Anti-Forensics - The Keys to the Farm

datagram, Winter 2009

1. Introduction

Hello, I'm datagram, and I run www.lockpickingforensics.com and www.lockwiki.com. This article describes a unique lock picking tool, dubbed the "Tricerapick", invented by a member of the popular lockpicking forum, Lockpicking101.com. It was an attempt to create an anti-forensics lock pick through the use of modified key segments. It is both creative and interesting, and a great example of the ingenuity of the locksport community.

This article begins with a discussion of the requirements for an anti-forensics pick, and the reasons why most are unreliable. We'll look at other anti-forensics picks that have been tested, and the degree of success they have had with evading forensic detection. We'll look at the Tricerapick, and how it works to pick a lock. Finally, we'll look at any forensic evidence left by Tricerapicks.

I can be reached at datagram.layerone@gmail.com. See http://www.lockpickingforensics.com/ for more contact information. Corrections, additions, comments, and criticism are all welcome.

If you have any ideas for an anti-forensics lockpicking tool that you'd like examined for forensic evidence, you're welcome to send me a prototype of the tool and sample locks that have been picked using it. Contact me for more information!

2. Anti-Forensics Tools

Each time I give a presentation about forensic locksmithing, whether it is to locksmiths or locksport enthusiasts, the same question comes up: Couldn't someone use a plastic pick to evade detection by a forensic locksmith? The most common suggestions I get are:

- A standard pick with well rounded and polished edges
- A pick made entirely of plastic or carbon fiber
- A thin steel pick coated with Teflon, rubber, or similarly soft material
- A brass pick (the logic being brass picks would leave the same marks as brass keys)
- A standard pick with some form of rolling ball on the tip

The fundamental challenge with anti-forensics tools is the requirement that the tool be thin enough to be usable. In most locks, this means the tool cannot be thicker than 0.030" (0.762mm), and preferably closer to 0.020" (0.508mm) for locks with difficult warding patterns. The vast majority of non-metal tools bend or break at such small sizes. Additionally, most materials do not provide the same tactile feedback as traditional steel tools, making the picking process more difficult.

Maneuvering lockpicking tools inside a lock scratches the internal components, particularly the key pins, plug walls, and pin chambers (Figure 2.1). Many of these scratches appear different than normal wear, at angles and locations inconsistent with the use of a key. The scratches left by lockpicking tools are considered an identifiable tool mark by forensic investigators.

Figure 2.1: Tool marks from the pin-tumblers of a lock picked *once* with steel tools.

Tool marks occur for three reasons. First, the hardness of the materials; the lockpicking tool is made of a much harder material than the pins (brass pins and steel tools, traditionally). Second, the key has a broad surface area which contacts with the pins, but the picking tool is considerably thinner. To lift pin stacks, the thin surface of the pick requires greater vertical force than a key. With the pin stacks pushing down and the picking tool pushing up, the pins are scratched by the picking tool. Finally, lockpicking uses premature tension to cause binding between the pins, plug, and cylinder. Binding pins require more force to properly position than using a key, facilitating tool marks and material transfer.

The lockpicking process is almost guaranteed to leave forensic evidence when traditional tools are used, even if the tools are simply inserted and removed once. Creating a lockpicking tool that is strong enough to position components but soft enough to not leave scratches (or other discernible evidence) is the challenge of anti-forensics. It is a more difficult problem than it appears, and one that does not have a great deal of public research available.

All traditional lockpicking tools that I have come across leave some form of easily identifiable forensic evidence. Many materials leave marks similar to traditional steel tools. Others leave different yet distinct tool marks and trace evidence. The rest are usually not strong enough to withstand the picking process, making them unusable as picks. To date, the types of picks and materials I have tested or come across in the field include:

- Aluminum
- Brass
- Carbon fiber
- Copper
- Fiberglass
- Plastic (various)
- Rubber (various)
- Rubber coated steel
- Steel
- Teflon coated steel
- Wood (various)

In my experience, wood, plastic, and rubber provide little tensile strength, making them generally poor picks. Most coated metals have one of two problems, either the coating is too thin to prevent marks from the underlying metal, or the underlying metal is too weak to provide adequate tensile strength. The process of coating the metal tool also quickly increases the thickness of the tool.

With current technology, I don't see any reason for a professional attacker to inconvenience themselves with any so-called anti-forensics lockpicking tools given the durability, maneuverability, and feedback of traditional steel tools. Non-steel tools often need to be thicker to provide durability, causing dampened feedback and poor maneuverability in the lock. Increased difficulty in picking the lock means a longer time to entry—something all attackers want to minimize.

So to answer the question, can plastic/other picks be used to evade detection? Yes, theoretically. Currently it seems like a poor trade for the attacker, especially considering that most of the anti-forensics tools don't work as advertised.

3. Carbon Fiber & Fiberglass Tools

Two materials commonly associated with anti-forensics are carbon fiber and fiberglass. Both provide more strength than traditional plastic and rubber tools, and are considerably softer than steel. So far, they seem like perfect candidates. Like plastic and rubber, the usefulness of different carbon fiber and fiberglass strains varies greatly. The ideal candidate provides high vertical strength at thicknesses between 0.020” (0.508mm) and 0.030” (0.762mm) and facilitates feedback transfer from the picking process.

Admittedly, I am not an expert on the many types of carbon fiber and fiberglass available. I've only tested tools that are available locally, commercially, developed by the locksport community, and those tested from a limited number of investigations. It's very possible that there is a special composition that may facilitate anti-forensics, but I'm not qualified to know the difference. A pick is a pick, and thus far all samples that I've tested have left forensic evidence.

Figure 3.1: Working examples of carbon fiber (top) and fiberglass (bottom) lockpicking tools.

It's possible to make functional lockpicking tools out of both materials (Figure 3.1), but do they stand up to forensic investigation? Simply: no, and neither is very durable. Both tools leave marks similar to traditional steel tools. Fiberglass tools have a fairly unique tool mark as well as trace evidence because of the nature of the material. Durability wouldn't matter if the pick withstood one picking session and did not leave forensic evidence, unfortunately this is not the case. Without anti-forensics capabilities there is little reason to choose either material over steel tools.

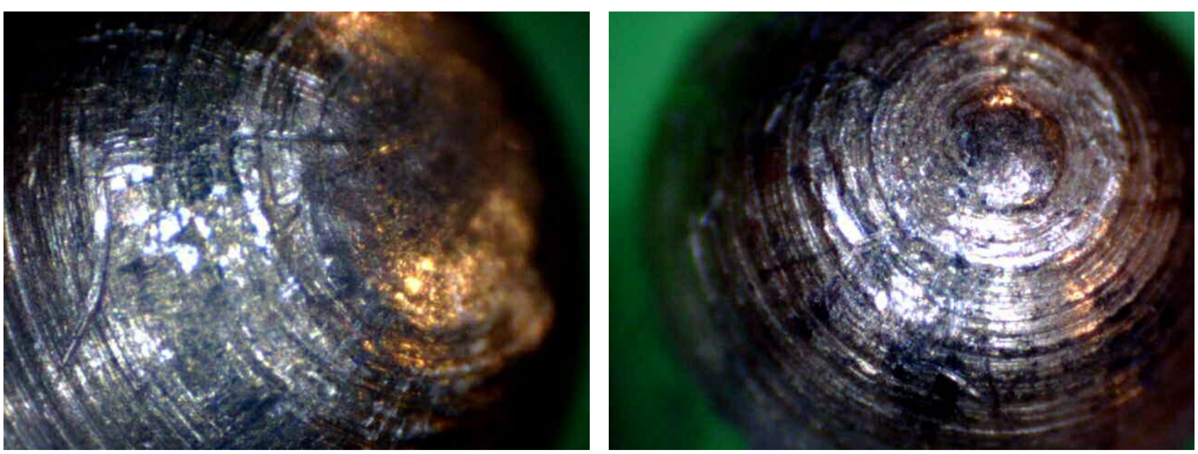
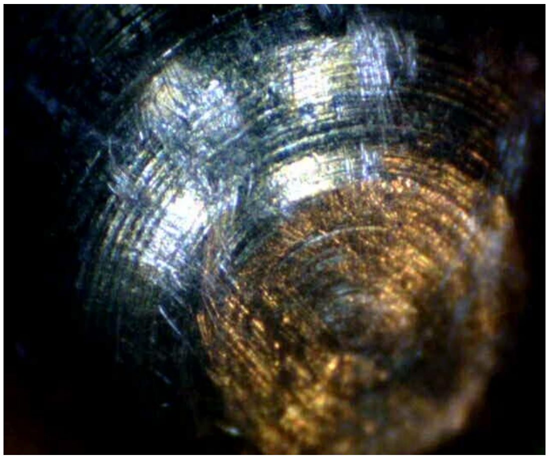


Figure 3.2: Tool mark evidence left by a carbon fiber lockpicking tool from a lock that was picked one time. Notice the light scratches and polishes made on the bottom of the pins.

The pictures above (Figure 3.2) are pins from a lock that has been picked once with a carbon fiber pick. The picture on the left shows tool marks similar to those made by traditional steel tools, but they are less defined. The picture on the right has tool marks that are harder to spot; the light scratches and what appears to be a light polish, near 6 and 7 o'clock.



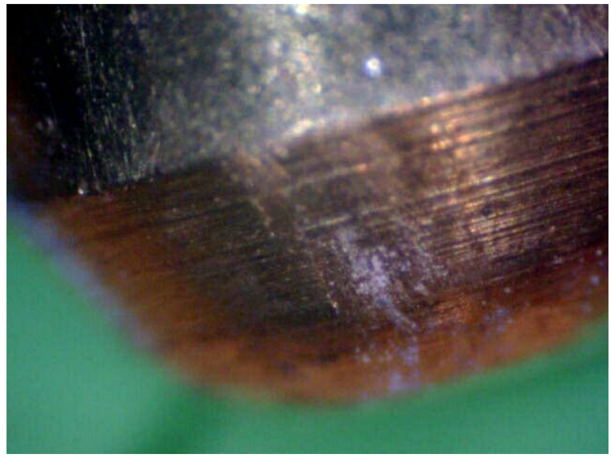


Figure 3.3 (left): Tool marks made by a fiberglass pick, note the “wispy” style of scratches.
Figure 3.4 (right): Trace evidence (fiberglass dust) found on the pins in the lock.

Fiberglass tools leave a considerably different tool mark (Figure 3.3). In the photo, we see a variety of small scratches along the bottom of the pin-tumbler. Each scratch is actually a set of smaller scratches, caused by the fibers weaved through the fiberglass. Fiberglass also leaves distinct forensic evidence in the form of fiberglass dust inside the plug (Figure 3.4). As a foreign material, fiberglass found in a lock is a valuable clue for the forensic locksmith.

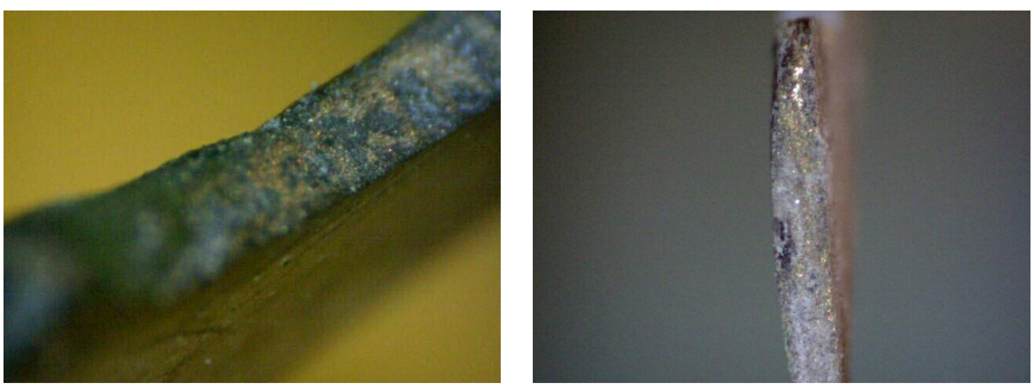


Figure 3.5: Brass and lubricant material transfer on both carbon fiber and fiberglass picks.

In both cases, the tools also take away small amounts of brass and lubricant from the lock (Figure 3.5). It's possible that a suspect can be linked to a crime scene based on this type of material transfer should the lockpicking tools be found on their persons. In some cases, the type of brass used in a lock may be proprietary, definitively linking a set of tools to a type of lock.
So all in all, carbon fiber and fiberglass picks do work; they can pick a lock. Unfortunately, their

poor durability and inability to provide anti-forensics capabilities make them poor alternatives for traditional steel tools. It's possible that a clever combination of these materials with a plastic or rubber coating could provide longevity and forensic resistance, but thus far I haven't seen a working pick with these qualities.

4. Keys to the Farm

Every year I'm fascinated by the creativity and perseverance of the locksport community. Many recent breakthroughs in physical security exploitation have come not from research departments, but locksport enthusiasts experimenting and finding different ways of beating some of the best locks in the world. Some of my favorites have been: the Medecoder by Jon King, the Kwikset Smart Key decoder by Shane Lawson (valanx), and the CLIQ attacks by Jord Knaap, Marc Tobias, Tobias Bluzmanis, and TOOOL NL.

The main focus of this article is to discuss a new lockpicking creation by FarmerFreak, dubbed the “Tricerapick”. Farmer is a member of the Lockpicking101.com forums who has posted several times on The Open Source Lock forum about different ideas to make a pick-resistant lock. Many of these are exceptional and all are interesting. He contacted me with an anti-forensics lockpicking idea he had, and after fleshing it out he sent me some test samples to perform forensics on. The Tricerapick is a cross between a tryout key and a lock pick, and is one of the most creative tools I've seen. In total, it is a ten piece set – nine picking tools and a tension tool. The tools are visually distinct as modified portions of real keys (Figure 4.1).

Figure 4.1: The Tricerapick lockpicking set (first edition, 10 pieces)

The tool works by applying tension to the plug, then uses different key tools to raise various pin stacks. While picking the lock, the tool resembles a composite key system, and in many ways it is. Farmer has since expanded the set to sixteen pieces to account for difficult pin combinations.

The tools are used by gently moving in and out of the lock to find the shear line, much like a tryout key or a half diamond pick. You start by using the lowest depth from each group of three, maneuvering each inside the lock while applying tension with the tension tool. For every two pins you use one tool to find the shear lines. If the shear line cannot be found, you swap them out for higher depth pieces in each group, as needed. Once the correct position and key tools are found, the pieces are kept inside the plug until the lock is picked and plug rotated.

Admittedly, I did not have much luck with the tool when I tried to use it. It took me a while to open a sample lock he sent me, but I suspect that's due to a lack of familiarity with the tool. With a bit of practice this could be a viable method of surreptitious entry, but it is more difficult than traditional tools. Farmer was kind enough to put up a video of him [demonstrating the Tricerapick](). The video does a better job showing how this tool works than I can put into words; watch it!

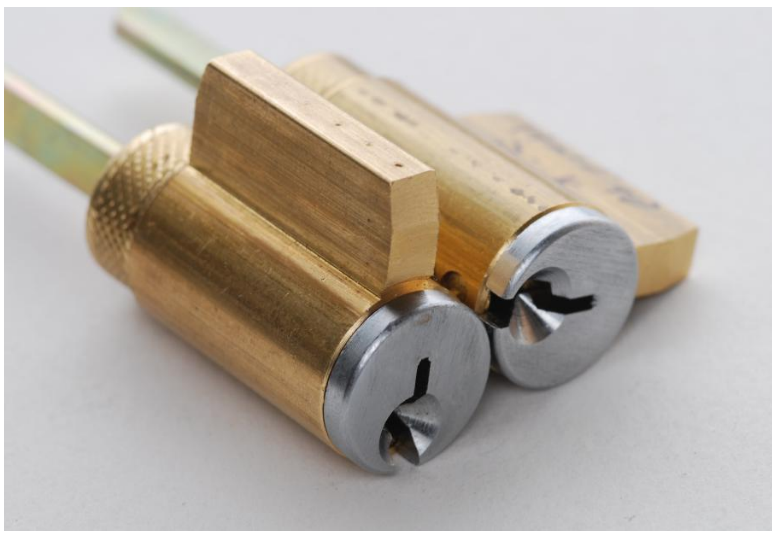


Figure 4.2: Locks used for the examination of Tricerapick tool marks.

The locks used in these tests were 6 pin off-brand Schlage knock-offs using SC4 keyways in a key-in-knob style cylinder. The pins, plug, and cylinder are made of brass. Bottom pins in the lock have the traditional Schlage-style pointed tips. As a requirement by me, Farmer had to use new locks to ensure nothing other than the working key and Tricerapick had been used.

To disassemble these locks I removed the metal from the top of the bible. Being that the tool is so similar to a regular key, I did not want to shim the lock or use a working key for fear of contaminating evidence. As always, forensic-safe tools were used to work with the pins, namely plastic tweezers and a soft rubber pin tray. I use a soft, bright green modeling clay to hold the pins for examination with the microscope.

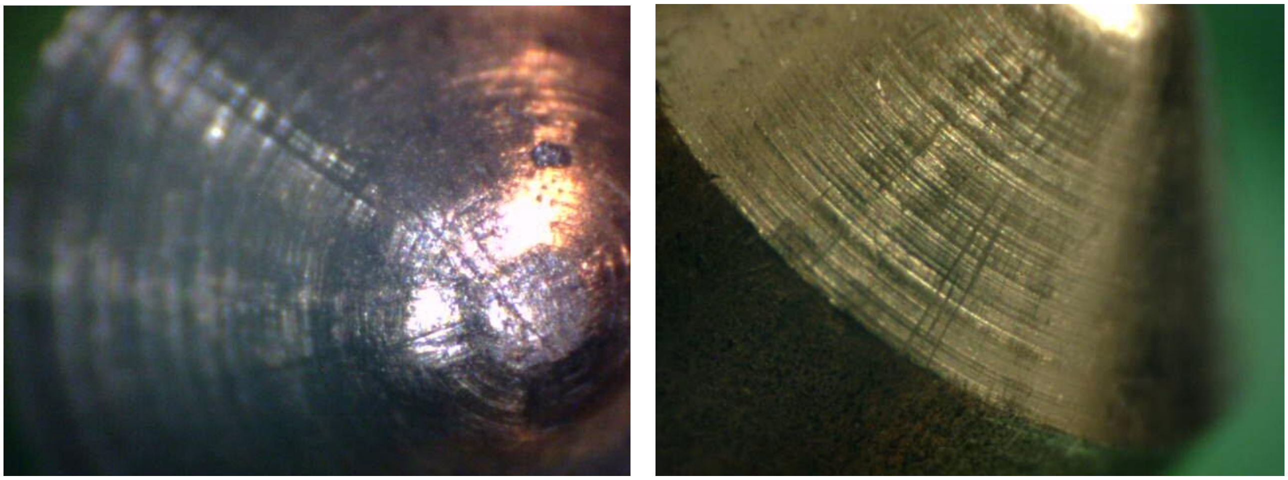


Figure 4.3: Normal wear tracks on pointed pin-tumbler key pins. Caused by the use of a key.

Before we look at any evidence left by the Tricerapick, we need to know what to expect from a lock with normal wear. Unlike other lock brands, Schlage pin-tumblers use pointed bottom pins. Only a minor change from the rounded bottom pins used in other locks, but it does have an effect on how they wear down. One major difference is that pointed pins do not rotate as freely. Pointed pins commonly have visible key tracks on each pin (Figure 4.3). Rounded pins distribute wear evenly, causing rings around the base of the pins. A detailed look at normal wear is available on Lockpicking Forensics' Normal Wear page.

So does this tool leave forensic evidence? Though the tool is more difficult to use than traditional steel tools, it would be extremely valuable if it evaded forensic detection. In spite of the tool resembling and functioning like a normal key, it does in fact leave various forms of forensic evidence. The use of premature tension along with the metal of the tool (albeit brass) still creates evidence on the bottom of the key pins. There are a different tool marks left by the Tricerapick, each being inconsistent with normal wear.

The first type of tool mark appears as light bumps on the tips of the pins, presumably from positioning of the tools inside the lock (Figure 4.4). This is distinctly different from both key bumping and pick gun impact marks, which have a broader, flatter surface area (see Lockpicking Forensics' page on key bumping for more information).

Figure 4.4 (Left): Light material displacement is visible on the tip of the key pin. Caused by movement of the tool against binding and set pin stacks.

Tool marks may also appear as exaggerated key tracks along the slopes of the key pins (Figure 4.5). The tracks are caused by the extra vertical force required to lift a binding pin, or to maneuver under a pin that has already been set. This is similar to normal wear, but instead the tracks are deeper, with uneven and sometimes wavering tracks. In addition to this, key tracks can be off-center, and even at angles inconsistent with the use of a normal key (Figure 4.6). Though the Tricerapick is made from keys it is slightly smaller than a real key. This gives it more mobility within the plug, allowing it to make key tracks inconsistent with normal wear.

Figure 4.5: A distinct key track, caused by the Tricerapick. In addition to being quite deep in the brass, there is a slight wave in the center of the tool mark; something atypical of normal wear.

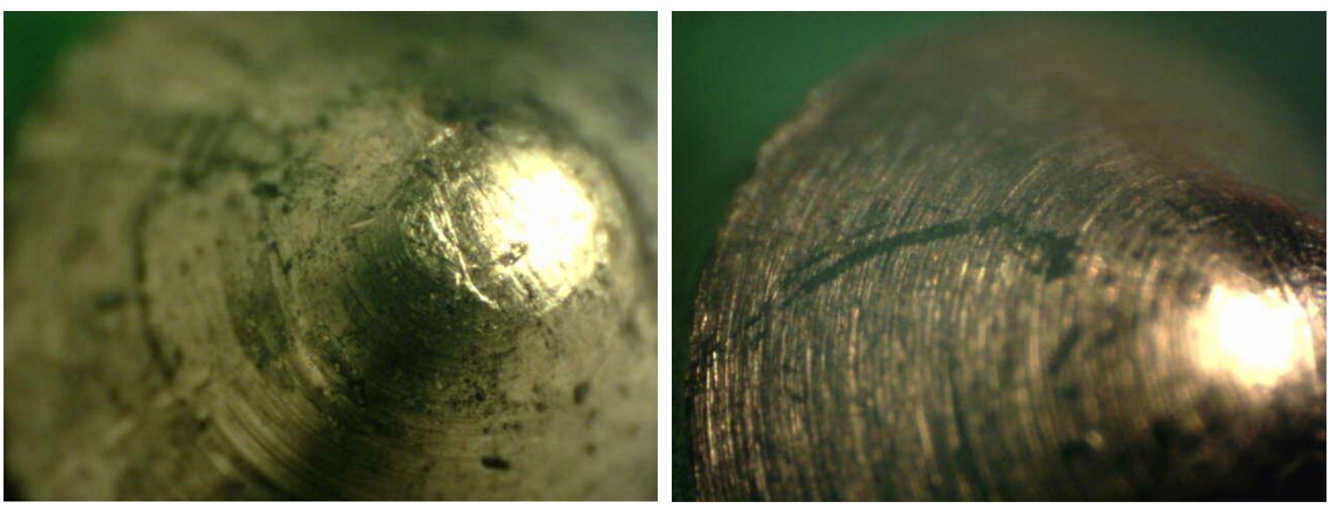


Figure 4.6: Key tracks left by the Tricerapick may be uncommon. Off-center tracks on the tip of the pin are common (left), as well as oddly shaped key tracks on the slope of the pin (right).

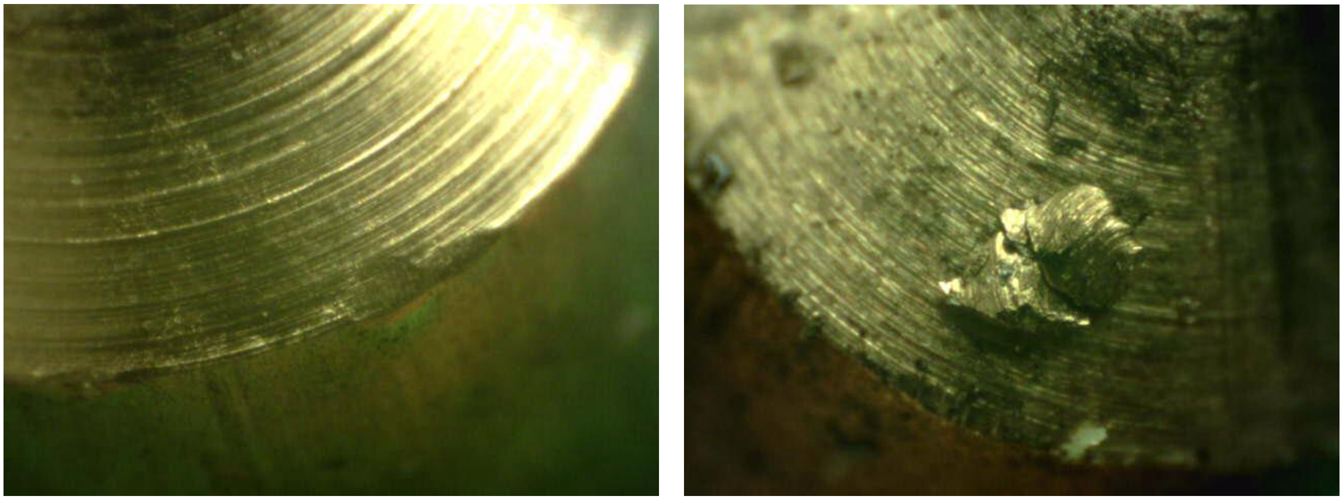


Figure 4.7: Miscellaneous tool marks left by the Tricerapick: distortions to the edges of the key pins (left), and strange material transfer/displacement between tools and pins (right).

Finally, there are a few other interesting tool marks and oddities. I found fairly common distortions to the edges of the bottom of the key pins (Figure 4.7, left). This sometimes appears in normal wear, but is usually due to poorly cut keys, or keys with a very high MACS. There's also a mild amount of material transfer between the key tools and the pins (Figure 4.7, right). Small bits of brass can (and do) transfer between the tool and the pins. We also find fibers on various pins (Figure 4.8). These may have come from something Farmer had in his pocket or on his worktable when he was making the tool. In a real investigation, these may be important pieces of evidence that help link a suspect back to the crime scene.

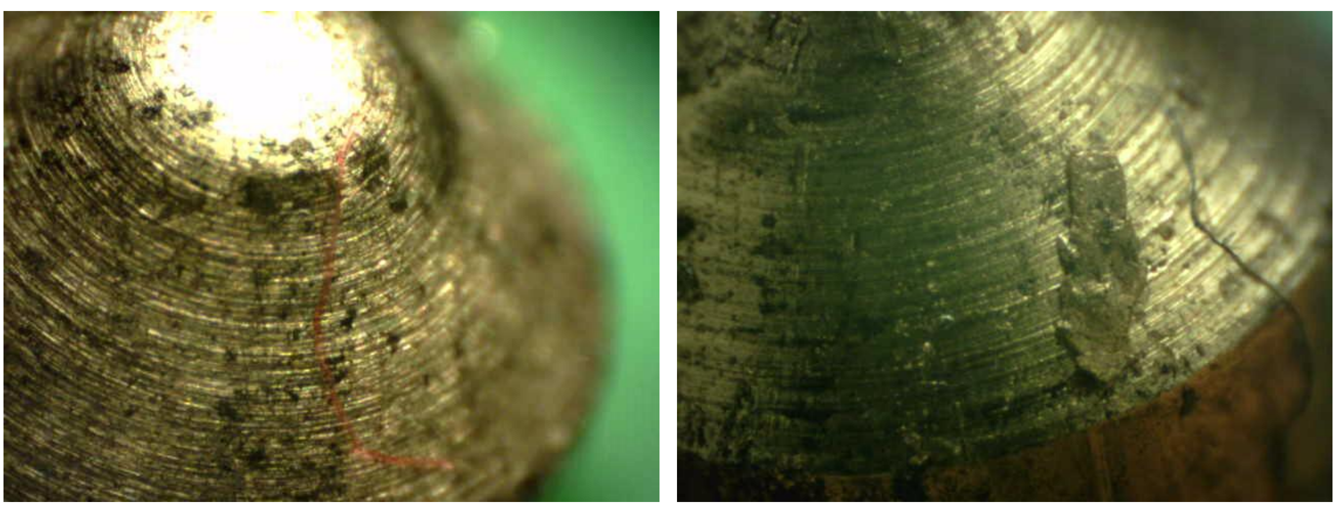


Figure 4.8: Red and black fibers found on the key pins of the locks. In the photo on the right, we also see more material transfer in the form of a mysterious blob (the technical term for "couldn't afford to call the crime lab for LP Forensics articles").

On the tools themselves we can identify a few important clues. First, it is fairly obvious that the tools were made using factory original Schlage SC4 keys. We can determine this by the partial Schlage logo, the material of the key, and the length of the key blade (Figure 4.9, left). The surface of the tool can tell us what tools were used to make the Tricerapick (Figure 4.9, right).


