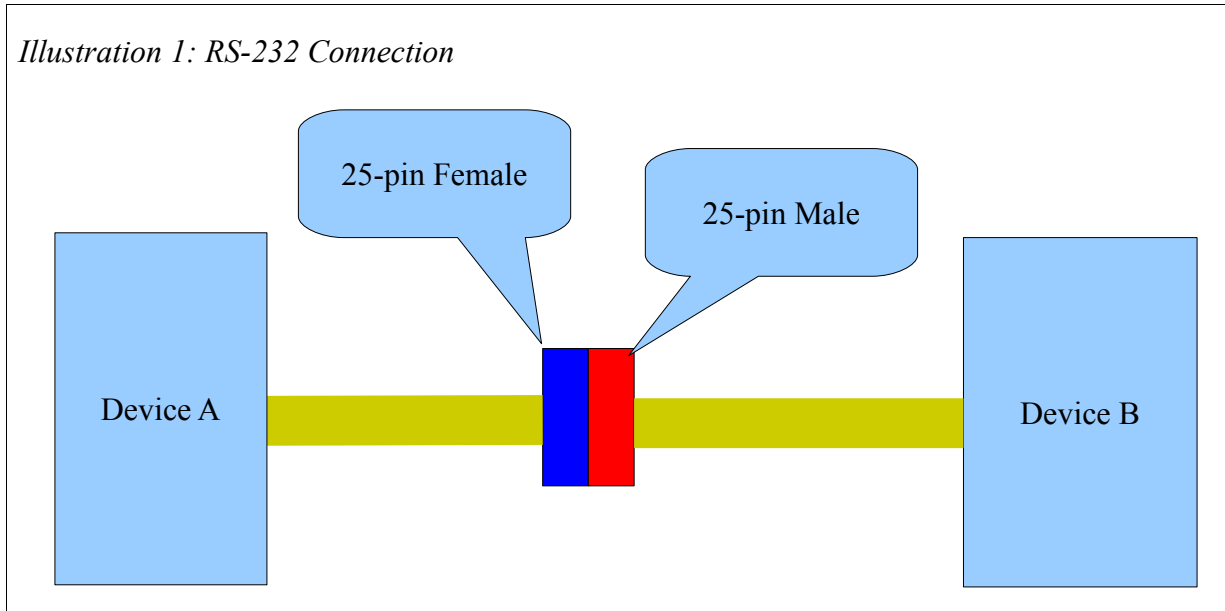
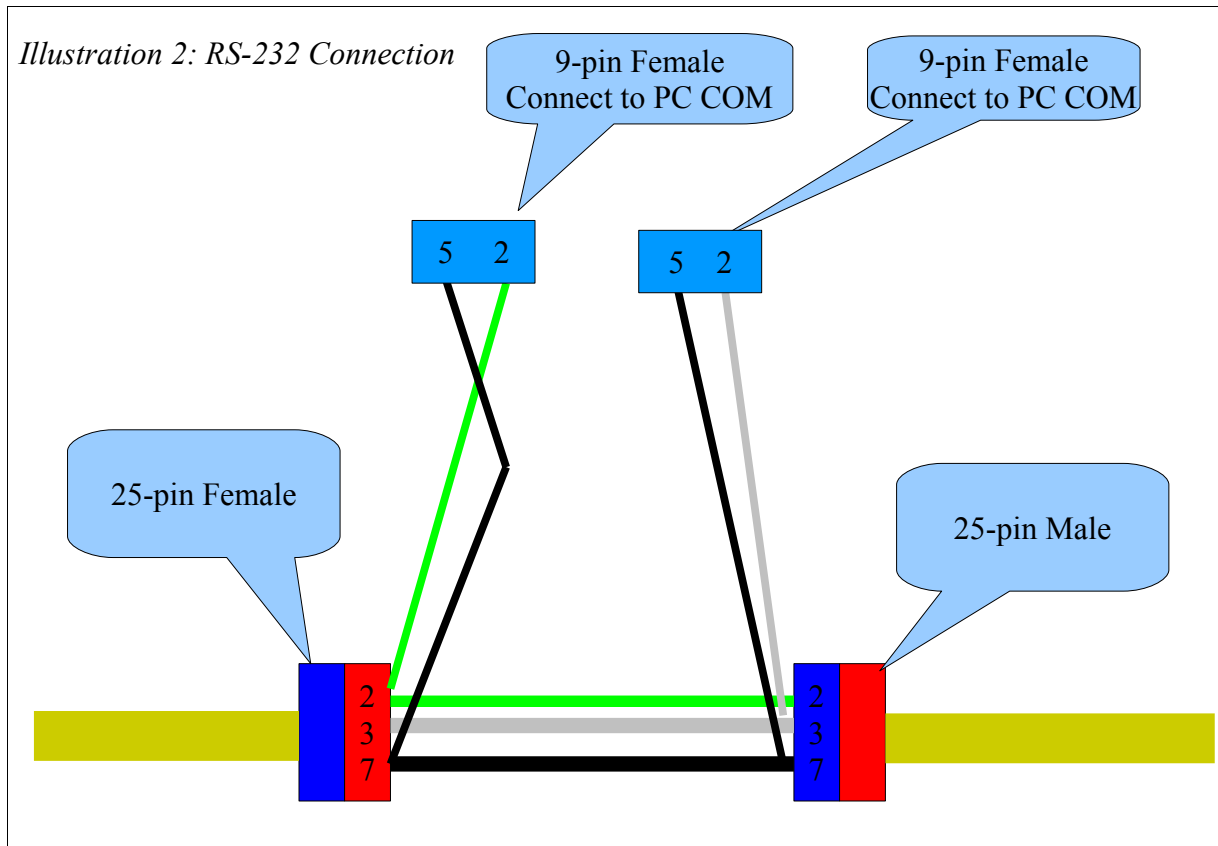


