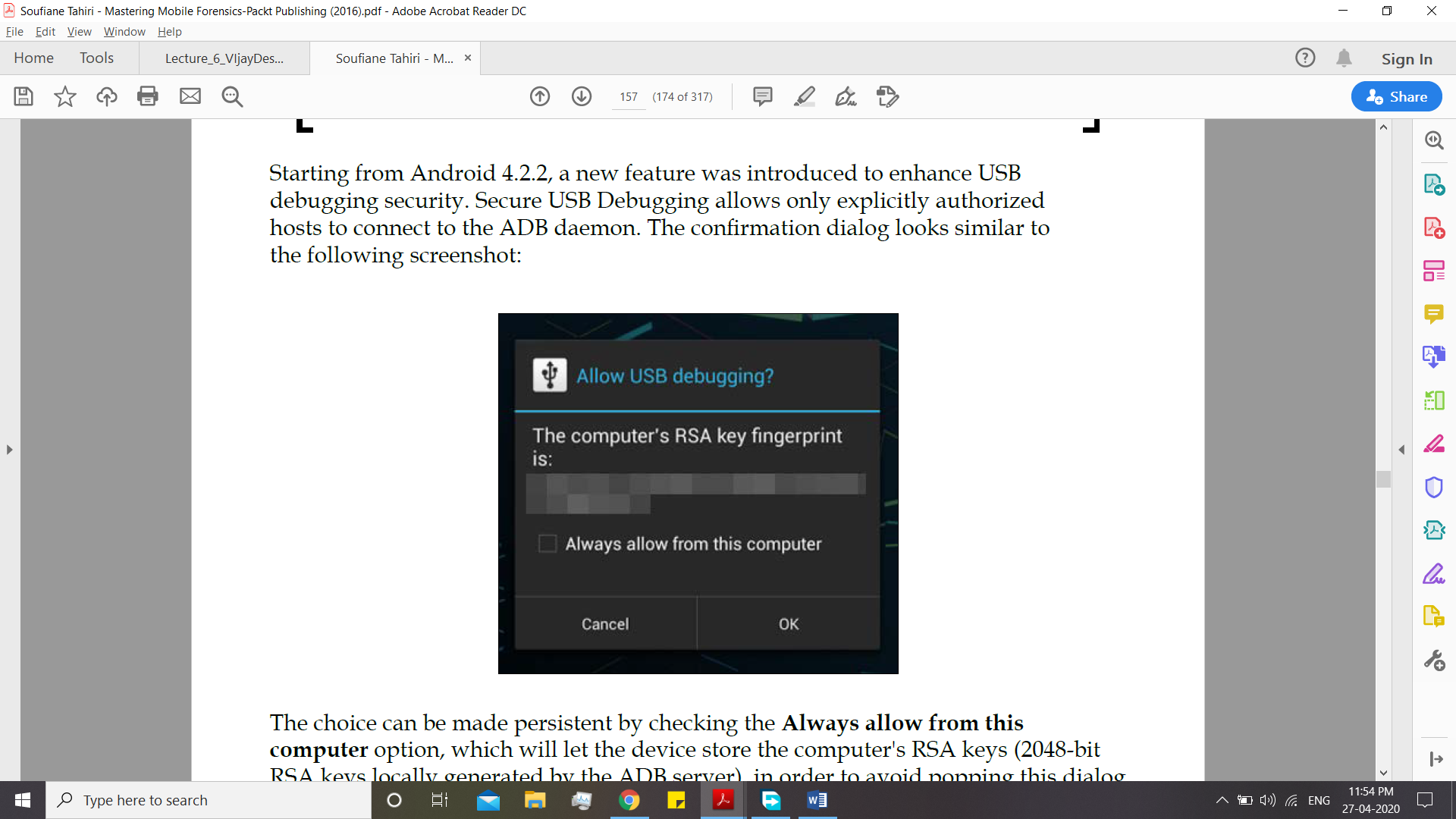
Performing Logical Data Acquisition

Step 1: Install the forensic tool ADB:

<http://www.howtogeek.com/125769/how-to-install-and-use-abd-the-android-debug-bridgeutility/>

Step 2: Enable the USB Debugging on Mobile.



Step 3: Check the following location for adbkey and adbkey.pub

**Windows**: %USERPOFILE%\.android or C:\Windows\System32\config\systemprofile\.android\

If the location contains these two files that means the mobile device has trusted the desktop in past.

**Step 4:** Navigate to the installed ADB folder after you have installed in cmd and run

**$ adb devices**

**List of devices attached**

**\* daemon not running. starting it now on port 5037 \***

**\* daemon started successfully \***

**90000a7854ca device**

**Step 5:** Run the Shell

**$ adb shell**

**root@generic:/ #**

The sharp # symbol means that you have root access on the device.

Step 6: Run the queries for data now and copy them using the command.

Some Example Command:

**# ls -l data/data/**

**adb pull [-p] [-a] < remote file path on device. > [<local file path>]**

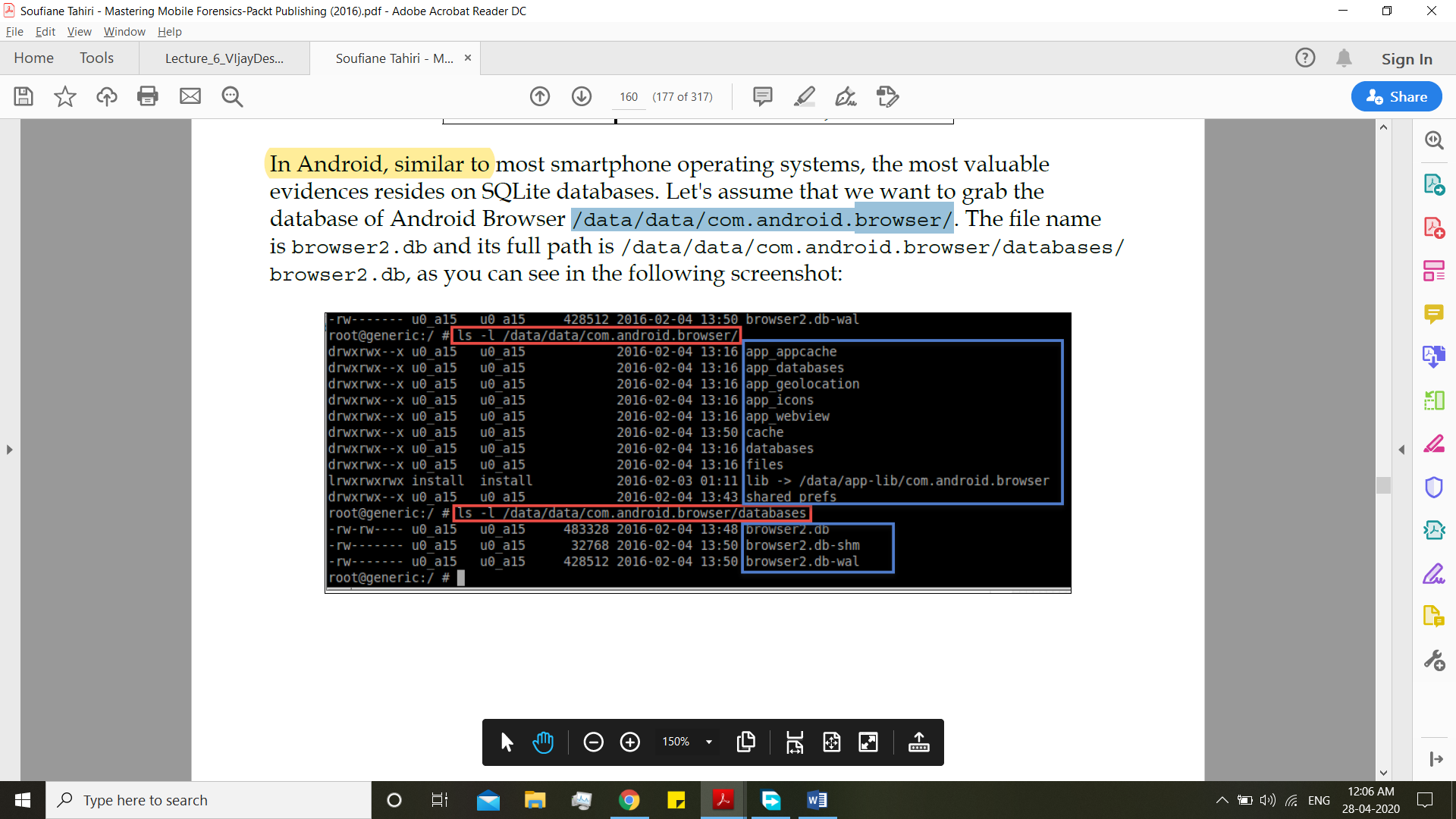
Here, –p and –a are optional parameters to respectively show the transfer's progress and to copy a pulled file's timestamp and mode.

