VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

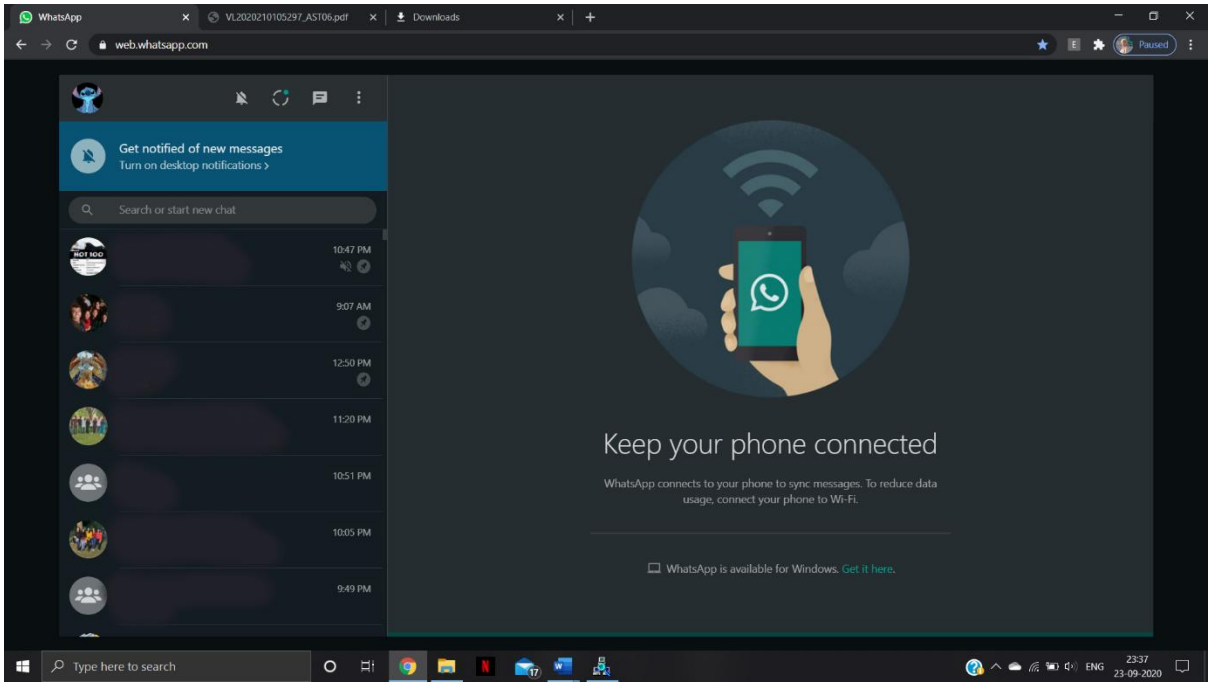
Lab Assessment-VI, SEPTEMBER 2020

B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

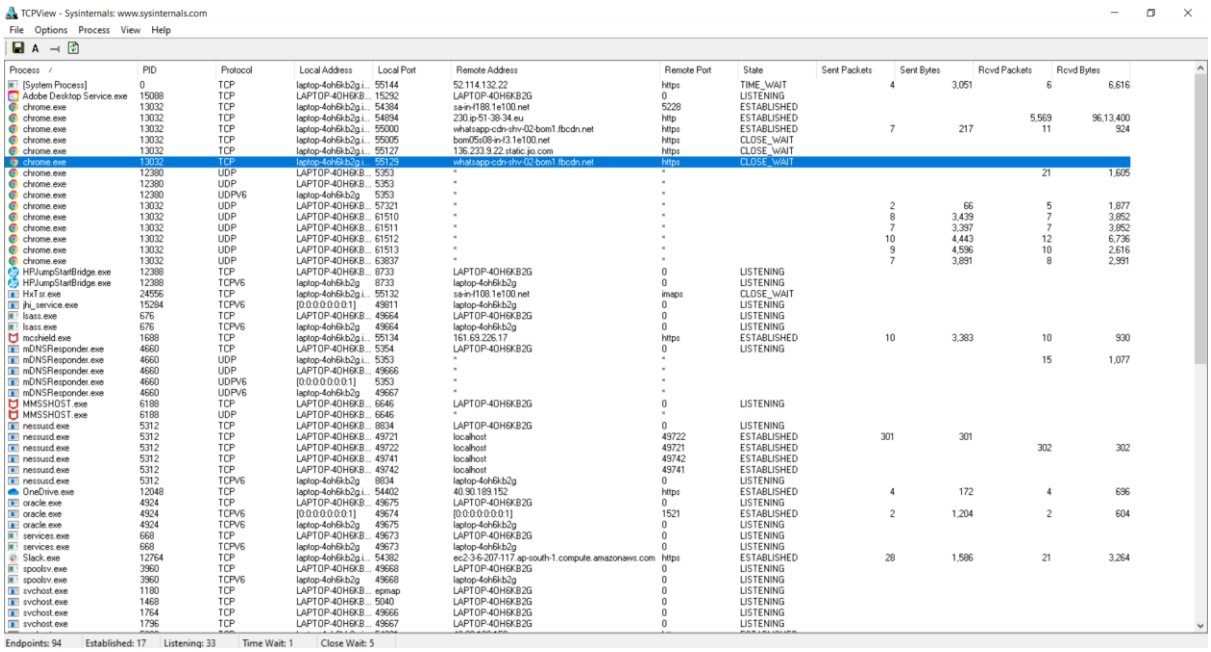
Exercises on TCPView

1. Create a new tab in chrome and type web.whatsapp.com



2. Take a snapshot showing the attributes of the process running in chrome.exe with WhatsApp

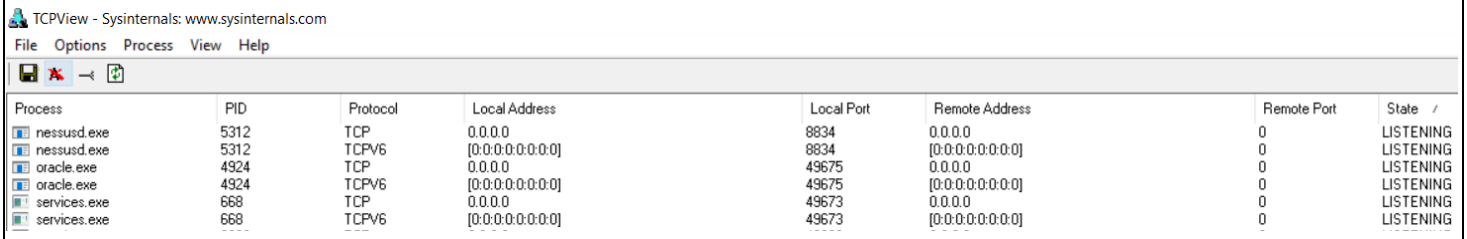
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
chrome.exe	13032	TCP	laptop-4oh6kb2g.iballbaton.com.in	55129	whatsapp-cdn-shv-02-bom1.fbcdn.net	https	CLOSE_WAIT



3. Identify any two processes which are in listening state, established state and time-wait state.

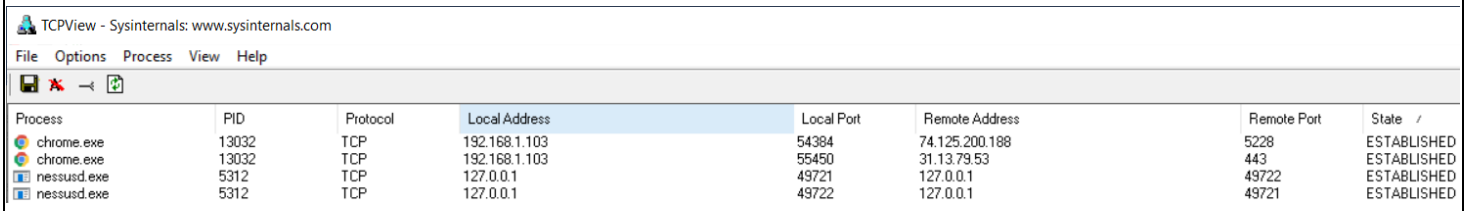
Listening:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
nessusd.exe	5312	TCP	0.0.0.0	8834	0.0.0.0	0
nessusd.exe	5312	TCPV6	[0:0:0:0:0:0:0:0]	8834	[0:0:0:0:0:0:0:0]	0
oracle.exe	4924	TCP	0.0.0.0	49675		0
oracle.exe	4924	TCPV6	[0:0:0:0:0:0:0:0]	49675	[0:0:0:0:0:0:0:0]	0
services.exe	668	TCP	0.0.0.0	49673		0
services.exe	668	TCPV6	[0:0:0:0:0:0:0:0]	49673	[0:0:0:0:0:0:0:0]	0



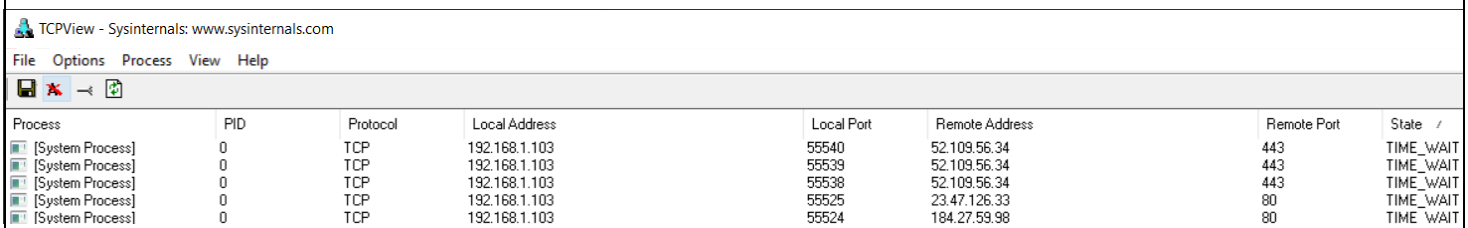
Established:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	13032	TCP	192.168.1.103	58384	74.125.200.188	5228
chrome.exe	13032	TCP	192.168.1.103	55450	31.13.79.53	443
nessusd.exe	5312	TCP	127.0.0.1	49721	127.0.0.1	49722
nessusd.exe	5312	TCP	127.0.0.1	49722	127.0.0.1	49721



Time_Wait:

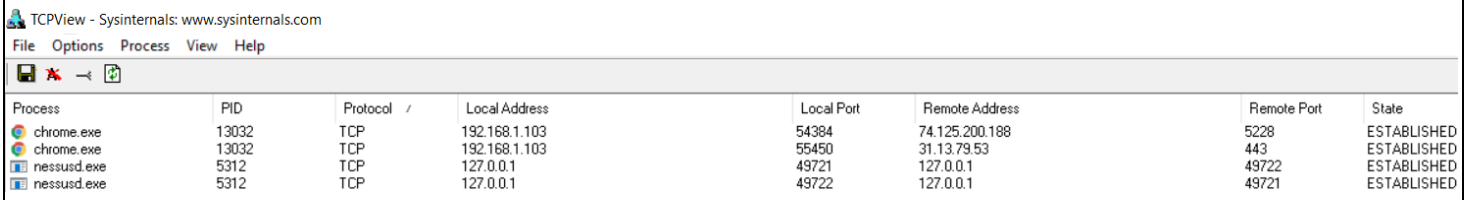
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
[System Process]	0	TCP	192.168.1.103	55540	52.109.56.34	443
[System Process]	0	TCP	192.168.1.103	55539	52.109.56.34	443
[System Process]	0	TCP	192.168.1.103	55538	52.109.56.34	443
[System Process]	0	TCP	192.168.1.103	55525	23.47.126.33	80
[System Process]	0	TCP	192.168.1.103	55524	184.27.59.98	80



4. Identify any two processes which are using TCP protocol, TCPV6, UDP protocol and UDPV6.

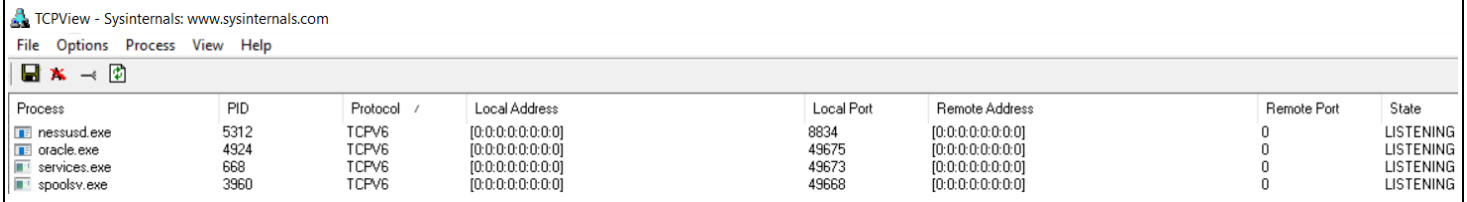
TCP:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
chrome.exe	13032	TCP	192.168.1.103	58384	74.125.200.188	5228	Established
chrome.exe	13032	TCP	192.168.1.103	55450	31.13.79.53	443	Established
nessusd.exe	5312	TCP	127.0.0.1	49721	127.0.0.1	49722	Established
nessusd.exe	5312	TCP	127.0.0.1	49722	127.0.0.1	49721	Established



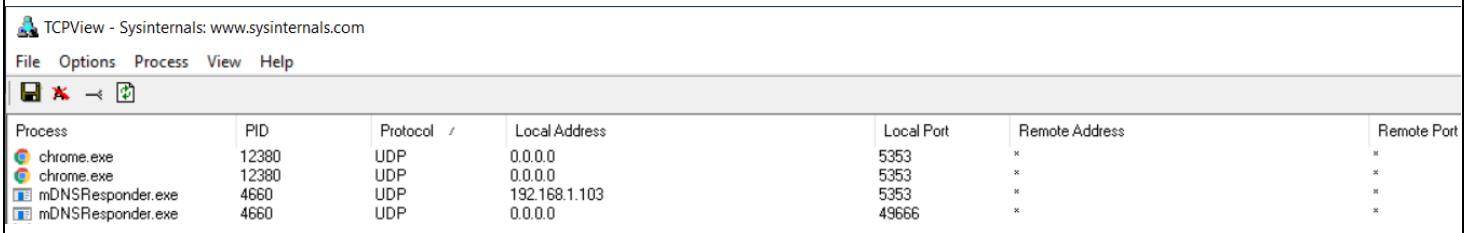
TCPV6:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
nessusd.exe	5312	TCPV6	[0:0:0:0:0:0:0:0]	8834	[0:0:0:0:0:0:0:0]	0	Listening
oracle.exe	4924	TCPV6	[0:0:0:0:0:0:0:0]	49675	[0:0:0:0:0:0:0:0]	0	Listening
services.exe	668	TCPV6	[0:0:0:0:0:0:0:0]	49673	[0:0:0:0:0:0:0:0]	0	Listening
spoolsy.exe	3960	TCPV6	[0:0:0:0:0:0:0:0]	49668	[0:0:0:0:0:0:0:0]	0	Listening



UDP:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	12380	UDP	0.0.0.0	5353	*	*
chrome.exe	12380	UDP	0.0.0.0	5353	*	*
mDNSResponder.exe	4660	UDP	192.168.1.103	5353	*	*
mDNSResponder.exe	4660	UDP	0.0.0.0	49666	*	*



UDPV6:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	12380	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*
mDNSResponder.exe	4660	UDPV6	[0:0:0:0:0:0:0:1]	5353	*	*
mDNSResponder.exe	4660	UDPV6	[0:0:0:0:0:0:0:0]	49667	*	*
scvhost.exe	4496	UDPV6	[0:0:0:0:0:0:0:0]	500	*	*
scvhost.exe	3520	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*

TCPView - Sysinternals: www.sysinternals.com

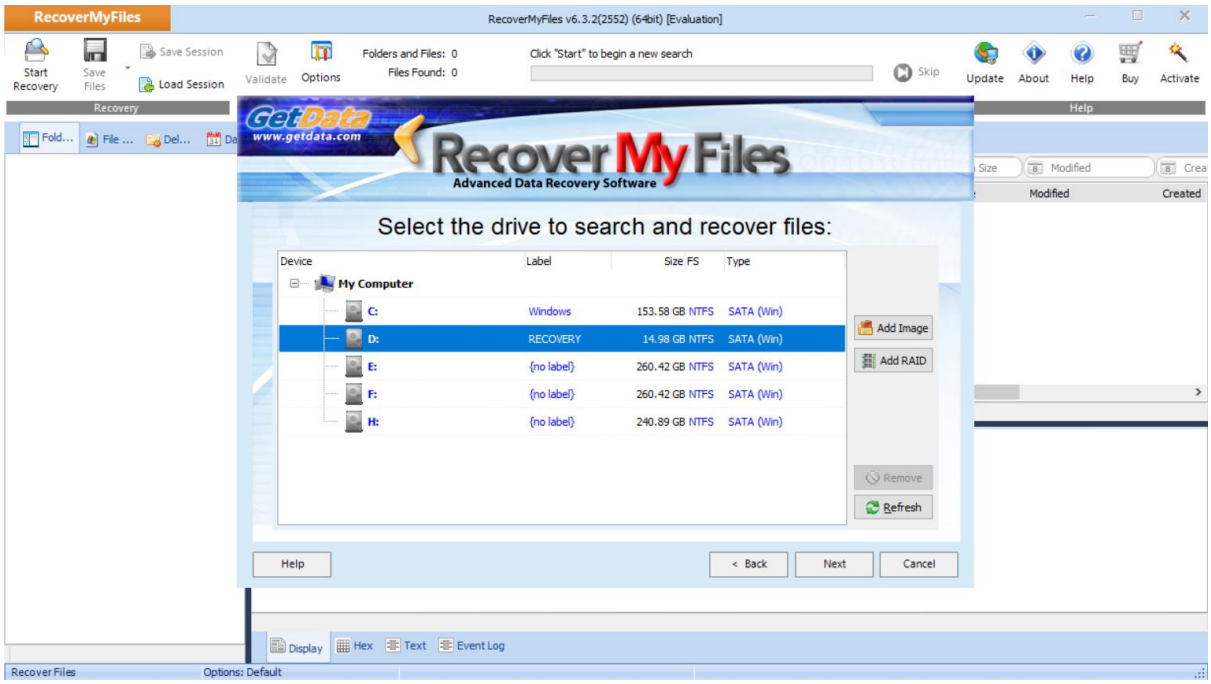
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	12380	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*
mDNSResponder.exe	4660	UDPV6	[0:0:0:0:0:0:0:1]	5353	*	*
mDNSResponder.exe	4660	UDPV6	[0:0:0:0:0:0:0:0]	49667	*	*
svchost.exe	4496	UDPV6	[0:0:0:0:0:0:0:0]	500	*	*
svchost.exe	3520	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*

Exercises on Recover my Files

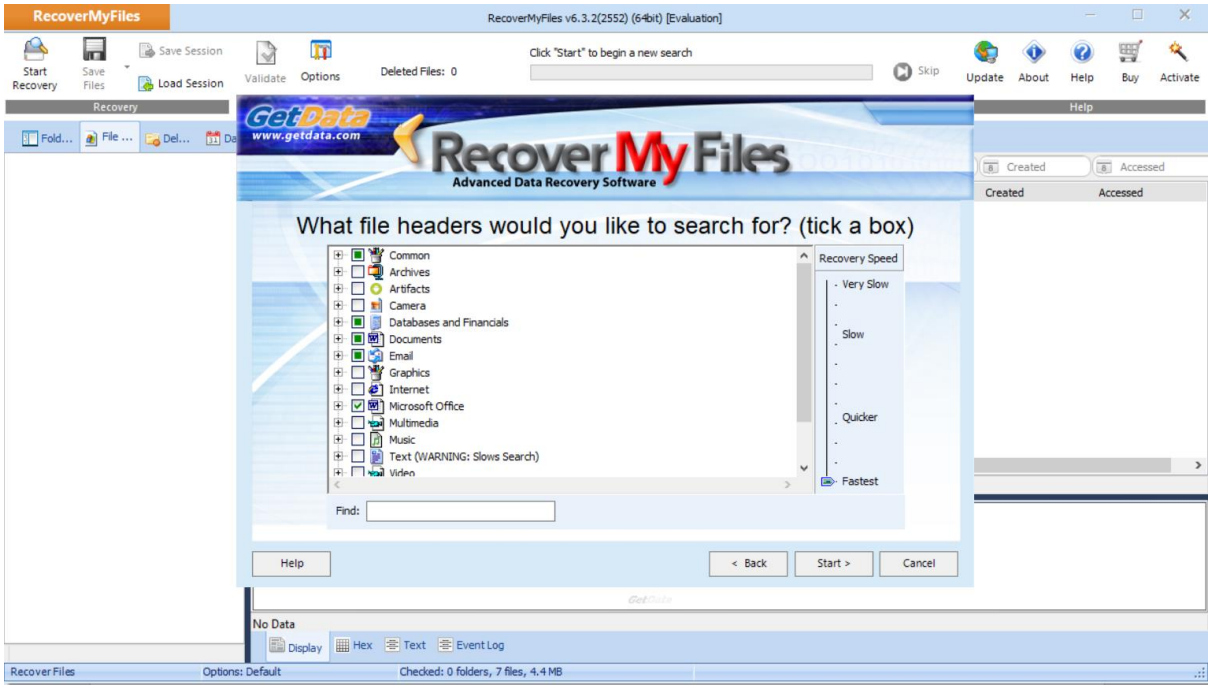
1. Perform a search for specific type of file in a specific drive
2. Perform recovery of deleted files in a specific drive

Selected \D: drive to search files:

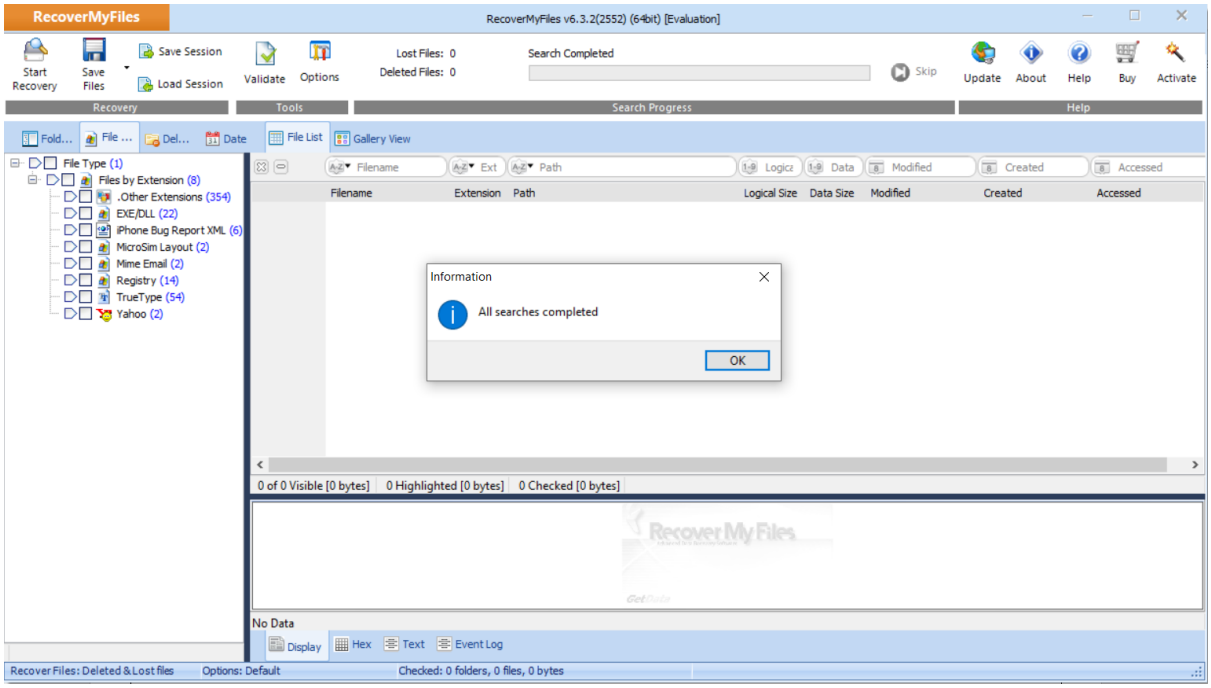


Selected “Search for deleted files, then search for selected “Lost File” types.” option:

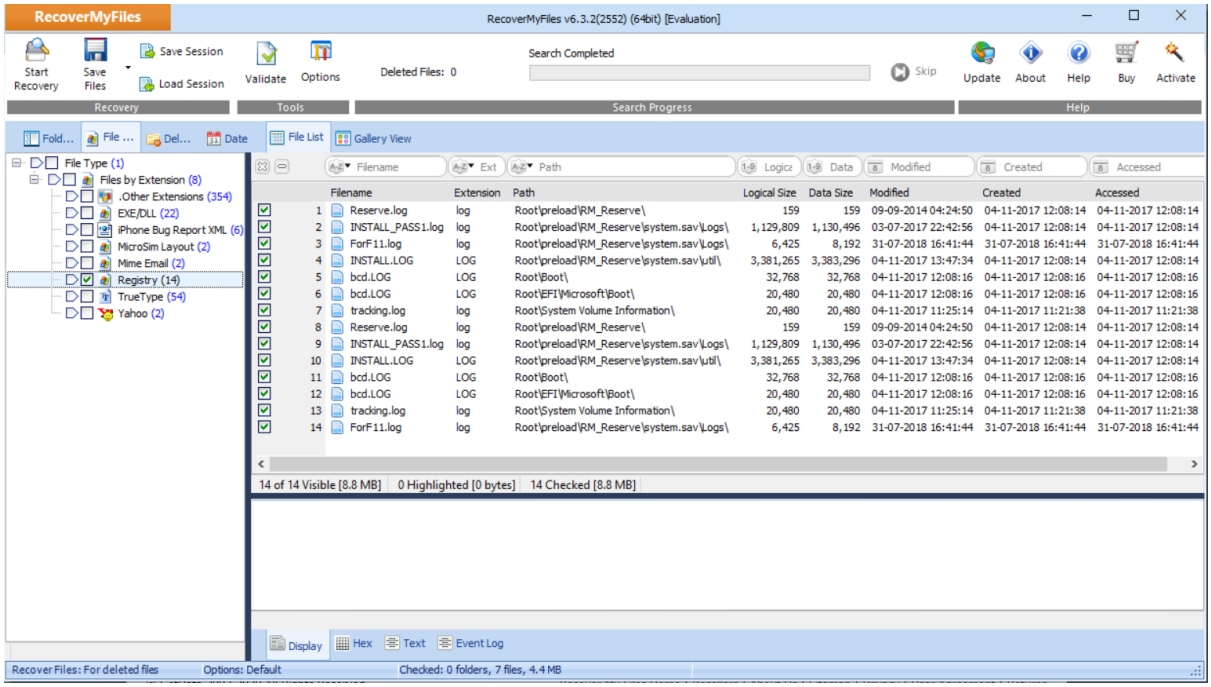
Selected “Microsoft Office” file header:



Search is completed:



Displaying “Registry (.log)” file types searched:



****