Topic 1: Working with Volatile Data

Once the computer forensics investigator has ascertained the legal authority and scope of the investigation, he or she will be able to collect live volatile data from the suspect computers. Discuss with other classmates what types of data are considered volatile, and the methods by which investigators must collect and preserve volatile data. Identify the consequences of not collecting or preserving volatile data to the investigation.

Edward Jackson

5/30/2015 12:55:34 PM

Reporting is critical

Volatile data is describe as any kind of data that is available while a digital device is powered on and could be lost once the machine is turned off. For example, volatile data is stored in RAM, DNS cache files, Internet history, and cookies, as well as can be considered "live" information such as usernames, IP addresses, running services and processes, routing tables, and paging files (Easttom, 2014).

Why is capturing volatile data important in a forensic investigation? Any kind of "live" data could contain clues or become proof of a crime, and more importantly, can be used to identify a suspect. Thus, if a digital device is left on at the scene of the crime, volatile data could become critical to solving the case (Mac Forensics Lab, 2010).

Of course, capturing live data is not necessarily an easy task, and if collected improperly, could render the evidence useless. So, the methods used in the collection of live data should be scientific and only ones that have been approved by the forensic community.

According to Eroraha (2008), at netSecurity Forensic Labs, there are specific tools that should be used to collect volatile data. These tools include using Scalpel to analyze network traffic, ManTech's MDD to dump memory to an img file, RegRipper to assess the registry, and online Malware scanners if suspicious activity is still running.

While I thought that list was pretty good, there are still other important details that should be logged. For instance, the forensic investigator should always take photographs of the device screen (before they begin examining live data), the user that is logged into the device should be recorded, all details of network connections should be added to the report, and a list of the running services

and processes should be recorded. It is important to note, reporting will be essential to the investigation, thus it is imperative that every step the investigator takes be added to the forensic report. It is also crucial that *each* step have a timestamp.

As far operating system tools are concerned, there are tools in many operating systems that can aid the investigator in the investigation. For example, in Microsoft desktop operating systems there are tools such as ipconfig.exe, which will return network interface details; netstat.exe returns active sessions with port numbers and connected IP addresses; arp.exe displays current ARP entries; and route.exe "prints" to screen active routes (Microsoft, 2015).

The whole point of using all of these tools and techniques is to preserve data. Once the device has been turned off, there is no guarantee that any of that data will still be available for analysis. In most cases, the volatile data should be considered lost once the device has been powered off.

References

Easttom, C. (2014). *System forensics, investigation, and response* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.

Eroraha. (2008). Responding to the digital crime scene: Gathering volatile data. Retrieved from https://www.owasp.org/images/2/29/NetSecurity-RespondingToTheDigitalCrimeScene-GatheringVolatileData-TechnoForensics-102908.pdf

Mac Forensics Lab. (2010). Importance of volatile data. Retrieved from http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=document_general_info&cPath=5_24&products_id=197

Microsoft. (2015). Cmd.exe. Retrieved from the Microsoft operating system.

Topic 2: Policy and Procedure

As a new computer forensics investigator (and as a matter of forensics policy and procedure) you will need to understand the procedures for recovering deleted data. A computer user may make an attempt to delete information, but the file may still be available to the forensics examiner. Discuss the steps to recover deleted files in a system with a **Windows/Linux/Mac** operating system and the process of recovering files from a damaged hard drives.

Edward Jackson

5/30/2015 2:10:11 PM

Use the right tools

An important part of every forensic investigation will be finding data that has been deleted. This means the forensic investigator will need to understand the procedures for recovery data, and which tools may be used to aid them in this recovery process. Because there are many different types of operating systems on the market, the investigator should learn how to use data recovery tools for Linux, Macs, and Windows.

