Cybersecurity Tools

م.د.ابراهيم محمد الحليمه

2025

Penetration testing

Penetration testing, also known as “pen test”, simulates an attack on a computer system in order to evaluate the security of that system. Examples of penetration testing tools include Metasploit, Kali Linux, Netsparker, and Wireshark.

Packet sniffers

A packet sniffer, also called a packet analyzer, protocol analyzer or network analyzer, is used to intercept, log, and analyze network traffic and data. Examples of tools include Wireshark, Tcpdump, and Windump.

Packet Sniffer Software

Wireshark

The world’s most popular network protocol analyzer, Wireshark gives you a microscopic view of your network activity.
Using Wireshark, you can inspect hundreds of protocols and browse your captured network data using a graphical user interface (GUI) or via the TTY (teletypewriter) mode TShark utility.

Wireshark Features

Live capture and offline analysis•
Read and write in a variety of different capture file formats, including tcpdump (libpcap), •
Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, and many others
Rich VoIP analysis•
Export output to XML, PostScript, CSV, or plain text•

What is Wireshark used for?
Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security. Networks must be monitored to ensure smooth operations and security.

Why do hackers use Wireshark?
Many times, cybersecurity pros use Wireshark as a quick and dirty way to identify traffic bursts during attacks. It's also possible to capture the amount of traffic generated between one system and another.

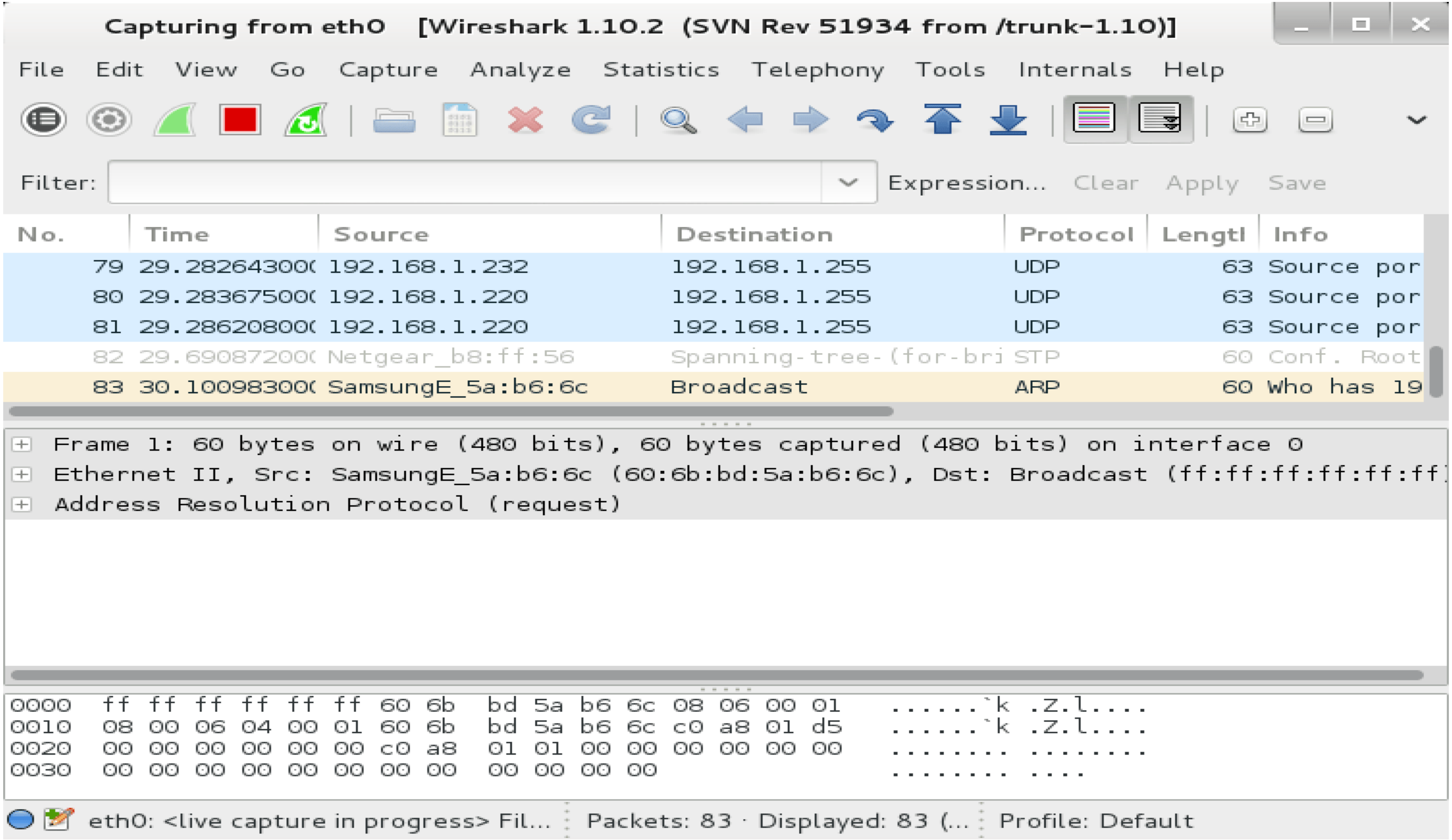
Is Wireshark a security risk?
Because there is always the potential for Wireshark exploits, special care should be taken to avoid security related problems while running Wireshark or at least to reduce the possible impact.

How to work on Wireshark?

After starting Wireshark, do the following:

Select Capture | Interfaces..1
Select the interface on which packets need to be captured. 2
Click the Start button to start the capture..3
Recreate the problem. 4
Once the problem which is to be analyzed has been reproduced, click on Stop. 5
Save the packet trace in the default format..6

Can Wireshark detect viruses?
Identifying malware traffic using Wireshark involves analyzing the captured network packets to identify patterns, behaviors, and indicators of compromise (IoCs). Examine DNS traffic for suspicious domain names. Look for traffic using non-standard or uncommon protocols. Analyze HTTP and HTTPS traffic for anomalies.

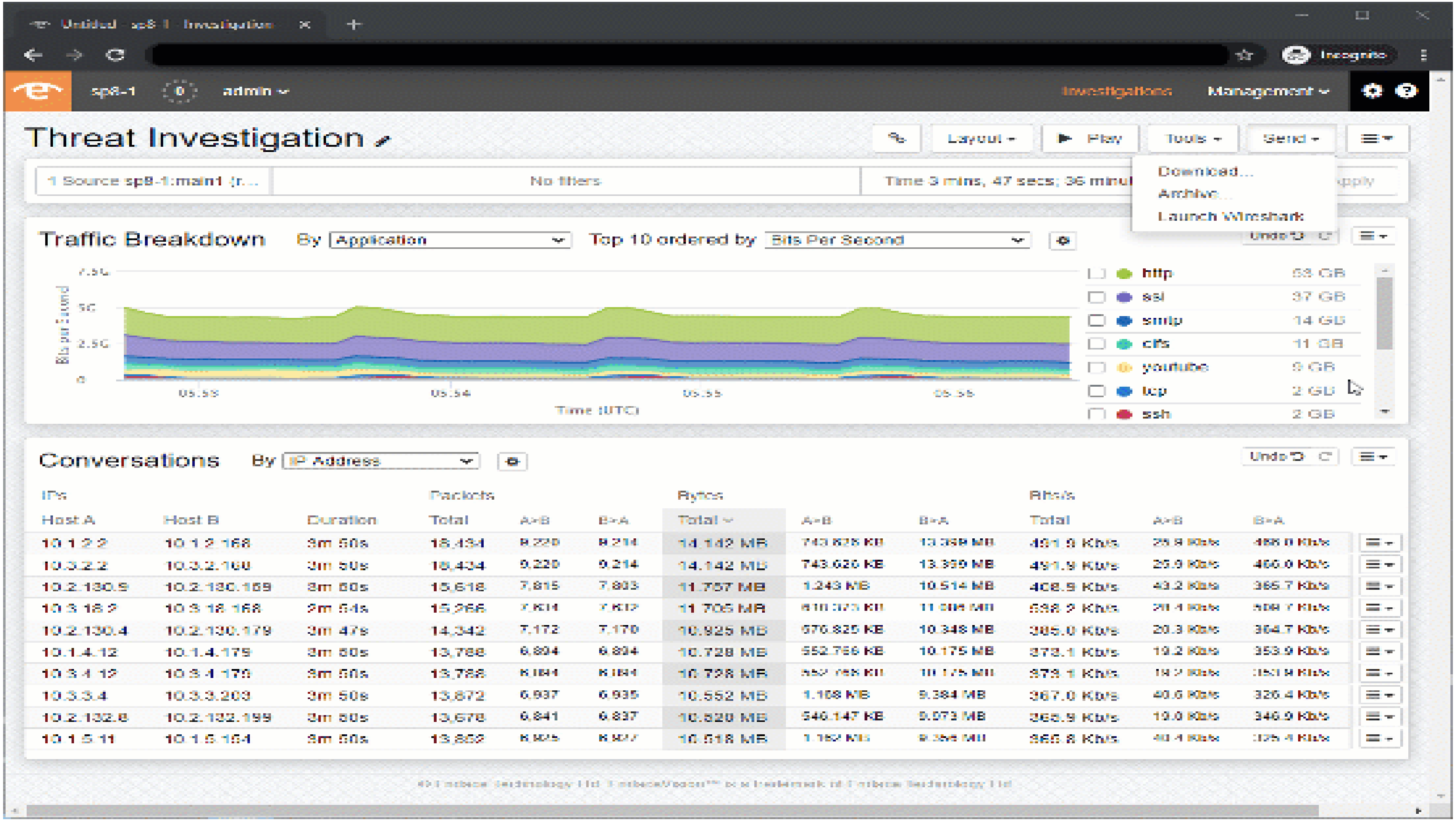


```
No.    Time          Source               Destination              Protocol  Lengtl  Info
   79  29.28264300(  192.168.1.232        192.168.1.255            UDP           63  Source por
   80  29.28367500(  192.168.1.220        192.168.1.255            UDP           63  Source por
   81  29.28620800(  192.168.1.220        192.168.1.255            UDP           63  Source por
   82  29.69087200(  Netgear_b8:ff:56     Spanning-tree-(for-bri   STP           60  Conf. Root
   83  30.10098300(  SamsungE_5a:b6:6c    Broadcast                ARP           60  Who has 19
```

