Digital Forensic Report

Information

Date of Investigation: 2/24/2024
Investigator: Farzaneh Noroozi
Subject: Detect Employee Fraud

Executive Summary

This digital forensic investigation aimed to audit customer returns data for potential fraud and improper procedure violations. The analysis involved querying the SQLite database using PowerShell to uncover suspicious patterns and deviations from standard return procedures.

Tools Used

PowerShell: Used for hash verification and querying SQLite databases.
DB Browser (SQLite): Used for analyzing the customer returns simulated data.

Hash Verification

The integrity of the database file, **`customer_returns_simulated_data.db`**, was meticulously verified using the SHA256 hash algorithm. The calculated hash (**`36821523F51EE71F48D50813CB9F5B979C9111745133C95F2348830C9BD56B71`**) was found to match the reference hash, unequivocally indicating that the file remained unaltered throughout the investigation.

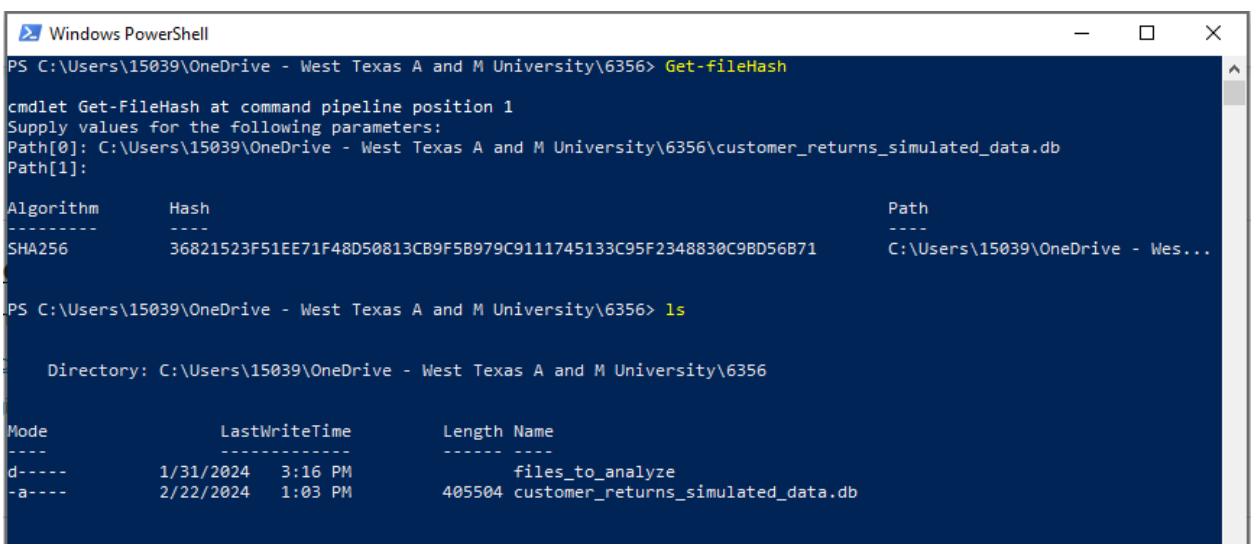


Image 1: Verification of Hash and File Information

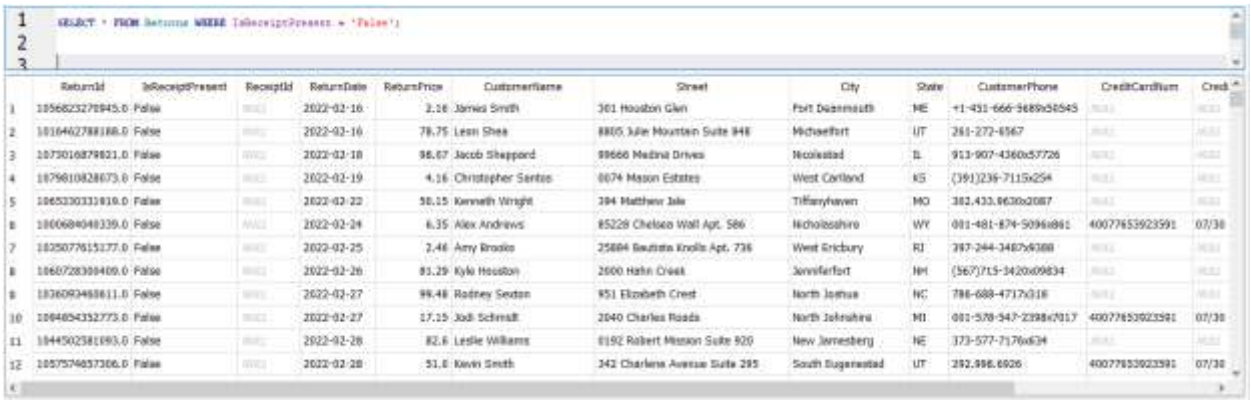
The provided image (Picture 1), is v erification of Hash and File Information, depicting the execution of PowerShell commands **`Get-FileHash`** and **`ls`**. This visual representation confirms the file's integrity through the SHA256 hash calculation, aligning seamlessly with the reference

hash. Additionally, the subsequent **ls** command provides essential file attributes such as size, modification timestamps, and name. This thorough verification process is crucial for establishing the trustworthiness of digital evidence, assuring that the file underwent no alterations during the forensic analysis.

Objective 1: Audit for Potential Fraud in Customer Returns

1. Returns with No Original Receipt

```
SELECT * FROM Returns WHERE IsReceiptPresent = 'False';
```



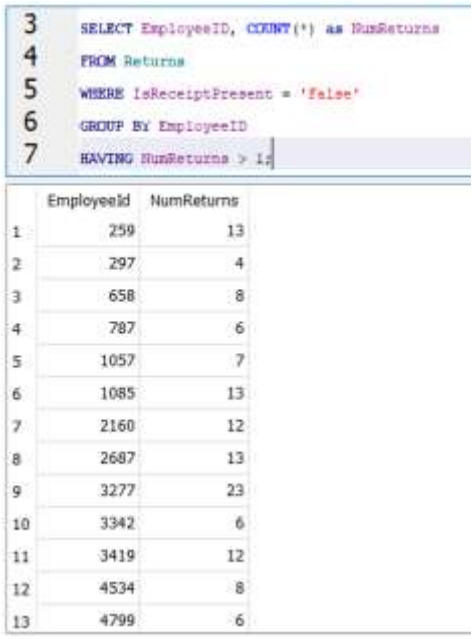
