FORENSICS V2 LAB SERIES

Lab 03: Live Forensics

Document Version: 2021-01-11

Contents

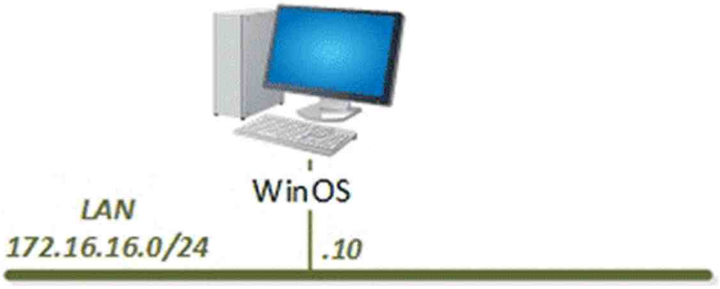
Introduction

When dealing with digital evidence, it is important to know the correct methodologies and procedures that are acceptable for collecting electronic data. This lab aims to teach the student how to collect relevant evidence and navigate a live computer to review key artifacts that may aid in the full examination without altering evidence.

Objectives

- Review the hard drive file structure
- Review frequent paths for an average user(s)
- Document all action/steps taken

Lab Topology



Lab Settings

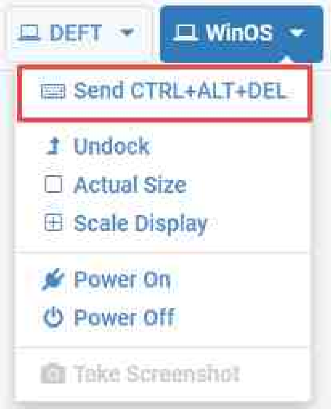
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

1 Getting Familiar with Digital Evidence & Forensic Toolkit (DEFT 8) & Digital Advance Recovery Toolkit (DART)

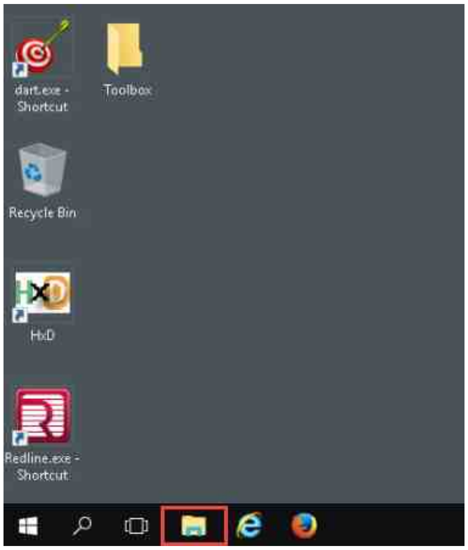
Live analysis of a computer requires certain tools that can ascertain valuable data while leaving very small footprints. One of these tools is the Digital Evidence & Forensic Toolkit (DEFT). This is a full Linux operating system that can also be used for live analysis and incident response. It has a full suite of tools, and we will be utilizing a few of them in this lab.

1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

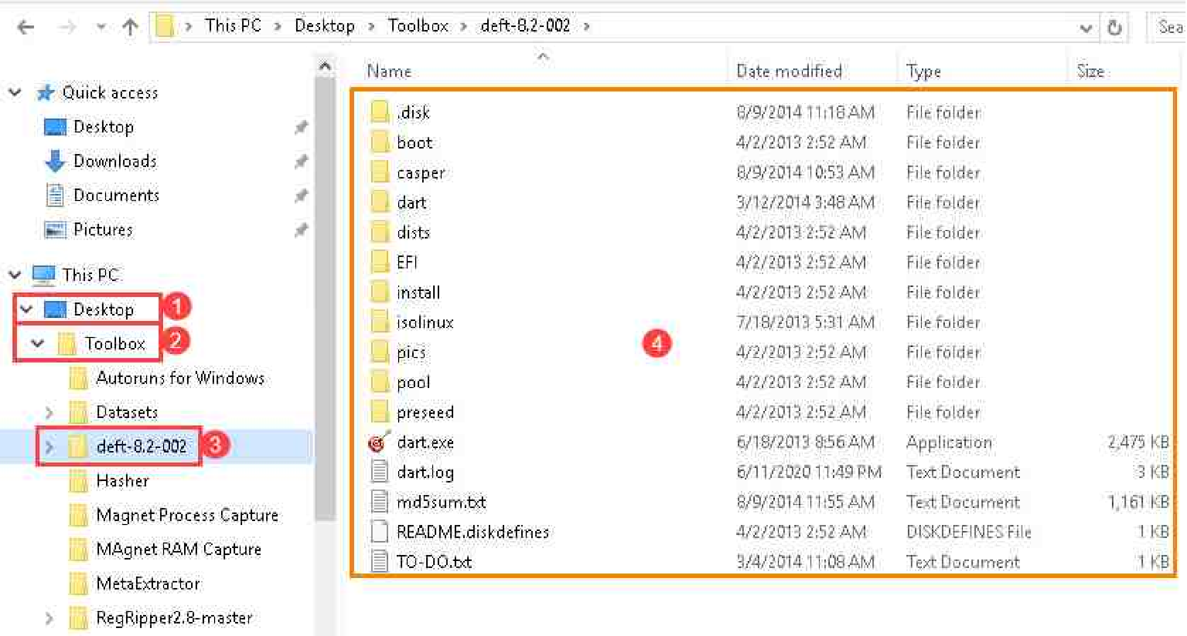


   b. Log in as `Administrator` using the password: `Train1ng$`.

2. Once you are logged into the VM, open file explorer by clicking the icon on the taskbar as highlighted in red below.



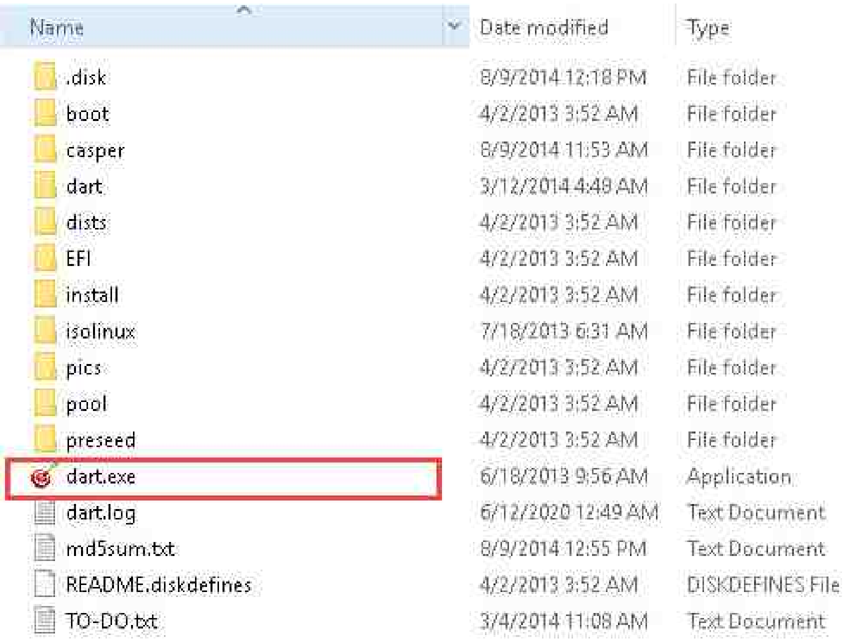
3. Within File Explorer, browse to Desktop > Toolbox > deft-8.2-002, as seen in items 1, 2, and 3 below. This will allow you to view the extracted contents of the DEFT ISO file, as seen in item 4.



Name	Date modified	Type	Size
.disk	8/9/2014 11:16 AM	File folder	
boot	4/2/2013 2:52 AM	File folder	
casper	8/9/2014 10:53 AM	File folder	
dart	3/12/2014 3:48 AM	File folder	
dists	4/2/2013 2:52 AM	File folder	
EFI	4/2/2013 2:52 AM	File folder	
install	4/2/2013 2:52 AM	File folder	
isolinux	7/18/2013 5:31 AM	File folder	
pics	4/2/2013 2:52 AM	File folder	
pool	4/2/2013 2:52 AM	File folder	
preseed	4/2/2013 2:52 AM	File folder	
dart.exe	6/18/2013 8:56 AM	Application	2,475 KB
dart.log	6/11/2020 11:49 PM	Text Document	3 KB
md5sum.txt	8/9/2014 11:55 AM	Text Document	1,161 KB
README.diskdefines	4/2/2013 2:52 AM	DISKDEFINES File	1 KB
TO-DO.txt	3/4/2014 11:08 AM	Text Document	1 KB

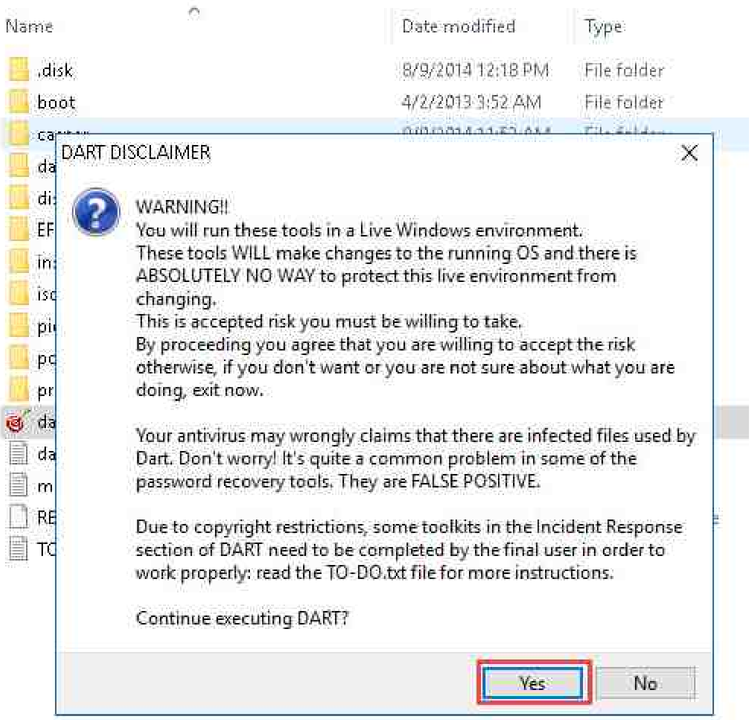
It is important to note that the tools contained within DEFT can be reported as False Positives in antivirus programs. When practicing in the real-world environment, be sure to disable antivirus solutions to prevent them from complicating the capture process.

4. Once the folder is opened, you will see the following folder structure appear. These are the files and folders that make up the DEFT 8 operating system. In this exercise, we will only be using the Digital Advance Recovery Toolkit (DART) feature of DEFT. DART is a handy live response toolkit that has applications designed for extracting valuable evidence from running systems. To open DART, double-click the dart.exe icon highlighted below.



Name	Date modified	Type
.disk	8/9/2014 12:18 PM	File folder
boot	4/2/2013 3:52 AM	File folder
casper	8/9/2014 11:53 AM	File folder
dart	3/12/2014 4:49 AM	File folder
dists	4/2/2013 3:52 AM	File folder
EFI	4/2/2013 3:52 AM	File folder
install	4/2/2013 3:52 AM	File folder
isolinux	7/18/2013 6:31 AM	File folder
pics	4/2/2013 3:52 AM	File folder
pool	4/2/2013 3:52 AM	File folder
preseed	4/2/2013 3:52 AM	File folder
dart.exe	6/18/2013 9:56 AM	Application
dart.log	6/12/2020 12:49 AM	Text Document
md5sum.txt	8/9/2014 12:55 PM	Text Document
README.diskdefines	4/2/2013 3:52 AM	DISKDEFINES File
TO-DO.txt	3/4/2014 11:08 AM	Text Document

5. When opening, DART will display the DART DISCLAIMER window. Read it carefully to understand the risk that is taken when performing an analysis on a computer that is booted into its operating system. It will also provide details about common issues. Click the Yes button as highlighted below to continue.



WARNING!!
You will run these tools in a Live Windows environment.
These tools WILL make changes to the running OS and there is ABSOLUTELY NO WAY to protect this live environment from changing.
This is accepted risk you must be willing to take.
By proceeding you agree that you are willing to accept the risk otherwise, if you don't want or you are not sure about what you are doing, exit now.

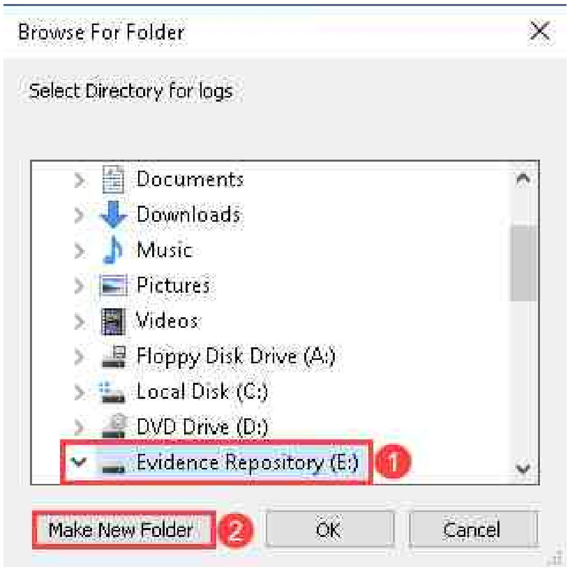
Your antivirus may wrongly claims that there are infected files used by Dart. Don't worry! It's quite a common problem in some of the password recovery tools. They are FALSE POSITIVE.

Due to copyright restrictions, some toolkits in the Incident Response section of DART need to be completed by the final user in order to work properly: read the TO-DO.txt file for more instructions.

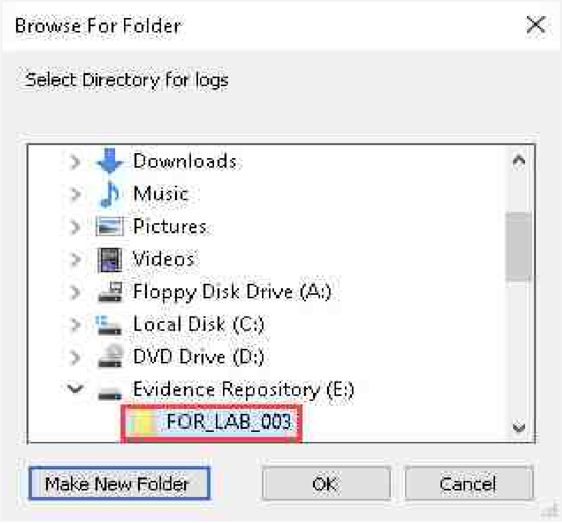
Continue executing DART?

Note taking is a very important factor in ensuring that you are able to regurgitate what exactly happened when you interacted with the evidence item. The DART logs assist in this detailed recording, which makes it extremely vital. It should always be used and stored on a drive prepared for evidence storage and NEVER on the computer being examined.

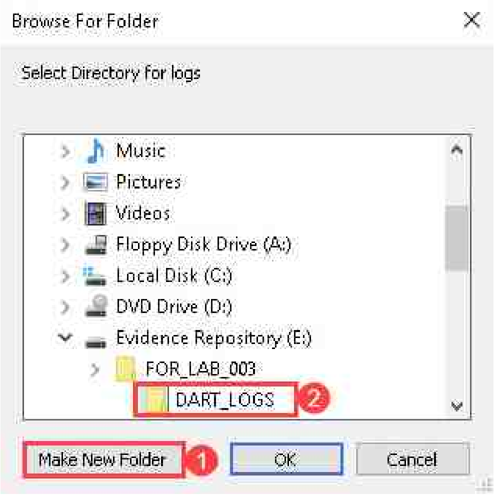
6. The next window that will appear is the Browse For Folder window. DART creates a log of actions taken while using it, and it requires a path to store the log file. To adhere to forensic procedures, the logs must be stored on an external evidence drive to prevent creating more artifacts than necessary and potentially overwriting data on the host's system. Let us make a new folder in the Evidence Repository drive that has the drive letter (E:). To do this, browse to Evidence Repository (E:) and click Make New Folder as seen in items 1 and 2 below.



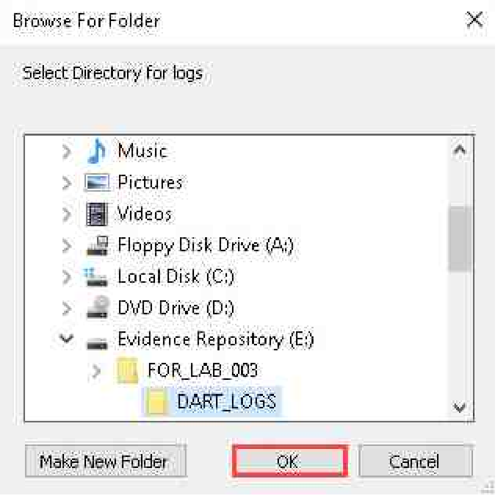
7. Let us name the new folder `FOR_LAB_003` as highlighted below.



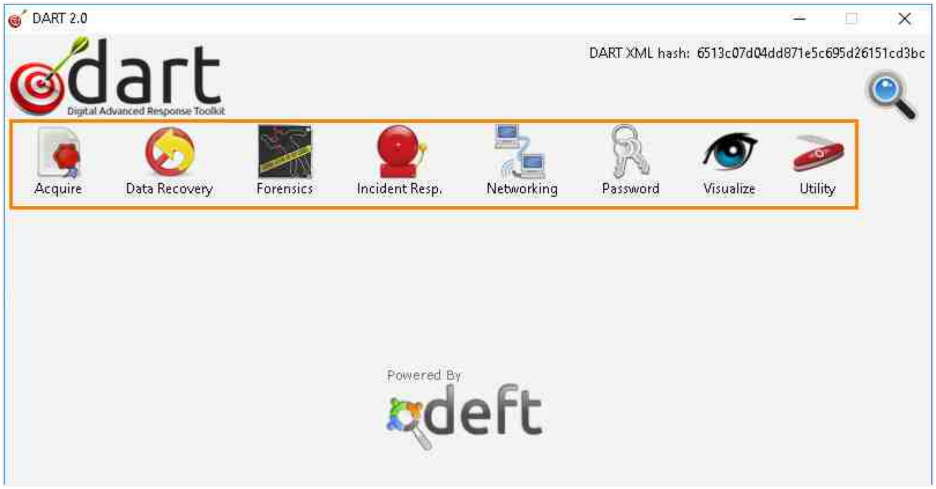
8. Inside the folder called FOR_LAB_003, we will create another new folder by clicking Make New Folder again, and we will call it `DART_LOGS` as highlighted in items 1 and 2 below.



9. Once the folder is created, click OK as highlighted below.



10. You will now be presented with the DART 2.0 home page. From this window, you will be able to navigate the different categories of applications offered in DART. The categories are outlined in the table below the following screenshot.



Acquire	This category contains applications that will allow you to burn, copy, or create forensic images.
Data Recovery	The Data recovery category contains apps that are ideal for finding and restoring deleted information even after it has been removed from the recycle bin.
Forensics	The forensics category contains the most tools. It provides applications that can recover data from web browsers, view e-mails, check for encryption, examine files, create file hashes, view instant messaging data, and identify peer to peer software. It has a whole suite of tools that are specifically designed for extracting data from the windows operating system.
Incident Resp.	The incident response category helps you learn about the system and has some antivirus tools that help with investigating compromised systems.
Networking	The networking category contains tools that provide data about the computer's network connections. It can reveal Wireless network data, reveal cookies**,** and sniff network traffic, etc.
Password	The Password category has a myriad of tools designed for finding, revealing**,** and cracking various types of passwords. Some categories are browser passwords, Wi-F**i** passwords, and Asterisk passwords, etc.
Visualize	The Visualize category contains tools that allow you to view different types of data. It contains software that allows you to view graphics, multimedia**,** and documents.
Utility	The utility category is somewhat of a miscellaneous list of useful software. Tools that allow you to erase drives, read hexadecimal files, perform screen captures, and more.

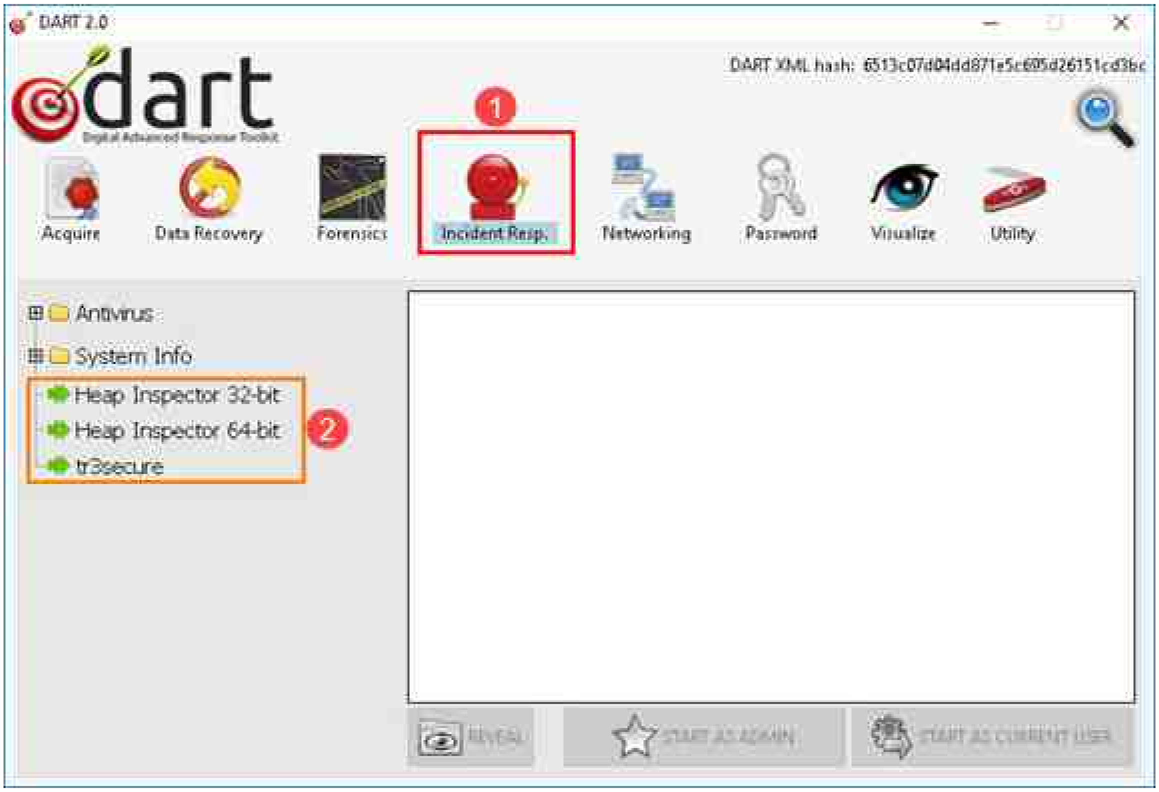
11. Now that you are familiar with DART 2.0. Let us move to the next task, getting information using Drive Manager.

