King Fahd University of Petroleum and Minerals

Electrical Engineering Department

EE 400, Experiment # 6

Data Traffic Capture and Protocol Analysis

Objective:

Introduction to data packet capturing and analysis of individual packet contents including the details associated with the protocols used.

Introduction:

Ethereal is a GUI network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file. Like other protocol analyzers, Ethereal's main window shows 3 views of a packet.

1. It shows a summary line, briefly describing what the packet is.
2. A protocol tree is shown, allowing you to drill down to exact protocol or field that you interested in.
3. Finally, a hex dump shows you exactly what the packet looks like when it goes over the wire.

In addition, Ethereal has some features that make it unique. It can assemble all the packets in a TCP conversation and show you the ASCII (or EBCDIC, or hex) data in that conversation (TCP stream). Display filters in Ethereal are very powerful; more fields are filterable in Ethereal than in other protocol analyzers, and the syntax you can use to create your filters is richer

Important Menu Items

File:Open, File:Close, File:Reload
: Open, close, or reload a capture file. The *File:Open* dialog box allows a filter to be specified; when the capture file is read, the filter is applied to all packets read from the file, and packets not matching the filter are discarded.

File:Print Packet
: Print a fully-expanded protocol tree view of the currently-selected packet. Printing options can be set with the *Edit:Preferences* menu item.

File:Quit
: Exits the application.

Edit:Capture Filters
: Edits the saved list of capture filters, allowing filters to be added, changed, or deleted.

Edit:Display Filters
: Edits the saved list of display filters, allowing filters to be added, changed, or deleted.

Edit:Protocols
: Edits the list of protocols, allowing protocol dissection to be enabled or disabled.

Capture:Start

Initiates a live packet capture (see Capture Options below). A temporary file will be created to hold the capture. The location of the file can be chosen by setting your TMPDIR environment variable before starting **Ethereal**. Otherwise, the default TMPDIR location is system-dependent, but is likely either */var/tmp* or */tmp*.

Capture:Stop

In a capture that updates the packet display as packets arrive (so that Ethereal responds to user input other than pressing the ``Stop'' button in the capture packet statistics dialog box), stops the capture.

Display:Options

Allows you to sets the format of the packet timestamp displayed in the packet list window to relative, absolute, absolute date and time, or delta, to enable or disable the automatic scrolling of the packet list while a live capture is in progress or to enable or disable translation of addresses to names in the display.

Display:Match

Creates a display filter, or adds to the display filter strip at the bottom, a display filter based on the data currently highlighted in the protocol tree, and applies the filter.

If that data is a field that can be tested in a display filter expression, the display filter will test that field; otherwise, the display filter will be based on absolute offset within the packet, and so could be unreliable if the packet contains protocols with variable-length headers, such as a source-routed token-ring packet.

The **Selected** option creates a display filter that tests for a match of the data; the **Not Selected** option creates a display filter that tests for a non-match of the data. The **And Selected**, **Or Selected**, **And Not Selected**, and **Or Not Selected** options add to the end of the display filter in the strip at the bottom an AND or OR operator followed by the new display filter expression.

Display:Prepare

Creates a display filter, or adds to the display filter strip at the bottom, a display filter based on the data currently highlighted in the protocol tree, but doesn't apply the filter.

Display:Collapse All

Collapses the protocol tree branches.

Display:Expand All

Expands all branches of the protocol tree.

Tools:Follow TCP Stream

If you have a TCP packet selected, it will display the contents of the data stream for the TCP connection to which that packet belongs, as text, in a separate window, and will leave the list of packets in a filtered state, with only those packets that are part of that TCP connection being displayed. You can revert to your old view by pressing ENTER in the display filter text box, thereby invoking your old display filter (or resetting it back to no display filter).

The window in which the data stream is displayed lets you select whether to display:
whether to display the entire conversation, or one or the other side of it;
whether the data being displayed is to be treated as ASCII or EBCDIC text or as raw hex data;
and lets you print what's currently being displayed, using the same print options that are used for the *File:Print Packet* menu item, or save it as text to a file.

Tools:Decode As

If you have a packet selected, this menu item will present a dialog allowing you to change which dissectors are used to decode this packet. The dialog has one panel each for the link layer, network layer and transport layer protocol/port numbers, and will

allow each of these to be changed independently. For example, if the selected packet is a TCP packet to port 12345, using this dialog you can instruct Ethereal to decode all packets to or from that TCP port as HTTP packets.

WINDOWS

Main Window

The main window is split into three panes. You can resize each pane using a ``thumb'' at the right end of each divider line. Below the panes is a strip that shows the current filter and informational text.

Top Pane

The top pane contains the list of network packets that you can scroll through and select. By default, the packet number, packet timestamp, source and destination addresses, protocol, and description are displayed for each packet; the *Columns* page in the dialog box popped up by *Edit:Preferences* lets you change this (although, unfortunately, you currently have to save the preferences, and exit and restart Ethereal, for those changes to take effect).

If you click on the heading for a column, the display will be sorted by that column; clicking on the heading again will reverse the sort order for that column.

An effort is made to display information as high up the protocol stack as possible, e.g. IP addresses are displayed for IP packets, but the MAC layer address is displayed for unknown packet types.

The right mouse button can be used to pop up a menu of operations.

The middle mouse button can be used to mark a packet.

Middle Pane

The middle pane contains a *protocol tree* for the currently-selected packet. The tree displays each field and its value in each protocol header in the stack. The right mouse button can be used to pop up a menu of operations.

Bottom Pane

The lowest pane contains a hex dump of the actual packet data. Selecting a field in the *protocol tree* highlights the corresponding bytes in this section.

The right mouse button can be used to pop up a menu of operations.

Current Filter

A display filter can be entered into the strip at the bottom. A filter for HTTP, HTTPS, and DNS traffic might look like this:

```
tcp.port == 80 || tcp.port == 443 || tcp.port == 53
```

Selecting the *Filter:* button lets you choose from a list of named filters that you can optionally save. Pressing the Return or Enter keys, or selecting the *Apply* button, will cause the filter to be applied to the current list of packets. Selecting the *Reset* button clears the display filter so that all packets are displayed.

Preferences

The *Preferences* dialog lets you control various personal preferences for the behavior of **Ethereal**.

Column Preferences

The *Columns* page lets you specify the number, title, and format of each column in the packet list.

The *Column title* entry is used to specify the title of the column displayed at the top of the packet list. The type of data that the column displays can be specified using the *Column format* option menu. The row of buttons on the left perform the following actions:

TCP Streams Preferences

The *TCP Streams* page can be used to change the color of the text displayed in the TCP stream window. To change a color, simply select an attribute from the ``Set:'' menu and use the color selector to get the desired color. The new text colors are displayed in a sample window.

User Interface Preferences

The *User Interface* page is used to modify small aspects of the GUI to your own personal taste:

Capture Preferences

The *Capture* page lets you specify various parameters for capturing live packet data; these are used the first time a capture is started.

The *Interface:* combo box lets you specify the interface from which to capture packet data, or the name of a FIFO from which to get the packet data. You can specify whether the interface is to be put in promiscuous mode or not with the *Capture packets in promiscuous mode* check box, can specify that the display should be updated as packets are captured with the *Update list of packets in real time* check box, and can specify whether in such a capture the packet list pane should scroll to show the most recently captured packets with the *Automatic scrolling in live capture* check box.

Protocol Preferences

There are also pages for various protocols that Ethereal dissects, controlling the way Ethereal handles those protocols.

The *Edit Capture Filter List* dialog lets you create, modify, and delete capture filters, and the *Edit Display Filter List* dialog lets you create, modify, and delete display filters.

The *Capture Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter to be used when capturing packets.

The *Display Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter to be used to filter the current capture being viewed.

The *Read Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter to be used to as a read filter for a capture file you open.

The *Search Filter* dialog lets you do all of the editing operations listed, and also lets you choose or construct a filter expression to be used in a find operation.

In all of those dialogs, the *Filter name* entry specifies a descriptive name for a filter, e.g. **Web and DNS traffic**. The *Filter string* entry is the text that actually describes the filtering action to take, as described above.The dialog buttons perform the following actions:

Capture Options

The *Capture Options* dialog lets you specify various parameters for capturing live packet data.

The *Interface:* field lets you specify the interface from which to capture packet data or a command from which to get the packet data via a pipe.

The *Limit each packet to ... bytes* check box and field lets you specify a maximum number of bytes per packet to capture and save; if the check box is not checked, the limit will be 65535 bytes.

The *Capture packets in promiscuous mode* check box lets you specify whether the interface should be put into promiscuous mode when capturing.

The *Filter:* entry lets you specify the capture filter using a tcpdump-style filter string as described above.

The *File:* entry lets you specify the file into which captured packets should be saved, as in the *Printer Options* dialog above. If not specified, the captured packets will be saved in a temporary file; you can save those packets to a file with the *File:Save As* menu item.

The *Use ring buffer* check box lets you specify that the capture should be done in ``ring buffer'' mode; the *Number of files* field lets you specify the number of files in the ring buffer.

The *Update list of packets in real time* check box lets you specify whether the display should be updated as packets are captured and, if you specify that, the *Automatic scrolling in live capture* check box lets you specify the packet list pane should automatically scroll to show the most recently captured packets as new packets arrive.

The *Stop capture after ... packet(s) captured* check box and field let you specify that Ethereal should stop capturing after having captured some number of packets; if the check box is not checked, Ethereal will not stop capturing at some fixed number of captured packets.

If ``ring buffer'' mode is not specified, the *Stop capture after ... kilobyte(s) captured* check box and field let you specify that Ethereal should stop capturing after the the file to which captured packets are being saved grows as large as or larger than some specified number of kilobytes (where a kilobyte is 1000 bytes, not 1024 bytes). If the check box is not checked, Ethereal will not stop capturing at some capture file size (although the operating system on which Ethereal is running, or the available disk space, may still limit the maximum size of a capture file).

If ``ring buffer'' mode is specified, that field becomes the *Rotate capture file very ... kilobyte(s)* field, and specifies the number of kilobytes at which to start writing to a new ring buffer file; the check box is forced to be checked, as ``ring buffer'' mode requires a file size to be specified.

The *Stop capture after ... second(s)* check box and field let you specify that Ethereal should stop capturing after it has been capturing for some number of seconds; if the check box is not checked, Ethereal will not stop capturing after some fixed time has elapsed.

The *Enable MAC name resolution*, *Enable network name resolution* and *Enable transport name resolution* check boxes let you specify whether MAC addresses, network addresses, and transport-layer port numbers should be translated to names.

Display Options

The *Display Options* dialog lets you specify the format of the time stamp in the packet list. You can select ``Time of day'' for absolute time stamps, ``Date and time of day'' for absolute time stamps with the date, ``Seconds since beginning of capture'' for relative time stamps, or ``Seconds since previous frame'' for delta time stamps. You can also specify whether, when the display is updated as packets are captured, the list should automatically scroll to show the most recently captured packets or not and whether addresses or port numbers should be translated to names in the display on a MAC, network and transport layer basis.

Exercise:

1. Connect your computer to a port on HP Ethernet switch.
2. Launch Ether Real Protocol Analyzer software.
3. Go to **Capture Menu** and click on **Start**. Another small window will open.
4. Uncheck the options ***Capture packets in promiscuous mode, Enable MAC name resolution, Enable network name resolution, Enable transport name resolution***.
5. Check the options ***Update list of packets in real time and Automatic scrolling in live capture.***
6. Click **OK**.
7. Capturing process will start immediately. Start a TELNET session.
8. Stop the capturing process and analyze the packets.
9. Repeat the same process for a HTTP session.
10. Connect your computer to a port on 3Com Ethernet hub and repeat the above.