New issue

Jump to bottom

HTML in String fields is not escaped if only preview is loaded #577

Closed **MartinEnders** opened this issue on May 30, 2020 · 1 comment

MartinEnders commented on May 30, 2020 • edited

Version: docker-image latest (as of 29.05.2020 - Docker Image mongo-express:latest@sha256:bae0a154c4d73f1e61a532148942c582fbfad22944638d4307a4710daa1398b6)

Problem

I use a MongoDB collection to save HTML-Dokuments in a string property of documents and use mongo-express to access the Mongo Database. Especially when the properties with the HTML content are not loaded directly because of their size and I click on
`*** LARGE PROPERTY ***~106 KBPreview:"Click to fetch this property` the HTML content is loaded and rendered by the browser.

If you need further information please feel free to ask - I'll try to answer as fast as possible.

Reconstruction

If you create a Collection e.g. with mongo-express and create a document like the following. Bigger than 100kB and starting with HTML tags. Save the document and when you look in the HTML sources of the collection-view page than you will find that the HTML tags are not escaped.

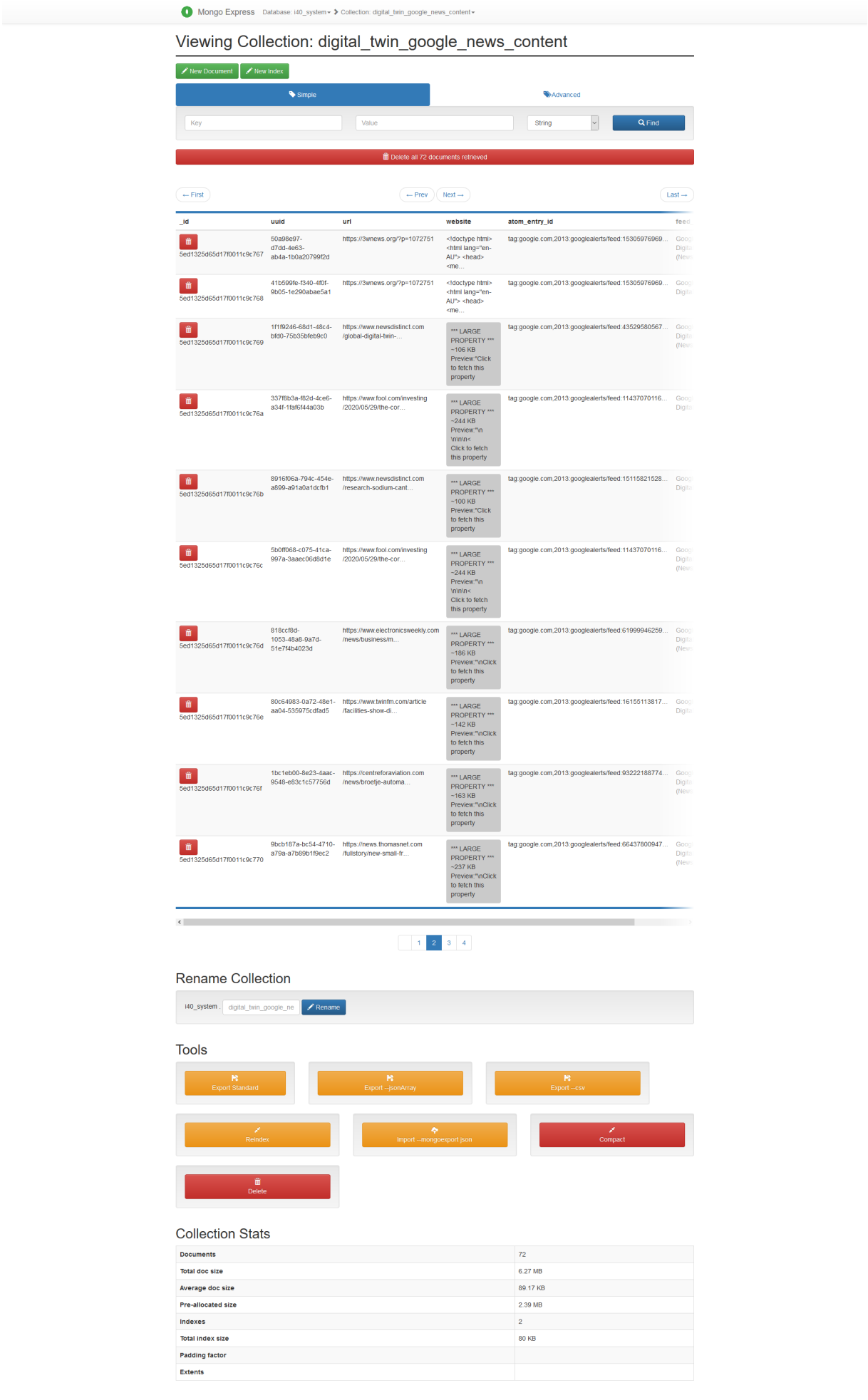
```
{
    _id: ObjectId('5ed226e15df10e00077733ba'),
    html: '<!DOCTYPE html> </table>hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world!
hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello
world! hello world! hello world!
```

world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world!
hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello

hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello
world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world!

```
world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world!
hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello world! hello
```

Normal View:


Mongo Express
Database: i40_system
Collection: digital_twin_google_news_content
Viewing Collection: digital_twin_google_news_content
New Document
New Index
Simple
Advanced
Key
Value
String
Find
Delete all 72 documents retrieved
← First
← Prev
Next →
Last →
_id
uuid
url
website
atom_entry_id
feed
5ed1325d65d17f0011c9c767
50a98e97-d7dd-4e63-ab4a-1b0a20799f2d
https://3wnews.org/?p=1072751
<!doctype html> <html lang="en-AU"> <head> <me...
tag:google.com,2013:googlealerts/feed:15305976969...
5ed1325d65d17f0011c9c768
41b599fe-f340-4f0f-9b05-1e290abae5a1
https://3wnews.org/?p=1072751
<!doctype html> <html lang="en-AU"> <head> <me...
tag:google.com,2013:googlealerts/feed:15305976969...
5ed1325d65d17f0011c9c769
1f1f9246-68d1-48c4-bfd0-75b35bfeb9c0
https://www.newsdistinct.com/global-digital-twin-...
*** LARGE PROPERTY *** ~106 KB Preview:"Click to fetch this property
tag:google.com,2013:googlealerts/feed:43529580567...
5ed1325d65d17f0011c9c76a
337f8b3a-f82d-4ce6-a34f-1faf6f44aa03b
https://www.fool.com/investing/2020/05/29/the-cor...
*** LARGE PROPERTY *** ~244 KB Preview:"\n \n\n\n< Click to fetch this property
tag:google.com,2013:googlealerts/feed:11437070116...
5ed1325d65d17f0011c9c76b
8916f06a-794c-454e-a899-a91a0a1dcfb1
https://www.newsdistinct.com/research-sodium-cant...
*** LARGE PROPERTY *** ~100 KB Preview:"Click to fetch this property
tag:google.com,2013:googlealerts/feed:15115821528...
5ed1325d65d17f0011c9c76c
5b0ff068-c075-41ca-997a-3aaec06d8d1e
https://www.fool.com/investing/2020/05/29/the-cor...
*** LARGE PROPERTY *** ~244 KB Preview:"\n \n\n\n< Click to fetch this property
tag:google.com,2013:googlealerts/feed:11437070116...
5ed1325d65d17f0011c9c76d
818ccf8d-1053-48a8-9a7d-51e7f4b4023d
https://www.electronicsweekly.com/news/business/m...
*** LARGE PROPERTY *** ~186 KB Preview:"\nClick to fetch this property
tag:google.com,2013:googlealerts/feed:61999946259...
5ed1325d65d17f0011c9c76e
80c64983-0a72-48e1-aa04-535975cdfad5
https://www.twinfm.com/article/facilities-show-di...
*** LARGE PROPERTY *** ~142 KB Preview:"\nClick to fetch this property
tag:google.com,2013:googlealerts/feed:16155113817...
5ed1325d65d17f0011c9c76f
1bc1eb00-8e23-4aac-9548-e83c1c57756d
https://centreforaviation.com/news/broetje-automa...
*** LARGE PROPERTY *** ~163 KB Preview:"\nClick to fetch this property
tag:google.com,2013:googlealerts/feed:9322188774...
5ed1325d65d17f0011c9c770
9bcb187a-bc54-4710-a79a-a7b89b1f9ec2
https://news.thomasnet.com/fullstory/new-small-fr...
*** LARGE PROPERTY *** ~237 KB Preview:"\nClick to fetch this property
tag:google.com,2013:googlealerts/feed:66437800947...
1
2
3
4
Rename Collection
i40_system .
digital_twin_google_ne
Rename
Tools
Export Standard
Export --jsonArray
Export --csv
Reindex
Import --mongoexport json
Compact
Delete
Collection Stats
Documents
72
Total doc size
6.27 MB
Average doc size
89.17 KB
Pre-allocated size
2.39 MB
Indexes
2
Total index size
80 KB
Padding factor
Extents

Opened a first HTML content attribute by creation on "Large Property":

Indexes

Name	Columns	Size	Attributes	Actions
_id_	_id ASC	36 KB		DEL
atom_entry_id_1_feed_description_1	atom_entry_id ASC feed_description ASC	44 KB	unique: true	DEL

Mongo Express Database: i40_system > Collection: digital_twin_google_news_content

