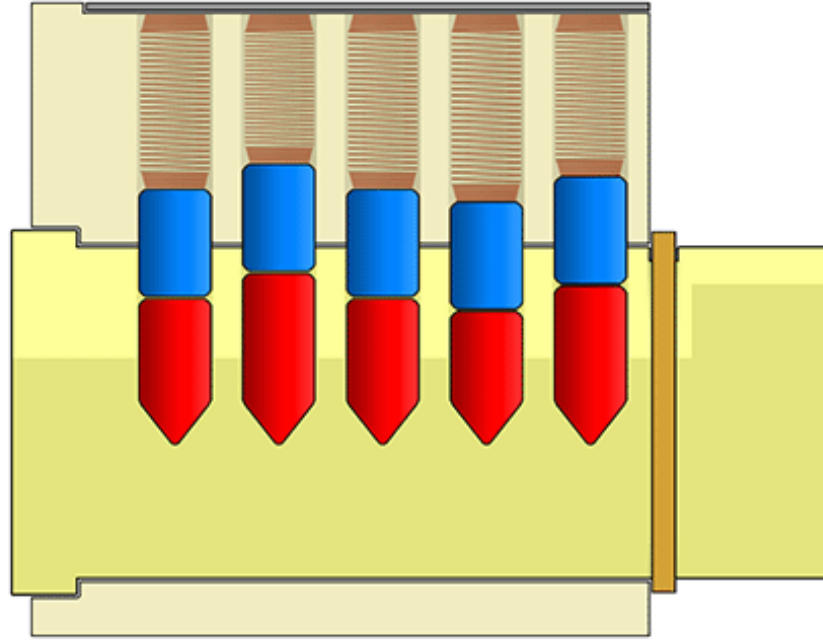


# Locks and History



Lots of slides provided by:



# Standard Humble Bragging Introduction

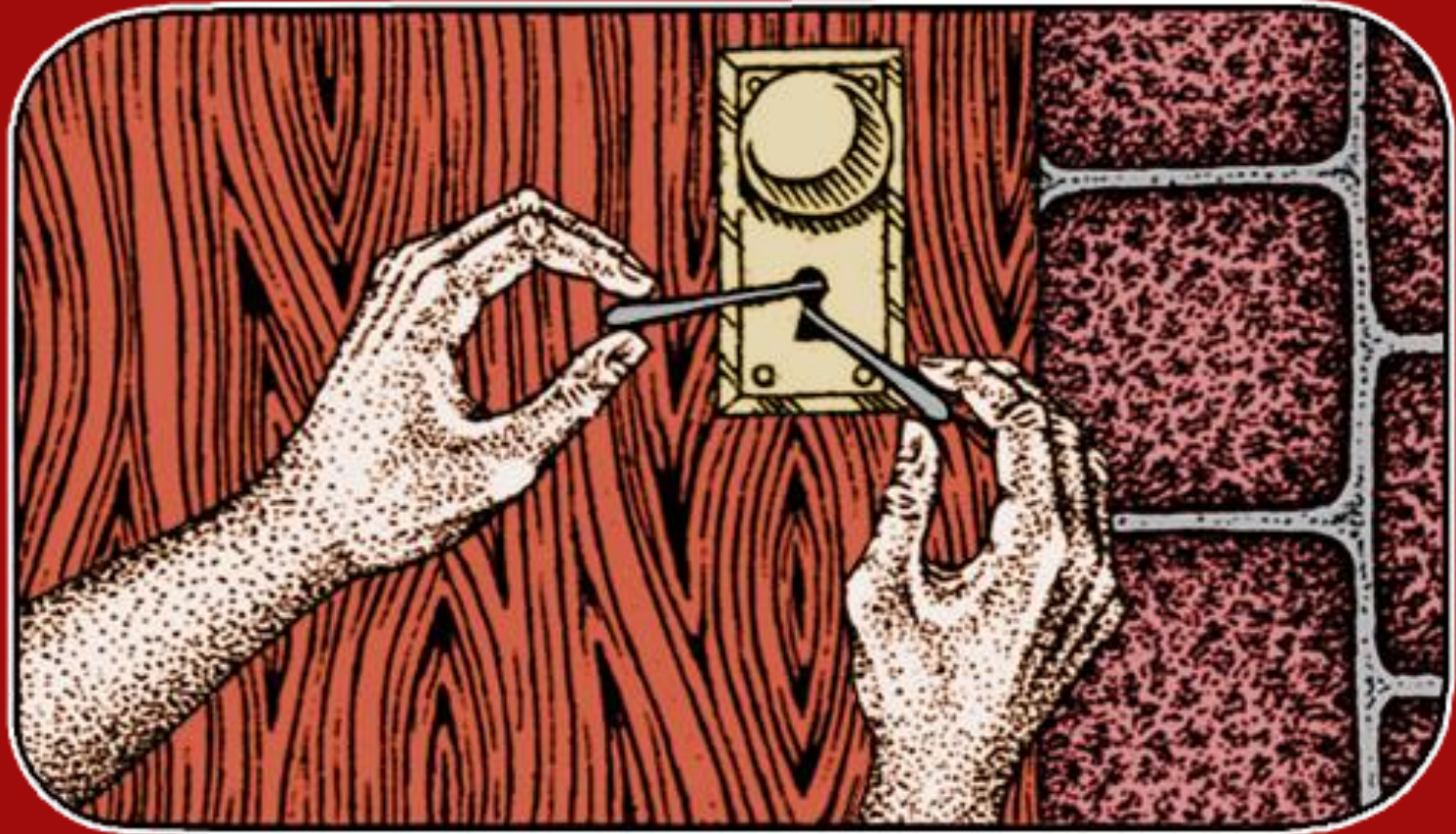
---

Email: [chris@casper.im](mailto:chris@casper.im)

Career: Army, DISA, Sikorsky, Deloitte, consulting

Why locks and lockpicking? Started off as useful skill, became a hobby.

You're teaching people how to pick locks!?



# Criminals don't pick locks

---

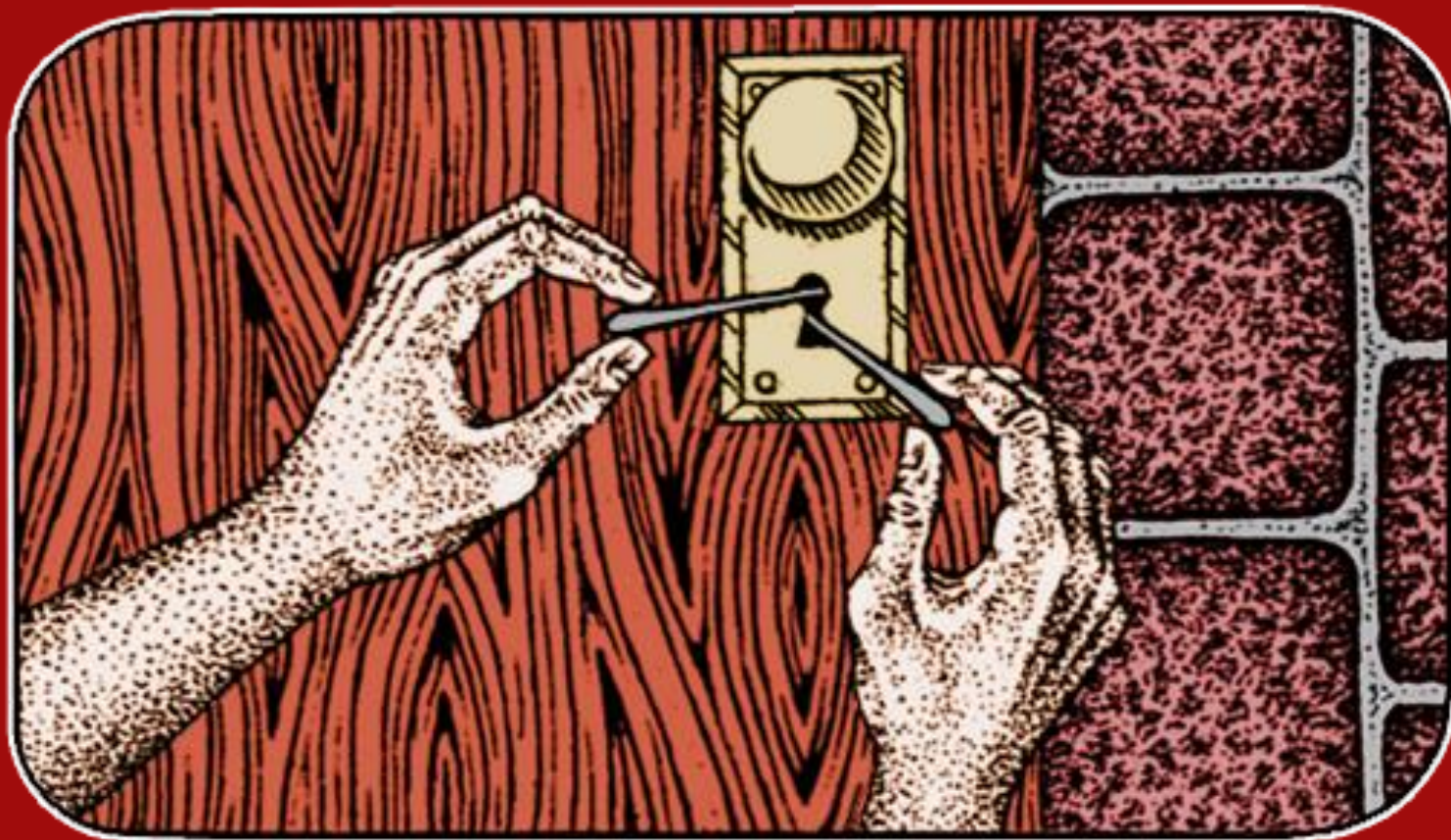
They tend to use bolt cutters, bricks or a good kick to steal things.



Or they get elected to office.



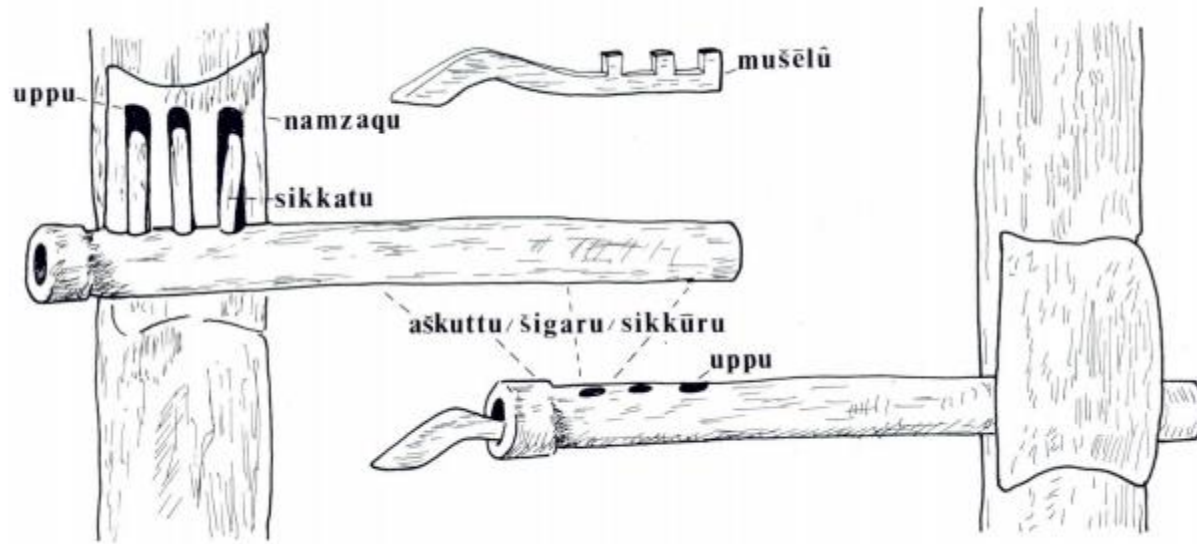
# A Brief History of Locks



# 3300 year old pin tumbler lock

---

Earliest example found in Palace of Khorsabad in Assyria, 700BC around the reign of Sargon II. All wood construction, with three tumblers.



First record of any lock was in 1300BC, listed on a Greek Linear B tablet found in Crete.

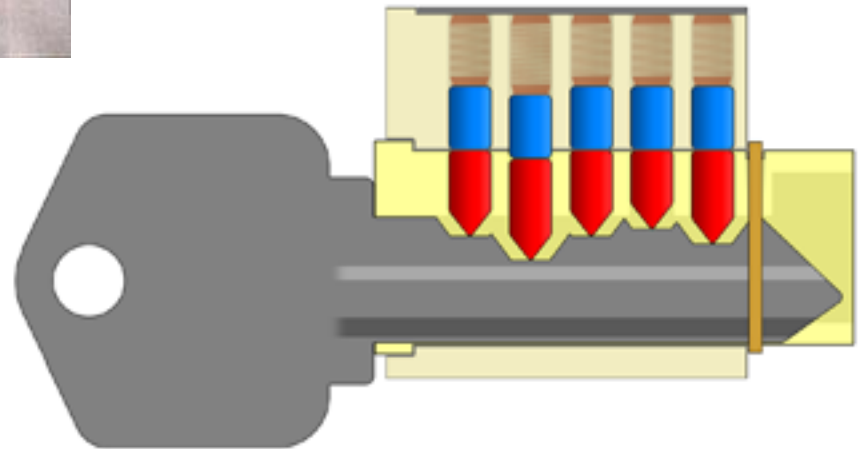
# Mind if I borrow that?

---



The Egyptians borrowed the design from the Assyrians. Greeks borrowed the design from the Egyptians. Both added minor refinements.

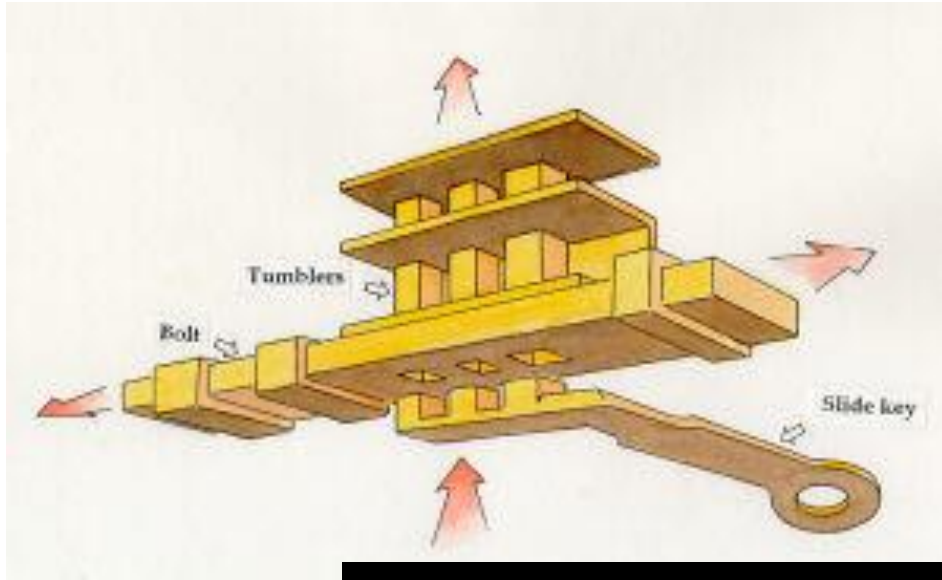
Look familiar?





# What did the Romans ever do for us?

---



# Padlocks!

---



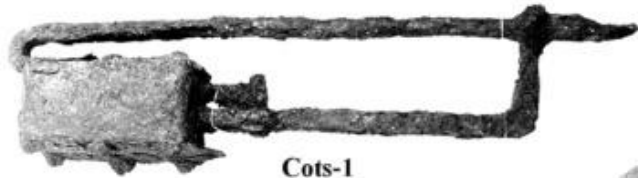
5073A



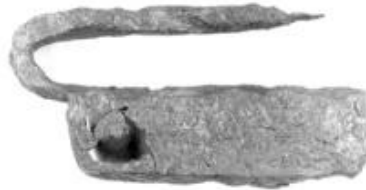
5073B



5073E



Cots-1

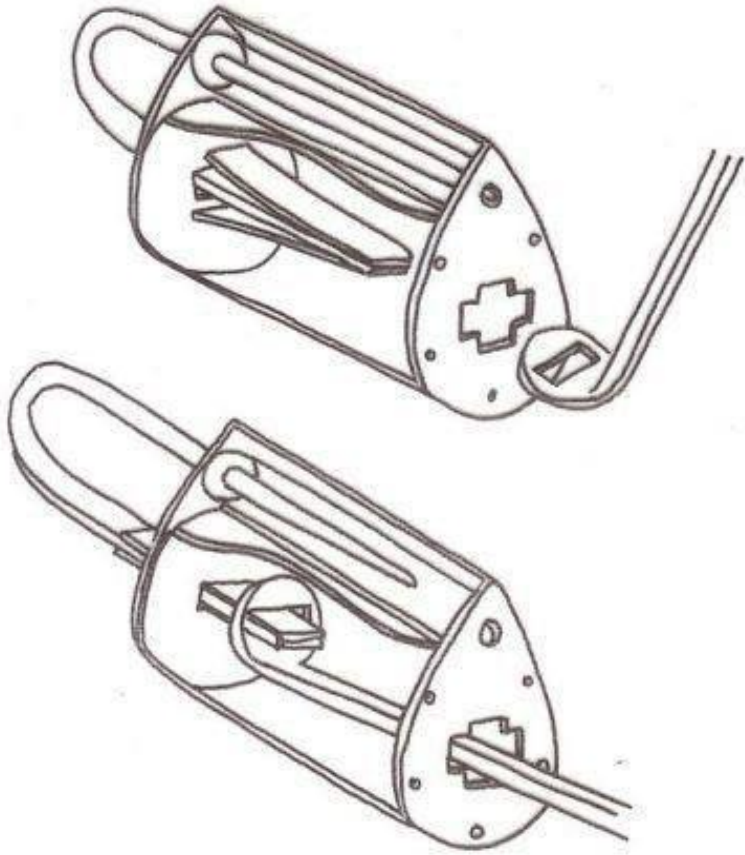


Cots-2

100 AD – 300 AD

Not long after Marcus Aurelius was  
Emperor of Rome

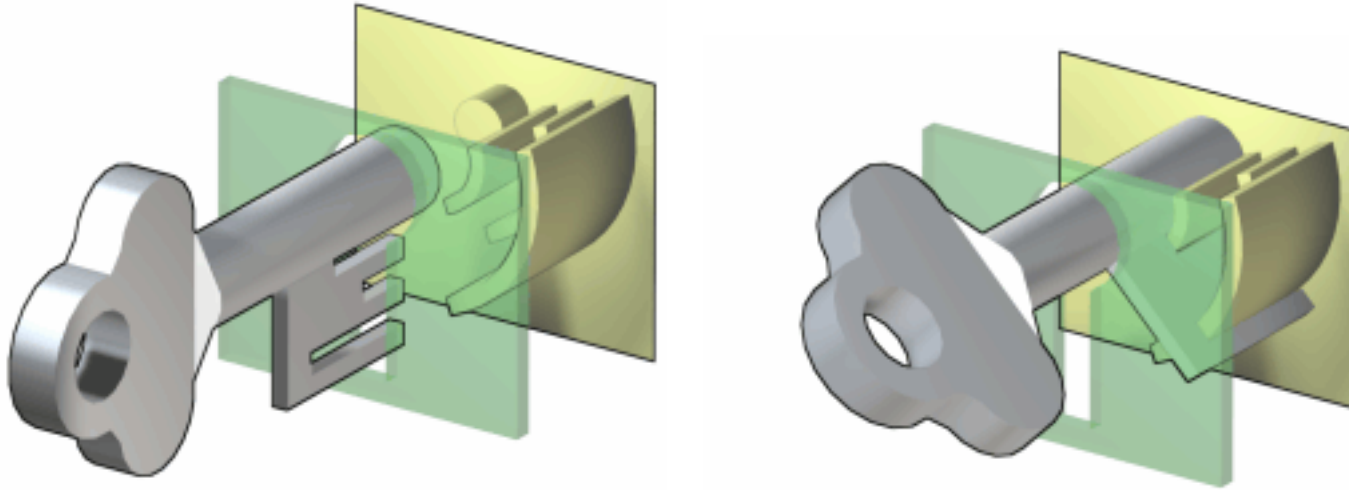
# Can't forget about the Vikings





# Ward Locks

---



How old? No one knows. Both ancient China and Rome used them.

Still used by cheap padlocks today.

# Lever Locks

---



Single lever locks used during the Roman era, but mostly operated as ward locks.

First modern lever lock - 1778 by Robert Barron of England

Just how good were these locks?

---

Well. No one knows. It was 'secret'.

But not very well.

# Toilets and High Security Locks — Dawn of a New Era

---



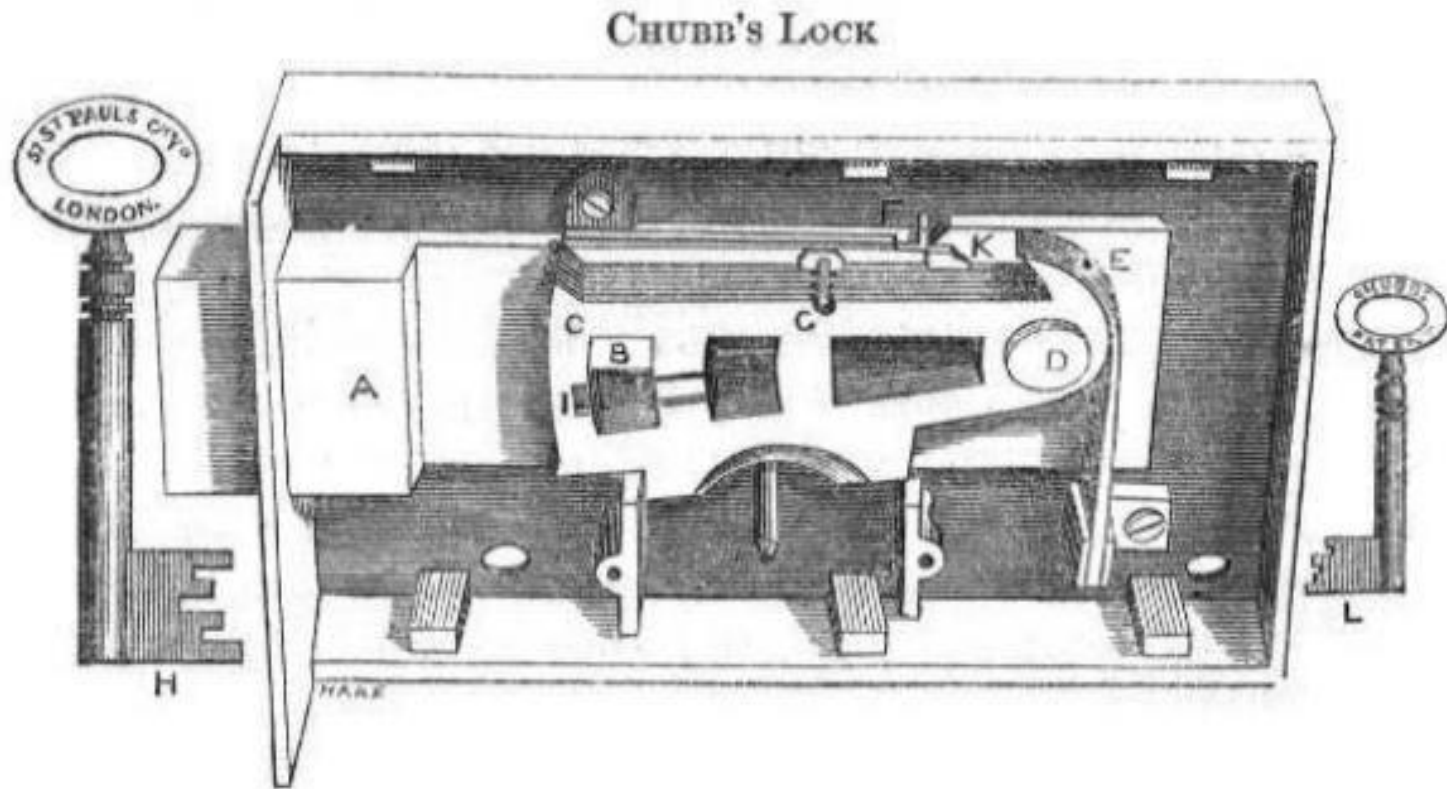
Bramah Safety Lock

Joseph Bramah, also creator of first flush toilet, created the first high security lock in 1770s.



# Rise of the Mass Production High Security Locks

---



Invented by Jeremiah Chubb of Portsmouth, England in 1818



# Alfred Charles Hobbs

---



Probably one of the first white hat hackers



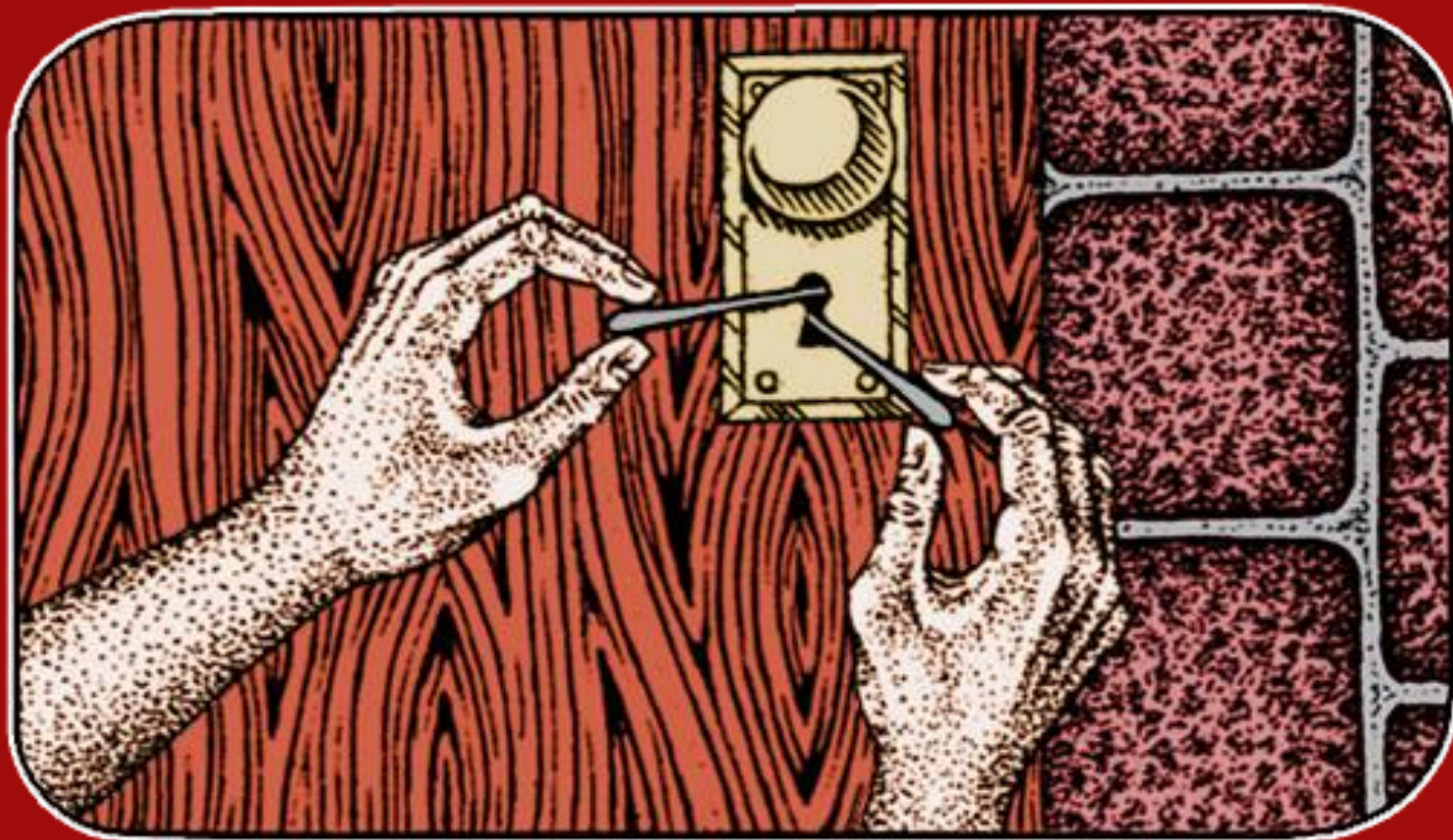
# Great Exhibition of the Works of Industry of All Nation



VIEW FROM THE ARCADE ROAD OF  
THE CRYSTAL PALACE IN HYDE PARK FOR GRAND INTERNATIONAL EXHIBITION OF 1851.  
*Dedicated to the Royal Commissioners.*

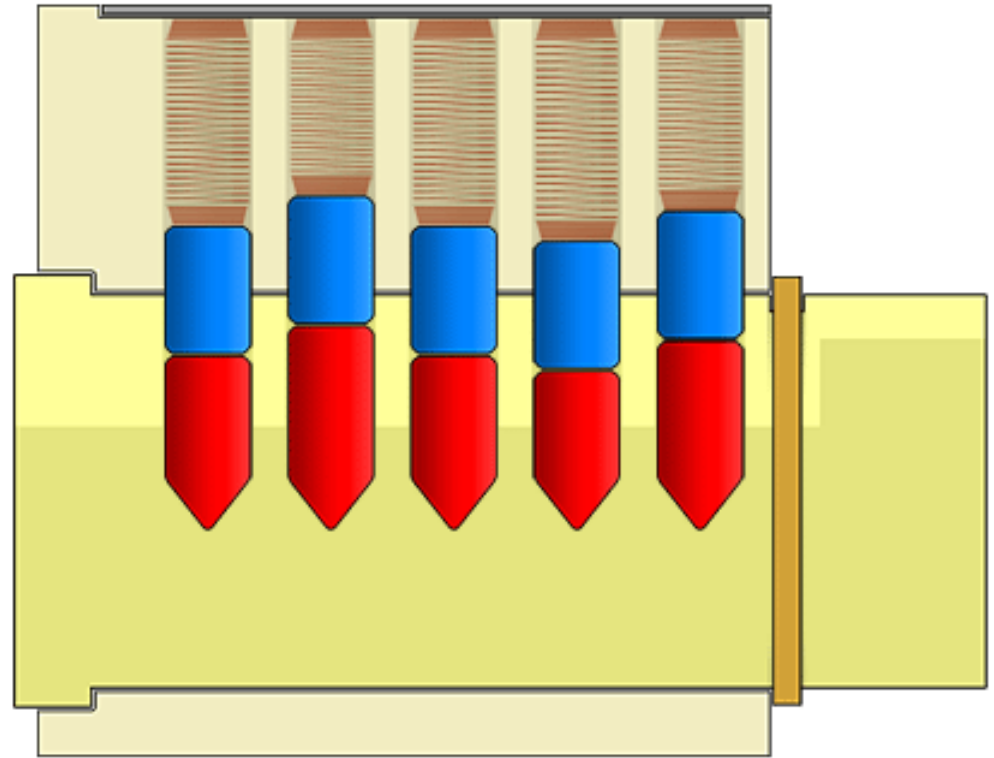


## Act 2 — Lock Picking



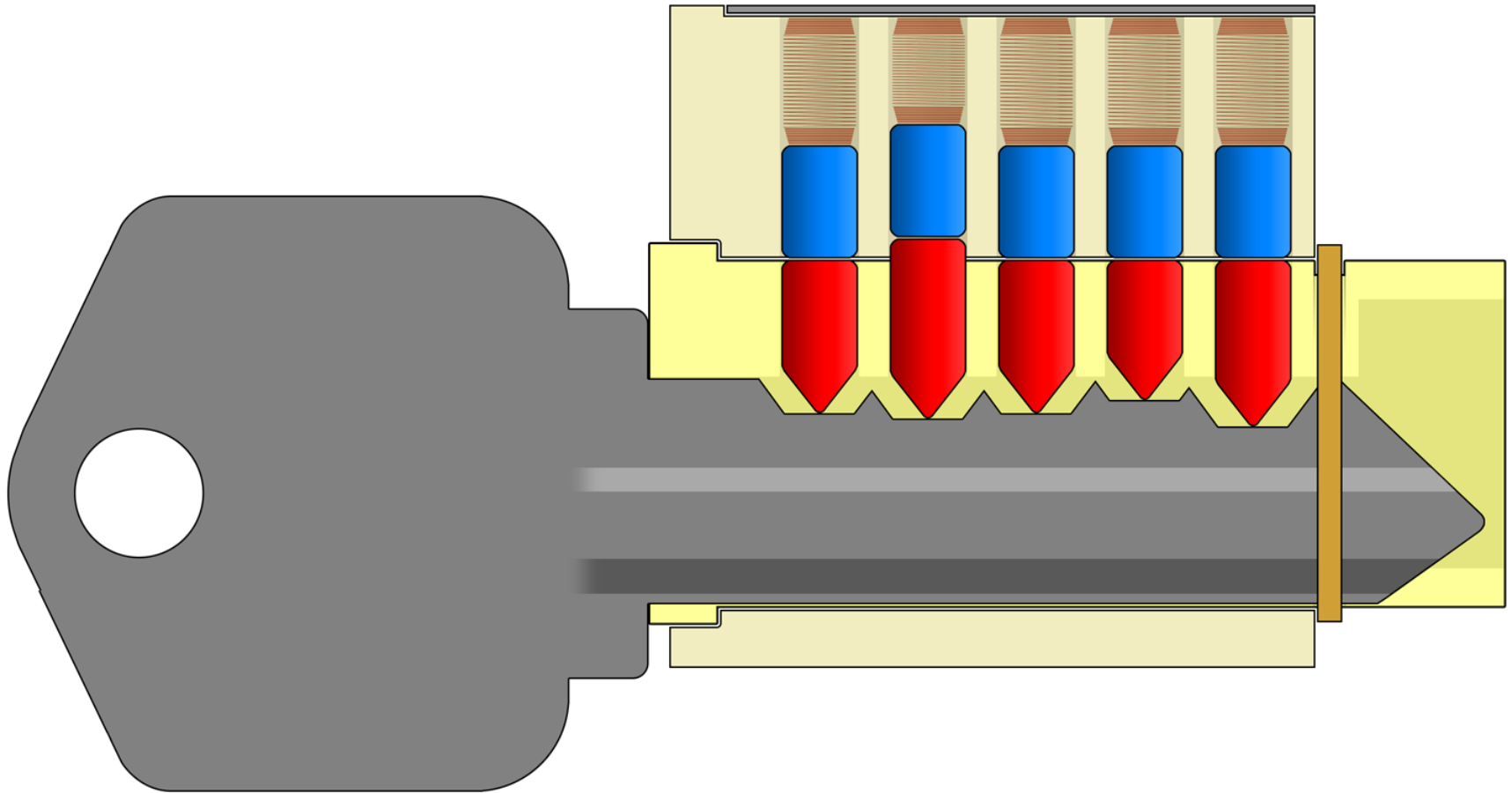
# The lock on your front door

---



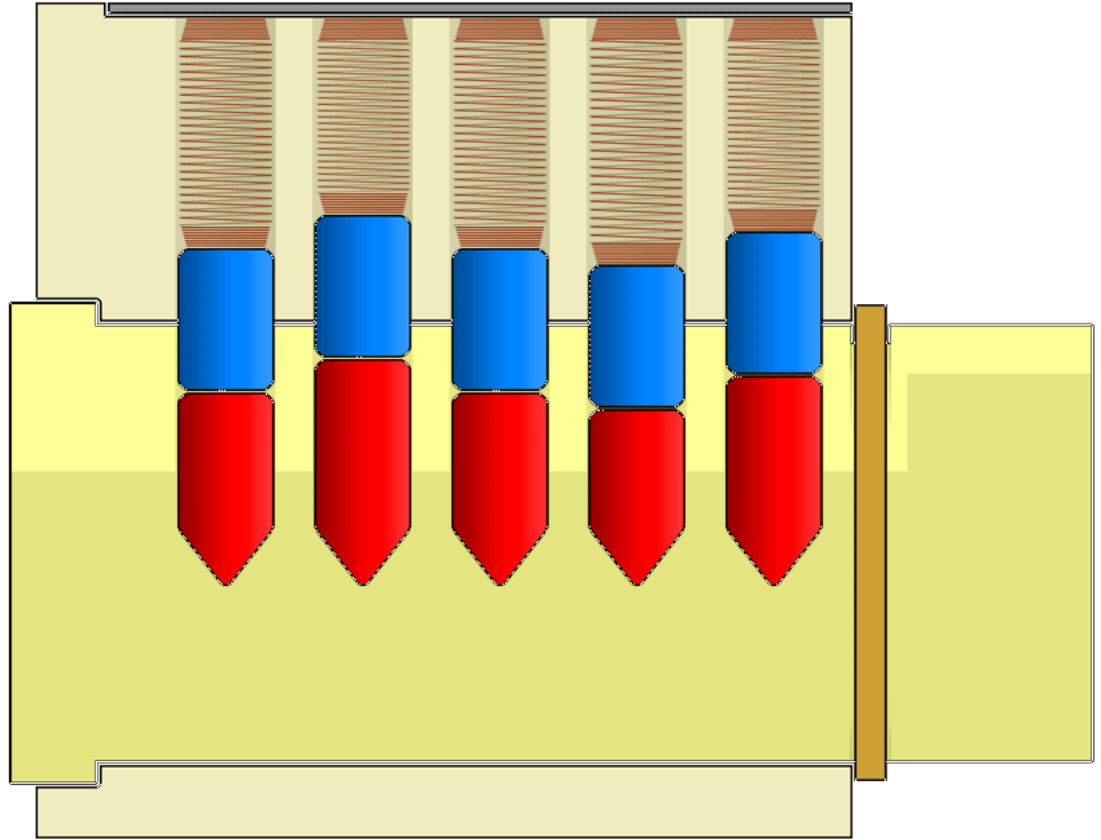
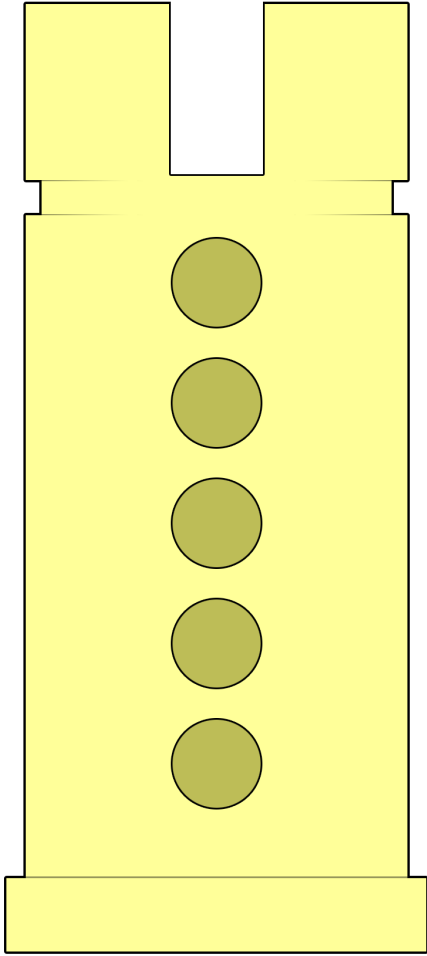
# How your front door lock opens

