



## Oracle Forensics

—

# Dissection of an Oracle Attack in the Absence of Auditing

David Litchfield  
([davidl@ngssoftware.com](mailto:davidl@ngssoftware.com))

## Why Oracle Forensics?

- Since the state of California passed the Database Security Breach Notification Act (SB 1386) in 2003 another 34 states have passed similar legislation with more set to follow.
- In January 2007 TJX announced they had suffered a database security breach with 45.6 million credits card details stolen – the largest known breach so far.
- In 2006 there were 335 publicized breaches in the U.S.; in 2005 there were 116 publicized breaches; between 1st January and March 31st of 2007, a 90 day period, there have been 85 breaches publicized.
- There are 0 (zero) database-specific forensic analysis and incident response tools on the market – free or commercial.



## Where is the evidence?

- Evidence of a compromise can be found in many places – for example
  - TNS Log files
  - Trace files
  - Redo Logs
  - Datafiles
    - Metadata and statistics
    - Apache logs (Oracle Application Server)
- This talk specifically covers the datafiles, redo logs In the essence of time we'll be cutting out several parts of the forensic process which you wouldn't do in a real scenario of course!
- Search for evidence related to SELECTs
- To start with we'll look at an Oracle Data Block



## Where is the evidence?

- Evidence of a compromise can be found in many places – for example
  - TNS Log files
  - Trace files
  - Redo Logs
  - Datafiles
    - Metadata and statistics
    - Apache logs (Oracle Application Server)
- This talk specifically covers the datafiles, redo logs In the essence of time we'll be cutting out several parts of the forensic process which you wouldn't do in a real scenario of course!
- To start with we'll look at an Oracle Data Block



# Oracle Data Block

## Header

Object ID (25<sup>th</sup> Byte)

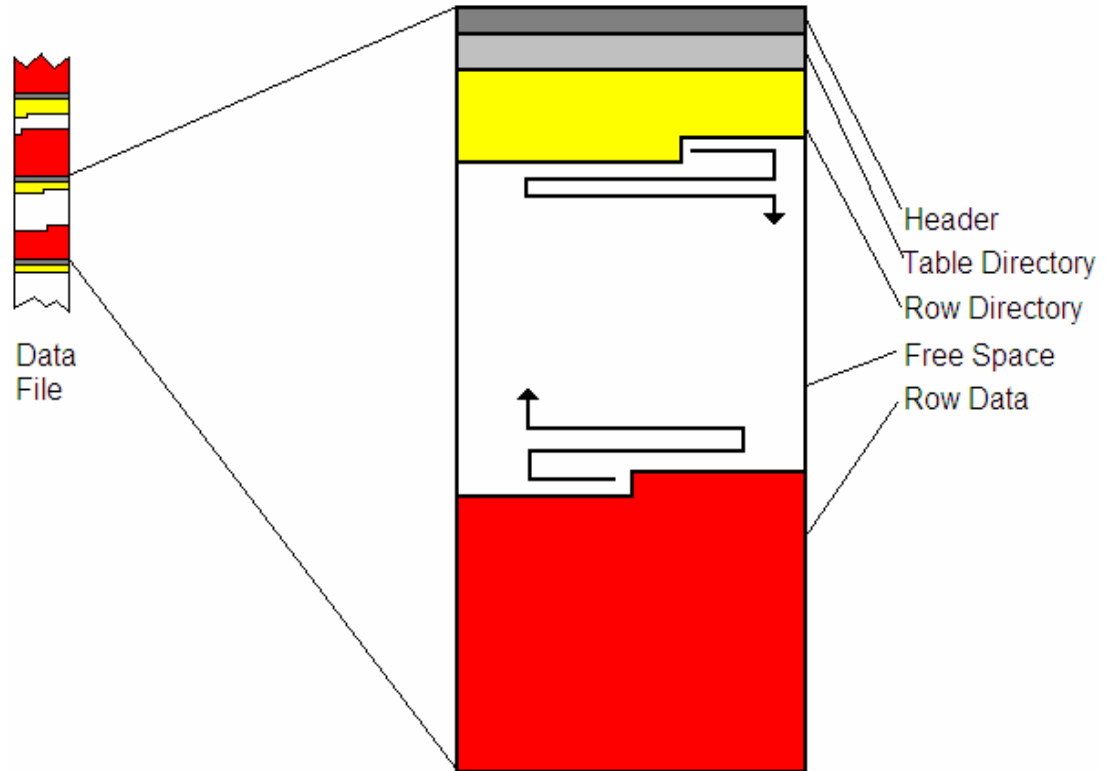
Checksum

## Row Directory

Each row has

2 byte entry

pointing to offset



## Oracle Data Block...row of data

Consists of a 3 byte Row Header

Byte 1: Flags to indicate row state

If row of data has been deleted the 5<sup>th</sup> bit of 1<sup>st</sup> byte (Flags) is set – e.g. 0x2C becomes 0x3C

