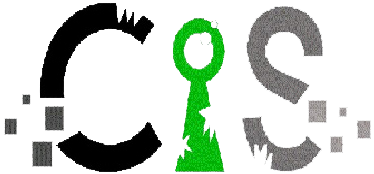
****

**Standard Operating Procedure for Mobile Forensics**

V.1.0

Document details:

|  |  |
| --- | --- |
| Created by | Vaibhav Sharma |
| Created on | 24-09-2018 |
| 1st Level approval by |  |
| 2nd Level approval by |  |

Document history:

|  |  |  |
| --- | --- | --- |
| Updated on | Updated by | Remarks |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1. Introduction 3](#_Toc525807522)

[2. Abbreviations used in Naming cases 3](#_Toc525807523)

[3. Naming Convention 3](#_Toc525807524)

[4. Methods 4](#_Toc525807525)

[a. ADB Push 4](#_Toc525807526)

[i. Software 4](#_Toc525807527)

[ii. Preparation 4](#_Toc525807528)

[iii. Acquisition and Authentication 4](#_Toc525807529)

[iv. Data Analysis 4](#_Toc525807530)

[v. Reporting 5](#_Toc525807531)

[b. ADB DD Image 5](#_Toc525807532)

[i. Software 5](#_Toc525807533)

[ii. Preparation 6](#_Toc525807534)

[iii. Acquisition and Authentication 6](#_Toc525807535)

[iv. Data Analysis 6](#_Toc525807536)

[v. Reporting 7](#_Toc525807537)

[c. J Tagging 7](#_Toc525807538)

[i. Software 7](#_Toc525807539)

[ii. Preparation 7](#_Toc525807540)

[iii. Acquisition and Authentication 7](#_Toc525807541)

[iv. Data Analysis 7](#_Toc525807542)

[v. Reporting 8](#_Toc525807543)

# Introduction

With the advent of technology, the information that Mobile phones handles for users has grown multifolds; they are not used just for calling purposes but rather play the role of digital assistant by managing emails, maintaining daily schedules, navigating the routes, they have become indispensible source of valuable data.

This document specifies the procedure that should be followed in order to conduct a mobile forensic investigation wherein the investigator may encounter online or offline mobile phones

# Abbreviations used in Naming cases

* + - CP : Cellular Phone
    - SP : Satellite Phone
    - DK : Desktop
    - LP : Laptop
    - PD : Pen Drive
    - SC : SIM Card
    - MC : Memory Card
    - OE : Original Evidence
    - OC : Original Copy (First copy / Image of OE; intended to be retained untouched)
    - WC : Working Copy (Second copy / Image of OE; intended to be used for evidence processing)
    - PWD : Present Working Directory

# Naming Convention

Case Naming: The name of the cases should consist of 5 characters in the following format:

First 3 letters should refer to the project name, eg. STG for Project Sting, followed by 2 digits representing the Year, Example: STG18

Evidence Labeling: The evidence label should consist of 12 characters wherein the number for the Evidence artifact should be appended to the case name. Further, the 1-digit evidence artifact number will represent the following

1 : Cell Phone Memory

2 : First SIM Card

3 : Second SIM Card

4 : Third SIM Card

5 : Fourth SIM Card

6 : Memory Card

**<3 Chars for Project abbreviation> <2-Digits for Year of initiating the case investigation> ‘-‘ <2 Chars for Evidence type i.e Cell Phone (CP), SIM Card (SC), etc> <2 digits for Evidence Sequence number i.e 02 for Cell Phone no.2> <1 digit for evidence artifact # i.e 1 for Phone Memory, 2 for 1st SIM Card, 3 for 2nd SIM Card> ‘-‘ <’OC’ for Original Copy, ‘WC’ for Working Copy>**.

# Methods

# ADB Push

**Platform Supported :** Android

# Software

We shall use the following software on our Workstation for extracting the forensic evidence:

* ADB
* NetCat

We shall use the following software on the Evidence Device to gaining Root level access :

* Kingoroot.apk

We shall use the following software on the Evidence Device to Communicate with the Workstation :

* BusyBox 🡪 NetCat
* BusyBoc 🡪 DD

We shall use the following software on our Workstation for Analyzing the forensic evidence:

* X-Ways Forensics

# Preparation

# Procedure

# Acquisition and Authentication

* Physical Data acquisition
  + iOS
  + Android
  + Others
* Logical Data acquisition
  + iOS
  + Android
  + Others
* Cloud data acquisition
* SIM data acquisition
* Memory card data acquisition
* Acquisition of data from the synced computer systems

# Data Analysis

* Basic data
  + Contacts
  + Messages
  + Call Logs
  + Scheduled tasks
  + Bluetooth History
  + Wifi History
  + USB device History
* Internet data
* Emails
* Social Media
  + Whatsapp
  + Facebook
  + Twitter
  + Telegram
  + Instagram
  + Others
* Cloud data
  + iCloud
  + Google Drive
  + Others
* GPS data
* Deleted data

# Reporting

# ADB Physical Dumping

**Platform Supported :** Android

# Software

We shall use the following software on our Workstation for extracting the forensic evidence:

* ADB
* NetCat

We shall use the following software on the Evidence Device to gain Root level access :

* Kingoroot.apk

We shall use the following software on the Evidence Device to Transfer physical dump to the Workstation:

* BusyBox 🡪 NetCat

We shall use the following software on the Evidence Device for Generating a Physical dump:

* BusyBox 🡪 DD (on both Evidence Device and our Workstation)

We shall use the following software on our Workstation for analyzing the forensic evidence:

* X-Ways Forensics

OR

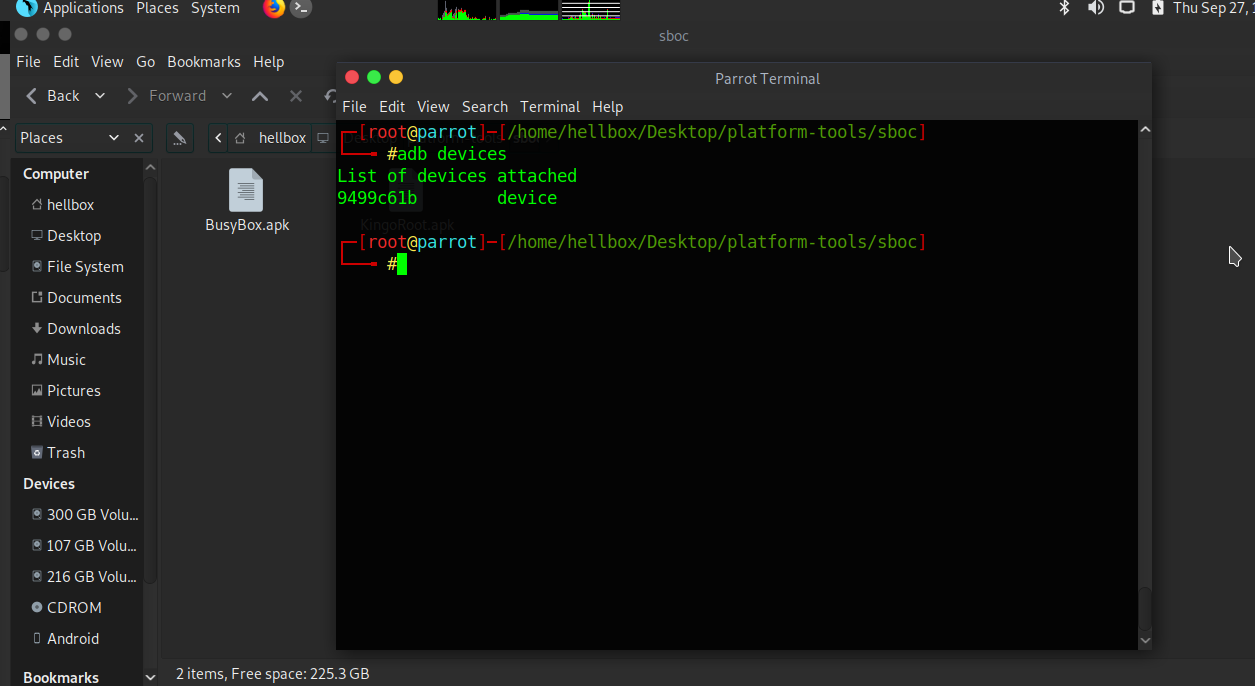
* Data Carving tool (Salvation Data SPF+, MPE)

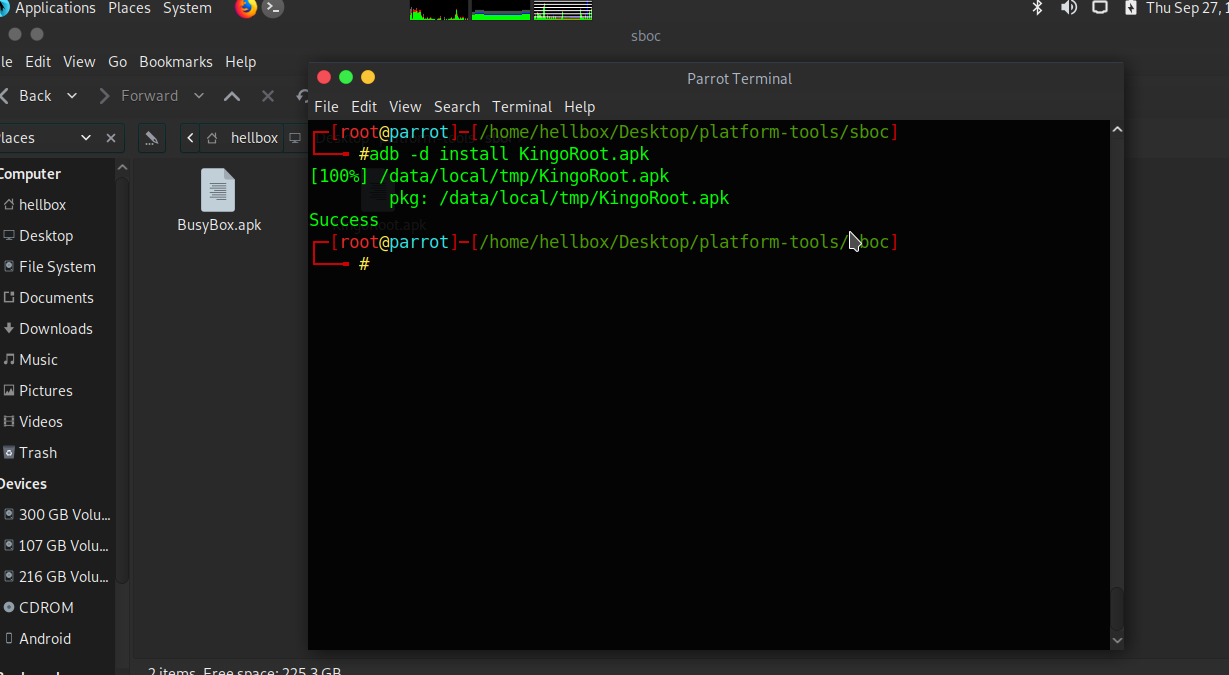
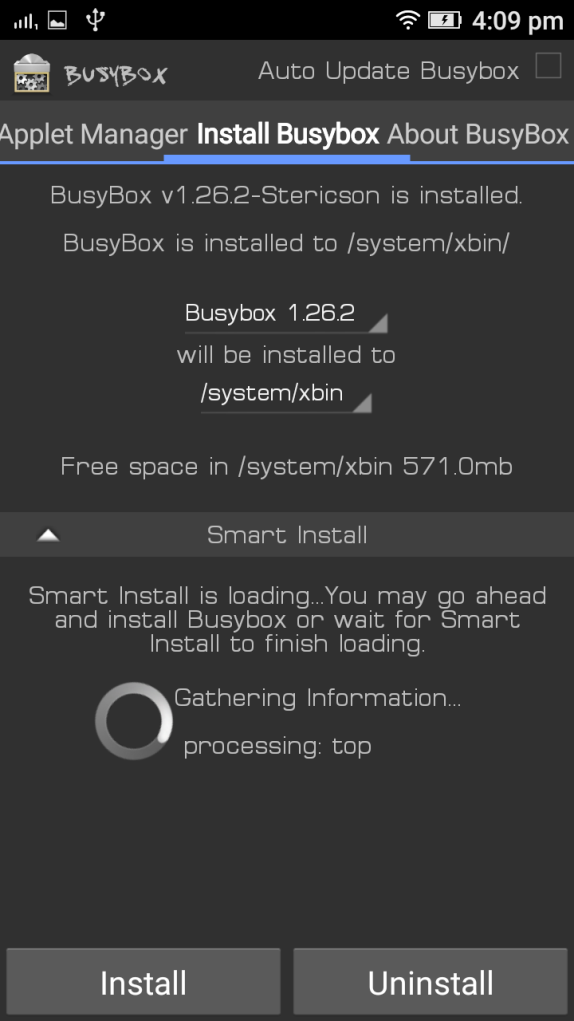
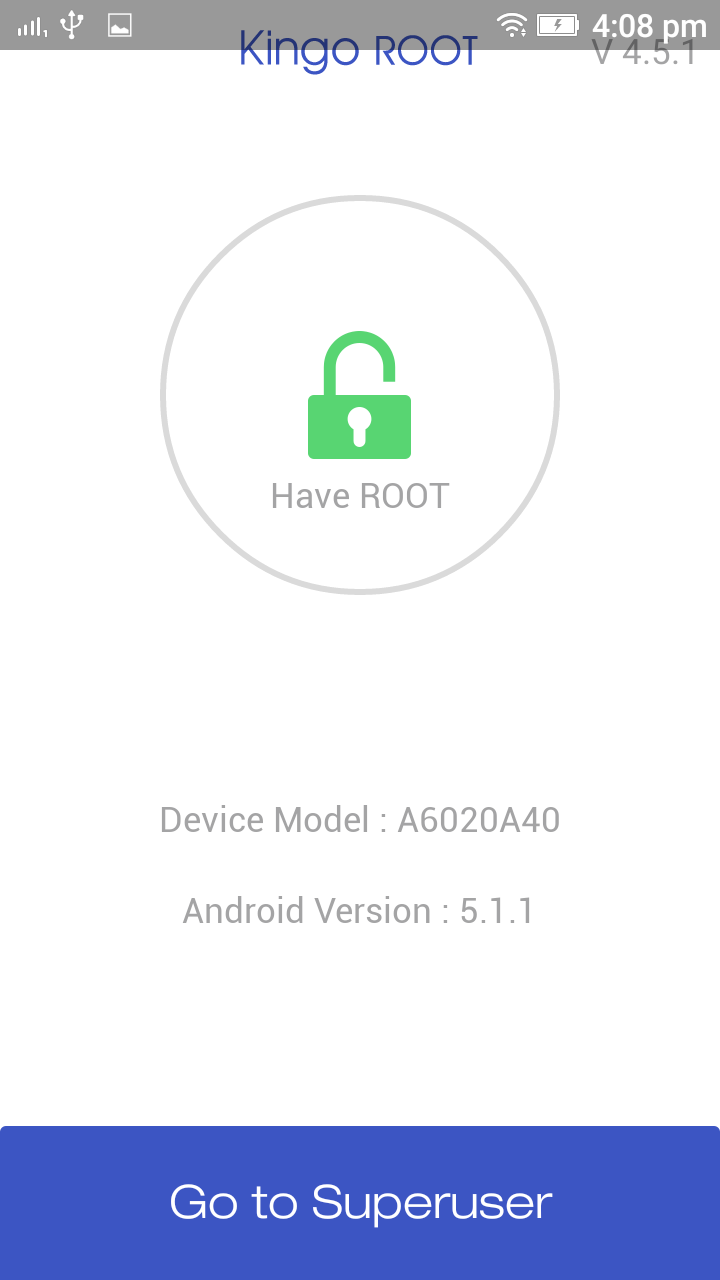
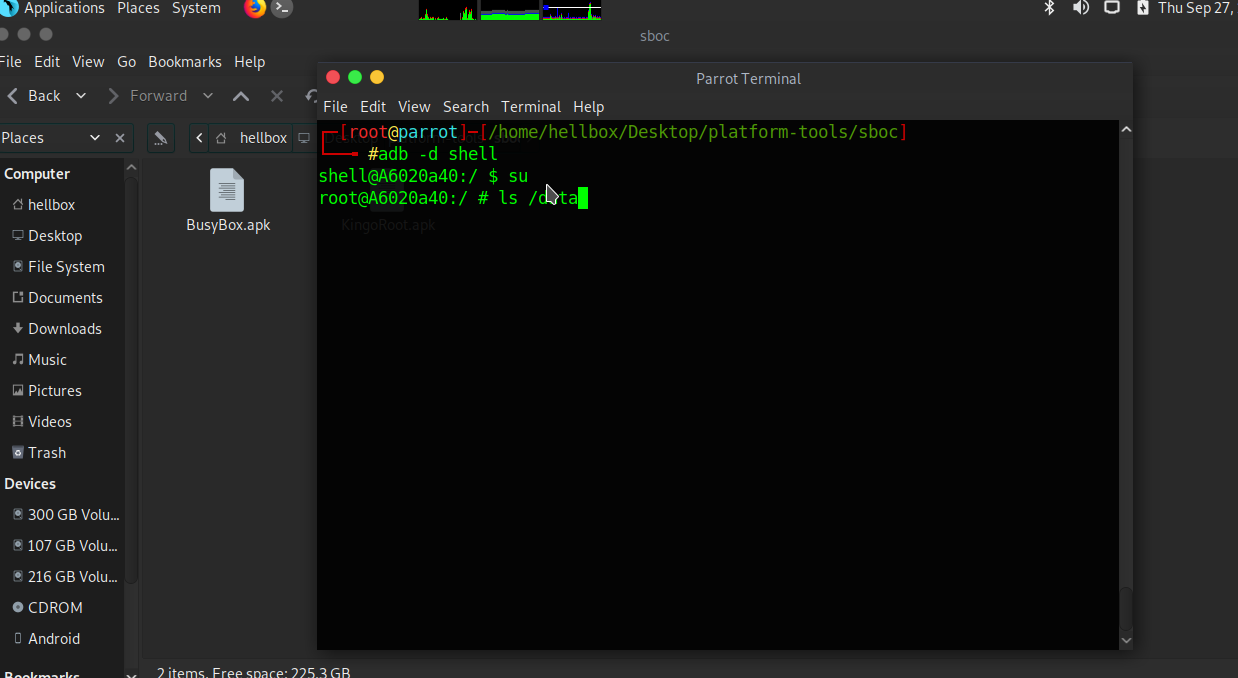
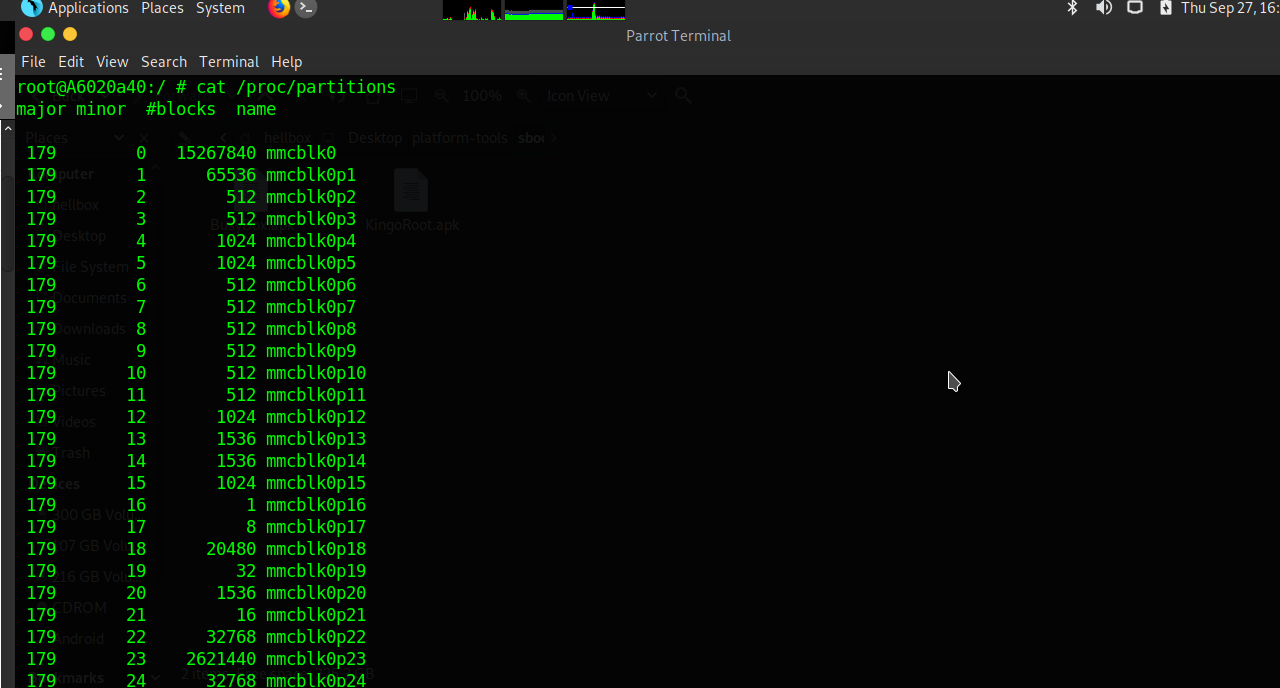
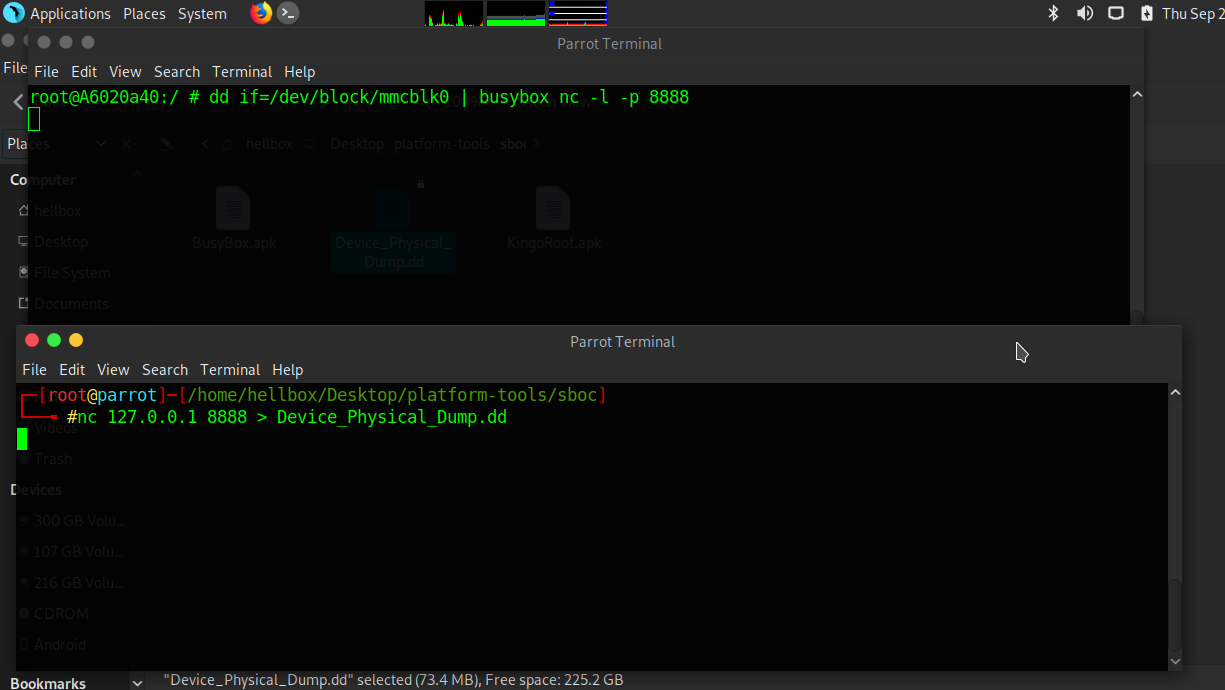
# Preparation

* Configure ADB on your Workstation
* Download kingoroot.APK and busybox.apk files and add them to the Case folder
* Start USB Debugging on the Evidence device
* Connect the Evidence device to the Workstation through USB Cable

# Procedure

* Assuming you are Running a Linux Based OS; open up a terminal and keep the PWD as the Case Directory where the APKs lie
* Confirming that ADB is correctly configured on your Workstation, type the command:

**adb devices**

* If the connected device is showing up on ADB as a device then we are good for the next step, else unlock the phone and redo the above step
* To install the APKs we type in the commands ‘**adb –d install KingoRoot.apk**’ and after its install type ‘**adb –d install BusyBox.apk**’
* Now open the evidence device, open KingoRoot app and press ‘**one click Root**’ button
* Once the root is complete open BusyBox app and install it
* Now come back to the Workstation and in the same terminal window type in ‘**adb –d shell**’ and hit Enter, if you got the phone shell then we can move ahead. If not, please refer to \_\_\_\_\_ to proceed
* Type in ‘**su**’ for switching to root user. Now you should get access to the root shell
* Now just to confirm the root privilege, type in ‘**ls /data**’ - if it displays the contents of the folder then we have the Root Privilege
* Now type ‘**cat /proc/partitions**’ to list down all the partitions. Pick the appropriate physical Partition, which in most cases will be ‘**mmcblk0**’
* Open another terminal window and type in ‘**adb forward tcp:8888 tcp:8888**’ which just forwards the tcp traffic on port 8888 on adb connection to the base network on tcp port 8888
* In the old/previous terminal with the Evidence device shell, type in ‘**dd if=/dev/block/mmcblk0 | busybox nc –l –p 8888**’ this command simply uses dd commandline tool to create a Physical Partition image of the Evidence device and then pipe the output to NC(NetCat) which in turn starts to transfer data to anybody listening to port no 8888 on the local setup
* Now come back on the newly opened terminal window and type in ‘**nc 127.0.0.1 8888 > Evicence\_Device\_PhysicalDump.dd**’. This starts netcat to allow the workstation to listen on the port 8888 of loopback address. It simply generates a .dd copy of the physical partition on the Evidence device

# Acquisition and Authentication

* Physical Data acquisition
  + Android
* Memory card data acquisition

# Data Analysis

* Basic data
  + Contacts
  + Messages
  + Call Logs
  + Scheduled tasks
  + Bluetooth History
  + Wifi History
  + USB device History
* Internet data
* Emails
* Social Media
  + Whatsapp
  + Facebook
  + Twitter
  + Telegram
  + Instagram
  + Others
* GPS data
* Deleted data

# Reporting

# Salvation Data SPF+

**Platform Supported :** Android, IOS

# Software

We shall use the following software on our Workstation for extracting the forensic evidence:

* ADB
* NetCat

We shall use the following software on the Evidence Device to gaining Root level access :

* Kingoroot.apk

We shall use the following software on the Evidence Device to Communicate with the Workstation :

* BusyBox 🡪 NetCat
* BusyBoc 🡪 DD

We shall use the following software on our Workstation for Analyzing the forensic evidence:

* X-Ways Forensics

# Preparation

# Procedure

# Acquisition and Authentication

* Physical Data acquisition
  + iOS
  + Android
  + Others
* Logical Data acquisition
  + iOS
  + Android
  + Others
* Cloud data acquisition
* SIM data acquisition
* Memory card data acquisition
* Acquisition of data from the synced computer systems

# Data Analysis

* Basic data
  + Contacts
  + Messages
  + Call Logs
  + Scheduled tasks
  + Bluetooth History
  + Wifi History
  + USB device History
* Internet data
* Emails
* Social Media
  + Whatsapp
  + Facebook
  + Twitter
  + Telegram
  + Instagram
  + Others
* Cloud data
  + iCloud
  + Google Drive
  + Others
* GPS data
* Deleted data

# Reporting

# J Tagging

**Platform Supported :** Android, IOS, BlackBerry , Bar Phones, Windows Phones, ETC

# Software

We shall use the following software on our Workstation for extracting the forensic evidence:

* ADB
* NetCat

We shall use the following software on the Evidence Device to gaining Root level access :

* Kingoroot.apk

We shall use the following software on the Evidence Device to Communicate with the Workstation :

* BusyBox 🡪 NetCat
* BusyBoc 🡪 DD

We shall use the following software on our Workstation for Analyzing the forensic evidence:

* X-Ways Forensics

# Preparation

# Procedure

# Acquisition and Authentication

* Physical Data acquisition
  + iOS
  + Android
  + Others
* Logical Data acquisition
  + iOS
  + Android
  + Others
* Cloud data acquisition
* SIM data acquisition
* Memory card data acquisition
* Acquisition of data from the synced computer systems

# Data Analysis

* Basic data
  + Contacts
  + Messages
  + Call Logs
  + Scheduled tasks
  + Bluetooth History
  + Wifi History
  + USB device History
* Internet data
* Emails
* Social Media
  + Whatsapp
  + Facebook
  + Twitter
  + Telegram
  + Instagram
  + Others
* Cloud data
  + iCloud
  + Google Drive
  + Others
* GPS data
* Deleted data

# Reporting