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: SamsungE_5a:b6:6c (60:6b:bd:5a:b6:6c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 60 6b  bd 5a b6 6c 08 06 00 01   ......`k .Z.l....
0010  08 00 06 04 00 01 60 6b  bd 5a b6 6c c0 a8 01 d5   ......`k .Z.l....
0020  00 00 00 00 00 00 c0 a8  01 01 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

eth0: <live capture in progress> Fil... Packets: 83 · Displayed: 83 (... Profile: Default



Threat Investigation

1 Source sp8-1:main1 (r... | No filters | Time 3 mins, 47 secs; 36 minu... | Apply

Traffic Breakdown

By Application · Top 10 ordered by Bits Per Second

□	🟩 http	53 GB
□	● ssl	37 GB
□	● smtp	14 GB
□	● cifs	11 GB
□	● youtube	9 GB
□	● tcp	2 GB
□	● ssh	2 GB

Conversations

By IP Address

IPs			Packets			Bytes			Bits/s		
Host A	Host B	Duration	Total	A>B	B>A	Total	A>B	B>A	Total	A>B	B>A
10.1.2.2	10.1.2.168	3m 50s	18,434	9,220	9,214	14.142 MB	743.626 KB	13.399 MB	491.9 Kb/s	25.9 Kb/s	466.0 Kb/s
10.3.2.2	10.3.2.168	3m 50s	18,434	9,220	9,214	14.142 MB	743.626 KB	13.399 MB	491.9 Kb/s	25.9 Kb/s	466.0 Kb/s
10.2.130.9	10.2.130.159	3m 50s	15,618	7,815	7,803	11.757 MB	1.243 MB	10.514 MB	408.9 Kb/s	43.2 Kb/s	365.7 Kb/s
10.3.18.2	10.3.18.168	2m 54s	15,266	7,634	7,632	11.705 MB	610.323 KB	11.095 MB	538.2 Kb/s	28.4 Kb/s	509.7 Kb/s
10.2.130.4	10.2.130.179	3m 47s	14,342	7,172	7,170	10.925 MB	576.825 KB	10.348 MB	385.0 Kb/s	20.3 Kb/s	364.7 Kb/s
10.1.4.12	10.1.4.175	3m 50s	13,788	6,894	6,894	10.728 MB	552.766 KB	10.175 MB	373.1 Kb/s	19.2 Kb/s	353.9 Kb/s
10.3.4.12	10.3.4.175	3m 50s	13,788	6,894	6,894	10.728 MB	552.766 KB	10.175 MB	373.1 Kb/s	19.2 Kb/s	353.9 Kb/s
10.3.3.4	10.3.3.203	3m 50s	13,872	6,937	6,935	10.552 MB	1.168 MB	9.384 MB	367.0 Kb/s	40.6 Kb/s	326.4 Kb/s
10.2.132.8	10.2.132.199	3m 50s	13,678	6,841	6,837	10.520 MB	546.147 KB	9.973 MB	365.9 Kb/s	19.0 Kb/s	346.9 Kb/s
10.1.5.11	10.1.5.164	3m 50s	13,852	6,925	6,927	10.518 MB	1.162 MB	9.356 MB	365.8 Kb/s	40.4 Kb/s	325.4 Kb/s

© Endace Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd.