



VIT[®]

Vellore Institute of Technology

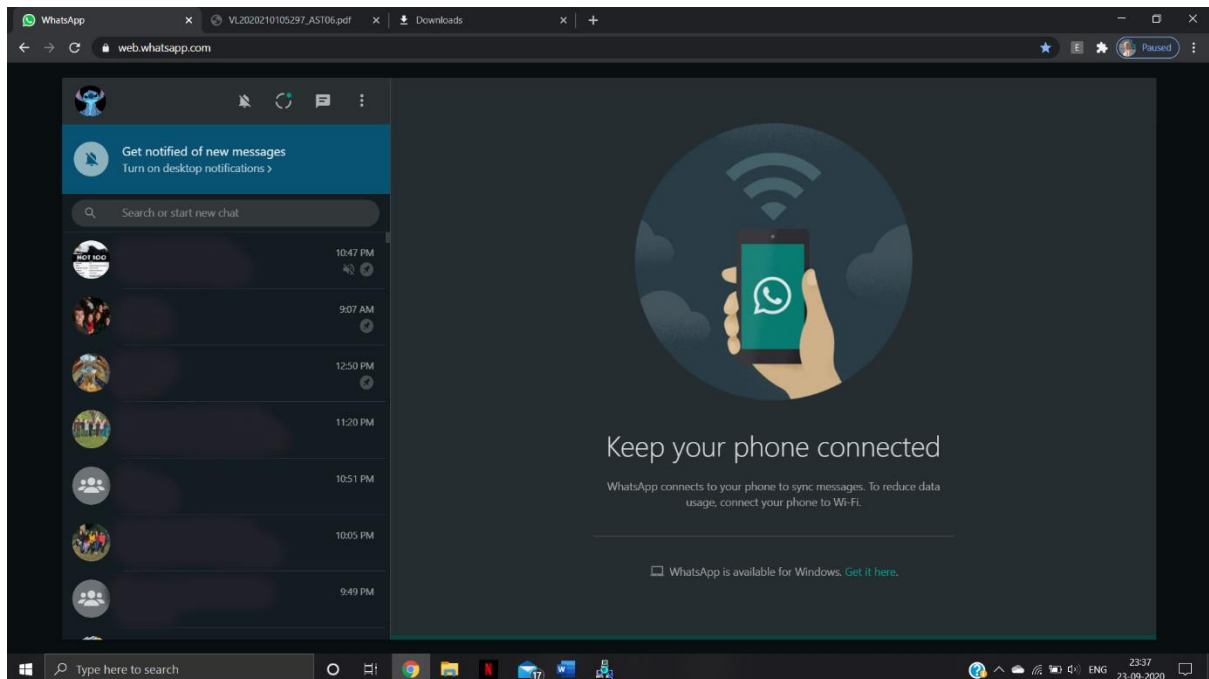
(Deemed to be University under section 3 of UGC Act, 1956)

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	55129	whatsapp-cdn-shv-02-bom1.fbcdn.net	https	CLOSE_WAIT

