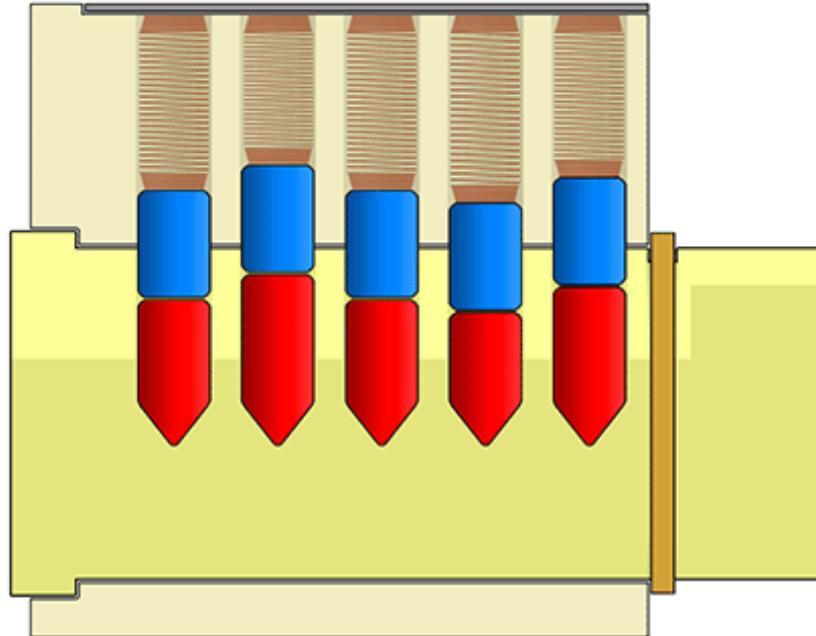


Locks and History



Lots of slides provided by:



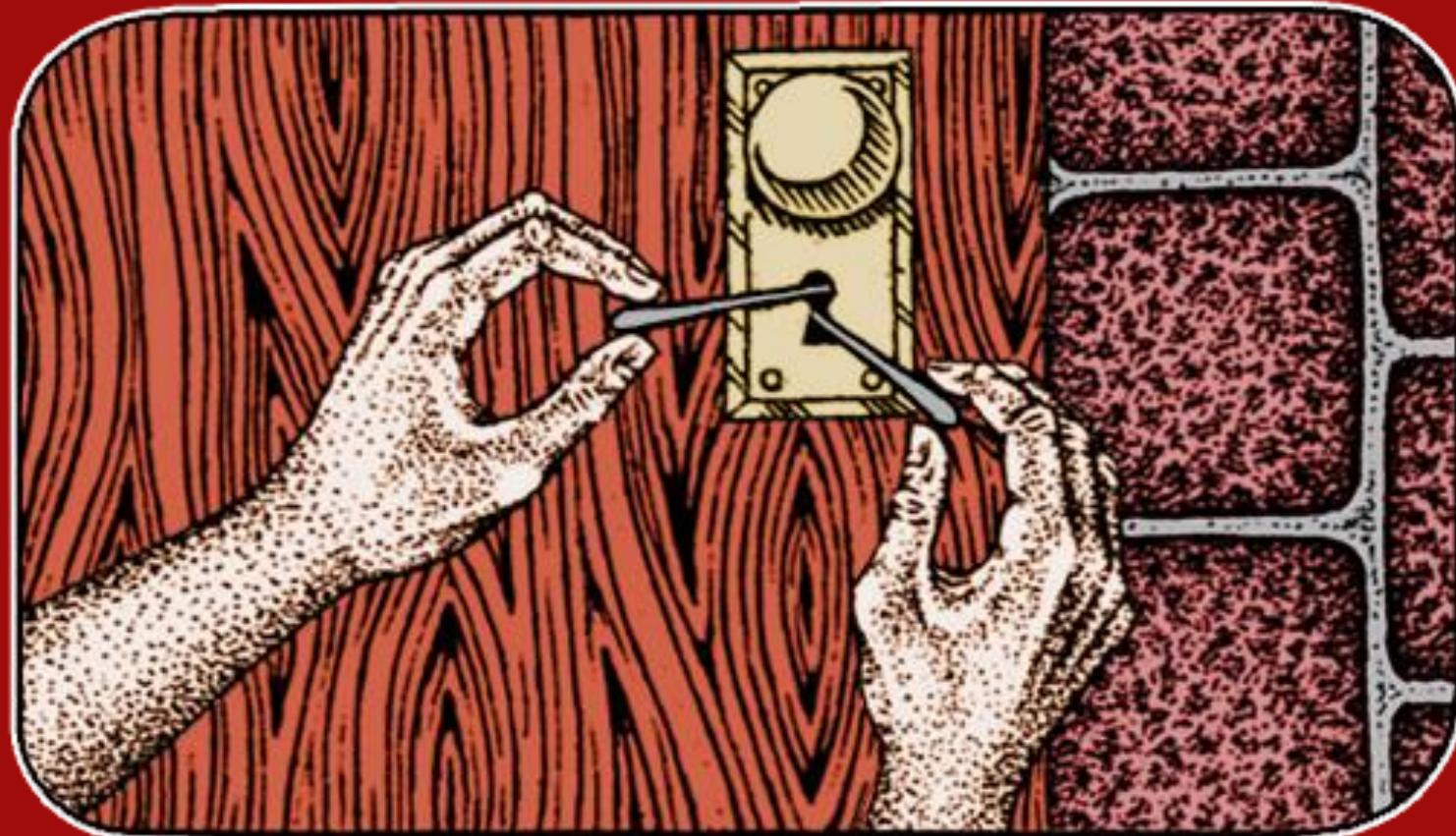
Standard Humble Bragging Introduction

Email: 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!?



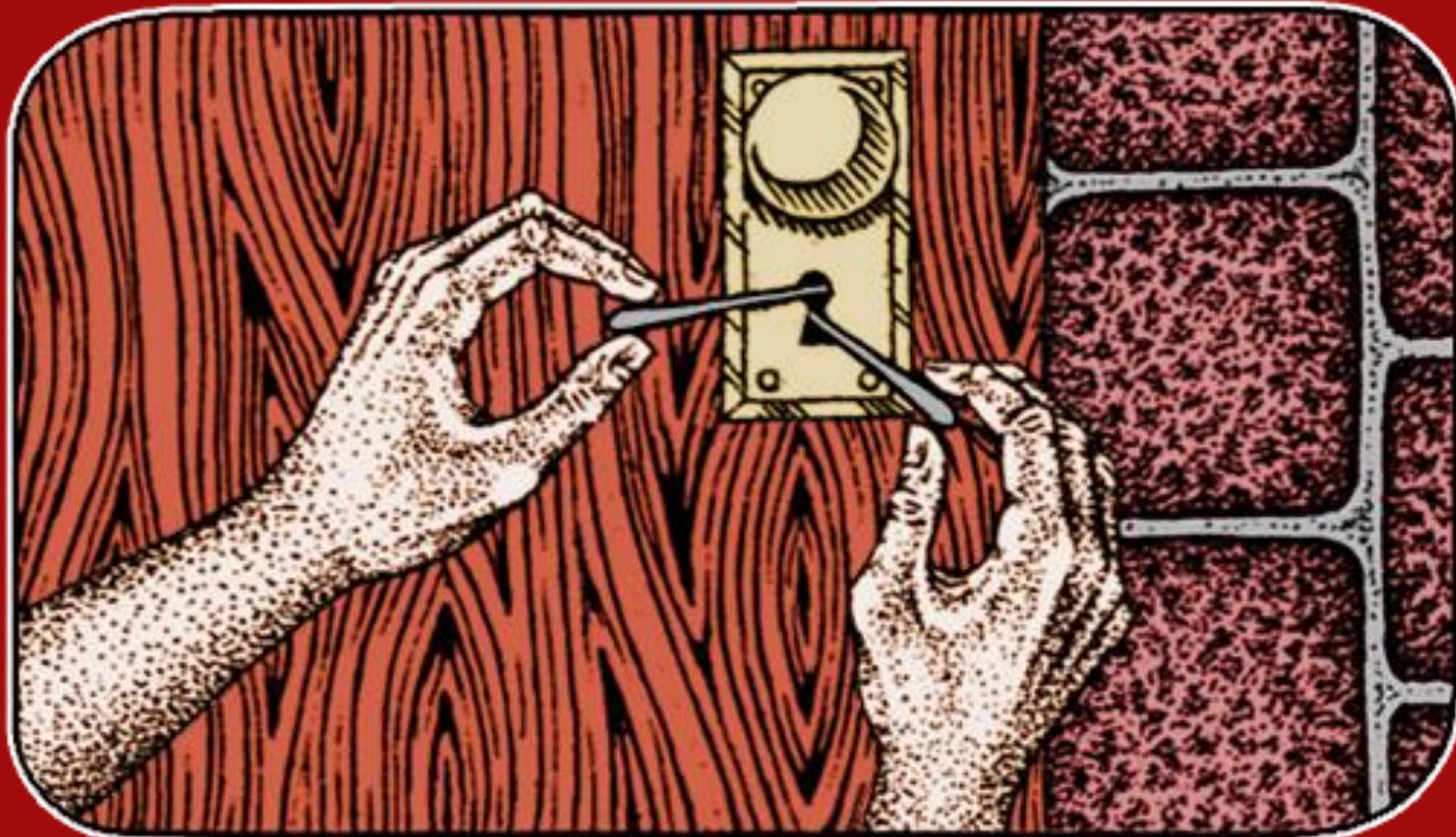
Criminals don't pick locks

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



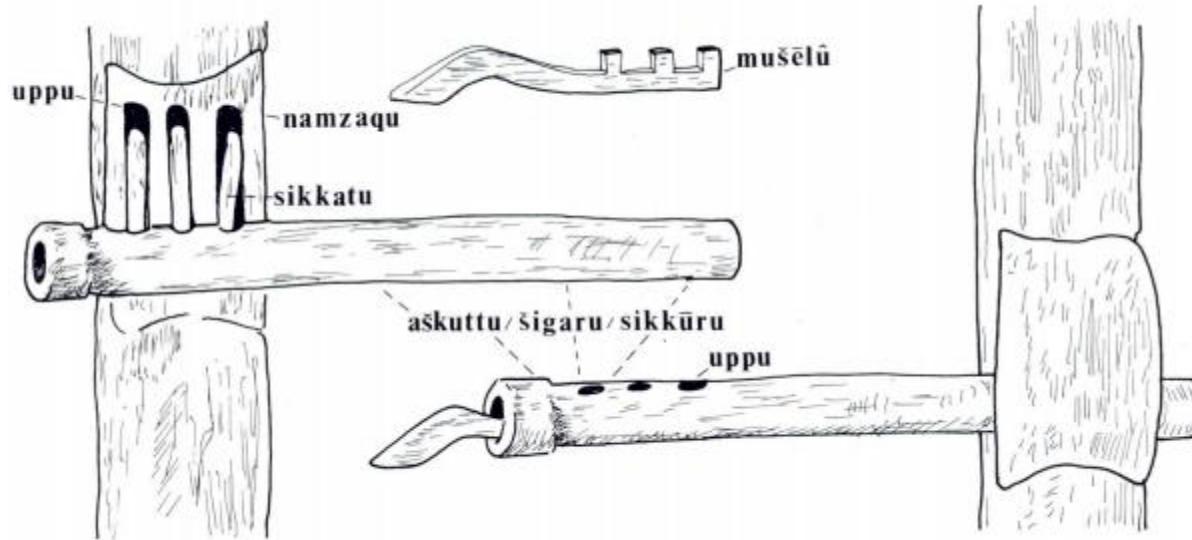
Or they get elected to office.

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.



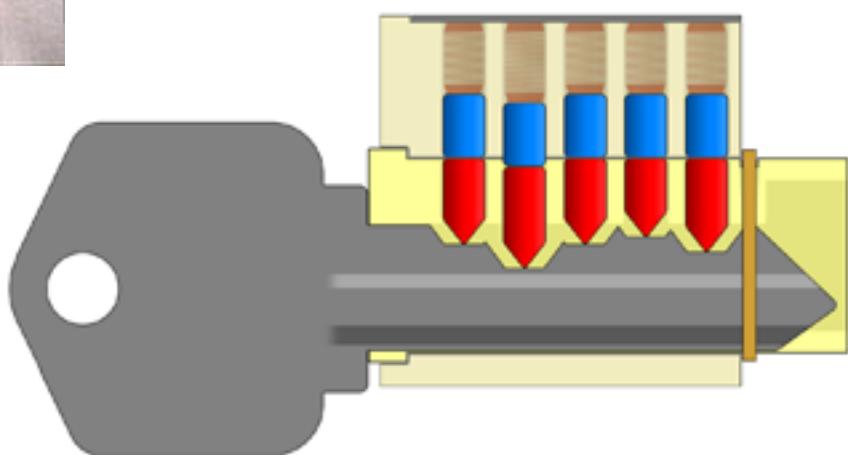
First record of any lock was in 1300BC, listed on a Greek Linear B tablet found in Crete.

Mind if I borrow that?

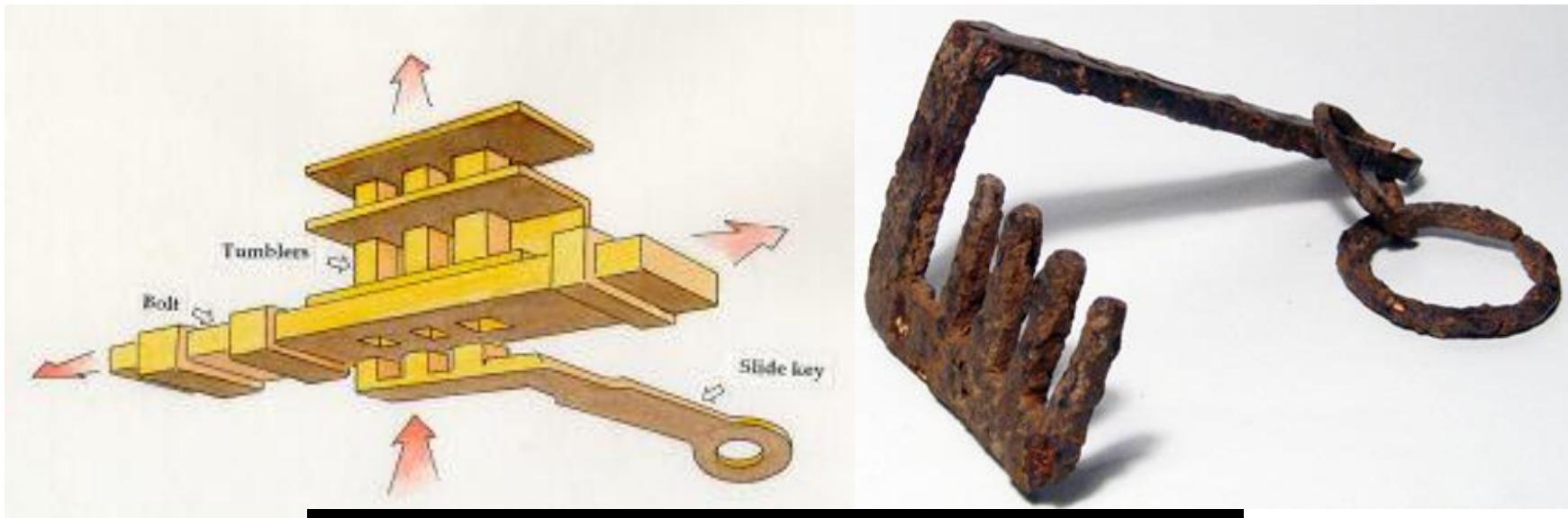


The Egyptians borrowed the design from the Assyrians. Greeks borrowed the design from the Egyptians. Both added minor refinements.

Look familiar?



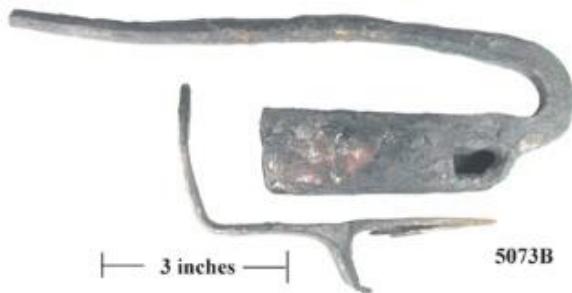
What did the Romans ever do for us?



Padlocks!



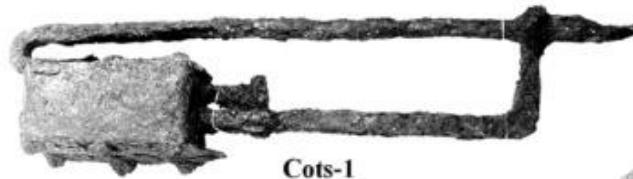
5073A



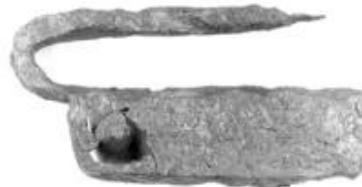
5073B



5073E



Cots-1

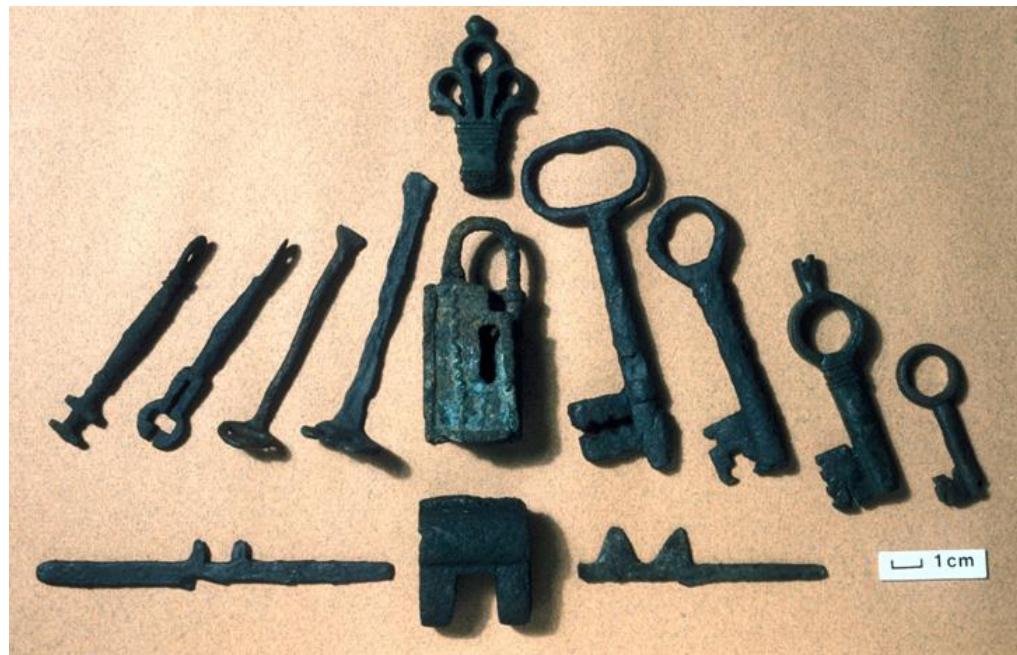
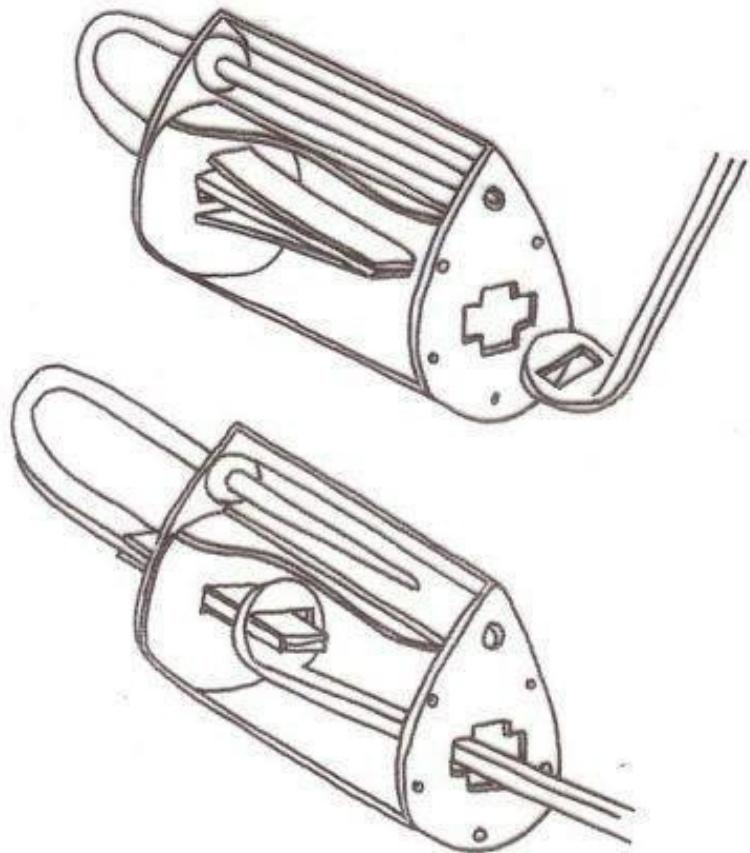


Cots-2

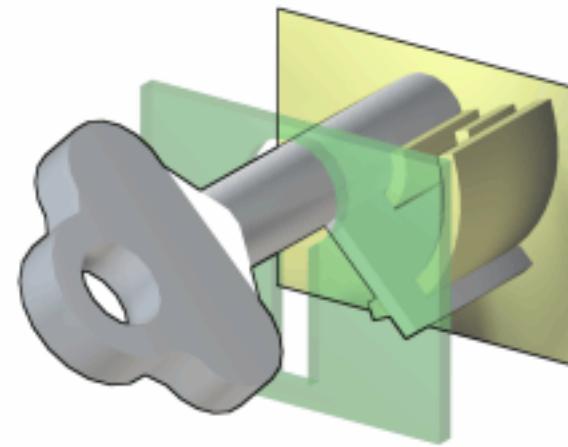
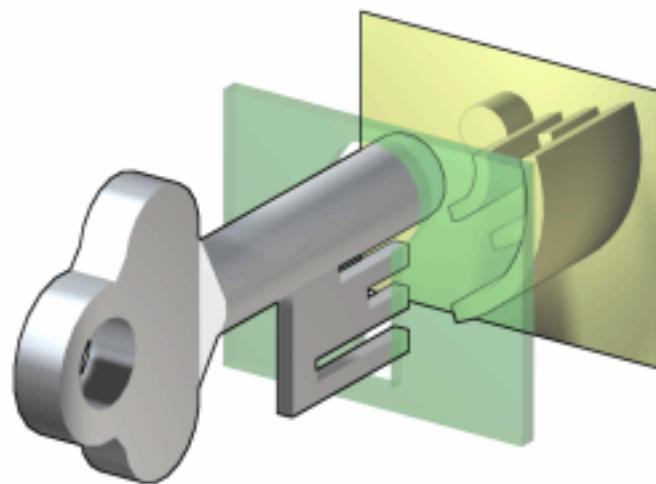
100 AD – 300 AD

Not long after Marcus Aurelius was
Emperor of Rome

Can't forget about the Vikings



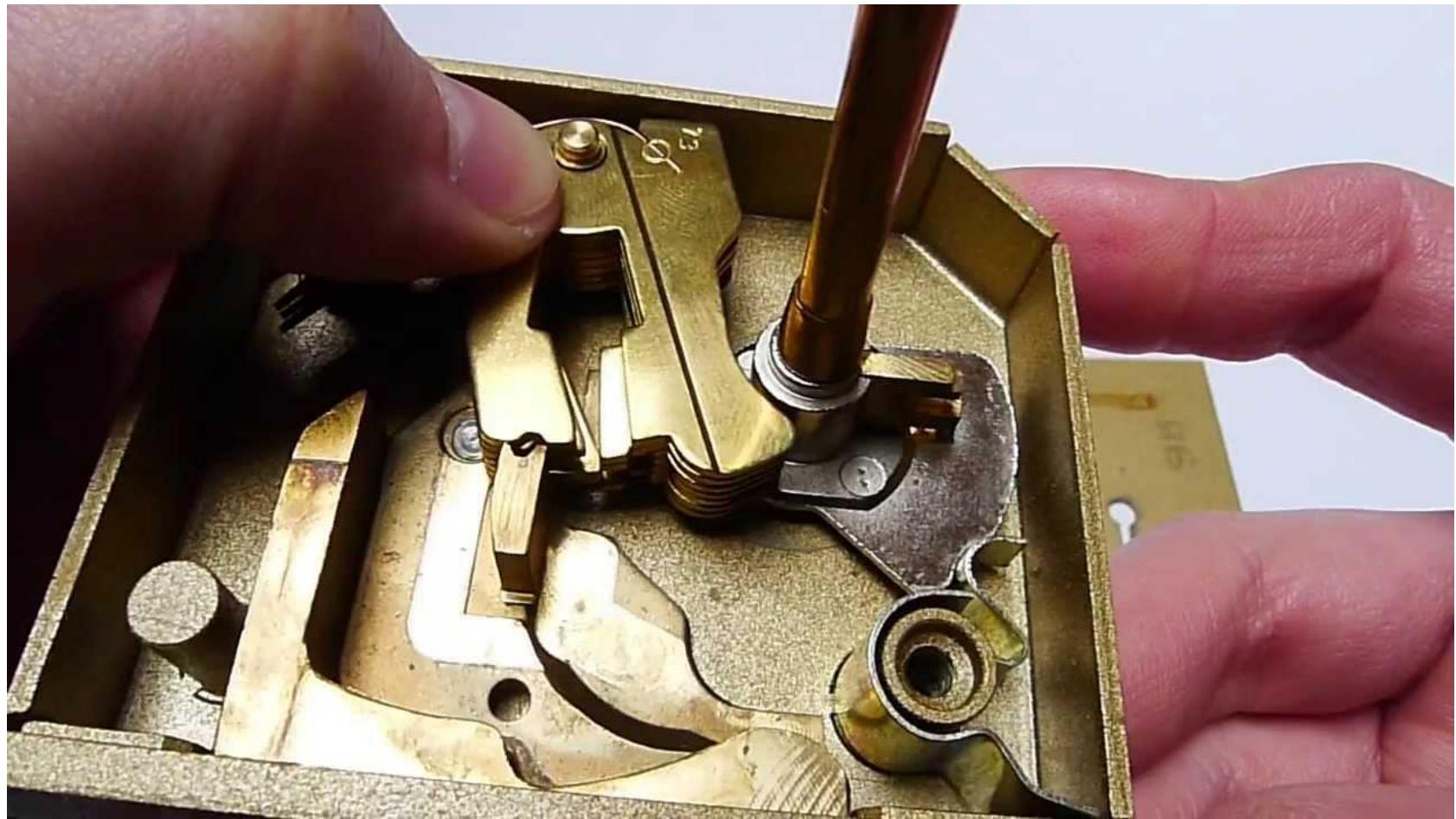
Ward Locks



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

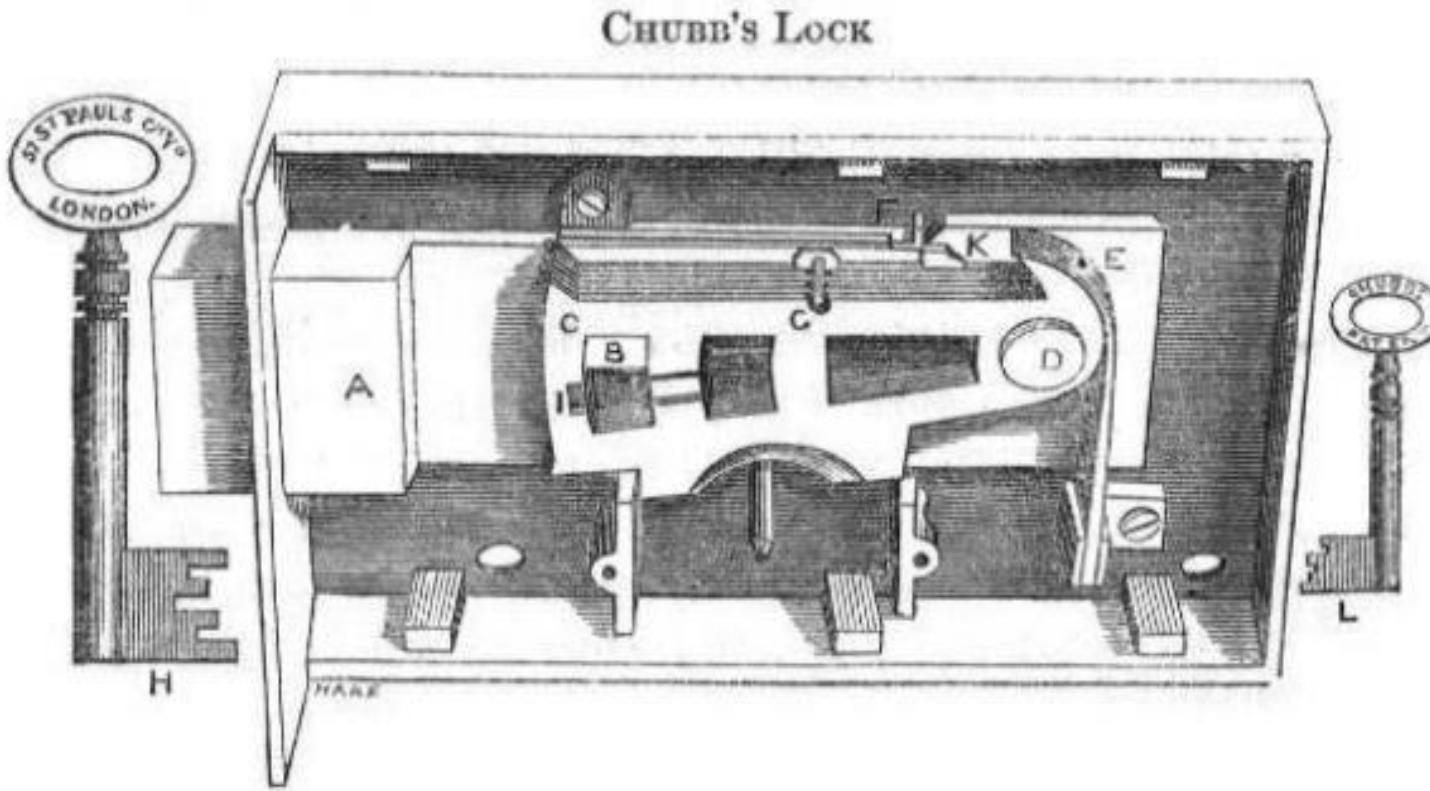


Bramah Safety Lock

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 Nations



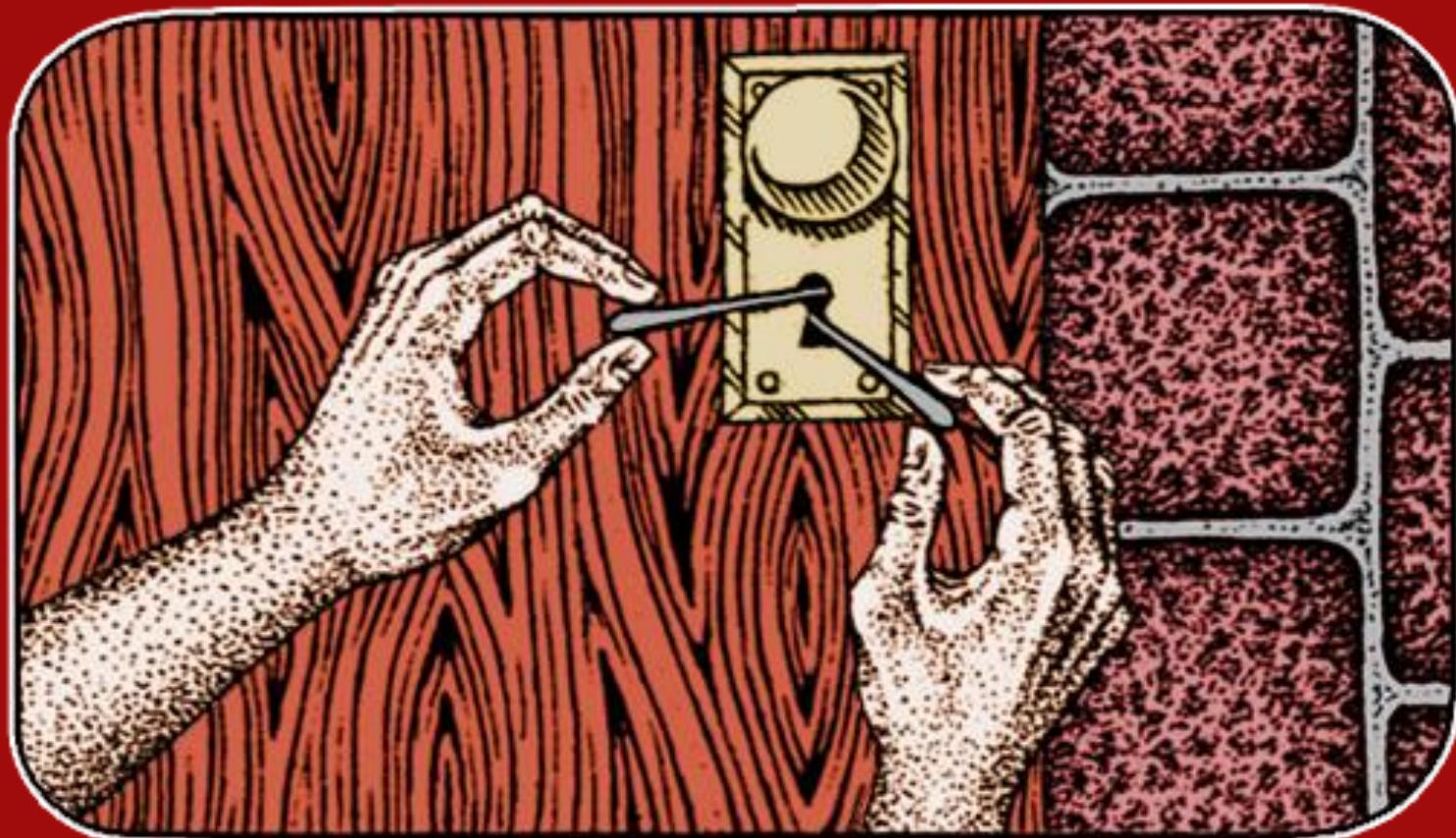
THE CRYSTAL PALACE IN HYDE PARK FOR GRAND INTERNATIONAL EXHIBITION OF 1851.
Dedicated to the Royal Commissioners.

VIEW FROM THE ANGLISBRIDGE ROAD OF

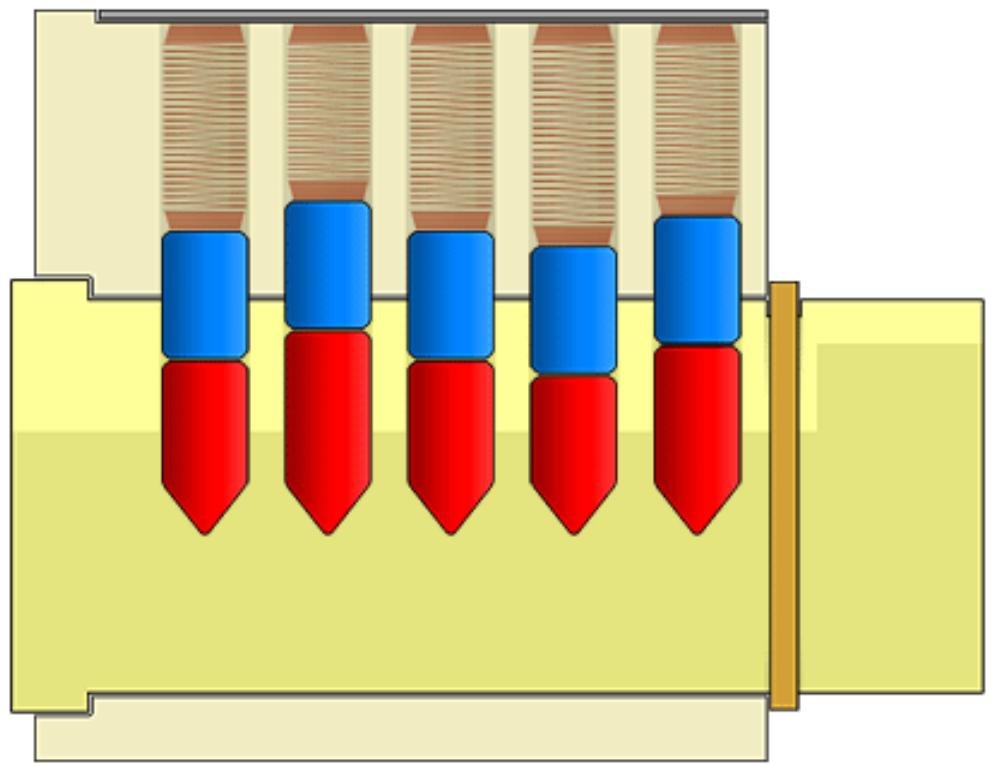
JO. JOHNSON & CO. LTD. 1851.

ROB. BIGG ENGRAVERS & PRINTERS.

