Using trusted shell and binaries from incident response CD:

Perform the following steps:
Mount the ISO image on /media/Trusted_tools directory using this command:

```
$mount /Trusted_tools.iso  /media/Trusted_tools
```

Verify that the ISO image has been mounted successfully. Use `df` command to check the mounted drives:

```
root@ubuntu:/home/ipar# df

Filesystem 1K-blocks  Used  Available  Use%  Mounted on
/dev/loop1 12998      12998 0          100%  /media/Trusted_tools
```

Now, the PATH environment variables (where the system would look for binaries and shared libraries) should be set so that only trusted binaries and shared libraries are used.

Command	**Purpose**
`gnome-terminal -e /media/Trusted_tools/bin/bash`	Start a known good shell from mounted Trusted_tools CD
Use the new shell (Terminal Window) for further steps	
`sudo su`	Gain the root access (use the ipar user account password)
`cd /media/Trusted_tools /bin`	Move to the mounted directory containing the known good binaries.
`PATH=“/media/Trusted_tools/bin”`	Set the PATH variable to the location of the known good binaries
`LD_LIBRARY_PATH=“/media/Trusted_tools/lib”`	Set the LD_LIBRARY_PATH variable to the location of the known good libraries i.e. /media/Trusted_tools /lib
`export PATH`	Make the PATH variable to be in the environment. The subsequently executed commands will use this path for binaries
`export LD_LIBRARY_PATH`	Add the LD_LIBRARY_PATH variable to be in the environment. The subsequently executed commands will use this path to access shared libraries.
`echo $PATH`	Verify the PATH variable
`echo $LD_LIBRARY_PATH`	Verify the LD_LIBRARY_PATH variable

For entire incident response process, make sure that you use the trusted shell (terminal window) to run the tools/commands only from Trusted_tools directory.