



Identification and Detection of Fake iPhone on Basis of Systematic Analysis by Cyber Forensic Techniques: Case Study

Swanand Gulabrao Gorde*, Vitthal G. Mulik, C. S. Kamat, B. B. Daundkar

Directorate of Forensic Science Laboratories, Govt. of Maharashtra,
Mumbai, Maharashtra, India

Abstract: Now days mobile has become essential part of life of common man. People buy mobiles on basis of Popularity of manufacturer . Every mobile company wants their sales have to be boosted, so some companies manufacture duplicate or clone mobile which exactly look like popular mobile and take advantage of popularity. They sell these mobiles to public on same price as popular mobile and people who buy them come to know after use, they have purchased a duplicate product. They got involved in fraud. We solved case of these fake mobile such as iphone with the help of forensic techniques ,Identification of such fake iPhone explained in this research paper.

Keywords: *iphone, fake mobile, cyber forensics, mobile forensics, Forensic Extractions of devices, computer forensics*

I. INTRODUCTION

Nowadays iPhone becoming more and more popular gadget in India. It has become a status symbol in Indian society. The Popularity of iPhone has reached at its peak in India. It has become a dream phone for youngsters in India.

[1] The iPhone runs on Apple's own mobile operating system iOS, the second most popular smartphone operating system in the market. As of the third quarter of 2015, the iPhone made Apple the second-largest mobile phone vendor in the world, with a global market share of 9.6 percent.

The iPhone has changed Apple's business dramatically. iPhone sales have risen strongly over the years, from around 1.4 million iPhones sold in 2007 to almost 170 million units worldwide in 2014. In total, Apple has sold more than 590 million iPhones from 2007 to 2014 worldwide. In the third quarter of 2015, iPhone sales accounted for more than 60 percent of Apple's total revenue, generating more than 31 billion U.S. dollars in revenues.

With growing popularity of iPhone, some people want to hijack the market of iPhone with the help of fake iPhone or clone iPhone. These iPhones are introduced to unknown users who don't even know that they are buying fake iPhone in price of real iPhone. After some days, they realize that they have a clone version of iPhone which looks like iPhone but not an actual iPhone. This type of new crime of phone cloning has risen with every popular mobile brand in the world. So it's now becoming necessary to educate users on how to buy genuine products. This research is based on how to identify fake iPhone by forensic methods. Some methods are weak in identifications and detection of fake mobile. In this paper some steps are introduced which can forensically prove that the mobile is genuine or not.

II. SOME METHODS TO IDENTIFY FAKE iPhone

1. Check screws.

The pentalobe screws were used in iPhone whereas normal cross screws are used in fake phones. Whereas Apple always uses pentalobe screws.



Fig. 1 Example of original screws

2. The location of the buttons needs to be checked.

In the real iPhone, the sleep/wake button is on the top right corner, while the volume switch and ringer switch are on the upper left side. If the switch or buttons are not situated at right position, then one should understand that the iPhone is fake.

3. The screen should be checked.

The screen of original iPhone should be clear and not pixelated.

4. Identify original Apple logo.

On the back cover of phone, one must see an iPhone logo. If one can't find the logo, then it's a fake iPhone.



Fig. 2 Example of Apple logo

5. You must check the serial number.

Go to "Settings," choose "General," and then click on "About." This will give the serial number of the device. one can then access the Apple website [3] and enter the iPhone serial number to see if it is a real iPhone. Once there, just enter the serial number. If it is undetected, then the phone is a cloned one.

6. iPhone has fixed memory capacity.

The original iPhone should have fixed capacity storage, like 16GB, 32GB and 64GB. The fake one requires a memory card to expand its memory capacity, which can only expand up to 8gb at most. If a memory card slot is found at the back or the side of the phone, then it's a fake one.

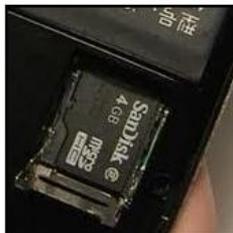


Fig. 3 Example of memory card slot

7. The welcome screen should show logo of apple.

This is also a must, especially when one can't distinguish between the fake iPhone and the original one by looking at its physical features. Try to turn off then turn on the iPhone. A fake iPhone will have a welcome screen, like the word "Welcome," while the original one will show the logo of the iPhone. On the home screen one can find an iPhone store icon. Try to click on it. If it redirects to the Googleplay store, then it's certainly a fake iPhone.

8. Siri can run on iPhone only.

The Siri application can only be launched from an original iPhone, and the fake one definitely can't run it.

9. The operating system is iOS.

If there is any application other than iOS, it is 100 percent fake. Apple uses only iOS as its official operating system.

10. Run iTunes application.

Connect the phone to a computer and try to run iTunes. If one receives an error, then it means iTunes has not recognized iPhone; thus there is a possibility that it is a fake iPhone.

11. The font setting.

Another thing that makes a fake iPhone really funny is when one tries to check the font of messages, it gives you a Chinese character, so one has to configure the phone to enable English settings.

