CSI:
CRIME SCENE INVESTIGATION

Database forensics invesigation

/*SQL Server as Digital Evidence Repository*/

Summary

- Current state
- Data breach examples
- Investigation process
- Digital forensics requirements (from database perspective)
- Practical digital evidence collection examples
- Houston, we have a problem
- Conclusion

COVID-19 Reality check

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

Jürgen Stock, INTERPOL Secretary General

Data breach examples

- Examples

World's Biggest Data Breaches & Hacks

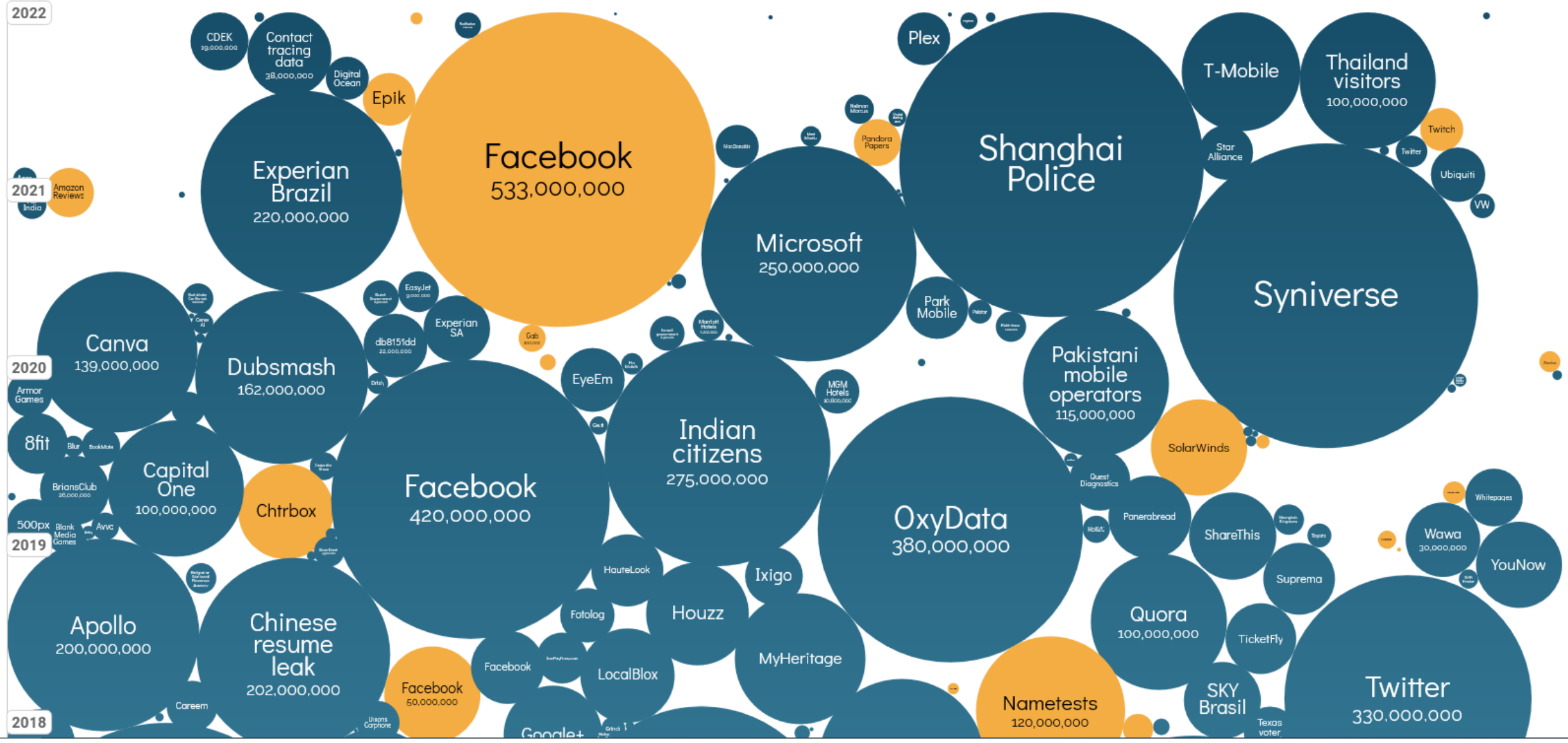
Selected events over 30,000 records

UPDATED: Sep 2022

interesting story

size: records lost **filter**

search...



SolarWinds Breach

November 2020

Capitol Hill call it “act of war” or a “digital Pearl Harbor

38,000 enterprise customers around the world

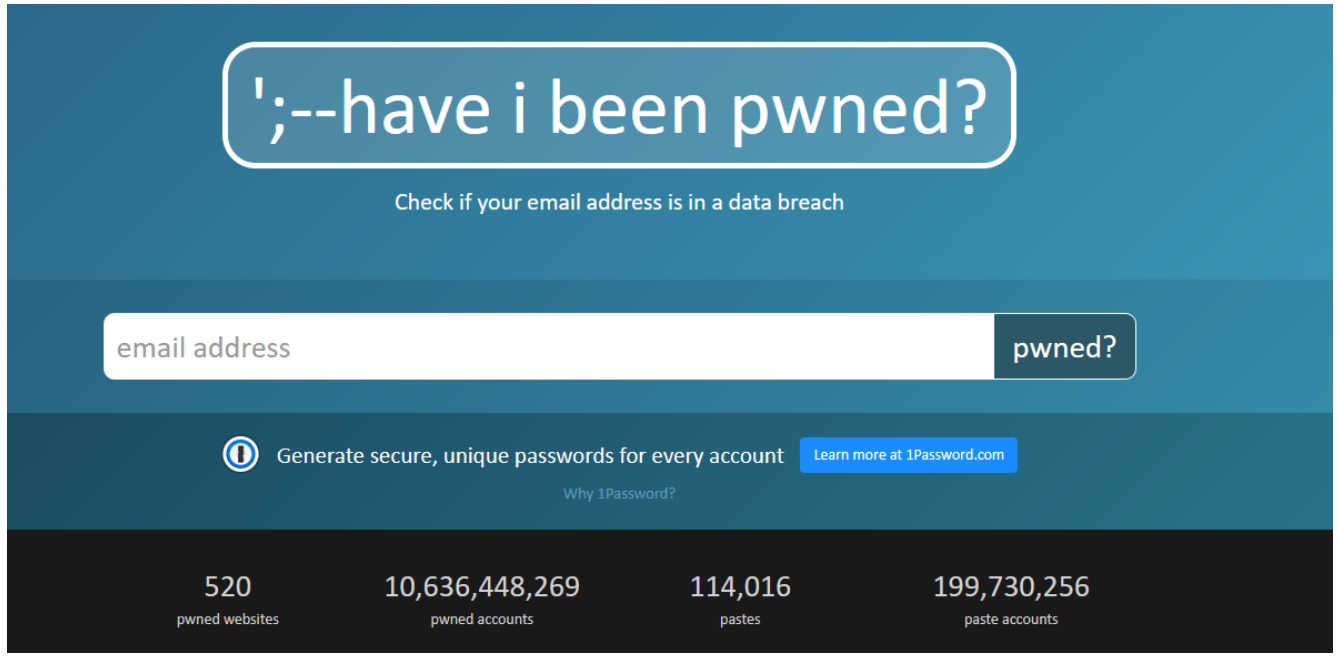
https://www.fastcompany.com/90672384/microsoft-president-brad-smith-solarwinds-exclusive

T-Mobile (August 2021)

- T-Mobile Hacker Who Stole Data on 50 Million Customers: ‘Their Security Is Awful’
- Used an unprotected router to access millions of customer records in the mobile carrier’s latest breach
- The data includes social security numbers, phone numbers, names, physical addresses, unique IMEI numbers, and driver licenses information

