Digital Forensics

What is it?

Based on NIST, digital forensics is: “In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony.” (https://csrc.nist.gov/glossary/term/digital-forensics)

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved and / or the type of the examined digital evidence; computer forensics, network forensics, log analysis, mobile forensics, etc. The typical forensic process encompasses the identification of potential sources of digital evidence and its acquisition and subsequent analysis. The whole process is performed by following internationally accepted procedures, such as the ACPO Good Practice Guide on Digital Evidence, and maintaining a proper chain of custody. The process leads to the production of a digital forensics analysis report, which can be presented in the courts of law.

Who is it directed at?

Digital forensics is directed to the whole phasm of business organizations. Either in the private or in the public sector, either small or big sized companies, all organisations might fall victim of a hacking attack, suffer an information security breach or need to investigate an employee’s misconduct (ex. fraud), which might not necessarily be information security related. At this point each and every organisation needs to decide whether to issue a digital forensics analysis by a specialized digital forensics investigator and uncover for example the exact conditions, extent and impact of an identified web server attack or investigate the incident inhouse with the risk of failing to find out what really happened in the aforementioned attack and destroying valuable evidence.

Why is it important?

Digital forensics is the proper and internationally recognized way to handle a security or a corporate incident, whether information security or non-information security based, for organisations who want a procedure that is solid, will stand in a court of law and will assist them in handling the incident internally based on existing corporate procedures, as well as externally based on existing regulations such as the General Data Protection Regulation or the NIS Directive. organisations need to be certain that the investigation of an incident will be conducted in a way that cannot be disputed either corporate wise or legal wise. In the end of the day, the CEO, in a corporate investigation involving an employee that is accused of conducting fraud, needs to be certain that (a) the digital media used by the employee are seized, acquired and analyzed in a forensically sound manner, (b) the produced analysis report answers, when possible, any questions related to the incident (who did what, when, how and why) and (c) the produced analysis report helps him reach a decision regarding the accountability of the employee involved in the incident. It should be noted that in the aforementioned scenario the Company may decide to take disciplinary actions for the employee involved in the incident, who may then decide to

turn against the company in the courts of law claiming that he / she was fired on non-justifiable grounds. In such a case, it is evident how important a properly conducted digital forensics investigation is, as it will "protect" the business from possible further damage in the courts of law.

Where is it taking place?

Digital forensics covers the whole phasm of business organizations. It starts on the organizations premises with interviews and digital evidence identification and acquisition. Based on the type and the amount of the identified digital evidence the latter might be performed on site or off site. Following acquisition, the digital evidence is analyzed in a digital forensics lab and a report is produced, which is handed to the organization. As the investigation progresses further questions might need to be asked or further digital evidence might need to be acquired, as for example it might be uncovered that another machine, which has not already been acquired, is involved in the investigated incident (ex. it is also hacked). Upon handing of the digital forensics report the digital forensics investigator might be called upon to testify in the courts of law as an expert witness, in order to support / explain the produced report and justify / explain the findings and / or the procedure followed. Evidence is protected throughout the investigation process and appropriate measures are taken to protect the integrity, confidentiality and availability of all digital evidence.

When is it going to make an impact?

In a world of data breaches, constantly emerging threats, potentially malicious insiders and constant computer security attacks digital forensics constitutes the tool that will help a business handle an incident properly and emerge from it with the minimum damage possible. The reality shows that it is not a matter of if you will get breached, it is a matter of when. Thus, organisations need to be ready to handle such a breach. The reason for that is twofold. On the one side organisations need to be able to find out what actually happened and on the other side adhere to existing regulations (GDPR, NIS, etc.) and prove due diligence. The only way to achieve that is to call a digital forensics investigator, who will investigate any incident in a forensically sound manner by means of a digital forensics' analysis.

For example, in a personal data breach scenario, the affected organization is obliged, based on articles 33 and 34 of the General Data Protection Regulation (2016/679), to inform the responsible Data Protection Authority as well as the affected data subjects. If the organization does not perform a proper investigation, which involves digital forensics, and reaches the wrong conclusions, then the organization might end up being fined with a large monetary fine, which might have been avoided if a proper investigation had been performed and the true extent of the data breach was uncovered.

How will it affect your business?

Digital forensics will help organisations uncover the full nature of an incident and perform the proper actions based on the results of the digital forensics investigation. For example, in an incident where a web server hosting personal data is hacked, the digital forensics investigation will help the web server's owner uncover if personal data have been accessed by the attackers, thus a personal data breach has occurred, and subsequently perform the necessary actions based on articles 33 and 34 of the General Data Protection Regulation (Notification of a personal data breach to the supervisory authority and Communication of a personal data breach to the data subject).