One-Click Forensic Analysis: A SANS Review of EnCase Forensic

When security incidents occur, law enforcement needs forensic information in hours, not days. The new features in EnCase Forensic 8 purport to assist investigators in gathering and analyzing key data in a more efficient manner. Learn more in this product review of EnCase Forensic 8.

SANS

A SANS Product Review

One-Click Forensic Analysis:

A SANS Review of EnCase Forensic

Written by **Jake Williams**

June 2018

Sponsored by:

OpenText

Executive Summary

SANS evaluated OpenText's EnCase Forensic product to test its capability to analyze digital forensic data. At the outset, we were worried that EnCase v8 shared the same user interface shortcomings that plagued earlier releases of EnCase v7. We were pleasantly surprised and found v8 to combine all the best features of both v6 and v7, such as Pathways and faster indexing support, as well as adding new features of significant value. We found EnCase Forensic to be capable at performing forensic analysis tasks.

EnCase Forensic has many features that less experienced analysts might overlook, including its capability to truly support multiple monitors, robust keyword searching (including regular expressions), and a fully extensible platform through EnCase App Central and the EnScript programming language.

But OpenText didn't stop there. Although few analysts think of EnCase Forensic as a mobile forensics tool, the product supports both acquisition and analysis of mobile devices, including data stored in the cloud. EnCase Forensic also allows analysts to perform a 1:1 network preview and evidence acquisition of remote devices using a portable agent. This feature allows those organizations that might lack more robust enterprise forensic tools (like EnCase Enterprise) to operate like the Fortune 500 enterprises without a comparable budget. Finally, EnCase Forensic has a feature called *Pathways* that will help jump-start investigations and enable junior analysts to take a

more active role in investigations. With the Pathways feature, senior analysts can create forensic data processing playbooks, ensuring consistent processing of data that's as easy as clicking links on a web page.

In our test, EnCase Forensic performed admirably, and we recommend that any organization purchasing forensic software consider it. EnCase Forensic has many enterprise-level features in a single tool that are simply unmatched by its competitors.

Test Setup and Key Features

For this test, SANS used a Microsoft Windows 7 (x64) disk image in Expert Witness (.E01) format. The disk image was obtained before the start of this evaluation. Although EnCase Forensic can acquire forensic images, that functionality was not tested here. The system that SANS evaluated had extensive event logs, USB activity and multiple user logons, as well as web browser usage—ensuring that we examined the features a typical investigator would use. EnCase Forensic v8.06 was loaded on a Windows 10 x64 laptop running a 7th Generation Intel Core i7 processor, 32GB RAM, and a 1TB SSD.

EnCase Forensic is a very feature-rich product, and any full evaluation of the product could easily fill multiple papers. In this evaluation, SANS specifically evaluated the following features, each of which will be covered in-depth in this paper:

- Acquisition of Forensic Data Features
  - Device Acquisition
  - Direct Network Preview
- Productivity and Workflow Features
  - Pathways
  - Indexing
  - Keyword Searching
  - EnScripts and App Central
  - 4th Pane
- Evidence Processor Features
  - Prioritization
  - Entropy Analysis
  - Email Processing
  - Internet Artifact Processing

Acquisition of Forensic Data Features

EnCase Forensic has made strides in improving acquisition of forensic data through advances in device acquisition and use of the Direct Network Preview.

Device Acquisition

We didn't explicitly test device acquisition as part of this product review; however, it is worth mentioning because many readers are probably unfamiliar with the myriad device acquisition options that EnCase Forensic offers. Although many examiners don't think of EnCase Forensic as a tool for mobile device acquisition, the tool supports acquiring and parsing data from a wide range of mobile devices, tablets and other nontraditional devices (e.g., Garmin GPS systems). Those potential users who spend their time performing *only* mobile device analysis might be disappointed in the mobile device analysis options, but for those organizations unable to justify the expense of dedicated mobile device forensic software, these features help bridge an important capability gap.

Armed with these acquisition and analysis features, investigators can create a single case that includes a laptop, tablet and mobile phone image from a suspect user and analyze them together. Placing all the evidence into a single case allows analysts to make correlations that might be missed if they were using multiple software platforms for analysis.

Another important feature in EnCase Forensic is the capability to acquire data from cloud services in a repeatable, forensically sound manner. This feature is especially important in the context of mobile devices because much of the data used by a suspect user is actually stored in the cloud, not on the device itself. EnCase Forensic can parse an image acquired from a mobile device, extract the authentication token stored on the device, authenticate it with a remote service and download data. Of course, investigators should ensure that they have explicit authorization to connect to the cloud service, either through written permission from the suspect user or through a court order. Currently, EnCase Forensic supports the following cloud services:

- Amazon Alexa
- Facebook
- Gmail
- Google Drive
- Google Locations
- Twitter

The robust acquisition capabilities of EnCase Forensic make it a clear leader for an all-in-one forensics platform capable of acquiring and analyzing myriad device types.

Direct Network Preview

The Direct Network Preview functionality of EnCase Forensic enables organizations without the budget for expensive enterprise acquisition tools to perform acquisition of forensic data over the network. Direct Network Preview is limited to one connected device at a time. So, while it isn't suitable for mass acquisitions, it is definitely well-suited for triage of a suspect machine or ad hoc acquisition tasks.

Even for organizations that have EnCase Basic (formerly EnCase Enterprise), there may not be a licensed agent on each machine on the network. This is particularly true for legacy Unix hosts. EnCase Forensic solves this problem by allowing investigators to

create portable agents—or optionally, installers—that can be deployed individually to target machines to allow for data acquisition. The available agents for EnCase Forensic v8.06 are shown in Figure 1.

Obtaining a Direct Network Preview is as easy as either installing the remote agent or running the portable agent from the command line without installation. Direct Network Preview supports the acquisition of physical memory and process memory, as well as access to those drives connected to the machine. By default, the portable agent listens on **`TCP port 4445`**, a port that is unlikely to be listening on heavily segmented networks; however, the portable agent can be started to listen on any TCP port, making it easier to operate across ports already permitted by internal access control lists. See Figure 2.

A valuable use for Direct Network Preview is acquiring a logical volume image of a device that is using full disk encryption. By acquiring the volume image from a running system, the analyst can obtain a decrypted volume image. If the same drive were removed from the machine and a physical image were taken, the analyst would have to obtain the decryption keys to analyze the data. While EnCase Forensic also supports decrypting full disk encryption, acquiring the logical volume in a decrypted state can enable a faster analysis. Direct Network Preview was evaluated in our test and provided remote access to the physical volume, the logical volume (disk partition), physical memory and individual process virtual memory spaces. See Figure 3.

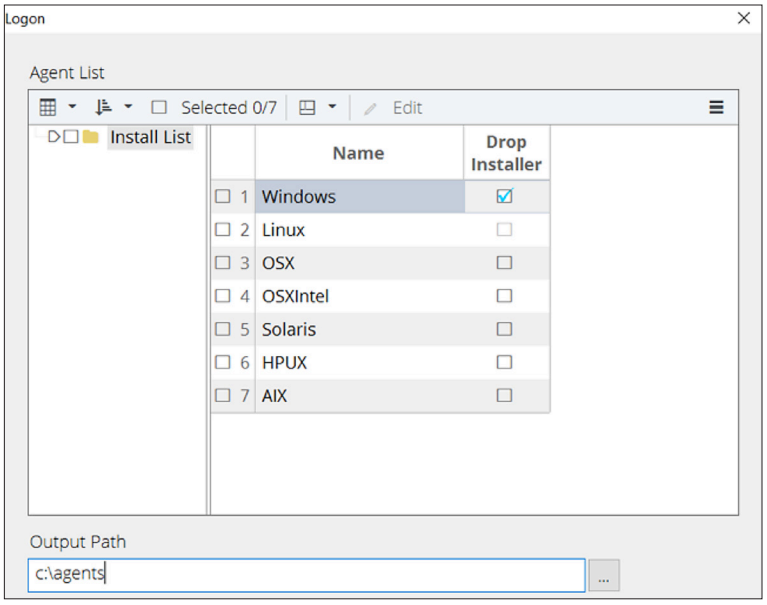

Figure 1. Available Direct Network Preview Agents

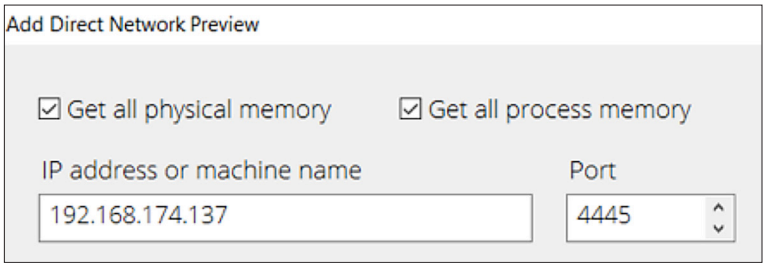

Figure 2. Configuring Direct Network Preview

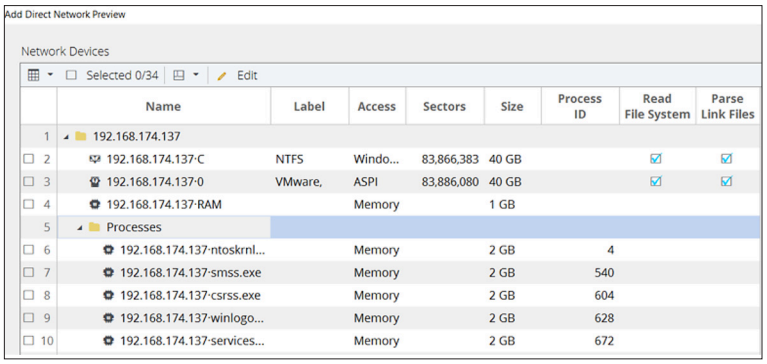

Figure 3. Direct Network Preview Volumes and Processes

Productivity and Workflow Features

EnCase Forensic includes a number of productivity and workflow features that enable more efficient investigations. The features evaluated in this review include Pathways, Indexing, Keyword Searching, EnScripts and App Central, and 4th Pane.

Pathways

The EnCase Pathways feature makes investigations phenomenally easier, particularly for junior analysts. With Pathways, analysts can merely click their way to success by following a predefined workflow. Although the Pathways feature seems to have been originally created as a "beginner" feature, we found ourselves returning to it for case processing because much of what we wanted to do was already in a preinstalled Pathway. Even senior investigators already familiar with the operation of EnCase Forensic are likely to benefit from Pathways for the efficiency of quick access to common investigative tasks.

EnCase Forensic comes with two Pathways installed. The first is Full Investigation, and as the name implies, this feature would be used when the analyst intends to conduct a full forensic investigation of a system. See Figures 4 and 5.

Figure 4. Full Investigation Pathway Processing Options

The other preinstalled Pathway is Preview/Triage. This Pathway is better suited to answering a specific question (such as "What websites did the user view?") without fully processing the machine. Another excellent use case for this Pathway is the application of a set of known malicious hashes to quickly determine whether further investigation on the machine is necessary. An example use case for this feature would be to load known malware hashes to quickly determine whether the "Trojan defense" might be used in a wrongful termination case. If known malware is found on the suspect image, the organization would likely route the case to a much more senior investigator.

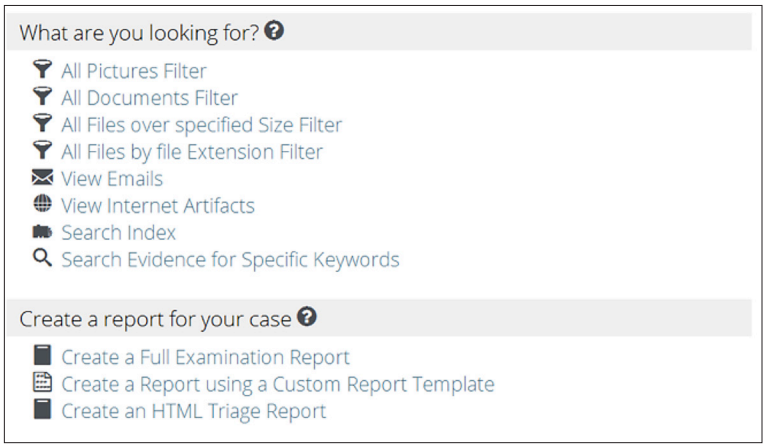

Figure 5. Full Investigation Pathway Analysis Links

The killer feature of Pathways is its capability to enable analysts to create their own Pathways. By defining custom Pathways, the investigation process can be standardized across multiple cases and even for multiple analysts. Custom EnScripts can be used in custom Pathways, further expanding the flexibility of EnCase Forensic.

One potential use for this feature is creating a new Pathway for triaging a potential malware infection. Decoding artifacts of execution is always important for investigating malware compromises. An investigator might want to parse **`ShimCache`** (aka **`AppCompatCache`**) and **`Prefetch`** data from every disk image they triage. After obtaining EnScripts from App Central (see page 7) to parse these artifacts, the analyst can create a new Pathway to perform these actions. This makes creating the case, adding the evidence, running the EnScripts and creating a quick triage report as easy as clicking the links in the EnCase Forensic user interface.

This sample scenario for creating a custom Pathway may not be pertinent to all who use EnCase Forensic, but it is hard to overstate the value of being able to create custom Pathways. This feature allows senior analysts to literally code their investigation process into the forensic tool. If you can click a link, you can process evidence for an investigation. Of course, you still need skills to analyze and make sense of the data, but standardizing processing is a precondition of standardizing analysis. No other commercial forensic platform available today offers this level of customization and flexibility to enable workflow standardization across myriad case types.

Indexing

EnCase Forensic v8 has undergone multiple enhancements to its indexing engine. Most of the changes accelerate the speed with which the case processes. SANS analysts did not perform side-by-side comparisons to determine how much faster EnCase Forensic v8 completed indexing compared to v7. In our evaluation, indexing seemed much faster than in previous versions. In fact, while our evaluation is purely qualitative, indexing completed so much faster than expected that we originally thought there was an error. Thankfully, there was not.

One of the biggest value-adds of text searching in EnCase Forensic is the expanded language support. EnCase Forensic can index in multiple languages and character sets, including languages that primarily use multibyte character sets (e.g., Arabic or Cyrillic). If an analyst knows the suspect system uses additional languages, they can enable the specific languages in the EnCase Evidence Processor.

Keyword Searching

Keyword searching in EnCase Forensic is easier than ever. Analysts can search keywords for use in the EnCase Evidence Processor either during indexing or through a raw (non-indexed) image in the Evidence tab. While searches against non-indexed data obviously take longer to complete, for many scenarios it makes sense to index the evidence only if some condition is shown to be true. One such condition might be the presence of a particularly interesting string. A United States Department of Defense investigator looking for leakers, for instance, might index the entire volume of an unclassified machine only if they first found the string **`"TOP SECRET"`** in the acquired volume. EnCase Forensic makes such an assessment possible with raw keyword searching, allowing investigators to perform keyword searches prior to fully indexing data.

When building keyword lists, it helps to know what you'll be getting before executing a time-consuming search. Most analysts have had the experience of performing a search and waiting for the results only to find that a keyword was spelled incorrectly or some other such error. With its Keyword Tester, EnCase Forensic helps the analyst avoid this time-wasting encounter. See Figure 6.

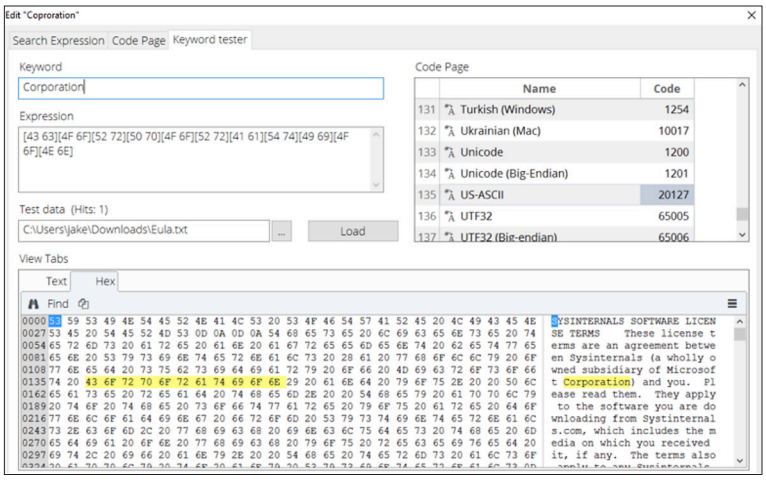

Figure 6. Keyword Tester

This feature allows the analyst to load a sample file and verify that the expected patterns will be discovered. Note that this "preview" feature does not properly parse Microsoft Office documents and other complex file formats. All the same, it is a useful feature as it enables analysts to maximize their productivity.

In addition to supporting keyword searching in practically any conceivable code page, EnCase Forensic supports searching for keywords using regular expressions. EnCase calls this feature *GREP*, and it supports most regular expression options. This is useful if you generally know what you are looking for, but need to use a wild card for the expression.

In the case under test, a metallurgy engineer, who works in metals such as adamantium and vibranium, has used the suspect machine. Because the analyst believes that the subject's machine was compromised, the organization wants to determine which specific precious metals the user had information about on his machine to perform a damage assessment. The investigator could type an exhaustive list of rare metals, but this approach is suboptimal. Because the investigator knows that all metals synthesized by the organization are given trade names ending in *-ium*, the analyst can initiate a GREP search to discover additional metal variants which might otherwise be missed. The creation of a GREP keyword is illustrated in Figure 7.

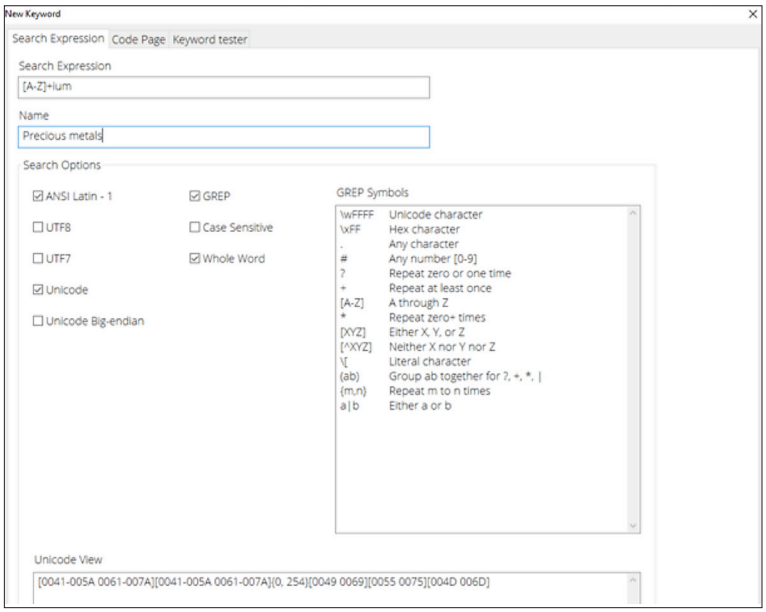

Figure 7. GREP Regular Expressions

EnScripts and App Central

One of the central features of EnCase Forensic has always been that it enables users to extend the platform through the EnScript programming language. Although most other vendors have chosen to build all supported features directly into their platforms, EnCase Forensic uses a much different paradigm: allowing the end user to expand the platform. In our test experience, this model is preferred because it future-proofs analysis. New forensic artifacts are discovered regularly, and providing analysts with the ability to incorporate them into the platform without a formal feature request is a huge enabler.

This EnScript feature also allows analysts to build capabilities for detecting custom artifacts. In one client environment, we discovered a log file that contained telemetry/debugging data for an application deployed throughout the enterprise. Unbeknownst to us, the application was tracking process-creation events. The attacker was apparently unaware of this as well because they were surgically cleaning a process-creation event (**`event ID 4688`**) from the Windows Security Event Log but not cleaning the same entries from the telemetry log. Obviously, no vendor has parsers for custom telemetry and debugging logs built into their product; however, with EnCase Forensic, we were able to build a custom EnScript to parse these logs. Further, EnScript made it possible to compare process-creation events in the custom log with those in the Windows Event Logs and to find discrepancies. This made it trivial to highlight those things the attackers specifically didn't want the investigators to see.

But not every forensics shop has developers available to build custom EnScripts. In the past, analysts could search for scripts published by various authors on their respective websites. When running scripts from third parties, there is always some question of safety. After all, you wouldn't simply download random macros to execute in your Microsoft Office documents. Now there's App Central, where users can download scripts, many of which OpenText maintains directly. All EnScripts in App Central are submitted by vetted developers, reducing the chances of malicious scripts entering the official EnCase Forensic ecosystem.

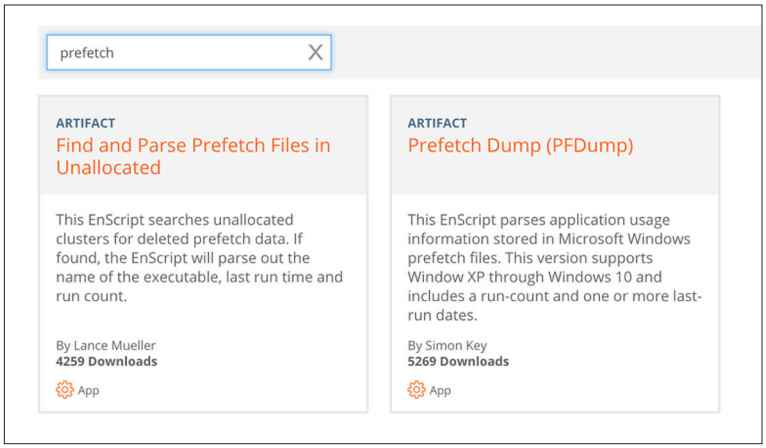

Figure 8. EnCase App Central

During this product review, we downloaded App Central and discovered prebuilt scripts for parsing **`Prefetch`** and **`ShimCache`**. See Figure 8.

Unfortunately, there was no EnScript in App Central for parsing **`AmCache`**, but perhaps that's to be expected because it's a relatively new artifact. A quick Google search, however, did turn up an **`AmCache`** EnScript from a reputable developer. While we would have preferred to install all of our EnScripts from App Central, this example still highlights the real power the EnCase Forensic platform offers.

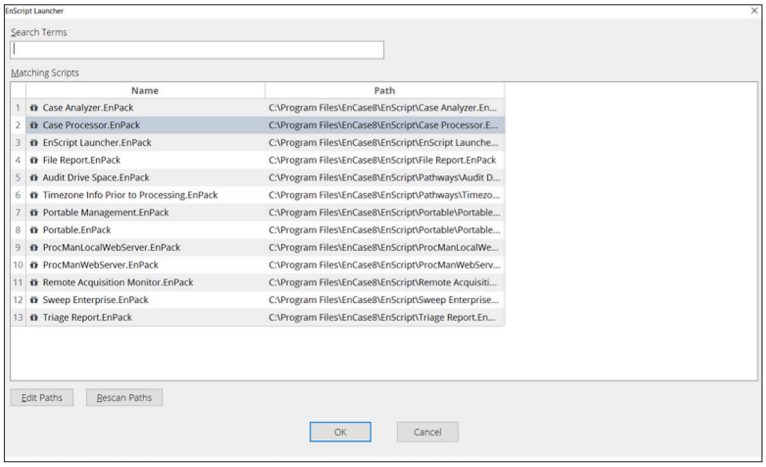

Figure 9. EnScript Launcher

Once EnScripts have been loaded into the system, the new EnScript Launcher makes it easier than ever to launch scripts. In previous versions, launching EnScripts was a more cumbersome process, but in EnCase Forensic v8, EnScripts can be launched directly by using hot keys. By using the Ctrl+Shift+R hot key combination, the EnScript Launcher pops up. This user interface was obviously written with analyst input. Perhaps the best thing about this user interface is that keyboard focus is immediately placed in the Search Terms box, allowing the analyst to quickly select and execute an EnScript without ever having to touch the mouse. Features like this one, which allow the analyst to maximize efficiency, are obvious throughout the newest EnCase Forensic product release. See Figure 9.

4th Pane

One tested feature in EnCase Forensic that many analysts are sure to love is called *4th Pane*. Using this feature, analysts can undock the View Pane of EnCase Forensic (normally at the bottom of the user interface) and move it independently from the rest of the user interface. This feature allows analysts to maximize their use of multiple monitors, which is very common among forensics practitioners. See Figure 10.

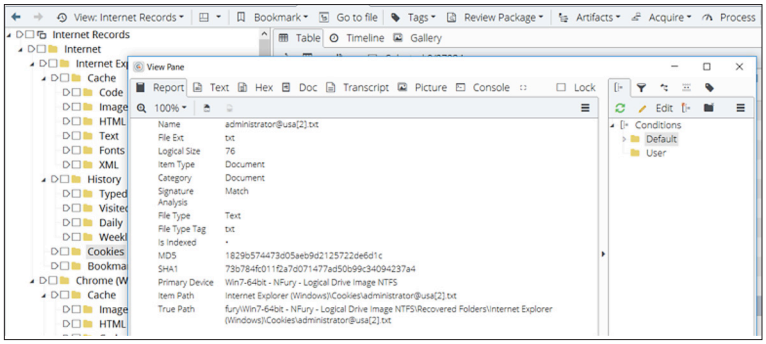

Figure 10. 4th Pane

One aspect of the 4th Pane feature was difficult to figure out at first: How do you move the exposed pane back into the main user interface? It turns out that no special magic is required. By clicking the X to close the detached 4th Pane, it is automatically re-docked in the main user interface. When re-docking the detached pane, the specific tab in use (Hex, Doc, etc.) does not change, ensuring a seamless transition for the analyst when undocking and re-docking.

Evidence Processor

The EnCase Evidence Processor is the focal point for analyzing evidence in the case. The Evidence Processor contains several interesting features, which were well thought-out and obviously analyst driven. A few features of the EnCase Evidence Processor that will be discussed in this section are:

- Prioritization
- Entropy analysis
- Email processing
- Internet artifact processing

The EnCase Evidence Processor user interface is shown in Figure 11.

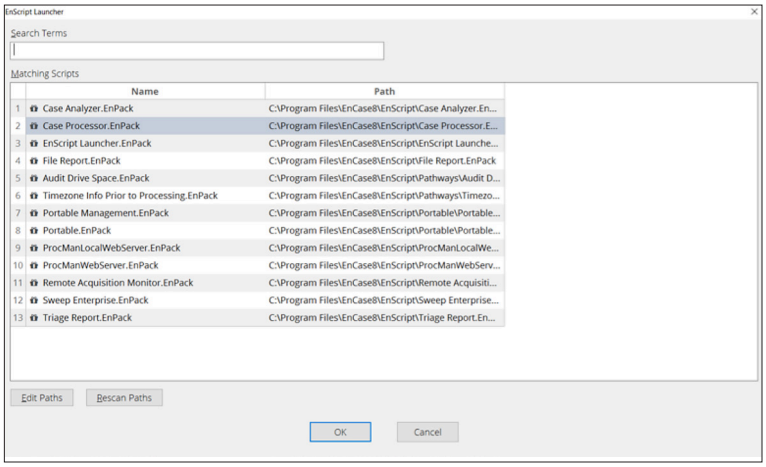

Figure 11. EnCase Forensic Evidence Processor User Interface

Prioritization

The EnCase Evidence Processor offers an option to prioritize specific processing. This setting allows the analyst to view those results first—before any other analysis has been completed. This option is particularly useful if the analyst is working a high priority case and needs to answer specific questions quickly while the case continues to process in the background. The prioritization user interface allows analysis of both documents and pictures to be prioritized. These are two items that are central to many forensic investigations. Further, the interface allows the investigator to limit the system to processing files found within a specific date range. One mildly frustrating feature of the prioritization user interface is that the Tab key does not move the user's cursor between month/day/year fields. The prioritization user interface is shown in Figure 12.

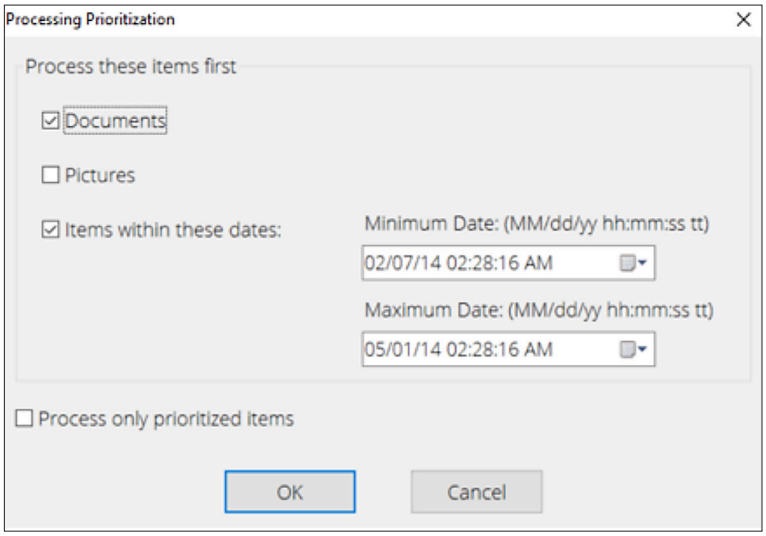

Figure 12. Case Prioritization User Interface

This functionality would have been useful in a recent insider data theft case: The employee had thousands of documents on her machine, but the organization was especially interested in those documents created during the week the employee submitted her resignation. Rather than processing the entire case to answer questions about specific documents, the investigator needs only to open the prioritization user interface, fill in the date range in question and begin the processing. The results in which the investigator is most interested will finish processing first, allowing the

analyst to immediately answer some tactical questions about the case. Meanwhile, the remaining documents on the system will continue processing in the background, which is useful in the event additional document analysis is required.

The case prioritization feature would also be useful for minimizing the collateral processing of evidence, if so dictated by either legal counsel or the organization's policy. Suppose an employee attached a bring-your-own device, such as a phone or tablet, to the network for three days, contrary to organizational policy. The investigator could select the *Process only prioritized items* checkbox within a defined date range to process only those documents with timestamps during the period the device was connected to the network, preserving the suspect's privacy.

Entropy Analysis

The EnCase Evidence Processor also supports entropy analysis under the Hash Analysis option. *Entropy* is a measure of how random a particular file is. A text file, for example, will likely contain a relatively limited number of different characters. As a result, it is deemed to have low entropy. A zip file, on the other hand, has very high entropy because the data is compressed mathematically. Although entropy analysis is disabled by default, in some specific cases it can be a great tool if enabled. The Entropy Analysis configuration user interface is shown in Figure 13.

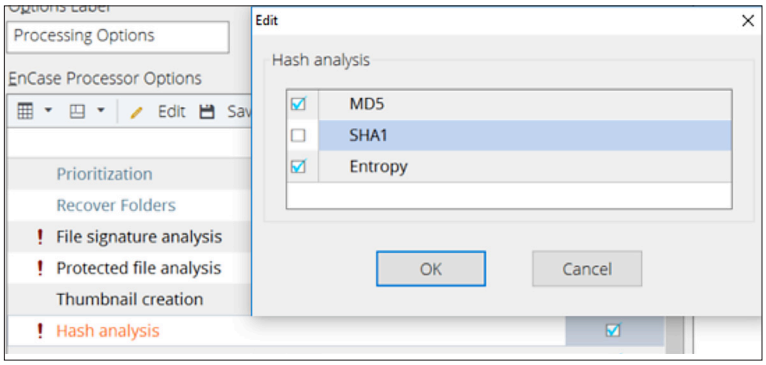

Figure 13. Entropy Analysis User Interface

Within incident response investigations, locating malware on a potentially infected endpoint is always important. Entropy analysis is an important tool in locating malware because many malware authors use packers to obfuscate their code and cloak it from detection by antivirus scans. In doing this, the malware author is also leaving an observable glitch in the matrix, so to speak, by changing the file's properties—specifically, its entropy. Because packers compress or encrypt the original malware code and leave only a small unpacking stub, packed programs have a very high entropy compared to other executable files. This is particularly true of programs found in the Windows system folders because malware authors love to hide there and Microsoft does not typically pack its programs. In our test, the EnCase Evidence Processor was able to discover several malware files on the test image.

Another prime use case for entropy analysis is in locating hidden, encrypted containers. Technologically advanced users may use hidden, encrypted containers to hide contraband data in a plausibly deniable manner. Because proper encryption renders any container files completely random, any encrypted containers should be located using entropy analysis. Although our test image did not include hidden, encrypted containers, based on EnCase Forensic's entropy analysis performance in our test, we are confident these containers would be discovered.

Email Processing

EnCase supports investigating files stored in a number of email processing options. Although investigation of the **PST** (Microsoft Outlook) format is fairly common among forensic software products, Lotus Notes support is somewhat sparser. EnCase supports the detection and processing of multiple email mailbox formats, including **EDB** (Microsoft Exchange), **DBX** (Outlook Express) and even Unix-style **MBOX** files. Figure 14 shows the email processing options available.

The test image, unfortunately, only contained a **PST** file, so we did not explicitly test the rest of the functions. The author, however, has used EnCase in the past to parse Lotus Notes. The performance then was on par with **PST** parsing. But there's a reason that **PST** is at the top of the list of parsers: It is the most prevalent format used in today's enterprise environments. A preview of one of the suspect's emails in a **PST** file discovered when the case was processed is shown in Figure 15.

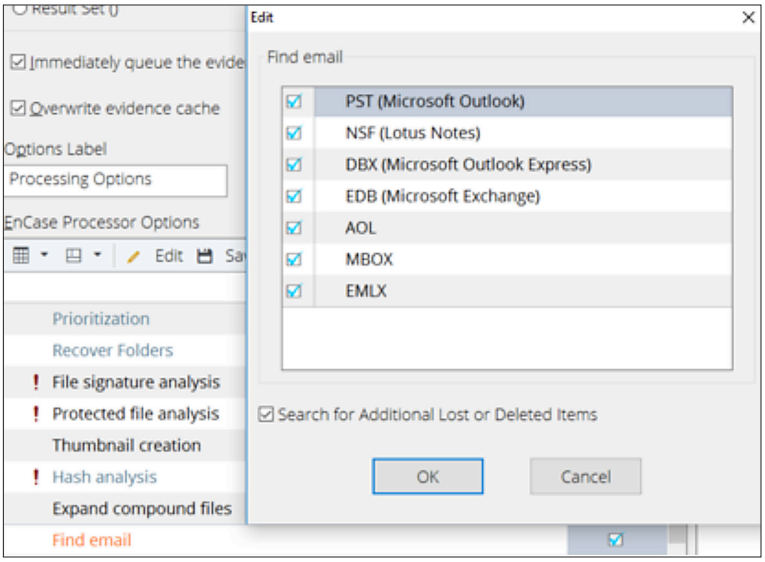

Figure 14. Email Processing Options

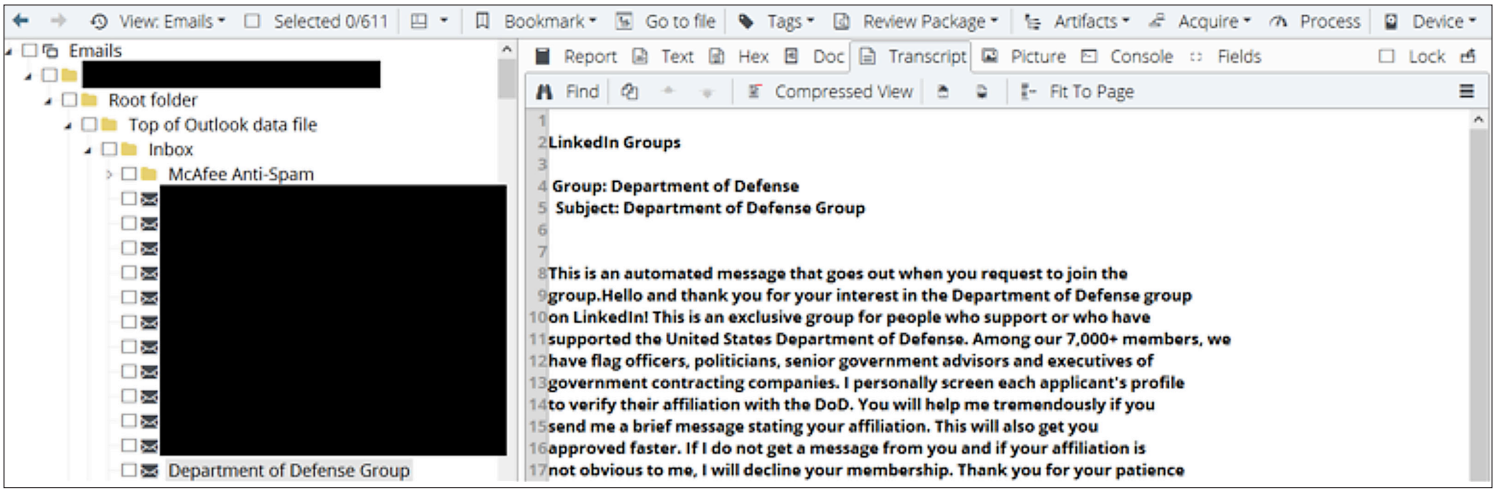

*Figure 15. Viewing Email in a **PST** File*

Internet Artifact Processing

The EnCase Evidence Processor also parses Internet artifacts from several major web browsers. One web browser that is notably absent from the list is Microsoft Edge. OpenText has indicated that while some web history activity for Edge is supported in v8.06, full support for parsing all Edge artifacts will be available in a future release. The list of supported browsers is shown in Figure 16.

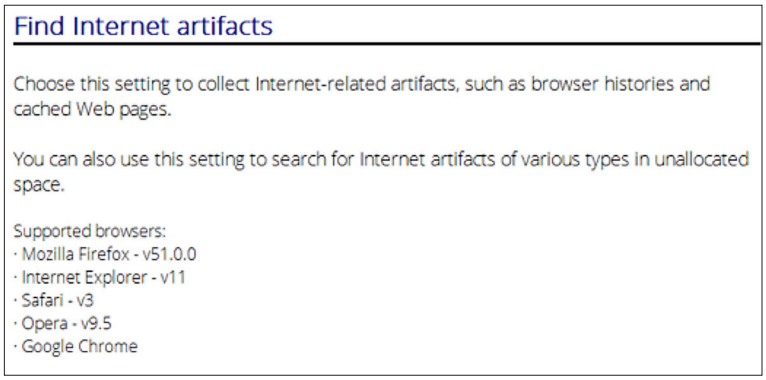

Figure 16. Supported Browsers for Internet Artifact Processing

In our test of EnCase Evidence Processor, we were able to successfully parse Microsoft Internet Explorer artifacts. EnCase Evidence Processor displayed all relevant information from the artifacts parsed. A cookie from **usa.gov** is displayed in Figure 17; this cookie indicates the user likely visited this site.

If EnCase Forensic can't provide all the options the analyst desires for viewing files in Internet history, an EnScript in App Central is available to extract all browser-related artifacts for processing using external tools. Although these artifacts could be extracted manually, this is a great use case for extending the EnCase Forensic platform using EnScripts and automating an otherwise tedious task.

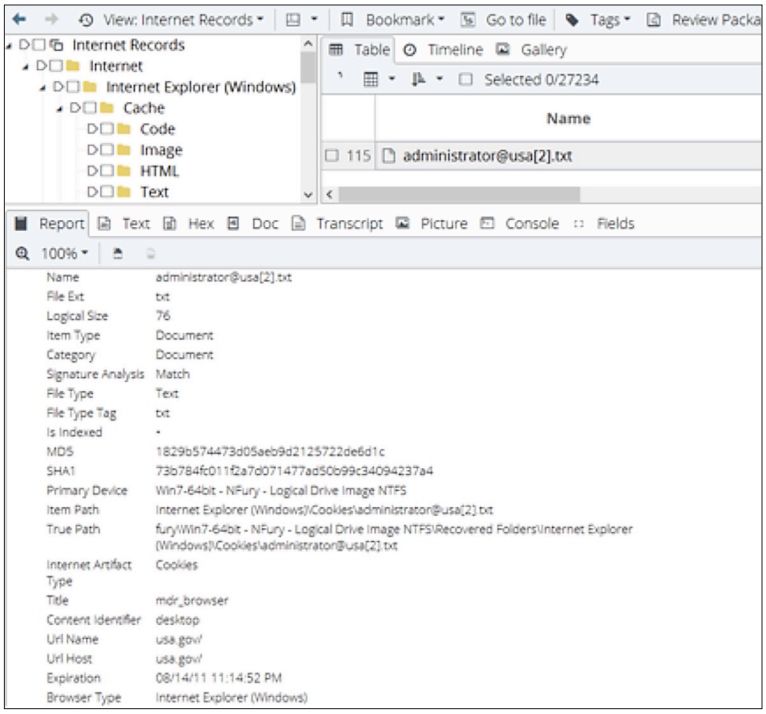

Figure 17. Viewing Cookies

Conclusion

We found the EnCase Forensic v8.06 product to perform well when processing our sample data set during the review. The layout and features of EnCase Forensic were obviously analyst inspired and ensure a relatively easy workflow. From the support for using multiple monitors with the 4th Pane feature to the extensibility of the platform with EnScripts, EnCase Forensic is a robust tool for organizations of any size. Organizations operating on smaller budgets will appreciate the inclusion of mobile forensics capabilities and Direct Network Preview, making EnCase Forensic a far more versatile product than many of its competitors' offerings.

About the Author

Jake Williams is a SANS analyst, senior SANS instructor, course author and designer of several NetWars challenges for use in SANS' popular, "gamified" information security training suite. Jake spent more than a decade in information security roles at several government agencies, developing specialties in offensive forensics, malware development and digital counterespionage. Jake is the founder of Rendition InfoSec, which provides penetration testing, digital forensics and incident response, expertise in cloud data exfiltration, and the tools and guidance to secure client data against sophisticated, persistent attack on-premises and in the cloud.

Sponsor

SANS would like to thank this paper's sponsor:

opentext™

Last Updated: October 15th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Houston 2018	Houston, TXUS	Oct 29, 2018 - Nov 03, 2018	Live Event
SANS Gulf Region 2018	Dubai, AE	Nov 03, 2018 - Nov 15, 2018	Live Event
SANS Sydney 2018	Sydney, AU	Nov 05, 2018 - Nov 17, 2018	Live Event
SANS DFIRCON Miami 2018	Miami, FLUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS London November 2018	London, GB	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS Dallas Fall 2018	Dallas, TXUS	Nov 05, 2018 - Nov 10, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS Mumbai 2018	Mumbai, IN	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Rome 2018	Rome, IT	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Osaka 2018	Osaka, JP	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CAUS	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS ICS410 Perth 2018	Perth, AU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
Secure DevOps Summit & Training 2018	OnlineCOUS	Oct 22, 2018 - Oct 29, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced