bmm testlabs

bmm signatures v2.0
user manual

Contents

Introduction to BMM Signatures

BMM Signatures was created to provide a tool for the verification of gaming software. The application can be used to generate signatures for folders, individual files, and groups of files. It also has support to generate a signature for full media and partitions on devices such as Compact Flash cards, hard disk drives, or solid state drives. BMM Signatures can also use the Gaming Standards Association's (GSA) Game Authentication Terminal (GAT) protocol.

BMM Signatures is available for download or on a USB Flash Drive by contacting your local BMM office. The application will need to be installed on a computer. If the computer running the application has access to the internet, it will be able to auto update.

BMM Signature Program Features

BMM Signatures supports the following hashing algorithms:

- SHA-1
- CRC16
- MD5
- SHA-256
- CRC32
- CHECKSUM
- SHA-512
- HMAC SHA1
  (Seeded with a string or hex value)

System Requirements

BMM Signatures v2.0 supports the following desktop operating systems: Windows Vista, Windows 7, and Windows 8. BMM Signatures also supports the following server operating systems: Windows Server 2003, Windows Server 2008, and Windows Server 2012.

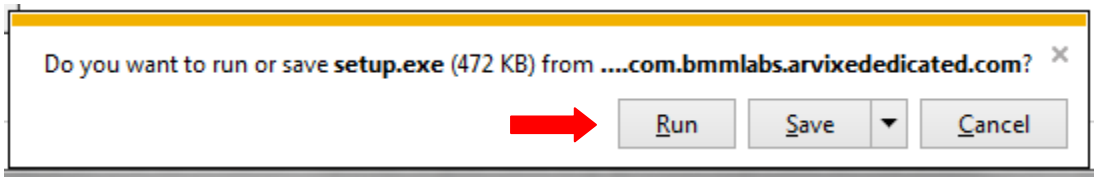
Recommended Minimum Hardware Requirements:

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 4 gigabyte (GB) RAM
- Graphics card with a screen resolution of 1680x1050
- USB Port
- Serial Port (or USB to serial adaptor) for GAT

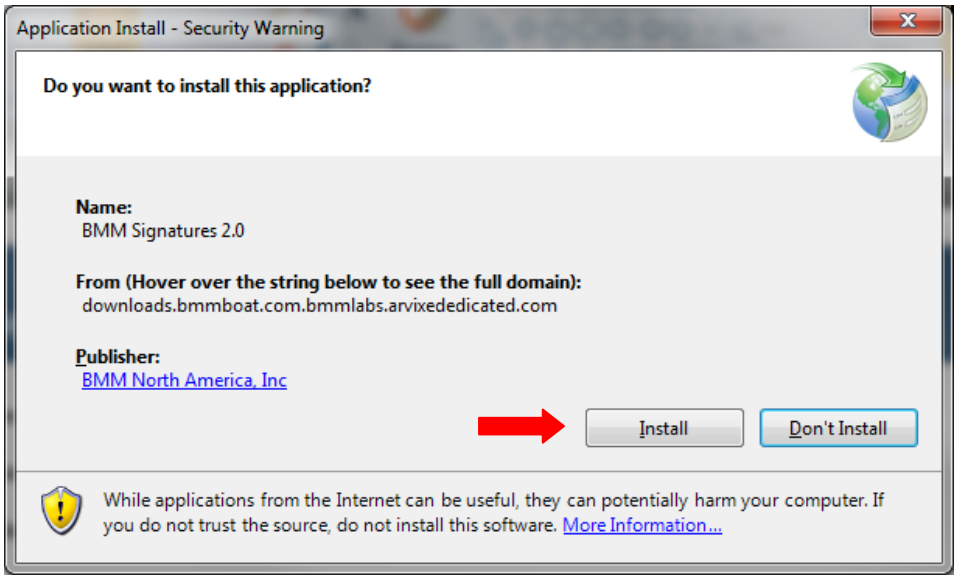
Installing BMM Signatures

1. Point a web browser to this address: http://downloads.bmmboat.com.bmmlabs.arvixededicated.com.
2. Click the Install button at the bottom of the webpage.

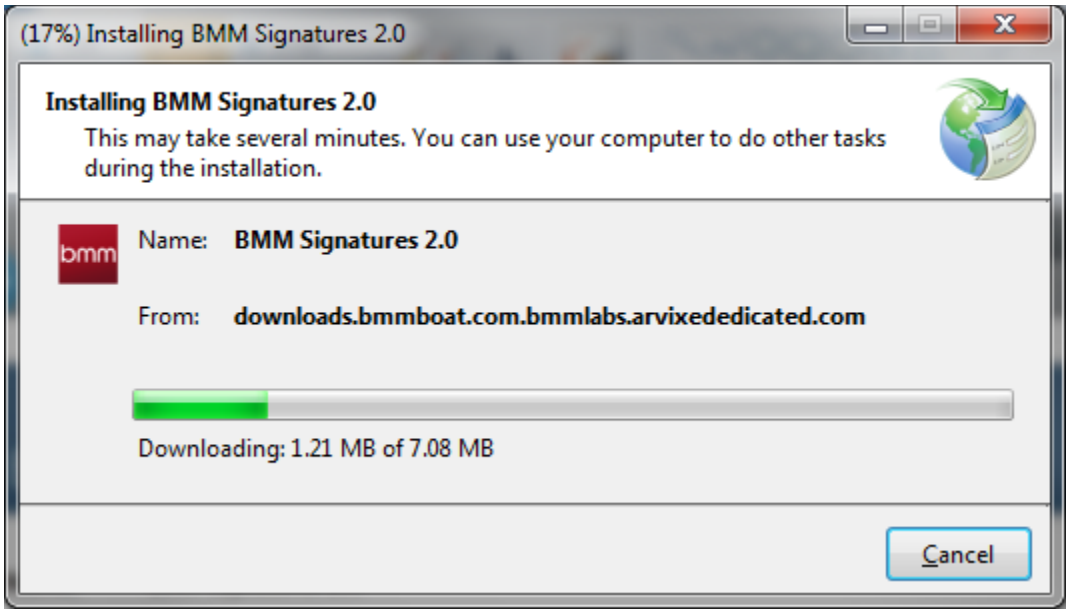
3. Click “Run” from the confirmation dialog.



4. Click install on the “Application Install – Security Warning”



5. BMM Signatures will download.

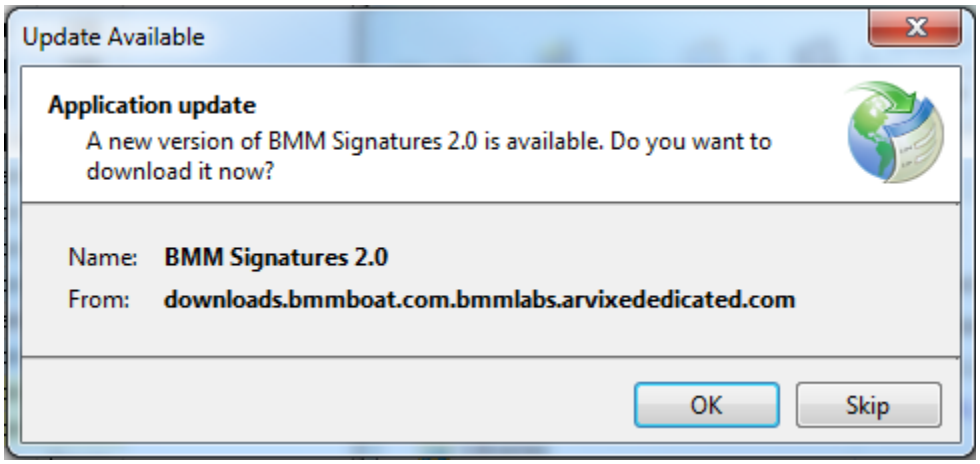


6. Click “Yes” on the security warning dialog, and BMM Signatures will run. BMM Signatures requires Administrator Privileges in order to perform verification on full media signatures on drives and partitions.

