# Lab 06 - Email

In this lab examine a PST captured during the intellectual property theft case that's been used throughout the text.

We will be using the vApp in the IA Lab labeled <username>\_CSC388\_Zwach\_Email. All files for this lab are in the \Users\DSU\Desktop\Evidence directory of the Windows VM.

## Deliverables

A single new Word or PDF document containing:

* Reponses to lab steps 2-7, lab step 9, and the writing prompts

## Lab Steps

1. Load Jim Shu's PST in OS Forensics.
2. How many emails are in the deleted items folder?

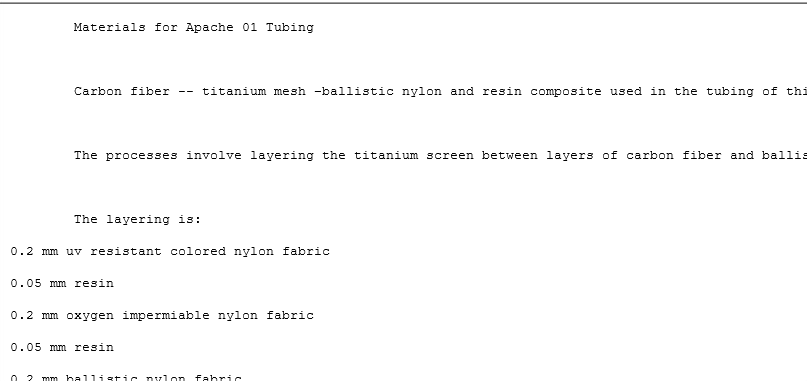
3

1. How many emails are *<recovered>*?

6

1. Do any emails contain content related to the IP theft alleged throughout the book? If so, what is the content?

in the recovered emails there’s a string of emails with Sam Spade buying some bike frame specs for something in the range of 10k dollars



1. How many emails did Jim Shu receive from Sam Spade?

4

1. How many emails did Jim Shu send to Sam Spade?

2

1. What sort of attachments do you see on the various emails?

An image file with some strange sketch, and an rtf file with what looks like manufacturing specifications for a bike frame.

1. Process Jim Shu's PST in Autopsy
2. How many total different email addresses were found?

12 unique addresses were found

## Writing Prompts

1. Is it easy to identify the emails between Jim and Sam? Why or why not?

In OSForensics they were separated out as recovered, which highlighted them making it pretty easy.

1. Based on this brief experience, do you think it's practical as an investigator to review all email for a particular suspect inbox or would you focus more on keyword and date range searches? Why?

I would say it’s practical as an investigator to focus on keyword searches within date ranges, especially in modern contexts where inboxes are lined with hundreds of spam emails every day... going through every message would be ludicrous.

1. Compare and contrast your experiences using Autopsy and OS Forensics to explore the PST. What appeared to be the strengths and weaknesses of each?

OS forensics makes it easy to search the PST, and review individual emails matching our filters. Autopsy gives a good overview of the whole inbox, stripping out attatchements, summarizing unique email addresses and enumerating the communications with them, etc.

## Notes

* Feel free to explore the other files in the Evidence directory as well