Innovative Techniques of Digital Crime Investigation

Mr. Shrinivas D Desai1[1], Mr. Prashant Narayankar[2*].

[1, 2] Department of Information Science and Engineering, B.V.B College of Engineering and Technology, Vidyanagar, Hubbali, India.
[1]sd_desai@bvb.edu, [2]Prashant_narayankar@bvb.edu.

Abstract: Computer forensics is a new and fast growing form of investigative technique in which forensic specialist use modern forensic software tools, to solve digital crime cases. Choosing appropriate forensic tool for solving real-time digital crime cases is most expected graduate attribute, for those who have opted "Computer forensic" as an elective course. In this paper we present pedagogy for developing skill of choosing most appropriate software tool for analyzing and investigating digital crime cases. Assignment activities are designed to develop competencies such as i) Ability to identify, select and apply forensic tool to solve image, audio and video doctored cases. ii) Ability to evaluate the suitability and limitations of the tool used to solve problem.

To solve image forensic cases, a tool having feature of error level analysis and meta data analysis is found to be more appropriate, while for solving audio doctored cases, tool having feature of frequency response analysis as well as difference calculator is found to be most appropriate. In case of video doctored crimes, tools having feature of noise analysis, level sweep, clone detection, and magnification is found to be most appropriate. Assessment of outcome is carried out by recording attainment of Graduate Attribute (GA), Competency (CA) and Performance Indicators (PI). Skill of identifying, choosing and applying appropriate forensic tool to solve digital crime cases is observed among student.

Keywords: Cybercrime; Digital Evidence.

1. Introduction

Computer forensic is a process of obtaining and analysing digital information. Digital information is also digital evidence, which can be any information stored or transmitted in digital form. Computer forensics has many other disciplines like network forensics, data recovery and disaster recovery. Network forensics yields information about how intruder gained access to a network. Data recovery helps in recovering a data which is lost during power surge or server crash and disaster recovery uses computer forensic technique to recover the information which clients have lost. Many cases are physically categorized into civil, criminal and administrative cases. But in computer forensics cases are categorized into law enforcement agency and corporate investigation cases [1].

Corresponding Author
*Prashant Narayankar, Department, IS & E, BVBCET, Vidyanagar, Hubbali, India
Prashant_narayankar@bvb.edu

2. Challenges in Cybercrime Investigations

Cyber crime is using computers as a target or weapon in committing crime. The first ever cyber crime was in 1820[2]. Some of common cyber crime cases are financial fraud, disruption of networks , theft of information, misuse of computer resources , denial of service, employee abuse in work environment , planting malicious software for destructive activities , cyber vandalism , hacking into others account, cyber terrorism , child pornography , copyright violation and piracy[3].Several security measures are used for protection of information and resources like use of passwords, firewalls, antivirus, biometrics and many more. Inspite of such security measure, there are exist some criminals who are also hackers and computer experts, who become successful in using computers for crime. Every nation has a cyber laws which have to abide by citizens. When such cybercrimes take place, a complaint has to be lodged at cyber cell police in their jurisdiction. However, investigations of such cases are not easy. There are several challenges like data acquiring, nature of virtual environment and protection of digital evidence. The criminals often spoof their machine addresses to hide their identity, use fake or compromised accounts for crime. They also destroy the evidence. Therefore, we require efficient computer forensic and security techniques for detecting crimes.

3. Cybercrime Case Study Analysis

Case study analysis describes the seven different scenarios which we have considered for our experimentation.

A. Dana Loesch Fake Video Case

Ms. Dana Loesch, a famous personality has campaign for NRA (National Rifle Association of America) video_1. But she was surprised to see a doctored video which portray her aggressively in video_2. She claims the scene is baseless and doctored without her permission. She is requesting digital crime investigator to inspect the video and generate detailed investigation report regarding doctoring of video.

B. Madan Mohan Singh Fake Affidavit Case

Mr. Madan Mohan Singh claims that, he found an Affidavit (A 853761) which is faked one, and the signature is forged. He has given his sample signature (10 signs) and asks you to prove that the affidavit is fake and forged. Investigate the case using appropriate tool and generate detailed investigation report.

C. Fake Image Case

A set of images which are suspected to be doctored are considered and examined to prove the authenticity of the images using appropriate tool. Generate detailed investigation report for fake and genuine images.

D. Amithabh Bachchan Fake Audio Case.

Mr. Amithabh Bachchan (AB), a famous actor claims that his voice is used with fake background to create a video A, without his permission or notice. Voice from an original video is taken and dubbed and fit into some other video. As a digital crime investigator, we need to inspect the video and generate detailed investigation report regarding doctoring of video.

E. Fake call case

A person is receiving mobile call from following numbers. 09102953395 And 09250401085 identify the intention of the call. And investigate the case, generate forensic report accordingly.

F. Movie Copyright Violation Case.

A film director has complained that his film is dubbed in other language, without permission. And is a case of copyright violation. Inspect the video and generate detailed investigation report regarding doctoring of video.

G. Amithabh Bachchan Audio Forgery Case

Mr. Amithabh Bachchan (AB), a famous actor claims that his voice is mimicked by unknown person, without his permission or notice. As a digital crime investigator to inspect the audio for forgery case, and generate detailed investigation report regarding this crime.

4. Tool Description

Cyber forensic tools are openly available in the internet, but some tools are available only with enterprise edition with legal licensing. Following tools are open source tools which we have used for our investigation.

A. Audio Diffmaker (ADT)

It is a freeware tool which is used to determine the absolute difference between two audio recordings. The difference recording that result is only what has changed between the two recordings. If anything - a change of component, a treatment, mechanical damping, etc. - is having any audible effect on the audio signal in a system, the difference recording will have audible content. The end result is primarily intended to be evaluated by ear [2].

B. Guiffy (GIDT)

It is an advanced cross platform image file compare diff Tool. It compares bmp, gif, jpeg, jpg, png, and wbmp formats. To compare images it considers three filters B&W, Shades, and Heat and creates image metrics based on pixel difference, threshold and color difference percentage [3].

C. Praat Tool

It is open source program which is used to analyse the speech signals. It is also cross platform tool which can be used over different operating systems [4].

D. Phone forensic express or Mobiledit or True Caller

Using this tool forensic examiner will be able extract all data from mobile. Extracted data may involve photos, deleted data, call history, contacts, text messages etc. True caller online tool can also be used to solve fake call cases [5, 6].

E. Signature Verification tool

It is used to identify the fake signature made by the culprits. Signatures are unique, this tool help us to identify the fraud signatures or forgery [7].

F. WinMD5

It is widows based hash value generator tool. It uses Message Digest algorithm to generate digital has for file or any data. Comparison of hash value will show us whether the original data is tampered or not [8].

G. Bolide Tool

It is image comparer, which will compare RAW, JPEG, J2K, BMP, GIF, PNG, TIFF, TGA image formats with cross platforms [9].

H. Online forensic portals

Many online open sources are available on internet for forensic analysis. To solve above mentioned case scenarios we have use different portals which are namely, Imageforensic.com, Photoforensic.com, Imageedited.com, DiffNow.com, forensically beta tool and free izitru.

5. Methodology

A. Ms. Dana Loesch's Fake Video Case.

Above mentioned case has two separate video's namely video_1 and video_2, one is genuine and another one is fake. To identify the fake and genuine video's we have used GD tool.

Following are steps to investigate fake/genuine video.

Step 1: Extract frames from both videos at rate of 2 frames/second and store these frames with respect to time.

Step 2: Compare frame of video_1 with frame of video_2 taken in 'i' th second until all frames in original frames in original video get over using GIDT.

i=1,2,…..,n where 'n' is 15

This tool compares 2 frames and shows the difference between these frames if any. These differences can be viewed in Heat map, B & W and Shades.

Step 3: Comparing the frames of given two video at specific second.

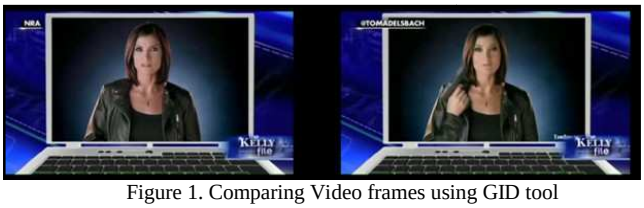


Figure 1. Comparing Video frames using GID tool

Figure 2. Difference in the video frame

Results shows that about 90% of the frames have very minute changes and remaining 10% of the frames have lot of difference as shown in above figure.

Observations:

By analysing the result which we got from GID tool, we can conclude that the video_2 is tampered; hence we can say that video_1 is genuine video.

B. Fake Affidavit/Signature case.

Mr. Madan Mohan Singh claims that, he found an Affidavit (A 853761) which is faked one, and the signature is forged. He has given his sample signature (10 signs) and asks you to prove that the affidavit is fake and forged. To solve this case we have used Guiffy image comparison tool.

Step 1: Crop the signature which is present on the affidavit (A853761)

Step 2: Compare cropped signature image with sample signatures given using Guiffy (GID) tool and conclude whether signature genuine or fake.

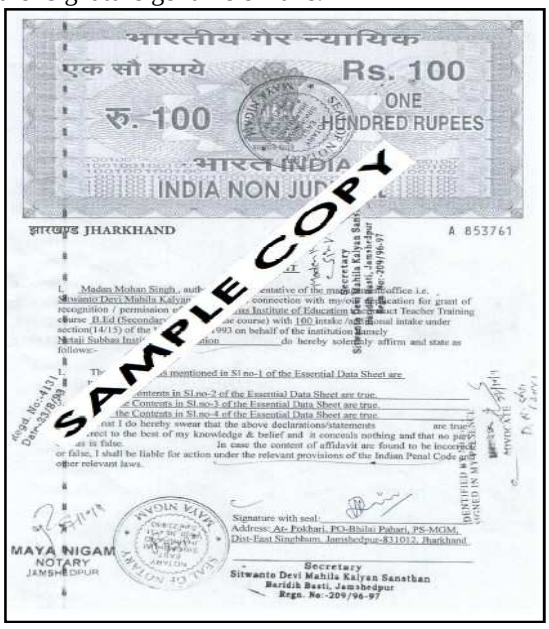


Figure 3. Sample Affidavit

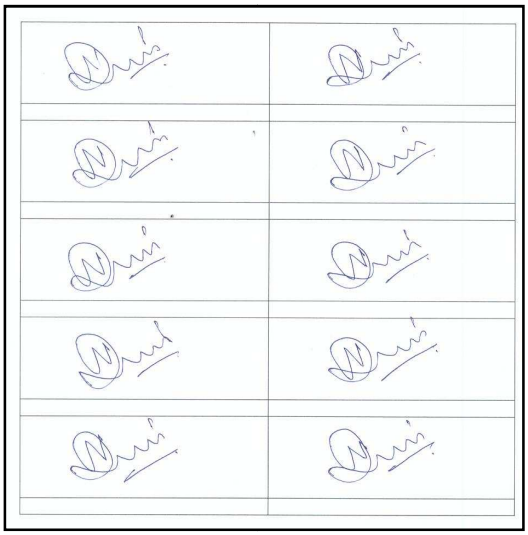


Figure 4. Sample Signature

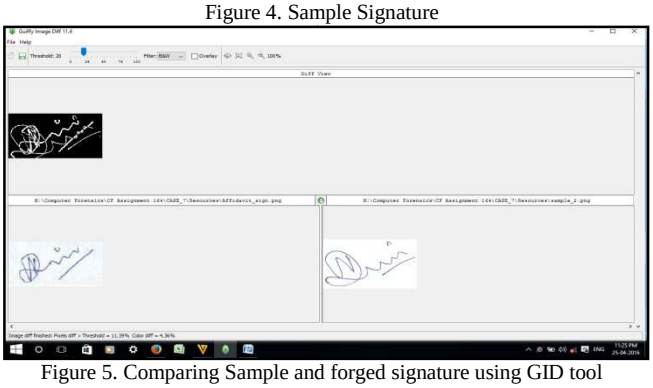


Figure 5. Comparing Sample and forged signature using GID tool

Observations:

By analysing the result which we got from GID tool, we can conclude that overlapped cropped images of signatures are mismatching, so above given affidavit is forged.

C. Genuine or Fake Image.

To identify fake/genuine image we have considered some set of images, those set of images consist both doctored and genuine images. Foto Forensics is an online tool which helps us to identify the fake/genuine image. This online tool marks the doctored content of the image with white highlighting. For example following image shows where it is doctored. Foto forensics also generates metadata of an image which will help in investigation process.

Figure 6. Sample Image

Figure 7. Doctored content in the image

D. Mr. Amithabh Bhachan(AB) Fake Voice case

Mr. AB, a famous actor claims that his voice is used with fake background to create a video A, without his permission or notice. He is requesting digital crime investigator to inspect the video and generate detailed investigation report regarding doctoring of video. In this case video B is original. For above mentioned scenario there are 2 videos, 1 is fake and 1 is genuine. Following are steps to investigate fake/genuine Audio.

Step 1: Given that video B is original. So use audio file of video B and compare it with audio file of video A. Extract audio "Fake.wav" from "video A" and audio "Actual.wav" from "video B" using media player.

Step 2: After extracting compare these two audio files by the tool Praat.

Step 3: Results obtained from the tool show that two audio files are same.

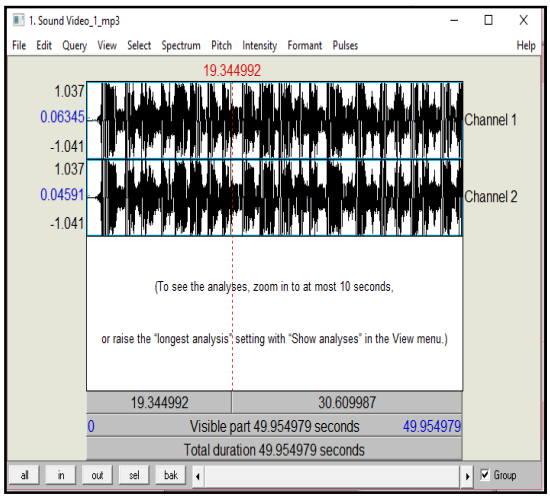


Figure 8. Audio for video1

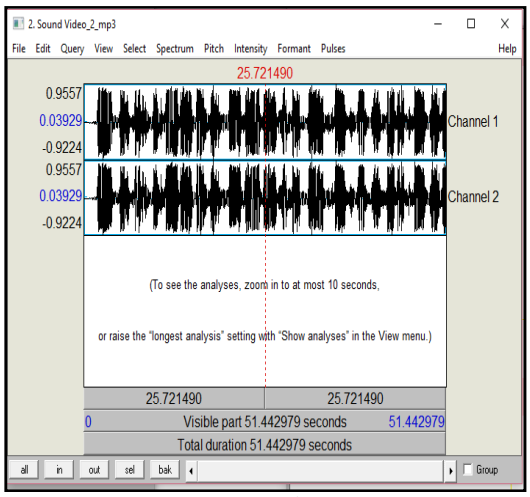


Figure 9. Audio for video2

Observations:

Based on the result obtained from the tool it is clear that both audio files are same. Since video2 is original and it has background of Mr. AB's voice then Video1 is also having his voice as background even though video is different. Hence, we can say that complaint given by Mr. AB is true.

E. Fake Calls.

A person is receiving mobile call from following numbers. 09102953395 And 09250401085 identify the intention of the call. An audio clip of fake call in which a women is asking for ATM card details of SBI customer and convincing him that new ATM card will be issued by replacing old card. Generally these kind of unknown calls asking for bank details and personal details are quite common now days. To solve this kind of cases we need law agency involvement, detailed information about the fake caller's location, IMSE and Sim card details. For above mentioned scenario we have taken a tool called True caller and Mobiledit.

Figure 10. 09250401085 details

Figure 11. 09102953395 details

Observations: By analysing the results we got from True caller app we can conclude that mobile numbers mentioned in our case are fake mobile numbers. And by analysing audio record we can say that the intentions of call are to collect the ATM card and PIN information.

F. Copyright Violation Case

A film director has complained that his film is dubbed in other language, without permission. And is a case of copyright violation. As we discuss about copyrights, all the rights about product, service and other issues are reserved by copyright holders. In our scenario we have considered a video clip of a movie, it's actually Hindi movie but it is dubbed in Tamil language without permission of the director. To solve this case we have used sample Hindi video and wavepad tool. Following are the steps we carried out to solve this case.

Step 1: Given movie clip is in Tamil, We also have considered sample video in Hindi version. Extract the audio from both videos.

Step 2: Compare the audio file of both videos i.e. Hindi.mp3 and Tamil.mp3 using wavepad tool.

