No images? Click here

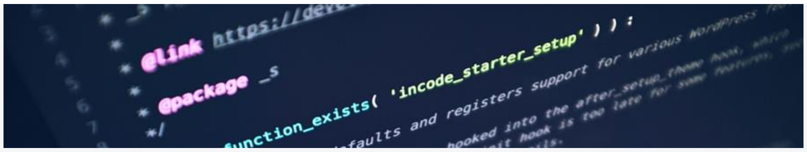
Compliance Analysis

Brian J. Kelly, Cyber Analyst - IPPC Technologies

This month I'll be revisiting another article I wrote as an officer back in 2002 for News & Views, the bi-weekly newsletter of the United States Probation and Pretrial System. In the article entitled "Compliance Analysis Versus Computer Forensics", I discussed the practice of "compliance analysis", a term I coined early on to differentiate examinations of computer systems. True computer/digital forensics examinations focus on taking specific steps to preserve the integrity of the evidence while uncovering bits and bytes that may be deep into regions of the digital media (i.e. unallocated space). While advancements in technology in this field have made extraction and examination methods faster and more mobile, there will always be a standard any digital forensics examiner should maintain.

Compliance analysis techniques were viewed as more appropriate for pretrial/probation/parole scenarios where standard rules of evidence may not apply and immediate results were needed. Over time, tools like Field Search and osTriage were introduced for the purposes of examining live media while making minimal changes. In the world of mobile devices, such as iPhones, etc., true forensic examinations may not be possible because even the most robust of tools require the device to be booted into the OS for data extraction. Ultimately, maximum effort should still be taken during any examination to assure minimal alteration of the original evidence.

Express Scan, a service provided by IPPC, is designed to conduct a quick examination of a device. Exams can be conducted prior to any installation or periodically throughout the monitoring process using the IC Toolkit USB (Windows and Mac devices). Keeping officer safety in mind, certain devices (Windows legacy machines) can be configured for remote examination (available via Enhanced package). This is especially useful if a person under supervision is reporting a technical issue that caused the monitoring application to stop capturing data. Even a one day gap of time is enough opportunity to engage in violation behavior. Express Scan can conduct an examination of the device to try and account for this “lost” time. Some examples of the type of the data collected by Express Scan is System Information, Installed Programs, Multimedia content (i.e. photos, videos), Documents, Web content (history, etc), and much more. An Express Scan user guide is available on all IC Toolkits. For more information on Express Scan or other IPPC services, please contact us by calling 888 WEB-IPPC (932-4772).



ORIGINALLY PUBLISHED OCTOBER 13, 2002 (NEWS & VIEWS vol. XXVIII, no. 21)

Compliance Analysis Versus Computer Forensics

by Senior U.S. Probation Officer - Cybercrime Specialist

Brian J. Kelly (New York Eastern)

In the world of computer and Internet crime investigations, computer forensics plays an integral part in the gathering of evidence. Law enforcement agencies around the world have dedicated entire units of highly trained individuals, along with a vast amount of resources, to tackle this issue. This process becomes more complicated and lengthy as personal computers, software applications, etc. handle more complex tasks and store massive amounts of data.

Computer forensics involves preserving digital evidence for a criminal trial. Examiners must prove that there have been no changes to the data on the seized system. To do this, they must use various software and hardware products to make a bit-by-bit copy of a seized hard drive and properly examine the contents without altering the data. This requires thousands of dollars worth of equipment and properly trained, full-time examiners.

Compliance analysis, on the other hand, is a simpler and faster process that involves viewing a defendant/offender's files at "arm's length" (i.e., pornographic images, word documents relating to identity theft, temporary internet files relating to credit card fraud). To do this, the officer does not have to make a copy of the hard drive. A computer forensic examination is usually conducted after a full investigation by a law *enforcement agency and after a search or arrest warrant has been executed. Compliance analysis is more appropriate for probation and pretrial services officers, as they are not conducting a full-blown investigation. Compliance analysis is done in the field prior to installation of monitoring software, during a random inspection, or when there is a suspicion of violation of the conditions of supervision.*

Officers performing compliance analysis should keep accurate notes of what was done and should be prepared to articulate why it was done. Officers should be trained to properly shut down and seize the system immediately if evidence of new criminal activity is detected. The system, along with the officer’s notes, can then be turned over to the proper law enforcement agency or a local electronic crimes task force that will most likely have an extensive computer forensic lab available.

A compliance analysis “field kit” can be comprised of the following items:

-Analysis Application - An application designed to scan files for images, keywords, etc., that can be launched from a CD ROM or other removable medium. It allows the officer to easily examine contents of files;

-USB Flash Drive - A small, portable means of mass storage;

-Various freeware/shareware/software tools - Small applications that can perform various tasks such as generating MD5 hash values and gathering PC system information;

-Blank floppy disks and CD-RWs;

-Labels, twist ties, small evidence bags; and

-Notebook.

Share

Tweet

Share

Forward

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET

Preferences | Unsubscribe