Sindhu. K. K, Shweta Tripathi, Dr.B.B. Meshram / IOSR Journal of Engineering (IOSRJEN)
www.iosrjen.org ISSN : 2250-3021
Vol. 2 Issue 2, Feb.2012, pp.214-221

Digital Forensic Investigation on File System And Database Tampering

Sindhu. K. K
Computer Engineering Department
Shah and Anchor Kutchhi Engg College
Mumbai, India

Shweta Tripathi
Computer Engineering Department
Fr. C. Rodrigues Institute of Technological,
Navi Mumbai, India

Dr.B.B. Meshram
Computer Engineering Department
Veeramata Jeejabhai Technological Institute,
Mumbai, India

***Abstract*:- Digital forensics is the identification, extraction, analysis and documentation of digital evidence from storage media. It is relatively new technology which is increasingly becoming important as the criminals aggressively expand the use of technology. Digital information is fragile and it can be easily modified or destroyed like File system and Database tampering. In the course of the investigation, the investigator should assure that digital evidences are not modified unauthorized and authenticate submission in the court of law. Our paper explains forensic investigation procedures using a WinHex tool[10]. Main focus of our paper is digital forensic investigation of different locations of windows file system and oracle database are explained. Evidence collection from hidden locations of windows file system and oracle 10g database will help the investigators in trustful and thorough investigation.**

Keywords Cybercrime, Digital forensic, File system forensic, Database Investigation.

I. Introduction

Computers are integral part of our life. A significant percentage of today's transactions and processes take place using Computer and Internet. People have readily adopted this technology and have innocently trusted it while performing many tasks, with ignorance about the limitations and threats to their securities. With this advance in technology, an equally advanced form of crimes has emerged. Different types of cyber attacks from various sources may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself. So the companies and products aim to take assistance of legal and computer Forensics. Digital forensics is the science of identifying, extracting, analyzing and presenting the digital evidence that has been stored in the digital devices. Various digital tools and techniques are being used to achieve this. Forensic tools and techniques are integral part of criminal investigations used to investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. This paper organized into two sections first section explains how a crime is investigating. Second section explains for collecting evidence from a file system and database. Digital Forensic Science covers Storage Media forensics, Network forensics, Firewall forensics, Device forensics, Database forensics, Mobile device forensics, Software forensics, live systems forensics etc. In this paper we explain Storage media Forensics and network forensics.

II. Cyber - Crime Investigation.

A. Investigation processes

The entire investigation process can be divided into four phases.

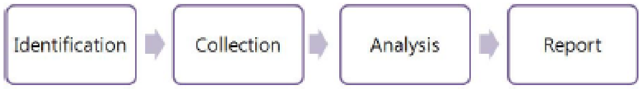

Fig 1 Shows Investigation processes

1. Identification: In this phase it collects the information of the compromised system. System Configuration, software loaded , User profiles etc
2. Collection Phase; Collects the evidence from the compromised system.
   Evidence is most commonly found in files and Databases that are stored on hard drives and storage devices and media. If file deleted, recovering data from the deleted files and also collects evidence file deleted files.
3. Analysis phase: Analyse the collecting data/files and finding out the actual evidence.
4. Report phase: The audience will be able to understand the evidence data which has been acquired from the evidence collection and analysis phases. The report generation phase records the evidence data found out by each analysis

component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody.

III. Storage media Forensics.

A. Basic Steps in storage media investigation.

1. Replication of forensic image: - Nonintrusive acquisition of a replicated image of data extracted from the questioned device.
2. For integrity perform Hash value calculation.
3. Conducting a file-fragment recovery procedure to recover files and folders to a new location.
4. Examine all files especially deleted files
5. Reviewing typical evidentiary objects such as:
   a. Analyse free spaces, slack spaces and bad sectors
   b. Application software file.
   c. Digital camera, printer and ancillary devices.
   d. E-mails, Games & Graphics images
   e. Internet chat logs & Network activity logs
   f. Recycle folders
   g. System and file date / time objects
   h. User-created directories, folders, and files
   i. Latent data extraction from page, temp, and registry space.
6. Copy the content of the evidentiary object into text files.
7. Searching for key-term strings.
8. Reviewing file notations.
9. Scrutinize applications or indications of as file eradications, file encryption, file compressors or file hiding utilities.
10. Preparing evidence summaries, exhibits, reports, and expert findings based on evidentiary extracts and investigative analysis.

B. Hidden data analysis in storage media

Suspects can hide their sensitive data in various areas of the file system such as Volume slack; file slack, bad clusters, deleted file spaces. [16]

Hard disk*:* The maintenance track / Protected Area on ATA disks are used to hide information. The evidence collection tools can copy the above contents.

File System Tables: A file allocation table in FAT and Master File Table in NTFS are used to keep track of files. These entries are manipulated to hide vital and sensitive information. [16]

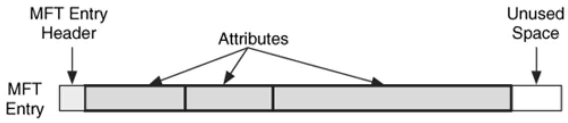

Figure 2 . MFT Structure.[16]

File Deletion: When a file is deleted, the record of the file is removed from the table, thereby making it appear that it does not exist anymore. The clusters used by the deleted file are marked as being free and can now be used to store other data. However, although the record is gone, the data may still reside in the clusters of the hard disk. That data we can recover by calculate starting and end of the file in Hex format and copy it into a text file and save with corresponding extension.

Recover a JPEG file

- Open file in the hex format
- Check the file signature
- Copy From starting signature upto ending signature.

For example (JPEG/JPG/JPE/JFIF file starting signature is FF D8 FF E1 XX XX 45 78 69 66 00 (EXIF in ascii Exchangeable image file format trailer is FF D9).
Open the file with corresponding application.

Partition Tables: Information about how partitions are set up on a machine is stored in a partition table, which is a part of the Master Boot Record (MBR). When the computer is booted, the partition table allows the computer to understand how the hard disk is organized and then passes this information to the operating system. When a partition is deleted, the entry in the partition table is removed, making the data inaccessible. However, even though the partition entry has been removed, the data still resides on the hard disk.

Slack space: A file system may not use an entire partition. The space after the end of the volume called *volume slack* that can be used to hide data. The space between Partitions is also vulnerable for hiding data. *file slack* space is another hidden storage. When a file does not end on a sector boundary, operating systems prior to Windows 95 a fill the rest of the sector with data from RAM, giving it the name *RAM slack.* When a file is deleted, its entry in the file system is updated to indicate its deleted status and the clusters that were previously allocated to storing are *unallocated* and can be reused to store a new file. However, the data are left on the disk and it is often possible to retrieve a file immediately after it has been deleted. The data will remain on the disk until a new file overwrites them however, if the new file does not take up the entire cluster, a portion of the old file might remain in the slack space. In this case, a portion of a file can be retrieved long after it has been deleted and partially overwritten.

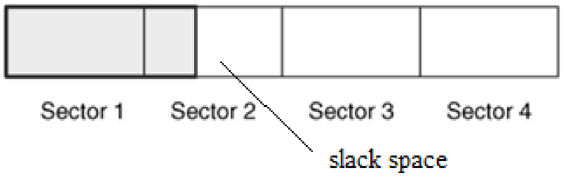

Figure 3. file slack [16]

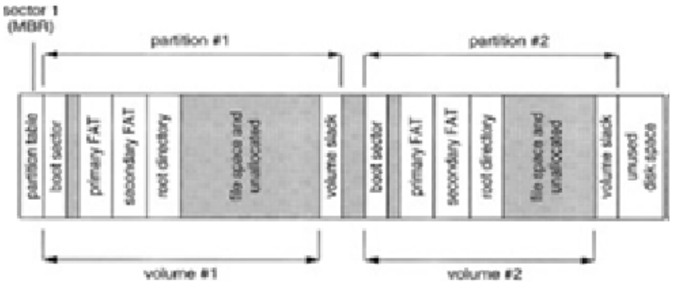

Figure 4. . shows disk structure with two partitions, each containing a FAT formatted volume.

Free space: However, when a file is moved from one hard disk or partition to another, it is actually a multistep process of copying and deleting the file. First, a new copy of the file is created on the target partition. After the file has been copied, the original file is then deleted. This process also requires some housekeeping in the FAT or MFT tables. A new entry is created in the table on the partition where it has been copied, whereas the record for the deleted file is removed from the table on its partition. When a file get deleted, that space considered as free space, there also criminal can hide sensitive information.[16]

Faked Bad Clusters: Clusters marked as bad may be used to hide data. In NFTS, bad clusters are marked in metadata file called $BadClus, which is in MFT entry 8. Originally, $BadClus is a sparse file which file size is set to the size of entire file system. When bad clusters are detected, they will be allocated to this file. The size of data that can be hidden with this technique is unlimited. Suspects can simply allocate more clusters.[16][17]

C. Storage Media Investigation using WinHex Tool.[18]

WinHex Tool : WinHex is a universal hex editor, particularly helpful in computer forensics, data recovery, low-level data editing.

Main Functions of WinHex Tool:[18]

1. Disk cloning and imaging,
2. Hex View of File.
3. Mass hash calculation for files (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD, ...)
4. Gathering slack space, free space, inter-partition space, and generic text from drives and images
5. File and directory catalog creation for all computer media
6. Concatenating and splitting files, unifying and dividing odd and even bytes/words
7. Analyzing and comparing files
8. Particularly flexible search and replace functions
11. Easy detection of and access to NTFS alternate data streams (ADS)
10. Lightning fast powerful physical and logical search capabilities for many search terms at the same time

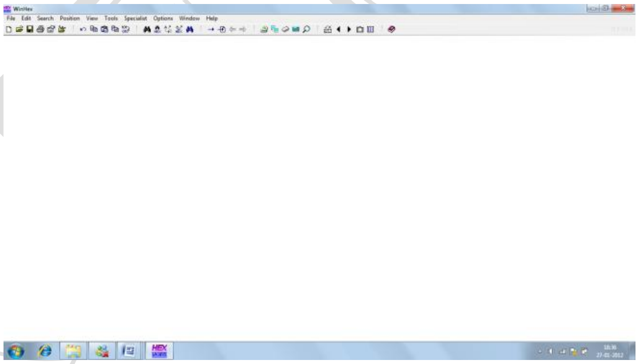

Figure 4. shows the Screen shot of WinHex Tool[18]

Investigation steps:

1. Assesses the crime Scene

2. Evidence Collection

2.1 Select a Tool eg: WinHex[18]
2.2 Create image of the compromised system disk.
2.3 open WinHex
2.4 open particular drive (Tools →open disk)
2.5 Calculate Hash value of the drive/disk
(Tools →compute hash)
Store hash value in a text file.
2.6 Recover the necessary files and deleted files from the disk image.(Specialist →Interpret as image)
2.7 Copied into a folder.
2.8 Start analysis of the content recovered files of files.
2.9 Image analysis ie hidden data inside an image can be analyse using Stegnography tools (Stools),
2.10 Check Header and footer of application file. Copy header and footer and paste into text pad.

Examples with WinHex [18]:

1)Create an image of DISK using WinHex Tool[18]

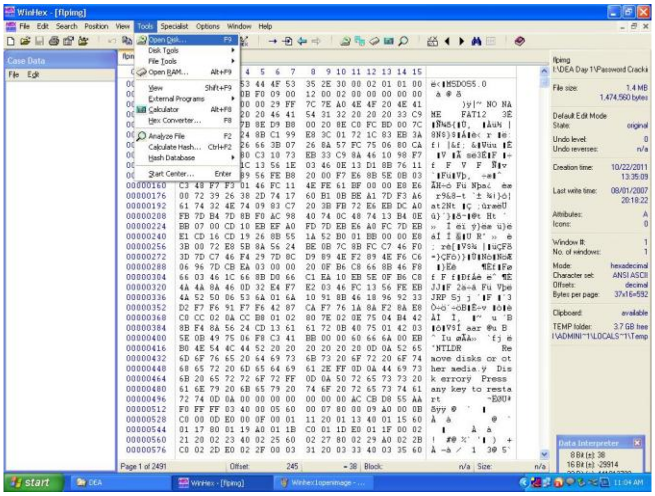

Figure 5. Screen shot of creation of disk image and save the image as .img file.

3. Analyse the Disk image
   3.1.1 Calculate Hash value of image (Tools→compute hash)
   3.1.2 Compare the Hash value of original with image. If equal start analysis else acquired data altered.
   3.2 Recover the necessary files and deleted files from the disk image.(Specialist →Interpret as image)
   3.3 Copied into a folder.
   3.4 Start analysis of the content recovered files of files.
   3.5 Image analysis ie hidden data inside an image can be analyse using Stegnography tools (Stools)
   3.6 Check Header and footer of application file. Copy header and footer and paste into text pad. Sometimes evidence should be present in Header and footers.

4. Conclude the investigation and Generate Report.

Recover Deleted file using WinHex.

1) Open Drive image
2) Make as file view mode
3) Recover the necessary files and deleted files from the disk image.(Specialist →Interpret as image)
4) Copied into a folder.
5) Start analysis of the content recovered files.

Open drive image – select file and right click

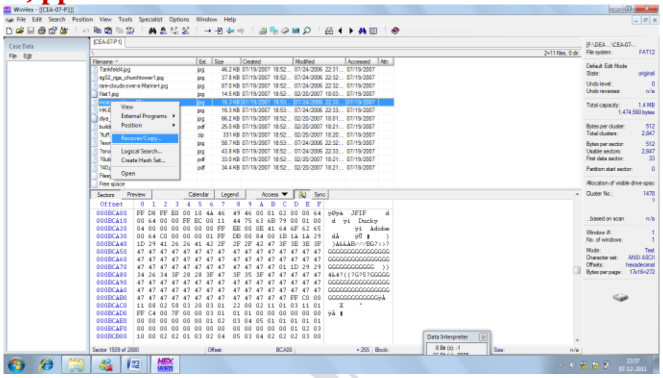

Figure. 6. Screen shot of Recover/copy deleted file

D. Windows Recycle bin Analysis using WinHex.[5][6][7]

Recycle Bin is a temporary holding container for files that have been recently discarded (deleted) by the user. Analysis of deleted files often provides useful information for the forensic computer examiner. With the Windows XP implementation, the first folder is named “RECYCLER”. With Windows 7 and Windows Vista, the first folder is named “$Recycle.Bin”. Each of these folders is normally hidden from the user by the Operating System, so the forensic examiner must remember to unhide these folders before they can be viewed.

Windows XP Recycle Bin File Structure [6]:

C:\RECYCLER\
S-1-5-21-51003140-4199384537-3980697693-500
S-1-5-21-3345512350-4226073239-312180513-1000
DC1.txt
INFO2
S-1-5-21-3345512350-4226073239-312180513-1001
DC2.pf
DC3.pf
INFO2

DC files and INFO2 file contains the information about the deleted files. “D” stands for “drive”. “C” refers to the identifier of the drive (above 1, we are dealing with “Drive C:\”). “1” is the unique identifier of the file. In this example, this file was the first to be sent to the recycle bin. Subsequent deleted files on the C:\ drive would be named DC1, DC2, DC3, etc. “txt” simply refers to the file extension that was on the file that was deleted. Windows XP also stores the metadata associated with the file’s deletion – such as the file-name, file-path, file-size, and time-of-deletion. All of this metadata is stored in the file named INFO2.

Windows 7 and Windows Vista Recycle Bin File Structure [6][7]

C:\$Recycle.Bin\
S-1-5-21-51003140-4199384537-3980697693-500
S-1-5-21-3345512350-4226073239-312180513-1000
$IPTEYOA.txt
$RPTEYOA.txt
S-1-5-21-3345512350-4226073239-312180513-1001
$IGDRVPB.pf
$IW1EQ3V.pf
$RGDRVPB.pf
$RW1EQ3V.pf

$IPTEYOA.txt contains the metadata about the deleted file,

WinHex to open the file $IPTEYOA. At offset 0x8, one will see the 64 bit hexadecimal value “6A F7 0F 00”, convert “6A F7 0F 00” from Little Endian to Big Endian format which represents the file size. 00 0F F7 6A.
Converting this hexadecimal value to a decimal (using a conversion calculator)5 one gets 1,046,378 bytes (or about 1 MB), which represents the actual size of the file that was deleted.
At offset 0x10 is the hexadecimal value
D0 DD 76 3C 2B A9 C8 01 is the time at which the file was deleted
Converting this hexadecimal value to a decimal value (again, by using a conversion calculator) we get the number 128,538,592,543,170,000. Machor states that this number is the time the file was deleted, but expressed as the number of 100 nano-seconds from January 1, 1601. To convert this number to a more usable size, one multiplies the number by 100 (to convert it from 100 nano-seconds to nano-seconds) and then divides it by 1,000,000,000 to convert it from nano-seconds to seconds. Winhex tool has the facility to show the time exactly. The final result is 4/28/2008 8:27:34, which is precisely when the file was deleted. offset 0x18 is the start of the file-path.