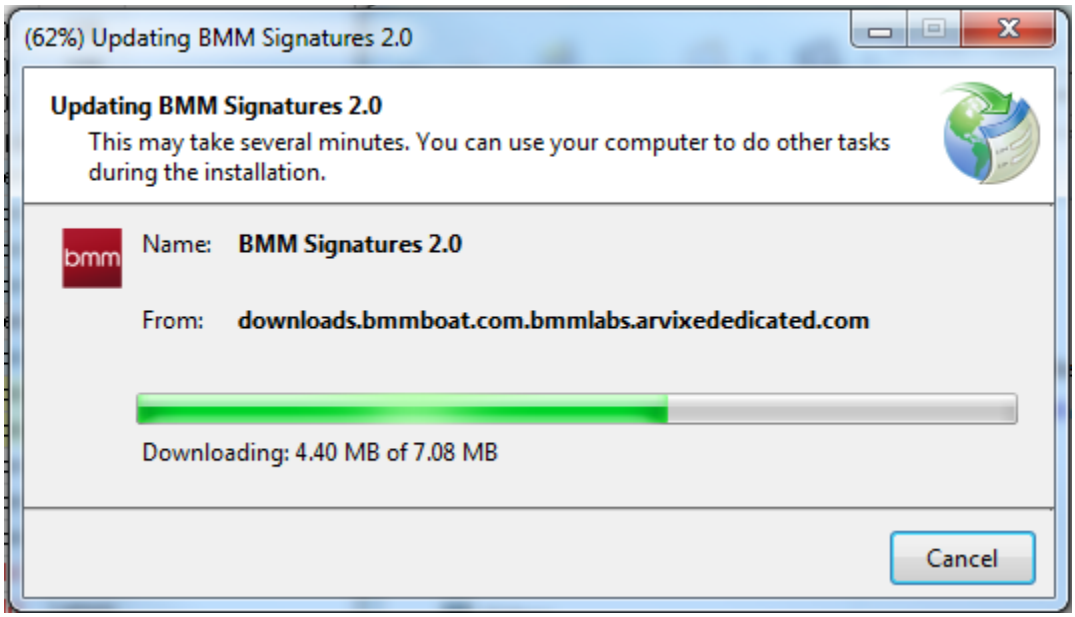
Running BMM Signatures

1. Double click on the BMM Signatures v2.0 icon on the desktop.

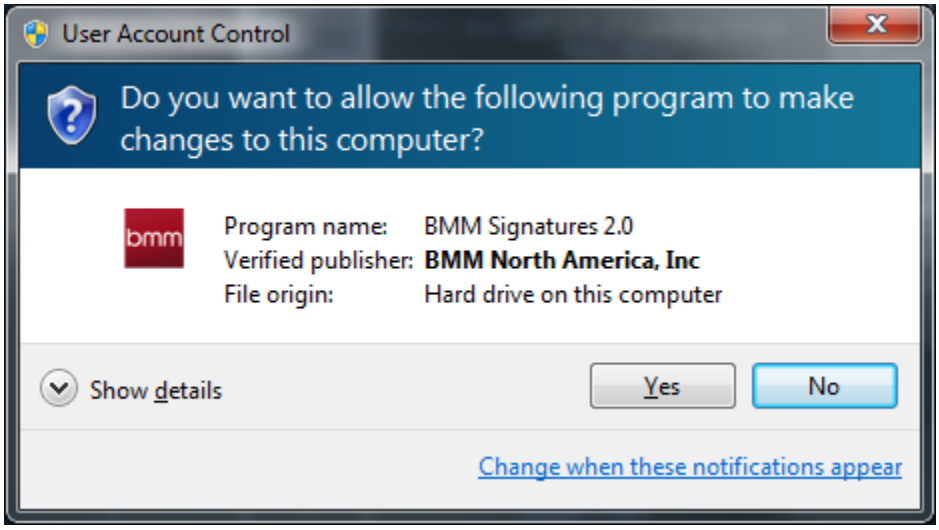
2. If an update is available, a dialog will open, click “OK” on the dialog.



3. BMM Signatures will update and then automatically run.



4. Click “yes” on the User Account Warning dialog. BMM Signatures need administrator access in order to perform media signatures.



