Lab 3

By :- Faraz Ahmed

Table of Contents

1. Executive Summary

- I started my investigation on 20th April 2025 and the objective of my investigation was to perform a digital forensics investigation on the image of the hard-disk (E01 disk) of the suspect. This forensics case about a major data breach that happened in a small retail and construction company called Angela Carver's Housing where they discovered their sensitive employee information (PII) was displayed on a malicious website which raise concerns to an unauthorized data exfiltration. The main suspect according to the company is Josh Mosko, a recently hired employee who may have been responsible for the breach. So, I used a tool called Autopsy to run full hard-disk scan to assist me with digital forensics investigation.

The main evidences for this case are the main phishing email received by Josh from unknown attacker, the replied mail sent by him after he leaked Employee and Customer data with the attacker and the suspicious alert from the Microsoft account of Josh regarding change of credentials which is done by the attacker. Other important evidence to support my conclusion are the different browser history and google searches done by Josh after he realized that he leaked the data with the attacker and got phishing by him.

Hence, my final decision according to all of the evidence and resources provided by Autopsy is that Josh Mosko was phished into sharing sensitive employee data with the attacker so I think we cannot fully blame Josh for the overall data breach in the company. He was fooled into thinking that a legit employee of the company is asking for that sensitive data and that caused him sharing it with the attacker. But Josh didn't report this email to the IT team after he realized that he was phished which makes him at fault for all of this.

So, according to me, company should train all of its employees (specially newly hired employees) how to treat these type of phishing attacks and also apply email filtering in all of the systems in the company. They should also implement Multi-Factor Authentication (MFA) in every sensitive and crucial company accounts.

2. Introduction

2.1 Case Background

- I am hired as a digital forensic specialist to investigate a data breach which happened at a small retail and construction company named Angela Carver's Housing where some of the sensitive employee information (personally identifiable information) was sourced on a known malicious website causing harm and concerns to the data security and unauthorized data exfiltration. The main suspect for this investigation is company's recently hired employee- Josh Mosko which may be responsible for this overall breach. So, company provided me with Mosko's hard drive for full data analysis and investigate it.

2.2 Objectives

- The main objective of this forensic investigation is to analyze the data inside the hard disk of Josh Mosko who is the prime suspect for any evidence regarding unauthorized data exfiltration and assemble every evidence according to different timelines to construct a proper report to present it to high executive officers in that company. Thus, to figure out if we should blame Josh behind all of these attacks or not.

3. Methodology

3.1 Tools Used

- The different tools used for forensics investigation are:-

i. Virtual Machine with Linux O.S. in vSphere.
ii. Autopsy

3.2 Procedures

- So, the Angela Carver Housing Organization's provided me with Josh Mosko's hard drive for investigation of all of the data inside it. The name of the drive was E01 drive which then we have to make an image of it which is an essential step for every digital forensics investigation to maintain the integrity of the original disk.
- We will primarily conduct our investigation on forensic tool called Autopsy. To open Autopsy, we need to open Terminal from the menu of the Linux VMware. Then create a new case and enter the basic details about this case and start the case. After that, we will be given a lot of options to select such as File Type Identification, Hashing and Hash Lookup, Keyword Search, File Extraction, Email Parsing, Recent Activity Analysis, EXIF Metadata Analysis and many other Ingest Modules that can help in forensic investigation.
- After scan is completed, we can see different file systems and result in the result page which we will conduct our basic investigation.

3.3 Chain of Custody and/or Integrity

- To comply and maintain the integrity of the original hard drive (E01 drive) of the suspect- Josh Mosko, we made an image of that drive which is the most primary and essential step for any and every forensic investigation. We can take as many images or copies of that drive as possible and the more backup we have, the better it will be when it comes to proving overall integrity of that hard-drive and investigation. Then we can scan the image drive on Autopsy for evidence and make separate folder on Desktop dedicated to store all of the evidence collected from Autopsy investigation.

4. Findings and Analysis

4.1 Timeline of Events

- 03/20/2025 23:51:41- This is when Josh received an unknown phishing email by acarver@gmail.com which made Josh share some sensitive employee data with the attacker.
- 03/20/2025 19:59:32- This is where Josh tried to log into the Microsoft account but his credentials failed which means that attacker changed his credentials when he got phished by that email.
- 03/21/2025 00:31:11- Then this is when Josh replied to the attacker's email (which he doesn't know is an attacker) to confirm that he submitted all employee data stated in that email.

4.2 Evidence Analysis

- At 03/20/2025 23:51:41, Josh received an unknown phishing email to joshmosko@angelacarverhousing.com (which is legit email address assigned by organization) from acarver@gmail.com which is not organization's assigned email and in the email, attacker mentioned that Josh have to urgently upload Employee and Customer Data which basically tricks Josh into uploading it and thus leaking the employee's sensitive data to that attacker. Then at 03/21/2025 00:31:11, he replied to the attacker's email by confirming that he uploaded the data through his/her link. Then after that 03/20/2025 19:59:32, Josh got locked out of his Microsoft account as his credentials were changed by the attacker who got hold of his original credentials and changed it.

4.3 Interesting Evidence

- 03/20/2025 22:35:48- After getting to know that he leaked employee's data, Josh thought that the attacker will sell social security number for some money so he was just curious to search it on google as "what is the price of a social security number?".
- 03/20/2025 22:36:16- After that, Josh also got curious to search that how much will attacker gain by selling employee's emails by searching "how much does an email sell for?" on google.
- 03/20/2025 22:40:04- Then he started thinking if the company can track these types of things by again searching "can companies track things send from my personal email?" on google.
- 03/20/2025 22:42:44- Then he got to know that type of email is called as Phishing Email so he got curious to find out more about it on google by searching "how to identify a phishing email" and then surfed to different sites like Reddit and Quora to get more information.
- 03/21/2025 00:10:38- After that he got worried that he might be in serious trouble so he googled about "is it okay to send personal documents from work to my personal email".

5. Conclusion and Recommendations

5.1 Summary of Findings

- ➢ So first John received an unknown email in joshmosko@angelacarverhousing.com from unknown attacker acarver@gmail.com which said that Josh has to upload the Employee and Customer Data by clicking the external link which could easily be for malicious intentions and uploaded the sensitive Employee and Customer Data to the attacker. So now attacker has all of the sensitive data and then John replied to that email by confirming that he uploaded all of the Employee and Customer Data through that external link. Then Josh received an alert from his Microsoft account that some suspicious activity is going on in his account and then he got logged out from his account and his credentials were changed by the attacker which now Josh can't even reset his account. So, he got worried what's going on so he started doing research on this topic using google, reddit and Quora and realized that he got phishing by an unknown attacker.

5.2 Mitigation Steps

- ➢ Some of the mitigation steps which an organization should take are:-

i. User Training and Awareness- Train every employee regarding how to detect and report phishing mails to IT team.

ii. Email Filtering- Company should deploy spam filters, secure email gateways and block some malicious IP addresses and domains.

iii. Restrict Suspicious Email- Company we implement certain email threat detection tools which will by default block all of the suspicious emails and also use AI/ML to restrict some of the email to certain actions.

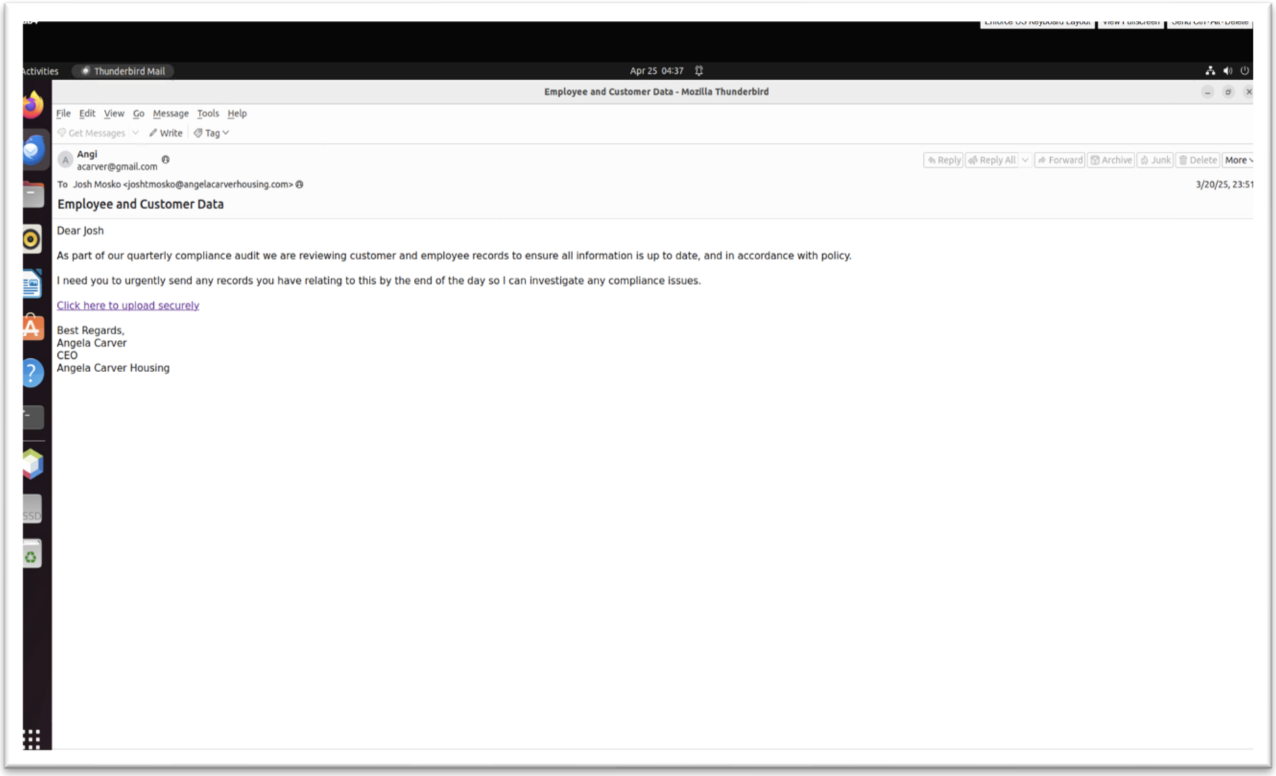
iv. Multi-Factor Authentication (MFA)- Every employee in the company should enable MFA in some critical systems and some crucial email accounts.

v. Least Privilege- Company should restrict sharing of sensitive data outside the company's environment and assign limited user permission to handle that data.