Check yourself please

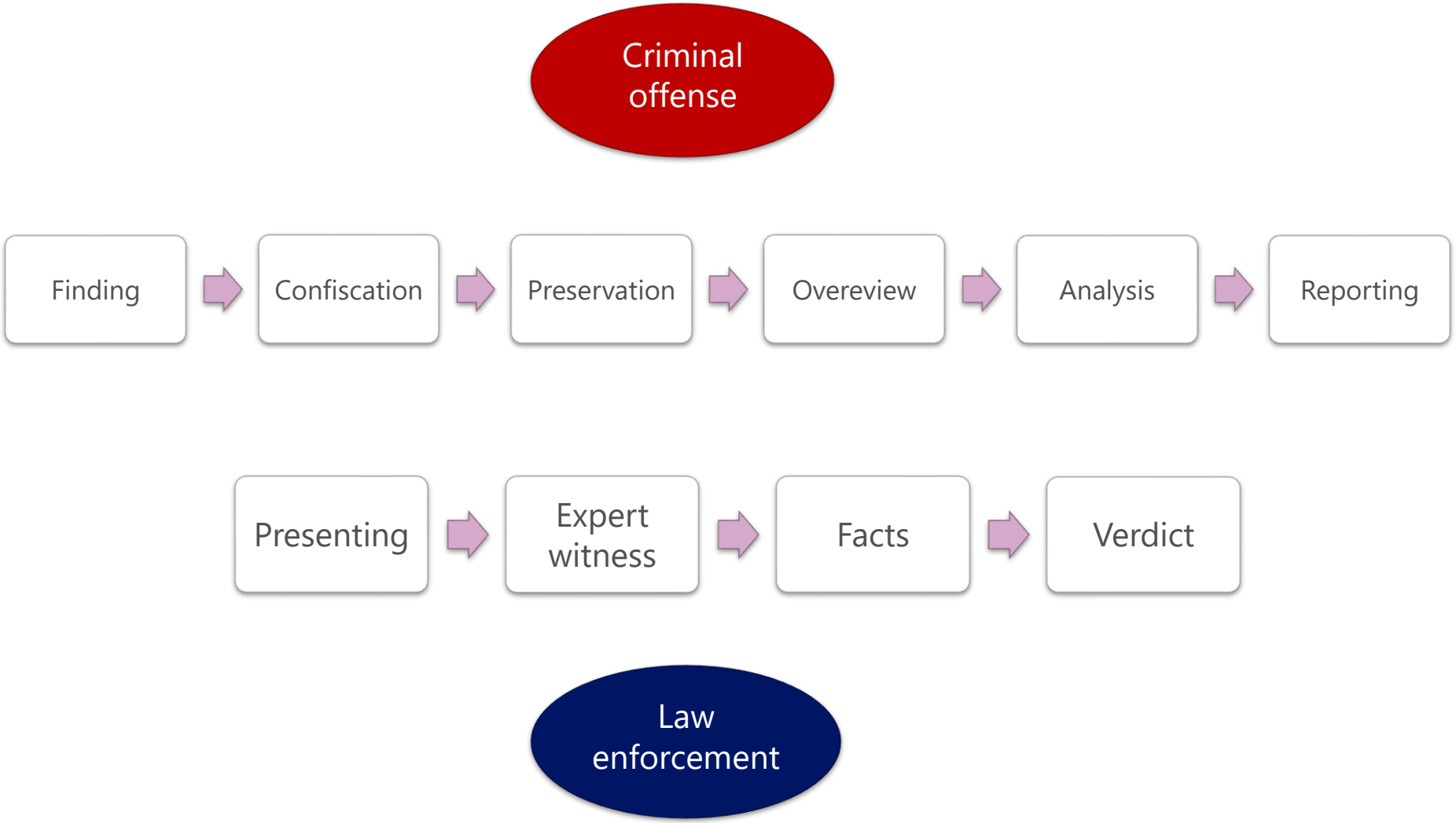
- https://haveibeenpwned.com/



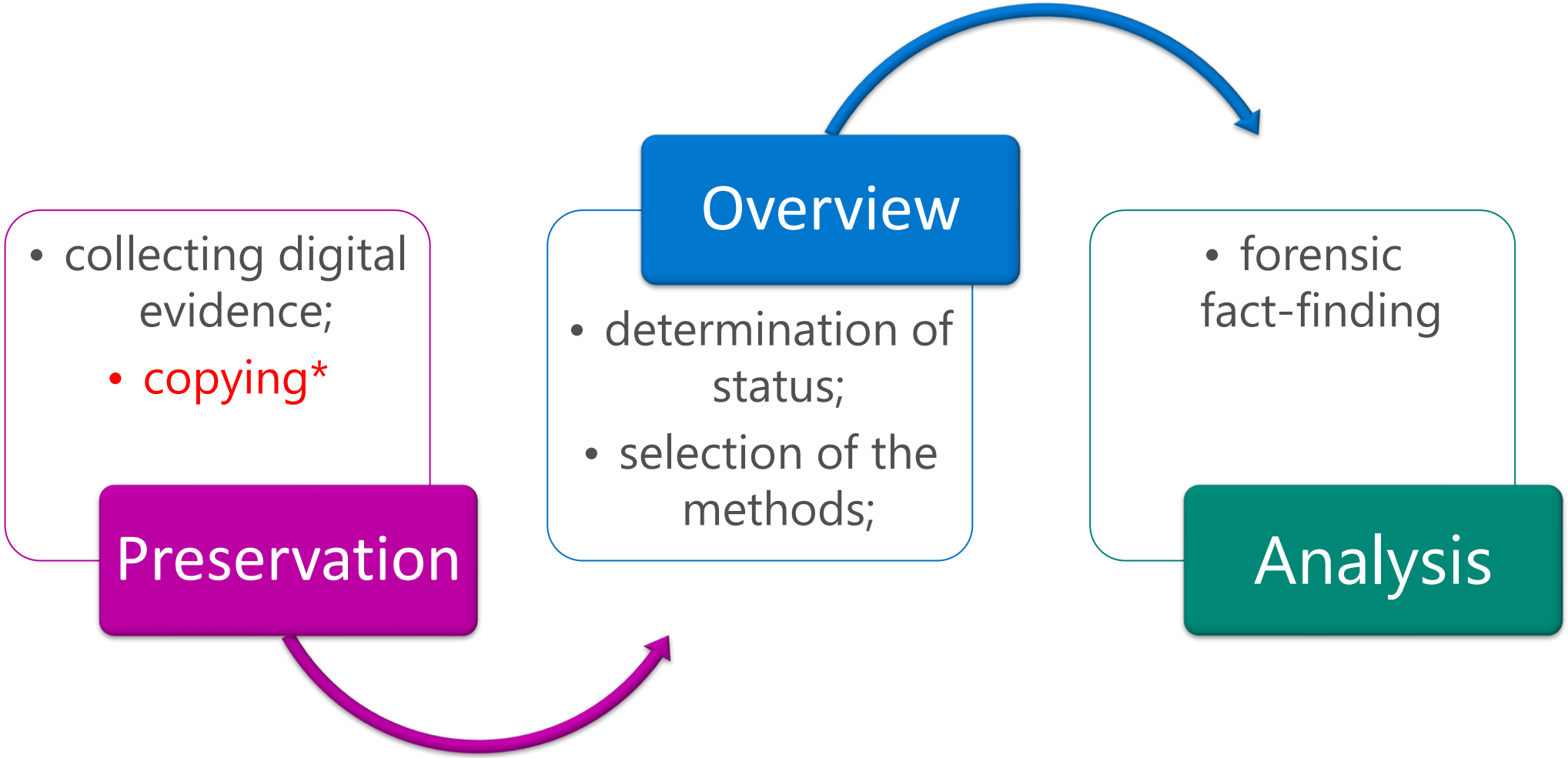
Investigation process

- General picture
- Database critical areas

General picture



Database critical areas

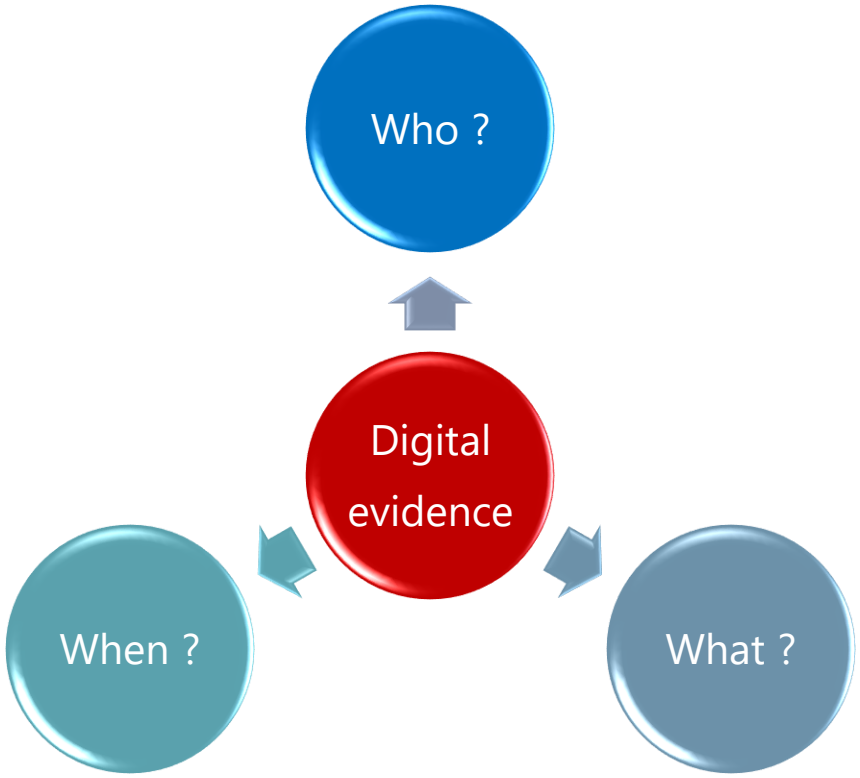


Digital forensics requirements *for db

- It is simple, implement access control;
  - Simple access control;
  - Advanced access control;

Access control

- The only way for a quality collection of digital evidence
- Independent from the client



Simple access control

Results | Messages

	StudentID	Prezime	Ime	Datum	Url	RemoteIp	RemoteAgent	Referer
8	3486	ći	siv	201 07 11:30:38.517	/nastava/index_predmet.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/nastava/index_predmet.aspx
9	3766	oki	anas	201 07 11:30:36.593	/nastava/dokumenti/index.aspx	10.0.0.1	Mozilla/5.0 (X11; U; Linux i686; bs; rv:1.9.2.14) Gec...	/nastava/dokumenti/index.aspx
10	3486	ći	siv	201 07 11:30:36.157	/nastava/index_predmet.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/nastava/index.aspx
11	3486	ći	siv	201 07 11:30:36.110	/nastava/index.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/nastava/index.aspx
12	3090	ola	ar	201 07 11:30:34.970	/obavijesti/opsimije.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/default.aspx
13	3090	ola	ar	201 07 11:30:34.750	/default.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/default.aspx
