SUPPORT MANUAL
ON
CYBER CHECK SUITE

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY
TRAINING TO TECHNICAL TEACHERS
DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION
SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta
Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Mr. Vipul Mandhar (Project Assistant)

Table of Contents

Introduction to Cyber Check Suite 4

The main features of Cyber Check are 5

Task 1: What is the procedure for creating a new user?....... 10

(Default password of Admin user = cyber) 10

Task 2: How do you load a particular evidence file for analysis?... 10

Task 3: What are the default contents in the CyberCheck report? How do you see the number of partitions available in an evidence file? Note down the type of partitions available and total sectors occupied by each partition......................... 12

Task 4: How do you verify the hash value of an evidence file?... 14

Task 5: How do you start a search process for a particular key word?... 14

Task 6: How can you view the search hits of a search process?... 20

Task 7: What are all the items that can be book marked for later use? 21

Task 8: How do you add a book-marked item into the report? 24

Task 9: How can you view the entire pictures available in an evidence file? 24

Task 10: How can you see a signature-mismatched file? 27

Task 11: How can you search for files, which are created within a particular time frame?.. 27

Task 12: How do you perform a search for a particular key word in unallocated cluster area? 29

Task 13: How can you exclude system files from the keyword search? 34

Task 14: How can you search for files based on file extension? 35

Task 15: How can you find out the hash value of a file from CyberCheck? 38

Task 16: How can you search for files with same hash value? 40

Task 17: How can you view all the deleted files in an evidence file? 41

Task 18: How can you recover a deleted file? 41

Task 19: How can you recover a deleted folder? 43

Task 20: What is the information available in Block view? 45

Task 21: How do you view the sectors allocated to a particular file? 47

Task 22: How do you view the clusters allocated to a particular file? 48

Task 23: How do you view the cluster chain of a particular file? 49

Task 24: Add a picture file into the report and observe what happened in the report? 49

Task 25: How do you start partition recovery? 51

Task 26: How do you start format recovery? 53

Task 27: How can you preview a storage media locally? 55

Task 28: How do you initiate carving process from unallocated clusters, Disk Slack? 57

Task 29: Where can you see the carved files from unallocated clusters, Disk Slack? 57

Task 30: How do you export a carved file? 58

Task 31: How do you append a carved file to report? 58

Task 32: How do you see the carved files in gallery view? . 59

Introduction to Cyber Check Suite

Cyber Check is a forensic analysis tool developed by C-DAC, Thiruvananthapuram, for analysing the Evidence file acquired by the Imaging tool True Back (Forensic Imaging tool developed by C-DAC, Thiruvananthapuram). It is also capable of analyzing raw images generated by other Cyber Forensic Tools. MD5 Hash Algorithm is used in Cyber Check for verifying data integrity. When loading the software, it performs a self-integrity check on itself. If the Cyber Check Executable is corrupted, it will display a message notifying that Cyber Check Executable is corrupted, cannot continue with analysis. Further loading of the software will be terminated. It should be noted, the Cyber Check do the self-integrity check while loading the software itself. If the software is corrupted beyond loading it, it may not be possible to load the software at all. In this case, the software may be considered as totally corrupted.

The main features of Cyber Check are

- Standard Windows application on Windows, XP and Vista.
- Self-Integrity check
- Minimum system configuration check.
- Analyses evidence file containing FAT12/16/32, NTFS, CDFS,
- Linux EXT2/3 FS, Unix FS2 (Free BSD), Solaris and Reiser file systems.
- Support for GUID Partitioning (GPT) table.
- Facility for analyzing evidence files having DD and Encase formats.
- Facility for analyzing multiple evidence files.
- User login facilities.
- Creates log of each analysis session and Analyzing officer’s details.
- Block by block data integrity verification while loading evidence file.
- Explorer type view of contents of the whole evidence file.
- Display of folders and files with all attributes.
- Sorting of file attributes up to 5 levels.
- Show/Hide system files.
- Text/Hex view of the content of a file.
- Picture view of an image file.
- Gallery view of images.
- Graphical representation of the following views of an evidence file.

    - Disk View
    - Cluster View
    - Block View
- Timeline View of
    - All files
    - Deleted files
    - Time anomaly files
    - Signature Mismatched files
    - Files created within a time frame
- Single and Multiple Keyword search.
- Search with GREP expressions.
- Search with Unicode characters.
- Extraction of Disk, Partition, File and MBR Slacks.
- Exclusive search in slack space.
- Data recovery from deleted files and slack space.
- Exporting files, folders and slack content.
- Exporting folder structure including file names into a file.
- Exporting files on to an external viewer.
- Extraction of unused unallocated clusters and exclusion from search space.
- Extraction of lost clusters.
- Exclusive search in data extracted from lost clusters.

- In-place or zero storage file carving facility from lost clusters, unallocated clusters, disk slack and within a file.
- Exporting Swap files.
- Exclusive search in data extracted from Swap files.
- File search based on hash value.
- File search based on extension.
- Exclusion of system files from search space.
- Multiple sorting based on file attributes.
- Local and Network preview of storage media
- Partitions previewing facility.
- Book marking facility for data, files and folders
- Mailbox viewer
- Registry viewer
- Expansion trigger at different levels of folder structure
- Recovery of deleted partitions
- Recovery of formatted media
- Facility for analyzing raw images
- Identification of Password protected files MS office files
- Identification of overwritten files
- Unicode support
- Indian Language support
- Virtual Keyboard for entering Unicode characters.

- Support for dynamic disk analysis
- Customized hash set library creation
- Support for scripting
- Predefined filters for analysis.
- Facility for user defined filters.
- Customization of File Signature Library
- Facility for extracting deleted mails from .dbx files.
- Identification of steganographed files.
- Facility for viewing nested ZIP file listing.
- Extract Recycle Bin files
- Internet History Viewer
- Facility to view metadata of Microsoft office files
- Data Carving from Unallocated & Lost clusters, Disk Slack
- Index based searching
- Anti-forensics detection
- Generation of analysis report with the following features.
    - Complete information of the evidence file system.
    - Complete information of partition and drive geometry.
    - Hash verification details.
    - User login and logout information.
    - Exported content of text file and slack information.
    - Includes picture file as image.

    - Customization of report
    - Save report.
    - Print report.
- Support to load MobileCheck 2.0 images
- Mount image to drive
- Windows 7Hibernate File Analysis
- Browser Forensics
    - Internet Explorer
    - Google Chrome
    - Mozilla FireFox
- Windows 8 Forensics
- GPS information extraction from JPEG images
- Memory Analysis
- Expand the content of TAR files
- Identifying Document languages
- Log and Event File Analysis
- Integrated virtual environment Vmdk and Vhd file analysis
- "In built viewing facility for Video files like MP4, 3gp, Fly, WMV, Divx, Avi"
- Prefetch Analysis for WindowsXP/7/8
- Removal of Evidence
- Integration of F-RAN
- Integration of F-Tex
- Known File Filters updation
- Enhancements on volume shadow copy Analysis
- Gallery Selection with SHIFT Key

Data Recovery and Analysis Tool

(Note: The exercise may be carried out on the evidence file)

Task 1: What is the procedure for creating a new user?

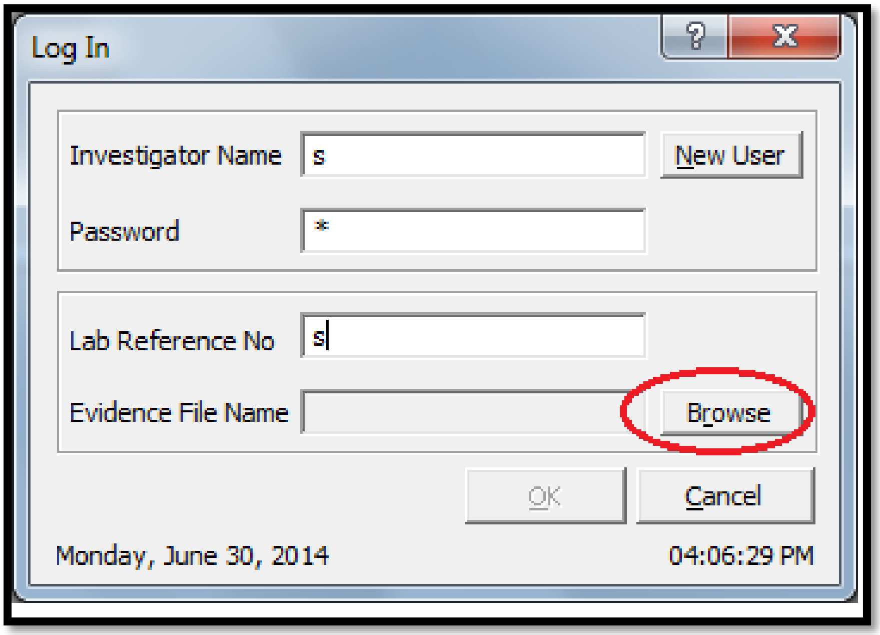
Solution: Run CyberCheck6.0 > File > New >> User Setting Window Click "Add User"

(Default password of Admin user = cyber)

Task 2: How do you load a particular evidence file for analysis?

Solution: Select **File□New** or click on **New**🗋 tool bar button

Click the **Browse** button for specifying the Evidence File Name.



Log In

Investigator Name: s

Password: *

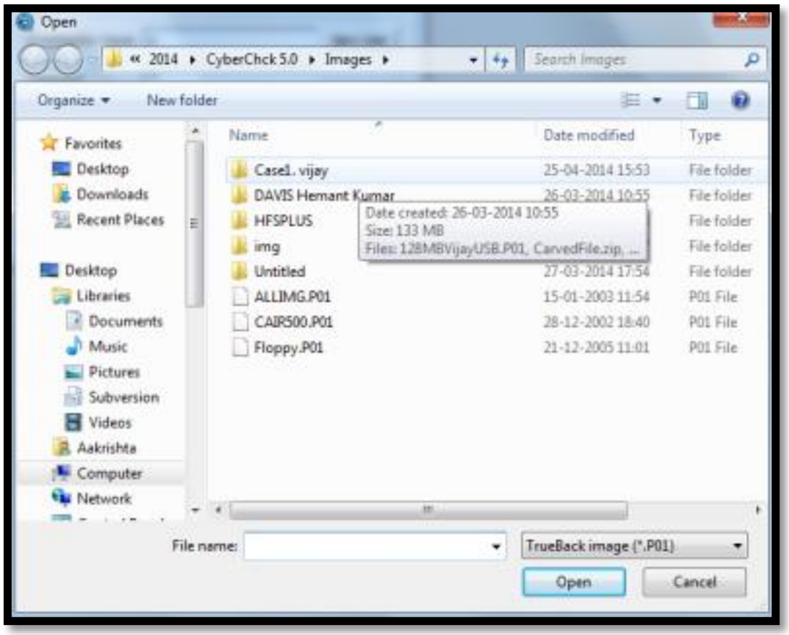
Lab Reference No: s

Evidence File Name:

Monday, June 30, 2014

04:06:29 PM

- A File Open dialog box will be displayed for browsing and selecting the desired image file.

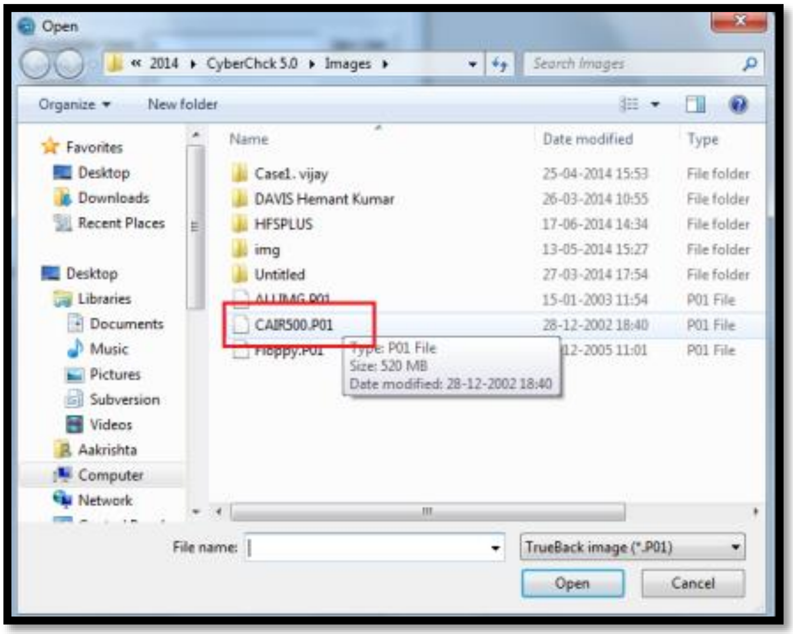


Name	Date modified	Type
Case1. vijay	25-04-2014 15:53	File folder
DAVIS Hemant Kumar	26-03-2014 10:55	File folder
HFSPLUS		File folder
img		File folder
Untitled	27-03-2014 17:54	File folder
ALLIMG.P01	15-01-2003 11:54	P01 File
CAIR500.P01	28-12-2002 18:40	P01 File
Floppy.P01	21-12-2005 11:01	P01 File

Date created: 26-03-2014 10:55
Size: 133 MB
Files: 128MBVijayUSB.P01, CarvedFile.zip, ...

File name:
TrueBack image (*.P01)

- Select the image **(Evidence File .000 or .P01)** and press the **Open** button



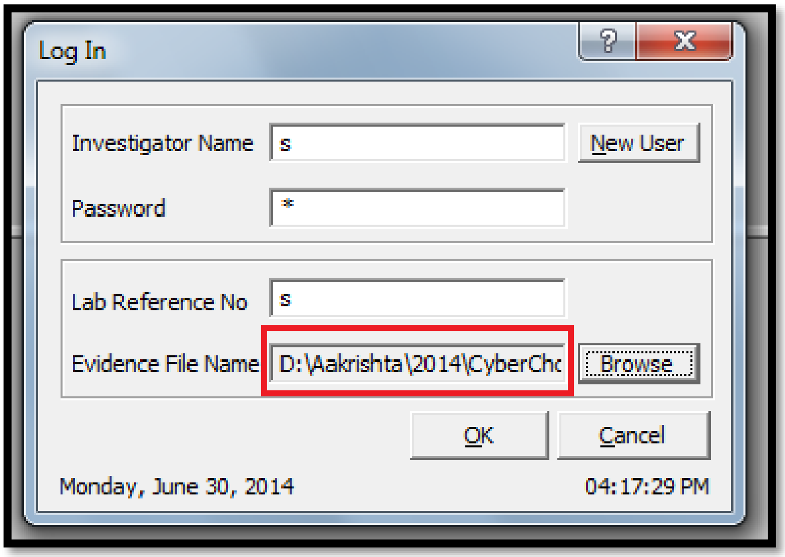
Name	Date modified	Type
Case1. vijay	25-04-2014 15:53	File folder
DAVIS Hemant Kumar	26-03-2014 10:55	File folder
HFSPLUS	17-06-2014 14:34	File folder
img	13-05-2014 15:27	File folder
Untitled	27-03-2014 17:54	File folder
ALLIMG.P01	15-01-2003 11:54	P01 File
CAIR500.P01	28-12-2002 18:40	P01 File
Floppy.P01	12-2005 11:01	P01 File

Type: P01 File
Size: 520 MB
Date modified: 28-12-2002 18:40

File name:
TrueBack image (*.P01)

- Then the Evidence file path is loaded in the Log in window. Click **OK** button

.



Log In

Investigator Name: s

Password: *

Lab Reference No: s

Evidence File Name: D:\Aakrishta\2014\CyberChc

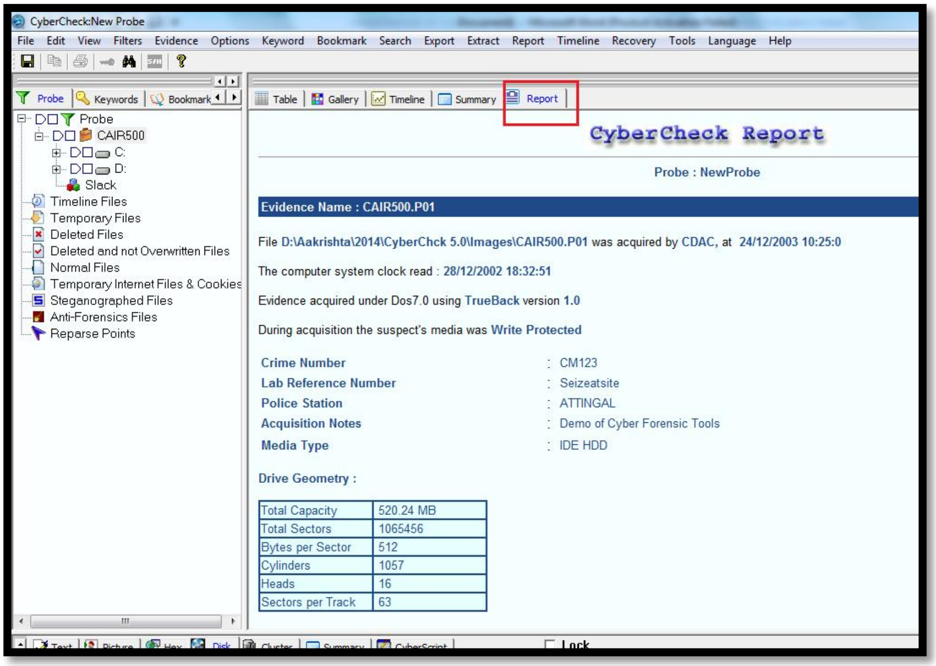
Monday, June 30, 2014

04:17:29 PM

Task 3: What are the default contents in the CyberCheck report? How do you see the number of partitions available in an evidence file? Note down the type of partitions available and total sectors occupied by each partition.

Solution: Default contents in the CyberCheck report are

- Complete information of the Evidence file system
- Complete information of the partitions and drive geometry
- Hash Verification details
- User login and logout information



CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Table Gallery Timeline Summary Report
Probe
CAIR500
C:
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Text Picture Hex Disk Cluster Summary CyberScript
Lock

CyberCheck Report

Probe : NewProbe

Evidence Name : CAIR500.P01

File D:\Aakrishta\2014\CyberChck 5.0\Images\CAIR500.P01 was acquired by CDAC, at 24/12/2003 10:25:0

The computer system clock read : 28/12/2002 18:32:51

Evidence acquired under Dos7.0 using TrueBack version 1.0

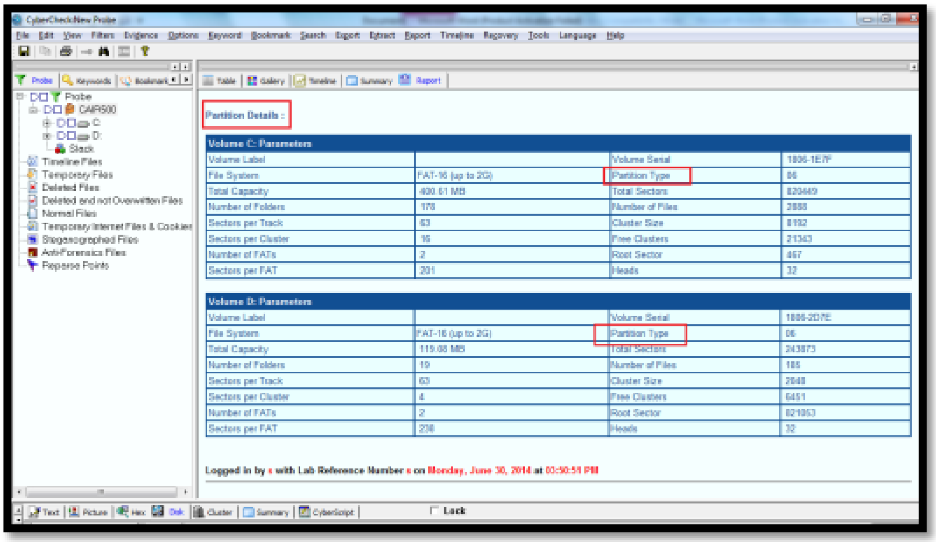
During acquisition the suspect's media was Write Protected

Crime Number	:	CM123
Lab Reference Number	:	Seizeatsite
Police Station	:	ATTINGAL
Acquisition Notes	:	Demo of Cyber Forensic Tools
Media Type	:	IDE HDD

Drive Geometry :

Total Capacity	520.24 MB
Total Sectors	1065456
Bytes per Sector	512
Cylinders	1057
Heads	16
Sectors per Track	63

Partition details available in the evidence file can be viewed from the **Report** tab.



CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Table Gallery Timeline Summary Report
Probe
CAIR500
C:
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Text Picture Hex Disk Cluster Summary CyberScript
Lock

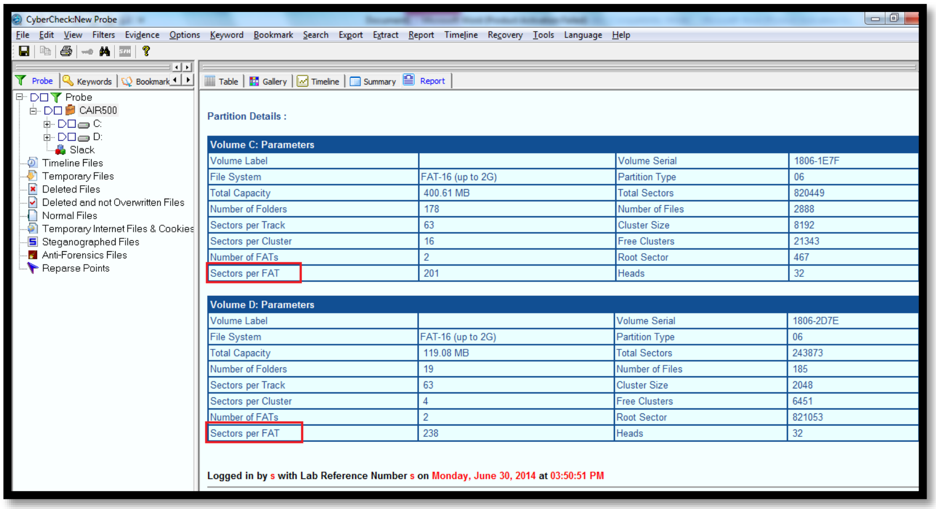
Partition Details :

Volume C: Parameters			
Volume Label		Volume Serial	1806-1E7F
File System	FAT-16 (up to 2G)	Partition Type	06
Total Capacity	400.61 MB	Total Sectors	820449
Number of Folders	178	Number of Files	2888
Sectors per Track	63	Cluster Size	8192
Sectors per Cluster	16	Free Clusters	21343
Number of FATs	2	Root Sector	467
Sectors per FAT	201	Heads	32

Volume D: Parameters			
Volume Label		Volume Serial	1806-207E
File System	FAT-16 (up to 2G)	Partition Type	06
Total Capacity	119.08 MB	Total Sectors	243873
Number of Folders	19	Number of Files	185
Sectors per Track	63	Cluster Size	2048
Sectors per Cluster	4	Free Clusters	6451
Number of FATs	2	Root Sector	821063
Sectors per FAT	238	Heads	32

Logged in by s with Lab Reference Number s on Monday, June 30, 2014 at 03:50:51 PM

Total sectors occupied by each partition can be viewed from the Partition Details Table in the **Report** tab.



Partition Details :

Volume C: Parameters			
Volume Label		Volume Serial	1806-1E7F
File System	FAT-16 (up to 2G)	Partition Type	06
Total Capacity	400.61 MB	Total Sectors	820449
Number of Folders	178	Number of Files	2888
Sectors per Track	63	Cluster Size	8192
Sectors per Cluster	16	Free Clusters	21343
Number of FATs	2	Root Sector	467
Sectors per FAT	201	Heads	32

Volume D: Parameters			
Volume Label		Volume Serial	1806-2D7E
File System	FAT-16 (up to 2G)	Partition Type	06
Total Capacity	119.08 MB	Total Sectors	243873
Number of Folders	19	Number of Files	185
Sectors per Track	63	Cluster Size	2048
Sectors per Cluster	4	Free Clusters	6451
Number of FATs	2	Root Sector	821053
Sectors per FAT	238	Heads	32

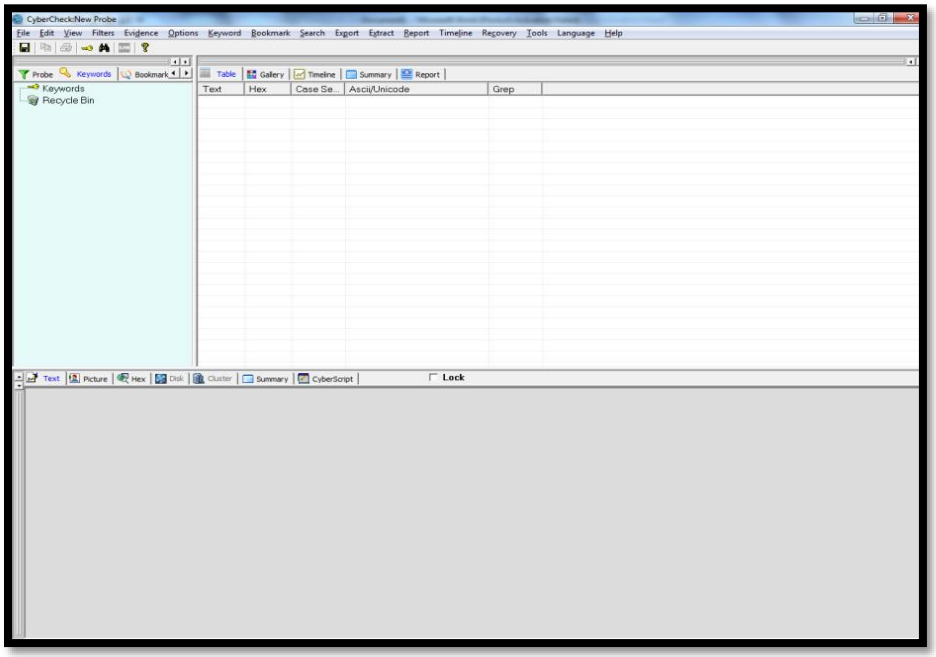
Logged in by s with Lab Reference Number s on Monday, June 30, 2014 at 03:50:51 PM

Task 4: How do you verify the hash value of an evidence file?

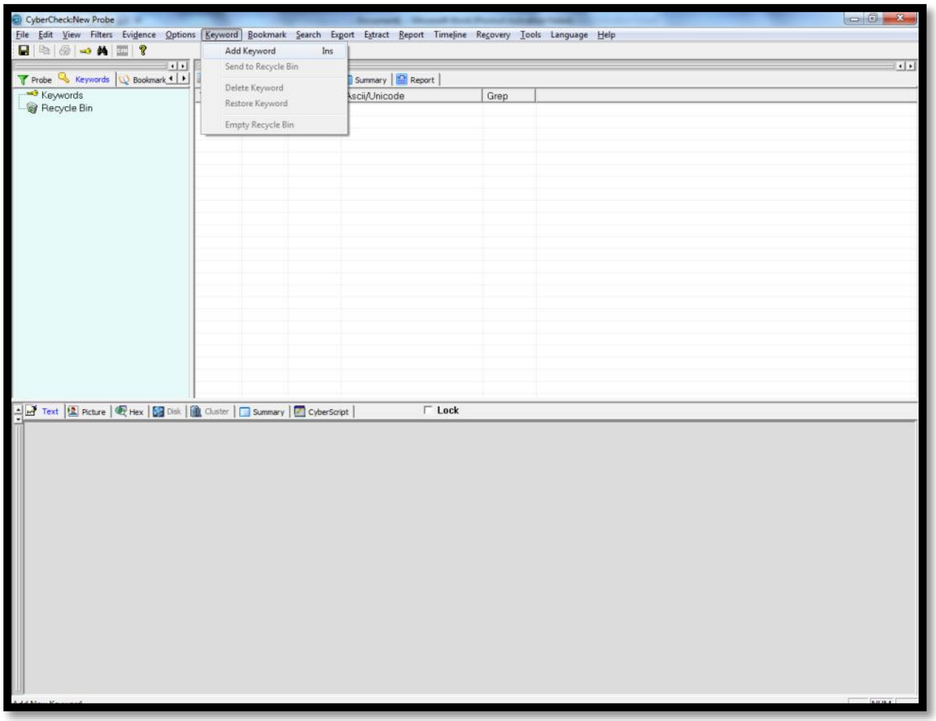
Solution: Select Options>Hash Evidence menu item from the main user interface of CyberCheck

Task 5: How do you start a search process for a particular key word?

