# Unix/Linux LIVE RESPONSE

*A quick reference guide*

This quick reference guide (QRG) provides the first steps to be taken in Unix/Linux systems in case of any incident. The QRG includes the important commands to be used quickly to collect volatile and select some important non-volatile data.

## Collecting Volatile Data

| No. | Task | Explanation |
|---|---|---|
| 1 | Mount your Thumb Drive<br>*If not automatically detected and done: cd /media/ | • Create a mount folder<br>  ○ mkdir /mnt/mount1<br>• Check TD device:<br>  ○ fdisk -l<br>locate your TD by checking the type column<br>• Mount your TD<br>  ○ mount /dev/sdb# /mnt/mount1<br>where cdrom is your TD device<br>• Change to the new pointed point with root privileges<br>  ○ Sudo su cd /mnt/mount1 |
| 2 | Execute a trusted shell | • Run the trusted shell from your TD<br>  ○ [root@name /mnt/mount1] # ./bash |
| 3 | Record the system date and time | • [root@name /mnt/mount1] # echo "Case Number (), Responder Name: (your name), Start Time and date:" >> (path where to store)/date_time.txt<br>• [root@name /mnt/mount1] # ./date >> /(path where to store)/date_time.txt |
| 4 | Record the watch (real) date and time | • [root@name /mnt/mount1] # echo "Watch date and time are: **(Enter the real time here)**" >> /(path where to store)/date_time.txt |
| 5 | List apps associated with open ports | • [root@name /mnt/mount1] # ./netstat –anp >> /(path where to store)/apps.txt<br>• [root@name /mnt/mount1] # ./lsof -n >> /(path where to store)/apps2.txt |
| 6 | List all open files | • [root@name /mnt/mount1] # ./lsof >> /(path where to store)/open_files.txt |
| 7 | Determine open ports | • [root@name /mnt/mount1] # ./netstat –an >> /(path where to store)/all_open_ports.txt<br>• [root@name /mnt/mount1] # ./netstat -ln >> /(path where to store)/open_ports_listening.txt |
| 8 | List all running processes | **(Standard syntax)**<br>• [root@name /mnt/mount1] # ./ps –ef >> /(path where to store)/running_process.txt<br>Or<br>**(BSD syntax )**<br>• [root@name /mnt/mount1] # ./ps –aux >> /(path where to store)/running_process.txt |
| 9 | List recent connections (routing) | • [root@name /mnt/mount1] # ./netstat –rn >> /(path where to store)/route_table.txt<br>• [root@name /mnt/mount1] # ./ip route list >> /(path where to store)/ip_route_list.txt |
| 10 | Get clipboard contents | • [root@name /mnt/mount1] # ./xsel -b >> /(path where to store)/clipboard_contents.txt |
| 11 | Record arp cache | • [root@name /mnt/mount1] # ./arp -a >> /(path where to store)/arp_cach.txt |
| 12 | Look for suspicious connection - sniffers | • [root@name /mnt/mount1] # ./netstat –i >> /(path where to store)/suspicious_connection.txt |
| 13 | Take a memory snapshot using LiME (d)<br>*Optional at this stage* | Check Resources section for downloading LiME<br>• [root@name /mnt/mount1] # cd ./LiME/src/<br>• [root@name /mnt/mount1] # make<br>• [root@name /mnt/mount1] # insmod **kernel_name** "path=**(path where to store)**/test.mem format=lime" |

## Collecting Non-Volatile Data

| No. | Task | Explanation |
|---|---|---|
| 1 | Record IP information | [root@name /mnt/mount1] # ./ip addr show > /(path where to store)/ip_info.txt |
| 2 | Record checksums for all files | [root@name /mnt/mount1] # ./find / -type f –xdev –exec ./md5sum -b {} \; > /(path where to store)/all_checksums.chk |
| 3 | Record system information and variables | • [root@name /mnt/mount1] # ./uname –a >> /(path where to store)/system_info.txt<br>• [root@name /mnt/mount1] # set >> /(path where to store)/set.txt |
| 4 | Determine who is logged on, last logged on, and failure logon attempts | • List who is logged on:<br>  ○ [root@name /mnt/mount1] # ./w >> /(path where to store)/whoison.txt<br>• Last log on:<br>  ○ [root@name /mnt/mount1] # ./last >> /(path where to store)/Last_loggedon.txt<br>• Failure login attempts:<br>• [root@name /mnt/mount1] # ./lastb >> /(path where to store)/failure_loggedon_attempts.txt |
| 5 | Record modification, and access times of all files | • List access time for all files:<br>  ○ [root@name /mnt/mount1] # ./ls –alRu / >> /(path where to store)/accessTime_All.txt<br>• List inode modification time:<br>  ○ [root@name /mnt/mount1] # ./ls –alRc / >> /(path where to store)/inode_modificationTime_All.txt<br>• List modification time for all files:<br>• [root@name /mnt/mount1] # ./ls –alR / >> /(path where to store)/modificationTime_all.txt |
| 6 | List scheduled tasks | • [root@name /mnt/mount1] # ./crontab -l >> /(path where to store)/schedualtasks.txt<br>• [root@name /mnt/mount1] # ./crontab -l -u root >> /(path where to store)/schedualtasks_root.txt |
| 7 | List mounted file systems | • [root@name /mnt/mount1] # ./mount >> /(path where to store)/mounted_devices.txt |
| 8 | List partition table | • [root@name /mnt/mount1] # ./fdisk -l >> /(path where to store)/partitions_table.txt |
| 9 | Collect system logs | • Locate below binaries that need specialized apps to access and copy them to your TD:<br>  ○ sudo find / -iname "**logname***" -type f<br>(important log files: utmp, w wtmp, last, lastlog , lastlog, pacct , lastcomm- can be found in /bin, /sbin, /usr/bin, /usr/sbin)<br><br>Copy below important directories:<br>• [root@name /mnt/mount1] # ./cp -r /var/ /(path where to store)/<br>• [root@name /mnt/mount1] # ./cp -r /temp/ /(path where to store)/<br>• [root@name /mnt/mount1] # ./cp -r /dev/ /(path where to store)/<br>• [root@name /mnt/mount1] # dmesg –T >> (path where to store)/dmesg_logs.log |
| 10 | Record KLM (Kernel Loaded Modules) | [root@name /mnt/mount1] # ./lsmod >> (path where to store)/loaded_modules_list.txt |
| 11 | Copy important config files | • [root@name /mnt/mount1] # ./cp -r /etc/ /(path where to store)/<br>If there is a time constrain, copy the below files then extract the others from the image:<br>  ○ /etc/passwd<br>  ○ /etc/shadow<br>  ○ /etc/group<br>  ○ /etc/hosts<br>  ○ /etc/host.equiv<br>  ○ ~/.rhosts<br>  ○ /etc/hosts.allow<br>  ○ /etc/hosts.deny<br>  ○ /etc/syslog.conf<br>  ○ /etc/inetd.conf<br>/etc/xinetd.conf |

## After Completing the Collection

| No. | Task | Explanation |
|---|---|---|
| 1 | Records system date and time | • [root@name /mnt/mount1] # echo "Completed at:" >> (path where to store)/date_time.txt<br>• [root@name /mnt/mount1] # ./date >> /(path where to store)/date_time.txt |
| 2 | Document commands used during your response | • [root@name /mnt/mount1] # ./history >> /(path where to store)/command_history.txt |
| 3 | Unmount your TD | • [root@name /mnt/mount1] # umount /mnt/mount1 |
| 4 | OPTIONAL: Capture the entire hard drive | After doing the first response and capturing all volatile and selected non-volatile data, start to create full image desk by using dd:<br>• Identify the main desk (look for root directory /):<br>  ○ [root@name /mnt/mount1] # ./df<br>• Calculate the original MD5 for the disk<br>  ○ [root@name /mnt/mount1] # ./md5sum /dev/"disk" > /(path where to store)/original_checksum.txt<br>• Start capturing the disk:<br>  ○ [root@name /mnt/mount1] # dd if=/dev/'disk' of=(path where to store)/disk.img bs=1k<br>• Calculate the checksum of the image file:<br>  ○ [root@name /mnt/mount1] # ./md5sum /( path where to store)/disk.img > /(path where to store)/image_checksum.txt<br>• Compare and verify the two checksums<br>  ○ [root@name /mnt/mount1] # ./cat /(path where to store)/*_checksum.txt |

## Resources

| No | Tool/Resource | Website |
|---|---|---|
| 1 | LiME | • Download: https://github.com/504ensicsLabs/LiME<br>• Install: https://www.jamesbower.com/linux-memory-analysis/ |
| 2 | Installing MD5sum | • sudo apt install -y ucommon-utils<br>• md5sum --version |
| 3 | man command | • Use **man** command with any tool in case if you need more information<br>• https://ss64.com/bash/man.html |