CCL
SOLUTIONS
GROUP

Rabbit Hole

Discover More

RabbitHole is setting a new standard in forensic data exploration tools.

Now you can drill down into data and effortlessly switch to the optimal view for the data format you are looking at.

It's not just about saving time but also enabling analysts to understand the results they get better and faster – all of which translates neatly into greater job throughput and higher quality output.

New in RabbitHole 2.2

Introducing Data Type Detection

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. You always retain control and are free to override the 'guessed' formats and make your own selections.

Also new in RabbitHole 2.2

- ✓ ABX reparser for viewing Android Binary XML artefacts on Android 12+
- ✓ Updates to the Chromium IndexedDB reparser to support a wider range of data types and changes to the format
- ✓ LZFSE Compression reparser
- ✓ MessagePack reparser

Go further

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

Drill down into data

Working seamlessly to understand data embedded in other data, with no need to export between different software.

Save time

An intelligent, intuitive experience - more time to work with the data, less time spent wrangling with the tools.

Multi-task

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

Looking into RabbitHole

RabbitHole combines an expanding range of data format viewers into a single interface. It introduces the concept of 'Reparsing' – letting you take some or all of the data from one view and reparse it into a new, more appropriate format, all within the same tool.

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.

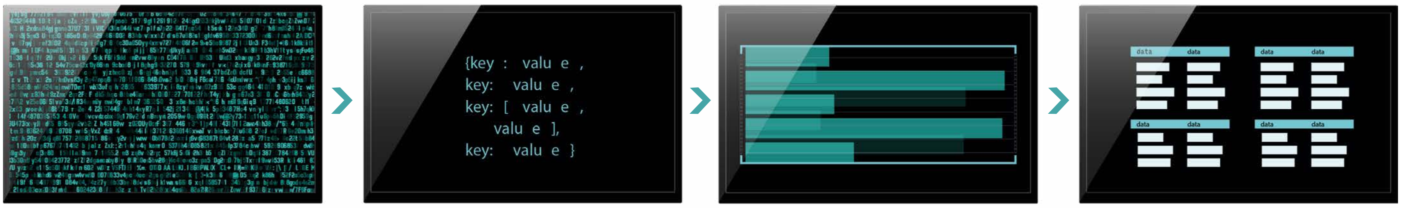
Reviewing these embedded fields in a traditional database viewer would require exporting the data, selecting and running a second tool, importing the data, then potentially finding a second layer of data to export. In RabbitHole, you simply right click the data and choose a more appropriate view.

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.



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
- Mozilla LZ4 Compression
- Plist (Binary)
- Plist (Text/XML)
- PM Records
- Protocol Buffer
- 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