VIEWING COLLECTION: DIGITAL_TWIN_GOOGLE_NEWS_CONTENT

New Document | New Index

Simple | Advanced

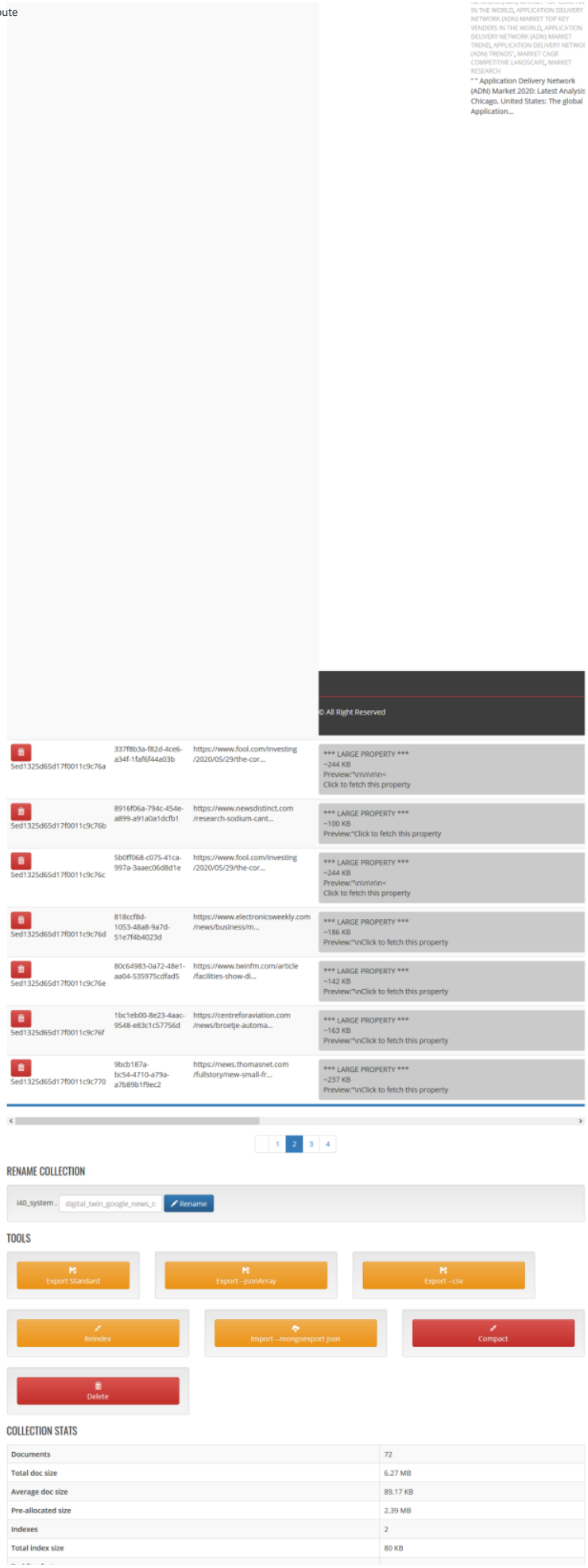
Key | Value | String | Find

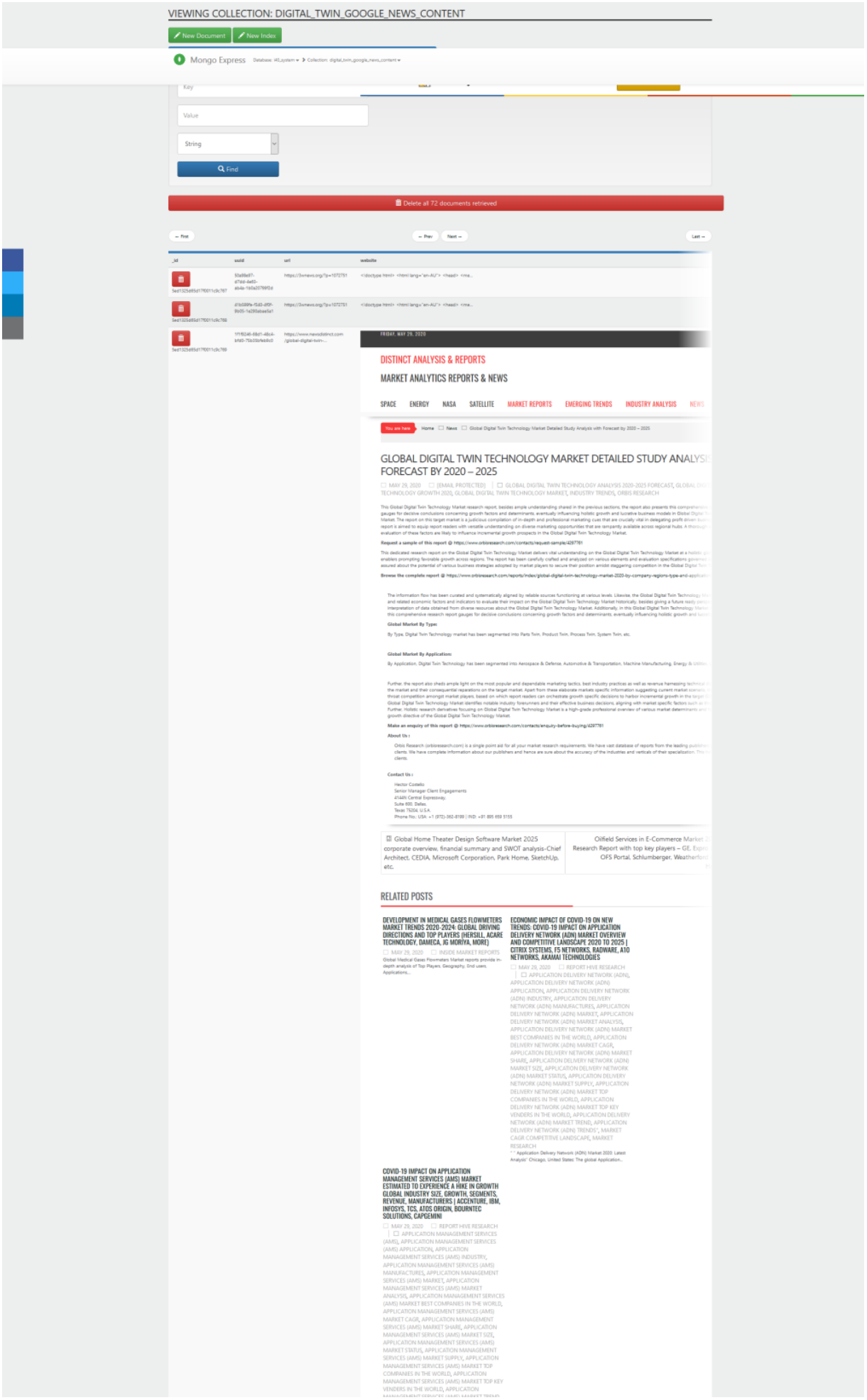
Delete all 72 documents retrieved

← First | ← Prev | Next → | Last →

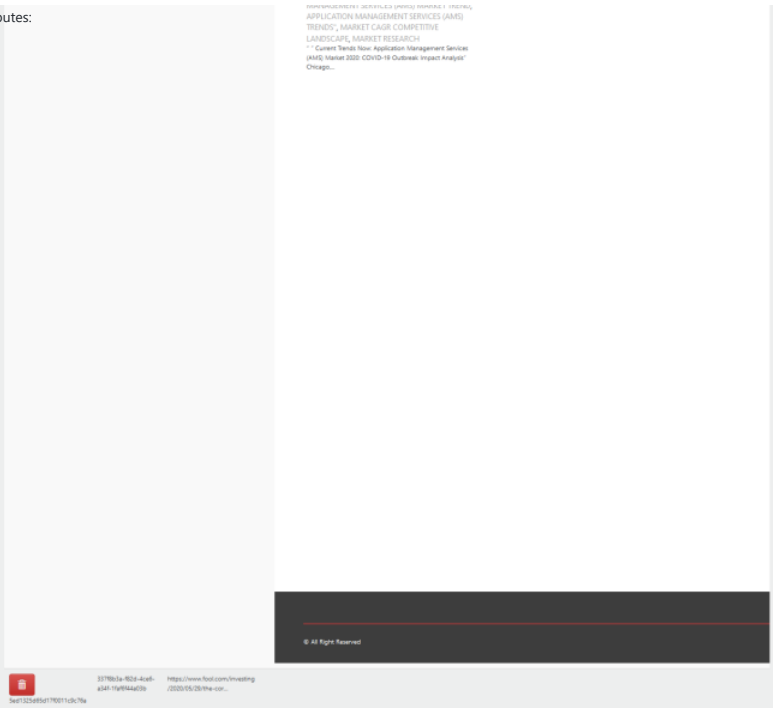
_id	uuid	url	website
5ed1325d65d17f0011c9c767	50a98e97-d7dd-4e63-ab4a-1b0a20799f2d	https://3wnews.org/?p=1072751	<!doctype html> <html lang="en-AU"> <head> <me...
5ed1325d65d17f0011c9c768	41b599fe-f340-4f0f-9b05-1e290abae5a1	https://3wnews.org/?p=1072751	<!doctype html> <html lang="en-AU"> <head> <me...
5ed1325d65d17f0011c9c769	1f1f9246-68d1-48c4-bfd0-75b35bfeb9c0	https://www.newsdistinct.com/global-digital-twin-...	FRIDAY, MAY 29, 2020 DISTINCT ANALYSIS & REPORTS MARKET ANALYTICS REPORTS & NEWS SPACE ENERGY NASA SATELLITE MARKET REPORTS EMERGING You are here Home News Global Digital Twin Technology Ma GLOBAL DIGITAL TWIN TECHNOLOGY MARKET DETAILE FORECAST BY 2020 – 2025 MAY 29, 2020 GLOBAL DIGITAL TWIN TECHNOL DIGITAL TWIN TECHNOLOGY GROWTH 2020, GLOBAL DIGITAL TWIN TECHNOLOGY M This Global Digital Twin Technology Market research report, besides amp sections, the report also presents this comprehensive research report ga growth factors and determinants, eventually influencing holistic growth Digital Twin Technology Market. The report on this target market is a jud professional marketing cues that are crucially vital in delegating profit dr aimed to equip report readers with versatile understanding on diverse re available across regional hubs. A thorough assessment and evaluation o incremental growth prospects in the Global Digital Twin Technology Mar **Request a sample of this report @** https://www.orbisresearch.com/conta This dedicated