Windows 10 Mail App Forensics

darkdefender · Follow

6 min read · May 27, 2019

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

- **\Users\<username>\AppData\Local\Comms\Unistore\data**

As shown below, this directory's sub-directories are a list of numerals that contain folders in alphabetical order. The numbers represent a different segment of an email, which I could have figured out just by looking within each folder, but I was lucky to find this post along the way to help me out: syntricate.com/digitalforensics.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

- AppData\Local\Comms\Unistore\data\0; Windows phone data
- AppData\Local\Comms\Unistore\data\2; contact lists within the account
- AppData\Local\Comms\Unistore\data\3; the contents/body of the email
- AppData\Local\Comms\Unistore\data\5; calendar invitations
- AppData\Local\Comms\Unistore\data\7; email attachments
- AppData\Local\Comms\Unistore\data\33; contents of invitations, maybe

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

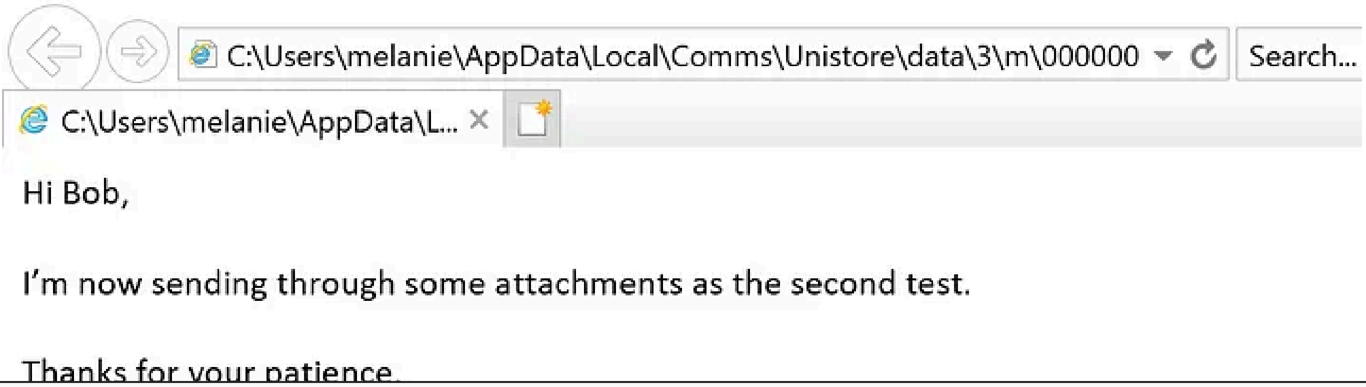
✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

And viewing the email after it's exported and saved as a .html file. Saves your brain from processing all those html tags:


C:\Users\melanie\AppData\Local\Comms\Unistore\data\3\m\000000
Search...
C:\Users\melanie\AppData\L... ×

Hi Bob,

I'm now sending through some attachments as the second test.

Thanks for your patience.

Medium

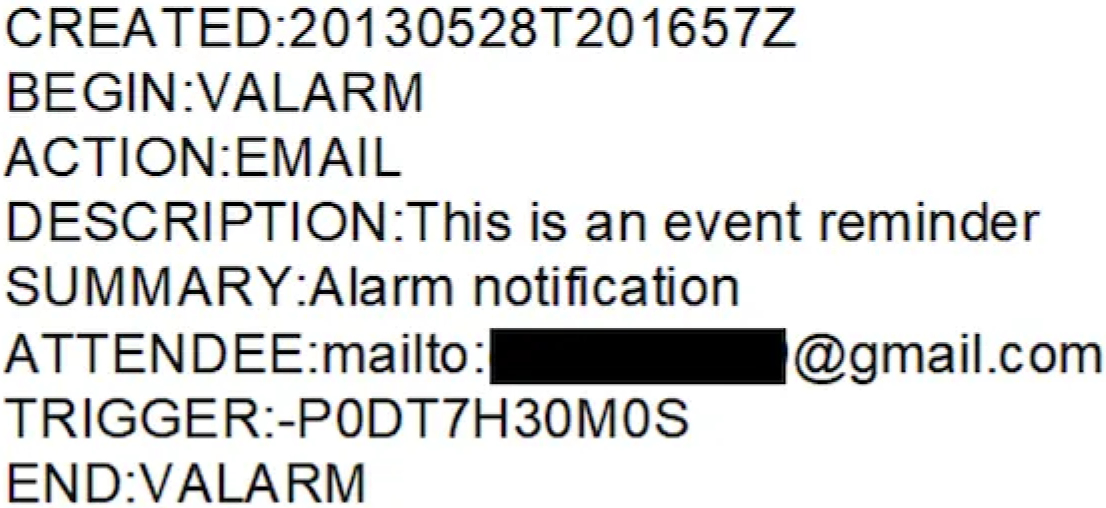
Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app



```
CREATED:20130528T201657Z
BEGIN:VALARM
ACTION:EMAIL
DESCRIPTION:This is an event reminder
SUMMARY:Alarm notification
ATTENDEE:mailto:[redacted]@gmail.com
TRIGGER:-P0DT7H30M0S
END:VALARM
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

value. Unfortunately, this was linked to my work email account, so I'm not able to show much of the contents, but I do believe the .dat files within \data\33 shows you the body of appointments or meeting invitations that have been sent to an email.

While a web browser will show you meaningless text:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

. . .

Now that we've gone through most of the directories within \AppData\Local\Comms\Unistore\data\, there is another artefact that stores similar data within the Comms directory.

Contained in **\AppData\Local\Comms\UnistoreDB**, there is a database called **store.vol** which, as the name suggests, stores email content in one repository. The notable tables within this database include Message, Contact

Medium

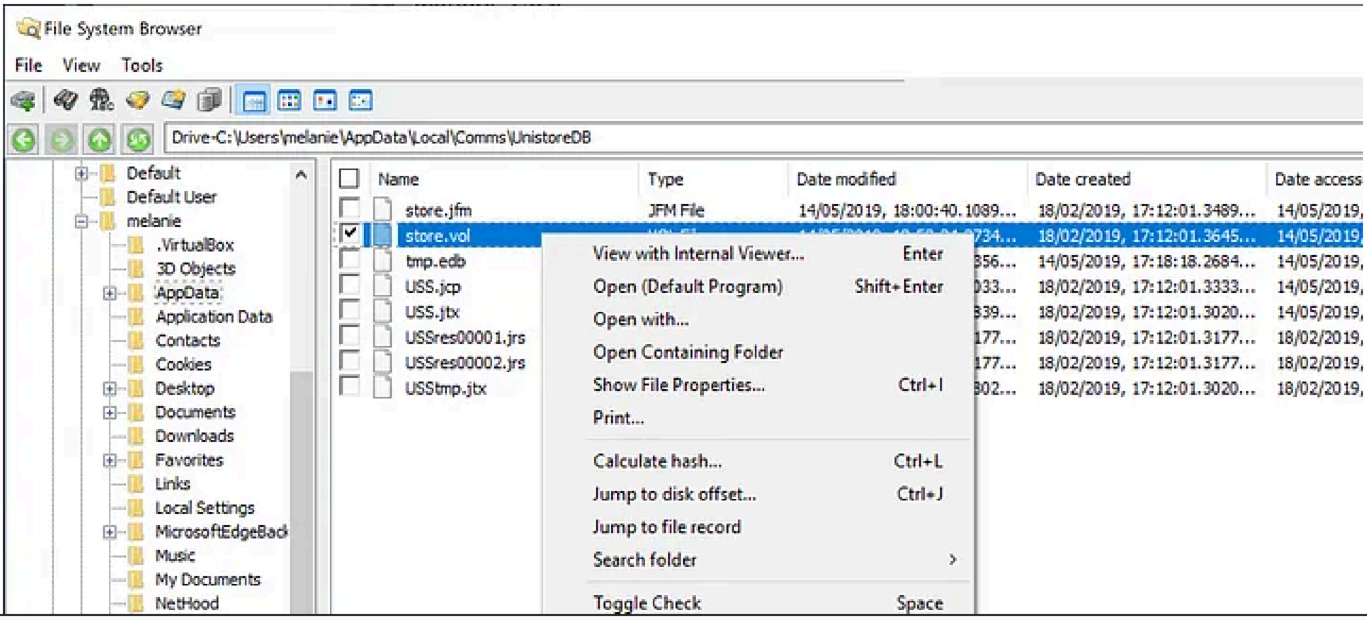
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Drive-C:\Users\melanie\AppData\Local\Comms\UnistoreDB

□	Name	Type	Date modified	Date created	Date access
□	store.jfm	JFM File	14/05/2019, 18:00:40.1089...	18/02/2019, 17:12:01.3489...	14/05/2019,
☑	store.vol		734...	18/02/2019, 17:12:01.3645...	14/05/2019,
