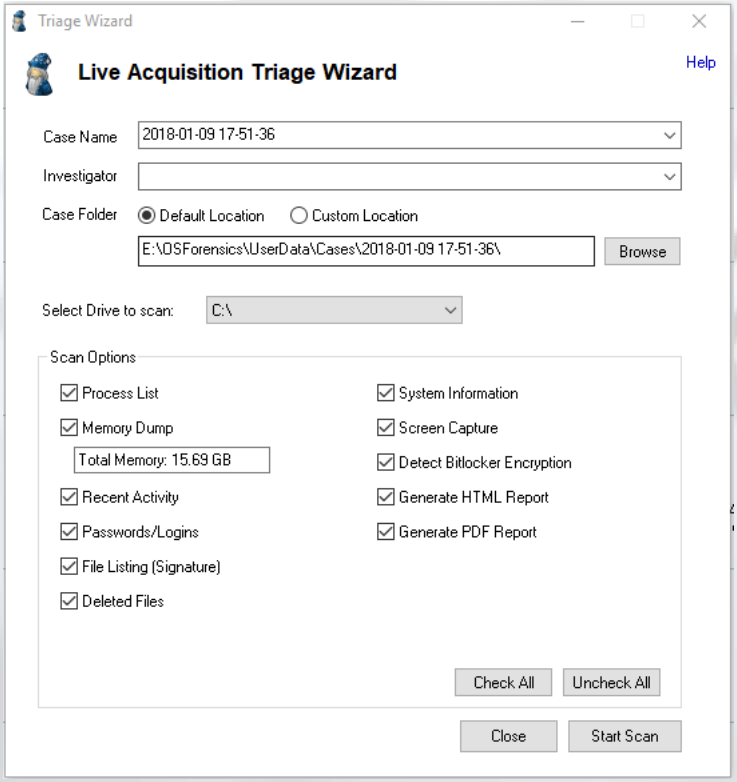
Using the "Triage Wizard"

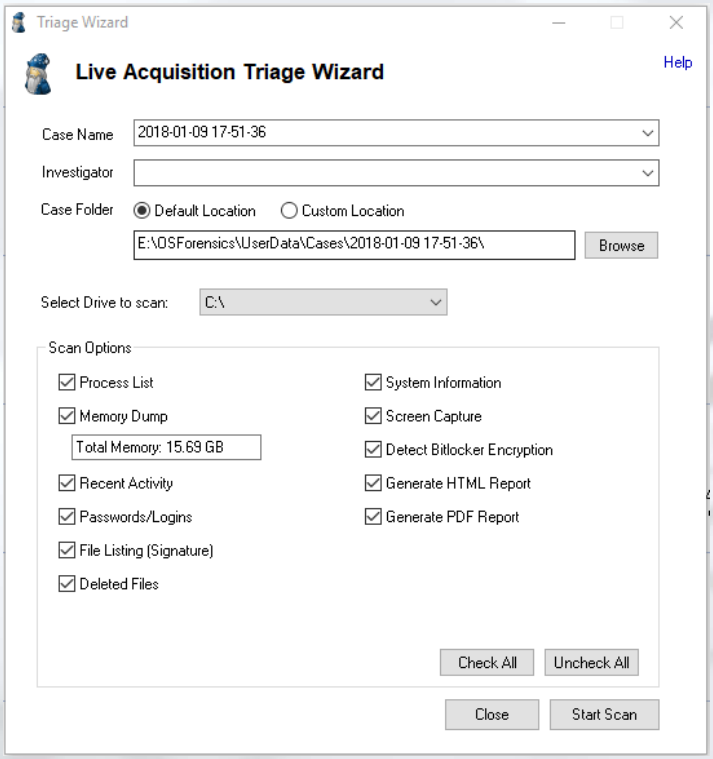
for live system analysis



Introduction…

Introduced in version 5 of OSForensics, the *Triage Wizard (TW*) provides users with a fully automated, simple solution for *Digital Evidence Triage (DET)*. The *TW* enables all levels of users to perform *DET* with incredible speed and ease of use.

What exactly is Digital Evidence Triage (DET)? - The purpose of *DET* is to quickly locate, identify and capture, (in a forensically-sound manner), basic system information, user activity, and other files and artifacts of interest from a digital media source.

