

Module 12

Network Traffic Monitoring

Module Objectives

1. Understanding the Need for and Advantages of Network Traffic Monitoring
2. Understanding the Network Traffic Signatures
3. Understanding the Categories of Suspicious Traffic Signatures
4. Overview of Attack Signature Analysis Techniques
5. Understanding Network Monitoring for Suspicious Traffic
6. Overview of Various Network Monitoring Tools



Module Flow



1. **Understand the Need and Advantages of Network Traffic Monitoring**
2. **Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic**
3. **Perform Network Monitoring for Suspicious Traffic**

Network Traffic Monitoring



- Network monitoring is a **retrospective security approach** that involves monitoring a network for abnormal activities, performance issues, bandwidth issues, etc.
- Network monitoring is an integral part of **network security** and is a demanding task within the network security operations of organizations
- Continuous network traffic monitoring and analysis are required for effective **threat detection**

Need for Network Monitoring

Even when security tools are in place, attackers can find ways to **bypass** such security mechanisms to enter the network

Security tools generally use **signature-based detection** techniques. Hence, they are often unable to identify continuously changing attack signatures/patterns

Security tools are generally not designed to identify **behavioral anomalies** and are unable to detect activities of attackers that are initiated before and during an attack





Advantages of Network Monitoring

Monitoring network traffic helps in

- Understanding how data flows in a network
- Optimizing network performance
- Avoiding bandwidth bottlenecks
- Detecting signs of malicious activity
- Finding unnecessary and vulnerable applications
- Investigating security breaches

Module Flow



1. **Understand the Need and Advantages of Network Traffic Monitoring**
2. **Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic**
3. **Perform Network Monitoring for Suspicious Traffic**

Network Traffic Signatures

- A signature is a set of **traffic characteristics** such as a source/destination IP address, ports, Transmission Control Protocol (TCP) flags, packet length, time to live (TTL), and protocols. Signatures are used to define the type of activity on a network



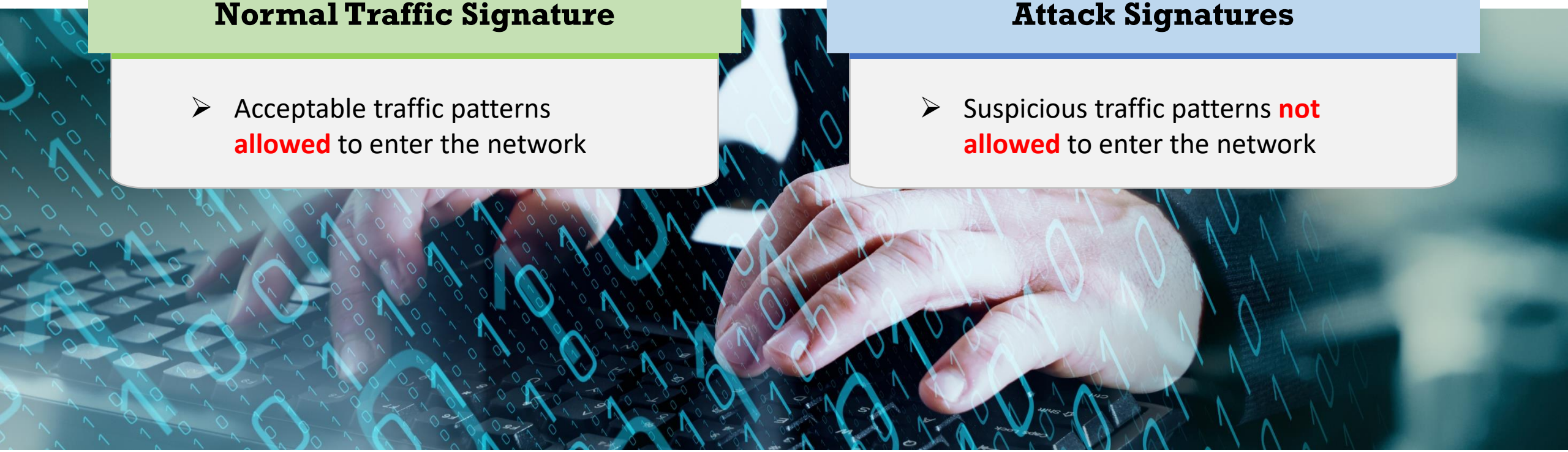
Types of Signatures

Normal Traffic Signature

- Acceptable traffic patterns **allowed** to enter the network

Attack Signatures

- Suspicious traffic patterns **not allowed** to enter the network





Baselining Normal Traffic Signatures

- A network baseline is the **accepted behavior** for normal network traffic. It is a benchmark to differentiate between normal and suspicious traffic
- Network traffic baselines differ between organizations and change over time according to the **operating environment** and prevailing **threat scenario**

Some considerations to create a baseline for normal traffic:

- TCP/IP communication involves a three-way handshake for normal traffic
- A SYN flag appears at the beginning and a FIN flag at the end of a connection
- All conversations originating inside the demilitarized zone (DMZ) are trusted traffic items
- Any traffic violating the network policies is malicious traffic; e.g., the existence of File Transfer Protocol (FTP) traffic when this type is restricted indicates a potential issue

Categories of Suspicious Traffic Signatures

Informational

Traffic containing certain signatures that may appear suspicious but **might not be malicious**

