



DES 数据库取证分析大师系统
用户手册

南京西数科技有限公司版
权所有 侵权必究
20210121

目录



《西数 DES 数据库取证分析大师系统使用手册》

目录

- 一： 产品简介 1
 - 1.1 软件名称 1
 - 1.2 软件系统要求 1
 - 1.3 软件功能 1
 - 1.4 软件特点： 1
- 二、软件注册与安装 1
 - 2.1 软件安装 1
 - 2.2 软件注册 2
- 三、软件功能组件与设置 3
 - 3.1 初始界面 3
 - 3.2 加载 EXP/DP 按钮..... 3
 - 3.3 加载 DBF 按钮..... 4
 - 3.4 加载磁盘功能 5
 - 3.5 加载镜像功能 5
 - 3.6 远程协助 5
 - 3.7 文件上传 5
 - 3.8 系统设置 6
 - 3.9设置参数功能 6
- 四、恢复损坏 ORACLE 的备份文件（DMP） 7
 - 4.1 加载 DMP 文件 7
 - 4.2 解析 DMP 文件 7
 - 4.3 查看表数据..... 8
 - 4.4 设置导出环境..... 10

2

4.5 导出表数据到 ORACLE 数据库中.....	11
4.6 导出表数据为脚本文件.....	13
4.7 查询已恢复的表数据.....	14
五、恢复损坏 ORACLE 实体库文件 (DBF)	17
5.1 加载 DBF 文件.....	17
5.2 解析 DBF 文件.....	18
5.3 查看表数据.....	20
5.4 设置导出环境.....	20
5.5 导出表数据.....	20
5.6 查询已恢复的表数据.....	21
六、关于.....	22
6.1使用说明.....	22
6.2技术论坛.....	22
6.3自动更新.....	22
6.4关于我们.....	23

《西数 DES 数据库取证分析大师系统使用手册》

免责声明：请用户在查阅本手册后了解并清楚本软件的各项功能，本公司对于因硬件故障、硬盘误操作，产品维修或者其他意外情况引起的个人数据丢失和损坏不负任何责任，也不对由此造成的其他间接损失承担责。同时我们也无法控制用户对本说明书阐明的产品使用功能和用途产生误解或者有侵犯隐私权或者法律的纠纷面而承担任何责任，也不对因使用本产品而引起的第三方索赔负责。

一：产品简介

1.1 **软件名称**：西数 DES 数据库取证分析大师系统（英文名：Oracle Extractor）

1.2 **软件系统要求**：Windows 32/64 位

1.3 **软件功能**：本产品用于 Oracle 数据库文件的解析，将损坏数据库导出为正常数据库等功能。常用于数据库 DBF\DMP 文件由于物理硬盘、病毒攻击、文件意外损坏等情况下的数据恢复，支持 DBF 碎片级别的数据库恢复，并支持多版本的 Oracle 数据库解析，支持快速导入，支持多种字符集等。

1.4 软件特点：

- 1.4.1、支持各版本 ORACLE 的 DMP\DBF 数据库文件解析。
- 1.4.2、支持硬盘物理损坏、勒索病毒攻击、页损坏等数据库文件解析。
- 1.4.3、支持一键将表以及其他数据导入 ORACLE 实体库。
- 1.4.4、支持一键将所有数据库导出为脚本文件形式。
- 1.4.5、支持 Oracle 各种类型的字符集。
- 1.4.6、支持 DBF\DMP 碎片恢复。
- 1.4.7、支持文件系统镜像碎片扫描，收集数据库碎片。
- 1.4.8、支持多版本数据库快速导入数据。

二、软件注册与安装

2.1 软件安装

下图为程序解压后的文件，无需任何安装步骤，双击运行红色框标记的主程序 EXE 文件即可。如图 2.1

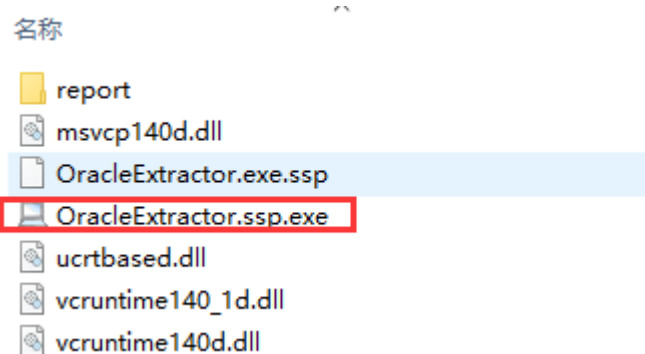


图 2.1

2.2 软件注册

本软件配备了 USB 加密狗程序，如需使用，需要购买加密狗后，插入主机，安装加密狗自带的软件驱动，程序会自动匹配加密狗密钥，双击运行主程序即可。加密狗如下图2.2



