



# Network Analysis Visualization (NAV)

Meghan Allen and Peter McLachlan  
December 15, 2004



# Problem

- Network traffic analysis is necessary for many home and corporate users
  - Security threats are on the rise on the internet
  - Users are interested in their bandwidth usage
- Analyzing network data is a difficult challenge
- Traditional network analysis software only provides detailed text based output
  - These packages do not provide an overview, or capabilities to pop-out important information
  - No dynamic filtering, static queries only
  - Finding specific events can be challenging



# Ethereal

The screenshot displays the Ethereal interface with a packet capture of a TCP ACK segment. The packet list table is as follows:

No. -	Time	Source	Destination	Protocol	Info
55999	11:03:35.357	128.189.142.254	Broadcast	ARP	who has 128.189.142.174? Tell 128.189.142.254
56000	11:03:35.455	128.189.142.217	128.189.142.255	NBNS	Name query[Short Frame]
56001	11:03:35.536	128.189.142.81	128.189.142.255	NBNS	Name query[Short Frame]
56002	11:03:35.656	128.189.142.254	Broadcast	ARP	who has 128.189.142.135? Tell 128.189.142.254
56003	11:03:36.210	128.189.142.217	128.189.142.255	NBNS	Name query[Short Frame]
56004	11:03:36.286	128.189.142.81	128.189.142.255	NBNS	Name query[Short Frame]
56005	11:03:36.289	NorteNe_c0:66:e1	Bay-Networks-(Syno	SONMP	SONMP - Segment Hello
56006	11:03:36.290	NorteNe_c0:66:e1	Bay-Networks-(Syno	SONMP	SONMP - FlatNet Hello
56007	11:03:36.679	128.189.142.66	207.46.106.22	MSNMS	PNG
56008	11:03:36.733	207.46.106.22	128.189.142.66	MSNMS	QNG 44
56009	11:03:36.840	128.189.142.66	207.46.106.22	TCP	1061 -> 1863 [ACK] Seq=1704 Ack=4936 win=62596 Len=0
56010	11:03:36.959	128.189.142.217	128.189.142.255	NBNS	Name query[Short Frame]
56011	11:03:37.709	128.189.142.217	128.189.142.255	NBNS	Name query[Short Frame]
56012	11:03:37.767	128.189.142.254	Broadcast	ARP	who has 128.189.142.194? Tell 128.189.142.254
56013	11:03:38.456	128.189.142.254	Broadcast	ARP	who has 128.189.142.194? Tell 128.189.142.254
56014	11:03:38.500	128.189.142.69	128.189.142.255	NBDS	Direct_group datagram[Short Frame]
56015	11:03:39.105	128.189.142.175	128.189.142.255	NBDS	Direct_group datagram[Short Frame]
56016	11:03:39.106	128.189.142.60	128.189.142.255	NBNS	Release[Short Frame]

The selected packet (No. 56009) details are:

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
- Total Length: 40
- Identification: 0x5076 (20598)
- Flags: 0x04 (Don't Fragment)
- Fragment offset: 0
- Time to live: 127
- Protocol: TCP (0x06)
- Header checksum: 0x6315 (correct)
- Source: 128.189.142.66 (128.189.142.66)
- Destination: 207.46.106.22 (207.46.106.22)
- Transmission Control Protocol, Src Port: 1061 (1061), Dst Port: 1863 (1863), Seq: 1704, Ack: 4936, Len: 0
  - Source port: 1061 (1061)
  - Destination port: 1863 (1863)
  - Sequence number: 1704 (relative sequence number)
  - Acknowledgement number: 4936 (relative ack number)
  - Header length: 20 bytes
  - Flags: 0x0010 (ACK)
  - Window size: 62596
  - Checksum: 0xe74e (correct)

Hex dump (0000-0030):

```
0000 00 05 85 21 7c 00 00 02 55 bf 26 95 08 00 45 00  . . . . . U. & . . . E.
0010 00 28 50 76 40 00 7f 06 63 15 80 bd 8e 42 cf 2e  . (Pv@ . . . c. . . . B.
0020 6a 16 04 25 07 47 91 f2 8f 22 e7 21 78 19 50 10  j . . % G . . . ! x . P.
0030 f4 84 e7 4e 00 00  . . . N . .
```



# Objective

- Develop a tool for network visualization
  - Focus on common protocols and services
  - Focus on log files
- Our intention is to provide high level information at-a-glance





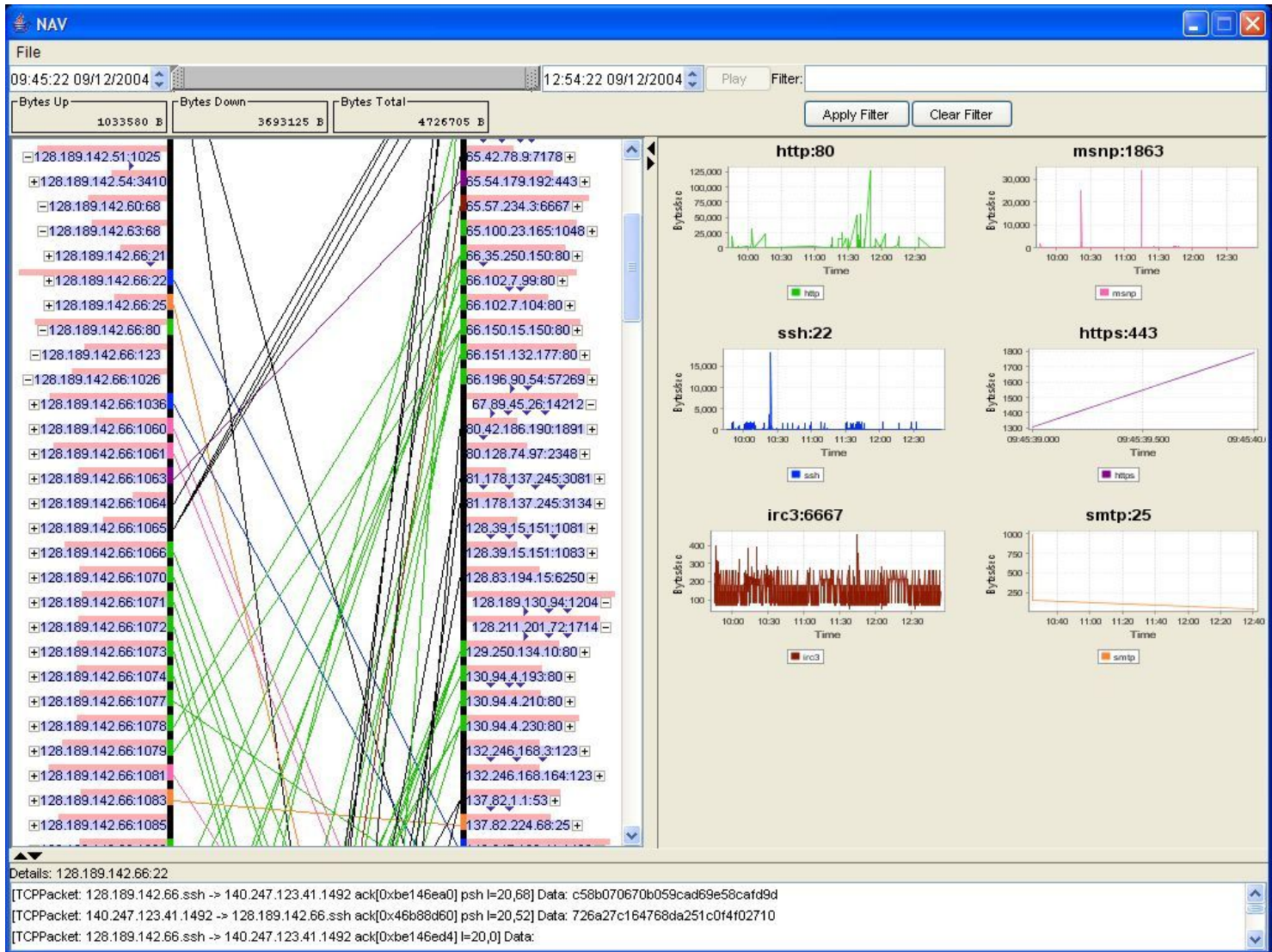
## Related work

- Visual Information Security Utility for Administration Live (VISUAL) [1]
- PortVis [2]
- NVisionIP [3]
- The Spinning Cube of Potential Doom [4]



# Solution

- NAV provides two overviews and a detail view
  - IP wall view displays connections between local and remote machines colour coded by port number
  - Services view contains a trellis structure of graphs displaying information based on the port number
- Users can dynamically filter on time
- Users can statically filter on a number of packet level details





## IP wall view

- Displays connections between local and remote machines
- Ability to collapse and aggregate IP address ranges
- Allows connection hiding to avoid line snarls
- Displays total traffic per address/port pair



## Service view

- Displays a graph for each pre-selected service only if data exists
- Graph displays traffic (bytes/s) against time
- Log based time axis can be toggled
- Service selection is user specified



## Detail view

- Drag and drop from IP wall view or services view to display detailed packet information
- Displays packets for a single IP address or a single port number at a time



# Evaluation

- Strengths
  - Good overviews of the information
  - Quickly shows active services that consume network resources
- Weaknesses
  - Performance/Scalability
  - Application is not feature complete



# Future work

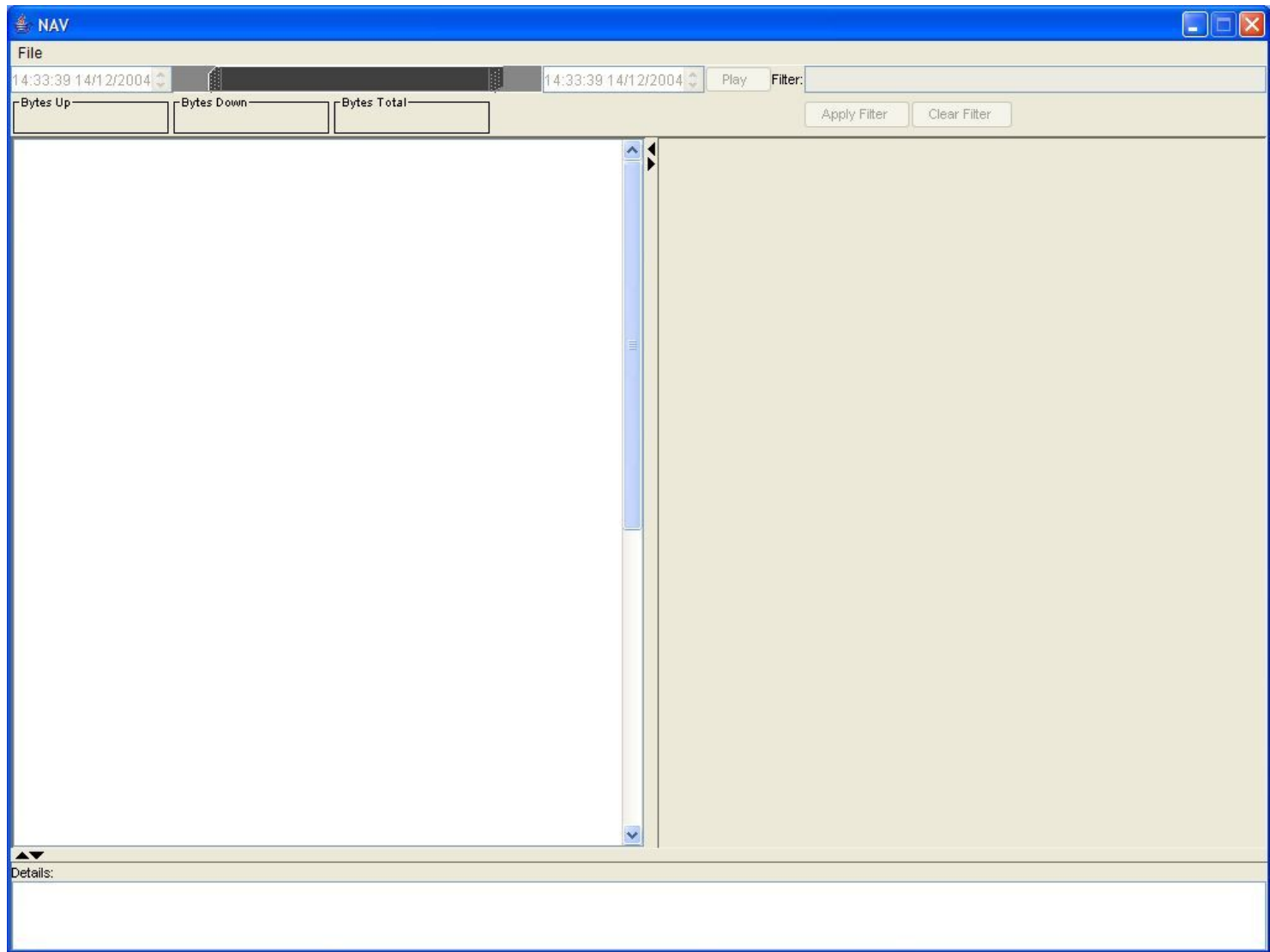
- Intrusion detection
- DNS recognition for IP addresses
- Expanded preferences
- Detect unexpected traffic
- Animation of connections on the wall view





