Lockpicking Forensics

by datagram
www.lockpickingforensics.com
www.lockwiki.com

Black Hat USA Briefings, 2009
www.blackhat.com

If you've been to a computer security conference recently you've no doubt seen people learning how to pick locks and crack safes. In the United States, interest in physical security has become a natural extension of the growing number of people interested in computer security. Many computer security events now host some form of lockpicking event, or an area where people can learn about locks, safes, and methods to compromise them, commonly known as a lockpicking village.

At many of these events attendees focus on techniques to compromise locks and safes without discussing the forensic evidence they leave behind. Many instructors and speakers (the author included) portray many of these techniques in a manner that leads people to believe that they *cannot* be detected. In some cases this is true, but the vast majority of tools and techniques leave distinct forensic evidence.

This paper describes forensic locksmithing, the field of forensic investigation that relates to lock and keying systems. Included in this paper is normal wear and tear, evidence left behind by a variety of entry techniques, keying system analysis, and the investigative process.

This paper was written as a companion to my BlackHat USA Briefings 2009 talk and does not provide exhaustive coverage of the topic. A more thorough resource on forensic locksmithing (and contact information) is available at www.lockpickingforensics.com.

Destructive vs. Covert vs. Surreptitious Entry

Before we begin, we need to understand the difference between ways lock or keying systems are compromised. Methods of entry are generally classified as being destructive, covert, or surreptitious. Essentially, the distinction between them rests on the type of forensic evidence they leave behind. When we discuss whether or not methods of entry leave behind forensic evidence we restrict our view to lock-related evidence. It is quite possible that “forensic-proof” techniques leave behind evidence that is unrelated to the locking mechanisms, such as hair, fingerprints, or other trace evidence.

- Destructive entry techniques cause damage to or destruction of locks, safes, or surrounding components. Surrounding components are commonly doors, windows, and walls. Regular “users” of the locking system are capable of identifying destructive entry techniques.

- Covert entry techniques are non-destructive and do not leave obvious forensic evidence. They are not discovered by regular users, but *can be identified by a qualified forensic investigator*.

- Surreptitious entry techniques are non-destructive and do not leave any discernible forensic evidence. Surreptitious techniques are not discovered by regular users, and *qualified investigators may be unable to identify them*, depending on the technique.

In short, the difference between covert and surreptitious entry is the ability for a qualified forensic investigator to identify if a tool or technique was used. The paper will cover the most common types of covert and surreptitious entry techniques. Information on destructive techniques is available at http://www.lockpickingforensics.com.

Forensic Locksmithing

In 1976 a gentleman named Art Paholke (Chicago PD) decided to perform a variety of tests on locks and safes to determine whether or not various type of attacks against them left forensic evidence. He combined this with an analysis of how different levels of wear affected the evidence. Mr. Paholke's work was quite influential and his methods provide the basis for many of the techniques in use today. From his work the concept of forensic locksmithing developed.

In modern day, the forensic locksmith assists investigative agencies in criminal investigations, insurance claims, and security maintenance by providing the facts surrounding the compromise of a lock or key system. In this regard, the forensic locksmith identifies the method of entry, tools used, skill level of attacker(s), the relative security of the system, and evidence that may be used to identify suspects. The forensic locksmith does not solve cases for the investigative agency, rather they provide facts, evidence, and insight that may be used to affect the outcome of an investigation.

Don Shiles, former president of the International Association of Investigative Locksmiths, defines forensic locksmithing as:

> "T*he study and systematic examination of a lock or other security device or associated equipment using scientific methods to determine if and how the device was opened, neutralized, or bypassed. These examinations include the use of various types of forensic techniques, [...] and includes microscopic examination, micro photography, regular photography, physical disassembly of the device or devices, and on occasion laboratory techniques, such as metallurgy and tool mark identification may be conducted.*"

The forensic locksmith functions much like the traditional crime scene investigator but has extensive knowledge of the tools and techniques used to compromise lock and keying systems. With this knowledge the investigative agency can better understand and identify potential suspects. In addition to this, the forensic locksmith may be asked to provide testimony to explain their findings. In other cases, they provide independent testimony to explain or clarify compromise tools and techniques, lock and keying systems, and various related topics to a judge or jury.

Normal Wear

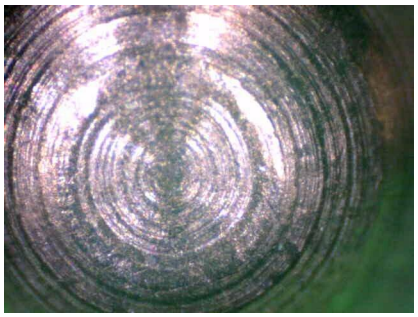
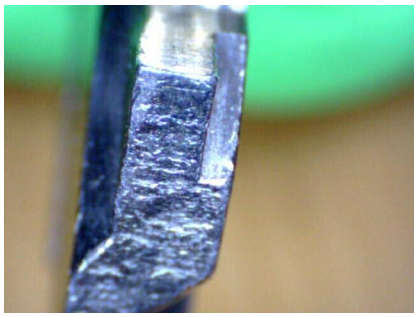
In order to identify compromise of a locking system it is important to know what the lock components and keys look like when they are used normally.

The amount and nature of the wear on components varies and is highly dependent on the lock, key, and component materials. The most common material for pin-tumbler locking cylinders, keys, and components is brass. Cylinders and components (pins, levers, wafers, etc) also commonly use nickel-silver and steel. Keys are made from a wide variety of materials besides brass, such as nickel-silver, aluminum, iron, steel, zamak, and various proprietary alloys.

The nature of wear also depends on the design of the key and the components. Unfortunately, I cannot display all possible combinations of designs and materials. The following is a microscopic examination of different stages of wear on a standard pin-tumbler cylinder (Falcon FA3, 6 chambers, pinned for 5). The cylinder, plug, pin-tumblers, and key are all made out of brass. Bottom pins in this cylinder have rounded tips. Prior to disassembly, the key to this cylinder was used no more than ten times. For the sake of space, I will only show 1-2 pins of each stage, rather than all 5.

Note: Photos are all taken with a digital microscope ranging from 10-200x magnification.

New

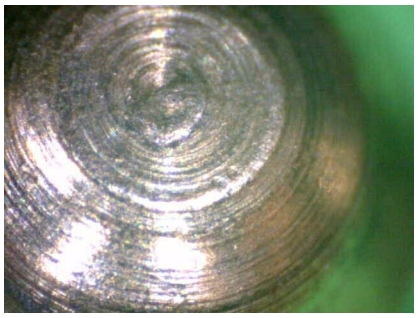
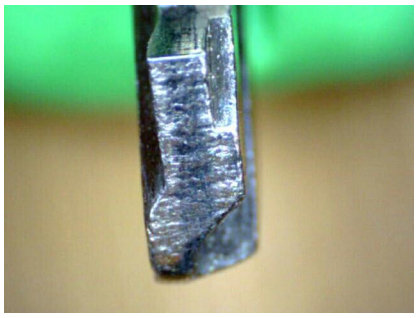




New pins are clean, with no dust, grease, or dirt. Light abrasions and corrosion may exist depending on how the pins were stored prior to being used in the lock. Factory original pins usually do not exhibit these characteristics. A clear indication that pin has not been used is the fresh milling marks around the tip of the pin.

Up close, we notice many small imperfections in the tip of the pin. Very light scratches, dents, and bumps are visible. The dents and bumps are natural imperfections in the manufacturing process, while the light scratches are likely from the use of a key.

The key for this lock is also new. It is factory original, made of brass, and has been cut with a high speed key machine. As stated above, it has been used a few times, and because of this we can see a light track in the center of the key where it has picked up lubricant from the pins.

250 Uses

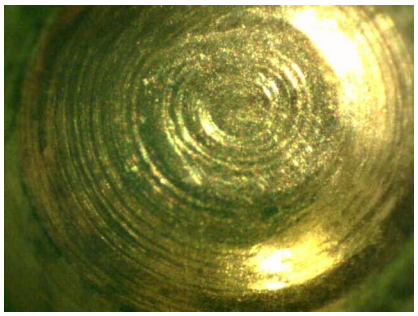
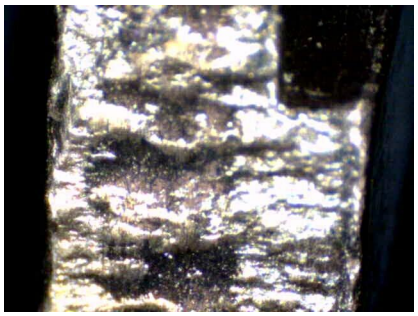




After 250 uses (roughly 3-6 months of use) a ring develops around the pin. This is the key gliding under the pins, spread around the tip because insertion and removal lightly rotates them back and forth. The key is also lightly polishing the pins, too.

Up close we can see that the ring is actually due to the milling marks starting to be removed and lightly polished. The pin has also been slightly distorted in the very center, also due to the key making contact with it.

The key has also started to show signs of wear, mostly in the center where the pins have been touching it. In this particular case, wear resembles a staircase pattern. In addition, the key has picked up more lubricant, making the line on the key considerably darker.

1,500 Uses

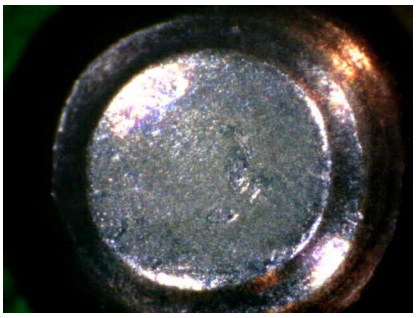
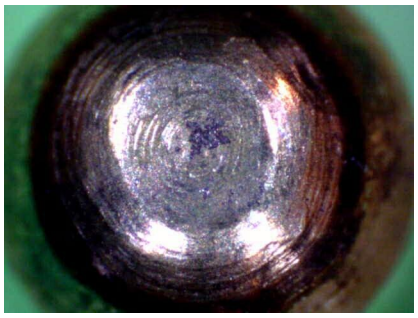
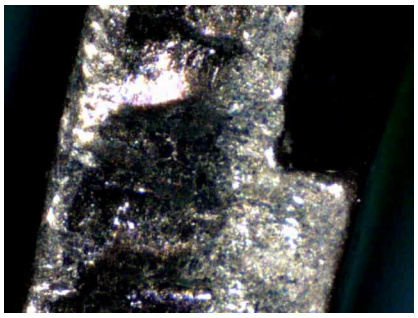




At 1,500 uses (roughly 1.5-2 years of use) a distinct change in the appears of the pins. The key has been used so many times that the milling marks have almost completely been removed. Again, slight scratches on the pin are being caused by the key becoming more jagged as it too wears down.

What is most interesting is that pin 5 (the furthest back) has considerably less wear, and more visible scratches. This all makes sense; it is only touched by the tip of the key, and the tip of the key is the most worn down because it makes contact with all of the pins.

The key continues to wear and collect lubricant. Image shown at high zoom to show the literal pits that are being created. At this point, certain ramps on the key may be acting like a file when going in and out of the lock. As seen above, this translates to more light scratches on the tips of the pins.

5,000 Uses

At 5,000 uses (roughly 5-6 years of use) the front pin (left) has no milling marks, and almost all scratches have been polished away. From this point on wear looks similar to this, with light markings sometimes being created by wear of the key.

Compared to other pins, pin 5 (center) continues to show reduced signs of wear and retain its milling marks. We can also now see that wear is not evenly distributed on this pin, as it resembles an oval shape. Compare with above picture and 1,500 use pictures.

They key (right) continues to wear down, with small craters from the previous example now very large and uneven. Slight imperfections like this in the key will cause light, seemingly random scratching on the soft brass on the pins. Stronger key materials may even act as a file against pins.


The face of a lock that has seen moderate to heavy use will have many dents and imperfections caused by normal use. How many times have you went to unlock a door and slightly missed the keyway? In the photo (left), many small dents and scratches from normal use are visible.

In shoulder stopped locks (almost all pin-tumbler locks qualify), continued use will cause light impact marks along the face of the plug (right). This is normal, and should not be confused with the extreme material displacement that occurs during key bumping.

Lockpicking

Lockpicking is a general term for a wide variety of covert entry techniques, all of which attack the locking components directly. Unlike impressioning or decoding, lockpicking attempts to open the lock without producing a working key or decoding the correct position of components. There are many different lockpicking tools for various lock types.

In almost all cases of lockpicking two tools are used. A tension tool is used to gently apply tension to the lock, and a pick is used to position components. As tension is applied to the plug, bolt, or other component, locking components will bind in some way. The pick can be used to determine which component is binding and then used to position it properly. The correct position of a component is known by the attacker through feedback in the form of touch, sound, or sight. The tension tool holds properly positioned components in place, and the attacker repeats the process. Once all components are properly positioned the lock can be unlocked or locked.

The nature of lockpicking necessitates that strong materials be used for tension and picking tools. Tools are commonly made out of steel, iron, and aluminum. Tools are thin (on average 0.025" with pin-tumbler picks) and require a medium amount of force to move locking components. When contacting the softer brass or nickel-silver of locking components, pick and tension tools leave marks in the form of gouges and scratches. The best source of forensic evidence of lockpicking are on the components themselves, but the lock housing, bolt, and cam may also be examined, depending on the type of lock.

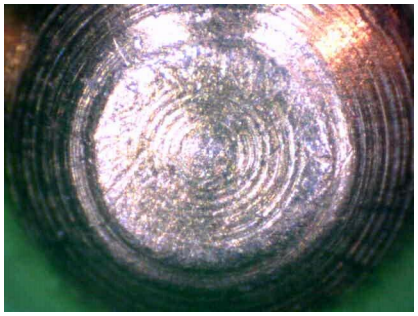
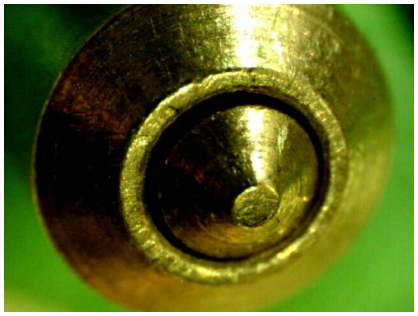
Forensic Evidence



The act of using a pick tool is invasive, and we expect the stronger material of the pick tool to cause marks on the softer brass or nickel-silver of the lock components. In the photo (left), we see scratches where the pick tool was used to lift the pin. These appear to be single-pin picking marks due to their shape, size, and position.

This photo (center) is similar to the last, but instead there are many varied, elongated scratches at different angles and depths on the pin. This type of marking is indicative of a pick that is designed to be gently rubbed against the pins at varying height and tension. Of course, this is the technique known as raking or rake picking.

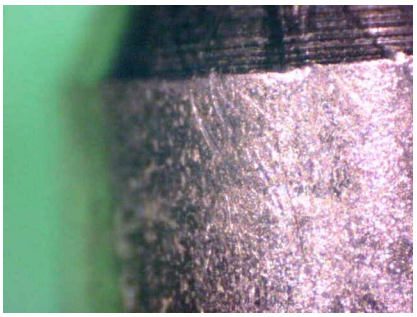
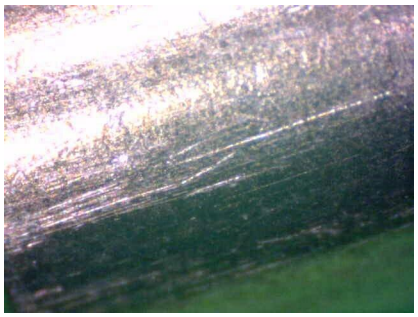
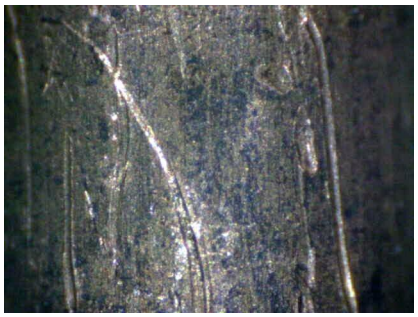
In this photo (right), marks left appear to be a combination of both picking techniques. Many attackers will attempt to lightly rake as many pins as possible and then proceed to use single-pin picking against the rest. This may be necessary in the case of security pins that are triggered while raking, also.

The marks left by an attacker are in many ways indicative of their skill level. In this photo (left), deep and plentiful pick marks are shown. The attacker, an amateur, used extreme force on both tension and pick tools. The extreme tension causes pins to bind against plug and require more force to be lifted.

In this photo (center), pick marks are extremely light but still visible in the center of the pin. We can also see some marks on the side of the pin which are more defined. This is a very skilled attacker who uses extremely light tension and picking force to reduce forensic evidence. Despite much higher picking skill, we still find similar forensic evidence.

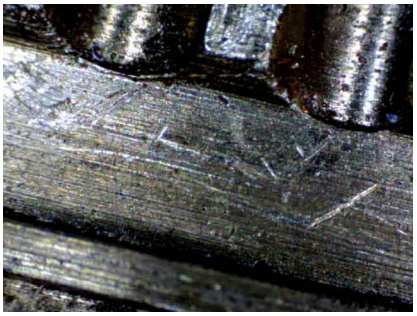
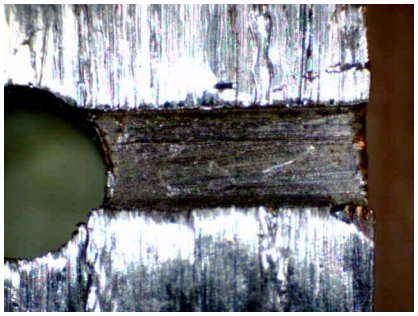
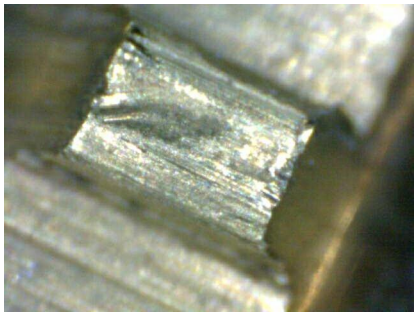
In other cases, marks may be light due to stronger materials being used for components. In this photo (right), nickel silver pins from a Mul-T-Lock telescoping pin-tumbler are used. Marks are present, but much lighter than in our normal examples.

For the attacker, it is difficult to not touch the sides of pins. This can happen during raking as well as single-pin picking. Marks left on the sides of pins are quite noticeable and not as prone to wear and those in the center of the pin. In the photo (left), light scratches at varied angles are visible.

In the case of low-high pinning combinations it is even harder to lift pins without touching other pins. In this photo (center), several long scratches travel up the side of the pin. Interestingly, we may be able to measure the length of scratches to determine if the attacker raised the adjacent pin high enough.

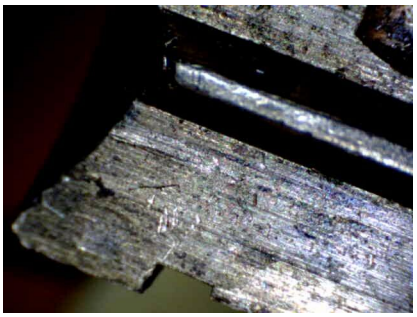
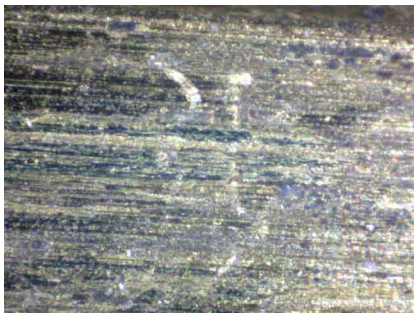
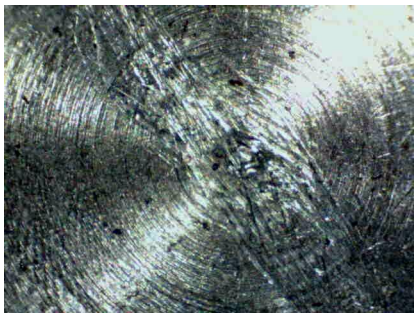
Like the bottoms of the pins, the sides can tell a great deal about the skill level of the attacker. In this photo (right), gouges on the sides of the keys are rather deep, caused by extreme force being used on both the tension and picking tools. With this much material removed, it may be possible to identify pin material on a suspect's possessions.

Inside the plug we also expect to find various forensic evidence. In this photo (left), the plug walls have scratches are various angles that are inconsistent with the use of a key.

The top of the keyway is a great area for forensic evidence because a properly cut key will never touch here. Of course, pin-tumblers never touch here either, as this are is between pin chambers. For these reasons we consider this a “virgin” area where any tool marks found are indicative of something suspicious. In this photo (center), light scratching on the top of the keyway is visible.

Marks can also be found higher on the plug walls, near the pin chambers and internal warding. In this photo (right), a large mark is found on an internal ward (between pin chambers). From the shape, angle, and size of the mark we can rule out a key as the culprit. If a key did do this, it would likely be present on other wards inside the lock, too.

Tensions tools used in lockpicking also leave identifiable forensic evidence. When we take the plug apart, we can usually find light scratching and scuffing at the front of the keyway. Marks can be at the top or the bottom of the plug, depending on the tension preferences of the attacker, and how clear they are may help us determine their skill level. In the photo (left), light scratching and a definitive tension tool mark (the line) are visible.

Light tension is preferred when pick locks with security pins or other high security features. Often only a feather touch is needed to pick a lock, though excessive tension is a beginner mistake. In this photo (center) light scratches are visible, as well as the final resting position of the tool (the clearest mark). The light scratches are usually caused by having to fiddle with the tension tool to get it seated properly.

In addition to the pins and plug we can look at the cam of the lock. While evidence on the cam is not always available, it does help indicate the skill level of an attacker. At many locksport events the cams are removed and you'll notice people with the pick sticking out the back of the lock. When mounted, they are hitting the cam instead, creating a good deal of forensic evidence. In this photo (right), excessive scratching on the cam indicates a low-skill attacker.

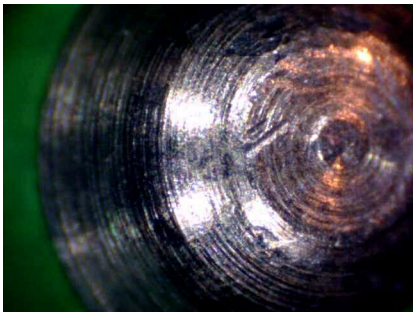
Pick Guns

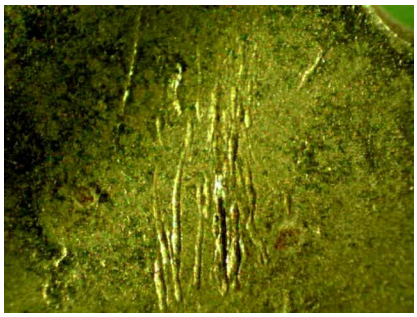
Pick guns are a covert entry tool used to pick pin-tumbler based locks. Pick guns have manual and electric variants, each with their own type of forensic evidence. Both work to rapidly separate pin pairs at the shear-line to allow the plug to rotate. Pick guns are similar in function to bump keys.

Manual pick guns are spring-loaded tools that resemble a toy gun with a lockpick attached to the front. The lockpick is interchangeable, and referred to as the "needle." To open the lock, the needle is inserted in the lock and placed under all pin stacks. As with lockpicking, a separate tension tool is used to apply tension and rotate the plug. Light tension is applied to the tension tool and the trigger of the pick gun is fired. According to physics, the kinetic energy transfers from bottom pin to top pin, causing the top pins to "jump" in their chambers. If all top pins jump above the shear-line at the same time, the plug can be rotated to unlock the lock.

Electric and vibrational pick guns work on a similar principle, but instead oscillate the needle back and forth, causing it to vibrate. The tool is controlled to get the resonating frequency of the needle at the right point so that top pins jump above the shear-line. In the case of vibrational or electric pick guns, we will see considerably more evidence on the plug walls because the device is constantly moving.

Forensic Evidence





The striking of the pick gun needle against the bottom pins causes very clear forensic evidence. Unlike picking, which causes scratches, the pick gun causes impact marks that, when done many times, begin to resemble the spokes of a bicycle along the circumference of the pin. In this photo (left), several impact marks are visible.

The marks left by a pick gun are so distinct, compared to the rest of the pin, that is is often possible to count them to determine how many times the pick gun was triggered. Each time the needle strikes, the bottom pins may rotate slightly, allowing marks to be separate and distinct. In this photo (center), a multitude of impact marks along the tip of the pin are visible.

As with lockpicking, the cam of the lock may have marks on it if the needle of the pick gun is inserted too far. Just like the impact marks on the tips of the pins, we can usually count how many times the pick gun was used if it touched the game. In this photo (right), many marks are visible on the cam caused by repeated use of a pick gun. It is likely that cam material will linked to and found on the pick gun, if it is ever recovered.

Key Bumping

Key bumping is a covert entry technique against pin-tumbler locks that uses a specially prepared key to "bump" top pins above the shear-line. There are two types of key bumping, pull-out and minimal movement, but both produce similar forensic evidence on the bump key and the lock.

To bump a lock, a key is acquired that fits the keyway of the lock. The key is modified so that all cuts are at their lowest depths or lower. If done by hand, a key gauge or micrometer can be used to measure the key and ensure cuts are deep enough. If done with a key machine, the key may be duplicated from a working bump key, or cut by code to the lowest depths.

In the pull-out method, the key is inserted into the lock fully then withdrawn one pin space. In the minimal movement method, the key is further modified by removing material from the tip and shoulder of the key. The minimal-movement key is inserted completely into the lock. In both cases, light tension is applied to the key and a tool (known as a bump hammer) is used to impact the bow of the key, causing the key to be forced into the lock. The impact on the key causes kinetic energy to travel from the key to the top pins, causing the top pins to momentarily jump. If all top pins jump above the shear-line while tension is applied the plug is free to rotate.

Forensic Evidence

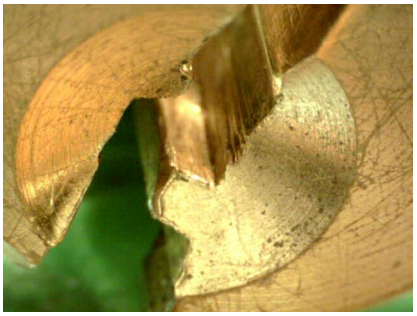


The act of key bumping basically slams the key against the bottom pins to allow for kinetic energy to be transferred from the key to the top pins. Because they are immobile and absorb the kinetic energy, this causes considerable damage to the bottom pins in the form of large dents. In the photo (left), a large dent is visible on the pin, inconsistent with normal wear (and lockpicking or pick guns, for that matter).

A bump key that is cut by hand, with a low speed key cutter, or made of a considerably stronger material (steel, iron, nickel-silver) than the pins may act as a file as it impacts bottom pins. In this photo, light scratches can be seen traveling through the bumping dent. It is possible that marks are distinguishable enough and can be linked to a specific bump key, though this is rare.

Bumping is rarely 100% successful, either because bottom pins are bumped above shear line, or top pins are not bumped high enough. When this happens the tension applied will misfire, causing one or more top pins to bind. This causes light shearing against the bottom of the top pins, visible in this photo (right).





The pin chambers within the plug may also be damaged by bumping. When kinetic energy does not properly transfer to the top pin, the pin stack may instead press against the chamber walls (caused by the movement of the bump key). Repeated bumping may cause these areas to distort, stretching in various directions. In the photo (left), the pin chamber is stressed is distorted in many directions, but mostly to the top left.

One of the most noticeable pieces of evidence from key bumping is damage to the face of the lock. This is caused by the shoulder of the key impacting the area above and below the keyway. The use of modified shoulders may prevent this from happening, commonly done with a glue gun stick (and referred to as a glue gun shoulder). In the photo (center), a large dent above the keyway is present, inconsistent with normal wear.

In the minimal-movement method, material is removed from the tip and shoulder. This makes the method work but also inserts the key far enough that in some cases affects the keyway. This is due to the key material getting thicker as it reaches the bow. In the photo (right), this distortion can be seen around the edges of the keyway.

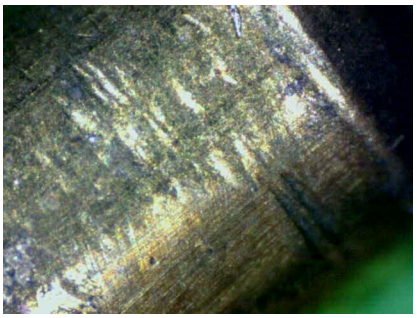
Impressioning

Impressioning is a covert entry technique that creates a working key for a target lock. Impressioning has two variants: copying, which focuses on making a mold of a working key; manipulation, which focuses on using a blank key to manipulate lock components to determine their proper positions. This page will focus on manipulation-based impressioning.

Manipulation-based impressioning works by taking a blank key that fits a target lock, applying extreme torque to the key (thus binding components), and manipulating the key blank in order to produce marks on the key. This is correct for pin-tumbler locks, but the actual process varies for different lock designs. The theory behind impressioning is that components at the wrong position will bind and become immobile. When the soft brass key contacts the immobile components, a mark should be produced. When a component is properly positioned it should no longer bind and thus no longer leave marks. The blank is used to gather marks, then filed in those positions. This is repeated until all components are in their proper position and the lock opens.

There are variations on the manipulation process that use pressure responsive materials, such as lead, tape, or plastic to facilitate the process of impressioning. In these cases we may also find material transfer as the soft materials rub against the keyway and inside of the plug.

Forensic Evidence

Because we are forcibly binding bottom pins at or above the shear line we expect to see marks on the pins where this occurred. In the photo (left) we can see several marks where the pin was bound against the plug in the form of straight lines sheared into the pin. (Note: the scratches to the left are pick marks)

Sometimes, impressioning marks are so clear that we can count the rounds of impressioning (right). If marks are far apart the forensic locksmith can also measure the distance between them. This may indicate a more skilled attacker if they are using factory depth increments to speed up the impressioning process.


The key blank may be specially prepared for impressioning via manipulation in a variety of ways. One of the possibilities is the use of Ultraviolet ink and an ultraviolet light source. This is an interesting technique, but as you can see in the photo (left) it leaves ultraviolet ink residue on the face and insides of the lock.

When using UV impressioning, UV ink is reapplied each time the blank is filed. In turn, the pins will have a large amount of UV reside on them. Notice the obvious key pattern of UV ink across the sides of the pin (right). In addition, the UV pen fibers may have been stuck to the key and left behind on the pins or the plug walls.

Decoding

Decoding is a general term for a class of covert and surreptitious entry methods, all of which have the expressed purpose of decoding the proper position of components in a lock through an examination of the key or internal components. Decoding is probably the most ambiguous of all the compromise methods, with a wide variety of tools and techniques used.

Decoding does not necessarily create a key for the lock, like impressioning would, nor does it always open the lock, as is the case with lockpicking. The power of decoding is the ability to gather information

that allows the production of working keys for the lock. Decoding is also powerful because many forms are surreptitious, thus leave no discernible forensic evidence.

Keys can be directly examined and decoded. Key decoding focuses on identifying the pattern of bitting cuts on the key. These can be determined by looking at the code numbers stamped on the key, or through direct measurement of each cut with a ruler, micrometer, or caliper. These measurements are used to determine the manufacturer's bitting code so that a key may be easily made. Sophisticated locksmithing tools are available that will automatically identify the bitting code based on the cuts and keyway profile of the key. This is the most basic of decoding methods, and may be problematic with high-security keys that have advanced features like sidebars, angled bitting cuts, moving parts, or magnetic/electronic components.

Components inside the lock can also be decoded through invasive, manipulative tools. These tools have radically different designs, and are generally specific to particular brand or model of lock. Most manipulative tools focus on measuring each component to determine: weight, range of movement, shape, spacing, and alignment. Many manipulative decoding tools resemble traditional lockpicking tools with the addition of a measurement device. Opening the lock via lockpicking is sometimes a pre-requisite to decoding the components. Many tools also decode the lock as they pick it. The standard tubular lockpick and the Sputnik tool are the most popular examples. Manipulation of combination locks requires no invasive tools and is discussed more thoroughly in the Anti-Forensics section.

Disassembly of the lock can also be done to directly measure all internal components. This can be a complicated procedure depending on what type of lock it is and how it is installed. This process usually requires the lock be compromised first so that the door can be opened. Facilities with lax security measures may leave doors unlocked and unguarded, allowing someone to quickly remove, disassemble, and decode a lock. Reassembly and re-installation of the lock is equally important, and if done incorrectly can cause the lock or proper key to no longer function. In the photo, a hotel safe lock has been (almost) completely disassembled. Consider the implications if the safes in the hotel were master keyed, or keyed with a predictable pattern.

Visual/optical decoding focuses on observation or surveillance of the key or internal components without needing to invasively manipulate them. A photograph of a standard key's bitting is enough to decode the bitting code. Surveillance may be used against combination locks to observe the correct combination being entered by an authorized user. Optical decoding uses tools like borescopes or otoscopes to look inside the lock at the internal components. Optics can be used to look at the size, shape, color, alignment, and spacing of internal components. In the photo (right), pin-tumblers can be decoded because they are color-coded to make self-rekeying easier.

Radiological imaging is a form of surreptitious decoding that uses penetrating radiation (X, beta, and gamma rays) to "see" inside the lock or safe, revealing the proper positions of components. This is most often used against rotary combination locks to determine the position of each gate in the wheel pack. While very effective against many combination locks, it is expensive and only used by medium-high skill attackers.

Thermal imaging is another form of surreptitious decoding that uses special devices to look at thermal residue left on keypad or pushbutton combination locks. This reveals buttons recently pushed, but may

not directly reveal the combination sequence. Like radiological imaging, this is generally not used by low skill attackers.

As you can see, decoding is a vast array of techniques with forensic evidence equally varied. Manipulation-based decoding tools provide forensic evidence that is similar to lockpicking, but may vary depending on the specific techniques. Examination of keys may leave forensic evidence depending on the type of tools used. Visual, optical, radiological, and thermal decoding are all considered surreptitious and leave no lock related forensic evidence.

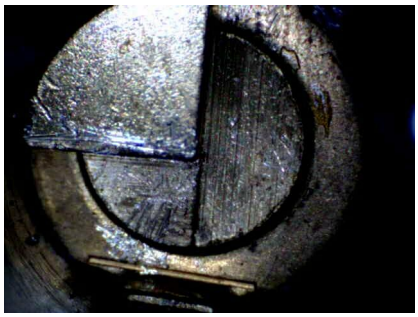
Bypass

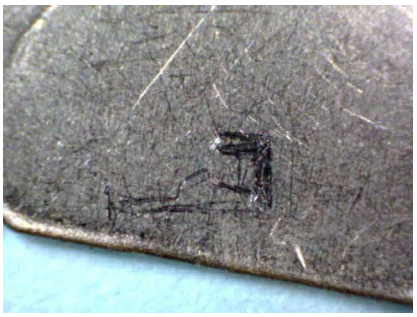
Bypass is a form of covert entry that attempts to circumvent the security of the lock by attacking the cam, bolt, or locking knobs directly. While lockpicking focuses on defeating the security of the lock through manipulation of components, bypass goes directly to retracting the bolt without affecting the integrity of the components. Certain bypass techniques are also forms of destructive entry, but bypass generally refers to non-destructive methods.

Attacks against the cam or actuator are a class of bypass that is surprisingly effective. In this attack, a poorly designed cam or actuator may be manipulated without affecting components. This vulnerability is somewhat uncommon, but extremely effective and easy to do when present. Because tools must generate a mild amount of torque as well as travel through the plug, they leave distinct tool marks.

Spring loaded bolts or latches are subject to an attack known as shimming. In shimming, a wedge is used to separate the bolt from the spring, or the bolt from the recess (such as in a door). The classic credit card trick to open doors is a popular example of this technique. Low-security padlocks are also commonly susceptible to shimming of the shackle. Shimming against doors is also known as loiding.

Forensic Evidence





Cam manipulation is one of the most common bypass methods. The American 700 (old models) suffer from this vulnerability. Essentially, the cylinder is not required to move in order to actuate the cam. In the photo (left), tool marks left on the cam and back plate indicate that bypass was used as the method of entry.

In response to the above attack American Lock issued a hardware patch to prevent the bypass method. It is just a small metal disc, and in the photo (right) we can see tool marks from where bypass was attempted. The 700 has since been redesigned because another attack against this component makes bypass again possible.

Key Analysis

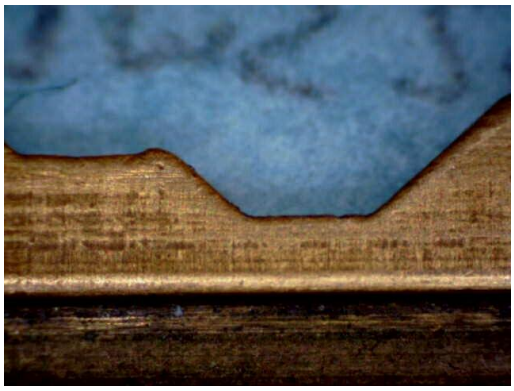
While investigation of locks is important, it is more common that the keying system has been compromised. Much like the cryptography world, systems are not usually broken by some awe-inspiring flaw but instead by the simple act of obtaining the proper keys. The keys to a specific lock can yield just as much information as the lock itself, sometimes more so because of the possibility of hair, fiber, and fingerprint transfer when handling keys. While examination of locks is excellent for determining the method of entry, examination of keys is doubly excellent for the identification of suspects.

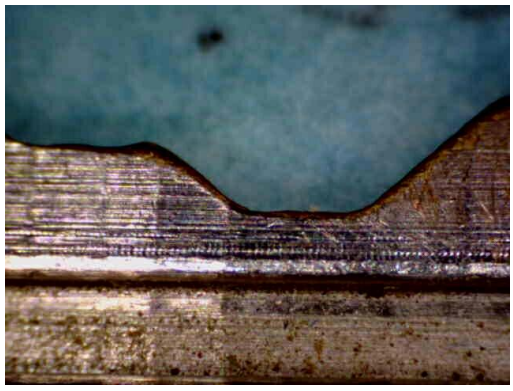
When the forensic locksmith receives a key, they examine it in a variety of ways to determine its characteristics, place of original, history, and any evidence that may help to determine how it has been used. The cuts, keyway, and codes on a key are always examined for information.

Many keys have codes that identify cuts and keyway. Bitting codes may be direct (literal) or indirect (obfuscated). In the case of indirect codes, the manufacturer may be able to determine to whom and where the key belongs. Other information may also be stamped on the key, such as the name of lock brand, key brand, or the locksmith/hardware store that produced the key. All of which may be used to identify a suspect.

The material of a key is also important to many forensic investigations. The material of a key can identify factory original keys, and in some cases specific third-party manufacturers. Certain manufacturers use proprietary alloys to increase longevity and strength of their keys, some of which can be traced back to them. The plating on a key also provides some clues. Manufacturers usually plate factory-original keys *after* they are cut, while locksmiths and hardware stores will remove the plating of a blank key when making cuts. The plating material may also be used to identify the key blank manufacturer.

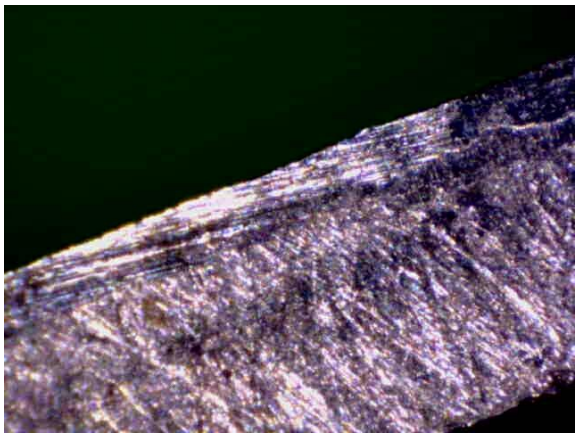
Key Duplication

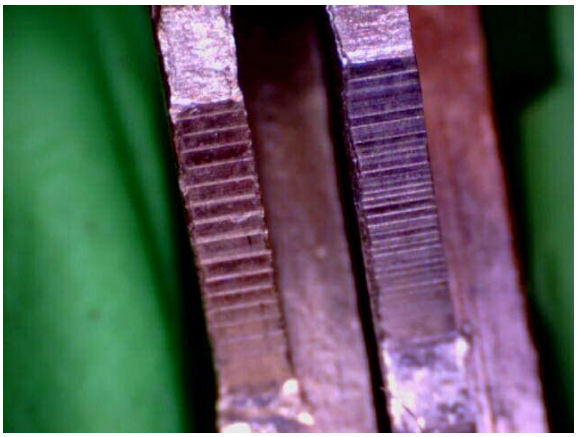




Keys can be duplicated in many ways, but the most common is duplication by hand or with a key machine. Identifying an original vs. duplicate key is an important function of the forensic locksmith. In addition, the forensic locksmith may be able to determine if the key was recently duplicated. Which of these two photos shows the original key, and which is the duplicate. Why?

In this photo (right), the duplicate key is shown. Notice that the ramps and valleys of the key are slightly different than the previous photo. In addition, we see that the key is nickel-silver plated, with no plating on the cuts. Depending on the factory-original specifics, this may also indicate that it is a duplicate key.

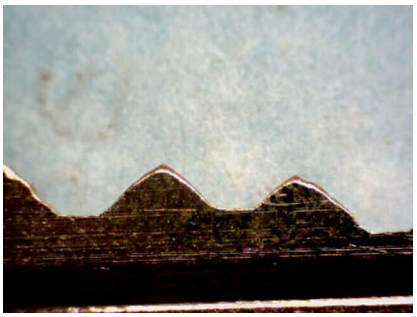


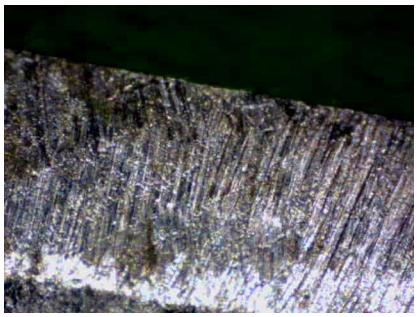


When a key is duplicated with a stylus-based key machine a mark is left on the side of the original key (left). This is due to the stylus being gently dragged against the key, and resembles a long, straight, polished line. This cannot be confused with wear of the key because it is not in the direct center of the key.

Keys can be examined to determine the speed and blade design of the key machine was used to cut them. This photo (right) shows a comparison of two keys, with the one of the left being cut with a lower speed key cutter. If a key machine is found with a suspect, it can be examined to determine if it was used to cut a specific key.

Handmade Keys



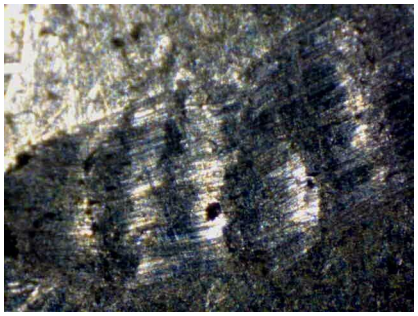


Possession of keys that are made by hand are, in a general sense, somewhat suspicious. In most cases hand made keys are easily identified by measuring the ramp angles, shoulder to first cut distance, and the distance between cuts. Hand-made keys generally have imperfect, jagged ramp angles and poorly spaced cuts.

In this photo (center) we see many groups of scratches, with slightly different angles, across the bitting of the key. This is consistent with the use of a file. Specifically, this is a flat file being used on the broad side. With a tool mark comparison we can determine the size, shape, and grade of the file(s) used.

In this photo (right) we see a series of cuts with variable depth valleys and light material removal around the edges. This is consistent with use of a dremel. Again, tool mark comparison can determine exactly which dremel bit(s) may have been used. These can be linked with tools found in a suspects possessions.

Tool Mark Identification

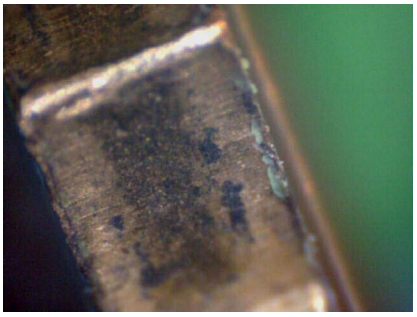
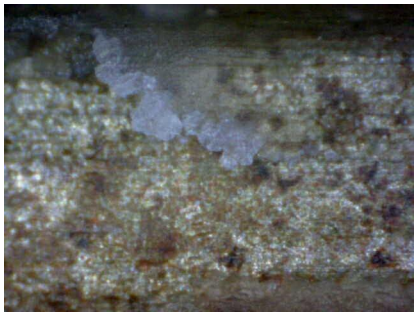
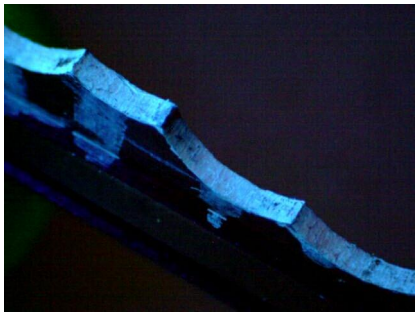



Sometimes marks will be left on the key as a result of normal or malicious use. When a key is duplicated with a cutter, the clamp to hold the original or the blank may leave a mark. In addition, some covert entry techniques may leave tool marks. In this photo (left) we see a set of rather deep marks on the bow.

Close up (center) we see a distinct pattern on the largest tool mark. We can hypothesize what made this, and perform a tool mark comparison to confirm. This particular mark was made by a pair of vice grips being used to impression (via manipulation) a blank key. The key should also be examined for impressioning marks.

In many covert entry techniques a key is used as a tool to affect entry. Keys with unusual marks or deformations can provide clues as to their use or intended purpose. In this photo (right), the shoulder of the key is deformed and compressed. This happens to be a bump key's shoulder, caused by impact against the face of the lock.

Material Transfer

Various materials are transferred to the key during use. Generally hair, fiber, and fingerprints will be examined by a crime lab. The forensic locksmith, however, may examine the findings of the crime lab to identify the uses of materials found on keys. In this photo (left) we see a light green residue, which happens to be modeling clay.

In this photo (center) we find small traces of white wax left in the warding of the key. Both this and the previous image indicate that the key has been impressioned (via copying). Through further analysis we may be able to link these and other materials to those found in a suspects possessions.

Keys should also be viewed under various light sources to fight material residue that may not be visible with the naked eye. In this photo (right), a key is being viewed under ultraviolet light to discover traces of ultraviolet ink along the key bitting area, indicative of impressioning via manipulation.

Anti-Forensics & Surreptitious Entry

Forensics is a never ending cat and mouse game. Investigators look for better methods to determine what happened while attackers are look for better ways to cover their tracks. So called 'anti-forensics' are various techniques and methods to conceal evidence of entry.

In many cases the forensic locksmith is asked to provide an assessment of how plausible certain surreptitious entry techniques are against a given lock. This can be done through a series of laboratory tests, an analysis of the required skills, tools, or money required, and examination of the installation and configuration details of the lock. Cases of completely surreptitious entry are viewed by the investigators on the basis of what facts and logical conclusions present themselves.

The idea of anti-forensics materials in tools is a popular but not well researched (publicly) area. Lock picks made of soft materials such as wood or plastic would, in theory, not leave any marks on the considerably stronger brass, nickel-silver, or steel components. While they sound great in theory, they are considerably harder to use in practice. Tools made of these materials are considerably weaker, less maneuverable, and more prone to fracture or breakage than the steel normally used in tools. These types of tools also exhibit drastically reduced feedback capabilities, important in many covert entry techniques, when compared to metal. Coating standard tools with other materials has also been attempted, with limited success. The best example is Teflon coated lock picks, which do not leave traditional marks, but still leave marks.

Investigative Process

Investigations are broken down into several steps: crime scene investigation, laboratory examinations, investigative reports, and expert testimony. Some investigations may not require all steps; evidence may be mailed to you, testimony may not be required, and so on.

The goal of the investigation should be clearly defined from the start. Many investigations will not require that you exhaust all possibilities, but instead give you a clear, direct goal. For example, identifying if a key could have been used to open a lock, if the lock has any pick marks, or if a key machine was used to make a specific key. All of this depends on who the forensic locksmith is working for; insurance companies only need facts relating to their liability, but criminal investigations will be looking for as much information as possible.

A thorough treatment of the investigative process as it relates to forensic locksmithing is available on the Forensic Investigation page of Lockpicking Forensics.

Resources

Unfortunately, few free and readily accessible resources are available for forensic locksmithing. LockpickingForensics.com and LockWiki.com are they only sites that deal with the topic in-depth. There are at least three books that deal with the subject, but more often than not it is combined with generic forensic investigation or tool mark identification literature.

Currently, the best English book on the subject is Locks, Safes, and Security by Marc Weber Tobias. Chapters 24-27 deal extensively with forensic investigations of locks and keys. If you can afford it, it is highly recommended. The forensic section can be purchased individually, but I would recommend buying the full book instead. I would also recommend buying the multimedia edition of the book rather than the

print version. The multimedia edition comes with a wealth of audio and video recordings that deal with forensic locksmithing.

If you can read German, then Manfred Göth's book Werkzeugspur ("Tool Traces") is available. I do not read German, but I am told this book is excellent. Manfred Göth also authored the chapter on forensics in Oliver Diederichsen's book Impressionstechnik ("Impressioning"). This book is available in both English and German.

The International Association of Investigative Locksmiths (IAIL) provides licensing and certification for forensic/investigative locksmiths. More information is available on their website.

There have been many articles published in locksmith and safe technician magazines over the past few decades. Most, if not all, are unavailable in digital form and cannot be re-published due to copyright laws. A few are included in the digital version of Locks, Safes, and Security, mentioned above.

If you are interested in general locksmithing or locksport resources, visit the Links page on Lockpicking Forensics or the Community Portal on Lockwiki.

About the Author

My name is datagram and I run LockpickingForensics.com and LockWiki.com. Information on future events including lectures, workshops, and lockpicking villages can be found on the Events page. Feel free to contact me with any questions, comments, or criticisms about this paper or the website(s).

This paper is one of many forensic locksmithing and locksport articles on LockpickingForensics.com.