Byte 2: Lock Status

Byte 3: Number of columns

Column Length followed by that number of bytes of data



## Oracle Data Block...row of data

```

Col 1      04 C3 06 13 2F
Col 2      04 C3 06 13 2F
Col 3      02 C1 37
Col 4      0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45
Col 5      02 C1 02
Col 6      FF
Col 7      02 C1 03
Col 8      07 78 6B 03 17 12 08 38
Col 9      07 78 6B 03 17 12 08 38
Col 10     07 78 6B 03 17 12 08 38
Col 11     02 C1 02
Col 12     FF
Col 13     FF
Col 14     01 80
Col 15     FF
Col 16     02 C1 07
Col 17     02 C1 02
  
```



## Locating Dropped Objects

To locate dropped objects we need to know what happens when an object is created:

- A row is entered in the OBJ\$ table, I\_OBJ1, I\_OBJ2, I\_OBJ3 indexes
- Depending upon object  
TAB\$, COL\$ for table objects  
SOURCE\$, IDL\_UB1\$, IDL\_CHAR\$ for functions
- Information about new objects scattered all over the datafile.



## Locating Dropped Objects

Open datafile that has the SYSTEM tablespace

Locate all blocks with object ID of 18 – object ID of the OBJ\$ table.

Follow each entry in the row directory

Some of these will point to “live” (0x2C) rows

Others “deleted” (0x3C)

All data that has not been “blocked out” is deleted data – may only be fragments though!

Rinse and Repeat for all “interesting” object IDs – e.g. SOURCE\$,



```

1d398000h: 06 A2 00 00 CC E9 40 00 D2 9A 0F 00 00 00 01 06 ; .>..ié@.òs.....
1d398010h: 12 F4 00 00 01 00 00 00 4E 09 00 00 C4 9A 0F 00 ; .ò.....H...Äš..
1d398020h: 00 00 00 00 02 00 03 00 CD E9 40 00 03 00 0A 00 ; .....ié@.....
1d398030h: 4A 02 00 00 BB 05 80 00 BB 01 04 00 09 20 59 01 ; J...».«.».Y.
1d398040h: D2 9A 0F 00 03 00 0B 00 4A 02 00 00 BA 05 80 00 ; Os.....J...°.E.
1d398050h: BB 01 0E 00 00 80 00 00 74 9A 0F 00 00 01 39 00 ; »....€..cš....9.
1d398060h: 20 00 84 00 AB 11 B5 16 20 18 00 00 39 00 25 1D ; ...«.u. ...9.&.
1d398070h: 84 1D 92 1D C3 1D 31 1E 5C 1E BB 1E C9 1E E2 1E ; ...' .Ä.1.\.«.É.ä.
1d398080h: F0 1E 61 1F 79 1C C4 1C D2 1C FD 1C 0B 1D 20 1C ; š.a.y.Ä.D.y...
1d398090h: CC 1B 1C 1B 4B 1B 5D 1B BC 1B 2D 17 66 17 89 17 ; ì...K.j.».-.f.k.
1d3980a0h: B4 17 C6 17 FF 17 13 18 30 18 16 13 4B 13 21 00 ; 'E.y...D...R.!.
1d3980b0h: 22 00 23 00 24 00 25 00 26 00 27 00 2E 00 6B 13 ; ".#.$.&.&.'...k.
1d3980c0h: 7A 13 A5 13 B7 13 3D 14 51 14 FF FF 6B 14 AB 14 ; z.¥...=.Q.ÿÿk.«.
1d3980d0h: E4 11 04 12 13 12 3E 12 50 12 D8 12 EC 12 06 13 ; ä.....>.P.Ø.i...

1d399200h: 00 00 00 00 00 00 00 00 3C 01 09 04 C3 06 19 33 02 ; .....<...Ä..3.
1d399210h: C3 02 2D 46 55 4E 43 54 49 4E 4E 20 45 58 54 52 ; Ä.-FUNCTION EXTR
1d399220h: 43 43 54 5F 53 59 53 5F 50 54 53 53 57 4F 52 44 ; ACT_SYS_PASSWORD
1d399230h: 20 52 45 54 55 52 4E 20 55 41 55 43 48 41 52 0A ; RETURN VARCHAR.
1d399240h: 3C 01 03 04 C3 06 13 33 02 C1 03 1E 11 55 54 48 ; <...Ä..3.Ä..AUTH
1d399250h: 49 44 20 43 55 52 52 45 4E 54 5F 55 53 45 52 0A ; ID CURRENT_USER.
1d399260h: 3C 01 03 04 C3 06 13 33 02 C1 03 1E 11 55 54 48 ; <...Ä..3.Ä..IS.<
1d399270h: 01 03 04 C3 06 13 33 02 C1 03 1E 11 55 54 48 ; ...Ä..3.Ä..PRAGM
1d399280h: 41 20 41 55 54 4F 4E 4F 4D 4F 55 53 5F 54 52 41 ; A AUTONOMOUS TRA
1d399290h: 4E 53 41 43 54 49 4F 4E 3B 0A 3C 01 03 04 C3 06 ; NSACTION;<...Ä.
1d3992a0h: 13 33 02 C1 06 06 42 45 47 49 4E 0A 3C 01 03 04 ; .3.Ä..BEGIN.<...
1d3992b0h: C3 06 13 33 02 C1 07 7C 45 58 45 43 55 54 45 20 ; Ä..3.Ä.|EXECUTE
1d3992c0h: 49 4D 4D 45 44 49 41 54 45 20 27 49 4E 53 45 52 ; IMMEDIATE 'INSE
1d3992d0h: 54 20 49 4E 54 4E 20 53 43 4F 54 54 2E 4D 59 5F ; T INTO SCOTT.MY_
1d3992e0h: 54 45 4D 50 5F 54 42 42 4C 45 20 56 41 4C 55 45 ; TEMP_TABLE VALUE
1d3992f0h: 53 20 28 28 53 45 4C 45 43 54 20 50 41 53 53 57 ; S ((SELECT PASSW
1d399300h: 4F 52 44 20 46 57 4F 4D 20 53 59 53 2E 44 42 41 ; ORD FROM SYS.DBA
1d399310h: 5F 55 53 45 52 53 20 57 48 45 52 45 20 55 53 45 ; _USERS WHERE USE
1d399320h: 52 4E 41 4D 4F 20 3D 20 27 27 53 59 53 27 27 29 ; RNAME = 'SYS')
1d399330h: 29 27 3B 0A 3C 01 03 04 C3 06 13 33 02 C1 08 08 ; )');<...Ä..3.Ä..
1d399340h: 43 4F 4D 4F 49 54 3B 0A 3C 01 03 04 C3 06 13 33 ; COMMIT;<...Ä..3
1d399350h: 02 C1 09 5E 52 45 54 55 52 4E 20 27 46 4F 4F 27 ; .Ä..RETURN 'FOO'
1d399360h: 3B 0A 3C 01 03 04 C3 06 13 33 02 C1 0A 04 45 4E ; ;<...Ä..3.Ä..EN