14	3090	ola	ar	201 07 11:30:30.547	/default.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/default.aspx
15	NULL	NULL	NULL	201 07 11:30:28.220	/login.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/Default.aspx
16	4045	obm	fi	201 07 11:30:28.187	/logout.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/Default.aspx
17	3486	ći	siv	201 07 11:30:27.983	/nastava/index.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/uspjeh.aspx
18	3486	ći	siv	201 07 11:30:25.297	/uspjeh.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/obavijesti/opsimije.aspx
19	2919	iča	naj	201 07 11:30:21.563	/nastava/dokumenti/pretraga.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 6.0; hr; rv:1....	/nastava/dokumenti/pretraga.aspx
20	4045	obm	fi	201 07 11:30:16.297	/Default.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/login.aspx
21	3486	ći	siv	201 07 11:30:15.923	/obavijesti/opsimije.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/default.aspx
22	NULL	NULL	NULL	201 07 11:30:15.890	/login.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/login.aspx
23	3486	ći	siv	201 07 11:30:15.780	/default.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; ...	/default.aspx
24	2919	iča	naj	201 07 11:30:14.017	/nastava/dokumenti/pretraga.aspx	10.0.0.1	Mozilla/5.0 (Windows; U; Windows NT 6.0; hr; rv:1....	/nastava/dokumenti/pretraga.aspx

Advanced access control

- Everything that has a simple access control, plus:
- Data on the DML event
- Data on DDL events

Results | Messages

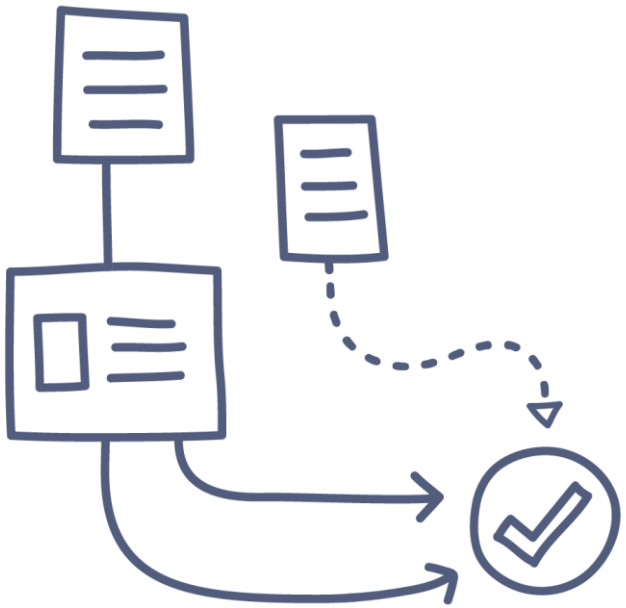
	DatabaseLogID	PostTime	DatabaseUser	Event	Schema	Object	TSQL
71	64	2017-10-27 14:33:01.860	dbo	CREATE_TABLE	Production	ProductModelProductDescriptionC...	CREATE TABLE [Production].[ProductModelProductDescription...
72	65	2017-10-27 14:33:01.863	dbo	CREATE_TABLE	Production	ProductPhoto	CREATE TABLE [Production].[ProductPhoto]([ProductPhotoI...
73	66	2017-10-27 14:33:01.867	dbo	CREATE_TABLE	Production	ProductProductPhoto	CREATE TABLE [Production].[ProductProductPhoto]([Produ...
74	67	2017-10-27 14:33:01.873	dbo	CREATE_TABLE	Production	ProductReview	CREATE TABLE [Production].[ProductReview]([ProductRevi...
75	68	2017-10-27 14:33:01.877	dbo	CREATE_TABLE	Production	ProductSubcategory	CREATE TABLE [Production].[ProductSubcategory]([Product...
76	74	2017-10-27 14:33:01.907	dbo	CREATE_TABLE	Sales	SalesOrderHeaderSalesReason	CREATE TABLE [Sales].[SalesOrderHeaderSalesReason]([...
77	69	2017-10-27 14:33:01.880	dbo	CREATE_TABLE	Purchasing	ProductVendor	CREATE TABLE [Purchasing].[ProductVendor]([ProductID] [i...
78	70	2017-10-27 14:33:01.887	dbo	CREATE_TABLE	Purchasing	PurchaseOrderDetail	CREATE TABLE [Purchasing].[PurchaseOrderDetail]([Purch...
79	71	2017-10-27 14:33:01.890	dbo	CREATE_TABLE	Purchasing	PurchaseOrderHeader	CREATE TABLE [Purchasing].[PurchaseOrderHeader]([Purc...
80	72	2017-10-27 14:33:01.897	dbo	CREATE_TABLE	Sales	SalesOrderDetail	CREATE TABLE [Sales].[SalesOrderDetail]([SalesOrderID] [i...
81	73	2017-10-27 14:33:01.903	dbo	CREATE_TABLE	Sales	SalesOrderHeader	CREATE TABLE [Sales].[SalesOrderHeader]([SalesOrderID]...
82	75	2017-10-27 14:33:01.913	dbo	CREATE_TABLE	Sales	SalesPerson	CREATE TABLE [Sales].[SalesPerson]([BusinessEntityID] [in...
83	76	2017-10-27 14:33:01.917	dbo	CREATE_TABLE	Sales	SalesPersonQuotaHistory	CREATE TABLE [Sales].[SalesPersonQuotaHistory]([Busine...
84	77	2017-10-27 14:33:01.920	dbo	CREATE_TABLE	Sales	SalesReason	CREATE TABLE [Sales].[SalesReason]([SalesReasonID] [in...
85	78	2017-10-27 14:33:01.923	dbo	CREATE_TABLE	Sales	SalesTaxRate	CREATE TABLE [Sales].[SalesTaxRate]([SalesTaxRateID] [i...