图 2.2

三、软件功能组件与设置

3.1 初始界面如图 3.1

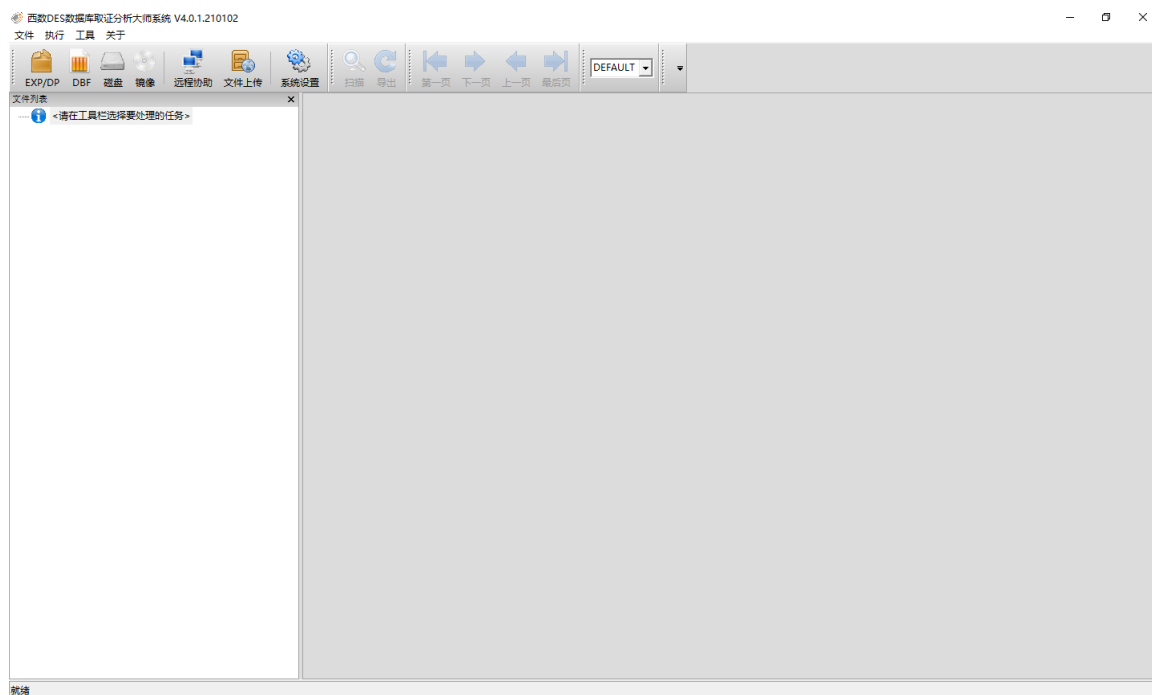


图 3.1

3.2 加载 EXP/DP 按钮，单击此按钮，提示选择框，选择故障 DMP 文件。

如图 3.1.1 与 3.1.2

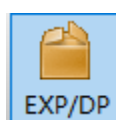


图 3.1.1

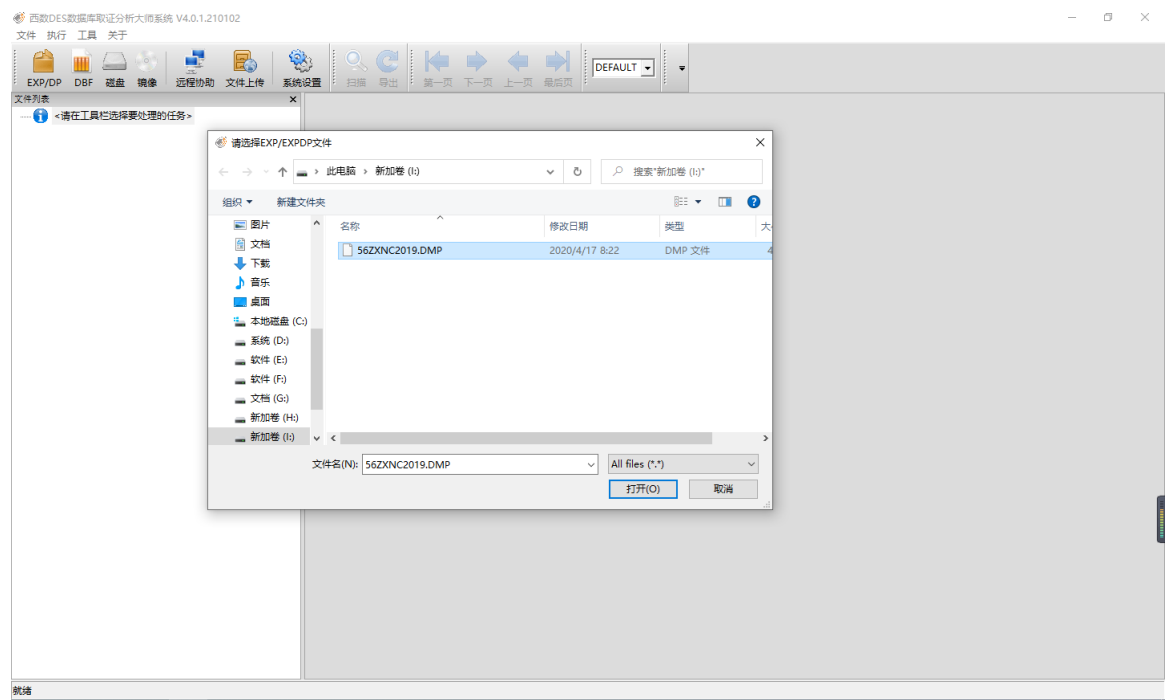


图3.1.2

3.3 加载 DBF 按钮, 单击此按钮, 提示选择框, 选择 DBF 所在的文件夹目录, 如 DBF 文件在 D:\XX\XX.DBF, 仅需要选中 XX 文件夹即可, 程序自动加载文件夹下面的相关文件。

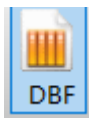


图3.3.1

如图3.3.2、3.3.3

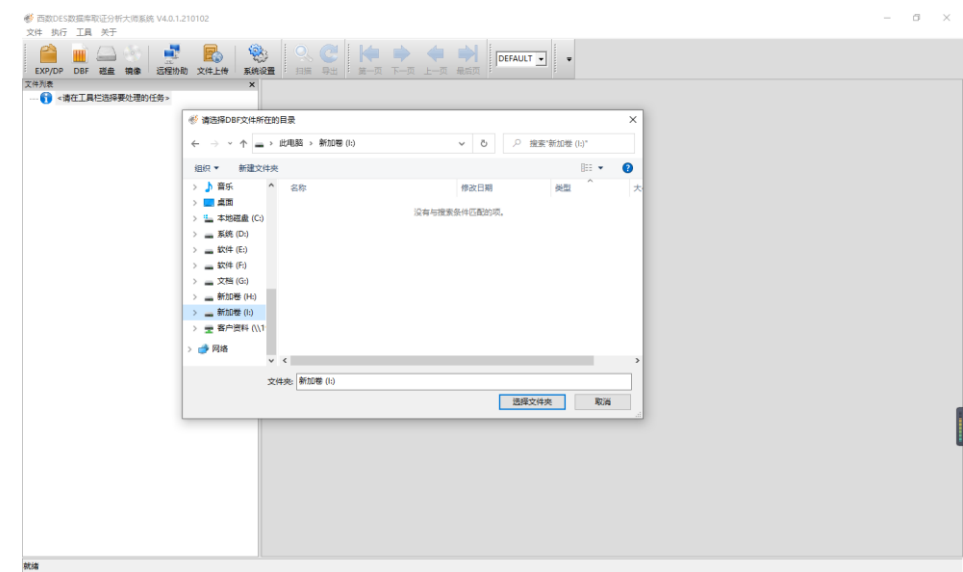


图 3.3.2

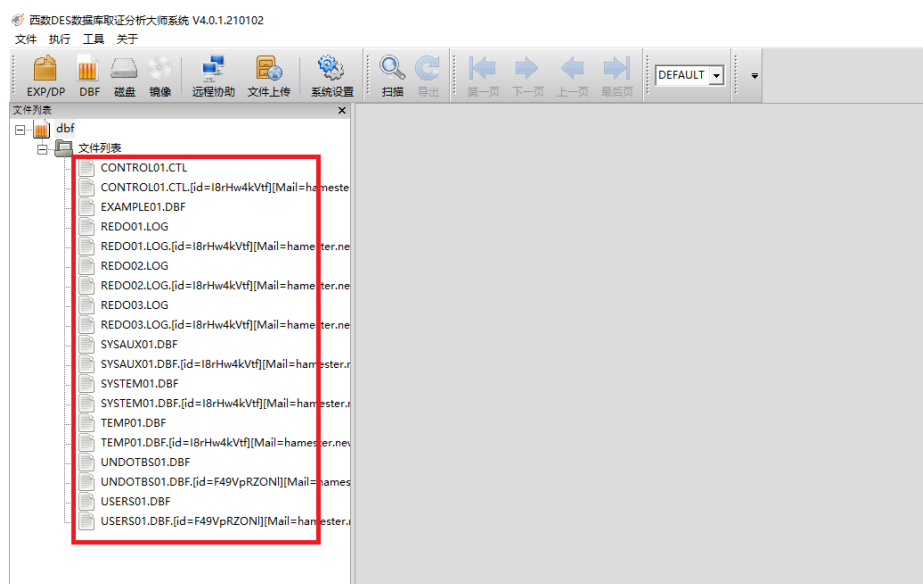
图3.3.3

3.4 **加载磁盘功能**，此功能为加载当前设备所连接的物理存储，点击后，提示需要选中恢复的物理硬盘。此功能等待后续开放。如图 3.4.1



图 3.4.1

3.5 **加载镜像功能**，此功能为加载镜像文件，镜像文件可以是文件或者硬盘形式，点击后，提示需要选中恢复的镜像文件或磁盘。此功能等待后续开放。如图



3.5.1

图 3.5.1

3.6 **远程协助**，点击后，自动连接官方网站，可以获取官方联系方式或者技术支持服务。如图 3.6.1

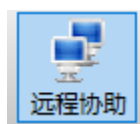


图 3.6.1

3.7 **文件上传**，点击后，将自动跳转到官方网站，获取文件上传方



式、账号、口令等信息。如图 3.7.1

图 3.7.1

3.8 系统设置，点击此按钮，显示对程序的相关设置选项，根据使用情况、机器配置、用户需求等进行自定义设置。如图：3.8.1、3.8.2



图 3.8.1

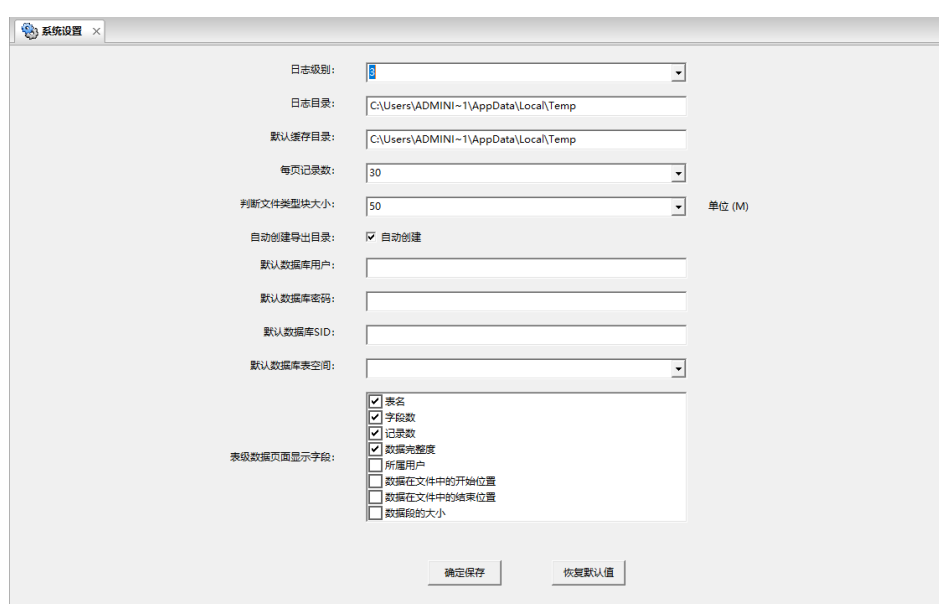


图 3.8.2

3.9设置参数功能：

(1) 日志级别：分为 0-4 级别，0 为最快，生成的日志文件大小较小，内容较少，4 为最慢，生成的日志文件较大，内容较多。默认为 3 即可，如遇到特殊案例，需要特别分析，需要将日志级别调大，便于定位故障。

(2) 日志目录：一般默认即可，可以自定义，用于记录当前解析案例的记录。

(3) 默认缓存目录：设置为空间较大的存储分区。

(4) 每页记录数：用于显示每页数据表的记录条数。设置越大，显示数量越多。

(5) 判断文件类型块大小：设置越小，判断越精确，但速度较慢，一般默认即可。

(6) 自动创建导出目录：便于分辨不同的数据库恢复目录。默认。

(7) 默认数据库用户：默认用户为用户自定义创建的用户名，根据恢复的故障数据库进行对应，数据库解析后会显示用户名及其用户名下面的表数据，手动输入需要恢复的对应的用户名即可。

(8) 默认数据库密码：用户在建立用户名的时候所设置的密码，可以自行在 oracle 环境中更改与重新创建。

(9) 默认数据库 SID：用户在 ORACLE 环境中登陆所需要的服务器 SID，如默

认的ORACLE 环境的 SID 为：ORCL。

(10) 默认数据库的表空间：用户在导出数据表的时候，程序会自动创建表空间或者默认使用当前 ORACLE 环境中的表空间。

(11) 表级数据页面显示字段：根据数据需求，界面处设置显示所需要的字段内容，表数据一般需要表名、字段数、记录数、数据库完整度勾选，其他根据需求勾选。

四、恢复损坏 ORACLE 的备份文件（DMP）

4.1 加载 DMP 文件

4.1.1 单机 EXP/DP 按钮，跳出选择 DMP 的选择窗口，双击选中需要解析的 DMP 文件，如图 4.1.1

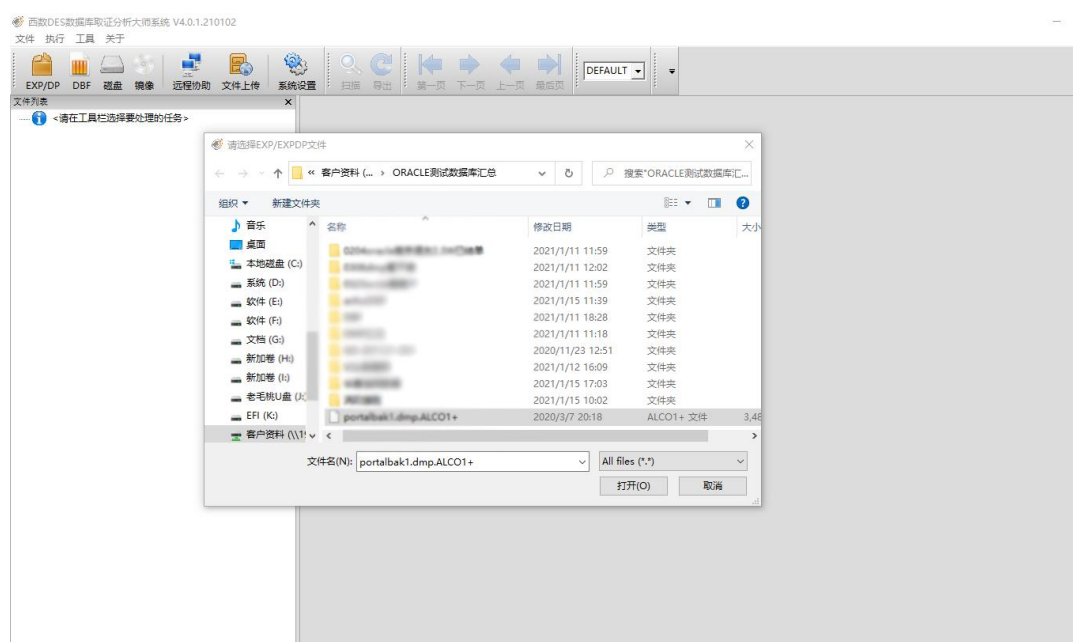


图 4.1.1

4.2 解析 DMP 文件

4.1.2 双击选中后，程序会自动开始执行扫描解析程序，如图 4.1.2。等待扫描结束即可。右侧显示完整的数据解析进度与日志。如图 4.1.3

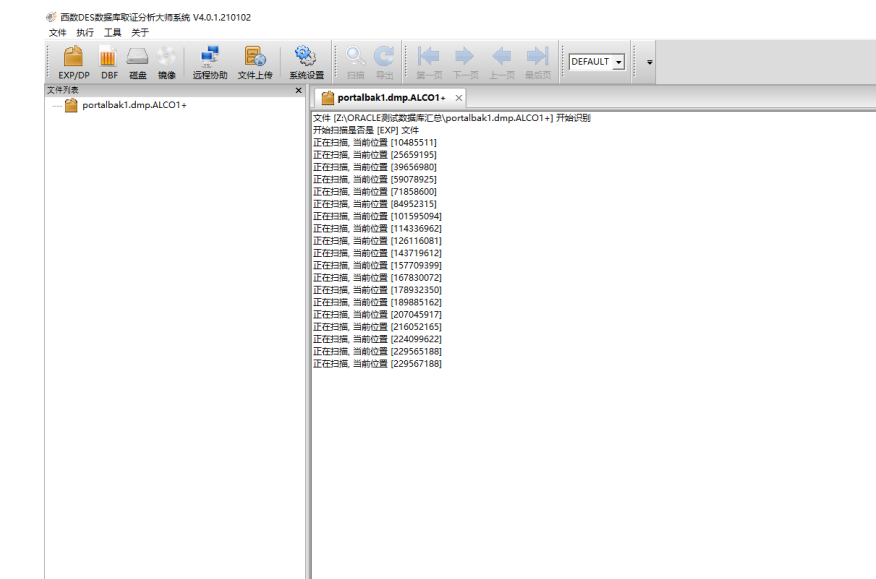


图 4.1.2

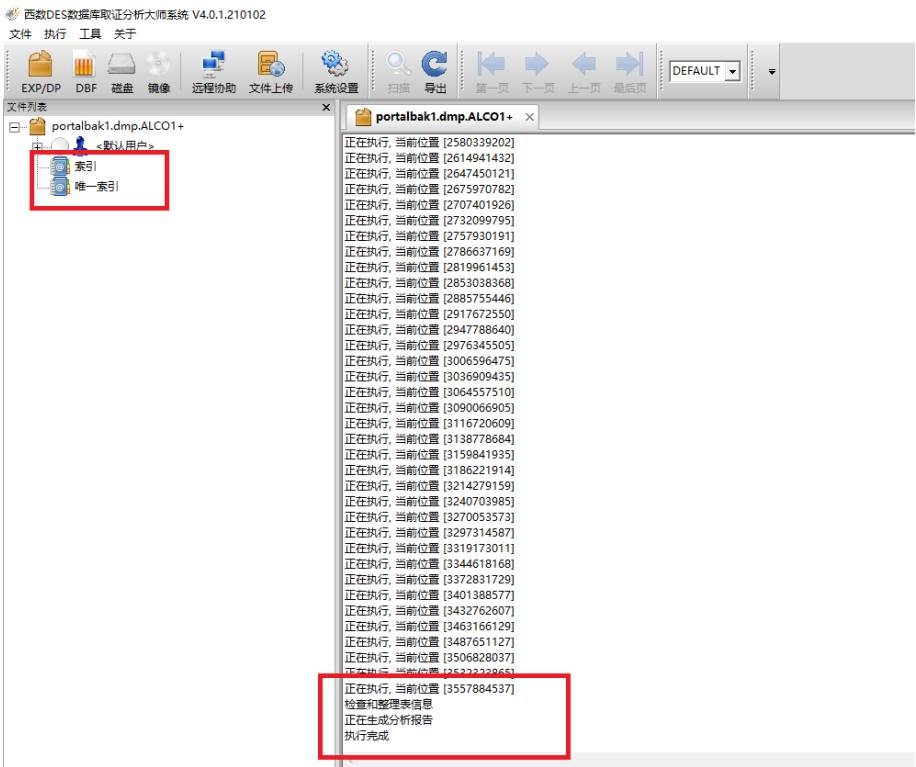


图 4.1.3

4.3 查看表数据

4.3.1 左侧列出 DMP 中所有的数据集, 包含表、视图、索引、唯一索引、序列、存储过程、触发器。如图 4.3.1

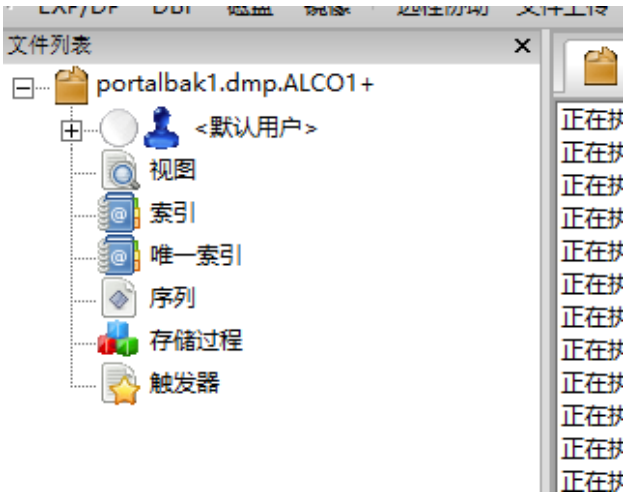
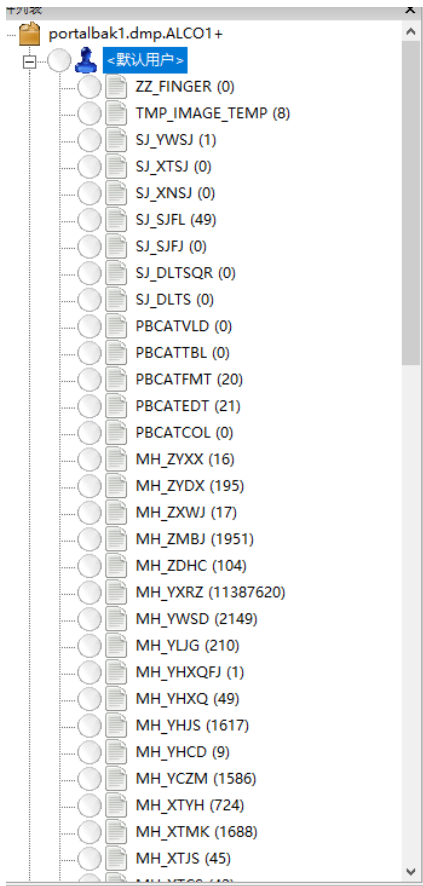


图 4.3.1

4.3.2 展开默认用户左侧 + 号, 即可看见所有的表, 如图 4.3.2.1.双击表名,



右侧可以预览选中的表数据。如图 4.3.2.2

图 4.3.1

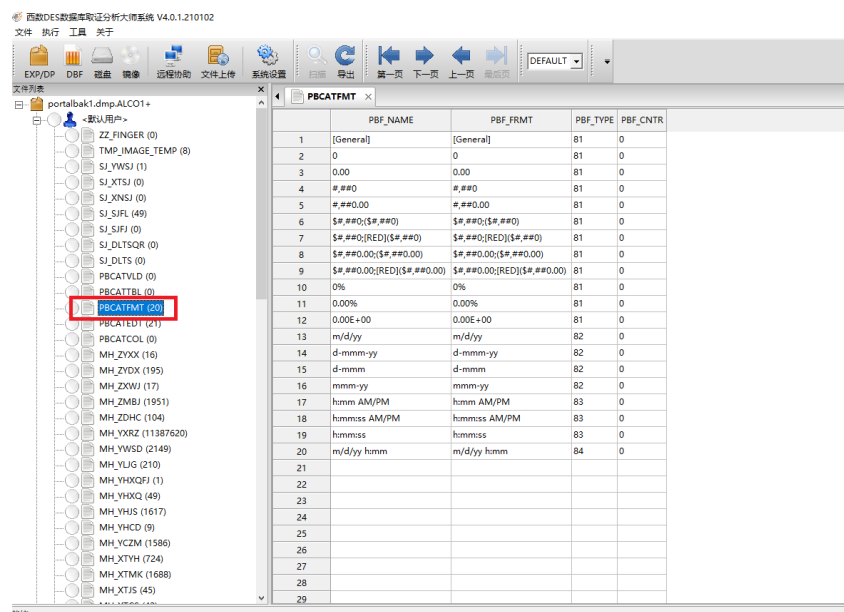


图 4.3.2.2

4.4 设置导出环境

4.4.1 打开工具栏上的导出按钮，调出导出设置界面，如图 4.4.1.1.

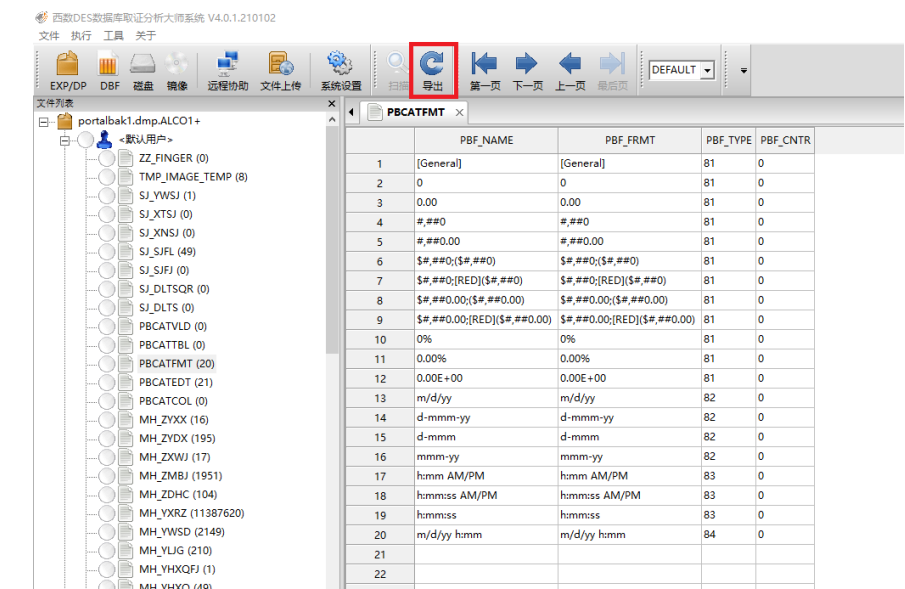


图 4.4.1.1

目标：导出为脚本文件形式或者导入到目标 ORACLE 数据库环境中。

目标： ☒ 文件 ☐ 数据库

范围：全部导出包含表、视图等其他数据，已选择的仅仅导出选中的数据。

范围： ☒ 全部 ☐ 已选择的

类型：根据用户需求，选中。

类型： ☒ 表 ☐ 视图 ☐ 索引 ☐ 存储过程 ☐ 函数 ☐ 序列 ☐ 触发器

存储/缓存目录：导出时需要用到的临时存放的文件目录或者是导出为文件时候存放脚本的目录。

存储/缓存目录： H:\test

选项：忽略记录数为 0 的表，不导出没有数据的表。导出 SQL 脚本，勾选后，导出的文件数据后，自动生成可执行的 bat 脚本，方便用户导入。

选项： ☐ 忽略记录数为0的表 ☐ 导出SQL脚本

4.5 导出表数据到 ORACLE 数据库中

4.5.1 在左侧表名中，选中需要导出的表名，设置好导出的参数(导出之前，必须先 在ORALE 中建立对应的ORACLE 用户和密码，用于存储导出的表或者其他所有数据，本例用户名为 TEST,密码 123,SID:ORCL), 点击导出，右侧会显示导出进度与当前导出的表。如图 4.5.1.1、4.5.1.2.

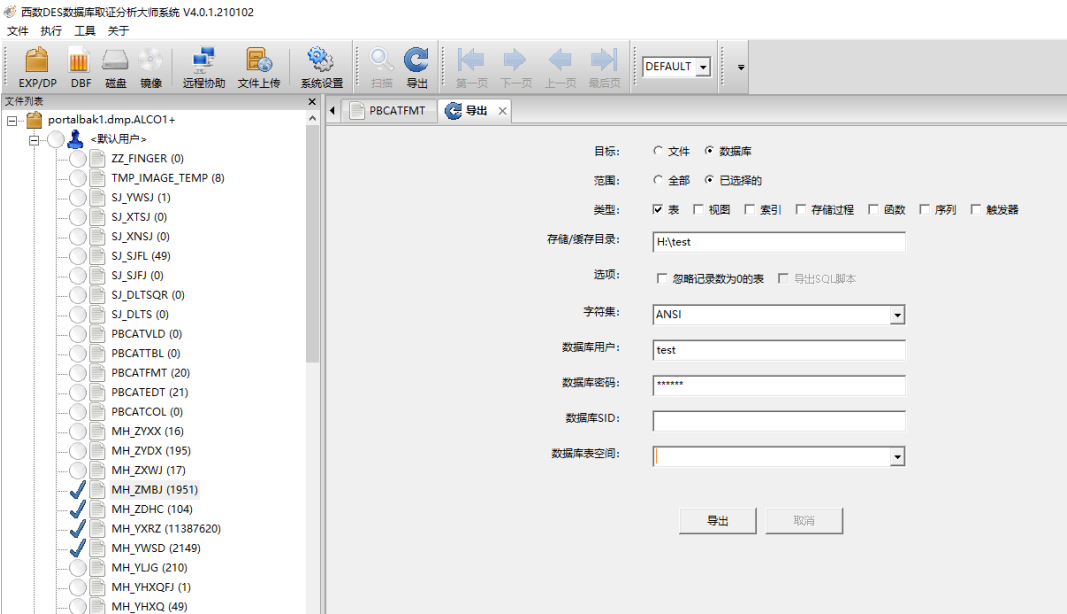


图 4.5.1.1

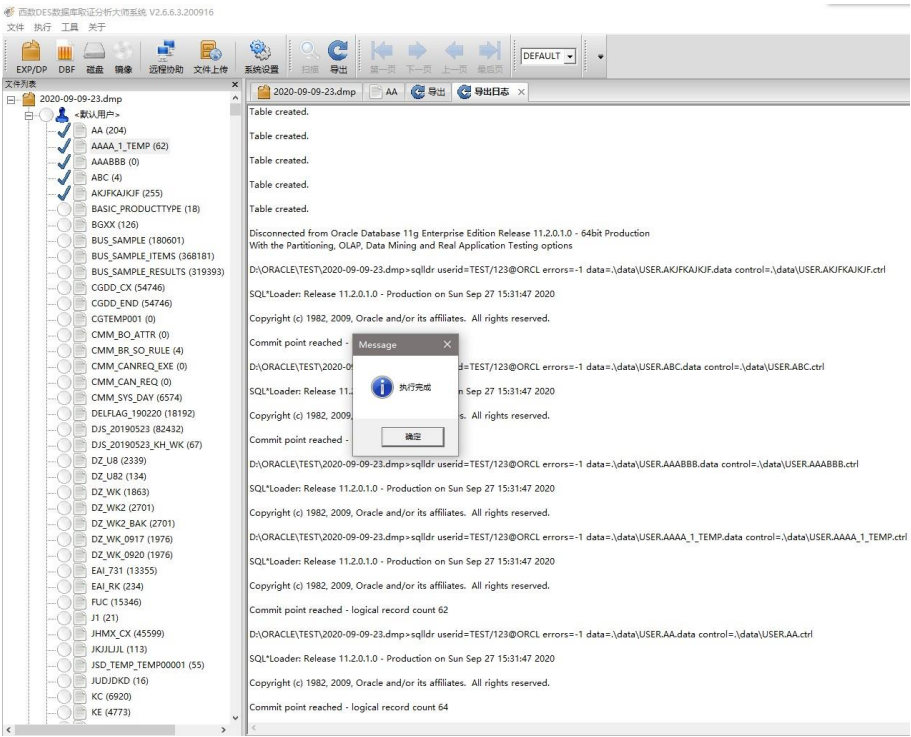


图 4.5..1.2

4.6 导出表数据为脚本文件

4.6.1 导出为脚本文件，双击运行 db 即可自动导入数据，导出的参数设置图：4.6.1.2

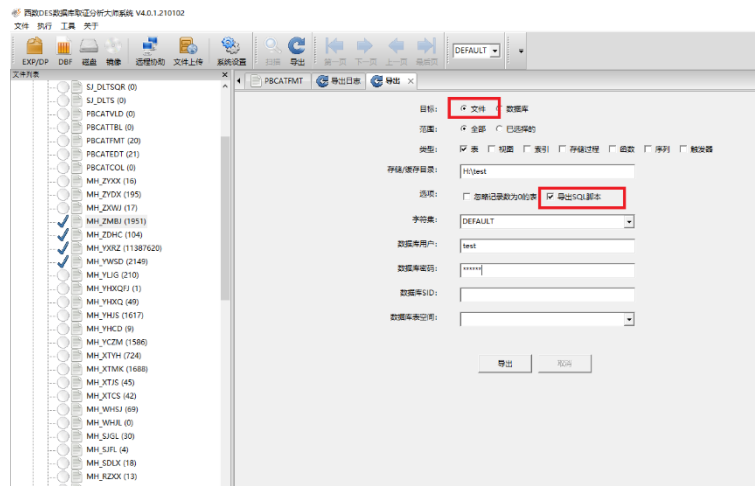


图 4.6.1.2

4.6.2.运行脚本文件导入数据库。如图 4.6.2.1， 4.6.2.2

新加卷 (H:) > test > portalbak1.dmp.ALCO1+				搜索"portal"
名称	修改日期	类型	大小	
data	2021/1/16 17:51	文件夹		
lob	2021/1/16 17:53	文件夹		
db	2021/1/18 13:27	Windows 批处理...	1 KB	
tables	2021/1/18 13:27	Microsoft SQL S...	1 KB	
USER.MH_YWSD	2021/1/18 13:27	文本文档	1 KB	
USER.MH_YXRZ	2021/1/18 13:27	文本文档	1 KB	
USER.MH_ZDHC	2021/1/18 13:27	文本文档	1 KB	
USER.MH_ZMBJ	2021/1/18 13:27	文本文档	1 KB	
USER.SJ_SJFJ	2021/1/16 17:54	文本文档	0 KB	
USER.SJ_SJFL	2021/1/16 17:54	文本文档	1 KB	
USER.SJ_XNSJ	2021/1/16 17:54	文本文档	1 KB	
USER.SJ_XTSJ	2021/1/16 17:54	文本文档	1 KB	
USER.SJ_YWSJ	2021/1/16 17:53	文本文档	1 KB	
USER.TMP_IMAGE_TEMP	2021/1/16 17:53	文本文档	1 KB	
USER.ZZ_FINGER	2021/1/16 17:53	文本文档	1 KB	

图 4.6.2.1

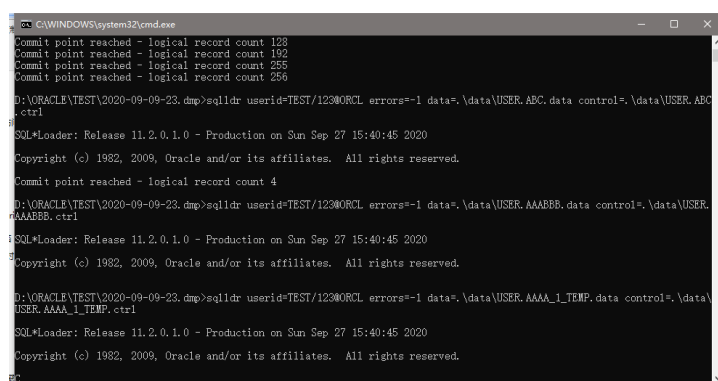


图 4.6.2.2

4.7 查询已恢复的表数据

4.7.1 可以利用相关 ORACLE 辅助工具进行数据表查询，这里采用 NAVICAT 进行数据查询。如图 4.7.1

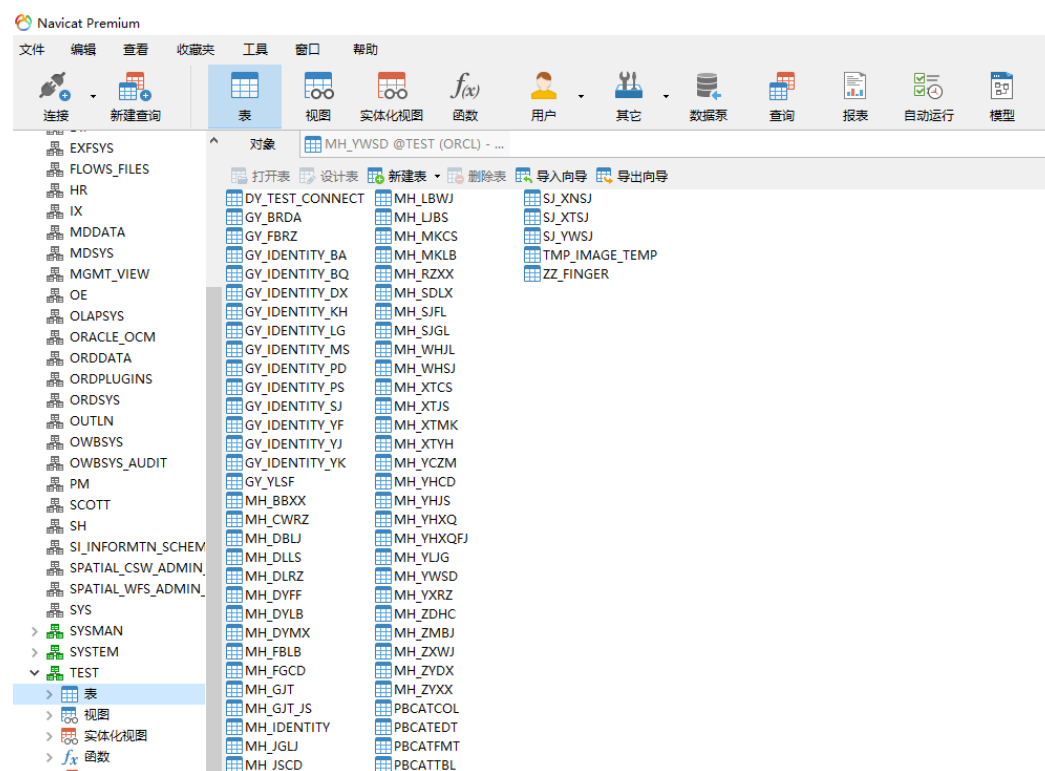


图 4.7.1

4.7.2 利用查询语句查询表数据，如图 4.7.2

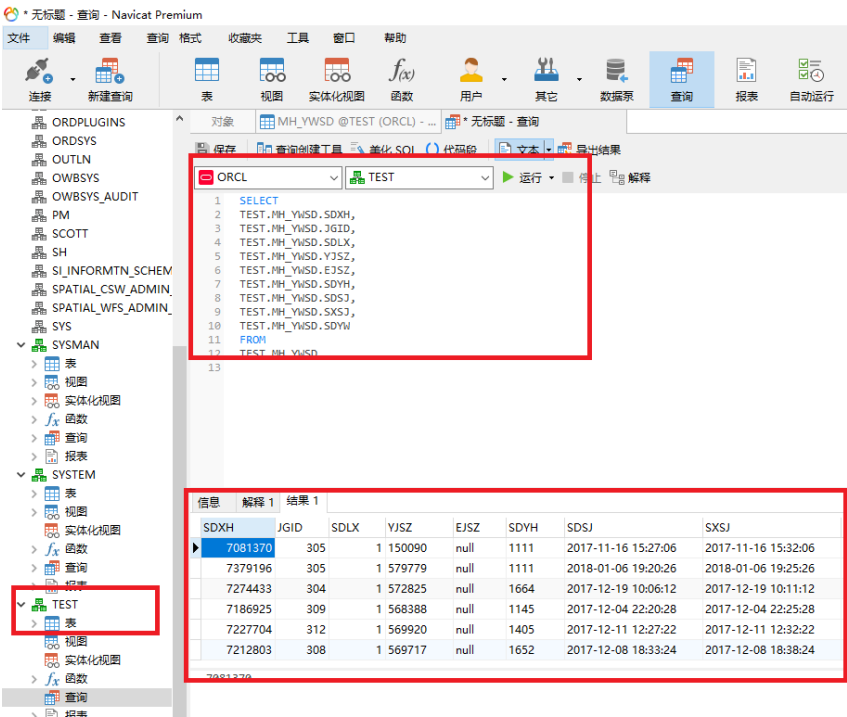


图 4.7.2

4.8 表数据的多种排序方式，如图 4.8

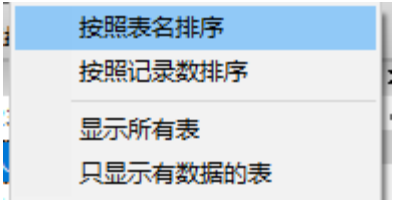


图 4.8

4.8.1 按照表名进行排序，按照 ABCDEF 等字母顺序进行排序。如图 4.8.1.1

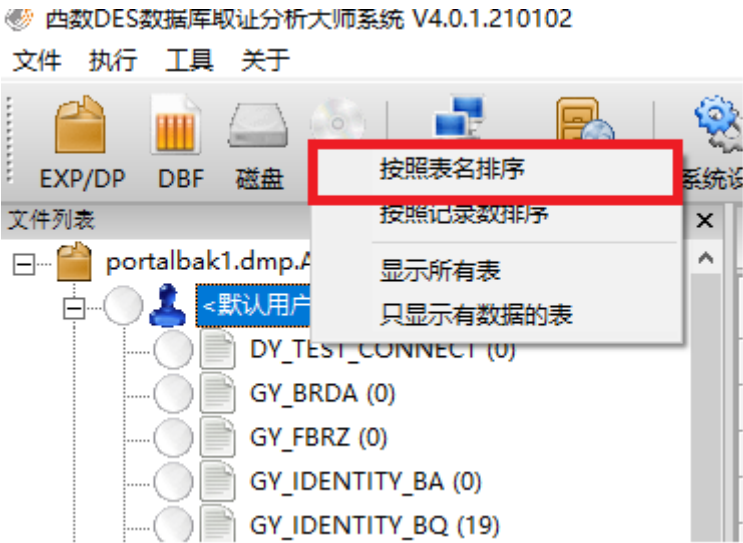


图 4.8.1.1

4.8.1 按照记录数进行排序，按照表记录数据从大到小排序。如图 4.8.1.2

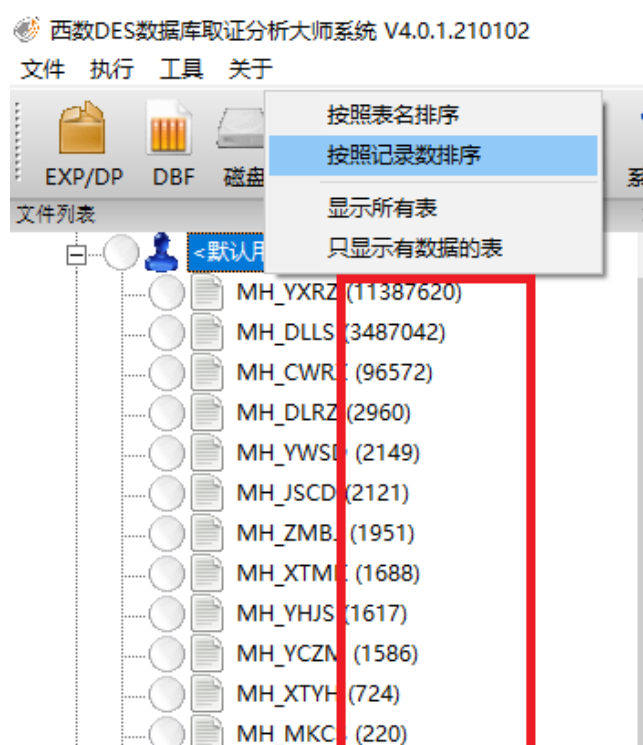
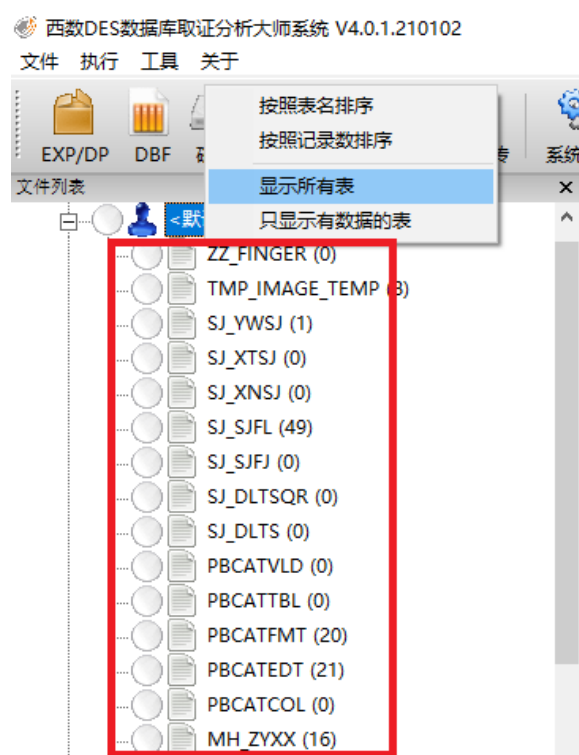


图 4.8.1.2



4.8.2 显示所有表，显示所有有数据和无数据的表。如图 4.8.1.3

图 4.8.1.3

4.8.3 只显示有数据的表， 只显示有数据记录的表名。如图 4.8.1.4

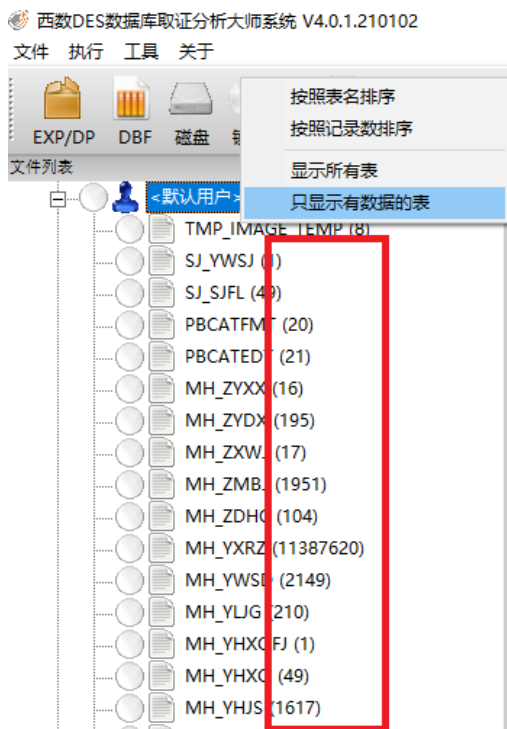


图 4.8.1.4

五、恢复损坏 ORACLE 实体库文件（DBF）

5.1 加载 DBF 文件

5.1.1 选中 DBF 所在的文件夹，例如：D:\ORACLE\DATA\XX.DBF， 仅需选中 DATA 文件夹即可，程序会自动判断 DBF 文件，并将相关文件加入到程序要解析的列表中。
如图： 5.1.1

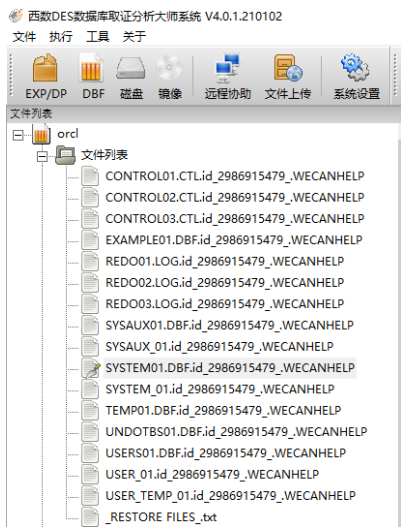


图 5.1.1

5.1.1 设置系统 DBF 文件, 一般这类文件为 SYSTEM01.DBF, 由于有些客户自定义了系统文件, 需要用户自行判断, 比如下图: 5.1.2、5.1.3

