Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
(Cyber Security and Digital Forensics)
Institute of Forensic Science
Gujarat Forensic Sciences University

digvijay.rathod@gfsu.edu.in

Android Debug Bridge

Android Debug Bridge

✓Android Debug Bridge (adb) is a versatile **command-line tool** that lets you communicate with a device.

✓The adb command facilitates a variety of device actions, such as **installing and debugging apps**, and it **provides access to a Unix shell** that you can use to run a variety of commands on a device.

- ✓**A client,** which sends commands.
  - ✓The client runs on your development machine.
  - ✓You can invoke a client from a command-line terminal by issuing an adb command.
- ✓**A daemon (adbd),**
  - ✓which runs commands on a device. The daemon runs as a background process on each device.

Android Debug Bridge Commands

- ✓ adb connect device_ip_address
- ✓ adb devices
  - ✓ offline : The instance is not connected to adb or is not responding.
  - ✓ device : The instance is connected to the adb server.
  - ✓ no device : There is no device connected.
- ✓ adb kill-server - reset your adb host
- ✓ adb start-server

Android Debug Bridge Commands

- ✓ adb connect device_ip_address
- ✓ adb devices
  - ✓ adb devices

    List of devices attached

    4df16ac5115e4e04 device [serial no of the device]

    7f1c864544456o6e device [serial no of the device]
- ✓ adb shell -s4df16ac5115e4e04 [serial no of the device]
- ✓ if you wants to back to santoku shell form the android the press ctrl + D or exit

Android Debug Bridge Commands

- ✓ adb push <local> <remote> - pushes the file <local> to <remote>
- ✓ Example
- ✓ adb.exe push Pictures/index.png /sdcard/Pictures

- ✓ adb pull <remote> [<local>] - pulls the file <remote> to <local>. If <local> isn't specified, it will pull to the current folder.
- ✓ Example
- ✓ adb.exe pull /sdcard/Pictures/index.png

Android Debug Bridge Commands

- ✓ In Android, the logcat command provides a way to view the system debug output. Logs from various applications and portions of the system are collected in a series of circular buffers which then can be viewed and filtered by this command:
- ✓ adb logcat - allows you to view the device log in real-time.
- ✓ You can use adb logcat -b radio to view radio logs, and adb logcat -C to view logs in colour

Android Debug Bridge Commands

- ✓ Example
- ✓ adb.exe shell logcat – b radio –v time
- ✓ https://developer.android.com/studio/command-line/logcat.html

Android Debug Bridge Commands

- ✓ adb install <file> - installs the given .apk file to your device
- ✓ https://payatu.com/wp-content/uploads/2016/01/diva-beta.tar.gz
- ✓ Example
- ✓ adb.exe install C:\gfsu\diva.apk

Android Debug Bridge Commands

- adb shell - launches a shell on the device
- shell@android:/ $ ls
  - ls
  - acct
  - cache
  - config
  - ddata
  - default.prop , dev, efs, etc, factory etc...

ADB Basic Linux Commands

- ✓ shell@android:/ $
- ✓ a.ls
- ✓ b.cat
- ✓ c.cd
- ✓ d.cp
- ✓ e.chmod
- ✓ f.dd
- ✓ g.rm
- ✓ h.mkdir
- ✓ i.df
- ✓ j.ps
- ✓ k.mount
- ✓ l. exit / $a or $ Q or <Ctrl> D

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
(Cyber Security and Digital Forensics)
Institute of Forensic Science
Gujarat Forensic Sciences University

digvijay.rathod@gfsu.edu.in

Santoku

Santoku

- ✓Santoku Linux flavor and its free and open source
- ✓Name was suggested by Thomas Cannon of viaForensics (who happens to be the project leader of Santoku Linux)
- ✓Santoku Linux is aimed at
  - ✓Mobile Forensics,
  - ✓Mobile Malware Analysis, and
  - ✓Mobile Security Testing;

- ✓GNU/Linux distro designed to help you in every aspect of your
  - ✓mobile forensics,
  - ✓mobile malware analysis,
  - ✓reverse engineering and
  - ✓security testing

- ✓Tools available in the Santoku are:
  - ✓Development Tools:
  - ✓Penetration Testing:
  - ✓Reverse Engineering:
  - ✓Wireless Analyzers:
  - ✓Device Forensics:
  - ✓Mobile Infrastructure:

✓If you are into mobile security and mobile forensics then this distribution is definitely right for you.

✓Mobile Forensics:

1. Firmware flashing tools for multiple manufacturers
2. Imaging tools for NAND, media cards, and RAM
3. Free versions of some commercial forensics tools
4. Useful scripts and utilities specifically designed for mobile forensics

✓Mobile Malware Analysis:

1. Mobile device emulators
2. Utilities to simulate network services for dynamic analysis
3. Decompilation and disassembly tools
4. Access to malware databases

✓Mobile Security Testing

1. Decompilation and disassembly tools
2. Scripts to detect common issues in mobile applications
3. Scripts to automate decrypting binaries, deploying apps, enumerating app details, and more

- ✓ Configuration Steps of Santoku
- ✓https://santoku-linux.com/

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
(Cyber Security and Digital Forensics)
Institute of Forensic Science
Gujarat Forensic Sciences University

digvijay.rathod@gfsu.edu.in

Appie

✓Appie – Android Pentesting Portable Integrated Environment

✓Appie is a software package that has been pre-configured to function as an Android Pentesting Environment on any windows based machine without the need of a Virtual Machine (VM) or dualboot.

✓https://manifestsecurity.com/appie/

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
(Cyber Security and Digital Forensics)
Institute of Forensic Science
Gujarat Forensic Sciences University

digvijay.rathod@gfsu.edu.in