IV Database Forensics

Database Forensics is a branch of digital forensic science relating to the forensic study of databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a database user. Alternatively, a forensic examination may focus on identifying transactions within a database system or application that indicate evidence of wrong doing, such as fraud.

A. Identifying Locations For Evidence

Redo Logs: A Redo Entry [8], otherwise known as a Redo Record, contains all changes for a given SCN. A SCN or System Change Number is like a marker that Oracle can use to indicate a particular instance of a state. In other words if the state of the database changes, for example by someone performing an INSERT followed by a COMMIT, then Oracle can track this using a SCN. If the state needs to be restored at some point in the future then this can be achieved using the SCN to indicate which “version” of the database’s state you want.
The entry has a header and one or more “change vectors”. There may be one or more change vectors for a given event. For example, if a user performs an INSERT on a table that has an index then several change vectors are created. There will be a redo and undo vector for the INSERT and then an insert leaf row for the index and a commit. Each change vector has its own operation code that can be used to differentiate between change vectors. The table below lists some of the more common ones:

5.1	Undo Record
5.4	Commit
11.2	INSERT on single row
11.3	DELETE
11.5	UPDATE single row
11.11	INSERT multiple rows
11.19	UPDATE multiple rows
10.2	INSERT LEAF ROW
10.4	DELETE LEAF ROW
13.1	Allocate space [e.g. after CREATE TABLE]
24.1	DDL

The forensic examiner must go through each redo entry and work out what has happened and attempt to separate those which are “normal” and those which are part of an attack.

Data Blocks[9]:.When the block is filled up, the server starts filling a new block. Each row in the block has a three byte header. The first byte is a marker and contains a set of flags to indicate the row’s state. For example, if the row has been deleted the 5th bit of the byte is set. For example, a common set of flags value for a marker is 0x2C – which becomes 0x3C when the “deleted” flag is set. This is an important point to remember as it is a key indicator when looking for dropped objects.

TNS Listeners log file and the audit trail : To be able to log into the RDBMS an attacker [10] needs to know the Service Identifier or SID for the database. Before Oracle 10g this could be extracted from the TNS Listener with the SERVICES or STATUS command. Here’s something to be careful of with the audit trail. When a user successfully logs on a row is created in the audit trail. This has an ACTION# number of 100 (LOGON) and the TIMESTAMP# column reflects when the logon occurred In building a timeline of events this is important. This effectively hides when the user actually logged on. However, if we describe the AUD$ table we can see a

LOGOFF$TIME column. If we then query this column, too, we can reconcile the logon and logoff times

Live Response: When the database is shutdown cleanly this would wipe the audit trail making the task of the forensic examiner that little bit harder [11]. Of course, the attacker could do more than just wiped the audit trail in such a trigger. Due to issues like this and the loss of volatile information, some organizations prefer to perform an analysis on the system whilst it’s still powered on and connected to the network. This is called a Live Response. Live Response is all about recovering and safely storing volatile data for later analysis, in other words, all the information that will disappear when the machine is disconnected from the network and switched off. Further, Live Response gives the forensic examiner the chance to collect non-volatile evidence in a “humanreadable” format that’s easier to peruse than its stored binary version – for example event logs.

Views: There are a number of virtual tables and views that Oracle maintains for performance purposes [12]. These views are accessible to DBAs and can often contain evidence of attacks. Two of these views are of particular interest – V$SQL and V$DB_OBJECT_CACHE. The V$SQL fixed view contains a list of recently executed SQL. Evidence of an attacker’s activities may be found in this fixed view and careful examination of the SQL_TEXT should reveal this.

Oracle Recycle Bin : Whenever a table is dropped, the table and any [13] dependent objects such as indexes and triggers are moved to the Recycle Bin. This way, if it is decided that the table has been dropped in error, it can be recovered from the Recycle Bin using the UNDROP statement.

System Change Number: During a forensic examination of a compromised [14] Oracle database server the SCN and its timestamp can help tell the investigator whether a block of data has been changed. This is especially useful in those cases where there is an absence of other evidence such as the redo logs or audit trail. As with all forensic examinations it's critical not to change any evidence so any investigation should take place on a cold data file and not a live data file.

The main source of evidence as follows[15]:

1. Listener log –logs connections to the listener, use lsnrctl to administrate it.Can be found in /u01/app/oracle/oracle/product/10.2.0/db_4/network/listener.log

2. Alert log – system alerts important to DB e.g processes starting and stopping. Can be found in /u01/app/oracle/admin/orcl/bdump

3. Sqlnet.log – some failed connection attempts such as “Fatal NI connect error 12170”.

4. Redo logs - current changes that have not been checkpointed into the datafiles (.dbf).
/u01/app/oracle/oradata/orcl/redo02.log
/u01/app/oracle/oradata/orcl/redo01.log
/u01/app/oracle/oradata/orcl/redo03.log

5. Archived redo logs – previous redo logs that can be applied to bring back the data in the db to a previous state using SCN as the main sequential identifier. This can be mapped to timestamp.

6. Fine-Grained Auditing audit logs viewable from FGA_LOG$ and DBA_FGA_AUDIT_TRAIL VIEW.

7. Oracle database audit SYS.AUD$ table and DBA_AUDIT_TRAIL VIEW.

8. Oracle mandatory and OS audit /u01/app/oracle/admin/orcl/adump

9. Home-made trigger audit trails - bespoke to the system.

10. Agntsrvc.log – contains logs about the Oracle Intelligent agent.

11. IDS, Web server and firewall logs should also be integrated to the incident handling timeline. This will rely heavily on well synchronised time in the network as previously mentioned.

B Steps to collect the evidence from database files.

With the help of the above study we have identified the steps which are useful in collecting the evidences.

Step1. Setup the evidence collection server by the following ways:

- firstly by mapping a drive if the system is running on Windows or has Samba and then using file redirection:
  D:\>listdlls.exe > z:\case-0001-listdlls.txt
- The second method is to pipe output over the network using netcat or cryptcat.
-

Step2. **Perform the following general steps to get basic information like:**

System time and date*:* The incident responder should first record the system time and date of system that they’re investigating.

***Logged on users* :** The list of users that are currently logged on to the system and from where and for how long is extremely useful.

List all users and groups :Obtain a list of all users, gathering details on when they last logged in, and groups on the server and group membership.

***List open ports and connections* :**All open and connected TCP ports should be collected as well as listening UDP ports.

List running processes **:** A list of all running processes should be obtained. Close attention should be paid to suspicious looking entries and also any shells such as cmd.exe or /bin/sh – indeed keep an eye out for //bin/sh (note two slashes) as this may indicate an overflow or format string exploit has been launched. The forensic examiner should also get a list of each process's parent process.

List of DLLs or shared objects **:** A list of the DLLs or shared objects that are loaded by each process should be obtained. Keep an eye out for odd looking names; on Windows look out for DLLs that are loaded via a UNC path across the network.

List of open handles **:** As well as what file handles a process has open a list of other handles should be obtained as well. Whilst this can reveal what an attacker may have been doing it can also help identify "parentless" processes.

Perform memory dumps **:** Memory dumps of all running process should be gathered even in what appear to be "normal" looking processes. The reason for this is to catch cloaking attacks – an attacker may launch a benign process like "notepad" and using CreateRemoteThread() load code into its address space.

Perform system memory dump **:** A dump of all system memory should be performed. This will cover those bit of memory not dumped when dumping each process.

Get file names and MACTimes**:** The incident responder should perform a full recursive directory list of every disk and get file and directory names as well as their creation, access and modification times. They should also gather information about each file's owner and any special attributes such as whether the read only, system or hidden attributes are set.

Dump registry information **:** On Windows all registry information should be dumped.

Locate and take copies of log files and message logs**:** All of the servers log files and event and message logs should be copied to the collection server for analysis. These logs will vary from system to system depending upon what services are running.

Step3. Collect the Oracle files of Interest

The Oracle specific log, trace and control files can be located in various places. Firstly we need to know where each instance of Oracle is installed this can be extracted from the ORACLE_HOME environment variable if set. On Windows the HKEY_LOCAL_MACHINE\Software\Oracle Registry key stores information about each Oracle home.

Step4. Get the previously executed SQL

Get a copy of the most recently executed SQL. This can be retrieved from the V$SQL fixed view. On Oracle 10g the query should be:

```
SQL> SELECT LAST_ACTIVE_TIME,
PARSING_USER_ID, SQL_TEXT FROM V$SQL
ORDER BY LAST_ACTIVE_TIME ASC;
```

This will list the SQL that was executed by who and when from the V$SQL fixed view.