DART contains many tools that we won't be able to cover in this course. Feel free to navigate the options and test the different software. They each have their own help files to teach you what they are for and how to use them.

2 Using Drive Manager to Get Drive Information

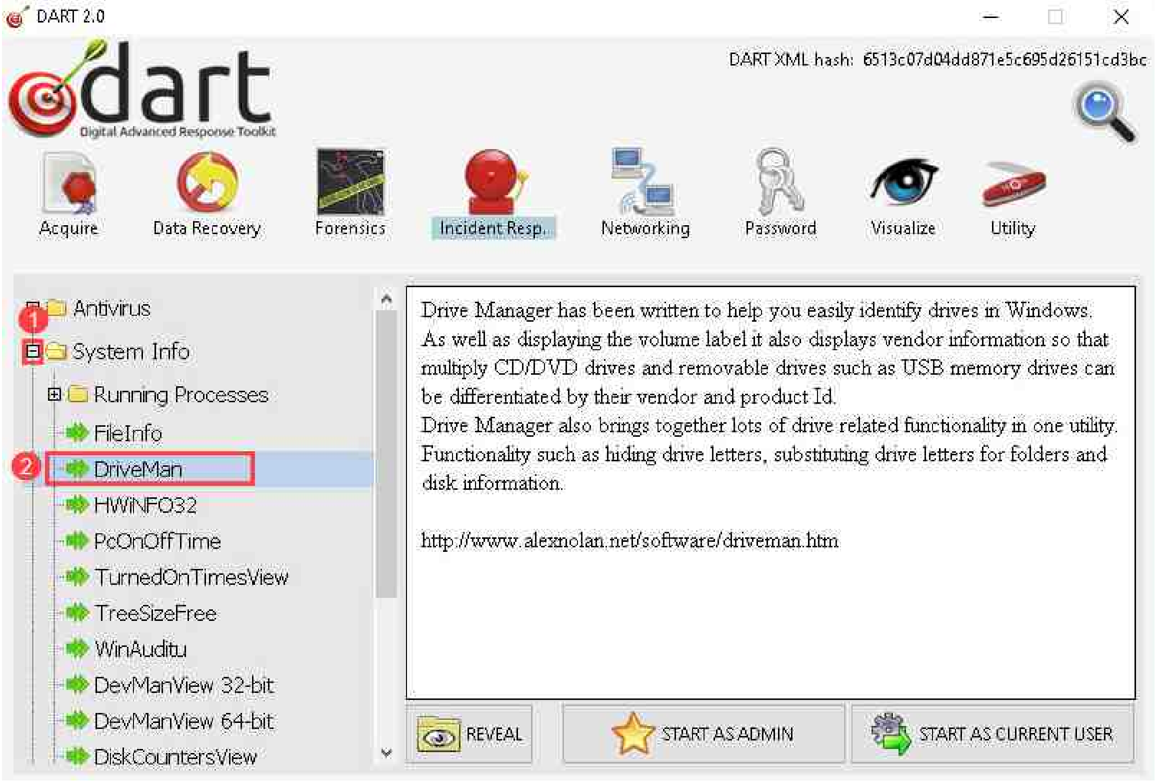
Now that you are familiar with the DART interface, let us look at a few of the tools. The first one we will use is Drive Manager. This tool helps to display the connected drives in a Microsoft Windows operating system and provides lots of details about them.

1. DART should already be open. If it is not, reopen it and click on the Incident Resp. category, as seen in item 1 below. The Items on the left side of the window are the names of the different programs. The ones with the arrow beside them, highlighted in item 2 below, are programs.



Some programs are further categorized in folders. To expand them, click the plus (+) beside the folder name.

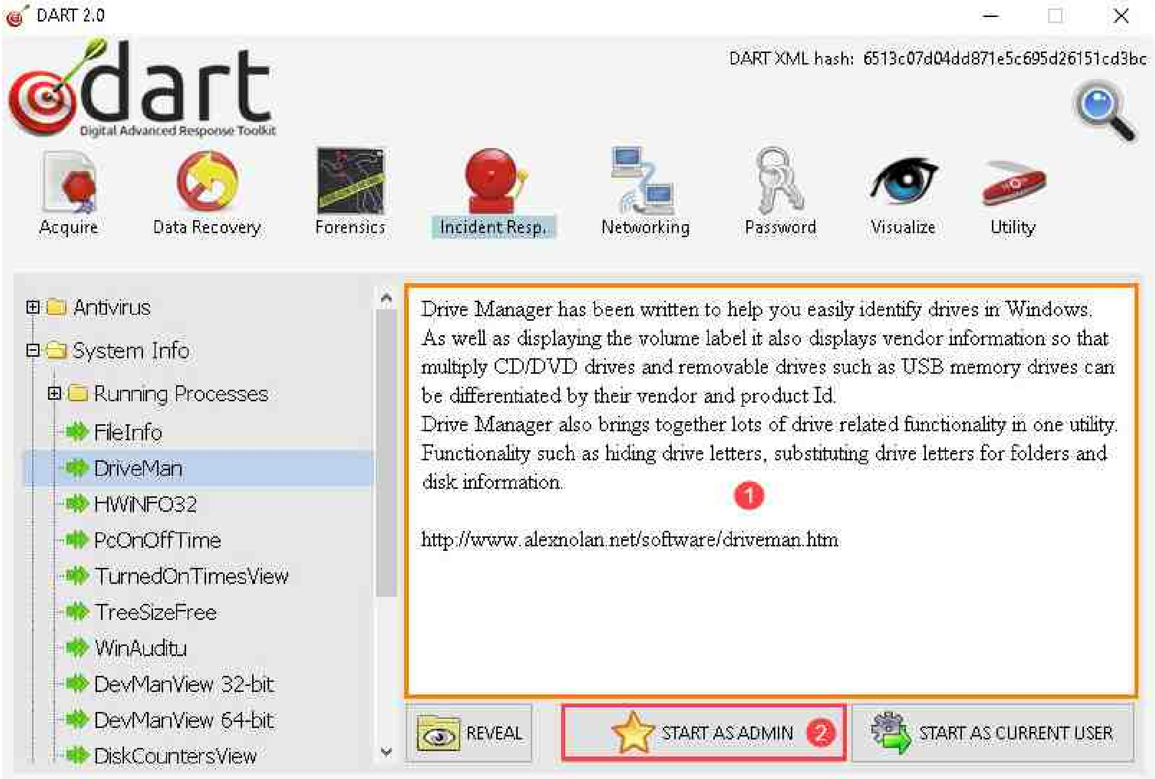
2. In this exercise, we will be using the Drive Manager tool (DriveMan), which is found in the System Info folder. Click the + sign beside the System Info folder, as seen in item 1, to expand it and view the contents. Next, click DriveMan from the list of programs that appear, as seen in item 2 below.



Drive Manager has been written to help you easily identify drives in Windows. As well as displaying the volume label it also displays vendor information so that multiply CD/DVD drives and removable drives such as USB memory drives can be differentiated by their vendor and product Id.
Drive Manager also brings together lots of drive related functionality in one utility. Functionality such as hiding drive letters, substituting drive letters for folders and disk information.

http://www.alexnolan.net/software/driveman.htm

3. Once you have DriveMan selected, you will see a description of the tool in the right pane, as seen in item 1. To open the program, click START AS ADMIN highlighted in item 2 below.

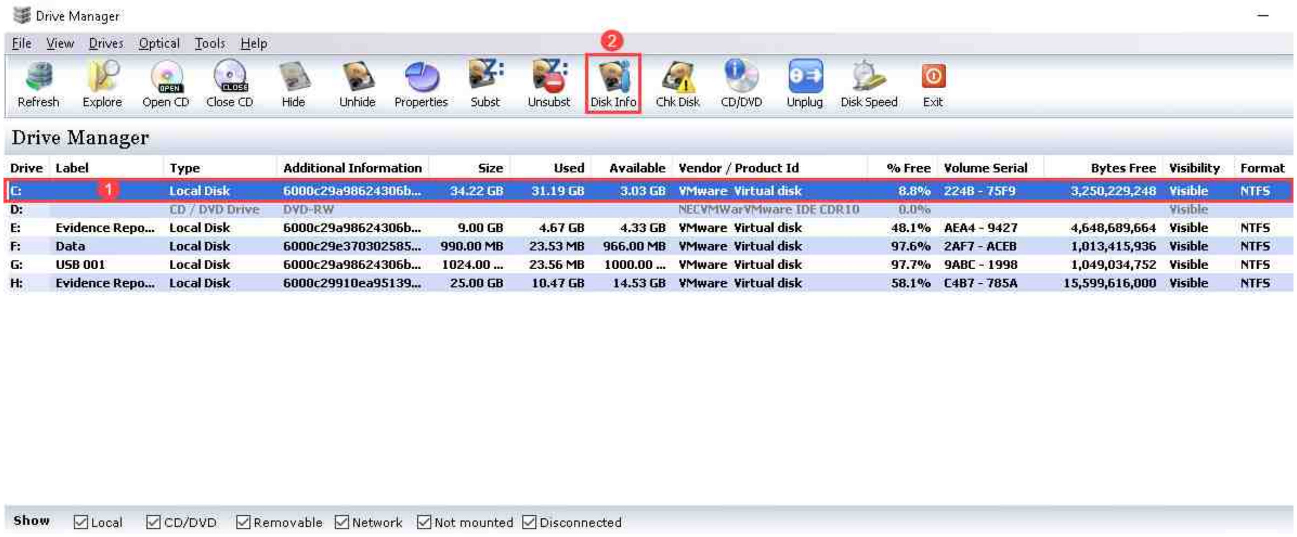


DART XML hash: 6513c07d04dd871e5c695d26151cd3bc

Drive Manager has been written to help you easily identify drives in Windows. As well as displaying the volume label it also displays vendor information so that multiply CD/DVD drives and removable drives such as USB memory drives can be differentiated by their vendor and product Id.
Drive Manager also brings together lots of drive related functionality in one utility. Functionality such as hiding drive letters, substituting drive letters for folders and disk information.

http://www.alexnolan.net/software/driveman.htm

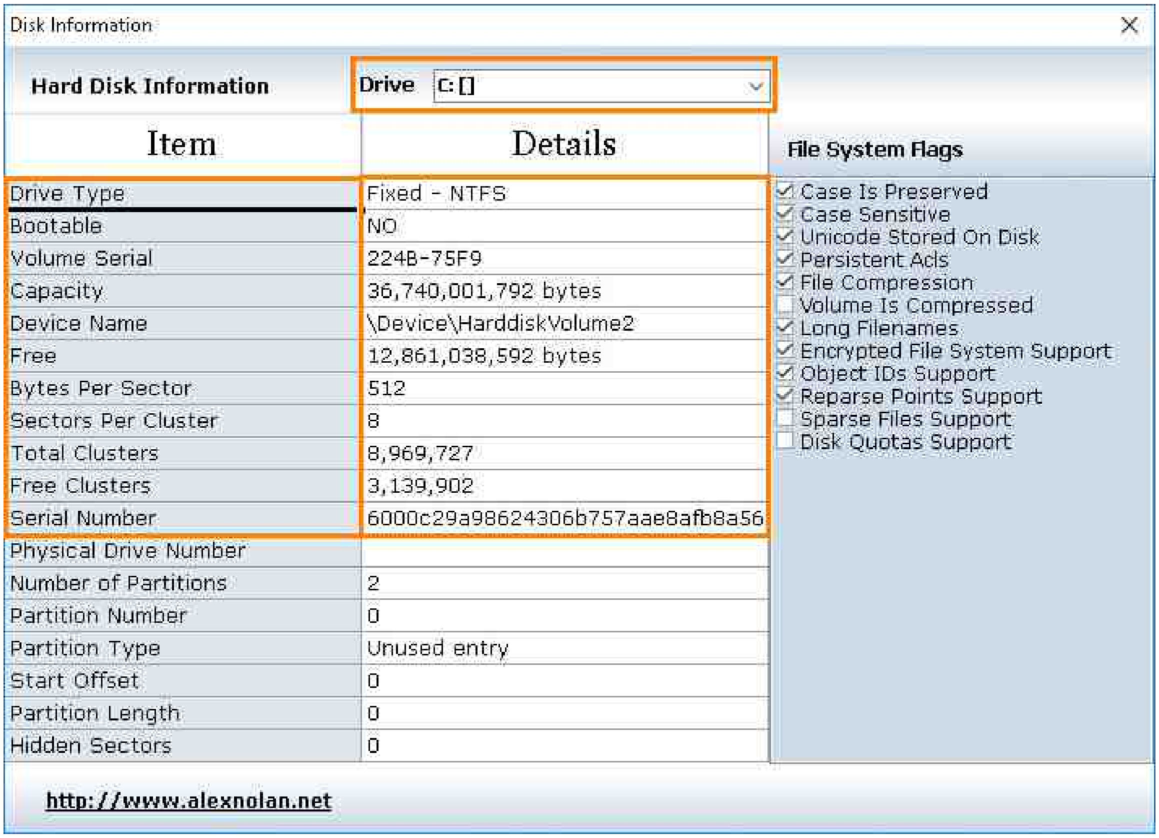
4. The Drive Manager application will open and will instantly list all the drives currently connected to the computer. The application has several options that can be used to gather information and perform actions on each drive. In this exercise, we will be using the Disk Info option. To begin, let us click the drive bearing the drive letter (C:) as seen in item 1 below. Once you have the (C:) volume selected, click the Disk Info option from the toolbar highlighted in item 2 below.



Drive Manager

Drive	Label	Type	Additional Information	Size	Used	Available	Vendor / Product Id	% Free	Volume Serial	Bytes Free	Visibility	Format
C:		Local Disk	6000c29a98624306b...	34.22 GB	31.19 GB	3.03 GB	VMware Virtual disk	8.8%	224B - 75F9	3,250,229,248	Visible	NTFS
D:		CD / DVD Drive	DVD-RW				NECVMWarVMware IDE CDR10	0.0%			Visible	
E:	Evidence Repo...	Local Disk	6000c29a98624306b...	9.00 GB	4.67 GB	4.33 GB	VMware Virtual disk	48.1%	AEA4 - 9427	4,648,689,664	Visible	NTFS
F:	Data	Local Disk	6000c29e370302585...	990.00 MB	23.53 MB	966.00 MB	VMware Virtual disk	97.6%	2AF7 - ACEB	1,013,415,936	Visible	NTFS
G:	USB 001	Local Disk	6000c29a98624306b...	1024.00 ...	23.56 MB	1000.00 ...	VMware Virtual disk	97.7%	9ABC - 1998	1,049,034,752	Visible	NTFS
H:	Evidence Repo...	Local Disk	6000c29910ea95139...	25.00 GB	10.47 GB	14.53 GB	VMware Virtual disk	58.1%	C4B7 - 785A	15,599,616,000	Visible	NTFS

5. The Disk info window will provide details about the selected drive. Here you can find the hard drive's serial number, the volume serial number, the total size of the hard drive in bytes, the allocated and unallocated clusters, the physical disk name, and whether the drive is fixed or removable. This information is essential when trying to account for all the disk space as well as getting drive serial numbers. The physical serial number is also good for evidence documentation and chain of custody.



Disk Information

Hard Disk Information

Drive C: []

Item	Details
Drive Type	Fixed - NTFS
Bootable	NO
Volume Serial	224B-75F9
Capacity	36,740,001,792 bytes
Device Name	\Device\HarddiskVolume2
Free	12,861,038,592 bytes
Bytes Per Sector	512
Sectors Per Cluster	8
Total Clusters	8,969,727
Free Clusters	3,139,902
Serial Number	6000c29a98624306b757aae8afb8a56
Physical Drive Number	
Number of Partitions	2
Partition Number	0
Partition Type	Unused entry
Start Offset	0
Partition Length	0
Hidden Sectors	0

File System Flags

☑ Case Is Preserved
☑ Case Sensitive
☑ Unicode Stored On Disk
☑ Persistent Acls
☑ File Compression
□ Volume Is Compressed
☑ Long Filenames
☑ Encrypted File System Support
☑ Object IDs Support
☑ Reparse Points Support
□ Sparse Files Support
□ Disk Quotas Support

http://www.alexnolan.net

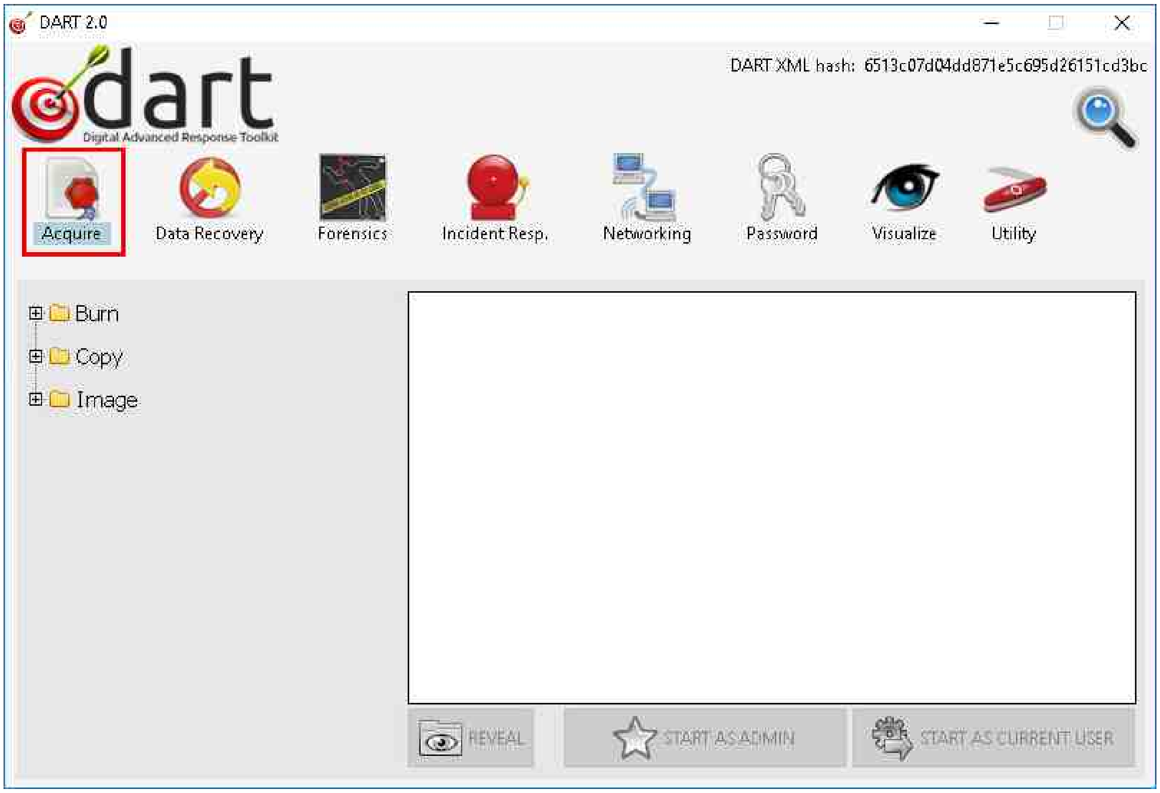
Drive Manager has many other useful features. For more information on the other uses, you can click on the Help menu option on the main Drive Manager window.

6. Now that you have reviewed the disk's details, it is time to look at the contents to get a better understanding of the data within it. Close the Drive Manager information before moving to the next task.

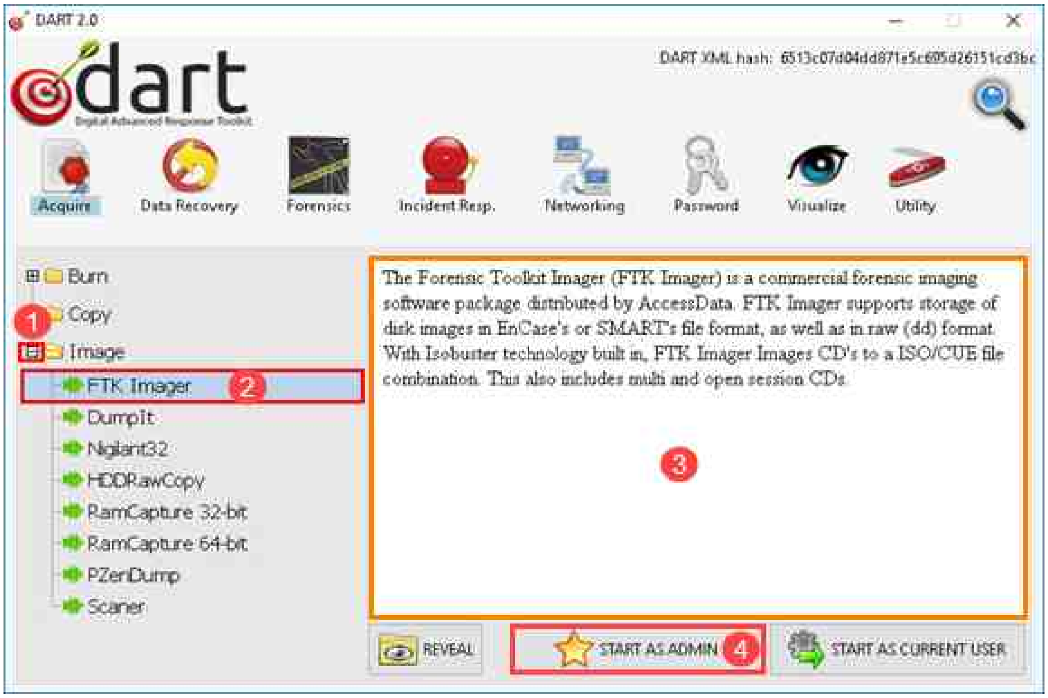
3 Using FTK Imager to Identify Windows User Directories

Now that you are familiar with the DART interface, let us look at a few of the tools. The first one we will use is FTK Imager. You should already be familiar with FTK Imager from our first and second labs. In this exercise, we will use FTK Imager to go a bit deeper and show you how to browse to and identify the users' files and folders.