research report on the Global Digital Twin Technology Ma perspective, rendering conscious statistical analysis and a wholistic persp carefully crafted and analyzed on various elements and evaluation specif readers to remain assured about the potential of various business strate Twin Technology Market. **Browse the complete report @** https://www.orbisresearch.com/reports/ to-2025 The information flow has been curated and systematically aligned by re also includes substantial cues and offers an in-house analysis of global Digital Twin Technology Market historically, besides giving a future rea interpretation of data obtained from diverse resources about the Glob report, besides ample understanding shared in the previous sections. growth factors and determinants, eventually influencing holistic growth **Global Market By Type:** By Type, Digital Twin Technology market has been segmented into Part **Global Market By Application:** By Application, Digital Twin Technology has been segmented into Aero Further, the report also sheds ample light on the most popular and de The report is a conscious means to address some of the most glaring c these elaborate markets specific information suggesting current marke as well as cut throat competition amongst market players, based on w Global Digital Twin Technology Market. Furthermore, in the course of t forerunners and their effective business decisions, aligning with marke Digital Twin Technology Market. Further, Holistic research derivatives h market determinants and factors representing factors, challenges, tre Technology Market. **Make an enquiry of this report @** https://www.orbisresearch.com/con **About Us :** Orbis Research (orbisresearch.com) is a single point aid for all your m authors across the globe. We specialize