How to eavesdrop on a 25-pin RS-232 serial connection.

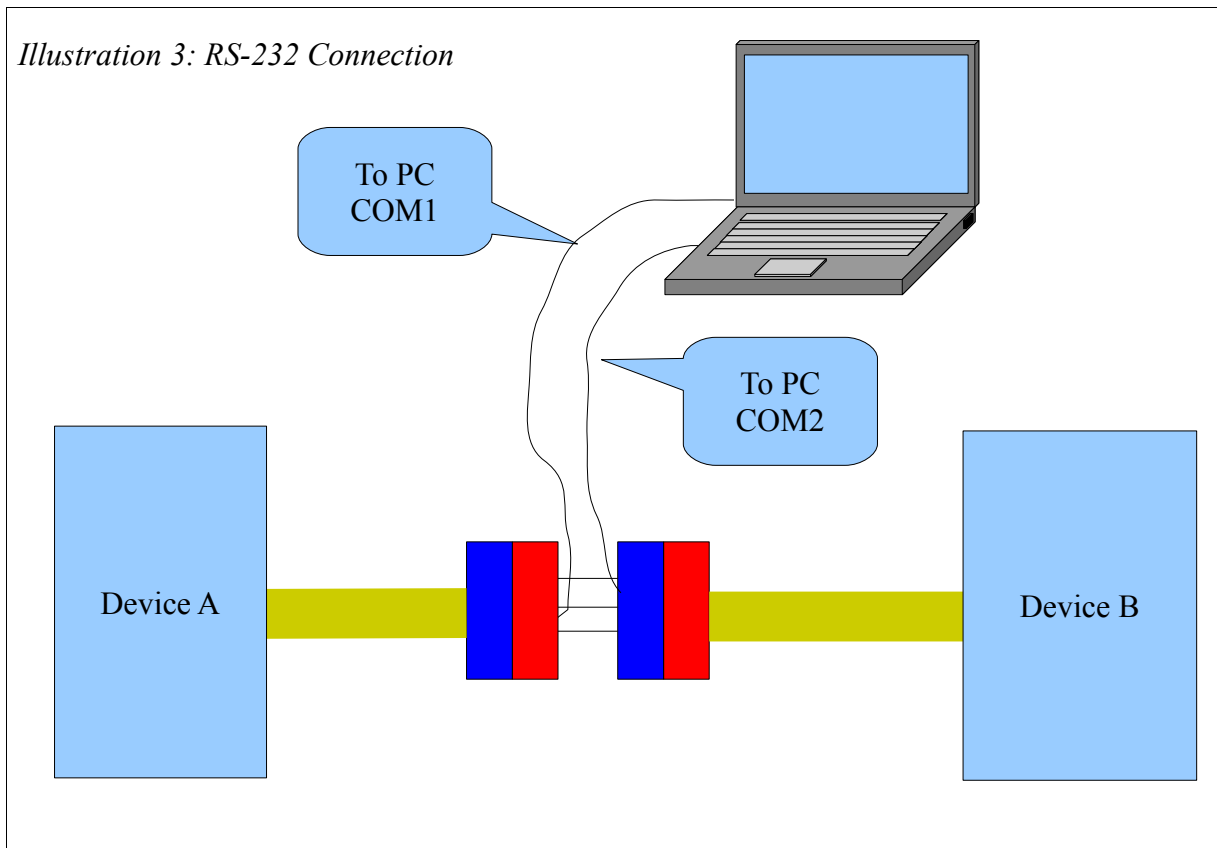
Illustration 1: RS-232 Connection shows a simple system with two RS-232 devices communicating through a 25-pin RS-232 connection.



It is simple to build an eavesdropping dongle to insert into the working system.



The wiring connection is quite simple – simply pass through pins 2-2 (green wire), 3-3 (gray wire) , and 7-7 (black wire) on the 25-pin male to female section. Then branch off pin 2 (green) to pin 2 on one of the 9-pin female connectors. The other monitor PC connector has pin 3 (gray) to pin 2 on the 9-pin female. Connect the pin 7 (black) ground wire to pin 5 on each 9-pin.

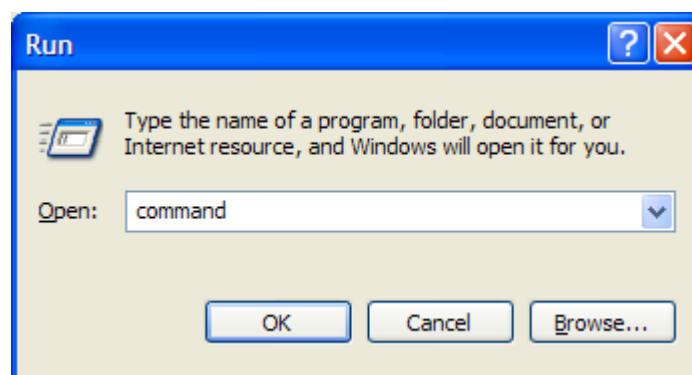


After connecting the cable to device A, B, and com1 and com2 of the PC, start the serial monitor eavesdropping program SERMON.EXE. You can get a copy from this link:

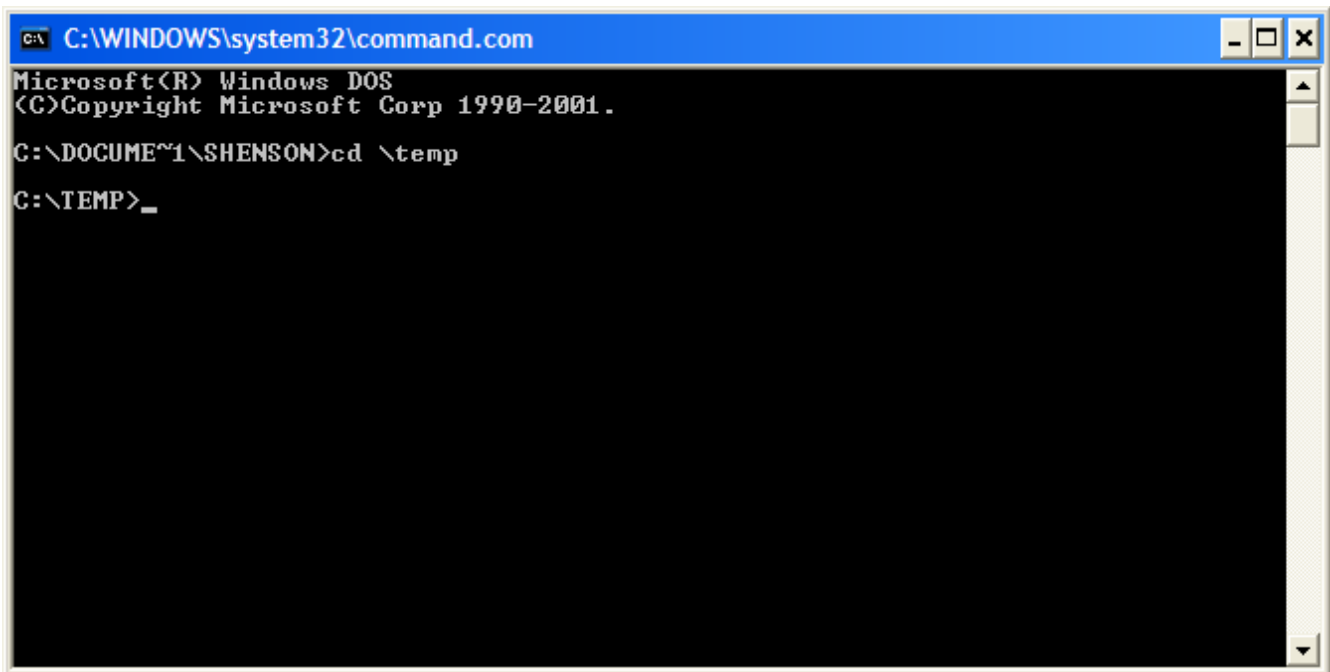
<http://www.niobrara.com/programs/SERMON.EXE>

Save this program in the c:\temp\ folder.

Now open a command prompt by selecting START>RUN>command



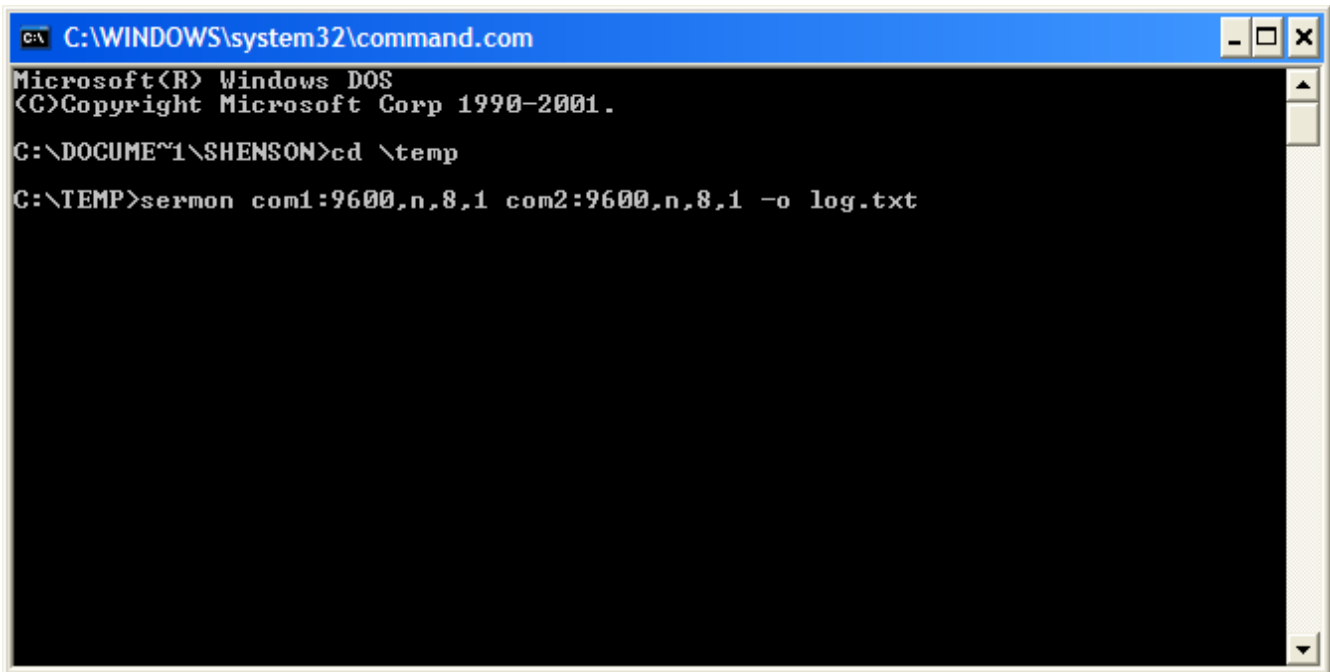
Now change directories to the c:\temp\ folder with the command cd \temp



```
C:\WINDOWS\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\DOCUMENTS\SHENSON>cd \temp
C:\TEMP>_
```

Now start the monitor program from the command line.

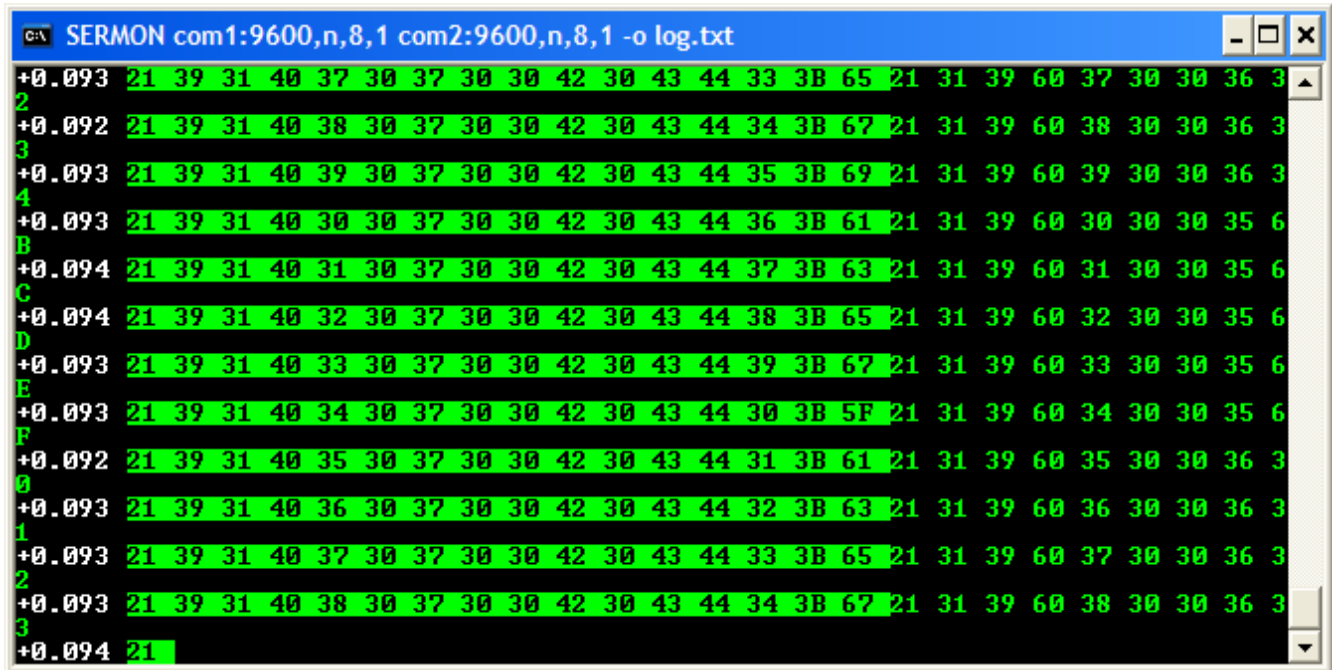
NOTE: if the PC's comm ports are not 1 and 2, simply insert the correct number in the command line.



```
C:\WINDOWS\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\DOCUMENTS\SHENSON>cd \temp
C:\TEMP>sermon com1:9600,n,8,1 com2:9600,n,8,1 -o log.txt
```

In the above example, the PC has COM1 and COM2 and the serial parameters of the 25-pin connection are 9600 baud, NONE parity, 8 data bits, and 1 stop bit. The -o option will also send the capture to the text file “log.txt”.

If there is communication in progress, the new window should look something like this:



The data from one serial port is inverted from the other. All the data is shown in hexadecimal. When there is a gap between characters of > 60mS, the time will be displayed at the front of a new line in white.

Viewing the capture log in Notepad will look something like this:

