Windows 10 Mail App Forensics

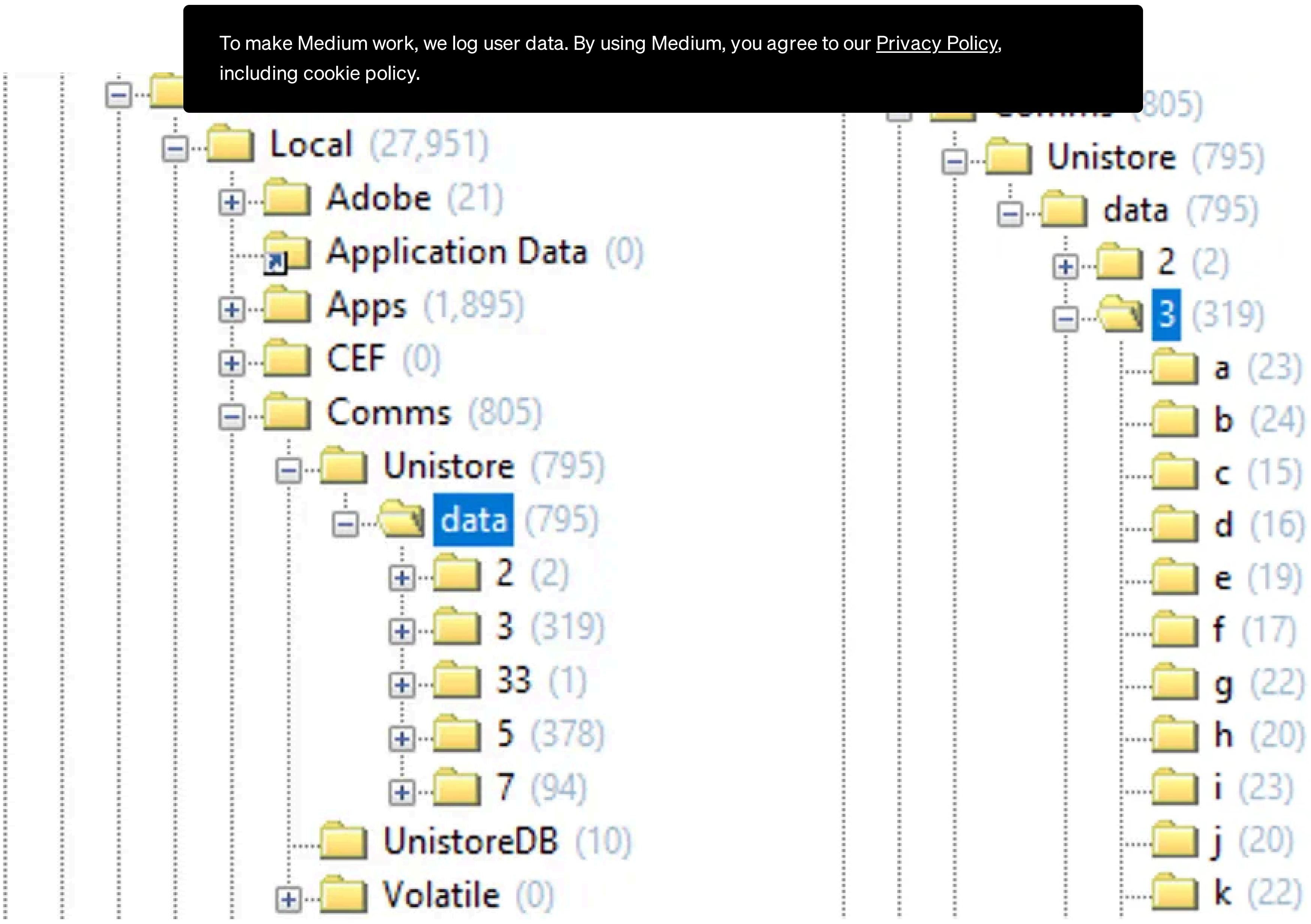
darkdefender · Follow
6 min read · May 27, 2019

While working on a forensics case, I stumbled across a folder in AppData\Local called “Comms”. Not knowing what this was at the time, I glanced through and realised that these are logs and artefacts of the Windows 10 Mail application.

For this blog post, I was able to replicate the findings in a Windows 10 virtual machine by creating some test email accounts. Fun fact! You know how there are services for temporary email addresses like Guerrilla Mail? There are also temporary phone numbers you can use incase you need a 2FA code for email account verification (such as receivesms.org, or this non-dodgy site). Pretty cool stuff.

Anyways, once you load up the mail app and start firing away some emails, the logs are written almost instantaneously. The directory in question is:

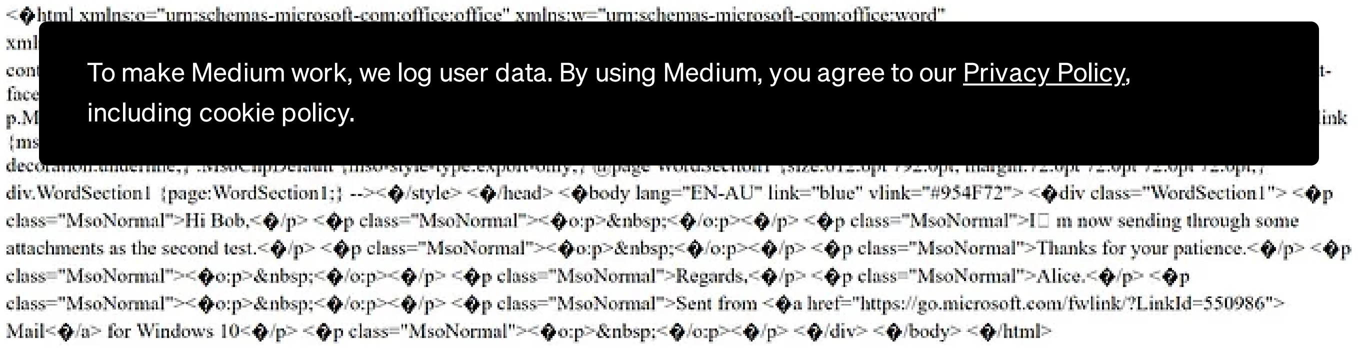
- **\Users\<username>\AppData\Local\Comms\Unistore\data**



Directory Listings for the Windows 10 Mail App Artefacts

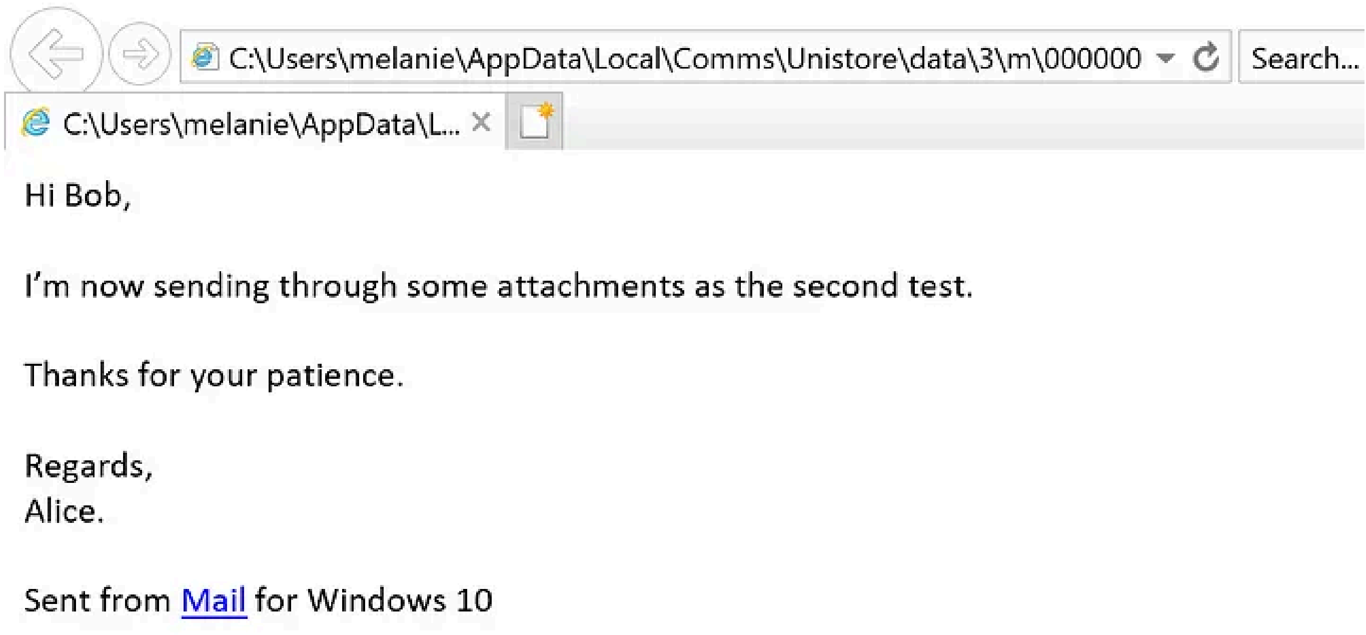
Let’s go through each of them:

- 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



```
<�html xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:w="urn:schemas-microsoft-com:office:word"
xml
cont                                                                                                      t-
face
p.M                                                                                                       ink
{ms
decoration:underline;} .MsoChpDefault {mso-style-type:export-only;} @page WordSection1 {size:612.0pt 792.0pt; margin:72.0pt 72.0pt 72.0pt 72.0pt;}
div.WordSection1 {page:WordSection1;} --><�/style> <�/head> <�body lang="EN-AU" link="blue" vlink="#954F72"> <�div class="WordSection1"> <�p
class="MsoNormal">Hi Bob,<�/p> <�p class="MsoNormal"><�o:p>&nbsp;<�/o:p><�/p> <�p class="MsoNormal">I□ m now sending through some
attachments as the second test.<�/p> <�p class="MsoNormal"><�o:p>&nbsp;<�/o:p><�/p> <�p class="MsoNormal">Thanks for your patience.<�/p> <�p
class="MsoNormal"><�o:p>&nbsp;<�/o:p><�/p> <�p class="MsoNormal">Regards,<�/p> <�p class="MsoNormal">Alice.<�/p> <�p
class="MsoNormal"><�o:p>&nbsp;<�/o:p><�/p> <�p class="MsoNormal">Sent from <�a href="https://go.microsoft.com/fwlink/?LinkId=550986">
Mail<�/a> for Windows 10<�/p> <�p class="MsoNormal"><�o:p>&nbsp;<�/o:p><�/p> <�/div> <�/body> <�/html>
```

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.

Regards,
Alice.

Sent from Mail for Windows 10

\data\5

The .dat files in this directory represent calendar invitations, however from what I've found during this investigation, it unfortunately doesn't save many juicy details… see for yourself in the example below. OSForensics was able to show more metadata by reading it in the Hex/Strings view, which had the name of the appointment, and who scheduled it in.

