Belkasoft X
Evidence Center

"An outstanding feature is the cyber security forensic investigation view (Incident Investigation tab)"

TAKAYA KAWASAKI
Kawasaki is digital forensic analyst.
He has over 8 years of digital forensics experience
as a vendor investigator and corporate CSIRT member.

Japan

OVERVIEW

Belkasoft Evidence Center X can handle various OS types for investigation and may be used for a diverse range of investigations, but it seemed like a tool that shines more in cyber security forensic investigations than in malpractice investigations.
With few configuration items and outstanding ease of error checking, there is little learning cost involved with the tool per se, making it a friendly tool for starters who are new to high-performance, comprehensive forensic tools.

DETAILS

Positioning among comprehensive forensic tools

I presume there are three major categories of comprehensive forensic tools (respectively centering on the directory tree view, artifact view, and document search/review), out of which this tool seemed to be one of those centering on the artifact view. It also seemed to run fast for this type of tool, which was a plus.

It shouldn't be uncommon to use several of these tools for investigation in practice. However, this tool showed a lack of flexibility when cooperating with document review tools as mentioned later, which may mean that it is intended to cover the whole investigation with a single tool.

As for target OS for analysis, it covers not only Windows but also macOS/iOS/Android/Linux(ext*), and is capable of detecting and processing Android emulators and VM virtual disc files contained in the discs being analyzed as independent discs, which makes this product suitable for use in various investigations. It also offers its interface in Japanese, which seemed rather natural for the most part.

Currently there aren't so many macOS-compatible artifacts, so that is something you cannot expect too much on.

*More info on compatible images and file systems here: https://belkasoft.com/x

Use experience in malpractice investigation

It is a good point that many artifacts can be easily investigated via the artifact view (Artifact tab in this tool), but it felt rather awkward to use in conjunction with other document review tools because of the lack of freedom (L01 output, filename extension, Live/delete-dependent output folders, etc.) around file narrow-down filters and export functions in the directory tree view (File System tab in this tool). Also the incapability to display files and information in the recursive manner in the file system tab and artifact tab felt like a deterrent to investigation efficiency, so future improvements are desired in these areas.

Oftentimes in cases such as typical malpractice investigations on information leakage that require document reviews, the key to efficient completion of investigation lies in the flexibility when narrowing down files subject to review and exporting, thus it is necessary to check if the usage may suit the ordinary flow of investigation.

In addition, it is worth noting that, in malpractice investigations, the weak approach to proprietary metadata, as opposed to file systems, contained in MS Office documents and so forth (such as "author") makes detailed investigations in this regard difficult. Also, the time information can only be displayed in the UTC format in many scenes. While this may be advantageous in that there is less room for error as long as the specifications are understood, the conversion required each time is a tedious extra step nonetheless.

