Topic 3 Acquisition, examination and analysis of evidence in computers and networks Part 6

Learning Outcome

After successfully completing this lecture, you will be able to

- Describe and plan the traffic data and network event logs acquisition
- Acquire the network traffic data and network event logs

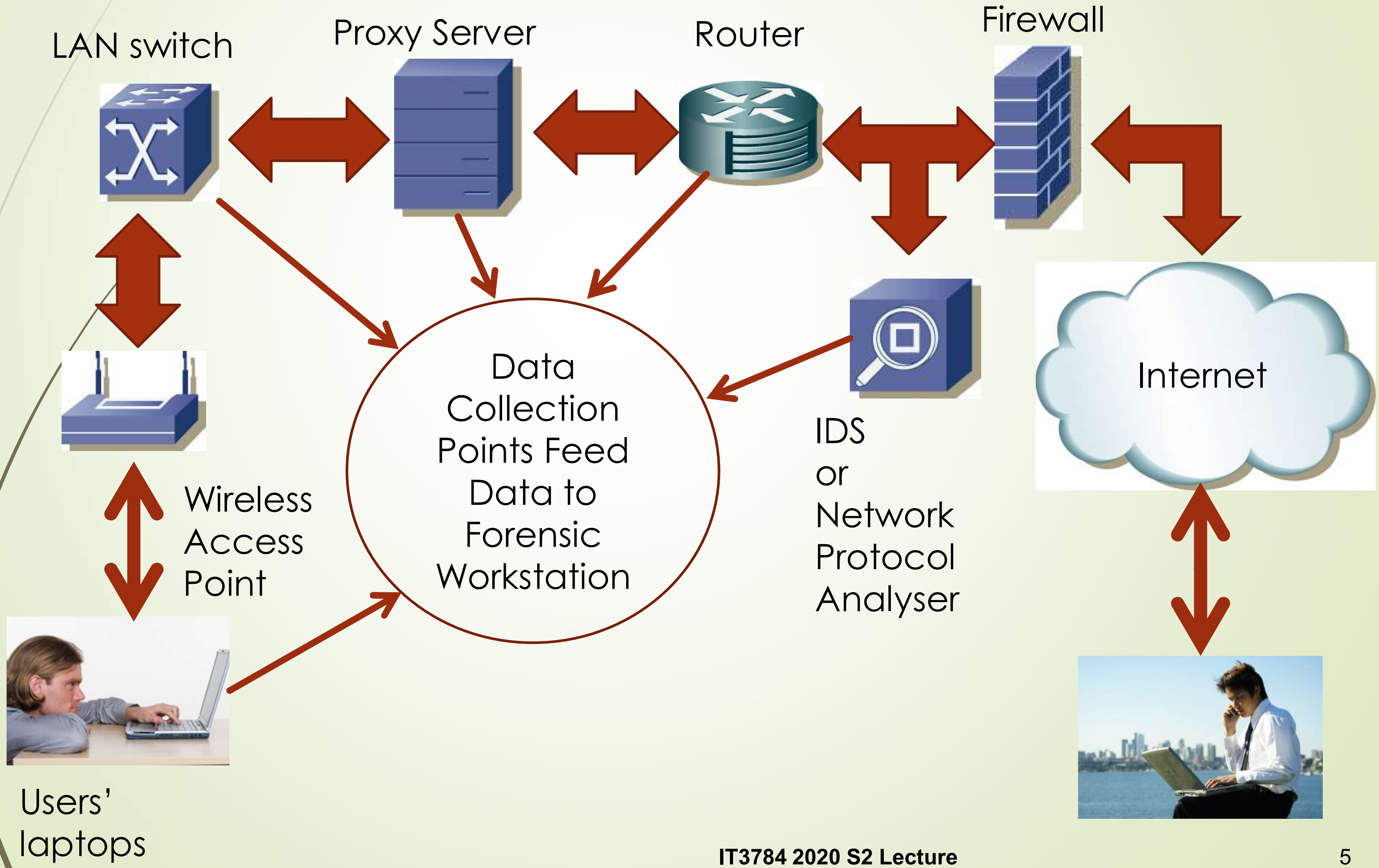
Road Map

- Acquire Network Traffic Data
- Acquire Network events

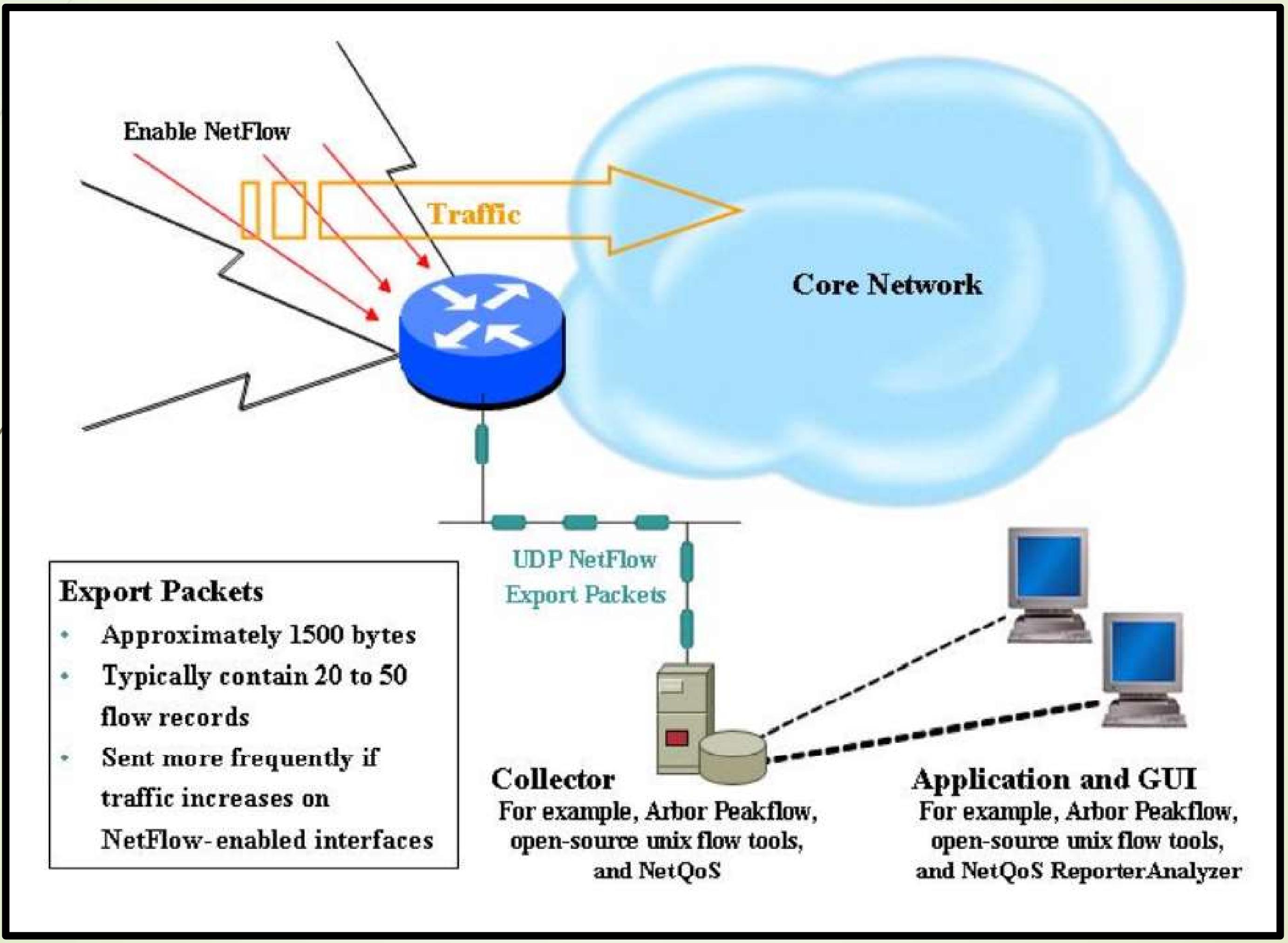
Where can we capture (acquire) network traffic?

- Warning: You must obtain the permission from the owner of the network BEFORE collection of data packets from the network.
- Run a network monitoring or a network protocol analyser tool such as Wireshark, tcpdump or IDS like Snort
  - At the routers, LAN switches, end points, a network server such as proxy server to collect
    - Broadcast traffic, such as ARP and BROWSER, and
    - Unicast traffic sent and received at the end point
  - At a forensic PC connected to the mirror port of a Internet Router, to collect
    - Unicast traffic between computers in the untrusted Internet and the computers in the trusted intranet

Network Data Collection Points


LAN switch
Proxy Server
Router
Firewall
Wireless Access Point
Data Collection Points Feed Data to Forensic Workstation
IDS or Network Protocol Analyser
Internet
Users' laptops

Cisco Router NetFlow captures ALL network traffic packets



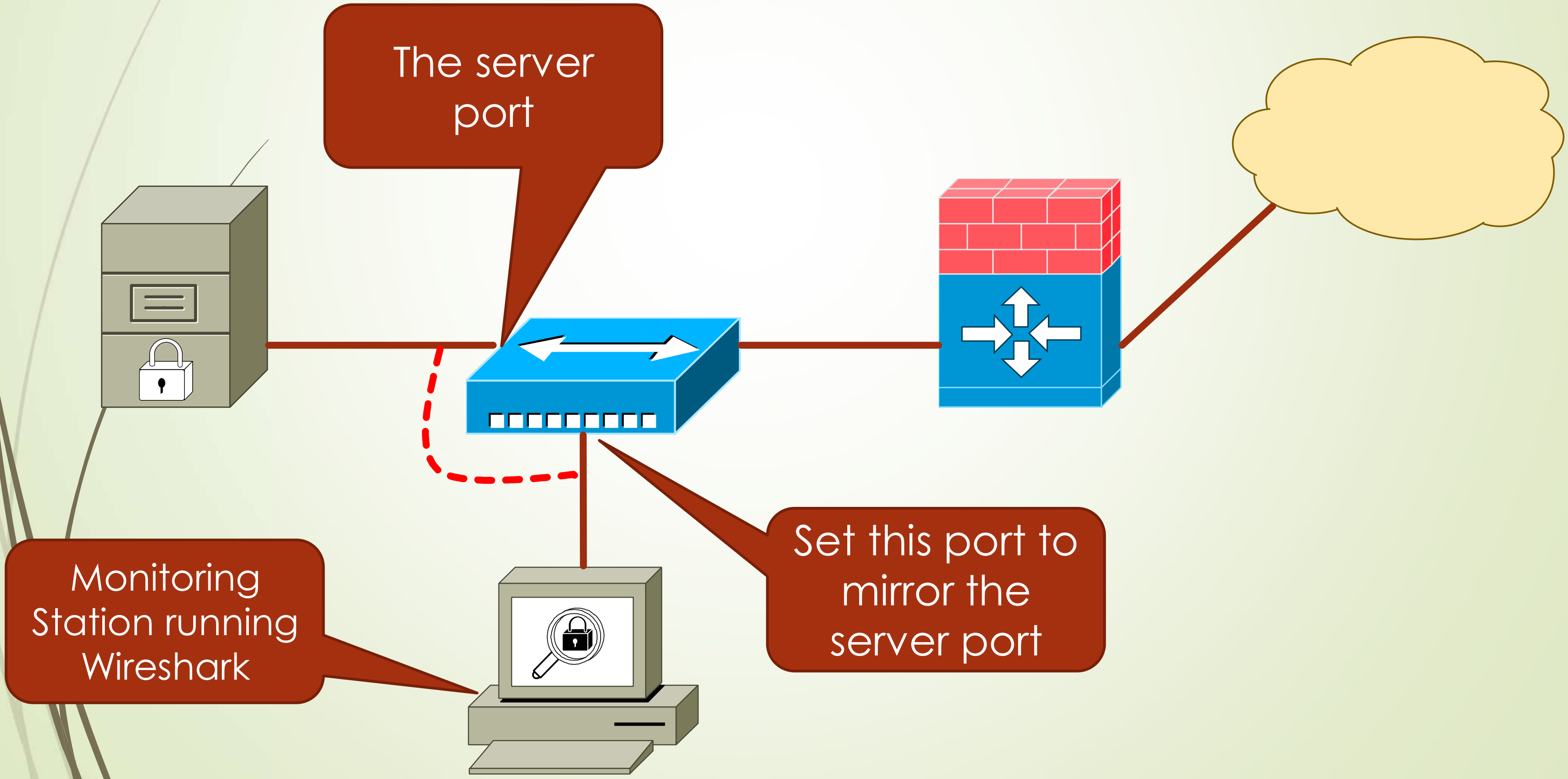
Export Packets

- Approximately 1500 bytes
- Typically contain 20 to 50 flow records
- Sent more frequently if traffic increases on NetFlow-enabled interfaces

Collector
For example, Arbor Peakflow, open-source unix flow tools, and NetQoS

Application and GUI
For example, Arbor Peakflow, open-source unix flow tools, and NetQoS ReporterAnalyzer

Collect Traffic Data Through Port Mirroring



The server port

Set this port to mirror the server port

Monitoring Station running Wireshark

How to Collect Traffic Data

- Full-Packet Capture
  - Use Wireshark for full-packet capture
  - Use tshark or tcpdump for selective packets capture
- Protocol Header Capture
  - Use NetFlow to capture only the content of the protocol headers but not the protocol data

Example:
Tshark Commands

tshark -w fullcapture.pcap

- To capture all traffic data and store into the file fullcapture.pcap

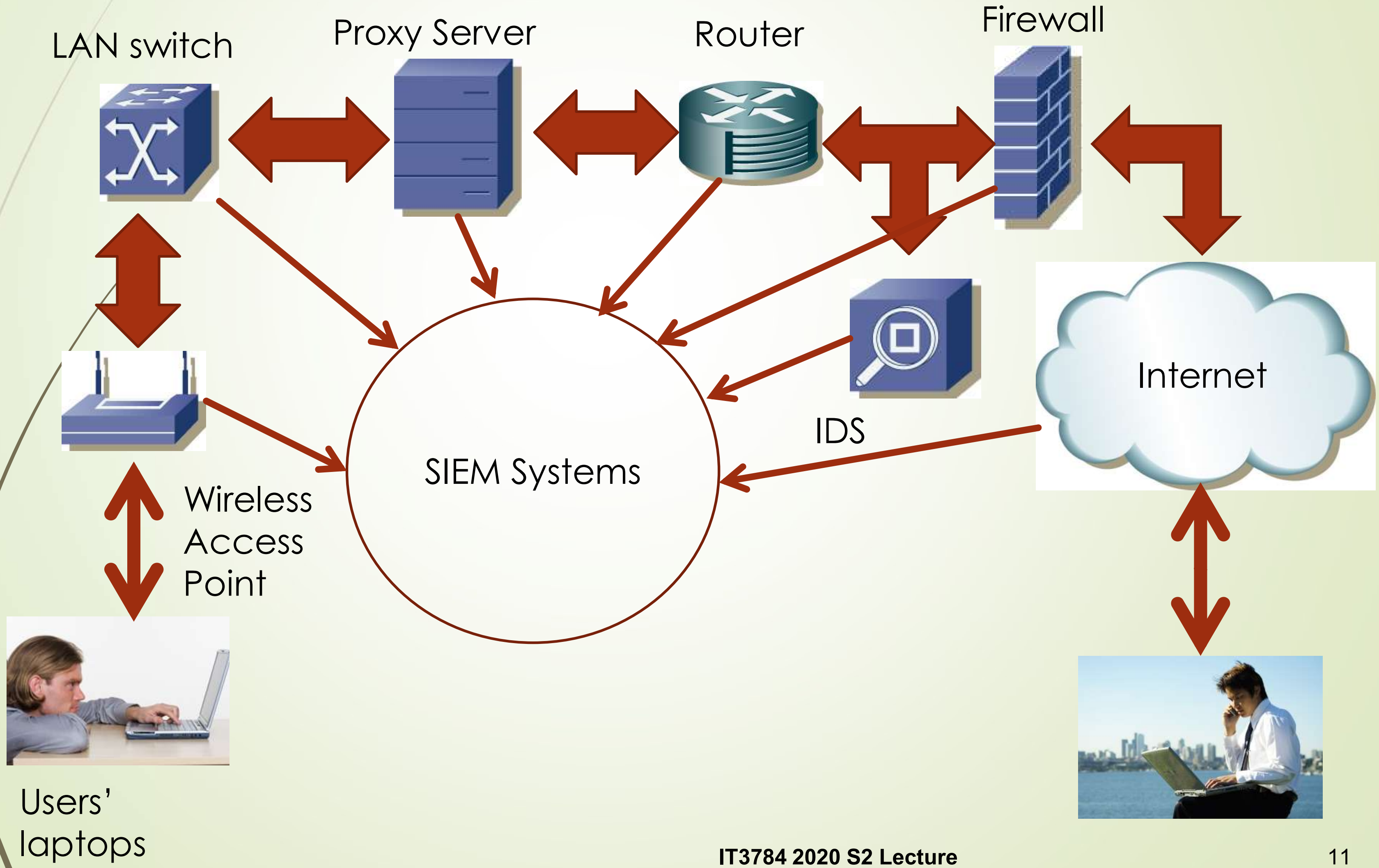
tshark -f "net 172.20.128.0/21“ –w Sub1.pcap

- To capture traffic data from/to the computers in the subnet 172.20.128.0/21 and store into the file Sub1.pcap
    - Full tshark manual at https://www.wireshark.org/docs/man-pages/tshark.html

Where can we capture network events?

- Warning: You must obtain the permission from the owner of the network BEFORE collection of data packets from the network.
- Run a security information and event management (SIEM) servers, such as Splunk, to collect, examine and analysis network events (evidence)
- Network events
  - Windows Servers Events (System, Applications and Security)
  - Network devices events from routers, firewalls, IDS, proxy servers, LAN switches and WiFi Access Points

Network Events Collection Points



Syslog
(Read the details in Wikipedia.org)

- A common system/network events logging system
- History
- System message components
  - Facility
  - Severity level
  - Message
- Logger
- Network Protocol
- Internet Standard documents

13

Syslog

- Learn more on syslog System message components and deployment from youtube
- Answer review questions on syslog

14

Summary

- Network evidence includes network traffic data and network events
- Network traffic data acquired by IDS or network protocol analyser.

15

References

1. Section 6 “Using Data from Network Traffic”, Guide to Integrating Forensic Techniques into Incident Response SP800-86 NIST, csrc.nist.org
2. Syslog, Wikipedia.org