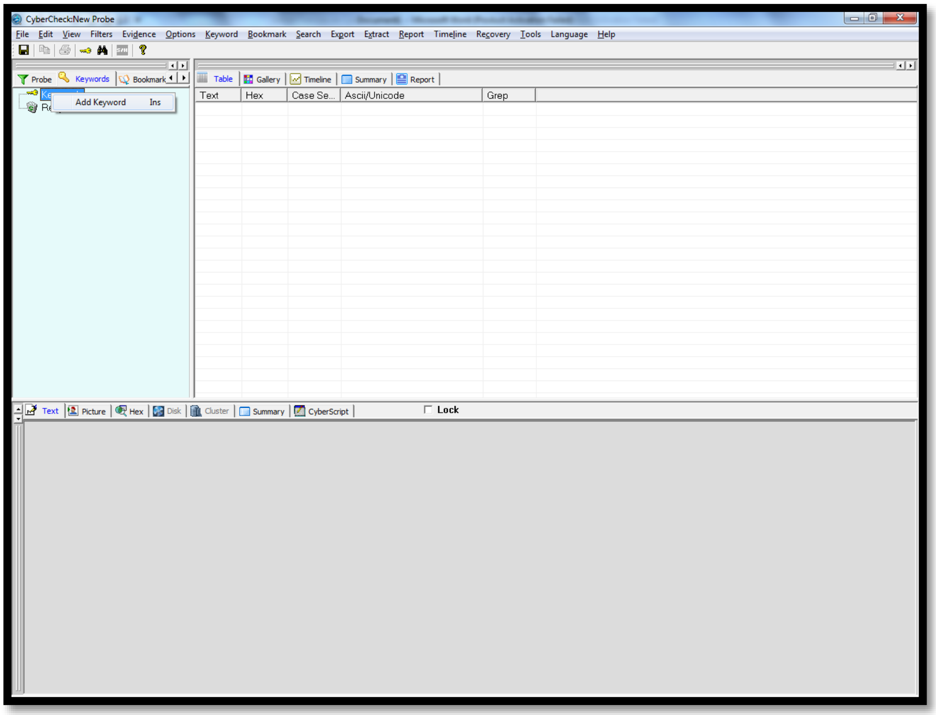
Solution: Select Keyword tab from left pane



- Click **Add Keyword** option from the Keyword menu. This sub-menu item will become enabled, only when in the Keywords tab in the left pane.

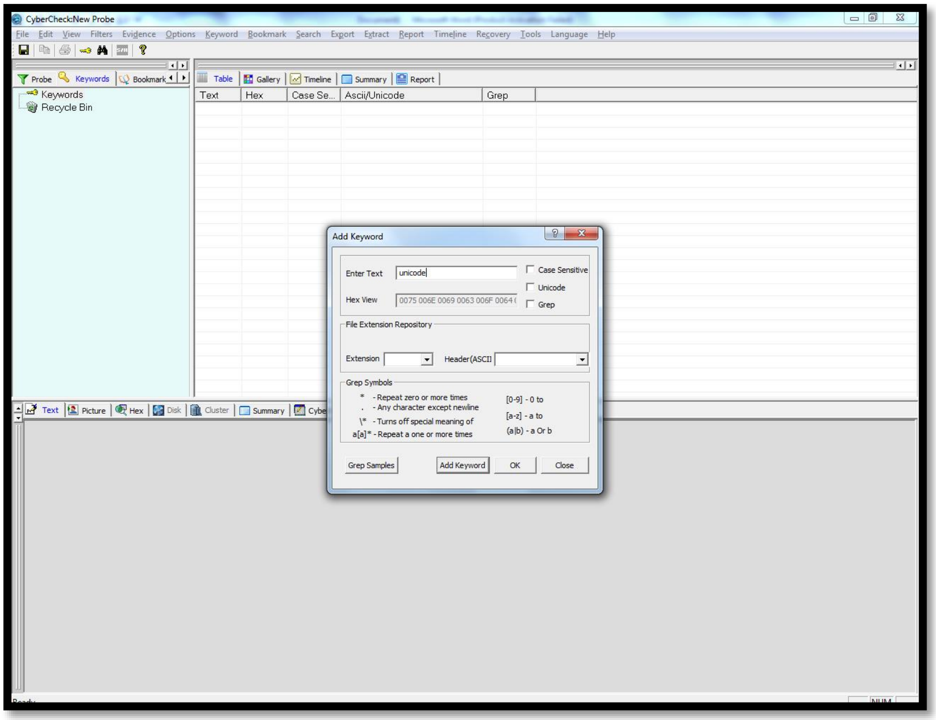


Or Right click **Keywords** and select **Add Keyword.**


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Add Keyword Ins
Table Gallery Timeline Summary Report
Text Hex Case Se... Ascii/Unicode Grep
Text Picture Hex Disk Cluster Summary CyberScript
□ Lock

The fourth item (item with **key** symbol) in the toolbar also has the same functionality.

On clicking Add Keyword option a new dialog box appears. Add the specified keyword in Enter Text box. Hex View shows the hex value of the entered text. Keyword to be searched can be made Case sensitive, Unicode or Grep type.


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Hex Case Se... Ascii/Unicode Grep
Text Picture Hex Disk Cluster Summary Cybe
Add Keyword
Grep Samples
Add Keyword
OK
Close

Enter Text: unicode

Hex View: 0075 006E 0069 0063 006F 0064 (

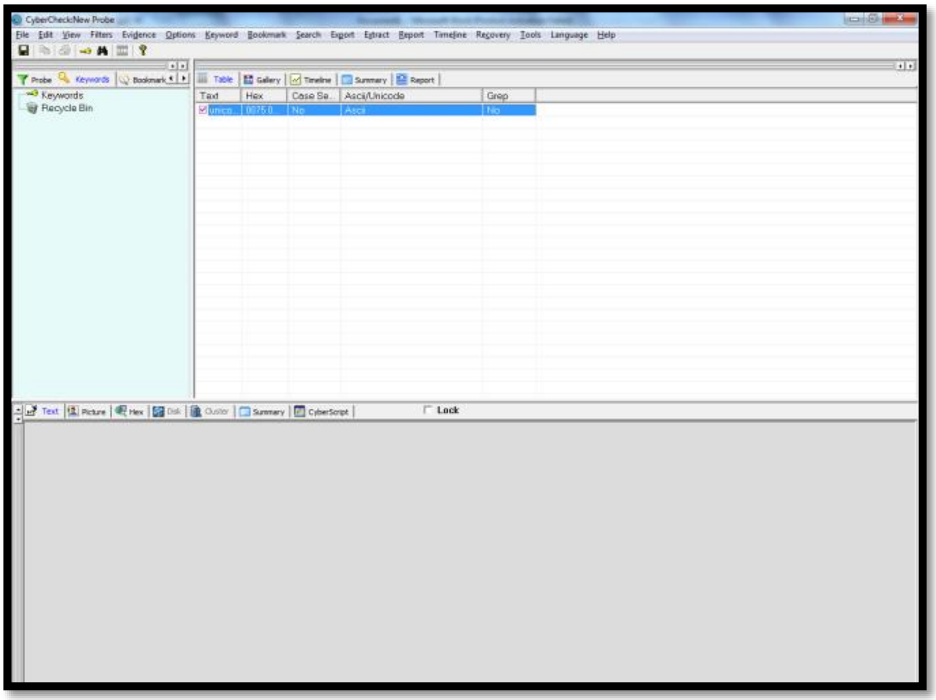
□ Case Sensitive
□ Unicode
□ Grep

File Extension Repository

Extension: ▾ Header(ASCII ▾

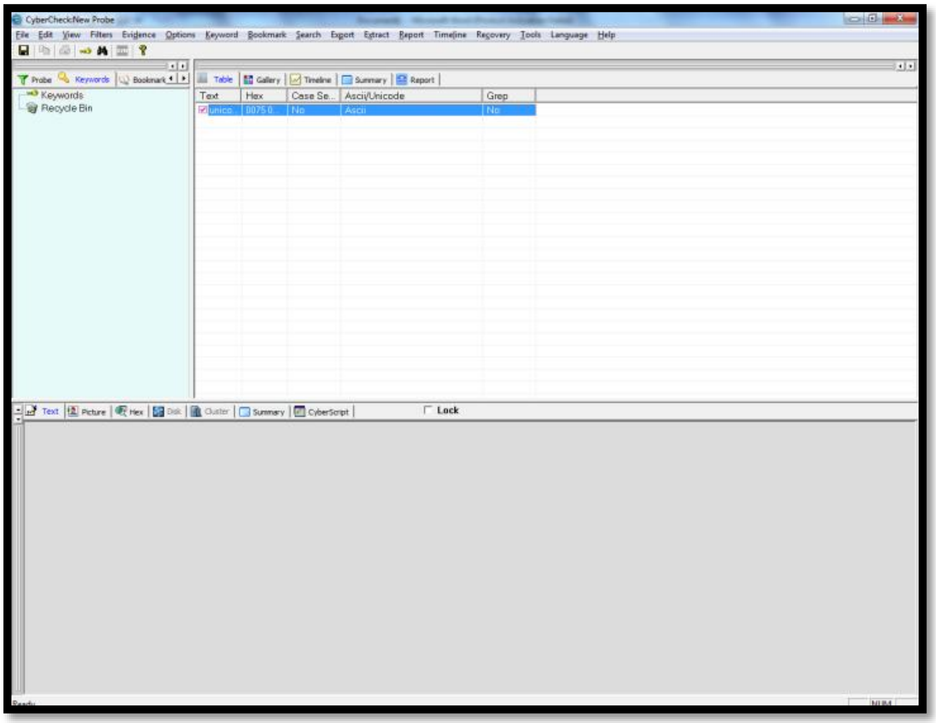
Grep Symbols

* - Repeat zero or more times
. - Any character except newline
* - Turns off special meaning of
a[a]* - Repeat a one or more times
[0-9] - 0 to
[a-z] - a to
(a|b) - a Or b


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock

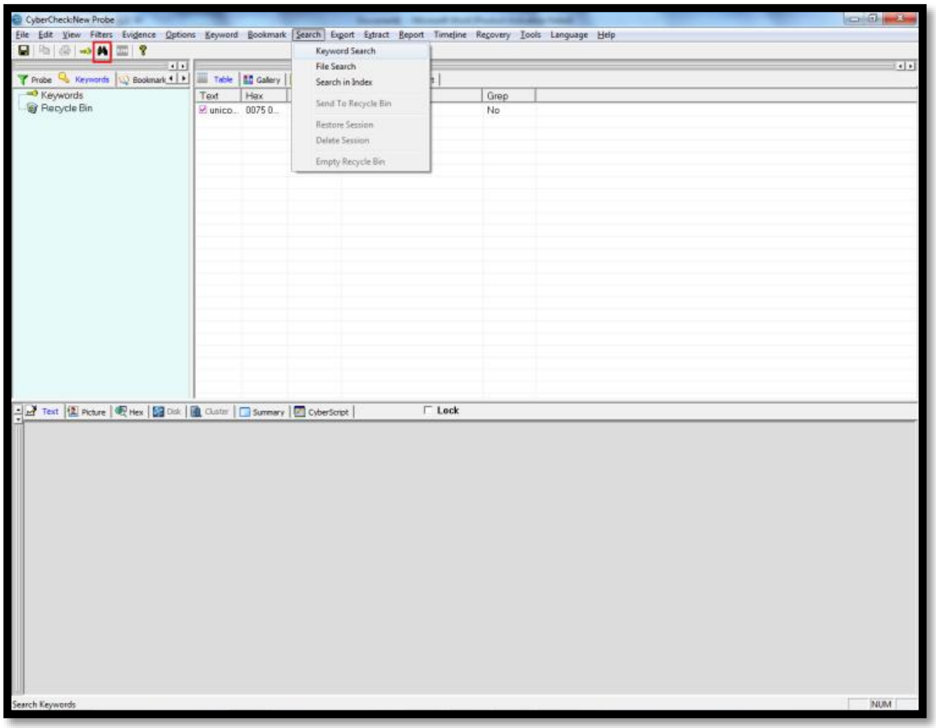
Text	Hex	Case Se...	Ascii/Unicode	Grep
☑ unico...	0075 0...	No	Ascii	No

After entering the keyword, click **OK** button, the entered keyword will then be added to a list of keywords to form a Table of keywords. To search for multiple keywords, press **Add Keyword** button. To search for a particular keyword added, check the appropriate check boxes in the table.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock
Ready
NUM

Text	Hex	Case Se...	Ascii/Unicode	Grep
☑ unico...	0075 0...	No	Ascii	No

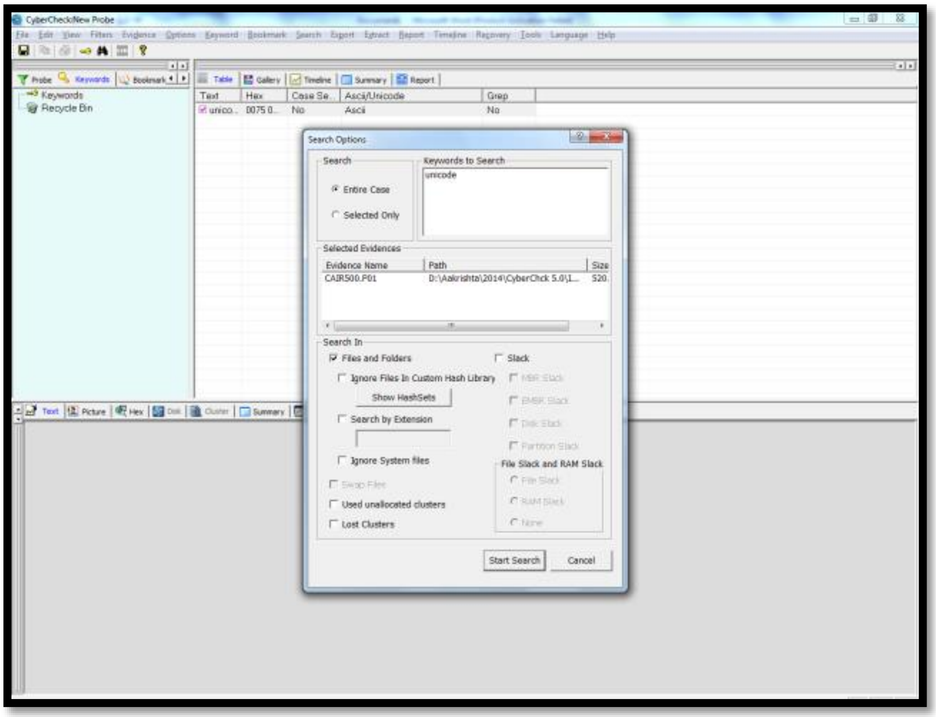
Go to **Search** option, and select **Keyword Search** or click the **Binocular** icon in tool bar



Text	Hex	Grep
☑ unico...	0075 0...	No

Select the keyword(s) to be searched from the table of keywords. Click on **Entire Case** to search through the entire folders and files of the evidence file. To search in a particular file, click on the **Selected Only** radio button. (Select the desired files and folders before selecting *Search□Keyword Search* menu item).There are other options like Files and

Folders, Used unallocated clusters, lost clusters and Slack for limiting the search space. Press **Start Search**.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary
Search Options
Start Search
Cancel
Show HashSets

Text	Hex	Case Se..	Ascii/Unicode	Grep
☑ unico...	0075 0...	No	Ascii	No

Search Options

Search: ● Entire Case ○ Selected Only

Keywords to Search: unicode

Selected Evidences

Evidence Name	Path	Size
CAIR500.P01	D:\Aakrishta\2014\CyberChck 5.0\1...	520.

Search In

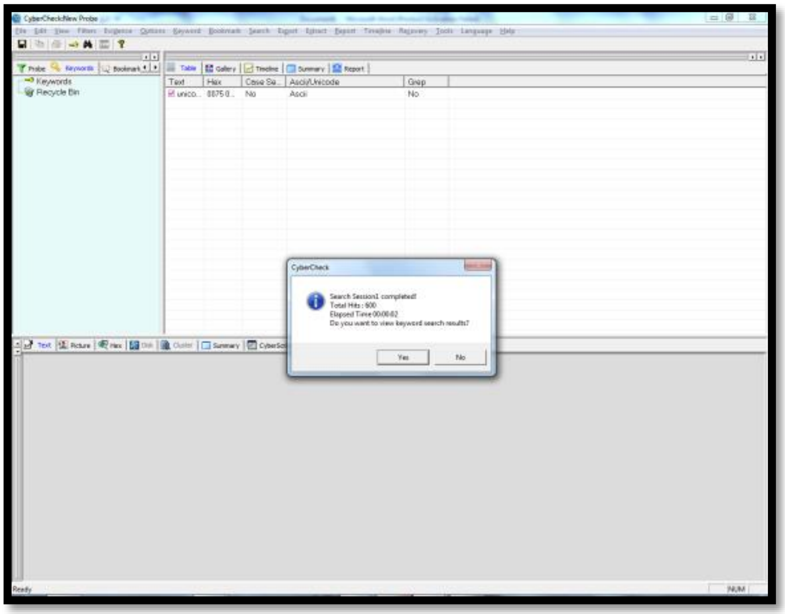
☑ Files and Folders
□ Ignore Files In Custom Hash Library
□ Search by Extension
□ Ignore System files
□ Swap Files
□ Used unallocated clusters
□ Lost Clusters

□ Slack
□ MBR Slack
□ EMBR Slack
□ Disk Slack
□ Partition Slack

File Slack and RAM Slack: ○ File Slack ○ RAM Slack ○ None

A progress bar is shown to show the progress of searching. To know the number of hits, place the mouse pointer on the progress bar for some time. A tool tip will appear indicating the number of hits occurred at that time. On completion of the search process, a message box showing the total hits and elapsed time is displayed.

Click the **‘yes‘button**, to go to the currently added session in the search pane.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScr
Ready
NUM

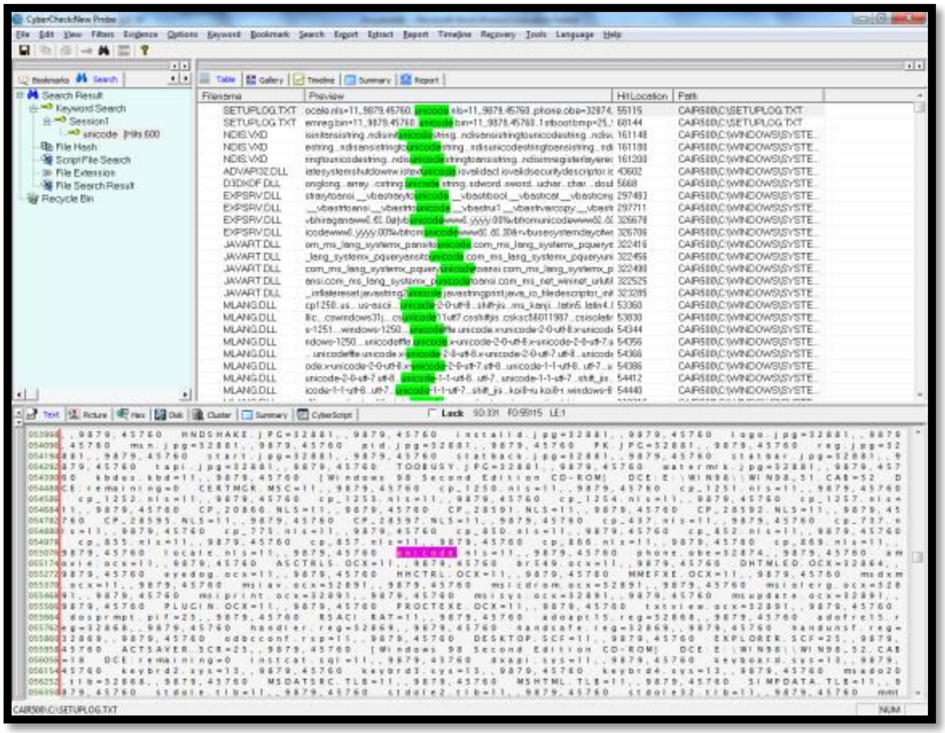
Text	Hex	Case Se...	Ascii/Unicode	Grep
unico...	0075 0...	No	Ascii	No

CyberCheck

Search Session1 completed!
Total Hits : 600
Elapsed Time 00:00:02
Do you want to view keyword search results?

Task 6: How can you view the search hits of a search process?

Solution: Search results displays files that contain the searched keyword. The keywords are highlighted in **green** with selected file’s keyword in the text viewer in the bottom pane. Search tab in the left pane displays the session number and the number of hits for that keyword.



Filename	Preview	HitLocation	Path
SETUPLOG.TXT	ocale.nls=11,.9879.45760. unicode.nls=11,.9879.45760..phone.obe=32874.	55115	CAIR500\C:\SETUPLOG.TXT
SETUPLOG.TXT	emreg.bin=11,.9879.45760. unicode.bin=11,.9879.45760..1stbootbmp=25,:	68144	CAIR500\C:\SETUPLOG.TXT
NDIS.VXD	isinitansistring..ndisinitunicodestring..ndisansistringtounicodestring..ndis	161148	CAIR500\C:\WINDOWS\SYSTE...
NDIS.VXD	estring..ndisansistringtounicodestring..ndisunicodestringtoansistring..ndi	161188	CAIR500\C:\WINDOWS\SYSTE...
NDIS.VXD	ringtounicodestring..ndisunicodestringtoansistring..ndisimregisterlayere	161208	CAIR500\C:\WINDOWS\SYSTE...
ADVAPI32.DLL	idatesystemshutdownw.istextunicode.isvalidacl.isvalidsecuritydescriptor.ic	43602	CAIR500\C:\WINDOWS\SYSTE...
D3DXOF.DLL	onglong...array...cstring.unicode.string..sdword..sword..uchar...char...doul	5668	CAIR500\C:\WINDOWS\SYSTE...
EXPSRV.DLL	strarytoansi.__vbastrarytounicode.__vbastrbool.__vbastrcat.__vbastrcmp	297483	CAIR500\C:\WINDOWS\SYSTE...
EXPSRV.DLL	__vbastrtoansi.__vbastrtounicode.__vbastrui1.__vbastrvarcopy.__vbastr	297711	CAIR500\C:\WINDOWS\SYSTE...
EXPSRV.DLL	vbhiragenawwd.6l.0a\vbunicodewwwd.yyyy.00%vbfromunicodewwwd0.dl	326678	CAIR500\C:\WINDOWS\SYSTE...
EXPSRV.DLL	icodewwwd.yyyy.00%vbfromunicodewwwd0.d0.308rvbusesystemdayofwe	326706	CAIR500\C:\WINDOWS\SYSTE...
JAVART.DLL	om_ms_lang_systemx_pansitounicode.com_ms_lang_systemx_pqueryt	322416	CAIR500\C:\WINDOWS\SYSTE...
JAVART.DLL	_lang_systemx_pqueryansitounicode.com_ms_lang_systemx_pqueryuni	322456	CAIR500\C:\WINDOWS\SYSTE...
JAVART.DLL	com_ms_lang_systemx_pqueryunicodetoansi.com_ms_lang_systemx_p	322498	CAIR500\C:\WINDOWS\SYSTE...
JAVART.DLL	ansi.com_ms_lang_systemx_punicodetoansi.com_ms_net_wininet_urlutil	322525	CAIR500\C:\WINDOWS\SYSTE...
JAVART.DLL	_inflatereset.javastring?unicode.javastringprint.java_io_filedescriptor_init	323285	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	cp1250..us...us-ascii....unicode-2-0-utf-8...shift-jis...ms_kanji...latin5..latin4..l	53360	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	llc....cswindows31j....csunicode11utf7.csshiftjis..csksc56011987...csisolatir	53830	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	s-1251....windows-1250....unicodeffe.unicode.x-unicode-2-0-utf-8.x-unicode	54344	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	ndows-1250....unicodeffe.unicode.x-unicode-2-0-utf-8.x-unicode-2-0-utf-7.a	54356	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	...unicodeffe.unicode.x-unicode-2-0-utf-8.x-unicode-2-0-utf-7.utf-8...unicode	54368	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	ode.x-unicode-2-0-utf-8.x-unicode-2-0-utf-7.utf-8...unicode-1-1-utf-8...utf-7...u	54386	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	unicode-2-0-utf-7.utf-8...unicode-1-1-utf-8...utf-7...unicode-1-1-utf-7...shift_jis	54412	CAIR500\C:\WINDOWS\SYSTE...
MLANG.DLL	icode-1-1-utf-8...utf-7...unicode-1-1-utf-7...shift_jis...koi8-u.koi8-r.windows-8	54440	CAIR500\C:\WINDOWS\SYSTE...

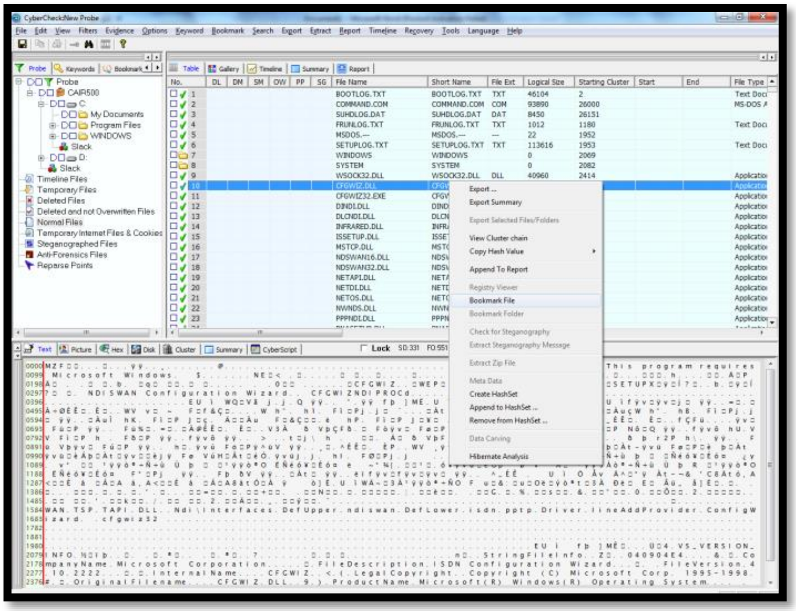
CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Bookmarks Search
Search Result
Keyword Search
Session1
unicode [Hits 600
File Hash
Script File Search
File Extension
File Search Result
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock SO:331 FO:55115 LE:1
CAIR500\C:\SETUPLOG.TXT
NUM

Task 7: What are all the items that can be book marked for later use?

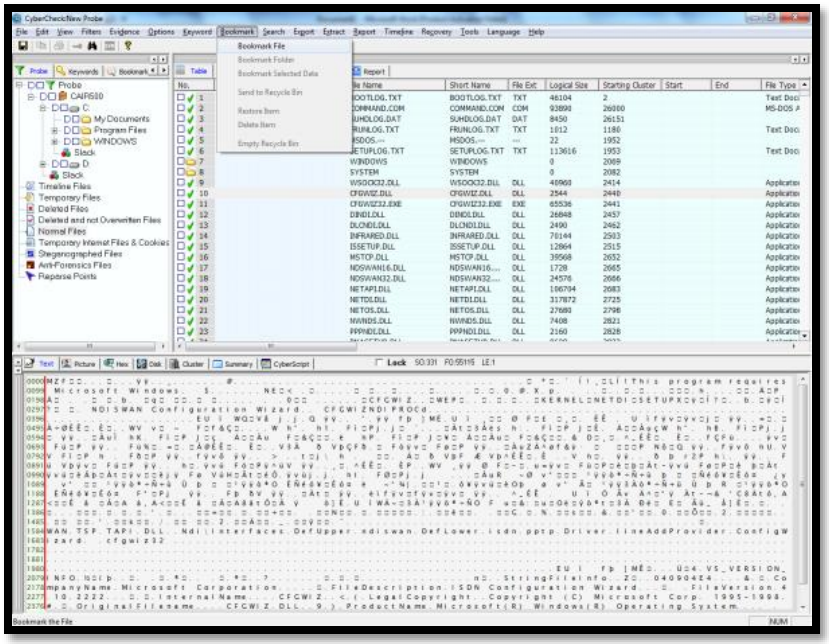
Solution: The Bookmarks tab view provides three options namely:

- **Folders** - This contains information regarding all bookmarked folders
- **Files** - This contains information regarding all bookmarked files.
- **Selected Data** - This contains information regarding the data selected for bookmarking during the analysis

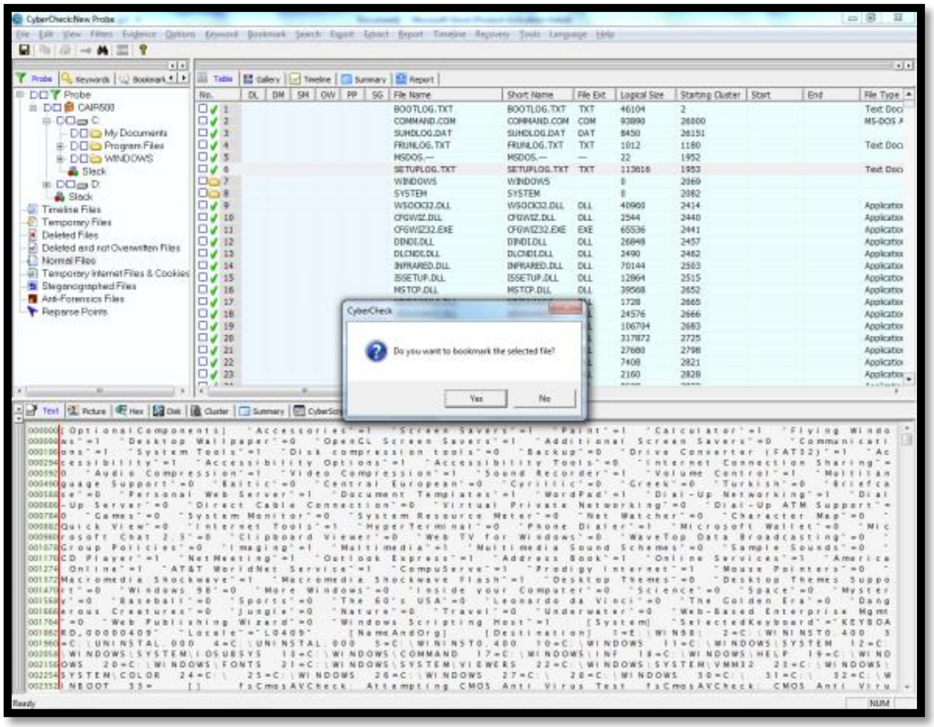
To bookmark a file, select the desired file from the **Table View**, right click and select **Bookmark File** from the context menu.



Bookmarking a file can also be done by selecting **Bookmark> Bookmark File** from main menu.