in delivering customized repo hence are sure about the accuracy of the industries and verticals of th market research study for our clients. **Contact Us :** Hector Costello Senior Manager Client Engagements 4144N Central Expressway, Suite 600, Dallas, Texas 75204, U.S.A. Phone No.: USA: +1 (972)-362-8199 | IND: +91 895 659 5155 Global Home Theater Design Software Market 2025 corporate overview, financial summary and SWOT analysis-Chief Architect, CEDIA, Microsoft Corporation, Park Home, SketchUp, etc. Oilfield Servic Researcl International RELATED POSTS DEVELOPMENT IN MEDICAL GASES FLOWMETERS MARKET TRENDS 2020-2024: GLOBAL DRIVING DIRECTIONS AND TOP PLAYERS (HERSILL, ACARE TECHNOLOGY, DAMECA, JG MORIYA, MORE) MAY 29, 2020 INSIDE MARKET REPORTS Global Medical Gases Flowmeters Market reports provide in-depth analysis of Top Players, Geography, End users, Applications.... ECONOMIC IMPACT OF COVID-19 ON NEW TRENDS: COVID-19 IMPACT ON APPLICATION DELIVERY NETWORK (ADN) MARKET OVERVIEW AND COMPETITIVE LANDSCAPE 2020 TO 2025 | CITRIX SYSTEMS, F5 NETWORKS, RADWARE, A10 NETWORKS, AKAMAI TECHNOLOGIES MAY 29, 2020 REPORT HIVE RESEARCH | APPLICATION DELIVER NETWORK (ADN), APPLICATION DELIVER NETWORK (ADN) APPLICATION, APPLICATION DELIVERY NETWORK (ADN) INDUSTRY, APPLICATION DELIVERY NETWORK (ADN) MANUFACTURES, APPLICATION DELIVERY NETWORK (ADN) MARKET, APPLICATION DELIVERY NETWORK (ADN) MARKET ANALYSIS, APPLICATION DELIVERY NETWORK (ADN) MARKET BEST COMPANIES IN THE WORL APPLICATION DELIVERY NETWORK (ADN) MARKET CAGR, APPLICATION DELIVERY NETWORK (ADN) MARKET SHARE, APPLICATION DELIVERY NETWORK (ADN) MARKET SIZE, APPLICATION DELIVERY NETWORK (ADN) MARKET STATUS, APPLICATION DELIVERY NETWORK (ADN) MARKET SUPPLY, APPLICATION DELIVER NETWORK (ADN) MARKET TOP COMPAN

