Network Forensics

## Summary

This lab uses Wireshark to perform a forensic analysis of an email network capture between Alice and an unknown associate.

## Tools/Resources

Wireshark, preinstalled on Parrot

## Tasks

**Story**

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

“We believe Ann may have communicated with her secret lover, Mr. X, before she left,” says the police chief. “The packet capture may contain clues to her whereabouts.”

You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence.

The evidence packet capture is in the class files on canvas ([Lab18-evidence.pcap](https://mycourses.unh.edu/courses/124903/files/11819946?wrap=1))

* Provide answers to the following questions in a DOCX or PDF submitted to Canvas
  + What is Ann’s email address?
  + What is Ann’s email password?
  + What is Ann’s secret lover’s email address?
  + What two items did Ann tell her secret lover to bring?
  + What is the NAME of the attachment Ann sent to her secret lover?
  + What is the MD5sum of the attachment Ann sent to her secret lover?
  + In what CITY and COUNTRY is their rendezvous point?
  + What is the MD5sum of the image embedded in the document?
    - Hint: The correct answer is **NOT**: e3001a972e718aebb75ba070b1e5434c

## Submission

Upload to Canvas the answers to the questions.

## Walkthrough

1. Download pcap: <https://mycourses.unh.edu/files/11819946/download?download_frd=1>
2. Load into Wireshark

A screenshot of a computer

Description automatically generated

1. What is Ann’s email address? [sneakyg33k@aol.com](mailto:sneakyg33k@aol.com)

Filter smtp packets then follow email stream (note there is more than one email stream). The timestamps are a good indication which packet belong to which smtp stream.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. What is Ann’s email password? 558r00lz

Decode the base64, this deletes various whitespace not part of the actual attachment.

A screenshot of a computer program

Description automatically generated

1. What is Ann’s secret lover’s email address? [mistersecretx@aol.com](mailto:mistersecretx@aol.com)

Needed second email

A screenshot of a computer

Description automatically generated

Same base64 process as previous step.

1. What two items did Ann tell her secret lover to bring? A fake passport and a bathing suit

Just read the email details

A screenshot of a computer

Description automatically generated

1. What is the NAME of the attachment Ann sent to her secret lover? secretrendezvous.docx

Again, read the mail details

1. What is the MD5sum of the attachment Ann sent to her secret lover?

Cut and paste the base64 in the email stream to ann.b64, the here doc trick works well. Then convert the b64 and open the docx

A computer screen with green and white text

Description automatically generated

1. In what CITY and COUNTRY is their rendez-vous point? Playa del Carmen, Mexico

A map with red dots and a map with a picture of a boat

Description automatically generated with medium confidence

1. What is the MD5sum of the image embedded in the document? aadeace50997b1ba24b09ac2ef1940b7

Export of the image does NOT work as it alters the image. Unzip the docx then take the md5

A screenshot of a computer screen

Description automatically generated

## Additional Thoughts

How does UNH’s current email implementation protect against password discovery? UNH email client is HTTPS not SMTP based.

Why does SMTP send passwords in the clear? 1) Connections to the server were considered physically secured. 2) The overhead of encryption was considered too difficult/expensive.

Why is the image MD5 not e3001a972e718aebb75ba070b1e5434c? Word changes the image resolution when saving, thus impacting the md5.