**ANSWERS**

**Exif Tool:**

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

1. What kind of camera was used to take this photo?
   1. Canon PowerShot S40
2. What kind of lens was used?
   1. 7.1 - 21.3 mm shot at 21.3 mm
3. Was the flash used?
   1. Auto, Did not fire
4. If applicable, what are the latitude and longitude?
   1. N/A
5. What is the exact date and time this picture was taken?
   1. December 14, 2003 12:01:44PM (timezone not specified)
   2. (16 years, 7 months, 7 days, 1 hour, 46 minutes, 56 seconds ago, assuming image timezone of US Pacific)
6. What type of file is this?
   1. 480 × 360 JPEG
   2. 32,764 bytes (32 kilobytes)

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

1. What kind of camera was used to take this photo?
   1. Apple iPhone 4
2. What kind of lens was used?
   1. 3.9 mm
3. Was the flash used?
   1. Auto, Did not fire
4. If applicable, what are the latitude and longitude?
   1. Latitude/longitude: 21° 7' 40.8" North, 86° 45' 0" West ( 21.128000, -86.750000 )
   2. Altitude: 22 meters (74 feet)
   3. Camera Pointing: East-southeast
5. What is the exact date and time this picture was taken?
   1. December 27, 2010 11:17:34AM
6. What type of file is this?
   1. 2,592 × 1,936 JPEG (5.0 megapixels)
   2. 2,304,239 bytes (2.2 megabytes)

**Stepic Review:**

I'm the cutest puppy ever! Congrats on decrypting my special message :)

**Challenge through PCAP: Part 1**

1. What is the name of Ann’s IM buddy?
   1. sec558user1
2. What was the first comment in the captured IM conversation?
   1. Here’s the secret recipe… I just downloaded it from the file server. Just copy to a thumb drive and you’re good to go >:-)
3. What is the name of the file Ann transferred?
   1. recipe.docx
4. What is the magic number of the file you want to extract (first four bytes)?
   1. 0x504B0304 (Note: one byte = 8 bits = 2 hex digits!)
5. What was the MD5sum of the file?
   1. 8350582774e1d4dbe1d61d64c89e0ea1
6. What is the secret recipe?
   1. Recipe for Disaster:
      1. 1 serving
   2. Ingredients:
      1. 4 cups sugar
      2. 2 cups water
      3. In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

**Challenge through PCAP: Part 2**

[**Challenge through PCAP: Part 2 Answers**](https://blogs.itb.ac.id/18212018tiaradwiputriii4033forensikdigitalsem1t15d16/2015/11/30/anns-aurora-ann-skips-bail-challenge/)

1. What is Anna’s email address?
   1. sneakyg33k@aol.com
2. What is Anna’s email password?
   1. 558r00lz
3. What is Annâ€™s secret loverâ€™s email address?
   1. mistersecretx@aol.com
4. What two items did Ann tell her secret lover to bring?
   1. A fake passport and a bathing suit
5. What is the NAME of the attachment Ann sent to her secret lover?
   1. secretrendezvous.docx
6. What is the MD5sum of the attachment Ann sent to her secret lover?
   1. 9e423e11db88f01bbff81172839e1923
7. In what CITY and COUNTRY is their rendez-vous point?
   1. Playa del Carmen, Mexico
8. What is the MD5sum of the image embedded in the document?
   1. aadeace50997b1ba24b09ac2ef1940b7

**Challenge through PCAP: Part 3**

[**Challenge through PCAP: Part 3 Answers**](https://blogs.itb.ac.id/18212018tiaradwiputriii4033forensikdigitalsem1t15d16/2015/12/10/sans-forensic-challenges-puzzle-3-anns-appletv/)

1. What is the MAC address of Ann’s AppleTV?
   1. 00:25:00:fe:07:c4 (002500fe07c4 will also be accepted)
2. What User-Agent string did Ann’s AppleTV use in HTTP requests?
   1. AppleTV/2.4
3. What were Ann’s first four search terms on the AppleTV (all incremental searches count)?
   1. h
   2. ha
   3. hac
   4. hack
4. What was the title of the first movie Ann clicked on?
   1. Hackers
5. What was the full URL to the movie trailer (defined by “preview-url”)?
   1. http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640×278.h264lc.d2.p.m4v
6. What was the title of the second movie Ann clicked on?
   1. Sneakers
7. What was the price to buy it (defined by “price-display”)?
   1. $9.99
8. What was the last full term Ann searched for?
   1. iknowyourewatchingme