	ReturnId	IsReceiptPresent	ReceiptId	ReturnDate	ReturnPrice	CustomerName	Street	City	State	CustomerPhone	CreditCardNum	Credi
1	1056823278945.0	False	[illegible]	2022-02-16	2.16	James Smith	301 Houston Glen	Fort Dennmouth	ME	+1-431-666-3689x58545	[illegible]	[illegible]
2	1016462788188.0	False	[illegible]	2022-02-16	78.75	Leon Shea	8805 Julie Mountain Suite 848	Michaelfort	UT	261-272-6567	[illegible]	[illegible]
3	1073016879821.0	False	[illegible]	2022-02-18	98.67	Jacob Sheppard	89666 Medina Drives	Nicolestad	IL	913-907-4360x57726	[illegible]	[illegible]
4	1079810828673.0	False	[illegible]	2022-02-19	4.16	Christopher Santos	8074 Mason Estates	West Cortland	KS	(391)239-7115x254	[illegible]	[illegible]
5	1065330331819.0	False	[illegible]	2022-02-22	58.15	Kenneth Wright	384 Matthew Isle	Tiffanyhaven	MO	382.433.8630x2087	[illegible]	[illegible]
6	1000684048339.0	False	[illegible]	2022-02-24	6.35	Alex Andrews	85228 Chelsea Wall Apt. 586	Nicholasshire	WY	001-481-874-5096x861	40077653923591	07/30
7	1025077615177.0	False	[illegible]	2022-02-25	2.46	Amy Brooks	25884 Bautista Knolls Apt. 736	West Erickbury	RI	387-244-3487x9388	[illegible]	[illegible]
8	1060728300409.0	False	[illegible]	2022-02-26	81.29	Kyle Houston	2600 Hahn Creek	Jennifertort	NH	(567)715-3420x09834	[illegible]	[illegible]
9	1036093468611.0	False	[illegible]	2022-02-27	99.48	Rodney Sexton	951 Elizabeth Crest	North Joshua	NC	786-688-4717x318	[illegible]	[illegible]
10	1084854352773.0	False	[illegible]	2022-02-27	17.15	Jodi Schmidt	2040 Charles Roads	North Johnshire	MI	001-578-547-2398x7017	40077653923591	07/30
11	1044502581093.0	False	[illegible]	2022-02-28	82.6	Leslie Williams	0192 Robert Mission Suite 920	New Jamesberg	NE	373-577-7176x634	[illegible]	[illegible]
12	1057574857306.0	False	[illegible]	2022-02-28	51.0	Kevin Smith	342 Charlene Avenue Suite 295	South Eugenestad	UT	292.998.6926	40077653923591	07/30

