**Cyber security Lab tool**

**Exercises** 9:

Perform Network analysis using the Network Miner tool

Aim:

extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files Perform Network analysis

Features:

* Network Miner is an [open source](https://www.netresec.com/?page=NetworkMinerSourceCode) network forensics tool .
* Network Miner can also be used to capture live network traffic by sniffing a network interface.
* Detailed information about each IP address in the analyzed network traffic is aggregated to a network host inventory, which can be used for passive asset discovery as well as to get an overview of which devices that are communicating.
* Network Miner is primarily designed to run in Windows, but can also be used in [Linux](https://www.netresec.com/?page=Blog&month=2014-02&post=HowTo-install-NetworkMiner-in-Ubuntu-Fedora-and-Arch-Linux).
* Network Miner has, become a popular tool among incident response teams as well as law enforcement. Network Miner is today used by companies and organizations all over the world.

How to download:

1. Open bellow web site

<https://www.netresec.com/?page=NetworkMiner>

1. Click on down network miner
2. Exact the file
3. Run that file with administrator