CCL SOLUTIONS GROUP

Rabbit Hole

New in RabbitHole v4 - More data formats. More from SQLite. More to discover

With the addition of RealmDB, MMKV and Mozilla IndexedDB, RabbitHole now supports 45 different datatypes in a single tool. Version 4 also builds on advanced SQLite forensics features, with new timestamp decoding and Insight features.

You don't know what you're missing

RabbitHole is a powerful data exploration tool, picking up where other tools leave off.

Add it to your digital forensics toolkit and you have one tool to train in, one tool to validate and one tool for drilling down through unprocessed data. With support for viewing, parsing and reporting on 45 data types, you can keep digging down to find data that might otherwise stay hidden - and potentially prove pivotal to your investigation.



"RabbitHole works by combining an expanding range of data format viewers into a single interface. It introduces the concept of 'Reparsing' – where RabbitHole takes data from one view, interprets it and presents it back to you in a more appropriate format, with just one simple click. It's about getting you close to the best view of the raw data quickly, efficiently and cost-effectively. Until you use it, you really don't know what you're missing."

Alex Caithness
Lead Developer, RabbitHole

Go further
Process and report on the data other tools can't reach, without the need for scripting and coding.

Drill down into data
Effortlessly understand live and deleted data embedded in other data, with no need to export between different software.

Save time
An intelligent, intuitive experience - less time needed to find out more, boosting both outcomes and throughput.

Buy once
Invest in a single tool with no need to validate multiple tools for multiple file formats.

+44 (0)1789 261 200
cclsolutionsgroup.com

First for digital forensics and cyber security

RabbitHole run-through

When you open a file or reparse data, RabbitHole works in the background to detect the format and highlights the most likely formats in the user interface - helping you navigate sometimes unfamiliar data types with greater speed and confidence. With RabbitHole, you are always in control, free to override the 'guessed' formats and make your own selections at any time.

1 App Databases

SQLite databases are the ubiquitous data storage format used by apps across multiple platforms. RabbitHole has an SQLite data viewer, but it is also very common to find other data structures encoded within database fields, for example: JSON or XML in text fields; property lists or protocol buffers encoded in blob fields.

Reviewing these embedded fields in a traditional database viewer would require exporting the data, selecting and running a second tool, importing the data, then potentially finding a second layer of data to export. In RabbitHole, you simply right click the data and choose a more appropriate view.

RabbitHole can also recover deleted data from SQLite databases, with recovered records rebuilt into a database so you can rapidly and effortlessly explore, query and report on them just as if they were live.

2 Obfuscated Exploit Code

Threat actors making use of command shell scripts may make use of multiple layers of encodings to hide the true meaning of the code. It is not uncommon to encounter multiple rounds of Base64, gzip compression, XOR encryption. In RabbitHole, there is no need to export data or run scripts; simply select the data, right click and choose the conversion you need to apply.

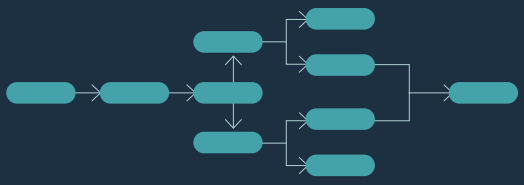
Reporting

Many of the views support exporting and generating reports from the data. The easy-to-use 'Tree Parser' allows you to quickly generate reports from hierarchical data structures (e.g. XML, JSON, Property Lists, Protocol Buffers, and more) through an intuitive graphical interface.



Runs

RabbitHole's 'Runs' feature lets you combine multi-stage processes into a single automated, repeatable process, no coding skills needed. A Run can be used again whenever the artefact is next encountered, even batch processing multiple files, to save you more time.



Supported Data Types:

- ABX (Android Binary XML)
- Base64
- Bencode
- Binary Deobfuscation
- Brotli Compression
- Chromium/Electron: IndexedDb
- Chromium/Electron: Local Storage
- Chromium/Electron: Session Storage
- Compound/OLE File
- Deflate Compression Algorithm
- Encode Text to Bytes
- Entropy Calculator
- Epoch Time
- Facebook Serialisation
- Flat Buffer
- GZip Compression
- Hash
- Hex Text
- Hex View
- HTML
- Image View
- Java Serialization Stream
- JSON
- LevelDb
- LZFSE Compression
- MessagePack
- MMKV
- Mozilla IndexedDB
- Mozilla LZ4 Compression
- Plist (Binary)
- Plist (Text/XML)
- PM Records
- Protocol Buffer
- RealmDB
- SEGB
- Snappy Compression
- SQLite
- String View
- Text Processor
- Text View
- URL
- URL Encoded String
- Windows Registry
- XML
- Zlib Compression

System requirements

Windows 10 or higher
.NET framework 4.8

+44 (0)1789 261 200
cclsolutionsgroup.com

First for digital forensics and cyber security