

بسمه تعالی

رویدادنگاری، ممیزی و جرم‌شناسی در

پایگاه داده‌ی MSSQL

## فهرست مطالب

۱	مقدمه	۳
۲	نحوه‌ی ثبت وقایع در پایگاه داده MSSQL	۳
۲-۱	انواع فایل‌های رویدادنگاری	۴
۲-۱-۱	فایل رویدادنگار خطا	۴
۲-۱-۲	ثبت رویدادها در ویندوز	۷
۲-۱-۳	ثبت رویدادهای مربوط به SQL Server Agent	۸
۲-۱-۴	ثبت رویدادهای مربوط به SQL Server Profiler	۱۰
۲-۱-۵	فایل رویدادنگاری تراکنش	۱۱
۳	نحوه‌ی انجام ممیزی در پایگاه داده MSSQL	۱۵
۳-۱	مؤلفه‌های ممیزی	۱۶
۳-۱-۱	ممیزی کارگزار	۱۶
۳-۱-۲	مشخصات ممیزی کارگزار	۱۸
۳-۱-۳	مشخصات ممیزی پایگاه داده	۱۹
۳-۲	خواندن داده‌های فایل ممیزی	۲۰
۳-۳	بهترین روش‌ها	۲۱
۴	ابزارهای جرم‌شناسی	۲۱
۴-۱	SysTools SQL Recovery	۲۲
۴-۲	ابزار ApexSQL	۲۵
۴-۲-۱	ابزار ApexSQL Log	۲۵
۴-۲-۲	ابزار ApexSQL Audit	۲۸
۴-۲-۳	ابزار ApexSQL Recover	۳۲
۵	جمع‌بندی	۳۳
۶	منابع	۳۴

## ۱ مقدمه

امروزه پایگاه‌های داده در برنامه‌های کاربردی مختلف کاربرد دارند. با توجه به ذخیره‌ی حجم زیادی از اطلاعات حساس در پایگاه‌های داده، لازم است که عملیات و تراکنش‌های رخ داده روی پایگاه‌های داده، مورد بررسی قرار گیرد تا مشخص شود هرکسی، چه عملیاتی را در چه زمانی انجام داده است. همچنین در بحث جرم‌شناسی پایگاه‌های داده، جمع‌آوری شواهد و اطلاعات برای تجزیه و تحلیل از اهمیت زیادی برخوردار است. شواهد در پایگاه داده شامل رخدادهای ثبت شده و ممیزی‌ها است. از این رو، ثبت رویدادها و تهیه‌ی ممیزی در تمامی پایگاه‌های داده مورد توجه قرار گرفته است.

با توجه به اهمیت ثبت وقایع و ممیزی برای نظارت بر اتفاقات درون پایگاه‌های داده، در این گزارش پایگاه داده MSSQL و روش‌های متفاوت ثبت وقایع و ممیزی در آن و ابزارهای جرم‌شناسی موجود برای این پایگاه داده مورد بررسی قرار گرفته است.

بر روی کارگزار عملیاتی SQL، فایل‌های رویدادنگاری<sup>۱</sup> مختلفی ایجاد می‌شوند که در بررسی مشکلات پیش آمده و مسائل مربوط به کارایی و خطاها کمک خواهند کرد. در بخش ۳، انواع فایل‌های رویدادنگاری در پایگاه داده MSSQL مورد بررسی قرار گرفته‌اند. ویژگی ممیزی در SQL Server امکان تهیه‌ی ممیزی از تمام اتفاقات رخ داده در کارگزار را فراهم می‌کند. در بخش ۴، نحوه‌ی انجام ممیزی در پایگاه داده MSSQL توضیح داده شده است. در بخش ۵، دو ابزار جرم‌شناسی معروف برای پایگاه داده‌ی MSSQL معرفی شده‌اند. بیشتر ابزارهای جرم‌شناسی SQL Server در حالت برون خط<sup>۲</sup> اجرا می‌شوند؛ زیرا تحلیل در حالت زنده و آنلاین ممکن است باعث توقف فعالیت کارگزار و از دست رفتن داده‌ها شود.

## ۲ نحوه‌ی ثبت وقایع در پایگاه داده MSSQL

در این بخش انواع فایل‌های رویدادنگاری در پایگاه داده MSSQL مورد بررسی قرار گرفته‌اند.

<sup>۱</sup> Log files

<sup>۲</sup> Offline

لازم به ذکر است که بررسی‌های انجام‌شده در این گزارش بر روی سیستم‌عامل ویندوز ۷ و سیستم مدیریت پایگاه داده‌ی MSSQL Server 2012 صورت گرفته است.

## ۲-۱ انواع فایل‌های رویدادننگاری

بر روی کارگزار SQL عملیاتی، فایل‌های رویدادننگاری مختلفی ایجاد می‌شوند که در بررسی مشکلات پیش‌آمده و مسائل مربوط به کارایی و خطاها کمک خواهند کرد. انواع فایل‌های رویدادننگاری موجود در این پایگاه داده، در جدول ۱ معرفی شده‌اند.

جدول ۱ انواع فایل‌های رویدادننگاری در MSSQL

اطلاعات ثبت‌شده در فایل	نوع فایل رویدادننگاری
رویدادهای خطا و پیغام‌های اطلاعاتی	فایل رویدادننگار خطا
اطلاعات بسیار دقیق درباره‌ی سلامت کارگزار SQL	ثبت رویدادها در ویندوز
پیام‌های هشدار و خطای مرتبط با کارهای اجراشده توسط SQL Server Agent	ثبت رویدادهای مربوط به SQL Server Agent
ثبت فعالیت‌های جاری پایگاه داده‌ی کارگزار برای رفع خطاهای مربوط به برنامه‌های کاربردی پایگاه داده	ثبت رویدادهای مربوط به SQL Server Profiler
تمامی تغییرات پایگاه داده	فایل رویدادننگار تراکنش

در ادامه هر یک از فایل‌های فوق شرح داده شده‌اند.

### ۲-۱-۱ فایل رویدادننگار خطا

مهم‌ترین فایل رویدادننگاری استفاده‌شده توسط کارگزار SQL، فایل رویدادننگار خطا است. این فایل برای رفع مشکلات کلی سیستم به کار می‌رود. فایل رویدادننگار خطا، شامل رویدادهای خطا و پیغام‌های اطلاعاتی است. برای یافتن محل ذخیره‌سازی فایل‌های رویدادننگار خطا از دستور زیر استفاده می‌شود (شکل ۱ محل فایل‌های رویدادننگار خطا در SQL Server را نشان می‌دهد):

**EXEC xp\_readerrorlog 0, 1, N'Logging SQL Server messages in file'**

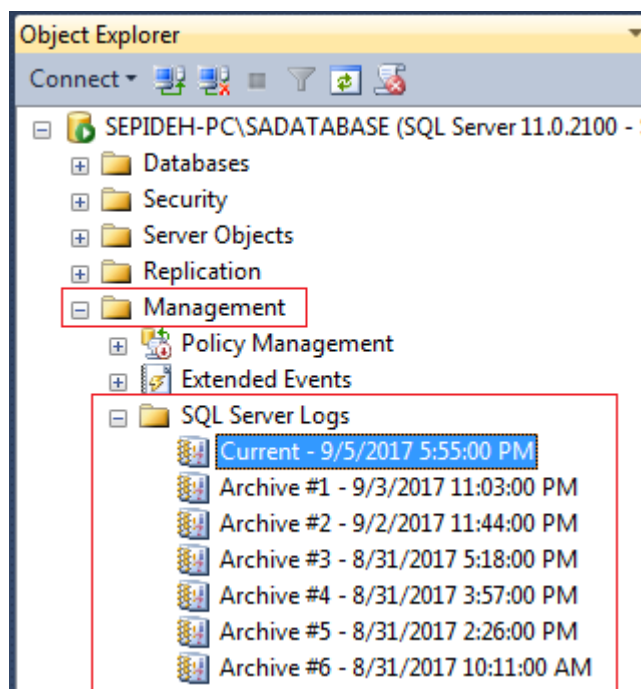
The screenshot shows the SQL Server Enterprise Manager interface. At the top, the command `EXEC xp_readerrorlog 0, 1, N'Logging SQL Server messages in file'` is entered in the command window. Below, the 'Messages' tab is active, displaying a single message in a table:

LogDate	ProcessInfo	Text
2017-09-05 17:55:06.220	Server	Logging SQL Server messages in file 'C:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.SADATABASE\MSSQL\Log\ERRORLOG'.

شکل ۱ محل فایل‌های رویدادنگار خطا در SQL Server

نام فایل رویدادنگار خطای فعلی، ERRORLOG است. کارگزار SQL، شش فایل رویدادنگار اخیر را نگه می‌دارد و هر یک از فایل‌ها را به صورت ERRORLOG.n با پسوند عددی یک تا شش نام‌گذاری می‌کند [۱]. فایل رویدادنگار خطای جدید با هر بار راه‌اندازی SQL Server instance، ایجاد می‌شود. همچنین می‌توان از رویه‌ی سیستمی `sp_cycle_errorlog` به منظور ایجاد فایل رویدادنگار خطای جدید بدون نیاز به راه‌اندازی مجدد SQL Server instance استفاده کرد [۲].

به منظور مشاهده‌ی محتوای فایل رویدادنگار خطا، می‌توان آن را با برنامه‌ی ویرایشگر متن، باز کرد. همچنین می‌توان محتوای این فایل‌ها را از Microsoft SQL Server Management studio مشاهده کرد (شکل ۲).



شکل ۲ مشاهده محتوای فایل‌های رویدادنگار خطا در SSMS

راه‌حل دیگر، استفاده از رویه‌ی ذخیره‌شده‌ی سیستمی `sp_readerrorlog` یا رویه‌ی ذخیره‌شده‌ی توسعه‌یافته‌ی `xp_readerrorlog` است. رویه‌ی `sp_readerrorlog`، چهار پارامتر زیر را دریافت می‌کند [۳]:

۱. مقداری برای مشخص شدن فایل رویدادنگار خطا به‌منظور خواندن: ۰ = فایل جاری، ۱ = فایل آرشیو شده‌ی اول و ...

۲. نوع فایل رویدادنگاری: ۱ یا Null = فایل رویدادنگار خطا، ۲ = SQL Agent log

۳. رشته‌ی شماره‌ی یک برای جستجو

۴. رشته‌ی شماره‌ی دو برای جستجو

در صورتی‌که به رویه هیچ پارامتری داده نشود، محتوای فایل رویدادنگار خطای جاری را نشان می‌دهد (شکل ۳).

```
EXEC sp_readerrorlog 0, 1;
EXEC xp_readerrorlog 0, 1;
```

	LogDate	ProcessInfo	Text
1	2017-09-05 17:55:06.030	Server	Microsoft SQL Server 2012 - 11.0.2100.60 (Intel X86) F...
2	2017-09-05 17:55:06.170	Server	(c) Microsoft Corporation.
3	2017-09-05 17:55:06.170	Server	All rights reserved.
4	2017-09-05 17:55:06.170	Server	Server process ID is 1168.
5	2017-09-05 17:55:06.170	Server	System Manufacturer: 'Apple Inc.', System Model: 'MacBo...
6	2017-09-05 17:55:06.190	Server	Authentication mode is MIXED.
7	2017-09-05 17:55:06.220	Server	Logging SQL Server messages in file 'C:\Program Files (x8...
8	2017-09-05 17:55:06.220	Server	The service account is 'WORKGROUP\SEPIDEH-PC\$'. ...
9	2017-09-05 17:55:06.260	Server	Registry startup parameters: -d C:\Program Files (x86)\...
10	2017-09-05 17:55:06.260	Server	Command Line Startup Parameters: -s "SADATABASE"
11	2017-09-05 17:56:19.520	Server	SQL Server detected 1 sockets with 4 cores per socket a...
12	2017-09-05 17:56:19.520	Server	SQL Server is starting at normal priority base (=7). This is a...
13	2017-09-05 17:56:19.520	Server	Detected 8102 MB of RAM. This is an informational mess...
14	2017-09-05 17:56:19.600	Server	Using conventional memory in the memory manager.
15	2017-09-05 17:56:29.960	Server	This instance of SQL Server last reported using a process ...

شکل ۳ مشاهده محتوای فایل رویدادنگار خطای جاری

## ۲-۱-۲ ثبت رویدادها در ویندوز

ثبت رویدادها در ویندوز<sup>۳</sup> به‌طور انحصاری توسط SQL server استفاده نمی‌شود؛ ولی یک منبع مهم اطلاعاتی برای رفع خطاهای کارگزار SQL به‌حساب می‌آید [۴]. ثبت رویدادها در ویندوز حاوی اطلاعات بسیار دقیقی درباره‌ی سلامت کارگزار SQL است. سه مورد اصلی برای ثبت رویداد در ویندوز شامل موارد زیر بوده که هر یک حاوی اطلاعاتی درباره‌ی زیرسیستم‌های مختلف کارگزار SQL هستند [۱]:

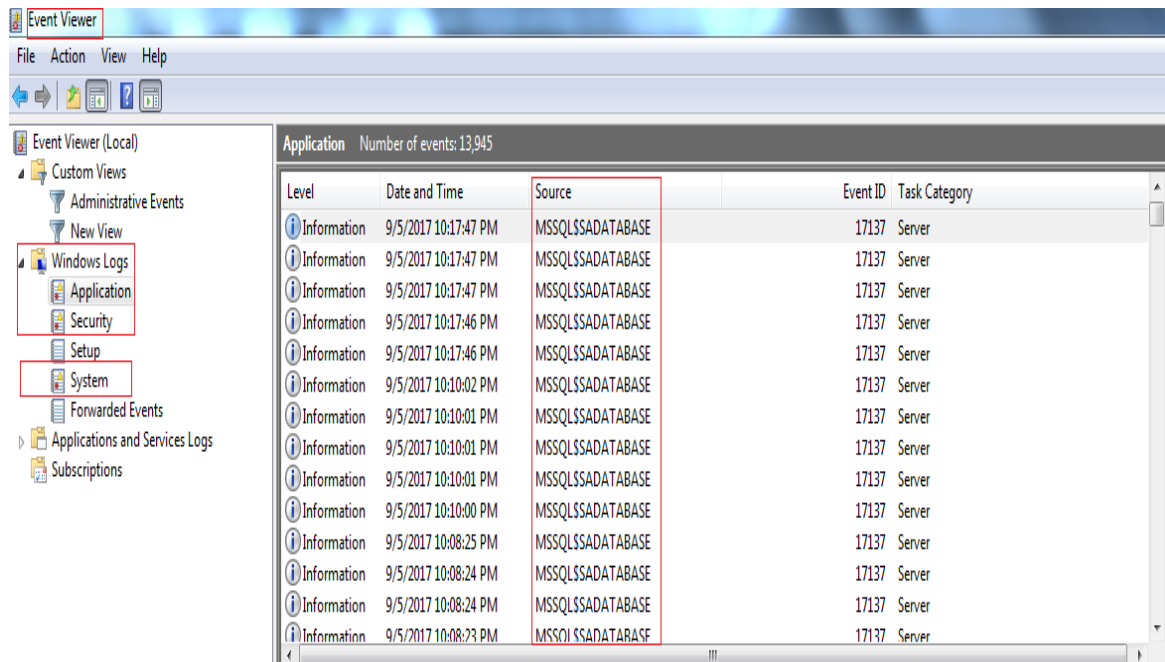
۱. برنامه‌ی کاربردی: رویدادهای درون کارگزار SQL و SQL Server agent را ثبت می‌کند.

۲. امنیت: اطلاعاتی در مورد تصدیق اصالت ثبت می‌شود.

۳. سیستم: رویدادهای راه‌اندازی و توقف سرویس را ثبت می‌کند.

<sup>3</sup> Windows event log

به‌منظور مشاهده‌ی این دسته از رویدادهای ثبت‌شده، از event viewer استفاده می‌شود (شکل ۴).



شکل ۴ ثبت رویدادها در ویندوز

### ۳-۱-۲ ثبت رویدادهای مربوط به SQL Server Agent

SQL Server agent زیرسیستم برنامه‌ریز کار<sup>۴</sup> است. این زیرسیستم، پیام‌های هشدار و خطای مرتبط با کارهایی که اجرا می‌کند را در فایل‌های رویدادنگاری خود می‌نویسد [۱]. برای یافتن محل فایل‌های رویدادنگاری مرتبط با SQL Server agent دستور زیر اجرا می‌شود (شکل ۵).

```
USE MASTER
GO
EXEC msdb..sp_get_sqlagent_properties
GO
```

<sup>4</sup> Job scheduling subsystem



```
USE MASTER
GO
EXEC msdb..sp_get_sqlagent_properties
GO
```

server_restart	jobhistory_max_rows	jobhistory_max_rows_p...	errorlog_file	errorlogging_level
	1000	100	C:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.SADATABASE\MSSQL\Log\SQLAGENT.OUT	3

شکل ۵ محل فایل‌های رویدادنگاری مرتبط با SQL Server agent

کارگزار SQL، ۹ فایل رویدادنگاری خطای مربوط به SQL Server agent را نگه می‌دارد. فایل رویدادنگاری جاری SQLAGENT.OUT نام دارد و فایل‌های آرشیو شده به ترتیب از یک تا نه (مطابق با شکل ۶) شماره‌گذاری شده‌اند [۱].

SQLAGENT.1	9/5/2017 6:00 PM	1 File	3 KB
SQLAGENT.2	9/3/2017 5:40 PM	2 File	3 KB
SQLAGENT.3	9/2/2017 6:25 PM	3 File	3 KB
SQLAGENT.4	8/31/2017 4:04 PM	4 File	3 KB
SQLAGENT.5	8/31/2017 2:33 PM	5 File	3 KB
SQLAGENT.6	8/31/2017 1:18 PM	6 File	3 KB
SQLAGENT.7	8/31/2017 9:37 AM	7 File	3 KB
SQLAGENT.8	8/31/2017 9:29 AM	8 File	3 KB
SQLAGENT.9	8/31/2017 9:22 AM	9 File	3 KB
SQLAGENT.OUT	9/6/2017 6:53 PM	OUT File	3 KB

شکل ۶ فایل‌های رویدادنگاری مرتبط با SQL Server agent

همان‌طور که بیان شد، به‌منظور خواندن فایل رویدادنگاری جاری مربوط به SQL Server agent از دستور زیر (مطابق با شکل ۷) استفاده می‌شود [۳].

```
EXEC xp_readerrorlog 0, 2;
```

```
EXEC xp_readerrorlog 0, 2;
```

	LogDate	ErrorLevel	Text
1	2017-09-06 18:49:22.000	3	[100] Microsoft SQLServerAgent version 11.0.2100.60 (x86 unicode retail build) : Process ID 2348
2	2017-09-06 18:49:22.000	3	[495] The SQL Server Agent startup service account is WORKGROUP\SEPIDEH-PC\$.
3	2017-09-06 18:49:36.000	1	[298] SQLServer Error: 229, The EXECUTE permission was denied on the object 'sp_sqlagent_update_agent_xps', database 'msdb', schema 'dbo'. [SQLSTATE 42000]...
4	2017-09-06 18:49:36.000	1	[000] The EXECUTE permission was denied on the object 'sp_sqlagent_update_agent_xps', database 'msdb', schema 'dbo'. [SQLSTATE 42000] (Error 229)
5	2017-09-06 18:49:36.000	1	[298] SQLServer Error: 229, The EXECUTE permission was denied on the object 'sp_sqlagent_update_agent_xps', database 'msdb', schema 'dbo'. [SQLSTATE 42000]...
6	2017-09-06 18:49:36.000	1	[000] The EXECUTE permission was denied on the object 'sp_sqlagent_update_agent_xps', database 'msdb', schema 'dbo'. [SQLSTATE 42000] (Error 229)
7	2017-09-06 18:53:33.000	3	[098] SQLServerAgent terminated (normally)

شکل ۷ مشاهده‌ی محتوای فایل رویدادنگاری جاری مرتبط با SQL Server agent

#### ۴-۱-۲ ثبت رویدادهای مربوط به SQL Server Profiler

SQL Server Profiler ابزار اصلی ردیابی برنامه‌ی کاربردی<sup>۵</sup> است و برای رفع خطاهای مربوط به برنامه‌های کاربردی پایگاه داده مورد استفاده قرار می‌گیرد. SQL Server Profiler فعالیت‌های جاری پایگاه داده‌ی کارگزار را برای تحلیل‌های آتی در فایل‌ی می‌نویسد. فایل‌های رویدادنگاری مربوط به SQL Server Profiler دارای ساختار log\_<log\_number>.trc هستند [۴]. برای یافتن مسیر پیش‌فرض ذخیره‌سازی این دسته از فایل‌های رویدادنگاری از دستور زیر استفاده می‌شود (شکل ۸):

```
SELECT path
FROM sys.traces
WHERE is_default = 1;
```

<sup>5</sup> Primary application tracing tool

```
SELECT path
FROM sys.traces
WHERE is_default = 1;
```

path
C:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.SADATABASE\MSSQL\Log\log_37.trc

شکل ۸ محل فایل‌های رویدادنگاری مربوط به SQL Server Profiler

برای مشاهده‌ی محتوای فایل رویدادنگاری جاری از دستور زیر استفاده می‌شود (شکل ۹):

```
SELECT *
FROM fn_trace_gettable
('C:\Program Files (x86)\Microsoft SQL
Server\MSSQL10_50.SADATABASE\MSSQL\Log\log_37.trc', default);
GO
```

```
SELECT *
FROM fn_trace_gettable
('C:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.SADATABASE\MSSQL\Log\log_37.trc', default);
GO
```

TextData	BinaryData	DatabaseID	TransactionID	LineNumber	NTUserName	NTDomainName	H
1 NULL	0xFFFE9002D1004D006900630072006F0073006F00660074...	NULL	NULL	NULL	NULL	NULL	N
2 NULL	NULL	NULL	NULL	NULL	NULL	NULL	N
3 NULL	NULL	NULL	NULL	NULL	NULL	NULL	N
4 SELECT [path] FROM [sys].[traces] WHERE [is_defa...	NULL	1	3592	NULL	Sepideh	Sepideh-PC	S
5 NO STATS:[mssqlsystemresource].[sys].[syscolpars]...	NULL	1	4775	NULL	Sepideh	Sepideh-PC	S
6 NO STATS:[mssqlsystemresource].[sys].[syscolpars]...	NULL	1	18529	NULL	Sepideh	Sepideh-PC	S
7 SELECT [path] FROM [sys].[traces] WHERE [is_defa...	NULL	1	34358	NULL	Sepideh	Sepideh-PC	S
8 SELECT * FROM fn_trace_gettable ('C:\Program...	NULL	1	49660	NULL	Sepideh	Sepideh-PC	S

شکل ۹ مشاهده‌ی محتوای فایل رویدادنگاری جاری مربوط به SQL Server Profiler

## ۲-۱-۵ فایل رویدادنگاری تراکش

هر پایگاه داده در SQL Server instance، دارای یک فایل رویدادنگاری است که تمامی تغییرات پایگاه داده در آن ثبت می‌شوند. به دلیل آنکه این نوع از فایل‌های رویدادنگاری به صورت مستقل پیش از اعمال تغییرات

نوشته می‌شود، در مواقع شکست<sup>۶</sup> در سخت‌افزار یا خطای برنامه‌ی کاربردی، امکان بازگرداندن<sup>۷</sup> یا برگشت به عقب<sup>۸</sup> تراکنش‌ها را فراهم می‌کند. به دلیل اهمیت نقش فایل‌های رویدادنگاری تراکنش، رخدادها در یک یا چندین فایل رویدادنگاری مجزا از فایل‌های داده ذخیره می‌شوند. رکوردهای رویدادنگاری، پیش از آنکه محتوای تغییر داده شده در حافظه‌ی بافر<sup>۹</sup> بر روی فایل‌های داده نوشته شوند، در فایل‌های رویدادنگاری تراکنش نوشته می‌شوند [۵].

ثبت رویداد تراکنش برای هر پایگاه داده موارد زیر را پشتیبانی می‌کند [۵]:

۱. در صورتی که عبارت ROLLBACK اجرا شود یا موتور پایگاه داده خطایی را شناسایی کند، امکان بازگشت به عقب تراکنش وجود دارد.
۲. در صورتی که کارگزار دچار مشکل شود و تراکنشی ناتمام بماند، امکان بازگشت به عقب تراکنش وجود دارد. زمانی که کارگزار SQL مجدداً راه‌اندازی شود، تراکنش به عقب بازگردانده می‌شود.
۳. تراکنش‌های ناتمامی که به دلیل شکست<sup>۱۰</sup> در کارگزار در فایل‌های رویدادنگاری نوشته شده ولی در فایل‌های داده نوشته نشده‌اند، قابل بازیابی هستند. زمانی که کارگزار SQL مجدداً راه‌اندازی شود، تراکنش‌ها در فایل‌های داده نوشته می‌شوند.
۴. یک پایگاه داده، گروه فایل<sup>۱۱</sup>، فایل یا صفحه‌ی بازسازی شده را می‌توان به نقطه‌ای که شکست در سخت‌افزار رخ داده است، روبه‌جلو راند<sup>۱۲</sup>. پس از آنکه آخرین فایل‌های پشتیبان کامل یا پشتیبان اختلافی<sup>۱۳</sup> اعمال شدند، می‌توان تراکنش‌ها را روبه‌جلو راند.

<sup>6</sup> Failure

<sup>7</sup> Restore

<sup>8</sup> Roll back

<sup>9</sup> Buffer cache

<sup>10</sup> Failure

<sup>11</sup> Filegroup

<sup>12</sup> Roll forward

<sup>13</sup> Differential backup

فایل یا فایل‌هایی که فایل‌های رویدادنگاری تراکنش را تشکیل می‌دهند به فایل‌های رویدادنگاری مجازی<sup>۱۴</sup> تقسیم می‌شوند. سایز فایل‌های مجازی و تعداد آن‌ها توسط موتور پایگاه داده تعیین می‌شوند. تعیین حداقل و حداکثر سایز فایل رویدادنگاری فیزیکی بر عهده‌ی مدیر سیستم است. همچنین مدیر می‌تواند فایل‌های فیزیکی جدیدی به فایل‌های رویدادنگاری اضافه کند، از آن فایل‌هایی را حذف کند و سایز فایل‌ها را تغییر دهد [۵].

به‌منظور به دست آوردن اطلاعاتی در مورد فایل رویدادنگاری تراکنش مربوط به یک پایگاه داده از دستور زیر استفاده می‌شود (شکل ۱۰).

```
USE AdventureWorks2012;  
  
SELECT name,  
       size, -- in 8-KB pages  
       max_size, -- in 8-KB pages  
       growth,  
       is_percent_growth  
FROM sys.database_files  
WHERE type_desc = 'LOG'
```

<sup>14</sup> Virtual log files

```
USE AdventureWorks2012;

SELECT name,
       size, -- in 8-KB pages
       max_size, -- in 8-KB pages
       growth,
       is_percent_growth
FROM sys.database_files
WHERE type_desc = 'LOG'
```

	name	size	max_size	growth	is_percent_growth
1	AdventureWorks2012_log	112	268435456	10	1

شکل ۱۰ اطلاعاتی در مورد فایل رویدادنگاری تراکنش مربوط به یک پایگاه داده

در شکل ۱۰ به دلیل آنکه پایگاه داده تنها دارای یک فایل رویدادنگاری تراکنش است، خروجی یک سطر دارد.

برای به دست آوردن مسیر فایل رویدادنگاری تراکنش مربوط به یک پایگاه داده از دستور زیر استفاده می‌شود (شکل ۱۱):

```
SELECT * FROM sys.master_files WHERE name =
'AdventureWorks2012_log';

select * from sys.master_files where name = 'AdventureWorks2012_log';
```

	:_desc	data_space_id	name	physical_name	state	state_desc
1	3	0	AdventureWorks2012_log	C:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.SADATABASE\MSSQL\DATA\AdventureWorks2012_log.ldf	0	ONLINE

شکل ۱۱ محل ذخیره‌سازی فایل رویدادنگاری تراکنش

به‌منظور مشاهده محتوای فایل رویدادنگاری تراکنش از تابع `fn_dblog()` استفاده می‌شود (شکل ۱۱):

```
select [Current LSN],
```

```
[Operation],
[Transaction Name],
[Transaction ID],
[Transaction SID],
[SPID],
[Begin Time]
FROM fn_dblog(null,null)
```

Current LSN	Operation	Transaction Name	Transaction ID	Transaction SID	SPID	Begin Time
80 00000020:000000ee:0005	LOP_ABORT_XACT	NULL	0000:00000355	NULL	NULL	NULL
81 00000020:000000ee:0006	LOP_BEGIN_XACT	INSERT	0000:00000356	0x010500000000000515000000C803469088D8182C29B084...	53	2017/09/07 12:40:
82 00000020:000000ee:0007	LOP_INSERT_ROWS	NULL	0000:00000356	NULL	NULL	NULL
83 00000020:000000ee:0008	LOP_COMMIT_XACT	NULL	0000:00000356	NULL	NULL	NULL
84 00000020:000000f0:0001	LOP_BEGIN_XACT	CREATE TABLE	0000:00000357	0x010500000000000515000000C803469088D8182C29B084...	53	2017/09/07 12:40:
85 00000020:000000f0:0002	LOP_LOCK_XACT	NULL	0000:00000357	NULL	NULL	NULL
86 00000020:000000f0:0003	LOP_INSERT_ROWS	NULL	0000:00000357	NULL	NULL	NULL
87 00000020:000000f0:0004	LOP_DELETE_ROWS	NULL	0000:00000357	NULL	NULL	NULL
88 00000020:000000f0:0005	LOP_ABORT_XACT	NULL	0000:00000357	NULL	NULL	NULL
89 00000020:000000f0:0006	LOP_BEGIN_XACT	INSERT	0000:00000358	0x010500000000000515000000C803469088D8182C29B084...	53	2017/09/07 12:40:
90 00000020:000000f0:0007	LOP_INSERT_ROWS	NULL	0000:00000358	NULL	NULL	NULL
91 00000020:000000f0:0008	LOP_COMMIT_XACT	NULL	0000:00000358	NULL	NULL	NULL

شکل ۱۱ مشاهده محتوای فایل رویدادنگاری تراکنش

### ۳ نحوه‌ی انجام ممیزی در پایگاه داده MSSQL

ویژگی ممیزی<sup>۱۵</sup> در SQL Server امکان تهیه‌ی ممیزی از تمام اتفاقات رخ داده در کارگزار را فراهم می‌کند. رویدادها از تغییرات در تنظیمات کارگزار تا تغییر در مقداری در جدول خاصی از پایگاه داده را شامل

<sup>15</sup> Auditing

می‌شوند. رکوردهای ممیزی در محل ثبت رویدادهای امنیتی <sup>۱۶</sup> ویندوز<sup>۱۶</sup>، محل ثبت رویدادهای کاربردی ویندوز<sup>۱۷</sup> یا در فایل نوشته می‌شوند. در SQL Server 2012 امکان ممیزی در سطح کارگزار در تمامی نسخه‌ها وجود دارد ولی ممیزی پایگاه داده تنها در نسخه‌های Developer، Evaluation و Enterprise قابل اعمال است [۶،۷].

### ۳-۱ مؤلفه‌های ممیزی

قابلیت ممیزی در SQL Server شامل سه جزء اصلی است [۶]:

۱. ممیزی کارگزار<sup>۱۸</sup>
۲. مشخصات ممیزی کارگزار<sup>۱۹</sup>
۳. مشخصات ممیزی پایگاه داده<sup>۲۰</sup>

#### ۳-۱-۱ ممیزی کارگزار

ممیزی کارگزار، سرآغازی برای تعریف مشخصات ممیزی در SQL Server است. ممیزی کارگزار در پایگاه داده‌ی master قرار دارد و برای تعریف موارد زیر قابل استفاده است [۶]:

۱. نام ممیزی کارگزار
  ۲. محل ذخیره‌ی اطلاعات ممیزی
- محل ذخیره‌سازی، شامل موارد زیر است:
- فایل
  - ثبت رویدادهای امنیتی در ویندوز<sup>۲۱</sup>

<sup>16</sup> Windows security log

<sup>17</sup> Windows application log

<sup>18</sup> Server Audit

<sup>19</sup> Server Audit specification

<sup>20</sup> Database audit specification



- ثبت رویدادهای مرتبط با برنامه‌های کاربردی در ویندوز<sup>۲۲</sup>
  - ۳. خط‌مشی بازنویسی بر روی فایل<sup>۲۳</sup>
  - ۴. تأخیر صف: حداکثر مقدار برحسب میلی‌ثانیه که سیستم ممکن است پیش از پردازش ممیزی صبر کند.
  - ۵. عکس‌العمل SQL Server در مواردی که تهیه‌ی ممیزی امکان‌پذیر نیست.  
گزینه‌های ممکن شامل موارد زیر هستند:
    - ادامه و نادیده گرفتن ثبت رویداد
    - خاموش کردن کارگزار
    - شکست عملیات<sup>۲۴</sup>
  - ۶. محدودیت سایز فایل و تعداد فایل‌های ممیزی
  - ۷. حداکثر تعداد فایل‌های ممیزی بدون استفاده از خط‌مشی بازنویسی<sup>۲۵</sup>
  - ۸. رزرو یا عدم رزرو فضای دیسک برای فایل‌های رویدادنگاری ممیزی
- در ادامه، پرسمانی به عنوان مثال به منظور تعریف ممیزی کارگزار آورده شده است [۸]:

```
CREATE SERVER AUDIT [AdventureWorksAudit_DDL_Access] TO FILE
(FILEPATH = N'C:\Users\Sepideh\Desktop\mssqlAudit'
,MAXSIZE = 10 MB
)
WITH
(Queue_Delay = 1000
,ON_FAILURE = CONTINUE
)
```

<sup>21</sup> Windows security log

<sup>22</sup> Windows application log

<sup>23</sup> File roll over policy

<sup>24</sup> Fail the operation

<sup>25</sup> Rollover

ممیزی در وضعیت غیرفعال ایجاد می‌شود و به صورت خودکار رویدادها را ثبت نمی‌کند؛ بنابراین پس از تعریف ممیزی باید آن را فعال کرد تا مقصد ممیزی، داده‌ها را دریافت کند.

```
ALTER SERVER AUDIT [AdventureWorksAudit_DDL_Access] WITH (STATE = ON)
```

## ۳-۱-۲ مشخصات ممیزی کارگزار

از برخی از رویدادها همچون تهیه‌ی ممیزی از رویداد بازیابی (SELECT از یک جدول)، به صورت انفرادی ممیزی تهیه می‌شود. به این رویدادهای انفرادی عمل ممیزی<sup>۲۶</sup> می‌گویند. در بیش‌تر موارد عمل‌های ممیزی با هم گروه‌بندی می‌شوند و گروه اعمال ممیزی<sup>۲۷</sup> را شکل می‌دهند. بدین ترتیب با گروه‌بندی و ایجاد واحدهای منطقی، تنظیم مشخصات ممیزی آسان‌تر می‌شود [۶].

مشخصات ممیزی کارگزار که در تمامی نسخه‌های SQL Server پشتیبانی می‌شود، برای تعریف ممیزی در سطح کارگزار مورد استفاده قرار می‌گیرد.

سه مورد زیر در تعریف مشخصه ممیزی کارگزار مشخص می‌شوند [۶].

۱. نام مشخصه‌ی ممیزی: این مورد اختیاری است و در صورت عدم تعیین، نام پیش‌فرضی اختصاص داده می‌شود.

۲. ممیزی کارگزار: مقصدی که باید رویدادهای انتخاب‌شده ثبت شوند را تعیین می‌کند.

۳. نوع عمل ممیزی: رویدادهایی هستند که باید از آن‌ها ممیزی تهیه شود.

در مشخصه‌ی کارگزار تمامی رویدادها در قالب گروه اعمال ممیزی گروه‌بندی شده‌اند. از جمله این گروه‌ها می‌توان به موارد زیر اشاره کرد:

SUCCESSFUL\_LOGIN\_GROUP ○

FAILED\_LOGIN\_GROUP ○

DBCC\_GROUP ○

<sup>26</sup> Audit action

<sup>27</sup> Audit action group

با پرسمان زیر می‌توان مشخصه کارگزار را ایجاد کرد و آن را که به‌صورت پیش‌فرض غیرفعال است را در وضعیت فعال قرار داد [۸]:

```
CREATE SERVER AUDIT SPECIFICATION [SQL2012_FailedLogins_DbChanges]
FOR SERVER AUDIT [AdventureWorksAudit_DDL_Access]
ADD (FAILED_LOGIN_GROUP),
ADD (DATABASE_CHANGE_GROUP)
WITH (STATE = ON)
GO
```

به‌منظور ایجاد مشخصه‌ی ممیزی کارگزار، یک کاربر نیاز به مجوز ALTER ANY SERVER AUDIT دارد و مجوز CONTROL SERVER اجازه‌ی مشاهده‌ی ممیزی را به کاربر می‌دهد.

```
GRANT ALTER ANY SERVER AUDIT TO test11
GRANT CONTROL SERVER TO test11
```

### ۳-۱-۳ مشخصات ممیزی پایگاه داده

مشخصات ممیزی پایگاه داده، از رویدادها در سطح پایگاه داده ممیزی می‌گیرد. با استفاده از مشخصه‌ی ممیزی پایگاه داده، ممیزی می‌تواند در سطح شیئی یا کاربر انجام شود ولی در سطح ستون قابل انجام نیست. به‌منظور ایجاد مشخصه‌ی ممیزی پایگاه داده، موارد زیر تنظیم می‌شوند [۸]:

۱. نام مشخصه‌ی ممیزی پایگاه داده. در صورتی‌که نامی مشخص نشود، مقدار پیش‌فرضی اختصاص داده می‌شود.
۲. ممیزی کارگزار که مشخصه‌ی ممیزی پایگاه داده به آن مرتبط می‌شود.
۳. نوع عمل ممیزی. در این فیلد می‌توان عمل ممیزی و گروه اعمال ممیزی را مشخص کرد.
۴. در صورت تعیین عمل ممیزی، نام شیئی برای تهیه‌ی ممیزی باید تعیین شود.
۵. شمای شیئی انتخاب‌شده
۶. نام principal یا استفاده از کلیدواژه public برای تهیه‌ی ممیزی از تمامی کاربران.

مثالی از ایجاد مشخصه‌ی ممیزی پایگاه داده در ادامه آورده شده است [۸]:

```
CREATE DATABASE AUDIT SPECIFICATION [AW_DDL_Access_dbSpec]
FOR SERVER AUDIT [AdventureWorksAudit_DDL_Access]
ADD (SCHEMA_OBJECT_ACCESS_GROUP),
ADD (SCHEMA_OBJECT_CHANGE_GROUP)
WITH (STATE = ON)
GO
```

به‌منظور تنظیم مشخصات ممیزی پایگاه داده، به کاربر باید مجوزهای ALTER ANY DATABASE AUDIT یا ALTER یا CONTROL روی پایگاه داده اعطا شوند.

```
GRANT ALTER ANY DATABASE AUDIT TO test11;

GRANT CONTROL TO test11;

GRANT ALTER TO test11;
```

## ۳-۲ خواندن داده‌های فایل ممیزی

اطلاعات ممیزی در فایل مقصد به‌صورت دودویی<sup>۲۸</sup> نوشته می‌شوند. به‌منظور خواندن فایل‌های دودویی ممیزی از تابع `fn_get_audit_file()` استفاده می‌شود. این تابع سه پارامتر نیاز دارد [۶]:

۱. الگوی فایل: مسیر یا مسیر فایل به همراه نام آن در این پارامتر مشخص می‌شوند. به‌منظور خواندن تمامی فایل‌های یک فولدر، پس از مسیر فولدر از \* استفاده می‌شود.

۲. نام فایل اولیه: مسیر و نام فایلی که خواندن اطلاعات از آن شروع می‌شود.

۳. محل شروع در فایل اولیه در این قسمت مشخص می‌شود.

به‌عنوان مثال می‌توان از تابع `fn_get_audit_file()` به صورت زیر استفاده کرد:

```
SELECT * FROM
fn_get_audit_file('C:\Users\Sepideh\Desktop\mssqlAudit\*',
default, default);
```

در شکل با توجه به تنظیمات انجام‌شده در بخش‌های پیشین، ممیزی مربوط به عدم موفقیت در ورود به کارگزار نشان داده شده است.

instance_name	database_name	schema_name	statement	additional_information
1	H-PC\SADATABASE			<action_info xmlns="http://sch
2	H-PC\SADATABASE		Login failed for user 'dr_B'. Reason: Password did not match that for the login provided. [CLIENT: <local machine>]	<action_info xmlns="http://sch
3	H-PC\SADATABASE		Login failed for user 'dr_B'. Reason: Password did not match that for the login provided. [CLIENT: <local machine>]	<action_info xmlns="http://sch
4	H-PC\SADATABASE			<action_info xmlns="http://sch
5	H-PC\SADATABASE		Network error code 0x6d occurred while establishing a connection; the connection has been closed. This may have ...	<action_info xmlns="http://sch

شکل ۱۳ اطلاعات ممیزی

اطلاعات ممیزی نوشته‌شده در windows security log یا application log با استفاده از **event viewer**<sup>۲۹</sup> قابل خواندن هستند.

### ۳-۳ بهترین روش‌ها

در ادامه برخی روش‌های پیشنهادی برای ممیزی بیان شده‌اند [۶]:

۱. نوشتن ممیزی در محل متمرکز
۲. تسهیل پردازش داده‌های ممیزی شده، با بارگذاری رویدادهای ثبت‌شده در پایگاه داده
۳. استفاده از یک فایل مقصد برای کارایی بهینه
۴. استفاده از ممیزی هدفمند به منظور به حداقل رساندن داده‌های جمع‌آوری‌شده و کارایی بهتر
۵. اطمینان از عدم مغایرت خط‌مشی بازنویسی بر روی فایل‌های رویدادننگاری در ویندوز با استراتژی ممیزی، در صورت نوشتن اطلاعات در Windows logs

## ۴ ابزارهای جرم‌شناسی

روش‌های جرم‌شناسی موجود در MSSQL Server، می‌توانند برای بررسی دسترسی‌های غیرمجاز به داده‌ها، کلاه‌برداری و جمع‌آوری اطلاعات برای تشخیص نفوذ استفاده شوند. در حقیقت جرم‌شناسی در SQL Server در موارد زیر کاربرد دارد [۹]:

<sup>۲۹</sup> ابزاری از ابزارهای مدیریتی ویندوز که در مسیر administrative tools -> control panel قرار دارد.

۱. تزریق SQL روشی است برای دسترسی به داده‌های حساس به صورت غیرمجاز که توسط مهاجمین استفاده می‌شود. در این مواقع جرم‌شناسی SQL Server، روشی است برای تشخیص تغییرات ایجادشده در پایگاه داده.

۲. تشخیص داده‌های تغییر داده شده

۳. تشخیص منشأ اصلی تغییرات و حملات

بیشتر ابزارهای جرم‌شناسی SQL Server در حالت برون‌خط<sup>۳۰</sup> اجرا می‌شوند؛ زیرا تحلیل در حالت زنده و برخط ممکن است باعث توقف فعالیت کارگزار و از دست رفتن داده‌ها شود [۱۰].

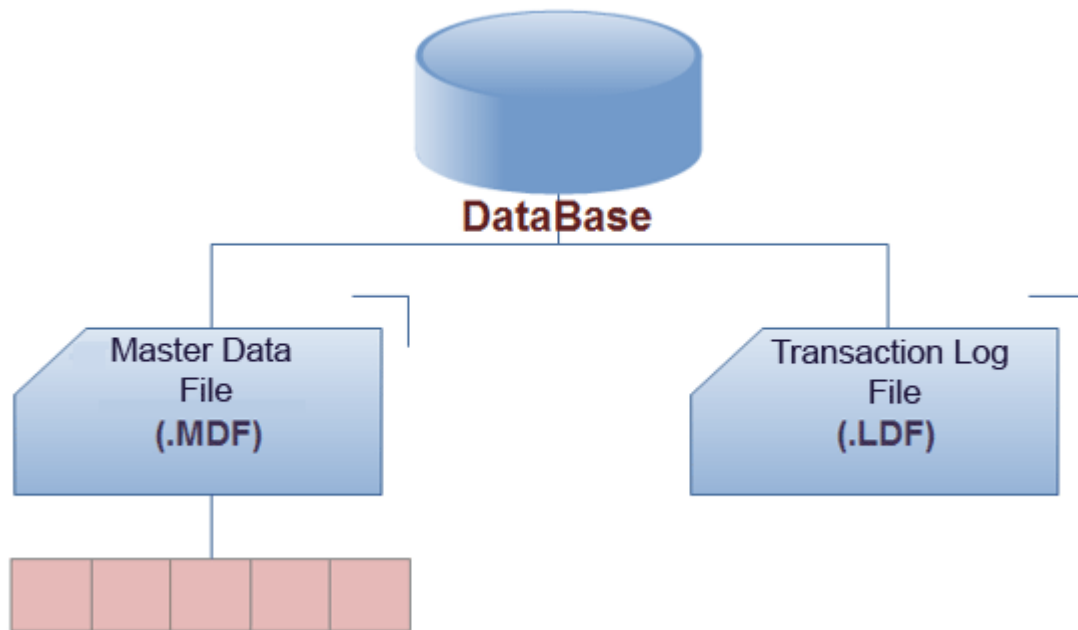
### ۴-۱ SysTools SQL Recovery

SQL Server پایگاه‌های داده خود را در سه دسته فایل ذخیره می‌کند. این فایل‌ها برای تحلیل و بررسی جرم‌شناسی بسیار مفید و سودمند هستند [۹]. سه دسته فایل شامل موارد زیر هستند (شکل ۱۲):

۱. فایل **mdf**: این دسته از فایل‌ها، داده‌های اصلی شامل جداول، توابع، قوانین و رویه‌های ذخیره‌شده را در خود نگه می‌دارند.

۲. فایل **ndf**: دسته‌ی دیگری از فایل‌های پایگاه داده هستند که توسط کاربر تعریف شده‌اند.

۳. فایل **ldf**: SQL Server از این دسته از فایل‌ها برای ذخیره‌سازی اطلاعات رخدادها استفاده می‌کند. تغییرات در پایگاه داده شامل درج، حذف و به‌روزرسانی در فایل‌های رویدادنگاری تراکنش ذخیره می‌شوند.



شکل ۱۲ فایل‌های ذخیره‌سازی پایگاه داده

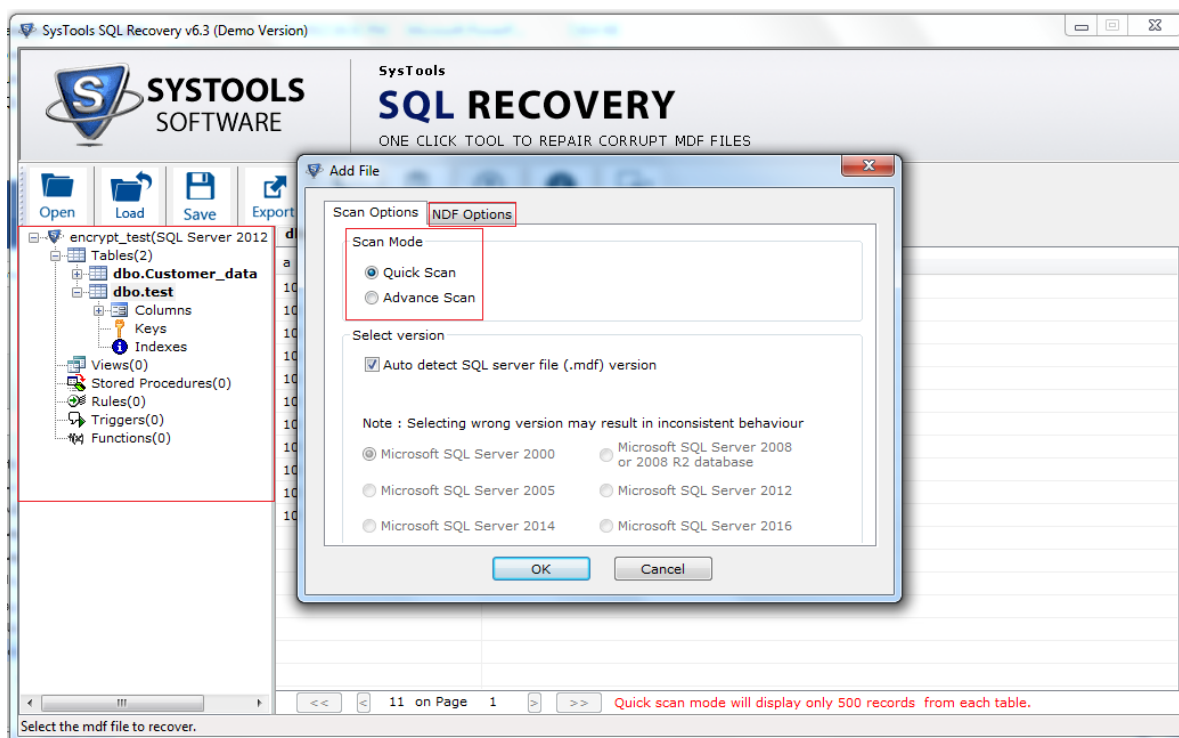
تحلیل فایل‌های مذکور در موارد مختلفی از جمله موارد زیر کاربرد دارد [۹]:

۱. شناسایی نقض امنیت داده

۲. شناسایی سطوح نفوذ به پایگاه داده

۳. بررسی اطلاعات ذخیره‌شده

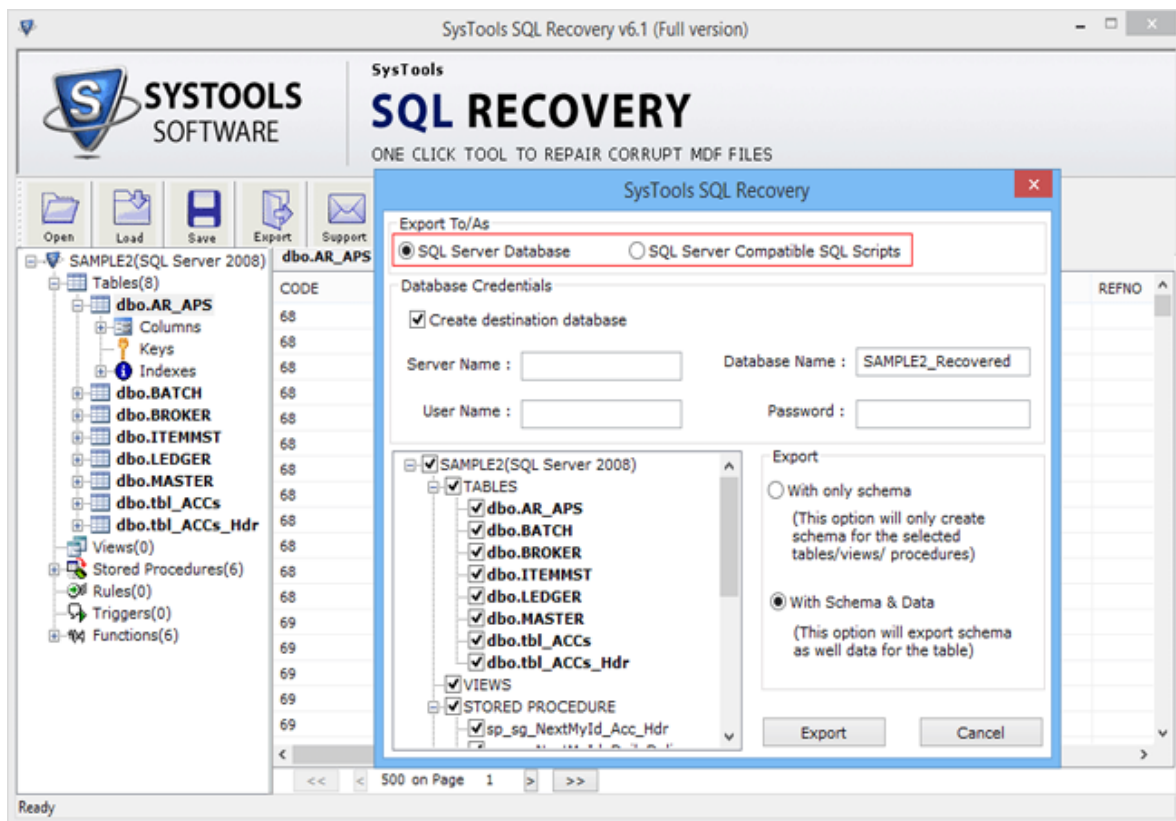
ابزار SysTools SQL Recovery برای تحلیل فایل‌های پایگاه داده MDF مورد استفاده قرار می‌گیرد. این ابزار می‌تواند تمامی تریگرها، قوانین، توابع و جداول ذخیره‌شده را بازیابی کند. این ابزار قابلیت تحلیل فایل‌های NDF را نیز دارد. با استفاده از الگوریتم‌های Quick scanning و advance scanning در این ابزار، می‌توان فایل‌های MDF و LDF را ترمیم و بازیابی کرد (شکل ۱۳). همچنین قابلیت بازیابی داده‌های حذف‌شده‌ی جداول که نتیجه‌ی فعالیت خرابکارانه‌ی مهاجمین است را دارد [۱۰]. لازم به ذکر است که این ابزار، ابزار متن‌بازی نیست و دارای نسخه‌ی آزمایشی با ویژگی‌های محدودی است.



شکل ۱۳ ابزار SysTools SQL Recovery

در هنگام تجزیه و تحلیل قانونی SQL Server، چالش بزرگی که محققان با آن روبه‌رو هستند، استخراج شواهد است. در این ابزار، محققان می‌توانند فایل SQL را در پایگاه داده SQL Server یا در اسکرپتی سازگار با SQL Server، استخراج کنند (شکل ۱۴) [۱۱].





شکل ۱۴ استخراج شواهد در SysTools SQL Recovery

## ۴-۲ ابزار ApexSQL

ApexSQL شامل ابزارهای مختلفی است که برخی از آنها همچون موارد زیر در جرم‌شناسی کاربرد دارند:

۱. ApexSQL Log

۲. ApexSQL Audit

۳. ApexSQL Recover

هیچ‌یک از این ابزارها متن‌باز نیستند.

### ۴-۲-۱ ابزار ApexSQL Log

این ابزار در موارد زیر کاربرد دارد [۱۲]:

۱. تهیه ممیزی از تغییرات در داده‌ها، شما و مجوزها

۲. عقب‌گرد یا اجرای مجدد تراکنش پایگاه داده (شکل ۱۵)

<input type="checkbox"/>	Operation	Schema	Object	User	Begin time
<input type="checkbox"/>	Update	dbo	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:02:57
<input type="checkbox"/>	Update	dbo	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:03:16
<input checked="" type="checkbox"/>	Insert	dbo	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:07:41
<input checked="" type="checkbox"/>	Delete	dbo	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:08:33
<input type="checkbox"/>	Delete	dbo	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:08:33

Save	Save as	Execute	Check syntax	Undo	Redo	Cut
------	---------	---------	--------------	------	------	-----

**Roll the changes back and preview the change script**

```

1 -- This UNDO script was generated with ApexSQL Log 2016.01.1149 on 11-27
2 -- NOTE: Operations in UNDO scripts are always output in descending order
3 -- SERVER GRAVEYARD\MSSQLSERVER2014
4 -- DATABASE ApexSQLLogTest
5
6 -- DELETE (00000028:000000F0:0002) done at 11-26-2015 16:08:33.303 by
7 INSERT INTO [dbo].[Employees] ([EmployeeName], [EmployeeLastName])
8 VALUES (N'Calvin' COLLATE SQL_Latin1_General_CP1_CI_AS, N'Cane' COLLATE
9 GO
10 -- INSERT (00000028:000000E8:0002) done at 11-26-2015 16:07:41.753 by
11 BEGIN TRANSACTION
12 DELETE FROM [dbo].[Employees] WHERE [EmployeeName] = N'Calvin' COLLATE
13 IF @@ROWCOUNT <= 1 COMMIT TRANSACTION ELSE BEGIN ROLLBACK TRANSACTION;
14 PRINT 'ERROR: STATEMENT AFFECTED MORE THAN ONE ROW. ALL THE CHANGES WERE
15 GO
16
17 -- FINISHED ON 11-27-2015 17:10:09.540
18 -- TOTAL OPERATIONS PROCESSED 2
19 -- END OF FILE
    
```

شکل ۱۵ عقب‌گرد یا اجرای مجدد تراکنش پایگاه داده

۳. اجرای معکوس تراکنش‌های غیرعمدی یا مخرب پایگاه داده به‌منظور ترمیم داده: بازیابی داده‌های خراب‌شده یا از دست‌رفته، بدون تکیه بر بازگرداندن کل پایگاه داده (شکل ۱۶).

<input type="checkbox"/>	Delete	dbo	Employees	GRAVEYARD\ImpostoR	11-26-2015 16:08:33
<input type="checkbox"/>	Delete	dbo	Employees	GRAVEYARD\ImpostoR	11-26-2015 16:08:33
<input checked="" type="checkbox"/>	Delete	dbo	Employees	GRAVEYARD\ImpostoR	11-26-2015 16:08:33
<input type="checkbox"/>	Delete	dbo	Employees	GRAVEYARD\ImpostoR	11-26-2015 16:08:33

**View deleted data for each operation**

Field	Type	Value
EmployeeName	nvarchar(50)	Philip
EmployeeLastName	nvarchar(50)	New
EmployeeDOB	nvarchar(50)	11/20/1988
EmployeeSalary	money	31000.0000
EmployeeEmail	nvarchar(50)	NewPhil@work.com

شکل ۱۶ اجرای معکوس تراکنش‌های غیرعمدی یا مخرب پایگاه داده

۴. بررسی قانونی اینکه چه کسی، چه چیزی را در چه زمانی تغییر داده است.

۵. نمایش تاریخچه کامل تغییرات سطرها

۶. تجسم تراکنش<sup>۳۱</sup>: نمایش، دسته‌بندی و مرتب‌سازی تراکنش‌ها همراه با گزینه‌های پیشرفته برای فیلترینگ (شکل ۱۷)

The screenshot shows the 'Grid filter' interface in SQL Server Enterprise Manager. On the left, there is a 'Grid filter' section with buttons for 'Open', 'Save', and 'Clear'. Below it are tabs for 'Time', 'DML', 'DDL', 'Users', and 'Other'. A list of operations is shown with checkboxes, including 'Create Default', 'Create Default Constraint', 'Create Foreign Key', 'Create Function', 'Create Index', 'Create Primary Key', 'Create Procedure', 'Create Rule', 'Create Schema', 'Create Sequence', 'Create Statistics', 'Create Table', and 'Create Trigger'. The 'Group by' section at the bottom has 'Object', 'Operation', and 'None' options.

Operation	Schema	Object
<input type="checkbox"/> Create Default Constraint		DF_employee_pub_id_2F10007B
<input checked="" type="checkbox"/> Create Default Constraint		DF_employee_hire_d_30F848ED
<input type="checkbox"/> Create Foreign Key		FK_employee_job_id_2D27B809
<input checked="" type="checkbox"/> Create Foreign Key		FK_employee_pub_id_300424B4
<input type="checkbox"/> Create Check Constraint		CK_emp_id
<input type="checkbox"/> Create Foreign Key		FK_pub_info_pub_id_286302EC
<input type="checkbox"/> Create Default Constraint		DF_titles_type_117F9D94
<input checked="" type="checkbox"/> Create Default Constraint		DF_titles_pubdate_1367E606
<input type="checkbox"/> Create Foreign Key		FK_titles_pub_id_1273C1CD
<input type="checkbox"/> Create Foreign Key		FK_roysched_title_1ED998B2
<input checked="" type="checkbox"/> Create Foreign Key		FK_sales_stor_id_1BFD2C07
<input type="checkbox"/> Create Foreign Key		FK_sales_title_id_1CF15040
<input type="checkbox"/> Create Foreign Key		FK_titleauth_au_id_164452B1
<input type="checkbox"/> Create Foreign Key		FK_titleauth_title_173876EA
<input type="checkbox"/> Create Type	dbo	SSN
<input type="checkbox"/> Create Procedure	dbo	AddTestHierarchy
<input type="checkbox"/> Insert	dbo	authors
<input type="checkbox"/> Insert	dbo	authors
<input type="checkbox"/> Insert	dbo	authors
<input checked="" type="checkbox"/> Insert	dbo	authors

شکل ۱۷ تجسم تراکنش

۷. نمایش مقادیر قبلی و بعدی در عملیات به‌روزرسانی (شکل ۱۸)

<sup>31</sup> Transaction visualization

<input checked="" type="checkbox"/>	Operation	Object	User	Begin time	End time
<input type="checkbox"/>	Delete	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:08:33	2015-11-26 16:08:33
<input type="checkbox"/>	Delete	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:08:33	2015-11-26 16:08:33
<input type="checkbox"/>	Delete	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:08:33	2015-11-26 16:08:33
<input type="checkbox"/>	Insert	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:17:55	2015-11-26 16:17:55
<input type="checkbox"/>	Insert	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:17:55	2015-11-26 16:17:55
<input type="checkbox"/>	Insert	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:17:55	2015-11-26 16:17:55
<input type="checkbox"/>	Insert	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:17:55	2015-11-26 16:17:55
<input type="checkbox"/>	Insert	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:17:55	2015-11-26 16:17:55
<input type="checkbox"/>	Update	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:18:37	2015-11-26 16:18:37
<input type="checkbox"/>	Update	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:18:41	2015-11-26 16:18:41
<input type="checkbox"/>	Update	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:19:16	2015-11-26 16:19:16
<input type="checkbox"/>	Update	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:19:43	2015-11-26 16:19:43
<input checked="" type="checkbox"/>	Update	Employees	GRAVEYARD\ImpostoR	2015-11-26 16:20:43	2015-11-26 16:20:43
<input type="checkbox"/>	Delete	Employees	GRAVEYARD\ImpostoR	2015-12-04 13:47:48	2015-12-04 13:47:48

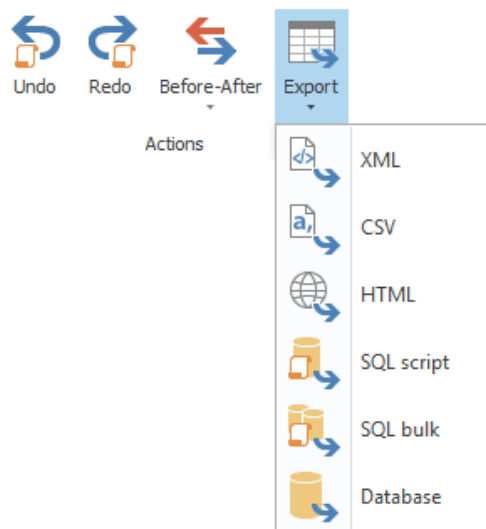
  

Field	Type	Old Value	New Value
EmployeeName	nvarchar(50)	David	David
EmployeeLastName	nvarchar(50)	Lang	Long
EmployeeDOB	nvarchar(50)	28/04/1984	28/05/1985
EmployeeSalary	money	38000.0000	39000.0000
EmployeeEmail	nvarchar(50)	David.Lang@work.com	David.Long@work.com

شکل ۱۸ نمایش مقادیر قبلی و بعدی در عملیات به‌روزرسانی

۸. نمایش اطلاعات رویدادهای تراکنش در قالب جدول یا استخراج آن در قالب‌های مختلف همچون

.HTML, .CSV, XML, SQL script (شکل ۱۹)



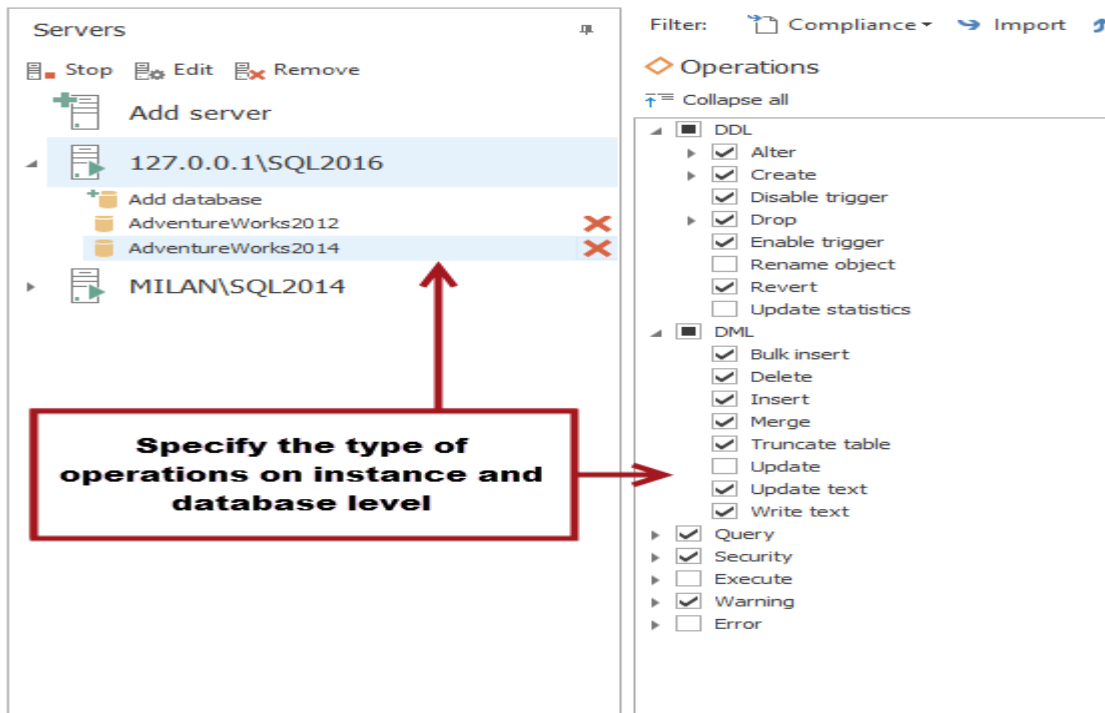
شکل ۱۹ استخراج اطلاعات رویدادهای تراکنش

## ۴-۲-۲ ابزار ApexSQL Audit

ابزار ApexSQL Audit برای تهیه ممیزی کاربرد داشته که از جمله ویژگی‌های آن می‌توان به موارد زیر اشاره

کرد [۱۲]:

۱. ممیزی از فعالیت‌های SQL Server: تهیه‌ی ممیزی از تمامی عملیات اجراشده بر روی SQL instance شامل تغییرات در DDL و DML، عبارات SELECT و فعالیت‌های مرتبط با ورود به پایگاه داده، کاربران و مجوزها (شکل ۲۰).



شکل ۲۰ ممیزی از فعالیت‌های SQL Server

۲. نمایش عبارات SQL اجراشده (شکل ۲۱).

Name: Complete audit trail Save Advanced

Event source:  Trace  Before-after  Internal

Filter:

- Servers: [Dropdown]
- Databases: [Dropdown]
- Schemas: [Dropdown]
- Objects: [Dropdown]
- Logins: [Dropdown]
- Client hosts: [Dropdown]
- Applications: [Dropdown]
- Text data: [Text Input]

Operations:

- DDL
- DML
- Query
- Security
- Execute
- Backup/restore
- Warning
- Error

Preview | Generate

Date	Server	Database	Login	Application	Client host	Operation
03/23/2017 11:45:13.977 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<b>SELECT cr.* FROM Sales.CurrencyRate cr</b>						
03/23/2017 11:45:04.547 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<b>SELECT ct.* FROM Person.ContactType ct JOIN Person.BusinessEntityContact bec ON ct.ContactTypeID = bec.ContactTypeID</b>						
03/23/2017 11:43:14.900 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<b>SELECT bom.* FROM Production.BillofMaterials bom</b>						
03/23/2017 11:42:19.080 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<b>SELECT c.* FROM Sales.Currency c</b>						
03/23/2017 11:41:58.373 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Update
<b>UPDATE [Sales].[Customer] set [Sales].[Customer].[PersonID] = @1,[Sales].[Customer].[StoreID] = @2,[Sales]</b>						
03/23/2017 11:41:26.587 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<b>SELECT ct.* FROM Person.ContactType ct</b>						
03/23/2017 11:41:18.517 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<b>SELECT a.* FROM Person.Address a INNER JOIN Person.BusinessEntityAddress bea ON a.AddressID = bea.AddressID</b>						

Total events: 179 << < 1/9 > >>

شکل ۲۱ نمایش عبارات SQL اجراشده

۳. نمایش اینکه چه کسی، چه چیزی را در چه زمانی انجام داده است (شکل ۲۲)

Name: Complete audit trail Save Advanced

Event source Preview Generate From To Columns

Trace  Before-after  Internal

**Filter**

Servers:

Databases:

Schemas:

Objects:

Logins:

Client hosts:

Applications:

Text data:

**Operations**

DDL  
 DML  
 Query  
 Security  
 Execute  
 Backup/restore  
 Warning  
 Error

Date	Server	Database	Login	Application	Client host	Operation
03/23/2017 11:45:13.977 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<code>SELECT cr.* FROM Sales.CurrencyRate cr</code>						
03/23/2017 11:45:04.547 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<code>SELECT ct.* FROM Person.ContactType ct JOIN Person.BusinessEntityContact bec ON ct.ContactTypeID = bec.ContactTypeID</code>						
03/23/2017 11:43:14.900 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<code>SELECT bom.* FROM Production.BillofMaterials bom</code>						
03/23/2017 11:42:19.080 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<code>SELECT c.* FROM Sales.Currency c</code>						
03/23/2017 11:41:58.373 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Update
<code>UPDATE [Sales].[Customer] set [Sales].[Customer].[PersonID] = @1, [Sales].[Customer].[StoreID] = @2, [Sales]</code>						
03/23/2017 11:41:26.587 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<code>SELECT ct.* FROM Person.ContactType ct</code>						
03/23/2017 11:41:18.517 PM	Goran-Pc\SQL2016SP1	AdventureWorks2014	root	Microsoft SQL Server Management Studio - Query	GORAN-PC	Select
<code>SELECT a.* FROM Person.Address a INNER JOIN Person.BusinessEntityAddress bea ON a.AddressID = bea.AddressID</code>						

Total events: 179 << < 1/9 > >>

شکل ۲۲ نمایش جزئیات مربوط به تراکنش‌ها

۴. نمایش تلاش‌های ناموفق برای ورود (شکل ۲۳)

Name: Logon activity history Save Advanced

Event source: Preview Generate From To Columns

Trace  Before-after  Internal

**Filter**

Servers:

Databases:

Schemas:

Objects:

Logins:

Client hosts:

Applications:

Text data:

**Operations**

DDL  
 DML  
 Query  
 Security  
 Execute  
 Backup/restore  
 Warning  
 Error

Date	Server	Login	Application	Client host	Operation
03/23/2017 11:43:14:900 PM	Goran-Pc\SQL2016SP1	dba	Microsoft SQL Server Management Studio	GORAN-PC	Audit login failed
Login failed for user 'dba'. Reason: Could not find a login matching the name provided.					
03/23/2017 11:43:12:950 PM	Goran-Pc\SQL2016SP1	root	Microsoft SQL Server Management Studio	GORAN-PC	Audit login failed
Login failed for user 'root'. Reason: Password did not match that for the login provided.					
03/23/2017 11:43:10:350 PM	Goran-Pc\SQL2016SP1	root	Microsoft SQL Server Management Studio	GORAN-PC	Audit logout
03/23/2017 11:42:11:350 PM	Goran-Pc\SQL2016SP1	root	Microsoft SQL Server Management Studio	GORAN-PC	Audit login
03/23/2017 11:42:09:150 PM	Goran-Pc\SQL2016SP1	sa	Microsoft SQL Server Management Studio	GORAN-PC	Audit logout
03/23/2017 11:41:29:150 PM	Goran-Pc\SQL2016SP1	sa	Microsoft SQL Server Management Studio	GORAN-PC	Audit login
03/23/2017 11:41:19:250 PM	Goran-Pc\SQL2016SP1	root	Microsoft SQL Server Management Studio	GORAN-PC	Audit login failed
Login failed for user 'root'. Reason: Password did not match that for the login provided.					
03/23/2017 11:40:15:250 PM	Goran-Pc\SQL2016SP1	sa	Microsoft SQL Server Management Studio	GORAN-PC	Audit login failed
Login failed for user 'sa'. Reason: Password did not match that for the login provided.					
03/23/2017 11:40:12:250 PM	Goran-Pc\SQL2016SP1	test	Microsoft SQL Server Management Studio	GORAN-PC	Audit logout
03/23/2017 11:38:12:250 PM	Goran-Pc\SQL2016SP1	test	Microsoft SQL Server Management Studio	GORAN-PC	Audit login
03/23/2017 11:37:20:350 PM	Goran-Pc\SQL2016SP1	test	Microsoft SQL Server Management Studio	GORAN-PC	Audit logout
03/23/2017 11:37:15:355 PM	Goran-Pc\SQL2016SP1	test	Microsoft SQL Server Management Studio	GORAN-PC	Audit login

Total events: 12 << < 1/1 > >>

شکل ۲۳ نمایش تلاش‌های ناموفق برای ورود

۵. تهیه ممیزی از عملیات درج، به‌روزرسانی و حذف، قبل و بعد از انجام عملیات

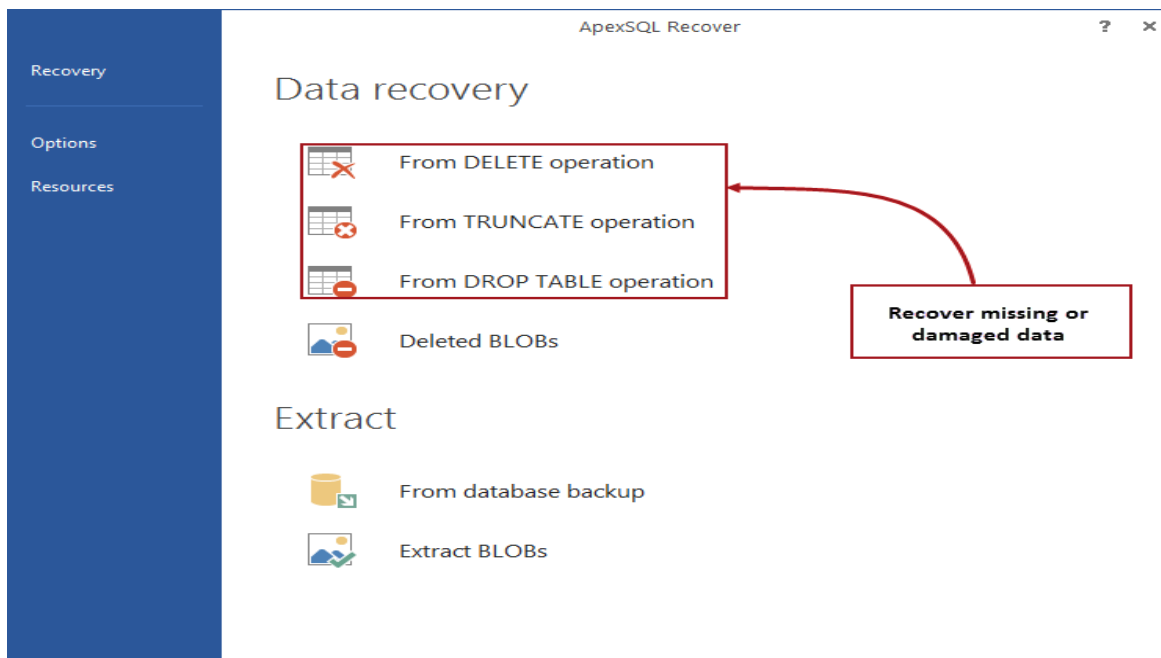
۶. مشخص کردن تغییر در مجموعه‌ای از داده‌ها

### ۳-۲-۴ ابزار ApexSQL Recover

ابزار ApexSQL Recover برای ترمیم و بازیابی داده‌های حذف‌شده کاربرد دارد. از جمله ویژگی‌های این ابزار می‌توان به موارد زیر اشاره کرد [۱۲]:

۱. بازیابی داده‌های از دست‌رفته با عملیات DELETE، TRUNCATE یا DROP TABLE (شکل ۲۴)





شکل ۲۴ بازبازی داده‌های از دست‌رفته

۲. بازبازی داده‌ها مستقیماً در پایگاه داده: بازبازی جداول از دست‌رفته مستقیماً در پایگاه داده
۳. بازبازی BLOB-های حذف‌شده و استخراج آن‌ها از فایل‌های داده
۴. فیلترینگ با جزئیات و تعیین محدوده‌ی زمانی که داده یا اشیا از دست‌رفته‌اند
۵. بازبازی ساختارهای جداول از دست‌رفته

## ۵ جمع‌بندی

بر روی کارگزار SQL، فایل‌های رویدادنگاری مختلفی ایجاد می‌شوند که در بررسی مشکلات پیش‌آمده و مسائل مربوط به کارایی و خطاها کمک خواهند کرد. ویژگی ممیزی در SQL Server امکان تهیه‌ی ممیزی از تمام اتفاقات رخ داده در کارگزار را فراهم می‌کند. رویدادها از تغییرات در تنظیمات کارگزار تا تغییر در مقداری در جدول خاصی از پایگاه داده را شامل می‌شوند. در SQL Server 2012 امکان ممیزی در سطح کارگزار در تمامی نسخه‌ها وجود دارد؛ ولی ممیزی پایگاه داده تنها در نسخه‌های Evaluation, Developer و Enterprise قابل‌اعمال است.

روش‌های جرم‌شناسی موجود در MSSQL Server، می‌توانند برای بررسی دسترسی‌های غیرمجاز به داده‌ها، کلاه‌برداری و جمع‌آوری اطلاعات برای تشخیص نفوذ استفاده شوند. در حقیقت جرم‌شناسی در SQL Server برای تشخیص تغییرات ایجادشده در پایگاه داده و منشأ اصلی تغییرات و حملات کاربرد دارد.

بیش‌تر ابزارهای جرم‌شناسی SQL Server در حالت برون‌خط اجرا می‌شوند؛ زیرا تحلیل در حالت زنده و آنلاین ممکن است باعث توقف فعالیت کارگزار و از دست رفتن داده‌ها شود.

## ۶ منابع

- [1]. <https://docs.mendix.com/refguide5/review-log-files-ms-sql-server>
- [2]. <https://docs.microsoft.com/en-us/sql/tools/configuration-manager/viewing-the-sql-server-error-log>
- [3]. <https://www.mssqltips.com/sqlservertip/1476/reading-the-sql-server-log-files-using-tsql/>
- [4]. <http://sqlmag.com/database-administration/sql-server-log-files-update>
- [5]. <https://www.red-gate.com/simple-talk/sql/learn-sql-server/managing-transaction-logs-in-sql-server/>
- [6]. <https://www.sqlshack.com/understanding-sql-server-audit/>
- [7]. <https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine>
- [8]. <https://solutioncenter.apexsql.com/how-to-setup-and-use-sql-server-audit-feature/>
- [9]. <https://www.systoolsgroup.com/forensics/sql-server/>
- [10]. <http://www.dataforensics.org/sql-mdf-forensics/>
- [11]. <http://www.xploreforensics.com/blog/sql-server-mdf.html>
- [12]. <https://www.apexsql.com>