6. Appendices

6.1 Screenshots and Logs

➢



Angi
acarver@gmail.com

To Josh Mosko <joshtmosko@angelacarverhousing.com>

3/20/25, 23:51

Employee and Customer Data

Dear Josh

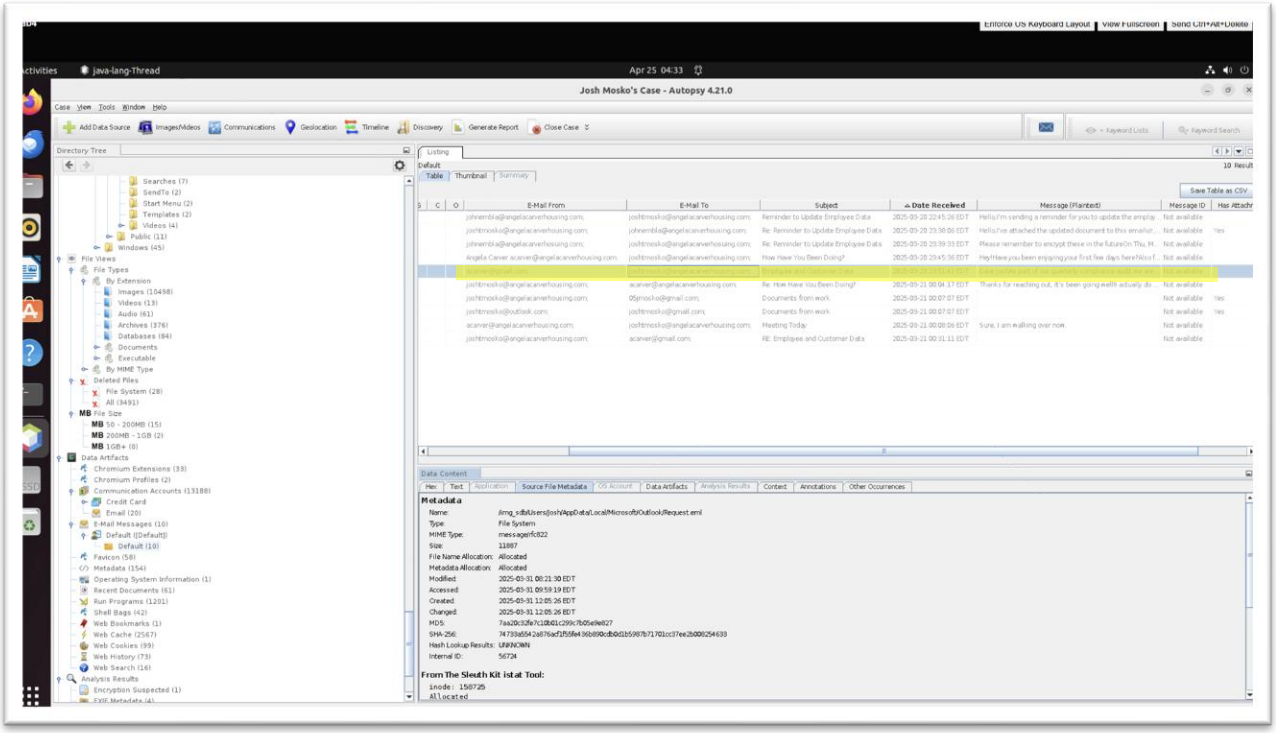
As part of our quarterly compliance audit we are reviewing customer and employee records to ensure all information is up to date, and in accordance with policy.

I need you to urgently send any records you have relating to this by the end of the day so I can investigate any compliance issues.

Click here to upload securely

Best Regards,
Angela Carver
CEO
Angela Carver Housing

Screenshot 1: Screenshot of Phishing email received by Josh from unknown attacker.



S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)	Message ID	Has Attachr
			johnembla@angelacarverhousing.com;	joshtmosko@angelacarverhousing.com;	Reminder to Update Employee Data	2025-03-20 22:45:26 EDT	Hello,I'm sending a reminder for you to update the employ...	Not available	
			joshtmosko@angelacarverhousing.com;	johnembla@angelacarverhousing.com;	Re: Reminder to Update Employee Data	2025-03-20 23:38:06 EDT	Hello,I've attached the updated document to this email.\r...	Not available	Yes
			johnembla@angelacarverhosuing.com;	joshtmosko@angelacarverhosuing.com;	Re: Reminder to Update Employee Data	2025-03-20 23:39:33 EDT	Please remember to encrypt these in the futureOn Thu, M...	Not available	
			Angela Carver acarver@angelacarverhousing.com;	joshtmosko@angelacarverhousing.com;	How Have You Been Doing?	2025-03-20 23:45:36 EDT	Hey!Have you been enjoying your first few days here?Also f...	Not available	
			acarver@gmail.com;	joshtmosko@angelacarverhousing.com;	Employee and Customer Data	2025-03-20 23:51:41 EDT	Dear Joshua, part of our quarterly compliance audit we are ...	Not available	
			joshtmosko@angelacarverhousing.com;	acarver@angelacarverhousing.com;	Re: How Have You Been Doing?	2025-03-21 00:04:17 EDT	Thanks for reaching out, it's been going well!I actually do ...	Not available	
			joshtmosko@angelacarverhousing.com;	05jmosko@gmail.com;	Documents from work	2025-03-21 00:07:07 EDT		Not available	Yes
			joshtmosko@outlook.com;	joshtmosko@gmail.com;	Documents from work	2025-03-21 00:07:07 EDT		Not available	Yes
			acarver@angelacarverhousing.com;	joshtmosko@angelacarverhousing.com;	Meeting Today	2025-03-21 00:08:06 EDT	Sure, I am walking over now.	Not available	
			joshtmosko@angelacarverhousing.com;	acarver@gmail.com;	RE: Employee and Customer Data	2025-03-21 00:31:11 EDT		Not available	

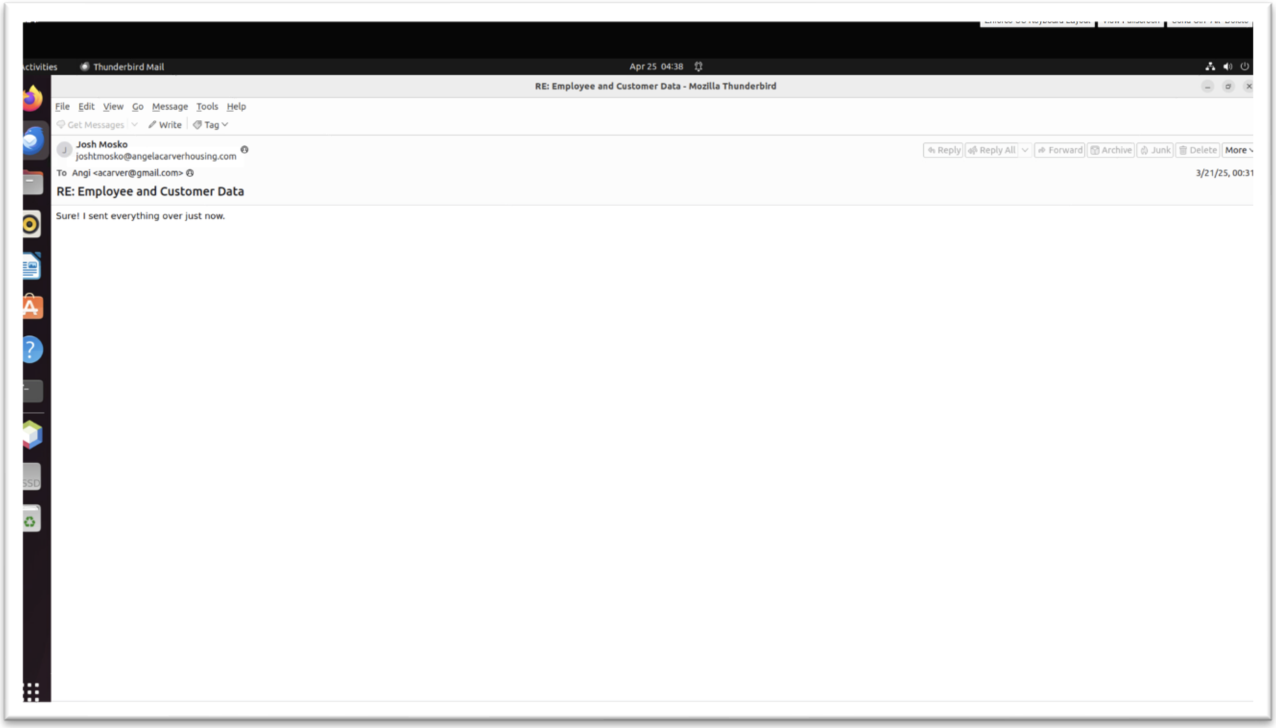
Metadata

Name:	/img_sdb/Users/Josh/AppData/Local/Microsoft/Outlook/Request.eml
Type:	File System
MIME Type:	message/rfc822
Size:	11887
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2025-03-31 08:21:30 EDT
Accessed:	2025-03-31 09:59:19 EDT
Created:	2025-03-31 12:05:26 EDT
Changed:	2025-03-31 12:05:26 EDT
MD5:	7aa20c32fe7c10b01c299c7b05e9e827
SHA-256:	74733a5542a876adf1f55fe436b890cdb0d1b5987b71701cc37ee2b008254633
Hash Lookup Results:	UNKNOWN
Internal ID:	56724

From The Sleuth Kit istat Tool:

```
inode: 158725
Allocated
```

Screenshot 2: Screenshot of date, time and hash value of the phishing email.