1. DART should already be open. If it is not, reopen it and click on the Acquire category highlighted below.

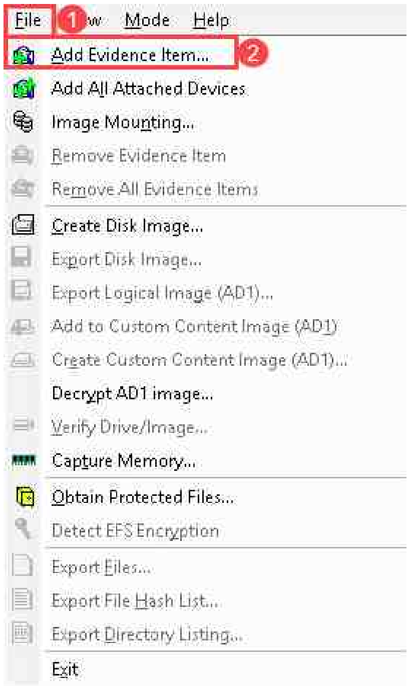


2. Click the + beside the folder called Image and then select FTK Imager by clicking it, as highlighted in items 1 and 2 below. Verify that FTK Imager is selected by looking at the right pane in the DART window highlighted in item 3 below. This is where you will see the description of the selected tool. If your description is correct, then let us go ahead and click START AS ADMIN as seen in item 4. This will launch FTK Imager lite, which is a portable version of this powerful tool.

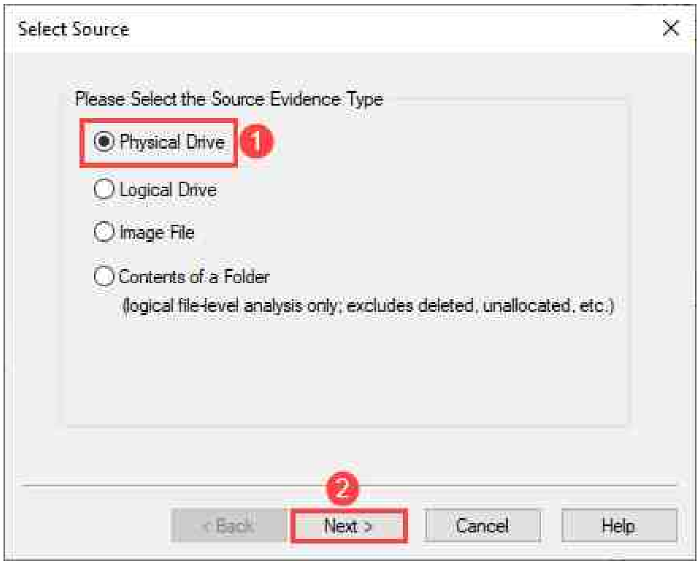


The Forensic Toolkit Imager (FTK Imager) is a commercial forensic imaging software package distributed by AccessData. FTK Imager supports storage of disk images in EnCase's or SMART's file format, as well as in raw (dd) format. With Isobuster technology built in, FTK Imager Images CD's to a ISO/CUE file combination. This also includes multi and open session CDs.

3. Now that you are in FTK Imager, let us load the Physical Drive 0 that has Local Disk (C:) volume. To do this, navigate to File > Add Evidence Item as highlighted in items 1 and 2 below.



4. You will be brought to the Select Source window. Let us select the Physical Drive radio button and then select Next, as seen in items 1 and 2, to proceed to the Select File window.


Select Source

Please Select the Source Evidence Type

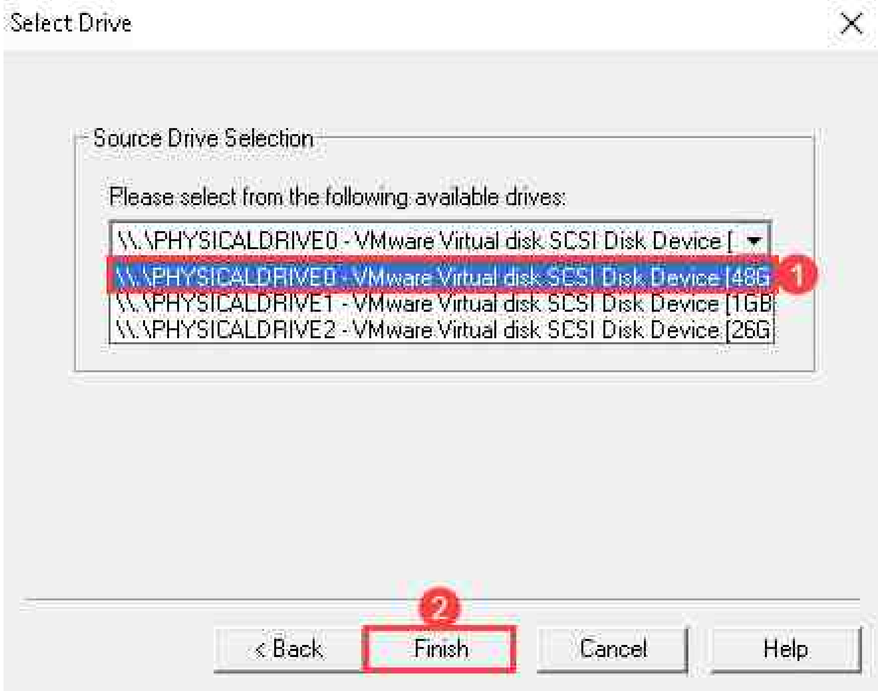
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

5. In the Select Drive window, you will have the option to select which drive you want to preview. Select PHYSICALDRIVE0 from the dropdown menu as seen in item 1 below, then click Finish once you have verified that you selected the correct drive, as seen in item 2.



Select Drive

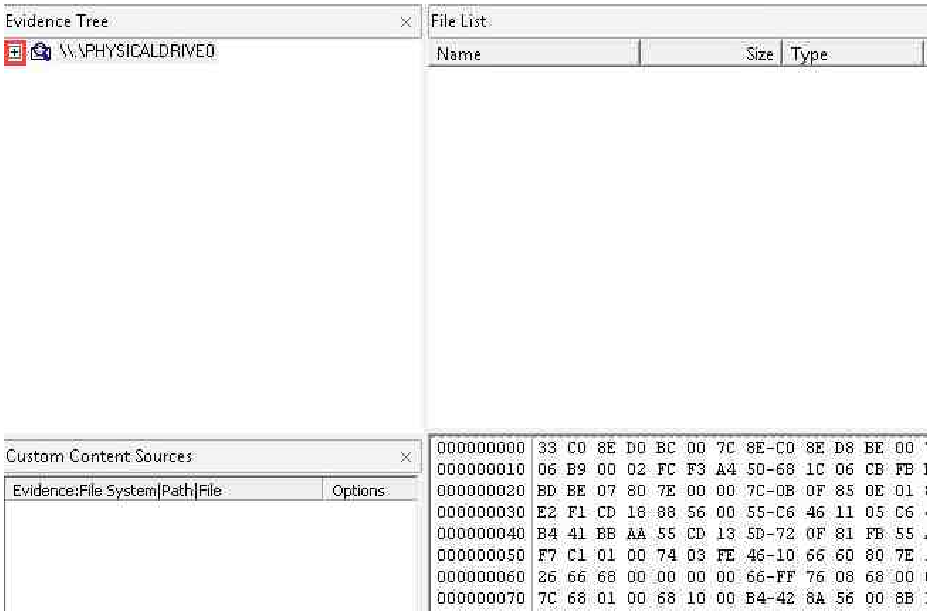
Source Drive Selection

Please select from the following available drives:

```
\\.\PHYSICALDRIVE0 - VMware Virtual disk SCSI Disk Device [
\\.\PHYSICALDRIVE0 - VMware Virtual disk SCSI Disk Device [48G
\\.\PHYSICALDRIVE1 - VMware Virtual disk SCSI Disk Device [1GB
\\.\PHYSICALDRIVE2 - VMware Virtual disk SCSI Disk Device [26G]
```

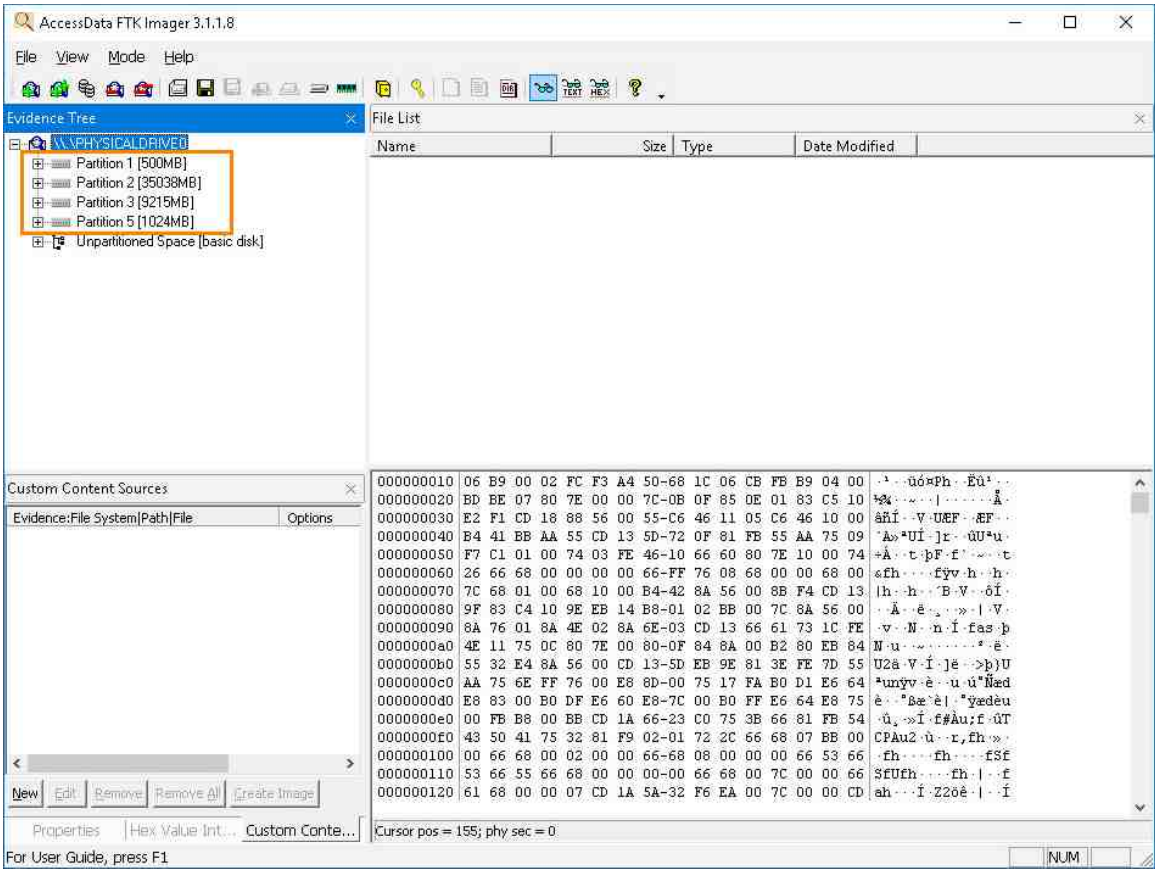
In some cases, 'Physical Drive 0' may be a secondary storage hard drive and may not have the folder structure for an operating system, It is very uncommon but possible. Ensure the correct drive is selected.

6. If you did everything correctly, you will now be back at FTK Imager's main window with PHYSICALDRIVE0 listed under the Evidence Tree Pane. We will now browse the hard drive and view its contents. To begin, click the + sign beside PHYSICALDRIVE0 as seen below. This will expand the tree and display the different partitions on the drive.



```
000000000  33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00
000000010  06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB
000000020  BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01
000000030  E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6
000000040  B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55
000000050  F7 C1 01 00 74 03 FE 46-10 66 60 80 7E
000000060  26 66 68 00 00 00 00 66-FF 76 08 68 00
000000070  7C 68 01 00 68 10 00 B4-42 8A 56 00 8B
```

7. Now that you can see all the partitions, you can determine which partition is the main data partition that contains the operating system and user files. To do this, use the name and the size of the partition. The size can be seen in square brackets beside the name of the partition, as seen below. The larger partitions normally contain user-created files and operating systems. In the example below, the partition called Basic data partition (2) is the largest partition. When you compare this to the size of the other partitions, you can see that it is 35038MB while the nearest partition size is 9215MB.



```
\\.\PHYSICALDRIVE0
    Partition 1 [500MB]
    Partition 2 [35038MB]
    Partition 3 [9215MB]
    Partition 5 [1024MB]
    Unpartitioned Space [basic disk]
```

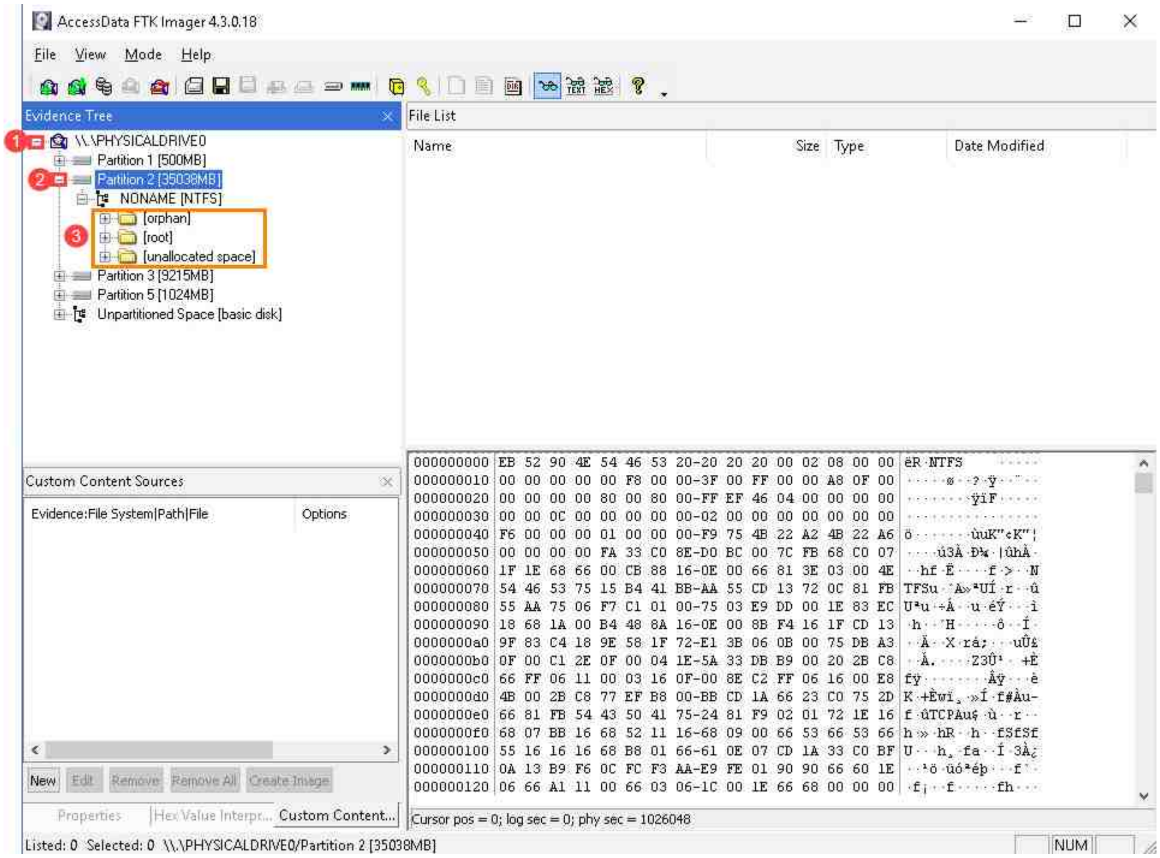
```
000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00 ·¹··üó¤Ph··Ëû¹··
000000020 BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10 ½¾··~··|······Å·
000000030 E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00 âñÍ··V·UÆF··ÆF··
000000040 B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09 ´A»ªUÍ·]r··ûUªu·
000000050 F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74 ÷Á··t·þF·f`·~··t
000000060 26 66 68 00 00 00 00 66-FF 76 08 68 00 00 68 00 &fh····fÿv·h··h·
000000070 7C 68 01 00 68 10 00 B4-42 8A 56 00 8B F4 CD 13 |h··h··´B·V··ôÍ·
000000080 9F 83 C4 10 9E EB 14 B8-01 02 BB 00 7C 8A 56 00 ··Ä··ë·¸··»·|·V·
000000090 8A 76 01 8A 4E 02 8A 6E-03 CD 13 66 61 73 1C FE ·v··N··n·Í·fas·þ
0000000a0 4E 11 75 0C 80 7E 00 80-0F 84 8A 00 B2 80 EB 84 N·u··~······²·ë·
0000000b0 55 32 E4 8A 56 00 CD 13-5D EB 9E 81 3E FE 7D 55 U2ä·V·Í·]ë··>þ}U
0000000c0 AA 75 6E FF 76 00 E8 8D-00 75 17 FA B0 D1 E6 64 ªunÿv·è··u·ú°Ñæd
0000000d0 E8 83 00 B0 DF E6 60 E8-7C 00 B0 FF E6 64 E8 75 è··°ßæ`è|·°ÿædèu
0000000e0 00 FB B8 00 BB CD 1A 66-23 C0 75 3B 66 81 FB 54 ·û¸·»Í·f#Àu;f·ûT
0000000f0 43 50 41 75 32 81 F9 02-01 72 2C 66 68 07 BB 00 CPAu2·ù··r,fh·»·
000000100 00 66 68 00 02 00 00 66-68 08 00 00 00 66 53 66 ·fh····fh····fSf
000000110 53 66 55 66 68 00 00 00-00 66 68 00 7C 00 00 66 SfUfh····fh·|··f
000000120 61 68 00 00 07 CD 1A 5A-32 F6 EA 00 7C 00 00 CD ah···Í·Z2öê·|··Í
```

Cursor pos = 155; phy sec = 0

For User Guide, press F1

On the right, in square brackets, it shows that the partition called Basic data partition is 35038MB. Which is calculated at 1024KB to 1MB. 35038MB divided by 1024KB equals = 34GB.

8. Let us click the + beside Basic data partition (2), seen in item 1, to expand the partition and view the file system. The file system in the screenshot below is called NONAME [NTFS], which indicates that the partition uses the New Technology File System (NTFS) file system. Let us expand the partition by clicking the + beside NONAME [NTFS], as seen in item 2. This will reveal three folders. There is the orphan folder, and it contains deleted files that were recovered but have no parent folder. Next is the root folder that contains the operating system and user files. The final folder is the unallocated space that represents free space as files.



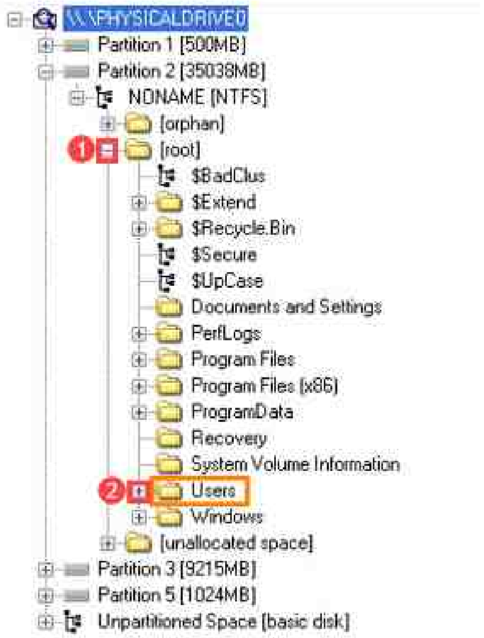
```
\\.\PHYSICALDRIVE0
  Partition 1 [500MB]
  Partition 2 [35038MB]
    NONAME [NTFS]
      [orphan]
      [root]
      [unallocated space]
  Partition 3 [9215MB]
  Partition 5 [1024MB]
  Unpartitioned Space [basic disk]
```

```
000000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 ëR·NTFS    ·····
000000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 A8 0F 00 ·····ø··?·ÿ··¨··
000000020 00 00 00 00 80 00 80 00-FF EF 46 04 00 00 00 00 ········ÿïF·····
000000030 00 00 0C 00 00 00 00 00-02 00 00 00 00 00 00 00 ················
000000040 F6 00 00 00 01 00 00 00-F9 75 4B 22 A2 4B 22 A6 ö·······ùuK"¢K"¦
000000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····ú3À·Ð¼·|ûhÀ·
000000060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E ··hf·Ë····f·>··N
000000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·´A»ªUÍ·r··û
000000080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC Uªu·÷Á··u·éÝ···ì
000000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··´H····ô··Í·
0000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä··X·rá;···uÛ£
0000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8 ··Á.····Z3Û¹· +È
0000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ········Âÿ···è
0000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
0000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
0000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
000000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
000000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
000000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f····fh···
```

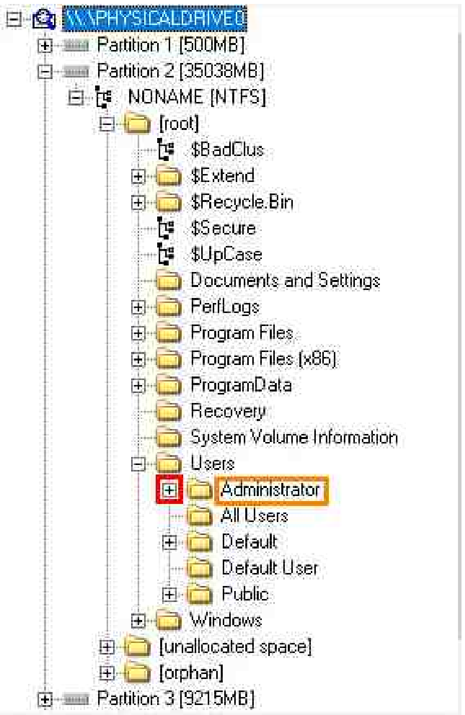
Cursor pos = 0; log sec = 0; phy sec = 1026048

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0/Partition 2 [35038MB]

9. Let us expand the folder called root by clicking the + sign beside it, as seen in item 1. Now that you expanded the root directory, you should begin seeing filenames and folders that are a bit more familiar. This is the root directory of the Windows operating system, and it is represented as the `C:\` drive. In this lab, we will only focus on the users' folders. To get to these folders, look for the folder called Users in the tree pane as seen in item 2 below and click the + sign beside it.



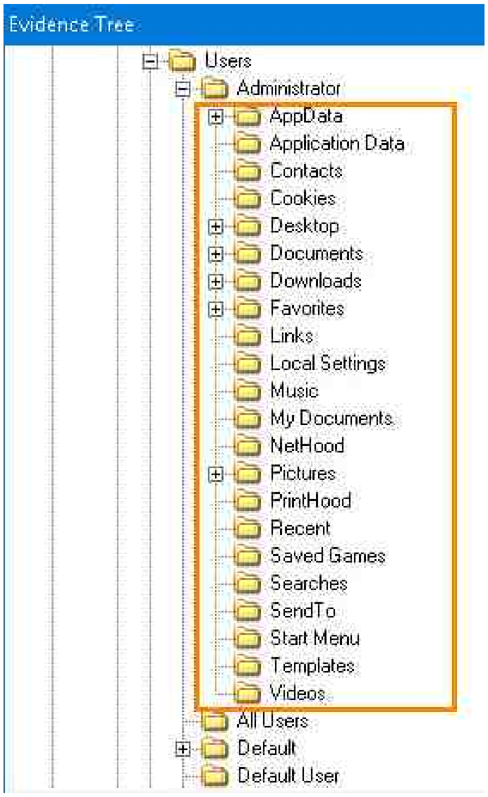
10. Now that you have expanded the Users folder, you will see the list of user profile folders bearing the name of their associated user. There are also some default user folders created by the Windows operating system for various reasons. In addition, there are several registry files that contain many valuable artifacts. Finding and examining the registry files will be covered in a different lab. For now, let us expand the folder called Administrator by clicking the + beside it as seen below.



```
\\.\PHYSICALDRIVE0
    Partition 1 [500MB]
    Partition 2 [35038MB]
        NONAME [NTFS]
            [root]
                $BadClus
                $Extend
                $Recycle.Bin
                $Secure
                $UpCase
                Documents and Settings
                PerfLogs
                Program Files
                Program Files (x86)
                ProgramData
                Recovery
                System Volume Information
                Users
                    Administrator
                    All Users
                    Default
                    Default User
                    Public
                Windows
            [unallocated space]
            [orphan]
    Partition 3 [9215MB]
```

11. You will now see some more familiar folders. These folders are the same folders that the user would see in the navigation pane of the Windows File Explorer. The comparison can be seen below.

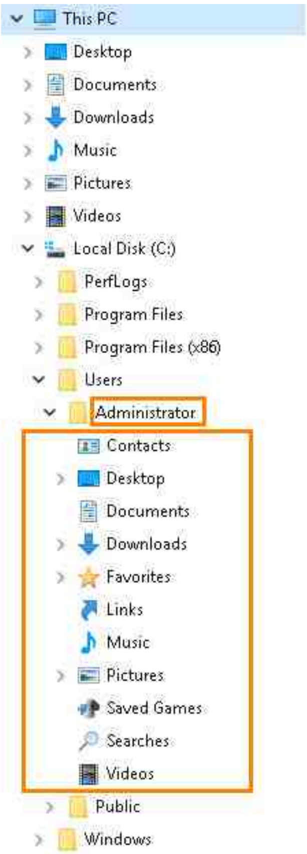
FTK Imager Tree pane



Evidence Tree

Users
Administrator
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
Pictures
PrintHood
Recent
Saved Games
Searches
SendTo
Start Menu
Templates
Videos
All Users
Default
Default User

Windows File Explorer



This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
PerfLogs
Program Files
Program Files (x86)
Users
Administrator
Contacts
Desktop
Documents
Downloads
Favorites
Links
Music
Pictures
Saved Games
Searches
Videos
Public
Windows

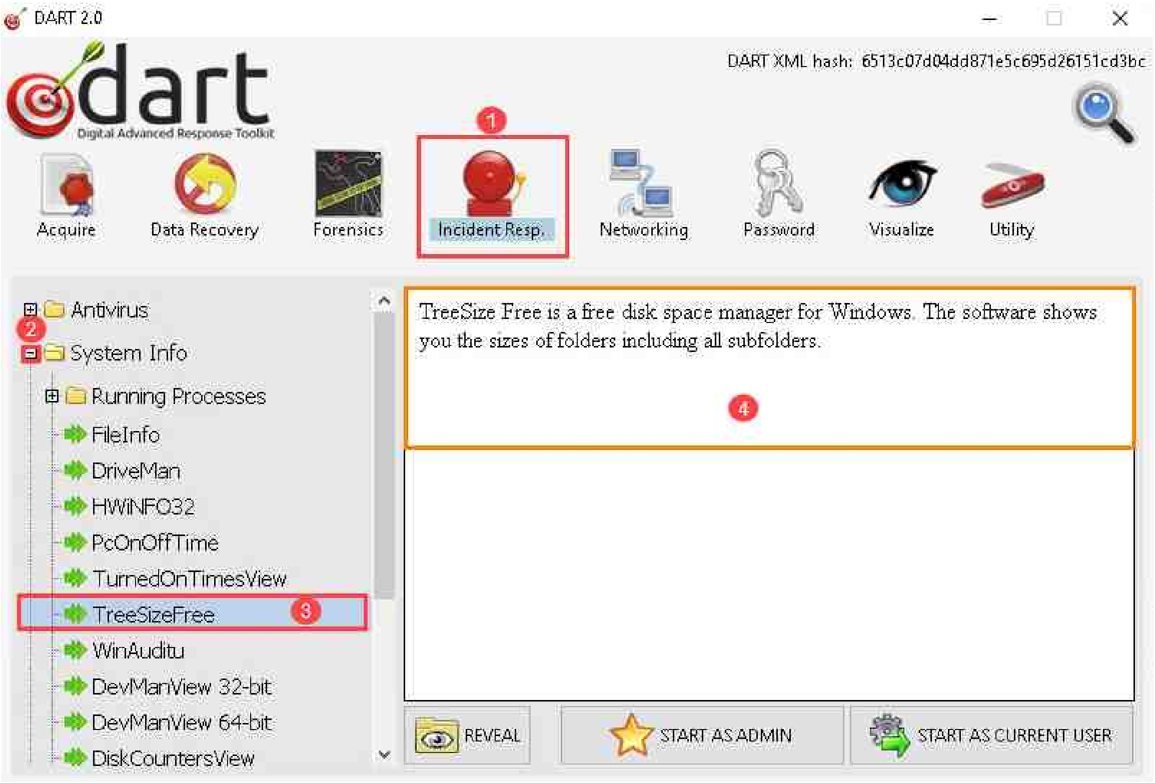
By default, system folders are hidden from the user. Using FTK Imager to view a hard drive will show all hidden folders and files that are stored on a hard drive to include deleted ones. For example, the folder AppData contains files created by different applications installed on the computer. It is not shown in the image on the right, but it is visible within FTK Imager.

12. You will also see several folders that you might not be familiar with. Feel free to browse these folders and familiarize yourself with their contents.
13. Being able to identify the user folders is a vital first step towards associating an individual with the contents of a folder. In the next exercise, you will need to remember these folders and how to get to them, as they will contain the majority of user-created data. Let us close FTK Imager by clicking the X at the top-right corner of the FTK Imager window.

4 Using TreeSizeFree to Get Drive Information

Let us look at another program in DART. This tool is called TreeSizeFree and is used to help get a better understanding of what files are on a computer and where to find them.

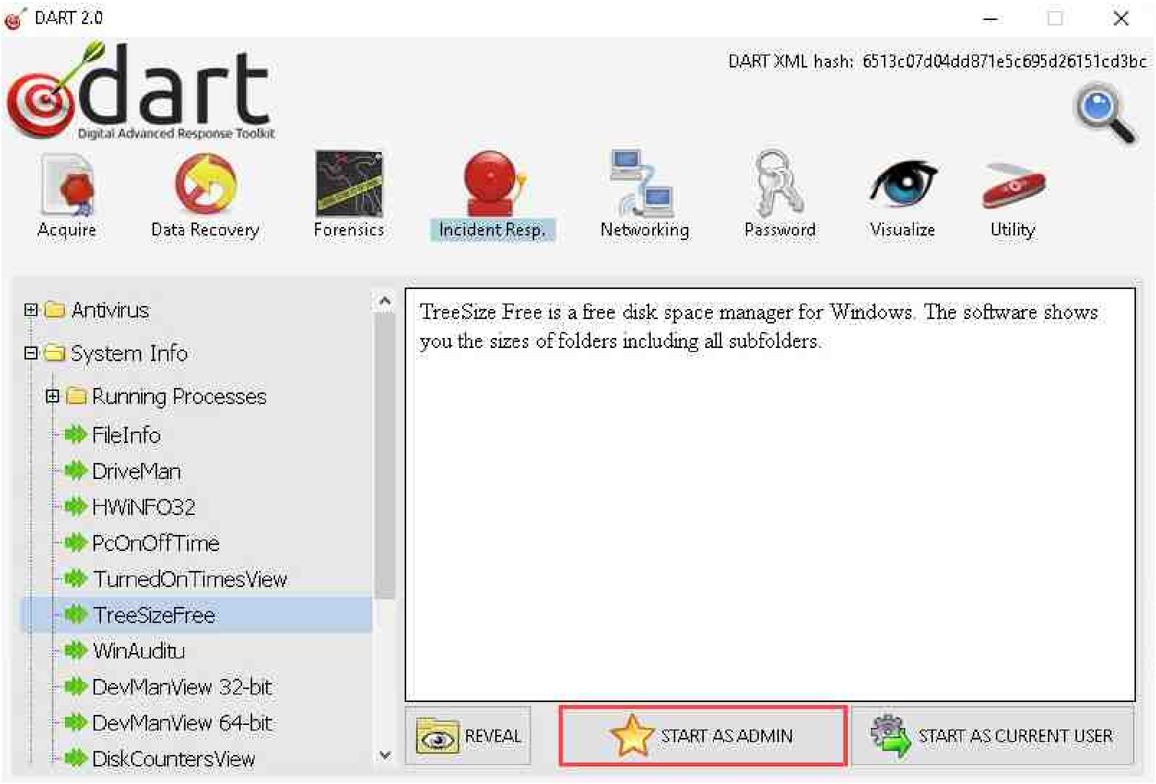
1. Let us begin by closing FTK Imager by clicking the X at the top-right corner of the FTK Imager window. DART should still be open from the last exercise; return to it. You will need to go back to the Incident Resp. category and expand the System Info folder again by clicking the + sign beside it, as seen in items 1 and 2 below. Click the TreeSizeFree application from the list of tools that appear when the folder is expanded, as seen in item 3.



TreeSize Free is a free disk space manager for Windows. The software shows you the sizes of folders including all subfolders.

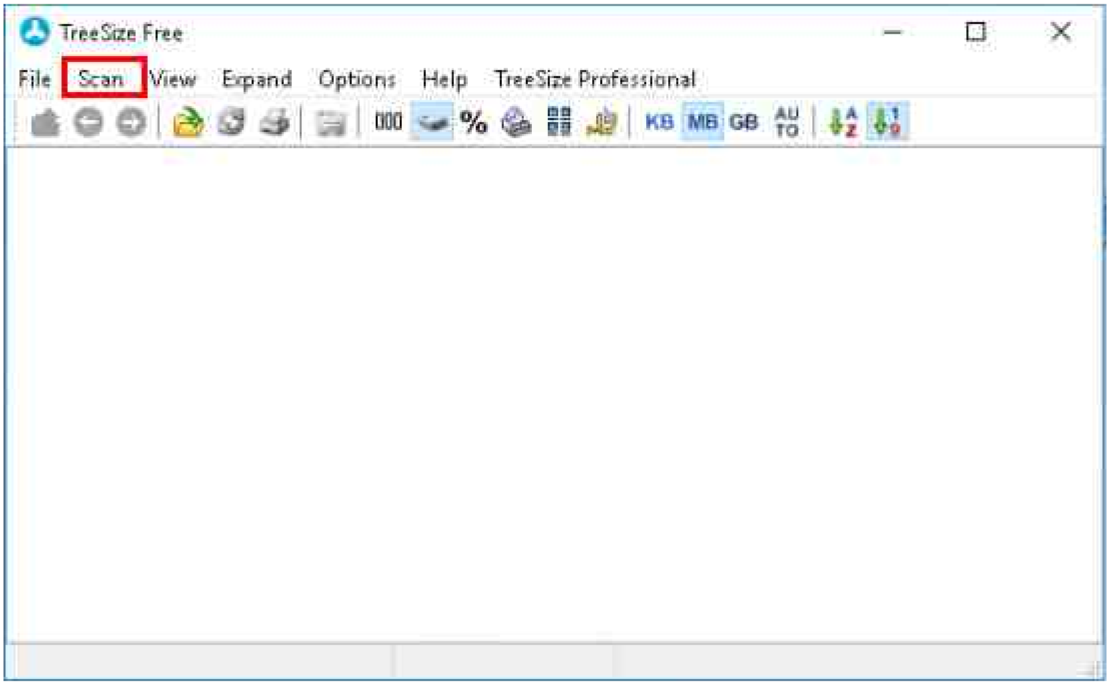
To verify that you have selected the correct tool, read the tool description in the pane on the right as seen in item 4.

2. Now that you have TreeSizeFree selected, let us run it by clicking START AS ADMIN as highlighted below.

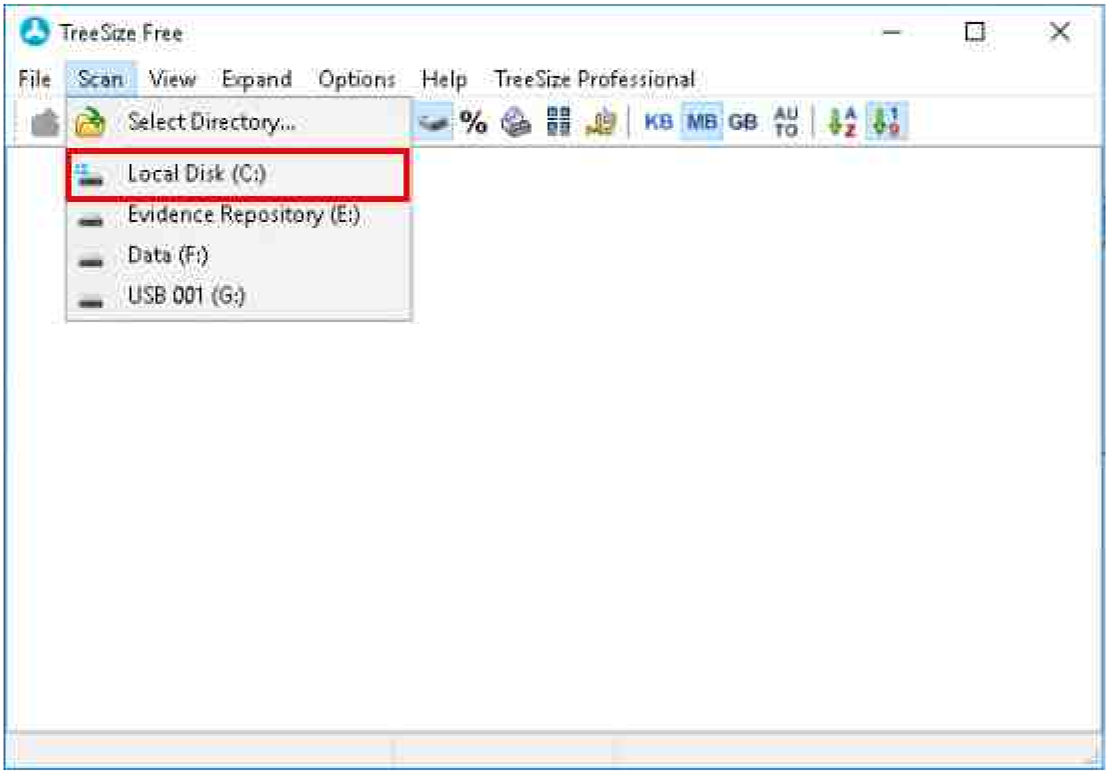


TreeSize Free is a free disk space manager for Windows. The software shows you the sizes of folders including all subfolders.

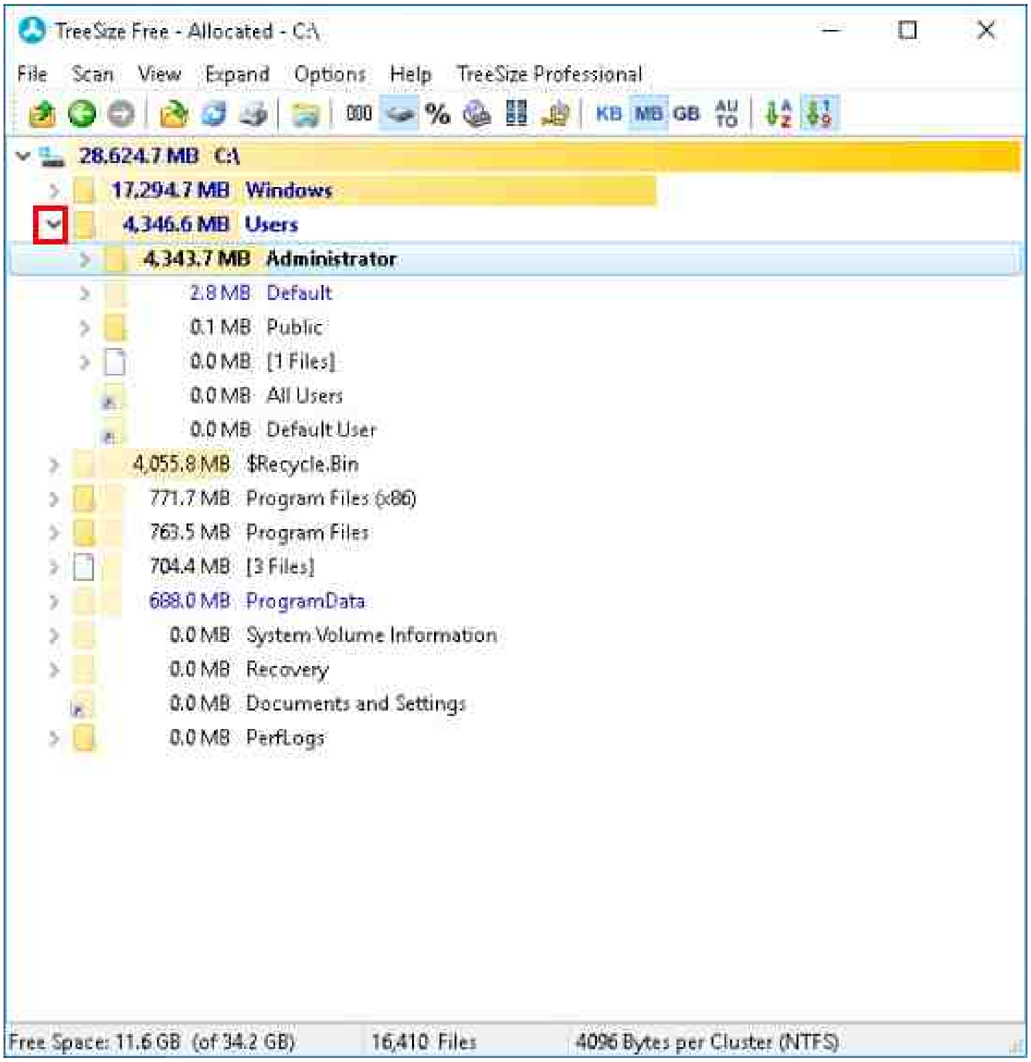
3. The TreeSizeFree main window will appear as seen below. To begin a folder scan, click the Scan dropdown menu option as seen below.



4. You will see several options there. The options will include all the disk drives that are attached to the computer. It will also give you the ability to scan a specific folder of your choice. In this exercise, we will be scanning the Local Disk (C:) volume to identify the largest files. To do this, click the Local Disk (C:) option as highlighted below.



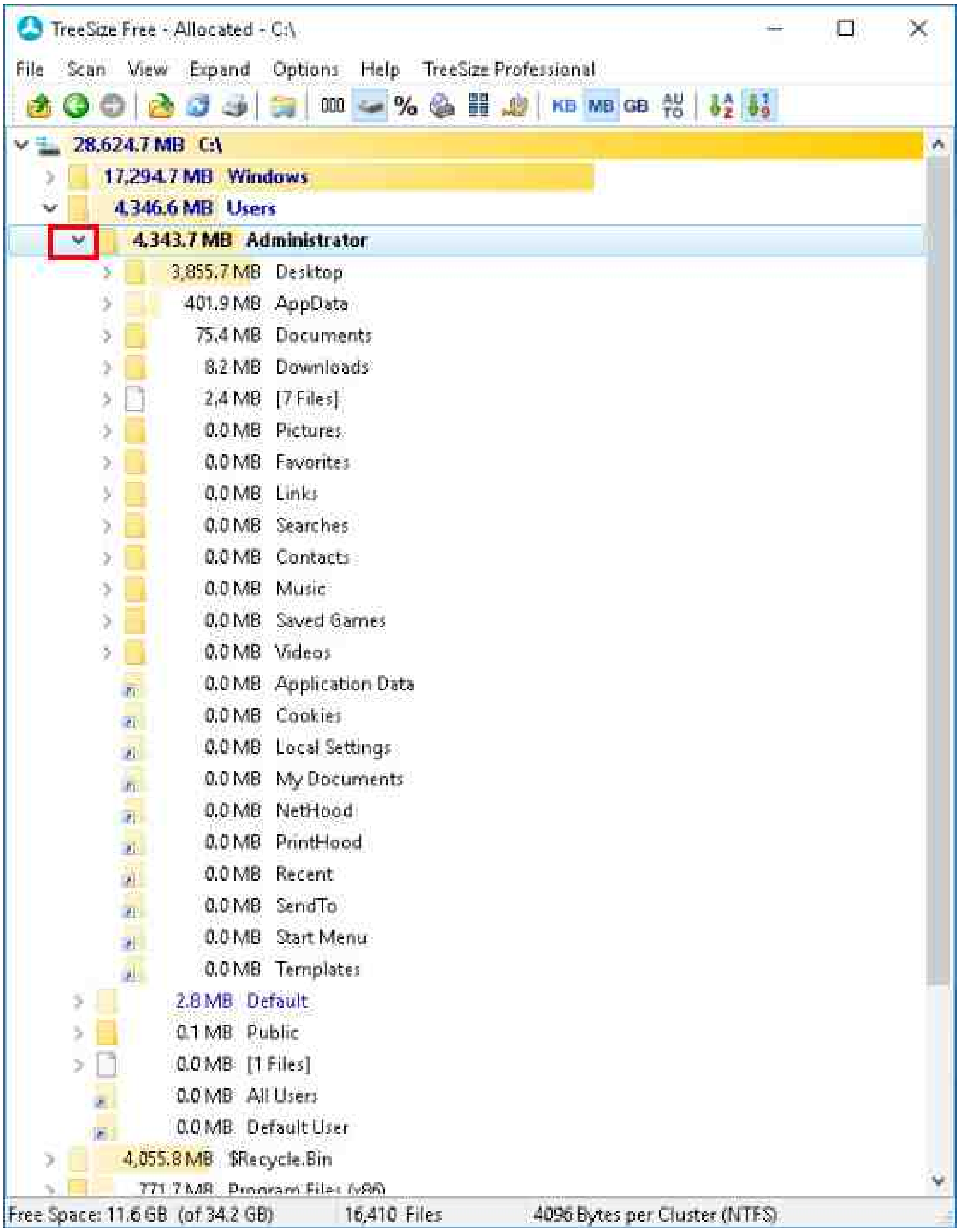
5. The scan will begin as soon as you click the disk drive. If you did everything correctly, you will see data like those in the screenshot below. Let us focus on the users' directories as this is where the average user will store most of their data. Using TreeSizeFree, click the arrow beside the directory called Users to expand it and view the source of the largest files in this folder hierarchy. TreeSizeFree will show you the size of the files in each sub-directory each time you expand a tree item. This is great for narrowing down the specific location of large files.



```
28,624.7 MB  C:\
  17,294.7 MB  Windows
   4,346.6 MB  Users
     4,343.7 MB  Administrator
         2.8 MB  Default
         0.1 MB  Public
         0.0 MB  [1 Files]
         0.0 MB  All Users
         0.0 MB  Default User
   4,055.8 MB  $Recycle.Bin
     771.7 MB  Program Files (x86)
     763.5 MB  Program Files
     704.4 MB  [3 Files]
     688.0 MB  ProgramData
       0.0 MB  System Volume Information
       0.0 MB  Recovery
       0.0 MB  Documents and Settings
       0.0 MB  PerfLogs
```

Free Space: 11.6 GB (of 34.2 GB) 16,410 Files 4096 Bytes per Cluster (NTFS)

6. Next, expand the folder called Administrator and look at the size of the contents of these folders.



```
28,624.7 MB  C:\
  17,294.7 MB  Windows
  4,346.6 MB  Users
    4,343.7 MB  Administrator
      3,855.7 MB  Desktop
      401.9 MB  AppData
      75.4 MB  Documents
      8.2 MB  Downloads
      2.4 MB  [7 Files]
      0.0 MB  Pictures
      0.0 MB  Favorites
      0.0 MB  Links
      0.0 MB  Searches
      0.0 MB  Contacts
      0.0 MB  Music
      0.0 MB  Saved Games
      0.0 MB  Videos
      0.0 MB  Application Data
      0.0 MB  Cookies
      0.0 MB  Local Settings
      0.0 MB  My Documents
      0.0 MB  NetHood
      0.0 MB  PrintHood
      0.0 MB  Recent
      0.0 MB  SendTo
      0.0 MB  Start Menu
      0.0 MB  Templates
    2.8 MB  Default
    0.1 MB  Public
    0.0 MB  [1 Files]
    0.0 MB  All Users
    0.0 MB  Default User
  4,055.8 MB  $Recycle.Bin
  771.7 MB  Program Files (x86)
Free Space: 11.6 GB  (of 34.2 GB)     16,410  Files     4096 Bytes per Cluster (NTFS)
```

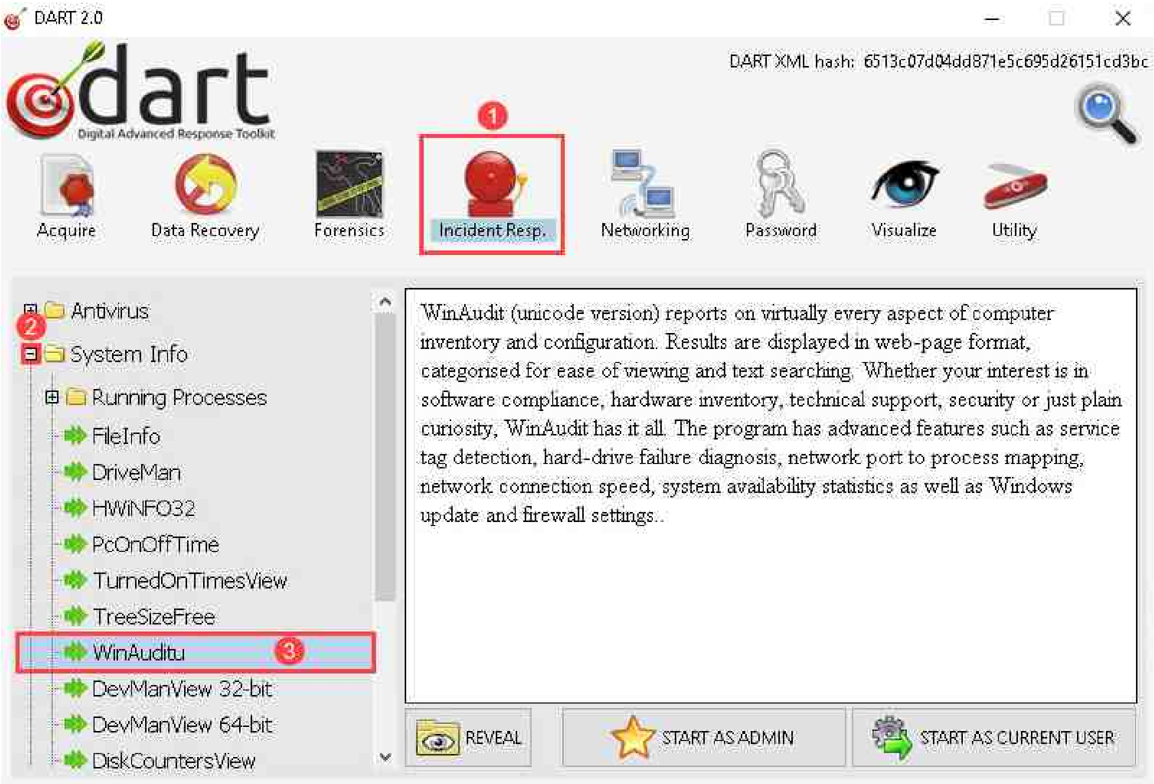
Files and Folders that appear grayed out are known as 'hidden files and folders'. A hidden file or folder doesn't primarily appear in the Windows File Explorer to help prevent important data from being accidentally deleted by users.

7. This method of searching through the file system based on the volume of data is a great way to focus your investigation on areas that might be of interest. This method is great for finding out if certain files were downloaded and where caches of illicit data are stored/hidden on a subject's system.
8. In this exercise, we have reason to believe that a user was using file-sharing software and downloaded a video file to their Downloads folder at C:\ > Users > Administrator > Downloads. Using TreeSizeFree, browse to the mentioned folder and note the name of any video files you see there.
9. Now that you have learned how to navigate the data based on size and the commonly known file paths, let us learn how to gather some other important system information. First, let us close TreeSizeFree by clicking the X at the top-right corner of the TreeSizeFree window.

5 Using WinAudit to Get Drive Information

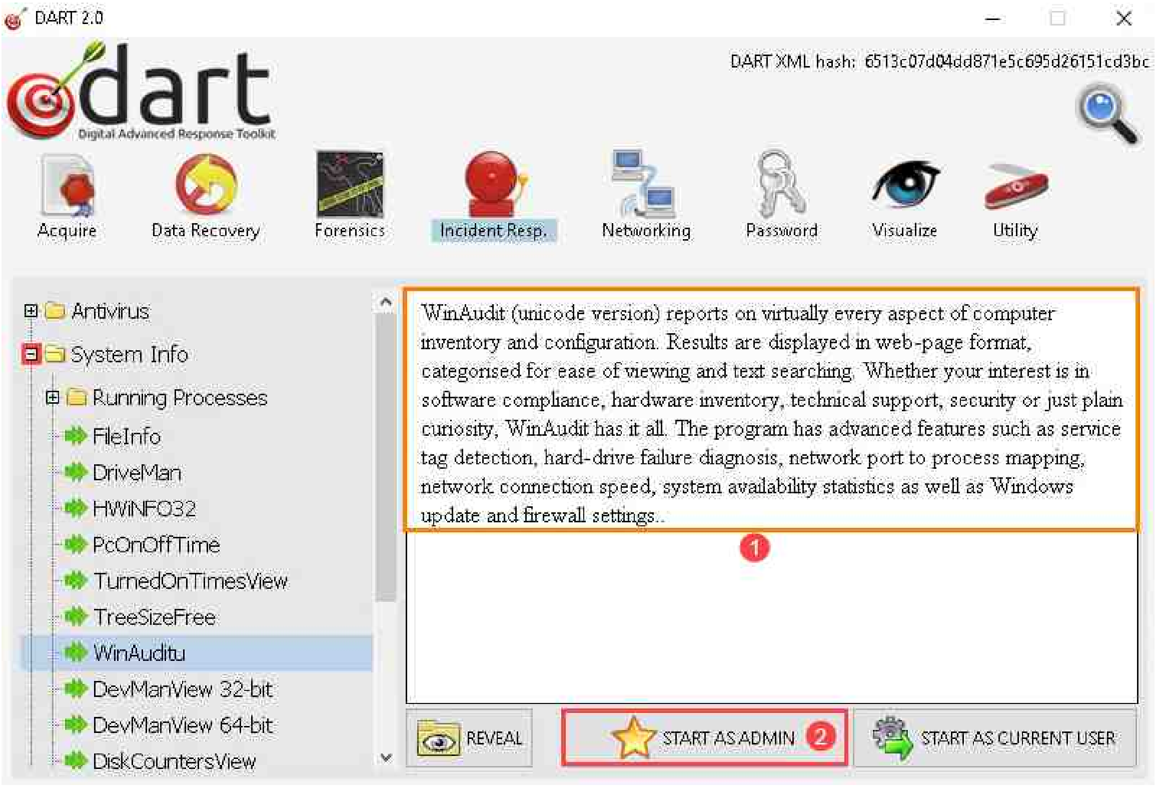
The live acquisition process can be daunting if you are new to it or unsure what kind of data you want to capture for future analysis. There are several tools available that can help to make the data capture process a lot less confusing. In this exercise, you will be using one of the tools that are great for this job. This tool is called WinAudit and is a free-to-use tool that captures a ton of helpful information that aids in understanding the computer and its users better.

1. Let us begin by launching WinAudit. To do this, go back to the DART main window and click the category called Incident Resp., seen in item 1 below. In the tree pane, expand the System Info folder by clicking the + beside it, and then click the application called WinAuditu as highlighted in items 2 and 3 below.



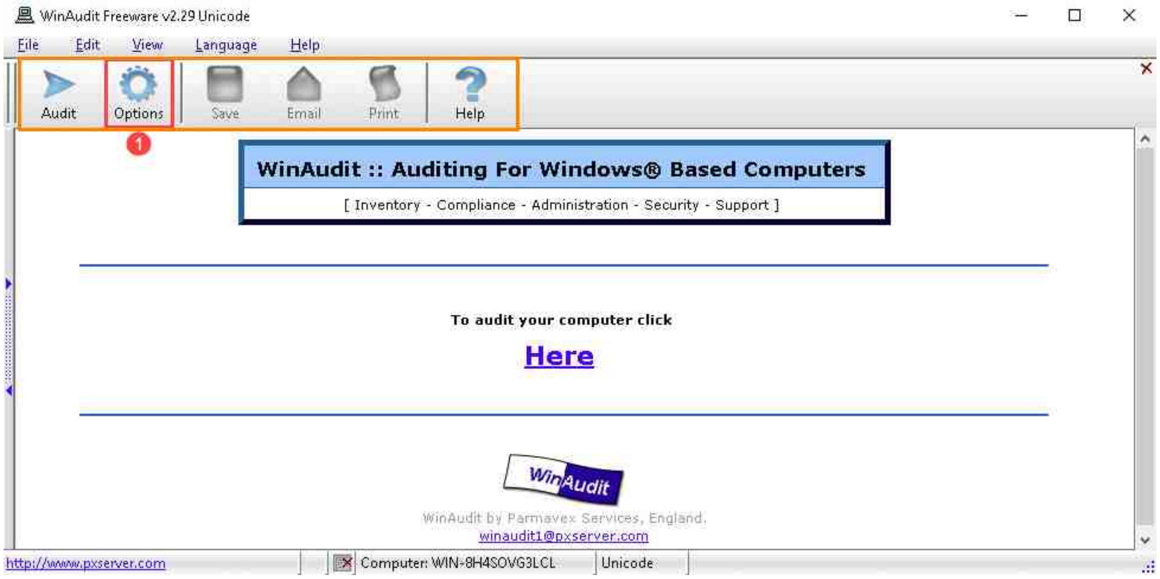
WinAudit (unicode version) reports on virtually every aspect of computer inventory and configuration. Results are displayed in web-page format, categorised for ease of viewing and text searching. Whether your interest is in software compliance, hardware inventory, technical support, security or just plain curiosity, WinAudit has it all. The program has advanced features such as service tag detection, hard-drive failure diagnosis, network port to process mapping, network connection speed, system availability statistics as well as Windows update and firewall settings..

2. If you did everything correctly, you should see the description of the selected tool in the right pane highlighted in item 1 below. Once you have verified that you selected the right option, click the START AS ADMIN button highlighted in item 2 below.

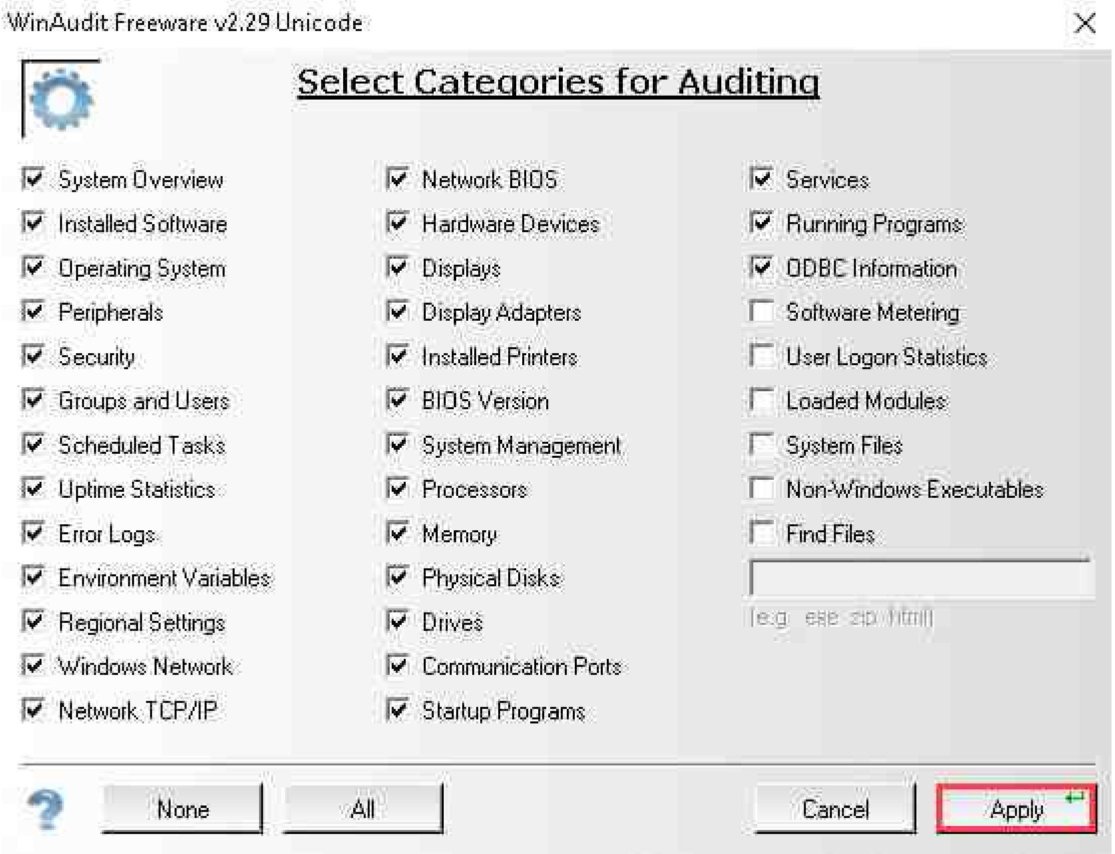


WinAudit (unicode version) reports on virtually every aspect of computer inventory and configuration. Results are displayed in web-page format, categorised for ease of viewing and text searching. Whether your interest is in software compliance, hardware inventory, technical support, security or just plain curiosity, WinAudit has it all. The program has advanced features such as service tag detection, hard-drive failure diagnosis, network port to process mapping, network connection speed, system availability statistics as well as Windows update and firewall settings..

3. You will see the window below; it is the main window for WinAudit v2.29. It is very easy to use. The options highlighted below are the main functions of this simple tool. Let us begin by clicking the Options button highlighted in item 1 below.


WinAudit Freeware v2.29 Unicode
File
Edit
View
Language
Help
Audit
Options
Save
Email
Print
Help
1
WinAudit :: Auditing For Windows® Based Computers
[Inventory - Compliance - Administration - Security - Support]
To audit your computer click
Here
WinAudit
WinAudit by Parmavex Services, England.
winaudit1@pxserver.com
http://www.pxserver.com
Computer: WIN-8H4SOVG3LCL
Unicode

4. The Options menu allows you to choose what data you want to be collected when you run the audit. Look at the many categories available. It gives you an idea of the types of data that will be collected and allows you to narrow your scope if you only want to focus on certain areas. For now, we will leave the default options selected. Let us just click Apply highlighted below.

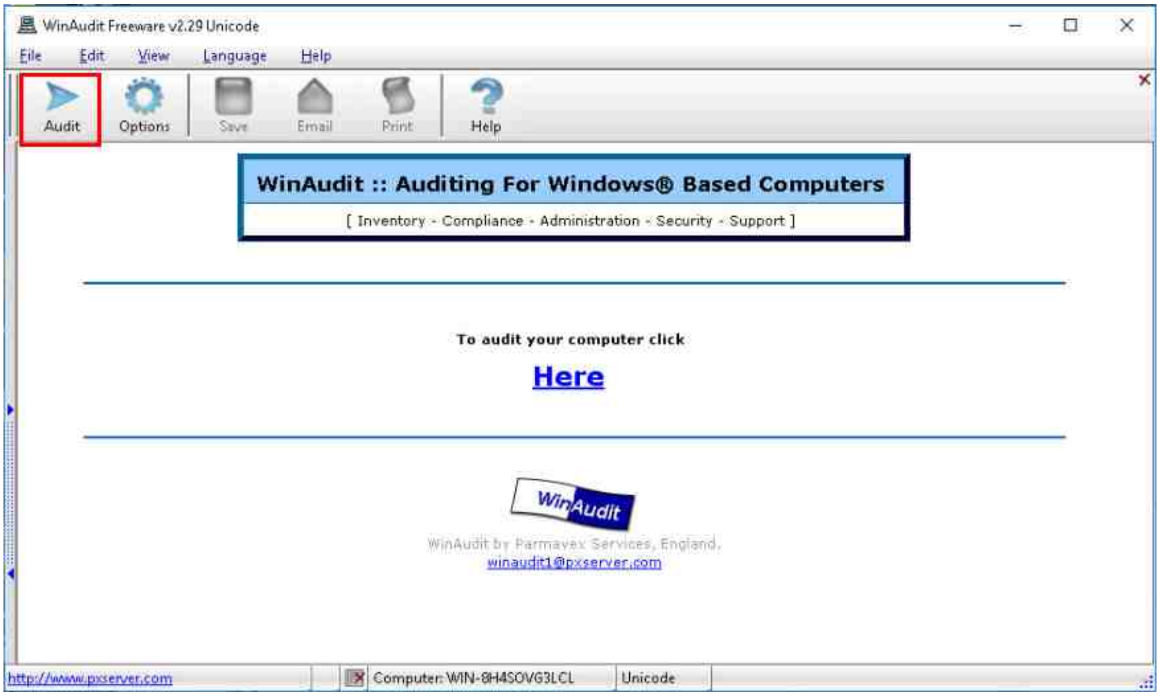


Select Categories for Auditing

- ☑ System Overview
- ☑ Installed Software
- ☑ Operating System
- ☑ Peripherals
- ☑ Security
- ☑ Groups and Users
- ☑ Scheduled Tasks
- ☑ Uptime Statistics
- ☑ Error Logs
- ☑ Environment Variables
- ☑ Regional Settings
- ☑ Windows Network
- ☑ Network TCP/IP
- ☑ Network BIOS
- ☑ Hardware Devices
- ☑ Displays
- ☑ Display Adapters
- ☑ Installed Printers
- ☑ BIOS Version
- ☑ System Management
- ☑ Processors
- ☑ Memory
- ☑ Physical Disks
- ☑ Drives
- ☑ Communication Ports
- ☑ Startup Programs
- ☑ Services
- ☑ Running Programs
- ☑ ODBC Information
- □ Software Metering
- □ User Logon Statistics
- □ Loaded Modules
- □ System Files
- □ Non-Windows Executables
- □ Find Files

(e.g. .exe .zip .html)

5. Now that we are back at the main window, let us run an audit. To run the audit, click the Audit button highlighted below.



WinAudit :: Auditing For Windows® Based Computers

[Inventory - Compliance - Administration - Security - Support]

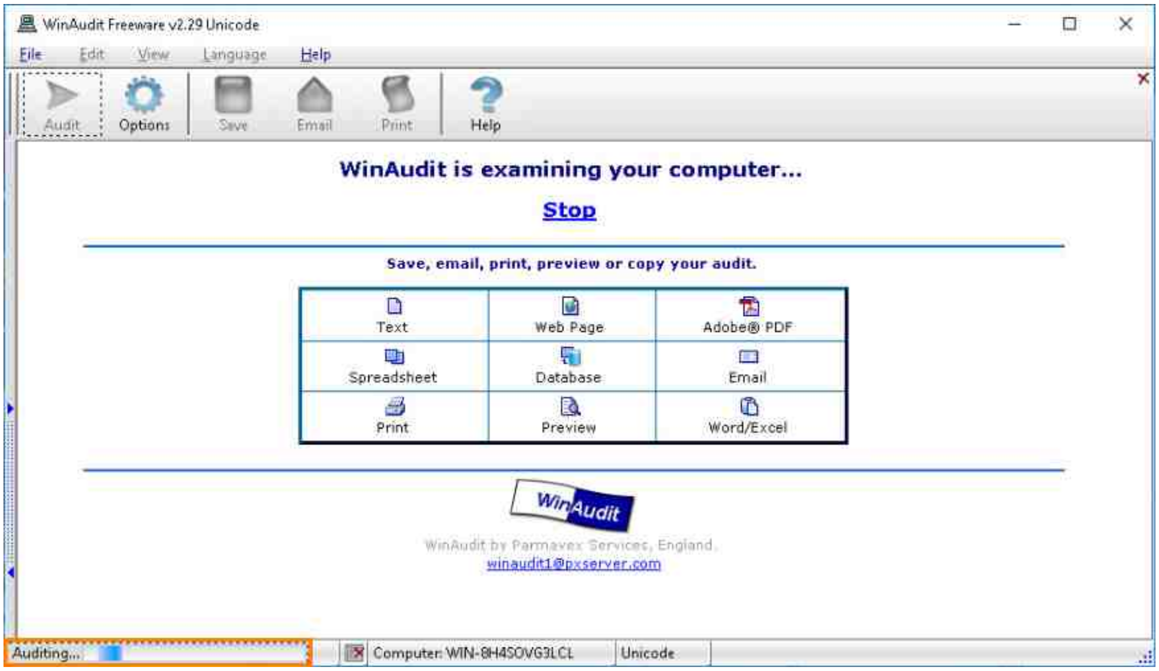
To audit your computer click

Here

WinAudit by Parmavex Services, England.
winaudit1@pxserver.com

http://www.pxserver.com | Computer: WIN-8H4SOVG3LCL | Unicode

6. The process will begin; its duration is dependent on the hardware specifications of the host. In the bottom-left corner of the main window, you will see the word Auditing… along with an animation as highlighted below. This is an indication that it is still gathering data.



WinAudit is examining your computer...

Stop

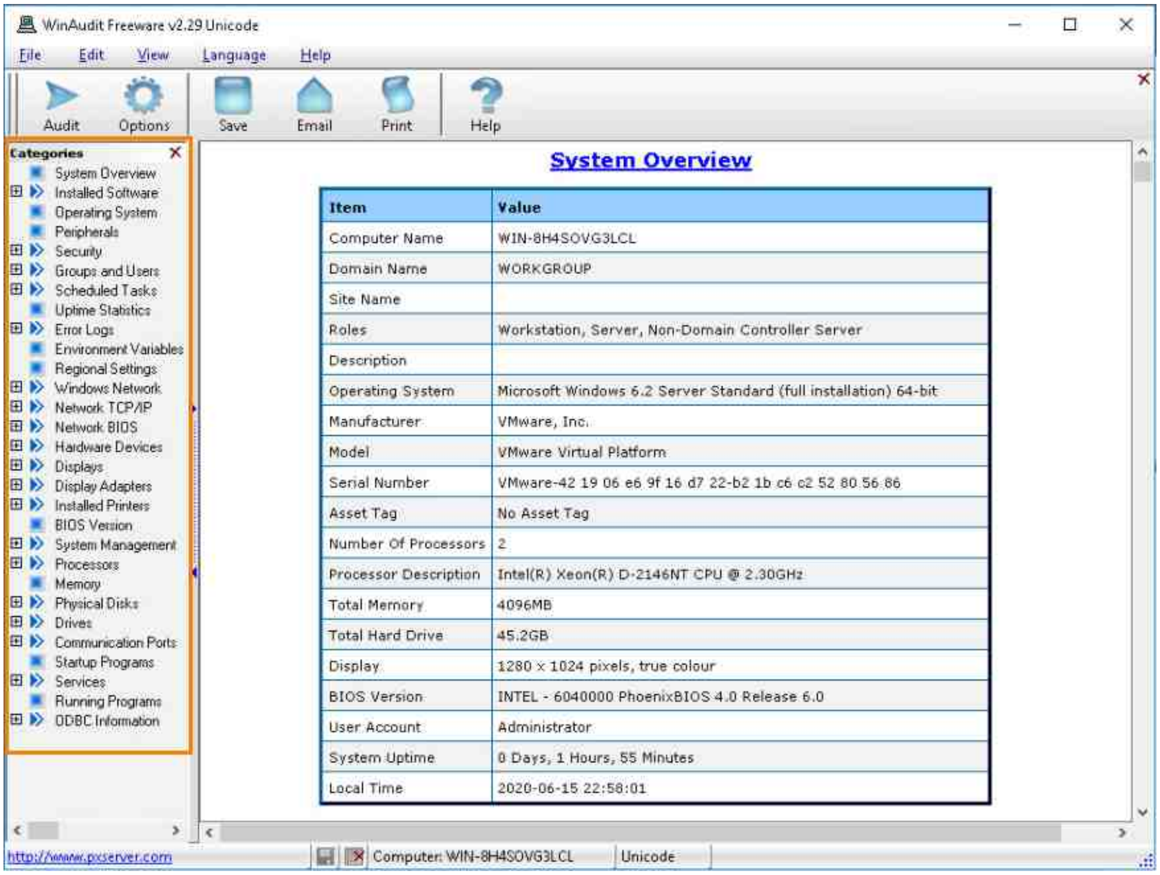
Save, email, print, preview or copy your audit.

Text	Web Page	Adobe® PDF
Spreadsheet	Database	Email
Print	Preview	Word/Excel

WinAudit by Parmavex Services, England.
winaudit1@pxserver.com

Auditing... | Computer: WIN-8H4SOVG3LCL | Unicode

7. Once the audit is done, you will see the familiar navigation pane. In this tool, it is called Categories pane, and, as usual, it is on the left side of the window, as highlighted below. This pane contains the various categories of captured data.

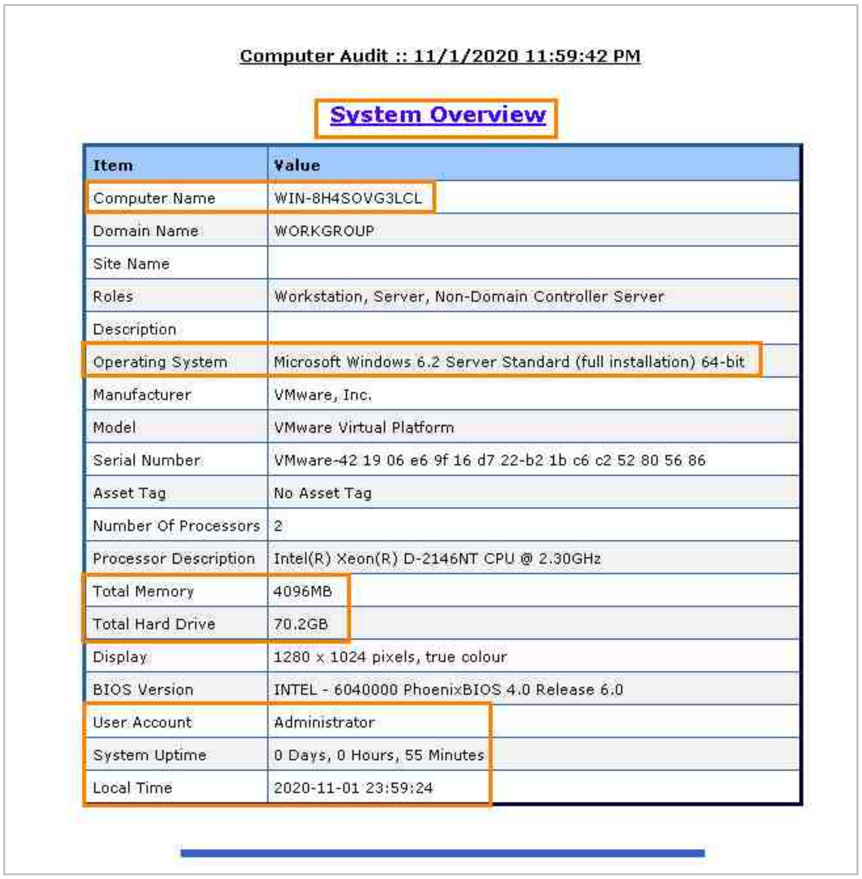


System Overview

Item	Value
Computer Name	WIN-8H4SOVG3LCL
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server, Non-Domain Controller Server
Description	
Operating System	Microsoft Windows 6.2 Server Standard (full installation) 64-bit
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Serial Number	VMware-42 19 06 e6 9f 16 d7 22-b2 1b c6 c2 52 80 56 86
Asset Tag	No Asset Tag
Number Of Processors	2
Processor Description	Intel(R) Xeon(R) D-2146NT CPU @ 2.30GHz
Total Memory	4096MB
Total Hard Drive	45.2GB
Display	1280 x 1024 pixels, true colour
BIOS Version	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
User Account	Administrator
System Uptime	0 Days, 1 Hours, 55 Minutes
Local Time	2020-06-15 22:58:01

8. For this exercise, we will be exporting the results as you normally would when collecting live data. Before we do this, though, let us take a quick look at some of the data.

9. If you notice, the System Overview category is already being displayed. In this category, you can find operating system and computer information such as the NetBIOS name, the operating system version, the hard drive size, and the total RAM, among others, as highlighted below. This is the top of the audit report you generated. To view the other categories, you can scroll down in the window. It is quite lengthy!

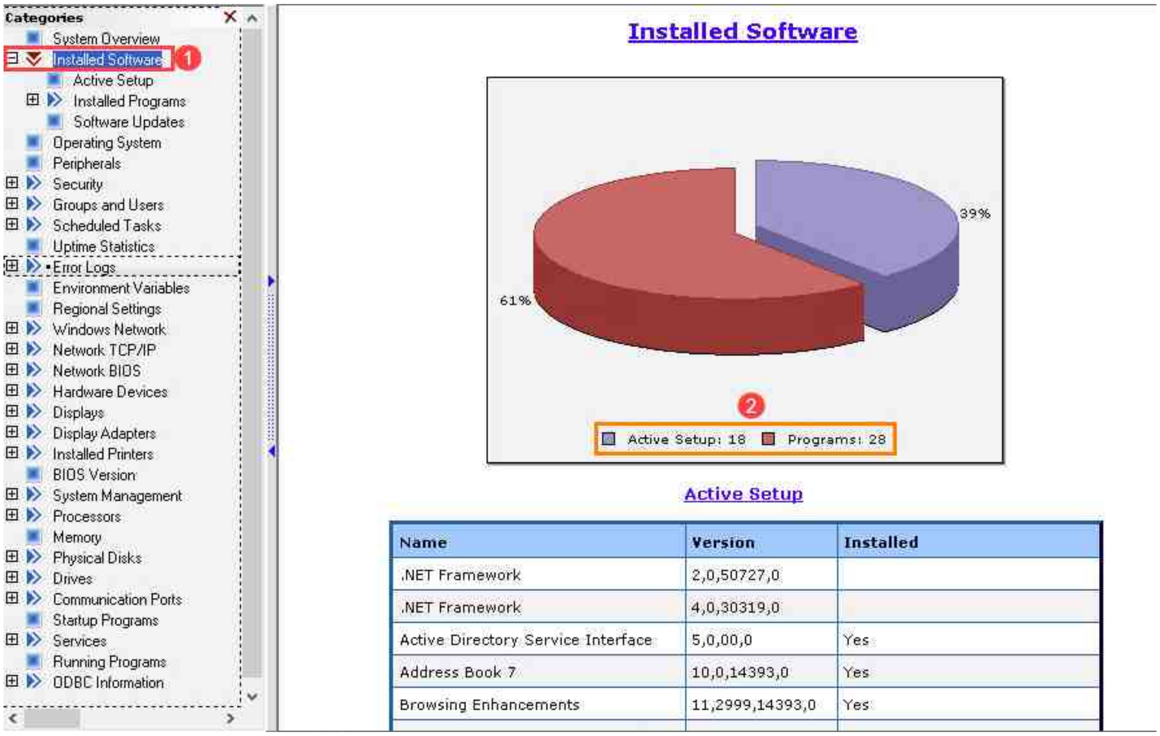


Computer Audit :: 11/1/2020 11:59:42 PM

System Overview

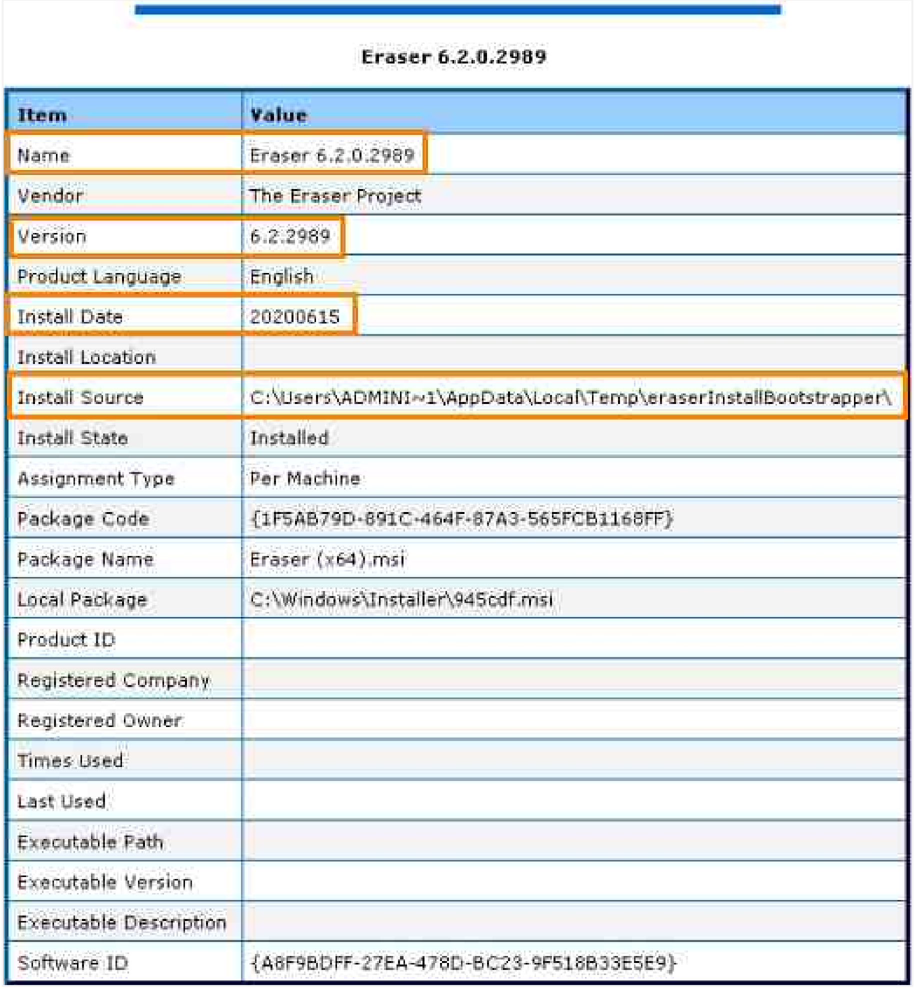
Item	Value
Computer Name	WIN-8H4SOVG3LCL
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server, Non-Domain Controller Server
Description	
Operating System	Microsoft Windows 6.2 Server Standard (full installation) 64-bit
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Serial Number	VMware-42 19 06 e6 9f 16 d7 22-b2 1b c6 c2 52 80 56 86
Asset Tag	No Asset Tag
Number Of Processors	2
Processor Description	Intel(R) Xeon(R) D-2146NT CPU @ 2.30GHz
Total Memory	4096MB
Total Hard Drive	70.2GB
Display	1280 x 1024 pixels, true colour
BIOS Version	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
User Account	Administrator
System Uptime	0 Days, 0 Hours, 55 Minutes
Local Time	2020-11-01 23:59:24

10. Now let us look at the Installed Software category by clicking Installed software in the Categories pane highlighted in item 1 below. This will show you a neat pie chart that shows the difference between the operating system software that is installed by default (called Active Setup highlighted below) and the software that was manually installed by the user (called Programs highlighted below).



Name	Version	Installed
.NET Framework	2,0,50727,0	
.NET Framework	4,0,30319,0	
Active Directory Service Interface	5,0,00,0	Yes
Address Book 7	10,0,14393,0	Yes
Browsing Enhancements	11,2999,14393,0	Yes

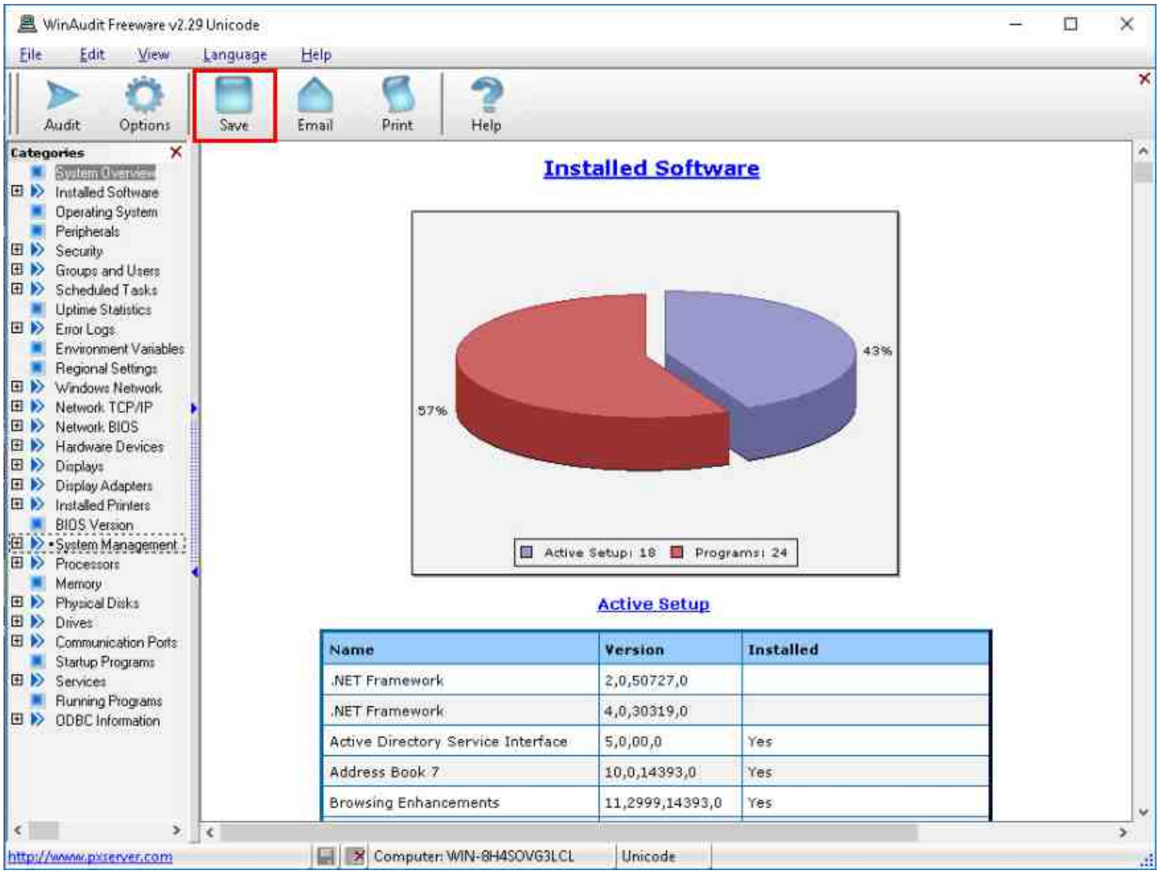
11. Still, in the Installed Software category, scroll down in the right pane to view a list of the installed software from both the Active Setup and Programs categories. Browse until you see the Installed Programs heading. This will provide detailed information about the manually installed programs. As you can see in the highlighted area, the name, version number, the install date, and the source of the installed program are all listed along with lots of other data. Please note that the type of data captured for each application can vary.



Eraser 6.2.0.2989

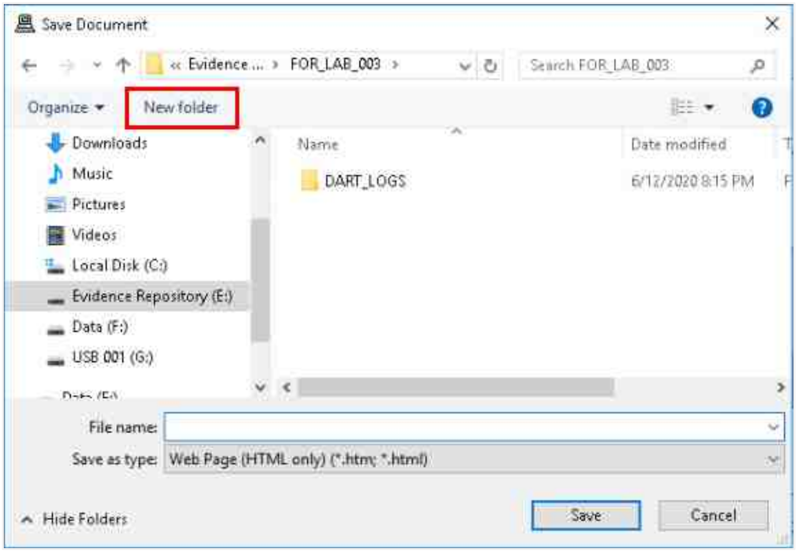
Item	Value
Name	Eraser 6.2.0.2989
Vendor	The Eraser Project
Version	6.2.2989
Product Language	English
Install Date	20200615
Install Location	
Install Source	C:\Users\ADMINI~1\AppData\Local\Temp\eraserInstallBootstrapper\
Install State	Installed
Assignment Type	Per Machine
Package Code	{1F5AB79D-891C-464F-87A3-565FCB1168FF}
Package Name	Eraser (x64).msi
Local Package	C:\Windows\Installer\945cdf.msi
Product ID	
Registered Company	
Registered Owner	
Times Used	
Last Used	
Executable Path	
Executable Version	
Executable Description	
Software ID	{A8F9BDFF-27EA-478D-BC23-9F518B33E5E9}

12. As you can see from the audit, the type of data collected is voluminous. For now, let us save what we have captured so that it can be reviewed later. To do this, go back to the toolbar and click Save as highlighted below.



Name	Version	Installed
.NET Framework	2,0,50727,0	
.NET Framework	4,0,30319,0	
Active Directory Service Interface	5,0,00,0	Yes
Address Book 7	10,0,14393,0	Yes
Browsing Enhancements	11,2999,14393,0	Yes

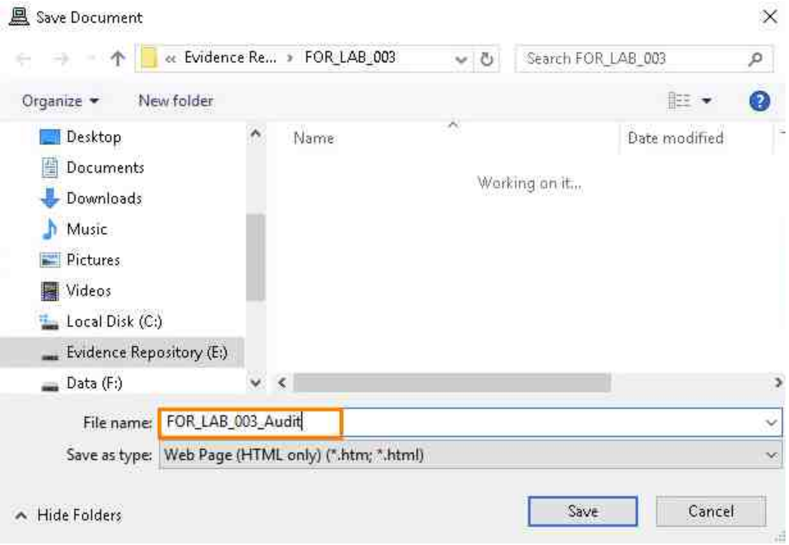
13. The Save Document window will appear, allowing you to browse to the location to which you want the file to be downloaded. Always remember to store the file on a different volume than the one you are performing the live analysis on. In this exercise, we will be saving the data to the Evidence Repository (E:) volume. To do this, navigate to Evidence Repository (E:) > FOR_LAB_003 and click New Folder as highlighted below.



File name:

Save as type: Web Page (HTML only) (*.htm; *.html)

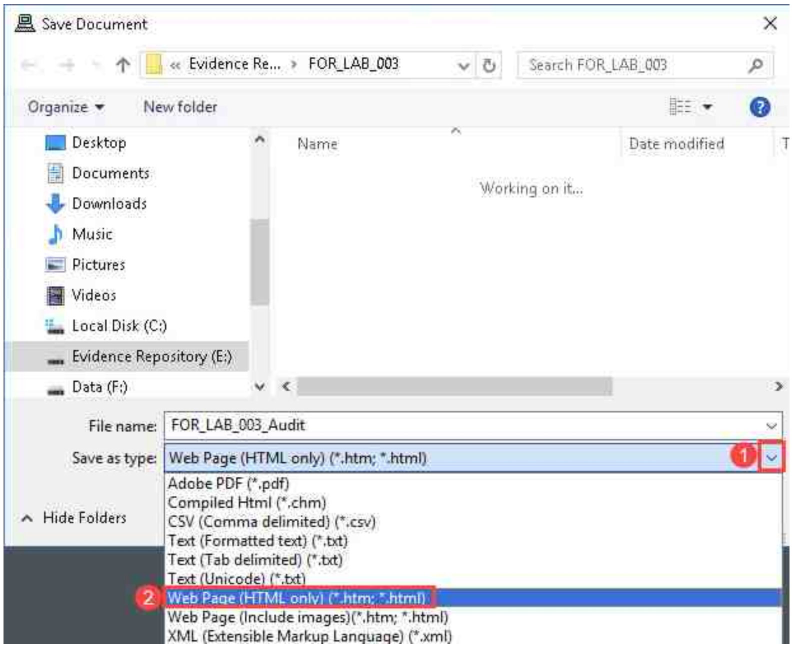
14. Name the new folder FOR_LAB_003_Audit and double-click it to open. Now that we have the location, let us name the file. Give it the name `FOR_LAB_003_Audit,` as highlighted below.



File name: FOR_LAB_003_Audit

Save as type: Web Page (HTML only) (*.htm; *.html)

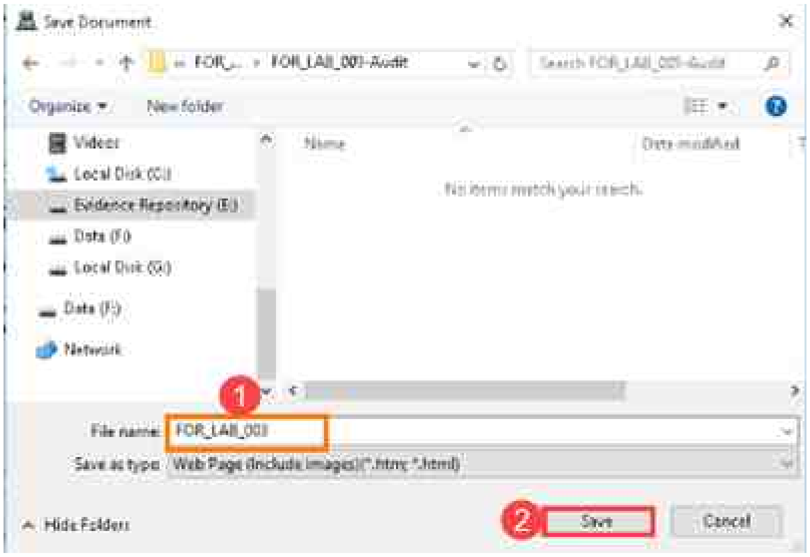
15. Next, let us save it as an HTML file. To do this, click the Save as type dropdown menu highlighted in item 1. From the dropdown menu, click Web Page (Include images) (*.htm;*.html) as highlighted below.



File name: FOR_LAB_003_Audit

Save as type: Web Page (HTML only) (*.htm; *.html)

16. Now that you have the right path, name, and format selected, you can click Save as highlighted in item 2 below.



File name: FOR_LAB_003

Save as type: Web Page (Include images)(*.htm; *.html)

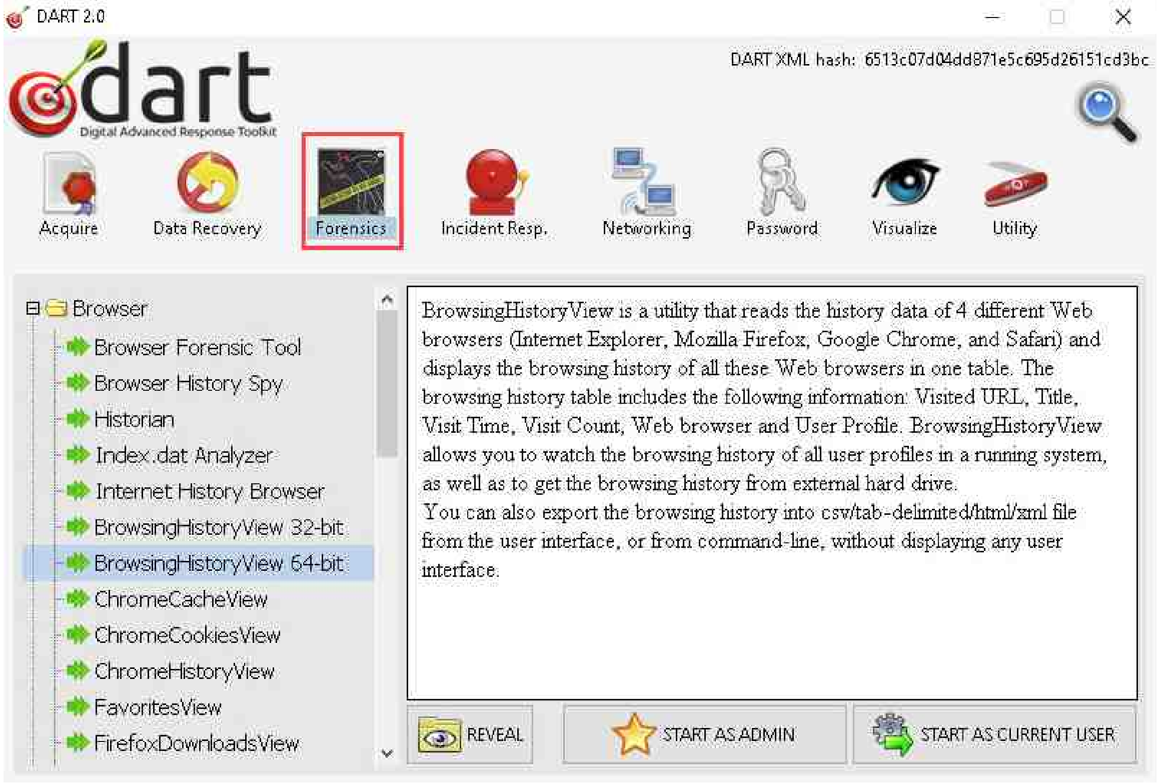
17. Now you have successfully saved the report to an HTML file in your evidence drive. This data can later be reviewed and used to assist in examining the computer. It can also be reviewed immediately using your onsite forensic workstation to gather the information that can lead to the recovery of additional evidence items.
18. Let us move on to one of the most important digital forensic artifacts on any computer, the browsing history. First, let us close WinAudit by clicking the X at the top-right corner of the WinAudit window.

> To view the html report, browse to the folder you saved it and double-click the file you created called FOR_LAB_003.htm

6 Using Browser History View to View and Capture Browsing History

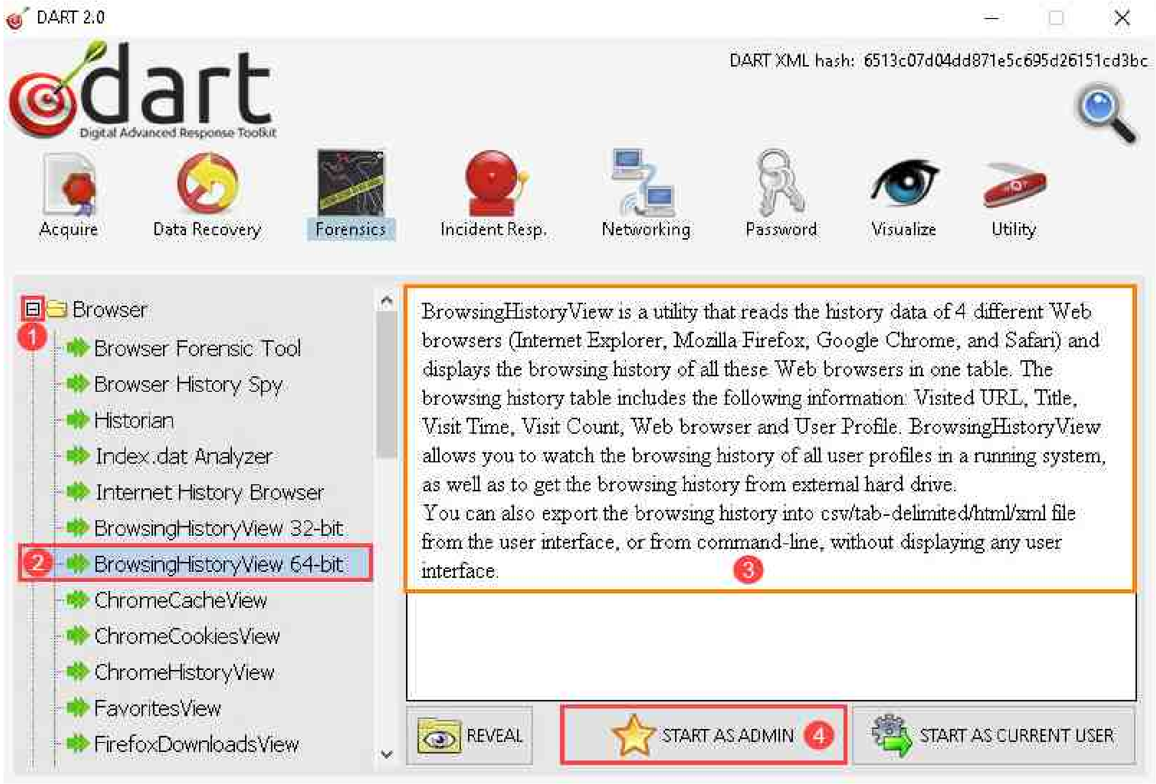
As you have seen in the previous exercises, the live analysis is all about quickly accessing some data for use before shutting the computer down. In some investigations, you may need to see if the user accessed certain websites. You may also want to check if they performed certain web searches. Web history is one of the artifacts that is going to provide you with this information.

1. One of the tools we use to view this history in a live environment is BrowsingHistoryView. This is another lightweight tool that can get the job done quickly. In this lab, you will learn how to open, view, and save the web history of a host. Let us begin by going back to the DART main window and click the Forensics category as highlighted below.



BrowsingHistoryView is a utility that reads the history data of 4 different Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Safari) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile. BrowsingHistoryView allows you to watch the browsing history of all user profiles in a running system, as well as to get the browsing history from external hard drive.
You can also export the browsing history into csv/tab-delimited/html/xml file from the user interface, or from command-line, without displaying any user interface.

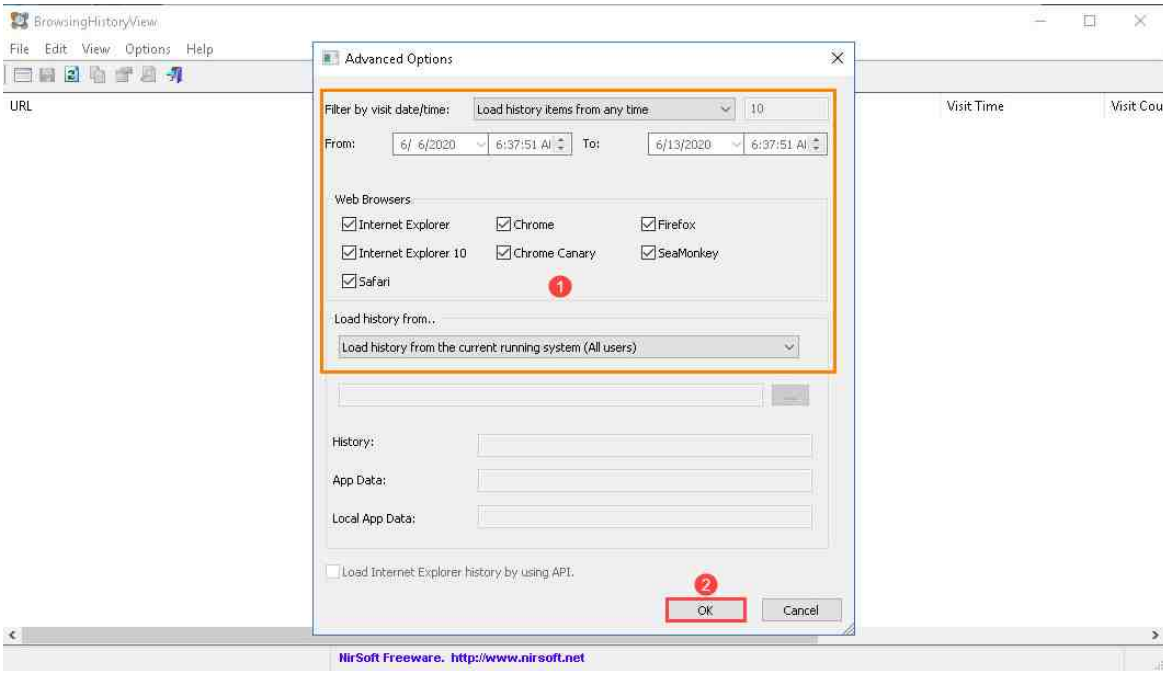
2. Now that you can see the list of Forensics tools in DART, click the + beside the Browser folder and then click BrowsingHistoryView 64-bit as highlighted in items 1 and 2. As usual, look at the right pane highlighted in item 3 below to verify that you have the right program selected. After you have verified this, click START AS ADMIN as highlighted in item 4.



DART XML hash: 6513c07d04dd871e5c695d26151cd3bc

BrowsingHistoryView is a utility that reads the history data of 4 different Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Safari) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile. BrowsingHistoryView allows you to watch the browsing history of all user profiles in a running system, as well as to get the browsing history from external hard drive.
You can also export the browsing history into csv/tab-delimited/html/xml file from the user interface, or from command-line, without displaying any user interface.

3. The BrowsingHistoryView software should now be open. You will be presented with the main window and a pop-up window called Advanced Options that appears in front of the main window. In this exercise, we will leave everything as the default and click OK as seen below.


BrowsingHistoryView
File Edit View Options Help
URL
Visit Time
Visit Cou
Advanced Options
1
2
OK
Cancel
NirSoft Freeware. http://www.nirsoft.net

Filter by visit date/time: Load history items from any time 10

From: 6/ 6/2020 6:37:51 AM To: 6/13/2020 6:37:51 AM

Web Browsers

☑ Internet Explorer ☑ Chrome ☑ Firefox

☑ Internet Explorer 10 ☑ Chrome Canary ☑ SeaMonkey

☑ Safari

Load history from..

Load history from the current running system (All users)

History:

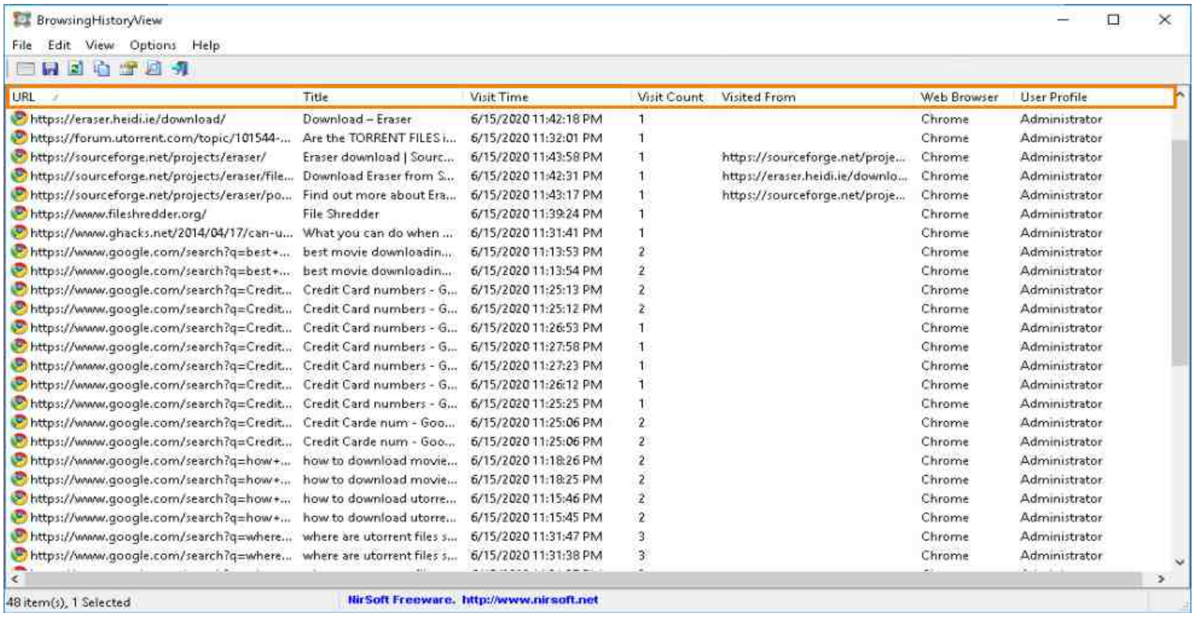
App Data:

Local App Data:

□ Load Internet Explorer history by using API.

The Advanced Options window gives you more flexibility. You can filter the web history by dates, browser, and the user account you want to target.

4. The BrowsingHistoryView software will now present you with all the browsing history it finds. You will see a window like the one below. As you see, there are several columns that provide useful data. The columns provide data about the specific URL that was visited, the title of the web page, the time it was visited, the number of times it was visited (Visit Count), any redirections (Visited From), the name of the web browser and the username of the person who accessed it. The column titles are highlighted below.

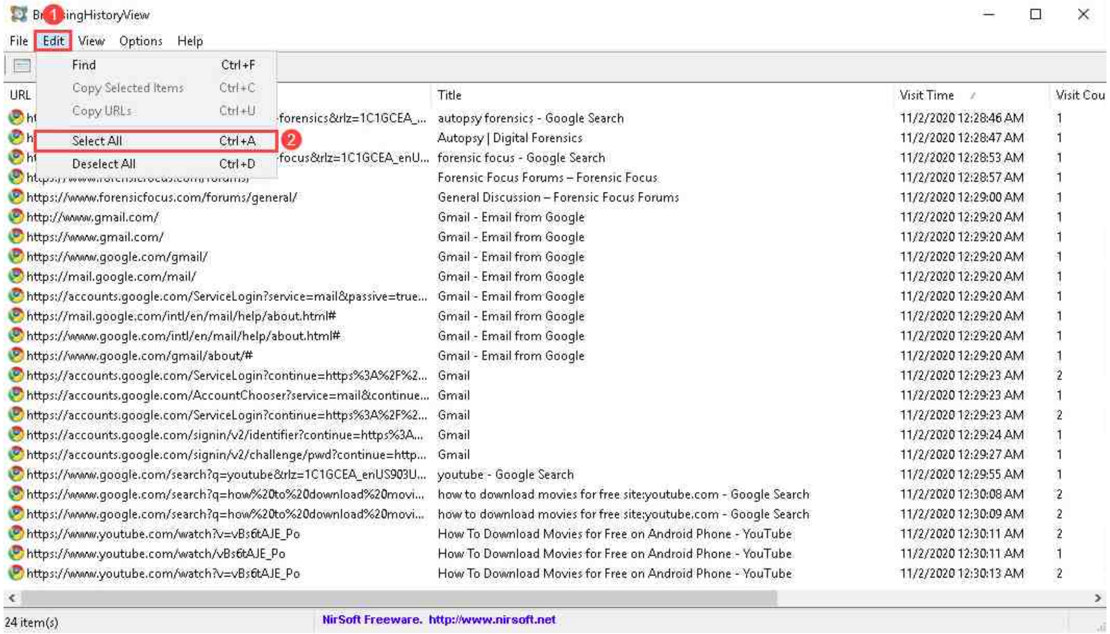


URL	Title	Visit Time	Visit Count	Visited From	Web Browser	User Profile
https://eraser.heidi.ie/download/	Download – Eraser	6/15/2020 11:42:18 PM	1		Chrome	Administrator
https://forum.utorrent.com/topic/101544-...	Are the TORRENT FILES i...	6/15/2020 11:32:01 PM	1		Chrome	Administrator
https://sourceforge.net/projects/eraser/	Eraser download | Sourc...	6/15/2020 11:43:58 PM	1	https://sourceforge.net/proje...	Chrome	Administrator
https://sourceforge.net/projects/eraser/file...	Download Eraser from S...	6/15/2020 11:42:31 PM	1	https://eraser.heidi.ie/downlo...	Chrome	Administrator
https://sourceforge.net/projects/eraser/po...	Find out more about Era...	6/15/2020 11:43:17 PM	1	https://sourceforge.net/proje...	Chrome	Administrator
https://www.fileshredder.org/	File Shredder	6/15/2020 11:39:24 PM	1		Chrome	Administrator
https://www.ghacks.net/2014/04/17/can-u...	What you can do when ...	6/15/2020 11:31:41 PM	1		Chrome	Administrator
https://www.google.com/search?q=best+...	best movie downloadin...	6/15/2020 11:13:53 PM	2		Chrome	Administrator
https://www.google.com/search?q=best+...	best movie downloadin...	6/15/2020 11:13:54 PM	2		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:25:13 PM	2		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:25:12 PM	2		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:26:53 PM	1		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:27:58 PM	1		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:27:23 PM	1		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:26:12 PM	1		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Card numbers - G...	6/15/2020 11:25:25 PM	1		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Carde num - Goo...	6/15/2020 11:25:06 PM	2		Chrome	Administrator
https://www.google.com/search?q=Credit...	Credit Carde num - Goo...	6/15/2020 11:25:06 PM	2		Chrome	Administrator
https://www.google.com/search?q=how+...	how to download movie...	6/15/2020 11:18:26 PM	2		Chrome	Administrator
https://www.google.com/search?q=how+...	how to download movie...	6/15/2020 11:18:25 PM	2		Chrome	Administrator
https://www.google.com/search?q=how+...	how to download utorre...	6/15/2020 11:15:46 PM	2		Chrome	Administrator
https://www.google.com/search?q=how+...	how to download utorre...	6/15/2020 11:15:45 PM	2		Chrome	Administrator
https://www.google.com/search?q=where...	where are utorrent files s...	6/15/2020 11:31:47 PM	3		Chrome	Administrator
https://www.google.com/search?q=where...	where are utorrent files s...	6/15/2020 11:31:38 PM	3		Chrome	Administrator

48 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

5. You can scroll through the list to see if you are familiar with some of the websites that this user visited. Now let us export this browsing data to our Evidence Repository (E:) volume. To do this, begin by clicking Edit from the Menu Bar and then clicking Select All highlighted below. This will highlight all the historical artifacts that the software collected.

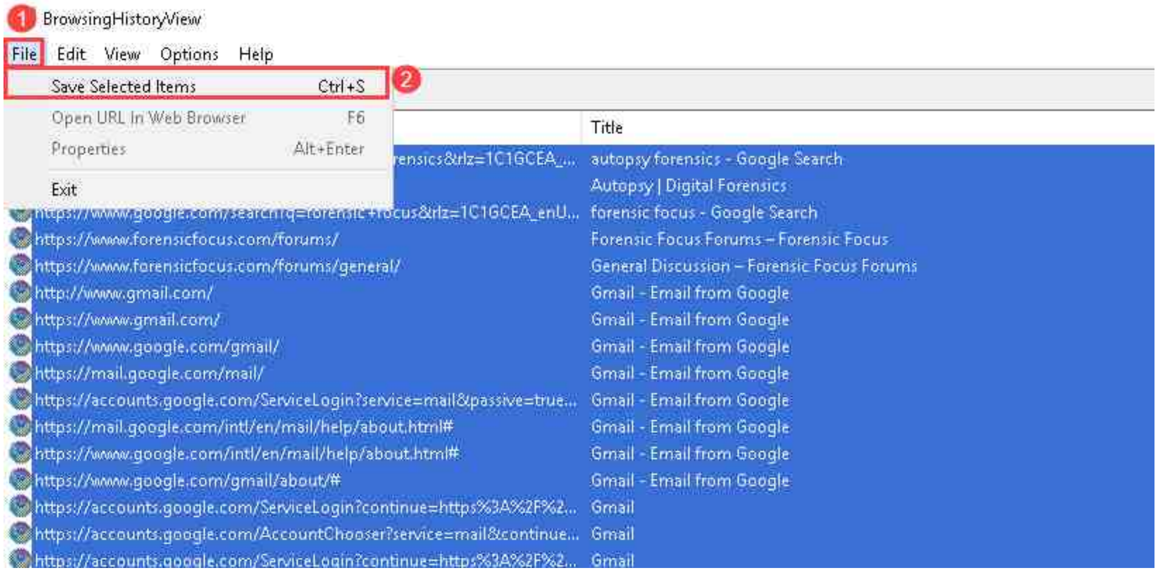


URL	Title	Visit Time	Visit Cou
ht ... -forensics&rlz=1C1GCEA_...	autopsy forensics - Google Search	11/2/2020 12:28:46 AM	1
h	Autopsy | Digital Forensics	11/2/2020 12:28:47 AM	1
ht ... -focus&rlz=1C1GCEA_enU...	forensic focus - Google Search	11/2/2020 12:28:53 AM	1
https://www.forensicfocus.com/forums/	Forensic Focus Forums – Forensic Focus	11/2/2020 12:28:57 AM	1
https://www.forensicfocus.com/forums/general/	General Discussion – Forensic Focus Forums	11/2/2020 12:29:00 AM	1
http://www.gmail.com/	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://www.gmail.com/	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://www.google.com/gmail/	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://mail.google.com/mail/	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://accounts.google.com/ServiceLogin?service=mail&passive=true...	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://mail.google.com/intl/en/mail/help/about.html#	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://www.google.com/intl/en/mail/help/about.html#	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://www.google.com/gmail/about/#	Gmail - Email from Google	11/2/2020 12:29:20 AM	1
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2...	Gmail	11/2/2020 12:29:23 AM	2
https://accounts.google.com/AccountChooser?service=mail&continue...	Gmail	11/2/2020 12:29:23 AM	1
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2...	Gmail	11/2/2020 12:29:23 AM	2
https://accounts.google.com/signin/v2/identifier?continue=https%3A...	Gmail	11/2/2020 12:29:24 AM	1
https://accounts.google.com/signin/v2/challenge/pwd?continue=http...	Gmail	11/2/2020 12:29:27 AM	1
https://www.google.com/search?q=youtube&rlz=1C1GCEA_enUS903U...	youtube - Google Search	11/2/2020 12:29:55 AM	1
https://www.google.com/search?q=how%20to%20download%20movi...	how to download movies for free site:youtube.com - Google Search	11/2/2020 12:30:08 AM	2
https://www.google.com/search?q=how%20to%20download%20movi...	how to download movies for free site:youtube.com - Google Search	11/2/2020 12:30:09 AM	2
https://www.youtube.com/watch?v=vBs6tAJE_Po	How To Download Movies for Free on Android Phone - YouTube	11/2/2020 12:30:11 AM	2
https://www.youtube.com/watch/vBs6tAJE_Po	How To Download Movies for Free on Android Phone - YouTube	11/2/2020 12:30:11 AM	1
https://www.youtube.com/watch?v=vBs6tAJE_Po	How To Download Movies for Free on Android Phone - YouTube	11/2/2020 12:30:13 AM	2

24 item(s)

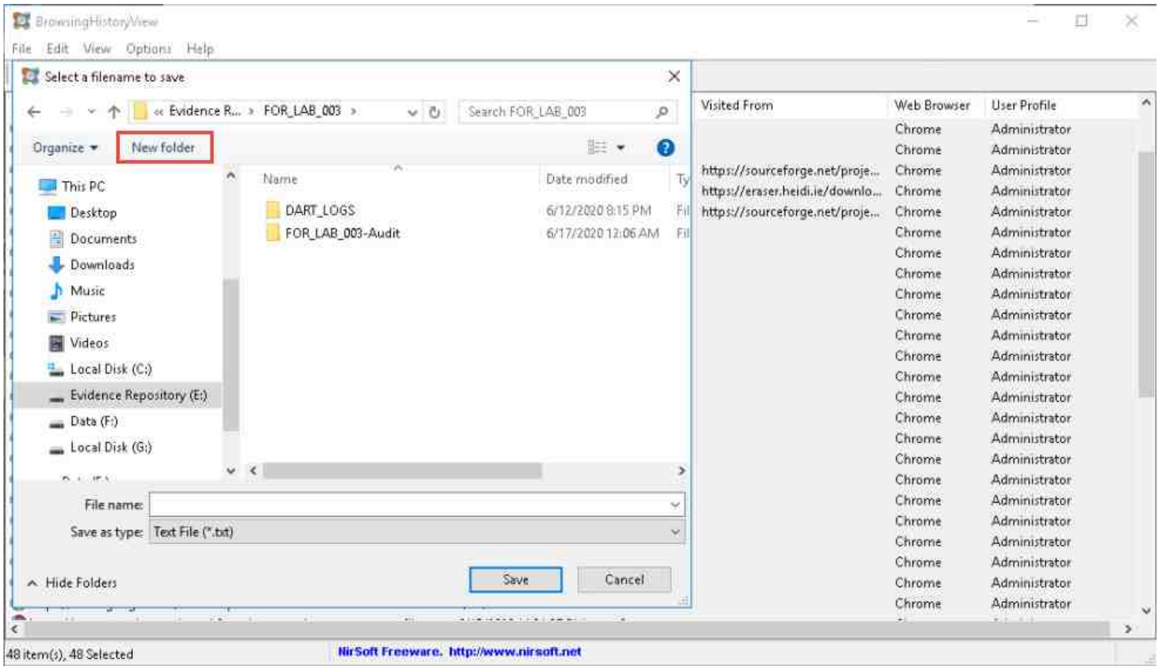
NirSoft Freeware. http://www.nirsoft.net

6. Next, click File in the File Menu and click Save Selected Items as highlighted in items 1 and 2 below.


1
BrowsingHistoryView
File Edit View Options Help
Save Selected Items Ctrl+S
2
Open URL In Web Browser F6
Properties Alt+Enter
Exit

	Title
...rensics&rlz=1C1GCEA_...	autopsy forensics - Google Search
	Autopsy | Digital Forensics
https://www.google.com/search?q=forensic+focus&rlz=1C1GCEA_enU...	forensic focus - Google Search
https://www.forensicfocus.com/forums/	Forensic Focus Forums – Forensic Focus
https://www.forensicfocus.com/forums/general/	General Discussion – Forensic Focus Forums
http://www.gmail.com/	Gmail - Email from Google
https://www.gmail.com/	Gmail - Email from Google
https://www.google.com/gmail/	Gmail - Email from Google
https://mail.google.com/mail/	Gmail - Email from Google
https://accounts.google.com/ServiceLogin?service=mail&passive=true...	Gmail - Email from Google
https://mail.google.com/intl/en/mail/help/about.html#	Gmail - Email from Google
https://www.google.com/intl/en/mail/help/about.html#	Gmail - Email from Google
https://www.google.com/gmail/about/#	Gmail - Email from Google
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2...	Gmail
https://accounts.google.com/AccountChooser?service=mail&continue...	Gmail
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2...	Gmail

7. The Select a filename to save window will appear, allowing you to browse to the intended destination. Let us browse to the folder you created earlier called FOR_LAB_003. To do this, navigate to Evidence Repository (E:) > FOR_LAB_003. Click the New Folder icon as highlighted below.



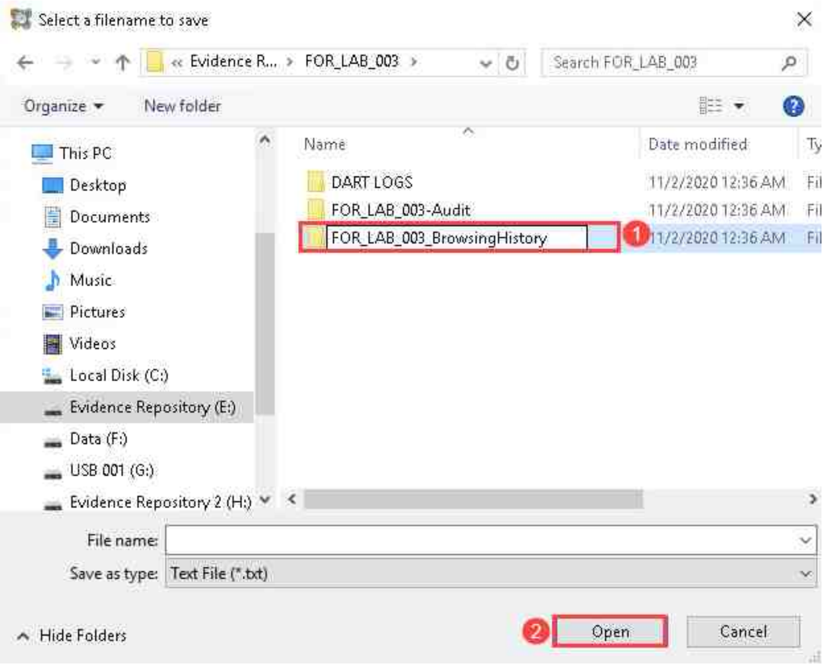
Name	Date modified
DART_LOGS	6/12/2020 8:15 PM
FOR_LAB_003-Audit	6/17/2020 12:06 AM

Visited From	Web Browser	User Profile
	Chrome	Administrator
	Chrome	Administrator
https://sourceforge.net/proje...	Chrome	Administrator
https://eraser.heidi.ie/downlo...	Chrome	Administrator
https://sourceforge.net/proje...	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator
	Chrome	Administrator

48 item(s), 48 Selected NirSoft Freeware. http://www.nirsoft.net

As we regularly mention, always ensure that the captured data is stored to the external drive and not on the one you are examining.

8. Name the new folder `FOR_LAB_003_BrowsingHistory` and click Open as seen in items 1 and 2 below.



Select a filename to save

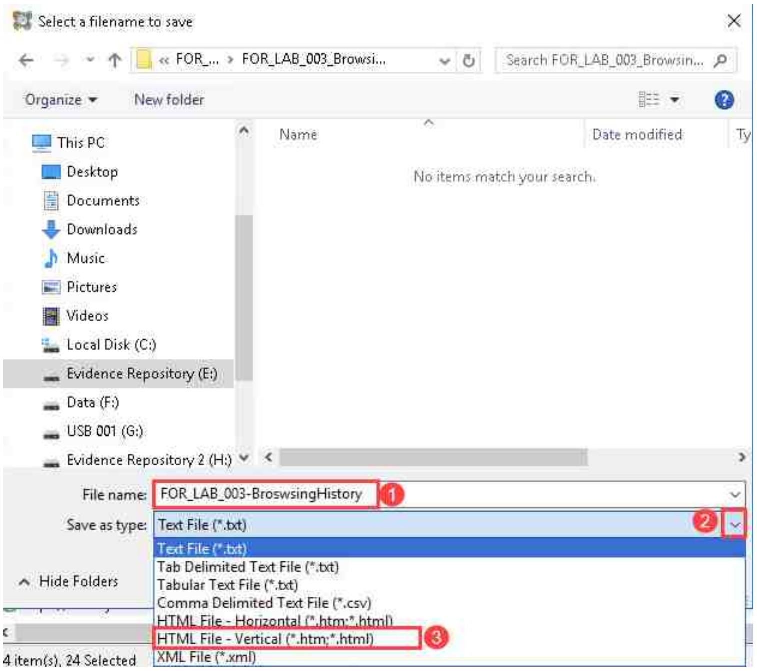
« Evidence R... › FOR_LAB_003 ›

Name	Date modified	Ty
DART LOGS	11/2/2020 12:36 AM	Fil
FOR_LAB_003-Audit	11/2/2020 12:36 AM	Fil
FOR_LAB_003_BrowsingHistory	11/2/2020 12:36 AM	Fil

File name:

Save as type: Text File (*.txt)

9. Now let us give the file the name `FOR_LAB_003-BrowsingHistory` as highlighted in item 1 below. Let us choose the file format of the browsing history report we want to capture. To do this, click the dropdown menu in the Save as type field and click HTML File - Vertical (*.htm;*.html) to save the export as an HTML file as highlighted in items 2 and 3 below.



Select a filename to save

« FOR_... › FOR_LAB_003_Browsi...

No items match your search.

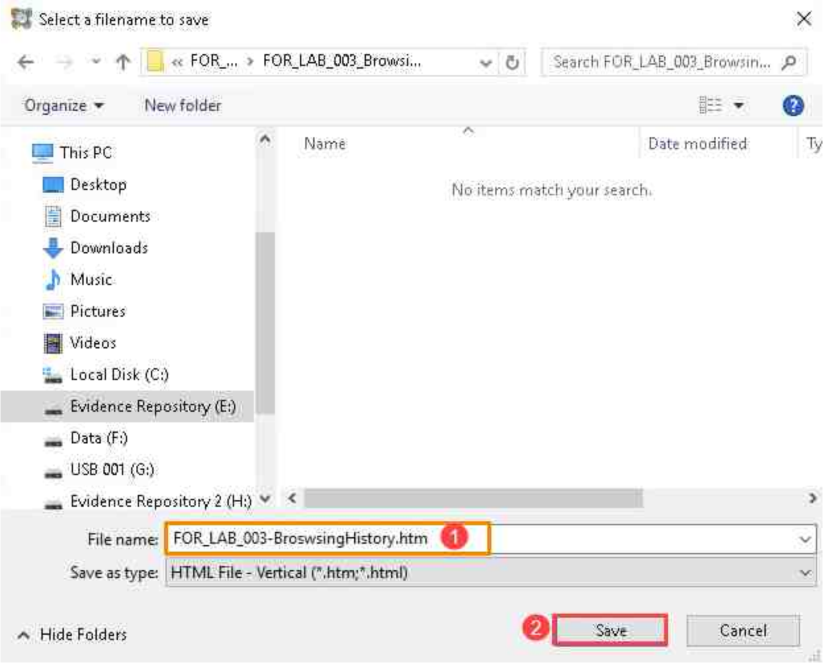
File name: FOR_LAB_003-BroswsingHistory

Save as type: Text File (*.txt)

- Text File (*.txt)
- Tab Delimited Text File (*.txt)
- Tabular Text File (*.txt)
- Comma Delimited Text File (*.csv)
- HTML File - Horizontal (*.htm;*.html)
- HTML File - Vertical (*.htm;*.html)
- XML File (*.xml)

4 item(s), 24 Selected

10. Once you have all the right options selected and you have verified that the file is being saved to the correct path, click Save as highlighted in item 2 below to export the history. Your HTML file will now be saved in the selected path awaiting your review.



Select a filename to save

« FOR_... › FOR_LAB_003_Browsi...

Search FOR_LAB_003_Browsin...

No items match your search.

File name: FOR_LAB_003-BroswsingHistory.htm

Save as type: HTML File - Vertical (*.htm;*.html)

To view the report, browse to the folder that you saved it in and double-click the file you created called FOR_LAB_003_BrowsingHistory.htm.

11. BrowsingHistoryView is the last program we will look at in this lab but feel free to review other programs in DART. There are password revealers, IM parsers, networks scanners, and much more. Once you are done, please close the open programs by clicking the X at the top-right corner of the windows.