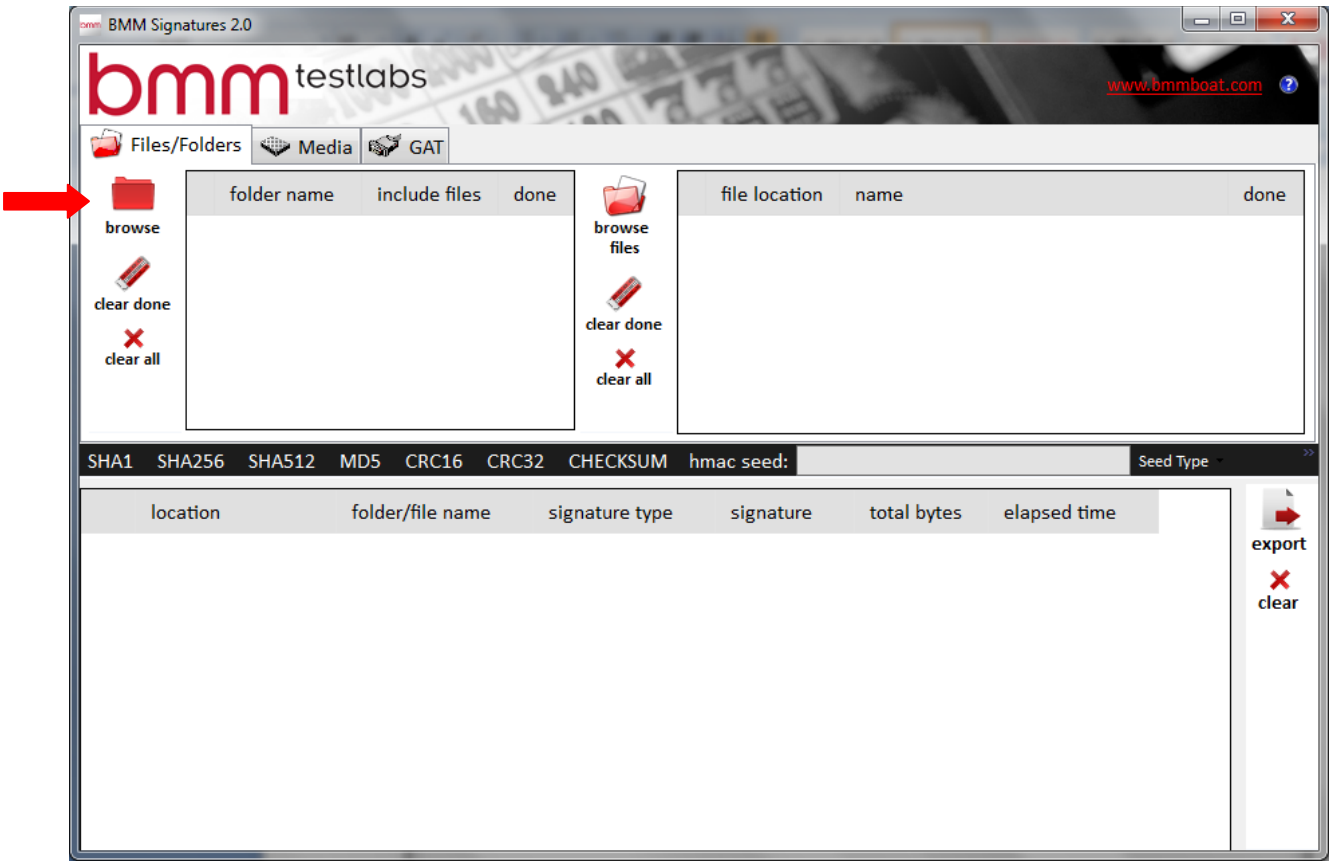
How to use BMM Signatures

Generating a Folder Signature

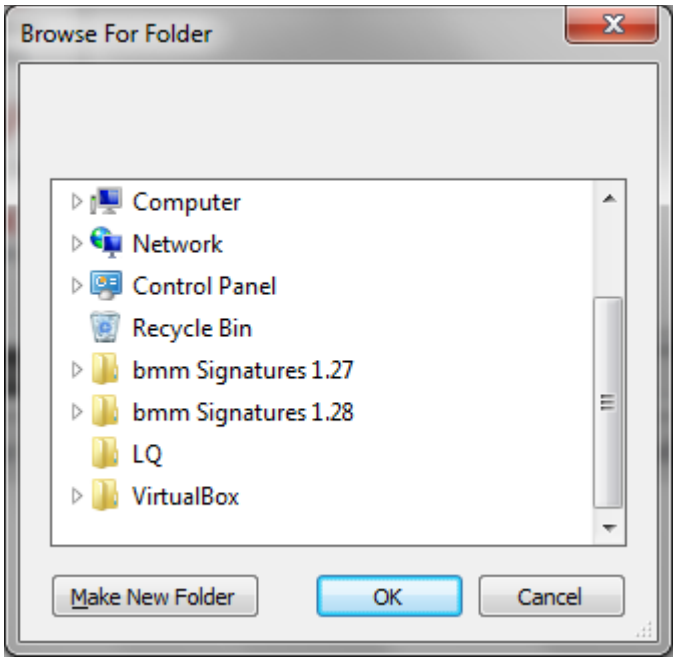
A Folder Signature is a single signature of the entire contents of a folder which includes all files and subfolders therein. The Folder Signature will change if the folders, subfolders or files within change by renaming, moving, or modifying.

Steps:

1. With BMM Signatures open and the “Files / Folders” tab selected, click on the “Browse” button.

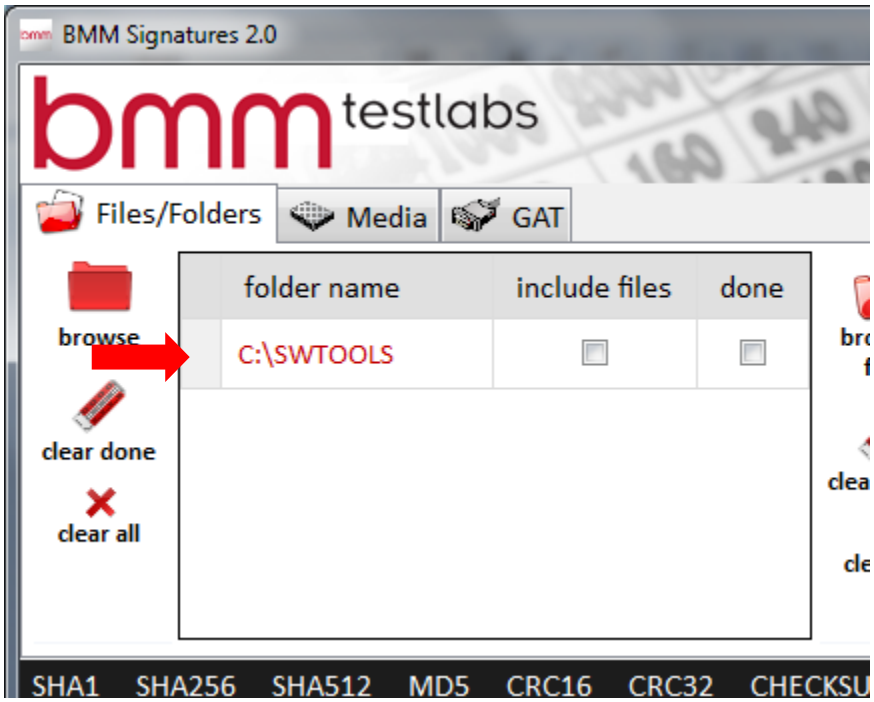


A dialog box labeled “Browse For Folder” will appear:

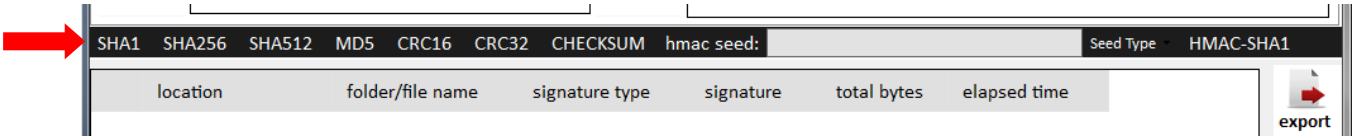


2. Navigate to the folder being used for verification.
3. Once selected, click on the “OK” button.

This action will insert the folder into the list. If the files contained inside the folder need to have individual signatures generated as well, click on the checkbox for “include files”. This will put the contents of the folder into the files list to the right.

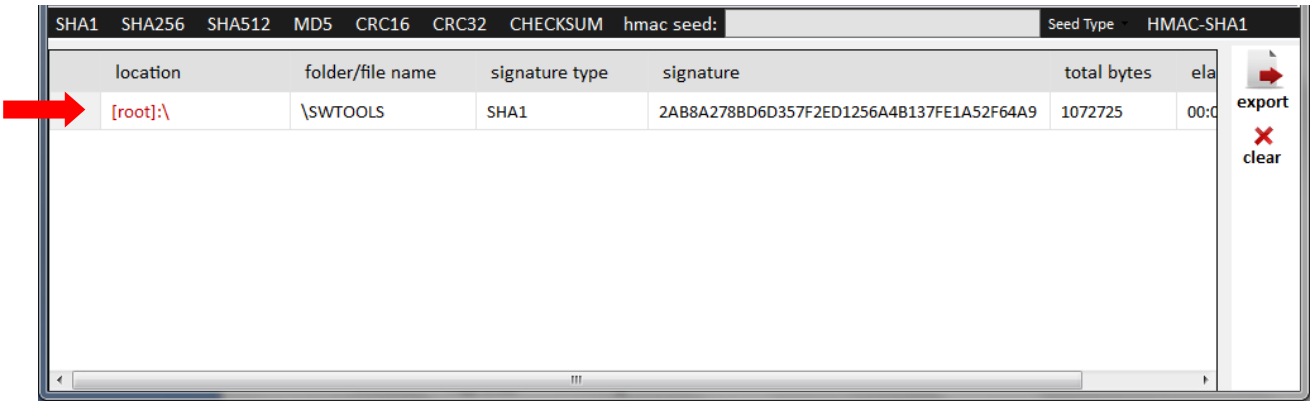


4. Next, click the type of signature to generate. Typically a SHA1 is used; however BMM Signatures can use other algorithms as well. When needing a HMAC-SHA1 signature, BMM Signatures allows for the entry of a seed. The seed can be in the form of a text string (characters a-z & numbers 1-0), or a hexadecimal string (characters a-f & numbers 1-0). To calculate more than one signature for a folder, click on the first signature type, next click on “clear done”, and then click on the next signature type. Repeat for each signature type needed.



5. In the bottom pane a list of the folders and their signatures will be displayed.

Note: Signatures shown here are for informational purposes only and are not to be used for verification.



Once a signature is generated for the folder, the checkbox in the done column will be checked. If the signatures need to be calculated again, uncheck the checkbox in the done column or click the “clear done” button to the left of the folder list.

To save or export the signatures calculated; please see the section on exporting results.

The following buttons are used with folder signatures:

The browse button brings up a dialog for the operator to select a folder to generate a signature from.

Once signatures for a folder have been generated, there will be a checkmark in the done column for that folder. This button will clear any done checkmarks so those signatures can be generated again.

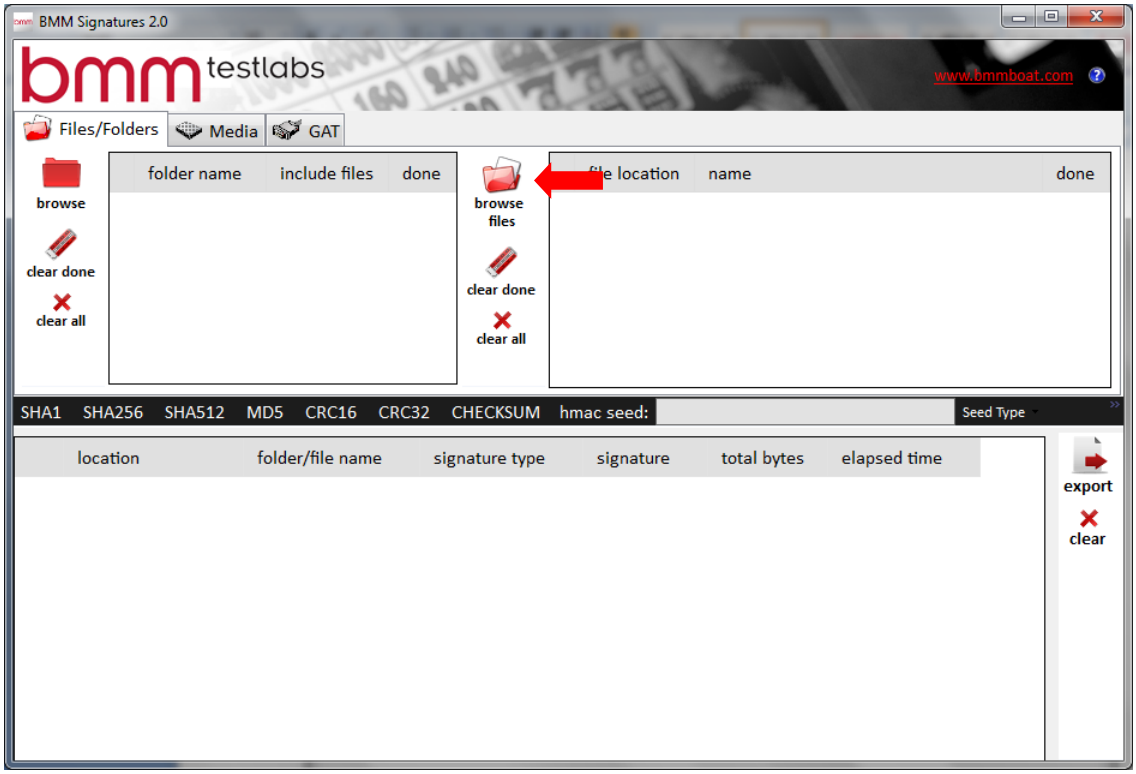
The clear all button will remove all items from the folder list.

Generating Individual File Signatures

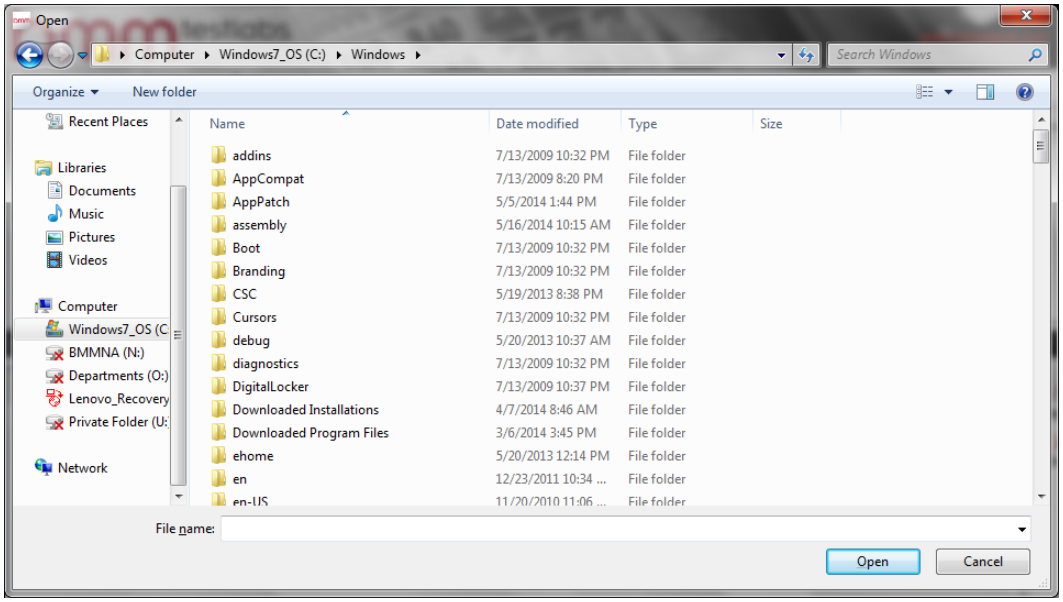
The Individual File Signature is used for generating single or multiple signatures for individual files.

Steps:

1. With BMM Signatures open and the “Files / Folders” tab selected, click on the “browse files” button.

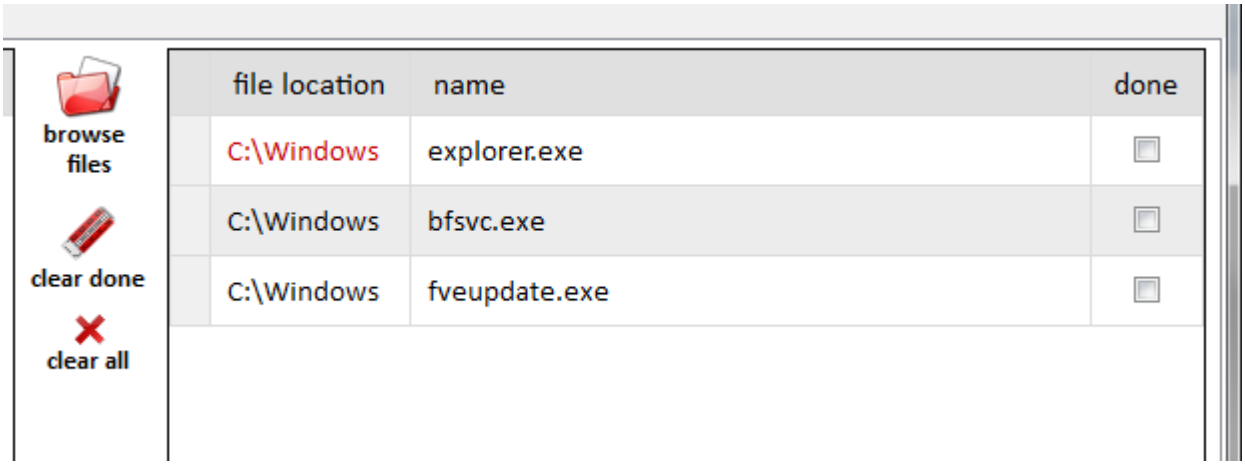


2. A dialog box labeled “Open” will appear.

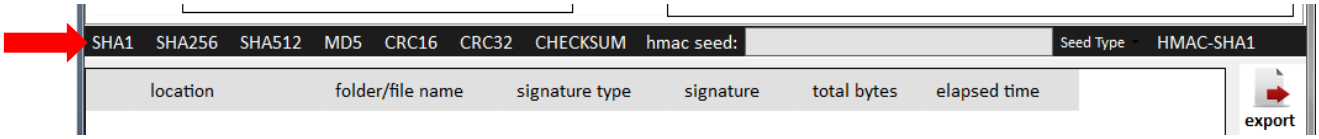


3. Navigate to the file(s) needed for verification.

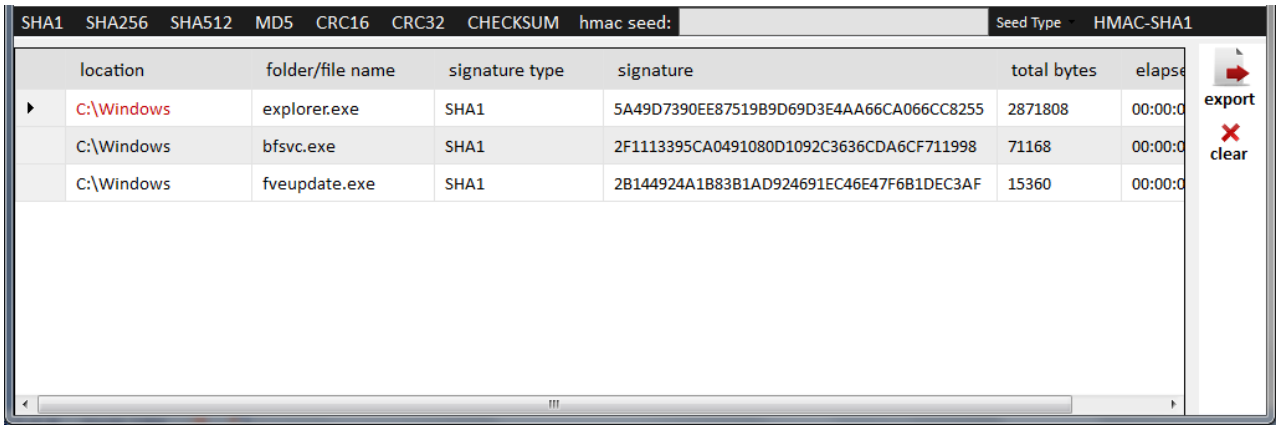
4. Once the file is selected, single click on the “Open” button. Note: Multiple files can be selected for multiple individual signatures to be generated. This action will insert the file(s) into the list for verification.



5. Next, click the type of signature to generate. Typically a SHA1 is used; however BMM Signatures can use other algorithms as well. When needing a HMAC-SHA1 signature, BMM Signatures allows for the entry of a seed. The seed can be in the form of a text string (characters a-z & numbers 1-0), or a hexadecimal string (characters a-f & numbers 1-0). To calculate more than one signature for a file, click on the first signature type, next click on “clear done”, and then click on the next signature type. Repeat for each signature type needed.



6. This will generate a signature of the file(s) selected. Note: Signatures shown here are for informational purposes only are not to be used for verification.



Once a signature is generated for the file(s), the checkbox in the done column will be checked. If the signatures need to be calculated again, uncheck the checkbox in the done column or click the “clear done” button to the left of the file list.

To save or export the signatures calculated; please see the section on exporting results.

The following buttons are used with individual file signatures:

The browse files button brings up a dialog for the operator to select one or more files to generate signatures for.

Just like the clear done button next to the list of folders, the clear done button next to files will remove the done checkmarks next to any files to the signatures for those files can be generated again.

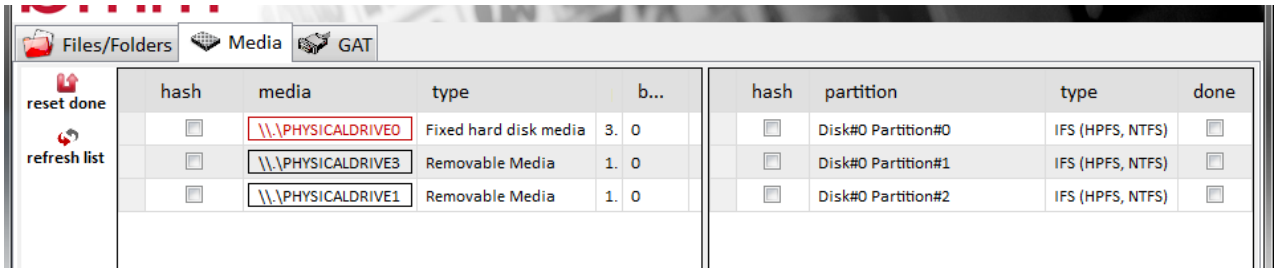
Just like the clear all button next to the list of folders, the clear all button next to the list of files will remove all files from the list.

Generating a Full Media Signature

A Full Media Signature is used for generating a single signature of the entire contents of a storage device (e.g. compact flash card, CD, DVD, etc.). This feature can be used on any media that can be connected to a computer and recognized as a drive. This feature cannot be used on EPROMs or other similar devices. Generating media signatures requires administrator privileges to the computer.

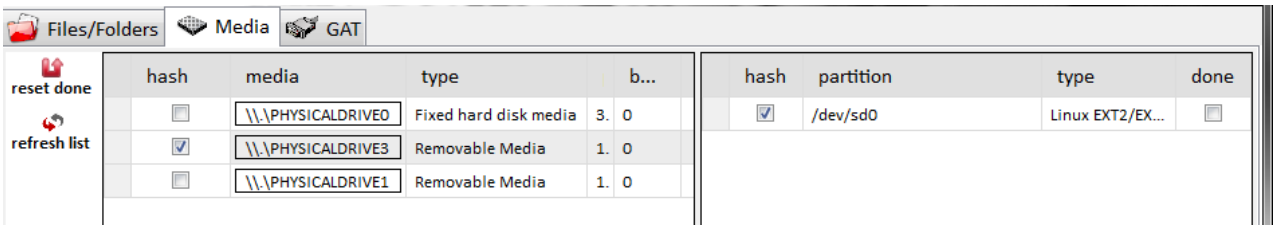
Steps:

1. With BMM Signatures open and the “Media” tab selected, single click on the drive that needs to be validated, or the drive containing the partition that needs to be validated.

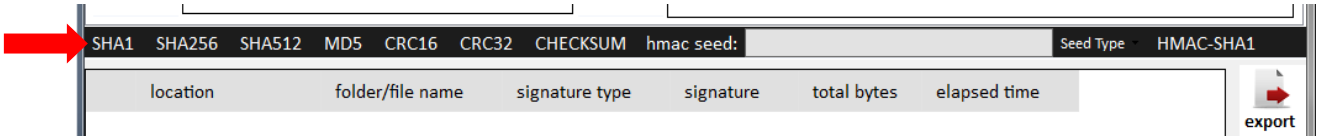


2. If the whole drive is being validated, check the “hash” box next to the drive.

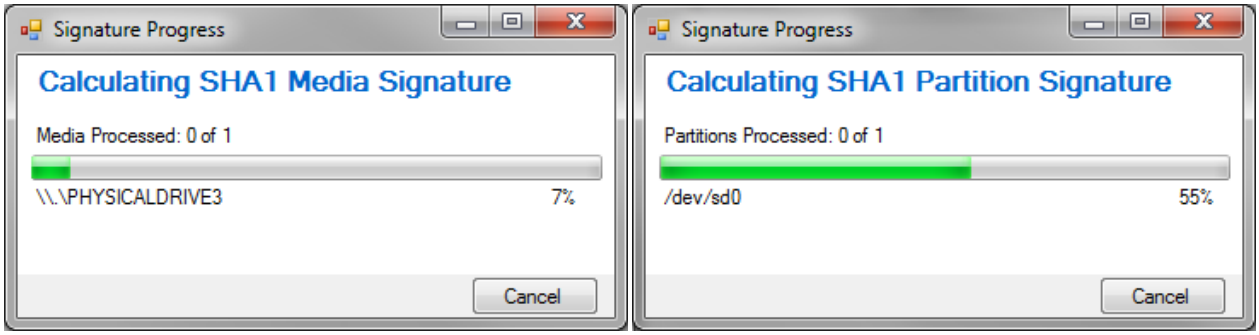
3. If one or more partitions are going to be validated, click the “hash” box next to each partition. The overall drive “hash” box may also be checked to include that in the signature calculation process.



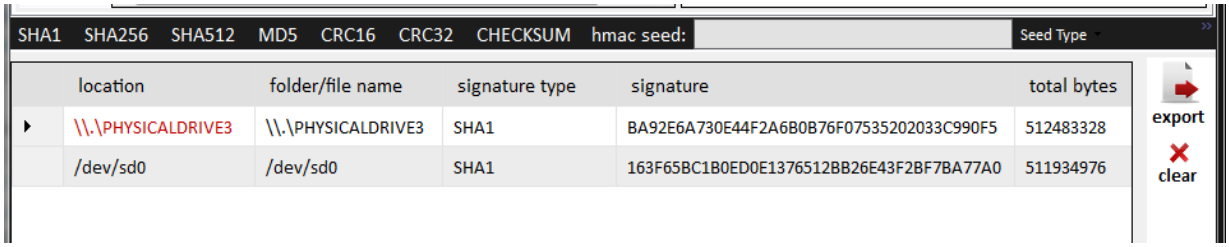
4. Once all of the drives and/or partitions are selected, click on the signature that needs to be generated. Typically a SHA1 is used; however BMM Signatures can use other algorithms as well. When needing a HMAC-SHA1 signature, BMM Signatures allows for the entry of a seed. The seed can be in the form of a text string (characters a-z & numbers 1-0), or a hexadecimal string (characters a-f & numbers 1-0). To calculate more than one signature for a folder, click on the first signature type, next click on “clear done”, and then click on the next signature type. Repeat for each signature type needed.



5. One or more dialogs will appear to show the current process for the partitions and/or whole media.



6. When the process is complete, the results will show in the bottom pane.



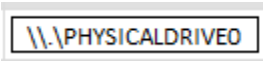
Once a signature is generated for the drives and/or partitions, the checkbox in the done column will be checked. If the signatures need to be calculated again, uncheck the checkbox in the done column or click the “reset done” button to the left of the drive list.

To save or export the signatures calculated; please see the section on exporting results.

The following buttons are used with media signatures:

The reset done button will clear the done checkmarks for physical drives and media which have had signatures generated.

The refresh list button will refresh the list of available physical drives and media for selection to generate signatures for. If you start BMM Signatures and then attach a CF card, the operator can click this button to refresh the list to show the CF card as available for signature calculation.



Each physical drive in the list is a button. When the button is clicked, all of the available partitions are shown in the partition list to the right of physical drive list.

Game Authentication Terminal (GAT)

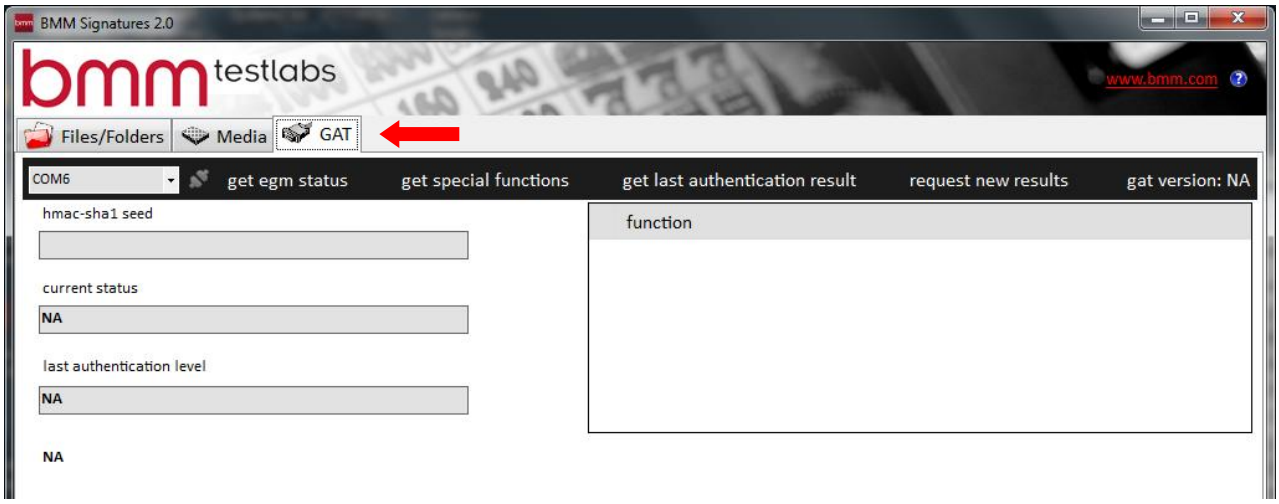
A Game Authentication Terminal or GAT signature makes a request to the gaming device's CPU to calculate the hash of the various program storage media on the gaming device. This is accomplished by connecting the computer running the BMM Signatures to the gaming device via a serial cable to a specific port on the gaming device. Once the computer is connected and communications established, the user can specify a seed value, and instruct the gaming device to calculate the HMAC-SHA1.

Steps:

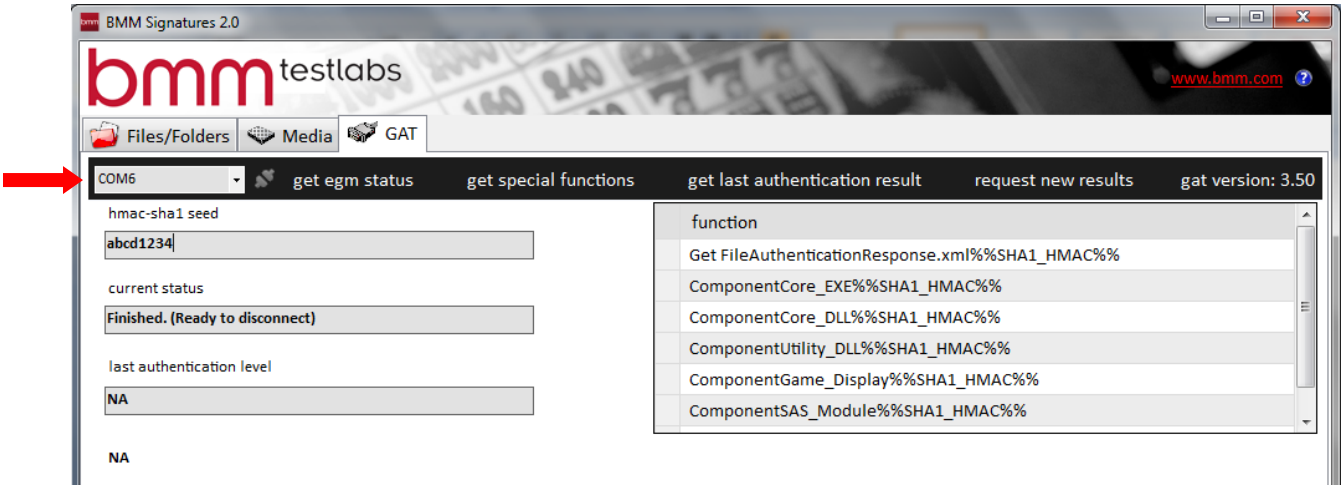
1. Open the main door of the gaming device's cabinet.
2. Locate the connector that is used for GAT communications. Please see the documentation for the gaming device or contact BMM Testlabs for assistance if the connector is unknown.

3. Double-click on the BMM Signatures 2.0 icon on the computer desktop.

4. Select the GAT tab from the UI



5. Select the COM port from the drop down box and the program will automatically connect to the game.



6. If needed, or desired, enter a value for the seed that will be communicated to the gaming device.

7. For a quick method to use the entered seed value and have the game calculate signatures for all components, click on the “request new results” button. For more control on what gets verified, continue with the next steps, otherwise proceed to step 10.

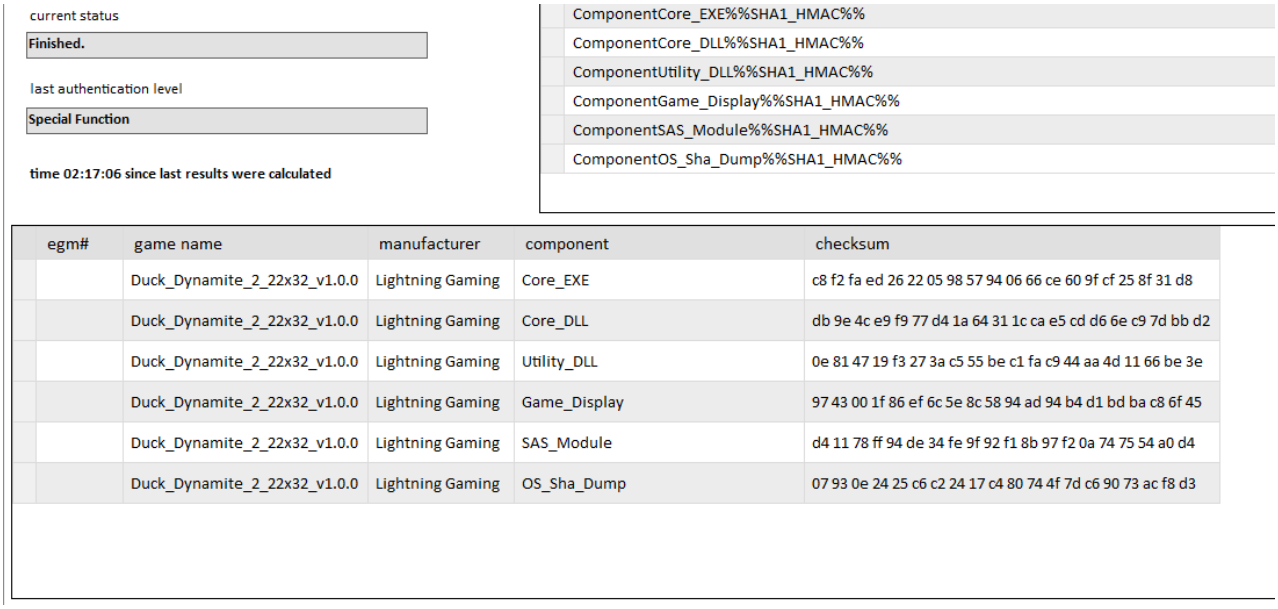
8. Click on the “get special functions” button to obtain a list of the components that the game can generate signatures for verification. Note: if any previous results are saved on the game, they will be erased.

9. From the Functions list, click on the item for verification.
   Note: Each gaming device may rename or change the position of the functions that will return the GAT signature response.

10. When the current status changes to “Calculating (Ready to Disconnect)” and the link button  lights up, press the button and the serial cable can be unplugged from the game, and connected to another game when checking a whole bank of games. When you reach back to the first game started, connect

the serial cable and click the “get egm status” button. If the current status says “Finished”, click on the “get last authentication result” button.

11. After clicking the “get last authentication result” button or if the serial cable was not disconnected, a list of the components and their signatures will appear in the bottom pane when the calculation is completed.



When performing GAT verifications, after each game returns the results of the authentication, the operator can enter the machine or asset ID into the “egm#” field in the results table. This will be saved with the results if exported. A very handy feature when checking a whole bank of games and verification analysis will be performed at a later time.

To save or export the signatures calculated; please see the section on exporting results.

The following buttons are used with GAT signatures:

get egm status The get egm status button queries the EGM for its current status.

get special functions The get special functions button will query the EGM for available components to generate a signature for. This button can cause the EGM to erase any currently stored and completed signatures.

get last authentication result The get last authentication result button will query the EGM for any currently stored and completed signatures that were previously requested.

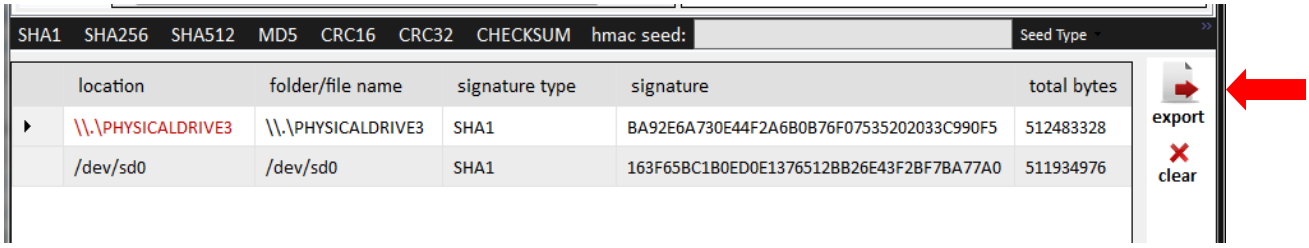
request new results The request new results is a quick shortcut to issue a request to the EGM to generate signatures for all components.

Exporting results from BMM Signatures

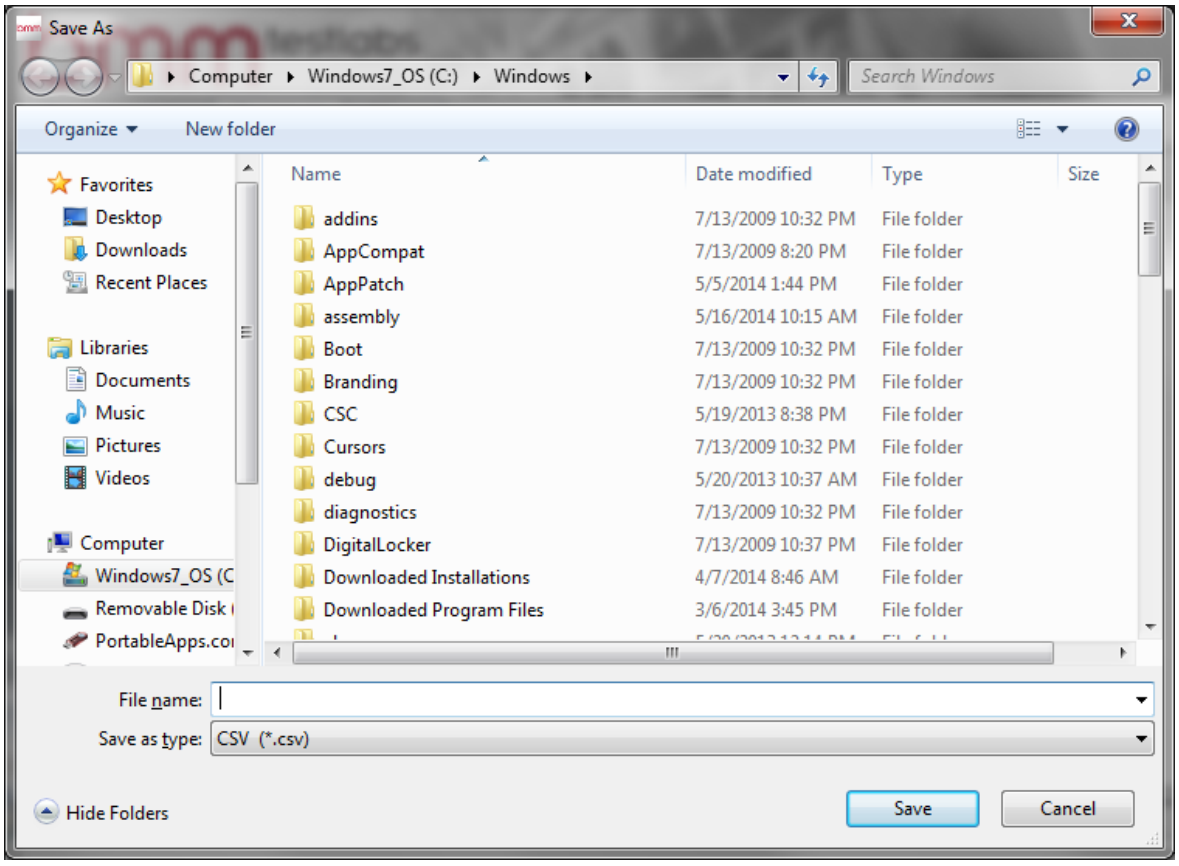
BMM Signatures can save or export the results accumulated in the bottom pane of the application, regardless of the type or combination of types of results. The exported results are saved to a comma separated values (CSV) file.

Steps:

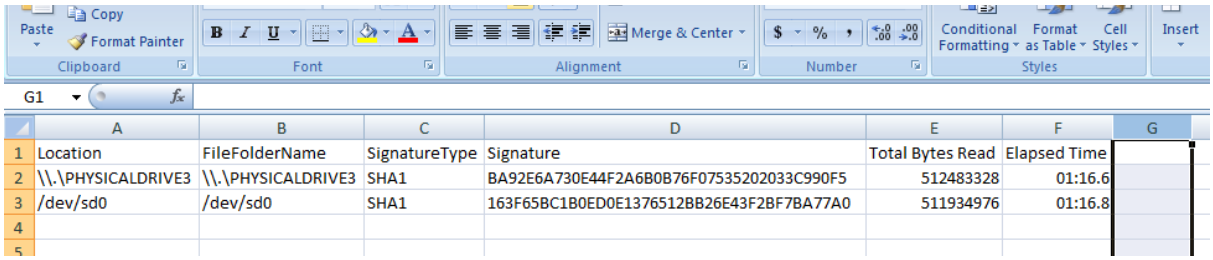
1. Click on the “export” button once a list of results is compiled.



2. A “Save As” dialog will open allowing the results to be saved in a convenient location with an operator specified name. The results will only save in a CSV format.



3. Once saved, the CSV file can be opened in either a text editor or in a spreadsheet program for easy manipulation to import into other databases or programs.



	A	B	C	D	E	F	G
1	Location	FileFolderName	SignatureType	Signature	Total Bytes Read	Elapsed Time	
2	\\.\PHYSICALDRIVE3	\\.\PHYSICALDRIVE3	SHA1	BA92E6A730E44F2A6B0B76F07535202033C990F5	512483328	01:16.6	
3	/dev/sd0	/dev/sd0	SHA1	163F65BC1B0ED0E1376512BB26E43F2BF7BA77A0	511934976	01:16.8	
4							
5							

The following buttons are used when exporting signatures:

export The export button will allow the operator to save the current results to a comma separated value (CSV) file. The filename that is selected will be overwritten if selected a second time. The CSV file is able to be opened in a spreadsheet program, such as Microsoft Excel, for further analysis after the signatures have been generated.

clear The clear button will remove all of the current results from the bottom results window. It will not reset the done checkmarks for folders or files.

Terms of Use

This application is only to be used with permission from BMM Testlabs. This application may not be redistributed without permission from BMM Testlabs.

This application will not work for every authentication situation. It is up to the user to decide if the situation is appropriate for using this application for authentication.

The Group Signature feature uses proprietary methods of generating signatures for a folder which are not shared by other applications. Use of the Group Signature feature results in creating signatures that are unique and different from similar tools.

The Partial Full Media feature is designed to allow the creation of a signature on a portion of the media and then verify the remaining portion of the media to insure that it contains only a specified HEX value. These signatures will not match when compared with another tool which generates a signature on the full media regardless of blank space.

THE LICENSED PROGRAM IS PROVIDED TO USERS ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LICENSED PROGRAM IS WITH THE USER. SHOULD THE LICENSED PROGRAM PROVE DEFECTIVE, THE USER ASSUMES THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.