How digital forensics unlocks the truth

DUBAI, UNITED ARAB EMIRATES, February 26, 2024 /EINPresswire.com/ -- Lucas Paus and Mario Micucci, the Security Researchers at ESET explain how to learn the cyber variety of CSI works, from sizing up the crime scene and hunting for clues to piecing together the story that the data has to tell

The burgeoning field of digital forensics plays a crucial role in investigating a wide range of cybercrimes and cybersecurity incidents. Indeed, in our technology-centric world, even investigations of 'traditional' crimes often include an element of digital evidence that is waiting to be retrieved and analyzed.

This art of uncovering, analyzing and interpreting digital evidence has seen substantial growth particularly in investigations involving various kinds of fraud and cybercrime, tax evasion, stalking, child exploitation, intellectual property theft, and even terrorism. Additionally, digital forensics techniques also help organizations understand the scope and impact of data breaches, as well as help prevent further damage from these incidents.

With that in mind, digital forensics has a role to play in various contexts, including crime investigations, incident response, divorce and other legal proceedings, employee misconduct probes, counterterrorism efforts, fraud detection and data recovery.

Let's now dissect how exactly digital forensics investigators size up the digital crime scene, hunt for clues and piece together the story that the data has to tell

1. Collection of evidence
First things first, it's time get your our hands on the evidence. This step involves identifying and gathering sources of digital evidence, as well as creating exact copies of information that could be linked to the incident. In fact, it's important to avoid modifying the original data and, with the help of appropriate tools and devices, create their bit-for-bit copies.

Analysts are then able to recover deleted files or hidden disk partitions, ultimately generating an

image equal in size to the disk. Labeled with date, time and time zone, the samples should be isolated in containers that shield them from the elements and prevent deterioration or deliberate tampering. Photos and notes documenting the physical state of the devices and their electronic components often help provide additional context and aid in understanding the conditions under which the evidence was collected.

Throughout the process, it's important to stick to strict measures such as the use of gloves, antistatic bags, and Faraday cages. Faraday cages (boxes or bags) are especially useful with devices that are susceptible to electromagnetic waves, such as mobile phones, in order to ensure the integrity and credibility of the evidence and prevent data corruption or tampering.

In keeping with the order of volatility, the acquisition of samples follows a systematic approach – from the most volatile to the least volatile. As also laid out in the RFC3227 guidelines of the Internet Engineering Task Force (IETF), the initial step involves collecting potential evidence, from data relevant to memory and cache contents and continues all the way to data on archival media.

2. Data preservation

In order to set the foundations for a successful analysis, the information collected must be safeguarded from harm and tampering. As noted earlier, the actual analysis should never be performed directly on the seized sample; instead, the analysts need to create forensic images (or exact copies or replicas) of the data on which the analysis will then be conducted.

As such, this stage revolves around a "chain of custody," which is a meticulous record documenting the sample's location and date, as well as who exactly interacted with it. The analysts use hash techniques to unequivocally identify the files that could be useful for the investigation. By assigning unique identifiers to files through hashes, they create a digital footprint that aids in tracing and verifying the authenticity of the evidence.

In a nutshell, this stage is designed to not only protect the collected data but, through the chain of custody, also to establish a meticulous and transparent framework, all while leveraging advanced hash techniques to guarantee the accuracy and reliability of the analysis.

3. Analysis

Once the data has been collected and its preservation ensured, it's time to move on to the nitty-gritty and the truly tech-heavy of the detective work. This is where specialized hardware and software come into play as investigators delve into the collected evidence to draw meaningful insights and conclusions about the incident or crime.

There are various methods and techniques to guide the "game plan". Their actual choice will often hinge on the nature of the investigation, the data under scrutiny, as well as the proficiency, field-specific knowledge and experience of the analyst.

Indeed, digital forensics requires a combination of technical proficiency, investigative acumen and attention to detail. Analysts must stay abreast of evolving technologies and cyberthreats to remain effective in the highly dynamic field of digital forensics. Also, having clarity about what you're actually looking for is just as paramount. Whether it's uncovering malicious activity, identifying cyberthreats or supporting legal proceedings, the analysis and its outcome are informed by well-defined objectives of the investigation.

Reviewing timelines and access logs is a common practice during this stage. This helps reconstruct events, establish sequences of actions, and identify anomalies that might be indicative of malicious activity. For example, examining RAM is crucial for identifying volatile data that might not be stored on disk. This can include active processes, encryption keys, and other volatile information relevant to the investigation.

4. Documentation
All actions, artifacts, anomalies, and any patterns identified prior to this stage need to be documented in as much detail as possible. Indeed, the documentation should be detailed enough for another forensic expert to replicate the analysis.

Documenting the methods and tools used throughout the investigation is crucial for transparency and reproducibility. It allows others to validate the results and understand the procedures followed. Investigators should also document the reasons behind their decisions, especially if they encounter unexpected challenges. This helps justify the actions taken during the investigation.

In other words, meticulous documentation is not just a formality – it is a fundamental aspect of maintaining the credibility and reliability of the entire investigative process. Analysts must adhere to best practices to ensure that their documentation is clear, thorough, and in compliance with legal and forensic standards.

5. Reporting
Now the time is right to summarize the findings, processes, and conclusions of the investigation. Often, an executive report is drafted first, outlining the key information in a clear and concise manner, without going into technical details.

Then a second report called "technical report" is drawn up, detailing the analysis performed, highlighting techniques and results, leaving aside opinions.

As such, a typical digital forensics report:
- provides background information on the case,
- defines the scope of the investigation together with its objectives and limitations,
- describes the methods and techniques used,
- details the process of acquiring and preserving digital evidence,
- presents the results of the analysis, including discovered artifacts, timelines, and patterns,

- summarizes the findings and their significance in relation to the goals of the investigation

Lest we forget: the report needs to adhere to legal standards and requirements so that it can withstand legal scrutiny and serve as a crucial document in legal proceedings.

With technology becoming increasingly woven into various aspects of our lives, the importance of digital forensics across diverse domains is bound to grow further. Just as technology evolves, so do the methods and techniques used by malicious actors who are ever so intent on obscuring their activities or throwing digital detectives 'off the scent'. Digital forensics needs to continue to adapt to these changes and use innovative approaches to help stay ahead of cyberthreats and ultimately help ensure the security of digital systems.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here