On selection, a message for confirming the process will be displayed. Click **Yes** button



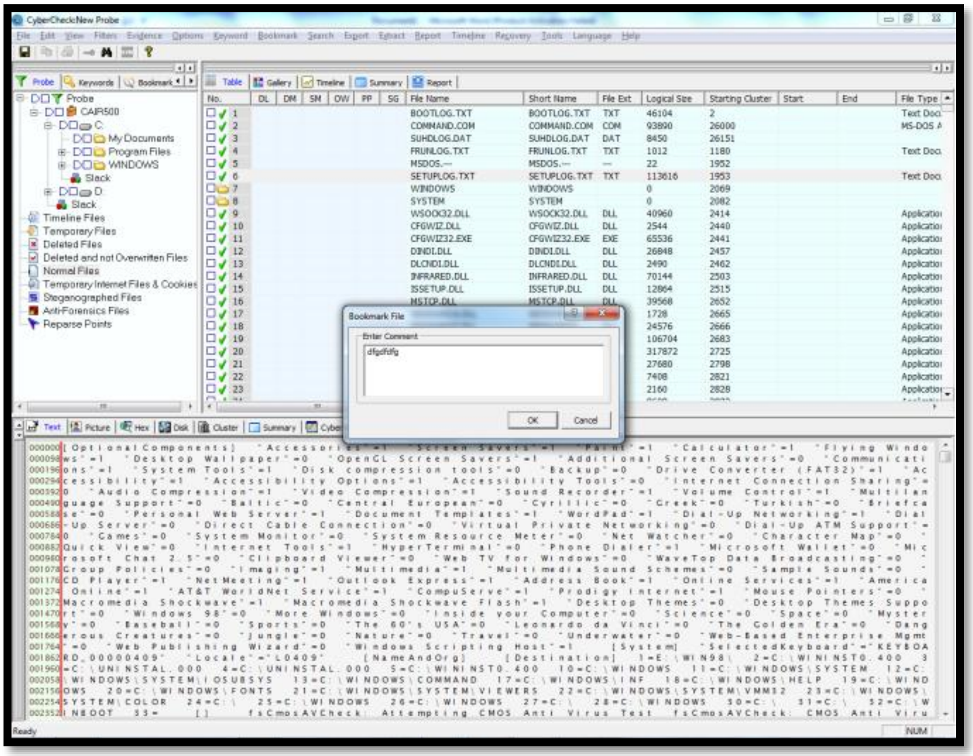
CyberCheck

Do you want to bookmark the selected file?

Yes | No

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1							BOOTLOG.TXT	BOOTLOG.TXT	TXT	46104	2			Text Doci
2							COMMAND.COM	COMMAND.COM	COM	93890	26000			MS-DOS A
3							SUHDLOG.DAT	SUHDLOG.DAT	DAT	8450	26151			
4							FRUNLOG.TXT	FRUNLOG.TXT	TXT	1012	1180			Text Doci
5							MSDOS.---	MSDOS.---	---	22	1952			
6							SETUPLOG.TXT	SETUPLOG.TXT	TXT	113616	1953			Text Doci
7							WINDOWS	WINDOWS		0	2069			
8							SYSTEM	SYSTEM		0	2082			
9							WSOCK32.DLL	WSOCK32.DLL	DLL	40960	2414			Applicatio
10							CFGWIZ.DLL	CFGWIZ.DLL	DLL	2544	2440			Applicatio
11							CFGWIZ32.EXE	CFGWIZ32.EXE	EXE	65536	2441			Applicatio
12							DINDI.DLL	DINDI.DLL	DLL	26848	2457			Applicatio
13							DLCNDI.DLL	DLCNDI.DLL	DLL	2490	2462			Applicatio
14							INFRARED.DLL	INFRARED.DLL	DLL	70144	2503			Applicatio
15							ISSETUP.DLL	ISSETUP.DLL	DLL	12864	2515			Applicatio
16							MSTCP.DLL	MSTCP.DLL	DLL	39568	2652			Applicatio
17										1728	2665			Applicatio
18										24576	2666			Applicatio
19										106704	2683			Applicatio
20										317872	2725			Applicatio
21										27680	2798			Applicatio
22										7408	2821			Applicatio
23										2160	2828			Applicatio

A dialog box will be displayed for entering comments, if any, to be attached with this file. Enter appropriate comment and press **OK** button for bookmarking the selected file.



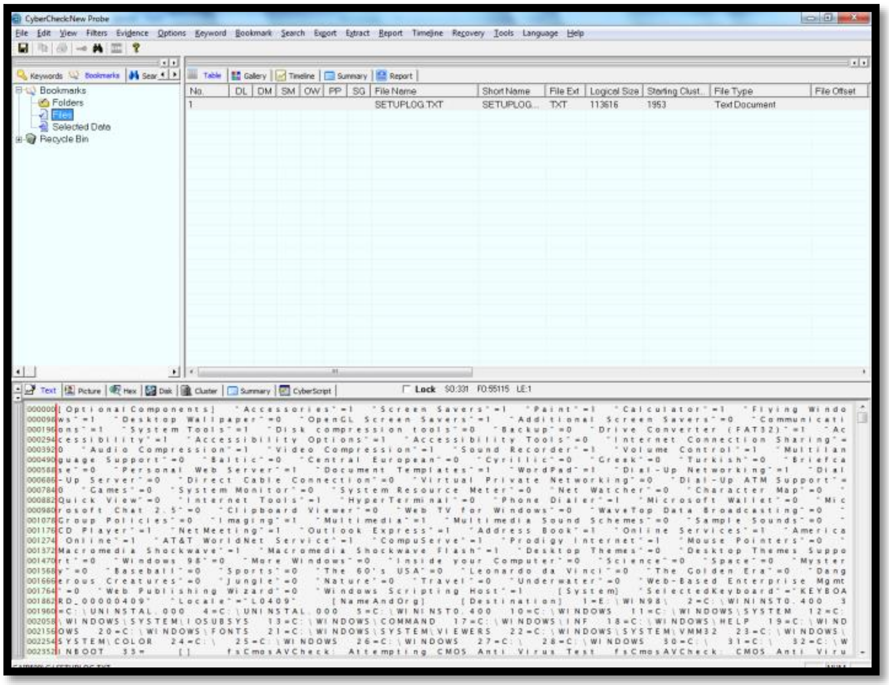
Bookmark File

Enter Comment

dfgdfdfg

OK | Cancel

The bookmarked file now gets added up under the **Bookmark** tab in the left pane


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Keywords Bookmarks Sear
Bookmarks
Folders
Files
Selected Data
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Clust...	File Type	File Offset
1							SETUPLOG.TXT	SETUPLOG...	TXT	113616	1953	Text Document	

□ Lock S0:331 F0:55115 LE:1

```
000000[Optional Components]  "Accessories"=1  "Screen Savers"=1  "Paint"=1  "Calculator"=1  "Flying Windo
000098ws"=1  "Desktop Wallpaper"=0  "OpenGL Screen Savers"=1  "Additional Screen Savers"=0  "Communicati
000196ons"=1  "System Tools"=1  "Disk compression tools"=0  "Backup"=0  "Drive Converter (FAT32)"=1  "Ac
000294cessibility"=1  "Accessibility Options"=1  "Accessibility Tools"=0  "Internet Connection Sharing"=
0003920  "Audio Compression"=1  "Video Compression"=1  "Sound Recorder"=1  "Volume Control"=1  "Multilan
000490guage Support"=0  "Baltic"=0  "Central European"=0  "Cyrillic"=0  "Greek"=0  "Turkish"=0  "Briefca
000588se"=0  "Personal Web Server"=1  "Document Templates"=1  "WordPad"=1  "Dial-Up Networking"=1  "Dial
000686-Up Server"=0  "Direct Cable Connection"=0  "Virtual Private Networking"=0  "Dial-Up ATM Support"=
0007840  "Games"=0  "System Monitor"=0  "System Resource Meter"=0  "Net Watcher"=0  "Character Map"=0  "
000882Quick View"=0  "Internet Tools"=1  "HyperTerminal"=0  "Phone Dialer"=1  "Microsoft Wallet"=0  "Mic
000980rosoft Chat 2.5"=0  "Clipboard Viewer"=0  "Web TV for Windows"=0  "WaveTop Data Broadcasting"=0  "
001078Group Policies"=0  "Imaging"=1  "Multimedia"=1  "Multimedia Sound Schemes"=0  "Sample Sounds"=0  "
001176CD Player"=1  "NetMeeting"=1  "Outlook Express"=1  "Address Book"=1  "Online Services"=1  "America
001274 Online"=1  "AT&T WorldNet Service"=1  "CompuServe"=1  "Prodigy Internet"=1  "Mouse Pointers"=0  "
001372Macromedia Shockwave"=1  "Macromedia Shockwave Flash"=1  "Desktop Themes"=0  "Desktop Themes Suppo
001470rt"=0  "Windows 98"=0  "More Windows"=0  "Inside your Computer"=0  "Science"=0  "Space"=0  "Myster
001568y"=0  "Baseball"=0  "Sports"=0  "The 60's USA"=0  "Leonardo da Vinci"=0  "The Golden Era"=0  "Dang
001666erous Creatures"=0  "Jungle"=0  "Nature"=0  "Travel"=0  "Underwater"=0  "Web-Based Enterprise Mgmt
001764"=0  "Web Publishing Wizard"=0  "Windows Scripting Host"=1  [System]  "SelectedKeyboard"="KEYBOA
001862RD_00000409"  "Locale"="L0409"  [NameAndOrg]  [Destination]  1=E:\WIN98\  2=C:\WININST0.400  3
001960=C:\UNINSTAL.000  4=C:\UNINSTAL.000  5=C:\WININST0.400  10=C:\WINDOWS  11=C:\WINDOWS\SYSTEM  12=C:
002058\WINDOWS\SYSTEM\IOSUBSYS  13=C:\WINDOWS\COMMAND  17=C:\WINDOWS\INF  18=C:\WINDOWS\HELP  19=C:\WIND
002156OWS  20=C:\WINDOWS\FONTS  21=C:\WINDOWS\SYSTEM\VIEWERS  22=C:\WINDOWS\SYSTEM\VMM32  23=C:\WINDOWS\
002254SYSTEM\COLOR  24=C:\  25=C:\WINDOWS  26=C:\WINDOWS  27=C:\  28=C:\WINDOWS  30=C:\  31=C:\  32=C:\W
002352INBOOT  33=  []  fsCmosAVCheck: Attempting CMOS Anti Virus Test  fsCmosAVCheck: CMOS Anti Viru
```

Task 8: How do you add a book-marked item into the report?

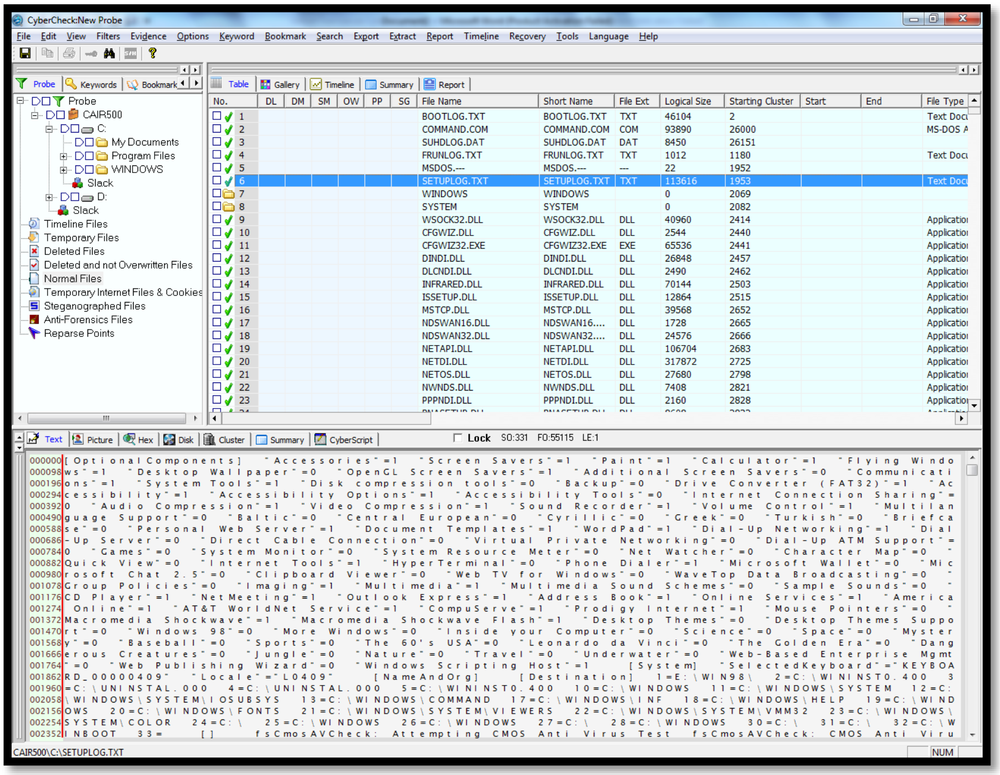
Solution: Two Methods are there:

a.) Go to Bookmark Tab view >> Right Click bookmarked items >> Append to Report

b.) On Table Tab view >> Right Click the Folders/Files >> Append to Report

Task 9: How can you view the entire pictures available in an evidence file?

Solution: The **Gallery view** in the Right pane is a quick way to see the entire pictures available in a folder as thumbnail views. For viewing pictures select a folder.

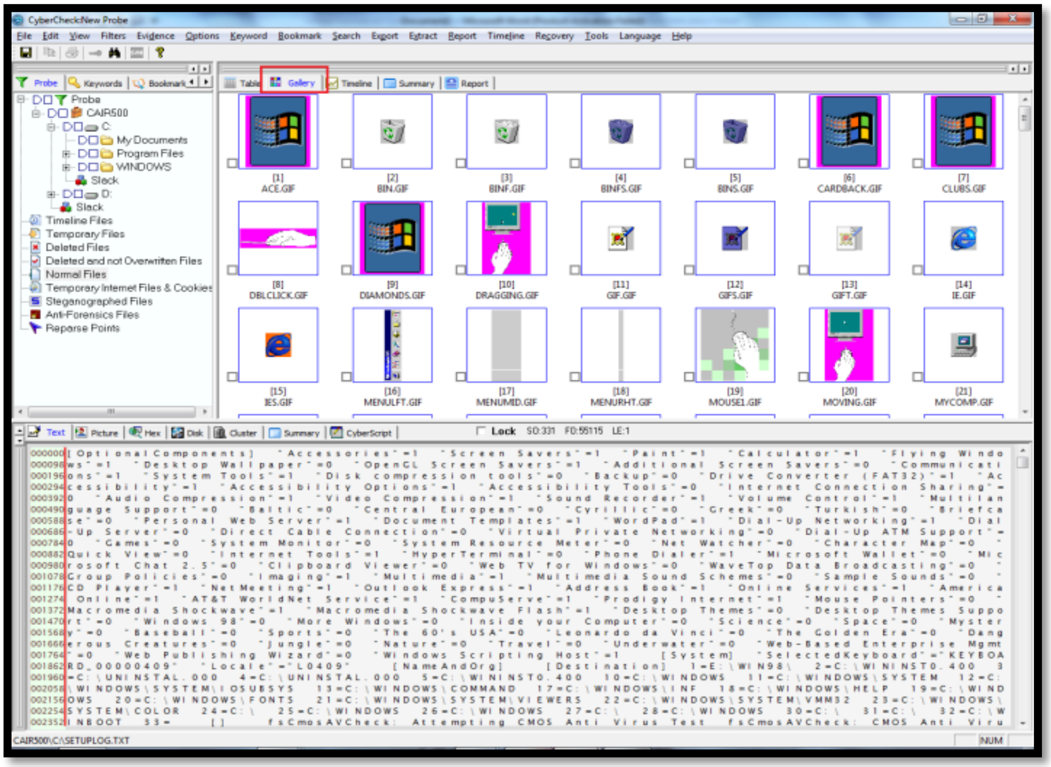

CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Probe
CAIR500
C:
My Documents
Program Files
WINDOWS
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock SO:331 FO:55115 LE:1
NUM

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1							BOOTLOG.TXT	BOOTLOG.TXT	TXT	46104	2			Text Doc
2							COMMAND.COM	COMMAND.COM	COM	93890	26000			MS-DOS A
3							SUHDLOG.DAT	SUHDLOG.DAT	DAT	8450	26151			
4							FRUNLOG.TXT	FRUNLOG.TXT	TXT	1012	1180			Text Doc
5							MSDOS.---	MSDOS.---	---	22	1952			
6							SETUPLOG.TXT	SETUPLOG.TXT	TXT	113616	1953			Text Doc
7							WINDOWS	WINDOWS		0	2069			
8							SYSTEM	SYSTEM		0	2082			
9							WSOCK32.DLL	WSOCK32.DLL	DLL	40960	2414			Applicatio
10							CFGWIZ.DLL	CFGWIZ.DLL	DLL	2544	2440			Applicatio
11							CFGWIZ32.EXE	CFGWIZ32.EXE	EXE	65536	2441			Applicatio
12							DINDI.DLL	DINDI.DLL	DLL	26848	2457			Applicatio
13							DLCNDI.DLL	DLCNDI.DLL	DLL	2490	2462			Applicatio
14							INFRARED.DLL	INFRARED.DLL	DLL	70144	2503			Applicatio
15							ISSETUP.DLL	ISSETUP.DLL	DLL	12864	2515			Applicatio
16							MSTCP.DLL	MSTCP.DLL	DLL	39568	2652			Applicatio
17							NDSWAN16.DLL	NDSWAN16....	DLL	1728	2665			Applicatio
18							NDSWAN32.DLL	NDSWAN32....	DLL	24576	2666			Applicatio
19							NETAPI.DLL	NETAPI.DLL	DLL	106704	2683			Applicatio
20							NETDI.DLL	NETDI.DLL	DLL	317872	2725			Applicatio
21							NETOS.DLL	NETOS.DLL	DLL	27680	2798			Applicatio
22							NWNDS.DLL	NWNDS.DLL	DLL	7408	2821			Applicatio
23							PPPNDI.DLL	PPPNDI.DLL	DLL	2160	2828			Applicatio

```
000000[Optional Components]  "Accessories"=1  "Screen Savers"=1  "Paint"=1  "Calculator"=1  "Flying Windo
000098ws"=1  "Desktop Wallpaper"=0  "OpenGL Screen Savers"=1  "Additional Screen Savers"=0  "Communicati
000196ons"=1  "System Tools"=1  "Disk compression tools"=0  "Backup"=0  "Drive Converter (FAT32)"=1  "Ac
000294cessibility"=1  "Accessibility Options"=1  "Accessibility Tools"=0  "Internet Connection Sharing"=
0003920  "Audio Compression"=1  "Video Compression"=1  "Sound Recorder"=1  "Volume Control"=1  "Multilan
000490guage Support"=0  "Baltic"=0  "Central European"=0  "Cyrillic"=0  "Greek"=0  "Turkish"=0  "Briefca
000588se"=0  "Personal Web Server"=1  "Document Templates"=1  "WordPad"=1  "Dial-Up Networking"=1  "Dial
000686-Up Server"=0  "Direct Cable Connection"=0  "Virtual Private Networking"=0  "Dial-Up ATM Support"=
0007840  "Games"=0  "System Monitor"=0  "System Resource Meter"=0  "Net Watcher"=0  "Character Map"=0  "
000882Quick View"=0  "Internet Tools"=1  "HyperTerminal"=0  "Phone Dialer"=1  "Microsoft Wallet"=0  "Mic
000980rosoft Chat 2.5"=0  "Clipboard Viewer"=0  "Web TV for Windows"=0  "WaveTop Data Broadcasting"=0  "
001078Group Policies"=0  "Imaging"=1  "Multimedia"=1  "Multimedia Sound Schemes"=0  "Sample Sounds"=0  "
001176CD Player"=1  "NetMeeting"=1  "Outlook Express"=1  "Address Book"=1  "Online Services"=1  "America
001274 Online"=1  "AT&T WorldNet Service"=1  "CompuServe"=1  "Prodigy Internet"=1  "Mouse Pointers"=0  "
001372Macromedia Shockwave"=1  "Macromedia Shockwave Flash"=1  "Desktop Themes"=0  "Desktop Themes Suppo
001470rt"=0  "Windows 98"=0  "More Windows"=0  "Inside your Computer"=0  "Science"=0  "Space"=0  "Myster
001568y"=0  "Baseball"=0  "Sports"=0  "The 60's USA"=0  "Leonardo da Vinci"=0  "The Golden Era"=0  "Dang
001666erous Creatures"=0  "Jungle"=0  "Nature"=0  "Travel"=0  "Underwater"=0  "Web-Based Enterprise Mgmt
001764"=0  "Web Publishing Wizard"=0  "Windows Scripting Host"=1    [System]  "SelectedKeyboard"="KEYBOA
001862RD_00000409"  "Locale"="L0409"    [NameAndOrg]    [Destination]  1=E:\WIN98\  2=C:\WININST0.400  3
001960=C:\UNINSTAL.000  4=C:\UNINSTAL.000  5=C:\WININST0.400  10=C:\WINDOWS  11=C:\WINDOWS\SYSTEM  12=C:
002058\WINDOWS\SYSTEM\IOSUBSYS  13=C:\WINDOWS\COMMAND  17=C:\WINDOWS\INF  18=C:\WINDOWS\HELP  19=C:\WIND
002156OWS  20=C:\WINDOWS\FONTS  21=C:\WINDOWS\SYSTEM\VIEWERS  22=C:\WINDOWS\SYSTEM\VMM32  23=C:\WINDOWS\
002254SYSTEM\COLOR  24=C:\  25=C:\WINDOWS  26=C:\WINDOWS  27=C:\  28=C:\WINDOWS  30=C:\  31=C:\  32=C:\W
002352INBOOT  33=  []  fsCmosAVCheck: Attempting CMOS Anti Virus Test  fsCmosAVCheck: CMOS Anti Viru
```

CAIR500\C:\SETUPLOG.TXT

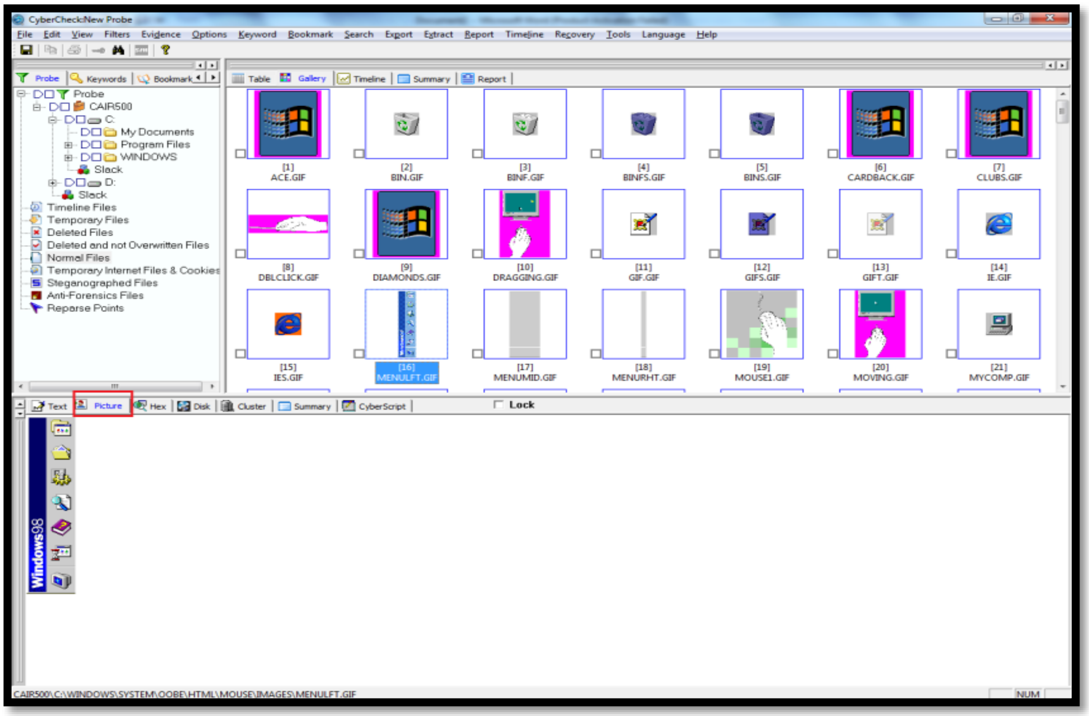
Select the **Gallery View** tab from the right pane. All the picture files available in that folder will be displayed in the gallery viewer.



```
000000[Optional Components] "Accessories"=1 "Screen Savers"=1 "Paint"=1 "Calculator"=1 "Flying Windo
000098ws"=1 "Desktop Wallpaper"=0 "OpenGL Screen Savers"=1 "Additional Screen Savers"=0 "Communicati
000196ons"=1 "System Tools"=1 "Disk compression tools"=0 "Backup"=0 "Drive Converter (FAT32)"=1 "Ac
000294cessibility"=1 "Accessibility Options"=1 "Accessibility Tools"=0 "Internet Connection Sharing"=
0003920 "Audio Compression"=1 "Video Compression"=1 "Sound Recorder"=1 "Volume Control"=1 "Multilan
000490guage Support"=0 "Baltic"=0 "Central European"=0 "Cyrillic"=0 "Greek"=0 "Turkish"=0 "Briefca
000588se"=0 "Personal Web Server"=1 "Document Templates"=1 "WordPad"=1 "Dial-Up Networking"=1 "Dial
000686-Up Server"=0 "Direct Cable Connection"=0 "Virtual Private Networking"=0 "Dial-Up ATM Support"=
0007840 "Games"=0 "System Monitor"=0 "System Resource Meter"=0 "Net Watcher"=0 "Character Map"=0 "
000882Quick View"=0 "Internet Tools"=1 "HyperTerminal"=0 "Phone Dialer"=1 "Microsoft Wallet"=0 "Mic
000980rosoft Chat 2.5"=0 "Clipboard Viewer"=0 "Web TV for Windows"=0 "WaveTop Data Broadcasting"=0 "
001078Group Policies"=0 "Imaging"=1 "Multimedia"=1 "Multimedia Sound Schemes"=0 "Sample Sounds"=0 "
001176CD Player"=1 "NetMeeting"=1 "Outlook Express"=1 "Address Book"=1 "Online Services"=1 "America
001274 Online"=1 "AT&T WorldNet Service"=1 "CompuServe"=1 "Prodigy Internet"=1 "Mouse Pointers"=0 "
001372Macromedia Shockwave"=1 "Macromedia Shockwave Flash"=1 "Desktop Themes"=0 "Desktop Themes Suppo
001470rt"=0 "Windows 98"=0 "More Windows"=0 "Inside your Computer"=0 "Science"=0 "Space"=0 "Myster
001568y"=0 "Baseball"=0 "Sports"=0 "The 60's USA"=0 "Leonardo da Vinci"=0 "The Golden Era"=0 "Dang
001666erous Creatures"=0 "Jungle"=0 "Nature"=0 "Travel"=0 "Underwater"=0 "Web-Based Enterprise Mgmt
001764"=0 "Web Publishing Wizard"=0 "Windows Scripting Host"=1 [System] "SelectedKeyboard"="KEYBOA
001862RD_00000409" "Locale"="L0409" [NameAndOrg] [Destination] 1=E:\WIN98\ 2=C:\WININST0.400 3
001960=C:\UNINSTAL.000 4=C:\UNINSTAL.000 5=C:\WININST0.400 10=C:\WINDOWS 11=C:\WINDOWS\SYSTEM 12=C:
002058\WINDOWS\SYSTEM\IOSUBSYS 13=C:\WINDOWS\COMMAND 17=C:\WINDOWS\INF 18=C:\WINDOWS\HELP 19=C:\WIND
002156OWS 20=C:\WINDOWS\FONTS 21=C:\WINDOWS\SYSTEM\VIEWERS 22=C:\WINDOWS\SYSTEM\VMM32 23=C:\WINDOWS\
002254SYSTEM\COLOR 24=C:\ 25=C:\WINDOWS 26=C:\WINDOWS 27=C:\ 28=C:\WINDOWS 30=C:\ 31=C:\ 32=C:\W
002352INBOOT 33= [] fsCmosAVCheck: Attempting CMOS Anti Virus Test fsCmosAVCheck: CMOS Anti Viru
```

CAIR500\C:\SETUPLOG.TXT

To see the enlarged image –Select the needed picture, which will be displayed in the **Picture viewer** in the bottom pane.

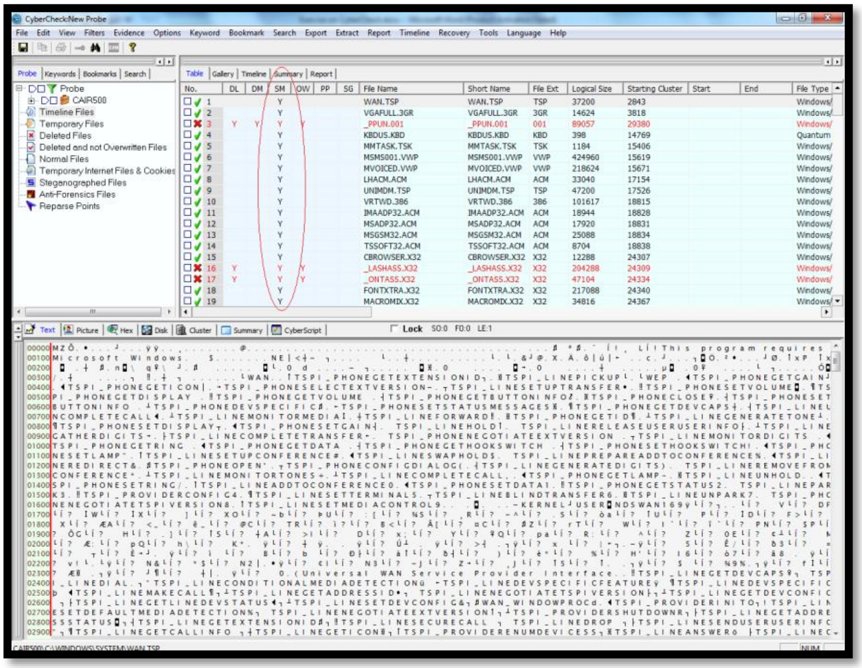


CAIR500\C:\WINDOWS\SYSTEM\OOBE\HTML\MOUSE\IMAGES\MENULFT.GIF

Task 10: How can you see a signature-mismatched file?

Solution: Option menu >> Check File Signature.

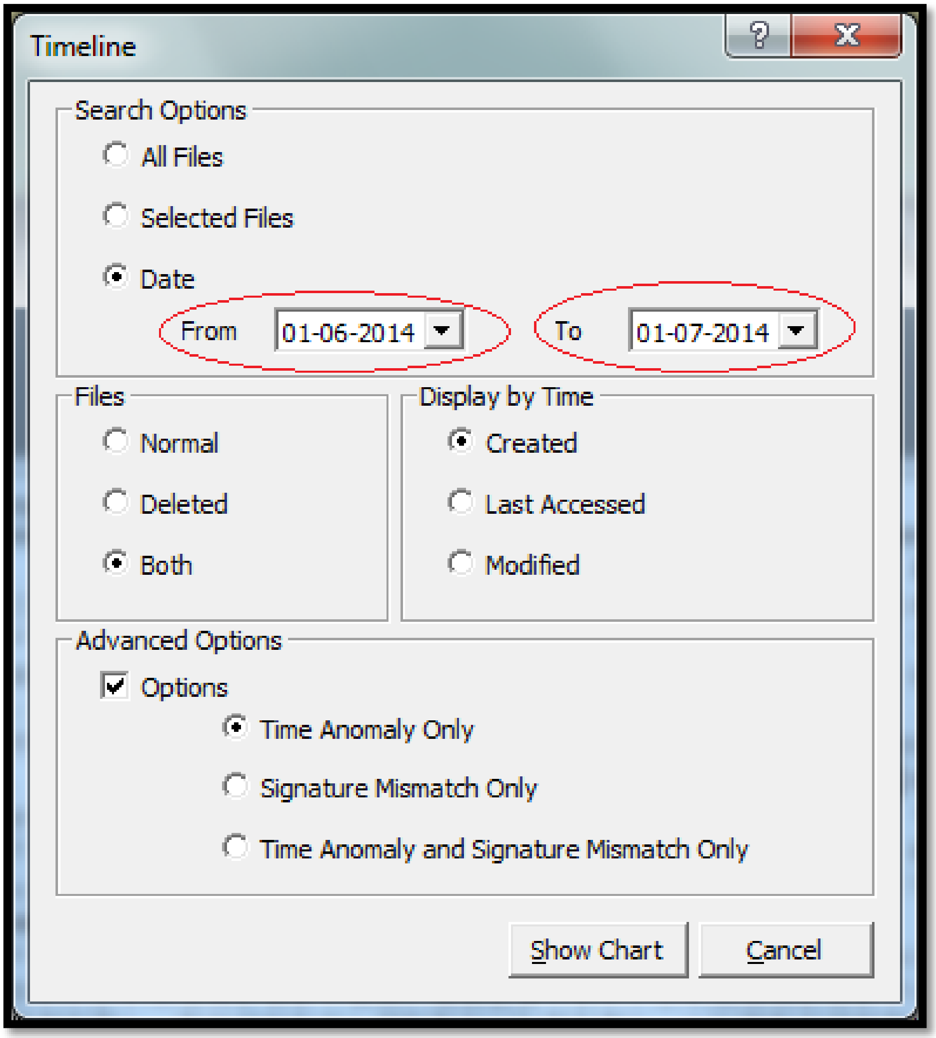
Those files, which have a signature mismatch, will display a status **"Y"** in the **SM** (Signature Mismatch) column in the Table View.


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
Probe
CAIR500
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock SO:0 FO:0 LE:1

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1			Y				WAN.TSP	WAN.TSP	TSP	37200	2843			Windows/
2			Y				VGAFULL.3GR	VGAFULL.3GR	3GR	14624	3818			Windows/
3	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows/
4			Y				KBDUS.KBD	KBDUS.KBD	KBD	398	14769			Quantum
5			Y				MMTASK.TSK	MMTASK.TSK	TSK	1184	15406			Windows/
6			Y				MSMS001.VWP	MSMS001.VWP	VWP	424960	15619			Windows/
7			Y				MVOICED.VWP	MVOICED.VWP	VWP	218624	15671			Windows/
8			Y				LHACM.ACM	LHACM.ACM	ACM	33040	17154			Windows/
9			Y				UNIMDM.TSP	UNIMDM.TSP	TSP	47200	17526			Windows/
10			Y				VRTWD.386	VRTWD.386	386	101617	18815			Windows/
11			Y				IMAADP32.ACM	IMAADP32.ACM	ACM	18944	18828			Windows/
12			Y				MSADP32.ACM	MSADP32.ACM	ACM	17920	18831			Windows/
13			Y				MSGSM32.ACM	MSGSM32.ACM	ACM	25088	18834			Windows/
14			Y				TSSOFT32.ACM	TSSOFT32.ACM	ACM	8704	18838			Windows/
15			Y				CBROWSER.X32	CBROWSER.X32	X32	12288	24307			Windows/
16	Y		Y	Y			_LASHASS.X32	_LASHASS.X32	X32	204288	24309			Windows/
17	Y		Y	Y			_ONTASS.X32	_ONTASS.X32	X32	47104	24334			Windows/
18			Y				FONTXTRA.X32	FONTXTRA.X32	X32	217088	24340			Windows/
19			Y				MACROMIX.X32	MACROMIX.X32	X32	34816	24367			Windows/

Task 11: How can you search for files, which are created within a particular time frame?

Solution: In the Timeline dialog select the **Date** and pick the appropriate **From** and **To** date and click the **Show Chart** button.



Timeline

Search Options

○ All Files

○ Selected Files

● Date

From 01-06-2014 To 01-07-2014

Files

○ Normal

○ Deleted

● Both

Display by Time

● Created

○ Last Accessed

○ Modified

Advanced Options

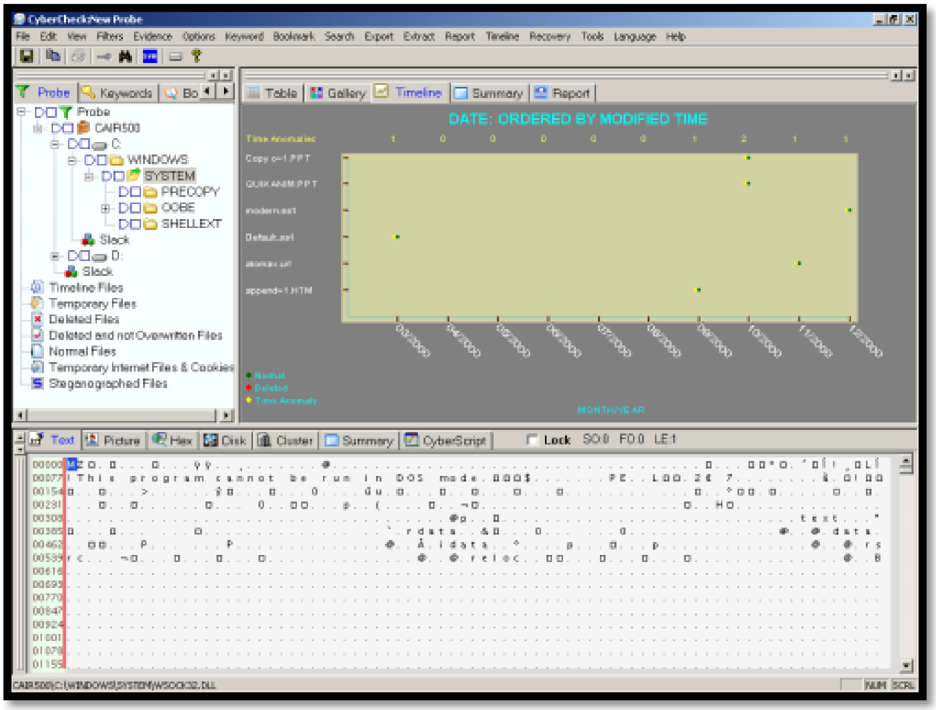
☑ Options

● Time Anomaly Only

○ Signature Mismatch Only

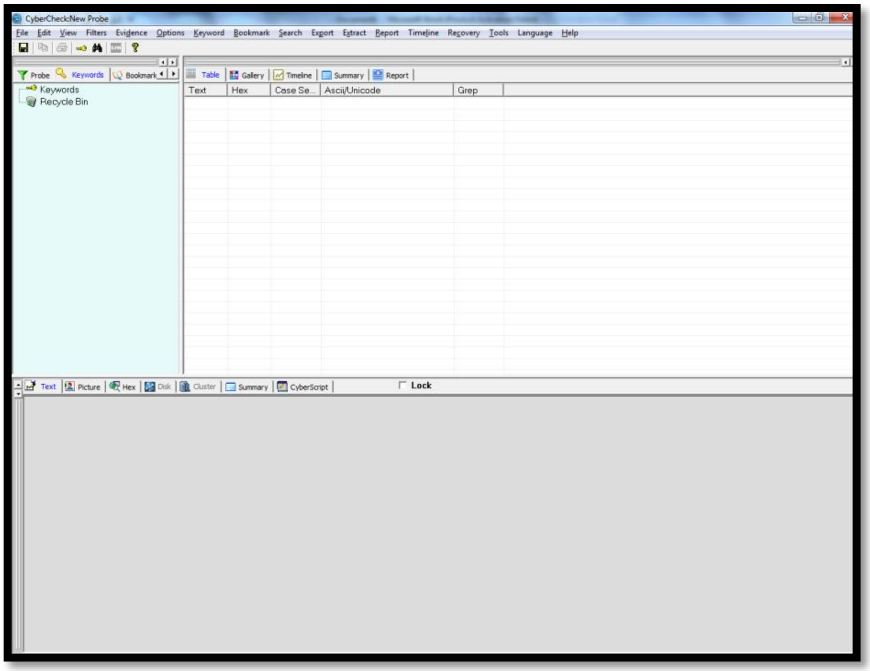
○ Time Anomaly and Signature Mismatch Only

Display the files, which are created within a time frame in the Timeline chart.

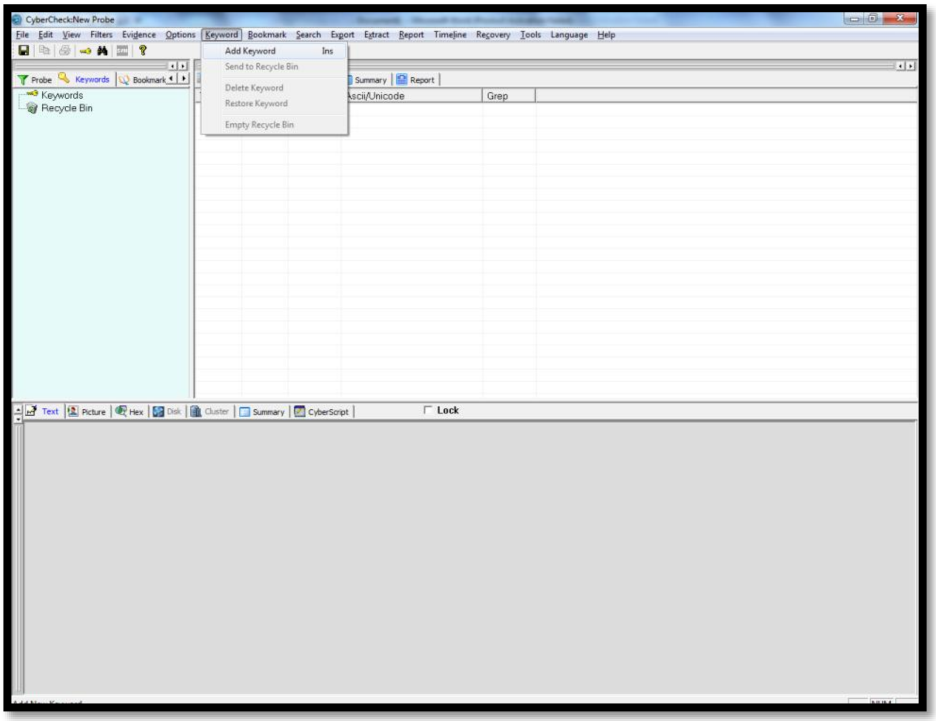


Task 12: How do you perform a search for a particular key word in unallocated cluster area?

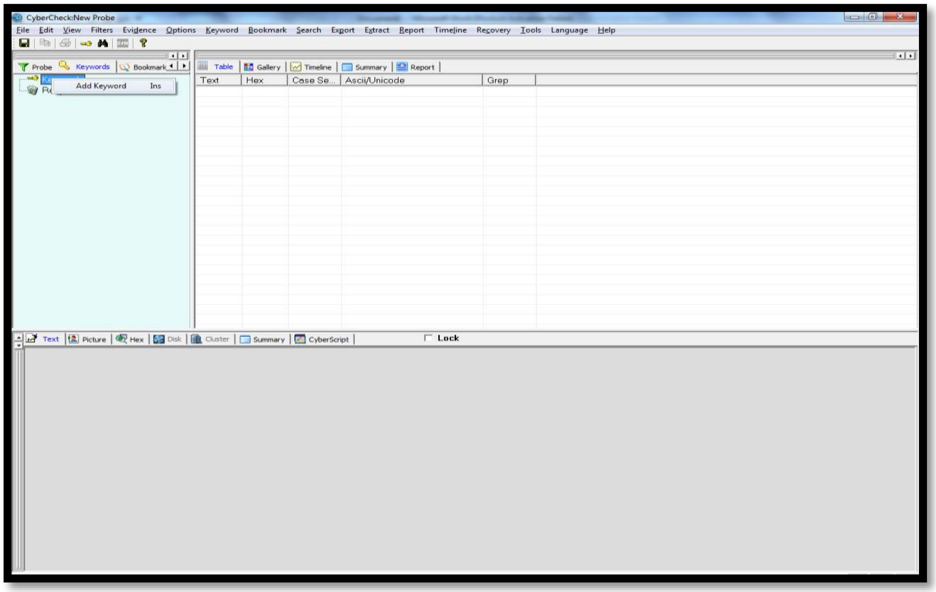
Solution: Select Keyword tab from left pane



Click **Add Keyword** option from the Keyword menu. This sub-menu item will become enabled, only when in the Keywords tab in the left pane.

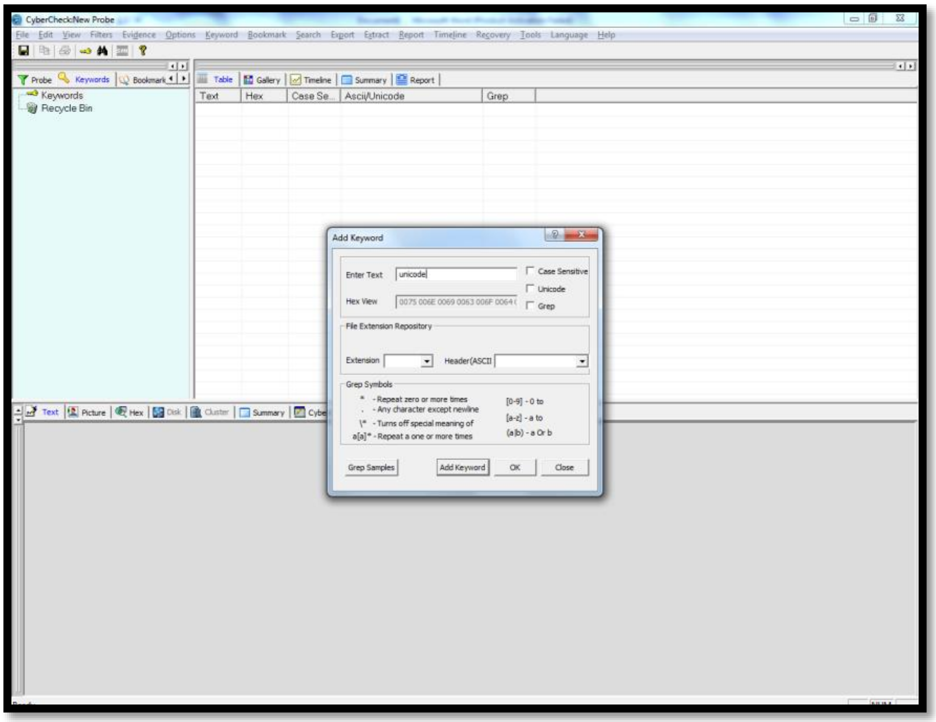


Or Right click **Keywords** and select **Add Keyword.**


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Add Keyword Ins
Table Gallery Timeline Summary Report
Text Hex Case Se... Ascii/Unicode Grep
Text Picture Hex Disk Cluster Summary CyberScript
Lock

The fourth item (item with **key** symbol) in the toolbar also has the same functionality.

On clicking Add Keyword option a new dialog box appears. Add the specified keyword in **Enter Text** box. Hex View shows the hex value of the entered text. Keyword to be searched can be made Case sensitive, Unicode or Grep type



Add Keyword

Enter Text: unicode

Hex View: 0075 006E 0069 0063 006F 0064 (

□ Case Sensitive
□ Unicode
□ Grep

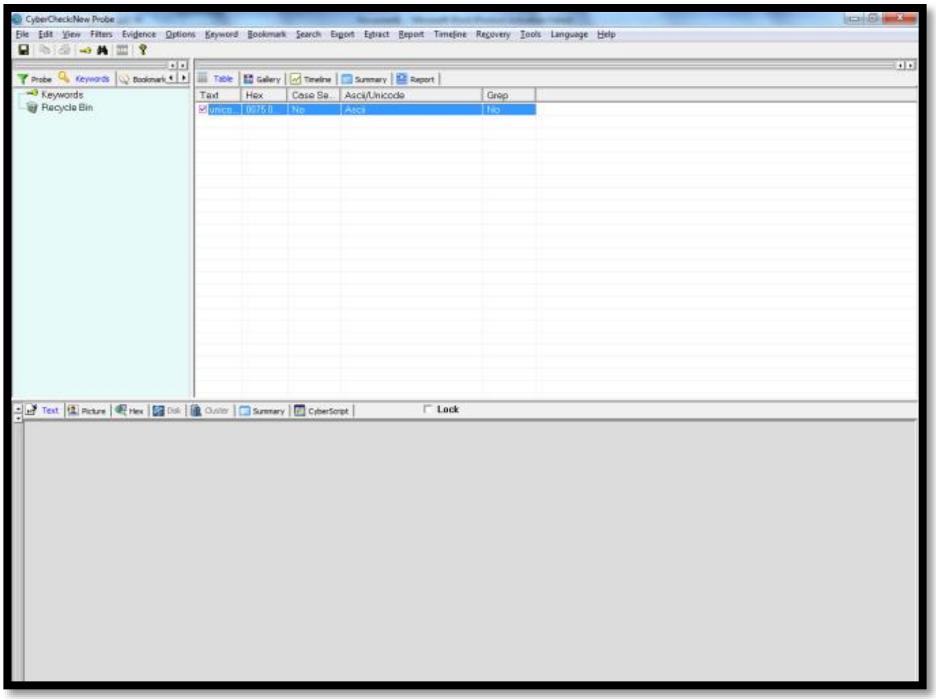
File Extension Repository

Extension:
Header(ASCII:

Grep Symbols

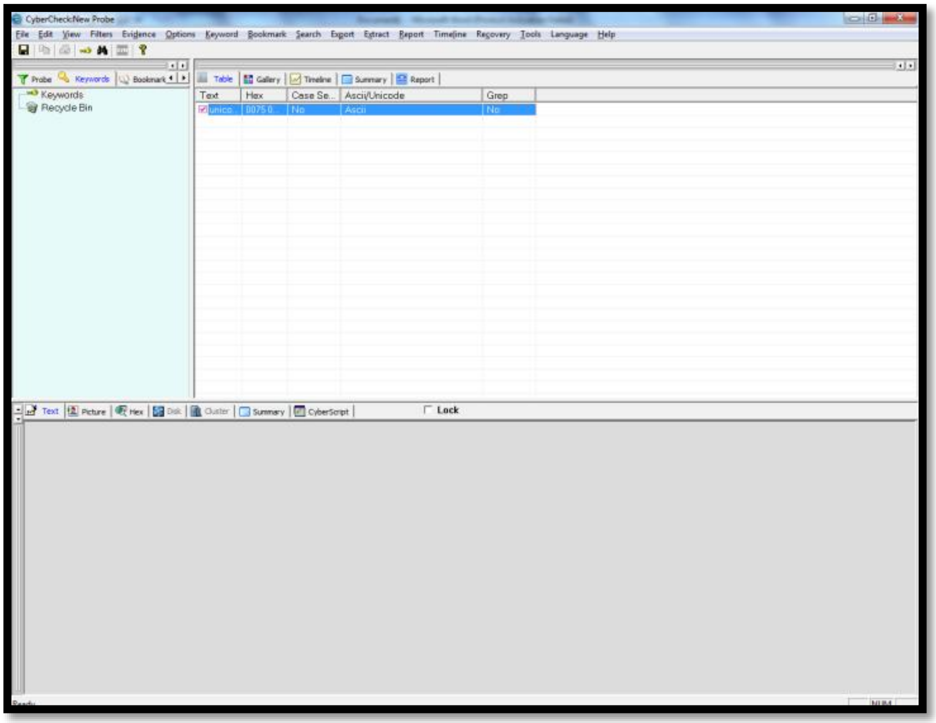
* - Repeat zero or more times
. - Any character except newline
* - Turns off special meaning of
a[a]* - Repeat a one or more times
[0-9] - 0 to
[a-z] - a to
(a|b) - a Or b

CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Hex Case Se... Ascii/Unicode Grep
Text Picture Hex Disk Cluster Summary Cybe
Grep Samples
Add Keyword
OK
Close


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock

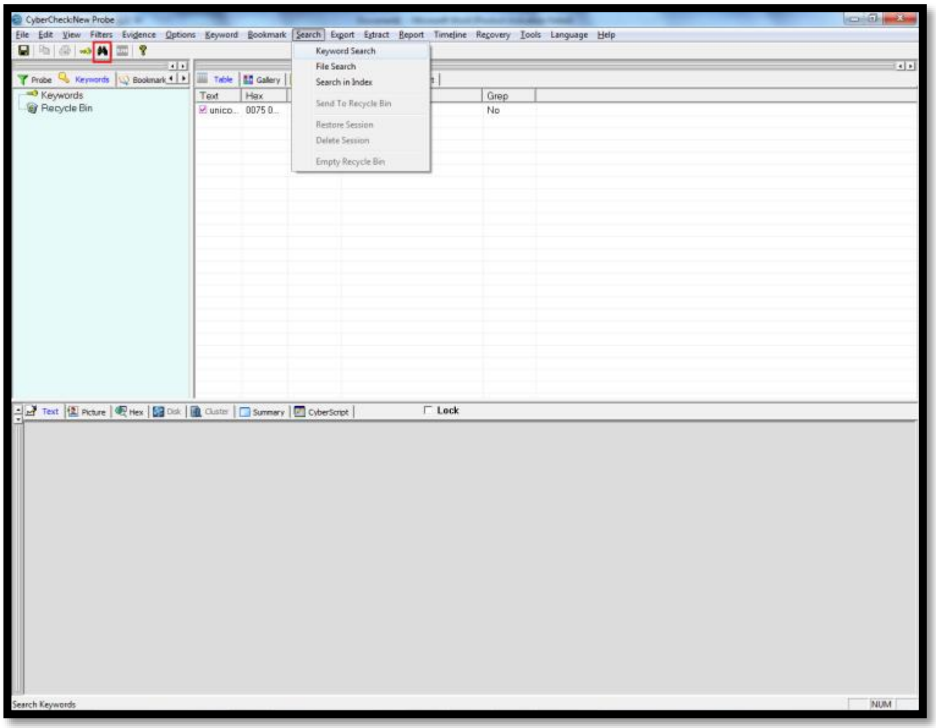
Text	Hex	Case Se..	Ascii/Unicode	Grep
☑ unico...	0075 0...	No	Ascii	No

After entering the keyword, click **OK** button, the entered keyword will then be added to a list of keywords to form a Table of keywords. To search for multiple keywords, press **Add Keyword** button. To search for a particular keyword added, check the appropriate check boxes in the table.


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock
Ready
NUM

Text	Hex	Case Se...	Ascii/Unicode	Grep
☑ unico...	0075 0...	No	Ascii	No

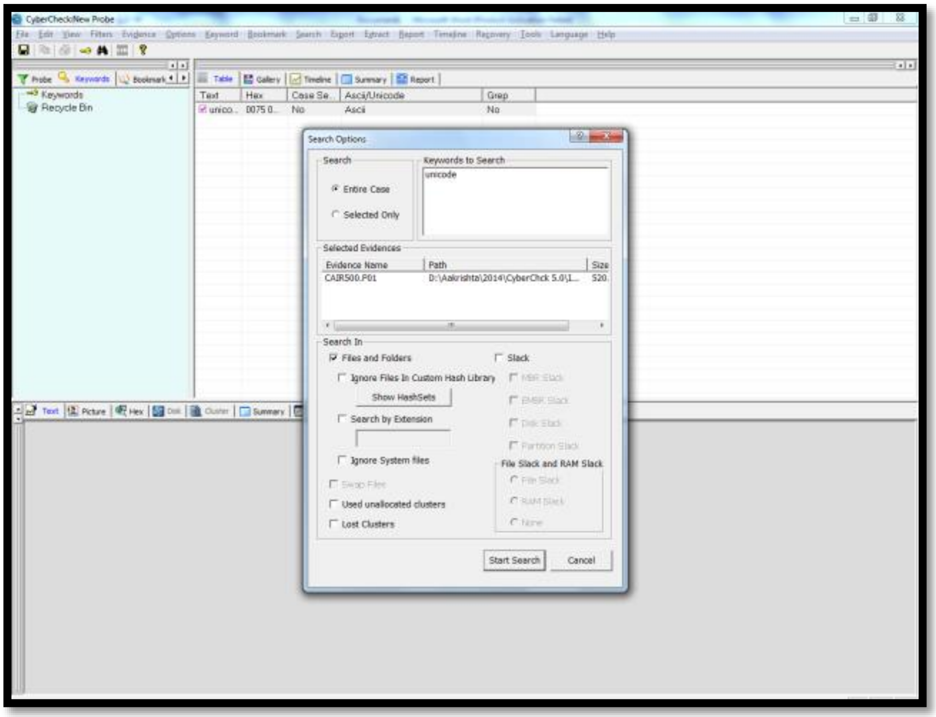
Go to **Search** option, and select **Keyword Search** or click the **Binocular** icon in tool bar



Select the keyword(s) to be searched from the table of keywords. Click on **Entire Case** to search through the entire folders and files of the evidence file. To search in a particular file, click on the **Selected Only** radio button. (Select the desired files and folders before selecting *Search > Keyword Search* menu item).

Click the Option options "Used unallocated clusters".

Press Start Search.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmark
Keywords
Recycle Bin
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary

Text	Hex	Case Se..	Ascii/Unicode	Grep
☑ unico...	0075 0...	No	Ascii	No

Search Options

Search
● Entire Case
○ Selected Only

Keywords to Search
unicode

Selected Evidences

Evidence Name	Path	Size
CAIR500.F01	D:\Aakrishta\2014\CyberChck 5.0\1...	520.

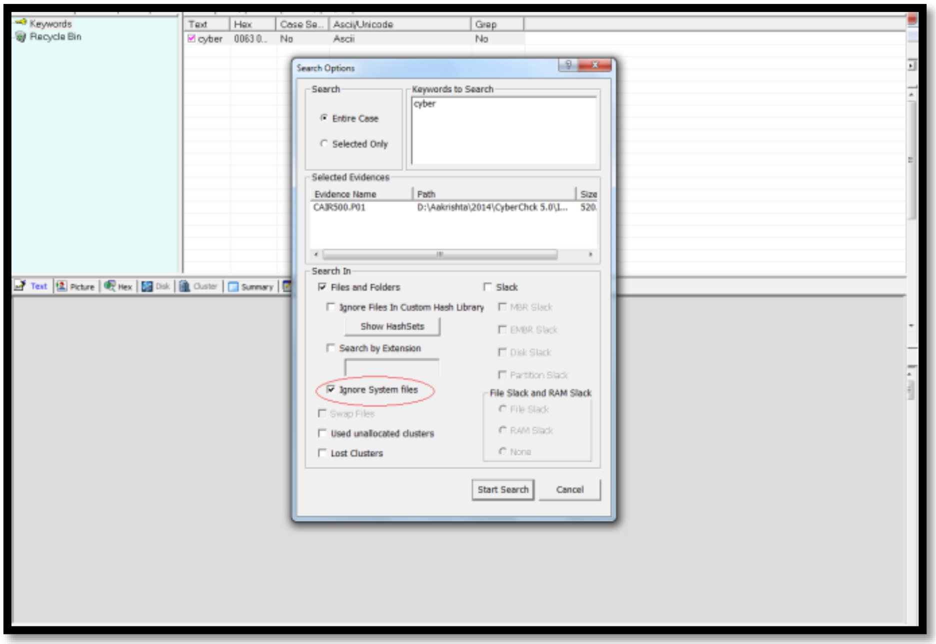
Search In
☑ Files and Folders
□ Ignore Files In Custom Hash Library
Show HashSets
□ Search by Extension
□ Ignore System files
□ Swap Files
□ Used unallocated clusters
□ Lost Clusters
□ Slack
□ MBR Slack
□ EMBR Slack
□ Disk Slack
□ Partition Slack

File Slack and RAM Slack
○ File Slack
○ RAM Slack
○ None

Start Search Cancel

Task 13: How can you exclude system files from the keyword search?

Solution: Repeat Question 12 Hints, and Tick the option "**Ignore System Files**" in **Search Options** window.



Search Options

Search

● Entire Case

○ Selected Only

Keywords to Search: cyber

Selected Evidences

Evidence Name	Path	Size
CAIR500.P01	D:\Aakrishta\2014\CyberChck 5.0\1...	520.

Search In

☑ Files and Folders

□ Ignore Files In Custom Hash Library

Show HashSets

□ Search by Extension

☑ Ignore System files

□ Swap Files

□ Used unallocated clusters

□ Lost Clusters

□ Slack

□ MBR Slack

□ EMBR Slack

□ Disk Slack

□ Partition Slack

File Slack and RAM Slack

○ File Slack

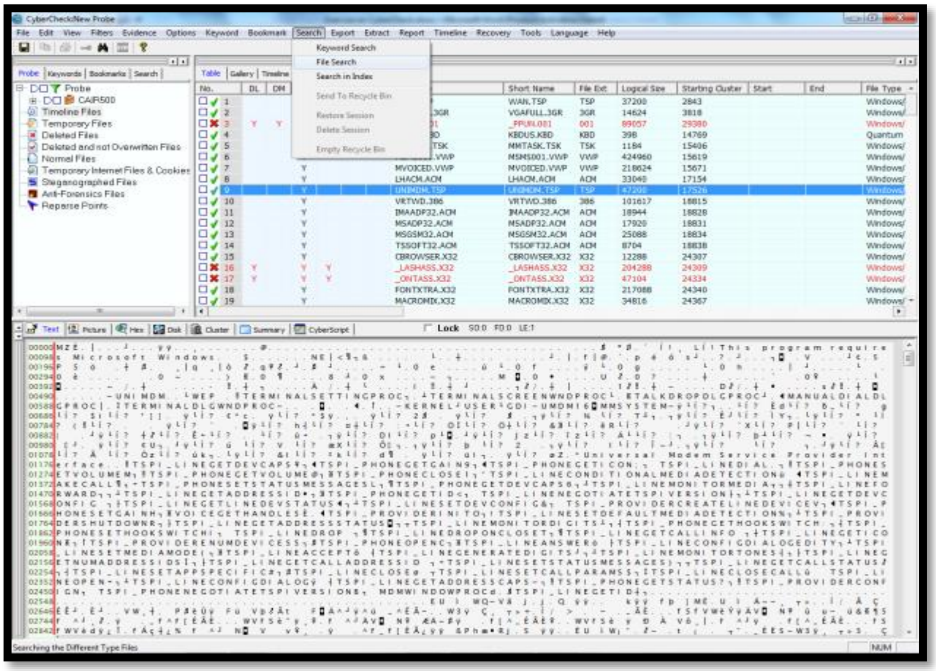
○ RAM Slack

○ None

Start Search | Cancel

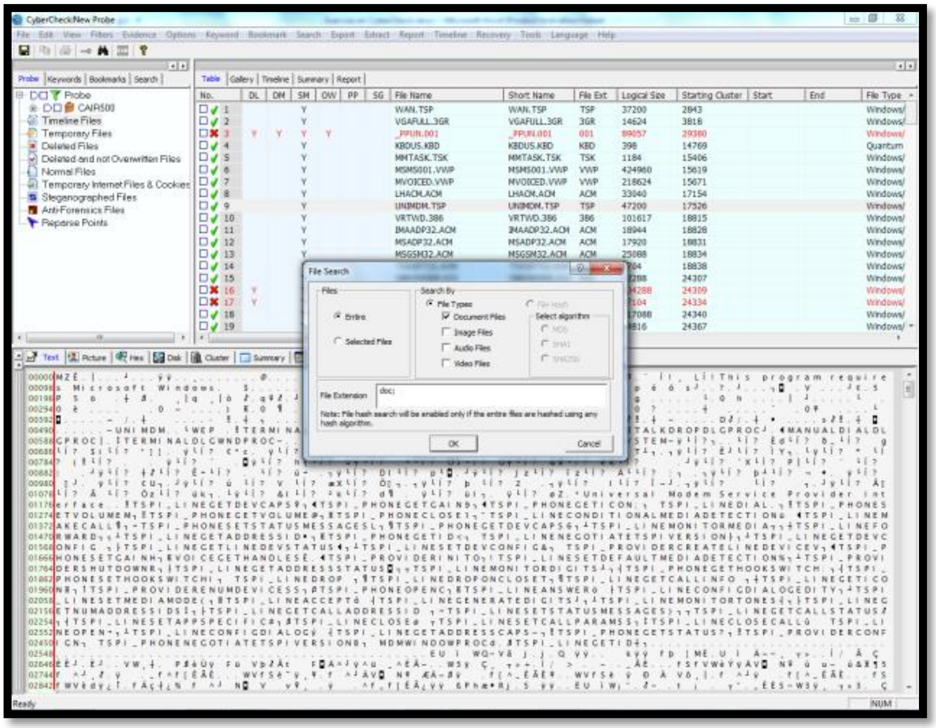
Task 14: How can you search for files based on file extension?

Solution: Select Search option from the main menu and then File Search



No.	DL	DM				Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1						WAN.TSP	TSP	37200	2843			Windows/
2					.3GR	VGAFULL.3GR	3GR	14624	3818			Windows/
3	Y	Y			1	_PPUN.001	001	89057	29380			Windows/
4					D	KBDUS.KBD	KBD	398	14769			Quantum
5					TSK	MMTASK.TSK	TSK	1184	15406			Windows/
6					.VWP	MSMS001.VWP	VWP	424960	15619			Windows/
7			Y		MVOICED.VWP	MVOICED.VWP	VWP	218624	15671			Windows/
8			Y		LHACM.ACM	LHACM.ACM	ACM	33040	17154			Windows/
9			Y		UNIMDM.TSP	UNIMDM.TSP	TSP	47200	17526			Windows/
10			Y		VRTWD.386	VRTWD.386	386	101617	18815			Windows/
11			Y		IMAADP32.ACM	IMAADP32.ACM	ACM	18944	18828			Windows/
12			Y		MSADP32.ACM	MSADP32.ACM	ACM	17920	18831			Windows/
13			Y		MSGSM32.ACM	MSGSM32.ACM	ACM	25088	18834			Windows/
14			Y		TSSOFT32.ACM	TSSOFT32.ACM	ACM	8704	18838			Windows/
15			Y		CBROWSER.X32	CBROWSER.X32	X32	12288	24307			Windows/
16	Y		Y	Y	_LASHASS.X32	_LASHASS.X32	X32	204288	24309			Windows/
17	Y		Y	Y	_ONTASS.X32	_ONTASS.X32	X32	47104	24334			Windows/
18			Y		FONTXTRA.X32	FONTXTRA.X32	X32	217088	24340			Windows/
19			Y		MACROMIX.X32	MACROMIX.X32	X32	34816	24367			Windows/

There are options to search **document**, **image**, **audio** and **video files**. On selecting these options corresponding file extensions are added in to the File Extension box. Any other extension required can be added in to File Extension edit box. By default the **Entire** case file is searched, search can be specified to **Selected Files** also.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
Probe
CAIR500
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary
Ready
NUM

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
□ ✓ 1			Y				WAN.TSP	WAN.TSP	TSP	37200	2843			Windows/
□ ✓ 2			Y				VGAFULL.3GR	VGAFULL.3GR	3GR	14624	3818			Windows/
□ ✗ 3	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows/
□ ✓ 4			Y				KBDUS.KBD	KBDUS.KBD	KBD	398	14769			Quantum
□ ✓ 5			Y				MMTASK.TSK	MMTASK.TSK	TSK	1184	15406			Windows/
□ ✓ 6			Y				MSMS001.VWP	MSMS001.VWP	VWP	424960	15619			Windows/
□ ✓ 7			Y				MVOICED.VWP	MVOICED.VWP	VWP	218624	15671			Windows/
□ ✓ 8			Y				LHACM.ACM	LHACM.ACM	ACM	33040	17154			Windows/
□ ✓ 9			Y				UNIMDM.TSP	UNIMDM.TSP	TSP	47200	17526			Windows/
□ ✓ 10			Y				VRTWD.386	VRTWD.386	386	101617	18815			Windows/
□ ✓ 11			Y				IMAADP32.ACM	IMAADP32.ACM	ACM	18944	18828			Windows/
□ ✓ 12			Y				MSADP32.ACM	MSADP32.ACM	ACM	17920	18831			Windows/
□ ✓ 13			Y				MSGSM32.ACM	MSGSM32.ACM	ACM	25088	18834			Windows/
□ ✓ 14										04	18838			Windows/
□ ✓ 15										288	24307			Windows/
□ ✗ 16	Y									4288	24309			Windows/
□ ✗ 17	Y									104	24334			Windows/
□ ✓ 18										7088	24340			Windows/
□ ✓ 19										816	24367			Windows/

File Search

Files
● Entire
○ Selected Files

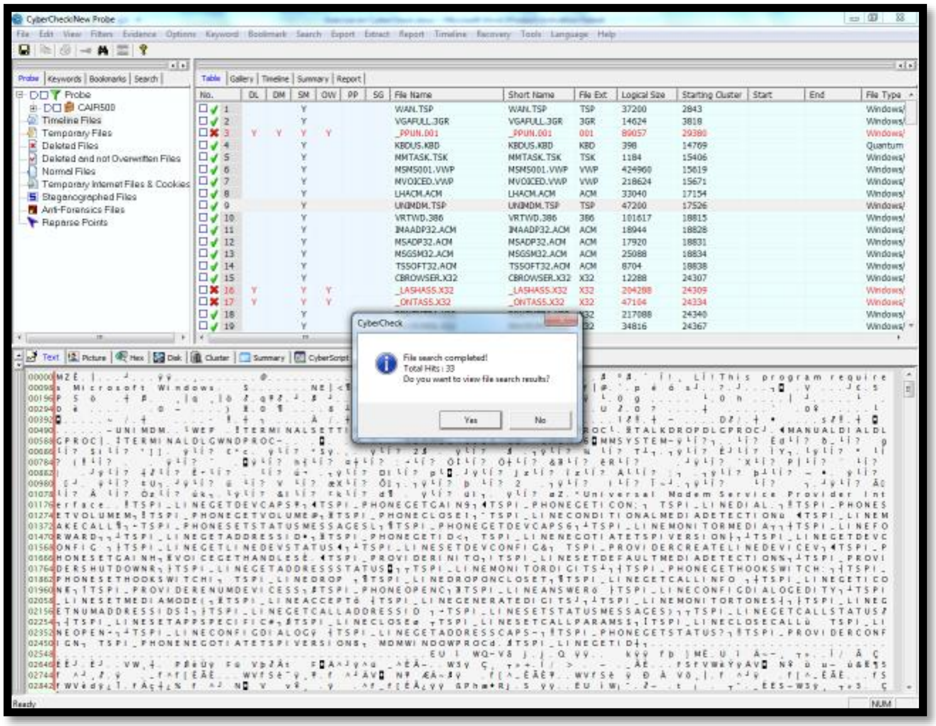
Search By
● File Types
☑ Document Files
□ Image Files
□ Audio Files
□ Video Files
○ File Hash
Select algorithm
○ MD5
○ SHA1
○ SHA256

File Extension: doc;

Note: File hash search will be enabled only if the entire files are hashed using any hash algorithm.

OK   Cancel

After specifying the File Types to be searched, click the **OK** button. On clicking the **OK** button, a progress bar will be displayed to indicate the progress of the search process. A message box will be displayed after the completion of search process. Click **Yes** to view the search results



CyberCheck\New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
Probe
CAIR500
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Ready
NUM

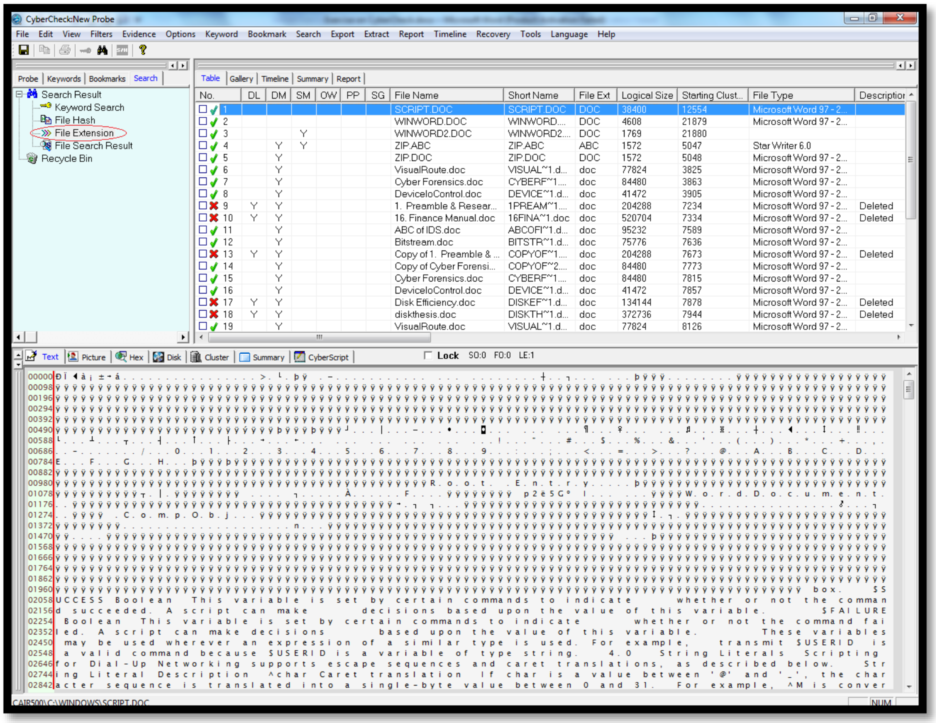
No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
□ ✓ 1			Y				WAN.TSP	WAN.TSP	TSP	37200	2843			Windows/
□ ✓ 2			Y				VGAFULL.3GR	VGAFULL.3GR	3GR	14624	3818			Windows/
□ ✗ 3	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows/
□ ✓ 4			Y				KBDUS.KBD	KBDUS.KBD	KBD	398	14769			Quantum
□ ✓ 5			Y				MMTASK.TSK	MMTASK.TSK	TSK	1184	15406			Windows/
□ ✓ 6			Y				MSMS001.VWP	MSMS001.VWP	VWP	424960	15619			Windows/
□ ✓ 7			Y				MVOICED.VWP	MVOICED.VWP	VWP	218624	15671			Windows/
□ ✓ 8			Y				LHACM.ACM	LHACM.ACM	ACM	33040	17154			Windows/
□ ✓ 9			Y				UNIMDM.TSP	UNIMDM.TSP	TSP	47200	17526			Windows/
□ ✓ 10			Y				VRTWD.386	VRTWD.386	386	101617	18815			Windows/
□ ✓ 11			Y				IMAADP32.ACM	IMAADP32.ACM	ACM	18944	18828			Windows/
□ ✓ 12			Y				MSADP32.ACM	MSADP32.ACM	ACM	17920	18831			Windows/
□ ✓ 13			Y				MSGSM32.ACM	MSGSM32.ACM	ACM	25088	18834			Windows/
□ ✓ 14			Y				TSSOFT32.ACM	TSSOFT32.ACM	ACM	8704	18838			Windows/
□ ✓ 15			Y				CBROWSER.X32	CBROWSER.X32	X32	12288	24307			Windows/
□ ✗ 16	Y		Y	Y			_LASHASS.X32	_LASHASS.X32	X32	204288	24309			Windows/
□ ✗ 17	Y		Y	Y			_ONTASS.X32	_ONTASS.X32	X32	47104	24334			Windows/
□ ✓ 18			Y				[illegible]	[illegible]	[illegible]	217088	24340			Windows/
□ ✓ 19			Y				[illegible]	[illegible]	[illegible]	34816	24367			Windows/

CyberCheck

File search completed!
Total Hits : 33
Do you want to view file search results?

Yes No

The files that match with the specified extensions will be displayed. Click on a file to view the content in the bottom pane. This set of files will be available in the **File Extension** folder in the **Search** Tab view, till it is replaced by the result of another File Search.


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe | Keywords | Bookmarks | Search
Search Result
Keyword Search
File Hash
File Extension
File Search Result
Recycle Bin
Table | Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
□ Lock S0:0 F0:0 LE:1
NUM

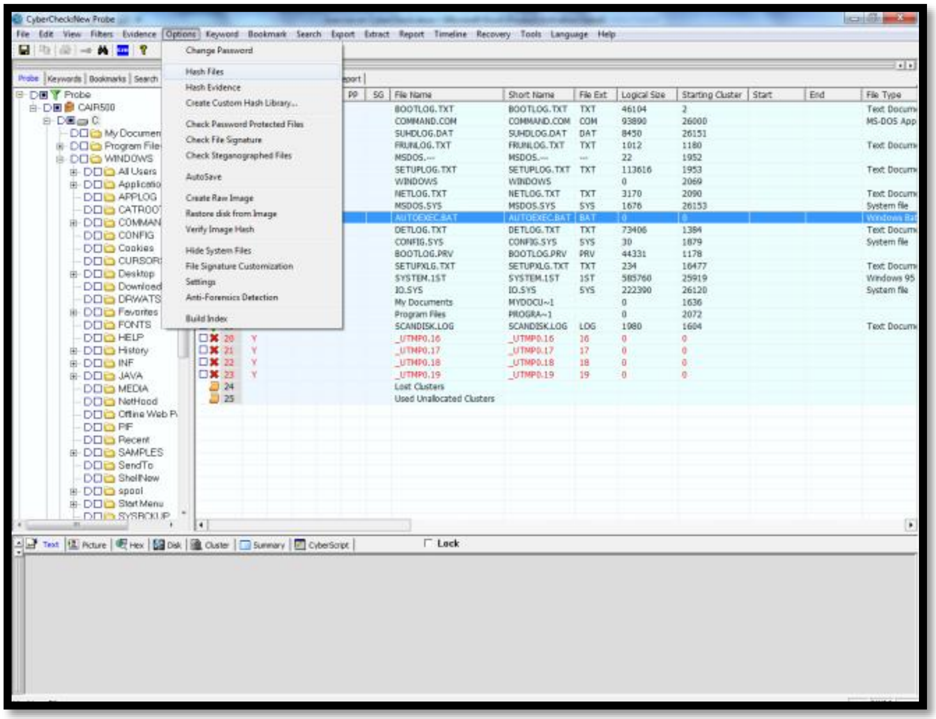
No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Clust...	File Type	Descriptior
□ ✓ 1							SCRIPT.DOC	SCRIPT.DOC	DOC	38400	12554	Microsoft Word 97 - 2...	
□ ✓ 2							WINWORD.DOC	WINWORD....	DOC	4608	21879	Microsoft Word 97 - 2...	
□ ✓ 3			Y				WINWORD2.DOC	WINWORD2....	DOC	1769	21880		
□ ✓ 4		Y	Y				ZIP.ABC	ZIP.ABC	ABC	1572	5047	Star Writer 6.0	
□ ✓ 5		Y					ZIP.DOC	ZIP.DOC	DOC	1572	5048	Microsoft Word 97 - 2...	
□ ✓ 6		Y					VisualRoute.doc	VISUAL~1.d...	doc	77824	3825	Microsoft Word 97 - 2...	
□ ✓ 7		Y					Cyber Forensics.doc	CYBERF~1....	doc	84480	3863	Microsoft Word 97 - 2...	
□ ✓ 8		Y					DeviceloControl.doc	DEVICE~1.d...	doc	41472	3905	Microsoft Word 97 - 2...	
□ ✗ 9	Y	Y					1. Preamble & Resear...	1PREAM~1....	doc	204288	7234	Microsoft Word 97 - 2...	Deleted
□ ✗ 10	Y	Y					16. Finance Manual.doc	16FINA~1.doc	doc	520704	7334	Microsoft Word 97 - 2...	Deleted
□ ✓ 11		Y					ABC of IDS.doc	ABCOFI~1.d...	doc	95232	7589	Microsoft Word 97 - 2...	
□ ✓ 12		Y					Bitstream.doc	BITSTR~1.d...	doc	75776	7636	Microsoft Word 97 - 2...	
□ ✗ 13	Y	Y					Copy of 1. Preamble & ...	COPYOF~1....	doc	204288	7673	Microsoft Word 97 - 2...	Deleted
□ ✓ 14		Y					Copy of Cyber Forensi...	COPYOF~2....	doc	84480	7773	Microsoft Word 97 - 2...	
□ ✓ 15		Y					Cyber Forensics.doc	CYBERF~1....	doc	84480	7815	Microsoft Word 97 - 2...	
□ ✓ 16		Y					DeviceloControl.doc	DEVICE~1.d...	doc	41472	7857	Microsoft Word 97 - 2...	
□ ✗ 17	Y	Y					Disk Efficiency.doc	DISKEF~1.d...	doc	134144	7878	Microsoft Word 97 - 2...	Deleted
□ ✗ 18	Y	Y					diskthesis.doc	DISKTH~1.d...	doc	372736	7944	Microsoft Word 97 - 2...	Deleted
□ ✓ 19		Y					VisualRoute.doc	VISUAL~1.d...	doc	77824	8126	Microsoft Word 97 - 2...	

```
02058 UCCESS Boolean  This variable is set by certain commands to indicate    whether or not the comman
02156 d succeeded. A script can make      decisions based upon the value of this variable.      $FAILURE
02254  Boolean  This variable is set by certain commands to indicate      whether or not the command fai
02352 led. A script can make decisions      based upon the value of this variable.     These variables
02450  may be used wherever an expression of a similar type is used. For example,   transmit $USERID is
02548  a valid command because $USERID is a variable of type string.   4.0   String Literals  Scripting
02646 for Dial-Up Networking supports escape sequences and caret translations, as described below.    Str
02744 ing Literal Description  ^char Caret translation  If char is a value between '@' and '_', the char
02842 acter sequence is translated into a single-byte value between 0 and 31.  For example, ^M is conver
```

CAIR500\C:\WINDOWS\SCRIPT.DOC

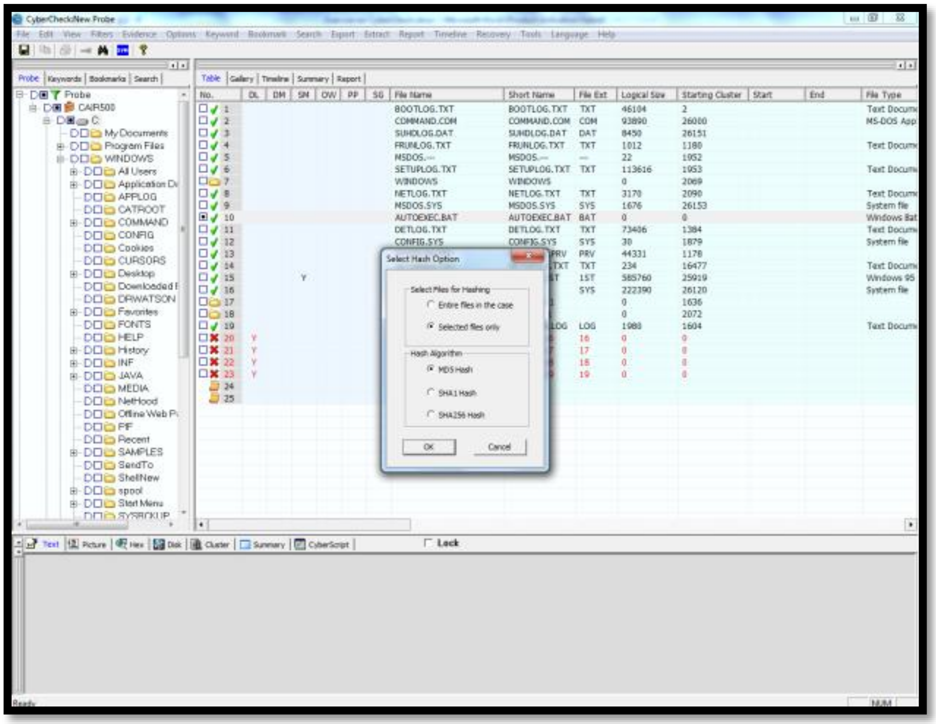
Task 15: How can you find out the hash value of a file from CyberCheck?

Solution: To take the hash values of a selected file, select the file by clicking the check box of the desired file and choose the Options >> Hash Files from the main menu.



PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
		BOOTLOG.TXT	BOOTLOG.TXT	TXT	46104	2			Text Docum
		COMMAND.COM	COMMAND.COM	COM	93890	26000			MS-DOS App
		SUHDLOG.DAT	SUHDLOG.DAT	DAT	8450	26151			
		FRUNLOG.TXT	FRUNLOG.TXT	TXT	1012	1180			Text Docum
		MSDOS.---	MSDOS.---	---	22	1952			
		SETUPLOG.TXT	SETUPLOG.TXT	TXT	113616	1953			Text Docum
		WINDOWS	WINDOWS		0	2069			
		NETLOG.TXT	NETLOG.TXT	TXT	3170	2090			Text Docum
		MSDOS.SYS	MSDOS.SYS	SYS	1676	26153			System file
		AUTOEXEC.BAT	AUTOEXEC.BAT	BAT	0	0			Windows Bat
		DETLOG.TXT	DETLOG.TXT	TXT	73406	1384			Text Docum
		CONFIG.SYS	CONFIG.SYS	SYS	30	1879			System file
		BOOTLOG.PRV	BOOTLOG.PRV	PRV	44331	1178			
		SETUPXLG.TXT	SETUPXLG.TXT	TXT	234	16477			Text Docum
		SYSTEM.1ST	SYSTEM.1ST	1ST	585760	25919			Windows 95
		IO.SYS	IO.SYS	SYS	222390	26120			System file
		My Documents	MYDOCU~1		0	1636			
		Program Files	PROGRA~1		0	2072			
		SCANDISK.LOG	SCANDISK.LOG	LOG	1980	1604			Text Docum
		_UTMP0.16	_UTMP0.16	16	0	0			
		_UTMP0.17	_UTMP0.17	17	0	0			
		_UTMP0.18	_UTMP0.18	18	0	0			
		_UTMP0.19	_UTMP0.19	19	0	0			
		Lost Clusters							
		Used Unallocated Clusters							

Choose ‘Selected’ option in the dialog box that appears and the hashing algorithm. Click OK. If the desired file is not chosen and ‘Selected’ option is clicked a message appears-No file(s)/folder(s) selected. Click on the check box near file(s)/folder(s) to select the desired item(s)”



No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
□ ✓ 1							BOOTLOG.TXT	BOOTLOG.TXT	TXT	46104	2			Text Docum
□ ✓ 2							COMMAND.COM	COMMAND.COM	COM	93890	26080			MS-DOS App
□ ✓ 3							SUHDLOG.DAT	SUHDLOG.DAT	DAT	8450	26151			
□ ✓ 4							FRUNLOG.TXT	FRUNLOG.TXT	TXT	1012	1180			Text Docum
□ ✓ 5							MSDOS.---	MSDOS.---	---	22	1952			
□ ✓ 6							SETUPLOG.TXT	SETUPLOG.TXT	TXT	113616	1953			Text Docum
□ 7							WINDOWS	WINDOWS		0	2069			
□ ✓ 8							NETLOG.TXT	NETLOG.TXT	TXT	3170	2090			Text Docum
□ ✓ 9							MSDOS.SYS	MSDOS.SYS	SYS	1676	26153			System file
▣ ✓ 10							AUTOEXEC.BAT	AUTOEXEC.BAT	BAT	0	0			Windows Bat
□ ✓ 11							DETLOG.TXT	DETLOG.TXT	TXT	73406	1384			Text Docum
□ ✓ 12							CONFIG.SYS	CONFIG.SYS	SYS	30	1879			System file
□ ✓ 13								PRV	PRV	44331	1178			
□ ✓ 14								TXT	TXT	234	16477			Text Docum
□ ✓ 15			Y					T	1ST	585760	25919			Windows 95
□ ✓ 16									SYS	222390	26120			System file
□ 17										0	1636			
□ 18										0	2072			
□ ✓ 19								LOG	LOG	1988	1604			Text Docum
□ ✗ 20	Y								16	0	0			
□ ✗ 21	Y								17	0	0			
□ ✗ 22	Y								18	0	0			
□ ✗ 23	Y								19	0	0			
24														
25														

Select Hash Option

Select Files for Hashing
○ Entire files in the case
● Selected files only

Hash Algorithm
● MD5 Hash
○ SHA1 Hash
○ SHA256 Hash

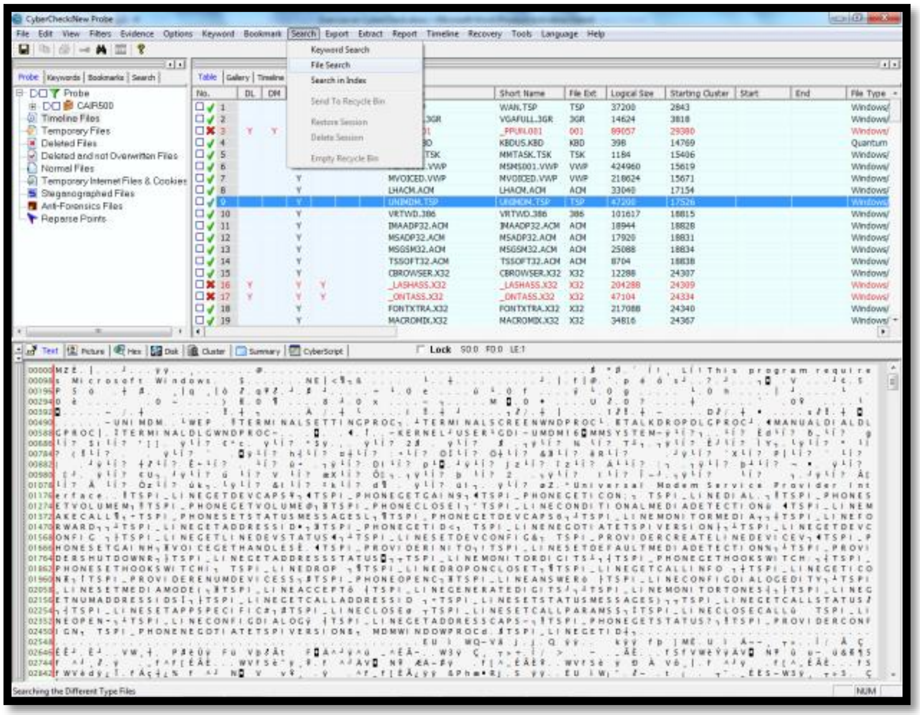
OK Cancel

On completion a message appears- “Hashing of Selected file(s) completed”. Hash value of each file will be added as an attribute of the file. This can be viewed in the Table view at the end of the attribute bar under the column MD5/SHA1 or SHA2 Hash Value in the right pane column.

Task 16: How can you search for files with same hash value?

Solution: On "Table View Tab " Right click any file >> Copy Hash Value .

Then Select Search option from the main menu and then File Search


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Keyword Search
File Search
Search in Index
Send To Recycle Bin
Restore Session
Delete Session
Empty Recycle Bin
Probe Keywords Bookmarks Search
Probe
CAIR500
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline
Text Picture Hex Disk Cluster Summary CyberScript
Lock S0:0 F0:0 LE:1
Searching the Different Type Files
NUM

No.	DL	DM				Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
☐ ✓ 1						WAN.TSP	TSP	37200	2843			Windows/
☐ ✓ 2					.3GR	VGAFULL.3GR	3GR	14624	3818			Windows/
☐ ✗ 3	Y	Y			01	_PPUN.001	001	89057	29380			Windows/
☐ ✓ 4					BD	KBDUS.KBD	KBD	398	14769			Quantum
☐ ✓ 5					.TSK	MMTASK.TSK	TSK	1184	15406			Windows/
☐ ✓ 6					.VWP	MSMS001.VWP	VWP	424960	15619			Windows/
☐ ✓ 7			Y		MVOICED.VWP	MVOICED.VWP	VWP	218624	15671			Windows/
☐ ✓ 8			Y		LHACM.ACM	LHACM.ACM	ACM	33040	17154			Windows/
☐ ✓ 9			Y		UNIMDM.TSP	UNIMDM.TSP	TSP	47200	17526			Windows/
☐ ✓ 10			Y		VRTWD.386	VRTWD.386	386	101617	18815			Windows/
☐ ✓ 11			Y		IMAADP32.ACM	IMAADP32.ACM	ACM	18944	18828			Windows/
☐ ✓ 12			Y		MSADP32.ACM	MSADP32.ACM	ACM	17920	18831			Windows/
☐ ✓ 13			Y		MSGSM32.ACM	MSGSM32.ACM	ACM	25088	18834			Windows/
☐ ✓ 14			Y		TSSOFT32.ACM	TSSOFT32.ACM	ACM	8704	18838			Windows/
☐ ✓ 15			Y		CBROWSER.X32	CBROWSER.X32	X32	12288	24307			Windows/
☐ ✗ 16	Y		Y	Y	_LASHASS.X32	_LASHASS.X32	X32	204288	24309			Windows/
☐ ✗ 17	Y		Y	Y	_ONTASS.X32	_ONTASS.X32	X32	47104	24334			Windows/
☐ ✓ 18			Y		FONTXTRA.X32	FONTXTRA.X32	X32	217088	24340			Windows/
☐ ✓ 19			Y		MACROMIX.X32	MACROMIX.X32	X32	34816	24367			Windows/

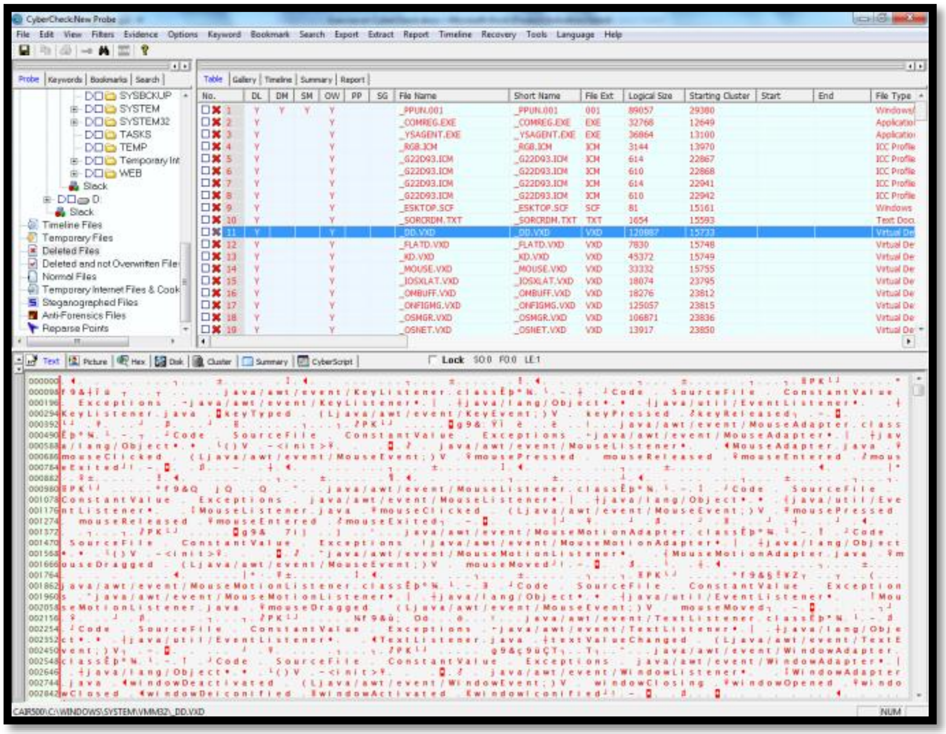
In "File Search" window dialog select the option "File Hash" and select the HASH algorithm. Type or the Paste the Hash value in Text box provided.

Task 17: How can you view all the deleted files in an evidence file?

Solution: Goto "Filter" menu >> Click Deleted files.

Task 18: How can you recover a deleted file?

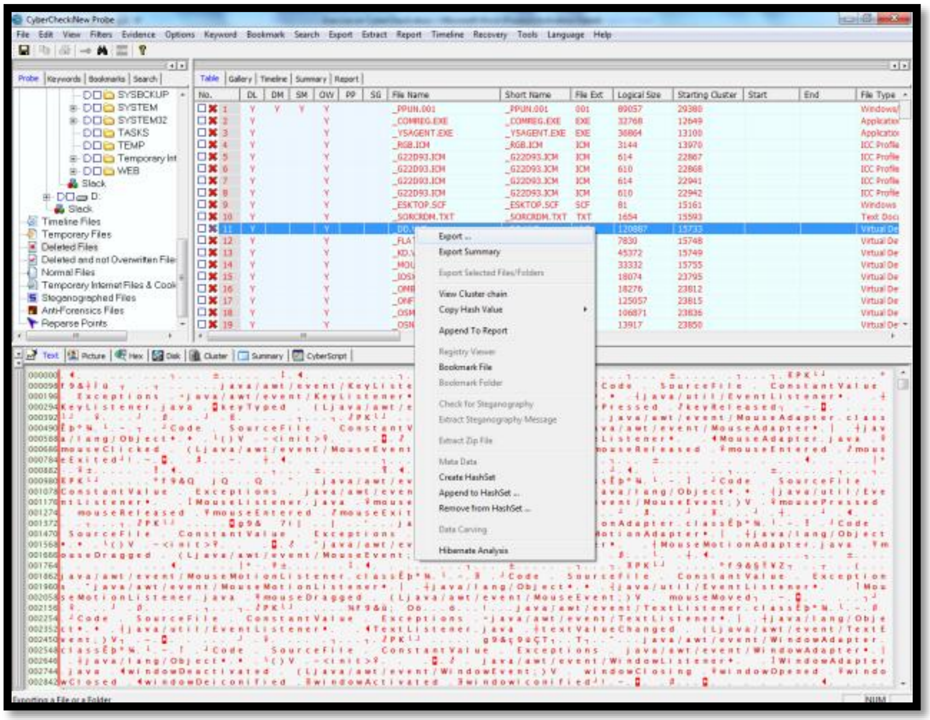
Solution: Select the desired file from the list of deleted files by checking the box of the appropriate file


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten File
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock SO:0 FO:0 LE:1
NUM

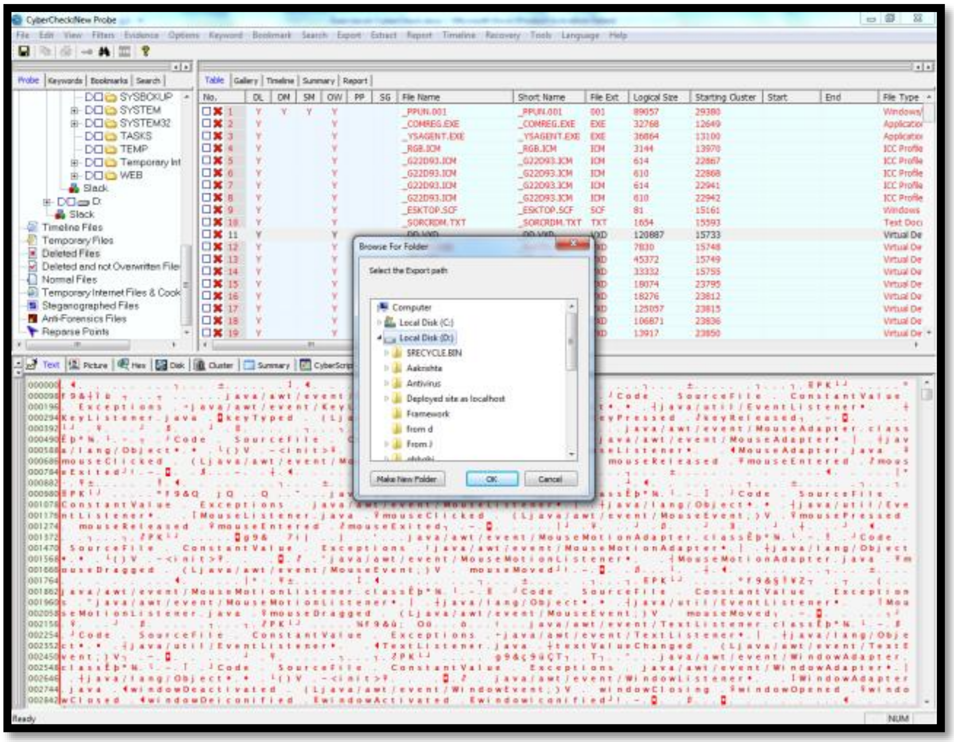
No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows/
2	Y			Y			_COMREG.EXE	_COMREG.EXE	EXE	32768	12649			Applicatio
3	Y			Y			_YSAGENT.EXE	_YSAGENT.EXE	EXE	36864	13100			Applicatio
4	Y			Y			_RGB.ICM	_RGB.ICM	ICM	3144	13970			ICC Profile
5	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	614	22867			ICC Profile
6	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	610	22868			ICC Profile
7	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	614	22941			ICC Profile
8	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	610	22942			ICC Profile
9	Y			Y			_ESKTOP.SCF	_ESKTOP.SCF	SCF	81	15161			Windows
10	Y			Y			_SORCRDM.TXT	_SORCRDM.TXT	TXT	1654	15593			Text Docu
11	Y			Y			_DD.VXD	_DD.VXD	VXD	120887	15733			Virtual De
12	Y			Y			_FLATD.VXD	_FLATD.VXD	VXD	7830	15748			Virtual De
13	Y			Y			_KD.VXD	_KD.VXD	VXD	45372	15749			Virtual De
14	Y			Y			_MOUSE.VXD	_MOUSE.VXD	VXD	33332	15755			Virtual De
15	Y			Y			_IOSXLAT.VXD	_IOSXLAT.VXD	VXD	18074	23795			Virtual De
16	Y			Y			_OMBUFF.VXD	_OMBUFF.VXD	VXD	18276	23812			Virtual De
17	Y			Y			_ONFIGMG.VXD	_ONFIGMG.VXD	VXD	125057	23815			Virtual De
18	Y			Y			_OSMGR.VXD	_OSMGR.VXD	VXD	106871	23836			Virtual De
19	Y			Y			_OSNET.VXD	_OSNET.VXD	VXD	13917	23850			Virtual De

CAIR500\C:\WINDOWS\SYSTEM\VMM32_DD.VXD

Either right click the desired file and select export or select Export|File/Folder



Specify a path into which the selected item is to be exported.



CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe | Keywords | Bookmarks | Search
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table | Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
Ready
NUM

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows/
2	Y			Y			_COMREG.EXE	_COMREG.EXE	EXE	32768	12649			Applicatio
3	Y			Y			_YSAGENT.EXE	_YSAGENT.EXE	EXE	36864	13100			Applicatio
4	Y			Y			_RGB.ICM	_RGB.ICM	ICM	3144	13970			ICC Profile
5	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	614	22867			ICC Profile
6	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	610	22868			ICC Profile
7	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	614	22941			ICC Profile
8	Y			Y			_G22D93.ICM	_G22D93.ICM	ICM	610	22942			ICC Profile
9	Y			Y			_ESKTOP.SCF	_ESKTOP.SCF	SCF	81	15161			Windows
10	Y			Y			_SORCRDM.TXT	_SORCRDM.TXT	TXT	1654	15593			Text Docu
11	Y			Y			DD.VXD	DD.VXD	VXD	120887	15733			Virtual De
12	Y			Y					XD	7830	15748			Virtual De
13	Y			Y					XD	45372	15749			Virtual De
14	Y			Y					XD	33332	15755			Virtual De
15	Y			Y					XD	18074	23795			Virtual De
16	Y			Y					XD	18276	23812			Virtual De
17	Y			Y					XD	125057	23815			Virtual De
18	Y			Y					XD	106871	23836			Virtual De
19	Y			Y					XD	13917	23850			Virtual De

Browse For Folder

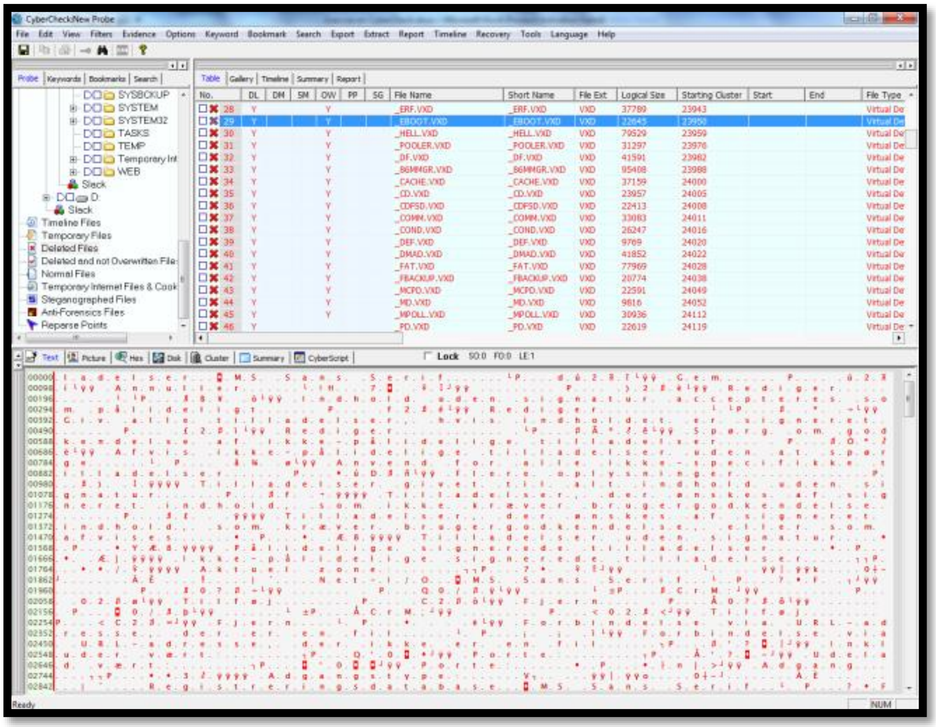
Select the Export path

- Computer
  - Local Disk (C:)
  - Local Disk (D:)
    - $RECYCLE.BIN
    - Aakrishta
    - Antivirus
    - Deployed site as localhost
    - Framework
    - from d
    - From J

Click OK, the item will be exported into the specified path, a message-“Successfully exported” will be displayed showing the path to which the file is exported.

Task 19: How can you recover a deleted folder?

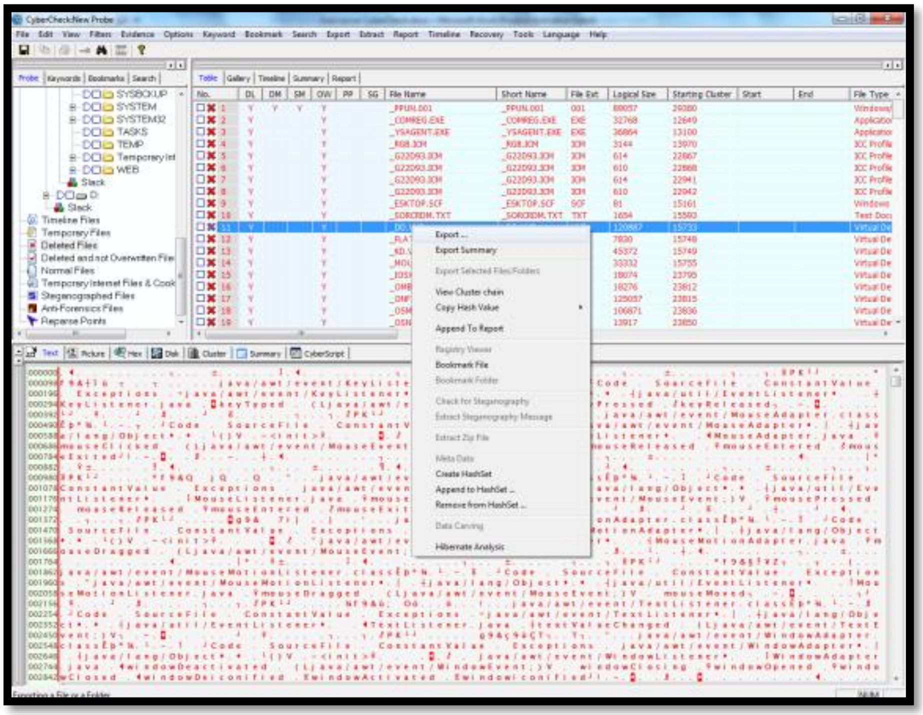
Solution: Select the desired folder from the list of deleted files by checking the box of the appropriate folder.



CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe | Keywords | Bookmarks | Search
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table | Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
Lock SO:0 FO:0 LE:1
Ready
NUM

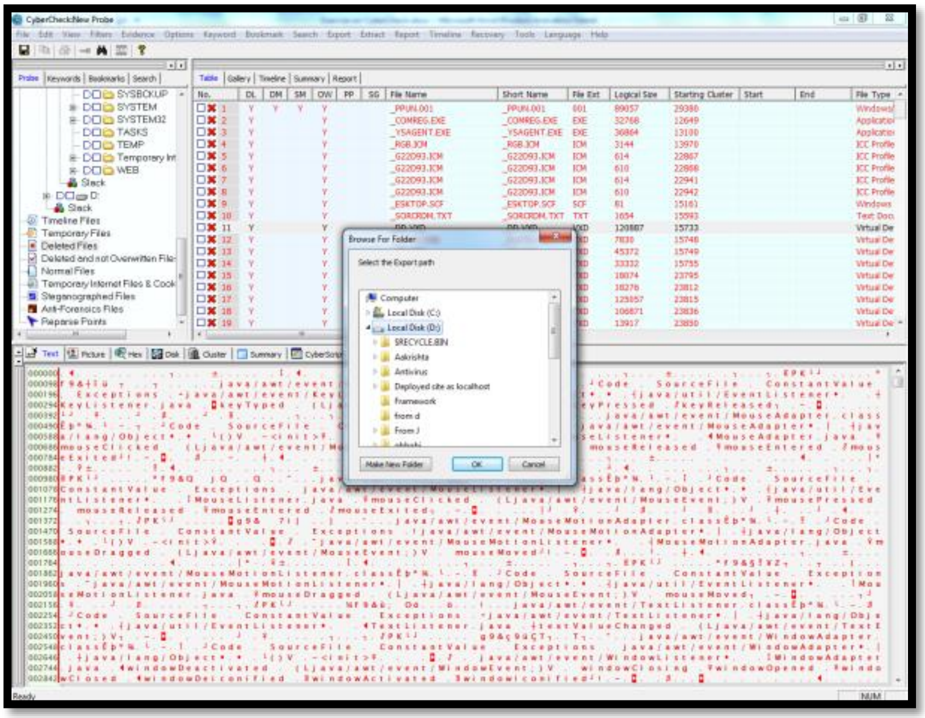
No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
28	Y			Y			_ERF.VXD	_ERF.VXD	VXD	37789	23943			Virtual De
29	Y			Y			_EBOOT.VXD	_EBOOT.VXD	VXD	22645	23950			Virtual De
30	Y			Y			_HELL.VXD	_HELL.VXD	VXD	79529	23959			Virtual De
31	Y			Y			_POOLER.VXD	_POOLER.VXD	VXD	31297	23976			Virtual De
32	Y			Y			_DF.VXD	_DF.VXD	VXD	41591	23982			Virtual De
33	Y			Y			_B6MMGR.VXD	_B6MMGR.VXD	VXD	95408	23988			Virtual De
34	Y			Y			_CACHE.VXD	_CACHE.VXD	VXD	37159	24000			Virtual De
35	Y			Y			_CD.VXD	_CD.VXD	VXD	23957	24005			Virtual De
36	Y			Y			_CDFSD.VXD	_CDFSD.VXD	VXD	22413	24008			Virtual De
37	Y			Y			_COMM.VXD	_COMM.VXD	VXD	33083	24011			Virtual De
38	Y			Y			_COND.VXD	_COND.VXD	VXD	26247	24016			Virtual De
39	Y			Y			_DEF.VXD	_DEF.VXD	VXD	9769	24020			Virtual De
40	Y			Y			_DMAD.VXD	_DMAD.VXD	VXD	41852	24022			Virtual De
41	Y			Y			_FAT.VXD	_FAT.VXD	VXD	77969	24028			Virtual De
42	Y			Y			_FBACKUP.VXD	_FBACKUP.VXD	VXD	20774	24038			Virtual De
43	Y			Y			_MCPD.VXD	_MCPD.VXD	VXD	22591	24049			Virtual De
44	Y			Y			_MD.VXD	_MD.VXD	VXD	9816	24052			Virtual De
45	Y			Y			_MPOLL.VXD	_MPOLL.VXD	VXD	30936	24112			Virtual De
46	Y						_PD.VXD	_PD.VXD	VXD	22619	24119			Virtual De

Either right click the desired folder and select export or select Export|File/Folder



No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows
2	Y			Y			_COMREG.EXE	_COMREG.EXE	EXE	32768	12649			Applicatio
3	Y			Y			_YSAGENT.EXE	_YSAGENT.EXE	EXE	36864	13100			Applicatio
4	Y			Y			_RGB.ICM	_RGB.ICM	ICM	3144	13970			ICC Profile
5	Y			Y			_G22093.ICM	_G22093.ICM	ICM	614	22867			ICC Profile
6	Y			Y			_G22093.ICM	_G22093.ICM	ICM	610	22868			ICC Profile
7	Y			Y			_G22093.ICM	_G22093.ICM	ICM	614	22941			ICC Profile
8	Y			Y			_G22093.ICM	_G22093.ICM	ICM	610	22942			ICC Profile
9	Y			Y			_ESKTOP.SCF	_ESKTOP.SCF	SCF	81	15161			Windows
10	Y			Y			_SORCRDM.TXT	_SORCRDM.TXT	TXT	1654	15583			Text Doc
11	Y			Y			DD.\			120687	15733			Virtual De
12	Y			Y			_RAT			7830	15748			Virtual De
13	Y			Y			_KD.\			45372	15749			Virtual De
14	Y			Y			_MOU			33332	15755			Virtual De
15	Y			Y			_IOSK			18074	23795			Virtual De
16	Y			Y			_OMB			18276	23812			Virtual De
17	Y			Y			_ONF			125037	23815			Virtual De
18	Y			Y			_OSM			106871	23836			Virtual De
19	Y			Y			_OSN			13917	23850			Virtual De

Specify a path into which the selected item is to be exported.

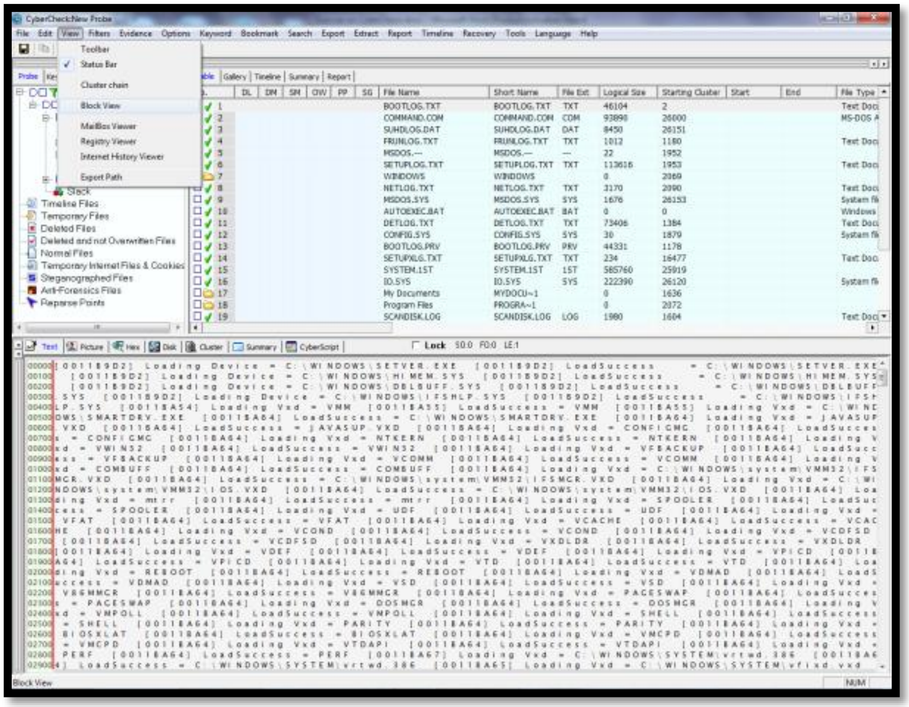

CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe | Keywords | Bookmarks | Search
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten File
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table | Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
Browse For Folder
Select the Export path
Computer
Local Disk (C:)
Local Disk (D:)
$RECYCLE.BIN
Aakrishta
Antivirus
Deployed site as localhost
Framework
from d
From J
Make New Folder
OK
Cancel
Ready
NUM

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1	Y	Y	Y	Y			_PPUN.001	_PPUN.001	001	89057	29380			Windows
2	Y			Y			_COMREG.EXE	_COMREG.EXE	EXE	32768	12649			Applicatio
3	Y			Y			_YSAGENT.EXE	_YSAGENT.EXE	EXE	36864	13100			Applicatio
4	Y			Y			_RGB.ICM	_RGB.ICM	ICM	3144	13970			ICC Profile
5	Y			Y			_G22093.ICM	_G22093.ICM	ICM	614	22867			ICC Profile
6	Y			Y			_G22093.ICM	_G22093.ICM	ICM	610	22868			ICC Profile
7	Y			Y			_G22093.ICM	_G22093.ICM	ICM	614	22941			ICC Profile
8	Y			Y			_G22093.ICM	_G22093.ICM	ICM	610	22942			ICC Profile
9	Y			Y			_ESKTOP.SCF	_ESKTOP.SCF	SCF	81	15161			Windows
10	Y			Y			_SORCRDM.TXT	_SORCRDM.TXT	TXT	1654	15593			Text Doc
11	Y			Y			[illegible]	[illegible]	VHD	120887	15733			Virtual De
12	Y			Y			[illegible]	[illegible]	[illegible]	7830	15748			Virtual De
13	Y			Y			[illegible]	[illegible]	[illegible]	45372	15749			Virtual De
14	Y			Y			[illegible]	[illegible]	[illegible]	33332	15755			Virtual De
15	Y			Y			[illegible]	[illegible]	[illegible]	18074	23795			Virtual De
16	Y			Y			[illegible]	[illegible]	[illegible]	18276	23812			Virtual De
17	Y			Y			[illegible]	[illegible]	[illegible]	125857	23815			Virtual De
18	Y			Y			[illegible]	[illegible]	[illegible]	106871	23836			Virtual De
19	Y			Y			[illegible]	[illegible]	[illegible]	13917	23850			Virtual De

Click OK, the item will be exported into the specified path, a message-“Successfully exported” will be displayed showing the path to which the file is exported

Task 20: What is the information available in Block view?

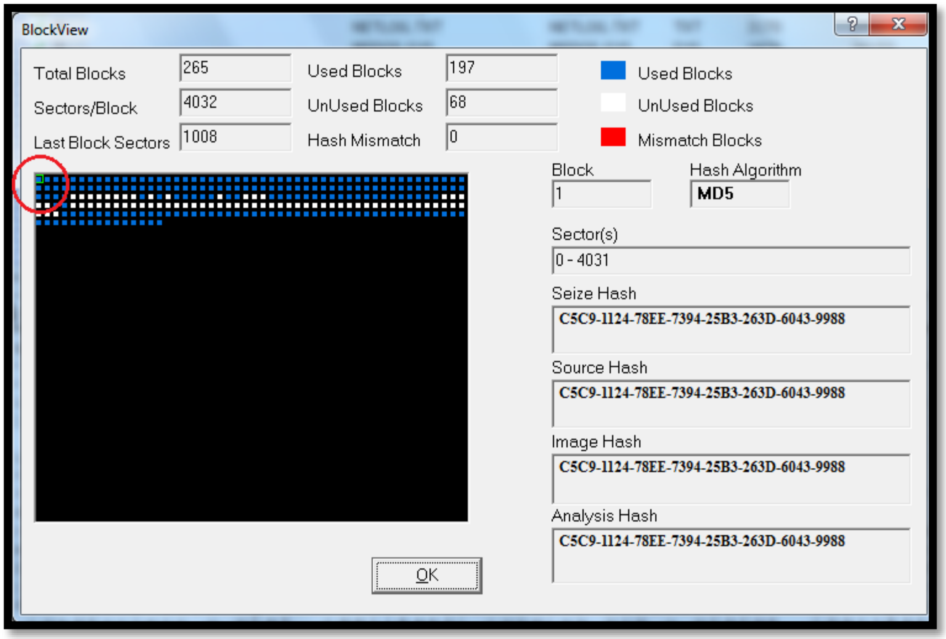
Solution: Block view is the block-by-block representation of the entire evidence file. Select View|Block View to display the blocks.


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Toolbar
✓ Status Bar
Cluster chain
Block View
MailBox Viewer
Registry Viewer
Internet History Viewer
Export Path
Probe
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
Lock S0:0 F0:0 LE:1
Block View
NUM

	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
✓ 1							BOOTLOG.TXT	BOOTLOG.TXT	TXT	46104	2			Text Doc
✓ 2							COMMAND.COM	COMMAND.COM	COM	93890	26000			MS-DOS A
✓ 3							SUHDLOG.DAT	SUHDLOG.DAT	DAT	8450	26151			
✓ 4							FRUNLOG.TXT	FRUNLOG.TXT	TXT	1012	1180			Text Doc
✓ 5							MSDOS.---	MSDOS.---	---	22	1952			
✓ 6							SETUPLOG.TXT	SETUPLOG.TXT	TXT	113616	1953			Text Doc
7							WINDOWS	WINDOWS		0	2069			
✓ 8							NETLOG.TXT	NETLOG.TXT	TXT	3170	2090			Text Doc
☐ ✓ 9							MSDOS.SYS	MSDOS.SYS	SYS	1676	26153			System fil
☐ ✓ 10							AUTOEXEC.BAT	AUTOEXEC.BAT	BAT	0	0			Windows
☐ ✓ 11							DETLOG.TXT	DETLOG.TXT	TXT	73406	1384			Text Doc
☐ ✓ 12							CONFIG.SYS	CONFIG.SYS	SYS	30	1879			System fil
☐ ✓ 13							BOOTLOG.PRV	BOOTLOG.PRV	PRV	44331	1178			
☐ ✓ 14							SETUPXLG.TXT	SETUPXLG.TXT	TXT	234	16477			Text Doc
☐ ✓ 15							SYSTEM.1ST	SYSTEM.1ST	1ST	585760	25919			
☐ ✓ 16							IO.SYS	IO.SYS	SYS	222390	26120			System fil
☐ 17							My Documents	MYDOCU~1		0	1636			
☐ 18							Program Files	PROGRA~1		0	2072			
☐ ✓ 19							SCANDISK.LOG	SCANDISK.LOG	LOG	1980	1604			Text Doc

```
00000[001189D2] Loading Device = C:\WINDOWS\SETVER.EXE [001189D2] LoadSuccess = C:\WINDOWS\SETVER.EXE
00100  [001189D2] Loading Device = C:\WINDOWS\HIMEM.SYS [001189D2] LoadSuccess = C:\WINDOWS\HIMEM.SYS
00200  [001189D2] Loading Device = C:\WINDOWS\DBLBUFF.SYS [001189D2] LoadSuccess = C:\WINDOWS\DBLBUFF
00300.SYS [001189D2] Loading Device = C:\WINDOWS\IFSHLP.SYS [001189D2] LoadSuccess = C:\WINDOWS\IFSH
00400LP.SYS [00118A54] Loading Vxd = VMM [00118A55] LoadSuccess = VMM [00118A55] Loading Vxd = C:\WIND
00500OWS\SMARTDRV.EXE [00118A64] LoadSuccess = C:\WINDOWS\SMARTDRV.EXE [00118A64] Loading Vxd = JAVASUP
00600.VXD [00118A64] LoadSuccess = JAVASUP.VXD [00118A64] Loading Vxd = CONFIGMG [00118A64] LoadSucces
00700s = CONFIGMG [00118A64] Loading Vxd = NTKERN [00118A64] LoadSuccess = NTKERN [00118A64] Loading V
00800xd = VWIN32 [00118A64] LoadSuccess = VWIN32 [00118A64] Loading Vxd = VFBACKUP [00118A64] LoadSucc
00900ess = VFBACKUP [00118A64] Loading Vxd = VCOMM [00118A64] LoadSuccess = VCOMM [00118A64] Loading V
01000xd = COMBUFF [00118A64] LoadSuccess = COMBUFF [00118A64] Loading Vxd = C:\WINDOWS\system\VMM32\IFS
01100MGR.VXD [00118A64] LoadSuccess = C:\WINDOWS\system\VMM32\IFSMGR.VXD [00118A64] Loading Vxd = C:\WI
01200NDOWS\system\VMM32\IOS.VXD [00118A64] LoadSuccess = C:\WINDOWS\system\VMM32\IOS.VXD [00118A64] Loa
01300ding Vxd = mtrr [00118A64] LoadSuccess = mtrr [00118A64] Loading Vxd = SPOOLER [00118A64] LoadSuc
01400cess = SPOOLER [00118A64] Loading Vxd = UDF [00118A64] LoadSuccess = UDF [00118A64] Loading Vxd =
01500 VFAT [00118A64] LoadSuccess = VFAT [00118A64] Loading Vxd = VCACHE [00118A64] LoadSuccess = VCAC
01600HE [00118A64] Loading Vxd = VCOND [00118A64] LoadSuccess = VCOND [00118A64] Loading Vxd = VCDFSD
01700 [00118A64] LoadSuccess = VCDFSD [00118A64] Loading Vxd = VXDLDR [00118A64] LoadSuccess = VXDLDR
01800[00118A64] Loading Vxd = VDEF [00118A64] LoadSuccess = VDEF [00118A64] Loading Vxd = VPICD [00118
01900A64] LoadSuccess = VPICD [00118A64] Loading Vxd = VTD [00118A64] LoadSuccess = VTD [00118A64] Loa
02000ding Vxd = REBOOT [00118A64] LoadSuccess = REBOOT [00118A64] Loading Vxd = VDMAD [00118A64] LoadS
02100uccess = VDMAD [00118A64] Loading Vxd = VSD [00118A64] LoadSuccess = VSD [00118A64] Loading Vxd =
02200 V86MMGR [00118A64] LoadSuccess = V86MMGR [00118A64] Loading Vxd = PAGESWAP [00118A64] LoadSucces
02300s = PAGESWAP [00118A64] Loading Vxd = DOSMGR [00118A64] LoadSuccess = DOSMGR [00118A64] Loading V
02400xd = VMPOLL [00118A64] LoadSuccess = VMPOLL [00118A64] Loading Vxd = SHELL [00118A64] LoadSuccess
02500 = SHELL [00118A64] Loading Vxd = PARITY [00118A64] LoadSuccess = PARITY [00118A64] Loading Vxd =
02600 BIOSXLAT [00118A64] LoadSuccess = BIOSXLAT [00118A64] Loading Vxd = VMCPD [00118A64] LoadSuccess
02700 = VMCPD [00118A64] Loading Vxd = VTDAPI [00118A64] LoadSuccess = VTDAPI [00118A64] Loading Vxd =
02800 PERF [00118A64] LoadSuccess = PERF [00118A67] Loading Vxd = C:\WINDOWS\SYSTEM\vrtwd.386 [00118A6
029004] LoadSuccess = C:\WINDOWS\SYSTEM\vrtwd.386 [00118A65] Loading Vxd = C:\WINDOWS\SYSTEM\vfixd.vxd
```

The blocks are displayed in three different colors representing: Blue - Used Blocks, White – Unused blocks and Red – Mismatched blocks. Information like total blocks, sectors per block, last block sector, used blocks, unused blocks and the number of blocks with hash mismatch are shown in the boxes provided. When a block is selected in the block view the corresponding block number, sectors in that block, seize hash, source hash, image hash and analysis hash are displayed.

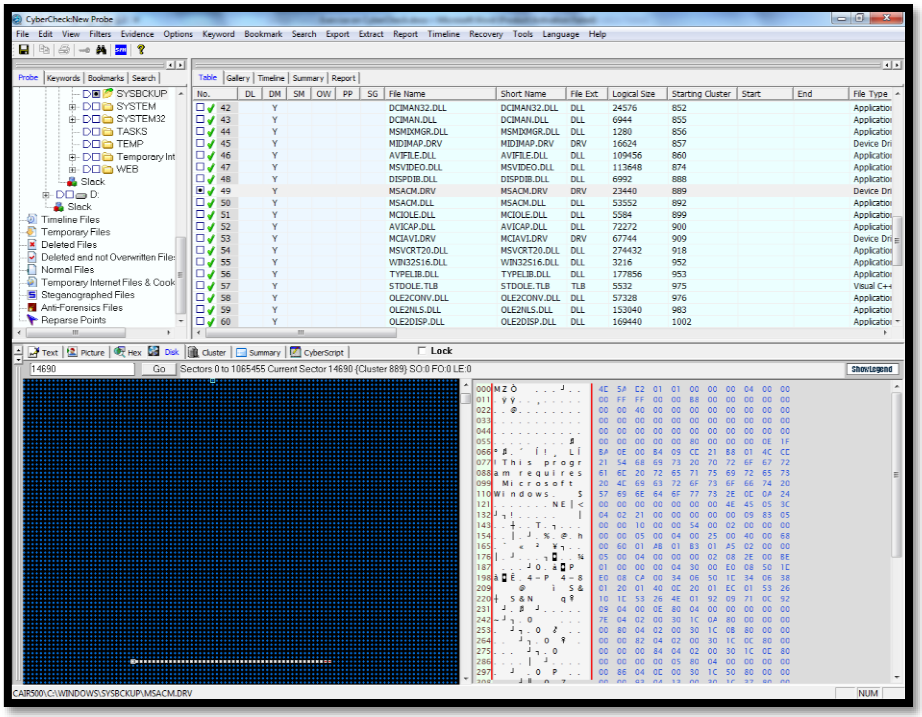


Total Blocks: 265
Sectors/Block: 4032
Last Block Sectors: 1008
Used Blocks: 197
UnUsed Blocks: 68
Hash Mismatch: 0
Block: 1
Hash Algorithm: MD5
Sector(s): 0 - 4031
Seize Hash: C5C9-1124-78EE-7394-25B3-263D-6043-9988
Source Hash: C5C9-1124-78EE-7394-25B3-263D-6043-9988
Image Hash: C5C9-1124-78EE-7394-25B3-263D-6043-9988
Analysis Hash: C5C9-1124-78EE-7394-25B3-263D-6043-9988

The selected block will be highlighted as a green square in the block view.

Task 21: How do you view the sectors allocated to a particular file?

Solution: To view the sectors allocated to particular file, select the file and click the Disk view in the bottom pane. The blocks highlighted in white are the sectors allocated to the selected file.



CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe | Keywords | Bookmarks | Search
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table | Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
Lock
Go
ShowLegend
NUM

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
□ ✓ 42		Y					DCIMAN32.DLL	DCIMAN32.DLL	DLL	24576	852			Applicatio
□ ✓ 43		Y					DCIMAN.DLL	DCIMAN.DLL	DLL	6944	855			Applicatio
□ ✓ 44		Y					MSMIXMGR.DLL	MSMIXMGR.DLL	DLL	1280	856			Applicatio
□ ✓ 45		Y					MIDIMAP.DRV	MIDIMAP.DRV	DRV	16624	857			Device Dri
□ ✓ 46		Y					AVIFILE.DLL	AVIFILE.DLL	DLL	109456	860			Applicatio
□ ✓ 47		Y					MSVIDEO.DLL	MSVIDEO.DLL	DLL	113648	874			Applicatio
□ ✓ 48		Y					DISPDIB.DLL	DISPDIB.DLL	DLL	6992	888			Applicatio
● ✓ 49		Y					MSACM.DRV	MSACM.DRV	DRV	23440	889			Device Dri
□ ✓ 50		Y					MSACM.DLL	MSACM.DLL	DLL	53552	892			Applicatio
□ ✓ 51		Y					MCIOLE.DLL	MCIOLE.DLL	DLL	5584	899			Applicatio
□ ✓ 52		Y					AVICAP.DLL	AVICAP.DLL	DLL	72272	900			Applicatio
□ ✓ 53		Y					MCIAVI.DRV	MCIAVI.DRV	DRV	67744	909			Device Dri
□ ✓ 54		Y					MSVCRT20.DLL	MSVCRT20.DLL	DLL	274432	918			Applicatio
□ ✓ 55		Y					WIN32S16.DLL	WIN32S16.DLL	DLL	3216	952			Applicatio
□ ✓ 56		Y					TYPELIB.DLL	TYPELIB.DLL	DLL	177856	953			Applicatio
□ ✓ 57		Y					STDOLE.TLB	STDOLE.TLB	TLB	5532	975			Visual C++
□ ✓ 58		Y					OLE2CONV.DLL	OLE2CONV.DLL	DLL	57328	976			Applicatio
□ ✓ 59		Y					OLE2NLS.DLL	OLE2NLS.DLL	DLL	153040	983			Applicatio
□ ✓ 60		Y					OLE2DISP.DLL	OLE2DISP.DLL	DLL	169440	1002			Applicatio

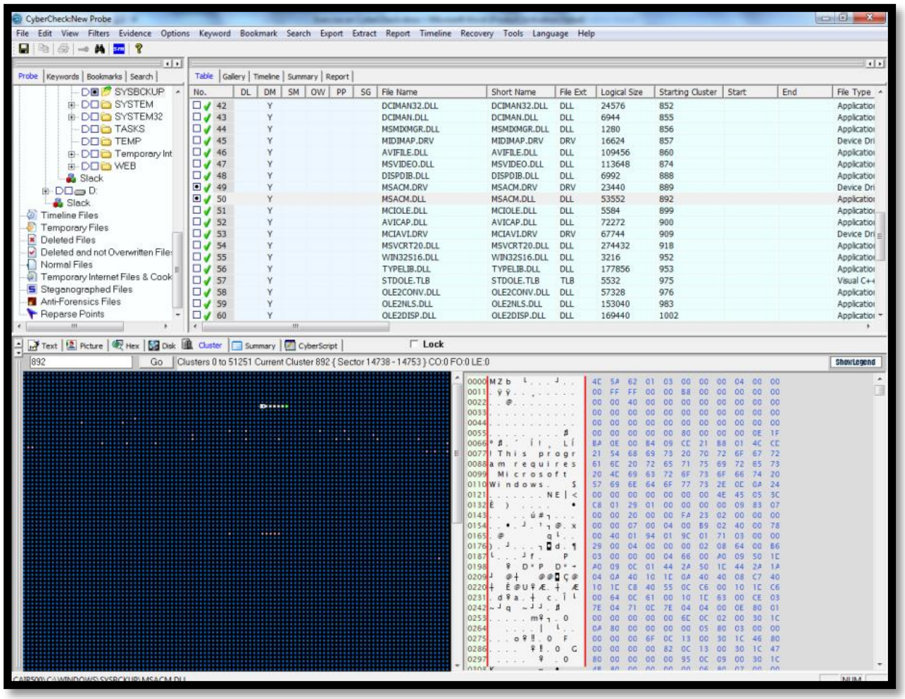
14690

Sectors 0 to 1065455 Current Sector 14690 {Cluster 889} SO:0 FO:0 LE:0

CAIR500\C:\WINDOWS\SYSBCKUP\MSACM.DRV

Task 22: How do you view the clusters allocated to a particular file?

Solution: Select the particular file and then click the Cluster view in the bottom pane. The blocks highlighted in white are the clusters allocated for the file.



No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
□ ✓ 42		Y					DCIMAN32.DLL	DCIMAN32.DLL	DLL	24576	852			Applicatio
□ ✓ 43		Y					DCIMAN.DLL	DCIMAN.DLL	DLL	6944	855			Applicatio
□ ✓ 44		Y					MSMIXMGR.DLL	MSMIXMGR.DLL	DLL	1280	856			Applicatio
□ ✓ 45		Y					MIDIMAP.DRV	MIDIMAP.DRV	DRV	16624	857			Device Dri
□ ✓ 46		Y					AVIFILE.DLL	AVIFILE.DLL	DLL	109456	860			Applicatio
□ ✓ 47		Y					MSVIDEO.DLL	MSVIDEO.DLL	DLL	113648	874			Applicatio
□ ✓ 48		Y					DISPDIB.DLL	DISPDIB.DLL	DLL	6992	888			Applicatio
☒ ✓ 49		Y					MSACM.DRV	MSACM.DRV	DRV	23440	889			Device Dri
☒ ✓ 50		Y					MSACM.DLL	MSACM.DLL	DLL	53552	892			Applicatio
□ ✓ 51		Y					MCIOLE.DLL	MCIOLE.DLL	DLL	5584	899			Applicatio
□ ✓ 52		Y					AVICAP.DLL	AVICAP.DLL	DLL	72272	900			Applicatio
□ ✓ 53		Y					MCIAVI.DRV	MCIAVI.DRV	DRV	67744	909			Device Dri
□ ✓ 54		Y					MSVCRT20.DLL	MSVCRT20.DLL	DLL	274432	918			Applicatio
□ ✓ 55		Y					WIN32S16.DLL	WIN32S16.DLL	DLL	3216	952			Applicatio
□ ✓ 56		Y					TYPELIB.DLL	TYPELIB.DLL	DLL	177856	953			Applicatio
□ ✓ 57		Y					STDOLE.TLB	STDOLE.TLB	TLB	5532	975			Visual C++
□ ✓ 58		Y					OLE2CONV.DLL	OLE2CONV.DLL	DLL	57328	976			Applicatio
□ ✓ 59		Y					OLE2NLS.DLL	OLE2NLS.DLL	DLL	153040	983			Applicatio
□ ✓ 60		Y					OLE2DISP.DLL	OLE2DISP.DLL	DLL	169440	1002			Applicatio

892 Go Clusters 0 to 51251 Current Cluster 892 { Sector 14738 - 14753 } CO:0 FO:0 LE:0

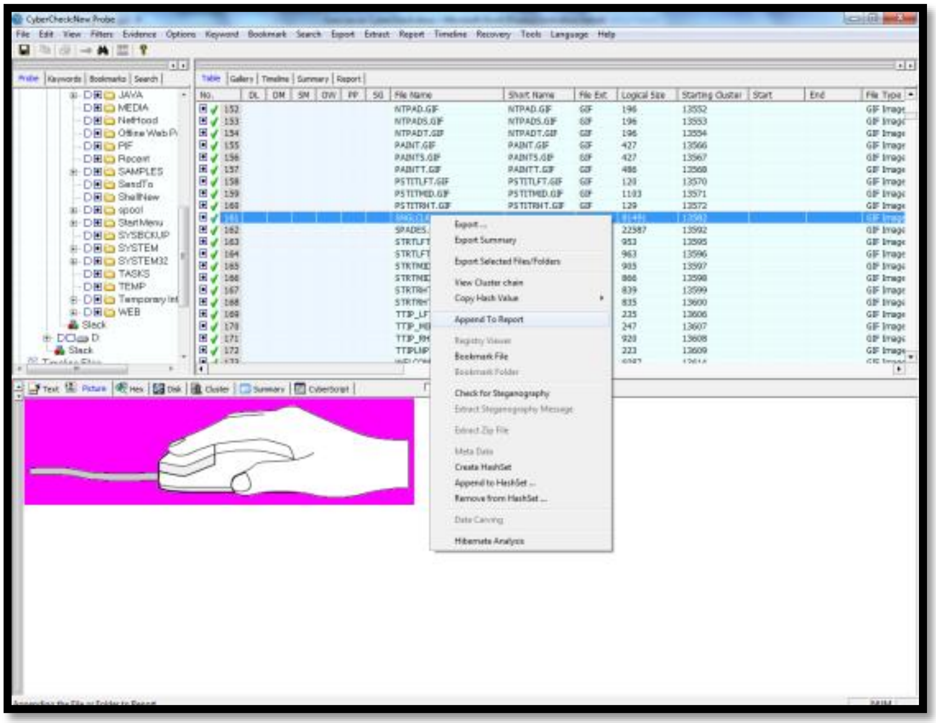
CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock
ShowLegend

Task 23: How do you view the cluster chain of a particular file?

Solution: Right click any file in Table view >> View Cluster Chain or from View menu >> Cluster chain

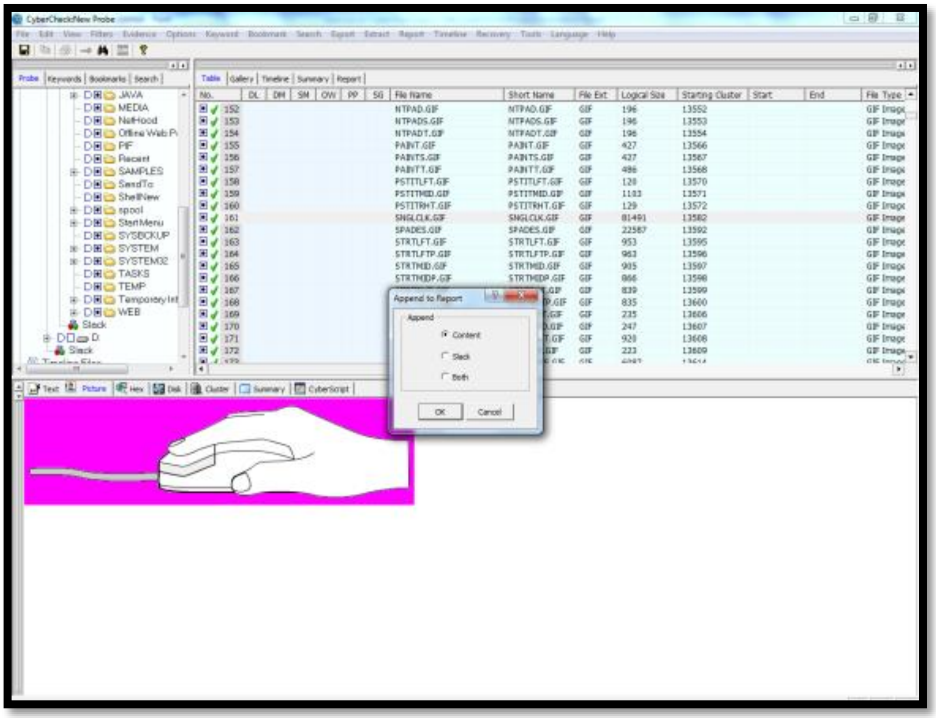
Task 24: Add a picture file into the report and observe what happened in the report?

Solution: To add a picture into the report, select the desired image file and either right click and ‘Append to Report’ or select the option from the Report menu in the main menu.



No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
152							NTPAD.GIF	NTPAD.GIF	GIF	196	13552			GIF Image
153							NTPADS.GIF	NTPADS.GIF	GIF	196	13553			GIF Image
154							NTPADT.GIF	NTPADT.GIF	GIF	196	13554			GIF Image
155							PAINT.GIF	PAINT.GIF	GIF	427	13566			GIF Image
156							PAINTS.GIF	PAINTS.GIF	GIF	427	13567			GIF Image
157							PAINTT.GIF	PAINTT.GIF	GIF	486	13568			GIF Image
158							PSTITLFT.GIF	PSTITLFT.GIF	GIF	120	13570			GIF Image
159							PSTITMID.GIF	PSTITMID.GIF	GIF	1103	13571			GIF Image
160							PSTITRHT.GIF	PSTITRHT.GIF	GIF	129	13572			GIF Image
161							SNGLCLK			81491	13582			GIF Image
162							SPADES.			22587	13592			GIF Image
163							STRTLFT			953	13595			GIF Image
164							STRTLFT			963	13596			GIF Image
165							STRTMID			905	13597			GIF Image
166							STRTMID			866	13598			GIF Image
167							STRTRHT			839	13599			GIF Image
168							STRTRHT			835	13600			GIF Image
169							TTIP_LF			235	13606			GIF Image
170							TTIP_MI			247	13607			GIF Image
171							TTIP_RH			920	13608			GIF Image
172							TTIPLIP			223	13609			GIF Image

A confirmation message appears, click yes. The next dialog asks whether to append the Content, Slack or Both. Select the Content option to just add the image file only.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe | Keywords | Bookmarks | Search
JAVA
MEDIA
NetHood
Offline Web P
PIF
Recent
SAMPLES
SendTo
ShellNew
spool
StartMenu
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Table | Gallery | Timeline | Summary | Report
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
152							NTPAD.GIF	NTPAD.GIF	GIF	196	13552			GIF Image
153							NTPADS.GIF	NTPADS.GIF	GIF	196	13553			GIF Image
154							NTPADT.GIF	NTPADT.GIF	GIF	196	13554			GIF Image
155							PAINT.GIF	PAINT.GIF	GIF	427	13566			GIF Image
156							PAINTS.GIF	PAINTS.GIF	GIF	427	13567			GIF Image
157							PAINTT.GIF	PAINTT.GIF	GIF	486	13568			GIF Image
158							PSTITLFT.GIF	PSTITLFT.GIF	GIF	120	13570			GIF Image
159							PSTITMID.GIF	PSTITMID.GIF	GIF	1103	13571			GIF Image
160							PSTITRHT.GIF	PSTITRHT.GIF	GIF	129	13572			GIF Image
161							SNGLCLK.GIF	SNGLCLK.GIF	GIF	81491	13582			GIF Image
162							SPADES.GIF	SPADES.GIF	GIF	22587	13592			GIF Image
163							STRTLFT.GIF	STRTLFT.GIF	GIF	953	13595			GIF Image
164							STRTLFTP.GIF	STRTLFTP.GIF	GIF	963	13596			GIF Image
165							STRTMID.GIF	STRTMID.GIF	GIF	905	13597			GIF Image
166							STRTMIDP.GIF	STRTMIDP.GIF	GIF	866	13598			GIF Image
167								.GIF	GIF	839	13599			GIF Image
168								P.GIF	GIF	835	13600			GIF Image
169								.GIF	GIF	235	13606			GIF Image
170								D.GIF	GIF	247	13607			GIF Image
171								T.GIF	GIF	920	13608			GIF Image
172								GIF	GIF	223	13609			GIF Image

Append to Report

Append

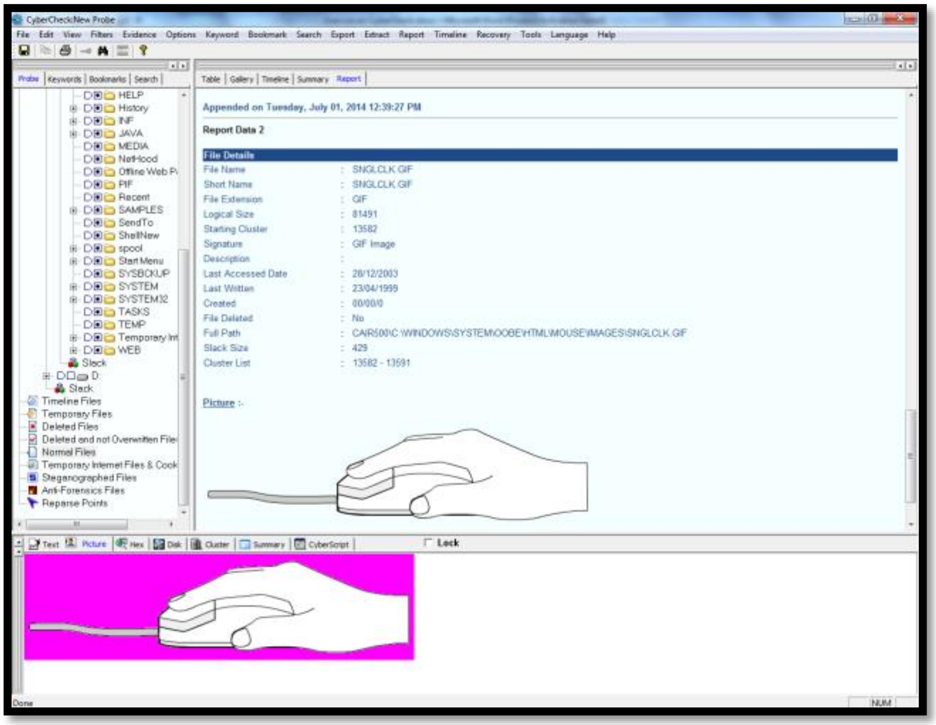
● Content

○ Slack

○ Both

OK Cancel

Enter a comment and then OK.A message-Item successfully appended to report appears. Take the report tab from the middle pane. The report shows the details of the appended image file such as file name, extension, logical size, starting cluster, accessed date, whether deleted or not etc.


CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
HELP
History
INF
JAVA
MEDIA
NetHood
Offline Web P
PIF
Recent
SAMPLES
SendTo
ShellNew
spool
Start Menu
SYSBCKUP
SYSTEM
SYSTEM32
TASKS
TEMP
Temporary Int
WEB
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cook
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock
Done
NUM

Appended on Tuesday, July 01, 2014 12:39:27 PM

Report Data 2

File Details

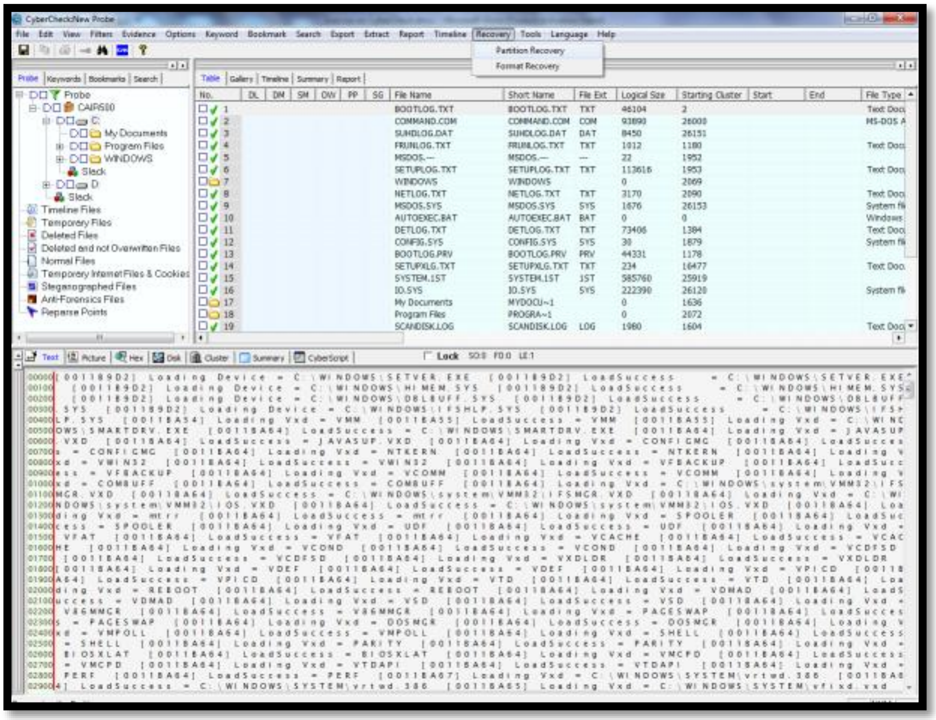
File Name : SNGLCLK.GIF
Short Name : SNGLCLK.GIF
File Extension : GIF
Logical Size : 81491
Starting Cluster : 13582
Signature : GIF Image
Description :
Last Accessed Date : 28/12/2003
Last Written : 23/04/1999
Created : 00/00/0
File Deleted : No
Full Path : C:\R500\C:\WINDOWS\SYSTEM\OOBE\HTML\MOUSE\IMAGES\SNGLCLK.GIF
Slack Size : 429
Cluster List : 13582 - 13591

Picture :-

Just after the file details of the image file, the image is displayed in the report.

Task 25: How do you start partition recovery?

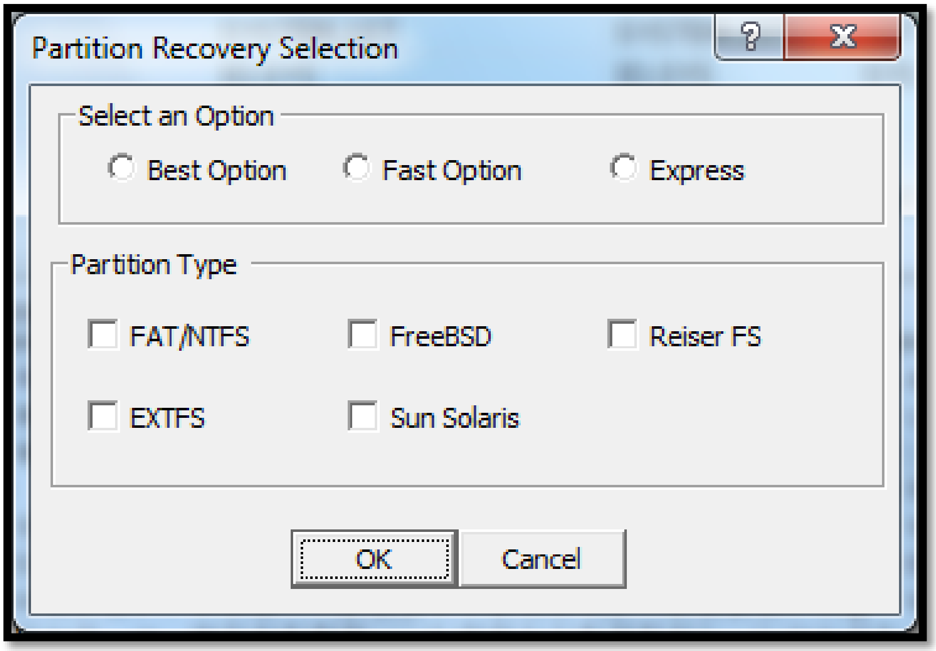
Solution: To recover the deleted partitions, select Recovery|Partition Recovery



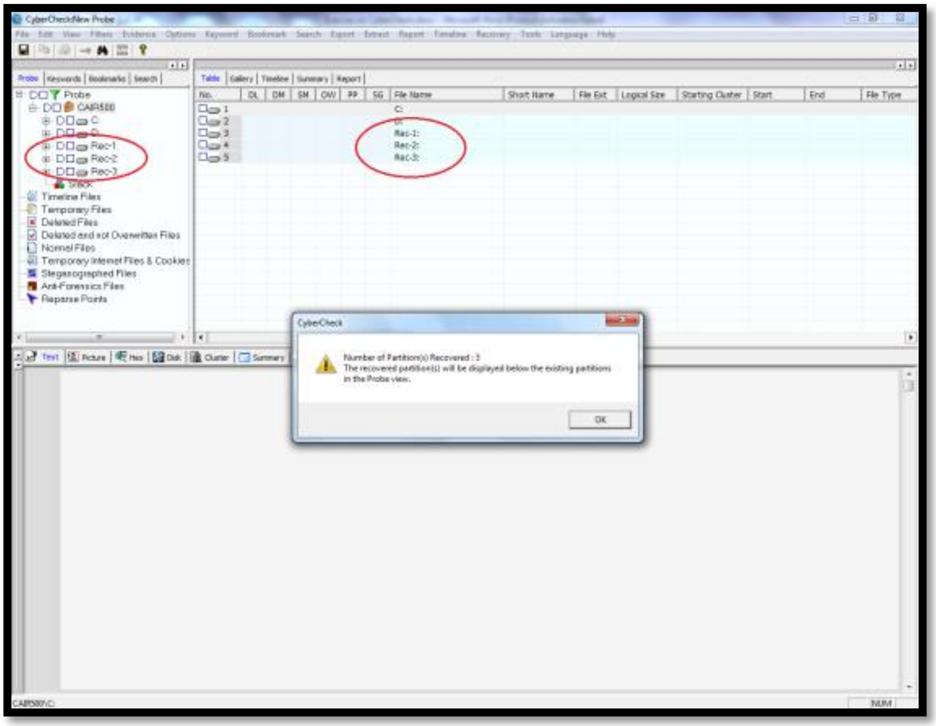
CyberCheckNew Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Partition Recovery
Format Recovery
Probe Keywords Bookmarks Search
Probe
CAIR500
C:
My Documents
Program Files
WINDOWS
Slack
D:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Restore Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary CyberScript
Lock SO:0 FO:0 LE:1

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1							BOOTLOG.TXT	BOOTLOG.TXT	TXT	46104	2			Text Doc
2							COMMAND.COM	COMMAND.COM	COM	93890	26000			MS-DOS A
3							SUHDLOG.DAT	SUHDLOG.DAT	DAT	8450	26151			
4							FRUNLOG.TXT	FRUNLOG.TXT	TXT	1012	1180			Text Doc
5							MSDOS.---	MSDOS.---	---	22	1952			
6							SETUPLOG.TXT	SETUPLOG.TXT	TXT	113616	1953			Text Doc
7							WINDOWS	WINDOWS		0	2069			
8							NETLOG.TXT	NETLOG.TXT	TXT	3170	2090			Text Doc
9							MSDOS.SYS	MSDOS.SYS	SYS	1676	26153			System fi
10							AUTOEXEC.BAT	AUTOEXEC.BAT	BAT	0	0			Windows
11							DETLOG.TXT	DETLOG.TXT	TXT	73406	1384			Text Doc
12							CONFIG.SYS	CONFIG.SYS	SYS	30	1879			System fi
13							BOOTLOG.PRV	BOOTLOG.PRV	PRV	44331	1178			
14							SETUPXLG.TXT	SETUPXLG.TXT	TXT	234	16477			Text Doc
15							SYSTEM.1ST	SYSTEM.1ST	1ST	585760	25919			
16							IO.SYS	IO.SYS	SYS	222390	26120			System fi
17							My Documents	MYDOCU~1		0	1636			
18							Program Files	PROGRA~1		0	2072			
19							SCANDISK.LOG	SCANDISK.LOG	LOG	1980	1604			Text Doc

Select the desired option. In the Best option each and every sector in the evidence file will be scanned and in the Fast option, only sectors with sector number, as multiple of 63 will be scanned.



Click OK to start the recovery process, the progress is shown in the progress-bar. The number of partition(s) recovered is displayed in a message box. The recovered partition(s) will be displayed below the existing partitions in the Probe view. Their names start with "Rec-". For example, if two partitions have been recovered, then the first partition will be shown with the name Rec-1 and the second one with the name Rec-2.



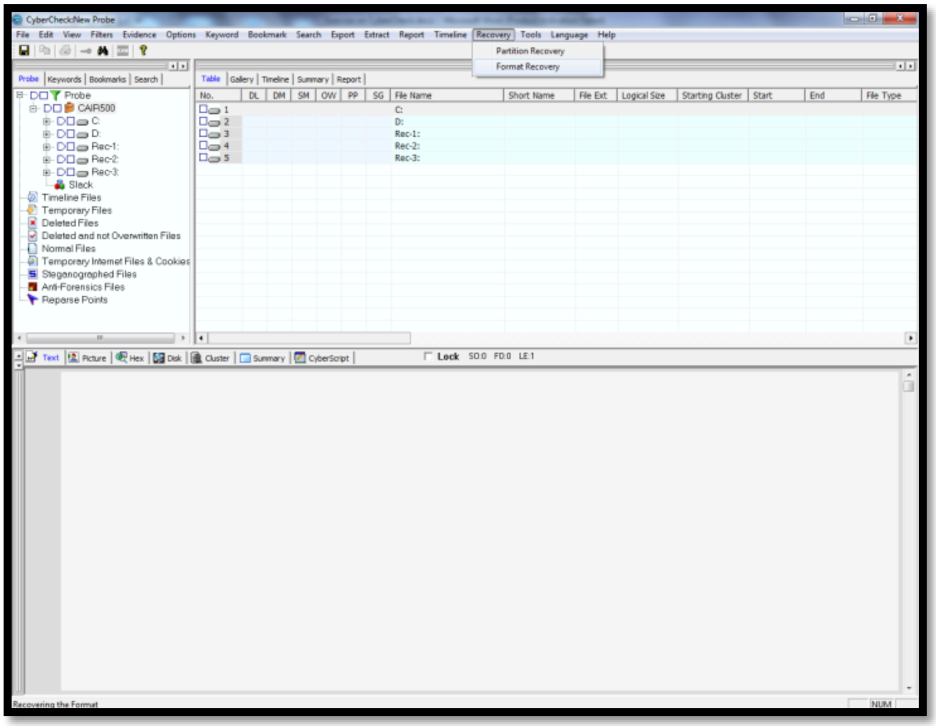
CyberCheck

Number of Partition(s) Recovered : 3
The recovered partition(s) will be displayed below the existing partitions in the Probe view.

To see the files & folders of recovered partition(s), click on the "+" symbol near the partition name (like that of an existing partition).

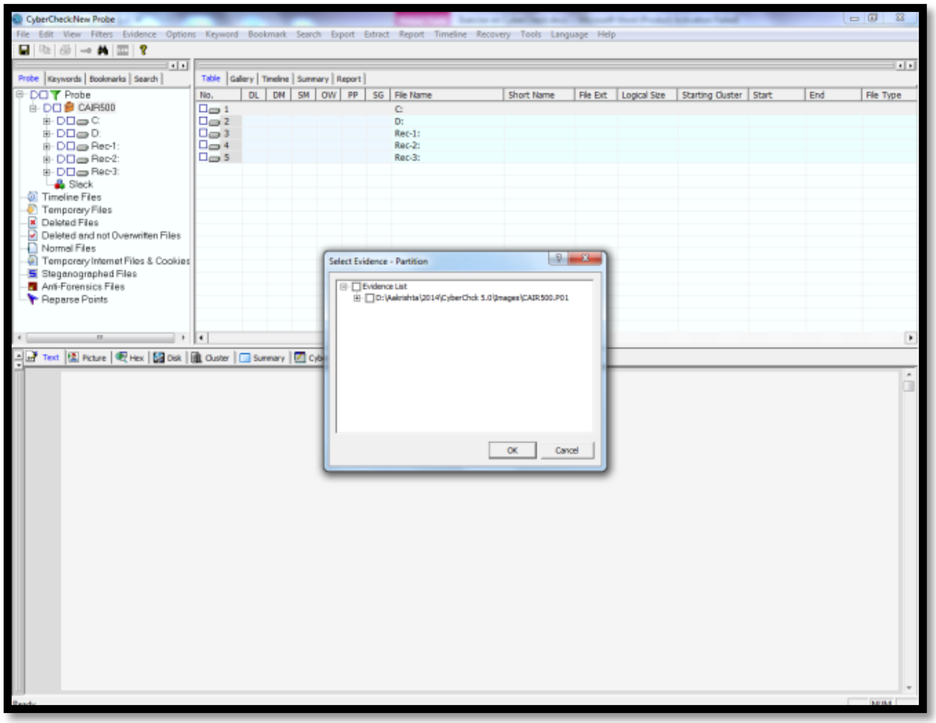
Task 26: How do you start format recovery?

Solution: Format recovery recovers the formatted partitions from the evidence file. Select Recovery|Format Recovery menu item from the main menu.


CyberCheck\New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Partition Recovery
Format Recovery
Probe | Keywords | Bookmarks | Search
Table | Gallery | Timeline | Summary | Report
Probe
CAIR500
C:
D:
Rec-1:
Rec-2:
Rec-3:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Text | Picture | Hex | Disk | Cluster | Summary | CyberScript
Lock SO:0 FD:0 LE:1
Recovering the Format
NUM

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
□ 1							C:							
□ 2							D:							
□ 3							Rec-1:							
□ 4							Rec-2:							
□ 5							Rec-3:							

All the available partitions are displayed for selecting the partition(s) to recover. Select the desired partition to recover by ticking the option. Click the OK button, the format recovery process starts and its progress is shown by a progress-bar.


CyberCheck:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Keywords Bookmarks Search
Probe
CAIR500
C:
D:
Rec-1:
Rec-2:
Rec-3:
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Summary Cyb
Select Evidence - Partition
OK
Cancel

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type
1							C:							
2							D:							
3							Rec-1:							
4							Rec-2:							
5							Rec-3:							

Select Evidence - Partition

- □ Evidence List
  - □ D:\Aakrishta\2014\CyberChck 5.0\Images\CAIR500.P01

On completion a message box is displayed- “Format Recovery Completed. The recovered files and folders, if any available, can be viewed by moving to the respective partition and looking for a folder named "Format Recover". Select the desired partition to find a folder named Format Recover. This folder will contain other folders (names starting with "CNo:") and they will contain the files recovered. If all partitions are selected for recovery, the menu option "Format Recovery" will be disabled after the completion of format recovery. If the Format recovery process is cancelled or not all partitions are selected then the menu option is not disabled

Task 27: How can you preview a storage media locally?

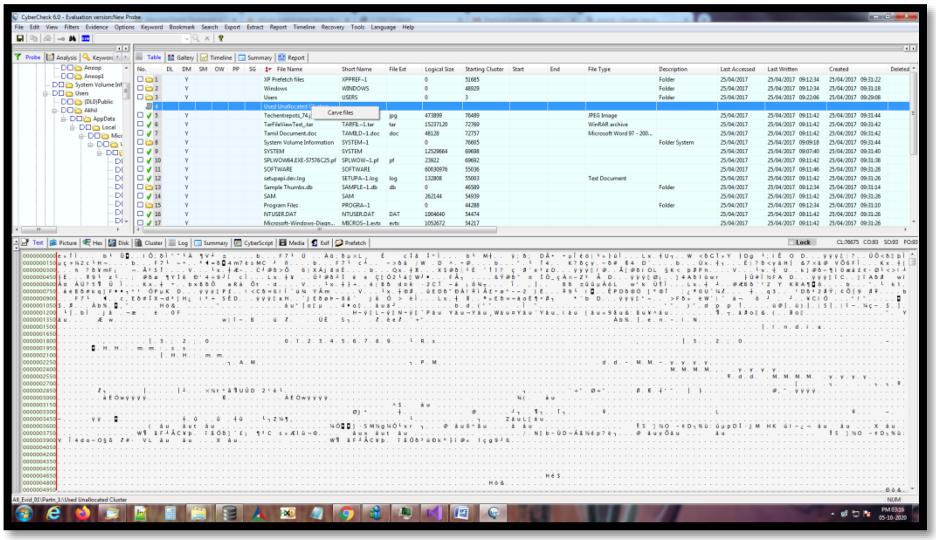
Solution: Run CyberCheck6.0

To display the details of storage media connected in the analysis machine.Select View|Storage Media Details. Or click on the Storage Media Details icon provided in the tool bar. A list box will be displayed, listing the details of the fixed storage media available in the analysis machine.

Carving Files in CyberCheck (In-place carving)

Task 28: How do you initiate carving process from unallocated clusters, Disk Slack?

Solution: Click a partition in the left tree. In the table view select ‘Used Unallocated Clusters’ and Right click it. Select ‘Carve Files’ from the context menu. A progress bar will appear in the bottom showing the carving progress. After completion, a message box will appear showing the carved file details.

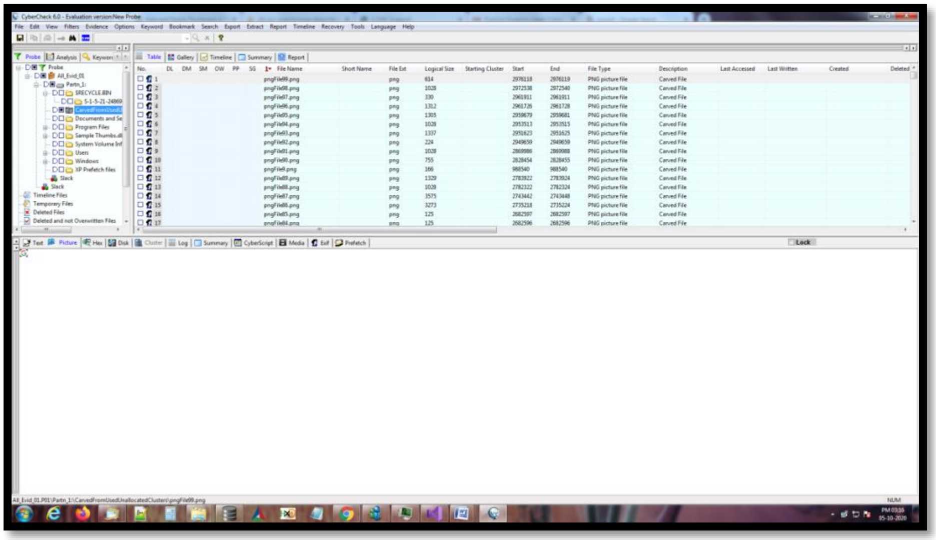


CyberCheck 6.0 - Evaluation version:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Table Gallery Timeline Summary Report
Carve files
Text Picture Hex Disk Cluster Log Summary CyberScript Media Exif Prefetch
Lock
CL:76675 CO:93 SO:93 FO:93

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type	Description	Last Accessed	Last Written	Created	Deleted
1		Y					XP Prefetch files	XPPREF~1		0	51685				Folder	25/04/2017	25/04/2017 09:12:34	25/04/2017 09:31:22	
2		Y					Windows	WINDOWS		0	48929				Folder	25/04/2017	25/04/2017 09:12:34	25/04/2017 09:31:18	
3		Y					Users	USERS		0	3				Folder	25/04/2017	25/04/2017 09:22:06	25/04/2017 09:29:08	
4							Used Unallocated Clusters												
5		Y					Techentrepots_74.j		jpg	473899	76489			JPEG Image		25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:44	
6		Y					TarFileViewTest_.tar	TARFIL~1.tar	tar	15237120	72769			WinRAR archive		25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:42	
7		Y					Tamil Document.doc	TAMILD~1.doc	doc	48128	72757			Microsoft Word 97 - 200...		25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:42	
8		Y					System Volume Information	SYSTEM~1		0	76605				Folder System	25/04/2017	25/04/2017 09:09:18	25/04/2017 09:31:44	
9		Y					SYSTEM	SYSTEM		12529664	69698					25/04/2017	25/04/2017 09:07:40	25/04/2017 09:31:40	
10		Y					SPLWOW64.EXE-57576C25.pf	SPLWOW~1.pf	pf	23922	69692					25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:38	
11		Y					SOFTWARE	SOFTWARE		60030976	55036					25/04/2017	25/04/2017 09:11:46	25/04/2017 09:31:28	
12		Y					setupapi.dev.log	SETUPA~1.log	log	132808	55003			Text Document		25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:26	
13		Y					Sample Thumbs.db	SAMPLE~1.db	db	0	46589				Folder	25/04/2017	25/04/2017 09:12:34	25/04/2017 09:31:14	
14		Y					SAM	SAM		262144	54939					25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:26	
15		Y					Program Files	PROGRA~1		0	44288				Folder	25/04/2017	25/04/2017 09:12:34	25/04/2017 09:31:10	
16		Y					NTUSER.DAT	NTUSER.DAT	DAT	1904640	54474					25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:26	
17		Y					Microsoft-Windows-Diagn...	MICROS~1.evtx	evtx	1052672	54217					25/04/2017	25/04/2017 09:11:42	25/04/2017 09:31:26	

Task 29: Where can you see the carved files from unallocated clusters, Disk Slack?

Solution: The result will be shown by clicking the folder ‘Carved from Used Unallocated clusters’ in the left tree view.

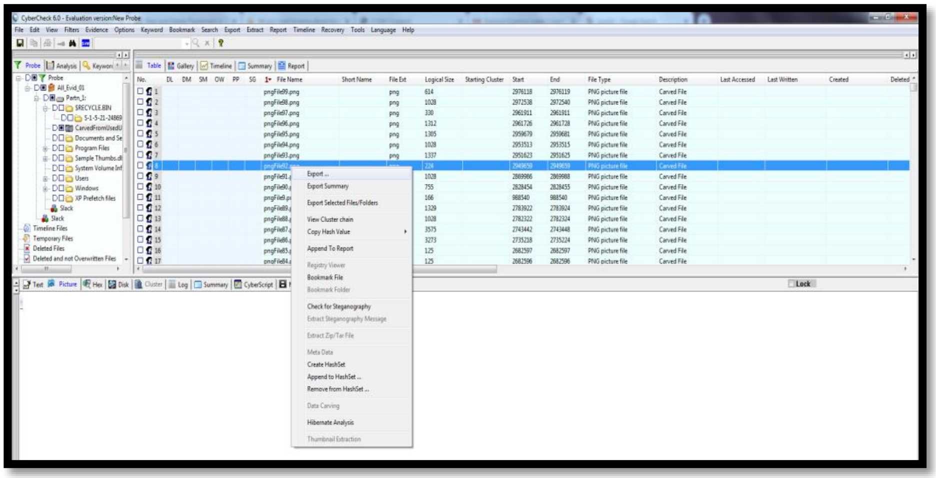

CyberCheck 6.0 - Evaluation version:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Analysis Keyword
Table Gallery Timeline Summary Report
Text Picture Hex Disk Cluster Log Summary CyberScript Media Exif Prefetch
Lock

No.	DL	DM	SM	OW	PP	SG	File Name	Short Name	File Ext	Logical Size	Starting Cluster	Start	End	File Type	Description	Last Accessed	Last Written	Created	Deleted
1							pngFile99.png		png	614		2976118	2976119	PNG picture file	Carved File				
2							pngFile98.png		png	1028		2972538	2972540	PNG picture file	Carved File				
3							pngFile97.png		png	330		2961911	2961911	PNG picture file	Carved File				
4							pngFile96.png		png	1312		2961726	2961728	PNG picture file	Carved File				
5							pngFile95.png		png	1305		2959679	2959681	PNG picture file	Carved File				
6							pngFile94.png		png	1028		2953513	2953515	PNG picture file	Carved File				
7							pngFile93.png		png	1337		2951623	2951625	PNG picture file	Carved File				
8							pngFile92.png		png	224		2949659	2949659	PNG picture file	Carved File				
9							pngFile91.png		png	1028		2869986	2869988	PNG picture file	Carved File				
10							pngFile90.png		png	755		2828454	2828455	PNG picture file	Carved File				
11							pngFile9.png		png	166		988540	988540	PNG picture file	Carved File				
12							pngFile89.png		png	1329		2783922	2783924	PNG picture file	Carved File				
13							pngFile88.png		png	1028		2782322	2782324	PNG picture file	Carved File				
14							pngFile87.png		png	3575		2743442	2743448	PNG picture file	Carved File				
15							pngFile86.png		png	3273		2735218	2735224	PNG picture file	Carved File				
16							pngFile85.png		png	125		2682597	2682597	PNG picture file	Carved File				
17							pngFile84.png		png	125		2682596	2682596	PNG picture file	Carved File				

All_Evid_01.P01\Partn_1\CarvedFromUsedUnallocatedClusters\pngFile99.png

Task 30: How do you export a carved file?

Solution: Select a carved file and right click it. Select Export from the context menu and select the location to which it is exported.

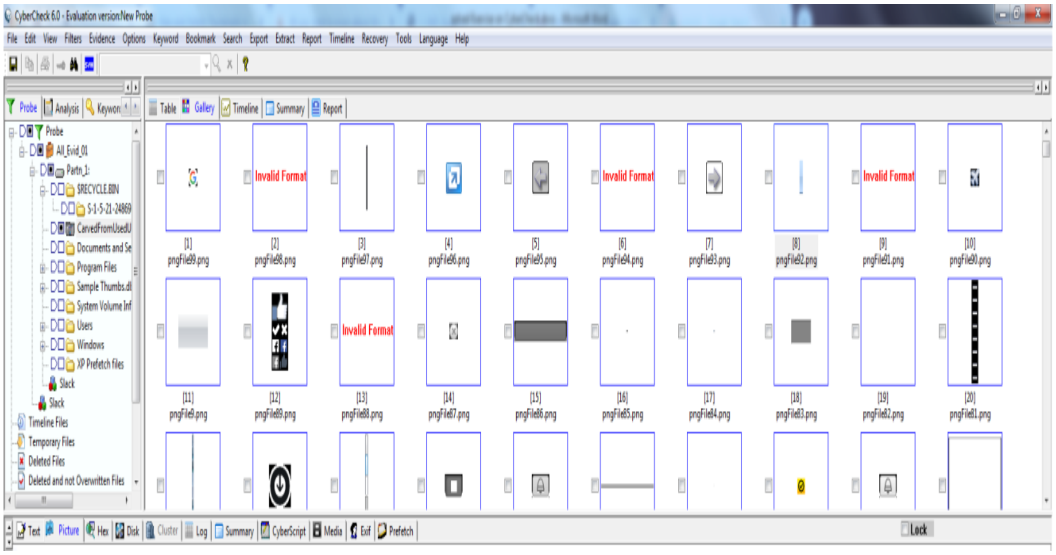


Task 31: How do you append a carved file to report?

Solution: Select a carved file and right click it. Select ‘Append to Report’ from the context menu.

Task 32: How do you see the carved files in gallery view?

Solution: Select Gallery tab while viewing the resultant carved files.


CyberCheck 6.0 - Evaluation version:New Probe
File Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe Analysis Keywor
Table Gallery Timeline Summary Report
Probe
All_Evid_01
Partn_1:
$RECYCLE.BIN
S-1-5-21-24869
CarvedFromUsedU
Documents and Se
Program Files
Sample Thumbs.dl
System Volume Inf
Users
Windows
XP Prefetch files
Slack
Slack
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Invalid Format
[1] pngFile99.png
[2] pngFile98.png
[3] pngFile97.png
[4] pngFile96.png
[5] pngFile95.png
[6] pngFile94.png
[7] pngFile93.png
[8] pngFile92.png
[9] pngFile91.png
[10] pngFile90.png
[11] pngFile9.png
[12] pngFile89.png
[13] pngFile88.png
[14] pngFile87.png
[15] pngFile86.png
[16] pngFile85.png
[17] pngFile84.png
[18] pngFile83.png
[19] pngFile82.png
[20] pngFile81.png
Text Picture Hex Disk Cluster Log Summary CyberScript Media Exif Prefetch
Lock