CCL
SOLUTIONS
GROUP

NEW Release 2.1

Drill down into data

Rabbit Hole

Setting a new standard
in forensic data
exploration tools

Your trusted data partner

Developed by CCL's R&D Centre of Excellence, 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.

That means stand-out performance and cost efficiency out of the box.

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 2.1

- Chromium IndexedDB reparser – for reading and reporting on data stored in IndexedDB in Chrome, Chromium-based applications
- Chromium Local Storage and Session Storage reparsers - for reading and reporting on data stored in Web Storage in Chrome, Chromium-based applications
- Bencode reparser for BitTorrent related artefacts
- Brotli compression reparser – Brotli compression is now found widely across a range of Chrome/ Chromium related artefacts where gzip was previous used
- Mozilla Flavour LZ4 Compression reparser – for decompressing Firefox LZ4 compressed data (e.g "jsonlz4" files)
- Search whole SQLite Databases using keywords or regular expressions/grep
- Bulk export blob fields form SQLite databases
- Automatically infer and decode Protocol Buffer structures
- Tree Parser interface now allows regex matches for Keys

Process and report on the data that other tools don't process, without the need for scripting or coding

Drill down into data seamlessly, and understand data embedded in other data, with no requirement to export between different tools

Enjoy an intelligent, user-centric experience – more time to work with the data, less time spent wrangling with the tools

Invest in one complete tool, avoiding the need to find, curate and validate multiple tools for multiple file formats

Your trusted data partner

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.

Retracing Your Steps

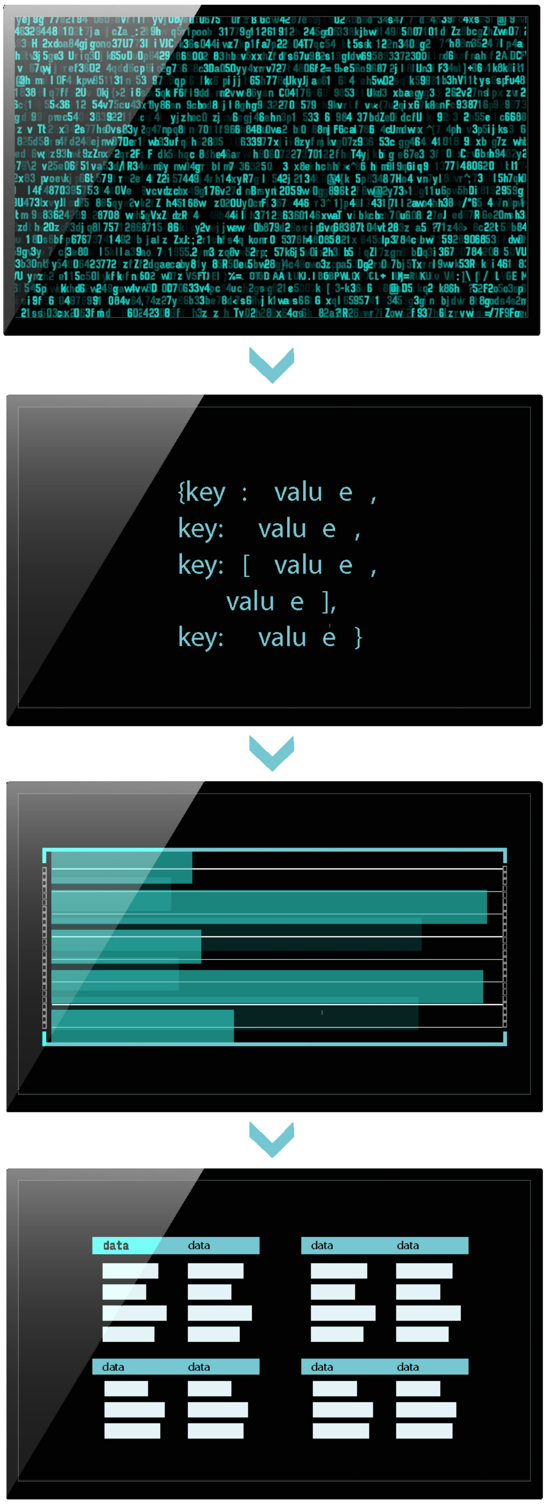
When using multiple different file viewers to process and understand your data, extra care must be taken to keep notes so that you can properly audit the different processes undertaken. In RabbitHole, all processes are automatically recorded: which data you processed and where that data came from - you can always trace your steps back through these movements.

RabbitHole also supports the ‘Dig’ project file format: if you are working within a dig, all data that you import and all processes will be recorded in a project file that you can share with other users, or return to if you need to recall your actions or dig further at a later date.

Your trusted data partner

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:

- 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
- 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

Canadian Distributor

TEELtechnologies
Canada

www.teeltechcanada.com
info@teeltechcanada.com