---



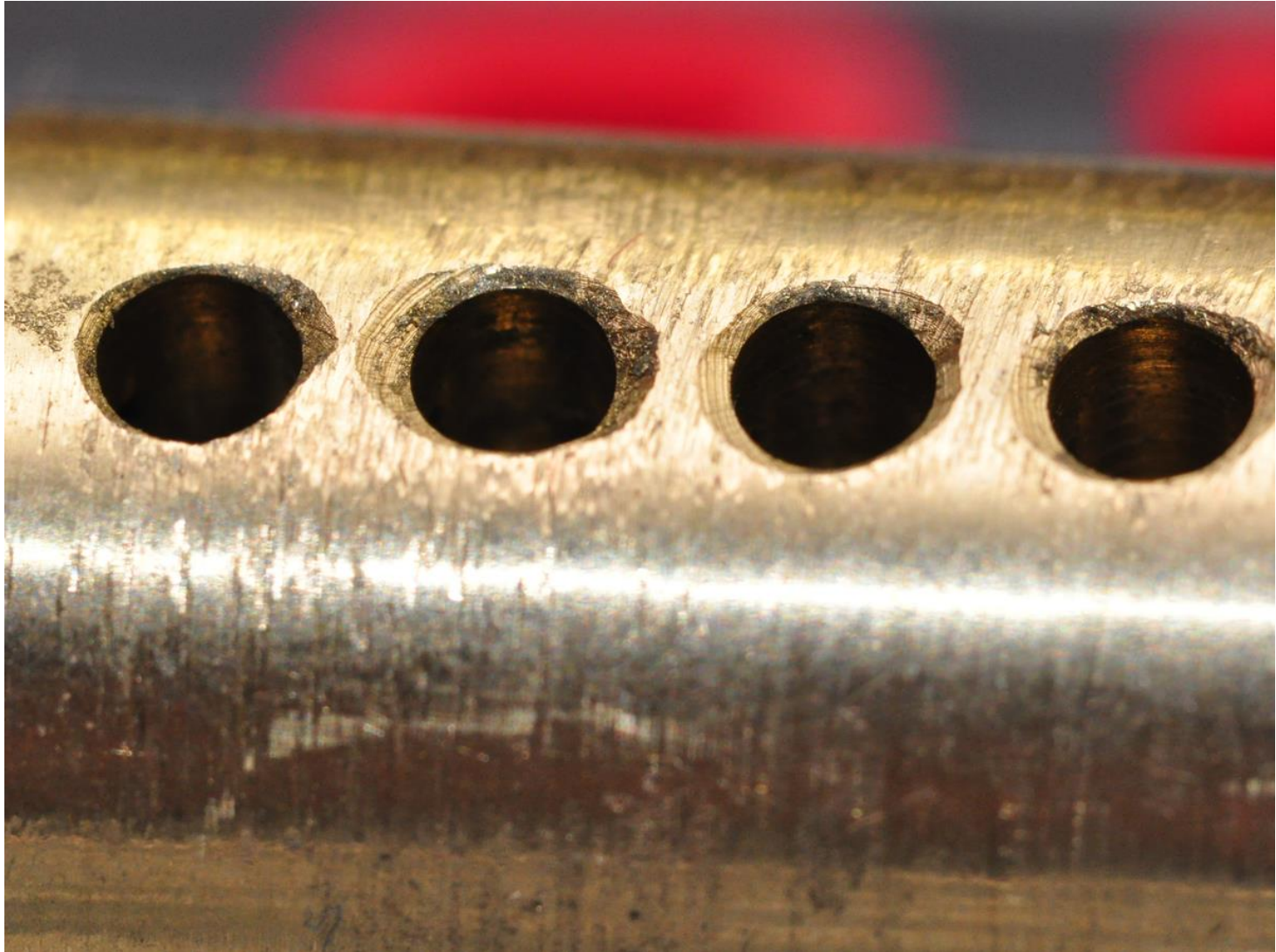
# In a Perfect World

---



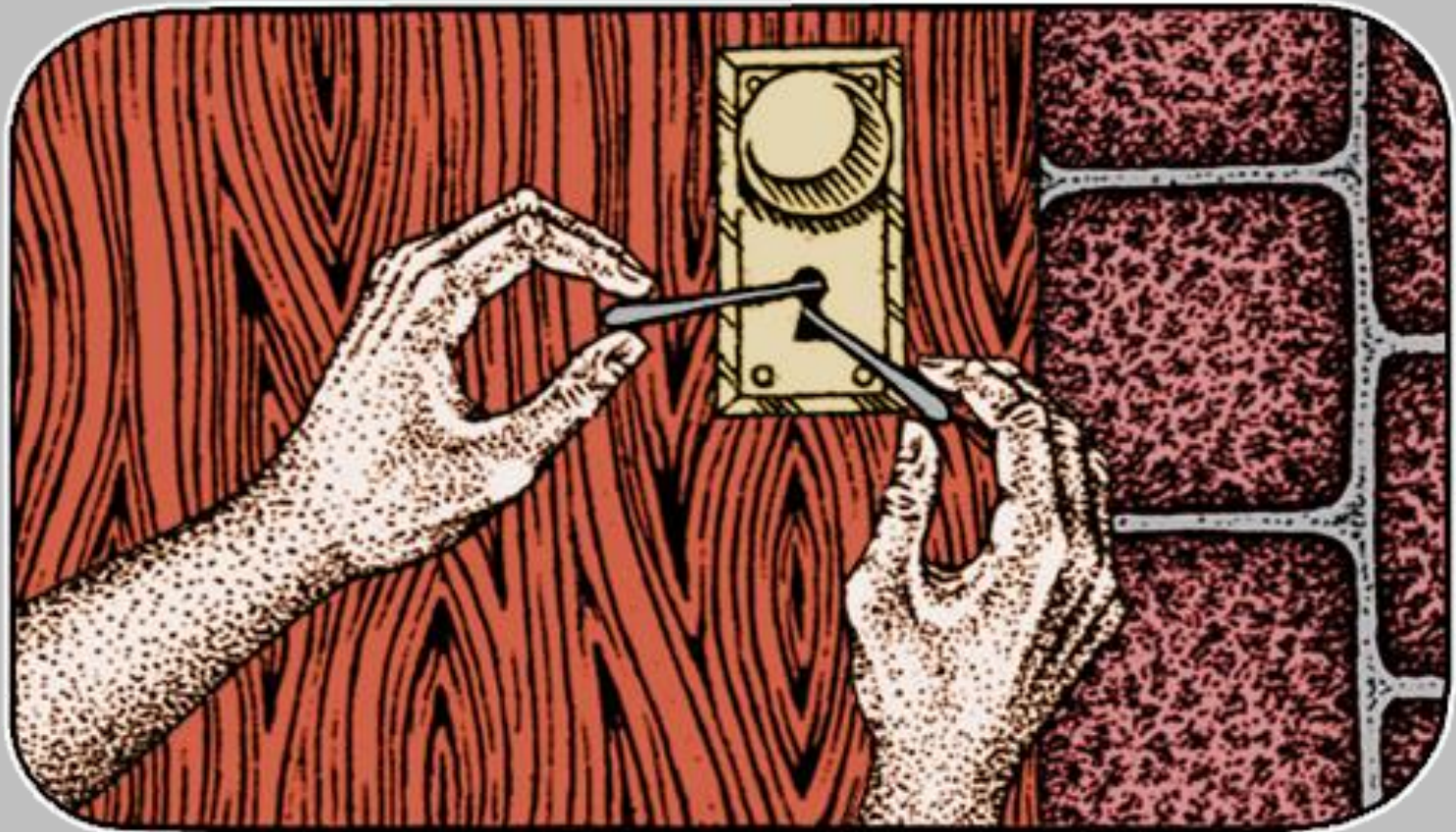
# In the Real World

---



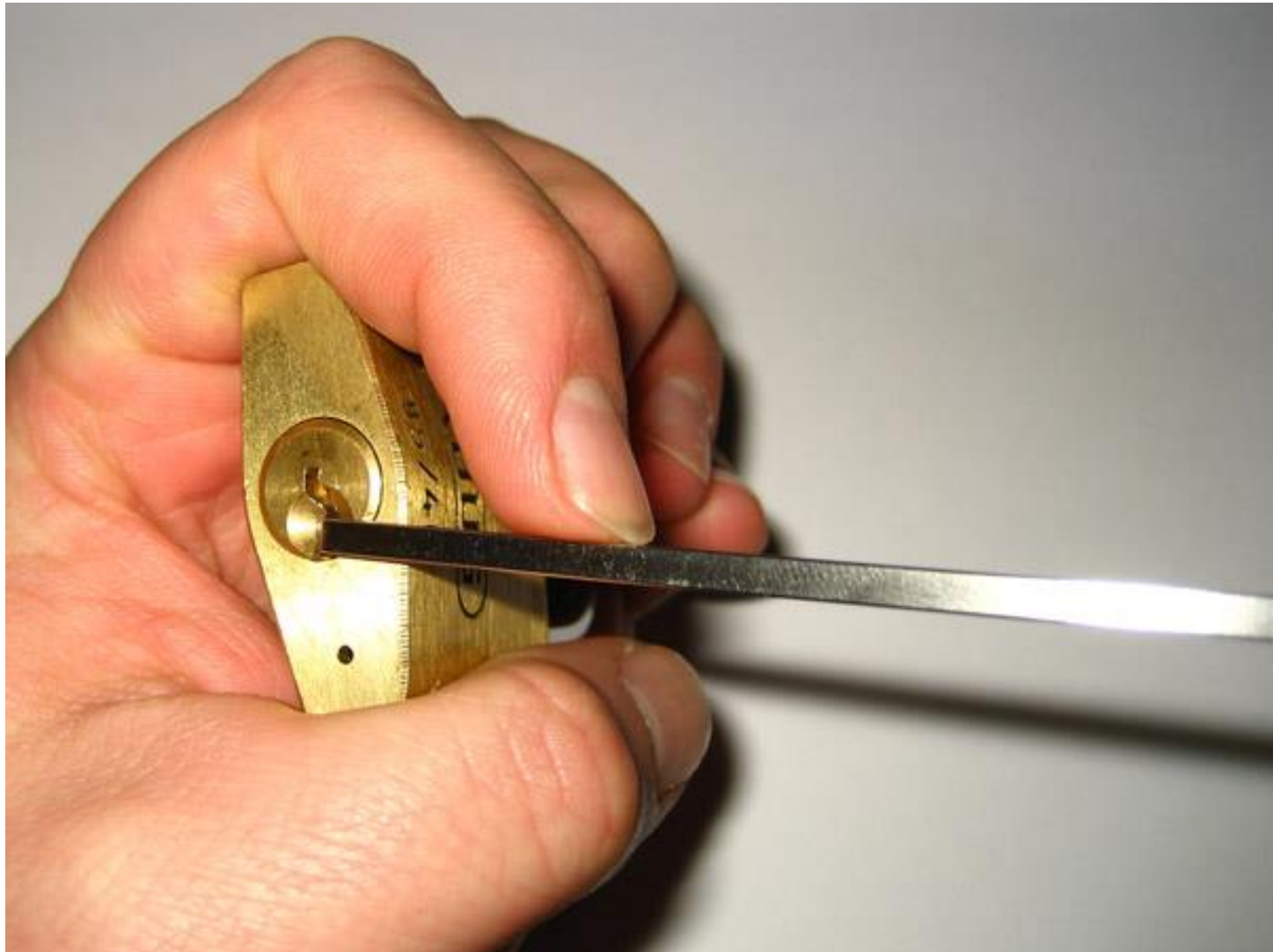


# Let's Teach You to Pick Locks



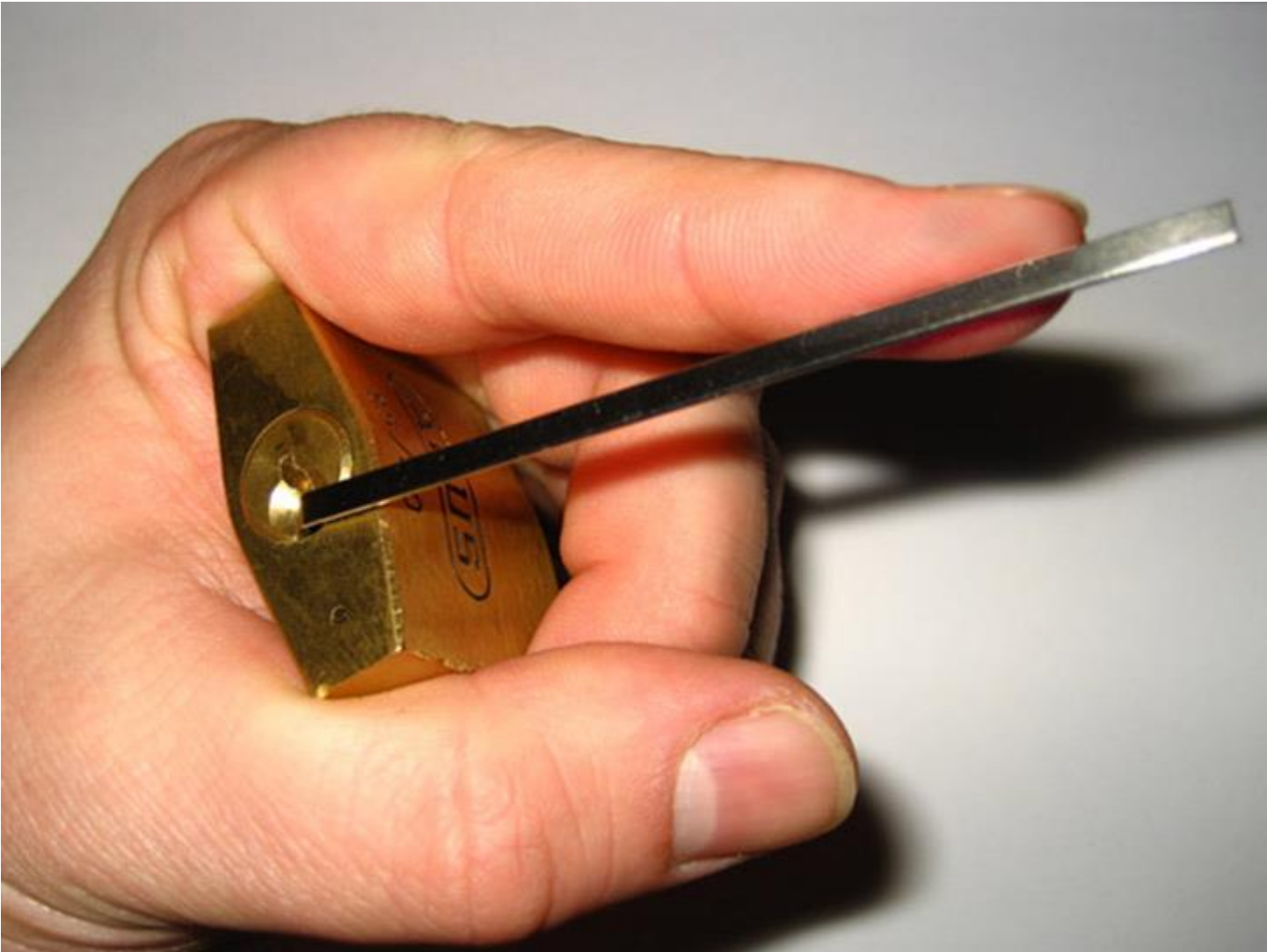
# Torsion Wrench Usage (Pushing)

---



# Best Turning Tool Usage (Pushing Out at Tip)

---





# Turning Tool Position: "Edge of the Plug"

---



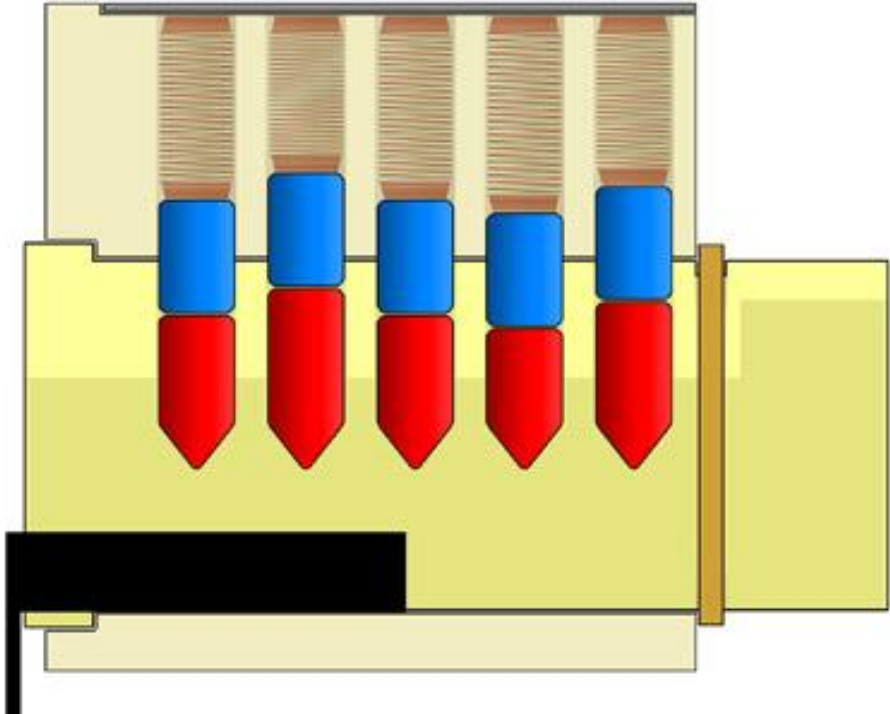
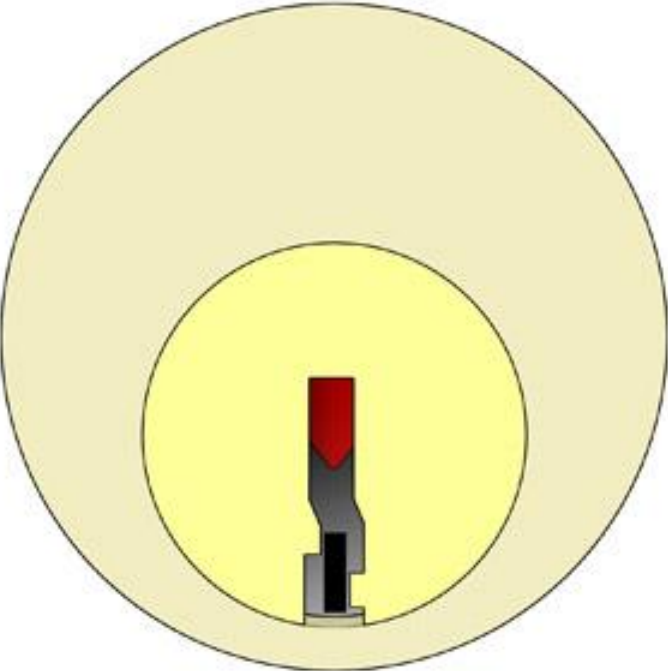
# "Standard" Turning Tools

---



# Space in the Keyway

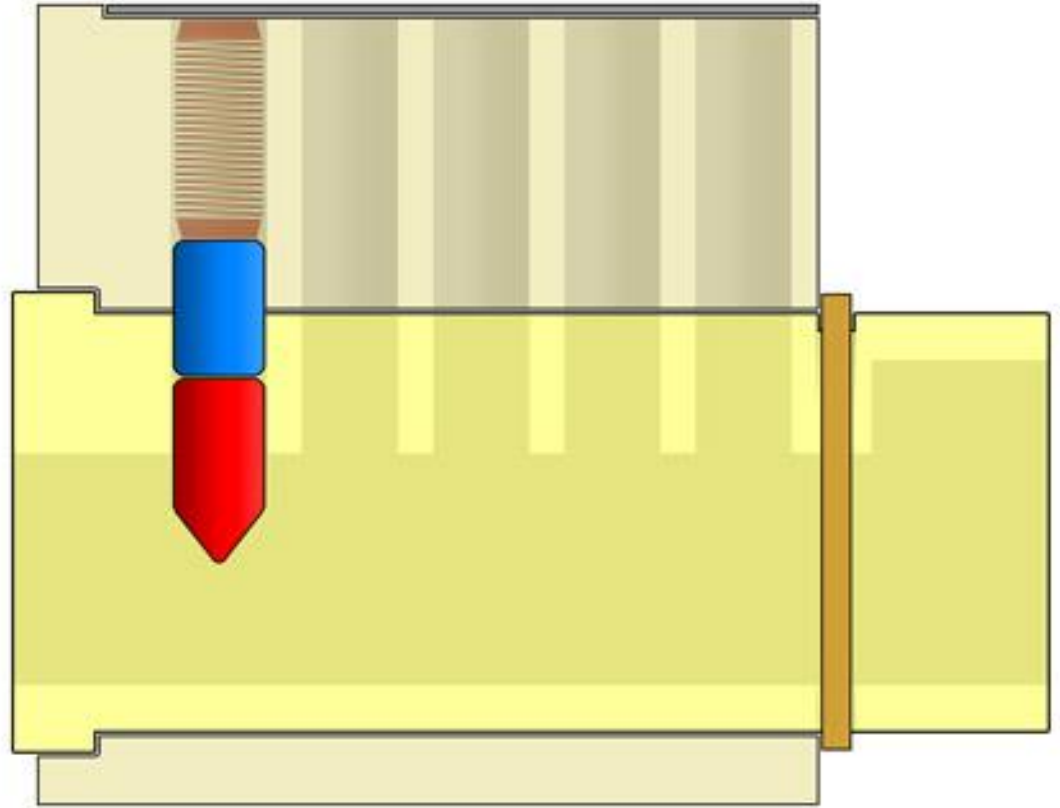
---





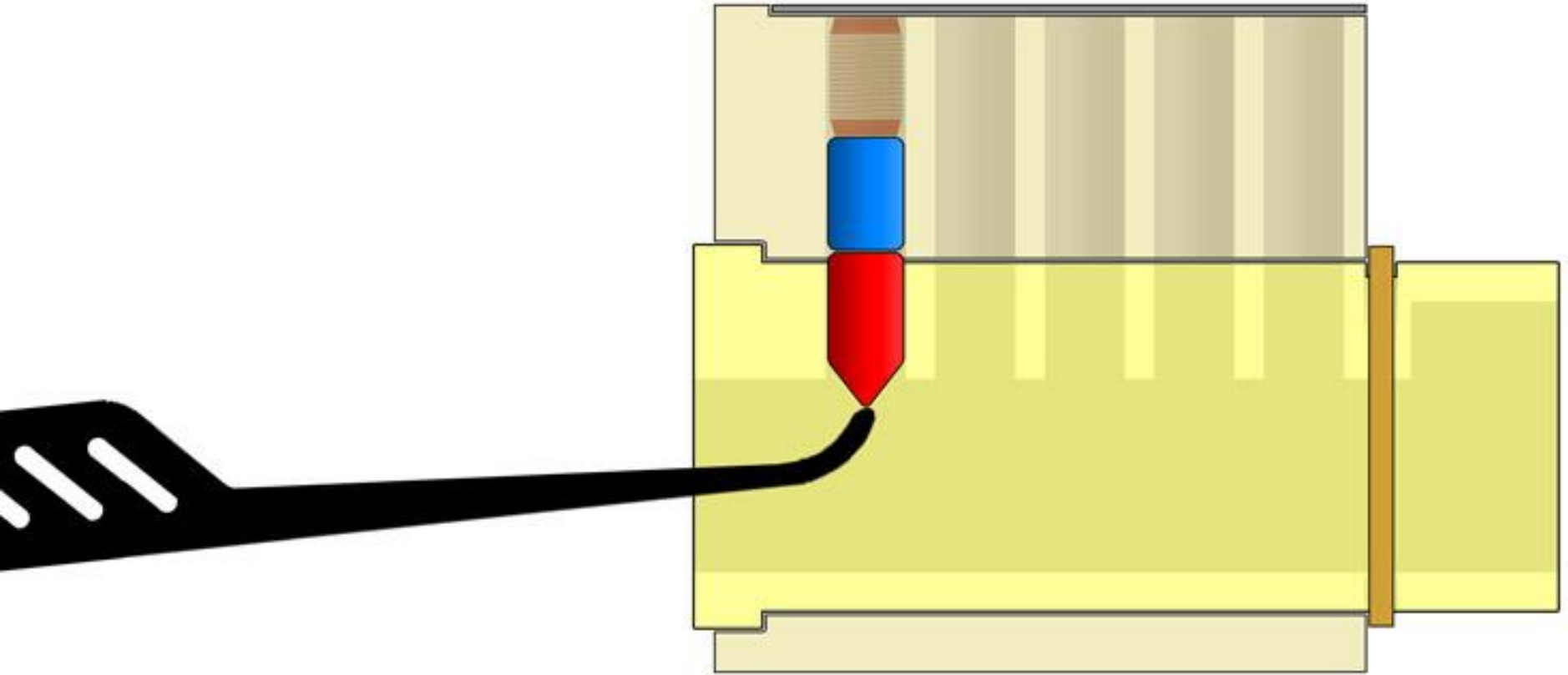
# Starter Exercises

---



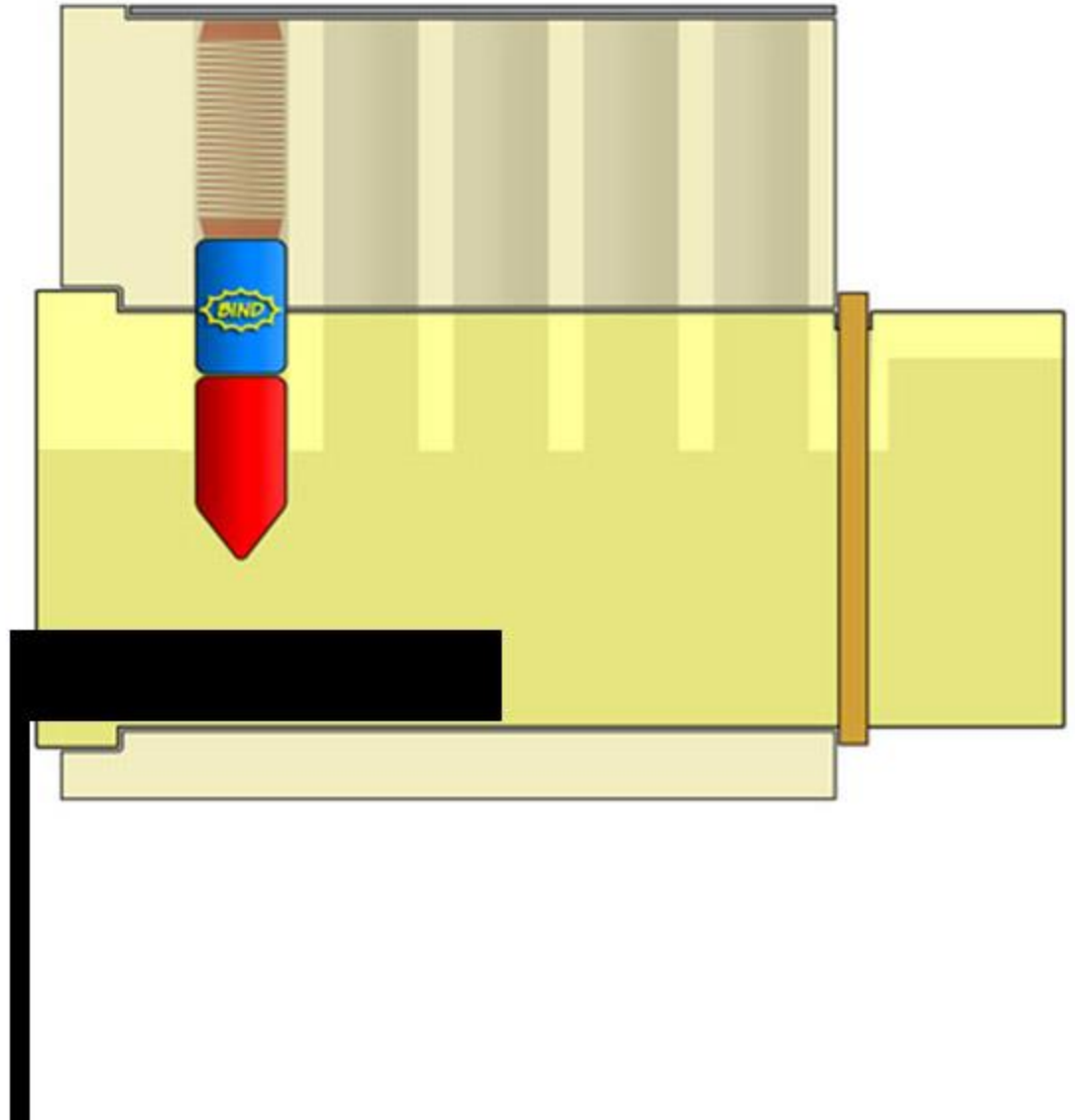
# Starter Exercises

---



# Starter Exercises

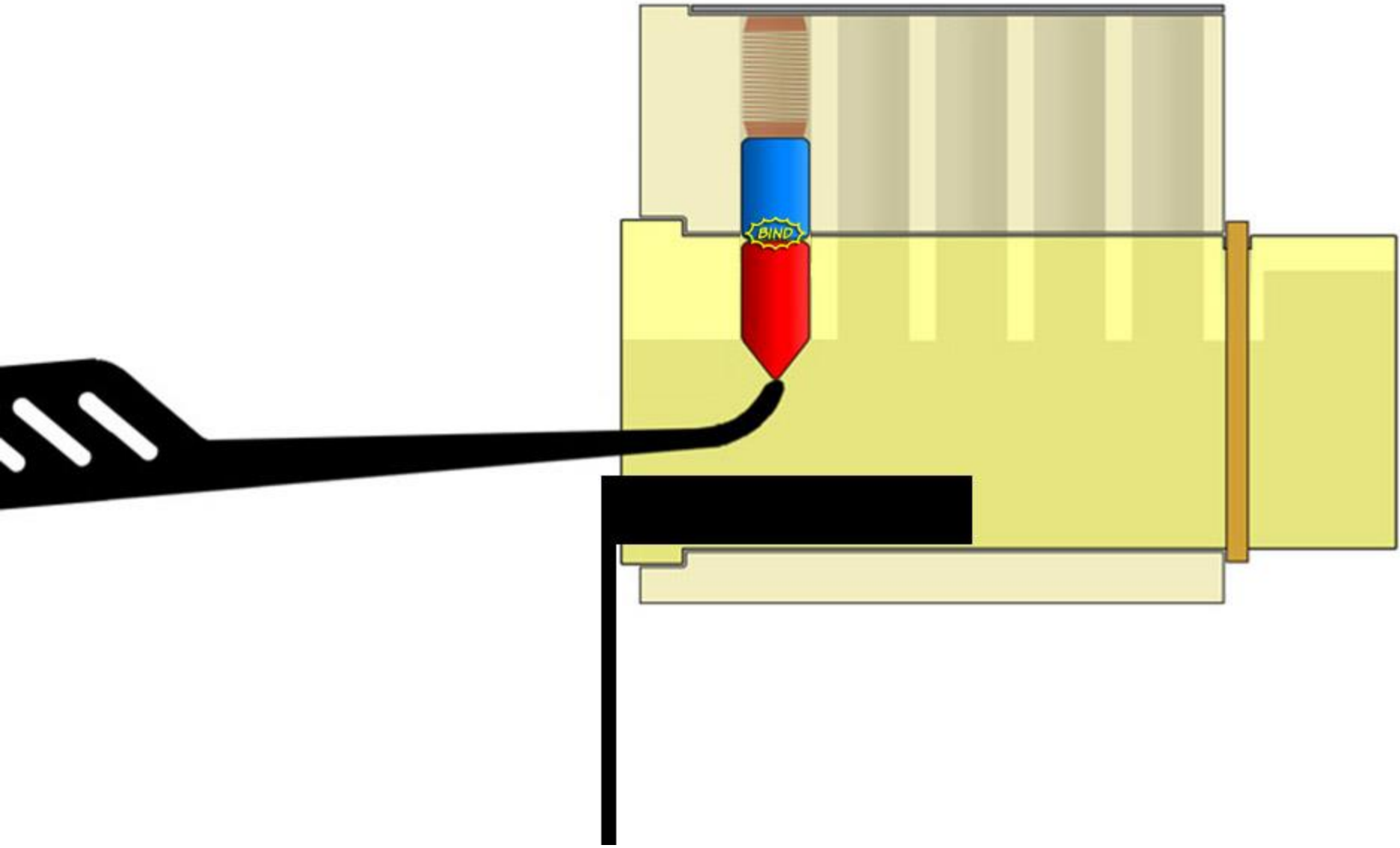
---



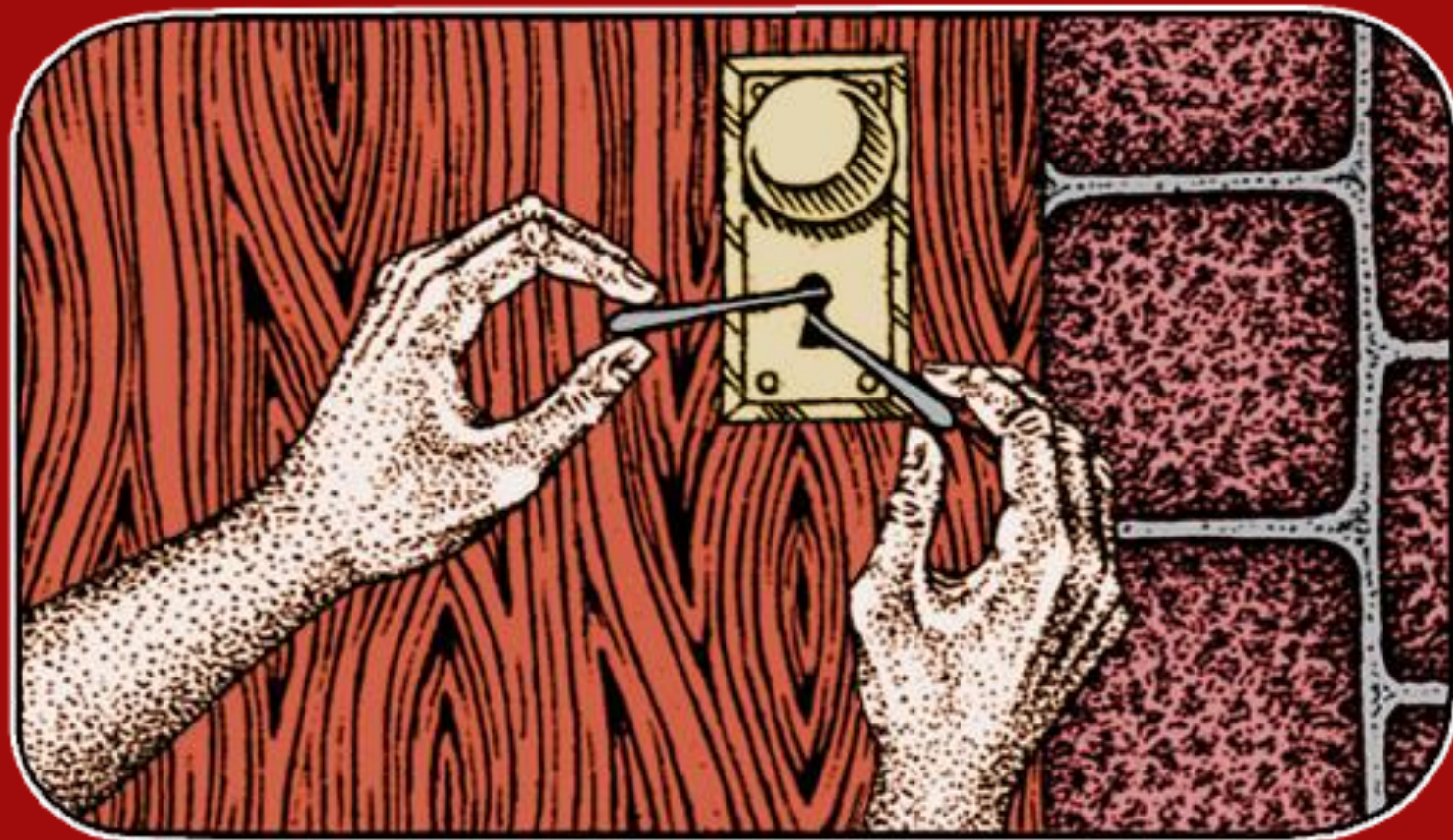


# Starter Exercises

---

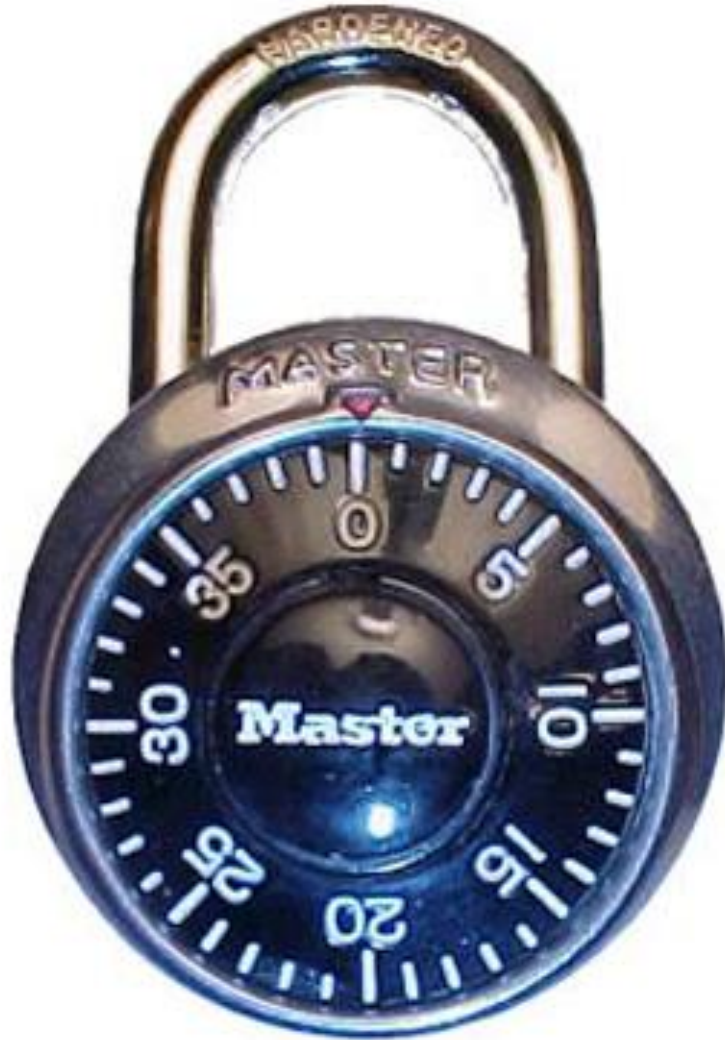


# Shimming Padlocks



# Combination Locks

---



# Padlock Shims

---





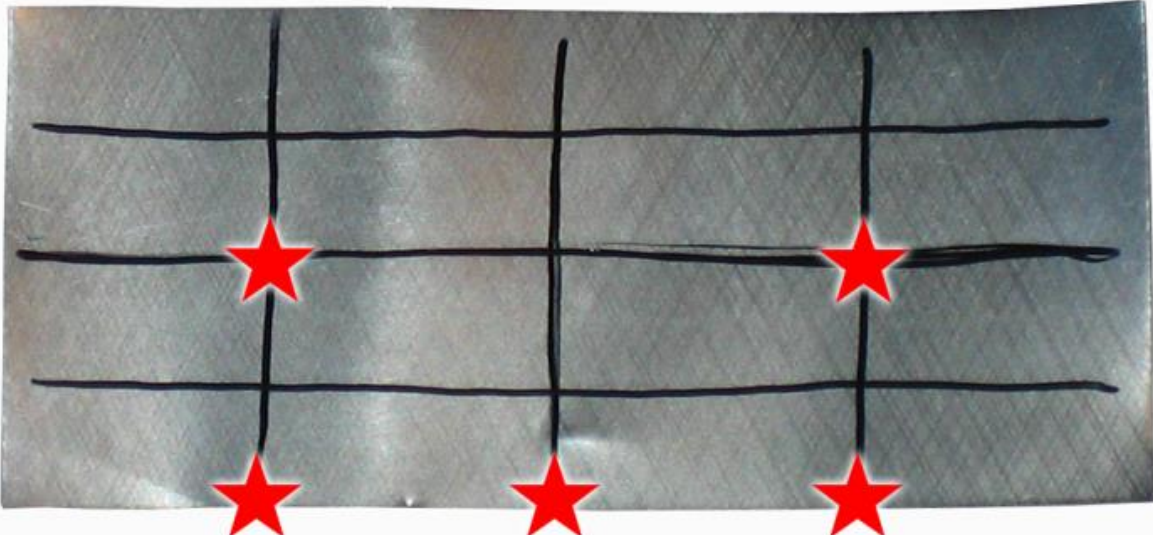
# Padlock Shims

---



# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---





# Homebrew Padlock Shims

---



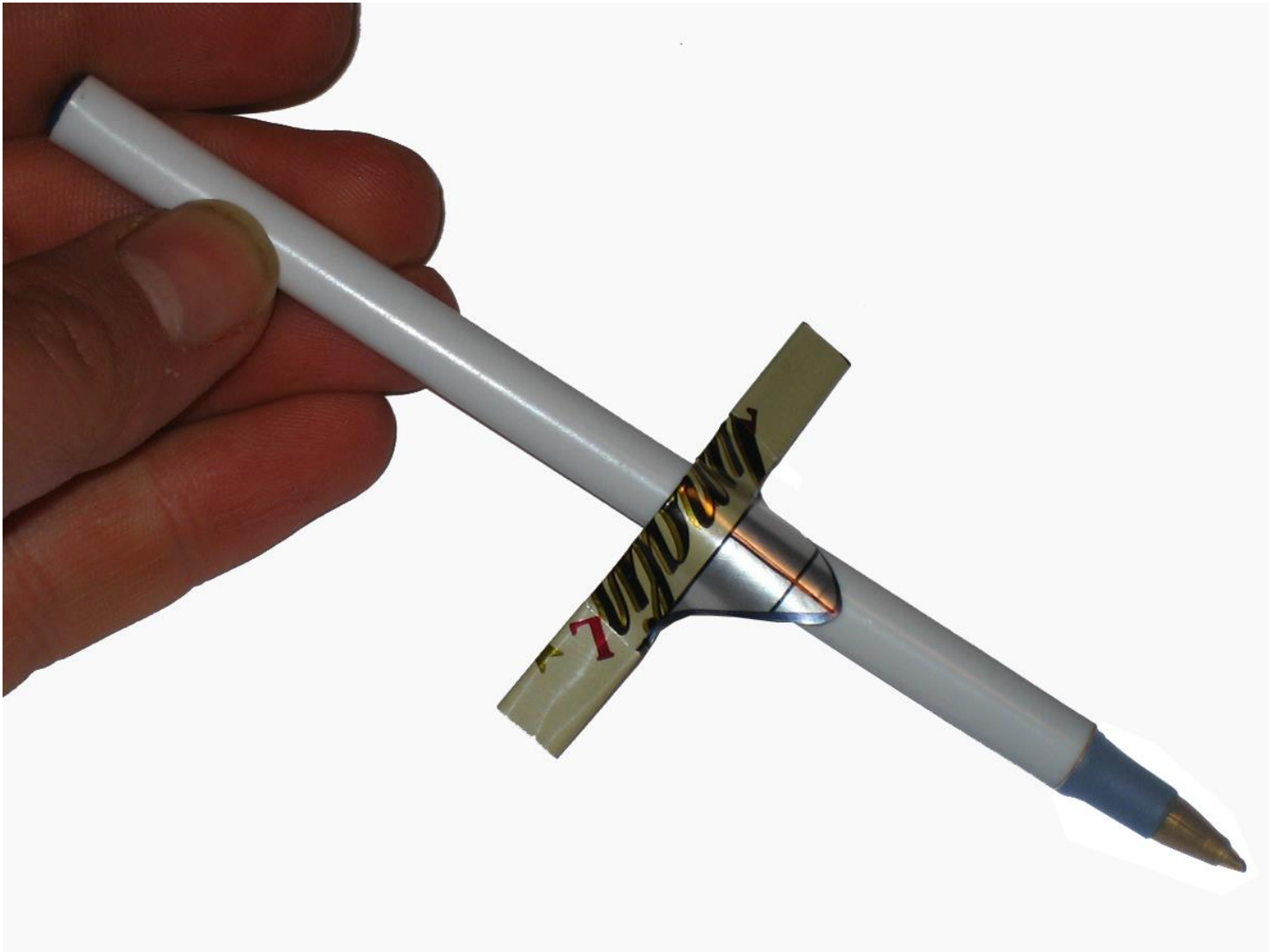
# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---





# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---



# Homebrew Padlock Shims

---





# Homebrew Padlock Shims

---



# Shim-Proof Padlocks... Double-Ball Mechanism

---

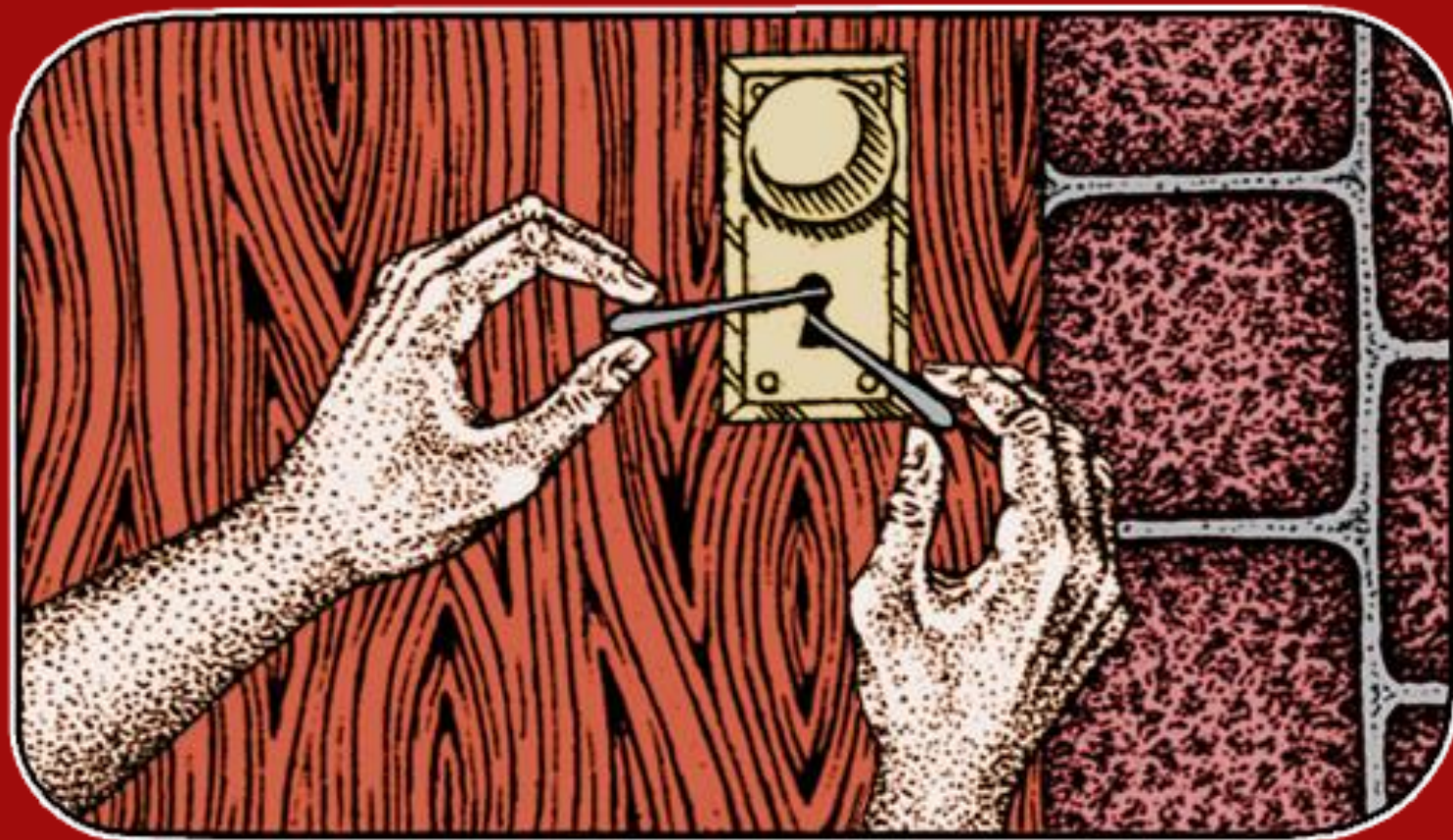


# Shim-Proof Padlocks... Double-Ball Mechanism

---



# Pick-Resistant Locks

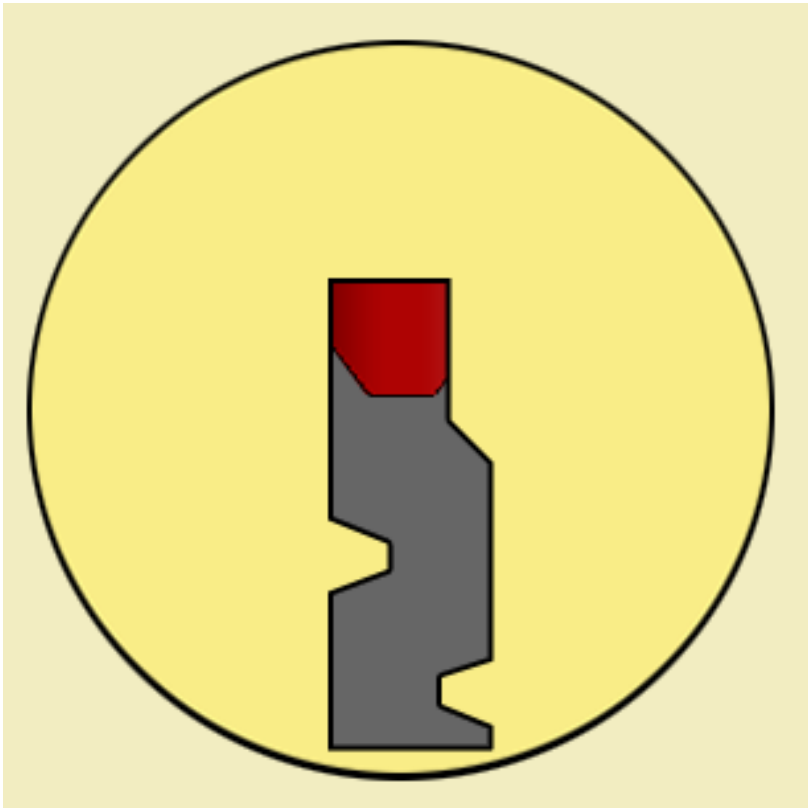




# Pick-Resistant Keyways

---

Simple...



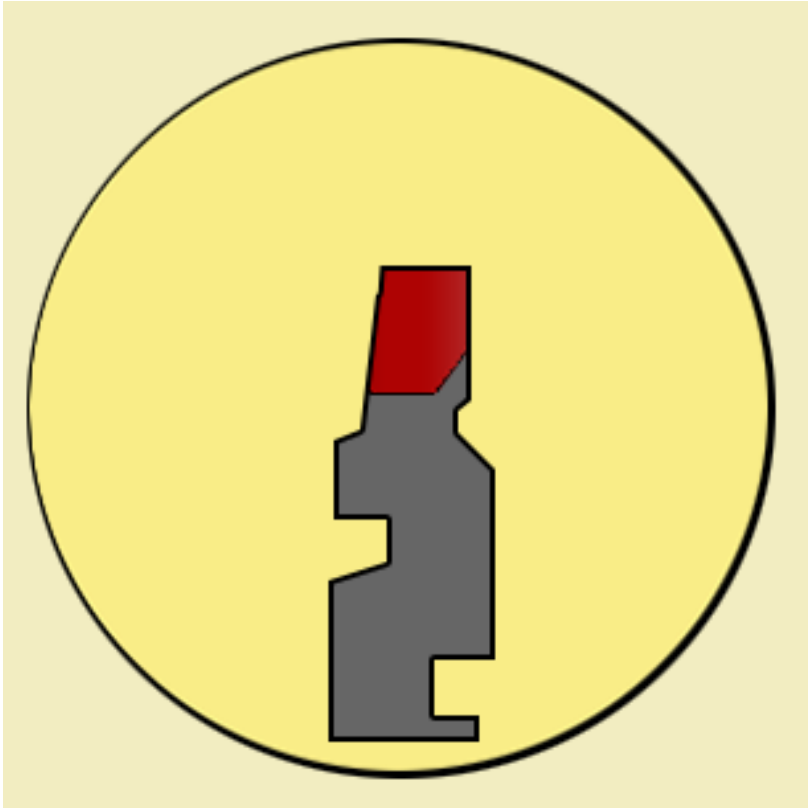
... straight and wide

# Pick-Resistant Keyways

---

Simple...

Medium...



... straight and wide

... straight but narrow

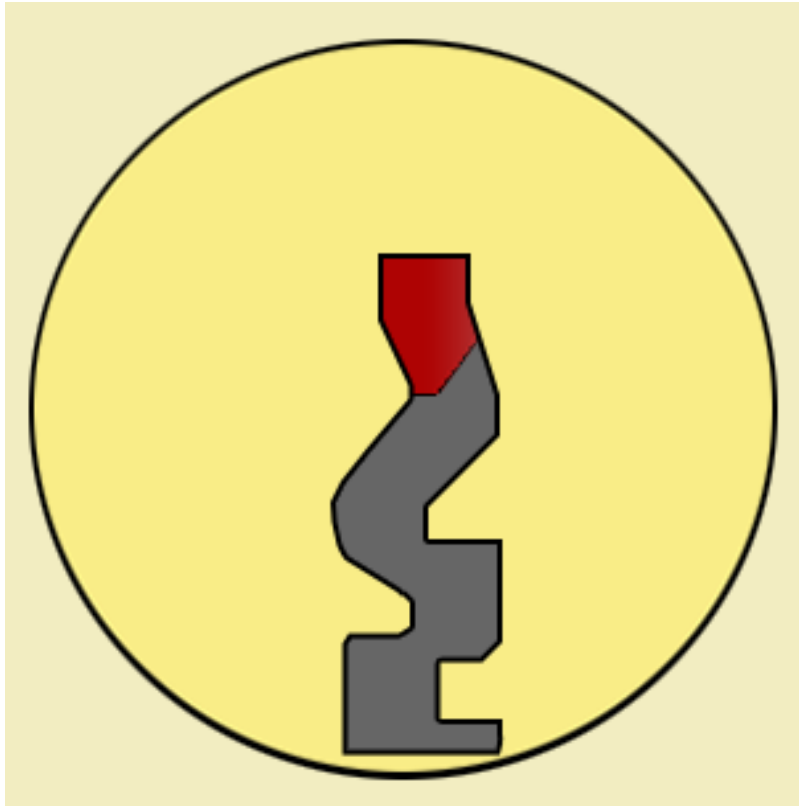
# Pick-Resistant Keyways

---

Simple...

Medium...

Complex...



... straight and wide

... straight but narrow

... thinner and curvy

# Pick-Resistant Keyways

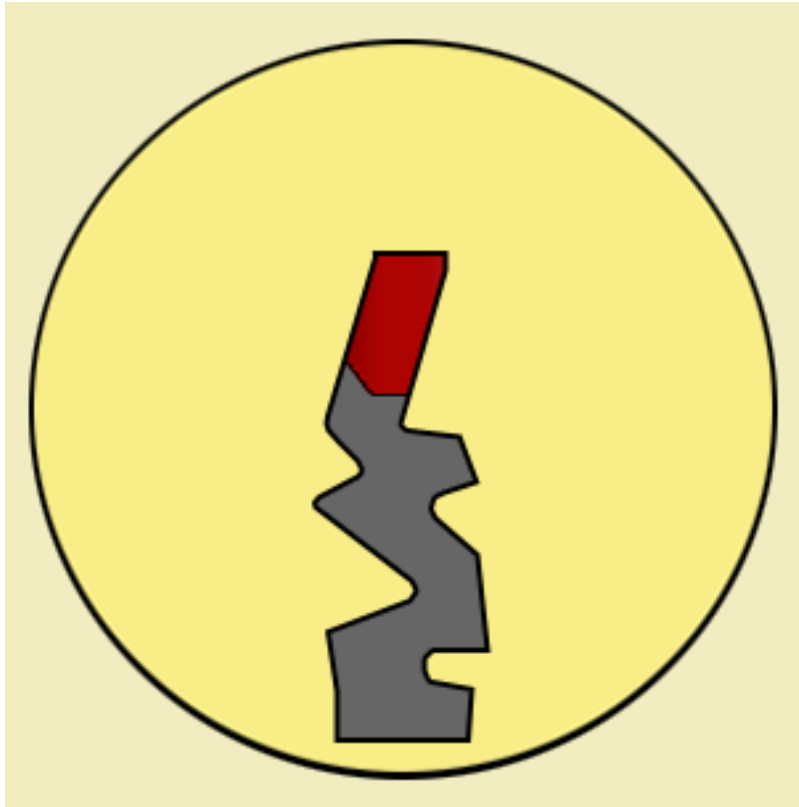
---

Simple...

Medium...

Complex...

Hard...



... straight and wide

... straight but narrow

... thinner and curvy

... lots of angles



# Pick-Resistant Keyways

---

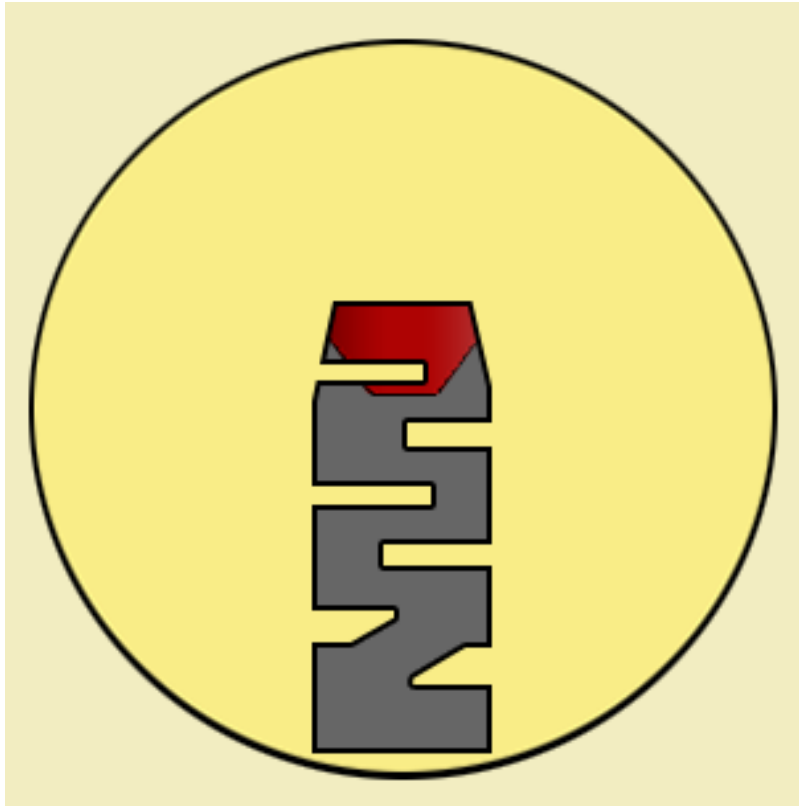
Simple...

Medium...

Complex...

Hard...

Fiendish...



... straight and wide

... straight but narrow

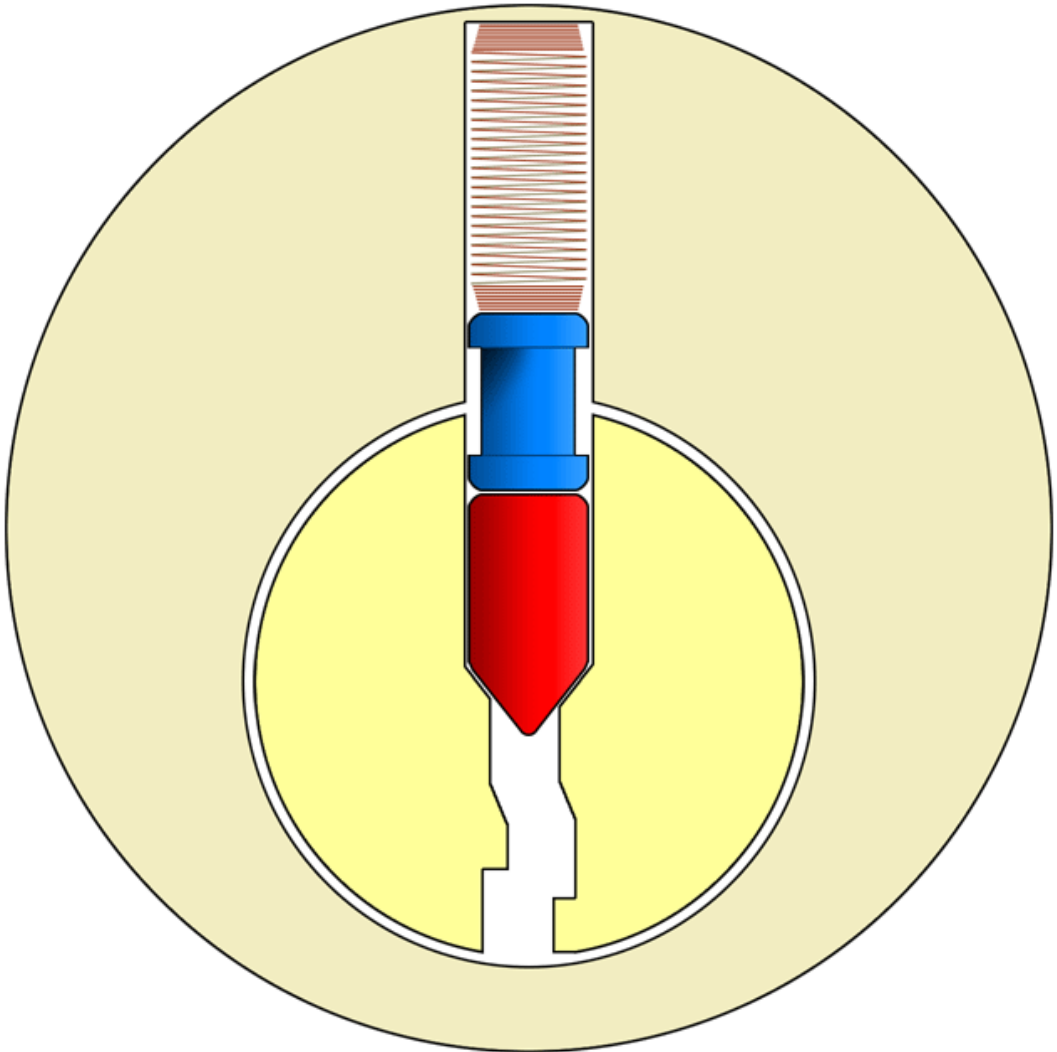
... thinner and curvy

... lots of angles

... overlapping wards

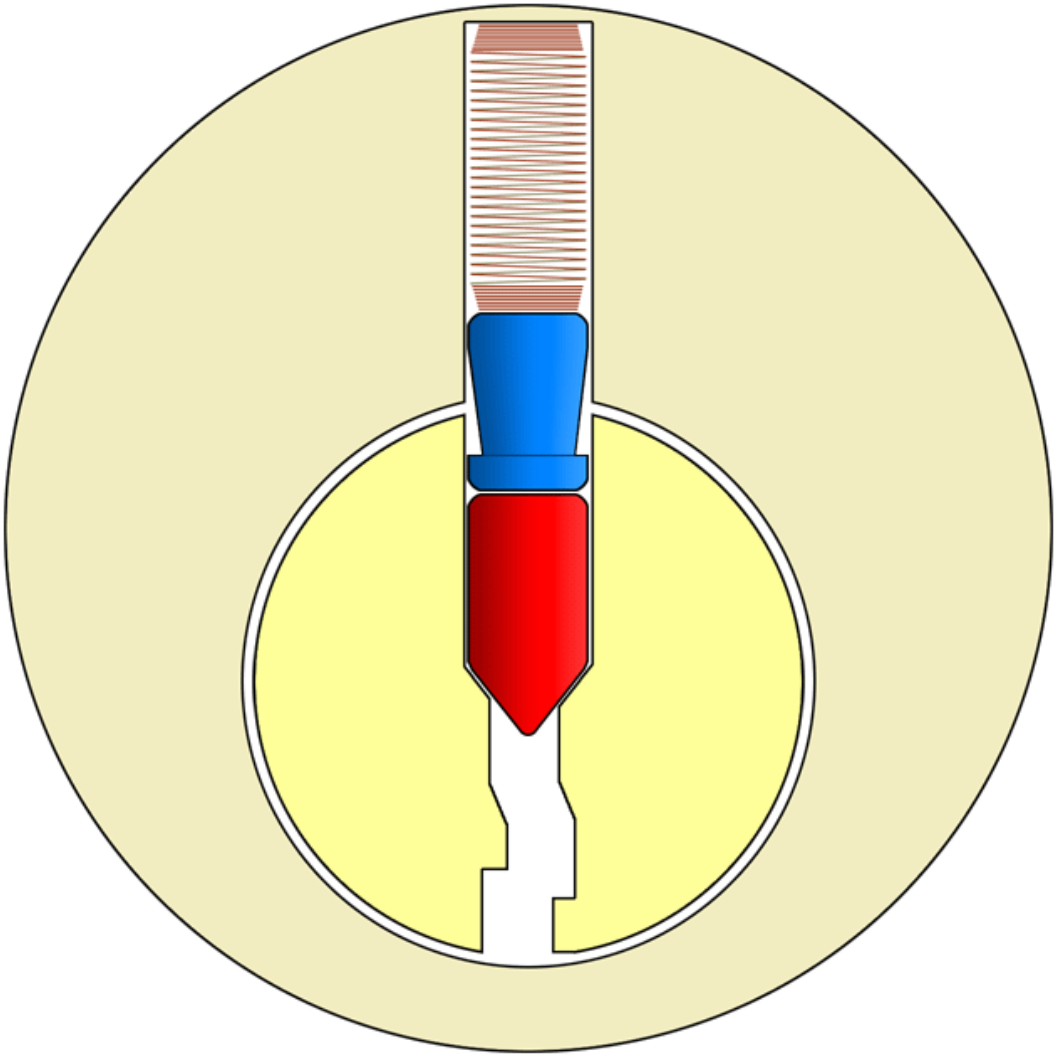
# Pick-Resistant Pins

---



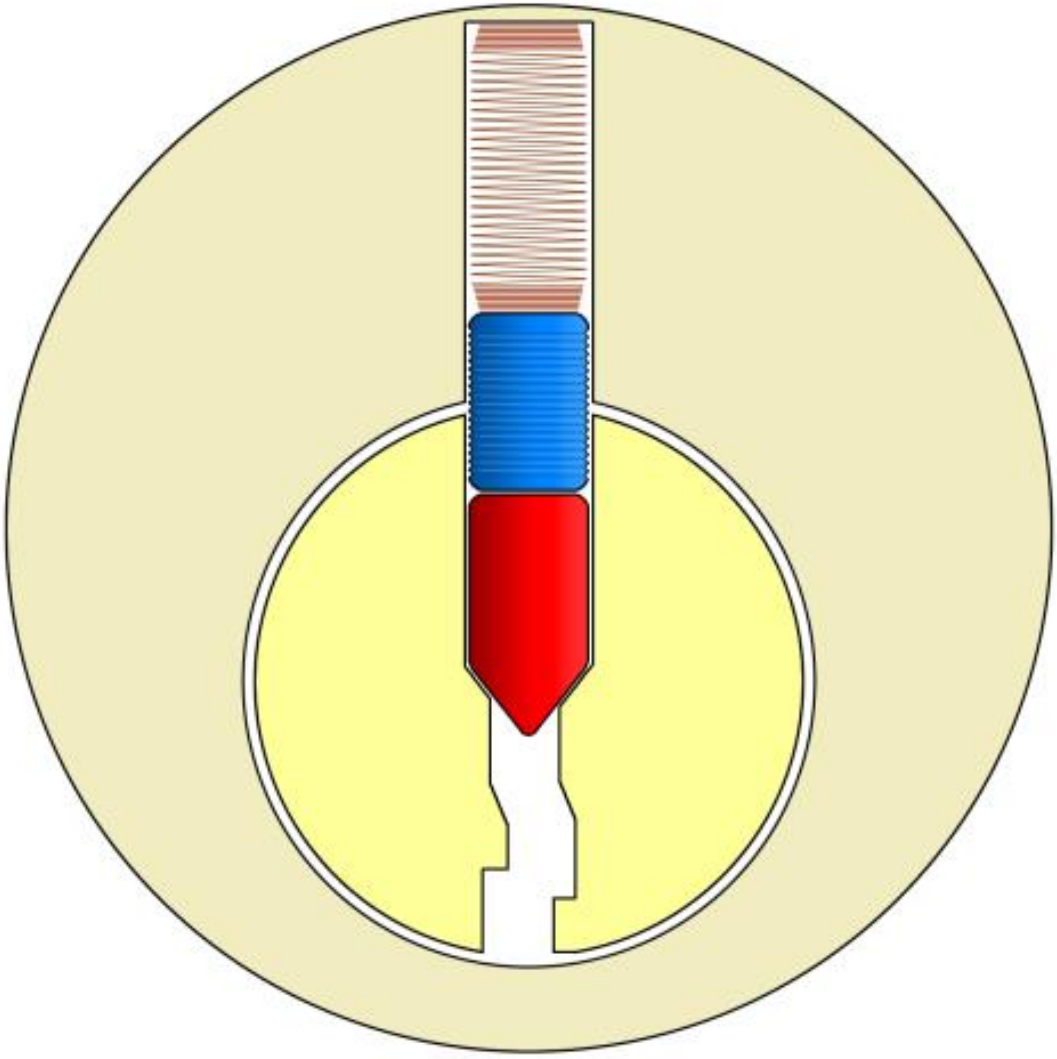
# Pick-Resistant Pins — Mushroom Pin

---



# Pick-Resistant Pins — Serrated Pin

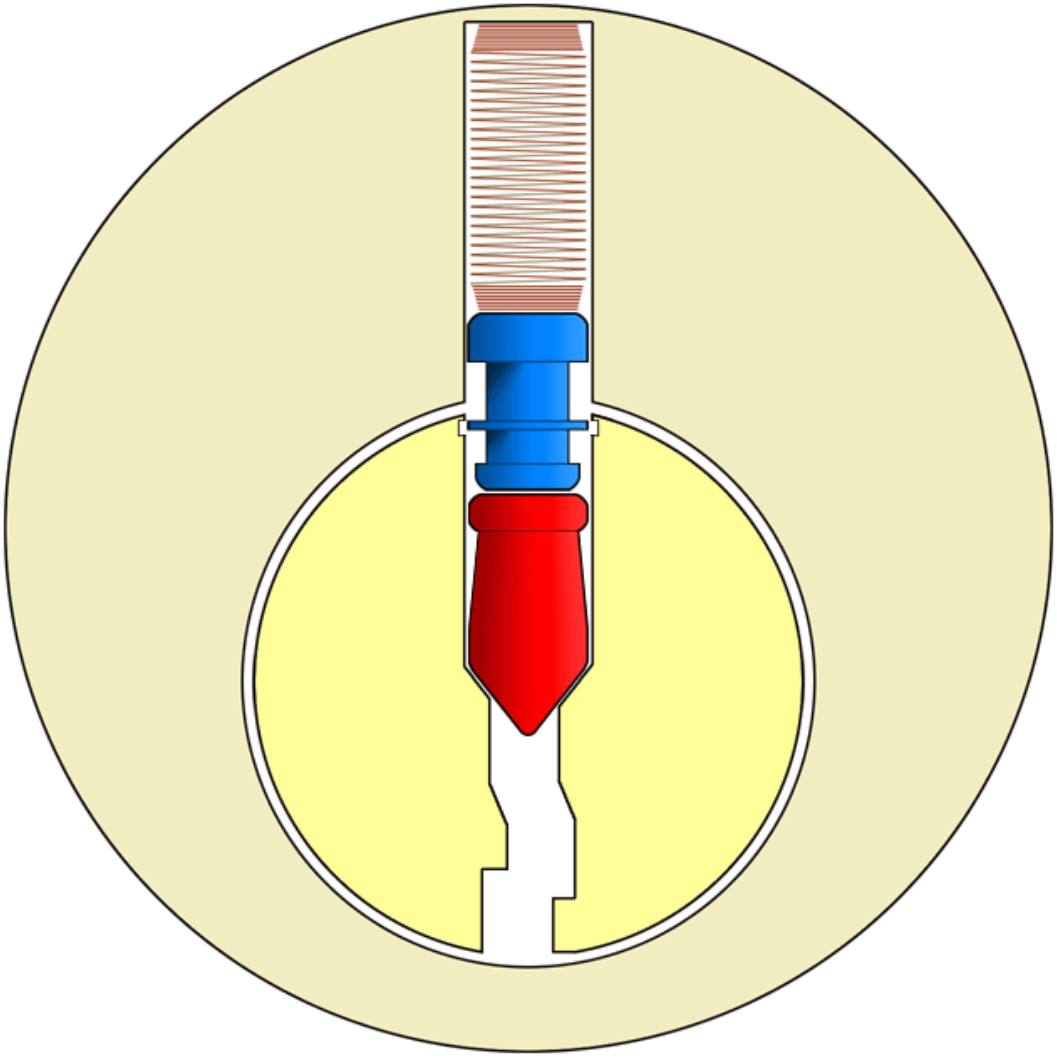
---





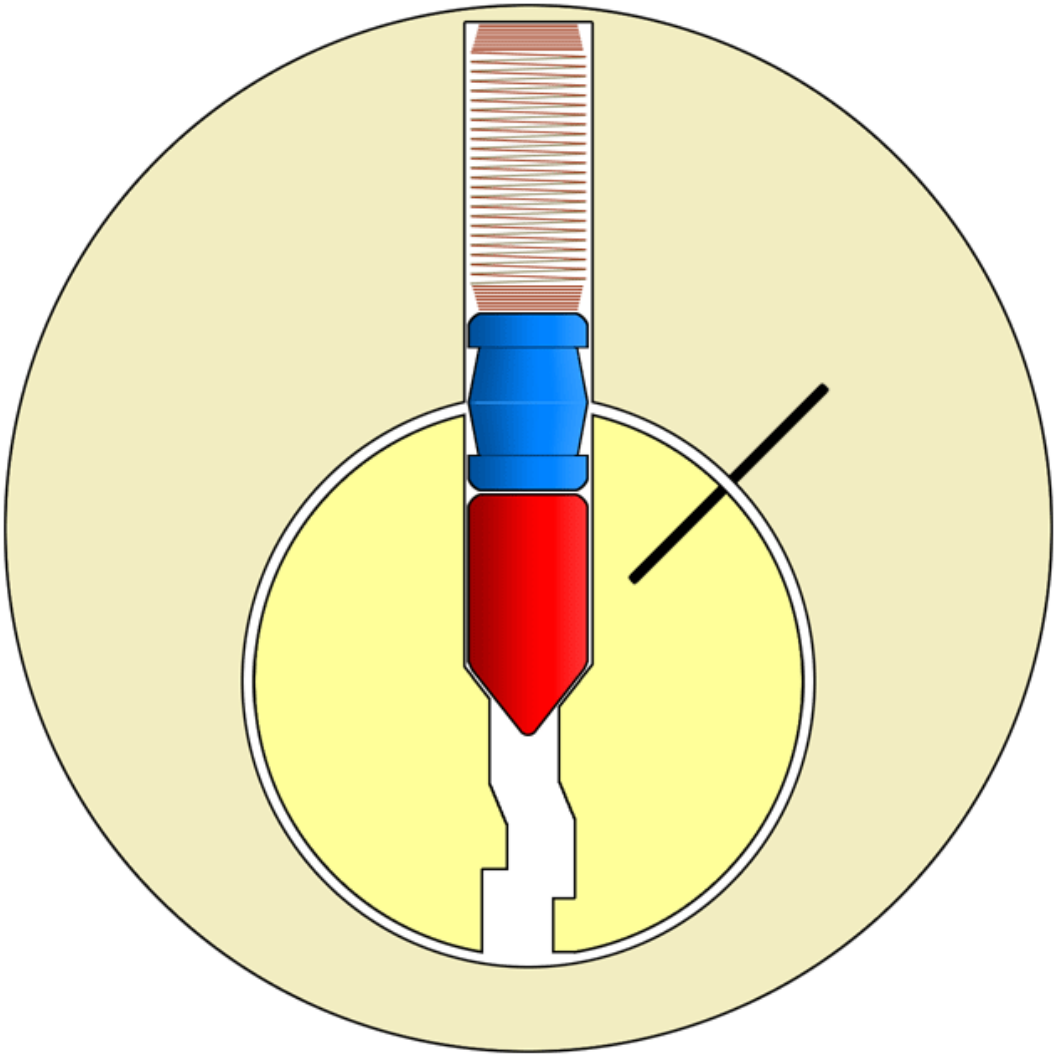
# Pick-Resistant Pins — ASSA "Sneaky" Pin

---

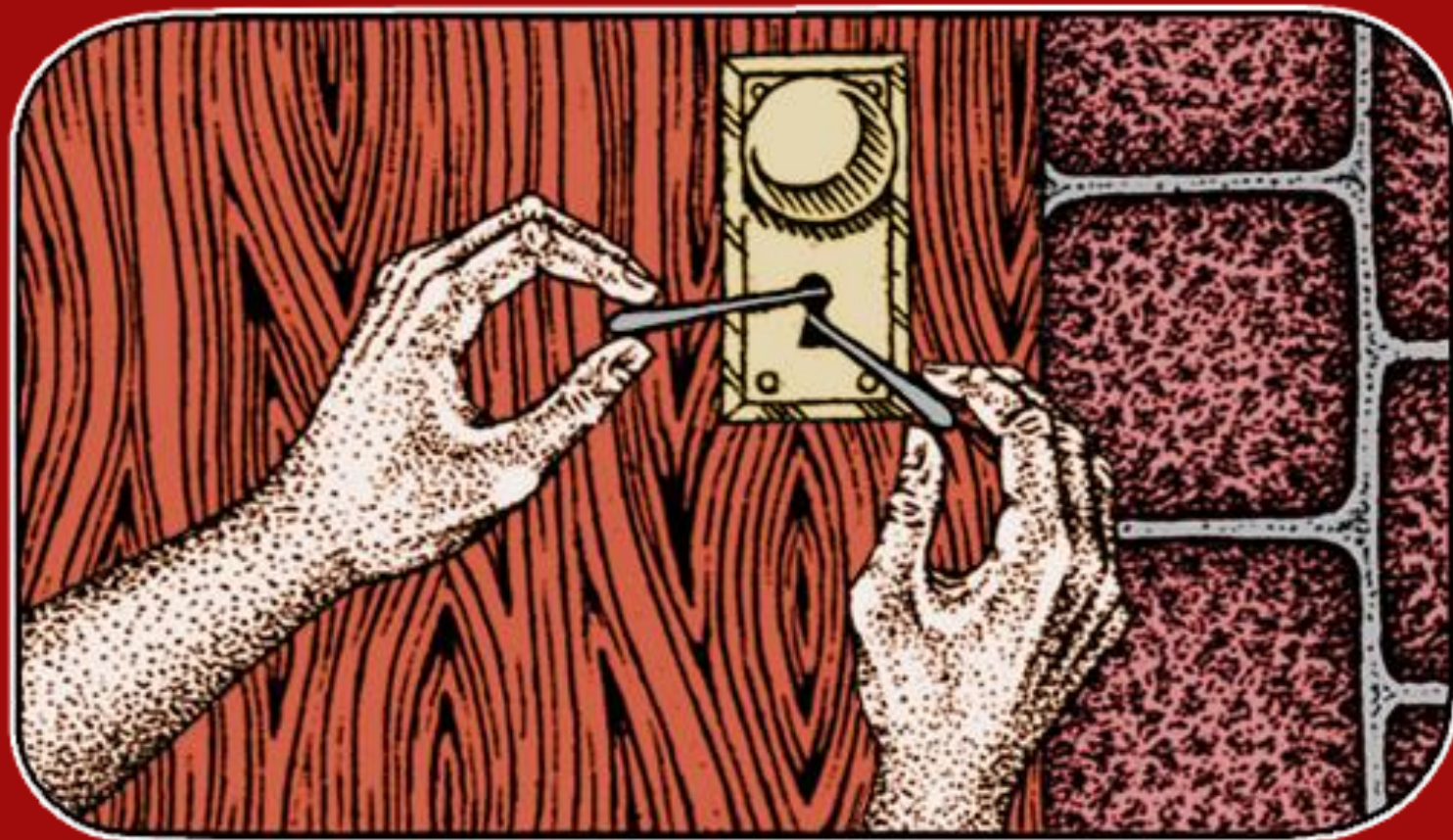


# Pick-Resistant Pins — TrioVing “Double Mushroom” Pin

---



# Bumping Attacks



# Lock Bumping

---

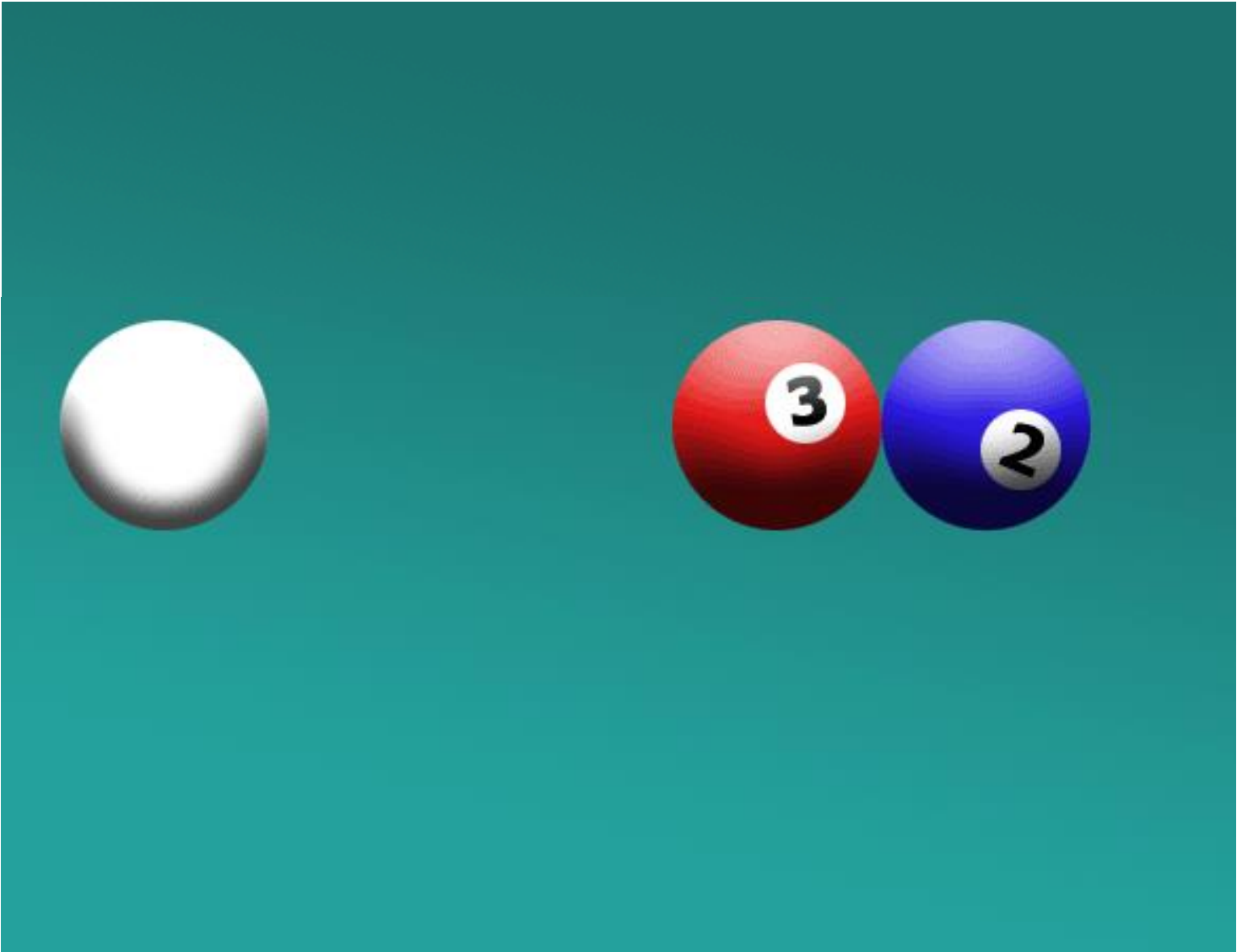
- Just a Special Key
- Little Special Skill
- Many Locks are Vulnerable
- Exploit Related to Pick Gun Physics





# Lock Bumping

---



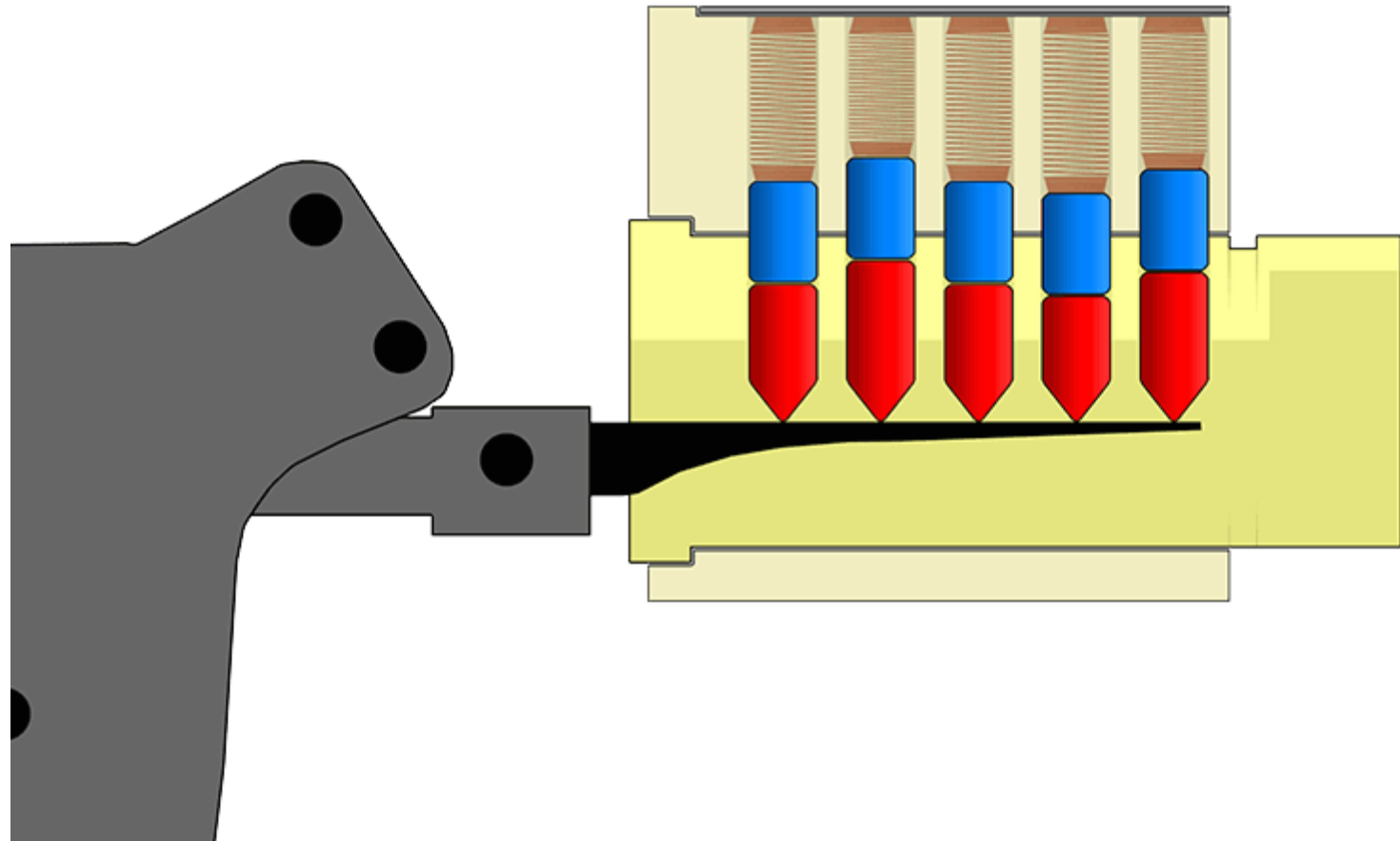
# Snapping Guns

---



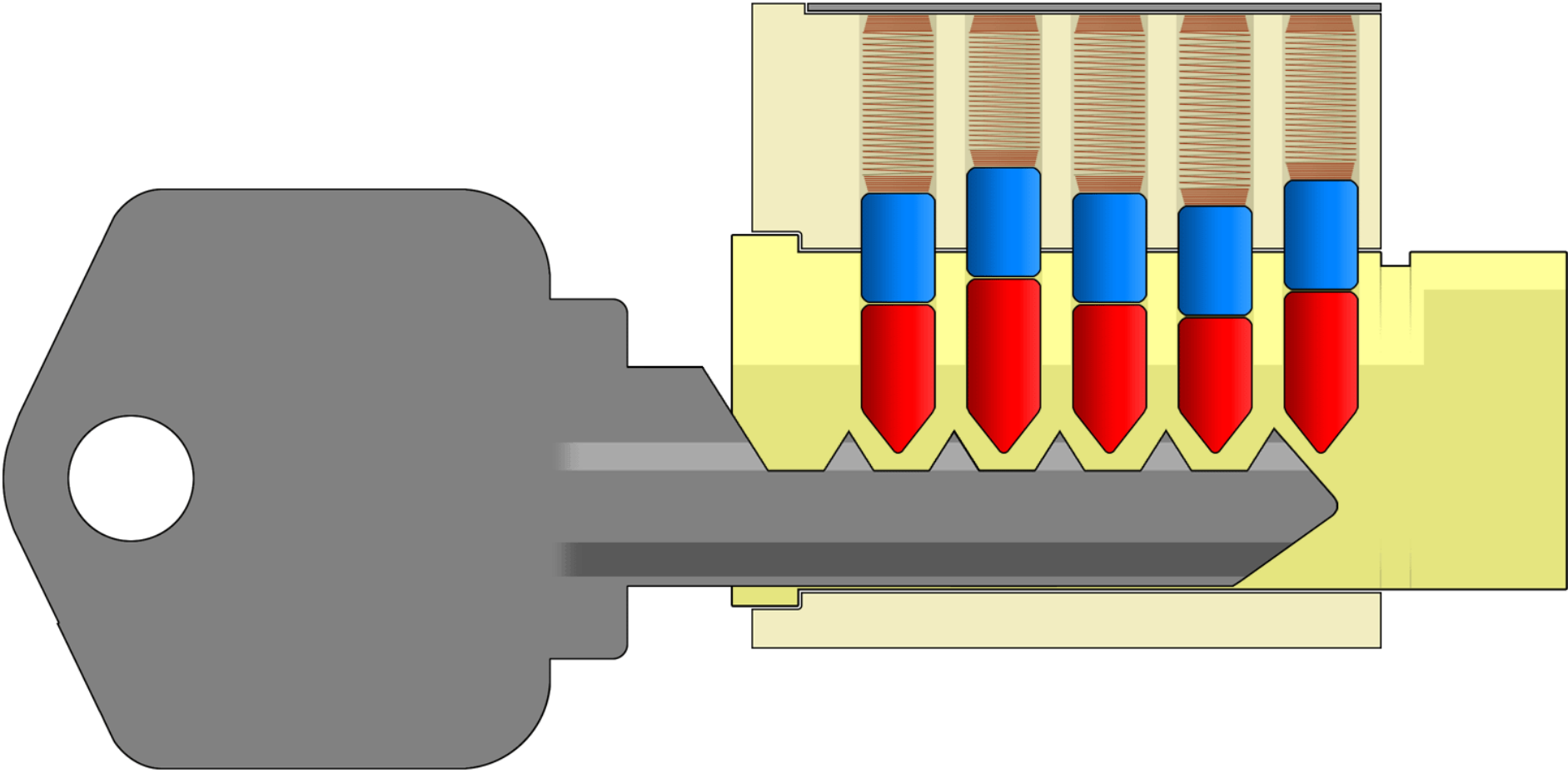
# Snapping Guns

---



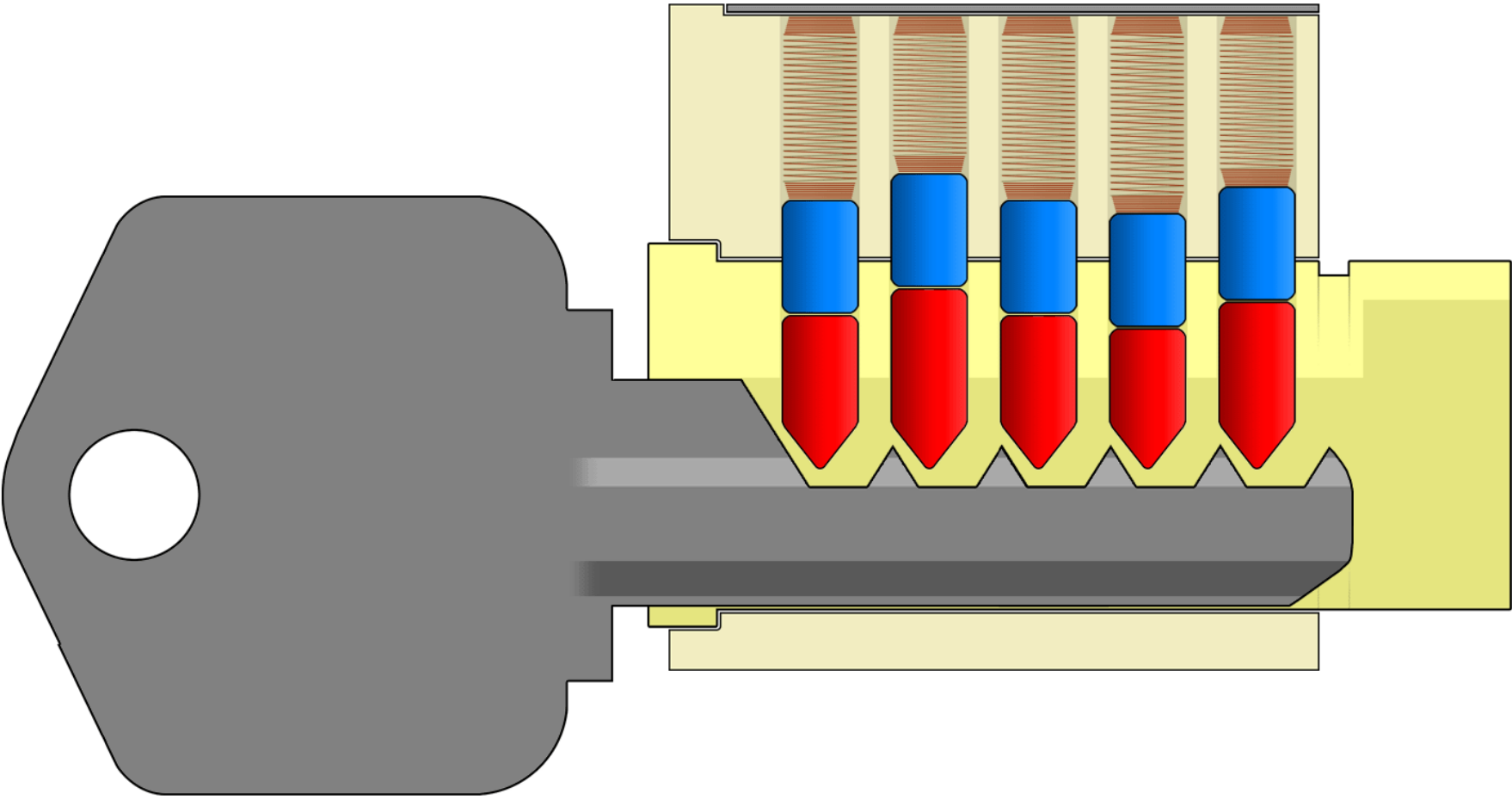
# Lock Bumping — Pull Method

---



# Lock Bumping — Push Method

---





# Lock Bumping

---



<http://tool.nl/bumping.pdf>

# Lock Bumping

---

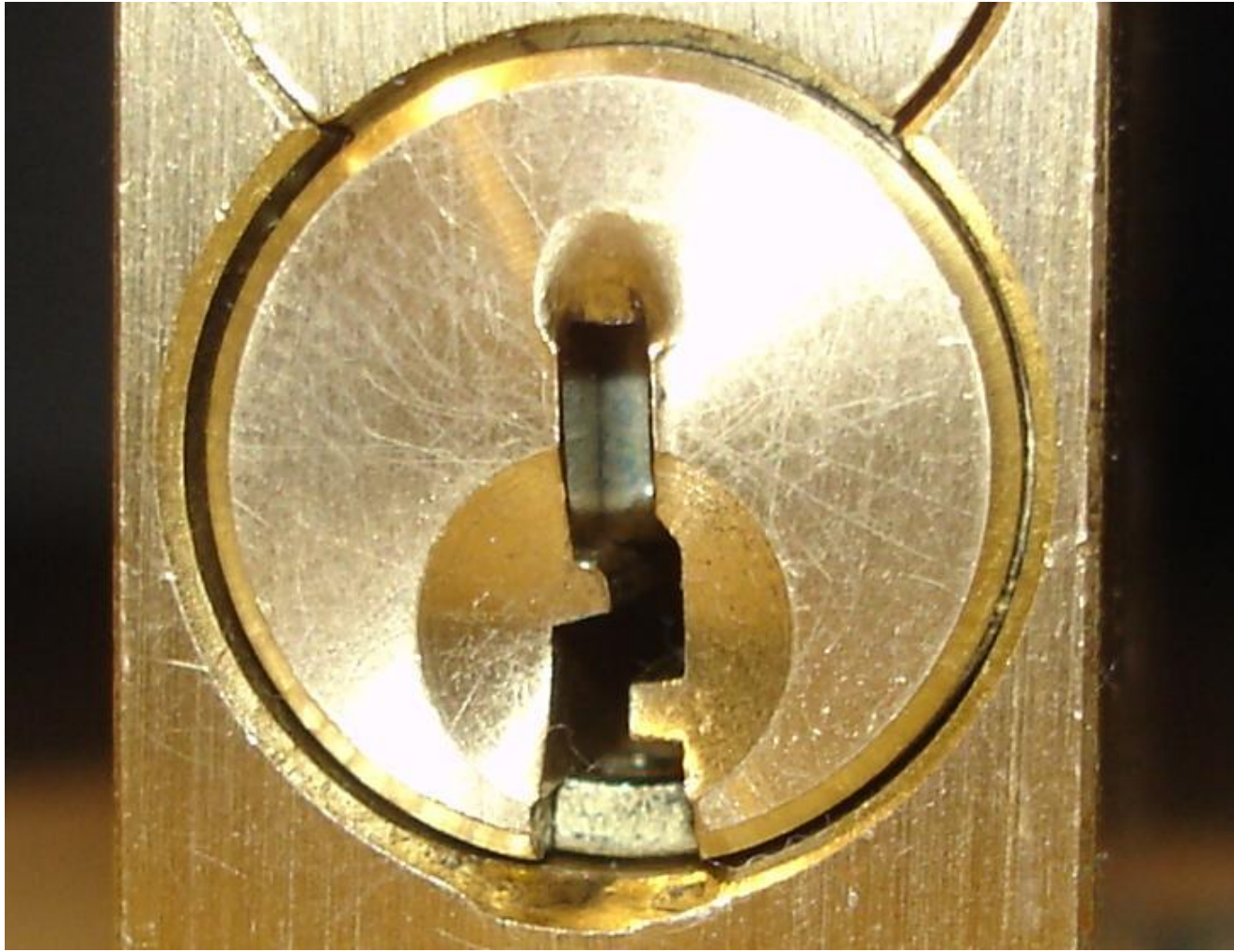
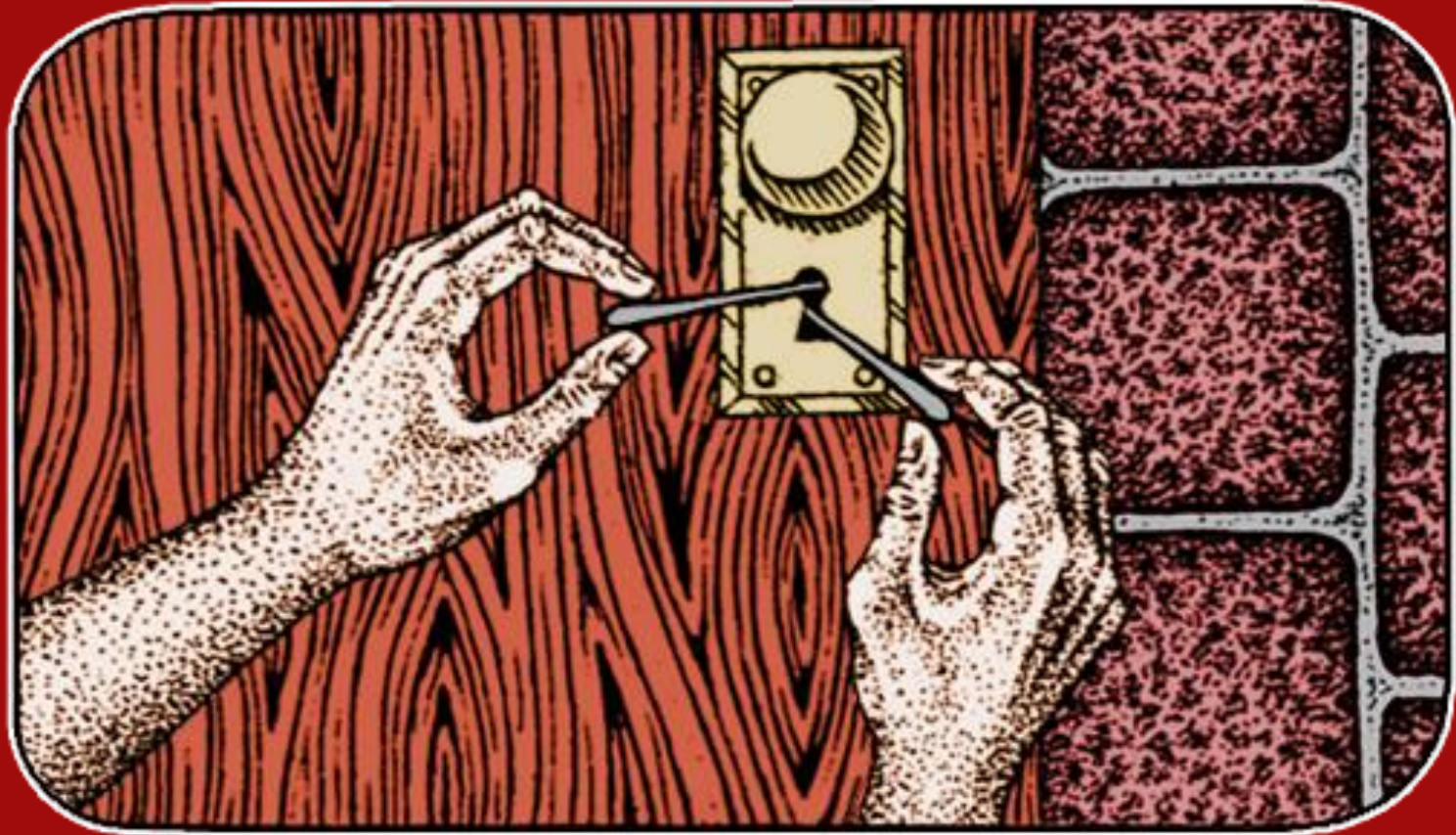


photo courtesy of dataqram



Looking for a better lock now?



- 1. ALOA logo / ALOA number**
- 2. Name Discrepancies**
- 3. Estimates & Itemized Invoice**
- 4. Credentials & Identification**
- 5. Your Right to Refuse**

# High security locks

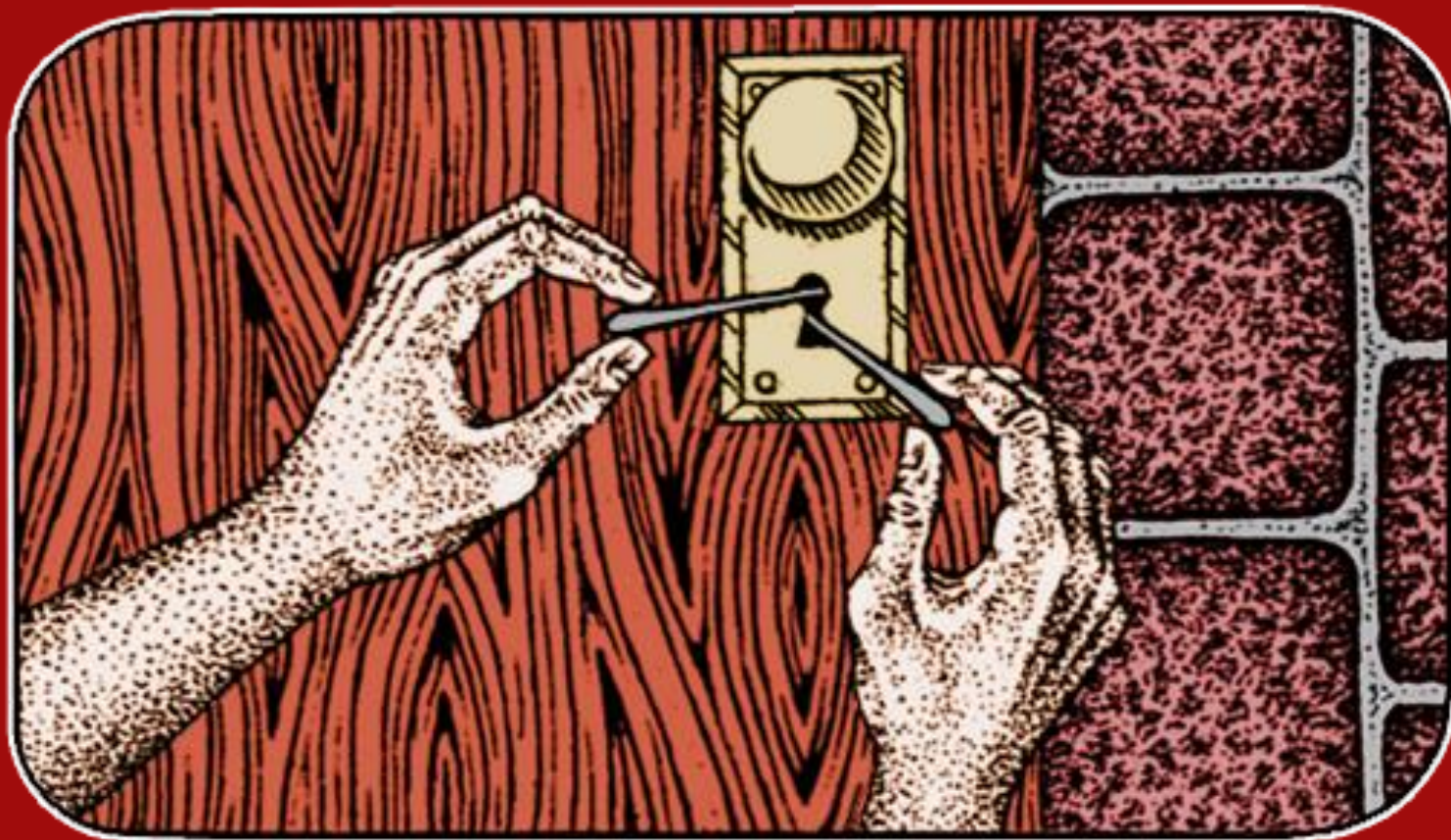
---

1. Abloy Protec2 — King of the Hill
2. Medeco
3. BiLock
4. Anything from

<https://securitysnobs.com/>



# Teleduplication and 3D Printing



# Attack: Teleduplication



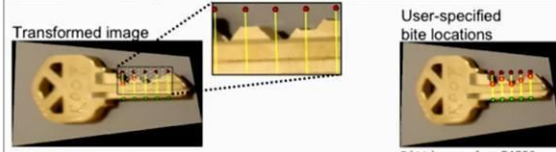
Reference Key



Target Key: Labeling key points



Transformed Target: Labeling cut depths



Bitting code: 74753

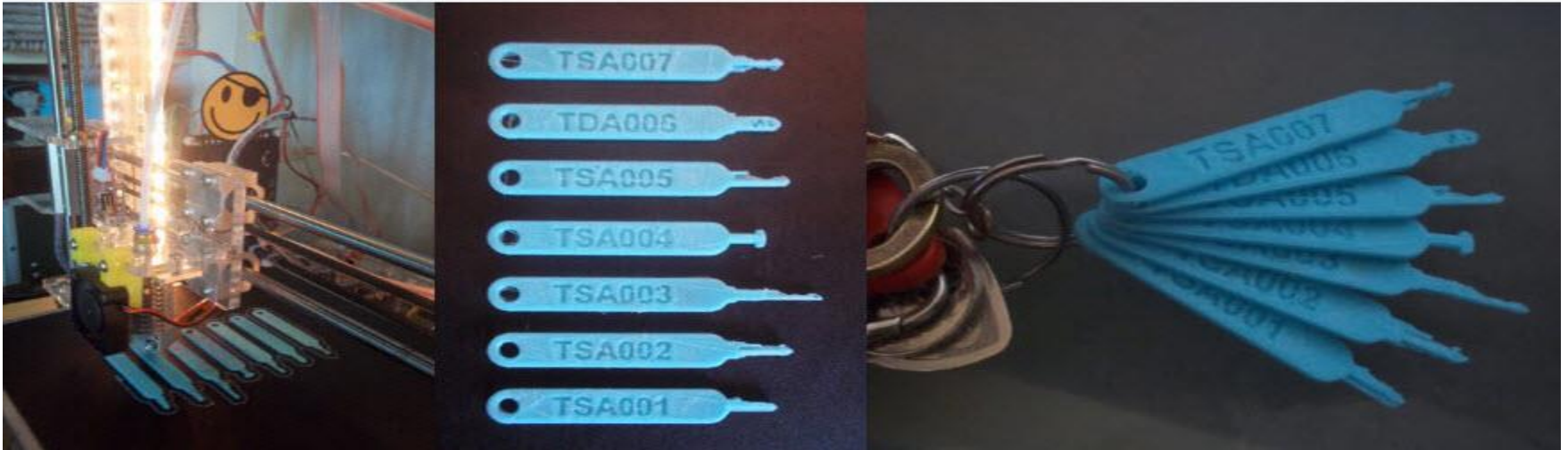
Okey, but no one is going to actually do this...

---





Yep.



<http://casper.im/locks/TSA-master-keys.zip>

# Not exactly new

---



In 2009, German and Dutch police used a 'special' handcuff key not available to the public. One decently high resolution picture, it was successfully replicated.

<http://www.thingiverse.com/thing:72351>



## Printed key strength



	PLA	Nylon/Acrylic	Alumide	Metal
Cost	\$0.08	\$2-\$8	\$3	\$10-\$25
Door Latch	Pass	May Fail	Pass	Pass
Door Unlock	Pass	Fail	Pass	Pass
Various Padlocks	Pass	Fail	Fail	Pass
Crash Bar	May Fail	Fail	Fail	Pass

# How easy is it?

---



Go to <https://github.com/ewust/keys>

Install python (programming compiler)

Run the following line for a bump key:

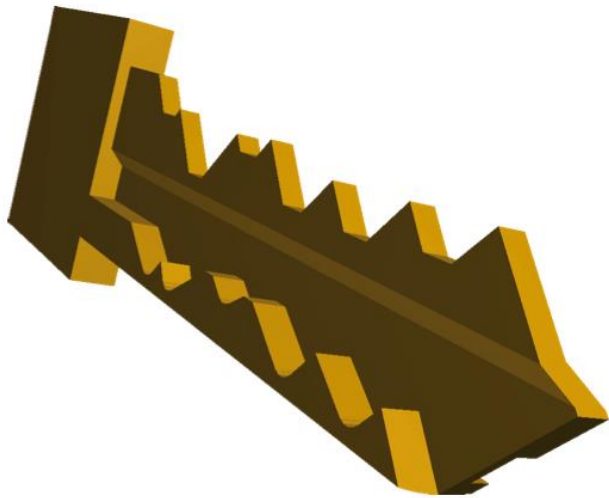
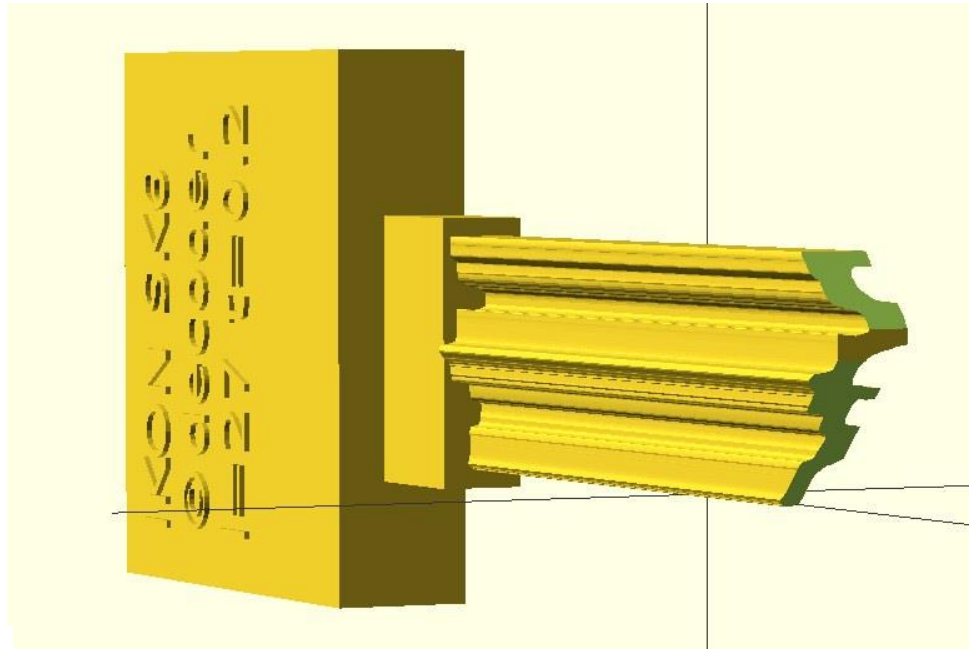
```
python KeywayDetection.py ./sample-lock.jpg -kc 9 9 9 9 9 9 9
```



Works even better for high security locks!

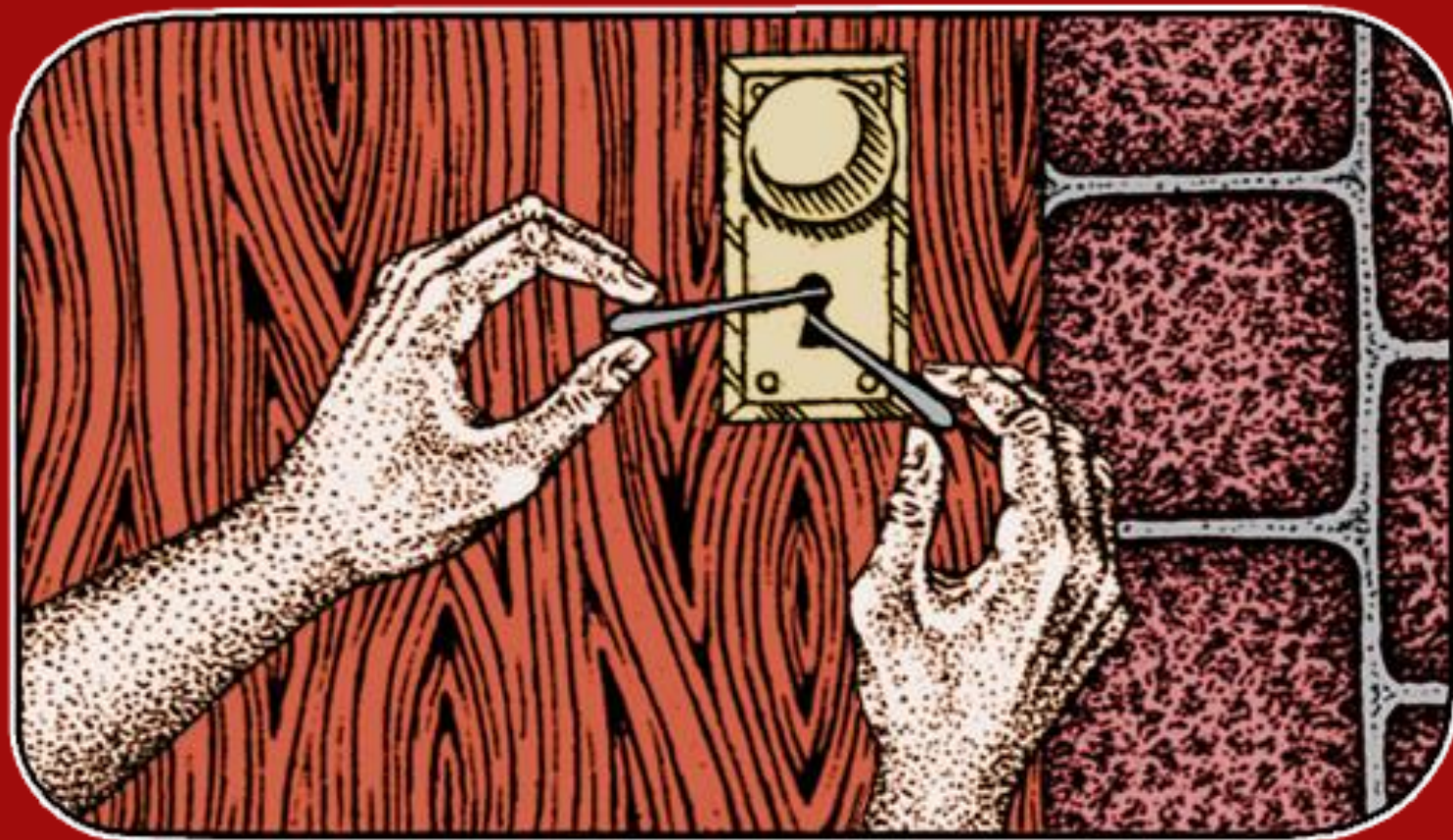
---

Ikon SK6




Schlage Primus

# Distinguishing Picks





# There are many lockpick vendors...



h p c w o r l d  
Designer and Manufacturer of Locksmithing Equipment Since 1956

PRODUCT INFORMATION

- Key Machines
- Key Machine Accessories
- Code Cards
- Software
- Car Openers
- Pick Sets
- Tools
- Security Storage
- Door Guards

May 1 through May 31, 2010  
**May Springtime Sale!**  
Click here to find out what's going on in May!

Have you seen...  
HPC Sales Policy  
Distributors  
Software Support  
Calendar of Events  
Instructions



LOCK PICKS.com  
BY BROCKHAUSE

HOME CONTACT US COMPANY INFO LOGIN

Product Categories  
LOCK ENTRY TOOLS  
Pick Guns (Electrical)  
Pick Sets  
Lock Bypass Tools  
Bump Keys & Tools  
Tubular Lock Picks  
Pick Set Parts  
Special Tension Tools  
Flag Spinners  
Destructive Entry  
AUTOMOTIVE  
Auto Opening Kits  
Individual Auto Pick Tools  
Out Keys

Offering locksmith supplies and equipment. You will find lock pick tools, key blanks, and key machines. We also offer other locksmith tools such as, key duplicators, pin sets, lock pick guns, tubular lock picks, lock picking equipment, key blanks, locksmith equipment, lock opening tools, professional burglar items, professional auto opening kits, air wedge bits, and lock stems, and tension tools. We are a professional locksmith supply company. LockPicks.com now offers the full line of VIKING Key Machines.



lockpicktools.com - lock picks, tension tools & auto lockpick tools - Mozilla Firefox

Lock Pick Tools, tension tools, automotive access & entry tools for locksmiths, lockpicking, lock smiths, law enforcement, law enforcement...

**Southern Specialties Co.**

www.lockpicktools.com

4 B's of Buying From Lockpicktools.com

- Best price - You will be buying from the manufacturer, no middle man
- Best quality - All our picks made from premium tempered stainless steel.
- Best delivery - All orders in by 2pm EST shipped same day
- Been in business for over 30 years designing and manufacturing lock smith to

New Releases | Featured Specials | Coming So



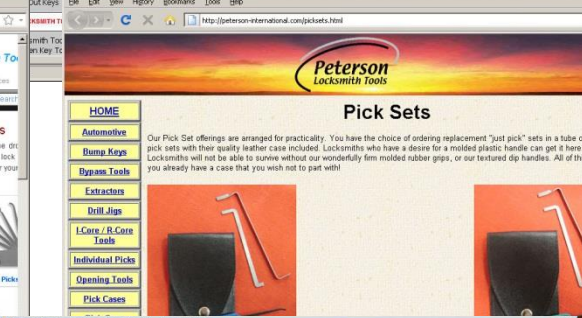
SOUTHORD  
Manufacturer of Lock Picks & Professional Locksmith Tools

SouthOrd Professional Lock Picks

Lock Pick Categories

Quality, Reliability, Innovation, Value, and Service  
have made SouthOrd® the industry leader in stainless steel professional locksmith tools. SouthOrd Lock Picks are constructed of Full Hard Spring Stainless Steel - only one of the reasons we are supplier to locksmiths and repo men worldwide, governmental agencies both domestic and foreign, elite military units including Navy Seals Teams and other Special Ops Forces, the 101st and 502nd Airborne, and law enforcement agencies, Federal, State, and Local. If you fall into one of the previously mentioned job fields, Click Here for Associated Discounts.

Our new SouthOrd MAX® Lock Picks are made of the strongest and most durable stainless steel in the world, High Yield, with a minimum tensile strength of 270,000 PSI. We are honored to have gained the confidence of so many, and we welcome you into the family of SouthOrd Locksmith Tools.



Peterson Locksmith Tools

Pick Sets

Our Pick Set offerings are arranged for practicality. You have the choice of ordering replacement "just pick" sets in a tube or complete pick sets with their quality leather case included. Locksmiths who have a desire for a molded plastic handle can get it here. Other Locksmiths will not be able to survive without our wonderfully firm molded rubber grips, or our textured dip handles. All of this is just if you already have a case that you wish not to part with!



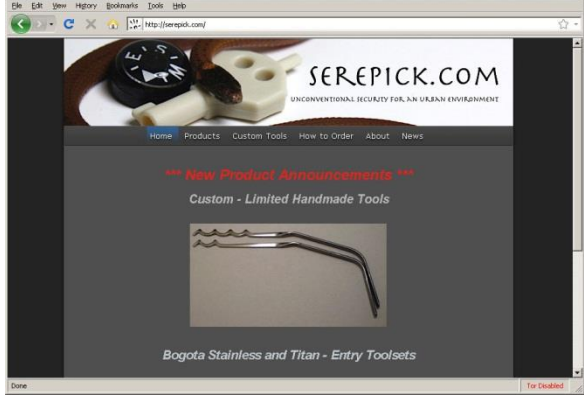
LOCK PICKS

RYTAN EXCLUSIVE  
Mini-Red™ & Mini-Blue™ plus Full Size Picks  
Full size picks have standard 2mm pick blade tip.  
Mini-Red™ & Mini-Blue™ plus Full Size Picks  
Full size picks have standard 2mm pick blade tip.

LOCK PICK INSTRUMENTS WITH TRADITIONAL SMOOTH STRAIGHT BLANKER HANDLES

LOCK PICK INSTRUMENTS WITH FAMOUS CURVED ERGONOMIC HANDLES

Model	Description	Price
SLP-6	Full Single Large Ball	RRP: 4.95
SLP-7	Full Double Ball	RRP: 4.95
SLP-8	Rytan Full Triple Ball	RRP: 7.95
SLP-9	1/2 Double Ball	RRP: 5.95
SLP-10	Standard Diamond	RRP: 10.00
SLP-11	Standard Full Flake	RRP: 11.00



SEREPICK.COM  
UNCONVENTIONAL SECURITY FOR AN URBAN ENVIRONMENT

Home Products Custom Tools How to Order About News

New Product Announcements™™™  
Custom - Limited Handmade Tools

Bogota Stainless and Titan - Entry Toolsets



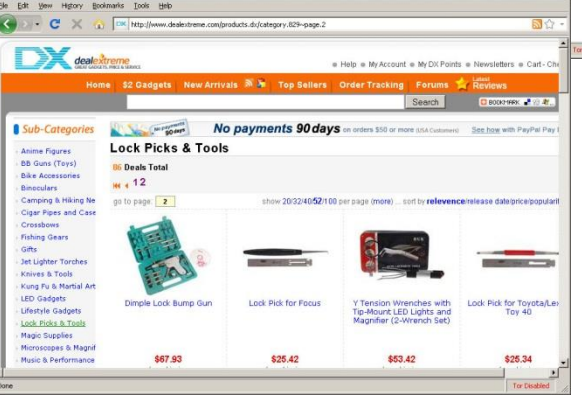
LockPickShop.com  
Toll Free Order Line for US/Canada  
1-877-919-LOCK

Home About Us Catalog Customer Service My Account Shopping Cart

Products

Lock Pick Combo Kit 1  
Lock Pick Combo Kit 2  
Lock Pick Combo Kit 3  
Lock Pick Combo Kit 4

Category Info:  
Our lock picking combo kits can't be beat. Jam-packed with the tools you need like SouthOrd lock pick sets, hand tools, locksmith training tools and books have been combined into "Proven" savings kits that are sure to please law enforcement personnel, locksmiths, lock picking hobbyists, enthusiasts and security professionals alike. At a 40% below retail it's a steal!



DX Deals  
No payments 90 days on orders \$50 or more (USA Customers) See how with PayPal Pay It Later

Sub-Categories  
Lock Picks & Tools

Deals Total  
12

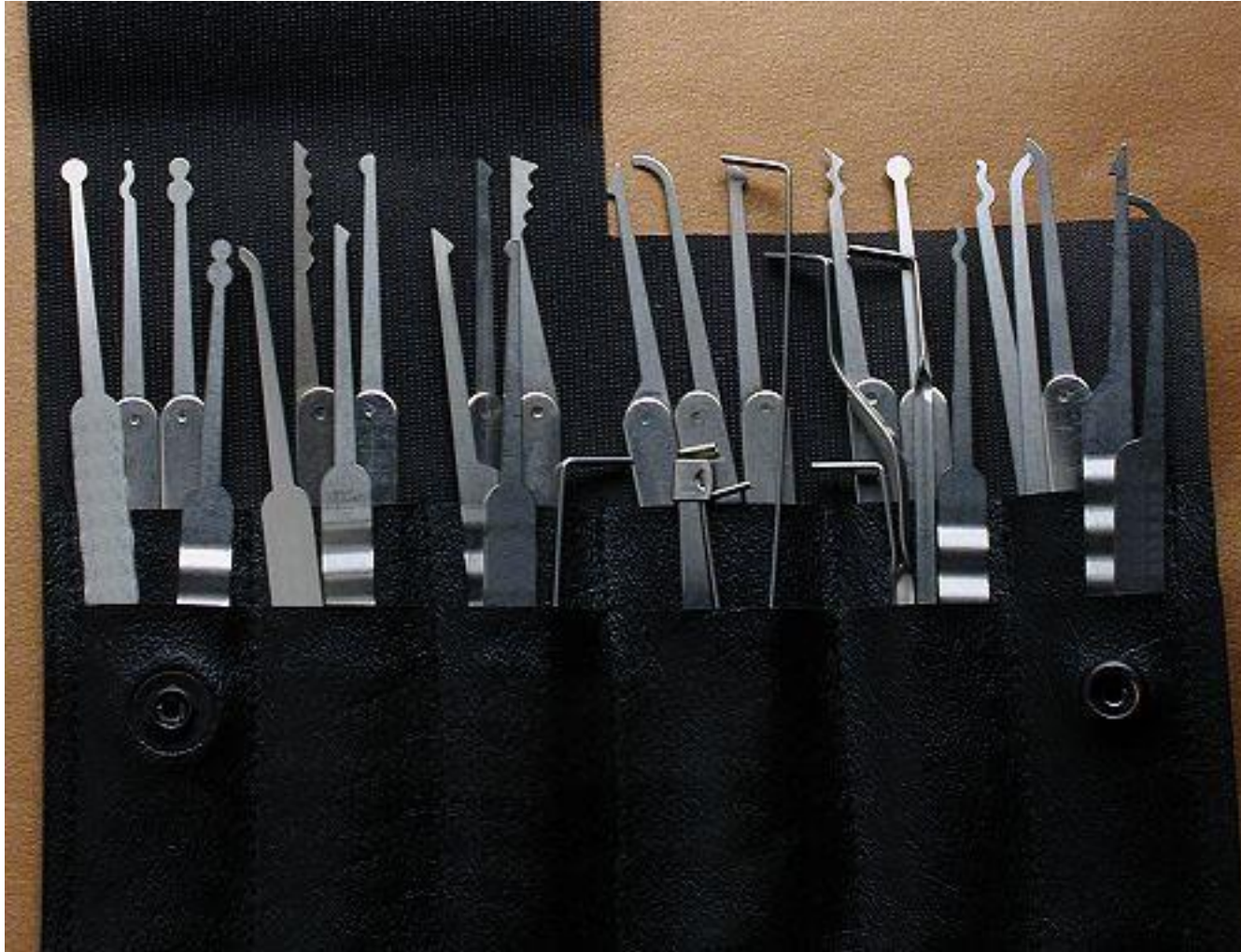
show 20/24/48/100 per page (more) sort by relevance/release date/pricelocked

Product	Price
Dimple Lock Bump Gun	\$97.93
Lock Pick for Focus	\$25.42
Y Tension Wrenches with Top-Mount LED Lights and Magnifier (2-Wrench Set)	\$53.42
Lock Pick for Toyota/Lexus (40)	\$26.34



See this? Don't buy this.

---



# First, let's talk about metal...

---



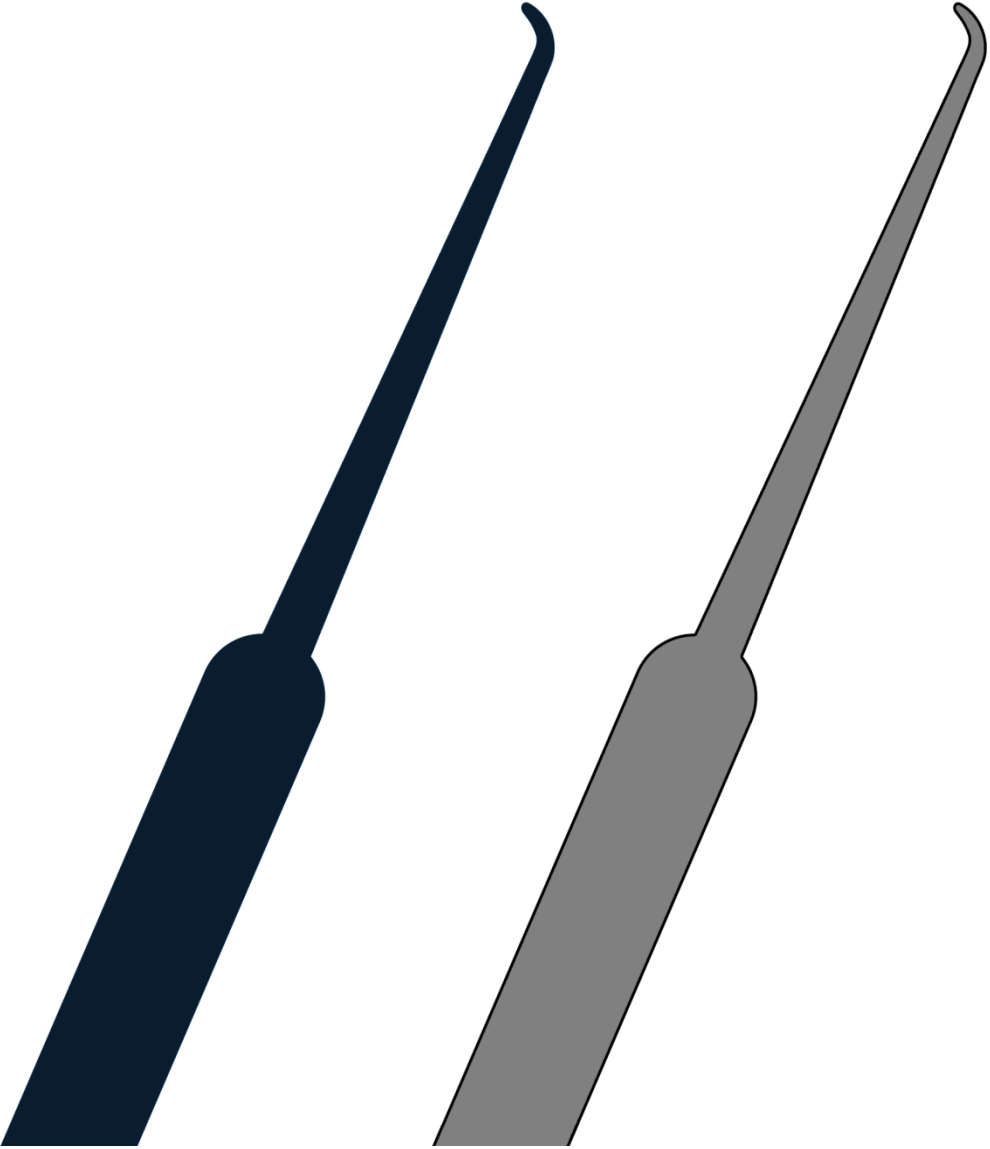
# Spring Steel

---



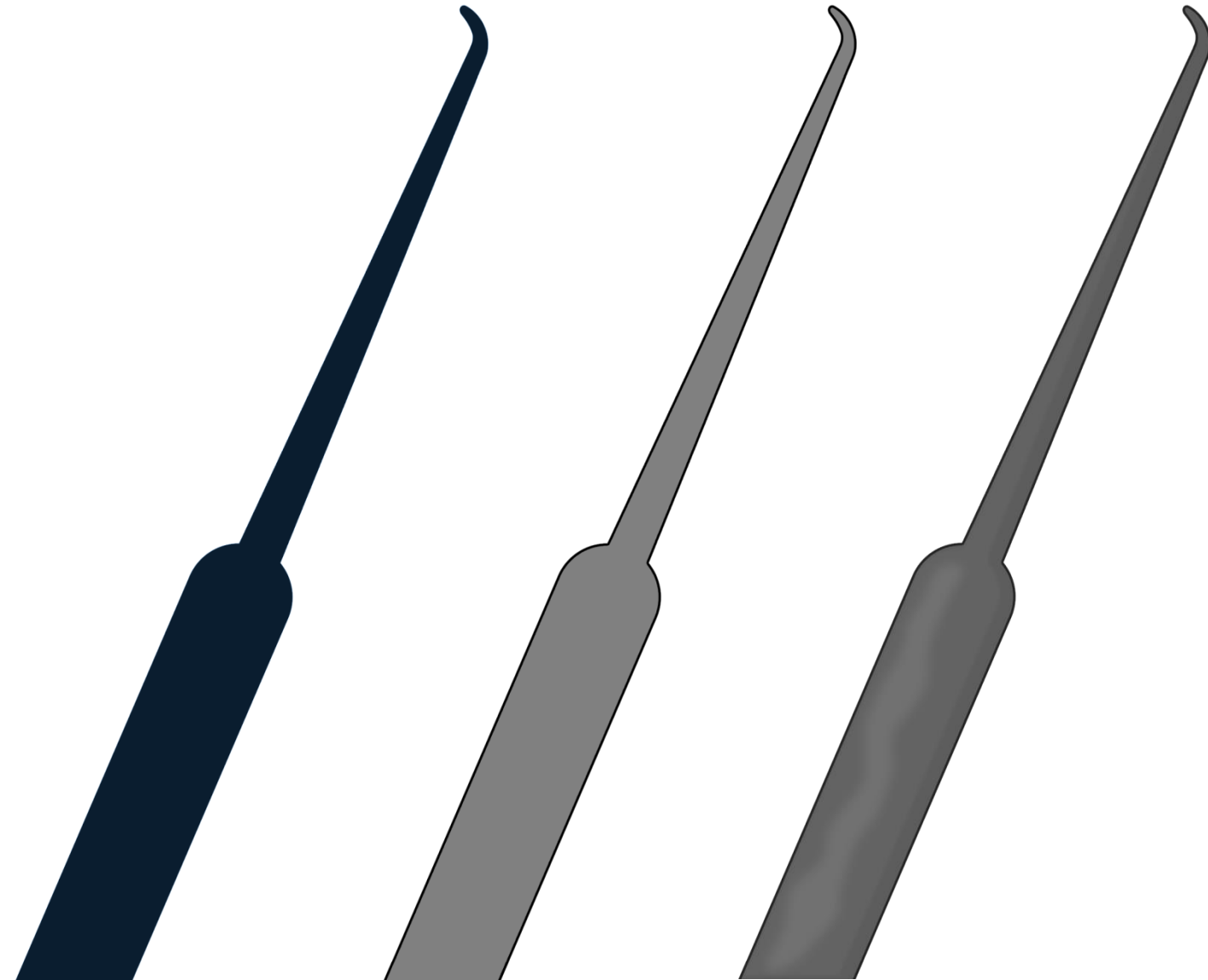
# Stainless Steel

---



# Titanium

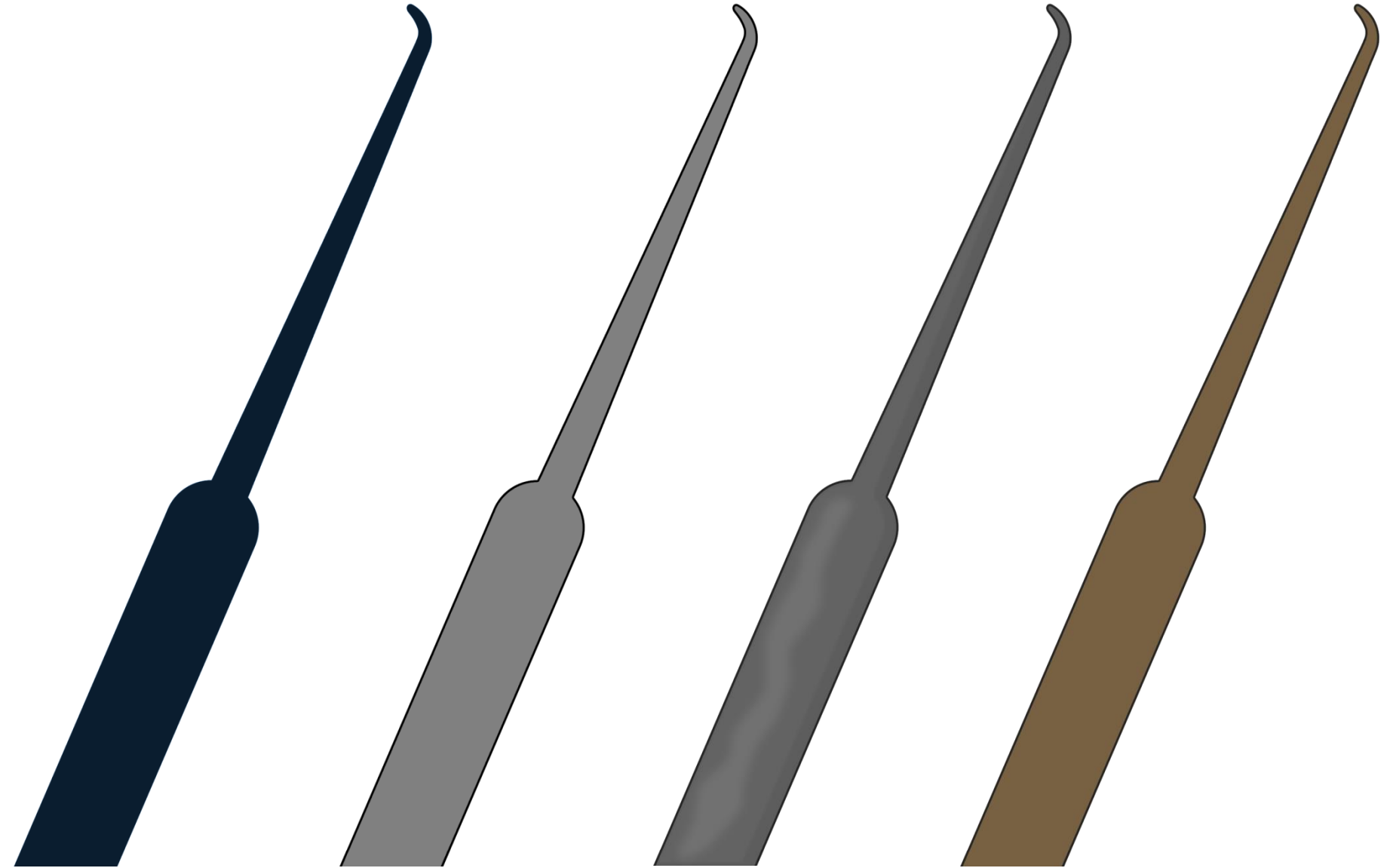
---





# Other Metals?

---



# Thickness

---



0.015" – Peterson "Government Steel"

0.020" – SouthOrd, Rytan, Southern Specialties, TOOOL

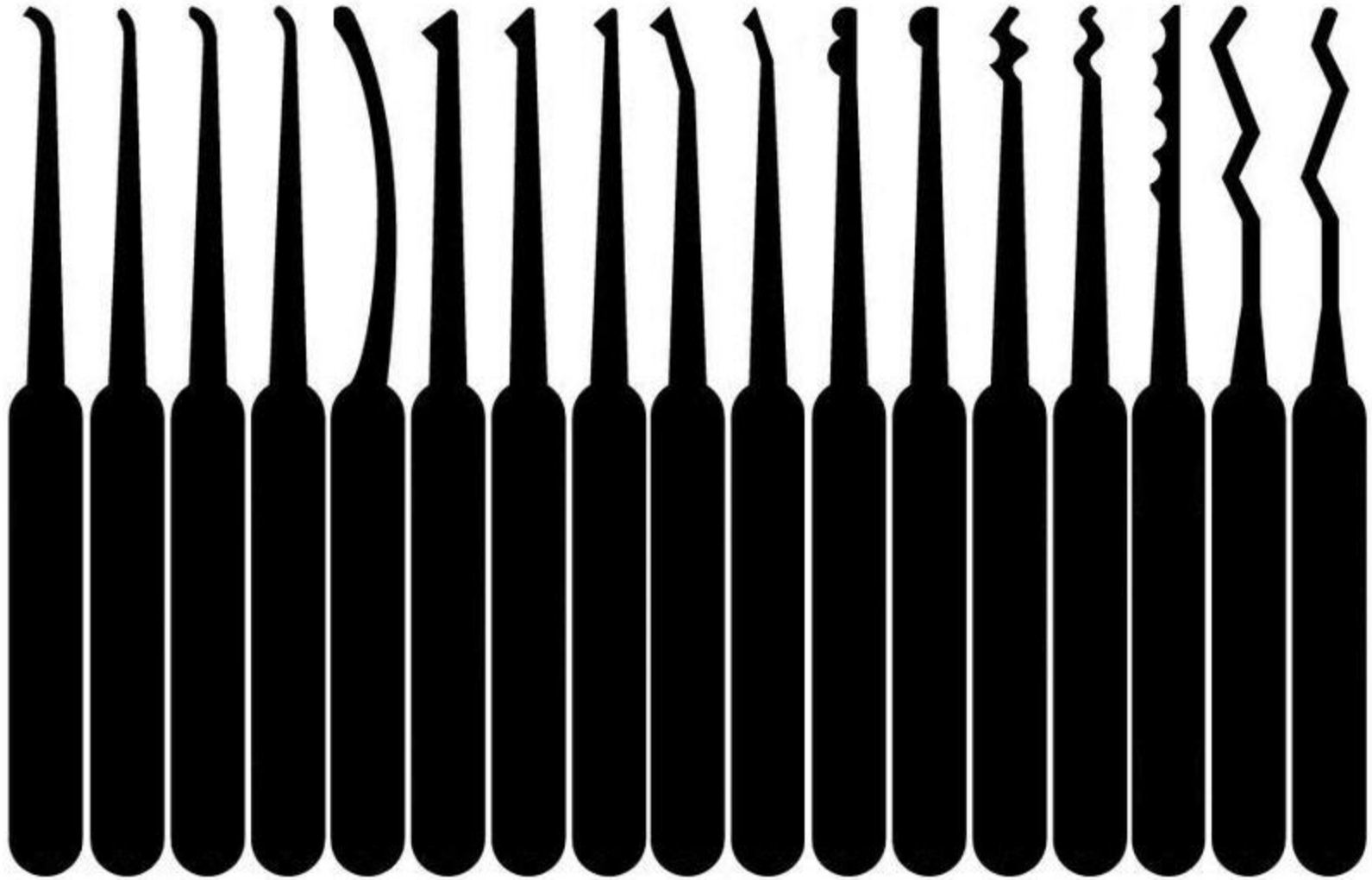
0.022" – HPC Stainless

0.025" – original TOOOL kits

0.028" – HPC Spring Steel

# The *real* confusing mess... Categories & Names

---



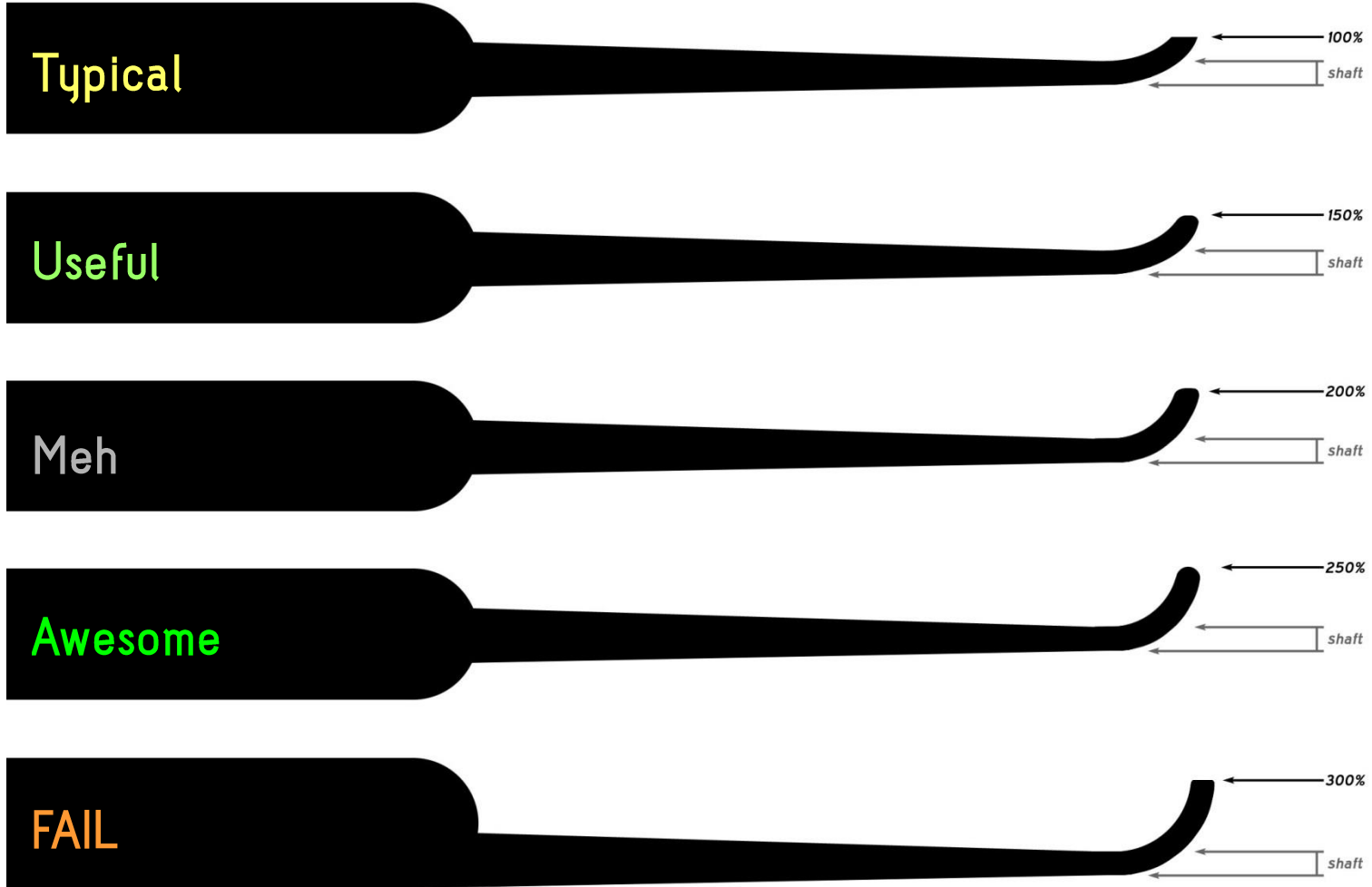
# Hooks (a.k.a. Lifters)

---



# Hooks (a.k.a. Lifters)

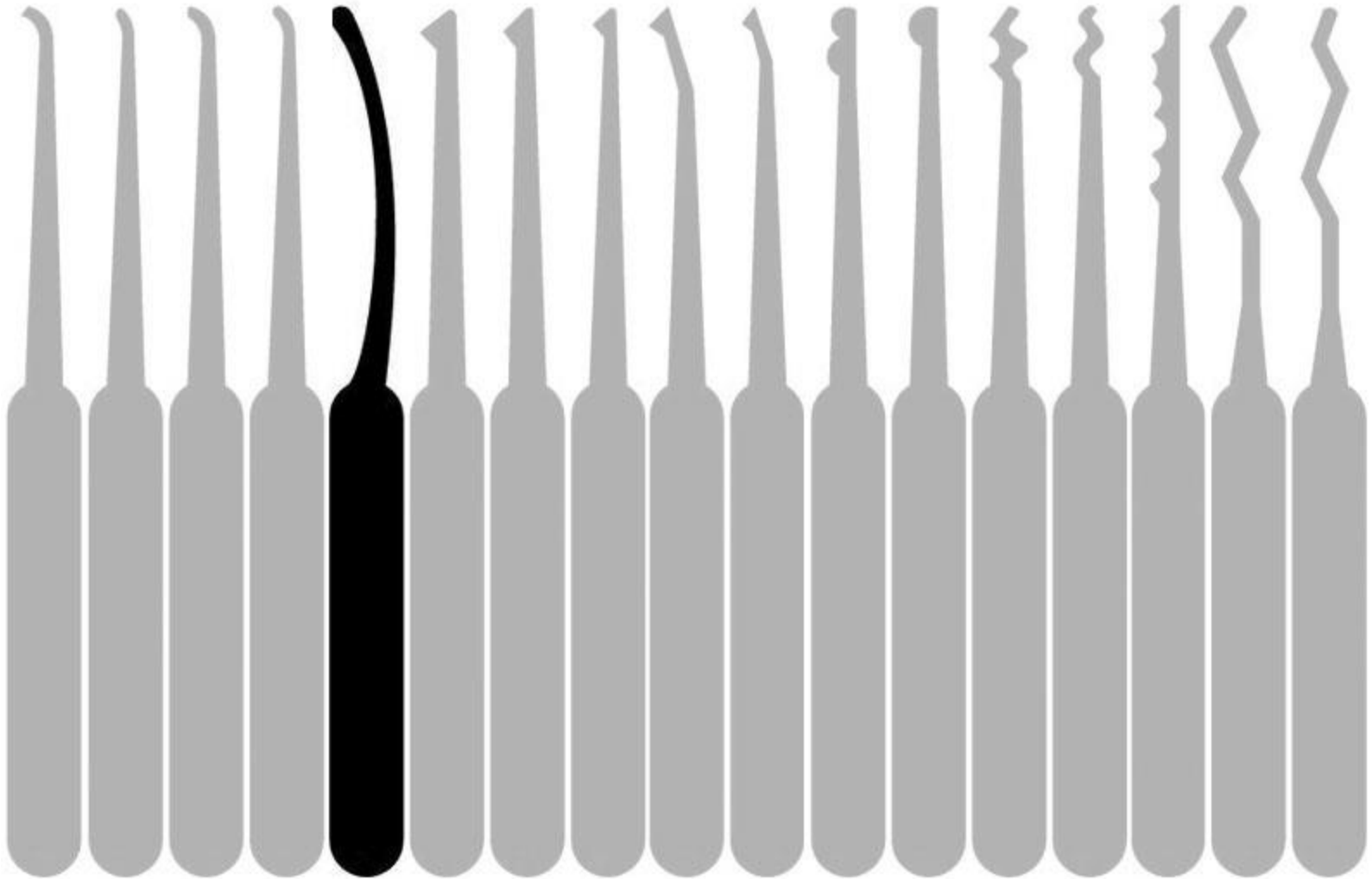
---





What would you call these?

---



# Reach Tools

---

**Deep Curve**

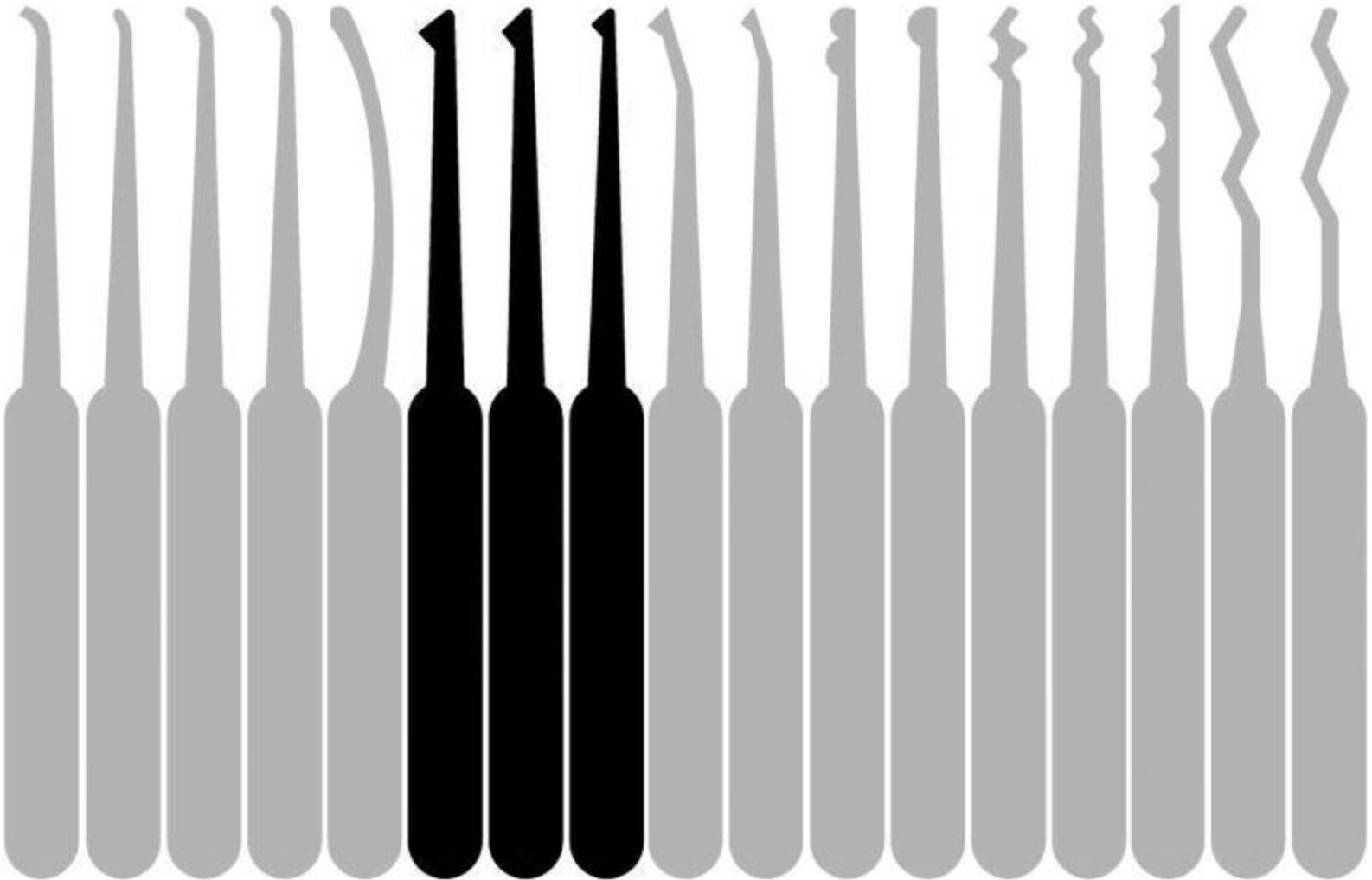


**Hybrid**



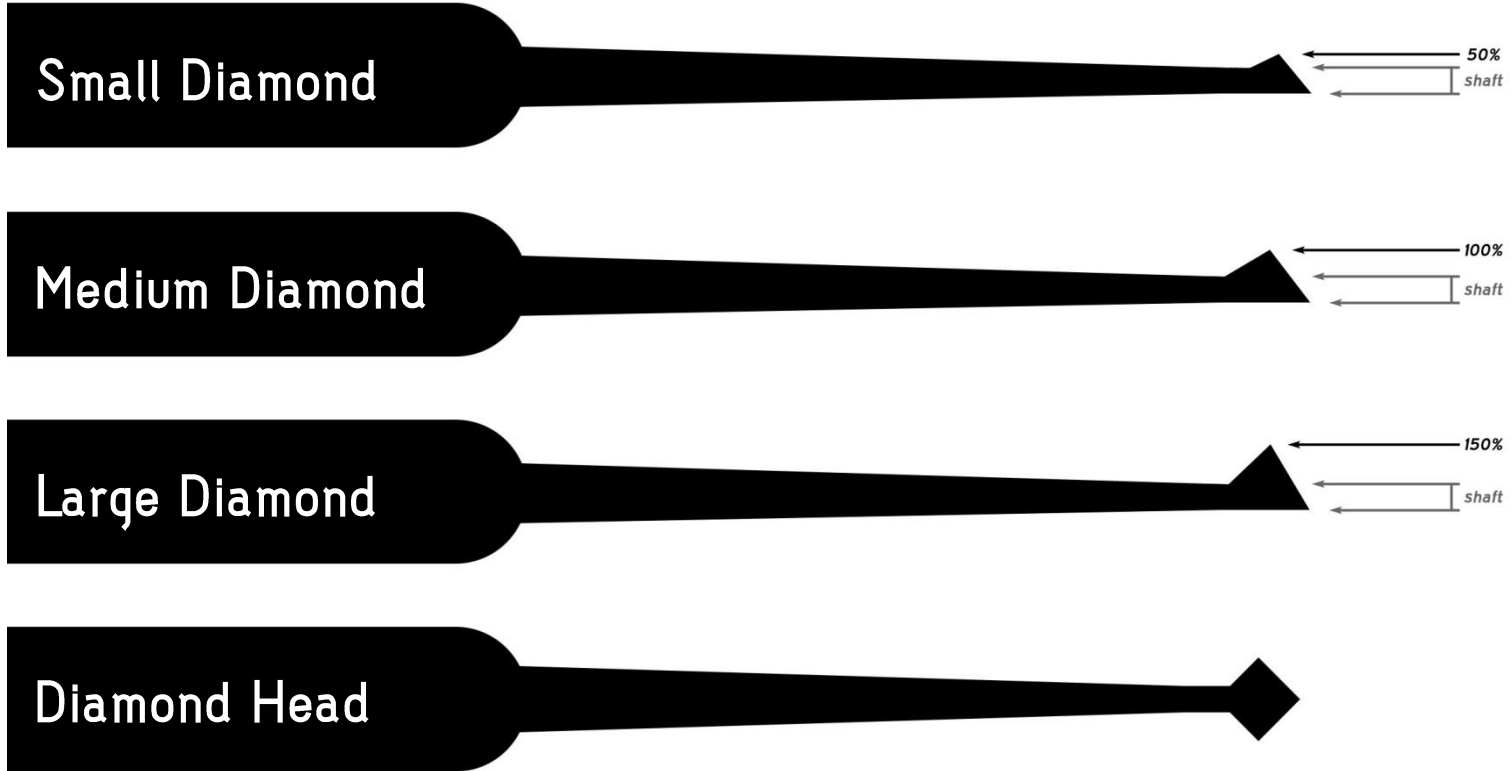
You've all seen these...

---



# Diamonds

---



# Diamonds

---

Maybe

← 50%  
← shaft

Yes

← 100%  
← shaft

No

← 150%  
← shaft

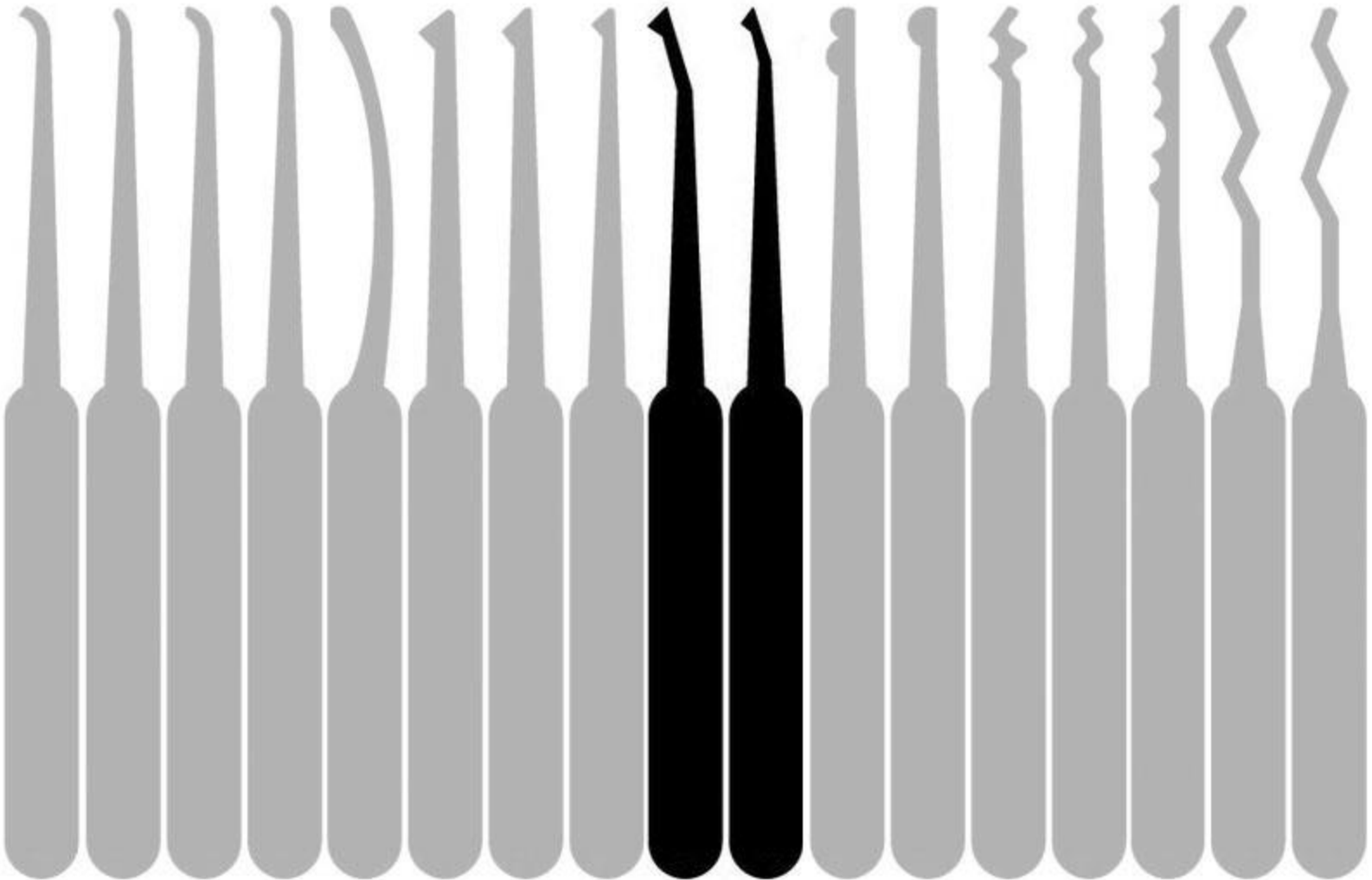
Dear God, Why??





How would you categorize *these...*?

---



# Offset Tools

---

Offset Diamond



Offset Ball



Offset Snake



# Offset Tools

---

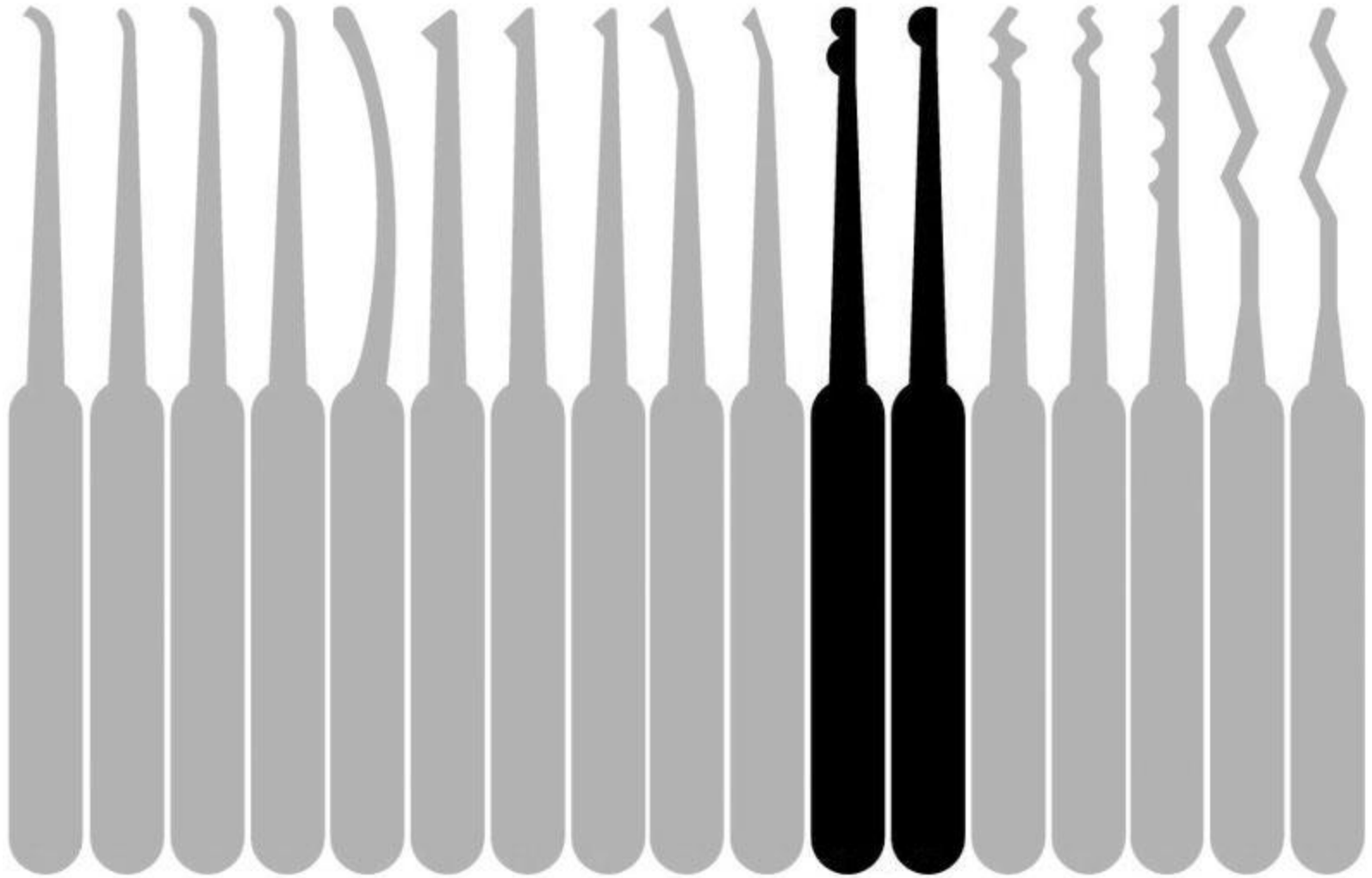
Yeah, sure.

Meh, why not?

I suppose.

Balls, balls, balls...

---



# Balls, balls, balls...

---

Single Ball

Snowman

Half Snowman

Half Ball





# Balls, balls, balls...

---

Pretty Useless

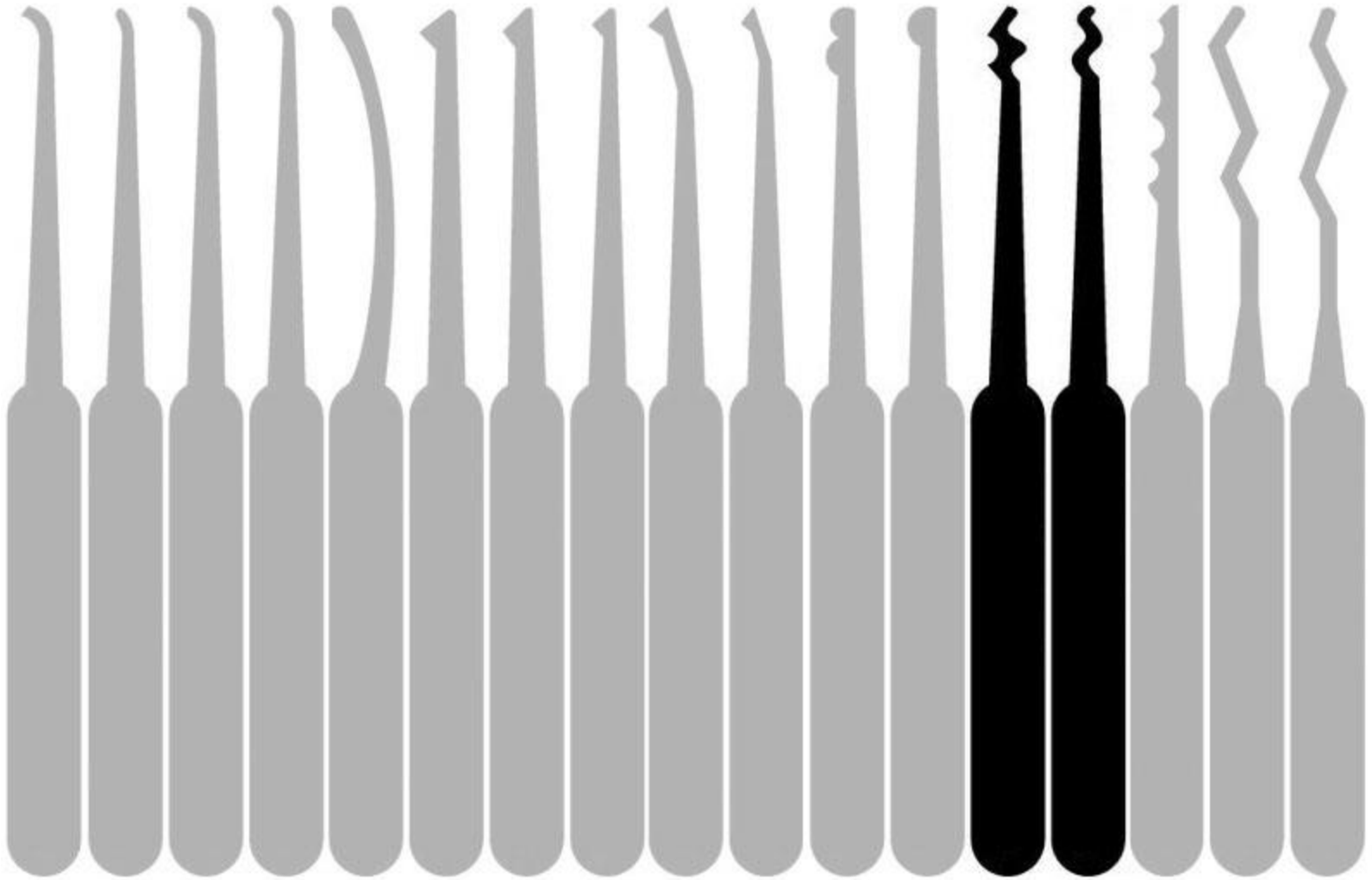
Can Be Useful

Tight Spaces?

We Will Mock You

What would you call these?

---



# Raking tools... Welcome to Crazy Land

---



# Raking Tools

---

Snake



a.k.a. C Rake, Double Rake

Three Quarter Snake



a.k.a. Rake-and-a-Half

Half Snake



a.k.a. Single Rake

Double Snake



a.k.a. Quad Rake

Stretched Snake



a.k.a. S Rake

Batarang



a.k.a. S Rake, Camel Back

# Raking Tools

---

Snake



a.k.a. C Rake, Double Rake

Three Quarter Snake



a.k.a. Rake-and-a-Half

Half Snake



a.k.a. Single Rake

Double Snake



a.k.a. Quad Rake

Stretched Snake



a.k.a. S Rake

Batarang



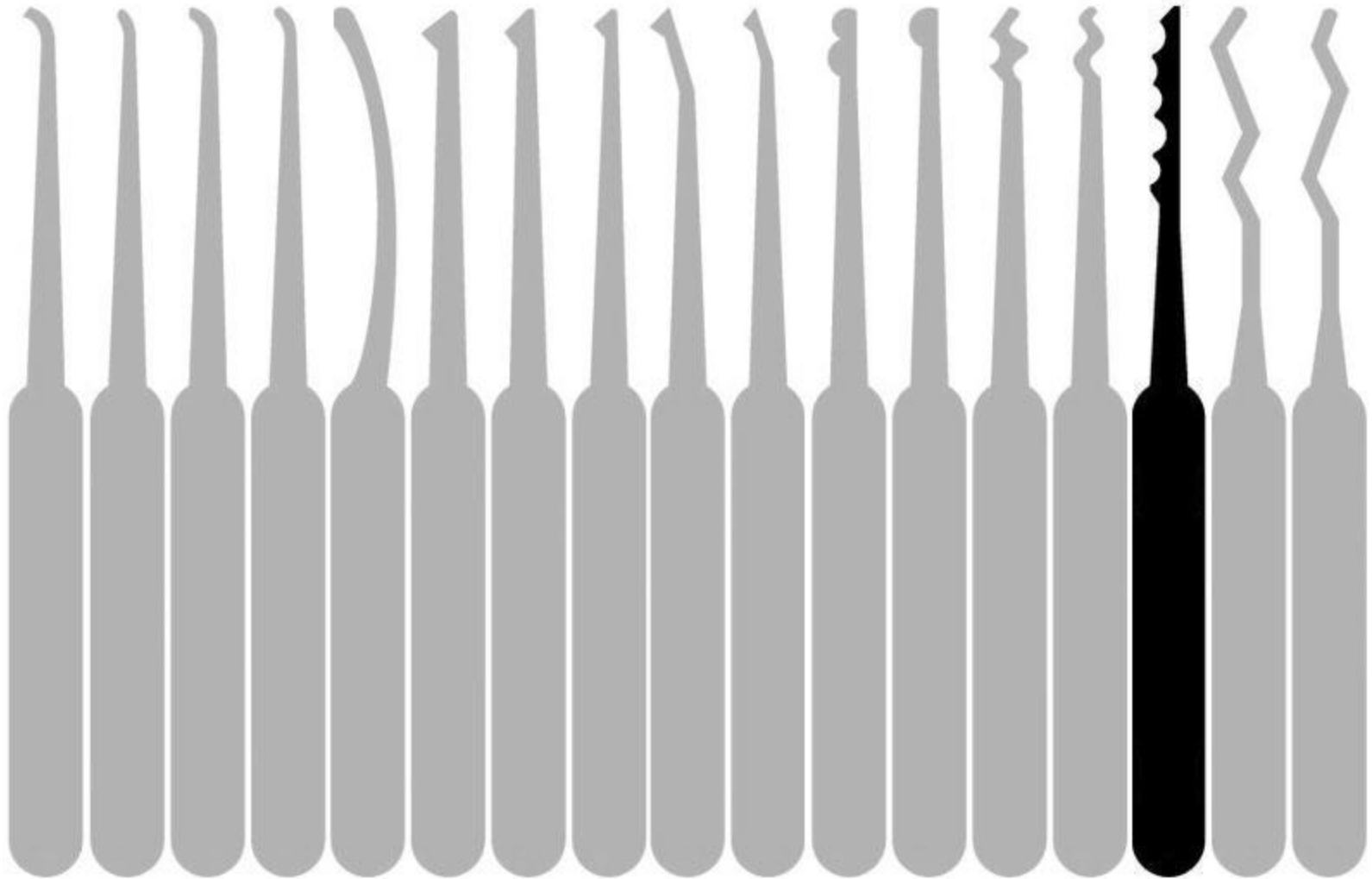
a.k.a. S Rake, Camel Back

*Dangerous Weakness*



What about something like *this...*

---



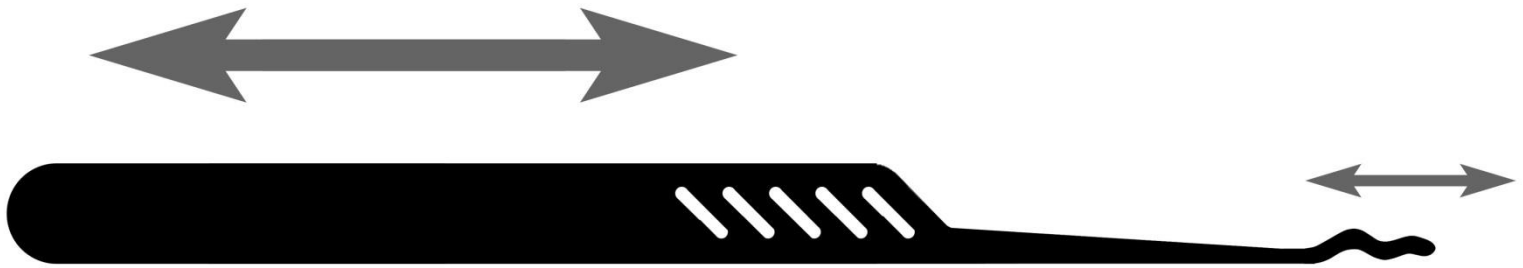
# “Raking” vs. “Lifting”

---



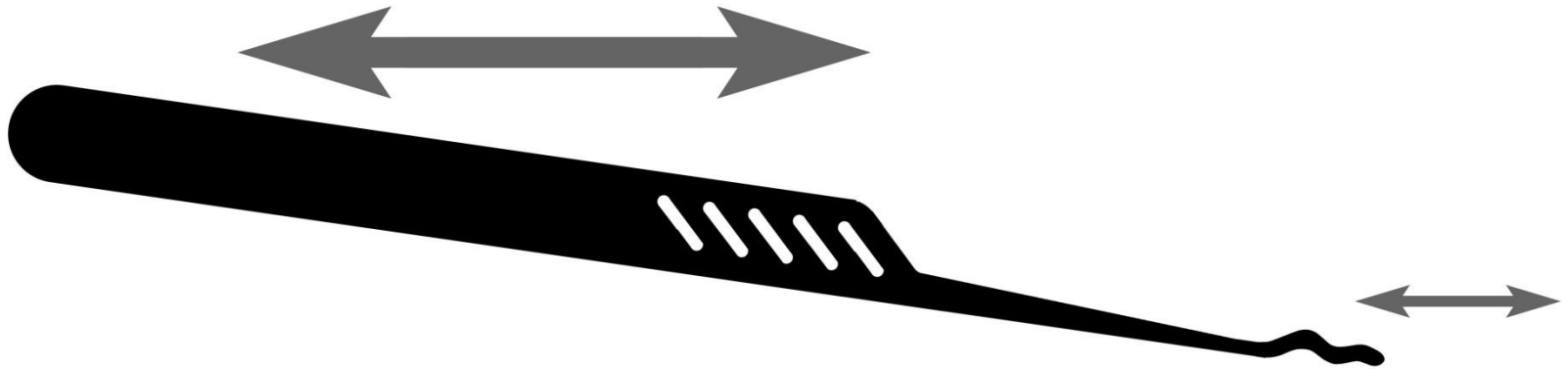
# Raking

---



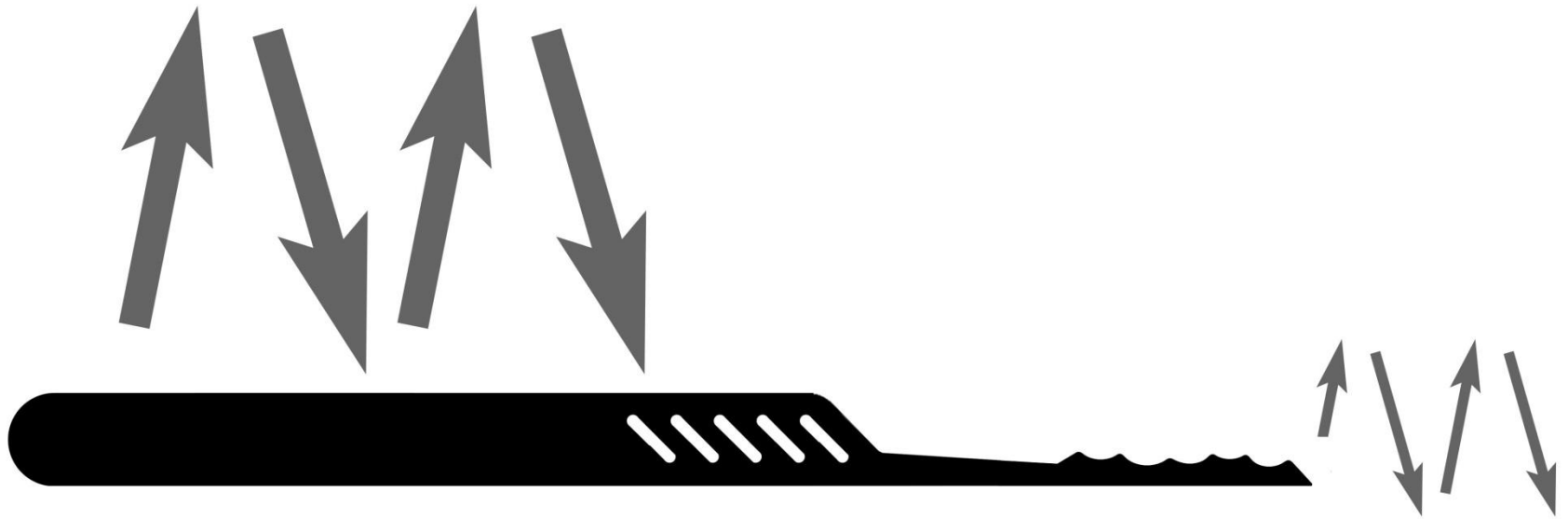
# Raking

---



# Lifting

---



# Jagged Lifters

---

Wedge Rake

a.k.a. W Rake, Short Jag,  
Ramped Tool, & Stupid

Long Rake

a.k.a. L Rake, Long Jag,  
Ripple, & Saw Tooth

Falle Slope

Falle Valley

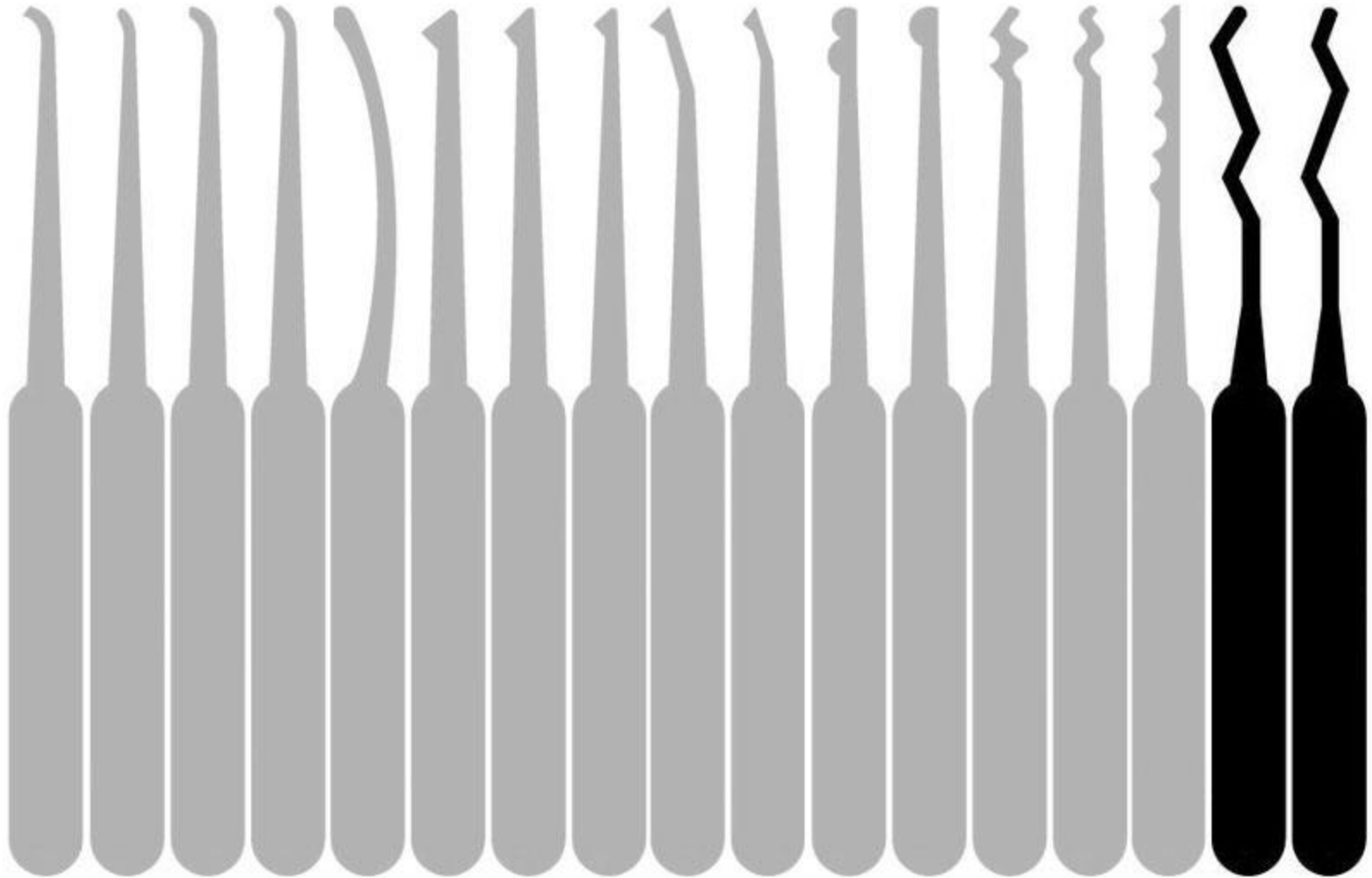
Falle Hump

a.k.a. Long Rimple



So, what on earth are *these*?

---



# King & Queen

---



King Pick



Queen Pick

# A major innovation in pick tools

---

*Thanks to Minnesota...*



*... with a nod to Colombia*

# Raimundo's Family of Tools

---



# It Started with Two Tools...

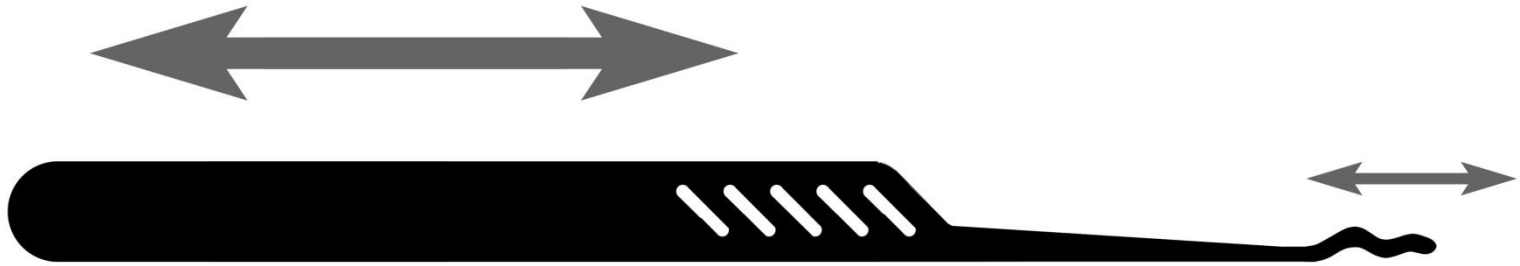
---



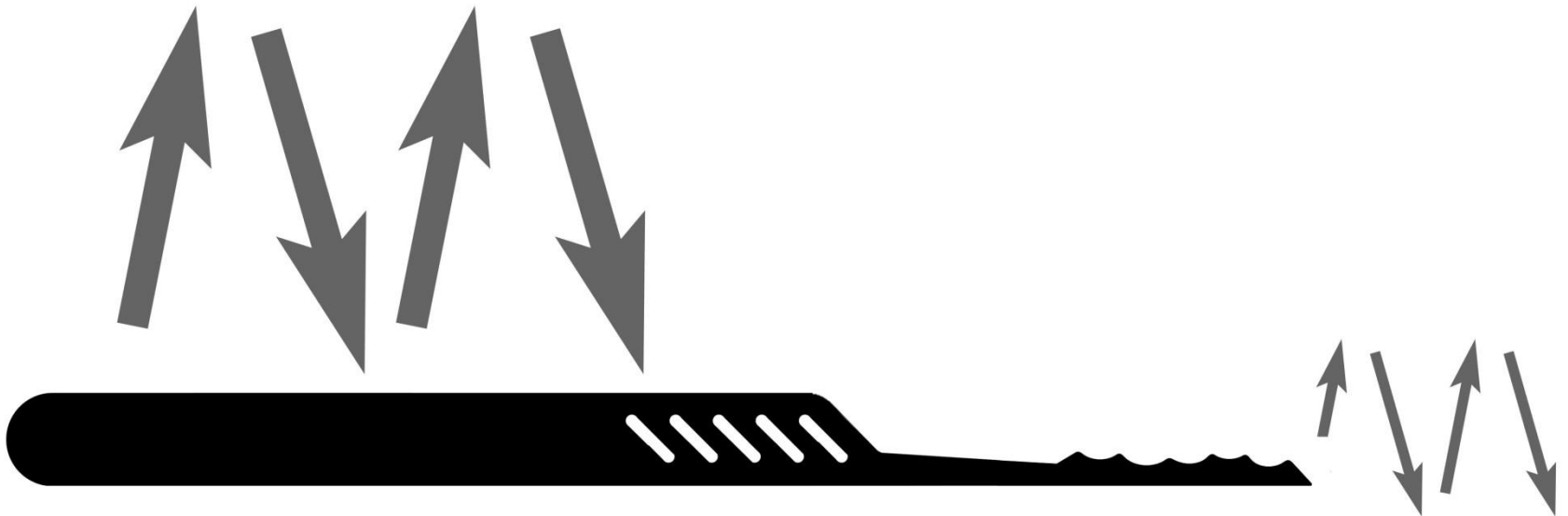
“Jiggler” Tools

# What is Jigging?

---



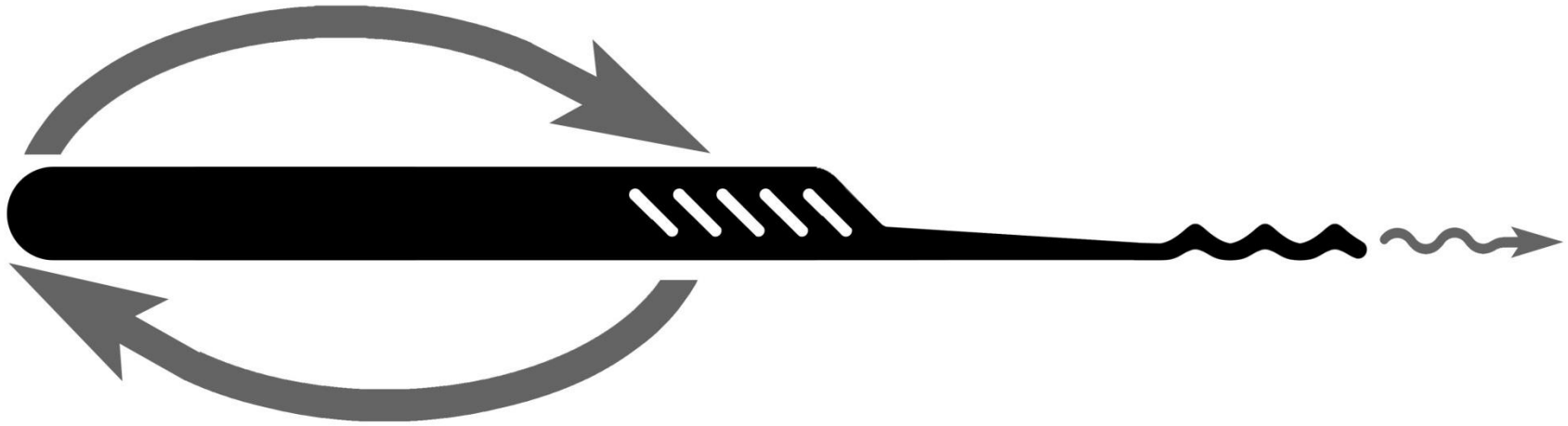
In Between Raking & Lifting...





# What is Jigging?

---



... There is "Jigging"

# Bogotá Family

---



Bogotá



Single Hump a.k.a. Hollow Half Diamond



# Bogotá Family

---



Bogotá



Single Hump a.k.a. Hollow Half Diamond



Two Hump a.k.a. Camel



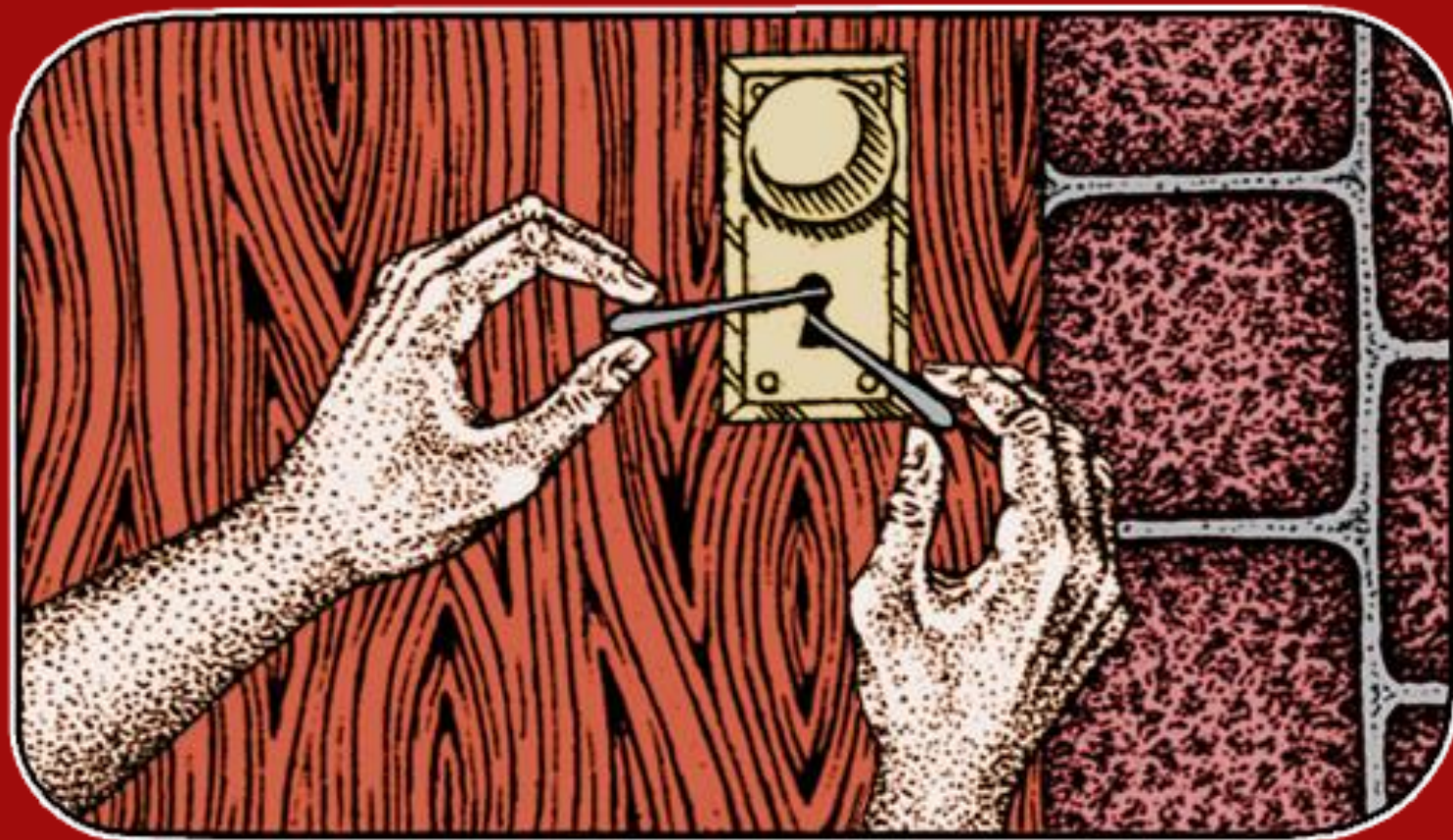
Quad Hump



Sabana

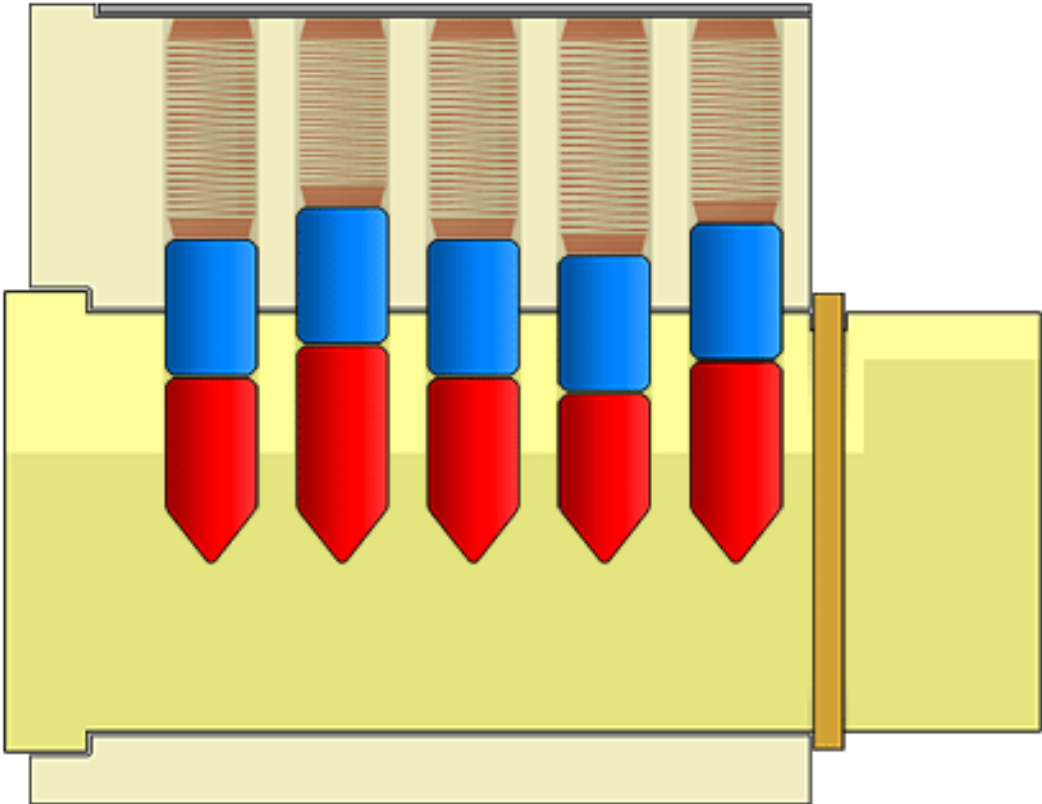
<http://theamazingking.com/bogota.html>

# Lockpicking & Forensics



# Keys Touch Very Specific Places

---





# Virgin Pins Have Specific Patterns From Manufacturing

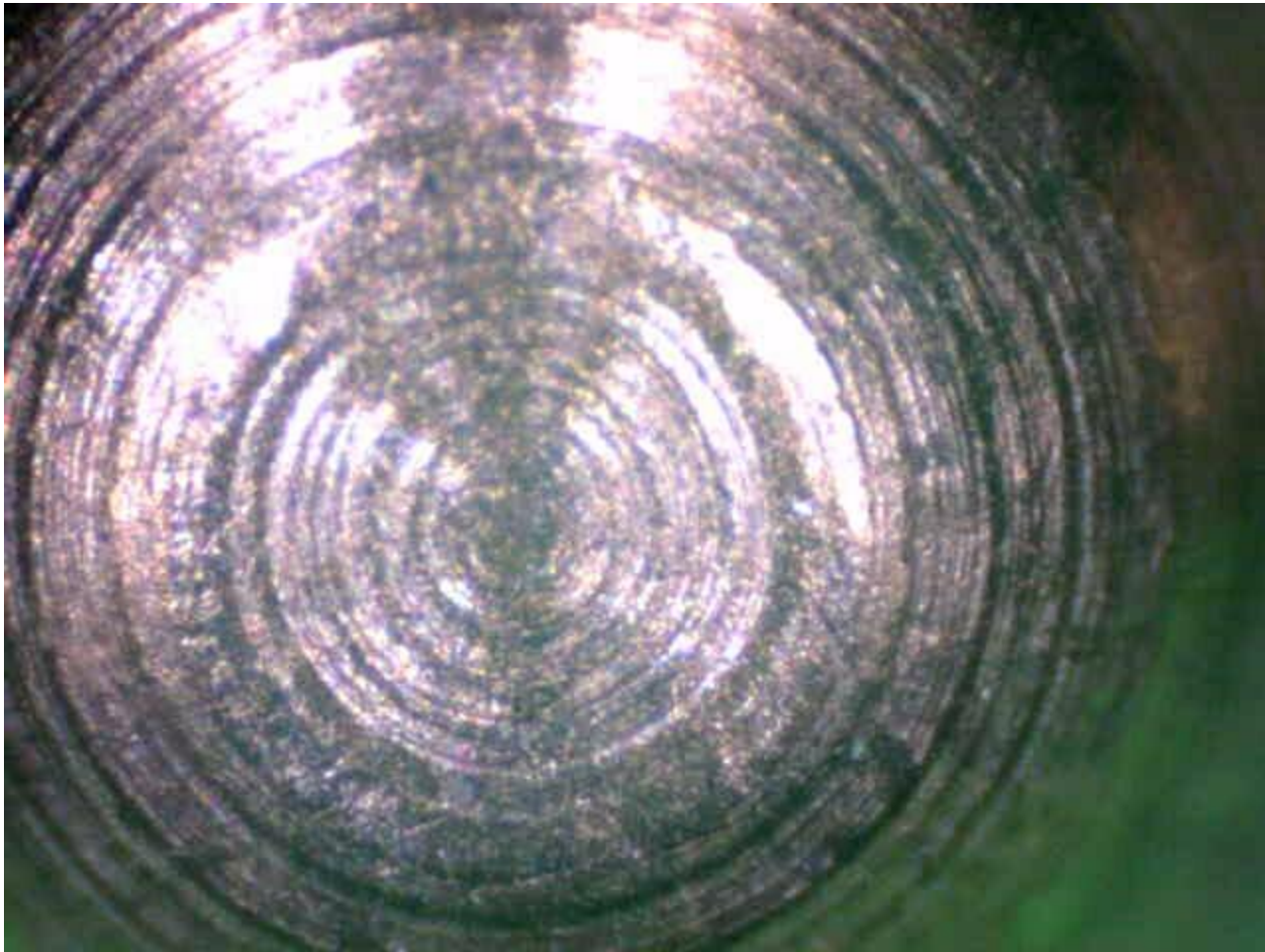
---





# Concentric Tiny Ridges on Pin Face

---



# Those Rings “Polish Away” With Use

---

250 Uses



# Those Rings "Polish Away" With Use

---

1500 Uses





# Those Rings “Polish Away” With Use

---

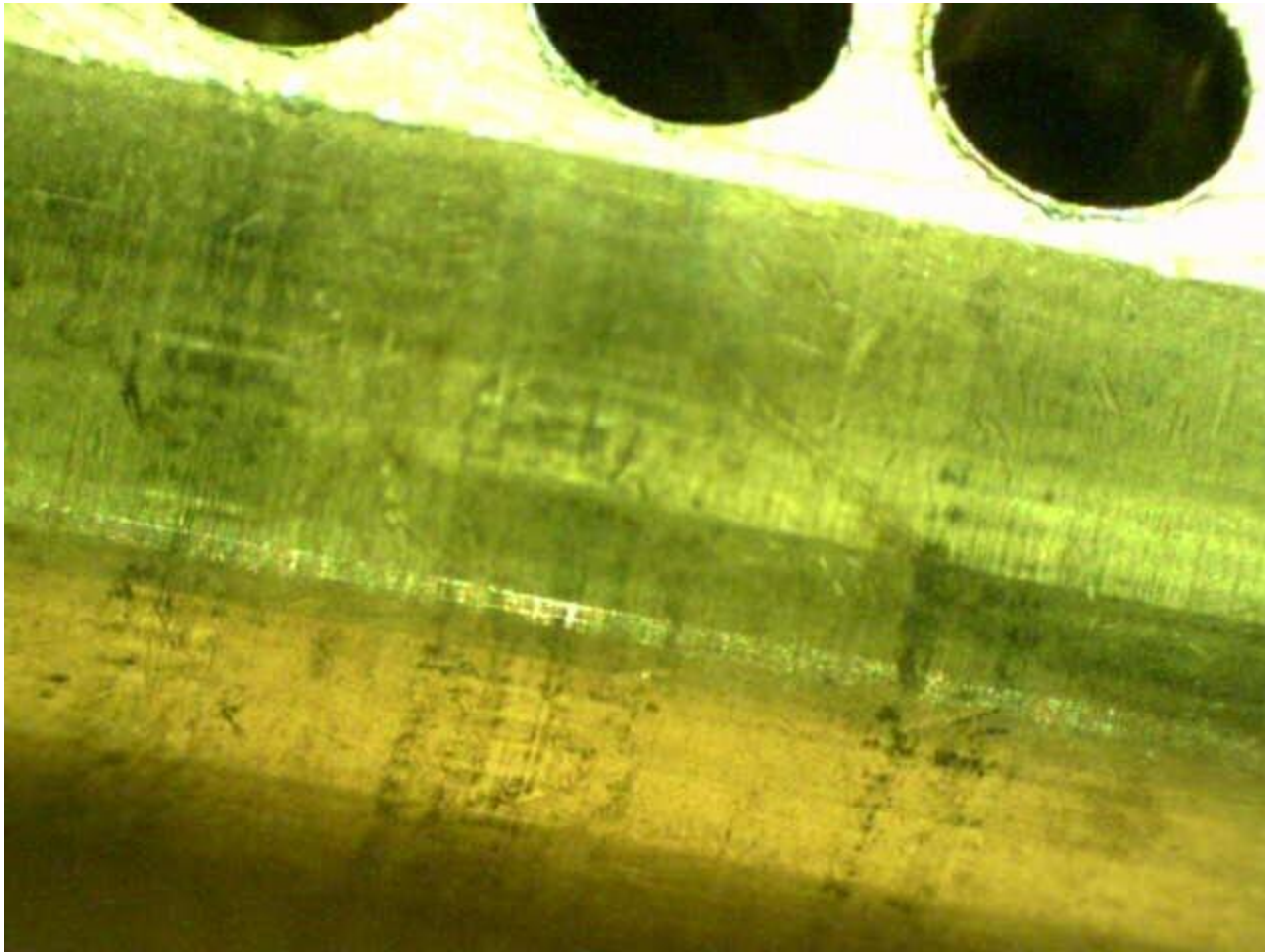
5000 Uses



# The Plug Picks Up Marks From Driver Pins

---

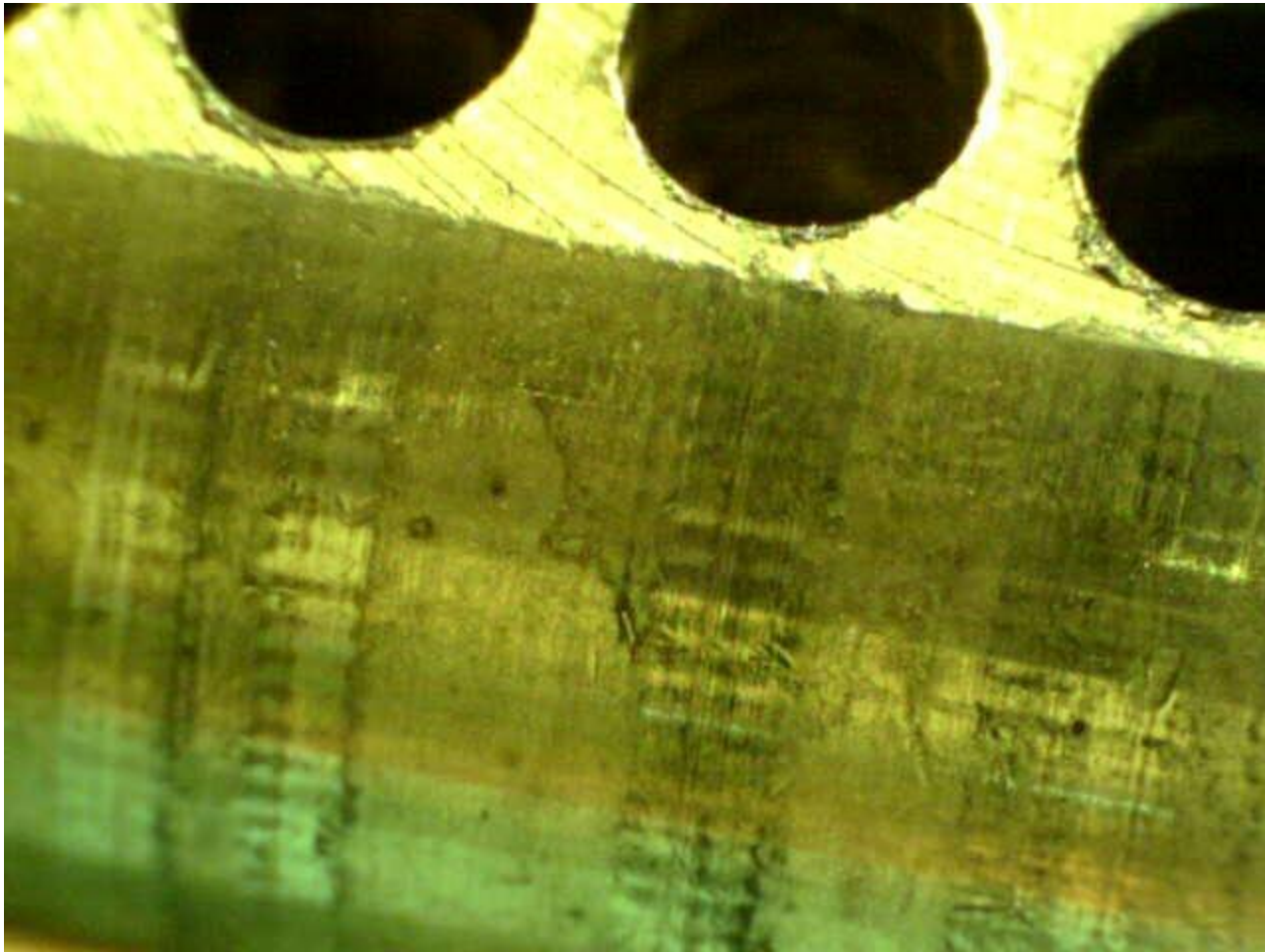
250 Uses



# The Plug Picks Up Marks From Driver Pins

---

1500 Uses

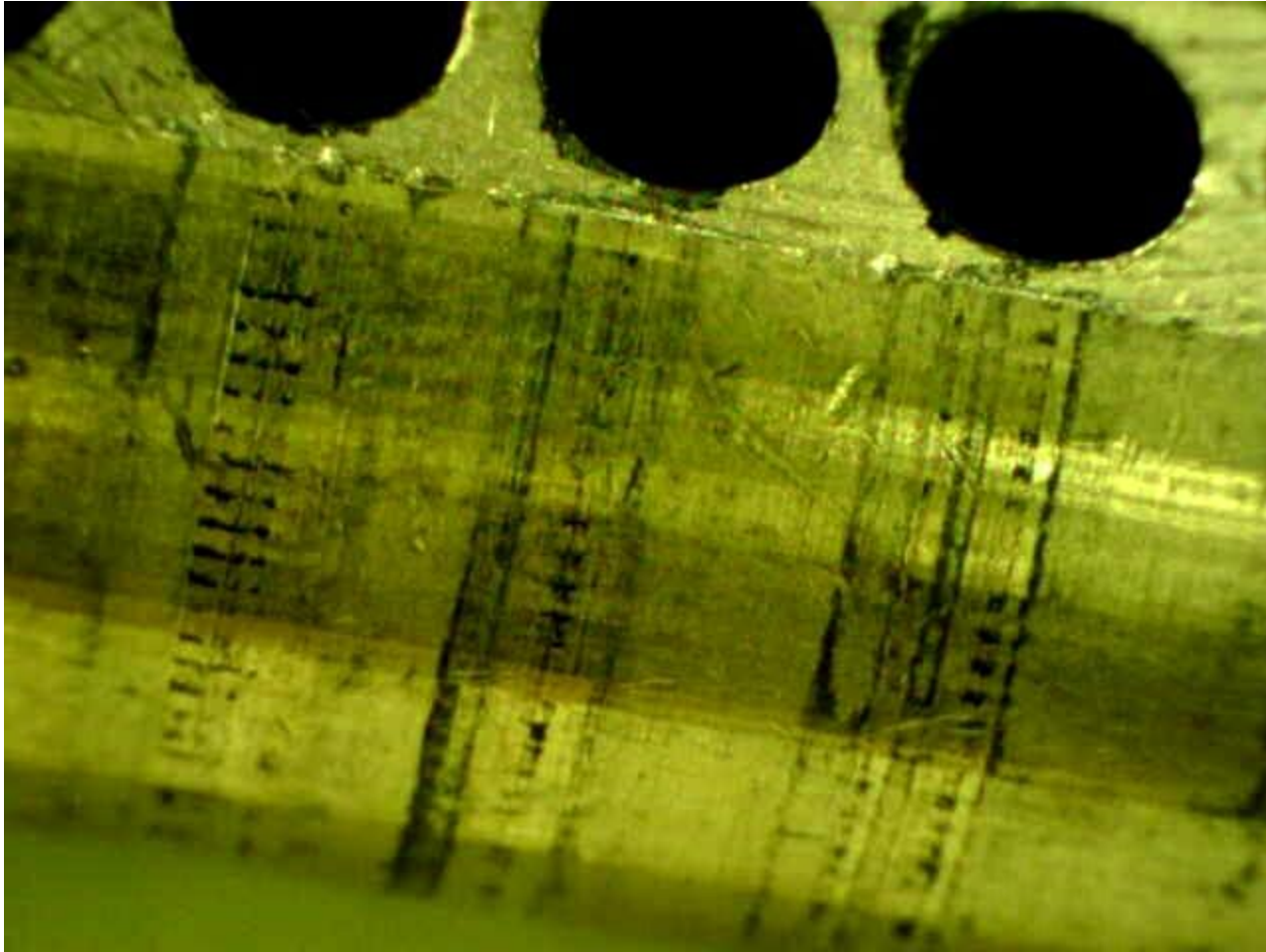




# The Plug Picks Up Marks From Driver Pins

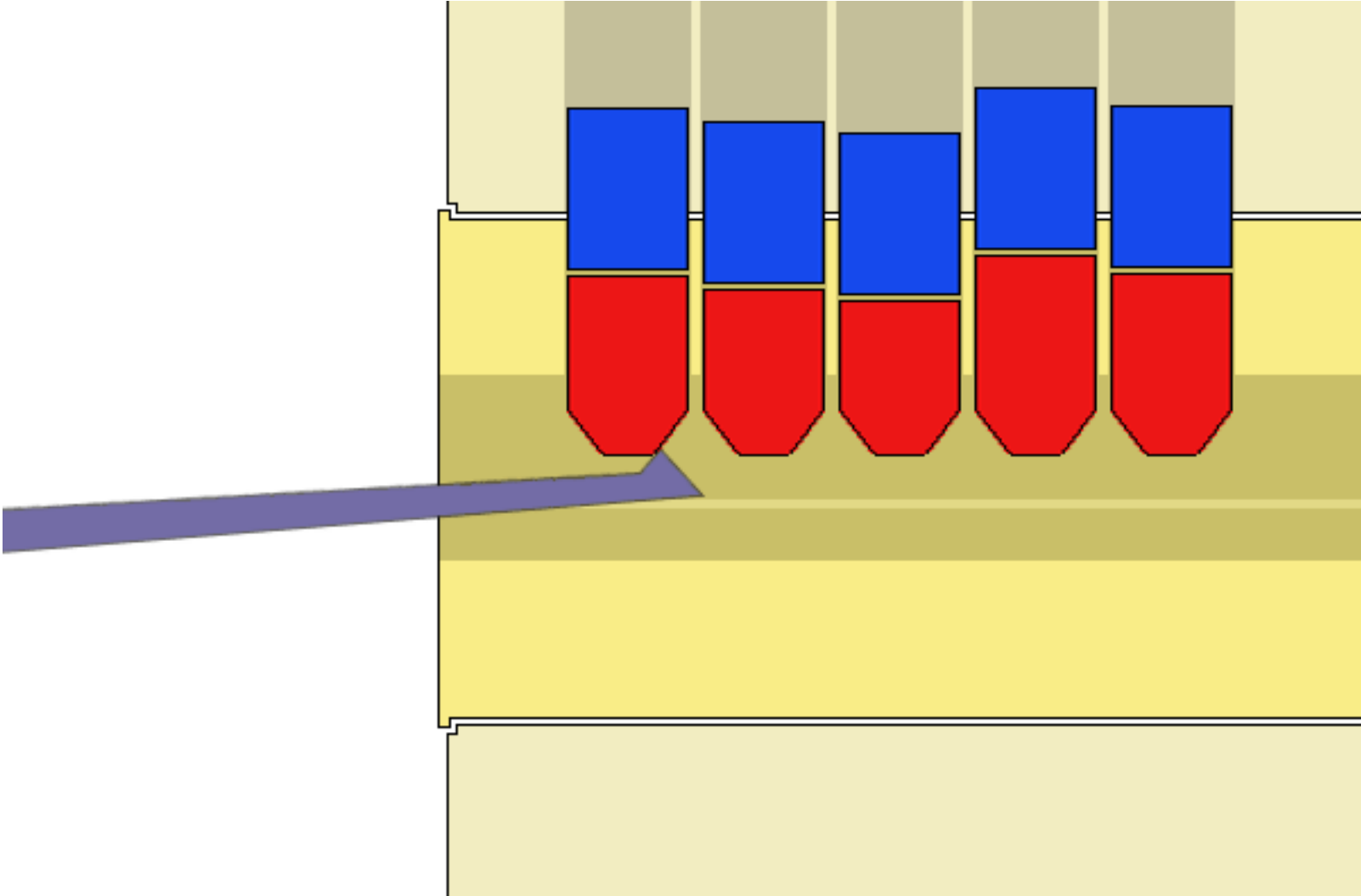
---

5000 Uses



# Picks Touch Places That Keys Don't

---



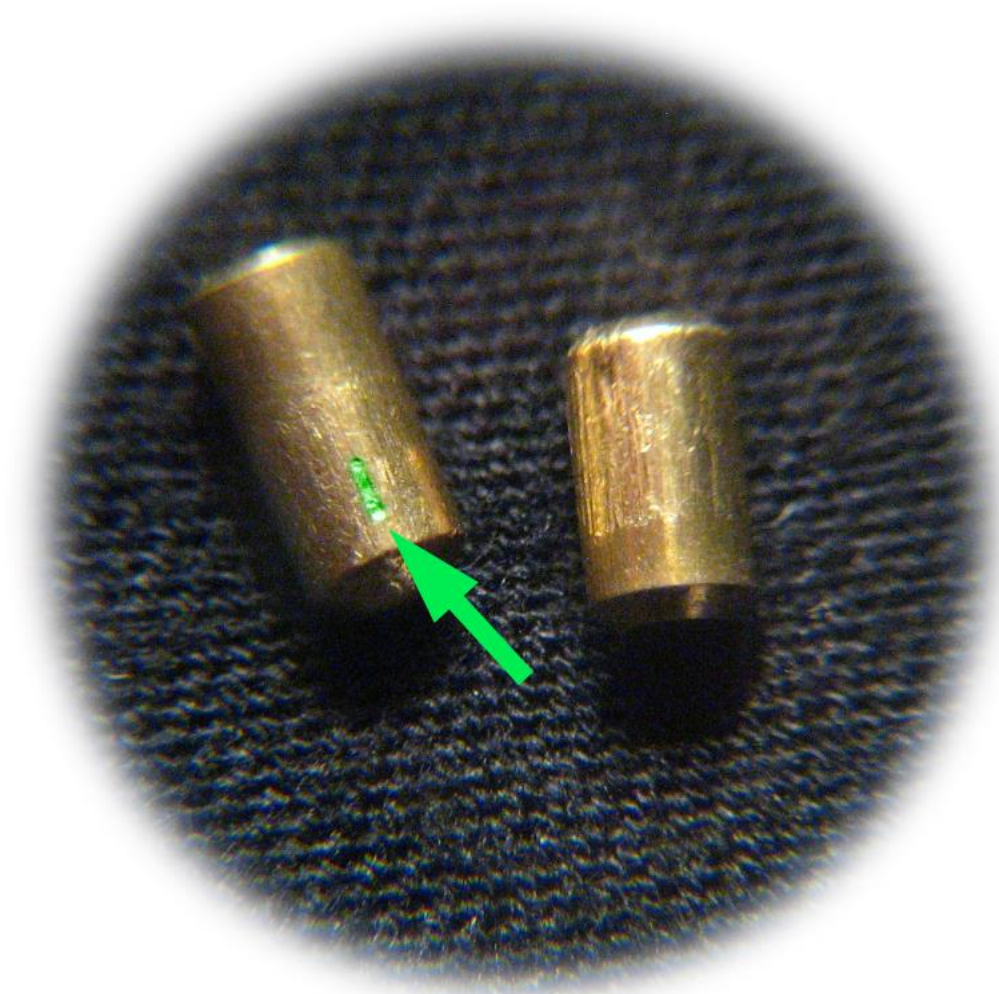
# Wear and Tear or Toolmarks?

---



# Wear and Tear or Toolmarks?

---





# Forensics — Lifting Picking

---



# Forensics — Raking

---





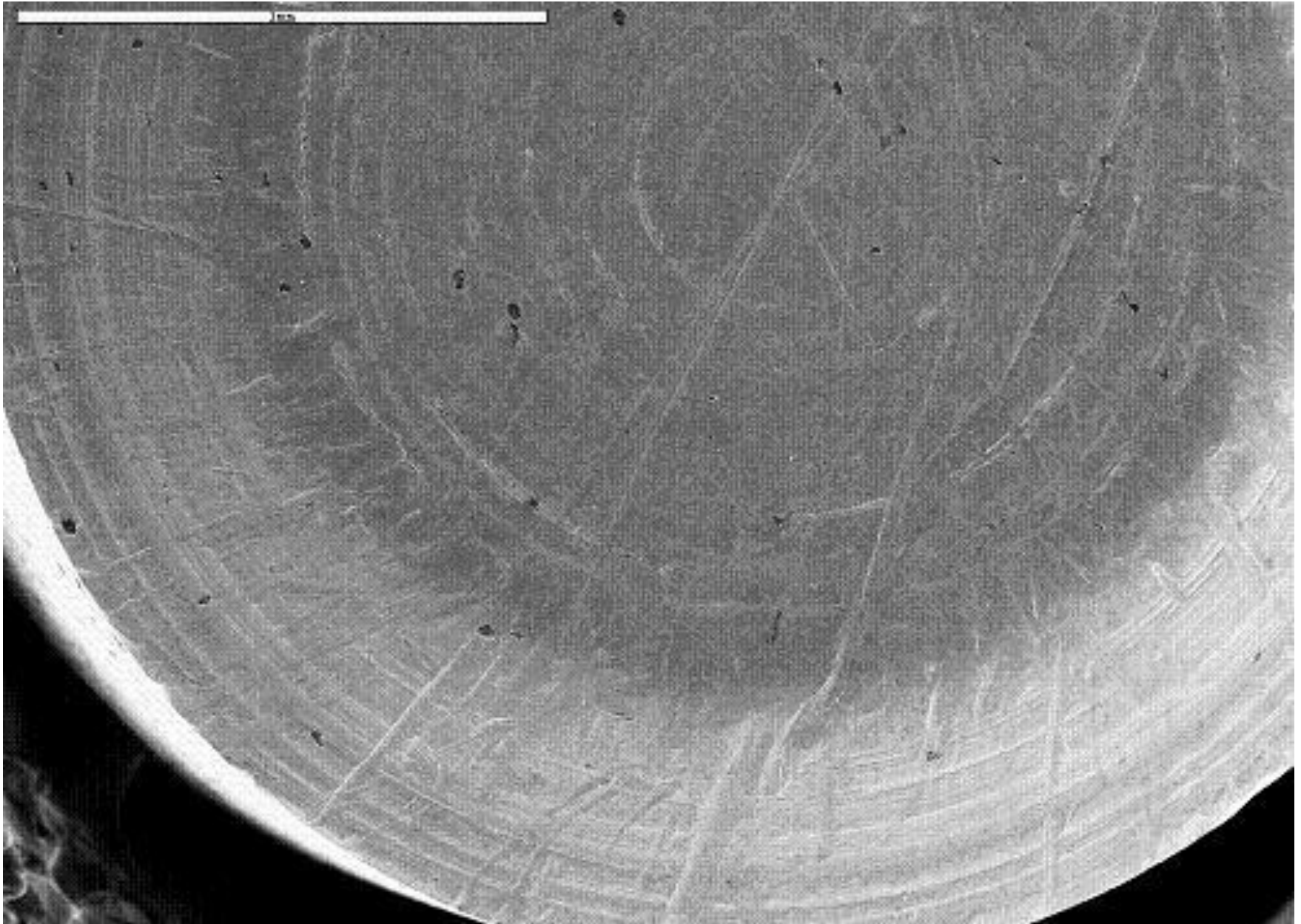
# Forensics — Mixed Styles of Picking

---



# Forensics — SEM - Picked

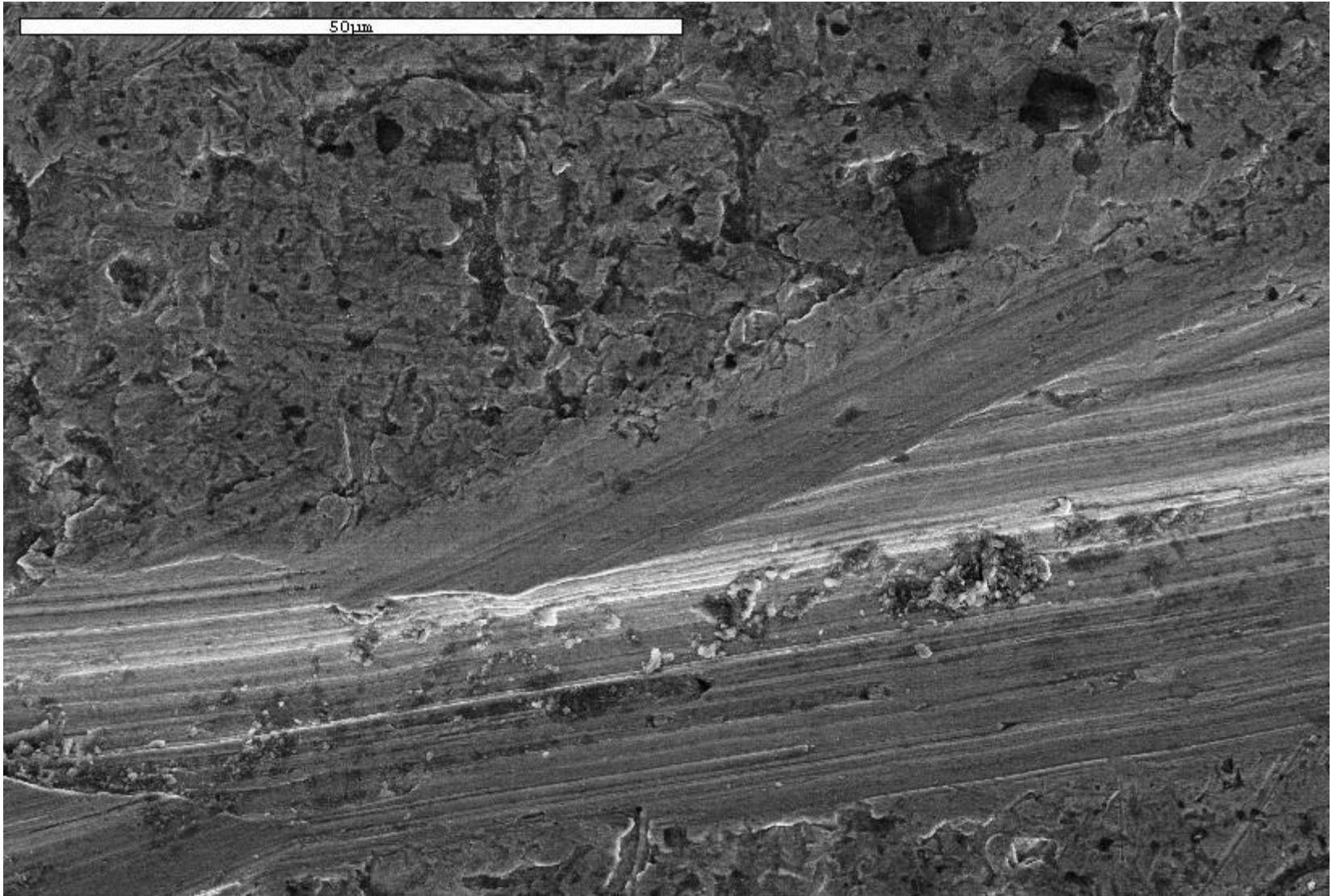
---





# Forensics — SEM — We must get closer...

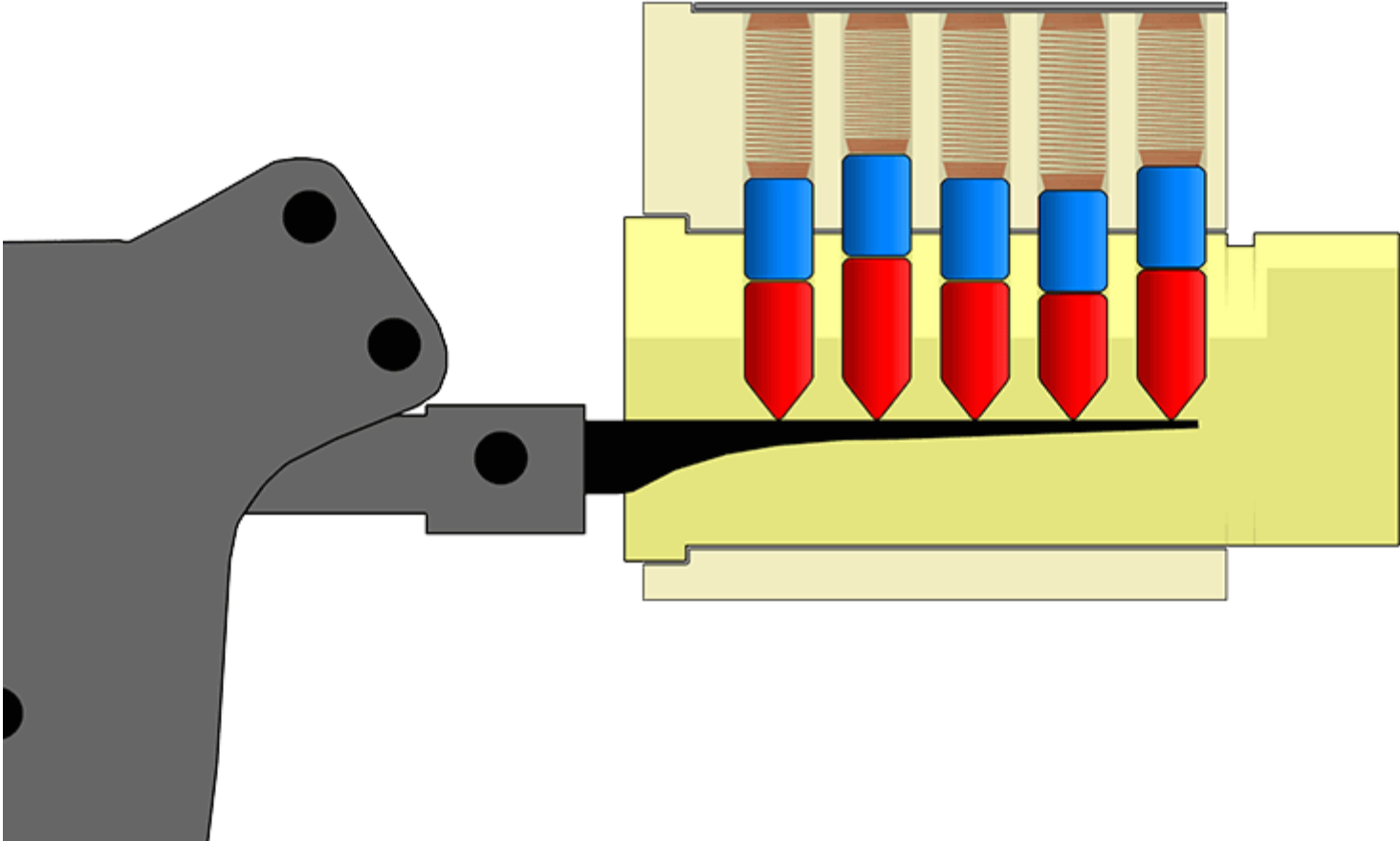
---



Source: Alcohol and access to a scanning electron microscope

# Forensics of Snapper Guns

---



# Repeated Snap Marks

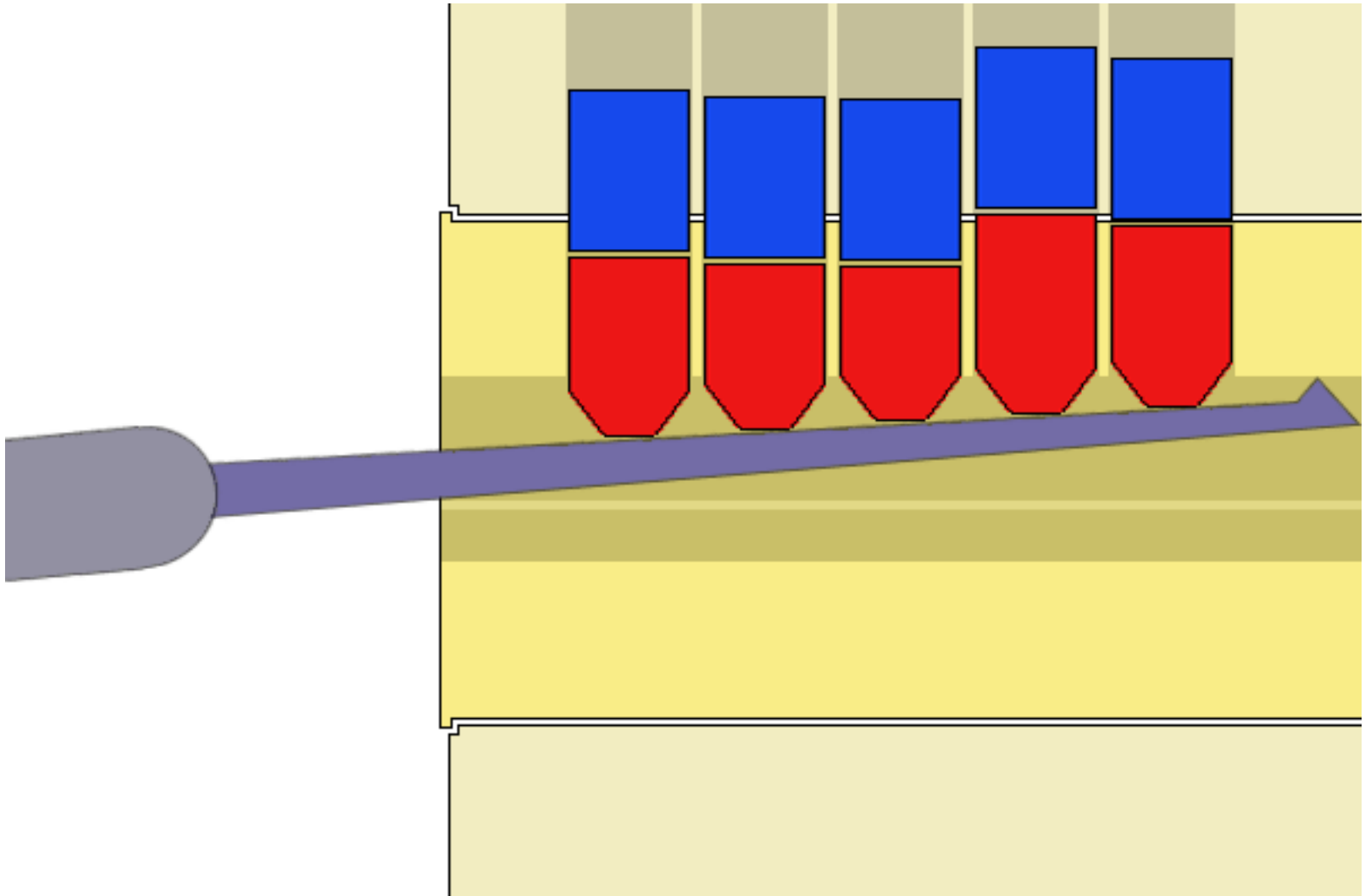
---





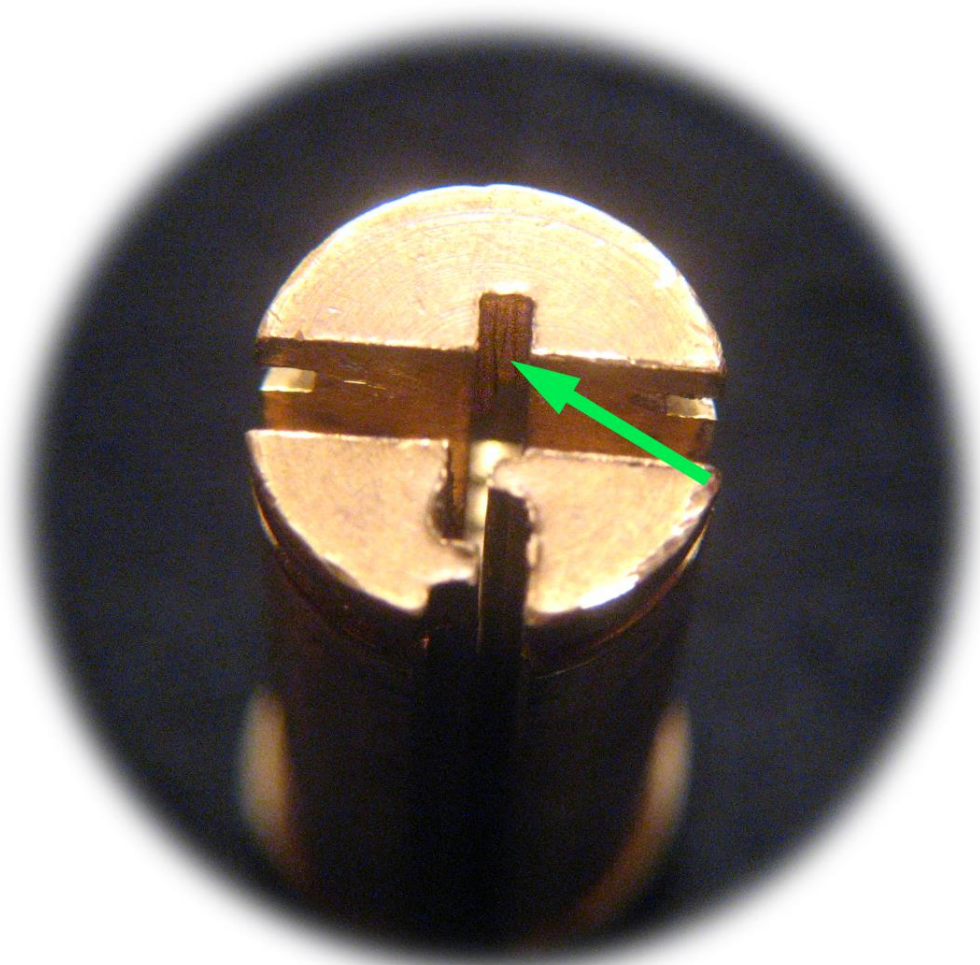
# Some People Poke Too Deep

---



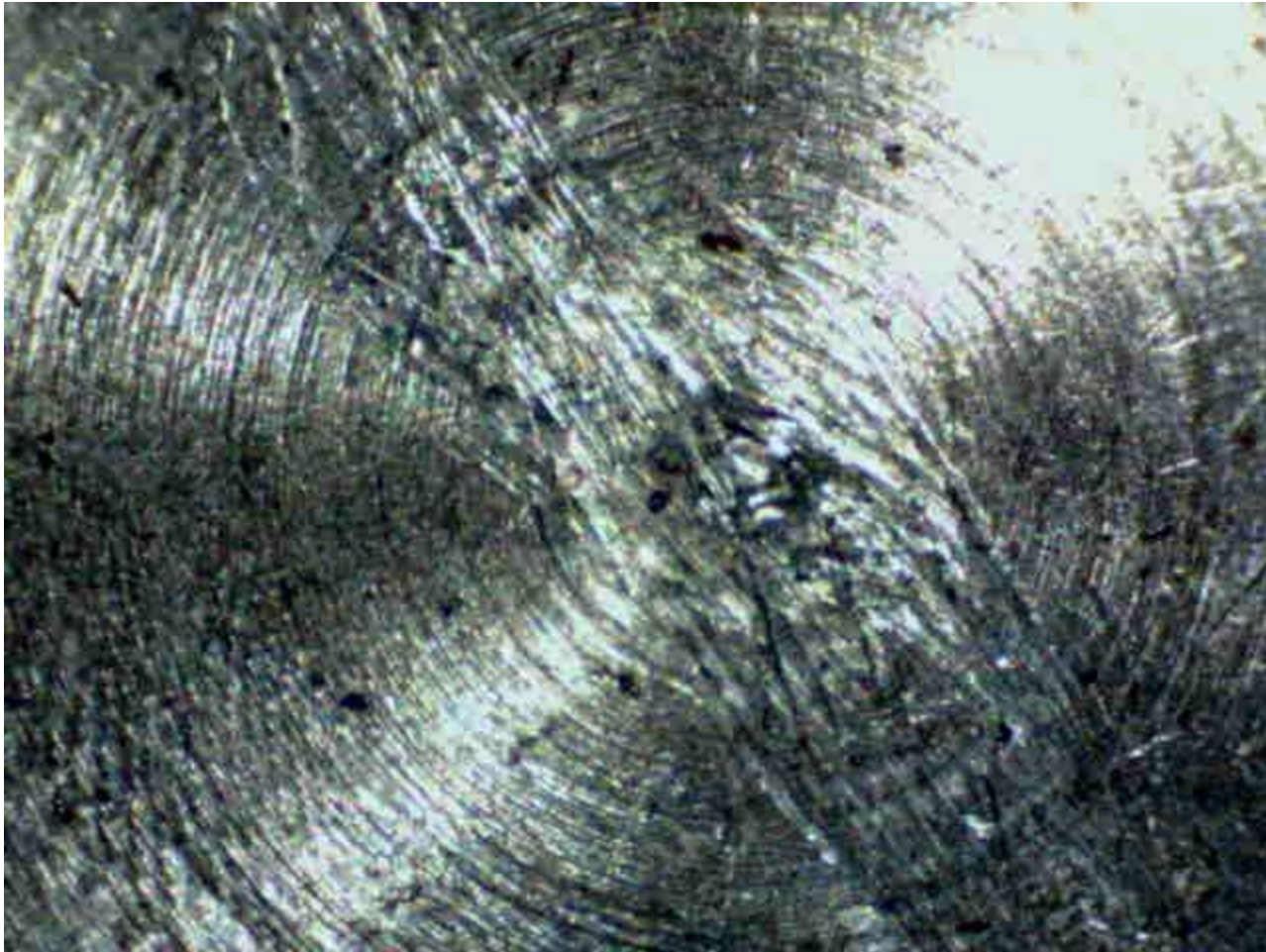
# Tools Too Deep — Marks in Rear Top of Keyway

---



# Tools in Too Deep – Marks on Tail Cap

---



# Tension Tools in the Keyway

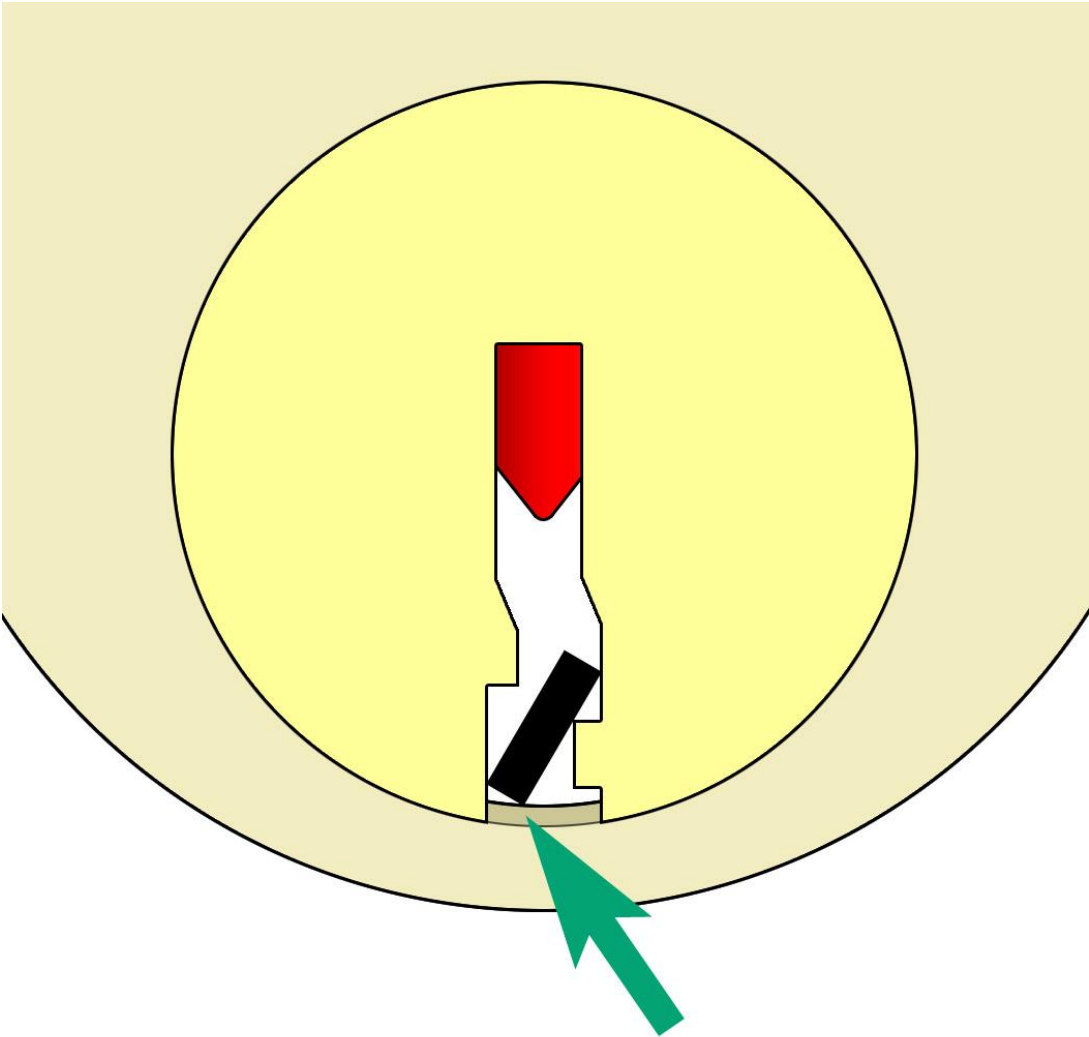
---





# Tension Tools can "Pinch" the Keyway

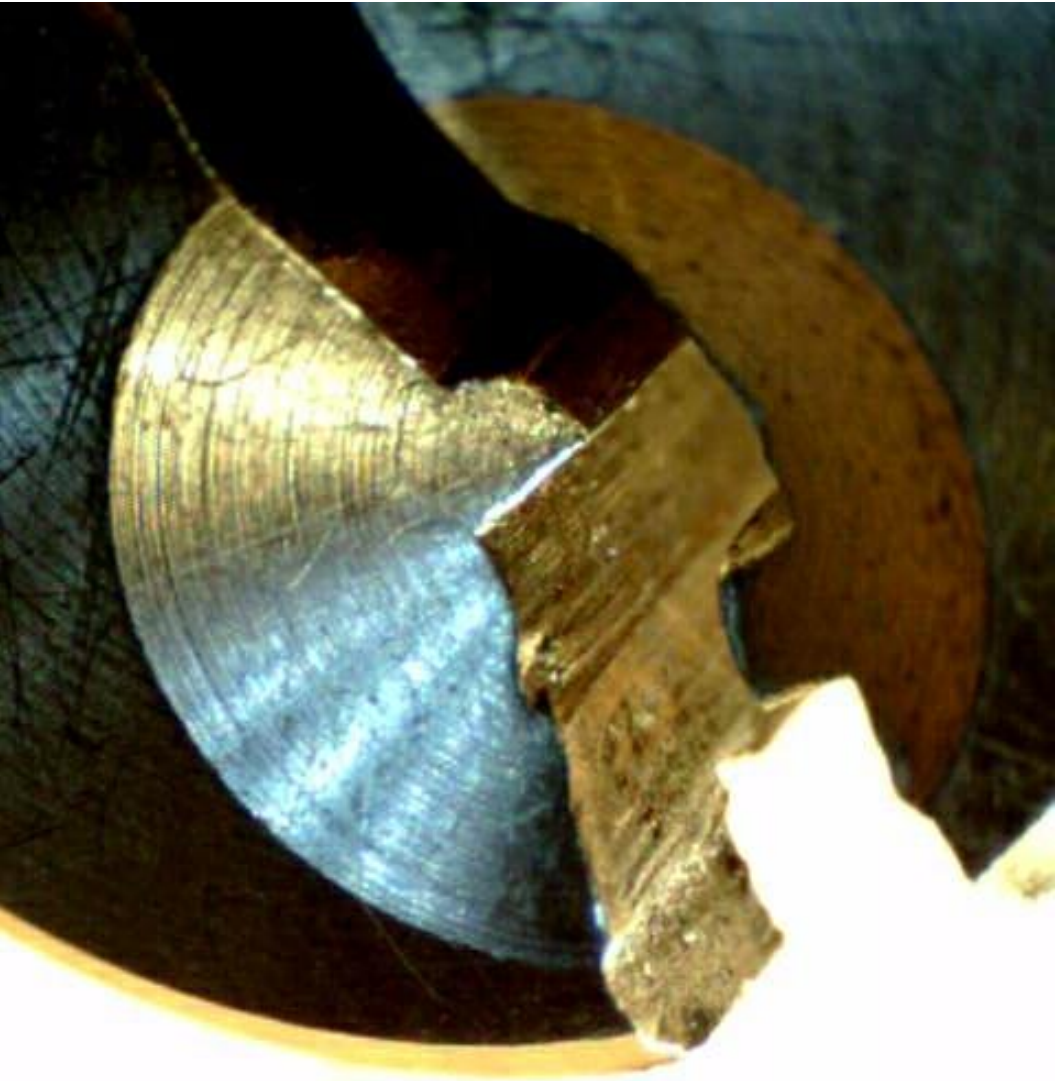
---





# Tension Tools can "Pinch" the Keyway

---



# Fraudulent Toolmarks

---



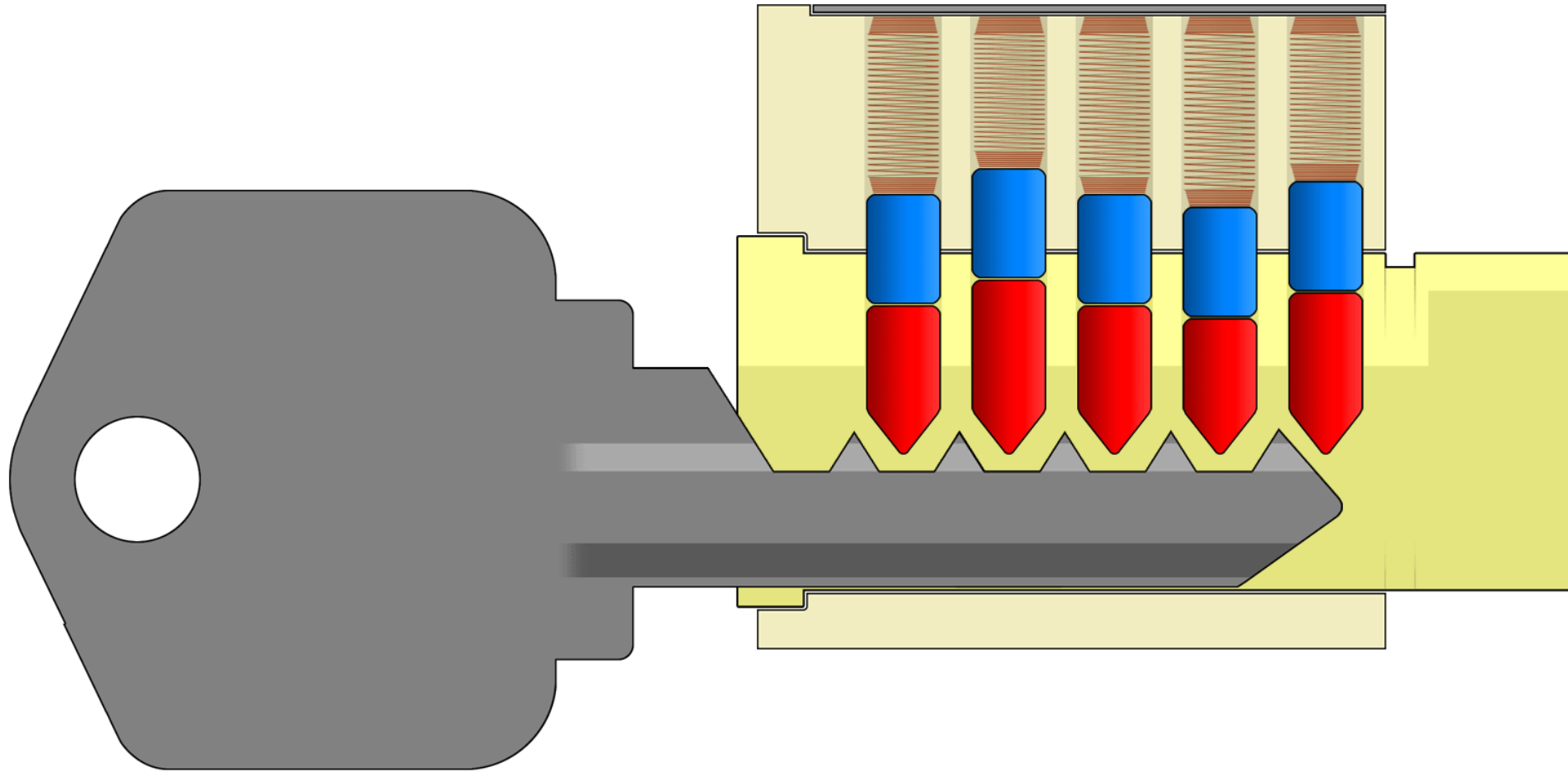
# Fraudulent Toolmarks

---



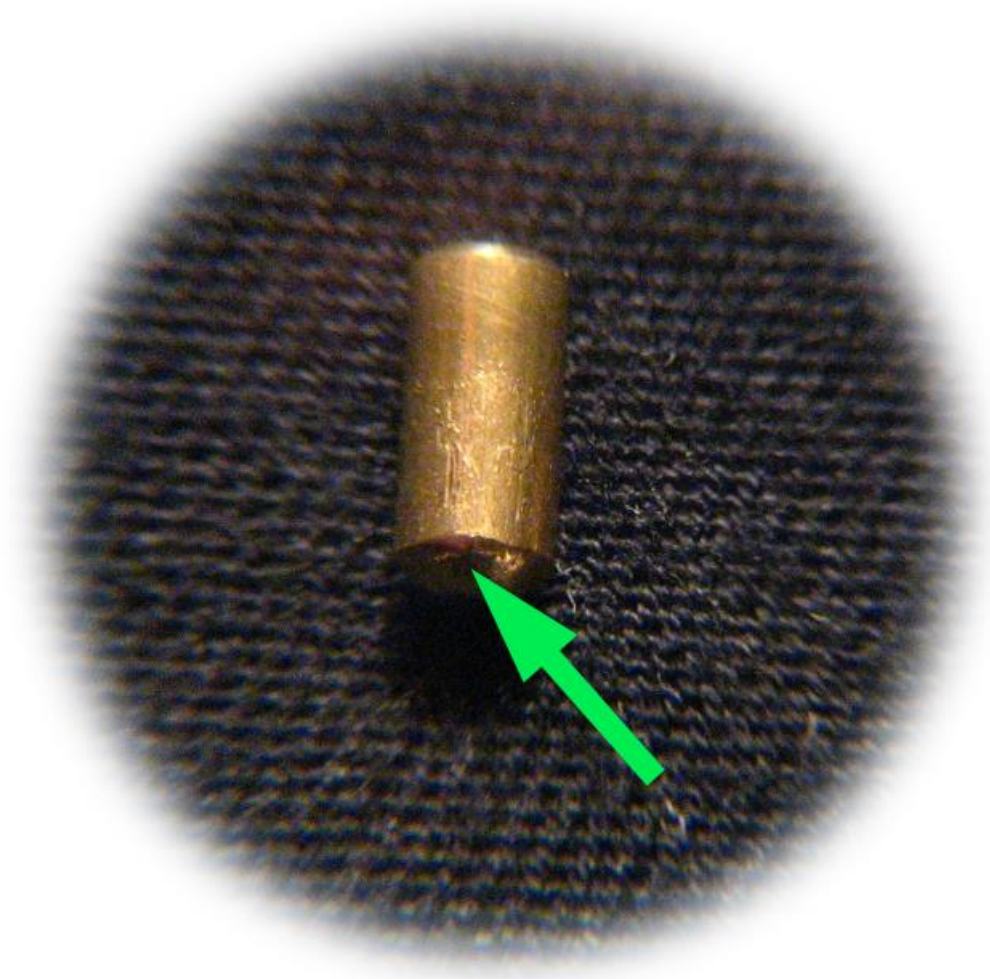
# Bump Key Forensics

---



# Bump Key Forensics

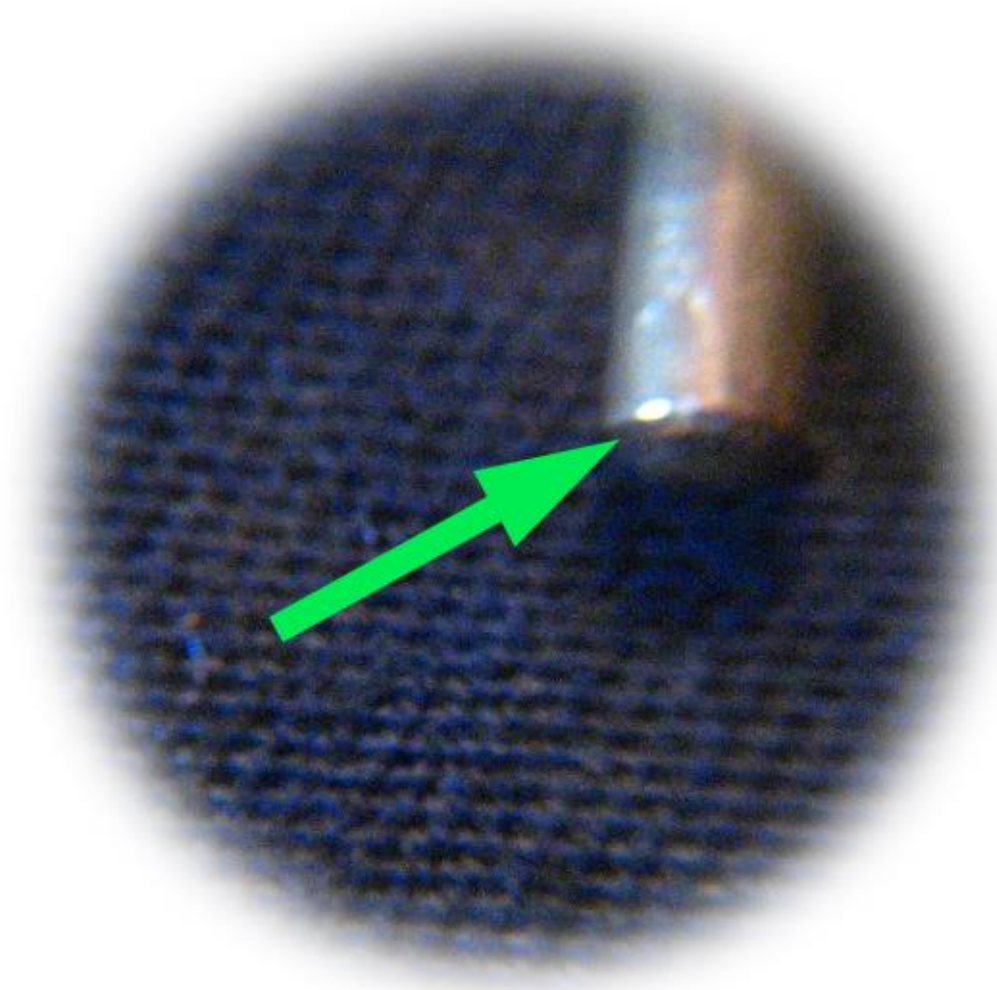
---





# Bump Key Forensics

---



# Bump Key Forensics

---

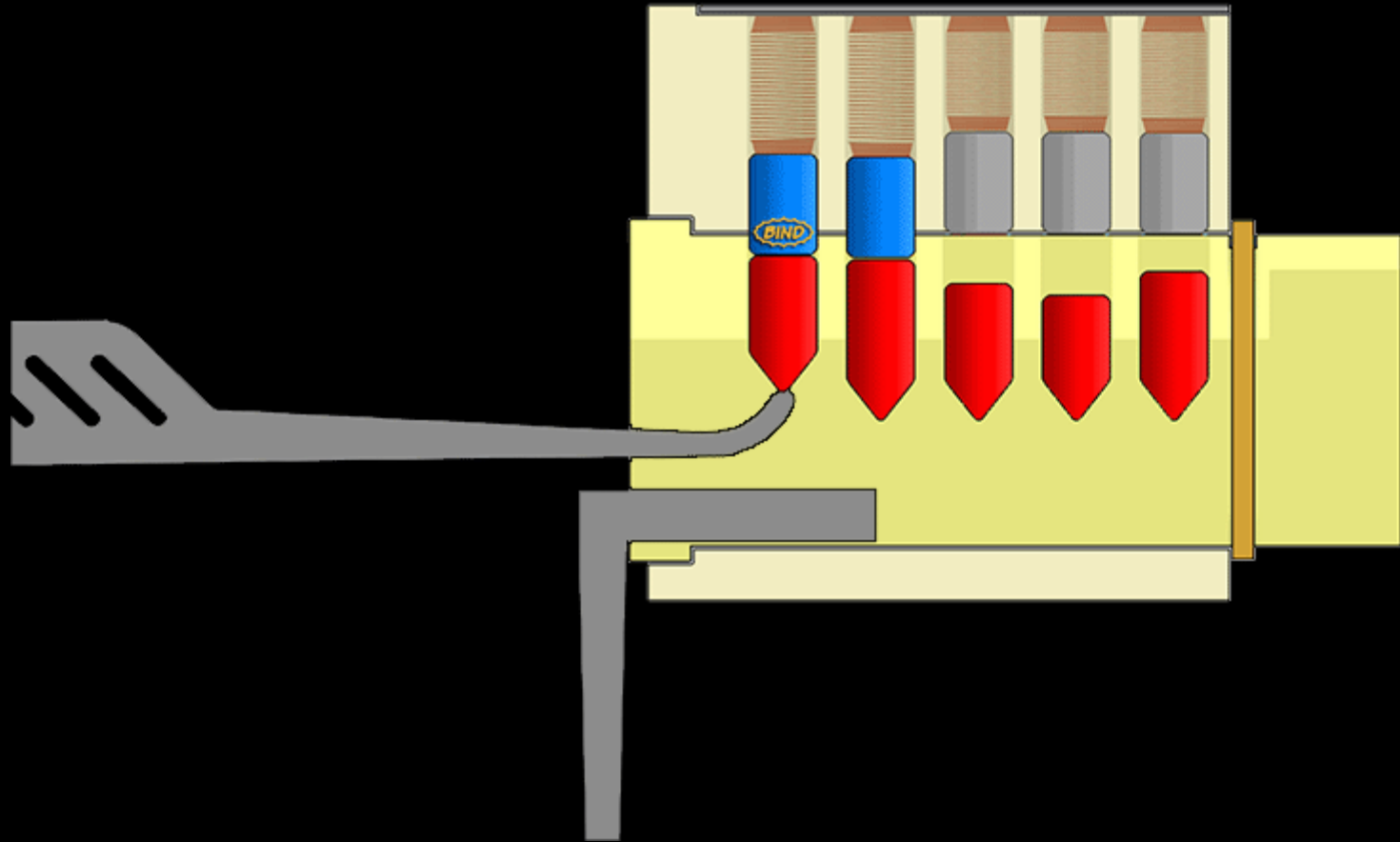


# Bump Key Forensics

---

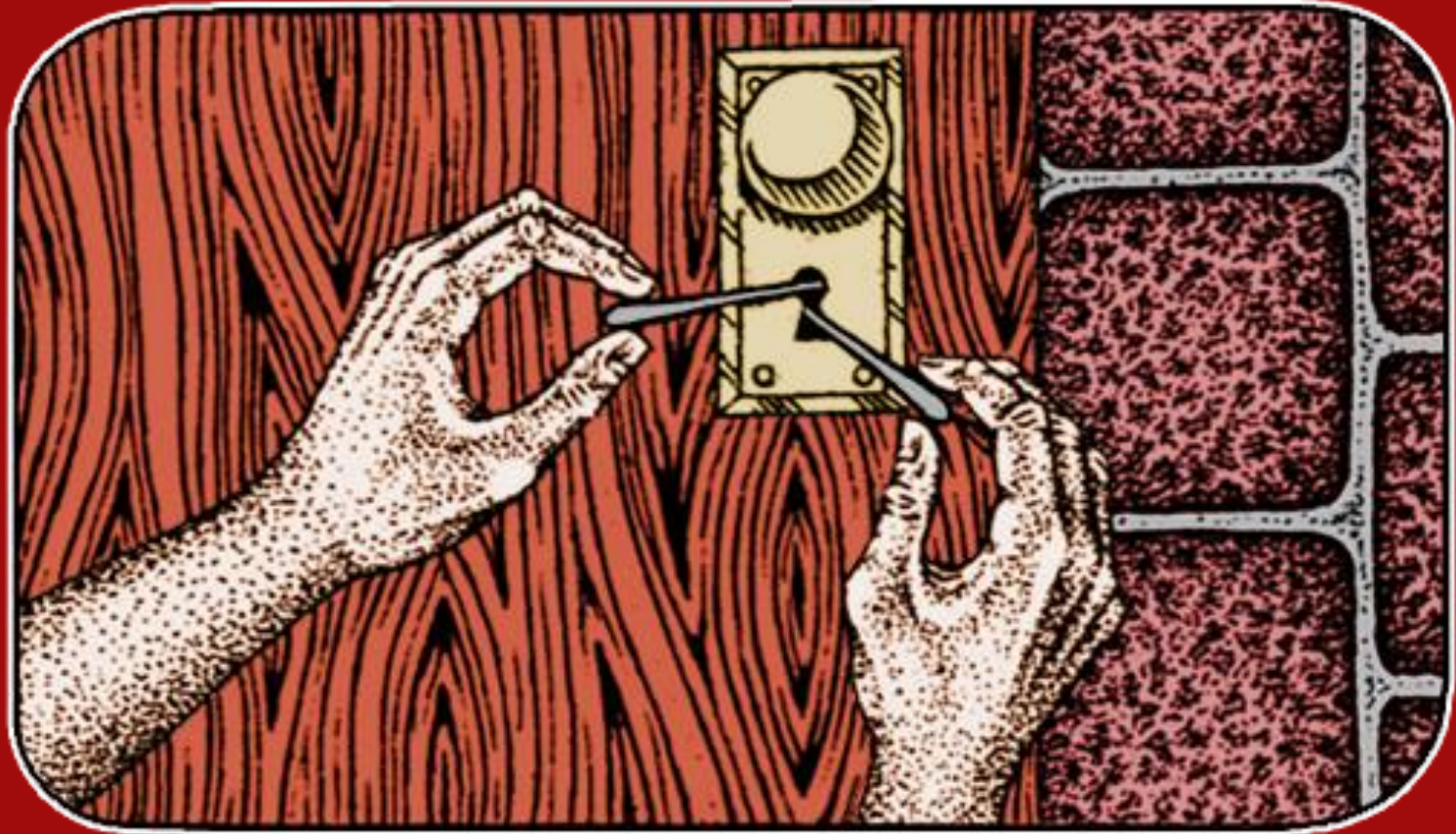


# Questions?





# Resources for Learning More





# Resources For Learning More

---

- Books

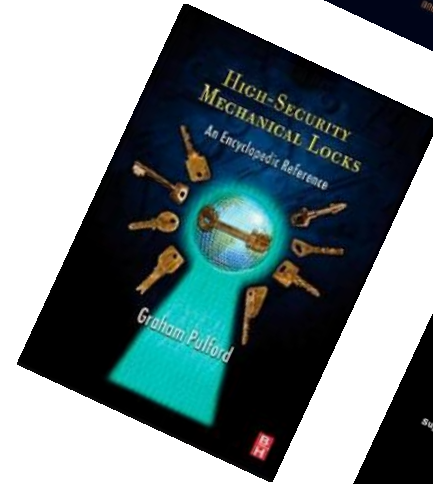
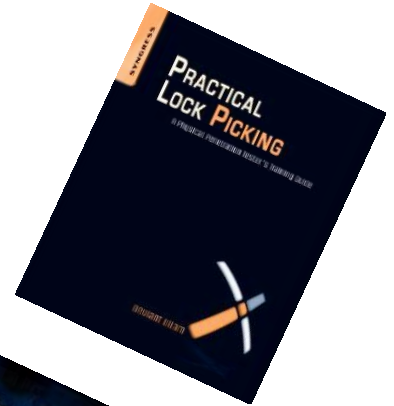
- *Practical Lock Picking & other books* by Deviant Ollam
- *High Security Mechanical Locks* by Graham Pulford
- *Locks, Safes, & Security* by Marc Tobias

- Videos

- [YouTube](#) & [Google](#)
- <http://connect.waaq.org/toool>
- <http://deviating.net/lockpicking/videos.html>

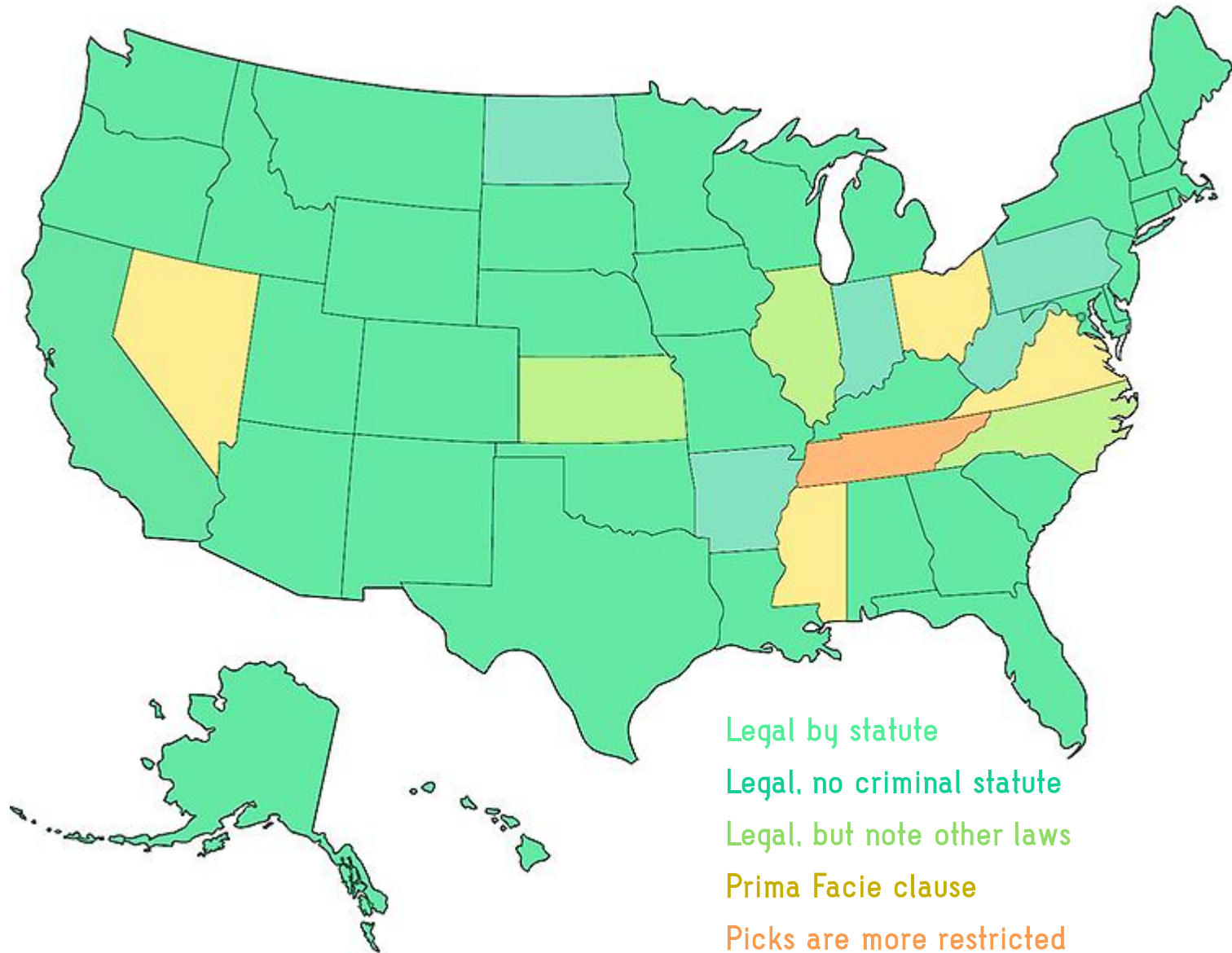
- On The Web

- <http://toool.us>
- <http://toool.nl>
- <http://blackbaq.nl>
- <http://deviating.net>



# Legal Questions

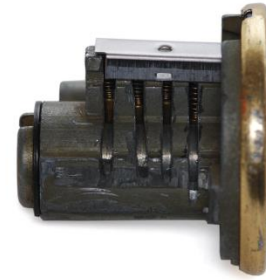
---



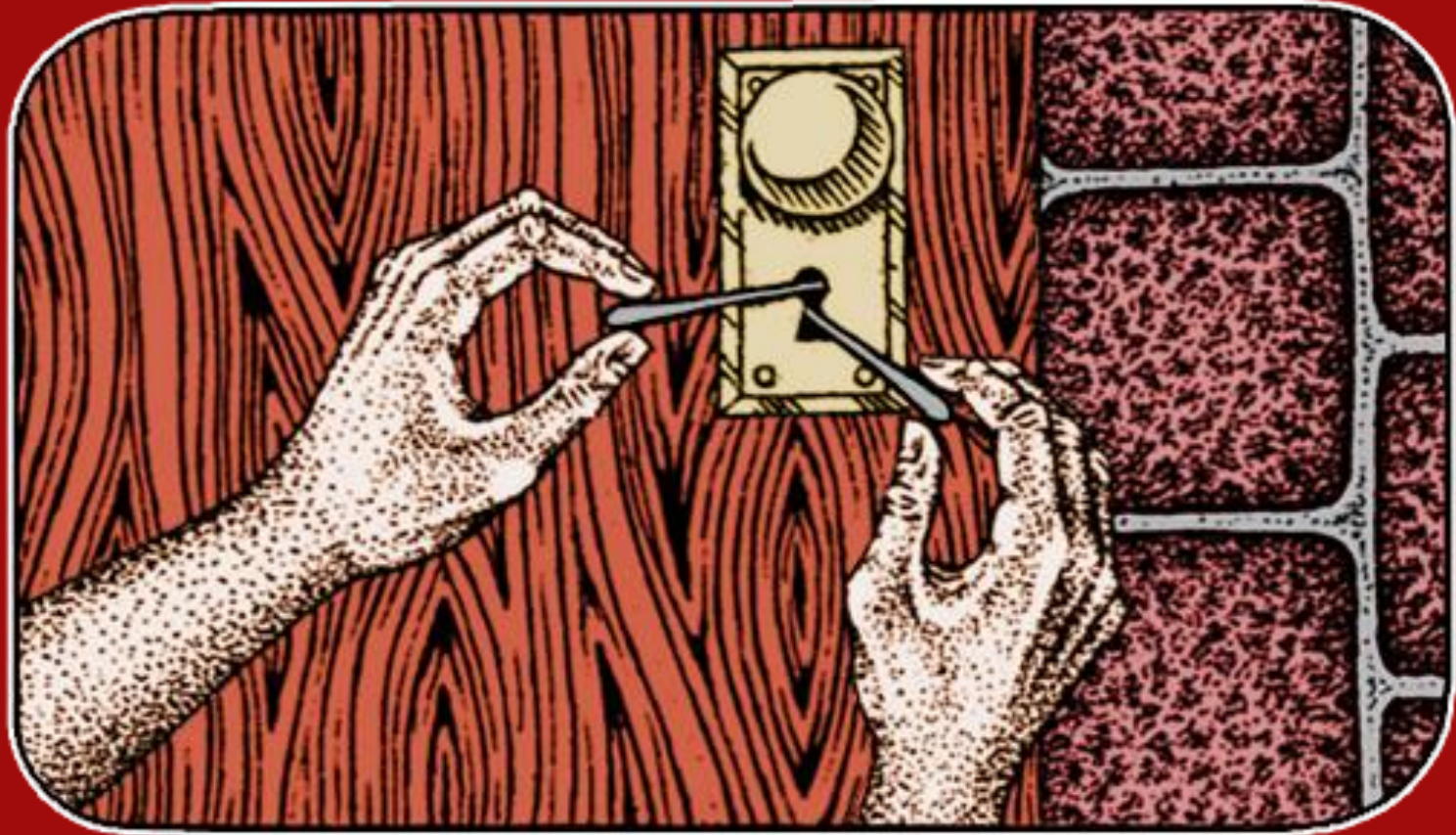
# Acquiring Locks

---

- Free
  - Basements, garages, yard sales
  - Ask neighbors, ask locksmiths
- For sale
  - Vary your sources
  - Hardware store vs. eBay
- Specialized
  - Progressive kits
  - Ultimate practice lock



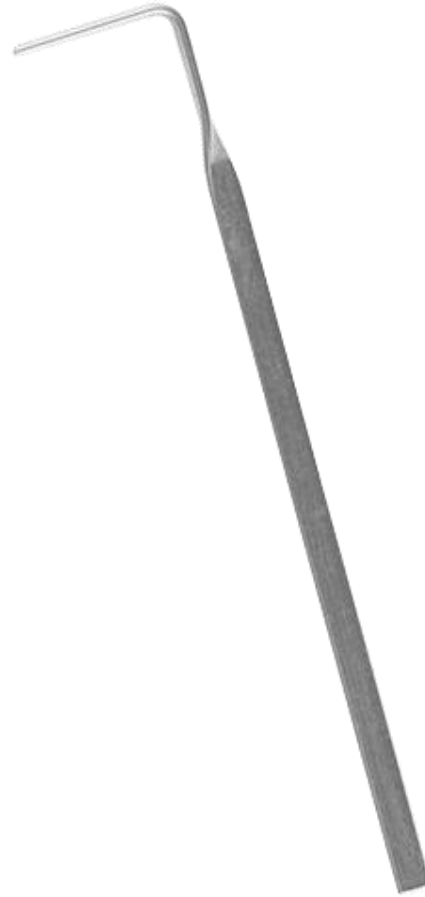
# Security in the Real World





# Security in the Real World

---





# Security in the Real World

---



# Security in the Real World

---

- Technical Finesse or Brute Force
  - \$100 lock in a \$10 door?
- Doors
  - Solid core, heavy hinge
  - Anti-thrust bolts and latches
- Windows
  - Shatterproof film
  - Vulnerable to lifting? (sliding glass)



# Security in the Real World

---

Lockpicking

Quick & Dirty ← *guard against these attacks*

Covert & High-Tech

# Thank You Very Much

---



<http://toool.us>

[info@toool.us](mailto:info@toool.us)

This presentation is Copyleft by Deviant Ollam.

You are free to reuse any or all of this material as long as it is attributed and freedom for others to do the same is maintained.