



ZENTEK
Forensics Limited

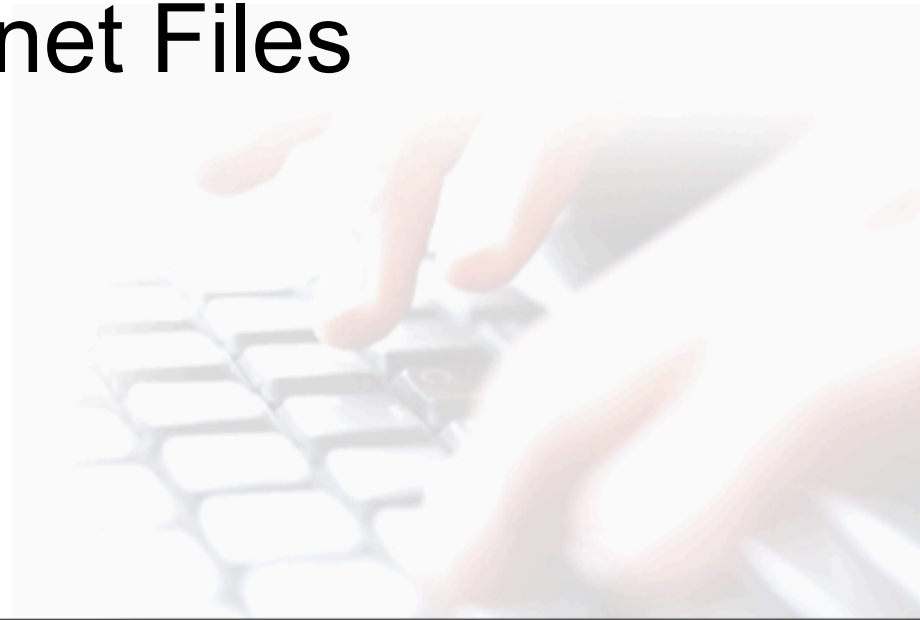
Gmail Artefacts





Old methods

- Cached HTML
- No encryption
- Simple recovery
- Extract Temporary Internet Files
- Carve for HTML





ZENTEK

Forensics Limited

EnCase Forensic

File Edit View Tools Help

New Open Save Print Add Device Search Refresh

Table Report Gallery Disk Code

	Name	Filter	In Report	Search Hits	Additional Fields	Message Size
<input type="checkbox"/>	10 index.dat		No	No	Yes	512
<input type="checkbox"/>	11 MailReg[1].v=8		No	No	Yes	9857
<input type="checkbox"/>	12 eval_register[1].last=		No	No	Yes	11868
<input type="checkbox"/>	13 eval_register[1].htm		No	No	Yes	40937
<input type="checkbox"/>	14 id_check[1]		No	No	Yes	2558
<input type="checkbox"/>	15 id_check[1].htm		No	No	Yes	7507
<input type="checkbox"/>	16 id_check62f59919[1]		No	No	Yes	2557
<input type="checkbox"/>	17 id_check[1]		No	No	Yes	2646
<input type="checkbox"/>	18 id_check63759919[1]		No	No	Yes	2559
<input type="checkbox"/>	19 last[1]		No	No	Yes	3208
<input type="checkbox"/>	20 last[1].htm		No	No	Yes	10656
<input type="checkbox"/>	21 login[1].htm		No	No	Yes	25546
<input type="checkbox"/>	22 id_checkc48eca59[1]		No	No	Yes	1049

Home Additional Fields

Records

Dell Latitude CPl

C

Internet Explorer (Window)

History

Daily

Weekly

Visited Link

Cache

Code

Image

HTML

XML

Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 869/19799

Yahoo! My Yahoo! Mail

Welcome, **mrevilrulez**

[\[Sign Out, My Account\]](#)

[Mail Home](#) - [Help](#)

[Mail](#) | [Addresses](#) | [Calendar](#) | [Notepad](#) | [mrevilrulez@yahoo.com](#) [\[Sign Out\]](#)

Check Mail - Compose - Search Mail | [Mail Upgrades](#) - [Mail Options](#)

[Choose from 10](#)

[Free Cell Phones](#)

Folders[[Add](#) - [Edit](#)]

- [Inbox \(1\)](#)
- [Draft](#)
- [Sent](#)
- [Trash \[Empty\]](#)



[Check your Credit!](#)

Welcome, Greg!

0% of 100.0MB

You have **1 unread message**:

[Inbox\(1\)](#)

Today's tip: Stop spammers from knowing you opened an email. Turn on the [security preference](#) to "Block HTML graphics." [Learn More.](#)





Improvements

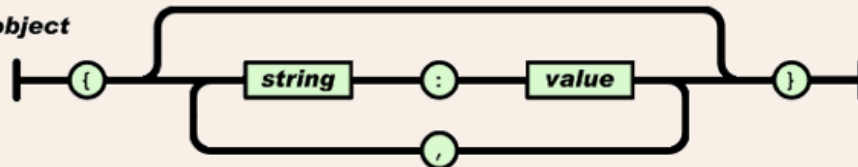
- Compression (GZIP to save on bandwidth)
- Cache Control
- Asynchronous Javascript And XML (AJAX)





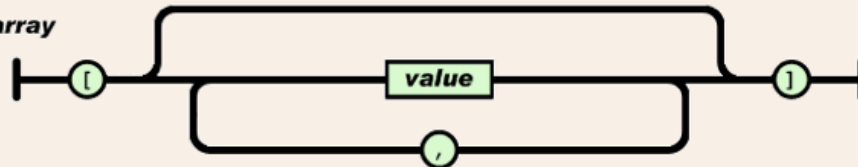
JSON

object



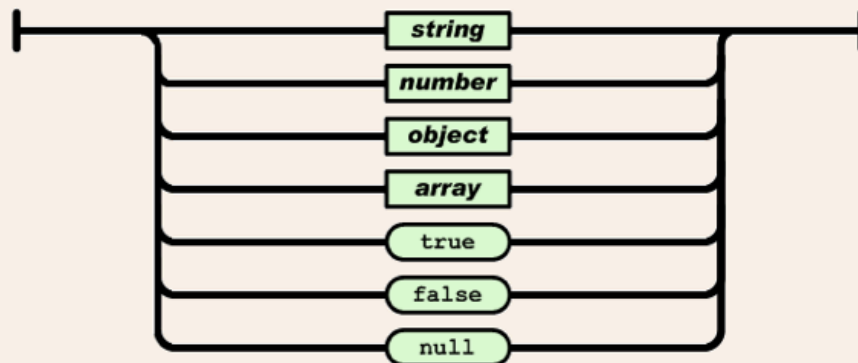
An *array* is an ordered collection of values. An array begins with [(left bracket) and ends with] (right bracket). Values are separated by , (comma).

array



A *value* can be a *string* in double quotes, or a *number*, or *true* or *false* or *null*, or an *object* or an *array*. These structures can be nested.

value



json.org



while(1);

JSON

```
[[["v","137s2mfg40boa","1c22e772e53ff3  
de","-902218240","1","vaknsvtjz8a"]  
,["gn","gsi test502"]  
,["cfs",[]  
,[]  
]  
,["i",50]  
,["st",1208038540]  
,["qu","0","6616","0","#006633",  
0,0,0,"0","6.5"]  
,["ft","Send photos easily from Gmail with  
Google's \u003ca href\u003d\"http://  
picasa.google.com\"
```





ZENTEK
Forensics Limited

Demo

- Firefox
- HTTPFox





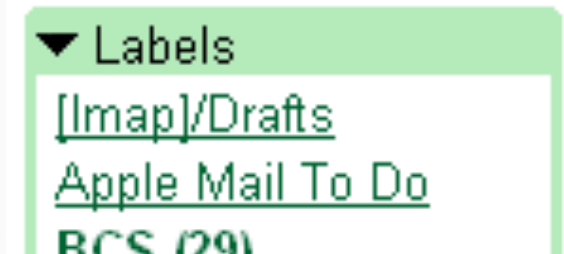
Tags -ct

Contacts

["ct", "Joe Bloggs", "joe@bloggs.co.uk"]

Labels

["ct", [{"[Imap]/Drafts", 0}], [{"Apple Mail To Do", 0}], [{"BCS", 29}] ...etc.