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Process]	0	TCP	laptop-4oh6kb2g	55144	52.114.132.22	https	TIME_WAIT	4	3,051	6	6,616
Adobe Desktop Service.exe	15008	TCP	LAPTOP-4OH6KB2G	15292	LAPTOP-4OH6KB2G	0	LISTENING				
chrome.exe	13032	TCP	laptop-4oh6kb2g	54384	sa-in-f108.1e100.net	5228	ESTABLISHED				
chrome.exe	13032	TCP	laptop-4oh6kb2g	54894	230.ip-51-38-34.eu	http	ESTABLISHED			5,569	96,134,000
chrome.exe	13032	TCP	laptop-4oh6kb2g	55000	whatsapp-cdn-shv-02-bom1.fbcdn.net	https	ESTABLISHED	7	217	11	524
chrome.exe	13032	TCP	laptop-4oh6kb2g	55005	bom0506bom05.1e100.net	https	CLOSE_WAIT				
chrome.exe	13032	TCP	laptop-4oh6kb2g	55127	136.233.9.22.static.js.com	https	CLOSE_WAIT				
chrome.exe	13032	TCP	laptop-4oh6kb2g	55129	whatsapp-cdn-shv-02-bom1.fbcdn.net	https	CLOSE_WAIT			21	1,805
chrome.exe	12380	UDP	LAPTOP-4OH6KB2G	5353	*	*	*				
chrome.exe	12380	UDP	LAPTOP-4OH6KB2G	5353	*	*	*				
chrome.exe	12380	UDPv6	laptop-4oh6kb2g	5353	*	*	*				
chrome.exe	13032	UDP	LAPTOP-4OH6KB2G	57321	*	*	*	2	66	5	1,877
chrome.exe	13032	UDP	LAPTOP-4OH6KB2G	61510	*	*	*	8	3,439	7	3,852
chrome.exe	13032	UDP	LAPTOP-4OH6KB2G	61511	*	*	*	7	3,397	7	3,852
chrome.exe	13032	UDP	LAPTOP-4OH6KB2G	61512	*	*	*	10	4,443	12	6,736
chrome.exe	13032	UDP	LAPTOP-4OH6KB2G	61513	*	*	*	9	4,596	10	2,616
chrome.exe	13032	UDP	LAPTOP-4OH6KB2G	63837	*	*	*	7	3,891	8	2,991
HPJumpStartBridge.exe	12388	TCP	LAPTOP-4OH6KB2G	8733	LAPTOP-4OH6KB2G	0	LISTENING				
HPJumpStartBridge.exe	12388	TCPv6	laptop-4oh6kb2g	8733	laptop-4oh6kb2g	0	LISTENING				
Halts.exe	24556	TCP	laptop-4oh6kb2g	55132	sa-in-f108.1e100.net	imap	CLOSE_WAIT				
fxl_service.exe	15284	TCPv6	[0:0:0:0:0:0:1]	49011	laptop-4oh6kb2g	0	LISTENING				
fxl_service.exe	676	TCP	LAPTOP-4OH6KB2G	49664	LAPTOP-4OH6KB2G	0	LISTENING				
fxl_service.exe	676	TCPv6	laptop-4oh6kb2g	49664	laptop-4oh6kb2g	0	LISTENING				
mchshd.exe	1688	TCP	laptop-4oh6kb2g	55134	161.69.225.17	https	ESTABLISHED	10	3,383	10	930
