Volatile evidence collection - Linux & Windows

Objectives:

At the end of this episode, I will be able to:

Understand what the concept of volatile evidence collection is.

Explain why using specific tools for both Windows and Linux should be a part of the volatile evidence collection steps taken by the IH&R team.

Identify how to install and use the various tools demonstrated.

External Resources:

Volatile evidence collection

```
Windows -

    systeminfo.exe

    date /t & time /t

    doskey /history

    net statistics workstation

    netstat -ab
    netstat -ano
    netstat -r

    Process explorer - download link:
https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer


Linux -

    uname -a

    lshw -short

    w

    last -a

    apt install net-tools --> netstat  |  ifconfig -a

    lsof

    lsmod

    apt install auditd -->  aureport
    ausearch -ui <userid> --interpret

    /etc/cron.daily

    Home directory and press Ctrl + H --> .bash_history

    ps auxww
```