of the attachment as found in the email, which is displayed in the Type
co

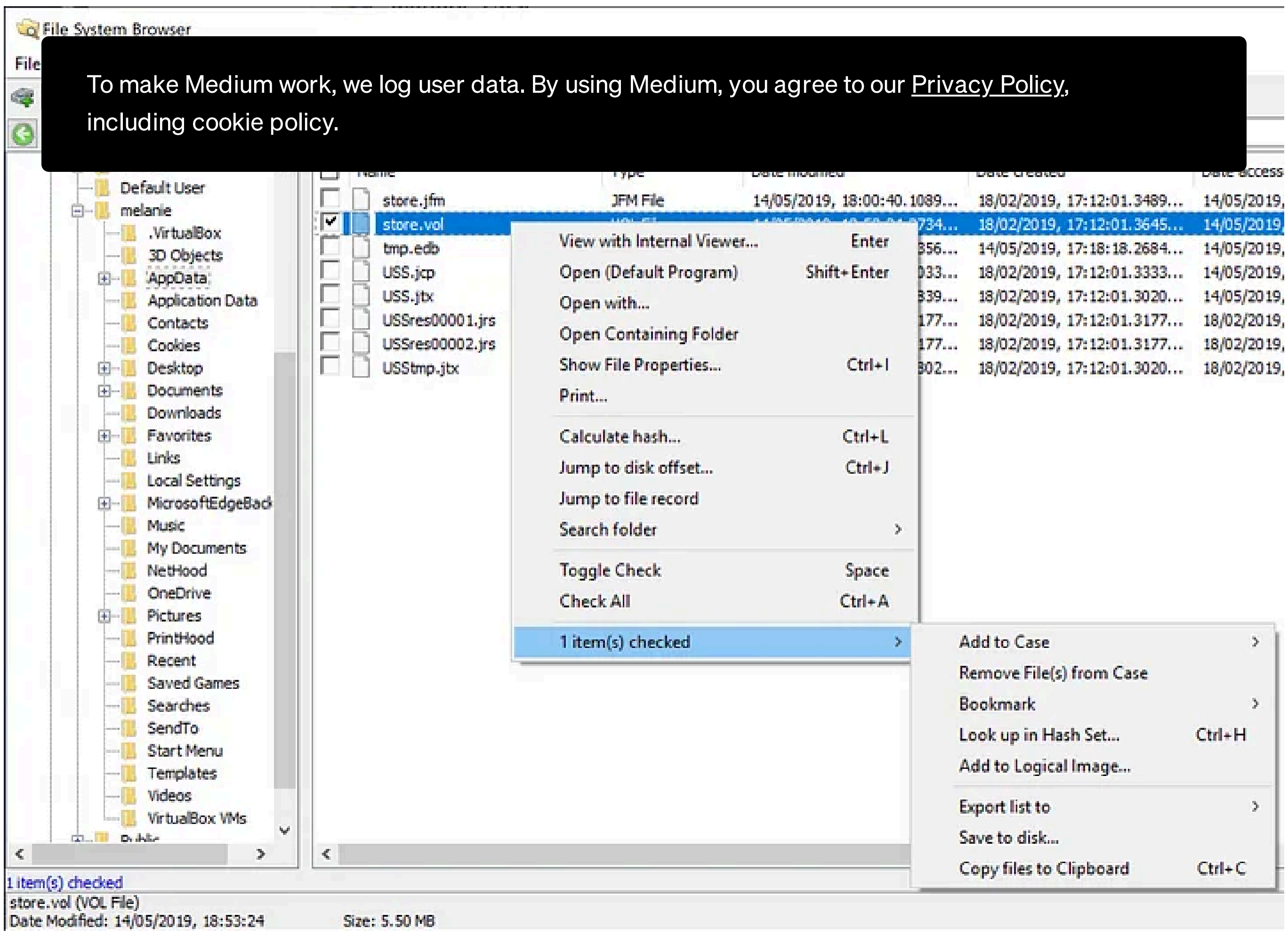
\data\33
Now this is purely speculation on my part. I haven't been able to find any research about this sub-directory, and my sample size is small, BUT, I was pleasantly surprised when OSForensics was able to give me something of value. Unfortunately, this was linked to my work email account, so I'm 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:

OSForensics however, can extract strings and display the hex/ascii content of the appointment. I thought this was neat.

OSForensics parsing .dat files in \data\33

You can see references to “Updated Webex Details Jan-2019”, and “ARCHIVED PRESENTATIONS”. I checked my inbox for these strings, and certainly enough, it displayed this text as the body of a webex meeting that I had been invited to attend earlier in the year.

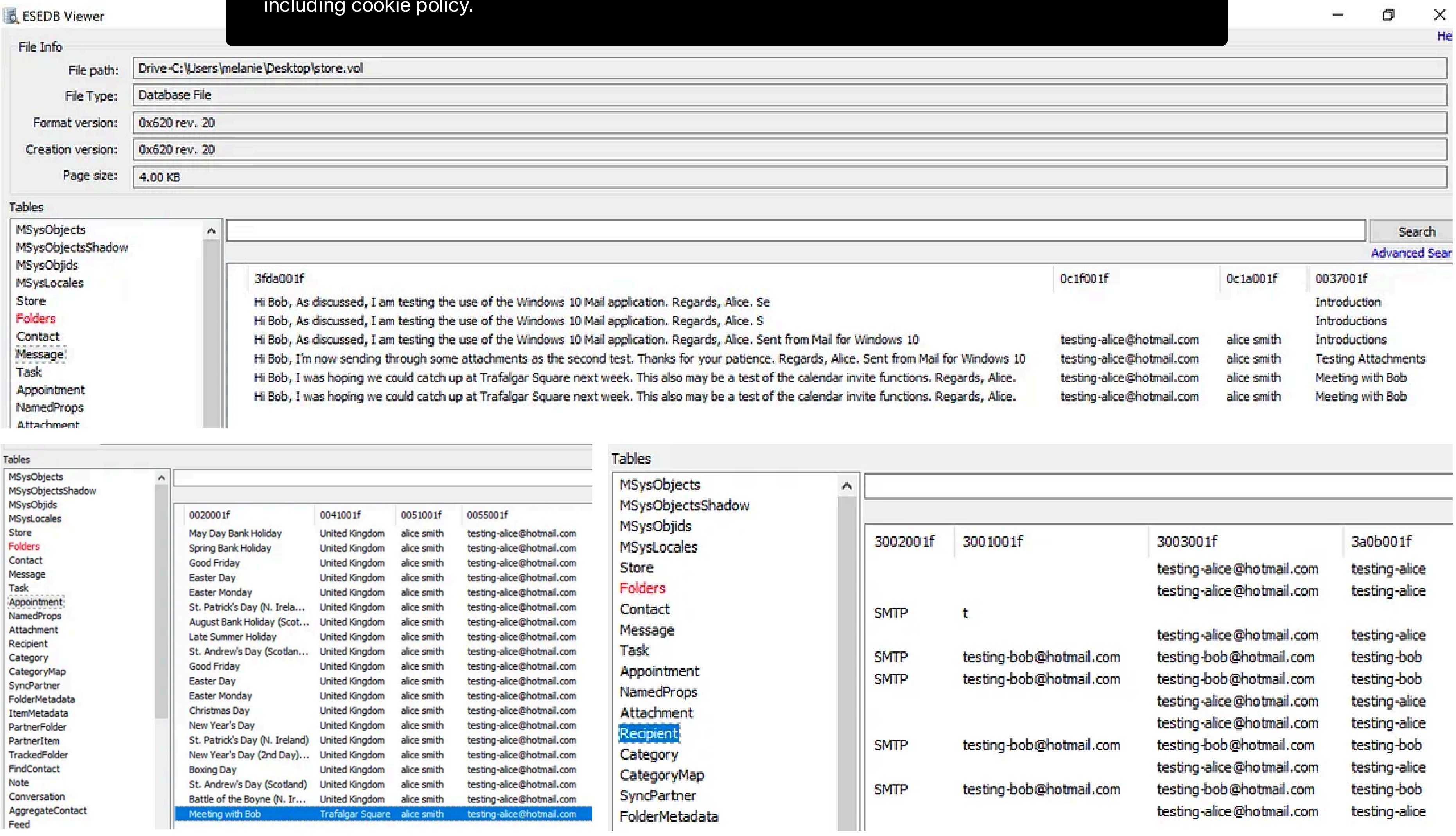


	Name	Type	Date modified	Date created	Date access
☐	store.jfm	JFM File	14/05/2019, 18:00:40.1089...	18/02/2019, 17:12:01.3489...	14/05/2019,
☑	store.vol		734...	18/02/2019, 17:12:01.3645...	14/05/2019,
☐	tmp.edb		356...	14/05/2019, 17:18:18.2684...	14/05/2019,
☐	USS.jcp		033...	18/02/2019, 17:12:01.3333...	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,

1 item(s) checked
store.vol (VOL File)
Date Modified: 14/05/2019, 18:53:24 Size: 5.50 MB

Using OS Forensics to Extract store.vol

Double-clicking store.vol here only gets you so far. You can see below that the String Viewer offered some email metadata and contents, but it wasn't being presented in the way that I hoped.



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

Tables

- MSysObjects
- MSysObjectsShadow
- MSysObjids
- MSysLocales
- Store
- Folders
- Contact
- Message
- Task
- Appointment
- NamedProps
- Attachment
- Recipient
- Category
- CategoryMap
- SyncPartner
- FolderMetadata
- ItemMetadata
- PartnerFolder
- PartnerItem
- TrackedFolder
- FindContact
- Note
- Conversation
- AggregateContact
- Feed

0020001f	0041001f	0051001f	0055001f
May Day Bank Holiday	United Kingdom	alice smith	testing-alice@hotmail.com
Spring Bank Holiday	United Kingdom	alice smith	testing-alice@hotmail.com
Good Friday	United Kingdom	alice smith	testing-alice@hotmail.com
Easter Day	United Kingdom	alice smith	testing-alice@hotmail.com
Easter Monday	United Kingdom	alice smith	testing-alice@hotmail.com
St. Patrick's Day (N. Irela...	United Kingdom	alice smith	testing-alice@hotmail.com
August Bank Holiday (Scot...	United Kingdom	alice smith	testing-alice@hotmail.com
Late Summer Holiday	United Kingdom	alice smith	testing-alice@hotmail.com
St. Andrew's Day (Scotlan...	United Kingdom	alice smith	testing-alice@hotmail.com
Good Friday	United Kingdom	alice smith	testing-alice@hotmail.com
Easter Day	United Kingdom	alice smith	testing-alice@hotmail.com
Easter Monday	United Kingdom	alice smith	testing-alice@hotmail.com
Christmas Day	United Kingdom	alice smith	testing-alice@hotmail.com
New Year's Day	United Kingdom	alice smith	testing-alice@hotmail.com
St. Patrick's Day (N. Ireland)	United Kingdom	alice smith	testing-alice@hotmail.com
New Year's Day (2nd Day)...	United Kingdom	alice smith	testing-alice@hotmail.com
Boxing Day	United Kingdom	alice smith	testing-alice@hotmail.com
St. Andrew's Day (Scotland)	United Kingdom	alice smith	testing-alice@hotmail.com
Battle of the Boyne (N. Ir...	United Kingdom	alice smith	testing-alice@hotmail.com
Meeting with Bob	Trafalgar Square	alice smith	testing-alice@hotmail.com

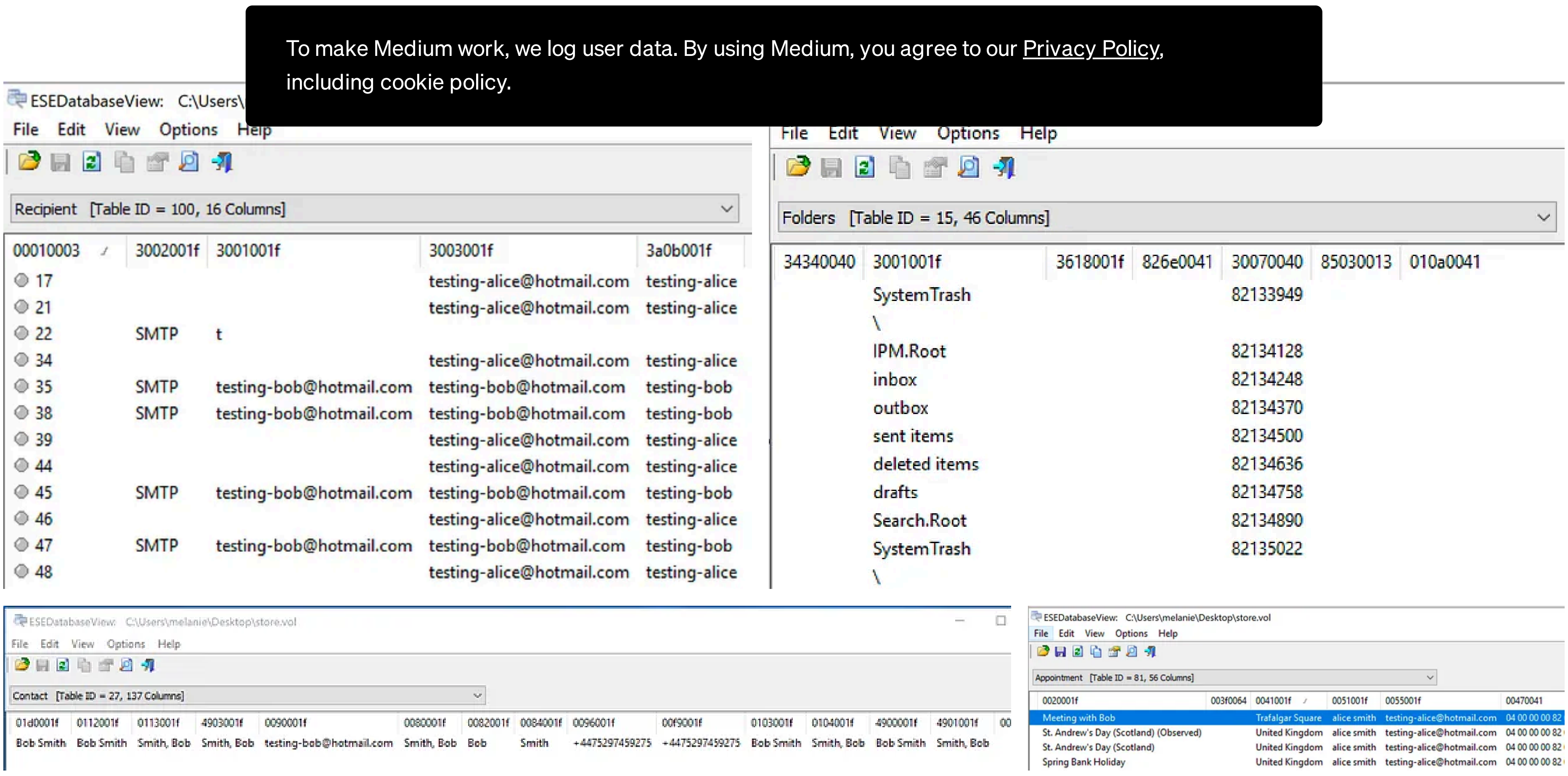
Tables

- MSysObjects
- MSysObjectsShadow
- MSysObjids
- MSysLocales
- Store
- Folders
- Contact
- Message
- Task
- Appointment
- NamedProps
- Attachment
- Recipient
- Category
- CategoryMap
- SyncPartner
- FolderMetadata

3002001f	3001001f	3003001f	3a0b001f
		testing-alice@hotmail.com	testing-alice
		testing-alice@hotmail.com	testing-alice
SMTP	t		
		testing-alice@hotmail.com	testing-alice
SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
		testing-alice@hotmail.com	testing-alice
		testing-alice@hotmail.com	testing-alice
SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
		testing-alice@hotmail.com	testing-alice
SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
		testing-alice@hotmail.com	testing-alice

Using OSForensic's ESEDB Viewer to parse store.vol

The **Message** table shows you what you'd expect, the body of the email (what was displayed in Unistore\data\3). However to find the person it was sent to, there is a separate table called **Recipient**, which is displayed in the bottom right. Towards the left, you'll see the **Appointment** table, which, amongst all the default holiday entries, you'll find 'Meeting with Bob', where Alice wanted to meet Bob in Trafalgar Square.


ESEDatabaseView: C:\Users\
File Edit View Options Help
Recipient [Table ID = 100, 16 Columns]
File Edit View Options Help
Folders [Table ID = 15, 46 Columns]

00010003	3002001f	3001001f	3003001f	3a0b001f
17			testing-alice@hotmail.com	testing-alice
21			testing-alice@hotmail.com	testing-alice
22	SMTP	t		
34			testing-alice@hotmail.com	testing-alice
35	SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
38	SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
39			testing-alice@hotmail.com	testing-alice
44			testing-alice@hotmail.com	testing-alice
45	SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
46			testing-alice@hotmail.com	testing-alice
47	SMTP	testing-bob@hotmail.com	testing-bob@hotmail.com	testing-bob
48			testing-alice@hotmail.com	testing-alice

34340040	3001001f	3618001f	826e0041	30070040	85030013	010a0041
	SystemTrash			82133949		
	\					
	IPM.Root			82134128		
	inbox			82134248		
	outbox			82134370		
	sent items			82134500		
	deleted items			82134636		
	drafts			82134758		
	Search.Root			82134890		
	SystemTrash			82135022		
	\					

ESEDatabaseView: C:\Users\melanie\Desktop\store.vol
File Edit View Options Help
Contact [Table ID = 27, 137 Columns]

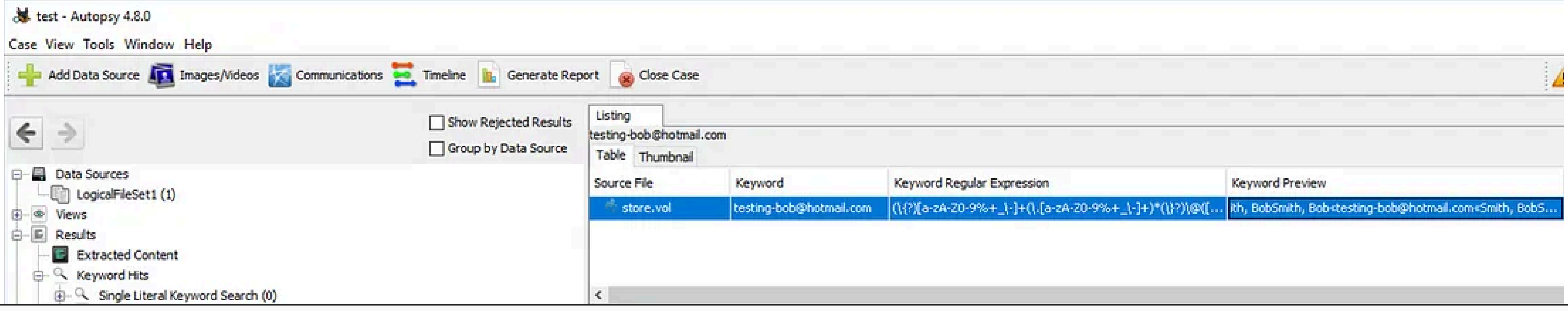
01d0001f	0112001f	0113001f	4903001f	0090001f	0080001f	0082001f	0084001f	0096001f	00f9001f	0103001f	0104001f	4900001f	4901001f	00
Bob Smith	Bob Smith	Smith, Bob	Smith, Bob	testing-bob@hotmail.com	Smith, Bob	Bob	Smith	+4475297459275	+4475297459275	Bob Smith	Smith, Bob	Bob Smith	Smith, Bob	

ESEDatabaseView: C:\Users\melanie\Desktop\store.vol
File Edit View Options Help
Appointment [Table ID = 81, 56 Columns]

0020001f	003f0064	0041001f	0051001f	0055001f	00470041
Meeting with Bob		Trafalgar Square	alice smith	testing-alice@hotmail.com	04 00 00 00 82
St. Andrew's Day (Scotland) (Observed)		United Kingdom	alice smith	testing-alice@hotmail.com	04 00 00 00 82
St. Andrew's Day (Scotland)		United Kingdom	alice smith	testing-alice@hotmail.com	04 00 00 00 82
Spring Bank Holiday		United Kingdom	alice smith	testing-alice@hotmail.com	04 00 00 00 82

Attempting to use NirSoft's ESEDatabaseView to parse store.vol

I even tried Autopsy (this is what desperation looks like). It parsed some email content, sure, but where are the tables? This was essentially a glorified version of OSForensics' String Viewer; notice 'Extracted Content' and 'Indexed Data'.



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…

This was fun! Over and out.

Dfir Forensics Windows1 Microsoft Investigation

12 2

Written by darkdefender

269 Followers

Your one and only source into the scandalous life of a DFIR consultant.

Follow

More from darkdefender

darkdefender

darkdefender

Nov

See all from darkdefender

Recommended from Medium

Practical OSINT

OSINT In War Zone: A Practical Guide to Use X (Twitter) Advance…

This article will guide you through using X (formerly Twitter)'s advanced search…

Sep 6 40

Sanskar Kalra

Unleashing BloodHound: A Guide to Dominating Active Directory…

BloodHound for Active Directory Enumeration: Installation, Usage, and…

Aug 26 2 2

Lists

Security Guy

Free Beginner’s Course in Hacking

Start Your Hacking Journey Here! All you need is an internet connection

✦ Oct 17 183

Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

✦ Jun 18 1.6K 53

See more recommendations

Help Status About Careers Press Blog Privacy Terms Text to speech Teams