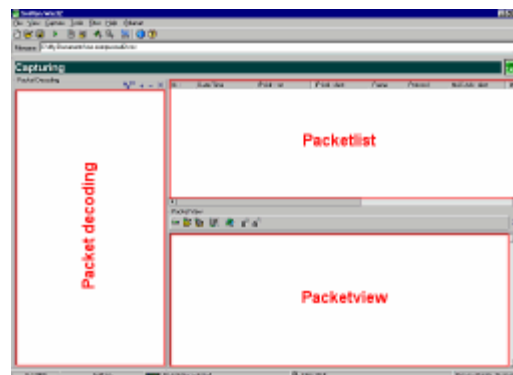


Sniff'em 1.01 Whitepaper

Graphical user Interface

Main Graphical user interface

Sniff'em™ uses a simple Graphical User interface, which allows simple usage while conserving powerful user manipulation. The main Graphical User Interface (GUI) is divided into three parts: The Packet list, Packet view and Packet decoding view.



Packet List

The Packet list pane displays incoming and outgoing Network packets in Chronological order.

```

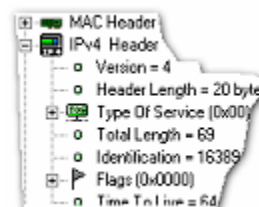
2  212.24.193.84  212.24.211.10  IP  TCP  20-53-52-43-00-00  44-45-53-5
3  212.24.211.10  212.24.193.84  IP  TCP  44-45-53-54-00-00  20-53-52-4
  
```

Additionally a right-click menu offers flexible options to Save, Edit Select, Remove, Invert, Export, Find, Refresh.



Packet Decoding

In the Packet Decoding view Packets are decoded and displayed in a Tree based structure. The main nodes are the different protocol Headers and Field values. These 3 panes interoperate based on User input, if you select a value from the Tree it will automatically show you where that value is located inside the raw Packet data in the Packet View by colouring the data parts of the packet in Blue.

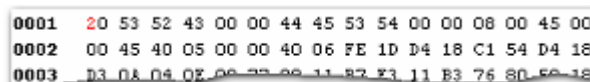


Double clicking a Tree view entry allows you to change the value of the selected field, which will immediately mirror the changes in the raw packet data and as such in the Packet view.



Packet View

The raw packet data will be represented in the Packet View, and Hexadecimal as well as an ASCII view on



the packet data. The selected Data part will be displayed as RED and is browsable by using your direction keys on your keyboard. BLUE values are displayed if a correspondent Packet Decoding Value has been selected. These values can be changed on the fly, by simply selecting the Packet view and typing on your keyboard, as such you are able to immediately change the contents of captured Network packets, even more, you are able to send them over the ether in the changed or original state.

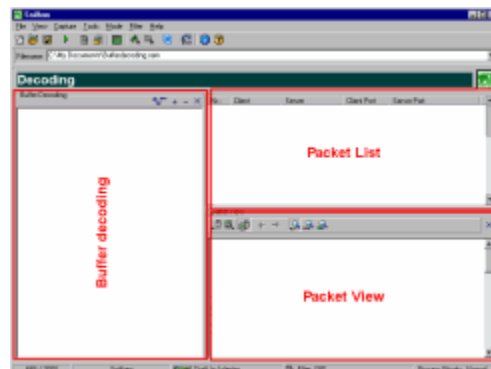
Again, a right-click menu offers flexible options such as New packet, Load packet, Save packet, Copy C style, Copy Packet style. The two copy options will copy to the raw packet data to the Clipboard, for further interaction.



Buffer Decoding

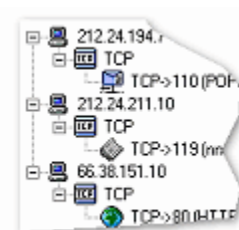
While the main Graphical user interface is a real-time display, the Buffer Decoding view does additional clustering, reassembly and decoding routines to offer a broad overview over the Network usage and Network captures currently within the Buffer.

The Buffer Size can be adjusted in the Settings menu, the more available RAM your PC configuration has the more Packets the Buffer can hold. Note that Sniff'em™ offers a way to open saved projects that has more packets than the Buffer can hold.



Buffer Decoding Tree

Buffer decoding is like the Packet decoding view Tree based structure representing the Source IP (Hostname or equivalent) together with the correspondent decoded protocols. Contrary to the Packet decoding view these protocols are session reassembled. As such, you are able to browse a whole Telnet session done by a host; you can follow exactly what they typed, in either ASCII, HEX or Packet data. The same goes for POP3, SMTP, IRC, IDENT, NETBEUI, DNS, HTTP and many more.



Packet List

The Packet List within the Buffer Decoding View shows the connections between Client and Server based on the protocol chosen, for instance if you choose POP3 for it is going to list all captured Network packets that were send from the selected IP to that Host using POP3 as Protocol. Furthermore it offers yet another right-click menu that lets you access the tagging

Nr.	Client	Server	Client Port	Server Port
1	66.38.151.10	212.24.193.84	80 (HTTP)	1098
2	66.38.151.10	212.24.193.84	80 (HTTP)	1099

feature of Sniff'em™ which is described in a paragraph at the bottom of this page.

Packet View

This view displays the content of the decoded Packets, as example, for HTTP, it shows all GET, POST requests and their response, for Telnet every command send and received. Note that you may choose if you only want to see the Received data, the Send data, or both, additionally you may view the content as plain ASCII or HEX or structured packet data.

```
GET /frames/ad.html?group=secnews&count=2 HTTP/1.0
Referer:
http://www.securityfocus.com/frames/ad.html?group=secn
Connection: Keep-Alive
User-Agent: Mozilla/4.73 [de]C-CKR-MCD DT (Win98; U)
Host: www.securityfocus.com
Accept: image/gif, image/x-bitmap, image/jpeg, image
```

Handy Feature Tagging

Right clicking on the Packet list within the Buffer Decoding view gives you the possibility to tag Session reassembled by Sniff'em™ and made visible inside the Main Graphical user interface.



The example bitmap shows a HTTP tagged packet and the result in the Main Graphical User Interface, note that you may tag five different Sessions which will have attributed five different coloured icons. Easy to spot these sessions within the Main graphical User Interface Packet List using this neafy feature.