Tags -ds

Default Labels

```
["ds", [{"inbox", 11}, {"drafts", 0}, {"spam", 13}]]
```



[Compose Mail](#)

[Inbox \(11\)](#)

[Starred](#) ★

[Chats](#) ☰

[Sent Mail](#)

[Drafts](#)

[All Mail](#)

[Spam \(13\)](#)

[Bin](#)





ZENTEK
Forensics Limited

Tags -gn

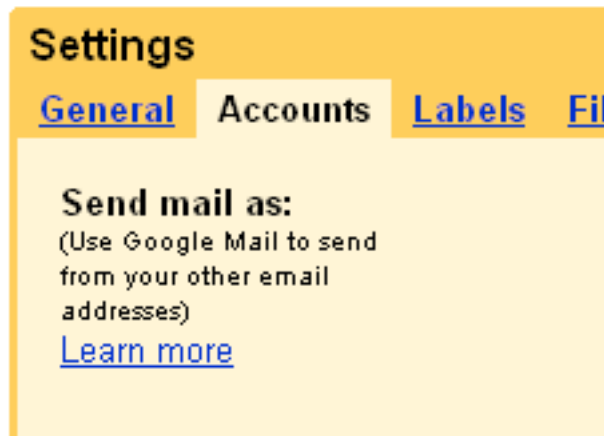
Google Name
Joe Bloggs





Tags -cfs

Alternate Account (POP3)





ZENTEK
Forensics Limited

Tags -cl

Contact List

```
["cl", "group", "\"Jane Doe\"  
\u003cjane@doe
```





ZENTEK
Forensics Limited

Tags

cs- Conversation Start

ms- Message Start

mb- Message Body

st- Login time(?)

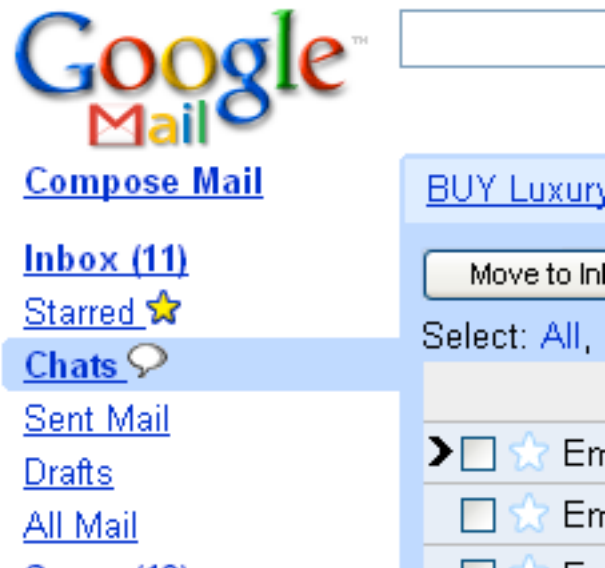
["st",1267051871]





Tags -t

Google Talk



```
[0]: "t"  
[1]  
[0]: "126cd09fc11d57da"  
[1]: 0  
[2]: 0  
[3]: "14 Feb"  
[4]: "003cspan id003d" _upro_emmajf  
[5]: "0026raquo;0026nbsp;"  
[6]: "Chat with Emma      "  
[7]: "me: l0026#39;m going for the kic  
[8]  
[9]: ""  
[10]: "126cd09fc11d57da"  
[11]: 0  
[12]: "14 February 2010 15:11"  
[13]: 1  
[14]: "[2 lines]"  
[15]: 0  
[16]: 0  
[17]: 1  
[2]  
[0]: "126cccf43c3df0ec"
```



ZENTEK
Forensics Limited

Tags -qu

Quota

```
["qu", "321", "7427", "4", "#006633",  
0,0,0, "0.3", "7.3"]
```

Get **Google Mail on your phone**. It's super fast. Visit <http://mobile.google.com/> on your phone's web browser. [Learn more](#)

You are currently using 321 MB (4%) of your 7427 MB.

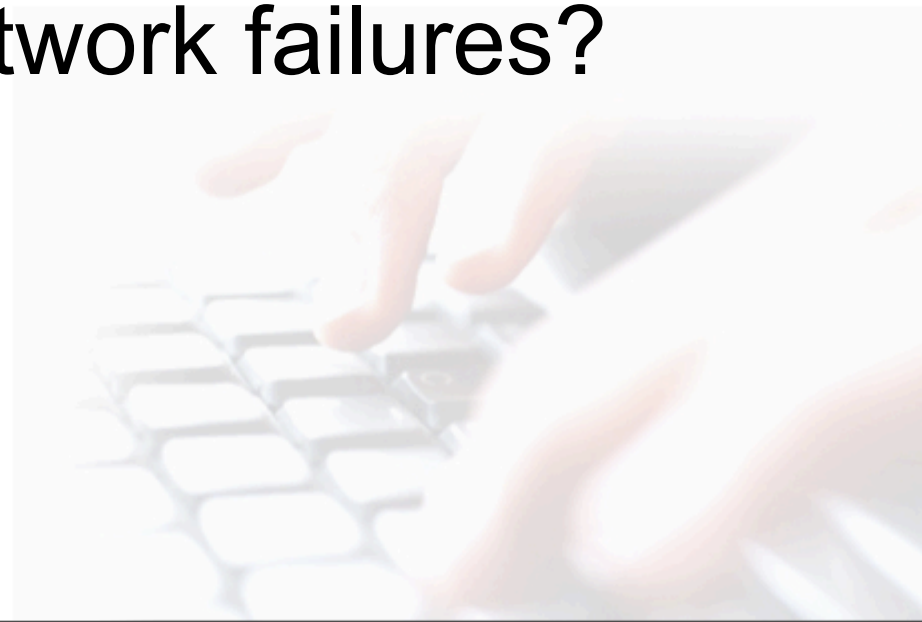
Google Mail view: **standard with chat** | [standard without chat](#) | [basic HTML](#) [Learn more](#)

©2010 Google - [Terms](#) - [Google Home](#)



Potential Locations

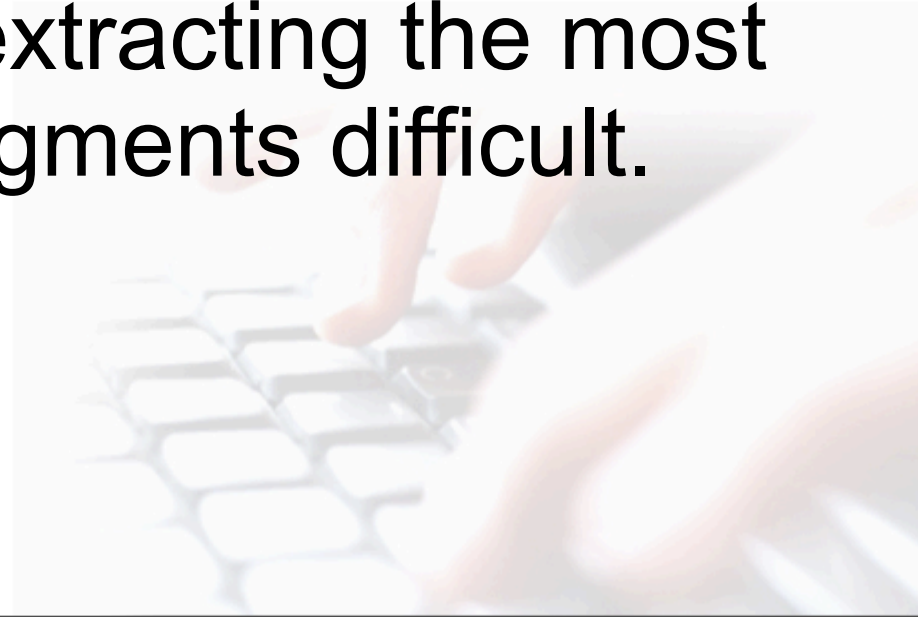
- Memory dumps
- Pagefile
- Hiberfil.sys (remember to decompress)
- Could be cached on network failures?





Extracting Messages

- Difficulty because of lack of caching
- Source from RAM could mean it's likely to be fragmented (4096 Bytes)
- Fragmentation makes extracting the most value out of existing fragments difficult.





ZENTEK
Forensics Limited

Demo Tools

- EnCase Scripts
- Internet Evidence Finder

