Karnataka High Court provides useful guidelines of Seizure of electronic evidence

Minimum guidelines may be implemented by the Police for seizure

- When carrying out a search of the premises as regards any electronic equipment, Smartphone or e-mail account the search team to be accompanied by a qualified Forensic Examiner.
- When carrying out a search of the premises, the investigating officer should not use the computer or attempt to search a computer for evidence. The usage of the computer and/or search should be conducted by a properly authorized and qualified person, like a properly qualified forensic examiner.
- At the time of search, the place where the computer is stored or kept is to be photographed in such a manner that the connections of wires including power, network,. etc., are captured in such photographs.
- The front and back of the computer and or the laptop while connected to all the peripherals are to be taken.
- A diagram should be prepared showing the manner in which the computer and/or the laptop is connected.
- If the computer or laptop is in the power-off mode, the same should not be powered on.
- If the computer is powered on and the screen is blank, the mouse could be moved and as and when the image appears on the screen, the photograph of the screen to be taken.

Minimum guidelines may be implemented by the Police for seizure .. Cont.

- If the computer is powered on, the investigating officer should not power off the computer. As far as possible, the investigating officer to secure the services of a computer forensic examiner to download the data available in the volatile memory i.e., RAM since the said data would be lost on the powering down of the computer or laptop.
- If the computer is switched on and connected to a network the investigating officer to secure the services of a forensic examiner to capture the volatile net work data like IP address, actual net work connections, net work logs, etc.,
- The MAC address also to be identified and secured,
- In the unlikely event of the Forensic examiner not being available, then unplug the computer, pack the computer and the wires in separate faraday overs after labeling them.
- In case of a laptop if the removal of the power cord does not shut down the laptop to locate and remove the battery.
- If the laptop battery cannot be removed, then shut down the laptop and pack it in a faraday bag so as to block any communication to the said laptop since most of the laptops, nowadays have wireless communication enabled even when the laptop is in the stand by mode.

Minimum guidelines may be implemented by the Police for seizure .. Cont.

- Seizure of networked devices: Apart from the above steps taken as regards seizure of the computer, laptop, etc., if the said equipment is connected to a network:
- To ascertain as to whether the said equipment is connected to any remote storage devices or shared network drives, if so to seize the remote storage devices as also the shared network devices.
- To seize the wireless access points, routers, modems, and any equipment connected to such access points, routers, modems which any some times be hidden.
- To ascertain if any unsecured wireless network can be accessed from the location. If so identify the same and secure the unsecured wireless devices since the accused might have used the said unsecured wireless devices.
- To ascertain who is maintaining the network and to identify who is running the network – get all the details relating to the operations of the network and role of the equipment to be seized from such network manager.
- To obtain from the network manager, network logs of the machine to be searched and/or seized so as to ascertain the access made by the ·said machine of the net work.

Minimum guidelines may be implemented by the Police for seizure .. Cont.

Mobile devices:

- Mobile devices would mean an include smartphone mobile phone, tablets GPS units, etc., during the course of seizure of any of the mobile devices apart from the steps taken in respect of a computer and/or laptop, the following additional steps to be taken.
- Prevent the device from communicating to network and/or receiving any wireless communication either through wifi or mobile data by packing the same in a faraday bag.
- Keep the device charged throughout, since if the battery drains out, the data available in the volatile memory could be lost.
- Look for slim-slots remove the sim card so as to prevent any access to the mobile network, pack the sim card separately in a faraday bag.
- If the device is in power off mode, the battery could also be removed and kept separately.
- If the device is powered on, then put it in an aeroplane mode in android device or airplane mode in a lOS device. 17.8. In an the cases above, the seized equipment should be kept as far as possible in a dust free environment and temperature controlled.
- While conducting the search, the investigating officer to seize any electronic storage devices like CD, DVD, Blu-Ray, pen drive, external hard drive, USB thumb drives, solid-state drives etc., located in the premises, label and pack them separately in a faraday bag.
- The computer storage media, laptop, etc., to be kept away from magnets, radio transmitters, police radios etc., since they could have an adverse impact on the data in the said devices.
- To carry out a search of the premises to obtain instructions manuals, documentation, etc., as also to ascertain if a password is written down somewhere since many a time person owning equipment would have written the password in a bo0k, writing pad or the like at the said location.
- The entire process and procedure followed to be documented in writing from the time of entry of the investigation/search team in to the premises until they exit.