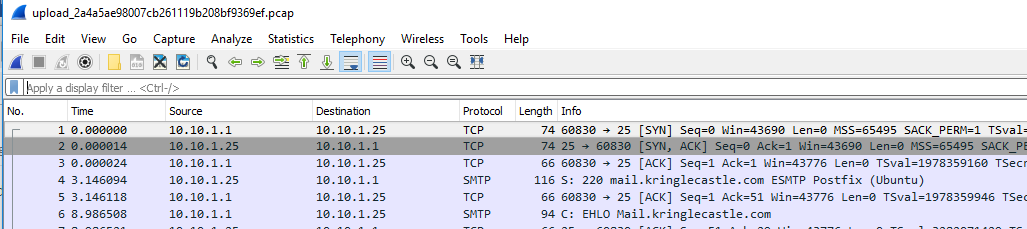
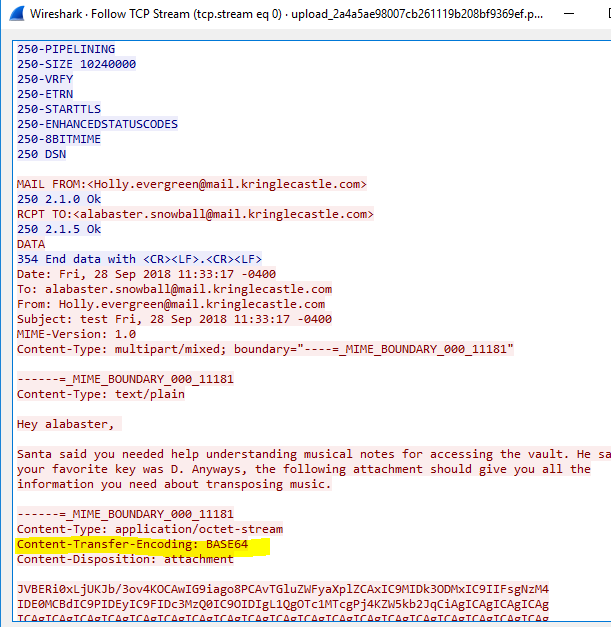
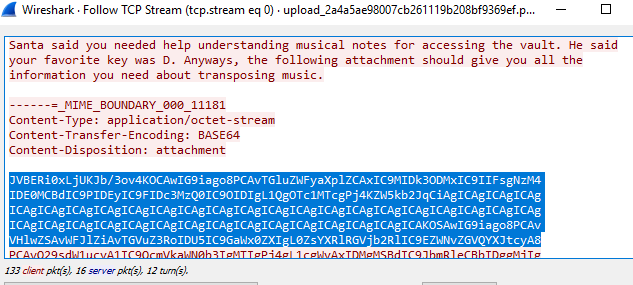
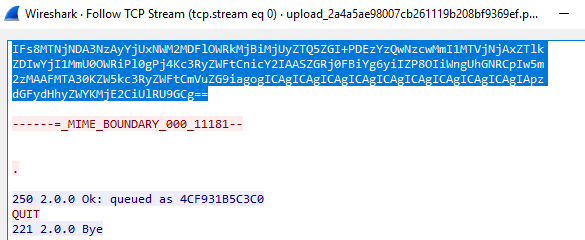
Objective--Network Traffic Forensics (Part 5)

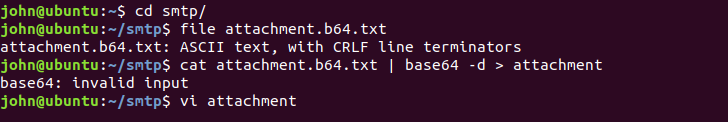
# Solution (at last!)

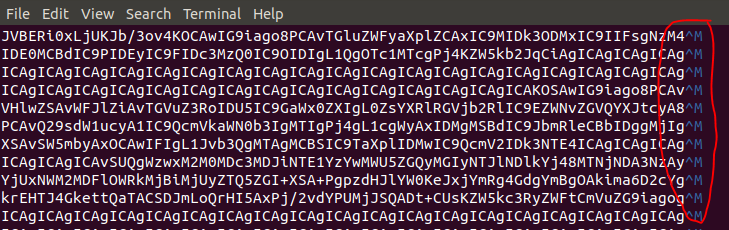
Now that we have the super\_secret\_packet\_capture.pcap file, we can answer the question. Wireshark shows that the file is one TCP stream, an unencrypted SMTP connection.  


Follow TCP > Stream gives us this.  


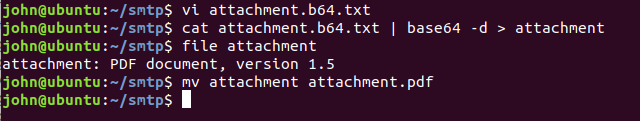
The attachment is encoded with BASE64, which is easy to decode. Select the top of the BASE64 text, then shift-click at the bottom and copy the BASE64 into a text editor.  
  
<snip>  


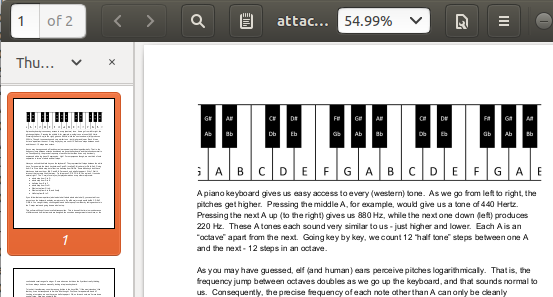
# Pasting files from Windows to Linux causes problems

I ran Wireshark in Windows and pasted the text to Linux; bad move.  




All those ^M characters cause problems. There is a fix. In vi, use :%s/[cntrl-V][cntrl-M]//g. This is similar to other Linux syntax for search and replace: s/searchfor/replacewith/g for global. Another way would be to use the translate command with -d for delete: tr -d ‘\r’ > file. Both ^M and \r mean “carriage return”. There’s another character, \n or line feed. At the end of lines Windows uses \r\n (carriage return, line feed, or CRLF) and Linux just uses \n. I should have done it all in Linux. What a pain.

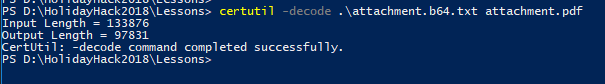
After fixing the ^M problems, it is easy to decode the file. 

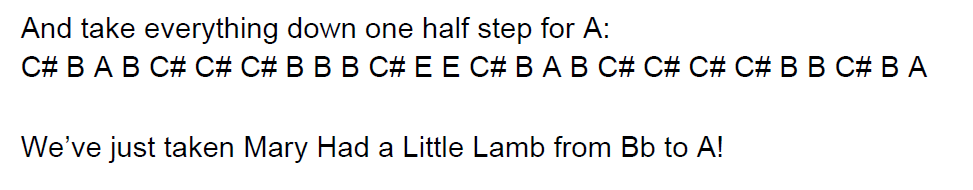


# Decoding Base64 in Windows

PowerShell can decode Base64, although the syntax is awkward. This will decode.  
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("U2VjcmV0TWVzc2FnZQ=="))

This will encode.  
[System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("SecretMessage"))

Windows certutil.exe is simpler if you don’t need a script.  


In either case, the end of the PDF file we extract has this.  


That’s a lot of work to find “Mary Had a Little Lamb”

# Up Next

We will need hints from Shinny Upatree and his Sleigh bell lottery terminal before we tackle the last objective. You can find him on the right side of the second floor, near the stairs.