ABSTRACT

A social network is a simple social structure made up of different individuals who are related to each other through interdependencies such as relationship, friendship, and business contacts. Social networking plays a vital role in the modern day society. Social network is the place, where any one can maintain the relationship with any one irrespective of their location. What succeeds invites attraction, both good and evil. Given the popularity of these social networking websites, evil intentions of hackers online must be monitored and addressed thoroughly. Risks of social networking include unauthorized account access and spread of malware. Recent incidents reveal the spread of crime through social networks and we have come across reports where cops have identified suspects using Facebook. The context of security in current global world is significant. The outline of the project is detecting the ways to find the evidence against; who ever use the social networks in unlawful ways. In this project the main focus is on the current popular social networks like Facebook, Orkut and Twitter. Examining the different locations on computer to find the evidence is the main task of this project.

TABLE OF CONTENTS
1. Background and Rationale

1.1 Introduction

1.2 Social Networks

1.3 Types of Social Networking

1.3.1 Facebook

1.3.2 MySpace

1.3.3 Twitter

1.3.4 Orkut

2. Narrative

2.1 Different types of security analysis

2.1.1 Personal Information Shared

2.1.2 Identity Theft

2.1.3 Applications on Social Network

2.2 Possible Attacks on Social Networks

2.2.1 Attacking Techniques
3. Testing and Evaluation

3.1 Forensics Tools used

3.1.1 FTK

3.1.2 EnCase

3.1.3 ProDiscover

3.2 Methodology

4. Experimentation

5. Results

5.1 Analysis and Results

6. Conclusion and Future Work

BIBLIOGRAPHY AND REFERENCES
LIST OF TABLES

Table 4-1 Test cases and respective expected results………………………………………43

Table 5-1 Test cases and results……………………………………………………………61
LIST OF FIGURES

Figure 1.1 Pictorial Representation of Networks ......................................................... 4
Figure 1.2 Face book Homepage ............................................................................. 7
Figure 1.3 Face book Applications ....................................................................... 8
Figure 1.4 Face book Security Features ................................................................. 9
Figure 1.5 Twitter Homepage .............................................................................. 16
Figure 1.6 Twitter after logging in ....................................................................... 18
Figure 1.7 Orkut User Traffic ............................................................................. 20
Figure 1.8 Orkut Home page .............................................................................. 22
Figure 1.9 Orkut features .................................................................................... 22
Figure 1.10 Orkut Applications page ................................................................. 23
Figure 4.1 FTK imager startup ............................................................................ 36
Figure 4.2 Adding the physical drive in FTK imager to acquire ....................... 37
Figure 4.3 Selecting the drive K, which contains evidence files ....................... 38
Figure 4.4 Selecting Raw Format to acquire image .............................................. 39
Figure 4.5 Selecting the destination to store the image ........................................ 40
Figure 4.6 Creating disk image ........................................................................... 41
Figure 4.7 Image verification .............................................................................. 42
Figure 5.1 AccessData FTK tool interface ......................................................... 45
Figure 5.2 Starting new case to analyze hard disk .............................................. 46
Figure 5.3 Case Log Options ............................................................................. 47
Figure 5.4 Evidence Processing Options ......................................................... 48
Figure 5.5 Filtering the evidence.................................................................49
Figure 5.6 Adding acquired image to analyze...........................................50
Figure 5.7 Completion of new case setup..................................................51
Figure 5.8 Processing Files.......................................................................52
Figure 5.9 Files retrieved...........................................................................53
Figure 5.10 Filtered files and documents selected.................................54
Figure 5.11 Bad extension files.................................................................55
Figure 5.12 File trying to launch...............................................................56
Figure 5.13 File trying to load into computer............................................57
Figure 5.14 Setup log file.........................................................................58
Figure 5.15 Phishing site trying to steal user credentials.......................60
1. BACKGROUND AND RATIONALE

1.1 Introduction

Rapid Growth in the dot com world has given a different form for communication over the computers for the past few years. Apart from email, this form of communications allows different users to share their information to the desired people all around the word through a common medium. The common example for such a medium is Social Networking, which is a web-based application used for incorporating different kinds of communities for people who share a common interest or activities. The basic types of services that are provided by the social networks are communities, friends list, testimonial, and the user’s profile. Even chat sessions and number of applications are available today. Significant number of applications is developed in gaming field given the interest all around in game development.

As there is a brisk growth of users using this social networking, the major issue that comes into play is security. The security issues that primarily considered are password protection, protection for the user private data and the privacy of the user. These security issues are not only the primary concerns of the users and the owners of the social networking, but also provide the wide scope to hackers if these security issues are not properly taken care of.

Apart from the common security issues, the main concern is the database of a particular social network, this has to be dealt with utmost care and some definite rules are to be framed in order to protect the privacy of the users, as this is the primary goal of the hackers to break into it where they can acquire lots of data and information.
The exponential growth in using the social networks can be seen in past few years. “Social networking has become a fundamental part of global online experience,” – John Burbank, CEO of Nielsen Online (Nielsen wire). As the social networks are becoming a part of personal lives, what about the security features? Only very few people who are in proficient in using the computers know about the attacks on this kind of web based social networks. But the people who are not aware of the computer security are the victims of the cyber attacks in loosing their private data. Apart from this, there are categories of people who are pretty much familiar with web accessing who are misusing the social networks in unlawful ways. Even there is scope for accessing others profiles by using their own methods. The focus of the project is to collect the evidence against such guys who involve in illegal activities. The project starts with analyzing the popular social networks available on Internet, their working mechanisms, and the applications that supported on the social networks. Different possible attacks are analyzed before collecting the evidence. The evidence is collected with the help of forensic tools like FTK, EnCase and Pro Discover. The process involves disk imaging and analysis of different files related to the browser perspective to the social networks on web.

1.2 Social Networks

A social network according to computer terminology is a social structure which is made of different individuals or organizations called nodes, where these nodes are connected by one or many but specific types of interdependencies. This interdependency may be any kind of relation such as a friendship, love, likes and dislike, regional relationship, prestige or knowledge [Jan Nagy 2009].
A social network uses network theory about nodes and ties to view the social relationships. A node in the network represents the individual actor, and ties represent the relationship between the nodes. There can be any kind of relationship between two nodes and also any number of relationships between them.