# References

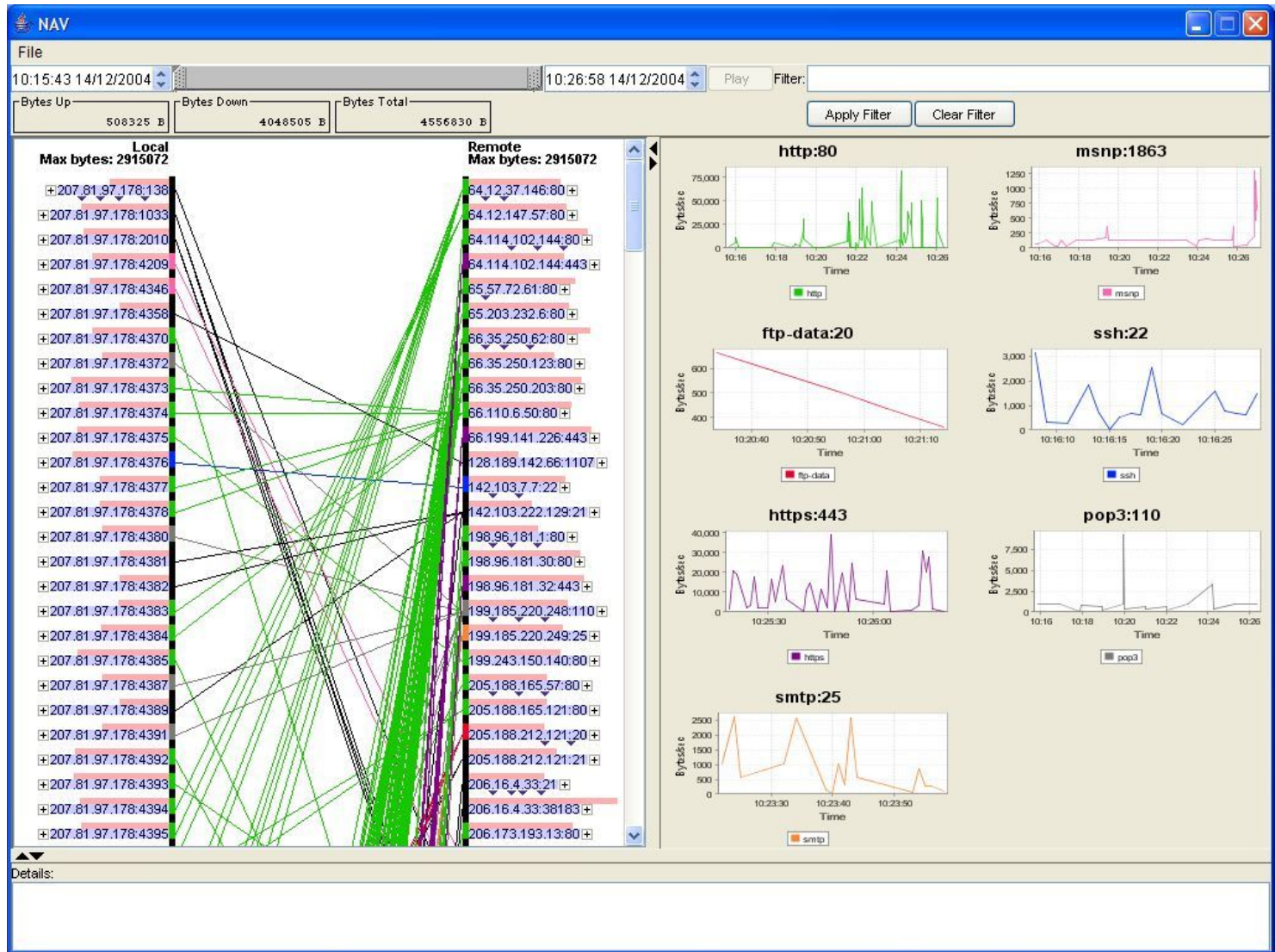
- [1] R. Ball, G. A. Fink and C. North, Home-centric visualization of network traffic for security administration, VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 55-64, 2004
- [2] K. Lakkaraju, W. Yurcik and A. J. Lee, NisionIP: netflow visualizations of system state for security situational awareness, VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 65–72, 2004
- [3] S. Lau. The Spinning Cube of Potential Doom. Communications of the ACM, pages 25-26, 2004.
- [4] J. McPherson, K. Ma, P. Krystosk and T. Bartoletti and M. Christensen. PortVis: a tool for port-based detection of security events . Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 73-81, 2004.



The screenshot shows the NAV (Network Analyzer) software interface. The main window has a title bar with the NAV logo and standard window controls. Below the title bar is a 'File' menu bar. The main area contains a timeline with two time markers: '14:33:39 14/12/2004' and '14:33:39 14/12/2004'. There are three columns labeled 'Bytes Up', 'Bytes Down', and 'Bytes Total'. A 'Filter' field is present with 'Apply Filter' and 'Clear Filter' buttons. An 'Open' dialog box is overlaid on the main window. The dialog box has a title bar with the NAV logo and a close button. It contains the following fields and controls:

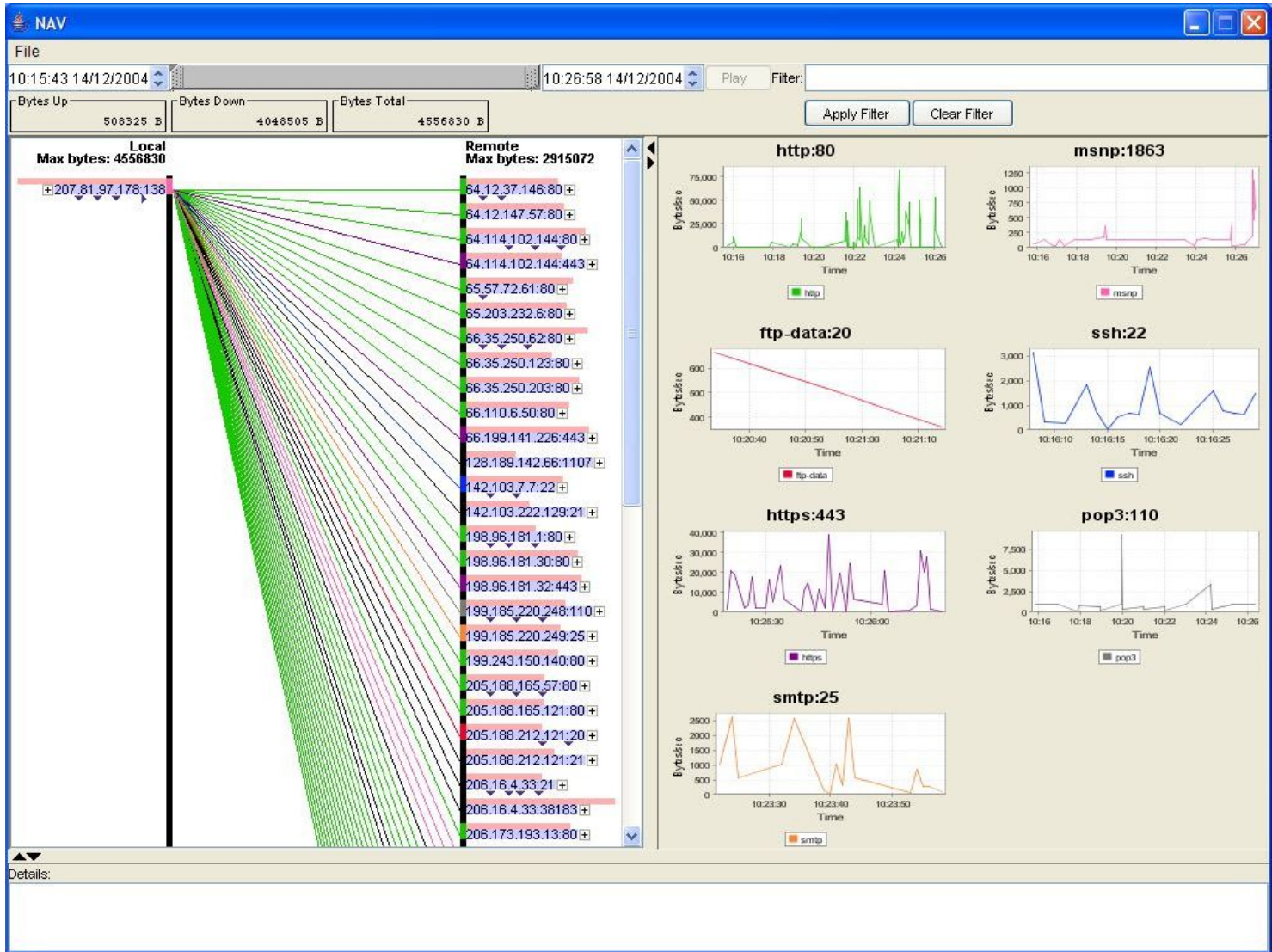
- Local Network Address:
- Local Network Mask:
- Begin date:  (with a dropdown arrow)
- End date:  (with a dropdown arrow)
- Filter:
- Filename:  (with a 'Browse ...' button)
- GO! button

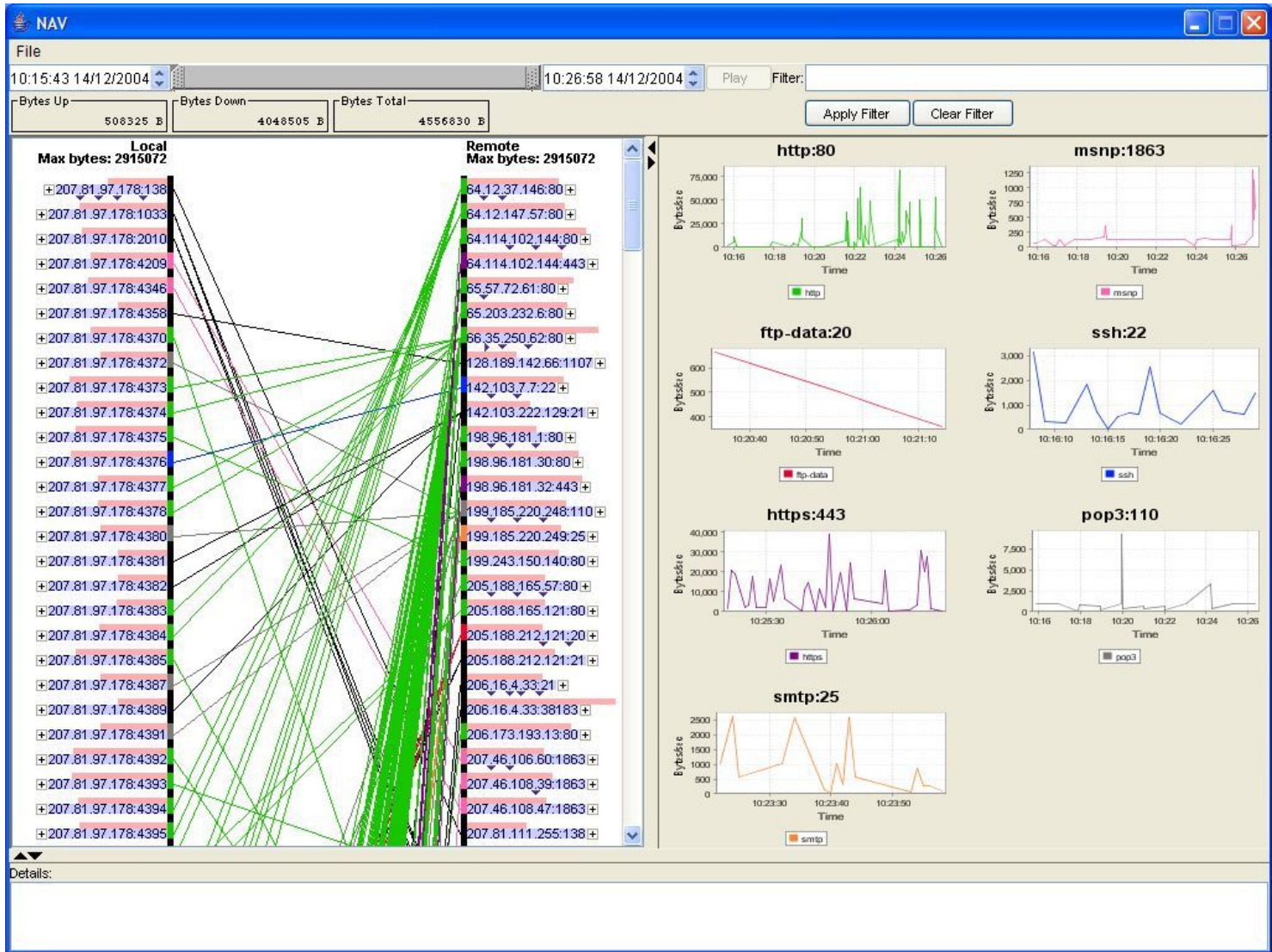
At the bottom of the main window, there is a 'Details:' section which is currently empty.

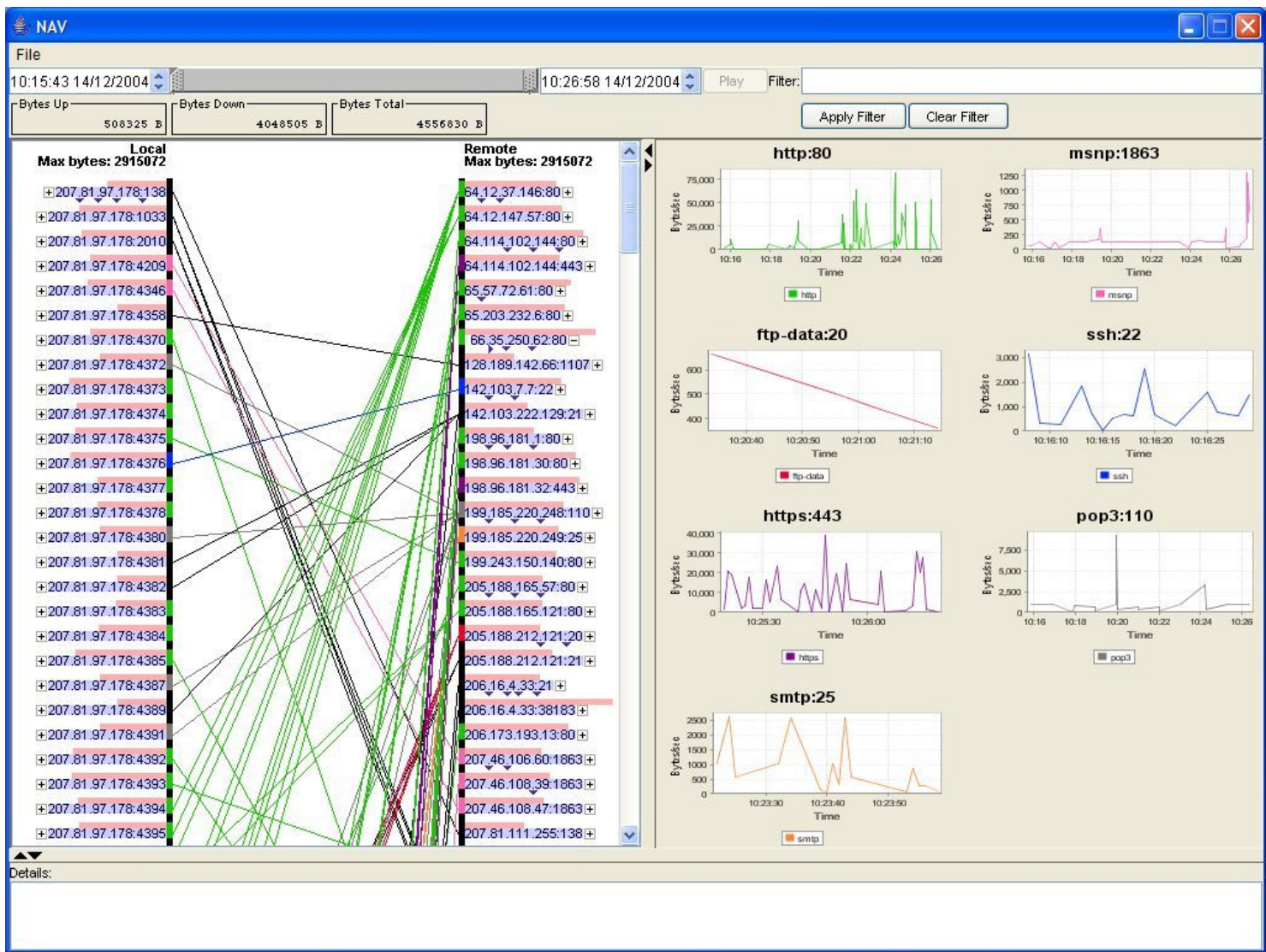
















NAV

File

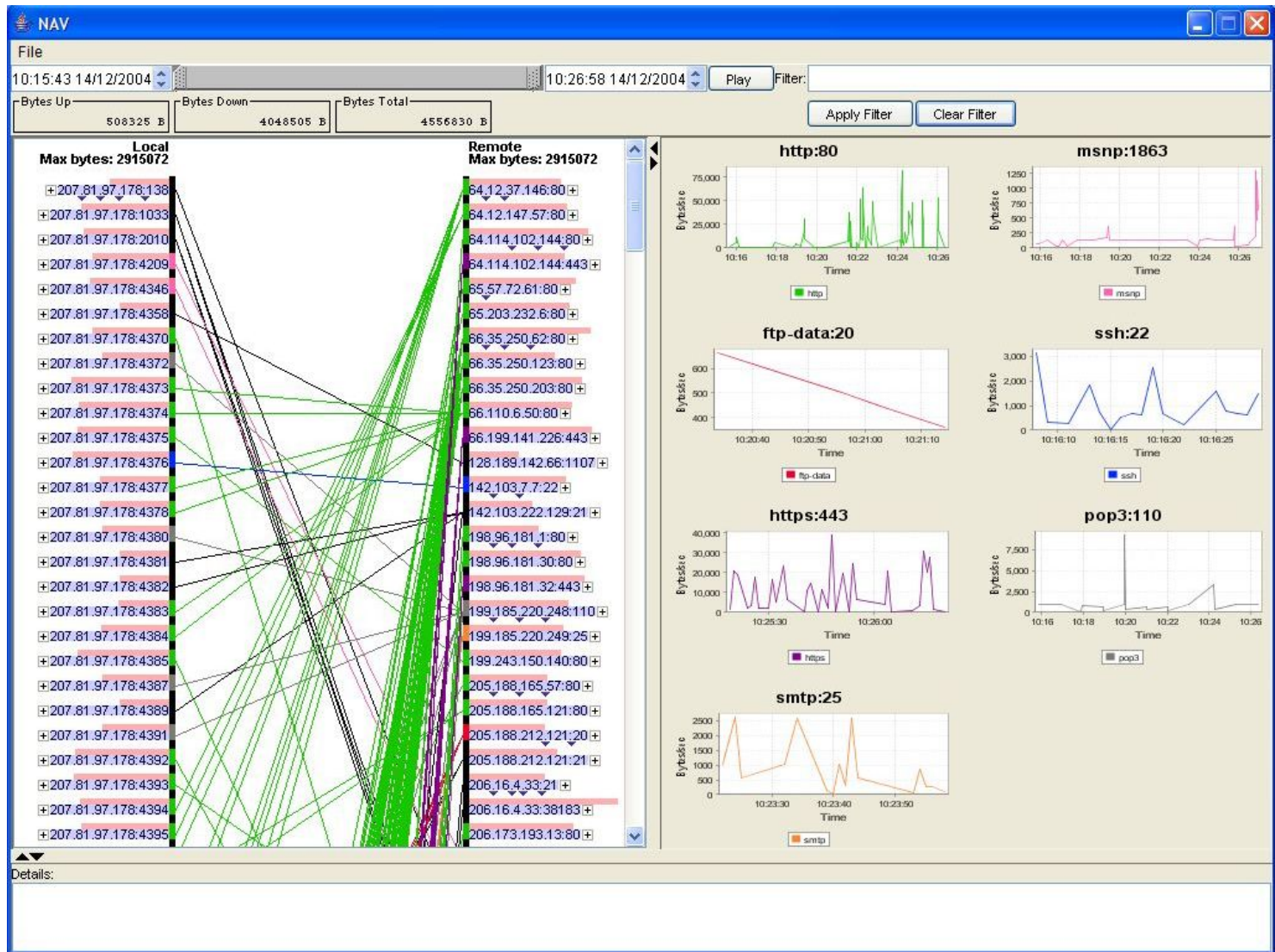
10:15:43 14/12/2004 10:26:03 14/12/2004 Play Filter: not top

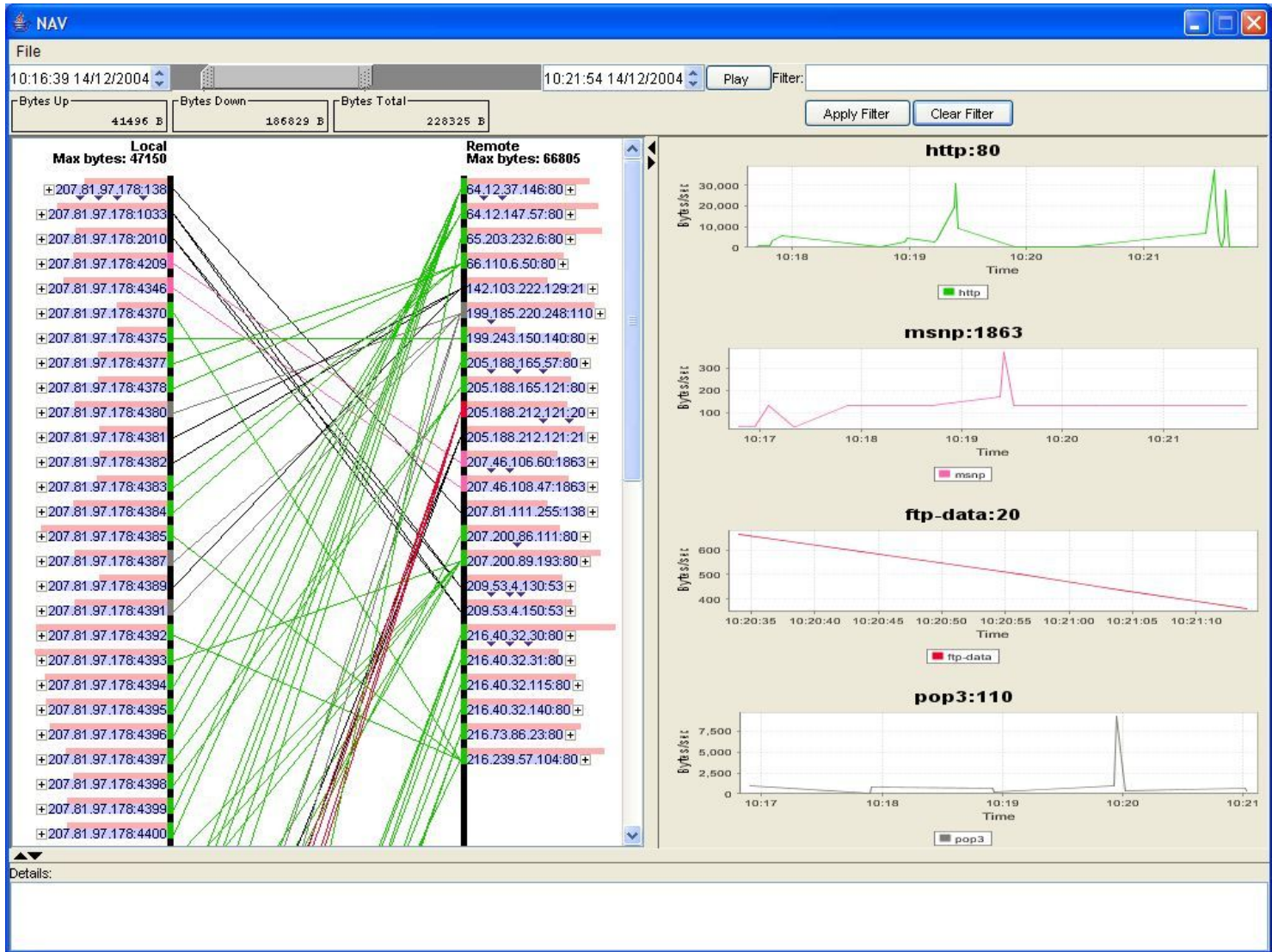
Bytes Up: 2523 B Bytes Down: 10468 B Bytes Total: 12991 B

Apply Filter Clear Filter

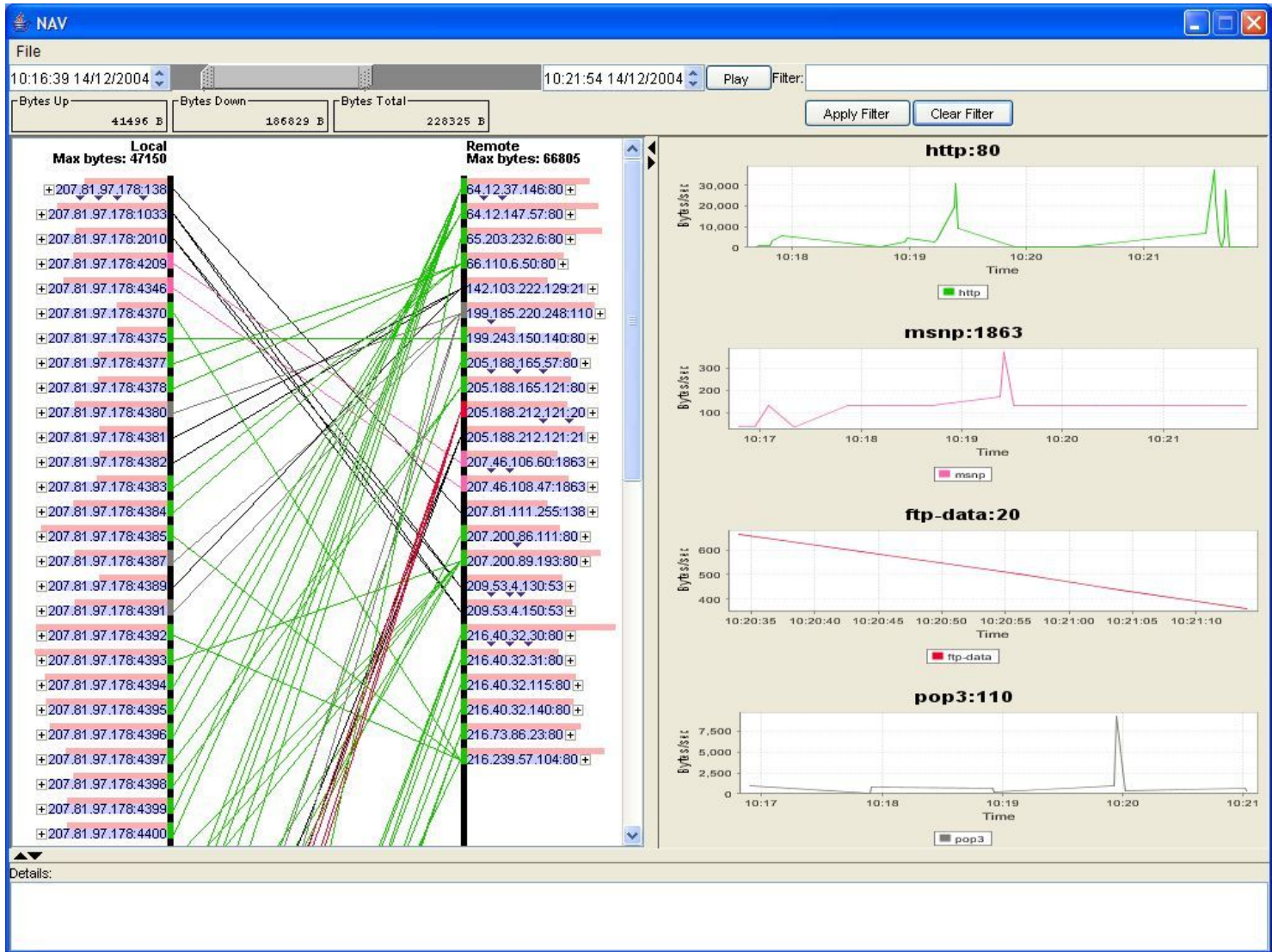
Local		Remote	
Max bytes: 7288		Max bytes: 10343	
207.81.97.178:138	207.81.111.255:138	207.81.111.255:138	207.81.111.255:138
207.81.97.178:1033	209.53.4.130:53	209.53.4.130:53	209.53.4.130:53
207.81.97.178:2010	209.53.4.150:53	209.53.4.150:53	209.53.4.150:53

Details:









The screenshot displays the NAV (NetworkMiner) application interface. A 'Preferences' dialog box is open in the center, allowing configuration of the network graph and service monitoring. The dialog has two main sections: 'Services' and 'Selected Services'.

**Services List:**

- 1ci-smcs
- 3Com-nsd
- 3com-amp3
- 3com-net-mgrnt
- 3com-tsmux
- 3com-webview
- 3comfaxrpc
- 3d-nfsd
- 3ds-lm
- 3l-l1
- 3m-image-lm
- 4-tieropmcli
- 4-tieropmgw
- 4talk
- 802-11-iapp
- 9pfs
- CAllic
- LiebDevMgmt\_A
- LiebDevMgmt\_C
- LiebDevMgmt\_DM
- a1-bs
- a1-misc
- a13-an
- a3-sdunode
- a4-sdunode

**Selected Services:**

- http
- msnp
- ftp-data
- ssh
- https
- irc3
- pop3
- smtp

**Number of services to display:**

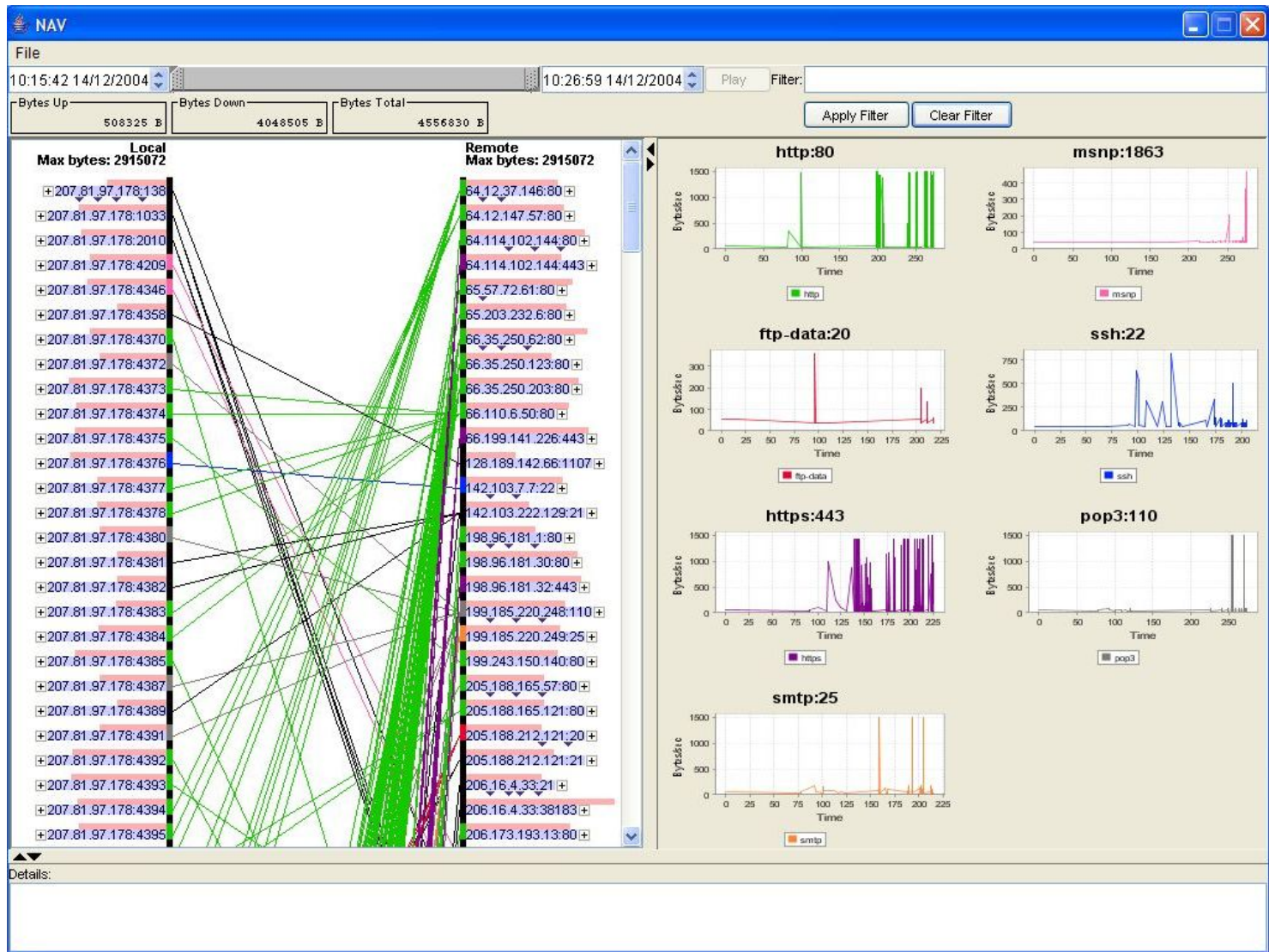
- 6
- 8
- 10
- 12

Use log based x-axes

Buttons: Set Color..., Ok, Cancel

**Background Interface:**

- NAV Window:** Shows a network graph with nodes and connections. A 'Local' section indicates 'Max bytes: 2915072'. A 'File' menu is visible at the top.
- Service Monitors:** Three line graphs show traffic over time for:
  - msnp:1863:** Y-axis 0-1250, X-axis 10:16-10:26.
  - ssh:22:** Y-axis 0-3000, X-axis 10:16-10:25.
  - pop3:110:** Y-axis 0-7500, X-axis 10:16-10:28.
- Details:** A section at the bottom for displaying details of selected nodes.





The screenshot shows the NAV (NetworkMiner) application interface. At the top, the title bar reads "NAV". Below it, the "File" menu is visible. The main window displays network traffic data, including a list of connections with columns for "Local", "Remote", and "Bytes". A "Preferences" dialog is open, showing a list of "Services" (1ci-smcs, 3Com-nsd, 3com-amp3, 3com-net\_mgmt) and a "Selected Services" list (http, msnp, ftp-data, ssh, https, irc3, pop3, smtp). A "Select Colour" dialog is also open, showing a color palette and a preview area. Three line graphs are visible on the right side of the main window, labeled "msnp:1863", "ssh:22", and "pop3:110", each showing traffic volume over time.

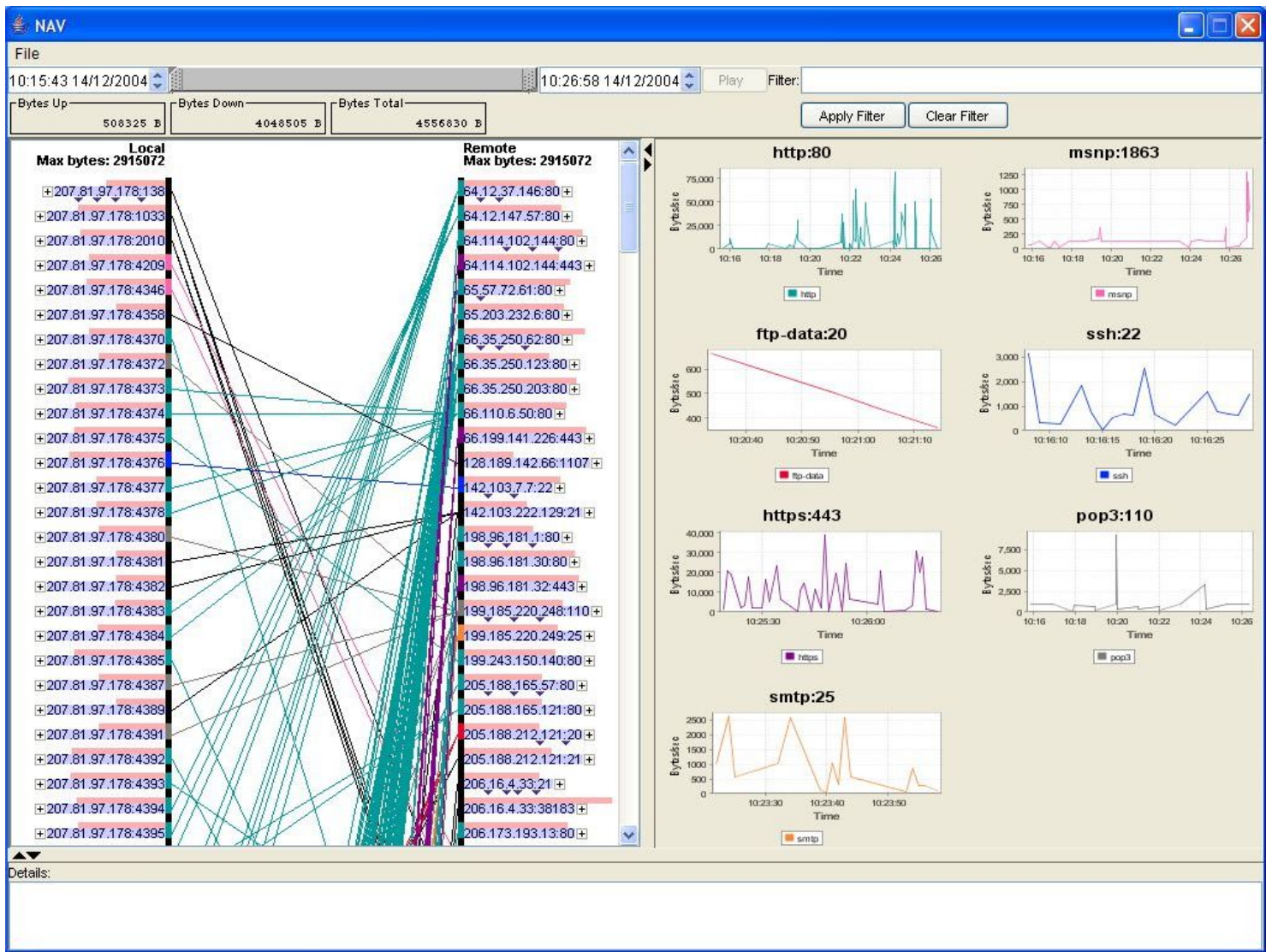
The screenshot shows the NAV (Network Analyzer) interface. At the top, the window title is "NAV". Below it, there's a "File" menu and a status bar showing the time "10:15:43 14/12/2004" and "10:26:58 14/12/2004". There are also buttons for "Play" and "Filter:". Below the status bar, there are three boxes for "Bytes Up" (508325 B), "Bytes Down" (4048505 B), and "Bytes Total" (4556830 B). There are also "Apply Filter" and "Clear Filter" buttons.

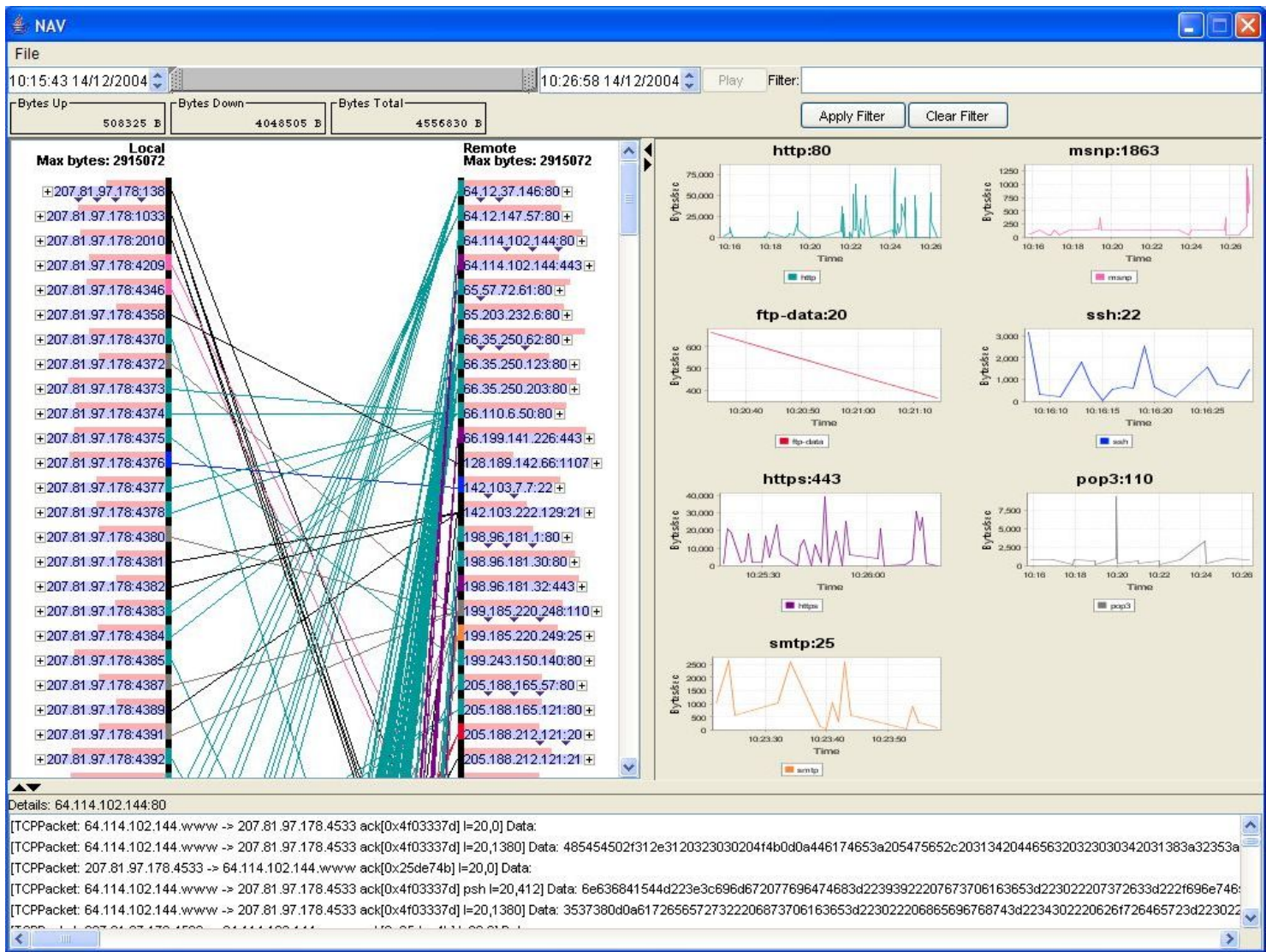
The main area is divided into "Local" and "Remote" sections. The "Local" section shows a list of IP addresses and ports, with a "Max bytes: 2915072" label. The "Remote" section shows a list of services and their status. A "Preferences" dialog box is open, showing a list of services and a "Selected Services" list. The "Selected Services" list includes http, msnp, ftp-data, ssh, https, irc3, pop3, and smtp. There are also buttons for "Set Color...", "Ok", and "Cancel".

On the right side, there are three time-series graphs for different services: "msnp:1863", "ssh:22", and "pop3:110". Each graph shows a line plot of activity over time, with a legend below it. The x-axis for all graphs is "Time" and the y-axis represents activity level.

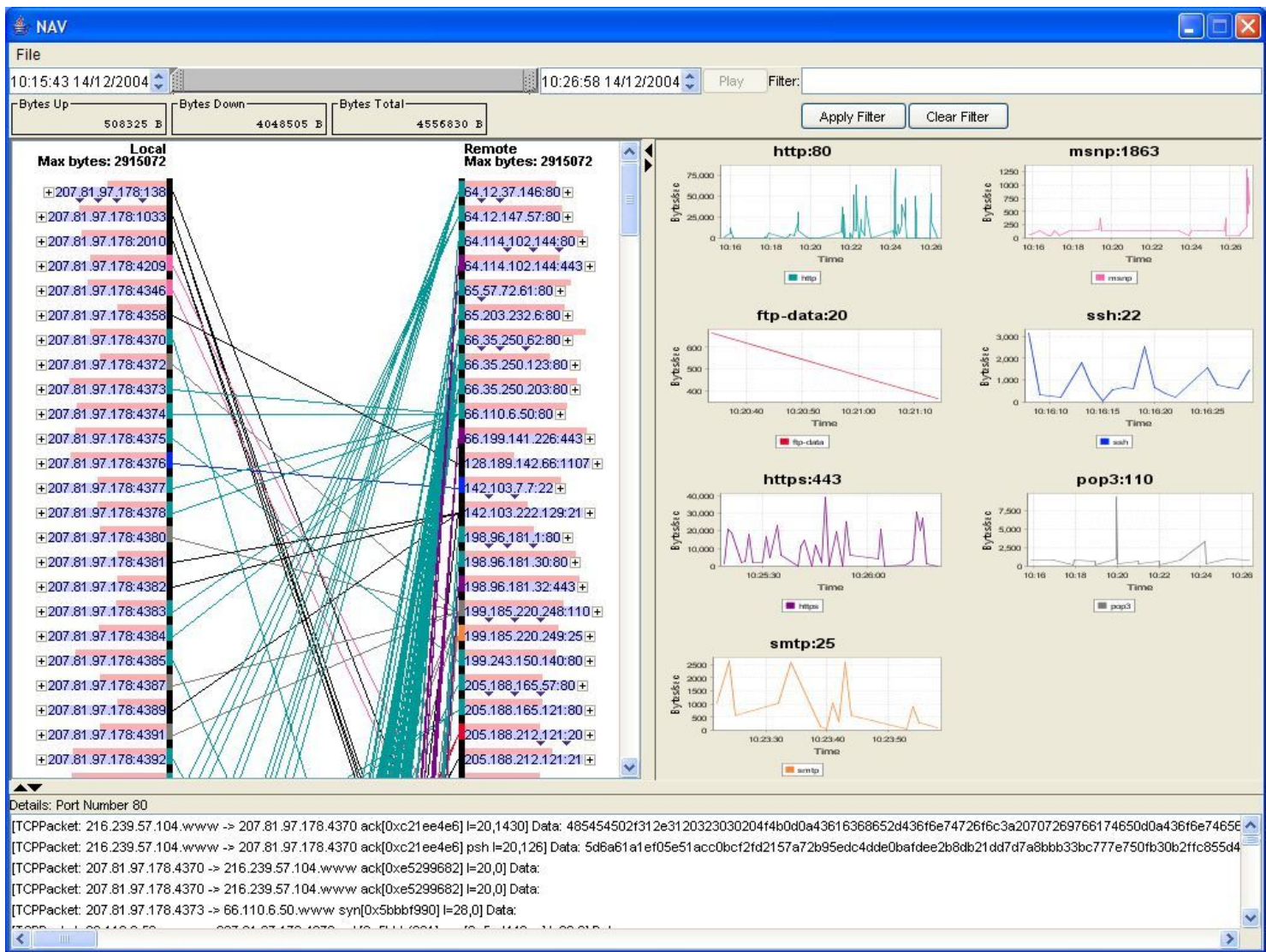
At the bottom, there's a "Details:" section which is currently empty.













NAV

File

10:15:43 14/12/2004 | 10:26:58 14/12/2004 | Play | Filter:

Bytes Up | Bytes Down | Bytes Total | Apply Filter | Clear Filter

Local	Remote
Max bytes: 0	Max bytes: 0

Details:

