JS|HELD

PERSPECTIVES

What Is Digital Forensics: Applications, Processes, and Real-World Scenarios

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

This paper will cover the application of digital forensics, the types of data digital forensics experts work with, the investigation process, and some example scenarios wherein digital forensics experts are called to help address impacts of the event. The following information may be of particular interest to various types of Insurance Professionals, Legal Community, and Law Enforcement depending on the identifiable activity and possible liability for what data may be involved.

WHAT IS DIGITAL FORENSICS?

The definition provided by EC-Council states, "Digital Forensics (DF) is a branch of forensic science focusing on the recovery and investigation of material found in digital devices related to cybercrime." Cybercrime is at an all-time high, with just the cybercrime insurance industry alone expecting to grow from $8 billion globally in 2020 to $20 billion by 2025. Although digital forensics can be related to cybercrime, it can also be related to any form of analysis that would include digital storage of data or data used within a function of everyday personal and business operations. This includes a multitude of computing devices and storage methods that are available to entire populations.

Digital forensics is the examination of available digital evidence following an event. Depending on the needs of the examination of the event, the collection of digital evidence can include many involved devices and contain multiple terabytes (TB) of data. Traditional events can include matters such as:

- Employee wrongdoing
- Ransomware / Malware
- Network breaches
- Unexplained activity on computing assets

However, as the scope of digital integration grows, more and more cases involve digital data or devices that can be examined to provide supporting information. This helps provide context for the event, including a timeframe and scope, and is frequently used to confirm actions of potentially malicious activities and determine need-to-notify obligations for clients who operate with personally identifiable information (PII) and personal health information (PHI).

HOW IS DIGITAL FORENSICS APPLIED?

Digital forensics is concerned with a broad range of data, allowing an expert to examine evidence for the unique circumstances surrounding an event. Each case and environment is different and presents unique challenges. It is common for cyber-insurance carriers to retain a digital forensics expert or organization to examine evidence surrounding a claim to verify the validity, scope of impact, and timeframe. Additionally, organizations outside of insurance retain digital forensics experts to assist in understanding what happened, how it happened, and how to proceed to assist with possible legal activity where liability or criminal aspects may be identified.

WHAT EVIDENCE CAN DIGITAL FORENSICS EXAMINE?

The evolution of digital forensics began with computer forensics and has expanded to include mobile devices, servers, and largely a multitude of devices that produce and/or store digital data. Today, forensics can even be performed on intangibles such as cloud infrastructure (IAAS, SAAS, etc.). Some common examples of intangibles include:

- Servers
- Computers
- Networking equipment (routers and switches)
- Video data solutions (NVR/DVR)

- Point of Sale systems
- Firewalls
- Proxies
- Cloud Hosted Applications and Infrastructure (Office 365, custom applications, VDI, etc.)
- Medical equipment / devices

Data is generated during the operation of the above sources, typically in the form of logs that can also be examined to provide further context. The ability to obtain, preserve, and examine these logs is critical to assist with a full analysis of an event.

WHAT DOES THE PROCESS LOOK LIKE?

Digital Forensics generally consists of the following phases:

1. **Identification** -- During the identification phase, the expert works with the client to determine the general details of what happened. This may include, but is not limited to:

    a. What was observed.

    b. What evidence might be available for collection.

    c. What steps have been taken in remediation.

2. **Collection** -- Collection builds on the information gathered in the identification phase. An expert will collect evidence that has been determined to be of relevance to the event in question.

3. **Analysis** -- During the Analysis phase, a "deep dive" is performed on the evidence collected, helping to build out a complete picture based on the available details regarding what happened and when.

4. **Documentation** -- Documentation usually takes the form of a timeline of the event and a report on the evidence gathered as well as findings from the analysis step.

5. **Presentation** -- The presentation phase is a chance to break down the technical documentation produced in phase 4 into bite-sized pieces for the client.

REAL-WORLD SCENARIOS: RANSOMWARE ATTACK & SERVICE INTERRUPTION

The following example focuses on a ransomware execution on a small-to-medium business network and will walk through what happens during the event, provide an example of a common response, and address the role digital forensics plays in that response.

"Smith Co." Ransomware Attack

Smith Co. is an organization focusing on logistics and has local Information Technology infrastructure. Following a seemingly normal week in the office, Mr. Smith, the owner of Smith Co., returns to his office to discover he is unable to log into his computer and receives an authentication error. He contacts the Information Technology (IT) contractor used by Smith Co. to establish and support their infrastructure. The contractor logs into the active directory server to reset Mr. Smith's password and is greeted by a ransom note. The contractor then goes on-site and investigates to determine the scope of the current issue and the impact on Smith Co.'s operations. It is determined that email, workstation logins, files on workstations and servers (including backups), and the primary production applications are all encrypted and therefore inoperable.

The contractor provides the contact information for a vendor to assist in remediation and describes the process of ransom negotiation the vendor will be engaging in. The vendor negotiates with the threat actor and Smith Co. pays the ransom. Smith Co. contacts their insurance company seeking remuneration for the expense involved in the event to recover pre-loss condition; it is mentioned that the location Smith Co. operates in requires notification of a breach to impacted parties including clients and employees in the case a breach occurs. The insurance company retains a digital forensics expert and breach coach3 on behalf of Smith Co. to investigate relevant devices to determine the scope of accessed data and whether data exfiltration occurred.

The digital forensics expert collects logs for the date of loss and historical data, where available, for infrastructure including servers, workstations, firewalls, and network switches. The expert then transfers the evidence to the lab for forensic imaging and investigation. A forensically sound copy is created, and the evidence is stored in a safe location. Investigation of the copy of the data begins with a search for the information relevant to the case. In this example, the work involves looking for accessed proprietary information for clients, payment data, and personally identifiable information for employees such as social security numbers, addresses, dates of birth, and so forth.

The forensics expert uses sources such as the network switches and firewalls to support the findings from the operating system level analysis of the workstations and servers. A detailed report is provided to the insurance company that will outline the findings of the analysis, including a timeline of activities. This report will allow for all parties involved to utilize this information, with the guidance of legal counsel, to determine proper methods to inform the impacted parties.

"Smith Co." Service Interruption

The example below focuses on a service interruption on a small-to-medium business network. It will walk through what happens during the event, provide an example of a common response, and address the role digital forensics plays in the response.

Smith Co. is an organization focusing on logistics and has a mix of locally hosted and cloud IT infrastructure. Following a seemingly normal week in the office, Mr. Smith, the owner of Smith Co., returns to his office to discover he is unable to log into his computer and receives an authentication error. He contacts the newly hired IT contractor used by Smith Co. to establish and support their infrastructure. The contractor logs into the active directory server to reset Mr. Smith's password and is unable to, receiving a connection failure error. The contractor then goes on-site and investigates to determine the scope of the current issue and the impact on Smith Co.'s operations. It is determined that many of Smith Co.'s devices are powered off.

The contractor attempts to power on Smith Co.'s devices, with mixed results. It is determined that approximately half of Smith Co.'s servers did not restart, which warrants loading their available backups for a possible method of recovery. This process (investigation and remediation) takes several hours, during which Smith Co. is unable to use their locally hosted applications such as their custom applications and associated databases; their cloud infrastructure, including Office 365 email and One Drive, are also impacted. Smith Co. retains a digital forensics expert to verify the root cause investigation performed by the IT contractor.

The digital forensics expert collects logs for the date of observed activity and historical data, where available, for infrastructure including power distribution units, servers, workstations, firewalls, and network switches. In cases where it is relevant, an examination of the physical hardware is in order. The expert then transfers the evidence to the lab for forensic imaging and investigation. A forensically sound copy is created for digital evidence, and the physical evidence and original copies are stored in a safe location. Investigation of the forensic copy of the data begins with a search for the information relevant to the case. In this example, the expert looks for anomalous events indicating instability or events which could lead to instability, such as configuration changes. Simultaneously, the hardware is investigated to determine its current state.

The forensics expert correlates the gathered data across devices to get a complete picture of the network operation as it was during the time of the event being identified. It is then possible to determine the root cause, impacted devices, and feasibility of recovery. The investigation reveals that the former IT contractor's account was used to sign in and delete key operating system and applications files on the impacted machines as well as to change the configuration of Office 365 and One Drive to render them inoperable. A report is provided to Smith Co. who is able to determine root cause, scope of impact, and, with the assistance of legal counsel, how to proceed.

CONCLUSION

Digital forensics work frequently involves unique challenges presented by the specific circumstances of the client and the event. It is vital to bring in digital forensics experts as early as possible when a relevant event

occurs and during subsequent remediation processes. As evidence is prone to deletion and being overwritten as time goes on, it is more difficult to provide a complete picture of events the longer it takes to begin analyses following a breach or similar event.

The information provided by a detailed analysis of the events can be invaluable to decision makers in an organization, when making coverage determinations for insurances policies, or when informing a legal or policy obligation.

ACKNOWLEDGMENTS

We would like to thank Alex Tarrant, Matt Scott & Troy Bates for providing insight and expertise that greatly assisted this research.

MORE ABOUT J.S. HELD'S CONTRIBUTOR

Troy Bates is an Executive Vice President in J.S. Held's Equipment Practice. He specializes in equipment damage assessment, feasibility of repair versus replacement, comparable replacement analysis / estimates, actual cash value estimates, production impact resolution, and claim evaluation. Troy has evaluated a wide variety of equipment and systems including, but not limited to, information technologies, electronics, medical equipment, telecommunications, and other specialized equipment. He focuses on high-end computer hardware, personal computers, application software, operating systems, programming languages, data recovery, printers and printing routing technology, telephone switch equipment, switches, routers, networking topologies, data cabling, and telecommunication cabling.

Contact Troy Bates at tbates@jsheld.com or
+1 714 660 9171.

REFERENCES

1. https://www.eccouncil.org/what-is-digital-forensics/

2. https://www.statista.com/topics/2445/cyber-insurance/