Reconnaissance

Traffic containing certain signatures that indicate an attempt to **gain information**



Unauthorized Access

Traffic containing certain signatures that indicate an attempt to **gain unauthorized access**

Denial of Service

Traffic containing certain signatures that indicate a DoS attempt that **floods** a server with a large number of requests

Attack Signature Analysis Techniques

Content-based signature analysis

- Attack signatures are contained in **packet payloads**



- Check for specific **strings** occurring in the suspicious payload



Context-based signature analysis

- Attack signatures are contained in **packet headers**



- Inspect packets for unusual/suspicious header information such as the following:
  - Source and destination IP addresses
  - IP options, protocols, and checksums
  - Source and destination port numbers
  - IP fragmentation flags, offset, or identification

Atomic-signature-based analysis

- **Single-packet** analysis is sufficient to detect attack **signatures**



Composite-signature-based analysis

- **Multiple-packet** analysis is required to detect attack **signatures**



Module Flow



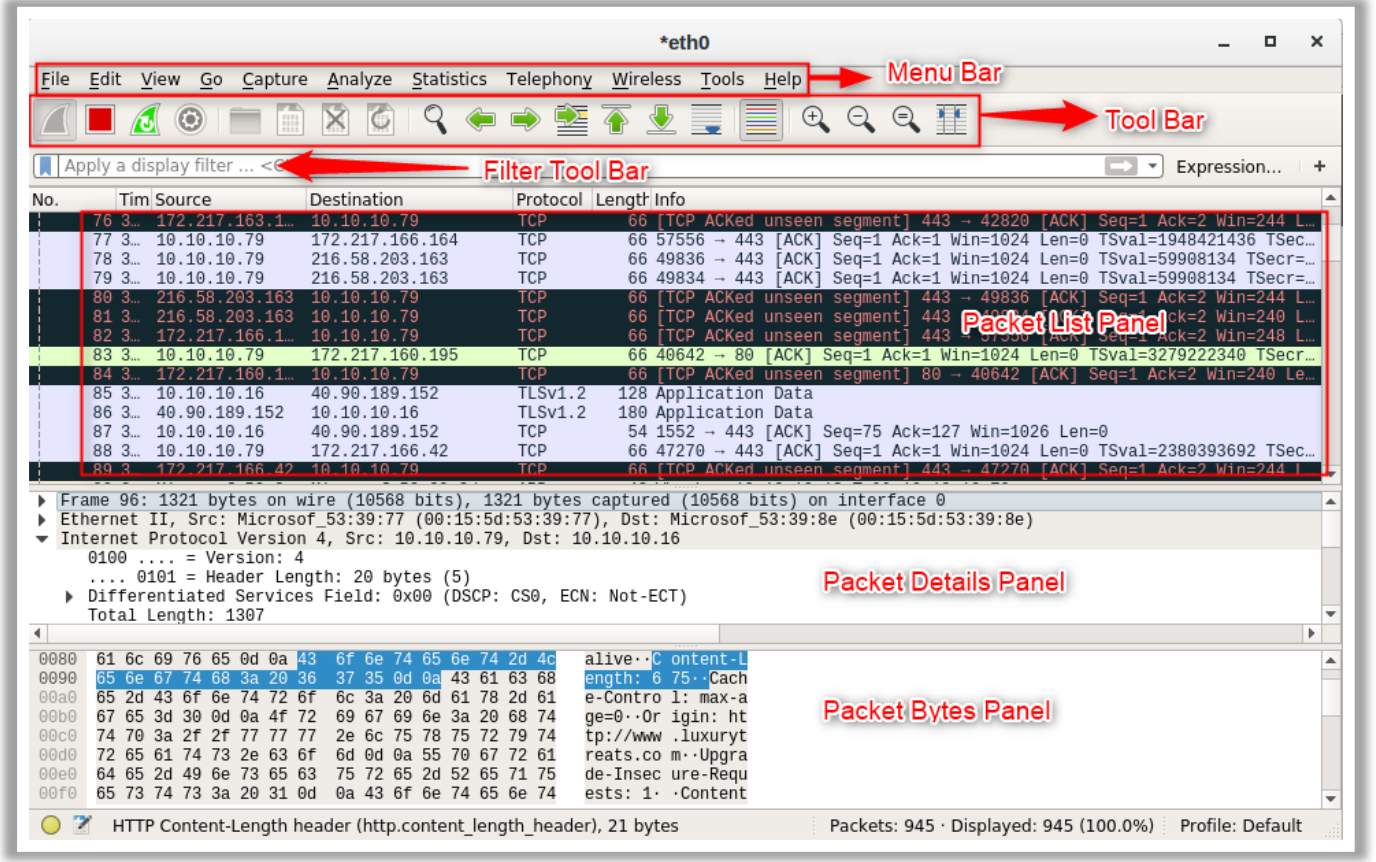
1. Understand the Need and Advantages of Network Traffic Monitoring
2. Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic
3. Perform Network Monitoring for Suspicious Traffic

Wireshark

- **Wireshark** is a widely used network sniffer for network monitoring and analysis
- It captures and intelligently browses the traffic on a network