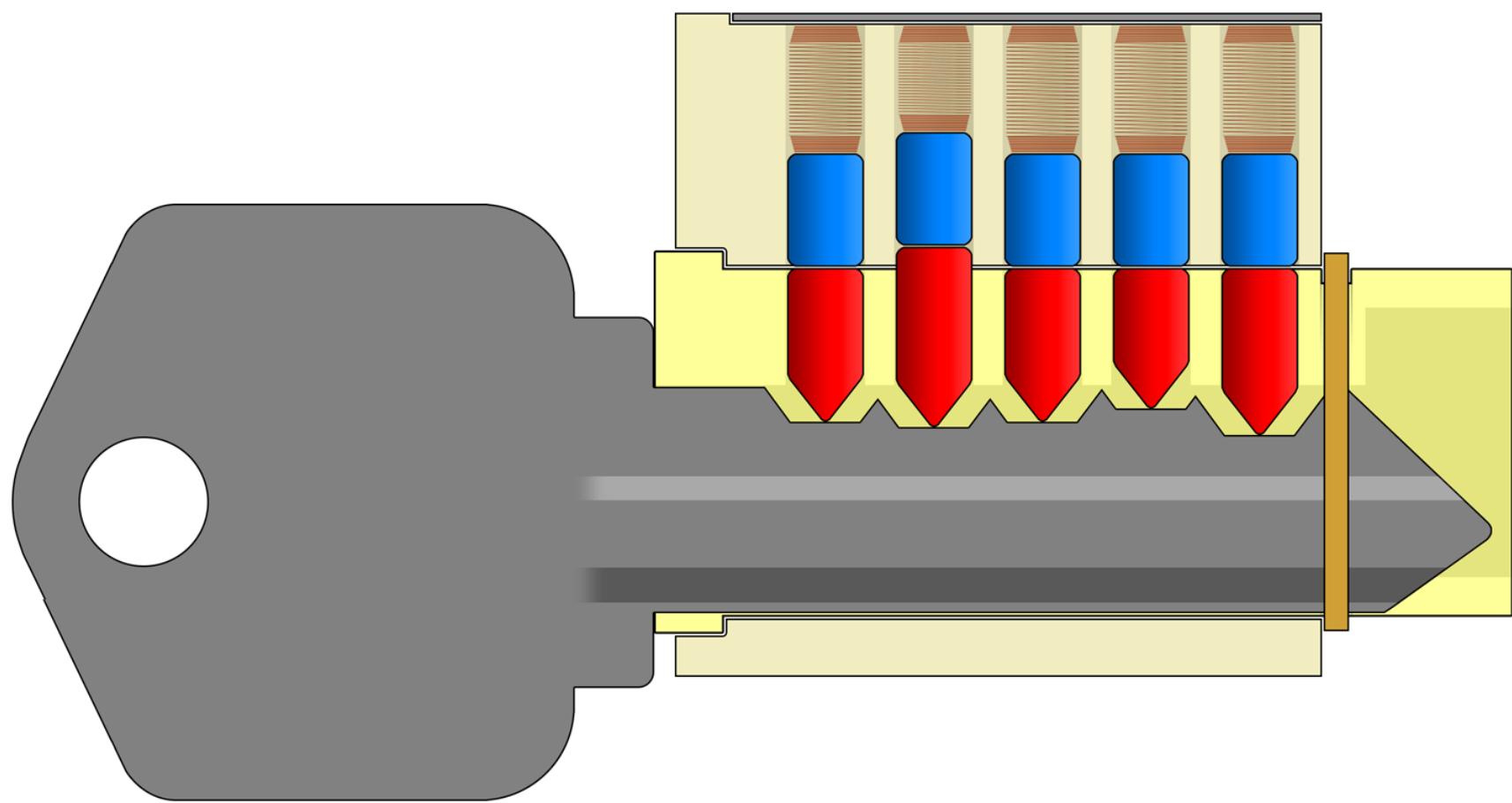
Act 2 – Lock Picking



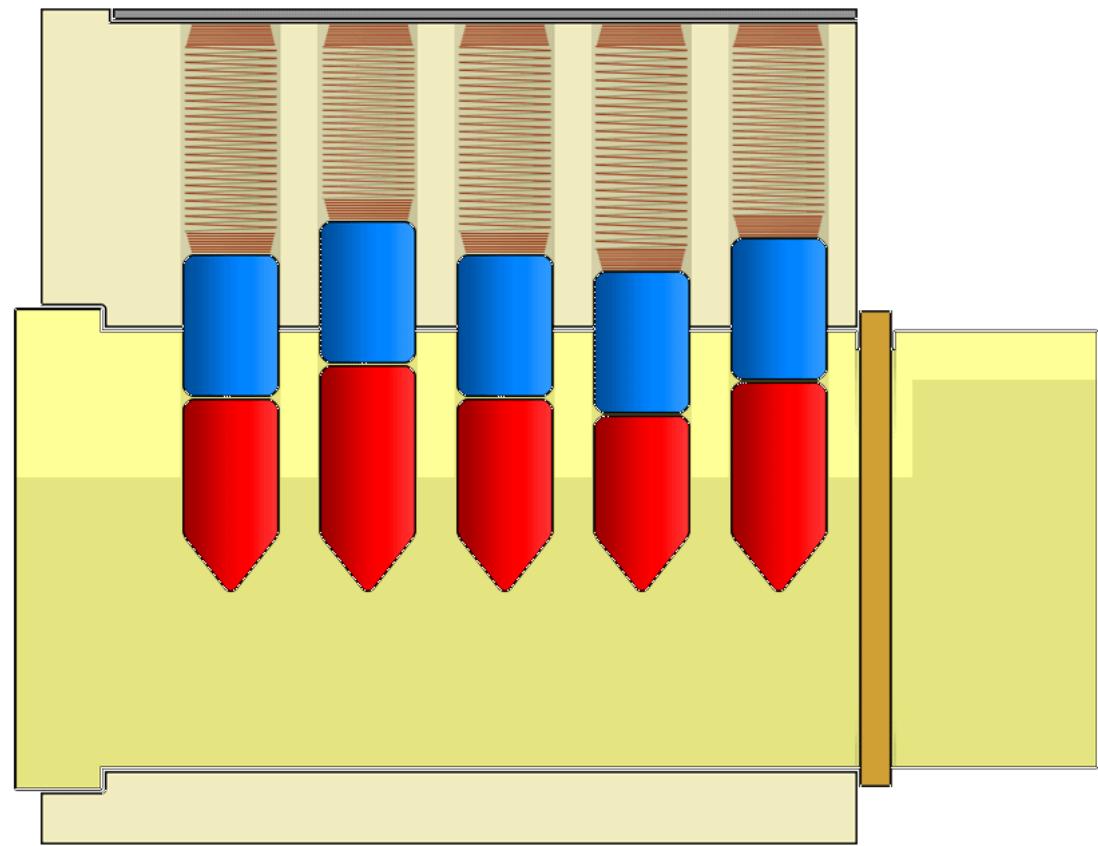
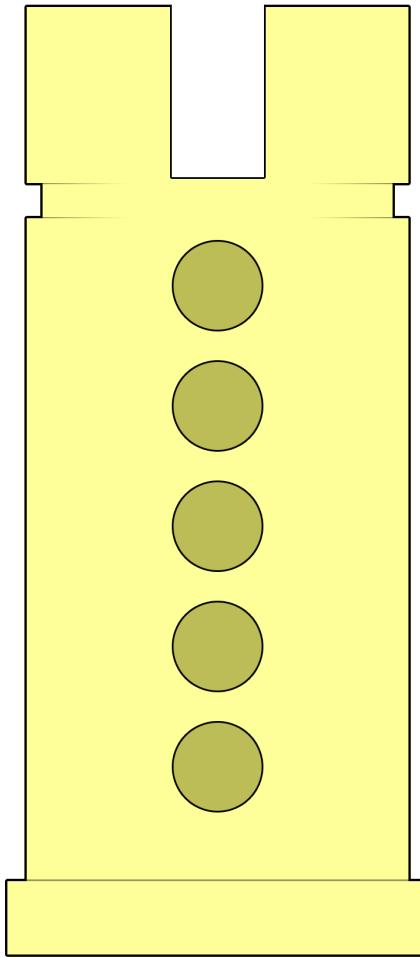
The lock on your front door



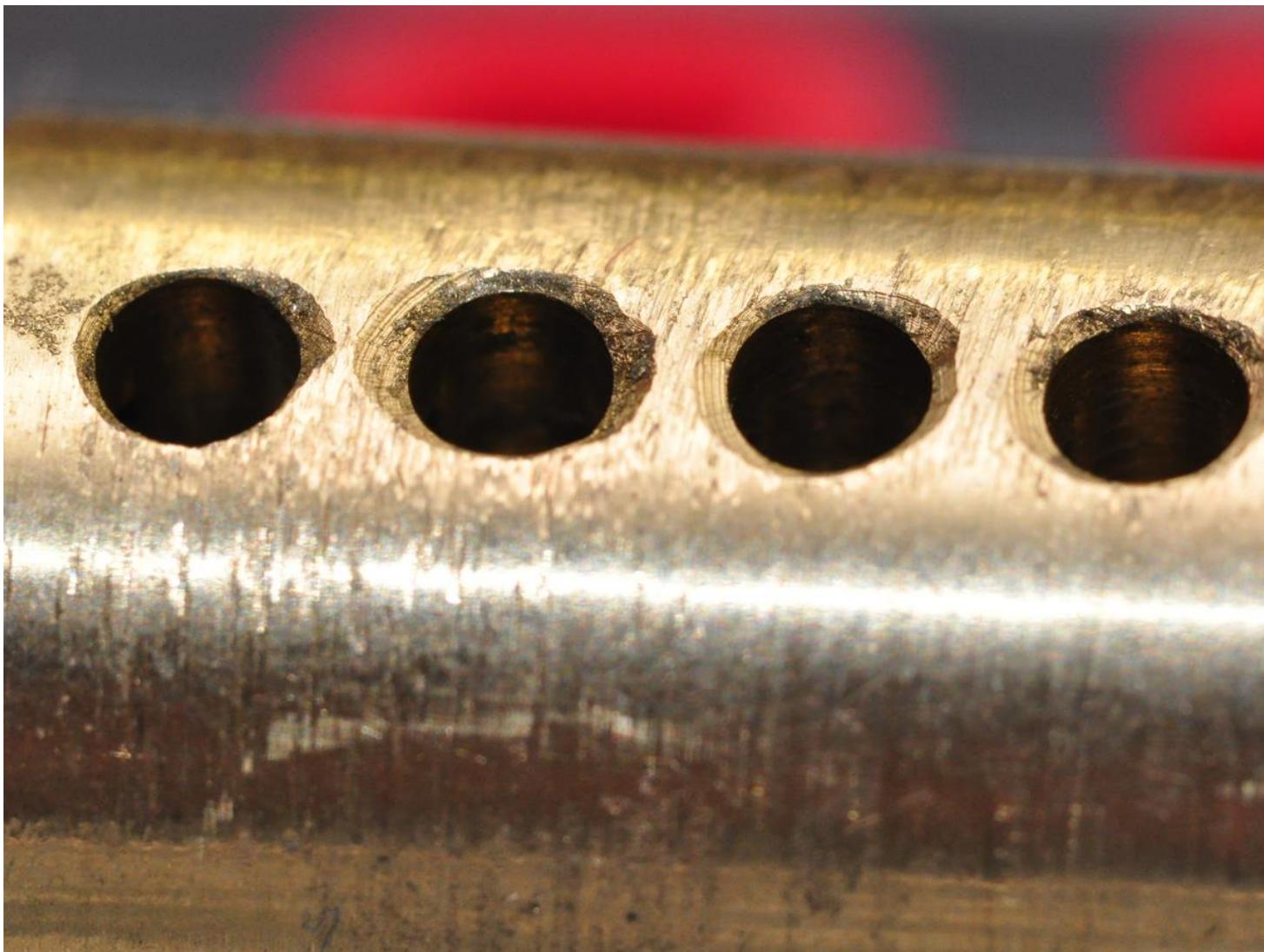
How your front door lock opens



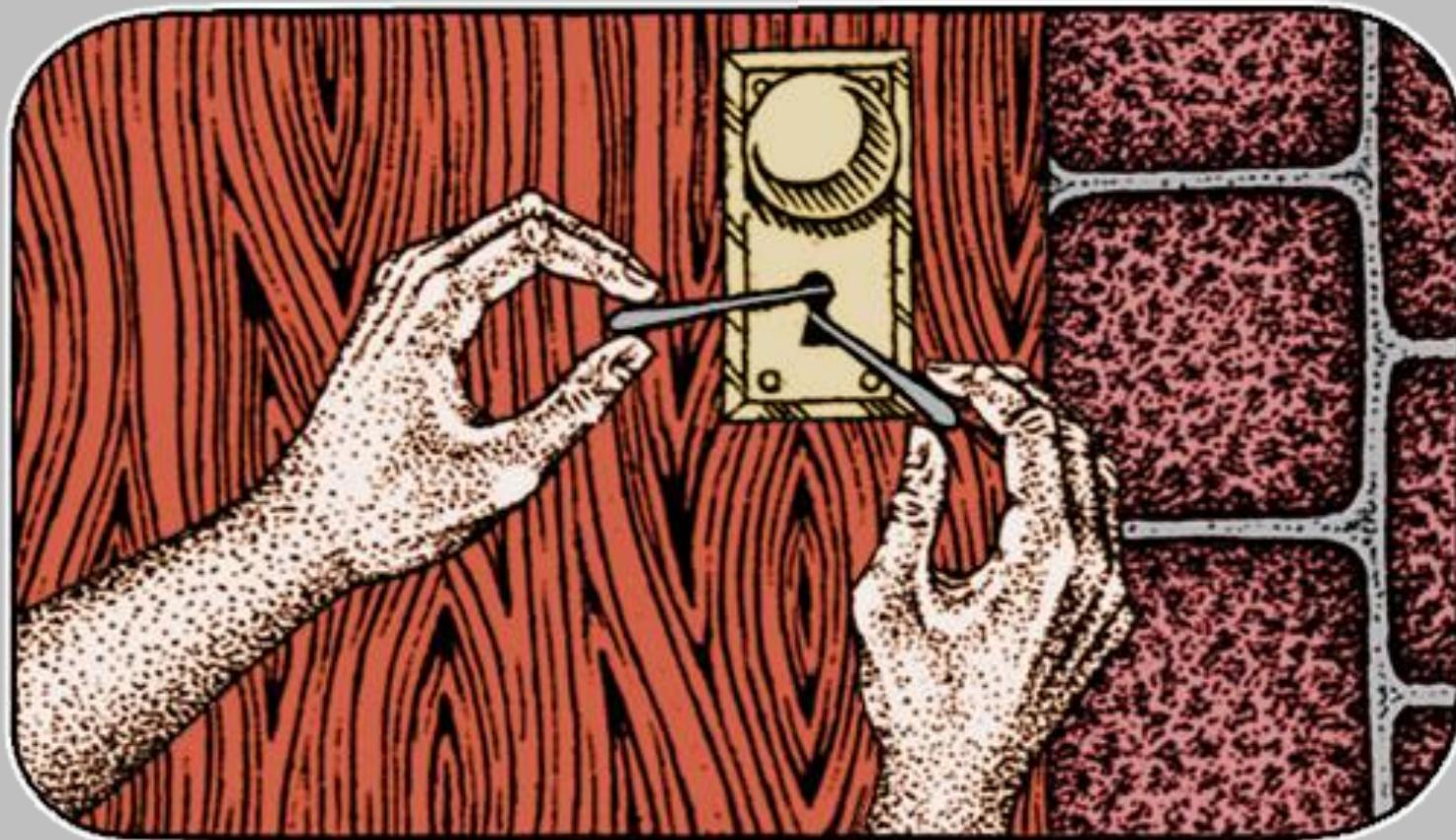
In a Perfect World



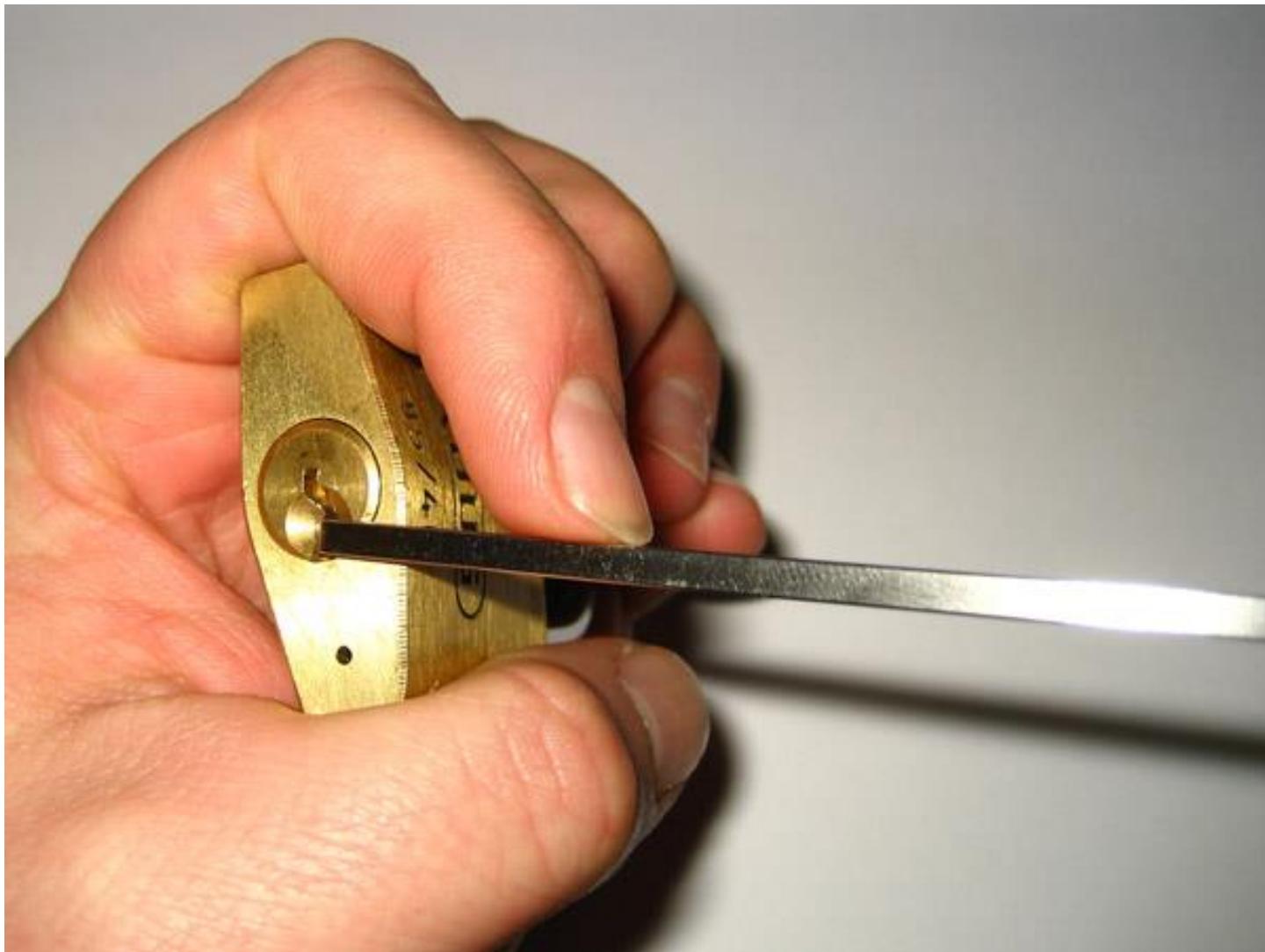
In the Real World



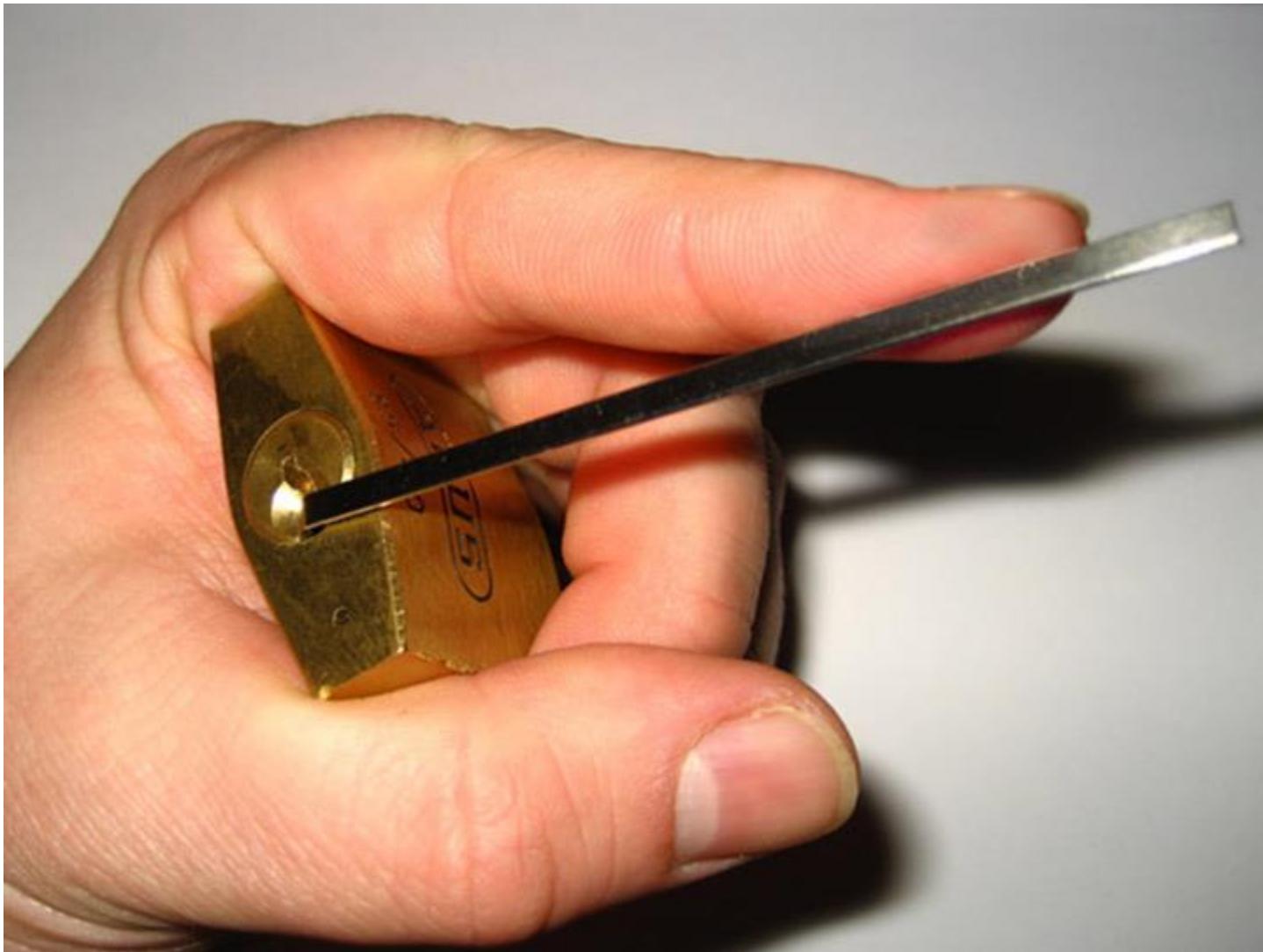
Let's Teach You to Pick Locks



Torsion Wrench Usage (Pushing)



Best Turning Tool Usage (Pushing Out at Tip)



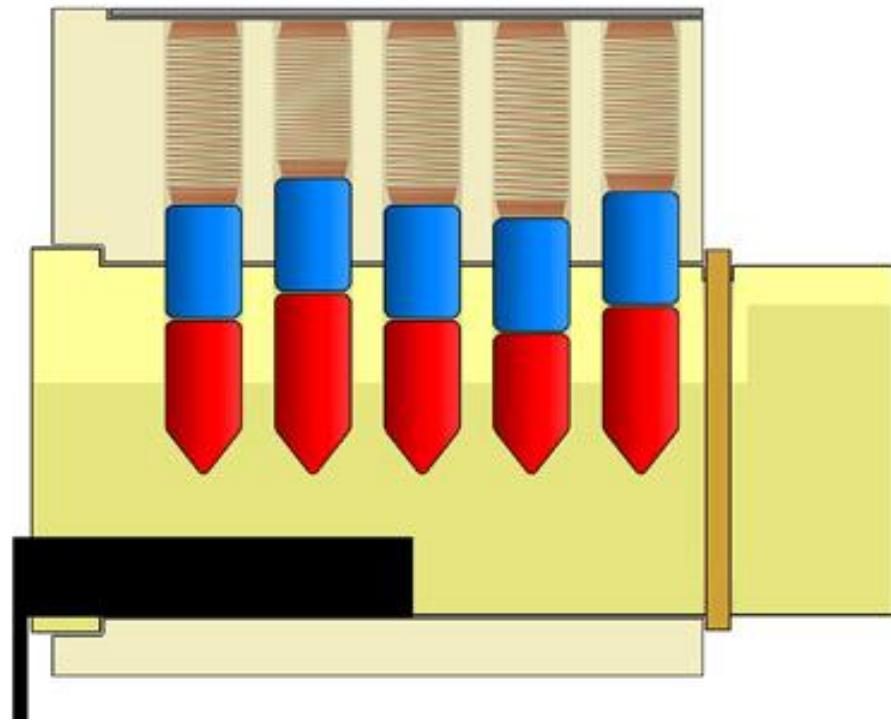
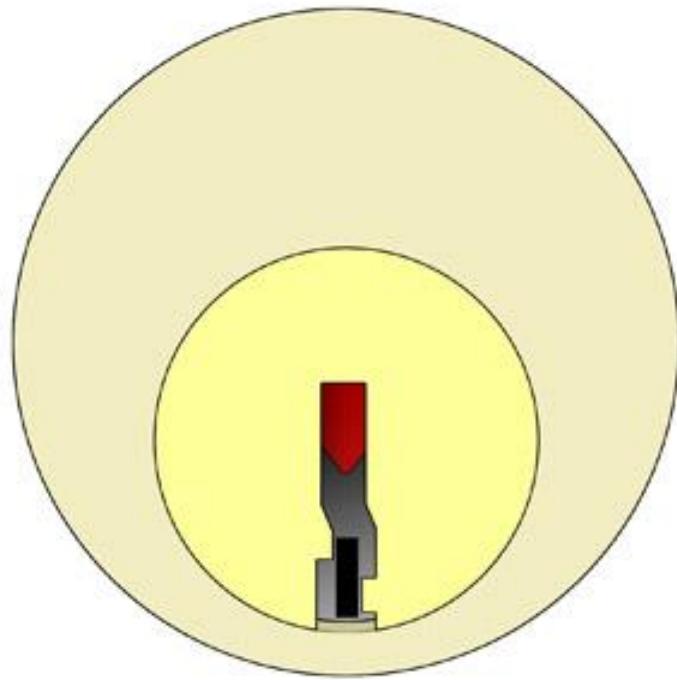
Turning Tool Position: “Edge of the Plug”



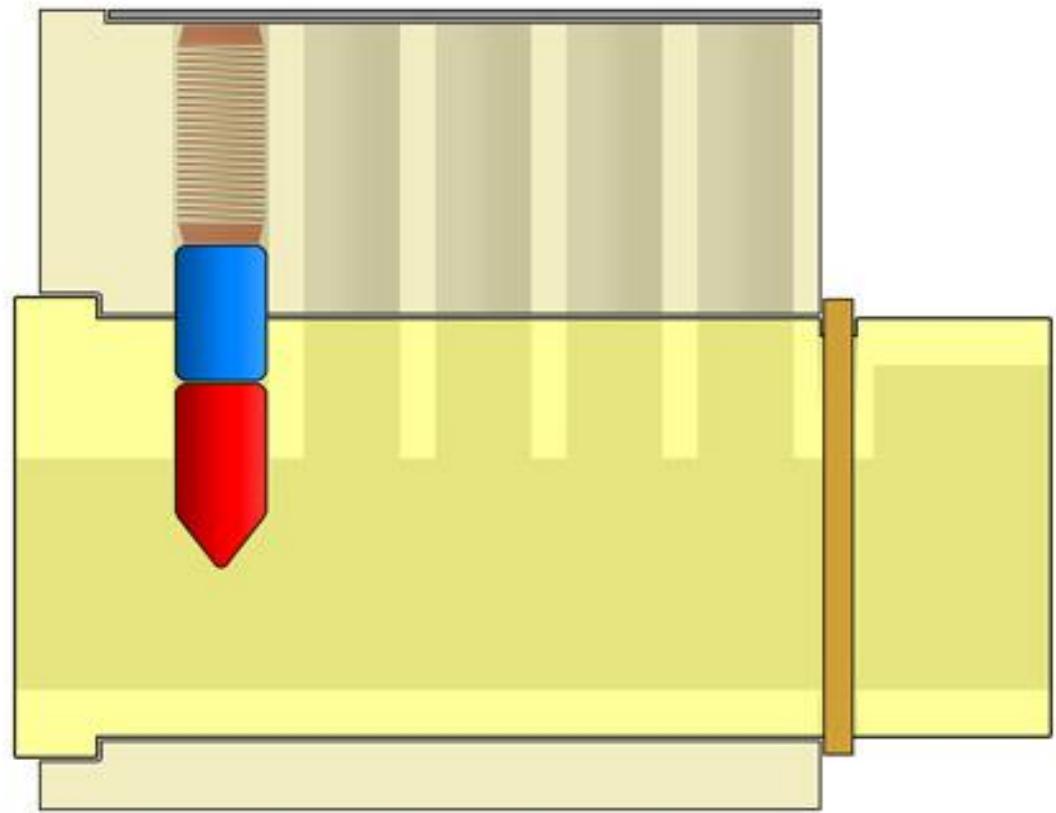
“Standard” Turning Tools



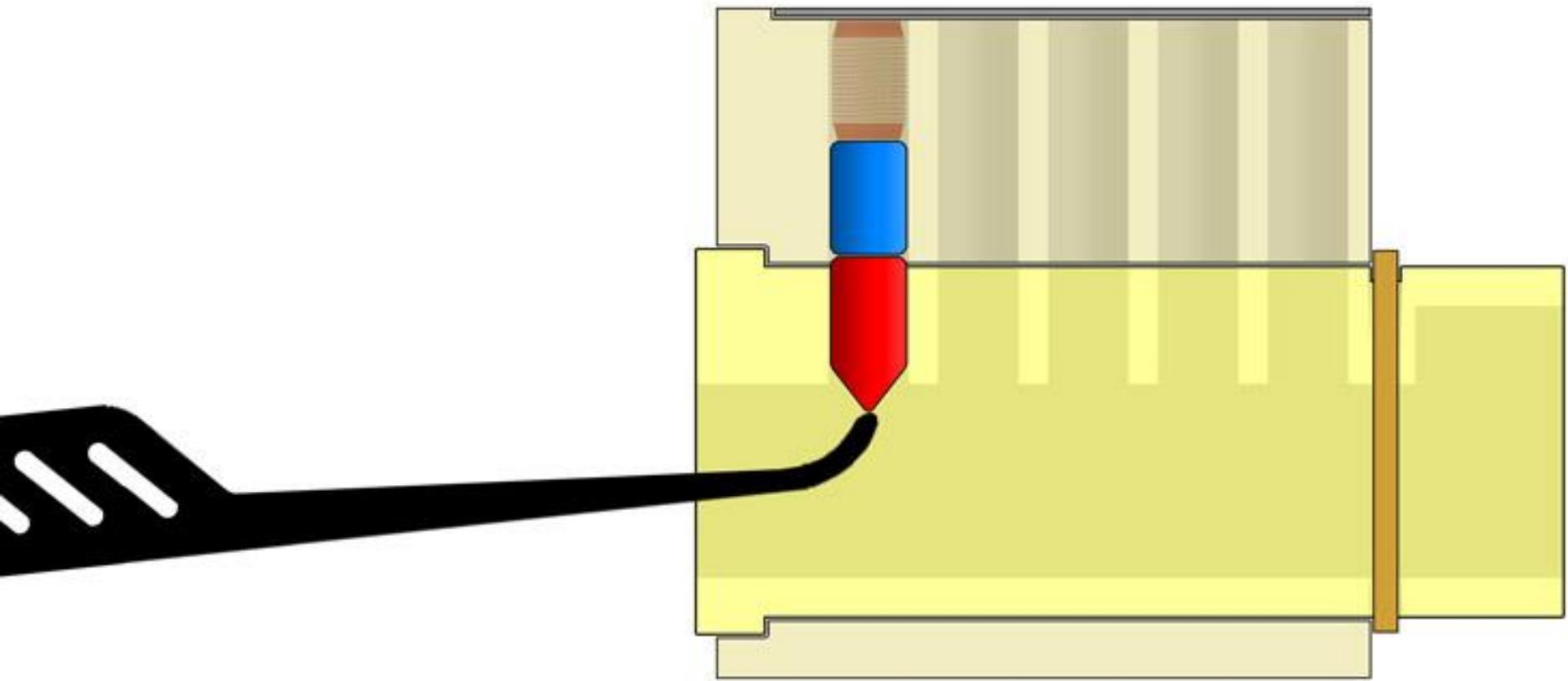
Space in the Keyway



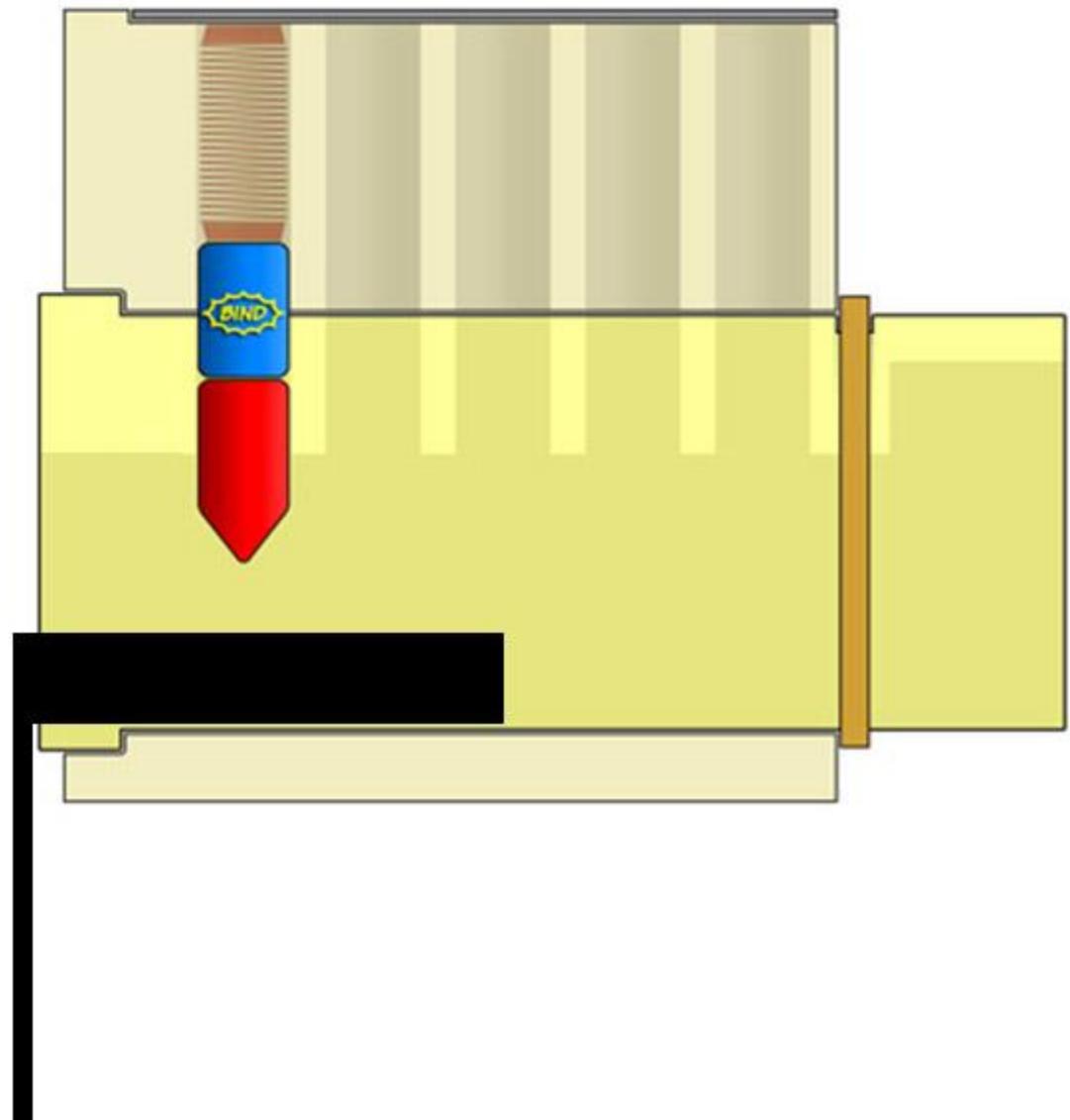
Starter Exercises



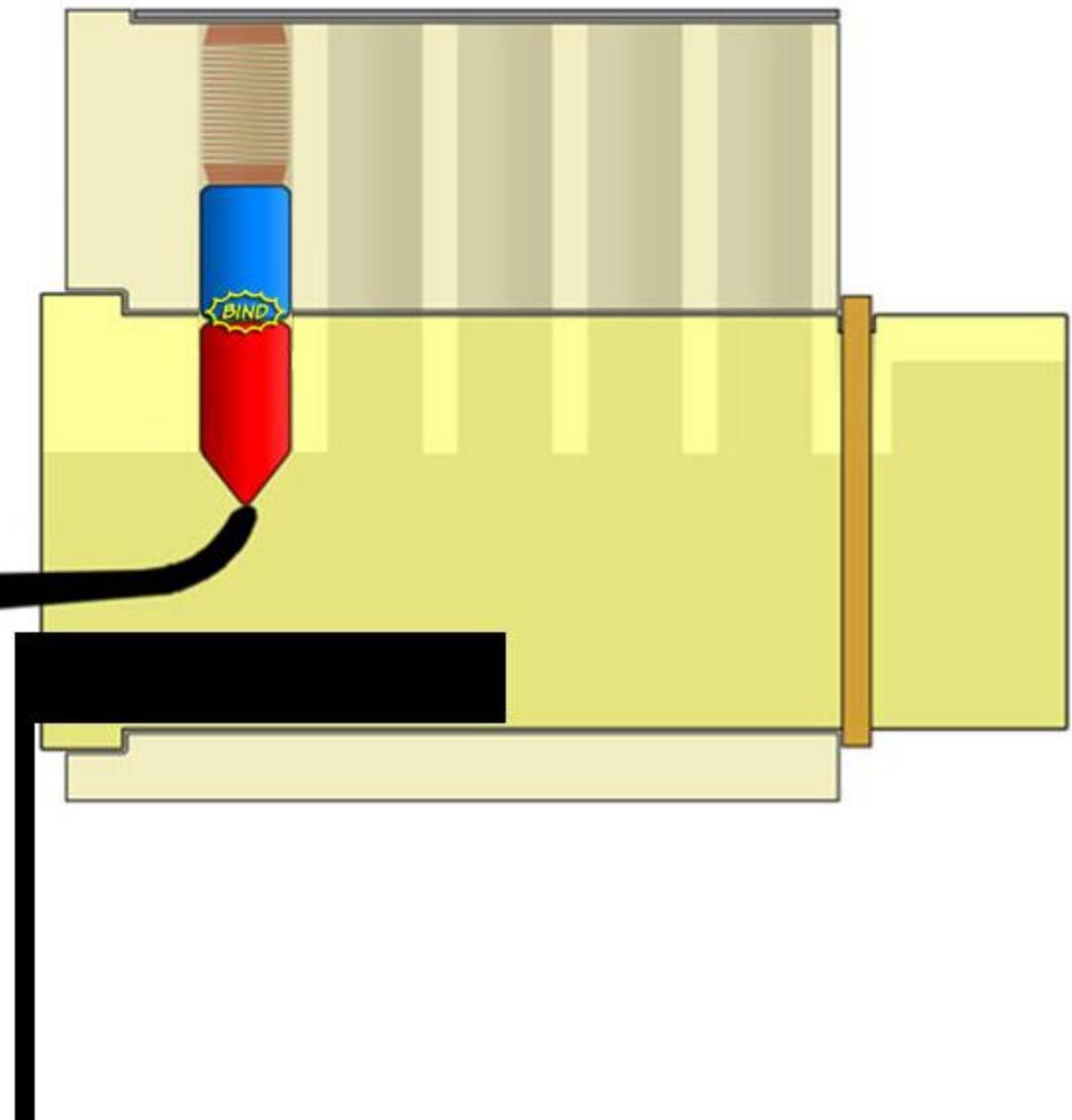
Starter Exercises



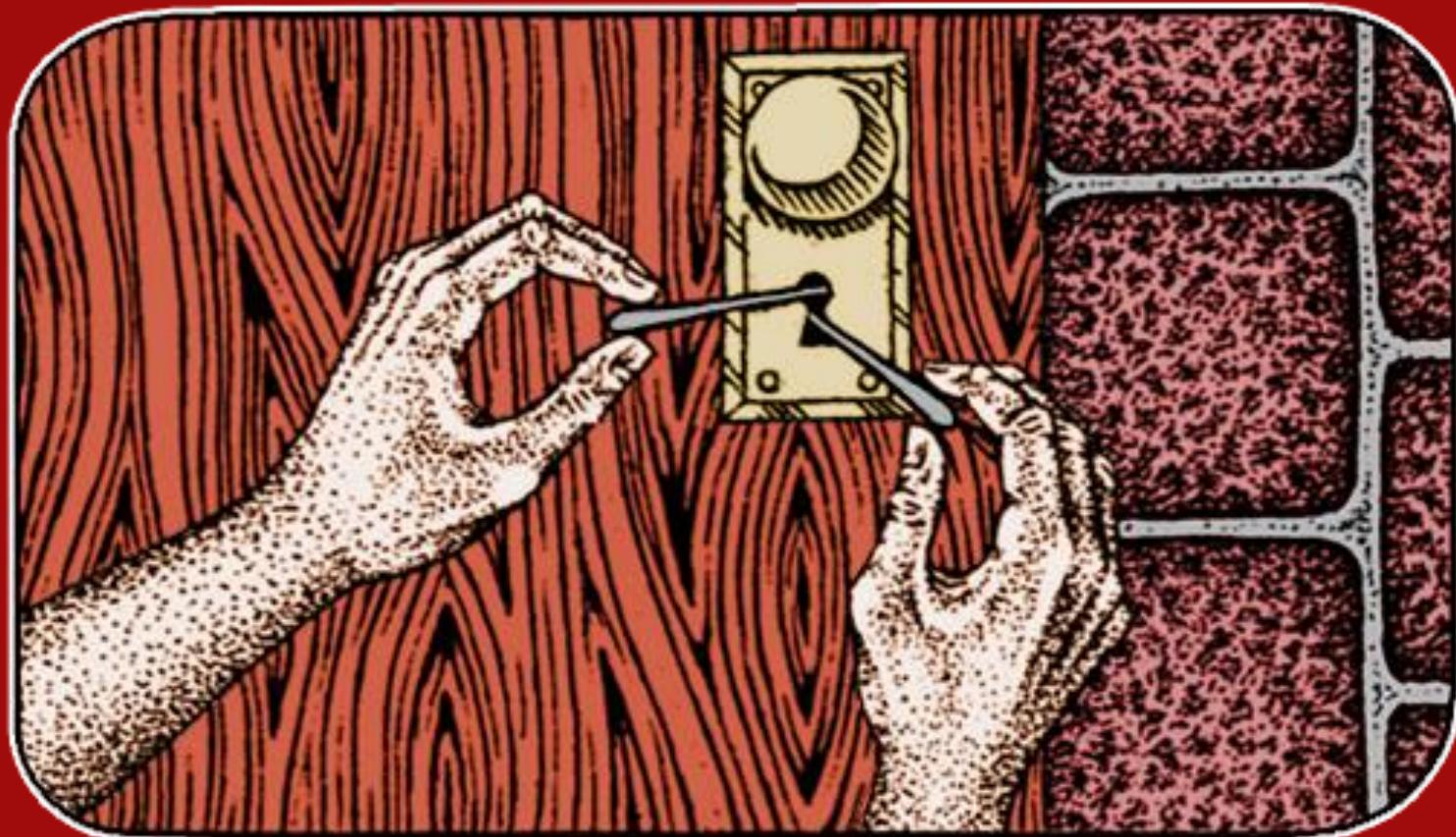
Starter Exercises



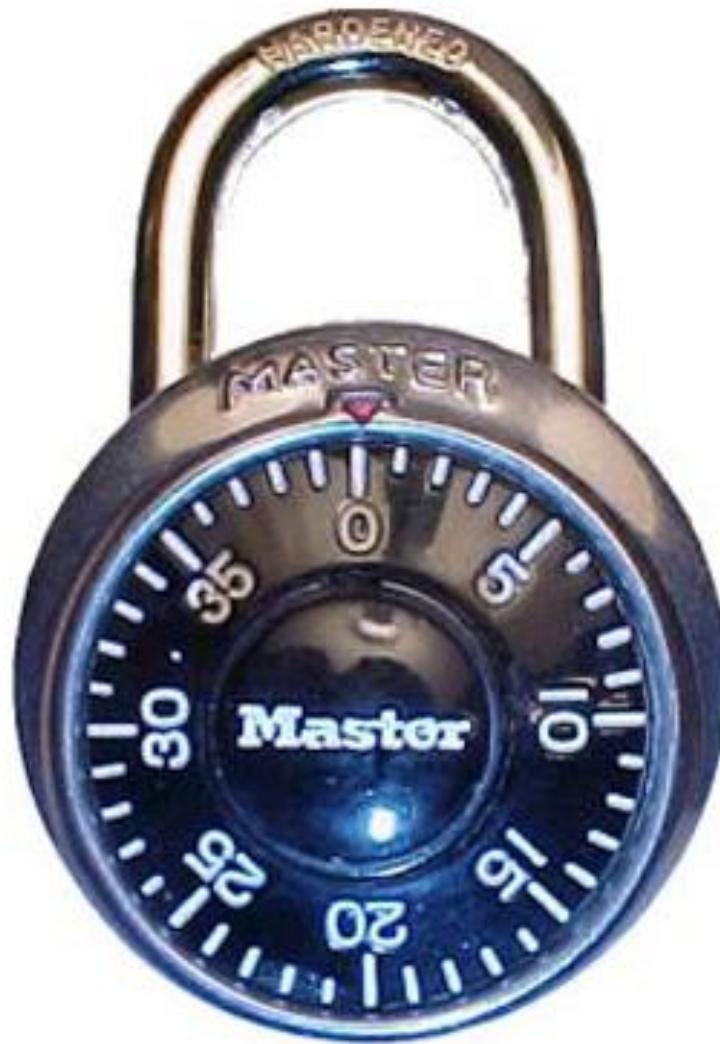
Starter Exercises



Shimming Padlocks



Combination Locks



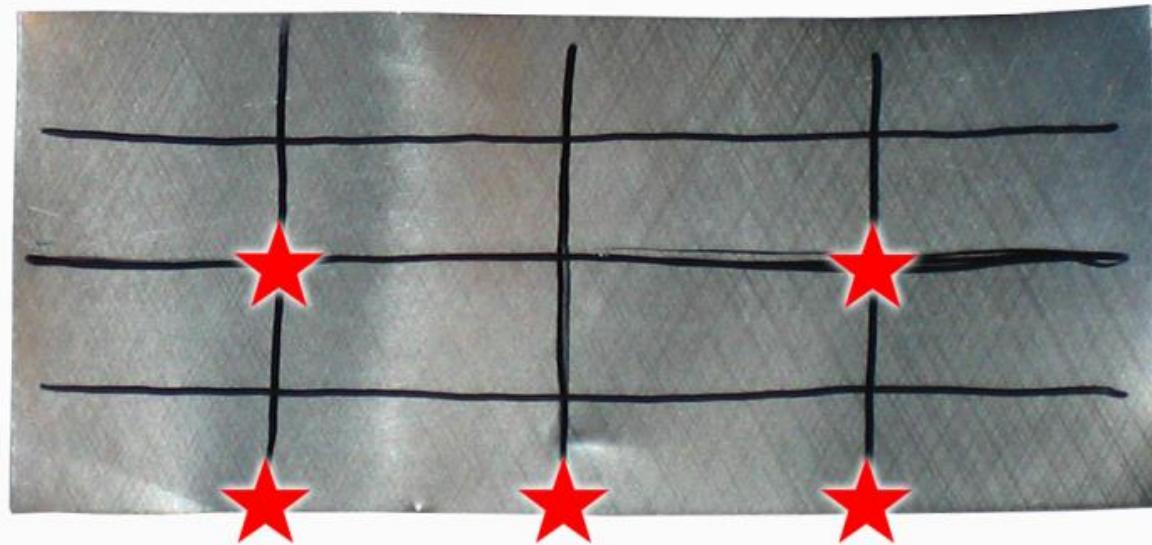
Padlock Shims



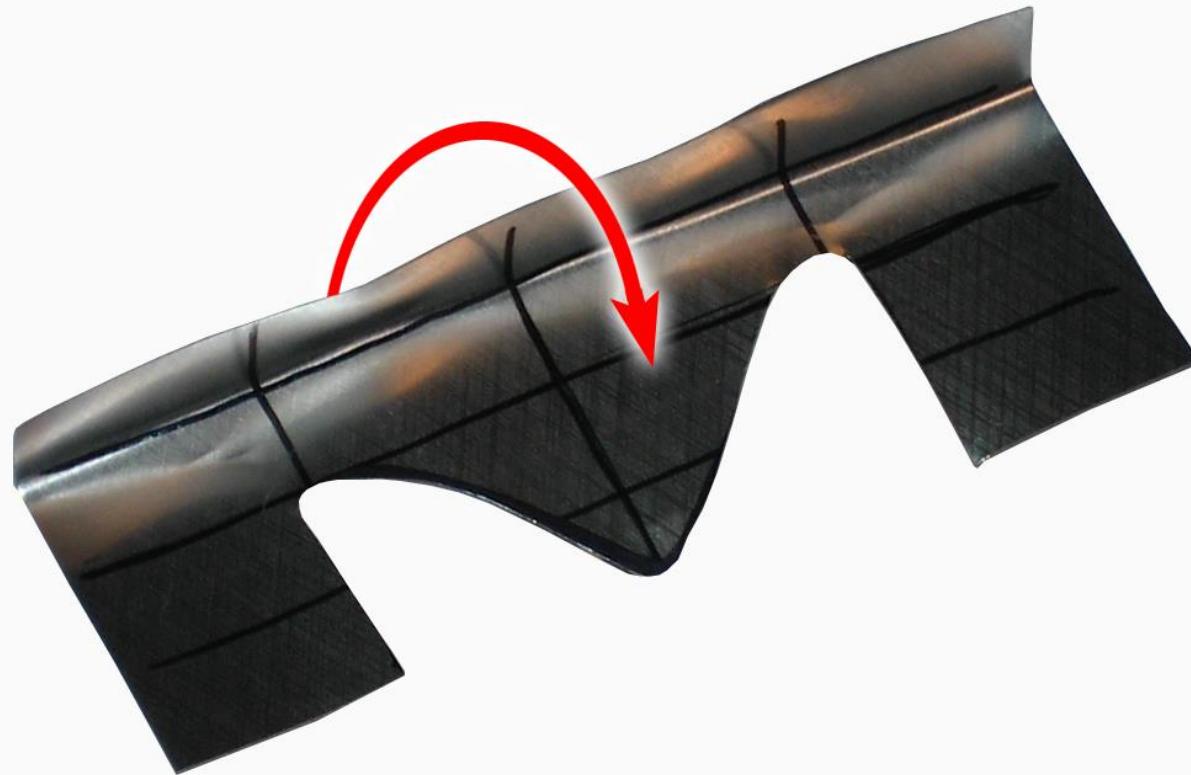
Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



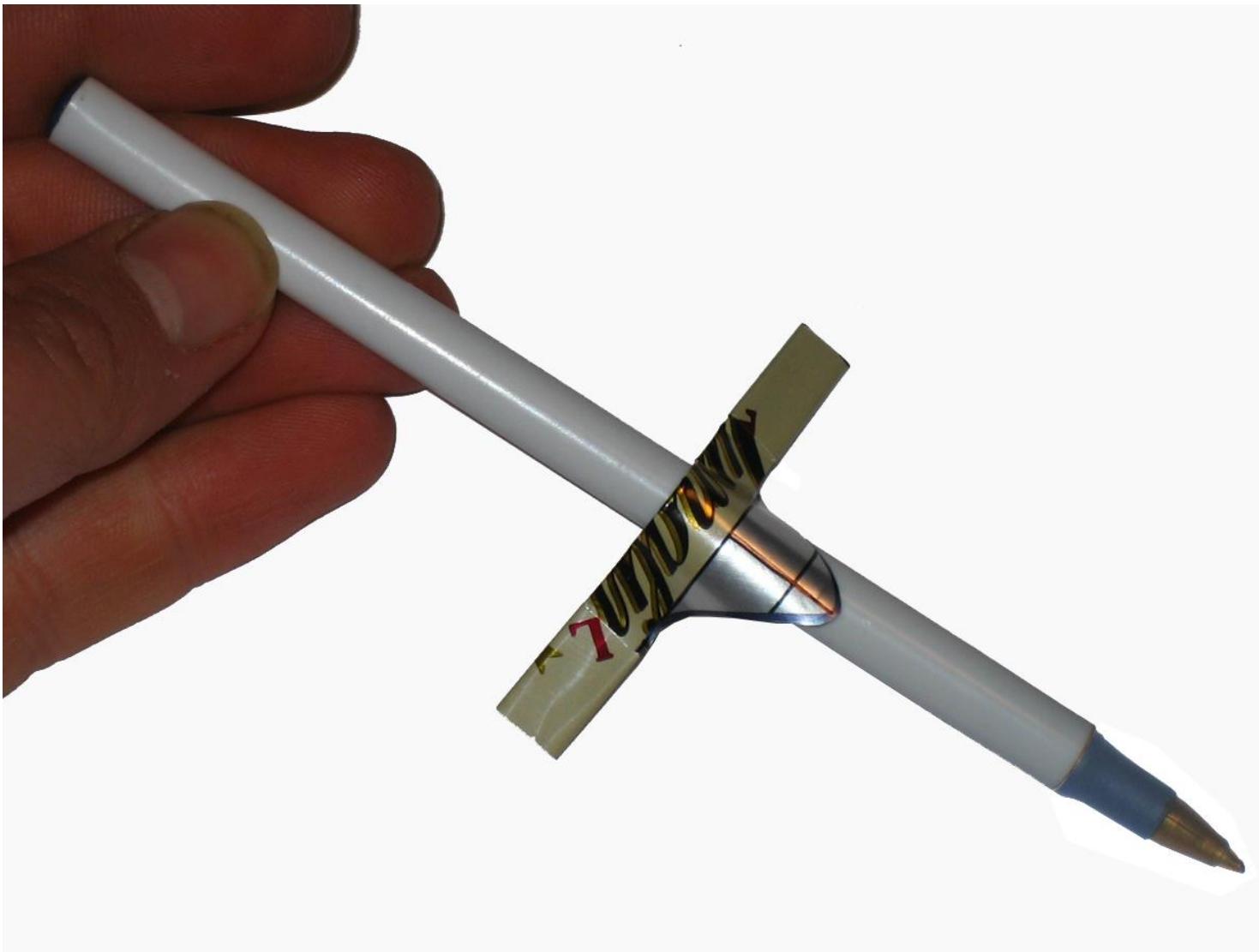
Homebrew Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



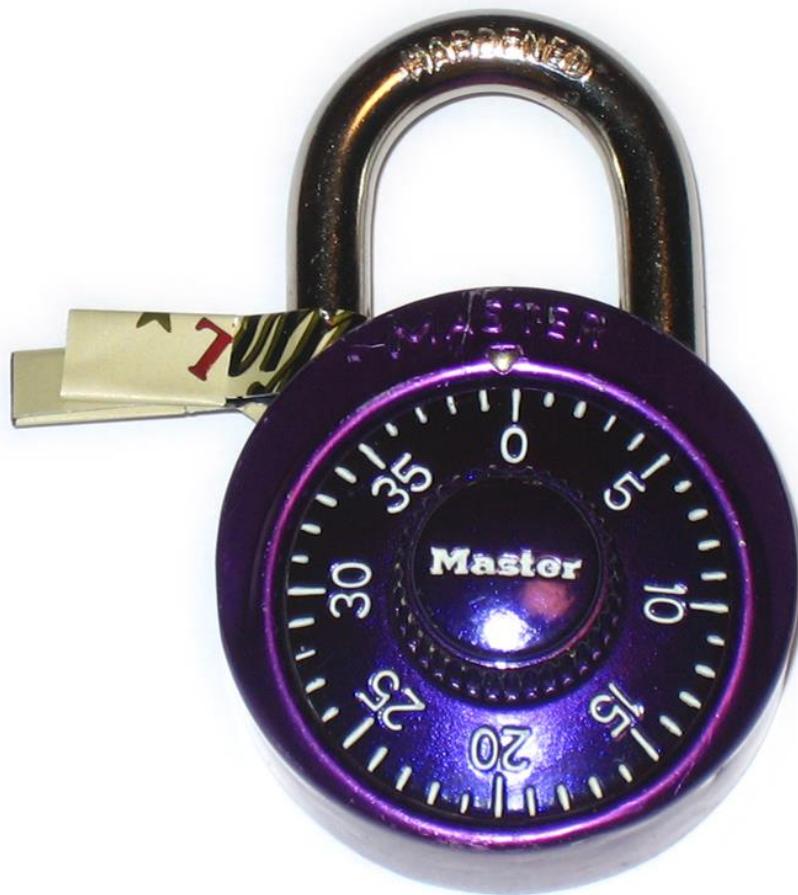
Homebrew Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



Homebrew Padlock Shims



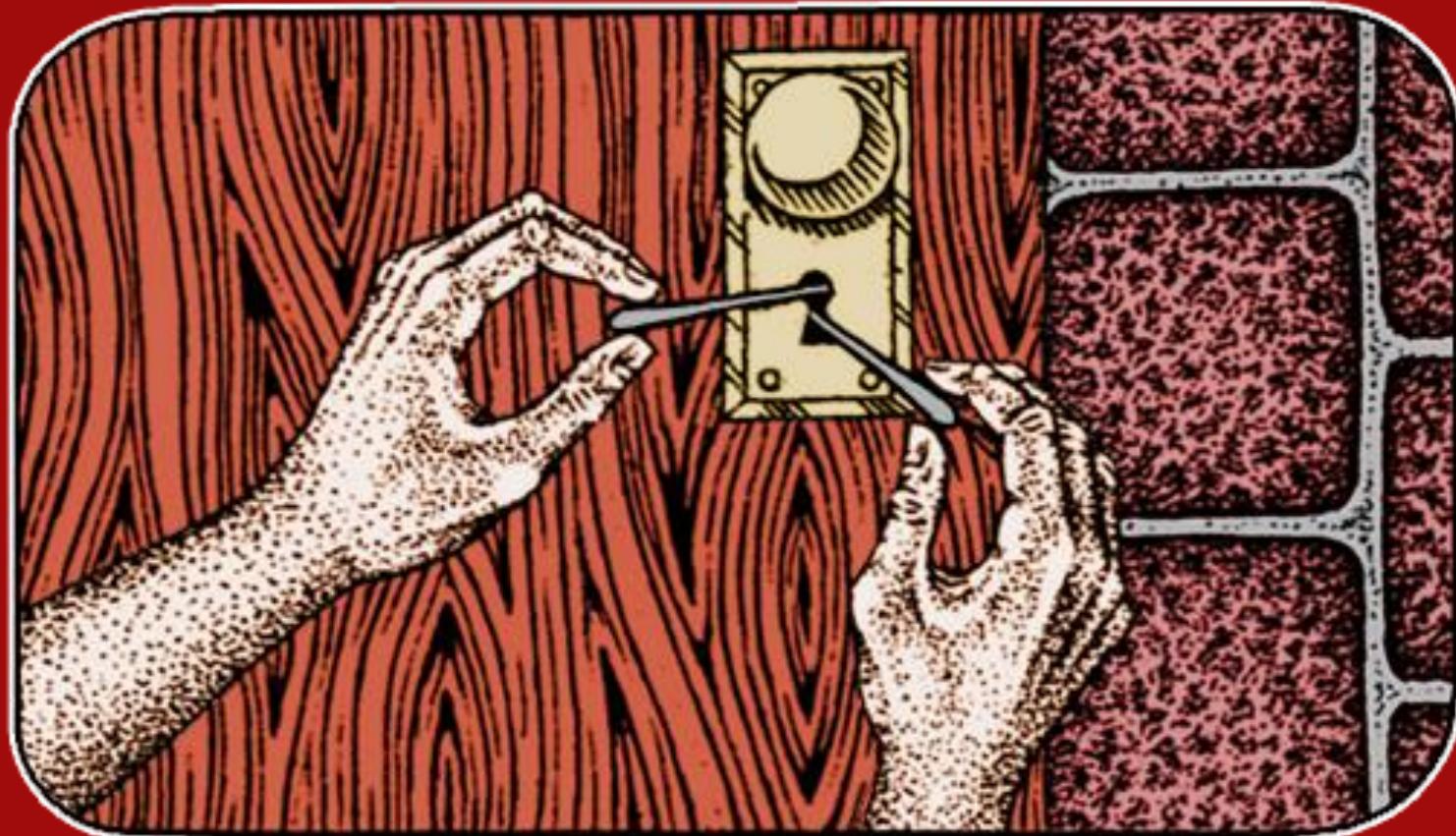
Shim-Proof Padlocks... Double-Ball Mechanism



Shim-Proof Padlocks... Double-Ball Mechanism

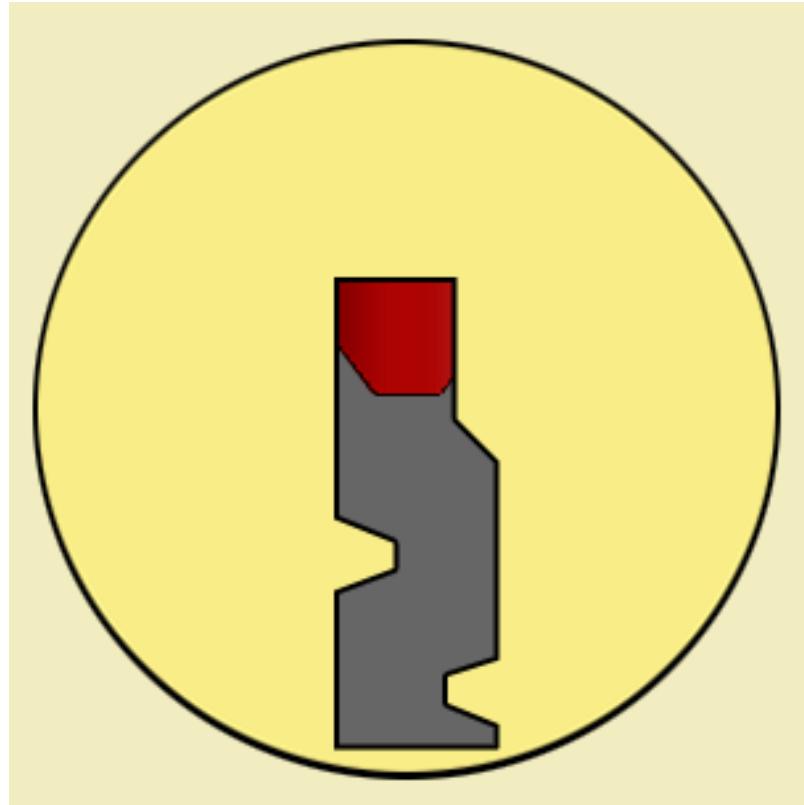


Pick-Resistant Locks



Pick-Resistant Keyways

Simple...

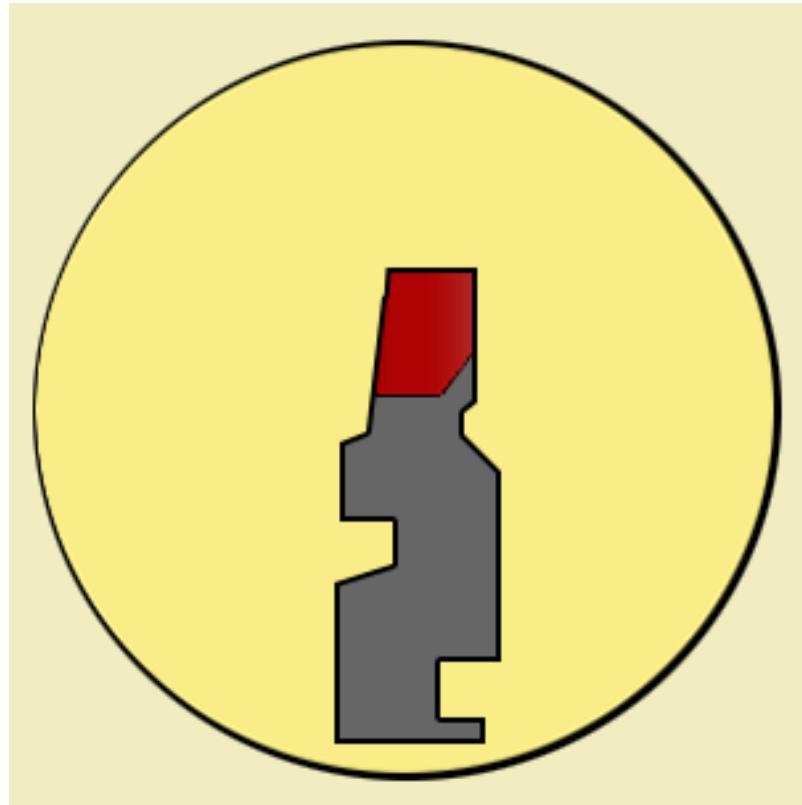


... straight and wide

Pick-Resistant Keyways

Simple...

Medium...



... straight and wide

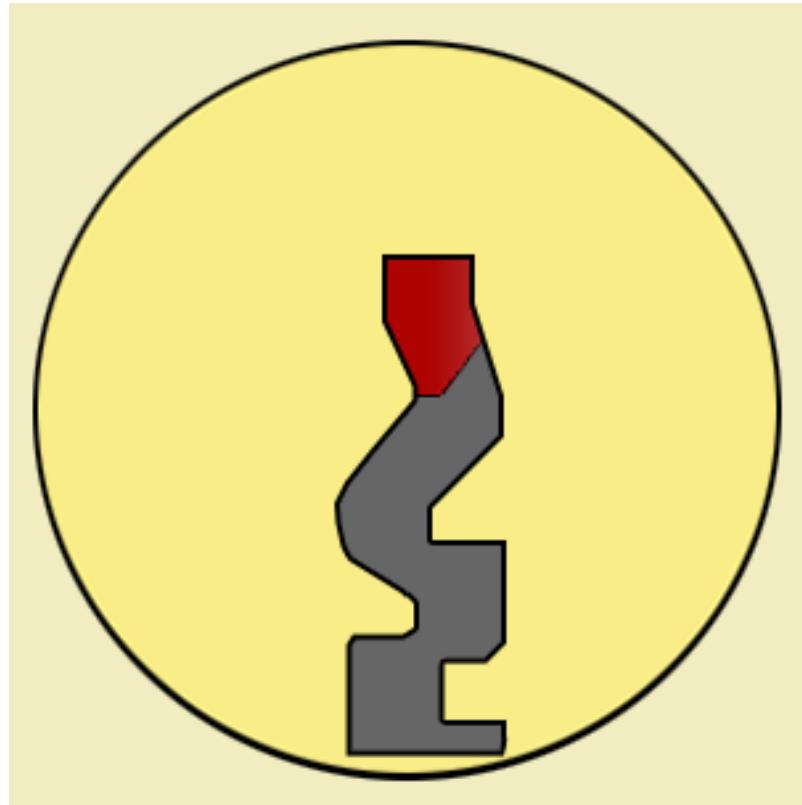
... straight but narrow

Pick-Resistant Keyways

Simple...

Medium...

Complex...



... straight and wide

... straight but narrow

... thinner and curvy

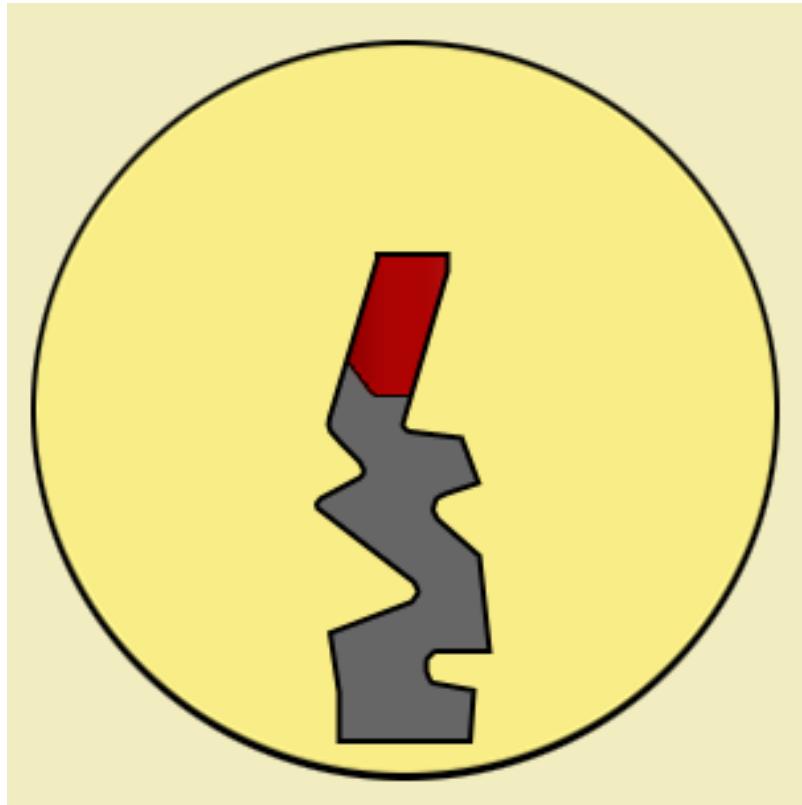
Pick-Resistant Keyways

Simple...

Medium...

Complex...

Hard...



... straight and wide

... straight but narrow

... thinner and curvy

... lots of angles

Pick-Resistant Keyways

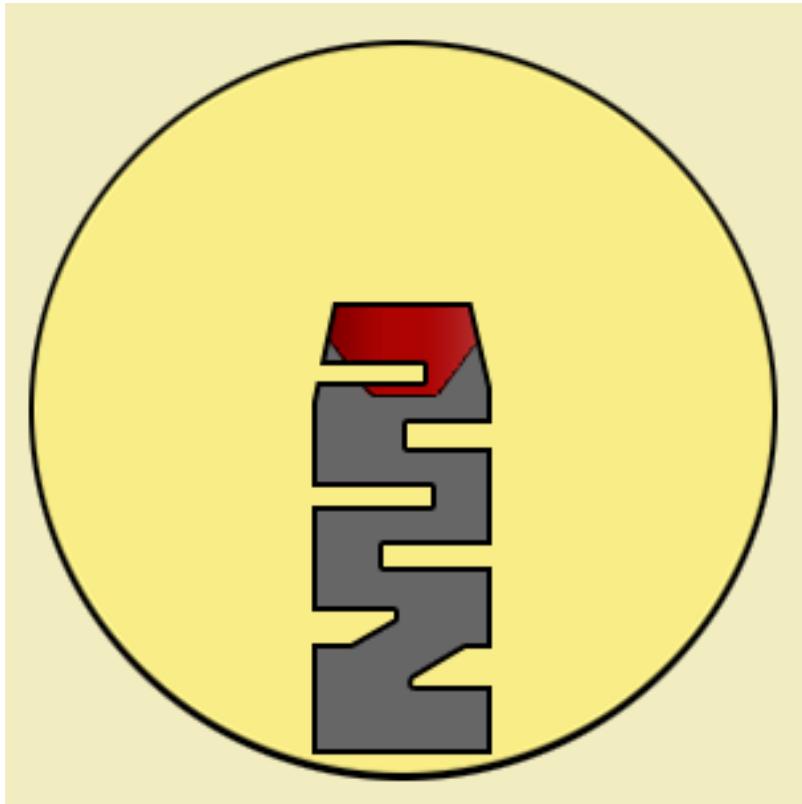
Simple...

Medium...

Complex...

Hard...

Fiendish...



... straight and wide

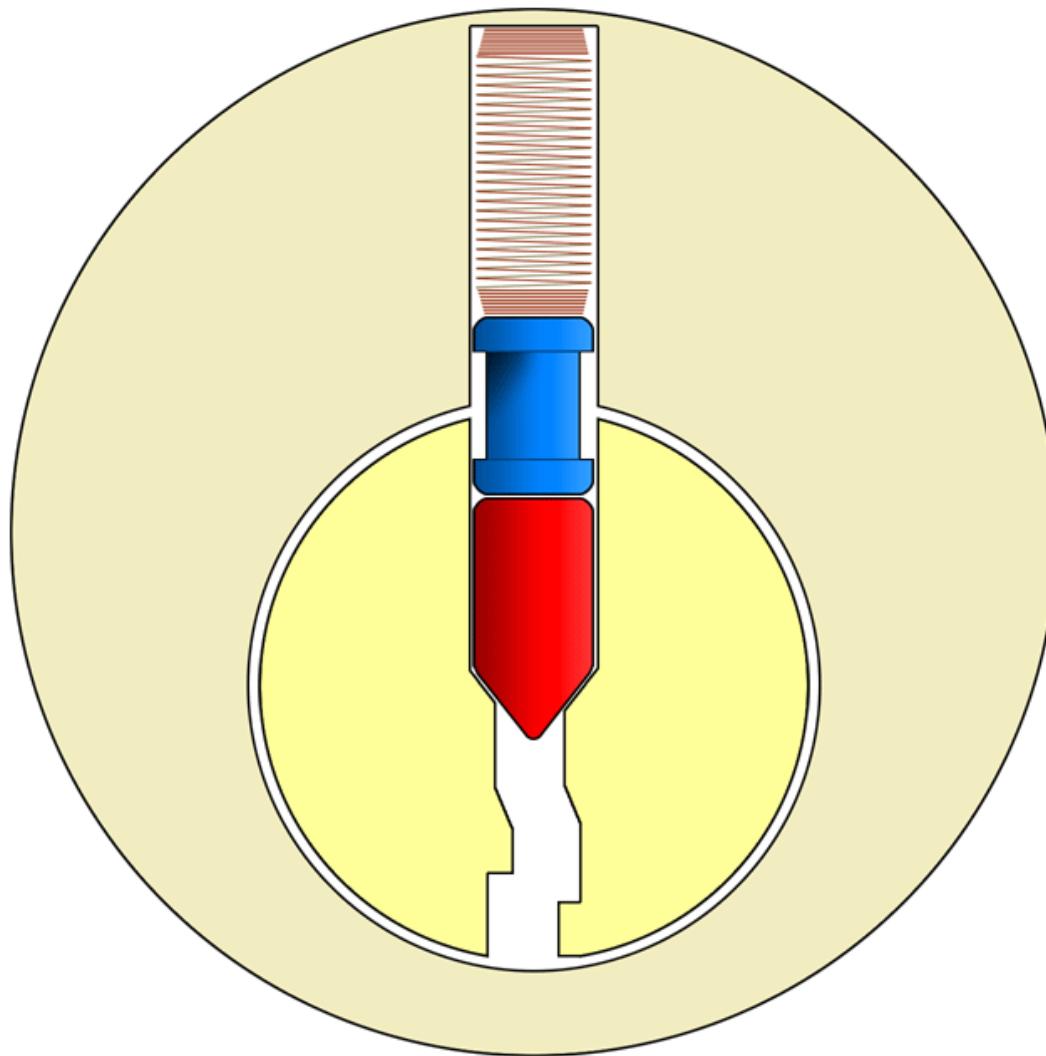
... straight but narrow

... thinner and curvy

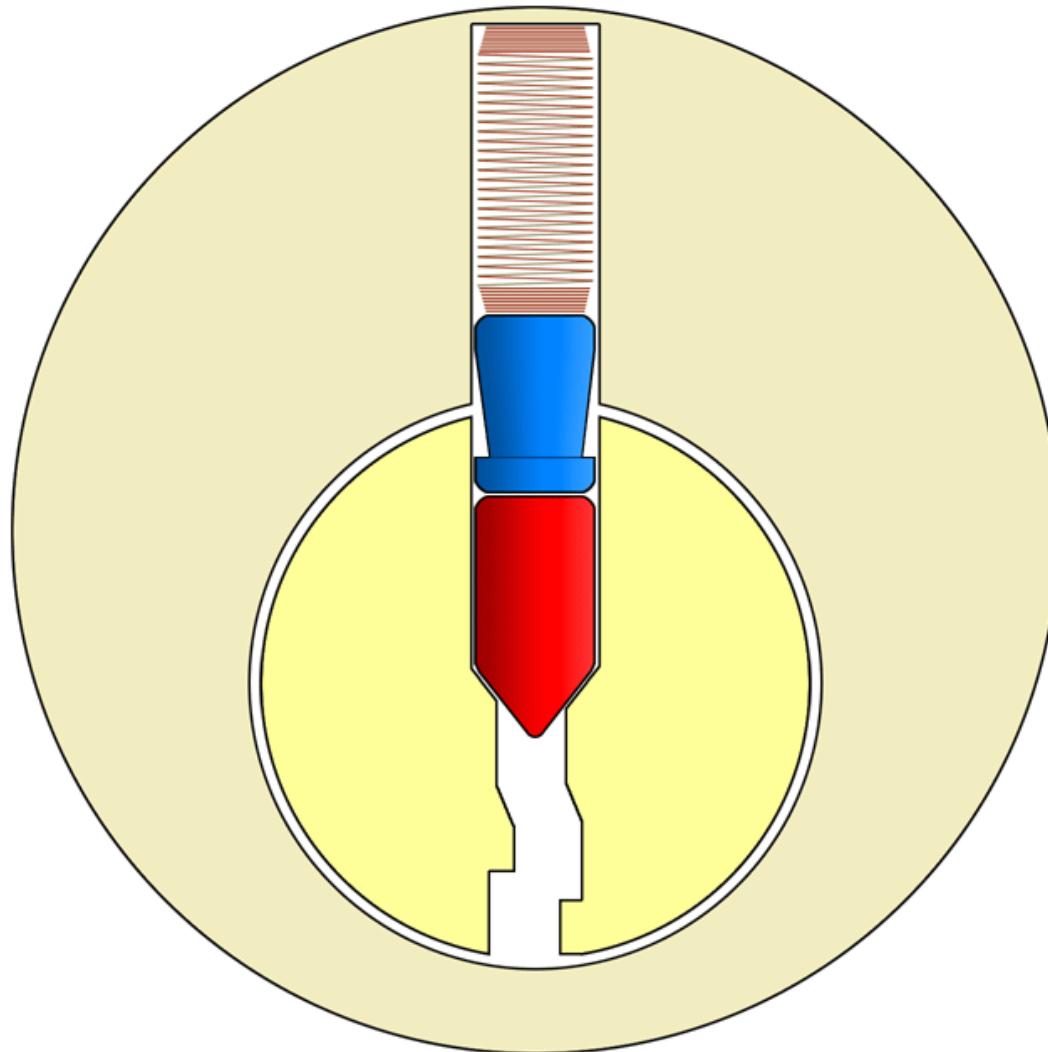
... lots of angles

... overlapping wards

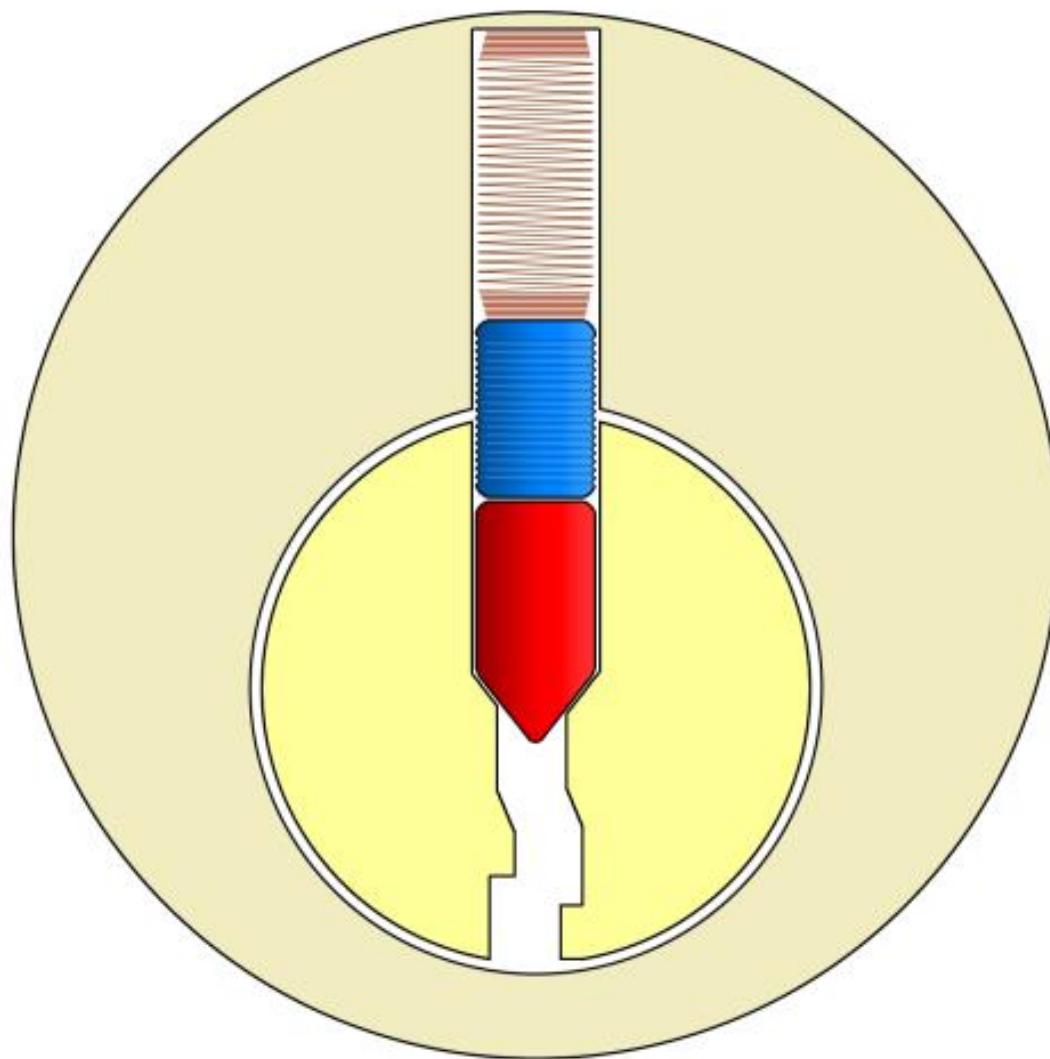
Pick-Resistant Pins



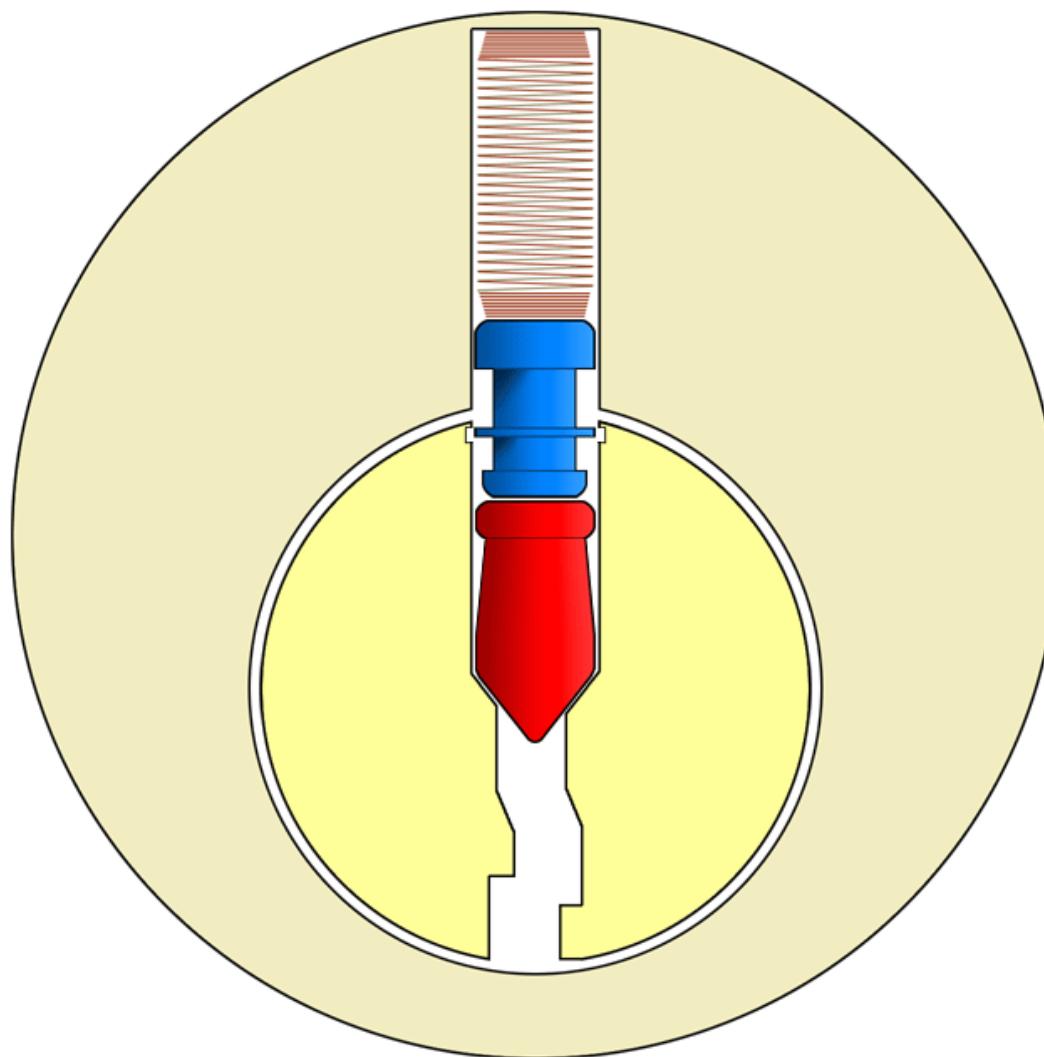
Pick-Resistant Pins — Mushroom Pin



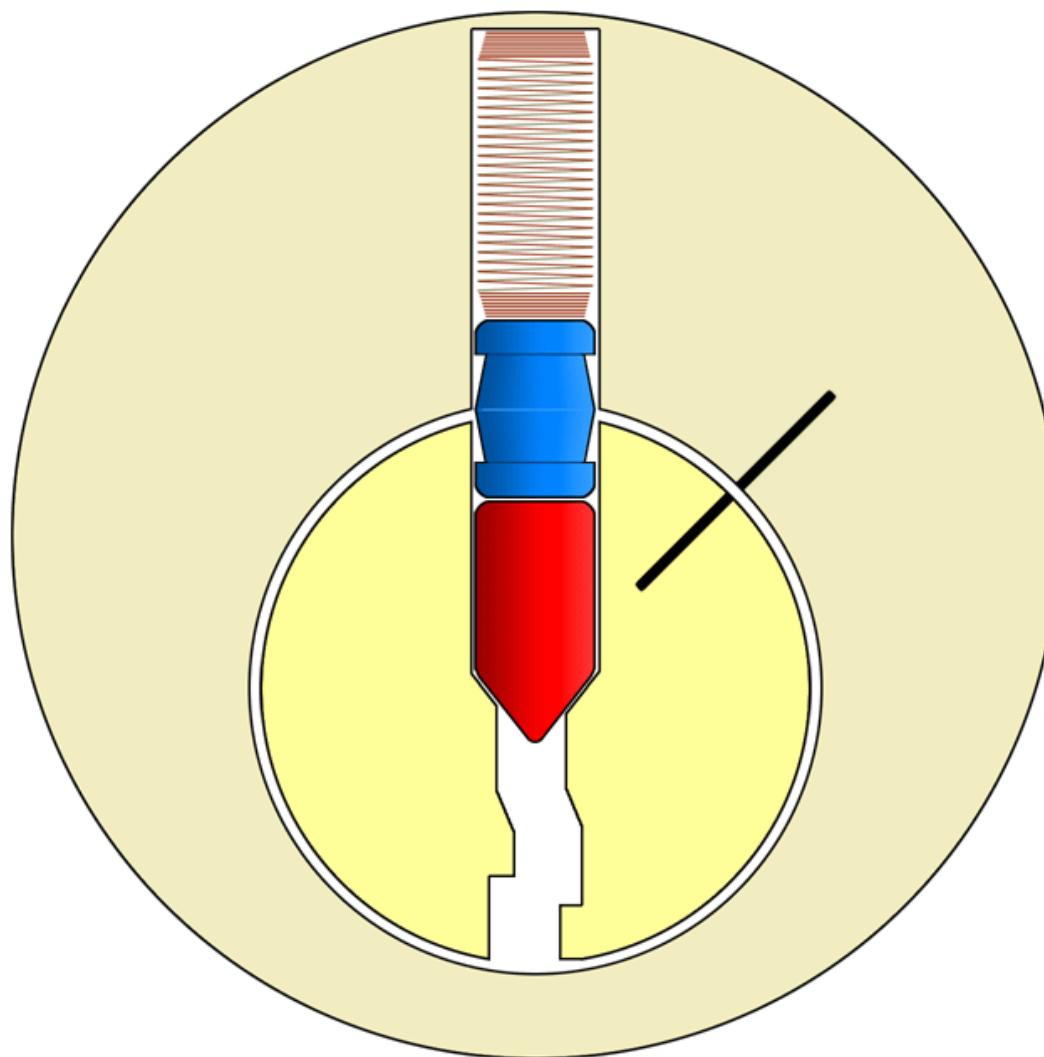
Pick-Resistant Pins — Serrated Pin



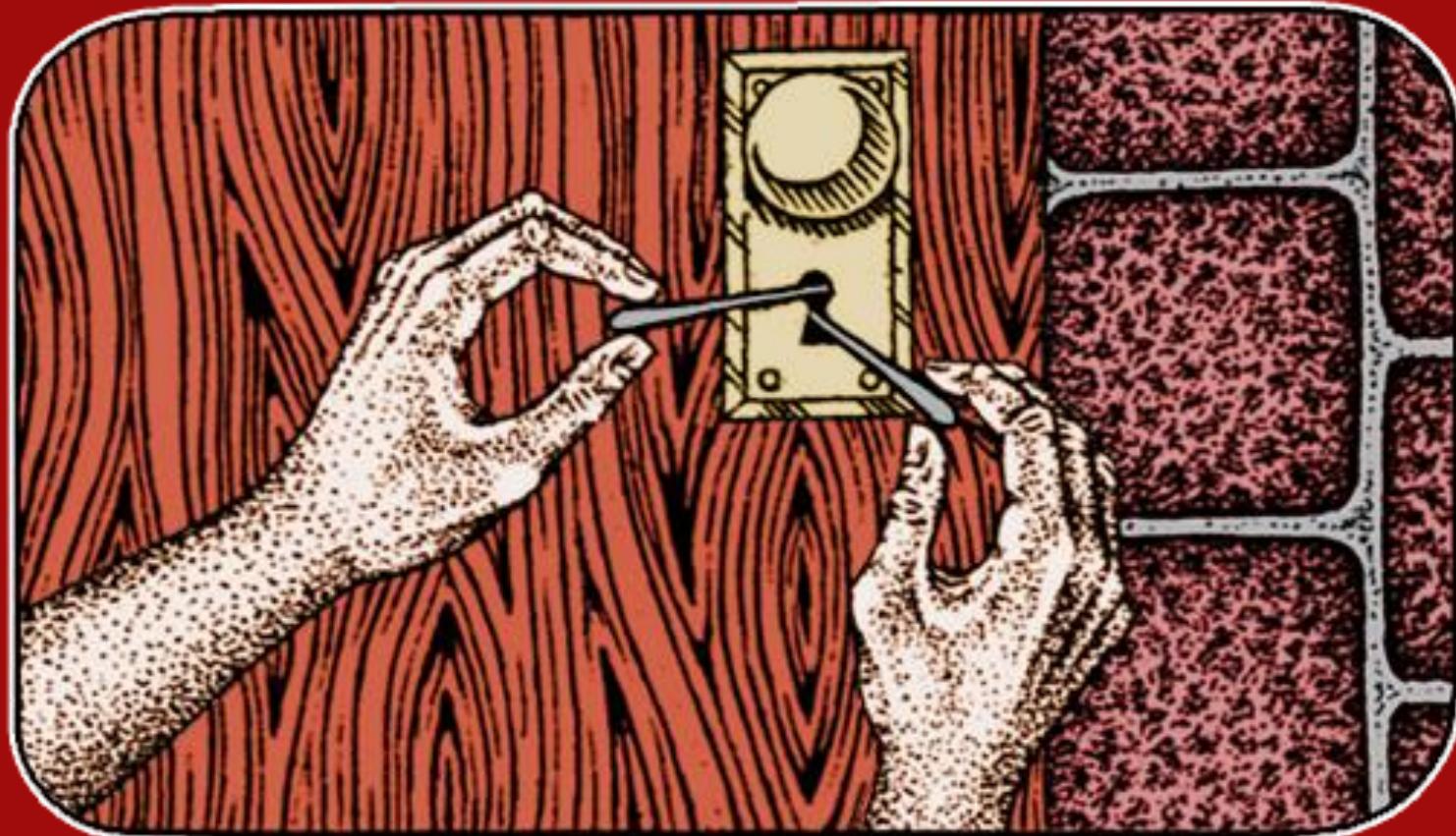
Pick-Resistant Pins – ASSA “Sneaky” Pin



Pick-Resistant Pins – TrioVing “Double Mushroom” Pin



Bumping Attacks

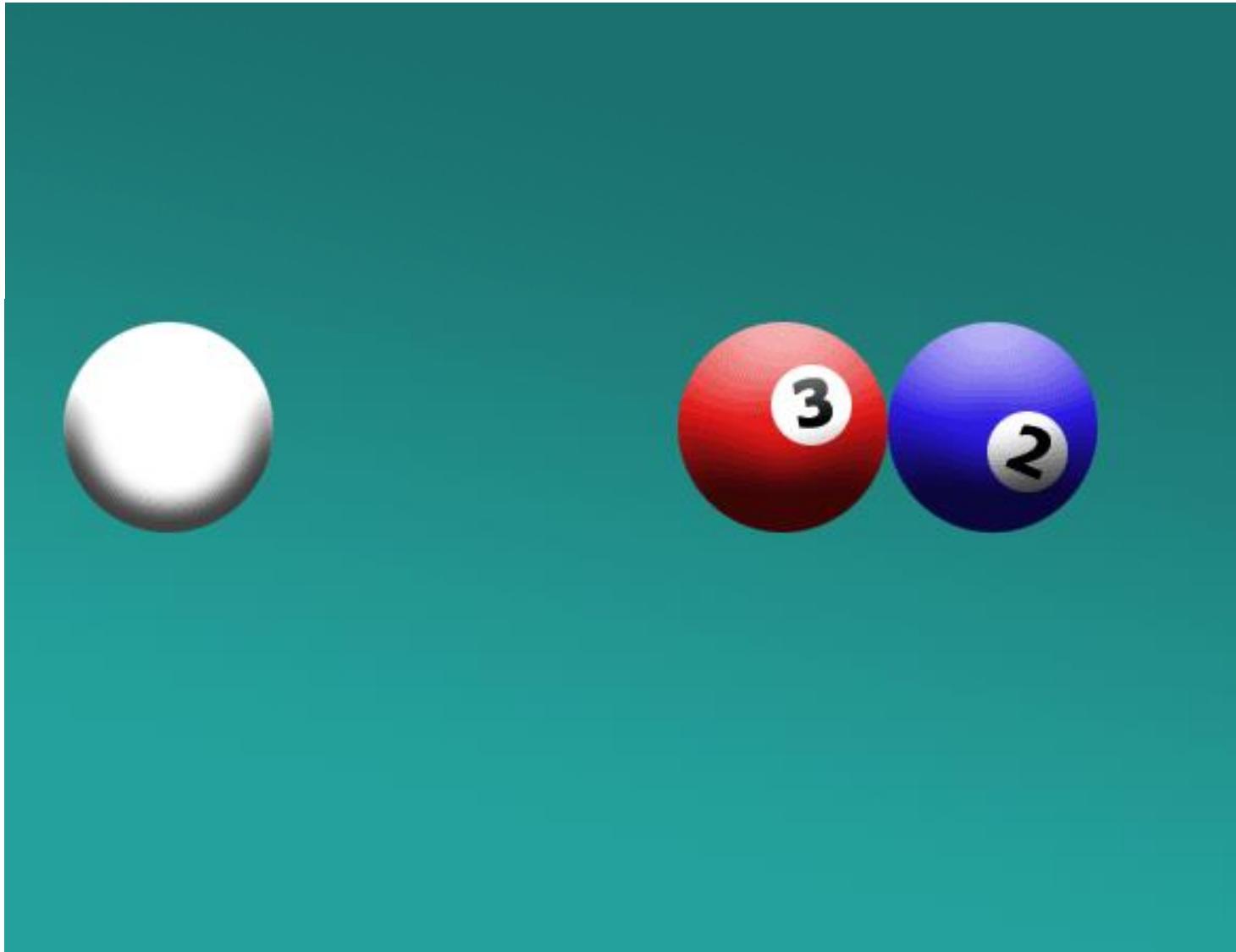


Lock Bumping

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



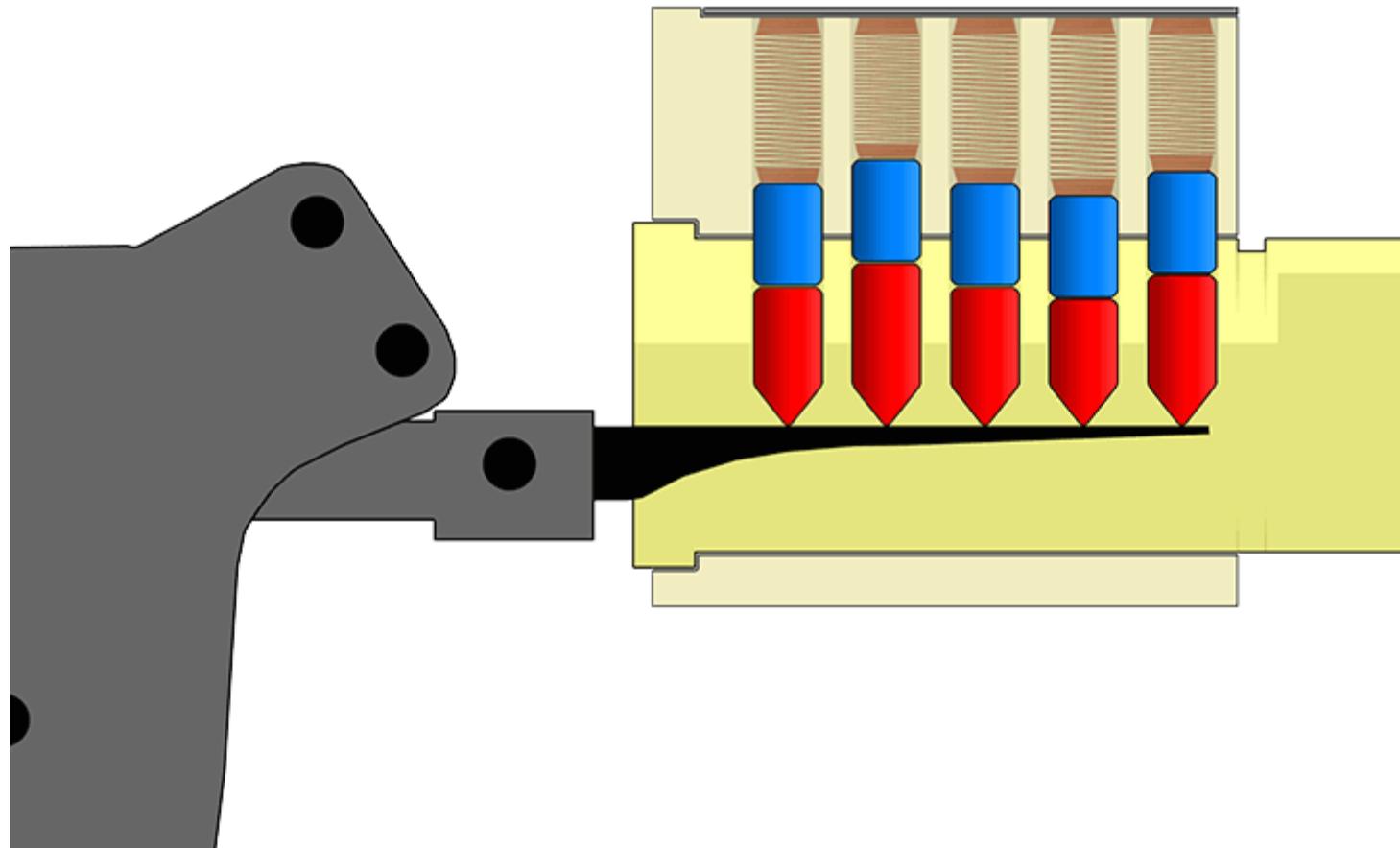
Lock Bumping



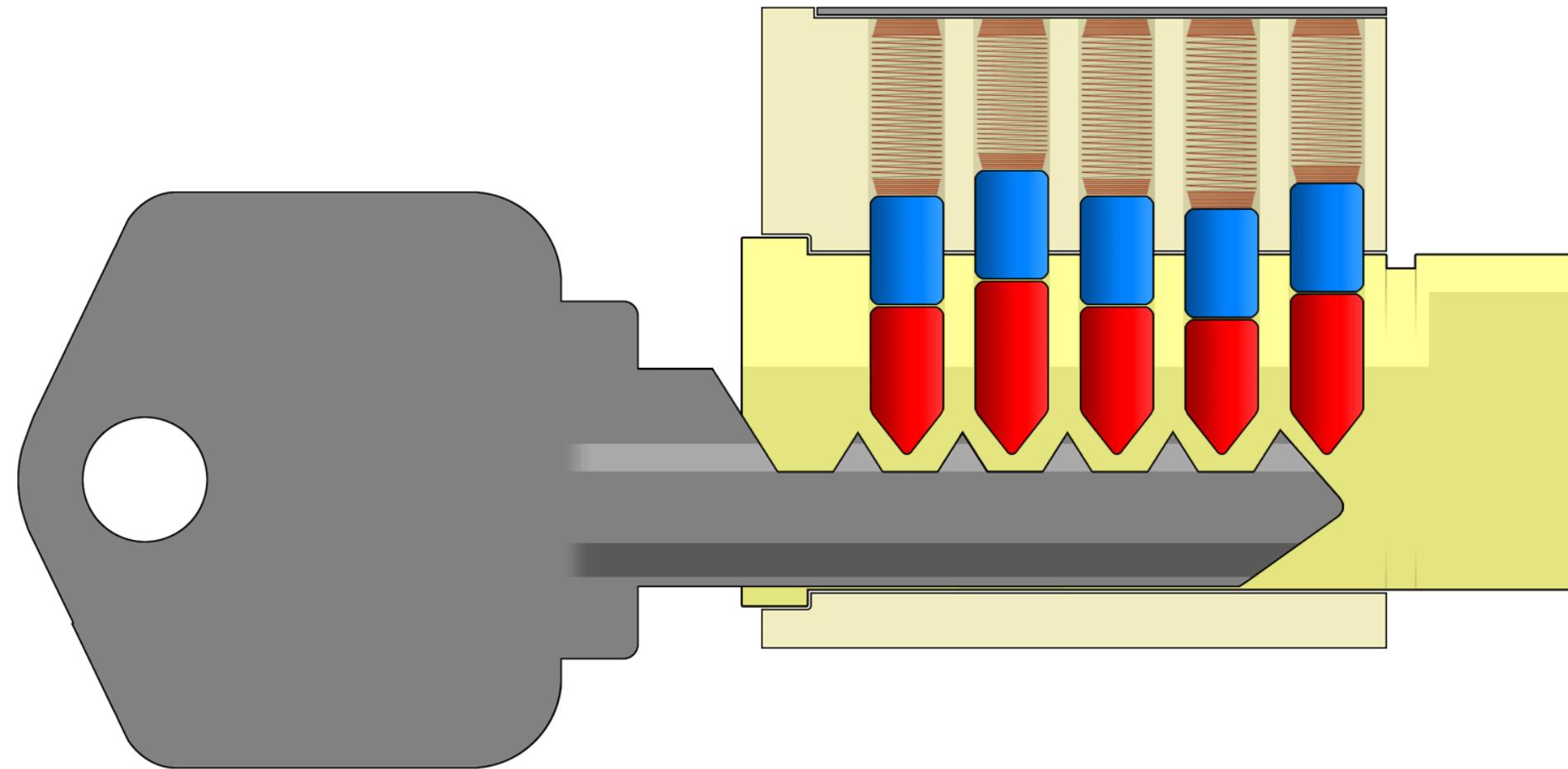
Snapping Guns



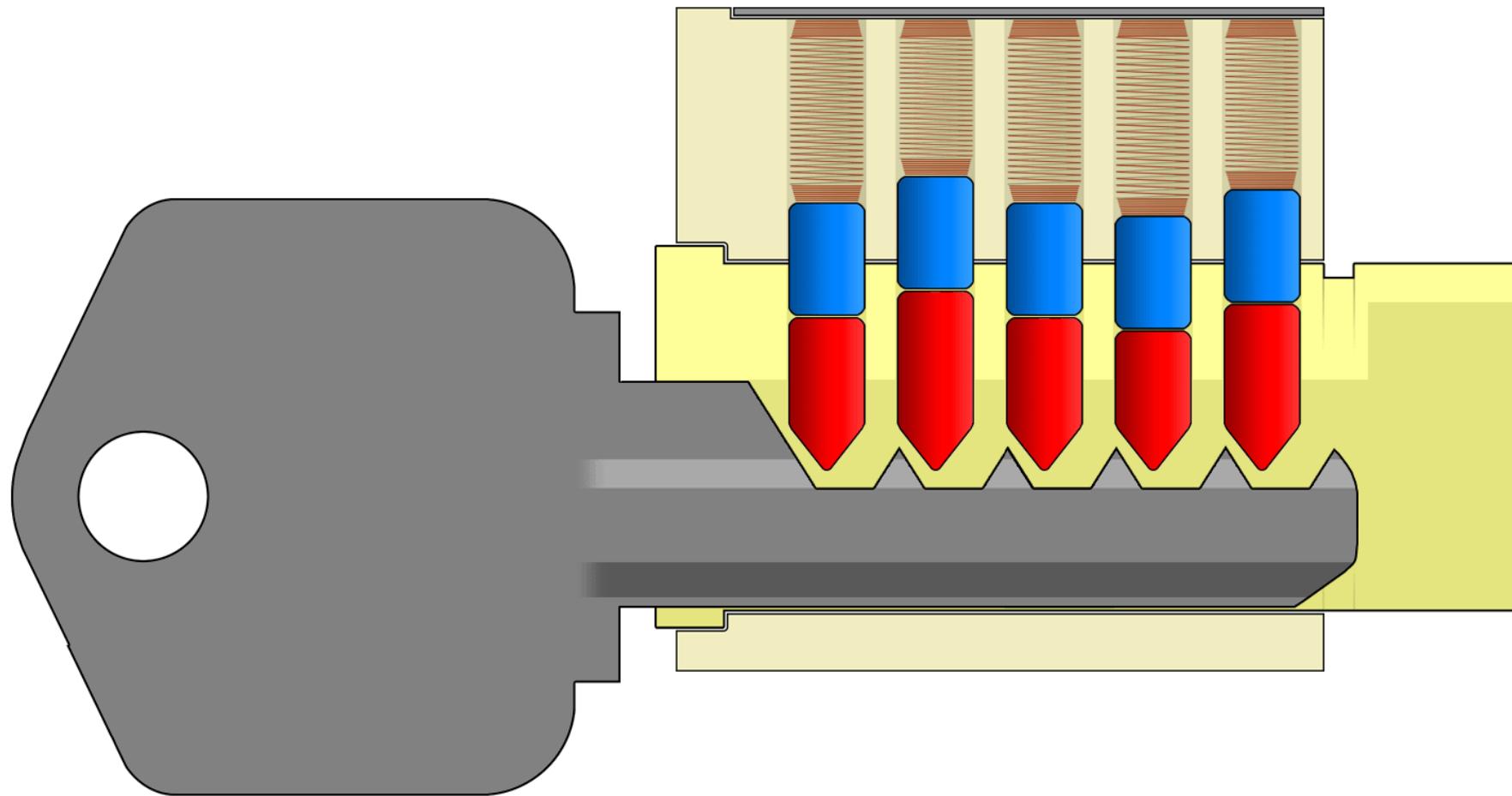
Snapping Guns



Lock Bumping – Pull Method



Lock Bumping – Push Method



Lock Bumping



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

Lock Bumping

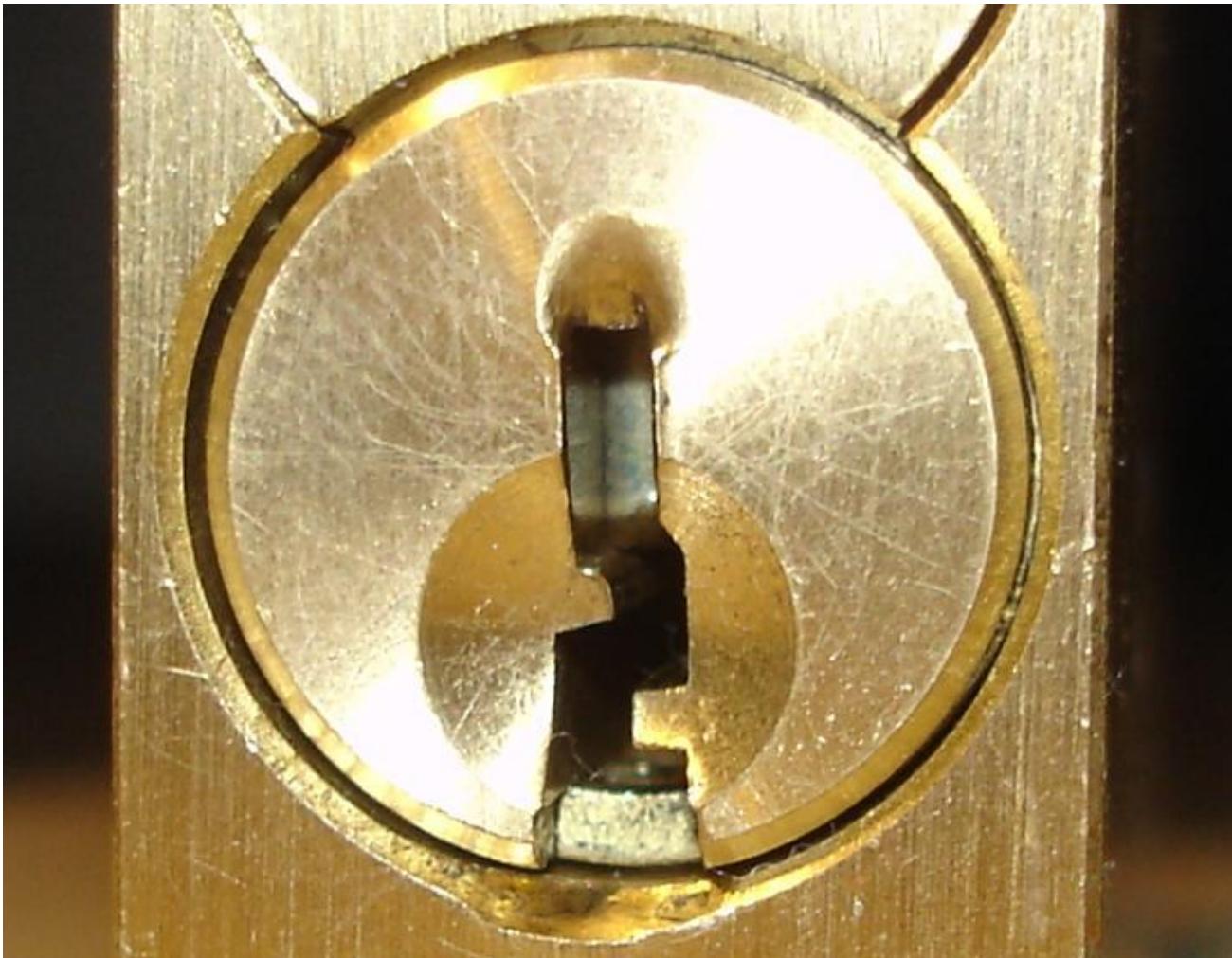
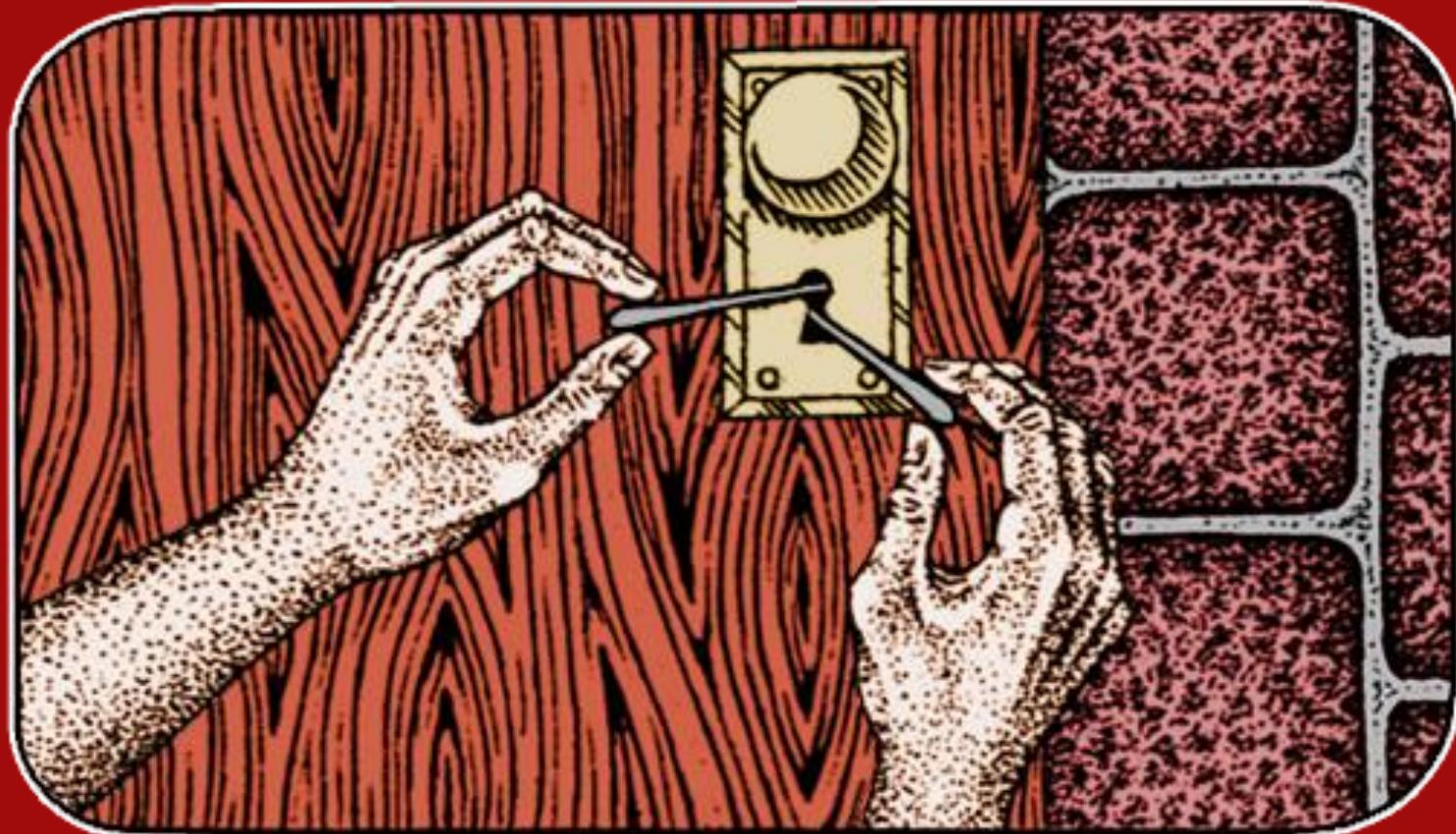


photo courtesy of datagram

Looking for a better lock now?



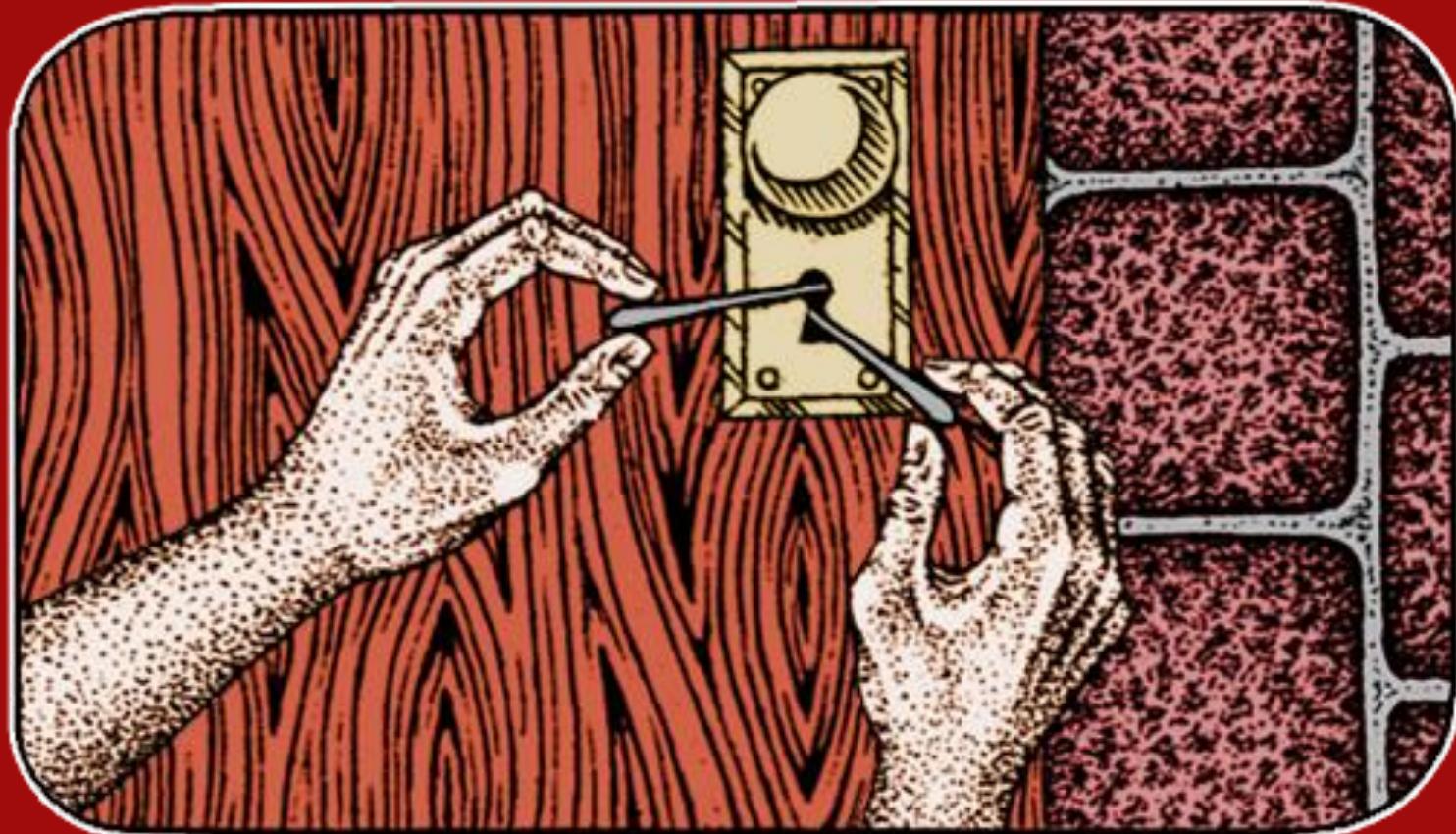
1. ALOA logo / ALOA number
2. Name Discrepancies
3. Estimates & Itemized Invoice
4. Credentials & Identification
5. Your Right to Refuse

High security locks

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

<https://securitysnobs.com/>

Teleduplication and 3D Printing



Tele... what?!

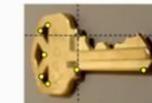
Attack: Teleduplication



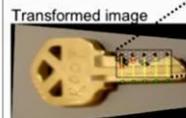
Target Key: Labeling key points



...



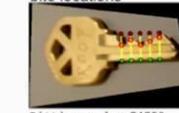
Transformed Target: Labeling cut depths



Transformed image



User-specified bite locations



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>

Material Strength

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)

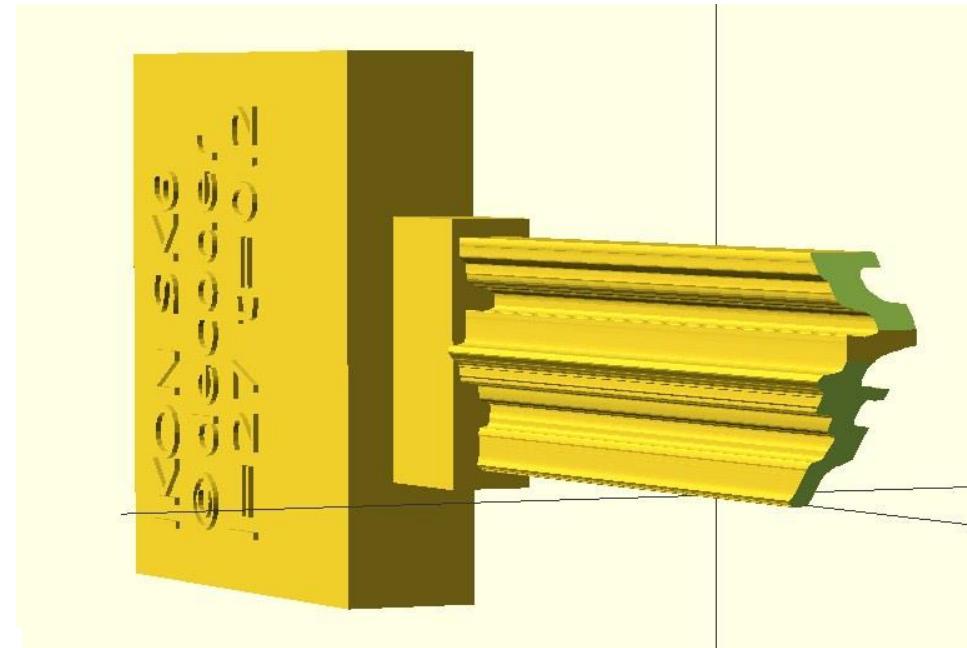
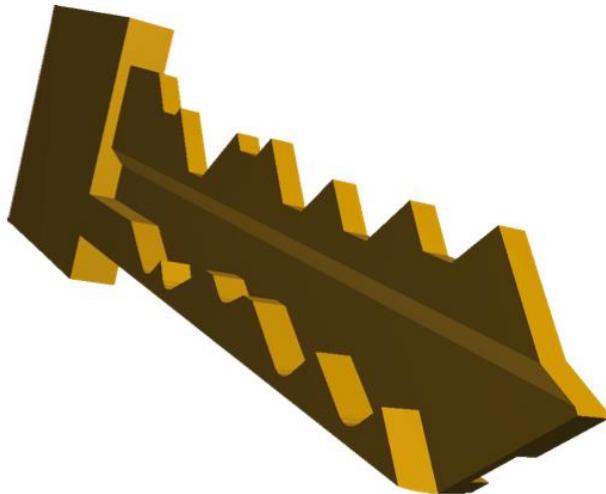
Run the following line for a bump key:

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



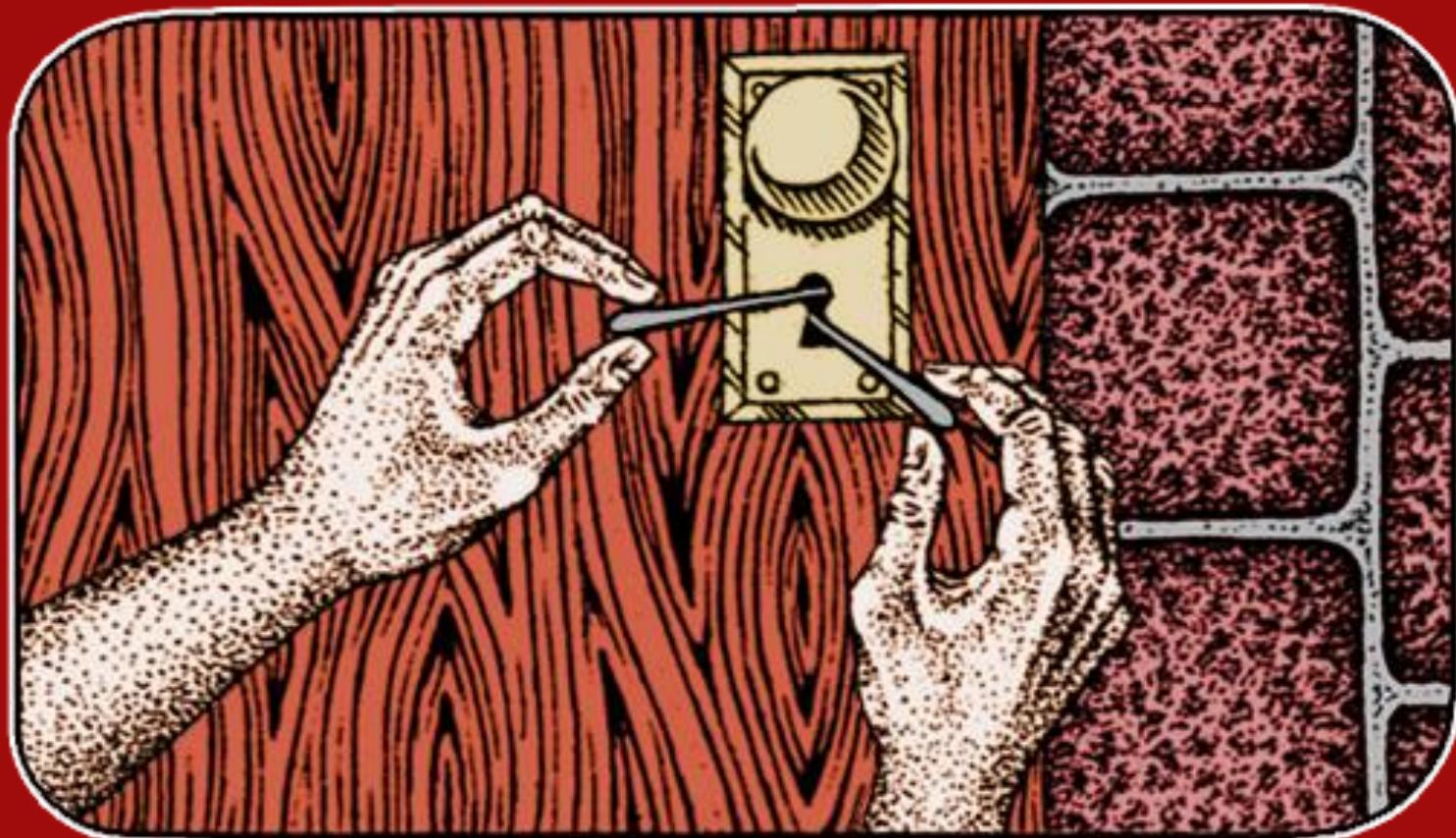
Works even better for high security locks!

Ikon SK6



Schlage Primus

Distinguishing Picks



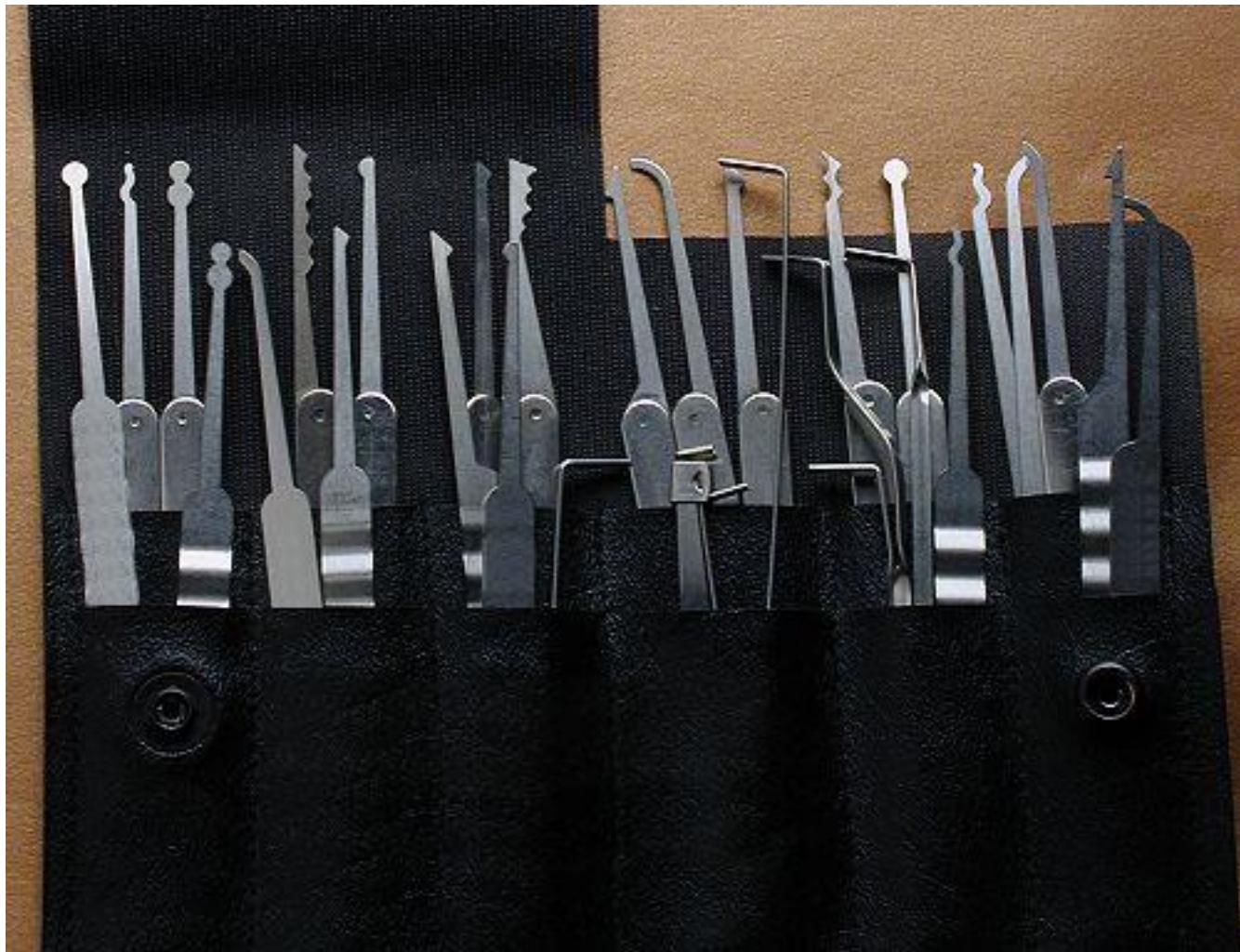
There are many lockpick vendors...

The image displays a grid of ten browser windows, each showing a different website for lockpicking supplies. The websites include:

- HPC, Inc. - Home - Mozilla Firefox
- Lock Picks, Locksmith Supply, Key Machines - Mozilla Firefox
- Lockpicktools.com - lock picks, tension tools & auto lockpick tools... - Mozilla Firefox
- SouthOrd STAINLESS STEEL LOCK PICKS - Mozilla Firefox
- Peterson Manufacturing | Pick Sets - Mozilla Firefox
- Ryan Inc. - LOCK PICKS - Mozilla Firefox
- SOUTHORD Professional Lock Picks
- Peterson Locksmith Tools
- Lock Picking Combo Kits - Save 15 - 35% - Mozilla Firefox
- DealExtreme: Lock Picks & Tools (Page 2) - Mozilla Firefox
- SEREPICK.COM
- LockPickShop.com
- DimeLock.com

Each window shows a different aspect of lockpicking equipment, such as individual picks, sets, tools, and tension wrenches, along with descriptions and pricing information.

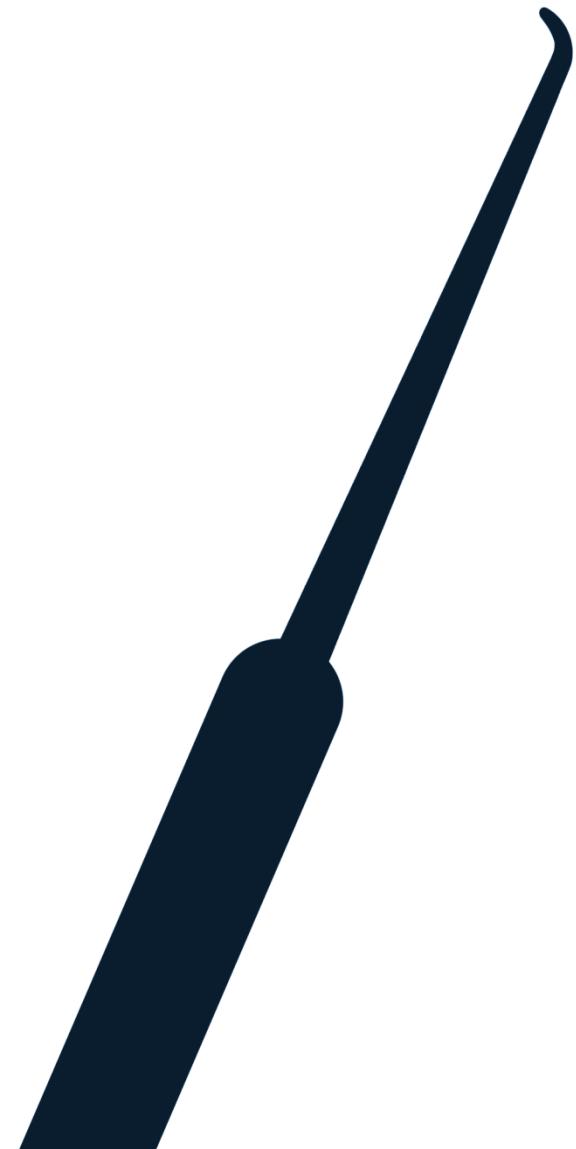
See this? Don't buy this.



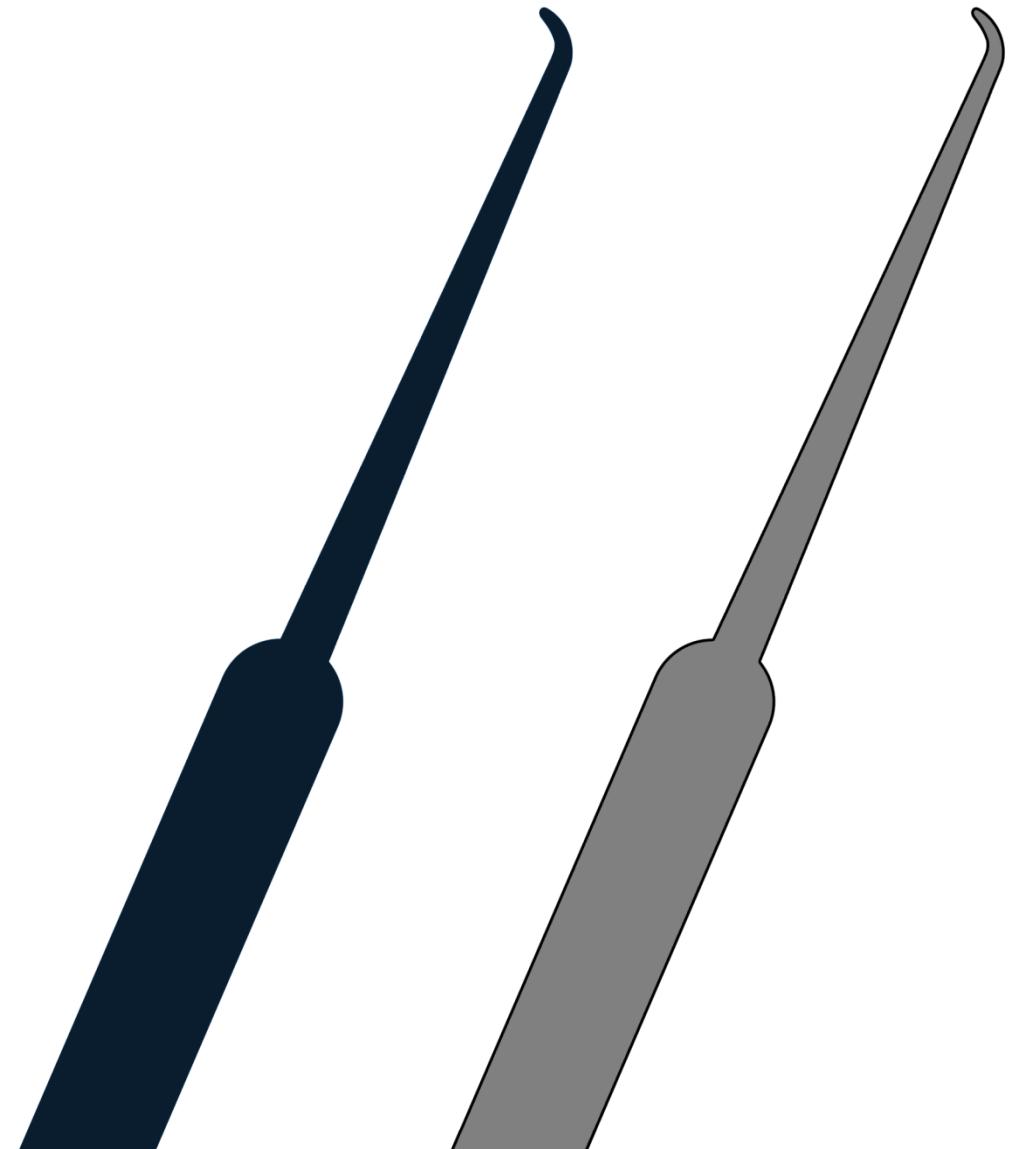
First, let's talk about metal...



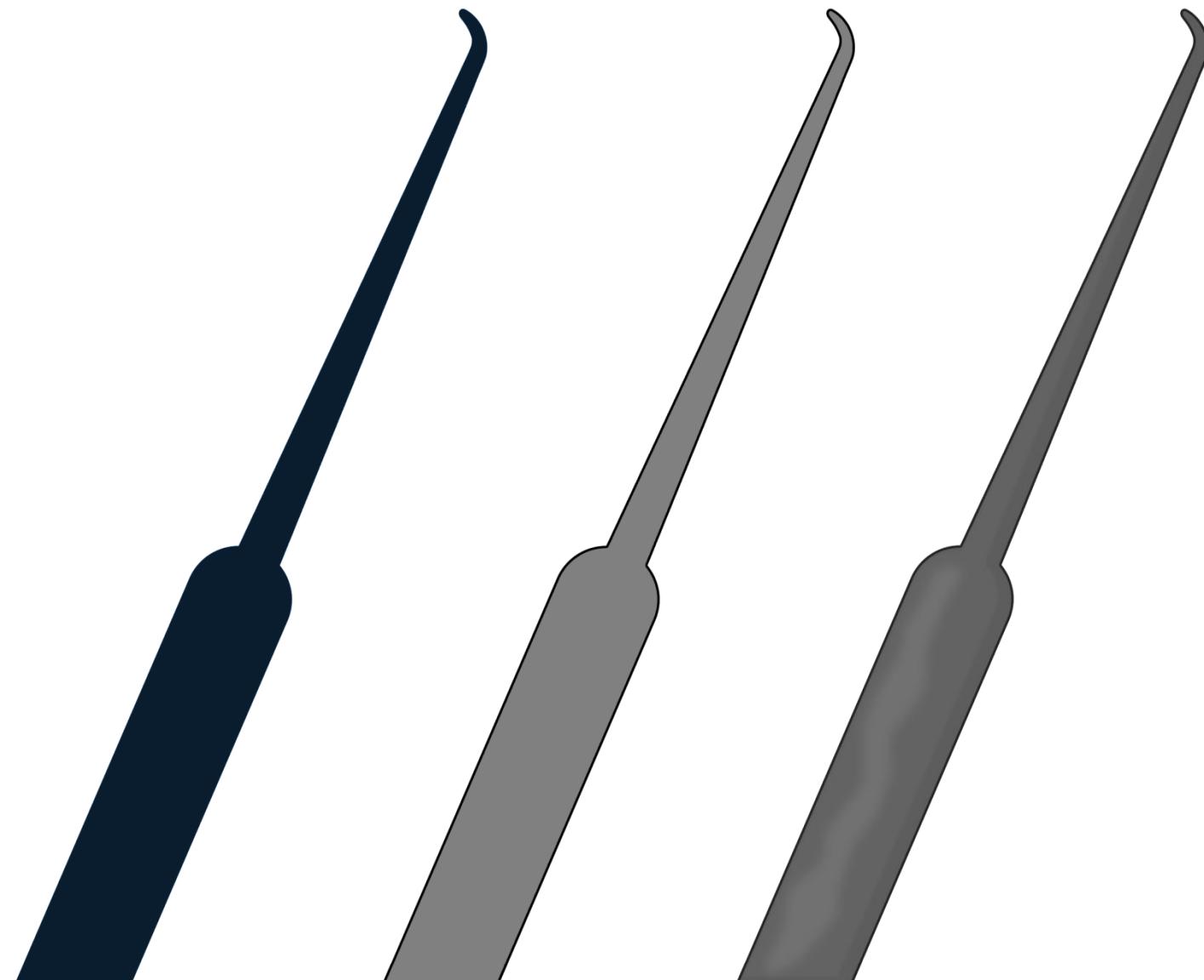
Spring Steel



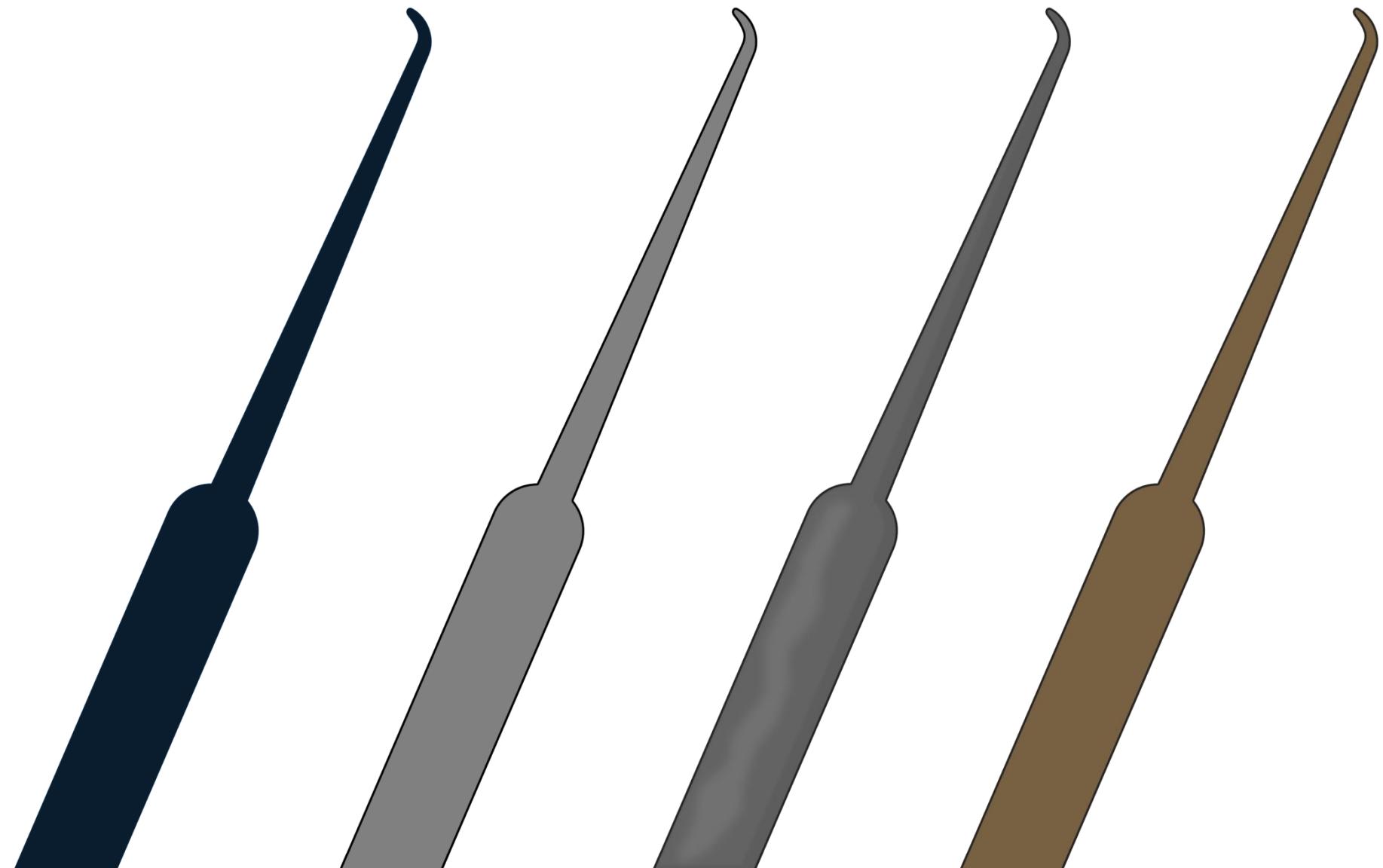
Stainless Steel



Titanium



Other Metals?



Thickness



0.015" – Peterson "Government Steel"

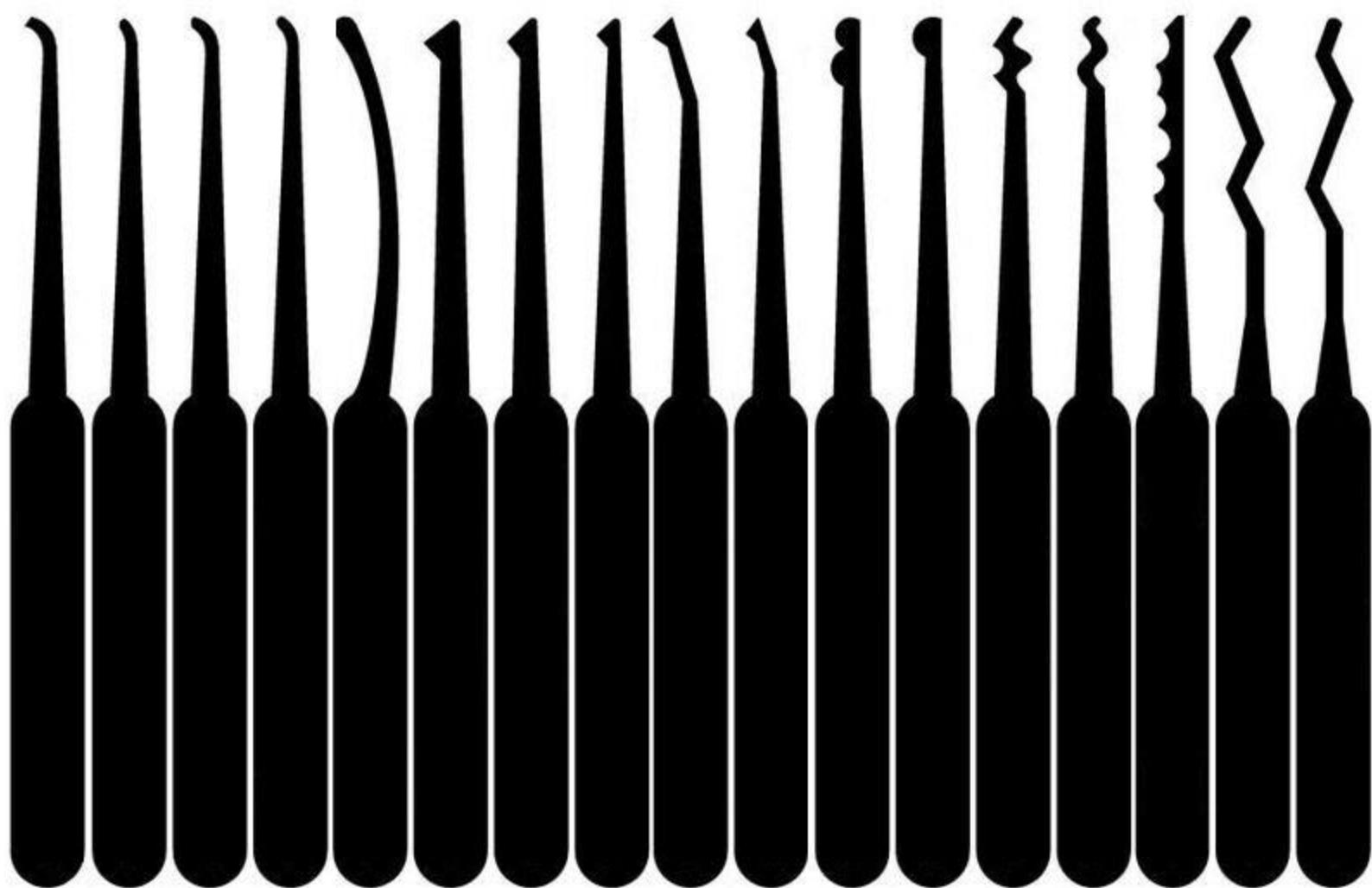
0.020" – SouthOrd, Rytan, Southern Specialties, TOOOL

0.022" – HPC Stainless

0.025" – original TOOOL kits

0.028" – HPC Spring Steel

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

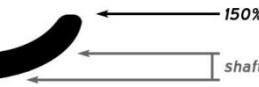


Hooks (a.k.a. Lifters)

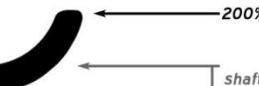
Short Hook (flat)



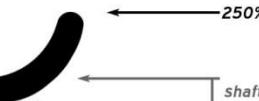
Short Hook (round)



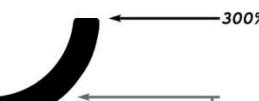
Medium Hook



Gonzo Hook

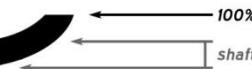


Long Hook

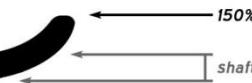


Hooks (a.k.a. Lifters)

Typical



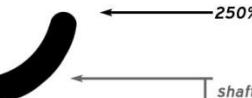
Useful



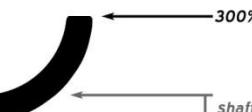
Meh



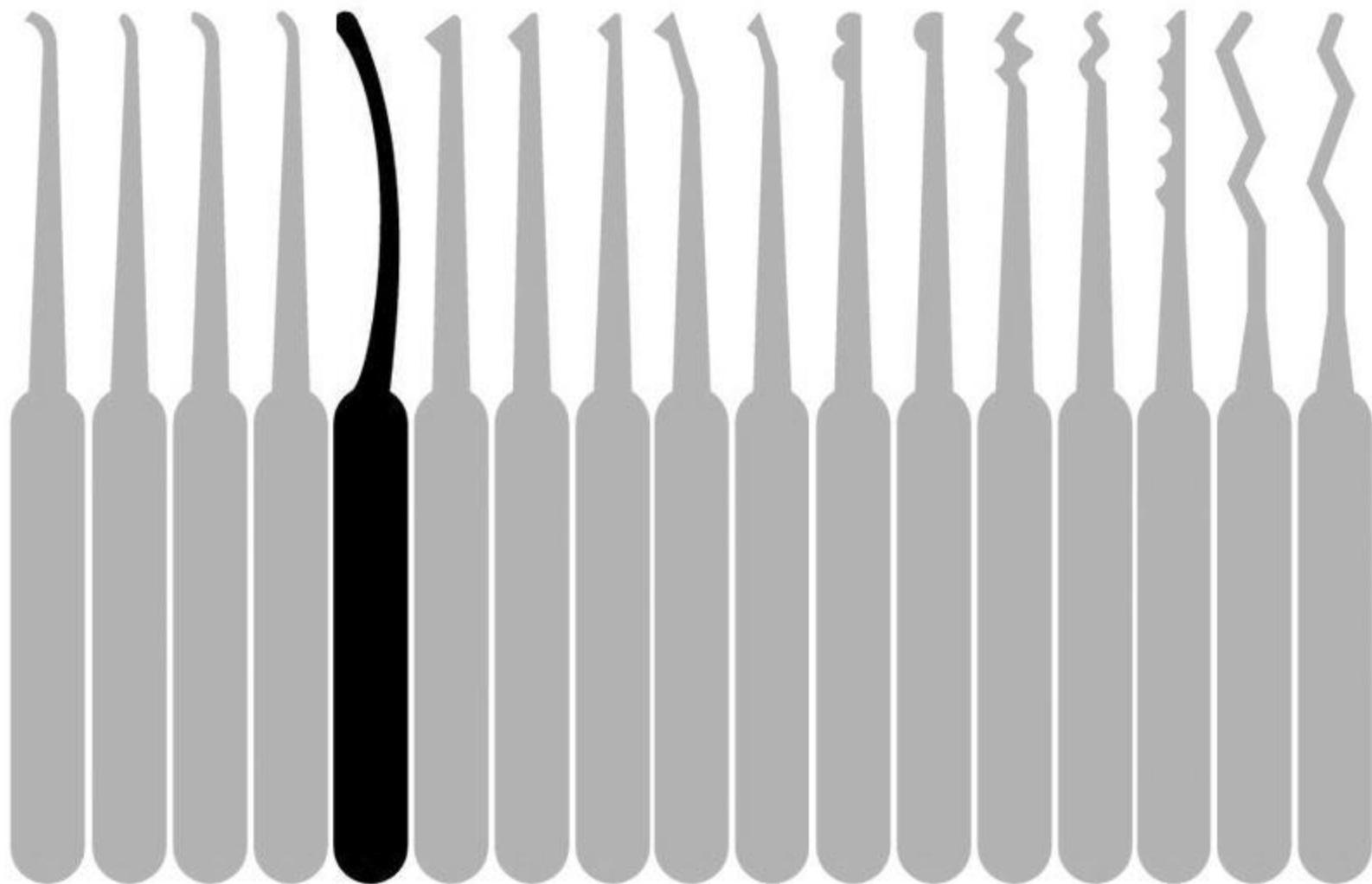
Awesome



FAIL



What would you call these ?

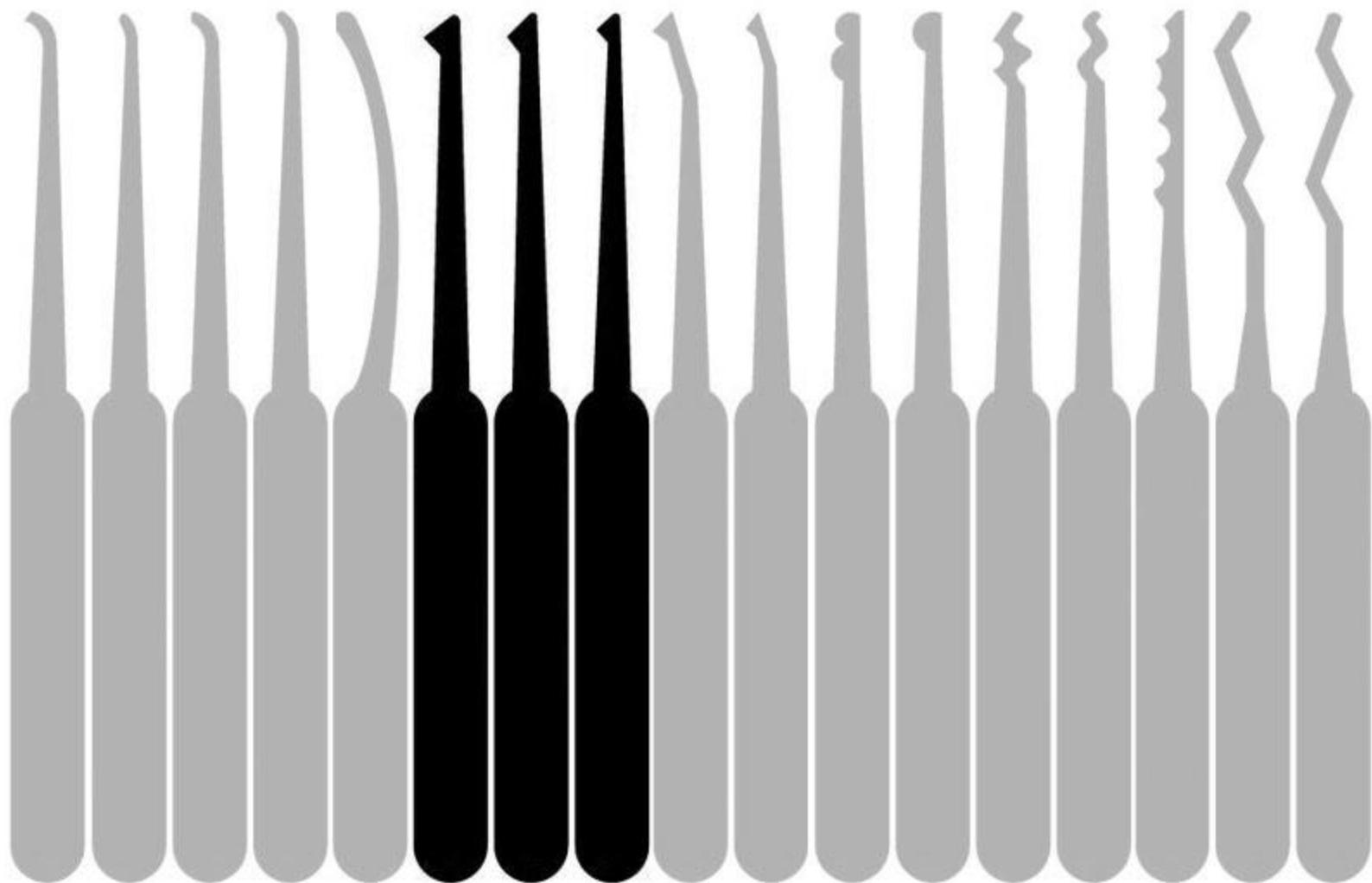


Reach Tools

Deep Curve

Hybrid

You've all seen these...



Diamonds

Small Diamond

50%
shaft

A diagram of a Small Diamond tool. It features a wide, flat triangular head at the left end and a long, thin shaft extending to the right. A horizontal double-headed arrow spans the distance from the tip of the head to the end of the shaft, labeled "50%" above it. Below the arrow is the word "shaft".

Medium Diamond

100%
shaft

A diagram of a Medium Diamond tool. It has a triangular head and a shaft. A horizontal double-headed arrow spans the distance from the tip of the head to the end of the shaft, labeled "100%" above it. Below the arrow is the word "shaft".

Large Diamond

150%
shaft

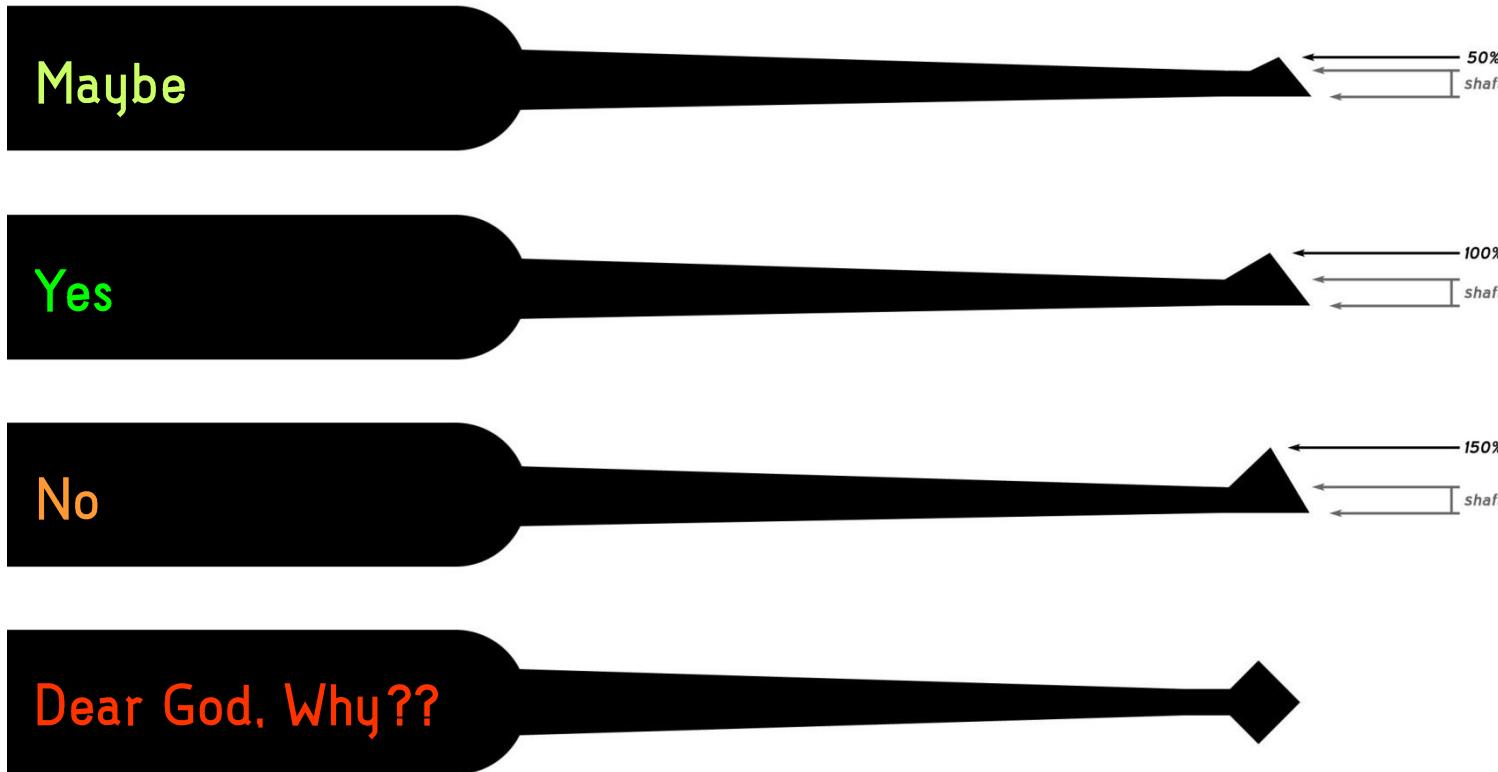
A diagram of a Large Diamond tool. It has a triangular head and a shaft. A horizontal double-headed arrow spans the distance from the tip of the head to the end of the shaft, labeled "150%" above it. Below the arrow is the word "shaft".

Diamond Head

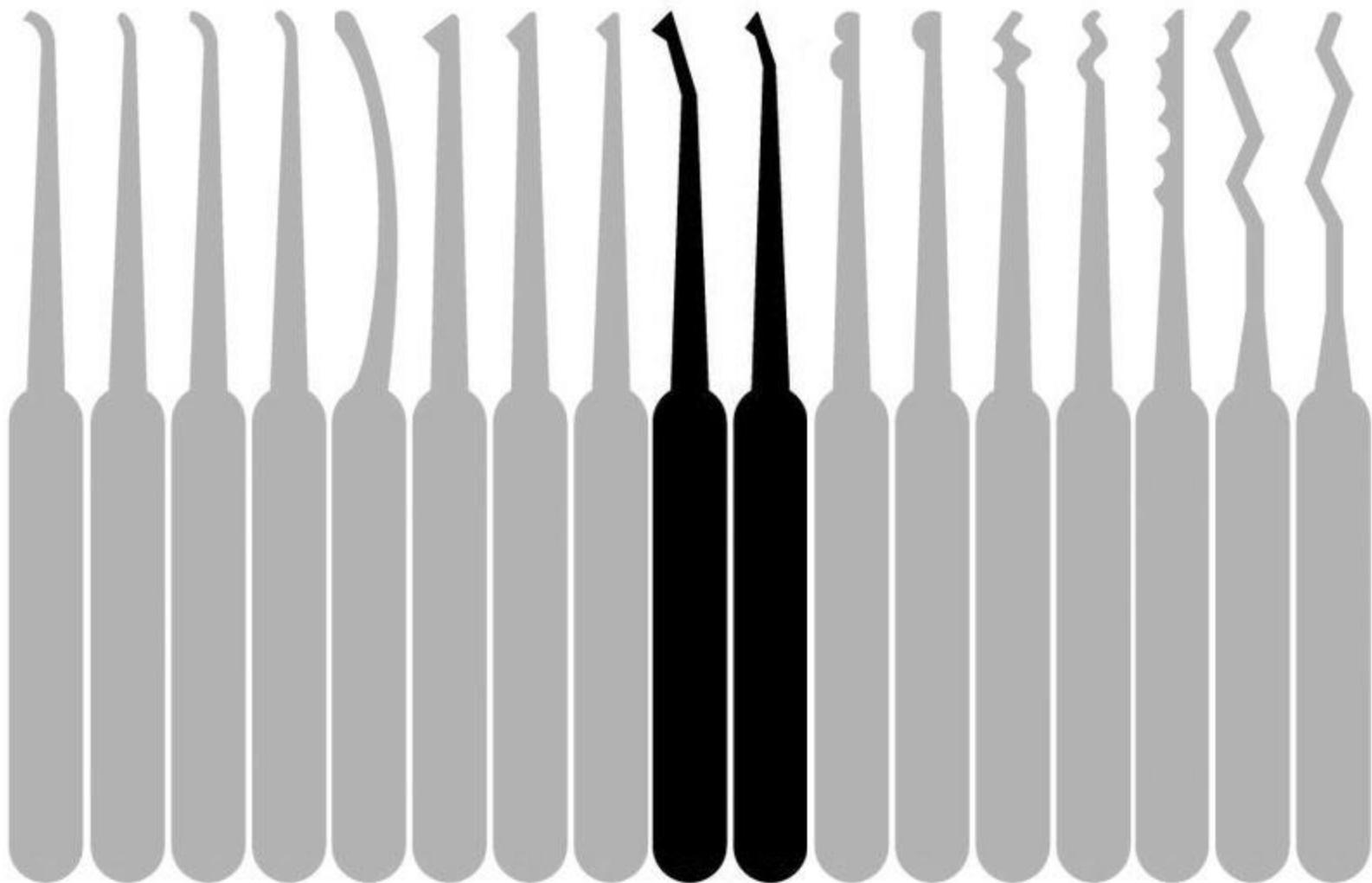
◆

A diagram of a Diamond Head tool. It has a triangular head and a shaft. The head is a solid black diamond shape pointing to the right. The shaft is a long, thin line extending from the base of the head.

Diamonds



How would you categorize *these*...?



Offset Tools

Offset Diamond

Offset Ball

Offset Snake

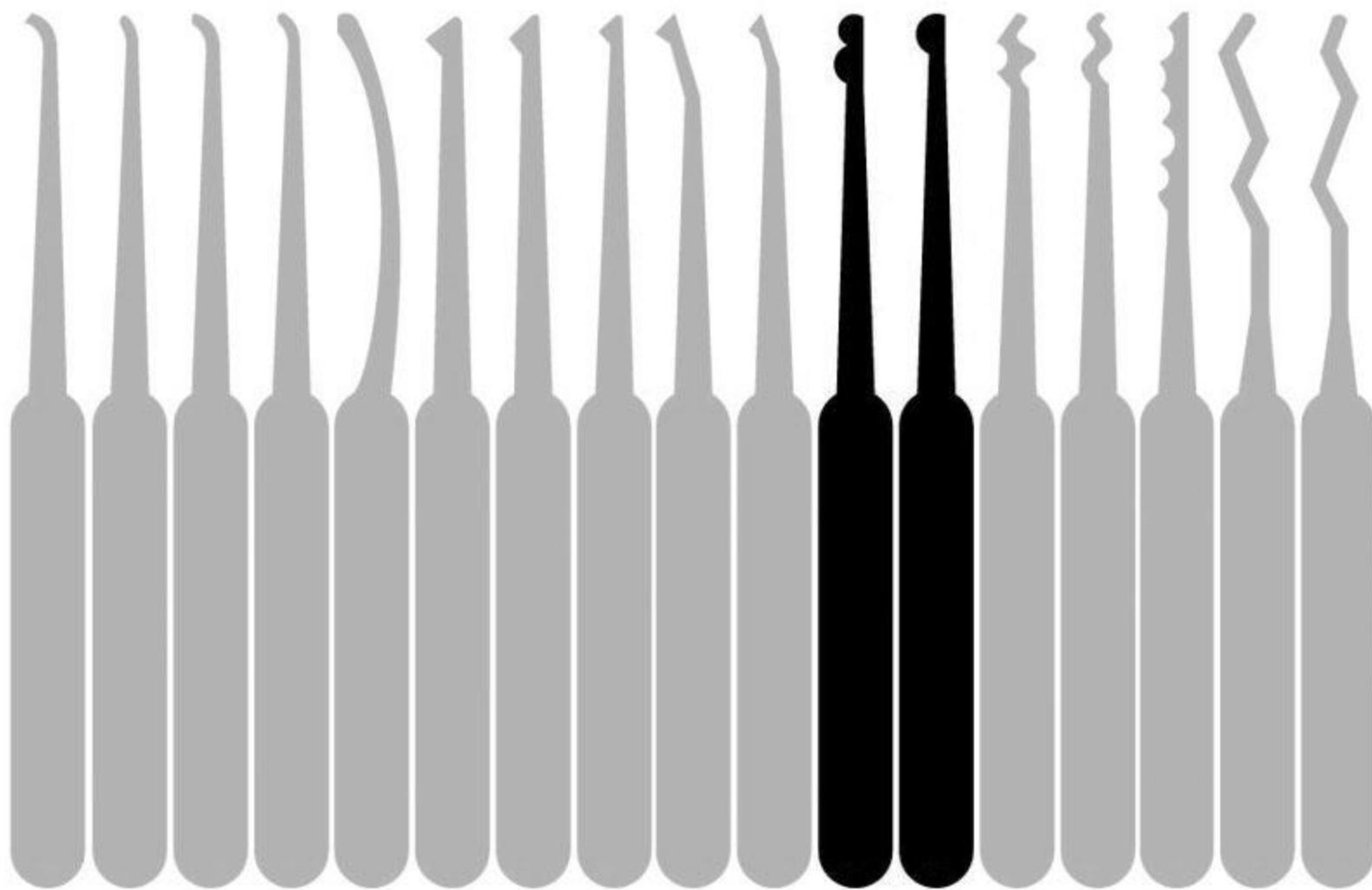
Offset Tools

Yeah, sure.

Meh, why not ?

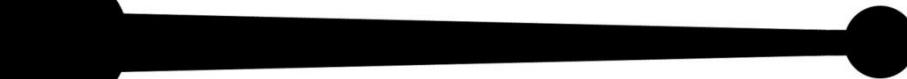
I suppose.

Balls, balls, balls...



Balls, balls, balls...

Single Ball



Snowman



Half Snowman



Half Ball



Balls, balls, balls...

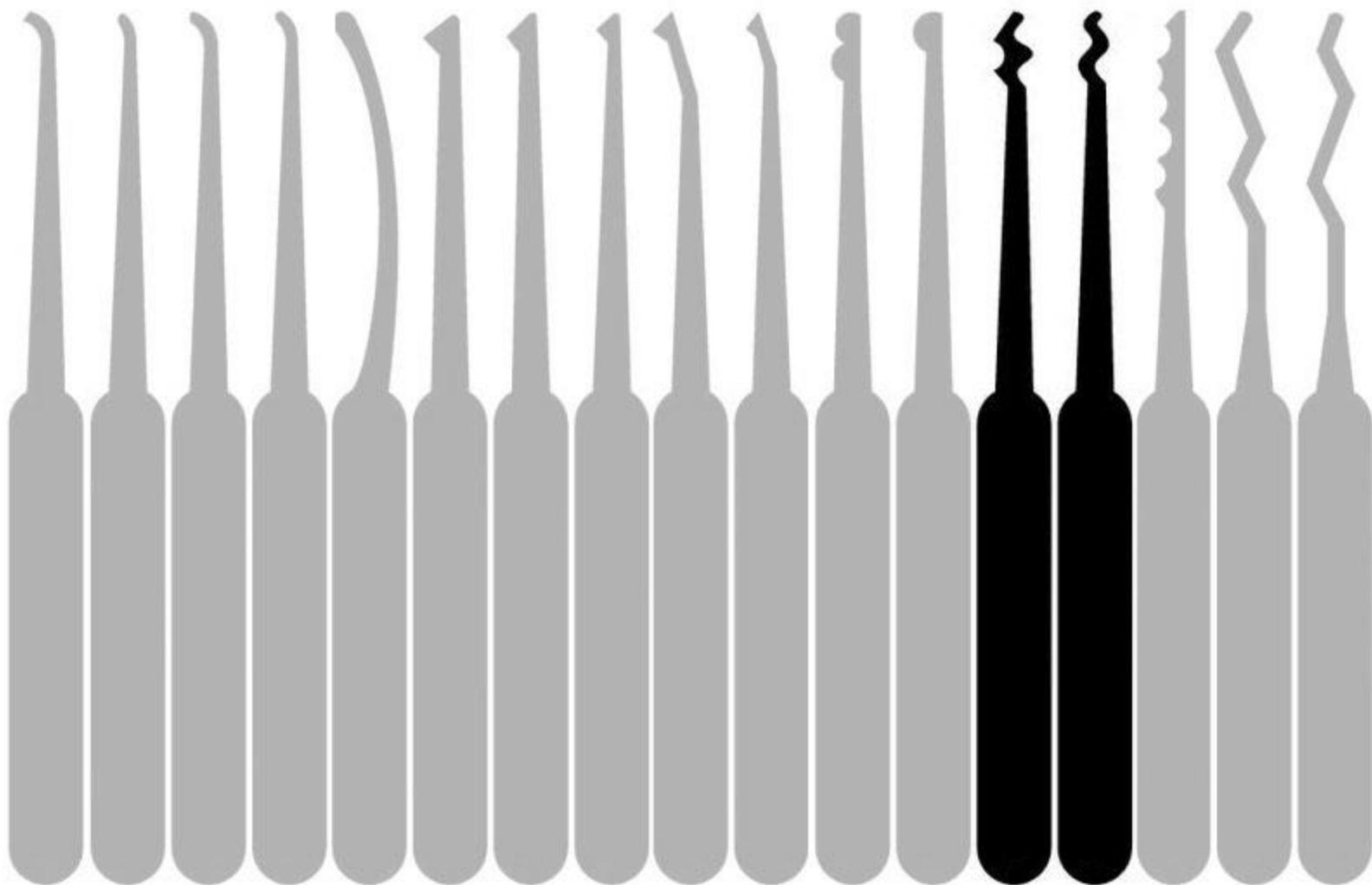
Pretty Useless

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

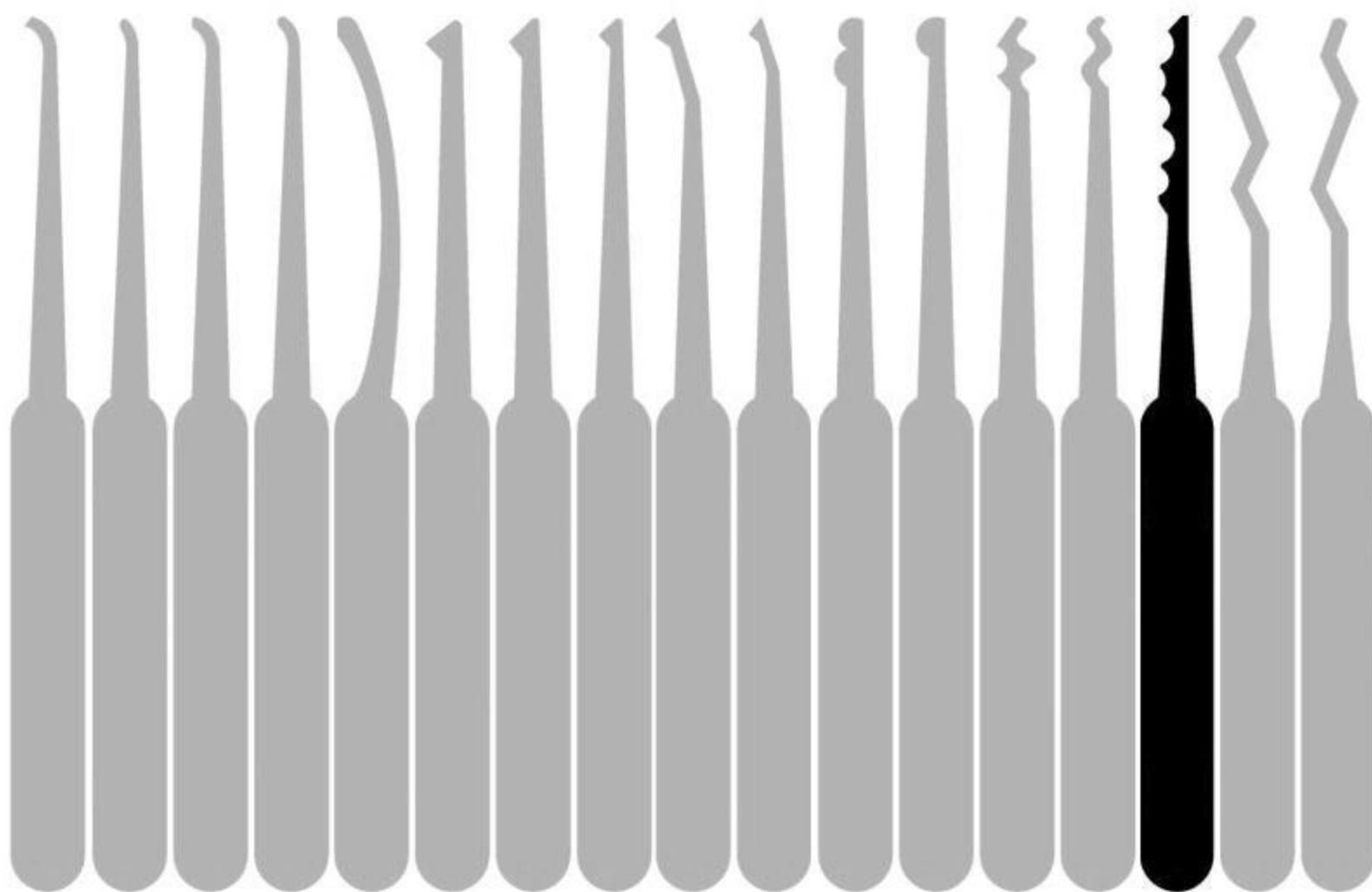
Batarang



a.k.a. S Rake, Camel Back

Dangerous Weakness

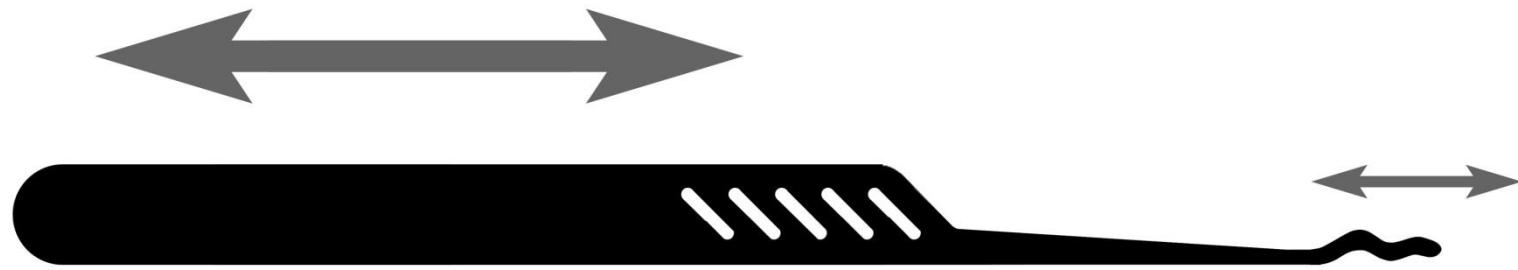
What about something like *this*...



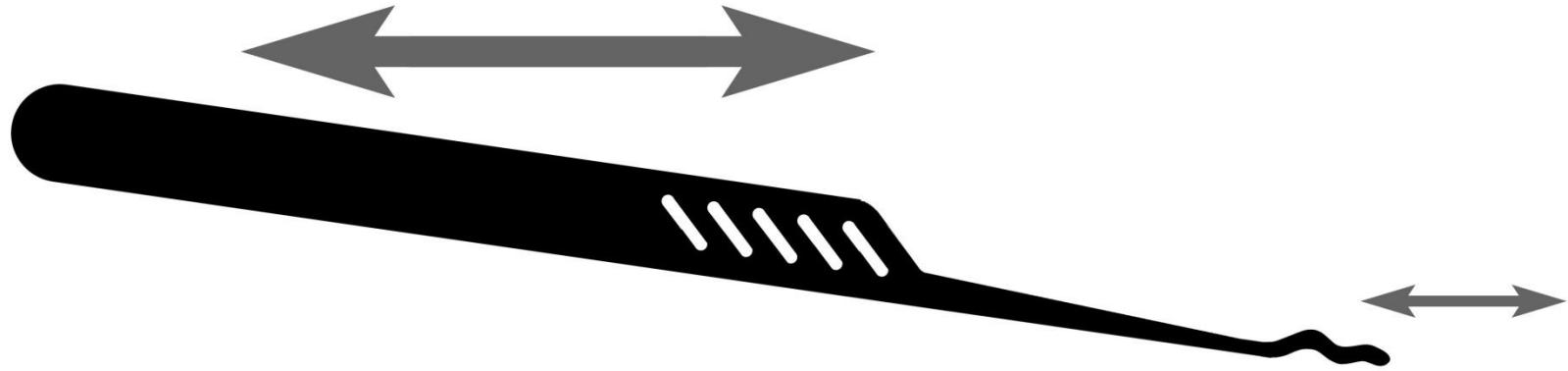
“Raking” vs. “Lifting”



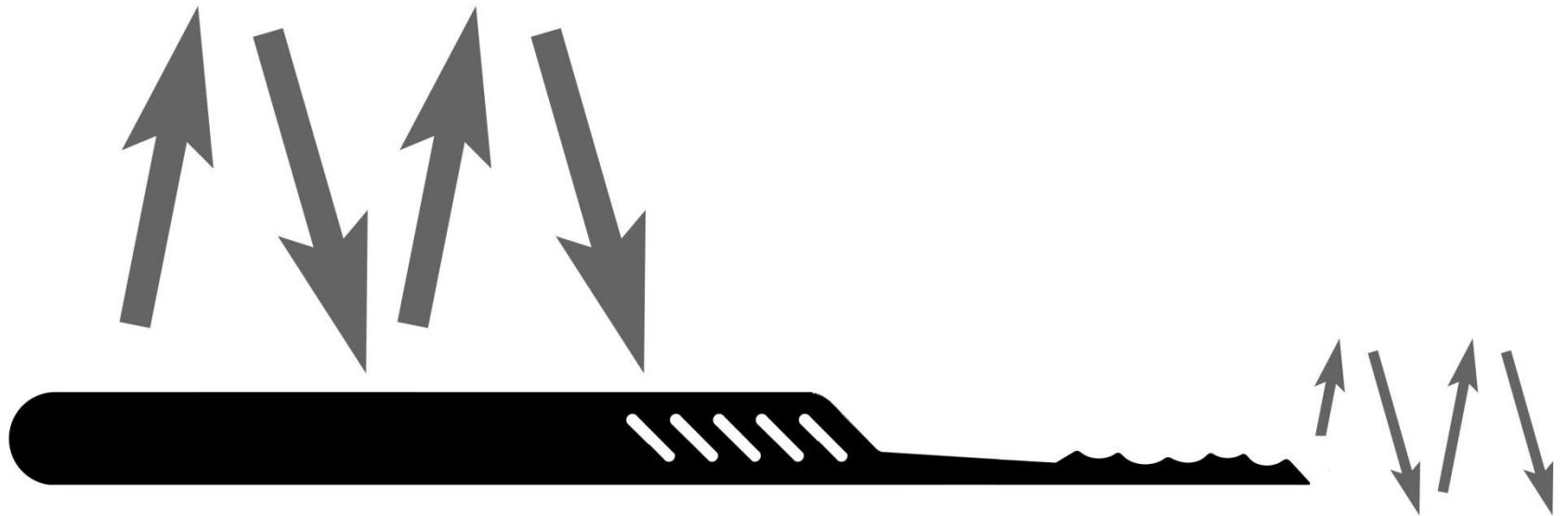
Raking



Raking



Lifting



Jagged Lifters

Wedge Rake

Long Rake

Falle Slope

Falle Valley

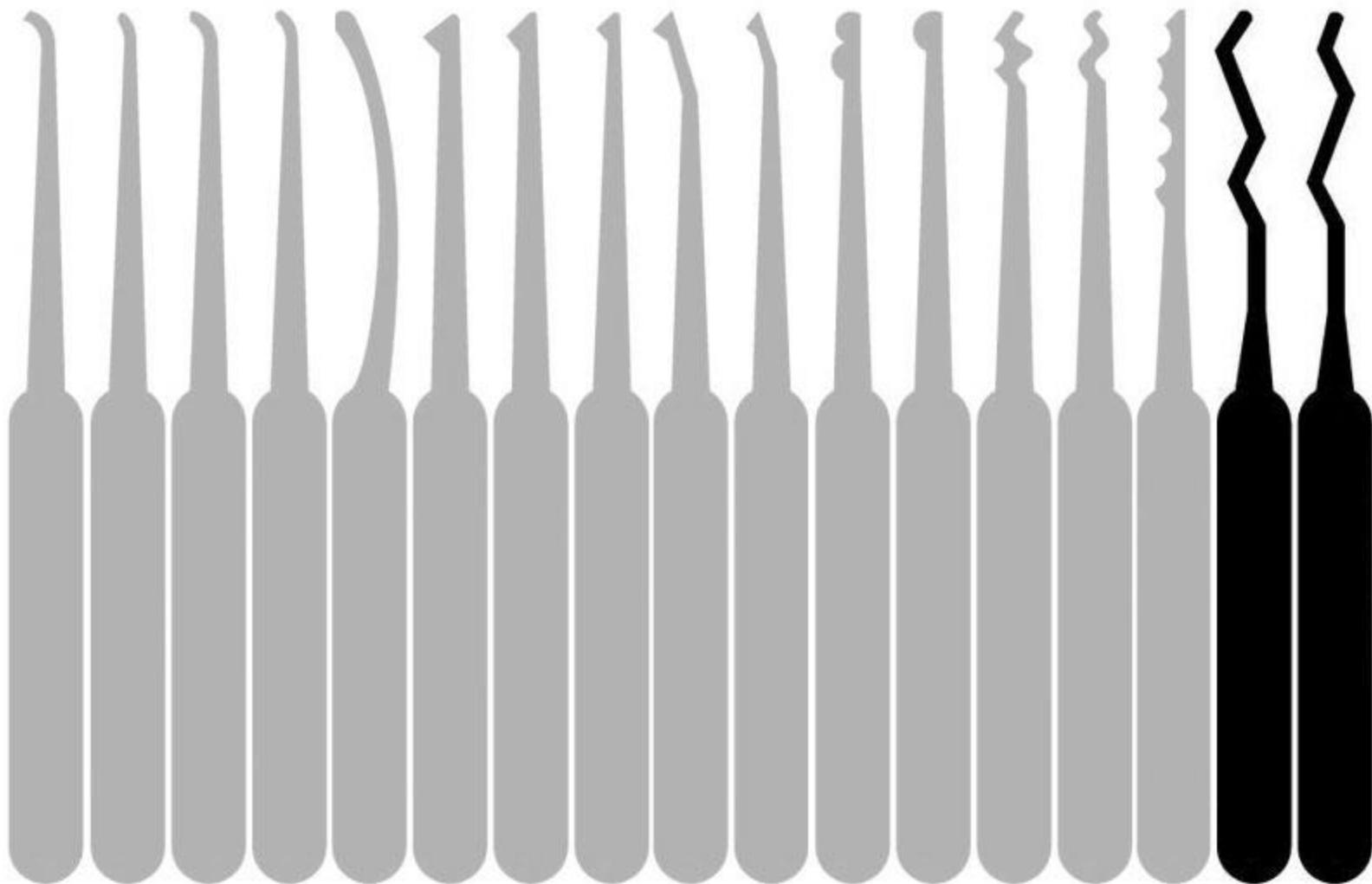
Falle Hump

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

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

a.k.a. Long Ripple

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

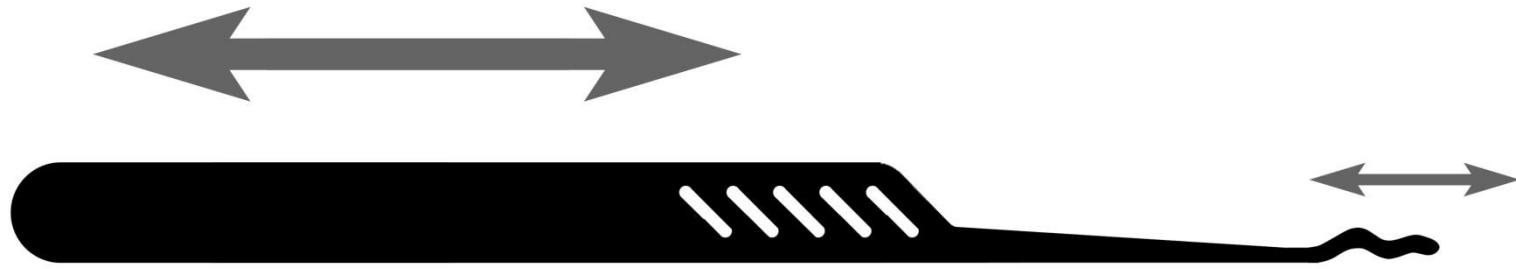


It Started with Two Tools...

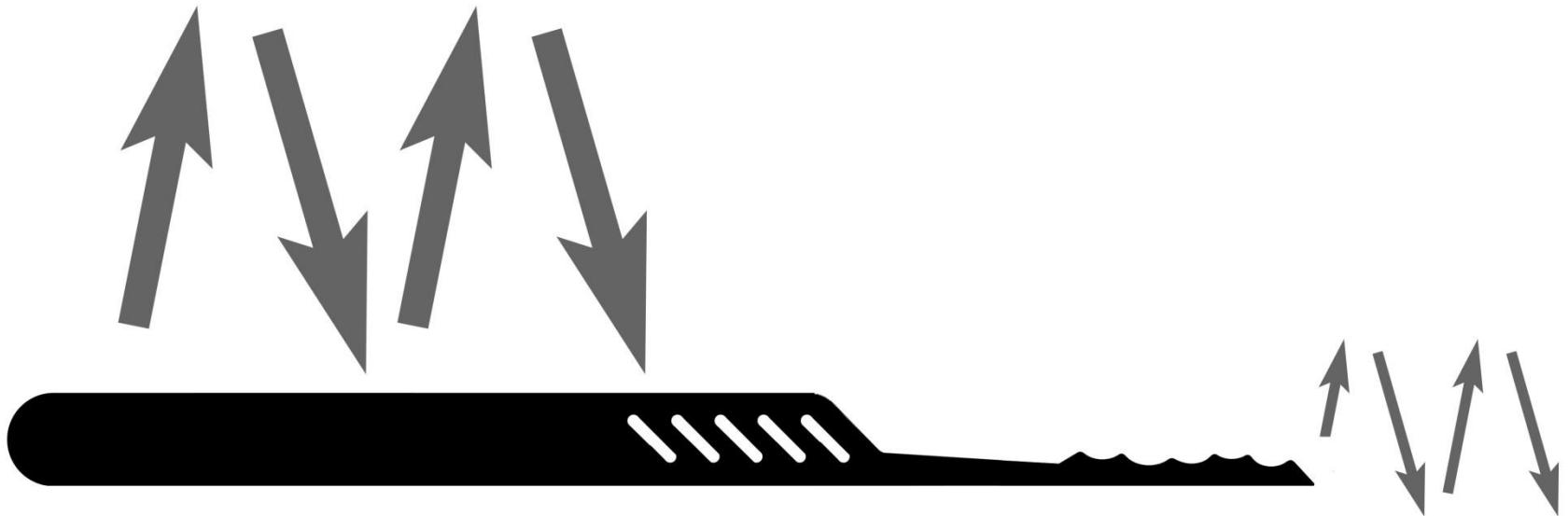


“Jiggler” Tools

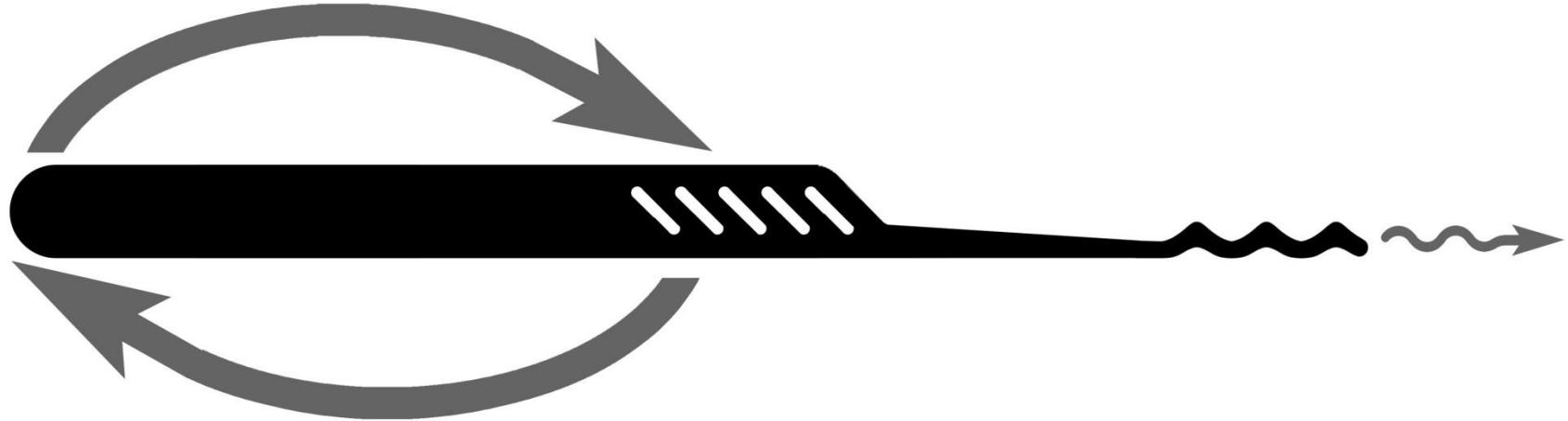
What is Jiggleing ?



In Between Raking & Lifting ...



What is Jiggleing?



... There is “Jiggleing”

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



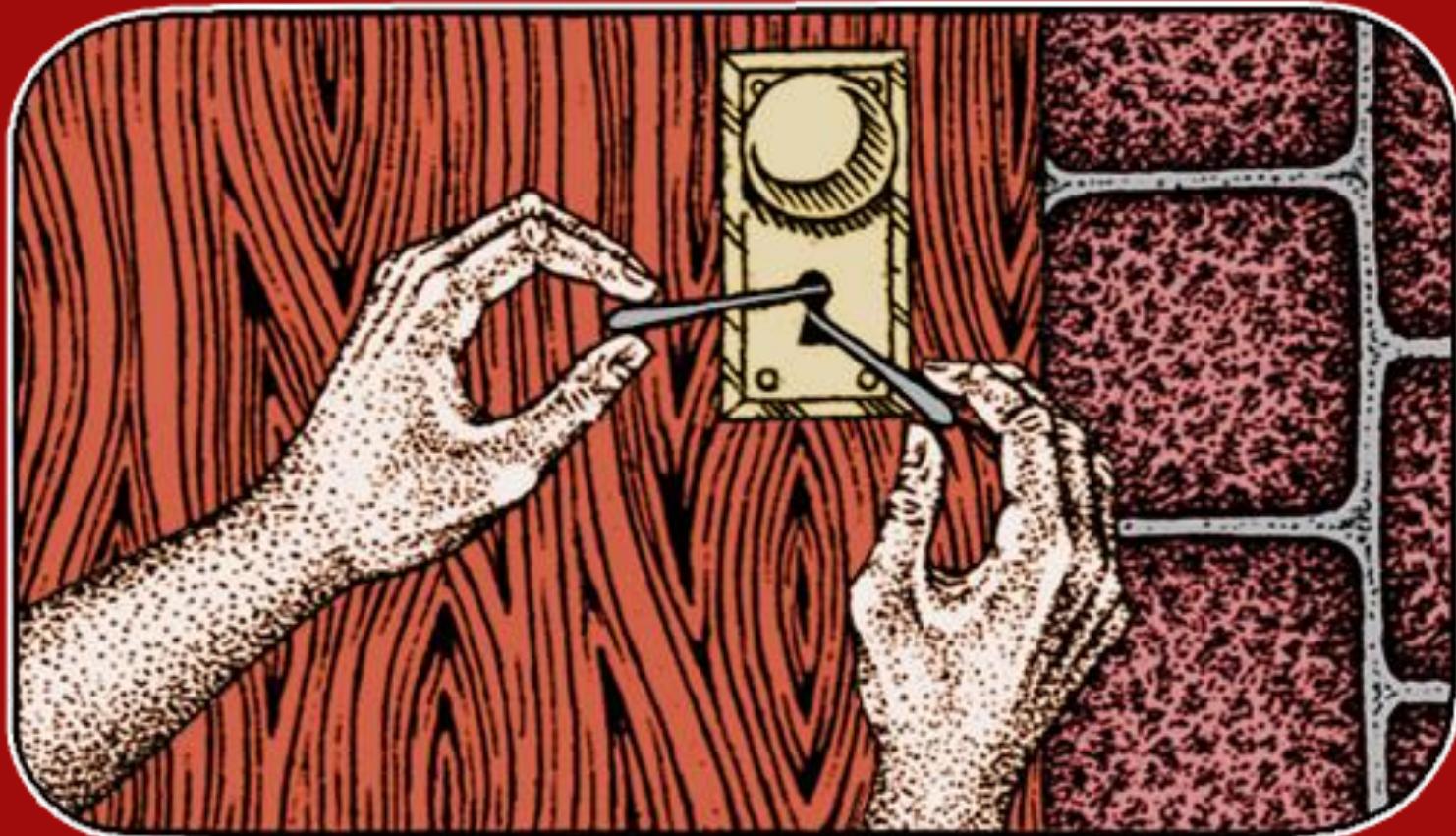
Quad Hump



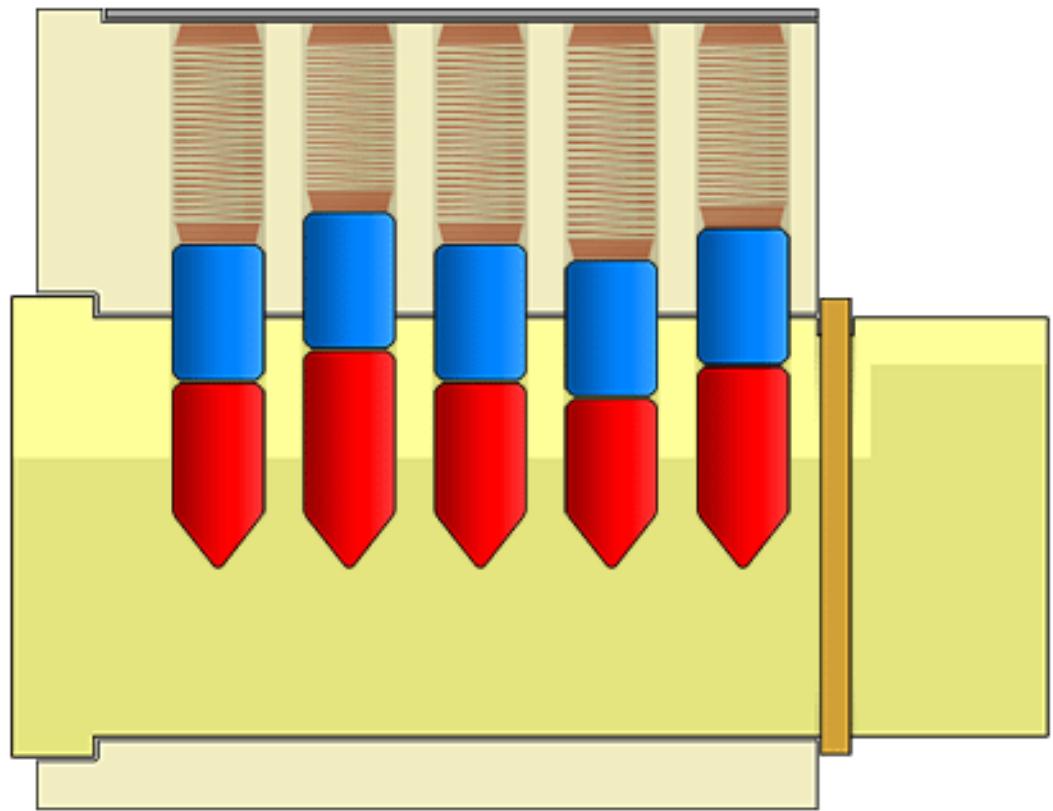
Sabana

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

Lockpicking & Forensics



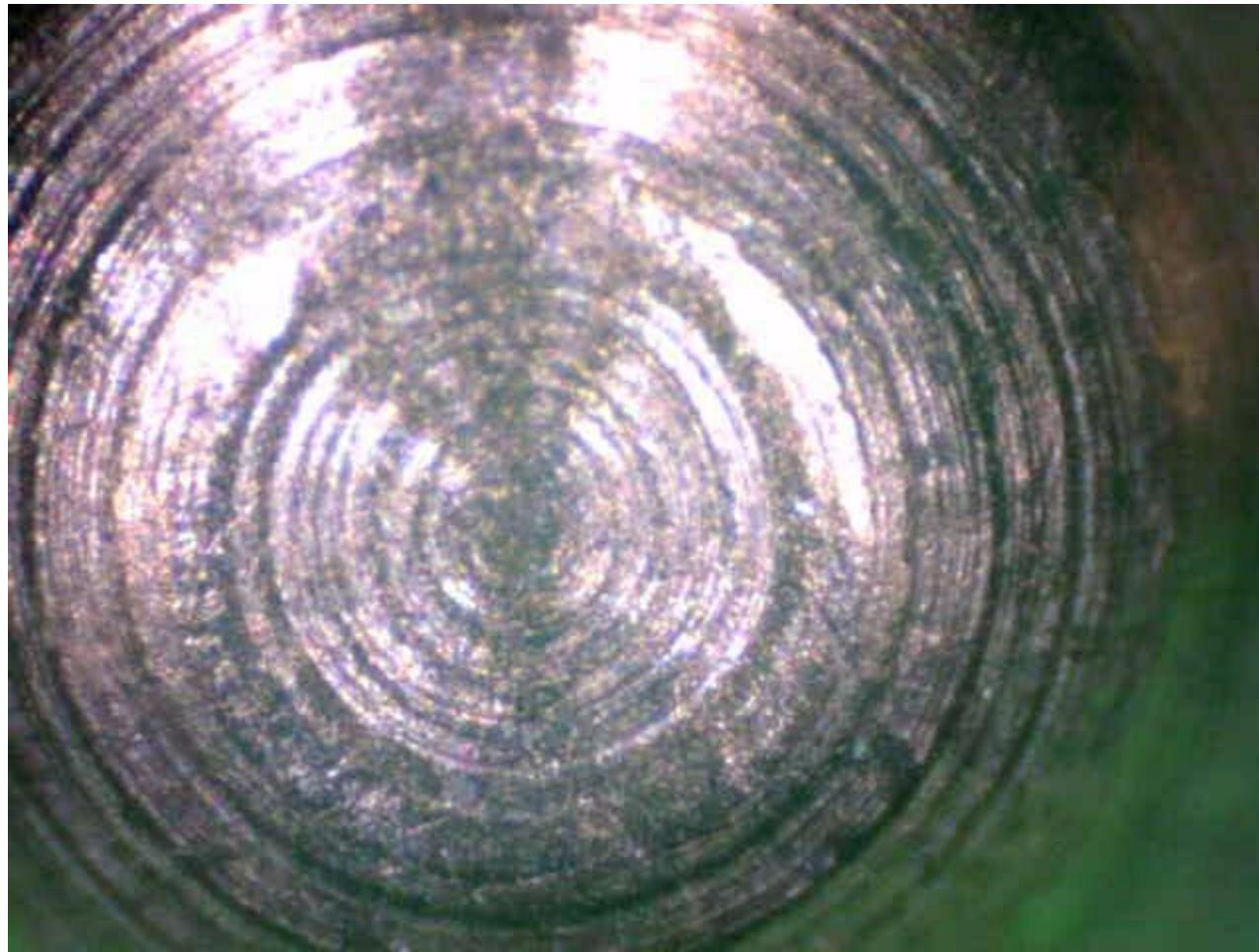
Keys Touch Very Specific Places



Virgin Pins Have Specific Patterns From Manufacturing



Concentric Tiny Ridges on Pin Face



Those Rings “Polish Away” With Use

250 Uses



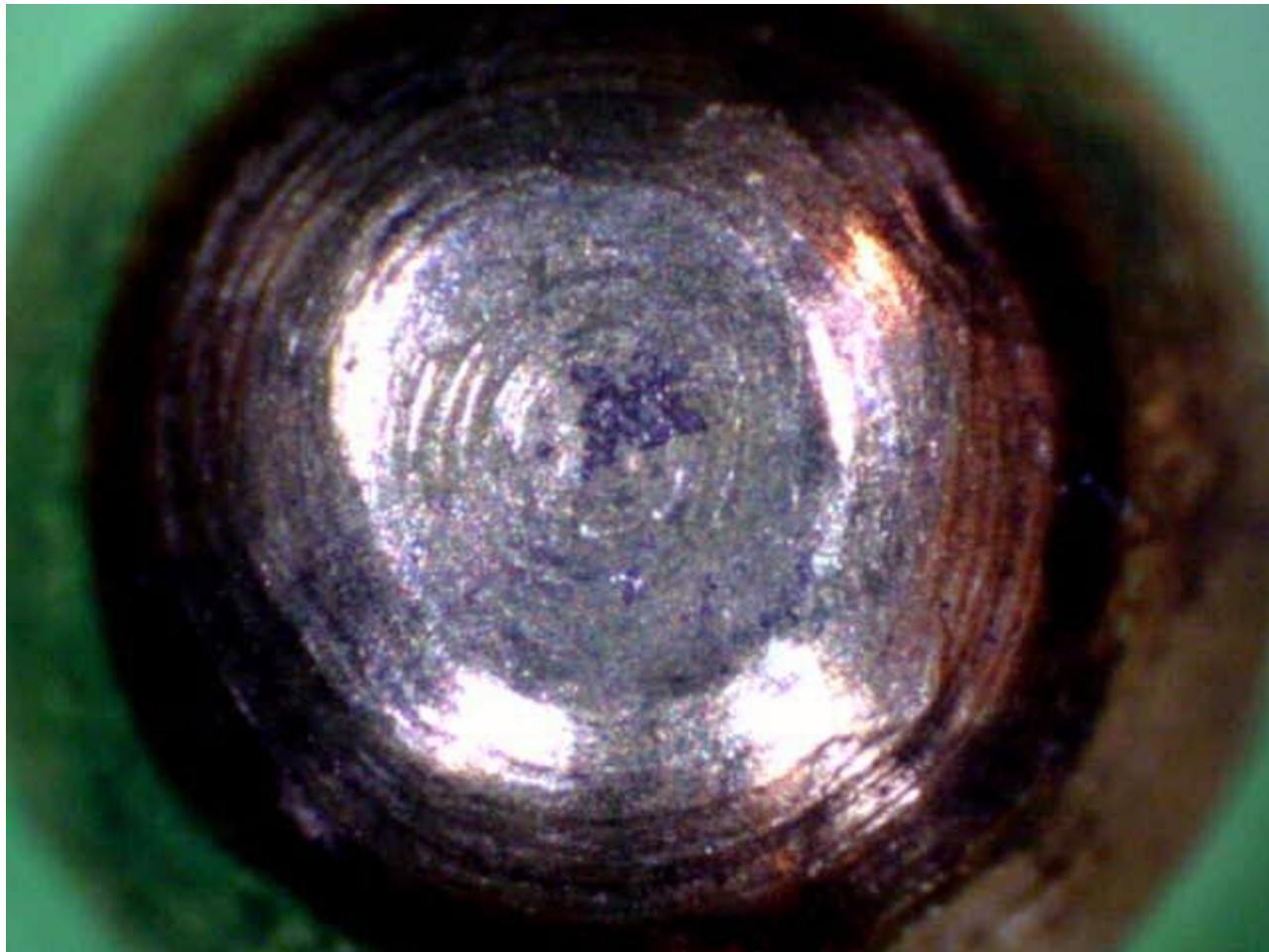
Those Rings “Polish Away” With Use

1500 Uses



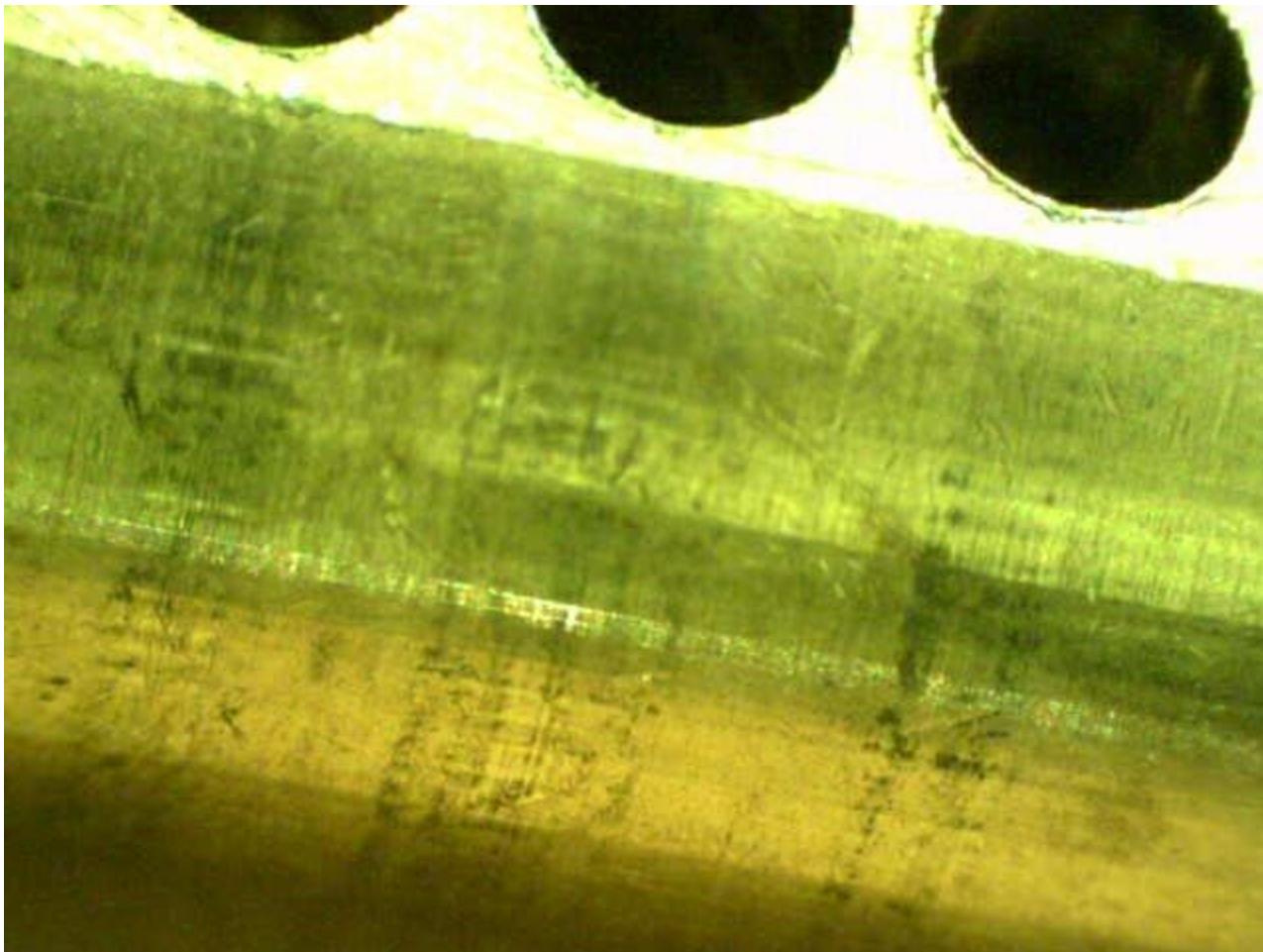
Those Rings “Polish Away” With Use

5000 Uses



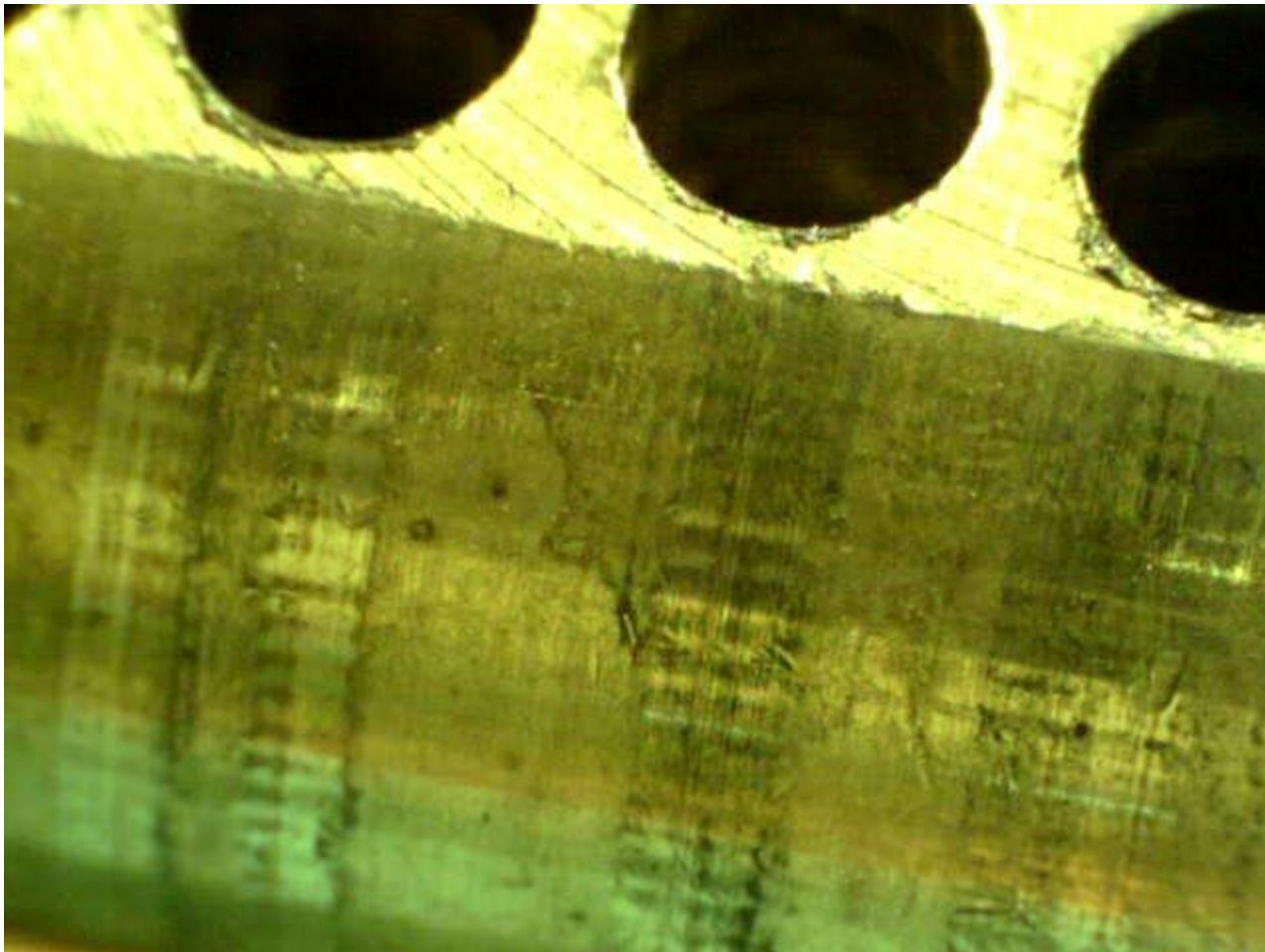
The Plug Picks Up Marks From Driver Pins

250 Uses



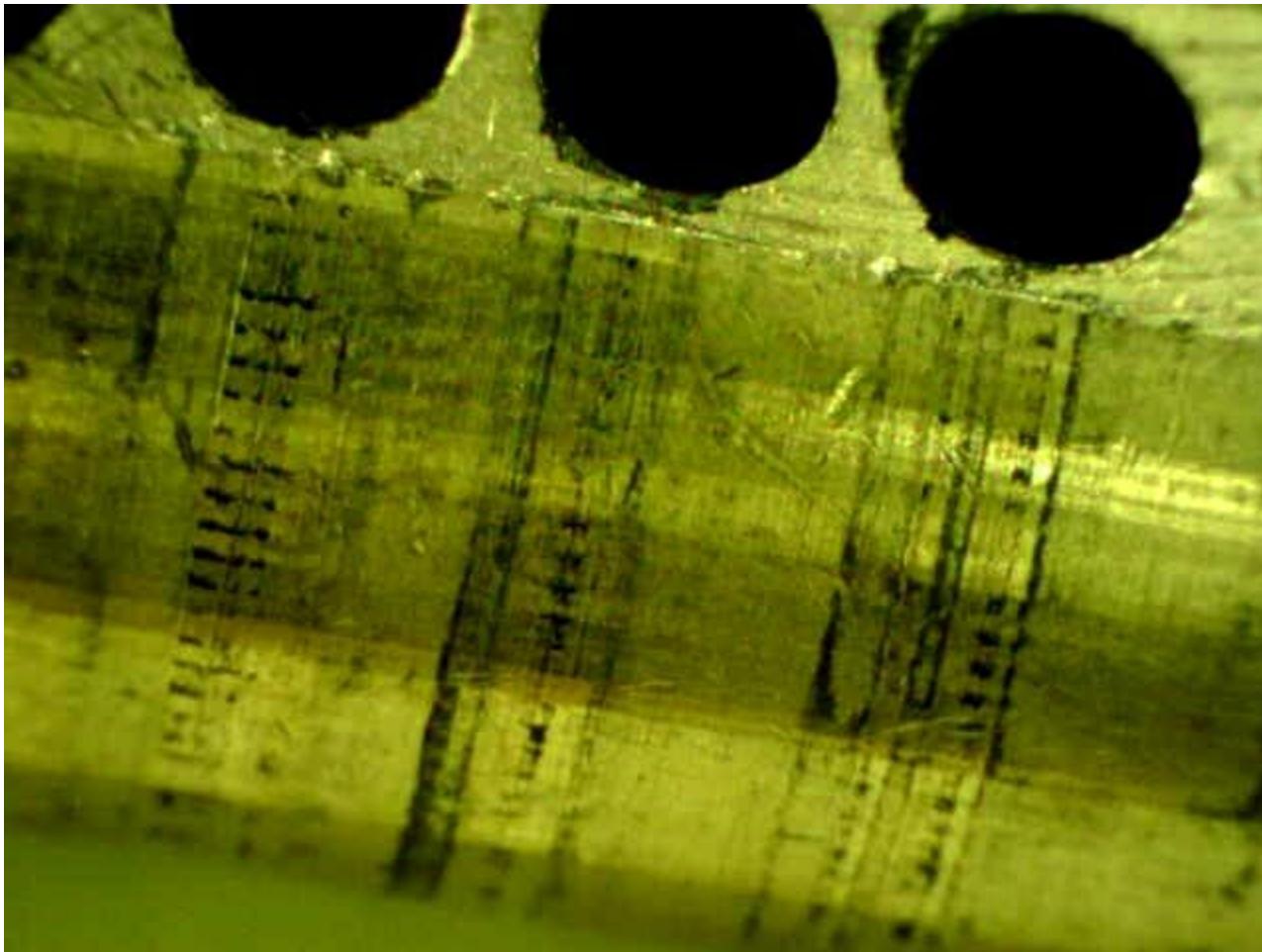
The Plug Picks Up Marks From Driver Pins

1500 Uses

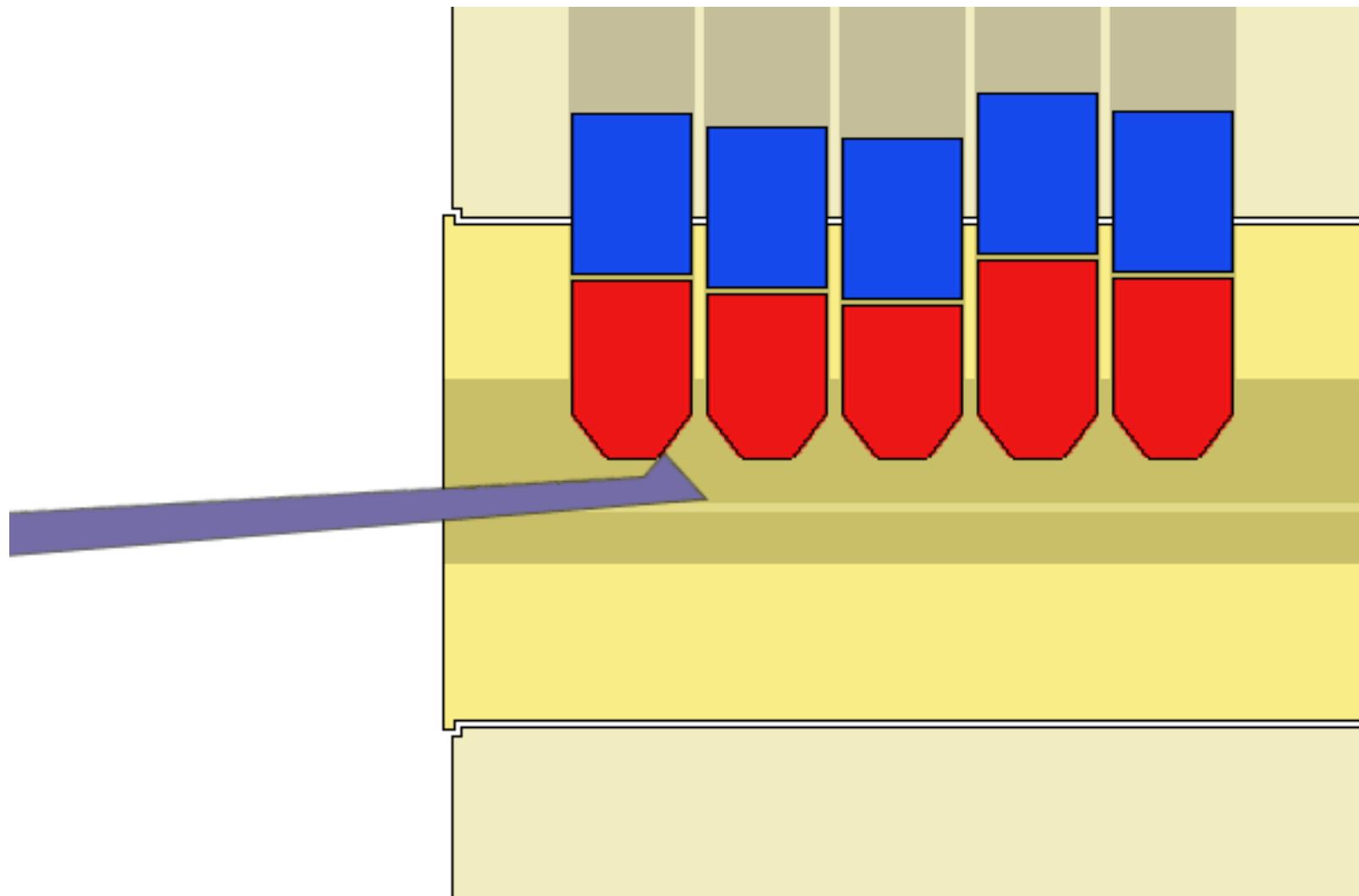


The Plug Picks Up Marks From Driver Pins

5000 Uses



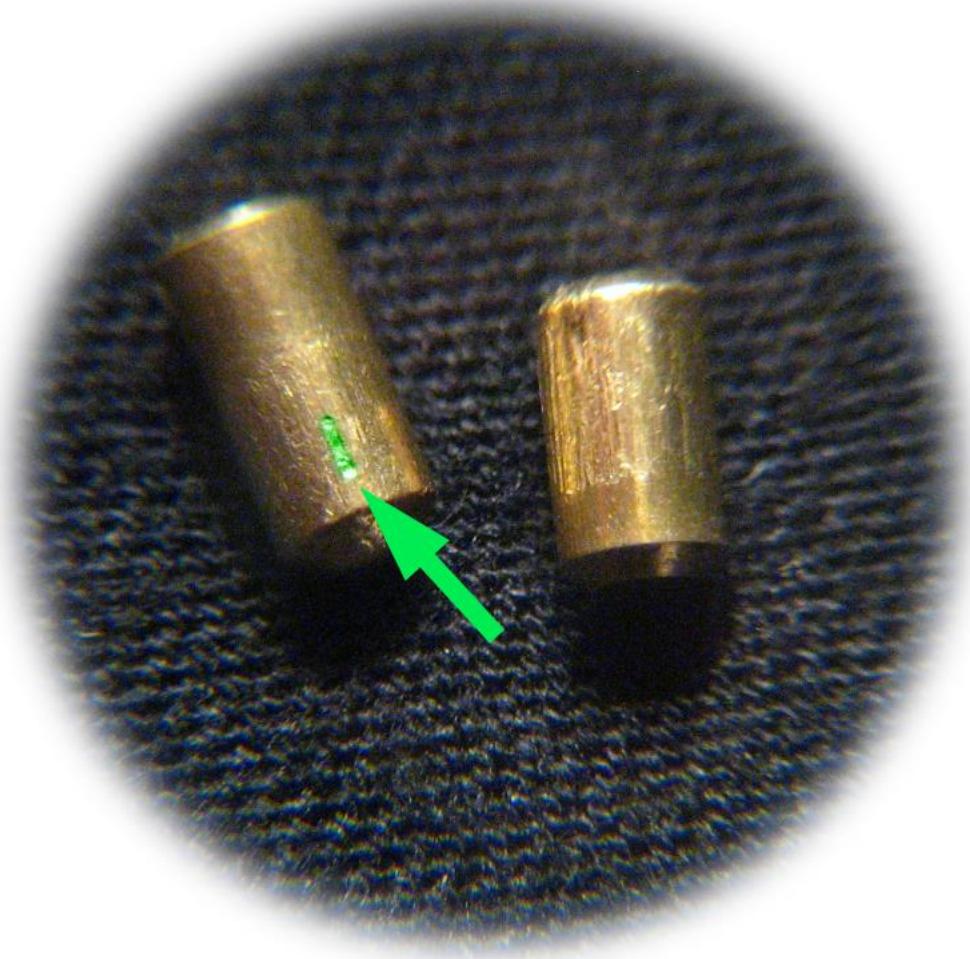
Picks Touch Places That Keys Don't



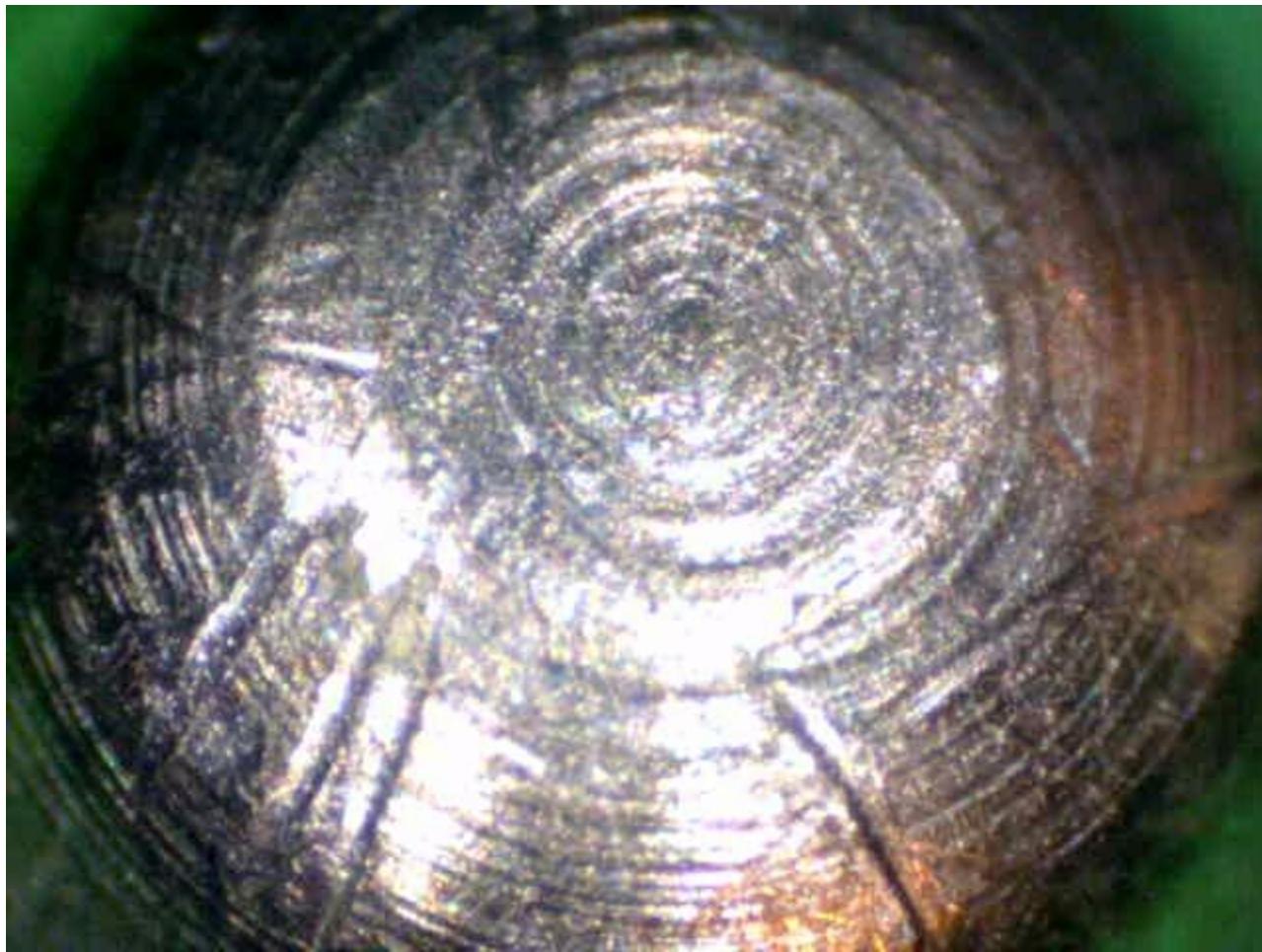
Wear and Tear or Toolmarks ?



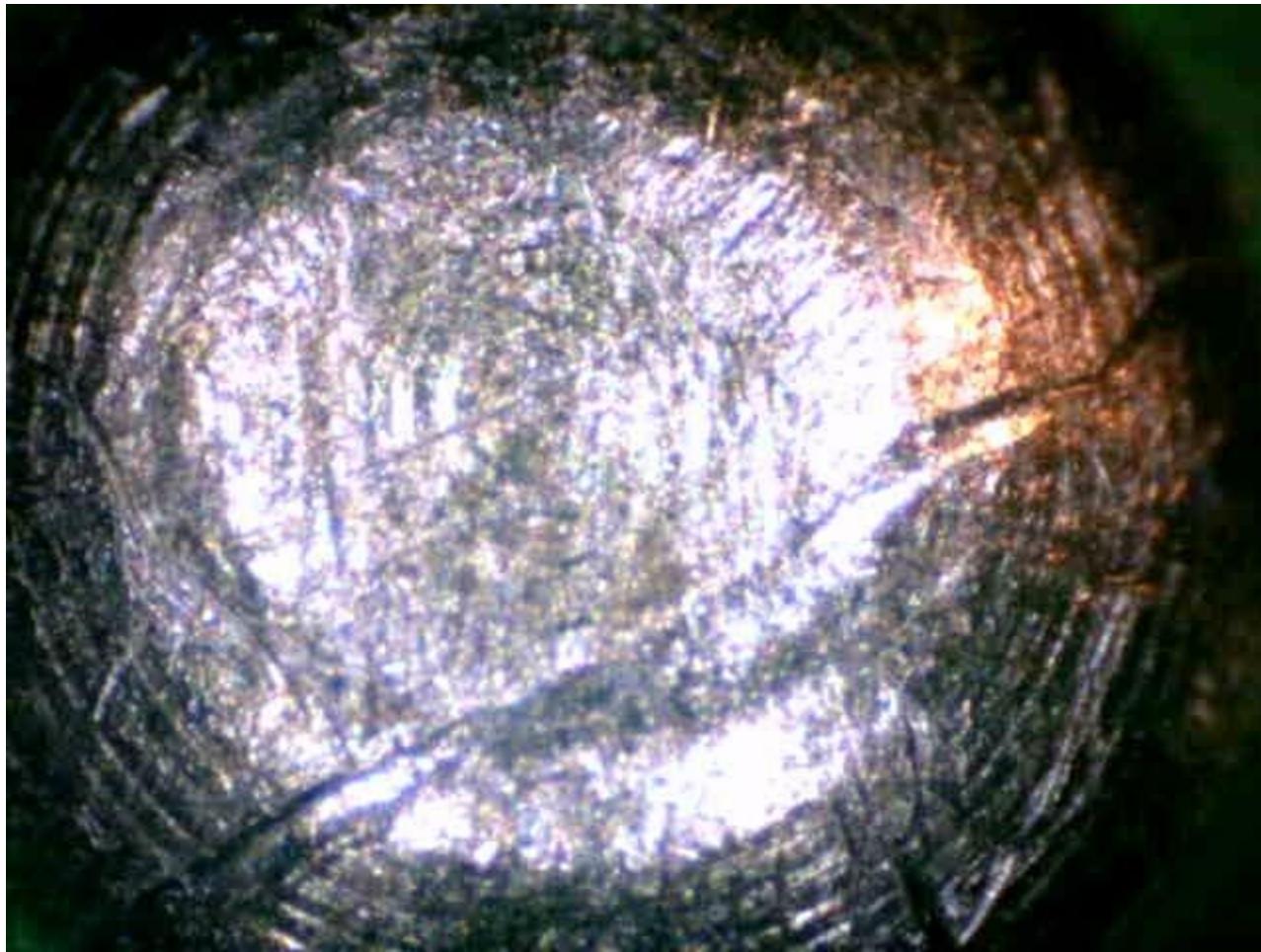
Wear and Tear or Toolmarks ?



Forensics – Lifting Picking



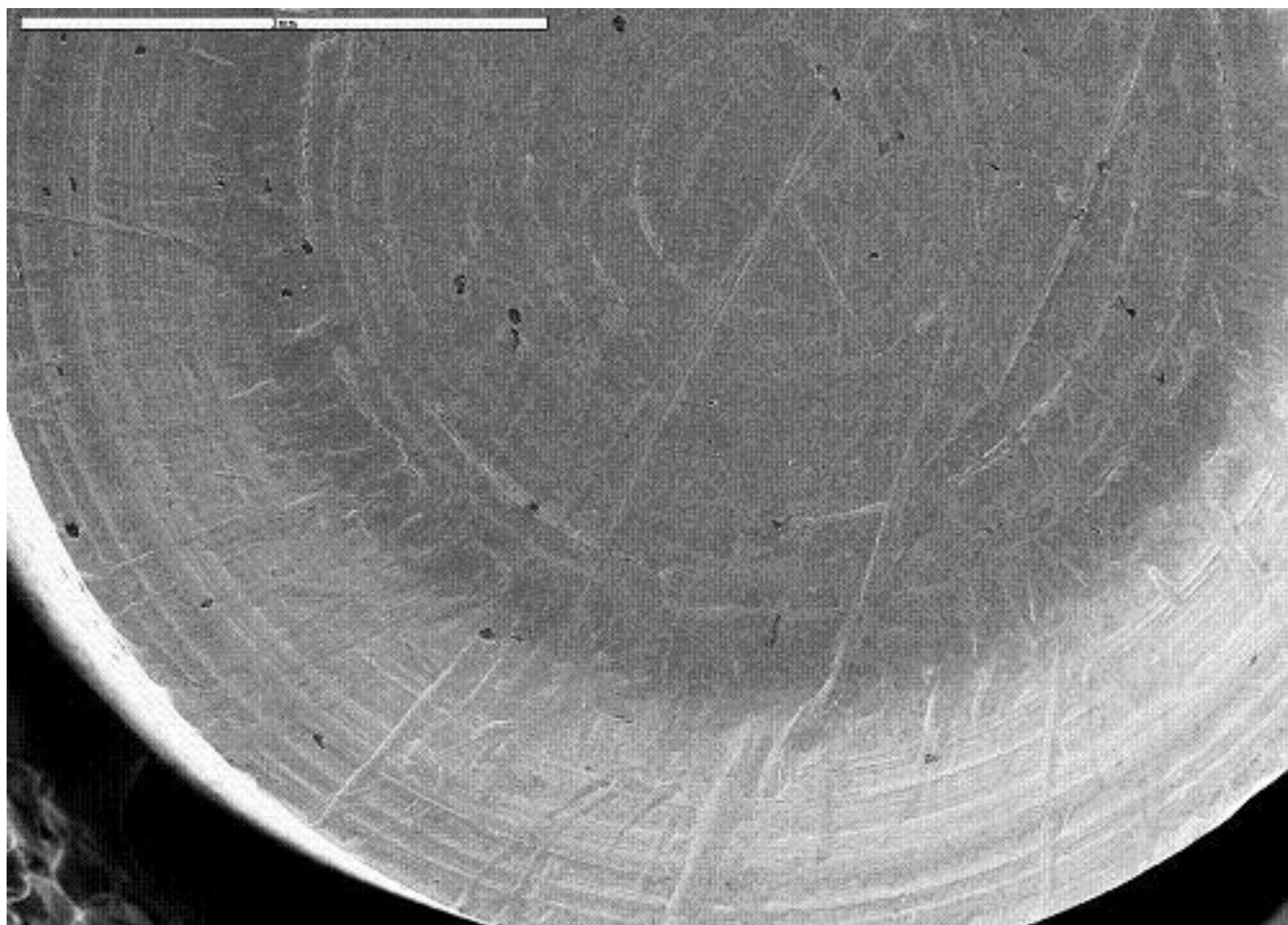
Forensics – Raking



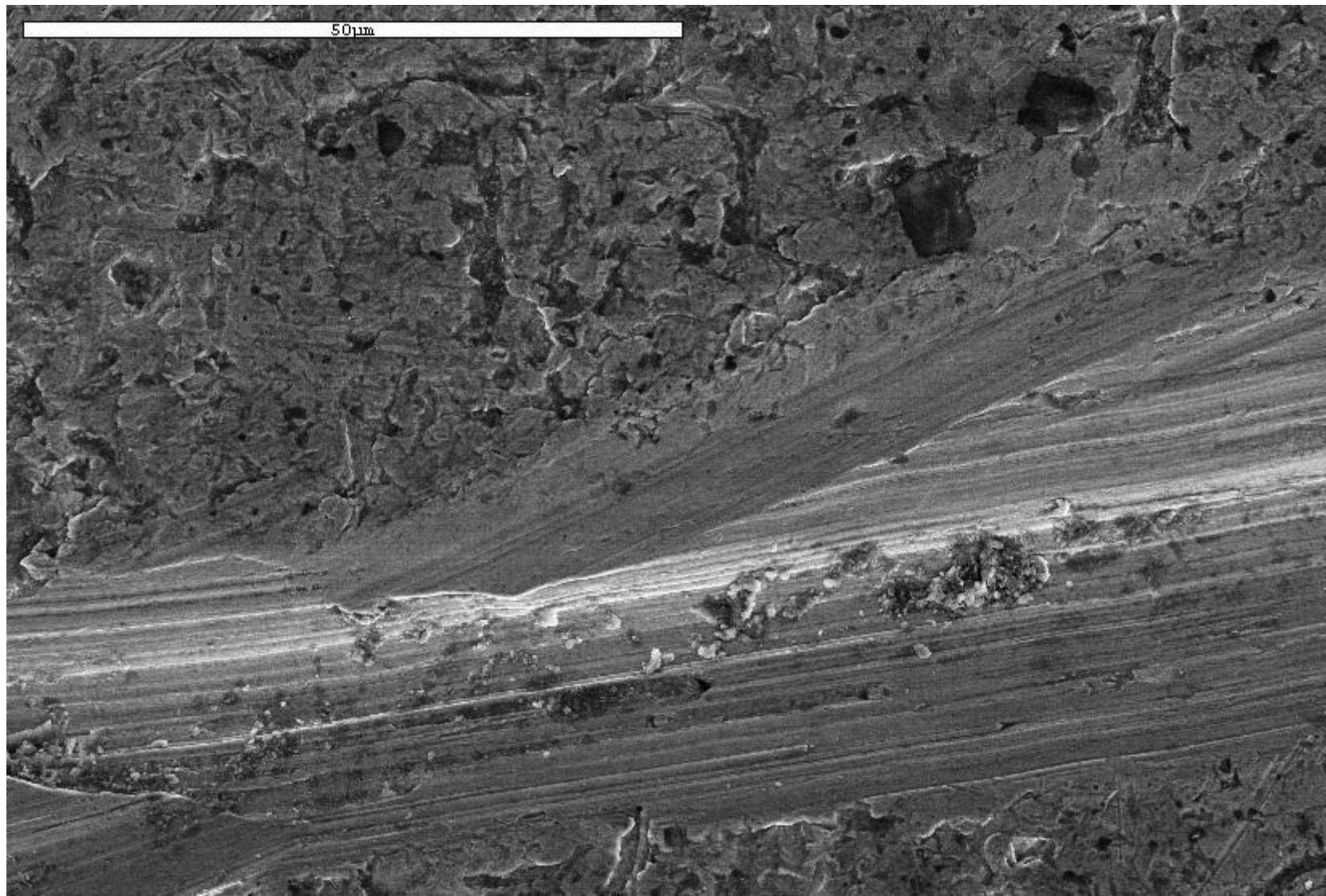
Forensics – Mixed Styles of Picking



Forensics – SEM - Picked

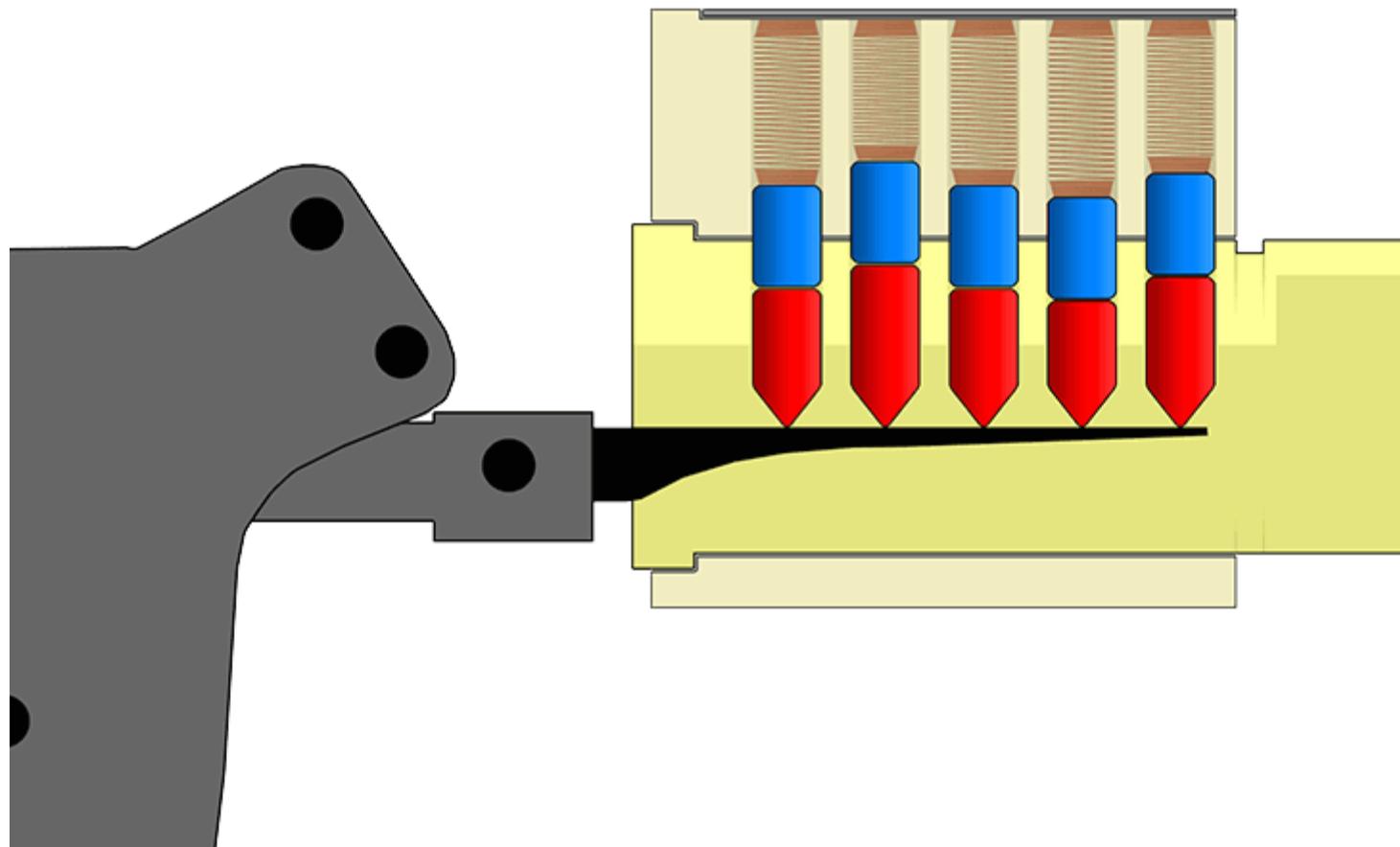


Forensics – SEM – We must get closer...



Source: Alcohol and access to a scanning electron microscope

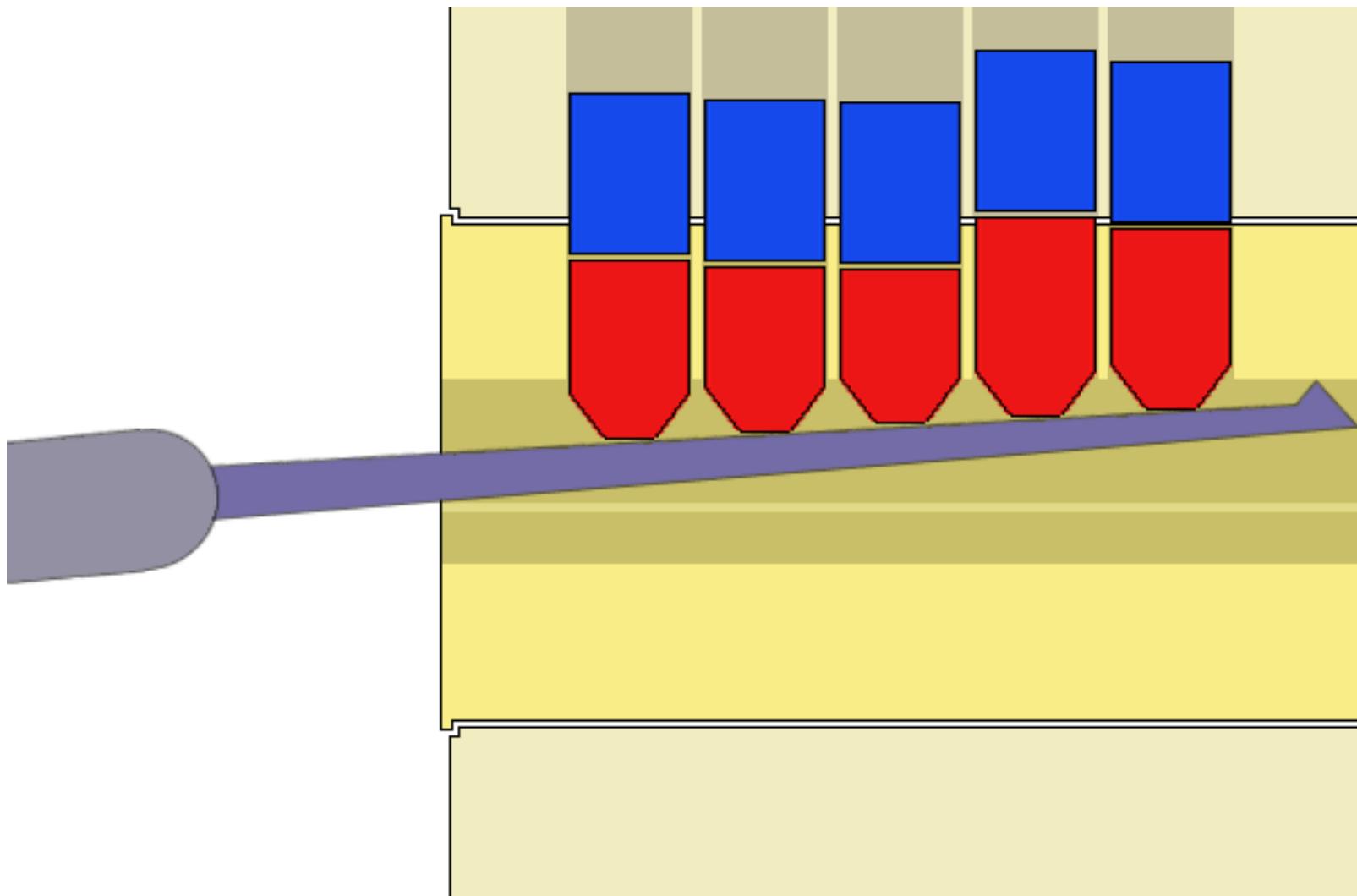
Forensics of Snapper Guns



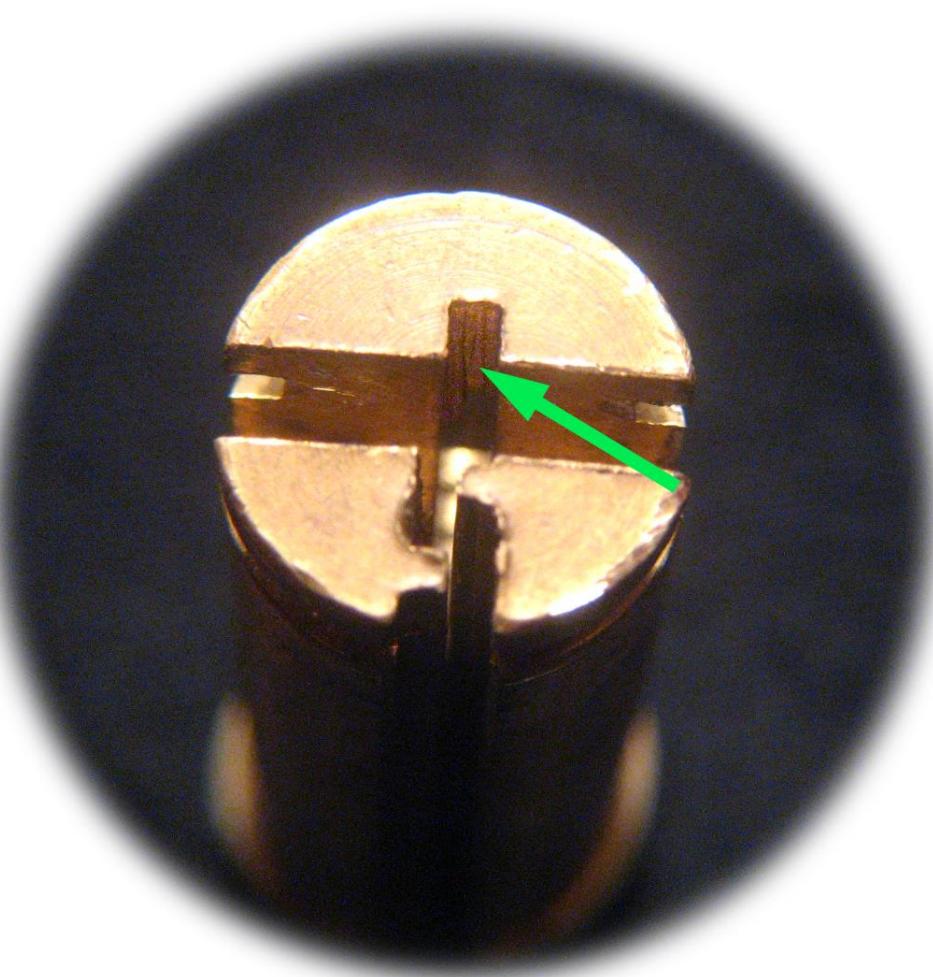
Repeated Snap Marks



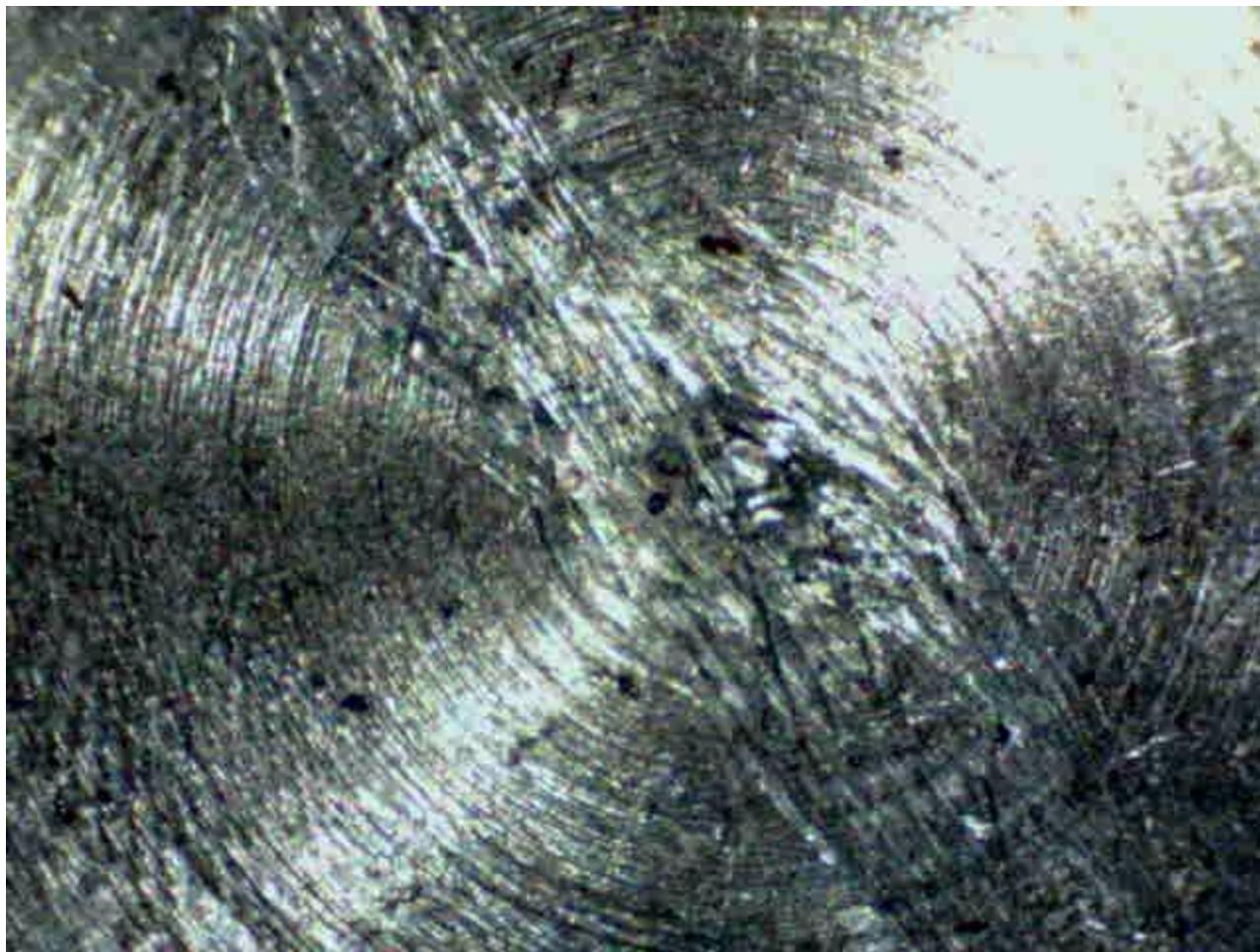
Some People Poke Too Deep



Tools Too Deep – Marks in Rear Top of Keyway



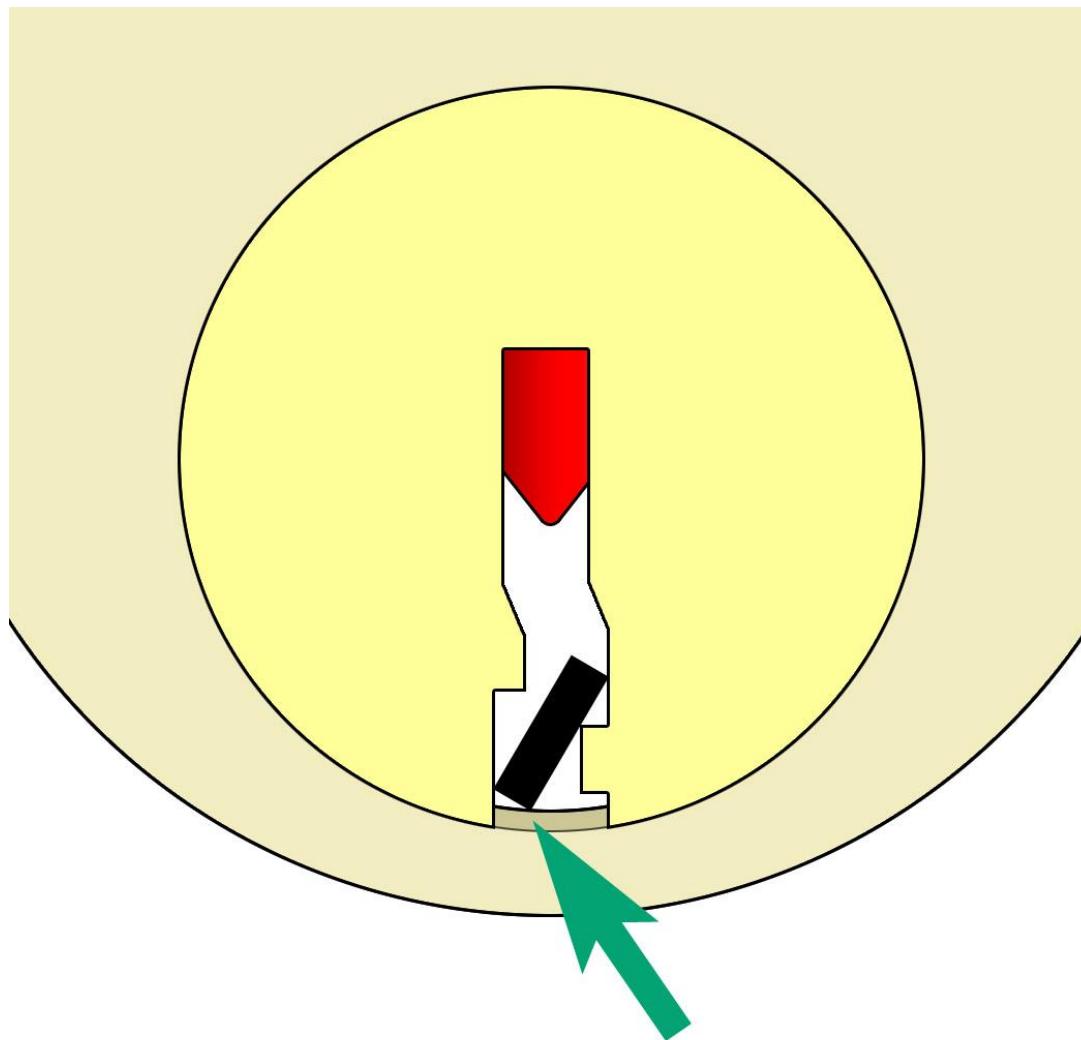
Tools in Too Deep – Marks on Tail Cap



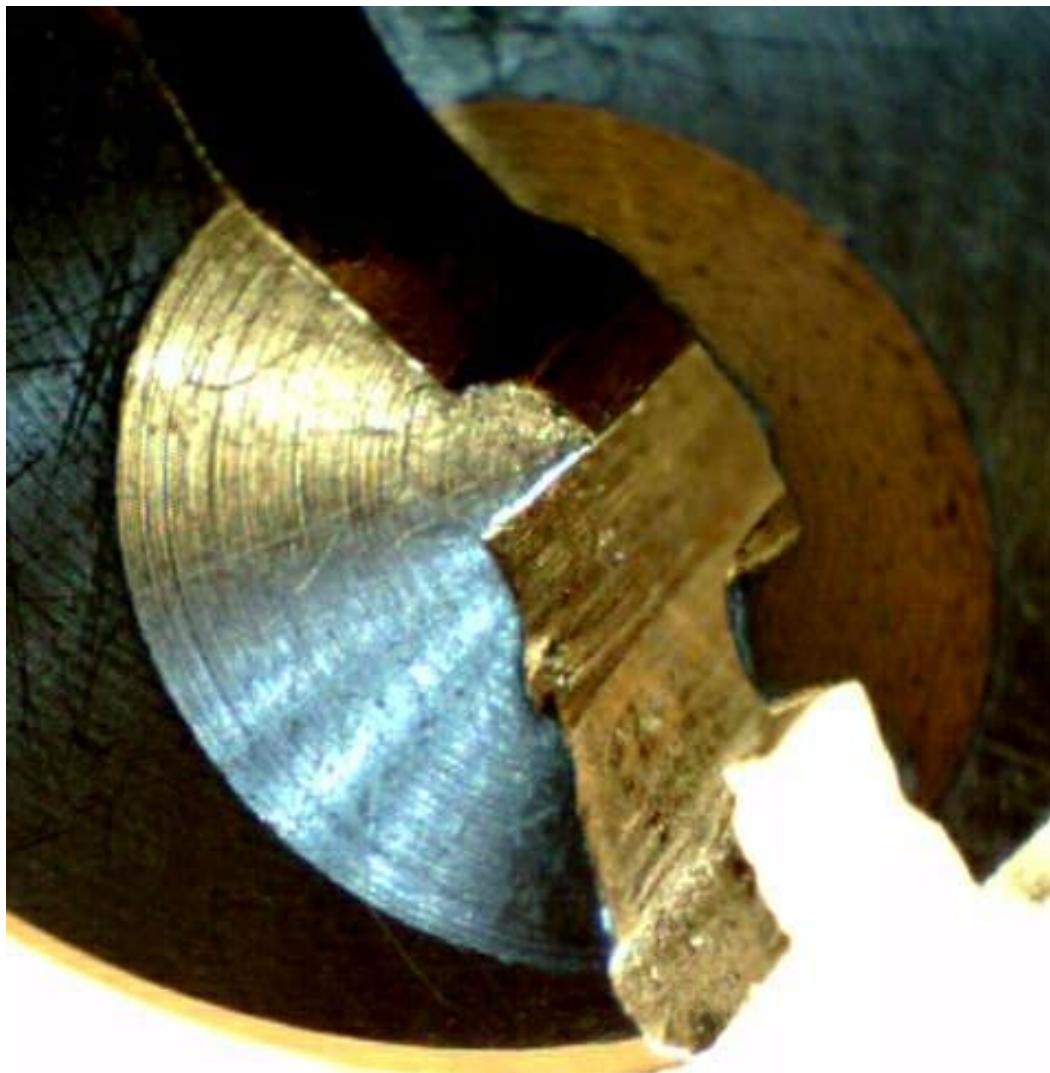
Tension Tools in the Keyway



Tension Tools can “Pinch” the Keyway



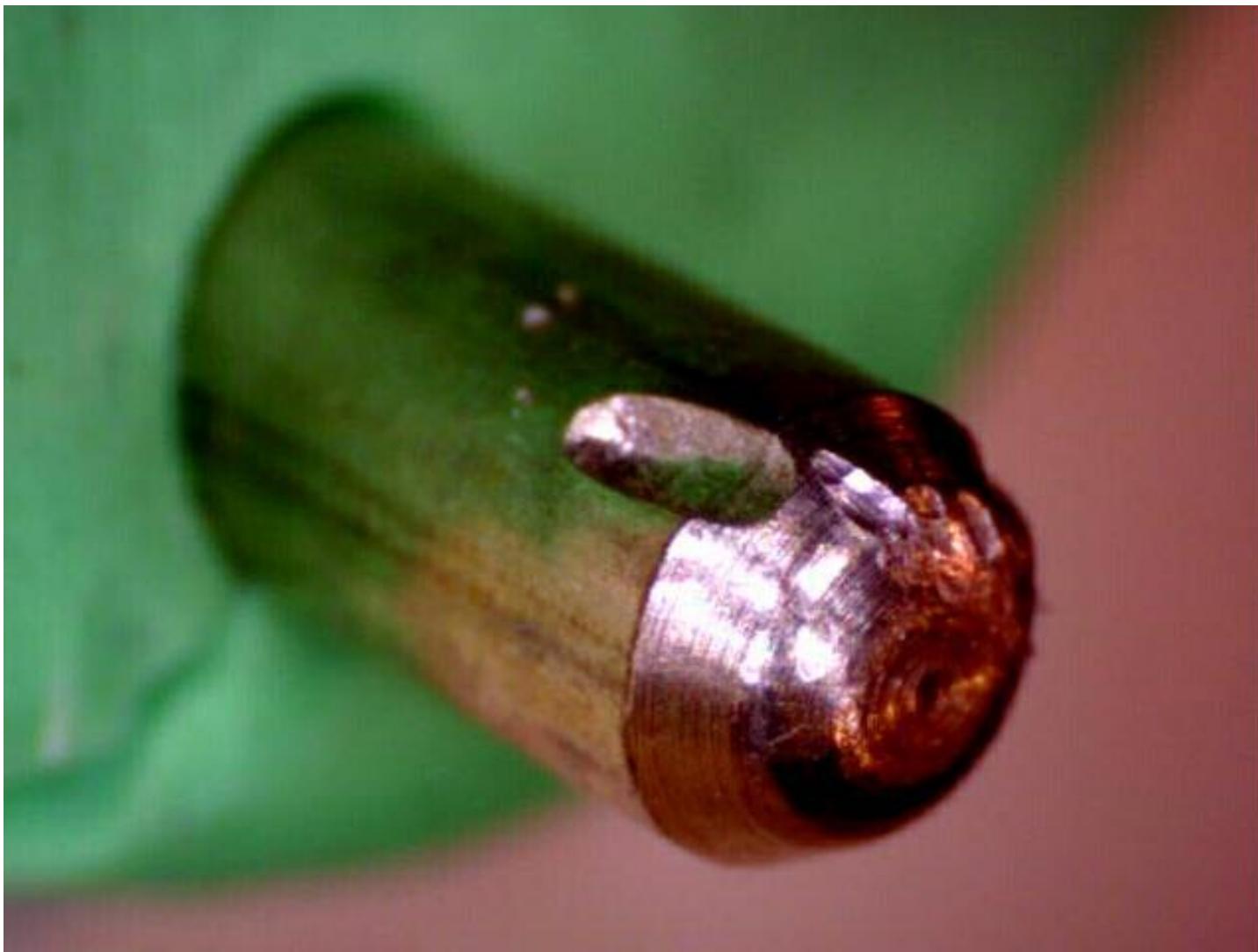
Tension Tools can “Pinch” the Keyway



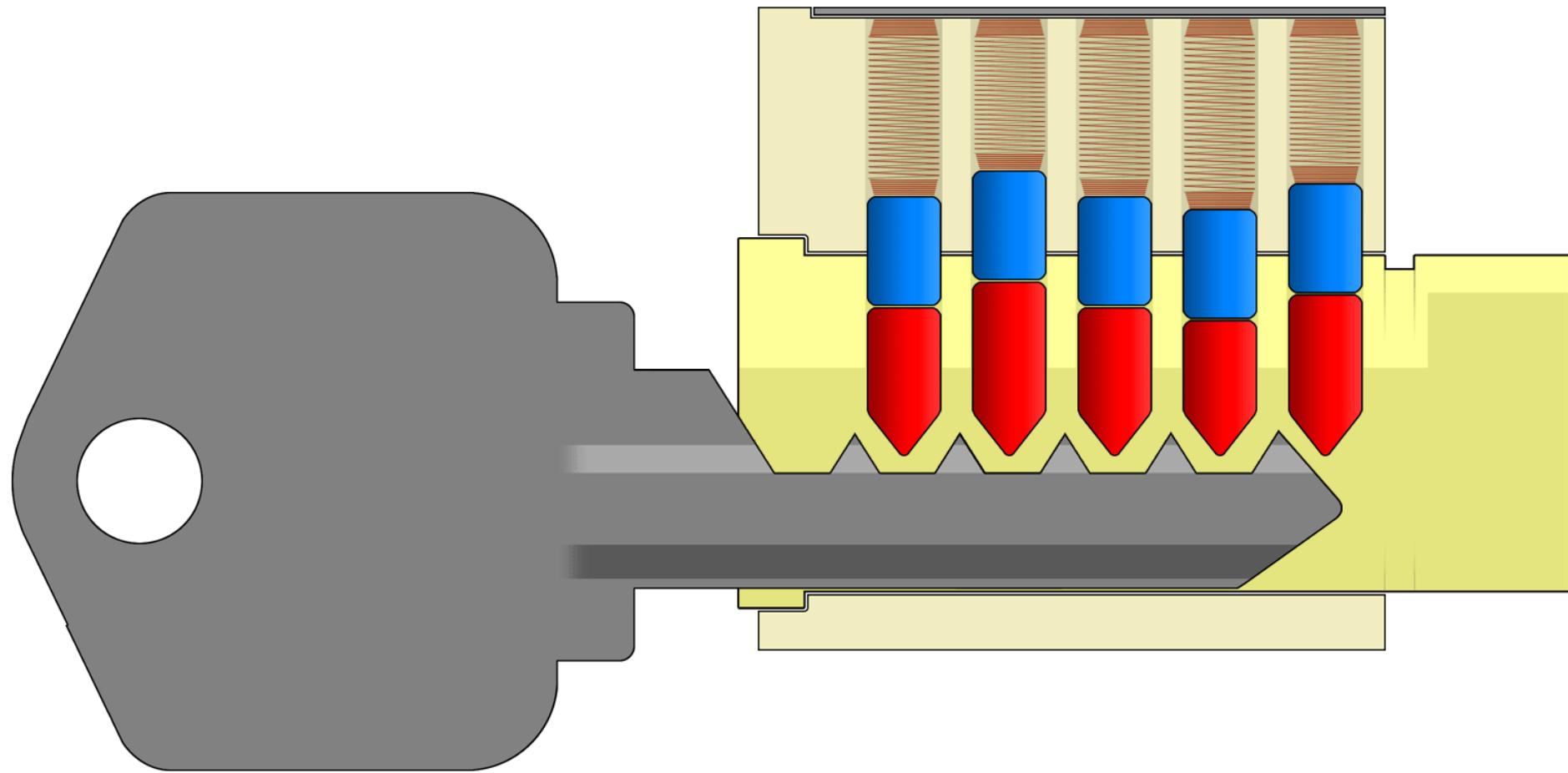
Fraudulent Toolmarks



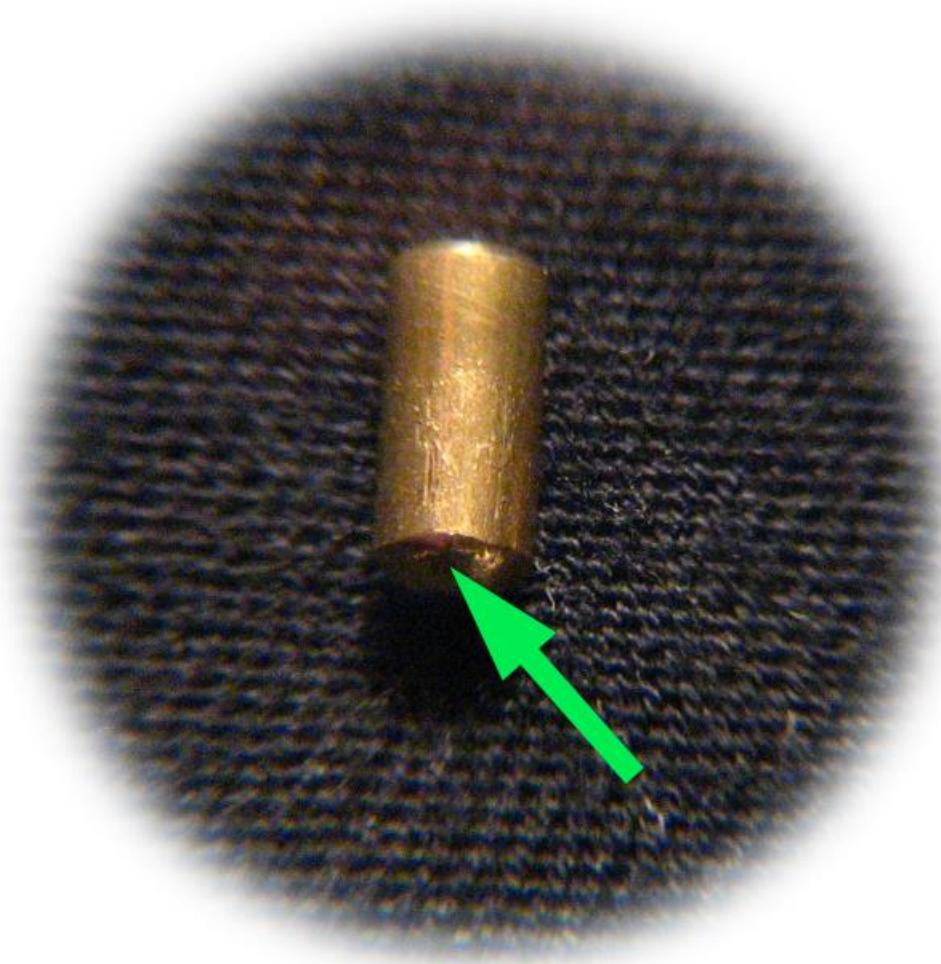
Fraudulent Toolmarks



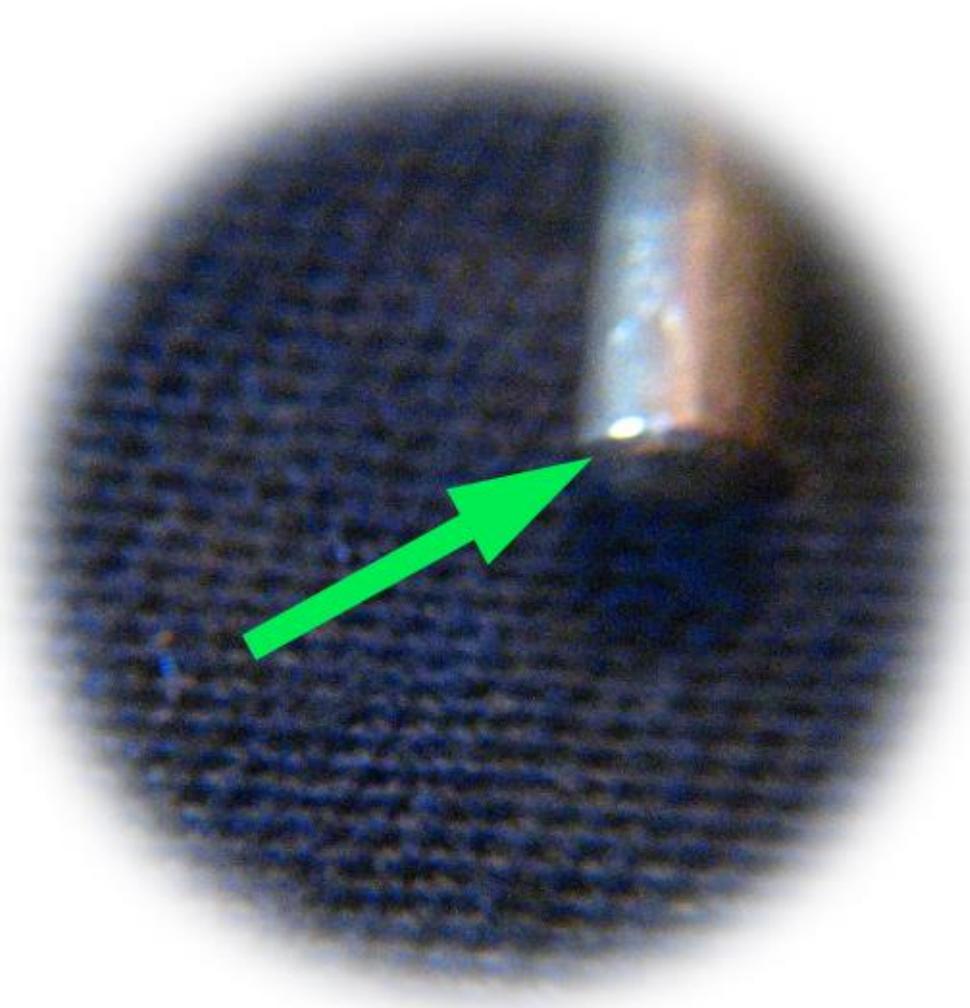
Bump Key Forensics



Bump Key Forensics



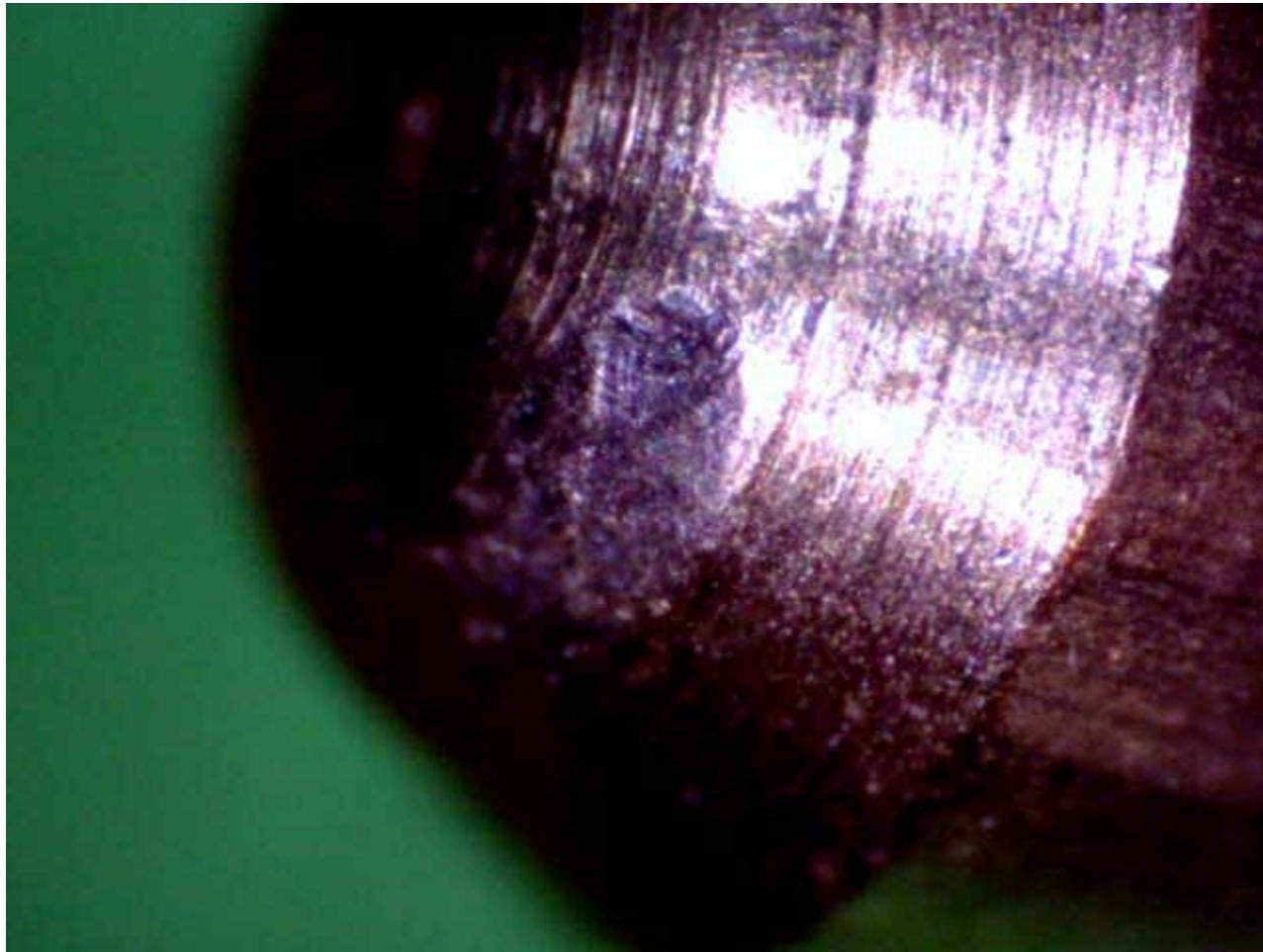
Bump Key Forensics



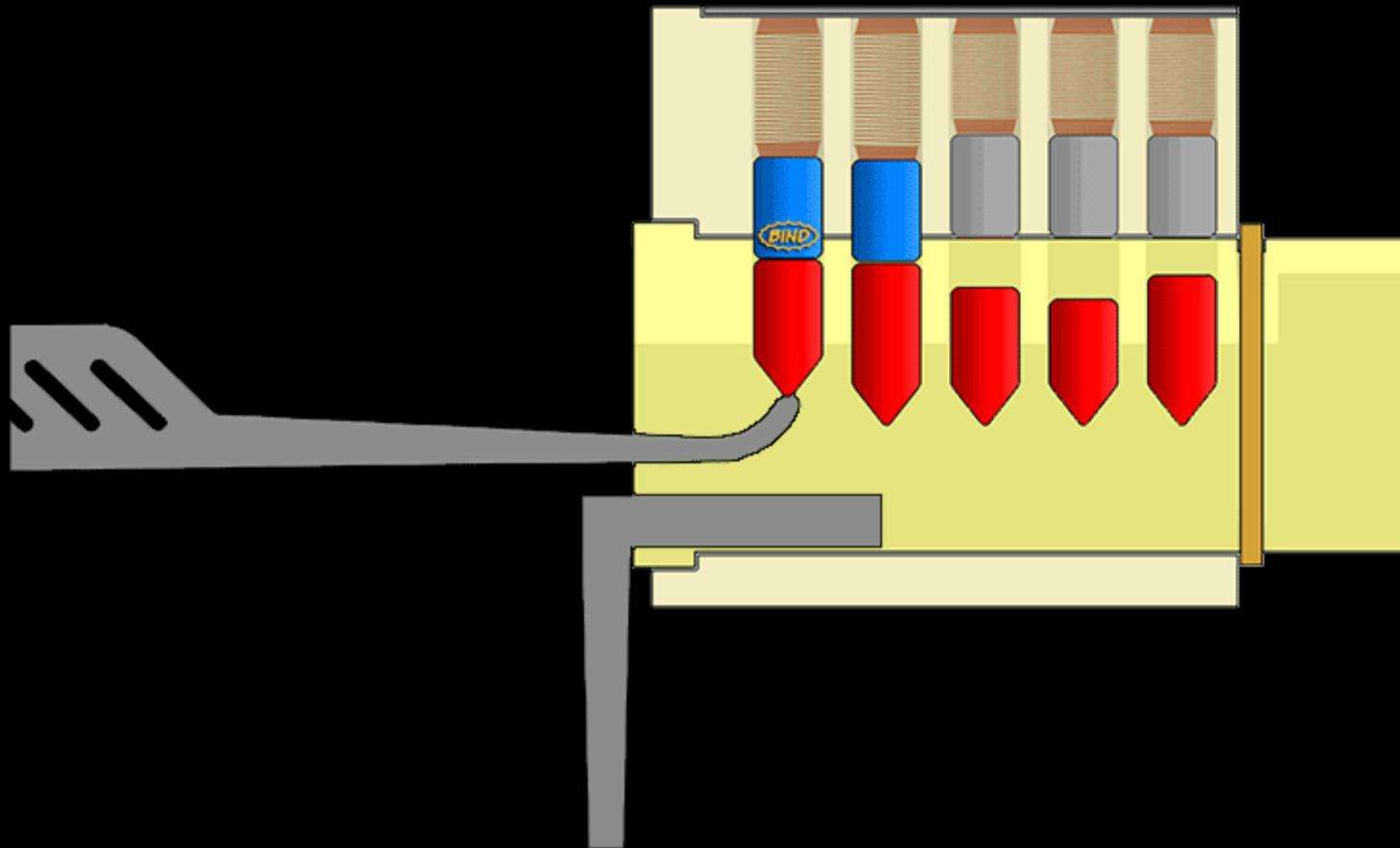
Bump Key Forensics



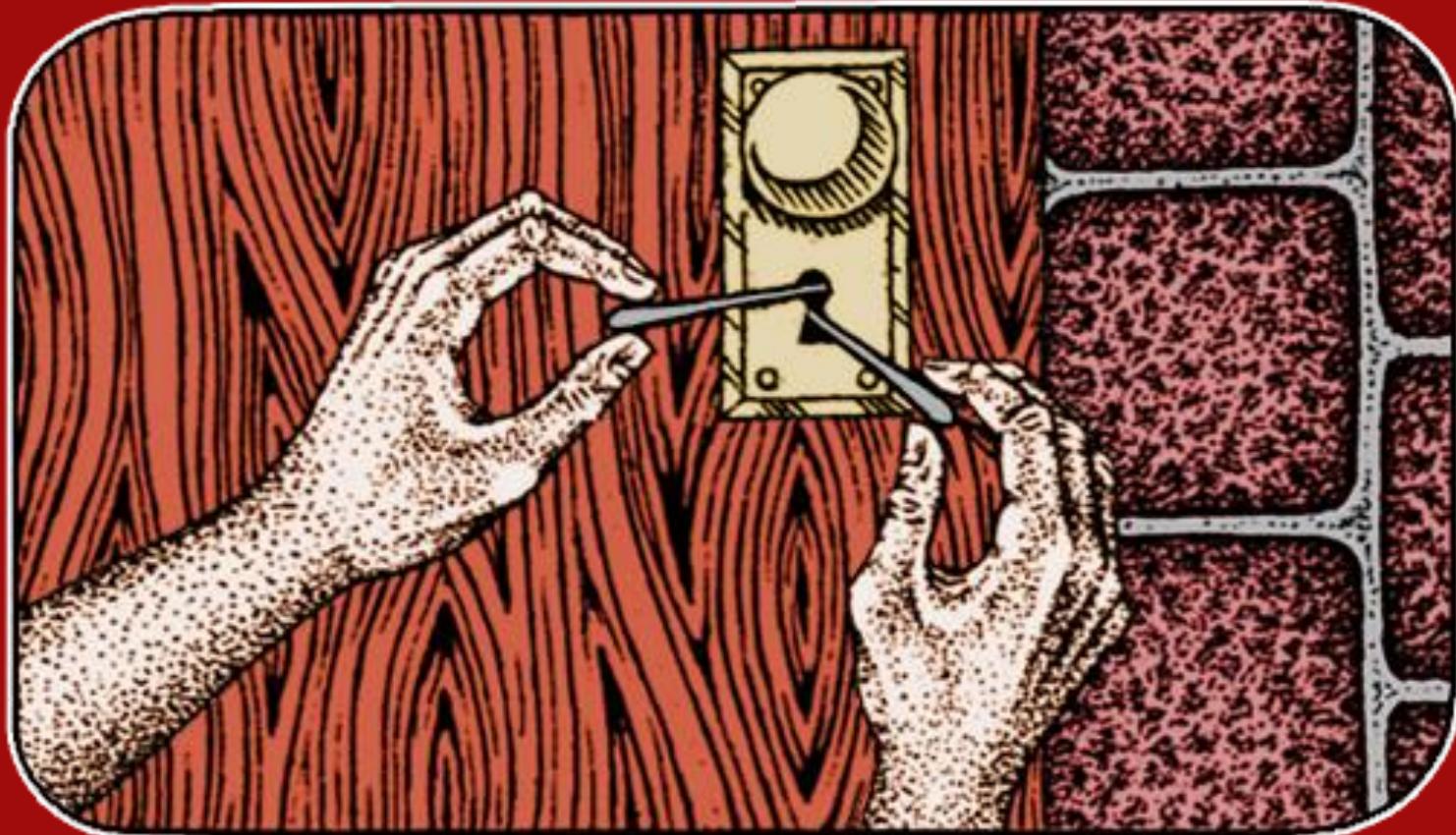
Bump Key Forensics



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

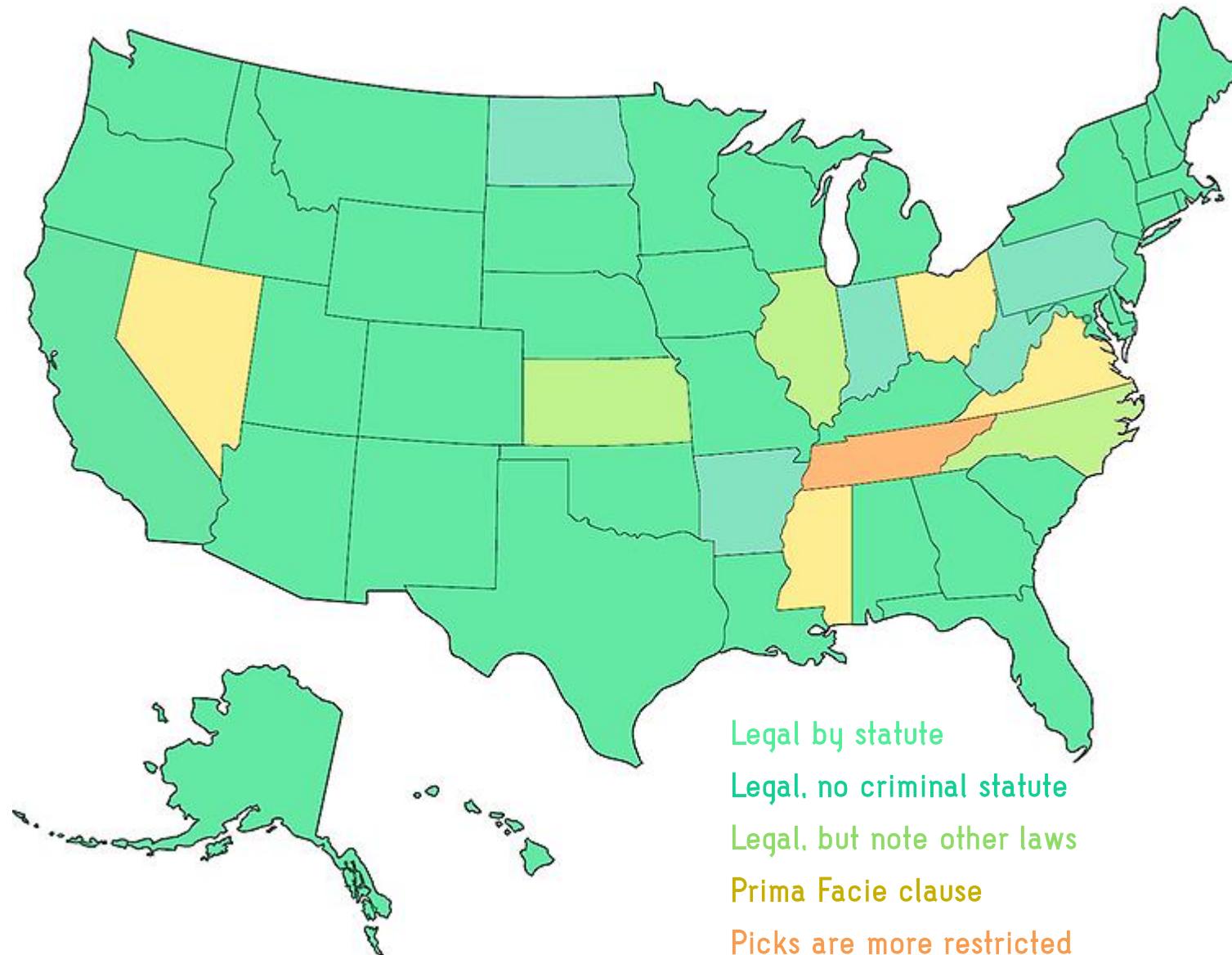
- [YouTube](#) & [Google](#)
- <http://connect.waaq.org/toool>
- <http://deviating.net/lockpicking/videos.html>

- On The Web

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



Legal Questions

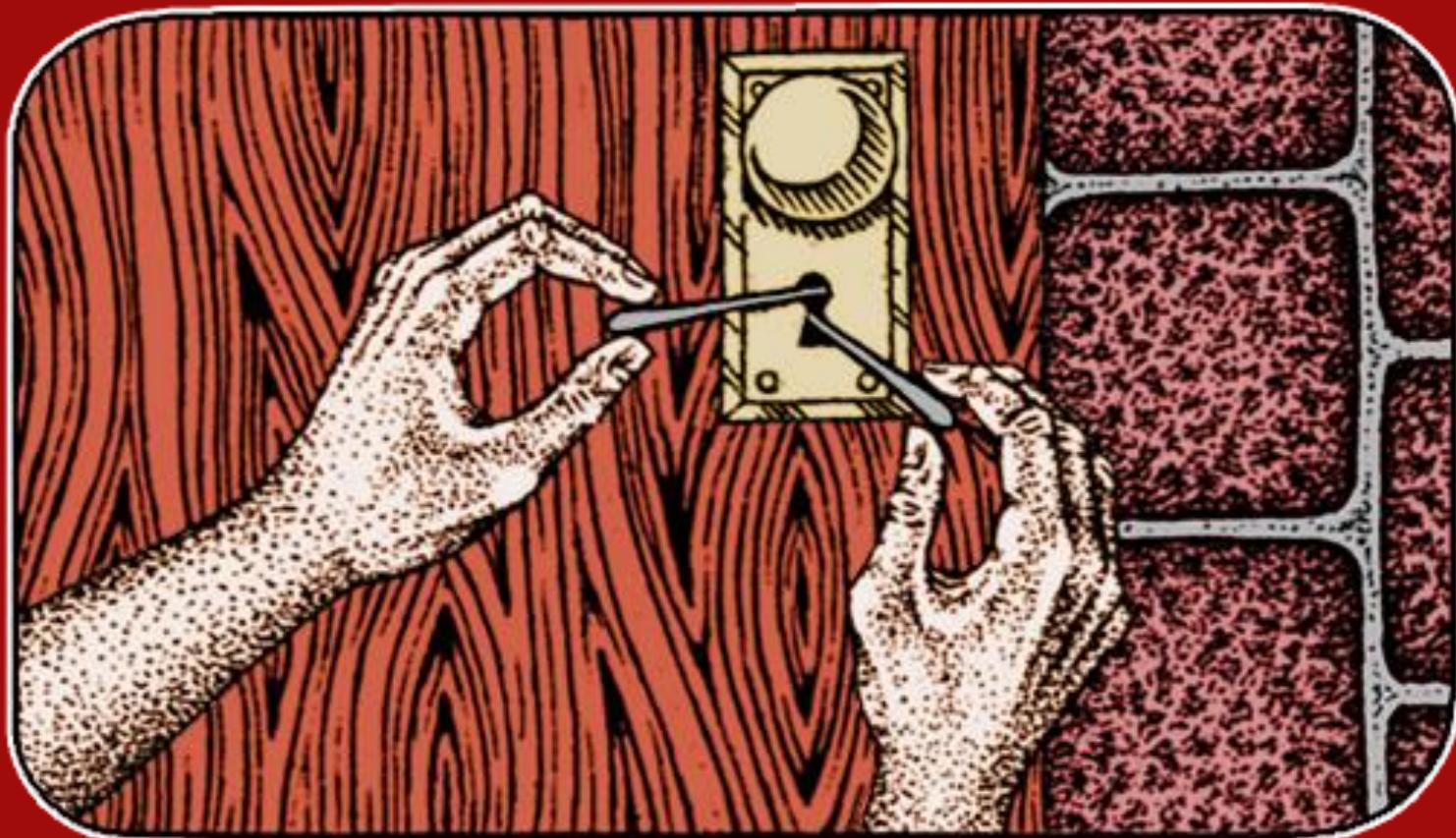


Acquiring Locks

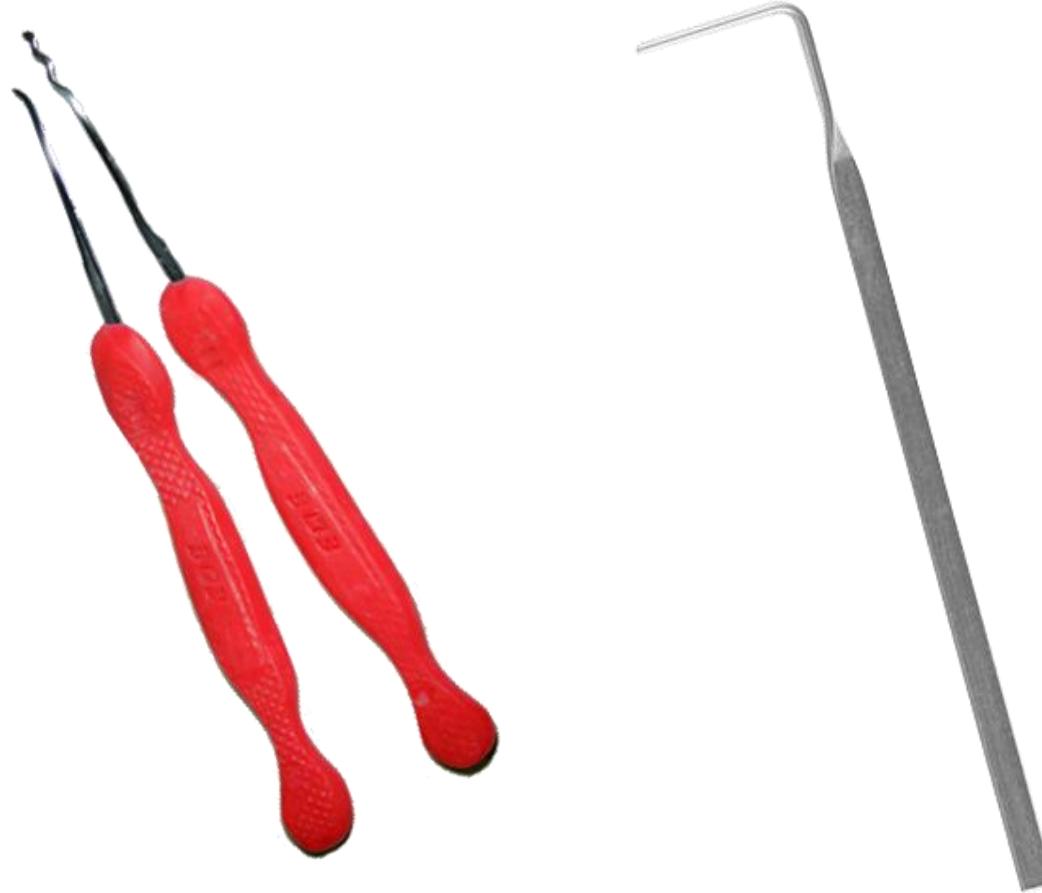
- Free
 - Basements, garages, yard sales
 - Ask neighbors, ask locksmiths
- For sale
 - Vary your sources
 - Hardware store vs. eBay
- Specialized
 - Progressive kits
 - Ultimate practice lock



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://tooool.us>

info@tooool.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.