Figure 4.9 (left): One of the Tricerapick tools, showing the partial SCHLAGE logo.
Figure 4.9 (right): Tool marks on the Tricerapick tools show a hand file was used to make them.

The tips of the tools also show interesting characteristics, particularly surface deformities that might be mirrored by the pins in a lock the tool was used on (Figure 4.10). Unfortunately, identifying those surface deformities is out of the scope of this article. The black area is lubricant transferred from the pins in the lock, another important piece of evidence.


Figure 4.10: The tips of two of the Tricerapick tools showing surface deformities and wear.

5. Rake Keys

The tools created by FarmerFreak are *not* the same as the “rake” keys made popular by the UK Bump Keys forum. Rake keys are essentially interactive tryout keys; a key cut like a rake pick that you jiggle back and forth in the lock. Personally, I don't think rake keys are a powerful tool. From what I have seen, cylinders rake-keyed open are easily picked, bumped, or impressioned. A high MACS in a lock with respectable tolerances defeats rake keys. A sufficiently large tryout key set should work on the same locks with the added benefit of surreptitious entry.

The main advantage of rake keys is the possibility they are confused with real keys and overlooked as evidence. The same is true of tryout keys, but those generally require an unusually large set of keys for all but the worst locks. Naturally, finding 30 or 50 keys at the crime scene or on a suspect is usually a red flag. Unfortunately, I have not had access to a set of working rake keys to test for forensic evidence. In theory they are surreptitious, but the premature tension and a strangely cut key may provide some form of evidence in the lock. More on this in the future!

6. Conclusion

FarmerFreak's creation is a shining example of the creativity of the locksport community. While the tool didn't evade forensics, it shows that non-traditional lockpicking tools exist, and many more are yet to be made. Many of these tools may leave forensic evidence, and understanding the unique tool marks of each is a priority for both investigators and forensic locksmiths.

What would be the security and insurance implications of a working, reliable anti-forensics picking tool? Given the overwhelming popularity of non-surreptitious techniques, the use of anti-forensics tools is not a major concern for most installations. As the value of the target rises, so does the usefulness of surreptitious and covert entry methods. At the level of major corporations, governments, and the military, the ability to surreptitiously defeat lock mechanisms is both a strong concern and a valuable weapon. In any case, a working anti-forensics picking tool would not be the end of the world. This is for a variety of reasons, but mostly because a new pick would not make lockpicking any easier to learn or perform in the field. Most anti-forensics tools do the exact opposite, in fact! Additionally, many investigations revolve around evidence unrelated to the lock; namely eyewitnesses, DNA evidence, and trace evidence (hair, fiber).

For the future, I'm working on creating and testing a variety of off-beat tool materials, such as ceramics and glass. Many locksport enthusiasts have contacted me with various ideas, and hopefully their projects will become the topic of future articles. Do you have any great ideas for a new lockpicking tool, or an anti-forensics lockpicking tool? Feel free to contact me if you'd like me to do forensics testing on it. Remember, no idea is too crazy, provided you can make a working, reliable tool that opens a lock.

Thanks for reading! I hope this article was interesting and useful to all who read it.

Credits, Thanks

A big thanks to FarmerFreak for taking the time to develop and test this tool, and for allowing me to examine it for forensic evidence. Many people were instrumental in helping prepare and review the article. In no particular order: Jon King (JK_the_Cjer), scorche, Doug Farre, Babak Javadi, Deviant Ollam, stderr, SCHUYLER Towne, Shane Lawson (valanx), mmca, Tom Ballard, Squelchtone, and GGTA.

References & Resources

Lockpicking Forensics – lockpickingforensics.com

The first and only website dedicated to forensic locksmithing. More articles on forensic locksmithing, anti-forensics, and locksport available on the Articles page. Be sure to visit the Links page for a list of related sites.

LockWiki – lockwiki.com

A collaborative online encyclopedia that focuses on locks, safes, and physical security. Feel free to help out and contribute! Lockwiki's Community Portal also lists many locksport groups and related sites that you might be interested in.

Lockpicking 101 – lockpicking101.com

The most popular lockpicking forum on the Internet. Useful if you want to get advice and information on a variety of locks and compromise methods, particularly lockpicking and key bumping.

Revision History

v1.00 – 01.17.10 – Initial release