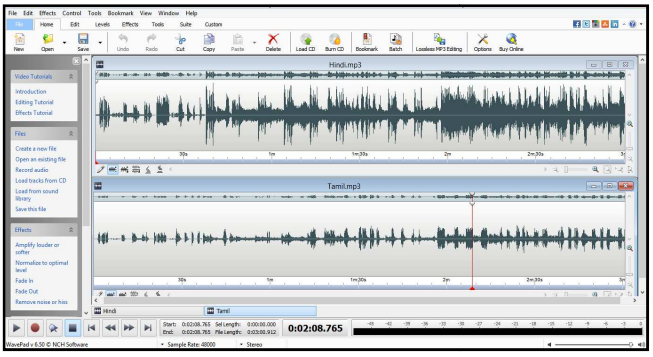


Figure 12. Comparison of Hindi and Tamil audio files

Observations:

By analysing the pulse rate of both Hindi audio and Tamil audio the pulse rate is different. Select 10 second & zoom in analyses Actual is varying more compared to Tamil audio.

Hence based on the result obtained by the tool it is clear that both audio files are different. By observing lip sync in both videos, we can Cleary say that Hindi audio matches perfectly with wave forms comparatively with Tamil audio. By this we can conclude that given movie clip is dubbed.

G. Amithabh Bhachan(AB) Voice Mimicked Case

Mr. AB, a famous actor claims that his voice is mimicked by unknown person, without his permission or notice. He is requesting digital crime investigator to inspect the audio for forgery case. In this case we have forged audio or mimicked audio which has to be compared with original AB voice, for original AB voice we are considering sample audio clip.

Step 1: Consider sample audio of Mr.AB and mimicked audio from this case.

Step 2: Compare both audio files using Audio_DiffMaker tool (ADT).

Observations:

AD tool compares two given audios and extracts waveforms of those audios. It also subtracts the waveforms of fake audio with genuine audio and generates difference between those audios. After comparing both waveforms if any difference occurs we can say that both audio are different, if not we can conclude that both audios are same.

In our experimentation we have conclude that both audios are different and given audio file is mimicked by an unknown person.

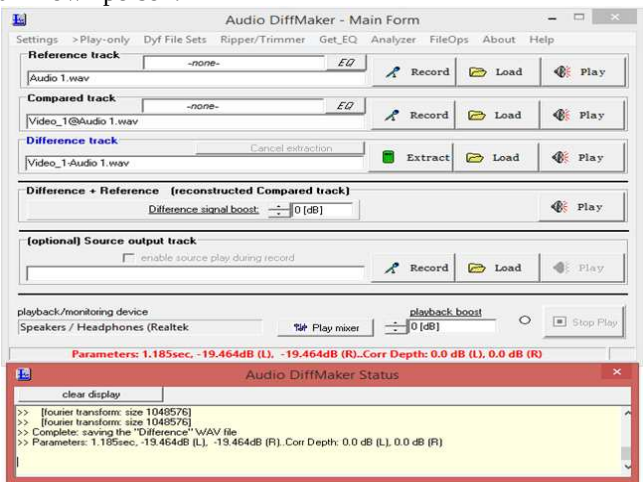


Figure 13. Comparison of Hindi and Tamil audio files

6. Achievements and Analysis

Computer forensic course is introduced in the curriculum for the first time, designing a course was bit challenging. Course design mainly has 4 course outcomes (CO) which are mentioned in below table.

Table 1. CO's with Addressing PO's

CO. No	Course Objective	Addressing PO's
CO.1	Explain set of procedure for processing and effective documentation of crime and incident scenes	PO1 - M, PO2 - H, PO10 – M.
CO.2	Identify appropriate software / hardware tools, techniques for digital crime investigation	PO1 - M, PO5 – H.
CO.3	Choose the appropriate data type and forensic procedure to carry out digital crime investigation	PO1 - M, PO4 – H.
CO.4	Explain procedure for investigating e-mail and cell phone crimes and violations	PO1 - M, PO2 - H, PO10 – M.

Computer forensic course mainly addresses 5 different Program Outcomes (PO's) namely PO 1, PO 2, PO 4, PO 5 and PO 10. In our paper we focus towards attainment of PO 5 which is use of modern tool usage. These POs are defined with NBA criteria. Assessment methods for Computer Forensics (CF) are based on SEE (Semester End Examination) and CIE (Continuous Internal Evaluation).

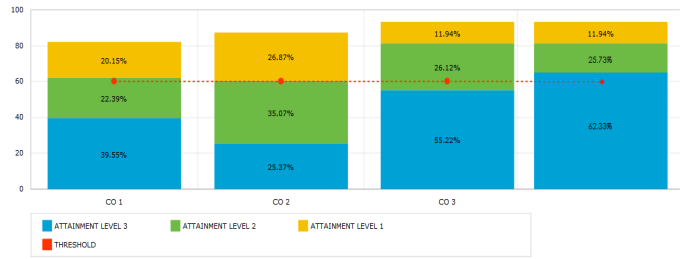
CIE assessment has activity where students are given with real world cybercrime scenario. These scenarios are mainly based on multimedia evidence such as image, audio, Video and it also evolves cases which have evidence like fake affidavit, fake calls etc. Above discussed cybercrime cases are given to the student's as CF course activity. Each students need to conduct a professional investigation with available forensic tools. After the conduction of investigation students come up with variety of results, these results are obtained by many available forensic tools which help us for better assessment towards PO 5.
Table 1 also defines degree of compliance with each PO's, M-medium, H-high and L-low. As with NBA criteria PO 2, PO4 and PO5 talks about identifying a problem, conducting investigation and modern tool usage respectively, the degree of compliance is also high for these PO's.

In order to assess the attainment of CO, a target of 60% of student will score more than 60% marks was set. The following table presents the attainment at various level. It is worth noting that CO 4, which focuses on "Modern tool usage" is having attainment of 3 (best).

CIE ATTAINMENT

CO	LEVEL 3	LEVEL 2	LEVEL 1	ATTAINMENT
CO 1	39.55%	61.94%	82.09%	**2**
CO 2	25.37%	60.44%	87.31%	**2**
CO 3	55.22%	81.34%	93.28%	**2**
CO 4	62.33%	88.06%	100%	**3**

The following figure presents the graphical representation of the same.



As a course, the attainment of various claimed POs are listed in below table. The score indicates better performance of students against all claimed PO

Final Attainment

Course Name	PO1			PO2			PO4			PO5			PO10		
	SEE	IA	Final	SEE	IA	Final	SEE	IA	Final	SEE	IA	Final	SEE	IA	Final
ISE437	**3**	**2**	**2.5**	**3**	**2**	**2.5**	**3**	**2**	**2.5**	**3**	**2**	**2.5**	**3**	**2**	**2.5**

7. Conclusion

Computer Forensic is enhancement of the computer security, whenever there is security breach, forensic investigator investigate the case using state of the art forensic tools and technique. In our paper we have solved seven cyber crime cases using different techniques. Each of the cyber case solving methodologies has its own advantage and disadvantages. In order to apply appropriate methods to solve a case, we should understand its nature, digital evidence, resources used to solve a crime, legal process of investigation and cyber laws defined in the governmental bodies. From our experiments it is obvious that we can techniques apt for given circumstances and evidences. We mainly dealt with identifying fake images, videos, audios and signature.

The demand for computer forensics is witnessed as the increasing numbers of digital crimes are registered now days. As cyber crimes are new to the society, we cannot find rules and regulations for all the crimes, so forensic investigator defines their own case law for those cases, for which there are no legal laws are defined in the governmental bodies. Cyber forensic tools such as ProDiscover and AccessData FTK can be used for even more detailed investigation of the cases.

References

1. Bill Nelson "Guide to Computer Forensics and Investigations", 4th Edition, CENGAGE Publication. 2009
2. Er Harpreet Singh Dalla ,Ms. Geeta , Cyber Crime – "A Threat to Persons, Property, Government", ,IJARCSSE , 2013
3. Cybercrime. Retrieved from https://en.wikipedia.org/wiki/(10 June 2016)
4. Guiffy Image Diff Tool. Retrieved from http://www.guiffy.com/Image-Diff-Tool.html (14 May 2016)
5. S. Rashidi , A. Fallah, , F. Towhidkhah, Scientia Iranica, "Feature extraction based DCT on dynamic signature verification" , Volume 19, Issue 6, Pages 1810 - 1819, December 2012
6. Praat Tool. Retrieved from http://www.fon.hum.uva.nl/praat/ (20 May 2016)
7. Truecaller App Retrieved from https://www.truecaller.com/ (25 May 2016)
8. Mobiledit is retrieved from http://www.mobiledit.com/ (26 May 2016)
9. Audio Diffmaker Working. Retrieved from http://www.libinst.com/Audio%20DiffMaker.htm (14 May 2016)