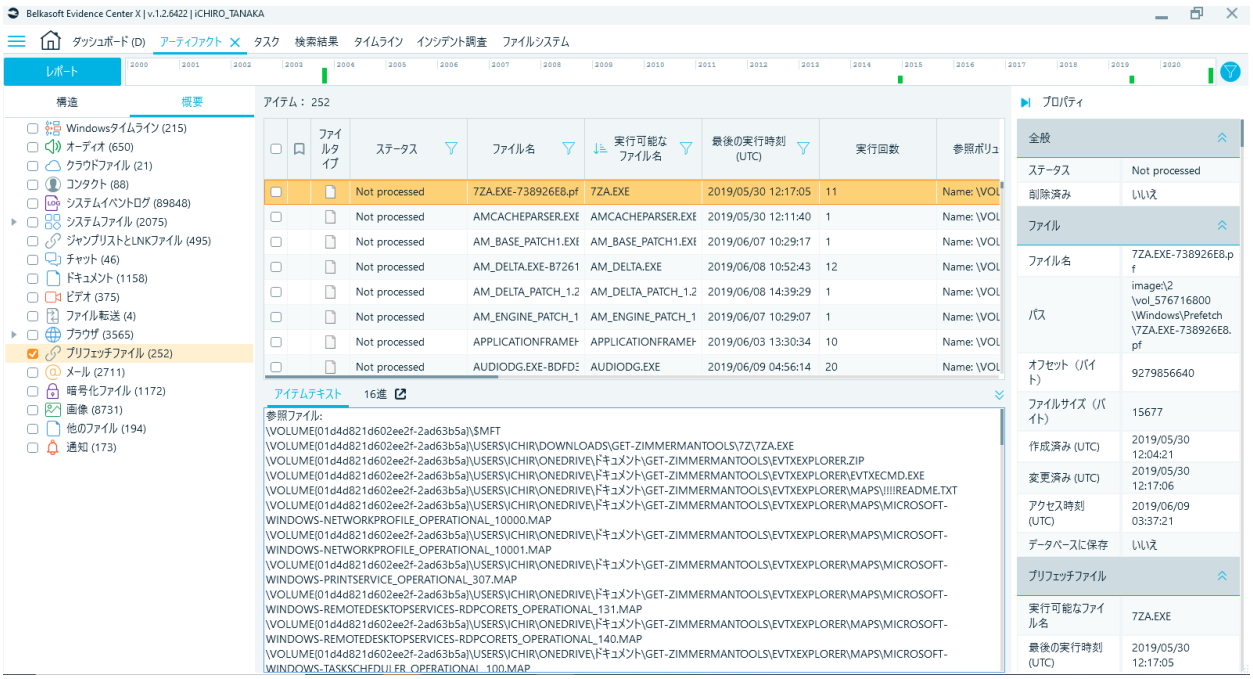

Fig. 1 Artifact tab

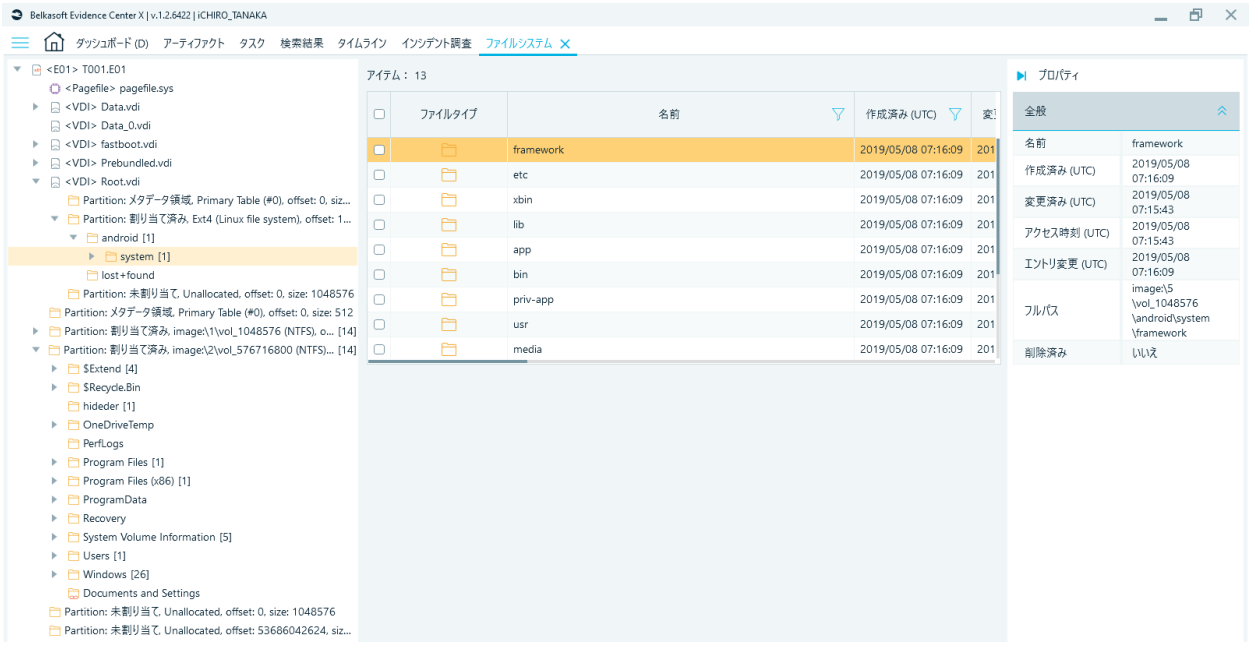

Fig. 2 File System tab

(Android emulator virtual disc within Windowsis also subject to analysis as an independent disc)

On the other hand, checking errors, a mandatory step with any forensic tool, is very easy to do, allowing for easy grasp of what's been done and what's not in the course of the investigation or report. This feature, while not too flashy, is an extremely useful factor that sure will benefit anyone from starters to professionals in any sort of investigation.

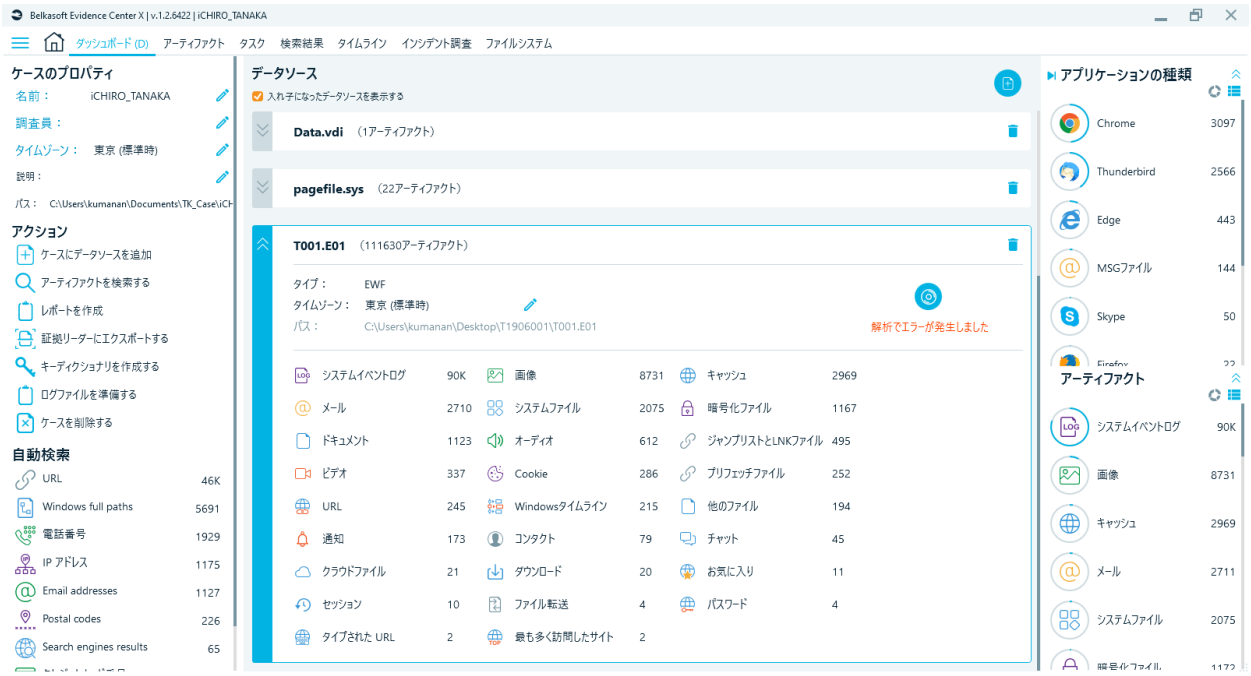

Fig. 3 Dashboard tab (presence of errors can be confirmed at a glance)

Fig. 4 Task tab (click the area marked with red frame in Fig. 3 to jump here)

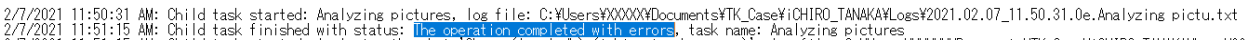

Fig. 5 Log file

(click the area marked with red frame in Fig. 4 to open the log,
where the area of error and the path of further detailed log are displayed)

Use experience in cyber security usage

The timeline function (Timeline tab) felt like a useful function, with detailed and comprehensible event classifications and filters.