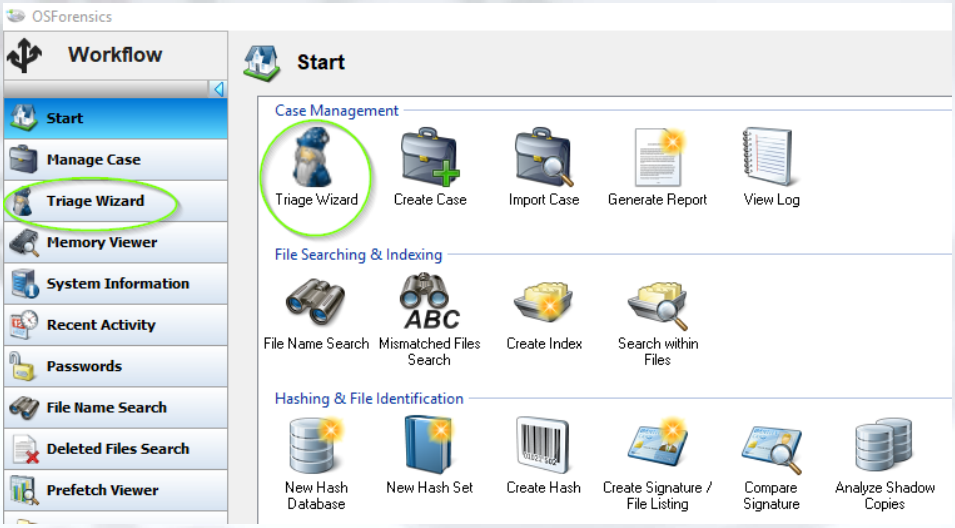


Though useful for all levels of users, the *TW* was designed for first responders and other "entry-level" users of OSForensics who may lack traditional forensic training and/or experience in digital evidence collection and processing. This means that non-forensic personnel can now acquire much of the same evidence traditionally recovered from a full forensic examination, in a matter of minutes and with a single click of the mouse.

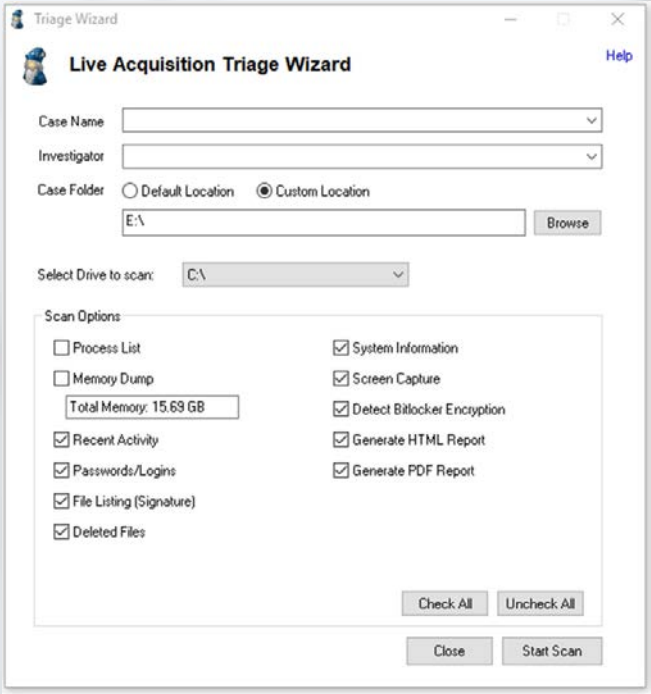
In addition to recovering files and artifacts of interest, the *TW* will also automatically generate an initial case report in HTML and/or PDF formats. These reports, and all other associated case files, are automatically saved to the case directory on the OSForensics USB device by default. Users can acquire a list of all running processes, create a Memory Image (a.k.a. "RAM Dump"), collect all web and user activity, passwords, user accounts, deleted files, system information , detect the presence of BitLocker Encryption and more. The *TW* will also capture a screenshot of the target system and create a searchable spreadsheet of all files on the file system, including file paths and date/time stamps.

The *TW* can literally be launched with a single click of the mouse. Collection times will vary, but typically take just a few minutes to complete if the "Memory Dump" option is not selected.

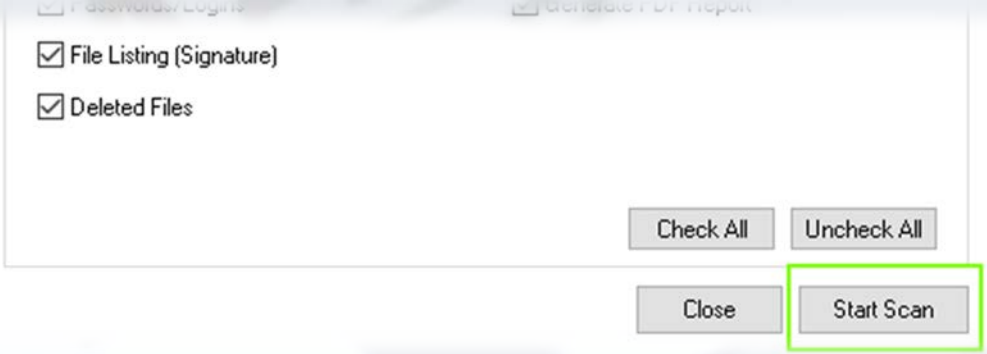
STEP 1. Launch the Triage Wizard - Open the OSForensics application and click the "Triage Wizard" icon located on the Start screen. You can also click the "Triage Wizard" module from the Workflow as shown below.



