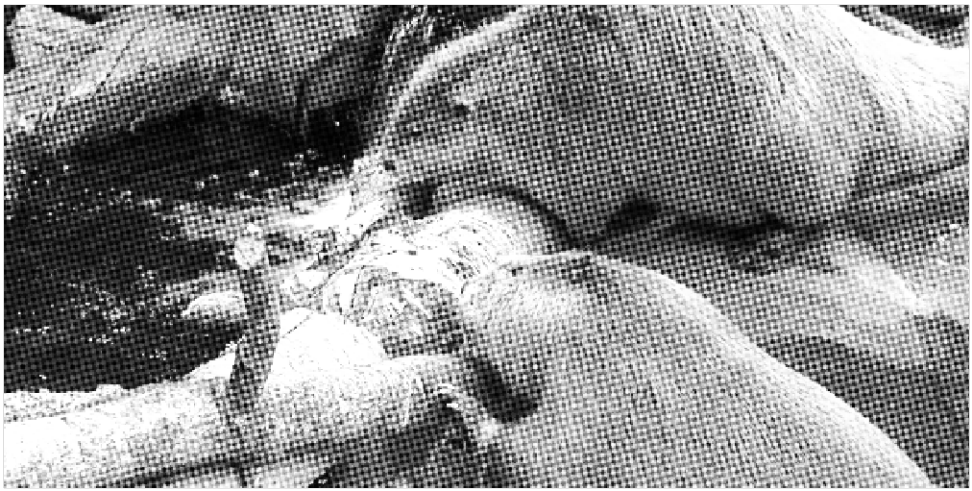
How To Get Things Burning

(Security Chapters)



How To Get Things Burning (Security Chapters)

Original text in German
Unknown title

English translation
How To Get Things Burning
2025
warriorup.noblogs.org/post/2025/09/28/how-to-get-things-burning

New edition
No Trace Project

Layout
No Trace Project
notrace.how/resources/#things-burning

Note from the No Trace Project:

This document includes the first three chapters of *How To Get Things Burning* and omits the last two, which were outside the scope of our project.

This brochure is intended for militants on the radical left who want to embark on a new or renewed path of persistently putting into question the overwhelming "lack of alternative" to the political shift to the right. The space for (emancipatory) movement has noticeably narrowed, and the methods of enforcing this narrowness have become more diverse, ranging from blatantly repressive to subtly manipulative.

This brochure is not a replacement for PRISMA,[1] which is now ten years old, because we essentially only focus on constructing time-delayed incendiary devices. And yet, this brochure attempts to do much more: presenting working methods that make clandestine militant action conceivable and feasible even beyond arson, despite the ever-expanding capabilities and powers of the investigating authorities.

The first part of the brochure therefore focuses on the traces that can lead to identification and how, so that we can avoid or at least minimize them. In particular, we devote more space to the topics of DNA traces, scent traces (mantrailing), and data traces, because many changes are forcing us to adapt our working methods.

Some may initially be shocked by the amount of work these adjustments entail and long for the days when they could "spontaneously" set off with the same balaclava and their tried and true leather gloves. We long for those times too, but wishing for them won't make them happen. We must fight for this room to maneuver, which likely involves militant action.

So, get to work on the unpleasant engagement of learning about the enemy and then head out into the night. A politically incisive and heart-warming bonfire—without a guaranteed ticket to jail—will make up for it.

Know your enemy and fight back!

[1] https://notrace.how/resources/#prisma

Contents

Avoiding Traces

This extensive chapter describes different types of evidence that police investigators use to get an idea of who may have committed an unsolved crime.

We do not discuss cell phones because such devices have no place in the preparation of direct actions. So leave that shit at home when doing reconnaissance, when shopping, during the action of course, when disposing of things, when publishing a claim afterwards—for anything that has something to do with the action.

The police's options for analyzing evidence lead us, in turn, to provide recommendations on how we can avoid or at least minimize certain types of evidence.

To avoid boring you, we'll start with the three most difficult types of traces: scent traces, DNA, and data traces. Then, things get a little more conventional: fingerprints, footprints, vehicle traces, tool traces, fire traces, material traces, and cameras. Last but not least, we look at how language characteristics are a highly underestimated yet unfortunately rich source of evidence.

Mantrailing

There have been many rumors about mantrailing dogs and their abilities for years, yet most militants still ignore the danger of being tracked down by such a search dog after an action. We will therefore briefly describe what these dogs can potentially do, how cops work with them, and the challenges they run into. In this text, we will only provide a few specific tips on how to thwart sniffer dogs because otherwise we would reveal too much to the authorities about how we mitigate mantrailing. However, if

you know how they work, it's not difficult to think up a few obstacles for the doggies yourself.

What is mantrailing?

In mantrailing, a dog doesn't follow footprints; it follows a trail consisting solely of the scent particles of the person it's looking for. For example, if you are riding a bike, the mantrailer can still find your scent even though you have never set foot on the ground. The dog knows which scent to look for because it is shown a so-called "scent object" prior to setting off. This object contains the scent particles of the person being searched for, so the dog can pick up the scent.

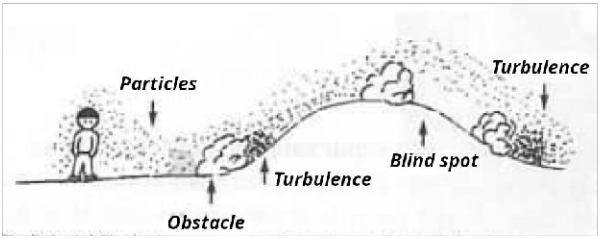
A skilled mantrailer can follow this scent particle trail over long distances, even if it is several days old. Ten-day-old tracks are no problem. Some dogs can even follow tracks that are 30 days old. A few years ago, mantrailers were primarily used to search for missing retirement home residents or murder victims. Today, many more such dogs exist in Germany, and the police also use them to find escape routes and perpetrators after actions by the radical left, for example.

Particle science

Every person loses around 40,000 skin cells per minute, which have an individual odor. Unfortunately, this cannot really be prevented. Additionally, we sweat particularly intensely on our hands, under our armpits, on our forehead, on the soles of our feet, and in the genital area, resulting in a potent odor cocktail. You may also have taken medication (e.g. psychotropic drugs or heart medication) that contributes to your smell, or eaten a lot of garlic, or sprayed yourself with your favorite perfume, or washed your hands daily with the mango, hibiscus, coconut and vanilla soap in your shared apartment. All of these factors, together with the individual characteristics of your metabolism, influence your smell. People who live together often have similar odor profiles because they spend time in the same places, use the same detergent, eat the same things or hug each other often.

The odor particles are then decomposed further by bacteria. However, the individual odor is not lost in the process. This decomposition process depends on the particles' specific characteristics and produces an unmistakable smell—much like how we recognize people we haven't seen in ten years despite their external changes. Only when a sufficient amount of material has been destroyed does the dog have difficulty finding the scent.

The amount of time the decomposition process takes depends on temperature, humidity, and soil conditions, among other things. At temperatures between 10 and 15°C with humid weather conditions, the tracks remain fresh for a long time. Dry heat or dry cold accelerate their decomposition. The particles keep particularly well on snow. On asphalt, the particles do not last as long as they do on natural surfaces. And so, the trail is subject to constant change and influenced by many factors.



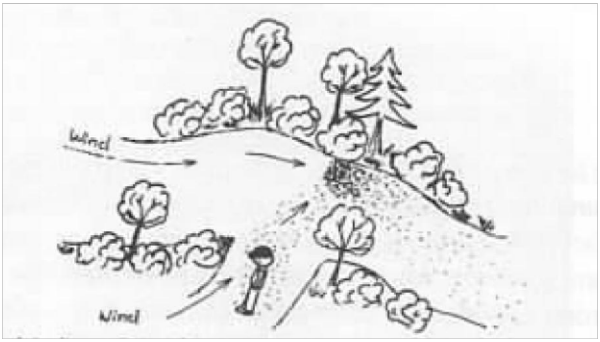
An example of how air current distribute odor particles. The spot labeled "turbulence" behind the first bush has the strongest odor, even though the person was never there. The spot labeled "blind spot" is where there is no odor.

The particles do not necessarily stay in one place either. They are blown, swirled, or carried away. They are microscopically small, sail to the ground, swirl around, catch on obstacles. These obstacles can be house walls, curbs, bushes, embankments, and so on. Therefore, the smell is not always directly where the person has walked, but often several meters to the side.

The human (i.e., the dog handler) never knows where the scent trail is. There are also no technological aids they can use to know this. Only the mantrailer (the dog) can recognize the tracks. This is why humans have no control over the course of the track: they are dependent on the dog and must interpret its behavior, carefully intervening to correct illogical behavior, such as due to how the dog doesn't understand the possibilities

of human behavior as well as humans do. For example, if the dog senses the scent on the roof of a garage on a path where the person they are looking for has probably walked, the dog will want to go onto the roof because that is where the scent is. However, the handler knows that even though scent particles have blown onto the roof, the person they're looking for has likely only used the adjacent path.

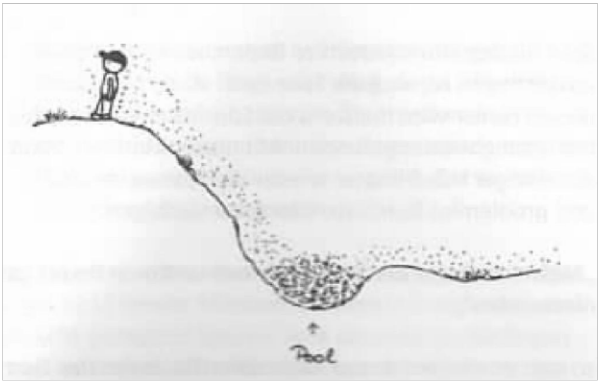
Such drifts are not the exception, but the rule. Wind, leaf blowers, and passing cars blow the particles away. Even the updraft generated by your own body heat means they don't simply fall vertically, but start by "sailing" through the air. Rain can also wash the particles away. Therefore, the trail is not straight—the dog has to smell where the particles are, and the human interprets a probable path. Or wind can blow the particles several hundred meters across a field so that they only remain in a furrow, or on a hot summer day an updraft can cause the particles to sail off again. Or rain washes the particles down a slope, causing them to remain in a place where the person being searched for has never been. Or you pause because you want to cross a road, and the waiting time causes many particles to fall away from you in one place and they blow into a cellar window. Then, the dog will indicate that the track leads there, and the cop will think: "Ah, maybe the person we're looking for was in this cellar." Or maybe the tracks lie by the side of the road for days, and then a storm arrives that blows them far away.

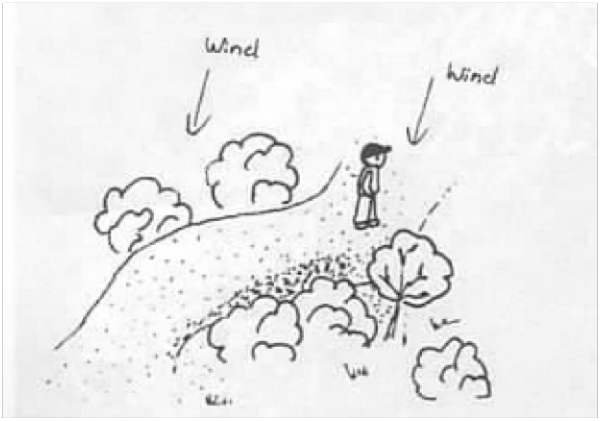


In this example, too, the wind ensures that the scent gathers and concentrates in a completely different place.

A well-trained mantrailer always looks for the freshest scent. So if you make a lot of circles around the scene before the action in an attempt to

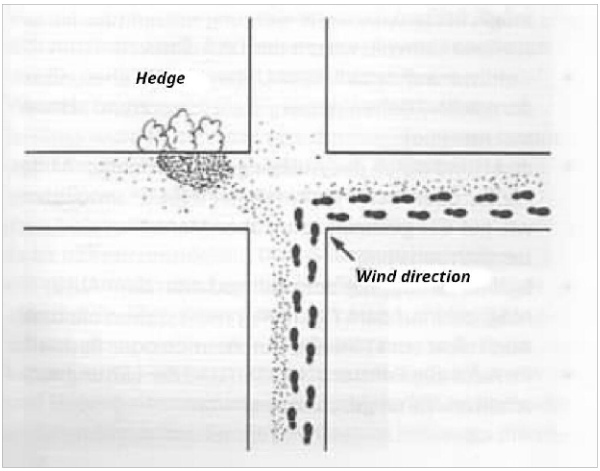
confuse the dog, you may get dizzy, but the dog will be able to identify and follow the most recent, freshest track. Of course, it is not impossible for a dog to follow your old tracks, too. For example, mantrailers often lead only to the general living environment of a suspect, not the specific place of residence, because the dog recognizes all the tracks you leave every day on your way to the bakery, supermarket, or friends' houses. The resulting complex pattern of tracks is not always clear enough for the cops to interpret. Tracks often lead to the vicinity of squats because the cops already suspect the perpetrators live there. This demonstrates that the supposedly neutral search for clues is always subject to the investigators' preconceptions and can therefore be manipulated.

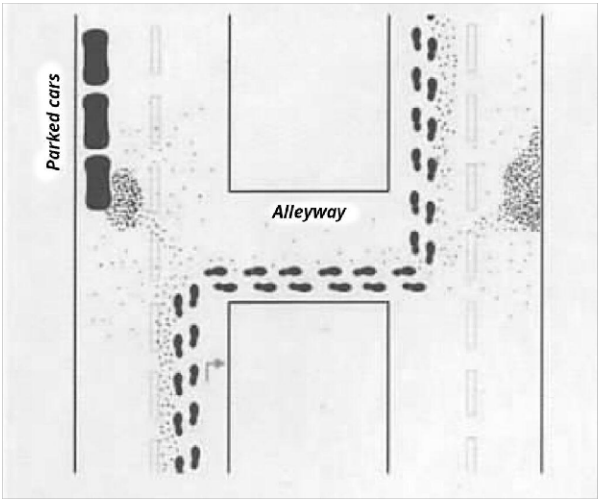




Busy squares and large urban intersections with many junctions are difficult for dogs. Not only does the volume of traffic impede the dog's search and

concentration—in large open spaces, the wind can often blow the scent particles away, for example, into the neighboring street. Scent particles can also be blown into bodies of water from bridges with open railings and are then no longer detectable in sufficient quantity. However,crossing a stream does not help to shake off a mantrailer; the dog can easily pick up the scent again on the other bank.





Ultimately, it all depends on the specific dog's skills. For example, one mantrailer successfully tracked a scent through Düsseldorf's main railway station, where there is a lot going on and 300,000 people pass through every

day! Whereas other dogs with only previous experience in the countryside or in a small town would have failed in a busy square.

Scent objects

Anything that smells like you can generally be used as a scent object for the dog to pick up your scent. This method is less effective with objects made of plastic or metal. Clothing, on the other hand, is ideal—except for shoes. Due to the updraft generated by body heat, relatively few particles land directly on your shoes. Glasses, paper, and natural materials are good at picking up scent traces.

If a scent object is carefully stored in a sealed jar, the scent will be retained for a long time and the object can still be used by a dog for tracking months or even years later.

Use of means of transportation

Unfortunately, it's no exaggeration when it comes to light that a dog has followed a trail for several hundred kilometers, even though the person being sought was traveling by car. There are several well-known examples of this, including after actions by anarchists. However, it's not the case that a dog leads the cops to the target person by sniffing for 300 kilometers without interruption. If there are indications that the person used a vehicle, the dog is put in a vehicle as well, and is only released at intersections, parking lots, rest areas, junctions, bus stops, and stores along the way to pick up the trail again. It may be enough for the car carrying the person to have driven past because particles have escaped the car through open windows or ventilation system and become lodged somewhere. However, it is easier for the dog to find the track if the person has gotten out of the car because this strengthens the track. This is the most common operational mistake which enables the mantrailer to find the scent again after a means of transportation has been used. With this method, a single dog can repeatedly pick up the scent and easily follow it for hundreds of kilometers.

"Most of the time the trail ends somewhere and you don't find anyone"

…according to an experienced mantrailer trainer. That gives us hope. Because although the dogs are capable of incredible feats in individual cases, the conditions in everyday life are of course not always ideal for them.

Many factors make it difficult for the dogs to find the scent:

- Odor contamination: The dog handler is often the last one to arrive at a "deployment site." By that time, many objects have been touched by other cops and become contaminated. It is not easy to find a suitable scent object.
- The mixture of old and fresh trails (see above).
- Busy areas, squares, and intersections.
- Trails are often older by the time the mantrailer comes into play.
- Long trails tire the dogs. Tracking is very tiring for them. This is why they are often replaced after half an hour (in busy urban environments).

We can also make it harder for the dogs to follow our tracks through our own behavior:

- Do not leave any unnecessary objects at the site of the action and avoid touching anything you don't need to.
- Do not ingest any odor-intensifying substances or allow them to touch your skin before the action.
- Wear clothes that you haven't worn before, and that are ideally non-porous (which also makes sense for minimizing DNA traces).
- Do not just travel on natural surfaces; also use surfaces that are more difficult for the dog to follow on (see above).
- Irritate the dog by using chlorine-based agents, pepper, or pepper spray (it is debatable how well this works, but mantrailers are quite sensitive).
- Whether on foot, by bike, or by car: do not pause along the escape route if possible! Not even to pee, take a deep breath, or talk.
- Close all car windows and turn off the ventilation. Keep the doors closed.

- Do not take the direct route home after an action. The longer the route, the greater the likelihood of them losing the track.
- Do not dispose of clothing or other items on the escape route (if possible). The dog will find them (and thus new tracks)!
- Don't let this information discourage you. Mantrailers are not always used, and often, they do not find enough tracks because external conditions are too poor. Use this information to outsmart the dogs!

Data medium detection dogs

North Rhine-Westphalia is the second federal state after Saxony to hire data medium detection dogs for the police.

Following the child abuse scandal in Lügde, five of the approximately 300 protection, narcotics, explosives, and arson detection, cadaver detection, banknote detection, and mantrailer dogs underwent further training in October 2019. Now, they can sniff out data mediums.

These detection dogs have been trained to find CDs, hard drives, memory cards, USB sticks, smartphones, and SIM cards. They are also trained to detect the chemicals used to manufacture data mediums.

Searching for data mediums is much more difficult for the dogs than searching for drugs because narcotics have a stronger odor. Therefore, to find data mediums, the dogs have to get much closer to the objects being searched. A data medium detection session lasts a maximum of 15 minutes, after which the dog is given a break.

DNA traces

Everyone leaves behind DNA traces in forensically usable quantities everywhere and at all times. These traces are long-lasting, and they potentially contain extensive information about the perpetrator.

All body cells contain DNA—deoxyribonucleic acid, which is usually abbreviated to DNA. From the point of view of the police, items such as cigarette butts, handkerchiefs, and glasses, as well as touched objects or paper are of particular interest. Usable DNA can also be found in urine,

feces, semen, vaginal secretions, and, of course, blood. Hair is a bit more complicated: until recently, hair that had fallen out without roots was unsuitable for identifying someone. However, analysis technologies are constantly improving, and researchers have succeeded in isolating nuclear DNA from rootless hair.

It is nearly impossible to avoid leaving behind DNA traces entirely. To significantly reduce the likelihood of leaving behind traces, it is necessary to wear new gloves, a face mask, closed headgear (e.g., a swimming cap), and clothes with long sleeves and pant legs that you haven't worn before. While it is true that everybody else leaves traces as well, such that in semi-public places simply sweeping up mixed dirt will only bring the police limited progress, relying on this alone is dangerous. Elaborate analyses are carried out in some investigative procedures, and if your DNA is found among many others, it is still there.

A central challenge for DNA forensics is finding traces that are related to the crime being investigated. What plays right into the hand of police is the fact that clothing fibers, which have been the focus of forensics all over the planet for decades, almost always yield usable DNA of the person wearing the clothes. Places where people have peed can also be of interest to investigators. Cigarette butts or saliva residue on stamps and envelopes are of legendary popularity. By the way, non-human cells are not helpful in confusing the police—the primers used for analysis to isolate individual DNA sequences are very species-specific. On the other hand, hair from a particular dog can be identified and provide clues to the police.

At best, DNA traces can be removed by wiping down and bleaching extremely smooth surfaces, and only if there are no crevices or similar things. Tools, paper, textiles or other objects with rough surfaces, on the other hand, are practically impossible to clean in this way, of either human, animal, or plant DNA (even this can be relevant, for example, if genetically modified plant traces are found on pruning shears).

DNA is an amazingly stable molecule. Therefore, it is difficult to chemically remove DNA traces, especially since sterilization (such as simple heating or alcohol) is insufficient. You have to smash the STRs (short tandem repeats, see the section “Creating the DNA profile”, p. 16), and they are small.

> What works quite well from experience is sodium hypochlorite, but it is not so easy to obtain. An alternative is bleach or aggressive cleaners that have sodium hypochlorite in them (see ingredients and follow directions for use).[2] Brand names include Dan Klorix or mold remover or Clorox (American product). Sodium hypochlorite is not very stable, so it is recommended to always use a new bottle. It stinks quite a bit, just like chlorine, and is aggressive on many materials, so use smooth work surfaces that are not sensitive to it, such as a plastic tub, wear intact rubber gloves and possibly also simple safety goggles. Take care when handling! Do not use together with other cleaners. And make sure that you get into all grooves and crevices with it.

Other products for destroying DNA, such as DNA-ExitusPlus or DNA Zap (made by Life Technologies), are also available in the laboratory industry. According to published studies, however, they are no more effective than bleach with 10% sodium hypochlorite. Hydrochloric acid-based cleaners, on the other hand, don't work as well.

> Heating metal objects in an oven at 250°C (482°F) for some time also destroys DNA. The safest way to destroy things you no longer need is incineration.

DNA trace profiles are stored indefinitely in the BKA (the federal investigative police agency of Germany) database without time limits for future comparisons, and do not have to originate from crimes that meet the criteria of a serious offense (or repeat offense). Therefore, it is ultimately completely unclear what DNA data the police have at their disposal. As

[2] *Translator's Note (T.N.):* The percentage of sodium hypochlorite should be present on the label, or on a "safety data sheet" for the product that can be found online. See "DNA You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces"[a] for information on appropriate concentrations of sodium hypochlorite.

[a] https://notrace.how/resources/#dna-you-say

long as trace profiles from crime scenes have not found a match and the investigations have not concluded, not only will DNA profiles indefinitely remain in evidence storage, but the biological trace materials they were sampled from will as well.

DNA sequencing

In practice, DNA analysis leads to a situation in which the burden of proof is reversed: it is no longer up to investigators to prove guilt; rather, it is up to individuals to prove their innocence by "voluntarily" being DNA sampled. Even now, the police occasionally collect material for DNA analysis from things like illegally pasted posters. Individuals whose DNA profile matches those sampled from the crime scene or alleged crime tools are pressured to prove their innocence. This effect is intensified by the longevity of the traces. If evidence is available, prosecution can occur decades later.

Finally, DNA sequencing can also be used to determine the characteristics of the person who left the trace. Since 2004, the analysis of chromosomal sex (i.e. XX, XY…) has been permitted. Special chromosomal characteristics (e.g. trisomies) are thus automatically recorded. Since 2019, the analysis of additional characteristics has also been permitted, including skin, hair, and eye color, as well as the epigenetic determination of the age of unidentified samples. There is (still) no legal basis in Germany for characteristics such as susceptibility to disease. An intermediate area is the analysis of family relationships: it is not permitted within the BKA's DNA database but is permitted in the context of mass genetic testing and for investigations and criminal proceedings. Additionally, the current DNA database also explicitly allows for the comparison of "partial" traces, i.e. profiles for which some STR counts are unavailable for whatever reason. At least technically, this makes it possible to search for relatives. We can only speculate about how often the rules are stretched here.

Creating the DNA profile

The fact that only the tiniest traces are sufficient to create DNA profiles is largely thanks to a technique called PCR (polymerase chain reaction),

invented in the early 1980s. PCR enables the copying of DNA traces in a test tube, producing any amount of the trace from the tiniest quantities —theoretically, a single DNA molecule suffices.

To create the "fingerprint," specific DNA "primers" are used to cut out small sections from the long DNA double helix at certain points and multiply them. The fingerprint is created by measuring the length of these segments. In 1995, the Federal Constitutional Court ruled that human dignity was not endangered by genetic analysis as long as no genetic information was obtained. Although this sounds paradoxical, it means that it is permitted to analyze so-called "non-coding regions" of DNA. These are sections of DNA that lie between "genes" (which contain blueprints for proteins) and were previously considered useless "junk" DNA. However, they are now examined by human genetics in relation to statistical correlations with diseases or traits. With the introduction of "extended DNA analyses" at the end of 2019, this distinction was finally eliminated and the analysis of coding DNA was permitted. Legislators argued that, since these concern externally recognizable characteristics, the technology is equivalent to a photograph or video recording in terms of data protection law. However, scientifically, this argument makes little sense because the analyzed gene variants also influence many other characteristics besides hair, skin, and eye color.

Within this "non-coding" DNA, there are zones in which a sequence of base combinations repeats a few or many times—in jargon this is called a short tandem repeat (STR). Some STRs vary considerably from person to person. Therefore, there are very different numbers of repeats in a population, which makes it possible to distinguish people according to these STR variants.

Science and industry have named some STRs, such as FGA, THO1, or D351358. A DNA profile consists of two numbers after a specific STR (e.g. FGA: 20, 23; THO1: 6, 9), indicating the frequency of repetition (one for each chromosome). Currently, the BKA determines at least 13 such STRs, and usually even 16 due to the number of STRs included in available test kits (previously test kits only had 8 STRs, so many previously stored DNA profiles will consist of fewer details). Other countries—the quasi-standard CODIS is set by the US—prefer more or fewer, or even

different STRs altogether. This also depends on which biotech companies have won the national race.

Areas of application of DNA profiles

Probability statements to establish identity: The most important application of DNA profiles is establishing identity—if the 26 numbers (two for each of the thirteen STRs) match, then the compared profiles most likely belong to DNA from the same person or their identical twin. However, it could also be a coincidence. The authorities like to categorically rule this out and cite the calculations of "biostatistics" as proof. Their argument is that, for example, with five equally frequent possible repeat values for each STR, there are over 1,000 quadrillion possible combinations for 13 analyzed STRs. However, in reality, the relationships are far more complicated because certain STR repeat patterns occur more frequently than others, as do certain combinations between different STRs. In particular, the comparative populations from which the frequencies of certain STR repeat patterns are determined must be questioned, because this forms the basis of the biostatistical calculations. In this respect, the probability calculations claimed by the authorities should be treated with the utmost skepticism, and possibly questioned by an independent expert. Additionally, many investigations do not involve complete DNA profiles, but only partial profiles, i.e. not all STRs could be determined from the trace. In such cases, any statistical probability statements are often much less convincing.

Familial descent: Matching STR patterns can not only be used to establish identity, but also to clarify familial descent. Since for a given STR, one repeat patterns originates from the father and the other from the mother, a direct biological relationship can be inferred when the DNA profile numbers of one of the chromosomes matches.

Other molecular genetic testing methods

Investigation of the "biogeographical" origin: When probability statements are made about the possible origin of the sampled individual, molecular genetic analysis methods other than the creation of the DNA profile described above are used. However, these analyses are not permitted

for storage in the BKA's DNA database. According to Section 81e of the German Criminal Code, molecular genetic analysis of "ancestry" is permitted without distinguishing between family and regional ancestry. However, the common legal interpretation is that the latter is not legal. Origin or ancestry analyses are now an international market, in which very approximate probability statements about the "biogeographical" origin are sold via "ancestry testing."

There are now extensive databases that record the frequencies of specific DNA markers in certain regions. In most cases, this involves analysis of STRs on the Y chromosome, which are only passed on from fathers to sons, or STRs of mitochondrial DNA (which is not located in the cell nucleus but in the cytoplasm), which (with exceptions) is only passed on from mothers to their children. Since both change only via mutations, certain mutation patterns that occur more frequently in certain regions than in others can be used to infer a probable origin.

Genetic testing companies also analyze so-called single nucleotide polymorphisms (SNPs), which are small deviations within the coding DNA, through the services they offer online.

Examination of phenotype characteristics: Although the detection of "genetic defects" (e.g. sickle cell anemia or cystic fibrosis) is prohibited, characteristics such as hair, skin, and eye color, as well as a person's approximate age, can be derived from DNA traces. However, the validity of such DNA analyses is very scientifically controversial. The accuracy of the prediction varies greatly depending on the available trace material and the characteristics of the person concerned. More complex characteristics, such as facial shape, cannot yet be determined. At the current state of research, it is therefore inaccurate to speak of a "genetic ghost image," as some scientists and politicians do.

Other biochemical analyses of body tissue: DNA is not the only focus of forensic biotechnicians. Isotope analysis, for example, is a noteworthy technique used to determine where a person lives or lived previously. This involves examining tissue samples to determine the ratios in which nuclei of different weights of common elements such as oxygen or calcium occur. These usually reflect the corresponding ratios in drinking water or other, regionally distinct foods. If their geographical distribution is

determined, the authorities can attempt to determine previous places of residence, particularly if—as in hair, teeth or bones—changes over time can be deduced.

Other ways to obtain DNA

Confiscated police samples: Another way for the police to obtain your DNA profile is by analyzing existing samples of your body cells that the police possess. Recently, for example, the confiscation of an alcohol test from a traffic stop came to light.

Undercover investigations: The police also collect DNA samples during undercover investigations. This was recently revealed in a case, and has already been observed many times before: investigators collect cigarette butts, stickers, glasses, or discarded paper to create DNA profiles of individuals during undercover surveillance.

Biobanks: It is also conceivable that the investigating authorities could confiscate biological material or test results from databases in hospitals or research institutes, so-called biobanks, i.e. blood or tissue samples that you have given voluntarily, for example for research or for a bone marrow donation database, and use these to obtain the DNA profile. The current legal opinion is unanimous in interpreting this as inadmissible, but it is not absolutely clear.

The Gene Diagnostics Act, for example, which came into force in 2010 with the intention of protecting informational self-determination with regard to medical genetic tests, does not regulate the issue of research databases. In principle, however, biobanks are not generally a source for comparative profiles in the search for a DNA trace profile submitted by the police (with the usual STR information) because they generally store different markers. However, it is conceivable that in special cases the police could extract specific "non-coding" markers from their trace samples and search for them in biobanks.

In addition, a recent study showed that it is essentially possible to match profiles of individuals in research databases with the profiles of their close relatives in forensic databases.

In this context, the coronavirus PCR test must also be viewed critically. Although the test itself only tests a throat or nasal swab for the presence of coronavirus RNA, the Robert Koch Institute requires in its guidelines that the testing laboratories store the sample for potential future testing. Some laboratories comply with this request, others claim that they "cannot afford this additional logistical effort."

Internet genetic tests: For a few years now, Internet genetic testing companies have heavily courted customers on the German market, promising "personalized" lifestyle tips or information about their supposed ancestry. In the US, the DNA databases of these companies are now regularly used to find suspects. To do this, law enforcement agencies sometimes create database profiles like ordinary users and upload the DNA sequences of the person they are looking for to find their possible relatives.

So far, there are no known examples of police accessing biobanks or data from private lifestyle testing services in Germany, though there are in other countries.

DNA in court: a statement of probability, not proof!

There are many reasons why "evidence" obtained through DNA analysis can be called into question! In principle, a match between a trace DNA profile and a personal DNA profile only allows statistical conclusions about the likelihood that the DNA profiles belong to the same person. The biostatistical assessments of the frequency of a profile in a population are themselves controversial and depend on the reference population used for the calculations. In any case, it is controversial whether even a very high probability statement can be considered the sole "evidence" in criminal proceedings and therefore sufficient for a conviction.

There are also a number of possible sources of error, such as contamination (e.g. by a manufacturer of cotton swabs, as has been famous since the "Phantom of Heilbronn" in which the cotton swabs used by many state police departments were contaminated by the same factory worker), or misinterpretation of raw data. The latter is particularly important in cases involving mixed traces and/or small amounts of degraded DNA material,

as these often only allows partial profiles to be created (i.e. not all STRs). After all, the presence of DNA at a certain location does not indicate how the material got there or what happened!

Artificial DNA

Energy supply companies (since 2016) and Deutsche Bahn (since 2011) have been using artificial DNA to protect metal cables, especially against theft. The copper core and the cable sheath are both coated with a marking liquid (that is only visible under UV light). Synthetic DNA is dissolved in the liquid and can be detected using polymerase chain reaction (PCR) methods. In some cases, particles smaller than 1 mm with an identifying engraving are dissolved in the liquid, and can be read under a microscope. Such a marker is also misleadingly called artificial DNA and unfortunately survives high heat!

Tools or items of clothing that come into contact with cables prepared in this way are clearly marked for traceability. This might not seem so bad, as all tools and clothing are disposed of cleanly after a successful action anyway. However, residues of artificial DNA from your clothes can also transfer to your bike's handlebars or saddle, or to car seats. Therefore, when working on cable ducts, you must meticulously choreograph changing clothes after the action.

Following "successful" pilot projects, this method is now also being used more frequently to protect buildings and technical equipment from burglary and theft. The "artificial DNA showers" used in the Netherlands and the UK to mark individuals who use an exit after an alarm has been triggered are not (yet) in use in Germany, as far as we know.

Data traces

Most of us are probably familiar with the situation where we stumble across something interesting online and want to find more information on the website of the company

involved. Stop right there! If you suspect that this could be an exciting target for a direct action, then stop your research and continue it with TAILS!

Law enforcement agencies are increasingly interested in the "digital" realm. During house raids, they almost always confiscate everything that looks like a computer, smartphone, data medium of any kind. Since Edward Snowden's publications, it has been known that secret services are collecting data from the Internet on a large scale—even automated, right up to "hacking" computers en masse. The investigating authorities use unnoticed access to our everyday computers to access our data before we encrypt it.

This is why the computer we use to access the Internet at home on a daily basis is off-limits for seriously sensitive content.

Given this situation, we recommend taking advantage of the available technological possibilities for self-protection instead of burying your head in the sand. Tails is a big step in this direction. This live operating system can be started from a DVD or USB stick without being installed on the computer. Your standard operating system on the hard drive remains untouched.

Why Tails?

When used correctly, Tails leaves no traces on the computer—your hard drive remains untouched. Any malware that may have been introduced (at the level of the operating system) cannot "persist" on a live DVD or a write-protected live USB, so it no longer impacts you the next time you start your computer. However, since Tails is software, it cannot protect against manipulated hardware.

The most important reasons for using a live operating system like Tails are its *amnesia* and *immutability*. After shutting down the computer, all data that you have not explicitly backed up to an (external) data medium is gone. The computer's amnesiac memory is also overwritten with random numbers during shutdown, and the hard drive remains untouched by

the Tails session: no system files that reveal which USB sticks you have used, no hidden traces of your Internet research, no references to "recently edited" documents and no remnants of image processing—everything is gone after you have finished your work. Your "normal" operating system (on the hard drive) of this computer remains unchanged, and the computer itself also bears no trace that this Tails session took place.

To ensure nothing is left behind during sensitive work, the Tails live operating system should be stored on an unalterable data medium (e.g. a burned DVD or a USB stick with a mechanical write protection switch). Note that this only applies to computers that do not already have compromised firmware in their BIOS (the internal base system of the computer). We therefore advise against using Tails with computers that have Windows or Mac installed on them.

With Tails, all network connections to the "outside" are routed via the Tor network. This means that you have fewer opportunities to inadvertently reveal your identity. Of course, even with Tails, it is important to understand the basics of Tor usage, such as the difference between concealing your identity and encrypting the connection. Tails integrates lots of security-relevant software and is regularly updated. You can expect a new version of Tails approximately every two months. Tails is based on the Debian Linux distribution—security updates and further software development are largely handled by Debian. The Tails developers aim to always stay close to Debian and limit modifications to what is necessary, which has the added benefit that Debian (or Ubuntu, which is also Debian-based) documentation often helps with questions about the software. Tails therefore largely consists of familiar software that has only been configured differently, if at all.

> Our recommendation: Get a computer dedicated to research and publishing. Its hard drive remains unused (ideally you should remove it), you use the computer ONLY WITH TAILS. NEVER use this computer for personal purposes (online bank transfers, checking your personal email, etc.) We also recommend that you not connect to the Internet with it at home.

Visit the Tails website (tails.net) for instructions on downloading (and verifying!) Tails, installing it on a USB stick or DVD, and configuring your computer to boot the Tails operating system on the USB stick or DVD instead of whatever is on its hard drive.

Researching and publishing—only via Tor

A large part of digital communication identifies the communicating parties through what is called an IP (Internet Protocol) address. The Internet Service Provider assigns an IP address (e.g. 172.16.254.1) to the router you use to access the Internet. This address is sent along with all network activity via a standardized protocol. Without Tor, your browsing, chatting or emailing can be traced back to the identity and location of this router.

If you do not take any additional precautions, the transmitted IP address reveals which router was used to access the Internet.

Additionally, each network adapter has an identifier called a MAC address (e.g. B4:89:91:C1:F4:CE). Each network adapter (e.g. the Wi-Fi or ethernet adapter) of your computer logs its own unique (physical) MAC address on the router. Depending on the Internet protocol used, this address is not transmitted "outside" (into the Internet). However, if you access the Internet via Wi-Fi in a public café, for example, the operator or an attacker can log your MAC address with little effort. This means your Internet activity can no longer be assigned only to the cafe's Wi-Fi router but also to the exact Wi-Fi adapter you are using on your computer! Even at home, an attacker who hacks your router can determine which computer (e.g. in your shared apartment) accessed a particular website.

Tails changes your MAC address(es)

If you walk through the city with your laptop, tablet, or smartphone turned on and with Wi-Fi activated, your Wi-Fi adapter will report its MAC address to all Wi-Fi routers within range, without you having to actively select them to establish such a connection! The routers of all Wi-Fi networks listed by the device have already identified your computer via

its Wi-Fi MAC address in an initial greeting! Therefore, if these fleeting "greetings" are recorded, you leave a traceable trail.

If application errors or other deanonymizing Tor problems occur, an attacker could identify your computer using the MAC address logged on the Wi-Fi router you used, if they gain access to it.

> For additional security, Tails replaces the MAC addresses of all network adapters activated in your computer's BIOS with random addresses before establishing the first network connection (while Tails is starting).

However, sometimes a Wi-Fi network will block these spoofed MAC addresses: some networks only allow access to a limited list of preset MAC addresses. You cannot use these networks securely.

Be careful with the UMTS stick

So, now it's getting a bit confusing, so we need to differentiate between the terms. The UMTS stick (used to connect to a mobile network) is also an independent network adapter (not to be confused with a USB Wi-Fi adapter!), and therefore also has its own MAC address. Tails should also overwrite this with a random address at startup. Nevertheless, the additional security of a changed MAC address is irrelevant here because your SIM card's unique identification number (IMSI) and your stick's unique serial number (IMEI) are also transmitted to the mobile phone provider each time you connect to the network. This enables identification and geographical localization. The UMTS stick works like a cell phone!

> If you don't want different Tails sessions to be associated with each other, don't use either the UMTS stick or the SIM card more than once! For sensitive research or publishing, both the UMTS stick and the SIM card must be disposed of!

Otherwise, various searches would be linked via the shared IMEI or the shared IMSI. Simply replacing the SIM card alone is not sufficient!

In conclusion, when researching, editing and publishing sensitive content, you should exhaust five aspects of security:

- Secure configuration of the relevant software (update Tails regularly)
- Obfuscation of the IP address via Tor (preset in Tails)
- Obfuscation of the MAC address (preset in Tails)
- Internet access in a place that's unusual for you, without cameras, without your cell phone or other Wi-Fi/Bluetooth devices.
- Anonymous purchase and hidden storage of a "research computer."

Establishing a network connection

After starting, Tails automatically searches for available network connections. To connect to a Wi-Fi network, you can click on the network manager (reveal it by first clicking the button in the top right corner) or select a network via the menu *Applications* > *System Tools* > *Settings* > *Network* and then enter the password.

It takes a while to connect to the Tor network and synchronize the system time—if successful, you'll see the message "Connected to Tor successfully." Now that you are connected to the Internet, all of your browsing, chat and email connections will be routed through the Tor network.

Browsing with Tor Browser

Once the Tails network manager has established a network connection, you can open Tor Browser under *Applications* > *Internet* > *Tor Browser*.

Note that there is active content on websites that can jeopardize your anonymity. Websites often use JavaScript, cookies, PDF documents or downloaded fonts. Such active website content can transmit many settings and characteristics of your computer (processor, screen resolution, installed fonts, installed plugins, etc.) via a so-called "fingerprint," which in the worst case could be identifying. In Tails, the default Tor Browser setting still allows scripts and plugins.

> Right at the start of your Internet browsing, you should set Tor Browser to an even more restrictive setting. To do so, click on the small shield icon in the Tor Browser menu bar and then on "Settings" select the "Safest" security level.

If some websites with active content are not displayed correctly with this highest security setting, you can lower the security level at any time. Note that doing so may compromise your anonymity!

Only store data in encrypted form

As previously mentioned, Tails does not save anything to the computer's hard drive. Therefore, you should use a USB stick to store your data. For security reasons, it should not look identical to the (preferably write-protected) USB stick with Tails installed on it!

> We strongly advise that you store all data in encrypted form only—on a USB stick formatted specifically for this project, on which no personal information is stored. To accomplish this, we create an "encrypted partition" on a new USB stick. Tails uses the Linux encryption software LUKS. You can then decrypt the data on any Linux operating system. However, it is not possible to exchange data with Windows or MacOS operating systems!

Create an encrypted partition on a data medium

Open the disk management software: *Applications* > *Utilities* > *Disks*. The Disks application lists all currently available disks and data mediums.

Identify the data USB stick: If you now insert the USB drive to be encrypted, a new "disk" should appear in the list. Clicking on it will display the details of the data medium. Carefully check whether you have selected the correct data medium (highlighted in blue)—i.e. whether the

description (brand, name, size) matches your USB! A mix-up with another data medium will delete its data.

Delete old stuff: Generally, an (unencrypted) partition with a standard file system exists on a newly bought USB stick that you must delete. To do so, select the affected partition, click the "Minus" icon, and confirm the deletion. We recommend deleting all partitions to avoid confusion, as well as not trying to mix encrypted and unencrypted data on the same stick.

Now click the "Plus" icon. A "Create partition" dialog box will appear, allowing you to configure the new partition:

Size: By default, the size is the same as the size of the free space. You can leave this as it is advisable to encrypt the entire data medium.

Delete: Before creating the new partition in the free space, overwrite it. You should definitely do this, but bear in mind that this overwriting will most likely not be complete (see the section "Deleting data", p. 31). If you want to be on the safe side, use an new USB.

Type: Here you select "Encrypted, compatible with Linux systems (LUKS+Ext4)."

Name: Choose a name for the data medium so that you can identify it later—please note that this name can be read by everyone!

Password: Choose a strong password. It should be complex enough that it cannot be cracked, but you must also be able to remember it![3] Then click "Create." This process may take a while. When the progress indicator disappears (the wheel stops turning), it is finished.

Opening an encrypted partition

When you insert an encrypted USB stick, you will then be prompted to enter the password. If it is the correct password, the partition will be displayed in the file manager as a disk with the name you have chosen. You can now copy files onto it or perform other file operations.

[3] *T.N.:* See "Threat Library: Digital best practices"[a] for advice on password strength.
[a]https://notrace.how/threat-library/mitigations/digital-best-practices.html

Before you remove the disk after you have finished your work, you must right-click on it in the file manager and then select “Eject”! This is important, because simply removing an encrypted data medium without ejecting first can corrupt it.

Remove metadata

Before photos can be published, the “metadata” stored in the image that uniquely identifies the camera used to take the photo must be removed. Some newer cameras (especially smartphones) even store the GPS coordinates in this metadata, in addition to the time and serial number. A thumbnail (preview photo in small format) can reveal image details that you have pixelated or otherwise made unrecognizable in the actual image. This metadata must be removed!

Unfortunately, LibreOffice documents and PDF files, for example, also contain metadata. Information such as user name, computer, fonts, file names, and directory locations of embedded images allow conclusions to be drawn about you or your computer.

To remove metadata from a file, use the application Metadata Cleaner.

> The greater the need for security, the simpler the data format you choose for publication should be.

Plain text format reveals the least about the computer on which the text was created. Note that the name of a document may also allow conclusions to be drawn about the author or their computer.

Identification of external data mediums

Every external data medium (hard drive or USB stick) is identified and registered by the drive management of the operating system (Linux, Windows and also MacOS). Using a data medium with Tails leaves no such traces, as all log files disappear from the (volatile) working memory when the computer is switched off and this is also overwritten with random numbers.

However: if you (also) use a data medium on a computer WITHOUT Tails, there is a risk that this computer will "remember" this data medium via a unique identification number.

If the computer is later seized or compromised, it can be determined that a certain USB stick was used, and when. (The reverse is not true: a non-compromised USB stick does not remember which computer it was inserted into). The clearly identifiable traces in the system log files therefore "links" your USB drive to all computers into which it has ever been inserted. We say this because we want to make it clear:

> Data mediums that have been used to store a sensitive document must be completely erased and destroyed (e.g. after publication).

Deleting data

Unfortunately, it is very complicated to "safely" get rid of data once it has been created. As everyone probably knows by now, simply deleting a file is not enough—the file remains completely intact, its name is simply removed from the list of available files on the data medium. The occupied space is released, but not overwritten.

Unfortunately, software techniques that overwrite individual areas of a data medium like a USB stick with different data patterns several times do not lead to the desired result!

For those who are impatient, here is the result of our explanations first:

> The safest option is to keep data only (temporarily) in the working memory! If data must be saved somewhere beyond an individual Tails session, then it must be saved to an external, fully encrypted data medium. A securely encrypted data medium is the best protection against (readable) traces.

> Erasure programs such as “wipe” or “srm” do not work reliably on flash media (USB sticks, SD cards, SSDs, etc.) due to their very nature. Even if the medium is overwritten entirely, traces may remain. Therefore, we also destroy data mediums with highly sensitive content.

Problems when overwriting data mediums: The physical properties of the data medium make it possible to reconstruct the previous content of an overwritten storage location. We will spare you the details explaining why the number of times it is overwritten is not so important!

The problem with magnetic hard drives is that the hard drive controller sorts out defective sectors (memory areas) and copies data previously stored. An overwriting program for “secure” deletion then no longer has access to these defective sectors. However, in the forensics laboratory these areas can be read—with potentially serious consequences for you.

With flash storage mediums such as USB sticks, SD cards, Compact-Flash cards and the newer SSD hard drives (solid-state disks), this problem of internal copying (outside the user's control) is the rule rather than the exception due to the memory's high susceptibility to errors. An overwrite procedure to “securely” delete individual files then only “catches” one of several copies. A recent research paper confirms that all software erasure techniques are unreliable when applied to flash storage, even when overwriting the entire storage medium.

> None of the programs tested were able to securely delete individual files!

Although it is limited, for instructions on how to overwrite the entire disk in Tails, see “Tails For Anarchists”.[4]

[4]https://anarsec.guide/posts/tails

Destroy the data medium

Precisely because of the inadequacy of software erasure techniques and the extensive capabilities of forensic data recovery, you should also destroy sensitive data mediums. Unfortunately, this is also more problematic than expected. Optical media are the easiest to destroy.

Magnetic hard drives are very difficult to destroy, you cannot simply throw them into a fire. The temperatures that a fire causes on the data-carrying disks (aluminum has a melting point of 660°C and glass becomes viscous at over 1000°C) only cause a slight deformation. Unscrewing the housing and removing the disks is at least necessary to generate higher temperatures on the disk itself.

In addition, a camping gas soldering torch is not sufficient for this task. You need thermite, a powder that burns at 2300°C in an improvised "combustion chamber" made of bricks that liquefies the disks. However, handling thermite requires a few precautions! As an alternative, you can also use forging furnaces that reach temperatures up to 1250°C. If this is too much effort for you, you should at least break the removed disks of the hard drive into small pieces and dispose of them in several places (be careful—risk of splinters!) However, due to the high data density, forensic experts could still find plenty of data fragments on it! Alternatively, you can sand down the surface of the individual disks with a drill and wire brush attachment.

Flash memory (USB sticks, SSD, SD cards, etc.) can also only be destroyed incompletely. You can use two pairs of pliers to break the circuit board out of the housing and then break the memory chips and circuit board into pieces before holding them in the flame of a camping gas soldering torch. You will only achieve partial decomposition of the transistor material. Caution—wear respiratory protection or keep your distance! The vapors are unhealthy.

Optical media (CD, DVD, BlueRay) can be completely and irrevocably destroyed with sufficient heat. The polycarbonate carrier material melts at 230°C (deformation). It decomposes at 400°C and burns at 520°C. A camping gas soldering torch is sufficient to melt or even burn the panes of polycarbonate, a thin layer of aluminum and a layer of lacquer.

Caution—wear respiratory protection or keep your distance! The vapors are unhealthy.[5]

Fingerprints

This is probably already on everyone's radar. Almost everyone has had to submit their fingerprints for their passport or new ID card. Sooner or later the database will be complete. You can't remove fingerprints from paper. Due to their acidic nature, fingerprints even remain "under" metallic surfaces. Simply wiping with alcohol or acetone is not enough. You have to remove the upper layers with sandpaper. Alcohol or acetone is sufficient for glass and plastic—but this will not remove your DNA!

Objects that have been in water for a long time can still retain fingerprints.

Wearing gloves consistently helps prevent fingerprints. If you use thin latex gloves, wear two on top of each other because they are so thin that fingerprints will otherwise "push through" them. With thicker dishwashing gloves, one layer is sufficient. We do not recommend spray-on bandaids as they can become brittle.

Shoeprints

Shoeprints are an often underestimated potential danger. They are as individual as fingerprints and can be used to draw conclusions about the height, weight, gait, etc. of the person who left them. If the shoe that left the shoeprints is found during a house raid, it can be identified with relative certainty, depending on the quality of the prints. Traces of soil or plant residue left on the shoe will do the rest. It is therefore advisable to dispose of the shoes after an action, especially if you have walked over snow, soil, etc.

However, shoeprints don't depend only on the shoe's model, but also on the way it's worn, which is quite individual. All shoes worn by the same

[5] *T.N.:* For further reading, see "Tails for Anarchists"[a] and "Tails Best Practices".[b]

[a] https://anarsec.guide/posts/tails

[b] https://anarsec.guide/posts/tails-best

person will show the same type of wear. If shoeprints are left in soil or snow, the police can make a plaster cast from it. Using this cast, they can often not only identify the shoe that left the print, but also match other shoes worn by the suspect to the cast based on the specific wear patterns found on the cast. So don't use old, worn shoes of yours, especially for actions where you have to walk on soft surfaces.

If you really want to be sure, buy cheap shoes shortly before an action, only touch the outside of them with gloves, and throw them away afterwards. However, there are bound to be DNA traces in shoes you have used, so never dispose of them near the action site.

Another way to make the cops' job more difficult is to put socks (without your DNA) over your shoes. This disguises the model and profile of the shoe and can also protect against video surveillance. But before doing this, try walking and running with the socks on.

Vehicle traces

The choice of a suitable vehicle should be well thought out. Consider whether a car is really necessary, because it carries many risks.

Cars leave behind tire tracks and, in the event of an accident, traces from the car's paint. Traces (especially paint) from an accident can be found both on the car and at the scene of the accident. Tire tracks and paint chips can be used to determine the car's model, and if the car is found, to determine whether the traces were left by this car specifically. Changing the tires, if possible both before and after the action, can make it more difficult to identify the tire tracks. Simply changing the tires after the action is not enough, as the police may be able to match the tire tracks found at the action site with tire tracks outside your home or in your garage. Also, when using a car, watch for leaking oil or fluids.

But by far the most important identifying characteristic of a car is its license plate. In order to pass at least one license plate check without being pulled over, the car's license plate can be swapped with another. Since most of us aren't able to manufacture license plates, you can steal them shortly before the action. It's important that the car from which you

steal the plate is the same model and color as the one used in the action, because, as a standard procedure, cops check the license plates of cars and know whether they have been reported stolen, their color and model. If the car hasn't been reported stolen and has the correct model and color, the likelihood of being pulled over is somewhat reduced.[6] Stolen license plates will however not pass a proper vehicle inspection.

To prepare for the risk of a vehicle inspection, you should hide your action materials well and, if possible, not in the obvious location of the trunk. Make sure the vehicle meets all legal standards. In Germany, don't forget your legally required warning triangle and first aid kit.

To remove a license plate, a screwdriver will usually do the trick. Try this for the first time in a quiet place where you can work without stress. After unscrewing it, you can use double-sided tape to attach the license plate to your car (watch out for rain) so it's easy to remove after the action.[7] Alternatively, you can smudge or mask license plates, especially on motorcycles, but this is conspicuous. Dealing with the license plate is also important for countering the increasing surveillance by toll and traffic management systems. Toll systems are sometimes used for Automatic License Plate Recognition. Also be aware of the risk of leaving traces in the car and try to avoid this, e.g. by packing the action materials well. In our opinion, it is almost impossible to avoid leaving DNA traces in the car you are using. Not only is a car a good carrier of traces, but it is also easy to track if a covert location tracker has been installed on it. The use of a car should therefore be avoided whenever possible.

Bikes can be a good alternative. They also leave tire tracks behind, which is often overlooked. We therefore recommend that you do not park the bike in the immediate vicinity of the action site. Depending on the surfaces, it may be a good idea to change the tires before and after the action.

---

[6] *T.N.:* If you steal a license plate from a car, you can replace it with another, random license plate (that cannot be traced back to you). This way, it might take longer for the car owner to notice the theft and report the license plate as stolen.

[7] *T.N.:* Rather than tape, we recommend using a "magnetic license plate holder" to attach the license plate to the car.

Individual features such as brand stickers can be easily covered with tape.[8] If you are wearing the action shoes while riding the bike, the pedals should also be covered with new adhesive tape. The gloves you wear while riding the bike must not be your action gloves. A brightly colored bike can easily be an eye-catcher. As with cars, it is important to meet the legal requirements for bikes, especially when you are out and about at night.

Cameras

The density of cameras in public spaces, especially indoor spaces that are publicly accessible, is constantly increasing. Although we in Germany are still far from the automated tracking of individual people across urban areas (as in London, Moscow, and many large Chinese cities), the camera landscape here is also becoming increasingly biometric and thus in principle able to search a database for people with the same eye-mouth-nose distance. It is not possible to deduce the range, aperture angle, and (distance-dependent) resolution of a camera just from what it looks like. There are too many different models to be able to do so. Basically, we have to assume that all cameras are recording.

When doing reconnaissance for suitable "camera-free" routes to and from a planned action location, you should at least check whether the cameras can pan or not. In the case of dome cameras (darkened hemispheres), you must assume they can pan, even if they often have a fixed viewing direction. Camera recordings from building entrances and stores are often used to investigate crimes. Most stores now have cameras for insurance reasons, and they are mostly installed inside but with a view of the street through the store door or shop window. Unfortunately, some motion detectors are also cameras. If warranted, only a case-by-case examination will help. Not every "Beware of camera" sign lives up to its promise, so always consult with another person to compare observations. Many mini cameras on doorbells only become active when the integrated motion detector detects a person in front of the door or when the doorbell has been pressed.

[8] *T.N.:* Covering features with tape is not ideal, as a taped up bike can look conspicuous. In addition, many bike features (e.g. the model and shape) cannot be concealed with tape. One solution is to steal a new bike for each action and dispose of it afterwards.

Dash cams

With dash cams increasingly appearing behind the windshields of cars, an extended video recording of public space is taking place—whether the vehicles are driving or parked. This includes at night, by the way, as the small cameras can record reasonably good infrared images at close range even in the dark. Of course, during the day, the quality (and therefore the range) is much better. The devices can record in a continuous loop. They overwrite old recordings only when the SD card memory is full, and even smaller memory cards can record several days of footage.

Since 2018, the use of these inexpensive monitoring tools has increased significantly, especially in larger new cars. In May 2018, the German Federal Court ruled that dash cams actually violate data protection regulations, but may be analyzed in the event of an accident. Consequently, many car insurers have recommended their use and some have even created financial incentives. In "normal operation" (without an accident), the recordings should be deleted more quickly. Unfortunately, it is trivial to restore deleted data on an SD card, so it can be assumed that dash cams will be requested by the police in the vicinity of the action site and along potential escape routes.

Traffic surveillance cameras

Although toll cameras on highways are only intended to check trucks subject to tolls, their automatic license plate recognition also recognizes all cars. In addition to the license plate, a photo of the driver is also taken. Typically in Germany, the images of car license plates are deleted immediately via axle counting and weight measurement. However, this can be deactivated for the investigation of serious criminal offenses. Additionally, many federal states have purchased similar mobile systems that operate license plate recognition for all vehicles at different locations.

Be careful if you come across such a license plate scanner (on a tripod) on your chosen route during test drives. And more importantly: make sure you don't drive too fast during the test drive so you won't be recorded by a (mobile) speed camera.

All methods that change or disguise your appearance help to provide passive protection against cameras, such as wearing a bulky jacket, a raincoat, umbrella, beards, wigs, hats…

Tool traces

There are many ways that tools can leave traces, and each tool is different. Therefore, we can only write a few basic things about the topic here. By tool traces, we mean identifying traces on both the tool and the object the tool is used on.

Each tool is unique and can be identified through both small irregularities from its production process, and normal wear and tear. It follows that each tool leaves unique traces on the object it is used on. For example, a cut sheet of paper can be matched to a specific pair of scissors (only if the cops have the scissors, of course). If the cops do not have the tool in their possession, typically only the type of tool can be determined, at least for mechanical tools which come into direct contact with the object the tool is used on.

Therefore, you should dispose of bolt cutters, screwdrivers, or whatever else is used in an action—get rid of any tool that came in direct contact with an object it was used on. Unfortunately, getting rid of the tool afterwards is not enough by itself. To stay with the scissors and paper example, the cops can not only match the cut paper to a particular pair of scissors, but also determine if separate pieces of paper were cut by the same scissors. So if you open a fence with the same bolt cutters you used to build your bunk bed, the cops will be able to determine this, even if the tool is long gone.

This is why it's necessary to acquire new tools for an action in order to work securely. They don't always have to be the best and most expensive.

Consumables such as tape, rope, cable (and their remnants) can be matched to each other. A small piece of cable in your home that matches a cable in the cops' possession can be a strong piece of evidence.

When working with either tape or glue, you need to be especially careful about cleanliness, as both fix dust and DNA traces.

Identifying traces can also be found on tools you make yourself, such as an incendiary device. Such traces are not limited to DNA or fingerprints. For example, to determine whether the same person made separate incendiary devices, it's often sufficient to examine identifying characteristics of the way the devices were constructed. Everyone interprets and implements a general, simple set of instructions differently. For example, everyone ties knots in a particular way, tapes something differently, uses a different construction method, and so on. The list does not end there and identifying characteristics cannot be completely avoided, but they can be reduced if you are aware of them. Even taking turns within the group to build materials for the action makes it harder for cops to attribute them to a specific group or person—this is even more relevant if an incendiary device fails to ignite. Additionally, sharing the task of building materials prevents unnecessary specialization within your group.

In the self-critical dissolution statement of the K.O.M.I.T.E.E.[9] published in 1995, they wrote that the cops were only able to easily attribute some actions to them because they always used the same type of igniter for their incendiary devices. So the decision for or against variation in device construction has to be made consciously and contextually. This also applies to possible variations in the chemicals used for an action and, as far as possible, their mixing ratios. Similarly, you should not always use the same brands or component types. In general, the simpler the igniter, the less evidence it will leave behind. A Molotov is the easiest to keep clean, and a chemical delay mechanism leaves fewer traces than a mechanical or electrical one. Serial numbers on components can also be a problem, especially with electrical delays. In the mid-1980s, an alarm clock used in a RZ[10] action was attributed to Ingrid Strobl due to a large-scale operation by the BKA in hardware stores. Since, according to the BKA, the RZ always used the same model of alarm clock, the stock of this model was given a unique serial number and everyone who bought it was filmed. This operation resulted in two people being jailed for a long time,

[9] *No Trace Project (N.T.P.) note:* The K.O.M.I.T.E.E. was a German far-left militant group active in 1994 and 1995.

[10] *N.T.P. note:* The Revolutionäre Zellen (RZ, *Revolutionary Cells*) were a German far-left militant group active from 1973 to 1995.

and the radical left movement was thoroughly investigated in a “terrorist association” case.

We therefore recommend varying the selection of means and materials, such as alarm clocks. It is difficult to remove serial numbers from alarm clocks because they are often located underneath fixed components. Embossing marks in metal can be milled out, but can nonetheless be restored by the cops because an embossing die also deforms the metal underneath. Embossing marks can only be permanently removed by embossing or chiseling over them, as this changes the structure of the entire piece, just like the initial embossing process.

Fire traces

Even though you must always be prepared for the risk of an incendiary device failing to ignite and thus leaving traces, it should be noted that even after a successful fire some traces can be analyzed. A fire leaves precise clues about what materials were used, the type of igniter and the place where the fire started. The police can reconstruct a lot from traces of soot, the gases in the air at the scene of a fire, as well as how and to what extent something was burned. Again, it is important to vary and use the simplest possible means. Always using the same mixture of accelerant or the same type of igniter is like leaving an autograph.

Material traces

By material traces (also known as “trace evidence”), we mean all traces that are unintentionally left behind on you, on your clothes or in places you have used. Again, there is no such thing as 100% security, but we can at least make the cops' job more difficult.

Let's start with traces on your clothes. Though invisible to the naked eye, there are many traces on your clothes that can't necessarily be removed by washing them. Depending on the type of action, these traces can be used by the cops in different ways. If you use spray paint, you can be sure that even though you can't see it, fine particles of paint will be on your clothes,

especially on your pants and shoes. The police can make these particles glow with a special lamp which is available in every police station. These traces of paint cannot be removed.

It's also impossible to remove the fine glass particles that are created when a pane of glass is broken. Unfortunately, these particles can be attributed to a specific pane based on the type of breakage. Again, washing clothes is of little help. Blood stains are also impossible to remove.

Disposing of your action clothing is often the only way to be as free of traces as possible. A simple, inexpensive coverall from the hardware store can help. You can take it off soon after the action and wear inconspicuous clothing underneath. However, be sure to practice taking it off beforehand and, if necessary, cut the bottom of the pant legs a little so you can get it over your shoes. Under no circumstances should you dispose of it near the action site, as it is sure to contain at least some traces of your DNA. We have already covered the topic of shoes and shoeprints.

Any clothing you wear will leave traces on your body. This is especially important if you are wearing gloves, as the cops will be able to tell that you were wearing gloves, and which ones, by looking for traces of fibers under your fingernails, for example.

Disguises such as beards and wigs also leave traces. Although it's almost impossible to prevent this, you should be aware that even after changing clothes and putting some distance between yourself and the action site, you will not be completely free of traces, and you may have left traces of fabric behind.

It is important to not wear anything with buttons that could get lost, and to avoid long scarves or clothing with fringes. Not only will they hinder your escape, but fabric can easily be left behind at the action site.

If you come into contact with gasoline during the action or while building a device, you should be aware that the scent is almost impossible to remove, which may be a problem if you are stopped by the police. Be careful not to spill accelerant on your skin or clothing when throwing a Molotov. The problem here is your own sense of smell—your nose develops a certain tolerance to a smell after being exposed to it for a long time, and you will no longer be able to tell if you smell like a small gas station.

If this is the case, and for example if they are investigating an arson, the police may put your hands in plastic bags so that they can later analyze whatever traces were on them. This is especially true for traces of gunshot residue that are left after firing a gun. Smoke residue tests are now also used to determine if an arrested demonstrator shot a firework or if someone set fire to a car with firelighter cubes. Traces of smoke often remain even after washing, which is another reason to dispose of your gloves.

Making action materials can also leave traces. If you work with powdered substances, you must assume that both your workspace and your clothes will be full of them. As far as we know, it's impossible to completely clean a workspace such that nothing is found by chemical forensic methods. So if you want to be on the safe side, your home should not be used for this type of work. Instead, use places which seem safe and cannot be traced back to you (i.e. not places linked to the radical left!), such as abandoned buildings. Wherever you end up working, you should be careful to avoid leaving behind any fingerprints, DNA traces, or pieces of wire, no matter how small.

Language characteristics

Grammar, spelling, vocabulary, regional idiosyncrasies and dialect can now be compared using computer programs. This analysis is not as conclusive as handwriting analysis (which is why handwriting is generally avoided), but it's becoming increasingly sophisticated. The BKA has a database of extortion letters and action claims that the police use for comparison. In one blackmail case, the perpetrators tried to disguise the fact that they were native German speakers by making grammatical mistakes, but the cops were able to detect this because the authors correctly spelled difficult words. Write simple sentences, avoiding unnecessary use of foreign words or jargon from your professional field. Vary the spelling of dates, abbreviations, and similarly distinctive references. An investigation into the alleged members of the "militante gruppe"[11] demonstrated that the police substantially cross-compare the content of action claims. Keywords

[11] *N.T.P. note:* The militante gruppe (mg, *militant group*) was a German far-left militant group active from 2001 to 2009.

and even slogans that appear in other texts—even publicly signed ones—are used by investigators to sniff in certain directions.

Even simple software that only statistically examines which are the 30 most frequently occurring words (or groups of words) in a text can already recognize similarities to other texts. The more comparative text material is available, the better the method works. Everyone who doesn't consistently encrypt their emails has already provided enough text material for a comparison sample.

Proofread your texts collectively and take turns writing them. This not only prevents specialization, but also protects you because everyone has their own individual writing style. In the best case scenario, the texts cannot be directly attributed to one person. Write only the bare minimum. The shorter the text, the less material you give the cops.

Shopping

Don't drive your car or bike into the store's parking lot, but park somewhere else, out of the view of cameras. Of course, do your shopping without networked devices such as smartwatches, cell phones, tablets, or other wireless devices. Leave your Bluetooth headphones at home too. Remember to remove your watch and rings before shopping, and only pay in cash, if you pay at all.

It has become very difficult, sometimes even impossible, to go shopping without being recorded by cameras. All hardware stores, supermarkets and drugstore chains use surveillance cameras to record people, and not just for 48 hours, as we've seen in some criminal proceedings. This makes it all the more important to a) change your appearance while shopping, b) do your shopping as far in advance as possible before the action and c) spread out your shopping locations, choosing ones that are farther away from the action location. Storing with people who are (presumably) not on the cops' radar is worth its weight in gold.

It makes sense to plan out your purchases. For example, we wouldn't buy firelighter cubes together with cleaning cloths at the same hardware store, as they are both used to construct the incendiary device. If the device ignition fails and it is found later on, the fiber traces will lead to exactly these cleaning cloths (the specific batch cannot be determined, but the brand and the manufacturer can be). A possible LKA / BKA inquiry will then ask: who bought these cleaning cloths from the five major hardware chains in the last two months, along with other items such as X brand of glue or Y brand of firelighter cubes? Such inquiries are not uncommon, especially at hardware stores, even at the scale of all of Germany. If such an inquiry returns a list of tens of thousands of purchases nationwide, with the exact time and potentially surveillance footage of the checkout area, this can be used to compare faces from the footage with the biometric passport/ID databases, which provides a long list of names (even if the identification doesn't work properly). Then, this list is checked for matches with people on the radical left known to the police. This process probably

takes a few days of investigative work, but it is not an effort that needs to be spared due to limited resources.

Therefore, if a component cannot be obtained without being recorded by a camera (e.g. in smaller stores) or abroad, then we should go shopping with fake glasses (which we don't use at any demos) and a cap (which covers all hair). Another option is a baseball cap with a wig made from real hair. Tampons can be used to reshape the cheek area (you will then be unable to speak properly!) and makeup can be used to create a different appearance for manual analysis of the surveillance footage. The prolonged period of the pandemic is currently "helping" us to go shopping inconspicuously while wearing face masks and gloves.

Look for items that are fully shrink-wrapped or whose packaging is closed. Otherwise, there is still a risk of leaving behind DNA traces on the item because cleaning is never 100% reliable (see the section on DNA traces, p. 13). If you buy small items, such as a few boxes of matches, ask the cashier for a bag. If your hands are already full with your money or other items such as an umbrella, it looks normal to ask the cashier to bag your purchases for you. Then, your prints and DNA will not be on the matchboxes. This will make building the device much easier later on.

Purchasing checklist

- The earlier, the better
- The farther away, the better
- Camera-free if possible; otherwise, visually "altered"
- Without Wi-Fi / Bluetooth devices
- Do not park at the store
- Packaged items are preferred
- Ask for a bag for small, unpackaged items
- Pay attention to discreet batch numbers on purchased items
- Pay only in cash, and destroy the receipt

Get accelerant casually

Buying gasoline or diesel on foot or by bike is too conspicuous. Too few people do that. It's easy for the cops to scan the gas station surveillance footage for exactly this behavior of filling spare fuel canisters without a car. Therefore, we should ask a friend with a car to fill up a spare fuel canister the next time they fill up at a gas station (preferably as far away from the action location as possible).[12] Only bring one canister per trip to the gas station, anything else is conspicuous. Many people wear disposable gloves when filling up, so doing the same is not unusual.[13] Place the canister in an unused shopping bag in the trunk to transport it without prints and with minimal DNA. However, before filling the PET (polyethylene terephthalate) bottles later on, we nonetheless still clean the canister with bleach-based cleaning agents.

PET bottles

PET bottles can be purchased clean in a half-wrapped six-pack. However, carry out an inspection first: make test purchases of bottles from different manufacturers and check them closely to ensure that no batch numbers are stamped or embossed on the bottle wall or lid. Sometimes, these imprints are hidden under the bottle label or inside the lid under the rubber seal. If the batch number is printed on, test whether it can rubbed off with a cloth and acetone (found in painting supplies or hardware store) without leaving residue. A batch number enables investigators to determine the approximate date of purchase, supermarket chain, and region.

---

[12] *T.N.:* See "Threat Library: Forensics > Arson"[a] for information on the theoretical capacity of investigators to determine at which gas station an accelerant sample was purchased. To mitigate this, you can: "Make the identification less likely to be effective by using a mix of accelerants of the same type coming from different sources (e.g. gasoline from different gas stations)."

[a] https://notrace.how/threat-library/techniques/forensics/arson.html

[13] *T.N.:* It is debatable whether wearing gloves in this way looks out of place—it is also possible to simply transfer the accelerant to a clean container afterwards, in a more private setting.

A Clean Construction

Note from the No Trace Project: In this section we have omitted a few sentences which were outside the scope of our project. We have replaced the omitted sentences with "[omitted]".

A clean room is required for constructing incendiary devices.[14] Ideally, it should be a room that is not associated with you AND that you haven't yet contaminated with your DNA by entering without protective clothing. For example, you could use a (basement) room of distant friends or an apartment rented (by someone else) in which you keep one room "clean" and only enter it in protective clothing. Since you will look like you just landed on the moon, you have to make sure that no neighbors can see you!

Depending on the security level, it is possible to use a section of an unclean room completely covered with plastic drop cloth (sold for painting) or a new tent (ideally at standing height). You can only enter this section via an "airlock" once you are already wearing clean protective clothing.

In both cases, there is an inside and an outside. Ideally, there should be two of you, since it is difficult to change into clean clothes and remove the clean ingredients from their "contaminated" outer packaging as a single person.

1) Getting dressed

Both people wear long-sleeved shirts and pants (even in the summer) and keep all the necessary (still packaged) materials outside the clean room / area. The "outside person" gets dressed there first: they put on latex gloves,

[14] *T.N.:* This is also debatable. In our view, a clean room is a good idea when the construction of an incendiary device involves a significant amount of time and physical manipulation (and indeed, the designs (B), (C), and (D) in the following section do require both), but a clean room is less necessary for incendiary devices which can be assembled quickly and simply. For a method of minimizing DNA contamination which is less extensive than setting up a clean room, see the description for incendiary device (A).

then a balaclava or bathing cap, and then new latex gloves. They use the gloves to put on a fresh painter coverall suit. The future "inside person" can assist by opening the packaging while wearing latex gloves and, holding out the opened packaging to the "outside person" while being careful not to touch the inside. Putting on the suit requires some practice, given that neither legs nor sleeves should touch the ground. It helps immensely if the future "inside person" (wearing a new pair of latex gloves) holds the sleeves and hood of the suit while the "outside person" climbs into the legs of the suit.

Then, the future "indoor person" opens the packaging of the dust masks and, without touching the mask(s), holds it out to the "outdoor person," who (wearing yet another new pair of latex gloves) removes the mask without touching the outer packaging, then puts it on. Finally, the "outside person" puts on new latex gloves yet again.

> The logic: gloves that have touched "DNA-contaminated" outer packaging or body parts should never touch the clean "contents" of the packaging. Take all individual steps slowly and carefully. It will happen that you find yourself thinking, "shit, now I should actually change my gloves…" And then you do, because you have given yourself enough disposable gloves and time. The job cannot be done conscientiously if you are rushed or don't have enough supplies!

Now, switch roles: The "outside person" who is already dressed assists the future "inside person" in getting dressed. This dressing also takes place outside, in front of the airlock to the clean room: put on latex gloves, put on a balaclava or bathing cap, and pull on a new pair of latex gloves. Carefully remove the painter coverall suit from the packaging (opened by the "outside person") and step into the suit legs—while the "outside person" (with fresh gloves) holds the sleeves. Close the zipper carefully, as the suits tear easily. If you will be working near the floor of the clean room or storing clean items near the floor, you will also need shoe covers (which are sold for painting).

Put on a new pair of latex gloves and take a dust mask out of its packaging (without touching the packaging), then put it on. Put on new latex gloves and then long-sleeved dishwashing gloves—done.

> Important: For a (bathroom) break, you must change your clothes completely. So make sure you bring several suits and masks for this purpose.

How do I put on new gloves?

1. Remove the first glove without letting it touch the packaging, grasping the glove only by the lower edge of the "sleeve" (not by the glove fingers!)
2. Take the second glove out of the packaging with your freshly "gloved" hand, again without letting it touch the packaging! When putting on the second glove, make sure the first glove never touches the second hand/arm. To accomplish this, overstretch the glove considerably.
3. In this way, your DNA will only be on the edge of the first glove (and of course on the inside of both gloves).
4. Before working with any materials that could be recovered at the action site, a pair of (dishwashing) gloves with the longest possible arm is pulled over the latex gloves. There should be "no" DNA on the outside of this second layer of gloves.

2) Set up the work area

For the "airlock", i.e. the entrance to the clean work area, you can use a "dust barrier" plastic entrance, which is available at stores that sell painting material. It consists of transparent plastic with a central zipper and can be stuck to a door frame. Alternatively, you can make a substitute with two hanging plastic sheets—the "outside person" opens their packaging and the "inside person" tapes the sheets to the door frame with clean masking tape without touching the door frame directly.

From now on, the "inside person" will stay inside and be "handed" everything through the airlock. Inside, the floor and all work and storage surfaces are generously covered with plastic sheets. You can use clean paper towels as a base for the immediate construction area. Place several (clean) garbage bags inside as well. You can sort the waste into "indifferent," "hot," and "particularly hot" to make disposal easier later on.

3) Hand through all the necessary materials

The "outside person" wears latex gloves to tear open the packaging of the necessary materials without touching the contents. They hold the airlock open and extend the opened package into the clean area to do this. The "inside person" does not touch the DNA-contaminated packaging, but rather removes the contents with clean dishwashing gloves and places them on the storage surface.

This is not possible with all materials. For example, the boxes of matches could have been touched by the sales clerk. In this case, the "inside person" opens the box and pours its contents onto an area of the work surface. Of course, the gloves must then be changed.

4) Constructing the igniters

Constructing the igniters takes time. [omitted] During this process, the "outside person" can help to discuss things from outside if anything is

unclear. The following section of this booklet contains three recipes for non-electric igniters with a delay time ranging from five to 180 minutes.

5) Disposal

Ideally, the pre-sorted waste should be disposed of far away from the future action location and spread over several garbage cans not in close proximity to each other. Do not dispose of anything contaminated by your DNA (such as gloves or the painter coverall suits) together with "obvious" materials like leftover matches or firelighter cubes.

We even recommend NOT to dispose of leftover matches TOGETHER with the firelighter cubes or the glue tube, but rather to dispose of the items individually in smaller garbage bags. We recommend wearing gloves when handling these garbage bags. If wearing gloves would be too conspicuous at some chosen disposal locations, then pour out the smaller garbage bags containing the "particularly hot" contents into the garbage bin, then dispose of the empty bag somewhere else.

Large residential complexes with publicly accessible garbage bins are ideal for "anonymous" disposal. Dispose of everything BEFORE you take action. Ideally, garbage collection will take place before the action date, as it has happened several times that the cops have searched the garbage bins in the vicinity around the action site.

Because of what was described in the sections on DNA traces, p. 13 and material traces, p. 41, you should not dispose of the items or clothing from the action itself too close to the action site! The mantrailer could track down the location. Especially if you are working with a longer delay, you can "treat" yourself to a longer journey to the disposal site.

6) Filling up with fuel

It's not a good idea to pour large quantities of fuel in a rented apartment with neighbors who share a wall. You will need a stand-alone house, a basement room (where you will not be disturbed by neighbors), a barn, or a garden shed without direct neighbors—or, if necessary, a section of

forest where you have never been before. Essentially, the enormous odor nuisance and your strange appearance are real obstacles. In the past, people have been busted because attentive neighbors saw them wearing gloves (and face masks). If you can't work with painter coverall suits in such a wooded area, then get some unused and one-use clothes with long sleeves and long pant legs.

Clean PET bottles can be obtained in half-wrapped six-packs. You will need a clean funnel, clean cloths, as well as bleach to clean the filled bottles afterwards.

It is also advisable to work in pairs for this step: one person holds the accelerant canister and pours while the other person holds the bottles. [omitted]

You need:

- 2 x 100 pairs of thin latex gloves (disposable)
- 4 x pairs of dishwashing gloves (preferably with longer sleeves)
- 6 x painter coverall suits (impermeable and preferably XXL)
- 4 x packages of thicker plastic sheeting (sold for painting)
- 6 x large cloths or paper towels for use as a work surface
- 1 x "dust barrier" plastic entrance or two additional pieces of plastic sheeting
- 1 x clean roll of masking tape
- 6 x pairs of shoe covers (sold for painting)
- 10 x 60L garbage bags
- 20 x 10–25L garbage bags for packaging the finished device(s)

…as well as other materials specific to the incendiary device design (see the following section).

This brochure attempts to [present] working methods that make clandestine militant action conceivable and feasible [...] despite the ever-expanding capabilities and powers of the investigating authorities.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.