Swimming with sharks

Goal

So far we've used Wireshark to capture live, familiar traffic on our computer. In this exercise we'll feel how it is to swim in strange waters - in someone else's traffic 🌊.

Background

You're a network analyst at the Network Forensics Operations Center (NFOC). The following email was received in our office today:

> Dear network analyst, My name is Alex Chan, and I am a lawyer from Singapore. My profession demands very high level of confidentiality, and I have to store all of my clients' data in the safest way possible.
>
> Recently I have learned about something called "Clear text protocols", which means that there are protocols which do not use encryption at all. If my computer uses any of these protocols, it might send out personal information like usernames, passwords or documents *unencrypted*. Having this kind of data exposed could be extremely harmful for my business.
>
> At your request, I have activated Wireshark for an hour and created a pcap file which is attached. During the capture time I've used Mail, An online Oracle database, My private website and Uploaded some files to a file server.
>
> I have no idea how to analyze all this data. Please, if you would be kind enough to analyze this and see if any private data was leaked.
>
> Thank you, alex@chanltd.com.sg

Instructions

Your goal is to analyze Alex's "alex.pcap", and find private information (names, addresses, passwords, etc) that was sent unencrypted. Write a report with all the screenshots of the data leaks you have found.

Hint:

- The format for saved Wireshark captures is called **PCAP**.
- To learn about clear text protocols, use Google!
- Don't forget to use filters! Port filters could be very handy here.
- Find between 3-4 leaks.

Alex is waiting for your report. Good luck!

To submit

Submit a word document with your report.

Sentinel