**EXIF Tool Review**

Take this image and find information related to these images:

**Image 1:** <https://www.exiv2.org/include/img_1771.jpg>

**Image 2:** <https://res.cloudinary.com/demo/image/upload/exif_sample.jpg>

1. What kind of camera was used to take this photo?
2. What kind of lens was used?
3. Was the flash used?
4. If applicable, what are the latitude and longitude?
5. What is the exact date and time this picture was taken?
6. What type of file is this?

**Stepic Review**

1. Decode the message in the image encrypted\_puppy.png

**Challenge through PCAP: Part 1**

*Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company’s prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company’s secret recipe.*

*Security staff have been monitoring Ann’s activity for some time, but haven’t found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann’s computer, (192.168.1.158) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.*

*“We have a* [*packet capture*](http://forensicscontest.com/contest01/evidence01.pcap) *of the activity,” said security staff, “but we can’t figure out what’s going on. Can you help?”*

You are the forensic investigator. Your mission is to figure out who Ann was IM-ing, what she sent, and recover evidence including:

1. What is the name of Ann’s IM buddy?

2. What was the first comment in the captured IM conversation?

3. What is the name of the file Ann transferred?

4. What is the magic number of the file you want to extract (first four bytes)?

5. What was the MD5sum of the file?

6. What is the secret recipe?

Here is your [evidence file](http://forensicscontest.com/contest01/evidence01.pcap):

<http://forensicscontest.com/contest01/evidence01.pcap>

MD5 (evidence.pcap) = d187d77e18c84f6d72f5845edca833f5

**Challenge through PCAP: Part 2**

*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*](http://forensicscontest.com/contest02/evidence02.pcap) *may contain clues to her whereabouts.” (Go download the file named evidence02.pcap)*

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

1. What is Ann’s email address?

2. What is Ann’s email password?

3. What is Ann’s secret lover’s email address?

4. What two items did Ann tell her secret lover to bring?

5. What is the NAME of the attachment Ann sent to her secret lover?

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

7. In what CITY and COUNTRY is their rendezvous point?

8. What is the MD5sum of the image embedded in the document?

**Challenge through PCAP: Part 3**

*Ann and Mr. X have set up their new base of operations. While waiting for the extradition paperwork to go through, you and your team of investigators covertly monitor her activity. Recently, Ann got a brand new AppleTV, and configured it with the static IP address 192.168.1.10.* [*Here is the packet capture*](http://forensicscontest.com/contest03/evidence03.pcap) *with her latest activity.*

You are the forensic investigator. Your mission is to find out what Ann searched for, build a profile of her interests, and recover evidence including:

1. What is the MAC address of Ann’s AppleTV?

2. What User-Agent string did Ann’s AppleTV use in HTTP requests?

3. What were Ann’s first four search terms on the AppleTV (all incremental searches count)?

4. What was the title of the first movie Ann clicked on?

5. What was the full URL to the movie trailer (defined by “preview-url”)?

6. What was the title of the second movie Ann clicked on?

7. What was the price to buy it (defined by “price-display”)?

8. What was the last full term Ann searched for?