Josh Mosko
joshtmosko@angelacarverhousing.com

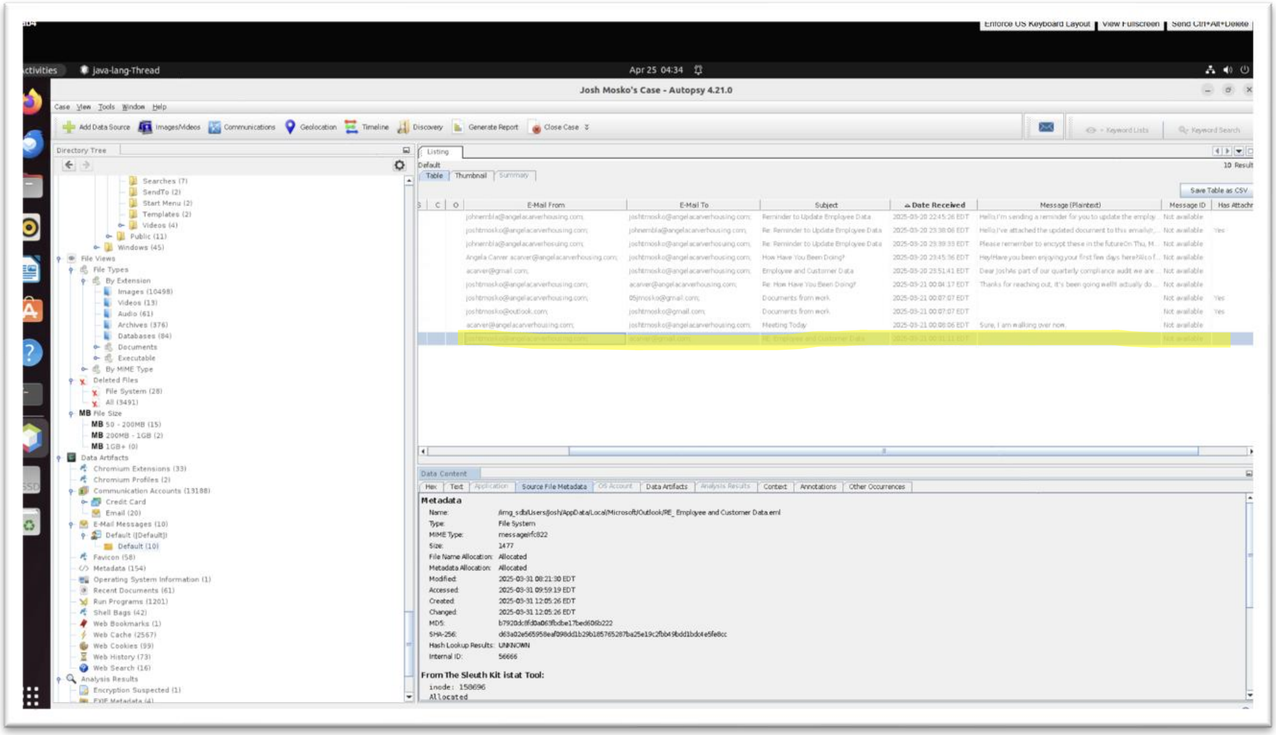
To Angi <acarver@gmail.com>

3/21/25, 00:31

RE: Employee and Customer Data

Sure! I sent everything over just now.

Screenshot 3: Screenshot of replied email sent by Josh to confirm uploading data to attacker.



S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)	Message ID	Has Attachr
			johnembla@angelacarverhousing.com;	joshtmosko@angelacarverhousing.com;	Reminder to Update Employee Data	2025-03-20 22:45:26 EDT	Hello,I'm sending a reminder for you to update the employ...	Not available	
			joshtmosko@angelacarverhousing.com;	johnembla@angelacarverhousing.com;	Re: Reminder to Update Employee Data	2025-03-20 23:38:06 EDT	Hello,I've attached the updated document to this email,r...	Not available	Yes
			johnembla@angelacarverhosuing.com;	joshtmosko@angelacarverhosuing.com;	Re: Reminder to Update Employee Data	2025-03-20 23:39:33 EDT	Please remember to encrypt these in the futureOn Thu, M...	Not available	
			Angela Carver acarver@angelacarverhousing.com;	joshtmosko@angelacarverhousing.com;	How Have You Been Doing?	2025-03-20 23:45:36 EDT	Hey!Have you been enjoying your first few days here?Also f...	Not available	
			acarver@gmail.com;	joshtmosko@angelacarverhousing.com;	Employee and Customer Data	2025-03-20 23:51:41 EDT	Dear Josh,As part of our quarterly compliance audit we are ...	Not available	
			joshtmosko@angelacarverhousing.com;	acarver@angelacarverhousing.com;	Re: How Have You Been Doing?	2025-03-21 00:04:17 EDT	Thanks for reaching out, it's been going well!I actually do ...	Not available	
			joshtmosko@angelacarverhousing.com;	05jmosko@gmail.com;	Documents from work	2025-03-21 00:07:07 EDT		Not available	Yes
			joshtmosko@outlook.com;	joshtmosko@gmail.com;	Documents from work	2025-03-21 00:07:07 EDT		Not available	Yes
			acarver@angelacarverhousing.com;	joshtmosko@angelacarverhousing.com;	Meeting Today	2025-03-21 00:08:06 EDT	Sure, I am walking over now.	Not available	
			joshtmosko@angelacarverhousing.com;	acarver@gmail.com;	RE: Employee and Customer Data	2025-03-21 00:31:11 EDT		Not available	

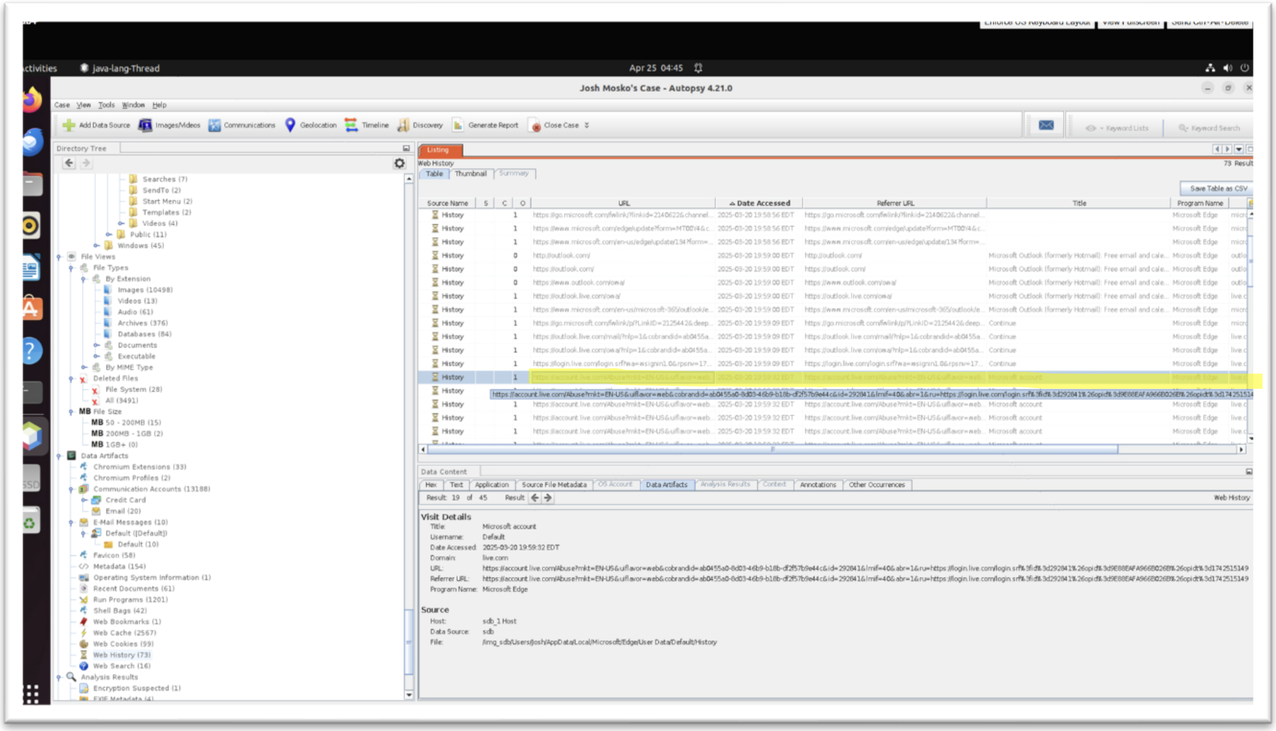
Metadata

Name: /img_sdb/Users/josh/AppData/Local/Microsoft/Outlook/RE_ Employee and Customer Data.eml
Type: File System
MIME Type: message/rfc822
Size: 1477
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2025-03-31 08:21:30 EDT
Accessed: 2025-03-31 09:59:19 EDT
Created: 2025-03-31 12:05:26 EDT
Changed: 2025-03-31 12:05:26 EDT
MD5: b7920dc8fd0a063fbdbe17bed606b222
SHA-256: d63a02e565958eaf098dd1b29b185765287ba25e19c2fbb49bdd1bdc4e5fe8cc
Hash Lookup Results: UNKNOWN
Internal ID: 56666