“Research in a number of academic fields has shown that social networks operate on many levels, from families up to the level of nations, and play a critical role in determining the way problems are solved, organizations are run, and the degree to which individuals succeed in achieving their goals”[Wiki 2009].
Figure 1.1 Pictorial Representations of Networks [Wiki].

Figure 1.1 gives the pictorial representation of Social Networks, in which the dots indicates individual nodes connected by blue lines are ties between nodes; ties indicates the communication between nodes. In social Networks nodes represent the individual actors and ties represent relationship between actors.
1.3 Different types of Social Networks

In the modern digital era of life, the distance between the people flooded by the different kind social networks available on the web world. These social networks are the scope to exchange ideas as well as data. Keeping in mind of the growing illegal activities through social networks, this project is a study and analysis of three such social networks Facebook, Orkut, and Twitter. The data that resides on the computer from where the social networks being used plays major role in forensic investigation [Mitchel, J. (nd)].

1.3.1 Facebook

Facebook is global social networking website that is operated and privately owned by Facebook, Inc. Facebook provides user with variety of options to maintain the contacts with friends loved ones and even with different people in the society. The options include adding friends sending public and private messages to friends, updating profile. In addition to this, users can part of different communities on the web through Facebook, like the city, workplace, school and regional communities. The Website's name stems from the colloquial name of books given at the start of the academic year by university administrations with the intention of helping students get to know each other better.

Mark Zuckerberg founded Facebook with his college roommates and fellow computer science students Eduardo Saverin, Dustin Moskovitz and Chris Hughes while he was a student at Harvard University. The Website's membership was initially limited to Harvard students, but was expanded to other colleges in the Boston area, the Ivy League, and Stanford University. It later expanded further to include any university
student, then high school students, and, finally, to anyone aged 13 and over. The Website currently has more than 300 million active users worldwide [Wiki 2009].

1.3.1.1 Platform and Applications

Although Facebook had very limited number of applications when it was first introduced, over a period of time span it has developed and launched many number of applications making the usage of the website more convenient and much more advanced for the users. The most popular applications that the Facebook toady has are as follows:

- Photos through this application the users can upload albums and photos, and status message, this application allows users to inform their friends of their whereabouts and actions. A user's Wall through this application it is visible to anyone who is able to see that user's profile, depending on privacy settings. In July 2007, Facebook began allowing users to post attachments to the Wall, whereas the Wall was previously limited to textual content only.

- Tag this application is used to label users in a photo. For example, if a photo contains a user's friend, then the user can tag the friend in the photo. This sends a notification to the friend that they have been tagged, and provides them a link to see the photo.

- Facebook released a Comet-based instant messaging application called "Chat" to several networks, which allows users to communicate with friends and is similar in functionality to desktop-based instant messengers.

- Facebook launched Gifts application on February 8, 2007, which allows users to send virtual gifts to their friends that appear on the recipient's profile. On July 20, 2008, Facebook introduced "Facebook Beta", a significant redesign of its user interface on
selected networks. The Mini-Feed and Wall were consolidated, profiles were separated into tabbed sections, and an effort was made to create a "cleaner" look. After initially giving users a choice to switch, Facebook began migrating all users to the new version beginning September, 2008. These are the some of the famous applications that are used in the Facebook, which made Facebook one of the leading social networks website in the dot com world [Facebook 2009].

Figure 1.2 Facebook Home Page.

Figure 1.2 is a pictorial representation of the Facebook home page, which consists of login Colum for the existing user to enter the users account and a signup Colum for the new user who is interested in creating a user account. The sign up Colum has five
different sections asking the user to enter the full name of the user, any existing email address, and password for the account, gender of the user and the date of birth of the user.

Figure 1.3 Facebook Applications.

Figure 1.3 is a pictorial representation of the applications in Facebook. This figure shows many applications and features available in Facebook. This figure shows applications like the friend’s list, requests, suggestions, Highlights and news feed.

Figure 1.4 shows the different security options available on Facebook. User can alter his/her settings according his/her preference. Examples for this kind of security feature are changing the password, changing the associated E-mail address with Facebook, and etc.
In January 2009 Facebook was ranked second most used social network worldwide after MySpace by compete.com [Facebook 2009].

**Privacy Settings:**

*Friend Lists:* Facebook provides an option to organize user’s friend list. User can create a group of friends according to category they belongs, like family, friends, school, organization, community, region and etc. Each group can be assigned with some privacy policies; as an example user may wants to give access to his photo album to only friends. One friend can be in two groups.

*Hide from search results:* Under Facebook privacy settings there is an option to users to hide their own profile from unwanted people to visit their profile. Even user can control his/ her visibility on search engines like Google, Yahoo and etc.
Tags on photos and videos: User can protect his/her name from tagging in photos or videos shared by others. There are four options provided by Facebook: Friends of Friends, Only Friends, Some Friends and Only Me, are the options can be used by Facebook user to allow people to tag his/her profile to shared photos or videos.

Wall Posts Privacy: User can customize his/her wall posts. User can avoid unnecessary wall posts on their wall. User has the possibility to restrict people from writing something on their wall, can hide unnecessary wall posts or News Feeds on his/her wall. User can avoid showing up his/her private stories on Friend’s News Feeds.

Contact Information Privacy: Users can set their contact information visibility; even they can hide their friend’s information visibility through their profile [Nick O’Neill].

Security Attacks:

Most Hilarious Video Attack:
One of the recent attacks that attract Facebook users to access a video tagged as most hilarious video ever on Facebook, and title of the video may vary. When clicked on the video link, it directs the user to a fake Facebook login page. With this, the attacker can steal the user’s login information. After sign-in process, then browser jumps to original Facebook and prompts to download HD media player. After this everything depends on location of the user. For example, if the user is from United States then it prompts to download HLV player to play this video, if the user is from United Kingdom it forces the user to take IQ quiz and redirects the user to a page containing win an iPad offer and forces the user to fill the details like address and phone number.
All this information will reach the attackers as soon as users hit the register button on the page win an iPad offer [websense].

Like Jacking:

Clickkacking or Likejacking is an attack that tricks the user to post a message to their own page saying that they like a malicious link. This worm attracts the users with messages like: “LOL This girl gets OWNED after a POLICE OFFICE reads her STATUS MESSAGE, The Prom Dress That Got This Girl Suspended From School”. When the user clicks on messages like this, this worm redirects the user to a blank page having message click here to continue. If the users click anywhere on the page, a message will be posted on the user’s newsfeed page saying that the user like that malicious link, it is shared among the friends of the user there by it spreads all over [Elinor Mills] [sophos].

One of Phishing Attack:

This attacks spreads as emails with different subjects like “Richard sent you a private message Subject: Hello check 121.im” and the link is redirected to Facebook like page which is actually a fake Facebook site prompting user to login. If the user enters is login details, they will be directed to the attacker [Aurellja].

Phishing Page with Exploits:

Looks like normal phishing techniques; phising page contains web exploit tool kit. This tool kit, depending up on the user browser delivers variety of exploits on to the user browser. For example, if Firefox is used then Web exploit tool kit forces Trojan
named TROJ_PIDEF.PAL .PDF format, which allows Trojan owner to run any malware function on victim’s computer. If any failure occurs in exploit, still the user safety is not ensured. The phishing page prompts the user to download updatetool.exe file. This executable drops the files into folder with hidden properties, passes unnoticed by users. This file alters registry entries, to load on system startup. Once they sit on operating system they start communicating with attacker’s computer through an accessing website. The injected file contains information such as where to download the updates for itself, website to monitor, credentials to steal and the address that the stolen information to sent. This malware waits until the user accesses the websites that were listed in it and steals the information that accessed through those sites [Web Threat Spotlight].

**Worm Based Virus:**

In this kind of attack a worm spreads as message on user’s accounts containing alluring link like ”LOL. You, have been caught on hidden camera”. This link redirects the user to YouTube like page and forces user to install certain flash player. When user tries to install flash player, a malware function installation will be started. The vicious side of the worm is that it captures the profile picture of infected user and adds it the linked website containing the worm. There by it looks like genuine for the next probable victim [Michael Arrington].

**Bredolab Attcak:**

This attack forces Facebook user download malicious executables on to their computers by sending a false message. The false message seems to receive from
Facebook support team. The message contains a .zip enclosed executable file, which on click downloads more malicious executables and joins the computer in Bredolab botnet. With Bredolab botnet gains the full access to the victim’s computer. The malicious executables just downloaded turns off the local firewall and runs identity related thefts [Ryan Naraine].

1.3.2 MySpace

MySpace is one of the leading social networking websites. Its headquarters are in Beverly Hills, California, USA, where it shares an office building with its immediate owner, Fox Interactive Media, which is owned by News Corporation. MySpace became the most popular social networking site in the United States in June 2006. The very first MySpace users were eUniverse employees. The company held contests to see who could sign-up the most users. The company then used its resources to push MySpace to the masses. eUniverse used its 20 million users and e-mail subscribers to quickly breathe life into MySpace, and move it to the head of the pack of social networking Websites. A key architect was tech expert Toan Nguyen who helped stabilize MySpace platform when Brad Greenspan asked him to join the team. Throughout the course of 2007 and 2008, MySpace redesigned many of the features of its site in both layout and in function. One of the first functions to be redesigned was the user home page, with features such as status updates, applications, and subscriptions being added in order to compete with Facebook. In 2008, MySpace homepage was redesigned. MySpace Music was recreated in fall of 2008 along with an updated version of MySpace profile [My Space 2009].
1.3.2.1 Platform and Applications

The applications that are provided by the MySpace are as follows:

- Bulletins are posts that are posted on to a "bulletin board" for everyone on a MySpace user's friend’s list to see. Bulletins are deleted after ten days.

- MySpace has a Groups feature, which allows a group of users to share a common page and message board. Groups can be created by anybody, and the moderator of the group can choose for anyone to join, or to approve or deny requests to join. In early 2006, MySpace introduced MySpace IM, an instant messenger that uses one's MySpace account as a screen name. MySpace user logs in to the client using the same e-mail associated with his or her MySpace account. Unlike other parts of MySpace, MySpace IM is stand-alone software for Microsoft Windows. Users who use MySpace IM get instant notification of new MySpace messages, friend requests, and comments.

- MySpace TV In early 2007, MySpace introduced MySpace TV, a service similar to the YouTube video sharing website. MySpace TV is now in beta mode, and will probably be launched as a separate site in either 2008 or early 2009. MySpace TV might be a standard channel that will be shown on television. The above mention is the some of the important applications that are used in Myspace Website users [MySpace 2009].

Privacy Settings:
Profile privacy setting: The default setting on profile privacy allows any MySpace user; this is applicable for any user over age 18 and above. User can control who can visit his/her profile by changing the setting to “Only my friends”, which is default to the users having the age under 18. Users who are above age 18 can control visibility of photo albums, videos and blogs. User can make play lists and events available to anyone [Myspace].

Security Attacks:

Koobface Attack:

This attack was detected by Kaspersky lab. Kaspersky detected two variants of attacks, in which one variant attacked Facebook and other attacked MySpace. Worm.Win32.Koobface.a attacked Myspace. This attack downloads a malicious code into MySpace account, which transform infected computer of a user into zombie computers, which forms a botnet. This worm creates a spam message, and sends it to the users in the friend list. Generally this message attracts the users with alluring video links. When user tries to access the video, it again prompts the user to install or update the flash player, with an executable file named “codecsetup.exe”. This malicious file downloads more malicious files, leads to identity theft [Kaspersky labs].

Image Attack:

The attacker makes a transparent cover image over MySpace website and forces user to click any where on the image. This single click redirect the user to a
MySpace like fake page, prompts user to login into their MySpace account. This fake link transports the user login information to the attacker. [Security Focus]

1.3.3 Twitter

Twitter is the one of the most comely used social networking service and it also falls under the micro logging service, that was developed and maintained by Twitter inc. According to the recent survey about 65 million tweets are posted each day, which is equivalent to about 750 tweets sent each second. The basic mechanism in this social networking site is to send and view the messages posted by different users, these messages in this networking site are known as tweets. The maximum length allowed to be entered and posted on a single tweet is 140 characters and the format is the text based and these messages are displayed on the account owner’s page.

Figure 1.5 Twitter homepage
Figure 1.5 shows how a Twitter home page looks like. It has the options like signup and sign in. It even provides the search bar to find people on Twitter.

### 1.3.3.1 Platform and Applications

Security is one of the prime concerns of the Twitter; Twitter collects the personnel data entered by the user of the account and gives them to the third party for its usage. One of the most important things that are Twitter does not encourage any kind of advertisements directly. The only way you can advertise is through sending tweets. Twitter faced serious security vulnerability in the year of September 2007 where user update can be made by other user and this vulnerability was later found to be SMS spoofing. Using this spoofing attack the attacker can retrieve the phone number of the user that is associated with the account; this was then resolved by issuing a personal identification number to access the account through SMS making it more secure. Before this vulnerability was discovered, another security issue was identified in 2005. This attack was to crack the administrator accounts passwords through the dictionary attack and pass all the illegal issues like the drugs and sexual information through these accounts that are cracked. This problem was fixed by introducing the verified accounts, through which all the celebrities and well-known people are asked to reveal their existing twitter account names. The other bug, which came in to light after these two attacks, was very important; it made the users to follow a different account without the user’s knowledge. This problem was then taken seriously and FTC has taken several steps to provide the security to the user’s information [Twitter].
1.6 Twitter after logging in

After singing into Twitter the wall page shows the tweets posted by the people the user follows. In figure 1.6 it clearly shows the tweets on the wall. Related links can be seen to the right corner of the screen.

Privacy Settings:

On twitter, user tweets will be displayed publicly if not the setting is done: protect my updates. Up on setting up protect my updates twitter stops publishing the user update information publicly; with this setting updates from the user only shared by the people, only who approved by the user [Ofzen and computing].
Security Attacks:

Denial of Service Attack:

On August 6, 2009 twitter website was shut down for 4 hours by the attack named Denial of Service (DoS). With this attack the hacker created a worm and sent it on network. This worm consumed the bandwidth that is designated for Twitter and few other social networks. In this attack some unnecessary information in huge volumes sent out in network, which makes network busy and causing DoS. “Cyxymu” is the user name from the account, which the DoS attack has been carried out. From the account Cyxymu in the form tweets the worm spread rapidly over the Twitter network there by causing huge network traffic. McAfee found that the hackers are using search engine optimization techniques to attract the people to access malicious websites. Such a method is used spreading the DoS attack [Miko] [Niko Nergaze] [Brian Prince].

Worm Infects Twitter:

In 2009 four serial attacks have been carried out. A worm, which was spread, attacked the Twitter by four different attacks in series of steps each time increasing the intensity of worm in spreading and stealing the personal information from Twitter accounts. This worm automatically updates the user information and statuses of users on Twitter website. This virus spread in to Twitter by using cross-scripting vulnerability concept [Stefanie Hoffman].

Phishing Attack:
The recent phishing attack on Twitter used torrents as medium to gain access to the Twitter user accounts. Innocent users who are looking for information in forums are the victims of this torrent-based attack. Attackers create some torrent links, which redirects the user to Twitter like page and prompts to enter login details. There by the attackers gains the access to user’s Twitter account [Stan Schroeder].

1.3.4 Orkut

On January 24th 2004 Google launched a revolutionary free-access social network called Orkut, to help the people in maintaining relationships with friends and loved ones. Orkut is named after Google employee Orkut Büyükkökten, who is the founder of Orkut. It provides the user with adding new friends and communities to his/her profile. Along with this feature Orkut also provides the user with additional space to upload photos and videos to their profiles.

![Traffic of Orkut on May 13, 2009](image)

Figure 1.7 Orkut User Traffic. [Wiki-Orkut]
Figure 1.7 shows the statistics of Orkut User Traffic in different countries. Even though in United States Facebook and MySpace are the most visited websites than the Orkut, India and Brazil have significant number of users. Statistics shows that 50% of the Orkut users are from Brazil followed by India with 15% dated May 13th 2009 [Wiki 2009].

1.3.4.1 Platform and Applications

A user first creates a "Profile", in which the user provides "Social", "Professional" and "Personal" details. Users can upload photos into their Orkut profile with a caption. Users can also add videos to their profile from either YouTube or Google Video with the additional option of creating either restricted or unrestricted polls for polling a community of users. There is an option to integrate GTalk (An instant messenger from Google) with Orkut enabling chatting and file sharing. Currently GTalk has been integrated in Orkut - users can directly chat from their Orkut page. The new features in Orkut are Themes. Users can change their interface from a wide range of colorful theme library. Themes are currently only available in India and Brazil. Members can make groups to join friends according to their wishes. Further, each member can become fans of any of the friends in their list and can also evaluate whether their friend is "Trustworthy", "Cool", "Sexy" on a scale of 1 to 3 (marked by icons) and is aggregated in terms of a percentage. Orkut allows anyone to visit anyone's profile, unless a potential visitor is on "Ignore List". Importantly, each member can also customize their profile preferences and can restrict information that appears on their profile from their friends and/or others. Another feature is that any member can add any other member on Orkut to his/her "Crush List" and both of them
will be informed only when both parties have added each other to their "Crush List" [Orkut 2009].

![Orkut Home Page](image1)

**Figure 1.8 Orkut Home Page.**

![Orkut features](image2)

**Figure 1.9 Orkut features.**

Figure 1.8 shows the Orkut home page, which has options for sign in, and signup. Figure 1.9 is a pictorial representation of the applications in Orkut. This figure shows many applications and features available in Orkut. This figure shows applications like the friends list, requests, suggestions, my communities and apps.
Figure 1.10 Orkut Applications Page.

Figure 1.10 is a pictorial representation of the applications in Orkut. This figure shows many applications and features available in Orkut. This figure shows applications like the ask friends, stylish fonts and scraps, photos and add apps tab.

