Que: Mobile Forensics Methodology in detail.

Ans: Broadly speaking there are 3 different methods of extracting evidence: physical acquisition, logical acquisition and filing system acquisition.

• Physical acquisition: this is often commonly the foremost used method. It consists of creating a uniform replica of the first , thereby preserving all potential evidence. This procedure has the advantage of it being possible to look for deleted elements. Its main disadvantage is its complexity compared to the opposite methods and therefore the time that it takes to hold it out.

• Logical acquisition: this consists in making a replica of the objects stored on the device. This makes use of the mechanisms implemented natively by the manufacturer, that is, people who are normally wont to synchronise the terminal with a computer in order that the specified information is requested from the mobile device's OS . it's the advantage of being a way simpler process than the previous one, although it doesn't allow an excellent amount of data to be accessed.

• File system acquisition: this enables all visible files to be obtained through the filing system , which doesn't include deleted files or hidden partitions. counting on the sort of investigation, it's going to be sufficient to use this method, which is a smaller amount complex than physical acquisition. to hold it out we employ the mechanisms integrated within the OS to repeat the files, Android Device Bridge (ADB) for Android. Through this method, it's possible to recover certain deleted information since some operating systems like Android and iOS employ a structure that uses SQLite databases to store much of the knowledge . during this way, when file records are deleted, they're only marked as available to be overwritten and, as such, they temporarily remain available, and it's therefore possible to recover them.

When it involves selecting the foremost suitable method, many aspects are taken under consideration , such as: the extent of thoroughness required, the deadline for completing the method , which sort of data it's necessary to obtain: volatile information, previously deleted information, information from third party applications, etc.

Another more practical method which will be useful when choosing the foremost suitable/possible way of acquiring evidence is that the following diagram, during which account is taken of various aspects like whether the USB debugging is activated, whether the terminal is locked or if there's access, etc.

If the method goes to be administered manually, one or more of the subsequent actions need to be performed:

- If the device is rooted we will attempt to remove the gesture.key or password.key enter accordance with the mode of protection established, which are stored in /data/system/ or copy them and decipher the pattern through a hash dictionary, like AndroidGestureSHA1, employing a tool like Android Pattern Lock Cracker for this.
- Install a personalised recovery like ClockWorkMod or Team Win Recovery Project (TWRP)and subsequently deactivate device access locking.
- The problem of fragmentation on mobile platforms causes the overwhelming majority of devices to be affected with vulnerabilities which will not be resolved for these models and, as such, counting on the Android version, it's possible to use a number of them to obtain access to the device, like CVE-2013-6271.
  Using brute force.

- When a 4-digit pin is employed as a security measure it’s been demonstrated that it’s possible to get it during a short period of your time , in around a maximum period of 16 hours.
- A more sophisticated technique could even be used, as was demonstrated by various members of the IT department of the University of Pennsylvania in what they called a Smudge Attack, which consists of obtaining the locking pattern from fingerprints on the screen of the mobile device, using photographs from different angles for this purpose, modifying the properties of sunshine and colour.