From The Sleuth Kit istat Tool:

```
inode: 158696
Allocated
```

Screenshot 4: Screenshot of date, time and hash value of the replied email sent by Josh.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://go.microsoft.com/fwlink/?linkid=2140622&channel...	2025-03-20 19:58:56 EDT	https://go.microsoft.com/fwlink/?linkid=2140622&channel...		Microsoft Edge	micro
History			1	https://www.microsoft.com/edge/update?form=MT00Y4&c...	2025-03-20 19:58:56 EDT	https://www.microsoft.com/edge/update?form=MT00Y4&c...		Microsoft Edge	micro
History			1	https://www.microsoft.com/en-us/edge/update/134?form=...	2025-03-20 19:58:56 EDT	https://www.microsoft.com/en-us/edge/update/134?form=...		Microsoft Edge	micro
History			0	http://outlook.com/	2025-03-20 19:59:00 EDT	http://outlook.com/	Microsoft Outlook (formerly Hotmail): Free email and cale...	Microsoft Edge	outlo
History			0	https://outlook.com/	2025-03-20 19:59:00 EDT	https://outlook.com/	Microsoft Outlook (formerly Hotmail): Free email and cale...	Microsoft Edge	outlo
History			0	https://www.outlook.com/owa/	2025-03-20 19:59:00 EDT	https://www.outlook.com/owa/	Microsoft Outlook (formerly Hotmail): Free email and cale...	Microsoft Edge	outlo
History			1	https://outlook.live.com/owa/	2025-03-20 19:59:00 EDT	https://outlook.live.com/owa/	Microsoft Outlook (formerly Hotmail): Free email and cale...	Microsoft Edge	live.c
History			1	https://www.microsoft.com/en-us/microsoft-365/outlook/e...	2025-03-20 19:59:00 EDT	https://www.microsoft.com/en-us/microsoft-365/outlook/e...	Microsoft Outlook (formerly Hotmail): Free email and cale...	Microsoft Edge	micro
History			1	https://go.microsoft.com/fwlink/p/?LinkID=2125442&deep...	2025-03-20 19:59:09 EDT	https://go.microsoft.com/fwlink/p/?LinkID=2125442&deep...	Continue	Microsoft Edge	micro
History			1	https://outlook.live.com/mail/?nlp=1&cobrandid=ab0455a...	2025-03-20 19:59:09 EDT	https://outlook.live.com/mail/?nlp=1&cobrandid=ab0455a...	Continue	Microsoft Edge	live.c
History			1	https://outlook.live.com/owa/?nlp=1&cobrandid=ab0455a...	2025-03-20 19:59:09 EDT	https://outlook.live.com/owa/?nlp=1&cobrandid=ab0455a...	Continue	Microsoft Edge	live.c
History			1	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=17...	2025-03-20 19:59:09 EDT	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=17...	Continue	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	Microsoft account	Microsoft Edge	live.c
History									
History			1	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uflavor=web...	Microsoft account	Microsoft Edge	live.c

https://account.live.com/Abuse?mkt=EN-US&uflavor=web&cobrandid=ab0455a0-8d03-46b9-b18b-df2f57b9e44c&id=292841&lmif=40&abr=1&ru=https://login.live.com/login.srf%3fid%3d292841%26opid%3d9E88EAFA966B026B%26opidt%3d174251514

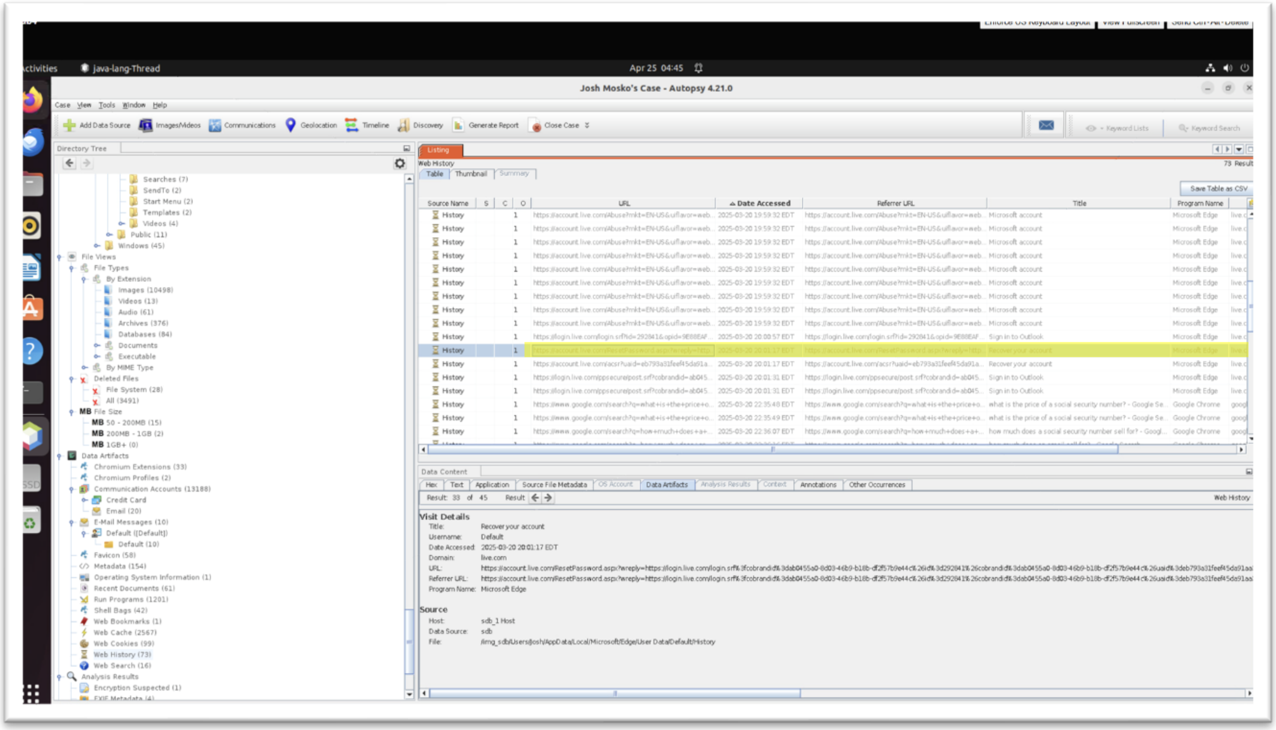
Visit Details

Title: Microsoft account
Username: Default
Date Accessed: 2025-03-20 19:59:32 EDT
Domain: live.com
URL: https://account.live.com/Abuse?mkt=EN-US&uflavor=web&cobrandid=ab0455a0-8d03-46b9-b18b-df2f57b9e44c&id=292841&lmif=40&abr=1&ru=https://login.live.com/login.srf%3fid%3d292841%26opid%3d9E88EAFA966B026B%26opidt%3d1742515149
Referrer URL: https://account.live.com/Abuse?mkt=EN-US&uflavor=web&cobrandid=ab0455a0-8d03-46b9-b18b-df2f57b9e44c&id=292841&lmif=40&abr=1&ru=https://login.live.com/login.srf%3fid%3d292841%26opid%3d9E88EAFA966B026B%26opidt%3d1742515149
Program Name: Microsoft Edge

Source

Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/josh/AppData/Local/Microsoft/Edge/User Data/Default/History

Screenshot 5: Screenshot of live alert detected by Microsoft Account for Josh's account.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://login.live.com/login.srf?id=292841&opid=9E88EAF...	2025-03-20 20:00:57 EDT	https://login.live.com/login.srf?id=292841&opid=9E88EAF...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://account.live.com/ResetPassword.aspx?wreply=http...	2025-03-20 20:01:17 EDT	https://account.live.com/ResetPassword.aspx?wreply=http...	Recover your account	Microsoft Edge	live.c
History			1	https://account.live.com/acsr?uaid=eb793a31feef45da91a...	2025-03-20 20:01:17 EDT	https://account.live.com/acsr?uaid=eb793a31feef45da91a...	Recover your account	Microsoft Edge	live.c
History			1	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	2025-03-20 20:01:31 EDT	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	2025-03-20 20:01:31 EDT	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:48 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:49 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+a+...	2025-03-20 22:36:07 EDT	https://www.google.com/search?q=how+much+does+a+...	how much does a social security number sell for? - Googl...	Google Chrome	googl

Data Content

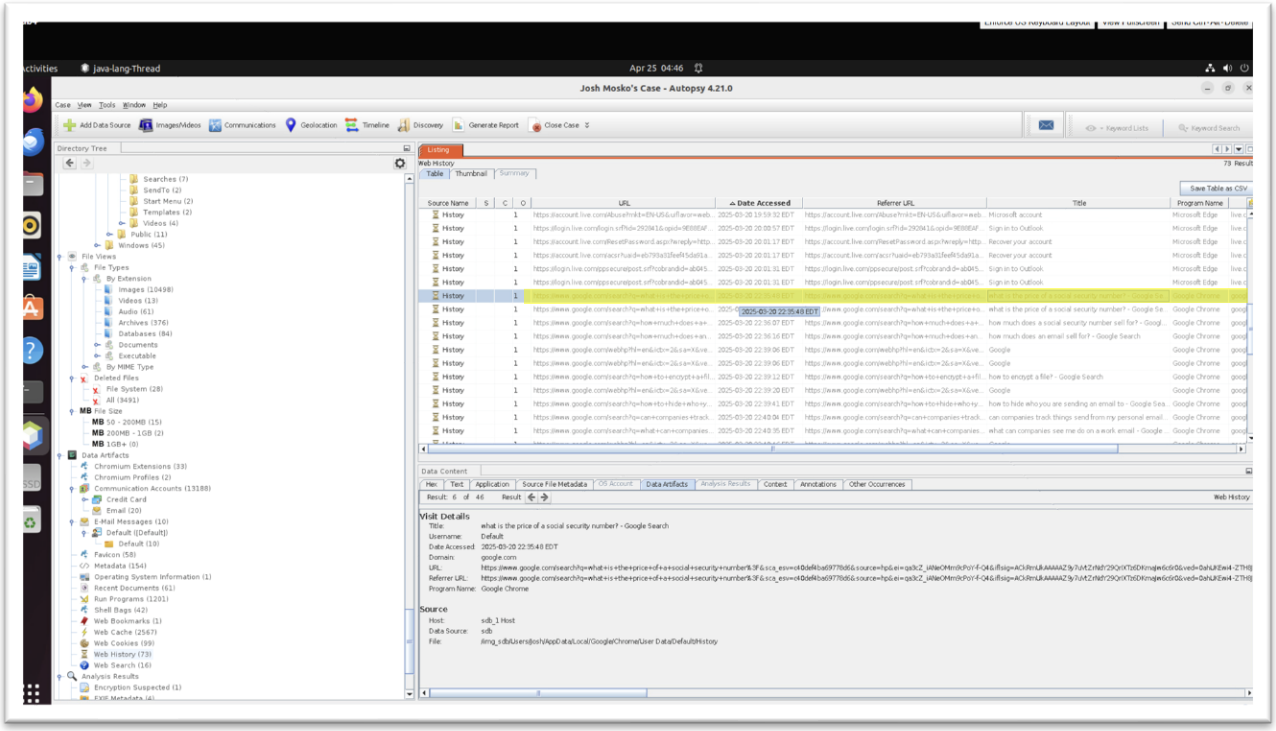
Result: 33 of 45 Result

Web History

Visit Details
Title: Recover your account
Username: Default
Date Accessed: 2025-03-20 20:01:17 EDT
Domain: live.com
URL: https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fcobrandid%3dab0455a0-8d03-46b9-b18b-df2f57b9e44c%26id%3d292841%26cobrandid%3dab0455a0-8d03-46b9-b18b-df2f57b9e44c%26uaid%3deb793a31feef45da91aa
Referrer URL: https://account.live.com/ResetPassword.aspx?wreply=https://login.live.com/login.srf%3fcobrandid%3dab0455a0-8d03-46b9-b18b-df2f57b9e44c%26id%3d292841%26cobrandid%3dab0455a0-8d03-46b9-b18b-df2f57b9e44c%26uaid%3deb793a31feef45da91aa
Program Name: Microsoft Edge

Source
Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/Josh/AppData/Local/Microsoft/Edge/User Data/Default/History

Screenshot 6: Screenshot of Reset Password of Josh's account in Microsoft.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://login.live.com/login.srf?id=292841&opid=9E88EAF...	2025-03-20 20:00:57 EDT	https://login.live.com/login.srf?id=292841&opid=9E88EAF...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://account.live.com/ResetPassword.aspx?wreply=http...	2025-03-20 20:01:17 EDT	https://account.live.com/ResetPassword.aspx?wreply=http...	Recover your account	Microsoft Edge	live.c
History			1	https://account.live.com/acsr?uaid=eb793a31feef45da91a...	2025-03-20 20:01:17 EDT	https://account.live.com/acsr?uaid=eb793a31feef45da91a...	Recover your account	Microsoft Edge	live.c
History			1	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	2025-03-20 20:01:31 EDT	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	2025-03-20 20:01:31 EDT	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:48 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:48 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+a+...	2025-03-20 22:36:07 EDT	https://www.google.com/search?q=how+much+does+a+...	how much does a social security number sell for? - Googl...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+an...	2025-03-20 22:36:16 EDT	https://www.google.com/search?q=how+much+does+an...	how much does an email sell for? - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+encrypt+a+fil...	2025-03-20 22:39:12 EDT	https://www.google.com/search?q=how+to+encrypt+a+fil...	how to encrypt a file? - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:20 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+hide+who+y...	2025-03-20 22:39:41 EDT	https://www.google.com/search?q=how+to+hide+who+y...	how to hide who you are sending an email to - Google Sea...	Google Chrome	googl
History			1	https://www.google.com/search?q=can+companies+track...	2025-03-20 22:40:04 EDT	https://www.google.com/search?q=can+companies+track...	can companies track things send from my personal email...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+can+companies...	2025-03-20 22:40:35 EDT	https://www.google.com/search?q=what+can+companies...	what can companies see me do on a work email - Google ...	Google Chrome	googl

Data Content

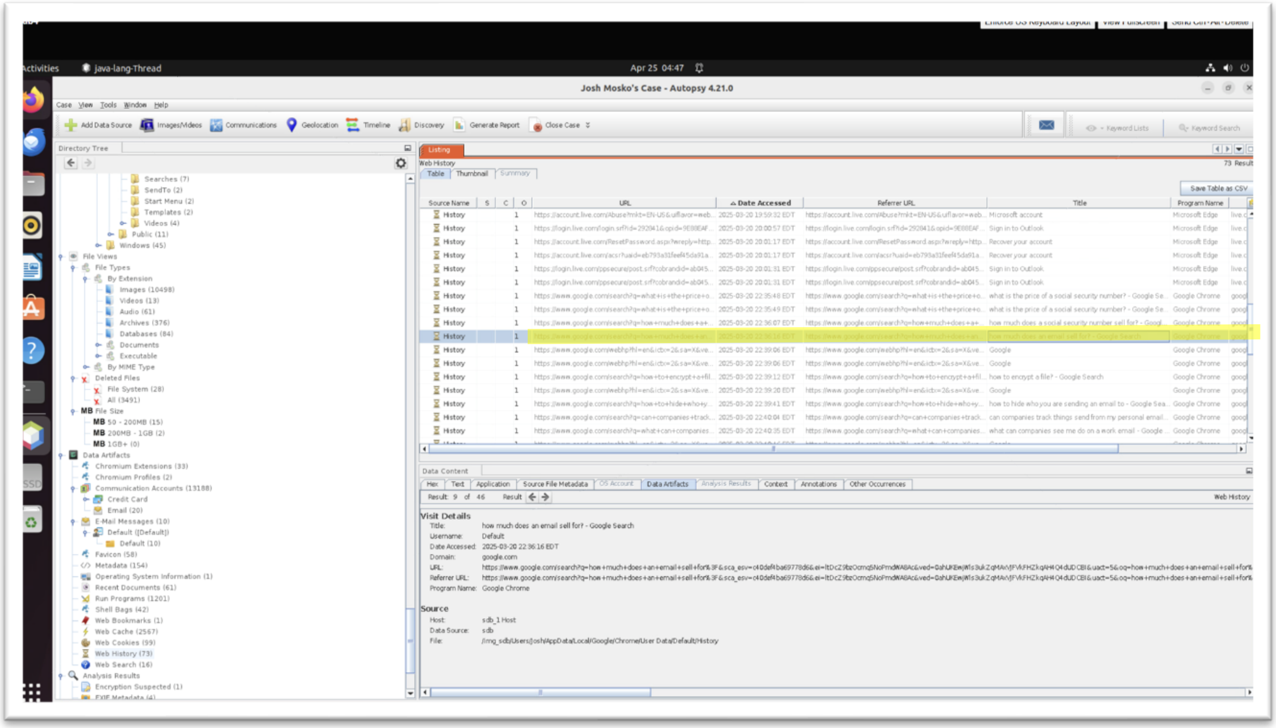
Result: 6 of 46 Result

Web History

Visit Details
Title: what is the price of a social security number? - Google Search
Username: Default
Date Accessed: 2025-03-20 22:35:48 EDT
Domain: google.com
URL: https://www.google.com/search?q=what+is+the+price+of+a+social+security+number%3F&sca_esv=c40def4ba69778d6&source=hp&ei=qa3cZ_iANeOMm9cPoY-f-Q4&iflsig=ACkRmUkAAAAAZ9y7uVtZrNdY29QrXTz6DKmajw6c6r0&ved=0ahUKEwi4-ZTH8
Referrer URL: https://www.google.com/search?q=what+is+the+price+of+a+social+security+number%3F&sca_esv=c40def4ba69778d6&source=hp&ei=qa3cZ_iANeOMm9cPoY-f-Q4&iflsig=ACkRmUkAAAAAZ9y7uVtZrNdY29QrXTz6DKmajw6c6r0&ved=0ahUKEwi4-ZTH8
Program Name: Google Chrome

