FTK-IMAGER

AIM: To familiarize Bit level Forensic Analysis of evidential image

DESCRIPTION:

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has not been tampered with. Forensic Imaging is defined as the processes and tools used in copying an electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, every sector, partition, files, folders, master boot records, deleted files, and unallocated spaces. The image is an identical copy of all the drive structures and contents.

Further, a forensic image can be backed up and/or tested on without damaging the original copy or evidence.Also, you can create a forensic image from a running or dead machine. It is a literal snapshot in time that has integrity checking.

Need for a Forensic Image :

- In today's world of crime, many cases have been solved by using this technique, as evidence apart from what is available through an operating system, has been found using this technique, as incriminating data might have deleted to prevent discovery during the investigation. Unless that data is overwritten and deleted securely, it can be recovered.
- One of the advantages includes the prevention of the loss of critical files.

- When you suspect a custodian of deleting or altering files. A complete forensic image will, to a certain extent, allow you to recover deleted files. It can also potentially be used to identify files that have been renamed or hidden.
- When you expect that the scope of your investigation could increase at a later date. If you aren't sure about the scope of your project, ALWAYS OVER COLLECT. It's better to have too much data than not enough, and you can't get much more data than a forensic image.
- When you expect that you or someone in your organization may need to certify or testify to the forensic soundness of the collection. In most cases, this need will never arise, but will almost certainly come into play in any criminal or potential criminal proceedings.
- The Imaging of random access memory (RAM) can be enabled by using Live imaging. Live imaging can bypass most encryption.

FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

With FTK Imager, you can:

- Create forensic images or perfect copies of local hard drives, floppy and Zip disks, DVDs, folders, individual files, etc. without making changes to the original evidence.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs.
- You can also preview the contents of the forensic images that might be stored on a local machine or drive.
- You can also mount an image for a read-only view that will also allow you to view the contents of the forensic image exactly as the user saw it on the original drive.

- Export files and folders from forensic images.
- View and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.

Pros Of FTK Imager

- It has a simple user interface and advanced searching capabilities.
- FTK supports EFS decryption.
- It produces a case log file.
- It has significant bookmarking and salient reporting features.
- FTK Imager is free.

Cons Of FTK Imager

- FTK does not support scripting features.
- It does not have multitasking capabilities.
- There is no progress bar to estimate the time remaining.
- FTK does not have a timeline view.

PROCEDURE:

To create a forensic image with FTK imager, we will need the following:

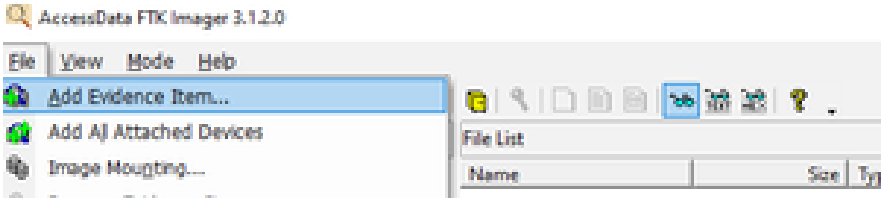
FTK Imager from Access Data, which can be downloaded using the following link: FTK Imager from Access DataA Hard Drive that you would like to create an image of.

Method :

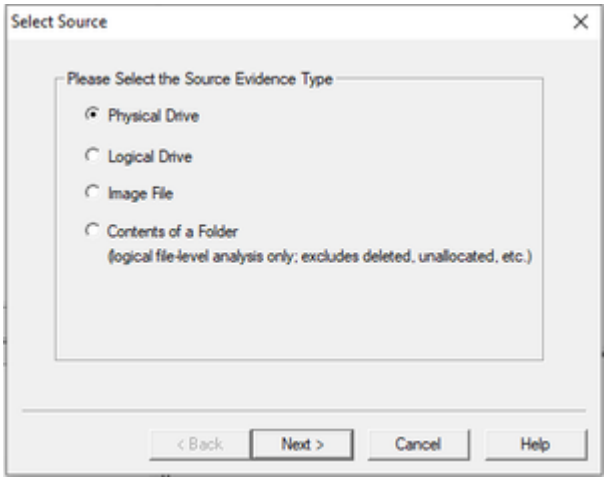
Step 1: Download and install the FTK imager on your machine.

Step 2: Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.

Step 3: In the menu navigation bar, you need to click on the *File* tab which will give you a drop-down, like given in the image below, just click on the first one that says, *Add Evidence Item*.



Step 4: After that, there will be a pop-up window that will ask you to Select the Source of the Evidence. If you have connected a physical hard drive to the laptop/computer you are using to make the forensic image, then you will select the Physical Drive here. Click on *Next.* Now, Select the *Physical Drive* that you would like to use. Please make sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your own OS drive.

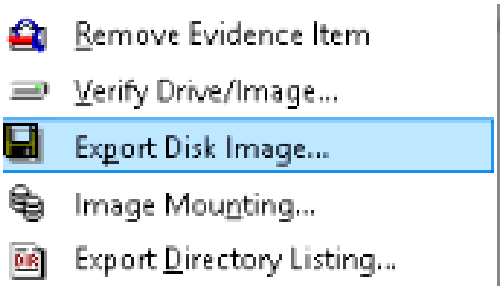


Step 5: Now, we will export the forensic images.

- Right-click on the Physical Drive that you would like to export in the FTK Imager window. Select *Export Disk Image* here.
- Click the *Add* button for the Image Destination.
- Select the Type of Forensic Image you would like to export. Select *E01* and Click *Next.*

- After that, you will have to enter information regarding the case now. You can either leave them blank or keep it general, this part is totally upon you.
- Next, you will need to Choose the Destination that you would like to export the forensic image and Name the Image.

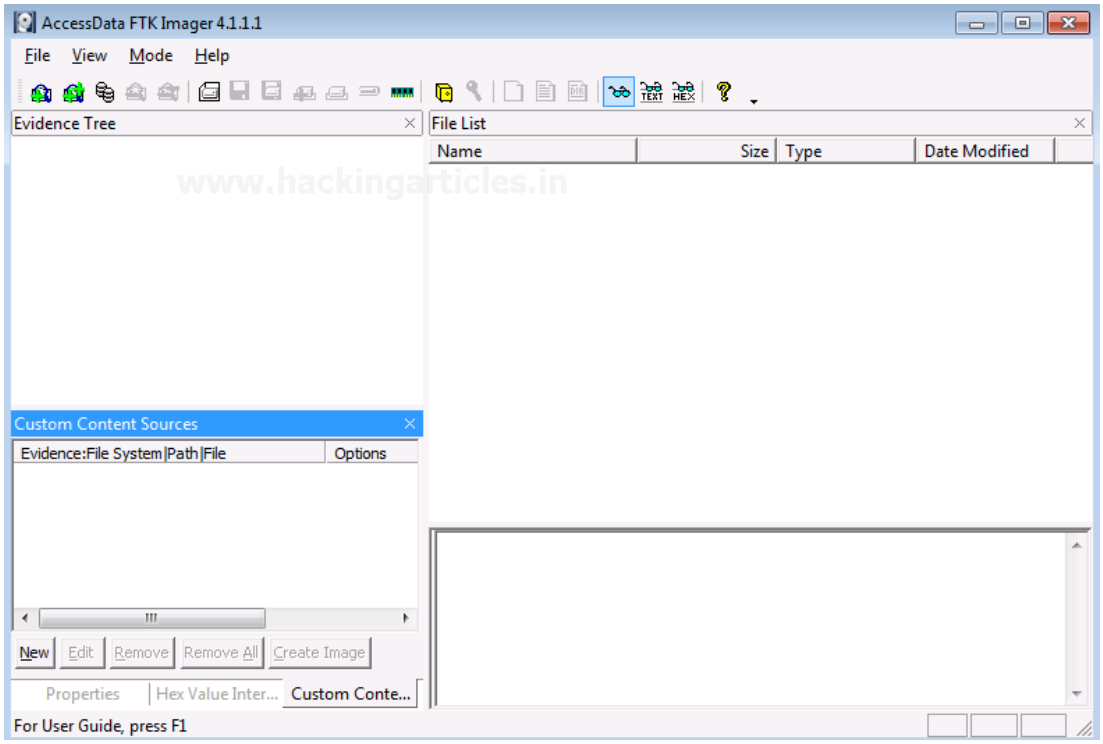
Lastly, you will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.



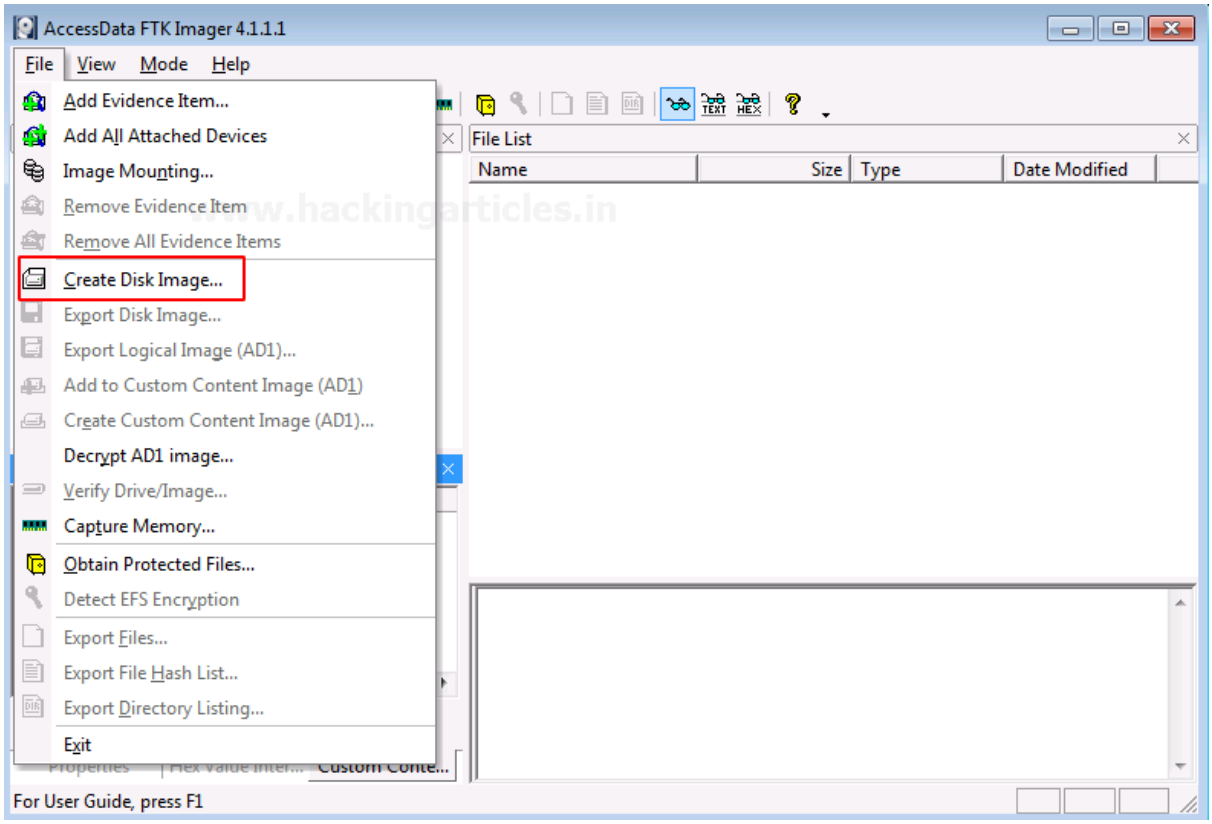
Creating a Forensic Image

Forensic Imaging is one of the most crucial steps involved in digital forensic investigation. It is the process of making an archival or backup copy of the entire hard drive. It is a storage file that contains all the necessary information to boot to the operating system. However, this imaged disk needs to be applied to the hard drive to work. One cannot restore a hard drive by placing the disk image files on it as it needs to be opened and installed on the drive using an imaging program. A single hard drive can store many disk images on it. Disk images can also be stored on flash drives with a larger capacity.

Open FTK Imager by AccessData after installing it, and you will see the window pop-up which is the first page to which this tool opens.

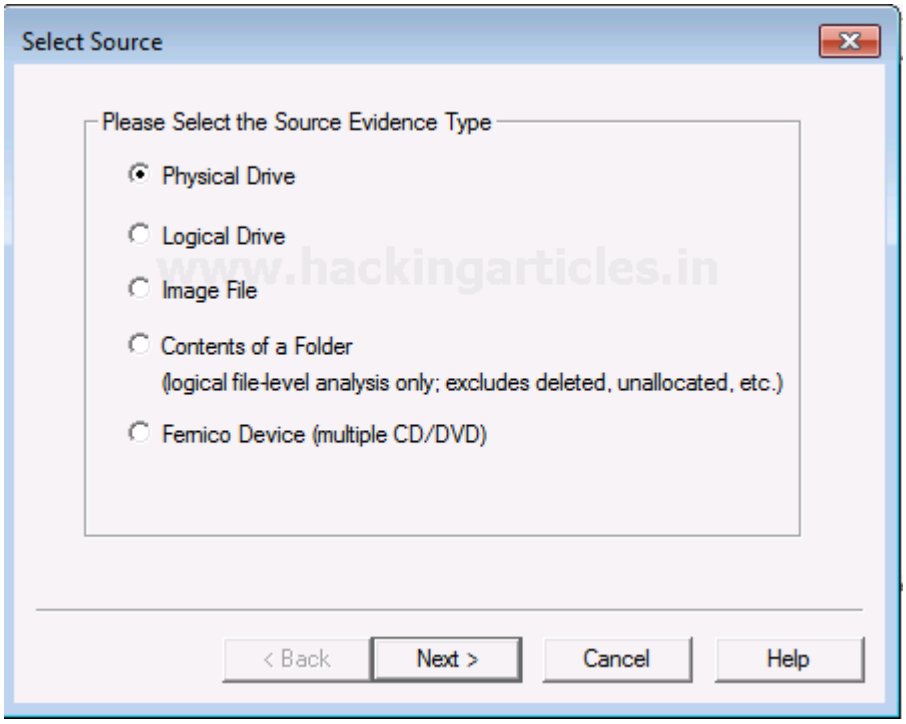


Now, to create a Disk Image. *Click on File > Create Disk Image*.

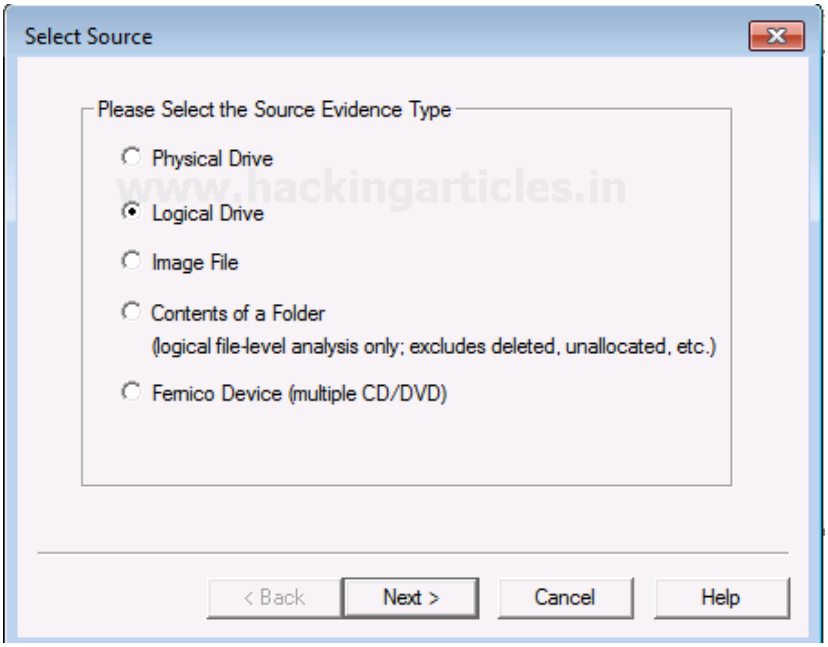


Now you can choose the source based on the drive you have. It can be a physical or a logical Drive depending on your evidence.

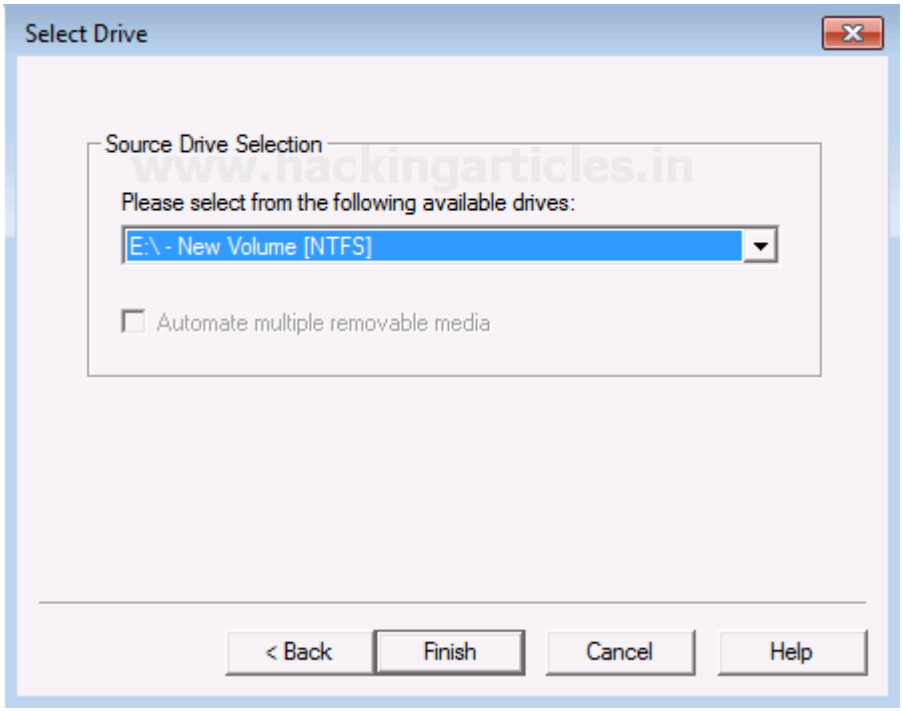
A Physical Drive is the primary storage hardware or the component within a device, which is used to store, retrieve, and organize data.



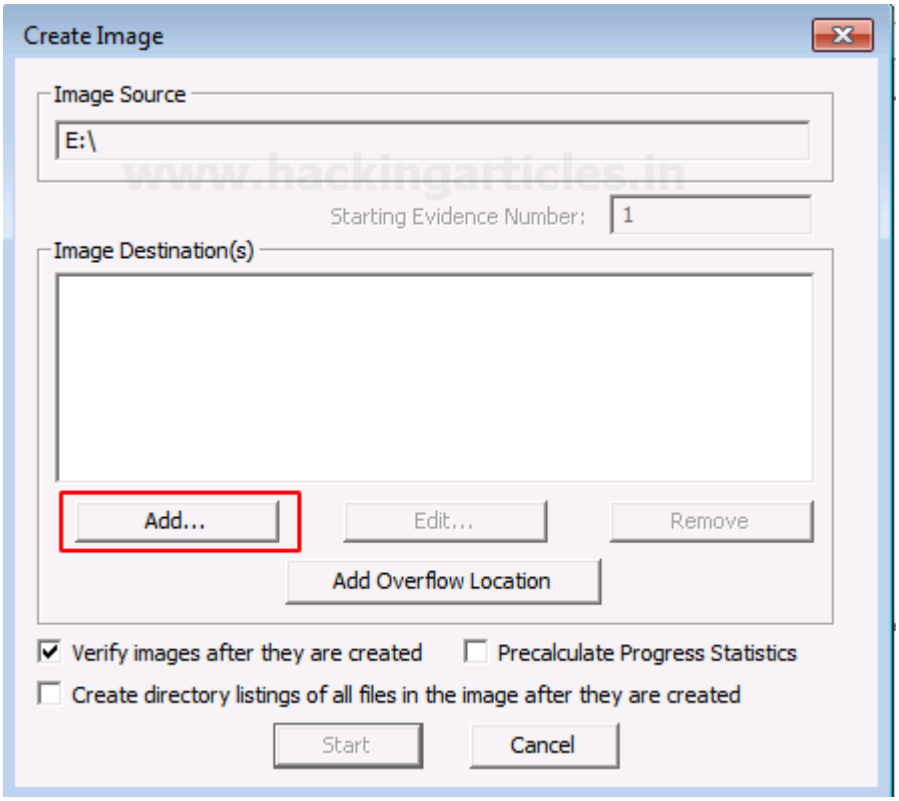
A Logical Drive is generally a drive space that is created over a physical hard disk. A logical drive has its parameters and functions because it operates independently.



Now choose the source of your drive that you want to create an image copy of.

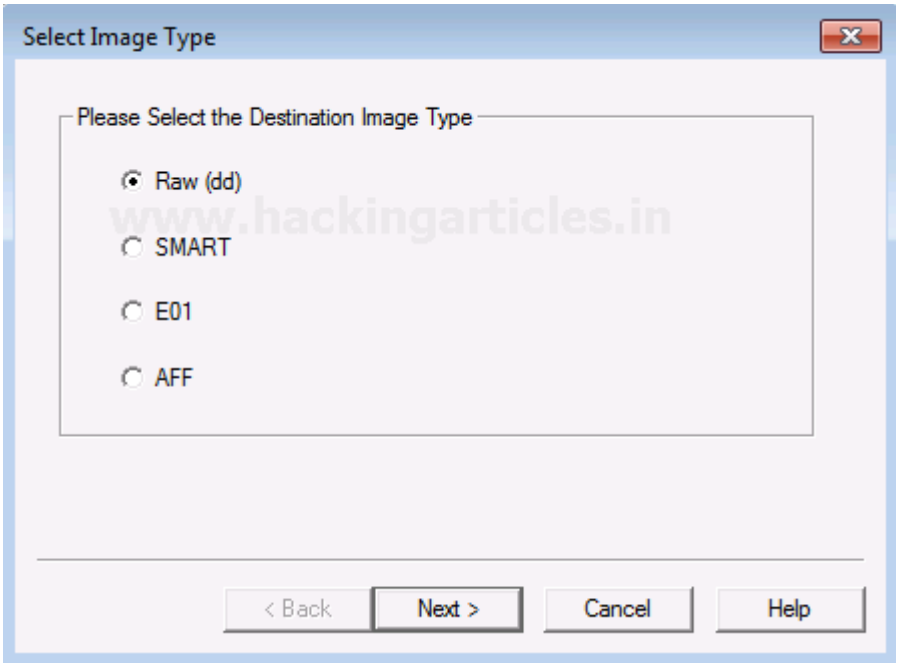


Add the Destination path of the image that is going to be created. From the forensic perspective, It should be copied in a separate hard drive and multiple copies of the original evidence should be created to prevent loss of evidence.

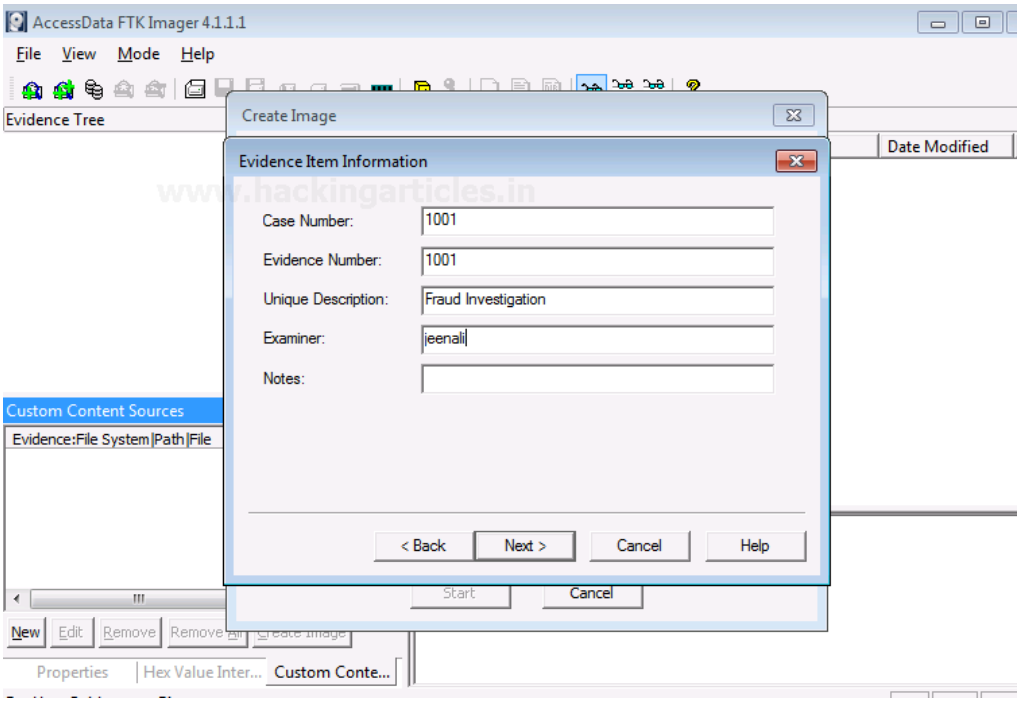


Select the format of the image that you want to create. The different formats for creating the image are:

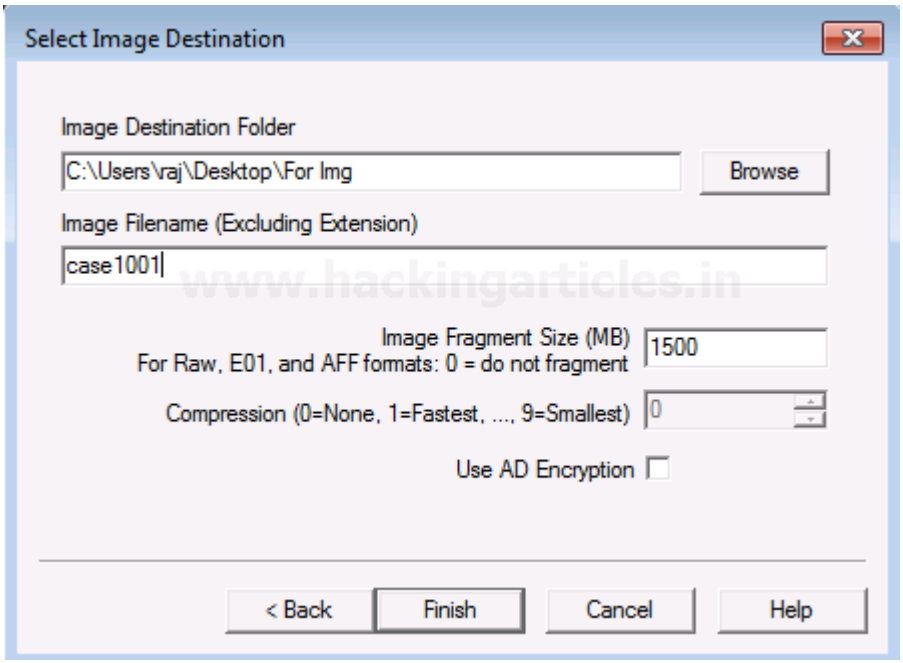
- Raw(dd): It is a bit-by-bit copy of the original evidence which is created without any additions and or deletions. They do not contain any metadata.
- SMART: It is an image format that was used for Linux which is not popularly used anymore.
- E01: It stands for EnCase Evidence File, which is a commonly used format for imaging and is similar to
- AFF: It stands for Advanced Forensic Format that is an open-source format type.



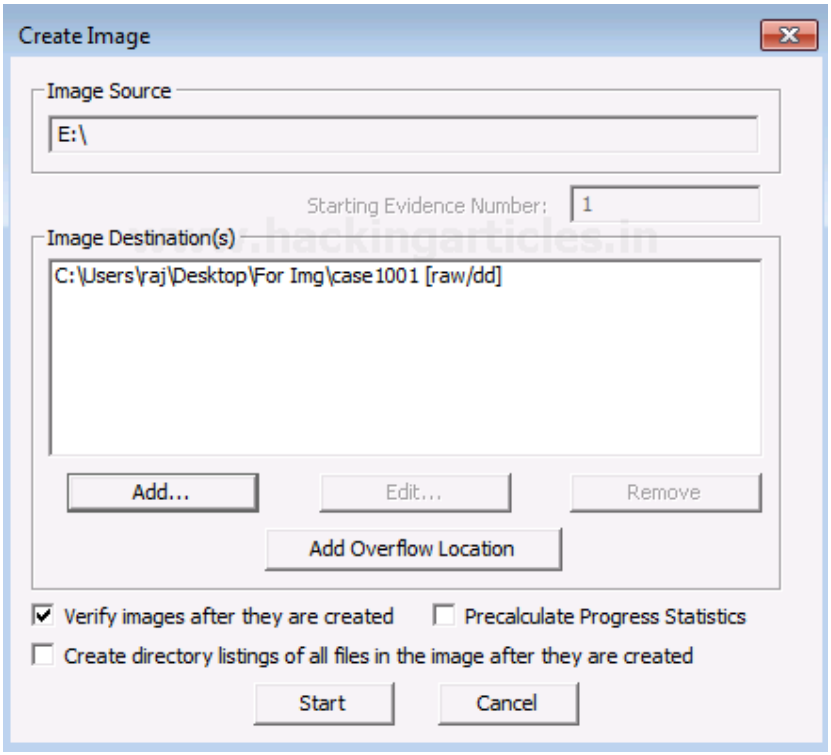
Now, add the details of the image to proceed.



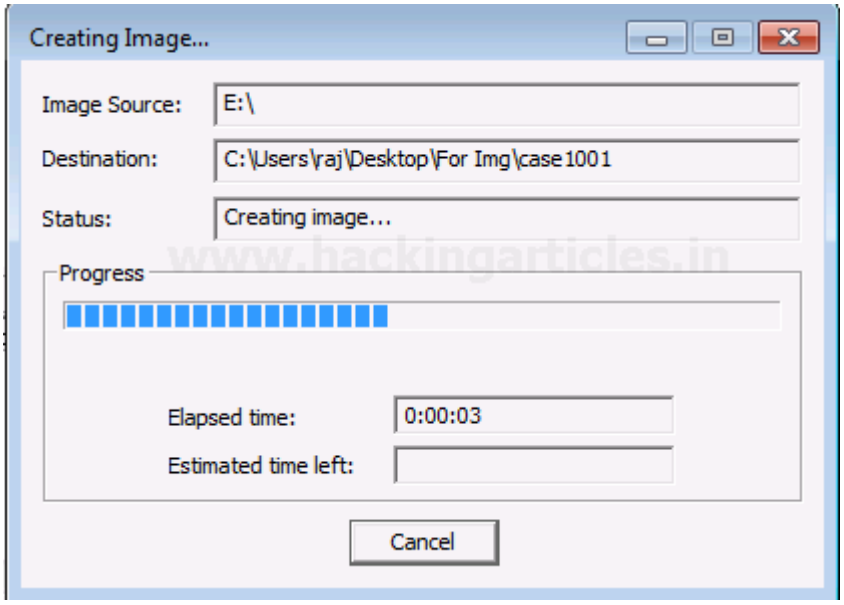
Now finally add the destination of the image file, name the image file and then click on *Finish.*



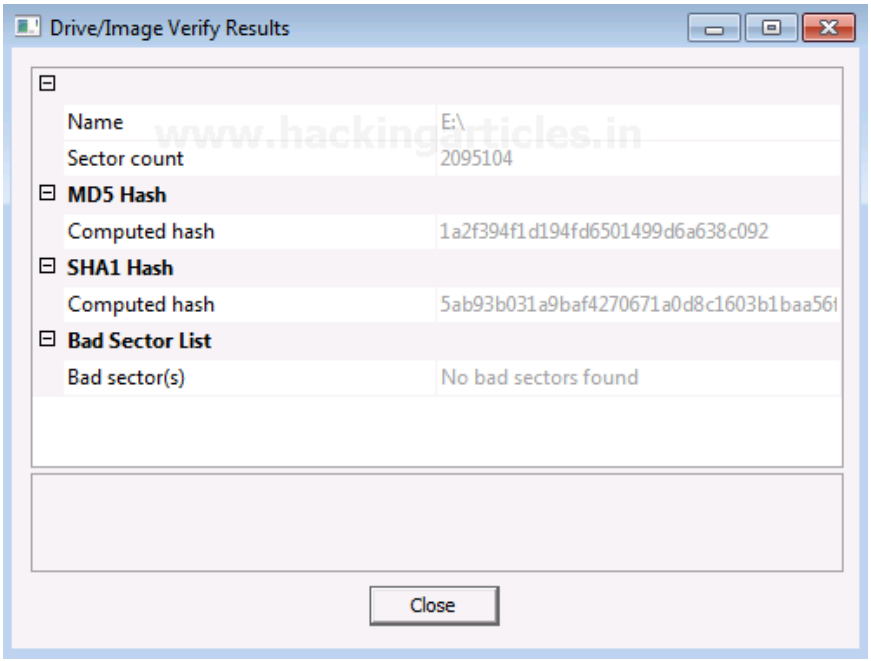
Once you have added the destination path, you can now start with the Imaging and also click on the verify option to generate a hash.



