Using trusted tools for incident response:

The tools available on the compromised system should not be used for incident response. A CD or USB drive of relevant tools from a trusted system must be used for live forensics and evidence collection. Incident response CDs (such as Helix and F-response) can be purchased for professional use.

A CD image of known trusted binaries can be created by following methods:

Method 1:
Compile the tools using static linking method. Static linking assembles all files together during compilation and therefore the executable binaries will not depend on any shared libraries. Save the binaries in a folder and burn that folder on to the CD.

Method 2:
The executable files produced by static compilation are comparatively larger in size. Alternatively, shared libraries from a trusted source be shared by the binaries to address the size requirement. The binaries and library dependencies are saved in bin and lib directories respectively.

1. Create a directory e.g. “Trusted_tools”.
2. Move to Trusted_tools and create two directories – “bin” and “lib”.
3. Copy the binaries of desired utilities such as bash, lsof, ps, top, cat etc. to the “bin” directory. E.g.

```
$cp /bin/lsof  /Trusted_tools/bin
```

4. Which command can be used to find the location of binaries. E.g.

```
$which lsof
```

5. Use ldd to find the shared libraries for each tool and save those in lib directory. E.g.

```
$ldd /bin/lsof

$cp /lib/x86_64-linux-gnu/libc.so.6 /Trusted_tools/lib
```

6. Create an ISO image of the Trusted_tools directory.

```
$mkisofs -o Truested_tools.iso /trusted_tools
```

7. Burn the ISO image on to the CD. Use the tools from the CD for incident response.

An ISO image of trusted tools has been created for this exercise. The ISO image is provided in root directory.