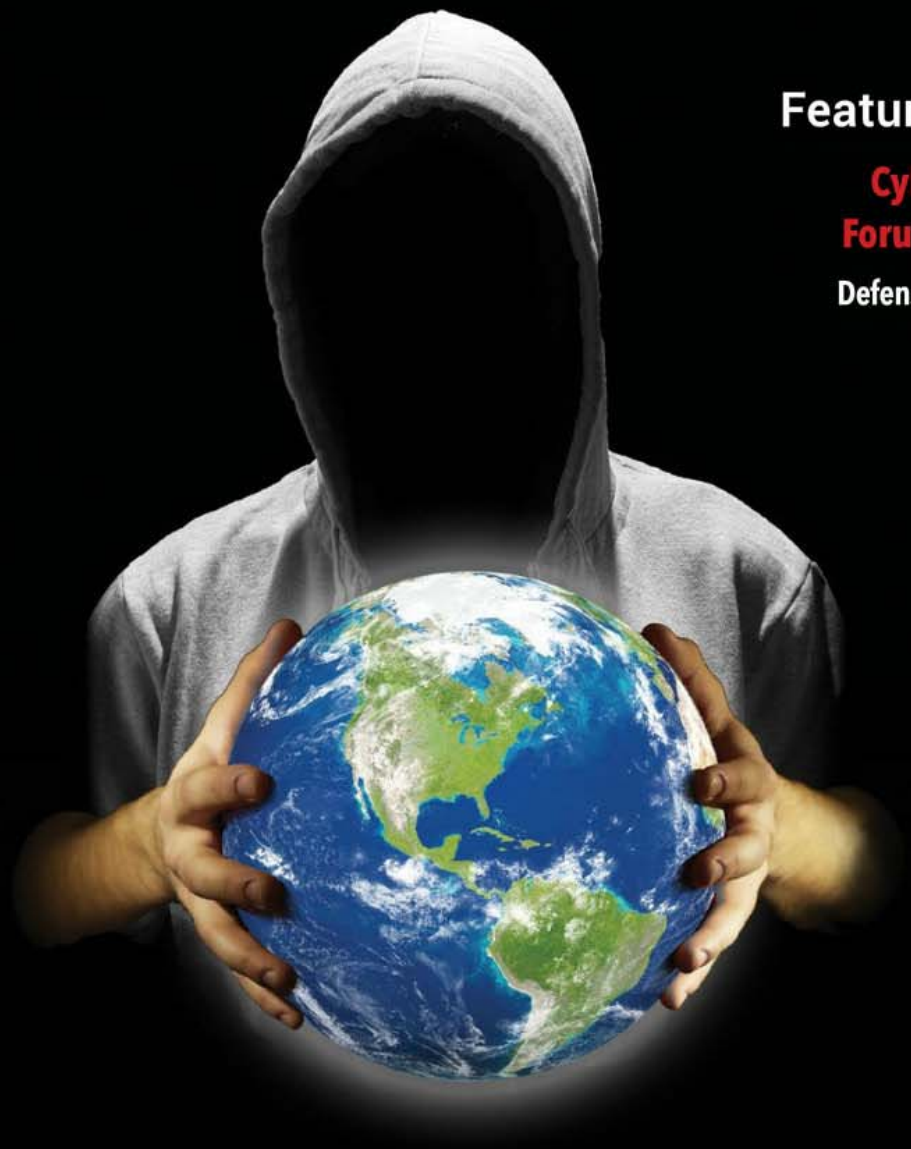
Spring 2015 Issue | Volume 3 | Number 7

United States {CYBERSECURITY} Magazine



Feature Article

Cyber Security Forum Initiative

Defense in the Age of Cyber-Warfare

Page 40

2015: It's All about the Data
BLACKOPS Partners

Who's Watching the Back Door?
e-End USA

Diving into the Deep Web
Emagine IT

Creating Your Ultimate Code-Cracker: the Design of Digital Forensic Workstations

John Samborski, CEO
Ace Computers

Today most records of individuals, businesses, government agencies, and even criminal organizations are stored on various types of electronic media. In order to properly investigate a suspect, evidence needs to be extractable from electronically stored information (ESI) sources without being corrupted.