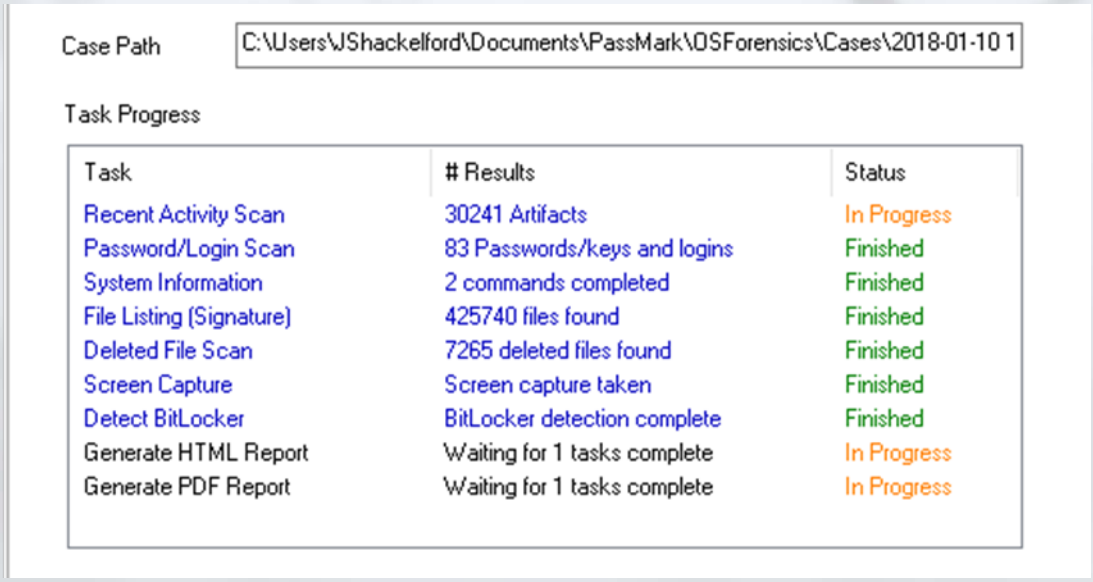
STEP 2. Review Default Settings - The Triage Wizard window will appear. Review the settings and make any necessary changes to the default settings prior to initiating the scan.



STEP 3. Start Scan – After confirming that the case folder location, drive, and scanning options are correct, simply click the "**Start Scan**" button to launch the Triage Wizard.

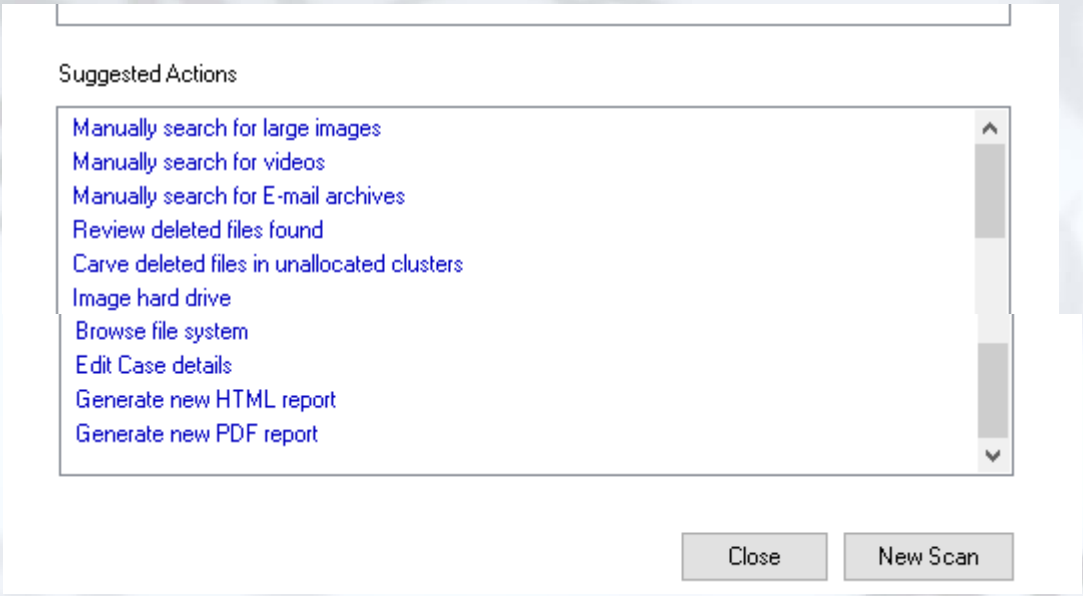


STEP 4. Review Results– You will see the status of each scan in real-time under the "Status" column. The process is complete when all scans show "Finished". To review results, simply click on the hyperlinks (in blue font) to review the data in the main OSForensics' interface.