□	tmp.edb		356...	14/05/2019, 17:18:18.2684...	14/05/2019,
□	USS.jcp		033...	18/02/2019, 17:12:01.3333...	14/05/2019,
□	USS.jtx		339...	18/02/2019, 17:12:01.3020...	14/05/2019,
□	USSres00001.jrs		177...	18/02/2019, 17:12:01.3177...	18/02/2019,
□	USSres00002.jrs		177...	18/02/2019, 17:12:01.3177...	18/02/2019,
□	USStmp.jtx		302...	18/02/2019, 17:12:01.3020...	18/02/2019,

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

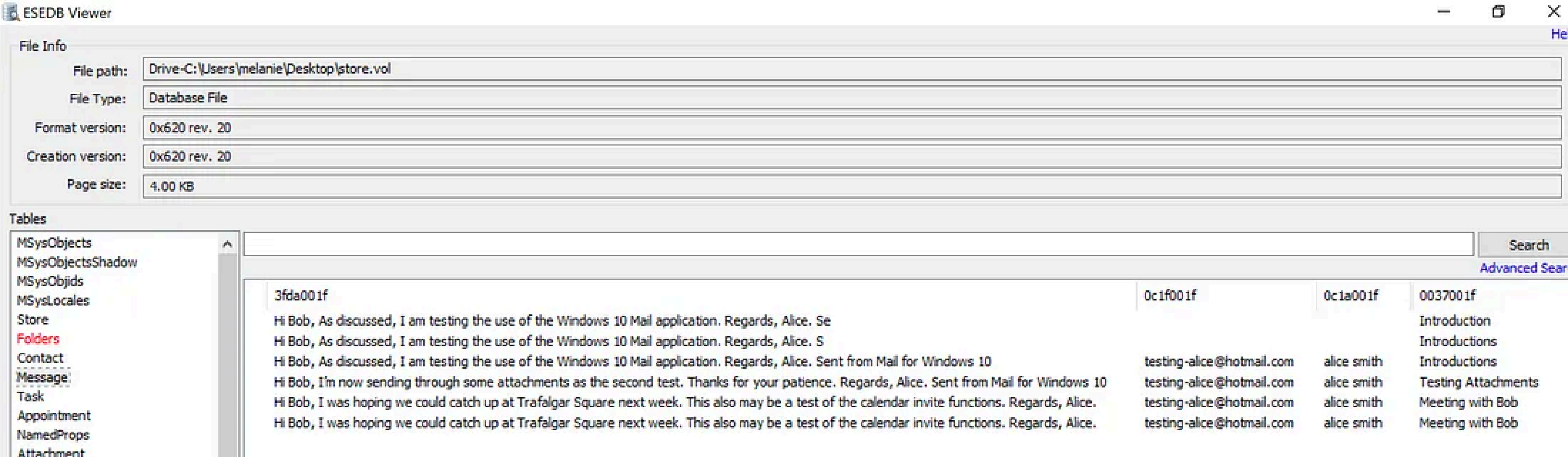
✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app



File Info

File path: Drive-C:\Users\melanie\Desktop\store.vol

File Type: Database File

Format version: 0x620 rev. 20

Creation version: 0x620 rev. 20

Page size: 4.00 KB

Tables

- MSysObjects
- MSysObjectsShadow
- MSysObjids
- MSysLocales
- Store
- Folders
- Contact
- Message
- Task
- Appointment
- NamedProps
- Attachment

3fda001f	0c1f001f	0c1a001f	0037001f
Hi Bob, As discussed, I am testing the use of the Windows 10 Mail application. Regards, Alice. Se			Introduction
Hi Bob, As discussed, I am testing the use of the Windows 10 Mail application. Regards, Alice. S			Introductions
Hi Bob, As discussed, I am testing the use of the Windows 10 Mail application. Regards, Alice. Sent from Mail for Windows 10	testing-alice@hotmail.com	alice smith	Introductions
Hi Bob, I'm now sending through some attachments as the second test. Thanks for your patience. Regards, Alice. Sent from Mail for Windows 10	testing-alice@hotmail.com	alice smith	Testing Attachments