Source
Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/Josh/AppData/Local/Google/Chrome/User Data/Default/History

Screenshot 7: Screenshot of Josh search "what is the price of a social security number" on google search.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	2025-03-20 19:59:32 EDT	https://account.live.com/Abuse?mkt=EN-US&uiflavor=web...	Microsoft account	Microsoft Edge	live.c
History			1	https://login.live.com/login.srf?id=292841&opid=9E88EAF...	2025-03-20 20:00:57 EDT	https://login.live.com/login.srf?id=292841&opid=9E88EAF...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://account.live.com/ResetPassword.aspx?wreply=http...	2025-03-20 20:01:17 EDT	https://account.live.com/ResetPassword.aspx?wreply=http...	Recover your account	Microsoft Edge	live.c
History			1	https://account.live.com/acsr?uaid=eb793a31feef45da91a...	2025-03-20 20:01:17 EDT	https://account.live.com/acsr?uaid=eb793a31feef45da91a...	Recover your account	Microsoft Edge	live.c
History			1	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	2025-03-20 20:01:31 EDT	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	2025-03-20 20:01:31 EDT	https://login.live.com/ppsecure/post.srf?cobrandid=ab045...	Sign in to Outlook	Microsoft Edge	live.c
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:48 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:49 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+a+...	2025-03-20 22:36:07 EDT	https://www.google.com/search?q=how+much+does+a+...	how much does a social security number sell for? - Googl...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+an...	2025-03-20 22:36:16 EDT	https://www.google.com/search?q=how+much+does+an...	how much does an email sell for? - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+encrypt+a+fil...	2025-03-20 22:39:12 EDT	https://www.google.com/search?q=how+to+encrypt+a+fil...	how to encrypt a file? - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:20 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+hide+who+y...	2025-03-20 22:39:41 EDT	https://www.google.com/search?q=how+to+hide+who+y...	how to hide who you are sending an email to - Google Sea...	Google Chrome	googl
History			1	https://www.google.com/search?q=can+companies+track...	2025-03-20 22:40:04 EDT	https://www.google.com/search?q=can+companies+track...	can companies track things send from my personal email...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+can+companies...	2025-03-20 22:40:35 EDT	https://www.google.com/search?q=what+can+companies...	what can companies see me do on a work email - Google ...	Google Chrome	googl

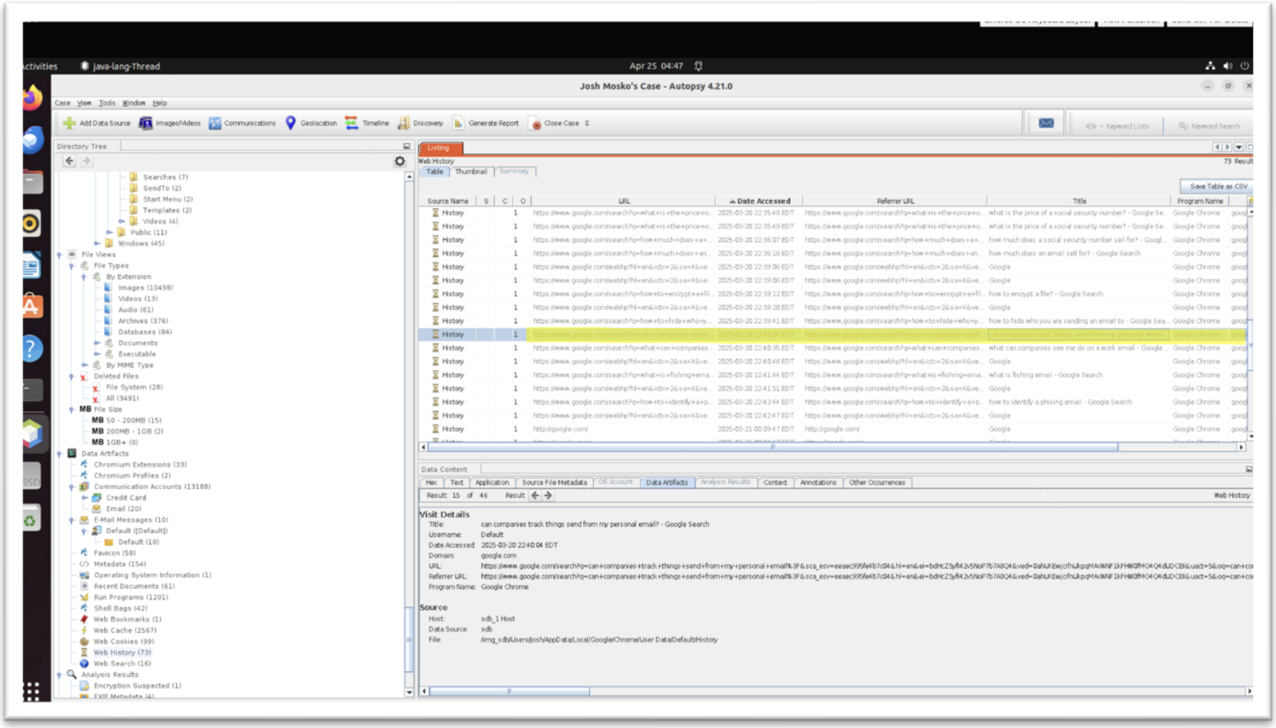
Visit Details

Title: how much does an email sell for? - Google Search
Username: Default
Date Accessed: 2025-03-20 22:36:16 EDT
Domain: google.com
URL: https://www.google.com/search?q=how+much+does+an+email+sell+for%3F&sca_esv=c40def4ba69778d6&ei=ltDcZ9bzOcmq5NoPmdWA8Ac&ved=0ahUKEwjWls3ukZqMAxVJFVkFHZkqAH4Q4dUDCBI&uact=5&oq=how+much+does+an+email+sell+for%
Referrer URL: https://www.google.com/search?q=how+much+does+an+email+sell+for%3F&sca_esv=c40def4ba69778d6&ei=ltDcZ9bzOcmq5NoPmdWA8Ac&ved=0ahUKEwjWls3ukZqMAxVJFVkFHZkqAH4Q4dUDCBI&uact=5&oq=how+much+does+an+email+sell+for%
Program Name: Google Chrome

Source

Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/Josh/AppData/Local/Google/Chrome/User Data/Default/History

Screenshot 8: Screenshot of Josh search "how much does an email sell for" on google search.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:48 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:49 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+a+...	2025-03-20 22:36:07 EDT	https://www.google.com/search?q=how+much+does+a+...	how much does a social security number sell for? - Googl...	Google Chrome	googl
History			1	https://www.google.com/search?q=how+much+does+an...	2025-03-20 22:36:16 EDT	https://www.google.com/search?q=how+much+does+an...	how much does an email sell for? - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+encrypt+a+fil...	2025-03-20 22:39:12 EDT	https://www.google.com/search?q=how+to+encrypt+a+fil...	how to encrypt a file? - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:20 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+hide+who+y...	2025-03-20 22:39:41 EDT	https://www.google.com/search?q=how+to+hide+who+y...	how to hide who you are sending an email to - Google Sea...	Google Chrome	googl
History			1	https://www.google.com/search?q=can+companies+track...	2025-03-20 22:40:04 EDT	https://www.google.com/search?q=can+companies+track...	can companies track things send from my personal email...	Google Chrome	googl
History			1	https://www.google.com/search?q=what+can+companies...	2025-03-20 22:40:35 EDT	https://www.google.com/search?q=what+can+companies...	what can companies see me do on a work email - Google ...	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:40:46 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=what+is+fishing+ema...	2025-03-20 22:41:44 EDT	https://www.google.com/search?q=what+is+fishing+ema...	what is fishing email - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:41:51 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	https://www.google.com/search?q=how+to+identify+a+p...	2025-03-20 22:42:44 EDT	https://www.google.com/search?q=how+to+identify+a+p...	how to identify a phising email - Google Search	Google Chrome	googl
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:42:47 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	googl
History			1	http://google.com/	2025-03-21 00:09:47 EDT	http://google.com/	Google	Google Chrome	googl

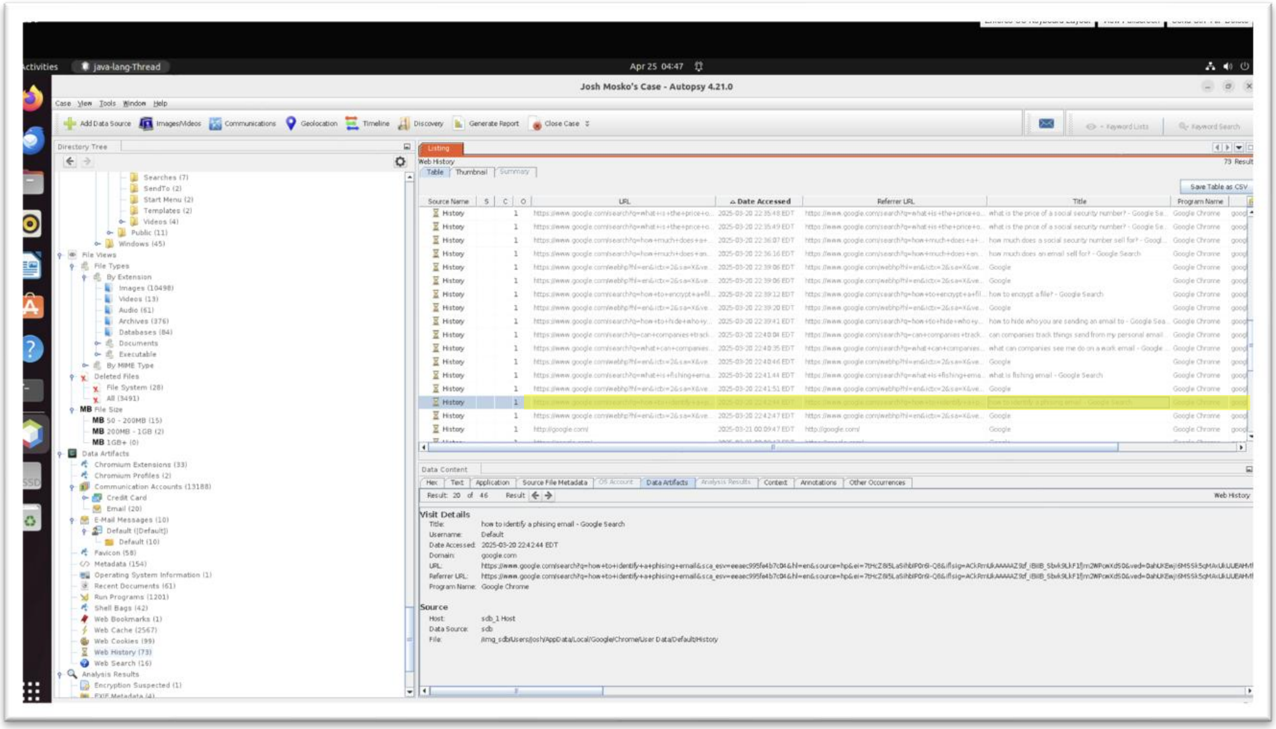
Visit Details

Title: can companies track things send from my personal email? - Google Search
Username: Default
Date Accessed: 2025-03-20 22:40:04 EDT
Domain: google.com
URL: https://www.google.com/search?q=can+companies+track+things+send+from+my+personal+email%3F&sca_esv=eeaec995fe4b7c04&hl=en&ei=bdHcZ5yfl42v5NoP7b7A8Q4&ved=0ahUKEwjcifnUkpqMAxWNF1kFHW0fMO4Q4dUDCBI&uact=5&oq=can+co
Referrer URL: https://www.google.com/search?q=can+companies+track+things+send+from+my+personal+email%3F&sca_esv=eeaec995fe4b7c04&hl=en&ei=bdHcZ5yfl42v5NoP7b7A8Q4&ved=0ahUKEwjcifnUkpqMAxWNF1kFHW0fMO4Q4dUDCBI&uact=5&oq=can+co
Program Name: Google Chrome

Source

Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/Josh/AppData/Local/Google/Chrome/User Data/Default/History

Screenshot 9: Screenshot of Josh search "can companies track things send from my personal email" on google search.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:48 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	goog
History			1	https://www.google.com/search?q=what+is+the+price+o...	2025-03-20 22:35:49 EDT	https://www.google.com/search?q=what+is+the+price+o...	what is the price of a social security number? - Google Se...	Google Chrome	goog
History			1	https://www.google.com/search?q=how+much+does+a+...	2025-03-20 22:36:07 EDT	https://www.google.com/search?q=how+much+does+a+...	how much does a social security number sell for? - Googl...	Google Chrome	goog
History			1	https://www.google.com/search?q=how+much+does+an...	2025-03-20 22:36:16 EDT	https://www.google.com/search?q=how+much+does+an...	how much does an email sell for? - Google Search	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:06 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	https://www.google.com/search?q=how+to+encrypt+a+fil...	2025-03-20 22:39:12 EDT	https://www.google.com/search?q=how+to+encrypt+a+fil...	how to encrypt a file? - Google Search	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:39:20 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	https://www.google.com/search?q=how+to+hide+who+y...	2025-03-20 22:39:41 EDT	https://www.google.com/search?q=how+to+hide+who+y...	how to hide who you are sending an email to - Google Sea...	Google Chrome	goog
History			1	https://www.google.com/search?q=can+companies+track...	2025-03-20 22:40:04 EDT	https://www.google.com/search?q=can+companies+track...	can companies track things send from my personal email...	Google Chrome	goog
History			1	https://www.google.com/search?q=what+can+companies...	2025-03-20 22:40:35 EDT	https://www.google.com/search?q=what+can+companies...	what can companies see me do on a work email - Google ...	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:40:46 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	https://www.google.com/search?q=what+is+fishing+ema...	2025-03-20 22:41:44 EDT	https://www.google.com/search?q=what+is+fishing+ema...	what is fishing email - Google Search	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:41:51 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	https://www.google.com/search?q=how+to+identify+a+p...	2025-03-20 22:42:44 EDT	https://www.google.com/search?q=how+to+identify+a+p...	how to identify a phising email - Google Search	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-20 22:42:47 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	http://google.com/	2025-03-21 00:09:47 EDT	http://google.com/	Google	Google Chrome	goog

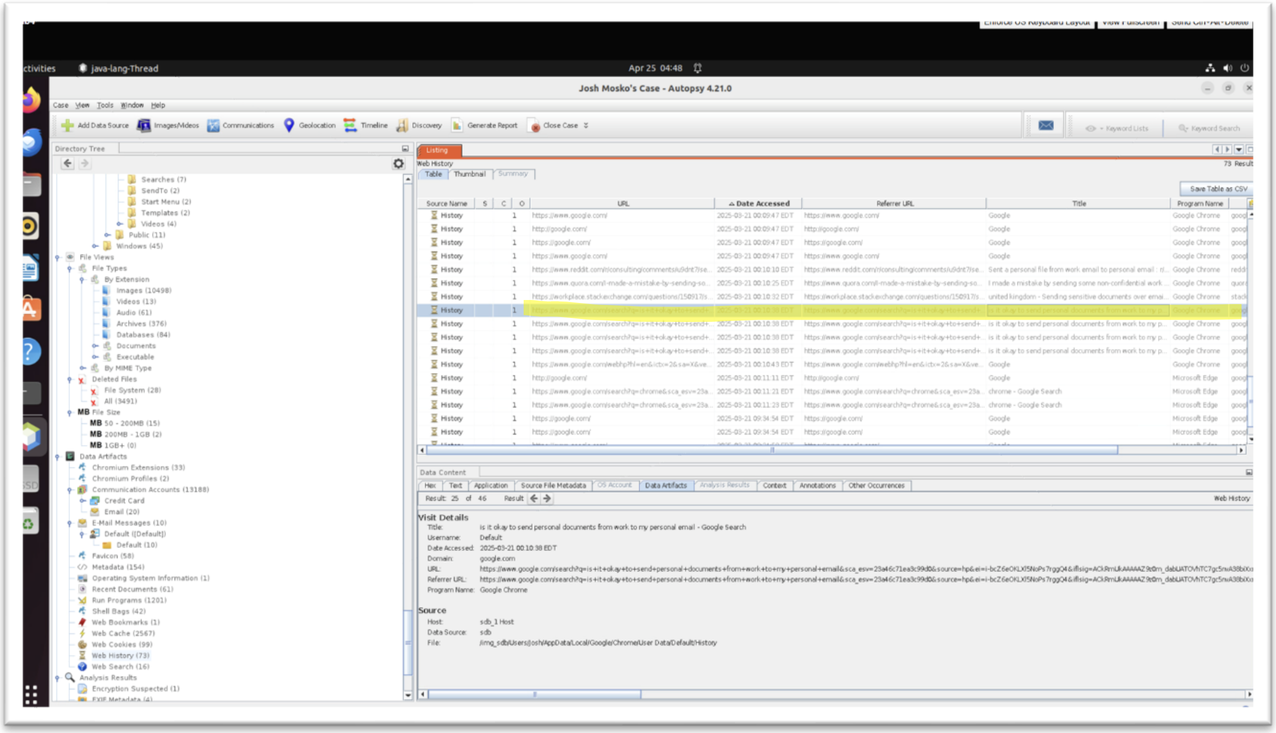
Result: 20 of 46 Result

Web History

Visit Details
Title: how to identify a phising email - Google Search
Username: Default
Date Accessed: 2025-03-20 22:42:44 EDT
Domain: google.com
URL: https://www.google.com/search?q=how+to+identify+a+phising+email&sca_esv=eeaec995fe4b7c04&hl=en&source=hp&ei=7tHcZ8l5LaSihbIP0n6I-Q8&iflsig=ACkRmUkAAAAAZ9zf_iBiIB_SbvK9LkF1fJm2WPcwXd50&ved=0ahUKEwjl6M5Sk5qMAxUkUUEAHf
Referrer URL: https://www.google.com/search?q=how+to+identify+a+phising+email&sca_esv=eeaec995fe4b7c04&hl=en&source=hp&ei=7tHcZ8l5LaSihbIP0n6I-Q8&iflsig=ACkRmUkAAAAAZ9zf_iBiIB_SbvK9LkF1fJm2WPcwXd50&ved=0ahUKEwjl6M5Sk5qMAxUkUUEAHf
Program Name: Google Chrome

Source
Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/josh/AppData/Local/Google/Chrome/User Data/Default/History

Screenshot 10: Screenshot of Josh search "how to identify a phishing email" on google search.



Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	
History			1	https://www.google.com/	2025-03-21 00:09:47 EDT	https://www.google.com/	Google	Google Chrome	goog
History			1	http://google.com/	2025-03-21 00:09:47 EDT	http://google.com/	Google	Google Chrome	goog
History			1	https://google.com/	2025-03-21 00:09:47 EDT	https://google.com/	Google	Google Chrome	goog
History			1	https://www.google.com/	2025-03-21 00:09:47 EDT	https://www.google.com/	Google	Google Chrome	goog
History			1	https://www.reddit.com/r/consulting/comments/u9dnt7/se...	2025-03-21 00:10:10 EDT	https://www.reddit.com/r/consulting/comments/u9dnt7/se...	Sent a personal file from work email to personal email : r/...	Google Chrome	redd
History			1	https://www.quora.com/I-made-a-mistake-by-sending-so...	2025-03-21 00:10:25 EDT	https://www.quora.com/I-made-a-mistake-by-sending-so...	I made a mistake by sending some non-confidential work ...	Google Chrome	quor
History			1	https://workplace.stackexchange.com/questions/150917/s...	2025-03-21 00:10:32 EDT	https://workplace.stackexchange.com/questions/150917/s...	united kingdom - Sending sensitive documents over emai...	Google Chrome	stack
History			1	https://www.google.com/search?q=is+it+okay+to+send+...	2025-03-21 00:10:38 EDT	https://www.google.com/search?q=is+it+okay+to+send+...	is it okay to send personal documents from work to my p...	Google Chrome	goog
History			1	https://www.google.com/search?q=is+it+okay+to+send+...	2025-03-21 00:10:38 EDT	https://www.google.com/search?q=is+it+okay+to+send+...	is it okay to send personal documents from work to my p...	Google Chrome	goog
History			1	https://www.google.com/search?q=is+it+okay+to+send+...	2025-03-21 00:10:38 EDT	https://www.google.com/search?q=is+it+okay+to+send+...	is it okay to send personal documents from work to my p...	Google Chrome	goog
History			1	https://www.google.com/search?q=is+it+okay+to+send+...	2025-03-21 00:10:38 EDT	https://www.google.com/search?q=is+it+okay+to+send+...	is it okay to send personal documents from work to my p...	Google Chrome	goog
History			1	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	2025-03-21 00:10:43 EDT	https://www.google.com/webhp?hl=en&ictx=2&sa=X&ve...	Google	Google Chrome	goog
History			1	http://google.com/	2025-03-21 00:11:11 EDT	http://google.com/	Google	Microsoft Edge	goog
History			1	https://www.google.com/search?q=chrome&sca_esv=23a...	2025-03-21 00:11:21 EDT	https://www.google.com/search?q=chrome&sca_esv=23a...	chrome - Google Search	Microsoft Edge	goog
History			1	https://www.google.com/search?q=chrome&sca_esv=23a...	2025-03-21 00:11:23 EDT	https://www.google.com/search?q=chrome&sca_esv=23a...	chrome - Google Search	Microsoft Edge	goog
History			1	https://google.com/	2025-03-21 09:34:54 EDT	https://google.com/	Google	Microsoft Edge	goog
History			1	https://google.com/	2025-03-21 09:34:54 EDT	https://google.com/	Google	Microsoft Edge	goog

Result: 25 of 46 Result

Web History

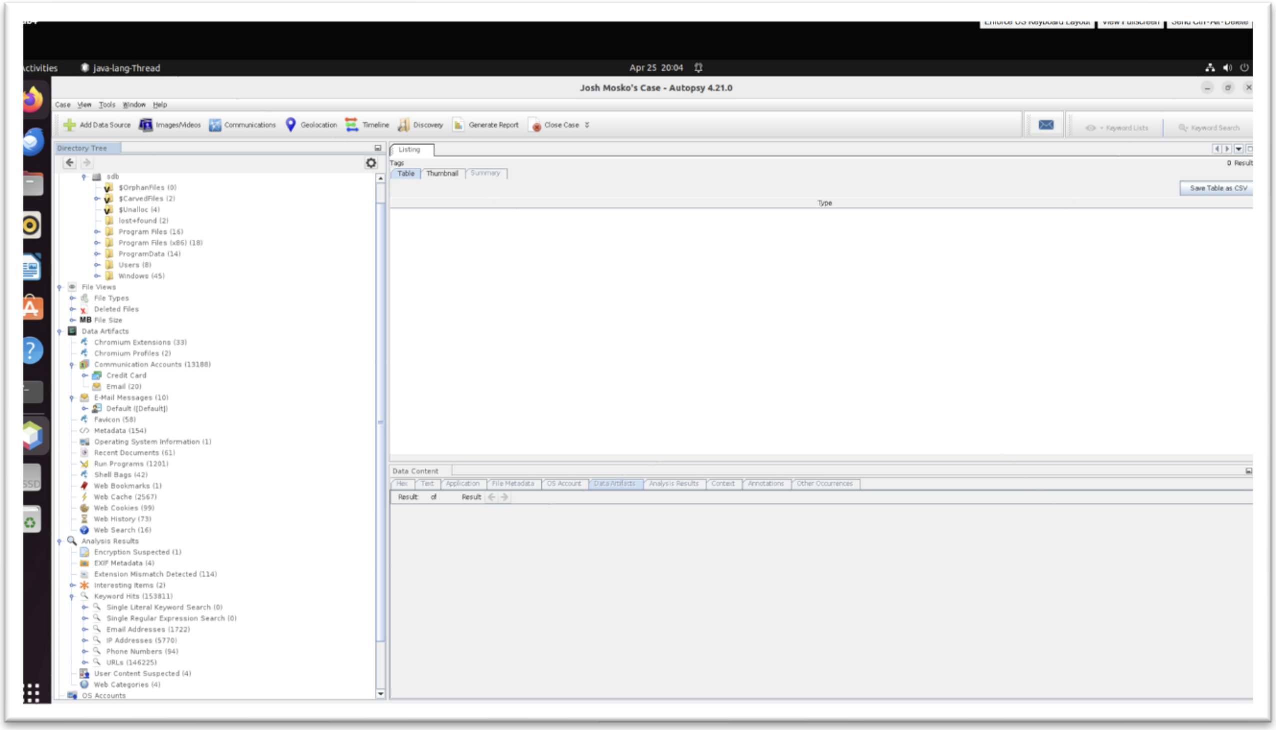
Visit Details
Title: is it okay to send personal documents from work to my personal email - Google Search
Username: Default
Date Accessed: 2025-03-21 00:10:38 EDT
Domain: google.com
URL: https://www.google.com/search?q=is+it+okay+to+send+personal+documents+from+work+to+my+personal+email&sca_esv=23a46c71ea3c99d0&source=hp&ei=i-bcZ6eOKLXl5NoPs7rggQ4&iflsig=ACkRmUkAAAAAZ9z0m_dabUATOVhTC7gc5nvA38biXo
Referrer URL: https://www.google.com/search?q=is+it+okay+to+send+personal+documents+from+work+to+my+personal+email&sca_esv=23a46c71ea3c99d0&source=hp&ei=i-bcZ6eOKLXl5NoPs7rggQ4&iflsig=ACkRmUkAAAAAZ9z0m_dabUATOVhTC7gc5nvA38biXo
Program Name: Google Chrome

Source
Host: sdb_1 Host
Data Source: sdb
File: /img_sdb/Users/Josh/AppData/Local/Google/Chrome/User Data/Default/History

Screenshot 11: Screenshot of Josh search "is it okay to send personal documents from work to my personal email" on google search.

6.2 Tool Outputs

- ➢ So, we can observe the output from the scan of Autopsy from Screenshot 12 that there are many default folders from Josh’s hard-disk image and also the ingest modules option which we selected before running the scan.



```
sdb
    $OrphanFiles (0)
    $CarvedFiles (2)
    $Unalloc (4)
    lost+found (2)
    Program Files (16)
    Program Files (x86) (18)
    ProgramData (14)
    Users (8)
    Windows (45)
File Views
  File Types
  Deleted Files
  MB File Size
Data Artifacts
  Chromium Extensions (33)
  Chromium Profiles (2)
  Communication Accounts (13188)
    Credit Card
    Email (20)
  E-Mail Messages (10)
    Default ([Default])
  Favicon (58)
  Metadata (154)
  Operating System Information (1)
  Recent Documents (61)
  Run Programs (1201)
  Shell Bags (42)
  Web Bookmarks (1)
  Web Cache (2567)
  Web Cookies (99)
  Web History (73)
  Web Search (16)
Analysis Results
  Encryption Suspected (1)
  EXIF Metadata (4)
  Extension Mismatch Detected (114)
  Interesting Items (2)
  Keyword Hits (153811)
    Single Literal Keyword Search (0)
    Single Regular Expression Search (0)
    Email Addresses (1722)
    IP Addresses (5770)
    Phone Numbers (94)
    URLs (146225)
  User Content Suspected (4)
  Web Categories (4)
OS Accounts
```

Screenshot 12: Screenshot of outputs from Autopsy application after scan is completed.

6.3 Glossary of Terms

- ➢ PII (personal identifiable information)- It is any sensitive information that can be used to identify an individual like full name, phone number, email address, social security number and home address.
- ➢ Image of a Disk- It is an exact, bit by bit copy of that original disk on which the forensics investigation is happening. This is done to maintain the integrity in the forensic investigation.
- ➢ VMware- It is a virtualization software that can run multiple virtual machines (VMs) on one physical machine.
- ➢ EXIF (exchangeable Image File Format) Metadata Analysis- It is hidden information which are stored in images clicked by cameras or smartphones which can be date and time, location, quality, etc.
- ➢ Phishing- It is a social engineering attack where attackers trick users into sharing certain sensitive information, clicking malicious website links and inviting malware into his/her systems.