Science and Justice, Volume 59, Issue 5, September 2019, pp. 565-572
DOI:10.1016/j.scijus.2019.06.004

# When finding nothing may be evidence of something: Anti-forensic and Digital Tool Marks

**By Graeme Horsman and David Errickson**

## Abstract

There are an abundance of measures available to the standard digital device users which provide the opportunity to act in an anti-forensic manner and conceal any potential digital evidence denoting a criminal act. Whilst there is a lack of empirical evidence which evaluates the scale of this threat to digital forensic investigations leaving the true extent of engagement with such tools unknown, arguably the field should take proactive steps to examine and record the capabilities of these measures. Whilst forensic science has long accepted the concept of toolmark analysis as part of criminal investigations, 'digital tool marks' (DTMs) are a notion rarely acknowledged and considered in digital investigations. DTMs are the traces left behind by a tool or process on a suspect system which can help to determine what malicious behaviour has occurred on a device. This article discusses and champions the need for DTM research in digital forensics highlighting the benefits of doing so.

**Keywords:** Digital Forensics; Anti Forensics; Digital Tool Marks; Investigation; Crime

## 1 Introduction

Whilst forms of digital data now play a role in the investigation and policing of many criminal acts, there is increasing concern surrounding the use of tools and processes which may hamper the effectiveness of any examination methods designed for this evidence type. This view was expressed recently by The Parliamentary Office of Science and Technology in the United Kingdom.

> 'Some criminals are aware of the techniques available to law enforcement and try to hide their digital activity. The processes they use, known as anti-forensics, tend only to occur in the most complex cases.' (The Parliamentary Office of Science and Technology, 2016 at p.3).

Similar assertions were also made by Pajek and Pimenidis as early as 2009 who indicated that 'in many cases investigation with such countermeasure techniques in place appears to be too expensive, or too time consuming to carry out. Often a case can end up being abandoned and investigators are left with a sense of personal defeat' (Pajek and Pimenidis, 2009 at p.145). Any course of action which prohibits the effective investigation of a criminal act will naturally instill concern in the digital forensic (DF) community (and indeed any forensic science community), yet it remains relatively unknown (a position which is likely to persist) as to the extent of use of such measures. Media coverage of so-called anti-forensic (for simplicity the term 'anti-forensic' will be utilised until further analysis in Section 2) measures in the DF field remains minimal, perhaps a by-product of the use of these processes; effective anti-forensic measures may never be detected in order to raise the hypothetical alarm. Further, there is little empirical research demonstrating evidence covering current so called anti-forensic tool usage and perceptions, as well as an assessment as to the extent of public and criminal engagement with privacy enhancing tools for anti-forensic purposes. Whilst limited evidence justifying concern maybe available, this alone should not be grounds for overlooking the threat posed by applications and procedures designed (or as a consequence of their use) to frustrate a DF investigation.

Published by Elsevier. This is the Author Accepted Manuscript issued with: Creative Commons Attribution Non-Commercial No Derivatives License (CC:BY:NC:ND 4.0).
The final published version (version of record) is available online at DOI:10.1016/j.scijus.2019.06.004. Please refer to any applicable publisher terms of use.

In the wider discipline of forensic science, ‘tools’ are often utilised by criminals to gain a mechanical advantage in many forms of illicit activities. This tool will leave impressions in a surface, and is often referred to as trace or impression evidence. For example, the use of wire cutters could be used to gain access to a property. As a parallel to DF, in routine crime scene work, the crime scene investigator (CSI) is often limited for time, yet it is paramount they draw upon their knowledge, experience, and interactions with others to identify meaningful trace evidence (Wyatt 2013). Failure to locate locate and recover impression evidence can be unforgivable (Bodziak 2000), and in turn prevent a full forensic analysis which will certainly misdirect the interpretation of events that occured. As a result, much as been published on the recovery, reliability and identification of physical toolmarks in forensic science (Refer to: Nichols 2018). However, in the field of DF, comparable research is sparse.

In 2016, Conlan, Baggili, and Breitinger offered comment on the requirement for DF to invest effort in the further examination and evaluation of the threats caused by techniques which obstruct DF processes. Such a sentiment was also offered by Al Fahdi et al., in 2013. The need to increase research activity in the anti-forensic area stems from the potential for those practitioners encountering such processes within an investigation failing to fully understand the impact they have had on a device under investigation.

The potential impact of under-researched anti-forensic processes is threefold:-

1. Failing to detect anti-forensic process usage on a system may prevent an effective investigation of both the local device being carried out and crucially, external sources of information. For example, tools removing suspicious Internet related content may cause a practitioner to assume no illicit activity has taken place. As a result, potential further sources of external evidence such as retained Internet Service Provider (ISP) logs or other external service data may never be requested and queried in order to identify the true extent of a criminal act.
2. Under researched anti-forensic procedures may lead to missed forensic opportunities where tools and procedures may leave behind ‘digital tools marks’ (discussed in Section 3) on a system which describe the functions it may have performed, offering indications as to what data has been tampered with.
3. Under researched anti-forensic procedures provide a barrier to establishing the true capability and effectiveness of these features, which in turn prevent any limitations and weaknesses being exploited for the purposes of evidence recovery.

This work seeks to emphasise the need to take note of processes which can disrupt a DF practitioner’s ability to accurately recover and interpret digital data. Section 2 begins by examining the correctness of current definitions of ‘anti-forensics’ (AF) in relation to DF and seeks to redefine the threats posed by this area. Section 3 introduces the concept of digital tool mark analysis, an under-researched area in DF. Finally, section 4 examines the challenges and areas for progressing this area of research.

## 2 Discussion

We are firmly within a technology driven era with digital devices documenting many aspects of an individual's’ life both passively and intentionally. Consequently, this digital data can often support the effective investigation of a criminal act should one take place, providing this

information can be both accessed and its reliability determined. The issue remains that this cannot be guaranteed in all cases. There is no doubt regarding the ability of digital evidence to enhance the policing of crime (with digital evidence featuring prominently within many digital crimes), yet its volatile nature means that its destruction and tampering in some cases can be attained with arguably relative ease. With societal shifts towards greater emphasis being placed on digital privacy and data protection, and, the use of privacy enhancing technologies to achieve these goals, concerns should be raised over the potential for an increasing number of seized devices to have retained less potential relevant digital content. Often measures which impact the presence and accuracy of digital evidence on a device are placed under the umbrella term of AF, a term which arguably misrepresents the threat posed in this area for DF and one which requires further analysis.

### 2.1 Anti-Forensics

AF is a term often adopted in DF to describe any procedure involved in the removal or degrading of the reliability of a piece(s) of digital evidence which a practitioner may expect to find or rely upon on a hypothetical standard device. Despite such a definition capturing the use of AF tools, it also subsequently describes an act which can be achieved via a number of processes which are standard to many operating systems and devices, coined here as 'disruptive technologies' - those which as a by product of their use can negatively impact DF processes. A problem with the term AF is that it is used to arbitrarily categorize all software and hardware which at any given time thwarts DF investigatory processes, regardless of intention and malice. Whilst there are tools designed specifically with the goal of being AF, this can also be achieved as a by-product of many legitimate privacy enhancing software features, for example private browsing modes which may reduce the presence of Internet browsing history on a system (Said et al., 2011; Marrington et al., 2012; Chivers, 2014). The issues surrounding the defining of AF can be seen in the work of Al Fahdi et al., (2013) who note that 'arguably both encryption and steganography are a form of Anti-forensics'. We suggest this is not wholly accurate. Despite both techniques potentially forming part of an AF process, they are not always AF *per-se* and both techniques may be utilised in legitimate privacy and security enhancing ways or with the intention to do so. A person's *mens-rea* is important when trying to establish AF context and to be AF, both techniques must be utilised in an intentional manner, and with the intention for their use to be AF. In absence of this intention, there is a risk that any function or process which manipulates digital data in a manner which negatively impacts a DF investigation is classified as AF.

The need for intention when correctly asserting the AF definition on a tool or process lies with the fields definition. Forensics is defined as 'the methods of science to provide information about a crime' (Cambridge Dictionary, 2018a). The addition of 'anti' ('opposed to or against a particular thing or person' (Cambridge Dictionary, 2018b)) results in a process with an insinuated intention as being 'against something'. The need for intention is key to distinguishing between a true AF process and one which is simply disruptive to forensic methods. This is acknowledged by Kessler (2007, p.1).

> 'anti-forensics is that set of tactics and measures taken by someone who **wants** to thwart the digital investigation process'.

Whilst AF tools and procedures provide a threat to DF, they do not solely pose an issue. Many AF definitions as too narrow, omitting to capture those processes which regardless of

intention, are disruptive to DF methods. Park et al. (2017 at p.31) offer a definition which covers to a greater degree the threats posed by technologies in this area.

> 'Anti-forensics, whether intentionally to disrupt investigations or simply an effort to make a computer system run better, is becoming of increasing concern to digital investigators.' (Park et al., 2017 at p.31).

The above definition provides an all encompassing coverage of acts which may disrupt the process of extracting and interpreting relevant digital content during an investigation but is arguably not wholly accurate. Rightly, the intention of a user is highlighted where to be AF, there must be an intention to disrupt the forensic investigation process. The issue remains with the latter suggestion of *'simply an effort to make a computer system run better*' being capture within the AF definition. Such acts cannot be AF if the user's initial intention was to enhance system performance and as a result of such processes, data which would have been useful during a DF investigation is compromised. Further, many performance enhancing processes are not designed to be AF, but '*performance enhancing*'. A tool not designed for the purpose of AFs cannot be an AF tool. However, such processes can be used in an AF manner, for example where standard procedures such as a 'disk-defrag' can be purposed for AF (reducing the potential for file recovery) as well as for legitimate performance enhancing abilities. Similarly, acts which simply adopt privacy enhancing technologies (PETs) as part of standard computer operations which have a byproduct of removing content from a system which would (should a crime be committed) be beneficial to an investigation cannot fall directly within this category. The original purpose of many PETs is for security and privacy, not to be AF, albeit it may be possible to utilise them in such a way.

Being AF is a mindset, and whilst there are dedicated AF tools, these tools are not the only way to be AF. Arguably AF is a term which can only be applied to a narrow set of applications which market themselves as for the purpose of combating forensic processes. Such tools are designed with the intention of removing content from a device which may lead to the prosecution of an individual who has carried out a criminal act. However these tools do not form the entirety of the risk posed in this area of DF. It is argued that the following two categories of threat persist in regards to the area of compromising DF processes:

Category 1: Dedicated AF tools.
Category 2: 'Disruptive Technologies'.

**2.2 Categories of Concern**

In 2009 Delp et al., stated that 'there is an abundance of readily available AF tools that can be used to mask or erase present digital evidence'. Whilst arguably there are many tools capable of tampering with potential digital evidence, it is an oversimplification to classify all as AF. The field of DF must acknowledge that a threat is posed by both dedicated AF technologies (Category 1) and passive disruptive technologies (Category 2); processes requiring an AF mind-set in order to be classified as malicious.

**2.2.1 Category 1: Dedicated AF tools**

For simplification of arguments, those tools designed for AF purposes can be typically placed in one of the the following six classifications.

1. *Data hiding*: Data hiding techniques are designed to place digital content beyond the discovery of an individual (unlike obfuscation where content may be present but non-intelligible) (Sabir et al., 2018). Data hiding may arguably be the weakest of the anti-forensic techniques available to a potential offender given the forensic capabilities available to many DF practitioners. To provide a contextualised example, a standard desktop computing device often permits full physical access to the digital media and ultimately it's operating system. Successful data hiding may rely upon placing content in uncommon system locations or relying on simply techniques of file name and extension changes (as any additional obfuscation techniques are likely to fall with categories 3 and 4 of this list). In such cases, for data hiding techniques to be successful, reliance is placed on the weakness of the investigating practitioner and their likelihood to overlook content (or through lack of knowledge) or fail to process this information with the necessary techniques (file signature analysis, appropriate file filtering/sorting etc.) to prevent content being missed.
2. *Data removal*: Data removal (terminology interchangeable with 'wiping') techniques are designed to place target information stored on digital media beyond the powers of recovery of DF techniques. Whilst standard file deletion does not achieve this by default (albeit sustained usage of a device leading to data being overwritten may have a similar effect), data removal involves the intentional and timely removal.
3. *Data obfuscation*: Obfuscation is a broad term which in the confines of DF is used to describe the use of algorithms and techniques (encryption, compression) to obscure data, making it unintelligible until specific access protocols are initiated. This may be as simple as supplying the correct authentication credentials to decrypt data. What distinguishes obfuscation methods from removal, is the ability to reverse obfuscation methods to ensure that data is retrievable by the correct person. The aim of obfuscation methods is to provide access to content only to those who have be predetermined.
4. *Data manipulation/editing/masking*: Examples include GPS Spoofing (Barton and Azhar, 2017). These methods take existing and meaningful data which a practitioner could use to reliably describe a set of events on a system and change it. If changes are detected, the reliability of event reconstruction if knowingly compromised. If such processes are undetected, erroneous examination results may be acquired.
5. *Data adding*: Often focus in relation to AF tools lies with the removal of a user's incriminating interactions on their system. However, there are tools which may seek to introduce incriminating evidence (Garfinkel, 2007).
6. *Physical destruction*: Physical destruction is a traditional AF methods and relies on a threshold of destruction being reached which places a device beyond the powers of specialist digital device recovery. Such techniques may be effective when local device storage is involved, yet with an increasing amount of data being stored remotely by service providers, physical destruction alone may not always be an effective anti-forensic technique.

### 2.2.2 Category 2: Disruptive Technologies

The second category of processes are defined as 'disruptive technologies' (See Figure 1). Disruptive technologies have a primary legitimate function and purpose, which may also have a detrimental impact on relevant digital data on a device in any subsequent investigation. An example of such an issue would be the use of a disk defragging utility, a process of reducing file defragmentation to improve the efficiency of a system drive (Microsoft, 2016). This feature

is non-AF, yet its use can impact the recoverability of data found in unallocated regions of a disk. As a result, any tool or process of this type is categorized as a disruptive technology which can be used anti-forensically. The tool itself is not AF, but subject to identifying the requisite intention of a suspect, it may be used in an AF manner. This raises an issue within the context of a DF examination - '*what distinguishes a malicious defrag from a normal one?*'.

The challenge with disruptive technology usage in a DF investigation is twofold:

1. Detecting that a disruptive technology has been utilised in a particular instance, given their function is legitimate system activity which in some cases may be difficult to distinguish from typical user behaviour.
2. Detecting that a disruptive technology has been used with the intention to be AF, distinguishing their use from instances such as genuine privacy or performance enhancing acts.

Whilst the former may be possible, the later challenge of establishing malicious disruptive technology usage is arguably impossible in many cases. Where a suspect has utilised a disruptive technology, the challenge is distinguishing genuine system maintenance or PETs usage from targeted attempts to remove potential behaviours documenting criminality from their system. The problem lies with establishing normal behaviours on a computer system - does a 'normal' (albeit there is no such thing) user defrag their disk every week? Utilise private browsing functions for every session? Encrypt their devices by default? There is likely no way to distinguish such actions and doing so risks undermine the conscientious user. Such acts highlight the difficulties with defining AF within DF.

As a result, it may not be possible in all cases to establish motive, but detecting disruptive technology usage in any case may help to explain the absence of, or assess the reliability of a piece of evidence on a given system. Whilst dedicated AF tools pose an issue, it is argued that the bigger threat is posed by the disruptive technologies available to many users through typical device usage which are enacted by a diligent user. Bespoke category 1 AF tools will always cause fear within DF, their enountered and documented use in a seized device is likely to be comparatively rare in comparison category 2.

Disruptive technologies can also be sub-grouped into three distinct areas for classification, notably PETS, operating system functionality and device functionality (See Figure 1).

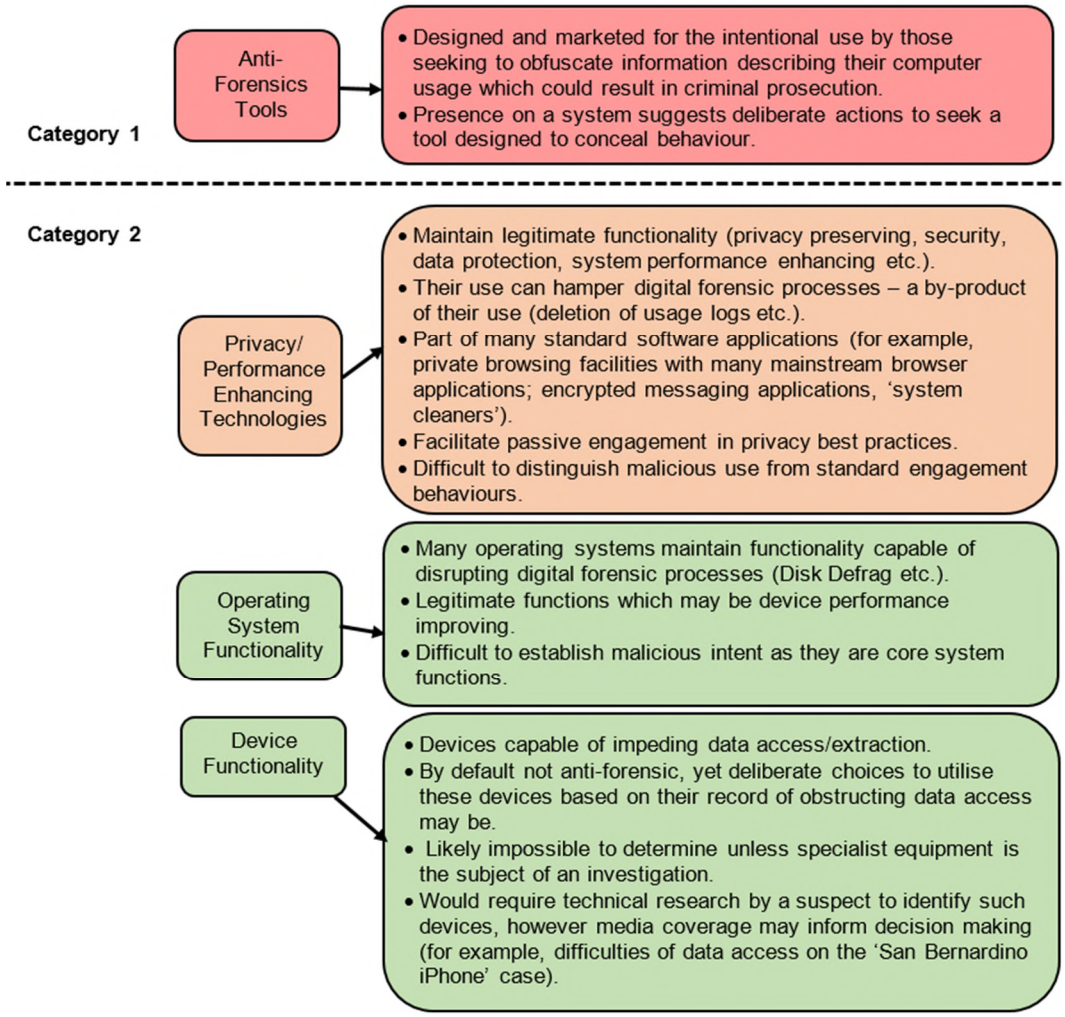



**Figure 1: A breakdown of Category 1 and 2 tools which may hamper DF investigations**

*A case study - The San Bernardino iPhone*: The San Bernardino iPhone provides provides an example of the difficulties of defining and investigating disruptive technologies. The scenario itself is briefly defined by Conlan et al., (2016) as follows.

> The FBI had to bypass anti-forensic techniques to acquire the iPhone 5C owned by the San Bernardino County, California government issued to its employee, Syed Rizwan Farook, one of the shooters involved in the December 2015 San Bernardino attack that killed 14 people and injured 22. The attackers died, but the iPhone 5C was recovered. It was **locked** with a **four-digit password hindering the forensic acquisition** process **due to built-in anti-forensic techniques** that **enforce encryption** and **auto-wiping** the device after **multiple unsuccessful password attempts**. (Conlan et al., 2016. p.66-67)

The issues such a description raises is that it assumes that both device passcodes and subsequent encryption and wiping are AF. This is not the case, but they can be used in an AF way. Arguably, the iPhone presents an example of a disruptive technology. Password protection, encryption and wiping on an iPhone device are designed for privacy enhancement and personal data protection, with many legitimate implementations including those stated by Apple themselves which include the future selling of a device to ensure all personal content

is removed (Apple, 2018). None of these processes are marketed for the purpose of AF by Apple. There are two approaches to analysing the San Bernardino iPhone case. The first is one of luck, and those involved were fortunate to collaborate on a device which at the time of the incident possessed significant investigatory issues. The second is that the device was researched and noted as a troublesome device to investigate due to its operating and device functionality (see Figure 1) and pre-selected intentionally as a disruptive technology to be used anti-forensically. Determining this mindset may not have been possible to establish in this case.

Regardless of which category a process falls into, practitioners are challenged with establishing their impact on a given case and any concerns around evidence recoverability and reliability. Given that DF investigations are often *post mortem*, practitioners are left to investigate the impact of a tool/process at which point the 'digital tool marks' (DTMs) left behind on a system may be crucial to determining what a user has carried out.

**3 Toolmarks**

The term 'toolmark' is a well established concept in the discipline of forensic science. For example, it is not uncommon for tools such as screwdrivers to be used during the undertaking of a physical crime when obtaining entry to a prohibited area (Baiker *et al* 2015). A screwdriver may be used to pry open a door, and due to the contact between the tool and the surface, the tool will leave specific characteristic impressions and marks behind. The recovery of this characteristic (a form of physical evidence) can help identify the type of tool that was initially used and in some instances identify the exact tool utilized. Similarly, in forensic archaeology, depending on the properties of the soil, toolmarks may be left in a grave, created by digging implements such as a spade or machine. As a result, these may be recovered from careful excavation processes and providing a link as to how the grave was initially dug (Hunter and Cox 2005). In addition, a fatal stabbing the analysis of a toolmark on the human body can determine the type of instrument that was used by the suspect (Norman *et al* 2018). Inevitably, all criminals use tools, however as Edmond Locard demonstrated, 'every contact leaves a trace'. Thus, once a toolmark has been identified at a scene or on a person, it is documented and in some cases recovered for further analysis. The documentation process utilises standard photographic recording and then depending on the size of the object or where the object is located, a silicone casting medium can be applied to copy the mark *in situ* (Dittmar *et al* 2015). The mark, or the silicone cast is then processed in the laboratory where its characteristics are examined and often compared to a replicated mark.

Normally the analysis is undertaken microscopically by comparing the mark against test impressions created by a suspected tool (Rowe 2014). There are three different characteristics that can be identified: class, sub-class, and individual characteristics (Baiker *et al* 2014). Class characteristics are determined before manufacture of the tool and possess global properties that are widely associated with the certain type of tool. The class characteristic is most useful in determining or refuting whether a toolmark was made by a suspected tool type (Baiker *et al* 2014). This can be subdivided into further categories such as whether the mark created had striations (microscopic parallel grooves), were compression / impression marks (an outline of a tool), or punctures (an outline of a tool, but may have striations associated with it), and therefore reduce the number of suspected tools in the identification process (Petraco 2010).

A tool's sub-class characteristics are described as, "*discernible surface features that are (1) produced incidental to manufacture, (2) significant in that they relate to a small group source (a subset of class to which they belong) and (3) arise from a source which changes over time*" (Baiker *et al* 2014: 187). Individual characteristics are most useful in specific tool identification because they are only associated with one tool. For example, the tool will change depending on how it is used. Therefore these changes, such as indentations, damage, and rust, are specific to that tool because each tool is used differently. As a result, the tool's mark left on a surface will be very different from a generic tool of the same class.

In forensic science, the methods for analysing tool marks are improving and although this aspect of the discipline has been surrounded by bias and subjectiveness in the past, newer statistical models using Bayesian and likelihood ratios are improving validation (Kukuchka *et al* 2017; Meuwly *et al* 2017). What is key to note is that forensic science have and continue develop and hone tool mark detection and identification techniques, benefiting investigation processes. Yet comparable advancements have not been made with regards to digital evidence with tool mark considerations being overlooked my academic research.

### 3.1 Digital Tool Marks

Similar to traditional tool mark analysis, it is possible that when a suspect attempts to interact with their computing system in a manner which may jeopardize the reliability and availability of any potential digital evidence, 'such techniques may leave traces that could alert investigators to missing evidence.' (The Parliamentary Office of Science and Technology, 2016 at p.3). These traces can be classified as DTMs (see figure 2).

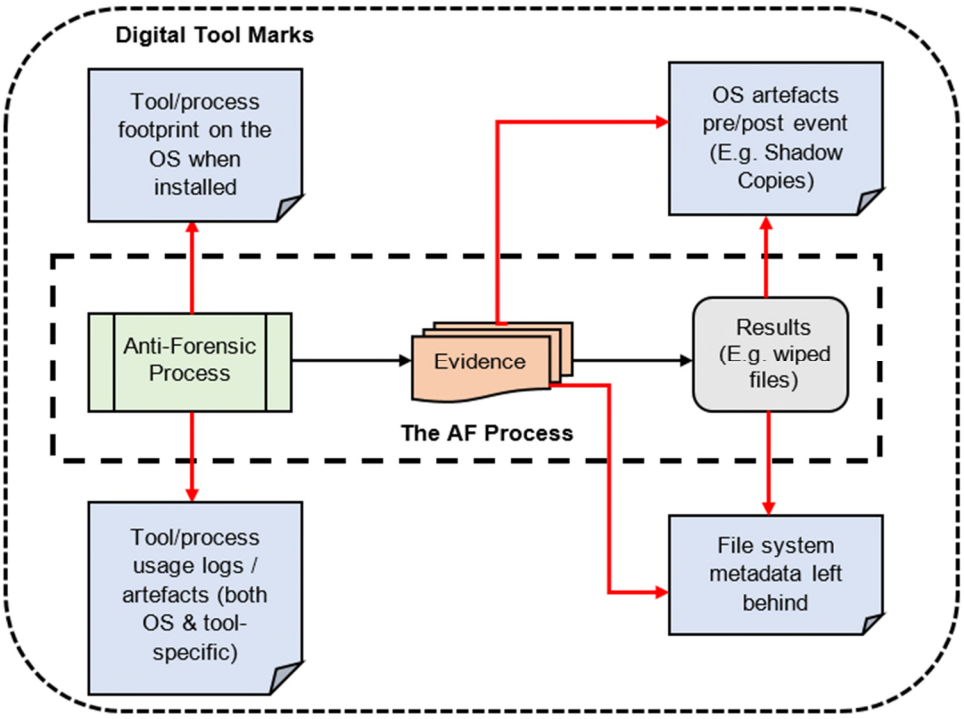



**Figure 2: Digital tool marks generated as a result of tool usage.**

When processes (either category 1 or 2) are initiated, their actions may leave behind information on a system which describes their usage for a given act. Examples include standard operating system usage files (e.g. prefetch, link files, executables), a tools specific

footprint on an operating system and its tool-specific logs and file system metadata as a result of its use.

Whilst those tools deemed wholly AF (category 1) are likely to try and ensure their DTMs are removed or are limited, this may not always be the case. Further, the challenge of category 2 processes lies with the fact that such usage may not be explicitly logged, particularly where the process used is a generic operating function for example, logs of historic disk drag usage may be limited. In this case, a DTM may be established via an analysis of the disk sectors for the purpose of evaluating contiguous file presences and fragmentation (or lack of). Identifying DTMs for a given tool/process offer the following benefits to the practitioner.

1. *Identify class of tool used:* DTMs may help to identify the type of tool used by a suspect (wiping, data obfuscation etc.).
2. *Identify the tool sub-class and individual characteristics*: Whilst in some cases, identifying the tool/process utilised will be possible due to its sustained existence on a platform (yet to be uninstalled), this may not always be the case. In such instances the practitioner may be left with the outcome of an AF event with the task of establishing both what has occurred and what has carried out an AF process. One of the key benefits of DTMs lies with the potential for them to be both unique and consistent, and therefore attributable to a specific tool/process. In addition, an identifiable tool/process may also have known limitations/weaknesses in regards to how it operates which may be important during an examination to ensure all available trace evidence is recovered and interpreted correctly post-event.
3. *Identify tool usage*: DTMs may indicate how a tool/process has been utilised on a system or even that a tool have been used at all. In the case of data removal a DTM may reveal the location or type of data which has been subject to removal. In turn, where data has been manipulated, DTMs may identify the data types which cannot be trusted as part of an investigation. DTMs may suggest that the absence or manipulation of data due to AF intent is indeterminate.
4. *Identify what it has done*: DTMs may reveal what acts have been carried out on a system. Marks may be bespoke to certain acts where for example secure wiping of files may alter specific file system metadata which is consistent with the act of wiping files using application ‘X’. In turn, DTMs might explain why certain evidence types cannot be found or interpreted in a manner which was to be expected.
5. *Effective resource allocation*: Although it is dangerous to assume that certain content may or may not be available without verifying this, in some cases, DTMs may allow a practitioner to effectively allocate their available investigation resources. For example, where a known strong encryption algorithm is used, a decision to abandon attempts to gain access may be taken to prevent case delays where a chance of success is minimal.

### 3.2 An Example:- Private Browsing

To provide an example, the simple scenario involving the initiation of a private browsing (PB) functionality (classified as a disruptive technology (category 2)) is offered (see Figure 3). Whilst PB does not completely preclude the chance of browser evidence recovery (for example, memory forensics and related memory artefacts may capture some browsed content), its core functionality of trying to prevent browsing session data from being locally stored on a device increases the potential for reduced evidence recovery. Even if a PB mode

simply operates a basic file deletion protocol of notable session data files following the closure of a PB session (see reportes of early PB implementations), natural overwriting of data pose a threat to evidential recovery. Often research establishes a primary goal of determining the effectiveness of a PB session. In the case of PB, this is often through the development of testing which aims to establish whether browser information can be recovered for the period of activity subject to PB. The success of a PB session is often determined by the ability to recover relevant content following an investigation.

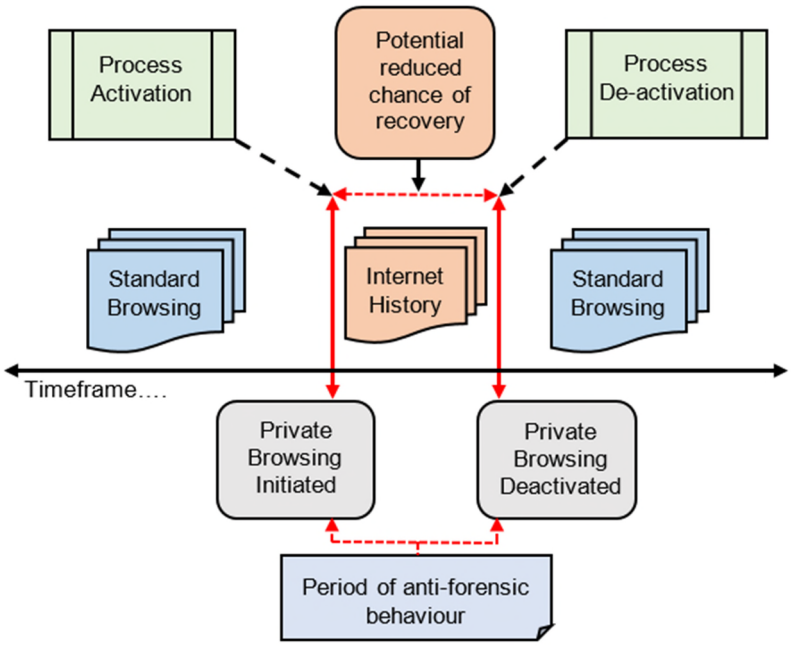



**Figure 3: Demonstration of a private browsing process.**

However, research often lacks consideration of any evidence denoting the frequency of use of the PB process itself. In the context of PB, this facility can be initiated multiple times throughout the course of a day in amongst times when standard browsing activity is also taking place. Determining the frequency of a PB event and the length of time of its initiation may provide a greater understanding of a suspect's usage of their device. If it can be established, both the activation and deactivation times of a PB process can help to provide reasoning behind the absence of a set of browsing data which a practitioner may expect to find as part of their investigation. If a PB process can be mapped against periods of 'data absence', a distinction can be made between data removed subject to an intention to be AF, and simply assumed periods of inactivity on the device itself. In doing so, establishing the frequency of use of PB provision may also inform future forensic procedures such as approaching external sources of potential evidence such as Internet Service Providers and their retained content. Take for example those subject to supervision orders (see for example measures taken for offences related to sexual offences, hacking etc.) requiring consistent checks of their Internet browsing history. It remains feasible that all illicit browsing is confined to a PB session which may be prohibited as part of an order. Whilst evidence of the browsed sites may be gone, establishing any evidence of PB DTMs may be sufficient to acknowledge a suspect has breached their supervision order.

## 4 Moving Forward

The concept of DTM analysis should not be confused with that of anti-anti-forensics (AAF), as a sub-discipline of DF covering a set of techniques and measures designed to counteract the operation and results of AF tools (mooted within the call for papers of the popular DFRWS (2019) conference). Whilst some procedures can be subject to AAF (for example, malicious encryption cracking), the term AAF does not accurately describe DTM investigation. DTM research focuses on reverse engineering leftover system data to determine any AF intended tool usage.

The move towards research focused on DTMs is one which should be viewed as a proactive one. As a discipline, the presence of recoverable data from a system should not be the only determinant of success in an investigation and we need to be able to identify when an individual has taken steps to disrupt investigatory purposes. Whilst establishing an intention to be AF will always provide a difficulty, DTM research should provide practitioners with a greater chance of identifying when something has attempted to disrupt or compromise digital content and the data subject to such procedures. DTM is a new and under researched area of DF and this work calls for a need for such work to be carried out. At the time of writing, there are no published works dedicated to DTMs in the context of a DF investigation. Whilst many publications document the success or failure of AF techniques, few consider their footprint from use.

Although the concept of AAF offers hope, it is naive to consider that its impact can be significant in a lot of cases. In some instances AAF is not possible, for example, where the overwriting of data is something which can be achieved with relative easy and is not reversible. As a result, the prevention of tackling of tools and procedures which potentially compromise digital data is likely unpreventable. Instead, focus should be turned towards the traces left behind by their usage in order to make sense of the available content left on a system post-event, yet achieving this is difficult.

### 4.1. How to capture this content:- A DTM Database?

Practitioners of forensic toolmark identification recognised the need to exchange information, best practices, and to further research in the discipline. To achieve this, The Association of Firearm and Toolmark Identification was created in 1969. This group has produced a number of resources including a specialist peer-reviewed journal, a glossary for common terminology, and they host annual training seminars (AFTE 2018). Similarly, a large number of publications have been produced on tool marks such as color atlases that form a reference database. For example, Petraco (2010) published a book which included rationals on decision making, instructions on methodological approaches, and reference images on tools and the marks that they produce. For DF practitioners to harvest the value of DTM it requires similar sustained initiatives which research into both category 1 and 2 processes and the tools available. Conlan, Baggili, and Breitinger (2016) provide a list of what they categorise as available AF tools. Whilst this provides an insight into the availability of this content, the next required step is to examine their DTMs created as a result of their usage. Collating this information into a single resource may support DF practitioners in their investigations for the reasons previously noted in this article.

*Bad idea?*: As with the sharing of any information in relation to the forensic sciences, it is not impossible for it to be accessed and utilised in a malicious way. Therefore arguably, a DTM database would have to have vetted access and be a non-public resource. As a result, it would

prevent those seeking to commit criminal acts from upskilling and identifying those tools which performance the best. Further, the resource should not be a resource for tool developers to hone their AF applications.

Assuming that DTM data should be investigated, collected, and stored, the question remains as to what should be recorded. This following is a breakdown of key information required:-

1. *Tool/process effectiveness*: An important feature of AF evaluation is determining whether a tool/process is successful in what it claims to do, and if not, to what extent it performs its functions. Evaluating the effectiveness of a process can ensure that investigatory resources and effectively implemented and a device is thoroughly investigated. For example, where a data hiding process is known to be reversible using protocol 'X', this may prevent practitioners from writing-off ever gaining access to this content under the believe that a utilised cipher may be too difficult to crack.
2. *Settings*: Distinguishing the default settings of a tool provides an evaluation of the threat it poses to an investigation. For example, a data-removal tool which by default simply deletes content and must be customised in order to securely erase content. Changes of settings to more complex AF measures can impart both knowledge and intent regarding the tampering of content and possible subsequent masking of an offence
3. *Operating system presence*: A tool/processes' footprint on a device and operating system should be mapped in order to identify what presence it leaves when operated. This must be completed for multiple operating system types and devices. In doing so, it supports the identification of such tools by an investigator, particularly in cases where a tool may seek to obfuscate its presence and could potentially be overlooked.
4. *Operating system interaction*: A tool/process must interact with a device's operating system in order to carry out its functions. This very act creates a trace within various operating system artefacts which are potentially recoverable by a practitioner. Whilst some tools may seek to remove this content they may not do so completely. Establishing the artefacts left on a system by a tool interacting with it may help to determine if a tool has been run and subsequently how it has run.
5. *DTMs*: It is also necessary to identify DTMs which describe the usage of a tool/process on a system. These describe the characteristics of a tool's usage on a system, for example, tools which amended file system metadata to a specific value when manipulating file data may be a DTM bespoke to tool 'X'.
6. *Tool implementation and metadata*: Application files should be hashed and stored to allow future identification of a tool in other investigations. Installer file metadata and hash values should be recorded. Tools version numbers and their course should be recorded.

**5 Concluding Remarks**

There is a need to examine and record the impact of tools which may disrupt DF inventory processes in order to support practitioners identify when a suspect may have taken steps to conceal illicit behaviours. Such work cannot be solely fixated on the concepts of AF, and a broader examination of all technologies capable of hindering a DF examination (captured within both categories of tool/process offered in this article) must be undertaken. In doing so, the field begins to develop a resource which can help to identify and evaluate both the capabilities of these tools and the characteristics of their usage on a system which can help

to both explain ‘missing’ data from a system or highlight content which may have had its reliability compromised.

**References**

AFTE (2018) What is AFTE? https://afte.org/about-us/what-is-afte [Accessed 03/11/2018]

Al Fahdi, M., Clarke, N.L. and Furnell, S.M., 2013, August. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In Information Security for South Africa, 2013 (pp. 1-8). IEEE. - their survey highlighted AF as a high priority area for research

Apple (2018) ‘iOS Security’ Available at: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf (Accessed: 12 October 2018)

Baiker, M., Keereweer, I., Pieterman, R., Vermeij, E., Weerd, J. V. D., Zoon, P. 2014. Quantitative comparison of striated toolmarks. Forensic Science International 242: 186-199.

Baiker, M., Pieterman, R., Zoon, P. 2015. Toolmark variability and quality depending on the fundamental parameters: Angle of attack, toolmark depth and substrate material. Forensic Science International 251: 40-49.

Barton, T.E.A. and Azhar, M.H.B., 2017, October. Open source forensics for a multi-platform drone system. In International Conference on Digital Forensics and Cyber Crime (pp. 83-96). Springer, Cham.

Bodziak, W. J. 2000. Awareness, Detection, and Treatment of Footwear Impression Evidence. In Bodziak, W. J. 2000. Footwear Impression Evidence (2nd Eds) 1-26; CRC Press: Florida.

Cambridge Dictionary (2018a) ‘Forensic’ Available at: https://dictionary.cambridge.org/dictionary/english/forensic (Accessed: 12 October 2018)

Cambridge Dictionary (2018b) ‘Anti’ Available at: https://dictionary.cambridge.org/dictionary/english/anti (Accessed: 12 October 2018)

Chivers, H., 2014. Private browsing: A window of forensic opportunity. *Digital Investigation*, *11*(1), pp.20-29.

Conlan, K., Baggili, I. and Breitinger, F., 2016. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital investigation, 18, pp.S66-S75.

DFRWS (2019) ‘Location’ Available at: https://www.dfrws.org/conferences/dfrws-eu-2019 (Accessed: 12 October 2018)

Dittmar J. M., Errickson, D., Caffell, A. 2015. The comparison and application of silicone casting material for trauma analysis on well preserved archaeological skeletal remains. *Journal of Archaeological Science: Reports* 4: 559-564.

Garfinkel, S., 2007, March. Anti-forensics: Techniques, detection and countermeasures. In 2nd International Conference on i-Warfare and Security (Vol. 20087, pp. 77-84).

Hunter, J. & Cox, M. 2005. Forensic Archaeology: advances in theory and practice. Taylor & Frances: UK.

Kessler, G.C., 2007, March. Anti-forensics and the digital investigator. In Australian Digital Forensics Conference (p. 1).

Kukucka, J., Kassin, S. M., Zapf, P. A., Dror, I. E. 2017. Cognative Bias and Blindness: A global survey of forensic science examiners. *Journal of Applied Research in Memory and Cognition* 6: 452-459.

Marrington, A., Baggili, I., Al Ismail, T. and Al Kaf, A., 2012, December. Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers. In *Computer systems and industrial informatics (iccsii), 2012 international conference on* (pp. 1-6). IEEE.

Meuwly, D., Ramos, D., Haraksim, R. 2017. A guidelines for the validation of likelihood ratio methods used for forensic evidence evaluation. *Forensic Science International* 276: 142-153.

Microsoft (2016) 'Ways to improve your computer's performance' Available at: https://support.microsoft.com/en-gb/help/17126/windows-7-improve-performance-defragmenting-hard-disk (Accessed: 12 October 2018)

Nichols, R. 2018. Firearm and Toolmark Identification: The Scientific Reliability of the Forensic Science Discipline. Academic Press: London.

Norman, D. G., Watson, D. G., Burnett, B., Fenne, P. M., Williams, M. A. 2018. The cutting edge - Micro-CT for quantitative toolmark analysis of sharp force trauma to bone. Forensic Science International 283: 156-172.

Pajek, P. and Pimenidis, E., 2009, September. Computer anti-forensics methods and their impact on computer forensic investigation. In International Conference on Global Security, Safety, and Sustainability (pp. 145-155). Springer, Berlin, Heidelberg.

Park, K.J., Park, J.M., Kim, E.J., Cheon, C.G. and James, J.I., 2017. Anti-Forensic Trace Detection in Digital Forensic Triage Investigations. Journal of Digital Forensics, Security and Law, 12(1), p.8.

The Parliamentary Office of Science and Technology (2016) 'Digital Forensics and Crime' Available at: http://researchbriefings.files.parliament.uk/documents/POST-PN-0520/POST-PN-0520.pdf Post Note Number 520 March 2016 (Accessed: 15 October 2018)

Petraco, P. 2010. Colour Atlas of Forensic Toolmark Identification. CRC Press: Boca Raton.

Rowe, W. F. 2014. Firearms and Tool Marks. In: James, S. H., Nordby, J. J., Bell, S. 2014. Forensic Science: An introduction to scientific and investigative techniques. CRC Press: London.

Sabir, M.F., Jones, J.H., Liu, H. and Mbaziira, A.V., 2018, March. A Non-Algorithmic Forensic Approach for Hiding Data in Image Files. In Proceedings of the 2nd International Conference on Compute and Data Analysis (pp. 60-64). ACM.

Said, H., Al Mutawa, N., Al Awadhi, I. and Guimaraes, M., 2011, April. Forensic analysis of private browsing artifacts. In Innovations in information technology (IIT), 2011 International conference on (pp. 197-202). IEEE.

Wyatt, D. 2013. Practising crime scene investigation: trace and contamination in routine work. Policing and Society 24 (4): 443-458.



https://dspace.org/

# When finding nothing may be evidence of something: Anti-forensics and digital tool marks

**Horsman, Graeme; Errickson, David**

**2019-06-03**
Elsevier
https://doi.org/10.1016/j.scijus.2019.06.004
Horsman G, Errickson D. When finding nothing may be evidence of something: Anti-forensics and digital tool marks. Science and Justice, Volume 59, Issue 5, September 2019, pp. 565-572

Downloaded from a DSpace repository. https://dspace.org/