Evidental Weight of Collected Data in Case of an Incident

Marian Svetlik

svetlik@df-pro.cz

Digital Forensic Licensed Expert
Institute for Digital Forensic Analysis
www.idfa.eu, info@idfa.eu
Pocernicka 168/1a
100 99 Praha, Czech Republic

Abstract

Based on my many years of experience it is evidentiary, that in solving security incidents in the IS, it is necessary to concentrate response in two basic directions. The first one is the elimination of incident, e.g. in accordance with ISO/IEC 27035. However, it appears that virtually every security incident (in the case of extensive interpretation) could be considered as a criminal offence, which is needed to be investigated using law enforcement authorities. For that, it is necessary to provide enough digital evidence. This is the second direction of the investigation of security incidents. Constantly increasing demands for their systematic investigation, e.g. in connection with the new security requirements and regulatory measures, for example. GDPR, additional demands on the skills of professionals in information security are on the place. One of the professional guidelines in the area of data security is also providing digital evidence about the incident.

It is obvious that in the process of the incident identification, the primary task of this is elimination and there is no time to invite the police to gather digital evidence in parallel, despite the fact that it would be often superfluous. Therefore, the obligation to gather digital evidence is logically shifted from the police to the owner of the data, respectively to CSIRT team, because ex-post gathering digital evidence by police probably does not bring relevant results.

CSIRT team members must be able and competent to gather and protect digital evidence in a manner that will be usable for any further investigations in cases where the incident spawns a criminal offence and thus the investigation moves into the plane of the criminal proceedings. Based on many years of practical experience in this paper will be formulated some rules that are recommended to use in gathering digital evidence in the event of an investigation of security incidents. Although some of the rules listed here may seem simple and obvious, experience shows that even this is often not respected. It will also be noted that the gathering of digital evidence requires

special knowledge, attitudes and devices, using which can significantly increase the evidence weight of gathered data.

Keywords: digital evidence, incident investigation, CSIRT, evidential weight, gathering digital evidence.

1 Problem identification

Process of the security incident investigations in the IT environment is defined in lot of well known sources, documents and standards.

It is necessary, however, to emphasize that virtually all of the recommendations and procedures for security incident investigations are focused almost exclusively on the technical solution to the elimination of the incident and the solution of related processes. Solving the technical and technological impacts and measures to prevent the recurrence of an incident are not enough for closing the case. Unfortunately, virtually none of the above recommendations and standard does not address the implications of parts, that are not technological in nature.

Each security incident raises the damage, it is an undeniable fact. The damage incurred in direct connection with the security incident and its solution, the direct and indirect costs of its identification, examination and elimination, are not subject to the above mentioned recommendations and standards and there are not usually placed procedures, methods and processes of their examination, identification, quantification and procedurally-legal investigation. Certainly, it is necessary to take into account, in particular, procedural (e.g. labour practices and regulations) are dependent from the local jurisdiction and, therefore, internationally accepted procedures and recommendations for their solution cannot be set universally.

However, in the investigation of any security incident, it is necessary to remember that the process of the solution cannot be limited only to the technological side of the case. As mentioned above, each incident causes damage that is not negligible. Even in our (Czech) criminal code can be inferred, that even a minor incident on a regular basis causes damage, which exceeds without problems the border of the crime.

Even in case of seemingly minor security incident, we must always consider the possibility that its range (usually without major problems) may grow into a criminal offence. The boundaries, when it can be solved internally, or when it is necessary to invite Law Enforcement bodies, is naturally dependent on local legislation and whether the owner of the infected/damaged assets has or does not have the obligation to involve Law Enforcement institutions.

To illustrate this, we will use a simple diagram that illustrates two parallel processes that are required to investigate a security incident. The upper process is generally known from the recommendations and standards (e.g. ISO / IEC 27035 [1]) and the bottom process displays a process-legal solution:

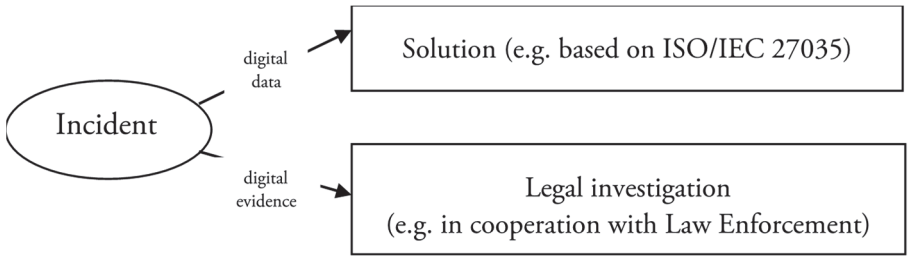

Figure 1: Parallel technical and judicial investigation of security incident.

It is probably obvious that for a lawful solution of an incident (labour law or criminal law), it is necessary to obtain, secure and correctly interpret the evidence on which such a solution is based. In the case of information technology, this is primarily digital evidence.

Both security incident investigation processes should, in the optimal case, run in parallel, immediately after the occurrence of the incident. It is obvious that, with time (sometimes even a few minutes, not to mention hours, days, weeks, or often even months), relevant information in information systems is rapidly extinguished (whether by the active activity of the attacker or by the normal activity of the information system itself).

For both processes, input is also important - digital data and digital evidence. At first glance it might seem that there is no difference between them. Digital evidence is, in fact, also digital data. But the difference here is. Digital evidence is a subset of a more general set of digital data and therefore has specific characteristics that distinguish it from general digital data.

At this point it is necessary to mention one potential misunderstanding that may result from the understanding of the essence of evidence, as defined in our (Czech) Criminal Procedure Code. Since I am not a lawyer, I will only interpret it in my own words: "*... everything which can help to clarify reality can be used as evidence...*" If so, then why do you want to separate from a (general) digital data a special set of digital evidence? I do not want to complicate the situation with passages from the theory of criminalistics about the factual, temporal, local and causal link of the criminalistics traces with the event under investigation or with the completeness and legality of obtaining evidence and other attributes.

In the field of information (digital) technology, compared to the ordinary material world, the situation is much more complicated. I do not need to emphasize to IT experts that almost any kind of intervention can be done in digital data without being clearly recognizable it in subsequent investigations and examinations. Generally, every activity in the information system leaves digital traces in it, but when I know what I'm doing, I can eliminate such traces of unfair action, or at least minimize it to such a degree that it will not be discoverable by the current means. This is more or less successfully used by intruders.

However, in the case of legal solutions, we can very often find that there is always a potential suspicion that acquired traces (digital evidence) could be questioned just because *"in the digital environment, almost anything can be done with digital data, without it being subsequently revealed"*.

The above reasons are one of the reasons why it is necessary to understand the differences between digital data and digital evidence. If the technical solution of a security incident is the primary objective of eliminating the incident as soon as possible and restore the system to its original state (primarily technical and economic reasons), the primary aim of the legal solution is to detect the perpetrator of the incident and to collect sufficient quality and unquestionable evidence to convict the perpetrator (legal reasons) and to ensure the organization the possibility of legal recovery of the damage (legal/economic reasons).

2 Example from practice

Do such considerations have practical applications? Certainly! I'll show you a real example from the banking environment.

A bank is responsible for safe communication with clients (e.g. inernetbanking). If the client reports suspicion of misuse of his/her access to his or her account, the bank's security team must verify that fact. In addition to investigating inside the bank system, team has to go out to the client and secure traces from his computer (mobile, tablet) to detect potential security attacks on client devices. To do this, specialists collect data from the device (in a standard way data from memory and data from disks), which then analyze in the laboratories and identify a potential new way of attack of their bank system.

However, the attack on the client's account may, in parallel, cause material damage to the client himself (the theft of his funds). So the client will report the damage to the police as a suspicion of a criminal act, and the police will deal in parallel with this case as a criminal offense.

Generally both teams, the security team of the bank and the police investigation team, follow their own rules. In investigating such incidents, the key period is from the onset of the incident, to the data collection. If a bank team appears to the client first (this is the most probable situation), he can irrevocably destroy the evidence for criminal proceedings in case improper data handling. However, if a police investigator appears to the client first, he will most likely acquire the client's devices, and for the bank it will be difficult to have the access to the data in a considerable time period.

Because for both teams is the core to correct, reliable, and both technically and process-clean and accurate data gathering, the solution is to set-up a unified (and forensically correct) way of gathering such digital evidence. This ensures that whatever the data is provided by any team, they will be used for security analysis in the bank and at the same time for criminal investigations.

And since the security teams of the bank are objectively more operational than the police investigation teams, the question of the proper qualifications of the bank's experts arises not only in the field of security incident investigation but also in the area of the right (in terms of procedural law, forensic) gathering of digital evidence. If digital evidence is gathered using the right procedure and technology, it can be used for both - police criminal investigations security incident investigations.

I note that this example is generalized, but it is based on my own experience when I lead certified training of bank security teams with the aim of teaching them the right and internationally recognized digital evidence seizing procedures.

The above concrete example of the need for seizing digital evidence by internal security experts is not unique. This requirement arises from their internal initiative and the need for effective cooperation with the police. In recent years, however, a stronger emphasis has been placed on information security and personal data protection, including regulatory requirements, and the need for reliable investigating of serious security incidents. And since in these cases time plays a key role, there is no other way than to do first investigation steps (especially forensic data seizing) by internal experts, than to wait for the police authorities.

3 Correct handling of digital evidence

In the introduction, I said that as an evidence can be used anything that can help to clarify the matter. This is also true for digital data. However, (at least in Czech) the principle of free evaluation of evidence applies. This means that individual evidence (and thus digital data) may have different weight and importance in their assessment by the court. It is not just about the context in which the digital data are relevant to the matter, but also about the credibility of such digital data.

3.1 General Requirements for Digital Evidence

There are several sources [e.g. 2] about the properties of digital data from a criminalistic point of view. We will only discuss the most important ones here:

3.1.1 Identity

It must be undeniably ensured that the digital evidence exactly matches the data that was in the computer technology at the time of their seizing. Practically, special methods and procedures are used, as well as special SW and HW resources that reliably ensure that no unintentional change of original source data occurs in the process of making copies of data (so-called forensic copies).

3.1.2 Integrity

Because, in general, digital data can be easily destroyed or altered (whether deliberately or negligently), the basic requirement for digital evidence (as a specific subset of digital data) is to preserve its integrity from seizing it to a final judgment. In short, the data must be seized in a way that ensures that they remain unchanged throughout all their life. This can be easily achieved by acquiring several (at least two) copies of the seized data and obtaining some suitable form of electronic signature, respectively, calculation of the appropriate control sum (hash).

3.1.3 Complexity

The data must be seized to the extent that it comprehensively covers information related to the investigated fact. Here we come across the first more complex problem in determining the range of data being seized. Since the data need to be provided in the early stages of a security incident investigation, it is difficult to predict the scope of data ahead. Additionally, experts know that complex information about data is found in a variety of areas of the system in most information systems, apart from data itself there are metadata, various system and application logs, directly and indirectly related information, data already deleted, and often data in the free storage space, file system file relics, and so on. Therefore, whenever technically feasible, it is advisable to ensure maximum data availability, preferably using a so-called binary image of a data repository (a copy of data from the first to the last sector).

3.1.4 Proportionality

Seemingly contrary to the requirements of complexity, we must always take into account the requirement of proportionality. This requirement arises from the fact that the data to be seized must be in direct, time, factual or causal relationship with the case under investigation. Seizing and possibly non legal use of other data (e.g. unrelated personal data) could cause further potential damage.

We could also list a number of other requirements, but these are some of the crucial ones with which the security team meets. If "Identity" and "Integrity" are requirements that can be solved by virtually exclusively technical means (and naturally, the practices and skills of team members in handling), "Complexity" and "Proportionality" require the team to take a different look at the data seizing process. In deciding this, it is necessary to take into account not only the view of the purely technical solution of the incident but also the process-legal view (see Chapter 1) and to take into account also the potential future requirements for evidence that will be needed to resolve the incident through labour law or criminal law.

In the introduction to this chapter, I have stated that if digital data is used as evidence, their weight in judging by court may be different. But if we want to create the prerequisites for our digital evidence to have a high weight of proof, we must ensure that it has at least the above characteristics. Otherwise, they are likely to be questioned in a court case.

4 Conclusion

On the basis of the above-mentioned, I can clearly summarize the following facts:

- The current situation is characterized by an enormous increase in security incidents, which is more and more of a considerable scale and impact. There are growing regulatory requirements to address and investigate security incidents. This is linked to the overworking of police authorities by crime in this area. In addition, there is objectively a lack of skilled and operative qualified police personnel. This requires that the security teams of the organization should perform not only standard security incident investigation actions (eg in accordance with ISO / IEC 27035), but also take on the initial actions required in the case of the criminal investigation of the impact of security incidents.
- The above is directly related to the acquisition of knowledge, skills and practical experience with the digital evidence gathering process that would be applicable even in criminal cases. While virtually any digital data may be potentially usable as digital evidence, the use of specific seizing procedures can achieve a significant increase in its probative value. Digital evidence obtained by a forensically clean manner may also be used for security incident handling techniques, even with a significantly higher degree, because of forensically seized data may have a significantly higher added value in the standard (technical) response to a security incident.

- Providing forensic data, in a fair way, has two opposing effects:
    1. The qualification requirements for security teams are increasing and the demands for their equipment are increased by special HW and SW resources;
    2. Forensically properly seized digital evidence generally contains more comprehensive information and data, including their context in the information system, allowing for a much more detailed and credible investigation of the incident and finding optimal preventive measures. They may be retrospectively used as digital evidence (or after analysis as the source of such digital evidence) in cases where a security incident must be reclassified later as a criminal act and must be resolved by a judicial process.

The recently adopted ISO / IEC 27037 [3] standard can be recommended as the first aid that can be used to solve the issue of digital evidence gathering within an organization. As stated above, the security team of the organization is also the "first responder" team in providing digital evidence.

Nevertheless, this standard is not composed in the happiest way [4]. Already at the time of adoption, some of its passages were obsolete or at least questionable. Anyway, as the first source of information on how to gather and deal with digital evidence can serve as the first inspiration.

Due to my objections to this standard (not only I, but also the large professional community), I can only recommend close cooperation with forensic experts in the field of digital evidence. Developments in this area are also extremely dynamic, and it is only logical that the latest trends can be traced only to a narrow specialization in digital forensics area.

References

[1] International Organization for Standardization, ISO/IEC 27035:2011

[2] PORADA, V., STRAUS, J., *Kriminalistika: (výzkum, pokroky, perspektivy)*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, pp. 35 - 36

[3] International Organization for Standardization, ISO/IEC 27037:2012

[4] Svetlik, M., ISO/IEC 27037, Digital Forensic Journal, 2/2014, ISSN 2336-4750, pp. 27-28