Image Tracker

Prepared By Khyati Thakkar 12MCEI30



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING INSTITUTE OF TECHNOLOGY NIRMA UNIVERSITY AHMEDABAD-382481

May 2014

Image Tracker

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering (Information and Network Security)

> Prepared By Khyati Thakkar 12MCEI30

Guided By Ms. Rupal Kapdi (Internal Guide) & Mr. Nilay Mistry (External Guide)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING INSTITUTE OF TECHNOLOGY NIRMA UNIVERSITY AHMEDABAD-382481

May 2014

Certificate

This is to certify that the major project report entitled "Image Tracker" submitted by Khyati Thakkar (12MCEI30), towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering (Information and Network Security) of Nirma University, Ahmedabad is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Ms. Rupal Kapdi Internal Guide & Asst. Professor, Dept. of Computer Science & Engg., Institute of Technology, Nirma University, Ahmedabad Mr. Nilay MistryExternal Guide & Asst. Professor,Dept. of Digital Forensics,Institute of Forensics Science,Gujarat Forensics Sciences University,Gandhinagar

Prof. Sharada Valiveti	Dr. Sanjay Garg
Assoc. Professor & M.Tech. INS Coordinator,	Professor & Head,
Dept. of Computer Science & Engg.,	Dept. of Computer Science & Engg.,
Institute of Technology,	Institute of Technology,
Nirma University, Ahmedabad	Nirma University, Ahmedabad

Dr. K. Kotecha, Director, Institute of Technology, Nirma University, Ahmedabad I, Khyati Thakkar (12MCEI30), give undertaking that the major project entitled "Image Tracker" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering (Information and Network Security) of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Khyati Thakkar (12MCEI30) Date: Place:

Endorsed by

Ms. Rupal Kapdi Mr. Nilay Mistry Internal Guide External Guide

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to Ms. Rupal Kapdi, Internal Guide & Assistant Professor, Dept. of Computer Science & Engg., Institute of Technology, Nirma University, Ahmedabad and Mr. Nilay Mistry, External Guide & Assistant Professor, Dept. of Digital Forensics, Institute of Forensics Science, Gujarat Forensics Sciences University, Gandhinagar and Mr. Abdul Zummerwala, Project Scientist, BISAG, Gandhinagar for their valuable guidance and continual encouragement throughout this work. The appreciation and continual support they have imparted has been a great motivation to me in reaching a higher goal. Their guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

My deepest thank you is extended to **Prof. Sharada Valiveti**, Coordinator M.Tech. - INS, Dept. of Computer Science & Engg., Institute of Technology, Nirma University, Ahmedabad for an exceptional support and continual encouragement throughout the Major Project.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Dept. of Computer Science & Engg., Institute of Technology, Nirma University, Ahmedabad, **Dr. K. Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad and **Dr. M S Dahiya**, Hon'ble Director, Institute of Forensics Science, Gujarat Forensics Sciences University, Gandhinagar for their kind support and providing basic infrastructure and healthy research environment.

I would also thank Ms. Twinkle Patel (12MCEI38), Mr. Madhur Tewani (12MCEI29), my other colleague friends, the institution and all faculty members of Dept. of Computer Science & Engg., Institute of Technology, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

> - Khyati Thakkar 12MCEI30

Abstract

The Internet is a global network connecting millions of computers. So anyone from any corner of this world can upload or download anything to and from the Internet. Moreover, social networking is being widely used by people to share each and every update of their life. So in this era of communication, lots of cyber crimes are taking place and they are increasing day-by-day and one of them is, social media crime. Image Tracker will help reducing such kind of crimes as it is the functionality which embeds the source computer's unique identifier i.e. MAC address into the image by modifying exif data. So, if any such crime takes place by editing and uploading someone's image then the computer, on which the image has been lastly modified and has been uploded, can be traced down by fetching unique identifier of that computer from the image.

Key words: Image Tracker, Morphing Detection, MAC address within Image, Track Source of Image

Contents

C	ertificate	iii
U	ndertaking	iv
A	cknowledgements	v
A	bstract	vi
Li	st of Figures	x
1	Introduction	1
	1.1 Problem Definition	. 2
	1.2 Chapter Organization	. 2
2	Motivation	3
	2.1 Domain Study	. 3
3	Literature Survey	5
	3.1 GIMP Architecture	. 6
	3.2 GIMP Plug-in Development	. 7
	3.3 Exif Tags	. 7
4	Study of Available Techniques	9
	4.1 TinEye	. 9
	4.2 PicScout	. 10
	4.3 PhotoSecrets	. 10
5	Proposal	11
	5.1 Challenges	. 11
	5.2 Proposed Solution	. 11

6	Implementation Details	13
	6.1 Implementation Methodology	13
7	Results	15
8	Conclusions	32
	8.1 Current Status	32
	8.2 Future Work	32
9	Paper Published	33

List of Figures

3.1	GIMP Repositories	5
3.2	GIMP Architecture	6
3.3	Snapshot of Exif data of an Image	8
4.1	TinEye GUI	9
4.2	PicScout GUI	10
4.3	PhotoSecrets GUI	10
6.1	Implementation Methodology	13
7.1	How to go to Python-Fu Console	15
7.2	Python-Fu Console	16
7.3	Code for New Plug-in in Python	16
7.4	Saving New Plug-in	17
7.5	Presence of New Plug-in in GIMP	17
7.6	Code to fetch MAC address in Python	18
7.7	Returned MAC address in the form of 48-bit number	18
7.8	Confirming MAC address	19
7.9	Code to print MAC address in human readable format $\ldots \ldots \ldots \ldots \ldots$	20
7.10	Returned MAC address in human readable format $\hfill \ldots \hfill \hfill \ldots \hfill \hfill \ldots \hfill \ldots \hfill \hfill \ldots \hfill \ldots \hfill \ldots \hfill \hfill \ldots \hfill \hfill \ldots \hfill \hfill \hfill \ldots \hfill $	20
7.11	Path to extract Pexif source	21
7.12	Compiling and building Pexif \ldots	21
7.13	Installing Pexif	22
7.14	Final Plug-in Code	23
7.15	Copying Plug-in Code in GIMP	24
7.16	Plug-in Existence in GIMP	24
7.17	Original Image in .jpg Format	25
7.18	Edited Image in .jpg Format	25

7.19	Edited Image in .jpg Format in Hex Editor	26
7.20	Original Image in .png Format	26
7.21	Edited Image in .png Format	27
7.22	Edited Image in .png Format in Hex Editor	27
7.23	Original Image in .gif Format	28
7.24	Edited Image in .gif Format	28
7.25	Edited Image in .gif Format in Hex Editor	29
7.26	Original Image in .tif Format	30
7.27	Edited Image in .tif Format	30
7.28	Edited Image in .tif Format in Hex Editor	31

Introduction

The Internet is a global network connecting millions of computers. Due to the increasing amount of data available online, the World Wide Web has become one of the most valuable resources for information retrievals and knowledge discoveries. So, anyone from any corner of this world can upload or download anything to and from the Internet. Moreover, social networking is being widely used by people to share each and every update of their life. It has been playing a major role in people's lives. But there also exists a community which misuses such information for financial gains or else for any personal benefits. This is a community which never shows up anywhere in the physical world but plays a significant role on the Internet and they are hackers. In this era of communication, lots of cyber crimes are being performed by them and they are increasing day-by-day and one of them is, social media crime.

Significant number of cases have been filed in which some person's images have been modified in some bad manner and then they have been uploaded on the world wide web on some social networking websites and the original culprit haven't been found for long time as there is no technique available which can directly trace down the computer from which the image has been modified and uploaded on the web. The maximum possible detail is the ip address of the ISP (Internet Service Provider) to which the computer was connected. ISP uses DHCP (Dynamic Host Configuration Protocol) to allocate ip addresses to hosts but that ip address changes everytime the host disconnects and reconnects to the ISP. The ip addresses and the time when they were used by which computer are stored in the form of log files on ISP but ISP maintains these log files for specific amount of time only, due to limited storage capabilities. After that, the log files may get destroyed. So, it is very difficult to know which ip address was used by which computer at what time and thus, the computer used by culprit cannot be traced so easily.

1.1 Problem Definition

Image Tracker helps reducing such kind of crimes as it is the functionality which embeds the source computer's (on which the image has been lastly modified) unique identifier i.e. MAC address into the image by modifying the image's exif data. So, if any such crime takes place by editing and uploading someone's image then the computer, from which it has been uploaded, can be traced down by fetching unique identifier of that computer from the image.

1.2 Chapter Organization

This section gives brief information of all the chapters. Chapter 1 gives the introduction about the topic and the report. Chapter 2 gives the details about why this project was necessary to be carried out. Chapter 3 contains the literature survey of GIMP basics, the existing methodologies of GIMP plug-in development and exif tags. Chapter 4 contains various available techniques of backtracking to the source of the image. Chapter 5 gives details about challenges found in existing techniques and the proposal of this project. Chapter 6 explains the methodology of implementation for the plug-in that is to be developed. Chapter 7 shows the results of the plug-in implemented for embedding MAC address into the image. Chapter 8 concludes with current status and the future work. Chapter gives details of research papers published.

Motivation

There are many image tracking services online like TinEye, PicScout, PhotoSecrets, ePHO-TOzine etc. But they only provide the URL, by backtracking, from where the image has been used and not the exact source from where it has been uploaded. Some of them are purely commercial websites which shares and tracks images for financial gains. The objective of this work is to address the issues and propose solutions as compared to the present works for similar kinds of problems. This is due to the motivation behind the work to make the proposed technique innovative, simple and less computational.

2.1 Domain Study

This project is about working on images and there are lots of websites as well as lots of tools which work on images. To narrow down, first thing is to select a proper tool for image editing and that tool should be open source so as to make changes to it. The popular tools for image modification are:

- 1. Adobe Photoshop
- 2. Picasa
- 3. Paint
- 4. Paint.net
- 5. Microsoft Office Picture Manager

6. GIMP

But none of them, except GIMP, are open source. Picasa and Paint were open source in earlier times but they are not anymore due to some security reasons. So, the most desired tool which is open source as well as popular is GIMP.

Literature Survey

GIMP (GNU Image Manipulation Program) is an image retouching and editing tool and is released as free and open-source software.[17] There are versions available for most operating systems including Linux and Microsoft Windows. GIMP has tools used for image retouching and editing, free-form drawing, resizing, cropping, converting between different image formats etc. Animated images such as GIF and MPEG files can be created using an animation plug-in.

To build a new plug-in for GIMP, we need to first study its source code and the methods for developing plug-in. The GIMP source code lives in the gimp repository on the GNOME git server. The GNOME git server hosts a couple of GIMP related repositories:

Module	Description
babl	Pixel format conversion library
gegl	Generic Graphical Library
gimp	GIMP and the standard set of plug-ins
gimp-data-extras	GIMP Data files such as brushes, gradients, patterns and the like
gimp-gap	GIMP Animation Package, a set of plug-ins that provide video editing functionality
gimp-help-2	GIMP User Manual
gimp-perl	GIMP Perl bindings and a bunch of nice gimp-perl scripts
gimp-plugin-template	GIMP Plug-In Template, a starting ground for plug-in developers
gimp-plugins-unstable	GIMP plug-ins from the past, a collection of unstable and unmaintained plug-ins
gimp-ruby	GIMP Ruby-based scripting plug-in
gimp-tiny-fu	GIMP Tiny-Fu, a drop-in replacement for Script-Fu
gimp-web	the GIMP web site, available at www.gimp.org
gimp-web-devel	the source of the pages you are reading right now

Figure 3.1: GIMP Repositories

[1]

From all of these, GIMP source resides in the GIMP folder. In that, the code of our concern resides at following paths:

- gimp-2.8.6 \app \plug-in
- gimp-2.8.6 \libgimp
- gimp-2.8.6 \plug-ins

3.1 GIMP Architecture



Figure 3.2: GIMP Architecture
[2]

Here are the steps of how it works:

- 1. The GIMP script interface is centered on the Procedural database (PDB). [2]
- 2. At startup, The GIMP looks into a predefined set of places for scripts and plug-ins, and asks each new script to identify itself. [2]
- The plug-in declares itself to the PDB at that time, and passes informations like the position it wishes to get in the menu hierarchy, input parameters, and output parameters.
 [2]
- When a script or a plug-in wants to use our plug-in, it gets through the PDB, which manages communicating parameters in one direction and the other in a transparent way.
 [2]
- 5. Internal functions that wish to get exposed to plug-ins have to be packaged first in the core, that will register them in the PDB, and secondly in the libging that will allow the function to be called as a normal one. [2]

3.2 GIMP Plug-in Development

There are two methods to develop a GIMP plug-in:

- 1. Develop a C plug-in using a library called libging and an associated utility named gimptool.
- 2. Develop a Python plug-in using the Python-Fu interactive console which is in-built in GIMP.

3.3 Exif Tags

EXIF stands for Exchangeable Image File Format, and is a standard for storing interchange information in image files, especially those using JPEG compression.[15] Most digital cameras now use the EXIF format.

The Japan Electronic Industries Development Association (JEIDA) produced the initial definition of Exif.[14] The metadata tags defined in the Exif standard cover a broad spectrum:

- 1. **Date and time information.** Digital cameras will record the current date and time and save this in the metadata.[14]
- 2. Camera settings. This includes static information such as the camera model and make, and information that varies with each image such as orientation, aperture, shutter speed, focal length, metering mode, and ISO speed information.[14]
- 3. A thumbnail, for previewing the picture on the camera's LCD screen, in file managers, or in photo manipulation software.[14]
- 4. Descriptions.
- 5. Copyright information.

For editing exif data of an image using Python in GIMP, Pexif library is compulsory. Pexif is a Python library for parsing and more importantly editing EXIF data in JPEG files. The library contains some examples as well as some usable standalone PexifScripts.[12] Pexif can be downloaded from http: //code.google.com/p/pexif/downloads/list. The latest version is pexif-0.13.

There is one more external library exiftool, which can be used as an external library as currently GIMP has no support for manipulating EXIF data so we will use exiftool as our external library. Exiftool can be downloaded from *http*://www.sno.phy.queensu.ca/phil/exiftool/.

Figure 3.3: Snapshot of Exif data of an Image

[14]

Figure 3.3 is the snapshot captured while checking the exif data of some random image using exiftool.

Study of Available Techniques

4.1 TinEye



Figure 4.1: TinEye GUI

TinEye is the online service which helps searching an image but it has several limitations:

- Limited Index Size: Currently, the Tineye database is at about 700 million images. While that is an impressive number, one has to remember that Photobucket alone has over 5 billion images according to their numbers. The site does not seem to detect duplications on Photobucket, Flickr or other popular image sharing sites, focusing instead on blogs. Thus, many images that are known to have many copies return no results.
- 2. No Case Tracking: Currently, with Tineye, there is no way to track cases of plagiarism or copying so that they are not acted upon a second time.[3]
- 3. No Alerts System: Where writers have Google Alerts and even CopyAlerts, there is currently no system in Tineye that will alert artists to new copies of their work being posted.[3]

4.2 PicScout



Figure 4.2: PicScout GUI

PicScout also has some limitations, which are as follows:

- 1. Uses ImageExchange and ImageTracker applications so it is a dependent application.
- 2. Only monitors business usages.
- 3. Only covers North America, UK and Germany and not India.

4.3 PhotoSecrets



Figure 4.3: PhotoSecrets GUI

PhotoSecrets is also an online image exchange service but it consists of two important features:

- Copyright your photos
- Sell copyrighted photos

Thus, it's purely a commercial website.

Proposal

5.1 Challenges

There are several challenges found in the existing techniques, such as:

- 1. The problem with online image tracking service is, if you are looking for an image which is rarely available on the Internet or else not at all available then it is almost impossible to track it back.
- 2. There are very few image editing tools which are open source.
- 3. There are no tools available which gives any information about the origin of the image.

5.2 Proposed Solution

For developing a functionality which helps identifying the source of image, the unique identifiers of the computer need to be fetched successfully. Moreover, the process of narrowing down on a single tool which is open source as well as popular is also important. And after selection of tool, electing a proper method to develop the technique also matters a lot. The technique is developed for almost all image formats for e.g. .tiff, .jpg, .png etc. The objective of the proposed technique is to develop a cost-effective alternative for commercially available services and tools.

Following is the step wise proposal for the project:

- Narrowing down on a single tool taking into consideration both the open source and most widely used features.
- 2. Selecting a proper method to develop plug-in for selected tool.
- 3. Checking whether the method can fetch unique identifier of computer.
- 4. If yes, then developing final code.

Implementation Details

6.1 Implementation Methodology

GIMP is the most widely used open source tool for image editing and it has in-built interactive Python-Fu console so developing a Pyhton plug-in for GIMP would be more convenient and proper.



Figure 6.1: Implementation Methodology

So, after getting the Python plug-in successfully registered in GIMP, we have to verify whether it can fetch the MAC address of the computer. If so, we would start developing code for embedding fetched MAC address into image by manipulating exif data of the image.

Results

1. The first step is getting our plug-in registered in GIMP. Following are the steps shown for it:



Figure 7.1: How to go to Python-Fu Console

Go to Filters - > Python - Fu - > Console to get Python interactive console in GIMP. The command shown in Figure 7.2 is to test whether Python console responds properly. This is a sample code to get the new plug-in registered in GIMP shown in Figure 7.3. Figure 7.4 shows which path to be selected to save new plug-in.

Figure 7.5 shows that the new plug-in has been successfully registered in GIMP and it is showing at the time of loading GIMP.



Figure 7.2: Python-Fu Console

🥶 Python Console	×
<pre>GIMP 2.8.6 Python Console Python 2.7.5 (default, May 15 2013, 22:43:36) [MSC v.1500 32 bit (Intel)] >>> from gimpfu import * >>> def plugin_main(timg, tdrawable): print "Hello, world!" >>> register("python_fu_resize", "Saves the image at a maximum width and height", "Saves the image at a maximum width and height", "Nathan A. Good", "Nathan A. Good", "2010", "KImage>/Image/Resize to max", RGB*, GRAY*", [], [], plugin_main) >>> >>> main()]</pre>	M H
<u>H</u> elp <u>C</u> lose <u>B</u> rowse <u>C</u> lear <u>Save</u>	

Figure 7.3: Code for New Plug-in in Python

2. After getting the new plug-in successfully registered in GIMP, the next step is to check whether the MAC address can be fetched from Python console in GIMP.

Figure 7.6 shows the code used to fetch MAC address in Python.

Figure 7.7 shows the MAC address fetched from the code above it.



Figure 7.4: Saving New Plug-in



Figure 7.5: Presence of New Plug-in in GIMP

Looking at the getnode documentation, it says that it will return a random long if it fails to detect the mac: "If all attempts to obtain the hardware address fail, we choose a random 48-bit number with its eighth bit set to 1 as recommended in RFC 4122." [16]

One other noticeable thing is that uuid.getnode() can fake the MAC address by returning

2 Python Console	х
<pre>GIMP 2.8.6 Python Console Python 2.7.5 (default, May 15 2013, 22:43:36) [MSC v.1500 32 bit (Intel)] >>> from uuid import getnode as get_mac >>> mac = get_mac()</pre>	*
	III
	4
<u>H</u> elp <u>Close Browse Clear Save</u>	

Figure 7.6: Code to fetch MAC address in Python

🥶 Python Console	X
<pre>GIMP 2.8.6 Python Console Python 2.7.5 (default, May 15 2013, 22:43:36) [MSC v.1500 32 bit (Intel)] >>> mac = get_mac() >>> mac 219948122195246L >>> </pre>	
<u>H</u> elp <u>C</u> lose <u>B</u> rowse <u>C</u> lear <u>S</u> ave	

Figure 7.7: Returned MAC address in the form of 48-bit number

a random 48-bit number which may not be what is expected. Also, there's no explicit indication that the MAC address has been faked, but it can be detected by calling getnode() twice and seeing if the result varies. If the same value is returned by both calls, you have the MAC address, otherwise you are getting a faked address.

Vython Console	3
<pre>GIMP 2.8.6 Python Console Python 2.7.5 (default, May 15 2013, 22:43:36) [MSC v.1500 32 bit (Intel)] >>> from uuid import getnode as get_mac >>> mac = get_mac() >>> from uuid import getnode as get_mac >>> mac = get_mac() >>> mac 219948122195246L >>> </pre>	
<u>H</u> elp <u>C</u> lose <u>B</u> rowse <u>C</u> lear <u>S</u> ave	

Figure 7.8: Confirming MAC address

Looking at figure 7.8, it is confirmed that the MAC address has been returned and it's not fake as same value is returned by both calls.

uuid.getnode represents current MAC address as an integer, this one-liner code in figure 7.9 formats this number in a standard MAC address form.

Thus, the MAC address of computer is fetched successfully.

3. The next step after fetching the MAC address is to develop code which embeds this MAC into image.

The one way to do this is to use exif tags and to make use of exif and to edit or modify them in GIMP, the use of pexif library is must. Following are the steps to install pexif



Figure 7.9: Code to print MAC address in human readable format



Figure 7.10: Returned MAC address in human readable format

library.

	n library 🔻 Share with 👻 Burn	New folder				800 -	
Downloads	Name	Date modified	Туре	Size			
Favorites	Duild Duild	11/25/2013 10:49	File folder				
GNS3	scripts	11/25/2013 10:46	File folder				
Google	鷆 test	11/25/2013 10:46	File folder				
Links	🛃 pexif	4/22/2009 3:31 PM	Python File	42 KB			
My Documents	PKG-INFO	4/23/2009 5:58 AM	File	1 KB			
My Music	README	4/22/2009 3:15 PM	File	3 KB			
My Pictures	🛃 setup	4/22/2009 5:35 PM	Python File	2 KB			
Saved Gamer							
Searcher							
Tracing							
Computer							
comparer							
vetwork							
letwork Control Panel							
Network Control Panel Recycle Bin							
Network Control Panel Recycle Bin Da retire thai gay							
letwork control Panel lecycle Bin la retire thai gay chennai Express							
Network Control Panel Recycle Bin Da retire thai gay Chennai Express digant pics							
Network Control Panel Recycle Bin Da retire thai gay Chennai Express digant pics English Vinglish							
Vetwork Control Panel Recycle Bin as retire thai gay Chennai Express ligant pics inglish Vinglish E SPSC							
Vetwork Control Panel Recycle Bin as retire thai gay Chennai Express digant pics Singlish Vinglish GPSC Srishma pd 24-1:							
Network Control Panel Recycle Bin pa retire thai gay chennai Express inglish Vinglish i spSC prishma pd 24-1: pw							
Aetwork Control Panel Arcycle Bin Ar retire thai gay Chennai Express ligant pics nglish Vinglish 1 pSC sirishma pd 24-12 sw armela ne puchi							
Network Control Panel Recycle Bin Dar setire thai gay Chennai Express inglish Vinglish : SPSC Srishma pd 24-1: pw aamela ne puchi rooject daily wor							
Network Control Panel Recycle Bin as retire thai gay Chennai Express Jigant pics Singlish Vinglish ; BPSC Srishma pd 24-1: pw parnela ne puchi project daily wor Jamaiya V astava							
Network Control Panel Recycle Bin ba retire thai gay Chennai Express digant pics Gnglish Vinglish (GPSC Gristma pd 24-1: Ipw parnela ne puchi project daily wor Ramaiya Vastava							

Figure 7.11: Path to extract Pexif source

Figure 7.11 shows the path where the pexif source should be extracted so that it can be installed successfully.

👞 Administrator: C:\Windows\System32\cmd.exe	٢.
Microsoft Windows [Version 6.1.7600] Copyright <c> 2009 Microsoft Corporation. All rights reserved.</c>	•
C:\Windows\system32>cd	
C:\Windows≻cd	
C:\>cd Python27\pexif-0.13	=
G:\Python27\pexif-0.13>\python.exe setup.py build running build running build_py creating build creating build\lib copying pexif.py -> build\lib running build_scripts creating build\scripts-2.7 copying and adjusting scripts\dump_exif.py -> build\scripts-2.7 copying and adjusting scripts\setgps.py -> build\scripts-2.7 copying and adjusting scripts\getgps.py -> build\scripts-2.7 copying and adjusting scripts\getgps.py -> build\scripts-2.7 copying and adjusting scripts\setgps.py -> build\scripts-2.7 copying and adjusting scriptsgetgps.py -> build\scripts-2.7 copying and adjusting scriptsmezone.py -> build\scripts-2.7 copying and adjusting scripts\timezone.py -> build\scripts-2.7 copying and adjusting scripts\timezone.py -> build\scripts-2.7 copying and adjusting scripts\timezone.py -> build\scripts-2.7	



After successfully compiling and building, all the scripts are built in build\scripts-2.7.

```
C:\Python27\pexif-0.13>..\python.exe setup.py install
running install
running build_py
running build_scripts
running build\lib\pexif.py -> C:\Python27\Lib\site-packages
byte-compiling C:\Python27\Lib\site-packages\pexif.py to pexif.pyc
running install_scripts
copying build\scripts-2.7\getgps.py -> C:\Python27\Scripts
copying build\scripts-2.7\setgps.py -> C:\Python27\Scripts
copying build\scripts-2.7\setgps.py -> C:\Python27\Scripts
copying build\scripts-2.7\setgps.py -> C:\Python27\Scripts
copying build\scripts-2.7\timezone.py -> C:\Python27\timezone.py -> C:\Python27\t
```

Figure 7.13: Installing Pexif

Returning to command prompt shows that pexif is successfully installed. After successful installation, the scripts are copied into C:\Python27\Scripts, which is shown in figure 7.13.

Figure 7.14 shows the final plug-in code that embeds the MAC address into the image in its Artist field which is one of the unused Exif field.

We have to copy and paste that code into "C:\Program Files\GIMP 2\lib\gimp\2.0\plugins" path so that we can see the plug-in existence in GIMP.

Moreover, the highlighted line shows that this plug-in uses an external script i.e. exiftool.exe which is located at "C:\Windows" path, which helps GIMP in modifying Exif data as GIMP does not have support for manipulating Exif data.

Figure 7.16 shows the existence of plug-in in GIMP File menu. The plug-in also has shortcut Ctrl+S assigned to it.

4. The final step is to show resulted images that have MAC addresses embedded into them. Here, it is shown for different image file formats like .jpg, .png, .gif and .tif. The plug-in works for all of these image file formats.

Following are the command prompt snapshots that show the comparison between the original image and the image after using the plug-in.

```
_ 🗆 🗙
7% Sample.py - E:\project\review 4\Sample.py
File Edit Format Run Options Windows Help
#!/usr/bin/env python
import os
import commands
import subprocess
import platform
import uuid
from gimpfu import *
import os.path
print ':'.join(['{:02x}'.format((uuid.getnode() >> i) & 0xff) for
i in range(0,8*6,8)][::-1])
tag1 = '-Artist='+':'.join(['{:02x}'.format((uuid.getnode() >> i) & 0xff) for
i in range(0,8*6,8)][::-1])
def insert_MAC(image, drawable):
    name = image.filename
   cmd = r'C:\Windows\exiftool.exe'
    cmdlist = [cmd, tag1, name]
    p = subprocess.Popen(cmdlist, stdout=subprocess.PIPE)
    out = p.stdout.readlines()
    return
register(
    "insert MAC",
    "Save",
    "This script adds MAC as EXIF. It is extremely good at it",
    "Khyati Thakkar",
    "Abdul Zummerwala",
    "March 2014",
    "<Image>/File/Save",
    "*",
    [],
    [],
    insert_MAC)
main()
                                                                             Ln: 38 Col: 6
```

Figure 7.14: Final Plug-in Code

ize 👻 🤫 Open	▼ Burn Net	wtolder									E •
My Pictures * My Videos project	oilify.exe	pagecurl.exe	palette-offset.py	palette-sort.py	palette-to-gradie nt.py	photocopy.exe	pixelize.exe	plasma.exe	plugin-browser.e xe	polar-coords.exe	print.exe
Saved Games Searches Tracing Computer	*		ę				*	*	*	*	R
Network Control Panel	procedure-brows er.exe	pyconsole.py	pyconsole.pyc	py-slice.py	python-console. py	python-eval.py	qbist.exe	red-eye-removal. exe	ripple.exe	rotate.exe	Sample.p
Recycle Bin NET Material 201 picasaoriginals pa retire thai gay	*	* }	* }	*		*	*	*	*	* }	:
BARC Chennai Express	sample-colorize.e xe	script-fu.exe	selection-to-path .exe	semi-flatten.exe	sharpen.exe	shift.exe	sinus.exe	smooth-palette.e xe	softglow.exe	sparkle.exe	sphere-desig exe
inglish Vinglish 2 SPSC Brishma pd 24-12		*	*	*	*	*	*	*	*	*	:
SRO pw E barnela ne puchi	text-brush.py	threshold-alpha.e xe	tile.exe	tile-glass.exe	tile-paper.exe	tile-seamless.exe	tile-small.exe	twain.exe	unit-editor.exe	unsharp-mask.ex e	value-invert
Photos project daily wor Ramaiya Vastava TCS	*	*	*	*	.	*	*	*	*	\odot	
hxDSetupEN.zip	value-propagate. exe	van-gogh-lic.exe	video.exe	warp.exe	waves.exe	web-browser.exe	web-page.exe	whirl-pinch.exe	wind.exe	win-snap.exe	

Figure 7.15: Copying Plug-in Code in GIMP



Figure 7.16: Plug-in Existence in GIMP

		A
:\Users\Khyati\Downloads>exi	tool.exe nature.jpg_original	
ExifTool Version Number	: 9.37	
'ile Name	: nature.jpg_original	
irectory	÷.	
'ile Size	: 14 kB	
'ile Modification Date/Time	: 2014:05:11 13:59:08+05:30	=
'ile Access Date/Time	: 2014:05:11 14:03:04+05:30	
'ile Creation Date/Time	: 2014:05:11 14:03:04+05:30	
'ile Permissions	: rw-rw-rw-	
'ile Type	: JPEG	
ІІМЕ Туре	: image∕jpeg	
FIF Version	: 1.01	
lesolution Unit	: None	
Resolution	: 1	
Resolution	: 1	
mage Width	: 300	
mage Height	: 168	
ncoding Process	: Baseline DCT, Huffman coding	
lits Per Sample	: 8	
olor Components	: 3	
Cb Cr Sub Sampling	: YCbCr4:4:4 (1 1)	
mage Size	: 300×168	
:\Users\Khyati\Downloads>		

Figure 7.17: Original Image in .jpg Format

C:\Windows\system32\cmd.exe	the second se	x
C:\Users\Khyati\Downloads>exift ExifTool Version Number File Name Directory File Size File Modification Date/Time File Creation Date/Time File Creation Date/Time File Permissions File Iype JFIF Version Exif Byte Order X Resolution Y Resolution Artist Y Cb Cr Positioning Image Width Image Height Encoding Process Bits Per Sample Color Components Y Cb Cr Sub Sampling Image Size C:\Users\Khyati\Downloads>	<pre>ool.exe nature.jpg : 9.37 : nature.jpg : : 14 kB : 2014:05:11 14:55:25+05:30 : 2014:05:11 14:55:25+05:30 : 2014:05:11 14:03:04+05:30 : rw-rw-rw- JPEG : image/jpeg : 1.01 : Big-endian (Motorola, MM) : 1 : 1 : None : c8:0a:a9:b1:45:2e : Centered : 300 : 168 : Baseline DCT, Huffman coding : 8 : 3 : YCbCr4:4:4 (1 1) : 300x168</pre>	

Figure 7.18: Edited Image in .jpg Format

🔊 HxD - [C:\Use	ers\Kł	hyati	\Dow	/nloa	ads\n	atur	e.jpg]									
🕼 File Edit	Searc	h V	iew	Ana	lysis	Ext	ras	Wine	dow	?							
	~	e al		10	·			C 1			1.						
: 🛄 🖾 🖌 🔤	Sum.			10			AN	SI		•	ne	x		1			
📓 nature.jpg																	
Offset (h)	00	01	02	03	04	05	06	07	80	09	0A	0B	0C	OD	0E	OF	
00000000	FF	D8	FF	ΕO	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿàJFIF
00000010	00	01	00	00	FF	E1	00	74	45	78	69	66	00	00	4D	4D	ÿá.tExifMM
00000020	00	2A	00	00	00	08	00	05	01	1A	00	05	00	00	00	01	.*
00000030	00	00	00	4A	01	1B	00	05	00	00	00	01	00	00	00	52	JR
00000040	01	28	00	03	00	00	00	01	00	01	00	00	01	ЗB	00	02	. (;
00000050	00	00	00	12	00	00	00	5A	02	13	00	03	00	00	00	01	Z
00000060	00	01	00	00	00	00	00	00	00	00	00	01	00	00	00	01	-0.0
00000070	00	00	00	01	00	00	00	01	63	38	3A	30	61	3A	61	39	
00000080	3A	62	31	3A	34	35	3A	32	00	14	2.0	DB	10	15	1.4	17	:b1:45:2e.y0."
00000090	10	14	19	12	17	13	17	14	12	17	14	19	15	10	12	16	
000000A0	10	10	10	10	20	10	17	7.2	10	1 -	17	21	21	21	10	20	/ % 111%
0000000000	28	25	25	20	10	15	22	20	22	20	27	21	20	21	23	2.9	+ 292-7/-+
000000000	07	07	07	05	00	OF	18	10	10	18	20	20	20	24	20	201	+
0000000000	20	20	20	20	20	20	20	20	28	28	20	20	20	20	20	20	_ //
000000E0	20	20	20	20	20	25	20	20	21	20	25	20	20	20	20	20	/ / /
00000100	20	20	20	2C	2 F	20	20	20	20	20	20	20	20	20	20	20	
00000110	FF	co	00	11	08	00	A8	01	2C	03	01	11	00	02	11	01	ÿÀ"
00000120	03	11	01	FF	C4	00	1B	00	00	02	03	01	01	01	00	00	,
00000130	00	00	00	00	00	00	00	00	01	03	00	02	04	05	06	07	
00000140	FF	C4	00	3C	10	00	01	02	05	03	02	03	07	02	04	05	ÿÄ.<
00000150	04	03	00	00	00	01	02	11	00	03	12	21	31	04	41	51	- !1.AQ
00000160	22	61	05	71	81	06	13	32	91	A1	B1	FO	42	C1	14	52	"a.q2`;±ðBÁ.R
00000170	D1	F1	15	23	62	72	E1	16	33	43	C2	25	53	92	FF	C4	Ññ.#brá.3CÂ%S'ÿÄ
00000180	00	1B	01	00	02	03	01	01	01	00	00	00	00	00	00	00	
00000190	00	00	00	00	01	02	03	04	05	06	07	FF	C4	00	39	11	ÿÄ.9.
000001A0	00	01	03	02	03	06	05	03	04	02	01	04	03	01	00	00	
000001B0	01	00	02	11	03	21	04	31	41	12	51	61	71	81	FO	13	!.1A.Qaq.ð.
000001C0	22	91	A1	B1	05	C1	D1	14	32	E1	F1	15	42	52	23	53	"`;±.ÁÑ.2áñ.BR#S
000001D0	62	92	24	72	A2	33	FF	DA	00	0C	03	01	00	02	11	03	b′\$r¢3ÿÚ
000001E0	11	00	ЗF	00	ΕO	Β4	7D	21	78	Α4	1A	04	4A	8D	02	25	?.à'}!x¤J%
000001F0	46	81	12	83	43	94	D5	90	21	14	8A	Β4	24	94	81	0A	FfC″Õ.!.Š´\$″
00000200	40	85	1A	04	20	D0	D0	A3	40	85	1A	04	28	D0	26	83	0 ĐĐ£0 (Đ&f
00000210	40	89	55	86	9A	90	D0	A3	40	84	1A	04	28	D0	21	46	0%U†š.Đ£0"(Đ!F
00000220	81	35	1A	04	26	26	49	B 3	82	C4	C5	15	2B	Β4	07	00	.5&&I³,ÄÅ.+´
00000230	44	81	29	85	A9	52	90	95	33	39	01	FE	DB	6F	1E	46	D.)©R.•39.þÛo.F

Figure 7.19: Edited Image in .jpg Format in Hex Editor

C:\Users\Khyati\Downloads>exiftool.exe nature.png_original ExifTool Version Number : 9.37 File Name : nature.png_original Directory : . File Size : 110 kB File Modification Date/Time : 2014:05:11 14:00:20+05:30 File Access Date/Time : 2014:05:11 14:03:04+05:30 File Creation Date/Time : 2014:05:11 14:03:04+05:30 File Permissions : rw-rw-rw- File Type : PNG MIME Type : image/png Image Width : 300 Image Width : 300 Image Height : 168 Bit Depth : 8 Color Type : RGB with Alpha Compression : Deflate/Inflate Filter : Adaptive Interlace : Noninterlaced SRGB Rendering : Perceptual Gamma : 2.2 Pixels Per Unit X : 3780 Pixels Per Unit X : 3780 Pixels Per Unit Y : 3780 Pixel Ser Unit S : Meters Image Size : 300x168 C:\Users\Khyati\Downloads>	GRI C:\Windows\system32\cmd.exe	- 0 ×
	C:\Users\Khyati\Downloads>exiftool.exe nature.png_original ExifTool Version Number : 9.37 File Name : nature.png_original Directory : nature.png_original Eile Size : 110 kB File Modification Date/Time : 2014:05:11 14:00:20+05:30 File Access Date/Time : 2014:05:11 14:03:04+05:30 File Creation Date/Time : 2014:05:11 14:03:04+05:30 File Creation Date/Time : 2014:05:11 14:03:04+05:30 File Permissions : rw-rw-rw- File Type : PNG MIME Type : PNG MIME Type : image/png Image Width : 300 Image Height : 168 Bit Depth : 8 Color Type : RGB with Alpha Compression : Deflate/Inflate Filter : Adaptive Interlace : Noninterlaced SRGB Rendering : 2.2 Pixels Per Unit X : 3780 Pixel Ser Unit X : 3780 Pixel Units : Meters Image Size : 300x168 C:\Users\Khyati\Downloads>	E

Figure 7.20: Original Image in .png Format

C:\Users\Khyati\Downloads>exiftool.exe nature.png	
ExifTool Version Number: 9.37File Name: nature.pngDirectory:File Size: 110 kBFile Modification Date/Time: 2014:05:11 15:09:11+05:30File Access Date/Time: 2014:05:11 15:09:11+05:30File Creation Date/Time: 2014:05:11 14:03:04+05:30File Permissions: rw-rw-rw-File Iype: inage/pngImage Width: 300Image Height: 168Bit Depth: 8Color Type: RGB with AlphaCompression: Deflate/InflateFilter: AdaptiveInterlace: NoninterlacedSRGB Rendering: 2.2Pixels Per Unit X: 3780Pixel Ser Unit X: 3780Pixel Units: MetersArtist: c8:0a:a9:b1:45:2eImage Size: 300×168	×
C:\Users\Khyati\Downloads>_	

Figure 7.21: Edited Image in .png Format

iiii File Edit iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	Searc Searc 0 00 77 7C FD E4 36 E9 4C 55	h V natu 01 45 C8 29 19 21 06 C6	iew re.pr 02 E5 18 57 8F 74 24	Ana 16 99 96 AC 5E BB 4F 03	04 2D CA 7B 01 07	Ext 05 18 32 C2 2C AD	AN: 06 48 70 7F 2F	Wind SI 07 59 B3 F8 58	08 DC AF DA	? • 09 BC 77	he 0A C5 C0	OB CE 8A	OC FF E9	OD FE A1	0E 13 FB	0F C6 04	wEå−HYÜԿÅÎÿþ.£ ÈÊ20°¯wÀŠé:û.
) 00 77 7C FD E4 36 E9 4C	natu 01 45 C8 29 19 21 06 C6	e.pr 02 E5 18 57 8F 74 24	16 99 96 AC 5E 8B 4F 03	04 2D CA 7B 01 07	 05 18 32 C2 2C AD 	AN: 06 48 70 7F 2F	SI 07 59 B3 F8 58	08 DC AF DA	• 09 BC 77	0A C5 C0	OB CE 8A	OC FF E9	OD FE A1	0E 13 FB	OF C6 OA	wEå−HYÜԿÅÎÿþ.Æ È.⊣Ê20°¯wÀŠé:û.
nature.jpg Offset(h 0001B740 0001B750 0001B760 0001B770 0001B780 0001B780 0001B740 0001B740 0001B780 0001B780 0001B780 0001B780 0001B780 0001B780 0001B780 0001B780) 00 77 7C FD E4 36 E9 4C	natu 01 45 C8 29 19 21 06 C6	02 E5 18 57 8F 74 24	03 96 AC 5E 8B 4F 03	04 2D CA 7B 01 07	05 18 32 C2 2C AD	06 48 70 7F 2F	07 59 B3 F8 58	08 DC AF DA	09 BC 77	0A C5 C0	0B CE 8A	OC FF E9	OD FE A1	0E 13 FB	OF C6	wEå−−.HYÜԿÅÎÿp.Æ ∣ÈÊ2p³¯wÀŠé:û.
Offset(h 0001B740 0001B750 0001B760 0001B770 0001B780 0001B780 0001B7A0 0001B7B0) 00 77 7C FD E4 36 E9 4C 55	01 45 C8 29 19 21 06 C6	02 E5 18 57 8F 74 24	03 96 AC 5E BB 4F 03	04 2D CA 7B 01 07	05 18 32 C2 2C AD	06 48 70 7F 2F	07 59 B3 F8 58	08 DC AF DA	09 BC 77	0A C5 C0	0B CE 8A	OC FF E9	OD FE A1	0E 13 FB	OF C6 0A	wEå−−.HYÜษÅÎÿp.Æ ∣È.¬Ê2p³¯wÀŠé;û.
0001B740 0001B750 0001B760 0001B770 0001B780 0001B780 0001B780 0001B780	77 7C E4 36 E9 4C	45 C8 29 19 21 06 C6	E5 18 57 8F 74 24	96 AC 5E BB 4F 03	2D CA 7B 01 07	18 32 C2 2C AD	48 70 7F 2F	59 B3 F8 58	DC AF DA	BC 77	C5 C0	CE 8A	FF E9	FE A1	13 FB	C6	wEå−−.HYÜ+₄ÅÎÿþ.Æ È.¬Ê2p³¯wÀŠé;û.
0001B750 0001B760 0001B770 0001B780 0001B790 0001B7A0 0001B7B0 0001B7C0	7C FD E4 36 E9 4C	C8 29 19 21 06 C6	18 57 8F 74 24	AC 5E BB 4F 03	CA 7B 01 07	32 C2 2C AD	70 7F 2F	B3 F8 58	AF DA	77	C0	8A	E9	A1	FB	٥A	lÈ.⊣Ê2p³ wÀŠé;û.
0001B760 0001B770 0001B780 0001B790 0001B7A0 0001B7B0 0001B7C0	FD E4 36 E9 4C	29 19 21 06 C6	57 8F 74 24	5E BB 4F 03	7B 01 07	C2 2C AD	7F 2F	F8	DA	1 5							
0001B770 0001B780 0001B790 0001B7A0 0001B7B0 0001B7C0	E4 36 E9 4C	19 21 06 C6	8F 74 24	BB 4F 03	01 07	2C AD	2 F	58		15	E7	F6	B3	B 7	91	1E	ý)W^{Â.øÚ.çö³.`.
0001B780 0001B790 0001B7A0 0001B7B0 0001B7C0	36 E9 4C	21 06 C6	74 24	4F 03	07	AD			D9	0B	E2	73	88	DB	7F	ЗA	ä».,/XÙ.âs^Û.:
0001B790 0001B7A0 0001B7B0 0001B7C0	E9 4C	06 C6	24	03			BA	32	AO	B2	17	A 7	BD	30	ED	45	6!t0°2 °.§¥01E
0001B7A0 0001B7B0 0001B7C0	4C	C6	00		ZE	47	19	4E	15	E9	3E	F6	FE	9F	E8	C5	é.ŞG.N.é>öþŸèÅ
0001B7B0 0001B7C0	55		90	57	71	6F	55	A1	23	5A	05	6C	FF	5F	00	96	LÆ.WqoU;#Z.lÿ
0001B7C0		57	7F	07	2C	AB	AE	EC	D8	2A	8E	01	96	55	53	06	UW,≪®ìØ*ŽUS.
	58	6E	4E	СВ	2A	2C	0B	9F	FD	15	8E	CA	0D	5A	79	01	XnNË*,.Ÿý.ŽÊ.Zy.
0001B7D0	CB	C0	CA	0D	58	36	0D	FC	9F	80	65	E2	5B	03	2C	FE	ËÀÊ.X6.üŸ€eâ[.,þ
0001B7E0	77	7F	A5	62	FF	4B	9A	E1	7E	6C	EC	F1	79	10	60	E5	w.¥bÿKšá~lìñy.`å
0001B7F0	FD	1F	В9	81	CA	FE	77	F6	FF	FC	04	70	BA	C6	70	C6	ý.¹.Êþwöÿü.p°ÆpÆ
0001B800	8E	11	EE	D6	0E	7E	F6	F6	11	7D	FA	C6	21	7D	ΟA	58	Ž.1Ö.~öö.}úÆ!}.X
0001B810	7D	C2	D4	F9	ED	8B	A 8	E1	69	F9	2E	BF	BA	D3	99	42	}ÂÔùí<¨áiù.¿°Ó™B
0001B820	BF	C3	44	FA	2D	3E	F7	ЗA	64	FC	4B	CF	6F	D6	FE	97	¿ÄDú->÷:düKÏoÖþ—
0001B830	76	EB	F9	E7	F6	EB	22	3B	8A	4F	1E	5E	43	DB	B8	47	vëùçöë";ŠO.^CÜ,G
0001B840	5B	2F	AC	D1	DC	63	53	F5	C6	33	1B	01	BC	FD	FF	E3	[/¬NÜcSõÆ3¼ýÿã
0001B850	FC	7F	57	26	AF	68	42	3D	36	47	00	00	00	18	74	45	ü.W& hB=6GtE
0001B860	58	74	41	72	74	69	73	74	00	63	38	ЗA	30	61	ЗA	61	XtArtist. <mark>c8:0a:a</mark>
0001B870	39	ЗA	62	31	ЗA	34	35	ЗA	32	65	49	CE	88	A 5	00	00	9:b1:45:2e <mark>IÎ^¥</mark>
0001B880	00	00	49	45	4E	44	AE	42	60	82							IEND®B`,

Figure 7.22: Edited Image in .png Format in Hex Editor

C:\Windows\system32\cmd.exe	International Control of Control	
C:\Users\Khyati\Downloads>exif ExifTool Version Number File Name Directory File Size File Modification Date/Time File Access Date/Time File Creation Date/Time File Permissions File Type MIME Type GIF Version Image Width Image Height Has Color Map Color Resolution Depth Bits Per Pixel Background Color Image Size C:\Users\Khyati\Downloads>_	<pre>ftool.exe nature.gif_original 9.37 nature.gif_original . 26 kB 2014:05:11 14:01:09+05:30 2014:05:11 14:03:04+05:30 2014:05:11 14:03:04+05:30 rw-rw-rw- GIF image/gif 89a 300 168 Yes 8 0 300×168</pre>	E

Figure 7.23: Original Image in .gif Format

cs. C:\Windows\system32\cmd.exe		- 0 ×
C:\Users\Khyati\Downloads>exif ExifTool Version Number File Name Directory File Size File Modification Date/Time File Access Date/Time File Creation Date/Time File Permissions File Type GIF Version Image Width Image Height Has Color Map Color Resolution Depth Bits Per Pixel Background Color XMP Ioolkit Artist Image Size C:\Users\Khyati\Downloads>	<pre>'tool.exe nature.gif : 9.37 : nature.gif : 29 kB : 2014:05:11 15:21:07+05:30 : 2014:05:11 15:21:07+05:30 : 2014:05:11 14:03:04+05:30 : rw-rw-rw- : GIF : image/gif : 89a : 300 : 168 : Yes : 8 : 8 : 8 : 0 : Image::ExifTool 9.37 : c8:0a:a9:b1:45:2e : 300x168</pre>	

Figure 7.24: Edited Image in .gif Format

🔊 HxD - [C:\Use	ers\Kl	hyati	\Dov	vnloa	ads\r	natur	e.gif										
🔛 File Edit	Searc	h V	iew	Ana	lysis	Ext	ras	Win	dow	?							
	~	en B		10	·			CT			1.						
: 💷 🖾 T 🖬	Conne		-	10			AN	51		•	ne	x		1			
ature.jpg	ED.	natu	re.pr	ng	50 I	natur	e.gif										
							-										
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF	
00000320	58	4D	50	3C	ЗF	78	70	61	63	6B	65	74	20	62	65	67	XMP xpacket beg</th
00000330	69	6E	ЗD	27	EF	BB	BF	27	20	69	64	ЗD	27	57	35	4D	in='ï≫¿' id='₩5M
00000340	30	4D	70	43	65	68	69	48	7A	72	65	53	7A	4E	54	63	0MpCehiHzreSzNTc
00000350	7A	6B	63	39	64	27	ЗF	ЗE	0A	3C	78	ЗA	78	6D	70	6D	zkc9d'?>. <x:xmpm< th=""></x:xmpm<>
00000360	65	74	61	20	78	6D	6C	6E	73	ЗA	78	ЗD	27	61	64	6F	eta xmlns:x='ado
00000370	62	65	ЗA	6E	73	ЗA	6D	65	74	61	2F	27	20	78	ЗA	78	be:ns:meta/' x:x
00000380	6D	70	74	6B	ЗD	27	49	6D	61	67	65	ЗA	ЗA	45	78	69	mptk='Image::Exi
00000390	66	54	6F	6F	6C	20	39	2E	33	37	27	3E	0A	3C	72	64	fTool 9.37'>. <rd< th=""></rd<>
000003A0	66	ЗA	52	44	46	20	78	6D	6C	6E	73	ЗA	72	64	66	ЗD	f:RDF xmlns:rdf=
000003B0	27	68	74	74	70	3A	2F	2F	77	77	77	2E	77	33	2E	6F	http://www.w3.o
000003C0	72	67	2F	31	39	39	39	2F	30	32	2F	32	32	2D	72	64	rg/1999/02/22-rd
000003D0	66	2D	73	79	6E	74	61	78	2D	6E	73	23	27	3E	OA	AO	f-syntax-ns#'>
000003E0	20	3C	72	64	66	ЗA	44	65	73	63	72	69	70	74	69	6F	<rdf:descriptio< th=""></rdf:descriptio<>
000003F0	6E	20	72	64	66	3A	61	62	6F	75	74	3D	27	27	0A	20	n rdf:about=''.
00000400	20	78	6D	6C	6E	73	ЗA	74	69	66	66	ЗD	27	68	74	74	xmlns:tiff='htt
00000410	70	3A	2F	2F	6E	73	2E	61	64	6F	62	65	2E	63	6F	6D	p://ns.adobe.com
00000420	21	74	69	66	66	21	31	2E	30	2F	27	3E	0A	20	20	3C	/tiff/1.0/'>. <
00000430	74	69	66	66	3A	41	72	74	69	73	74	3E	63	38	3A	30	tiff:Artist>c8:0
00000440	61	3A	61	39	3A	62	31	3A	34	35	3A	32	65	30	21	74	a:a9:b1:45:2ek/t
00000450	69	66	66	3A	41	72	74	69	73	74	3E	OA	20	30	21	72	111:Artist>.
00000480	201	25	3A 72	44	00	73	63	12	09	25	07	20	10	70	32	UA 70	dr:Description>.
00000470	30	21	/2 CD	64	24	SA C1	3Z		20	36	20	30	22	20	20	20	.
00000480	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	mpmecay.
00000490	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000480	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000400	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000400	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
000004F0	20	20	20	20	20	20	20	20	20	20	20	20	01	20	20	20	
000004F0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	•
00000500	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000510	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000520	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000530	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000540	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00000550	20	0A	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
1	-																

Figure 7.25: Edited Image in .gif Format in Hex Editor

C:\Windows\system32\cmd.exe	
G:\Users\Khyati\Downloads>exift Evifteel Heneier Number	ool.exe nature.tlf_orlginal
EXIFICOI Version Mumber	· 7.37
File Mane	nature.tlf_orlginal
Directory	44 LD
File Size File Medification Date/Time	- 44 KD - 2014-05-11 14-01-20-05-20
File Access Date /Time	· 2014.05.11 14.01.27.03.30
File Access Date/Time	· 2014.05.11 14.03.04+05.30
File Permissions	· 2017-0J-11 17-0J-07-0J-J0
File Tune	TIPE
MIME Tune	image/tiff
Frif Bute Owder	: Little-endian (Intel II)
Subfile Tune	: Full-resolution Image
Image Width	: 300
Image Height	: 168
Bits Per Sample	8888
Compression	: LZW
Photometric Interpretation	: RGB
Strip Offsets	: (Binary data 93 bytes, use -b option to extrac
t)	, , , , , , , , , , , , , , , , , , ,
Samples Per Pixel	: 4
Rows Per Strip	: 10
Strip Byte Counts	: (Binary data 84 bytes, use -b option to extrac
t)	
X Resolution	: 96.012
Y Resolution	: 96.012
Planar Configuration	: Chunky
Resolution Unit	: inches
Predictor	: Horizontal differencing
Extra Samples	: Unassociated Alpha
lmage Size	: 300×168
C:\Users\Khyati\Downloads>	

Figure 7.26: Original Image in .tif Format

C:\Windows\system32\cmd.exe												
		~										
G:\Users\Khyati\Downloads>exiftool.exe_nature.tif												
ExifTool Version Number	: 9.37											
File Name	: nature.tif											
Directory	·											
File Size	: 44 kB											
File Modification Date/Time	: 2014:05:11 15:26:19+05:30	E										
File Access Date/Time	: 2014:05:11 15:26:19+05:30											
File Creation Date/Time	: 2014:05:11 14:03:04+05:30											
File Permissions	: PW-PW-PW-											
File Type	: TIFF											
MIME Type	: image/tiff											
Exif Byte Order	: Little-endian (Intel, II)											
Subfile Type	: Full-resolution Image											
Image Width	: 300											
Image_Height	: 168											
Bits Per Sample	: 8 8 8 8											
Compression	: LZW											
Photometric Interpretation	: RGB											
Strip Offsets	: (Binary data 96 bytes, use -b option	n to extrac										
t)												
Samples Per Pixel	: 4											
Rows Per Strip	: 10											
Strip Byte Counts	: (Binary data 84 bytes, use -b option	n to extrac										
t)												
K Resolution	: 96.012											
Y Resolution	: 96.012											
Planar Configuration	: Chunky											
Resolution Unit	: inches											
Artist	: c8:0a:a9:b1:45:2e											
Predictor	: Horizontal differencing											
Extra Samples	: Unassociated Alpha											
Image Size	: 300×168											
C:\Users\Khyati\Downloads>												

Figure 7.27: Edited Image in .tif Format

🔟 HxD - [C:\Users\Khyati\Downloads\nature.tif]																	
El File Edit	Searc	h V	iew	Ana	lysis	Ext	ras	Wind	wob	?							
	~	en B	-		.,												
🛄 🚰 🖬	Cum	9	+	16			AN	SI		•	he	x		1			
📓 nature.jpg	FD	natu	re.pr	ng	FC r	natur	e.gif	FD	na	ture.	tif						
Offset(h)	00	01	02	03	04	05	06	07	08	09	AO	0B	oc	OD	OE	OF	
00000000	49	49	22	00	08	00	00	00	16	00	मन	00	04	00	01	00	TT★ b
00000010	00	00	00	00	00	00	00	01	04	00	01	00	00	00	2C	01	
00000020	00	00	01	01	04	00	01	00	00	00	A8	00	00	00	02	01	
00000030	03	00	04	00	00	00	16	01	00	00	03	01	03	00	01	00	
00000040	00	00	05	00	00	00	06	01	03	00	01	00	00	00	02	00	
00000050	00	00	11	01	04	00	11	00	00	00	1E	01	00	00	15	01	
00000060	03	00	01	00	00	00	04	00	00	00	16	01	04	00	01	00	
00000070	00	00	A0	00	00	00	17	01	04	00	11	00	00	00	62	01	b.
00000080	00	00	1A	01	05	00	01	00	00	00	Α6	01	00	00	1B	01	
00000090	05	00	01	00	00	00	AE	01	00	00	1C	01	03	00	01	00	
000000A0	00	00	01	00	00	00	28	01	03	00	01	00	00	00	02	00	
00000080	00	00	38	01	02	00	12	00	00	00	B6	01	00	00	3D	01	;
000000000	03	00	01	00	00	00	02	51	00	00	52	01	03	00	01	00	·····
000000000	00	00	02	51	00	00	00	21	04	00	01	00	00	00	00	51	
000000E0	00	00	00	03	0.0	00	CR	01	00	00	03	51	01	00	02	00	÷ 0
00000100	00	00	00	00	00	00	04	51	01	00	01	00	00	00	FC	00	Q
00000110	00	00	00	00	00	00	08	00	08	00	08	00	08	00	CB	04	È.
00000120	00	00	73	0B	00	00	56	13	00	00	77	1B	00	00	6E	24	sVwn\$
00000130	00	00	C7	2E	00	00	14	39	00	00	C 8	43	00	00	3B	4D	ç9ÈC;M
00000140	00	00	08	55	00	00	0A	60	00	00	77	6B	00	00	FA	76	U`wkúv
00000150	00	00	3C	83	00	00	C1	8F	00	00	2A	9C	00	00	C2	A7	<fá*œâ§< td=""></fá*œâ§<>
00000160	00	00	AB	06	00	00	E3	07	00	00	21	08	00	00	F7	80	«ã!÷.
00000170	00	00	59	A0	00	00	4D	0A	00	00	Β4	0A	00	00	73	09	YM´s.
00000180	00	00	CD	07	00	00	02	0B	00	00	6D	0B	00	00	83	0B	Ímf.
00000190	00	00	42	0C	00	00	85	0C	00	00	69	0C	00	00	98	0B	Bi~.
000001A0	00	00	39	09	00	00	00	77	01	00	E8	03	00	00	00	77	9w
000001B0	01	00	E8	03	00	00	63	38	3A	30	61	3A	61	39	3A	62	ec8:0a:a9:b
00000100	31	3A	34	35	3A	32	65	00	00	00	00	20	00	33	20	00	1.15 26
00000100	00	28	00	99	28	00	00	28	00	11	20	28	00	00	28	33	1
000001E0	55	20	00	55	20	99	55	20	00	55	20	00	55	CC TT	00	80	.+1.+".+1.+y.0 US UF UPM UT UU E
00000200	00	00	80	33	00	80	66	00	80	99	00	80	CC	00	80	77	€3.€f.€™.€Ì.€♡
00000210	00	AA	00	00	AA	33	00	AA	66	00	AA	99	00	AA	cc	00	.aa3.af.am.at.
00000220	AA	FF	00	D5	00	00	D5	33	00	D5	66	00	D5	99	00	D5	°ÿ.ÕÕ3.Õf.Õ™.Õ
00000230	СС	00	D5	FF	00	FF	00	00	FF	33	00	FF	66	00	FF	99	Ì.Õÿ.ÿÿ3.ÿf.ÿ™

Figure 7.28: Edited Image in .tif Format in Hex Editor

Conclusions

8.1 Current Status

The plug-in has been developed which embeds the computer's MAC address into the image(which is edited on that computer using GIMP) by editing the image's Exif data and result can be seen by fetching the Exif data of that image with command **exiftool.exe filename.fileformat** or by opening the image in any hex editor.

8.2 Future Work

Currently, the plug-in only embeds the MAC address of computer on which the image has been lastly modified. The project can be extended to modify the plug-in code in such a manner that the image can be made to contain the series of all the MAC addresses of the computers on which it has been modified.

Paper Published

Paper Published in: SAPIENCE'14 International Conference on Security and Authentication on 27-28th March, 2014 organized jointly by the department of Computer Applications, Sree Narayana Gurukulam College of Engineering (SNGCE) and School of Computer Science, Mahatma Gandhi University (MG University), Kerala.

Paper Title: A Novel Approach to Find the Artifacts of GodMode

Paper Authors: Ms. Khyati Thakkar, Ms. Twinkle Patel, Mr. Madhur Tewani, Mr. Kishan Varshney, Mr. Nilay Mistry and Dr M S Dahiya

Paper Abstract: Windows operating system (OS) is highly used by computer users across the globe. Windows OS is coming up with various secret tricks and tweaks to get into the administration control. "GodMode" is one of the hidden secret through which one can access the whole control panel administration though the user is either guest or standard user with limited privileges. By using GodMode, users can access any of the control panel settings from a single folder, which is a concept actually based upon NTFS virtual folder. Forensic Investigation of such hidden secret can give proper and supportive conclusion to the investigator, whether control panel settings opened directly or through the GodMode, also which user created the GodMode and controlled the system. This paper has some approaches given through which investigator can identify whether GodMode operations are done over the system to breach the privileges of administrator or not.

Bibliography

- [1] http://developer.gimp.org/git.html
- [2] http://developer.gimp.org/writing a plug in/1/index.html
- [3] http : //www.plagiarismtoday.com/2008/08/19/tineye protecting images preventing orphans/
- [4] http://www.linuxplanet.com/linuxplanet/tutorials/6720/1
- [5] http://www.linuxplanet.com/linuxplanet/tutorials/6720/2
- [6] http://www.python-forum.org/viewtopic.php?f = 6&t = 177
- [7] http://code.activestate.com/recipes/550811 jpg files redater by exif data/
- [8] http://www.endlesslycurious.com/2011/05/11/extracting-image-exif-data-with-python/
- [9] http://www.blog.pythonlibrary.org/2010/03/28/getting photo metadata exif using python/
- [10] http://stackoverflow.com/questions/159137/getting mac address
- [11] http://code.activestate.com/recipes/578277 get mac address of current interface in one line o/
- [12] http://code.google.com/p/pexif/
- [13] http://code.google.com/p/pexif/downloads/list
- [14] $http://en.wikipedia.org/wiki/Exchangeable_image_file_format$
- [15] http://www.exif.org/
- [16] http://www.ietf.org/rfc/rfc4122.txt

- [17] http://en.wikipedia.org/wiki/GIMP
- [18] http://www.sno.phy.queensu.ca/phil/exiftool/
- [19] https://raw.githubusercontent.com/akkana/gimp plugins/master/save export clean.py
- [20] http://docs.gimp.org/2.6/en/gimp-concepts-shortcuts.html
- [21] https://github.com/akkana/gimp plugins
- [22] http : //webcache.googleusercontent.com/search?q = cache : http : //blog.defron.org/2013/01/gimp script save as png.html
- [23] http://shallowsky.com/software/gimp save/
- [24] http://www.gimphelp.org/python_save_as_ipg.shtml
- [25] $http://www.gimphelp.org/DL/Python_scripts/save_as_jpg.py$