IT/Dev CONNECTIONS

SQL Server Forensics

Who did what?

Brian Kelley
Data Architect
Truth Solutions

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

About Me

- Database / Infrastructure Architect
- Database Administrator
- SQL Server security columnist / blogger
- IT Auditor

Contact Information

K. Brian Kelley

Email: kbriankelley@acm.org

Twitter: @kbriankelley

Infrastructure/Security Blog: https://truthsolutions.wordpress.com

Personal Development Blog: https://gkdba.wordpress.com

Agenda

- Basics on Handling Evidence
- Forensics on the Fly
- Preparing Beforehand
- Outside of SQL Server

Evidence Handling

Basics for a Security Investigation

- Name a First Responder
- Try to Preserve Everything as Is
- Log Everything – Who, What, When, How
- Extra Precautions for Live SQL Server

Basics for Other Investigations

- Understand Intent
- Try to Preserve As Is
- Record Everything

Forensics on the Fly

Forensics on the Fly

How do you approach this effort?

What tools / techniques do you use?

(group activity)

Forensics on the Fly – Questions to Ask

- Who/what has access?
- When did it happen?
- What are the recovery models?
- What audit logs do I have?

Some Quick Techniques

- Current Activity
- Cached Plans
- SQL Server Error Log
- Default Trace / Schema Changes History Report

More Involved

- Ring Buffers
- Transaction Log

IT/Dev CONNECTIONS

Preparing Beforehand

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

“A failure to prepare is preparing to fail.”

Delivered by KNect365 TMT an Informa business

Forensics Outside of SQL Server

What do you usually set up?

How often is any of it reviewed?

(group activity)

Old School

- SQL Server traces (Profiler)
- C2 setting
- Common Criteria setting
- Triggers

In the Modern Era

- Audit Object
- Extended Events
- Policy Based Management (limited)

IT/Dev CONNECTIONS

Audit Support

	Server Level	Database Level
SQL Server 2008	EE only	EE only
SQL Server 2008R2	EE only	EE only
SQL Server 2012	All	EE only
SQL Server 2014	All	EE only
SQL Server 2016	All	All as of SP1
SQL Server 2017	All	All

Outside of SQL Server

Forensics Outside of SQL Server

Where else do you look?

What's most helpful?

(group activity)

Outside of SQL Server

- OS Application Event Log
- Application Logs!
- Network Trace Captures

What We Covered

- Basics on Handling Evidence
- Forensics on the Fly
- Preparing Beforehand
- Outside of SQL Server

Remaining Questions?

K. Brian Kelley

Email: kbriankelley@acm.org

Twitter: @kbriankelley

Infrastructure/Security Blog: https://truthsolutions.wordpress.com

Personal Development Blog: https://gkdba.wordpress.com