**Privacy Settings:**

Orkut provides the privacy settings in four categories, my updates, profile visitors, allow scraps to be written by, and allow content viewed by. My updates: with this option user can has choice to share his/her updates on photos, videos, testimonials and profile changes with their friends. Profile visitors: User can choose option get notifications on his/her profile when visited by friends or anyone, and can stop the notifications sent, when user visits others profile. Allow scraps to be viewed: Orkut user can have control over who can visit his/her scraps. Allow content to be viewed: Orkut user can restrict the others from viewing personal information of that user, like photo albums, videos and testimonials [teck in]. Recently Orkut added a new feature called private scraps; with this feature the scrap from a sender is visible to user and sender only [Doree].
Security Attacks:

XSS:

XSS is a message-based attack, in which Orkut users receives the messages from their friends, the message consists malicious code in it. Even if the user tries to read the scraps from account the malicious code starts its action. It works based on cross site scripting, and executes the malicious code, which in turn steals Orkut users credentials, cookies, redirects them to a fake page, and automatically installs key loggers and viruses on the victim computer [Vikas].

Spam phishing attack:

This attack starts from “Updates from my Friends” section. Spam messages will be posted as message update from friend of that user. A typical spam message will be a link like “CHECK my nude pictures”, which redirects the user to website “hxpx://orkut2010new.blogspot.com”. This page looks very similar to Orkut login page, which prompts the user to enter login information. This redirected page will send the user credentials to the attacker [Satyendra Kumar].

Spoofed Email Attack:

With this attack spam emails will be sent to Orkut users. Summary of the email will be like this, the user being investigated and will be terminated with in 72 hours. If the user wants to stay connected with Orkut click the link below. When the user clicks the link malicious code will be executed on the victim’s computer. This Trojan downloaded called “regulamento_orcut.exe”. This Trojan downloads other malicious
file named “fax.exe”. This malicious file automatically duplicates itself on different location of the victim computer with different names. This file starts up along with the operating system in the victim’s computer, and monitor user activity on browser to steal users credentials [Aurellja 2008].
2. NARRATIVE

This project analyses possibilities of misusing social network sites due to irresponsible behavior of users. Recent surveys show that problems in social networks are more often to occur, due to the fact that openness is one of the key features of these sites. Social engineering can be misused by attackers concerning social network with the purpose of gaining sensitive information. There is a conflict between users ‘security awareness and their actual behavior’, so called privacy paradox. This project is interested in the amount of information that can be retrieved from the hard drive when an illegal activity took place. There might be sensitive information stored on hard drive that could be useful as evidence in case. Hard drive of a computer is analyzed through a series of steps to estimate security vulnerabilities of social network.

The first step of the project is taking the clean disk image. Then the designed test cases are deployed on that computer. In this project, four different operating systems are used, in that one operating system is chosen to perform the search operation when there is a lot of information hard drive. For analyzing the hard drive, this project uses three forensic tools: FTK, EnCase and ProDiscover. FTK and EnCase are used to capture the disk image explained in the next sections Forensic Tools Used. This section explains more about security analysis and possible attacks on social networks.

2.1 Social Networks and Security Analysis

2.1.1 Personal Information Shared

Social networks provide space for users to update their personal information on web. Personal information can be updated on web in two modes: private and
public. Due to limiting preferences in private information, most users expose their personal data on web that forces them to be easily attacked. Personal information on social networks may reveal more information about that particular user from different websites [R. Gross and A.Acquisti]. Most teenagers on social networks reveal their personal information to their friends on the web. Power full search options available breaking the barriers to reach any one web, and technology improvements are threats to digital security wall. The technology advancements are becoming the roots to the loss of private information [Jan Nagy and Peter Petcho].

2.1.2 Identity Theft

Identity theft is a big challenge to any social network user. The traces of personal information like name, date of birth, location etc in the hands of hackers or attackers leads to this issue. Identity theft is nothing but stealing the personal information like social security number name and other credentials and pretend like other user. Social networks are prone to this kind of attacks. Phishing, Spyware are the example ways to do identity theft. It is easier list the user details by knowing their name and location. Even first three digits of social security number reveal information like where it was generated and the physical location of the user [R. Gross and A.Acquisti]. With all these details any one makes a clone to the other account and may misuse the account.

2.1.3 Applications on Social Networks

There is exponential growth in number of users of social networks in last 5 years. What made an impact on such growth? The answer for the question is simply the competition. iPhone proved as top most in mobile sector because of its extensive
application list. Apple and Facebook have realized the importance of third party applications and took step towards accepting third party applications on their platforms. From there, it spread to all other social networks. In early days of third party applications, they needed an authentication process to get approved and that became cumbersome to website maintainers. As this information is made public, key concerns about security issue have been raised. Of the available Application Programming Interfaces (API), APIs are divided into two groups public and private. With the public APIs does not support much to authentication and security where as private APIs made to work with the authentication process. Private APIs requires high level data accessing so they made an agreement process with users to share their information. Recently, many social networking vendors concentrated on security and enforcing security protocols in developing the applications [Marc Grosz et all].

2.2 Possible Attacks on Social Networks

In the year 2005, a very dangerous attack on MySpace is noticed named as Sammy attack. Sammy attack spread over MySpace very fast by using the loopholes in the named social network. Even though Sammy attack did not extract the personal information on the social network, it seriously effected the functioning of the social network. In 2009, now popular social network Twitter effected with attack Mikeyy. Twitter was attacked by Mikeyy and altered personal profiles in Twitter. In the same year another vulnerability was discovered, namely Koobface. It first attacked Facebook and then spread to other social networks.
Attackers are now capable of extracting more information such as commercial and corporation secrets along with personal information through social networks using the worms they designed [Chengyu Fan]. In the survey reports from Sopho shows that 62.8 percent of employees revealed their personal information on social networks [Sophos]. Cyber criminals are using the social networks efficiently for illegal earnings by using malware and spam applications. Over 40,000 malicious files have been collected by Kaspersky Lab in the year of 2008 [Gostev].

2.2.1 General Attacking Techniques

Spam: Earlier spam spread by using email, which spreads through social networks. Spam damages the network by residing at the computer. Spam mainly spreads through advertisements with help of friend list on the social network.

Third party applications: Flaws and security features in the third party applications are the major areas through which attackers can get access to the social networks. As number of applications increases, more number of flaws increase there by resulting in loss of data.

Worm: Worms will replicate themselves automatically by their self-replicate nature. Worms are specialized in stealing the personal information like password, bank account number etc.

XSS: Web page code is injected into the social networks, which steals COOKIE, takeover the account access and forces the user to download malware.

Plug-in: Some applications on social networks prompt user to install some plug-ins like flash and Silverlight. The flaws in the plug-ins are threat to personal information.
**Phishing:** In this attack, attacker pretends like a legitimate user and sends requests to the other users by using his own URLs, which gains access to others personal information on their acceptance to the request [Chengyu Fan].

**Viral Marketing:** Attackers makes use of weakness of users to receive advertisements from friends. The attackers make the marketing malware functions through attracting videos or advertisements. The only investment for the attackers is marketing the videos or advertisements [NisheethShrivastava].
3. TESTING AND EVALUATION

3.1 Forensic Tools Used

3.1.1 FTK

Forensic Toolkit (FTK) is a widely known computer forensics software tool used for ensuring relevant solutions. FTK generates images of the information to be saved. The tool analyzes the registry entries in the computer apart from shepherding investigation. File decryption is provided by FTK. Generating reports is not far from FTK as the tool is quite capable of doing this. The tool boasts of reconstructing passwords of over hundred applications. Users can access over two hundred unique file formats apart from creating auditing reports and case documents. FTK is adaptable to different available forensics solutions. Sophisticated search approaches are implemented by FTK to retrieve images, documents, and deleted documents. It can also obtain privileged information that has already been stored.

FTK is designed to acknowledge objectionable content using file filter concepts such as Known File Filter (KFF) that supposedly includes about forty five million hashes. FTK allows distributed processing which is very effective. The tool also includes very sophisticated analytic approaches such as RAM dump analysis, acknowledging objectionable content, effective search index and assists known cryptic approaches. Rich graphic interface supported by numerous features place FTK as a unique forensics analysis tool enabling crystal clear information reporting and multi-code assistance.
3.1.2 EnCase

Encase is a computer forensic tool that is used for analyzing the digital media and this product was introduced by Guidance Software. This software plays a vital role in finding and investigating criminal and network crime evidences. The law enforcement department for collecting digital forensic evidence also uses this software. This software includes different types of tools which are used for recovering different types of files and acquisition of data. Encase is undoubtedly one of the most important and well-known forensic software used in the market, this software is well known for verification of the evidences. Encase is most commonly used for making an image of the hard drive or any other digital media, as soon as the image is made the encase starts verification of the digital media whose image was made. One of the important feature of Encase is that it can be used in large organizations where the systems are connected in wide area network and can be used on any system in that network without disrupting any kind of operations. Snapshot is a special feature that comes with Encase, which enables the examiner to make snapshot of the key violent and binary date that is quickly available on different systems on the network. This software also has an important feature to analyze the data live without visible to the attacker.

3.1.3 ProDiscover

Another tool that looks at assisting security is ProDiscover. This tool makes a big impact for administrators or developers who use it. ProDiscover efficiently addresses incident response and provides e-discovery. This tool retrieves information by safeguarding evidence. ProDiscover provides search facility for the whole drive enabling smooth forensic analysis. Support for VMware software is provided as well in this tool. Preview of large document volume is offered.
ProDiscover independently creates, maintains cryptic approaches to establish data integrity feature. The tool dynamically provides the preview and searches the privileged region of hard drive apart from retrieving lost files and scrutinizes old files.

3.2 Methodology

The main aim of the project is to find evidence in support to the case that involved social networks. The collection of evidence starts with analyzing the hard drive on which the social network has been used. The evidence related to the case can be identified by carefully looking into files that have been altered with the use of social networks. This information can be extracted with help of forensic tools like FTK, EnCase, ProDiscover and more tools available.

The steps followed in this project are:

Step 1: Clean hard Drive Image

A clean hard drive is taken, that just installed with the operating system. This project uses the hard drive with windows 7 operating system. In order to estimate the performance of the search operations in tools, the volume of files to be searched is increased significantly by installing three operating systems that share the file system. Given the large number of files in a single operating system installation, the combination of files in three operating systems meets our test criterion. The hard disk has been removed from the testing computer and connected to forensic workstation to capture the disk image. To capture the disk image, FTK and EnCase are used. Bit-to-bit copy format is used to guarantee no loss in evidence. To ensure data integrity, write-blocker has been used. Write-blocker prevents the alteration of information on the evidence disk by forensic workstation.
Step 2: Performing the test cases

Now the hard disk is connected to Internet, and different activities are performed on social networks. The social networks used for this project are Facebook, Orkut and Twitter.

The test cases as follows:

1) Chat session has been established on the specified social networks and continued for a while. Then chat history on the browser has been cleared.

2) Played with different third party applications like games, future cookies, business applications, health applications, quiz applications and more.

3) Advertisements and videos have been accessed.

4) Public and private messages have been exchanged and few of them were deleted.

5) New friend requests sent from the evidence computer and accepted few. Some of the friends from friend list have been deleted. Made the user join in few communities and withdrawn from few communities.

6) User profile has been updated.

7) Some of the applications added to favorites.

8) The pop up messages have been accessed, some plug-ins have been installed.

These test cases are performed, to check the information flow when any activity is performed. This project records the changes in the hard drive because of these activities. These test cases are deployed in two conditions: one when firewall is turned on and the second when the firewall is turned off.
Step 3: Imaging the Hard Drive

Now the hard drive has been connected to the forensic workstation for examination. The hard disk image has been captured with the help of the forensic tools FTK and EnCase.

Step 4: Examining the images

The two images before any activity and after deploying the test cases are examined by using the tool FTK.

Step 5: Reporting the changes

The difference between the contents in the two images have been examined, and logged. Initially the size of the contents in both images gives the picture of amount data that might exchange through social networks. The report includes different URLs accessed other than the social network URLs.
4. EXPERIMENTATION

Step 1: Acquiring Clean Hard Disk Image

![Figure 4.1 FTK imager startup](image)

Figure 4.1 shows the FTK imager interface. FTK imager is used to acquire hard disk image, as the first step in the project. A clean hard disk is taken and image is acquired. The hard disk image acquiring is shown in this section.
Figure 4.2 Adding the physical drive in FTK imager to acquire

Figure 4.2 shows image acquisition processing step, which involves selecting the drive to capture the image. In this project, the hard drive consists two logical drives, in which only one logical drive contains operating system files. This project analyses the changes made to system files when social networking websites are accessed. So, only the logical drive that contains operating system files is added as evidence drive. In figure 4.3, it is clearly visible that K drive is added as evidence drive. K drive contains all the system files, which needs to be investigated.
Figure 4.3 Selecting the drive K, which contains evidence files
Figure 4.4 Selecting Raw Format to acquire image

Important step in any forensic investigation is to avoid data loss. To make sure there is no loss in data the hard disk image formed by using bit-by-bit copy. Figure 4.4 shows the options available for selecting the image format in FTK imager tool. Raw (dd) is bit-by-bit format used in this project.
Figure 4.5 Selecting the destination to store the image

For further investigation, the image needs to be saved on the forensic investigating computer. Figure 4.5 shows selecting the destination to store the image on forensic workstation.
Figure 4.6 Creating disk image

Figure 4.6 shows progress in acquiring the hard disk image in “Raw” format.
After finishing the acquisition, image needs to be verified to ensure data integrity. To check the integrity, FTK imager computes hash value of the hard disk and the image. Drastic change in hash value can be seen, even with change of single bit. Figure 4.7 shows the verification result; found match in both computed and report hash values.
Step 2:

Table 4-1 Test cases and respective expected results

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Expected Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat session has been established and continued for a 5 minutes</td>
<td>Expected to retrieve the information exchanged and time of the chat session</td>
</tr>
<tr>
<td>Third party applications have been accessed.</td>
<td>Expected to view the concerned URLs and time frames</td>
</tr>
<tr>
<td>Advertisements and videos on social networks have been viewed; some flash players have been downloaded.</td>
<td>Expected to retrieve the links and installed files.</td>
</tr>
<tr>
<td>Public and private messages have been exchanged</td>
<td>Expected to retrieve the messages and the timings</td>
</tr>
<tr>
<td>Managing friends (adding, deleting and editing)</td>
<td>Expected to retrieve friend list and alterations to friend list</td>
</tr>
<tr>
<td>Community list management</td>
<td>Expected to retrieve community list</td>
</tr>
<tr>
<td>User profile has been updated</td>
<td>Expected to retrieve the modifications to the user profile and the time of modification</td>
</tr>
<tr>
<td>Some of the applications have been added to favorites and some applications have been removed from favorites list</td>
<td>Expected to retrieve the favorites list and modifications</td>
</tr>
</tbody>
</table>

Table 4-1 shows the test cases prepared. The table consists the test cases and the expected results in forensic perspective for each test case. When session established expected to retrieve the messages exchanged and the time when the chat session established, same expectation for public and private messages exchanged. When the third party applications, videos or advertisements accessed expected to retrieve the URL belongs and the time of access. When friend’s list, communication list,
application list and user profiles expected to retrieve the respective URLs and time of access.

**Step 3: Acquiring the image of hard disk after deploying the test cases**

Again FTK imager tool is used to acquire the image of the hard drive after deploying the test cases. Hard drive is connected to the forensic workstation using write blocker, to avoid the data contamination. The same procedure used as in the step 2 to acquire the image of hard drive.

Step 4 in the process shown in the next section Results.
5. RESULTS

Step 4: Examining Hard Disk Image

Figure 5.1 shows the AccessData FTK tool interface and startup page. AccessData FTK tool is used to analyze the hard disk and to retrieve the files from evidence image. The tools filters retrieve files based on their properties. FTK categorizes the files in to three columns, namely Evidence items, File status and File Category.
Figure 5.2 Starting new cases to analyze hard disk

Figure 5.2 shows setting up new case to analyze the evidence files stored by acquiring the hard drive image. FTK provides options to open new case, open existing case, preview evidence and go directly to working program.
FTK provides case log options to prepare the evidence report to submit in court. The case log options are case and evidence events, error messages, book marking events, searching events, Data carving/Internet searches and other events. Default setting is to include all options in the report. Figure 5.3 shows all options.
Figure 5.4 Evidence Processing Options

Figure 5.4 shows the operation list that the FTK tool to do along with retrieving evidence files. MD5 hash and SHA1 algorithms are included to check the integrity of the evidence. KFF files are not important as in most cases. Entropy test is used to determine whether the file’s data is compressed or encrypted. Such files contain no plain text and will not be indexed. Full Text Index is a powerful search engine, which enables investigator to do instantaneous searching of textual data. Data carving allows: automatically find specific
file types embedded in other files and from free space. Retrieve results using Data Carving Option on tools Menu.

![Refine Index - Default](image)

**Figure 5.5 Filtering the evidence**

In order to save time and resources, and/or to make searching more efficient, investigator may choose to exclude certain kinds of data from being indexed. Here, investigator can choose default settings that will apply to each evidence item that gets added to the case.
To exclude item from being indexed, investigator can make any changes to the settings.

Figure 5.5 shows the index options.

![Add Evidence to Case dialog box](image)

Figure 5.6 Adding acquired image to analyze

Any number of evidences can be added to the case. There are several types of evidence items. The main types of the evidence are acquired image of drive, local drive, folder and individual file. This project uses the acquired image to analyze the evidence. Figure 5.6 shows the add device options.
Figure 5.7 Completion of new case setup

Figure 5.7 shows the setup completion for the case. In the figure, it is clearly shown what are the options included in the case. Even though all this option may take additional time in retrieving the files but adds more information support the evidence.
Figure 5.8 Processing Files

Figure 5.8 shows the process of retrieving the files from the evidence image. In the process it shows that total files examined around are 2600, but the files added and indexed only 52. This index features filters out files that are unnecessary in the case. The log for the case is updated every 10 min. Current action can be seen in the figure “Reading data” and the item size that currently the FTK tool retrieving.
Figure 5.9 Files retrieved

Figure 5.9 shows the retrieved files using AccessData FTK. AccessData FTK retrieved all files from the image of the hard drive and categorized according the properties of the files. In total, around 4700 files recovered from the image. The left column shows the total number of evidence items added and examined, total file items present in the evidence image and total filtered in files. Middle column shows the files depending on their status, like bad extension files, deleted files, duplicate files and etc. Right column filters the files based on type of the file. Different types of files that are filtered by AccessData FTK are documents, spreadsheets, databases, archives, e-mails, graphics and etc. this makes searching process easy. The bottom pane shows the files up on filter
selection. Right pane shows the content of the file up on selection. FTK provides an option to export the files to the forensic workstation. In the bottom panel individual files will be shown with attributes file name, full path, extension, file type, category subject, create date, modified date and accessed date.

Figure 5.10 Filtered files and documents selected

File scessetup log tells the configuration of the system and user privileges. This file shows the users who logged in to the system and what time they accessed the computer, which plays supportive role in evidence report. This is clearly visible in the right panel in figure 5.10. The highlighted box shows that a user with administrative privileges login details. Downloaded log file shows the latest user login details.
Figure 5.11 Bad extension files

Figure 5.11 shows the files retrieved with bad extension. These files are loaded into the system when the advertisements and video files accessed. Files with .wpl extension are loaded into computer and automatically spread in different locations. The file extension and the file content are different in these files. By making use of bad extensions these files attacks the user to access them and upon clicking they run according to their original extension.
Figure 5.12 File trying to launch

Again some files with bad extension are automatically launched on computer and result in improper functioning of computer. This is observed while preparing the test cases and able to retrieve those malfunctioning application by using FTK. These files when retrieved try to launch automatically on investigating computer. The auto launch operation by the file is shown in figure 5.12. These files are downloaded when a flash player is installed on the testing computer during the test case process.
Figure 5.13 File trying to load into computer

In figure 5.13 we can see the file trying to load on to computer. This file entered into the testing computer with different file extension. When the bad extension file is accesses it asking for the permission to load into computer. These files came into testing computer with the help of cookies on social networking websites. Up on clicking this file stores onto the user computer and makes clones of it on different areas of the computer. These clones monitor the user activities and collect the user credentials and transports it to the attacker through the web media.
Figure 5.14 Setup log file

Figure 5.14 shows setup log file, which shows the different files that accessed the testing computer along with date and time. The log entries tell the information about the users and their activities. This log contains information about user activities, includes the access to the different files and time when accessed, changes made to the operating system files. Log even stores the user privileges, when log in takes place.

Some of the Cookies retrieved:

1) lv=Sun, 29 Aug 2010 02:03:50 GMT&mra=Sun, 29 Aug 2010 02:11:15 GMT

facebook.com/

2) lv=Sun, 29 Aug 2010 02:33:27 GMT&mra=Sun, 29 Aug 2010 02:50:48 GMT

twitter.com/

3) lv=Sun, 29 Aug 2010 02:05:37 GMT&mra=Sun, 29 Aug 2010 02:06:01 GMT

facebook.com/home.php?#!/profile.php?id=1756405671&ref=pymk
These are the some of the cookies that have been recovered and analyzed. The very first and second cookie log entry shows the timings the Facebook and Twitter access timings on the tested computer. The third cookie entry tells user activity, and that is a profile visit, and the timings shows when this event had occurred. The fourth entry shows TexasHoldem application access timings. Fifth one in the list is a recovered URL from cookies files gives the information about a fishing site that tried to steal the information from the Facebook user.
Figure 5.15: Phishing site trying to steal user credentials.

Figure 5.15 shows the interface of the phishing site, which looks like Facebook page, but the URL in browser URL pane is not original Facebook login page. This URL belongs to some unknown attacker. This URL upon user login credentials entry transports the user credentials to the attacker.
5.1 Analysis of Results

Table 5-1 Test cases and results

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Results using FTK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat session has been established and continued for a 5 minutes</td>
<td>Unable retrieve chat items</td>
</tr>
<tr>
<td>Third party applications have been accessed.</td>
<td>Able to retrieve the URLs for the applications and can be distinguished based on the time.</td>
</tr>
<tr>
<td>Advertisements and videos on social networks have been viewed; some flash players have been downloaded.</td>
<td>Able to retrieve URL information and timings</td>
</tr>
<tr>
<td>Public and private messages have been exchanged</td>
<td>Unable to retrieve the messages</td>
</tr>
<tr>
<td>Managing friends (adding, deleting and editing)</td>
<td>Unable to retrieve the friend’s list</td>
</tr>
<tr>
<td>Community list management</td>
<td>Unable to retrieve community list but able to see the URL belongs</td>
</tr>
<tr>
<td>User profile has been updated</td>
<td>Able to retrieve the concern URLs but not profile changes.</td>
</tr>
<tr>
<td>Some of the applications have been added to favorites and some applications have been removed from favorites list</td>
<td>Only the applications accessed URLs are retrieved but not the favorites list.</td>
</tr>
</tbody>
</table>

Table 5-1 shows the test cases and the obtained results. These test cases performed on a single computer. To record some of the attacks it took 3 months of time. This happened because the attacks won’t hit every time. Moreover some of the attacks passed unnoticed. Such a long time in waiting made difficult in performing the same test case for number of times. So this project tested the attacks only twice. But the hard disk analysis was carried
out 10 times, expected the same results, and ended up with expected results. Some of the URLs that are recovered mainly the spam URLs when tried point on browser after three days they have been expired. This shows that capturing the attacks is a tedious job. This project mainly focused on analyzing the hard drive and the changes happened to the content of the hard drive because of security attacks on Social Networking sites. This is a time taking process to check each and every file on the hard disk, to check for the modifications on the hard drive.
CONCLUSION AND FUTURE WORK

The project contributes significantly by analyzing security in popular social networks such as Facebook, Orkut and MySpace. FTK toolkit is used for security analysis in social networks and user activities are monitored. This project gives the detailed information about the security attacks happened recently, and generalizes the types of attacks on social networks. This project dealt with hard disk to give the primary evidence, based on the modifications carried out by security attacks on Social Networks. This report also shows different activities took place on the user computer while accessing the Social Networks. Cookie information was retrieved successfully listing time of url access by users. Malware activity is identified fruitfully. The evidence collected using FTK projects limits of FTK tool in analyzing the Social Network attacks. Major part of future work would include extending current idea using other forensics tools such as EnCase and ProDiscover. Accessing confidential data such as friends list and profile of friends in social networks would pave way for access to chat history, which has great potential to reveal critical information. Limitation of FTK tool in retrieving the chat session content and content of messages exchanged gives the scope to experimenting with some scripting tools like PHP, Javascript and etc.
BIBLIOGRAPHY AND REFERENCES


[Twitter] http://blog.twitter.com


