Forensics with the evidences that can be

Design, Architecture

Forensics is branch ofscience that deals with the evidences that can be presented in the Court ofLaw.

Its sub-domain that deals with acquiring and analysing data from computers, smartphones and other digital devices is known as digital forensics. TheOperating System (OS) used in Android smartphones is derived from those used incomputers. Due to therapid growth in mobile technology, new challenges have been introduced forforensic investigators.

The speed at which new models are being designed andlaunched makes the application of old forensic procedures very difficult. Eachcase or investigation of the new model needs to be considered differently andrequires steps which could be different and unique to the case. With thesechallenges in mobile forensics 1, syncing mobiles phone to a computer usingsoftware becomes difficult. Androidsmartphones are the most popular choice in the already crowded mobile phonemarket.

They are gaining even a higher market share with exponential growthrate. The reason for the popularity of these devices is that they are featurerich, cost efficient and user friendly. Android smartphones provide a number offeatures and data centric information such as data files, contact details, runningapplications, games and many more. The data from these devices can be extractedusing various forensic tools which are both open source and paid. However, there is no simple universally accepted method which can be used with 100 %surety to fetch data from Android smartphones in a forensically sound mannerThe established approach to digital forensics 2 (developed for personalcomputers) is generally inappropriate for Android

smartphones. Consequently, recovering evidences from the Android smartphones in accordance withestablished principles of forensic evidence is complex and time consuming.

The architecture of a commercial mobile analysistool is not open source, primarily to protect the commercial interests of the manufactures. Hence, an investigator or a researcher is unable to capture the data flowbetween the tool and the mobile device, the memory map of the device and otherfiner details which can help him in gathering the data from the point ofcarrying out forensics. However, all tools use simple android based commands inthe backend, which are nothing but Linux commands to access the mobile. In simple terms, an android device can betreated like a memory card connected to a computer from which photos need to beaccessed. However, the difference is that in case of an android mobileconnected to a forensic workstation, it does not open an auto play window togive access to the treasure stored inside it. This information has to bemanually extracted through android commands from it.

Towards this, the androidarchitecture 3 which is Linux based as depicted in Fig 1, was studied indetail. Mobile forensics whichdraws its lineage from digital forensics deals with forensic analysis of mobiledevices. Hence, mobile can be called as an Android world. The most popularoperating system being used in mobile phones is Android, iOS and Windows withWindows phone stated to be obsolete soon, Android which is already a worldleader, would further garner a strong support among mobile users. Thereforethis research is focused on Android mobiles, nonetheless other OS based mobilesare also

being studied to find newer methods of data extraction. In the case of Mobileforensics an investigator focuses on mainly two types of acquisition i.

e. physical and logical. Logical acquisition encompasses acquiring the file systemof the device which includes the system files and the user data. The physicalacquisition includes the physical memory of the mobile device including thedeleted data. The general tendency is to delete the data from the mobile aftercommitting a crime. Hence, there is a lot of emphasis on recovering deleteddata from the mobile phone. One very importantdifference between PC and mobile forensics is the preservation of integrity.

Since a mobile cannot be imaged in a similar way as a hard drive, preservationof integrity of digital evidence becomes difficult. With disk encryption beingadopted for mobile data protection, the forensic analysis process becomes allthe more challenging. Non availability of costly commercial forensic analysistools and lack of expertise further compounds the problem. In this paper, androiddebugging bridge (adb) commands have been used to extract the data manuallyfrom the android phone. Using these commands the complete memory of the phonecan be accessed thereby easing the process of forensic analysis. For thepurpose of this research, a two pronged approach has been followed.

First, thedata extraction has been done using a virtual android device created in anandroid emulator like genymotion 4. Second, a real device having the same ornearly matching android kernel version is taken and the process is repeated toestablish the authenticity of the research being done.