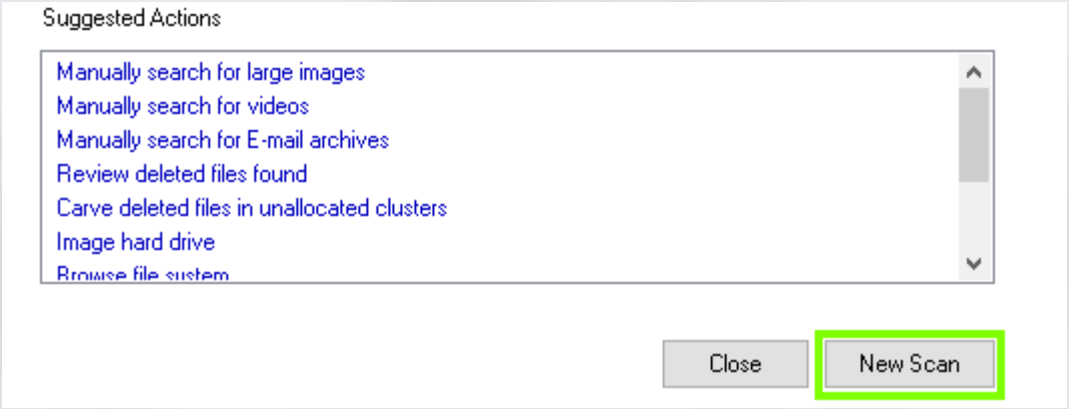


Task	# Results	Status
Recent Activity Scan	30241 Artifacts	In Progress
Password/Login Scan	83 Passwords/keys and logins	Finished
System Information	2 commands completed	Finished
File Listing (Signature)	425740 files found	Finished
Deleted File Scan	7265 deleted files found	Finished
Screen Capture	Screen capture taken	Finished
Detect BitLocker	BitLocker detection complete	Finished
Generate HTML Report	Waiting for 1 tasks complete	In Progress
Generate PDF Report	Waiting for 1 tasks complete	In Progress

STEP 5. Choose Additional Actions – In addition to generating a new report, users have the ability to perform additional actions after the initial TW scan. These additional actions can be seen in the image below.

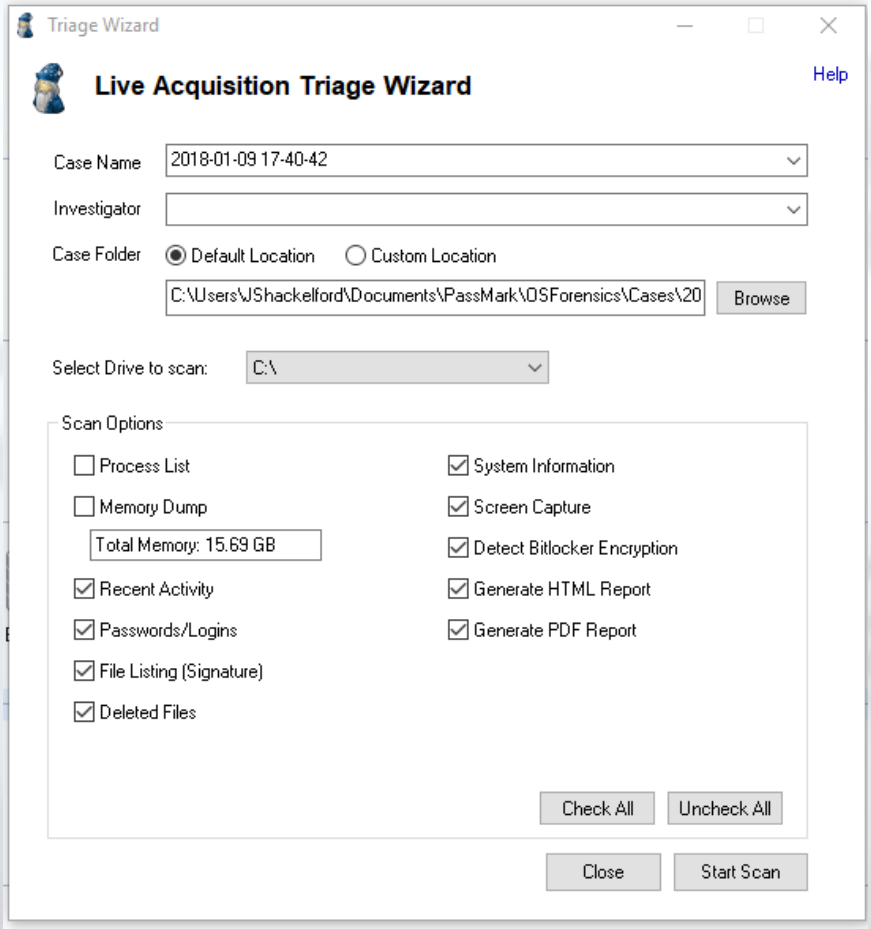


STEP 6. New Scan – Closing the *TW* window will not reset/delete the results. Only closing the OSForensics application or running a secondary scan will do this. This does NOT however, effect any generated reports. If you need to perform an additional scan either on the same drive, or a different one, you will simply choose the "New Scan" button as shown below and repeat steps 2-5.



Configurable Options…

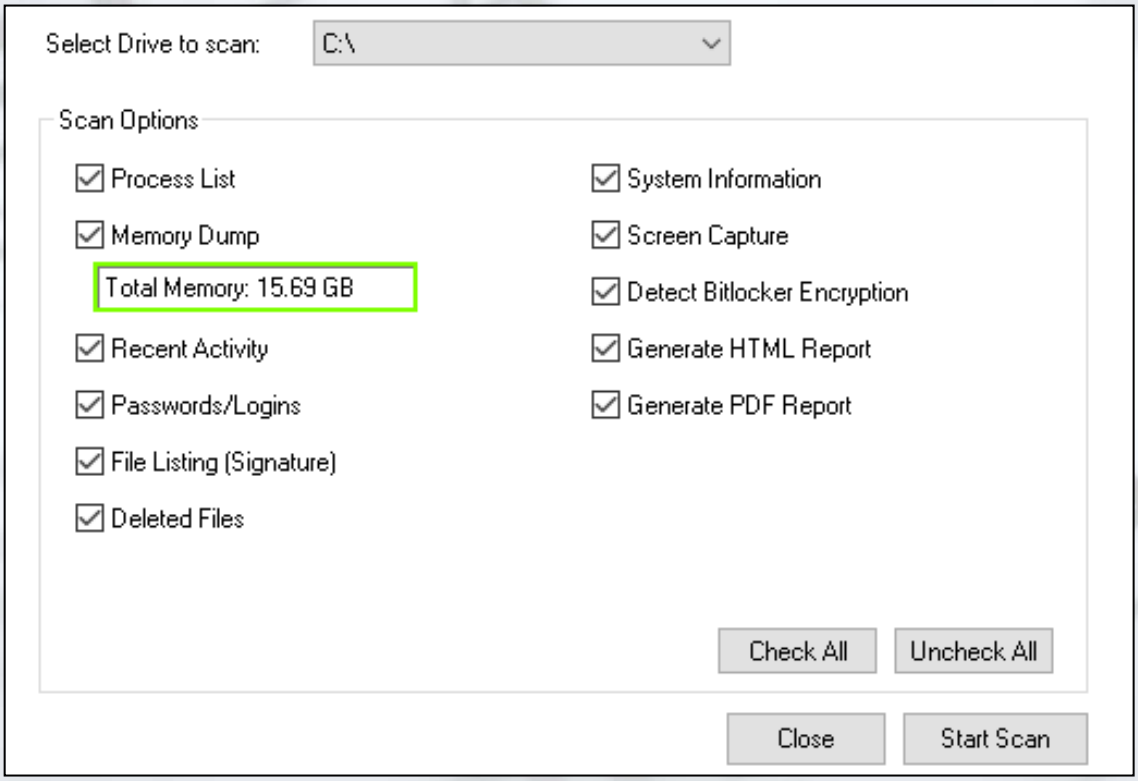
A case name will automatically be assigned, but can be changed by the user. The default naming convention uses the current date/time of the system clock and is displayed as **{YEAR–MONTH–DAY HOUR–MINUTE–SECOND}.** The user can enter their name in the "Investigator" field and choose a custom location to store the case data, or choose to use the default setting.



The **C:** drive is set as the default drive, as it is most likely the Operating System drive and the drive you will find the majority of user activity and other artifacts of interest.

Configurable Options…

When running OSF from a USB, all options are check-marked by default. The *TW* will display the total amount of RAM memory* on the system prior to initiating the scan as show in the image below.



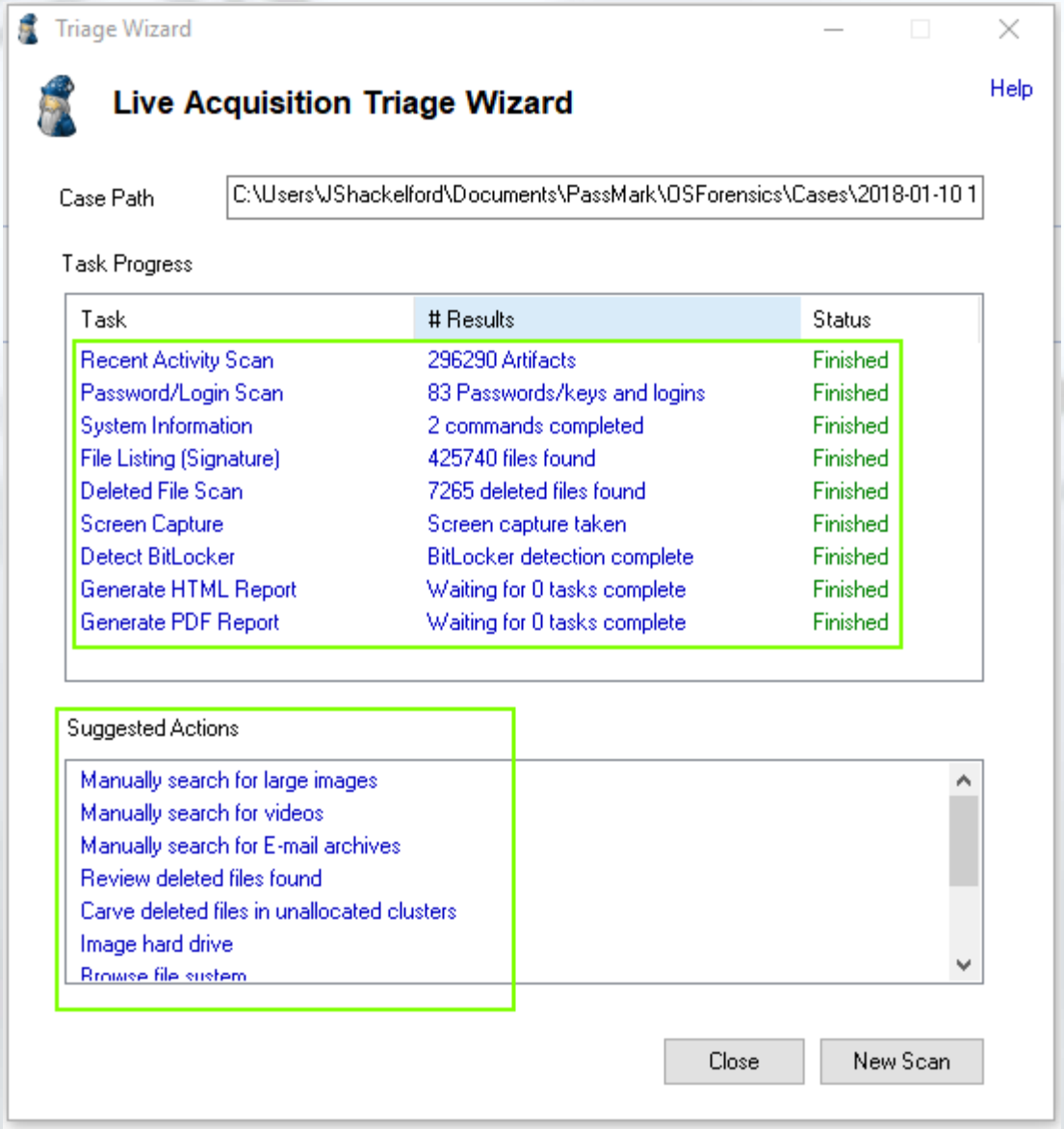
*Creating a full Memory Dump file can be a time-consuming process depending on several factors. The amount of RAM (e.g., Memory), in addition to the type of USB device and port being used, are the major contributing factors in determining how long this operation will take. If you do decide to collect a Memory Dump, please make sure you have sufficient space on your USB device as the dump file will be the same size as the total memory displayed. For example, a computer with 16GB's of RAM, would generate a 16GB Memory Dump file. It is highly advised to utilize USB 3.0 devices and ports when collecting a Memory Dump for optimal speeds.

Understanding the Scans

- **Process List** – Identifies and documents all running processes on the target computer.
- **Memory Dump** – Creates a binary image file of the entire contents of the RAM which can later be analyzed using OSForensics and/or with our free memory analysis tool, *Volatility Workbench*.
- **Recent Activity** – Recovers all user activity, such as accessed websites, USB drive history, event logs, registry artifacts, wireless networks, recent downloads, Peer-2-Peer activity and much more.
- **Passwords/Logins** – Recovers a wide variety of user account and password information, including online accounts and passwords, email accounts, Windows User account passwords, WiFi networks and passwords, and even Windows software product keys.
- **File Listing (Signature)** – Parses the file system and creates a .csv spreadsheet of every file on the drive, including the file path and date/time stamp metadata. The spreadsheet also includes the total number of files, total size of all files and more.
- **Deleted Files** – Performs a basic search for recently deleted files on the target disk. This scan does not perform advanced "file carving" operations which can be time consuming depending on the amount of free space on the drive. File carving can be performed after the completion of the initial scan. To perform file carving, simply select the "Carve Deleted Files from Unallocated Space" scan from the list of additional scans that are available.
- **System Information** – Identifies and documents all detailed information about the target computer including hard drive information, RAM and CPU data, OS info, time zone settings and much more.
- **Screen Capture** – Creates a screen capture image of the target computer (excluding the OSForensics app) to document what was open or viewable on the monitor at the time of analysis.
- **Detect BitLocker Encryption** – Scans the computer system for any internal or external drives that are encrypted with BitLocker full-disk encryption.
- **Generate HTML Report** – Creates an automated HTML report in the case directory.
- **Generate PDF Report** - Creates an automated PDF report in the case directory.