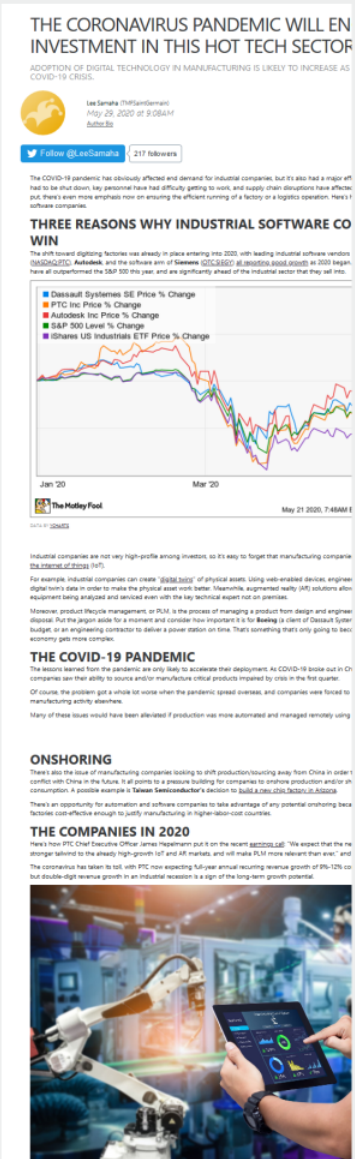
Opened a second HTML content attribute

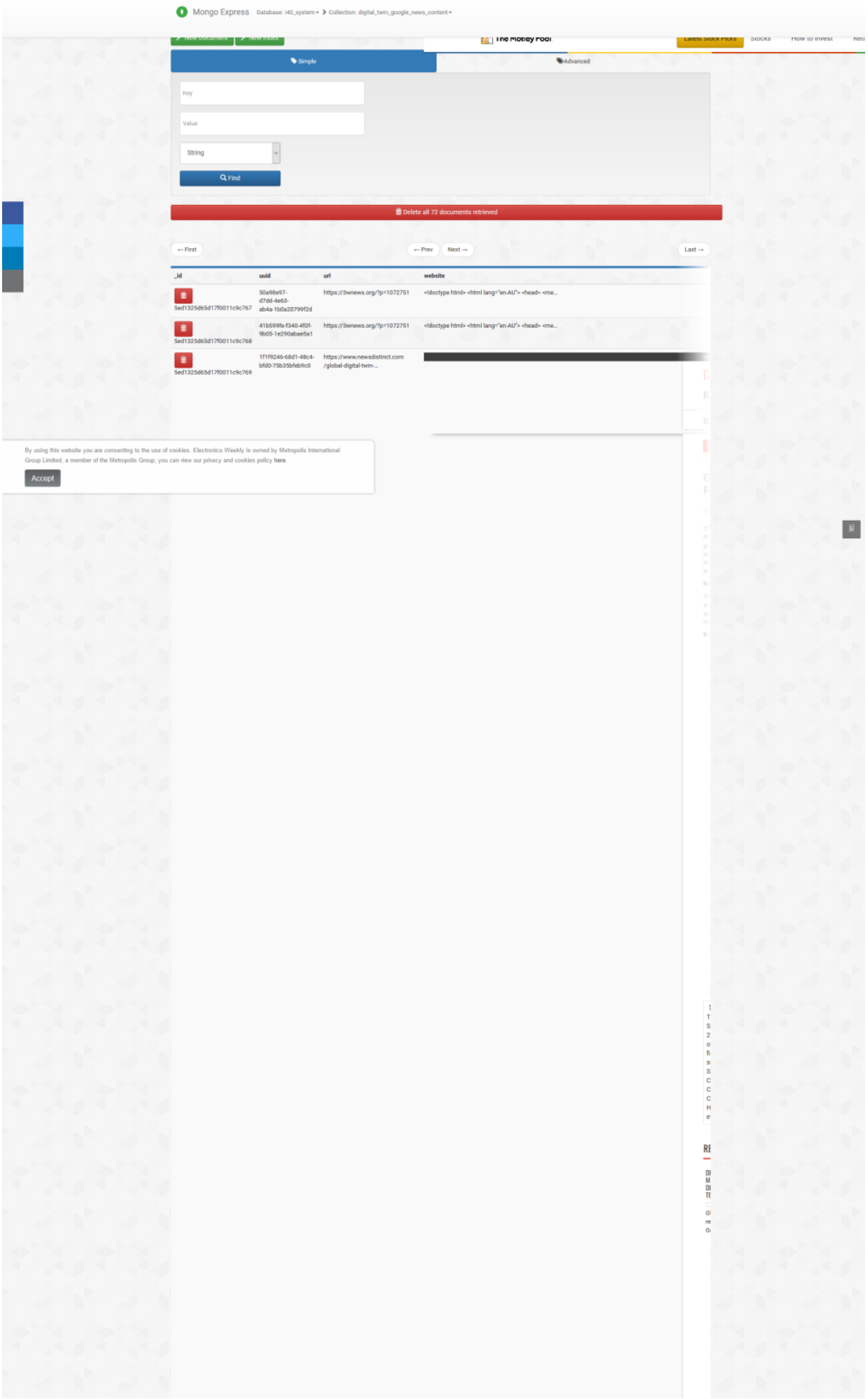


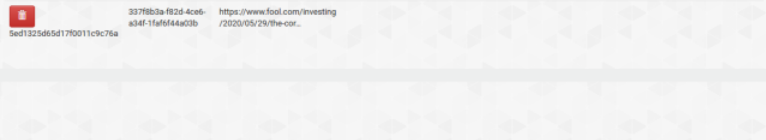

VIEWING COLLECTION: DIGITAL_TWIN_GOOGLE_NEWS_CONTENT
New Document
New Index
Mongo Express
Key
Value
String
Find
Delete all 72 documents retrieved
_id
uuid
url
website
FRIDAY, MAY 29, 2020
DISTINCT ANALYSIS & REPORTS
MARKET ANALYTICS REPORTS & NEWS
SPACE
ENERGY
NASA
SATELLITE
MARKET REPORTS
EMERGING TRENDS
INDUSTRY ANALYSIS
GLOBAL DIGITAL TWIN TECHNOLOGY MARKET DETAILED STUDY ANALYSIS FORECAST BY 2020 – 2025
RELATED POSTS
DEVELOPMENT IN MEDICAL GASES FLOWMETERS MARKET TRENDS 2020-2024: GLOBAL DRIVING DIRECTIONS AND TOP PLAYERS (HERSILL, ACARE TECHNOLOGY, DAMECA, JG MORIYA, MORE)
ECONOMIC IMPACT OF COVID-19 ON NEW TRENDS: COVID-19 IMPACT ON APPLICATION DELIVERY NETWORK (ADN) MARKET OVERVIEW AND COMPETITIVE LANDSCAPE 2020 TO 2025 | CITRIX SYSTEMS, F5 NETWORKS, RADWARE, A10 NETWORKS, AKAMAI TECHNOLOGIES
COVID-19 IMPACT ON APPLICATION MANAGEMENT SERVICES (AMS) MARKET ESTIMATED TO EXPERIENCE A HIKE IN GROWTH GLOBAL INDUSTRY SIZE, GROWTH, SEGMENTS, REVENUE, MANUFACTURERS | ACCENTURE, IBM, INFOSYS, TCS, ATOS ORIGIN, BOURNTEC SOLUTIONS, CAPGEMINI

Opened multiple HTML content attributes:

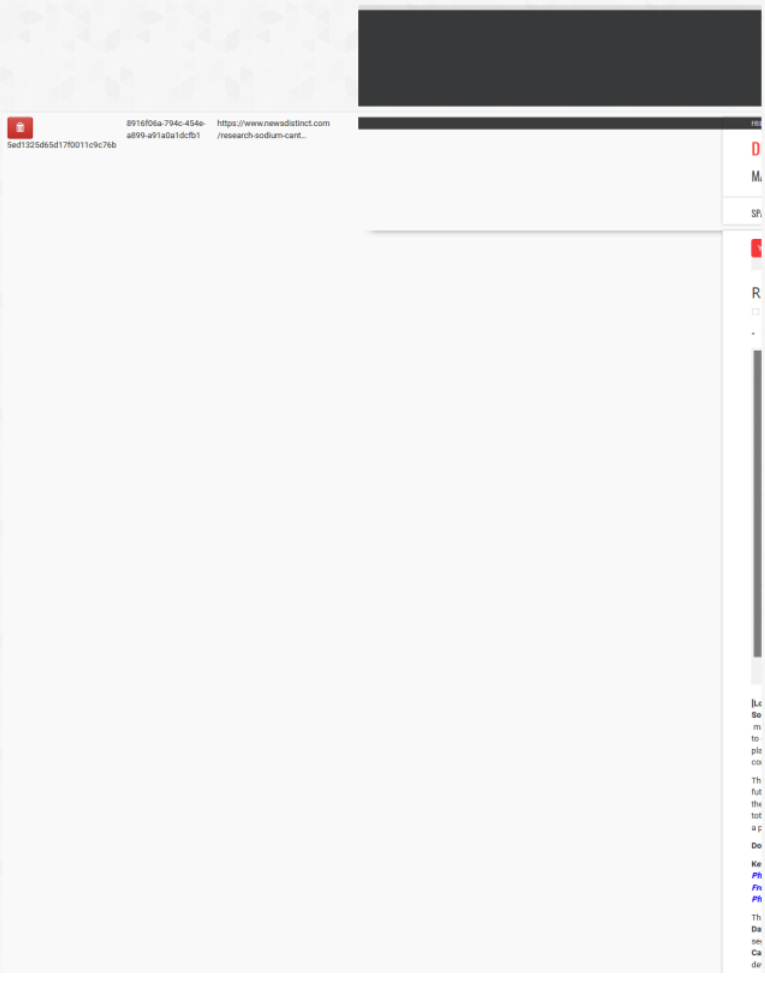


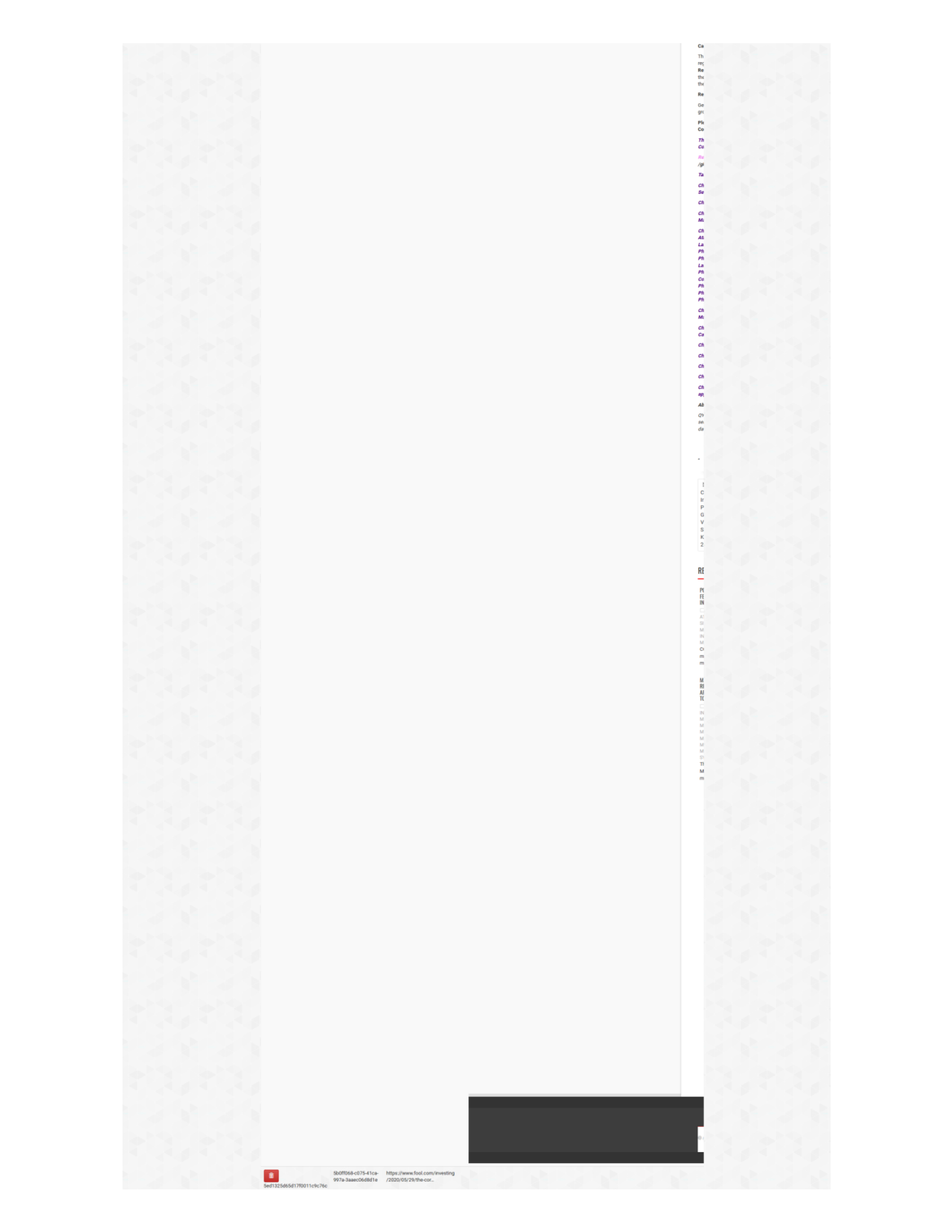



Mongo Express
Database: i40_system
Collection: digital_twin_google_news_content
Simple
Advanced
Key
Value
String
Find
Delete all 72 documents retrieved
← First
← Prev
Next →
Last →
_id
uuid
url
website
5ed1325d65d17f0011c9c767
50a98e97-d7dd-4e63-ab4a-1b0a20799f2d
https://3wnews.org/?p=1072751
<!doctype html> <html lang="en-AU"> <head> <me...
5ed1325d65d17f0011c9c768
41b599fe-f340-4f0f-9b05-1e290abae5a1
https://3wnews.org/?p=1072751
<!doctype html> <html lang="en-AU"> <head> <me...
5ed1325d65d17f0011c9c769
1f1f9246-68d1-48c4-bfd0-75b35bfeb9c0
https://www.newsdistinct.com/global-digital-twin-...
By using this website you are consenting to the use of cookies. Electronics Weekly is owned by Metropolis International Group Limited, a member of the Metropolis Group; you can view our privacy and cookies policy here.
Accept



5ed1325d65d17f0011c9c76a	337f8b3a-f82d-4ce6-a34f-1fafbf44a03b	https://www.fool.com/investing/2020/05/29/the-cor...