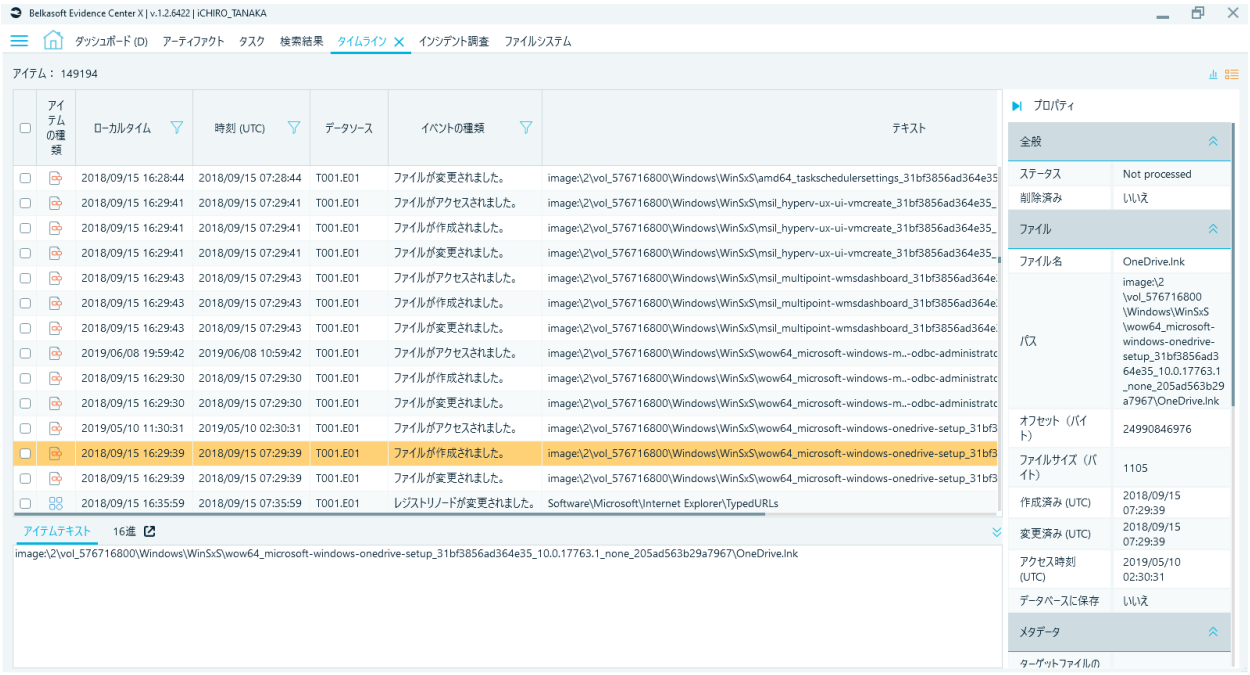

Fig. 6 Timeline tab

An outstanding feature is the cyber security forensic investigation view (Incident Investigation tab), which accommodates viewpoint-oriented listing of artifacts typically seen in cyber security forensics such as Persistence (although the Japanese translation “josetsu” for this word sounds a bit unnatural), Execution, and System event logs. Personally I’m quite fond of this comprehensible display of artifacts sorted by investigation viewpoints.

System event logs serve to cut out frequently used event logs for analysis on the ID level, which, to users’ delight, allows for smooth operation of lateral movements and powershell command investigations.

Fig. 7 Part of events displayed on timeline filter screen (timeline encompasses not only timestamps of files but also parse results of various artifacts such as program execution, event log, registry changing, mail/message reception, web browsing, etc.)

It is also a welcomed feature that, in the view displaying the information on event log 4624, Logon type is cut out as a field ready for sorting. It may have been even better if Logon type filtering was possible, so that’s something to look forward to in the future.
From yet another point of view, the analysis has a relative coverage of files of artifacts subject to triage in fast forensics as parsing targets, which appears to suit today’s demands.

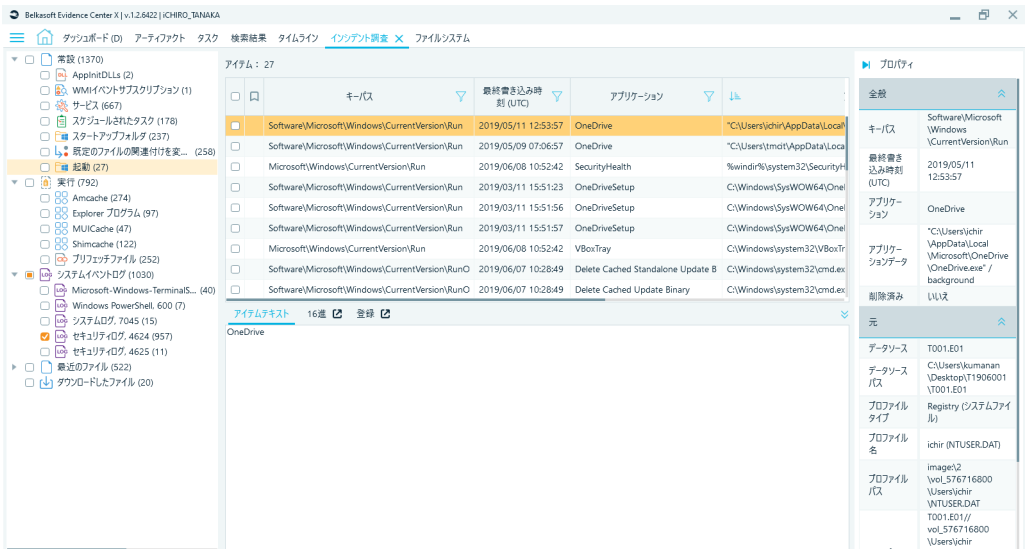

Fig. 8 Incident Investigation tab (Persistence display)

Fig. 9 Incident Investigation tab (security log)

VERIFICATION ENVIRONMENT

Tool reviewed

Belkasoft Evidence Center X Ver.1.2.6422

Analysis target OS (self-made Test data used)

Windows 10 Pro Ver.1809 (and 1511)

mac0S Ver.10.15.3

Miscellaneous

This review contains only personal opinions of the author, not to represent the groups or organizations the author takes part in.