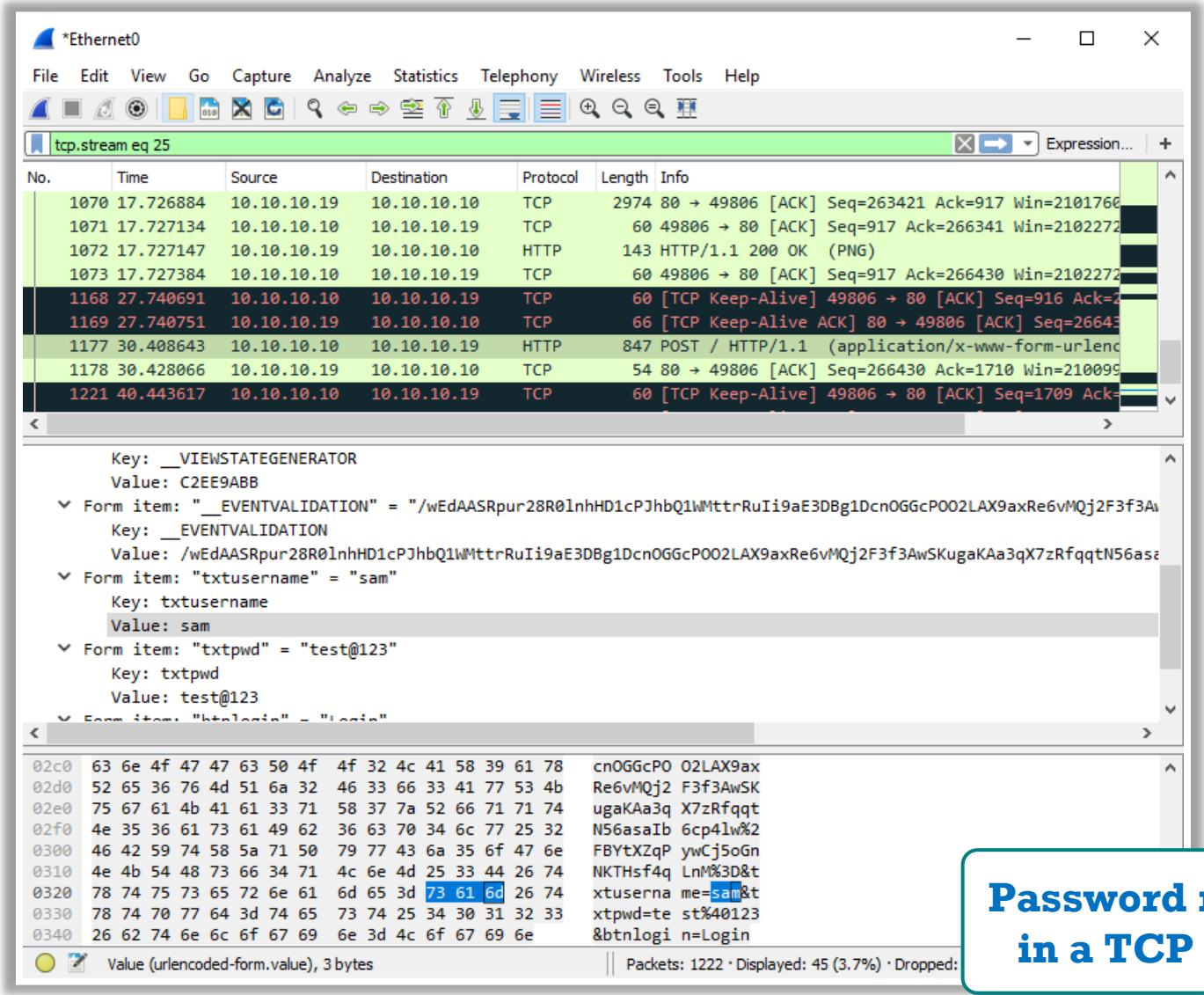
Components of Wireshark

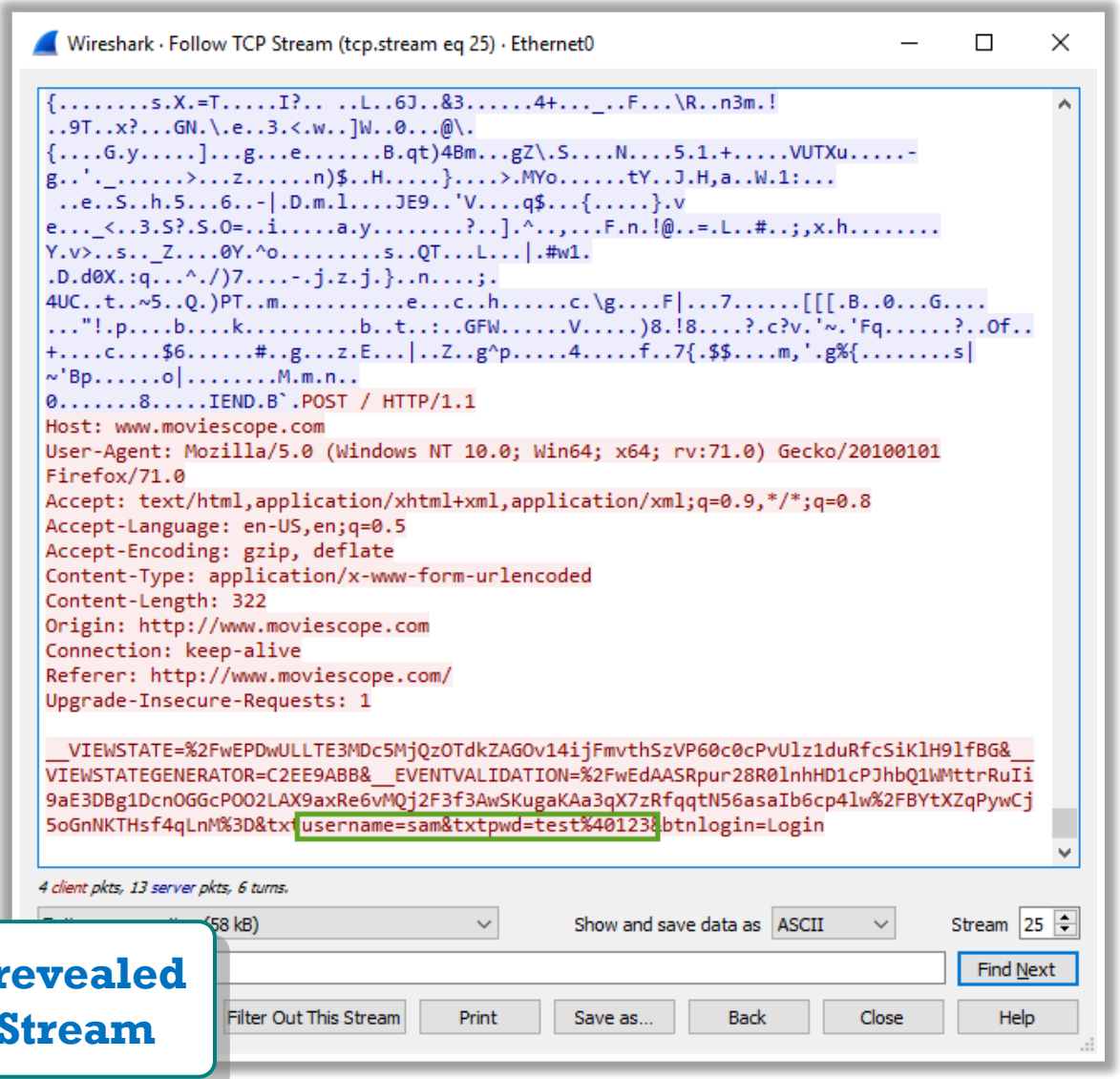
- ✓ **Menu bar**: Hosts the features of Wireshark
- ✓ **Toolbar**: Hosts the most frequently used tools and icons
- ✓ **Filter toolbar**: Filters the traffic based on filter options
- ✓ **Packet list panel**: Displays the captured packets
- ✓ **Packet details panel**: Displays detailed information about the captured packets at a granular level
- ✓ **Packet byte panel**: Displays the captured packet's bytes in a hex dump format



https://www.wireshark.org

Follow TCP Stream in Wireshark





Password revealed in a TCP Stream

Display Filters in Wireshark

- Display filters are used to **change the view of packets** in the captured files

1. **Display Filtering by Protocol** → Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, or ip

2. **Monitoring the Specific Ports** →
   - `tcp.port==23`
   - `ip.addr==192.168.1.100 machine`
     `ip.addr==192.168.1.100 && tcp.port=23`

3. **Filtering by Multiple IP Addresses** →
   `ip.addr == 10.0.0.4 or`
   `ip.addr == 10.0.0.5`

4. **Filtering by IP Address** →
   `ip.addr == 10.0.0.4`

5. **Other Filters** →
   - `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
   - `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
   - `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Additional Wireshark Filters

01 `tcp.flags.reset==1`
Displays all TCP resets

02 `udp contains 33:27:58`
Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset

03 `http.request`
Displays all HTTP GET requests

04 `tcp.analysis. Retransmission`
Displays all retransmissions in the trace

05 `tcp contains traffic`
Displays all TCP packets that contain the word “traffic”

06 `!(arp or icmp or dns)`
Masks out arp, icmp, dns, or other protocols and allows you to view traffic of your interest

07 `tcp.port == 4000`
Sets a filter for any TCP packet with 4000 as a source or destination port

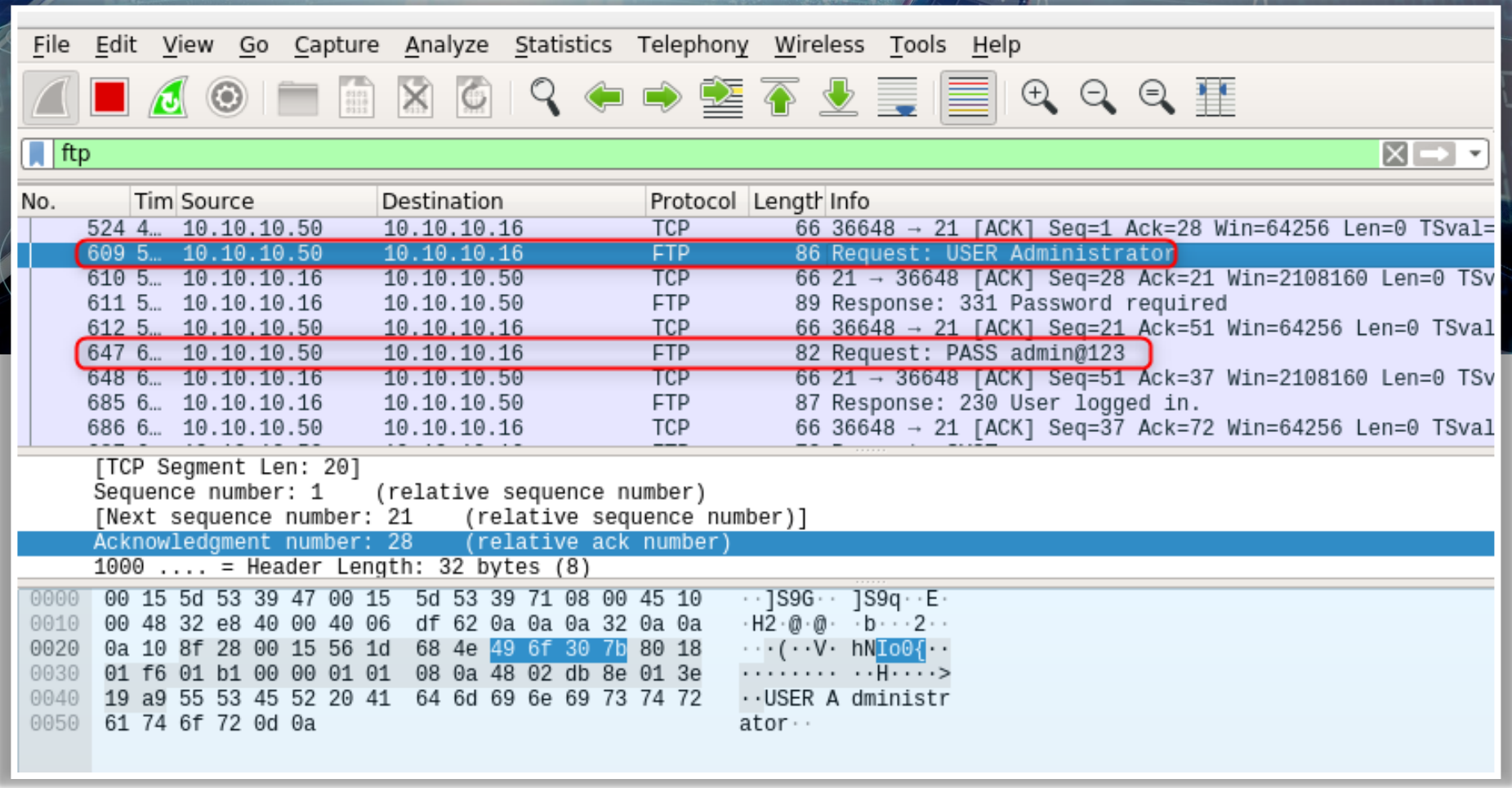
08 `tcp.port eq 25 or icmp`
Displays only SMTP (port 25) and ICMP traffic

09 `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
Displays only traffic in the LAN (192.168.x.x), between workstations and servers — no Internet

10 `ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`
Filter by a protocol (e.g., SIP) and filter out unwanted IPs

Monitoring and Analyzing FTP Traffic

- FTP is used to transfer files over **TCP**, and its default port is **21**
- FTP sends data in a cleartext format
- Use the **ftp** filter to check whether any unauthorized FTP sessions have been established in the network



Monitoring and Analyzing Telnet Traffic

Telnet can provide access to remote hosts including most network equipment and operating systems

Telnet is **not encrypted**; the password and all other data are transmitted as cleartext

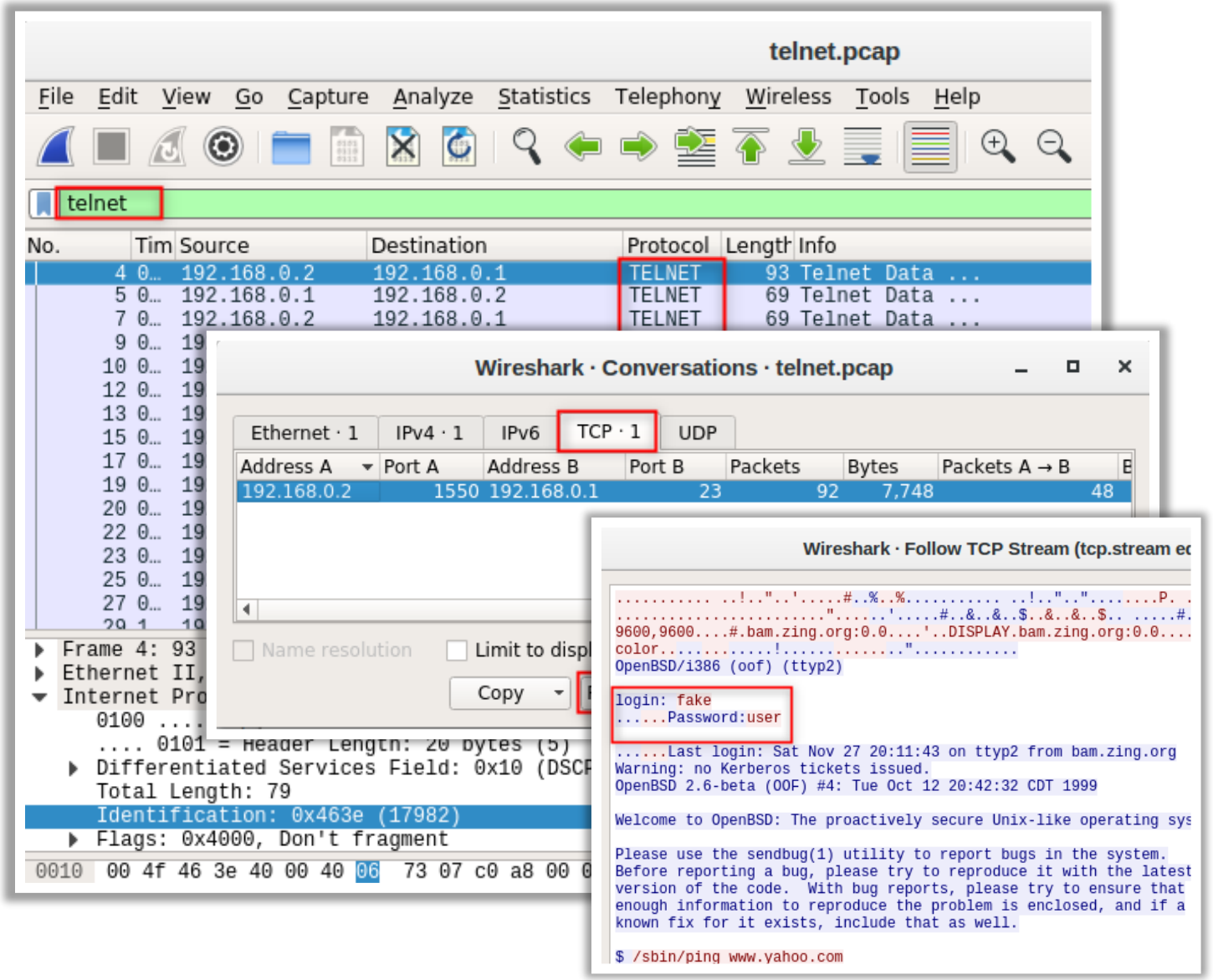
Ideally, it should be disabled; enabling it poses huge **security risks** to the network

It is essential to check whether any Telnet session is established within the network



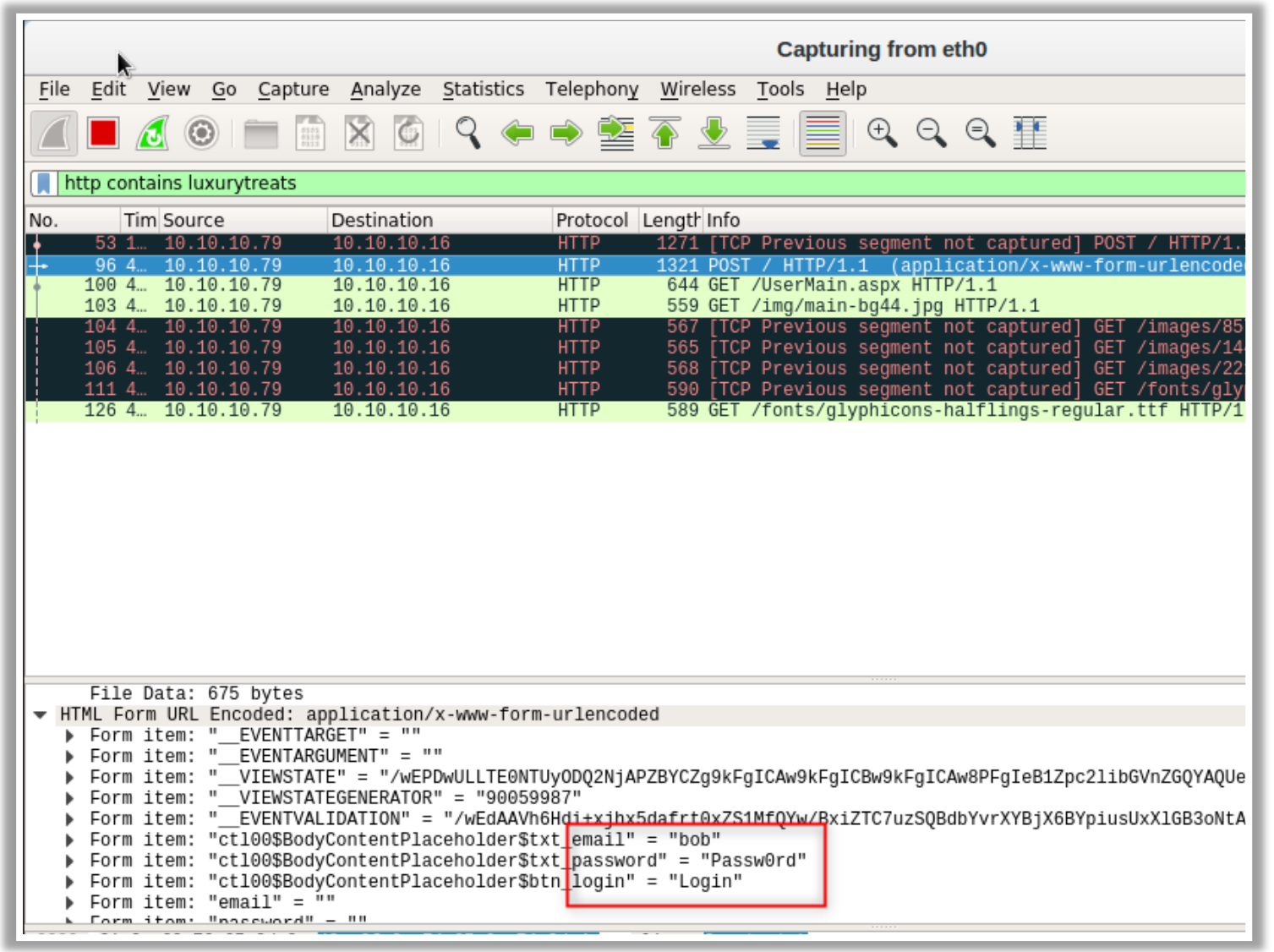
Monitoring and Analyzing Telnet Traffic (Cont'd)