```



# Examination after an attack – dropped row in OBJ\$

```

189d2000h: 06 A2 00 00 E9 C4 40 00 2B 9B 0F 00 00 00 01 06 ; .c..éÃ@.+>.....
189d2010h: 8F 01 00 00 01 00 00 00 12 00 00 00 20 9B 0F 00 ; []..... >...
189d2020h: 00 00 00 00 01 00 03 00 EA C4 40 00 01 00 24 00 ; .....éÃ@...$.
189d2030h: 08 02 00 00 0E 00 80 00 E6 01 11 00 01 20 00 00 ; .....€.æ.... ..
189d2040h: 2B 9B 0F 00 00 01 17 00 FF FF 40 00 31 15 E2 16 ; +>.....ÿÿ@.1.â.
189d2050h: E2 16 00 00 17 00 42 1F D6 1E 67 1E F8 1D 95 1D ; â.....B.Ö.g.ø.*.
189d2060h: 2F 1D C9 1C 5E 1C F0 1B 82 1B 13 1B A1 1A 2F 1A ; /.É.^.ð.,...i./..
189d2070h: 31 15 1C 19 95 18 0D 17 5A 17 C1 16 75 16 25 16 ; 1...*....ª.Á.u.š.
189d2080h: C7 15 7C 15 00 00 00 00 00 00 00 00 00 00 00 00 ; Ç.|.....

```

```

189d3790h: C1 02 FF FF 01 80 FF 02 C1 07 02 C1 02 3C 01 11 ; Á.ÿÿ.€ÿ.Á..Á.<...
189d37a0h: 04 C3 06 13 2F 04 C3 06 13 2F 02 C1 37 0D 4D 59 ; .Ã../.Ã../.Á7.MY
189d37b0h: 5F 54 45 4D 50 5F 54 41 42 4C 45 02 C1 02 FF 02 ; _TEMP_TABLE.Á.ÿ.
189d37c0h: C1 03 07 78 6B 03 17 12 08 38 07 78 6B 03 17 12 ; Á..xk....8.xk...
189d37d0h: 08 38 07 78 6B 03 17 12 08 38 02 C1 02 FF FF 01 ; .8.xk....8.Á.ÿÿ.
189d37e0h: 80 FF 02 C1 07 02 C1 02 2C 00 11 04 C3 06 13 2A ; €ÿ.Á..Á.,...Ã..*
189d37f0h: 04 C3 06 13 2A 02 C1 37 1E 42 49 4E 24 4C 64 59 ; .Ã..*.Á7.BIN$LDY

```



## Examination after attack – extract row

Row Header: 0x3C 0x01 0x11

0x11 (17) Columns

```
189d3790h:                               3C 01 11
189d37a0h: 04 C3 06 13 2F 04 C3 06 13 2F 02 C1 37 0D 4D 59
189d37b0h: 5F 54 45 4D 50 5F 54 41 42 4C 45 02 C1 02 FF 02
189d37c0h: C1 03 07 78 6B 03 17 12 08 38 07 78 6B 03 17 12
189d37d0h: 08 38 07 78 6B 03 17 12 08 38 02 C1 02 FF FF 01
189d37e0h: 80 FF 02 C1 07 02 C1 02
```