5ed1325d65d17f0011c9c76b
8916f06a-794c-454e-a899-a91a0a1dcfb1
https://www.newsdistinct.com/research-sodium-cant...



5ed1325d65d17f0011c9c76d

818ccf8d-1053-48a8-9a7d-51e7f4b4023d

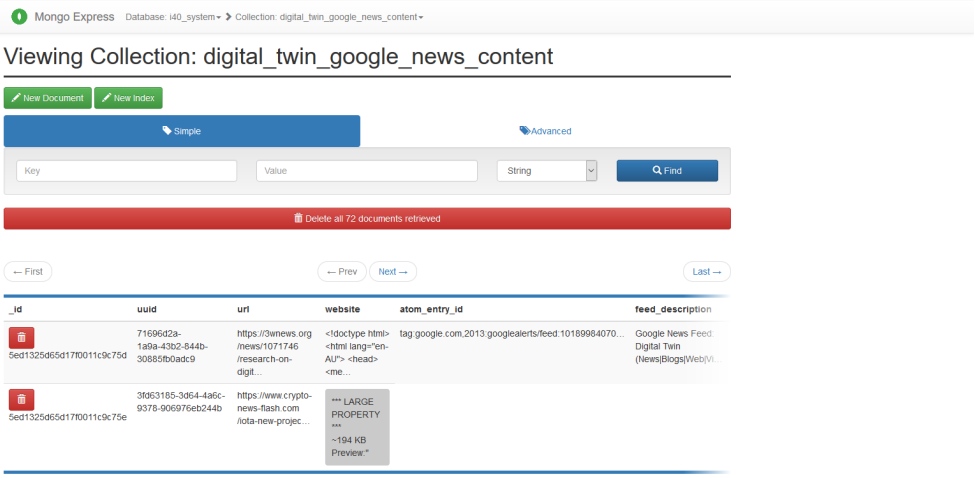
https://www.electronicsweekly.com/news/business/m...

5ed1325d65d17f0011c9c76e
80c64983-0a72-48e1-aa04-535975cdfad5
https://www.twinfm.com/article/facilities-show-di...
SafeGroup

MartinEnders commented on May 30, 2020 Author

I had a look at the HTML-source of the overview-page and it seems that the preview content of the big attributes ("Async on-demand loading of big document properties (>100KB default) to keep collection view fast") is not escaped:

Screenshot of mongo-express in browser:

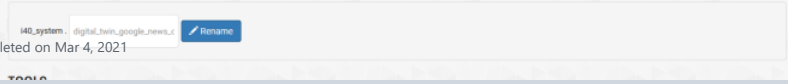


Screenshot of the HTML source of the above page:

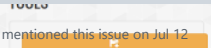
```
        <td><div class="tableContent">

        https://www.crypto-news-flash.com/iota-new-projec…
        </div></td>

        <td><div class="tableContent">

        <div class="tooDamnBig" doc_id="%225ed1325d65d17f0011c9c75e%22" doc_prop="website" title="Max prop size: 100 KB">*** LARGE PROPERTY ***<br>~194 KB<br>Preview:"<!DOCTYPE html><!--[if I<br>Click to fetch this property</
        </div></td>

        <td><div class="tableContent">

        tag:google.com,2013:googlealerts/feed:37837622195…
        </div></td>

        <td><div class="tableContent">

        Google News Feed: Digital Twin (News|Blogs|Web|Vi…
        </div></td>

      </tr>
```

1 2 3 4

MartinEnders changed the title ~~RENAME COLLECTION~~ ~~fields is not escaped~~ HTML in String fields is not escaped if only preview is loaded on May 30, 2020



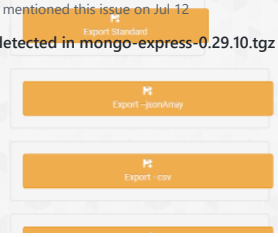
dozoisch closed this as completed on Mar 4, 2021



mend-bolt-for-github bot mentioned this issue on Jul 12

CVE-2021-21422 (Medium) detected in mongo-express-0.29.10.tgz - autoclosed pustovitDmytro/ianus#38

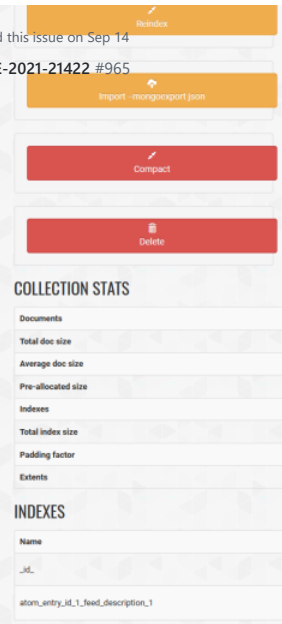
Closed



BlackthornYugen mentioned this issue on Sep 14

Media cell vulnerability CVE-2021-21422 #965

Closed



COLLECTION STATS

Documents	72
Total doc size	6.27 MB
Average doc size	89.17 KB
Pre-allocated size	2.39 MB
Indexes	2
Total index size	80 KB
Padding factor	
Extents	

INDEXES

Name	Columns	Size	Attributes	Actions
_id_	_id ASC	36 KB		DEL
atom_entry_id_1_feed_description_1	atom_entry_id ASC feed_description ASC	44 KB	unique: true	DEL