TAG CYBER

HIGH-SPEED FORENSIC PROCESSING OF DIGITAL EVIDENCE USING ENCASE

EDWARD AMOROSO, TAG CYBER

opentext™

TAG CYBER

HIGH-SPEED FORENSIC PROCESSING OF DIGITAL EVIDENCE USING ENCASE

EDWARD AMOROSO

High-speed forensic processing is imperative in modern investigations, given the need for rapid mitigation and response in both law enforcement and corporate investigations. Recent independent tests show that the OpenText EnCase platform[1] supports stringent performance requirements.

INTRODUCTION

The role of digital forensics in cyber-related investigations has shifted recently from static, after-the-fact reviews to dynamic, real-time analysis. This change carries with it the obligation for modern forensic platforms to integrate with working security platforms, including public clouds, mobile apps and social media. It also demands support for processing a variety of new formats, protocols, systems and standards.

One consideration that has remained constant, however, is the requirement that forensic analysts complete their task in a reasonable amount of time. While this remains largely non-real time for most applications (e.g., processing a large batch of evidence), the performance of commercial platforms is an increasingly important functional issue, especially as digital forensic investigations evolve, as mentioned above.

In this report, we outline how modern digital forensics has evolved from its more traditional foundation. We then explain the performance requirements that emerge for such forensic usage, and we summarize some recent testing reported by the OpenText team for its popular EnCase platform. Examination of this testing and the results provides good insight into this emerging concern for digital forensics.

SUMMARY OF MODERN DIGITAL FORENSICS

Traditional digital forensic support generally involved capturing a device and then analyzing its contents using off-line tools. This would be done in most cases by connecting to the device physically and then taking an image of its memory content and configuration for subsequent investigation. This usually involved for computers, phones and disk drives, and the motivation was usually driven by some investigative case.[2]

Such early forensic efforts, which remain valid today, have always had the great advantage of being performed mostly off-line from any live network, and without any more significant time pressure than the need to provide interim or final analysis results to the case investigator. Such pressure might have been measured in days or even weeks, so the forensic analyst could work through the image processing carefully and deliberately.

This forensic process has changed in many ways in recent years. Perhaps most prominent is the fact that digital forensics involves collecting data from systems that are more transient and even temporary. Virtual infrastructure, for example, can be spun up and down quickly, and the associated forensic capture process must have the capability to collect relevant data when it exists. The casual nature of early processing methods will not work in these cases.

Modern digital forensic investigative lifecycles include the familiar collect, check, connect, construct, consider and consult tasks. The evolution of this lifecycle from current digital forensic data targets (i.e., mobiles, PCs, servers and networks) has resulted in a new emphasis on cloud, SaaS, IoT devices, virtualized systems and even new types of network technologies, such as 5G (see Figure 1 below).

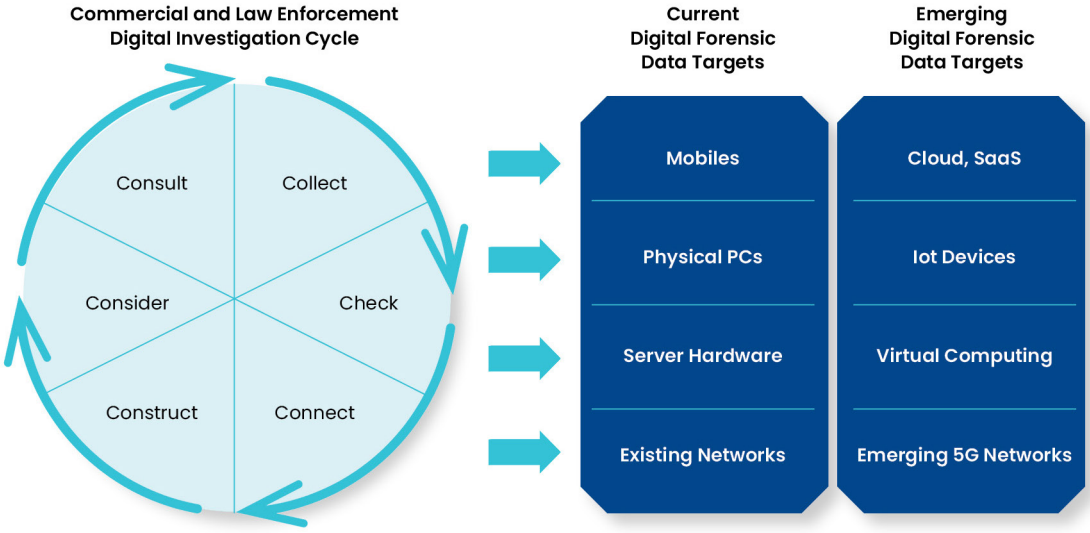

Figure 1. Evolution of Digital Forensics

As shown above, the types of systems that require forensic capture are no longer just electronic devices that can be obtained and connected manually to create memory images. Instead, the target systems of interest are often virtual and stored in public cloud or SaaS infrastructure. These systems require a different process for obtaining data and analyzing it to support the forensic investigation—and this new process introduces performance objectives.

FORENSIC PERFORMANCE AND ENCASE TESTING

As most forensic investigators and scientists will attest, performance has certainly been a constant comparison factor in selecting a commercial platform. Performance requirements have been expressed, however, more as the need to provide a reasonable response time when processing evidence. No clear benchmarks for performance comparison are generally accepted for comparison.

The urgency of this situation is changing, as the fast-paced world in which we live demands more rapid results from investigative processing. In some cases, people's lives can hinge on the results of an investigation. Speed is necessary to help investigators complete cases more quickly, sometimes bringing the bad guys to justice—or helping the innocent regain their lives. Performance is the prime gating factor in establishing closure for many investigative cases.

The EnCase team recently ran performance benchmarks on their platform. The TAG Cyber analyst team reviewed the results and has concluded that the completion times appear to exceed best practices in this area. At a high level, our prior experience suggests that processing large batches of evidence, in most practical cases, is measured in days. Obviously, this varies with the size of the evidence, but practitioners should resonate with the general idea.

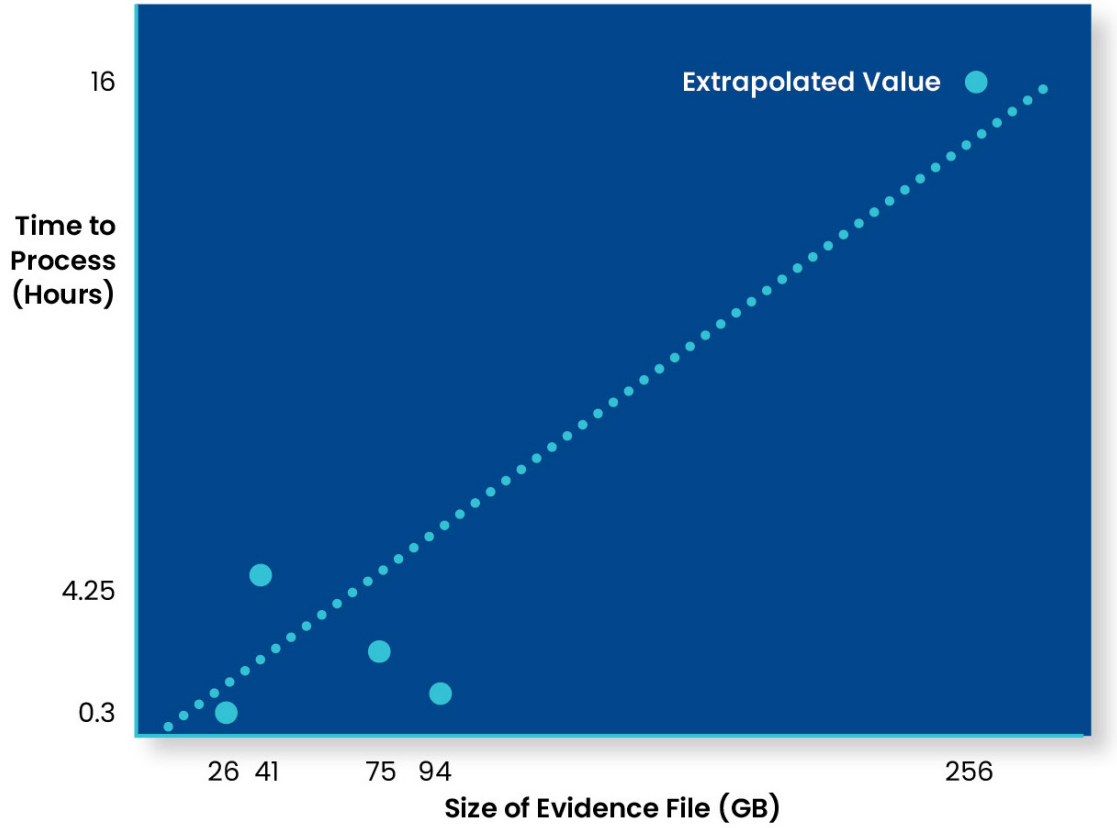

Figure 2. Mapping of EnCase Performance Tests

The performance tests were described in a series of blogs recently posted by OpenText.[3] In one particular case, a Silicon Forensics workstation running EnCase Forensic v21.4 was used for the testing. It contained an Intel i7-7700 processor, 32GB of RAM and NVMe hard drives, running the Windows 10 operating system. The evidence file contained 41GB of photos, emails, internet searches, documents and chats.

The test data showed that the EnCase Forensic platform processed the 41GB of evidence in about four hours and 14 minutes. Extrapolating this result to 256GB, which is an oft-found evidence file size, the processing time would be about 26 hours. As suggested earlier, while this is difficult to connect to a fixed benchmark, the processing result reduces performance times from units of days to units of hours—and this is for evidence batches that are nontrivial in size.

According to another public blog from OpenText, an official from a European police agency also ran testing involving evidence from half a million emails. This individual used EnCase Forensic v21.4 to process 13 Outlook data files into 75GB of evidence. This was indexed and mapped to thumbnails—and the work was completed in 2.5 hours. Another 26GB Outlook data file with 91,000 objects and 41,000 emails was processed in 20 minutes. Finally, a 94 GB file was completed in 51 minutes.

While these actual numbers are tough to map to a specific framework context for comparison, they do line up well with our general guidance that processing of this magnitude should move from units of days to units of hours (or less). Results show that the EnCase platform delivers these kinds of metrics. As the forensic community continues to develop a deeper understanding of its key role in law enforcement and enterprise security, one would hope that more formal industry performance benchmarks might be developed.[4] This would include testing to ensure that a given platform is consistently updated to add features that can improve performance.

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and nonclients alike—all from a former practitioner perspective.

[1] *https://security.opentext.com/encase-forensic; https://security.opentext.com/encase-endpoint-investigator*

[2] *https://www.sciencedirect.com/science/article/pii/B9780124201255000091*

[3] *https://blogs.opentext.com/*

[4] *The OpenText team shared information that suggested superior performance results to competing platforms. The evidence was compelling, but TAG Cyber refrains from product comparisons unless the results are repeated in an independent test. Customers of OpenText should request this competitive information, nevertheless, and can make their own local assessment.*