Practical digital evidence collection

- SQL Audit
- Temporal tables
- DDL triggers
- DML triggers

SQL Audit

- Audit Server is built in server object
  - Native DDL to control the configuration and administration
  - Supports all security levels
- Audit object automatically logs all activities in:
  - File
  - Windows Application Log
  - Windows Security Log
- Granularity in defining **who**, **what** and **when**



SQL Audit facts

- Very fast
- Starts with the SQL Server engine
- Working through GUI/Code
- Audit logs are not encrypted
- Writing in the files was significantly faster than in the event logs
- There is no option to store logs into database tables

Protecting Audit Data

Windows Security Log

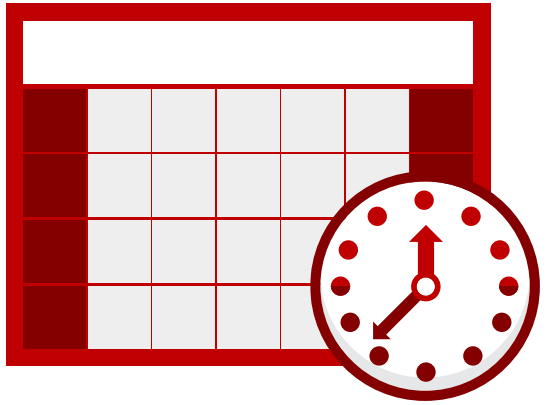
- "Tamper-proof" log
- DBA cannot clear log (assuming not an Administrator)

Copy Audit logs to secure location

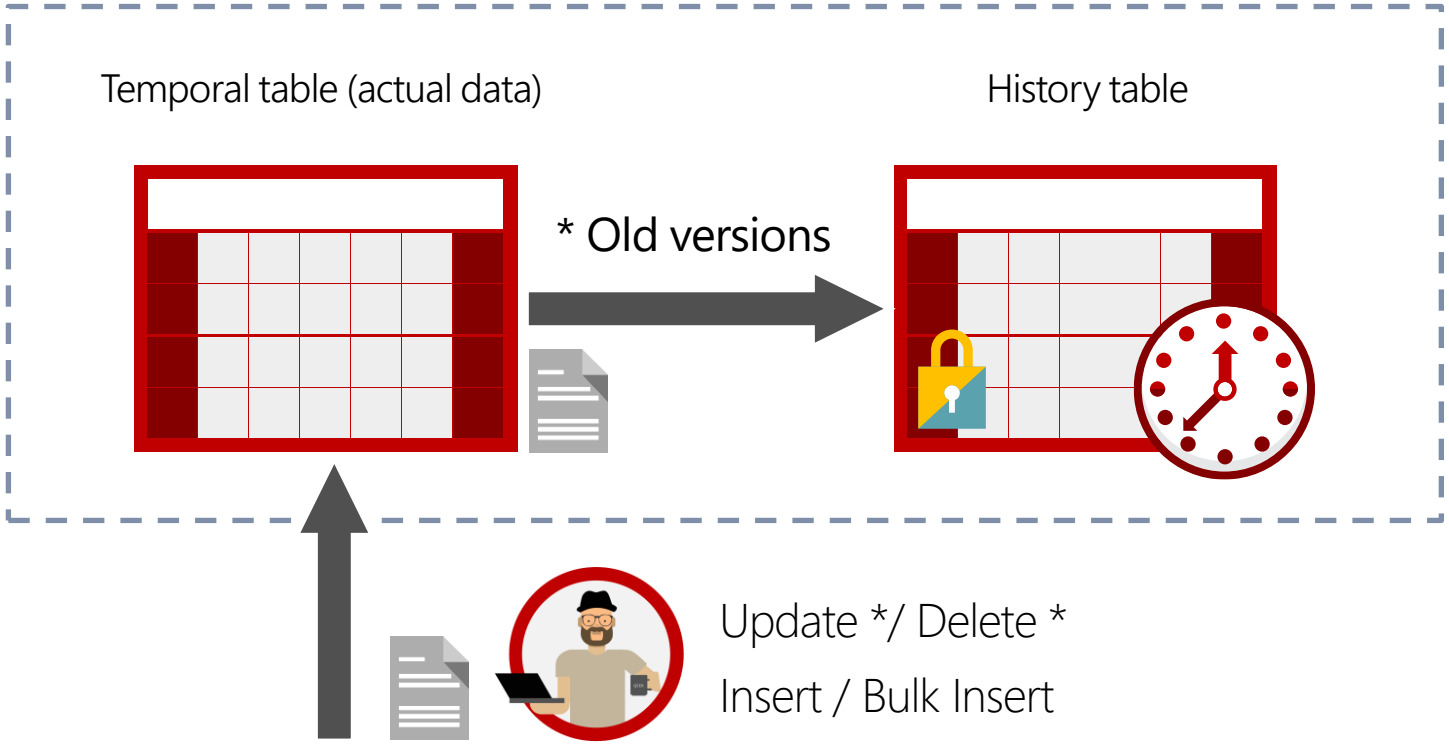
- Directory or share inaccessible by service account or DBA
- Audit logs files are shared-read and cannot be tampered with while active

Temporal tables

- Provides correct information about stored facts at any point in time
- Each temporal table consists of two tables
  - current data
  - historical data
- Tracking data changes over time
- Auditing all changes to data
- Maintaining a slowly changing dimension
- Recovering from accidental data changes and application errors



How it works?




```
SELECT * FROM
Person.BusinessEntityContact
FOR SYSTEM_TIME BETWEEN
         @Start AND @End
         WHERE ContactTypeID = 17
```

DDL triggers

- Accompanied by changes in the scheme of objects within the database;
  - CREATE, ALTER, DROP;
- Only when DDL events need to be colected

DML triggers

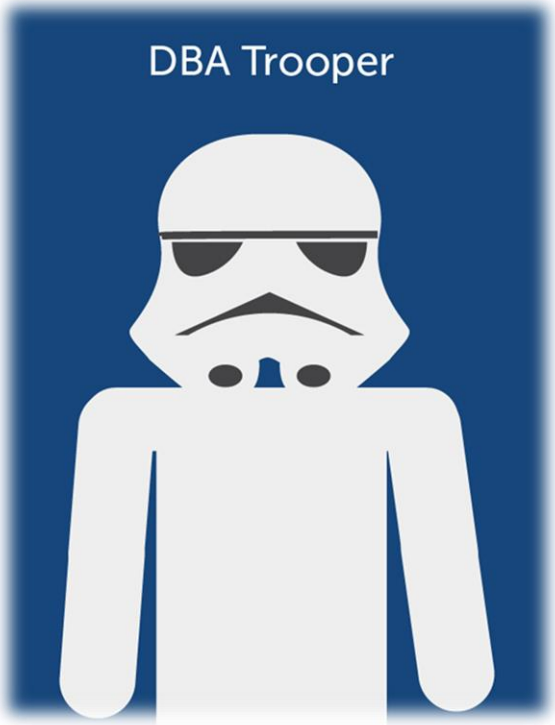
- DML operations
  - INSERT
  - UPDATE
  - DELETE
- AFTER types of SQL triggers
- Performance can be an issue
  - No need to put trigger on all tables;
  - CLR triggers can be a solution

Houston, we have a problem

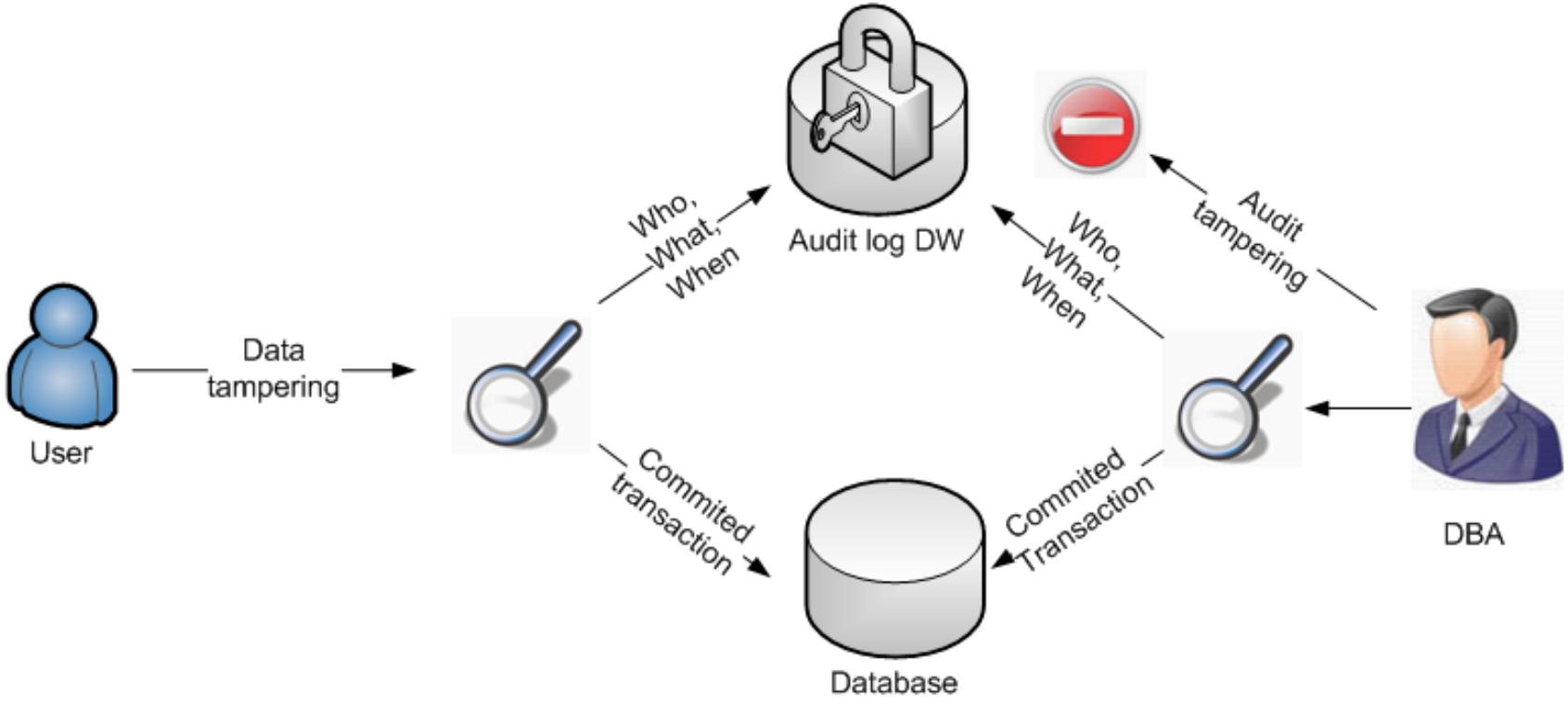
- Tampering?
- Model proposal

Tampering

- Seen so far are these methods secure enough to be used in digital forensics?*excpet SQL Audit



Model proposal



Conclusion

- Challenging
- Require different set of skills
- Combination of different data sources:
  - Servers, network, backup‘s, data and log files
- Questionable data integrity
- You can‘t rely only on standard forensic software tools
- Test it and improve it

10 COOLEST JOBS IN CYBERSECURITY

WHY THEY MAKE A DIFFERENCE AND HOW TO QUALIFY FOR THEM

Initial Jobs With Lots of Advancement Opportunities

1 DIGITAL FORENSIC ANALYST; INVESTIGATOR

"The thrill of the hunt! It's CSI for cyber geeks! You never encounter the same crime twice."