Example:

Lets Assume we what to see Browser’s data:

We run:

**# ls –l /data/data/com.android.browser/**



Now pull all the db

**$ adb pull /data/data/com.android.browser/databases/browser2.db /home/soufiane/Desktop/AndroidBrowserDBs/browser2.db**

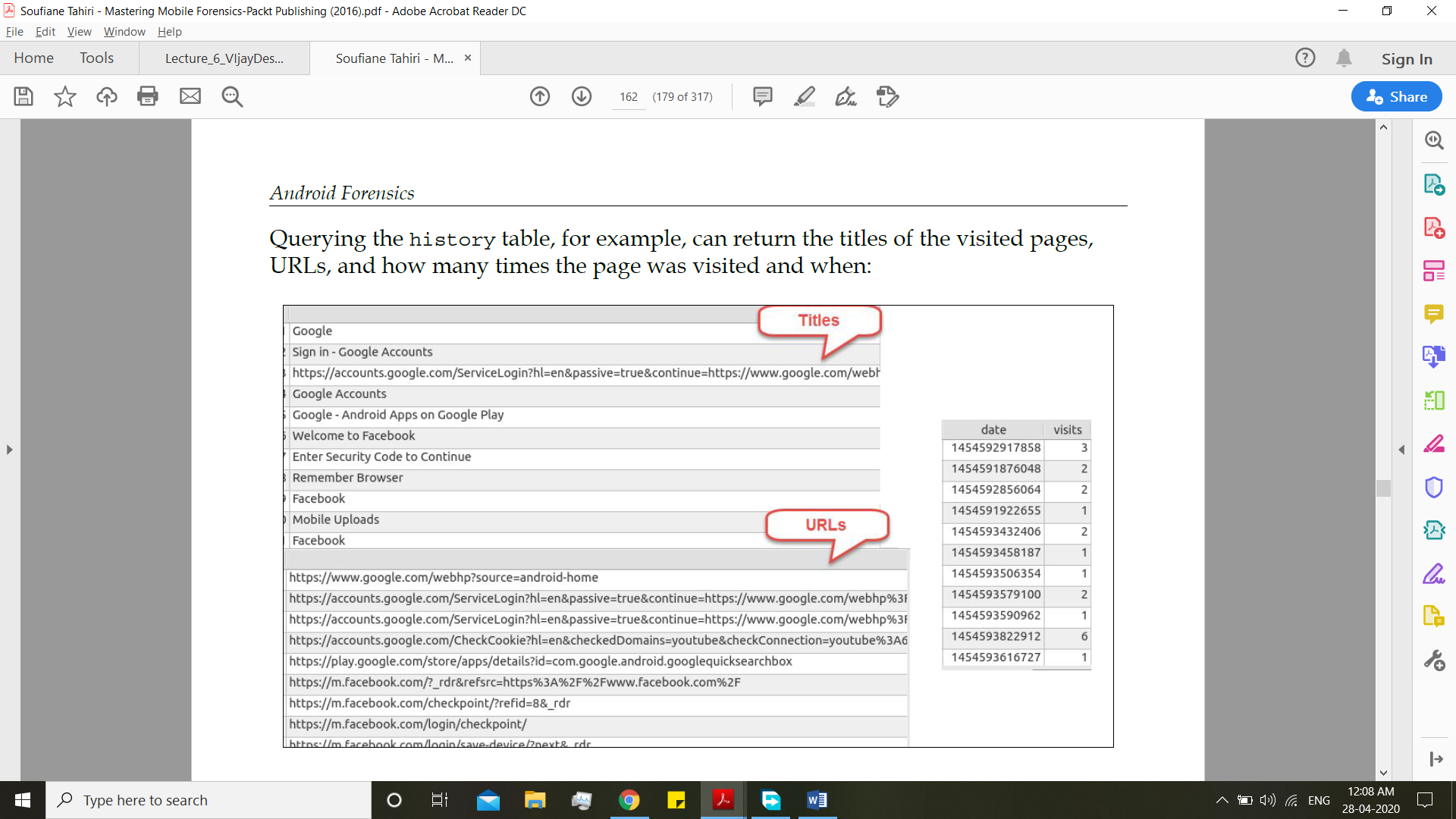
**1466 KB/s (483328 bytes in 0.321s)**

**$ adb pull /data/data/com.android.browser/databases/browser2.db-shm /home/soufiane/Desktop/AndroidBrowserDBs/browser2.db-shm**

**395 KB/s (32768 bytes in 0.080s)**

**$ adb pull /data/data/com.android.browser/databases/browser2.db-wal /home/soufiane/Desktop/AndroidBrowserDBs/browser2.db-wal**

**1242 KB/s (428512 bytes in 0.336s)**



ADB offers the possibility to extract a full backup of the device using the following command:

**adb backup [-f <file>] [-apk|-noapk] [-shared|-noshared] [-all]**

**[-system|nosystem] [<packages>]**

****

**Convert .ab file to .tar and extract it.**