Universiti Malaysia PAHANG

Computer Forensic & Investigation

Network Forensics Overview

Editors
Dr. Abdulghani Ali Ahmed
Wan Nurulsafawati Wan Manan
Faculty of Computer Systems & Software Engineering
abdulghani@ump.edu.my

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

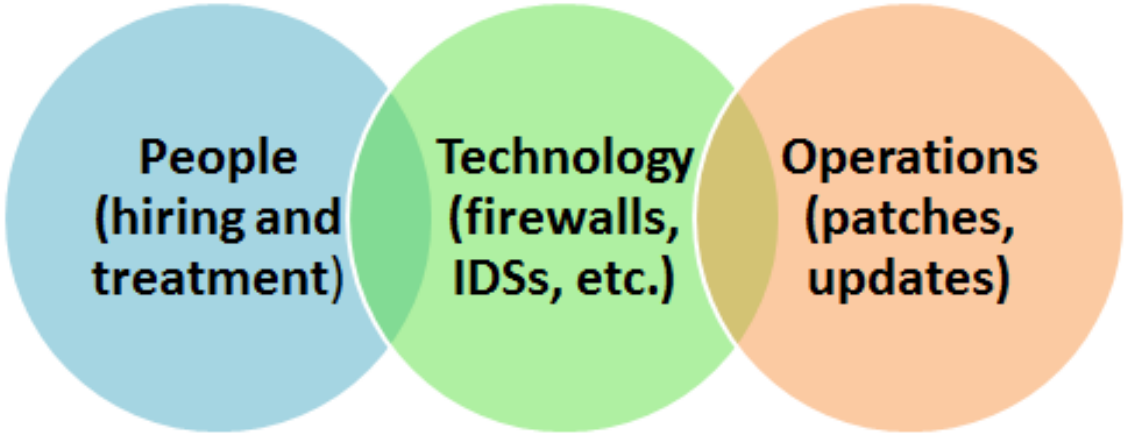
Network Forensics Overview

- **Network forensics**
  - To study attack behavior, network incoming and outgoing traffic is investigated.
  - Hackers / invaders leave trail behind
- Define the reason of malicious traffic in the network.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Secured the Network

- **Layered network defense strategy**
  - OSI layers
- **Defense in depth (DiD)**
  - There are 3 protection strategies:



Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Secured the Network (cont.)

- Testing both networks and servers is important
- Forensic investigator should regularly update his knowledge about the recent methods and strategies of hackers.
  - What kind of methods local attackers use to penetrate networks

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

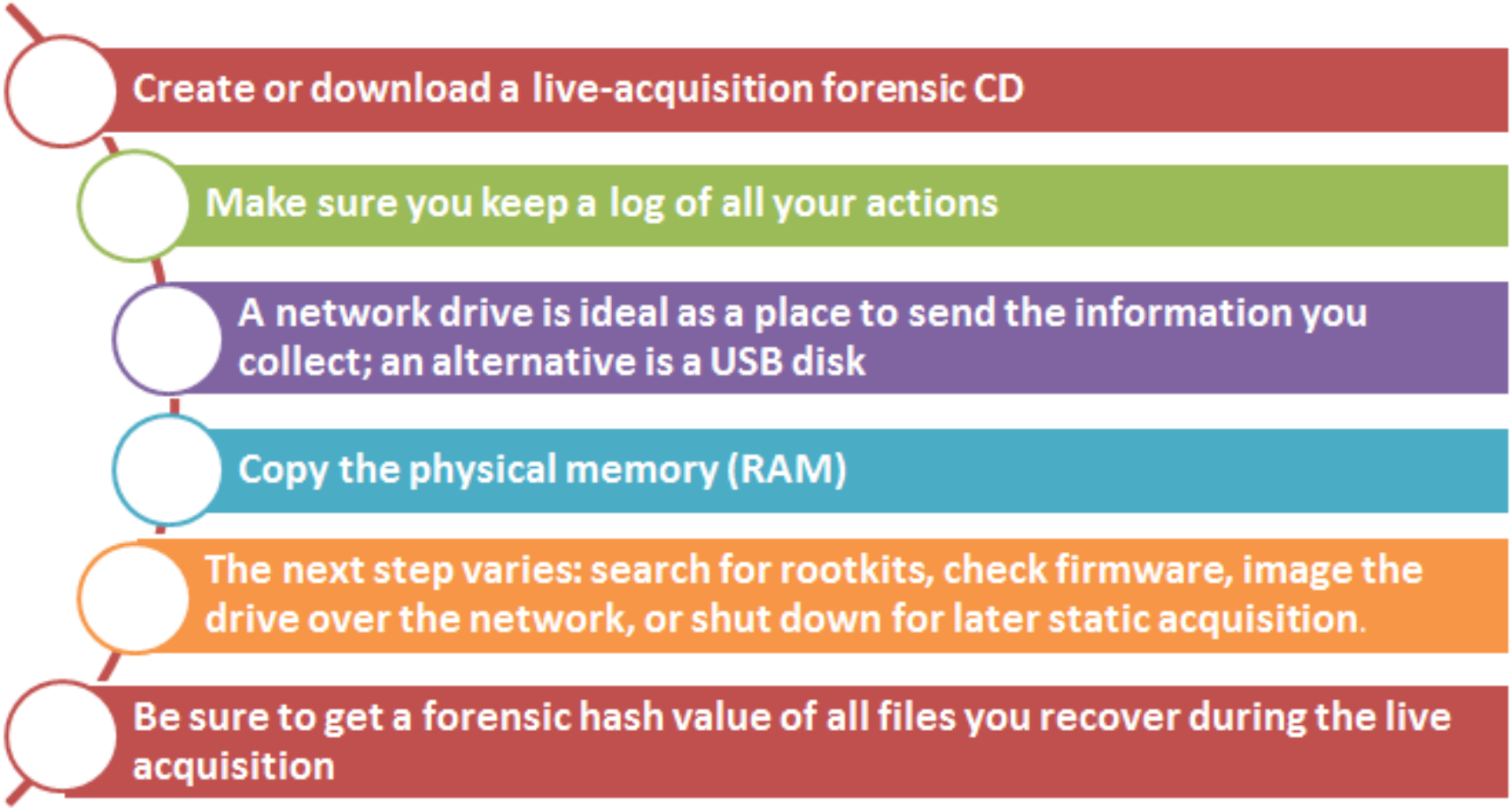
Performing Live Acquisitions

- Live Acquisition is suitable when dealing with active hackers.
- Live acquisition is necessary to capture possible data/evidence before taking a system offline.
  - Hackers may leave evidential data only in running system or RAM
- Live acquisitions don't necessarily practice standard procedure of forensics

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

How to Perform Live Acquisitions

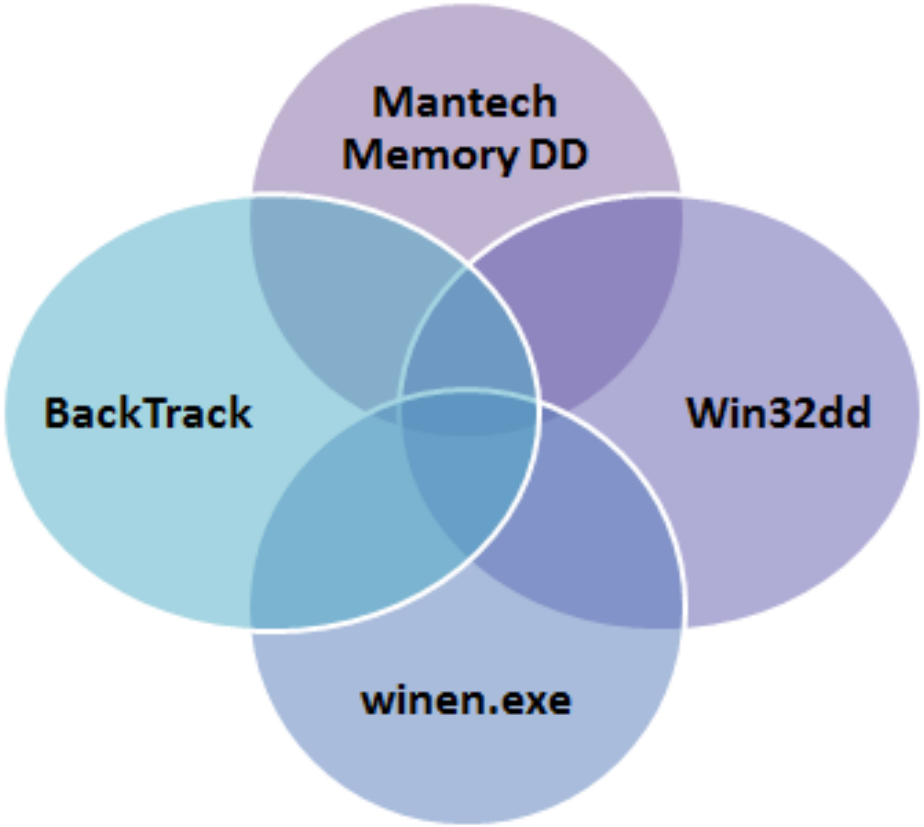
Steps



Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Performing a Live Acquisition in Windows

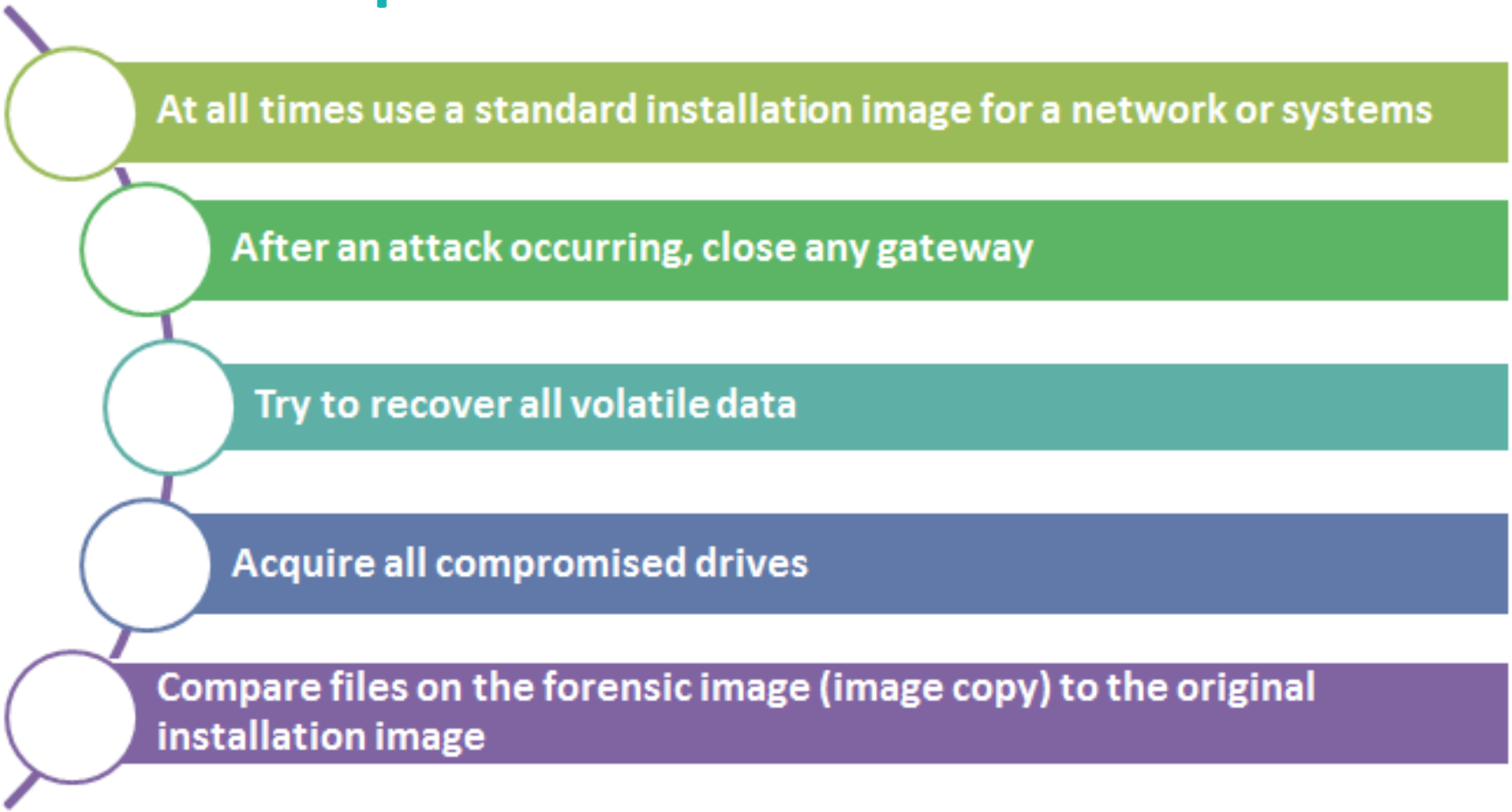
Tools of capturing RAM data



Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Developing Standard Procedures for Network Forensics

- **Standard procedure**



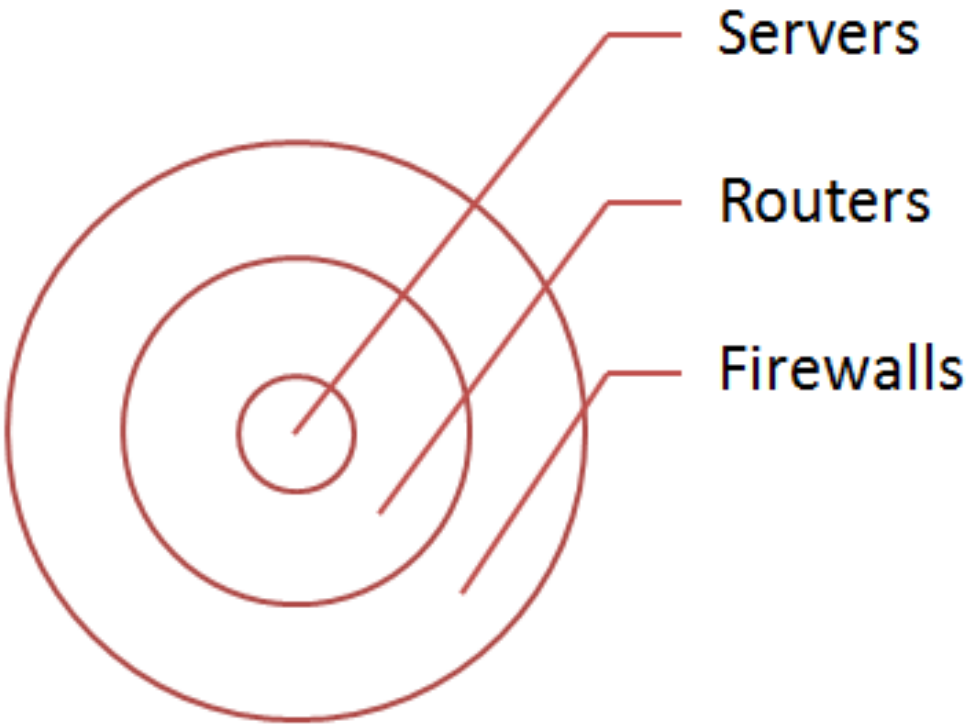
Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Developing Standard Procedures for Network Forensics (cont.)

- **Computer forensics**
  - Investigate the copied image in order to discover if there is any change on the content.
- **Network forensics**
  - Restore disk drives to recognize hacker's violence.
- **Practice strategy of quarantined system**
  - Make sure to prevent malicious software to affect other systems

Reviewing Network Logs

- Monitor inbound and outbound packets at:



Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Reviewing Network Logs

- **Many tools can be used to investigate traffic**
  - Such as Tcpdump tool.
- **Attackers have open targets**
  - Disclose information about other companies may put them at risk of attack

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Using Network Tools

- **Sysinternals**
  - A collection of open source tools for investigating Windows products such as:
  - **RegMon**
  - **Process Explorer**
  - **PsTools**

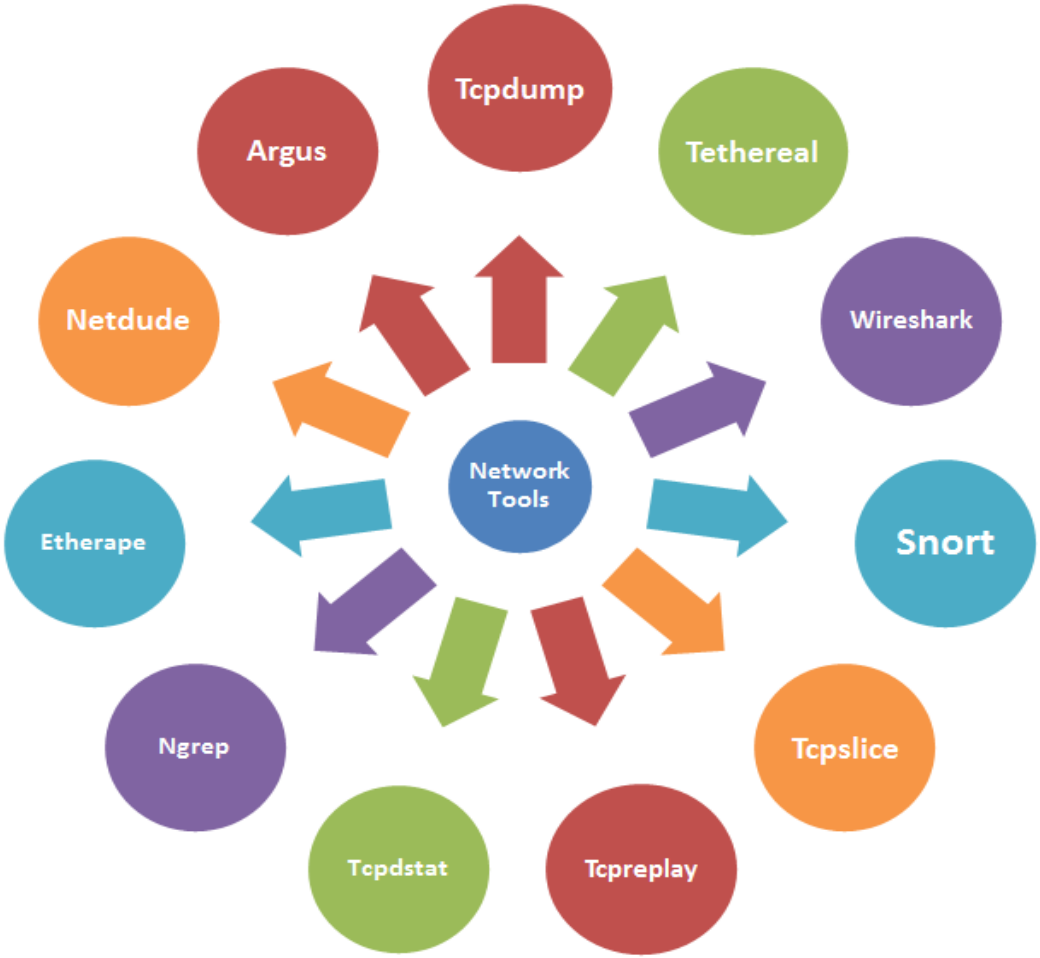
Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Using Packet Sniffers

- **Packet sniffers**
  - Hardware or software to monitor network packets.
  - Typically applied at layer 2 or 3 in OSI model.
  - Format is similar to PCAP
  - Packet headers can be inspected to identify some of network packets by inspecting the TCP flags fields.

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Tools



Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).

Questions

?

Source: (Nelson et al., Guide to Computer Forensics and Investigations 4th Edition, 2015).