You are the detective in the world of cybersecurity – searching computers and networks for evidence in the wake of an incident.

2 PENETRATION TESTER FOR SYSTEMS AND NETWORKS

"Be a hacker, but do it legally and get paid a lot of money!"

You look for security vulnerabilities in target systems and networks to help enterprises improve their security.

3 APPLICATION PEN TESTER

"We desperately need more of this, application security has been such a black hole for so long."

You're a programming/security wizard - testing applications before deployment so they don't present opportunities for intruders.

4 SECURITY OPERATIONS CENTER (SOC) ANALYST

"The fire ranger. Better catch the initial blaze, or there goes the forest."

With an eye for detail and anomalies, you see things most others miss. You implement active prevention, active detection, active monitoring, active response.

5 CYBER DEFENDER; SECURITY ENGINEER (ENTERPRISE AND ICS)

"A leg up on your IT and engineering buddies; talk shop with them but you are saving the world from the bad guys, too."

You implement and tune firewalls, IPS/IDS, patching, admin rights, monitoring, application white listing, more.

More Advanced Jobs – Open After A Few Years of Great Performance and Specialized Training

6 HUNTER; INCIDENT RESPONDER

"The secret agent of geekdom. You walk in and say 'OK I'll take it from here.'"

While everyone else is running around shouting, "The system's dead!," you have the sense and skills to rationally figure out why.

7 SECURITY ARCHITECT

"You get to design the solution, and not just for the perimeter."

You are creative and on top of the game both technically and in business; You design and build defensible systems and are part of an adept team.

8 SECURE SOFTWARE DEVELOPMENT MANAGER

"Coolest software developers"

You protect the development team from making errors that will allow hackers to penetrate your organization and steal data. You are a programmer, but a programmer with special powers.

9 MALWARE ANALYST / REVERSE ENGINEER

"The technical elite! Only go here if you have been called. You know who you are."

You look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, and what it is trying to do or has done.

10 TECHNICAL DIRECTOR /CISO

"Making decisions; making things happen. That's coolness."

You are at the top of the tech ladder. A strategic thinker, you're hands on the design and deployment of solutions. You hold the keys to tech infrastructure.

1 CYBER FAST TRACK

"I loved CyberStart challenges - the coolest game I ever played."

"Taught me a lot; proved cybersecurity wasn't too hard to learn."

"The most fun I have had learning."

DISCOVER IF YOU HAVE THE APTITUDE

CYBERSTART: THE GAME

- No need for cyber or IT experience
- More than **250 fun challenges** protecting "real-world" bases
- **Available completely online** Everything you need is in the online Field Manual and hints.
- 19 U.S. Governors launched statewide programs for their students.

LEARN MORE AT CYBERSTART.US

2

CATAGORY/TOPIC	MODULES
Computer Hardware /Data	6
Linux and Windows	7
Networking	6
Programming	6
Common Attacks & Security	10
Others (Kali, Google, etc)	11

"We now hire cybersecurity grads only if they have hands-on mastery of these foundations" (CISO, multi $billion Silicon Valley tech leader)

MASTER THE FOUNDATIONS

CYBERSTART: ESSENTIALS

- Core technologies: How they work and are attacked
- Online, hands-on immersion training, in **46 modules**
- Progress at your own pace. Quizzes and tests on each module
- **National exam** to reach silver or gold levels

3 EMPLOYER INTERVIEWS BEFORE ACCEPTANCE

GET SKILLS EMPLOYERS NEED AND A COOL JOB!

- Veterans' Academies, Women's Academies, and Open Academies
- Three SANS immersion courses and three high value GIAC certifications
- **%90 job placement** in 6 months
- Also available as Certificate in Applied Cyber Security (ACS) at SANS.edu and other accredited colleges and universities

LEARN MORE AT USCYBERACADEMY.SANS.ORG

"Completing the SANS VetSuccess Academy not only influenced my career plans, it defined them - opening doors that were inaccessible to me otherwise. In fact, being selected into the VetSuccess program was a "hitting the jackpot" moment for me."

Ed Russell, USAF (ret) NTT Security

UNITED STATES CYBER ACADEMY


Osijek
E70
E-75
Novi Sad
Нови Сад
Slavonski
Brod
E70
E-70
E661
Šabac
Bijeljina
Шабац
Bosna i
Hercegovina
Tuzla
Zenica
Sarajevo
Kraljeve Vode
Златибор
Šibenik
Split
Mostar
Crna Gora
Dubrovnik
Podgorica