International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 2 –NOVEMBER 2014.

NETWORK FORENSICS

A.RaviKiran

Asst. Professor, Department of M.B.A, K.B.N College, PG Centre, Vijayawada. (AP)

Abstract— Research in the field of network forensics is gradually expanding with the propensity to fully accommodate the tenacity to help in adjudicating, curbing and apprehending the exponential growth of cybercrimes. However, investigating cybercrime differs, depending on the perspective of investigation. This paper presents the findings on the critical features for each perspective, as well as their characteristics of Network forensics. The paper also presents a review of existing frameworks on network forensics. Furthermore, the paper discussed on Network forensics: Tapping the Internet.

I. INTRODUCTION

Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.

The F.R.E.D. family of forensic workstations consists of integrated forensic processing platforms capable of handling the most challenging computer case. Available in mobile, stationary and laboratory configurations, these systems are designed for both the acquisition and examination of computer evidence. F.R.E.D. professional forensic systems, and the Digital Intelligence Ultra Bay 3d universal write protected imaging bay, deliver the ability to easily duplicate evidence directly from IDE/SAS/SATA hard drives, USB devices, C-DAC developed indigenous tools for collecting digital evidence pertinent to different areas like disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics.

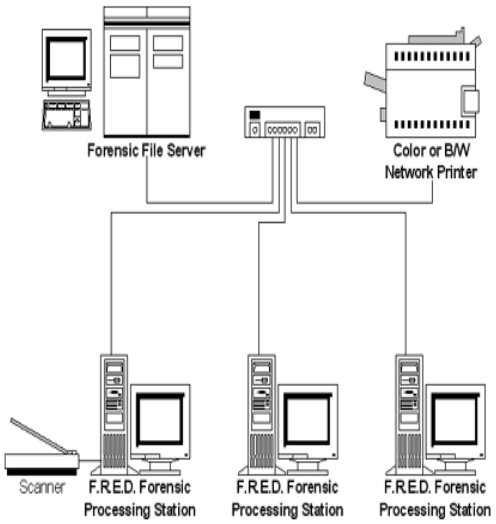
Cyber Forensic Solutions

Disk Forensics Tool: Suite with Disk imaging (True Imager), Data recovery and analysis (Cyber Check), S/W for tracing sender of e-mail, Forensic Data Carving (F-DaC), Forensic Registry analysis (F-Ran) and Forensic Thumbnail extraction (F-Tex) tools

Network Forensics Tool: Suite with Network Session Analyser (NeSA), Forensic Log Analyser and S/W for tracing sender of e-mailMobile Device Forensics Tools: Software solution for acquisition and analysis of mobile phones, smart phones, Personal Digital Assistants (PDA) and other mobile devices (Mobile Check), s/w for analysing Call Data Records of various service providers (Advik) and forensic solution for imaging and analysing SIM cards (SIMXtractor)

Live Forensics Tool (Win Lift): Software solution for acquisitions and analysis of volatile data present in running Windows systems

Portable Forensics Toolkit: True Traveller is a portable forensics toolkit.



What is a Forensic Network?

Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

A Forensic Network is a series of processing and imaging computers connected and integrated directly with a high-speed, high-capacity server to share resources. The file server operates as the backbone of the Forensic Network and is used as a central storage facility for Forensic Images as well as applications software for use by the client processing and

imaging stations. Workstation clients on the network perform the actual imaging and processing tasks, while the central file server stores the images and case work. High speed scanners and color printers can also be made available as shared resources on the network. Multiple forensic clients can access case and image files simultaneously without duplicating information on several workstations. File and image storage space is centralized at the file server reducing the localized storage requirements at the workstation clients..

Forensic networks are typically physically isolated from other networks (including the Internet) due to the sensitive nature of the data being stored. This means that the forensic network must also have its own network services such as DNS, DHCP, and user account management. Lastly, there must be support for the long-term archival of evidence utilizing removable media - typically tape backups.

How Can a Forensic Network be used?

The client workstations in a forensic network are used for the actual acquisition of forensic images. However, rather than storing those images locally on each client, the images are recorded directly to the high-capacity fault-tolerant storage array on the file server over the network. These workstations can be pre-configured to access the network directly from DOS or Windows operating environments. Only a minimum of local storage is required on each client processing station for the operating system(s) and temporary work space. In fact, CD and network PXE boot disk images are provided such that each station can be brought completely onto the network requiring absolutely no hard drive facilities at all!

The forensic file server maintains a high capacity RAID6 storage array. Each RAID module hs two redundant power supplies as a dedicated power source for the RAID array itself. This online storage is used for maintaining forensic images as well as application and forensic software and utilities. The file server is also configured with a Robotic Tape Library for system backups and offline storage of case information and images once online access to the information is no longer required. This file server comes pre-configured and installed with a highly optimized SUSE Linux Enterprise Server. Microsoft Certified (MCSE, MCPS) and Novell Certified (CNA, CNE) personnel on our staff ensure that these network operating systems are properly configured and installed prior to delivery.

Once the forensic images are recorded directly on file server storage space, any forensic client workstation on the network can be used to process the information. Images can be restored directly from the network to work drives on each client or processed in place on the file server. Multiple clients can be used to process a single image simultaneously from the network without requiring local storage at the workstations. One or more shared printers may be installed on the network in order to provide print services to all the client workstations.

The file server can also be used to store "functional" images of operating environments for testing and analysis. Symantec Ghost images can be preconfigured and stored on the file server and then restored to any of the network clients as needed. Want to see how a particular piece of software behaves in Windows? Deployment of pre-configured functional images can be a tremendous time saver when needed to research or test the behaviour of multiple operating systems!

The forensic file server not only serves as a centralized facility for the storage of forensic images, case information, and functional images, but also a resource for the production and printing of reports and other day-to-day operational requirements. Furthermore, this centralized resource can also be used to allow or deny access to any of the forensic images or information on the laboratory network as your organization's requirements dictate.

Why a Forensic Network?

Faster Than a Local Hard Drive

Image a hard drive directly to a Forensic File Server 25% faster than you can image to a local mechanical hard drive... DIRECTLY to the server over standard Copper Gigabit Ethernet. There's no need to image to your workstation and then copy it up to a slow server.

Significantly Faster Than a Windows Server

A Forensically Optimized Network Operating System is 30% faster than Windows Server running on the same hardware!

12.1 GB/Minute Imaging Speeds From Four Workstations Simultaneously

Real-world forensic benchmark utilizing Tableau Imager (TIM) to image drives connected to the Ultra Bay III on our FRED Workstations.

Keep Your Existing Clients

Use the same Operating Systems on your desktop as always (i.e. Windows 7). Our Forensic Network Operating System integrates seamlessly with your existing clients - no additional client software is required.

Centralized File Storage

Consolidate your storage investment. No need to buy lots of standalone hard drives to pass around your lab. No wondering where that case data is. Stop wasting money on individual hard drives or portable RAID arrays.

Centralized Access Control/Security

Decide who has access to what evidence from a single vantage point. Determine which investigators have access to which cases.

Centralized File Sharing

Allow multiple investigators to work on a single case using a single set of Data Files.

Centralized Data Backup

Backup and Restore data from a single vantage point into a single offline repository using a 16 tape LTO-5 robotic tape library. Maintain your data in two separate locations at all times (online and offline).

0 to 60 in Two Days

FREDC equipment is typically installed in 2 days. Equipment assembly and configuration on Day 1, and your

orientation/training on Day 2. Take your lab from an outdated workstation centric environment to a fully optimized forensic network in 2 days. (Your MIS / IT guys have been relying on networks since the late 80's - now its your turn to blow them away.)

Completely Configured

It's a complete network in a rack including all TCP/IP services (DNS / DHCP). Just connect your workstations with Cat 5e or Cat6 Gigabit Ethernet and you're ready to go! We establish a proven storage architecture that makes your access control simple and your backup activities manageable. We even set up your backup jobs and establish your automatic drive mappings for you. Instead of imaging to a local hard drive (i.e. "D:") you simply use your network drive letters instead (i.e. "R:").

Easy to Maintain

We provide approximately a full day of orientation/training for the person(s) who will be managing the server. Since our server runs like an appliance (no blue screens, no weekly patches), the routine tasks are minimal. Adding/Removing Investigator accounts, performing Backups, and modifying access control (if required) are essentially all that needs to be done.

Easy to Use

The only thing your investigators (users) will notice is new (network) drive letters. Everything else stays the same!

What Options Should be Considered When Designing a Forensic Network:

How much online RAID6 storage do you require?How many Forensic

Reading the Navy's email, the hackers hopped through a computer at Los Alamos Laboratory. And unknown to the attackers, every packet in or out of Los Alamos over the Laboratory's Internet connection was recorded and preserved for later analysis on magnetic tape.

The incident in the Persian Gulf became a cause celebre in the years that followed. Tsutomu Shimomura bragged about the incident in his book Takedown. Many experts in the field of computer security used the story as proof, of sorts, that the U.S. military was asleep at the switch when it came to computer security.

One of the more dramatic outcomes of the incident was a videotape played at the annual meeting of the American Association for the Advancement of Science in February 1993 -- a video that showed each of the attacker's keystrokes, replete with mistakes, and the results, as he systematically penetrated the defenses of the ship's computer and scavenged the system.

In the decade that followed the Gulf War, Moore's law had its way not only with processors, but with bandwidth and storage as well -- but each unequally. While the clock on the average workstation surged from 25 Mhz to 1.1 Ghz, and while the typical "big" hard drive jumped from a few hundred megabytes to 160 GB, bandwidth increased at a comparatively modest rate -- from 28.8 kbps to 384 kbps for many homes and small businesses. Even today, few businesses have more than a T1's worth of Internet bandwidth.

These trends are accelerating. For the foreseeable future, both the amount of information that we can store and our ability to process that information will far outpace the rate at which we can transmit information over large distances. As a result, where it once took the prowess of a national laboratory to systematically monitor all of the information sent over its external Internet connection, now this capability is available to all.

Today some organizations are following Los Alamos's precedent and routinely recording some or all of the traffic on their external Internet connections. Little of this information is actually analyzed. Instead, it is collected in expectation that it might be useful at some future point. After all, if you want to be able to review the information moving over your Internet connection at some point in the future, you must record it now -- fast as they are, today's processors still can't travel back through time.

Capturing everything moving over the network is simple in theory, but relatively complex in practice. I call this the "catch it as you can" approach. It's embodied in the open source programs tcpdump and windump, as well as in several commercial systems like NIKSUN's NetVCR and Net Intercept, which my company, Sandstorm Enterprises, recently brought to market.

Another approach to monitoring is to examine all of the traffic that moves over the network, but only record information deemed worthy of further analysis. The primary advantage of this approach is that computers can monitor far more information than they can archive -- memory is faster than disk. So instead of being forced to monitor the relatively small amount of network traffic at the boundary between the internal network and the external network, you can actively monitor a busy LAN or backbone.

A second advantage of this approach is privacy -- captured traffic almost invariably contains highly confidential, personal, and otherwise sensitive information: if this data is never written to a computer's disk, the chances of it being inappropriately disclosed are greatly reduced.

In some circumstances, it may not even be legal to record information unless there is a compelling reason or court order. Call this the "stop, look, and listen" approach. This approach, pioneered by Marcus Ranum in the early 1990s, is now the basis of Ranum's Network Flight Recorder (NFR) as well as Raytheon's Silent Runner, the open source snort intrusion detection system, Net Witness by Forensics Explorers, and even the FBI's "Carnivore" Internet wiretapping system (since renamed DCS 1000).

Recently, Information Security magazine coined the term Network Forensic Analysis Tool (NFAT) to describe this entire product category. (Ranum coined the term "Network Forensics" back in 1997.)

With the heightened interest in computer security these days, many organizations have started to purchase monitoring

appliances or have set up their own monitoring systems, using either commercial or open source software. If you are charged with setting up such a project, or if you are just curious about the technical, ethical, and legal challenges these systems can cause, read on.

Build a Monitoring Workstation

In many ways, a system that you would use for monitoring a computer network looks a lot like any other high-end Windows or UNIX workstation. Most run on a standard Intel-based PC and capture packets with an Ethernet interface running in promiscuous mode.

"Catch it as you can" systems immediately write the packets to a disk file, buffering in memory as necessary, and perform analysis in batches. As a result, these systems need exceptionally large disks -- ideally RAID systems. "Stop, look and listen" systems analyze the packets in memory, perform rudimentary data

This is not the result we were expecting, and it goes directly against the conventional wisdom that says SCSI is inherently better than IDE. Nevertheless, it does seem to be the ugly truth, at least for straightforward read/write tests in a single-user environment. Although we saw the highest performance with a hardware-based RAID 5 system manufactured by Advanced Computer & Network Corporation, we saw nearly the same performance with a RAID 5 system based on the 3Ware Escalade 7000 RAID controller.

Long-term storage of captured data is another problem entirely. Although you can build a terabyte RAID system for less than $2,000, backing this system up will set you back $4,000 for the AIT II tape drive and $120 for each 100GB cartridge. Absent extraordinary requirements, most users will elect not to back up their capture disks, and instead archive specific capture runs to CD-R or DVD-RAM drives.

Analysing the Data

After you've taken measures to collect the information, your next big decision will be the analysis tools that you can bring to the table. If you have built your own system, your primary analysis tools will be tcpdump and the strings command. You can use tcpdump to display the individual packets or filter a few packets out of a large data set. The strings command, meanwhile, will give you a rough

Doing the monitoring. Corporations generally have free rein to monitor their own networks, provided that employees and network users are told in advance that the monitoring may be taking place. (It is not necessary to inform the employees before each specific instance of monitoring, however, so most corporations generally inform their employees with a posted policy and leave it at that.)

ISPs are required under the Electronic Communications Privacy Act (ECPA) to protect the privacy of their customers' electronic communications they can't eavesdrop on communications or disclose intercepted contents -- unless one of the parties to the communication has given consent, or if the monitoring is needed to maintain system operations, or in cases of a court-authorized intercept.

Generally speaking, most ISPs require their users to give implicit consent to any and all monitoring as part of their "terms of service" agreement, so for most practical purposes the ECPA doesn't give ISP users any privacy at all. Law enforcement agencies have the right to monitor without the consent or the knowledge of the individuals being monitored, provided they can obtain authorization from a court. However, they have the added restriction of minimization -- they can only capture and record information specified in their warrant.

II. CONCLUSION

Full-content network monitoring is no longer the province of spooks and spies -- it's increasingly a practice that serves a variety of goals for both computer security and overall network policy. These days the underlying hardware is certainly up to the task, and some of the software that's out there, both commercial and free, is exceedingly good.

What hasn't caught up is our understanding of what to do with this technology -- what it is good for, and what uses should be declared out of bounds. In particular, few of the commercial or free offerings have facilities for watching the watchers -- that is, for logging the ways the systems have been used in an attempt to prevent misuse. Likewise, few organizations have developed policies for the appropriate use of this technology, other than catch-all .

III. REFERENCES

[1] NatarajanMeghanathan, Sumanth Reddy Allam and Loretta A. Moore, “Tools and Techniques for Network Forensics”, International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,April 2009

[2] Yong Guan, “Network forensics”, chapter 20, Computer and Information Security Handbook, Publisher: Morgan Kaufmann, Pub. Date: May 22, 2009, Print ISBN-10: 0-12-374354-0,WebISBN-10: 0080921949

[3] Sriranjani Sitaraman, SubbarayanVenkatesan, “Computer and Network Forensics”, chapter III, Digital crime and Forensic Investigation in Cyberspace Book, Edited by PanagiotisKanellis, EvangelosKiountouzis, Nicholas Kolokotronis, and DrakoulisMartakos, 2006, ISBN-10: 1591408725.

[4] Andrew Case, Andrew Cristina, LodovicoMarziale,Golden G. Richard, and VassilRoussev. Face: Automateddigital evidence discovery and correlation.Digit. Investig.,5:S65–S75, September 2008.

[5] Advanced automated threat analysis system. http://www.threatexpert.com.