Step5. Getting a list of users and roles.

The incident responder should get a complete listing of all users on the system.

```
SQL> SELECT USER#, NAME, ASTATUS,
PASSWORD, CTIME, PTIME, LTIME FROM
SYS.USER$ WHERE TYPE#=1;
```

Step6. Getting a list of dropped tables

In 10g, if a user has dropped any tables and they have not been purged from the
recyclebin then a list of dropped tables should be present. This may indicate evidence of an attack:

```
SQL> SELECT U.NAME, R.ORIGINAL_NAME,
R.OBJ#, R.DROPTIME, R.DROPSCN
FROM SYS.RECYCLEBIN$ R, SYS.USER$ U WHERE
R.OWNER#=U.USER#;
```

Step7. Getting information about PL/SQL objects

The source of PL/SQL objects should be retrieved and analyzed. Much of the source is encrypted or "wrapped" to use the Oracle term. The incident responder should obtain an "unwrapper" to examine the clear text as an attacker can modify a PL/SQL object and re-encrypt it to hide their attack.

Step8. Finishing Up

Once all queries have been executed the spool file should be closed and sqlplus can be closed.

```
SQL> SPOOL OFF
SQL> QUIT
Disconnected from Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 – Production with the Partitioning, OLAP and Data Mining options
C:\oracle\product\10.2.0\db_1\BIN>
```

Once disconnected from the server an md5 checksum should be made of the spool file and recorded with a witness present.

V. Conclusion.

There are many ways of securing the database and file system. The attackers have the methods to violate the security. Then comes the role of forensic analyst who should have a thorough knowledge of the basics of a database and file system and also the information about the same on which he is going to perform the analysis. The forensic analyst should also be able to think from the attacker's point of view. Based on different cases, the digital evidences can be collected from the specified locations. If the intensions of the attacker are known identifying the attacked location may be easier. Thinking from the attacker's point of view this paper gives a contribution towards the identification of the general locations in a database and the file system for collecting the digital evidences.

VI. References

Journals

[1] H. Achi, A. Hellany & M. Nagrial. Network Security Approach for Digital Forensics Analysis 2008 IEEE.

[2] .Stephen K. Brannon, and Thomas Song Computer Forensics: Digital Forensic Analysis Methodology. Computer Forensics Journal January 2008 Volume 56

[3] Cheong Kaiwee. Analysis of Hidden Data in NTFS File system. Whitepaper.

[4]. Mamoun, Alazab, Sitalakshmi Venktraman, Paul Watters. Effective Digital forensic Analysis of the NTFS Disk Image. Ubicc Journal, vol 4.

[5]. Timothy R. Leschke. Cyber Dumpster-Diving: $Recycle.Bin Forensics for Windows 7 and Windows Vista.

[6]. Keith J. Jones Forensic Analysis of Microsoft Windows Recycle Bin Records.

[7]. Gao Qinquan,Wu shunxiang. Research of Recycle Bin Forensic Analysis Platform Based On XML Techniques.

[8] Oracle Forensics Part 1: Dissecting the Redo Logs DavidLitchfield [davidl@ngssoftware.com]

[9] Oracle Forensics Part 2: Locating dropped objects DavidLitchfield

[10] Oracle Forensics: Part 3 Isolating Evidence of Attacks against the Authentication Mechanism David Litchfield

[11] Oracle Forensics Part 4: Live Response David Litchfield

[12] Oracle Forensics Part 5: Finding Evidence of Data Theft in the Absence of Auditing David Litchfield

[13] Oracle Forensics Part 6: Examining Undo Segments, Flashback and the Oracle Recycle Bin David Litchfield

[14] Oracle Forensics Part 7: Using the Oracle System Change Number in Forensic Investigations David Litchfield

[15] ORACLE FORENSICS IN A NUTSHELL 25/03/2007

Books

[16] Brian Carrier . File system Forensic Analysis. Publisher addison Wesley Professional .publication Date. March 17, 2005.

[17] Karen Kent, Suzanne Chevaller, Tim Grance, Hung Dang. Guide to Integrating Forensic Techniques into incident response.

Website

[18] http://www.WinHex.com