**POST MORTEM EXAMINATION CHECKLIST**

**WINDOWS SYSTEM**

|  |  |  |
| --- | --- | --- |
| YOUR LOGO HERE |  | Your Contact Information Here |

Review

1. Lab request form is reviewed for information

2. Search authority is confirmed for forensic analysis

3. Case agent is called to ensure the exam is still needed and to ask any questions

System Hardware Examination

1. Photograph all four sides of the computer

2. Open case and photograph interior of computer

3. Remove hard drive(s) if possible

4. Photograph hard drive label and jumper settings (if present)

Case Folder Creation

1. Create main case folder \\forensic files\year\case #

2. Create subfolder for each piece of evidence, ex: \\forensic files\year\case#\Item #1

Forensic Imaging

1. Connect hard drive to hardware write blocker

2. Image drive using validated imaging tool

3. Place image file in appropriate folder created in forensic files folder

4. Take screen capture showing drive geometry and partition information

Registry File Exportation

1. Export the SAM, System, and all NTUSER.dat registry hives

2. View the System hive to find out time zone settings

BIOS Examination

1. Once hard drive is removed or disconnected turn on computer and check BIOS

2. Note date/time settings

1. Note clock used to compare time settings (e.g., atomic clock / cellular phone)

SAM File Cracking

1. Using DNA/PRTK crack the SAM file for any account passwords and document findings
2. Print cracked password results as a .pdf and include it in the report
3. Consider using a word list from FTK if password is not cracked as expected
4. Dump the NTUSER.dat registry hives into PRTK and print report as .pdf

Forensic Computer Settings

1. Change time zone settings to reflect the same as the suspect’s computer
2. Change the system time to match the BIOS time found on the suspect computer
3. Ensure a/v software has latest definitions update prior to examination

Case Processing with Forensic Tool

1. Process case with forensic tool of choice
2. Save the case processing files in the \\forensic files\year\case#\Item#
3. Consider data carving options

Create Virtual Machine (VM)

1. Mount the forensic image using FTK Imager
2. Create a VM of the image file
3. Create a folder called case #, item #, VM (ex: - 08-0001-1-VM)
4. Save the VM to the above folder
5. Copy the folder to the \\cases\year\case#\folder
6. Launch the VM of the suspect computer and take necessary screen captures

Malware and Rootkit Scan

1. Using a/v tool, scan the mounted drive(s) for malware and report on any findings

Begin Forensic Examination Report

1. Using the Word template begin the forensic report
2. Save the report to the \\cases\year\case#\Reports\Report.docx
3. Keep forensic report up to date with the forensic analysis

Forensic Analysis

1. Review file structure and overall layout of media
2. View all registry files and begin doing registry analysis

SAM Registry Hive Analysis

1. Document the user accounts and screen capture all user created accounts
2. Ensure that last logon times, SID’s/RID’s, logon count, etc. are shown in screen capture
3. Include all user accounts in SAM report
4. Include anything else pertinent to the investigation
5. Create html report of SAM hive

System Registry Hive Analysis

1. Document the time zone settings
2. Document the computer name
3. Document the USB storage devices and mounted devices
4. Include anything else pertinent to the investigation
5. Export this information to the html report

Software Registry Hive Analysis

1. Document the OS and OS installation date
2. Document programs set to run upon startup
3. Document registered owner and organization
4. Include anything else pertinent to the investigation
5. Export this information to the html report

NTUSER.Dat Registry Hive Analysis

1. Document typed URL’s
2. Document MRU’s
3. Document last opened/saved
4. Document special software settings
5. Document protected storage system provider
6. Include anything else pertinent to the investigation

Additional Analysis

1. Perform forensic analysis based on investigative needs
2. Conduct needed keyword searches
3. Export files as needed
4. Compare information from VM to Forensic Results to find additional evidence
5. Document everything in report
6. Export findings to html report

Other tools

1. Consider using other forensic tools such as NetAnalysis, File Extractor Pro, etc.

Create Folder Structure for CD/DVD Report

1. Create folder within \\cases\year\case#\CD
2. Inside CD folder create folder “Reports”
3. Within “Reports” folder place Word report and create a .pdf report from the Word report
4. Modify the contents html page to include all needed bookmarks
5. Move all data over from Forensic Exam folder under the “Report” folder
6. Modify the “Master Banner” html page to show correct agency and case number

Report Approval

1. Send the report to supervisor for peer/technical review
2. Comments will be placed into the report using Word’s review function
3. Correct any items and resubmit for approval
4. Create CD/DVD once approval is given to distribute the report

This is developed to be a guideline for forensic examiners. It is understood that cases may present special circumstances which will require the examiner to deviate from this checklist.