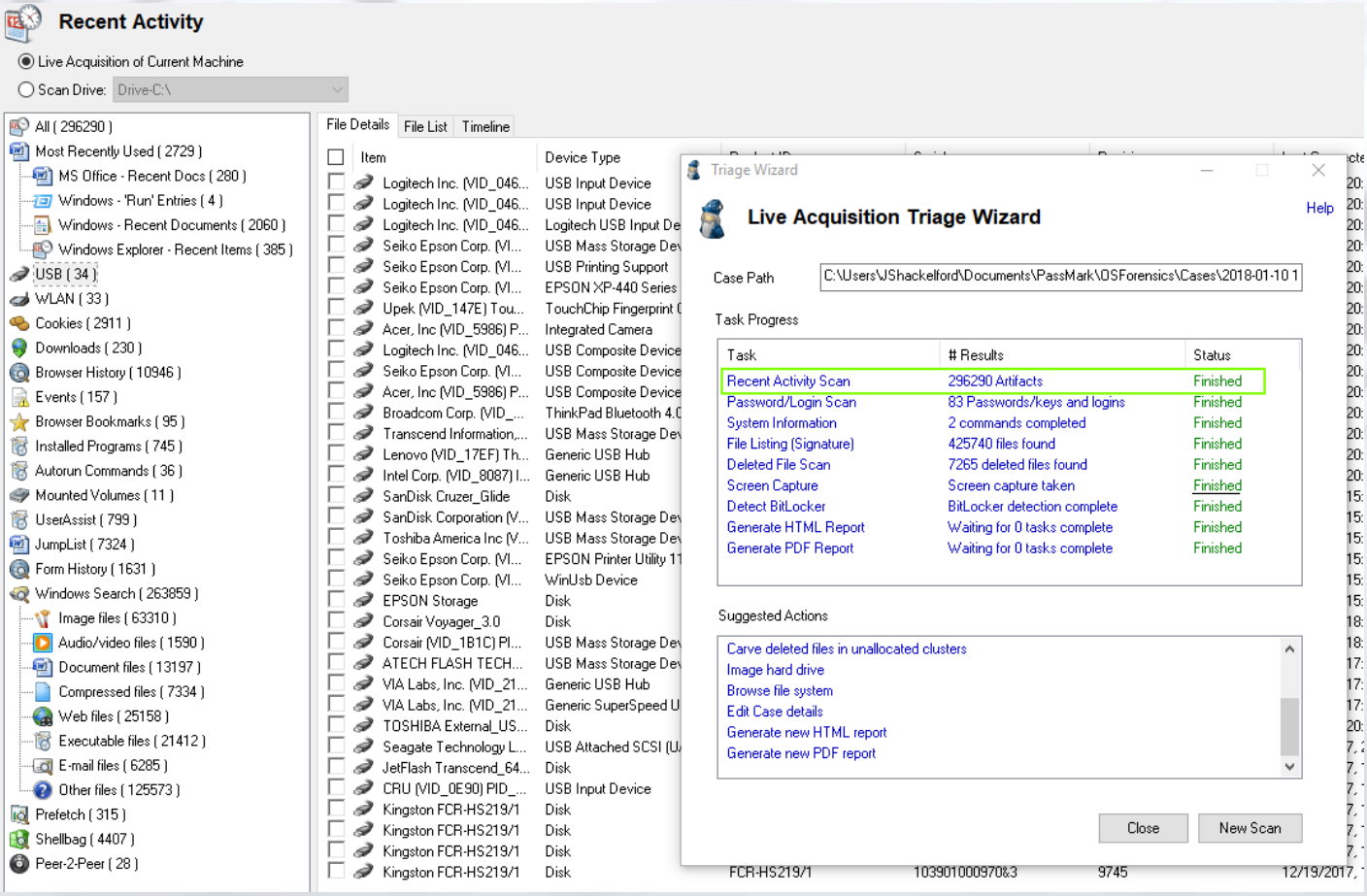
Reviewing Results…

Once completed, you can click on the various scans to review the results within the main OSForensics interface, or take further action by choosing from several additional options in the "Suggested Actions" window. If review will be conducted at a later date and time by viewing the generating reports, you can simply shutdown OSForensics and safely eject your USB device at this point.



Reviewing Results…

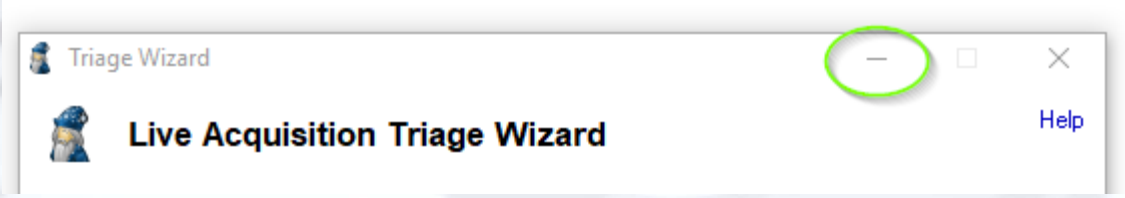
In the example displayed below, you can see that after the user clicked on the "Recent Activity Scan" in the *TW* window, the results are displayed in the main OSForensics' interface for review. Users can now review all results from the initial scan (e.g., Recent Activity, Passwords and User Accounts, System Information, Deleted Files, etc.) by clicking on the blue hyperlinks in the *TW* window.



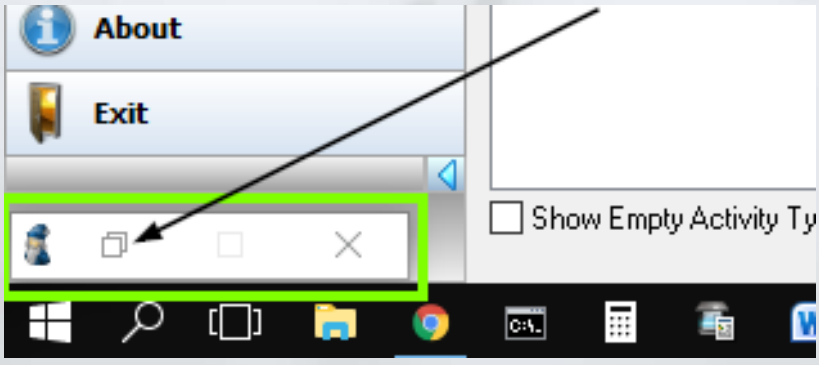
During review, users can add files of interest to the case through check-marking and right-click options, then generate a new report by clicking the "Generate new HTML/PDF report" option from the list of additional actions.

Reviewing Results…

On single-monitor systems, you may wish to minimize the *TW* window while reviewing results. To minimize, simply click the Minimize button on the window as shown below. (Clicking outside of the TW window will not minimize it.)



To restore the window, simply locate the minimized window in the lower left-hand corner of the screen and select the Maximize button and displayed below.



Useful Links…

To download a 30-DAY TRIAL of OSForensics, please visit us at:
https://www.osforensics.com/download.html

You can download the OSForensics USER MANUAL for FREE at:
https://www.osforensics.com/downloads/OSF_help.pdf

For TRAINING & CERTIFICATION, please visit:
https://www.osforensics.com/training.html

For FAQs and TUTORIALS, please visit:
https://www.osforensics.com/faqs-and-tutorials/faqs.html

You can access VIDEO DEMONSTRATIONS at:
https://www.osforensics.com/faqs-and-tutorials/video_demonstrations.html

Register for our FREE USER FORUM at:
https://www.passmark.com/forum/index.php

To request a SALES QUOTE, please fill out a short form at:
https://www.osforensics.com/quote.html

Or send an email request to:
sales@passmark.com

For GENERAL INQUIRIES, please contact us at:
info@passmark.com

PASSMARK SOFTWARE