In my research, I found tools and commands that can be used in the recovery of files for all three operating systems. For Linux, a couple simple commands are: $**rm** -rf /path/to/myfile, **dd** if=/dev/mapper/wks01-root of=recovered.file.001 bs=4096 count=1 skip=7235938,# file recovered.file.001 (Stack Exchange, 2013). A more robust method to recovering Linux files is to use third party software. I found the Stellar Linux Data Recovery software, which is meant to aid the investigator in quick recovery, advanced recovery, deleted file recovery, and searching a lost volume (Stellar Data Recovery, 2011). The advantages of using software is that the recovery process will be more intuitive (using a GUI), return much more data, and the investigator will be able to save and load images for analysis.

For Macs, I did find a few commands that could be used to recover files; they were very similar to the Linux commands---for example, you could use **rm** -rf ./Desktop/myScript.sh. But, I went searching for software. I found EaseUS Data Recovery Wizard for Mac (there is a Windows version as well!). The EaseUS software will scan a Mac partition and return deleted files matching: graphic, documents, audio, video, email, archive, and other (EaseUS, 2015). The advantage of using this software is that files are returned with their original names and all of their original content. Just as a matter of information, I also found three other software apps to recovery Mac files; they are SubRosaSoft, FileSalvage, and Prosoft Data Rescue.

Finally, for Windows machines, it was no surprised that the most amount of undelete/recovery software applications were returned. The first one that came back in the search engine was Recuva. Recuva is recovery software that will undelete, unerase, and recover files from damaged disks (Piriform, 2015). One

thing I liked about the Recuva software is that it can recover data from the Windows computer, recycle bin, MP3 players, and even digital memory cards. For information purposes, other great recovery applications include Undelete Plus, PC Inspector, File Recovery, and Restoration (Pash, 2008).

References

EaseUS. (2015). EaseUS data recovery wizard for Mac. Retrieved from http://www.easeus.com/mac/mac-data-recovery-resource/recover-mac-deleted-file-from-trash.htm

Pash. (2008). How to recover deleted files with free software. Retrieved from http://lifehacker.com/393084/how-to-recover-deleted-files-with-free-software

Piriform. (2015). Recuva. Retrieved from https://www.piriform.com/recuva

Stack Exchange. (2013). Unix/Linux undelete/recover deleted files. Retrieved from http://unix.stackexchange.com/questions/80270/unix-linux-undelete-recover-deleted-files

Stellar Data Recovery. (2011). How to recover deleted files from a LINUX volume using Stellar Linux Data Recovery software? Retrieved from http://www.stellarinfo.com/support/kb/index.php/article/recover-deleted-files-from-linux

Procedures and Best Practices

This unit looks at forensics procedures and best practices pertaining to the collection and processing of physical, logical, and special content data. After this unit you will be able to explain how the investigators perform the various evidence collection, documentation, and preservation actions. In addition to the study of forensics collection, this unit identifies the steps of a forensic investigation during this early stage and explains how to perform the preliminary volatile evidence collection from a live system.

Outcomes

After completing this unit, you should be able to:

- Determine the procedures for processing the incident scene and collecting physical evidence including physical computer evidence.
- Evaluate the procedures for processing the incident scene for digital and logical evidence, volatile data, and special content data.

Course outcome(s) practiced in this unit:

IT550-3: Select forensic analysis tools for securing digital evidence and investigations.

What do you have to do in this unit?

- Complete assigned Reading.
- Participate in Discussion.
- Complete unit Assignment.
- Participate in Seminar or complete Alternative Assignment.
- Complete the optional Learning Activity.

Read Chapters 6 and 8 in*System Forensics, Investigation, and Response.*

Key Terms | Unit 3

Forensics: Data imaging of common computer types.

Physical evidence: Physical evidence related to documents, or printouts.

Logical evidence: Evidence gained from the Operating System and File Structure.

Live collection: Data collection from a live system or network.

Digital evidence: Evidence stored or transmitted in a digital form.

Evidence transport: Use of tools and equipment for evidence transport.

Forensics acquisition: Acquiring the physical evidence and digital forensics data.

Forensic examination: Physical and logical examination of forensics data, and drive details.

Forensic analysis: Performing file, data hiding, and time frame analysis.

Attending live Seminars is important to your academic success, and attendance is highly recommended. The Seminar allows you to review the important concepts presented in

each unit, discuss work issues in your lives that pertain to these concepts, ask your instructor questions, and allows you to come together in real time with your fellow classmates. There will be a graded Seminar in Units 1 through 5 in this course. You must either attend the live Seminar, or you must complete the Seminar alternative assignment in order to earn points for this part of the class.

Option 1: Attend Seminar:

The Seminar will look into the Unit 3 topics and Assignment, as well as an introduction to the VSCL hands-on labs for the course.

Remember, if you do not participate in the weekly Seminar, you need to complete the alternative assignment.

Outcomes addressed in this activity:

Unit Outcomes:

- Determine the procedures for processing the incident scene and collecting physical evidence including physical computer evidence.
- Evaluate the procedures for processing the incident scene for digital and logical evidence, volatile data, and special content data.

Course Outcome:

IT550-3: Select forensic analysis tools for securing digital evidence and investigations.

Assignment Instructions:

This Assignment provides the hands on element to your studies. It gives you the opportunity to gain practical experience using the tools and techniques associated with performing a Byte-Level computer audit. Complete the lab entitled **"Documenting a Workstation Configuration Using Common Forensics Tool"** using the document in Doc Sharing.

Individual Virtual Lab Project:
Perform a computer audit using the following tools:
a. WinAudit
b. DevManView
c. Frhed

Lab Details: To be provided through the detailed instruction for using VSCL as given by Jones & Bartlett Learning, LLC.

Save your document and any screen shots in a zip file using the following file name format: Username-IT550-Assignment-Unit# (Example: TAllen-IT550 Assignment-Unit3). Submit your file to the Unit 3 Assignment Dropbox by the end of Unit 3.

Written Assignment Requirements:

All lab steps are completed, including screenshots and explanations where required. Assessment question answers contain sufficient information to adequately address the questions. The lab report and the answers are accurate and complete, as well as free from grammar and spelling errors.

For more information and an example of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable Assignments and Discussion posts. If you have any questions, please contact your professor.

Assignment Requirements	Points Possible	Points Earned
Student was able to successfully use forensic tool called WinAudit to perform scenario based investigations and submitted the required screenshots showing understanding and usage of the tool.	0–20	
Student was able to successfully use forensic tool called DevMan View to perform scenario based investigations and submitted the required screenshots showing understanding and usage of the tool.	0–20	
Student was able to successfully use forensic tool called Frhed to perform scenario based investigations and submitted the required screenshots showing understanding and usage of the tool.	0–20	
Assessment worksheet for the lab "Documenting a Workstation Configuration Using Common Forensics Tool" is completed, with responses that are accurate, complete and well-written.	0–40	
Total (Sum of all points)	0–100	
Less points deducted for spelling, grammar and APA errors.		

http://kucourses.com/re/DotNextLaunch.asp?courseid=11502612&userid=8468444&sessionid=c3f51f543a&tabid=27gRodvJXiiBfVKg+f8NzdYkwUrLERVG5kiKtEbIBf8Ttbi1vusxRuUYaRAsJyqlcljozNerzvACgQ450x4rvw==&sessionFirstAuthStore=true&macid=spbYa+d7DjF6dptJ2lZb/q1GRr3ds/6N20gAmqVs9ELw82T2Y7PJjGT/kkUo8mNL1RGIvmJXEt7ukHdrRT1QQtX4qeCE5ulK3baQn87eXXEhIjk6K1FjUudOxTB+4pu6GYzVati3w6/6+I8VaL8Cvh9KAr9VawpoMeqT5+57ykZHSKD7OwjN6ipDQsZ6VxjICi5aVqluRF3wQRfTETsrj9kXxHniqnehITw/+Nrs2wrwpG9MktxlpeN3P00UN0Fs

Access the Labs Below:

- Unit 3: Documenting a Workstation Configuration using Common Forensic Tools
- Unit 4: Automating E-mail Evidence Discovery Using P2 Commander
- Unit 5: Decoding an FTP Protocol Session for Forensic Evidence