mDNSResponder.exe	4660	TCP	LAPTOP-4OH6KB2G	5354	LAPTOP-4OH6KB2G	0	LISTENING			15	1,077
mDNSResponder.exe	4660	UDP	laptop-4oh6kb2g	5353	*	*	*				
mDNSResponder.exe	4660	UDPv6	LAPTOP-4OH6KB2G	49666	*	*	*				
mDNSResponder.exe	4660	UDPv6	[0:0:0:0:0:1]	5353	*	*	*				
mDNSResponder.exe	4660	UDPv6	laptop-4oh6kb2g	49667	*	*	*				
MMSSHOST.exe	6188	TCP	LAPTOP-4OH6KB2G	6646	LAPTOP-4OH6KB2G	0	LISTENING				
MMSSHOST.exe	6188	UDP	LAPTOP-4OH6KB2G	6646	*	*	*				
nsuend.exe	5312	TCP	LAPTOP-4OH6KB2G	8834	LAPTOP-4OH6KB2G	0	LISTENING				
nsuend.exe	5312	TCP	LAPTOP-4OH6KB2G	49721	localhost	49722	ESTABLISHED	301	301	302	302
nsuend.exe	5312	TCP	LAPTOP-4OH6KB2G	49722	localhost	49721	ESTABLISHED				
nsuend.exe	5312	TCP	LAPTOP-4OH6KB2G	49741	localhost	49742	ESTABLISHED				
nsuend.exe	5312	TCP	LAPTOP-4OH6KB2G	49742	localhost	49741	ESTABLISHED				
nsuend.exe	5312	TCPv6	laptop-4oh6kb2g	8834	laptop-4oh6kb2g	0	LISTENING				
nsuend.exe	5312	TCPv6	laptop-4oh6kb2g	54402	40.90.188.152	https	ESTABLISHED	4	172	4	696
Oracle.exe	4924	TCP	LAPTOP-4OH6KB2G	49675	LAPTOP-4OH6KB2G	0	LISTENING				
Oracle.exe	4924	TCPv6	[0:0:0:0:0:1]	49674	[0:0:0:0:0:1]	1521	ESTABLISHED	2	1,204	2	604
Oracle.exe	4924	TCPv6	laptop-4oh6kb2g	49675	laptop-4oh6kb2g	0	LISTENING				
services.exe	668	TCP	LAPTOP-4OH6KB2G	49673	LAPTOP-4OH6KB2G	0	LISTENING				
services.exe	668	TCPv6	laptop-4oh6kb2g	49673	laptop-4oh6kb2g	0	LISTENING				
Stack.exe	12754	TCP	laptop-4oh6kb2g	54382	ec2-96-207-117.ap-south-1.compute.amazonaws.com	https	ESTABLISHED	28	1,586	21	3,254
spoolsv.exe	3960	TCP	LAPTOP-4OH6KB2G	49668	LAPTOP-4OH6KB2G	0	LISTENING				
spoolsv.exe	3960	TCPv6	laptop-4oh6kb2g	49668	laptop-4oh6kb2g	0	LISTENING				
svchost.exe	1180	TCP	LAPTOP-4OH6KB2G	5040	LAPTOP-4OH6KB2G	0	LISTENING				
svchost.exe	1468	TCP	LAPTOP-4OH6KB2G	5040	LAPTOP-4OH6KB2G	0	LISTENING				
svchost.exe	1764	TCP	LAPTOP-4OH6KB2G	49666	LAPTOP-4OH6KB2G	0	LISTENING				
svchost.exe	1786	TCP	LAPTOP-4OH6KB2G	49667	LAPTOP-4OH6KB2G	0	LISTENING				