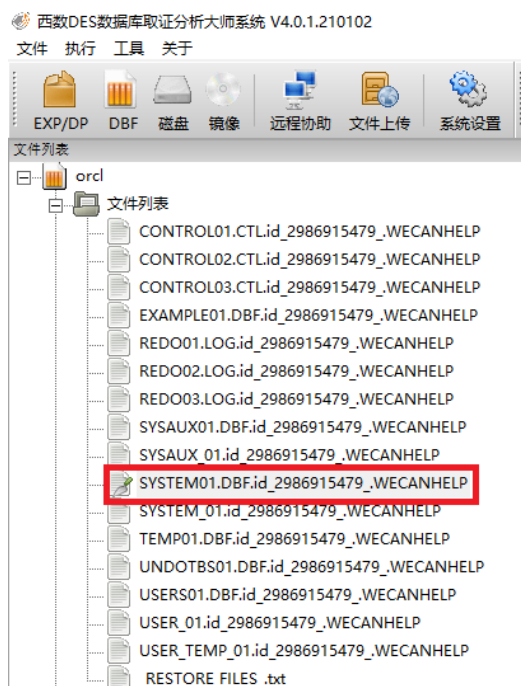


图 5.1.2

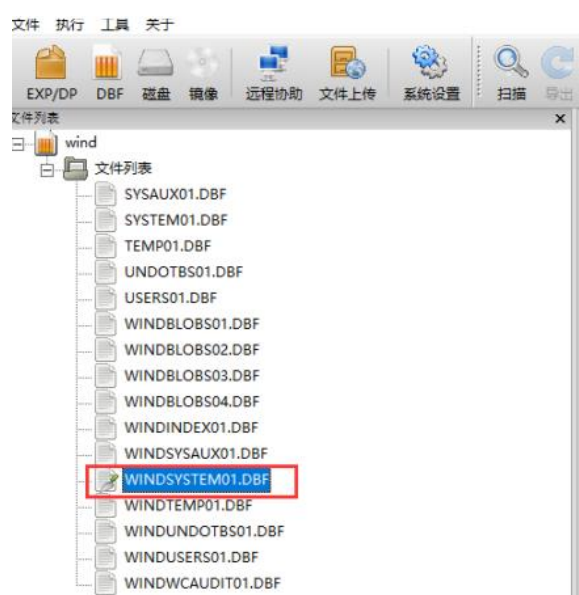


图 5.1.3

5.2 解析 DBF 文件

5.2.1 设置好系统 DBF 文件以后，点击工具栏上的扫描按钮，程序会自动进行扫描，右侧会显示具体的扫描进度。如图 5.2.1.1、5.2.1.2

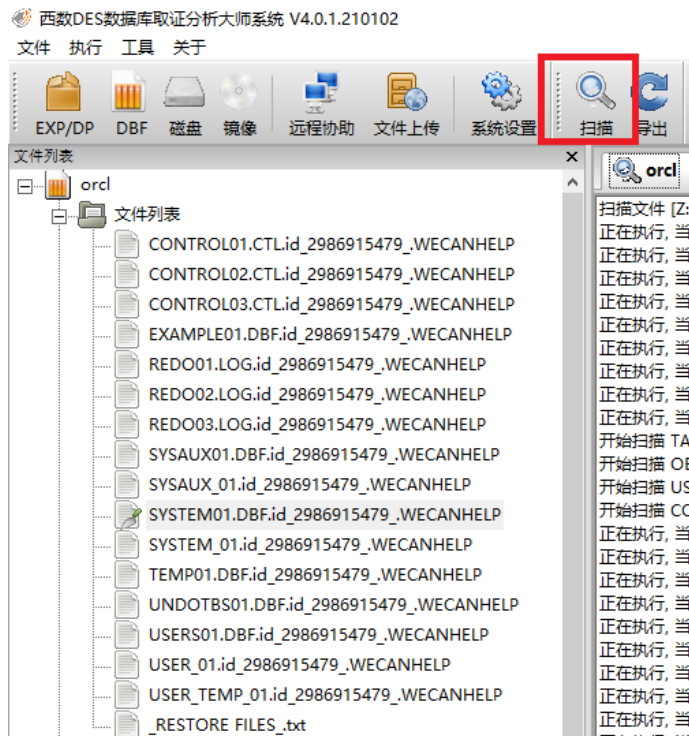


图 5.2.1.1

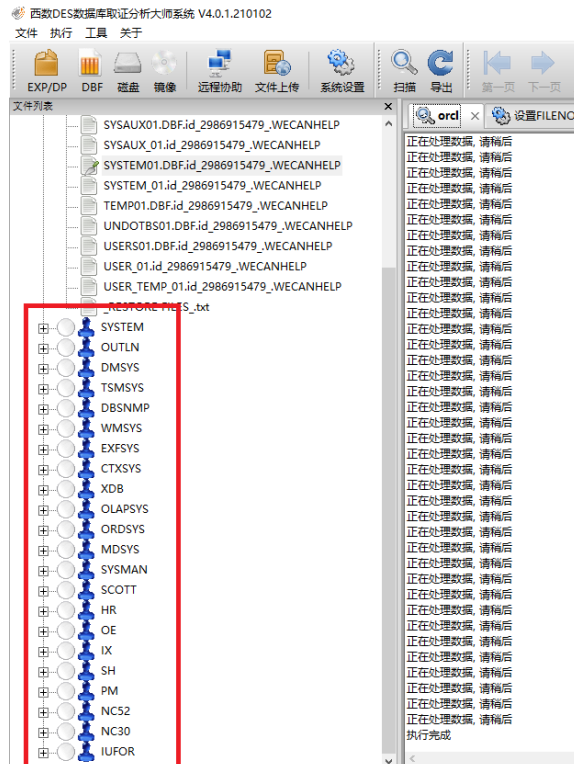


图 5.2.1.2

5.3 查看表数据

展开默认用户左侧 + 号，即可看见所有的表。如图 5.3

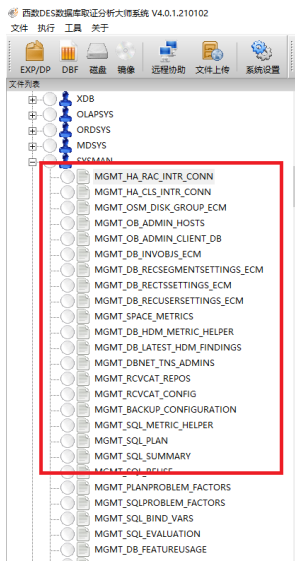


图 5.3

5.4 设置导出环境,

打开工具栏上的导出按钮，调出导出设置界面。如图 5.4.



图 5.4

5.5 导出表数据

运行脚本文件导入数据库。如图 5.5.1, 5.5.2, 5.5.3

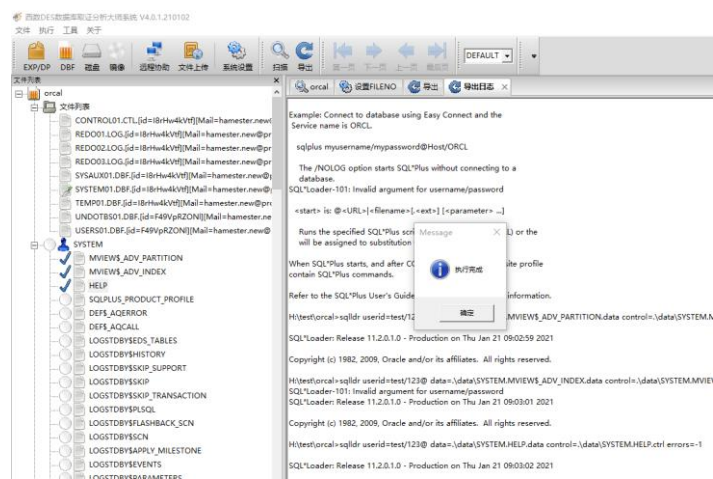


图 5.5.1

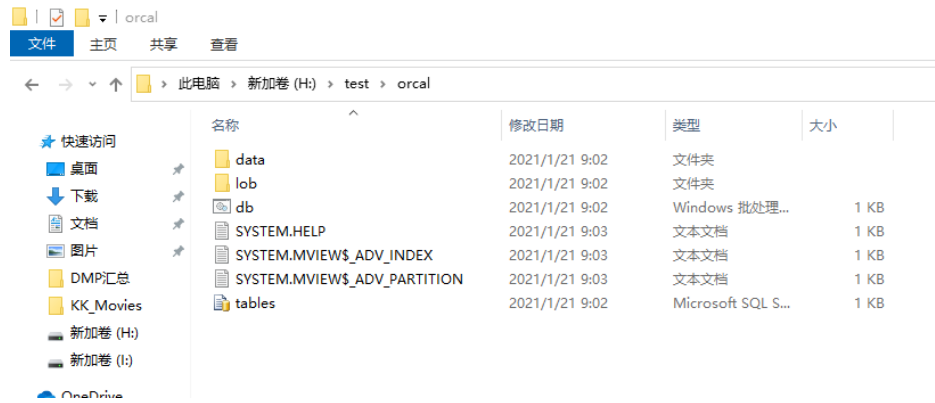
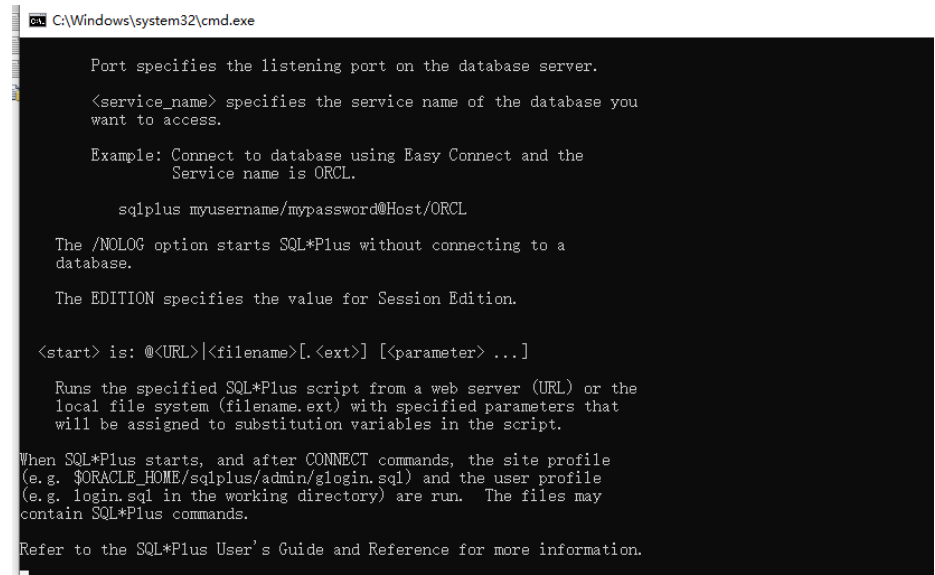


图 5.5.2



5.5.3

5.6 查询已恢复的表数据

可以利用相关 ORACLE 辅助工具进行数据表查询，这里采用 NAVICAT 进行数据查询。如图 5.6

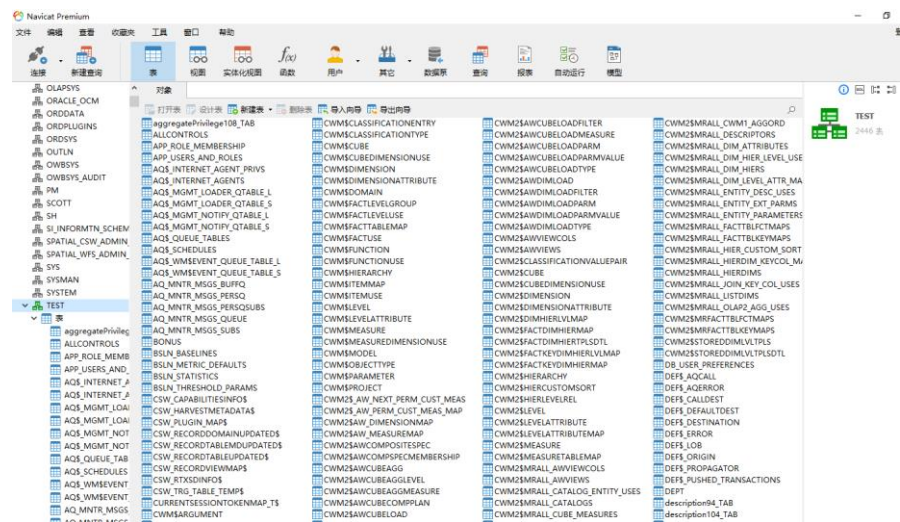


图 5.6

六、关于

6.1 使用说明

使用说明自动连接到官方网站，可以获取使用手册以及技术支持方面的资料。

6.2 技术论坛

技术论坛自动连接到官方网站论坛，论坛可以发帖，提问，互动等进行技术交流。

6.3 自动更新

程序自动更新，无需手动，可以第一时间使用到最新版本的程序。

6.4 关于我们



南京西数科技有限公司
20210121