

**CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE - 4**

DATE: 06.08.2020

Installing, Understanding and Exploring the functionalities of the following

Software:

1. Monitoring Ports and Outbound Connections - TCPView & Curports

Download Sources :

- <https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview>
- <https://www.nirsoft.net/utils/cports.html>

References :

- <https://www.vladan.fr/tcpview-and-curports-two-handy-tools-to-track-open-ports/>
- <https://sourcedaddy.com/windows-7/tcpview.html>

Implement the following :

- Resolve Addresses
- Refresh rate Change
- Whois
- Process Properties
- Kill Processes
- Close Connections
- Copy - Save the information in HTML File, XML File, Text File

2. Recovering any Deleted /Lost Files - Recover MyFiles

Download Source:

- <http://www.recovermyfiles.com/recovery-checklist.php>

References :

- <http://www.recovermyfiles.com/data-recovery-help/software.php>

**CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE - 4**

DATE: 06.08.2020

Functionalities :

- Recover Drive
- Recover Files
- Options to try : Deleted File; Lost File; Corrupted File; Hard disk – Formatted Disk, USB Drive, SD Card.

3. Web Activity Monitoring and Recording - Power Spy

Note :

Install Windows as a Guest OS inside your VMWare and in that Guest OS execute the following: (or)

Temporarily Disable any AV software on your machine/Try in VM – NAT mode of Network Adapter

Download Source :

<https://www.ematrixsoft.com/download.php?p=power-spy-software>

Reference Source:

- <https://www.youtube.com/watch?v=QXj5r7B56EU>

Note :

- In a word document, copy the command you have used for each task and show the screen shot for each step output.
- The IP address of your machine has to appear (ipconfig/ifconfig command) in each screen shot (For reliability)