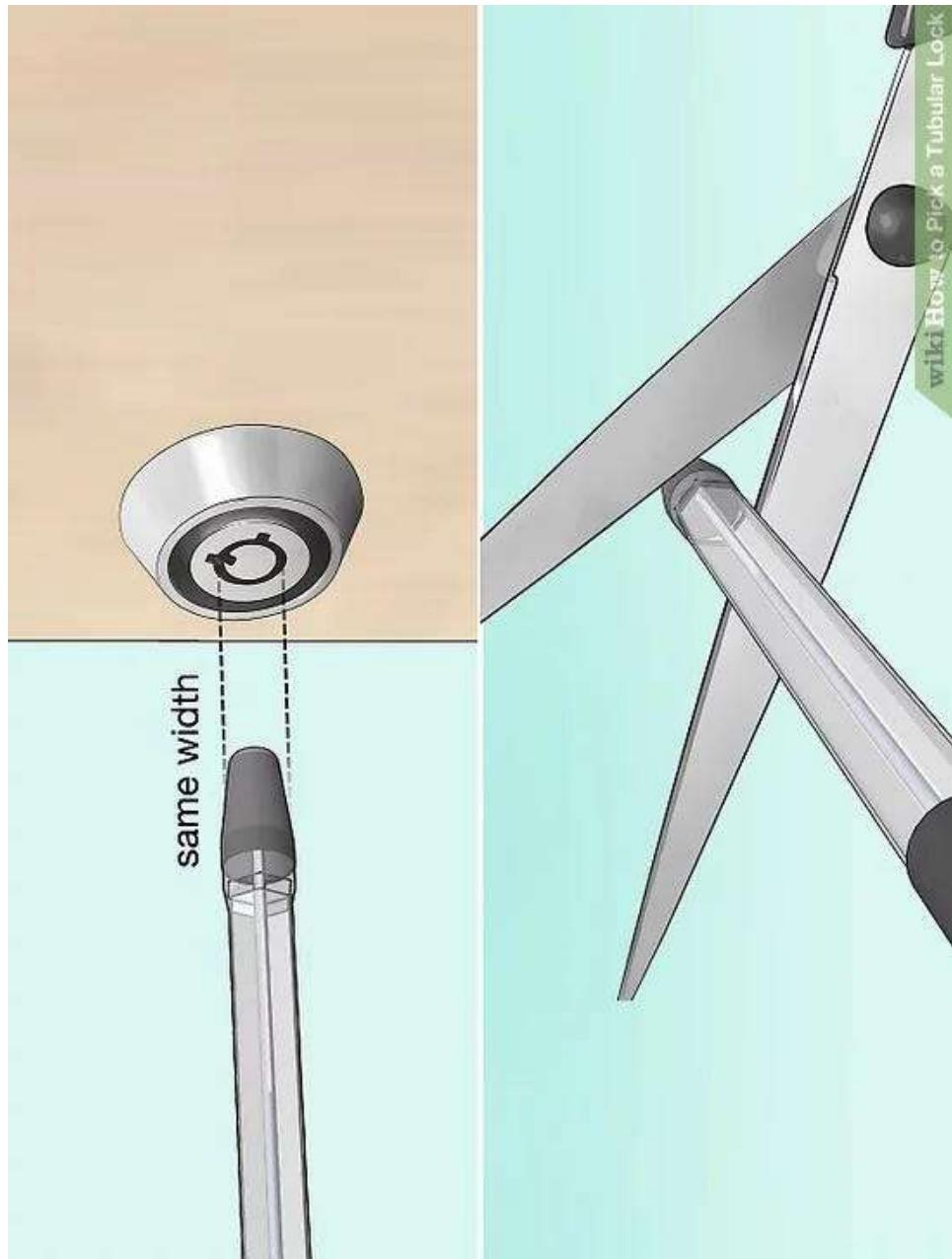
Técnica 7 : Herramienta tubular

- En este caso existen herramientas específicas para esta tarea no siendo necesario utilizar una herramienta pin a pin para ello.
- Esta herramienta simula una llave con tantas agujas como pines tenga la cerradura y permite ir ajustando cada pin hasta que permita la apertura de las cerradura



Brico – Picking

- Todo lo visto hasta el momento requiere de herramientas específicas para la apertura de cerraduras tubulares. Pero teniendo un boli cerca del mismo diámetro que la cerradura, podríamos llegar a usarlo como ganzúa para su apertura.



Cerradura de Discos

- Existen cerraduras en las que no existen pinos, sino que tienen una sucesión de discos apilados que cuando llegan a una configuración determinada abren el mecanismo.

- Estas cerraduras son las llamadas Disk Detainer Lock o cerraduras de discos.



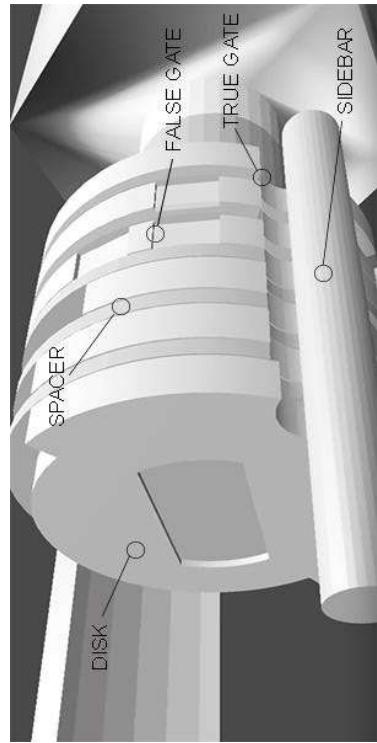
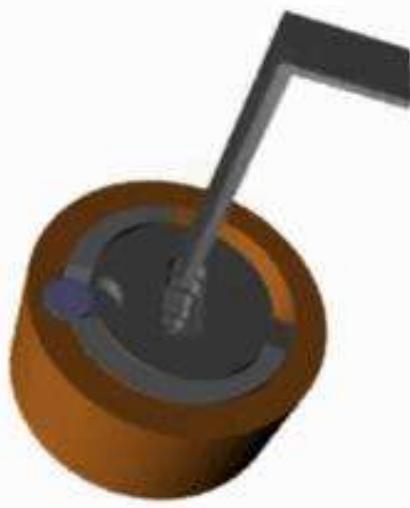
Herramientas

- Existen herramientas específicas para este tipo de cerraduras que van variando altura y el giro para poder configurar los discos y facilitar la apertura.



Técnica 8 : Apertura discos

- Se introduce la punta de la herramienta en la oquedad del cerrojo (no penséis mal ¡PUERKOS!).
- Lentamente se va bajando y girando los discos hasta encontrar la posición en la que el mecanismo queda totalmente liberado.
- Para que quede totalmente liberado hay que hacer que el cilindro interior caiga sobre las aperturas que tienen los discos y no sobre las "false gates".



Puertas de emergencia

- Las puertas de emergencia suelen ser un sitio poco vigilado y por normativa tienen que estar operativas. Esto implica que solo pueden ser abiertas con un mecanismo sencillo desde la parte interior del edificio. Pero y si no fuese así?



Herramientas



- Por un lado vamos a necesitar una PRY-Bar que no es más que una palanca pequeña con la que hacer fuerza y separar la puerta un poco del marco permitiendo que podamos introducir algo para liberar el mecanismo de apertura.

- Plancha de plástico



- También puede usarse una herramienta que consiste en un cojín de aire y una perilla que sirven para hacer presión entre el marco y la puerta para desestabilizarla y así poder colar un gancho y abrir el mecanismo.

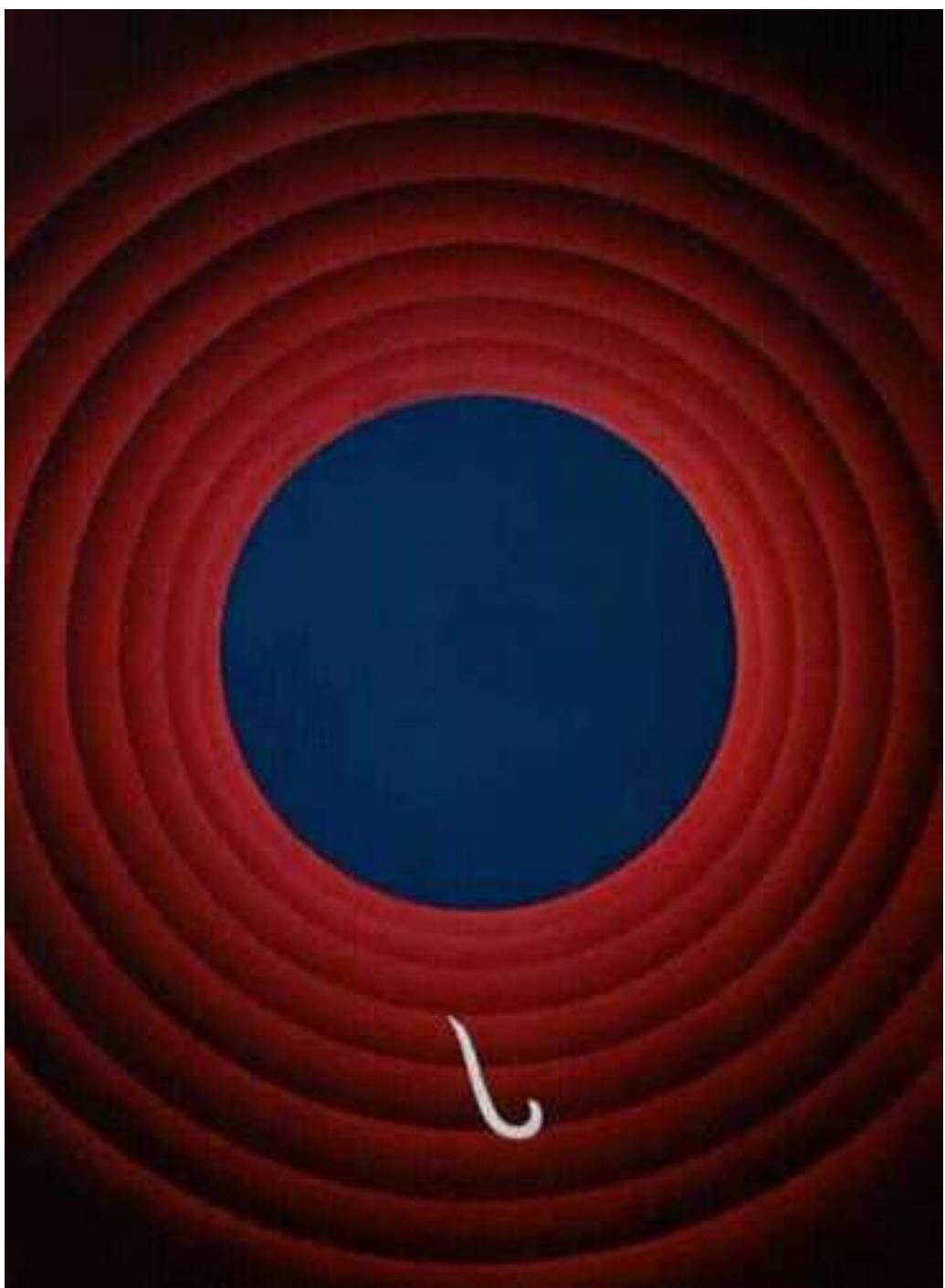
Técnica 9 – Apertura encubierta

Introducimos la Prybar a través del marco de la puerta, normalmente tienen una lengüeta para evitar que se abran desde fuera. Hacemos fuerza para separar la lengüeta del marco y así abrir un pequeño hueco.

A través de la rendija abierta se introduce la placa plástica y se pasa haciendo una cuña desde dentro hacia fuera para liberar el mecanismo de apertura.

Rezamos para que su apertura no tenga unida a una alarma que avise de nuestra fechoría.





Bibliografía y referencias

- Bibliografía
 - Visual Lockpicking Guide : 3rd Edition
 - LockCowboy [1](#) [2](#) [3](#)
 - [MIT Guide to lockpicking](#)
- Referencias
 - Canal de Lockpicking Lawyer: <https://www.youtube.com/@lockpickinglawyer>
 - Canal de Tallan Lockpick: <https://www.youtube.com/@TallanPick>
 - Canal de Lock Noob: <https://www.youtube.com/@LockNoob>
 - Canal de Red Cells Hacking: <https://www.youtube.com/@redcellshacking>
 - Canal de Bosnian Bill: <https://www.youtube.com/@bosnianbill>