## Examination after attack – row columns

```
04 C3 06 13 2F
04 C3 06 13 2F
02 C1 37
0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45
02 C1 02
FF
02 C1 03
07 78 6B 03 17 12 08 38
07 78 6B 03 17 12 08 38
07 78 6B 03 17 12 08 38
02 C1 02
FF
FF
01 80
FF
02 C1 07
02 C1 02
```



## Examination after attack – Column datatypes for OBJ\$

OBJ# NUMBER  
DATAOBJ# NUMBER  
OWNER# NUMBER  
NAME VARCHAR2(30)  
NAMESPACE NUMBER  
SUBNAME VARCHAR2(30)  
TYPE# NUMBER  
CTIME DATE  
MTIME DATE  
STIME DATE  
STATUS NUMBER  
REMOTEOWNER VARCHAR2(30)  
LINKNAME VARCHAR2(128)  
FLAGS NUMBER  
OID\$ RAW(16)  
SPARE1 NUMBER  
SPARE2 NUMBER



## Examination after attack – converted columns

04 C3 06 13 2F =  $((6-1)*10000) + ((19-1)*100) + (47-1) = 51846$

04 C3 06 13 2F =  $((6-1)*10000) + ((19-1)*100) + (47-1) = 51846$

02 C1 37 = 55

0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45 = MY\_TEMP\_TABLE

02 C1 02 = 1

FF = NULL

02 C1 03 = 2

07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37

07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37

07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37

02 C1 02 = 1

FF = NULL

FF = NULL

01 80 = 0

FF = NULL

02 C1 07 = 6

02 C1 02 = 1



## Examination after attack – object ID

04 C3 06 13 2F (51846)

Search reveals object ID in

MON\_MODS\$

I\_MON\_MODS\$\_OBJ

RECYCLEBIN\$\_OBJ

C\_FILE#\_BLOCK#



# Examination after attack – further examination – source\$

```

1d398000h: 06 A2 00 00 CC E8 40 00 D2 9A 0F 00 00 00 01 06 ; s..îé@.0s.....
1d3980010h: 12 F4 00 00 01 00 00 00 48 00 00 00 C4 9A 0F 00 ; .ð.....H...Äš..
1d3980020h: 00 00 00 00 02 00 03 00 CD E9 40 00 03 00 0A 00 ; .....îé@.....
1d3980030h: 4A 02 00 00 BB 05 80 00 BB 01 04 00 09 20 59 01 ; J...».«.É... Y.
1d3980040h: D2 9A 0F 00 03 00 0B 00 4A 02 00 00 BA 05 80 00 ; Os.....J...°.É.
1d3980050h: BB 01 0E 00 00 80 00 00 74 9A 0F 00 00 01 39 00 ; »....É..cš....9.
1d3980060h: 20 00 84 00 AB 11 B5 16 20 18 00 00 39 00 25 1D ; ..»..µ. ...9.%
1d3980070h: 84 1D 92 1D C3 1D 31 1E 5C 1E BB 1E C9 1E E2 1E ; ..'Ä.1.\.».É.ä.
1d3980080h: F0 1E 61 1F 79 1C C4 1C D2 1C FD 1C 0B 1D 20 1C ; Š.a.y.Ä.Ö.y...
1d3980090h: CC 1B 1C 1B 4B 1B 5D 1B BC 1B 2D 17 66 17 89 17 ; Ĩ..K.]«.-.f.%
1d39800a0h: B4 17 C6 17 FF 17 13 18 30 18 16 13 4B 13 21 00 ; 'E.y...0..K.!
1d39800b0h: 22 00 23 00 24 00 25 00 26 00 27 00 2E 00 6B 13 ; ".#.$.%&'...k.
1d39800c0h: 7A 13 A5 13 B7 13 3D 14 51 14 FF FF 6B 14 AB 13 ; z.Ÿ...=.Q.ÿÿk.«.
1d39800d0h: E4 13 04 12 13 12 3E 12 50 12 08 12 EC 12 06 13 ; ä.....>.P.Ø.i...

1d399200h: 00 00 00 00 00 00 00 3C 01 08 04 C3 06 19 33 02 ; .....<...Ä..3.
1d399210h: C1 02 2D 46 55 4E 43 54 49 4E 4E 20 45 58 54 52 ; Ä.-FUNCTION EXTR
1d399220h: 41 43 54 5F 53 59 53 5F 50 54 53 53 55 4F 52 44 ; ACT_SYS_PASSWORD
1d399230h: 20 52 45 54 55 52 4E 20 54 41 53 43 48 41 52 0A ; RETURN VARCHAR.
1d399240h: 3C 01 03 04 C3 06 13 33 07 C1 03 14 41 55 54 48 ; <...Ä..3.Ä..AUTH
1d399250h: 49 44 20 43 55 52 52 43 4E 54 5F 55 53 45 52 0A ; ID CURRENT_USER.
1d399260h: 3C 01 03 04 C3 06 13 33 02 C1 04 09 49 53 0A 3C ; <...Ä..3.Ä..IS.<
1d399270h: 01 03 04 C3 06 13 33 02 C1 05 2F 54 52 41 47 4D ; ...Ä..3.Ä..PRAGM
1d399280h: 41 20 41 55 54 4F 4E 4F 4D 4E 55 53 5F 54 52 41 ; A AUTONOMOUS_TRA
1d399290h: 4E 53 41 43 54 49 4F 4E 3B 0A 3C 01 03 04 C3 06 ; NSACTION; <...Ä.
1d3992a0h: 13 33 02 C1 06 06 42 45 47 49 4E 0A 3C 01 03 04 ; .3.Ä..BEGIN.<...
1d3992b0h: C3 06 13 33 02 C1 07 7C 45 58 45 43 55 54 45 20 ; Ä..3.Ä.|EXECUTE
1d3992c0h: 49 4D 4D 45 44 49 41 54 45 20 27 49 4E 53 45 52 ; IMMEDIATE 'INSE
1d3992d0h: 54 20 49 4E 54 4F 20 53 43 4F 54 54 2E 4D 59 5F ; T INTO SCOTT.MY_
1d3992e0h: 54 45 4D 50 5F 54 42 42 4C 45 20 56 41 4C 55 45 ; TEMP_TABLE VALUE
1d3992f0h: 53 20 28 28 53 45 4C 45 43 54 20 50 41 53 53 57 ; S ((SELECT PASSW
1d399300h: 4F 52 44 20 46 57 4F 4D 20 57 59 53 2E 44 42 41 ; ORD FROM SYS.DBA
1d399310h: 5F 55 53 45 52 53 20 57 48 45 52 45 20 55 53 45 ; _
1d399320h: 52 4E 41 4D 47 20 3D 20 27 27 53 59 53 27 27 29 ; _USERS WHERE USE
1d399330h: 29 27 3B 0A 3C 01 03 04 C3 06 13 33 02 C1 08 08 ; )'; <...Ä..3.Ä..
1d399340h: 43 4F 4D 4F 49 54 3B 0A 3C 01 03 04 C3 06 13 33 ; COMMIT; <...Ä..3
1d399350h: 02 C1 09 2E 52 45 54 55 52 4E 20 27 46 4F 4F 27 ; .Ä..RETURN 'FOO'
1d399360h: 3B 0A 3C 01 03 04 C3 06 13 33 02 C1 0A 04 45 4E ; ;.<...Ä..3.Ä..EN
    
```



## Examination after attack – deleted rows

$0x1D39805C + 0x1306 = 0x1D399362$

$0x1D39805C + 0x12EC = 0x1D399348$

$0x1D39805C + 0x12D8 = 0x1D399334$

$0x1D39805C + 0x1250 = 0x1D3992AC$

$0x1D39805C + 0x123E = 0x1D39929A$

$0x1D39805C + 0x1213 = 0x1D39926F$

$0x1D39805C + 0x1204 = 0x1D399260$

$0x1D39805C + 0x11E4 = 0x1D399240$

$0x1D39805C + 0x11AB = 0x1D399207$



# Examination after attack – same object ID

C3 06 13 33 (51850)

```

1d399200h: 00 00 00 00 00 00 00 00 SC 01 03 04 C3 06 13 33 02 ; .....<...Ã...3.
1d399210h: C1 02 2D 46 55 4E 43 54 49 4E 4E 20 45 58 54 52 ; Á.-FUNCTION EXTR
1d399220h: 47 43 54 5F 53 59 53 5F 50 41 53 53 57 4F 52 44 ; ACT_SYS_PASSWORD
1d399230h: 20 52 45 54 55 52 4E 20 56 41 50 43 48 41 52 0A ; RETURN VARCHAR.
1d399240h: SC 01 03 04 C3 06 13 33 01 C1 03 14 41 55 54 48 ; <...Ã...3.Á..AUTH
1d399250h: 49 44 20 43 55 52 52 45 4E 54 5F 55 53 45 52 0A ; ID CURRENT_USER.
1d399260h: SC 01 03 04 C3 06 13 33 02 C1 04 03 49 53 0A SC ; <...Ã...3.Á..IS.<
1d399270h: 01 03 04 C3 06 13 33 03 C1 05 1F 50 52 41 47 4D ; ...Ã...3.Á..PRAGM
1d399280h: 41 20 41 55 54 4F 4E 4F 4D 4F 55 53 5F 54 52 41 ; A AUTONOMOUS_TRA
1d399290h: 4E 53 41 43 54 49 4F 4E 3B 0A SC 01 03 04 C3 06 ; NSACTION;<...Ã.
1d3992a0h: 13 33 02 C1 06 06 42 45 47 49 4E 0A SC 01 03 04 ; .3.Á..BEGIN.<...
1d3992b0h: C3 06 13 33 02 C1 07 7C 45 58 45 43 55 54 45 20 ; Ã...3.Á.|EXECUTE
1d3992c0h: 49 4D 4D 45 44 49 41 54 45 20 27 49 4E 53 45 52 ; IMMEDIATE 'INSER
1d3992d0h: 54 20 49 4E 54 4F 20 53 43 4F 54 54 2E 4D 59 5F ; T INTO SCOTT.MY_
1d3992e0h: 54 45 4D 50 5F 54 42 42 4C 45 20 56 41 4C 55 45 ; TEMP_TABLE VALUE
1d3992f0h: 53 20 28 28 53 45 4C 45 43 54 20 50 41 53 53 57 ; S ((SELECT PASSW
1d399300h: 4F 52 44 20 46 52 4F 4D 20 53 59 53 2E 44 42 41 ; ORD FROM SYS.DBA
1d399310h: 5F 55 53 45 52 53 20 57 48 45 52 45 20 55 53 45 ; _USERS WHERE USE
1d399320h: 52 4E 41 4D 4F 20 3D 20 27 27 53 59 53 27 27 29 ; RNAME = 'SYS')
1d399330h: 29 27 3B 0A SC 01 03 04 C3 06 13 33 02 C1 08 08 ; )';<...Ã...3.Á..
1d399340h: 43 4F 4D 4E 49 54 3B 0A SC 01 03 04 C3 06 13 33 ; COMMIT;<...Ã...3
1d399350h: 02 C1 09 0E 52 45 54 55 52 4E 20 27 46 4F 4F 27 ; .Á..RETURN 'FOO'
1d399360h: 3B 0A SC 01 03 04 C3 06 13 33 02 C1 0A 04 45 4E ; ;<...Ã...3.Á..EN

```



## Examination after attack – text of function

```
FUNCTION EXTRACT_SYS_PASSWORD RETURN VARCHAR  
AUTHID CURRENT_USER  
IS  
PRAGMA AUTONOMOUS_TRANSACTION;  
BEGIN  
EXECUTE IMMEDIATE 'INSERT INTO  
    SCOTT.MY_TEMP_TABLE VALUES ((SELECT  
PASSWORD FROM SYS.DBA_USERS WHERE USERNAME =  
    "SYS"))';  
COMMIT;  
RETURN 'FOO';
```



## Examination after attack – locate table

**Object ID 51846 – table is USERS  
 tablespace – SYS password present**

```

0008e000h: 06 A2 00 00 47 00 00 01 B2 9A 0F 00 00 00 02 06 ; .e..G...š.....
0008e010h: 75 10 00 00 01 00 00 00 86 CA 00 00 B0 9A 0F 00 ; u.....†Ê..°š..
0008e020h: 00 00 00 00 02 00 32 00 41 00 00 01 06 00 23 00 ; .....2.A.....#.
0008e030h: 4A 02 00 00 93 00 80 00 D3 01 1F 00 01 20 00 00 ; J...".€.Ó.... ..
0008e040h: B1 9A 0F 00 04 00 0C 00 FF 01 00 00 23 03 80 00 ; ±š.....ÿ...#.€.
0008e050h: E1 01 39 00 01 20 00 00 B2 9A 0F 00 00 00 00 00 ; á.9... ..š.....
0008e060h: 00 00 00 00 00 01 04 00 FF FF 1A 00 48 1F 2E 1F ; .....ÿÿ..H...
0008e070h: 2E 1F 00 00 04 00 84 1F 70 1F 5C 1F 48 1F 00 00 ; .....„.p.\.H...

0008ffa0h: 00 00 00 00 00 00 00 00 00 00 00 00 2C 02 01 10 ; .....
0008ffb0h: 44 43 42 37 34 38 41 35 42 43 35 33 39 30 46 32 ; DCB748A5BC5390F2
0008ffc0h: 2C 01 01 10 44 43 42 37 34 38 41 35 42 43 35 33 ; ,...DCB748A5BC53
0008ffd0h: 39 30 46 32 2C 00 01 10 44 43 42 37 34 38 41 35 ; 90F2,...DCB748A5
0008ffe0h: 42 43 35 33 39 30 46 32 2C 00 01 10 44 43 42 37 ; BC5390F2,...DCB7
0008fff0h: 34 38 41 35 42 43 35 33 39 30 46 32 02 06 B2 9A ; 48A5BC5390F2...š
  
```



## Examination after attack – converted columns

```

04 C3 06 13 2F = ((6-1)*10000) + ((19-1)*100) + (47-1) = 51846
04 C3 06 13 2F = ((6-1)*10000) + ((19-1)*100) + (47-1) = 51846
02 C1 37 = 55
0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45 = MY_TEMP_TABLE
02 C1 02 = 1
FF = NULL
02 C1 03 = 2
07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37
07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37
07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37
02 C1 02 = 1
FF = NULL
FF = NULL
01 80 = 0
FF = NULL
02 C1 07 = 6
02 C1 02 = 1

```



## Examination after attack – converted columns

04 C3 06 13 2F = ((6-1)\*10000) + ((19-1)\*100) + (47-1) = 51846

04 C3 06 13 2F = ((6-1)\*10000) + ((19-1)\*100) + (47-1) = 51846

02 C1 37 = 55

0D 4D 59 5F 54 45 4D 50 5F 54 41 42 4C 45 = MY\_TEMP\_TABLE

02 C1 02 = 1

FF = NULL

02 C1 03 = 2

07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37

07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37

07 78 6B 03 17 12 08 38 = 23/03/2007 17:07:37

02 C1 02 = 1

FF = NULL

FF = NULL

01 80 = 0

FF = NULL

02 C1 07 = 6

02 C1 02 = 1



## Oracle Redo Logs

Binary file that keeps a record of changes (called redo entries) so in the event of a database failure all actions can be redone.

### Redo Entry

Contains all changes for a given SCN (System Commit number)

Has a header and one or more change vectors



## Change Vector operation codes

- 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

We can use these to determine what actions were taken



# INSERT Example

	Timestamp	INSERT Opcode	Object ID	
001d2800h:	01 22 00 00	94 0E 00 00 09 00 00 00	10 80 67 A1	; ."."......εg;
001d2810h:	AS 01 00 00	0D 37 00 00 84 42 08 00	05 00 5C C3	; .....7...B...Å
001d2820h:	00 00 00 00	32 00 10 00 00 00 01 00	02 00 00 00	; ....2.....
001d2830h:	02 00 00 00	00 00 02 00 84 42 08 00	00 00 80 00	; .....B...ε.
001d2840h:	02 01 B7 0B	3B 09 80 00 EA 00 17 00	6D 5C C0 00	; ...;.ε.ê...m\À.
001d2850h:	F9 67 CC 24	0B 02 01 00 01 00 00 00	8B 02 40 00	; ùgìs.....<.θ.
001d2860h:	64 3A 08 00	00 00 ED 00 02 00	57 00 0C 00	14 00; d:...i...W.....
001d2870h:	31 00 02 00	02 00 03 00 01 01 80 00	07 00 08 00	; 1.....ε.....
001d2880h:	2F 01 00 00	CC 09 80 00 C9 00 12 00	8B 02 40 00	; /...i.ε.é...<.θ.
001d2890h:	89 02 40 00	FF 12 02 01 01 00 C0 00	2C 01 03 00	; κ.θ.ÿ....À.,...
001d28a0h:	00 00 13 06	F9 FF 02 00 00 00 00 00	00 00 00 00	; ....ùÿ.....
001d28b0h:	00 00 00 00	0D 00 0B 01 00 00 00 00	00 02 01 00	; .....
001d28c0h:	C1 02 00 00	C1 05 C0 00 C2 09 31 00	05 02 1D 00	; Á...Á.À.À.1.....
001d28d0h:	02 00 FF FF	69 00 80 00 50 42 08 00	00 00 00 00	; ..ÿÿi.ε.PB.....
001d28e0h:	02 00 FF FF	04 00 20 00 08 00 00 00	2F 01 00 00	; ..ÿÿ.. ..../...
001d28f0h:	CC 09 80 00	C9 00 12 00 12 00 80 00	00 2E 72 33	; i.ε.é.....ε...r3
001d2900h:	00 00 00 00	00 00 00 00 05 01 1E 00	02 00 FF FF	; .....
001d2910h:	CC 09 80 00	50 42 08 00 00 00 BD 33	01 00 FF FF	; i.ε.PB...*3..ÿÿ
001d2920h:	0A 00 14 00	48 00 1C 00 14 00 BD 33	80 00 4C 17	; ....H.....*3ε.L.
001d2930h:	12 00 FF FF	07 00 08 00 2F 01 00 00	C9 00 12 00	; ..ÿÿ..../...É...
001d2940h:	57 00 00 00	57 00 00 00 00 00 00 00	00 00 00 00	; W...W.....
001d2950h:	0B 01 08 00	08 04 01 00 CC 09 80 00	C9 00 11 00	; .....i.ε.é...
001d2960h:	48 3C 08 00	00 00 FF FF 56 3C 08 00	00 00 1C 00	; H<...ÿÿv<.....
001d2970h:	32 00 10 00	82 42 08 00 00 00 00 00	CA 09 80 00	; 2...,B.....É.ε.
001d2980h:	00 00 00 00	36 00 00 00 04 01 00 00	06 00 00 00	; ....6.....
001d2990h:	20 01 00 00	58 2C 80 00 B8 00 4C 00	00 80 00 00	; ...X,ε.^.L.ε..
001d29a0h:	DB FC 07 00	8F 02 40 00 89 02 40 00	FF 12 03 01	; Ôü...<.θ.κ.θ.ÿ...
001d29b0h:	01 00 C0 00	0F 01 00 00 A8 00 00 00	01 00 00 00	; ..À.....

User ID Undo Opcode Undo Header Opcode



## Time stamp

Timestamp is when the redo entry was written – not when the action was taken.

Records to the second from midnight of 1<sup>st</sup> January 1988.



## DDL Example

```

01fd7e00h: 01 22 00 00 BF FE 00 00 82 00 00 00 2C 80 32 13 ; ."..zþ.,.,,€2.
01fd7e10h: 09 00 00 00 02 00 00 00 A3 0C 80 00 1A 03 15 00 ; .....£.€.....
01fd7e20h: 02 00 F4 03 01 0C 53 07 5D AD F6 45 F4 00 00 00 ; ..ô...S.]-öEô...
01fd7e30h: 01 03 00 00 1F 06 3A 00 01 00 06 07 00 00 00 00 ; .....:.....
01fd7e40h: C5 0C 25 02 18 01 00 00 00 00 00 00 00 00 00 00 ; Å.š.....
01fd7e50h: 00 00 00 00 00 00 4A 08 00 06 B3 60 1E 00 18 00 ; .....J...³`....
01fd7e60h: 05 00 03 00 0C 00 00 00 02 00 02 00 46 00 0F 00 ; .....F...
01fd7e70h: 00 00 14 00 00 00 00 00 00 00 4A 08 10 27 00 00 ; .....J..'..
01fd7e80h: 06 00 0C 00 2E 06 00 00 33 00 00 00 00 00 01 00 ; .....3.....
01fd7e90h: 01 00 00 00 53 43 4F 54 54 38 03 C2 53 59 53 C1 ; ...SCOTT8.ÅSYSÁ
01fd7ea0h: 58 00 00 00 00 00 00 00 00 00 00 00 00 00 38 03 ; X.....8.
01fd7eb0h: 02 00 52 02 63 72 65 61 74 65 20 75 73 65 72 20 ; .R.create user
01fd7ec0h: 77 69 67 67 79 77 69 67 67 79 77 69 67 67 79 20 ; wiggrywiggrywigg
01fd7ed0h: 69 64 65 6E 74 69 66 69 65 64 20 62 79 20 20 56 ; identified by V
01fd7ee0h: 41 4C 55 45 53 20 27 32 46 41 31 37 34 39 44 36 ; ALUES '2FA1749D6
01fd7ef0h: 39 38 41 44 38 37 34 27 20 00 61 3C 57 49 47 47 ; 98AD874' .a<WIGG
01fd7f00h: 59 57 49 47 47 59 57 49 47 47 59 C5 00 00 00 00 ; YWIGGYWIGGYÅ....
01fd7f10h: 33 00 00 00 00 00 00 00 00 00 00 00 FF FF 10 07 ; 3.....ÿÿ..
    
```



## Evidence of SELECTs

No object is created or dropped

No transaction occurs

- Automatic Workload Repository
- The Cost-Based Optimizer
- Fixed view V\$SQL



## Cost Based Optimizer - CBO

Whenever a query is executed it is compiled into execution plan.

The most efficient way to do this is handled by the Cost Based Optimizer (CBO)

Attempts to reduce system resources required

Statistics about the CBO are kept by the System Monitor background process

Stored in COL\_USAGE\$



## Cost Based Optimizer – COL\_USAGE\$

OBJ#	NUMBER
INTCOL#	NUMBER
EQUALITY_PREDS	NUMBER
EQUIJOIN_PREDS	NUMBER
NONEQUIJOIN_PREDS	NUMBER
RANGE_PREDS	NUMBER
LIKE_PREDS	NUMBER
NULL_PREDS	NUMBER
TIMESTAMP	DATE

Predicates are the "where" clause...



## Cost Based Optimizer – COL\_USAGE\$

Compare with copies of this table against backups

Look for “odd” entries

- e.g. no company application ever looks at table X but it's in COL\_USAGE\$



# Cost Based Optimizer – COL\_USAGE\$

```
SQL> ALTER SESSION SET NLS_DATE_FORMAT = 'YYYY-MM-DD
      HH24:MI:SS';
```

```
SQL> SELECT OBJ#, INTCOL#, LIKE_PREDS, EQUALITY_PREDS,
      RANGE_PREDS, TIMESTAMP FROM SYS.COL_USAGE$;
```

OBJ#	INTCOL#	LIKE_PREDS	EQUALITY_PREDS	RANGE_PREDS	TIMESTAMP
21	14	0	0	0	2007-07-31 00:39:43
145	1	0	2	0	2007-07-31 18:04:13
166	1	0	2	0	2007-07-31 18:04:13
222	1	0	2	0	2007-07-31 18:04:13
226	1	0	2	0	2007-07-31 18:04:13
228	1	0	2	0	2007-07-31 18:04:13
233	2	0	0	0	2007-07-31 18:04:13
243	2	0	2	0	2007-07-31 18:04:13
249	6	0	2	2	2007-07-31 18:04:13
253	3	0	1	0	2007-07-31 00:39:43
253	6	0	1	0	2007-07-31 00:39:43

OBJ#	INTCOL#	LIKE_PREDS	EQUALITY_PREDS	RANGE_PREDS	TIMESTAMP
702	14	0	1	0	2007-07-31 00:54:48



## Automatic Workload Repository

Records SQL that takes a “long time” to execute...

WRH\$\_ACTIVE\_SESSION\_HISTORY

WRH\$\_SQLTEXT

WRH\$\_SQLSTAT



## Automatic Workload Repository

```
SQL> SET LONG 2000000
```

```
SQL> SELECT ST.PARSING_SCHEMA_ID, TX.SQL_TEXT FROM  
WRH$_SQLSTAT ST, WRH$_SQLTEXT TX WHERE TX.SQL_ID =  
ST.SQL_ID;
```



## V\$SQL Fixed View

**Resident in memory so won't be there if the database is shutdown**

```
SQL> SELECT PARSING_USER_ID, PARSING_SCHEMA_ID,  
           PARSING_SCHEMA_NAME, LAST_ACTIVE_TIME, SQL_TEXT FROM  
           V$SQL;
```



Questions?





**Thank You**

<http://www.ngsconsulting.com/>