Now let us wait for a few minutes for the image to be created.



After the image is created, a Hash result is generated which verifies the MD5 Hash, SHA1 Hash, and the presence of any bad sector.

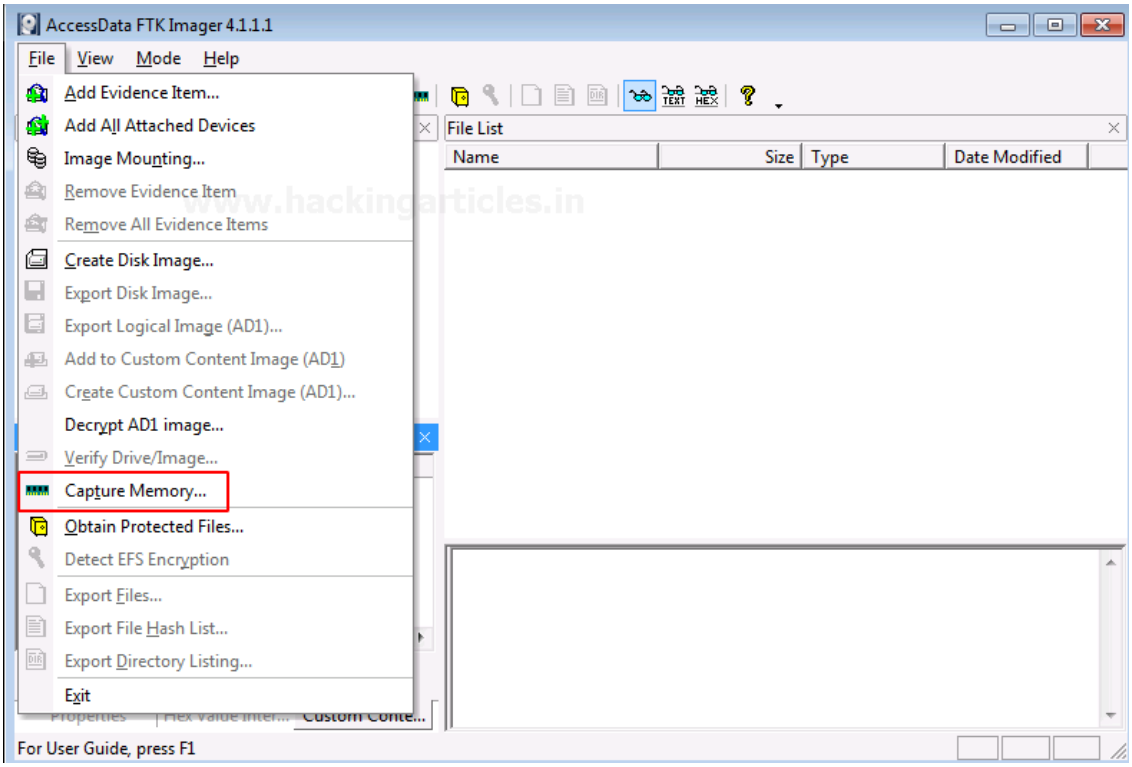


Capturing Memory

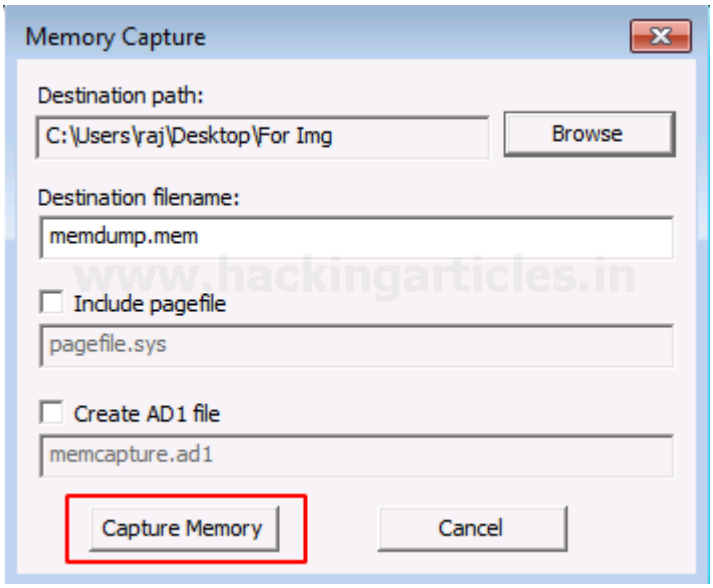
It is the method of capturing and dumping the contents of a volatile content into a non-volatile storage device to preserve it for further investigation. A ram analysis can only be successfully conducted when the acquisition has been performed accurately without corrupting the image of the volatile memory. In this phase, the investigator has to be careful about his decisions to collect the volatile data as it won't exist after the system undergoes a reboot.

Now, let us begin with capturing the memory.

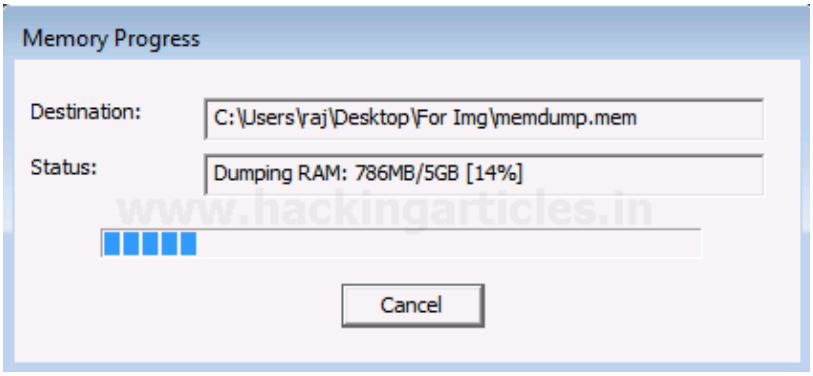
To capture the memory, click on *File* > *Capture Memory*.



Choose the destination path and the destination file name, and click on *capture memory.*

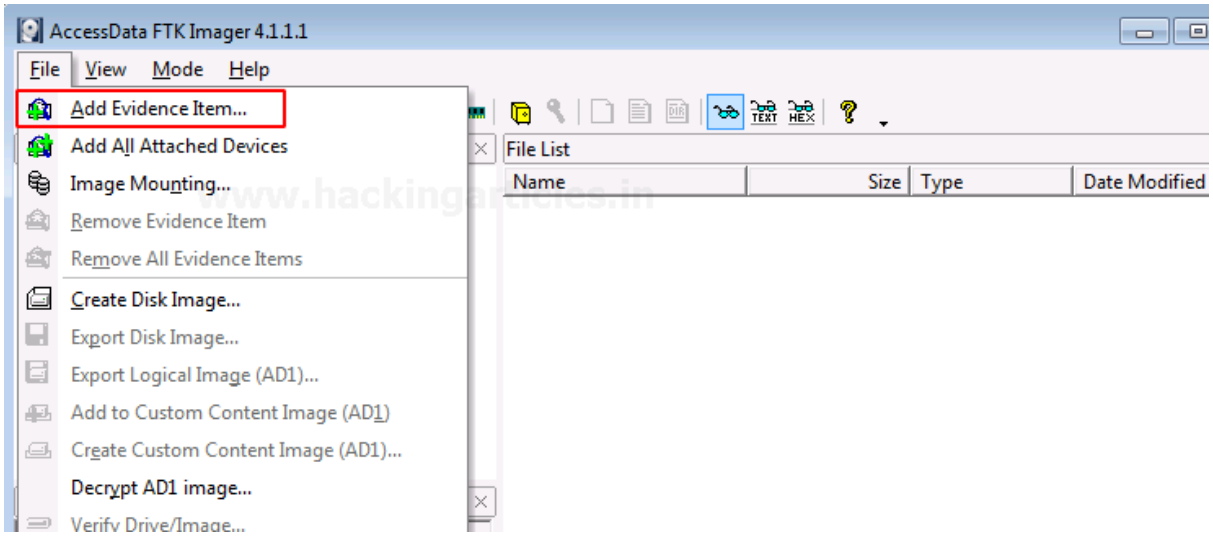


Now let us wait for a few minutes till the ram is being captured

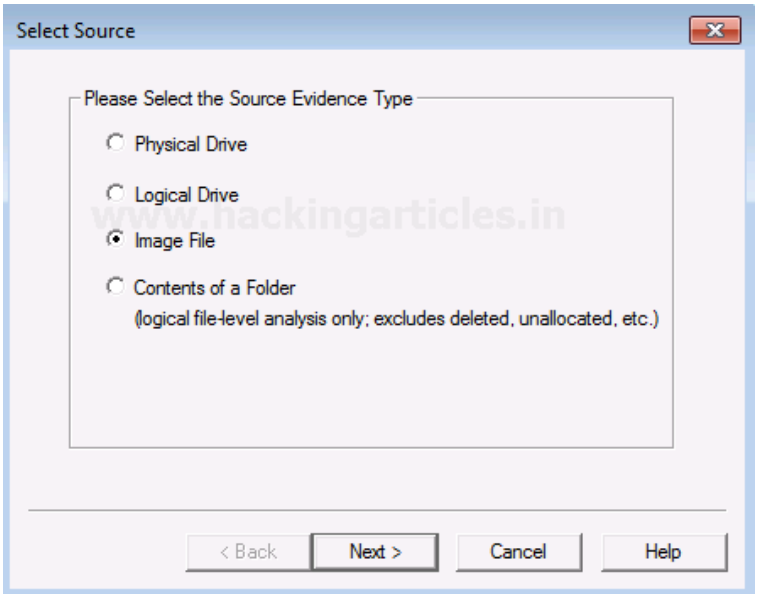


Analyzing Image Dump

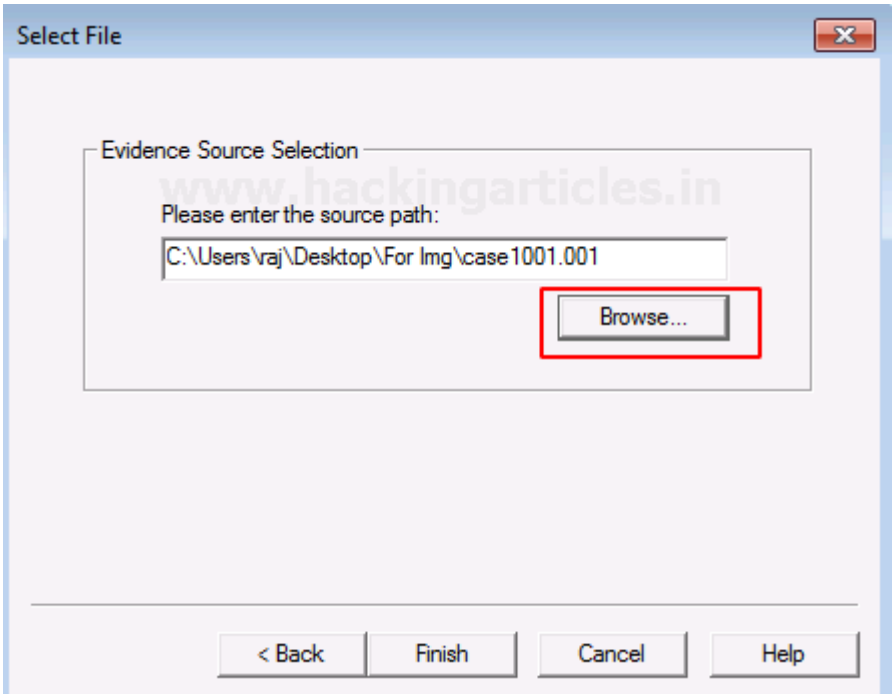
Now let us analyze the Dump RAW Image once it has been acquired using FTK imager. To start with analysis, click on *File> Add Evidence Item*.



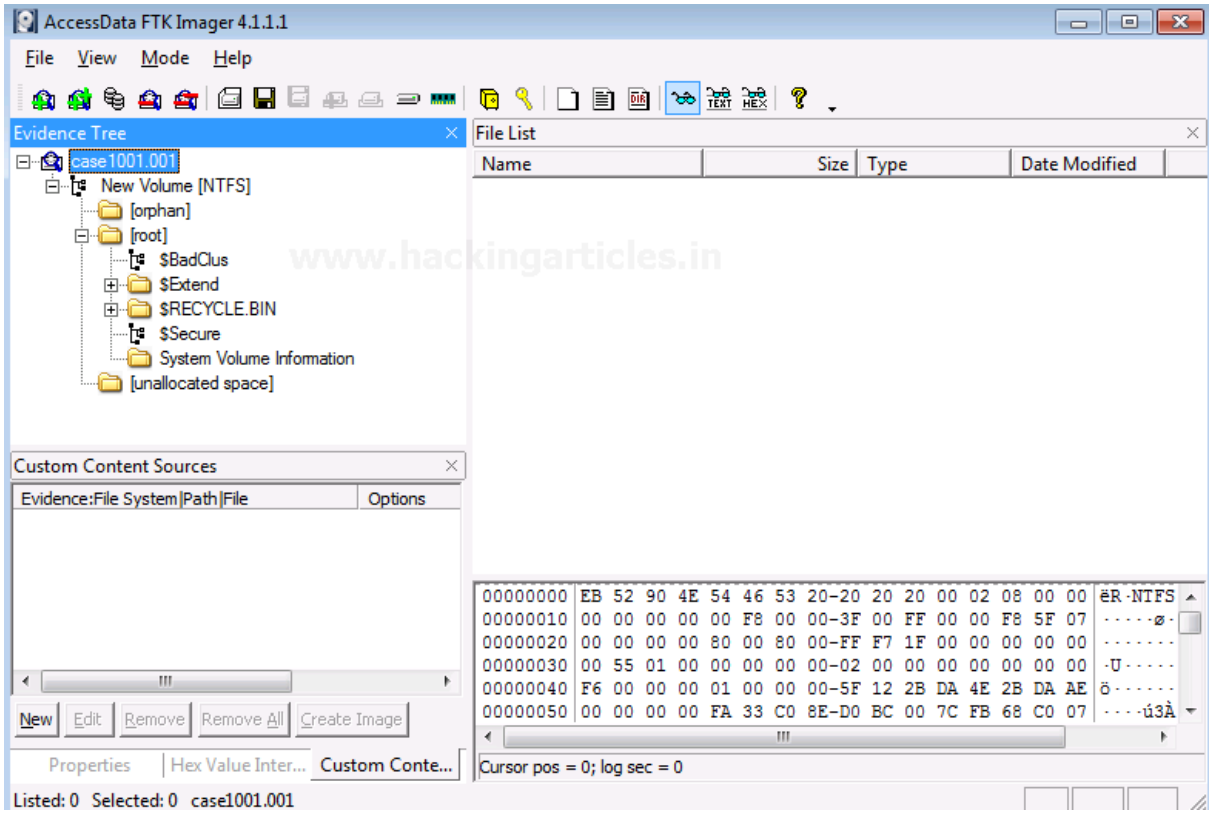
Now select the source of the dump file that you have already created, so here you have to select the image file option and click on Next.



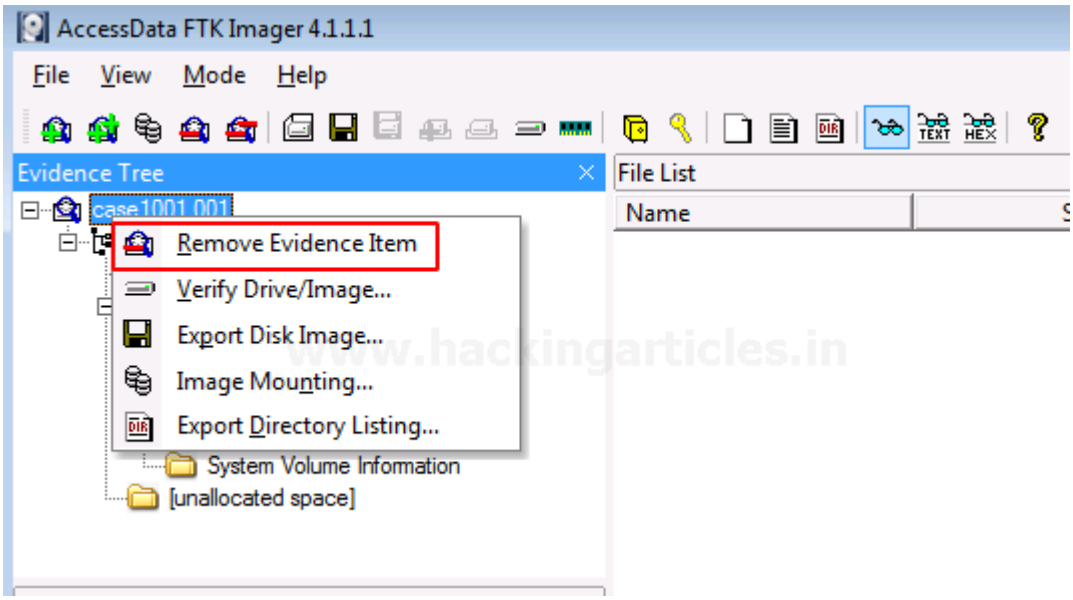
Choose the path of the image dump that you have captured by clicking on Browse.



Once the image dump is attached to the analysis part, you will see an evidence tree which has the contents of the files of the image dump. This could have deleted as well as overwritten data.

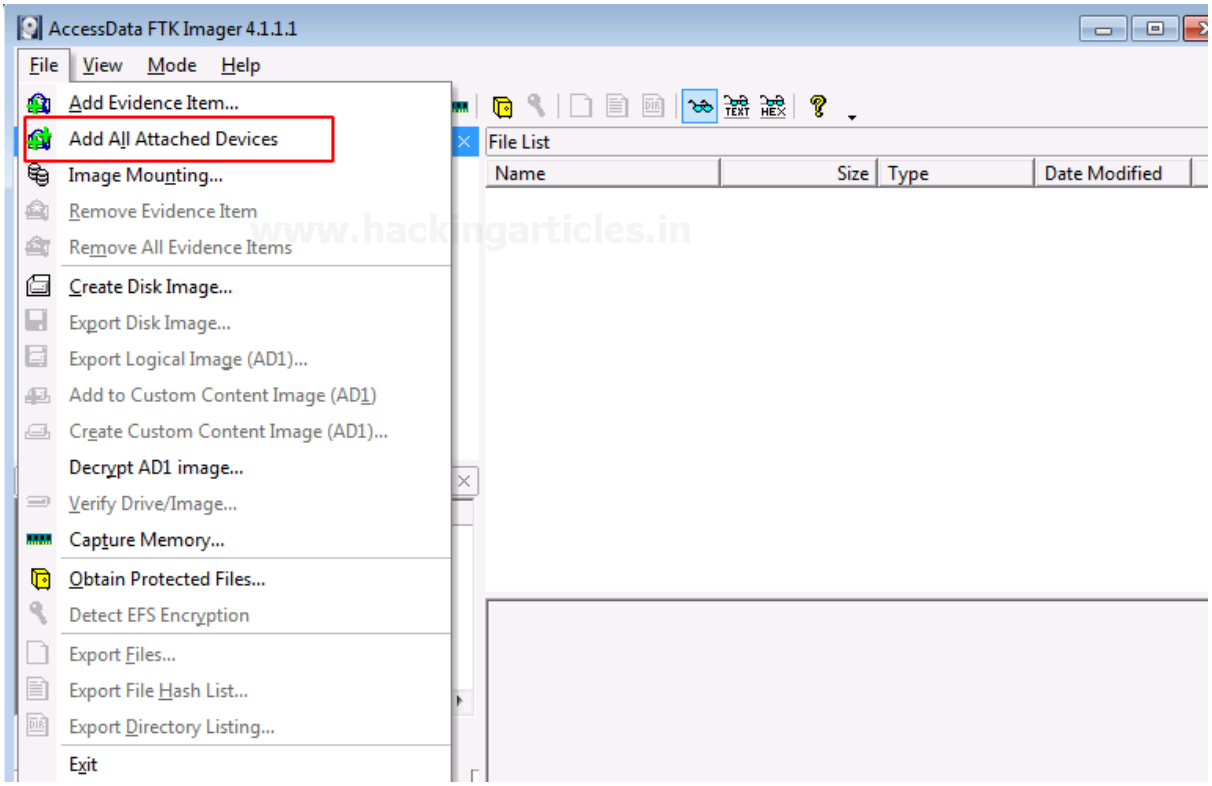


To analyze other things further, we will now remove this evidence item by right-clicking on the case and click on *Remove Evidence Item.*

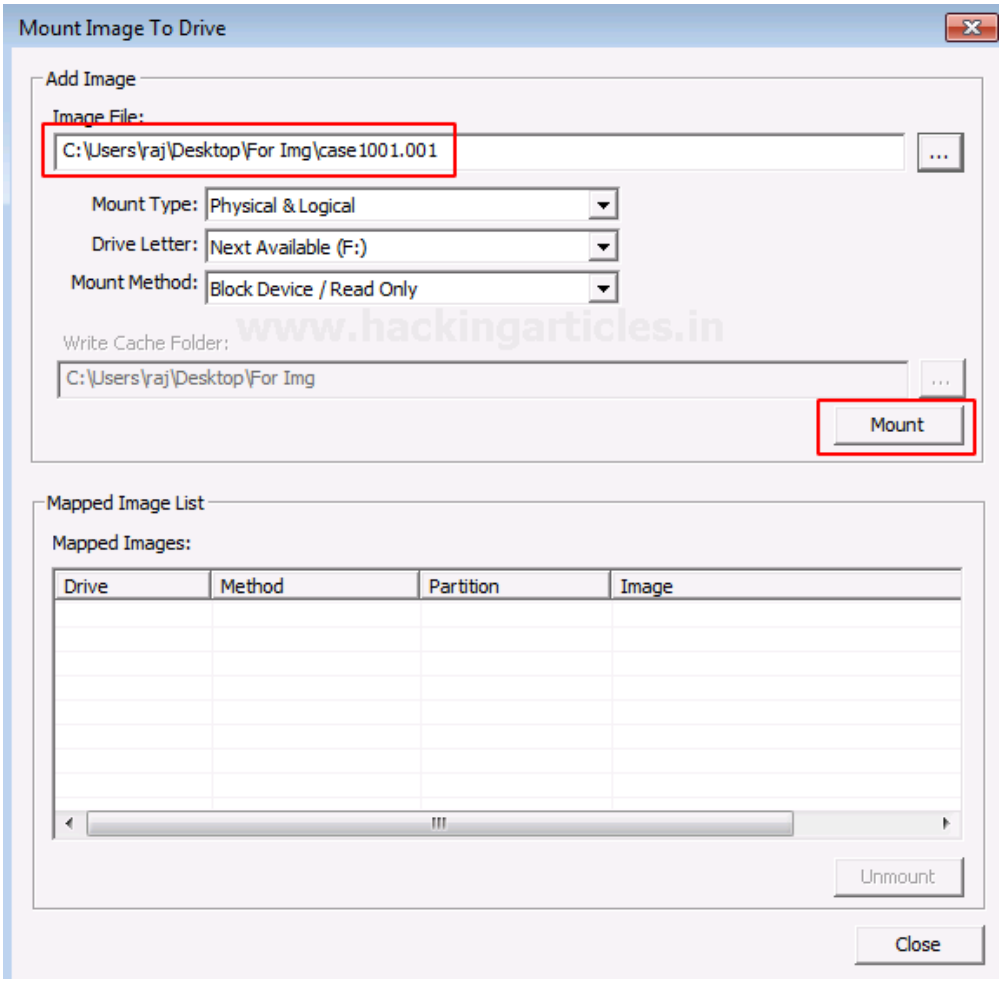


Mounting Image to Drive

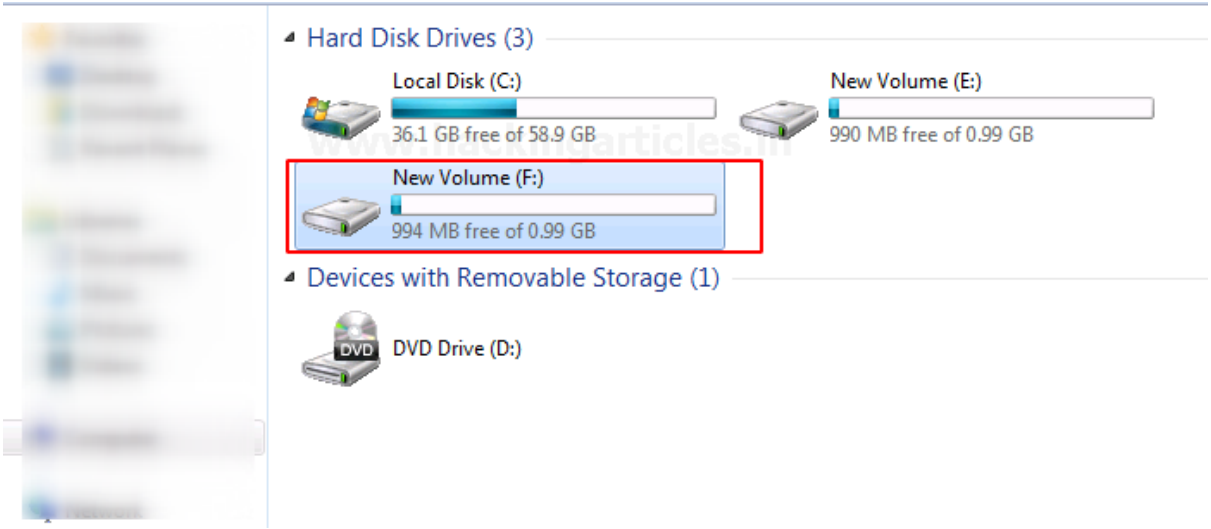
To mount the image as a drive in your system, click on *File* > *Image Mounting*



Once the Mount Image to Drive window appears, you can add the path to the image file that you want to mount and click on *Mount*.

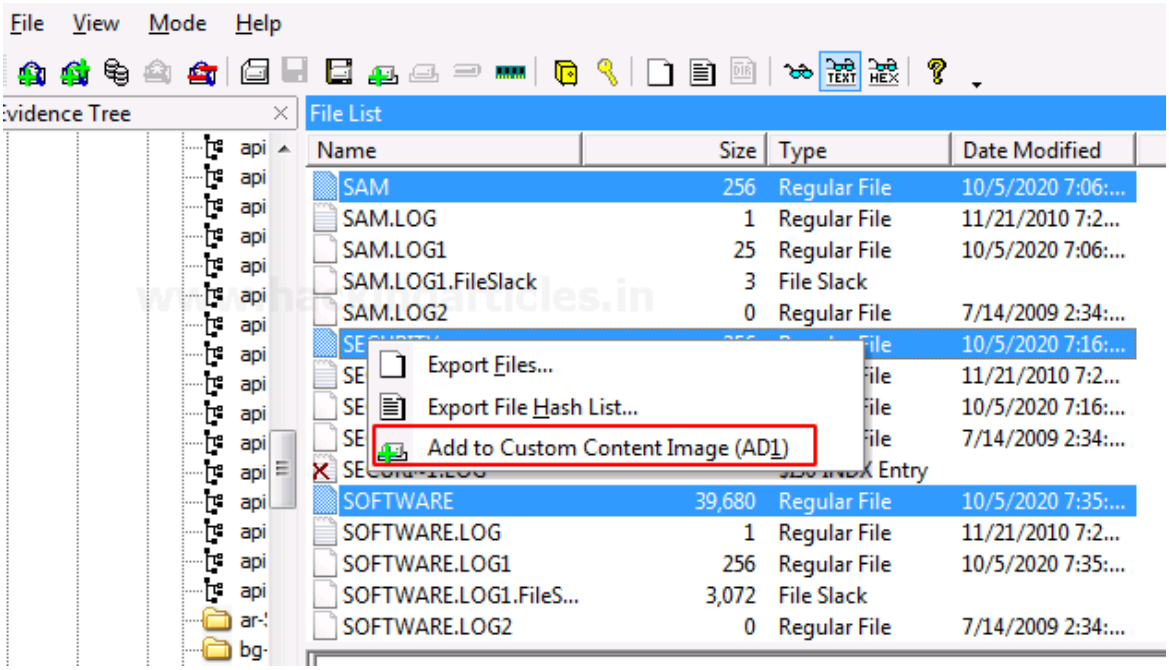


Now you can see that the image file has now been mounted as a drive.

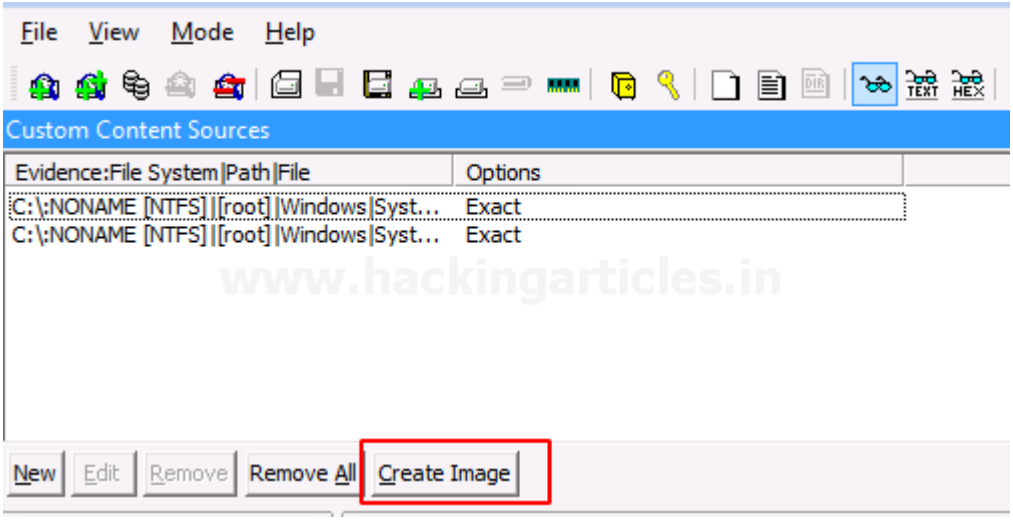


Custom Content Image with AD Encryption

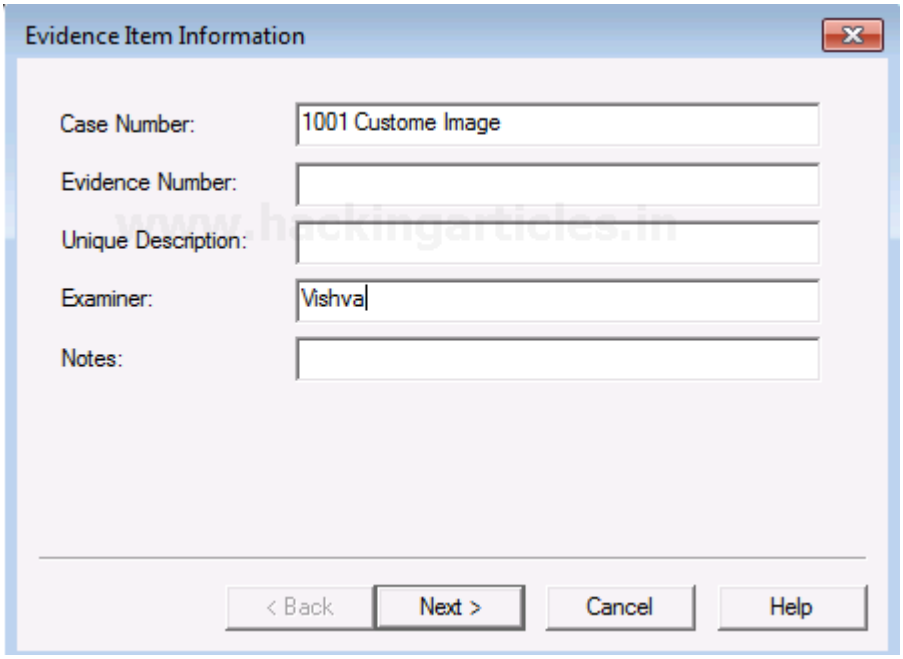
FTK imager has a feature that allows it to encrypt files of a particular type according to the requirement of the examiner. Click on the files that you want to add to the custom content Image along with AD encryption.



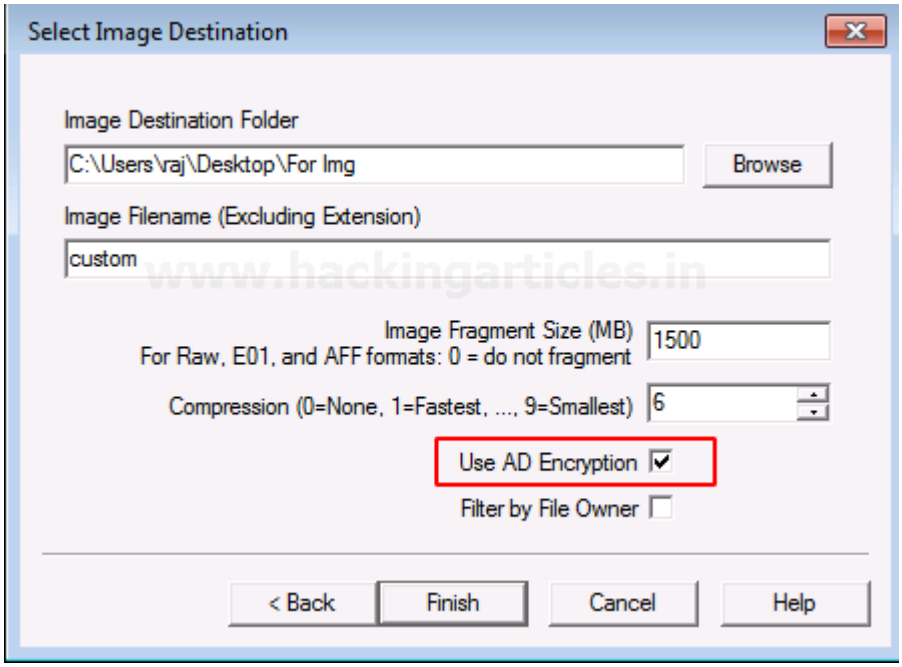
All the selected files will be displayed in a new window and then click on Create Image to proceed.



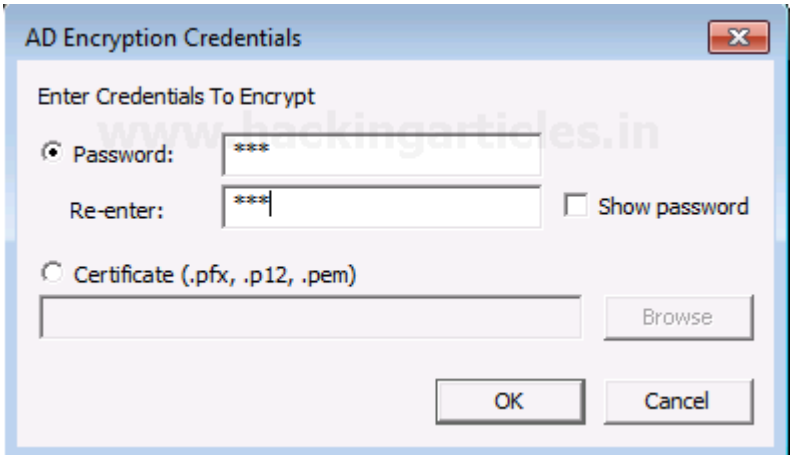
Fill in the required details for the evidence that is to be created.



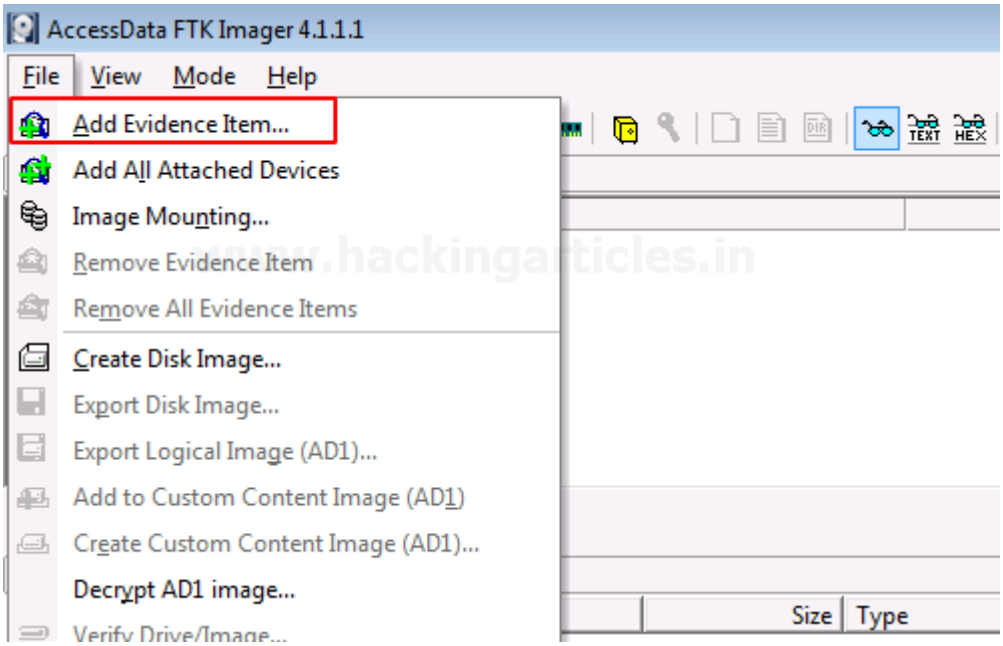
Now add the destination of the image file that is to be created, name the image file and then check the box with AD encryption, and then click on Finish.



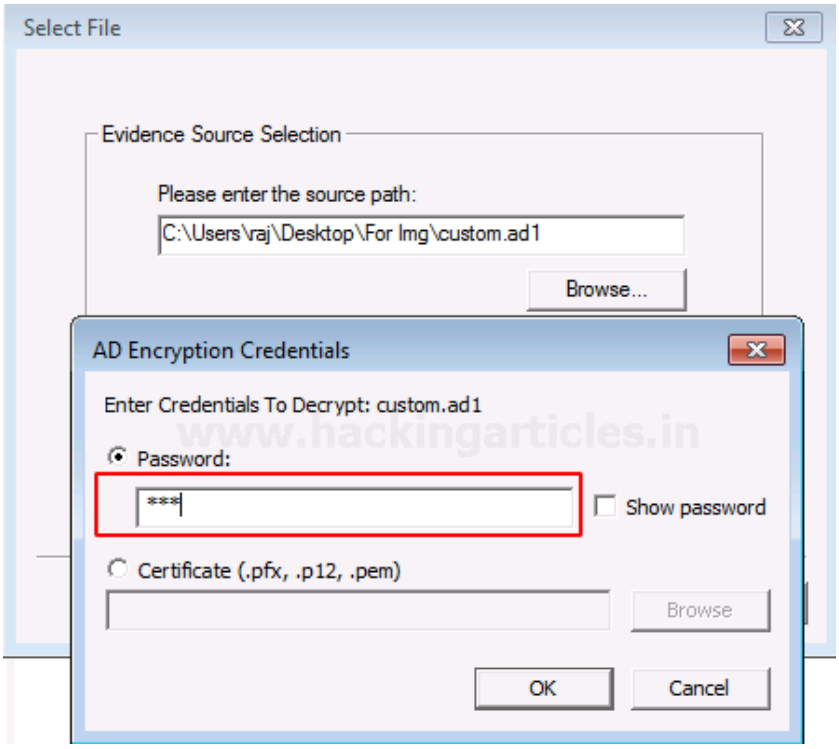
A new window will pop-up to encrypt the image, Now renter and re-enter the password that you want to add for your image.



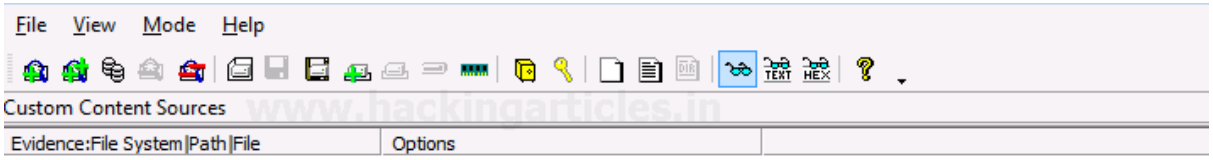
Now to see the encrypted files, click on *File> Add Evidence Item…*

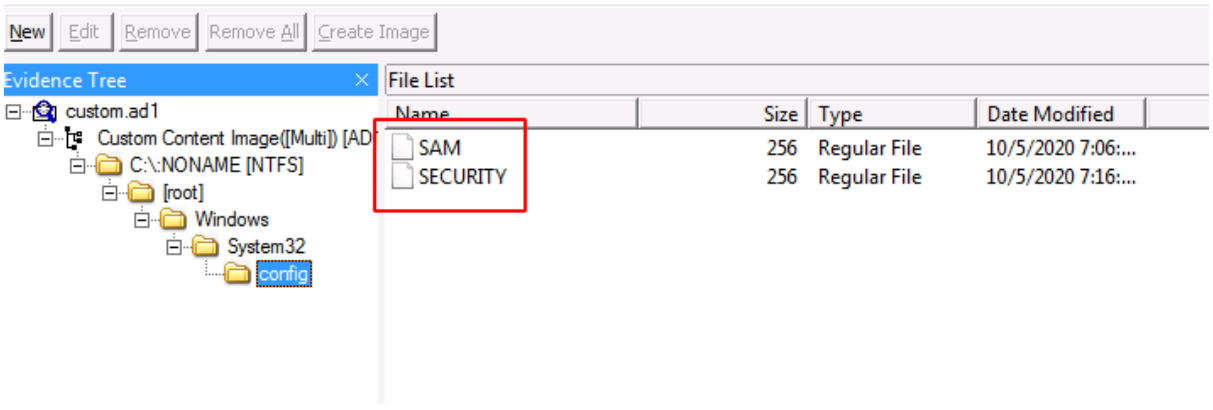


The window to decrypt the encrypted files will appear once you add the file source. Enter the password and click OK.



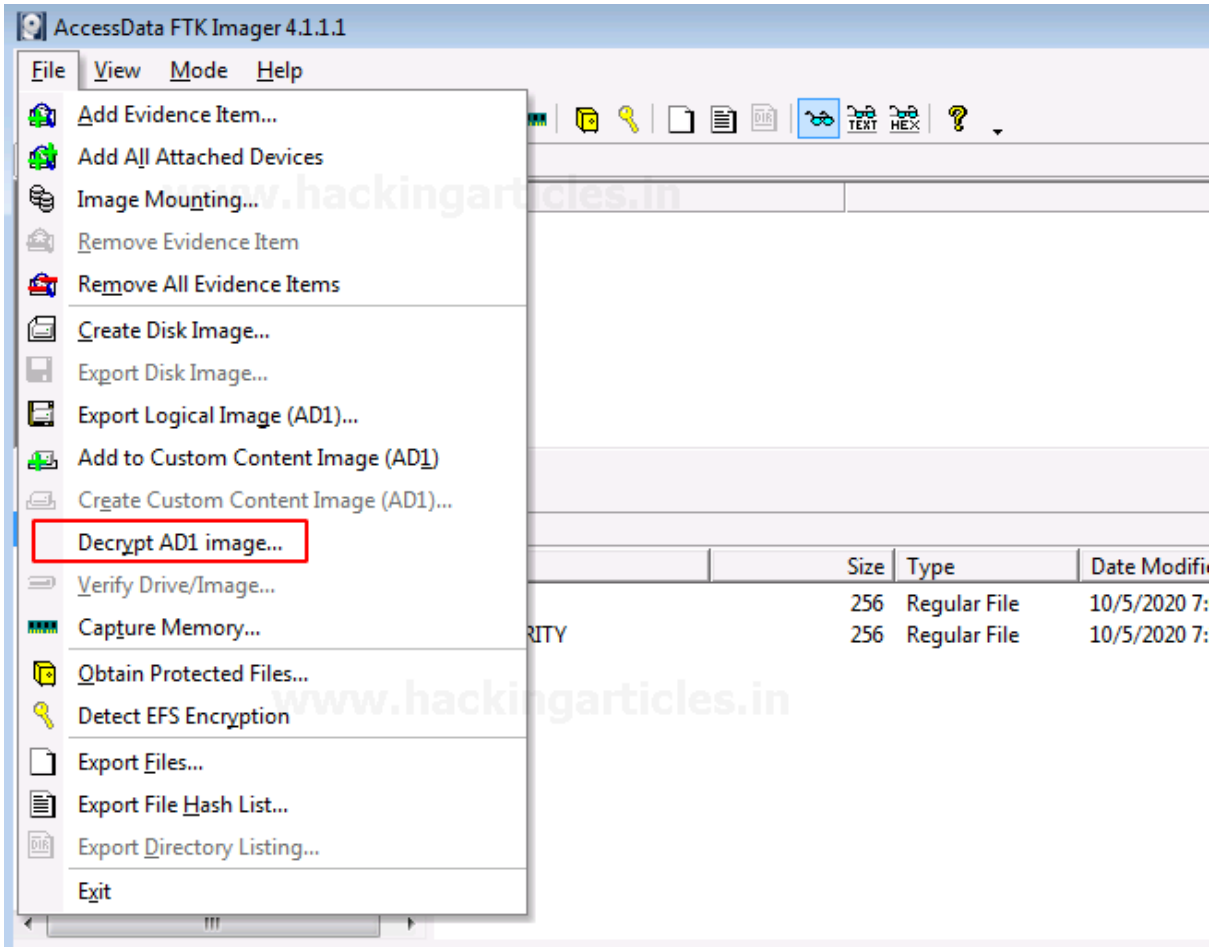
You will now see the two encrypted files on entering the valid passwords.



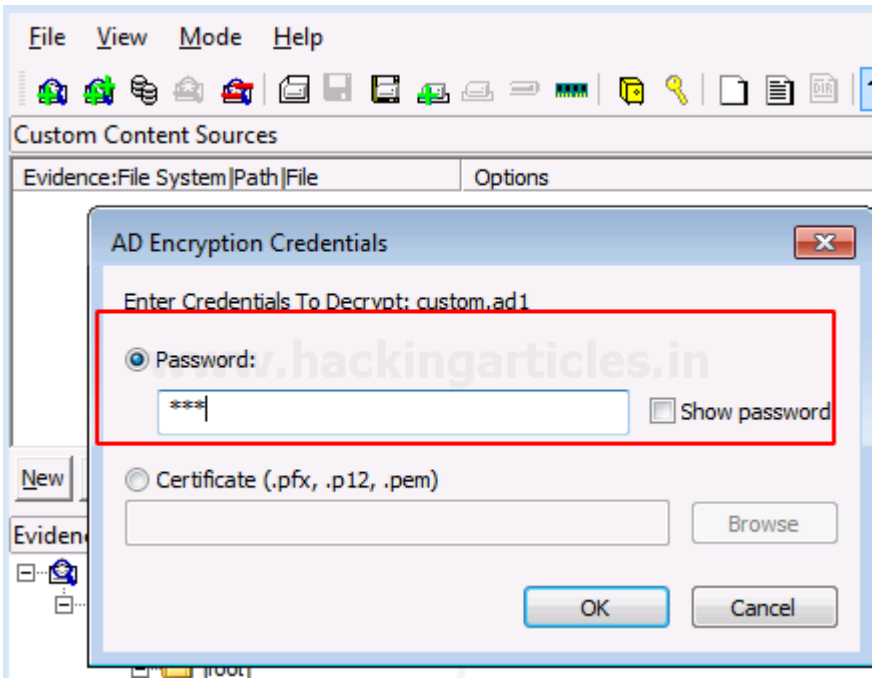


Decrypt AD1 Image

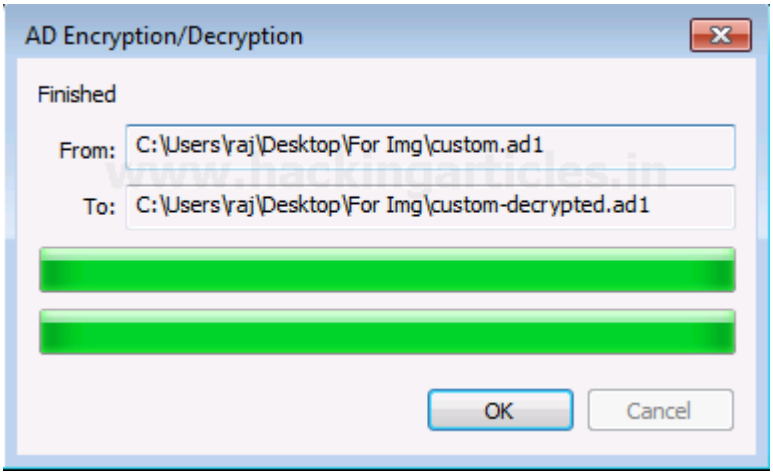
To decrypt the custom content image, click on *File> Decrypt AD1 Image.*



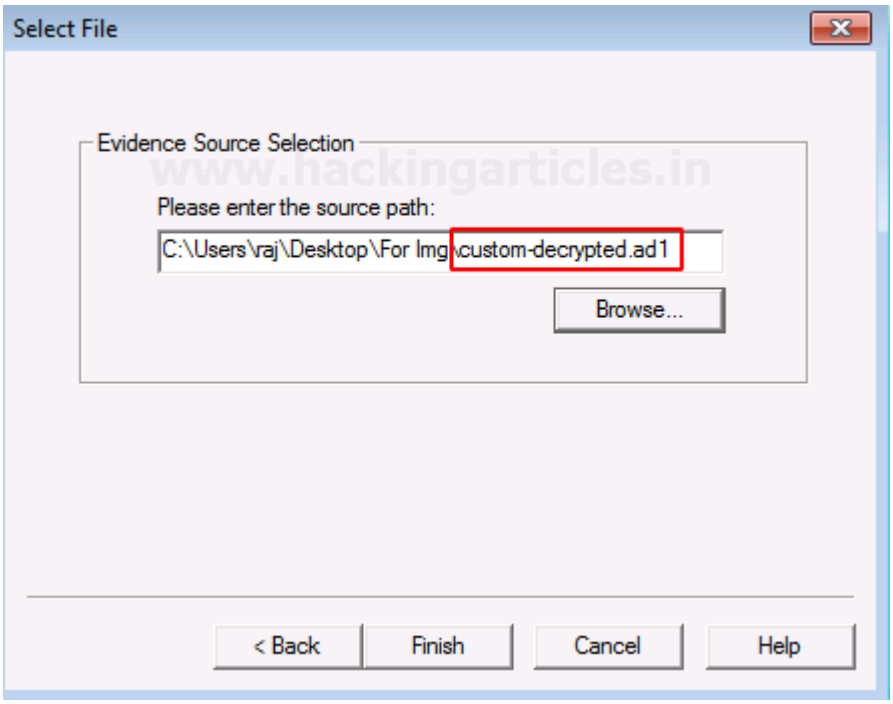
Now you need to enter the password for the image file that was encrypted and click on Ok.



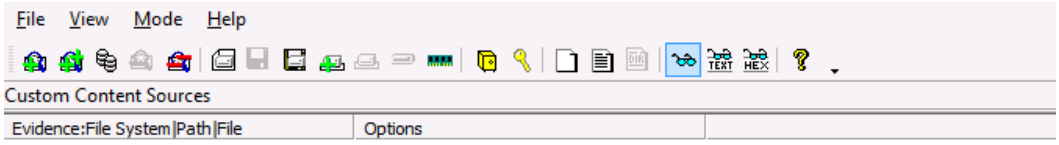
Now, wait for a few minutes till the decrypted image is created.

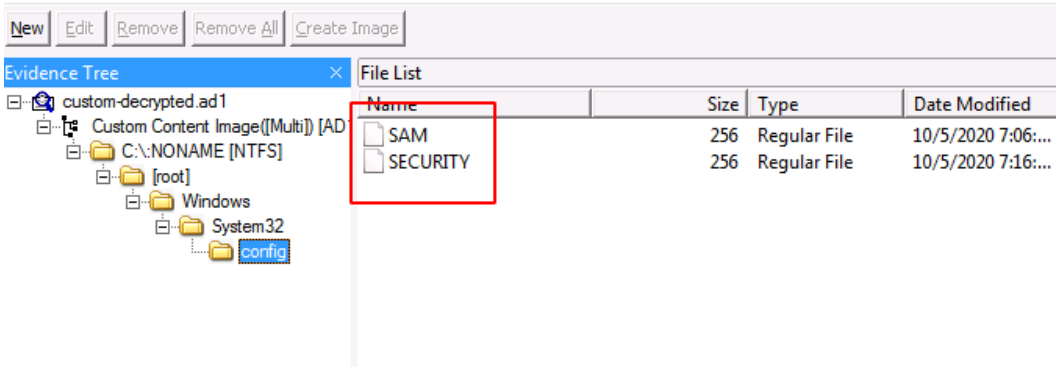


To view the decrypted custom content image, add the path of the decrypted file and click on Finish.



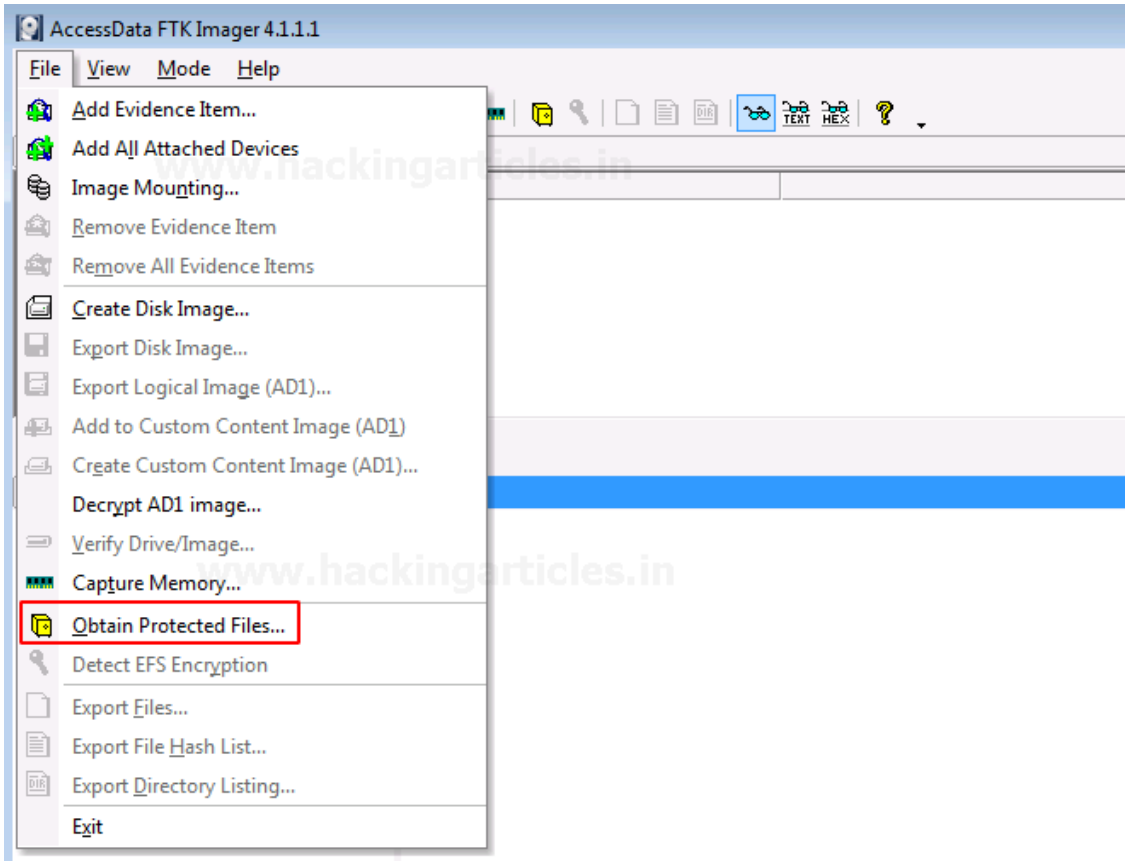
You will now be able to see the encrypted files by using the correct password to decrypt it.



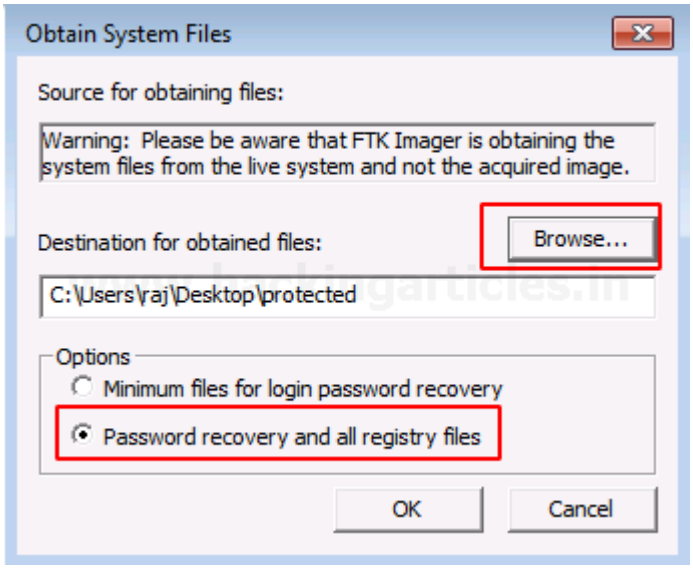


Obtain Protected Files

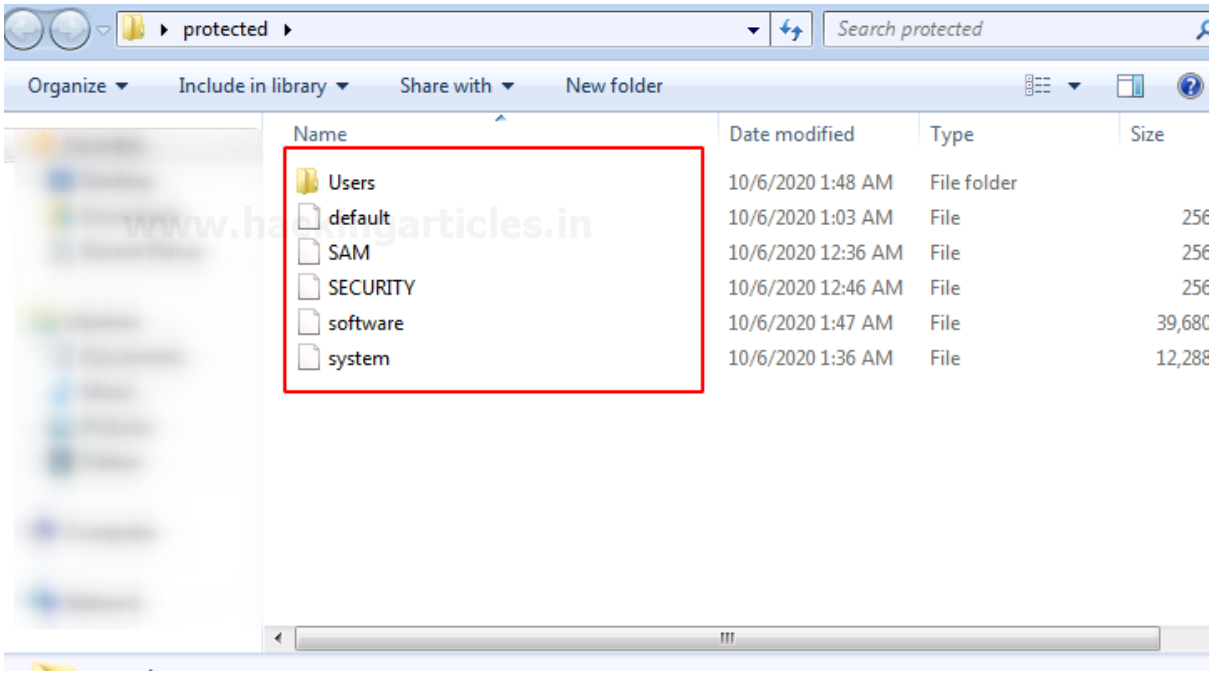
Certain files are protected on recovery, to obtain those files, click on *File> Obtain Protected Files*



A new window will pop and click on browse to add the destination of the file that is protected and click on the option that says password recovery and all registry files and click on OK.

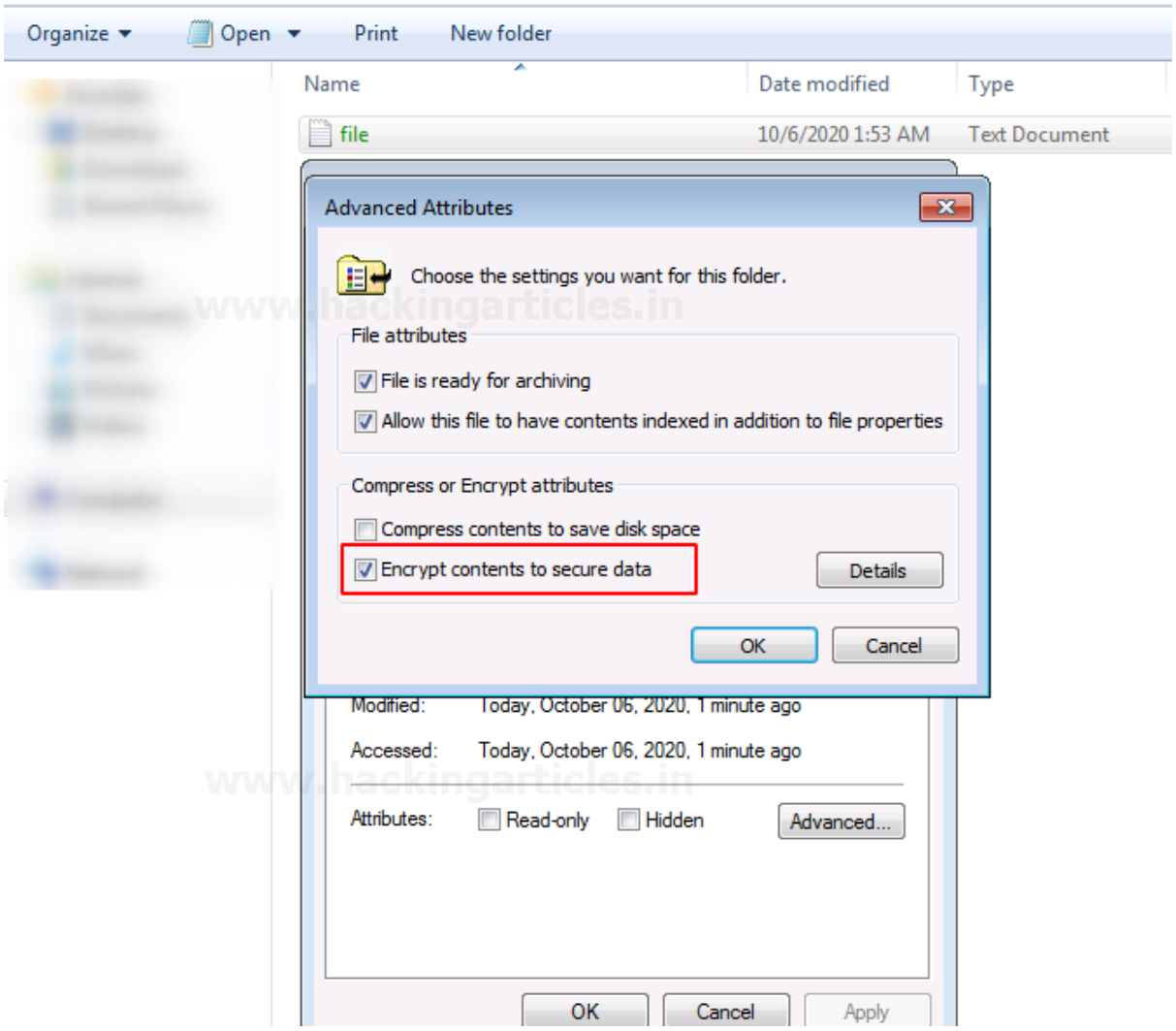


Now you will see all the protected files in one place

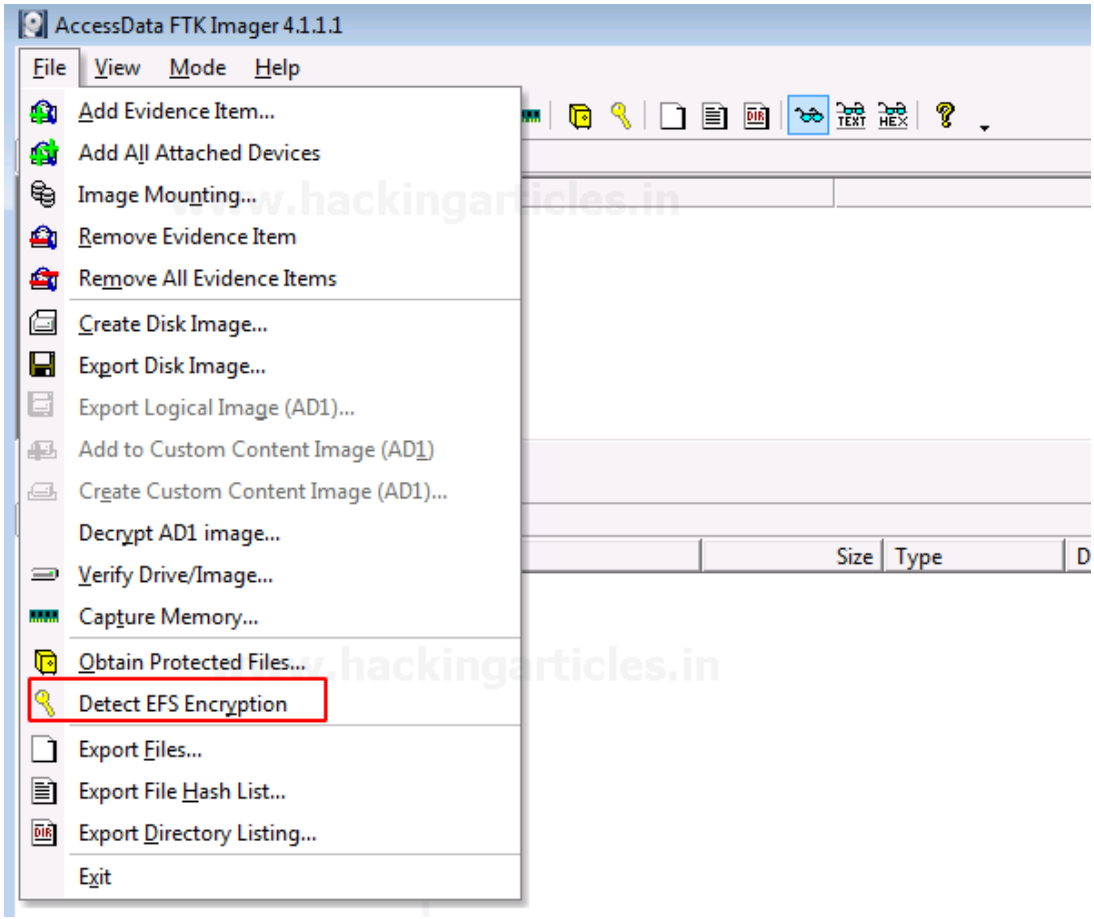


Detect EFS Encryption

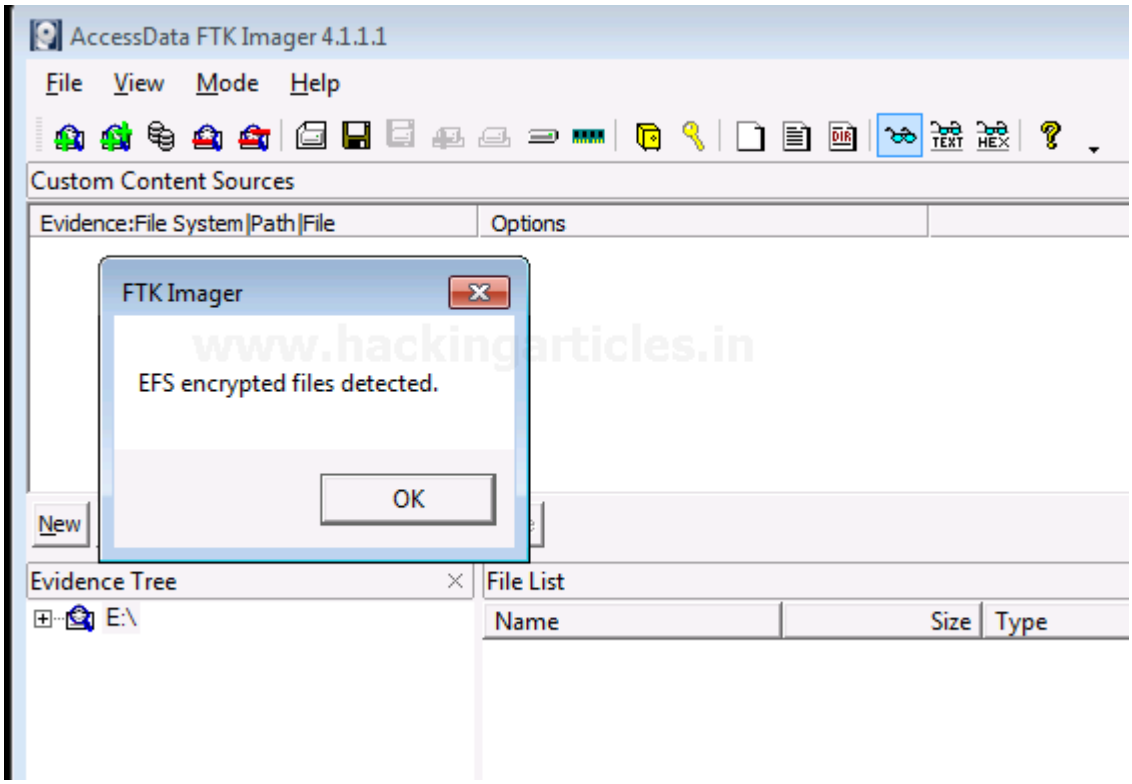
When a folder or a file is encrypted, we can detect it using this feature of the FTK Imager. A file is encrypted in a folder to secure its content.



To detect the EFS encryption, click on *File >Detect EFS Encryption*

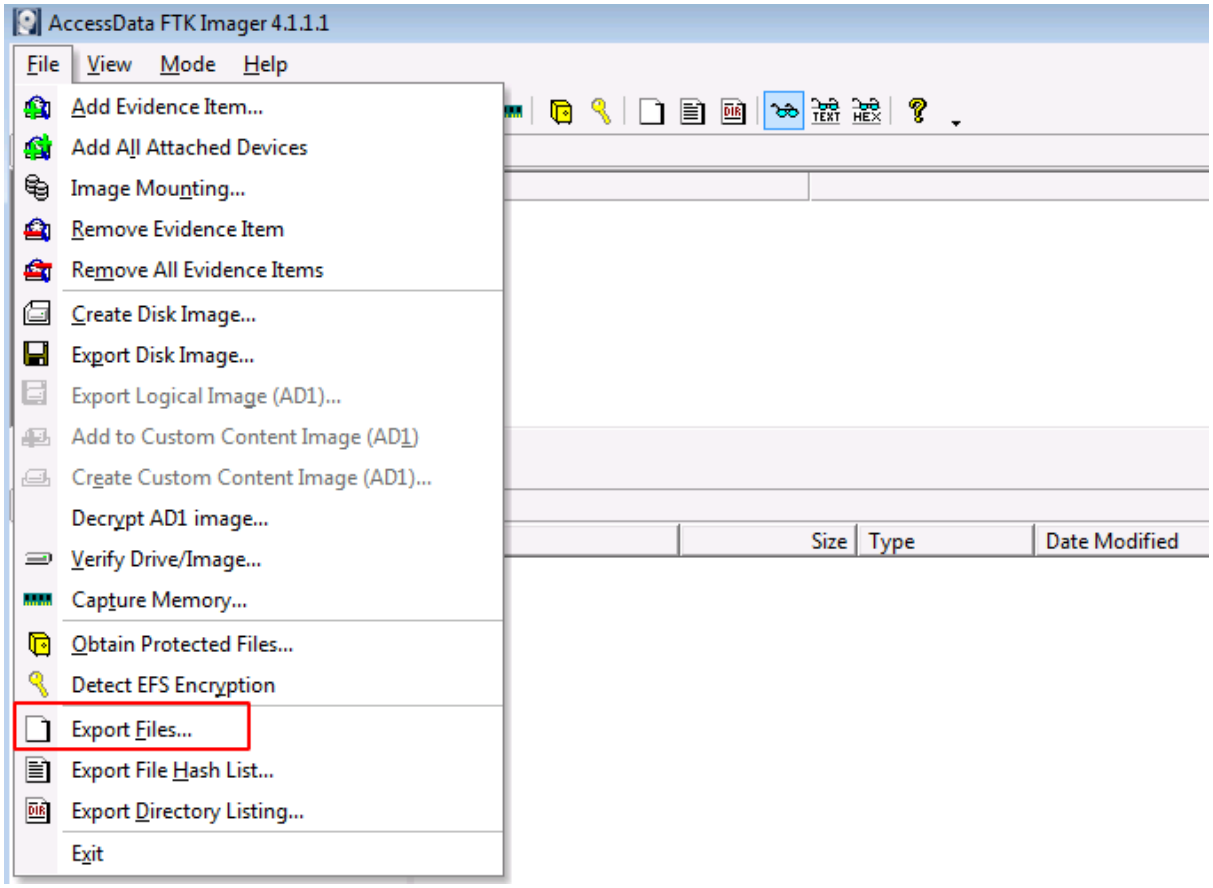


You can see that the encryption is detected.

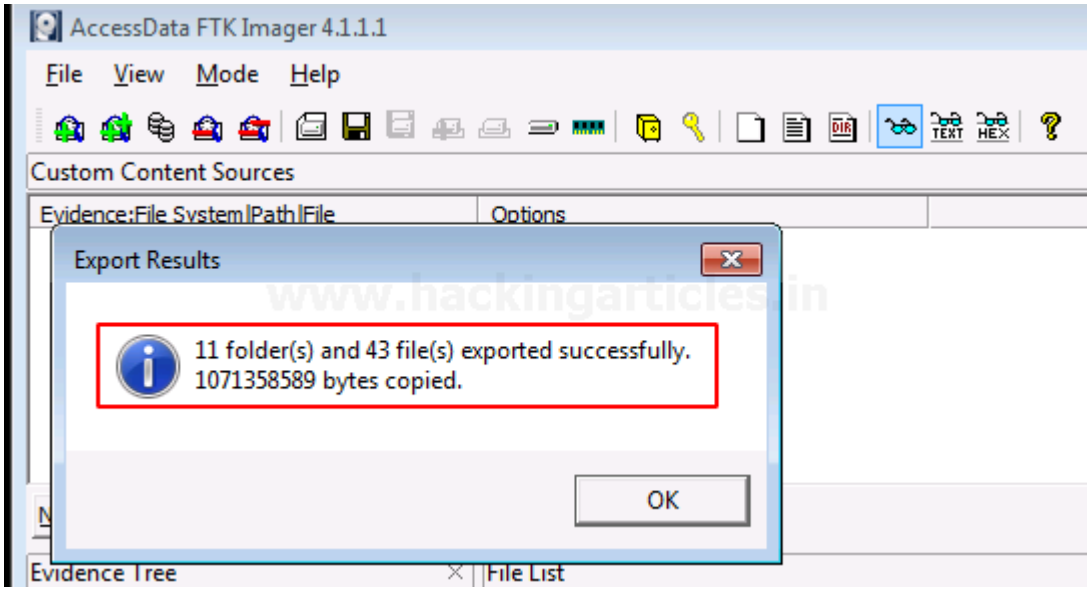


Export Files

To export the files and folders from the imaged file to your folder, you can click *File > Export Files*



You can now see the results of the export of the number of files and folders that have been copied to the system.


AccessData FTK Imager 4.1.1.1
File View Mode Help
Custom Content Sources
Evidence:File System|Path|File
Options
Export Results
11 folder(s) and 43 file(s) exported successfully.
1071358589 bytes copied.
OK
Evidence Tree
File List

HEX EDITOR

AIM: To familiarize file signature analysis

DESCRIPTION

A hex editor is a computer program used to view and edit binary files. A binary file is a file that contains data in machine-readable form. Hex editors allow editing the raw data contents of a file, instead of other programs which attempt to interpret the data for you. Since a hex editor is used to edit binary files, they are sometimes called a binary editor or a binary file editor. If you edit a file with a hex editor, you are said to hex edit the file, and the process of using a hex editor is called hex editing.

A typical hex editor has three areas: an address area on the left, a hexadecimal area in the center, and a character area on the right. In the most powerful hex editors, these areas can be configured to display other values. Every file on your machine is made up of a series of bytes. A byte is just a number that can store a value from 0 up to 255 inclusive. Every byte in a file is assigned a number, called its address, starting at 0 for the first byte of the file, 1 for the second byte, etc.

Hexadecimal Area

The middle hexadecimal area is the most commonly used area of a hex editor. It lists each byte of the file in a table, usually sixteen bytes per line. If Figure 2, the first 8 bytes of the file would be '4D 5A 90 00 03 00 00 00'. Each byte is listed in a special notation called hexadecimal notation, sometimes called hex code. Most numbers in our world are represented in decimal or base-10 notation, meaning we use 10 different digits (0 up to 9). Hexadecimal or base-16 notation uses 16 different digits: 0 up to 9 and then the letters A, B, C, D, E, F to represent 10, 11, 12, 13, 14, and 15. Numbers in hexadecimal notation commonly have an 'h' written after them, or an '0x' written before them to indicate that they are in base-16 notation (for example: 1Fh or 0xA7). To convert a 2-digit hexadecimal number

to a regular number, multiply the first digit by 16 and add it to the second digit. For example, 3A = 3*16 + 10 = 58.

Character Area

Although each byte in a file can store a value from 0 to 255, what matters is what this data means. One way bytes are used is to assign a different letter or symbol to each possible value. For example, the byte value 65 could represent the character 'A' and the value 33 could represent the symbol '!'. The byte values 0 to 127 are usually assigned letters and symbols according to a standard called ASCII (although other standards exist). The character area on the right of the hex editor displays the ASCII representation of each of the bytes in the hexadecimal area. For example in Figure 2, the second byte of the file (5A) is displayed as 'Z' in the character area. Some byte values represent special codes that cannot be displayed in the character area. If there is no character that can be displayed, usually a '.' is displayed in the hex editor.

Address Area

The address area on the left side of the hex editor displays the address of the first byte of each line. The addresses are usually displayed in hexadecimal format, but many hex editors can display addresses in decimal format as well. In Figure 2, the address of the first byte of the first line would be 0, and the address of the first byte of the second line would be 0010h (or 16 in decimal format). Remember that addresses start from 0 so if you have a file of 512 bytes, the byte addresses would range from 0 up to 511. Some hex editors also have a ruler along the top of the hex editor to help you know the addresses of other bytes in the file.

Editing Data

Data can be edited in a hex editor just like a normal text editor. A hex editor has a cursor that can be moved by clicking with the mouse or using the cursor keys. Position the cursor over the byte you want to edit, and type the value you want to

change to using the keyboard. The cursor can be switched between the hexadecimal area and the character area by pressing the 'Tab' key. When the cursor is in the hexadecimal area, you have to enter byte values in hexadecimal notation, but when the cursor is in the character area, you can enter regular characters just like a text editor. Good hex editors always have an Overwrite mode and an Insert mode. In Overwrite mode, typing values on the keyboard just changes the existing byte values, but in Insert mode, typing on the keyboard inserts new bytes into the file. You can switch between Insert and Overwrite mode by pressing the 'Ins' key. Data can also be edited by selecting a set of bytes. Selections are made just like a text editor: click and drag the mouse or hold the 'Shift' key while moving the cursor. Once a selection has been made, the file can be edited using the standard Cut, Copy, and Paste commands on the Edit menu.

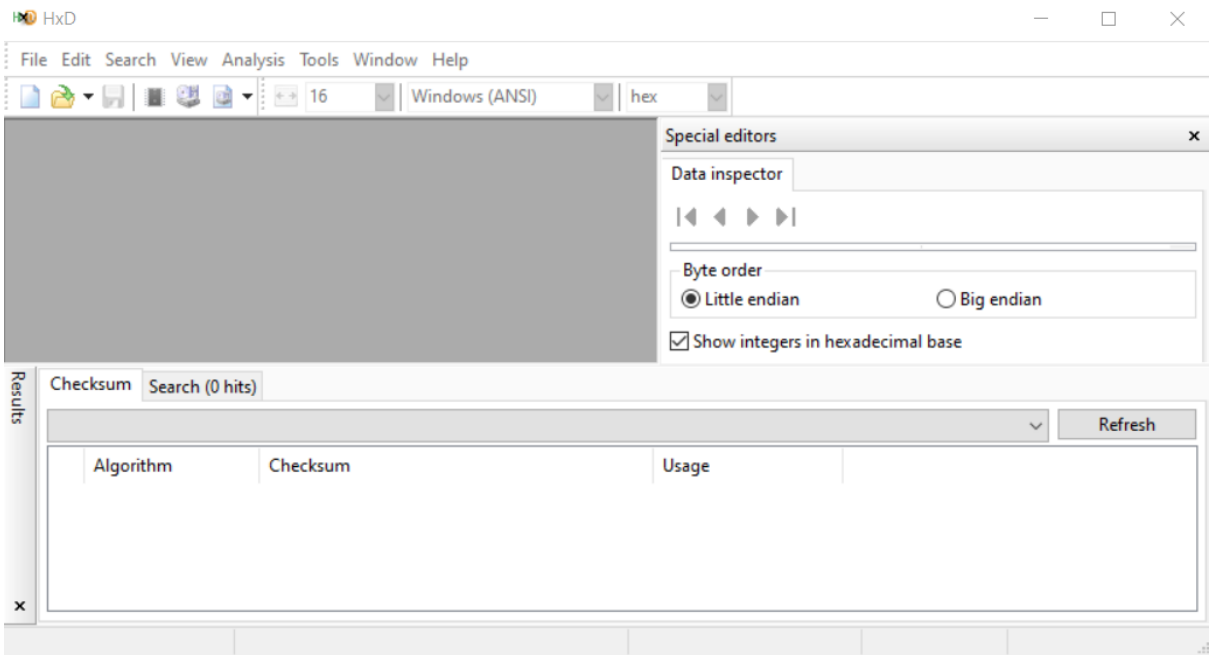
Advanced Features

The best hex editors in the world contain a whole host of other tools to help you work with binary files. For example, you could use a Find tool to locate certain bytes in a file, or a Binary Comparison tool to compare binary bytes between two files. Some hex editors can even edit the bytes of hard drives and processes just like you would a binary file. The most advanced feature of hex editors is now the ability to place a template over a file that allow you to understand what the bytes of a binary file actually mean.

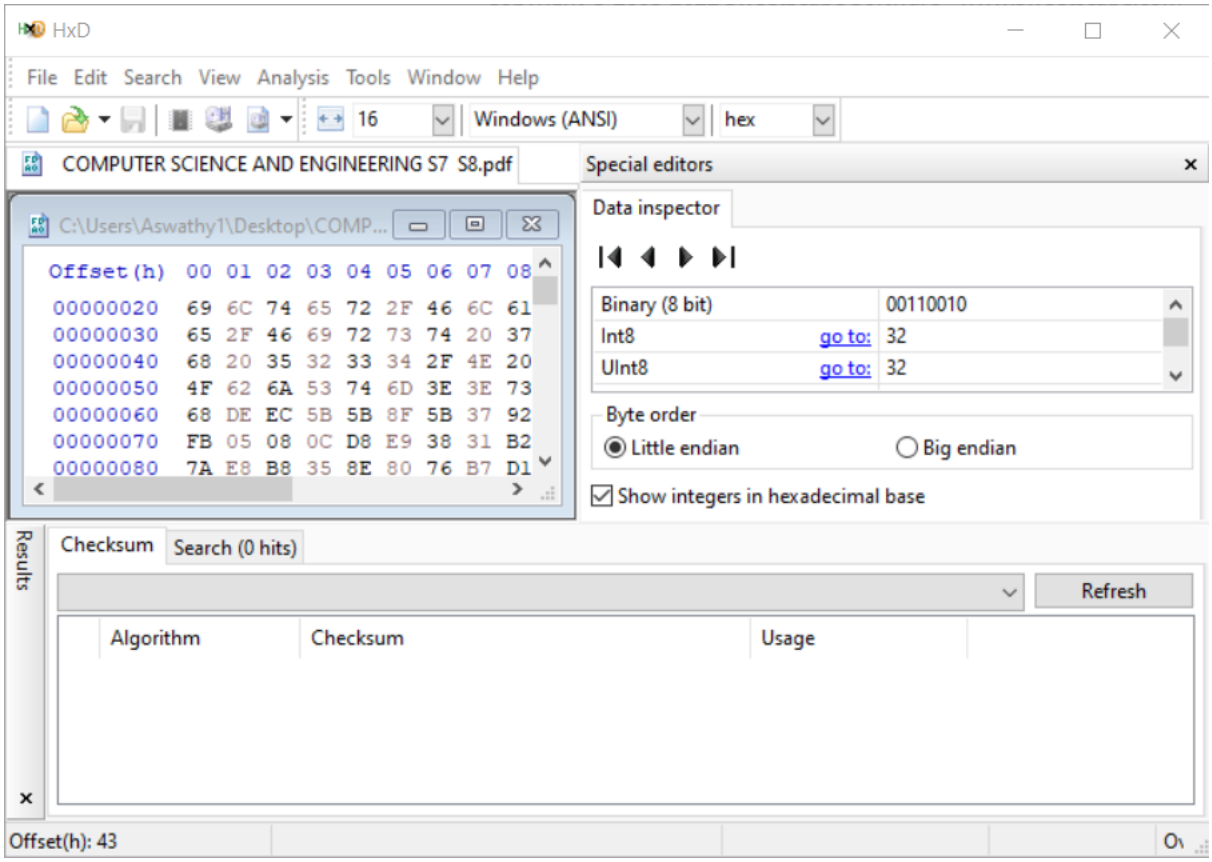
PROCEDURE

- The Hex Editor Window is the main method of viewing and editing binary files in 010 Editor (to edit text files see Using the Text Editor). A Hex Editor Window is displayed for each binary file that is loaded in the editor.
- Each file is displayed in a File Tab that displays a shortened form of the file name but the full file name can be viewed in the application title bar or in a hint popup displayed by placing the mouse cursor over the File Tab.

- The Hex Editor Window is divided into a left and a right area. By default, the left area displays the bytes of the file as a series of hexadecimal bytes and the right area displays the bytes as a series of characters.
- At the far right of the editor by the scroll bar, the Mini Map displays the bytes of the file interpreted as a set of colors. To the left of the Hex Editor Window is a list of addresses. Each address indicates the file position of the first byte on the line.
- At the top of the window a Ruler indicates the byte offsets from the address on that line. The editor can be changed to display data in a number of different formats and to modify how the Hex Editor Window displays data see Using Edit As.



Hex editor window

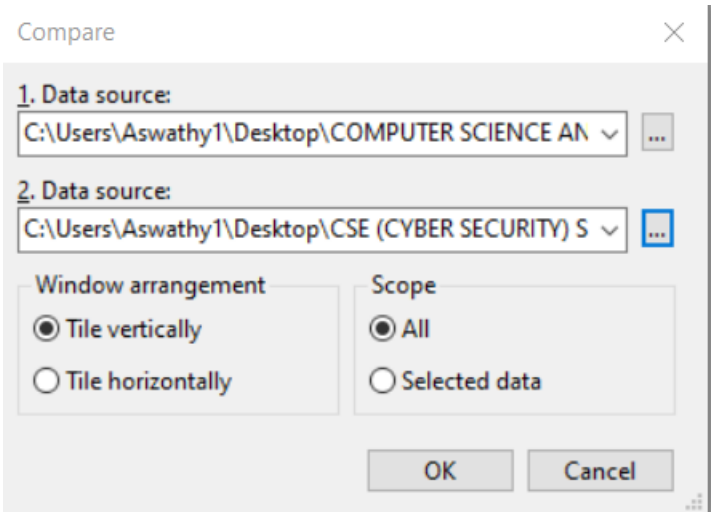


Hex value of a file

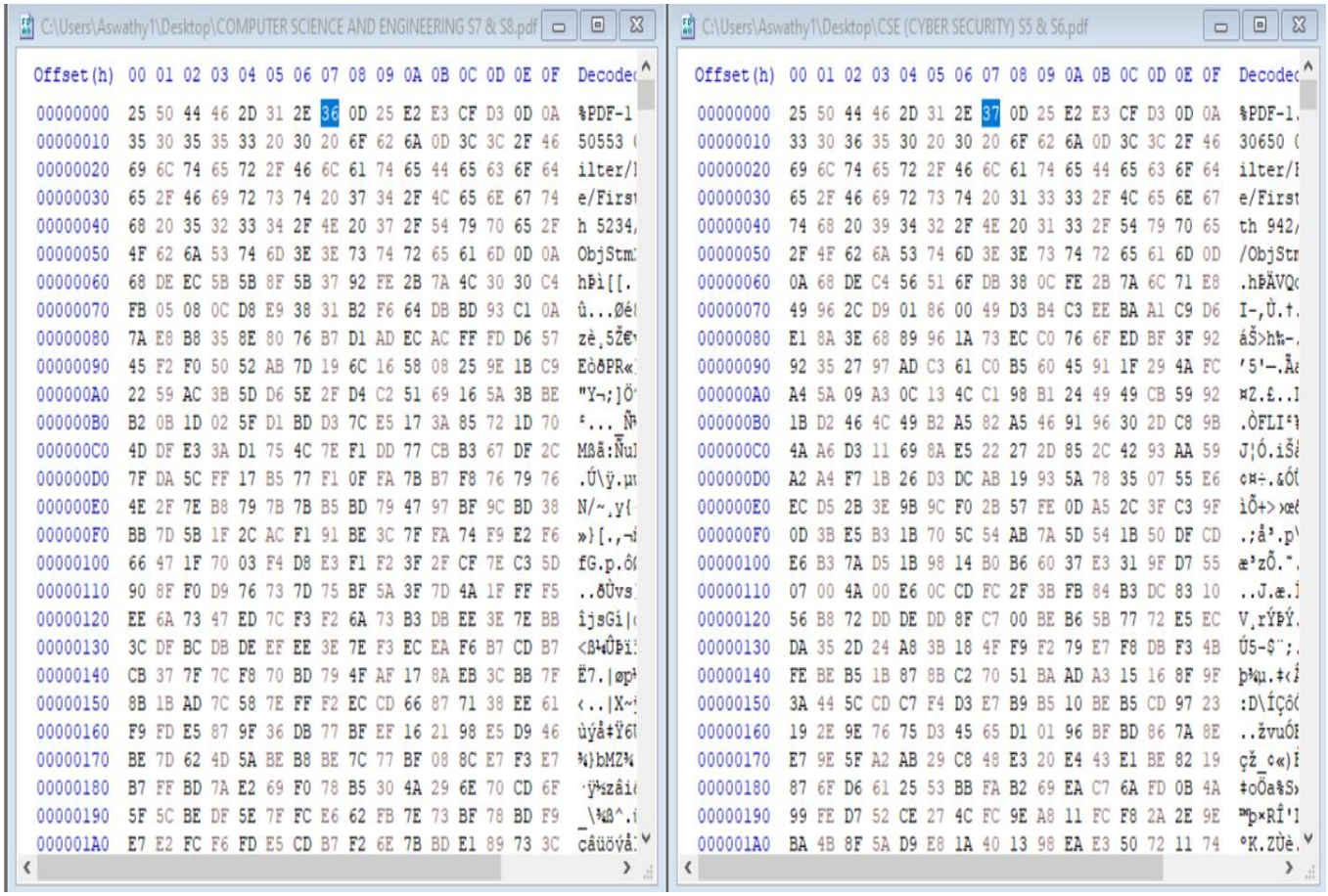
- The Compare Files tool allows the binary comparison of two files or two blocks of data for byte-by-byte differences. Note that this comparison is different than most text editors which only compare line-by-line. Access the Compare Files tool by clicking the 'Tools > Compare Files...' menu option.
- Enter the two files to compare in the File A and File B fields. Each field contains a drop-down list of all open files sorted alphabetically followed by a list of recent files sorted by access time. Click the browse button beside either field to use a file dialog box to select a file. Note that if exactly two files are open in the main Tab Group in 010 Editor, the file names for those two files will be automatically entered in these fields, otherwise the current file is listed in File A and the most recent compare is listed in File B.
- The Comparison tool supports two different algorithms: Binary and Byte by Byte. The Byte by Byte algorithm compares corresponding bytes between the two files (e.g. each byte at address n of file A is compared only against the

byte at address n of file B) and will usually run quickly. The Binary algorithm tries to identify blocks within the files that match. This algorithm is fast when the number of differences is low between the files, but slows down if a number of differences exist (the algorithm is O(d2) where d is the number of differences). Select which algorithm to use in the Comparison Type box.

- Two options exist for running comparisons in the Options box. If the Match Case toggle is enabled, then ASCII strings must match exactly, otherwise strings with a mixture of upper and lowercase letters will match. If the Enable Synchronized Scrolling toggle is enabled then after the comparison, scrolling one of the files will cause the other file to scroll as well. Synchronized scrolling can be turned off using the 'Window > Synchronize Scrolling' menu option (see the Window Menu for more information).

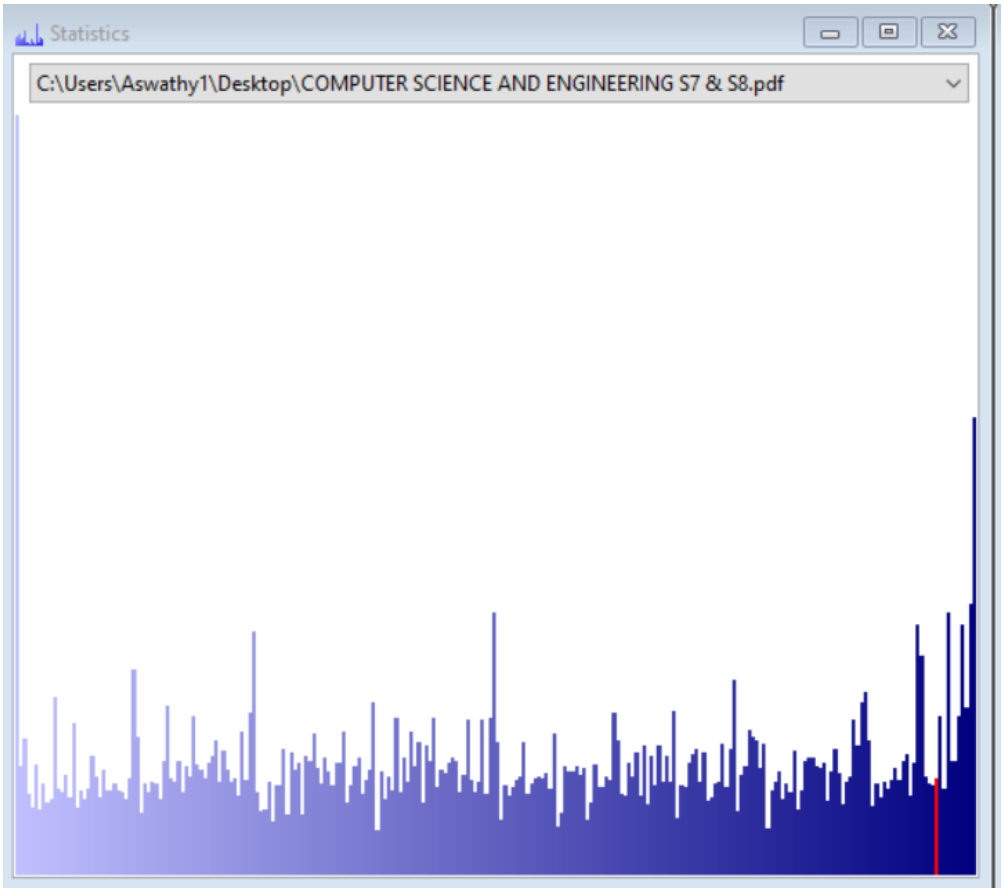


Selecting two files for comparison



Comparing two files with hex values

- Hex Editor Neo provides unique capability of calculating several file statistics. You may calculate General Statistics and Pattern Statistics for any opened document. In addition, Descriptive Statistics is calculated for both modes, and Entropy Analysis is performed for General Statistics mode.
- Statistics Tool Window is used to display the results of statistics calculations. To calculate statistics, open (or activate) the document for which you wish to calculate it, and execute the Tools » Statistics » Refresh command.
- Statistics is always calculated for the whole file, unless the selection is present in the current editor window. If selection is present, statistics calculation is limited to this selection. Multiple selections are fully supported.



Static analysis of a file

HASHCALC

AIM: To calculate the checksum values and HMACs for files as well as for text and hex strings.

DESCRIPTION:

A hash calculator can be several things but, in a very broad sense, refers to a program or function that accepts some type of input and then runs that input through an algorithm to create an output value, such as a large number or a block of symbols. The term often is used in data transmission to refer to a program that creates a type of key with an algorithm so anyone receiving the data transmitted can use the same algorithm to get the same key to see if the data arrived intact and unmodified. In computer programming, the term "hash calculator" can be used to indicate a hash function that turns some type of data into a hash key that then is processed by another algorithm to create an index into an array in which the information can be stored. Although both concepts of the calculator are similar, the results are very different and usually are not interchangeable. One common property of a hash calculator, regardless of its use, is that the hash value generated will always be the identical for a given piece of data, regardless of where or when the program is run.

At its core, a hash calculator is just a program or function that creates a hash from some data. A hash is just a word for a value and can be anything from a number to a string of hundreds of alphanumeric characters, depending on how it is being used. The data that are added to a hash calculator to create a hash also can be almost anything. When used for error checking in data transmission, the source for a hash value usually is a complete document or data file, such as an email or an image file. In programming, because the hash value is used to determine where data records are stored in a hash table, the input value usually is some part of a data record that is unique, such as the last name of a person, a phone number or

In the case of data transmission, a hash calculator uses any one of hundreds of different mathematical algorithms to create the unique hash value for the information being transmitted. This can be something as simple as adding all the values of all the bytes in a file, in which case the hash value is the sum. It also can be much more complex, involving counting blocks of bits or redundantly processing different sequences of numbers. One of the most important aspects of any hash algorithm, however, is that the resulting hash value must always be the same if the same data is used as input. This concept means that, if a file is transmitted with its own calculated hash value, then the receiver of the data can use a hash calculator with the same algorithm to determine if the hash values for the data match, verifying that the data were received intact and without errors or changes.

In programming, the term "hash calculator" frequently is used to describe a function that converts a piece of datum into a hash value. Unlike data transmission, the number generated by the calculator in this instance is not necessarily used for verification but to calculate an index into a hash table where the information will be stored. An intermediary hash value is calculated to allow for a larger number of data records to be predictably placed into a smaller hash table, with some records generating the same values under certain circumstances. Both the algorithm used to calculate a hash value and the data used as input are fairly arbitrary for a hash table and usually application-specific.

PROCEDURE:

- HashCalc is a fast and easy-to-use calculator that allows to compute checksum values and HMACs for files, as well as for text and hex strings. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.
- Checksum is a calculated value that is used to determine the integrity of data. The sender of the data calculates checksum value by taking the sum of the

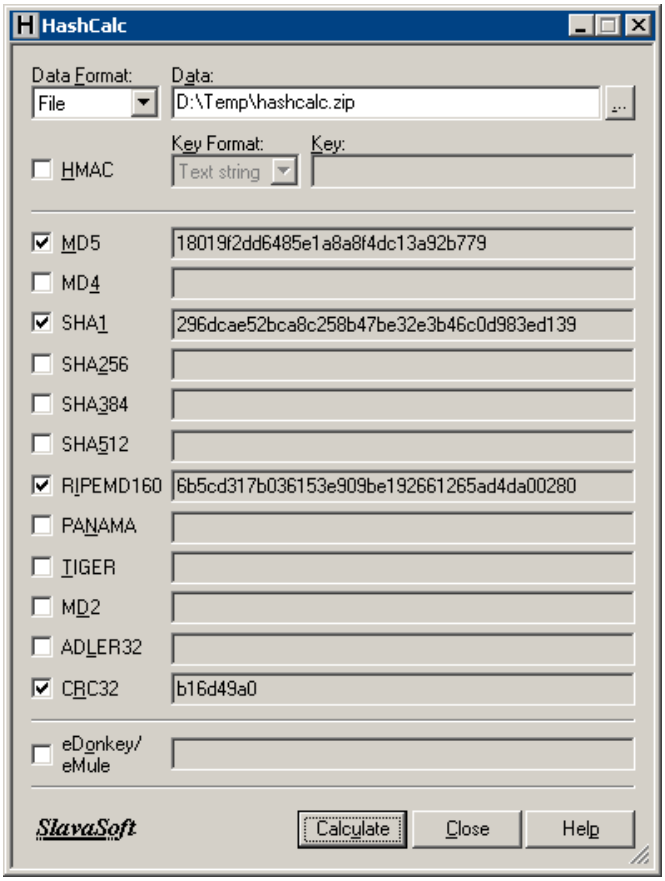
binary data transmitted. When receiving the data, the receiver can perform the same calculation on the data and compare it with the checksum value provided by the sender. If the two values match, the receiver has a high degree of confidence that the data was received correctly.

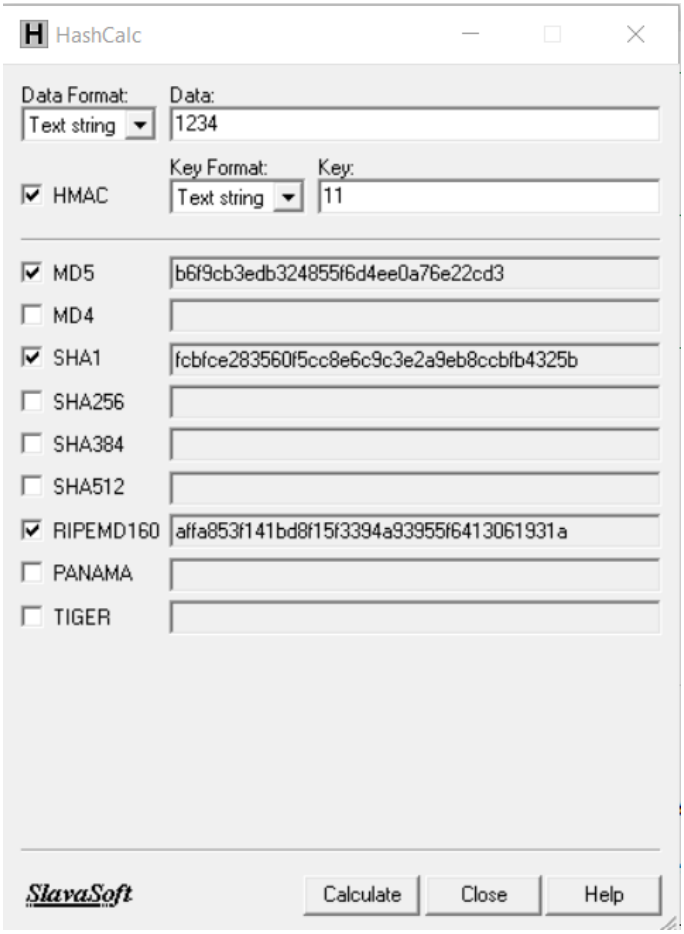
- Checksum value is also called hash value. The data that is calculated can be a file, a text string, or a hexadecimal string.
- The most commonly used checksum is MD5 (Message-Digest algorithm 5) hash. MD5 was designed by Professor Ronald L. Rivest in 1991 to replace an earlier hash function, MD4. MD5 checksum is a 128-bit hash value (32 characters).
- In practice, checksum value is mainly used in two situations.

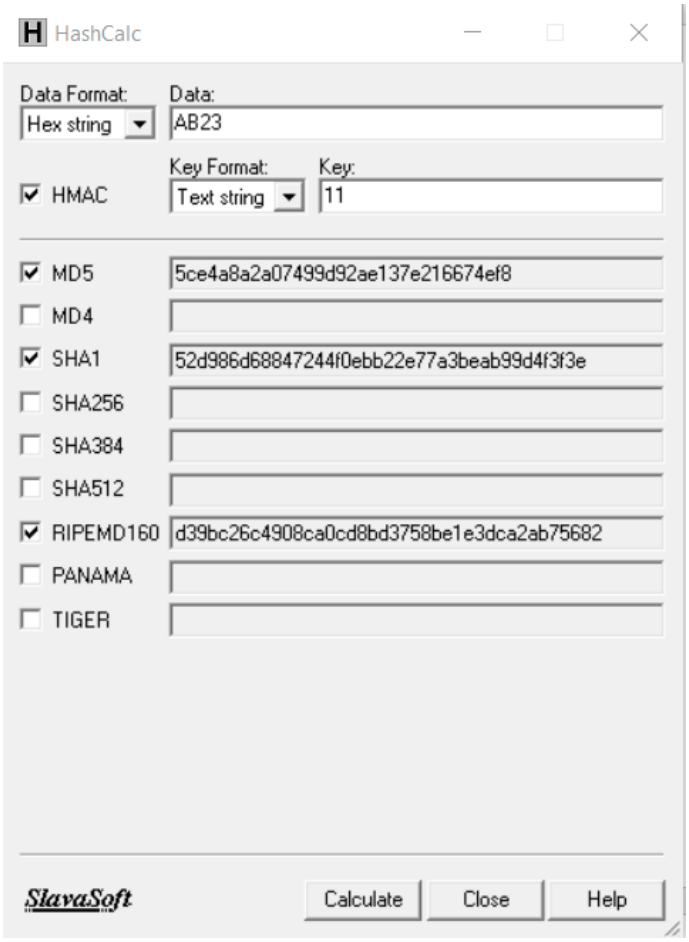
✓ First, it can be used to check data integrity when data is sent through telecommunication networks such as Internet.

✓ Second, it can be used to check data integrity of stored data to see if the data has been modified or changed in any way over time.

- HashCalc is such a free utility that you can easily install to calculate checksum values of any files.


HashCalc
Data Format:
File
Data:
D:\Temp\hashcalc.zip
...
HMAC
Key Format:
Text string
Key:
MD5
18019f2dd6485e1a8a8f4dc13a92b779
MD4
SHA1
296dcae52bca8c258b47be32e3b46c0d983ed139
SHA256
SHA384
SHA512
RIPEMD160
6b5cd317b036153e909be192661265ad4da00280
PANAMA
TIGER
MD2
ADLER32
CRC32
b16d49a0
eDonkey/
eMule
SlavaSoft
Calculate
Close
Help


HashCalc
Data Format:
Text string
Data:
1234
HMAC
Key Format:
Text string
Key:
11
MD5
b6f9cb3edb324855f6d4ee0a76e22cd3
MD4
SHA1
fcbfce283560f5cc8e6c9c3e2a9eb8ccbfb4325b
SHA256
SHA384
SHA512
RIPEMD160
affa853f141bd8f15f3394a93955f6413061931a
PANAMA
TIGER
SlavaSoft
Calculate
Close
Help


HashCalc
Data Format:
Hex string
Data:
AB23
HMAC
Key Format:
Text string
Key:
11
MD5
5ce4a8a2a07499d92ae137e216674ef8
MD4
SHA1
52d986d68847244f0ebb22e77a3beab99d4f3f3e
SHA256
SHA384
SHA512
RIPEMD160
d39bc26c4908ca0cd8bd3758be1e3dca2ab75682
PANAMA
TIGER
SlavaSoft
Calculate
Close
Help

REGEDIT

AIM:

To Familiarize the Windows Registry and Registry Editor

DESCRIPTION:

The Windows Registry also holds information regarding recently accessed files and considerable information about user activities, besides configuration information. Hence, this article serves the purpose is to provide you with a depth understanding of the Registry and Wealth of information it holds. Today most administrators and forensic analysts, the registry probably looks like the entrance to a dark.

The system was largely managed by several files-specifically, autoexec.bat, config.sys, win.ini (on windows) and system.ini. So, various settings within these files determined what programs were loaded and how the system looked and responded to user input, a central hierarchical database that maintains configuration settings for the application, hardware devices, and users. When the administrator or Forensics expects opens Regedit.exe, he sees a tree-like structure with five root folders, or "hives". HKEY_CLASSES_ROOT hive contains configuration information relating to which application is used to open various files on the system.

- HKEY_CURRENT_USER − loaded user profile for the currently logged-on-user.
- HKEY_LOCAL_MACHINE−contains a vast configuration information for the system, including hardware settings and software settings.
- HKEY_USERS− contains all the actively loaded user profile for that system
- HKEY_CURRENT_CONFIG−contains the hardware profile the system uses at startup.

PROCEDURE:

Suppose your computer lies in the hand of a malicious person without your consent. Then how can you determine, what exactly he would have done to your computer. You can track his activity through inspecting the registry as follows −

Most Recent User list

(HKEY_CURRENT_USER\software\microsoft\windows\currentversion\Explorer\RunMRU)

It contains with the information provided from the RunMRU key, an examiner can gain better understanding fo the user they are investigating and the application that is being used. In this above figure, you can see the user has opened cmd, Notepad, MSPaint etc.

USB Connection

(HKEY_LOCAL_MACHINE\SYSTEM\controlset001\Enum\USBSTOR.)

This key stores the contents of the product and device ID values of any USB devices that have ever been connected to the system.

Attached Hardware List –

(HKEY_LOCAL_MACHINE\SYSTEM|MountedDevices.)

This information can be useful to a forensic examiner as it shows any connected storage device has been recognized by the operating system. If the examiner notes a discrepancy between the physically attached devices and the ones reported here, it can be an indication that some device was removed prior to the evidence being seized.

Malicious Software Running − (HKEY_CURRENT_USER\Software\ )

This information will be quite informatic for Forensics Examiner as it could see the hacker used VPN such as CyberGhost which is used for being anonymous.

Recent Applications Used−

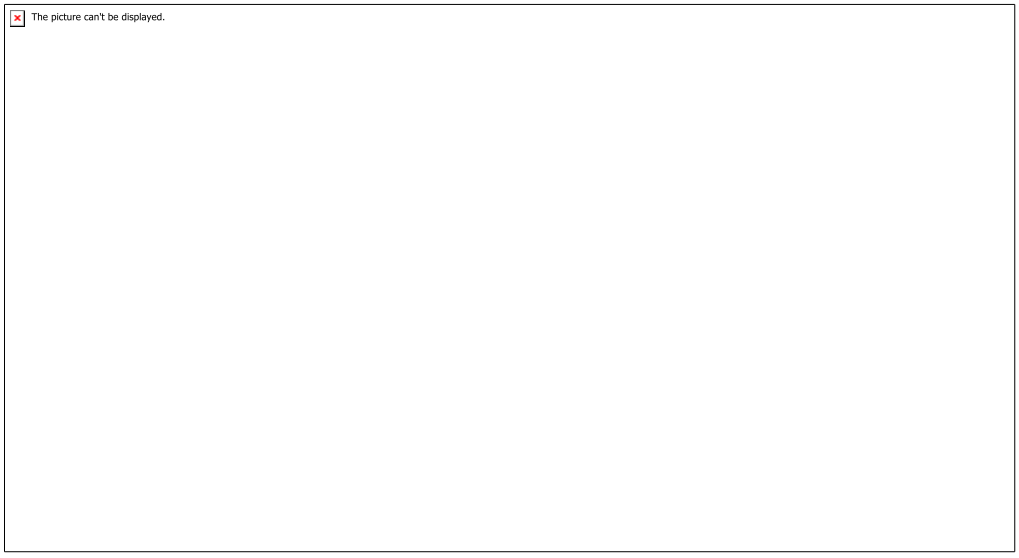
(HKEY_CURRENT_USER\SOFTWARE\Microsoft\Currentversion\Search\RecentApps)

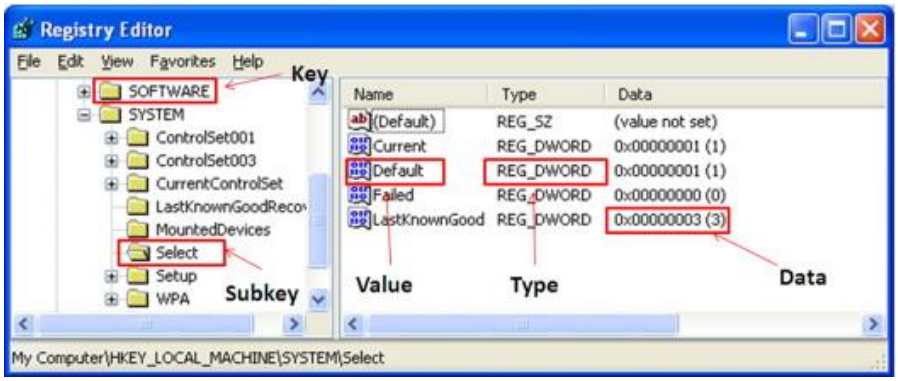
By navigating to the said key will give information for last accessed applications list by the user.

Internet Explorer information

(HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\TypedURL.)

Internet Explorer is the native Web browser in Windows operating system. It utilizes the Registry extensively in the storage of data, like many applications. From the said key, we can obtain such information.





HTTRACK

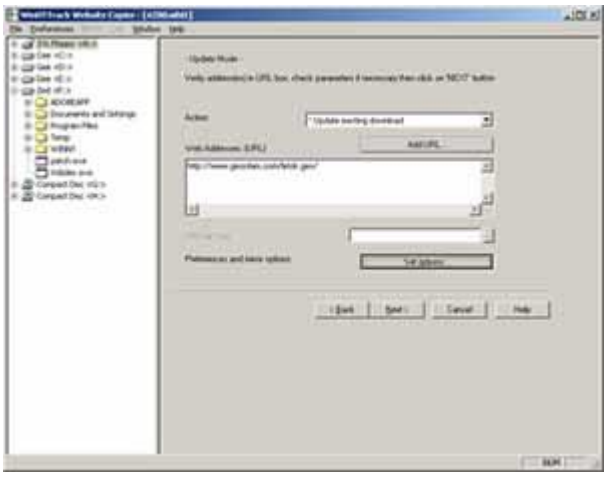
AIM:

To familiarize the cyber forensic tool httrack

DESCRIPTION:

HTTrack is an easy-to-use offline browser utility. It allows you to download a World Wide Website from the Internet to a local directory, building recursively all directories, getting html, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system.

WinHTTrack (Windows release of HTTrack) and WebHTTrack (Linux/Unix release of HTTrack) are very similar, but not exactly identical. You may encounter minor differences (in the display, or in various options) between these two releases. The engine behind these two release is identical.



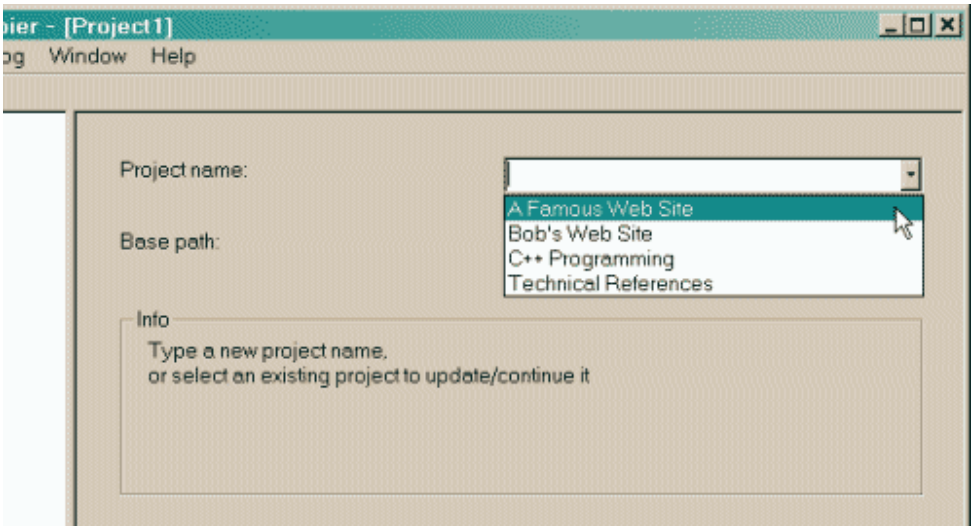
PROCEDURE:

Step 1: Choose a project name and destination folder

- Change the destination folder if necessary

  It is more convenient to organize all mirrors in one directory, for example My Web Sites.If you already have made mirrors using HTTrack, be sure

- Select a new project name OR select an existing project for update/retry



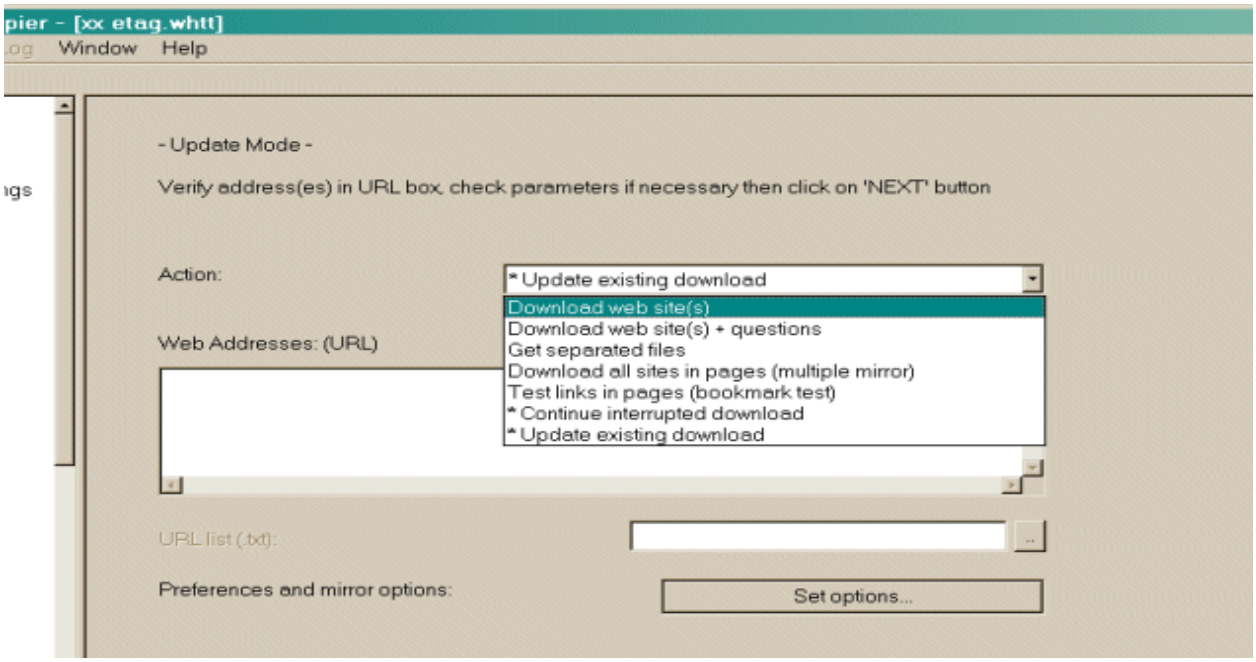
- Click on the NEXT button

Step 2 : Fill the addresses

Select an action,the default action is Download web sites

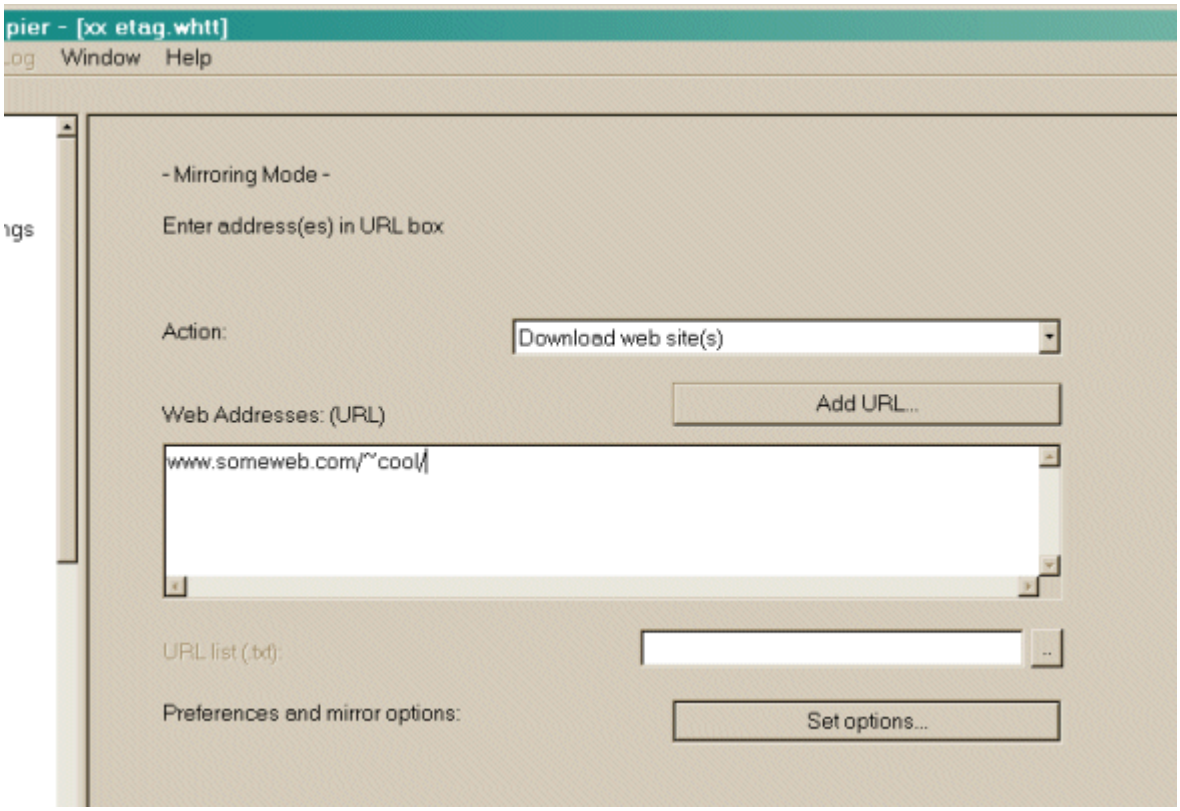
- ✓ *Download web site(s)* Will transfert the desired sites with default options
- ✓ *Download web site(s) + questions* Will transfert the desired sites with default options, and ask questions if any links are considered as potentially downloadable
- ✓ *Get individual files* Will only get the desired files you specify (for example, ZIP files), but will not spider through HTML files

- ✓ *Download all sites in pages* (multiple mirror) Will download all sites that appears in the site(s) selected. If you drag&drop your boormark file, this option lets you mirror all your favorite sites
- ✓ *Test links in pages* (bookmark test) Will test all links indicated. Useful to check a bookmark file
- ✓ *Continue interrupted download* Use this option if a download has been interrupted (user interruption,crash..)
- ✓ *Update existing download* Use this option to update an existing project. The engine will recheck the complete structure, checking each downloaded file for any updates on the web site.



- Enter the site's addresses

  You can click on the *Add a URL* button to add each address, or just type them in the box



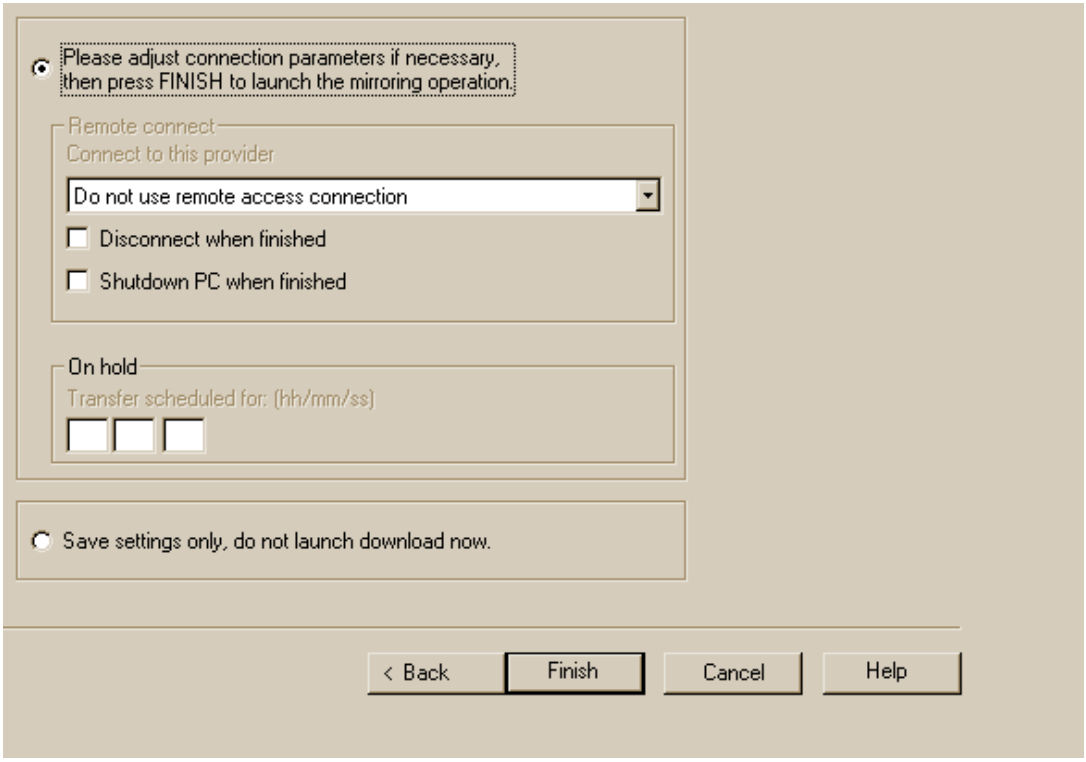
- You may define options by clicking on the **Set options** button.You can define filters or download parameters in the option panel.
- You may also add a URL by clicking on the **Add a URL** button.This option lets you define additional parameters (login/password) for the URL, or capture a complex URL from your browser.
- Click on the NEXT button.

Step 3 : Ready to start

- If you want, you may connect immediately or delay the mirrorIf you don't select anything, HTTrack will assume that you are already connected to the Internet and that you want to start the mirror action now
    - Connect to this provider, you can select here a specific provider to connect to when begining the mirror if you are not already connected to the Internet.

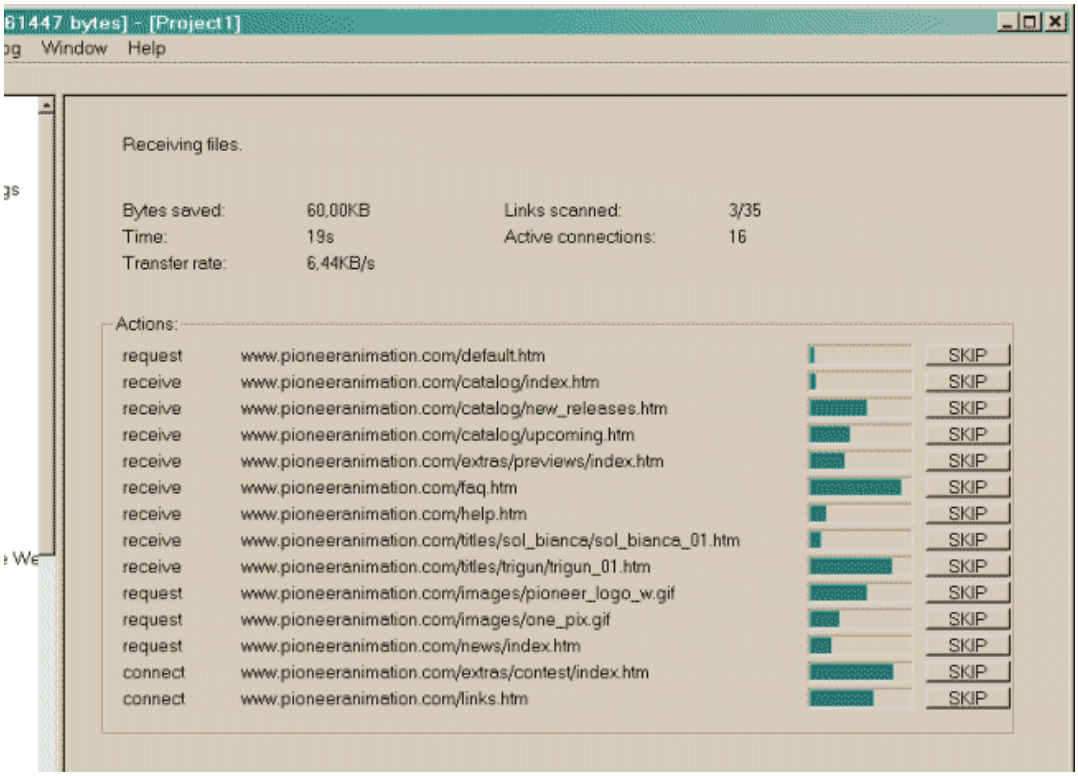
- Disconnect when finished ,Click on this checkbox to ask httrack to disconnect the network when mirror is finished.
- Shutdown PC when finished,Click on this checkbox to ask httrack to shutdown your computer when mirror is finished.
- On Hold,you can enter here the time of the mirror start. You can delay up to 24 hours a mirror using this feature.

- Click on the FINISH button

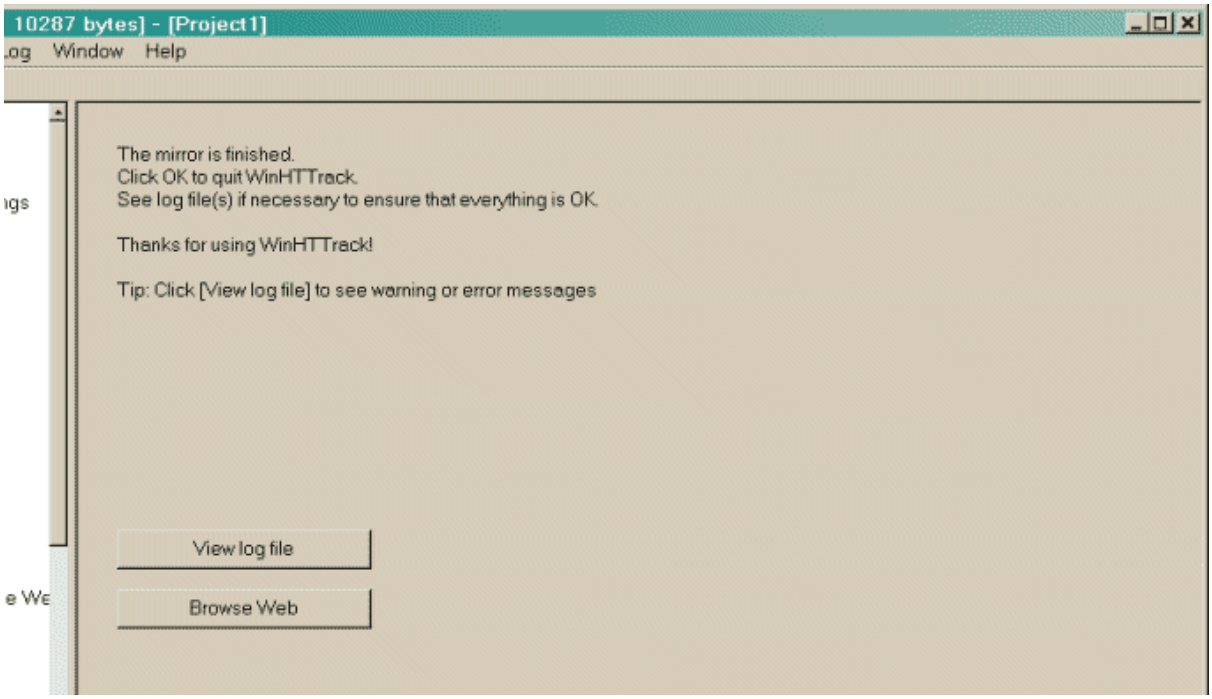


Step 4 : Wait

Wait until the mirror is finishing,You can cancel at any time the mirror, or cancel files currently downloaded for any reasons (file too big, for example)Options can be changed during the mirror: maximum number of connections, limits...



Step 5 : Check the result ,You may check the error log file, which could contain useful information if errors have occurred.



WIRESHARK

AIM:

To provide deeper understanding of Network Protocol Analysis using Wireshark

DESCRIPTION:

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Wireshark can be used in the following ways:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyze dropped packets.
- It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

Wireshark is similar to tcpdump in networking. Tcpdump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic

end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or port mirroring is used to extend capture at any point.

Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

Features of Wireshark

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.
- It can also capture raw USB traffic.
- Various settings, like timers and filters, can be used to filter the output.
- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

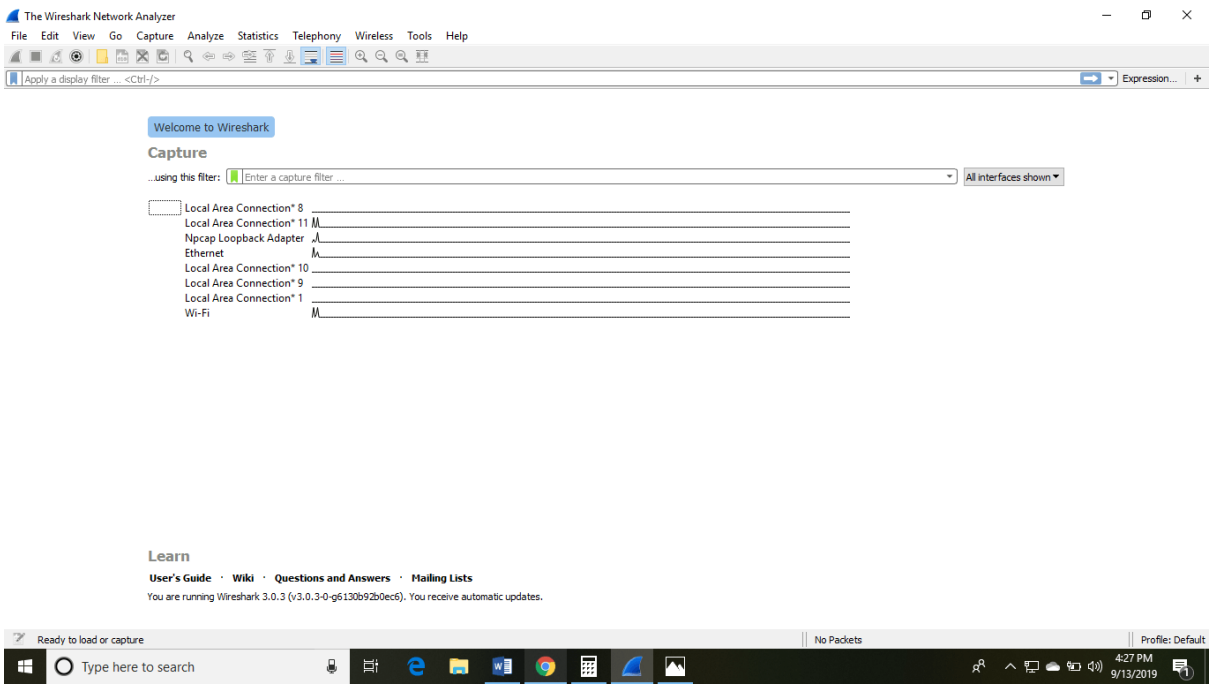
PROCEDURE

Below are the steps to install the Wireshark software on the computer:

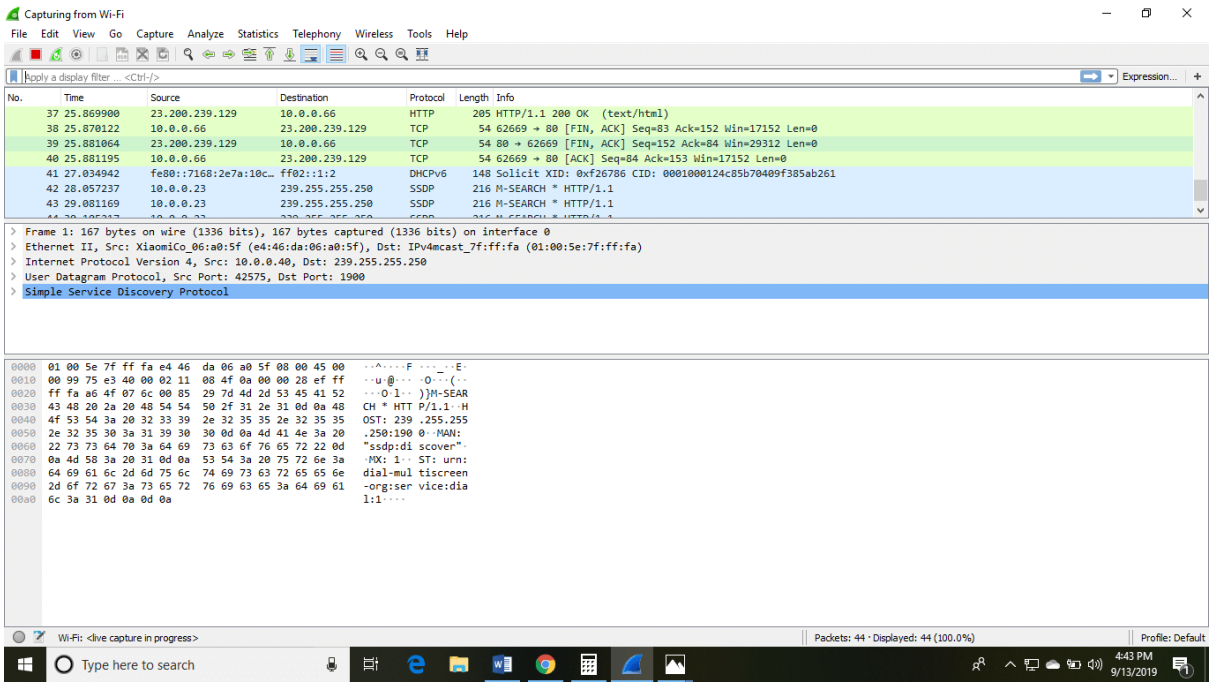
- Open the web browser.
- Search for 'Download Wireshark.'
- Select the Windows installer according to your system configuration, either 32-bt or 64-bit. Save the program and close the browser.
- Now, open the software, and follow the install instruction by accepting the license.

The Wireshark is ready for use.

On the network and Internet settings option, we can check the interface connected to our computer.If you are Linux users, then you will find Wireshark in its package repositories.By selecting the current interface, we can get the traffic traversing through that interface. The version used here is 3.0.3. This version will open as:



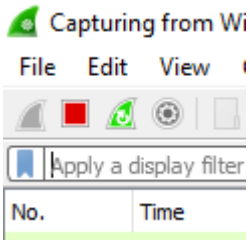
The Wireshark software window is shown above, and all the processes on the network are carried within this screen only. The options given on the list are the Interface list options. The number of interface options will be present. Selection of any option will determine all the traffic. For example, from the above fig. select the Wi-Fi option. After this, a new window opens up, which will show all the current traffic on the network. Below is the image which tells us about the live capture of packets and our Wireshark will look like:



The above arrow shows the packet content written in hexadecimal or the ASCII format. And the information above the packet content, are the details of the packet header.

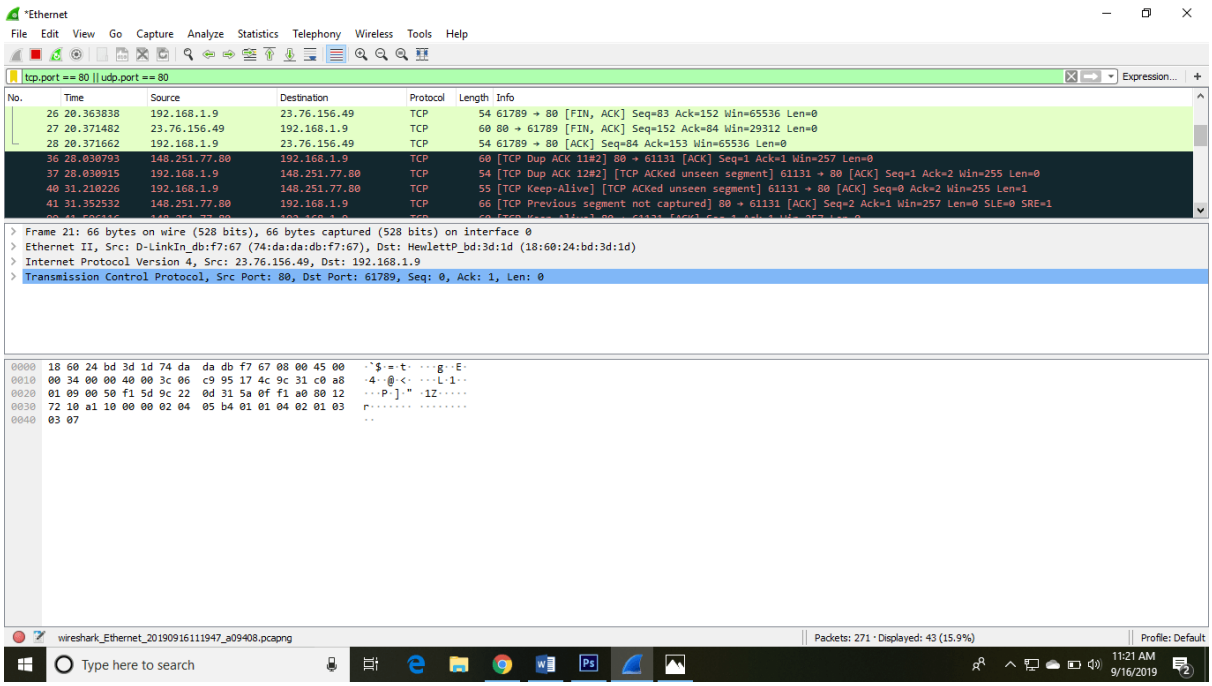
It will continue listening to all the data packets, and you will get much data. If you want to see a particular data, then you can click on the red button. The traffic will be stationary, and you can note the parameters like time, source, destination, the protocol being used, length, and the Info. To view in-depth detail, you can click on that particular address; a lot of the information will be displayed below that.

There will be detailed information on HTTP packets, TCP packets, etc. The red button is shown below:



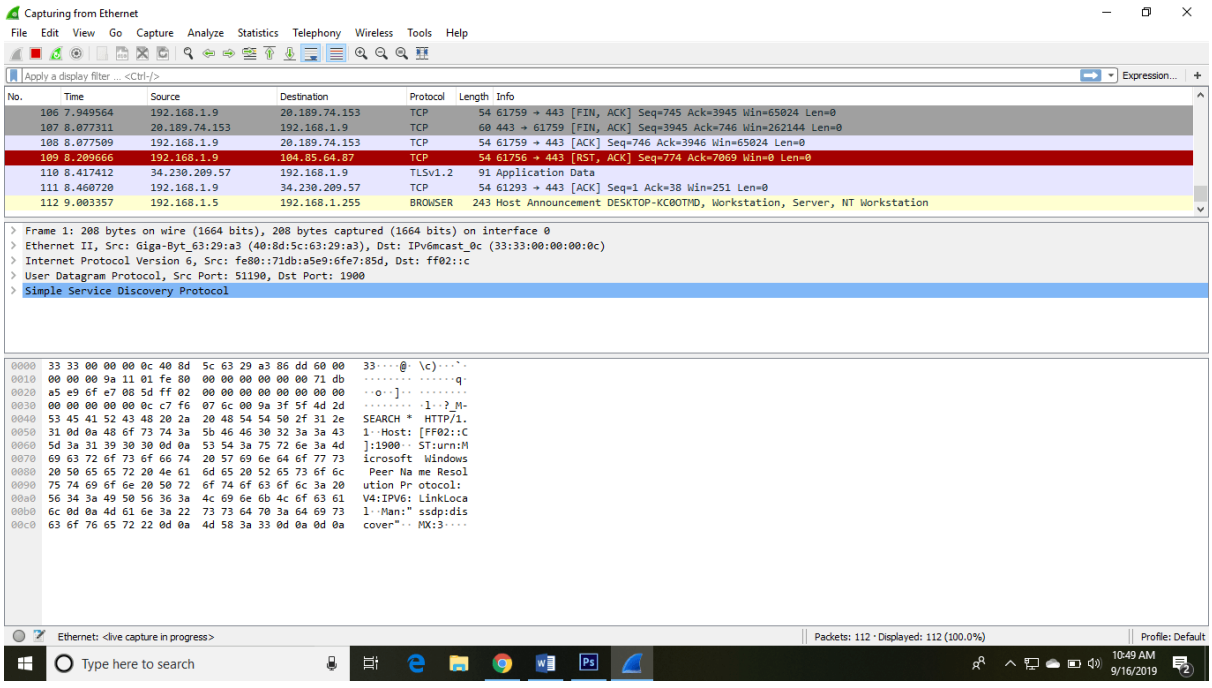
The screen/interface of the Wireshark is divided into five parts:

- ✓ First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.
- ✓ The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.
- ✓ Next comes the packet header- detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.
- ✓ The bottom window called the packet contents window, which displays the content in ASCII and hexadecimal format.
- ✓ At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:

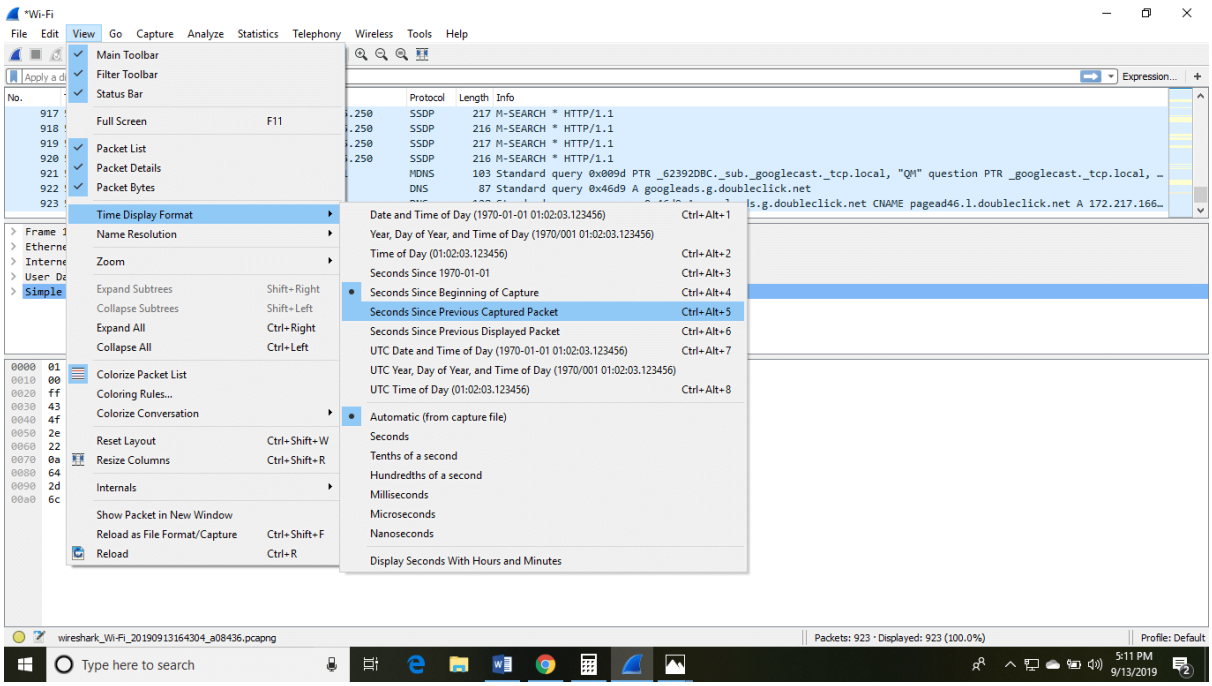


You can also select the connection to which your computer is connected. For example, in this PC, we have chosen the current network, i.e., the ETHERNET.

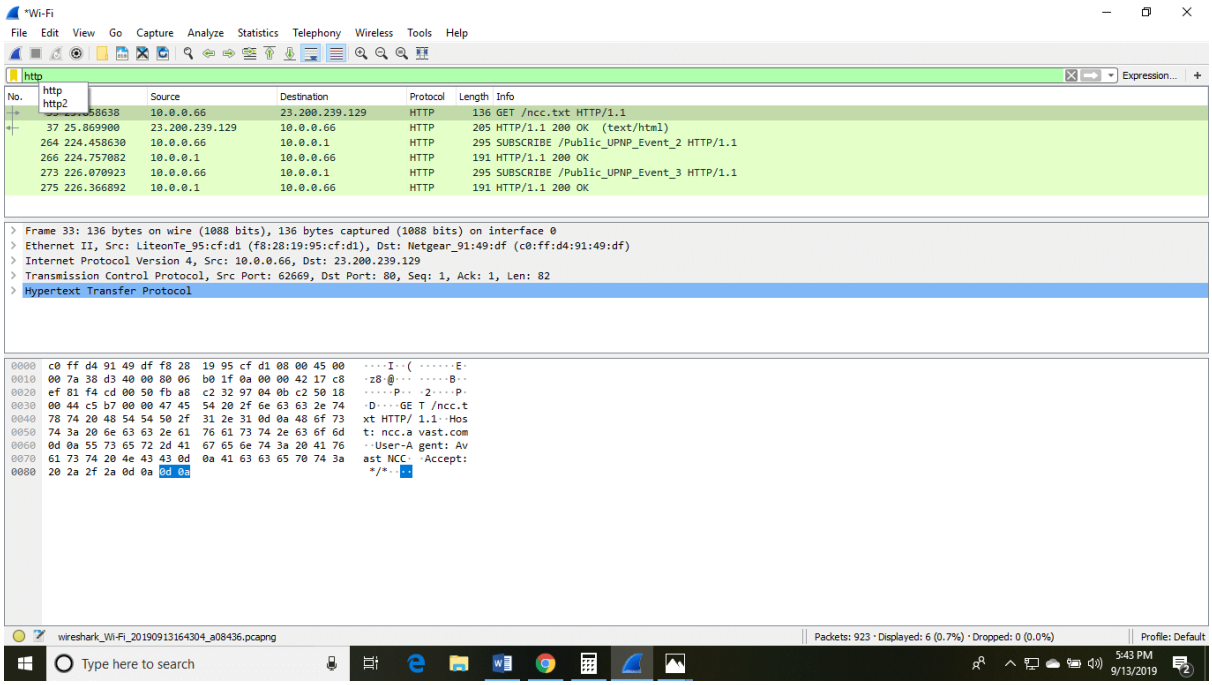
After connecting, you can watch the traffic below:



In view option on the menu bar, we can also change the view of the interface. You can change the number of things in the view menu. You can also enable or disable any option according to the requirements.

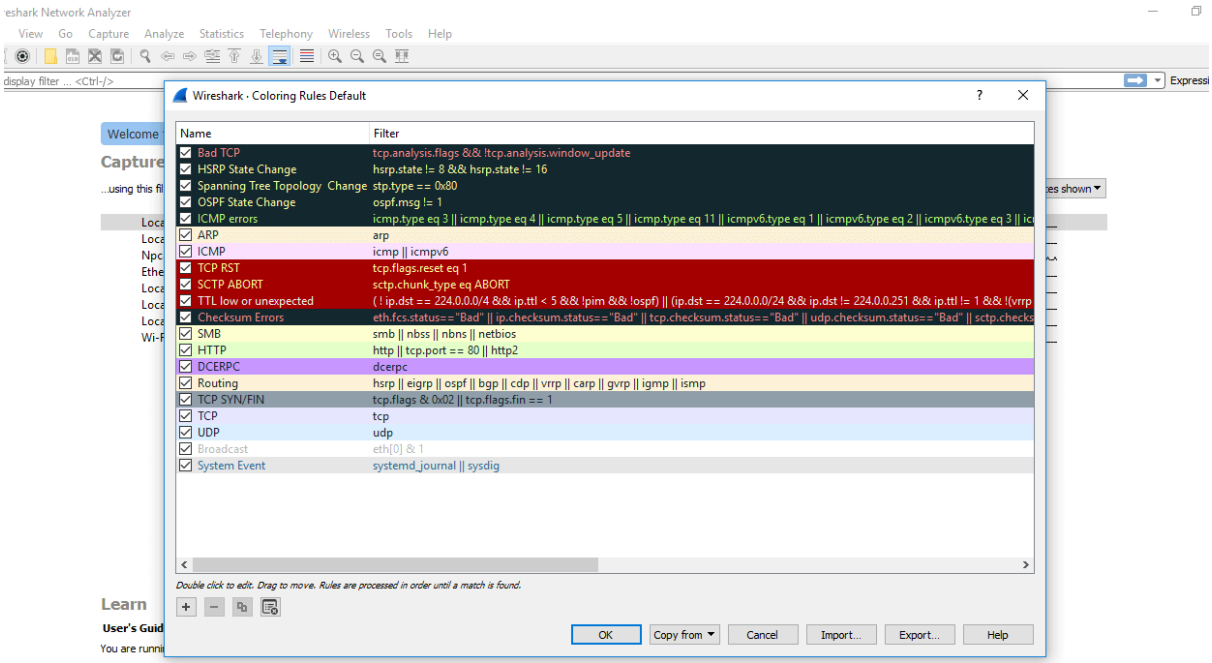


There is a filter block below the menu bar, from where a large amount of data can be filtered. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed.



If you want to filter according to the source, right-click on the source you want to filter and select 'Apply as Filter' and choose '...and filter.'

Steps for the permanent colorization are: click on the 'View' option on the menu bar and select 'Coloring Rules.' The table will appear like the image shown below:



For the network administrator job, advanced knowledge of Wireshark is considered as the requirements. So, it is essential to understand the concepts of the software. It contains these 20 default coloring rules which can be added or removed according to the requirements. Select the option 'View' and then choose 'Colorize Packet List,' which is used to toggle the color on and off. Whenever we type any commands in the filter command box, it turns green if your command is correct. It turns red if it is incorrect or the Wireshark does not recognize your command.

If you have a Linux system, you'd install Wireshark using the following sequence (notice that you'll need to have root permissions):

$ sudo apt-get install wireshark

$ sudo dpkg-reconfigure wireshark-common

$ sudo usermod -a -G wireshark $USER

$ newgrp wireshark

Once you have completed the above steps, you then log out and log back in, and then start Wireshark:

$ wireshark

Wireshark tries to help you identify packet types by applying common-sense color coding. The table below describes the default colors given to major packet types.

Color in Wireshark	Packet Type
Light purple	TCP
Light blue	UDP
Black	Packets with errors
Light green	HTTP traffic
Light yellow	Windows-specific traffic, including Server Message Blocks (SMB) and NetBIOS

Color in Wireshark	Packet Type
Dark yellow	Routing
Dark gray	TCP SYN, FIN and ACK traffic

In Wireshark, just go to Statistics >> I/O Graph, and you'll see a graph similar to the one below:

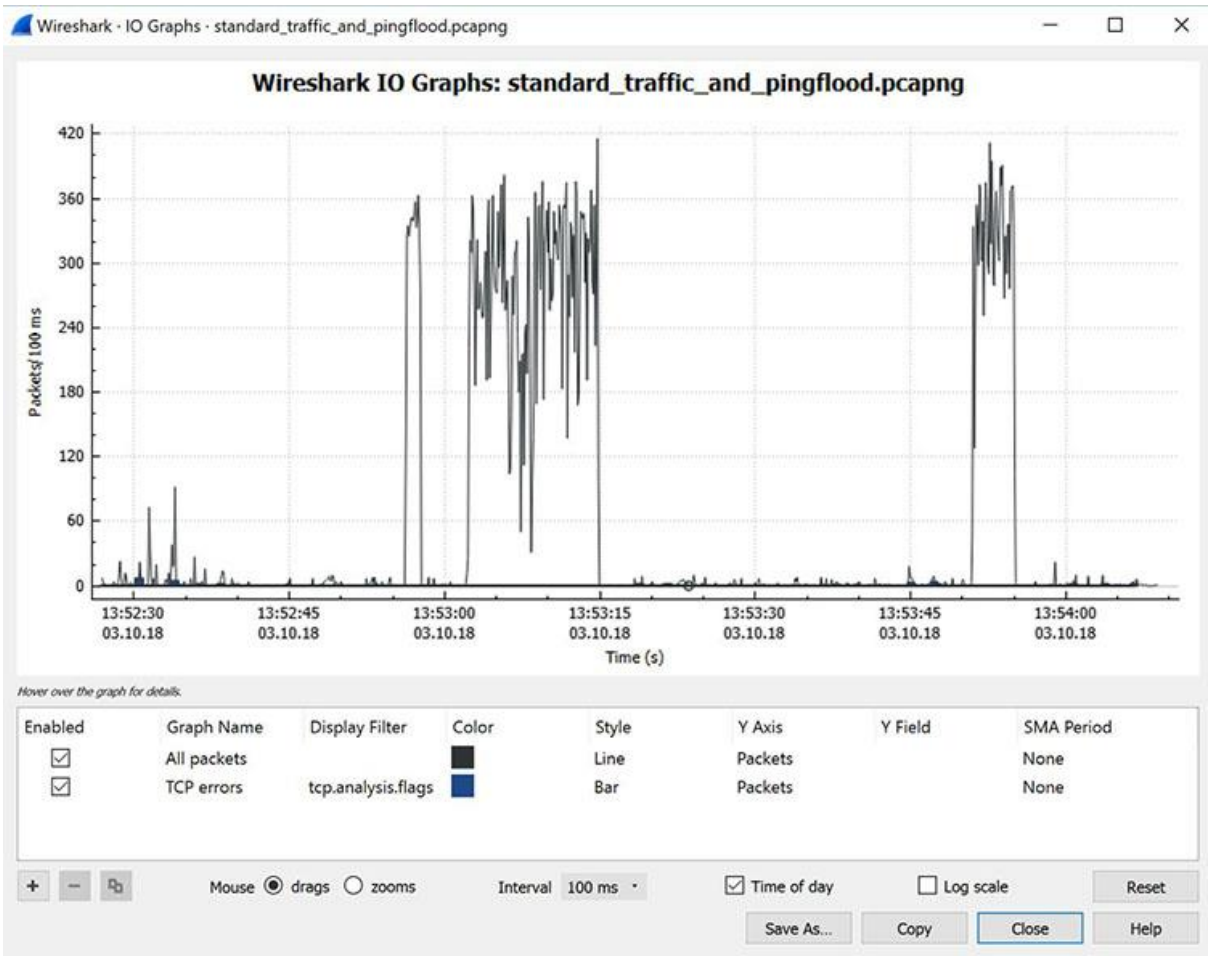


Figure : Viewing the input/output traffic graph in Wireshark

This particular graph is showing typical traffic generated by a home office. The spikes in the graph are bursts of traffic that were caused by generating a Distributed Denial of Service (DDoS) attack using a few Linux systems.

In this case, three major traffic bursts were generated. Many times, cybersecurity pros use Wireshark as a quick and dirty way to identify traffic bursts during attacks.

It's also possible to capture the amount of traffic generated between one system and another. If you go to Statistics and then select Conversations, you will see a summary of conversations between end points, as shown below in Figure.

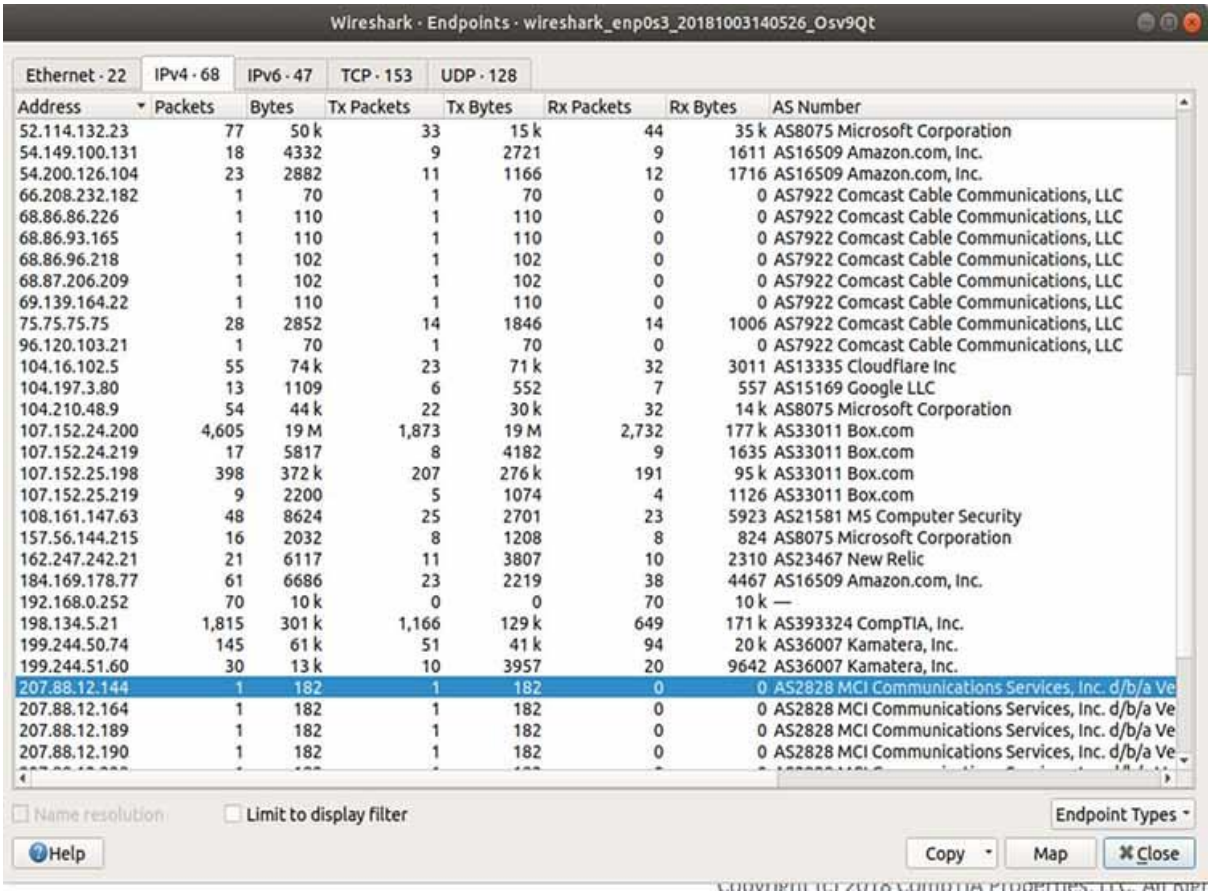


Figure: Viewing endpoint conversations in Wireshark

In the above case, Wireshark was used to see if an old piece of equipment from MCI communications that was running on a client's network could be traced.

It turned out that the client didn't know this device was even on the network. Thus, it was removed, helping to make the network a bit more secure. Notice, also, that this

network connection is experiencing a lot of traffic to Amazon (administering a server in AWS at the time) and Box.com (using Box for system backup at the time).

In some cases, it is even possible to use Wireshark to identify the geographic location of source and destination traffic. If you click on the Map button at the bottom of the screen , Wireshark will show you a map, providing its best guess of the location of the IP addresses you've identified.

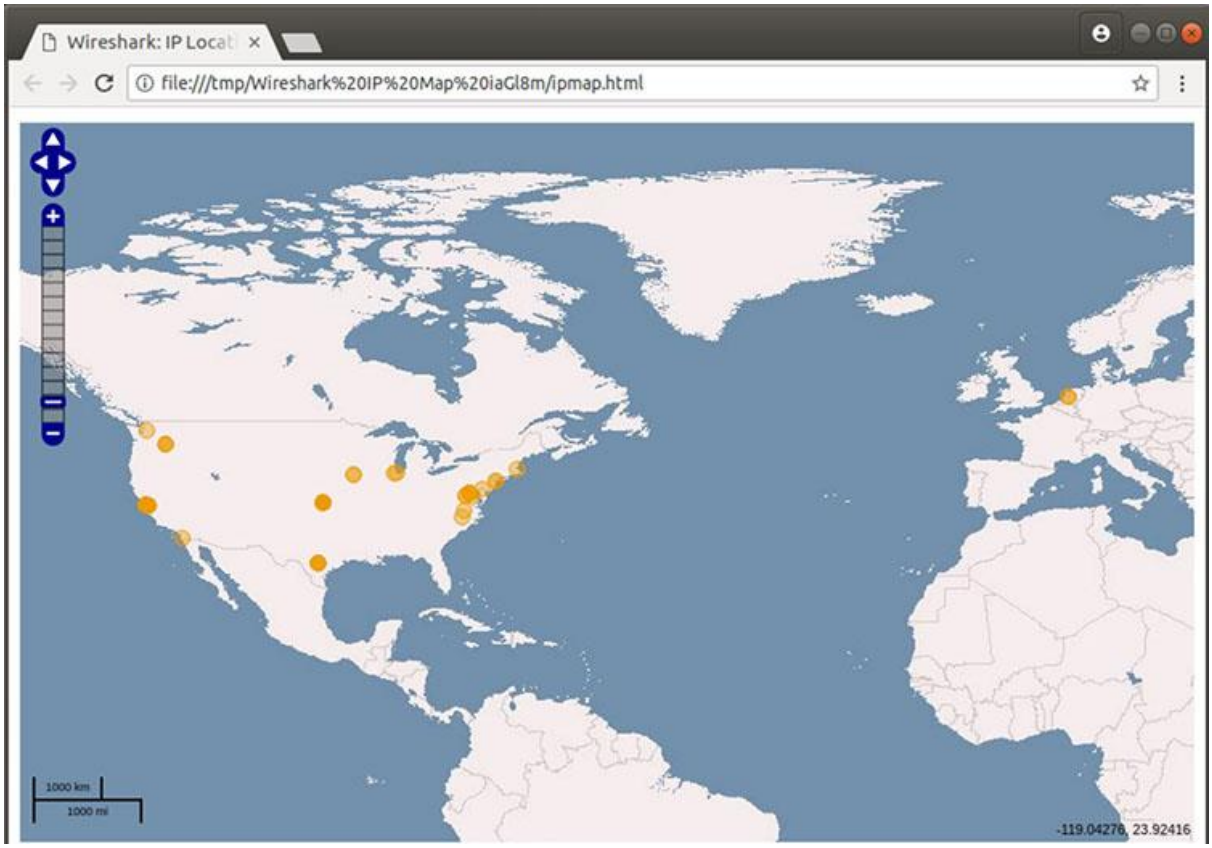


Figure: Viewing geographic estimations in Wireshark

Because IPv4 addresses can be easily spoofed, you can't rely completely on this geographical information. But it can be fairly accurate.

You can apply Wireshark filters in two ways:

1. In the Display Filter window, at the top of the screen
2. By highlighting a packet (or a portion of a packet) and right-clicking on the packet

Wireshark filters use key phrases, such as the following:

`ip.addr`	Specifies an IPv4 address
`ipv6.addr`	Specifies an IPv6 address
`src`	Source - where the packet came from
`dst`	Destination - where the packet is going

You can also use the following values:

`&&`	Means “and,” as in, “Choose the IP address of 192.168.2.1 and 192.168.2.2”
`==`	Means “equals,” as in “Choose only IP address 192.168.2.1”
`!`	Means “not,” as in, do not show a particular IP address or source port

Valid filter rules are always colored green. If you make a mistake on a filter rule, the box will turn a vivid pink.

For example, let’s say you want to see packets that have only the IP address of 18.224.161.65 somewhere inside. You would create the following command line, and put it into the Filter window:

ip.addr == 18.224.161.65

Figure shows the results of adding that filter:

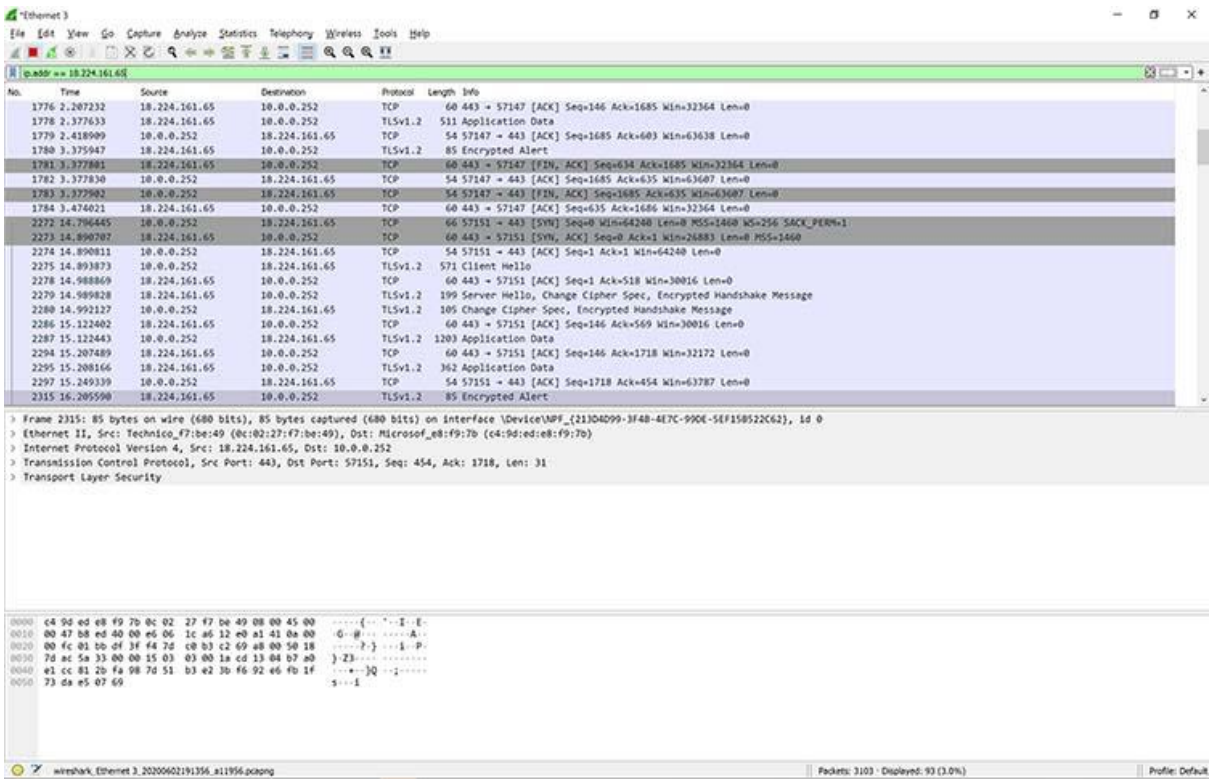


Figure: Applying a filter to a capture in Wireshark

Alternatively, you can highlight the IP address of a packet and then create a filter for it. Once you select the IP address, right-click, and then select the Apply As Filter option.

You'll then see a menu of additional options. One of those is called Selected. If you choose Selected, then Wireshark will create a filter that shows only packets with that IP address in it.

You can also decide to filter out a specific IP address using the following filter, also shown in Figure:

!ip.addr==18.224.161.65

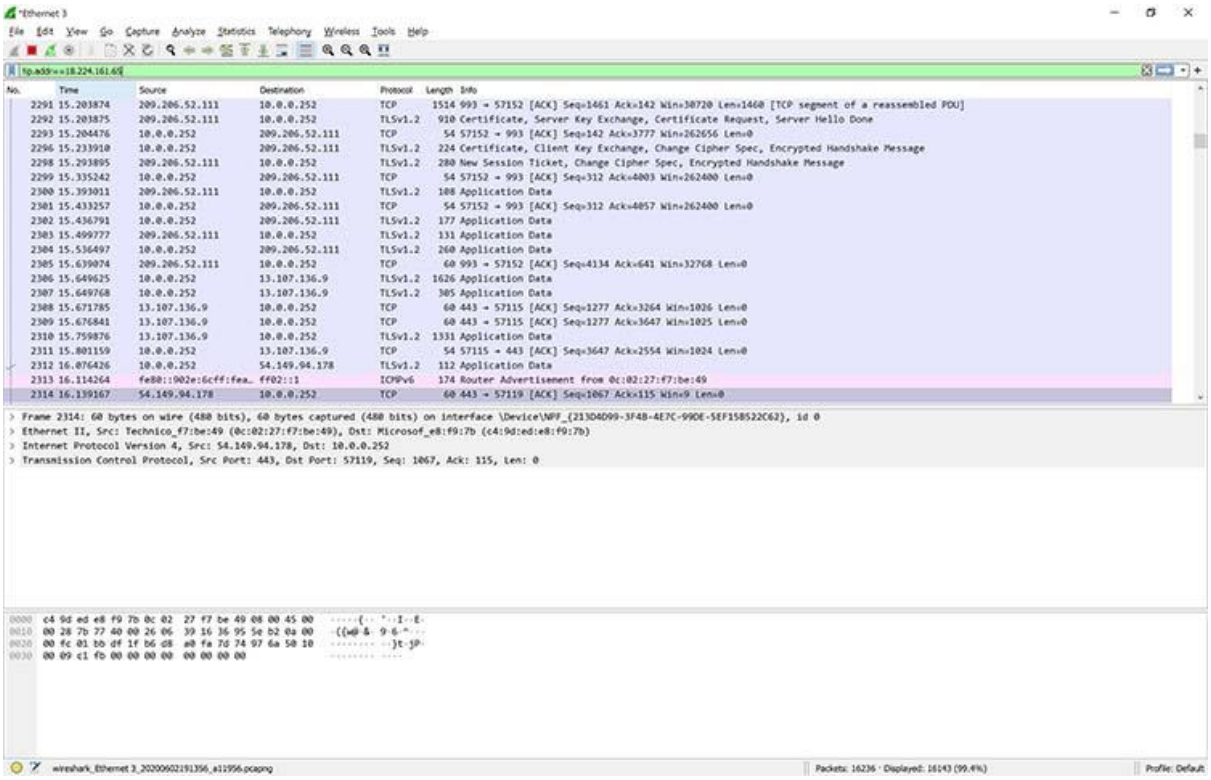


Figure: Filtering out a specific IP address in Wireshark

You're not limited to just IPv4 addresses. For example, if you want to see if a particular computer is active and using an IPv6 address on your network, you can open up a copy of Wireshark and apply the following rule:

ipv6.dst == 2607:f8b0:400a:15::b

This same rule is shown in Figure.

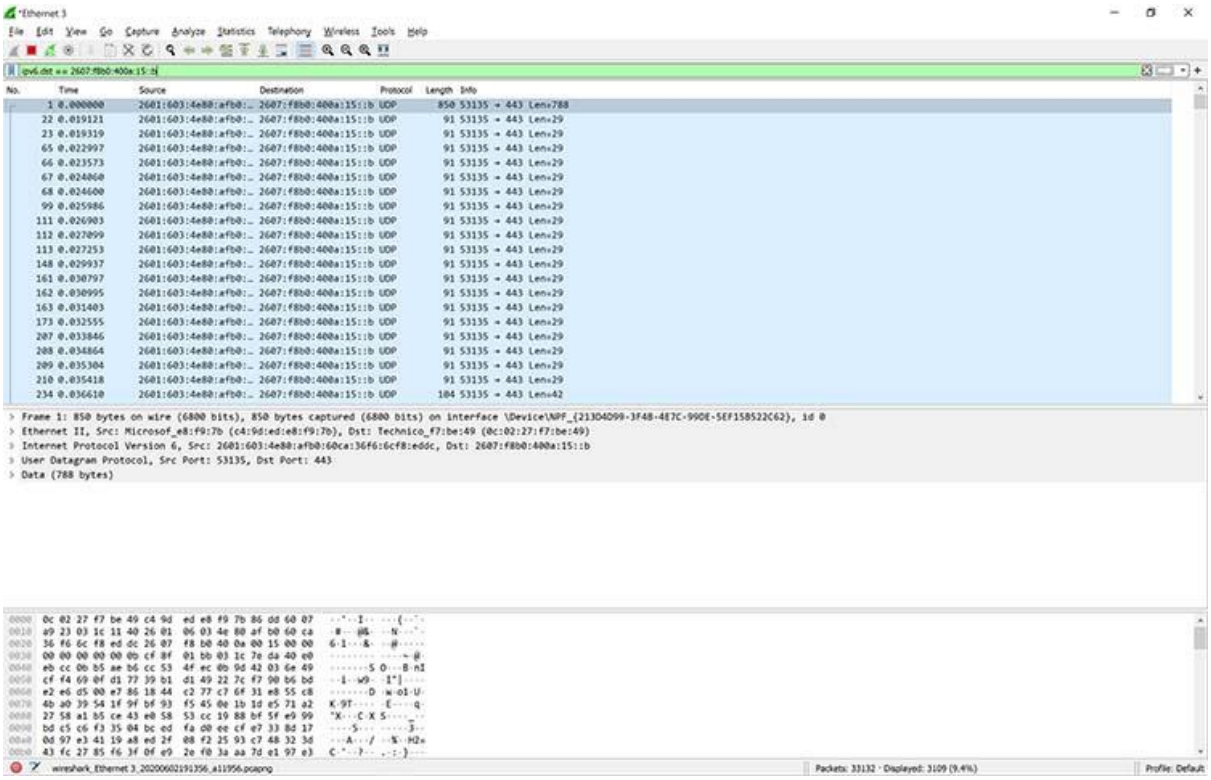


Figure: Applying an IPv6 filter in Wireshark

Clearly, this system is alive and well, talking on the network. There are so many possibilities.

Additional filters include:

`tcp.port==8080`	Filters packets to show a port of your own choosing – in this case, port 8080
`!(ip.src == 162.248.16.53)`	Shows all packets except those originating from 162.248.16.53
`!(ipv6.dst == 2607:f8b0:400a:15::b)`	Shows all packets except those going to the IPv6 address of 2607:f8b0:400a:15::b

`ip.addr == 192.168.4.1 && ip.addr == 192.168.4.2`	Shows both 192.168.4.1 and 192.168.4.2
`http.request`	Shows only http requests – useful when troubleshooting or visualizing web traffic

Nmap Command in Linux

AIM:

To familiarize working of nmap in linux

DESCRIPTION:

Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

- ✓ Real time information of a network
- ✓ Detailed information of all the IPs activated on your network
- ✓ Number of ports open in a network
- ✓ Provide the list of live hosts
- ✓ Port, OS and Host scanning

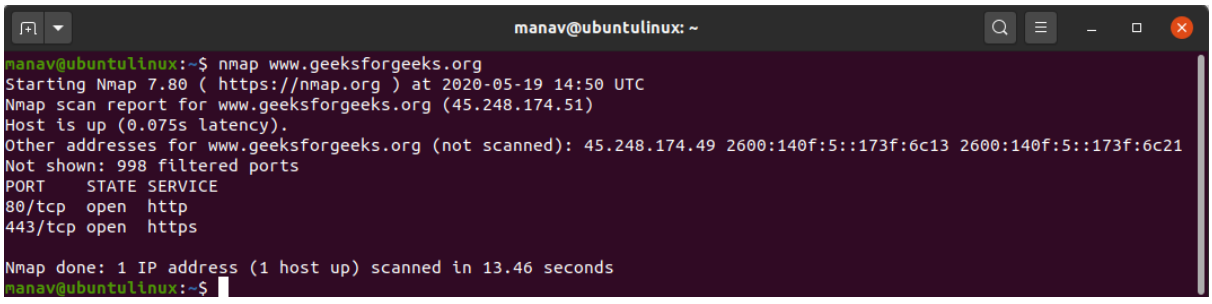
PROCEDURE:

- Installing Nmap

  sudo apt-get install nmap

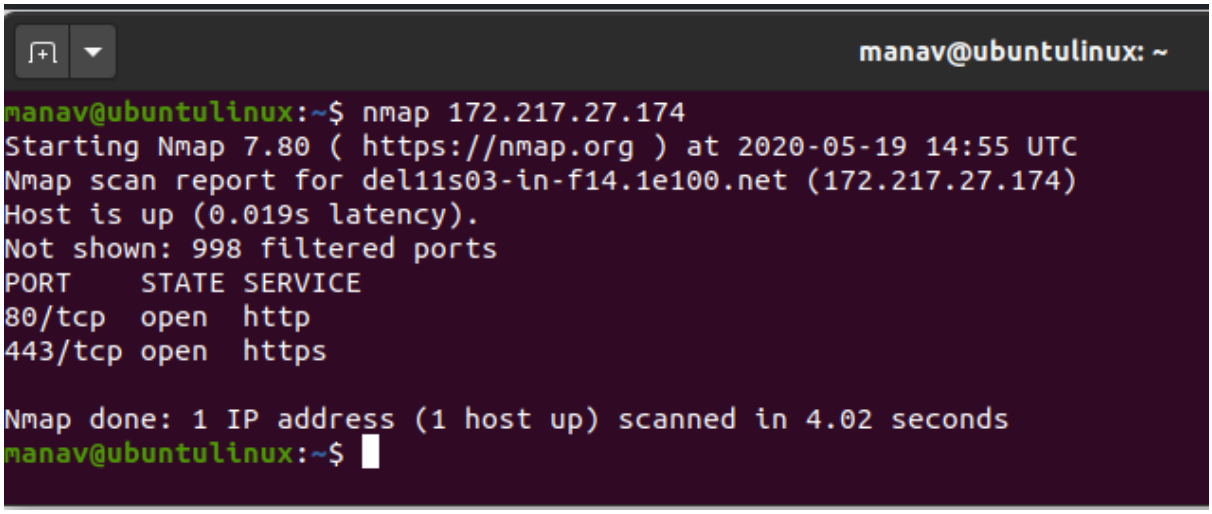
- To scan a System with Hostname and IP address. First, Scan using Hostname

  nmap www.geeksforgeeks.org



- Now let's Scan using IP Address

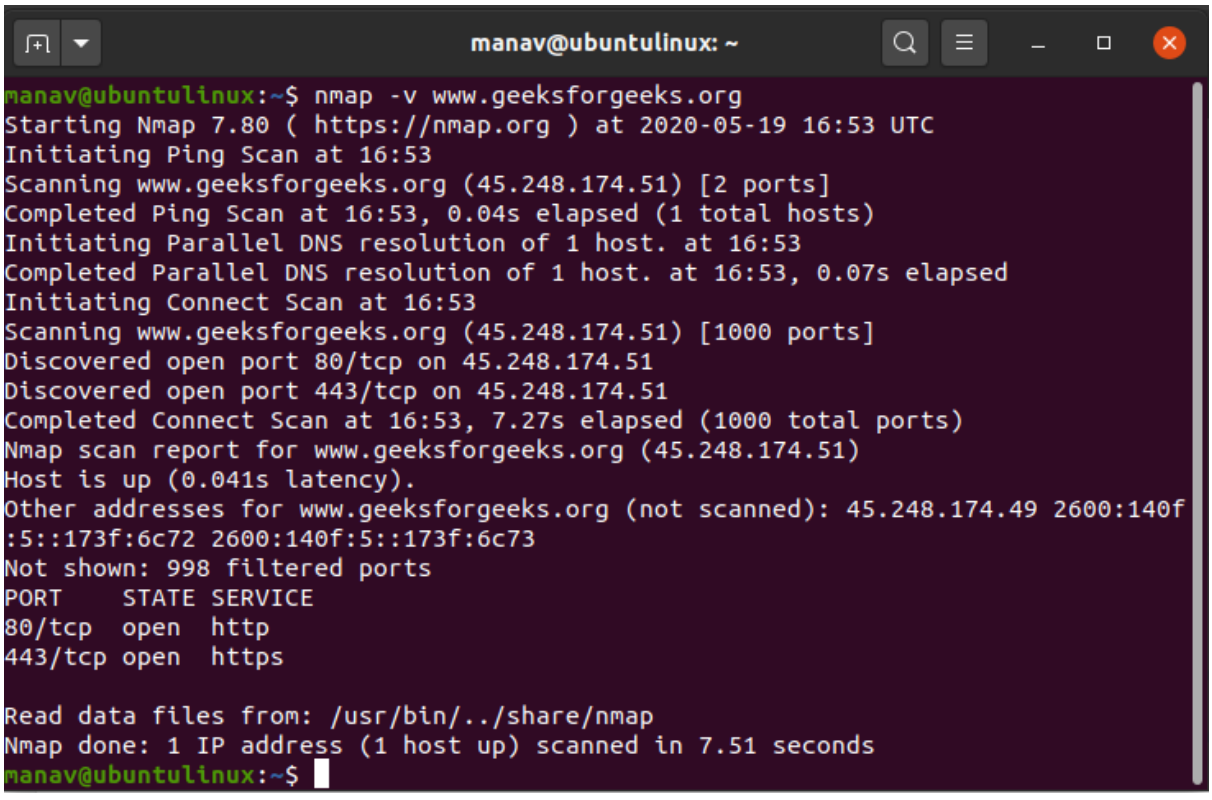
  nmap 172.217.27.174



The nmap command allows scanning a system in various ways. In this we are performing a scan using the hostname as “geeksforgeeks” and IP address “172.217.27.174”, to find all open ports, services, and MAC addresses on the system.

- To scan using “-v” option.

  nmap -v www.geeksforgeeks.org



It is used to get more detailed information about the remote machines.

- To scan multiple hosts

nmap 103.76.228.244 157.240.198.35 172.217.27.174

We can scan multiple hosts by writing IP addresses or hostnames with nmap.

- To scan whole subnet

nmap 103.76.228.*

We can scan a whole subnet or IP range with nmap by providing "*" with it. It will scan a whole subnet and give the information about those hosts which are Up in the Network.

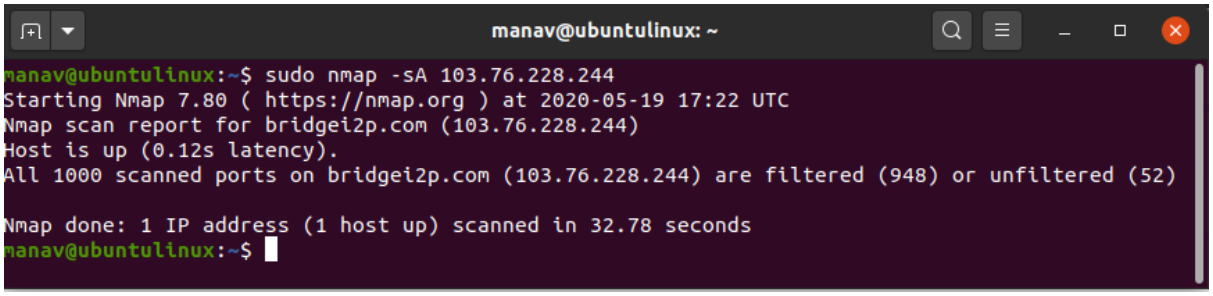
- To scan specific range of IP address

nmap 192.168.29.1-20

We can specify the range of IP addresses. This command will scan IP address 192.168.29.1 to 192.168.29.20 .

- To scan to detect firewall settings.

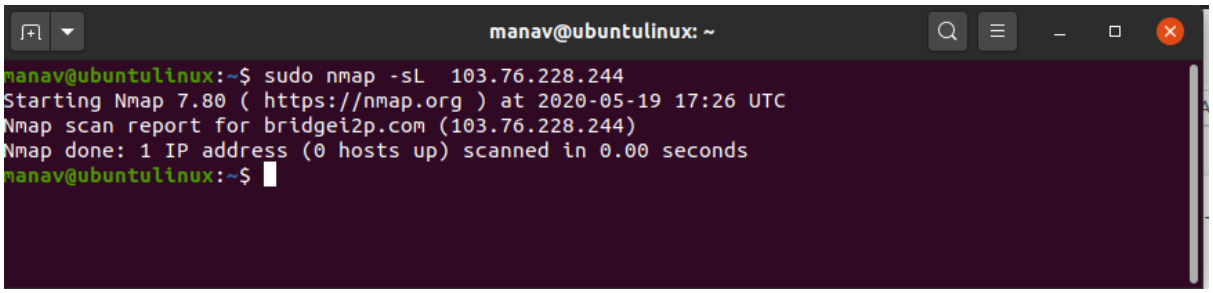
sudo nmap -sA 103.76.228.244



Detecting firewall settings can be useful during penetration testing and vulnerability scans. To detect it we use "-sA" option. This will provide you with information about firewall being active on the host. It uses an ACK scan to receive the information.

- To identify Hostnames

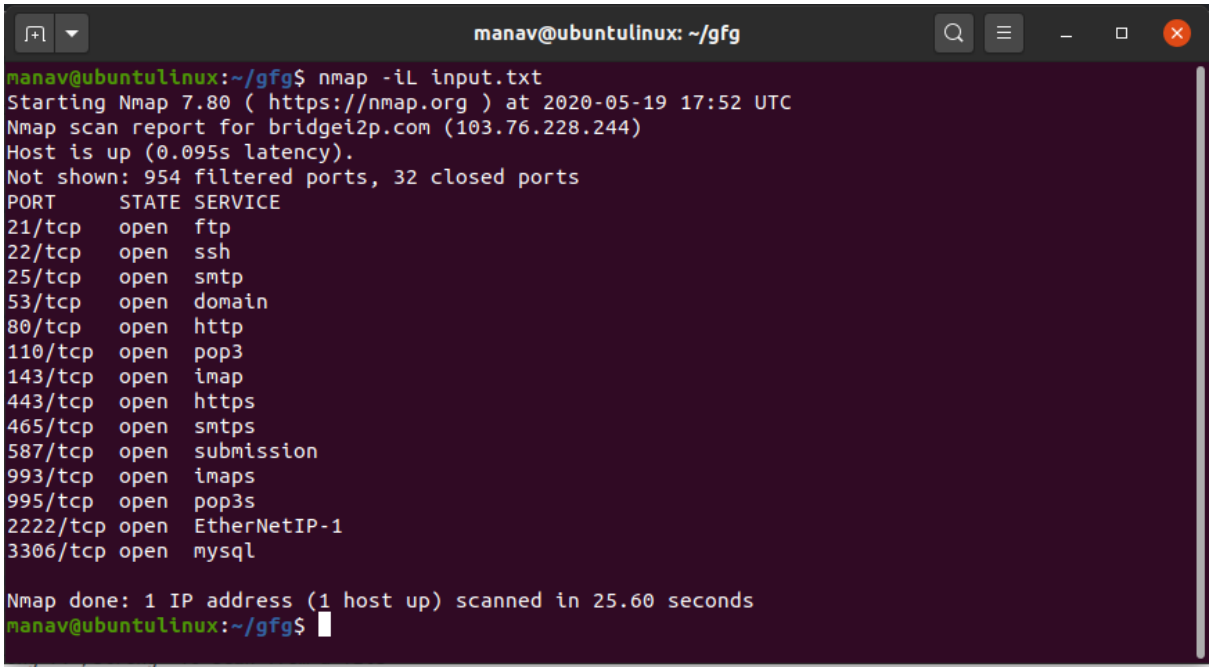
sudo nmap -sL 103.76.228.244



We use "sL" option to find hostnames for the given host by completing a DNS query for each one. In addition to this "-n" command can be used to skip DNS resolution, while the "-R" command can be used to always resolve DNS.

- To scan from a file

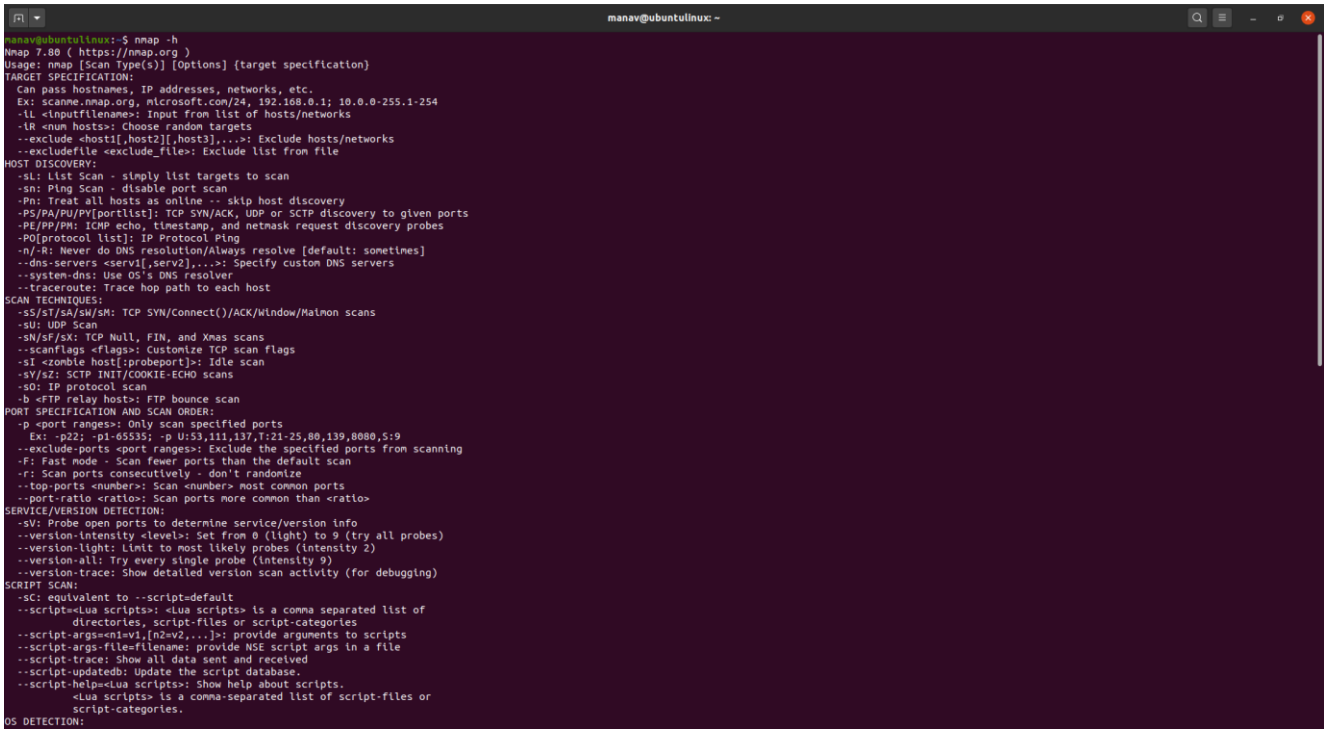
nmap -iL input.txt

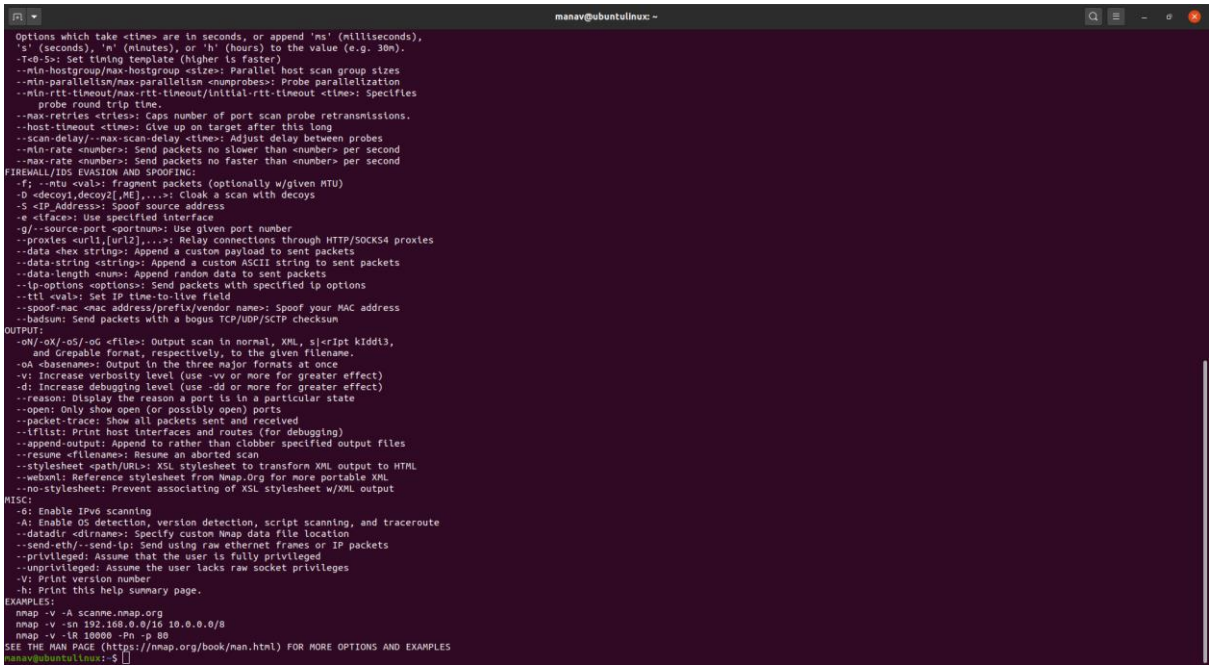


If we have a long list of addresses that we need to scan, we can directly import a file through the command line. It will produce a scan for the given IP addresses.

- To get some help

nmap -h

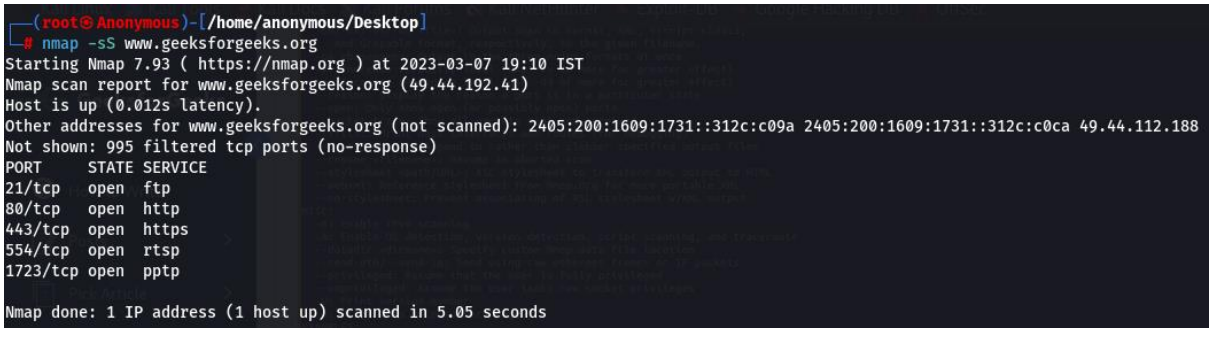




We use the “-h” option if we have any questions about nmap or any of the given commands. It shows the help section for nmap command, including giving information regarding the available flags.

- Here -sS flag is used for TCP SYN Scan, which is a stealthy and efficient method of scanning for open ports on a target system.

nmap -sS <Domain Name>



- Here “-oG” flag can be used to store the nmap result in to specific file.

nmap -sS <Domain Name> -oG <file-path>

```
┌──(root㉿Anonymous)-[/home/anonymous/Desktop]
└─# nmap -sS www.geeksforgeeks.org -oG nmap_result
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:11 IST
Nmap scan report for www.geeksforgeeks.org (23.64.140.209)
Host is up (0.013s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c09a 2405:200:1609:1731::312c:c0ca 23.64.140.218
rDNS record for 23.64.140.209: a23-64-140-209.deploy.static.akamaitechnologies.com
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
```

- The "-sU" flag is used with nmap to perform a UDP scan, which allows the user to discover open UDP ports and services on a target system.

nmap -sU <Domain Name>

- The "-sn" flag is used with nmap to perform a ping scan, which sends ICMP requests to a target host or network to determine hosts is up or not.

nmap -sn <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous]
└─# nmap -sn  www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:18 IST
Nmap scan report for www.geeksforgeeks.org (49.44.112.188)
Host is up (0.018s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c0ca 2405:200:1609:1731::312c:c09a 49.44.192.41
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

- The "-p" flag is used with nmap to perform scan on a specific port or range of ports. (In our case it will scan port 80,443 and 21)

nmap -p 80 443 21 <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous]
└─# nmap -p 80 443 21 www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:16 IST
Nmap scan report for www.geeksforgeeks.org (23.64.140.209)
Host is up (0.016s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c09a 2405:200:1609:1731::312c:c0ca 23.64.140.218
rDNS record for 23.64.140.209: a23-64-140-209.deploy.static.akamaitechnologies.com

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 3 IP addresses (1 host up) scanned in 1.48 seconds
```

- We can also specify the range of ports to scan on a network. (In this case it will scan all the ports in the range of 1 to 80)

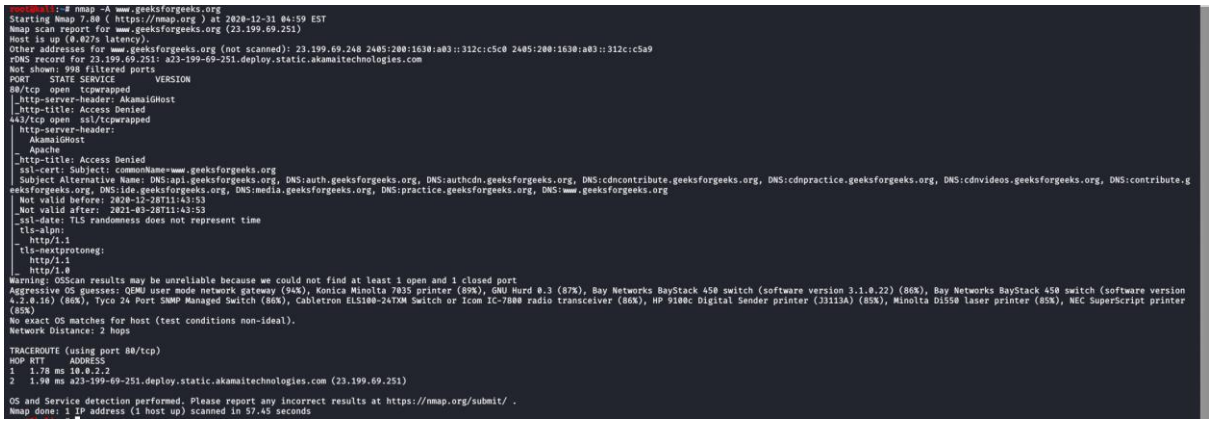
nmap -p 1-80 <Domain Name>

```
┌──(root㉿Anonymous)-[/home/anonymous]
└─# nmap -p 1-80 www.geeksforgeeks.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 19:17 IST
Nmap scan report for www.geeksforgeeks.org (49.44.192.41)
Host is up (0.0098s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 2405:200:1609:1731::312c:c0ca 2405:200:1609:1731::312c:c09a 49.44.112.188
Not shown: 78 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
```

- Here -A indicates aggressive, it will give us extra information, like OS detection (-O), version detection, script scanning (-sC), and traceroute (–traceroute). It even provides a lot of valuable information about the host.

nmap -A <Domain Name>



- Using this command we can discover the target hosting service or identify additional targets according to our needs for quickly tracing the path.

nmap --trace out <Domain Name>

```
root@kali:~# nmap --trace out  www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 05:10 EST
Failed to resolve "out".
Nmap scan report for www.geeksforgeeks.org (23.199.69.251)
Host is up (0.0047s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 23.199.69.248 2405:200:1630:a03::312c:c5a9 2405:200:1630:a03::312c:c5c0
rDNS record for 23.199.69.251: a23-199-69-251.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.75 ms 10.0.2.2
2   1.86 ms a23-199-69-251.deploy.static.akamaitechnologies.com (23.199.69.251)

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds
```

- Here it will display the operating system where the domain or ip address is running, but will not display the exact operating system available on the computer. It will display only the chance of operating system available in the computer. The command will just guess the running operating system (OS) on the host.

nmap -O <Domain Name>

```
root@kali:~# nmap -O  www.geeksforgeeks.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 04:57 EST
Nmap scan report for www.geeksforgeeks.org (23.199.69.248)
Host is up (0.029s latency).
Other addresses for www.geeksforgeeks.org (not scanned): 23.199.69.251 2405:200:1630:a03::312c:c5a9 2405:200:1630:a03::312c:c5c0
rDNS record for 23.199.69.248: a23-199-69-248.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (99%), QEMU (96%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (99%), QEMU user mode network gateway (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
```

NMAP-VULNERABILITY SCANNER

AIM: To scan vulnerabilities using nmap in windows operating system

DESCRIPTION:

Nmap vulnerability scanning is the process of using Nmap to scan for and identify known vulnerabilities. The goal of Nmap vulnerability scanning is to gather information about a target host, system, network, or an information technology asset, test it for weaknesses, attempt to exploit those weaknesses, and report on the findings so appropriate security measures can be taken to eliminate any reported problems. Nmap vulnerability scanning may also be conducted to check the effectiveness of an organization's security policy, adherence to compliance regulations, company-wide awareness of security measures, and the ability of an organization to flag and respond to security threats and violations.

Nmap is capable of:

- ✓ Scan Active IPs

  Get detailed reporting on every IP on your network to figure out if a certain IP address is compromised and needs further investigation. Nmap can flag compromised IPs and report on whether they're being used by a legitimate network service or a hacker.

- ✓ Scan Your Entire Network

  Nmap can help you visualize and map out your entire local network. It can also show you a list of active live hosts, available ports, and the operating systems running on every device connected.

- ✓ Scan for Vulnerabilities

  In addition to a number of network scanning functions, Nmap can also be used to identify vulnerabilities in your network. The tool gives you a front-row view of what attackers would see if they attempt to infiltrate your network defenses. This can help you prepare better for any future cybersecurity threats.

- ✓ Visualize Your Network

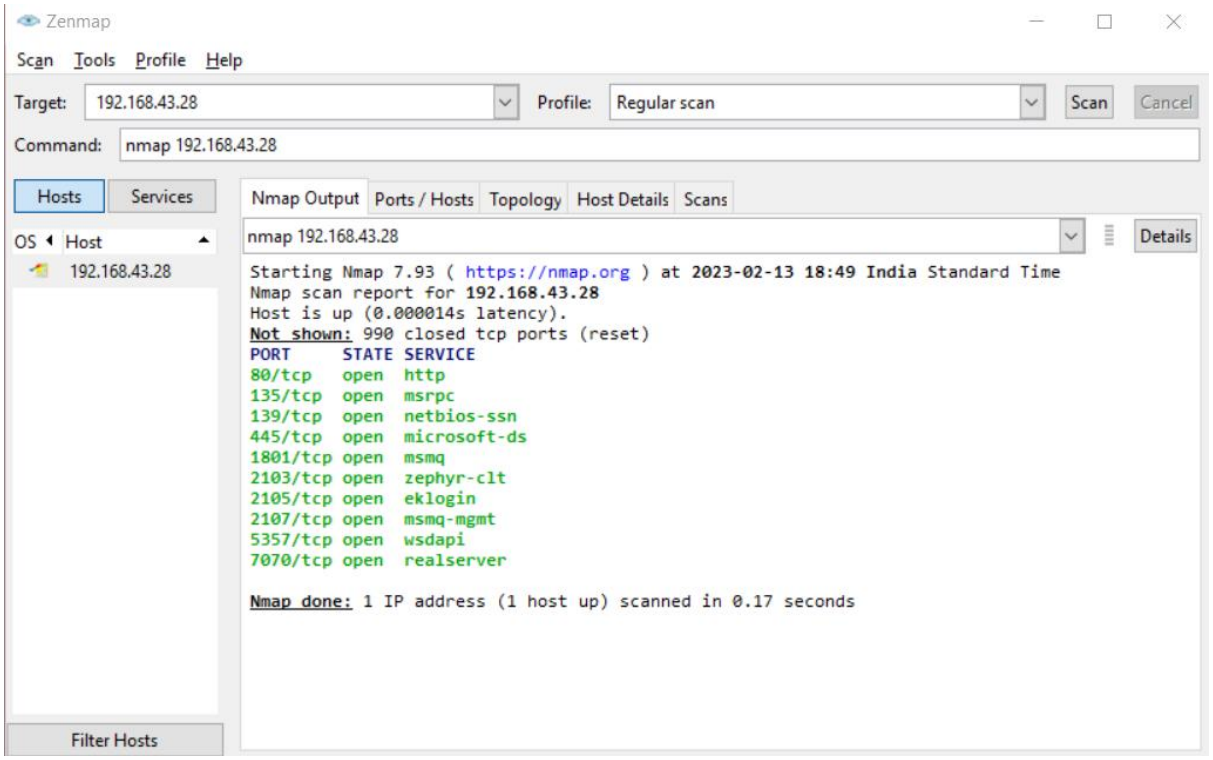
  Nmap is a command-line tool. But it has a graphical user interface called Zenmap that can help you visually map your network so you can understand it better and prepare reports that are easier to understand.

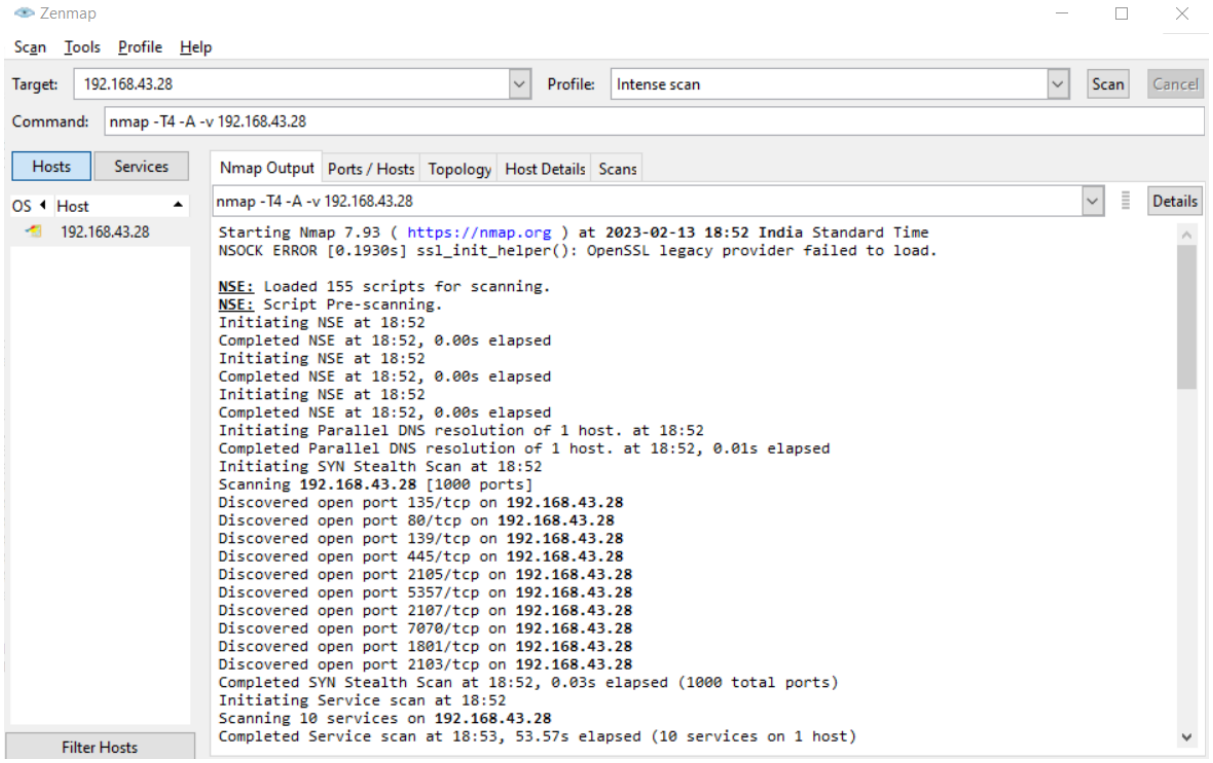
PROCEDURE

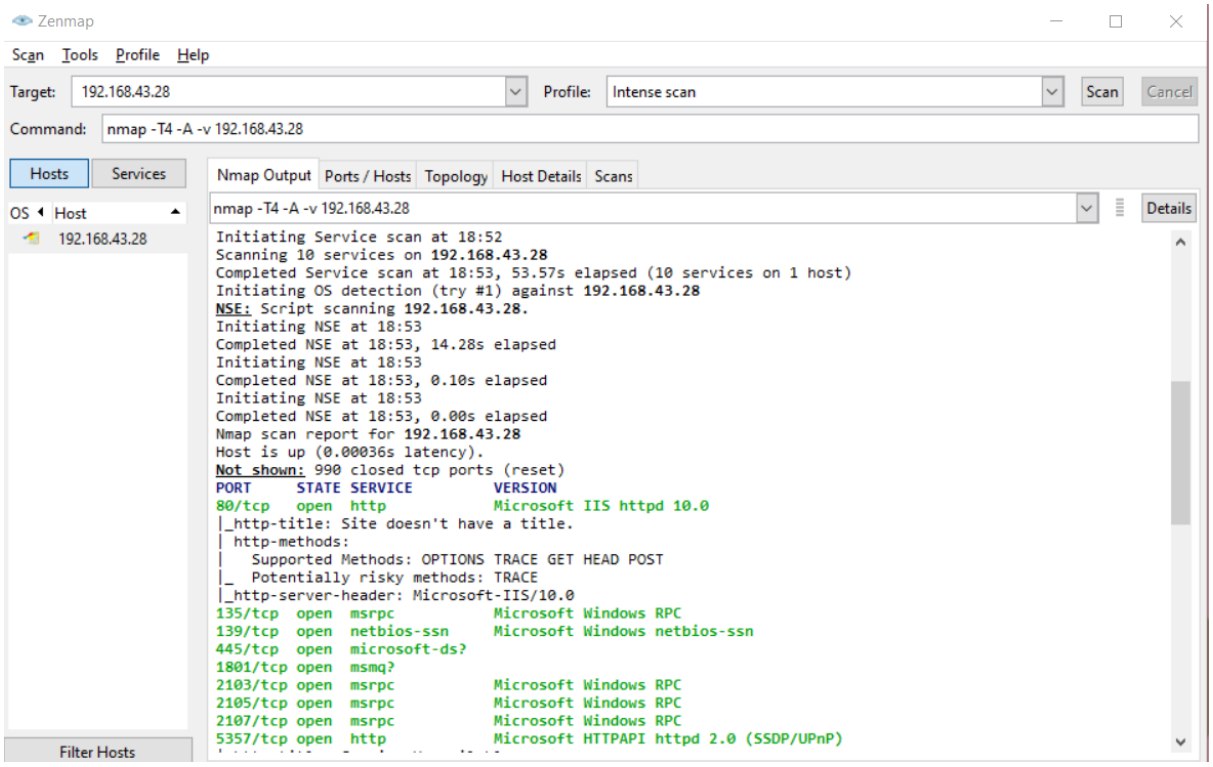
The primary uses of Nmap can be broken into three core processes.

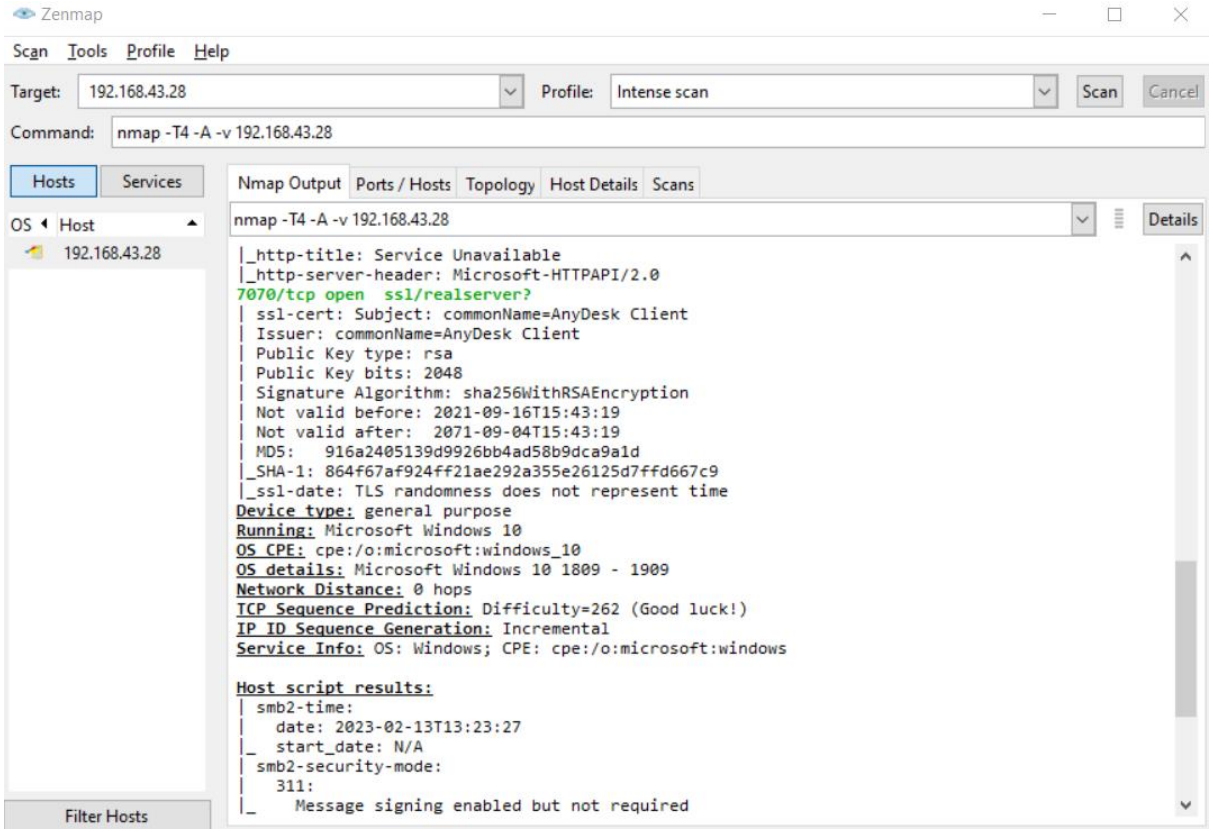
- ✓ First, the program gives you detailed information on every IP active on your networks, and each IP can then be scanned. This allows administrators to check whether an IP is being used by a legitimate service, or by an external attacker.
- ✓ Secondly, Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device. This makes it a valuable tool in ongoing system monitoring, as well as a critical part of pentesting.
- ✓ Thirdly, Nmap has also become a valuable tool for users looking to protect personal and business websites. Using Nmap to scan your own web server, particularly if you are hosting your website from home, is essentially simulating the process that a hacker would use to attack your site.

OBSERVATION






Zenmap
Scan Tools Profile Help
Target: 192.168.43.28
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.43.28
Hosts
Services
OS Host
192.168.43.28
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.43.28
Details
Initiating Service scan at 18:52
Scanning 10 services on 192.168.43.28
Completed Service scan at 18:53, 53.57s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against 192.168.43.28
NSE: Script scanning 192.168.43.28.
Initiating NSE at 18:53
Completed NSE at 18:53, 14.28s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.10s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Nmap scan report for 192.168.43.28
Host is up (0.00036s latency).
Not shown: 990 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
| http-methods:
| Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
1801/tcp open msmq?
2103/tcp open msrpc Microsoft Windows RPC
2105/tcp open msrpc Microsoft Windows RPC
2107/tcp open msrpc Microsoft Windows RPC
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 192.168.43.28
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.43.28
Hosts
Services
OS Host
192.168.43.28
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.43.28
Details
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
7070/tcp open ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-09-16T15:43:19
| Not valid after: 2071-09-04T15:43:19
| MD5: 916a2405139d9926bb4ad58b9dca9a1d
|_SHA-1: 864f67af924ff21ae292a355e26125d7ffd667c9
|_ssl-date: TLS randomness does not represent time
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2023-02-13T13:23:27
|_ start_date: N/A
| smb2-security-mode:
| 311:
|_ Message signing enabled but not required
Filter Hosts

```
NSE: Script Post-scanning.
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.71 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2050 (87.470KB)
```