Endpoints: 94 Established: 17 Listening: 33 Time Wait: 1 Close Wait: 5

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

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help



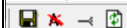
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
nessusd.exe	5312	TCP	0.0.0.0	8834	0.0.0.0	0	LISTENING
nessusd.exe	5312	TCPV6	[0:0:0:0:0:0:0:0]	8834	[0:0:0:0:0:0:0:0]	0	LISTENING
oracle.exe	4924	TCP	0.0.0.0	49675	0.0.0.0	0	LISTENING
oracle.exe	4924	TCPV6	[0:0:0:0:0:0:0:0]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

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

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
chrome.exe	13032	TCP	192.168.1.103	54384	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

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

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help



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

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

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
chrome.exe	13032	TCP	192.168.1.103	54384	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
spoolsv.exe	3960	TCPV6	[0:0:0:0:0:0:0:0]	49668	[0:0:0:0:0:0:0:0]	0	Listening

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

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
spoolsv.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	*	*

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

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:

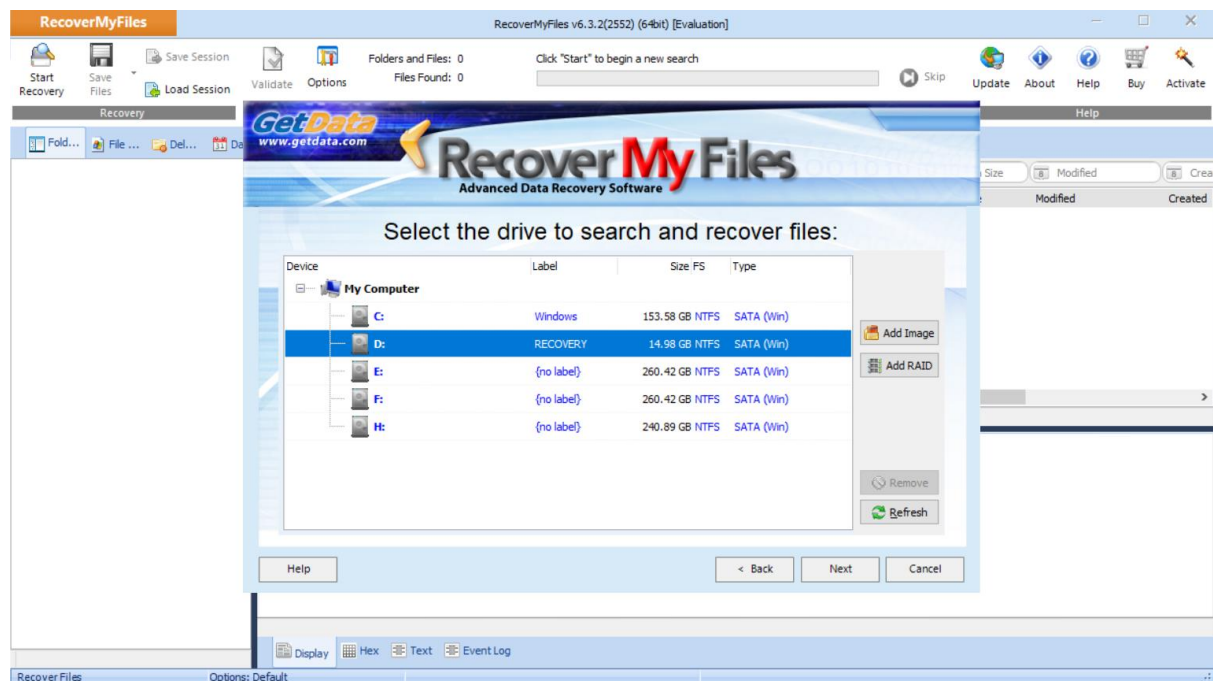
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	12380	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*
mDNSResponder.exe	4660	UDPV6	[0:0:0:0:0:0:0:1]	5353	*	*
mDNSResponder.exe	4660	UDPV6	[0:0:0:0:0:0:0:0]	49667	*	*
scvhost.exe	4496	UDPV6	[0:0:0:0:0:0:0:0]	500	*	*
scvhost.exe	3520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

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

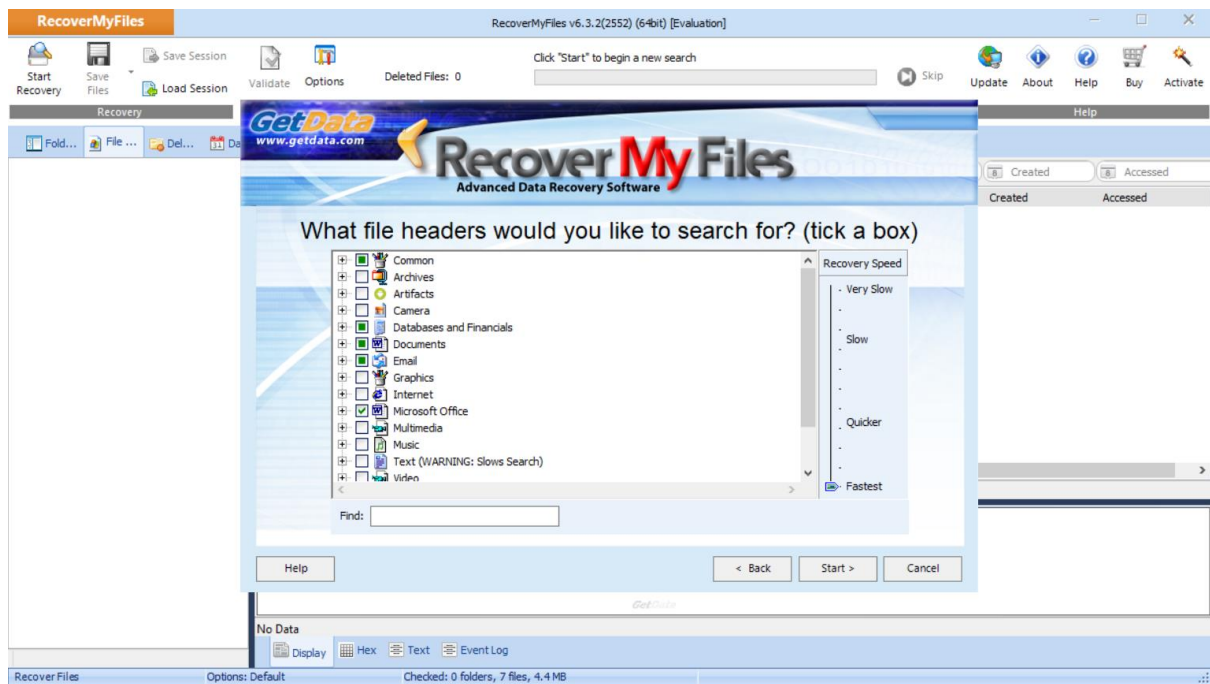
Selected \D: drive to search files:



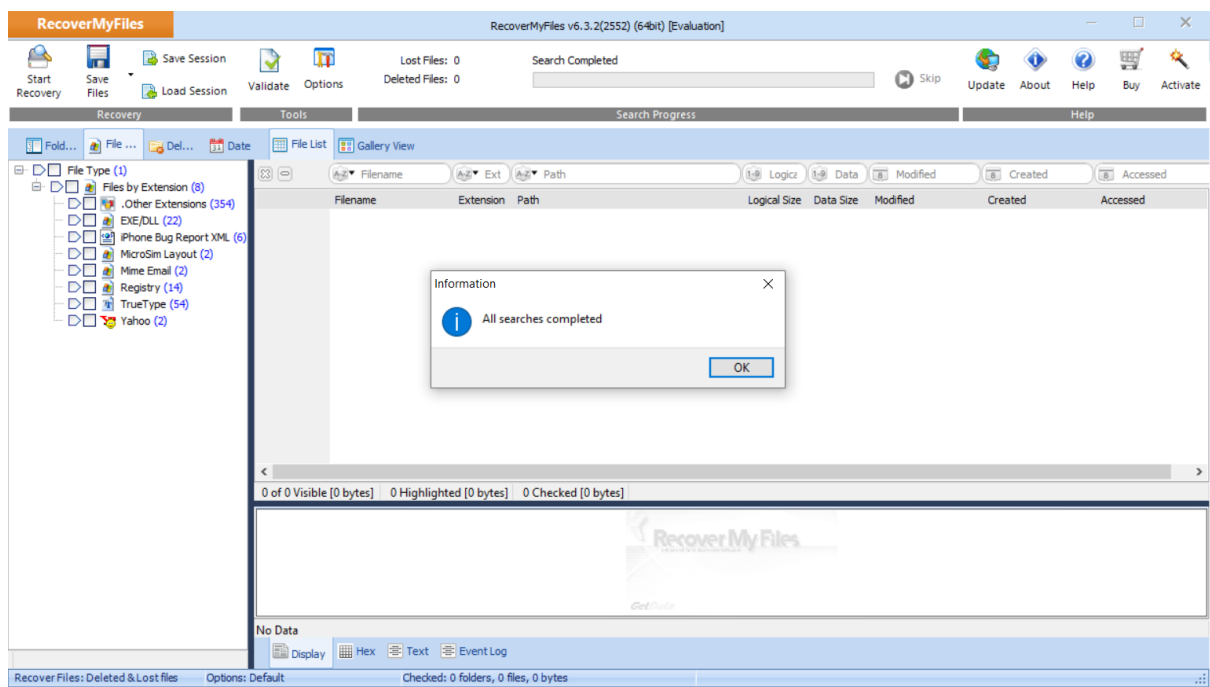
Selected "Search for deleted files, then search for selected "Lost File" types." option:



Selected "Microsoft Office" file header:



Search is completed:



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

RecoverMyFiles

RecoverMyFiles v6.3.2(2552) (64bit) [Evaluation]

Start Recovery

Save Files

Save Session

Load Session

Validate

Options

Deleted Files: 0

Search Completed

Skip

Update

About

Help

Buy

Activate

Recovery

Tools

Search Progress

Help

Fold...File...Del...Date

File List

Gallery View

File Type (1)

Files by Extension (8)

EXE/DLL (22)

iPhone Bug Report.XML (6)

MicroSim Layout (2)

Mime Email (2)

Registry (14)

TrueType (54)

Yahoo (2)

Filename	Extension	Path	Logical Size	Data Size	Modified	Created	Accessed
1 Reserve.log	log	Root\preload\RM_Reserve\	159	159	09-09-2014 04:24:50	04-11-2017 12:08:14	04-11-2017 12:08:14
2 INSTALL_PASS1.log	log	Root\preload\RM_Reserve\system.sav\Logs\	1,129,809	1,130,496	03-07-2017 22:42:56	04-11-2017 12:08:14	04-11-2017 12:08:14
3 ForF11.log	log	Root\preload\RM_Reserve\system.sav\Logs\	6,425	8,192	31-07-2018 16:41:44	31-07-2018 16:41:44	31-07-2018 16:41:44
4 INSTALL.LOG	LOG	Root\preload\RM_Reserve\system.sav\util\	3,381,265	3,383,296	04-11-2017 13:47:34	04-11-2017 12:08:14	04-11-2017 12:08:14
5 bcd.LOG	LOG	Root\Boot\	32,768	32,768	04-11-2017 12:08:16	04-11-2017 12:08:16	04-11-2017 12:08:16
6 bcd.LOG	LOG	Root\EFI\Microsoft\Boot\	20,480	20,480	04-11-2017 12:08:16	04-11-2017 12:08:16	04-11-2017 12:08:16
7 tracking.log	log	Root\System Volume Information\	20,480	20,480	04-11-2017 11:25:14	04-11-2017 11:21:38	04-11-2017 11:21:38
8 Reserve.log	log	Root\preload\RM_Reserve\	159	159	09-09-2014 04:24:50	04-11-2017 12:08:14	04-11-2017 12:08:14
9 INSTALL_PASS1.log	log	Root\preload\RM_Reserve\system.sav\Logs\	1,129,809	1,130,496	03-07-2017 22:42:56	04-11-2017 12:08:14	04-11-2017 12:08:14
10 INSTALL.LOG	LOG	Root\preload\RM_Reserve\system.sav\util\	3,381,265	3,383,296	04-11-2017 13:47:34	04-11-2017 12:08:14	04-11-2017 12:08:14
11 bcd.LOG	LOG	Root\Boot\	32,768	32,768	04-11-2017 12:08:16	04-11-2017 12:08:16	04-11-2017 12:08:16
12 bcd.LOG	LOG	Root\EFI\Microsoft\Boot\	20,480	20,480	04-11-2017 12:08:16	04-11-2017 12:08:16	04-11-2017 12:08:16
13 tracking.log	log	Root\System Volume Information\	20,480	20,480	04-11-2017 11:25:14	04-11-2017 11:21:38	04-11-2017 11:21:38
14 ForF11.log	log	Root\preload\RM_Reserve\system.sav\Logs\	6,425	8,192	31-07-2018 16:41:44	31-07-2018 16:41:44	31-07-2018 16:41:44

14 of 14 Visible [8.8 MB] 0 Highlighted [0 bytes] 14 Checked [8.8 MB]

Display

Hex

Text

Event Log

Recover Files: For deleted files Options: Default Checked: 0 folders, 7 files, 4.4 MB