Digital forensics is the acquisition, scientific examination, and analysis of data retrieved from digital devices (computers, mobile phones, game consoles, memory sticks, etc.) in such a way that the information can be used in a court of law or for the purposes of the retriever without any disturbance to that evidence. Digital forensics often requires workstations that are dedicated to and designed for the task.

In order to design forensic workstations, the first determination is both the source and the destination of the media that needs to be forensically read, retrieved from suspect data, and included in the chain of custody. In other words, the workstation needs to have the ability to demonstrate who has had access to the digital information being used as evidence. Special measures should be taken when conducting a forensic investigation if the results will be used as evidence in a court of law. One of the most important steps is to ensure that the evidence has been accurately collected and that there is a clear chain of custody from the scene of the crime, to the investigator, and ultimately to the court.

Another key design decision is the workstation's **purpose: data acquisition, processing, or both**. Many systems are multi-purpose and can perform forensic data acquisition and processing equally well. Another important consideration is the required processing speed and the number of processors, processor cores, and amount of memory anticipated for the data processing. Systems are available with 1-4 processors and up to 1TB of RAM. A popular configuration involves two Intel® Xeon™ 6-core (each) processors and 256GB of DDR4 memory. The number of processors and cores per processor should be determined by the system requirements of the software that the system will run.

It's also important to consider the **type of media** the system needs to acquire data from. Once this is established, the next step is to plan and include write-protected data acquisition methods. The most basic media is a hard drive write-blocked forensic bridge. Write-blocked drive bay-mounted forensic bridges are available for all common hard drive types such as IDE, SATA, SAS, SCSI, IEEE1394 (Firewire), and USB, with adapters for using 3.5", 2.5", and 1.8" drives. A write-blocked flash media card reader is also useful for forensically reading media cards such as SD and CompactFlash cards. A read-only media card reader is best, since it will prevent accidental corruption or addition to the source data. A read-write switchable reader can potentially be corrupted, but by using a model that is incapable of writing data, that source of error can be eliminated. It's simple to add a standard external flash reader/writer to the system. Although it will be obvious to users that this external flash is capable of corrupting data, the internal model should be write-blocked at all times.

Optical media is another common source of forensic data. This media is typically not written to without specialized software, so a standard DVD or Blu-Ray reader/writer will perform this work adequately.

Once the data can be read in a forensically safe manner, it needs to be stored on either a target drive, a RAID array,

or both. With the storage system defined, the design of the RAID system or the allowance of destination drive bays needs to be specified.

Another decision is whether **graphic processing units (GPU)** should be included for assistance in breaking passwords. Normally, systems are shipped with a single graphics card for display purposes, but users can also leverage the intense processing power of the GPU for assistance in brute-force password cracking through massively parallelized iterative attempts. By using a higher-end graphics card or multiple graphics cards, the forensic system can also be used to shorten the time needed to break a password installed on a system or to open up files which have been encrypted. The current top-of-the-line card is the NVIDIA GeForce Titan-X, which is a single GPU card with 3,072 processing cores that costs about $1000. While this is five times the cost of a standard video card, it can be well worth the expense for password breaking/decryption work.

Specialized password/decryption servers and clusters with multiple GPU-optimized systems designed for 24-7 operation are also available, and are frequently used in the federal market by major government and law enforcement agencies.

Obviously, there are numerous items to consider when designing a forensic workstation and since the system components change often, it is best to work with a **systems integrator** who is actively involved in the market. The systems integrator will know how to optimize the design based on the latest software, hardware, and thermal techniques. For government agencies, it also makes sense to work with a firm that can custom-design a system to exacting specifications and has popular contracting vehicles available to facilitate the purchase directly without the complications of contracting procedures.

About the Author

John Samborski, P.E. is a recognized expert in forensic information technology, with an extensive history of innovation and thought leadership in system integration. Since founding Ace Computers in 1983, he has aggressively pursued the development of custom, cost-effective products and services in concert with well-known industry leaders. He was a founding member of the Intel Premier Board of Advisors in 2002 and was awarded a lifetime position. Ace Computers is one of the largest, oldest, and most respected custom technology developers and builders in the U.S. and holds numerous federal and state level contracts.

ACECOMPUTERS