- Perform the following to check for established Telnet sessions:
  - Go to the **Statistics** Menu and click on **Conversations**
  - Go to the **TCP tab** and select the appropriate Telnet communication indicated by port 23 and click **Follow Stream…**
  - The Telnet traffic and the credentials will be viewable in cleartext



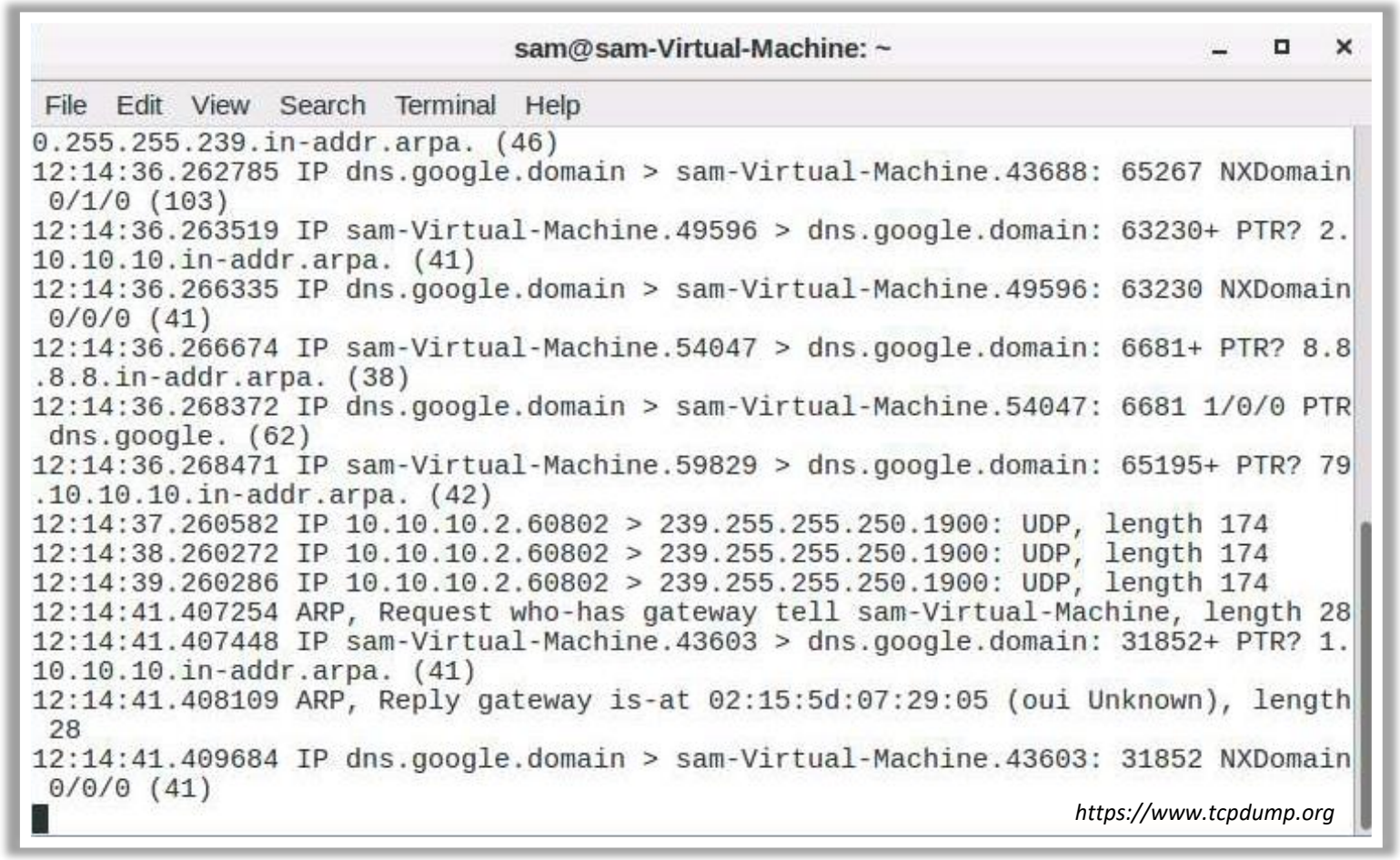
Monitoring and Analyzing HTTP Traffic

- The HTTP sends information in **plain text**
- Monitor and analyze HTTP traffic for the following purposes:
  - Check whether any sensitive information is sent using HTTP
  - Detect malicious traffic
  - Check the traffic against a policy violation
  - Detect applications using unnecessary/restricted services
- Use the **http** filter to check the specific HTTP traffic



Network Sniffers for Network Monitoring

tcpdump | tcpdump is a command-line network analyzer or a packet sniffer that helps in **capturing** and **analyzing network traffic**

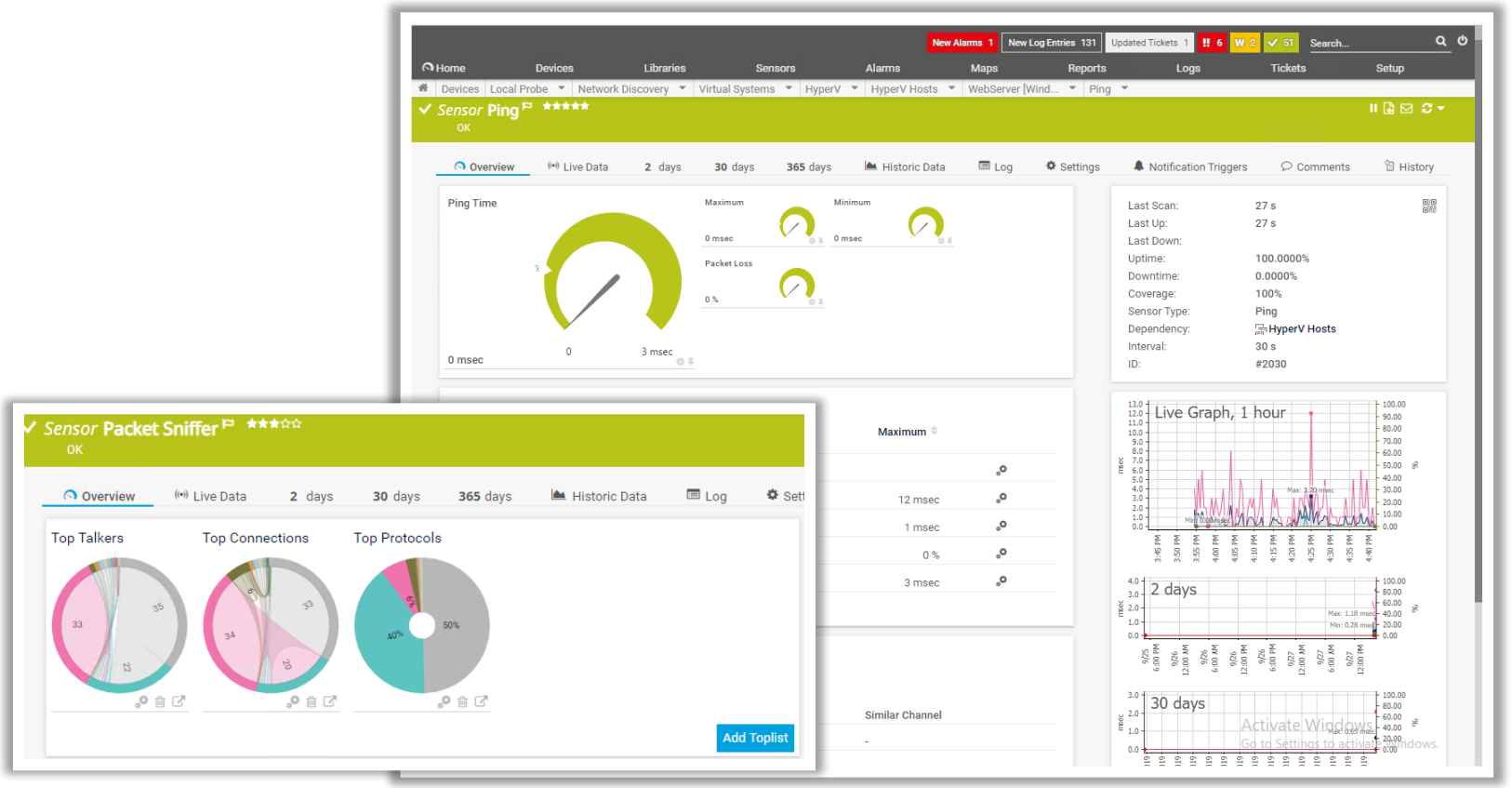


- **Riverbed Packet Analyzer Plus**
  https://www.riverbed.com
- **OmniPeek**
  https://www.liveaction.com
- **Observer Analyzer**
  https://www.viavisolutions.com
- **SolarWinds Deep Packet Inspection and Analysis**
  https://www.solarwinds.com
- **Xplico**
  https://www.xplico.org

Network Monitoring Tools

PRTG Network Monitor

A network monitoring software that supports remote management using any web browser or smartphone, various notification methods, and the monitoring of multiple locations



https://www.paessler.com

SolarWinds Network Performance Monitor
https://www.solarwinds.com

ManageEngine OpManager
https://www.manageengine.com

Capsa Free Network Analyzer
https://www.colasoft.com

Monitis Network Monitoring Solution
https://www.monitis.com

Nagios Network Analyzer
https://www.nagios.com

Module Summary



- This module has discussed the need for and advantages of network traffic monitoring
- It has discussed the network traffic signatures
- It has also discussed the categories of suspicious traffic signatures
- This module also discussed the attack signature analysis techniques and network monitoring for suspicious traffic
- Finally, this module ended with an overview of various network monitoring tools