12. Only one SIM card can be used in iPhone.

When you check how many SIM cards can run in an iPhone, a dealer of the fake one may proudly tell you that two SIM cards can be run at the same time. Then one will know that it is a fake dual SIM iPhone. The iPhone uses one SIM card. The original iPhone bears a label that says "designed by Apple California and assembled in China". Without this kind of mark, the phone is not original.

13. The built-in applications should be checked.

The original iPhone should have built-in Apple applications, such as Compact, Compass, Settings, Calculator, Music and Photos. If one of those are missing, the phone might be jailbroken. To be sure it is an original phone, try to restore the original firmware. If some built-in applications are still missing after restoring the original firmware, then it is a clone iPhone.

14. Check for the warranty.

Sellers of fake iPhones will not give a warranty of a certified iPhone service center.

15. Ask the price.

If it is being sold far cheaper than a regular iPhone's suggested price, then think twice before buying the product. [2]

III. VISUAL ANALYSIS OF FAKE iPhone

In cyber forensics, some time you have to prove according to a questionnaire that whether or not a given phone is fake. One such type of fake iPhone case was received in a forensic science laboratory where the opinion of a cyber forensic expert was asked regarding the genuineness of the iPhone. Using all the above techniques {II}.

- (a) checked the location of buttons but it is in the right place.
- (b) checked logo but it looked like the original one.
- (c) checked screws but they are of the same size as the original one.
- (d) It also had a fixed memory capacity of 32 GB.
- (e) Checked the welcome screen and it showed the iPhone logo.
- (f) Checked built-in applications which are in iPhone but the softwares also worked correctly.
- (g) All iOS applications were installed in the mobile.
- (h) Fonts were also in English and not Chinese in phone settings.
- (i) The iPhone uses one SIM card and this had only one SIM card.
- (j) The original iPhone should bear a label that says it's "designed by Apple California and assembled in China." and the exhibit has the same one.



Fig. 4 Duplicate iPhone

- (k) It had all iPhone built-in applications.
- (l) checked serial number on body and entered serial number on Apple site and it said it is genuine.

When all external parameters were checked and found matching with genuine then it became more confusing and complicated. So some cyber forensic techniques were applied to exhibit to know whether it is genuine or not.

IV. IN-DEPTH ANALYSIS USING CYBER FORENSIC TECHNIQUES

It's not sufficient to check the serial number on the back cover of an iPhone; one should also check its IMEI number by dialing *#06#. In this exhibit, after dialing *#06#, it gave me an IMEI number which, when cross-checked on the Apple website, showed that it is not genuine. This method is not sufficient to prove in court that it is not genuine.



Fig. 5 Screen after dialing *#06#

Then in the second method, the iPhone was connected to a workstation where Oxygen Forensic Tool [4] was installed. After connecting the iPhone, it showed an Android logo and gave the model name as 'MD298ZP/A'. This showed that it does not contain Apple iOS, but a cyber forensic expert has to prove it through a report. Surprisingly, when the phone was acquired, it didn't show the IMEI which was found by dialing *#06#.

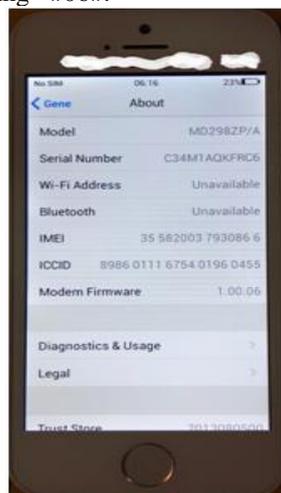


Fig. 6 Screen shows IMEI and model name and serial number

Then after going for third option of forensics tool i.e. UFED TOUCH [5] it also didn't show the IMEI which was needed for court evidence. The manufacturer's name was found to be 5S through UFED TOUCH extraction which is different from real iPhone. By all this it become pretty convincing that it was not genuine iPhone but IMEI number plays most important part in mobile forensics and still couldn't come to any conclusion through two tools.

Hence third tool was used which is XRY [6]. The phone was connected to the XRY and after extraction it gave the same IMEI number which was found after dialing *#06#. Now there were number of evidence to prove that it's not an iPhone.[7][8]

First one with oxygen forensics, it was found that it was an android. Second one with the UFED TOUCH where manufacturer's name was found to be 5S and model number was also found and in the last XRY gave IMEI number which doesn't match with back cover IMEI number and hence it is proved that it is not iPhone by forensic analysis.

V. CONCLUSION

The above methods shows that it has become a necessity to carry out various analysis methods during investigation of case. One has to try each and every tools, technical and non-technical methods to narrow down your investigation. Till you get desired result.

In our case, we had to go through all possible means and methods to prove that the device was indeed not a genuine Apple iPhone product.

REFERENCES

- [1] <http://www.statista.com/statistics/263401/global-apple-iphone-sales-since-3rd-quarter-2007/>
- [2] http://visihow.com/Determine_Fake_vs._Real_Iphone
- [3] <https://checkcoverage.apple.com/>
- [4] <http://oxygen-forensic.com>
- [5] <http://cellebrite.com/Mobile-Forensics/Products/ufed-touch>
- [6] <http://msab.com/products/xry>
- [7] <http://www.champlain.edu>
- [8] https://en.wikipedia.org/wiki/Mobile_device_forensics