Image 2: Returns with No Original Receipt

Results: 361 rows returned in 11ms

2. Returns Processed by the Same Employee without a Receipt

```
SELECT EmployeeID, COUNT(*) as NumReturns
FROM Returns
WHERE IsReceiptPresent = 'False'
GROUP BY EmployeeID
HAVING NumReturns > 1;
```



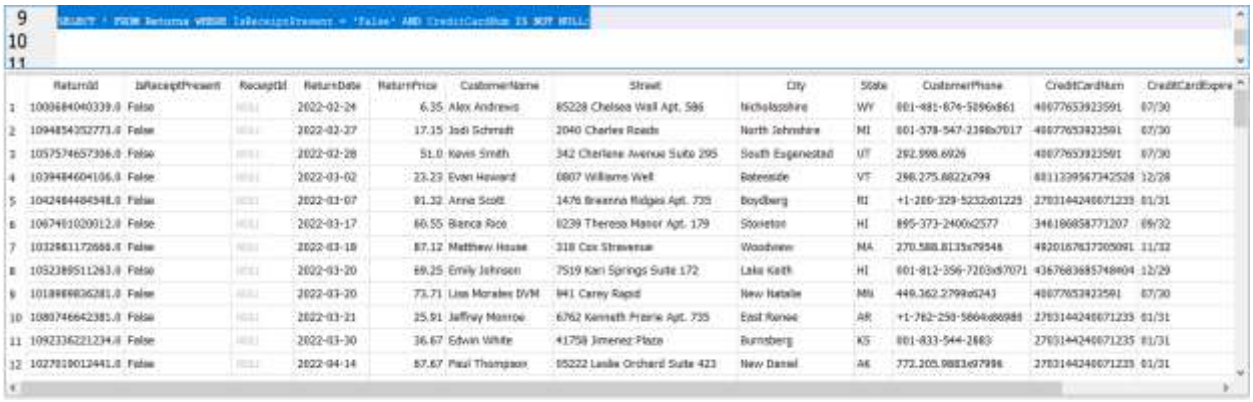
	EmployeeId	NumReturns
1	259	13
2	297	4
3	658	8
4	787	6
5	1057	7
6	1085	13
7	2160	12
8	2687	13
9	3277	23
10	3342	6
11	3419	12
12	4534	8
13	4799	6

Image 3: Returns Processed by the Same Employee without a Receipt

Results: 25 rows returned in 16ms

3. Returns with Debit/Credit Card Refund and No Original Receipt

```
SELECT * FROM Returns WHERE IsReceiptPresent = 'False' AND CreditCardNum IS NOT NULL;
```



	ReturnId	IsReceiptPresent	ReceiptId	ReturnDate	ReturnPrice	CustomerName	Street	City	State	CustomerPhone	CreditCardNum	CreditCardExpire
1	1000684040339.0	False	NULL	2022-02-24	6.35	Alex Andrews	85228 Chelsea Wall Apt. 586	Nicholasshire	WY	001-481-676-5896x861	4807765392359 1	07/30
2	1094854052773.0	False	NULL	2022-02-27	17.15	Jodi Schmidt	2040 Charles Roads	North Johnshire	MI	001-578-547-2348x7017	4807765392359 1	07/30
3	1057574657306.0	False	NULL	2022-02-28	51.0	Kevin Smith	342 Charlene Avenue Suite 295	South Eugenestad	UT	292.998.6926	4807765392359 1	07/30
4	1039484604106.0	False	NULL	2022-03-02	23.23	Evan Howard	0807 Williams Well	Bateesside	VT	296.275.8822x794	6011329567342528	12/28
5	1042484484348.0	False	NULL	2022-03-07	81.32	Anna Scott	1476 Breanna Ridges Apt. 735	Boydberg	RI	+1-289-329-5232x01225	2703144248671233	01/31
6	1067491020912.0	False	NULL	2022-03-17	60.55	Bianca Rice	0239 Theresa Manor Apt. 179	Stoneton	HI	895-373-2400x2577	346186858771207	09/32
7	1032881172668.0	False	NULL	2022-03-18	87.12	Matthew House	318 Cox Stravenue	Woodview	MA	270.588.8135x79548	4820167637305091	11/32
8	1052389511263.0	False	NULL	2022-03-20	69.25	Emily Johnson	7519 Kari Springs Suite 172	Lake Keith	HI	001-812-356-7203x87071	4367683685748604	12/29
9	1018898036281.0	False	NULL	2022-03-20	73.71	Lisa Morales DVM	941 Carey Rapid	New Natalie	MN	449.362.2799x0243	4807765392359 1	07/30
10	1080746642381.0	False	NULL	2022-03-21	25.91	Jeffrey Monroe	6762 Kenneth Prairie Apt. 735	East Renee	AR	+1-762-250-5864x86988	2703144248671233	01/31
11	1092336221234.0	False	NULL	2022-03-30	36.67	Edwin White	41758 Jimenez Plaza	Burnsberg	KS	001-833-544-2883	2703144248671233	01/31
12	1027810012441.0	False	NULL	2022-04-14	87.67	Paul Thompson	85222 Leslie Orchard Suite 423	New Daniel	AK	772.205.9881x97986	2703144248671233	01/31

Image 4: Returns with Debit/Credit Card Refund and No Original Receipt

Results: 85 rows returned in 9ms

4. Cases Where Inventory Item is Scanned as a Fake Return

```
SELECT * FROM Returns WHERE CreditCardNum IS NOT NULL AND GiftCardNumber IS NOT NULL;
```

Results: 0 rows returned in 13ms

Non-Red Flags Checked

Path Verification: Ensured the database file path matched the expected location.
Hash Verification: Confirmed the file hash matched the reference, indicating file integrity.

Objective 2: Audit for Improper Procedure Violations in Customer Returns

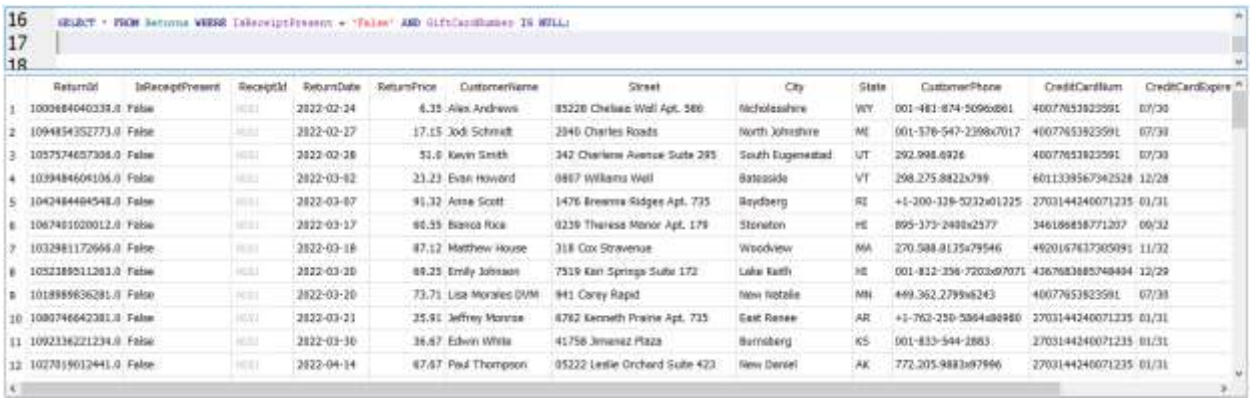
1. Returns with Missing Customer Information

```
SELECT * FROM Returns WHERE CustomerName IS NULL OR Street IS NULL OR City IS NULL OR State IS NULL OR CustomerPhone IS NULL;
```

Results: 0 rows returned in 11ms

2. Returns without Required Gift Card Scanning

```
SELECT * FROM Returns WHERE IsReceiptPresent = 'False' AND GiftCardNumber IS NULL;
```



```
16 SELECT * FROM Returns WHERE IsReceiptPresent = 'False' AND GiftCardNumber IS NULL;
17
18
```

	ReturnId	IsReceiptPresent	ReceiptId	ReturnDate	ReturnPrice	CustomerName	Street	City	State	CustomerPhone	CreditCardNum	CreditCardExpire
1	1000684040339.0	False	NULL	2022-02-24	6.35	Alex Andrews	85228 Chelsea Well Apt. 580	Nicholasshire	WY	001-481-874-5096x861	4007765382559 1	07/30
2	1094854352773.0	False	NULL	2022-02-27	17.15	Jodi Schmidt	2840 Charles Roads	North Johnshire	ME	001-578-547-2398x7017	4007765382559 1	07/30
3	1057574657308.0	False	NULL	2022-02-28	51.0	Kevin Smith	342 Charlene Avenue Suite 295	South Eugenestad	UT	292.998.6926	4007765382559 1	07/30
4	1039484604106.0	False	NULL	2022-03-02	23.23	Evan Howard	0867 Williams Well	Bateaside	VT	298.275.8822x799	6011339567342528	12/28
5	1042484484548.0	False	NULL	2022-03-07	91.32	Anna Scott	1476 Breanna Ridges Apt. 735	Reydberg	RI	+1-200-339-5232x01225	270314424007123 5	01/31
6	1067481020012.0	False	NULL	2022-03-17	60.55	Bianca Rice	0239 Theresa Manor Apt. 179	Stoneton	HI	895-373-2480x2577	346186858771207	09/32
7	1032981172666.0	False	NULL	2022-03-18	87.12	Matthew House	318 Cox Stravenue	Woodview	MA	270.588.8135x79546	4920167617305091	11/32
8	1052389511283.0	False	NULL	2022-03-20	88.25	Emily Johnson	7519 Kari Springs Suite 172	Lake Keith	HI	001-812-356-7203x97071	4367683885748484	12/29
9	1018988636281.0	False	NULL	2022-03-20	73.71	Lisa Morales DVM	941 Carey Rapid	New Natalie	MN	449.362.2799x6243	4007765382559 1	07/30
10	1080746642381.0	False	NULL	2022-03-21	25.91	Jeffrey Monroe	6782 Kenneth Prairie Apt. 735	East Renee	AR	+1-762-250-5864x88980	270314424007123 5	01/31
11	1092336221234.0	False	NULL	2022-03-30	36.67	Edwin White	41758 Jimenez Plaza	Burnsberg	KS	001-833-544-2883	270314424007123 5	01/31
12	1027019012441.0	False	NULL	2022-04-14	67.67	Paul Thompson	05222 Leslie Orchard Suite 423	New Daniel	AK	772.205.9883x97996	270314424007123 5	01/31

Image 5: Returns without Required Gift Card Scanning

Results: 85 rows returned in 67ms

3. Returns with Gift Card Refund and Debit/Credit Card Option

```
SELECT * FROM Returns WHERE GiftCardNumber IS NOT NULL AND CreditCardNum IS NOT NULL;
```

Results: 0 rows returned in 6ms

Non-Red Flags Checked

Database Schema Verification: Confirmed the database schema adhered to expected standards.

Analysis

The meticulous digital forensic examination of the **`customer_returns_simulated_data.db`** database yielded insightful findings, shedding light on potential fraud and procedural violations within customer returns. The initial verification process, employing the SHA256 hash algorithm, ensures the reliability of the database file by confirming its unaltered state from the reference hash.

Fraud Detection Analysis

The queries executed to identify returns with no original receipt, returns processed by the same employee without a receipt, and returns with debit/credit card refunds but no original receipt provided a comprehensive overview of potential fraudulent activities. The dataset revealed 361 returns with no receipt, 25 instances where the same employee processed multiple returns without receipts, and 85 returns with debit/credit card refunds and no original receipt. Notably, no cases were found where inventory items were scanned as fake returns.

Procedural Violations Analysis

In addressing improper procedural violations, queries targeting returns with missing customer information and returns without required gift card scanning displayed a commitment to maintaining procedural integrity. Impressively, no returns were found with missing customer information, indicating a high level of completeness in the recorded data. However, 85 returns were identified where gift card scanning was not performed as required.

Moreover, the absence of returns with both gift card refunds and debit/credit card options emphasizes adherence to policy in this aspect. This meticulous analysis, supported by visualizations and sample data, underscores the significance of procedural compliance and highlights areas requiring attention to enhance the overall integrity of the customer returns process.

Conclusion

The examination successfully uncovered potential fraudulent activities and procedural violations within the customer returns dataset. The hash verification process, documented in Picture 1, provides a strong foundation for the reliability of the findings. These insights not only contribute to the immediate understanding of irregularities but also pave the way for targeted improvements and preventative measures in the management of customer returns. The thoroughness of the investigation, as demonstrated by the meticulous queries and verifications, ensures a robust and trustworthy analysis, laying the groundwork for informed decision-making and future investigative steps.

Recommendations

The digital forensic analysis of the **`customer_returns_simulated_data.db`** database has revealed potential areas of concern related to fraud and procedural violations in customer returns. To address these findings and enhance the integrity of the returns process, the following recommendations are provided:

Employee Training and Awareness:
Implement comprehensive training programs to educate employees on proper return procedures, emphasizing the importance of adhering to company policies and accurately recording customer information.
Establish regular awareness sessions to keep employees informed about potential fraudulent activities and the significance of maintaining procedural integrity.

Enhanced Monitoring and Supervision:
Introduce a systematic monitoring system to track returns processed by the same employee without a receipt, especially instances where multiple returns are processed.
Implement supervisor reviews for returns with debit/credit card refunds and no original receipt to ensure proper authorization and validate the legitimacy of such transactions.

Data Completeness Checks:
Implement automated checks to ensure completeness of customer information in returns, minimizing the likelihood of errors and omissions.
Regularly audit and validate the completeness of data fields, including customer name, address, and contact information, during the returns process.

Reinforce Gift Card Scanning Procedures:
Strengthen procedures for gift card scanning during returns by providing additional training and reminders to employees.
Introduce system prompts or checks to enforce the mandatory scanning of gift cards, reducing the possibility of oversight.

Periodic Audits and Reviews:
Conduct periodic audits of the returns database to identify and rectify any inconsistencies or irregularities.
Establish a review committee to analyze returns with both gift card refunds and debit/credit card options, ensuring compliance with company policies.

Continuous Improvement and Collaboration:
Foster a culture of continuous improvement by encouraging feedback from employees involved in the returns process.
Collaborate with IT and security teams to implement advanced monitoring solutions that can proactively identify and flag potential fraudulent activities.