



Configuring Time Zones

Configuring Time Zones

» How to configure and view time in Wireshark

» What is UTC?

- How to display in Wireshark columns
- Other settings

» Epoch time

- January 1 00:00:00 of 1970

Configuring Time Zones

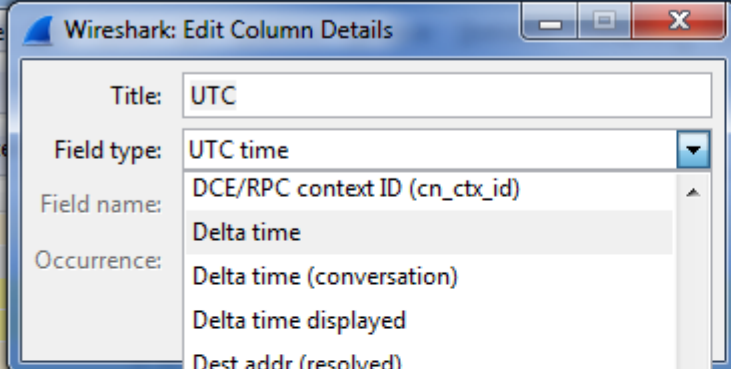
*Local Area Connection [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	UTC	Source	Destination	Protocol
1	0.000000000	2014-08-26 19:30:17.718662000	10.121.78.2	224.0.0.2	HSRP
2	0.045398000	2014-08-26 19:30:17.764060000	00:60:b9:ec: Broadcast		ARP
3	0.103142000	2014-08-26 19:30:17.821804000	10.121.90.10	10.121.91.25	NBNS
4	*REF*	*REF*	10.121.90.17	10.121.91.25	NBNS
5	0.010265000	2014-08-26 19:30:18.003653000	10.121.90.2	224.0.0.2	HSRP
6	*REF*	*REF*	10.121.90.19	239.255.255.	SSDP
7	0.058670000	2014-08-26 19:30:18.320833000	10.121.90.3	224.0.0.2	HSRP
8	0.209820000	2014-08-26 19:30:18.471983000	10.121.78.3	224.0.0.2	HSRP
9	0.286658000	2014-08-26 19:30:18.548821000	10.121.78.2	224.0.0.2	HSRP
10	0.323794000	2014-08-26 19:30:18.585957000	10.121.90.10	10.121.91.25	NBNS
11	0.655751000	2014-08-26 19:30:18.917914000	10.121.90.2	224.0.0.2	HSRP
12	0.855452000	2014-08-26 19:30:19.117615000	28:d2:44:4f: Broadcast		ARP

Configuring Time Zones



The image shows the 'Wireshark: Edit Column Details' dialog box. The 'Title' field is set to 'UTC'. The 'Field type' dropdown is set to 'UTC time'. The 'Field name' dropdown is set to 'DCE/RPC context ID (cn_ctx_id)'. The 'Occurrence' dropdown is set to 'Delta time'. The 'Field name' dropdown is also set to 'Delta time (conversation)'. The 'Field name' dropdown is also set to 'Delta time displayed'. The 'Field name' dropdown is also set to 'Dest addr (resolved)'. The 'Field name' dropdown is also set to 'Dest addr (unresolved)'. The 'Field name' dropdown is also set to 'Dest port (resolved)'. The 'Field name' dropdown is also set to 'Dest port (unresolved)'. The 'Field name' dropdown is also set to 'Destination address'. The 'Field name' dropdown is also set to 'Destination port'. The 'Field name' dropdown is also set to 'Expert Info Severity'. The 'Field name' dropdown is also set to 'FW-1 monitor if/direction'.

Wireshark: Edit Column Details

Title: UTC

Field type: UTC time

Field name: DCE/RPC context ID (cn_ctx_id)

Occurrence: Delta time

Delta time (conversation)

Delta time displayed

Dest addr (resolved)

Dest addr (unresolved)

Dest port (resolved)

Dest port (unresolved)

Destination address

Destination port

Expert Info Severity

FW-1 monitor if/direction

Wireshark 1.12.0 [v1.12.0-0-g4fab41a from master-1.12]

Tools Internals Help

Expression... Clear Apply Save

No.	Source	Destination	Protocol	Length
6	10.121.78.2	224.0.0.2	HSRP	
7	00:60:b9:ec::Broadcast		ARP	
8	10.121.90.10	10.121.91.25	NBNS	
9	10.121.90.17	10.121.91.25	NBNS	
10	10.121.90.2	224.0.0.2	HSRP	
11	10.121.90.19	239.255.255.255	SSDP	
12	10.121.90.3	224.0.0.2	HSRP	
13	10.121.78.3	224.0.0.2	HSRP	
14	10.121.78.2	224.0.0.2	HSRP	
15	10.121.90.10	10.121.91.25	NBNS	
16	10.121.90.2	224.0.0.2	HSRP	
17	28:d2:44:4f::Broadcast		ARP	
18	10.121.90.3	224.0.0.2	HSRP	
19	10.121.90.10	10.121.91.25	NBNS	
20	10.121.78.3	224.0.0.2	HSRP	

Configuring Time Zones

» Adjusting time views

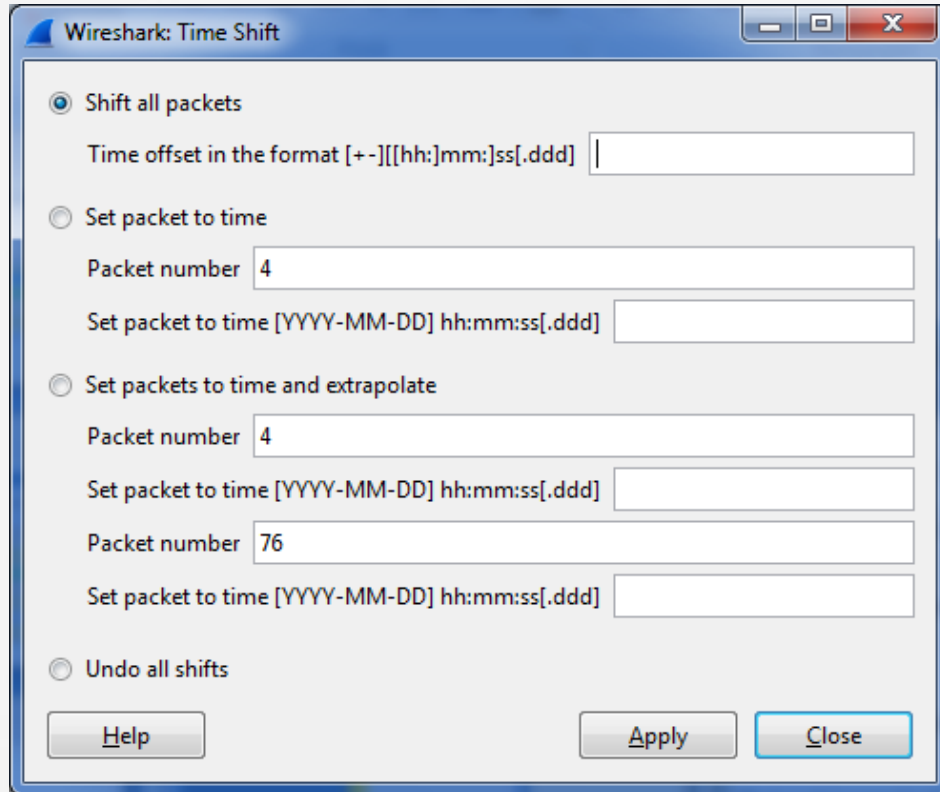
» Preferences

- Create new columns
- Edit column details (new time settings)
- Make references

» Using delta

- Used to trace out problems (applications)

Configuring Time Zones



Questions?