Hi Bob, I was hoping we could catch up at Trafalgar Square next week. This also may be a test of the calendar invite functions. Regards, Alice.	testing-alice@hotmail.com	alice smith	Meeting with Bob
Hi Bob, I was hoping we could catch up at Trafalgar Square next week. This also may be a test of the calendar invite functions. Regards, Alice.	testing-alice@hotmail.com	alice smith	Meeting with Bob

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Appendix?

Now that the easy part is over, I wanted to share the internal struggle I faced trying to find software that would correctly parse 'store.vol'. I attempted to use NirSoft's ESEDatabaseView, which was able to extract some metadata, but not the contents of the email. You'll see similarities below between ESEDatabaseView and OSForensics in terms of the column naming, or lack thereof.

Medium

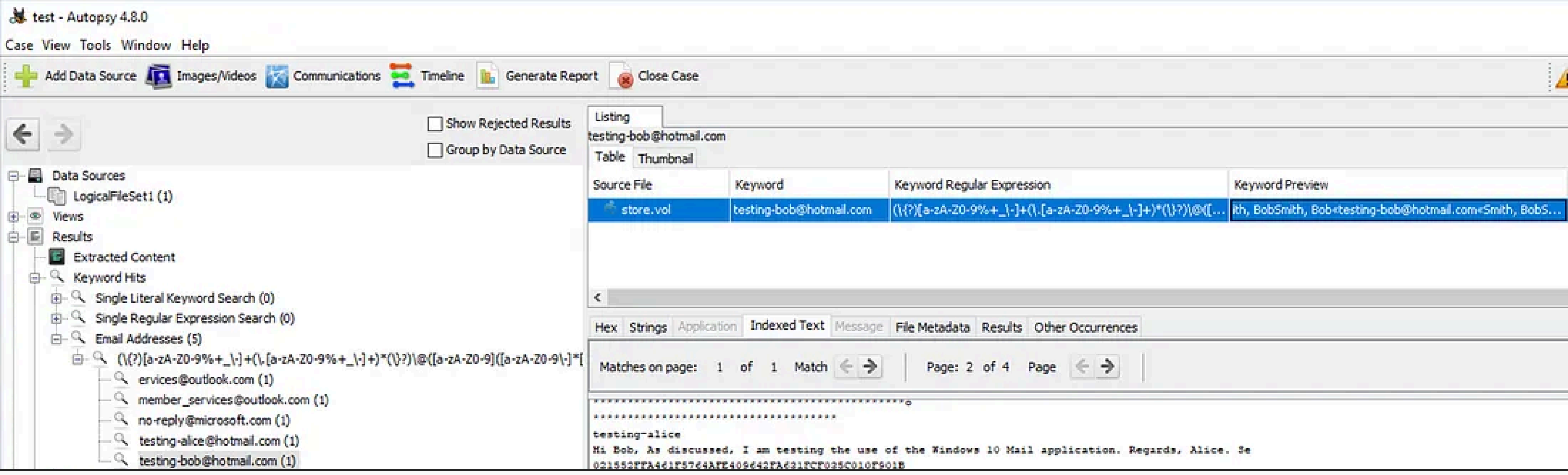
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Source File	Keyword	Keyword Regular Expression	Keyword Preview
store.vol	testing-bob@hotmail.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...	ith, BobSmith, Bob<testing-bob@hotmail.com<Smith, BobS...

```
**************************************************g
*************************************
testing-alice
Hi Bob, As discussed, I am testing the use of the Windows 10 Mail application. Regards, Alice. Se
021552FFA461F5764AFE409642FA631FCF025C010F901B
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

-- 2

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app