Oxygen で抽出したメールを EML 形式で出力する方法

Ver. 1.0



Copyright © 2023 Cyber Defense Institute, Inc. All Rights Reserved

目次

1	イントロダクション	2
2	EML 形式でのデータ出力方法	2

1 イントロダクション

本ガイドでは、Oxygen Forensic Extractor で抽出済みのデータ内のメールを EML 形式で出力する方法を紹介します。出力した EML 形式ファイルは、お手持ちのメールソフトやエディタ等でご確認いただけます。

2 EML 形式でのデータ出力方法

 Oxygen Forensic Detective の Applications の一覧から対象アプリケーションの解析画面に遷移します (ここでは例として Gmail の解析画面に遷移します)。

Inciden	ime zone (UTC+09:00) Tokyo (Asia) OS Android OS t number Add incident number Add evidence number		
> Statistics Extraction in	nfo Owner General info	Device Photos Note	٥
> General sections 11			
> Analytics 7			
 Applications 33 			
Airbnb 422	Digital Wellbeing 2,684	Downloads 3	DuckDuckGo Privacy Br 86
Event Log 5	Facebook 355	Facebook Messenger 146	Foursquare
Google 1,559	Google Chrome	Google Docs	Google Drive
Google Duo	Google Home	Google Keep	Google Mail 371
Google Maps 62	Google photos 749/4	HouseParty 32	Kakao Talk 41/5

2. 出力したいデータにチェックを入れます(デフォルトでは全てのデータがチェックされています)。

👽 Oxygen Forensic® Detective									
📃 🎧 M Google Mail - Go	😑 🎧 🔭 Google Mail - Google Pixel 3 ×								
i Extraction info 🚹 Exp	i_ Extraction info 🝙 Export → 🙀 Reset filters 📋 View → 🖓 Maps 👷 Geo data →								
M Google Mail	≪ ‡	All data	Files Contacts Chats	Timeline Social Graph		Tind text	^	~	>> Details
✓ Categories	371	☑ ☆	🧷 🗸 💫 🗸 Time	stamp (Tokyo)	Subject		From	^	
✓ ▲ Accounts	8		2022,	/02/14 13:13:41 (UTC+9)	dアカウントを不正アクセスから守行	ろう!(パスワードレス認証	daccount@		XX Key Evide
(i) General	1	☆							So
Cached info	7		<div bacolor="white"></div>						Source
✓ 佐井場攻太 (saiba.seme.	. 225	<pre><div <="" marginwidth="0" pre=""></div></pre>							Sour
Polders	15		marginheight="0" style="width:100%:fon	n					
🗸 💬 Mails	210		t-size:16px;font-						D
Unsorted	210		Sans,Hiragino Kaku Go						Time stamp
🗸 🔄 Cache	138			(02/14/12:0E-E0/0/EC-10)	@CatheComptet*(instrain al .a			
Files	138	202.		/02/14 15:05:56 (01C+9)	@SaibaSemetaさん、Twitter (")思	画大Uを確認しましょう notify	noury@twit	ptwit	
		¥							From



3. 解析画面上部にある[Export]ボタンの横にある[▼]をクリックしてください。

👽 Oxygen Forensic® Detective							
😑 🎧 🎦 Google Mail - Google Pixel 3 ×							
i Extraction info	Export 🗸	$\bigvee_{\times} Re$	set filter	rs 📒	View	- 🖓	Ma
M Google Mail	: >>	All data	Files (Contacts	Chats	Timeline	S
✓ Categories	371	☑ ☆	0	~ 💊	~ Time	stamp (To	okyo
✓ Accounts	8			Ø	2022	/02/14 13	:13:
i General	1	☆					
Cached info	7		< div b	acolor-'	white's		
	005		NULL N	gcolor=	white >		

4. [Export to separate files…]をクリックしてください。

🔊 Oxygen Forensic® Detective							
📃 🏠 🎦 Google Mail - Google Pixel 3 ×							
i] Extraction info	Export 🗸	٦	View	- 0			
M Google Mail	Export to file	acts	Chats	Timeline			
✓ Categories	Export to sep	₽.	~ Time	stamp (T			
✓ ↓ Accounts	Export geolocations				2022	/02/14 1	
i General	1	☆					
Cached info	7		<div bgc<="" th=""><th>olor='</th><th>white"></th><th></th></div>	olor='	white">		

- 5. Export wizard が開きますので、General report settings > Export format から[EML]を選択します。
- 6. [Export]をクリックして、出力を開始してください。

👽 Export wizard - Template: User template (26) X							
🔅 General	General report settings						
🐻 Files	Select the data to export, specify the path and format of the report.						
Export folder D:¥ File name (+++++=							
	Export format EML Construction Group by remote party						
	Export Can	cel					

7. 出力が完了すると、Oxygen Forensic Detective 画面右下の Notifications center に[Open folder]ボタン が表示されますので、クリックしてください。



8. 下図のように EML 形式のファイルがローカルに出力されているのが確認できます。



※ 本ガイドの検証環境では Thunderbird (メールソフト)を使用しているため、

上図ではアイコンや種類が Thunderbird のものになっています。

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0 2023年03月07日		初版発行